Контролер доступу з розпізнаванням облич

Посібник користувача

Версія 1.0.0

Передмова

Загальний

У цьому посібнику описуються функції та операції Контролера доступу з розпізнаванням осіб (далі іменованого «Контролер доступу»). Уважно прочитайте перед використанням пристрою та збережіть посібник для подальшого використання.

Інструкції з техніки безпеки

У посібнику можуть зустрічатися такі сигнальні слова.

Сигнальні слова	Значення
DANGER	Вказує на високу потенційну небезпеку, яка, якщо її не запобігти, призведе до смерті чи серйозних травм.
WARNING	Вказує на середню чи низьку потенційну небезпеку, яка, якщо її не уникнути, може призвести до легкої чи середньої травми.
CAUTION	Вказує на потенційний ризик, який, якщо його не запобігти, може призвести до пошкодження майна, втрати даних, зниження продуктивності або непередбачуваним результатам.
TIPS	Надає методи, які допоможуть вам вирішити проблему або заощадити час.
NOTE	Надає додаткову інформацію як додаток до тексту.

Історія змін

Версія	Зміст перегляду	Час випуску
Версія 1.0.0	Перший випуск.	Червень 2023 р.

Повідомлення про захист конфіденційності

Як користувач пристрою або контролер даних, ви можете збирати персональні дані інших осіб, такі як їх обличчя, відбитки пальців та номерний знак. Вам необхідно дотримуватися місцевих законів та правил захисту конфіденційності, щоб захищати законні права та інтереси інших осіб, реалізуючи заходи, які включають, але не обмежуються: надання чіткої та видимої ідентифікації для інформування людей про існування зони спостереження та надання необхідної контактної інформації.

Про керівництво

- Керівництво має виключно довідковий характер. Між керівництвом та продуктом можуть бути виявлені незначні відмінності.
- Ми не несемо відповідальності за збитки, що виникли в результаті експлуатації виробу способами, відповідними керівництву.
- Керівництво оновлюватиметься відповідно до останніх законів та правил відповідних юрисдикцій. Для Для отримання докладної інформації див. паперовий посібник користувача, використовуйте наш CD-ROM, відскануйте QR-код або відвідайте наш офіційний веб-сайт. Керівництво призначене лише для довідки. Між електронною та паперовою версіями можуть бути виявлені незначні відмінності.
- Усі проекти та програмне забезпечення можуть бути змінені без попереднього письмового повідомлення. Оновлення продукту

може призвести до деяких відмінностей між фактичним продуктом та керівництвом. Будь ласка, зв'яжіться зі службою підтримки клієнтів для отримання останньої версії програми та додаткової документації.

- Можуть бути помилки друку або відхилення в описі функцій, операцій та технічних даних. У у разі виникнення сумнівів чи суперечок ми залишаємо за собою право остаточного пояснення.
- Оновіть програмне забезпечення зчитувача або спробуйте інше популярне програмне забезпечення зчитувача, якщо Посібник (у форматі PDF) не відкривається.
- Всі товарні знаки, зареєстровані товарні знаки та назви компаній у посібнику є власністю їхніх власників.
- Будь ласка, відвідайте наш веб-сайт, зверніться до постачальника або служби підтримки клієнтів, якщо при використанні пристрою виникли будь-які проблеми.
- У разі виникнення будь-якої невизначеності чи розбіжності ми залишаємо за собою право остаточного роз'яснення.

Важливі запобіжні заходи та попередження

У цьому розділі представлений контент, що охоплює правильне поводження з контролером доступу, запобігання небезпеці та запобігання пошкодженню майна. Уважно прочитайте перед використанням контролера доступу та дотримуйтесь інструкції при його використанні.

Вимоги до транспортування

Транспортуйте, використовуйте та зберігайте контролер доступу за допустимих умов вологості та температури.

Вимоги до зберігання

Зберігайте контролер доступу за допустимих умов вологості та температури.

Вимоги до встановлення

- Не підключайте адаптер живлення до контролера доступу, коли адаптер увімкнено.
- Строго дотримуйтесь місцевих правил та стандартів електробезпеки. Переконайтеся, що напруга навколишнього середовища стабільно та відповідає вимогам до електроживлення контролера доступу.
- Не підключайте контролер доступу до двох або більше типів джерел живлення, щоб уникнути пошкодження контролера доступу.
- Неправильне використання акумулятора може призвести до пожежі або вибуху.

- Персонал, який працює на висоті, повинен вживати всіх необхідних заходів для забезпечення особистої безпеки, включаючи носіння каски та ременів безпеки.
- Не розміщуйте контролер доступу в місцях, які піддаються сонячному світлу або поблизу джерел тепла.
- Бережіть контролер доступу від вологи, пилу та кіптяви.
- Встановіть контролер доступу на стійку поверхню, щоб запобігти його падінню.
- Встановлюйте контролер доступу в місці, що добре провітрюється, і не блокуйте його вентиляцію.
- Використовуйте адаптер або блок живлення для шафи, наданий виробником.
- Використовуйте шнури живлення, рекомендовані для вашого регіону та відповідні номінальним характеристикам. потужності.
- Джерело живлення має відповідати вимогамES1 у стандарті IEC 62368-1 і бути не вище PS2. Зверніть увагу, що вимоги до джерела живлення залежать від етикетки контролера доступу.
- Контролер доступу – це електроприлад класуI. Переконайтеся, що джерело живлення контролера доступу підключено до розетки із заземленням.

Вимоги до експлуатації

- Перед використанням перевірте правильність живлення.

- Не від'єднуйте шнур живлення збоку контролера доступу до адаптера.

- Експлуатуйте контролер доступу в межах номінального діапазону вхідної та вихідної потужності.
- Використовуйте контролер доступу за допустимих умов вологості та температури.
- Не допускайте потрапляння рідини на контролер доступу та не допускайте її потрапляння на нього. Переконайтеся, що на контролері доступу немає предметів, наповнених рідиною, щоб запобігти потраплянню рідини до контролера.
- Не розбирайте контролер без професійних інструкцій.
- Цей продукт є професійним обладнанням.
- Контролер доступу не підходить для використання в місцях, де можлива присутність дітей.

Зміст

1 Огляд

Контролер доступу — це панель керування доступом, яка підтримує розблокування за допомогою облич, паролів, відбитків. пальців, карт, QR-кодів та їх комбінацій. Завдяки алгоритму глибокого навчання він відрізняється швидшим розпізнаванням і вищою точністю. Може працювати з платформою управління, яка відповідає різним потребам клієнтів.

Він широко використовується в парках, житлових районах, бізнес-центрах та на фабриках, а також ідеально підходить для таких місць, як офісні будівлі, урядові будівлі, школи та стадіони.

- Конфігурації можуть відрізнятися залежно від моделі продукту, будь ласка, зверніться до фактичного продукту.

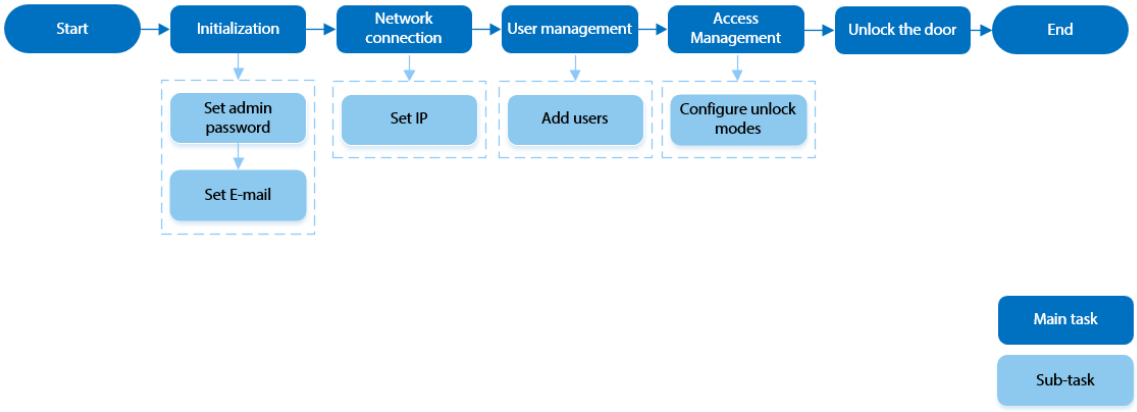
- Пристрої з несенорним екраном повинні підключатися до миші для конфігурацій. У цьому посібнику як Прикладом використовується пристрій із сенсорним екраном.
- Деякі моделі підтримують підключення до модулів розширення, таких як модульQR-коду, модуль відбитків пальців і т. д. Тип модулів розширення, що підтримуються контролером доступу, може відрізнятися, див. фактичний продукт.

2 локальних операції

- Зміни можуть відрізнятися залежно від конкретного продукту.
- Моделі з сенсорним екраном не вимагають підключення дротовоїUSB-миші. У цьому розділі як приклад використовуються моделі із сенсорним екраном.
- Зовнішні модулі розширення доступні лише для деяких моделей.
- Ви можете побачити, що деякі тексти інтерфейсу користувача не відображаються через обмежений простір. Довго натисніть на текст протягом 3 секунд, і він відобразиться.

2.1 Базова процедура налаштування

Малюнок 2-1 Базова процедура налаштування



2.2 Загальні значки

Таблиця 2-1 Опис іконок

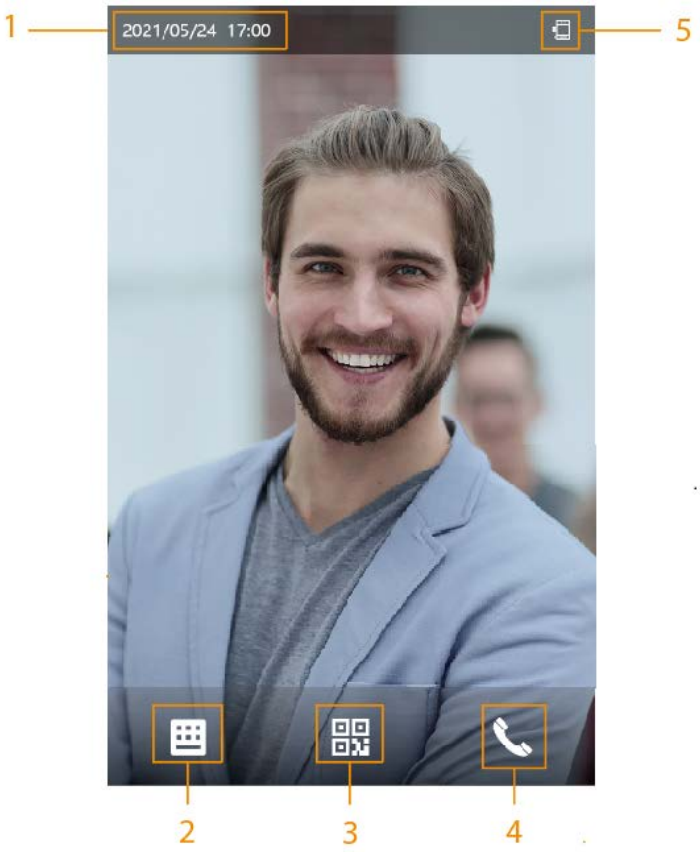
Ікона	Опис
	Головне меню значок.
	Підтвердження значок.
	Відкрийте першу сторінку списку.
	Відкрийте останню сторінку списку.
або	Перейти до попередньої сторінки списку.
або	Перейдіть до наступної сторінки списку.
	Повернутися до попереднього меню.
	Увімкнено.
	Вимкнено.
	Видалити
	Пошук

2.3 Екран очікування

Ви можете розблокувати двері за допомогою облич, карти, паролів та QR-коду. Ви також можете здійснювати дзвінки через функцію домофону. Методи розблокування можуть відрізнятися залежно від моделі продукту.

- Якщо протягом 30 секунд не буде здійснено жодних дій, контролер доступу перейде в режим очікування.
- Цей посібник призначений лише для довідки. Невеликі відмінності можуть бути виявлені між екраном очікування у цьому посібнику та на самому пристрої.

Рисунок 2-2 Екран режиму очікування



Таблиця 2-2 Опис головного екрана

Ні.	Ім'я	Опис
1	Дата та час	Поточна дата та час.
2	Пароль	Введіть пароль користувача, пароль адміністратора або тимчасовий пароль, щоб розблокувати двері.

Ні.	Ім'я	Опис
3	QR-код	Натисніть на QR-код і відскануйте QR-код, щоб розблокувати двері. Для моделей, які мають автономний модуль QR-коду або підключають модуль розширення QR. Значок не буде відображатись. Ви можете просто помістити свій код OR перед лінзою контролера доступу або модуля розширення, він буде автоматично відсканова.
4	Інтерком	● Коли контролер доступу працює як сервер, він може викликати VTO та VTH. ● Коли платформа управління функціонує як сервер, контролер доступу може викликати VTO, VTS та платформу управління. ● При роботі зDMSS може викликати DMSS.
5	Відображення статусу	Відображає стан Wi-Fi, мережі, модуля розширення, USB тощо. Wi-Fi та модулі розширення доступні лише в деяких моделях.

2.4 Ініціалізація

При першому використанні або після відновлення заводських налаштувань вам необхідно вибрати мову на Access Controller, а потім встановити пароль та адресу електронної пошти для облікового запису адміністратора. Ви можете використовувати обліковий запис адміністратора для входу в головне меню Access Controller та його веб-сторінку.

- Якщо ви забули пароль адміністратора, надішліть запит на скидання на вашу зареєстровану адресу електронної пошти.
- Пароль повинен складатися з 8–32 непустих символів та містити не менше двох типів символи верхнього регістру, малі літери, цифри та спеціальні символи (за винятком ' " ; : &).

2.5 Вхід у систему

Увійдіть у головне меню, щоб настроїти контролер доступу. Тільки обліковий запис адміністратора та обліковий запис адміністратора можуть увійти до головного меню контролера доступу. Під час першого використання використовуйте обліковий запис адміністратора для входу в екран головного меню, а потім ви зможете створити інші облікові записи адміністраторів.

Довідкова інформація

- Обліковий запис адміністратора: може увійти до головного меню контролера доступу, але не має прав доступу до дверей.
- Обліковий запис адміністратора: може входити до головного меню контролера доступу та має дозволи на доступ до двері.

Процедура

Крок 1 Натисніть та утримуйте екран очікування протягом 3 секунд.

Крок 2 Виберіть метод перевірки, щоб увійти до головного меню.

- Обличчя: Вхід до головного меню за допомогою розпізнавання обличчя.
- Відбиток пальця: увійдіть у головне меню, використовуючи відбиток пальця.

  Функція сканера відбитків пальців доступна лише у деяких моделях.
- Перфорація картки: увійдіть до головного меню, провівши карткою по зчитувачу.
- PWD: Введіть ідентифікатор користувача та пароль облікового запису адміністратора.
- admin: Введіть пароль адміністратора для входу до головного меню.

2.6 Методи розблокування

Ви можете відкрити двері за допомогою обличчя, пароля, відбитка пальця, карти та інших засобів.

2.6.1 Розблокування картками

Прикладіть картку до зони зчитування, щоб відчинити двері.

2.6.2 Розблокування по обличчю

Перевірте особистість людини, розпізнавши її обличчя. Переконайтеся, що обличчя знаходиться у центрі рамки розпізнавання осіб.

2.6.3 Розблокування за допомогою пароля користувача

Введіть ідентифікатор користувача та пароль, щоб розблокувати двері.

Процедура

Крок 1 Кран на екрані у режимі очікування.

Крок 2 Кран**Розблокувати паролем**, а потім введіть ідентифікатор користувача та пароль. Натисніть

Крок 3 **ДОБРЕ**.

2.6.4 Розблокування за допомогою пароля адміністратора

Введіть пароль адміністратора, щоб розблокувати двері. Двері можна розблокувати за допомогою пароля адміністратора, за винятком нормально зачинених дверей. Один пристрій дозволяє лише один пароль адміністратора.

Передумови

Пароль адміністратора було настроєно. Докладніше див. у розділі "2.7.3 Налаштування пароля розблокування адміністратора".

Процедура

Крок 1 Кран на екрані у режимі очікування.

Крок 2 Кран**Розблокувати за допомогою пароля адміністратора**, а потім введіть пароль адміністратора.

Крок 3 Натисніть

Пароль адміністратора не може бути використаний для розблокування, якщо статус дверей встановлений на "завжди" статус закрито.

2.6.5 Розблокування за QR-кодом

Процедура

Крок 1 На екрані очікування натисніть .

Крок 2 Поставте QR-код перед об'єктивом.

2.6.6 Розблокування по відбитку пальця

Додайте палець до сканера відбитків пальців. Ця функція доступна лише в деяких моделях.

2.6.7 Розблокування тимчасовим паролем

Відчиніть двері тимчасовим паролем.

Процедура

Крок 1 Додайте контролер доступу до DMSS.

DMSS згенерує тимчасовий пароль, який дозволить вам розблокувати двері до закінчення терміну його дії.

Крок 2 На головному екрані натисніть , а потім натисніть**Розблокувати тимчасовим паролем**.

Крок 3 Введіть тимчасовий пароль, а потім натисніть

2.7 Керування користувачами

Ви можете додавати нових користувачів, переглядати список користувачів/адміністраторів та редагувати інформацію про користувачів.

Зображення в цьому посібнику наведено лише для довідки та можуть відрізнятися від фактичного продукту.

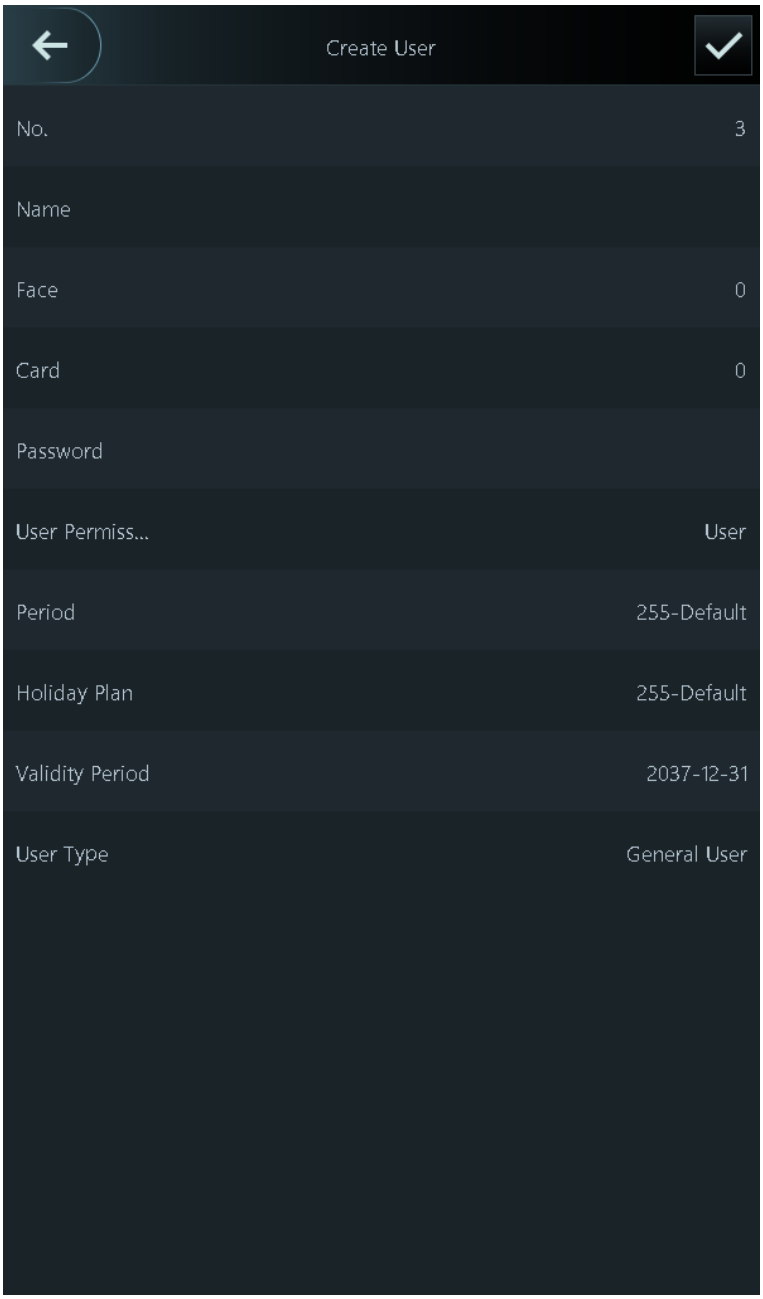
2.7.1 Додавання користувачів

Процедура

Крок 1 на**Головне меню**, вибирати**Управління персоналом**>**Створити**

Крок 2 **користувача**. Налаштуйте параметри інтерфейсу.

Рисунок 2-3 Додати нового користувача



Таблиця 2-3 Опис параметрів

Параметр	Опис
Ні.	Номер схожий на ідентифікатор співробітника і може складатися з цифр, літер та їх комбінацій, а максимальна довжина номера становить 32 символи.
Ім'я	Ім'я може містити до 30 символів (включаючи цифри, символи та літери).

Параметр	Опис
ФП	Реєстрація відбитків пальців. Користувач може зареєструвати до 3 відбитків пальців, і ви можете встановити відбиток пальця для відбитка пальця примусу. Сигналізація спрацює, якщо відбиток примусового пальця буде використаний для розблокування дверей.  ● Функція відбитків пальців доступна лише на деяких моделі. ● Ми не рекомендуємо вам встановлювати перший відбиток пальця як відбиток пальця під примусом. ● Один користувач може встановити лише один відбиток пальця під примусом. ● Функція розпізнавання відбитків пальців доступна, якщо контролер доступу підтримує підключення модуля розширення для розпізнавання відбитків пальців.
Обличчя	Помістіть обличчя в рамку, і зображення обличчя буде захоплено автоматично. Ви можете зареєструватися знову, якщо ви не задоволені результатом.
Картка	Користувач може зареєструвати максимум до 5 карток. Введіть номер своєї карти або проведіть нею по зчитувачу, після чого дані картки будуть раховані контролером доступу. Ви можете увімкнути**Карта примусу**функція. Сигналізація спрацює, якщо для розблокування дверей буде використано карту примусу.  Один користувач може встановити лише одну примусову карту.
Пароль	Введіть пароль користувача. Максимальна довжина пароля – 8 цифр. Пароль примусу – це пароль розблокування + 1. Наприклад, якщо пароль користувача – 12345, пароль примусу буде 12346. Сигналізація примусу спрацює, якщо для розблокування дверей буде використано пароль примусу.
Дозвіл користувача	● **Користувач**: Користувачі мають лише дозвіл на доступ до дверей або облік. робочого часу. ● **Адмін**: Адміністратори можуть налаштовувати контролер доступу, крім дозволів на доступ до дверей та відвідуваність.
Період	Люди можуть відчиняти двері або приймати відвідувачів протягом певного періоду. Докладніше про налаштування періодів див. "3.7.8.1 Налаштування періодів часу".
План відпустки	Люди можуть відчиняти двері або приймати відвідувачів під час певного свята. Докладніше про налаштування періодів див. розділ "3.7.8.2 Налаштування планів свят".
Термін дії	Встановіть дату, коли закінчується термін дії дозволів на доступ до дверей та присутність людини.

Параметр	Опис
Тип користувача	● **Звичайний користувач**: Звичайні користувачі можуть розблокувати двері. ● **Чорний список користувачів**: Коли користувачі з чорного списку відчиняють двері, спрацьовує сигналізація чорного списку. ● **Гість Користувач**: Гості можуть розблокувати двері протягом певного періоду чи певну кількість разів. Після закінчення певного періоду або часу розблокування вони не зможуть розблокувати двері. ● **Патрульний користувач**: Патрульні користувачі можуть реєструвати присутність на контролері доступу, але вони не мають доступу до дверей дозволу. ● **VIP-користувач**: Коли VIP відчинить двері, обслуговуючий персонал отримає повідомлення. ● **Інший користувач**: Коли вони відчиняють двері, вона залишається відкритою ще 5 секунд. ● **Користувальницький користувач1/Користувач 2**: Те саме і зі звичайними користувачами.
Відділення	Виберіть відділи, які корисні для налаштування розкладів відділів. Відомості про створення відділів див. у розділі "2.9.1 Налаштування відділів". Ця функція доступна лише в деяких моделях.
Режим розкладу	● Розклад роботи відділу: застосування розкладів роботи відділу користувачеві. ● Персональний розклад: застосування персональних розкладів до користувачеві. Про те, як налаштувати особисті або окремі розклади, див. розділ «2.9.4 Налаштування робочих розкладів». ◇ Ця функція доступна лише в деяких моделях. ◇ Якщо ви встановите режим розкладу на відділ розклад тут, особистий розклад у вас є налаштовано для користувача в**Відвідуваність**>**Розклад Зміни**>**Особистий розклад**стають недійсними.

Крок 3 Кран.

2.7.2 Перегляд інформації про користувача

Процедура

Крок 1 на**Головне меню**, вибирати**Управління персоналом**>**Список користувачів**, або виберіть**Користувач**>**Список адміністраторів**. Переглянути всіх

Крок 2 доданих користувачів та облікові записи адміністраторів.

- : Розблокувати за допомогою пароля.
- : Розблокування зчитування картки.

- : Розблокування за допомогою розпізнавання обличчя.
- : Розблокування за допомогою відбитка пальця.

Пов'язані операції

на**Користувач**на екрані ви можете керувати доданими користувачами.

- Пошук користувачів: натисніть та введіть ім'я користувача.
- Редагувати користувачів: натисніть користувача, щоб змінити інформацію про нього.
- Видалити користувачів
  - ◇ Видалити по одному: виберіть користувача, а потім натисніть . .
  - ◇ Видаляти партіями:
    - ○ на**Список користувачів**екран, натисніть для видалення всіх користувачів.
    - ○ на**Список адміністраторів**екран, натисніть для видалення всіх користувачів адміністраторів.

2.7.3 Налаштування пароля розблокування адміністратора

Ви можете розблокувати двері, ввівши лише пароль адміністратора. Пароль не обмежений типами користувачів. Для одного пристрої дозволено лише один пароль розблокування адміністратора.

Процедура

Крок 1 на**Головне меню**екран, виберіть**Користувач**>**Пароль розблокування адміністратора**.

Крок 2 Кран**Пароль розблокування адміністратора**, а потім введіть пароль. Увімкніть функцію

Крок 3 розблокування адміністратора.

2.8 Управління доступом

Ви можете налаштувати параметри для дверей, такі як режим розблокування, зв'язок із сигналізацією та розклад дверей. Доступні режими розблокування можуть відрізнятися залежно від моделі виробу.

2.8.1 Налаштування комбінацій розблокування

Використовуйте карту, відбиток пальця, обличчя або пароль або їхню комбінацію для розблокування дверей. Доступні режими Розблокування може відрізнятися залежно від моделі продукту.

Процедура

Крок 1 Вибирати**Управління контролем доступу**>**Розблокувати комбінацію**.

Крок 2 Виберіть методи розблокування.

Щоб скасувати вибір, торкніться вибраного методу ще раз.

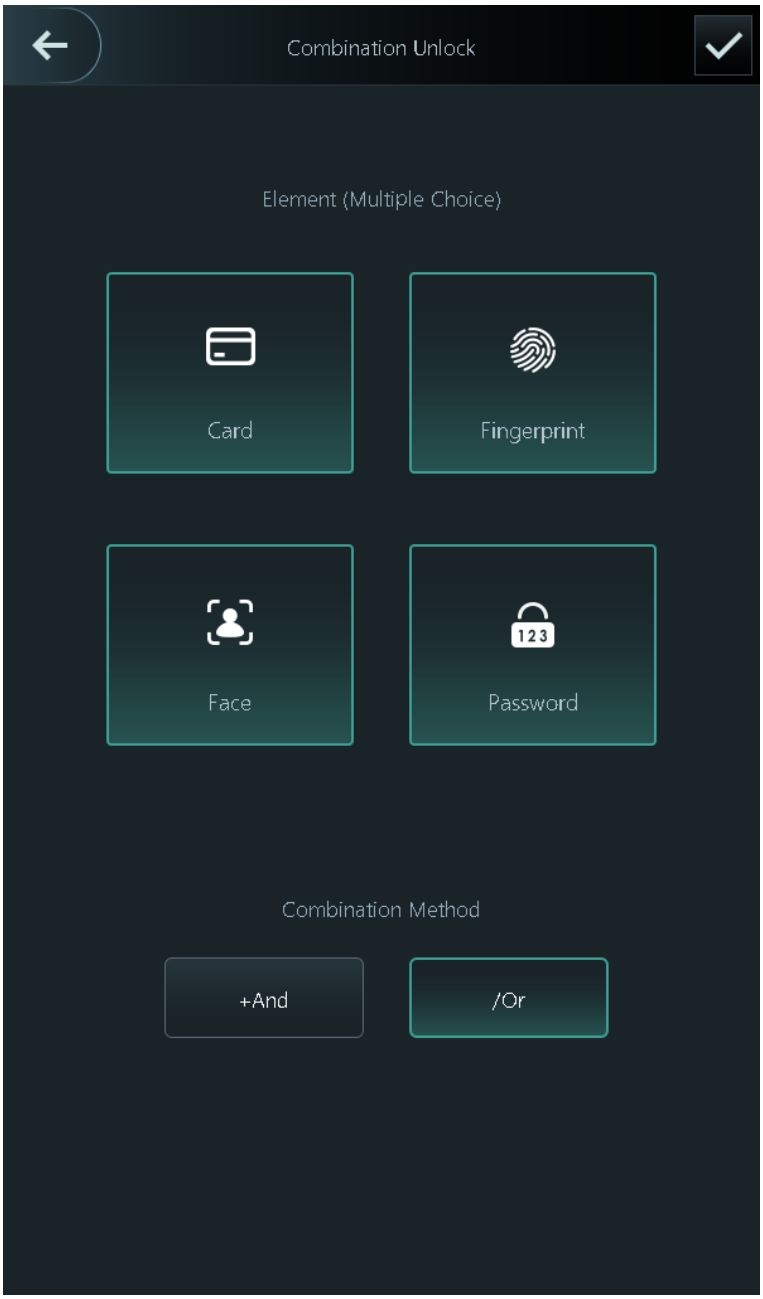
Крок 3 Натисніть +**І**або**/Або**для налаштування комбінацій.

- **+І**: Перевірте всі вибрані методи розблокування, щоб відкрити двері.

  Людям необхідно пройти перевірку в наступному порядку: карта, відбитки пальців, обличчя та пароль.

- **/Або**: Підтвердіть один із вибраних методів розблокування, щоб відкрити двері.

Малюнок 2-4 Елемент (множинний вибір)



Крок 4 Кран для збереження змін.

2.8.2 Налаштування будильників

У разі несанкціонованого доступу до входу або виходу спрацює сигналізація.

Процедура

Крок 1 Вибирати**Управління контролем доступу**>**Тривога**.

Крок 2 Увімкніть тип будильника.

Типи сигналів тривоги можуть бути різними залежно від моделі продукту.

Малюнок 2-5 Сигналізація

Таблиця 2-4 Опис параметрів сигналізації

Параметр	Опис
Антипасбек	Користувачі повинні підтвердити свою особу як для входу, так і для виходу; в в іншому випадку спрацює сигналізація. Це допомагає запобігти передачі власниками карток своїх карток іншим особам для надання їм доступу. Коли включена функція anti-passback, власник картки повинен залишити захищену зону через вихідний зчитувач, перш ніж система знову надасть йому доступ. Людям потрібно провести карткою за зчитувачем "in", щоб увійти до захищеної зони, і провести її за зчитувачем "out", щоб вийти з неї. Поки що послідовність "in, out, in, out і т.д.", система працюватиме нормально. ● Якщо людина увійде після верифікації, але вийде, не пройшовши верифікацію, при повторній спробі входу спрацює сигналізація, та у доступі йому буде відмовлено. ● Якщо людина увійде без перевірки, але вийде після перевірки, якщо повторній спробі входу спрацює сигналізація, та у доступі йому буде відмовлено. Якщо контролер доступу може підключити лише один замок, перевірка на Контролер доступу означає напрям "вхід", а перевірка на зовнішньому зчитувач карток означає напрям "вихід" за замовчуванням. Ви можете змінити налаштування на платформі управління.
Примус	Сигналізація спрацює, якщо для розблокування дверей буде використано карту примус, пароль примус або відбиток пальця примусу.

Параметр	Опис
Вторгнення	Якщо датчик дверцят увімкнений, при ненормальному відкриванні дверей спрацює сигналізація про вторгнення.
Двері зачинені	Сигналізація спрацює, якщо двері залишаться відчиненими довше певного часу. Воно може бути від 1 до 9999 секунд.

