Посібник користувача

Панель управління доступом C2-260

Про компанію

ZKTeco є одним із найбільших у світі виробників RFID та біометричних (відбитків пальців, обличчя, рисунків вен на долонях) зчитувачів. Асортимент продуктів включає зчитувачі та панелі управління доступом, камери для розпізнавання обличчя ближнього та дальнього радіусу дії, контролери доступу до ліфтів/поверхів, турнікети, контролери воріт із системою розпізнавання номерних знаків (LPR) і споживчі продукти, включаючи дверні замки з живленням від батареї, які зчитують обличчя та відбитки пальців. Наші рішення безпеки багатомовні та локалізовані понад 18 різними мовами. На сучасному виробничому об'єкті ZKTeco площею 700 000 квадратних футів, сертифікованому за стандартом ISO9001, ми контролюємо виробництво, дизайн продукту, складання компонентів і логістику/доставку – усе під одним дахом.

Засновники ZKTeco були налаштовані на незалежні дослідження та розробку процедур біометричної верифікації та створення біометричної перевірки SDK, який спочатку широко застосовувався в сферах безпеки ПК та автентифікації. Завдяки безперервному вдосконаленню розвитку та численним ринковим додаткам команда поступово створила екосистему автентифікації особи та розумну екосистему безпеки, які базуються на методах біометричної перевірки. Завдяки багаторічному досвіду індустріалізації біометричних перевірок, ZKTeco була офіційно заснована в 2007 році і зараз є однією з провідних світових компаній у галузі біометричної перевірки, яка володіє різними патентами та обрана Національним високотехнологічним підприємством протягом 6 років поспіль. Її продукція захищена правами інтелектуальної власності.

Про посібник

Цей посібник знайомить з роботою **Панелі управління доступом C2-260**.

Усі малюнки наведені лише для ілюстрації. Малюнки в цьому посібнику можуть не повністю відповідати реальним виробам.

Умовні позначення документів

Умовні позначення, що використовуються в цьому посібнику, перераховані нижче:

Умовні позначення графічного інтерфейсу

Для програмного забезпечення	
Позначення	**Опис**
Жирний шрифт	Використовується для позначення назв програмних інтерфейсів, наприклад, **OK**, **Confirm (Підтвердити)**, **Cancel (Скасувати)**
>	Цими дужками відокремлюються багаторівневі меню. Наприклад, File (Файл) > Create (Створити) > Folder (Папка).
Для пристрою	
Позначення	**Опис**
< >	Назви кнопок або клавіш для пристроїв. Наприклад, натисніть <OK>
[ ]	Назви вікон, пунктів меню, таблиць даних і полів взято у квадратні дужки. Наприклад, відкрийте вікно [New user] (Новий користувач).
/	Багаторівневі меню розділяються косою рискою. Наприклад, [File (Файл) / Create (Створити) / Folder (Папка)].

Символи

Позначення	Опис
	Цей символ передбачає інформацію про повідомлення або привертає увагу у посібнику.
	Загальна інформація, яка допомагає швидше виконувати операції.
	Інформація, яка є важливою.
	Заходи вжиті, щоб уникнути небезпеки чи помилок
	Твердження або подія, що попереджає про щось або служить застережливим прикладом.

Зміст

1 ІНСТРУКЦІЇ З ТЕХНІКИ БЕЗПЕКИ 4

1.1 Важливі інструкції з безпеки 4
1.2 Інструкція з монтажу 5

2 ВВЕДЕННЯ У СИСТЕМУ 7

2.1 Функціональні параметри системи 7
2.2 Технічні параметри продукту 7
2.3 Індикатори панелі управління 7

3 УСТАНОВКА ТА ПІДКЛЮЧЕННЯ 9

3.1 Процедура установки 9
3.2 Монтаж дротів панелі управління доступом 10
3.3 Встановлення системи панелі управління 11
3.4 Підключення клем панелі управління 12
3.5 З'єднання з дверними датчиками, вимикачами виходу, додатковими пристроями вводу та зв'язком розширення RS485 13
3.6 З'єднання зі зчитувачами RS485/Wiegand 16
3.7 Підключення релейного виходу 18

4 ЗВ'ЯЗОК З ОБЛАДНАННЯМ 20

4.1 Мережеві дроти та проводка управління доступом 20
4.2 TCP/IP зв'язок 21
4.3 ZKPanelWeb 21

5 ZKBIOACCESS 26

5.1 Вхід в систему 26
5.2 Активувати систему 26
5.3 Змінити пароль 26
5.4 Пристрій 27
5.4.1 Додавання пристрою 28
5.4.2 Плата вводу/виводу 32
5.4.3 Робота пристрою 33
5.5 Додати користувача і картку 40
5.6 Налаштування управління доступом 45
5.7 Моніторинг у реальному часі 45
5.8 Звіти 49

ДОДАТОК 1 51

Демонстрація підключення C2-260, WR485 та зчитувача Wiegand 51

ДОДАТОК 2 56

Заява про право на конфіденційність 56
Екологічно чисте виробництво 57

1 Інструкції з техніки безпеки

1.1 Важливі інструкції з безпеки

1. Перед початком роботи уважно прочитайте інструкцію та дотримуйтесь її. Зберігайте інструкцію для подальшого використання.
2. Аксесуари: Будь ласка, використовуйте аксесуари, рекомендовані виробником, або ті, що постачаються разом із виробом. Не рекомендується використовувати інші аксесуари, зокрема великі системи сигналізації та моніторингу. Основна система сигналізації та моніторингу повинна відповідати місцевим стандартам пожежної безпеки та безпеки.
3. Застереження щодо встановлення: Не встановлюйте це обладнання на нестійкий стіл, штатив, опору або підставку, щоб уникнути падіння та пошкодження обладнання або будь-якого іншого небажаного результату, що може призвести до серйозних травм. Тому дуже важливо встановлювати обладнання відповідно до інструкцій виробника.
4. Всі периферійні пристрої повинні бути заземлені.
5. Зовнішні з'єднувальні дроти не повинні бути оголеними. Всі з'єднання і неробочі кінці проводів повинні бути обмотані ізоляційними стрічками, щоб запобігти пошкодженню обладнання при випадковому дотику до оголених проводів.
6. Ремонт: Не намагайтеся проводити несанкціонований ремонт обладнання. Розбирання або від'єднання є ризикованим і може призвести до ураження електричним струмом. Всі ремонтні роботи повинні виконуватися кваліфікованим фахівцем.
7. У разі виникнення будь-якої з наведених нижче ситуацій, спочатку відключіть живлення від обладнання та негайно зверніться до фахівця.
   - ✧ *Пошкоджено шнур живлення або роз'єм.*
   - ✧ *На пристрій потрапила будь-яка рідина або матеріал.*
   - ✧ *Обладнання вологе або піддалося впливу несприятливих погодних умов (дощ, сніг тощо).*
   - ✧ *Якщо обладнання не працює належним чином, навіть якщо воно експлуатується відповідно до інструкцій, переконайтеся, що ви регулюєте тільки ті елементи управління, які вказані в інструкції з експлуатації. Неправильне регулювання інших компонентів керування може призвести до пошкодження обладнання; обладнання може вийти з ладу назавжди.*
   - ✧ *Обладнання падає або його продуктивність різко змінюється.*
8. Заміна компонентів: Якщо необхідно замінити компонент, тільки уповноважений технічний фахівець може замінити аксесуари, зазначені виробником.
9. Перевірка безпеки: Після ремонту обладнання технічний фахівець повинен провести перевірку безпеки, щоб забезпечити належну роботу обладнання.

10. Живлення: Експлуатуйте обладнання тільки з типом джерела живлення, зазначеним на етикетці. Якщо ви не впевнені щодо типу джерела живлення, зверніться до технічного спеціаліста.

Порушення будь-якого з наведених нижче застережень може призвести до травм або виходу з ладу обладнання. Ми не несемо відповідальності за завдані внаслідок цього збитки або травми.

- Перед встановленням вимкніть зовнішній ланцюг (який живить систему), зокрема замки.
- Перед підключенням обладнання до електромережі переконайтеся, що вихідна напруга знаходиться в межах зазначеного діапазону.
- Ніколи не підключайте живлення до завершення монтажу.

1.2 Інструкція з монтажу

1. Кабелі проводів під реле повинні відповідати металевим кабелям; для інших проводів можна використовувати ПВХ-кабелі, щоб запобігти виходу з ладу через пошкодження гризунами. Панель управління має належні антистатичні, блискавкозахисні та герметичні функції, тому переконайтеся, що її корпус і дріт заземлення змінного струму правильно з'єднані, а дріт заземлення змінного струму фізично заземлений.
2. Не рекомендується часто під'єднувати/від'єднувати з'єднувальні клеми, коли система увімкнена. Обов'язково від'єднуйте з'єднувальні клеми перед початком будь-яких зварювальних робіт.
3. Не від'єднуйте та не замінюйте будь-яку мікросхему панелі управління без дозволу, недозволена операція може призвести до пошкодження панелі управління.
4. Не рекомендується підключати будь-які інші допоміжні пристрої без дозволу. Про всі нестандартні операції необхідно заздалегідь повідомляти наших інженерів.
5. Не допускається підключення панелі управління до однієї розетки з будь-якими іншими пристроями, що споживають великий струм.
6. Зчитувачі карток і кнопки бажано встановлювати на висоті від **1,4 до 1,5 м** над землею або відповідно до звичної практики клієнтів для правильного налаштування.
7. Рекомендується встановлювати панелі управління в місцях, де обслуговування є простим, наприклад, у **приміщеннях з низьким рівнем електромагнітних перешкод**.
8. Наполегливо рекомендується, щоб відкрита частина будь-якої з'єднувальної клеми **не була довшою за 4 мм**, а для уникнення короткого замикання або порушення зв'язку внаслідок випадкового контакту з надмірно оголеними проводами можна використовувати спеціальні затискні інструменти.
9. Для збереження записів подій управління доступом періодично експортуйте дані з панелей управління.
10. Підготуйте контрзаходи відповідно до сценаріїв застосування на випадок несподіваного відключення електроенергії, наприклад, **виберіть живлення від ДБЖ**.

11. Якщо зчитувач RS485 підключений ззовні і має спільне джерело живлення з пристроєм (панель управління не підтримує перевірку відбитків пальців зчитувача RS485), рекомендується, щоб відстань між портом зчитувача RS485 і зчитувачем не перевищувала 100 м. В іншому випадку рекомендується використовувати окреме джерело живлення зчитувача.
12. Для захисту системи управління доступом від самоіндукції електрорушійної сили, що генерується електронним замком в момент вимкнення/ввімкнення, необхідно **паралельно з електронним замком підключити діод** (будь ласка, використовуйте FR107, що постачається з системою) для зняття самоіндукції електрорушійної сили під час підключення на місці для застосування системи управління доступом.
13. Рекомендується використовувати окремі джерела живлення для електронного замка та панелі управління.
14. Для живлення панелі управління рекомендується використовувати блок живлення, що постачається в комплекті з системою.
15. У місцях зі значними магнітними перешкодами рекомендується використовувати оцинковані сталеві труби або екрановані кабелі, а також належне заземлення.

2 Введення у систему

Система управління доступом - це нова модернізована система управління безпекою, яка є ефективним засобом управління безпекою та захистом. Вона в основному використовується для управління входами і виходами в місцях з високим рівнем захисту, таких як банки, готелі, технічні приміщення, офіси, розумні спільноти і заводи.

2.1 Функціональні параметри системи

- Високошвидкісний 32-розрядний 1,0 ГГц процесор і 64 Мб оперативної пам'яті.
- Вбудована операційна система LINUX.
- Дводверні односторонні/двосторонні.
- Кількість користувачів: 30 000.
- Максимально 30 000 власників карток.
- 200 000 записів подій в автономному режимі.
- Використовуйте комунікаційні технології Ethernet для надійного зв'язку.
- Панель управління з вбудованим сторожовим таймером (апаратним) для запобігання збою.
- Захист від перевантаження по струму, перенапруги та зворотної напруги на вході джерела живлення до панелі управління.
- Захист від перевантаження по струму для живлення зчитувачів карток.
- Миттєвий захист від перенапруги для всіх вхідних/вихідних портів.
- Миттєвий захист від перенапруги для комунікаційних портів.

2.2 Технічні параметри продукту

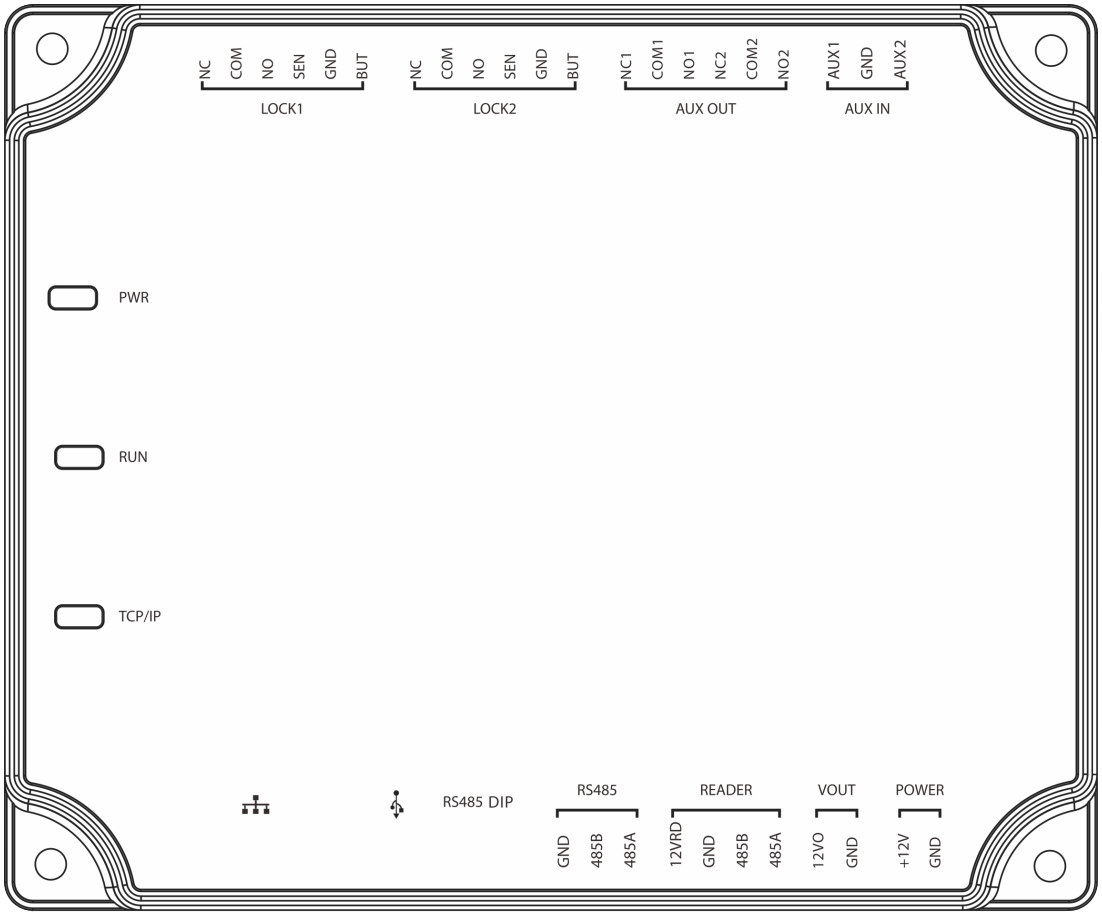
- Робоче джерело живлення: Номінальна напруга 12 В (±20%) постійного струму, номінальний струм ≥ 3A
- Робоче середовище: Температура від -10°C до 50°C; вологість від 20% до 80%.
- Вихід реле електронного замка: Максимальна напруга перемикання 36В (DC); Максимальний струм перемикання - 5A.
- Допоміжний релейний вихід: Максимальна напруга перемикання - 36 В (DC); Максимальний струм перемикання - 2 А.
- Знімні з'єднувальні клеми виготовлені з легованої сталі з немагнітними фланцевими матеріалами.
- Розміри панелі управління: 116.5 мм * 96.5 мм * 31.3 мм

2.3 Індикатори панелі керування

Коли C2-260 увімкнено, зазвичай індикатор POWER (червоний) горить постійно, індикатор RUN (зелений) повільно блимає (вказуючи на нормальний стан системи), а всі інші індикатори вимкнені.

Індикатор COMM (жовтий): Блимає, коли система обмінюється даними з іншими пристроями (наприклад, ПК). Коли індикатор блимає безперервно, це означає, що відбувається передача даних. Повільне блимання індикатора вказує на стан моніторингу в режимі реального часу.

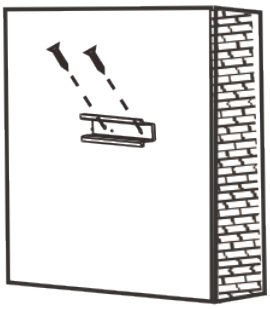
Діаграма індикаторів:

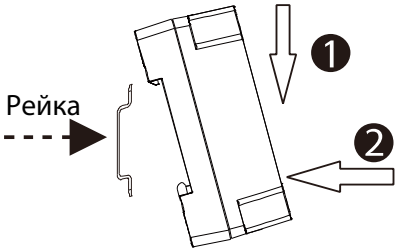


3 Установка та підключення

3.1 Процедура установки

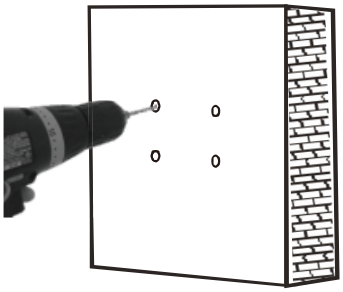
- Нижче описано процес встановлення рейок.

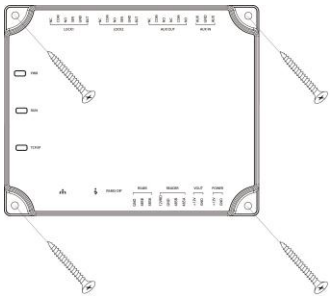




1) Закріпіть рейку на стіні ⋯▶ 2) Закріпіть пристрій на рейці.

- Нижче описано процес настінного монтажу.





1) Просвердліть отвори на стіні ⋯▶ 2) Закріпіть пристрій чотирма гвинтами

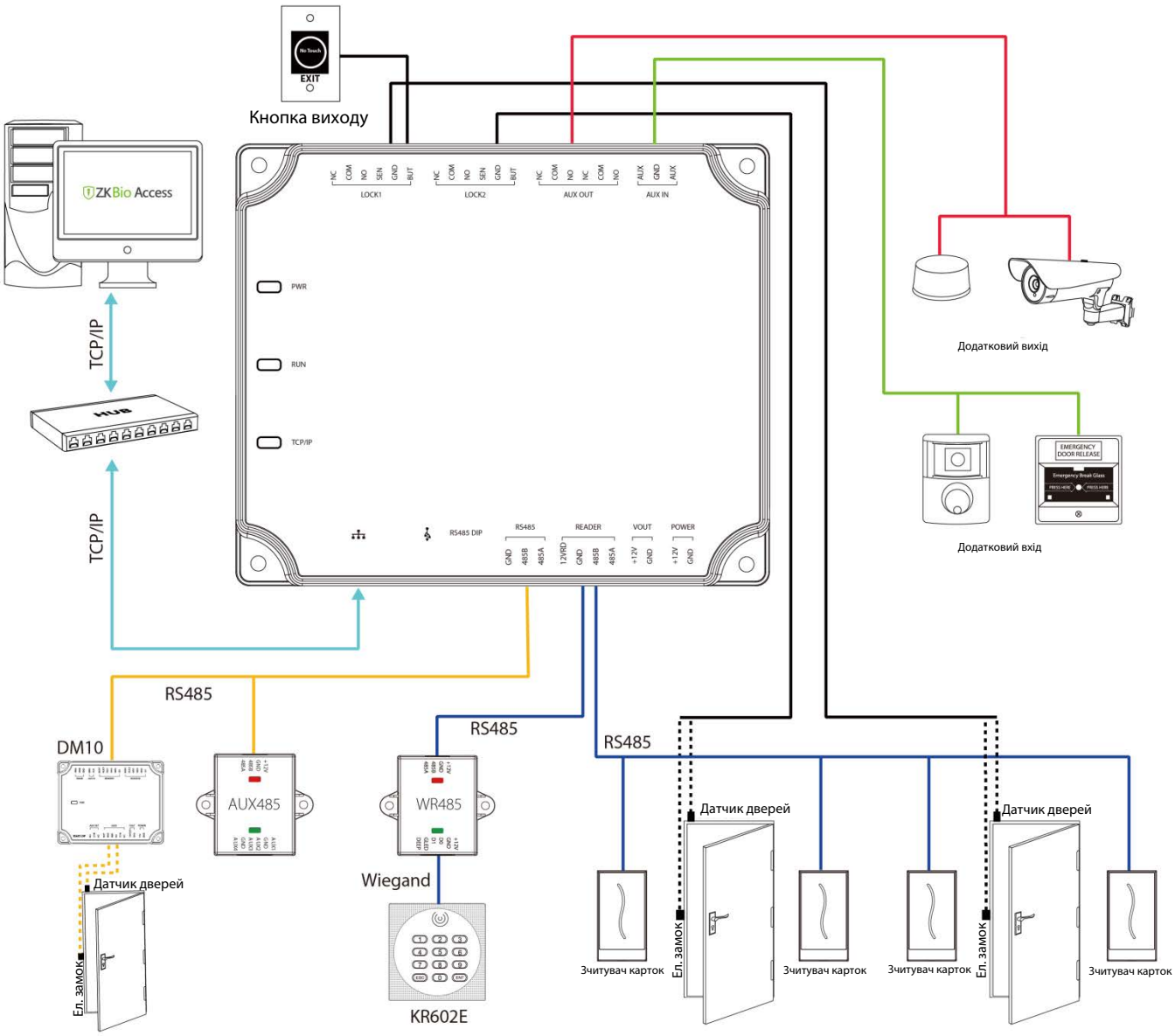
3.2 Монтаж дротів панелі управління доступом

Схема монтажу проводів панелі управління доступом

Примітки:

- Перед підключенням проводів переконайтеся, що джерело живлення відключено, інакше це може призвести до серйозних пошкоджень обладнання.
- Дроти системи управління доступом повинні бути розділені відповідно до сильного та слабкого струму; дроти панелі управління, дроти електронного замка та кнопки виходу повинні проходити через труби корпусу відповідно.

3.3 Встановлення системи панелі управління



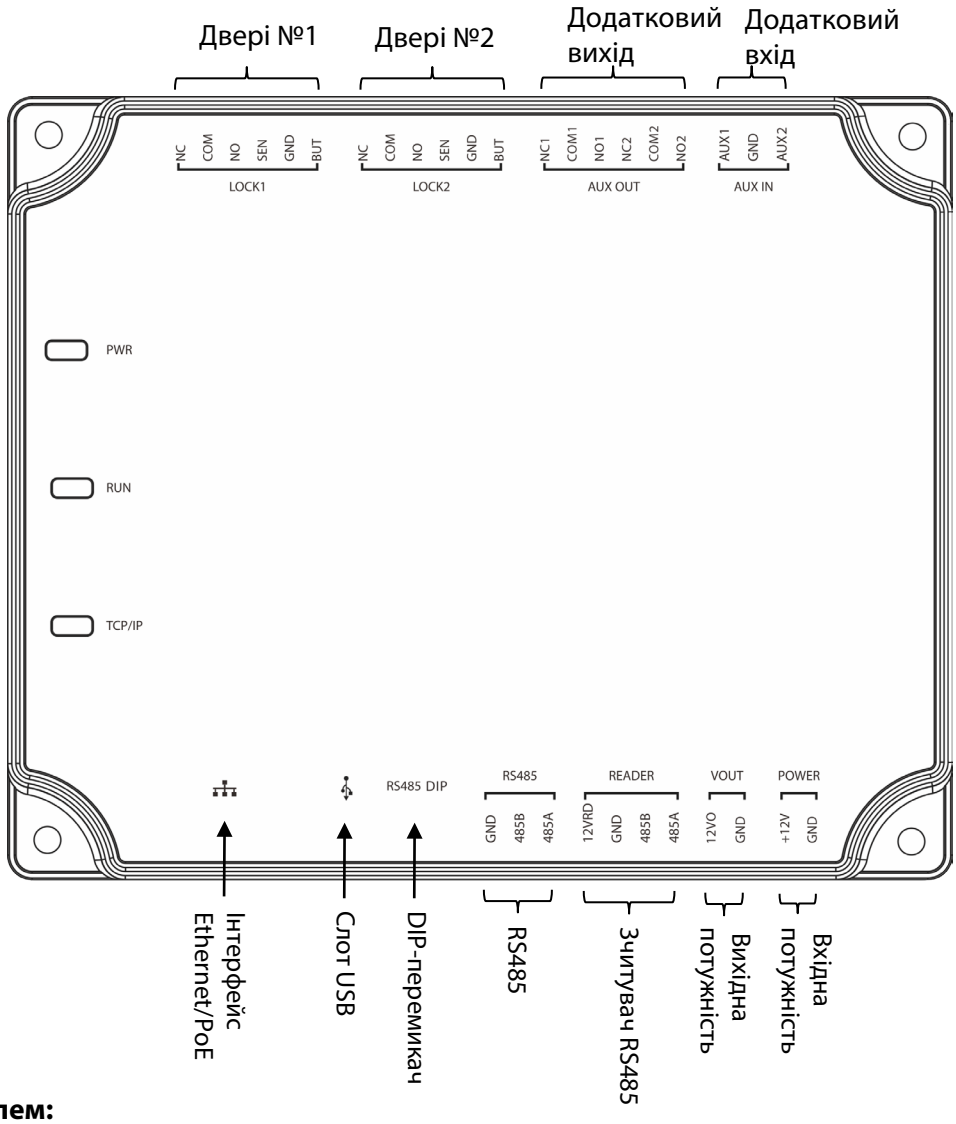
Схематична діаграма встановлення системи

Система управління доступом складається з двох частин: Робоча станція керування (ПК) та панель управління. Робоча станція керування та панель управління обмінюються даними через мережу TCP/IP та RS485. Дроти зв'язку слід прокладати якомога далі від високовольтних проводів і не можна прокладати паралельно з дротами живлення або в одному пучку з ними.

Робоча станція керування - це комп'ютер, підключений до мережі. За допомогою встановленого на ПК програмного забезпечення для управління доступом персонал може віддалено виконувати різні функції управління, такі як додавання/видалення користувачів, перегляд записів подій, відчинення/зачинення дверей та моніторинг стану кожної двері в режимі реального часу.

