

# КЕРІВНИЦТВО

## КОРИСТУВАЧА

Термінал контролю доступу та обліку

робочого часу з сенсорним екраном

2.4 дюйма

---

Версія: 1.1

Дата: Січ., 2019



## Огляд Керівництва

- Дане Керівництво знайомить з роботою призначених для користувача інтерфейсів і функцій меню терміналу обліку робочого часу та контролю доступу з сенсорним екраном 2.4 дюйма. Зображення в цьому посібнику можуть не відповідати зображенню вашого пристроя; зображення поточного пристроя має переважну силу.
- Не всі пристрої мають функції зі ★, фактичне пристрій має переважну силу.

## **ЗМІСТ**

1.	Інструкція по застосуванню .....	1
1.1	Спосіб притиску відбитка пальця .....	1
1.2	Режими верифікації .....	2
1.2.1	Верифікація по відбитку пальця 1: N .....	2
1.2.2	Верифікація по відбитку пальця 1: 1 .....	3
1.2.3	Верифікація по паролю .....	4
1.2.4	Верифікація по карті • .....	5
1.3	Початковий інтерфейс .....	6
2.	Головне меню.....	7
3.	Налаштування Дати / Часу.....	9
3.1	DST (Літній час) .....	9
4.	Керування користувачами.....	12
4.1	Додавання користувача .....	12
4.2	Налаштування контролю доступу .....	13
4.3	Пошук користувача .....	15
4.4	Редагування користувача .....	15
4.5	Видалення користувача .....	16
4.6	Стіль відображення користувача .....	17
5.	Роль користувача .....	18
5.1	Активація ролі користувача .....	18
5.2	Розподіл прав .....	19
6.	Налаштування зв'язку .....	20
6.1	Налаштування Ethernet .....	20
6.2	Налаштування послідовної зв'язку .....	20
6.3	Підключення ПК .....	23
6.4	Налаштування ADMS ★ .....	24
6.5	Установка Wiegand .....	25
6.5.1	Вхід Wiegand .....	25

6.5.2 Вихід Wiegand .....	28
6.5.3 Автоматичне визначення формату карт .....	29
7. Контроль доступу.....	32
7.1 Налаштування параметрів контролю доступу .....	33
7.2 Встановлення графіків .....	36
7.3 Налаштування свяtkovих днів .....	37
7.4 Налаштування груп доступу .....	38
7.4.1 Встановити свяtkовий день для групи доступу .....	39
7.5 Налаштування комбінованої верифікації .....	40
7.6 Налаштування заборони подвійного проходу .....	42
7.7 Налаштування параметрів примусу .....	44
7.7.1 Налаштування клавіші примусу .....	46
8. Системні налаштування .....	47
8.1 Параметри обліку робочого часу .....	47
8.2 Параметри відбитка пальця .....	49
8.3 Скидання до заводських налаштувань .....	50
8.4 Оновлення USB .....	53
9. Персоналізація налаштувань .....	54
9.1 Налаштування призначеного для користувача інтерфейсу .....	54
9.2 Налаштування голосу .....	55
9.3 Налаштування дзвінків .....	55
9.4 Налаштування станів сканування .....	56
9.5 Налаштування клавіш швидкого виклику .....	58
10. Управління даними .....	61
10.1 Управління даних .....	61
10.2 Резервне копіювання даних .....	62
10.3 Відновлення даних .....	62
11. Диспетчер USB .....	64
11.1 вивантажити на USB .....	64
11.2 Завантажити з USB .....	65

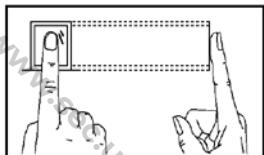
11.3 Налаштування параметрів завантаження .....	66
12. Пошук подій обліку робочого часу .....	67
12.1 Пошук записи обліку робочого часу .....	67
12.2 Пошук фотографій обліку робочого часу ★ .....	67
12.3 Пошук фотографії чорного списку ATT ★ .....	68
13. Налаштування друку ★ .....	69
13.1 Налаштування поля даних друку .....	69
13.2 Налаштування параметрів друку .....	69
14. Автоматичне тестування .....	71
15. Системна інформація .....	73
16. Пошук та усунення несправностей .....	75
17. Додатки .....	76
17.1 Функція фотографії-ідентифікатора ★ .....	76
17.2 Введення в Wiegand .....	77
17.3 Правило завантаження зображення .....	78
17.4 Функції друку • .....	79
17.5 Заява про права людини і конфіденційності .....	81
17.6 Опис екологічного використання .....	83

# 1. Інструкція по застосуванню

## 1.1 Спосіб притиску відбитка пальця

рекомендується використовувати **вказівний, середній і безіменний пальці**. Уникайте використання великого і маленького пальців.

### 1. Правильний спосіб притиску відбитка пальця:

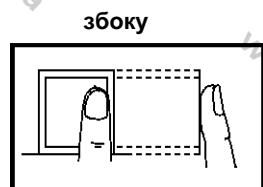


Притисніть палець горизонтально до датчика відбитків пальців;  
центр відбитка пальця повинен бути поєднаний з центром датчика.

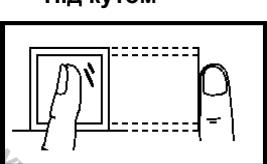
### 2. Неправильні способи притиску відбитка пальця:



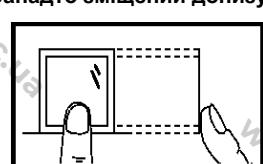
вертикальний



збоку



Під кутом



Задато зміщений донизу



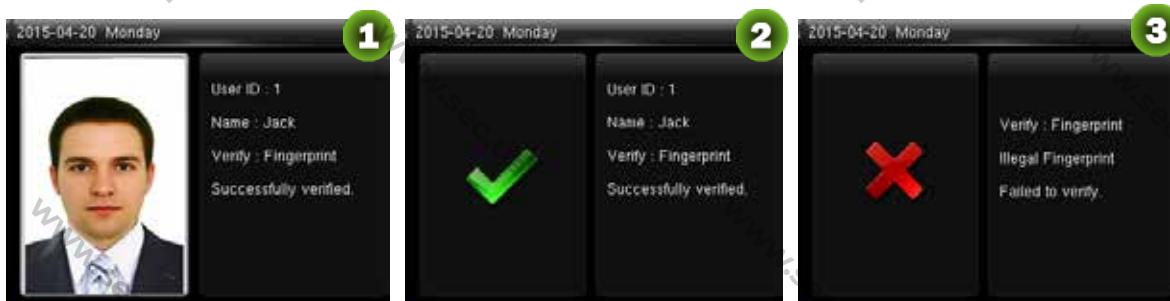
Будь ласка, використовуйте правильний спосіб притиску відбитків пальців для реєстрації та верифікації. Наша компанія не несе відповідальності за зниження ефективності верифікації, викликане неправильною роботою користувача. Права на остаточне тлумачення і зміна захищені.

## 1.2 Режими верифікації

### 1.2.1 Верифікація по відбитку пальця 1: N

Відповідно до цього способом верифікації за відбитками пальців відбиток пальців, зібрани датчиком, верифіцируються з усіма відбитками пальців, що зберігаються у пристрої.

Будь ласка, використовуйте правильний спосіб притиску відбитка пальця до датчика відбитків пальців (для отримання детальних інструкцій див. [1.1 Спосіб притиску відбитка пальця](#) ).



верифікація пройшла  
успішно

верифікація пройшла  
успішно

Верифікація не вдалася

#### • Примітки :

1. Коли пристрій видає «будь ласка, притисніть ваш палець ще раз», знову притисніть палець до датчика відбитків пальців. Якщо, після 2 спроб не вдається виконати верифікацію, система повертається до початкового інтерфейсу.

2. В пристроях, які мають функцію Фотографії-ідентифікатора

Рис. 1 буде відображатися на екрані після успішної верифікації, в іншому випадку буде відображатися Рис. 2.

- тільки деякі пристрою оснащені функцією
- Фотографії-ідентифікатора.

## 1.2.2 Верифікація по відбитку пальця 1: 1

При такому способі верифікації відбитка пальця відбиток пальця, отриманий датчиком, верифіцирується по відбитку пальця, відповідному введеному коду користувача. Будь ласка, використовуйте цей спосіб, коли виникають труднощі при верифікації відбитків пальців 1: N.



Введіть ідентифікатор користувача і натисніть [ M / OK].

Натисніть кнопку ▼, щоб вибрати « **відбиток пальця** » та натисніть [ M / OK].  
Потім притисніть палець до датчика відбитків пальця.

верифікація пройшла успішно



верифікація пройшла успішно



Верифікація не вдалася

### • Примітки:

1. Введіть Ідентифікатор користувача в початковий інтерфейс і натисніть кнопку [ M / OK]. Якщо відображається «Невірний ідентифікатор користувача!», Це означає, що ідентифікатор користувача не існує.
2. Коли на пристрій з'явиться повідомлення «Будь ласка, притисніть ваш палець ще раз»,

знову притисніть палець до датчика відбитків пальців. Якщо після 2 спроб не вдається виконати верифікацію, система повертається до початкового інтерфейсу.

3. У пристроях, що мають функцію Фотографії-ідентифікатора, Рис. 3 буде відображатися на екрані після успішної верифікації, в іншому випадку буде відображатися Рис. 4.

- тільки деякі пристрою оснащені функцією

#### Фотографії-ідентифікатора.

#### 1.2.3 Верифікація по паролю

При такому способі верифікації введений пароль верифіцирується паролем введеного ідентифікатора користувача.



Введіть ідентифікатор користувача і натисніть [ M / OK ].



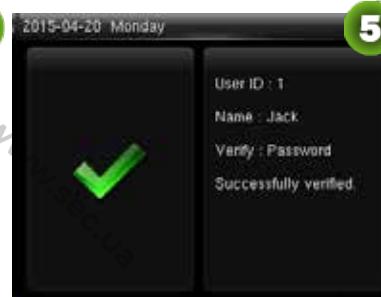
Виберіть «Пароль» і натисніть [ M / OK ].



Введіть пароль



верифікація пройшла успішно



верифікація пройшла успішно



верифікація НЕ вдалася

#### • Примітки:

1. Якщо відображається «Неправильний пароль», введіть пароль ще раз. якщо

верифікація після двох спроб все ще не вдається, система повертається до початкового інтерфейсу.

2. У пристроях, що мають функцію Фотографії-ідентифікатора, Рис. 4 буде відображатися на екрані після успішної верифікації, в іншому випадку буде відображатися Рис. 5.

- тільки деякі пристрою оснащені функцією

**Фотографії-ідентифікатора.**

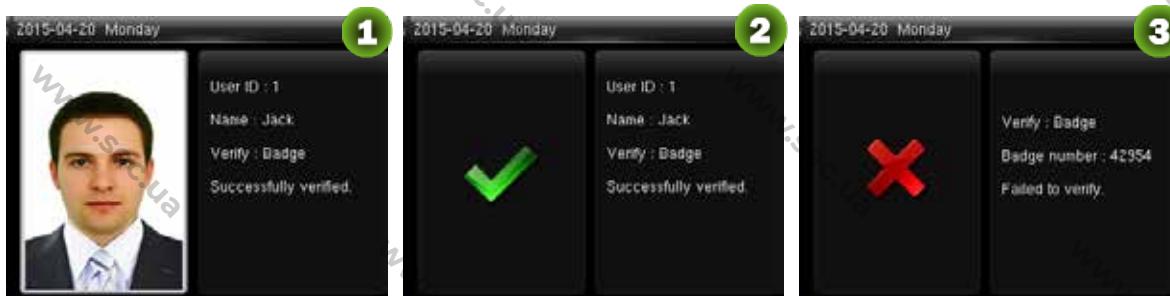
#### 1.2.4 Верифікація по карті •

- **Примітки:** Функція карти є опціональною, тільки пристрої з вбудованим модулем карти оснащені функцією верифікації по карті. Будь ласка, контактуйте з нашою технічною підтримкою в міру необхідності.

1. Проскануйте карту поруч зі зчитувачем карти (карта спочатку повинна бути зареєстрована).

2. Верифікація пройшла успішно

3. Верифікація не вдалася



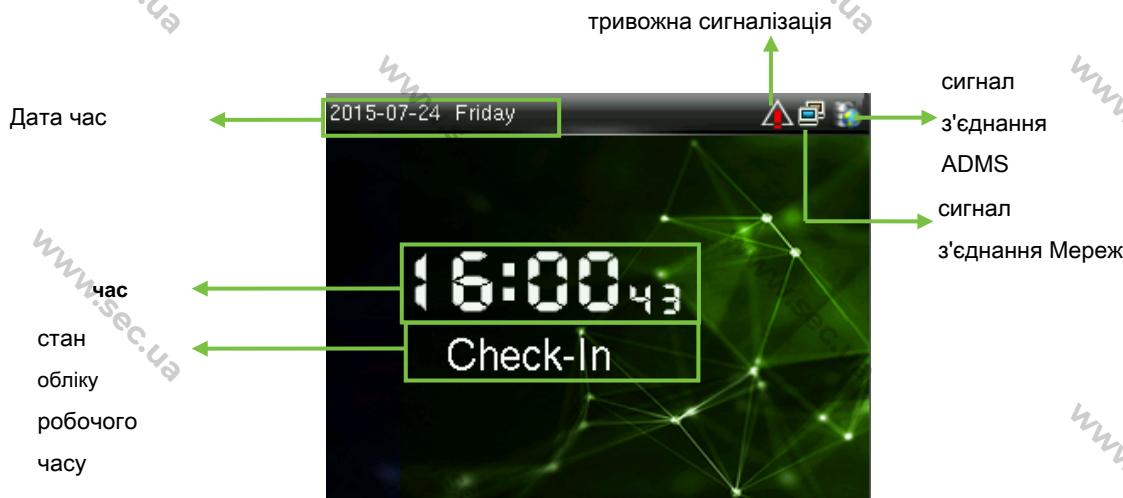
- **Примітки:** в пристроях, які мають функцію Фотографії-ідентифікатора, Рис. 1 буде відображатися на екрані після успішної верифікації, в іншому випадку буде відображатися Рис. 2.

- тільки деякі пристрою оснащені функцією

**Фотографії-ідентифікатора.**

### 1.3 Початковий інтерфейс

Коли пристрій включено початковий інтерфейс виглядає так, як показано нижче:



## 2.Основні меню

Коли пристрій перебуває в режимі очікування, натисніть [ М / OK], щоб відкрити Головне меню.



**Керування користувачами:** основна інформація про зареєстрованих користувачів, включаючи ідентифікатор користувача, ім'я, роль користувача, відбиток пальця, карта ★ (карти ID і MiFare є опціональними), пароль, призначена для користувача фотографія ★ і роль контролю доступу.

**Роль користувача:** установка ролі користувача для доступу в меню і зміни налаштувань.

**зв'язок:** установка відповідних параметрів зв'язку між пристроєм і ПК, включаючи такі параметри Ethernet, як IP-адреса і т.д., послідовний зв'язок, підключення ПК, бездротова мережа, ADMS ★ і налаштування Wiegand.

**система:** установка параметрів системи і оновлення прошивки, включаючи встановлення дати й часу, параметри обліку робочого дня і відбитку пальців, а також відновлення заводських налаштувань.

**персоналізація:** включає в себе відображення інтерфейсу, голос, дзвінок, режим клавіші стану сканування і налаштування сполучень клавіш швидкого виклику.