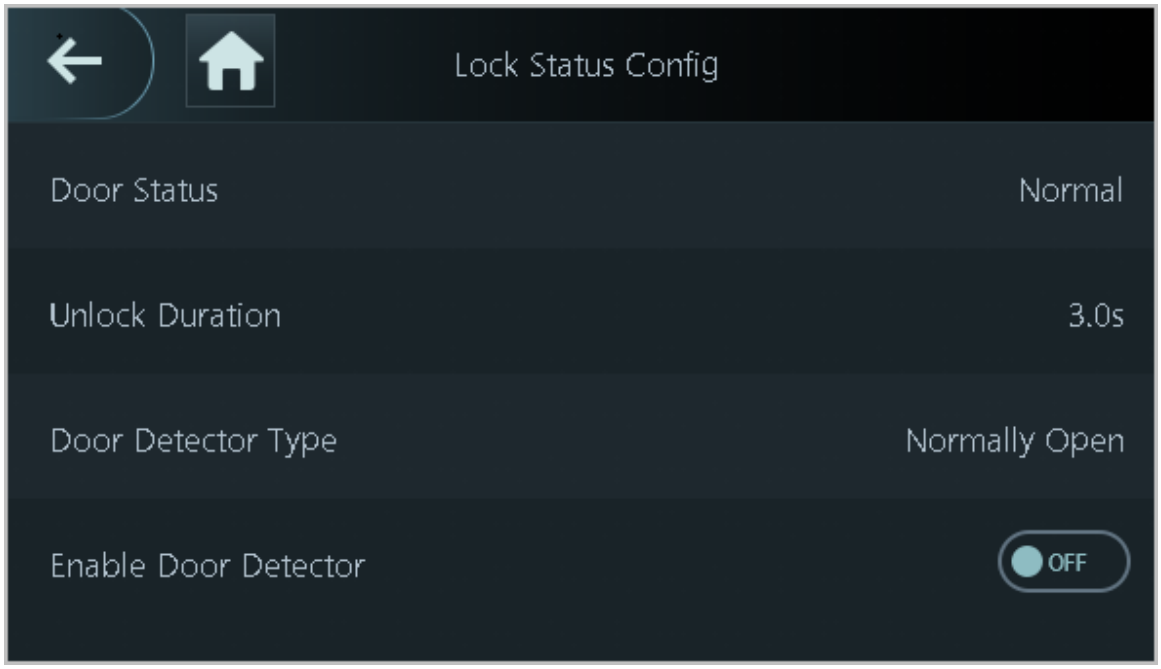
2.8.3 Налаштування статусу дверей

Процедура

Крок 1 на**Головне меню**екран, виберіть**Управління контролем доступу**>**Блокування статусу конфігурації**.

Крок 2 Встановити статус дверей.

Малюнок 2-6 Стан блокування



Таблиця 2-5 Опис параметрів

Параметр	Опис
Стан дверей	● **Нормально відкритий**: Двері весь час залишаються незачиненими ● **Нормально закритий**: Двері весь час залишаються замкненими ● **Нормальний**: Якщо**Нормальний**Якщо вибрано цей параметр, двері замикатимуться та відмикатися відповідно до ваших налаштувань.
Тривалість розблокування	Після того, як людині надано доступ, двері залишаться відчиненими. певного часу, щоб він міг пройти.
Тип дверного детектора	З дверним детектором, підключеним до пристрою, сигнали тривоги можуть спрацьовувати при ненормальному відкритті чи закритті дверей. Дверний детектор включає 2 типи, включаючи NC-детектор та NO-детектор. ● Нормально закритий: датчик знаходиться в замкнутому положенні, коли двері або вікно зачинені. ● Нормально відкритий: Розімкнутий ланцюг створюється, коли вікно чи двері фактично закриті.

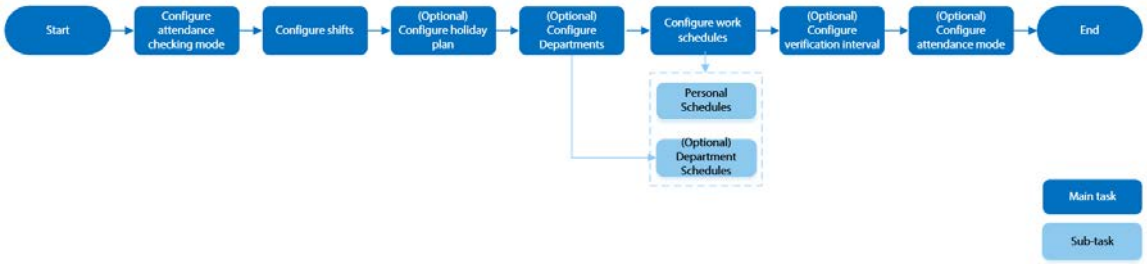
Параметр	Опис
Увімкнути детектор дверей	Сигналізація про вторгнення та закінчення часу виходу з дому набуде чинності тільки після включення цієї функції.

2.9 Управління відвідуваністю

Відвідуваність часу підтримує керування відвідуваністю як на локальному пристрої, так і Smart PSS Lite. У цьому розділ як приклад використовується тільки налаштування відвідуваності на локальному пристрої.

Ця функція доступна лише на деяких моделях серії 4,3 дюйми.

Малюнок 2-7 Схема конфігурації обліку робочого дня



2.9.1 Налаштування відділів

Процедура

Крок 1 Вибирати**Відвідуваність**>**Налаштування відділу**.

Крок 2 Виберіть відділ, а потім перейменуйте його.

Є 20 департаментів за промовчанням. Ми рекомендуємо вам їх перейменувати.

Малюнок 2-8 Створення відділів

Крок 3 Кран

2.9.2 Налаштування змін

Налаштуйте зміни, щоб визначити правила відвідування робочого часу. Співробітники повинні приходити на роботу в запланований час початку зміни та йти у призначений час закінчення, за винятком випадків, коли вони вирішують попрацювати понаднормово.

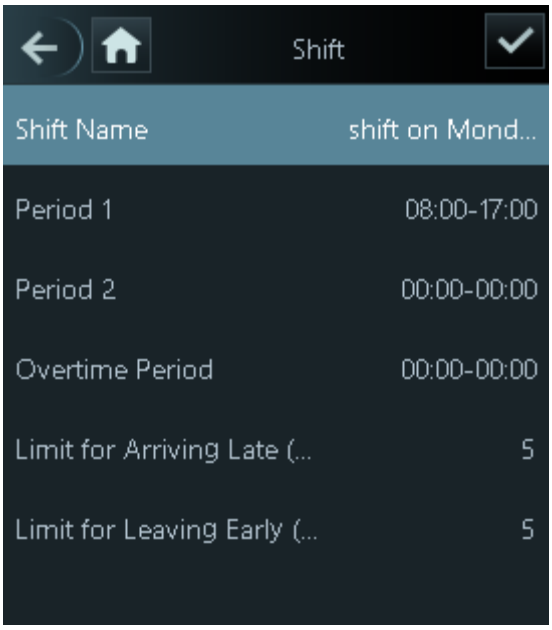
Процедура

Крок 1 Вибирати**Відвідуваність**>**Конфігурація зміни**.

Крок 2 Виберіть зміну.

Крок 3 Натисніть, щоб переглянути більше змін. Ви можете налаштувати до 24 змін. Налаштуйте параметри зміни.

Малюнок 2-9 Створення змін

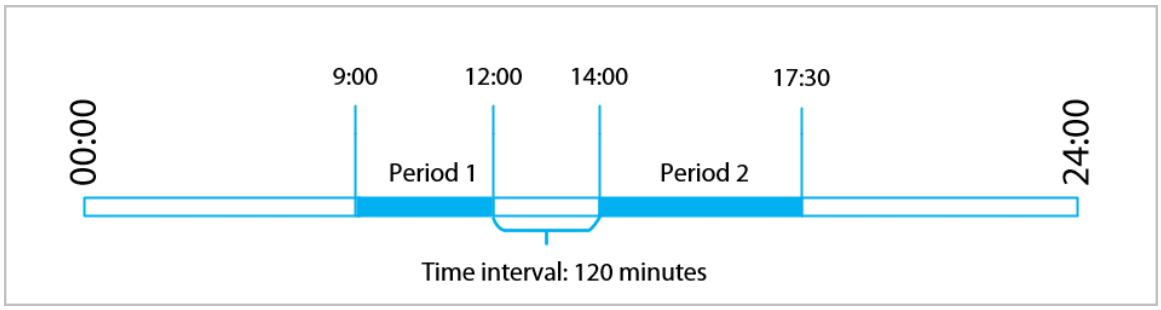


Таблиця 2-6 Опис параметрів зсуву

Параметр	Опис
Назва зміни	Введіть назву зміни.
Період 1	Вкажіть тимчасовий діапазон, протягом якого співробітники можуть відзначати початок та кінець робочого дня. Якщо ви встановлюєте лише один період відвідування, працівники повинні відзначати прихід і догляд у призначений час, щоб уникнути аномалії в них записи про відвідини. Наприклад, якщо ви встановлюєте період з 08:00 до 17:00, співробітники повинні відзначати прихід до 08:00 та відхід з 17:00 і далі. Якщо ви встановите 2 періоди присутності, ці 2 періоди не можуть перетинатися. Співробітники повинні відзначати прихід та догляд для обох періодів.
Період 2	
Період понаднормової роботи	Співробітники, які приходять на роботу або йдуть з роботи протягом певного періоду, вважатимуться працюючими понад звичайний робочий час.
Ліміт запізнення (хв)	Певна кількість часу може бути надана співробітникам, щоб вони могли приходити на роботу трохи пізніше і йти трохи раніше. Наприклад, якщо звичайний час приходу на роботу – 08:00, то допустимий період може бути встановлений у 5 хвилин для співробітників, які приходять до 08:05, щоб не вважатися запізнілими.
Ліміт раннього догляду (хв)	

- Якщо інтервал між двома періодами є парним числом, ви можете розділити інтервал часу на 2 і призначити першу половину інтервалу першому періоду, що буде часом виходу. Другу половину інтервалу слід призначити другому періоду як час приходу.

Малюнок 2-10 Тимчасовий інтервал (парне число)

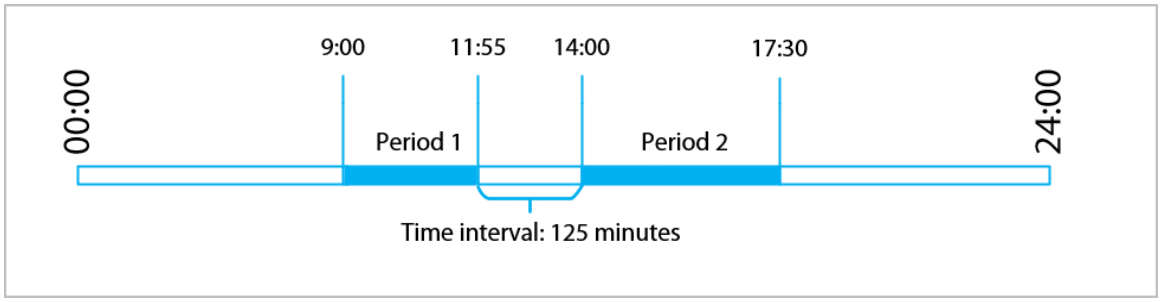


Наприклад: якщо інтервал становить 120 хвилин, то час відходу з роботи для періоду 1 складає з 12:00 до 12:59, а час приходу для періоду 2 складає з 13:00 до 14:00.

Якщо людина йде з роботи кілька разів протягом періоду 1, то дійсним буде останнім часом, а якщо вони реєструються кілька разів протягом періоду 2, найбільш ранній час вважатиметься дійсним.

- Коли інтервал часу між двома періодами є непарним числом, найменша частина інтервалу буде віднесена до першого періоду, що буде часом виходу. Найбільша частина інтервалу буде віднесена до другого періоду як час приходу.

Малюнок 2-11 Тимчасовий інтервал (парне число)



Наприклад: якщо інтервал становить 125 хвилин, то час відходу з роботи для періоду 1 — с 11:55 до 12:57, а час приходу з роботи для періоду 2 – з 12:58 до 14:00. Період 1 триває 62 хвилини, а період 2 - 63 хвилини.

Якщо людина йде з роботи кілька разів протягом періоду 1, то дійсним буде останнім часом, а якщо вони реєструються кілька разів протягом періоду 2, найбільш ранній час вважатиметься дійсним.

Увесь час відвідування точне до секунди. Наприклад, якщо звичайний час приходу час встановлений на 8:05 ранку, співробітник, який прийде на роботу о 8:05:59 ранку, не вважатиметься запізнення. Але співробітника, який прибув о 8:06 ранку, буде відзначено як запізнілий на 1 хвилину.

Крок 4 Кран

2.9.3 Налаштування планів на свята

Налаштуйте плани свят, щоб встановити періоди, протягом яких відвідуваність не відстежуватиметься.

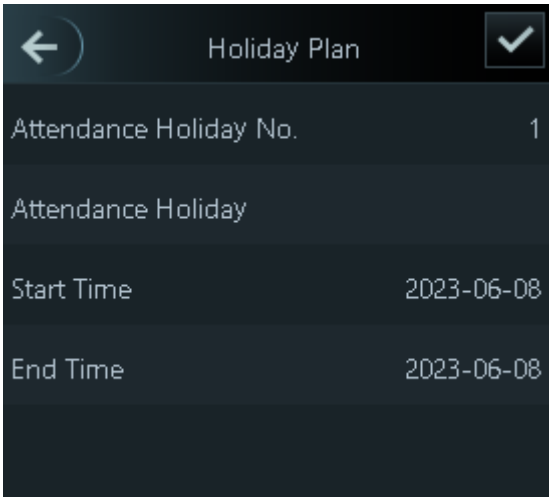
Процедура

Крок 1 Вибрати**Відвідуваність**>**Конфігурація зміни**>**Святковий день**.

Крок 2 Натисніть, щоб додати плани на відпустку.

Крок 3 Налаштуйте параметри.

Малюнок 2-12 Створення планів відпустки



Таблиця 2-7 Опис параметрів

Параметр	Опис
Відвідуваність Свято №	Число свята.
Відвідування свята	Назва свята.
Час початку	Час початку та закінчення свята.
Час закінчення	

Крок 4 Кран

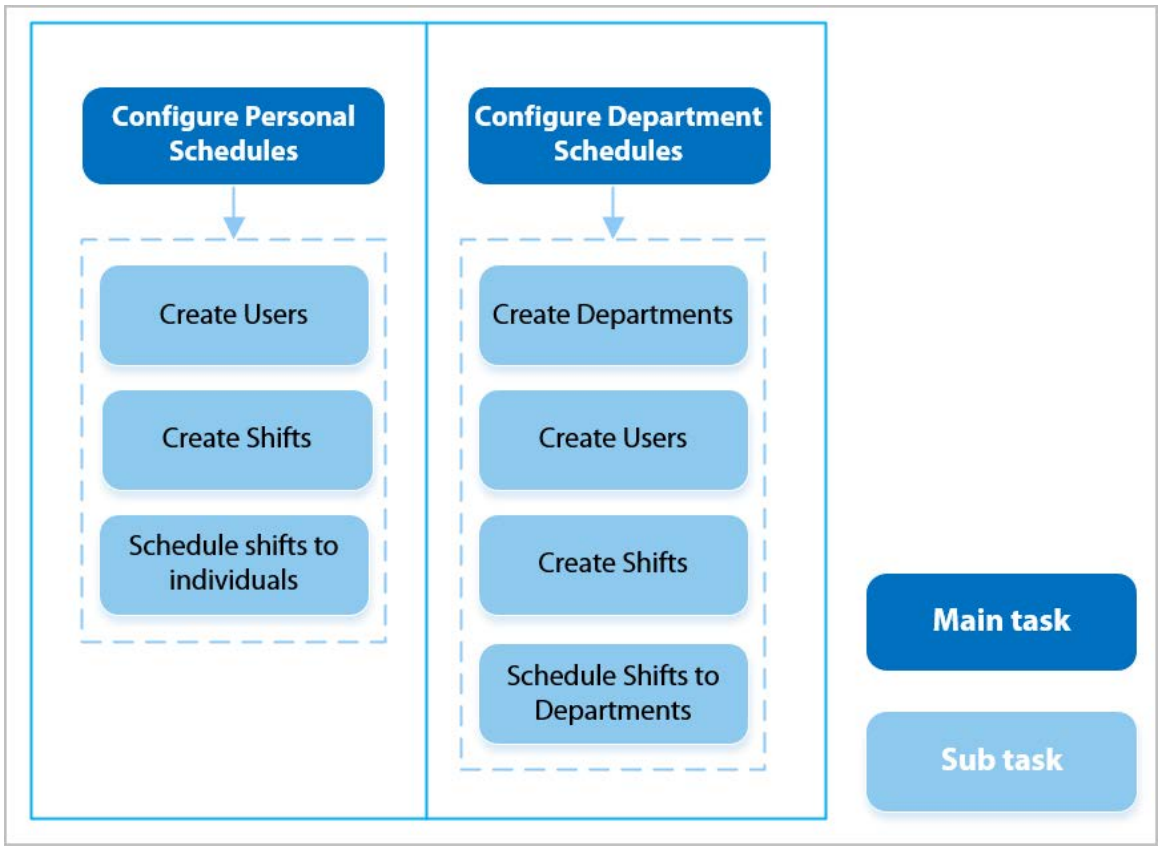
2.9.4 Налаштування графіків роботи

Графік роботи зазвичай відноситься до днів на місяць і годин на день, які співробітник повинен перебувати на роботі. Ви можете створити різні типи графіків роботи на основі різних осіб або відділів, а потім співробітники повинні дотримуватись встановлених графіків роботи.

Довідкова інформація

Скористайтеся блок-схемою для налаштування особистих графіків чи графіків відділів.

Малюнок 2-13 Налаштування графіків роботи



Процедура

Крок 1 Вибирати**Відвідуваність**>**Розклад Конфігурації**.

Крок 2 Встановіть графіки роботи окремих осіб.

1. Натисніть**Особистий розклад**.

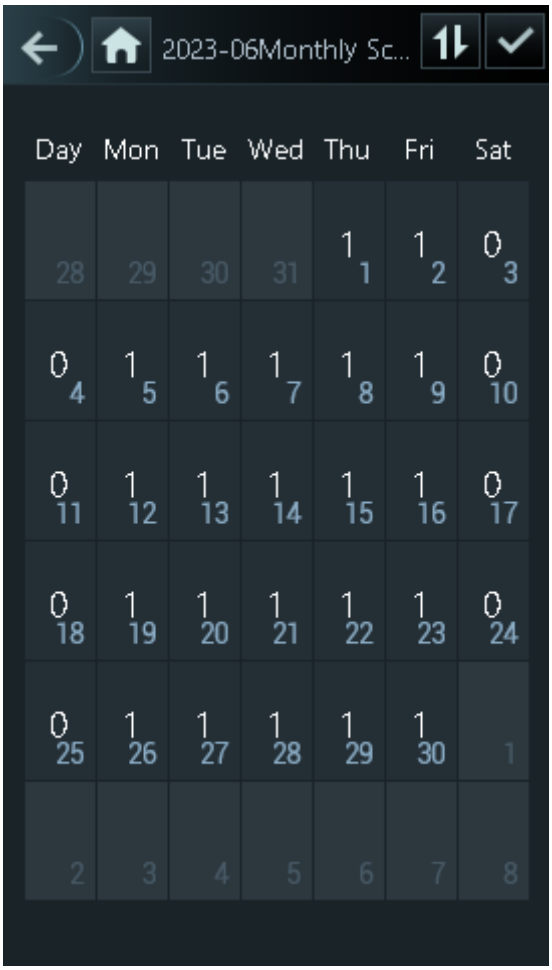
2. Введіть ідентифікатор користувача та натисніть .

3. У календарі виберіть день та зміну. Зміну заплановано на цей день.

Ви можете встановити графіки роботи лише на поточний та наступний місяць.

- 0 вказує на перерву.
- Від 1 до 24 вказує кількість певних змін. Про те, як налаштувати зміни, див. «2.9.2 Налаштування змін».
- 25 вказує на відрядження.
- 26 вказує на відпустку.

Малюнок 2-14 Графік змін для окремих осіб



4. Натисніть.

Крок 3 Встановіть графік роботи для відділів. 1.

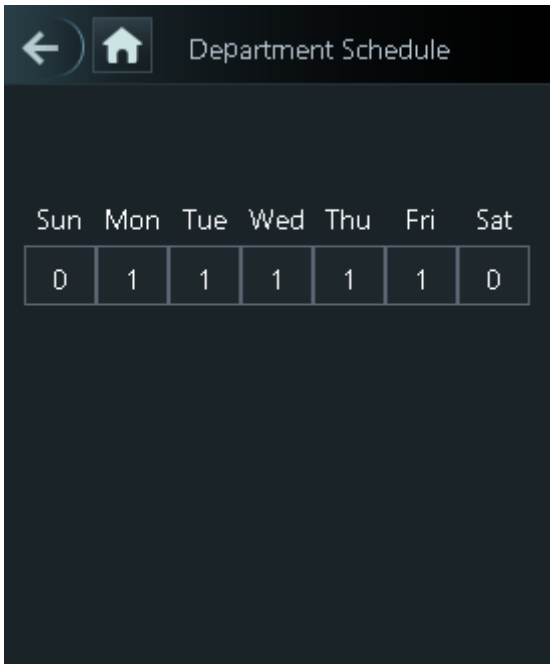
Натисніть**Розклад роботи відділу**.

2. Натисніть на відділ і виберіть зміни на тиждень.

Зміни плануються на тиждень.

- 0 вказує на спокій.
- 1–24 вказує кількість певних змін. Про те, як настроїти зміни, див. "2.9.2 Налаштування змін".
- 25 вказує на відрядження.
- 26 вказує на відпустку.

Малюнок 2-15 Планування змін у відділі



Певний графік роботи складається на тижневий цикл і буде застосовуватися до всіх співробітників відділення.

Крок 4 Кран

2.9.5 Налаштування інтервалу часу перевірки

Якщо співробітник відзначає прихід та відхід з роботи кілька разів протягом встановленого періоду, дійсним буде вважатися найраніше час.

Процедура

Крок 1 Вибирати**Відвідуваність**>**Інтервал перевірки (сек)**.

Крок 2 Введіть інтервал часу та натисніть .

2.9.6 Налаштування режимів присутності

При реєстрації приходу або відходу з роботи ви можете встановити режим обліку відвідуваності, щоб визначити статус відвідуваності.

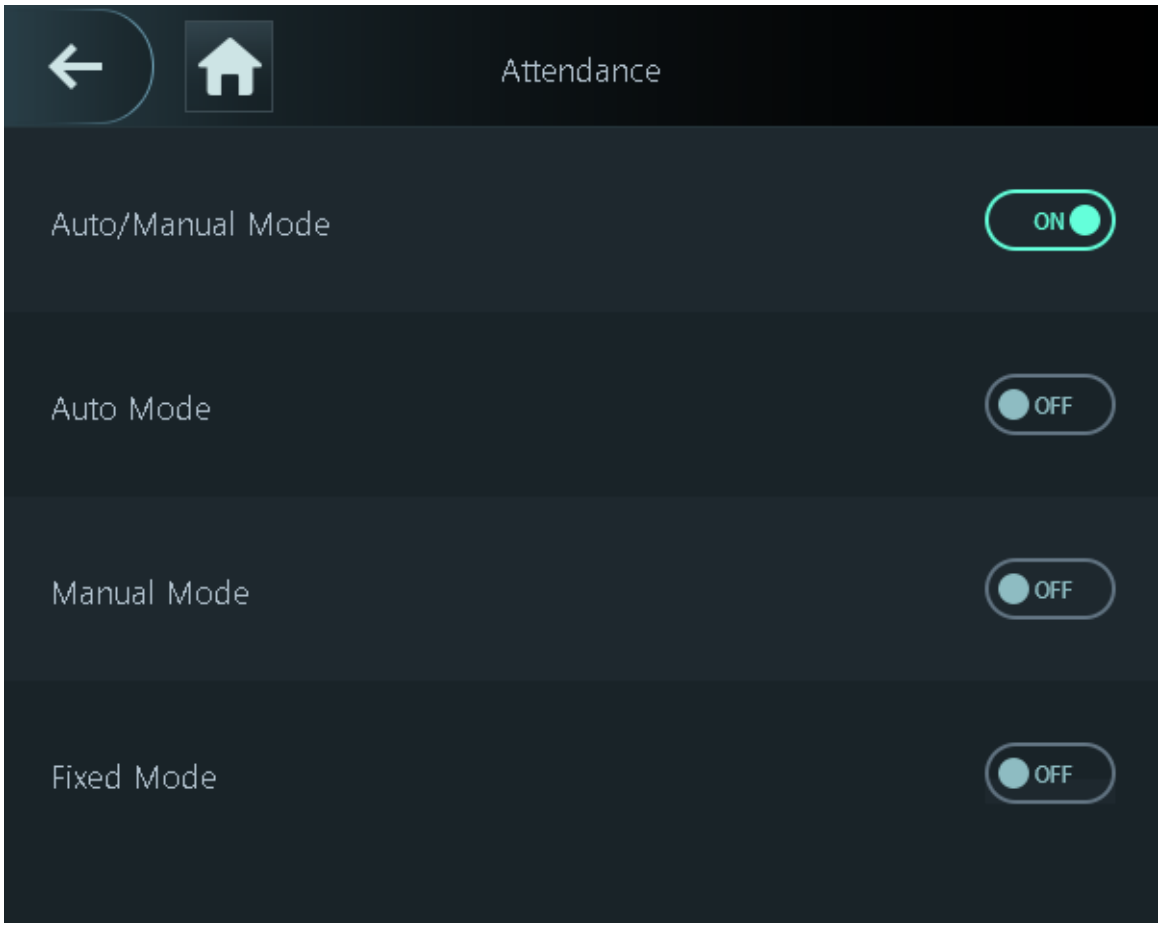
Процедура

Крок 1 На екрані головного меню виберіть**Відвідуваність**>**Налаштування режиму**. Давати

Крок 2 можливість**Локальний чи віддалений**, а потім встановіть режим перебування.

Записи про відвідування також будуть синхронізовані з платформою керування.

Малюнок 2-16 Режим присутності



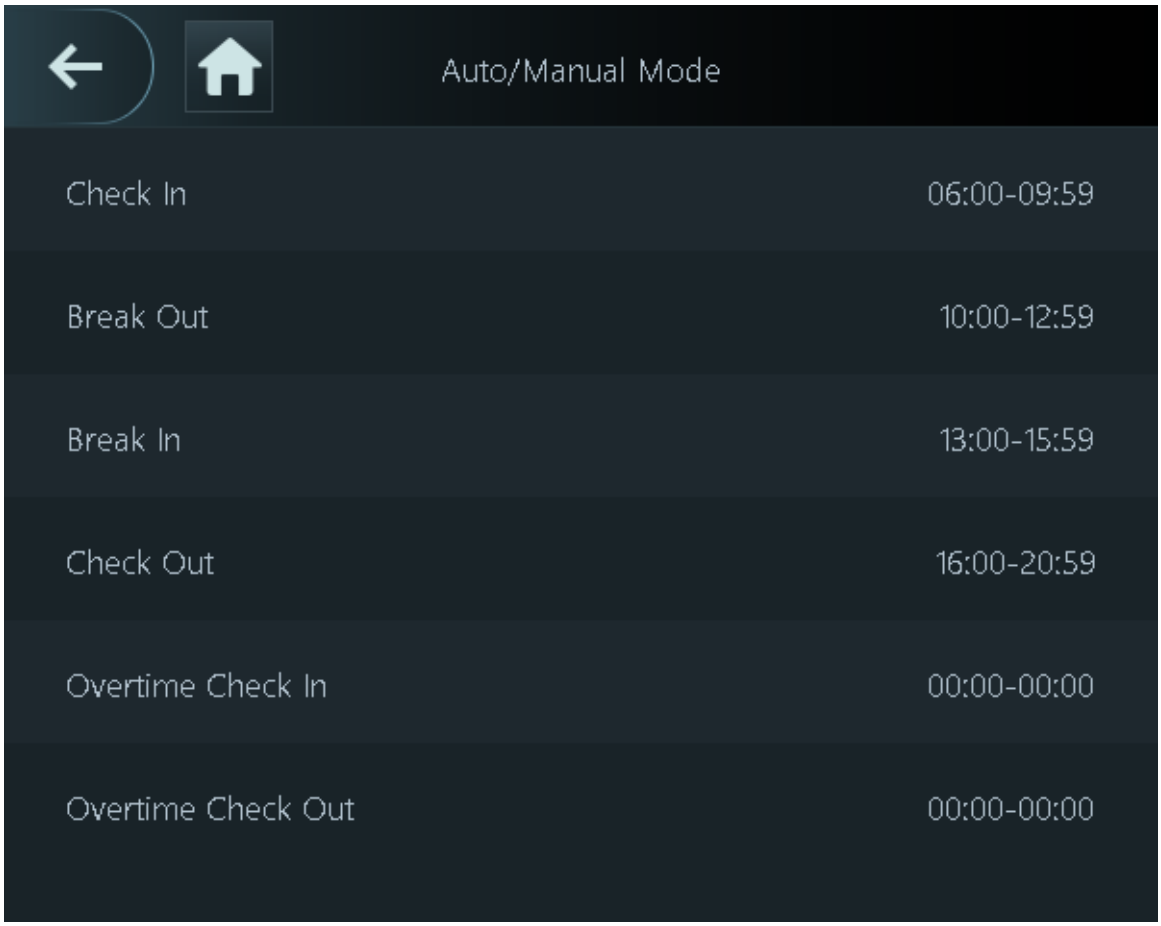
Таблиця 2-8 Режим відвідуваності

Параметр	Опис
Автоматичний/ручний режим	Статус відвідуваності відображається на екрані автоматично після того, як ви зареєструвалися на роботі або пішли з роботи, але ви також можете вручну змінити свій статус відвідуваності.
Автоматичний режим	На екрані автоматично відображається статус відвідування після того, як ви зареєструвалися на роботі чи пішли з роботи.
Ручний режим	Виберіть вручну статус відвідування під час реєстрації приходу або догляду.
Фіксований режим	Під час реєстрації вашого приходу або догляду на екрані весь час відображатиметься заданий статус відвідуваності.

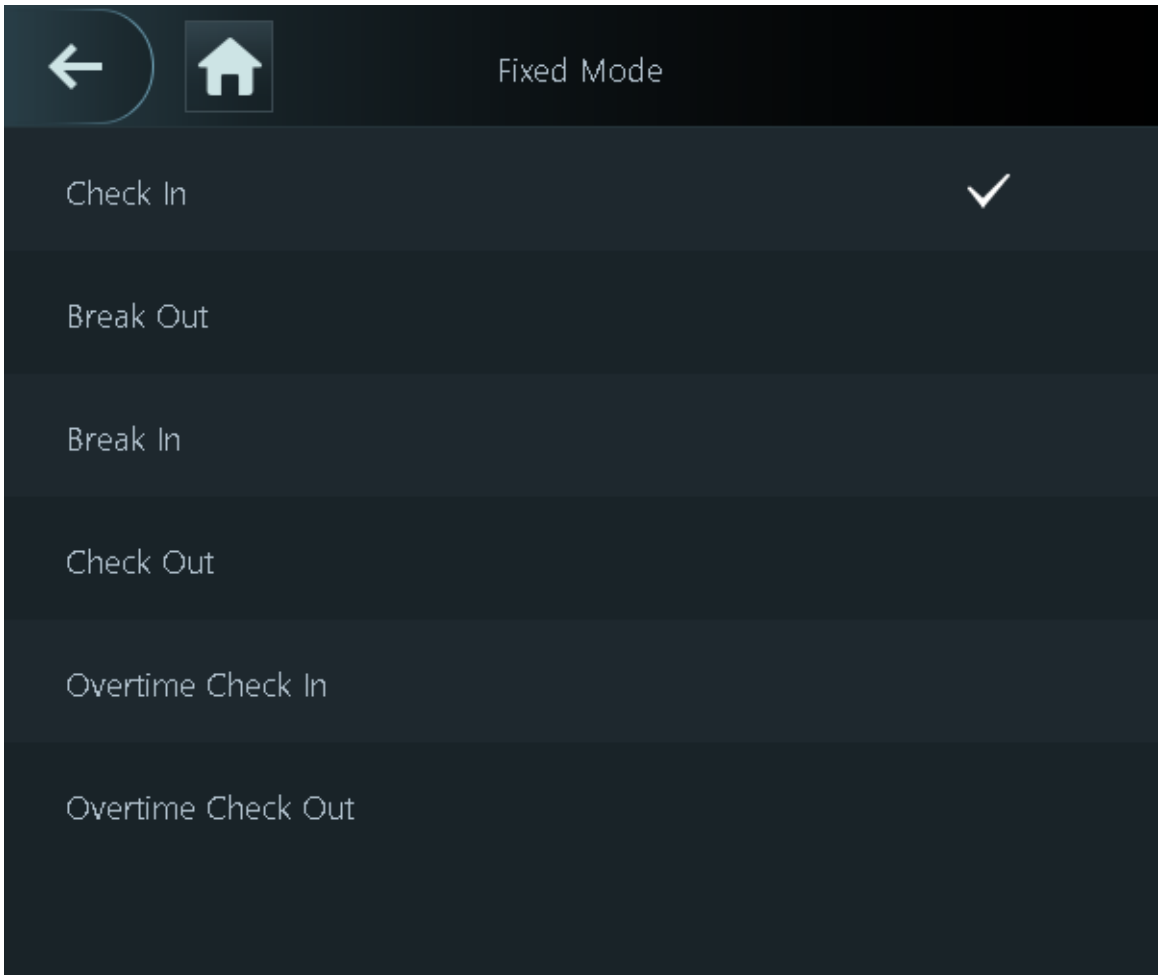
Крок 3 Виберіть режим відвідування.

