Доступ Standalone

Посібник користувача

V1.0.1

Передмова

Загальні відомості

Цей посібник представляє функції та операції Access Standalone. Уважно прочитайте перед використанням пристрою та зберігайте посібник для подальшого використання.

Інструкції з безпеки

У посібнику можуть з'являтися наступні сигнальні слова.

Сигнальні слова	Значення
DANGER	Вказує на високий потенційний ризик, який, якщо його не уникнути, призведе до смерті або серйозної травми.
WARNING	Вказує на середній або низький потенційний ризик, який, якщо його не уникнути, може призвести до незначних або помірних травм.
CAUTION	Вказує на потенційний ризик, який, якщо його не уникнути, може призвести до ушкодження майна, втрати даних, зниження продуктивності або непередбачуваних результатів.
TIPS	Надає методи, які допоможуть вам вирішити проблему або заощадити час.
NOTE	Надає додаткову інформацію як доповнення до тексту.

Історія змін

Версія	Зміст ревізії	Час випуску
V1.0.1	Оновлено конфігурації на платформі.	Листопад 2022
V1.0.0	Перше видання.	Січень 2022

Повідомлення про захист конфіденційності

Як користувач пристрою або контролер даних, ви можете збирати особисті дані інших осіб, такі як їх обличчя, відбитки пальців та номерний знак автомобіля. Вам потрібно дотримуватись місцевих законів і нормативних актів про захист конфіденційності, щоб захистити законні права та інтереси інших людей, вживаючи заходів, які включають, але не обмежуються: наданням чіткої та видимої ідентифікації, щоб повідомити людей про наявність зони спостереження та надати необхідну контактну інформацію.

Про посібник

- Посібник призначений лише для довідки. Можуть бути незначні відмінності між посібником і продуктом.
- Ми не несемо відповідальності за збитки, понесені внаслідок експлуатації продукту способами, які не відповідають інструкції.
- Інструкція буде оновлена відповідно до останніх законів та нормативних актів відповідних юрисдикцій.

  Для отримання детальної інформації дивіться паперову інструкцію користувача, використовуйте наш CD-ROM, скануйте QR-код або відвідайте
  наш офіційний веб-сайт. Інструкція призначена лише для довідки. Можуть бути незначні відмінності між електронною версією та паперовою версією.

- Усі дизайни та програмне забезпечення можуть бути змінені без попереднього письмового повідомлення. Оновлення продукту
  може призвести до появи деяких відмінностей між фактичним продуктом та посібником. Будь ласка, зв'яжіться з обслуговуванням клієнтів для отримання останньої програми та додаткової документації.

- Можливі помилки в друку або відхилення в описі функцій, операцій
  та технічних даних. Якщо виникають будь-які сумніви або спори, ми залишаємо за собою право на остаточне пояснення.
- Оновіть програмне забезпечення для читання або спробуйте інше популярне програмне забезпечення для читання, якщо посібник (у форматі PDF) не може бути відкритий.

- Усі торгові марки, зареєстровані торгові марки та назви компаній у посібнику є власністю їх відповідних власників.

- Будь ласка, відвідайте наш веб-сайт, зв'яжіться з постачальником або обслуговуванням клієнтів, якщо виникають будь-які проблеми під час використання пристрою.

- Якщо виникає будь-яка невизначеність або суперечка, ми залишаємо за собою право на остаточне пояснення.

Важливі запобіжні заходи та попередження

Цей розділ містить інформацію про правильне використання Access Standalone, запобігання небезпеці та запобігання шкоді майну. Уважно прочитайте перед використанням Access Standalone та дотримуйтесь вказівок під час його використання.

Вимоги до транспортування

Транспорт, використовуйте та зберігайте Access Standalone за дозволеними умовами вологості та температури

Вимоги до зберігання

Зберігайте Access Standalone за дозволеними умовами вологості та температури.

Вимоги до встановлення

 **WARNING**

- Не підключайте адаптер живлення до Access Standalone, поки адаптер увімкнений.
- Суворо дотримуйтесь місцевих електричних норм безпеки та стандартів. Переконайтеся, що напруга в навколишньому середовищі стабільна та відповідає вимогам живлення Access Controller.
- Не підключайте Access Standalone до двох або більше видів джерел живлення, щоб уникнути пошкодження Access Standalone.
- Неправильне використання батареї може призвести до пожежі або вибуху.

- Персонал, що працює на висоті, повинен вжити всіх необхідних заходів для забезпечення особистої безпеки, включаючи носіння шолома та страхувальних поясів.
- Не розміщуйте Access Standalone в місцях, що піддаються прямому сонячному світлу або поблизу джерел тепла.
- Тримайте Access Standalone подалі від вологи, пилу та сажі.
- Встановіть Access Standalone на стабільній поверхні, щоб запобігти його падінню.
- Встановіть Access Standalone у добре провітрюваному місці та не закривайте його вентиляцію.
- Використовуйте адаптер або блок живлення, наданий виробником.
- Використовуйте кабелі живлення, які рекомендовані для регіону та відповідають номінальним характеристикам потужності.
- Блок живлення повинен відповідати вимогам ES1 стандарту IEC 62368-1 і не перевищувати PS2. Зверніть увагу, що вимоги до блоку живлення підлягають маркуванню Access Stan dalone.
- Access Standalone є електричним приладом класу I. Переконайтеся, що блок живлення Access St andalone підключений до електричної розетки з захисним заземленням.

Вимоги до експлуатації

- Перевірте, чи правильний блок живлення перед використанням.

- Не виймайте кабель живлення з боку Access Standalone, поки адаптер уві мкнений.
- Використовуйте Access Standalone в межах номінального діапазону вхідної та вихідної потужності.
- Використовуйте Access Standalone за дозволеними умовами вологості та температури.
- Не падайте або не розбризкуйте рідину на Access Standalone, і переконайтеся, що на Access Standalone немає предметів, наповнених рідиною, щоб запобігти потраплянню рідини всередину.
- Не розбирайте Access Standalone без професійних інструкцій.

Зміст

1 Огляд продукту

Водонепроникний автономний доступ призначений для управління доступом у контрольованій зоні.

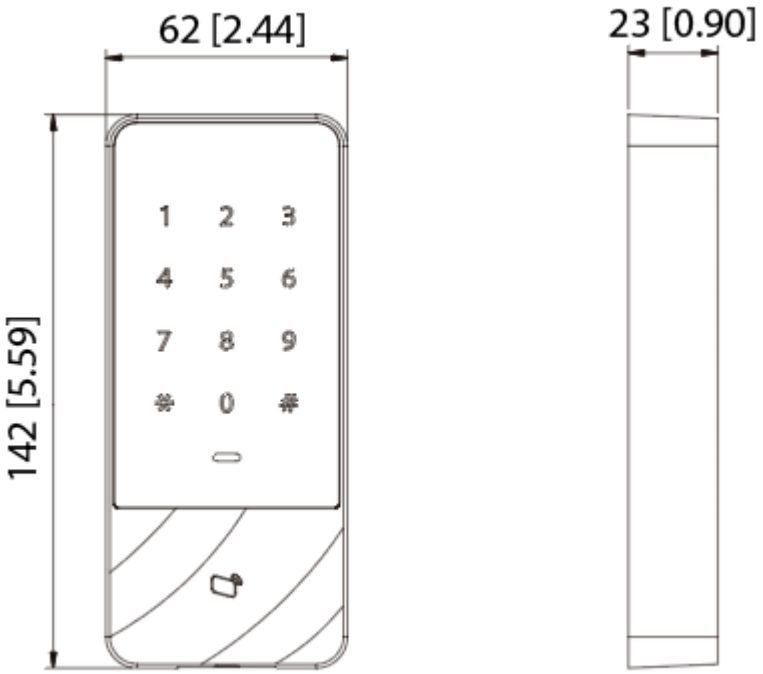
З акуратним зовнішнім виглядом та класом водонепроникності IPX6, його можна використовувати на вулиці.

Він має такі основні характеристики:

- Підтримує сенсорну клавіатуру та протокол TCP/IP.
- Підтримує 30,000 дійсних карток і може зберігати до 60,000 записів.
- Підтримує розблокування дверей за допомогою картки, картки + пароля та ідентифікатора користувача + пароля.
- Підтримує сигналізацію про понаднормову роботу, сигналізацію про вторгнення, сигналізацію про примус і сигналізацію про підробку.
- Підтримує гостьову картку, картку примусу, картку зі списком заборонених/дозволених та патрульну картку.
- Підтримує 128 груп розкладів, 128 груп періодів і 128 груп святкових періодів.

