

Посібник користувача Серія Horus E2

Мультибіометричний термінал контролю доступу

Дякуємо, що обрали наш продукт. Будь ласка, уважно прочитайте інструкцію перед початком роботи. Дотримуйтесь цих інструкцій, щоб забезпечити належну роботу пристрою. Зображення, наведені в цьому посібнику, слугують лише для ілюстрації.



Про компанію

ZKTeco є одним із найбільших у світі виробників зчитувачів RFID та біометричних даних (відбитків пальців, обличчя, вен долонь). Асортимент продукції включає зчитувачі та панелі контролю доступу, камери розпізнавання обличчя ближньої та дальньої дії, контролери доступу до ліфтів/поверхів, турнікети, контролери воріт розпізнавання номерних знаків (LPR) та споживчі товари, включно з дверними замками з живленням від батареї, які зчитують відбитки пальців та обличчя. Наші рішення безпеки є багатомовними та локалізовані понад 18 різними мовами. На сучасному, сертифікованому за стандартом ISO9001 виробничому комплексі ZKTeco площею 700 000 квадратних футів, ми контролюємо виробництво, дизайн продукції, збирання компонентів, а також логістику/доставку — все під одним дахом.

Засновники ZKTeco були налаштовані на незалежні дослідження та розробки процедур біометричної верифікації та перетворення на продукти SDK для біометричної верифікації, які спочатку широко застосовувалися у сфері безпеки ПК та аутентифікації особистості. З постійним вдосконаленням розробок та великою кількістю ринкових застосувань, команда поступово створила екосистему аутентифікації особистості та екосистему розумної безпеки, що ґрунтуються на технологіях біометричної верифікації. Маючи багаторічний досвід в індустріалізації біометричної верифікації, компанію ZKTeco було офіційно засновано у 2007 році, і зараз вона є одним із світових лідерів у галузі біометричної верифікації, володіючи різними патентами та будучи обраною Національним високотехнологічним підприємством протягом 6 років поспіль. Її продукція захищена правами інтелектуальної власності.

Про Посібник

У цьому посібнику описано роботу мультибіометричного терміналу контролю доступу Horus серії E2.

Всі зображення наведені виключно для ілюстрації. Зображення в цьому посібнику можуть не відповідати фактичним продуктам.

Функції та параметри з позначкою ★ доступні не на всіх пристроях.

Умовні позначення

У цьому посібнику використовуються такі символи:

Угоди про графічний інтерфейс

Для програмного забезпечення	
Позначення	Опис
Жирний шрифт	Використовується для ідентифікації назв інтерфейсів програмного забезпечення OK , Confirm (Підтвердити), Cancel (Скасувати).
>	Багаторівневі меню розділяються цими дужками. Наприклад, File (Файл) > Create (Створити) > Folder (Папка).
Для пристрою	
Позначення	Опис
< >	Назви кнопок або клавіш для пристроїв. Наприклад, натисніть <OK>.
[]	Назви вікон, пункти меню, таблиці даних та назви полів знаходяться в квадратних дужках. Наприклад, відкрийте вікно [New User] (Новий користувач).
/	Багаторівневі меню розділяються косими рисками. Наприклад, [File/ Create/Folder] (файл/створити/папка)].

Символи

Позначення	Опис
	Це примітка, на яку слід звернути більше уваги.
	Загальна інформація, яка допомагає швидше виконувати операції.
	Інформація, яка є важливою.
	Уникнути небезпеки та помилок.
	Заява або подія, яка попереджає про щось або служить застережливим прикладом.

Зміст

1	ОГЛЯД	8
2	ІНСТРУКЦІЯ З ЕКСПЛУАТАЦІЇ	8
	2.1 ПОЛОЖЕННЯ СТОЯЧИ, ВИРАЗ ОБЛИЧЧЯ ТА ПОСТАВА СТОЯЧИ.....	8
	2.2 РОЗТАШУВАННЯ ПАЛЬЦІВ★.....	10
	2.3 РЕЄСТРАЦІЯ ШАБЛОНУ ОБЛИЧЧЯ	10
	2.4 РЕЗЕРВНИЙ ІНТЕРФЕЙС.....	11
	2.5 ВІРТУАЛЬНА КЛАВІАТУРА	12
	2.6 РЕЖИМ ВЕРИФІКАЦІЇ	12
	2.6.1 ВЕРИФІКАЦІЯ ПАРОЛЯ.....	13
	2.6.2 ВЕРИФІКАЦІЯ ОБЛИЧЧЯ.....	14
	2.6.3 ВЕРИФІКАЦІЯ ВІДБИТКІВ ПАЛЬЦІВ ★.....	16
	2.6.4 ВЕРИФІКАЦІЯ КАРТКИ.....	18
3	ГОЛОВНЕ МЕНЮ	21
4	КЕРУВАННЯ КОРИСТУВАЧАМИ	22
	4.1 ДОДАТИ КОРИСТУВАЧА	22
	4.1.1 ДОДАВАННЯ КОРИСТУВАЧІВ ЧЕРЕЗ ПРИСТРІЙ.....	22
	4.2 ПОШУК КОРИСТУВАЧА	35
	4.3 РЕДАГУВАННЯ КОРИСТУВАЧА	36
	4.4 ВИДАЛЕННЯ КОРИСТУВАЧА	36
5	НАЛАШТУВАННЯ ДОСТУПУ	38
	5.1 ОПЦІЇ КОНТРОЛЮ ДОСТУПУ	38
	5.2 НАЛАШТУВАННЯ ПРАВИЛ ЧАСУ	39
	5.3 НАЛАШТУВАННЯ СВЯТКОВИХ ДНІВ	41
	5.4 НАЛАШТУВАННЯ ЗАХИСТУ ВІД ПОВТОРНОГО ПРОХОДЖЕННЯ	43
6	ЗАПИСИ КОНТРОЛЮ ДОСТУПУ	45
7	КЕРУВАННЯ ДАНИМИ	46
8	КЕРУВАННЯ СИГНАЛАМИ ТРИВОГИ	48
	8.1 ДОДАТИ СИГНАЛ ТРИВОГИ	48
	8.2 ВИДАЛЕННЯ СИГНАЛУ ТРИВОГИ	49
9	НАЛАШТУВАННЯ СИСТЕМИ	50

9.1 НАЛАШТУВАННЯ МЕРЕЖІ	50
9.1.1 НАЛАШТУВАННЯ ETHERNET.....	51
9.1.2 НАЛАШТУВАННЯ WI-FI.....	52
9.1.3 МОБІЛЬНА МЕРЕЖА.....	52
9.2 ДАТА І ЧАС	52
9.2.1 НАЛАШТУВАННЯ ДАТИ ТА ЧАСУ.....	52
9.2.2 НАЛАШТУВАННЯ ЧАСОВИХ ЗОН.....	54
9.2.3 НАЛАШТУВАННЯ ФОРМАТУ ДАТИ ТА ЧАСУ.....	55
9.3 НАЛАШТУВАННЯ ЗАПИСІВ КОНТРОЛЮ ДОСТУПУ	56
9.3.1 РЕЖИМ КАМЕРИ.....	57
9.3.2 НАЛАШТУВАННЯ ВЕРИФІКАЦІЇ.....	58
9.3.3 ТЕРМІН ДІЇ ІНФОРМАЦІЇ ПРО КОРИСТУВАЧА.....	59
9.4 НАЛАШТУВАННЯ ХМАРНОГО СЕРВІСУ	59
9.5 НАЛАШТУВАННЯ WIEGAND	60
9.5.1 WIEGAND ВХІД.....	61
9.5.2 WIEGAND ВИХІД	63
9.6 НАЛАШТУВАННЯ ДИСПЛЕЯ	64
9.7 НАЛАШТУВАННЯ СЕРІЙНОГО ПОРТУ	65
9.8 НАЛАШТУВАННЯ ЗВУКУ	66
9.9 БІОМЕТРИЧНІ ПАРАМЕТРИ	66
9.10 АВТОМАТИЧНЕ ТЕСТУВАННЯ	69
9.11 РОЗШИРЕНІ НАЛАШТУВАННЯ	71
9.12 ПРО ПРИСТРІЙ	72
9.13 НАЛАШТУВАННЯ БЕЗПЕКИ	73
9.14 ПЕРЕЗАПУСК	74
10 ПІДКЛЮЧЕННЯ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ZKBIO CVACCESS	75
10.1 ВСТАНОВЛЕННЯ АДРЕСИ ДЛЯ КОМУНІКАЦІЇ	75
10.2 ДОДАТИ ПРИСТРІЙ У ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ	76
10.3 ДОДАТИ ПЕРСОНАЛ У ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ	77
ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ	78
ЕКОЛОГІЧНО ЧИСТА ЕКСПЛУАТАЦІЯ	80

1 Огляд

Horus E2 від ZKTeco — це мультибіометричний термінал на базі Android, призначений для оптимізації обліку робочого часу та контролю доступу. Використовуючи передові технології ZKTeco, Horus E2 підтримує різноманітні методи аутентифікації, включаючи розпізнавання обличчя, сканування відбитків пальців, перевірку мультитехнологічних карток та сканування QR-кодів. Ці функції задовольняють різноманітні потреби користувачів у різних середовищах. Пристрій забезпечує надійне підключення завдяки двочастотному Wi-Fi та LTE, що полегшує безперебійну інтеграцію в мережу. Horus E2 сумісний з операційною системою Android 10, що спрощує інтеграцію з сторонніми додатками. Крім того, він включає в себе опціональний знімний резервний акумулятор, що підвищує його надійність і робить його ідеальним рішенням для мобільного обліку робочого часу та тимчасового управління об'єктом.

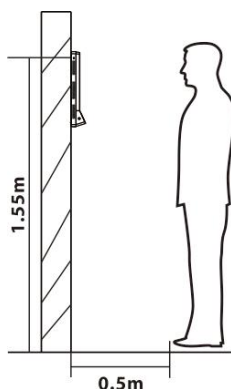
Horus E2 стандартно комплектується картковим модулем B133, який підтримує ідентифікаційні ID-картки та IC-картки. Horus E2 також ідеально підтримує картковий модуль Elatec і може підтримувати RFID-картки 125 кГц/134,2 кГц/13,56 МГц без заміни карткового модуля.

Якщо вищезазначена функція не відповідає потребам клієнтів, ми можемо надати вбудований комплект для розробки EDK та інструменти для налаштування. На основі нашої надійної та стабільної платформи команда дослідників і розробників клієнта може швидко розробити, інтегрувати та налагодити всю вбудовану систему для кращої масштабованості.

2 Інструкція з використання

2.1 Положення стоячи, вираз обличчя та постава стоячи

Рекомендована відстань

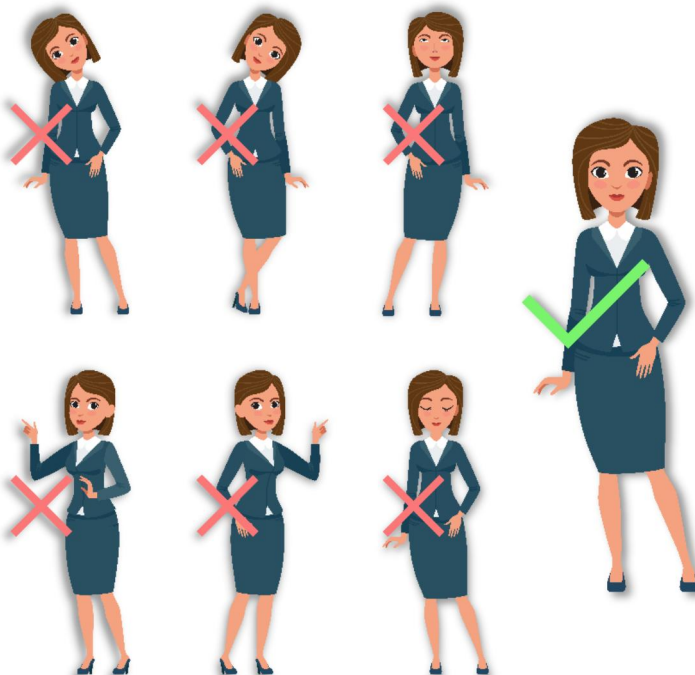


Відстань між пристроєм і користувачем (зріст якого становить від 1,55м до 1,85м) має становити 1,5м. Користувачі можуть трохи нахилитися вперед і назад, щоб поліпшити якість знятих зображень обличчя.

Рекомендовані вирази обличчя



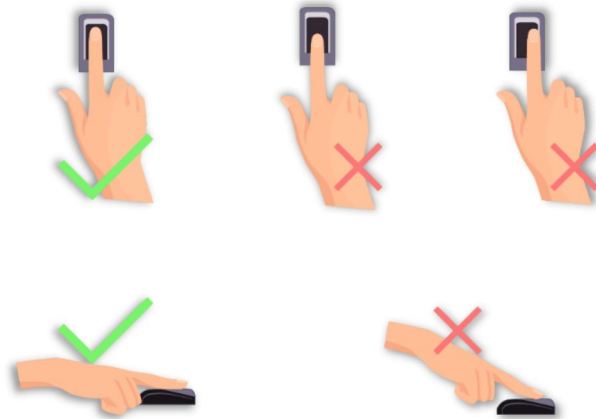
Рекомендовані пози стоячи



 **Примітка:** Під час реєстрації та перевірки, будь ласка, зберігайте природний вираз обличчя та поставу.

2.2 Розташування пальців ★

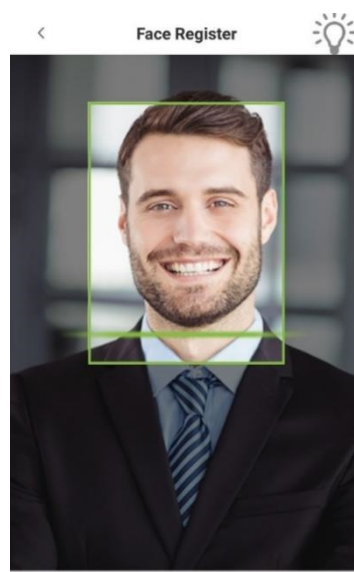
- **Рекомендовані пальці:** Вказівний, середній або безіменний пальці.
- Уникайте використання великого або мізинця, оскільки ними важко точно натиснути на сканер відбитків пальців.



 **Примітка:** Будь ласка, використовуйте правильний метод при натисканні пальцями на сканер відбитків пальців для реєстрації та ідентифікації.

2.3 Реєстрація шаблону обличчя

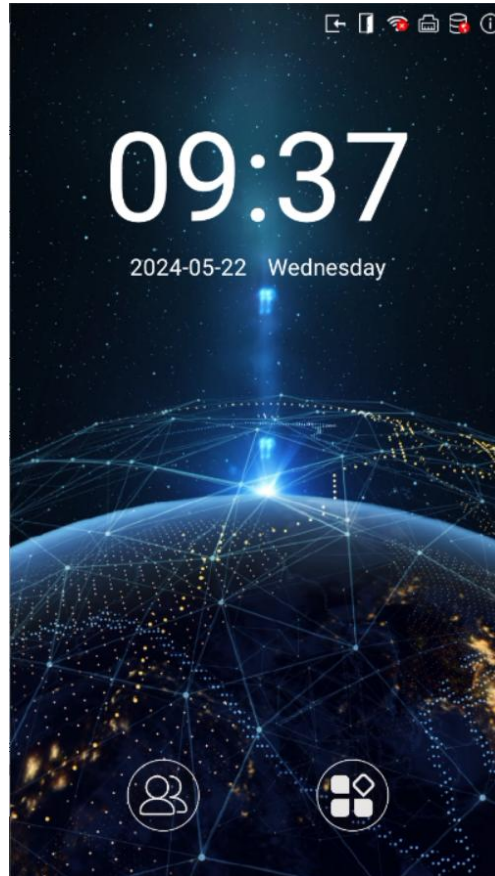
Під час реєстрації спробуйте розмістити своє обличчя в центрі екрана пристрою. Будь ласка, дивіться в камеру і не рухайтесь. Екран пристрою показано нижче:



Вирівняйте обличчя як показано відповідно у показаному прямокутнику

2.4 Інтерфейс режиму очікування

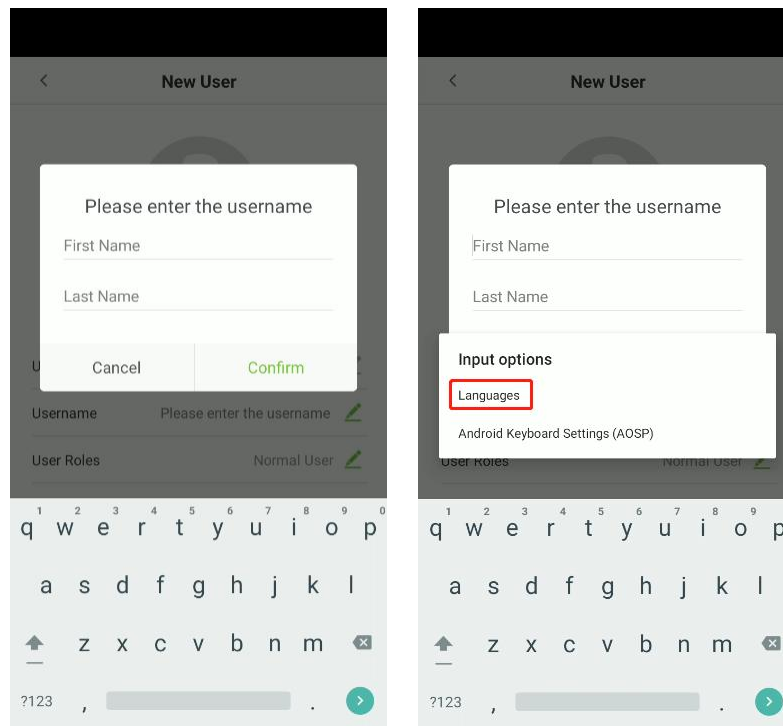
Після підключення джерела живлення пристрій відображає наступний інтерфейс режиму очікування.



Примітки:

1. Натисніть на  кнопку для входу в екран введення ідентифікаційного номера персоналу.
2. Натисніть на  кнопку для входу в головне меню.
3. Якщо для цього пристрою вже зареєстровано суперадміністратора, для входу в головне меню вам знадобиться дозвіл суперадміністратора.

2.5 Віртуальна клавіатура



Примітка: Типи клавіатур пристрою відповідатимуть мові системи.

- Натисніть і утримуйте кнопку «,», щоб встановити мову клавіатури.

2.6 Спосіб верифікації

Процес біометричного зіставлення можна класифікувати як «один до багатьох» або «ідентифікація» (1: N) та «один до одного» або «верифікація» (1:1). Нижче наведено опис кожного типу зіставлення та його особливостей.

1: N Процес ідентифікації

Процес біометричної ідентифікації «один до багатьох» (1: N) миттєво порівнює знятий біометричний шаблон особи з усіма біометричними шаблонами, що зберігаються в системі.

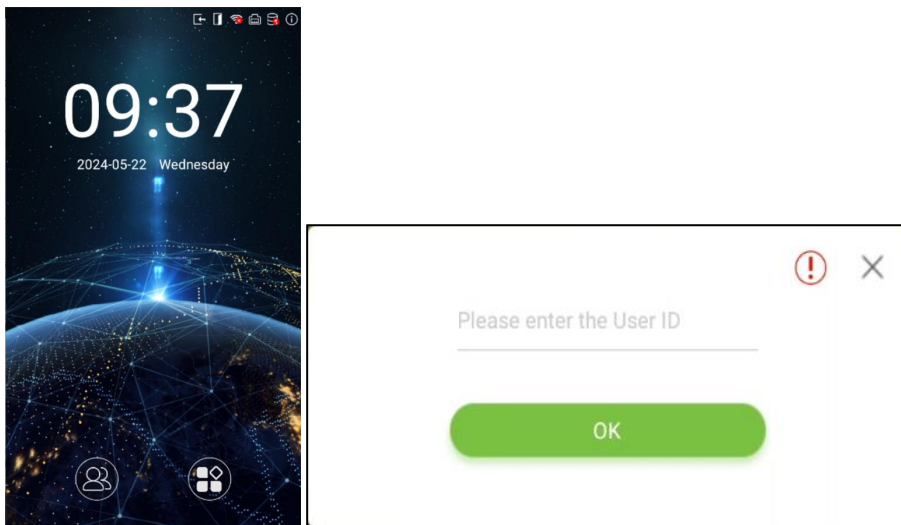
1:1 Процес верифікації

Процес біометричної верифікації 1:1 підтверджує особу людини шляхом порівняння знятого біометричного шаблону з біометричним шаблоном цієї особи, попередньо збереженим у базі даних.

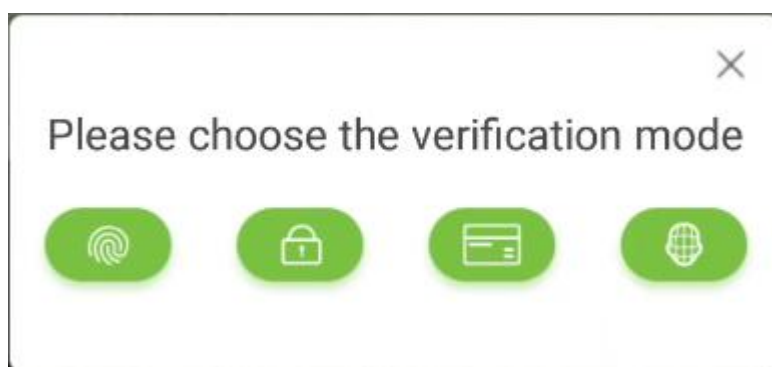
2.6.1 Верифікація пароля

Коли користувач вводить свій ID користувача та пароль у пристрій, дані порівнюються з ID користувача та паролем цього користувача, які були попередньо збережені в системі. Цей процес рекомендується для адміністраторів.

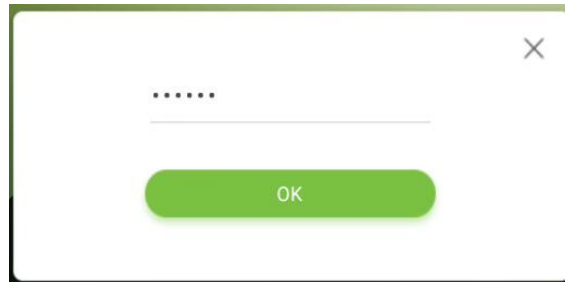
- На головному екрані натисніть на  кнопку, щоб увійти в режим перевірки пароля 1:1.
- На екрані введення введіть ID користувача та натисніть **[OK]**.



- Якщо користувач зареєстрував обличчя, відбиток пальця та картку на додаток до свого пароля, а спосіб перевірки встановлено як перевірка відбитка пальця/пароля/картки/обличчя, з'явиться такий екран.



- Натисніть на  кнопку пароля, щоб увійти в режим перевірки пароля. Введіть пароль і натисніть **[OK]**.



- Нижче наведено приклади успішної та неуспішної верифікації.



Успішна верифікація

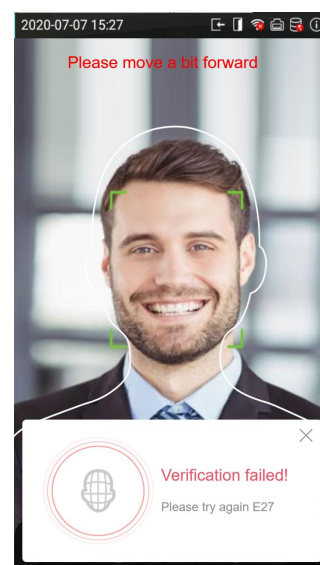
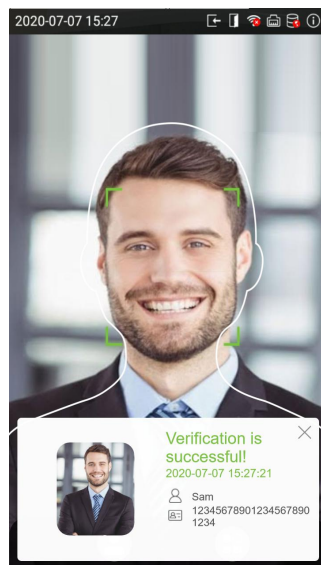


Неуспішна верифікація

2.6.2 Верифікація за допомогою розпізнавання обличчя

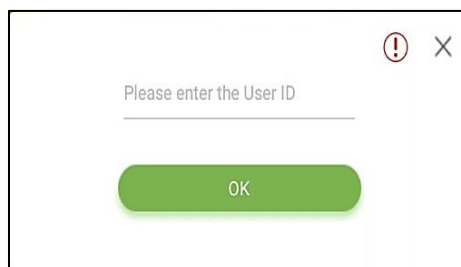
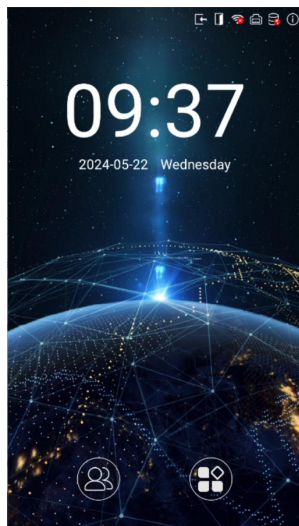
1: N Ідентифікація шаблону обличчя

- Цей спосіб ідентифікує отримане зображення обличчя користувача з усіма шаблонами обличчя, що зберігаються в пристрої.
- Нижче наведено приклади успішної та невдалої ідентифікації.