Крок 4 Налаштуйте параметри присутності.

Малюнок 2-17 Автоматичний/ручний режим



Малюнок 2-18 Фіксований режим



Таблиця 2-9 Параметри режиму відвідуваності

Параметри	Опис
Реєструватися	Зареєструйтесь, коли починається ваш звичайний робочий день.
Вибухнути	Позначте час звільнення, коли почнеться перерва.
Вламуватись	Позначте час закінчення перерви.
Перевірити	Відзначте час відходу з роботи на початку вашого звичайного робочого дня.
Понаднормова реєстрація	Позначте початок понаднормової роботи.
Понаднормова перевірка	Після закінчення понаднормової роботи відзначайте свій відхід з роботи.

2.10 Мережева взаємодія

Налаштуйте мережу, послідовний порт та порт Wiegand для підключення контролера доступу до мережі.

Послідовний порт та порт Wiegand можуть відрізнятися залежно від моделі контролера доступу.

2.10.1 Налаштування IP-адреси

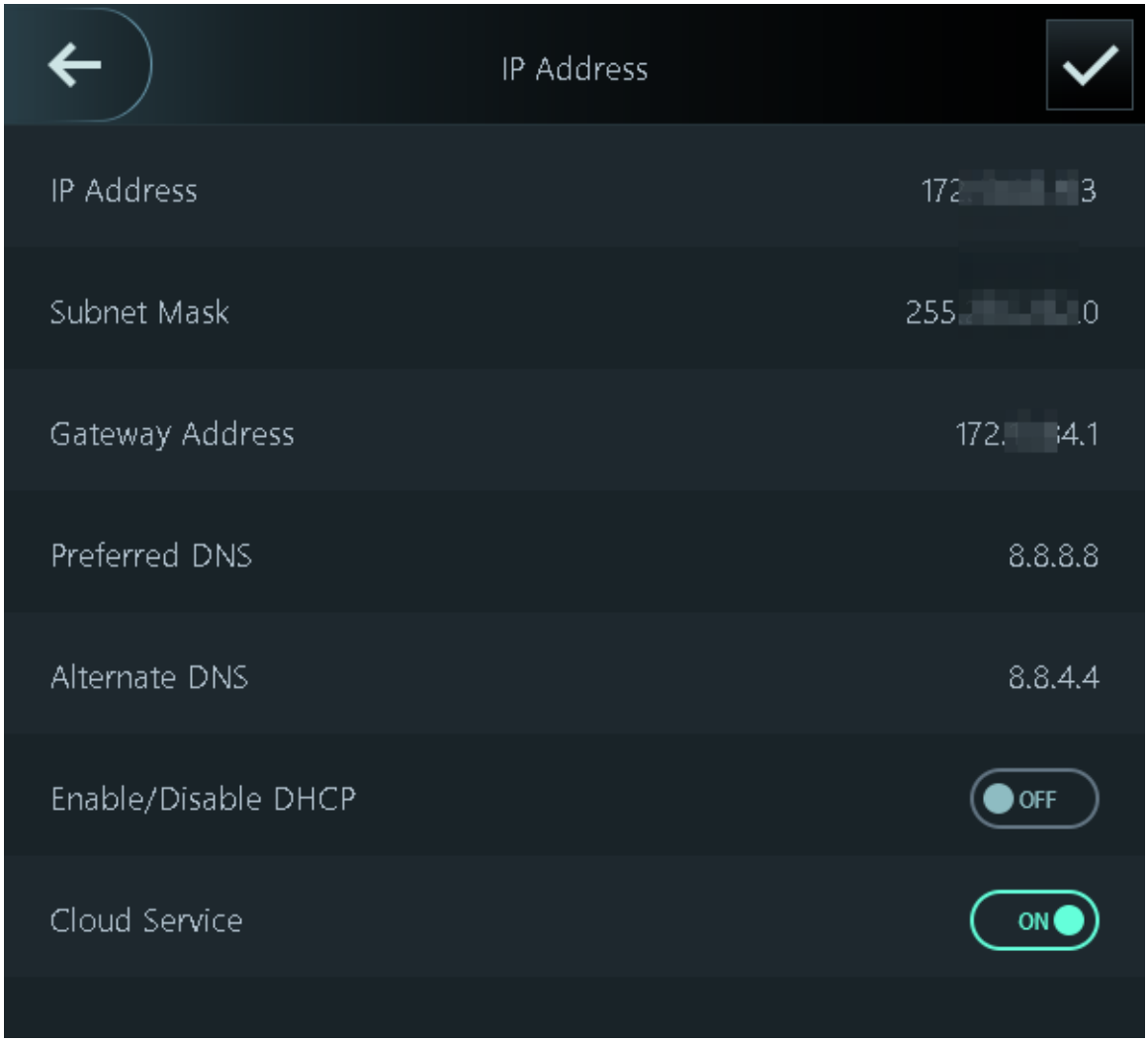
Встановіть IP-адресу для контролера доступу, щоб підключити її до мережі. Після цього ви можете увійти на веб-сторінку та платформу управління, щоб керувати контролером доступу.

Процедура

Крок 1 на**Головне меню**, вибирати**Налаштування зв'язку**>**Мережа**>**IP-адреса**.

Крок 2 Встановіть IP-адресу.

Рисунок 2-19 Конфігурація IP-адреси



Таблиця 2-10 Параметри конфігурації IP

Параметр	Опис
IP-адреса/Маска підмережі/Адреса шлюзу	IP-адреса, маска підмережі та IP-адреса шлюзу повинні знаходитися в одному сегменті мережі.
Переважний DNS	IP DNS-сервер.
Альтернативний DNS	Альтернативна IP-адреса DNS-сервера.

Параметр	Опис
Увімкнути/вимкнути DHCP	Це скорочення від Dynamic Host Configuration Protocol (протокол динамічної конфігурації хоста). При включенні DHCP контролеру доступу автоматично призначаються IP-адреса, маска підмережі та шлюз.
Хмарний сервіс	Керуйте пристроями без використання DDNS, налаштовуйте зіставлення портів та розгортайте транзитні сервери.

2.10.2 Налаштування активної реєстрації

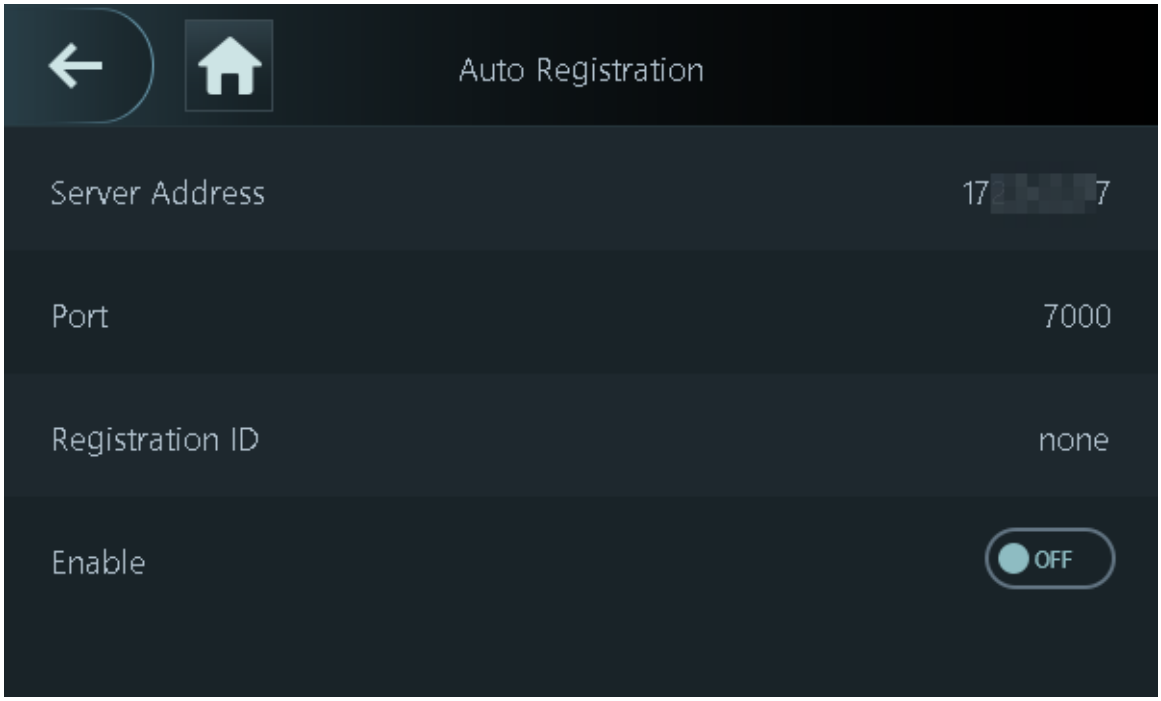
Додайте пристрій на платформу керування, щоб ви могли керувати ним із цієї платформи.

Процедура

Крок 1 на**Головне меню**, вибирати**Комунікація**>**Мережа**>**Автоматична реєстрація**.

Щоб не наражати систему ризиків безпеки та втрати даних, контролюйте управління дозволу платформи.

Малюнок 2-20 Активна реєстрація



Крок 2 Увімкніть функцію автоматичної реєстрації та встановіть параметри.

Таблиця 2-11 Автоматична реєстрація

Параметр	Опис
Адреса сервера	IP-адреса платформи управління.
Порт	Номер порту платформи управління.

Параметр	Опис
Реєстраційний ідентифікатор	Введіть ідентифікатор пристрою (визначається користувачем).  При додаванні контролера доступу до платформи керування реєстраційний ідентифікатор, який ви вводите на платформі управління, має відповідати певного реєстраційного ідентифікатора на контролері доступу.

Крок 3 Увімкніть функцію.

2.10.3 Налаштування Wi-Fi

Ви можете підключити контролер доступу до мережі через мережу Wi-Fi.

Процедура

Крок 1 на**Головне меню**, вибирати**Комунікація**>**Мережа**>**Wi-Fi**.

Крок 2 Увімкніть Wi-Fi.

Функція Wi-Fi доступна лише у деяких моделях.

Крок 3 Кран для пошуку доступних бездротових мереж.

Крок 4 Виберіть бездротову мережу та введіть пароль.

Якщо система не знаходить мережу Wi-Fi, натисніть**SSID**Щоб ввести ім'я Wi-Fi.

Крок 5 Натисніть .

2.10.4 Налаштування послідовного порту

Процедура

Крок 1 на**Головне меню**, вибирати**Налаштування зв'язку**>**Послідовний порт**.

Крок 2 Виберіть тип порту.

Таблиця 2-12 Опис порту

Зовнішній пристрій	Опис
Контролер доступу	Вибирати**Контролер доступу**коли контролер доступу функціонує як зчитувач карток, і контролер доступу буде надсилати дані контролеру доступу для керування доступом. Тип вихідних даних: ● Номер картки: виводить дані на основі номера картки, коли користувачі проводять своєю картою, щоб відімкнути двері; виводить дані на основі номери першої карти користувача, коли користувачі використовують інші методи розблокування ● Ні: Виводить дані на основі ідентифікатора користувача.
Кардрідер	Контролер доступу підключається до зчитувача карток.
Читач (ОСДП)	Контролер доступу підключається до зчитувача карток за протоколом OSDP.

Зовнішній пристрій	Опис
Модуль безпеки керування дверима	Кнопка виходу з дверей, керування замком та пожежний зв'язок стають неефективними після увімкнення модуля безпеки.
Турнікет	Коли контролер доступу підключено до турнікету, а плата контролера доступу турнікета підключена до зовнішнього модуля QR-коду або модуля зчитування карт, плата передаватиме дані перевірки на турнікет.

2.10.5 Налаштування Wiegand

Контролер доступу підтримує як режим уведення, так і режим виведення Wiegand.

Процедура

Крок 1 На веб-сторінці виберіть**Налаштування зв'язку**>**Віганд**.

Крок 2 Виберіть Wiegand.

- Вибирати**Вхід Wiegand**при підключенні зовнішнього зчитувача карток до контролера доступу.
- Вибирати**Вихід Віганда**коли контролер доступу функціонує як зчитувач карток, і вам необхідно підключити його до іншого терміналу доступу.

Малюнок 2-21 Вихід Wiegand

Таблиця 2-13 Опис виходу Wiegand

Параметр	Опис
Тип виходу Wiegand	Виберіть формат Wiegand, щоб прочитати номери карт або ідентифікаційні номери. ● **Віганд26**: Зчитує 3 байти або 6 цифр ● **Віганд34**: Зчитує 4 байти або 8 цифр ● **Віганд66**: Зчитує 8 байт або 16 цифр
Ширина імпульсу	Введіть ширину імпульсу та інтервал виходу Wiegand.

Параметр	Опис
Інтервал імпульсу	
Тип вихідних даних	Виберіть тип вихідних даних. ● **Ні.**: Система виводить дані на основі ідентифікатора користувача. Формат даних - шістнадцятковий або десятковий. ● **Номер картки**: Система виводить дані на основі номера першої картки користувача.

Крок 3 Натисніть**Застосовувати**.

2.11 Системні налаштування

2.11.1 Налаштування часу

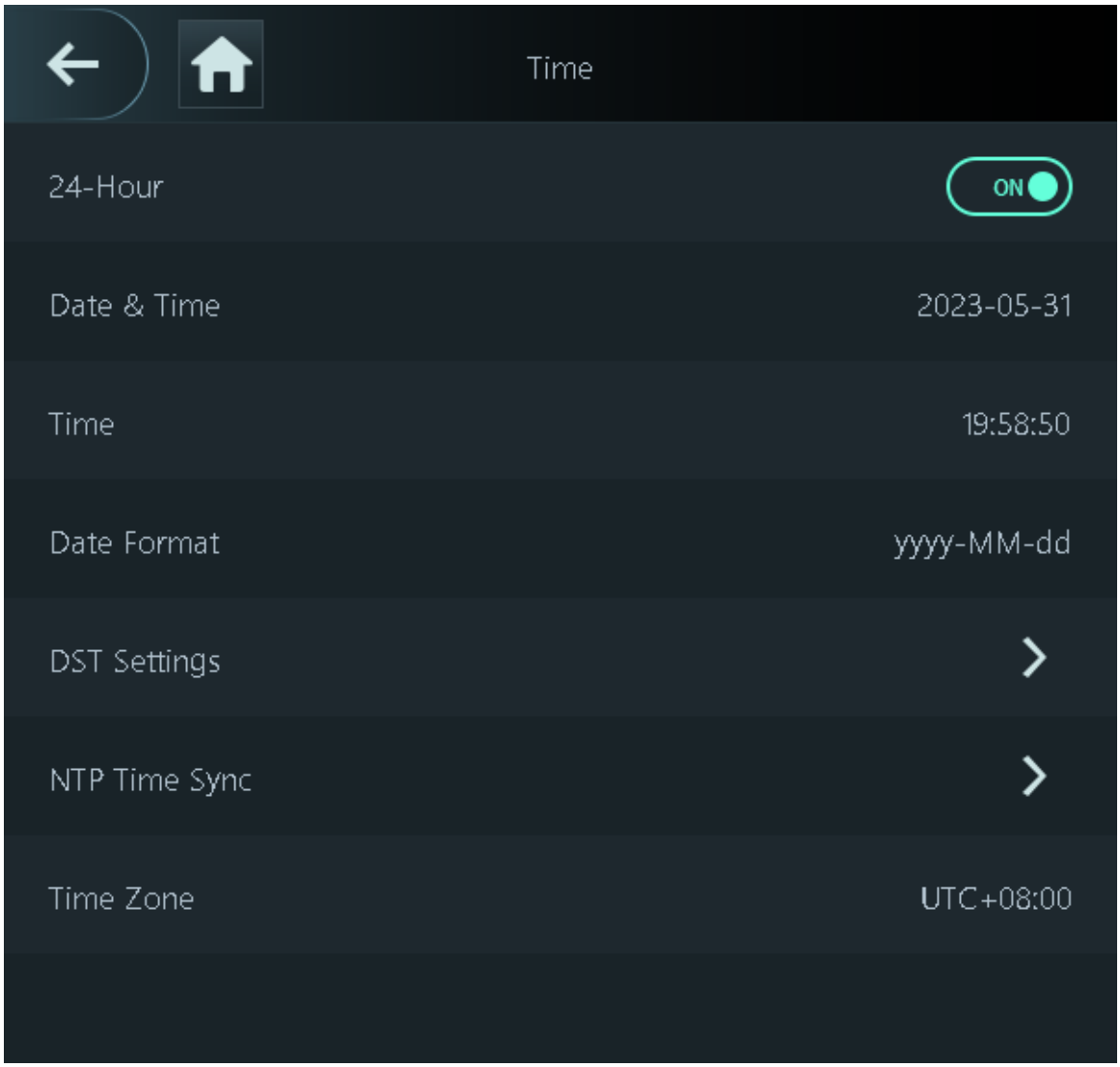
Налаштуйте системний час, такий як дата, час та NTP.

Процедура

Крок 1 на**Головне меню**, вибирати**Системні налаштування**>**Час**.

Крок 2 Налаштуйте системний час.

Малюнок 2-22 Час



Таблиця 2-14 Опис тимчасових параметрів

Параметр	Опис
24-годинна система	Час відображається у 24-годинному форматі.
Дата та час	Призначте дату.
Час	Встановіть час.
Формат дати	Виберіть формат дати.
Налаштування літнього часу	1. Натисніть**Налаштування літнього часу**та увімкніть його. 2. Вибрати**Дата**або**Тиждень**з**літній час**Список типів. 3. Введіть час початку та закінчення. 4. Натисніть

Параметр	Опис
Синхронізація часу NTP	Сервер мережного протоколу часу (NTP) - це машина, виділена в як сервер синхронізації часу для всіх клієнтських комп'ютерів. Якщо ваш комп'ютер налаштовано на синхронізацію з сервером часу в мережі, ваш годинник показуватиме той самий час, що і сервер. Коли адміністратор змінює час (на літній час), всі клієнтські машини в мережі також будуть оновлено. 1. Натисніть**Перевірка НТП**, а потім увімкніть його. 2. Налаштуйте параметри. ● **Адреса сервера**: Введіть IP-адресу NTP-сервера, та контролер доступу автоматично синхронізує час із NTP-сервером. ● **Порт**: Введіть порт NTP-сервера. ● **Інтервал**: Введіть інтервал синхронізації часу.
Часовий пояс	Виберіть часовий пояс.

2.11.2 Налаштування параметрів обличчя

Процедура

Крок 1 У головному меню виберіть**Системні налаштування**>**Конфігурація параметрів**

Крок 2 **особи**. Налаштуйте параметри обличчя та натисніть .

Малюнок 2-23 Параметр особи (01)

Таблиця 2-15 Опис параметрів обличчя

Ім'я	Опис
Поріг розпізнавання обличчя	Налаштуйте рівень точності розпізнавання облич. Вищий поріг означає більш високу точність та менший рівень хибного розпізнавання.
Максимальне відхилення кута розпізнавання обличчя	Встановіть найбільший кут, під яким особа може бути розташована виявлення обличчя. Чим більше значення, тим більше діапазон для кута обличчя. Якщо кут, під яким розташована особа, не входить у заданий діапазон, воно може бути виявлено неправильно.
Відстань між зіницями	Для успішного розпізнавання потрібна певна кількість пікселів між очима, зване зіничною відстанню. Значення за замовчуванням - 45 пікселів. Це число змінюється в залежності від розміру обличчя та відстані між обличчям та лінзою. Якщо доросла людина знаходиться на відстані 1,5 метра від лінзи, зінова відстань зазвичай становить 50-70 пікселів.
Справжній інтервал осіб (сек)	Якщо людина успішно верифікована занадто багато разів, контролер доступу видає запит про успішну верифікацію протягом певного інтервалу часу.
Недійсний інтервал осіб (сек)	Якщо людині не вдається пройти верифікацію обличчя надто багато разів, контролер доступу видає повідомлення про невдалу верифікацію протягом певного проміжок часу.
Включити антиспуфінг	Це не дозволяє людям використовувати фотографії, відео, маски та інші замінники для отримання несанкціонованого доступу.
Увімкнути Beautifier	Прикрасьте зроблені знімки облич.
Увімкнути виявлення шолома	Виявляє захисні каски. Двері не будуть розблоковані для людей, які не носять каску.
Параметри маски	● Режим маски: ◇ **Не виявляти**: Маска не виявляється при розпізнаванні обличчя ◇ **Нагадування про маску**: Маска виявлена під час розпізнавання обличчя Якщо людина не носить маску, система нагадає їй про необхідність надіти маску, але доступ їй все одно буде дозволено. ◇ **Без маски вхід не дозволено**: Маска виявлена під час розпізнавання обличчя Якщо людина не носить маску, система нагадає їй про необхідність надіти маску, і доступ буде заборонено. ● Поріг розпізнавання маски: чим вищий поріг, тим точніше буде розпізнавання обличчя людини в масці і тим нижче буде хибне розпізнавання.

Ім'я	Опис
Розпізнавання кількох осіб	Розпізнає від 4 до 6 зображень облич одночасно. Комбінована розблокування не може бути використане з цим, і двері будуть розблоковані, коли один із людей успішно пройде перевірку.  Кількість підтримуваних зображень осіб може різнитися залежно від моделі товару.
Режим освітлювача	● Авто: Підсвічування вмикається в умовах низького освітлення. ● Вимкнути: освітлювач постійно вимкнений.  Ця функція доступна лише в деяких моделях.

2.11.3 Настроювання гучності

Ви можете налаштувати гучність динаміка та мікрофона.

Процедура

Крок 1 на**Головне меню**, вибрати**Системні налаштування**>**Налаштування гучності**.

Крок 2 Вибрати**Гучність звукового сигналу**або**Гучність мікрофона**, а потім натиснітьабо щоб налаштувати гучність.

2.11.4 Налаштування мови

Змініть мову на контролері доступу.**Головне меню**, вибрати**Системні налаштування**> **Мова**, виберіть мову для контролера доступу.

2.11.5 Налаштування екрана

Налаштуйте час вимкнення дисплея та час виходу із системи.

Процедура

Крок 1 на**Головне меню**, вибрати**Система**>**Налаштування екрана**. Кран**Час виходу із системи**або**Налаштування вимкнення екрана**, а потім натисніть або для налаштування часу.

- Час виходу із системи: система повертається в режим очікування після певного часу бездіяльності.
- Налаштування вимкнення екрана: система повертається до екрана очікування, а потім екран вимикається після певного часу бездіяльності. Наприклад, якщо час виходу з системи встановлено на 15 секунд, а час вимкнення екрана встановлено на 30 секунд, система повертається до екрана очікування через 15 секунд, потім екран вимикається ще через 15 секунд.

Час виходу з системи повинен бути меншим за час вимкнення екрана.

2.11.6 (Необов'язково) Налаштування параметрів відбитків пальців

Налаштуйте точність виявлення відбитків пальців. Чим вище значення, тим вище поріг схожості та точність.

Довідкова інформація

Ця функція доступна лише на деяких моделях, а деякі підтримують підключення до відбитка пальця. модуль розширення.

Процедура

Крок 1 на**Головне меню**, вибрати**Системні налаштування**>**Налаштування параметрів відбитків пальців**.

Крок 2 Натисніть або , щоб налаштувати значення.

2.11.7 Відновлення заводських налаштувань

Процедура

Крок 1 на**Головне меню**, вибрати**Системні налаштування**>**Заводські налаштування за замовчуванням**.

Крок 2 Відновіть заводські налаштування, якщо потрібно. Відновіть заводські налаштування, якщо потрібно.

- **Заводські налаштування за замовчуванням**: Скидає всі конфігурації та дані, за винятком параметрів IP та типу модуля розширення
- **Відновити параметри за замовчуванням (за винятком інформації про користувача та журналів)**: Скидає все конфігурації, за винятком інформації про користувача та журналів.

2.11.8 Перезавантаження пристрою

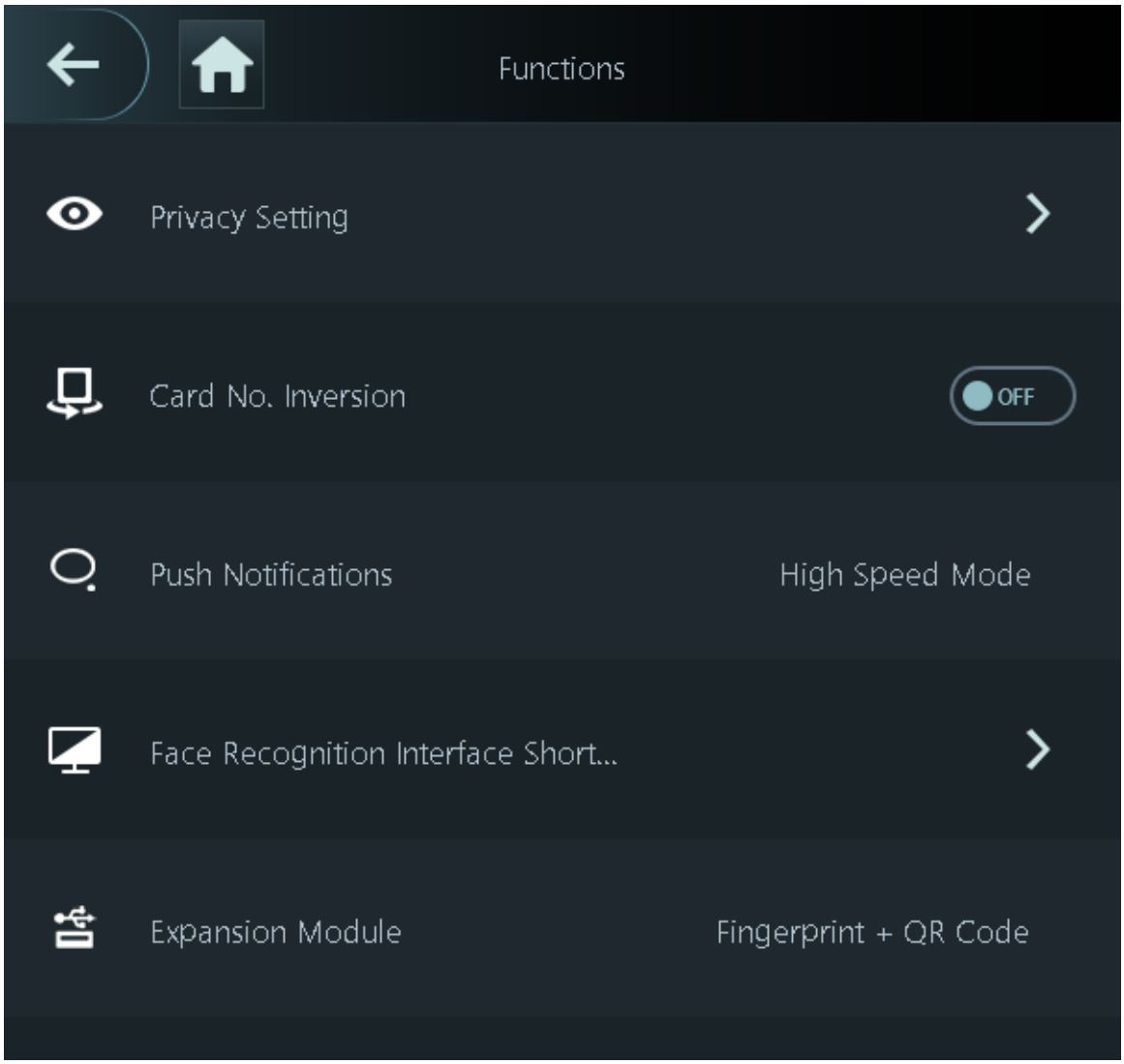
на**Головне меню**, вибрати**Системні налаштування**>**Перезапуск**, та контролер доступу буде перезапущено.

2.12 Налаштування функцій

на**Головне меню**екран, виберіть**Функції**.

Функції можуть відрізнятися залежно від моделі виробу.

Малюнок 2-24 Функції



Таблиця 2-16 Опис функції

Параметр	Опис
Приватна ситуація	● Скидання пароля: пароль можна скинути, увімкнувши цю функцію. ● УвімкнутиHTTPS: Hypertext Transfer Protocol Secure (HTTPS) – це протокол для безпечного зв'язку через комп'ютерну мережу. Якщо увімкнено HTTPS, для доступу до команд CGI використовуватиметься HTTPS; в в іншому випадку буде використовуватися HTTP. При увімкненні HTTPS контролер доступу автоматично перезапуститься. ● УвімкнутиCGI: Common Gateway Interface (CGI) пропонує стандартний протокол для веб-серверів для виконання програм, аналогічних тому, як консольні програми працюють на сервері, що динамічно генерує веб-сторінки. CG I включений за замовчуванням. ● УвімкнутиSSH: Secure Shell (SSH) - це криптографічний мережевий протокол для безпечної роботи мережевих служб незахищеної мережі. Дані, що передаються, будуть зашифровані після включення цієї функції. ● Зображення відбитка пальця: Зображення відбитка пальця відображається під час розблокування за допомогою відбитка пальця. Ця функція доступна лише в деяких моделях. ● Захоплення: зображення обличчя будуть захоплюватися автоматично, коли люди відчиняють двері. Функцію увімкнено за замовчуванням. ● Очистити всі знімки: видалити всі автоматично зроблені фотографії.
Номер картки. Інверсія	Коли контролер доступу під'єднується до стороннього пристрою через вхідний порт Wiegand, а номер картки, який зчитує контролер доступу, знаходиться в зворотному порядку від фактичного номера картки. У цьому випадку ви можете увімкнути цю функцію.

Параметр	Опис
Push-сповіщення	Відображає повідомлення на екрані, коли людина перевіряє свою особу на контролері доступу. ● Режим високої швидкості: система пропонує**Успішно перевірено**або**Не авторизовано**на екрані. ● Простий режим: відображає ідентифікатор користувача, ім'я та час перевірки після надання доступу, а також відображає**Не авторизовано**та час авторизації після відмови у доступі. ● Стандарт: відображає зареєстроване зображення особи користувача, ідентифікатор користувача, ім'я та час перевірки після надання доступу, а також відображає**Не авторизовано**та час перевірки після відмови у доступ. ● Контрастний режим: відображає захоплене зображення обличчя та зареєстроване зображення особи користувача, ідентифікатор користувача, ім'я та час авторизації після надання доступу, а також відображає**Не авторизовано**після відмови у доступі.
Ярлик інтерфейсу розпізнавання осіб	Виберіть методи перевірки особи на екрані очікування. ● Пароль: його піктограма відображається на екрані в режимі очікування. ● QR-код: його піктограма відображається на екрані в режимі очікування. ● Дверний дзвінок: його піктограма з'являється на екрані в режимі очікування. ◇ Дзвінок: натисніть піктограму дзвінка на екрані режиму очікування та контролер доступу задзвонить. ◇ Будильник: натисніть на значок дзвіночка і зовнішній пристрій сигналізації задзвонить. Ця функція доступна лише в деяких моделях. ◇ Налаштування рінгтону: виберіть рінгтон ◇ Час рінгтону (сек): Встановіть час дзвінка (1-30 секунд). Значення за замовчуванням – 3. ● Дзвінок: його піктограма відображається на екрані в режимі очікування. ● Тип виклику: ◇ Виклик кімнати: натисніть піктограму виклику в режимі очікування та введіть номер кімнати, щоб здійснити дзвінок. ◇ Центр керування викликами: натисніть піктограму дзвінка в режимі очікування, а потім зателефонуйте до центру керування. ◇ Користувацька кімната для дзвінків: натисніть піктограму дзвінка на екрані очікування, щоб зателефонувати до заздалегідь визначеної кімнати. Переконайтеся, що контролер доступу додано до DMSS. ● УвімкнутиSIP: можна ввімкнути SIP, щоб налаштувати контролер доступу на SIP-сервер.