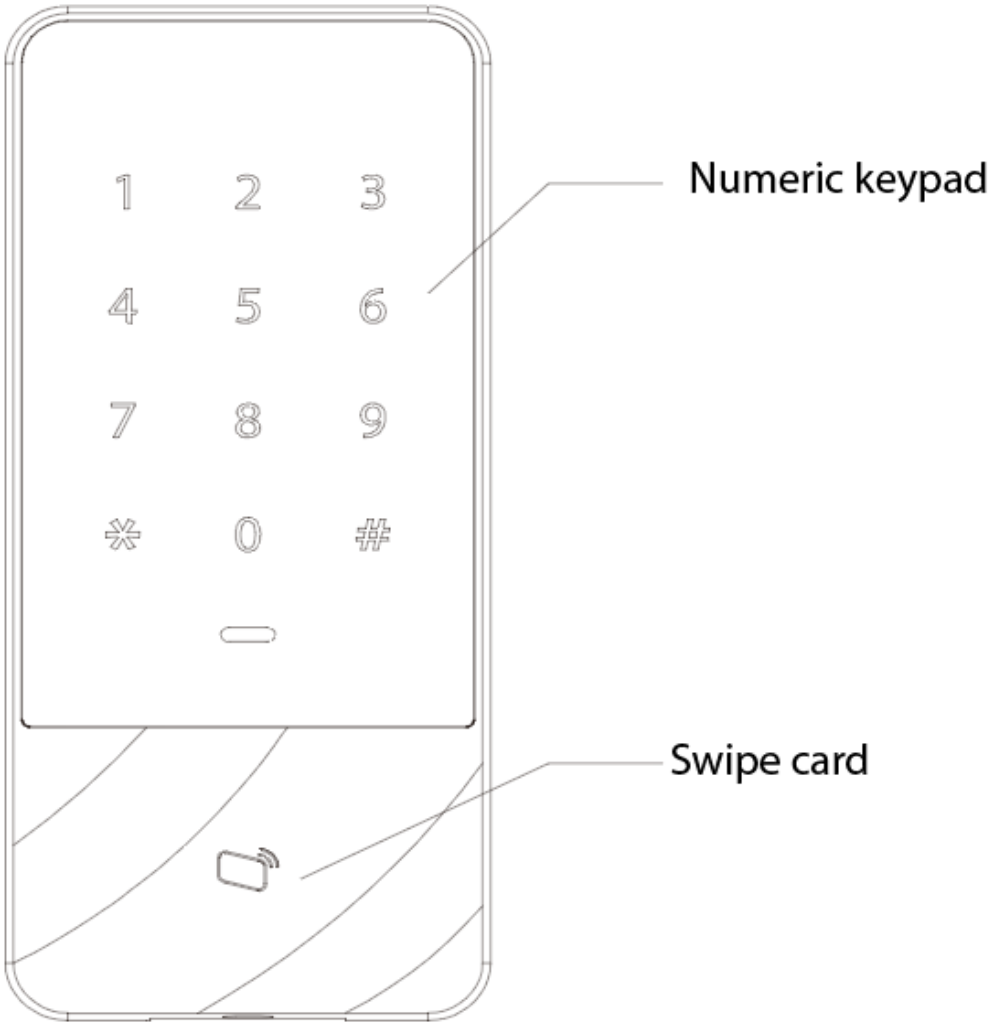
1.1 Розміри

Рисунок 1-1 Розміри (мм [дюйм])



1.2 Структура

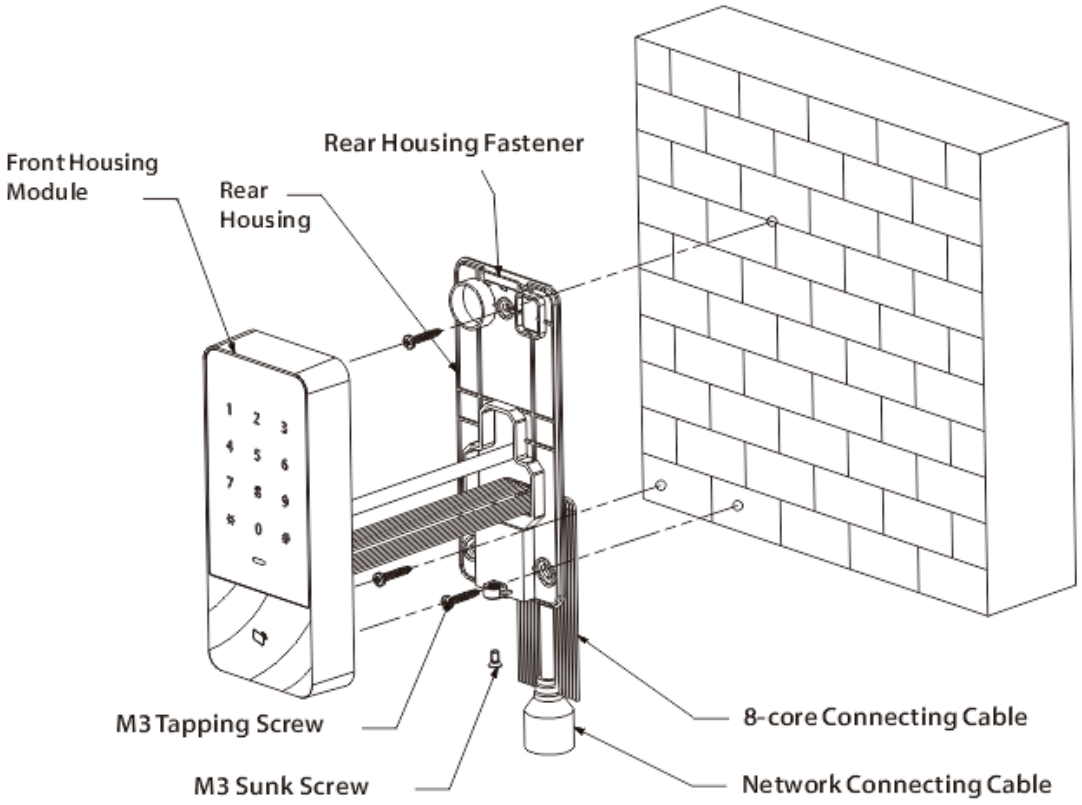
Рисунок 1-2 Структура



2 Встановлення

Фонові дані

Рисунок 2-1 Встановлення



Процедура

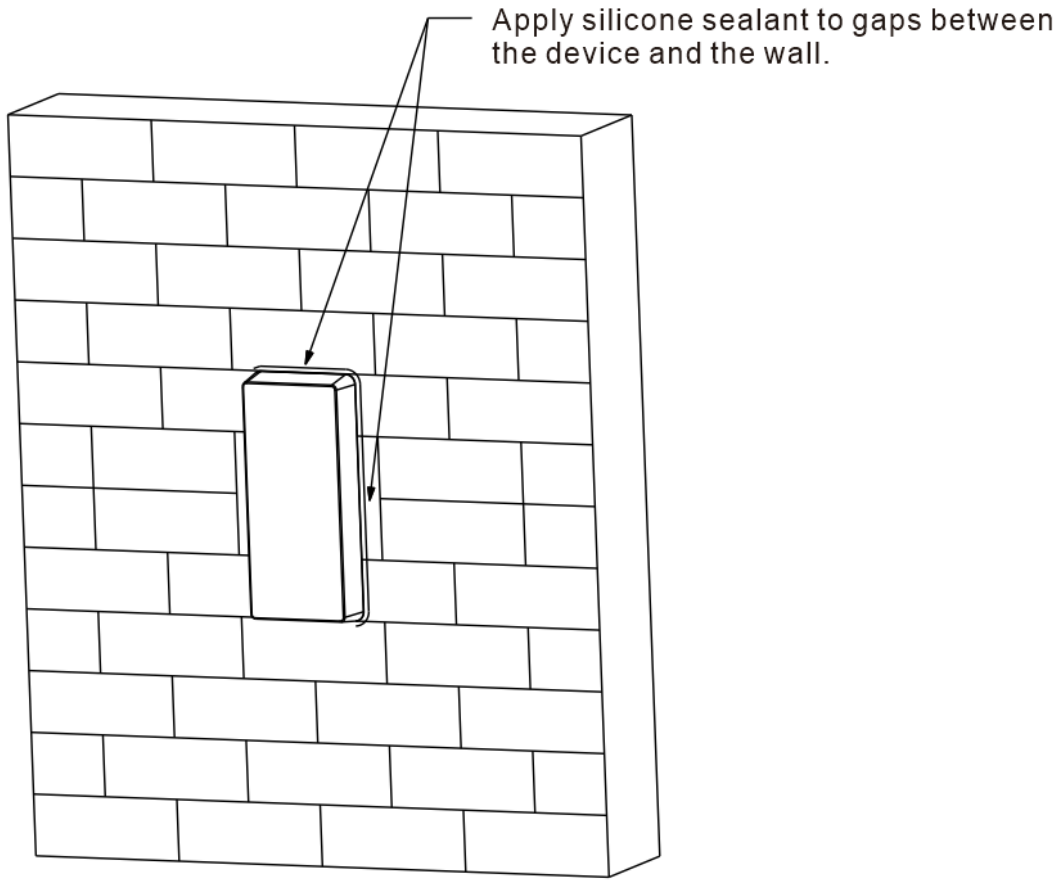
Крок 1 Закріпіть задній корпус на стіні за допомогою гвинтів M3; залиште простір для проводки для мережевого підключення між заднім корпусом і стіною.

Крок 2 Пропустіть мережевий підключаючий кабель і два 8-провідні підключаючі кабелі через щілину заднього корпусу та стіни, а потім затягніть гвинти M3.