**Управління даними:** видалення даних обліку робочого часу, видалення всіх даних, видалення ролі адміністратора, видалення екранних заставок і т. д.

**Контроль доступу:** включає установку параметрів управління замком.

**Диспетчер USB:** для передачі таких даних, як призначені для користувача дані і журнали подій обліку робочого часу з USB-диска на допоміжне програмне забезпечення або інші пристрої.

**Пошук подій обліку робочого часу:** пошук записів, збережених на пристрії після успішної верифікації.

**Друк ★:** установка інформації і функцій друку (якщо принтер підключений до пристрою).

**Автоматичне тестування:** автоматичне тестування різних функцій модулів, включаючи РК-дисплей, голос, клавіатуру, датчик відбитків пальців, камеру ★ і тестування годин реального часу.

**Інформація про систему:** для перевірки ємності пристрою, інформації про пристрій і прошивці.

### 3.Настройкі Дати / Часу



У початковому інтерфейсі натисніть [ М / OK]> Система> Дата і час, щоб увійти в інтерфейс налаштування дати / часу. Включає в себе встановлення дати, часу, 24-годинних годин, формат дати і літнього часу.

При відновленні до заводських налаштувань формат дати може бути відновлений (РРРР-ММ-ДД).

- **Примітка:**

При відновленні заводських налаштувань дата / час пристрою не будуть відновлені (якщо дата / час встановлені на 18:30 1 січня 2020 року, після скидання налаштувань дата / час залишаться встановленими на 18:30 січня 1, 2020).

#### 3.1 DST (Літній час)

DST, також зване **Літнім часом**, являє собою систему, яка регулює місцевий час для економії енергії. Час, прийняте у встановлені дати, називається «DST». Зазвичай час буде на одну годину вперед влітку. Це дозволяє користувачам спати або вставати раніше, а також зменшувати освітлення пристрій для економії енергії. Восени відновить стандартний час. Правила різні в різних країнах. В даний час майже 110 країн беруть DST.

Щоб задовільнити запит на DST, може бути налаштована спеціальна опція. Переведіть час на годину вперед в XX (годину) XX (день) XX (місяць), або переведіть час на годину назад в XX (годину) XX (день) XX (місяць).



натисніть [ М / OK]> Система> Дата і час> Літній час, потім натисніть [ М / OK], щоб включити літній час.

**Режим літнього часу:** режим літнього часу з вибором на основі режиму дати / часу і режиму тижнь / день.

**Налаштування переходу на літній час:** встановіть дату / час або тиждень / день для літнього часу у відповідності з вибором літнього часу.

#### Як встановити літній час?

Наприклад, налаштуйте годинник вперед на одну годину о 08:00 годині 1 квітня і назад на одну годину о 08:00 годин 1 жовтня (система повертається до вихідного часу).

- **На основі режиму дати / часу:**



- **На основі режиму тижні / дати:**



- **Примітки:**

1. Якщо місяць, коли починається літній час виявляється пізніше місяця, коли закінчується літній час, тоді літній час охоплює два різних року. Наприклад, час початку літнього часу - 2014-9-1 4:00, а час закінчення літнього часу - 2015-4-1 4:00.
2. Припустимо, що режим тижні / дня обраний в [ **Режим літнього часу**], і літній час починається з неділі шостий тижні вересня 2013 року. Згідно з календарем, вересень 2014 року не має шести тижнів, але має п'ять тижнів. В цьому випадку, в 2014 році, літній час починається в відповідний момент останньої неділі вересня.
3. Припустимо, що літній час починається з понеділка першої тижні вересня 2014 року. Згідно з календарем перша тиждень вересня 2015 року не має понеділка. В цьому випадку літній час починається з первого понеділка вересня 2015 року.

## 4.Управліні користувачами

### 4.1 Додавання користувача

Включаючи додавання супер-адміністратора і звичайного користувача.



У початковому інтерфейсі натисніть [ М / OK]> Управління користувачами>

**Новий користувач** щоб увійти в інтерфейс налаштування **нового користувача**. Налаштування включають в себе ввести код користувача, вибір ролі користувача, реєстрацію відбитка пальця і

номера карти ★ ( карта ID і Mifare є опціональною), установку пароля,

зробити фотографію користувача ★ і настройку ролі контролю доступу.

**Додати супер-адміністратора:** виберіть «Супер-адміністратор» в [ Роль користувача], якому дозволено керувати всіма функціями в меню.

Як показано нижче, користувач з ідентифікатором користувача 1 є супер-адміністратором.



**Додати звичайного користувача:** виберіть «Звичайний користувач» в [ Роль користувача]. Коли встановлено супер-адміністратор, звичайні користувачі можуть використовувати тільки відбиток пальця, пароль або карту для верифікації;

коли супер-адміністратор ще не встановлено, звичайні користувачі можуть керувати всіма функціями в меню.

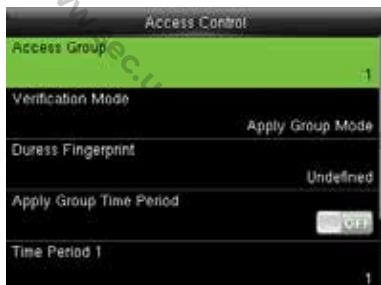
**пароль:** пароль становить від 1 до 8 цифр.

- **Примітки:**

1. Пристрій автоматично розподіляє ідентифікатор користувача по порядку, але користувач також може встановити його вручну.
2. Пристрій підтримує ідентифікатор користувача в діапазоні від 1 до 9 цифр.

## 4.2 Налаштування контролю доступу

Параметр контролю доступу полягає в тому, щоб налаштовувати доступ до відкритих дверей для всіх, включаючи настройку групи доступу, режим верифікації, використання зон дозволеного доступу і управління відбитками пальців примусу.



**Група доступу:** розподіл користувачів по різних групах контролю доступу для управління. Нові користувачі належать до групи 1 з настройками за замовчуванням, які можуть бути перерозподілені в інші групи.

**Режим верифікації:** користувач може вибрати групову або індивідуальну верифікацію. Якщо обрана індивідуальна верифікація, її спосіб, який використовується іншими членами групи, які не будуть порушенні.

**Тип індивідуальної верифікації:** включаючи пароль / відбиток пальця / карту, тільки відбиток пальця, тільки ідентифікатор користувача, тільки пароль, карту, відбиток пальця / пароль, відбиток пальця / карту, пароль / карту, ідентифікатор користувача & відбиток пальця, відбиток пальця &

пароль, відбиток пальця & карту, відбиток пальця & пароль & карту, пароль & карту, ідентифікатор користувача & відбиток пальця & пароль, відбиток пальця & карту & ідентифікатор користувача.



- **Примітки:** Індивідуальна верифікація має переважну силу над груповий верифікацією.

**Відбиток пальця примусу:** користувач може вибрати один або кілька зареєстрованих відбитків пальців в якості відбитка примусу. Після того, як цей відбиток буде верифіковано, активується сигнал примусу.



**приклад:** серед зареєстрованих відбитків пальців (6, 7, 8) виберіть восьмий відбиток як відбитка примусу.

**Застосуйте період санкціонованого доступу групи:**

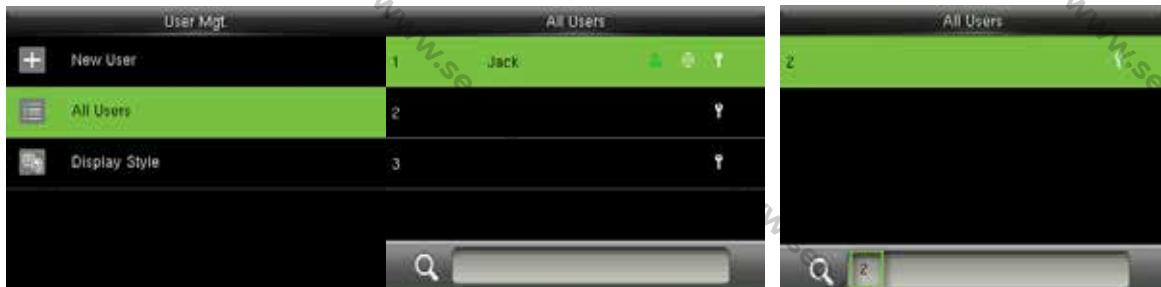
1. Якщо увімкнути, користувач використовує період за замовчуванням для своєї групи.
2. Коли ця функція відключена, користувачеві необхідно встановити особистий період санкціонованого доступу (без використання періоду санкціонованого доступу групи), який не вплине на період санкціонованого доступу інших членів групи.



- **Примітка:** кожен користувач може встановити максимум 3 періоди санкціонованого доступу.

### 4.3 Пошук користувача

Введіть ім'я користувача в списку користувачів для пошуку користувачів.



У початковому інтерфейсі натисніть [ M / OK] > Управління користувачем > Всі користувачі, щоб увійти в інтерфейс Всі користувачі. Введіть

«Ідентифікатор користувача» в , З'явиться відповідний користувач на малюнку вище показаний пошук користувача з ідентифікатором користувача «2».

### 4.4 Редагування користувача

Після вибору користувача, обраного за допомогою 4.3 Пошук користувача , Натисніть [ M / OK] і виберіть [ Редагувати], щоб увійти в інтерфейс редагування користувача.

або в початковому інтерфейсі натисніть [ M / OK] > управління користувачем > Всі користувачі > Пошук користувача > Натисніть

[M / OK]> Редагувати, щоб увійти в інтерфейс редагування користувача.

Спосіб редагування користувача такий же, як і при додаванні користувача, але ідентифікатор користувача редагувати не можна.



#### 4.5 Видалення користувача

Після вибору користувача, обраного за допомогою [4.3 Пошук користувача](#), Натисніть [ M / OK] і виберіть [ Видалити], щоб увійти в інтерфейс видалення користувача.

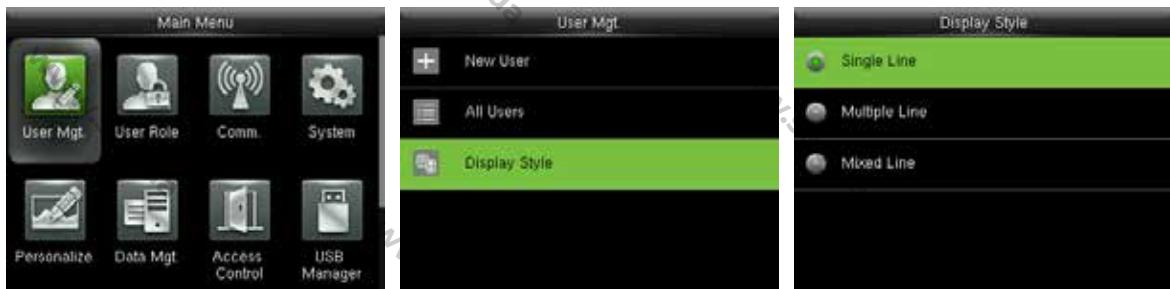
або в початковому інтерфейсі натисніть [M / OK] > управління користувачем > Всі користувачі > Пошук користувача > Натисніть [M / OK] > Видалити, щоб увійти в інтерфейс видалення користувача.



- **Примітка:**

1. Тільки коли користувач має зареєстрований відбиток пальця, пароль, карту ★ і фотографію користувача ★ буде відображатися відповідний елемент, що підлягає видаленню.
2. Тільки деякі пристрої оснащені функцією Ідентифікатора фотографій.
3. Функція карти є опціональною.

## 4.6 Стиль відображення користувача



У початковому інтерфейсі натисніть [ М / OK]> Управління користувачем>

**Стиль відображення**, щоб увійти в інтерфейс налаштування **стилю відображення**.

Деякі Стилі відображення показані нижче:

All Users	
1	Jack
2	
3	

стиль Однорядковий

All Users	
1	Jack
2	
3	

стиль Багаторядковий

All Users	
1	Jack
2	
3	

Стиль Змішаний

## 5.Роль користувача

Установка прав користувача на управління меню (може бути встановлено максимум 3 ролі). Коли роль користувача активована в [ управління користувача]> [Новий користувач]> [Роль користувача] Ви можете призначити відповідну роль кожному користувачеві.

**роль:** Суперкористувач повинен надати різні права новим користувачам. Щоб уникнути установки прав кожному користувачеві по одному ви можете встановити ролі користувачів для категоризації різних рівнів доступу в управлінні користувачами.

### 5.1 Активація ролі користувача



У початковому інтерфейсі натисніть [ M / OK]> Роль користувача>

прописується                    роль                    користувачу                    1            (2/3)            >                    активувати  
прописується                    роль.                    натисніть                    [M / OK],                    щоб                    активувати  
прописану роль.

Після активації прописуються ролей ви можете перевірити активуються ролі

користувачів                    в                    [Управління                    користувачем]                    >                    [Новий  
користувач]> [Роль користувача].

- **Примітки:** для активації ролі користувача потрібно як мінімум один зареєстрований адміністратор.

## 5.2 Розподіл прав



У початковому інтерфейсі натисніть [ M / OK]> Роль користувача>

Прописується роль користувача 1 (2/3)> Прописати роль користувача, щоб в інтерфейс розподілу прав Прописувати ролі користувача 1 (2/3). натисніть [ M / OK], щоб вибрати або скасувати операційне право до кожного меню для прописувати ролі

користувача 1 (2/3).

## 6. Настройкі зв'язку

### 6.1 Налаштування Ethernet



У початковому інтерфейсі натисніть [**M / OK**]> **Зв'язок**> **Ethernet**, щоб увійти в інтерфейс налаштування **Ethernet**.

Нижче наведені параметри, які є значеннями за замовчуванням, будь ласка налаштуйте їх у відповідність з актуальною ситуацією мережі.

**IP-адреса:** 192.168.1.201

**Маска підмережі:** 255.255.255.0

**Шлюз:** 0.0.0.0

**DNS:** 0.0.0.0

**Порт зв'язку TCP:** 4370

**DHCP:** протокол динамічної конфігурації хоста, який призначений для динамічного розподілу IP-адрес для клієнтів через сервер.

**Якщо DHCP активований IP не може бути встановлений вручну.**

**Відображати в рядку стану:** встановити відображати чи значок мережі в рядку стану.

### 6.2 Налаштування послідовної зв'язку

- **Включення / вимикання функції RS485**



натисніть [ M / OK], щоб увійти в головне меню і вибрати **Зв'язок**.



Натисніть кнопку ▼, щоб обрати **послідовну зв'язок** та натисніть [ M / OK], щоб увійти.



Виберіть RS232 / 485 і натисніть [ M / OK], щоб увійти.



Натисніть кнопку ▼, щоб вибрати **RS485** і натисніть вибрати RS485 натисніть [ M / OK] для входу.



Натисніть кнопку ▼, щоб функції ПК або головного відключення блоку, або вибрати RS485.

- **Примітки:** якщо RS485 використовується в якості функцію « **головного блоку** », її можна підключити до FR1200.
- **Включення / вимикання функції RS232**



натисніть [ M / OK], щоб увійти в головне меню і вибрати **Зв'язок**.



Натисніть кнопку ▼, щоб обрати **послідовну зв'язок** та натисніть [ M / OK], щоб увійти.



Оберіть **RS232 / 485** і натисніть [ M / OK], щоб увійти.



Виберіть RS232 i  
натисніть [ M / OK] для входу  
виберіть RS232



Натисніть кнопку ▼, щоб  
функції ПК або  
принтера ★, або  
відключити RS232

- **Примітки:**

1. Функції зв'язку RS485 і RS232 не можуть бути використані одночасно.
2. При виборі « функція друку ★ » і перезапуску пристрою відповідну інформацію про друк може бути встановлена в підміню « друк ». Для отримання більш докладної інформації про функції друку, звертайтеся в розділ 17.5 Функція друку ★ .