Параметр	Опис
Модуль розширення	Виберіть модуль розширення і контролер доступу перезавантажиться. ●  відображається у правому кутку екрана в режимі очікування, що означає, що налаштування пройшло успішно. ●  відображається у правому кутку екрана очікування, що означає збій налаштування.  ● Модуль розширення доступний лише у деяких моделях. ● Модуль розширення не підтримує гарячу заміну. ● Конфігурація для модуля розширення залишається не зміниться навіть після відновлення заводських налаштувань системи.

2.13 Керування USB-пристроями

Ви можете використовувати USB для оновлення контролера доступу, а також експортувати або імпортувати інформацію про користувачів або запису про відвідування через USB.

- Перед експортом даних або оновленням переконайтеся, що USB-накопичувач вставлений у контролер доступу. система. Щоб уникнути збою, не витягуйте USB і не виконуйте жодних операцій. Контролер під час процесу.
- Для експорту інформації з контролера доступу на інші пристрої необхідно використовувати USB-накопичувач. Обличчя Імпорт зображень через USB не дозволяється.
- Імпорт/експорт записів про відвідування доступний лише на деяких моделях.

2.13.1 Експорт на USB

Ви можете експортувати дані з контролера доступу до USB. Експортовані дані зашифровані та не можуть бути редаговані.

Процедура

Крок 1 на**Головне меню**, вибирати**USB-керування**>**USB-експорт**. Виберіть тип

Крок 2 даних, які ви хочете експортувати, а потім натисніть**ДОБРЕ**.

- Після експорту даних до Excel їх можна редагувати.
- USB-диск підтримує формат FAT32, а ємність сховища становить 4 ГБ-128 ГБ.

2.13.2 Імпорт із USB

Ви можете імпортувати дані з USB-накопичувача в контролер доступу.

Процедура

Крок 1 на**Головне меню**, вибирати**USB-керування**>**USB-імпорт**. Виберіть тип

Крок 2 даних, які ви хочете експортувати, а потім натисніть**ДОБРЕ**.

2.13.3 Оновлення системи

Оновіть систему контролера доступу через USB.

Процедура

Крок 1 Перейменуйте файл оновлення на «update.bin», помістіть його в кореневий каталог USB-накопичувача, а потім вставте USB-накопичувач у контролер доступу.

Крок 2 на**Головне меню**, вибирати**USB-керування**>**Оновлення через USB**. Кран

Крок 3 **ДОБРЕ**.

Контролер доступу перезавантажиться після завершення оновлення.

Не вимикайте контролер доступу під час оновлення.

2.14 Управління записами

У головному меню виберіть**Управління записами**>**Пошук записів розблокування**. Відображаються записи розблокування.

Ви можете шукати записи за ідентифікатором користувача.

2.15 Системна інформація

Ви можете переглянути обсяг даних та версію пристрою.

2.15.1 Перегляд ємності даних

на**Головне меню**, вибирати**Системна інформація**>**Місткість даних**, можна переглянути ємність сховища кожного типу даних.

2.15.2 Перегляд версії пристрою

на**Головне меню**, вибирати**Системна інформація**>**Версія пристрою**, можна переглянути версію пристрою, таку як серійний номер, версію програмного забезпечення та багато іншого.

3 веб-операції

На веб-сторінці також можна налаштувати та оновити контролер доступу.

Веб-конфігурації залежить від моделі контролера доступу.

3.1 Ініціалізація

Ініціалізуйте контролер доступу під час першого входу на веб-сторінку або після відновлення заводських налаштувань контролера доступу.

Передумови

Переконайтеся, що комп'ютер, який використовується для входу на веб-сторінку, знаходиться в тій самій локальній мережі, що й контролер доступу.

Процедура

Крок 1 Відкрийте браузер, перейдіть за IP-адресою (адреса за замовчуванням - 192.168.1.108) контролера доступу.

Ми рекомендуємо використовувати останню версію Chrome або Firefox.

Крок 2 Виберіть мову на контролері доступу.

Крок 3 Встановіть пароль та адресу електронної пошти, дотримуючись інструкцій на екрані.

- Пароль повинен складатися з 8–32 непустих символів та містити не менше двох типи наступних символів: великі, малі, цифри та спеціальні символи (за винятком ' " ; : &). Встановіть пароль високого ступеня безпеки за паролем. підказка за силою.
- Зберігайте пароль у безпеці після ініціалізації та регулярно змінюйте його, щоб підвищити безпеку.

3.2 Вхід у систему

Процедура

Крок 1 Відкрийте браузер, введіть IP-адресу контролера доступу у полі**Адреса**та натисніть клавішу Enter.

Крок 2 Введіть ім'я користувача та пароль.

- Ім'я адміністратора за замовчуванням – admin, а пароль – той, який ви встановили. під час ініціалізації. Ми рекомендуємо вам регулярно змінювати пароль адміністратора для підвищення безпеки.
- Якщо ви забули пароль адміністратора, ви можете натиснути**Забули свій пароль?**Для подробиці,

Крок 3 Натисніть**Авторизуватися**.

3.3 Скидання пароля

Якщо ви забули пароль адміністратора, скиньте пароль за допомогою електронного листа, надісланого за посиланням.

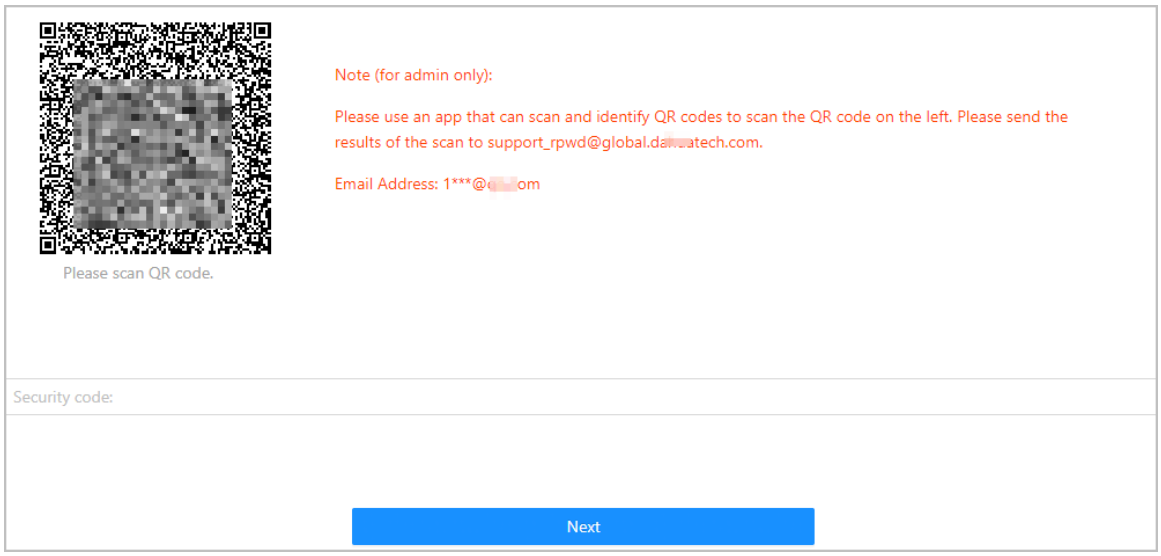
Процедура

Крок 1 На сторінці входу натисніть**Забули пароль**.

Крок 2 Уважно прочитайте підказку на екрані, а потім натисніть

Крок 3 **ДОБРЕ**. Відскануйте QR-код і ви отримаєте код безпеки.

Малюнок 3-1 Скидання пароля



- При скануванні того самого QR-коду буде згенеровано до двох кодів безпеки. Якщо код безпеки став недійсним, оновіть QR-код і знову відскануйте.
- Після сканування QR-коду ви отримаєте код безпеки на вказану вами адресу електронної пошти. адресу. Використовуйте код безпеки протягом 24 годин після отримання. Інакше він буде стають недійсними.
- Якщо неправильний код безпеки буде введено 5 разів поспіль, обліковий запис адміністратора буде заблоковано. заморожено на 5 хв.

Крок 4 Введіть код безпеки.

Крок 5 Натисніть**Наступний**.

Крок 6 Скиньте та підтвердіть пароль.

Пароль повинен складатися з 8–32 непустих символів та містити не менше двох з наступних символів:

такі типи символів: великі літери, малі літери, цифри та спеціальні символи

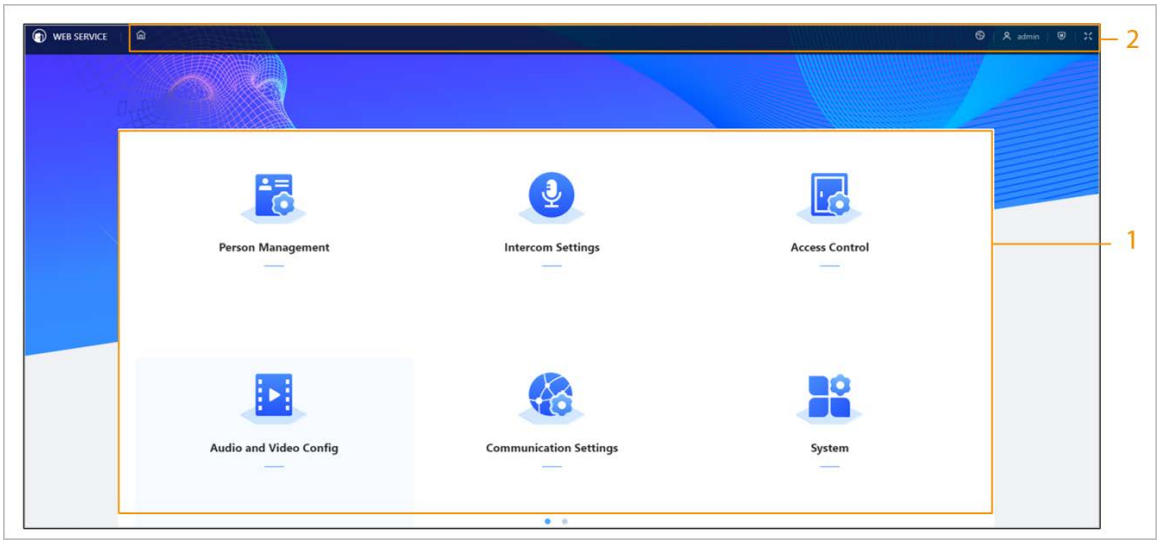
(за винятком ' " ; : &).

Крок 7 Натисніть**ДОБРЕ**.

3.4 Домашня сторінка

Домашня сторінка відображається після успішного входу до системи.

Малюнок 3-2 Домашня сторінка



Таблиця 3-1 Опис домашньої сторінки

Ні.	Опис
1	Головне меню.
2	• : Увійдіть на домашню сторінку • : Відображення на весь екран. • : Введіть**Безпека**сторінка. • admin: Вийдіть із системи або перезавантажте пристрій. • : Виберіть мову на пристрої.

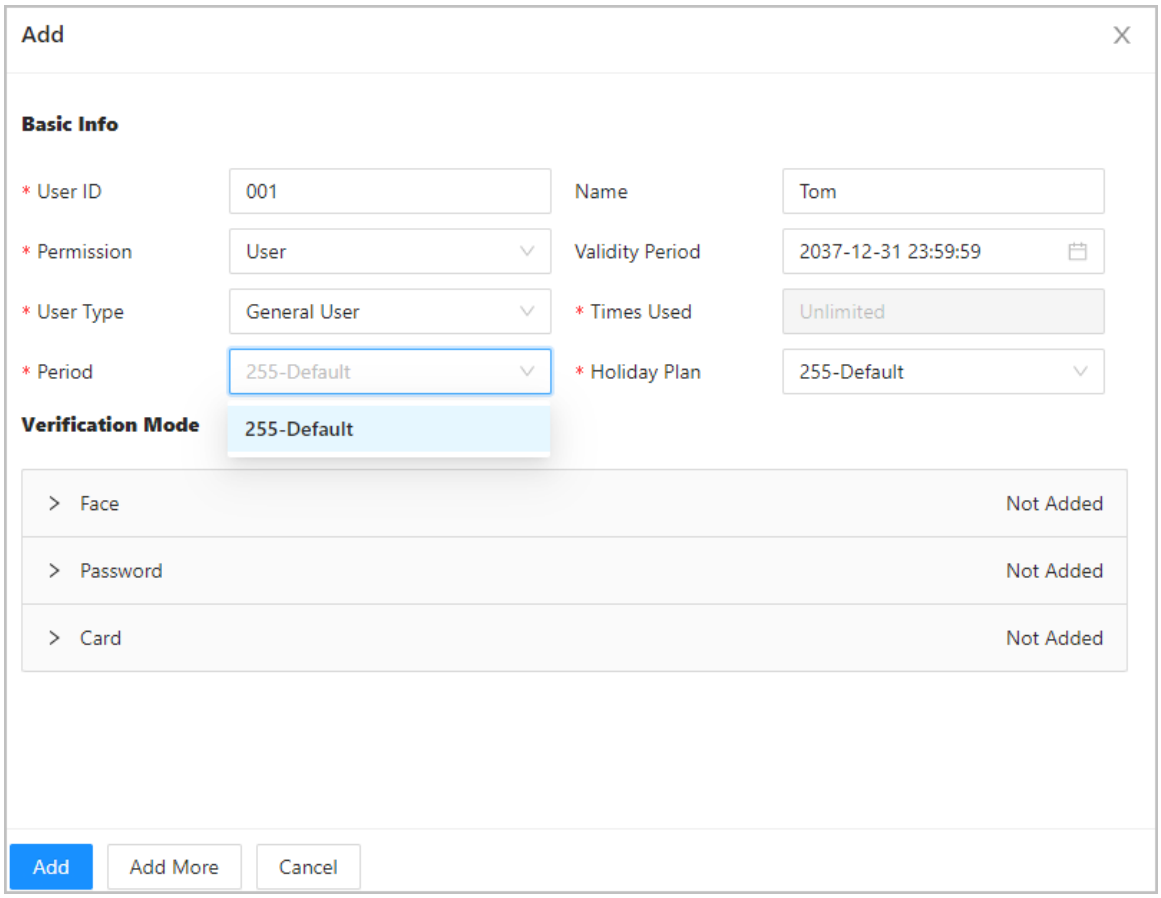
3.5 Додавання користувачів

Процедура

Крок 1 На головній сторінці виберіть**Управління персоналом**, а потім натисніть**Додавати**.

Крок 2 Налаштуйте інформацію про користувача.

Малюнок 3-3 Додавання користувачів



Таблиця 3-2 Опис параметрів

Параметр	Опис
ID користувача	Ідентифікатор користувача схожий на ідентифікатор співробітника та може складатися з цифр, літер та їх комбінацій, а максимальна довжина номери складає 32 символи.
Ім'я	Ім'я може містити до 30 символів (включаючи цифри, символи та літери).
Дозвіл	● **Користувач**: Користувачі мають лише дозвіл на доступ до дверей або облік. робочого часу. ● **Адмін**: Адміністратори можуть налаштовувати контролер доступу, крім дозволів на доступ до дверей та відвідуваність.
Термін дії	Встановіть дату, коли закінчується термін дії дозволів на доступ до дверей та присутність людини.

Параметр	Опис
Тип користувача	● **Звичайний користувач**: Звичайні користувачі можуть розблокувати двері. ● **Чорний список користувачів**: Коли користувачі з чорного списку відчиняють двері, обслуговуючий персонал отримує повідомлення. ● **Гість Користувач**: Гості можуть розблокувати двері протягом певного періоду чи певну кількість разів. Після закінчення певного періоду або часу розблокування вони не зможуть розблокувати двері. ● **Патрульний користувач**: Патрульні користувачі можуть реєструвати присутність на контролері доступу, але вони не мають доступу до дверей дозволу. ● **VIP-користувач**: Коли VIP-клієнт відчинить двері, обслуговуючий персонал отримає повідомлення. ● **Інший користувач**: Коли вони відчиняють двері, вона залишається відкритою ще 5 секунд. ● Користувальницький користувач1/Користувач 2: Те ж, що і у звичайних користувачів.
Час використання	Встановіть ліміт розблокування для відвідувачів. Після того, як час розблокування закінчиться, вони не можуть розблокувати двері.
Період	Люди можуть відчиняти двері або приймати відвідувачів протягом певного періоду.
План відпустки	Люди можуть відчиняти двері або приймати відвідувачів протягом певного періоду.
Обличчя	Натисніть**Завантажити**завантажити зображення обличчя. Кожна людина може додати лише до 2 зображень обличчя. Ви можете переглянути або видалити зображення обличчя після завантаження. Зображення особи має бути у форматі jpg і мати розмір менше 100 КБ.

Параметр	Опис
Картка	● Введіть номер картки вручну. 1. Натисніть**Додавати**. 2. Введіть номер картки та натисніть**Додавати**. ● Автоматично зчитує номер через зчитувач карток. 1. Переконайтеся, що кард-рідер підключено до вашого комп'ютера. 2. Натисніть**Прочитати карту**, а потім проведіть карткою по зчитувачу. Відображається 60-секундний зворотний відлік, щоб нагадати вам про необхідність провести карти, та система автоматично рахує номер картки. Якщо 60-секундний зворотний відлік минув, натисніть**Прочитати карту**ще раз, щоб розпочати новий відлік. 3. Натисніть**Додавати**. Користувач може зареєструвати максимум до 5 карток. Введіть номер своєї карти або проведіть нею по зчитувачу, після чого дані картки будуть раховані контролером доступу. Ви можете увімкнути**Карта примусу**функція. Сигналізація спрацює, якщо для розблокування дверей буде використано карту примусу. ● : Встановити примусову карту. ● : Редагувати номер картки. Один користувач може встановити лише одну примусову карту.
Пароль	Введіть пароль користувача. Максимальна довжина пароля – 8 цифр. Пароль примусу – це пароль розблокування + 1. Наприклад, якщо пароль користувача – 12345, пароль примусу буде 12346. Сигналізація примусу спрацює, якщо для розблокування дверей буде використано пароль примусу.
ФП	Реєстрація відбитків пальців. Користувач може зареєструвати до 3 відбитків пальців, і ви можете встановити відбиток пальця для відбитка пальця примусу. Сигналізація спрацює, якщо відбиток примусового пальця буде використаний для розблокування дверей. ● Функція відбитків пальців доступна лише на деяких моделі. ● Ми не рекомендуємо вам встановлювати перший відбиток пальця як відбиток пальця під примусом. ● Один користувач може встановити лише один відбиток пальця під примусом. ● Функція відбитків пальців доступна, якщоAccess Контролер підтримує підключення зчитувача модуля відбитків пальців.
Відділення	Додати користувачів до відділу. Якщо розклад відділу

Параметр	Опис
Режим розкладу	призначені людині, вони слідуватимуть встановленому графіку відділу. Про те, як створити відділ, див. розділ "2.9.1 Налаштування відділів". ● Розклад відділу: Призначте розклад відділу користувачеві. Докладніше див. у розділі "2.9.4 Налаштування розкладів роботи. ● Персональний графік: Призначте персональний графік користувачеві. Докладніше див. у розділі "2.9.4 Налаштування робочих графіків".  ◇ Ця функція доступна лише в деяких моделях. ◇ Якщо ви встановите режим розкладу на відділ розклад тут, особистий розклад у вас є налаштовано для користувача в**Відвідуваність**>**Розклад Зміни**>**Особистий розклад**недійсно.

Крок 3 Натисніть**ДОБРЕ**.

Пов'язані операції

- Імпортувати інформацію про користувача: Натисніть**Експортувати шаблон**, і завантажте шаблон і введіть в нього інформацію про користувачеві. Помістіть зображення обличчя та шаблон в той самий шлях до файлу, а потім натисніть**Імпорт інформації про користувача** для імпорту папки.

  Одночасно можна імпортувати до 10000 користувачів.
- Очистити: Очистити всіх користувачів.

3.6 Налаштування інтеркому

Контролер доступу може функціонувати як дверна станція для реалізації відеодомофону.

Функція внутрішнього зв'язку доступна лише в деяких моделях.

3.6.1 Використання пристрою як SIP-сервера

3.6.1.1 Налаштування SIP-сервера

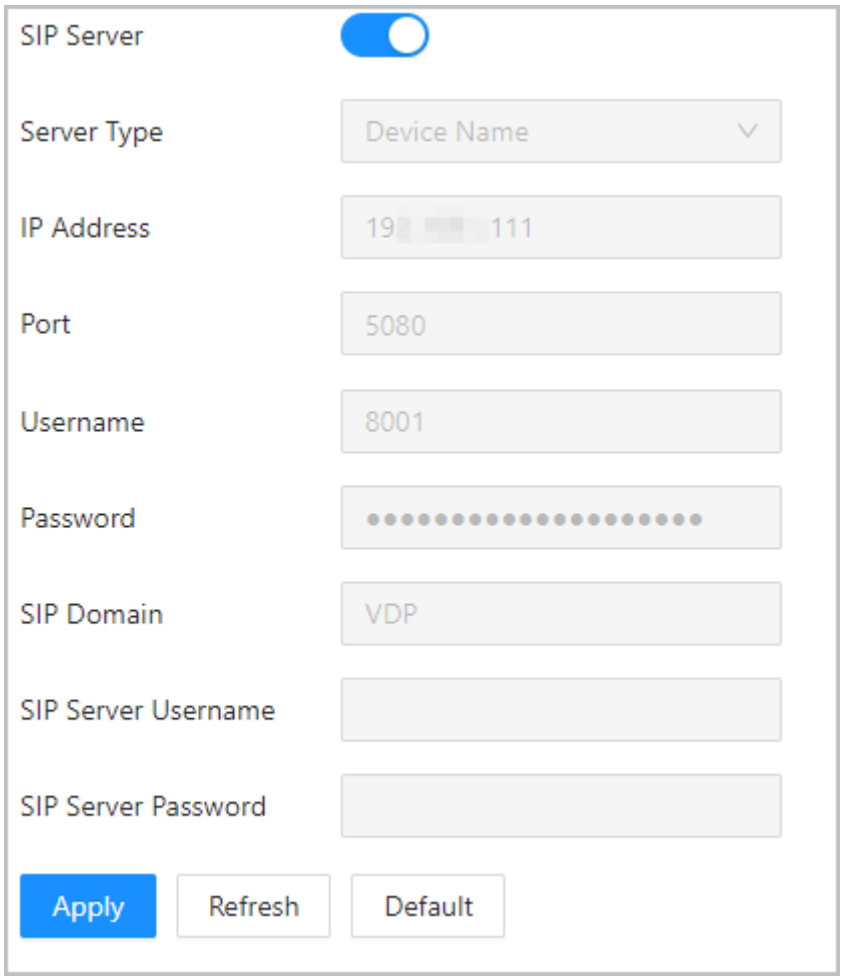
Коли контролер доступу функціонує як SIP-сервер, він може підключати до 500 пристроїв контролю доступу та відеодомофонів.

Процедура

Крок 1 Вибирати**Налаштування домофону**>**SIP-сервер**.

Крок 2 Вмикати**SIP-сервер**.

Рисунок 3-4 Використання контролера доступу як SIP-сервер



Крок 3 Натисніть**Застосовувати**.

3.6.1.2 Налаштування локальних параметрів

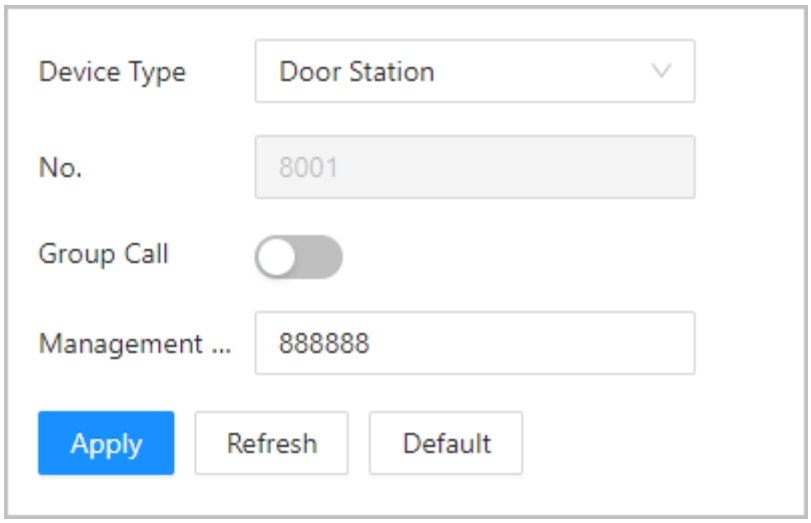
Коли Ваш пристрій функціонує як SIP-сервер, налаштуйте параметри Вашого пристрою.

Процедура

Крок 1 Вибирати**Налаштування домофону**>**Конфігурація локального**

Крок 2 **пристрої**. Налаштуйте параметри.

Рисунок 3-5 Основний параметр



Таблиця 3-3 Опис основних параметрів

Параметр	Опис
Тип пристрою	Вибирати**Дверна станція**.
Ні	Не вдається встановити.
Груповий виклик	При включенні функції групового виклику дверна станція одночасно викликає основний VTH та розширення. Налаштування набирає чинності після перезапуску дверної станції.
Центр управління	Стандартний номер дзвінка — 888888+VTS No. Щоб дізнатися VTS No, перейдіть на сторінку**Проект Налаштування**>**Загальний**центр управління.

Крок 3 Натисніть**Застосовувати**.

3.6.1.3 Додавання VTO

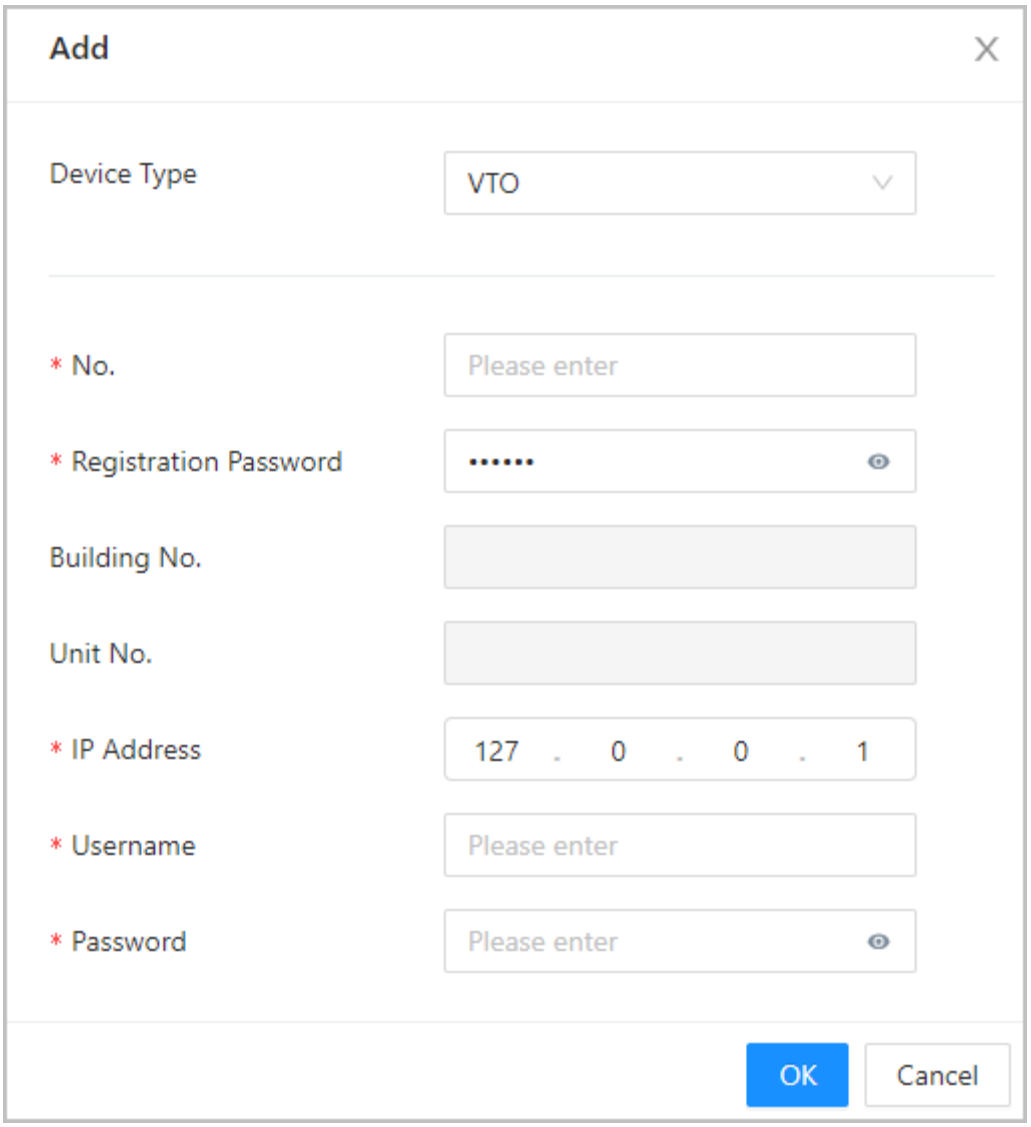
Коли контролер доступу функціонує як SIP-сервер, вам необхідно додати VTO до SIP-сервера, щоб вони могли дзвонити один одному.

Процедура

Крок 1 На веб-сторінці контролера доступу виберіть**Налаштування домофону**>**Налаштування пристрою**.

Крок 2 Натисніть**Додавати**, а потім настройте VTO.

Малюнок 3-6 Додати VTO



Таблиця 3-4 Додати конфігурацію VTO

Параметр	Опис
Тип пристрою	Вибрати**СОТ**.
Ні.	Введіть номер VTO. Щоб дізнатися номер VTO, перейдіть на сторінку**Пристрій**екран СОТ.
Реєстрація Пароль	Залишіть значення за промовчанням.
Номер будівлі Номер блоку	Неможливо настроїти.
IP-адреса	IP-адреса доданого VTO.
Ім'я користувача Пароль	Ім'я користувача та пароль, які використовуються для входу на веб-сторінку доданого VTO.

Крок 3 Натисніть**ДОБРЕ**.

3.6.1.4 Додавання VTH

Коли пристрій функціонує як SIP-сервер, ви можете додати всі VTH до одного пристрою до SIP-сервера.

щоб переконатися, що вони можуть телефонувати один одному.

Довідкова інформація

- За наявності основного VTH та додаткового номера спочатку необхідно увімкнути функцію групового дзвінка, а потім потім додайте основний VTH і розширення на**Управління ВТХ**сторінка. Як увімкнути групу виклик функції, див. «3.6.1.2 Налаштування локальних параметрів».
- Розширення не може бути додане, якщо не додано основні відеодомофони.

Процедура

Крок 1 На головній сторінці виберіть**Налаштування домофону**>**Налаштування пристрою**.

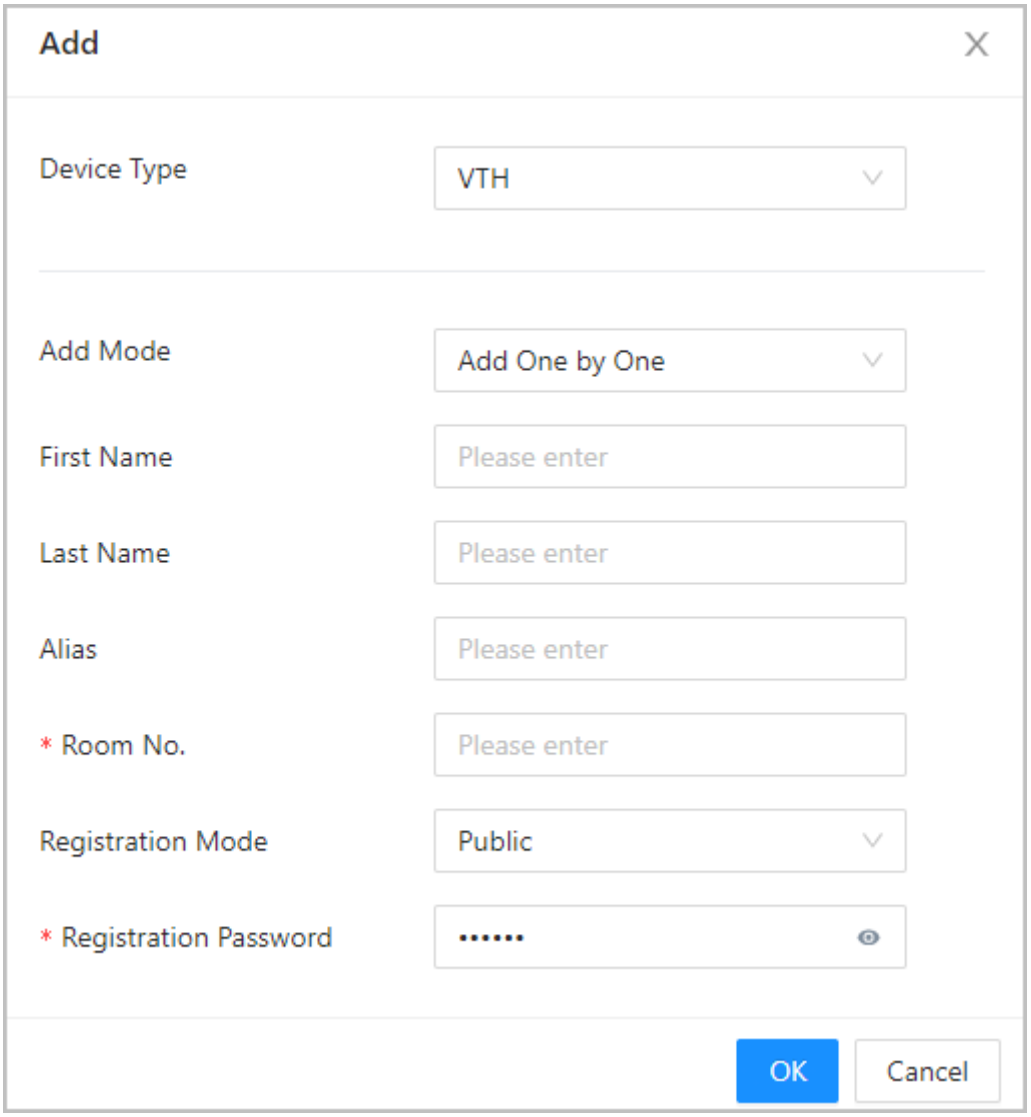
Крок 2 Додати VTH.