Крок 3 Прикріпіть верхню частину модуля переднього корпусу до кріплення заднього корпусу, а потім затягніть втоплені гвинти M3 внизу, щоб зафіксувати їх.

Крок 4 Нанесіть силіконовий герметик на щілини між пристроєм і стіною.

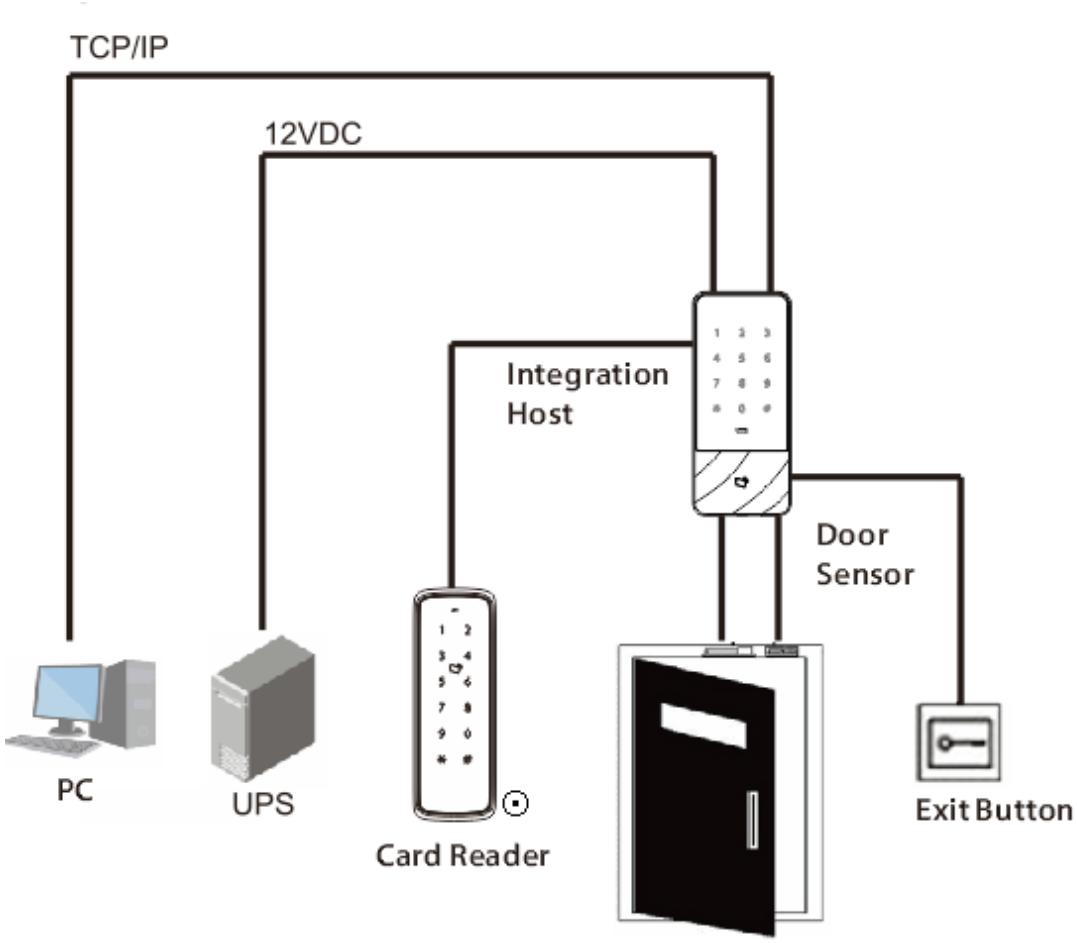
Рисунок 2-2 Нанесення силікону



3 Схема мережі

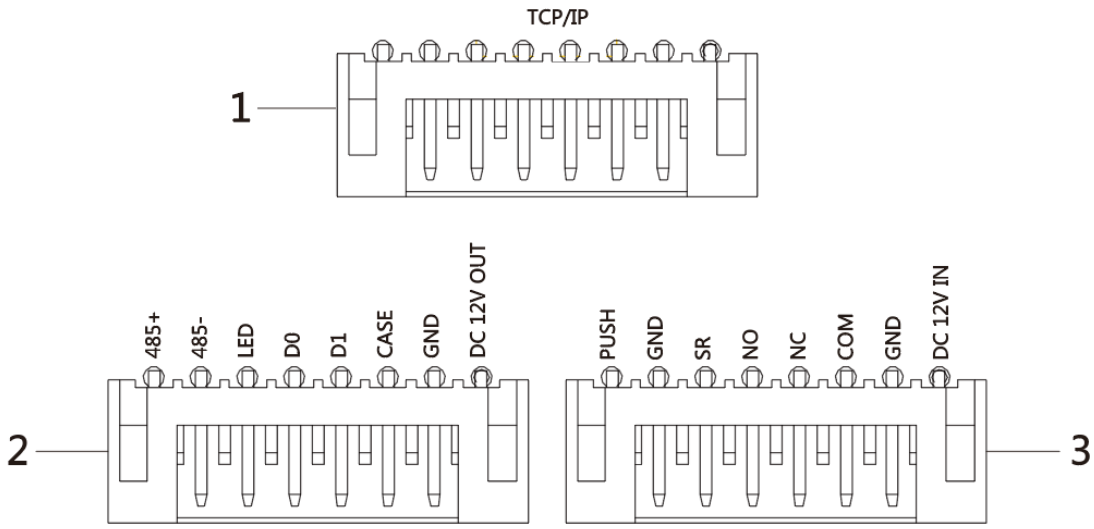
Схема мережі базової системи контролю доступу показана нижче.

Рисунок 3-1 Схема мережі



4 Проводка

Рисунок 4-1 Проводка



Таблиця 4-1 Опис проводки

№	Порт	Опис
1	RJ45	TCP/IP (мережевий порт).
2	485+	Підключає зчитувач карт RS-485.
	485-	
	LED	Підключає дріт LED зчитувача карт для передачі індикаторних сигналів.
	D0	Підключає зчитувач карт Wiegand.
	D1	
	КОРПУС	Підключає сигнали захисту від несанкціонованого доступу зчитувача карт.
	GND	Підключає заземлювальний дріт.
	12 VDC OUT	12 VDC живлення зчитувача.
3	PUSH	Підключає кнопку виходу з дверей.
	GND	Підключає заземлювальний провід, який спільний для датчика дверей та кнопки виходу з дверей.
	SR	Підключає датчик дверей.
	NO	Підключає NO порт замка дверей.
	NC	Підключає NC порт замка дверей.
	COM	Підключає COM-порт замка дверей.
	GND	Підключає заземлювальний провід.
	12 VDC ВХІД	Вхід живлення 12 VDC.

5 Локальна конфігурація

5.1 Головне меню

Процедура

Крок 1 Доторкніться до екрану, щоб розбудити Access Standalone, і натисніть #.

Індикатор світиться синім, і цифрова клавіатура вмикається, що означає, що пристрій розбуджено.

Крок 2 Введіть пароль адміністратора, а потім натисніть **#**

Крок 3 Після входу в головне меню ви можете натискати цифрові клавіші для налаштування параметрів.

Таблиця 5-1 Опис головного меню

Цифрова клавіша	Опис
0	Змінити пароль адміністратора.
1	Додати користувачів.
2	Видалити користувачів.
3	Встановити режими розблокування.
4	Встановити час утримання реле замка дверей.
5	Встановіть робочий режим.
6	Увімкніть сенсор дверей.
9	Відновити заводські налаштування.

- Пароль адміністратора за замовчуванням - 88888888.
- Індикатор світиться синім, що означає, що ви успішно ввійшли в головне меню.
- Індикатор світиться червоним. Після трьох звукових сигналів, індикатор світиться синім, що означає, що введено неправильний пароль.
- Після налаштувань натисніть *****, щоб повернутися на попередню сторінку.
- У головному меню натисніть *****, щоб вийти з головного меню.

5.2 Зміна пароля адміністратора

Регулярно змінюйте пароль адміністратора для покращення безпеки облікового запису.

Процедура

Крок 1 Увійдіть у головне меню.

Крок 2 натисніть **0** та **#**

Крок 3 Введіть новий пароль і натисніть **#**.

Крок 4 Підтвердіть новий пароль, а потім натисніть **#**

- Індикатор світла горить зеленим, і сигналізація звучить один раз, що означає, що пароль успішно змінено.
- Індикатор світла горить червоним, і сигналізація звучить три рази, що означає, що пароль не змінено.

5.3 Додавання користувачів

Додайте користувача та асоціюйте його з карткою.

Процедура

Крок 1 Увійдіть у головне меню.

Крок 2 натисніть **1** та **#** для додавання користувача.

1) Додати ідентифікатор користувача: введіть ідентифікатор користувача, а потім натисніть **#**

Якщо ідентифікатор користувача вже існує, його не можна додати.

2) Додати картку: проведіть карткою, а потім натисніть **#**

Якщо ви не хочете додавати картку, натисніть **#** , щоб пропустити цей крок.