- **Налаштування швидкості передачі даних**



У початковому інтерфейсі натисніть [ M / OK]> Зв'язок> Послідовна зв'язок> Швидкість передачі даних, щоб увійти в інтерфейс налаштування Швидкості передачі даних.

**Швидкість передачі:** швидкість зв'язку з ПК; Існує 5 варіантів швидкості передачі: 115200 (за замовчуванням), 57600, 38400, 19200 і 9600. Чим вище швидкість передачі, тим вище швидкість зв'язку, але при цьому вона менш надійна. Як правило, більш висока швидкість передачі може використовуватися, коли відстань зв'язку короткий; коли відстань зв'язку велика, вибір більш

низька швидкість передачі даних буде більш надійною.

### 6.3 Підключення ПК

- Установки ключів зв'язку

Для того, щоб вдосконалити безпеку даних необхідно встановити **ключ зв'язку** для зв'язку між пристроєм і ПК. Якщо в пристрії встановлений **Ключ зв'язку**, необхідно ввести правильний пароль підключення, коли пристрій підключено до програмного забезпечення ПК, щоб пристрій і програмне забезпечення робило можливим обмін даними.



У початковому інтерфейсі натисніть [ M / OK]> Зв'язок> Підключення ПК> Ключ зв'язку, щоб увійти в інтерфейс налаштування **Ключ зв'язку**. **Ключ зв'язку**: пароль за замовчуванням - 0 (без пароля). Ключ зв'язку може містити від 1 до 6 цифр і знаходиться в діапазоні від 0 до 999999.

- Налаштування ідентифікатора пристрію

Якщо використовується метод зв'язку RS485 / RS232, потрібно ввести цей ідентифікатор пристрою в програмний інтерфейс зв'язку.



У початковому інтерфейсі натисніть [ M / OK]> Зв'язок> Підключення ПК> Ідентифікатор пристрію, щоб увійти в інтерфейс налаштування

**Ідентифікатора пристрою.**

**Ідентифікатор пристрою:** ідентифікаційний номер пристрою,

який знаходиться в діапазоні від 1 до 254.

## 6.4 Налаштування ADMS ★

- Примітки:** тільки деякі пристрой оснащені функцією налаштування ADMS. Такі настройки, як IP-адреса і параметри порту, а також необхідність включення проксі-сервера і т. д., Використовуються в якості налаштувань для підключення до сервера ADMS.



У початковому інтерфейсі натисніть [**M / OK**]>**Зв'язок**>**ADMS**, щоб увійти в інтерфейс налаштування сервера **ADMS**. Коли вебсервер підключений успішно, головний інтерфейс буде відображати значок .

**Включити ім'я домену:** Коли активований, буде використовуватися

режим імені домена `http://...`, наприклад `http://www.XXX.com`. XXX по-значає доменне ім'я, коли цей режим включений; коли цей режим вимкнений, введіть формат IP-адреси в XXX.

**Адреса сервера:** IP-адреса сервера ADMS.

**Порт сервера:** порт, який використовується сервером ADMS.

**Включити проксі-сервер:** метод включення проксі. Щоб включити проксі,

будь ласка, встановіть IP-адресу і номер порту проксі-сервера. Дає змогу вказати IP проксі і адреси сервера буде однаковим.

## 6.5 Установка Wiegand



У початковому інтерфейсі натисніть [ М / OK]> Зв'язок> Установка Wiegand, щоб увійти в інтерфейс налаштування Установки Wiegand.

### 6.5.1 Вхід Wiegand

Роз'єм входу Wiegand підтримує зчитувач карт, або підключає пристрій в якості головного блоку до іншого пристрою (підлеглому блоку), утворюючи систему головний / підлеглий.



**Формат Wiegand:** користувач може вибрати один з наступних вбудованих форматів Wiegand:

Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37,

Wiegand 37a, і Wiegand

50.

**Ширина імпульсу (мкс):** ширина імпульсу, що посилається Wiegand. Значення за замовчуванням становить 100 мікросекунд, які можна регулювати в діапазоні від 20 до 100 мікросекунд.

**Імпульсний інтервал (мкс):** значення за замовчуванням становить 1000 мікросекунд, які можна регулювати в діапазоні від 200 до 20000 мікросекунд.

**Тип ідентифікатора:** вміст входу, включене у вхідній сигнал

Wiegand. можна вибрати ідентифікатор користувача або Номер картки.

**Визначення форматів Wiegand:**

формат <b>Wiegand</b>	визначення
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCCO Складається з 26 біт двійкових чисел, причому 1-й біт є бітом парній перевірки парності для 2-13-го бітів, 26-й біт є бітом непарної перевірки парності для 14-25-го бітів, а 2-25-й біти є номером карти.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCO Складається з 26 біт двійкових чисел, причому 1-й біт є бітом парній перевірки парності для 2-13-го бітів, 26-й біт є бітом непарної перевірки парності для 14-25-го бітів, 2-9-й біти є кодом зони і 10-25-й біти є номером карти. ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCO
Wiegand34	Складається з 34 біт двійкових чисел, причому 1-й біт є бітом перевірки парності для 2-17-го бітів, а 34-й біт є бітом перевірки непарності для 18-33-го бітів, а 2-25-й біти є номером карти.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCO Складається з 34 біт двійкових чисел, причому 1-й біт є бітом парній перевірки парності для 2-17-го бітів, 34-й біт є бітом непарної перевірки парності для 18-33-го бітів, 2-9-го бітів є кодом сайту, а 10-25-й біти є номером

	карти.
Wiegand36	<p>ОFFFFFFFCCCCCCCCCCCCCCCCMME</p> <p>Складається з 36 біт двійкових кодів. 1-й біт є бітом непарної перевірки парності від 2-го до 18-го бітів, а 36-й біт є бітом парній перевірки парності від 19-го до 35-го бітів. 2-17-й біт - це код пристрою, 18-33-й - номер карти, а 34-35-й - код виробника.</p>
Wiegand36a	<p>EFFFFFFFFFCCCCCCCCCCCCCO</p> <p>Складається з 36 біт двійкового коду. 1-й біт є бітом парній перевірки парності від 2-го до 18-го бітів, а 36-й біт є бітом непарної перевірки парності від 19-го до 35-го бітів. 2-19-й біт - це код пристрою, а 20-35-й - номер карти.</p>
Wiegand37	<p>ОММММSSSSSSSSSSCCCCCCCCCCCC</p> <p>CE</p> <p>Складається з 37 біт двійкового коду. 1-й біт є бітом непарної перевірки парності з 2-го по 18-й біти, а 37-й біт є бітом парній перевірки парності з 19-го по 36-й біти. 2-4-й біти - це код виробника, 5-16-й біти - код сайту, а 21-36-й біти - номер карти.</p>
Wiegand37a	<p>ЕМММFFFFFFFFSSSSCCCCCCCCCCCC</p> <p>О</p> <p>Складається з 37 біт двійкового коду. 1-й біт є бітом парній перевірки парності від 2-го до 18-го бітів, а 37-й біт є бітом непарної перевірки парності від 19-го до 35-го бітів. 2-4-й біти - це код виробника, 5-14-й біти - код пристрою, 15-20-й</p>

	біти - код сайту, а 21-36-й біти - номер карти.
Wiegand50	<p>ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCC CCCCCCCCCCCCCO</p> <p>Складається з 50 біт двійкового коду. 1-й біт - це біт парній перевірки парності з 2-го по 25-й біт, а 50-й біт - це біт непарної перевірки парності від 26-го до 49-го біта. 2-17-й біти - це код сайту, а 18-49-й біти - номер карти.</p>

- **Примітка:** С позначає номер карти, Е позначає біт парній перевірки парності, О позначає біт непарної перевірки парності, F позначає код пристрою, M позначає код виробника, P позначає біт парності, і S позначає код сайту.

### 6.5.2 Вихід Wiegand

Вихідний роз'єм Wiegand Output підтримує SRB, або підключає пристрій в якості підлеглого блоку до іншого пристрою (головний блок), утворюючи систему головний / підлеглий.



**SRB:** Оберіть [ ВКЛ.], щоб включити функцію SRB, а при виборі [ ВИКЛ.]

можна відключити цю функцію.

**Формат Wiegand:** користувач може вибрати один з наступних вбудованих форматів Wiegand:

Wiegand 26, Wiegand 26a, Wiegand 34, Wiegand 34a, Wiegand 36, Wiegand 36a, Wiegand 37, Wiegand 37a і Wiegand 50. Доступні кілька варіантів вибору, але фактичні формат Wiegand буде залежати від параметра в [ Вихідні біти Wiegand].

**наприклад:** якщо 26-бітний Wiegand26, 34-бітний Wiegand34a, 36-бітний Wiegand36, 37-бітний Wiegand37a і 50-бітний Wiegand50 обрані в

[ **Формат Wiegand**], а 36 біт вибрано в [ **Вихідні біти Wiegand**], то фактичний формат Wiegand для використання буде 36-бітний Wiegand36.

**Вихідні біти Wiegand:** кількість біт даних Wiegand. Після вибору [ **Вихідні біти Wiegand**] пристрій буде використовувати задану кількість бітів, щоб знайти відповідний формат Wiegand в [ **формат Wiegand**].

**Невдалий ідентифікатор:** визначається як вихідне значення налаштування від 0 до 65535.

Формат виведення [ **Формат Wiegand**].

**Код сайту:** він аналогічний ідентифікатором пристрою, його можна встановити вручну і поновити на Значення за замовчуванням. Становить від 0 до 256.

**Ширина імпульсу (мкс):** ширина імпульсу, що посилається Wiegand. Значення за замовчуванням становить 100 мікросекунд, яке можна регулювати в діапазоні від 20 до 100 мікросекунд.

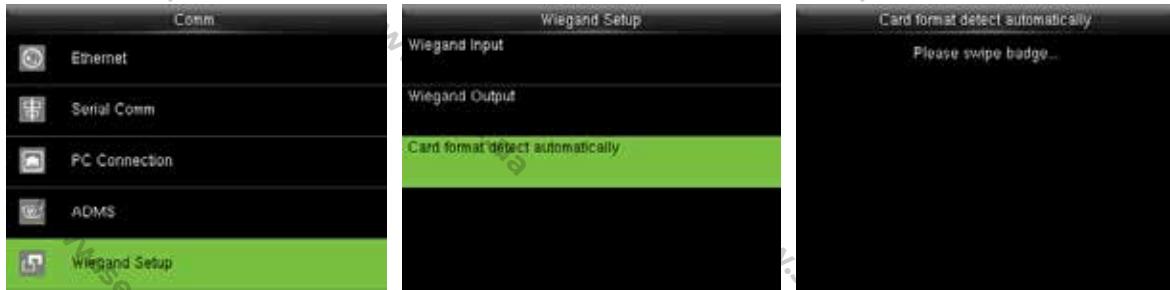
**Імпульсний інтервал (мкс):** значення за замовчуванням становить 1000 мікросекунд, які можна регулювати в діапазоні від 200 до 20000 мікросекунд.

**Тип ідентифікатора:** вміст вхідних даних включено у вхідній сигнал Wiegand. Можна вибрати ідентифікатор користувача або номер карти.

### 6.5.3 Автоматичне визначення формату карт

[**Автоматичне визначення формату карт**] допомагає користувачеві швидко визначити тип карти і її відповідний формат. У пристрої встановлено різні формати карт. Після зчитування карти система визначить її у вигляді різних номерів карт відповідно до кожного формату;

користувачеві потрібно лише вибрати елемент, еквівалентний фактичному номером картки, і встановити формат як формат Wiegand для пристрою. Ця функція також може бути застосована до функції читання карт і допоміжному зчитувача Wiegand.



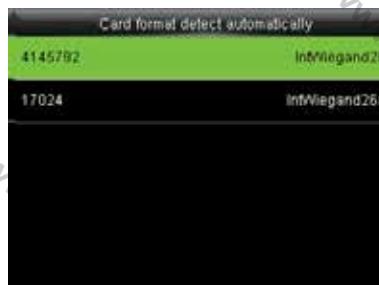
У початковому інтерфейсі натисніть [ M / OK]> Зв'язок> Установка Wiegand>

**Автоматичне визначення формату карт**, щоб увійти в інтерфейс

**Автоматичне визначення формату карт.**

#### Порядок роботи:

1. Після входу в інтерфейс [**Автоматичне визначення формату карт**] пристрої ідентифікації, проскануйте карту ID поруч з пристроєм зчитування карт (на локальному пристрої або допоміжному пристрої зчитування карт), інтерфейс покаже автоматично виявлені формати Wiegand і проаналізовані номера карт.



1. Виберіть елемент, що відповідає номеру фактичної карти в якості

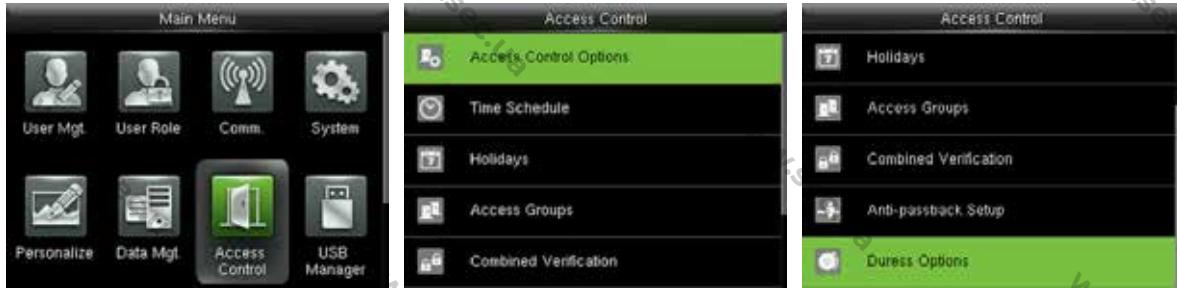
**[Формат Wiegand]** пристрою, який є форматом Wiegand для зчитування таких типів карт.



- **Примітки.** В інтерфейсі [ Автоматично визначення формату карти] пристрою з інтелектуальними картами пристрій не може визначити номер карти або формат Wiegand, тільки скануючи інтелектуальну карту. Для визначення формату Wiegand інтелектуальні карти необхідно підключити пристрій зчитування інтелектуальних карт до пристрою і просканувати інтелектуальні карти поруч з допоміжним пристроєм зчитування карт, щоб пристрій відобразило номер карти і формат Wiegand.

## 7. Контроль доступу

Параметр контролю доступу використовується для установки графіків, свяtkovих днів, груп доступу, комбінованої верифікації і т. д., Відповідні параметри для пристрою для управління замками і іншими пристроями.



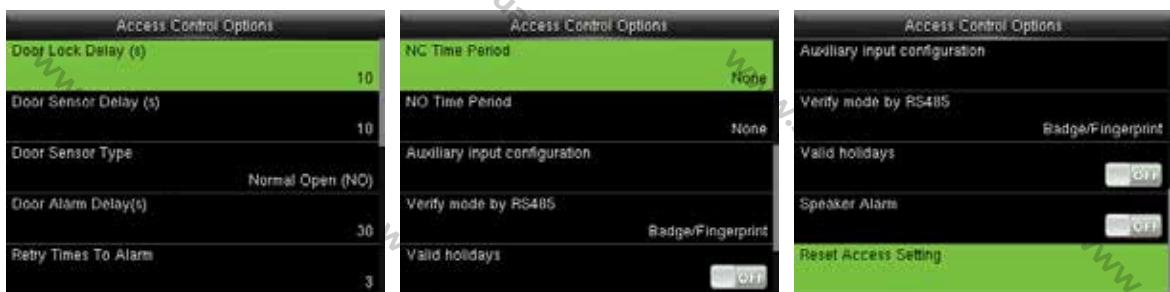
У початковому інтерфейсі натисніть [M / OK] > Контроль доступу, щоб увійти в інтерфейс налаштувань Контролю доступу.