3.4 Підключення клем панелі управління

C2-260 Схема підключення клем



- **Опис клем:**

1. До додаткового входу можна підключити інфрачервоні детектори тіла, пожежну сигналізацію або детектори диму.
2. До додаткового виходу можна підключити сигналізації, камери, дверні дзвінки тощо.
3. PC RS485 означає, що кабель RS485 підключений до DM10/AUX485 через цей порт. До порту зчитувача RS485 можна підключити зовнішній зчитувач RS485.
4. **Відновлення заводських налаштувань**: За замовчуванням DIP-перемикач №4 вимкнений. Якщо тричі протягом 5 секунд переключити його вгору-вниз протягом 5 секунд і, в кінці, повернути у ВВІМКНЕНЕ положення, після перезавантаження панелі управління доступом будуть відновлені заводські налаштування, а IP-адреса буде відновлена до значення за замовчуванням (192.168.1.201).
5. Вищевказані клеми налаштовуються за допомогою відповідного програмного забезпечення системи управління доступом. Будь ласка, зверніться до інструкції відповідного програмного забезпечення для отримання більш детальної інформації.

Порти панелі керування C2-260:

Номер	Функціональний порт	C2-260 (Дводверні двосторонні)
1	**Кнопка виходу**	2
2	**Реле блокування управління**	2
3	**Датчик дверей**	2
4	**Додатковий вхід**	2
5	**Додатковий вихід**	2
6	**Зчитувач RS485**	4
7	**Зв'язок з розширенням RS485**	✓
8	**TCP/IP**	✓

3.5 З'єднання з дверними датчиками, вимикачами виходу, додатковими пристроями вводу та зв'язком розширення RS485

1. Датчик дверей

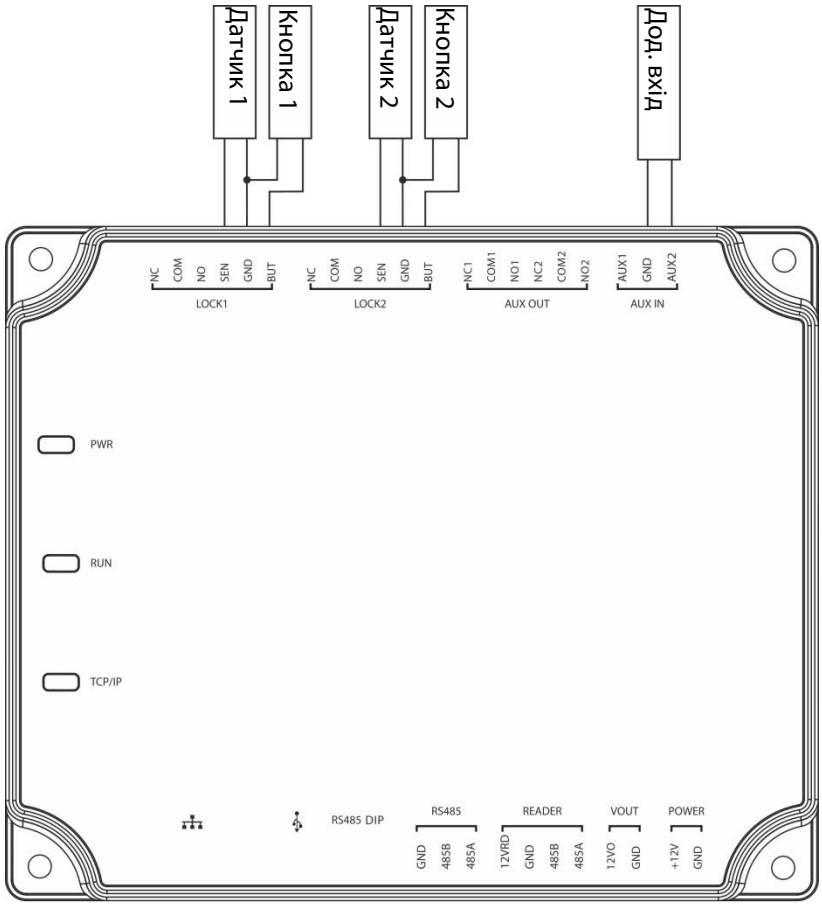
Датчик дверей використовується для визначення стану відчинення/зачинення дверей. За допомогою перемикача дверного датчика панель управління доступом може виявити несанкціоноване відчинення дверей і увімкнути тривогу. Крім того, якщо двері не зачиняються протягом певного часу після відчинення, панель управління також здійме тривогу. Рекомендується використовувати двожильні дроти перерізом понад 0,22 мм2. Датчик дверей можна не встановлювати, якщо немає необхідності контролювати стан відчинених/зачинених дверей, здіймати тривогу, якщо двері не зачинені тривалий час, контролювати наявність несанкціонованого доступу, а також використовувати функцію блокування.

2. Вимикач виходу

Вимикач виходу - це вимикач, встановлений всередині приміщення для відчинення дверей. Коли він увімкнений, двері відчиняються. Кнопка виходу кріпиться на висоті близько 1,4 м над землею. Переконайтеся, що вона розташована в правильному положенні без нахилу, а її з'єднання правильне і надійне. (Відріжте оголений кінець будь-якого невикористаного дроту та обмотайте його ізоляційною стрічкою). Переконайтеся, що немає електромагнітних перешкод (наприклад, вимикачів світла та комп'ютерів). Рекомендується використовувати двожильні дроти перерізом понад 0,3 мм2 як з'єднувальний провід між вимикачем виходу та панеллю управління.

3. Допоміжний вхід

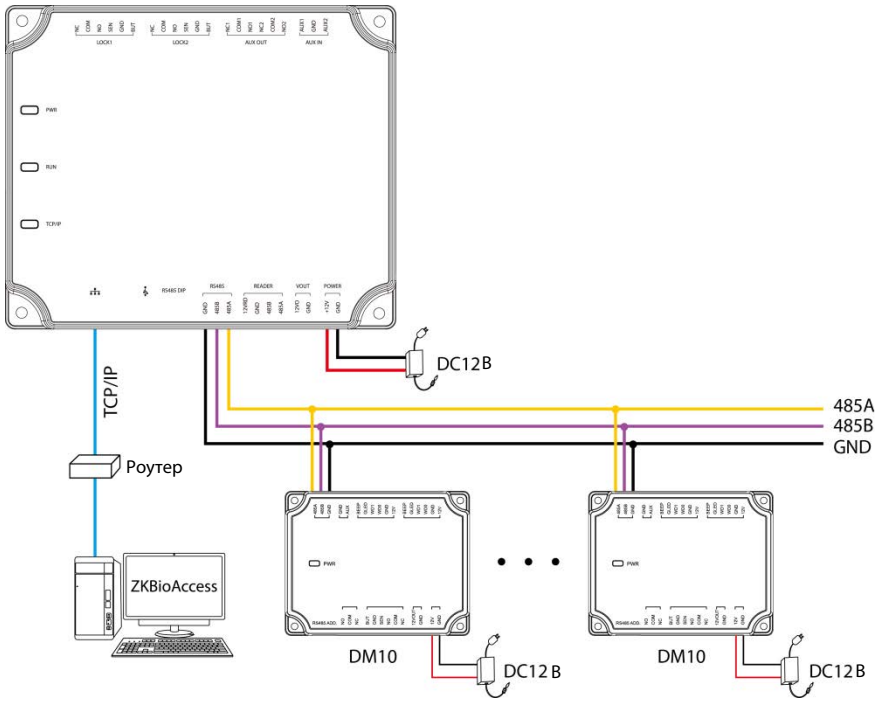
Панель управління має один допоміжний вхідний інтерфейс, до якого можуть підключатися інфрачервоні детектори тіла, детектори диму, детектори газу, віконні магнітні сигналізатори, бездротові вимикачі виходу тощо. Допоміжні входи налаштовуються за допомогою відповідного програмного забезпечення для управління доступом. Будь ласка, зверніться до посібника з відповідного програмного забезпечення для отримання більш детальної інформації.



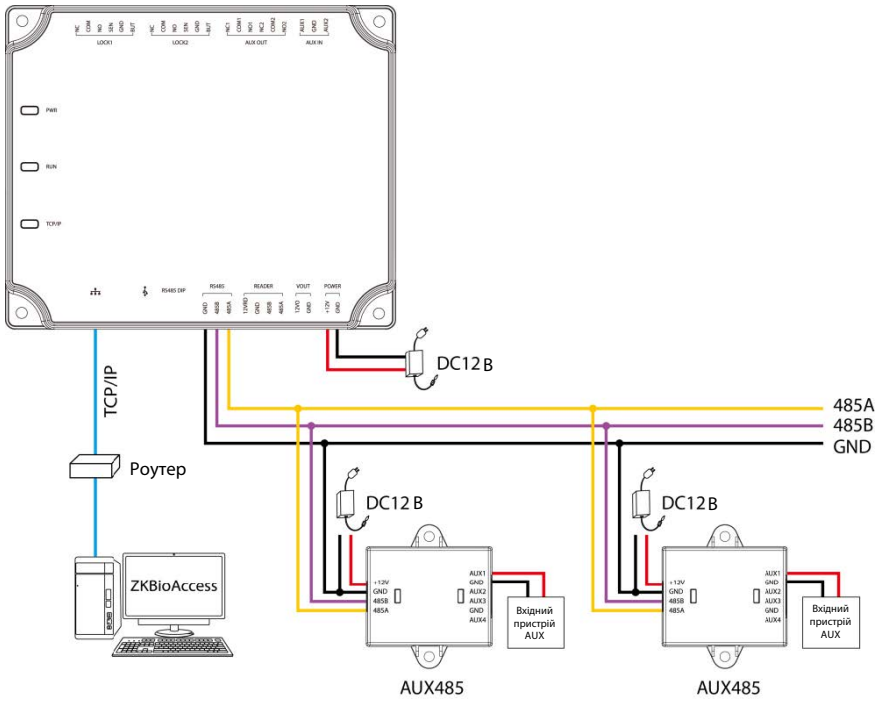
З'єднання між панеллю управління і дверними датчиками, вимикачами виходу та допоміжними вхідними пристроями

4. Зв'язок з розширенням RS485

Панель управління підтримує великі модулі, такі як **DM10** і **AUX485**, через RS485. До C2-260 можна підключити максимум вісім DM10 або максимум два AUX485. Як показано на наступному малюнку.



Підключення до DM10 через RS485



Підключення до AUX485 через RS485

Примітка:

1. До C2-260 можна підключити максимум вісім модулів DM10 або два модулі AUX485.
2. До кожного модуля AUX485 можна підключити максимум чотири допоміжні пристрої.
3. Для кожного модуля DM10/AUX485 потрібне окреме джерело живлення.

3.6 З'єднання зі зчитувачами RS485/Wiegand

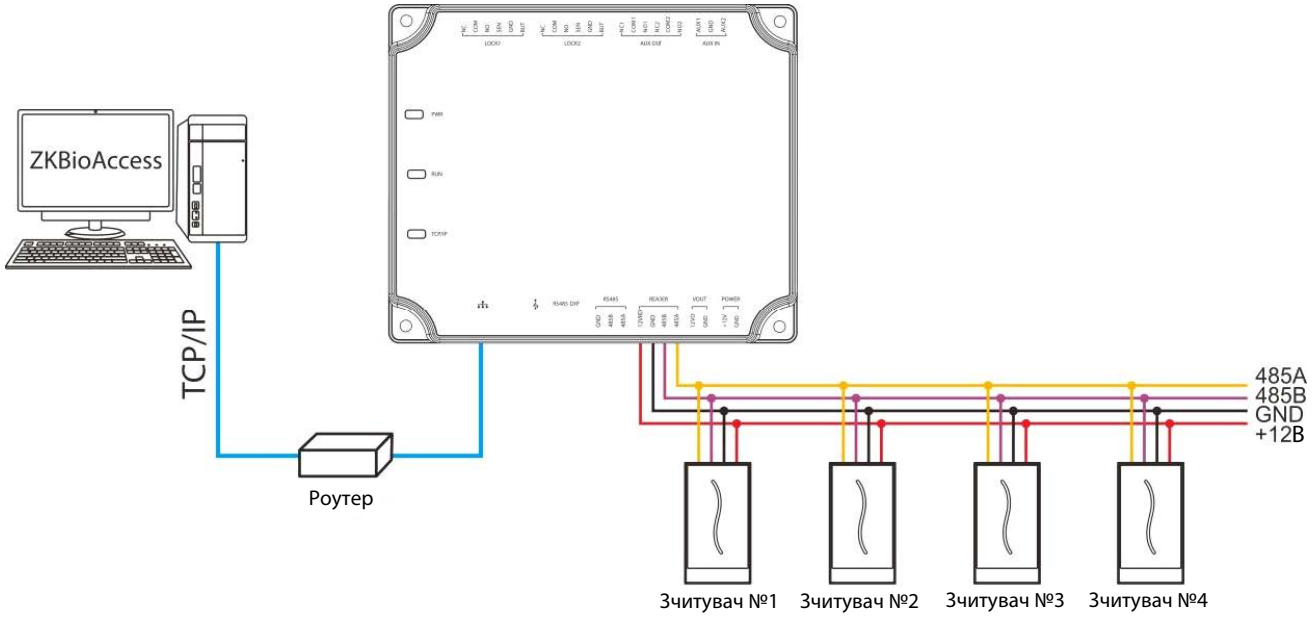
Панель управління підтримує зчитувач карт RS485. А також підтримує зчитувач Wiegand через **WR485.**

- **З'єднання зі зчитувачами RS485**

Панель управління підтримує чотири зчитувачі, які можуть бути підключені в двосторонньому режимі.

Підключення зчитувача RS485: Встановіть адресу RS485 (номер пристрою) зчитувача за допомогою DIP-перемикача або іншим способом.

Адреса RS485 / Панель управління	1	2	3	4
C2-260	Двері1 (Вхід)	Двері1 (Вихід)	Двері2 (Вхід)	Двері2 (Вихід)



З'єднання між панеллю управління та зчитувачами карток RS485

Один зчитувач з інтерфейсом RS485 може подавати максимум 750 мА (12 В) струму. Отже, загальний струм споживання повинен бути меншим за це максимальне значення, коли зчитувачі ділять живлення з панеллю. Для розрахунку, будь ласка, використовуйте максимальний струм зчитувача, а пусковий струм зазвичай більш ніж удвічі перевищує стандартний робочий струм.

На прикладі зчитувача карток KR502M-RS струм у режимі очікування становить менше 80 мА, а максимальний струм - менше 90 мА. При запуску пристрою миттєвий струм може досягати 180 мА. Для зчитувача RS485, враховуючи, що пусковий струм великий, тільки чотири зчитувачі можуть підключатися до джерела живлення через інтерфейс зчитувача RS485. Отже, до живлення панелі управління можна підключити лише 2 зчитувачі.

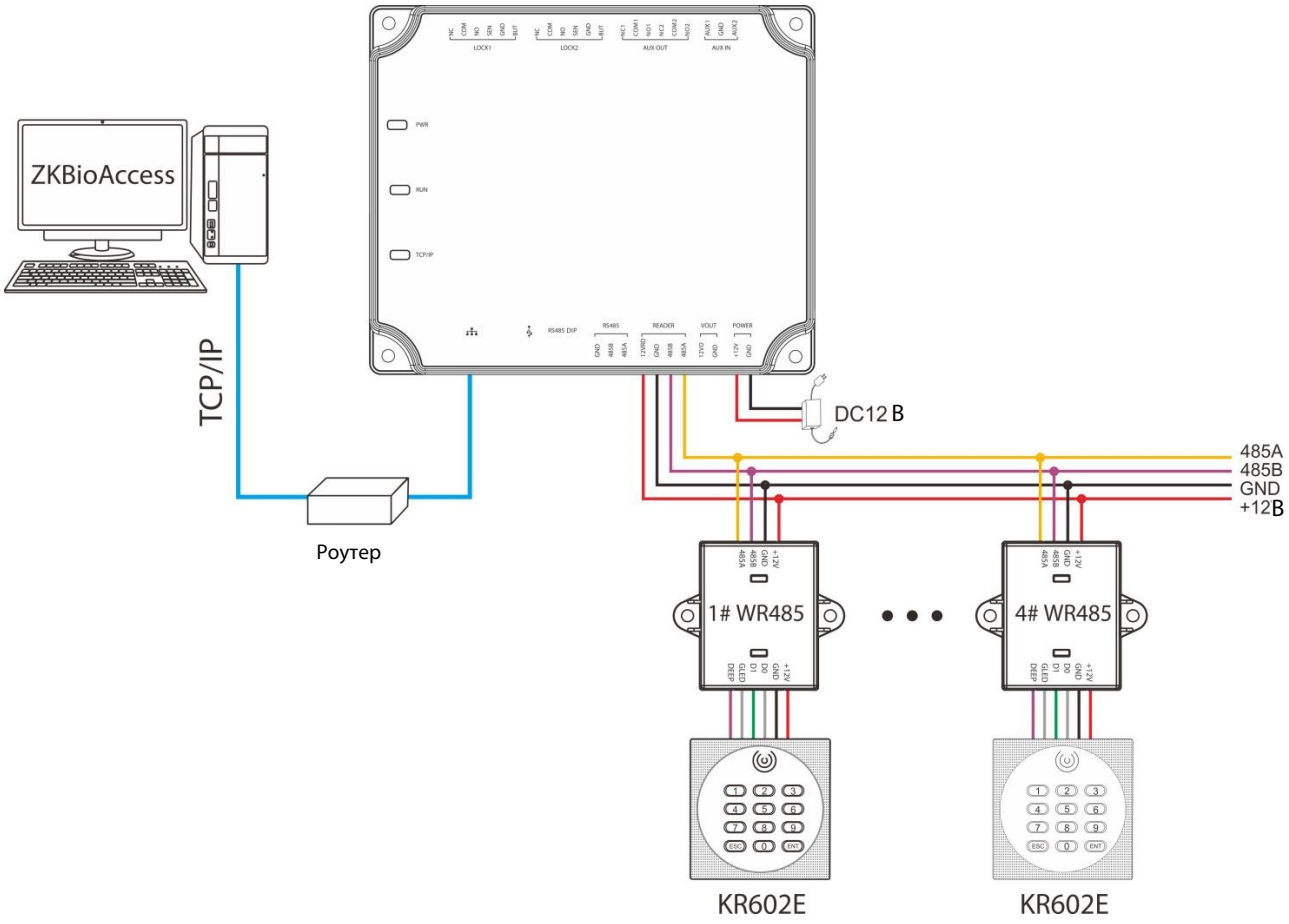
Якщо зчитувач RS485 підключений ззовні і має спільне джерело живлення з пристроєм, рекомендується, щоб відстань між портом зчитувача RS485 і зчитувачем не перевищувала 100 м.

В іншому випадку рекомендується використовувати окреме джерело живлення для зчитувача.

Для пристроїв, які споживають більше енергії, ми рекомендуємо використовувати різні блоки живлення для забезпечення стабільної роботи.

- **З'єднання зі зчитувачами Wiegand**

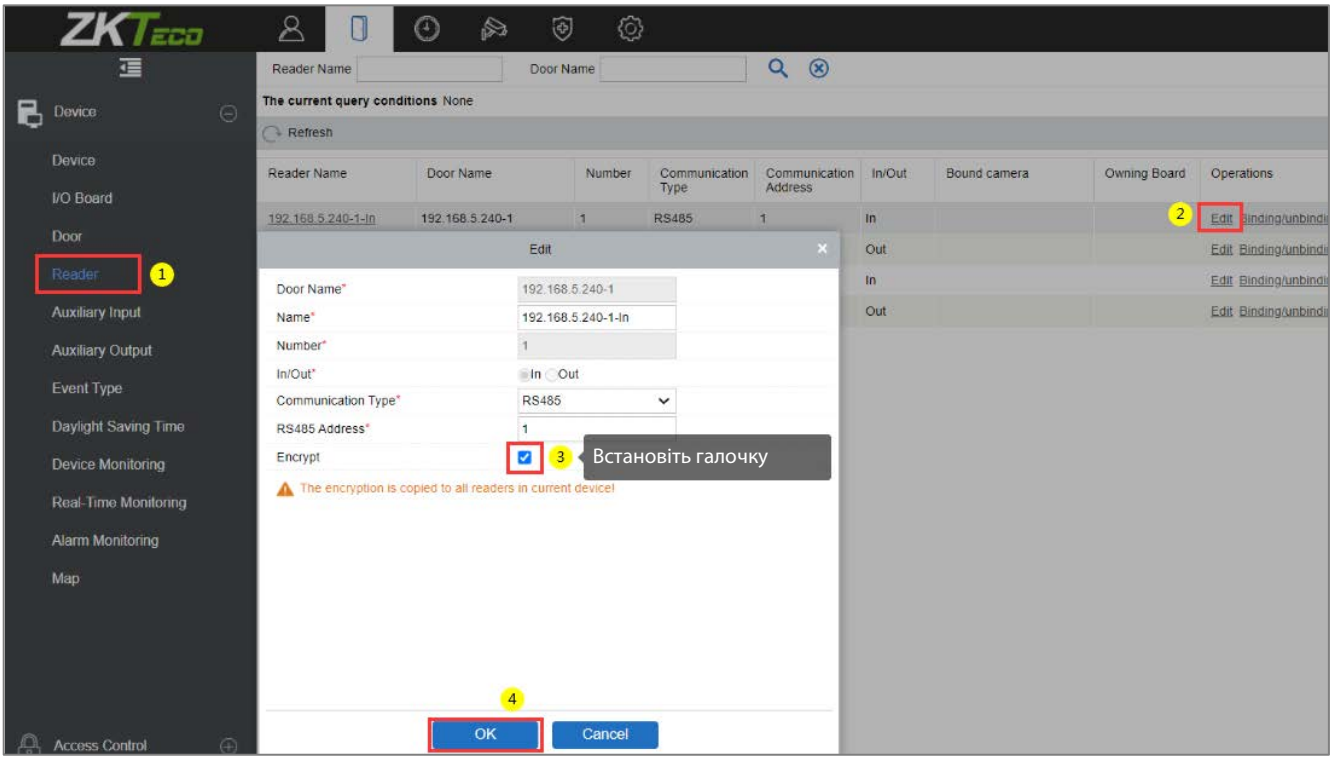
Панель управління підтримує підключення зчитувача Wiegand через модуль WR485. Підключення показано на малюнку нижче.



3'єднання між централлю та зчитувачами Wiegand через WR485

Примітки:

- До C2-260 можна підключити максимум чотири модулі WR485.
- Оскільки WR485 працює в режимі шифрування, після додавання панелі управління C2-260 до програмного забезпечення ZKBioAccess потрібно встановити опцію "**Encrypt**" (Шифрувати) для зчитувача Wiegand, щоб зчитувач Wiegand можна було використовувати у звичайному режимі. (Показано на наступному малюнку).
- Для більш детальної інформації та налаштувань параметрів див. Додаток 1.



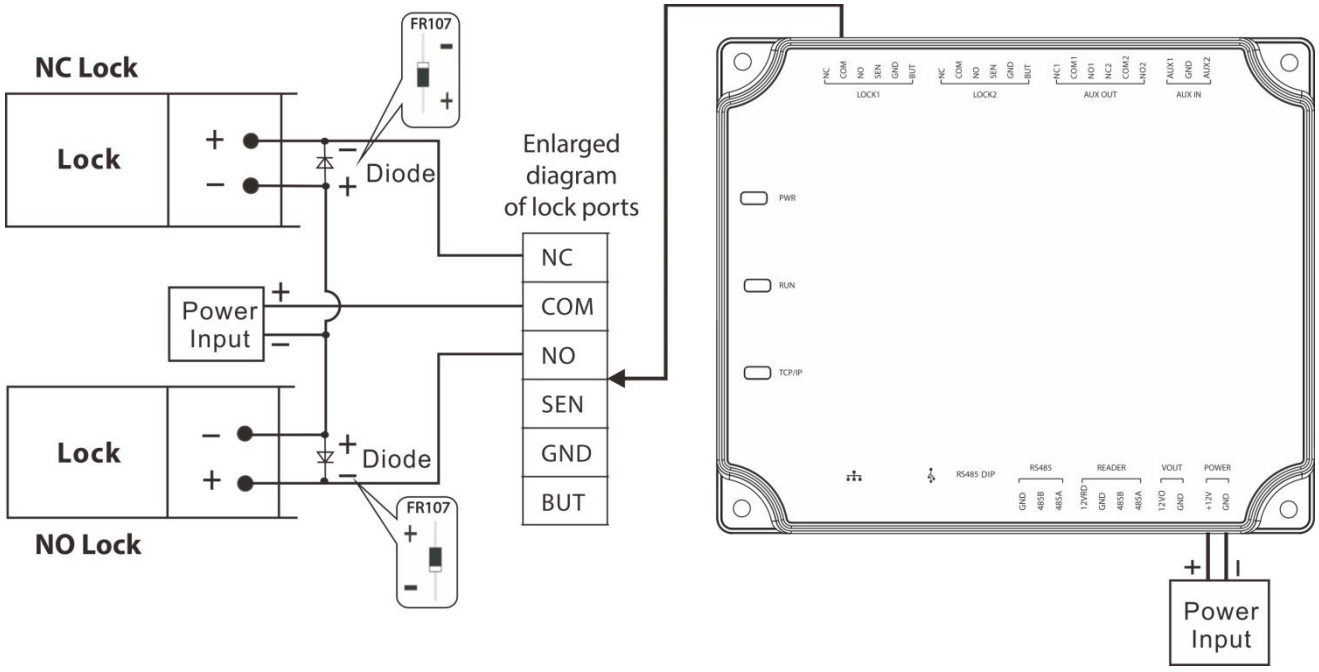
Щоб використовувати зчитувач Wiegand у звичайному режимі:

1. Натисніть **Reader** (Зчитувач) > **Edit** (Редагувати) і з'явиться вікно редагування.
2. Встановіть галочку біля **Encrypt** (Шифрування).
3. Натисніть **OK**, щоб зберегти.

3.7 Підключення релейного виходу

C2-260 має три реле (два за замовчуванням використовуються як керуючі замки, а третє - як допоміжні виходи). До реле допоміжних виходів можна підключити монітори, сигналізацію, дверні дзвінки тощо. Допоміжні виходи налаштовуються за допомогою відповідного програмного забезпечення для управління доступу. Будь ласка, зверніться до посібника з відповідного програмного забезпечення для отримання детальної інформації.