3) Додати пароль: введіть пароль і натисніть **#**

- Якщо ви не хочете встановлювати пароль, натисніть **#** , щоб пропустити цей крок.
- Встановіть пароль, якщо ви не додали номер картки. Якщо пароль не встановлено, користувача не можна додати.

Крок 3 Повторіть крок 2, щоб додати більше користувачів.

Індикатор світла горить зеленим кольором, і сигналізація звучить один раз, що означає, що користувач успішно доданий. Індикатор світла горить червоним кольором, і сигналізація звучить 3 рази, що означає невдачу при додаванні користувача.

Після додавання користувачів система залишається на екрані Додати користувача . Натисніть ***** щоб повернутися до головного меню.

5.4 Видалення користувачів

Видалити користувачів, і вони не матимуть дозволу на відкриття дверей.

Процедура

Крок 1 Увійдіть у головне меню.

Крок 2 натисніть **2** і **#**

- Просто проведіть карткою і натисніть **#** , щоб видалити користувача.
- Введіть ідентифікатор користувача і натисніть **#** , щоб видалити користувача.
- Введіть 0000 і натисніть **#** , щоб видалити всіх користувачів.

- Індикатор світла горить зеленим кольором, і сигналізація звучить один раз, що означає, що користувач успішно видалений. Індикатор світла горить червоним кольором, і сигналізація звучить три рази, що означає, що користувача не вдалося успішно додати. Після видалення система залишається на Видалити користувача екран. натисніть * щоб повернутися до головного меню.

5.5 Налаштування режимів розблокування

Налаштуйте режими розблокування дверей, такі як розблокування за допомогою картки, картки + пароля та ідентифікатора користувача + пароля.

Процедура

Крок 1 Увійдіть у головне меню.

Крок 2 натисніть **3** та **#**

Крок 3 Виберіть режим розблокування.

Таблиця 5-2 Вибір режиму розблокування

Режим розблокування	**Метод розблокування**
Картка (за замовчуванням): натисніть **0** та **#**	Проведіть карткою по зчитувачу карток, щоб розблокувати двері.
Картка + пароль: Торкніться **1** і **#**	Проведіть картку, введіть пароль, а потім торкніться **#** , щоб відкрити двері.
Ідентифікатор користувача + пароль: Торкніться **2** і **#**	Введіть ідентифікатор користувача і торкніться **#** , а потім введіть пароль і торкніться **#** , щоб відкрити двері.

Після налаштувань система автоматично повертається до головного меню. Торкніться , щоб вийти з головного меню.

5.6 Налаштування тривалості відкриття дверей

Двері залишаються відкритими протягом визначеного часу, щоб люди могли пройти, перш ніж вони автоматично закриються знову.

Процедура

Крок 1 Увійдіть у головне меню.

Крок 2 торкніться **4** і **#**

Крок 3 Введіть час (від 1с до 600с) і торкніться **#** .

Після налаштування система автоматично повертається до головного меню. натисніть * для виходу з головного меню.

5.7 Налаштування робочих режимів

Standalone доступ має 2 робочі режими. Він може функціонувати як контролер доступу або зчитувач карт.

Процедура

Крок 1 Увійдіть у головне меню.

Крок 2 натисніть **5** і **#**

Крок 3 Виберіть робочий режим.

- Контролер доступу: контролює доступ після того, як люди підтвердять свою особу.

  Натисніть **0** і **#**

- Зчитувач: лише зчитує картку.

  Натисніть **1** і **#**

Після налаштувань система автоматично повертається до головного меню. Натисніть *****

, щоб вийти з головного меню.

5.8 Налаштування детектора дверей

Детектор дверей може контролювати стан дверей і спрацьовувати сигналізацію, коли двері відкриваються ненормально.

Процедура

Крок 1 Увійдіть у головне меню.

Крок 2 натисніть **6** і **#**

Крок 3 Виберіть, чи увімкнено датчик дверей.

- Вимкнути (за замовчуванням): натисніть **0** і **#**
- Увімкнути: натисніть **1** і **#**

Після налаштувань система автоматично повертається до головного меню. натисніть *****

, щоб вийти з головного меню.

5.9 Відновлення заводських налаштувань

Процедура

Крок 1 Увійдіть у головне меню.

Крок 2 натисніть **9** і **#**

Крок 3 Введіть **000** , а потім натисніть **#**

Після налаштувань Access Standalone автоматично перезапуститься.

Відновлення до заводських налаштувань призведе до втрати даних. Будь ласка, зверніть увагу.

6 Налаштування Smart PSS Lite

Цей розділ представляє, як керувати та налаштовувати Access Standalone через Smart PSS Lite. Ви також можете налаштувати правила обліку часу на платформі, такі як зміни, режими, графіки та інше. Для деталей дивіться посібник користувача Smart PSS Lite.

6.1 Встановлення та вхід в систему

Встановіть та увійдіть у Smart PSS Lite. Для деталей дивіться посібник користувача Smart PSS Lite.

Процедура

Крок 1 Отримайте програмний пакет Smart PSS Lite від технічної підтримки, а потім встановіть та запустіть програмне забезпечення відповідно до інструкцій.

Крок 2 Ініціалізуйте Smart PSS Lite, коли ви входите вперше, включаючи налаштування пароля та запитань безпеки.

Встановіть пароль для першого використання, а потім налаштуйте запитання безпеки, щоб скинути свій пароль, коли ви його забудете.

Крок 3 Введіть своє ім'я користувача та пароль, щоб увійти в Smart PSS Lite.

6.2 Додавання пристроїв

Вам потрібно додати Access Standalone до Smart PSS Lite. Ви можете додавати їх партіями або індивідуально.

6.2.1 Додавання індивідуально

Ви можете додати Access Standalone індивідуально, ввівши їх IP-адреси або доменні імена.

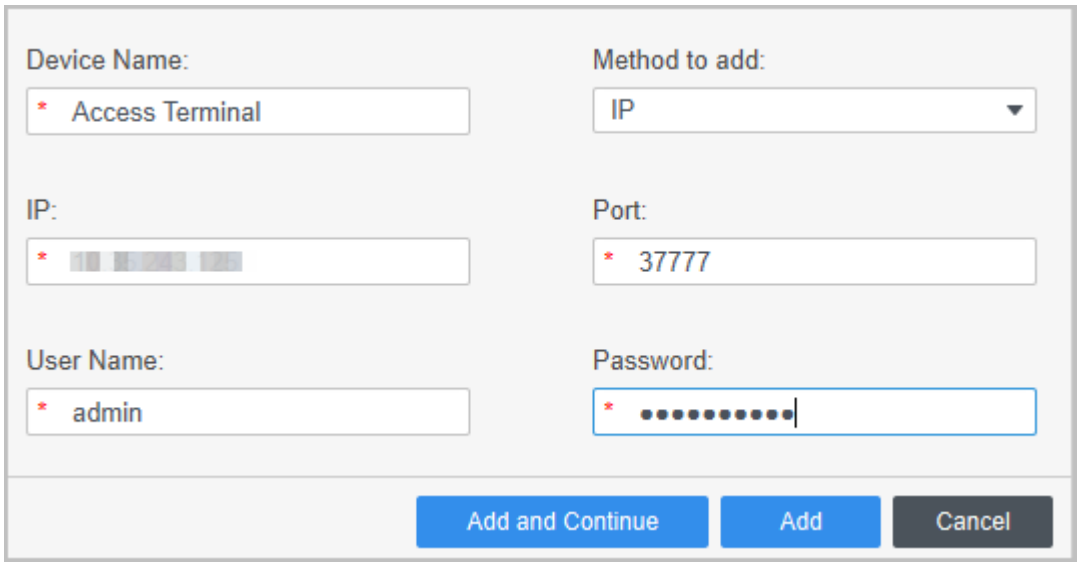
Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 Натисніть Диспетчер пристроїв і натисніть Додати

Крок 3 Введіть інформацію про пристрій.

Рисунок 6-1 Інформація про пристрій



Таблиця 6-1 Опис параметрів пристрою

Параметр	Опис
Назва пристрою	Введіть назву Access Standalone. Рекомендуємо вам назвати його на честь зони його встановлення.
Метод додавання	Виберіть **IP** для додавання Access Standalone, ввівши його IP адресу.
IP	Введіть IP-адресу Access Standalone.
Порт	Номер порту за замовчуванням - 37777.
Ім'я користувача/Пароль	Введіть ім'я користувача та пароль Access Terminal.

Крок 4 Натисніть . Додати

Доданий Access Standalone відображається на сторінці Пристрої . Ви можете натиснути Додати та Продовжити , щоб додати більше Access Standalone.

6.2.2 Додавання партіями

Рекомендуємо використовувати функцію автоматичного пошуку, коли ви хочете додати Access Standalone партіями. Переконайтеся, що Access Standalone, які ви додаєте, повинні бути в одному сегменті мережі.