Щоб отримати доступ зареєстрований користувач повинен відповісти таким умовам:

1. Час доступу користувача знаходиться в межах особистого часу доступу користувача або часу доступу групи.
2. Група користувачів повинна знаходитися в комбінованому доступі (коли в тому ж комбінованому доступі знаходяться інші групи, верифікація членів цих груп також необхідна для відкриття дверей).

В налаштуваннях за замовчуванням нові користувачі розподіляються в першу групу з часом доступу групи за замовчуванням і комбінованим доступом, позначену як група «1» і встановлюється в стан розблокування.

## 7.1 Налаштування параметрів контролю доступу



У початковому інтерфейсі натисніть [ М / OK]> Контроль доступу> Параметри контролю доступу, щоб увійти в інтерфейс налаштування **параметрів контролю доступу**.

**Час очікування дверного замка (сек)**: Період часу розблокування (від відкриття двері до автоматичного закриття) після того, як електронний замок отримує сигнал відкриття, відправлений з пристрою (значення знаходиться в діапазоні від 0 до 10 секунд).

**Час очікування датчика двері (сек)**: Коли двері відкриті, датчик двері буде перевірений через деякий час; якщо стан датчика двері не збігається зі станом режиму датчика двері, спрацює сигналізація. Період часу - це **Час очікування датчика двері** (значення коливається від 0 до 255 секунд).

**Тип датчика двері**: включає в себе "відсутня", «нормальне відкриття»( NO) і «нормальне закриття»( NC). **відсутня** означає, що датчик двері не використовується; **нормальне відкриття** означає, що двері відкриті, коли включено електрику; **нормальне закриття** означає, що двері закриті, коли включено електрику.

**Час очікування тривожної сигналізації двері (сек)**: коли стан датчика двері не відповідає стану типу датчика двері, сигнал тривоги спрацьовує через деякий час; цей період часу є **Часом очікування спрацювання тривожної сигналізації двері**

(Значення коливається від 1 до 999 секунд).

**Число повторних спроб до спрацьовування тривожної сигналізації**:

коли число невдалих верифікацій досягне встановленого значення (значення коливається від 1 до 9 разів), спрацьовує сигналізація. Якщо встановлене значення відсутній, сигнал тривоги не буде активований після невдалої верифікації.

**Період часу режиму Нормально закритий:** встановити період часу для режиму Нормально закритий, так щоб ніхто не міг отримати доступ протягом цього періоду.

**Період часу режиму Нормально відкритий:** встановити період часу для режиму Нормально відкритий, так щоб двері завжди була розблокована протягом цього періоду.

**конфігурація**

**Режим верифікації по RS485:** для включення функції зчитувача RS485; це спосіб верифікації, який використовується пристроєм, коли він є системою блоків головний / підлеглий.

**Діючі свяtkові дні:** щоб встановити, чи є налаштування

**Періоду часу Нормально закритий або періоду часу нормально відкритий** дійсними протягом встановленого періоду вихідного дня. Оберіть [ ВКЛ.], щоб включити встановлені періоди часу нормально закритий або нормально відкритий в свяtkові дні.

**Тривожна сигналізація динаміка:** коли [ тривожна сигналізація динаміка] включена, динамік подастъ сигнал тривоги при демонтажі пристрою.

**Скидання налаштувань доступу:** для скидання параметрів часу очікування дверного замка, часу очікування датчика двері, типу датчика двері, часу очікування тривожної сигналізації двері, часу повторних спроб до спрацьовування тривожної сигналізації, періоду часу

Нормально закритий, періоду часу Нормально відкритий, діючих свяtkових днів, тривожної сигналізації динаміка, напрямки заборони подвійного проходу, стану пристрою, функція примусу, тривожної сигналізації при порівнянні 1: 1, тривожної сигналізації при порівнянні 1: N, тривожної сигналізації по паролю і часу очікування тривожної сигналізації. Проте, вміст Вилучення даних доступу в [ Управ. даними] НЕ буде порушено.

<b>параметри доступу</b>	<b>заводські настройки по замовчуванням</b>
Час очікування дверного замка Час	10 сек
очікування датчика двері	10 сек
Режим датчика двері	відсутн.
Час тривожної сигналізації двері	30 сек
Число повторних спроб до спрацьовування тривожної сигналізації	3
Період часу режиму Нормально закритий період часу режиму	відсутня
Нормально відкритий Періоди дії режимів Нормально відкритий і	відсутня
Нормально закритий в свяtkові дні	відключено
Тривожна сигналізація динаміка	Отключеноа
Напрямок заборони подвійного проходу	заборона подвійного проходу відсутня
стан пристрою	зовнішній
кнопка довідки	відключений
Тривожна сигналізація при порівнянні 1: 1 Тривожною	відключений
сигналізації при порівнянні 1: N тривожна сигналізація	відключений
по паролю	відключений
Тривожна сигналізація часу очікування примусу 10 сек	

- **Примітки:** після встановлення **періоду часу Нормально закритий**, будь ласка добре за- блокуйте двері, в іншому випадку в **період часу Нормально закритий** може спрацювати сигналізація.

## 7.2 Встановлення графіків

**Графік** - це мінімальна одиниця часу налаштувань контролю доступу; для системи може бути встановлено не більше 50 **Графіків**. кожен **Графік** складається з 7 тимчасових періодів (тиждень), і кожен часовий період є дійсним часом протягом 24 годин.



У початковому інтерфейсі натисніть [ М / OK]> Контроль доступу> Графік, щоб увійти в інтерфейс **Графік**. номер **графіка** за замовчуванням - 1 (дійсний весь день), який можна редагувати.

**Чинний графік:** 00:00 ~ 23:59 (дійсний весь день) або коли час закінчення пізніше часу початку.

**Недіючий графік:** час закінчення завчасно початку.

### Приклад 1: настройка Графіка 02 (чинний)



3 неділі по суботу встановлюється 10:00 ~ 17:00, оскільки час закінчення пізніше часу початку. **Графік 2** є чинним.

## Приклад 2: установка Графіка 03 (недіючий)

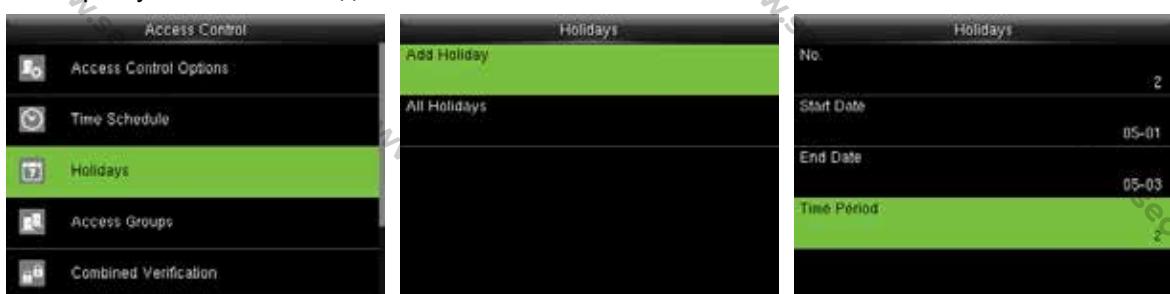


В графіку 3 щоденний час закінчення завчасно початку, тому графік 3 є нечинним.

- **Примітка:** Графік не може бути встановлений на два дні, що означає, що час закінчення повинен бути пізніше часу початку.

## 7.3 Налаштування свяtkovих dniv

Можна встановити час контролю доступу в свяtkovі dnі, який може бути застосовано до всіх користувачів в свяtkovі dnі.



У початковому інтерфейсі натисніть [ M / OK] > Контроль доступу >

Свяtkovі dnі > Додати свяtkovий день, щоб увійти в інтерфейс Додати свяtkovий день. Налаштування включають число, час початку, час закінчення і період часу дії.

Примітка: Дата початку / закінчення потрібно тільки для установки місяці (MM) і дати (DD), який може бути застосовано до всіх років. Як показано на малюнку вище: Свяtkovий день 2 починається з 1 травня кожного року, закінчується 3 травня кожного року з прийняттям Періоду часу дії 2 (з 10:00 до 17:00 з неділі по суботу).

Активувати функцію Свяtkovий день:

У початковому інтерфейсі натисніть [ M / OK]> Контроль доступу> Групи

доступу> Усі групи> Оберіть групу управління доступом>

Редагувати> Включити свяtkovі дні, натисніть [ M / OK], щоб включити (ВКЛ.) свяtkовий день.

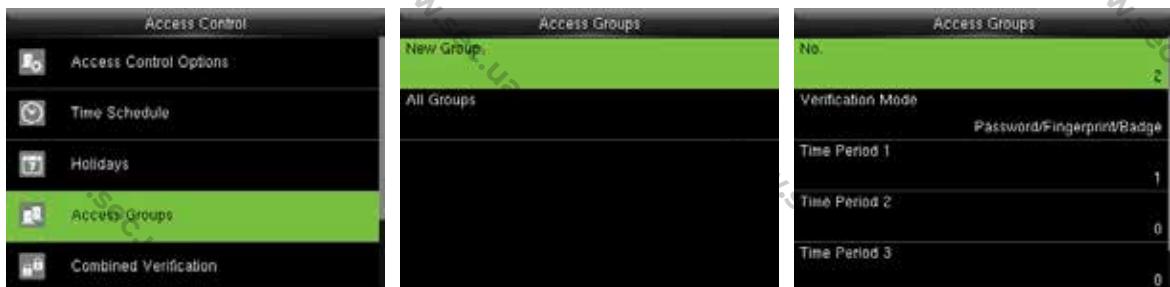
Включення / вимикання функції Свяtkовий день може бути застосовано до всіх користувачів в одній групі доступу.

#### 7.4 Налаштування груп доступу

Розподіл по групах полягає в управлінні користувачами в групах.

Період часу санкціонованого доступу групи користувачів за замовчуванням встановлений як період доступу групи, в той час як користувачі можуть встановлювати свій особистий час доступу. Кожній групі можна встановити не більше 3 періодів, за умови, що один з них діючий, група може бути успішно верифікована.

За замовчуванням новий зареєстрований користувач належить до Групи доступу 1, а також може бути приписаний до іншої групи доступу.



У початковому інтерфейсі натисніть [ M / OK]> Контроль доступу> Групи

доступу> Створити нову групу, щоб увійти в інтерфейс Створити нову групу. Нижче

наведені дані в якості прикладу:

No.	Verification Mode	Time Period 1	Time Period 2	Time Period 3
1	Fingerprint only	01 00 00		
2		01 00 00		
3		01 00 00		
4		01 00 00		
15		01 00 00		
17		01 02 03		

Як показано на наведених вище малюнках **Режим верифікації** групи доступу 17 є режимом тільки за відбитками пальців; встановлені Періоди доступу 1, 2 і 3, і функція Святкового дня включена.

#### 7.4.1 Встановити святковий день для групи доступу

**Для того, щоб включити функцію Святковий день:**

1. Встановіть **Графік** ( включаючи Графік доступу і Графік святкових днів)> встановіть **Святковий день**> пропишіть користувачів в групу доступу> встановіть для параметра [ **Включити Святкові дні**] групи доступу значення [ **ВКЛ.**].

• **Примітки:**

1. Коли функція Святковий день включена, учасники можуть отримати доступ тільки тоді, коли графіки групи доступу і святкового дня збігаються.

2. Коли функція святковий день відключена, час доступу користувачів в групі доступу немає буде порушено.

**наприклад:**

Якщо для Групи доступу 2 потрібно використовувати Графік святкового дня 2 в Міжнародний день працівника, то це означає, що користувачі можуть отримати доступ протягом 10:00 ~ 17:00 (Графік 2) з 1 по 3 травня.

**Метод роботи:**

1. Встановіть Графік 2 на 10:00 ~ 17:00 з неділі по суботу. Метод вимірювання наведено в прикладі настройки Періоду доступу 2 в розділі [7.2 налаштування графіків](#).
2. Використовуйте Графік 2 для святкових днів. Для способу установки свята, будь ласка, зверніться до [7.3 Налаштування святкових днів](#)
3. Для налаштування групи доступу, будь ласка, зверніться до [7.4 Налаштування групи доступу](#) для отримання інструкцій.
4. Увімкніть функцію **Святкового дня**. У початковому інтерфейсі натисніть

[ M / OK]> Контроль доступу> Групи доступу> Все групи> 2> натисніть [ M / OK]> Редагувати>  
Включити Свяtkovі дні, натисніть [ M / OK], щоб поставити [ ВКЛ.] для пункту [ Включити свя-  
ткові дні].



5. Користувачі в Групі доступу 2 проходять верифікацію для отримання доступу, настройка  
виконана успішно.

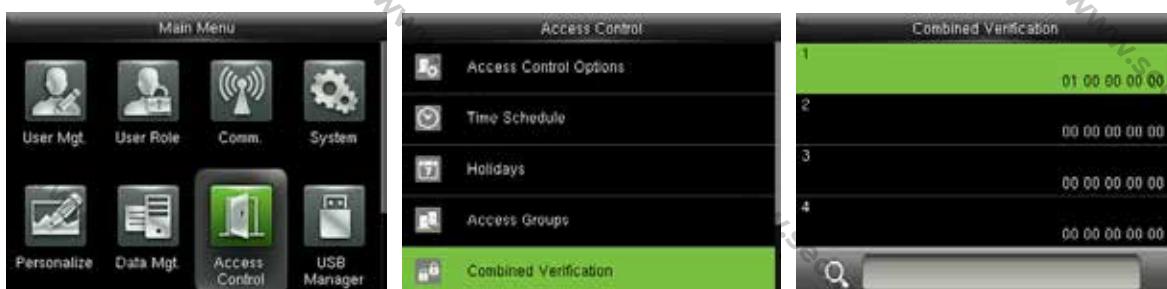
- **Примітки:** якщо свяtkовий день повинен бути чинним для всіх користувачів, виділіть всіх  
користувачів в одну групу або включите параметр [ Включити свяtkові дні] для всіх груп доступу.

## 7.5 Налаштування комбінованої верифікації

Об'єднайте двох або більше учасників, щоб забезпечити комбіновану верифікацію і підвищити  
безпеку.

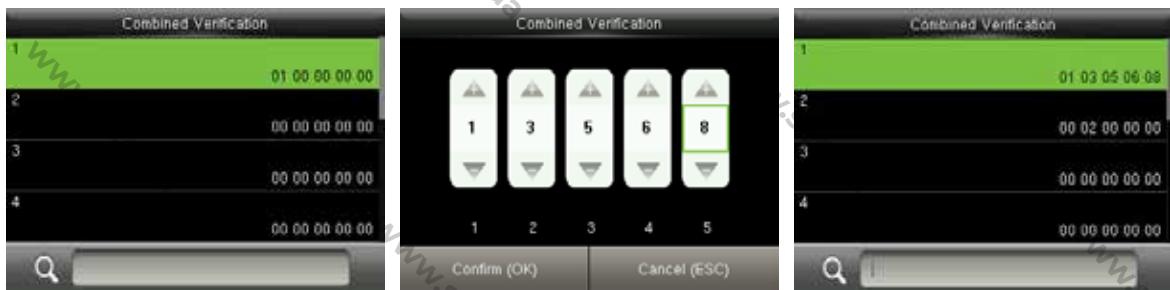
У комбінованій верифікації діапазон номера користувача:  $0 \leq N \leq 5$ ; всі користувачі можуть  
належати до однієї групи або максимум до 5 різних груп.