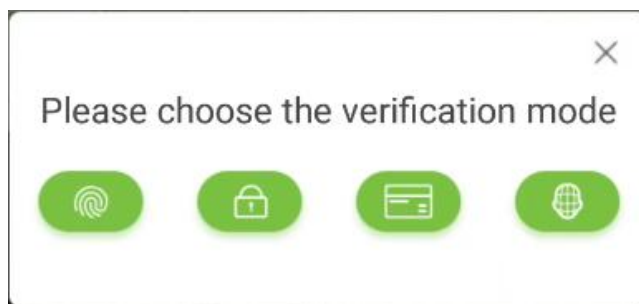


1:1 Перевірка шаблону обличчя

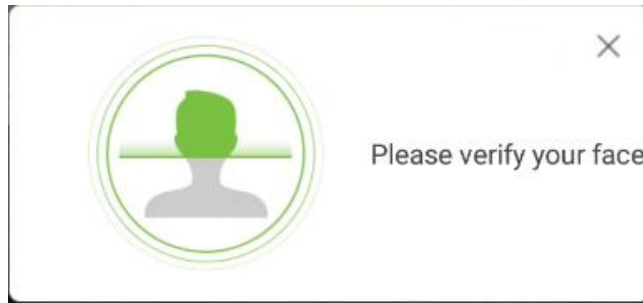
- Цей спосіб перевіряє обличчя користувача, зняте камерою, за шаблоном обличчя, пов'язаним з ID користувача, наданим користувачем.
- Натисніть  на головному інтерфейсі, щоб увійти в режим 1:1 перевірки обличчя. Введіть ID користувача, натисніть **[OK]**.



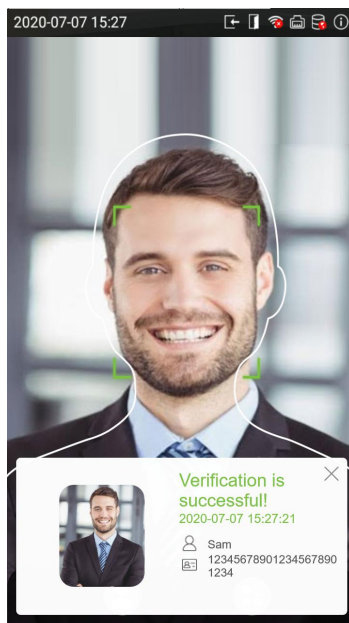
- Якщо користувач зареєстрував відбиток пальця, пароль і картку на додаток до свого обличчя, а спосіб перевірки встановлено як перевірка відбитка пальця/пароля/картки/обличчя, з'явиться наступний екран.
- Натисніть на кнопку обличчя  щоб увійти в режим перевірки обличчя.



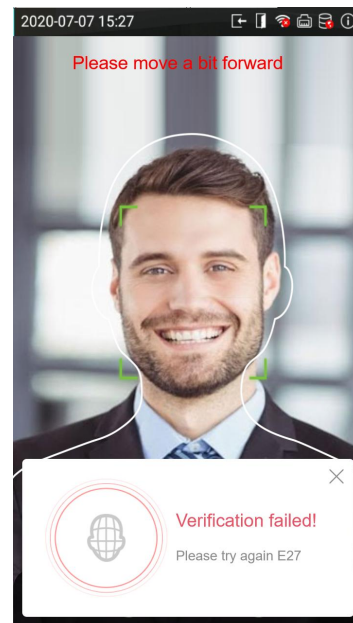
- Після появи запиту «Будь ласка, підтвердьте своє обличчя», розташуйте обличчя в центрі екрана пристрою для перевірки обличчя.



- Нижче наведено приклади успішної та неуспішної верифікації.



Успішна верифікація



Неуспішна верифікація

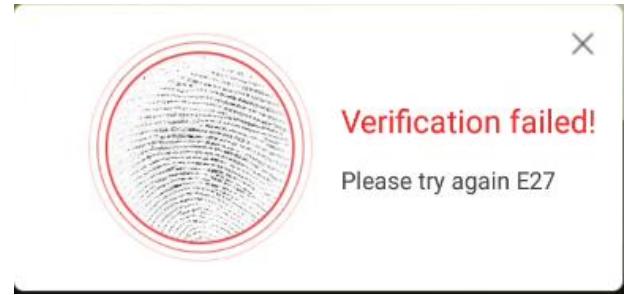
2.6.3 Верифікація за відбитком пальця ★

1: N Ідентифікація за відбитками пальців

- Цей спосіб порівнює відбиток пальця користувача, який притискається до сканера відбитків пальців, з усіма даними відбитків пальців, які попередньо збережені в пристрої.
- Щоб увійти в режим ідентифікації відбитків пальців, просто доторкніться пальцем до сканера відбитків пальців.
- Нижче наведено приклади успішної та неуспішної ідентифікації.



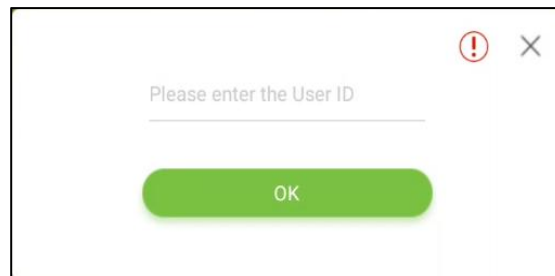
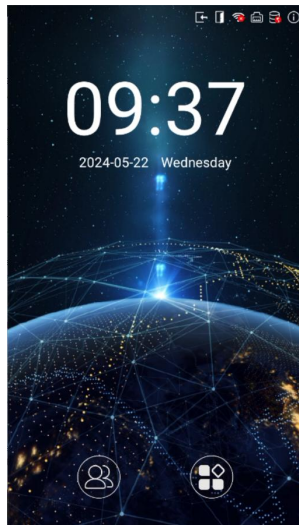
Успішна верифікація



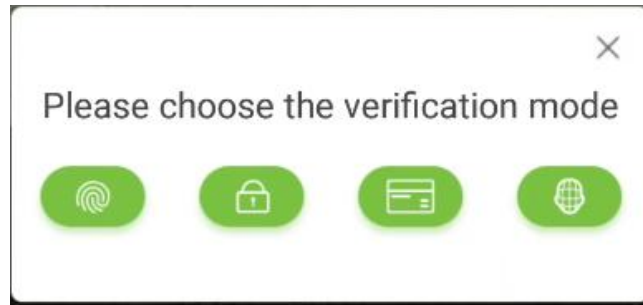
Неуспішна верифікація

1:1 Верифікація за відбитками пальців

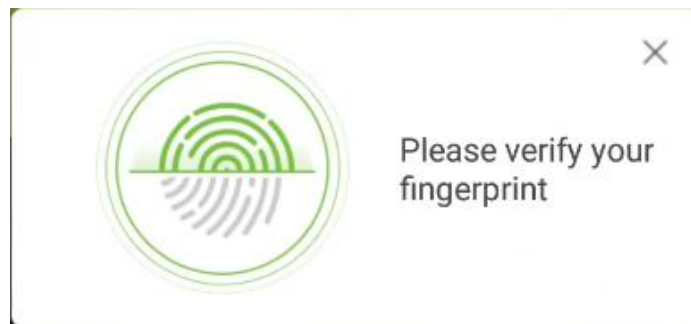
- Цей спосіб порівнює відбиток пальця користувача, який притискається до сканера відбитків пальців, із шаблонами відбитків пальців, пов'язаними з ідентифікатором користувача, який було введено за допомогою віртуальної клавіатури.
- Натисніть  кнопку на головному екрані, щоб увійти в режим перевірки відбитків пальців 1:1:
- Введіть ID користувача та натисніть **[ОК]**.



- Якщо користувач зареєстрував обличчя, пароль і картку на додаток до свого відбитка пальця, а спосіб верифікації встановлено як відбиток пальця/пароль/картка/обличчя, з'явиться наступний екран.
- Виберіть кнопку відбитка пальця  щоб увійти в режим перевірки відбитків пальців.



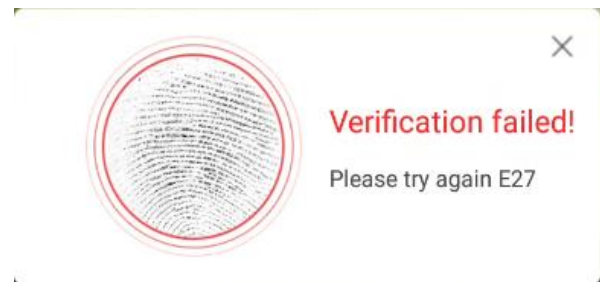
- Доторкніться пальцем до сканера відбитків пальців, щоб продовжити верифікацію.



- Нижче наведено приклади успішної та неуспішної верифікації.



Успішна верифікація



Неуспішна верифікація

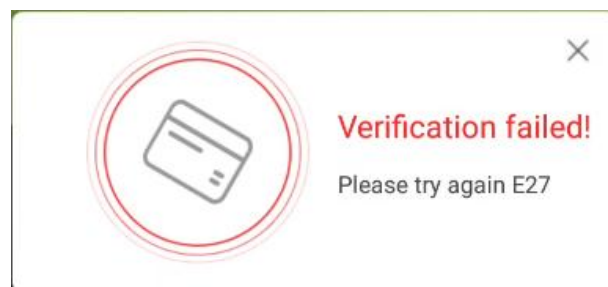
2.6.4 Верифікація картки

1: N Ідентифікація картки

- Щоб увійти в режим ідентифікації картки 1: N, покладіть зареєстровану картку на карткочитач.
- Нижче наведено приклади успішної та неуспішної ідентифікації.



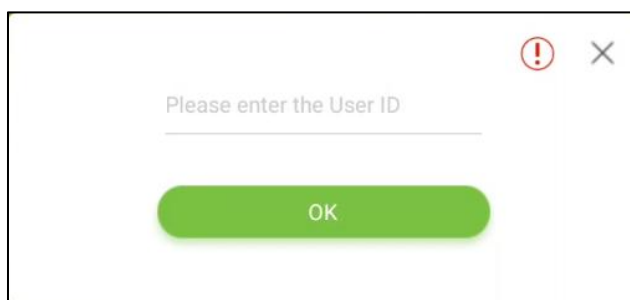
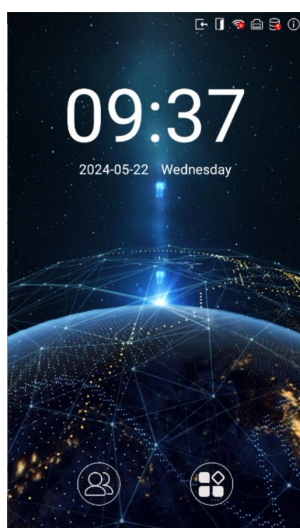
Успішна верифікація



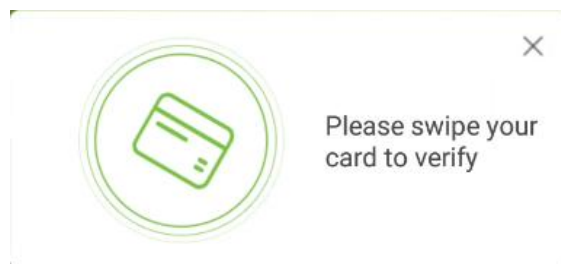
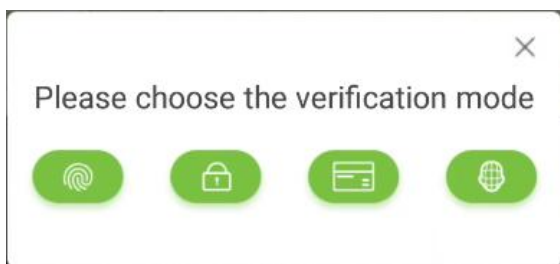
Неуспішна верифікація

1:1 Верифікація картки

- Щоб увійти в режим перевірки картки 1:1, натисніть кнопку  на головному екрані, щоб увійти в режим перевірки картки 1:1.
- Після цього введіть ID користувача та натисніть [OK].



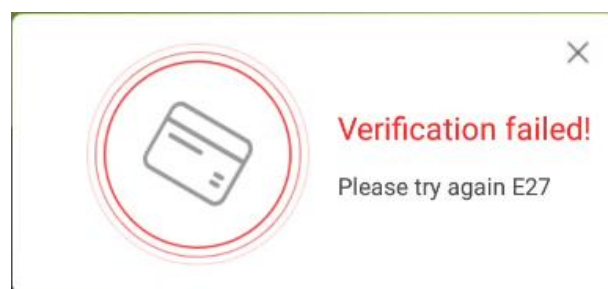
- Якщо користувач зареєстрував обличчя, пароль і відбиток пальця на додаток до своєї картки, а метод верифікації встановлено як верифікацію за відбитком пальця/паролем/карткою/обличчям, з'явиться наступний екран.
- Натисніть на кнопку  щоб увійти в режим перевірки картки. Після цього проведіть карткою, щоб підтвердити.



- Нижче наведено приклади успішної та неуспішної ідентифікації.



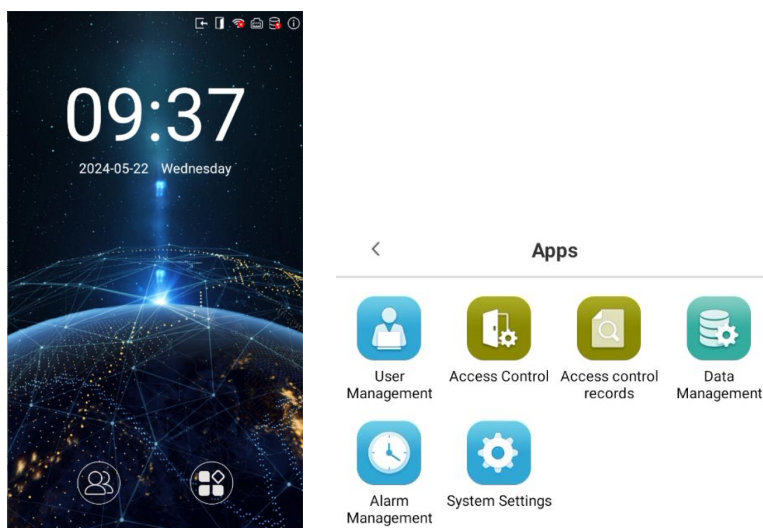
Успішна верифікація



Неуспішна верифікація

3 Головне меню

На інтерфейсі режиму очікування натисніть , щоб увійти в головне меню.



Операції меню

Меню	Функція
Керування користувачами (User Management)	Додавати, редагувати, переглядати та видаляти основну інформацію про користувача.
Контроль доступу (Access Control)	Для налаштування параметрів замка та відповідного пристрою контролю доступу Параметри контролю доступу, правила часу, налаштування святкових днів та налаштування режиму захисту від зворотного проходу.
Записи контролю доступу (Access control records)	Запитати вказаний запис доступу, перевірити фотографії доступу.
Керування даними (Data Management)	Щоб видалити всі відповідні дані з пристрою.
Керування сигналізацією (Alarm Management)	Після встановлення параметрів сигналізації пристрій автоматично відтворить заздалегідь обраний сигнал, коли настане визначений час. Сигнал зупиниться після закінчення встановленого часу.
Налаштування системи (System Settings)	Налаштуйте мережу, дату та час, параметри контролю доступу, хмарний сервіс, Wiegand, дисплей та звук, біометричні параметри, автоматичне тестування, розширені налаштування, послідовний порт та налаштування безпеки пристрою.



Примітка:

- Якщо на пристрої немає супер-адміністратора, будь-який користувач може увійти в меню, натиснувши кнопку. 
- Після призначення супер-адміністратора на пристрої для входу в меню буде потрібна перевірка. Після успішної перевірки користувачі зможуть увійти в меню.
- Для забезпечення безпеки пристрою рекомендуємо зареєструвати адміністратора під час першого використання цього пристрою. Детальні інструкції з експлуатації див. у розділі [Add User \(Додати користувача\)](#).

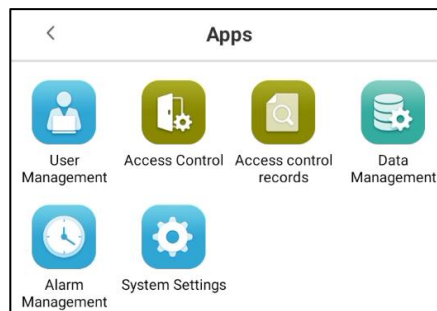
4 Керування користувачами

4.1 Додати користувача

Існує два способи додавання користувачів: додавання користувача за допомогою програмного забезпечення або додавання за допомогою пристрою.

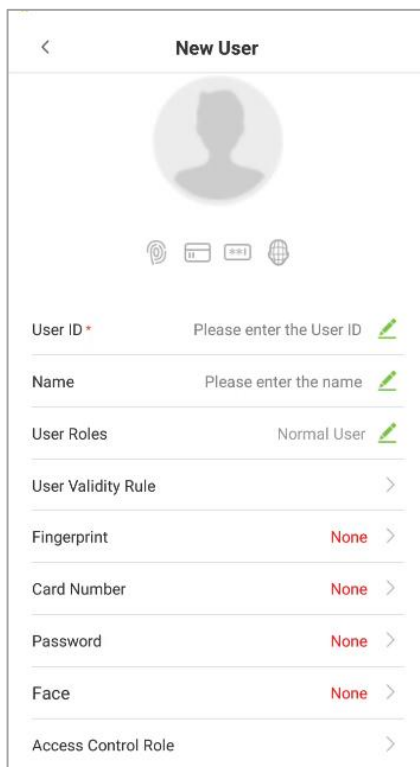
4.1.1 Додавання користувачів за допомогою пристрою

- Натисніть на  кнопку на інтерфейсі [**User Management** (Керування користувачами)] , щоб перейти до інтерфейсу створення користувача.



Реєстрація основної інформації про користувача

- У інтерфейсі **New User** (Новий користувач) натисніть **User ID** (Ідентифікатор користувача) і введіть унікальний ідентифікаційний номер, а потім натисніть **Name** (Ім'я) і введіть ім'я користувача.

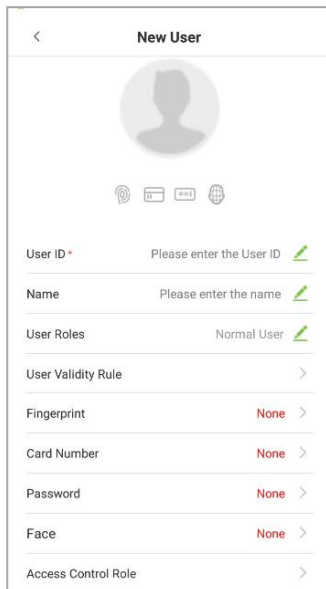


Примітка:

- Ім'я: максимальна довжина символів становить 64 (по 32 для імені та прізвища).
- ID користувача: ID користувача може містити від 1 до 14 цифр за замовчуванням.
- ID користувача можна змінити до першого входу в систему, але не можна змінити після входу.
- Повідомлення «This User ID already exists!» (Цей ID користувача вже існує!) означає, що введений ідентифікаційний номер вже використовується. У цьому випадку рекомендується ввести інший ідентифікаційний номер.

Реєстрація фотографії користувача

- У інтерфейсі **New User** (Новий користувач) натисніть  , щоб перейти до кнопки інтерфейсу камери.
- Рекомендується дивитися в об'єктив, а потім регулювати положення.
- В інтерфейсі **User Photo** (Фотографія користувача) натисніть кнопку  камери, щоб зробити фотографію.



New User

Placeholder for user photo

Icons: Fingerprint, ID Card, QR Code, Globe

User ID * Please enter the User ID ✓

Name Please enter the name ✓

User Roles Normal User ✓

User Validity Rule >

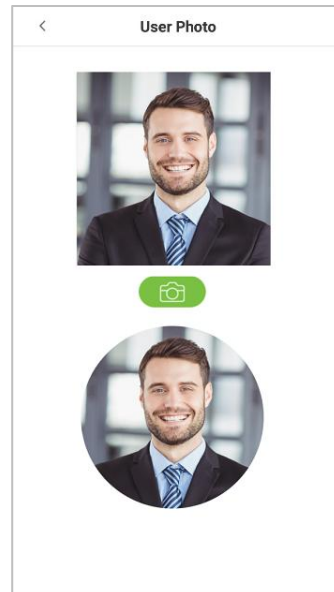
Fingerprint None >

Card Number None >

Password None >

Face None >

Access Control Role >



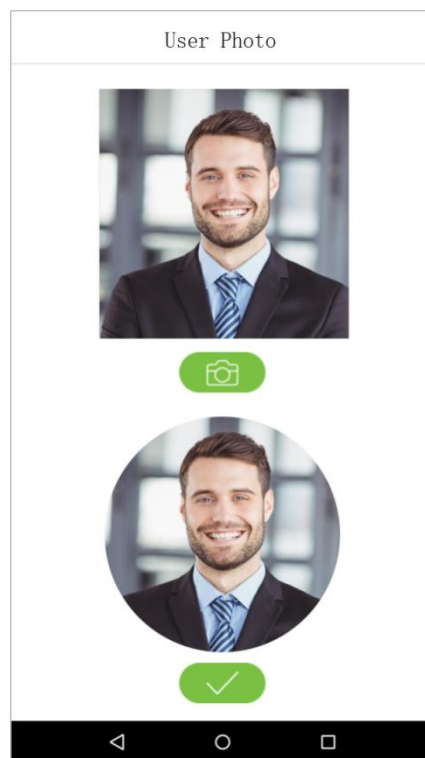
User Photo

Rectangular photo of a man in a suit

Camera icon

Circular photo of the same man

- Натисніть на  кнопку внизу, щоб успішно додати зроблене фото.



User Photo

Rectangular photo of a man in a suit

Camera icon

Circular photo of the same man

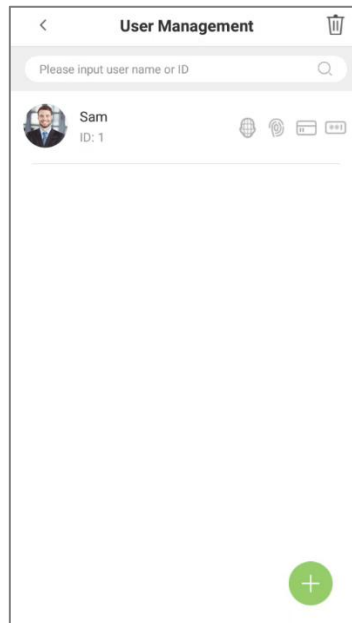
Green checkmark button

Android navigation bar

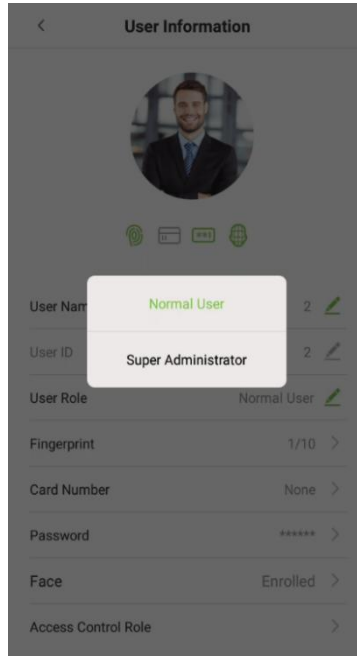
Роль користувача

Цей пристрій має два типи прав користувача: звичайний користувач і супер-адміністратор. Якщо на пристрої є супер-адміністратор, звичайні користувачі можуть перевіряти свої облікові записи лише за допомогою різних режимів перевірки, які вже встановлені для користувача. Але супер-адміністратор матиме більше прав, таких як доступ до головного меню, а також матиме такий самий доступ, як і звичайний користувач.

- В інтерфейсі **User Management** (Керування користувачами) натисніть на потрібне ім'я користувача зі списку користувачів, щоб встановити права користувача.



- В інтерфейсі «**User Information**» (Інформація про користувача) натисніть **[User Role]** (Роль користувача), а потім натисніть **[Normal User]** (Звичайний користувач) або **[Super Administrator]** (Супер-адміністратор), щоб встановити необхідні права.

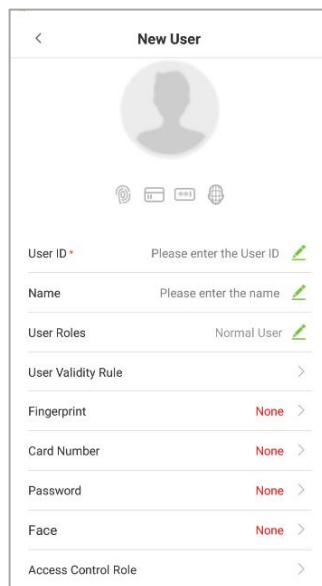


Примітка: Коли користувачеві надаються права суперадміністратора, для входу в головне меню буде потрібна верифікація.