1. За замовчуванням режим підключення дверного замка - "сухий режим". Як правило, електронний замок використовує зовнішнє джерело живлення окремо. Режим підключення реле дверного замка не може бути змінений, за винятком допоміжного вихідного реле. На схемі нижче на прикладі підключення дверного замка показано підключення вихідного реле.
2. Панель управління доступу має кілька виходів для електронних замків. Клеми COM і NO використовуються для замків, які розблоковуються при підключенні живлення і блокуються при відключенні живлення. Клеми COM і NC використовуються для замків, які блокуються при підключенні живлення і розблоковуються при відключенні живлення.
3. Наша панель управління доступу живиться від стандартного PoE або живлення від системи управління доступом. Ви можете вибрати одне з цих джерел живлення за потреби. Обидва блоки живлення забезпечують живлення 12В/3А лише для живлення панелі управління, зчитувачів Wiegand і вихідної потужності зчитувача RS485.
4. Для захисту системи управління доступом від самоіндукованої електрорушійної сили, що генерується електронним замком в момент вимкнення/ввімкнення, необхідно паралельно з електронним замком підключити діод (будь ласка, використовуйте FR107, що постачається з системою) для зняття самоіндукованої електрорушійної сили під час підключення на місці для застосування системи управління доступом.



Електрична схема підключення замка

4 Зв'язок з обладнанням

Програмне забезпечення фонового ПК може взаємодіяти з системою за двома протоколами (TCP/IP та RS485) для обміну даними та дистанційного керування.

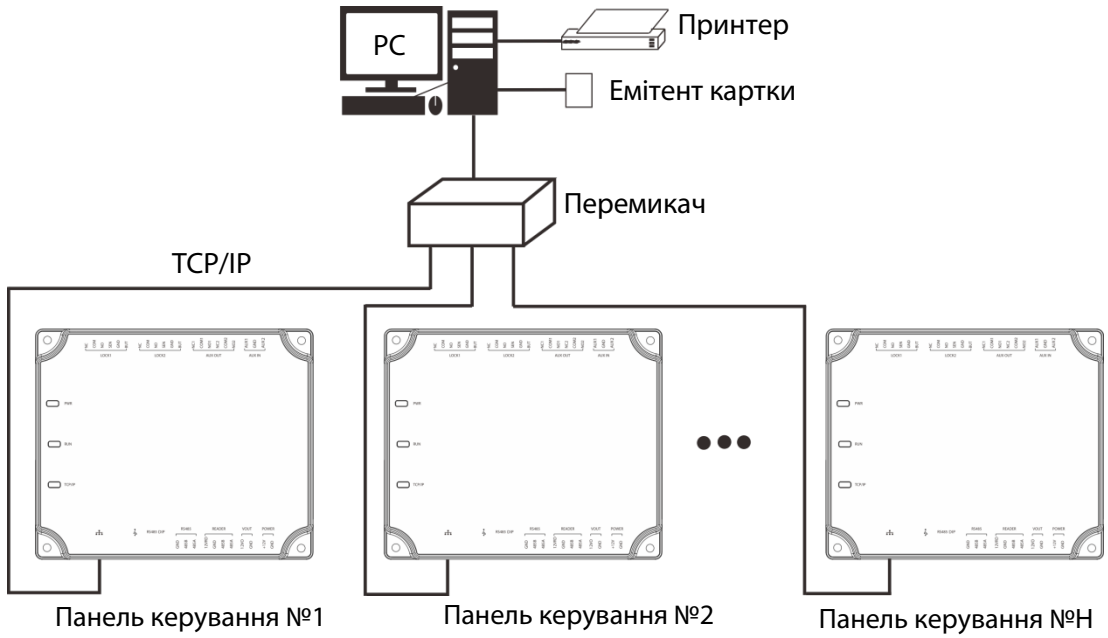
4.1 Мережеві дроти та проводка управління доступом

1. Живлення 12 В постійного струму, перетвореного з 220 В або PoE.
2. Оскільки електронний замок має великий струм, він генерує сильний сигнал перешкод під час роботи. Для зменшення такого ефекту рекомендується використовувати 4-х жильні дроти (RVVP 4Г-0,75мм2, два - для живлення, два - для датчика дверей).
3. В інтерфейсі RS485 використовуються 4-х жильні комунікаційні екрановані дроти (RVVSP 4*0,5мм2).
4. Інші кабелі керування (наприклад, вимикачі виходу) виготовлені з 2-жильних проводів (RVVSP 2Г-0,5мм2).
5. Вказівки по підключенню:
   - Сигнальні дроти (наприклад, мережеві кабелі) не можна прокладати паралельно або в одній обсадній трубі з потужними електричними дротами (наприклад, дротами електронних замків і силовими кабелями). Якщо з екологічних міркувань паралельне прокладання неминуче, відстань між ними має бути більше 50 см.
   - Намагайтеся уникати використання будь-якого провідника з роз'ємом під час розподілу. Якщо з'єднувач необхідний, він повинен бути обтиснутим або звареним. До з'єднання або відгалуження провідників не можна застосовувати механічну силу.
   - У будівлі розподільчі лінії повинні бути встановлені горизонтально або вертикально. Вони повинні бути захищені обсадними трубами (наприклад, пластиковими або залізними водопровідними трубами, які слід вибирати відповідно до технічних вимог внутрішньої розводки). Металеві шланги можна використовувати для стельової проводки, але вони повинні бути надійними і мати гарний вигляд.
   - Заходи екранування та екрануюче з'єднання: Якщо електромагнітні перешкоди в середовищі електропроводки виявляються значними під час обстеження перед будівництвом, необхідно розглянути питання екранування кабелів передачі даних під час проектування будівельної схеми. Загалом, екранний захист необхідний, якщо на будівельному майданчику є велике джерело радіоактивних перешкод або проводка повинна бути паралельною з джерелом живлення великого струму. Як правило, заходи екранування включають дотримання максимальної відстані від будь-якого джерела перешкод, а також використання металевих кабельних коробів або оцинкованих металевих водопровідних труб для забезпечення надійного заземлення з'єднання між екрануючими шарами кабелів передачі даних і металевими коробами або трубами. Зазначимо, що екрануючий корпус може мати екрануючий ефект лише тоді, коли він надійно заземлений.
   - Спосіб підключення заземлення: На місці прокладання проводки необхідні надійні дроти заземлення великого діаметру, що відповідають чинним національним стандартам, і повинні бути з'єднані у вигляді дерева, щоб уникнути утворення петлі постійного струму. Ці дроти заземлення повинні знаходитися далеко від грозових полів. Жоден блискавковідвід не може слугувати заземлювачем і гарантувати відсутність струму блискавки через будь-який заземлювач під час удару блискавки. Металеві жолоби та труби електропроводки повинні

бути безперервно та надійно з'єднані з заземлювачами за допомогою кабелів великого діаметру. Імпеданс цієї ділянки дроту не повинен перевищувати 2 Ом. Крім того, екрануючий шар повинен бути надійно з'єднаний і заземлений з одного кінця, щоб гарантувати рівномірний напрямок струму. Дріт заземлення екрануючого шару повинен бути підключений через провід великого діаметру (не менше 2,5 мм2).

4.2 TCP/IP зв'язок

Перехресний кабель Ethernet 10/100Base-T, тип перехресного мережевого кабелю, в основному використовується для каскадних концентраторів і комутаторів або для прямого з'єднання двох кінцевих точок Ethernet (без концентратора). Підтримуються як 10Base-T, так і 100Base-T.



Комунікаційна система TCP/IP

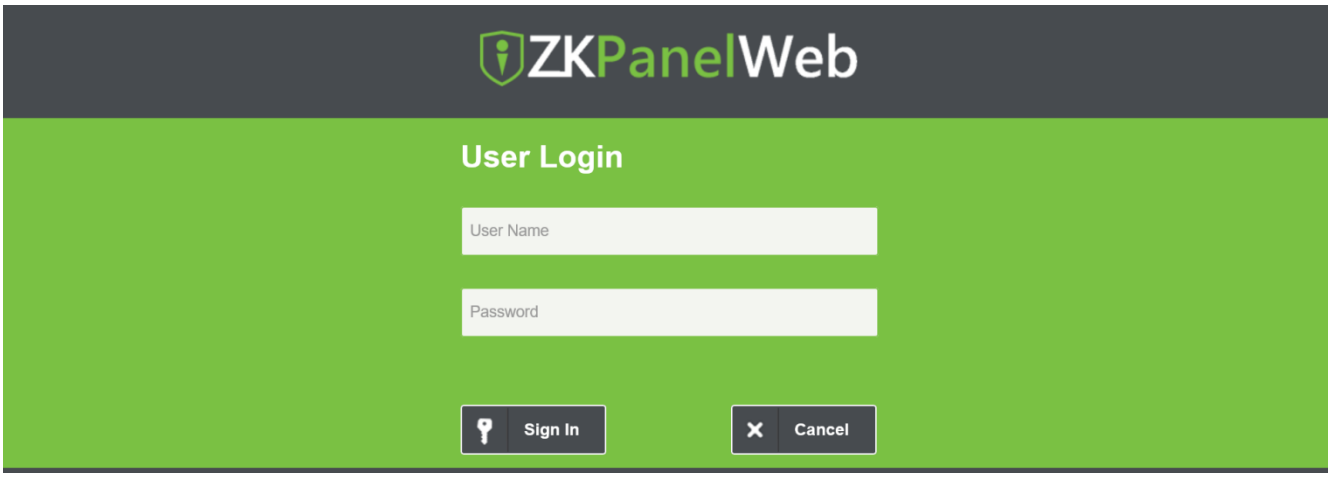
У програмі Access: Натисніть **Device** (Пристрій) > **Search Device** (Пошук пристрою), щоб знайти контролери доступу в мережі, і безпосередньо додайте з результату пошуку.

4.3 ZKPanelWeb

Ця вбудована функція нещодавно додана, щоб допомогти користувачеві зручніше керувати контролерами. Користувачі можуть використовувати функцію веб-сервера для виконання таких операцій, як конфігурація мережі, конфігурація push-зв'язку, синхронізація часу та управління обліковими записами користувачів.

- **Увійдіть на веб-сервер**

Створіть дійсний рядок з'єднання за допомогою TCP/IP.
Введіть IP-адресу контролера (за замовчуванням 192.168.1.201) в адресний рядок; введіть ім'я користувача та пароль (обидва - **admin**) і натисніть **[Sign in]** (Увійти), щоб отримати доступ до ZKPanelWeb.

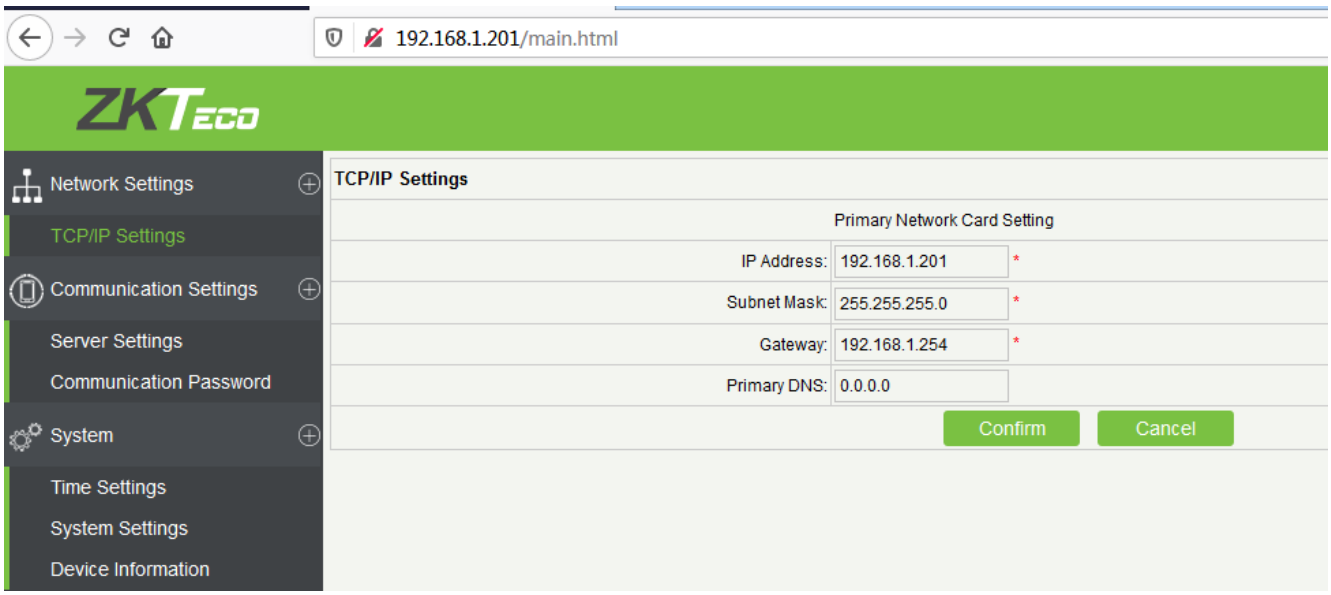


Примітка:

1. IP-адреси сервера (ПК) і контролера повинні знаходитися в одному сегменті мережі.
2. IP-адресу контролера можна знайти за допомогою пошуку пристроїв за допомогою програми BioSecurity ([**Access**] (Доступ) > [**Access Device**] (Пристрій доступу) > [**Device**] (Пристрій) > [**Search Device**] (Пошук пристрою)).

- **Налаштування TCP/IP**

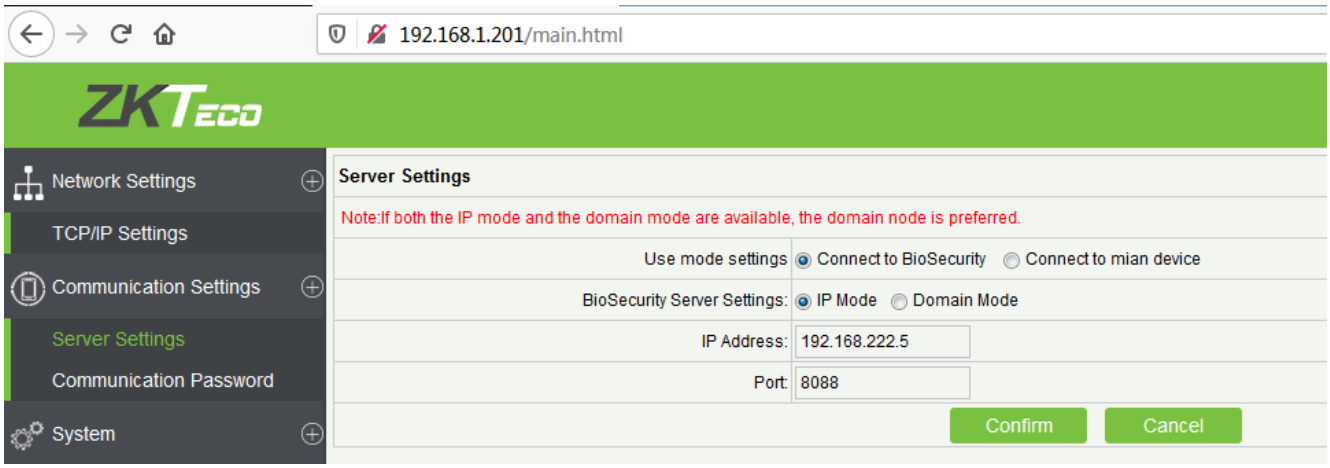
Натисніть **[TCP/IP Settings**] (Налаштування TCP/IP), щоб змінити IP-адресу та адресу шлюзу.



- **Налаштування зв'язку**

Налаштуйте параметри зв'язку в ZKPanelWeb і підключіть контролер до сервера (ПК); контролер буде автоматично передавати інформацію на сервер.

1) Налаштування сервера

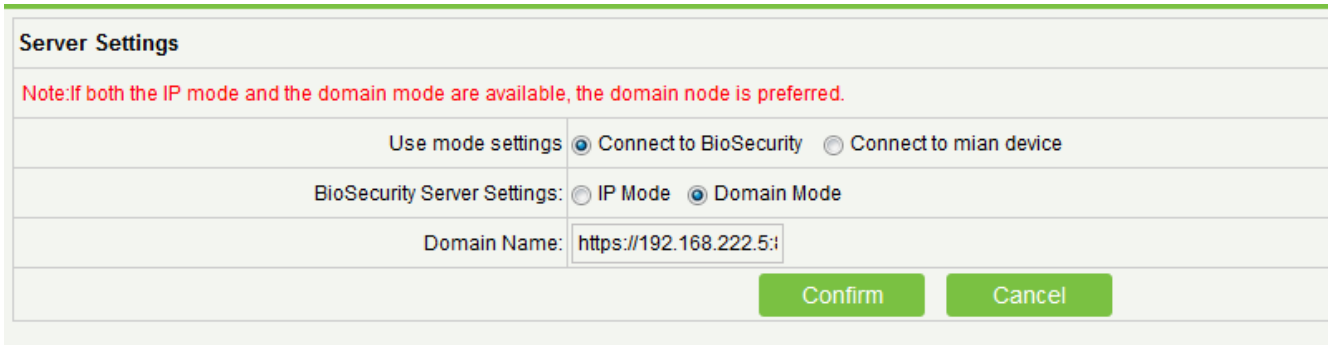


Використовуйте налаштування режиму: Режим за замовчуванням - Підключитися до BioSecurity.

Налаштування сервера BioSecurity: Для встановлення параметрів режиму IP та режиму домену.

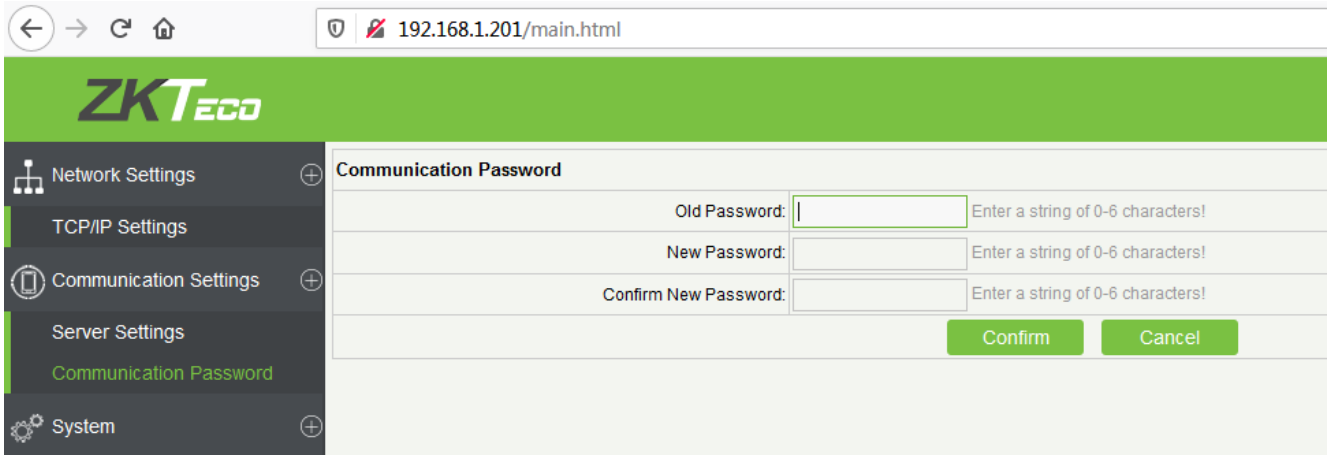
Режим IP: За замовчуванням IP-адреса сервера - 0.0.0.0, і ви можете змінити її відповідно до практичної ситуації.

Порт: Порт за замовчуванням - 8088, і ви можете змінити його відповідно до практичної ситуації.



Режим домену: Значення за замовчуванням дорівнює нулю, але ви можете змінити його значення. Якщо користувач хоче увійти до програмного забезпечення BioSecurity через HTTPS, то тут потрібно вказати доменне ім'я. Формат має вигляд: https://192.168.222.5:8088.

2) Пароль для зв'язку

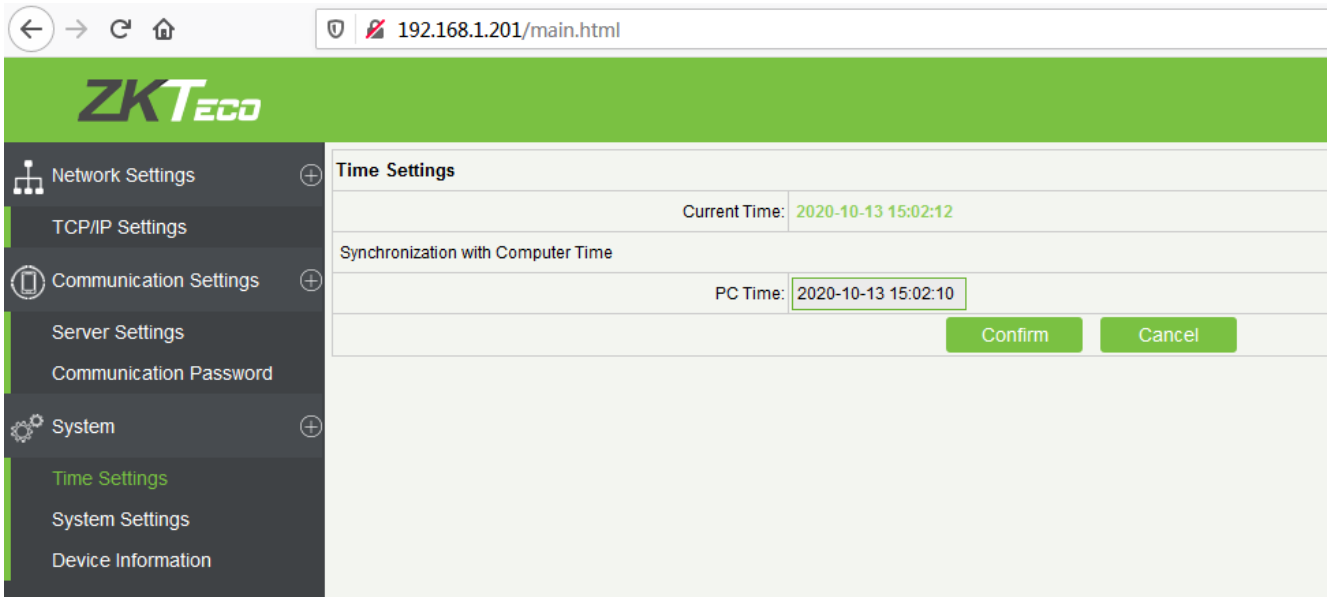


Пароль для зв'язку: вказує на те, що мережевий зв'язок зашифровано. Значення за замовчуванням дорівнює нулю, але ви можете змінити його значення.
Якщо ви налаштуєте пароль зв'язку тут, такий самий пароль зв'язку має бути налаштований на сервері, перш ніж можна буде встановити з'єднання.

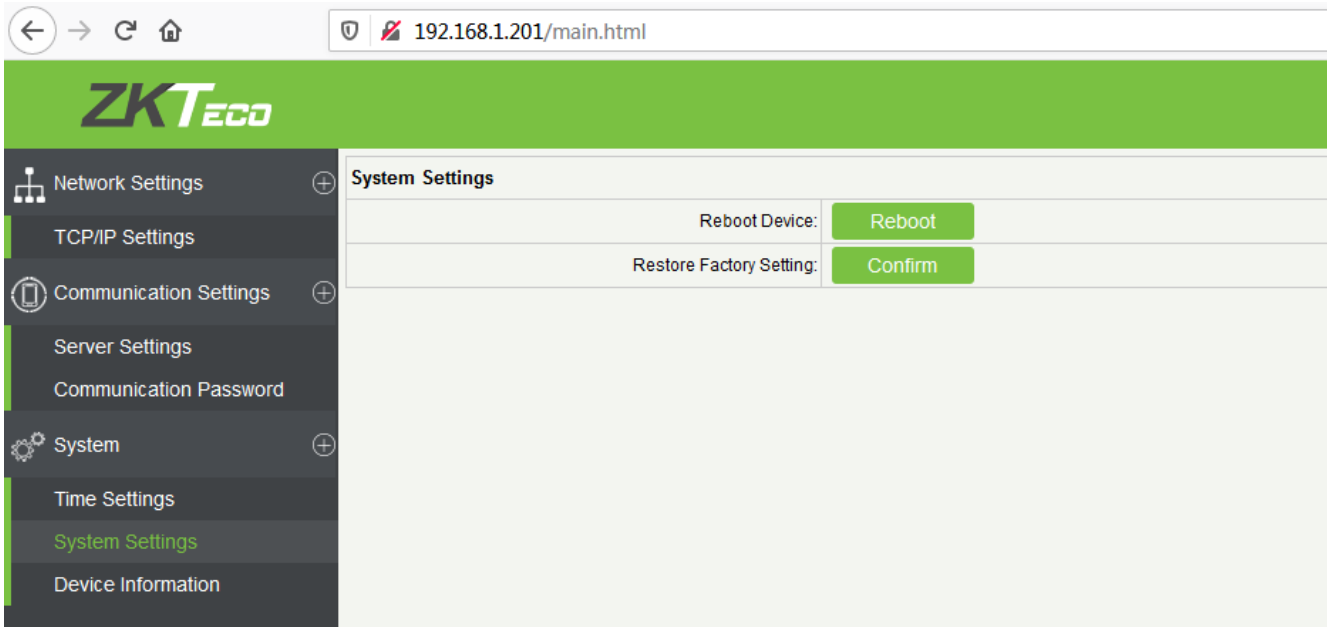
- **Система**

Тут користувач може синхронізувати час з комп'ютером, налаштувати систему та переглянути інформацію про пристрій.