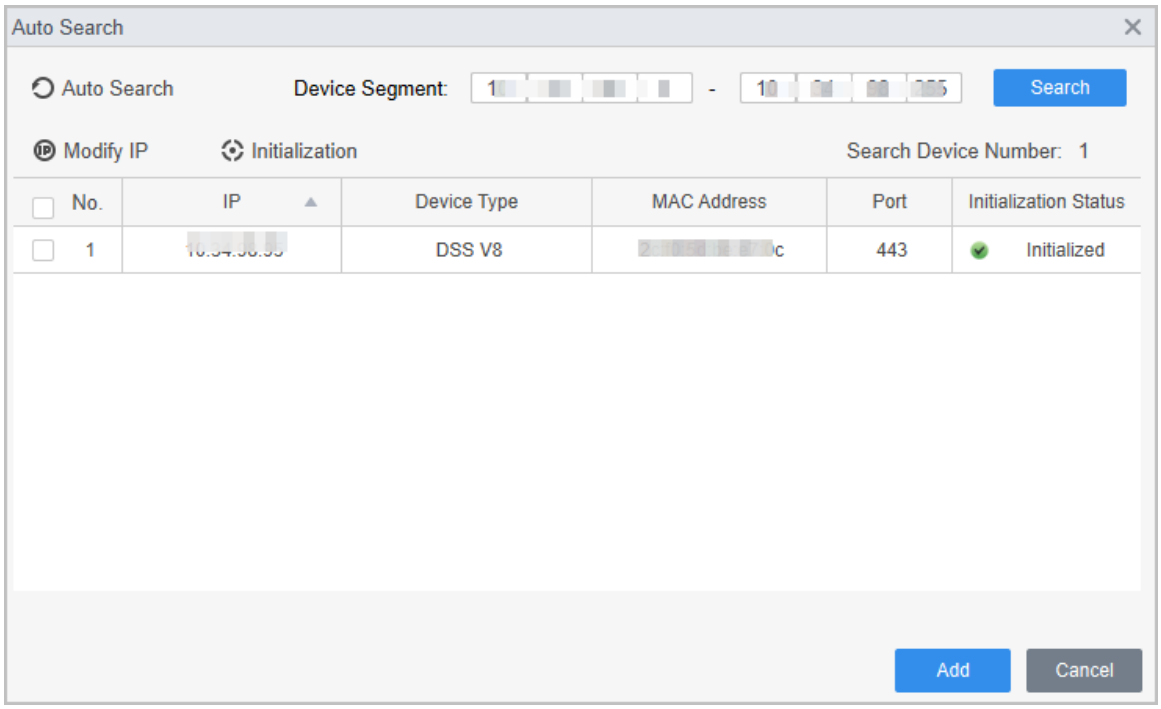
Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 Натисніть Менеджер пристроїв і шукайте пристрої.

- Натисніть Авто пошук , щоб шукати пристрої в одній локальній мережі.
- Введіть діапазон сегмента мережі, а потім натисніть Пошук.

Рисунок 6-2 Авто пошук



Список пристроїв буде відображено.

Виберіть пристрій, а потім натисніть Змінити IP , щоб змінити його IP-адресу.

Крок 3 Виберіть Access Standalone, який ви хочете додати до Smart PSS Lite, а потім натисніть Додати.

Крок 4 Введіть ім'я користувача та пароль Access Standalone.

Ви можете переглянути доданий Access Standalone на сторінці Пристрої

Access Standalone автоматично входить у Smart PSS Lite після додавання. Онлайн відобра--жається після успішного входу.

6.3 Управління користувачами

Додайте користувачів, призначте їм картки та налаштуйте їхні права доступу.

6.3.1 Налаштування типу картки

Встановіть тип картки перед тим, як призначити картки користувачам. Наприклад, якщо призначена картка є посвідченням особи, встановіть тип картки на посвідчення особи.

Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 **Натисніть Доступ до рішення** > **Менеджер персоналу** > **Користувач**

Крок 3 На Тип видачі картки і потім виберіть тип картки.

Переконайтеся, що тип картки відповідає фактично призначеній картці; в іншому випадку номер картки не може бути прочитаний.

Крок 4 Натисніть OK

6.3.2 Додавання користувачів

6.3.2.1 Додавання індивідуально

Ви можете додавати користувачів індивідуально.

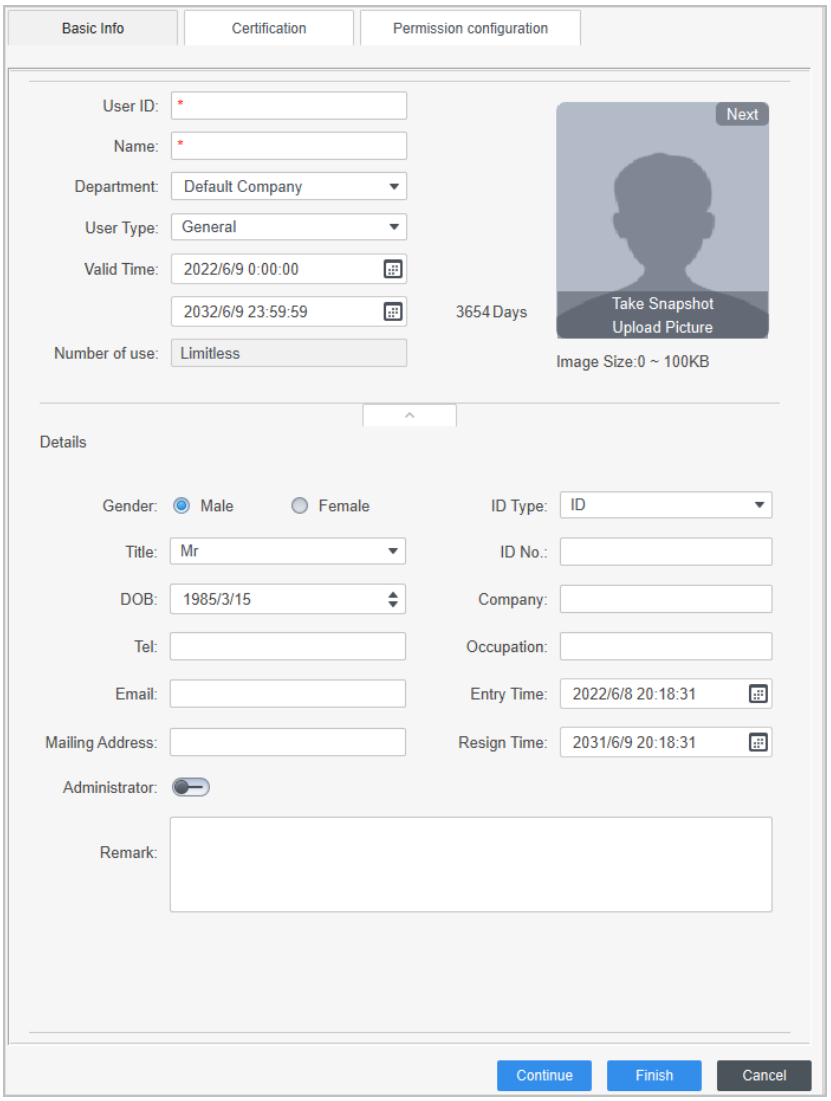
Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 **Натисніть Доступ до рішення** > **Менеджер персоналу** > **Користувач** > **Додати**

Крок 3 Натисніть Основна інформація вкладку та введіть основну інформацію про користувача, а потім імпортуйте зображення обличчя.