- **Примітка:** тільки номер групи, заданий в інтерфейсі Групи  
доступу, може бути обраний в налаштуванні Комбінованої верифікації.



В початковому інтерфейсі натисніть [ M / OK]> контроль доступу>Комбінована верифікація> 1  
щоб увійти в перший інтерфейс настройки Комбінованої  
верифікації 1.

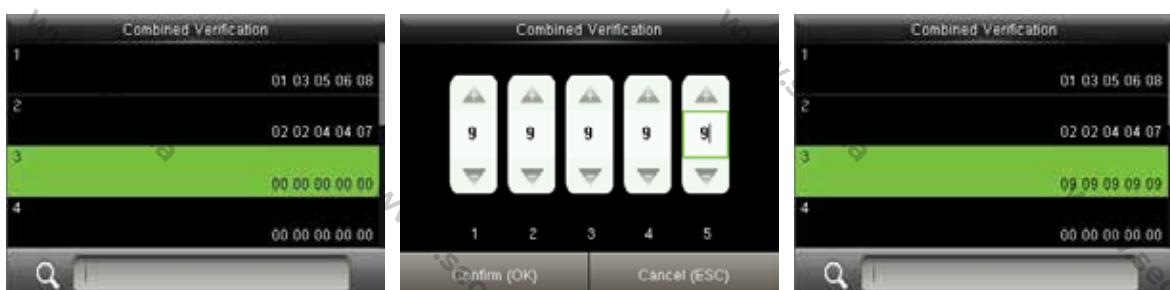
наприклад ( в інтерфейсі групи доступу встановлені наступні **Групи доступу**):



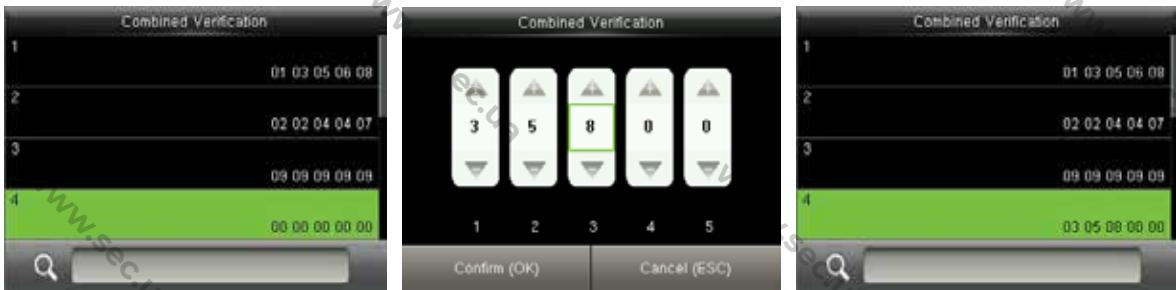
Як показано на малюнку вище, Комбінована верифікація 1 складається з п'яти учасників з п'яти різних груп - група доступу 1/3/5/6/8 відповідно.



Як показано на малюнку вище Комбінована верифікація 2 складається з п'яти учасників з трьох різних груп: двох членів з Групи доступу 2, двох з Групи 4 і одного з Групи 7.



Як показано на малюнку вище Комбінована верифікація 3 складається з п'яти учасників, і всі вони належать Групі доступу 9.

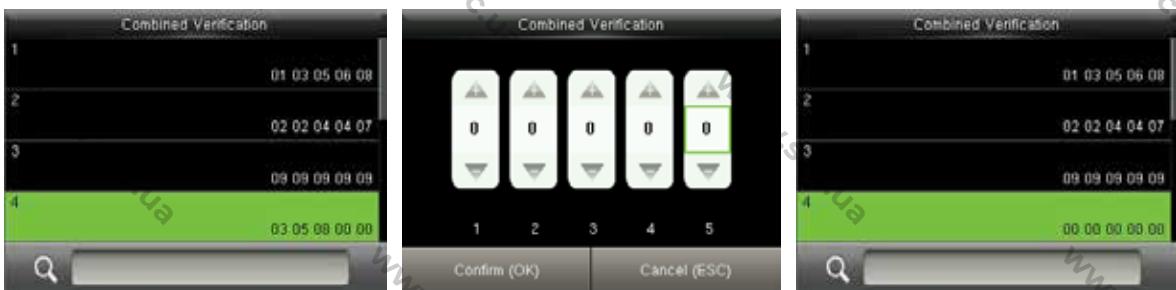


Як показано на малюнку вище Комбінована верифікація 4 складається з трьох учасників з трьох різних груп - Групи доступу 3, 5, 8 відповідно.

### **Видалення Комбінованої верифікації**

Щоб видалити комбіновану верифікацію встановіть для всіх номерів груп доступу значення 0.

Наприклад, щоб видалити комбіновану верифікацію 4, см. Рисунки нижче:



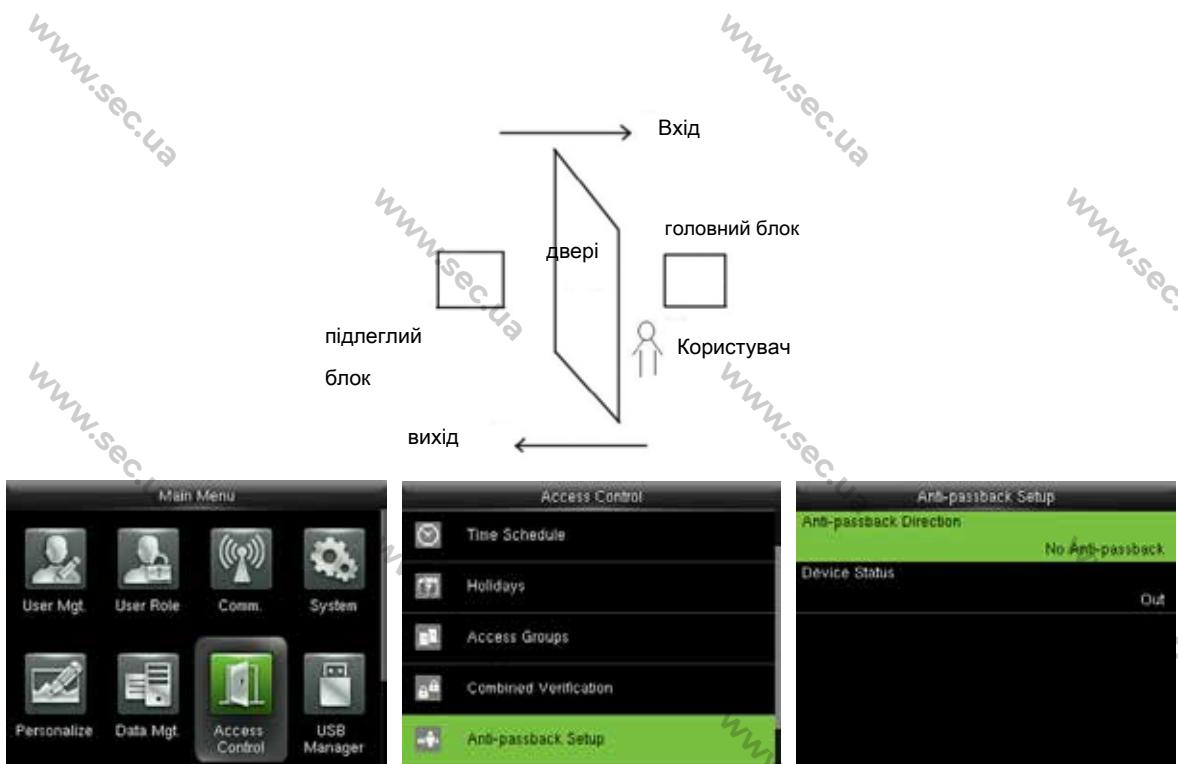
Якщо всі номера груп в Комбінованої верифікації 4 встановлені на 0, вона буде видалена.

### **7.6 Налаштування заборони подвійного проходу**

Щоб деякі люди, такі безпосередньо за користувачами, не входили в двері без верифікації, що призводить до проблем з безпекою, користувачі можуть включити функцію заборони подвійного проходу. Запис реєстрації входу повинна збігатися із записом реєстрації виходу, щоб відкрити двері.

Ця функція вимагає двох блоків для спільної роботи: одне встановлюється всередині двері (головний блок), інше - зовні двері (підлеглий блок). Два блоки обмінюються даними за допомогою сигналу

Wiegand. Формат Wiegand і тип виходу (ідентифікатор користувача / номер карти), прийняті головним і підлеглим блоками, повинні бути узгоджені.



У початковому інтерфейсі натисніть [ М / OK]> Контроль доступу> Установка заборони подвійного проходу, щоб увійти в інтерфейс Установка заборони подвійного проходу. Оберіть Напрямок заборони подвійного проходу і Стан блоку.

- **Напрямок заборони подвійного проходу Відсутність заборони подвійного проходу:** функція

Заборони подвійного проходу відключена, що означає, що проходження верифікації на головному або підпорядкованому блокі може розблоковувати двері. Стан обліку робочого часу не зарезервовано.

**Заборона подвійного проходу на вихід:** після того, як користувач зареєструвався на вихід користувач знову зможе зареєструватися на вихід, тільки якщо останній запис буде реєстрацією на вхід; в іншому випадку буде активована тривожна сигналізація. Проте, користувач може вільно зареєструватися на вхід.

**Заборона подвійного проходу на вхід:** після того, як користувач зареєструвався на вхід користувач знову зможе зареєструватися на вхід, тільки якщо останній запис буде реєстрацією на вихід; в іншому випадку буде активована тривожна сигналізація. Проте, користувач може вільно зареєструватися на вихід.

**Заборона подвійного проходу на вхід / вихід:** після того, як користувач зареєструвався на Вхід вихід користувач знову зможе зареєструватися на вхід, тільки якщо останній запис буде реєстрацією на вихід або користувач знову зможе зареєструватися на вихід, тільки якщо останній запис буде реєстрацією на вхід; в іншому випадку буде активована тривожна сигналізація.

**Припинено і збережена:** встановлено заборону подвійного проходу відключена, але стан обліку робочого часу зарезервовано.

- **стан блоку**

**Відсутня:** відключити функцію Заборони подвійного проходу.

**вихід:** всі записи на блоці є записами реєстрації на вихід.

**Вхід:** всі записи на блоці є записами реєстрації на вхід.

## 7.7 Налаштування параметрів примусу

Коли користувачі стикаються з примусом, вибирають режим тривоги з примусу, тоді пристрій, як зазвичай, відкриває двері і відправляє сигнал тривоги на пульт моніторингу.



У початковому інтерфейсі натисніть [ M / OK]> Контроль доступу> Параметри примусу,

щоб Увійти в інтерфейс налаштувань.

- **Примітки:** Наведені вище чотири типи методів спрацьовування тривожної сигналізації примусу

(функція примусу, тривожна сигналізація при збігу 1: 1, тривожна сигналізація при збігу 1: N і

тривожна сигналізація по паролю) встановлюються в положення [ ВІКЛ.] в настройках за

умовчанням.

**Функція примусу:** в стані [ ВКЛ.] натисніть «Кнопку примусу», а потім натисніть будь-який зареєстрований відбиток пальця (протягом 10 секунд), після успішної верифікації буде активована тривожна сигналізація примусу. В стані [ ВІКЛ.] натискання «Клавіші

примусу »не викличе тривожну сигналізацію.

**Тривожна сигналізація при збігу 1: 1:** в стані [ ВКЛ.], коли користувач використовує метод верифікації 1: 1 для верифікації будь-якого зареєстрованого відбитка пальця спрацьовує тривога. В стані [ ВІКЛ.] тривожна сигналізація не спрацьовує.

**Тривожна сигналізація при збігу 1: N:** в стані [ ВКЛ.], коли користувач використовує метод верифікації 1: N для верифікації будь-якого зареєстрованого відбитка пальця спрацьовує тривога. В стані [ ВІКЛ.] тривожна сигналізація не спрацьовує.

**Тривожна сигналізація по паролю:** в стані [ ВКЛ.], коли користувач використовує метод верифікації за паролем спрацьовує сигналізація. В стані [ ВІКЛ.] тривожна сигналізація не спрацьовує.

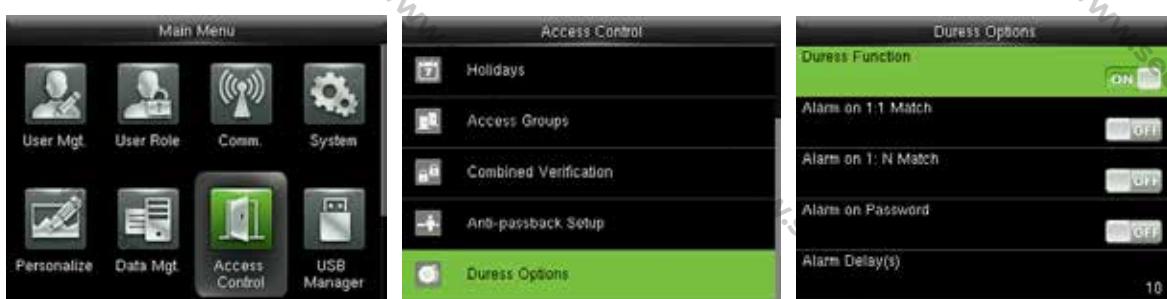
**Час очікування спрацювання тривожної сигналізації (сек):** коли тривожна сигналізація примусу спрацьовує пристрій відправить тривожну сигналізацію через 10 секунд (за замовчуванням); час очікування спрацювання тривожної сигналізації може бути змінено (значення знаходиться в діапазоні від 1 до 999 секунд).

### 7.7.1 Налаштування клавіші примусу

**функція примусу:** в стані [ ВКЛ.] натисніть «Кнопка примусу», а потім натисніть будь-який зареєстрований відбиток пальця (протягом 10 секунд), після успішної верифікації буде активований сигнал примусу. В стані [ ВИКЛ.] натискання «Клавіші примусу» не викличе тривожної сигналізації.

**встановити M / OK як клавіші примусу**

**1. Увімкніть функцію примусу:** в початковому інтерфейсі натисніть [ M / OK]> Контроль доступу> Параметри примусу> Функція примусу, натисніть [ M / OK]. Щоб включити Функцію примусу.



**2. Налаштування Клавіші примусу:** в початковому інтерфейсі натисніть

[M / OK]> Персоналізація> Швидкий доступ швидкого виклику>

виберіть клавішу [ M / OK]> натисніть [ M / OK]> Функція> Оберіть

параметр «Кнопка примусу». ( Меню клавіша примусу

буде відображатися після включення Функції Примус).



- Примітки:** Клавіші напрямки або ESC також можуть бути встановлені в якості клавіші примусу.

## 8. Системные настройки

### 8.1 Параметры отслеживания рабочего времени



У початковому інтерфейсі натисніть [ M / OK] > Система > Облік робочого часу, щоб увійти в інтерфейс налаштувань **Обліку робочого часу**.