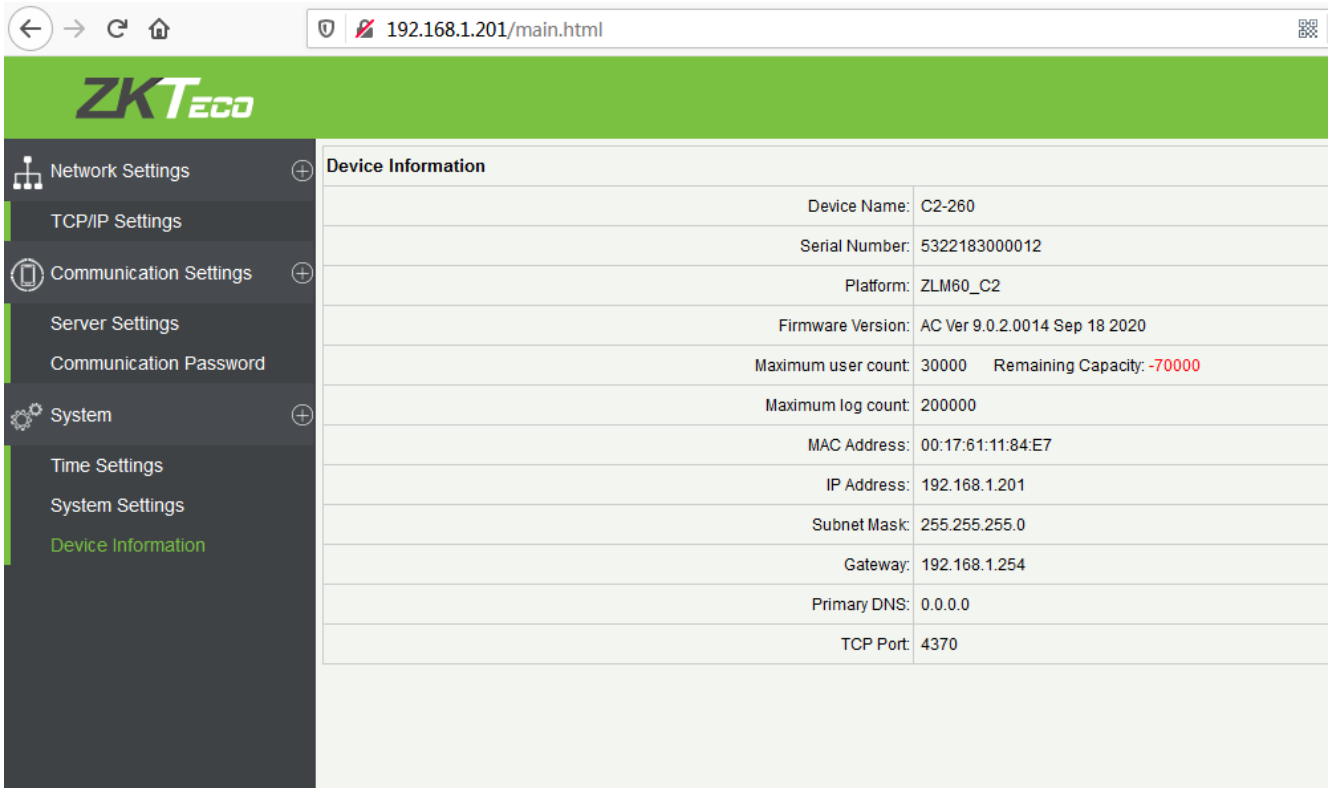
1) Налаштування часу



2) Налаштування системи



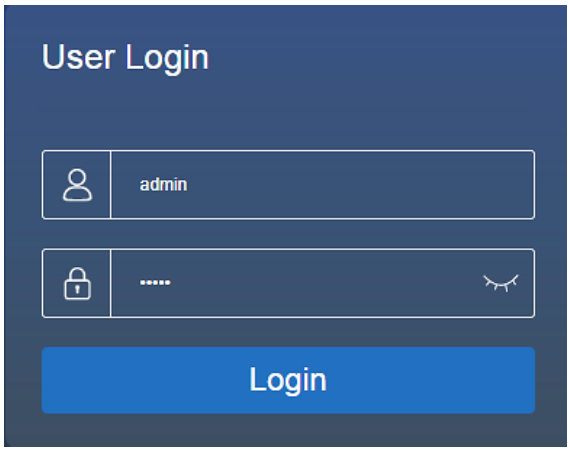
3) Інформація про пристрій



5 ZKBioAccess

Наступні розділи пояснюють функції програмного забезпечення ZKBioAccess після встановлення контролерів доступу.

5.1 Вхід в систему



Після встановлення програмного забезпечення двічі клацніть на іконку ZKBio Access , щоб відкрити програму. Ви також можете відкрити рекомендований браузер і ввести IP-адресу та порт сервера в адресний рядок. За замовчуванням IP-адресою є http://127.0.0.1:8098 .

Якщо програмне забезпечення не встановлено на вашому сервері, ви можете ввести IP-адресу та порт сервера в адресному рядку.

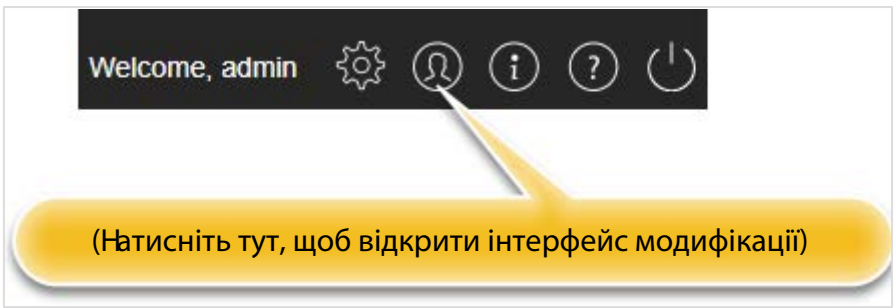
Примітка: Ім'я користувача суперкористувача - **admin**, пароль - **admin**, потім натисніть кнопку **Login** (Увійти). Після першого входу в систему вам потрібно скинути пароль.

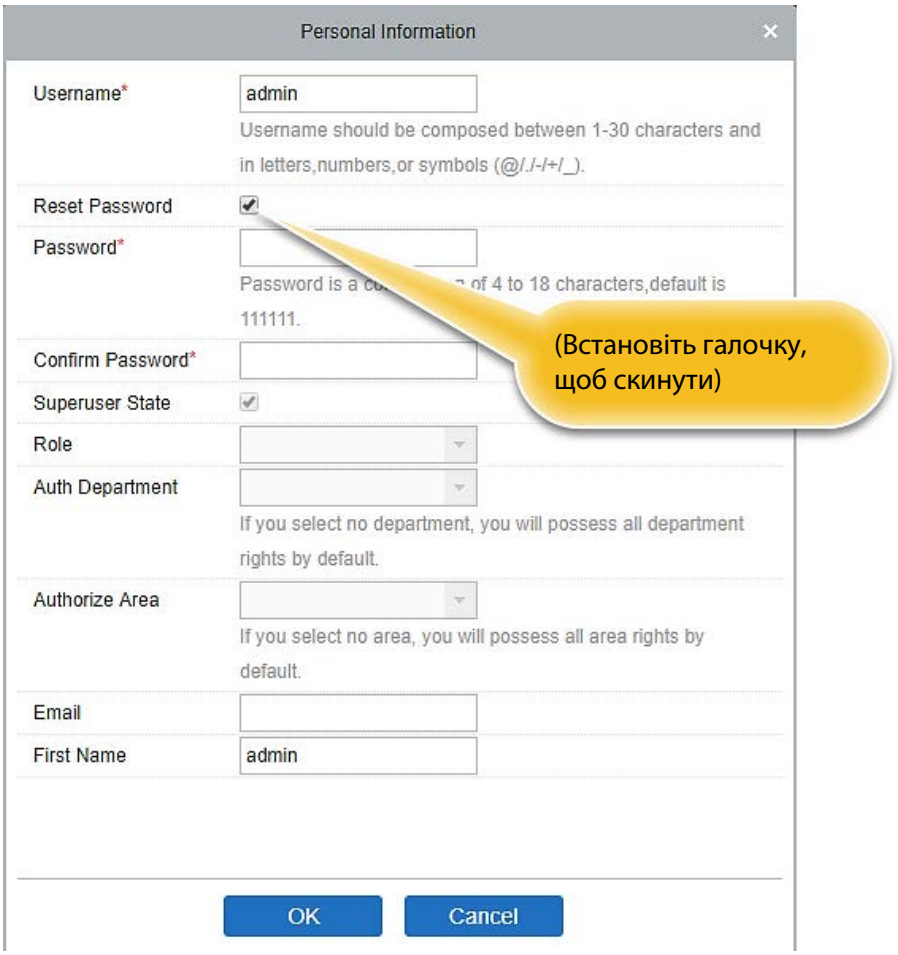
5.2 Активувати систему

Будь ласка, зверніться до відповідного документа про активацію ліцензії.

5.3 Змінити пароль

Ви можете змінити пароль для входу в систему в розділі "**Personal Information**" (Особиста інформація).





Встановіть галочку **Reset Password** (Скинути пароль), щоб змінити пароль.

Примітка: І суперкористувач, і новий користувач створюються суперкористувачем (пароль за замовчуванням для нових користувачів - 111111). Ім'я користувача не залежить від регістру, але пароль залежить від регістру.

5.4 Пристрій

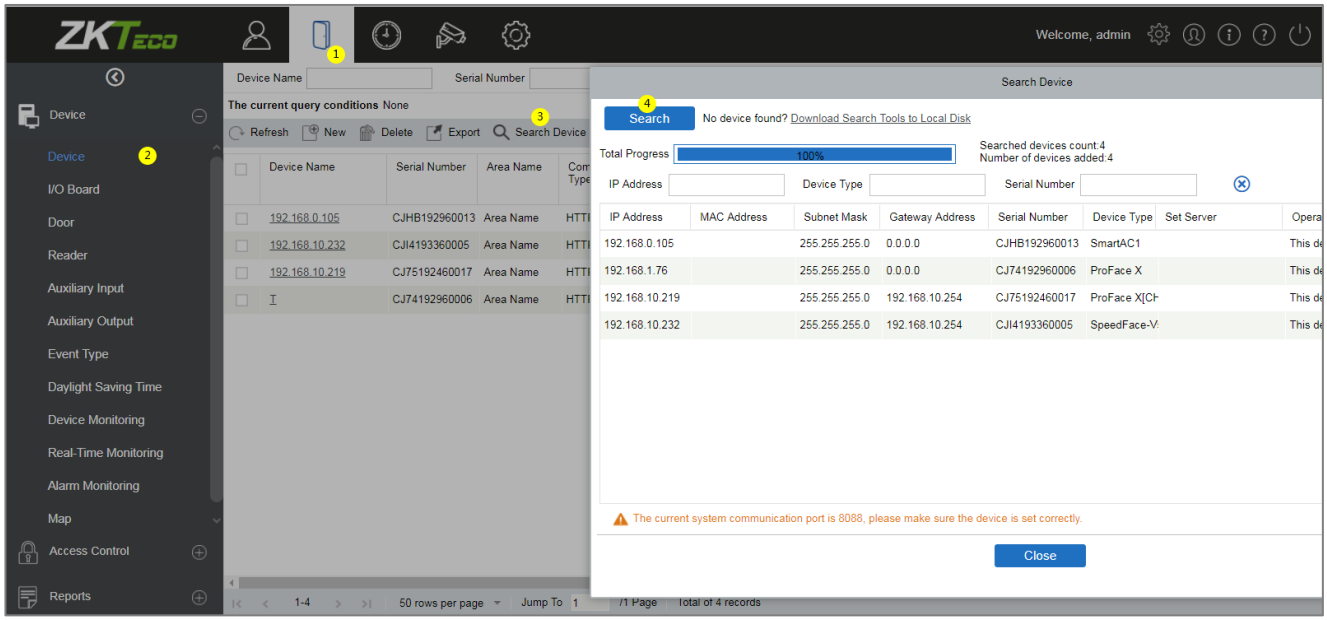
У розділі Device Settings (Налаштування пристрою) додається пристрій доступу, а потім встановлюються параметри зв'язку між підключеними пристроями, зокрема налаштування системи та пристрою. Після успішного встановлення зв'язку тут можна переглянути інформацію про підключені пристрої, а також виконати віддалений моніторинг, вивантаження та завантаження тощо.

5.4.1 Додавання пристрою

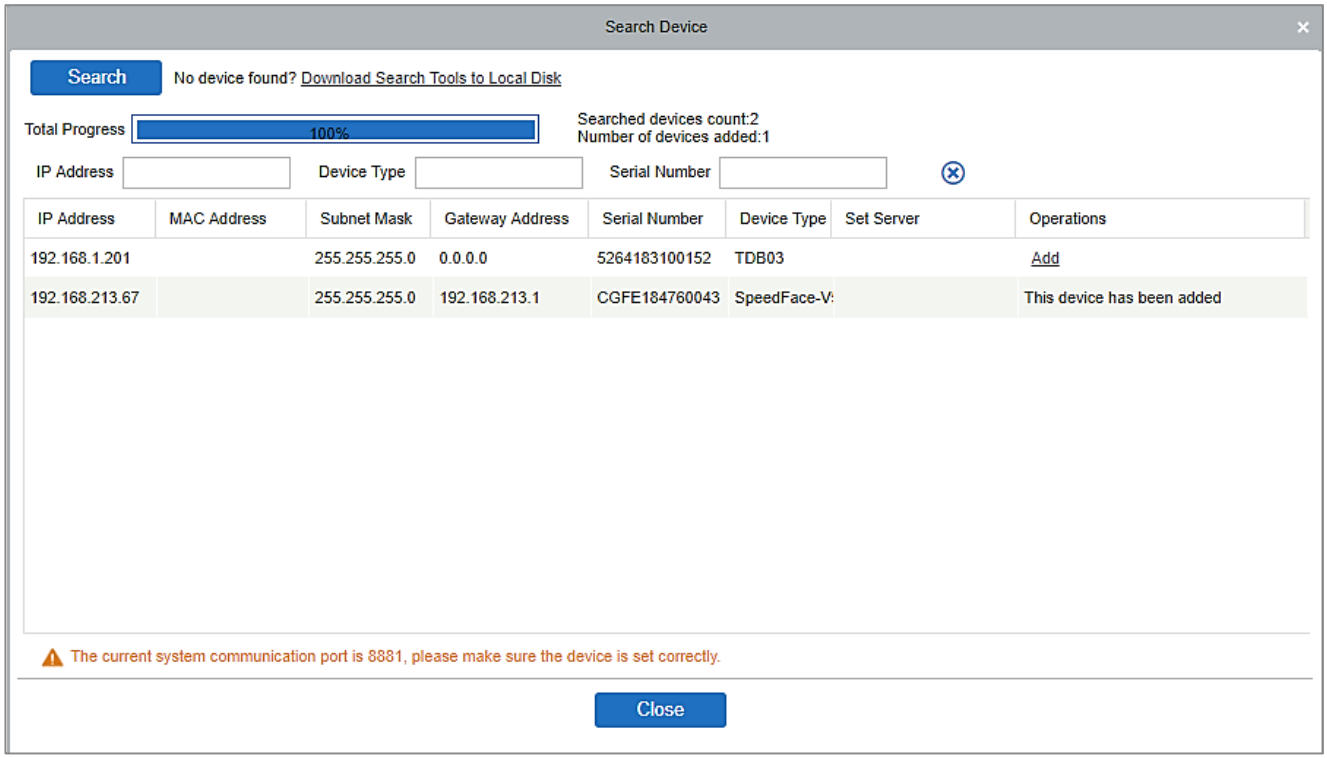
Пристрої доступу можна додати двома способами.

Додати пристрій за допомогою пошуку контролерів доступу.

Виконайте пошук контролерів доступу в мережі Ethernet.



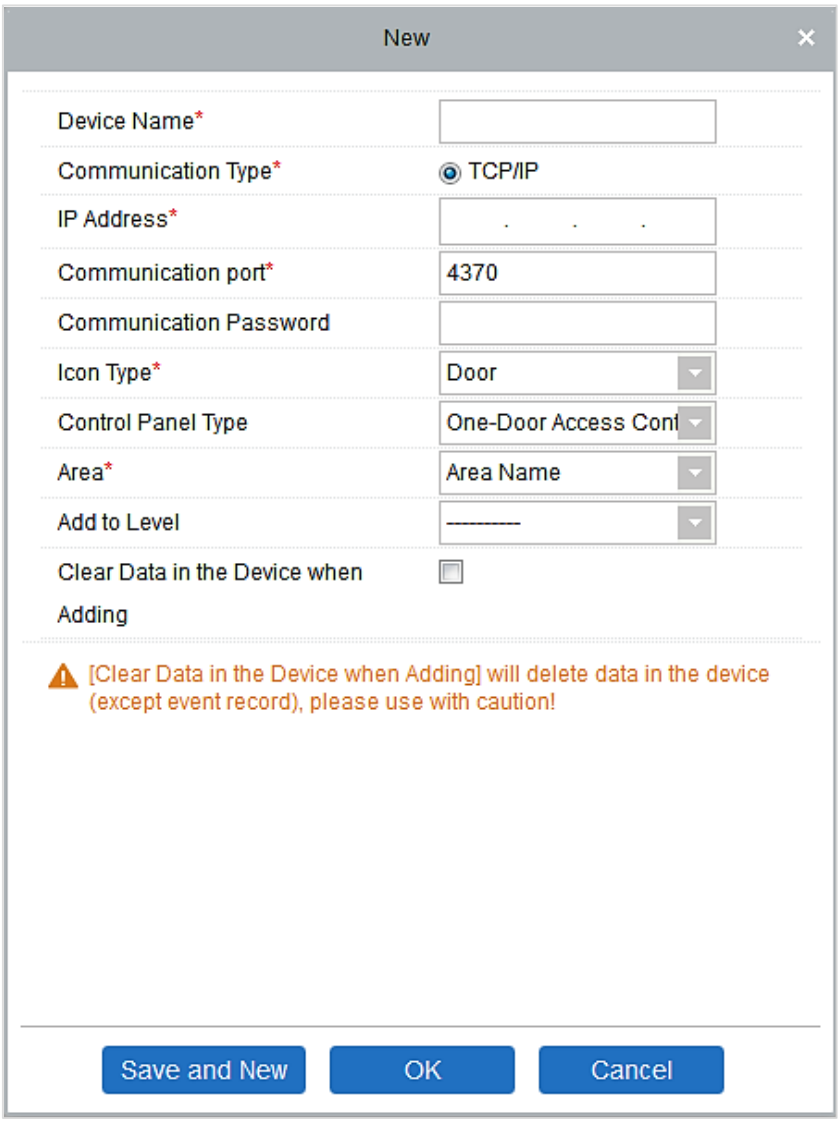
1. Натисніть **Access** (Доступ) > **Device** (Пристрій) > **Search Device** (Знайти пристрій), щоб відкрити інтерфейс пошуку.
2. Натисніть кнопку **Search** (Пошук), і з'явиться вікно **Searching.....** (пошук.....)
3. Після завершення пошуку буде відображено список і загальна кількість контролерів доступу.



Примітка: Режим широкомовлення UDP буде використовуватися для пошуку пристроїв доступу. Цей режим не може виконувати функцію крос-маршрутизатора. IP-адреса може забезпечити міжмережевий сегмент, але вона повинна знаходитися в тій самій підмережі, а шлюз і IP-адреса повинні бути налаштовані в тому самому сегменті мережі.

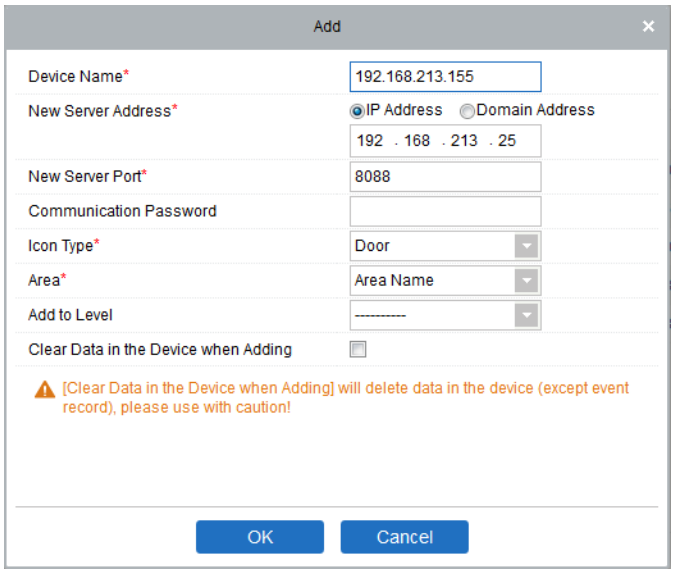
1. Натисніть **Add** (Додати) у списку пошуку.

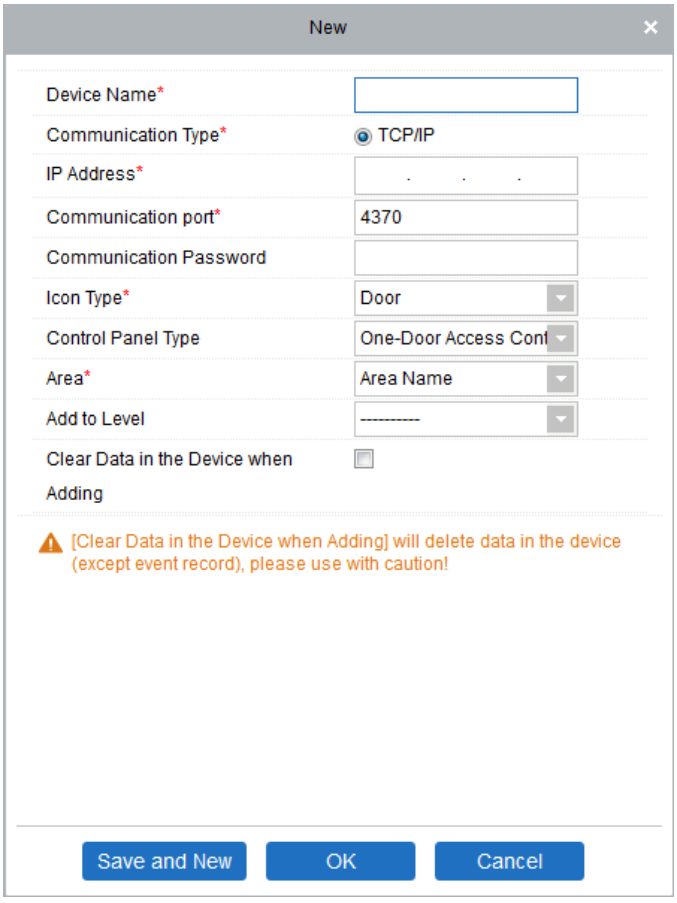
Якщо пристрій є pull-пристроєм, ви можете ввести назву пристрою і натиснути **OK**, щоб завершити додавання пристрою.



Clear Data in the device when Adding (Очищати дані на пристрої під час додавання): Якщо цей параметр вибрано, після додавання пристрою система очистить усі дані на ньому (окрім журналів подій).

Якщо пристрій з push-прошивкою, після натискання кнопки **Add** (Додати) з'являться наступні вікна. Якщо вибрано опцію IP-address у полі **New Server Address** (Адреса нового сервера), налаштуйте IP-адресу та номер порту. Якщо вибрано опцію Domain Address (Адреса домену) в **New Server Address** (адреса нового сервера), налаштуйте Domain Address (адресу домену), port number (номер порту) та DNS. Пристрій буде додано до програми автоматично.





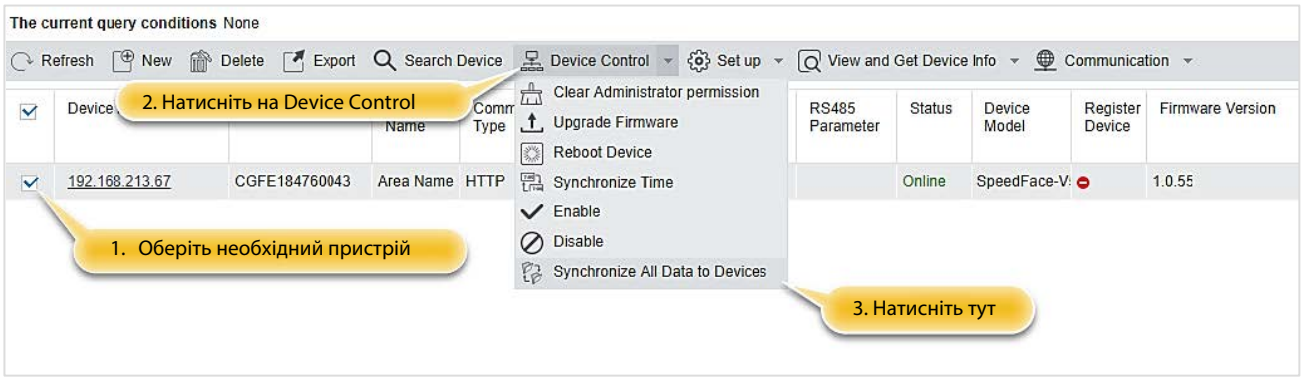
New Server Address (Нова адреса сервера): Щоб додати пристрій за IP Address (IP-адресою) або Domain Address (адресою домену), пристрої можна додати до програми, ввівши адресу домену.

New Server Port (Новий порт сервера): Встановіть точку доступу системи.

DNS: Встановіть DNS-адресу сервера.

Clear Data in the Device when Adding (Очистити дані в пристрої при додаванні): Якщо ця опція вибрана, то після додавання пристрою система очистить усі дані на ньому (окрім журналів подій). Якщо ви додаєте пристрій лише для демонстрації або тестування, немає потреби ставити цю галочку.

Примітка: При використанні одного з трьох вищезгаданих методів додавання пристроїв, якщо на оригінальному пристрої є залишкові дані, будь ласка, синхронізуйте з ними вихідні дані після додавання нового пристрою до програми, натиснувши **Device** (Пристрій) > **Synchronize All Data to Devices** (Синхронізувати всі дані з пристроями), інакше ці вихідні дані можуть конфліктувати з нормальним використанням.

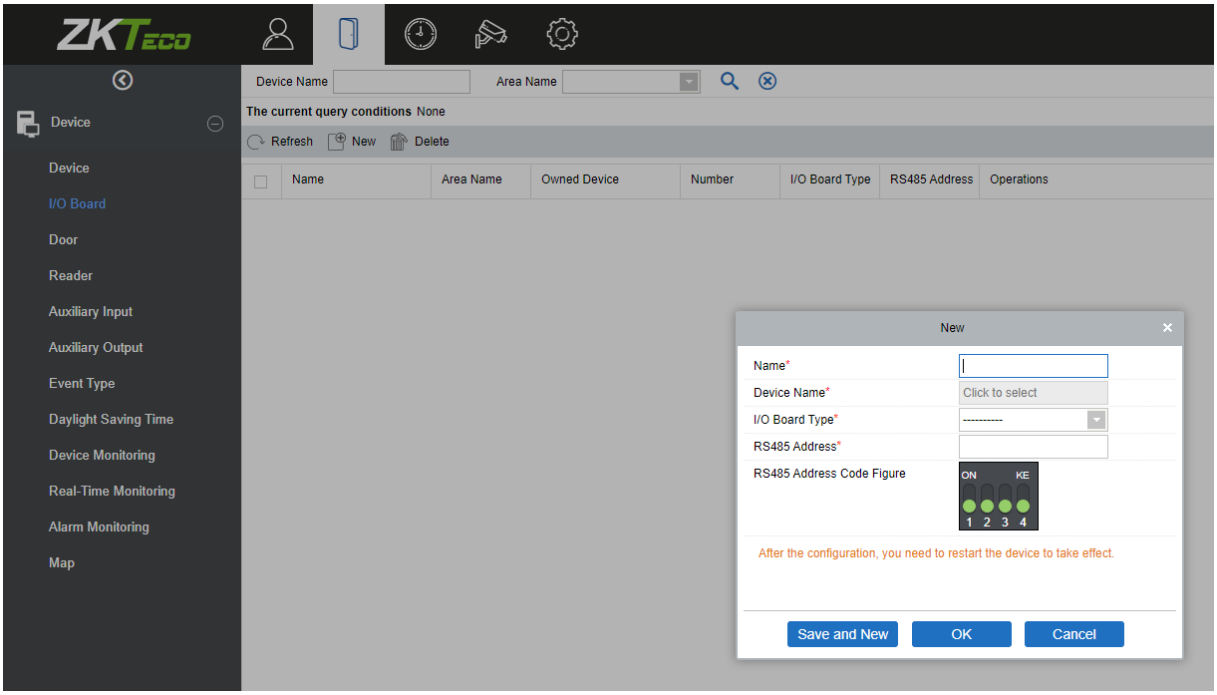


2. IP-адреса пристрою доступу за замовчуванням може конфліктувати з IP-адресою пристрою в локальній мережі. Ви можете змінити його IP-адресу: натисніть **Modify IP Address** (Змінити IP-адресу), і в інтерфейсі з'явиться діалогове вікно. Введіть нову IP-адресу та інші параметри (Примітка: Налаштуйте шлюз та IP-адресу в одному сегменті мережі).