- Додайте по одному.

  1. Натисніть**Додавати**.

  2. Налаштуйте параметри та натисніть**ДОБРЕ**.

Малюнок 3-7 Додайте по одному



Таблиця 3-5 Інформація про номер

Параметр	Опис
Ім'я	Введіть назву VTH, щоб легко розрізняти VTH.
Прізвище	
Псевдонім	
Номер кімнати	Введіть номер кімнати VTH. ● Номер кімнати складається з1–5 цифр і має відповідати номер кімнати на відеодомофоні. ● Коли є основнийVTH та розширення, номер кімнати основного VTH закінчується на -0, а номер кімнати розширення закінчується на -1, -2 чи -3. Наприклад, основний VTH – 101-0, а номер кімнати розширення – 101-1, 101-2... ● Якщо функція групового дзвінка не увімкнена, номер кімнати в формат 9901-xx встановити неможливо.
Номер кімнати	Введіть номер кімнати VTH. ● Номер кімнати складається з1–5 цифр і має відповідати номер кімнати на відеодомофоні. ● Коли є основнийVTH та розширення, номер кімнати основного VTH закінчується на -0, а номер кімнати розширення закінчується на -1, -2 чи -3. Наприклад, основний VTH – 101-0, а номер кімнати розширення – 101-1, 101-2... ● Якщо функція групового дзвінка не увімкнена, номер кімнати в формат 9901-xx встановити неможливо.
Режим реєстрації	Залишіть їх як значення за промовчанням.
Пароль реєстрації	

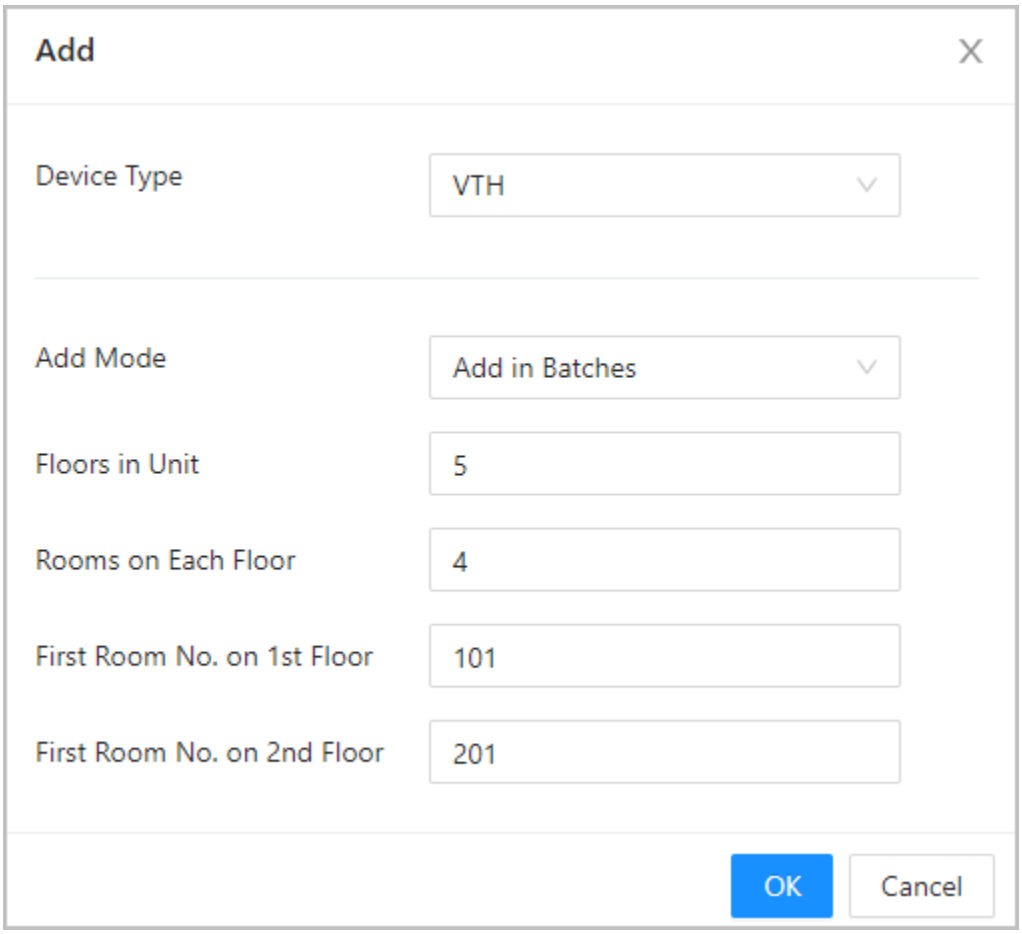
● Додайте порціями.

1. Натисніть**Додати партіями**.

2. Налаштуйте параметри.

3. Натисніть**Додавати**.

Малюнок 3-8 Пакетне додавання



Таблиця 3-6 Додати партіями

Параметр	Опис
Поверхи у блоці	Кількість поверхів будівлі, що варіюється від 1 до 99.
Кімнати на кожному поверсі	Кількість кімнат на кожному поверсі варіюється від 1 до 99.
Номер першої кімнати на 1 поверсі	Перша кімната на першому поверсі.
Номер першої кімнати на 2 поверсі	Номер першої кімнати на 2 поверсі = Перша цифра номера першої кімнати на 1 поверсі плюс 1. Наприклад, якщо номер першої кімнати на першому поверсі — 101, номер першої кімнати на 2 поверсі повинен бути 201.

3.6.1.5 Додавання СУДС

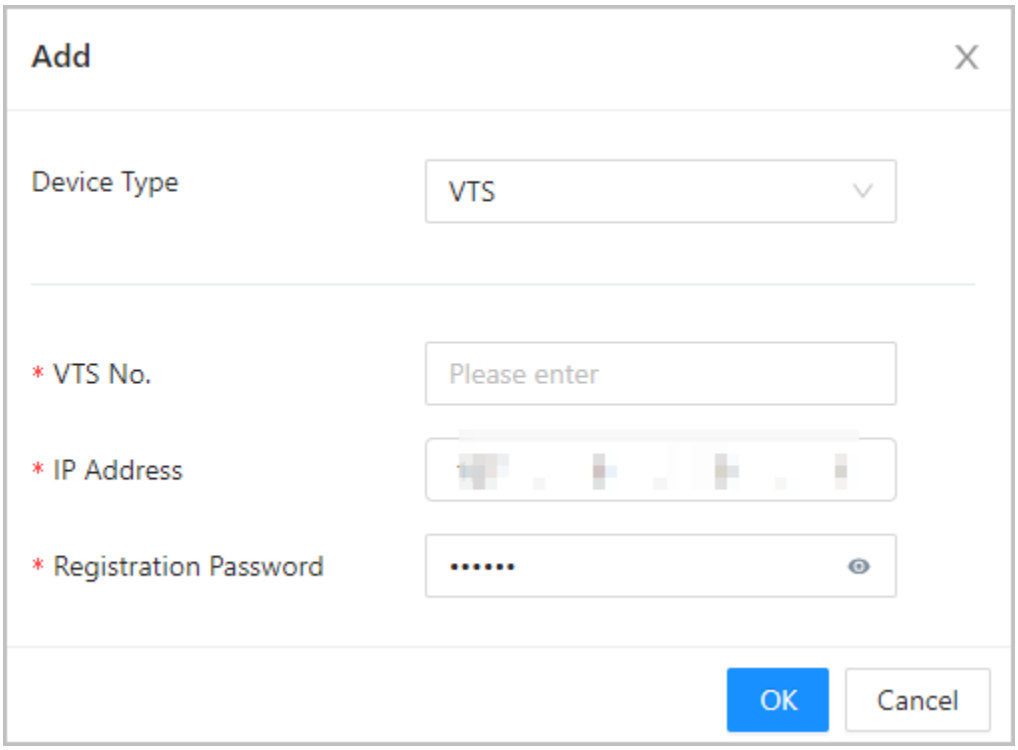
Коли пристрій функціонує як SIP-сервер, ви можете додати VTS до SIP-сервера, щоб переконатися, що вони можуть дзвонити один одному.

Процедура

Крок 1 На головній сторінці виберіть**Налаштування домофону**>**Налаштування пристрою**.

Крок 2 Натисніть**Додавати**, а потім виберіть параметри.

Малюнок 3-9 Управління СУДС



Крок 3 Натиснітьдобре.

3.6.2 Використання VTO як SIP-сервер

3.6.2.1 Налаштування SIP-сервера

Використовуйте інший VTO як SIP-сервер.

Процедура

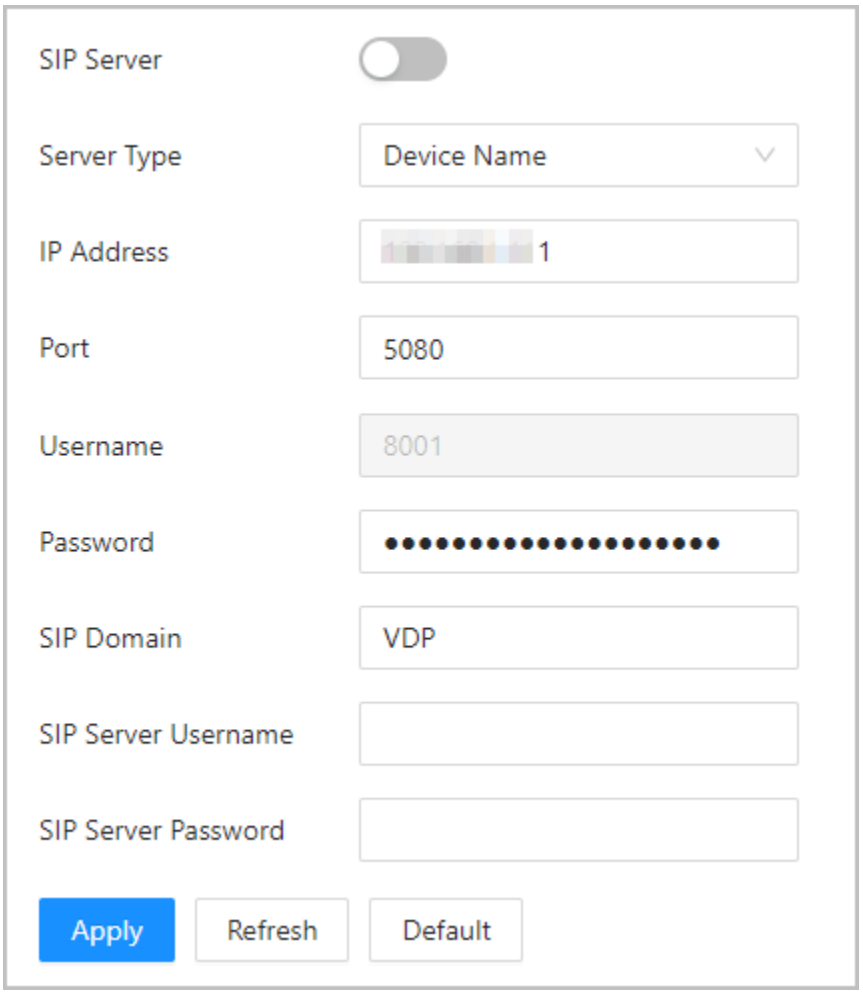
Крок 1 Вибиратиналаштування домофону>sip-сервер.

Крок 2 Вибиратипристрійзтип сервера.

Не вмикатиsip-сервер.

Крок 3 Налаштуйте параметри, а потім натиснітьдобре.

Малюнок 3-10 Використання VTO як SIP-сервер



Таблиця 3-8 Конфігурація SIP-сервера

Параметр	Опис
IP-адреса	IP-адреса СОТ.
Порт	5060 за промовчанням, коли VTO працює як SIP-сервер.
Ім'я користувача	Залишіть їх за промовчанням.
Пароль	
SIP-домен	ВДП.
Ім'я користувача SIP-сервера	Ім'я користувача та пароль для входу на SIP-сервер.
Пароль SIP-сервера	

Крок 4 Натисніть**Застосовувати**.

3.6.2.2 Налаштування локальних параметрів

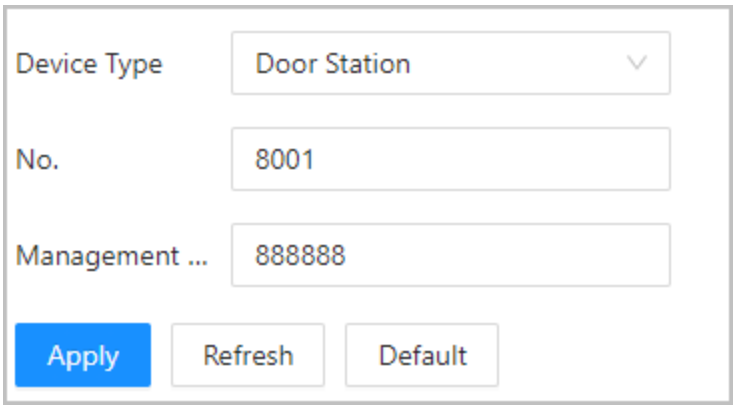
Налаштуйте параметри пристрою під час використання іншого VTO як SIP-сервера.

Процедура

Крок 1 Вибирати**Налаштування домофону**>**Конфігурація локального**

Крок 2 **пристрої**. Налаштуйте параметри.

Малюнок 3-11 Налаштування параметрів



Таблиця 3-9 Опис параметрів

Параметр	Опис
Тип пристрою	Вибрати**Дверна станція**.
Ні.	Номер СОТ. ● Номер повинен складатися з4 цифри. Перші 2 цифри мають бути 80, а останні 2 цифри починаються з 01. Наприклад, 8001. ● Якщо в одному підрозділі є кількаVTO номер VTO не може повторюватися.
Центр управління	Номер дзвінка центру керування — 888888. Залишіть його за промовчанням.

Крок 3 Натисніть**Застосовувати**.

3.6.3 Використання платформи як SIP-сервера

3.6.3.1 Налаштування SIP-сервера

Платформа управління використовується як SIP-сервер.

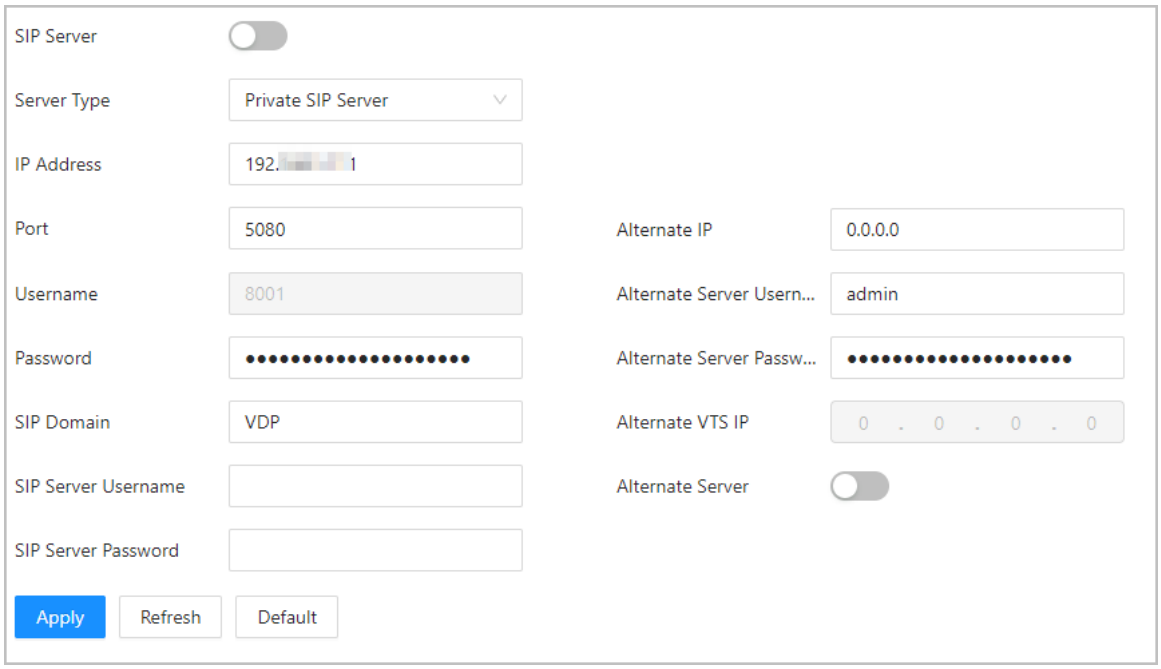
Процедура

Крок 1 Вибирати**Налаштування домофону**>**Приватний SIP-сервер**.

Крок 2 Вибирати**Приватний SIP-сервер**з**Тип сервера**.

Не вмикати**SIP-сервер**.

Малюнок 3-12 Використання платформи управління як SIP-сервер



Таблиця 3-10 Конфігурація SIP-сервера

Параметр	Опис
IP-адреса	IP-адреса платформи.
Порт	5080 за промовчанням, коли платформа працює як SIP-сервер.
Ім'я користувача Пароль	Залишіть їх за промовчанням.
SIP-домен	Залишіть значення за промовчанням.
Ім'я користувача SIP-сервера Пароль SIP-сервера	Ім'я користувача та пароль для входу на платформу.
Альтернативна IP-адреса	Альтернативний сервер буде використовуватися як SIP-сервер, якщо платформа не відповідає. ● Якщо ви увімкнете**Альтернативний сервер**цієї функції ви встановите контролер доступу як альтернативний сервер. ● Якщо ви хочете, щоб іншийVTO функціонував як альтернативний сервер, ви необхідно ввести IP-адресу, ім'я користувача, пароль VTO. Робити не ввімкнути**Альтернативний сервер**у цьому випадку. ● Ми рекомендуємо вам встановити основнийVTO як альтернативний сервер.
Альтернативний сервер Ім'я користувача Альтернативний сервер Пароль	Використовується для входу на альтернативний сервер.

Параметр	Опис
Альтернативна IP-адреса VTS	Введіть IP-адресу альтернативного VTS. Якщо платформа керування не відповідає, буде активовано альтернативний VTS, щоб переконатися, що VTO, VTH та VTS можуть один одного.

Крок 3 Натисніть**Застосовувати**.

3.6.3.2 Налаштування локальних параметрів

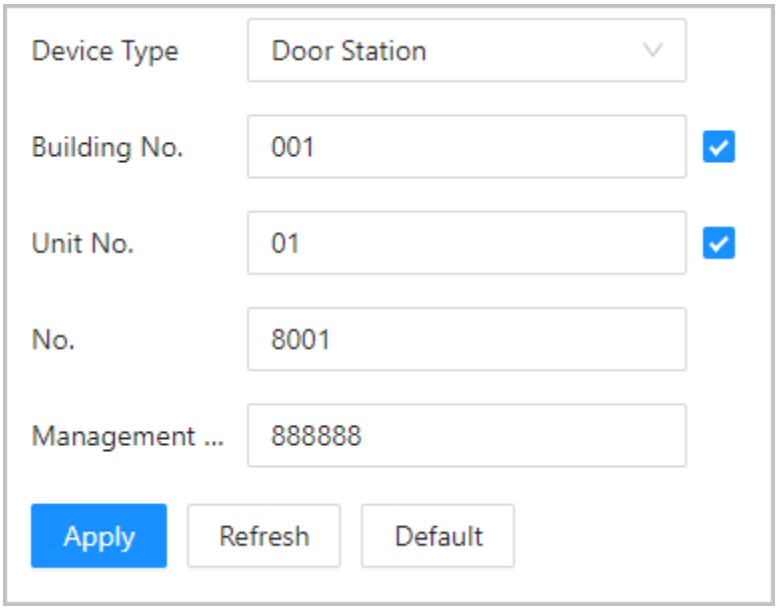
Налаштуйте параметри контролера доступу під час використання платформи як SIP-сервера.

Процедура

Крок 1 Вибрати**Налаштування домофону**>**Конфігурація локального**

Крок 2 **пристрої**. Налаштуйте параметри.

Рисунок 3-13 Основний параметр



Таблиця 3-11 Опис параметрів

Параметр	Опис
Тип пристрою	Виберіть станцію огорожі або дверну станцію залежно від місця встановлення.
Номер будівлі	Встановіть прапорець, а потім введіть номер будівлі, де встановлено панель виклику.
Номер блоку	Встановіть прапорець, а потім введіть номер блоку, в якому встановлена панель виклику.
Ні.	● Номер повинен складатися з4 цифри. Перші 2 цифри мають бути 80, а останні дві цифри повинні починатися з 01. Наприклад, 8001. ● Якщо в одному підрозділі є кількаVTO, номер VTO не може повторюватися.
Центр управління	Номер телефону за замовчуванням – 888888, коли VTO дзвонить до VTS. Залишіть його за промовчанням.

Крок 3 Натисніть**Застосовувати**.

Після налаштувань ім'я користувача в**Інтерком**>**КОВТОК**сторінка автоматично оновлюється. Переконайтеся, що Ім'я користувача збігається з номером дзвінка, коли ви додаєте пристрій до керування

платформи.

3.7 Налаштування контролю доступу

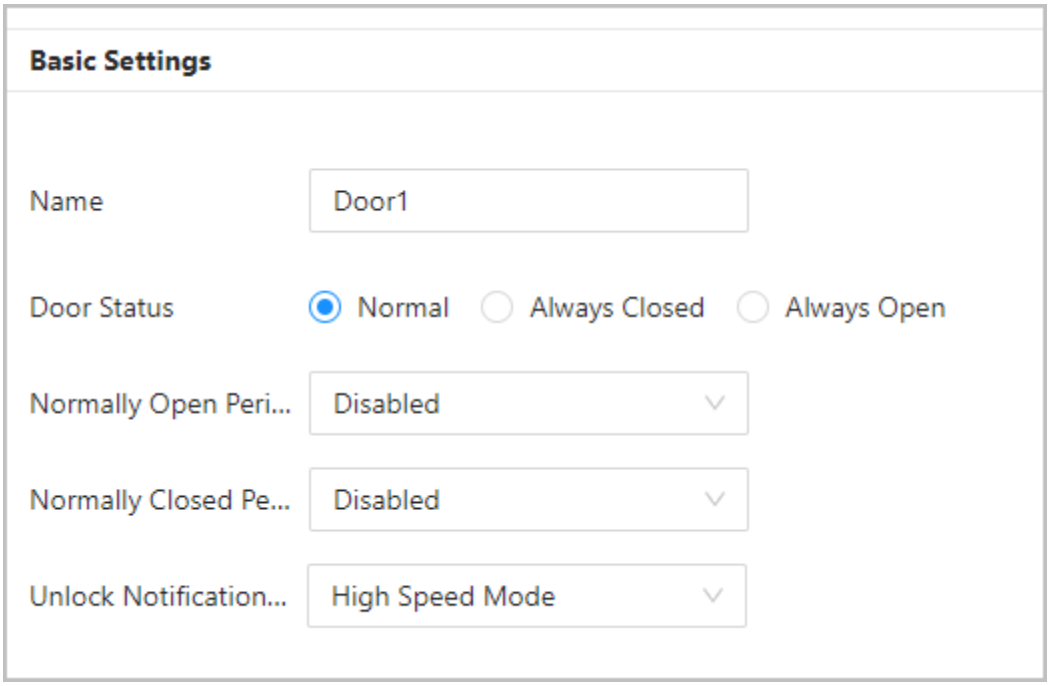
3.7.1 Налаштування основних параметрів

Процедура

Крок 1 Вибирати**Контроль доступу**>**Параметри контролю доступу**.

Крок 2 У**Основні налаштування**налаштувати основні параметри контролю доступу.

Рисунок 3-14 Основні параметри



Таблиця 3-12 Опис основних параметрів

Параметр	Опис
Ім'я	Назва дверей.
Стан дверей	Встановіть статус дверей. ● Нормальний режим: Двері будуть розблоковані та заблоковані відповідно до ваших налаштуваннями. ● Завжди відчинено: двері постійно залишаються відчиненими. ● Завжди закрито: двері весь час залишаються замкненими.
Нормально відкритий період	Коли ви обираєте**Нормальний**, ви можете вибрати шаблон часу з випадаючого список. Двері залишаються відчиненими або закритими протягом певного часу.
Період нормального закриття	

Параметр	Опис
Повідомлення про розблокування	Відображає повідомлення на екрані, коли людина підтверджує особистість на контролері доступу. ● Режим високої швидкості: система пропонує**Успішно перевірено**або **Не авторизовано**на екрані. ● Простий режим: відображає ідентифікатор користувача, ім'я та час перевірки після надання доступу; відображає**Не авторизовано**та час авторизації після відмови у доступі. ● Стандарт: відображає зареєстроване зображення особи користувача, ідентифікатор користувача, ім'я та час перевірки після надання доступу; відображає**Не авторизовано**та час перевірки після відмови у доступі. ● Контрастний режим: відображає захоплене зображення обличчя та зареєстроване зображення особи користувача, ідентифікатор користувача, ім'я та час авторизації після надання доступу; відображає**Не авторизовано**та час авторизації після відмови у доступі.

Крок 3 Натисніть**Застосовувати**.

3.7.2 Налаштування методів розблокування

Ви можете використовувати кілька методів розблокування, щоб розблокувати двері, наприклад, карту Bluetooth, відбиток пальця, карту та пароль. Ви також можете об'єднати їх, щоб створити власний метод розблокування.

Процедура

Крок 1 Вибирати**Контроль доступу**>**Параметри контролю доступу**. У

Крок 2 **Розблокувати налаштування**, виберіть режим розблокування.

- Комбіноване розблокування

  1. Вибрати**Комбінація розблокування**з**Режим розблокування**список.

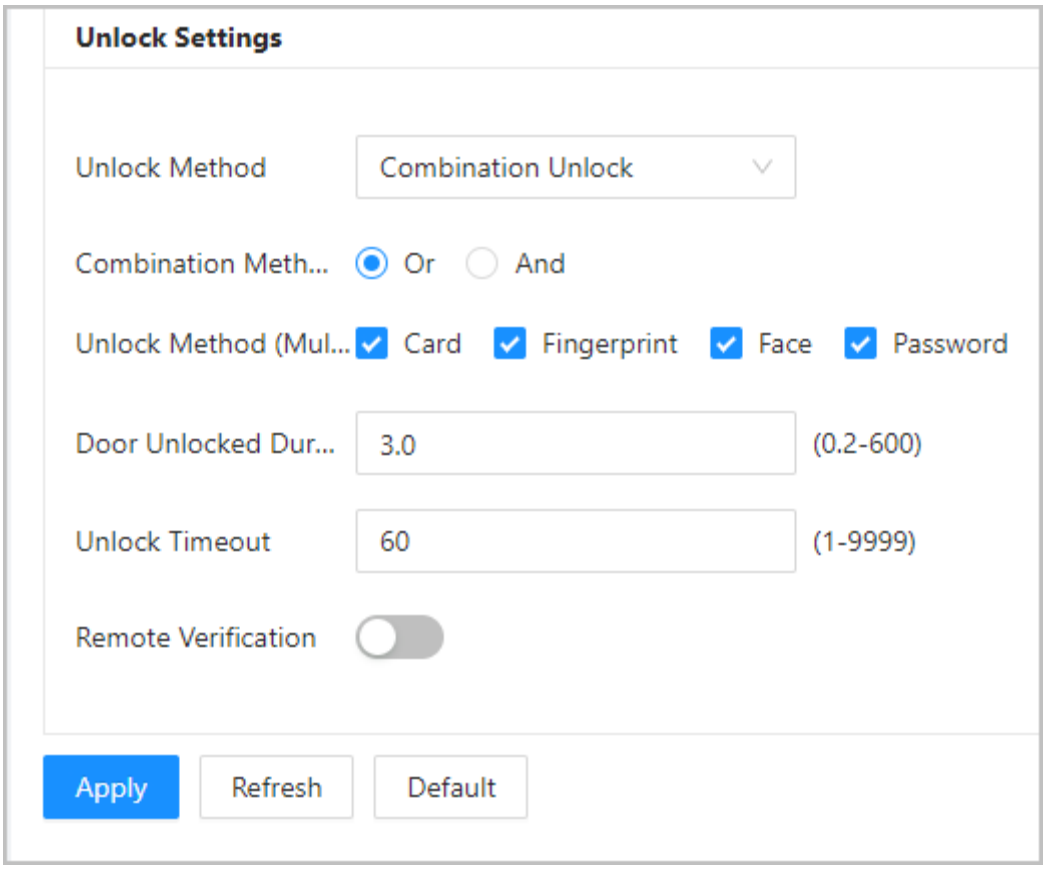
  2. Вибрати**Або**або**І**.

     ◇ Або: використовуйте один із вибраних методів розблокування, щоб відкрити двері.

     ◇ І: Використовуйте всі вибрані методи розблокування, щоб відкрити двері.

  3. Виберіть методи розблокування та налаштуйте інші параметри.

Рисунок 3-15 Налаштування розблокування



Таблиця 3-13 Опис налаштувань розблокування

Параметр	Опис
Метод розблокування (множинний вибір)	Методи розблокування можуть відрізнятися залежно від моделі продукту.
Тривалість розблокування дверей	Після того, як людині надано доступ, двері залишаться відчиненими протягом певного часу, щоб вона могла пройти. Воно варіюється від 0,2 до 600 секунд.
Тайм-аут розблокування	Якщо увімкнено детектор дверей та сигналізацію тайм-ауту розблокування, спрацює сигналізація тайм-ауту, якщо двері залишаться розблокованими довше заданого часу розблокування.
Віддалена перевірка	Відчиніть двері дистанційно.

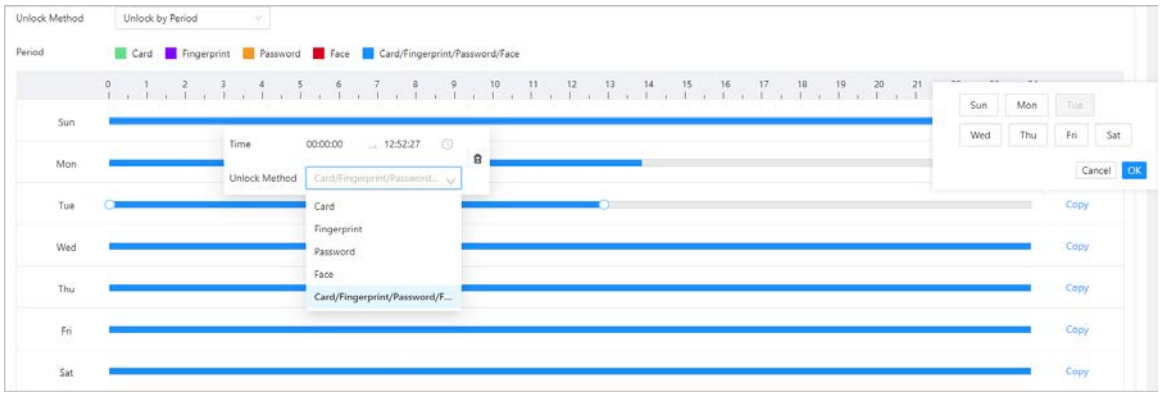
- Розблокувати за періодом

1. У**Режим розблокування**список, вибрати**Розблокувати за періодом**.
2. Перетягніть повзунок, щоб налаштувати час для кожного дня.

Ви також можете натиснути**Копіювати**для застосування налаштованого періоду часу до інших днів.

3. Виберіть метод розблокування для вказаного періоду часу та налаштуйте інші параметри.