**Дублювати період сканування (хв):** протягом встановленого періоду часу (одиниця виміру: хвилини) дубльовані журнали обліку робочого часу не будуть зарезервовані (значення знаходитьться в діапазоні від 1 до 999999 хвилин).

**режим камери \***: для настройки зйомки і збереження фотографій при верифікації; може бути застосовано до всіх користувачів. Включені 5 режимів:

1. **Відсутність фотографії:** при верифікації користувача фото не робиться.
2. **Зробити фотографію, збереження відсутнє:** при верифікації користувача фотографія робиться, але не зберігається.
3. **Зробити фотографію і зберегти:** при верифікації фотографія зроблена і збережена.
4. **Зберегти при успішної верифікації:** при успішній верифікації фотографія зроблена і збережена.
5. **Зберегти при невдалої верифікації:** фотографія зроблена і збережена при невдалої верифікації.

**фотографія** призначеного для користувача **відображення \***: відображається для користувача фотографію, коли користувач проходить

верифікацію. Увімкніть [ВКЛ.], щоб відобразити фотографію користувача, і [OFF.], щоб вимкнути її.

**Оповіщення журналу подій обліку робочого часу:** якщо залишилася ємність менше встановленого значення, пристрій автоматично попередить користувачів про залишилася ємності. Його можна відключити або встановити в діапазоні від 1 до 9999.

**Циклічне видалення даних ATT:** число журналів подій обліку робочого часу, які можна видалити за один раз, коли досягається максимальне заповнення. Його можна відключити або встановити в діапазоні від 1 до 999.

**Циклічне видалення фотографій ATT ★:** число фотографій обліку робочого часу, які можна видалити за один раз, коли досягається максимальне заповнення. Параметр можна відключити або встановити в діапазоні від 1 до 99.

**Циклічне видалення фотографій чорного списку ★:** число фотографій чорного списку, які можна видалити за один раз, коли досягається максимальне заповнення. Параметр можна відключити або встановити в діапазоні від 1 до 99.

**Підтвердження часу очікування екрана (сек):** відображення інтерфейсу інформації про верифікації після верифікації. Діапазон значень від 1 до 9 секунд.

Наприклад, якщо для параметра **Підтвердження часу очікування екрана (Сек)** встановлено значення 5 сек., то після успішної верифікації інтерфейс інформації про верифікації буде закрито після закінчення 5 сек.

**Зберегти записи несанкціонованої верифікації:** щоб встановити, чи будуть зберігатися невдалі верифікації, наприклад, викликані доступом відповідно до недійсними графіками або неприпустимою комбінованої перевіркою, при включені функції розширеного контролю доступу.

## 8.2 Параметри відбитка пальця



В початковому інтерфейсі натисніть [ M / OK]> Система> Відбиток пальця, щоб увійти в інтерфейс налаштування Відбиток пальця.

**Граничне значення збігу 1: 1:** при способі верифікації 1: 1 верифікація може бути успішною лише тоді, коли збіг між верифіковані і зареєстрованим відбитком пальця користувача перевищує це значення.

**Граничне значення збігу 1: N:** при способі верифікації 1: N

верифікація може бути успішною лише тоді, коли збіг між верифіковані і всіма зареєстрованими відбитками пальців перевищує це значення.

**Рекомендоване граничне значення збігу:**

FRR	FAR	значення збігу	граничне
		1: N	1: 1
Високий. Низький.	45		25
Сер. Сер.	35		15
Низький. Високий.	25		10

**Чутливість датчика відбитків пальців:** установка чутливості зчитувача відбитків пальців.

Рекомендується використовувати рівень за замовчуванням « середнє ». Коли середовище сухе, що призводить до повільного виявлення відбитків пальців, ви можете встановити рівень « Висока », щоб підвищити чутливість; коли середовище волога, що ускладнює

ідентифікацію відбитку пальця, ви можете встановити рівень « **НИЗЬКЕ** ».

**Виявлення в онлайн режимі** ★: встановити, чи потрібно виявляти помилковий відбиток пальця. Увімкніть [ **Виявлення в онлайн режимі**], пристрій виявить помилковий відбиток пальця під час реєстрації та верифікації, щоб його не можна було успішно зареєструвати або верифікувати.

**Час повторення 1: 1.** При верифікації 1: 1 або верифікації за паролем користувачі можуть забути зареєстрований відбиток пальця або пароль або натиснути невірний палець. Щоб скоротити процес повторного введення ідентифікатора користувача повтор дозволений; число повторних спроб може бути в межах 1 ~ 9.

**Зображення відбитка пальця:** встановити відображати чи зображення відбитка пальця на екрані при реєстрації або верифікації. Доступні чотири варіанти: Показати для реєстрації, Показати для порівняння, Завжди показувати, Відсутня.

### 8.3 Скидання до заводських налаштувань

Скидання таких даних, як настройки зв'язку і системних налаштувань до заводських.



У початковому інтерфейсі натисніть [ **M / OK**]> **Система**> **Скидання**> **OK**, щоб завершити настройку скидання.

Параметри скидання включають параметри контролю доступу, параметри примусу, увімкнути обмеження подвійного проходу, настройку зв'язку (а саме, настройки Ethernet, Послідовна зв'язок, Підключення ПК, ADMS ★ і установка Wiegand), персоналізації (такі, як Голосова підказка,

Підказка клавіатури, Гучність і час очікування до переходу в сплячий режим), закрити стан сканування і т.д.

<b>параметри</b>	<b>Заводські настройки за замовчуванням</b>
Параметри контролю доступу	<p>Час очікування дверного замка: 10 сек Час очікування датчика двері: 10 сек Тип дверного датчика: Відсутня час очікування спрацювання тривожної сигналізації: 30 сек Число повторів до спрацьування тривожної сигналізації: 3 рази Період дії режиму Нормально закритий: Відсутній Період дії режиму Нормально відкритий: Відсутній Час допоміжного виходу / відкриття замку ★: 255 сек Налаштування типу допоміжного виходу: Тригер відкриття дверей Режими нормально відкритий / нормально закритий для свяtkovих днів: ВИКЛ. Тривожна сигналізація динаміка: ВИКЛ.</p>
параметри примусу	<p>Параметри примусу: ВИКЛ. Тривожна сигналізація на основі збігу 1: 1: ВИКЛ. Тривожна сигналізація на основі збігу 1: N: ВИКЛ. Тривожна сигналізація по паролю: ВИКЛ.</p>

	Час очікування тривожної сигналізації: 10 сек
Напрямок заборони подвійного Заборона подвійного проходу відсутній проходу	
Ethernet	IP-адреса: 192.168.1.201 Маска підмережі: 255.255.255.0 DNS: 0.0.0.0
підключення ПК	Ключ зв'язку: 0 Ідентифікатор пристроя: 1
Хмарний сервер ★	Включити ім'я домену: ВИКЛ. Адреса сервера: 0.0.0.0 Порт сервера: 8081 Включити проксі сервер: ВКЛ. IP проксі-сервера: 0.0.0.0 Порт проксі-сервера: 0
установка Wiegand	Тип ідентифікатора входу / виходу Wiegand: ідентифікатор користувача Ширина імпульсу: 100 мкс Інтервал імпульсу 1000 мкс
Час бездіяльності до появи слайд-шоу	30 сек
Час бездіяльності до переходу в сплячий режим	30 хвилин
Час закінчення екрану меню Підказка	60 сек
клавіатури	ВКЛ.
голосова підказка	ВКЛ.
гучність	70

- **Примітка:** при скиданні до заводських налаштувань дата й час не будуть порушені.

Наприклад, якщо 1 січня 2020 року дата і час пристрої встановлені на 18:30, дата і час залишаться незмінними після скидання до заводських налаштувань.

## 8.4 Оновлення USB



Вставте USB-диск з файлом оновлення в порт пристрою і в початковому інтерфейсі натисніть [

**M / OK]> Система> Оновлення USB**, щоб завершити операцію оновлення прошивки.



Якщо необхідно оновлення, будь ласка зверніться до нашої служби техпідтримки. У звичайних обставинах оновлення прошивки не відновлюється.

## 9.Персоналізація налаштувань

### 9.1 Налаштування призначеного для користувача інтерфейсу



У початковому інтерфейсі натисніть [ М / OK]> Персоналізація> Інтерфейс користувача для установки Інтерфейсу користувача.

**шпалери:** в міру необхідності виберіть шпалери головного екрану, в пристрої можна знайти шпалери різних стилів.

**Мова:** в міру необхідності оберіть мову пристроя.

**Час закінчення екрану меню (сек):** якщо в інтерфейсі меню не виконується жодна операція, а час перевищує встановлене значення пристрій автоматично переходить на початковий інтерфейс. Ви можете відключити параметр або встановити значення 60 ~ 99999 секунд.

- Примітки:** якщо вибрано [ Відключено], система не вийде з інтерфейсу меню, навіть якщо не буде виконано жодних дій. Відключення цієї функції не рекомендується через велику споживаної потужності та небезпечності.

**Час бездіяльності до появи слайд-шоу (сек):** якщо в початковому інтерфейсі не відбувається ніяких операцій, а час перевищує встановлене значення з'явиться слайд-шоу. Його можна відключити (встановити на Відсутня) або встановити на 3 ~ 999 секунд.

**Інтервал слайд-шоу (сек):** є інтервалом між відображенням різних зображень слайд-шоу. Його можна відключити або встановити на 3 ~ 999 с.

**Час бездіяльності до переходу в сплячий режим (хв):** коли на

пристрій не виконується жодна операція і досягається встановлений час очікування пристрій переходить в режим очікування. Натисніть будь-яку клавішу або палець, щоб скасувати режим очікування. Ви можете відключити цю функцію або встановити значення від 1 до 999 хвилин. Якщо для цієї функції встановлено значення [ Відключено], пристрій не перейде в режим очікування.

- **Примітки:** відключення цієї функції не рекомендується через велику споживаної потужності.

**Стиль головного екрану:** вибір положення і способу відображення годин і клавіші стану.

**Ім'я компанії:** введіть ім'я компанії відповідним ПО.

## 9.2 Налаштування голосу



У початковому інтерфейсі натисніть [ M / OK]> Персоналізація> Голос, щоб увійти в інтерфейс налаштувань Голоси. Голосова підказка: Вкажіть, чи потрібно включати голосові підказки під час роботи, натисніть [ M / OK], щоб включити її.

**Підказка клавіатури:** Вкажіть, чи потрібно включати голос клавіатури під час натискання клавіатури, натисніть [ M / OK], щоб включити її.

**Гучність:** встановіть гучність пристрою. Натисніть кнопку .. щоб збільшити гучність, натисніть кнопку .. щоб зменшити гучність.

## 9.3 Налаштування дзвінків

Багато компаній вважають за краще використовувати дзвінок для позначення

робочого і неробочого часу. При досягненні запланованого часу для дзвінка пристрій буде автоматично відтворювати обрану мелодію дзвінка, поки не закінчиться тривалість дзвінка.



У початковому інтерфейсі натисніть [ М / OK]> Персоналізація> Графіки дзвінків> Новий графік дзвінка, щоб увійти в інтерфейс додавання.  
**Нового графіка дзвінка.**

**Стан дзвінка:** [ВКЛ.] для включення дзвінка, а [ ВИКЛ.] для його відключення.

**Час дзвінка:** дзвінок дзвонить автоматично при досягненні зазначеного часу.

**повторити:** встановити, чи повторювати дзвінок.

**рінгтон:** рингтон для дзвінка.

**інтервал часу очікування дзвінка (Сек):** для тривалості дзвінка. Значення варіється від 1 до 999 секунд.

#### 9.4 Налаштування станів сканування



У початковому інтерфейсі натисніть [ М / OK]> Персоналізація> Параметри стану сканування, щоб увійти в інтерфейс налаштувань Параметри стану сканування.

**Режим стану сканування:** Для вибору режиму стану

**сканування**, який включає наступні режими:

**1. Вимкн.**: відключення функції клавіші стану сканування. Ключ стану сканування, встановлений в меню **Швидкий доступ, швидкого доступу**, стане недійсним.

**2. Ручний режим**: для перемикання клавіші стану сканування вручну; клавіша стану сканування зникне після **закінчення часу стану сканування**.

**3. Автоматичний режим**: після вибору цього режиму встановіть час перемикання клавіші стану сканування в **Поєднаннях клавіш швидкого доступу**; коли час перемикання досягнуто, встановлена клавіша стану сканування переключиться автоматично.

**4. Ручний і автоматичний режим**: в цьому режимі на головному інтерфейсі відображається кнопка автоматичного перемикання стану сканування, в той же час підтримується ручне перемикання кнопки стану сканування. Після закінчення часу очікування клавіша стану сканування, перемикається вручну, стає клавішою стану сканування з автоматичним перемиканням.

**5. Ручний фікований режим**: після того, як клавіша стану сканування переключена вручну, клавіша стану сканування залишиться незмінною до наступного перемикання вручну.

**6. Фікований режим**: буде показаний тільки клавіша фікованого стану сканування, і її не можна перемкнути.

**Час закінчення стану сканування (сек)**: час закінчення відображення стану сканування. Значення варіюється від 5 до 999 секунд.

**Необхідну стан сканування**: чи потрібно вибирати стан обліку робочого часу при верифікації.

**ВКЛ .:** Вибір стану обліку робочого часу необхідний після верифікації.

**ВІКЛ** :: Вибір стану обліку робочого часу не потрібно після верифікації.

- **Примітка:** існує чотири стану сканування: реєстрація входу, реєстрація виходу, реєстрація входу при понаднормової роботи, реєстрація виходу при понаднормової роботи.

## 9.5 Налаштування клавіш швидкого виклику

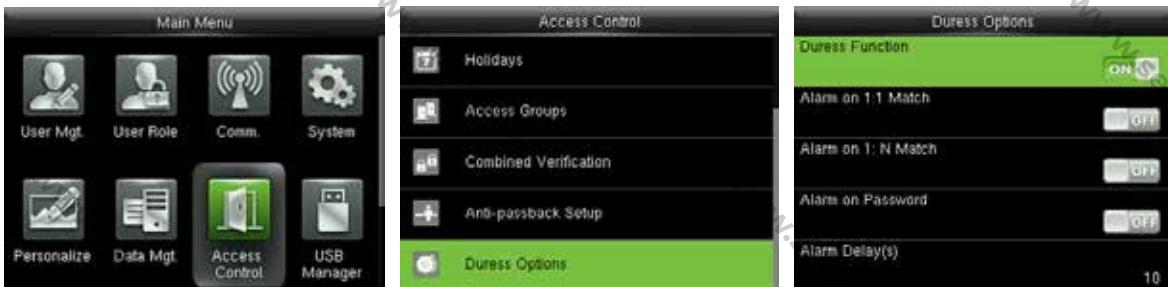
Швидкий виклик можна задати в якості клавіш стану сканування або клавіш функцій меню. Коли пристрій перебуває в головному інтерфейсі, натискання клавіші швидкого доступу відобразить стан обліку робочого часу або здійснить повернення в інтерфейс управління меню.



У початковому інтерфейсі натисніть [ М / OK]> Персоналізація> Швидкий доступ швидкого виклику, щоб увійти в інтерфейс налаштувань сполучення клавіш швидкого виклику.  
встановити М / OK як Клавіші Примусу.

**1. Увімкніть функцію примусу:** в початковому інтерфейсі натисніть

[М / OK]> Контроль доступу> Параметри примусу> Функція примусу, натисніть [ М / OK], щоб встановити параметр функція примусу на ВКЛ.