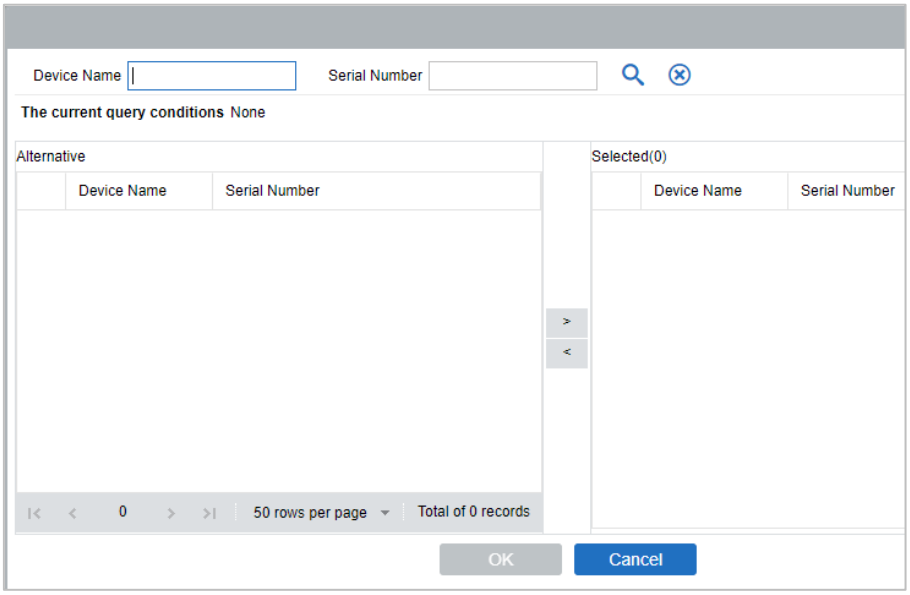
Примітка: Деякі PUSH пристрої підтримують SSL. Щоб скористатися цією функцією, виберіть порт HTTPS під час встановлення програмного забезпечення та переконайтеся, що прошивка пристрою підтримує SSL.

5.4.2 Плата вводу/виводу

У модулі пристрою натисніть **Device** (Пристрій) > **I/O Board** (Плата вводу/виводу) > **New** (Новий), щоб додати пристрій плати вводу/виводу до програмного забезпечення.



Введіть назву плати вводу/виводу. Виберіть пристрій, натиснувши на поле Device Name (Назва пристрою). З'явиться список пристроїв, як показано нижче:

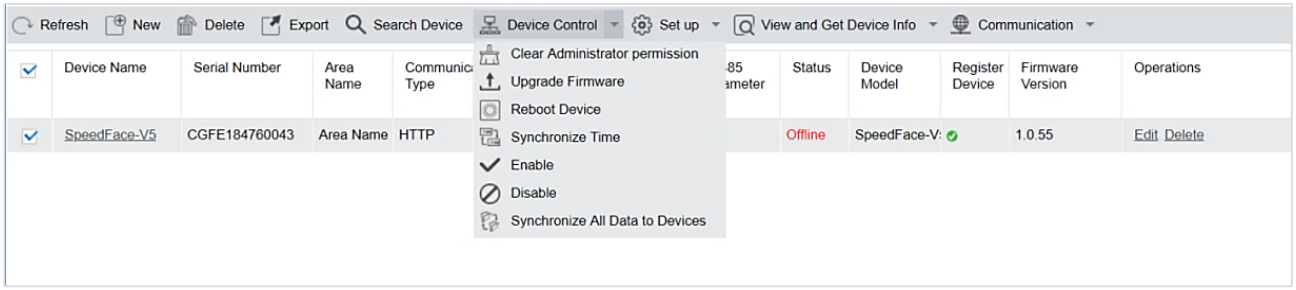


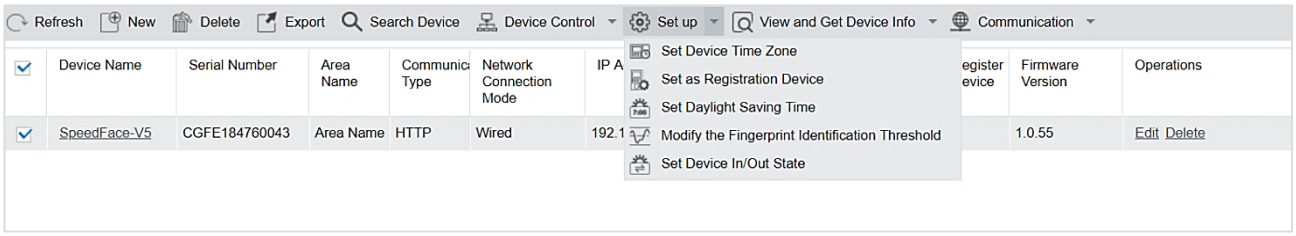
Виберіть пристрій і натисніть **OK**. Виберіть тип плати вводу/виводу. Встановіть кодову адресу RS485, натиснувши відповідну кнопку (Code Access). Натисніть **OK**, щоб зберегти дані. Ви можете переглянути всі додаткові входи в інтерфейсі **Auxiliary Input**.

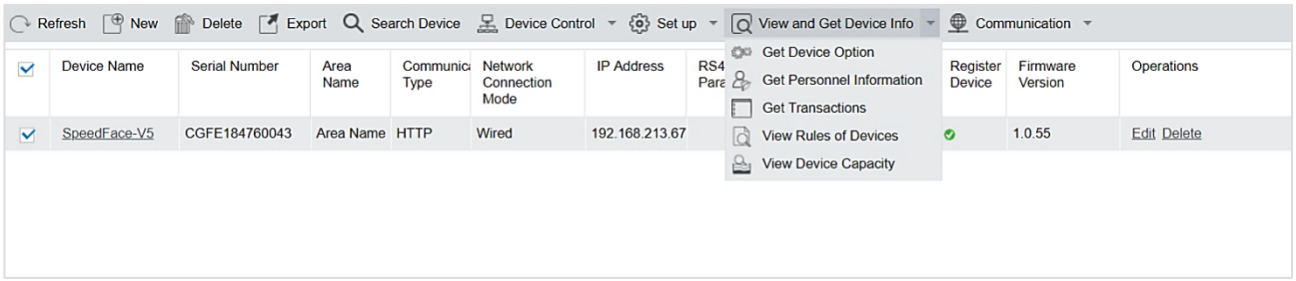
Примітка: Будь ласка, обирайте цей метод під час додавання **DM10** та **AUX485**.

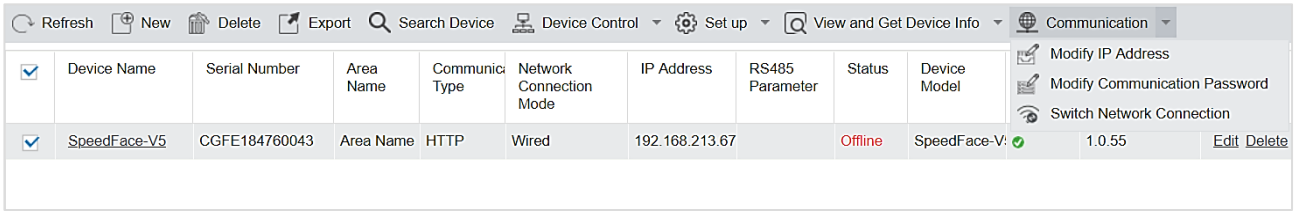
5.4.3 Робота пристрою

Для зв'язку між системою та пристроєм необхідно налаштувати завантаження даних, завантаження конфігурації, параметрів пристрою та системи. Користувачі можуть редагувати контролери доступу в межах відповідних рівнів у поточній системі; користувачі можуть лише додавати або видаляти пристрої в Device Management (Керуванні пристроями), якщо це необхідно.





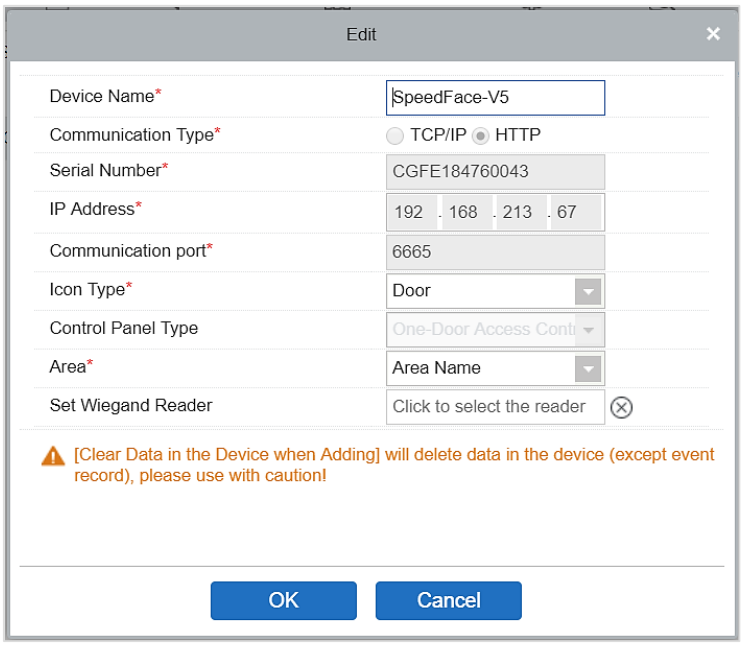




- **Редагування або видалення пристрою**

Редагувати: Клацніть на Device Name (назву пристрою) або натисніть кнопку **Edit** (Редагувати), щоб отримати доступ до інтерфейсу редагування.

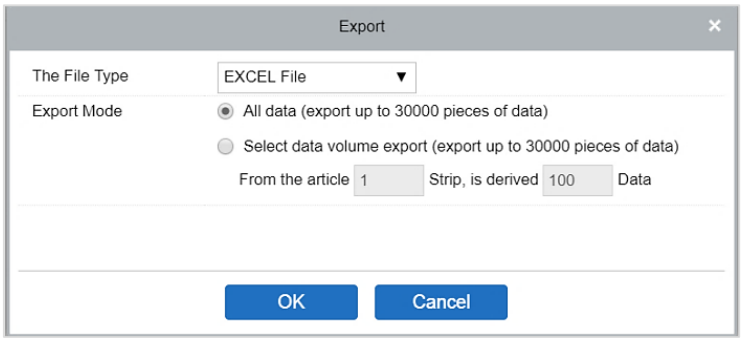
Видалити: Виберіть пристрій, натисніть **Delete** (Видалити) і натисніть **OK**, щоб видалити пристрій.

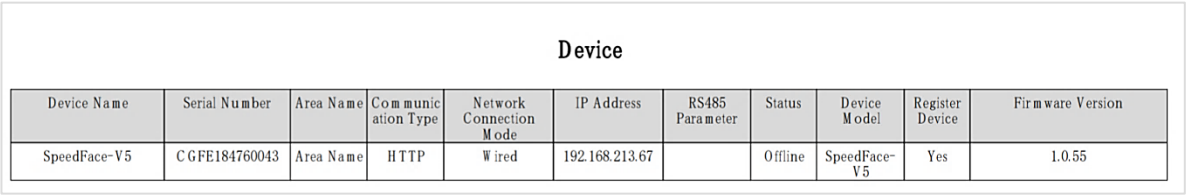


Для більш детальної інформації та налаштувань вищезазначених параметрів див. Пристрій. Деякі дані не можна редагувати. Ім'я пристрою має бути унікальним і не повинно збігатися з ім'ям іншого пристрою.
Тип панелі управління не може бути змінений. Якщо тип неправильний, користувачі повинні видалити пристрій і додати його знову вручну.

- **Експорт**

Інформацію про пристрій можна експортувати у форматах EXCEL, PDF та CSV.



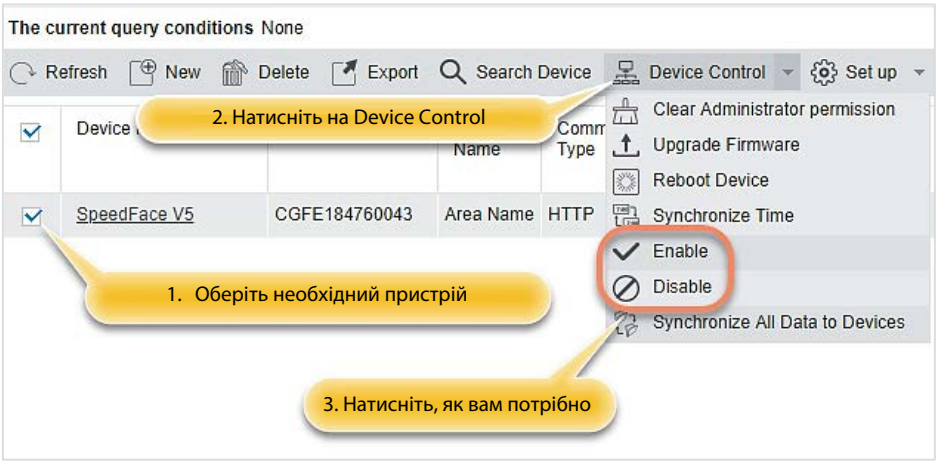


Device

Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Status	Device Model	Register Device	Firmware Version
SpeedFace-V5	CGFE184760043	Area Name	HTTP	Wired	192.168.213.67		Offline	SpeedFace-V5	Yes	1.0.55

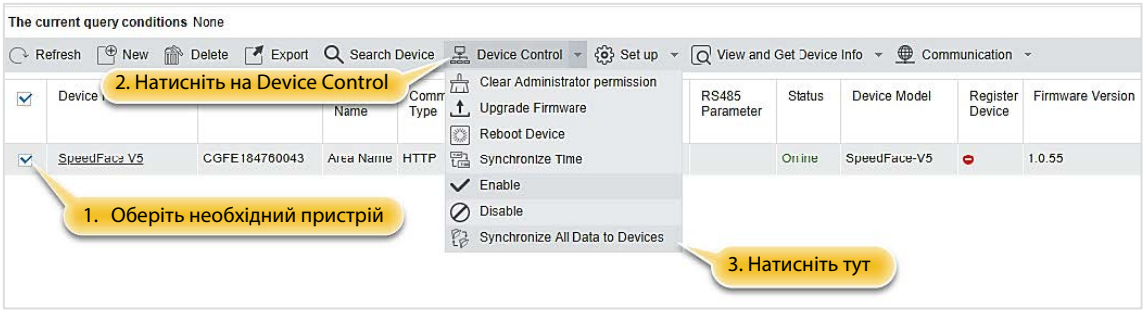
- **Вимкнути/Ввімкнути**

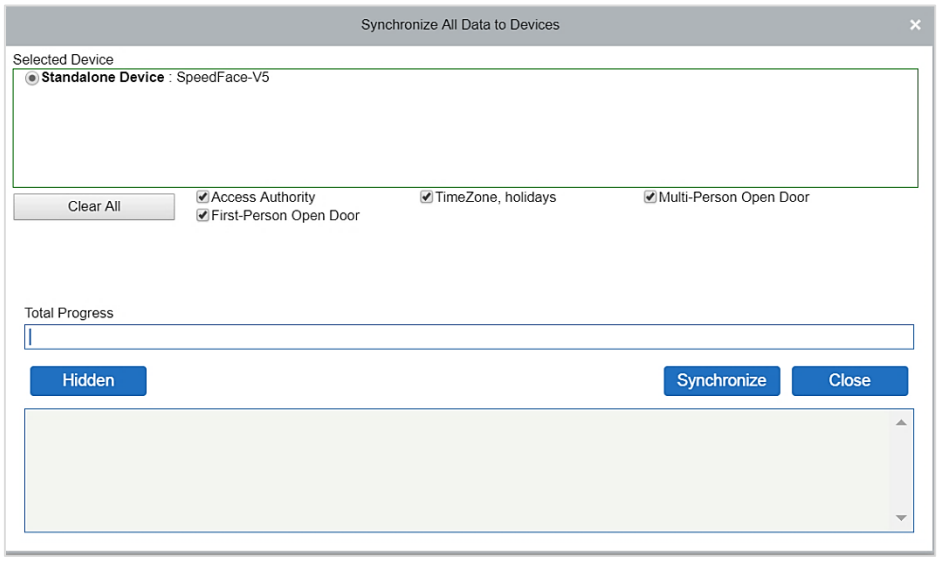
Виберіть пристрій, натисніть **Disable**/**Enable** (Вимкнути/Увімкнути), щоб зупинити/почати використання пристрою. Якщо зв'язок між пристроєм і системою перервано або пристрій вийшов з ладу, пристрій може автоматично перейти у вимкнений стан. Після налаштування локальної мережі або пристрою натисніть **Enable** (Увімкнути), щоб повторно підключити пристрій і відновити зв'язок між пристроями.



- **Синхронізація всіх даних на пристроях**

Щоб синхронізувати дані системи з пристроєм, виберіть пристрій і натисніть **Synchronize All Data to Devices** (Синхронізувати всі дані з пристроями), а потім натисніть **OK**, щоб завершити синхронізацію.

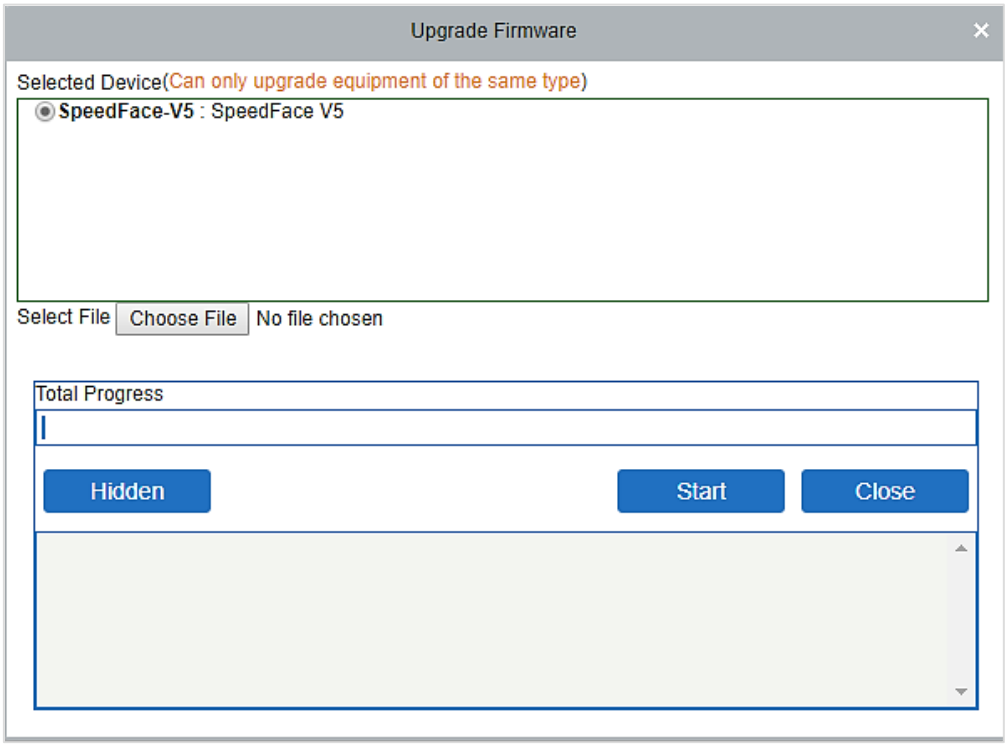




Примітка: **Синхронізація всіх даних на пристроях** спочатку видалить всі дані на пристрої (крім транзакцій), і таким чином завантажити всі налаштування заново. Будь ласка, слідкуйте за стабільним інтернет-з'єднанням та уникайте ситуацій з вимкненим живленням. Якщо пристрій працює нормально, будь ласка, використовуйте цю функцію з обережністю. Виконуйте її в рідкісних ситуаціях, щоб запобігти впливу на регулярне використання пристрою.

- **Оновлення прошивки**

Виберіть потрібний пристрій, який потрібно оновити, натисніть **Upgrade firmware** (Оновити прошивку), щоб увійти в інтерфейс редагування, потім натисніть **Choose File** (Вибрати файл), щоб вибрати файл оновлення прошивки (з назвою emfw.cfg), наданий програмним забезпеченням Access, і натисніть **OK**, щоб почати оновлення.



Примітка: Користувач не має права оновлювати прошивку без дозволу. Перед оновленням мікропрограми зверніться до дистриб'ютора або оновлюйте її, дотримуючись інструкцій дистриб'ютора. Несанкціоноване оновлення може вплинути на нормальну роботу пристрою.

- **Reboot Device** (Перезавантажити пристрій)

Це перезавантажить вибраний пристрій.

- **Synchronize Time** (Синхронізувати час)

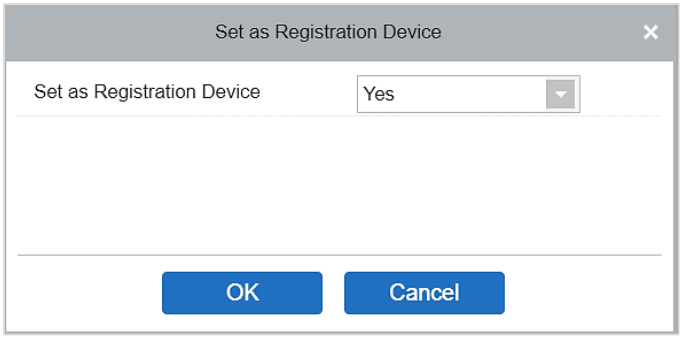
Це синхронізує час пристрою з поточним часом на сервері.

- **Set Device Time Zone (**Встановити часовий пояс пристрою)

Якщо пристрій підтримує налаштування часового поясу і не знаходиться в одному часовому поясі з сервером, необхідно встановити часовий пояс пристрою. Після встановлення часового поясу пристрій автоматично синхронізує час відповідно до часового поясу та часу сервера.

- **Set as Registration device** (Встановити як пристрій реєстрації)

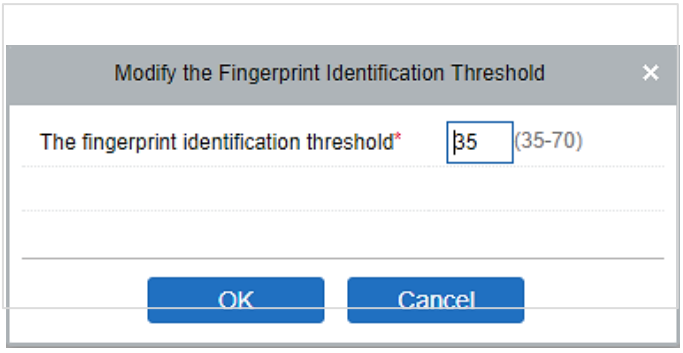
Встановлюйте пристрій реєстрації лише тоді, коли дані автономного пристрою, наприклад, про персонал, можуть автоматично завантажуватися.



- **Set Daylight Saving Time** (Встановити літній час)

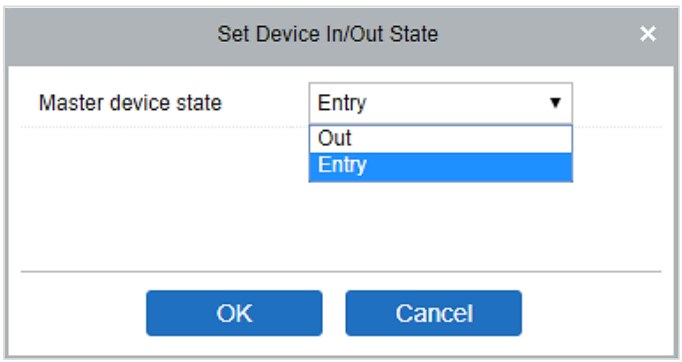
Відповідно до вимог різних регіонів, встановіть правила переходу на літній час.

- **Modify the fingerprint identification threshold (Ensure that the access controller supports fingerprint function)** (Змінити поріг ідентифікації за відбитками пальців (переконайтеся, що контролер доступу підтримує функцію ідентифікації за відбитками пальців))



- **Set Device In/Out State** (Встановити стан входу/виходу пристрою)

Це визначить стан головного пристрою як Entry (Вхід) або Out (Вихід).