Процес верифікації залежить від методу верифікації, який був використаний під час реєстрації користувача. Дивіться опис у розділі “**Verification Mode (Режим верифікації)**”.

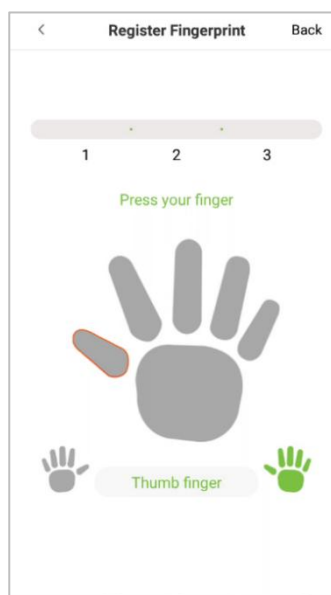
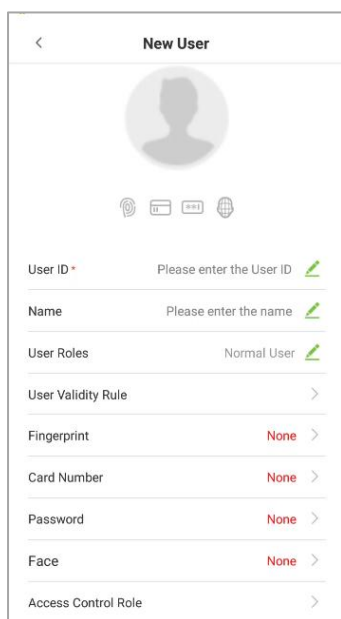
Реєстр режимів верифікації

- Різні режими верифікації використовуються для перевірки входу користувача.
- Режим верифікації включає реєстрацію обличчя, пароля, відбитків пальців ★ або номера картки користувача.
- У розділі **New User** (Новий користувач) натисніть на необхідний режим верифікації (відбиток пальця, номер картки, пароль, обличчя), щоб зареєструватися для верифікації.



Реєстрація відбитків пальців ★

- У меню **New User** (Новий користувач) натисніть **[Fingerprint]** (Відбиток пальця), щоб перейти до інтерфейсу реєстрації відбитків пальців.
- Натисніть на потрібну кнопку (ліворуч 🖐️ або 🖐️ праворуч) розташовану ліворуч і праворуч екрана, а потім натисніть на потрібний палець, щоб арегєструватися.

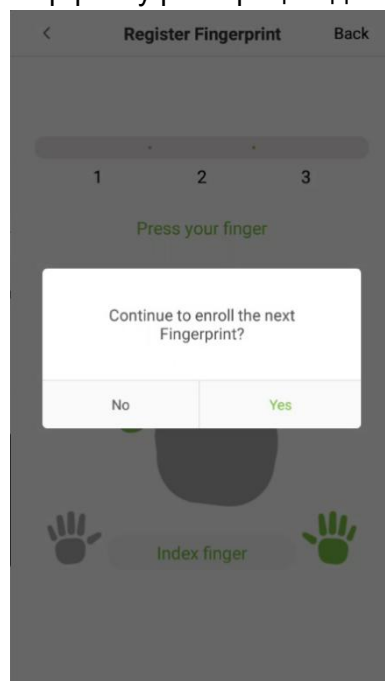


- Після вибору необхідного пальця тричі натисніть цим пальцем на сканер відбитків пальців.
- Зелений колір означає, що відбиток пальця успішно зареєстровано.

Примітка: Якщо ви натиснете різними пальцями на сканер відбитків пальців під час 2-го та 3-го разу, користувачеві буде показано повідомлення **«Please use the same finger»** (Будь ласка, використовуйте той самий палець), як показано на зображенні нижче.

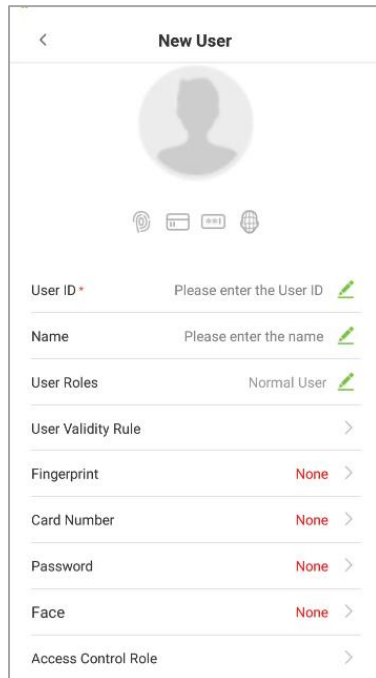


- Якщо відбиток пальця успішно зареєстровано, з'явиться діалогове вікно **Continue to enroll the next Fingerprint?** (Продовжити реєстрацію наступного відбитка пальця?).
- Натисніть **Yes** (Так), щоб записати наступний відбиток пальця, або **No** (Ні), щоб повернутися до інтерфейсу реєстрації відбитків пальців.

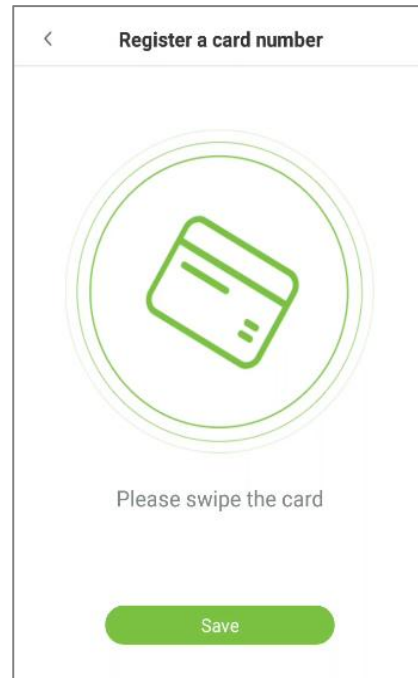


Реєстрація номера картки

- У інтерфейсі **New User** (Новий користувач) натисніть **Card Number** (Номер картки), щоб перейти на сторінку реєстрації номера картки.
- На інтерфейсі **Register a card number** (Зареєструвати номер картки) проведіть картою, щоб зареєструвати її.
- Якщо номер картки прочитано успішно, відобразиться номер картки. Натисніть **Save** (Зберегти), щоб оновити дані картки.



The screenshot shows the 'New User' registration screen. At the top, there is a back arrow and the title 'New User'. Below the title is a circular profile picture placeholder. Underneath are four small icons: a fingerprint, a card, a key, and a globe. The form consists of several fields: 'User ID *' with a placeholder 'Please enter the User ID' and a green pencil icon; 'Name' with a placeholder 'Please enter the name' and a green pencil icon; 'User Roles' with the value 'Normal User' and a green pencil icon; 'User Validity Rule' with a right arrow; 'Fingerprint' with the value 'None' and a right arrow; 'Card Number' with the value 'None' and a right arrow; 'Password' with the value 'None' and a right arrow; 'Face' with the value 'None' and a right arrow; and 'Access Control Role' with a right arrow.



The screenshot shows the 'Register a card number' screen. At the top, there is a back arrow and the title 'Register a card number'. The main area features a large green circular graphic containing a stylized card icon. Below this graphic, the text 'Please swipe the card' is displayed. At the bottom of the screen is a green rounded rectangular button labeled 'Save'.

Реєстрація пароля

- У інтерфейсі **New User** (Новий користувач) натисніть **Password** (Пароль), щоб зареєструвати пароль.
- У полі **Enter the password** (Введіть пароль) введіть пароль, а потім у полі **Confirm password** (Підтвердіть пароль) введіть той самий пароль ще раз.
- Натисніть **Confirm** (Підтвердити).



Примітка: Пароль користувача повинен складатися з 6-8 цифр.

Функція	Опис
	Натисніть на цю кнопку, щоб приховати пароль.
	Натисніть на цю кнопку, щоб зробити пароль видимим.

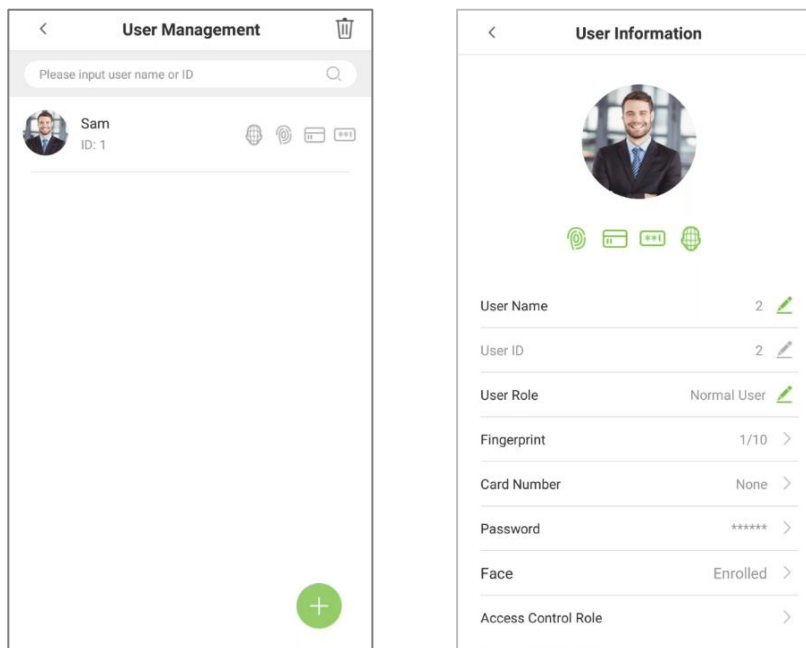
- Якщо пароль, введений в обох полях, не збігається, введіть правильний пароль ще раз.

- Зареєстрований пароль можна видалити або змінити.

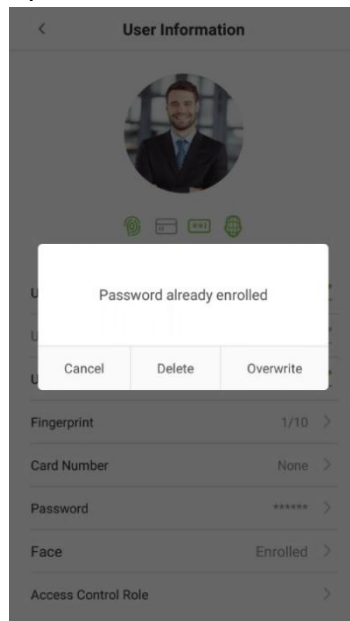
Видалити/перезаписати зареєстрований пароль

- В інтерфейсі **User management** (Керування користувачами) натисніть на потрібне ім'я користувача зі списку користувачів, щоб видалити або змінити пароль.

- В інтерфейсі **User information** (Інформація про користувача) натисніть **[Password]** (Пароль), щоб видалити або змінити.



- У спливаючому вікні натисніть **Delete/ Overwrite** (Видалити/Перезаписати), щоб видалити або змінити пароль.



Реєстрація обличчя

- У інтерфейсі **New User** (Новий користувач) натисніть **Face** (Обличчя), щоб перейти на сторінку реєстрації обличчя.
- В інтерфейсі **Face Register** (Реєстрація обличчя) перемістіть і відрегулюйте своє обличчя в області реєстрації.

New User

User ID * Please enter the User ID ✓

Name Please enter the name ✓

User Roles Normal User ✓

User Validity Rule >

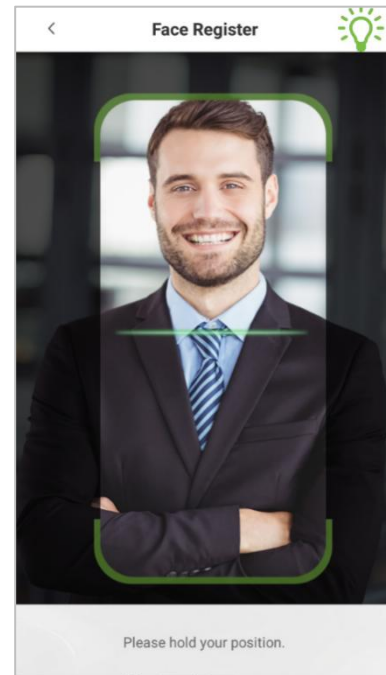
Fingerprint None >

Card Number None >

Password None >

Face None >

Access Control Role >



Налаштування терміну дії

Ця функція встановлює термін дії процесу перевірки відвідування працівника. Отже, після встановлення цього терміну дії працівник зможе перевіряти відвідування лише протягом встановленого часу. Якщо працівник підтвердить відвідування до або після визначеного часу, відвідування буде недійсним.

Перевірка відвідування є дійсною між визначеним початком і кінцем періоду, встановленим на певну кількість днів; це забезпечує точність до конкретних днів. Термін дії одного дня становить з 00:00 до 23:59; після закінчення цього терміну перевірка відвідування працівника буде недійсною.

- В інтерфейсі **“User Information”** (Інформація про користувача) натисніть **[User Validity Rule]** (Правило дійсності користувача), щоб встановити термін дії.



Примітка:

Якщо функція **User Validity Rule** (Правило дійсності користувача) не відображається в інтерфейсі **New User** (Новий користувач), то в головному меню натисніть **System Settings** (Налаштування системи) > **Access Control Record Settings** (Налаштування запису контролю доступу) і ввімкніть **User Validity Settings** (Налаштування дійсності користувача), після чого функція «**User Validity Rule**» (Правило дійсності користувача) з'явиться в інтерфейсі **User** (Користувач).

- У розділі **User Validity Rule** (Правило дійсності користувача) встановіть правило дійсності користувача, налаштувавши необхідну дату та час.

Рівень доступу

- Роль контролю доступу встановлює права доступу до дверей для кожного користувача.
- Це включає групу доступу, привілеї відбитків пальців, а також полегшує налаштування періоду доступу групи.
- У інтерфейсі **New User** (Новий користувач) натисніть **User Access Control Role** (Роль контролю доступу користувача), щоб встановити рівень доступу.

New User

User ID * Please enter the User ID

Name Please enter the name

User Roles Normal User

User Validity Rule

Fingerprint None

Card Number None

Password None

Face None

Access Control Role

User Access Control Role

Access Group 0

Time Period

Duress Fingerprint Not defined

Налаштування групи доступу

- У розділі **User Access Control Role** (Роль контролю доступу користувачів) натисніть **Access Group** (Група доступу), щоб розподілити зареєстрованих користувачів по різних групах для зручності управління.

User Access Control Role

Access Group 0

Time Period

Duress Fingerprint Not defined

Please choose the user's access group(0~99)

1

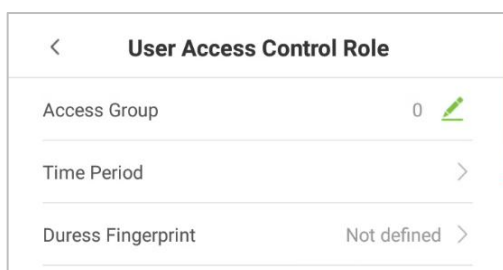
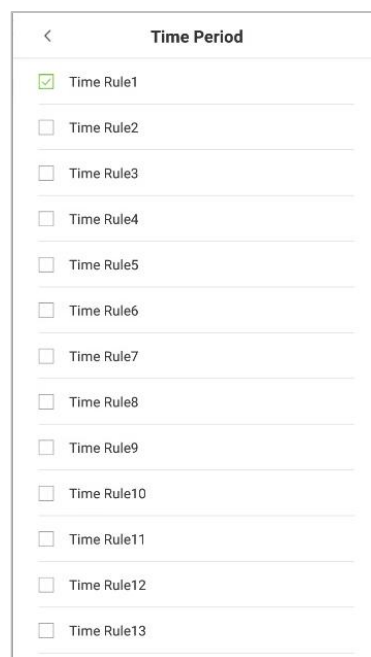
Cancel OK

- Нові користувачі будуть додані до групи 0 за замовчуванням, яку можна перепризначити до інших необхідних груп.
- Пристрій підтримує до 99 груп контролю доступу.

Встановіть часовий період

- Натисніть **Time Period** (Часовий період), щоб встановити час доступу для користувача.

- За замовчуванням користувачі дотримуються визначених налаштувань своїх груп.
- Якщо період часу не застосовується, слід встановити час доступу конкретного користувача.
- Така конфігурація не вплине на налаштування часу інших членів групи.

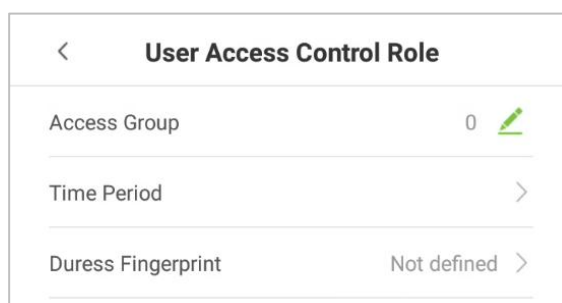




Примітка: Всього можна встановити 50 правил часу, за замовчуванням встановлено правило часу 1.

Відбиток пальця під примусом★

Користувач може вказати один або кілька відбитків пальців для реєстрації як відбитки пальців під примусом. Отже, як тільки користувач натисне відповідний палець на датчик і якщо перевірка буде успішною, система негайно увімкне сигнал тривоги.

- У розділі **User Access Control Role** (Роль контролю доступу користувачів) натисніть **Duress Fingerprint** (Відбиток пальця під примусом), щоб налаштувати доступ під примусом.



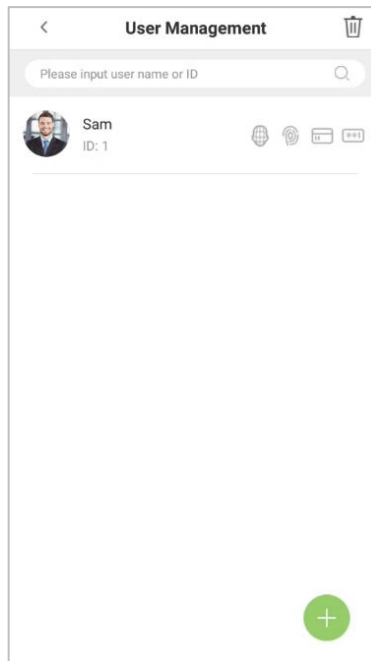
4.2 Пошук користувача

Функція **Search User** (Пошук користувача) дозволяє знайти потрібного користувача зі списку.

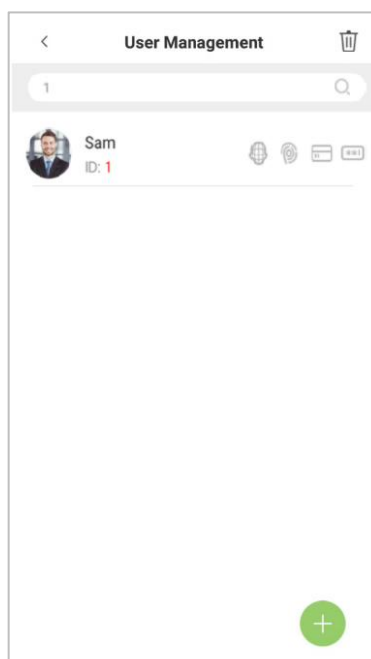
- Натисніть на панель пошуку, розташовану в інтерфейсі **[User Management]** (Керування користувачами), і знайдіть потрібне ім'я користувача.



Примітка: Необхідних користувачів можна шукати за їх ID, іменем користувача, прізвищем або повним ім'ям.

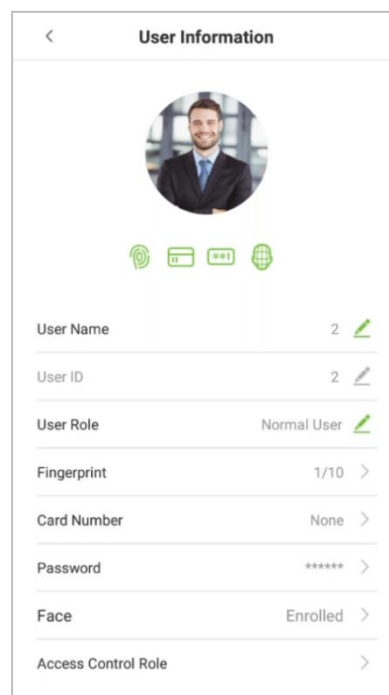
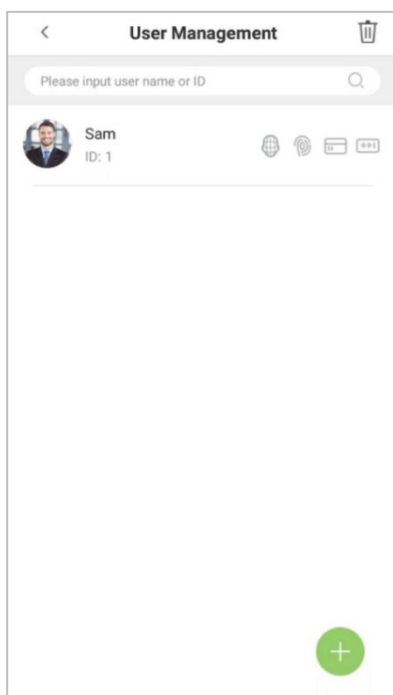


- Натисніть на панель **Search** (Пошук), щоб знайти користувачів з відповідним ідентифікатором/ім'ям, і система автоматично знайде користувачів з інформацією, що відповідає пошуковому запиту.



4.3 Редагування користувача

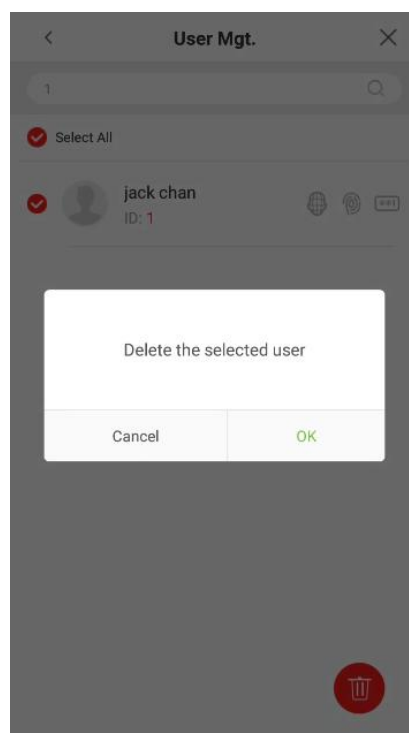
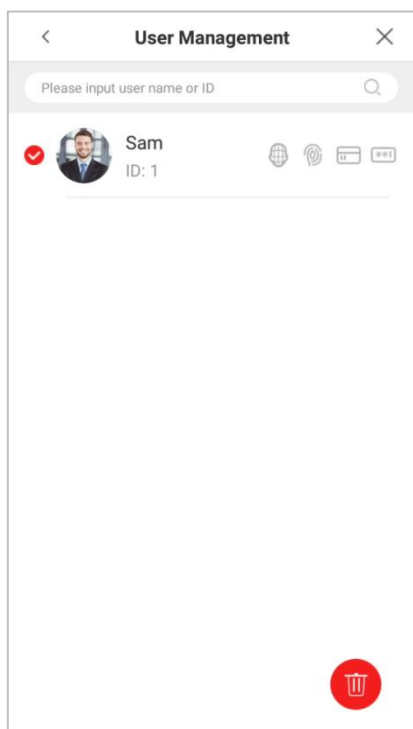
- В інтерфейсі **User Management** (Керування користувачами) натисніть на потрібного користувача зі списку, щоб редагувати його.
- В інтерфейсі **User Information** (Інформація про користувача) натисніть  відповідну кнопку **Edit** (Редагувати), щоб редагувати необхідну інформацію про користувача.



Примітка: Зверніть увагу, що ID користувача не можна змінити, а інші операції аналогічні додаванню нового користувача. Для отримання додаткової інформації див. розділ [“Add User \(Додати користувача\)”](#).

4.4 Видалення користувача

- В інтерфейсі **User Management** (Керування користувачами) виберіть потрібного користувача для видалення та натисніть кнопку  **Delete** (Видалити), щоб видалити його.
- У спливаючому вікні натисніть **OK**, щоб підтвердити видалення.



Примітка: Якщо ви видаляєте вибраного користувача, вся інформація, пов'язана з цим користувачем, буде видалена.