**2. Настройка Клавіші примусу:** в початковому інтерфейсі натисніть

[M / OK]> Персоналізація> Швидкий доступ швидкого виклику>

виберіть клавішу [ M / OK]> натисніть [ M / OK]> Функція> виберіть параметр

« **клавіша примусу** ».

(Меню клавіша примусу

відображатися після включення **Функції примусу**).



- Примітки:** Клавіші напрямки або ESC також можуть бути встановлені в якості клавіші примусу.

**Для установки Часу автоматичного перемикання:**

Виберіть будь-яку клавішу швидкого виклику і виберіть [ Параметри стану] у меню [ Функція], так щоб можна було встановити час автоматичного перемикання.

**Автоматичне перемикання:** при досягненні встановленого часу пристрій перемкне стан обліку робочого часу автоматично.



Коли клавіша швидкого виклику встановлено у вигляді **клавіші стану сканування**,

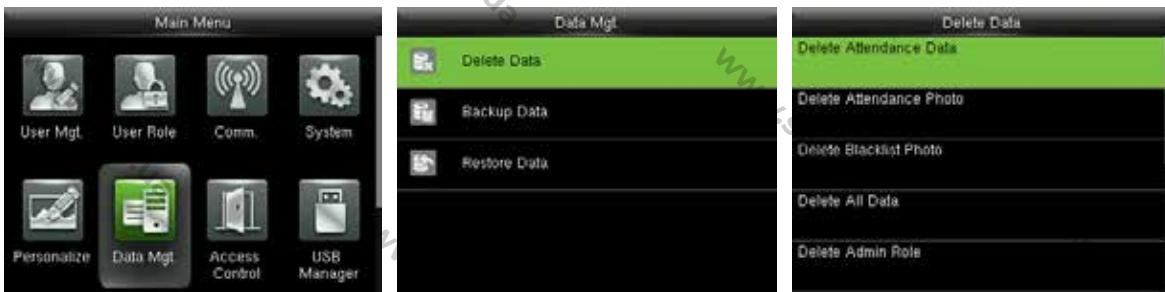
але режим [ **ВИКЛ.** ] обраний в меню [ **Режим стану сканування** ] (персоналізації>параметри стану сканування> Режим стану сканування> вибрати **ВИКЛ.** ), тоді

клавіша швидкого виклику не буде активована.

## 10. Управління даними

### 10.1 Управління даних

Для управління даними в пристрой, який включає видалення даних обліку робочого часу, видалення всіх даних, видалення ролі адміністратора і видалення заставок екрану і т.д.



У початковому інтерфейсі натисніть [ М / OK]> Управління даними> Видалити дані, щоб увійти в інтерфейс налаштувань **Видалити дані**.

**Видалити дані обліку робочого часу:** для видалення всіх даних обліку робочого часу в пристрой.

**Видалити фотографії обліку робочого часу \***: для видалення всіх призначених для користувача фотографій обліку робочого часу в пристрой.

**Видалити фотографії чорного списку \***: для видалення всіх фотографій чорного списку в пристрой, що означає фотографії зроблені після невдалих верифікації.

**Видалити всі дані:** для видалення всієї користувальницької інформацію, відбитки пальців і журнали подій обліку робочого часу і т.д.

**Видалити роль адміністратора:** для переведення всіх адміністраторів.

**Звичайні користувачі.**

**Видалити контроль доступу:** для видалення всіх даних доступу.

**видалити фотографію користувача \***: для видалення всіх призначених для користувача фотографій в пристрой.

**Видалити шпалери:** для видалення всіх шпалер в пристрой.

**Видалити заставки екрану:** для видалення всіх заставок екрану в пристрой.

(Детальніше про завантаження заставок см. В [17.4 Правило завантаження зображенъ](#).)

**Видалити дані резервної копії:** видалити всі дані резервної копії.

## 10.2 Резервне копіювання даних

Для резервного копіювання бізнес-даних або даних конфігурації на пристрій або USB-диск.

### Резервне копіювання на USB-диск



Вставте USB-диск. У початковому інтерфейсі натисніть [**M / OK**]> **Управління даними**> **Резервне копіювання даних**> **Резервне копіювання на USB-диск**> **Резервне копіювання вмісту**> виберіть вміст для резервного копіювання (**Бізнес-дані / Системні дані**)>

**Запуск резервного копіювання** для запуску резервного копіювання. Після завершення резервного копіювання перезапуск пристрою не потрібно.

- **Примітка:** операції **Резервного копіювання на Пристрій** такі ж, як і **резервне копіювання на USB-диск**.

## 10.3 Відновлення даних

Для відновлення даних на пристрой або з USB диска на пристрой. **Відновити з USB диска**.



Вставте USB-диск. У початковому інтерфейсі натисніть [ М / OK]> Управління даними> Відновити дані> відновити з **USB-диска**> **вміст**> виберіть вміст для відновлення ( **Бізнес-дані** /

**Системні дані**)> Почати відновлення> Оберіть **Так** для запуску відновлення. Після завершення відновлення натисніть [ OK], щоб автоматично перезапустити пристрій.

- **Примітки:** операції **Відновлення з пристрою** такі ж, як і при

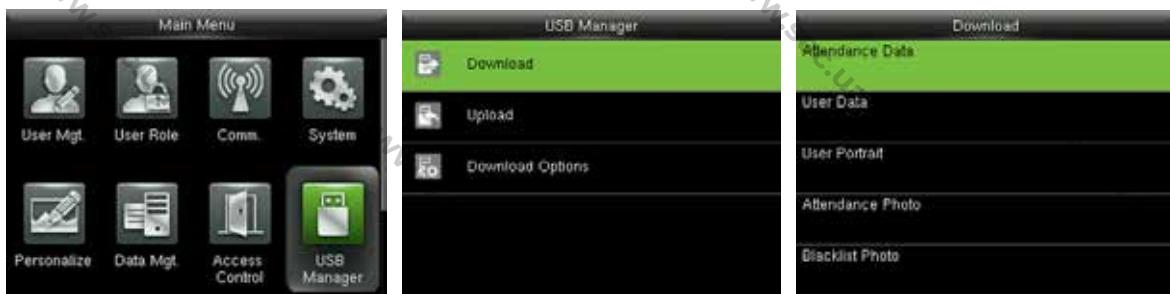
**Відновленні з USB-диска.**

## 11. Диспетчер USB

Завантажте або вивантажити дані між пристроєм і відповідним програмним забезпеченням за допомогою USB-диска.

Перед завантаженням / вивантаженням даних з / на USB-диск спочатку вставте USB-диск в USB-слот.

### 11.1 вивантажити на USB



У початковому інтерфейсі натисніть [ M / OK] > **Диспетчер USB** > **вивантажити на USB**, щоб увійти в інтерфейс **вивантажити на USB**. Період часу необхідно вибирати тільки при завантаженні **даних Обліку робочого часу**.

**Дані обліку робочого часу:** для завантаження даних обліку робочого часу за вказаний період часу на USB-диск

**зображення користувача \***: для завантаження всіх призначених для користувача фотографій з пристрою на USB-диск.

**Фотографії обліку робочого часу \***: для завантаження всіх фотографій обліку робочого часу з пристрою на USB-диск.

**Фотографії чорного списку \***: для завантаження всіх фотографій чорного списку ( фотографії, зроблені після невдалих верифікації) з пристрою на USB-диск.

## 11.2 Завантажити з USB



У початковому інтерфейсі натисніть [ М / OK]> Диспетчер USB> Завантажити, щоб увійти в інтерфейс Завантажити з USB.

призначенні для користувача      **дані:**      для      завантаження      всій      користувальницької інформації відбитків пальців з USB-диск на пристрій.

**зображення користувача** ★: для завантаження всіх призначених для користувача

фотографій з USB-диска на пристрій (Детальніше про завантаження призначених для користувача зображень см. в [17.4 Правило завантаження зображень](#) ).

**Заставка екрана:** для завантаження всіх заставок екрану з USB-диска на

пристрій. Ви можете обрати [ **Завантажити виbrane**

**зображення**] або [ **Завантажити всі зображення**]. зображення

будуть відображатися в головному інтерфейсі пристрою після завантаження

(специфікації заставок екрану см. в [17.4 Правило завантаження зображень](#) ).

**шпалери:** для завантаження всіх шпалер з USB-диска на пристрій. Ви можете

вибрати [ **Завантажити виbrane зображення**] або [ **Завантажити**

**всі зображення**]. Зображення будуть відображатися на екрані після завантаження

(специфікації шпалер см. в [17.4 Правило завантаження](#)

[зображень](#) ).

### 11.3 Налаштування параметрів завантаження

Для того, щоб зашифрувати дані обліку робочого часу на USB-диску або видалити дані обліку робочого часу.



У початковому інтерфейсі натисніть [ М / OK]> Диспетчер USB> Уст, щоб увійти в інтерфейс налаштувань **Параметрів завантаження**.

Натисніть [ М / OK], щоб включити або вимкнути параметри [ **зашифрувати дані обліку робочого часу**] і [ **Видалити дані ATT**].

- **Примітки:** зашифровані дані обліку робочого часу можна імпортувати тільки в програмному забезпеченні ZKTime.Net 3.0.

## 12. Пошук подій обліку робочого часу

При успішній верифікації користувачів записи подій обліку робочого часу зберігаються на пристрої. Ця функція дозволяє користувачам перевіряти журнали подій обліку робочого часу, фотографії обліку робочого часу ★ і фотографії чорного списку ★.

### 12.1 Пошук записи обліку робочого часу



У початковому інтерфейсі натисніть [ M / OK]> Пошук обліку робочого часу> Запис обліку робочого часу> введіть ідентифікатор користувача ( якщо ідентифікатор не введений буде виконаний пошук всіх записів)> виберіть Період часу> натисніть [ M / OK], потім будуть показані відповідні журнали подій обліку робочого часу.

### 12.2 Пошук фотографій обліку робочого часу ★



У початковому інтерфейсі натисніть [ M / OK]> Пошук подій обліку робочого часу

> фотографія обліку робочого часу > ввести

Призначений для користувача ідентифікатор ( якщо ідентифікатор не введений буде виконаний пошук всіх фотографій обліку робочого часу)> виберіть

**Період часу**> натисніть [ M / OK], потім будуть показані відповідні фотографії обліку робочого часу.

### 12.3 Пошук фотографії чорного списку ATT \*



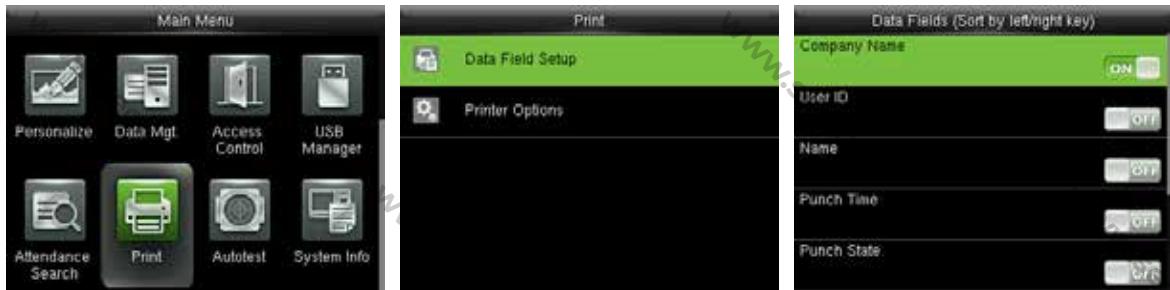
У початковому інтерфейсі натисніть [ M / OK]> Пошук подій обліку робочого часу> Фотографія чорного списку ATT> Оберіть **Період часу**> натисніть [ M / OK], потім будуть показані відповідні фотографії чорного списку.

- **Примітки:** параметр [ Зберегти при невдалої верифікації] повинен бути обраний в меню [ Режим камери] ( натисніть [ M / OK]> [Система]> [Облік робочого часу]> [Режим камери]> Оберіть зберегти при невдалої верифікації), так щоб зберегти фотографії чорного списку в пристрої.

## 13. Налаштування друку \*

Пристрої з функцією друку можуть роздруковувати записи подій обліку робочого часу, коли підключений принтер (ця функція є опціональною і може бути встановлена тільки в деяких пристроях).

### 13.1 Налаштування поля даних друку



У початковому інтерфейсі натисніть [ М / OK] > Друк > Установка поля друку > натисніть [ М / OK], щоб включити / вимкнути поля, які необхідно роздрукувати.

- **Примітки:** при друку положення полів інформації можна налаштовувати за допомогою лівої / правої клавіші: натисніть ліву клавішу для переходу до попереднього пункту, і натисніть праву клавішу для переходу до наступного пункту.

### 13.2 Налаштування параметрів друку



У початковому інтерфейсі натисніть [ М / OK] > Друк > Параметри друку > натисніть [ М / OK], щоб включити / вимкнути функцію Обрізка паперу.

- **Примітки:** для того, щоб включити функцію обрізка паперу

потрібно підключити принтер з функцією обрізки паперу, так щоб під час друку принтер обрізав папір відповідно до обраної інформацією друку.

## 14. Автоматичне тестування

Для автоматичного тестування правильної роботи всіх модулів в пристрой, включаючи РК-дисплей, звук, клавіатуру, датчик відбитка пальця, камеру ★ і годинник реального часу (RTC).



У початковому інтерфейсі натисніть [ **M / OK** ]> **Автоматичне тестування**, щоб увійти в інтерфейс **Автоматичне тестування**.

**Тестувати все:** для тестування РК, звуку, клавіатури, датчика відбитків пальців, камери ★ і RTC.

Під час тестування натисніть [ **M / OK** ], щоб перейти до наступного тестування, або натисніть [ **ESC** ] для виходу з тестування.

**Тестувати РК:** для тестування ефектів відображення РК-екрану з допомогою відображення повного кольору, чистого білого і чистого чорного для перевірки правильності відображення коліору на екрані. Під час тестування натисніть [ **M / OK** ], щоб перейти до наступного тестування, або натисніть [ **ESC** ], щоб вийти з тестування.

**Тестування голоси:** пристрой автоматично тестує заповнення зберігаються на пристрої голосового супроводу і автоматично тестує якість голосу. Під час тестування натисніть [ **M / OK** ], щоб перейти до наступного тестування, або натисніть [ **ESC** ], щоб вийти з тестування.

**Тестування клавіатури:** для тестування всіх клавіш і перевірки роботи їх функцій. Натисніть будь-яку клавішу в інтерфейсі тестування

**Тестування клавіатури;** якщо натиснута клавіша збігається із позначкою клавіші на екрані, тоді клавіша функціонує правильно. натисніть [ **M / OK**], або натисніть [ESC], щоб вийти з тестування.

**Тестування датчика відбитків пальців:** для тестування сканера відбитка пальця, натисніть відбиток пальця, щоб перевірити, чи є зібране зображення відбитка пальця чітким. При натисканні відбитка пальця на датчик зображення буде відображатися на екрані. натисніть [ **M / OK**] або [ **ESC**], щоб вийти з тестування.

**Тестувати камеру ★:** для тестування правильності роботи камери шляхом перевірки якості фотографій. Натисніть [M / OK] або [ESC], щоб вийти з тестування.

**Перевірка годин RTC:** для тестування годин реального часу. Пристрій перевіряє, чи правильно працюють годинник, перевіряючи секундомір натисніть [ **M / OK**], щоб почати відлік часу, і натисніть його ще раз, щоб припинити відлік, щоб побачити, чи точно секундомір відраховує час. натисніть [ **ESC**], щоб вийти з тестування.