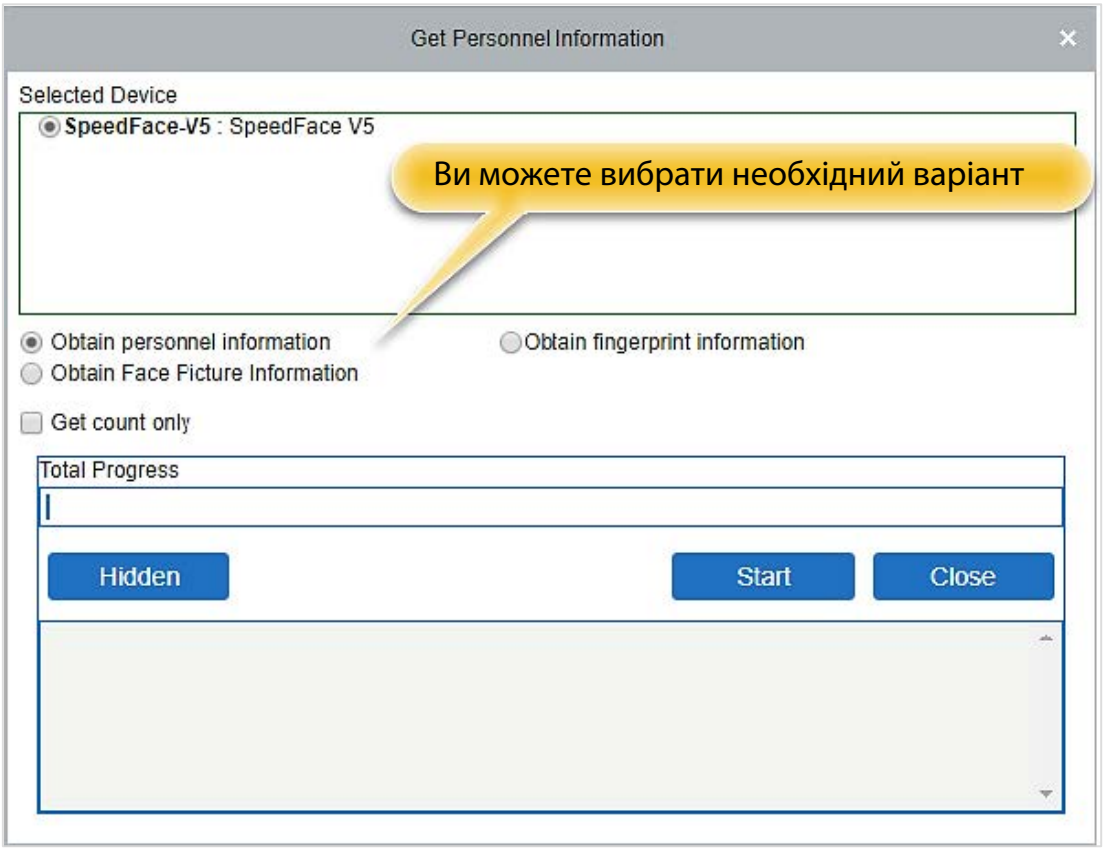


- **Get Device Option** (Отримати опцію пристрою)

Це отримує загальні параметри пристрою. Наприклад, він отримує версію прошивки після оновлення пристрою.

- **Get Personnel Information** (Отримати інформацію про персонал)

Це відображає поточну кількість персоналу, відбитків пальців, вен пальців і шаблонів обличчя в пристрої. Остаточне значення буде відображено у списку пристроїв.



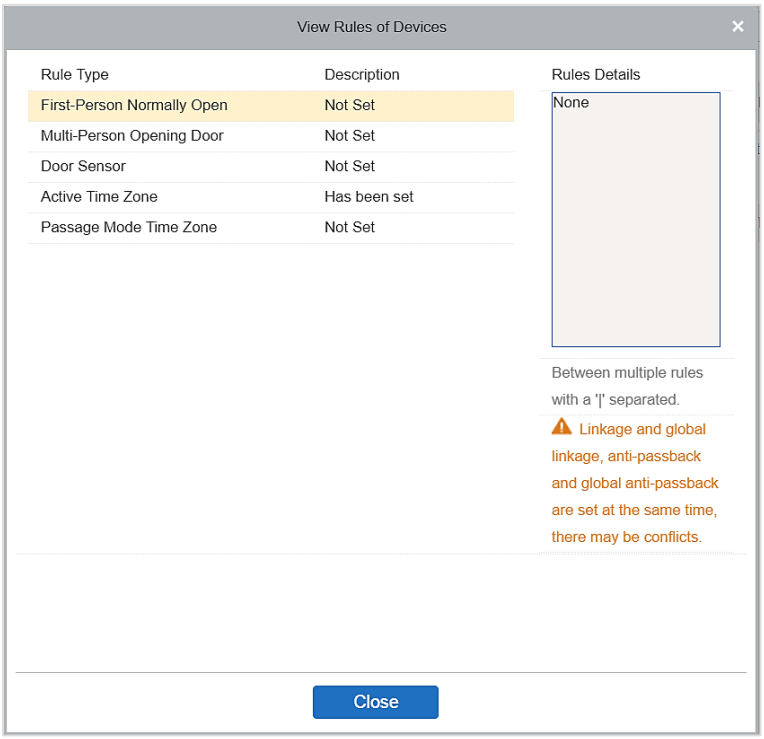
- **Отримати транзакції**

Це витягує транзакції з пристрою в систему. Для цієї операції передбачено два варіанти: Get New Transactions (Отримати нові транзакції) та Get All Transactions (Отримати всі транзакції).
Отримати нові транзакції: Система отримує нові транзакції тільки з моменту останньої зібраної та записаної транзакції. Повторні транзакції не будуть перезаписані.
Отримати всі транзакції: Система знову отримає транзакції. Повторювані записи не будуть показані двічі.
Коли стан мережі здоровий, а зв'язок між системою і пристроєм нормальний, система буде отримувати транзакції пристрою в режимі реального часу і зберігати їх у базі даних системи. Однак, якщо мережа перервана, або зв'язок перерваний з будь-якої причини, і транзакції пристрою не були завантажені в систему в режимі реального часу, можна скористатися функцією **Get Transactions** (Отримати транзакції), щоб отримати транзакції пристрою вручну. Крім того, за замовчуванням, система буде автоматично отримувати транзакції пристрою о 00:00 кожного дня.

Примітка: Контролер доступу може зберігати до 100 тисяч транзакцій. Коли кількість транзакцій перевищить цю кількість, пристрій автоматично видалить найстаріші збережені транзакції (за замовчуванням видаляє 10 тисяч транзакцій).

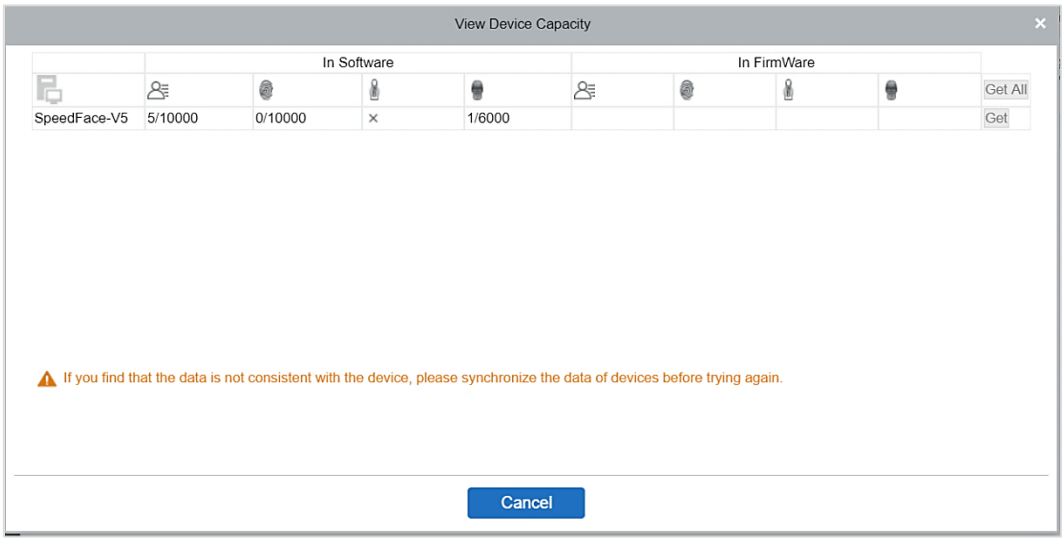
- **View Rules of Devices** (Переглянути правила для пристроїв)

Показує правила доступу на пристрої.



- **View Device Capacity** (Переглянути ємність пристрою)

Це відображає кількість біометричних даних персоналу в пристрої.



- **Modify IP Address** (Змінити IP-адресу)

Виберіть пристрій і натисніть **[Modify IP address]** (Змінити IP-адресу), щоб відкрити інтерфейс модифікації. Програма отримає від пристрою мережевий шлюз і маску підмережі у реальному часі. (Якщо цього не зробити, ви не зможете змінити IP-адресу). Потім введіть нову IP-адресу, шлюз і маску підмережі. Натисніть **OK**, щоб зберегти і вийти. Ця функція подібна до функції [Modify IP Address Function] (Змінити IP-адресу) у розділі Пристрій.

- **Modify Communication Password** (Змінити пароль зв'язку)

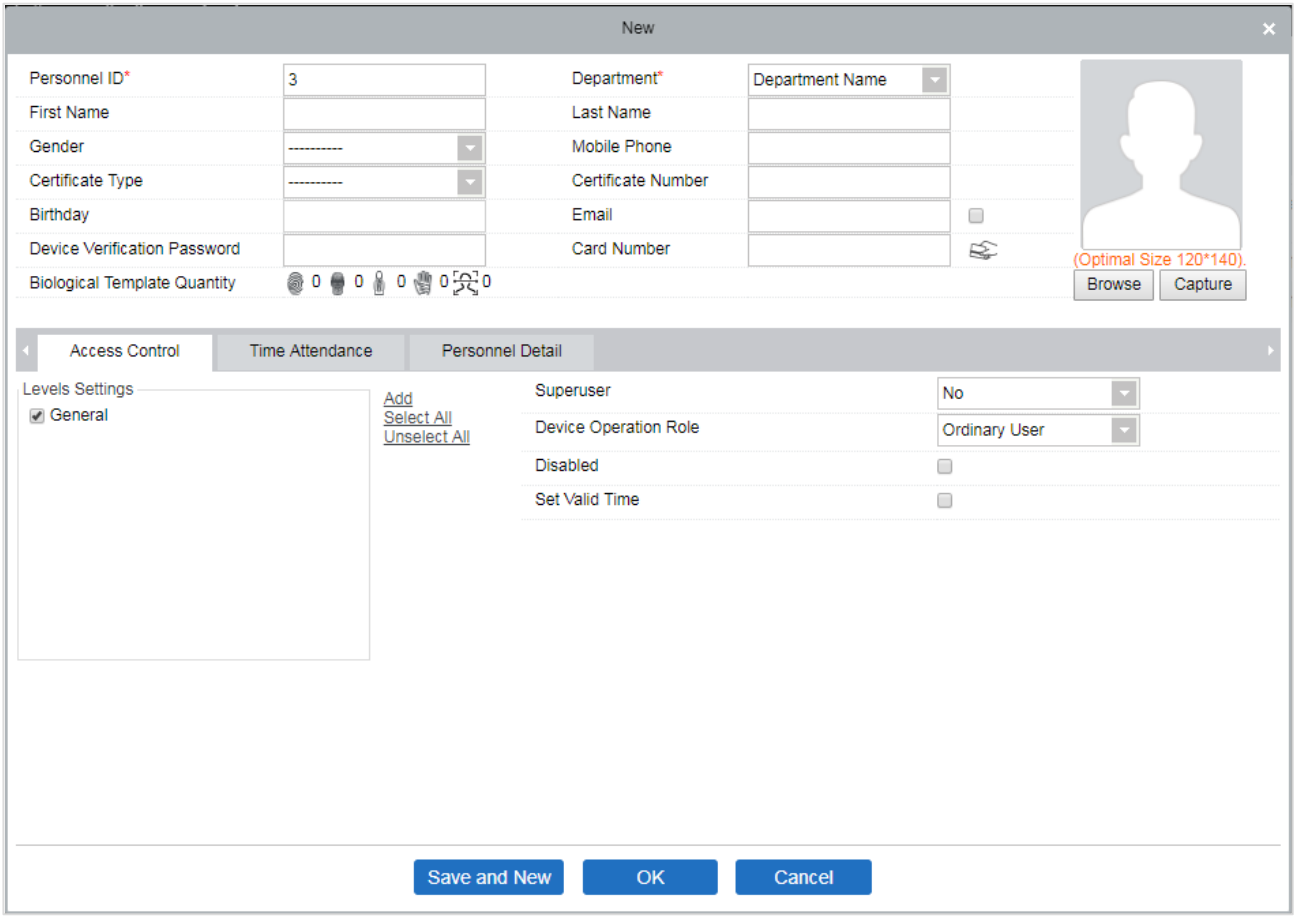
Перед зміною пароля система запитає старий пароль зв'язку. Після перевірки введіть новий пароль двічі і натисніть **OK**, щоб змінити пароль зв'язку.

Примітка: Пароль має бути комбінацією цифр і букв, що складається з 6 цифр.

Користувачі можуть змінювати пороги ідентифікації відбитків пальців у пристроях; вони варіюються від 35 до 70, за замовчуванням встановлено 55. Система буде зчитувати пороги з пристрою. Користувачі можуть переглянути список порогових пристроїв. За допомогою функції пакетної роботи можна змінити більше одного пристрою.

5.5 Додати користувача та картку

1. Виберіть **Personnel Management** (Управління персоналом) > **Personnel** (Персонал) > **New** (Новий).



Поля виглядають наступним чином:

Personnel ID (ідентифікатор персоналу): Ідентифікатор може складатися з 9 символів, в діапазоні від 1 до 79999999. Він може бути налаштований відповідно до ваших вимог. За замовчуванням ідентифікатор містить лише цифри, але може містити також літери.

Примітки:

1. Під час налаштування номера персоналу перевірте, чи підтримує поточний пристрій максимальну довжину і чи можна використовувати літери в ID персоналу.
2. Щоб змінити налаштування максимальної кількості символів у кожному номері персоналу та можливість використання літер, натисніть **Personnel** (Персонал) > **Parameters** (Параметри).

Department (Відділ): Виберіть зі спадного меню і натисніть **OK**. Якщо відділ не було встановлено раніше, з'явиться лише один відділ з назвою **Company Name** (Назва компанії).

First Name/Last Name (Ім'я/Прізвище): Максимальна кількість символів - 50.

Gender (Стать): Встановіть стать персоналу.

Mobile Phone (Мобільний телефон): Введіть номер телефону користувача.

Cetificate Type (Тип сертифіката): Існує чотири типи сертифікатів: Посвідчення особи, Паспорт, Водійське посвідчення та інші.

Certificate Number (Номер сертифіката): Введіть номер сертифіката.

Birthday (Дата народження): Введіть дату народження працівника.

Email: Введіть електронну пошту працівника. Максимальна довжина - 30 символів.

Device Verification Password (Пароль для входу на пристрій): встановіть пароль для входу на пристрій за допомогою облікових записів персоналу. Він може містити не більше 6 цифр. Він не може збігатися з паролем іншого користувача та паролем примусу.

Card number (Номер картки): Максимальна довжина - 10, і він не повинен повторюватися.

Personal Photo (Особисте фото): Надається функція попереднього перегляду зображення, що підтримує поширені формати зображень, такі як **JPG**, **JPEG**, **BMP**, **PNG**, **GIF** тощо. Найкращий розмір - 120×140 пікселів.

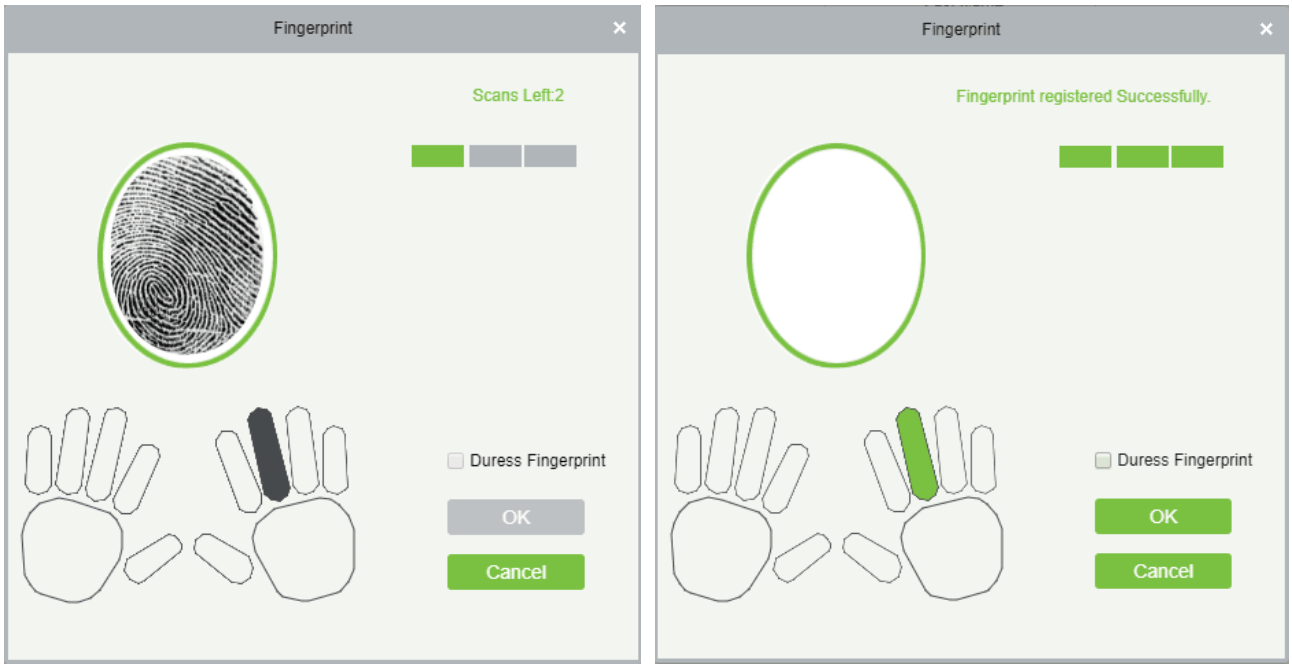
Browse (Перегляд): Натисніть **Browse** (Огляд), щоб вибрати фотографію на вашому локальному диску для завантаження.

Capture (Зробити знімок): Фотографування за допомогою камери дозволено, якщо до сервера підключено камеру.

Register Fingerprint / Finger Vein (Зареєструвати відбиток пальця / вену пальця): Зареєструйте відбиток пальця, вену пальця, долоні або обличчя персоналу. Щоб увімкнути тривогу та надіслати сигнал до системи, відскануйте відбиток пальця під примусом.

Як зареєструвати відбиток пальця:

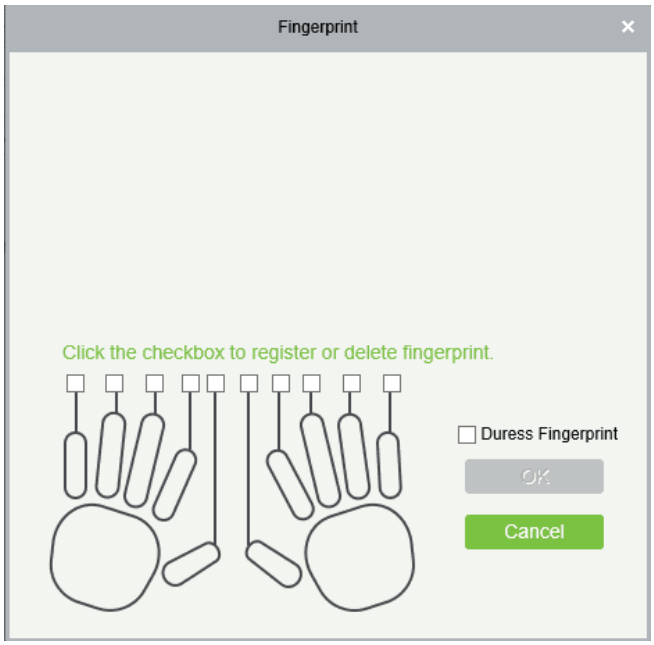
1. Наведіть курсор на іконку відбитка пальця, з'явиться спливаюче вікно реєстрації або діалогове вікно завантаження драйвера, натисніть кнопку **Register** (Зареєструвати).
2. Виберіть відбиток пальця, безперервно притискайте палець до датчика, доки не з'явиться повідомлення **"Fingerprint registered Successfully"** («Відбиток пальця успішно зареєстровано»).
3. Натисніть **OK**, щоб завершити реєстрацію.

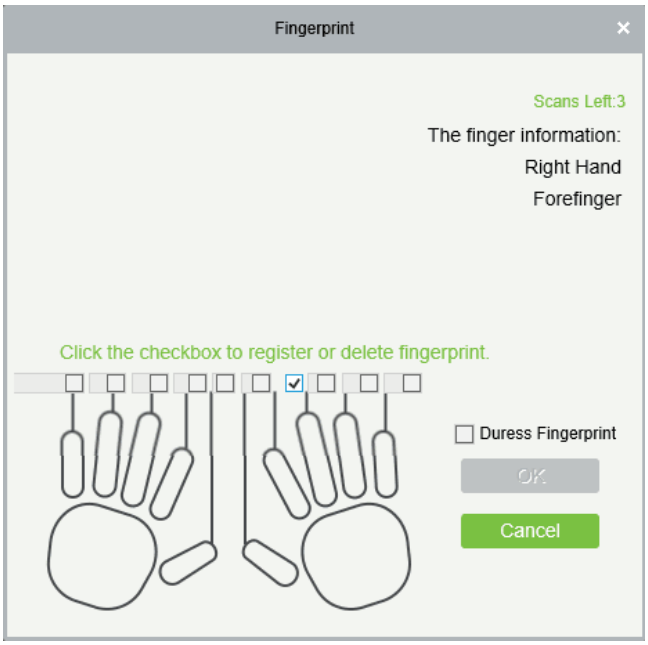


Натисніть на відбиток пальця, щоб видалити його. Якщо вам потрібно зареєструвати відбиток пальця під примусом, встановіть галочку "Відбиток пальця під примусом".

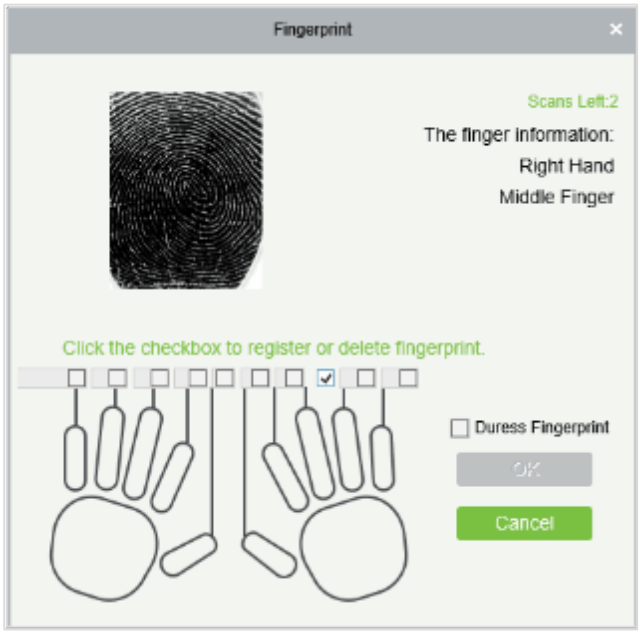
Примітки:

1. Якщо відбитки пальців повторюються, з'явиться запит «Не повторюйте введення відбитків пальців».
2. Якщо драйвер датчика відбитків пальців не встановлено, натисніть «Встановити драйвер» і система запропонує завантажити та встановити драйвер.
3. Після встановлення драйвера датчика відбитків пальців, якщо в браузері IE кнопка реєстрації відбитків пальців сірого кольору, тоді як в інших браузерах (наприклад, Firefox, Google) вона відображається нормально, ви можете змінити налаштування браузера IE наступним чином:
   a) В Internet Explorer натисніть **Tools** (Сервіс) > **Internet Options** (Властивості браузера) > **Security** (Безпека) > **Credible Sites** (Довірені сайти), додайте http://localhost до списку довірених сайтів, а потім перезапустіть Internet Explorer.
   b) В Internet Explorer натисніть **Tools** (Сервіс) > **Internet Options** (Властивості браузера) > **Advanced** (Додатково) > **Reset** (Скинути), щоб відкрити діалогове вікно «Скидання налаштувань Internet Explorer», натисніть **Reset** (Скинути) для підтвердження, а потім перезапустіть Internet Explorer (можна спробувати, якщо пункт 1 не допоміг).
   c) Якщо всі вищевказані налаштування не працюють, виконайте наступні дії (на прикладі браузера IE11): натисніть **Tools** (Сервіс) > **Internet Options** (Властивості браузера) > **Advanced** (Додатково) > **Security** (Безпека), встановіть галочку [Allow the software to run or install even if the signature is ...] (Дозволити запуск або встановлення програмного забезпечення, навіть якщо підпис ...) і зніміть галочку [Check for server certificate revocation] (Перевіряти наявність відкликання сертифіката сервера), після чого перезапустіть IE.
   d) Якщо версія браузера нижча за IE8, сторінка реєстрації відбитків пальців буде іншою:

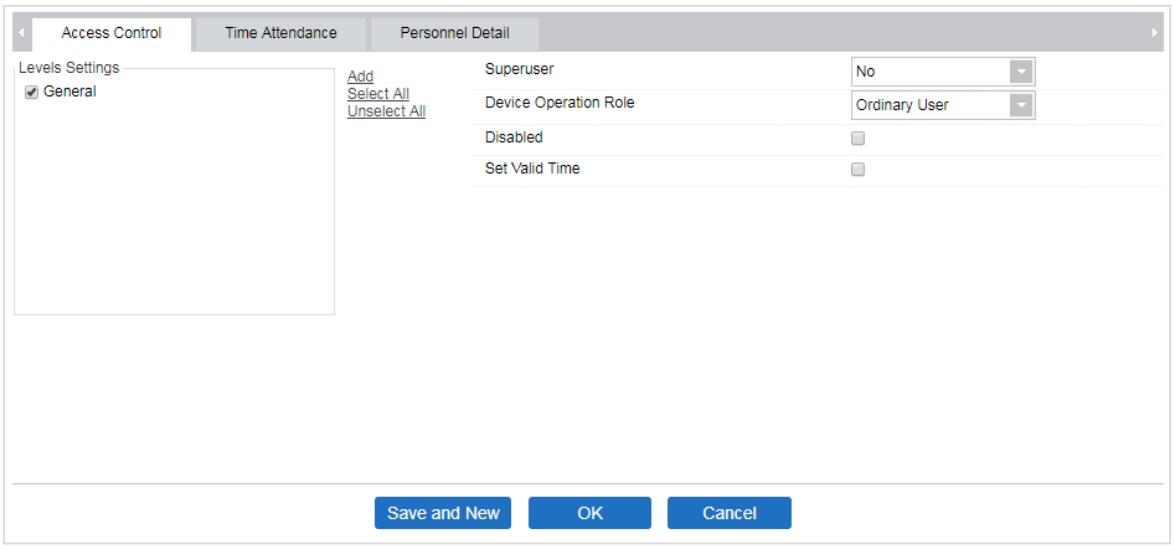




e) Система підтримує доступ за допомогою пристрою зчитування відбитків пальців Live20R та функцію запобігання підробці відбитків пальців.