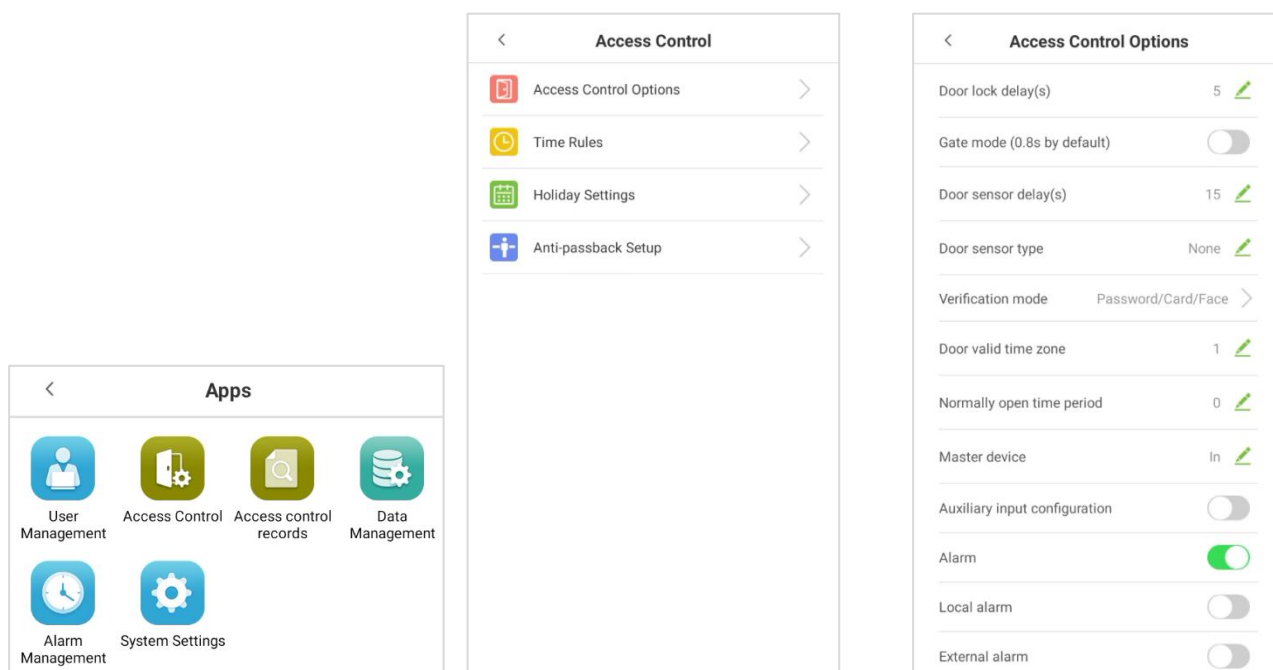
5 Налаштування доступу

Налаштування **Access Settings** (Налаштування доступу) полегшують налаштування параметрів доступу.

5.1 Параметри контролю доступу

Параметри контролю доступу використовуються для налаштування параметрів доступу.

- У **Main menu** (Головне меню) натисніть **[Access Control]** (Контроль доступу).



- Параметри контролю доступу включають наступні функції.

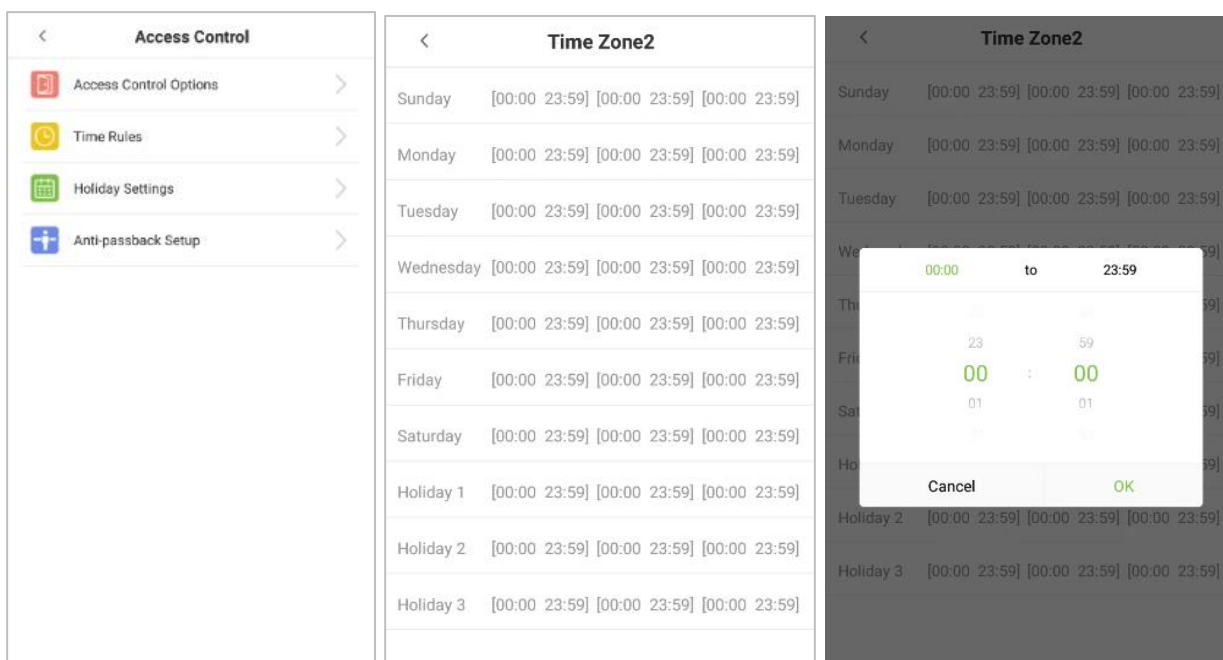
Опції меню	Опис функції
Затримка замка дверей	Час, протягом якого пристрій контролює електричний замок, щоб він перебував у розблокованому стані. Дійсне значення: 1–254 секунди.
Режим воріт	Перемикайте між положеннями ON (Увімкнено) та OFF (Вимкнено), щоб увімкнути або вимкнути режим «ворота». У положенні ON (Увімкнено) на цьому інтерфейсі буде вимкнено затримку блокування дверей.
Затримка датчика дверей	Якщо сигналізація увімкнена і стан датчика стану дверей не відновлюється протягом заданого часу, спрацює сигналізація. Діюче значення: 1~500 секунд.

Тип датчика дверей	Існує три типи датчиків: закритий, нормально відкритий і нормально закритий. Закритий: це означає, що датчик дверей не використовується. Нормально відкритий: це означає, що двері завжди залишаються відкритими, коли подається електроенергія. Нормально закритий: це означає, що двері завжди залишаються закритими, коли подається електроенергія.
Режим верифікації	Підтримуваний режим верифікації включає: відбиток пальця/пароль/обличчя/картка, відбиток пальця, ID користувача, пароль, обличчя, картка, відбиток пальця/пароль, відбиток пальця/картка, пароль/картка, ID користувача + відбиток пальця, відбиток пальця + пароль, відбиток пальця + картка, відбиток пальця + пароль + картка, пароль + картка, відбиток пальця + ID користувача + пароль, обличчя + відбиток пальця, обличчя + пароль, обличчя + картка, обличчя + відбиток пальця + картка та обличчя + відбиток пальця + пароль. За замовчуванням використовується відбиток пальця/пароль/обличчя/картка. ПРИМІТКА: Аутентифікація за відбитком пальця є опціональною функцією.
Час доступу до дверей	Встановити час роботи дверей, щоб вони були доступні тільки протягом цього періоду.
Нормальний час роботи	Запланований період часу для режиму Normally Open (Нормально відкрито), щоб двері завжди залишалися відкритими протягом цього періоду.
Головний пристрій	При налаштуванні головного та підлеглого пристроїв статус головного пристрою можна встановити як вихідний або вхідний. Вихідний: запис, перевірений на хості, є вихідним записом. Вхідний: запис, перевірений на хості, є вхідним записом.
Конфігурація допоміжного входу	Встановлює час розблокування дверей та тип допоміжного виходу допоміжного термінального пристрою. Типи допоміжних виходів включають «Немає», «Спусковий механізм відкриття дверей», «Спусковий механізм сигналу тривоги», «Спусковий механізм відкриття дверей та сигналу тривоги».
Сигналізація	Увімкніть сигналізацію, щоб встановити локальну та зовнішню сигналізацію. Вимкніть сигналізацію, щоб вимкнути обидві.
Місцева сигналізація	Коли спрацьовує сигналізація, пристрій видає звуковий сигнал.
Зовнішня сигналізація	Необхідно підключити зовнішній пристрій сигналізації, який спрацьовує при спрацьовуванні сигналізації.
Скидання налаштувань доступу	Параметри скидання контролю доступу включають затримку замка дверей, затримку датчика дверей, тип датчика дверей, режим перевірки, часовий діапазон дії дверей, часовий діапазон нормального відкриття, головний пристрій та сигнал тривоги. Однак дані контролю доступу, видалені в Data Mgt., не враховуються.
Час перевірки для декількох користувачів	Час, необхідний для багатокористувацької верифікації.

5.2 Налаштування правил часу

- В інтерфейсі **Access Control** (Контроль доступу) необхідно підключити програмне забезпечення, налаштувати правила часу.
- Вся система може визначити до 50 правил часу (за замовчуванням встановлено правило 1, яке не можна змінювати).

- Кожне правило часу представляє 7 часових поясів, тобто 1 тиждень і 3 вихідні дні, і кожен часовий пояс є стандартним 24-годинним періодом на день, і користувач може перевіряти тільки в межах дійсного періоду часу.
- Для кожного часового поясу ви можете встановити максимум 3 періоди часу. Відношення між цими періодами часу є «або».
- Якщо час перевірки припадає на будь-який з цих періодів, перевірка буде успішною і дійсною.
Формат часового поясу для кожного періоду: ГГ ММ-ГГ ММ, з точністю до хвилини за 24-годинним годинником.
Натисніть на сіре поле, щоб знайти необхідне правило часу. Введіть необхідний ідентифікатор правила часу (тобто шукайте як 2-50).
- На інтерфейсі часового поясу натисніть на день (тобто неділя, понеділок ...), в який потрібно встановити часовий період.
На інтерфейсі часового періоду 1 встановіть час початку та закінчення, а потім натисніть ОК.



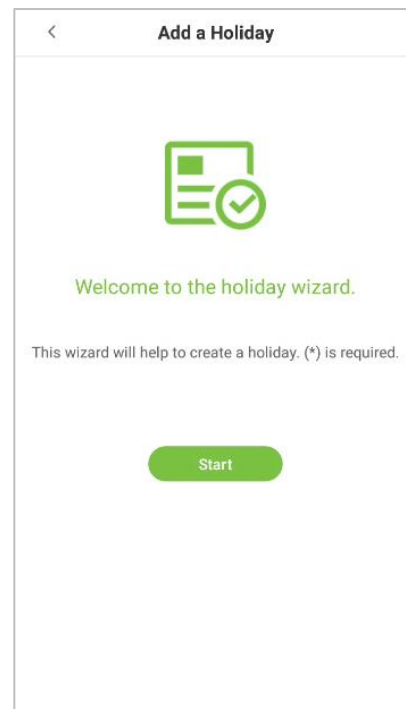
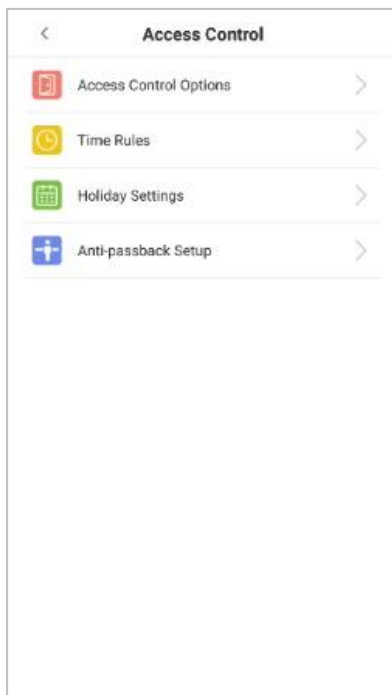
Примітка:

- Якщо час закінчення пізніше за час початку (наприклад, 00:00~23:59), це означає, що інтервал є дійсним.
- Ефективний період часу, протягом якого двері залишаються відчиненими або відкритими протягом усього дня, становить (00:00~23:59), а також коли час закінчення пізніше за час початку (наприклад, 08:00~23:59).
- За замовчуванням часова зона 1 вказує, що двері відкриті протягом усього дня, і її не можна редагувати.

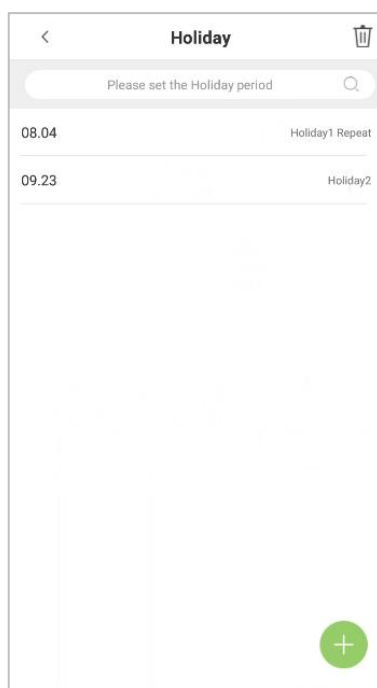
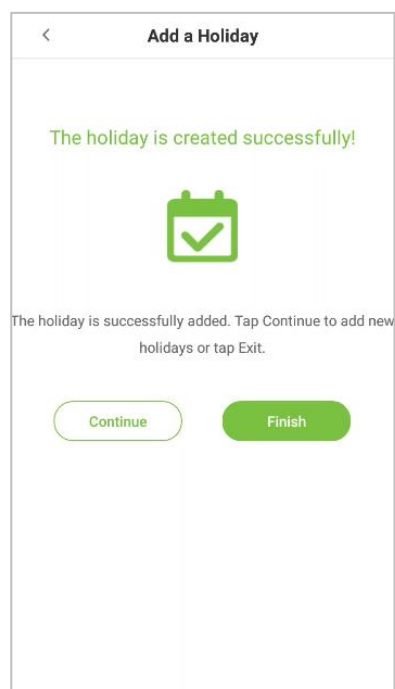
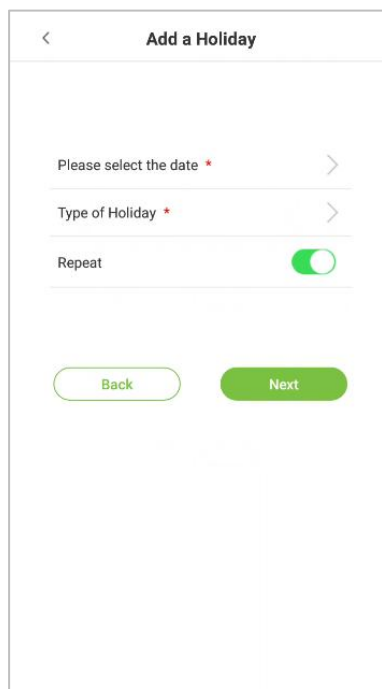
5.3 Налаштування святкових днів

Кожного разу, коли настає свято, вам може знадобитися спеціальний час доступу; але змінювати час доступу для кожного окремо надзвичайно незручно, тому ви можете встановити час доступу на свята, який буде застосовуватися до всіх користувачів, і користувач зможе відкривати двері під час свят. Час, встановлений тут, вважається стандартним.

- Натисніть **[Holiday setting]** (Налаштування святкових днів) і потім натисніть на  кнопку, щоб створити новий святковий день.



- На екрані **[Holiday setting]** (Налаштування святкових днів) виберіть дату та тип свята. Увімкніть **[Repeat]** (Повторити), щоб повторювати свято щороку, а потім натисніть **[Next]** (Далі).
- На цьому інтерфейсі натисніть **Finish** (Завершити), щоб успішно додати новостворений вихідний день, або натисніть **Continue** (Продовжити), щоб створити ще один вихідний день.



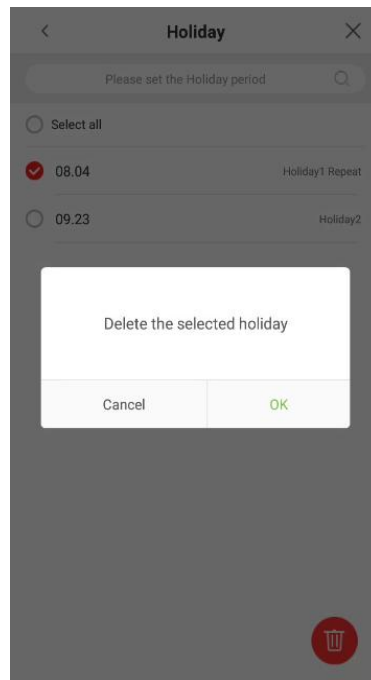
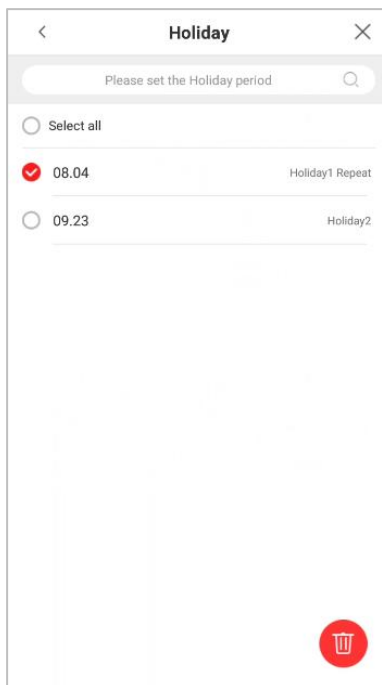
Редагувати святкові дні

- На інтерфейсі **Holiday period** (Період святкових днів) натисніть на необхідну відпустку, щоб змінити її.

Видалити святкові дні

- На інтерфейсі **Holiday period** (Період святкових днів) натисніть  кнопку, щоб видалити святкові дні.

- Виберіть свято, яке ви хочете видалити, натисніть на кнопку  в правому нижньому куті.
- У спливаючому вікні натисніть **ОК**, щоб підтвердити видалення.



5.4 Налаштування функції запобігання зворотньому проходу

Функція запобігання зворотньому проходу — це метод спрямованого контролю, що використовується для запобігання зловживанню системою контролю доступу. Ця функція передбачає певну послідовність дій, за якої пристрої контролю доступу повинні бути встановлені як зсередини, так і ззовні дверей для забезпечення доступу.

Отже, якщо будь-який співробітник увійде в зону з контрольованим доступом слідом за іншою особою без аутентифікації на біометричному пристрої, то наступного разу, коли ця особа спробує покинути зону, двері не відчиняться. Ця функція використовується для виявлення законності доступу користувача шляхом визначення останнього запису про доступ користувача та напрямку місцевого контролю, що дозволяє ефективно запобігати несанкціонованому проникненню.

Налаштування функції запобігання зворотньому проходу можна розділити на чотири типи:

- **Без функції «Anti-passback»:** Якщо первинний і вторинний пристрої не потребують налаштування, можна вибрати опцію «Без антипасбеку».
- **Антипасбек: вихід:** Після того, як користувач вибуває, тільки якщо останній запис є записом про вхід, користувач може знову вибути; в іншому випадку спрацює сигнал тривоги. Однак користувач може вільно входити..

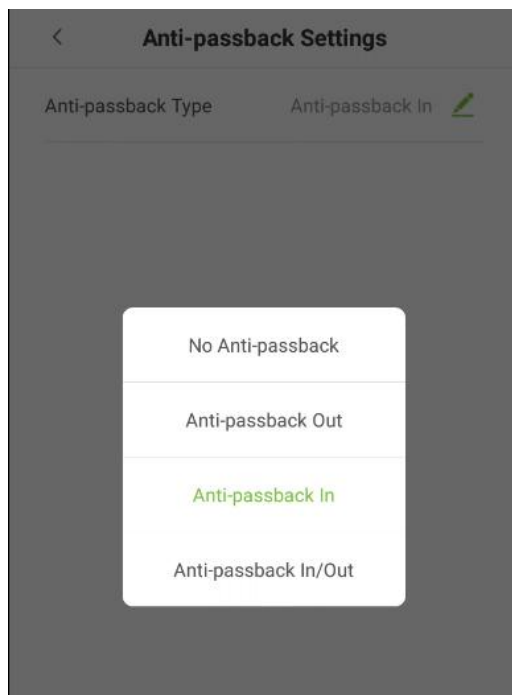
- **Антипасбек Вхід:** Після реєстрації користувача, тільки якщо останній запис є записом про виписку, користувач може зареєструватися знову; в іншому випадку спрацює сигнал тривоги. Однак користувач може вільно виписатися.
- **Антипасбек вхід/вихід:** Після того, як користувач зареєструвався/виписався, тільки якщо останній запис є записом про виписку, користувач може зареєструватися знову; або якщо це запис про реєстрацію, користувач може виписатися знову; в іншому випадку спрацює сигнал тривоги.



Примітка: Якщо під час першої перевірки у користувача немає запису, затвердження антипасбеку передається безпосередньо.

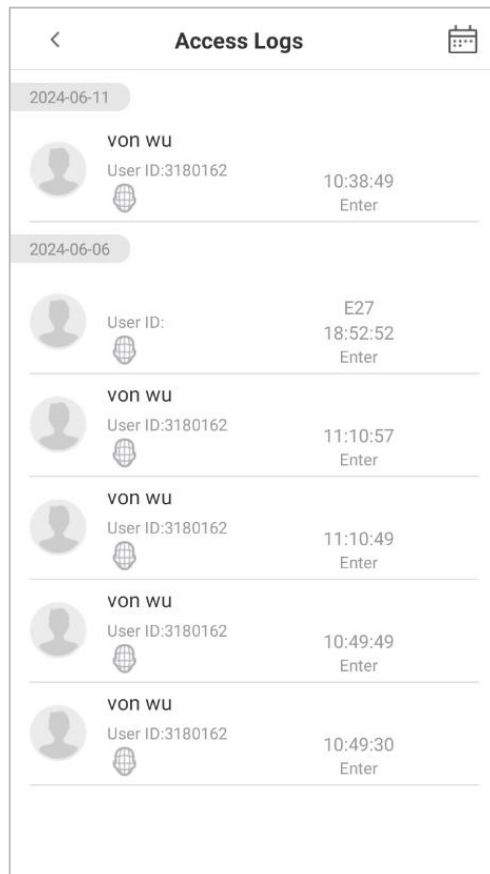
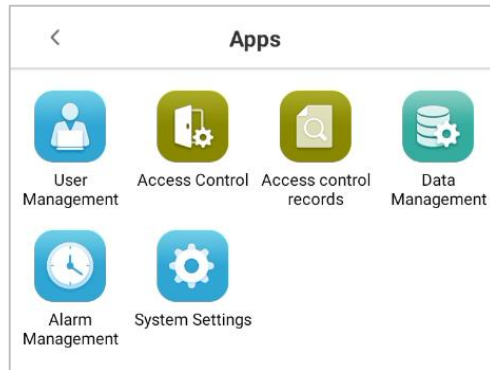
Цей напрямок доступу залежить від вибору напрямку керування пристроєм, що відповідає стану пристрою.

- Інтерфейс показаний нижче:



6 Записи контролю доступу

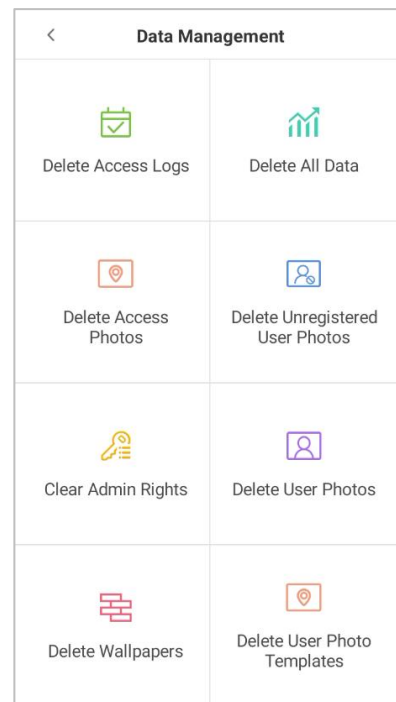
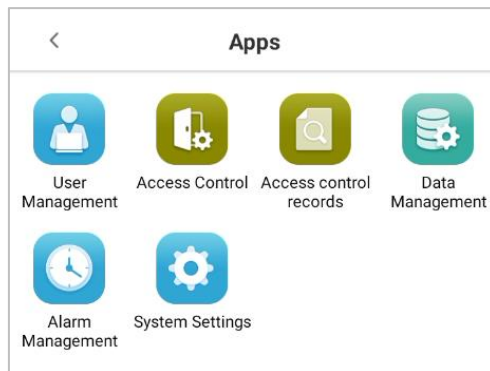
- Записи про доступ користувачів будуть зберігатися в пристрої, що полегшить пошук необхідних записів про відвідування.



7 Керування даними

Меню Data Management Settings (Налаштування управління даними) дозволяє користувачам керувати даними пристрою, включаючи Delete Access Logs (Видалити журнали доступу), Delete All Data (Видалити всі дані), Delete Access Photos (Видалити фотографії доступу), Delete Unregistered User Photos (Видалити фотографії незареєстрованих користувачів), Clear Admin Rights (Очистити права адміністратора), Delete User Photos (Видалити фотографії користувачів), Delete Wallpapers (Видалити шпалери) та Delete User Photo Templates (Видалити шаблони фотографій користувачів).