## 15. Системна інформація

Перевірте ємність даних, інформацію про пристрій і прошивці.



У початковому інтерфейсі натисніть [ М / OK]> Інформація про систему, щоб увійти в інтерфейс Інформація про систему.

Device Capacity		Device Info		Firmware Info	
User (used/max)	5/5000	Device Name	ProCapture	Firmware Version	Ver 0.0.1-20150619
Admin User	0	Serial Number	3383151500003	Bio Service	Ver 2.1.12-20150603
Password	4	MAC Address	00:17:61:12:51:98	Push Service	Ver 2.0.2-20150115
Fingerprint (used/max)	2/3000	Fingerprint Algorithm	ZKfinger VX10.0	Standalone Service	Ver 2.0.2-20150318
Badge (used/max)	1/5000	Platform Information	ZMM220_TFT	Dev Service	Ver 1.0.101-20141008

ємність пристрою

інформація про пристрій

Інформація про прошивці

**Ємність пристрою:** для відображення числа зареєстрованих користувачів, адміністраторів, паролів, відбитків пальців, карт, записів обліку робочого часу і фотографій обліку робочого часу ★, також для перевірки загального сховища користувачів, відбитків пальців, карт, записів обліку робочого часу і фотографій обліку робочого часу ★

**Інформація про пристрій:** для відображення імені пристрію, серійного номера, MAC-адреси, алгоритму ідентифікації відбитків пальців, інформації про платформу, версії MCU, виробника і дати виготовлення.

**Інформація про прошивці:** для відображення версії прошивки, служби Bio, служби Push, служби автономного устрою і служби Dev.

- **Примітка:** відображення ємності пристрою, інформації про пристрій і Інформації про прошивці на системному інформаційному інтерфейсі різних пристрів може відрізнятися; фактичне пристрій має переважну силу.

## 16. Пошук та усунення несправностей

- Датчик відбитку пальців не може ефективно сканувати і верифікувати відбитки пальців.

- Перевірте чи не мокрий палець, або чи не забруднений датчик пальців.
- Очистіть палець і датчик відбитків пальців і спробуйте знову.
- Якщо палець занадто сухий, подмімо на нього і спробуйте знову.
- після верифікації відображається «Невірний період санкціонованого доступу».
  - Зверніться до адміністратора, щоб перевірити має користувач право на отримання доступу протягом цього часу.

- Верифікація пройшла успішно, але користувач не може отримати доступ.

- Перевірте чи правильно встановлена для користувача привілей.
- Перевірте правильність проводки замку.
- Антивандальна сигналізація спрацювала.

Перевірте чи закріплени пристрій і задня панель разом; якщо ні,

антивандальна сигналізація спрацює і підніме тривогу, значок буде відображатися в правому верхньому куті інтерфейсу. Тільки коли для параметра [ **Тривожна сигналізація динаміка**] **(Контроль доступу> Параметри контролю доступу> тривожна сигналізація динаміка)** встановлено значення [ **ВКЛ**], динамік подасть сигнал тривоги.



## **17. Додатки**

## 17.1 Функція фотографії-ідентифікатора ★

- Примітки: Деякі моделі

підтримують функцію ідентифікації фотографій.

Коли функція ідентифікатора фотографії включена і користувач проходить верифікацію.



буде відображені не тільки інформація про ідентифікатор і ім'я користувача, а й фотографія, зареєстрована користувачем або збережена на USB-диску.

## [Порядок роботи]

Якщо використовується для користувача фотографія, зроблена пристроєм, фотографія буде відображатися відразу після перевірки користувача.

Якщо використовується фотографія користувача на USB-диску, порядок дій буде наступним:

(1) Створіть файл з ім'ям « **photo** » на USB-диску і збережіть фотографію користувача в файл.

(2) Формат фотографії повинен бути JPG, а файл повинен бути названий як ідентифікатор користувача. Наприклад: фотографія, відповідна користувачеві з ідентифікатором 154, повинна бути названа 154.jpg. (3) Вставте диск USB в порт USB пристрою і увійдіть в **Диспетчер USB**>

**Завантажити> Зображення користувача, щоб завантажити фотографії**

користувачів.

Фотографія буде показана після верифікації

користувача.

- Примітка:

(1) Ім'я фотографії повинно бути в межах 9 цифр. (2) Розмір фотографії повинен бути менше 15 КБ.

(3) Нещодавно завантажена фотографія замінить оригінальну фотографію користувача.

(4) При завантаженні користувальницею фотографії увійдіть в **Диспетчер USB>Завантажити>Зображення користувача** на USB-диску автоматично буде створений файл з ім'ям «photo», в якому будуть збережені всі завантажені призначені для користувача фотографії.

## 17.2 Введення в Wiegand

Протокол Wiegand26 - це стандартний протокол контролю доступом, розроблений Підкомітетом Стандарт Контролю Доступу, що входять в Асоціацію індустрії безпеки (SIA), і який використовується для порту і виходу безконтактного зчитувача інтелектуальних карт.

Протокол визначає порт між пристроєм читання карт і контролером, які широко використовуються в системах контролю доступу, безпеки та інших суміжних галузях. Він контролює роботу розробників пристріїв читання карт і виробників контролерів. Пристрії контролю доступу, вироблені нашою компанією, також застосовують цей протокол. ,

### цифровий сигнал

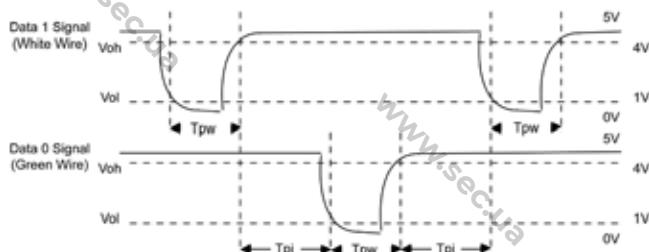
На Рис. 1 показана схема послідовності операцій пристрой читання карт, що відправляє цифровий сигнал в бітах на контролер доступу. На цій діаграмі Wiegand слід стандартному протоколу управління доступом SIA, який призначений для 26-розрядного пристроя зчитування карт Wiegand (з тривалістю імпульсу в межах від 20 мкс до 100 мкс і час перемикання імпульсів в межах 200 мкс і 20 мс). Сигнали Data1 і Data0 мають високий рівень (більше, ніж Voh), поки пристрій зчитування карт не буде готове до відправки потоку даних. Пристрій читання карт відправить асинхронний імпульс низького рівня (менше, ніж Voh), Передача потоку даних через провід Data1 або Data0 до блоку управління доступом (як пилообразна хвиля на Рис. 1).

Імпульси Data1 і Data0 не перекриваються і не синхронізовані. На Рис. 1 показана максимальна і мінімальна тривалість імпульсу (послідовні імпульси) і час перемикання імпульсів (Час між двома імпульсами), що допускається терміналами контролю доступу з використанням відбитка пальця серії F.

**Таблиця 1: Тривалість імпульсу**

знак	Визначено	Типове значення
Tpw	Ширина імпульсу	100 мкс
Tpi	інтервал імпульсу	1 мс

**Мал. 1: Діаграма послідовності**



### 17.3 Правило завантаження зображення

**1. Зображення користувача:** в файлі USB-диска необхідно створити файл з ім'ям «photo» і помістити в нього призначені для користувача фотографії. Ємність становить 8000 зображень (з огляду на фактичну ємність пристрою, рекомендується завантажити не більше 5000 зображень), причому кожне з них не повинна перевищувати 15 КБ. Ім'я зображення - x.jpg (x фактичний ідентифікатор користувача, макс. 9 цифр). Формат фото повинен бути JPG.

**2. Рекламне зображення:** необхідно створити файл з ім'ям

«Advertise» в файлі USB-диска і помістити в нього рекламні зображення. Ємність становить 20 зображень, кожне з яких не перевищує 30k. Ім'я та формат зображення не обмежені.

**3. Шпалери:** необхідно створити файл з ім'ям « **шпалери** » В файлі USB-диска і помістити шпалери в файл. Ємність становить 20 зображень, кожне з яких не перевищує 30k.

Ім'я та формат зображення не обмежені.

- **Примітка:** якщо розмір кожної фотографії користувача і фотографії обліку робочого часу не перевищує 10 КБ, пристрій може зберегти загальна кількість 10000 фотографій користувача і обліку робочого часу (з огляду на фактичну ємність пристрою, настійно рекомендується завантажити не більше 5000 фотографій користувачів та обліку робочого часу).

#### 17.4 Функції друку •

- **Примітки:** тільки деякі моделі підтримують функцію друку.

##### Інструкція по функціям

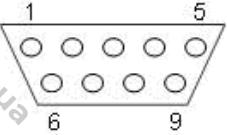
Ця функція підтримує тільки послідовний порт, але не друк через паралельний порт. Друкований контент виводиться в форматі RS232; інформація про верифікації буде виводитися кожен раз на послідовний порт. Друк доступна, якщо підключений принтер, або можна використовувати гіпертерміналу для зчитування вихідного вмісту.

##### Підключення принтера до пристрою

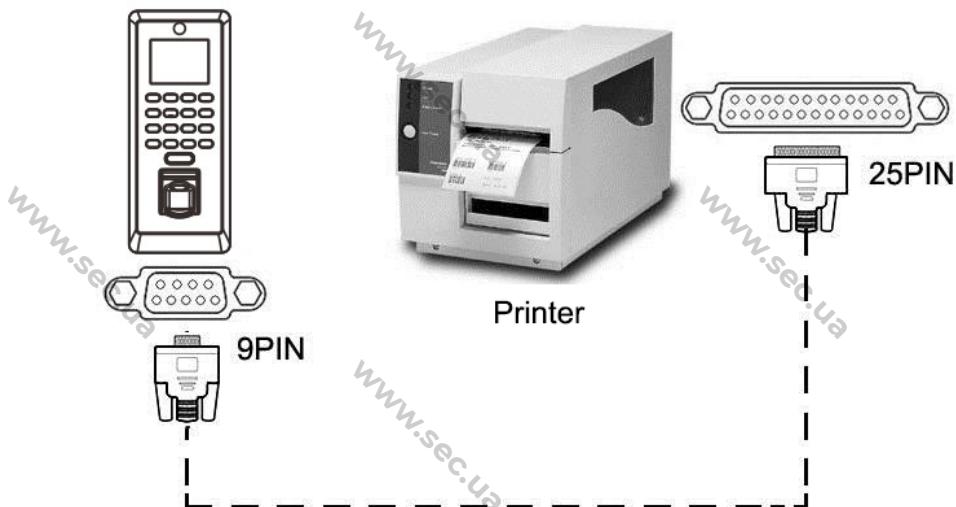
2 TXD <----> 3 RXD 3 RXD

<----> 2 TXD 5 GND <---->

7 FG

<b>RS232, порядок роз'ємів</b>	
--------------------------------	---

#### [Схема підключення]



#### [Операції]

1. У початковому інтерфейсі натисніть [**M / OK**]>**Зв'язок**>**Послідовна зв'язок**>**Швидкість передачі даних**, і виберіть 19200 в якості швидкості передачі.

2. У початковому інтерфейсі натисніть [**M / OK**]>**Друк.** щоб встановити формат і параметри друку, зверніться до розділу [13 Налаштування друку](#) ★ .

#### Примітка:

1. Швидкість передачі даних пристрою і принтера (гіпертерміналу) повинна бути однаковою.

2. Якщо формат друку за замовчуванням не задовільний, ви можете зв'язатися з нашою компанією, щоб налаштовувати інші формати.

## **17.5 Заява про права людини і конфіденційності**

**Шановні клієнти:**

Дякуємо

Як всесвітньо відомий постачальник біометричних технологій і послуг, ми приділяємо велику увагу дотриманню законів, що стосуються прав людини і недоторканності приватного життя в кожній країні, постійно проводячи дослідження та розробки.

Справжнім ми робимо наступні заяви:

1. Всі наші пристрою розпізнавання відбитків пальців для цивільного використання збирають тільки характерні точки відбитків пальців, а не зображення відбитків пальців, і, отже, ніяких проблем конфіденційності.

2. Характерні точки відбитків пальців, зібрані нашими продуктами, не можуть бути використані для відновлення оригінальних зображень відбитків пальців, отже, ніяких проблем конфіденційності.

3. Ми, як постачальник обладнання, не неємо юридичної, прямої чи опосередкованої відповідальності за будь-які наслідки, що винikли в результаті використання наших продуктів.

4. За будь-яких спорах, пов'язаних з правами людини або

недоторканністю приватного життя при використанні наших продуктів, звертайтесь безпосередньо до свого роботодавця.

Наше інше поліцейське обладнання або засоби розробки відбитків пальців забезпечать функцію збору вихідного відбитка пальця громадян. Що стосується того, чи є такий тип збору відбитків пальців порушенням вашої конфіденційності, будь ласка, зв'яжіться з урядом або

кінцевим постачальником обладнання. Ми, як виробник оригінального обладнання, не неємо юридичну відповідальність за будь-які порушення, що виникають в зв'язку з цим.

Закон Китайської Народної Республіки містить наступні положення, що стосуються свободи особистості:

1. Незаконний арешт, затримання або обшук громадян Китайської Народної Республіки заборонені; Порушення приватного життя заборонено.
2. Особисту гідність громадян Китайської Народної Республіки НЕ дотик.
3. Будинок громадян Китайської Народної Республіки НЕ дотик.
4. Свобода і таємниця листування громадян Китайської Народної Республіки охороняються законом.

Нарешті, ми ще раз підкреслюємо, що біометрія, як передова технологія розпізнавання, буде застосовуватися в багатьох секторах, включаючи електронну комерцію, банківська справа, страхування і юридичні питання. Щороку люди у всьому світі страждають від величезних втрат через ненадійність паролів. Розпізнавання відбитків пальців насправді забезпечує адекватний захист вашої особистості в умовах високої безпеки.

## **17.6 Опис екологічного використання**

Період екологічного використання (EFUP), позначений на цей продукт, відноситься до періоду безпеки, протягом якого продукт використовується в умовах, зазначених в інструкціях по продукту, без витоку шкідливих і шкідливих речовин.



EFUP цього продукту не поширюється на витратні матеріали, які необхідно регулярно замінювати, такі як батареї і т. д. ЕФУП батарей 5 років.

### **Назви і концентрація токсичних і небезпечних речовин або елементів**

Назва частин	Найменування частин Токсичні і небезпечні речовини або елементи					
	Pb	Hg	Cd	Сr6+	PBB	PBDE
чіп резистор	×	•	•	•	•	•
чіп конденсатор	×	•	•	•	•	•
чіп індуктор	×	•	•	•	•	•
чіп діод	×	•	•	•	•	•
компоненти ESD	×	•	•		•	•
зумер	×	•	•	•	•	•
адаптер	×	•	•	•	•	•
гвинти	•	•	•	×	•	•

• : Вказує, що це токсична або небезпечна речовина, що міститься у всіх однорідних матеріалах для цієї частини, нижче граничного вимоги в SJ / T11363-2006.

×: Вказує, що це токсична або небезпечна речовина, що міститься принаймні в одному з однорідних матеріалів для цієї частини, перевищує граничне вимога в SJ / T11363-2006.

Примітка: 80% деталей в цьому продукті виготовлені з безпечних для навколошнього середовища матеріалів. Вміщені в них небезпечні речовини або елементи в даний час не можуть бути замінені екологічно чистими матеріалами через технічні або економічних обмежень.