Рисунок 6-3 Додати основну інформацію

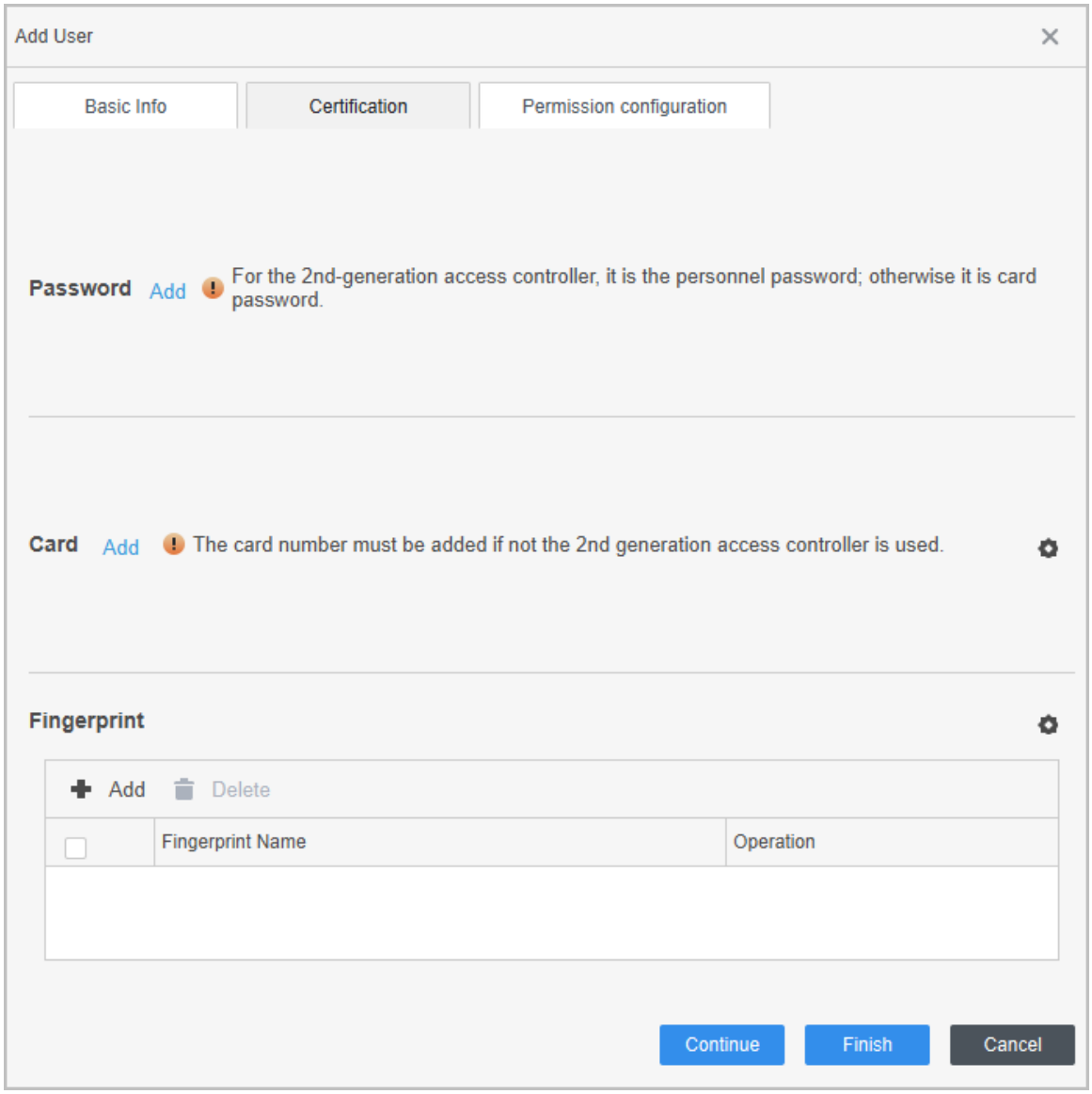


Крок 4 Натисніть вкладку Сертифікація , щоб додати інформацію про сертифікацію користувача.

- Налаштувати пароль: Пароль повинен складатися з 6–8 цифр.

- Налаштувати картку: Номер картки можна зчитати автоматично або ввести вручну. Щоб автоматично зчитати номер картки, виберіть зчитувач карток, а потім покладіть картку на зчитувач карток.
  1. У області Картка натисніть виберіть Емітент картки, а потім натисніть OK.
  2. Натисніть Додати , проведіть картку по зчитувачу карток. Номер картки відображається.
  3. Натисніть **OK**
     Після додавання картки ви можете встановити картку як основну або картку для екстрених ситуацій, або замінити картку на нову, або видалити картку.
- Налаштуйте відбиток пальця.
  1. У області Відбиток пальця натисніть виберіть Сканер відбитків пальців, а потім натисніть **OK**.
  2. Натисніть Додати відбиток пальця, тричі натисніть пальцем на сканер підряд.

Рисунок 6-4 Додати пароль, картку та відбиток пальця



Крок 5 Налаштуйте дозволи для користувача. Для отримання деталей див. "6.3.3 Призначення дозволу на доступ".

Крок 6 Натисніть Завершити

6.3.2.2 Додавання пакетами

Ви можете додавати користувачів пакетами.

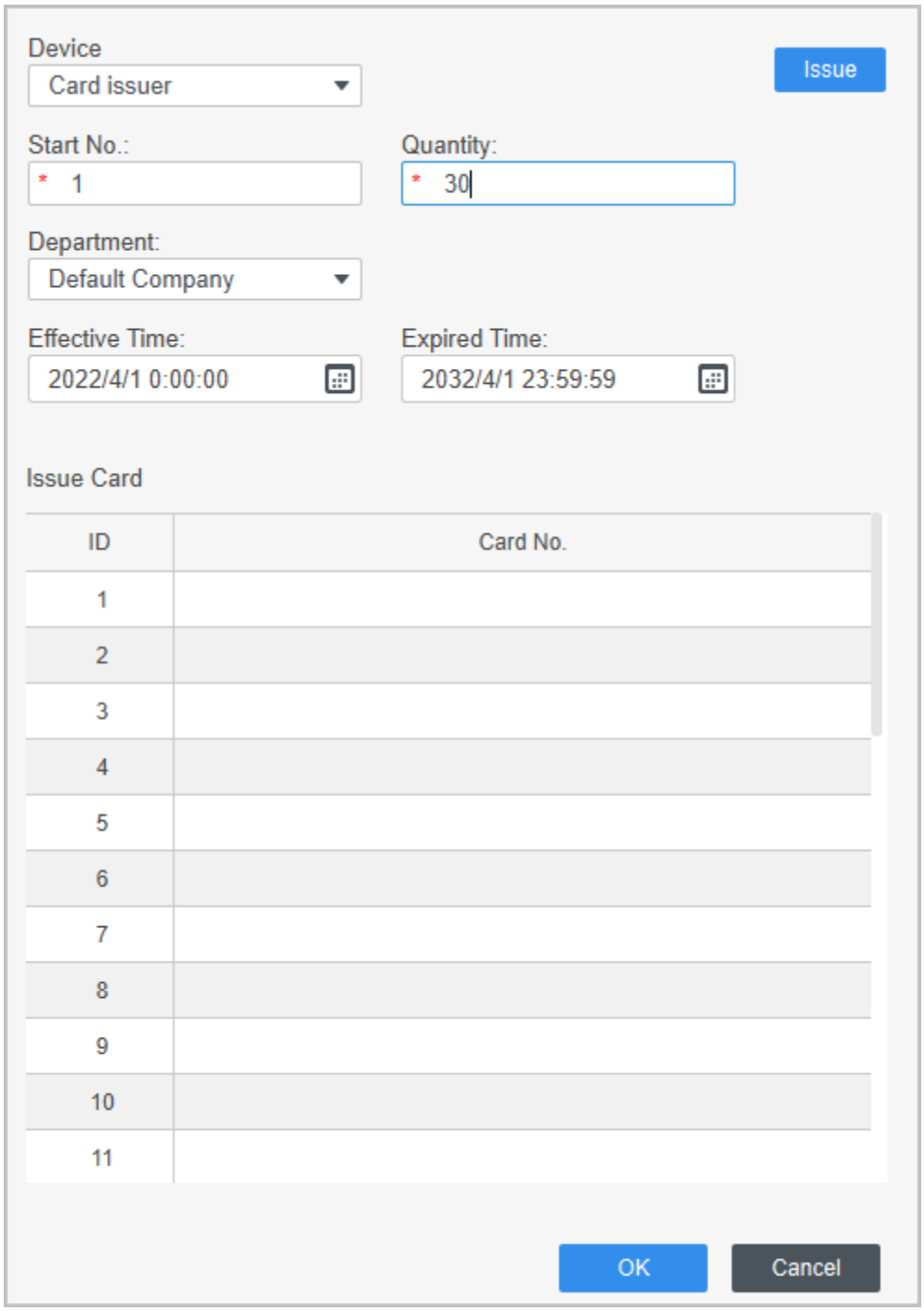
Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 **Натисніть Менеджер персоналу** > **Користувач** > **Пакетне додавання**

Крок 3 Виберіть Емітент карт зі списку Пристроїв , а потім налаштуйте параметри.

Рисунок 6-5 Додавання користувачів пакетами



Таблиця 6-2 Параметри додавання користувачів пакетами

Параметр	Опис
Початковий номер.	Ідентифікатор користувача починається з числа, яке ви визначили.
Кількість	Кількість користувачів, яких ви хочете додати.
Відділ	Виберіть відділ, до якого належить користувач.
Час дії/Час закінчення	Користувачі можуть відкрити двері протягом визначеного періоду.

Крок 4 Натисніть .Випустити

Номер картки буде прочитано автоматично.

Крок 5 Натисніть OK

Крок 6 На сторінці Користувач натисніть , щоб завершити інформацію про користувача.

6.3.3 Призначення дозволу на доступ

Створіть групу дозволів, яка є колекцією дозволів на доступ до дверей, а потім асоціюйте користувачів з групою, щоб користувачі могли відкривати відповідні двері.

Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 **Натисніть Рішення доступу** > **Менеджер персоналу** > **Налаштування дозволів**.