- У **Main menu** (Головному меню) натисніть **Data Management** (Керування даними), щоб керувати даними.



Опис функцій

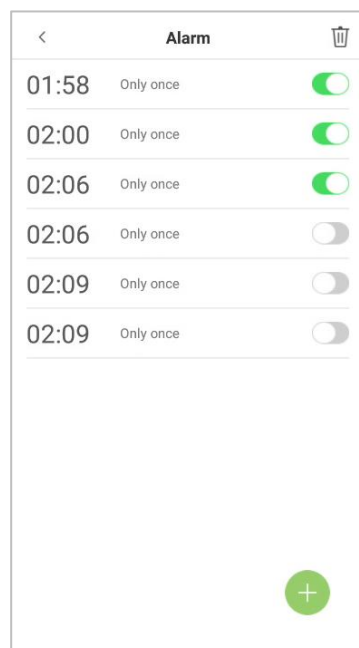
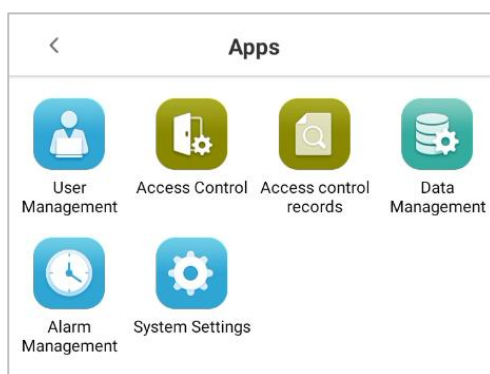
Назва функції	Опис функції
Видалити журнали доступу	- Видаляє всі журнали. - Видаляє журнали доступу за вказаний проміжок часу.
Видалити всі дані	Видаляє бізнес-дані, що зберігаються в пристрої, включаючи журнали доступу, паролі/біометричні дані обличчя, привілеї суперадміністратора, фотографії користувачів, дані користувачів та дані контролю доступу.
Видалити фотографії доступу	- Видаляє всі журнали - Видаляє недійсні облікові записи користувачів - Видаляє фотографії доступу за вказаний проміжок часу.
Видалити фотографії незареєстрованих користувачів	- Видаляє все (включно із записами доступу та фотографіями користувача у списку заблокованих) - Видаляє фотографії незареєстрованих користувачів у межах зазначеного часового діапазону.

Очистити права адміністратора	Змінює супер-адміністратора на звичайного користувача.
Видалити фотографії користувача	Видаляє всі фотографії користувача.
Видалити шпалери	Видаляє всі шпалери, збережені на пристрої.
Видалити шаблони фотографій користувачів	Видалити всі фотографії шаблонів користувачів.

8 Керування сигналами тривоги

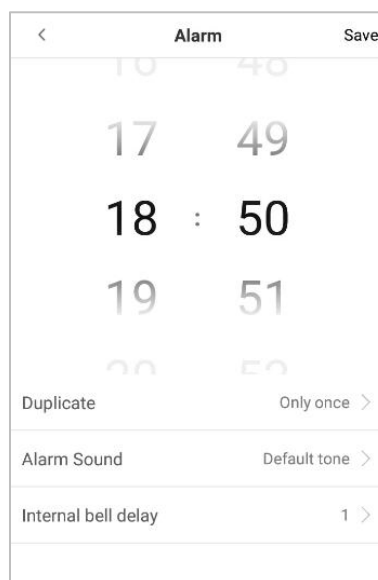
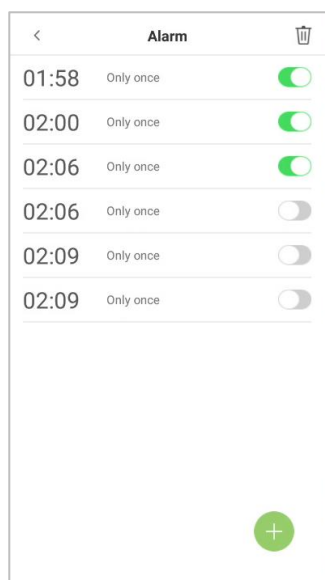
Після встановлення сигналу тривоги пристрій автоматично відтворить заздалегідь обраний сигнал тривоги, коли настане встановлений час. Він припинить дзвонити після закінчення встановленого часу.

- У **Main menu** (Головне меню) натисніть **Alarm Management** (Керування сигналами тривоги), щоб налаштувати параметри сигналу тривоги.



8.1 Додати сигнал тривоги

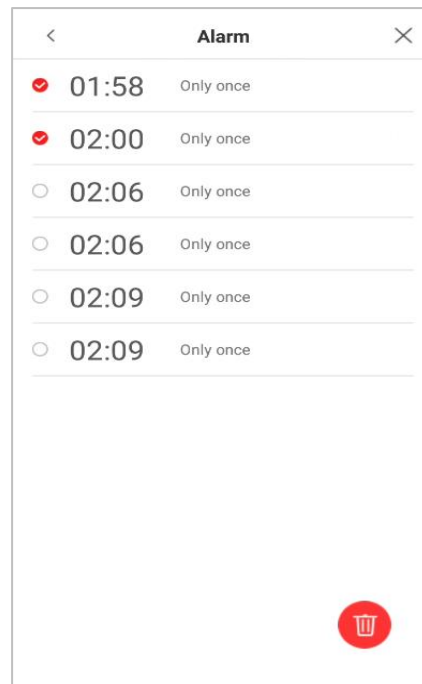
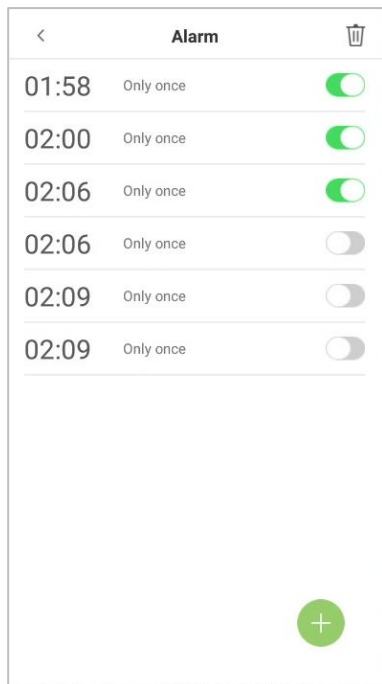
- На інтерфейсі **Alarm** (Сигнал тривоги) натисніть **кнопку**  для налаштування сигналу, а потім натисніть **Save** (Зберегти), щоб зберегти та оновити.



Menu Options	Function Description
Повтор	Встановить необхідну кількість повторень запланованого дзвінка.
Звук сигналу тривоги	Виберіть мелодію дзвінка.
Внутрішня затримка дзвінка	Встановить час повторення внутрішнього дзвінка. Діапазон допустимих значень: від 1 до 999 секунд.

8.2 Видалити сигнал тривоги

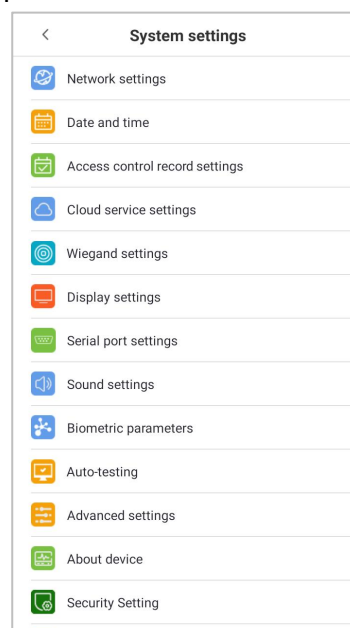
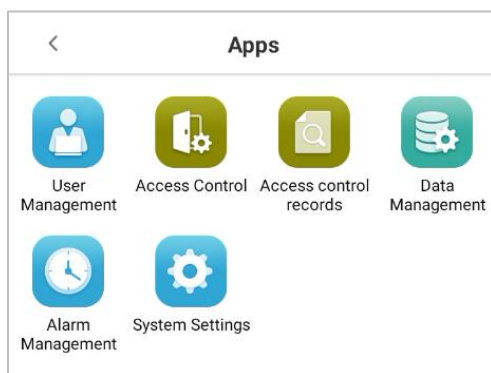
- На екрані Alarm (Сигнал тривоги) натисніть кнопку видалення , а потім виберіть необхідний будильник для видалення.
- Потім натисніть кнопку , яка відображається в правому нижньому куті екрана.



9 Налаштування системи

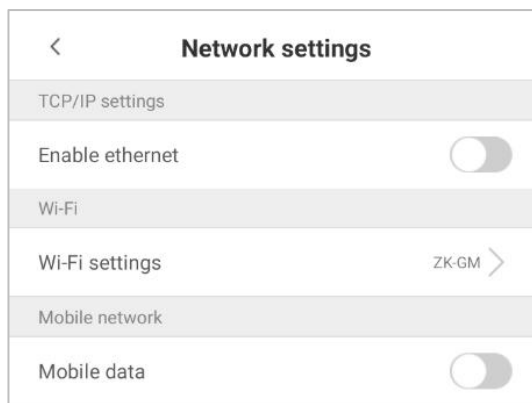
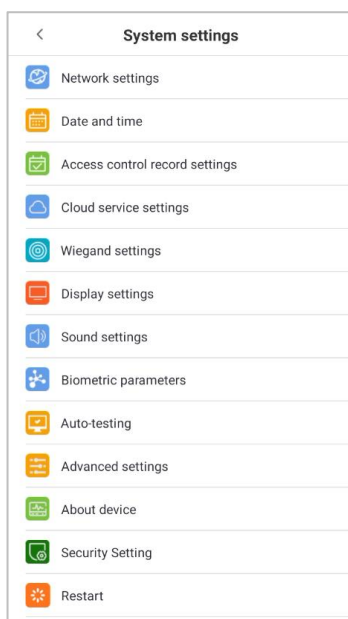
Системні налаштування використовуються для встановлення параметрів системи з метою максимального використання можливостей пристрою відповідно до вимог користувача. У цьому інтерфейсі користувач може редагувати налаштування мережі, налаштування записів контролю доступу, налаштування хмарних служб, налаштування Wiegand тощо.

- У **Main menu** (Головне меню) натисніть **[System Settings]** (Налаштування системи), щоб налаштувати параметри пристрою.



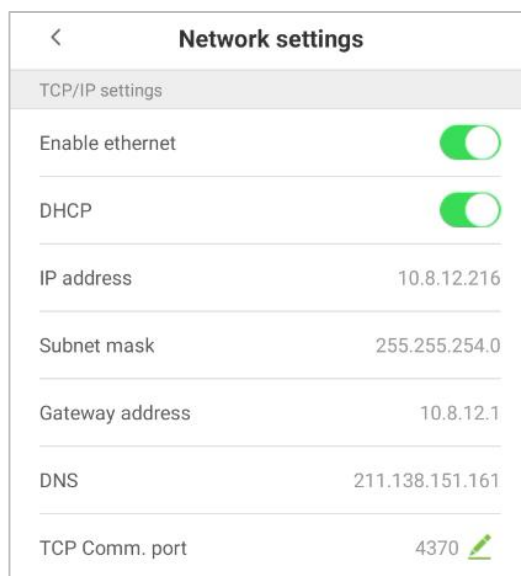
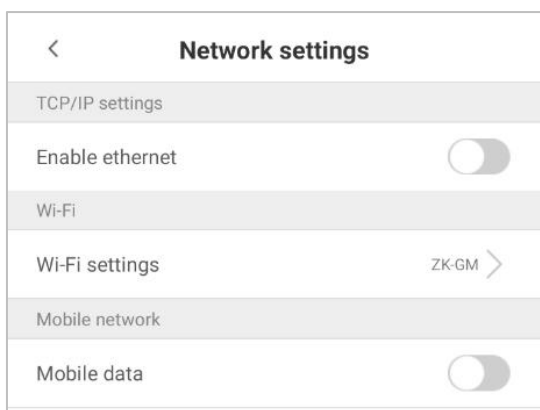
9.1 Налаштування мережі

- В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Network Settings]** (Налаштування мережі), щоб налаштувати параметри.



9.1.1 Налаштування Ethernet

Коли пристрій зв'язується з ПК через Ethernet, мережа повинна бути налаштована таким чином, щоб пристрій і комп'ютер знаходилися в одному сегменті мережі. Якщо пристрій не підключено до мережі, натисніть **[Enable ethernet]** (Увімкнути Ethernet) в інтерфейсі «Network Settings» (Налаштування мережі). З'явиться такий екран:

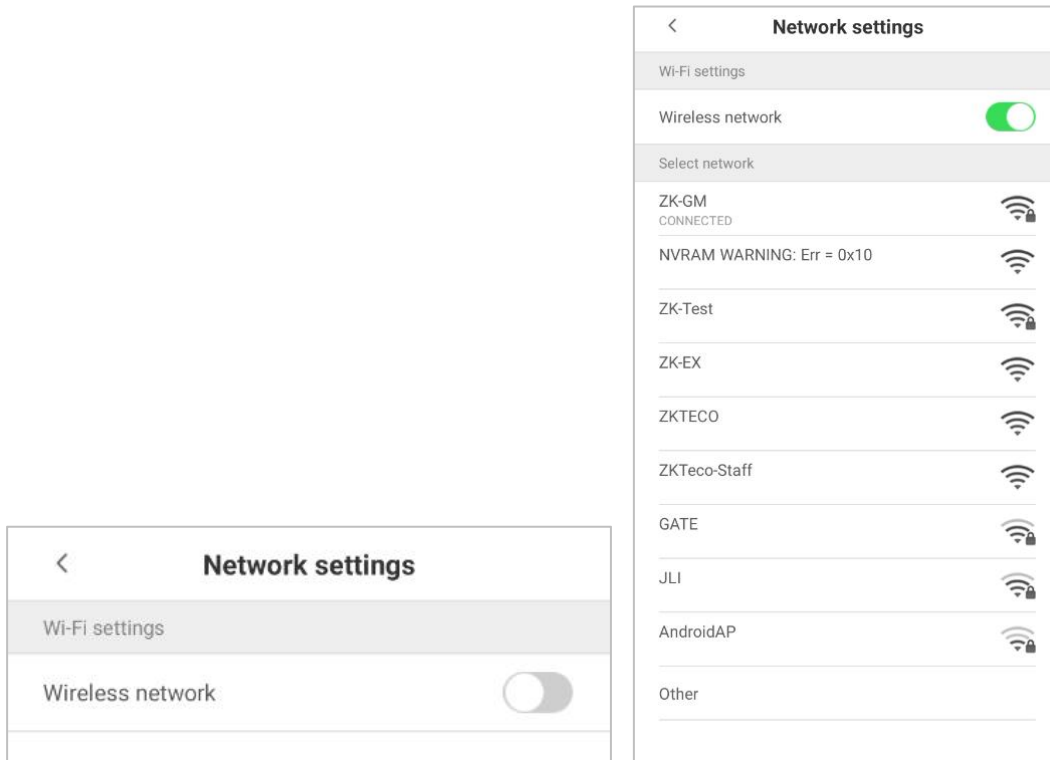


Опис функцій

Menu Options	Function Description
Увімкнення Ethernet	Увімкнути можливість змінювати параметри адреси мережі Ethernet. Якщо ця опція не увімкнена, користувачі не можуть змінювати параметри адреси мережі Ethernet.
DHCP	Увімкніть DHCP, щоб призначити IP-адресу внутрішній мережі або постачальнику мережевих послуг. Якщо DHCP увімкнено, ви не можете вручну встановити IP-адресу пристрою.
IP-адреса	IP-адреса за замовчуванням — 0.0.0.0 (може бути змінена).
Маска підмережі	IP-адреса за замовчуванням — 0.0.0.0 (може бути змінена).
Адреса шлюзу	IP-адреса за замовчуванням — 0.0.0.0 (може бути змінена).
DNS	IP-адреса за замовчуванням — 0.0.0.0 (може бути змінена).
Порт TCP Comm.	Стандартний порт TCP — 4370 (можна змінити).
Примітка: Коли пристрій не підключений до мережі, такі параметри, як IP-адреса та маска підмережі, мають значення 0.0.0.0; коли пристрій підключений до мережі, такі параметри, як IP-адреса та маска підмережі, автоматично відображаються як встановлені значення.	

9.1.2 Налаштування Wi-Fi

Коли пристрій зв'язується з ПК через Wi-Fi, мережа повинна бути налаштована таким чином, щоб пристрій і комп'ютер знаходилися в одному сегменті мережі. Якщо пристрій не підключено до мережі, натисніть **[Wi-Fi settings]** (Налаштування Wi-Fi) в інтерфейсі **«Network Settings»** (Налаштування мережі). З'явиться такий екран:



9.1.3 Мобільна мережа

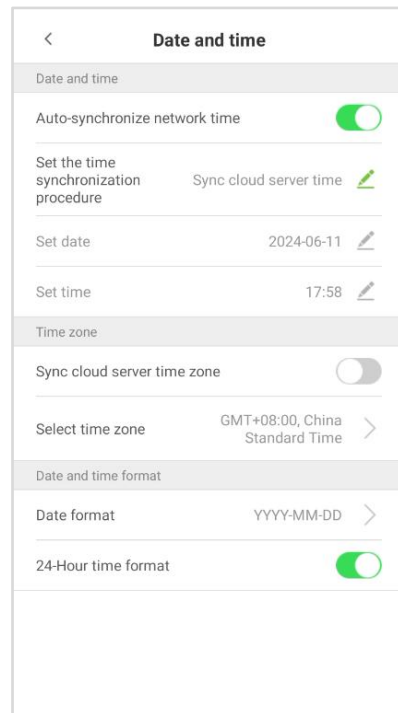
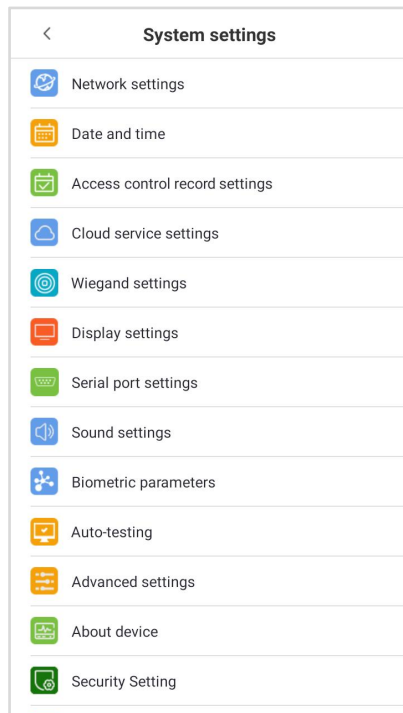
Ви можете отримати доступ до мережі через мобільні дані. Якщо пристрій не підключено до мережі, натисніть **[Mobile Data]** (Мобільні дані) в інтерфейсі **«Network Settings»** (Налаштування мережі). З'явиться такий екран:



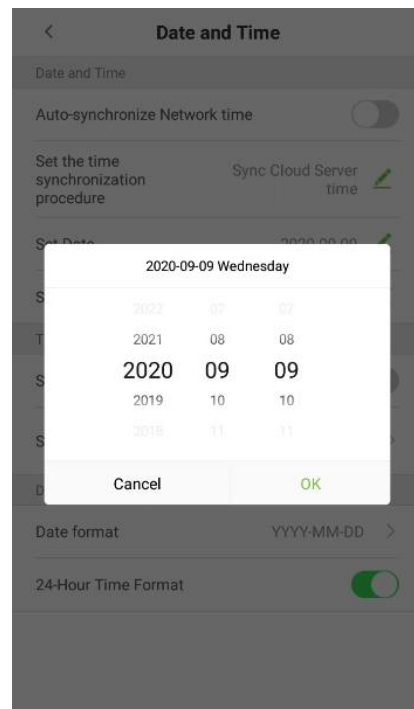
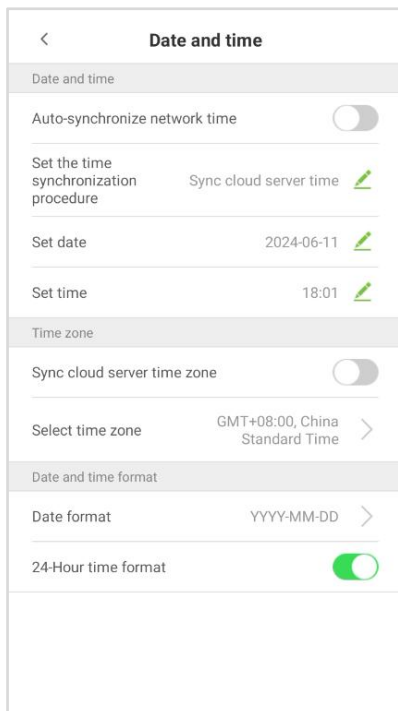
9.2 Дата та час

9.2.1 Налаштування дати та часу

- В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Date and Time]** (Дата та час), щоб перейти до інтерфейсу **Date and Time Settings** (Налаштування дати та часу).

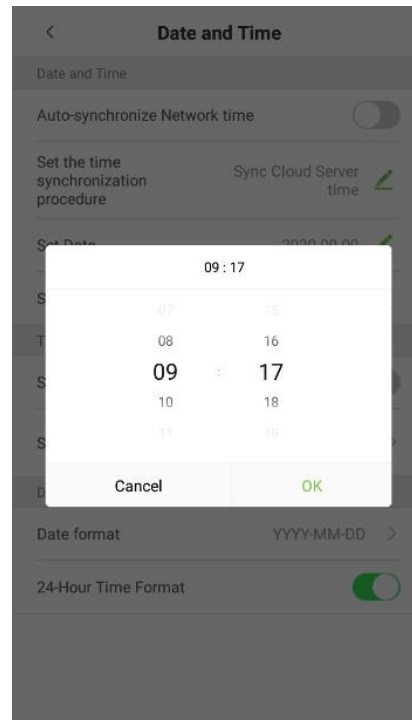
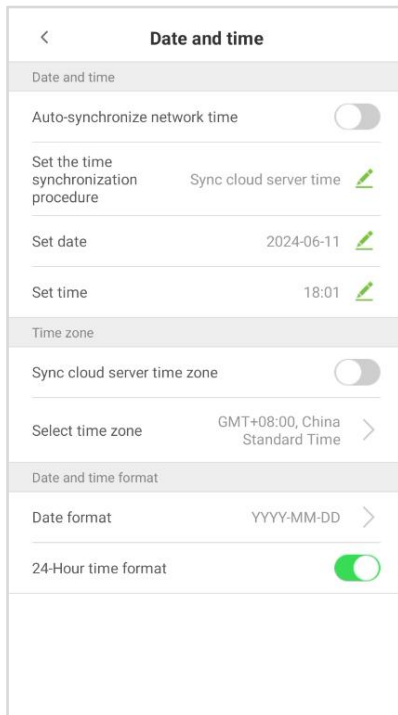


- Натисніть **[Set Date]** (Встановити дату) і проведіть пальцем вгору та вниз, щоб встановити рік, місяць і день.
- Після встановлення необхідної дати натисніть **[OK]**.



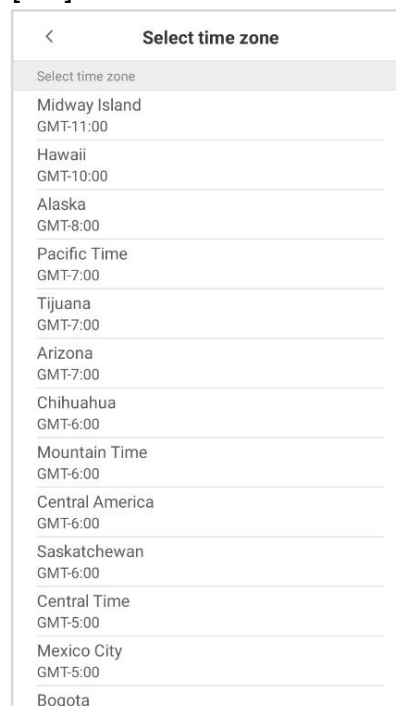
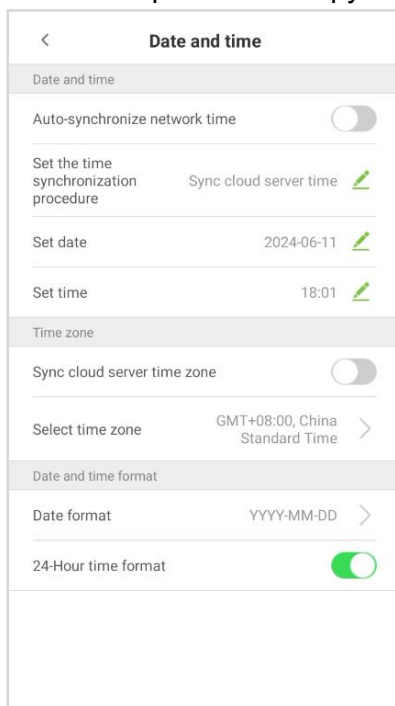
- Натисніть **[Set Time]** (Встановити час) і проведіть пальцем вгору та вниз, щоб встановити години та хвилини.