Малюнок 3-16 Розблокування за періодом



- Розблокування кількома користувачами.

  1. У**Режим розблокування**список, вибрати**Розблокування кількома користувачами**.

  2. Натисніть**Додавати**додавання груп.

  3. Виберіть спосіб розблокування, дійсний номер та список користувачів.

     ◇ Якщо додано лише одну групу, двері розблокуються лише після того, як кількість людей у групі, які надають доступ, зрівняється із зазначеним допустимим числом.

     ◇ Якщо додано більше однієї групи, двері розблокуються тільки після того, як кількість людей в кожній групі, що надали доступ, зрівняється із зазначеним допустимим числом.

     ◇ Можна додати до 4 груп.

     ◇ Дійсний номер вказує кількість людей у кожній групі, яким необхідно підтвердити свої дані. ідентифікатори на контролері доступу до того, як двері відчиняться. Наприклад, якщо дійсний Кількість встановлена на 3 для групи, будь-які 3 особи в групі повинні підтвердити свою особу, щоб відчиніть двері.

Крок 3 Натисніть**Застосовувати**.

3.7.3 Налаштування будильників

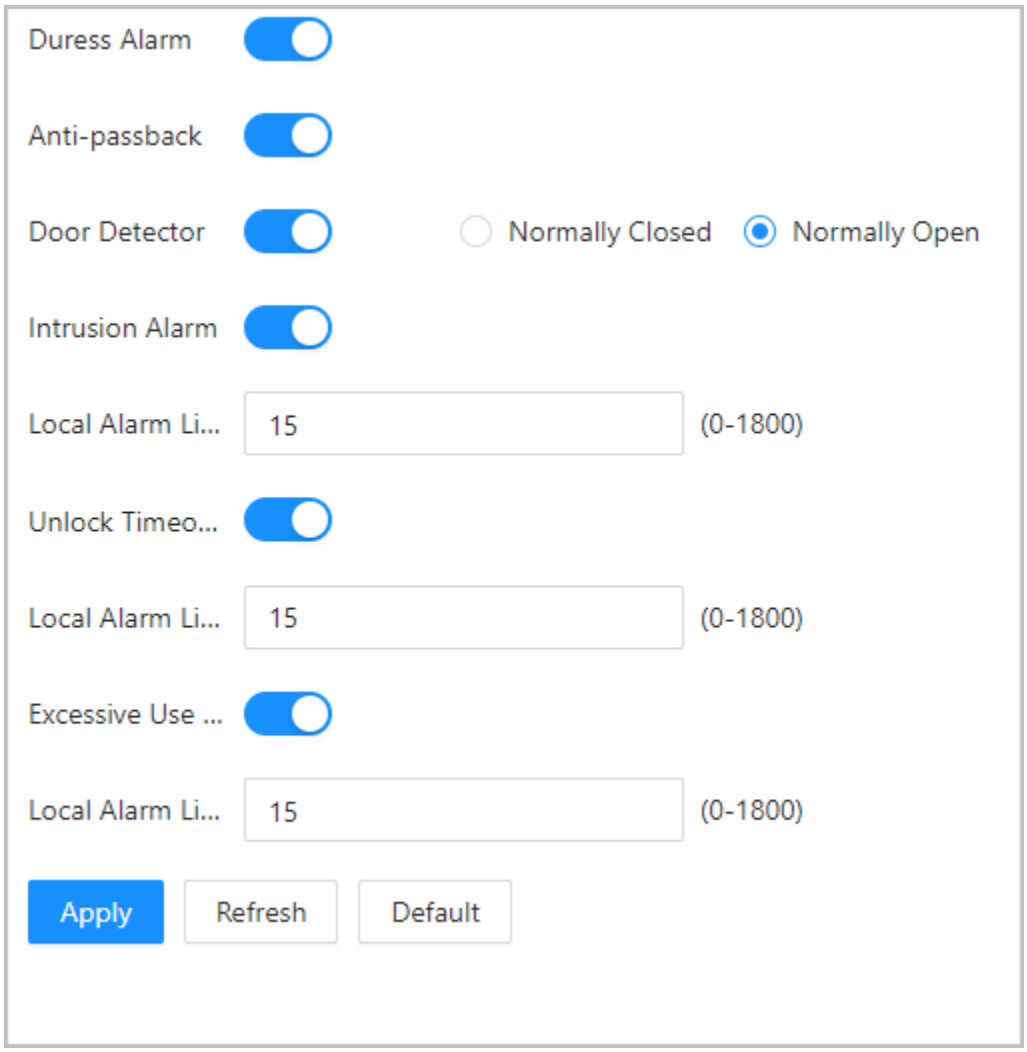
У разі виникнення позаштатної події доступу спрацьовує сигналізація.

Процедура

Крок 1 Вибирати**Контроль доступу**>**Тривога**>**Тривога**.

Крок 2 Налаштуйте параметри сигналізації.

Малюнок 3-17 Сигналізація



Таблиця 3-14 Опис параметрів сигналізації

Параметр	Опис
Сигналізація примусу	Сигналізація спрацює, якщо для розблокування дверей буде використано карту примус, пароль примус або відбиток пальця примусу.

Параметр	Опис
Антипасбек	Користувачі повинні підтвердити свою особистість як для входу, так і виходу; інакше спрацює сигналізація. Це допомагає запобігти передачі картки доступу власником картки іншій людині для входу. Коли увімкнено захист від повторного проходу, утримувач картки повинен залишити захищену зону через зчитувач на виході, перш ніж ніж система надасть інший вхід. ● Якщо людина увійде після авторизації та вийде без авторизації, при повторній спробі входу спрацює сигналізація, і доступ буде заборонено. ● Якщо людина увійде без дозволу і вийде після отримання дозволу, при повторній спробі входу спрацює сигналізація, і доступ буде заборонено. Якщо контролер доступу може підключити лише один замок, перевірка на контролері доступу означає напрямок входу, та перевірка на зовнішньому зчитувачі карток означає напрям виходу за замовчуванням. Ви можете змінити налаштування на платформі управління.
Детектор дверей	З дверним детектором, підключеним до пристрою, сигналізація може спрацьовувати при ненормальному відкриванні або зачиненні дверей. Дверний детектор включає 2 типи, включаючи NC-детектор та NO-детектор. ● Нормально замкнутий: датчик знаходиться у замкнутому положенні, коли двері або вікно зачинені. ● Нормально відкритий: Розімкнутий ланцюг створюється, коли вікно чи двері фактично закриті.
Сигналізація вторгнення	Якщо увімкнено детектор дверей та сигналізацію вторгнення, при ненормальному відкриванні дверей спрацює сигналізація вторгнення.
Розблокувати сигналізацію тайм-ауту	Якщо увімкнено детектор дверей та сигналізацію тайм-ауту розблокування, спрацює сигналізація тайм-ауту, якщо двері залишаться розблокованими довше заданого часу розблокування.
Сигналізація надмірного використання	Якщо неправильний пароль або картка буде використано 5 разів поспіль протягом 60 секунд, спрацює сигналізація про надмірне використання нелегальної карти, яка за промовчанням триває 15 секунд.
Локальний зв'язок із сигналізацією	Тривалість будильника. За замовчуванням 15 с.

Крок 3 Натисніть**Застосовувати**.

3.7.4 Налаштування глобальних зв'язків тривог (необов'язково)

Ви можете налаштувати глобальні тривоги зв'язку.

Процедура

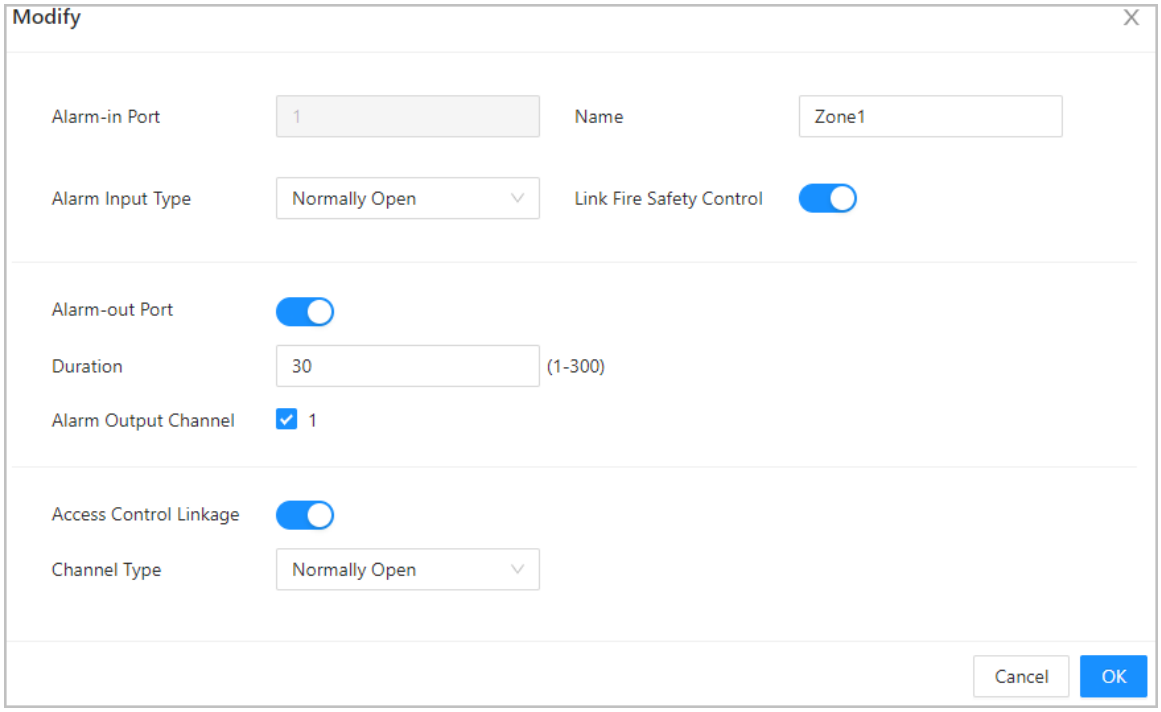
Крок 1 Вибирати**Контроль доступу**>**Тривога**>**Налаштування зв'язку із сигналом тривоги**.

- Якщо контролер доступу додано як платформу керування, налаштування сигналізації будуть синхронізовано із платформою.
- Ця функція доступна лише для моделей, що мають порти входу та виходу тривоги.
- Кількість вхідних та вихідних портів сигналізації різниться залежно від моделі продукт.

Крок 2 Налаштуйте вхід тривоги. 1.

Натисніть .

Малюнок 3-18 Глобальний зв'язок тривог



2. Налаштуйте назву будильника.

3. Виберіть тип пристрою тривоги.

- Нормально замкнутий: Вхід сигналізації знаходиться в стані нормально замкнутого ланцюга (NC), коли сигналізація не спрацювала. Розмикання нормально замкненого ланцюга активує сигналізацію.
- Нормально розімкнений: Пристрій входу сигналізації знаходиться в стані нормально розімкнутого ланцюга (АЛЕ), коли сигналізація не спрацювала. Замикання ланцюга включає сигналізацію.

4. Натисніть**Давати можливість**для увімкнення функції приєднання дверей.

Якщо ви увімкнете керування пожежною безпекою, вихід сигналізації та всі дверні з'єднання будуть вимкнені.

автоматично увімкнено зміну на**Завжди відкрито**статус, і всі двері відчиняться, коли спрацьовує пожежна сигналізація.

1. Виберіть вхід сигналу тривоги зі списку каналів входу сигналу тривоги, а потім натисніть**Вихід сигналу тривоги**.

2. Натисніть**Додавати**, виберіть канал тривоги, а потім натисніть**ДОБРЕ**.

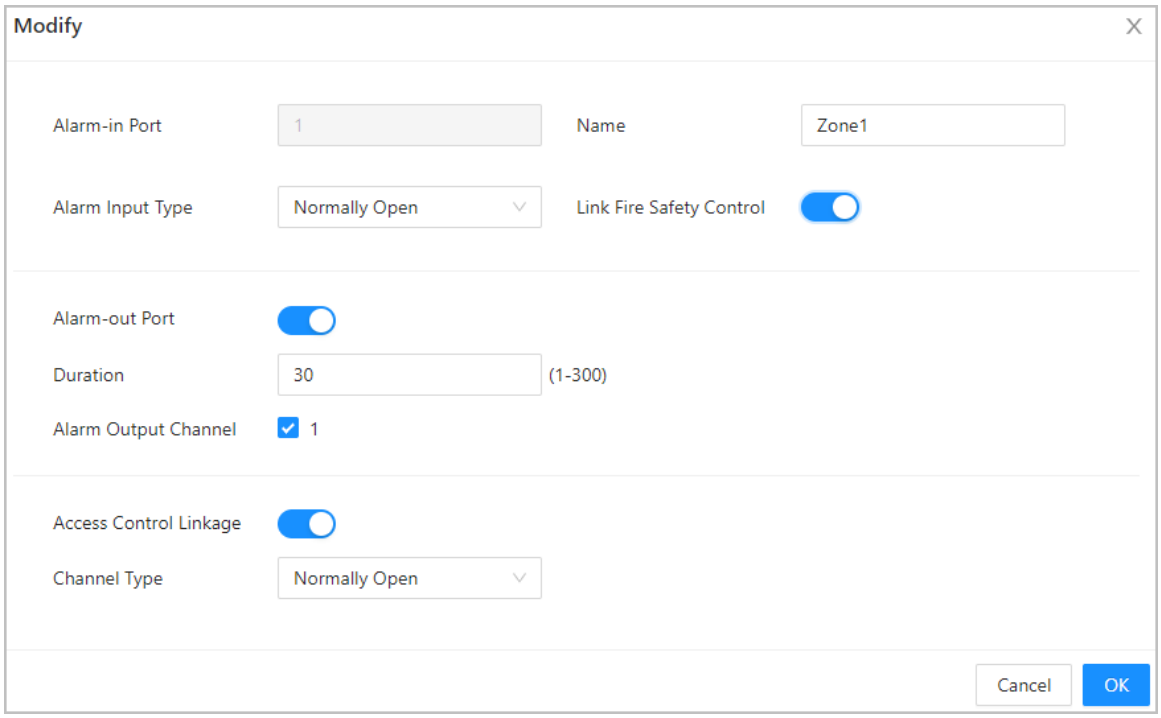
3. Натисніть**Застосовувати**.

Крок 3 Увімкніть функцію виходу тривоги, а потім введіть тривалість сигналу тривоги.

Крок 4 Увімкніть зв'язок електронного керування доступом, а потім виберіть статус дверей.

- Нормально закритий: двері автоматично зачиняються під час спрацювання сигналізації.
- Нормально відчинений: двері автоматично розблоковуються під час спрацювання сигналізації.

Рисунок 3-19 Вихід сигналу тривоги



3.7.5 Налаштування розпізнавання облич

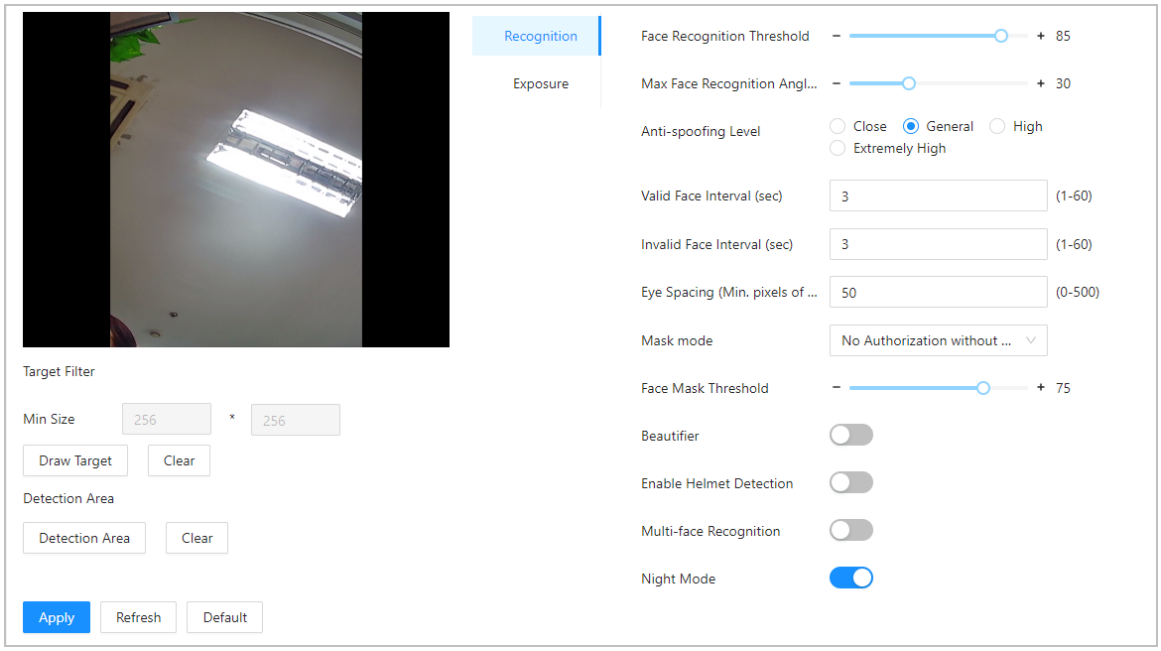
Налаштуйте параметри виявлення обличчя.

Процедура

Крок 1 Увійдіть на веб-сторінку.

Крок 2 Вибирати**Контроль доступу**>**Розпізнавання осіб**.

Рисунок 3-20 Параметри виявлення обличчя



Крок 3 Налаштуйте параметри.

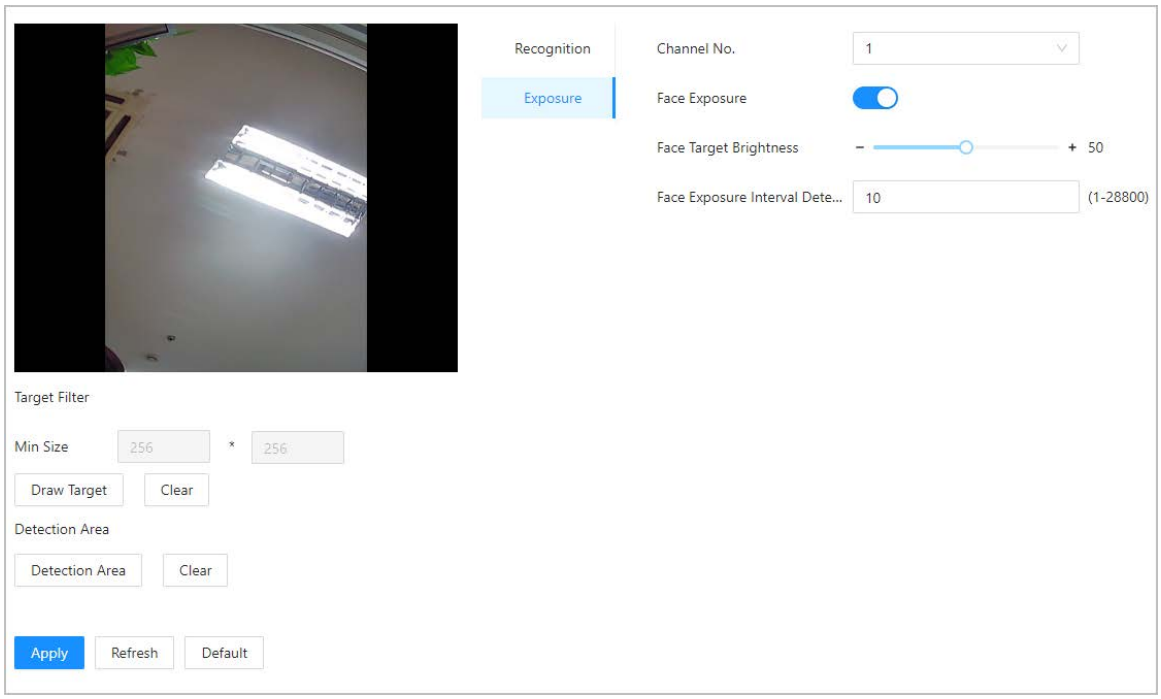
Таблиця 3-15 Опис параметрів обличчя

Ім'я	Опис
Поріг розпізнавання обличчя	Налаштуйте рівень точності розпізнавання облич. Вищий поріг означає більш високу точність та менший рівень хибного розпізнавання.
Максимальне відхилення кута розпізнавання обличчя	Встановіть найбільший кут, під яким особа може бути розташована виявлення обличчя. Чим більше значення, тим більше діапазон для кута обличчя. Якщо кут, під яким розташована особа, не входить у заданий діапазон, воно може бути виявлено неправильно.
Рівень захисту від підробки	Це не дозволяє людям використовувати фотографії, відео, маски та інші замінники для отримання несанкціонованого доступу.
Справжній інтервал осіб (сек)	Якщо людина успішно верифікована занадто багато разів, контролер доступу видає запит про успішну верифікацію протягом певного інтервалу часу.
Невірний інтервал осіб (сек)	Якщо людині не вдається пройти верифікацію обличчя надто багато разів, контролер доступу видає повідомлення про невдалу верифікацію протягом певного проміжок часу.
Відстань між очима (хв. пікселі відстані між очима)	Для успішного розпізнавання потрібна певна кількість пікселів між очима, зване зіничною відстанню. Значення за замовчуванням - 45 пікселів. Це число змінюється в залежності від розміру обличчя та відстані між обличчям та лінзою. Якщо доросла людина знаходиться на відстані 1,5 метра від лінзи, зінова відстань зазвичай становить 50-70 пікселів.
Режим маски	● Режим маски: ◇ **Не виявляти**: Маска не виявляється при розпізнаванні обличчя ◇ **Нагадування про маску**: Маска виявлена під час розпізнавання обличчя Якщо людина не носить маску, система нагадає їй про необхідність надіти маску, але доступ їй все одно буде дозволено. ◇ **Без маски вхід не дозволено**: Маска виявлена під час розпізнавання обличчя Якщо людина не носить маску, система нагадає їй про необхідність надіти маску, і доступ буде заборонено. ● Поріг розпізнавання маски: чим вищий поріг, тим точніше буде розпізнавання обличчя людини в масці і тим нижче буде хибне розпізнавання.
Прикрасник	Прикрасьте зроблені знімки облич.
Увімкнути виявлення шолома	Виявляє захисні каски. Двері не відчиняться, якщо людина не носить каску.

Ім'я	Опис
Розпізнавання кількох осіб	Розпізнає від 4 до 6 зображень облич одночасно. Комбінована розблокування не може бути використане з цим, і двері будуть розблоковані, коли один із людей успішно пройде перевірку. Кількість підтримуваних зображень осіб може різнитися залежно від моделі товару.
Нічний режим	У темних умовах на екрані в режимі очікування відображається білий фон. зображення для підвищення яскравості під час розпізнавання обличчя або QR-коду.
Режим освітлювача	● Авто: Підсвічування вмикається в умовах низького освітлення. ● Вимкнути: освітлювач постійно вимкнений. Ця функція доступна лише в деяких моделях.

Крок 4 Налаштуйте параметри експозиції.

Рисунок 3-21 Параметри експозиції



Таблиця 3-16 Опис параметрів впливу

Параметр	Опис
Номер каналу	● Канал1 – режим білого світла. ● Канал2 - режим інфрачервоного світла.
Обличчя експонування	Після включення функції експозиції обличчя обличчя буде експонуватися із заданою яскравістю для чіткого виявлення зображення обличчя.
Визначення інтервалу експозиції особи	Особа оголюватиметься лише один раз у певний проміжок часу.

Крок 5 Намалюйте область виявлення обличчя. 1)

Натисніть**Визначити регіон**.

2) Клацніть правою кнопкою миші, щоб намалювати область виявлення, а потім відпустіть ліву кнопку миші

повний малюнок.

Особа у вказаній області буде виявлена.

Крок 6 Намалюйте цільовий розмір.

1) Клацніть**Намалюйте ціль**

2) Намалюйте рамку розпізнавання облич, щоб визначити мінімальний розмір виявленої особи.

Контролер доступу може виявити особу лише в тому випадку, якщо її розмір перевищує заданий розмір.

Крок 7 Намалюйте зону виявлення. Натисніть

Крок 8 **ДОБРЕ**.

3.7.6 Налаштування параметрів картки

Довідкова інформація

Ця функція доступна лише в деяких моделях.

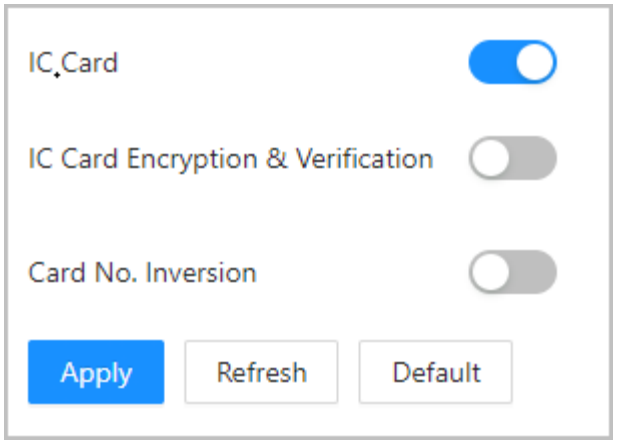
Процедура

Крок 1 Увійдіть на веб-сторінку.

Крок 2 Вибирати**Контроль доступу**>**Налаштування**

Крок 3 **карти**. Налаштуйте параметри картки.

Малюнок 3-22 Параметри картки



Таблиця 3-17 Опис параметрів картки

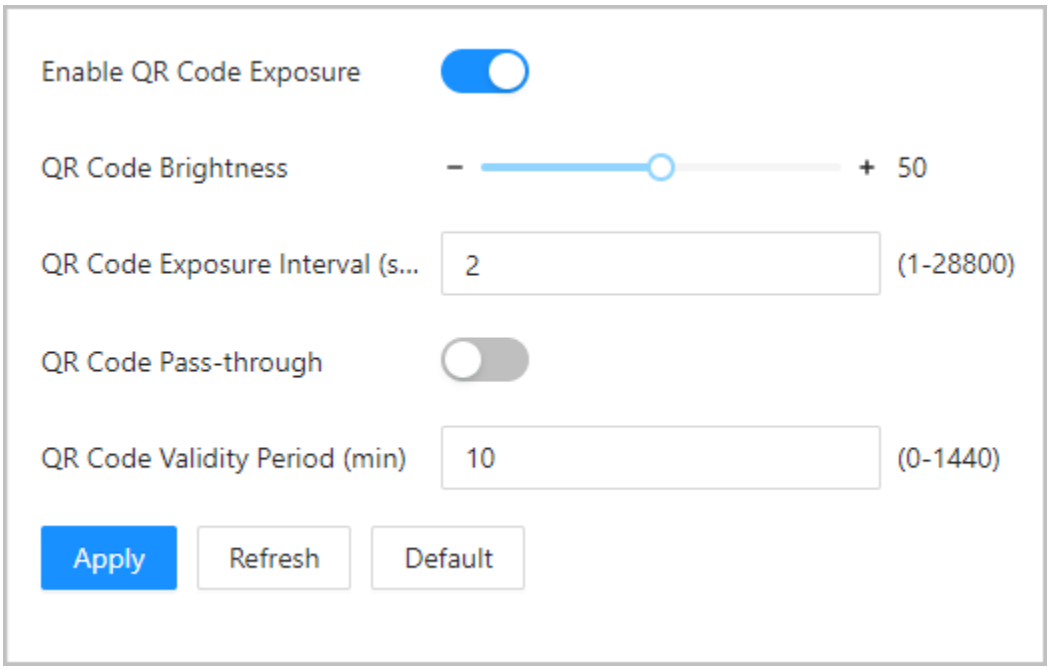
Параметр	Опис
IC-карта	При включенні цієї функції можна рахувати карту IC. Ця функція доступна лише в деяких моделях.
Шифрування та перевірка IC-карт	Зашифровану картку можна вважати, якщо цю функцію увімкнено.
Номер картки. Інверсія	Коли контролер доступу під'єднується до стороннього пристрою через вхід Wiegand, а номер картки, що зчитується контролером доступу, знаходиться у зворотному порядку від фактичного номера картки. У цьому випадку ви можете увімкнути цю функцію.

3.7.7 Налаштування QR-коду

Процедура

Крок 1 На веб-сторінці виберіть**Контроль доступу**>**Налаштування картки**.

Малюнок 3-23 QR-код



Таблиця 3-18 Параметри QRR-коду

Параметри	Опис
Увімкнути відображення QR-коду	QR-код буде експонуватися із заданою яскравістю, і його можна буде чітко виявити та прочитати.
Яскравість QR-коду	
Інтервал експозиції QR-коду (сек)	QR-код буде показаний лише один раз протягом певного інтервалу часу.
Прохід QR-коду	QR-код, рахований сторонньою платформою.
Термін дії QR-коду (хв)	Після того, як QR-код буде згенеровано, термін дії ваших QR-кодів буде тривати протягом певного часу, перш ніж закінчиться.

3.7.8 Налаштування розкладів

Налаштуйте часові інтервали та плани на святкові дні, а потім визначте, коли користувач має право відчиняти двері.

3.7.8.1 Налаштування періодів часу

Ви можете налаштувати до 128 груп (від 0 до 127) тимчасових періодів. У кожному періоді вам потрібно налаштувати розклад доступу до дверей на цілий тиждень. Люди можуть відчиняти двері тільки протягом запланованого часу.

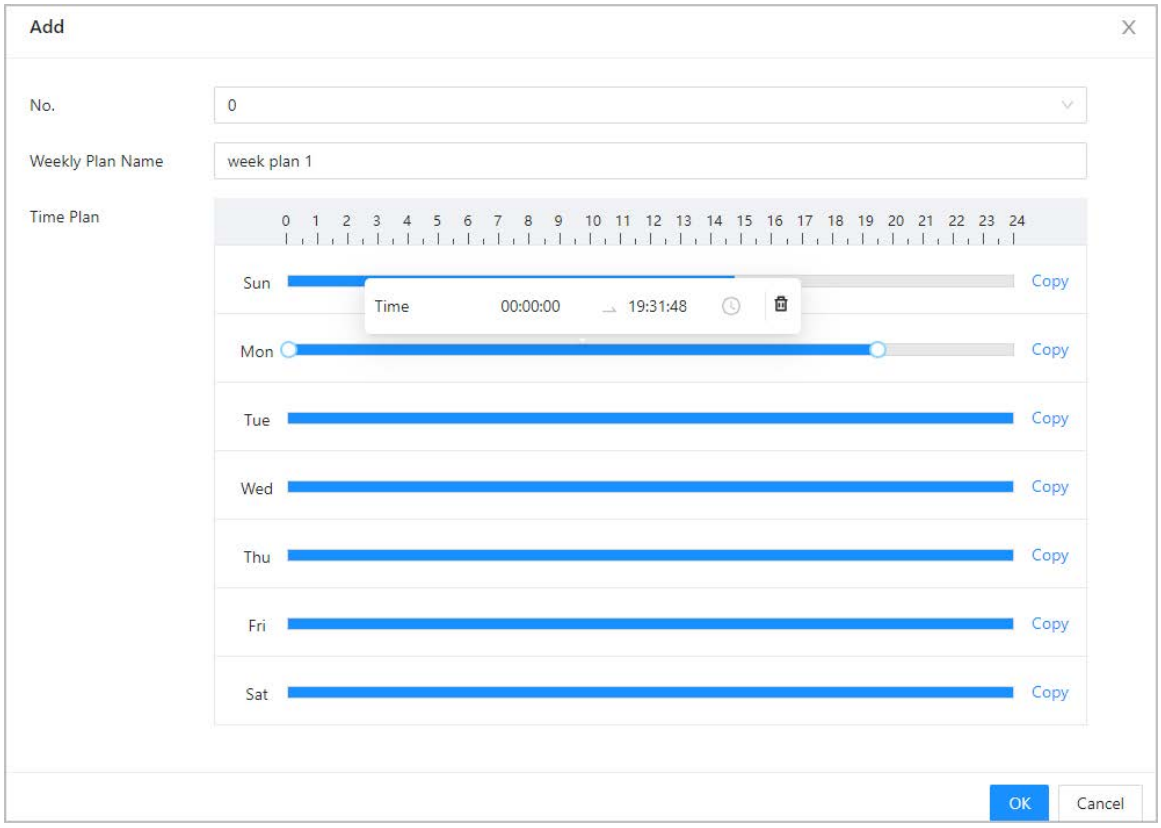
Процедура

Крок 1 Увійдіть на веб-сторінку.

Крок 2 Вибирати**Контроль доступу**>**Конфігурація періоду**>**Щотижневий план**. Натисніть

Крок 3 **Додавати**.

Малюнок 3-24 Налаштування періодів часу



Крок 4 Перетягніть повзунок часу, щоб налаштувати час для кожного дня.