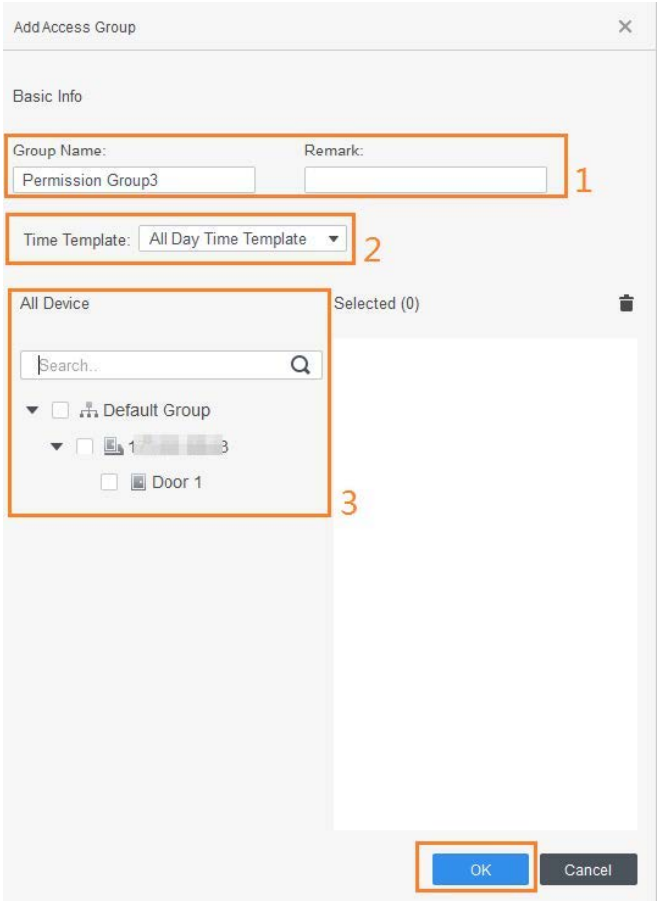
Крок 3 Натисніть .

Крок 4 Введіть назву групи, примітки (необов'язково) та виберіть шаблон часу.

Крок 5 Виберіть пристрій контролю доступу.

Крок 6 Натисніть OK

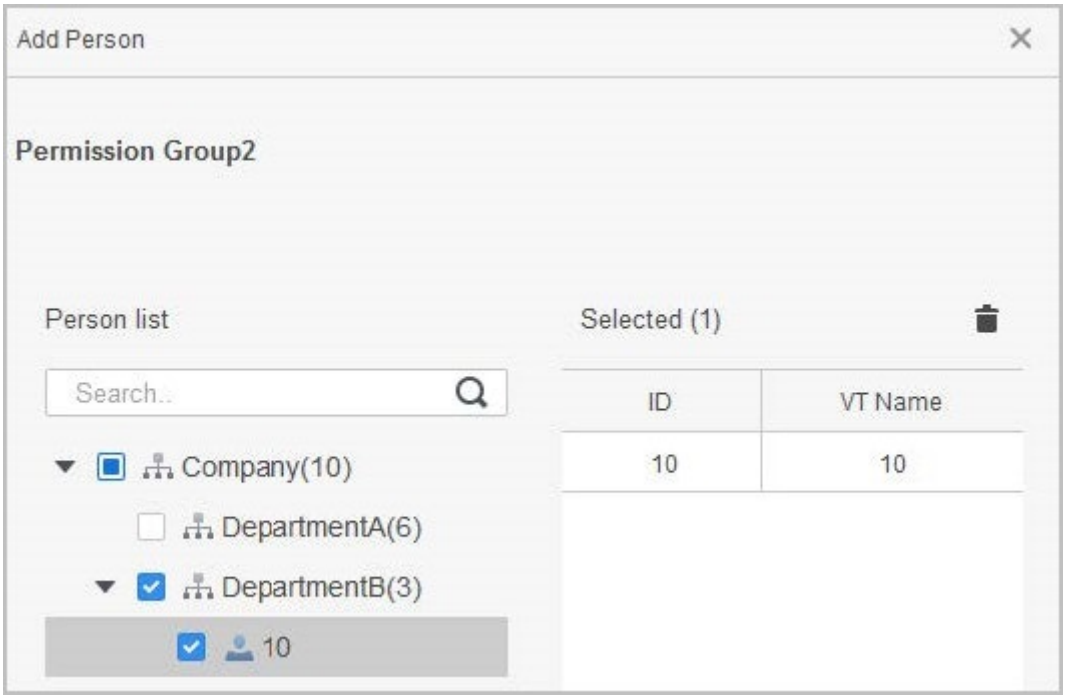
Рисунок 6-6 Створення групи дозволів



Крок 7 Натисніть групи дозволів, яку ви додали.

Крок 8 Виберіть користувачів, щоб асоціювати їх з групою дозволів.

Рисунок 6-7 Додати користувачів до групи дозволів



Крок 9 Натисніть OK

Користувачі в групі дозволів можуть відкрити двері після дійсної перевірки особи.

6.4 Управління доступом

6.4.1 Віддалене відкриття та закриття дверей

Ви можете віддалено контролювати та керувати дверима через Smart PSS Lite. Наприклад, ви можете віддалено відкрити або закрити двері.

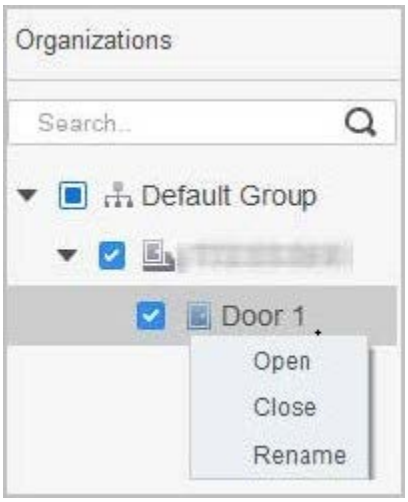
Процедура

Крок 1 Натисніть Рішення для доступу > Менеджер доступу на головній сторінці.

Крок 2 Віддалено керувати дверима.

- Виберіть двері, клацніть правою кнопкою миші та виберіть Відкрити або Закрити

Рисунок 6-8 Відкрита двері



- Клацніть або щоб відкрити або закрити двері.

Супутні операції

- Фільтрація подій: виберіть тип події в Інформація про подію, і список подій відображає вибраний тип події, наприклад, події тривоги та аномальні події.
- Блокування оновлення подій: клацніть щоб заблокувати список подій, після чого список подій перестане оновлюватися. Клацніть, щоб розблокувати.
- Видалення подій: клацніть , щоб очистити всі події в списку подій.

6.4.2 Налаштування завжди відкрито та завжди закрито

Після встановлення завжди відкрито або завжди закрито, двері залишаються відкритими або закритими весь час.

Процедура

Крок 1 Натисніть Рішення для доступу > Менеджер доступу на головній сторінці.

Крок 2 Натисніть Завжди відкрито або Завжди закрито , щоб відкрити або закрити двері.

Рисунок 6-9 Завжди відкрито або закрито

Двері залишатимуться відкритими або закритими весь час. Ви можете натиснути Нормальний , щоб відновити контроль доступу до нормального стану, і тоді двері будуть відкриватися або закриватися на основі налаштованих методів перевірки.

6.4.3 Моніторинг стану дверей

Процедура

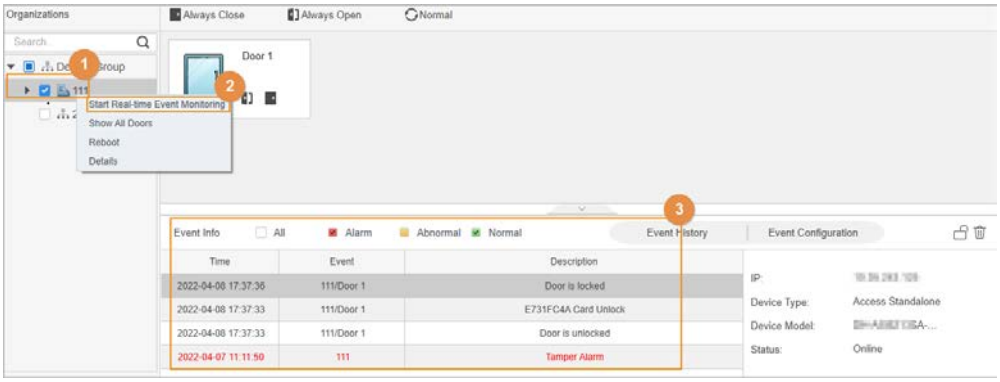
Крок 1 Натисніть Рішення для доступу > Менеджер доступу на головній сторінці.

Крок 2 Виберіть Access Standalone у дереві пристроїв, клацніть правою кнопкою миші на Access Terminal і потім виберіть Почати моніторинг подій у реальному часі

Події контролю доступу в реальному часі відображатимуться у списку подій.

Натисніть Зупинити моніторинг , події контролю доступу в реальному часі не відображатимуться.

Рисунок 6-10 Статус дверей монітора



Супутні операції

- Показати всі двері: Відображає всі двері, які контролюються Access Standalone.
- Перезавантажити: Перезапустіть Access Standalone.
- Деталі: Перегляньте деталі пристрою, такі як IP-адреса, модель та статус.

6.4.4 Перегляд деталей контролю доступу

Перегляньте IP-адресу, модель, статус, серійний номер, версію прошивки та іншу інформацію про

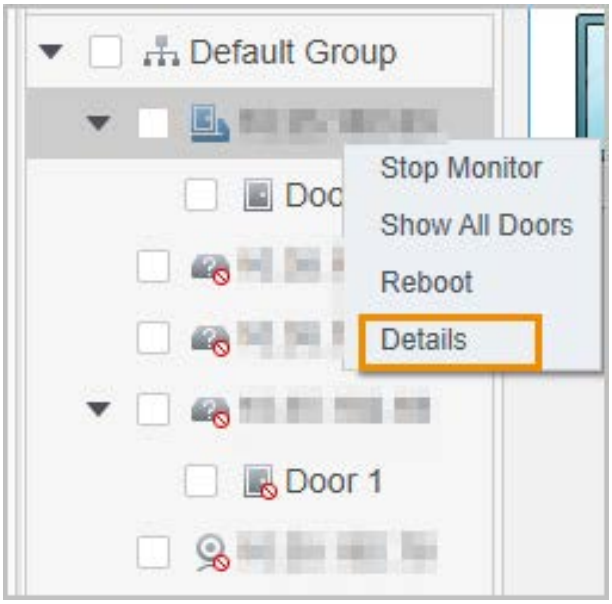
Access Standalone.