- Після налаштування часу натисніть **[OK]**.



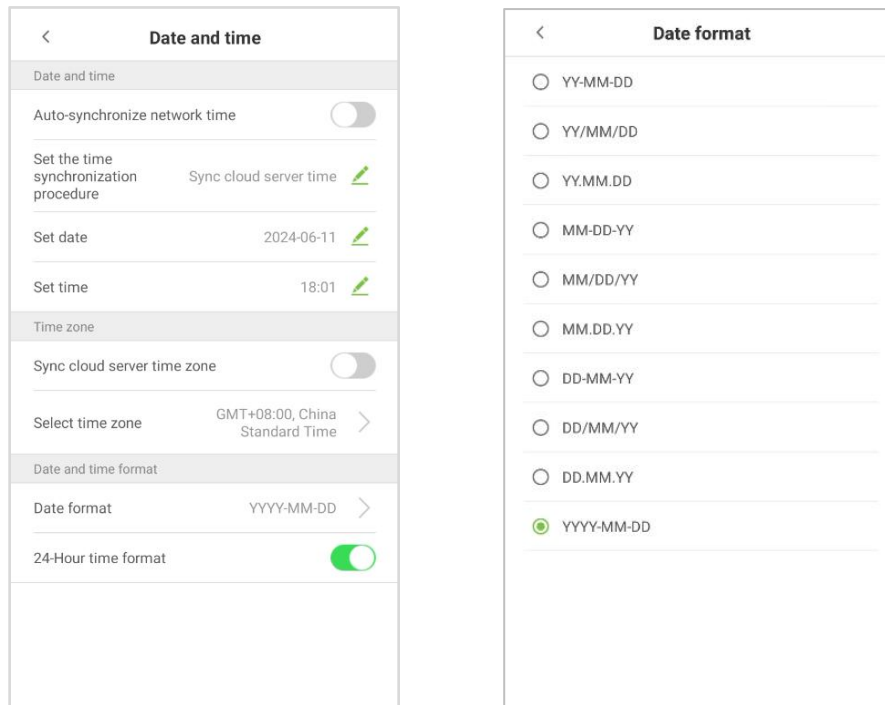
9.2.2 Налаштування часових зон

- Натисніть **[Select time zone]** (Вибрати часову зону), проведіть пальцем вгору і виберіть часовий пояс.
- Після завершення вибору натисніть **[OK]**.

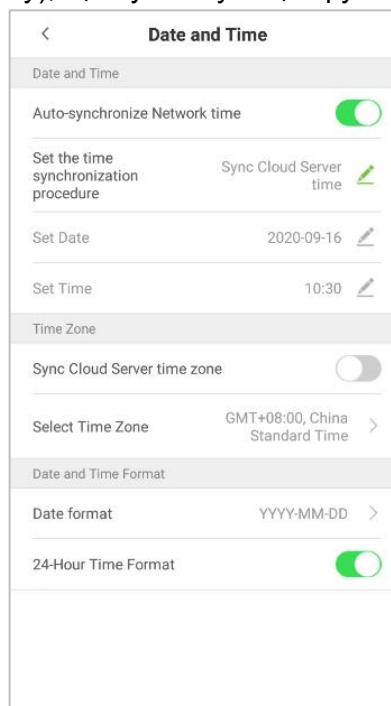


9.2.3 Налаштування формату дати та часу

- В інтерфейсі **Date and Time** (Дата і час) натисніть **[Date format]** (Формат дати).
- На інтерфейсі **Date Format** (Формат дати) виберіть необхідний формат дати.



- В інтерфейсі **Date and Time** (Дата і час) натисніть опцію **[24-Hour Time Format]** (24-годинний формат часу), щоб увімкнути цю функцію.

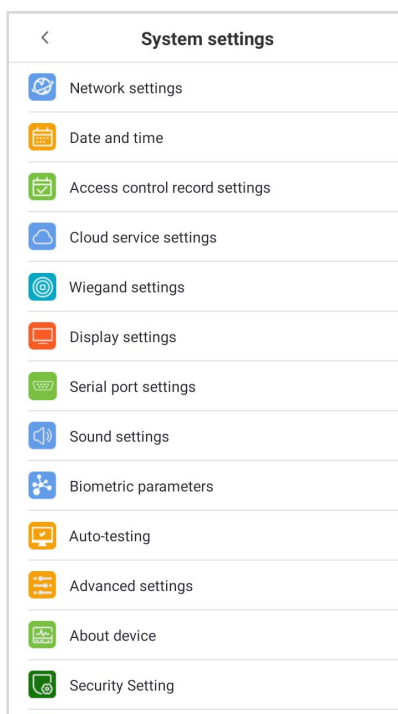


Опис функцій

Параметри меню	Опис
Автоматична синхронізація мережевого часу	Вона ввімкнена за замовчуванням. Користувачі можуть змінювати джерело синхронізації часу. Після вимкнення користувачі можуть змінювати процедуру синхронізації часу та встановлювати дату і час.
Синхронізація часу хмарного сервера	Використовується для синхронізації часу між програмним забезпеченням і сервером, до якого підключено пристрій.
Синхронізація мережевого часу	Він використовується для синхронізації фактичного часу в Інтернеті.
Синхронізація часового поясу хмарного сервера	Ця опція ввімкнена за замовчуванням і використовується для синхронізації часового поясу, встановленого програмним забезпеченням.
Вибір часовий пояс	Часовий пояс за замовчуванням — GMT + 8:00, стандартний час Китаю. Користувачі можуть вибрати часовий пояс відповідно до своїх потреб.
Формат дати	Змінити формат відображення дати
24-годинний формат часу	Після увімкнення цієї функції час перемикається становить 24 години.

9.3 Налаштування записів контролю доступу

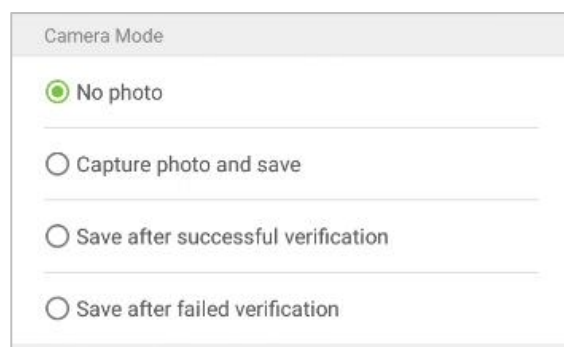
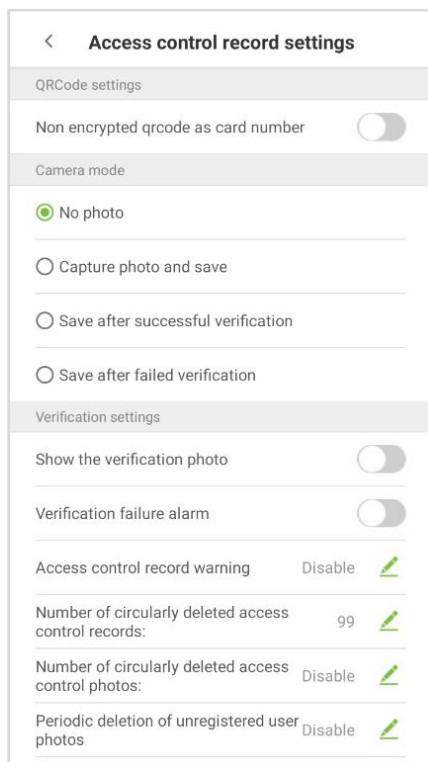
- В інтерфейсі **System Settings** (Налаштування системи) натисніть [**Access Control Record Settings**] (Налаштування записів контролю доступу), щоб перейти до інтерфейсу налаштувань записів доступу.



9.3.1 Режим камери

Ця функція дозволяє встановити умови, наприклад, чи потрібно зберігати фотографії та записи про відвідування після того, як пристрій зробить фотографію персоналу.

- Натисніть на необхідний **Camera Mode** (Режим камери), який ви хочете налаштувати:



- В інтерфейсі **Camera Mode** (Режим камери) користувачі можуть встановити, чи робити фотографії та зберігати їх під час перевірки доступу користувача. Налаштування застосовуються до всіх користувачів.

Опис функцій

Функція	Опис
Без фото	Якщо вибрано цей режим, пристрій не робить фотографії під час аутентифікації.
Зробити фотографію та зберегти	Якщо вибрано цей режим, пристрій робить фотографії користувачів і зберігає їх під час аутентифікації.
Зберегти після успішної верифікації	Якщо вибрано цей режим, то після проходження користувачем перевірки фотографія робиться, а потім зберігається.
Зберегти після невдалої верифікації	Якщо вибрано цей режим, пристрій робить фотографію, коли користувач не проходить верифікацію, і зберігає її.

9.3.2 Налаштування верифікації

Налаштування верифікації полегшують конфігурацію параметрів верифікації доступу.

Verification settings

Show the verification photo ☐

Verification failure alarm ☐

Access control record warning Disable

Number of circularly deleted access control records: 99

Number of circularly deleted access control photos: Disable

Periodic deletion of unregistered user photos Disable

Delay duration of the confirmation screen 3 second(s)

Facial recognition interval 5 second(s)

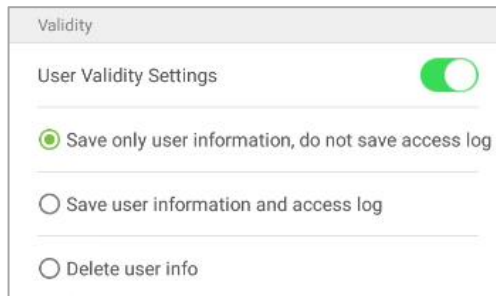
Опис функцій

Опції меню	Опис функцій
Показати фото для перевірки	Якщо ця опція увімкнена, фотографія користувача буде відображатися; якщо ні, фотографія користувача не буде відображатися.
Сигнал про невдалу перевірку	Сигнал тривоги пролунає, коли перевірка не пройде успішно. Час спрацьовування сигналу тривоги про невдалу перевірку можна встановити в діапазоні від 3 до 100 разів, а інтервал між невдалими перевірками — від 8 до 60 секунд.
Попередження про запис контролю доступу	Коли простір для записів контролю доступу досягне заданого значення, пристрій автоматично відобразить попередження про залишок пам'яті для записів. Якщо значення встановлено на 0, функція вимикається.
Кількість циклічно видалених записів контролю доступу	Коли пам'ять записів доступу досягне повної ємності, пристрій автоматично видалить задану кількість старих записів доступу. Якщо значення встановлено як 0, функція буде вимкнена.
Кількість циклічно видалених фотографій контролю доступу	Коли простір для зберігання фотографій контролю доступу буде заповнений, пристрій автоматично видалить задану кількість старих фотографій контролю доступу. Якщо значення встановлено як 0, функція буде вимкнена.
Періодичне видалення фотографій незареєстрованих користувачів	Коли простір для зберігання фотографій у блоці досягне повної ємності, пристрій автоматично видалить задану кількість старих фотографій із блоку. Якщо значення встановлено як 0, функція буде вимкнена.
Тривалість затримки підтвердження екрану	Це час, протягом якого інформація про користувача буде відображатися на екрані системи після успішної перевірки. Його можна встановити від 1 до 9 секунд.
Інтервал розпізнавання обличчя	Це інтервал часу для зіставлення шаблону обличчя, який користувачі можуть встановити від 0 до 9 секунд.

9.3.3 Термін дії інформації про користувача

Це використовується для визначення, чи періоди дії користувачів увімкнені чи вимкнені під час реєстрації користувачів.

- Натисніть **[User Validity Settings]** (Налаштування дійсності користувача), щоб увімкнути.
- Коли налаштування дійсності користувача ввімкнено, з'явиться наступний інтерфейс. Виберіть налаштування, яке ви хочете конфігурувати.



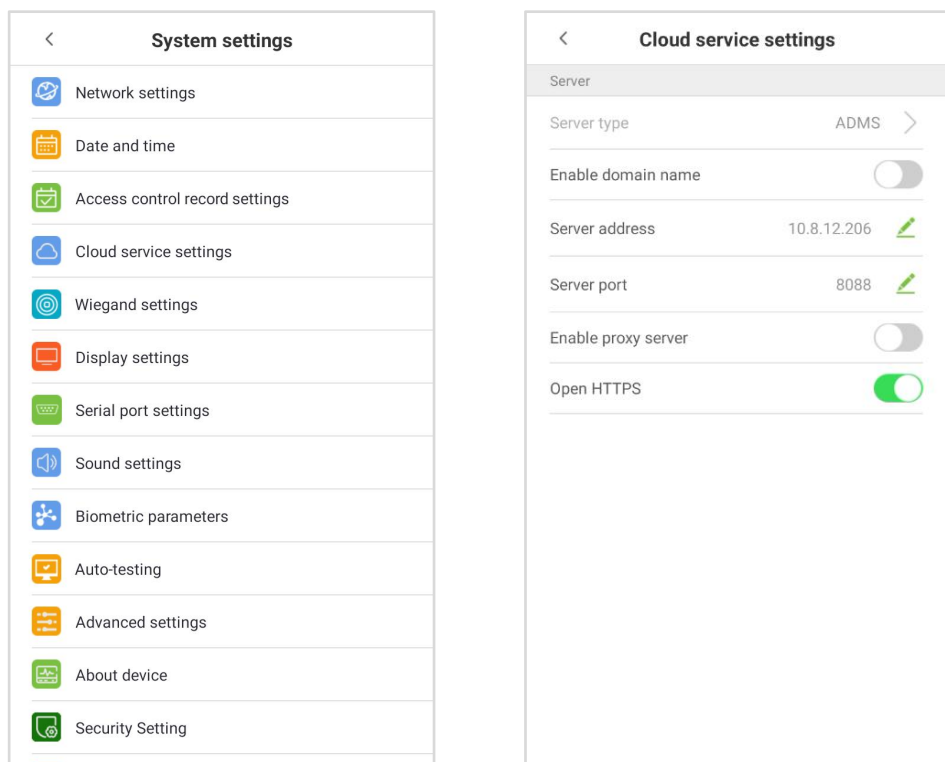
Опис функцій

Опції меню	Опис функції
Зберігати тільки інформацію про користувача, не зберігати журнал доступу	Якщо користувач не пройде повторну перевірку після закінчення терміну дії, інформація про користувача зберігається, а дані про відвідування не зберігаються.
Збереження інформації про користувача та журналу доступу	Якщо термін дії користувача закінчився, інформація про користувача буде збережена, а дані про відвідування будуть збережені.
Видалити інформацію про користувача	Якщо користувач не пройде повторну перевірку після закінчення терміну дії, інформація про користувача та записи про відвідування будуть повністю видалені.

 **Примітка:** Ця функція не буде активована відразу після закінчення терміну дії. Вона буде активована тільки після повторної перевірки системи та відображення повідомлення про помилку.

9.4 Налаштування хмарного сервісу

В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Cloud Service Settings]** (Налаштування хмарної служби), щоб перейти до інтерфейсу налаштувань хмарної служби.

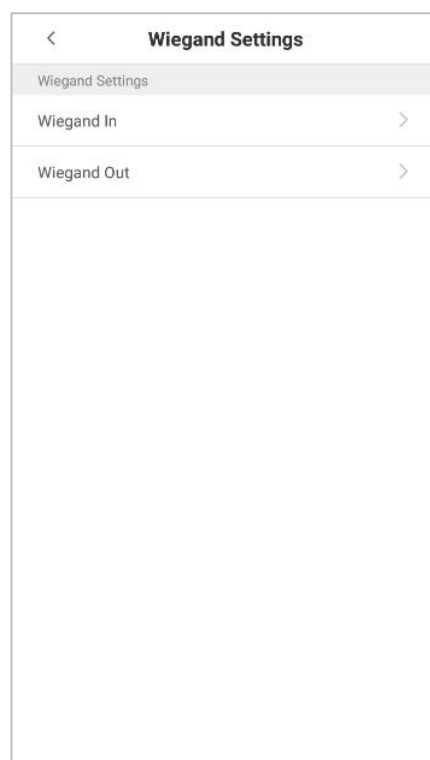
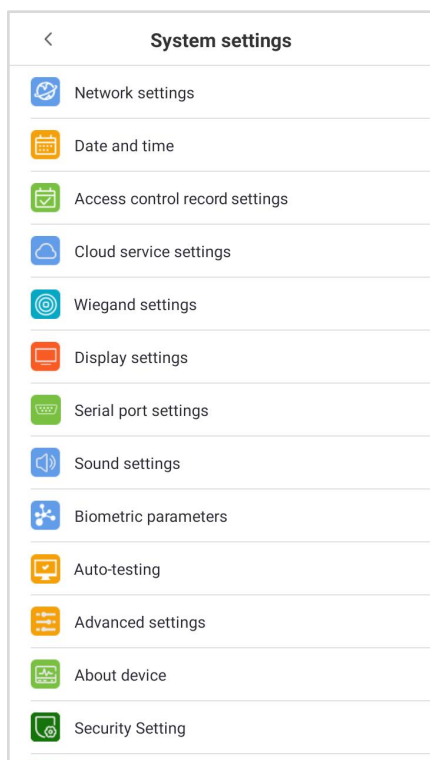


Опис функцій

Пункт		Опис
Увімкнути доменне ім'я	Адреса сервера	Коли ця функція увімкнена, буде використовуватися режим доменного імені «http://...», наприклад http://www.XYZ.com , а «XYZ» позначає доменне ім'я, коли цей режим увімкнено.
Вимкнути доменне ім'я	Адреса сервера	IP-адреса сервера ADMS.
	Порт сервера	Порт, який використовує сервер ADMS.
Увімкнути проксі-сервер		Якщо ви вирішили увімкнути проксі-сервер, вам потрібно вказати IP-адресу та номер порту проксі-сервера.
Відкрити HTTPS		Якщо ця функція увімкнена, для її активації потрібно перезапустити систему, після чого дані завантажуються на push-термінал. Адреса змінюється з HTTP на HTTPS.

9.5 Налаштування Wiegand

В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Wiegand Settings]** (Налаштування Wiegand), щоб відкрити інтерфейс, як показано нижче.



9.5.1 Wiegand вхід

В інтерфейсі налаштувань **Wiegand** натисніть **[Wiegand In]**, щоб відкрити налаштування.



Опис функцій

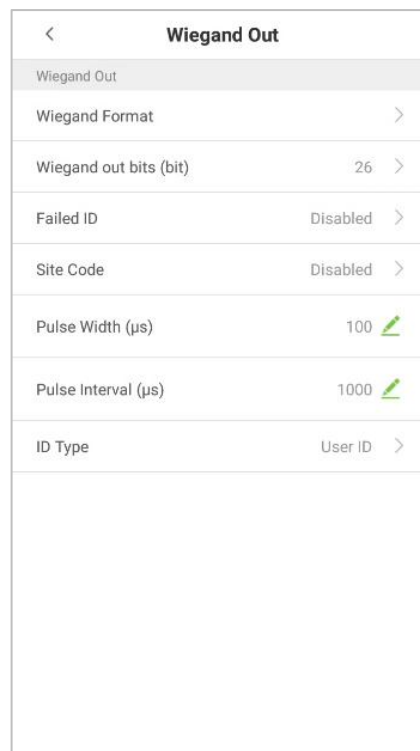
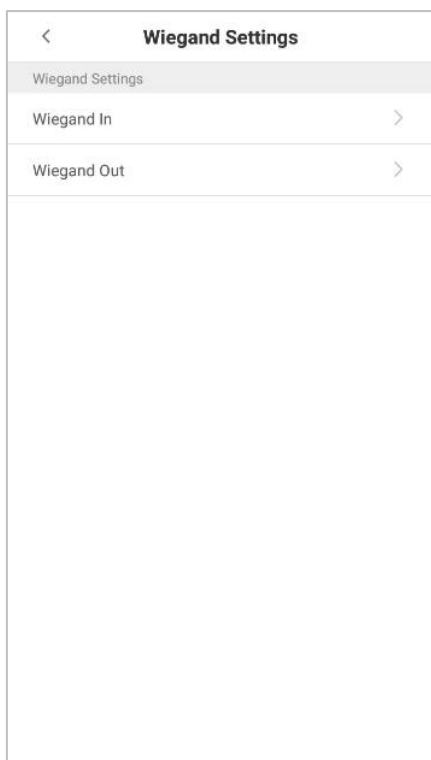
Опції меню	Опис функцій
Формат Wiegand	Значення Wiegand може бути 26 бітів, 34 бітів, 36 бітів, 37 бітів або 50 бітів.
Wiegand в бітах	Він відображає кількість бітів даних Wiegand. Після вибору бітів вхідних даних Wiegand пристрій буде використовувати задану кількість бітів для пошуку відповідного формату Wiegand у форматі Wiegand.
ID Тип	Користувач може ввести ID користувача або номер картки.

Різні поширені визначення формату Wiegand:

Формат Wiegand	Опис
Wiegand26	ЕССССССССССССССССССССССССССССССССО Складається з 26 бітів двійкового коду. 1-й біт є бітом парної парності 2-13-го бітів, а 26-й біт є бітом непарної парності 14-25-го бітів. 2-25-й біти є номерами карток.
Wiegand26a	ЕССССССССССССССССССССССССССССССО Складається з 26 бітів двійкового коду. 1-й біт є бітом парної парності 2-13-го бітів, а 26-й біт є бітом непарної парності 14-25-го бітів. 2-9-й біти є кодами сайту, а 10-25-й біти є номерами карток.
Wiegand34	ЕССССССССССССССССССССССССССССССССО Складається з 34 бітів двійкового коду. 1-й біт є бітом парної парності 2-17-го бітів, а 34-й біт є бітом непарної парності 18-33-го бітів. 2-25-й біти є номерами карток.
Wiegand34a	ЕССССССССССССССССССССССССССССССССО Складається з 34 бітів двійкового коду. 1-й біт є бітом парної парності 2-17-го бітів, а 34-й біт є бітом непарної парності 18-33-го бітів. 2-9-й біти є кодами сайту, а 10-25-й біти є кодами картки. numbers.
Wiegand36	ОFFFFFFFFFFFFFFFFFFFFССССССССССССССССССММЕ Складається з 36 бітів двійкового коду. 1-й біт є бітом непарної парності 2-18-го бітів, а 36-й біт є бітом парної парності 19-35-го бітів. 2-17-й біти є кодами пристроїв. 18-33-й біти є номерами карток, а 34-35-й біти є кодами виробників.
Wiegand36a	ЕFFFFFFFFFFFFFFFFFFFFССССССССССССССССССО Складається з 36 бітів двійкового коду. 1-й біт є бітом парної парності 2-18-го бітів, а 36-й біт є бітом непарної парності 19-35-го бітів. 2-19-й біти є кодами пристроїв, а 20-35-й біти є номерами карток.
Wiegand37	ОММММССССССССССССССССССССССССССССССССЕ Складається з 37 бітів двійкового коду. 1-й біт є бітом непарної парності 2-го до 18-го бітів, а 37-й біт є бітом парної парності 19-го до 36-го бітів. 2-й до 4-го біти є кодами виробника. 5-й до 16-го біти є кодами місця, а 21-й до 36-го біти є номерами карток.
Wiegand37a	ЕМММFFFFFFFFFFFFSSSSSSССССССССССССССССССО Складається з 37 бітів двійкового коду. 1-й біт є бітом парної парності 2-го до 18-го бітів, а 37-й біт є бітом непарної парності 19-го до 36-го бітів. 2-й до 4-го біти є кодами виробника. 5-й до 14-го біти є кодами пристрою, 15-й до 20-го біти є кодами місця, а 21-й до 36-го біти є номерами карток.
Wiegand50	ЕССО Складається з 50 бітів двійкового коду. 1-й біт є бітом парної парності 2-25-го бітів, а 50-й біт є бітом непарної парності 26-49-го бітів. 2-17-й біти є кодами сайту, а 18-49-й біти є номерами карток.
«С» позначає номер картки; «Е» позначає біт парної парності; «О» позначає біт непарної парності; «F» позначає код об'єкта; «М» позначає код виробника; «Р» позначає біт парності; «S» позначає код місця.	

9.5.2 Wiegand Вихід

В інтерфейсі **Wiegand Settings** (Налаштування Wiegand) натисніть **[Wiegand Out]** (Вихід Wiegand), щоб відкрити інтерфейс **Wiegand Out** (Вихід Wiegand).