Крок 5 (Необов'язково) Натисніть**Копіювати**щоб скопіювати конфігурацію на інші дні. Натисніть

Крок 6 **ДОБРЕ**.

3.7.8.2 Налаштування планів на свята

Ви можете налаштувати до 128 груп свят (від № 0 до № 127), і для кожної групи свят ви можете додати до 16 свят. Після цього ви можете призначити налаштовані групи свят плану свят. Користувачі можуть відчиняти двері лише у певний час у плані свят.

Процедура

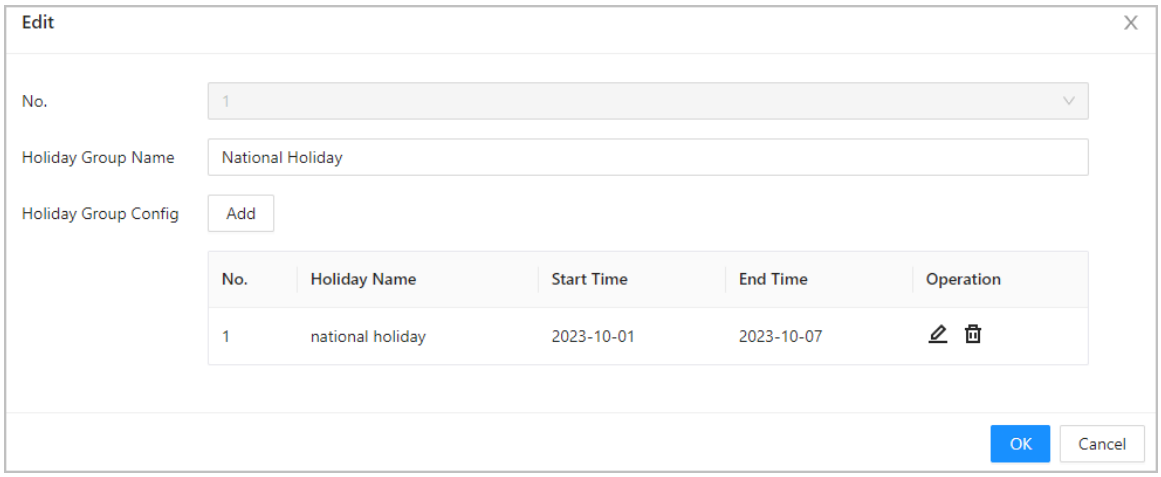
Крок 1 Увійдіть на веб-сторінку.

Крок 2 Вибирати**Контроль доступу**>**Конфігурація періоду**>**План відпустки**.

Крок 3 Натисніть**Управління святами**, а потім натисніть**Додавати**.

Крок 4 Виберіть номер для групи свят, а потім введіть назву групи.

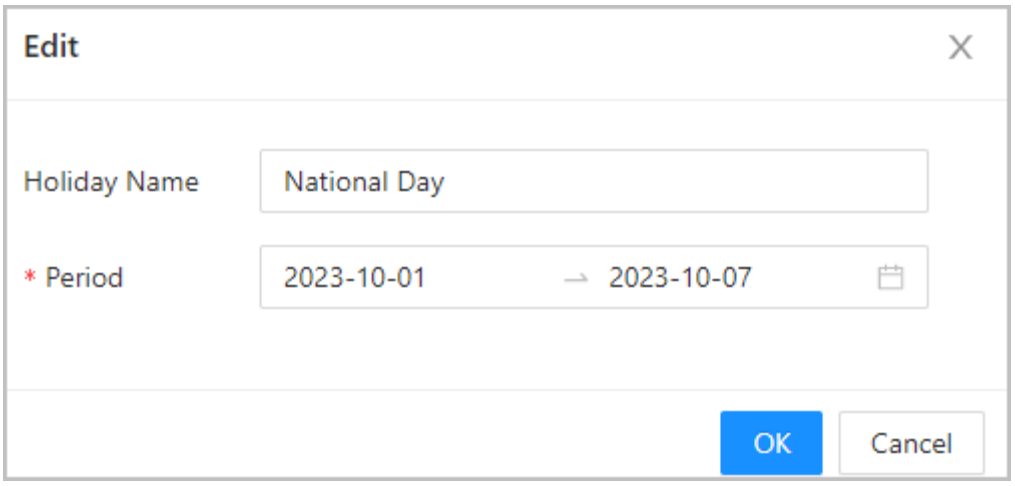
Малюнок 3-25 Додати групу свят



Крок 5 Натисніть**Додавати**, а потім додайте свято до групи свят.

Крок 6 Натисніть**ДОБРЕ**.

Малюнок 3-26 Додати свято до групи свят



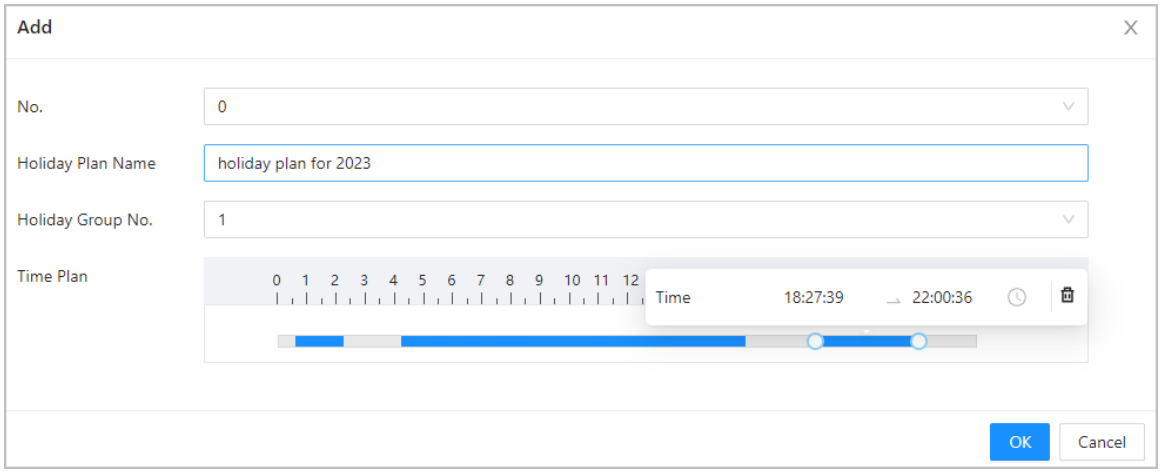
Крок 7 Натисніть**План управління**, а потім натисніть**Додавати**.

Крок 8 Виберіть номер плану відпустки, а потім введіть назву.

Крок 9 Виберіть групу свят, а потім перетягніть повзунок, щоб налаштувати час для кожного дня.

Підтримує додавання до 4 часових розділів на день.

Малюнок 3-27 Додати план відпустки



Крок 10 Натисніть**ДОБРЕ**.

3.7.9 Налаштування модулів розширення

Для контролера доступу, який підтримує підключення модулів розширення, налаштуйте тип модуля, що підтримується контролером доступу.

Довідкова інформація

- Тип розширення може відрізнятися залежно від моделі контролера доступу.
- Параметри модуля розширення зберігаються після відновлення заводських налаштувань контролера доступу.

Процедура

Крок 1 На веб-сторінці виберіть**Контроль доступу**>**Модуль розширення**.

Крок 2 Виберіть тип модуля, який підтримує Access Controller. Натисніть

Крок 3 **Застосовувати**.

Конфігурації набирають чинності після перезапуску контролера доступу.

- відображається в правому куті контролера доступу, якщо налаштування набуло чинності.
- відображається у правому куті контролера доступу, що означає, що тип налаштованого вами модуля розширення не відповідає фактичному модулю розширення, підключеного до контролера доступу.
- Якщо**Ніхто**вибрано і до контролера доступу не підключено модуль розширення, значок модуля розширення не відображатиметься.

3.7.10 Налаштування функцій порту

Деякі порти можуть функціонувати як різні порти, ви можете налаштувати їх на різні порти залежно від фактичних потреб.

Довідкова інформація

- Ця функція доступна лише в деяких моделях.
- Порти можуть відрізнятися залежно від моделі виробу.

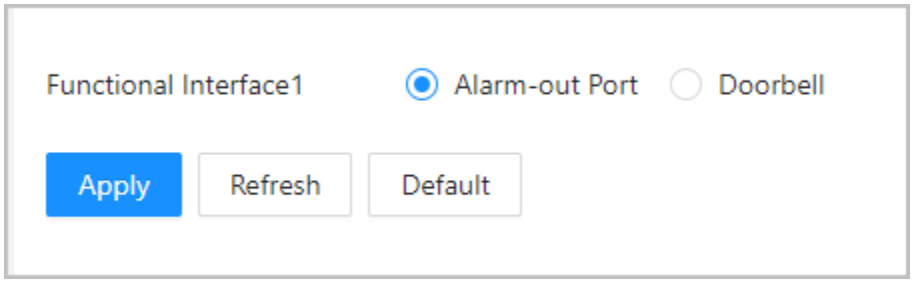
Процедура

Крок 1 На веб-сторінці виберіть**Контроль доступу**>**Конфігурація**

Крок 2 **порту**. Виберіть тип порту.

Крок 3 Натисніть**Застосовувати**.

Малюнок 3-28 Налаштування портів



3.8 Налаштування аудіо та відео

3.8.1 Налаштування відео

На головній сторінці виберіть**Відео Налаштування**, а потім настройте відеопотік, статус, зображення та експозицію.

Довідкова інформація

- Стандарт відео: Вибрати**НТСК**.
- Ідентифікатор каналу: Канал1 призначений для конфігурацій зображення у видимому світлі. Канал 2 призначений для конфігурацій зображення в інфрачервоному світлі.
- За промовчанням: відновити налаштування за промовчанням.
- Захоплення: зробити знімок поточного зображення.

Стандарт відео PAL – 25 кадрів за секунду, а стандарт відео NTSC – 30 кадрів за секунду.

3.8.1.1 Налаштування каналу 1

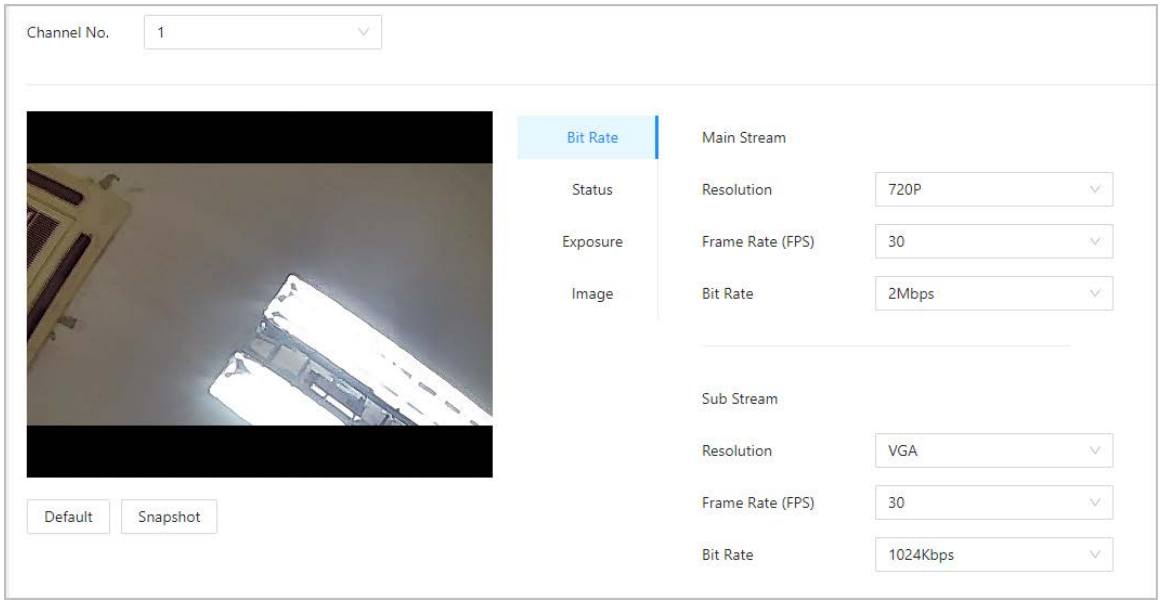
Процедура

Крок 1 Вибирати**Конфігурація аудіо та відео**>**Відео**.

Крок 2 Вибирати**1**з**Номер каналу**список. Налаштуйте швидкість

Крок 3 передачі даних.

Малюнок 3-29 Швидкість передачі

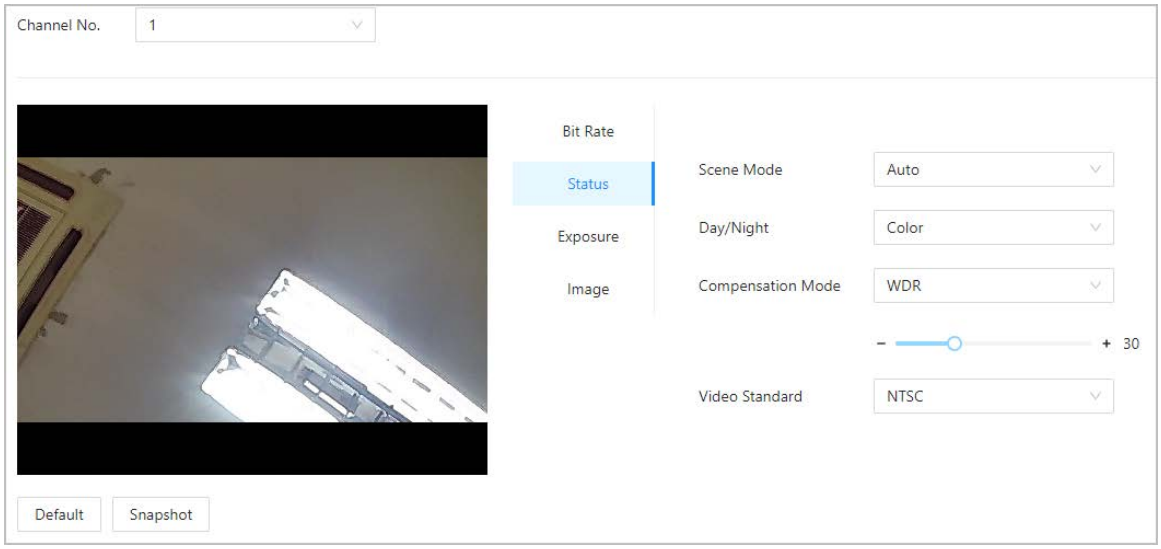


Таблиця 3-19 Опис швидкості передачі

Параметр		Опис
Основний формат	Дозвіл	Коли контролер доступу функціонує як VTO і підключається до VTH, Отримана межа потоку VTH становить 720p. При зміни дозволу на 1080p виклик та функціонування монітора може бути порушено.
	Частота кадрів (кадрів на секунду)	Кількість кадрів (або зображень) за секунду.
	Швидкість передачі	Обсяг даних, переданих через Інтернет-з'єднання за певний час. Виберіть відповідну пропускну здатність залежно від швидкості вашої мережі.
Додатковий потік	Дозвіл	Додатковий потік підтримує D1, VGA та QVGA.
	Частота кадрів (кадрів на секунду)	Кількість кадрів (або зображень) за секунду.
	Швидкість передачі	Він показує обсяг даних, переданих через інтернет з'єднання за певний проміжок часу.

Крок 4 Налаштуйте статус.

Малюнок 3-30



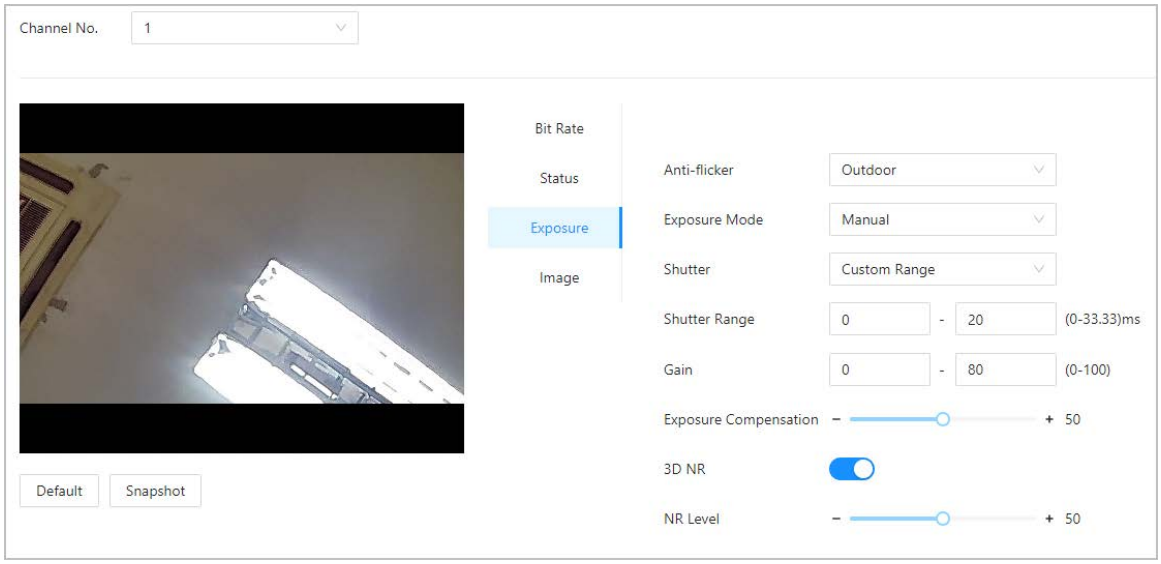
Таблиця 3-20 Опис зображення

Параметр	Опис
Режим сцени	Відтінок зображення відрізняється у різних режимах сцени. ● **Закривати**: Функцію режиму сцени вимкнено. ● **Авто**: Система автоматично налаштовує режим сцени на основі фотографічної чутливості. ● **Сонячно**: У цьому режимі відтінок зображення буде зменшено. ● **Ніч**: У цьому режимі буде збільшено відтінок зображення.

Параметр	Опис
День/Ніч	Режим «День/Ніч» впливає на компенсацію освітленості у різних ситуаціях. ● **Авто**: Система автоматично налаштовує режим «день/ніч» на основу фотографічної чутливості. ● **Барвистий**: У цьому режимі зображення кольорові. ● **Чорно-білий**: У цьому режимі зображення чорно-білі.
Режим компенсації	● **Забороняти**: Компенсацію вимкнено. ● **БЛК**: Компенсація контрового світла автоматично додає більше світла у темні області зображення, коли яскраве світло позаду затьмарює їх. ● **ВДР**: Система затемняє яскраві області та компенсує темні області, створюючи баланс для покращення загальної якості зображення. ● **КЛК**: Компенсація засвічення (HLC) - це технологія, що використовується в камерах відеоспостереження/IP-камери безпеки для обробки зображень, які піддаються впливу світла, наприклад фар або прожекторів. Датчик зображення камери виявляє сильні світлові плями на відео та зменшує експозицію у цих точках, щоб покращити загальну якість зображення.

Крок 5 Налаштуйте параметри експозиції.

Малюнок 3-31 Експозиція



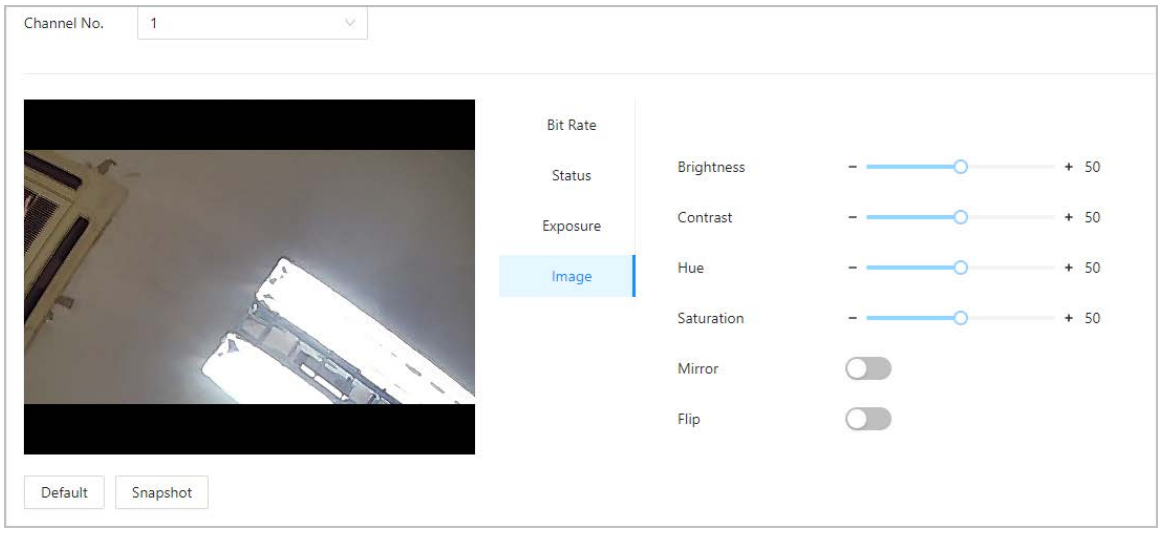
Таблиця 3-21 Опис параметрів експозиції

Параметр	Опис
Антиміготіння	Встановіть функцію «Антимігання», щоб зменшити мерехтіння та зменшити нерівномірність кольорів або експозиції. ● **50 Гц**: Якщо частота електромережі становить 50 Гц, експозиція автоматично регулюється залежно від яскравості навколишнього середовища, щоб запобігти поява горизонтальних ліній. ● **60 Гц**: Якщо частота електромережі становить 60 Гц, експозиція автоматично регулюється в залежності від яскравості навколишнього середовища, щоб зменшити поява горизонтальних ліній. ● **На відкритому повітрі**: Коли**На відкритому повітрі**вибраний, можна переключити режим експозиції.

Параметр	Опис
Режим експозиції	Ви можете налаштувати експозицію, щоб налаштувати яскравість зображення. ● **Авто**: Контролер доступу автоматично регулює яскравість зображень у залежність від навколишнього оточення. ● **Пріоритет витримки**: Контролер доступу регулює яскравість зображення в відповідно до встановленого діапазону затвора. Якщо зображення недостатньо яскраве, але значення затвора досягло свого верхнього чи нижнього межі, контролер доступу автоматично відрегулює значення посилення для ідеальний рівень яскравості. ● **Керівництво**: Ви можете вручну відрегулювати посилення та значення затвора, щоб налаштувати яскравість зображення. ◇ Коли ви обираєте**На відкритому повітрі**з**Антиміготіння**список, ви можете вибрати**Пріоритет витримки**як режим експозиції. ◇ Режим експозиції може відрізнятися залежно від моделі контролера доступу.
Затвор	Затвор - це компонент, який дозволяє світлу проходити протягом певного періоду. Чим вища швидкість затвора, тим коротший час експозиції і тим темніший зображення.
Приріст	Під час встановлення діапазону значень посилення якість відео покращиться.
Контакт Компенсація	Відео стане яскравішим за рахунок регулювання значення компенсації експозиції.
3D NR	При включенні функції 3D-шумопридушення (RD) можна знизити рівень відеошуму, щоб забезпечити більш високу чіткість відео. Ви можете встановити його оцінку, коли ця функція увімкнена. Вища оцінка означає більш чітке зображення.
Оцінка	

Крок 6 Налаштуйте зображення.

Малюнок 3-32 Зображення



Таблиця 3-22 Опис зображення

Параметр	Опис
Яскравість	Яскравість зображення. Більш високе значення означає яскравіші зображення.
Контраст	Контрастність — це різниця у яскравості чи кольорі, що робить об'єкт помітним. Чим більше значення контрастності, тим більше буде контраст кольору.
Відтінок	Належить до сили або насиченості кольору. Описує інтенсивність кольору чи його чистоту.
Насиченість	Насиченість кольору вказує на інтенсивність кольору зображення. У міру збільшення насиченості кольору здаються сильнішими, наприклад, більш червоними або більш синіми. Значення насиченості не змінює яскравість зображення.
Дзеркало	При включенні функції зображення відображатимуться з перевернутими лівою та правою сторонами.
Підкинути	Якщо увімкнути цю функцію, зображення можна перевертати.

3.8.1.2 Налаштування каналу 2

Процедура

Крок 1 Вибирати**Конфігурація аудіо та відео**>

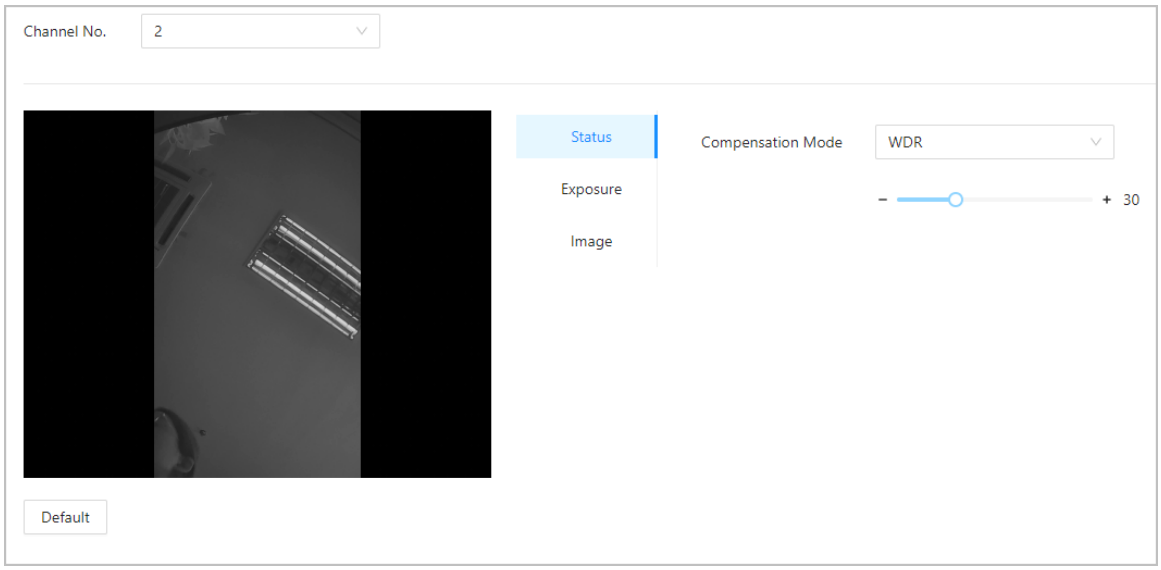
Крок 2 **Відео**. Вибирати**2**з**Номер каналу**список.

Крок 3 Виберіть 2 з**Номер каналу**. Налаштуйте

Крок 4 статус відео.

Ми рекомендуємо включати функцію WDR, коли особа знаходиться у контровому світлі.

Малюнок 3-33 Налаштування статусу

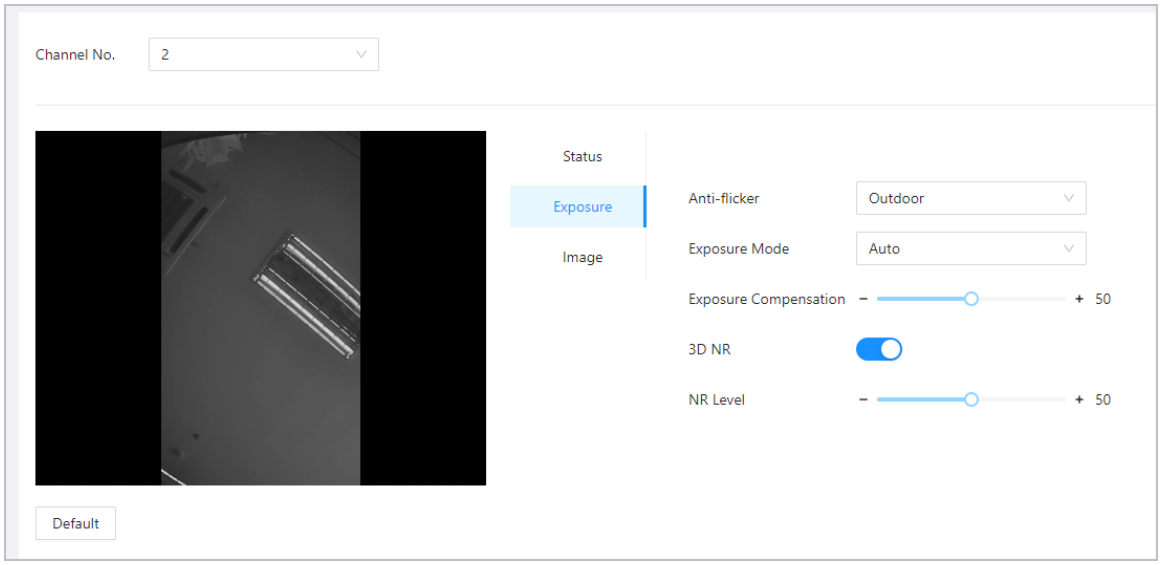


Таблиця 3-23 Опис статусу

Параметр	Опис
Режим компенсації	● **Забороняти**: Компенсацію вимкнено. ● **БЛК**: Компенсація контрового світла автоматично додає більше світла у темні області зображення, коли яскраве світло позаду затьмарює їх. ● **ВДР**: Система затемняє яскраві області та компенсує темні області, створюючи баланс для покращення загальної якості зображення. ● **КЛК**: Компенсація засвічення (HLC) - це технологія, що використовується в камерах відеоспостереження/IP-камери безпеки для обробки зображень, які піддаються впливу світла, наприклад фар або прожекторів. Датчик зображення камери виявляє сильні світлові плями на відео та зменшує експозицію у цих точках, щоб покращити загальну якість зображення.

Крок 5 Налаштуйте параметри експозиції.

Рисунок 3-34 Параметр експозиції



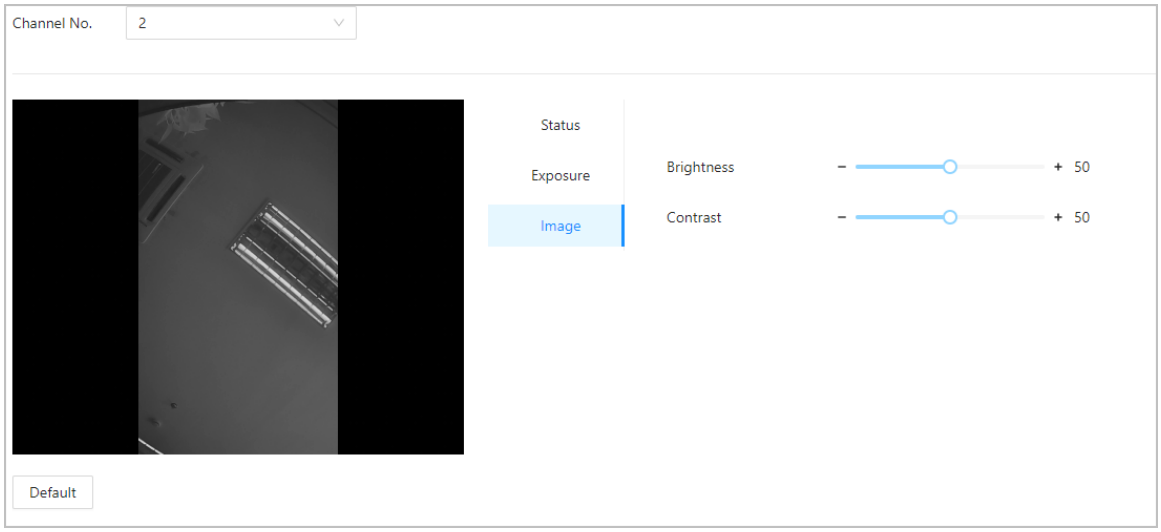
Таблиця 3-24 Опис параметрів експозиції

Параметр	Опис
Антиміготіння	Встановіть функцію «Антимігання», щоб зменшити мерехтіння та зменшити нерівномірність кольорів або експозиції. ● **50 Гц**: Якщо частота електромережі становить 50 Гц, експозиція автоматично регулюється залежно від яскравості навколишнього середовища, щоб запобігти поява горизонтальних ліній. ● **60 Гц**: Якщо частота електромережі становить 60 Гц, експозиція автоматично регулюється в залежності від яскравості навколишнього середовища, щоб зменшити поява горизонтальних ліній. ● **На відкритому повітрі**: Коли**На відкритому повітрі**вибраний, можна переключити режим експозиції.