Процедура

Крок 1 Натисніть Менеджер доступу на домашній сторінці. (Ви також можете натиснути Посібник з доступу >).

Крок 2 Натисніть на Access Standalone, який ви хочете переглянути в лівому дереві організації, клацніть правою кнопкою миші на пристрій, а потім натисніть Деталі , щоб переглянути детальну інформацію про пристрій.

Рисунок 6-11 Перегляд деталей



6.4.5 Перезавантаження Access Standalone

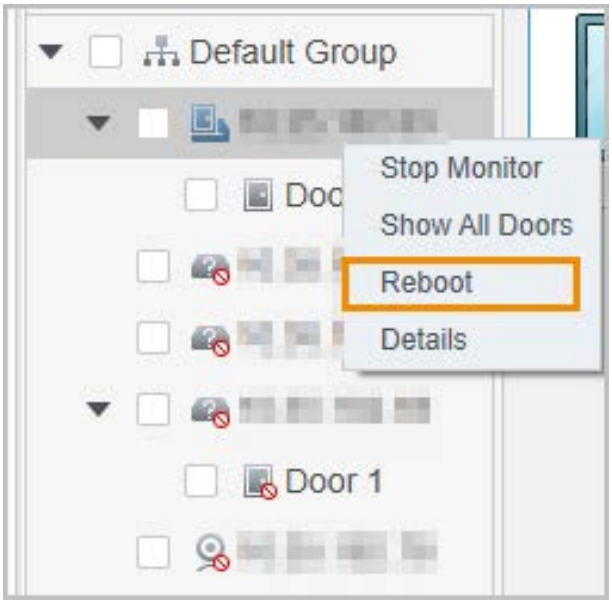
Підтримка віддаленого перезавантаження Access Standalone через платформу.

Процедура

Крок 1 Натисніть Менеджер доступу на домашній сторінці. (Ви також можете натиснути Посібник з доступу >).

Крок 2 Натисніть на Access Standalone, який ви хочете перезавантажити в лівому дереві організації, клацніть правою кнопкою миші на пристрій, а потім натисніть Перезавантажити, щоб перезавантажити пристрій.

Рисунок 6-12 Перезавантаження пристрою



Додаток 1 Рекомендації з кібербезпеки

Обов'язкові дії для забезпечення базової мережевої безпеки пристроїв:

1. **Використовуйте надійні паролі**

   Будь ласка, зверніть увагу на наступні рекомендації для встановлення паролів:

   - Довжина не повинна бути меншою за 8 символів.
   - Включайте принаймні два типи символів; типи символів включають великі та малі літери, цифри та символи.
   - Не містити ім'я облікового запису або ім'я облікового запису в зворотному порядку.
   - Не використовуйте послідовні символи, такі як 123, abc тощо.
   - Не використовуйте повторювані символи, такі як 111, aaa тощо.

2. **Оновлюйте прошивку та програмне забезпечення клієнта вчасно.**

   - Згідно зі стандартною процедурою в технологічній індустрії, ми рекомендуємо підтримувати прошивку вашого пристрою (такого як NVR, DVR, IP-камера тощо) в актуальному стані, щоб забезпечити систему останніми патчами безпеки та виправленнями. Коли пристрій підключено до публічної мережі, рекомендується увімкнути функцію "авто-перевірка оновлень", щоб отримувати своєчасну інформацію про оновлення прошивки, випущені виробником.
   - Ми рекомендуємо завантажити та використовувати останню версію програмного забезпечення клієнта.

"Приємно мати" рекомендації для покращення безпеки мережі вашого пристрою:

1. **Фізичний захист**

   Ми рекомендуємо вам забезпечити фізичний захист пристрою, особливо накопичувачів. Наприклад, розмі стіть пристрій у спеціальному комп'ютерному приміщенні та шафі, а також реалізуйте добре організований ко нтроль доступу та управління ключами, щоб запобігти несанкціонованому доступу осіб до фізичних конта ктів, таких як пошкодження апаратного забезпечення, несанкціоноване підключення знімних пристроїв (таких як USB флеш-накопичувач, послідовний порт) тощо.

2. **Регулярно змінюйте паролі**

   Ми рекомендуємо вам регулярно змінювати паролі, щоб зменшити ризик їх вгадування або зламу.

3. **Своєчасно встановлюйте та оновлюйте інформацію для скидання паролів**

   Пристрій підтримує функцію скидання пароля. Будь ласка, своєчасно налаштуйте відповідну інформацію для скида ння пароля, включаючи електронну пошту кінцевого користувача та запитання для захисту пароля. Якщо інф ормація змінюється, будь ласка, своєчасно внесіть зміни. При налаштуванні запитань для захисту пароля рекомендует ься не використовувати ті, які можна легко вгадати.

4. **Увімкніть блокування облікового запису**

   Функція блокування облікового запису увімкнена за замовчуванням, і ми рекомендуємо вам залишити її вві мкненою для забезпечення безпеки облікового запису. Якщо зловмисник кілька разів намагатиметься увійти з неправил ьним паролем, відповідний обліковий запис та IP-адреса джерела будуть заблоковані.

5. **Змініть порти за замовчуванням для HTTP та інших служб**

   Ми рекомендуємо вам змінити порти за замовчуванням для HTTP та інших служб на будь-який набір чисел між 1024–65535, зменшуючи ризик того, що сторонні особи зможуть вгадати, які порти ви використовуєте.

6. **Увімкнути HTTPS**

   Ми рекомендуємо вам увімкнути HTTPS, щоб ви могли відвідувати веб-сервіс через безпечний канал зв'язку.

7. **Прив'язка MAC-адреси**

   Ми рекомендуємо вам прив'язати IP-адресу та MAC-адресу шлюзу до пристрою, таким чином зменшуючи

ризик ARP-спуфінгу.

8. **Розумно призначайте облікові записи та привілеї**

   Відповідно до бізнес-вимог та управлінських вимог, розумно додайте користувачів та призначте їм мінімальний набір дозволів.

9. **Вимкніть непотрібні служби та виберіть безпечні режими**

   Якщо не потрібно, рекомендується вимкнути деякі служби, такі як SNMP, SMTP, UPnP тощо, щоб зменшити ризики.

   За необхідності, настійно рекомендується використовувати безпечні режими, включаючи, але не обмежуючись наступними службами:

   - SNMP: Виберіть SNMP v3 та налаштуйте надійні паролі шифрування та паролі аутентифікації.
   - SMTP: Виберіть TLS для доступу до сервера поштової скриньки.
   - FTP: Виберіть SFTP та налаштуйте надійні паролі.
   - AP гаряча точка: Виберіть режим шифрування WPA2-PSK та налаштуйте надійні паролі.

10. **Захищена передача аудіо та відео**

    Якщо ваші аудіо- та відеодані є дуже важливими або чутливими, ми рекомендуємо вам використовувати функцію зашифрованої передачі, щоб зменшити ризик крадіжки аудіо- та відеоданих під час передачі.

    Нагадування: зашифрована передача призведе до деякої втрати ефективності передачі.

11. **Захищений аудит**

    - Перевірка онлайн-користувачів: ми рекомендуємо регулярно перевіряти онлайн-користувачів, щоб дізнатися, чи пристрій увійшов без авторизації.
    - Перевірте журнал пристрою: переглядаючи журнали, ви можете дізнатися IP-адреси, які використовувалися для входу на ваші пристрої та їх ключові операції.

12. **Журнал мережі**

    Через обмежену ємність пам'яті пристрою збережений журнал обмежений. Якщо вам потрібно зберегти журнал на тривалий час, рекомендується увімкнути функцію журналу мережі, щоб забезпечити синхронізацію критичних журналів на сервер журналу мережі для відстеження.

13. **Створіть безпечне мережеве середовище**

    Щоб краще забезпечити безпеку пристрою та зменшити потенційні кіберризики, ми рекомендуємо:

    - Вимкніть функцію відображення портів маршрутизатора, щоб уникнути прямого доступу до внутрішніх пристроїв з зовнішньої мережі.
    - Мережу слід розділити та ізолювати відповідно до фактичних потреб мережі. Якщо немає вимог до зв'язку між двома підмережами, рекомендується використовувати VLAN, мережевий GAP та інші технології для розділення мережі, щоб досягти ефекту ізоляції мережі.
    - Встановіть систему автентифікації доступу 802.1x, щоб зменшити ризик несанкціонованого доступу до приватних мереж.
    - Увімкніть функцію фільтрації IP/MAC-адрес, щоб обмежити діапазон хостів, яким дозволено отримувати доступ до пристрою.