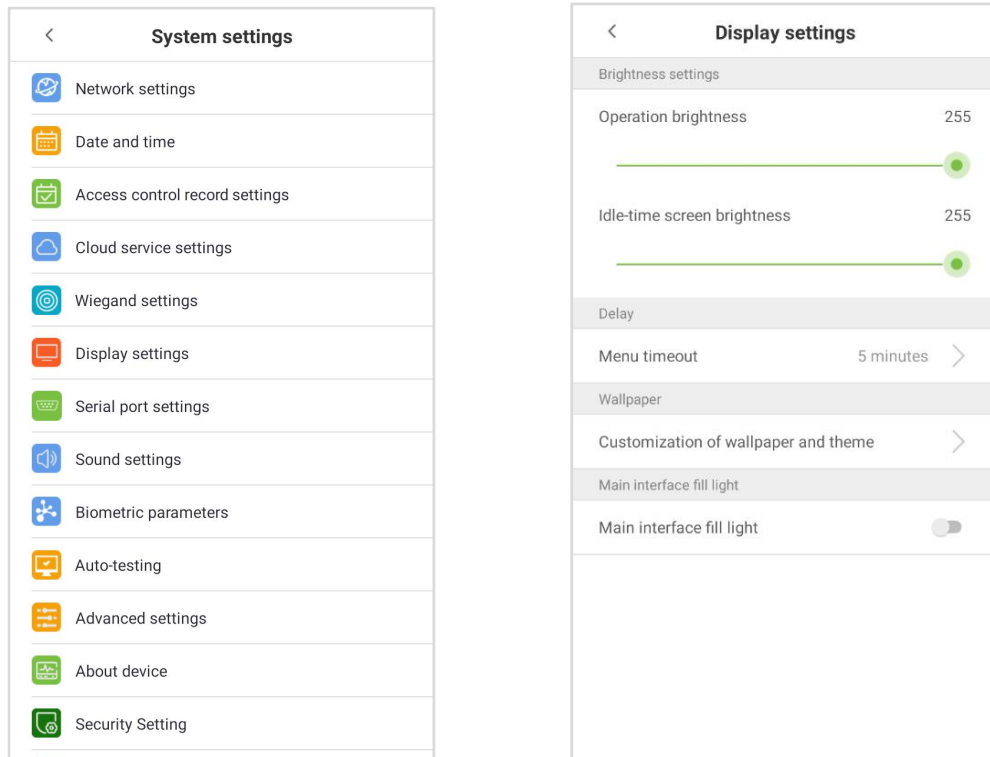


Function Description

Опції меню	Опис функції
Формат Wiegand	Значення формату Wiegand може бути 26 біт, 34 біт, 36 біт, 37 біт, 50 біт.
Біти Wiegand out	Вибравши формат Wiegand, ви можете вибрати одну з відповідних вихідних цифр у форматі Wiegand.
Неправильний ID	Якщо перевірка не пройшла, система надішле ідентифікатор, що не пройшов перевірку, на пристрій і замінить номер картки або ідентифікатор персоналу на нові.
Код сайту	Він схожий на ідентифікатор пристрою, за винятком того, що його можна встановити вручну і повторювати на різних пристроях. Значення за замовчуванням знаходиться в діапазоні від 0 до 256.
Ширина імпульсу (мкс)	Ширина імпульсу відображає зміни величини електричного заряду з високою частотою ємності, що регулярно відбуваються протягом певного часу.
Інтервал імпульсу (мкс)	Інтервал часу між імпульсами.
Тип ID	Виберіть тип ID як ID користувача або номер картки.

9.6 Налаштування дисплея

- В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Display Settings]** (Налаштування дисплея), щоб перейти до інтерфейсу **Display Settings** (Налаштування дисплея).



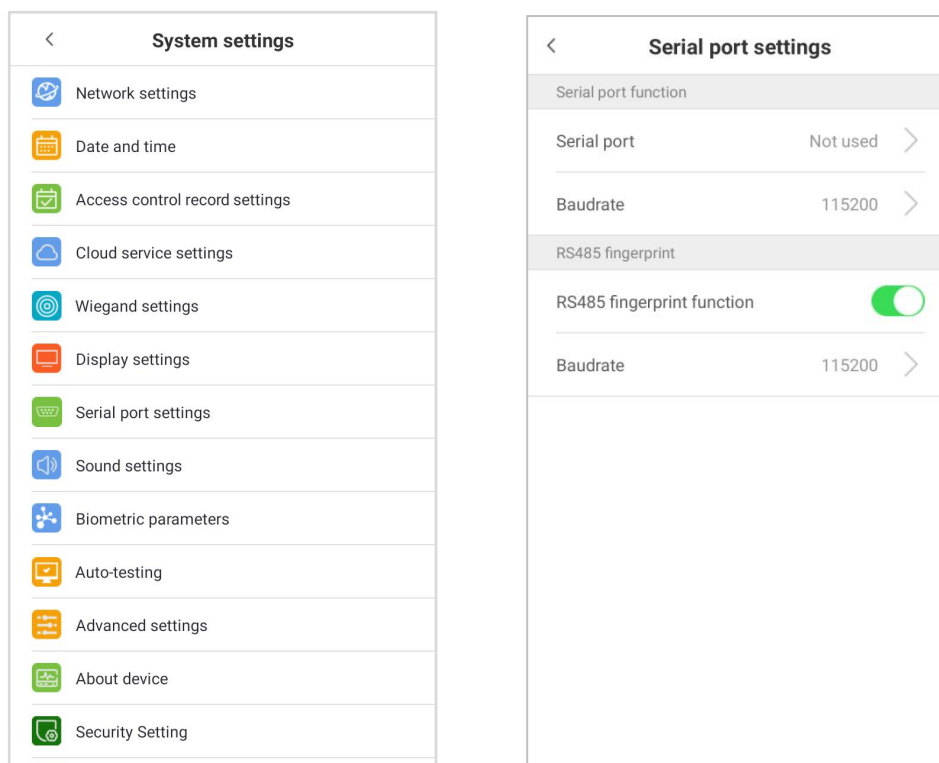
Опис функцій

Menu Options		Function Description
Налаштування яскравості	Робоча яскравість	Встановіть яскравість роботи пристрою, наприклад, під час налаштування параметрів або розпізнавання обличчя.
	Яскравість екрану в режимі очікування	Яскравість екрану, коли пристрій перебуває в режимі очікування.
Затримка	Час очікування меню	Тайм-аут меню виникає, коли протягом певного часу після входу користувача в меню не виконується жодна операція, і меню переходить в режим очікування. Параметри включають: 1 хвилина, 2 хвилини, 5 хвилин, 10 хвилин.
Шпалери	Налаштування шпалер та теми	Виберіть улюблені шпалери з інтерфейсу тематичних шпалер.

Основний інтерфейс заливки світлом	Основний інтерфейс заливки світлом	Коли яскравість навколишнього середовища виявляється нижчою за встановлене значення яскравості, на головному екрані з'являється підсвічування сторінки.
------------------------------------	------------------------------------	---

9.7 Налаштування послідовного порту

- В інтерфейсі налаштувань системи натисніть **[Serial port settings]** (Налаштування послідовного порту), щоб перейти до інтерфейсу налаштувань звуку.

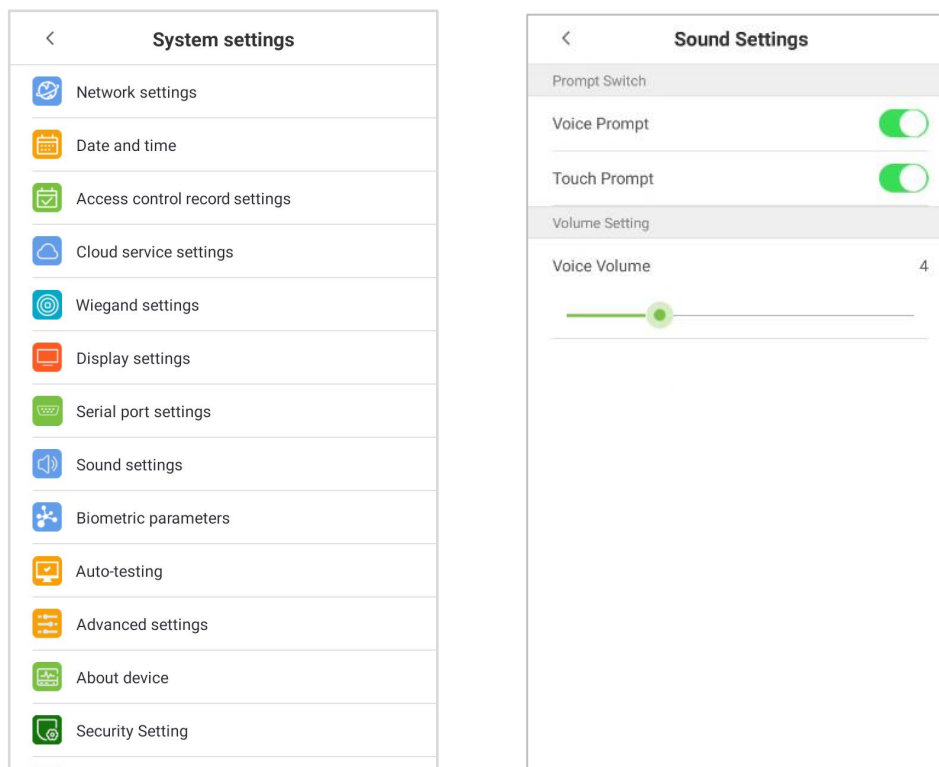


Опис функцій

Опції меню	Опис функцій
Послідовний порт	Не використовується: Не спілкуйтеся з пристроєм через послідовний порт.
Швидкість передачі даних	Швидкість передачі даних на ПК, є 4 варіанти швидкості передачі даних: 115200 (за замовчуванням), 57600, 38400 і 19200. Чим вища швидкість передачі даних, тим швидша швидкість зв'язку, але й менша надійність. Тому вищу швидкість передачі даних можна використовувати, коли відстань зв'язку коротка; коли відстань зв'язку велика, вибір нижчої швидкості передачі даних буде надійнішим.
Функція відбитків пальців RS485	Зв'язується з датчиком відбитків пальців RS485 через послідовний порт RS485.

9.8 Налаштування звуку

- В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Sound Settings]** (Налаштування звуку), щоб перейти до інтерфейсу налаштувань звуку.

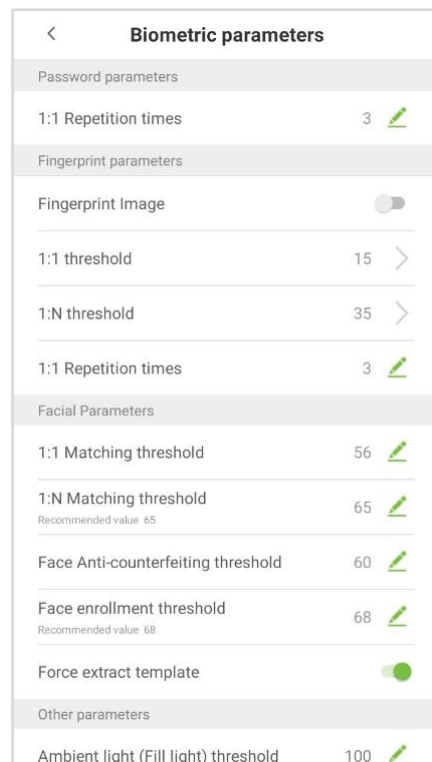
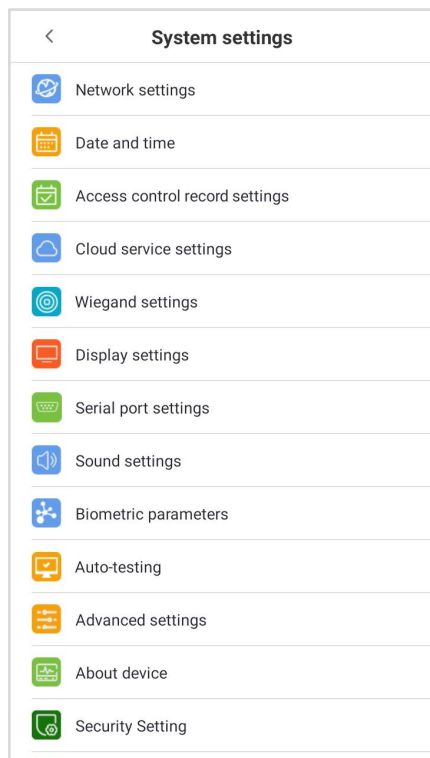


Опис функцій

Опції меню	Опис функцій
Голосова підказка	Коли голосові підказки увімкнені, користувачі отримуватимуть голосові підказки. Коли це налаштування вимкнене, голосові підказки не надходитимуть. Коли голосові підказки вимкнені, а потім знову увімкнені, рівень гучності автоматично встановлюється на 1.
Сенсорна підказка	Цей перемикач вмикає/вимикає підказки на сенсорному екрані. Коли підказки на сенсорному екрані ввімкнені, користувачі отримуватимуть підказки на сенсорному екрані. Коли підказки на сенсорному екрані вимкнені, підказки на сенсорному екрані не надходитимуть.
Гучність звуку	Використовується для регулювання гучності. Ця функція доступна тільки в разі увімкнення звукових підказок. Можна встановити значення від 0 до 15.

9.9 Біометричні параметри

- В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Biometric Parameters]** (Біометричні параметри), щоб перейти до інтерфейсу біометричних параметрів.



Опис функцій

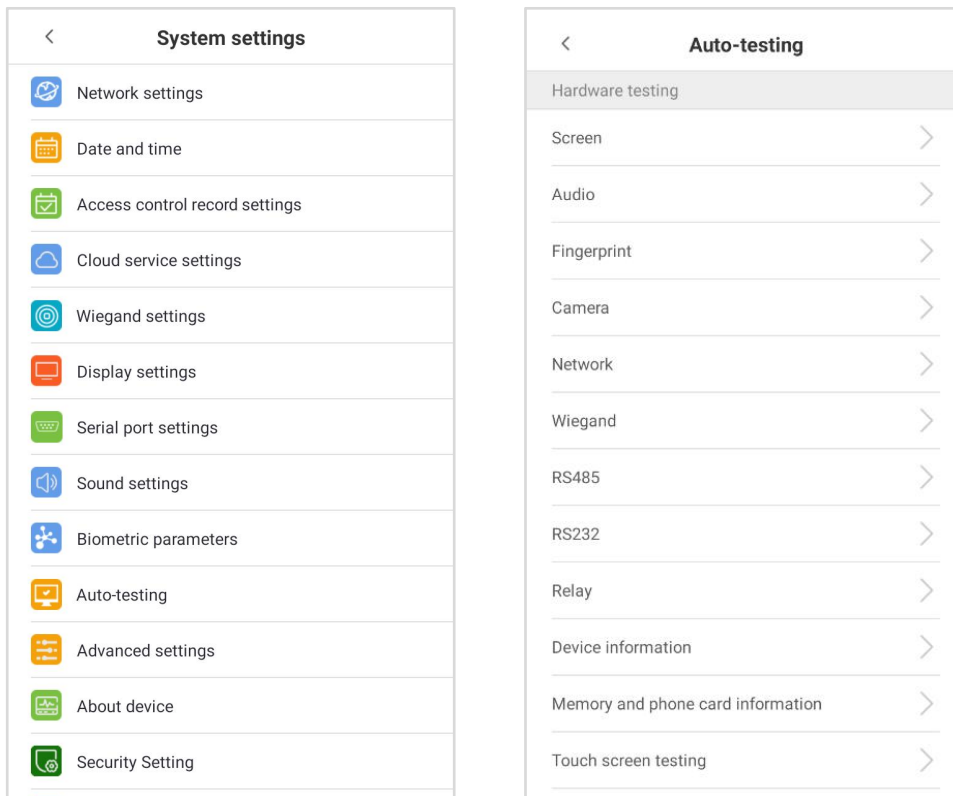
Меню		Опис функцій
Параметри пароля	1:1 Кількість повторень	Верхня межа кількості невдалих спроб перевірки пароля 1:1. Коли кількість невдалих спроб введення пароля досягає заданого значення, перевірка користувача завершується невдачею і, за необхідності, може бути повторена.
Параметри відбитків пальців ★	Зображення відбитка пальця	При увімкненні для перевірки буде відображено зображення відбитка пальця.
	1:1 Threshold	При проведенні перевірки відбитків пальців 1:1 дані відбитків пальців збираються і миттєво порівнюються з даними відбитків пальців за допомогою алгоритму 1:1. Це перетворюється на значення, яке потім порівнюється із заданим значенням. Якщо значення відсканованого відбитка пальця перевищує задане значення, перевірка проходить успішно. Якщо ні, перевірка провалюється. Чим вищий поріг, тим точніше збіг; чим нижчий поріг, тим вищий рівень успішності збігу.

	1: N Поріг	Під час проведення перевірки 1: N дані відбитків пальців збираються і миттєво порівнюються з усіма шаблонами відбитків пальців у системі за допомогою алгоритму 1: N. Це перетворюється на значення, яке порівнюється з заданим значенням. Якщо значення відсканованого відбитка пальця перевищує задане значення, верифікація проходить успішно. Якщо ні, верифікація провалюється. Чим вище поріг, тим точніше збіг; чим нижче поріг, тим вища ймовірність успішного збігу.
	1:1 Кількість повторень	Верхня межа кількості невдалих спроб верифікації відбитків пальців 1:1. Коли кількість невдалих спроб верифікації пароля досягає заданого значення, верифікація користувача завершується невдачею і за необхідності може бути повторена.
Параметри обличчя	Поріг відповідності 1:1	Під час проведення перевірки обличчя 1:1 дані обличчя збираються і миттєво порівнюються з даними обличчя за допомогою алгоритму 1:1. Це перетворюється на значення, яке потім порівнюється з заданим значенням. Якщо значення відсканованого обличчя перевищує задане значення, перевірка проходить успішно. Якщо ні, перевірка провалюється. Чим вище поріг, тим точніше збіг; чим нижче поріг, тим вища ймовірність успішного збігу.
	1: N Поріг відповідності	Під час проведення перевірки 1: N дані обличчя збираються і миттєво порівнюються з усіма шаблонами обличчя в системі за допомогою алгоритму 1: N. Це перетворюється на значення, яке порівнюється з заданим значенням. Якщо значення відсканованого обличчя перевищує задане значення, перевірка проходить успішно. Якщо ні, перевірка провалюється. Чим вище поріг, тим точніше збіг; чим нижче поріг, тим вища ймовірність успішного збігу.
	Поріг захисту від підробки обличчя	Встановіть параметр N. Розпізнавання є успішним лише тоді, коли точність розпізнавання перевищує N. Поріг розпізнавання обличчя — це поріг схожості, отриманий під час розпізнавання облич. (Може використовуватися з інфрачервоною системою захисту від підробки, буде більш суворим)
	Поріг реєстрації обличчя	У розпізнаванні обличчя, чим вище встановлено поріг, тим вищою буде точність розпізнавання обличчя, що може призвести до неможливості розпізнавання. Навпаки, якщо поріг занадто низький, точність розпізнавання обличчя буде нижчою, що може призвести до помилкових суджень та інших явищ. Значення за замовчуванням становить 76.

	Шаблон витягу обличчя	Для деяких фотографій низької якості можна заздалегідь застосувати шаблон після відкриття, але це може призвести до неправильної оцінки.
Інші параметри	Поріг освітлення навколишнього освітлення (додаткове освітлення)	Використовується для визначення яскравості навколишнього світла. Коли яскравість навколишнього середовища менше порогового значення, вмикається допоміжне світло; коли яскравість перевищує порогове значення, допоміжне світло не вмикається. Значення за замовчуванням — 100.
	Поріг виявлення руху	Використовується для виявлення наявності рухомої людини перед пристроєм, щоб визначити, чи ввімкнено функцію розпізнавання обличчя. Значення за замовчуванням — 500.
	Кут розпізнавання обличчя	Щоб обмежити кут обличчя при розпізнаванні обличчя, рекомендований поріг становить 20.
	Розмір обличчя для розпізнавання	Розмір обличчя під час розпізнавання обличчя. Чим менше значення, тим далі відстань виявлення, і навпаки, чим більше значення, тим ближче відстань.
	Антистрічковий ефект	Антикамерна водна хвиля, коли на відеосигнал камери впливають статична електрика, електромагнітні та інші перешкоди, що призводить до появи водних хвиль на зображенні і навіть до спотворення картини.
	Запобігання одночасному розпізнаванню обличчя з декількох входів	Якщо на вході, розташованому поруч, встановлено кілька пристроїв, увімкніть цю функцію, щоб запобігти одночасному розпізнаванню обличчя кількома пристроями. Встановіть поріг для трьох типів: високий, середній і низький. Чим вищий поріг, тим менша відстань між напрямними лініями і менший діапазон розпізнавання обличчя на екрані. Під час встановлення порогу рекомендується увімкнути функцію корекції допоміжних ліній.

9.10 Автоматичне тестування

- В інтерфейсі налаштувань системи натисніть **[Auto-Testing]** (Автоматичне тестування), щоб перейти до інтерфейсу автоматичного тестування.

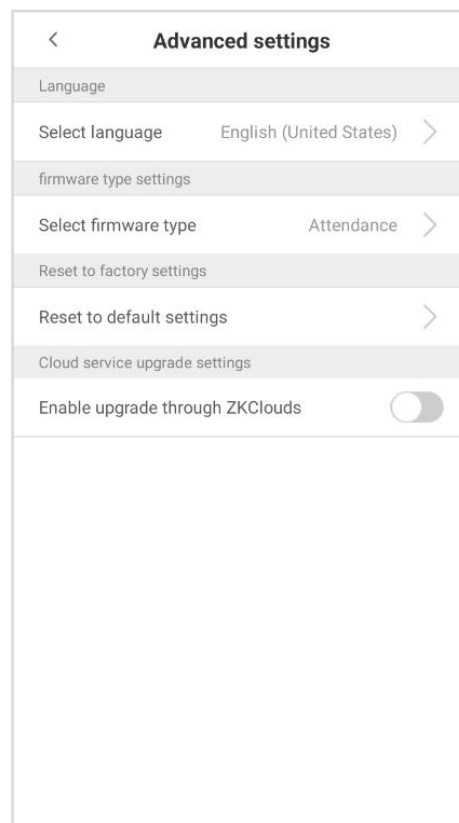
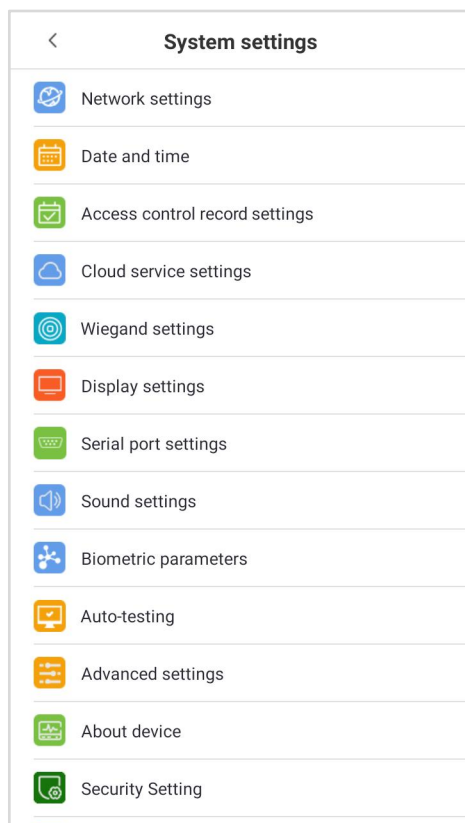


Опис функцій

Опції меню	Опис функції
Екран	Він використовується для тестування дисплея екрану. На екрані будуть відображатися червоні, зелені, сині, білі та чорні тести. Перевірте, чи колір екрану є рівномірним у всіх його частинах. Під час тестування натисніть будь-де на екрані, щоб продовжити тестування.
Аудіо	Пристрій автоматично перевіряє звукові підказки, відтворюючи аудіофайли, що зберігаються в пристрої. Перевірка голосу в основному перевіряє, чи аудіофайли пристрою є повними та чи аудіоефекти працюють належним чином. Натисніть клавішу «Назад», щоб вийти з тестування.
Відбиток пальця	Використовується для перевірки правильності функціонування сканера відбитків пальців. Перевірте, чи зображення відбитка пальця чітке і придатне для використання.
Камера	Він використовується для перевірки правильності функціонування камери. Перевірте зняте зображення, щоб переконатися, що якість зображення чітка і придатна для використання.
Мережа	Введіть IP-адресу та натисніть ring, щоб перевірити, чи можна успішно виконати ring мережі.
Wiegand	Перевірте Wiegand in і Wiegand out, щоб переконатися, що все працює.
RS485	Використовується для перевірки, чи може зчитувальна головка RS485 нормально передавати дані.
Реле	Використовується для перевірки нормальної роботи сигналу відкриття/закриття шафки та відкриття/закриття.

9.11 Додаткові налаштування

- У списку **System Settings** (Налаштування системи) натисніть **[Advanced settings]** (Додаткові налаштування), щоб перейти до інтерфейсу додаткових налаштувань.