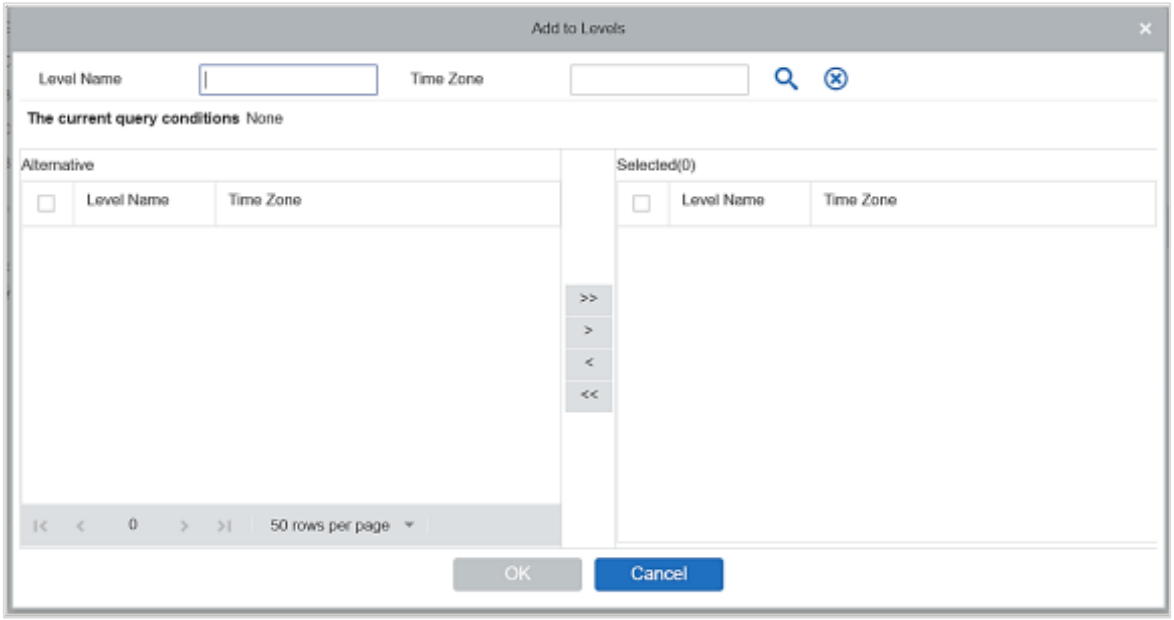


4. Щоб налаштувати параметри управління доступом для персоналу, натисніть **Access Control** (управління доступом).



Поля виглядають наступним чином:

Level Settings (Налаштування рівня): Натисніть **Add** (Додати), а потім встановіть правила проходження певних позицій у різних часових поясах.



Superuser (Суперкористувач): У роботі контролера доступу суперкористувач не обмежений правилами часових поясів і має надзвичайно високий пріоритет відчинення дверей.

Device Operation Role (Роль в роботі пристрою): Визначає рівень повноважень користувача на пристрої.

Disabled (Вимкнено): Тимчасово вимикає рівень доступу персоналу.

Set Valid Time (Встановити час дії): Двері можна налаштувати так, щоб вони відчинялися лише в певний час. Якщо галочку не встановлено, двері завжди відчинені.

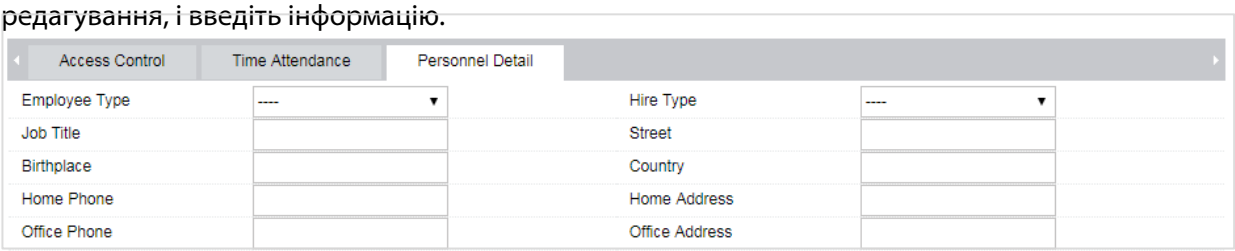
Примітка: Під час перевірки система автоматично шукатиме відповідні номери в бібліотеці відправлень.

За замовчуванням список інформації про персонал відображається у вигляді таблиці. Якщо вибрано Graphic Display (графічне відображення), будуть показані фотографії та номери. Наведіть курсор на фотографію, щоб переглянути детальну інформацію про особу.

Примітки:

- Не всі пристрої підтримують функцію «Вимкнено». Коли користувач додає пристрій, система повідомить користувача, чи підтримує поточний пристрій цю функцію чи ні. Будь ласка, оновіть пристрій, щоб використовувати цю функцію.
- Не всі пристрої підтримують функцію «Встановити час дії». Деякі пристрої дозволяють користувачам встановлювати лише рік, місяць і день місцевого часу. Коли користувач додає пристрій, система сповістить його про те, чи підтримує поточний пристрій цю функцію, чи ні. Будь ласка, оновіть пристрій, щоб використовувати цю функцію.

1. Натисніть **Personnel Detail** (Дані персоналу), щоб отримати доступ до деталей та інтерфейсу редагування, і введіть інформацію.



2. Після введення інформації натисніть **OK**, щоб зберегти і вийти, персональні дані будуть відображені в доданому списку.

5.6 Налаштування управління доступом

Система управлінням доступу може встановлювати рівні доступу зареєстрованих користувачів, а саме, дозволяти певному персоналу відкривати певні двері після перевірки протягом певного періоду. Керування системою управління доступу в першу чергу включає в себе часові зони управління доступом, вихідні дні управління доступом, налаштування дверей, рівні доступу, рівні доступу персоналу, моніторинг в режимі реального часу, звіти тощо.

Параметри системи управління доступом

- *255 часових поясів.*
- *Необмежені рівні доступу.*
- *Три типи свят і загалом 96 свят.*
- *Функція захисту від повторного входу.*
- *Функція відкриття декількох карток.*
- *Моніторинг в режимі реального часу.*
- *Функція блокування.*
- *Функція прив'язки.*
- *Функція нормального відкриття першої картки.*
- *Налаштування зчитувача.*
- *Налаштування допоміжних входів/виходів.*

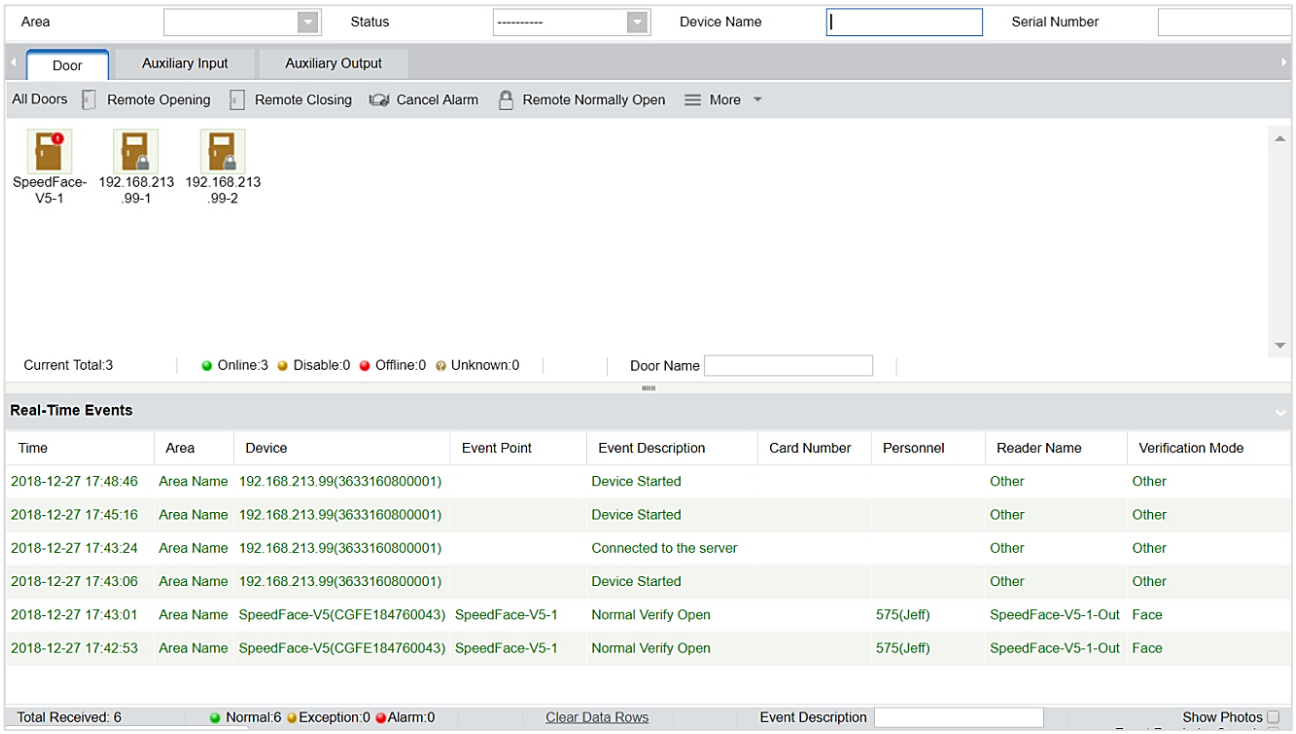
Для отримання додаткової інформації зверніться до "**Посібник користувача ZKBioAccess**."

5.7 Моніторинг у реальному часі

Натисніть **Access Device** (Пристрій доступу) > **Real-Time Monitoring** (Моніторинг у реальному часі).

Він відстежує стан і події дверей, налаштованих на панелі управління доступом в системі, в режимі реального часу, включаючи нормальні події та аномальні події (в тому числі тривожні). Інтерфейс Моніторингу в реальному часі має такий вигляд:

Іконки	Стан	Іконки	Стан
	Пристрій заблоковано		Двері вимкнено
	Датчик дверей не встановлено; реле замкнено		Датчик дверей не встановлено; реле розімкнуто
	Датчик дверей не встановлено, а поточна прошивка не підтримує поточну дію на пристрої		
	Онлайн-статус Двері зачинено; Реле замкнено		Онлайн-статус Двері зачинено; Реле розімкнуто
	Онлайн-статус Двері зачинено, а поточна прошивка не підтримує поточну дію на пристрої		
	Онлайн-статус Двері відчинено; Реле замкнено		Онлайн-статус Двері відчинено; Реле розімкнуто
	Онлайн-статус Двері відчинено, а поточна прошивка не підтримує поточну дію на пристрої		
	Тривога відчинення дверей; Реле замкнене		Тривога відчинення дверей; Реле розімкнуто
	Тайм-аут відчинення дверей, реле замкнене		Тайм-аут відчинення дверей, реле розімкнуто
	Тайм-аут відчинення дверей і поточна прошивка не підтримують поточну дію на пристрої		
	Тайм-аут відчинення дверей, реле замкнене/датчик дверей замкнений		Тайм-аут відчинення дверей, реле відкрито / датчик дверей закрито
	Тривога зачинення дверей; Реле замкнене		Тривога зачинення дверей; реле розімкнуто
	Тривога зачинених дверей, вказує на те, що поточна прошивка не підтримує поточну дію на пристрої		
	Датчик дверей не встановлено, Дверна тривога, Реле замкнене		Датчик дверей не встановлений, Дверна тривога, Реле розімкнуте
	Тайм-аут відчинення дверей, без стану реле/Датчик дверей закритий		Дверний замок
Без статусу реле вказує на те, що поточна прошивка не підтримує дію на пристрої.			



Різні іконки представляють стан наступним чином:

1. Двері

Дистанційне відчинення/зачинення: Можна керувати одними або всіма дверима.

Щоб керувати одними дверима, клацніть на них правою кнопкою миші та виберіть пункт **Remote Opening/Closing** (Дистанційне відчинення/зачинення) у спливаючому вікні. Щоб керувати всіма записами, безпосередньо натисніть **Remote Opening/Closing** (Дистанційне відчинення/зачинення) в опції Current All (Поточні всі).

У віддаленому відчиненні користувач може задати тривалість відчинення дверей (за замовчуванням - 15 секунд). Ви можете вибрати **[Enable Intraday Passage Mode Time Zone]** (Увімкнути внутрішньоденний часовий пояс режиму проходу), щоб увімкнути внутрішньоденні часові пояси режиму проходу, або встановити двері на Normal Open (NO), і тоді двері не будуть обмежені жодними часовими поясами (їх можна буде відчиняти в будь-який час).

Щоб зачинити двері, спочатку виберіть **[Disable Intraday Passage Mode Time Zone]** (Вимкнути внутрішньодобовий часовий пояс), щоб не дозволити іншим часовим поясам відчиняти двері, а потім виберіть **[Remote Closing]** (Дистанційне зачинення).

Примітка: Якщо функція [**Remote Opening /Closing**] (Віддалене відчинення/зачинення) не спрацьовує, перевірте, чи не від'єднані пристрої. Якщо від'єднані, перевірте підключення до мережі.

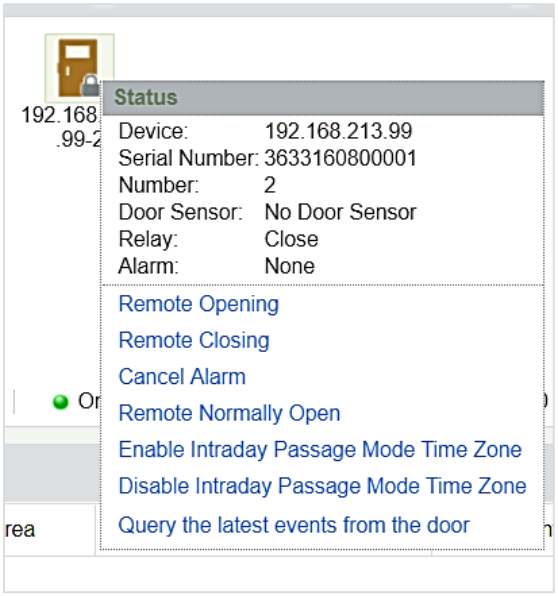
Скасувати тривогу: Якщо на інтерфейсі з'являться тривожні двері, пролунає звуковий сигнал тривоги. Тривогу можна скасувати як для окремих дверей, так і для всіх записів. Щоб керувати одними дверима, наведіть курсор на піктограму дверей, з'явиться меню, а потім виберіть у ньому пункт **Remote Opening/Closing** (Дистанційне відчинення/зачинення). Щоб керувати всіма дверима, безпосередньо натисніть **Remote Opening/Closing** (Дистанційне відчинення/зачинення) в опції Поточні всі.

Примітка: Якщо **скасувати тривогу** не вдається, перевірте, чи не від'єднано жодного пристрою. Якщо вони від'єднані, перевірте мережу.

Дистанційний Normally Open: переведе пристрій у режим Normally Open за допомогою дистанційного керування.

- **Швидке керування дверима**

Якщо ви наведете курсор на іконку дверей, ви зможете швидко виконати вищеописані операції. Крім того, ви можете запитувати останні події з дверей.

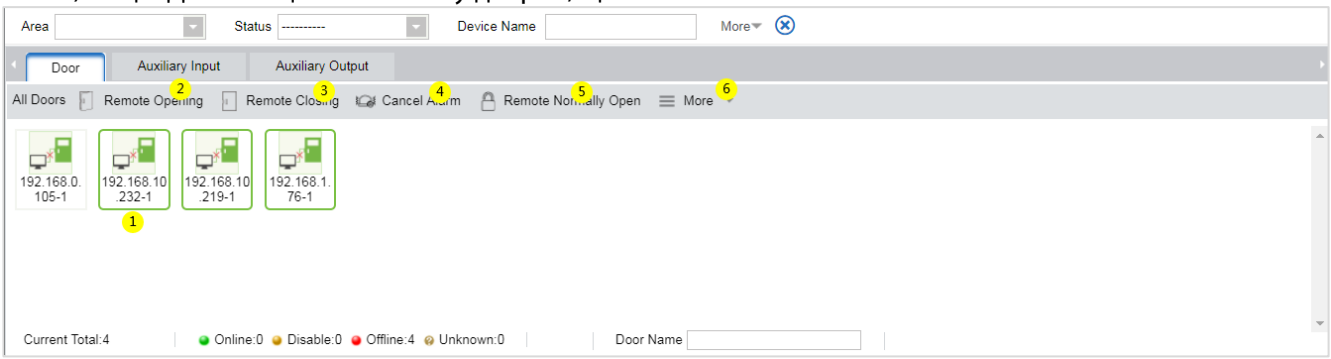


Запитувати останні події на дверях: Натисніть, щоб швидко переглянути поточні події на дверях.

Видати картку людині: Якщо ви обміняєте незареєстровану картку, в інтерфейсі моніторингу в режимі реального часу з'явиться запис із номером картки. Клацніть правою кнопкою миші на цьому номері картки, і з'явиться меню. Натисніть "Issue card to person" (Видати картку особі), щоб призначити цю картку одній особі.

- **Кілька варіантів вибору**

Ви можете вибрати кілька дверей одночасно для виконання таких операцій, як дистанційне відчинення (Remote Opening), дистанційне зачинення (Remote Closing), скасування тривоги (Cancel Alarm) тощо. Двічі клацніть на іконку дверей, щоб змінити їхні властивості.



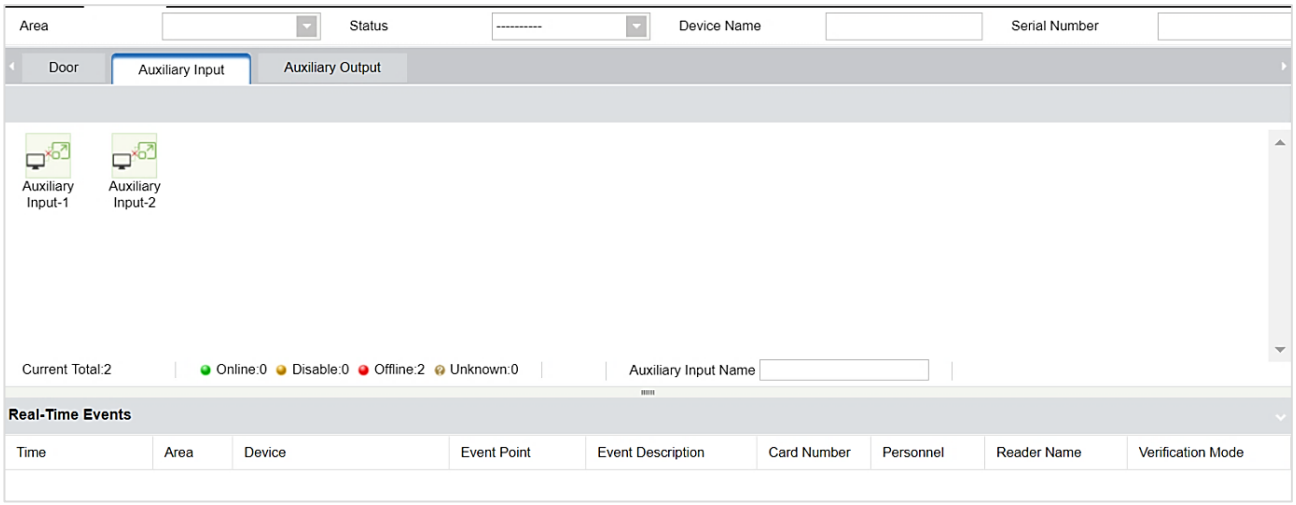
- **Моніторинг подій**

Система автоматично збирає записи про пристрої, за якими ведеться спостереження (за замовчуванням відображається 200 записів), включаючи нормальні та ненормальні події управління доступу (в тому числі тривожні). Нормальні події будуть позначені зеленим кольором, тривожні -

червоним, інші аномальні - помаранчевим.

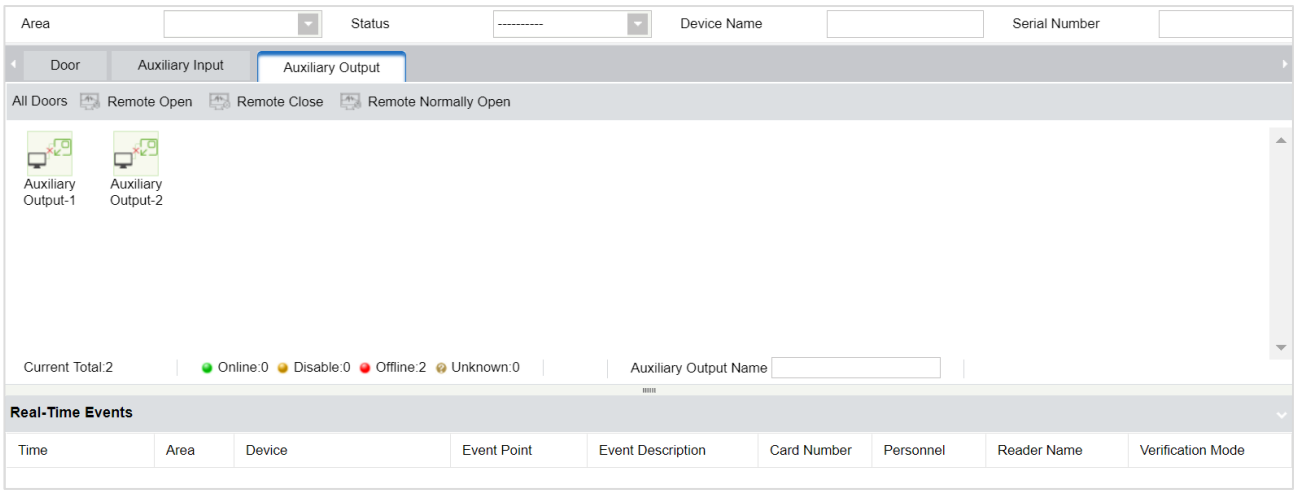
2. Додатковий вхід

Він відстежує поточні події допоміжного входу в режимі реального часу.



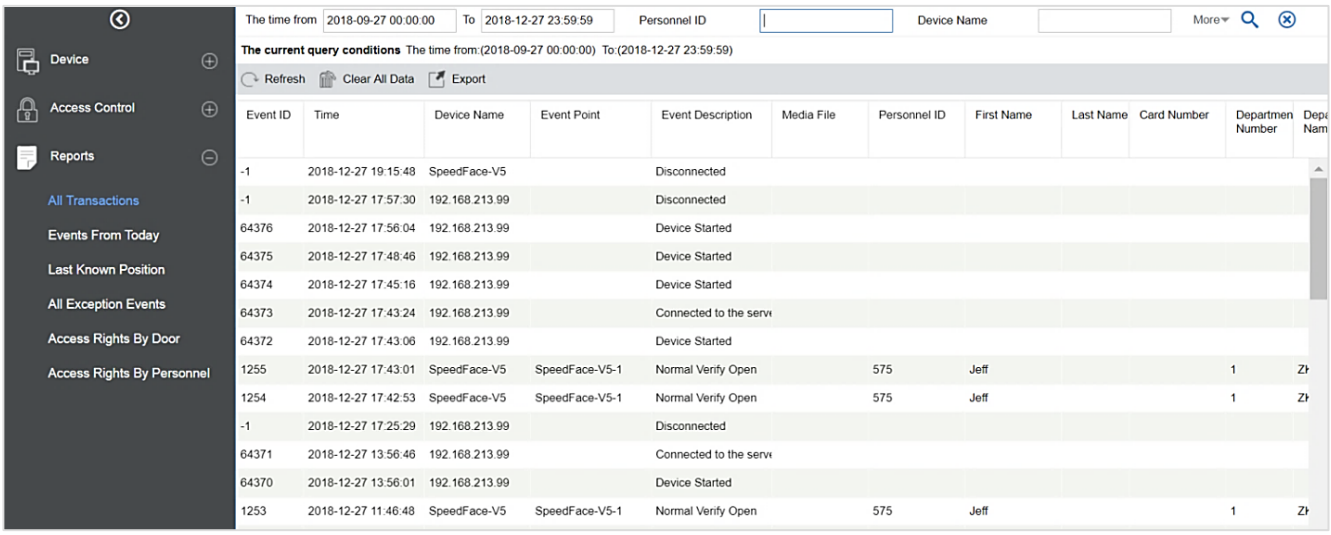
3. Додатковий вихід

Тут ви можете виконувати функції дистанційного відкриття, дистанційного закриття, дистанційного NO.



5.8 Звіти

Оскільки обсяг даних про контроль подій управління доступом великий, ви можете переглянути конкретні події управління доступом за допомогою умов запиту. За замовчуванням система відображає транзакції за останні три місяці. Натисніть [**Reports**] (Звіти) > [**All Transactions**] (Всі транзакції), щоб переглянути всі транзакції.



Media File (Медіафайл): Ви можете переглянути або завантажити фотографії та відео.

Clear All Data (Очистити всі дані): Ця функція використовується для очищення всіх транзакцій. Натисніть [**Clear All Data**] (Очистити всі дані). У спливаючому вікні натисніть OK, щоб видалити всі транзакції.

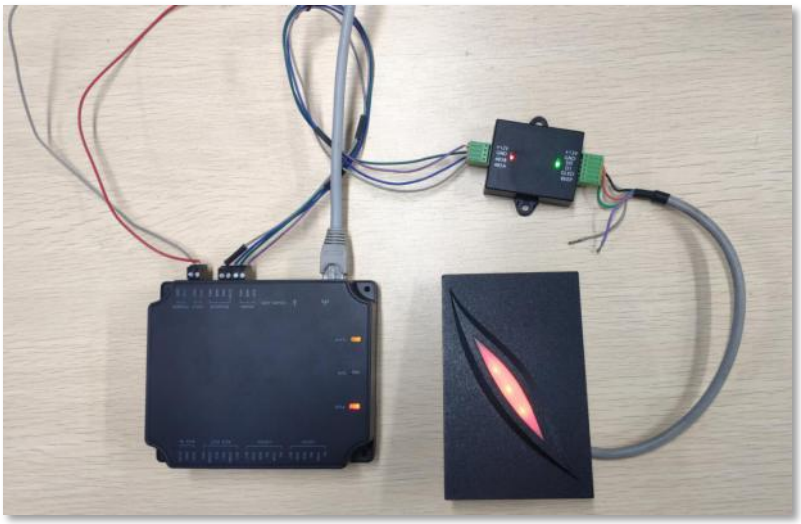
Export (Експорт): Ви можете експортувати всі транзакції у форматах Excel, PDF та CSV.