Опис функцій

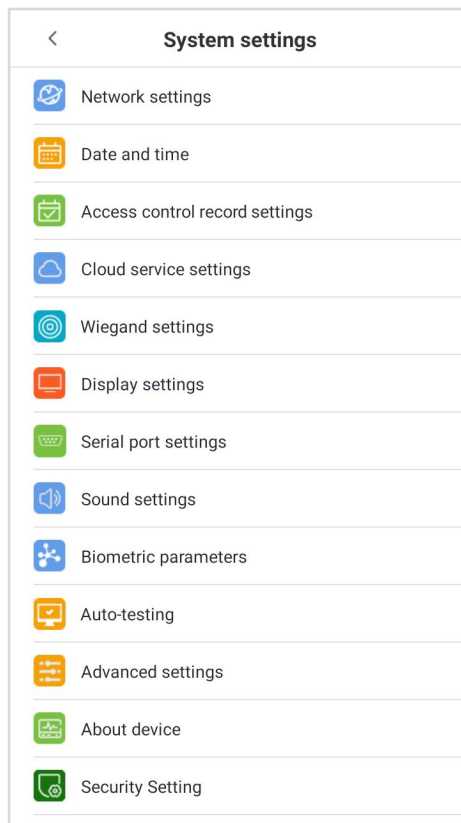
Опції меню	Опис функції
Виберіть мову	Підтримка традиційного китайського (Тайвань), традиційного китайського (Гонконг), спрощеного китайського, японського, англійського, іспанського, іспанського (Латинська Америка), французького, індонезійського, португальського (Бразилія), в'єтнамського, турецького, російського, перського, арабського, тайського, корейського.
Select firmware type	Він використовується для перемикання між прошивкою відвідування та прошивкою доступу. Після перемикання всі дані будуть видалені.
Reset to default settings	Відновить налаштування прошивки до значень за замовчуванням і виберіть, чи потрібно очистити дані.
ADB Network Debug	Інструмент ADB — це інструмент для налагодження Android. Це вікно командного рядка, яке використовується для взаємодії з симулятором або реальним пристроєм через комп'ютер.
Enable upgrade through ZKClouds	Він може використовувати програмне забезпечення для доставки файлу оновлення прошивки для онлайн-оновлення.



Примітка: Якщо вам потрібен файл для оновлення, зверніться до наших технічних фахівців. За звичайних обставин оновлення прошивки не рекомендується.

9.12 Про пристрій

- В інтерфейсі **System Settings** (Налаштування системи) натисніть **[About the Device]** (Про пристрій), щоб відкрити інтерфейс **About the Device** (Про пристрій).

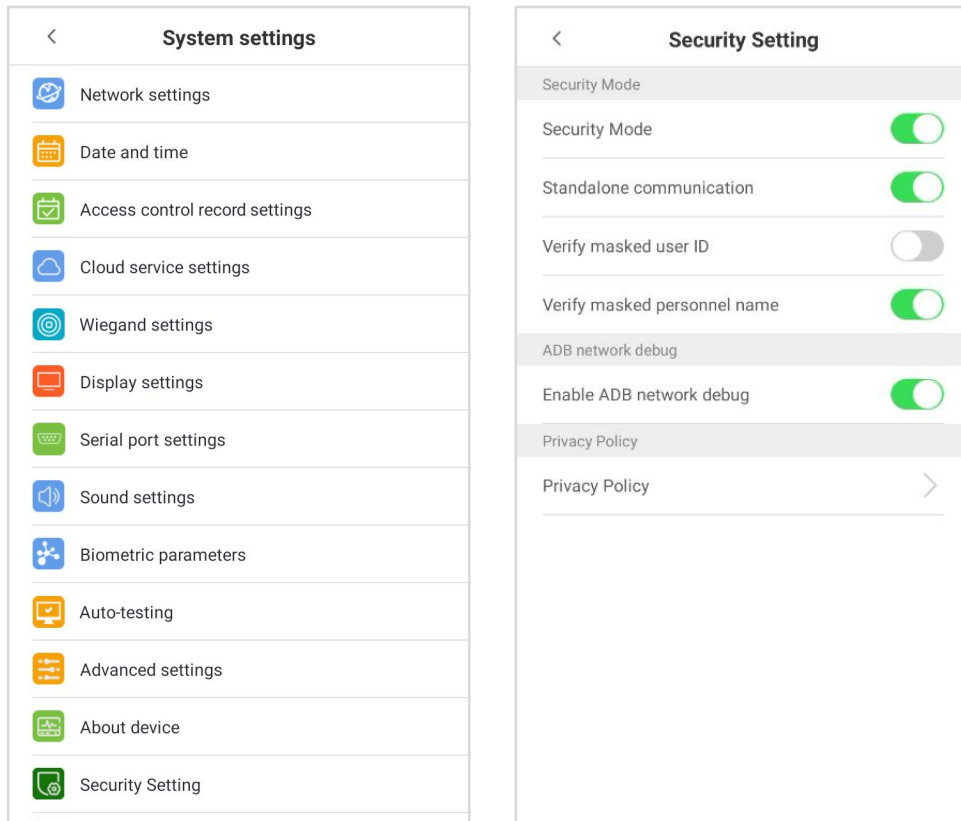


Опис функції

Опції меню	Function Description
Інформація про місткість	Він відображає поточну ємність пристрою користувача, відбитки пальців ★ та шаблони обличчя, адміністраторів, записи контролю доступу, фотографії контролю доступу, фотографії незареєстрованих користувачів та фотографії користувачів.
Інформація про пристрій	Він відображає основну інформацію про пристрій, інформацію про версію алгоритму та інформацію про версію прошивки.
Версія	Він відображає всі версії всіх системних додатків, таких як системні налаштування, управління даними та інші встановлені додатки.

9.13 Налаштування безпеки

- В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Security Setting]** (Налаштування безпеки), щоб відкрити інтерфейс **Security Setting** (Налаштування безпеки).

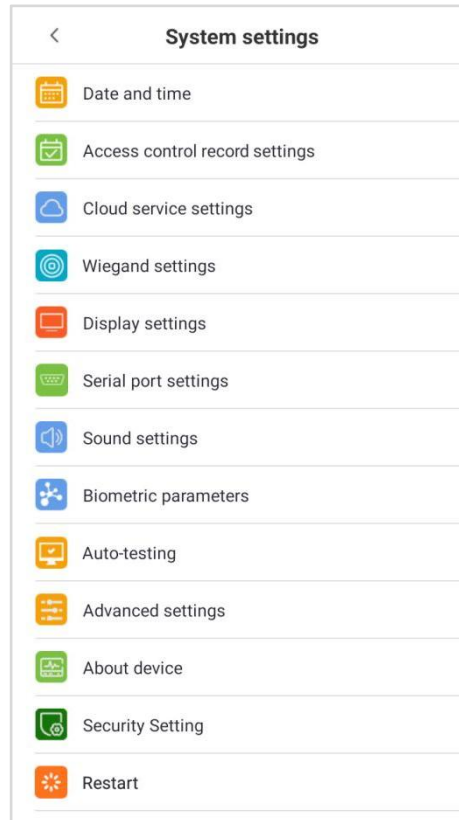


Опис функції

Опції меню	Опис функції
Режим безпеки	Фотографії користувачів будуть шифруватися в пристрої та під час обміну даними з програмним забезпеченням.
Автономна комунікація	Запустити автономний зв'язок.
ID користувача з маскою Verity	Після увімкнення функції ідентифікаційний номер працівника користувача не відображається під час перевірки відвідування.
ID користувача з маскою Verity	Після увімкнення цієї функції ім'я користувача не буде відображатися під час перевірки відвідуваності.
Увімкнути налагодження мережі ADB	Запустити налагодження мережі ADB.
Privacy Policy	Угода про конфіденційність доступу.

9.14 Перезапуск

- В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Restart]** (Перезапустити), щоб перезавантажити пристрій.



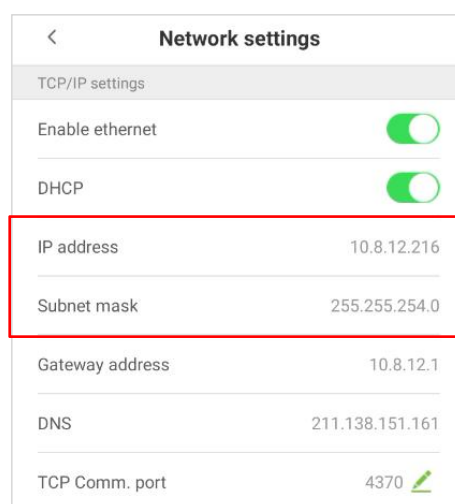
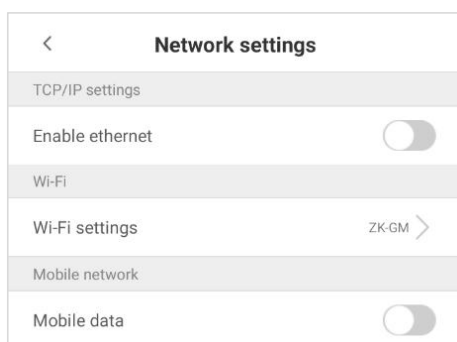
10 Підключення до програмного забезпечення ZKBio CVAccess

10.1 Встановити адресу зв'язку

Сторона пристрою

1. Натисніть **[Enable ethernet]** (Увімкнути Ethernet) в інтерфейсі **«Network Settings»** (Налаштування мережі), щоб встановити IP-адресу та шлюз пристрою.

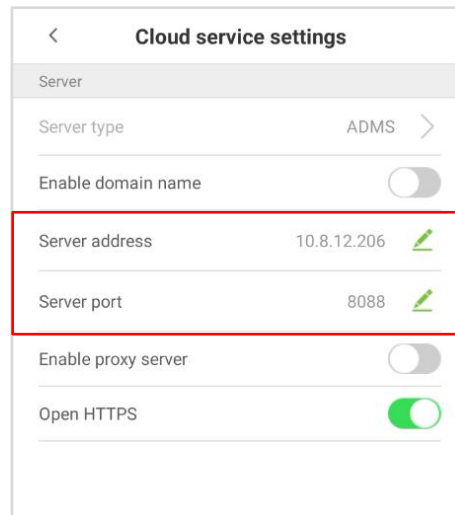
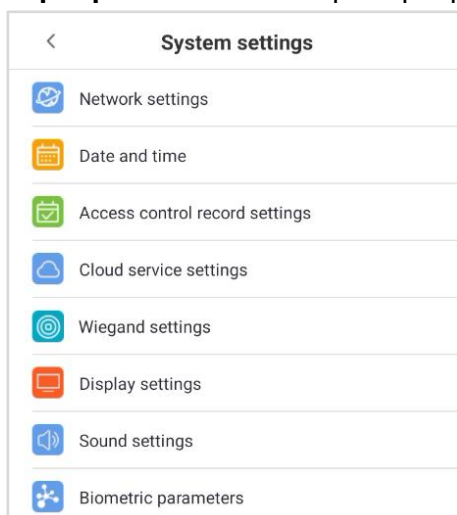
Примітка: Переконайтеся, що IP-адреса знаходиться в тому ж сегменті мережі, що й адреса сервера, і може зв'язуватися з сервером ZKBio CVAccess.



2. В інтерфейсі **System Settings** (Налаштування системи) натисніть **[Cloud Service Settings]** (Налаштування хмарної служби), щоб перейти до інтерфейсу **Cloud Service Settings** (Налаштування хмарної служби). Щоб налаштувати адресу сервера та порт сервера.

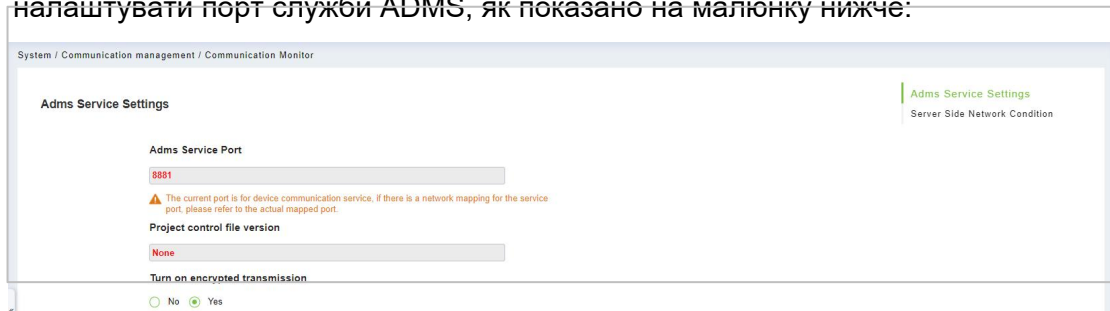
Адреса сервера: Встановіть IP-адресу сервера ZKBio CVAccess.

Порт сервера: Встановіть порт сервера як у ZKBio CVAccess.



Сторона програмного забезпечення

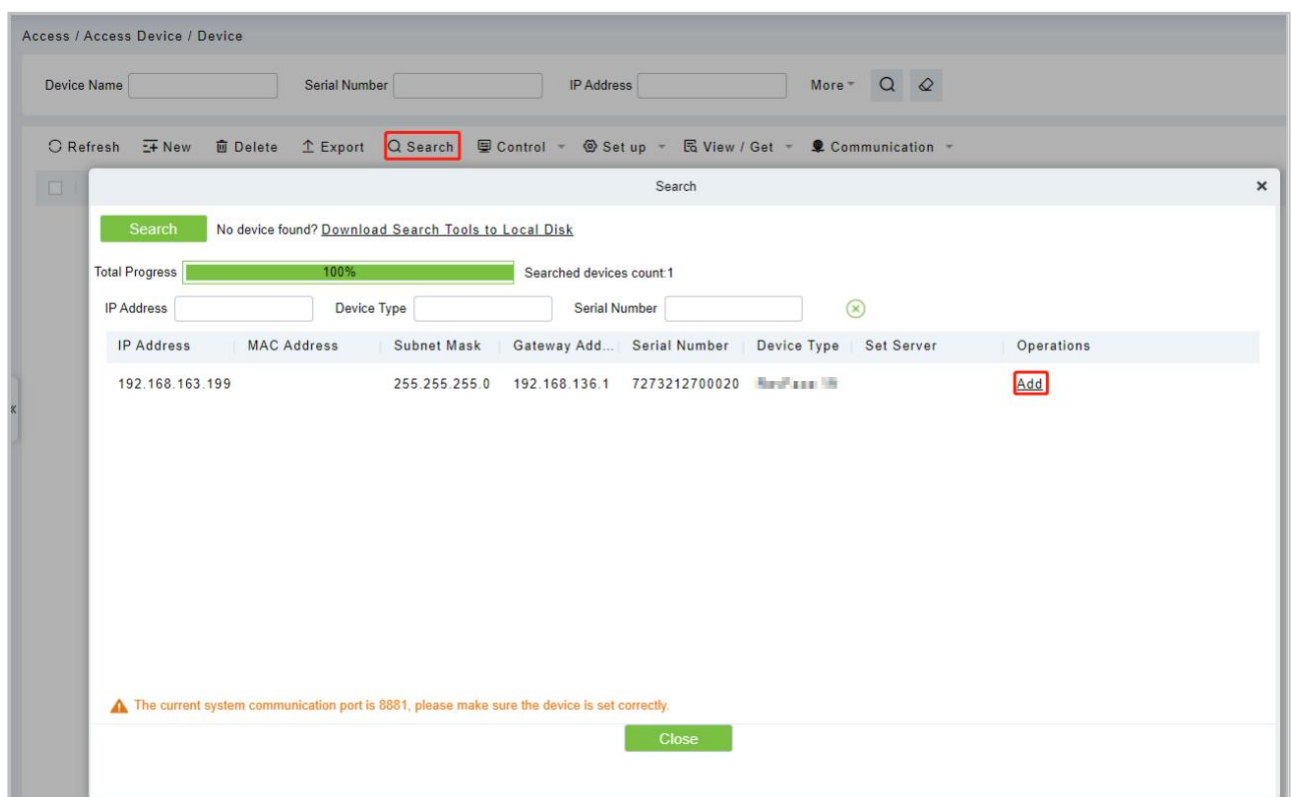
Увійдіть у програмне забезпечення ZKBio CVAcess, натисніть **[System (Система)]** > **[Communication (Комунікація)]** > **[Communication Monitor (Монітор комунікації)]**, щоб налаштувати порт служби ADMS, як показано на малюнку нижче:



10.2 Додати пристрій у програмне забезпечення

Додайте пристрій за допомогою пошуку. Процес виглядає наступним чином:

1. Натисніть **[Access (Доступ)]** > **[Device (Пристрій)]** > **[Search Device (Пошук пристрою)]**, щоб відкрити інтерфейс пошуку в програмному забезпеченні.
2. Натисніть **[Search] (Пошук)**, і з'явиться повідомлення **Searching...** (Пошук...).
3. Після пошуку буде відображено список і загальна кількість контролерів доступу.



Натисніть **[Add (Додати)]** у стовпці операції, з'явиться нове вікно. Виберіть тип піктограми, область та додайте до рівня з кожного випадаючого меню та натисніть **[OK]**, щоб додати пристрій.

10.3 Додати персонал у програмне забезпечення

1. Натисніть **[Personnel (Персонал)]** > **[Person (Особа)]** > **[New (Новий)]**:

The screenshot shows a 'New' personnel registration window. It contains two main sections: 'Personal Information' and 'Access Control'. The 'Personal Information' section includes fields for Personnel ID (2842), First Name, Last Name, Gender, Certificate Type, Birthday, Hire Date, Device Verification Password, Biometrics Type, Department Name, Mobile Phone, Certificate Number, Email, Position Name, and Card Number. There are also buttons for 'Browse' and 'Capture' next to a placeholder image. The 'Access Control' section has tabs for 'Access Control', 'Time Attendance', and 'Personnel Detail'. Under 'Access Control', there is a 'Levels Settings' section with a checked 'General' option and buttons for 'Add', 'Select All', and 'Unselect All'. To the right, there are settings for 'Superuser' (No), 'Device Operation Role' (Ordinary User), and checkboxes for 'Extend Passage', 'Access Disabled', and 'Set Valid Time'. At the bottom, there are buttons for 'Save and New', 'OK', and 'Cancel'.

2. Заповніть усі обов'язкові поля та натисніть **[OK]**, щоб зареєструвати нового користувача.
3. Натисніть **[Access (Доступ)]** > **[Device (Пристрій)]** > **[Control (Керування)]** > **[Synchronize All Data to Devices (Синхронізувати всі дані з пристроями)]**, щоб синхронізувати всі дані з пристроєм, включаючи нових користувачів.

Політика конфіденційності

Повідомлення:

Щоб допомогти вам краще користуватися продуктами та послугами ZKTeco (далі «ми», «наш» або «нас»), постачальника інтелектуальних послуг, ми постійно збираємо вашу особисту інформацію. Оскільки ми розуміємо важливість вашої особистої інформації, ми щиро ставимося до вашої конфіденційності та сформулювали цю політику конфіденційності, щоб захистити вашу особисту інформацію. Нижче ми навели політику конфіденційності, щоб ви могли точно зрозуміти заходи щодо захисту даних та конфіденційності, пов'язані з нашими інтелектуальними продуктами та послугами.

Перед використанням наших продуктів і послуг, будь ласка, уважно прочитайте і зрозумійте всі правила і положення цієї Політики конфіденційності. Якщо ви не погоджуєтеся з відповідною угодою або будь-якими її умовами, ви повинні припинити використання наших продуктів і послуг.

I. Зібрана інформація

Для забезпечення нормальної роботи продукту та поліпшення якості обслуговування ми будемо збирати інформацію, добровільно надану вами або надану з вашого дозволу під час реєстрації та використання, або отриману в результаті використання вами послуг.

- 1. Інформація про реєстрацію користувача:** під час першої реєстрації шаблон функції (шаблон відбитка пальця/шаблон обличчя/шаблон долоні) буде збережено на пристрої відповідно до типу пристрою, який ви вибрали, щоб перевірити унікальну схожість між вами та зареєстрованим ідентифікатором користувача. Ви можете за бажанням ввести своє ім'я та код. Вищезазначена інформація необхідна для використання наших продуктів. Якщо ви не надасте таку інформацію, ви не зможете регулярно користуватися деякими функціями продукту.
- 2. Інформація про продукт:** Відповідно до моделі продукту та наданого вами дозволу під час встановлення та використання наших послуг, під час підключення продукту до програмного забезпечення буде зібрано відповідну інформацію про продукт, на якому використовуються наші послуги, включаючи модель продукту, номер версії прошивки, серійний номер продукту та інформацію про ємність продукту. **Підключаючи свій продукт до програмного забезпечення, уважно прочитайте політику конфіденційності для конкретного програмного забезпечення.**

II. Безпека та керування продуктами

- 1.** Коли ви використовуєте наші продукти вперше, перед виконанням певних операцій необхідно встановити права адміністратора. В іншому випадку при вході в головне меню вам буде часто надходити нагадування про необхідність встановлення прав адміністратора. **Якщо ви все ще не встановили права адміністратора після отримання системного запиту, ви повинні бути обізнані про можливий ризик безпеки (наприклад, дані можуть бути змінені вручну).**

2. Усі функції відображення біометричної інформації у наших продуктах за замовчуванням вимкнені. Ви можете вибрати «Меню» > «Налаштування системи», щоб встановити, чи відображати біометричну інформацію. Якщо ви увімкнете ці функції, ми вважатимемо, що ви усвідомлюєте ризики для безпеки особистої інформації, зазначені в політиці конфіденційності.
3. За замовчуванням відображається лише ваш ідентифікатор користувача. Ви можете налаштувати відображення іншої інформації для перевірки користувача (такої як ім'я, відділ, фотографія тощо) за допомогою прав адміністратора. Якщо ви вирішите відображати таку інформацію, ми вважатимемо, що ви усвідомлюєте потенційні ризики для безпеки (наприклад, ваша фотографія буде відображатися на інтерфейсі пристрою).
4. Функція камери в наших продуктах за замовчуванням вимкнена. Якщо ви хочете увімкнути цю функцію, щоб робити фотографії себе для реєстрації відвідуваності або фотографувати незнайомих для контролю доступу, продукт увімкне звуковий сигнал камери. Після увімкнення цієї функції ми вважаємо, що ви усвідомлюєте потенційні ризики для безпеки.
5. Всі дані, зібрані нашими продуктами, шифруються за допомогою алгоритму AES 256. Всі дані, завантажені Адміністратором до наших продуктів, автоматично шифруються за допомогою алгоритму AES 256 і зберігаються в безпечному місці. Якщо Адміністратор завантажує дані з наших продуктів, ми припускаємо, що вам потрібно обробити ці дані і ви знаєте про потенційний ризик для безпеки. У такому випадку ви несеєте відповідальність за зберігання даних. Ви повинні знати, що деякі дані не можуть бути завантажені з міркувань безпеки даних.
6. Вся особиста інформація в наших продуктах може бути переглянута, змінена або видалена. Якщо ви більше не користуєтеся нашими продуктами, будь ласка, видаліть свої особисті дані.

III. Як ми обробляємо особисту інформацію неповнолітніх осіб

Наші продукти, веб-сайт та послуги призначені переважно для дорослих. Без згоди батьків або опікунів неповнолітні не можуть створювати власні облікові записи. Якщо ви є неповнолітнім, рекомендуємо попросити батьків або опікунів уважно прочитати цю Політику та користуватися нашими послугами або інформацією, яку ми надаємо, лише за згодою батьків або опікунів.

Ми будемо використовувати або розкривати особисту інформацію неповнолітніх, зібрану за згодою їхніх батьків або опікунів, лише в тому випадку і в тій мірі, в якій таке використання або розкриття дозволено законом або ми отримали явну згоду їхніх батьків або опікунів, і таке використання або розкриття має на меті захист неповнолітніх.

Екологічно чиста експлуатація



Термін «екологічно безпечний період експлуатації» продукту означає час, протягом якого цей продукт не виділяє токсичних або небезпечних речовин при використанні відповідно до вимог, викладених у цьому посібнику.

Екологічний термін експлуатації, зазначений для цього виробу, не включає батареї та інші компоненти, які швидко зношуються і потребують періодичної заміни. Екологічний термін експлуатації батареї становить 5 років.

Небезпечні або токсичні речовини та їх кількості

Назва компонента	Небезпечна/токсична речовина/елемент					
	Свинець (Pb)	Ртуть (Hg)	Кадмій (Cd)	Шестивалентний хром (Cr6+)	Полібромовані біфеніли (PBВ)	Полібромовані дифенілові ефіри (PBDE)
Чіп-резистор	×	○	○	○	○	○
Чіп-конденсатор	×	○	○	○	○	○
Чіп-індуктор	×	○	○	○	○	○
Діод	×	○	○	○	○	○
ESD-компонент	×	○	○	○	○	○
Дзвінок	×	○	○	○	○	○
Адаптер	×	○	○	○	○	○
Гвинти	○	○	○	×	○	○

Ця таблиця складена відповідно до положень SJ/T 11364.

○ вказує, що загальна кількість токсичних речовин у всіх однорідних матеріалах не перевищує межу, визначену в GB/T 26572.

○ вказує, що загальна кількість токсичного вмісту у всіх однорідних матеріалах перевищує межу, визначену в GB/T 26572.

Примітка: 80% компонентів цього продукту виготовлені з нетоксичних та екологічно чистих матеріалів. Компоненти, що містять токсини або шкідливі елементи, включені до складу через існуючі економічні або технічні обмеження, які не дозволяють замінити їх нетоксичними матеріалами або елементами.