All Transactions

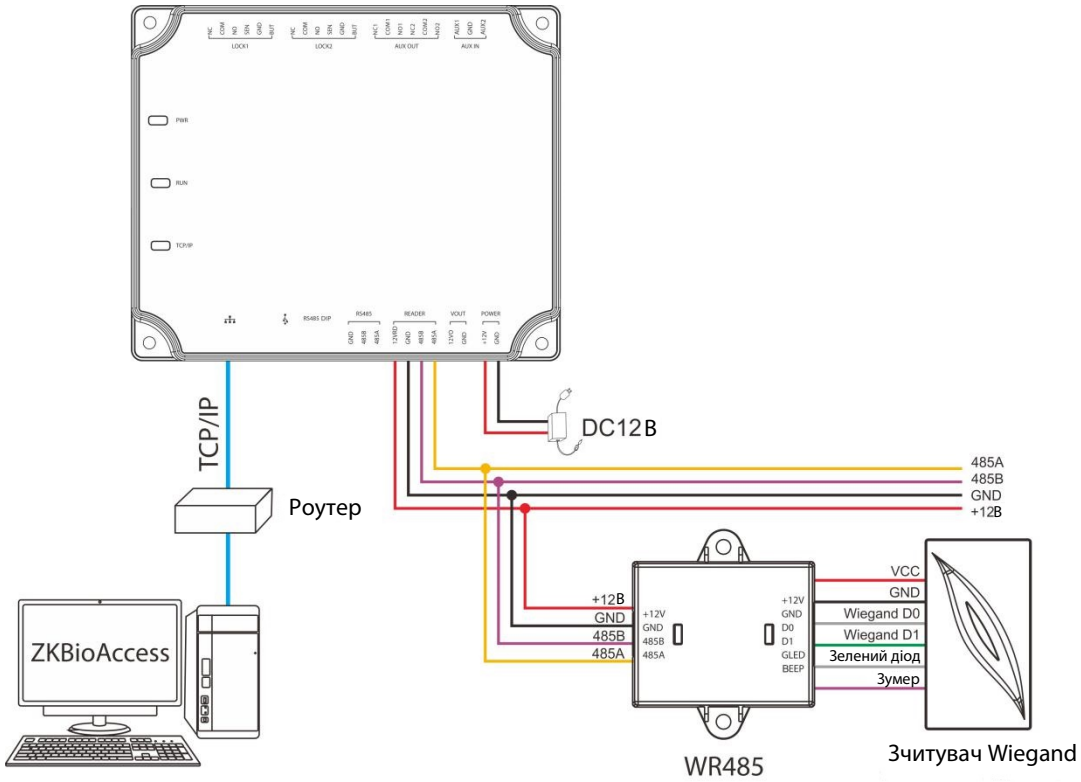
Event ID	Time	Device Name	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department Number	Department Name	Reader Name	Verification Mode	Area Name	Remark
-1	2018-12-27 19:15:48	SpeedFace-V5		Disconnected							Other	Other	Area Name	
-1	2018-12-27 17:57:30	192.168.213.99		Disconnected							Other	Other	Area Name	
64376	2018-12-27 17:56:04	192.168.213.99		Device Started							Other	Other	Area Name	
64375	2018-12-27 17:48:46	192.168.213.99		Device Started							Other	Other	Area Name	
64374	2018-12-27 17:45:16	192.168.213.99		Device Started							Other	Other	Area Name	
64373	2018-12-27 17:43:24	192.168.213.99		Connected to the server							Other	Other	Area Name	
64372	2018-12-27 17:43:06	192.168.213.99		Device Started							Other	Other	Area Name	
1255	2018-12-27 17:43:01	SpeedFace-V5	SpeedFace-V5-1	Normal Verify Open	575	Jeff			1	ZKTeco	SpeedFace-V5-1-Out	Face	Area Name	
1254	2018-12-27 17:42:53	SpeedFace-V5	SpeedFace-V5-1	Normal Verify Open	575	Jeff			1	ZKTeco	SpeedFace-V5-1-Out	Face	Area Name	
-1	2018-12-27 17:25:29	192.168.213.99		Disconnected							Other	Other	Area Name	
64371	2018-12-27 13:56:46	192.168.213.99		Connected to the server							Other	Other	Area Name	
64370	2018-12-27 13:56:01	192.168.213.99		Device Started							Other	Other	Area Name	
1253	2018-12-27 11:46:48	SpeedFace-V5	SpeedFace-V5-1	Normal Verify Open	575	Jeff			1	ZKTeco	SpeedFace-V5-1-Out	Face	Area Name	

Додаток 1

Демонстрація підключення C2-260, WR485 та зчитувача Wiegand

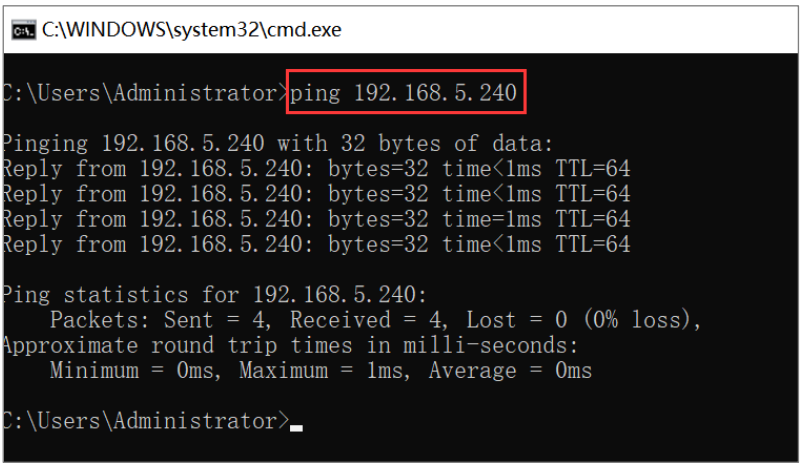


Крок 1: Підключіть C2-260, WR485 і зчитувач Wiegand згідно з наведеною нижче схемою.



Крок 2: Увімкніть C2-260 і підключіться до мережі.

Крок 3: Спробуйте пінгувати C2-260, щоб перевірити, чи працює мережа.

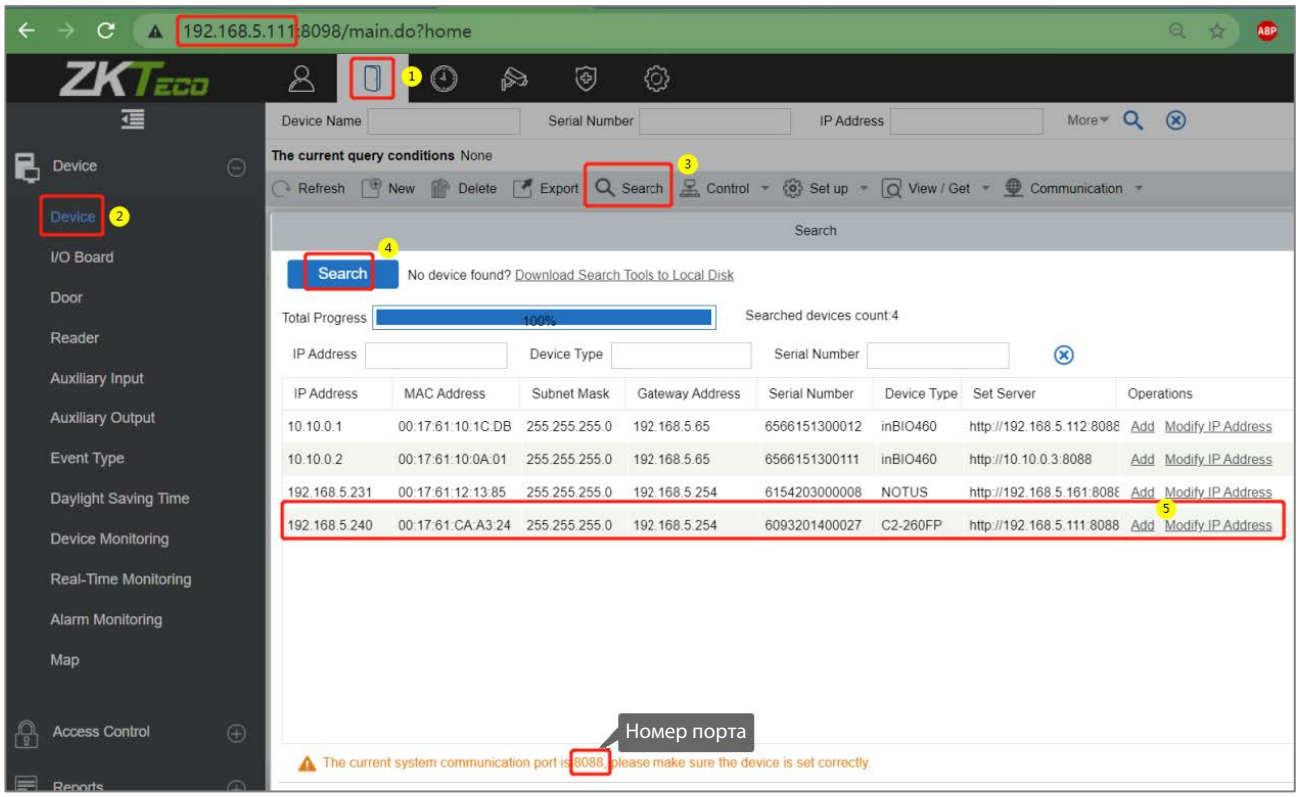


1) Одночасно натисніть [**Windows + R**] на комп'ютері, щоб відкрити вікно запуску і введіть «cmd».

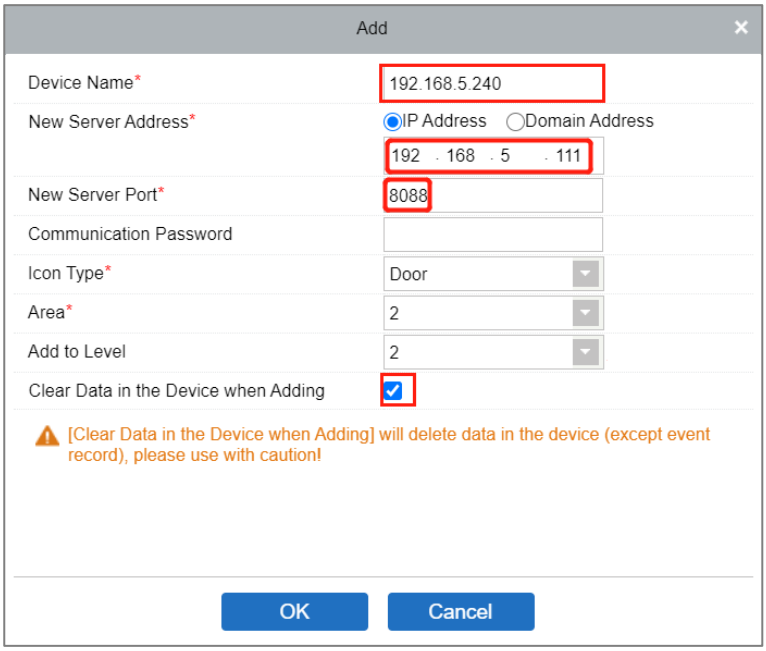
2) Введіть "ping device IP address", щоб пінгувати C2-260, щоб перевірити, чи встановлено зв'язок. Як показано на малюнку вище.

Крок 4: Додавання пристрою до програмного забезпечення **ZKBioAccess IVS**.

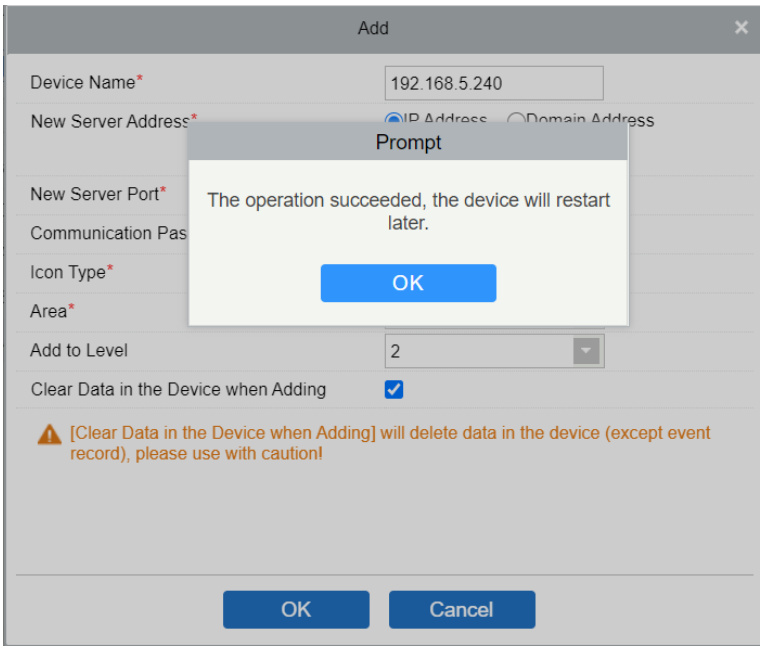
1) Відкрийте програмне забезпечення ZKBioAccess IVS і натисніть **Access** (Доступ) > **Device** (Пристрій) > **Search** (Пошук), щоб увійти в інтерфейс пошуку. Натисніть **Search** (Пошук), щоб здійснити пошук пристрою.
2) Після завершення пошуку номер порту буде відображено в нижній частині інтерфейсу пошуку. На наступному малюнку ми бачимо IP-адресу сервера (**192.168.5.111**) та номер порту (**8088**).



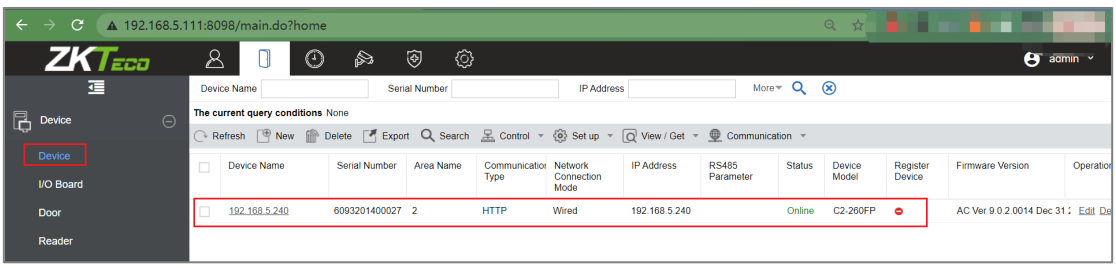
3) Натисніть **Add** (Додати) у списку пошуку. Потім введіть адресу сервера (**192.168.5.111**), порт (**8088**) та інші параметри у спливаючому вікні.



4) Натисніть **OK**, щоб зберегти налаштування. У разі успішного додавання пристрою з'явиться наступне вікно.

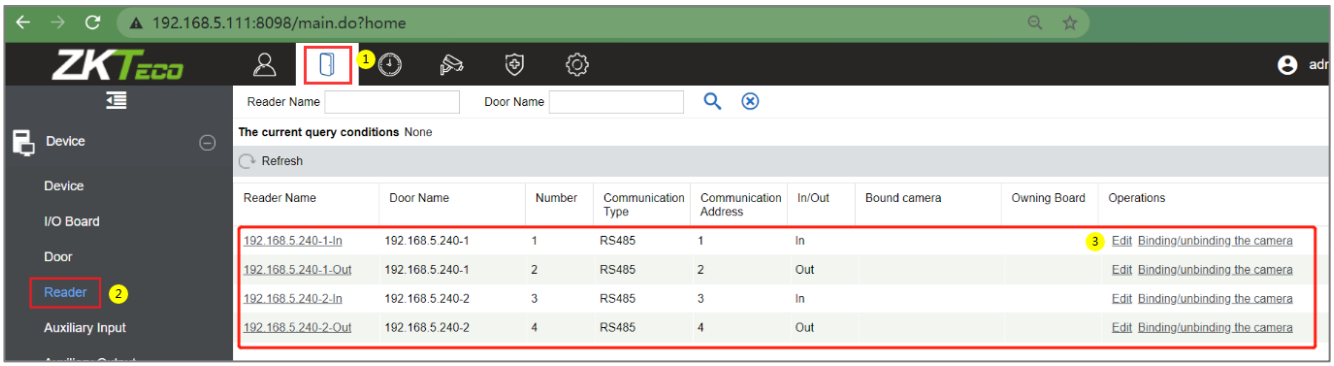


5) Після завершення, пристрій, доданий до програми, буде відображено у списку пристроїв.



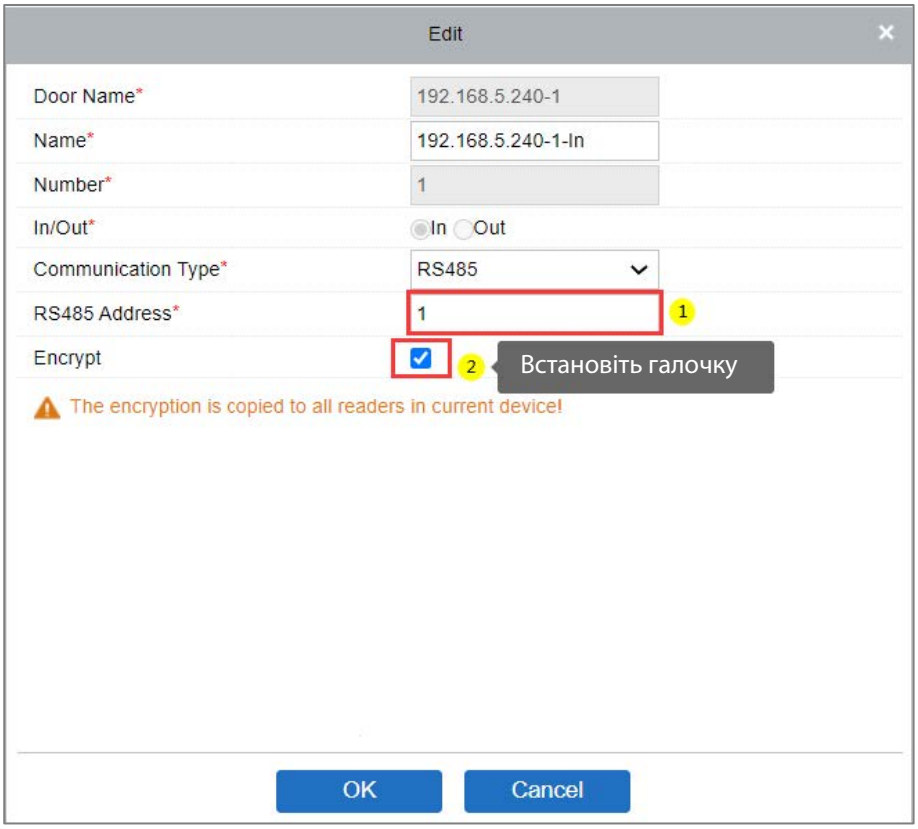
Крок 5: Налаштування параметрів зчитувача Wiegand.

1) Після додавання C2-260 до програмного забезпечення натисніть **Access** (Доступ) > **Device** (Пристрій) > **Reader** (Зчитувач), щоб переглянути зчитувач.



2) Встановіть адресу WR485 як **1**, встановивши DIP-перемикач № 1 у положення **ON**. Це означає, що зчитувач wiegand, який підключається через WR485, буде встановлений як зчитувач Door1(In) (**Примітка**: Рекомендується встановлювати адреси WR485 за допомогою DIP-перемикача перед подачею живлення).

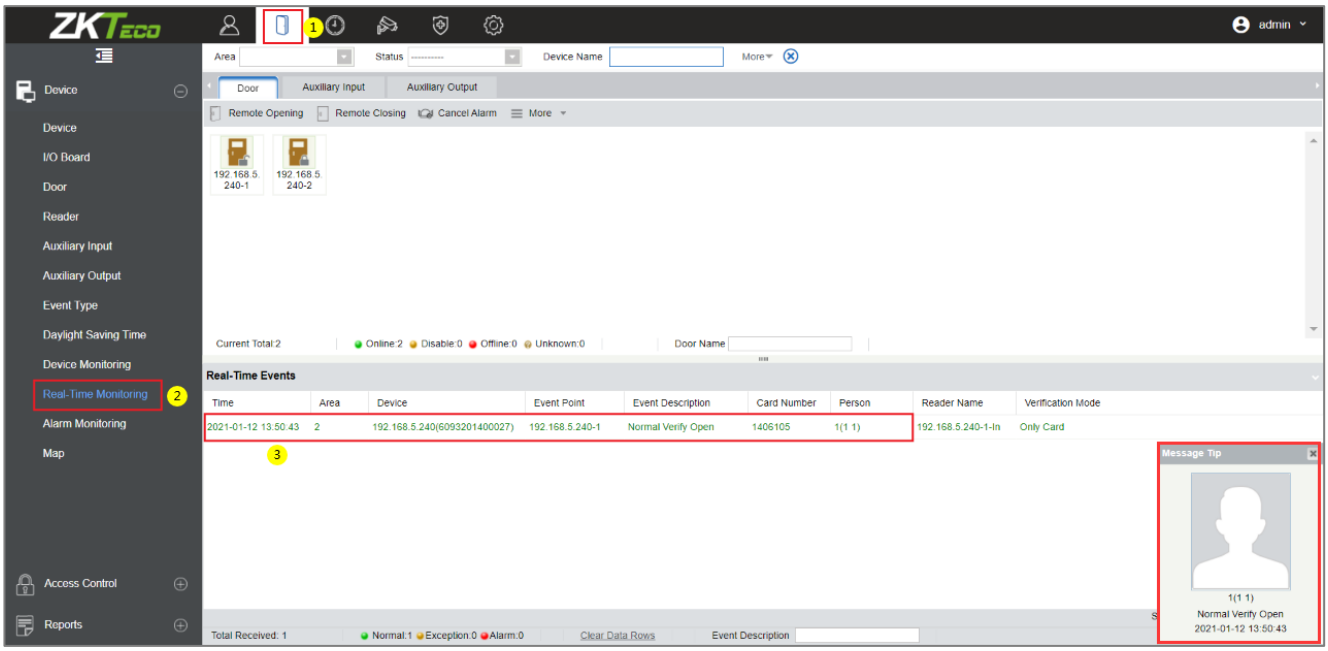
3) Натисніть **Edit** (Редагувати) «192.168.5.240-1-In», щоб встановити параметри. Оскільки WR485 працює в режимі шифрування, вам потрібно встановити галочку шифрування. Щоб зчитувач Wiegand можна було нормально використовувати. Як показано на наступному малюнку.



Крок 6: Перегляд записів у реальному часі.

Після успішного налаштування, коли співробітник проведе карткою по зчитувачу Wiegand, подію в режимі реального часу можна буде переглянути на сторінці **Real-Time Monitoring** (Моніторинг в реальному часі).

Натисніть **Access** (Доступ) > **Device** (Пристрій) > **Real-Time Monitoring** (Моніторинг у реальному часі) , щоб переглянути записи.



Додаток 2

Заява про право на конфіденційність

Шановні клієнти,

Дякуємо, що обрали цей гібридний продукт біометричного розпізнавання, розроблений та виготовлений компанією ZKTeco. Як всесвітньо відомий постачальник основних технологій біометричного розпізнавання, ми постійно розробляємо і досліджуємо нові продукти, а також прагнемо дотримуватися законів про конфіденційність кожної країни, в якій продається наша продукція.

Ми заявляємо, що

1. Всі наші цивільні пристрої розпізнавання відбитків пальців фіксують лише характеристики, а не зображення відбитків, і не передбачають захисту приватності.
2. Жодна з характеристик відбитків пальців, які ми фіксуємо, не може бути використана для відновлення зображення оригінального відбитка пальця і не передбачає захисту конфіденційності.
3. Як постачальник цього пристрою, ми не несемо жодної прямої чи опосередкованої відповідальності за будь-які наслідки, які можуть виникнути внаслідок використання вами цього пристрою.
4. Якщо ви хочете оскаржити порушення прав людини або питань конфіденційності, пов'язаних з використанням нашого продукту, будь ласка, зверніться безпосередньо до вашого дилера.

Інші наші пристрої для зняття відбитків пальців для правоохоронних органів або інструменти для розробки можуть знімати оригінальні зображення відбитків пальців громадян. Щодо того, чи є це порушенням ваших прав, будь ласка, зверніться до вашого уряду або кінцевого постачальника пристрою. Як виробник пристрою, ми не несемо жодної юридичної відповідальності.

Примітка:

Китайське законодавство містить наступні положення про особисту свободу громадян:

1. Не допускається незаконний арешт, затримання, обшук або посягання на особисту недоторканність.
2. Особиста гідність пов'язана з особистою свободою і не може бути порушена.
3. Не допускається посягання на житло громадянина.
4. Право громадянина на спілкування і таємницю цього спілкування охороняється законом.

Наостанок ми хотіли б ще раз підкреслити, що біометричне розпізнавання - це передова технологія, яка неодмінно буде використовуватися в електронній комерції, банківській, страховій, судовій та інших галузях у майбутньому. Щороку світ зазнає значних збитків через незахищеність паролів. Біометричні продукти слугують для захисту вашої ідентичності в середовищах з високим рівнем безпеки.

Екологічно чисте виробництво

Термін «екологічно безпечний період експлуатації» означає період часу, протягом якого цей виріб не виділяє токсичних або небезпечних речовин, якщо він використовується відповідно до умов, викладених у цьому посібнику.

Екологічний період експлуатації, зазначений для цього виробу, не включає акумуляторні батареї та інші компоненти, які легко зношуються і підлягають періодичній заміні. Екологічно безпечний термін експлуатації акумулятора становить 5 років.

Небезпечні або токсичні речовини та їхня кількість

Назва компоненту	Небезпечна/токсична речовина/елемент					
	Свинець (Pb)	Меркурій (Hg)	Кадмій (Cd)	Шестивалентний хром (Cr6+)	Полібромовані дифеніли (PBB)	Полібромовані дифенілові ефіри (PBDE)
Резистор мікросхеми	×	○	○	○	○	○
Конденсатор мікросхеми	×	○	○	○	○	○
Індуктор мікросхеми	×	○	○	○	○	○
Діод	×	○	○	○	○	○
Компонент ESD	×	○	○	○	○	○
Дзвінок	×	○	○	○	○	○
Адаптер	×	○	○	○	○	○
Гвинти	○	○	○	×	○	○

○ вказує на те, що загальна кількість токсичних речовин у всіх однорідних матеріалах є нижчою за межу, визначену стандартом SJ/T 11363-2006.

× іпоказує, що загальна кількість токсичних речовин у всіх однорідних матеріалах перевищує межу, визначену стандартом SJ/T 11363-2006.

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