Параметр	Опис
Режим експозиції	Ви можете налаштувати експозицію, щоб налаштувати яскравість зображення. ● **Авто**: Контролер доступу автоматично регулює яскравість зображень у залежність від навколишнього оточення. ● **Пріоритет витримки**: Контролер доступу регулює яскравість зображення в відповідно до встановленого діапазону затвора. Якщо зображення недостатньо яскраве, але значення затвора досягло свого верхнього чи нижнього межі, контролер доступу автоматично відрегулює значення посилення для ідеальний рівень яскравості. ● **Керівництво**: Ви можете вручну відрегулювати посилення та значення затвора, щоб налаштувати яскравість зображення. ◇ Коли ви обираєте**На відкритому повітрі**з**Антиміготіння**список, ви можете вибирати**Пріоритет витримки**як режим експозиції. ◇ Режим експозиції може відрізнятися залежно від моделі контролера доступу.
Контакт Компенсація	Відео стане яскравішим за рахунок регулювання значення компенсації експозиції.
3D NR	При включенні функції 3D-шумопридушення (RD) можна знизити рівень відеошуму, щоб забезпечити більш високу чіткість відео.
Рівень HP	Ви можете встановити його оцінку, коли ця функція увімкнена. Вища оцінка означає більш чітке зображення.

Крок 6 Налаштуйте параметри зображення.

Рисунок 3-35 Параметри зображення



Таблиця 3-25 Опис зображення

Параметр	Опис
Яскравість	Яскравість зображення. Більш високе значення означає яскравіші зображення.
Контраст	Контрастність — це різниця у яскравості чи кольорі, що робить об'єкт помітним. Чим більше значення контрастності, тим більше буде контраст кольору.

3.8.2 Налаштування звукових підказок

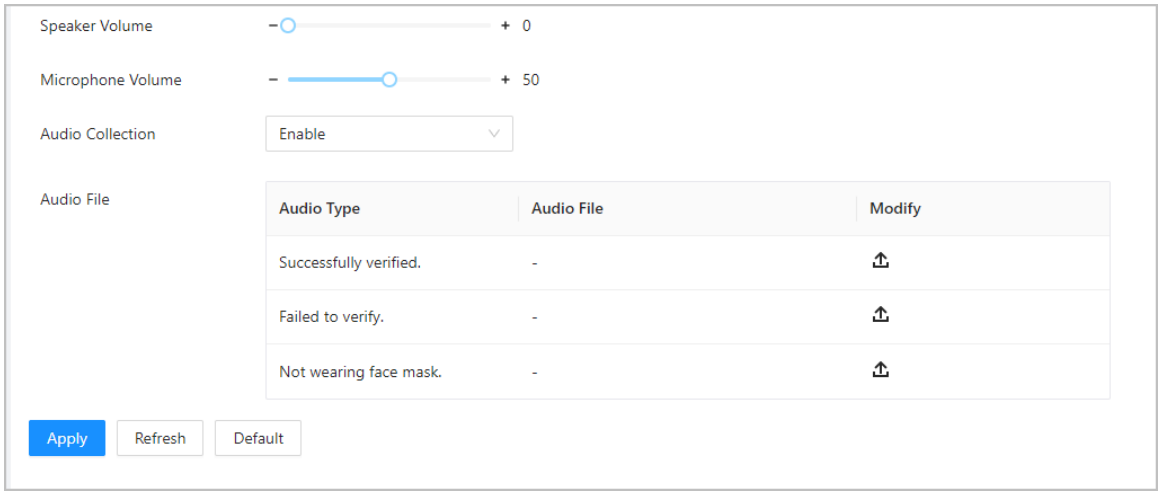
Встановіть звукові підказки під час перевірки особистості.

Процедура

Крок 1 Вибирати**Конфігурація аудіо та відео**>

Крок 2 **Аудіо**. Налаштуйте параметри звуку.

Рисунок 3-36 Налаштування параметрів звуку



Таблиця 3-26 Опис параметрів

Параметри	Опис
Спікер	Перетягніть повзунок, щоб відрегулювати гучність динаміка.
Гучність мікрофона	Перетягніть повзунок, щоб відрегулювати гучність мікрофона.
Аудіо Колекція	Якщо ця функція не увімкнена, під час відеодзвінка звук записуватися не буде.
Аудіофайл	Натисніть Завантажити аудіофайли на платформу.

Крок 3 Натисніть для завантаження аудіофайлів на платформу кожного типу аудіо.

Формат – MP3, розмір – менше 20 КБ.

Крок 4 Натисніть**Застосовувати**.

3.8.3 Налаштування виявлення руху

При виявленні об'єктів, що рухаються, і досягненні встановленого порогового значення екран активується.

Процедура

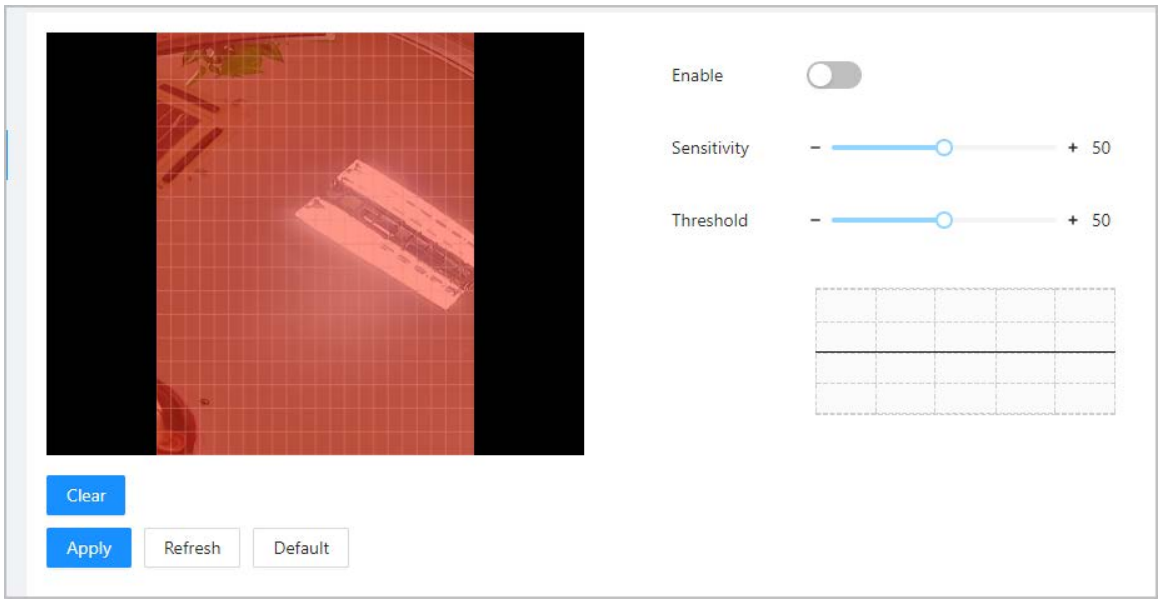
Крок 1 Вибирати**Конфігурація аудіо та відео**>**Налаштування виявлення руху**.

Крок 2 Увімкніть функцію виявлення руху.

Крок 3 Натисніть та утримуйте ліву кнопку миші, а потім намалюйте область виявлення у червоній області.

- Зона виявлення руху відображається червоним кольором.
- Щоб видалити існуючу область виявлення руху, натисніть**Прозорий**.
- Намальована вами область виявлення руху не буде областю виявлення руху, якщо ви намалюєте область виявлення руху за умовчанням.

Малюнок 3-37 Зона виявлення руху



Крок 4 Налаштуйте параметри.

- Чутливість: Чутливість до довкілля. Вища чутливість означає легше спрацьовування сигналізації.
- Поріг: відсоток площі об'єкта, що рухається, в зоні виявлення руху. Вищий поріг означає легше спрацьовування тривоги.

Крок 5 Натисніть**Застосовувати**.

Виявлення руху спрацьовує, коли з'являються червоні лінії; зелені лінії відображаються, коли Виявлення руху не спрацьовує.

3.8.4 Налаштування локального кодування

Встановіть область перегляду у відеообговоренні та попередньому перегляді.

Довідкова інформація

- Ця функція доступна лише в деяких моделях.
- Ця функція увімкнена за умовчанням під час роботи з VTH. Попередній перегляд може бути не доступно, коли цю функцію вимкнено.

Процедура

Крок 1 Увійдіть на веб-сторінку.

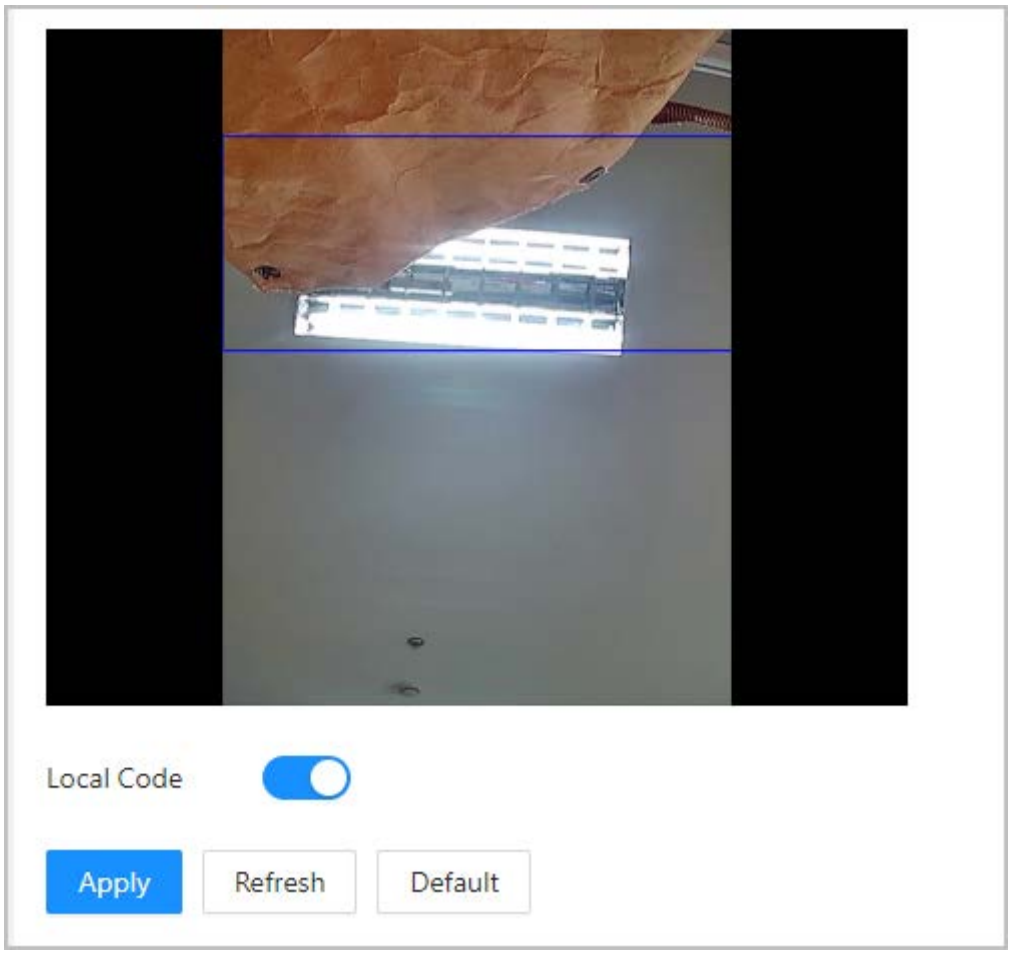
Крок 2 Вибирати**Конфігурація аудіо та відео**>**Налаштування виявлення руху**.

Крок 3 Вибирати**Давати можливість**Щоб увімкнути функцію, перетягніть поле в

Крок 4 вказане місце.

Поле означає область попереднього перегляду під час відеоконференції.

Малюнок 3-38 Локальне кодування



Крок 5 Натисніть**Застосовувати**.

3.9 Налаштування мережі

3.9.1 Налаштування TCP/IP

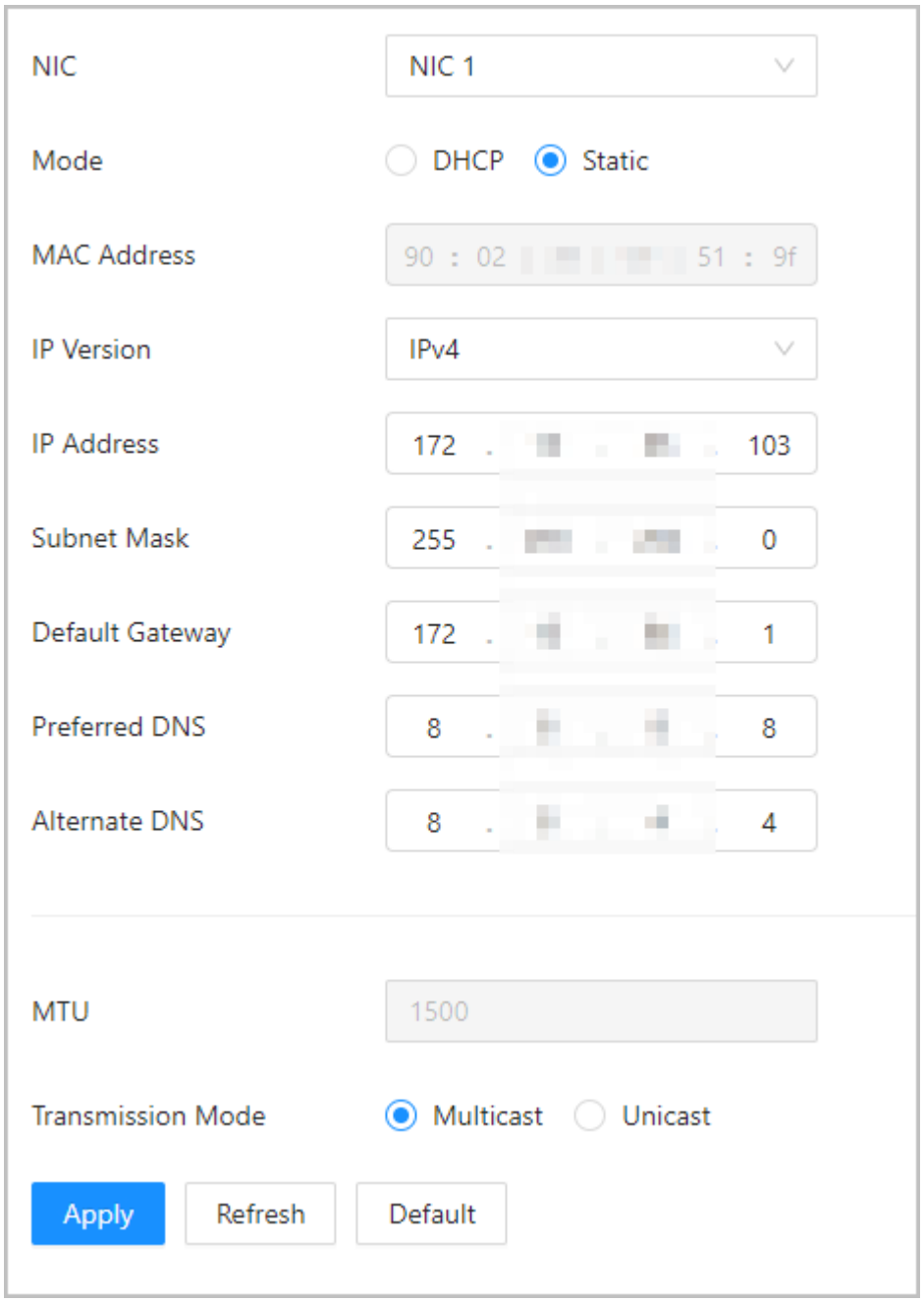
Вам необхідно налаштувати IP-адресу контролера доступу, щоб переконатися, що вона може взаємодіяти з іншими пристроями.

Процедура

Крок 1 Вибирати**Налаштування зв'язку**>**TCP/IP**.

Крок 2 Налаштуйте параметри.

Малюнок 3-39 TCP/IP



Таблиця 3-27 Опис TCP/IP

Параметр	Опис
Режим	● **Статичний**: Введіть IP-адресу, маску підмережі та шлюз вручну. ● **DHCP**: Це означає Dynamic Host Configuration Protocol При включенні DHCP контролеру доступу автоматично призначаються IP-адреса, маска підмережі та шлюз.
MAC-адреса	MAC-адреса контролера доступу.
IP-версія	IPv4 чи IPv6.
IP-адреса	Якщо ви встановите режим**Статичний**, налаштуйте IP-адресу, маску підмережі та шлюз.
Маска підмережі	

Параметр	Опис
За замовчуванням шлюз	 ● АдресаIPv6 представлений у шістнадцятковому форматі. ● ВерсіяIPv6 не потребує встановлення масок підмережі. ● IP-адреса та шлюз за замовчуванням повинні знаходитися в одному сегменті мережі.
Переважний DNS	Встановіть IP-адресу відданого DNS-сервера.
Альтернативний DNS	Встановіть IP-адресу альтернативного DNS-сервера.
МТУ	MTU (Maximum Transmission Unit) відноситься до максимального розміру даних, які можуть бути передані в одному пакеті мережі в комп'ютерних мережах. Більше значення MTU може підвищити ефективність передачі в мережі за рахунок скорочення кількості пакетів і пов'язаних з ними мережевих витрат. Якщо пристрій на мережному шляху не може обробляти пакети певного розміру, це може призвести до фрагментації пакетів або помилок передачі. У мережах Ethernet загальне значення MTU становить 1500 байт. Однак у деяких випадках, таких як використання PPPoE або VPN, можуть бути потрібні менші значення MTU для задоволення вимог певних мережевих протоколів або служб. Нижче наведено рекомендовані значення MTU для довідки: ● 1500: Максимальне значення для пакетів Ethernet, також значення замовчуванням. Це типове налаштування для мережевих підключень без PPPoE та VPN, деяких маршрутизаторів, мережевих адаптерів та комутаторів. ● 1492: Оптимальне значення для PPPoE ● 1468: Оптимальне значення для DHCP. ● 1450: Оптимальне значення для VPN.
Режим передачі	● Багатоадресна передача: ідеально підходить для відеоконференцій. ● Unicast: ідеально підходить для групових дзвінків.

Крок 3 Натисніть**ДОБРЕ**.

3.9.2 Налаштування Wi-Fi

Процедура

Крок 1 Вибирати**Налаштування зв'язку**>**TCP/IP**.

Крок 2 Увімкніть Wi-Fi.

З'являються всі доступні мережі Wi-Fi.

Функція Wi-Fi доступна лише у деяких моделях.

Крок 3 Кран +а потім введіть пароль Wi-Fi.

3.9.3 Налаштування порту

Ви можете обмежити доступ до контролера доступу одночасно через веб-сторінку, настільний клієнт та

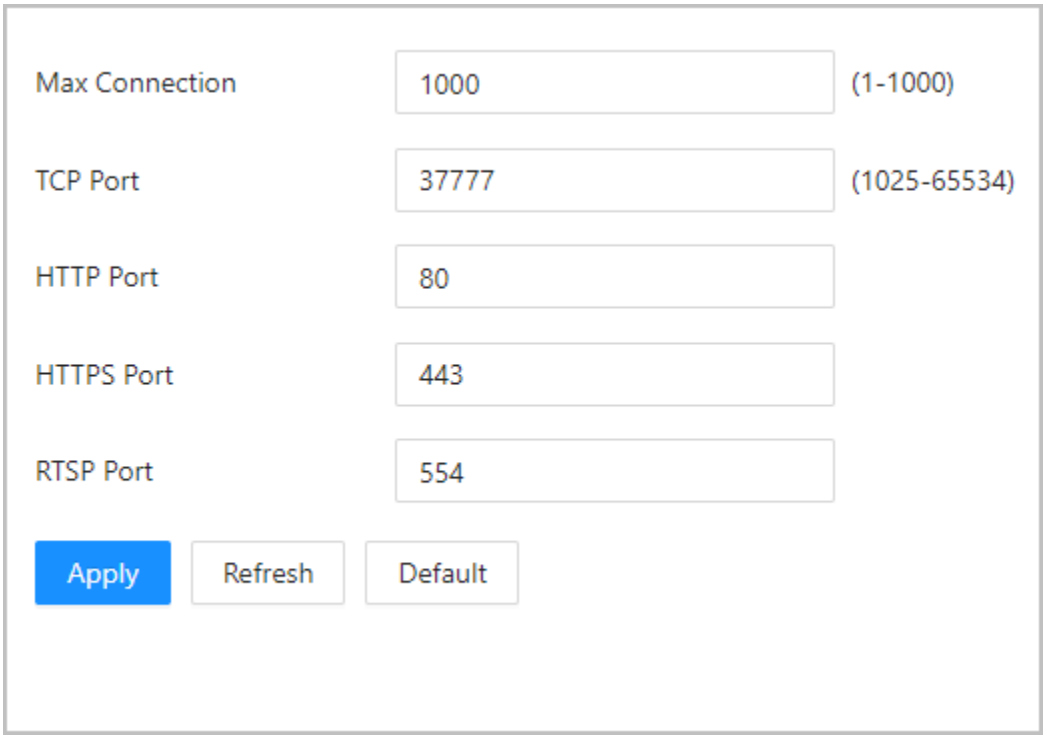
мобільного клієнта.

Процедура

Крок 1 Вибирати**Налаштування зв'язку**>**Порт**.

Крок 2 Налаштуйте порти.

Малюнок 3-40 Налаштування портів



За винятком**Макс. з'єднання**і**RTSP-порт**Вам необхідно перезапустити контролер доступу, щоб набирайте чинності після зміни інших параметрів.

Таблиця 3-28 Опис портів

Параметр	Опис
Макс. з'єднання	Ви можете встановити максимальну кількість клієнтів (наприклад, веб-сторінка, настільний клієнт та мобільний клієнт), які можуть отримати доступ до контролера доступу одночасно.
TCP-порт	Значення за замовчуванням – 37777.
HTTP-порт	Стандартне значення — 80. Якщо ви змінили номер порту, додайте номер порту після IP-адреси під час доступу до веб-сторінки.
HTTPS-порт	Значення за замовчуванням – 443.
RTSP-порт	Значення за замовчуванням – 554.

Крок 3 Натисніть**Застосовувати**.

3.9.4 Налаштування базової служби

Якщо ви бажаєте підключити контролер доступу до сторонньої платформи, увімкніть CGI та

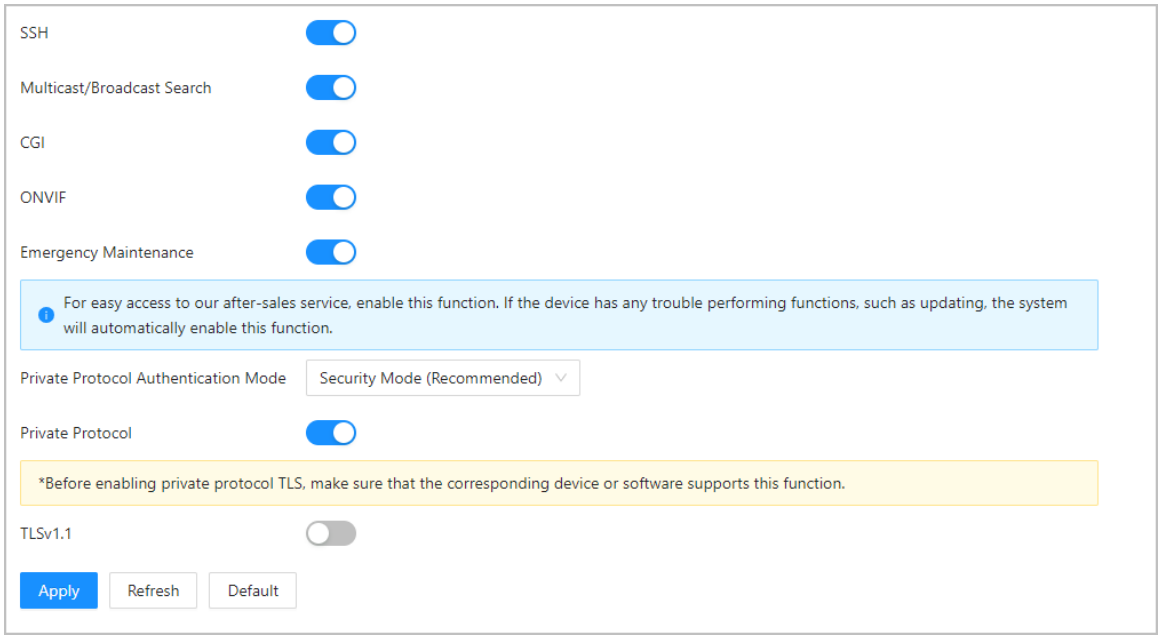
Опції ONVIF.

Процедура

Крок 1 Вибрати**Налаштування мережі**>**Базові послуги**.

Крок 2 Налаштуйте базову послугу.

Малюнок 3-41



Таблиця 3-29 Опис основних параметрів сервісу

Параметр	Опис
SSH	SSH (Secure Shell Protocol) – це протокол віддаленого адміністрування, який дозволяє користувачам отримувати доступ до своїх віддалених серверів, керувати ними та змінювати їх через Інтернет.
Пошук Multicast/Broadcast	Пошук пристроїв за протоколом багатоадресної або широкомовної передачі.
CGI	Інтерфейс загального шлюзу (CGI) являє собою точку перетину веб-серверів, через яку можливий стандартизований обмін даними між зовнішніми програмами та серверами.
ONVIF	ONVIF означає Open Network Video Interface Forum (Форум відкритого мережевого відеоінтерфейсу). Його мета – надати стандарт для інтерфейсу між різними пристрої безпеки на базі IP. Ці стандартизовані ONVIF Специфікації подібні до загальної мови, яку можуть використовувати всі пристрої для спілкування.
Аварійне обслуговування	За замовчуванням цю функцію увімкнено.
Приватний протокол Режим автентифікації	Встановіть режим автентифікації, включаючи безпечний режим та сумісність. Рекомендується вибрати**Режим безпеки**. ● Режим безпеки (рекомендовано): не підтримує доступ до пристрою за допомогою методів аутентифікації Digest, DES та відкритий текст, що підвищує безпеку пристрою. ● Сумісний режим: підтримує доступ до пристрою за допомогою методів аутентифікації Digest, DES та відкритого тексту зі зниженою безпекою.

Параметр	Опис
Приватний протокол	Платформа додає пристрої за протоколом TLSv1.1.  При включенні TLSv1.1 можуть виникнути ризики безпеки. Зверніть увагу.

Крок 3 Натисніть**Застосовувати**.

3.9.5 Налаштування хмарного сервісу

Хмарний сервіс пропонує послугу проникнення NAT. Користувачі можуть керувати кількома пристроями через DMSS.

Вам не потрібно подавати заявку на динамічне доменне ім'я, налаштовувати зіставлення портів або розгортати сервер.

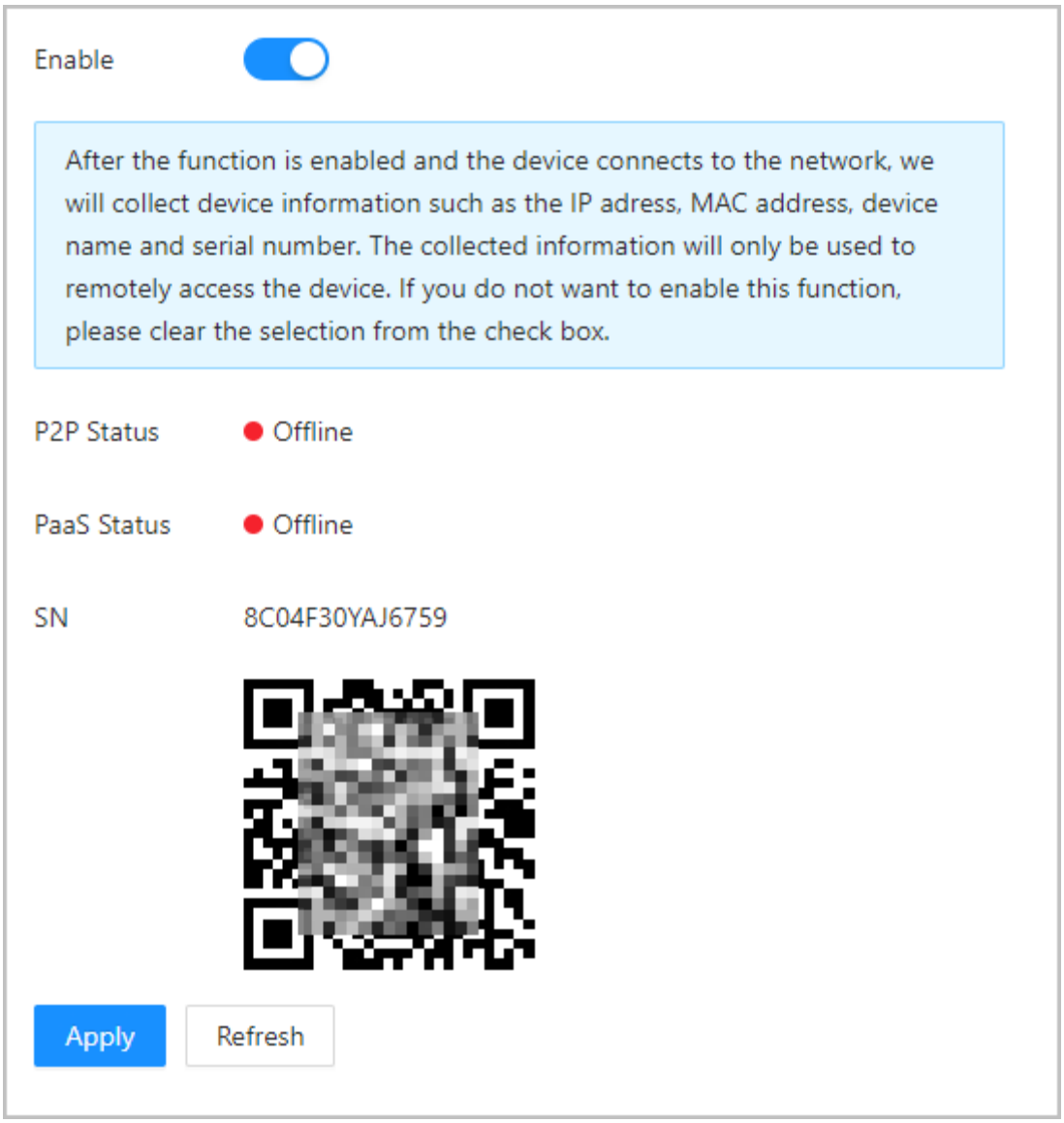
Процедура

Крок 1 На головній сторінці виберіть**Налаштування мережі**>**Хмарний сервіс**.

Крок 2 Увімкніть функцію хмарного сервісу.

Хмарний сервіс переходить у режим онлайн, якщо P2P та PaaS перебувають у режимі онлайн.

Малюнок 3-42 Хмарний сервіс



Крок 3 Натисніть**Застосовувати**.

Крок 4 Щоб додати пристрій, відскануйте QR-код за допомогою DMSS.

3.9.6 Налаштування активної реєстрації

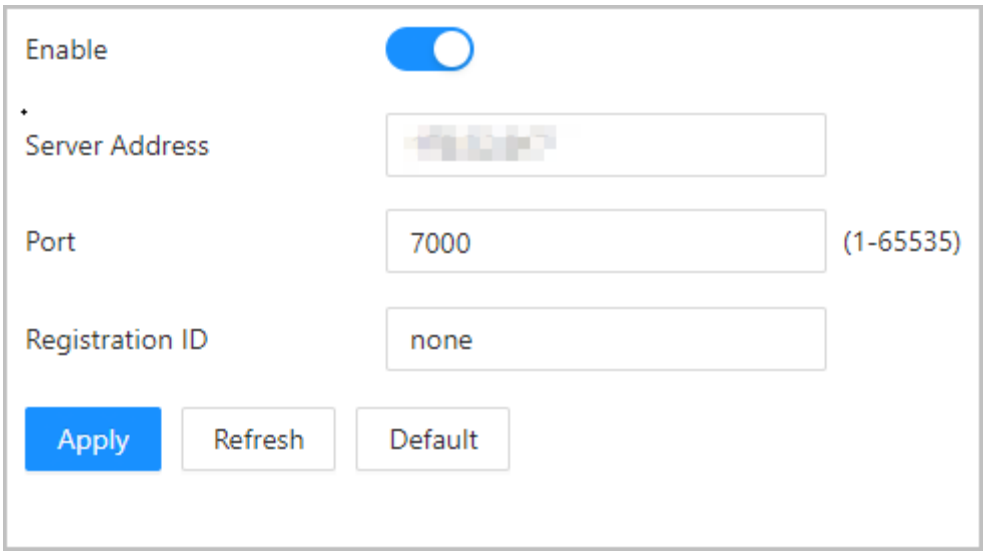
Активна реєстрація дозволяє додавати пристрої на платформу керування без ручного введення інформації про пристрій, такий як IP-адреса та порт.

Процедура

Крок 1 На головній сторінці виберіть**Налаштування мережі**>**Автоматична реєстрація**.

Крок 2 Увімкніть автоматичну реєстрацію та налаштуйте параметри.

Малюнок 3-43 Автоматична реєстрація



Таблиця 3-30 Опис автоматичної реєстрації

Параметр	Опис
Адреса сервера	IP-адреса або доменне ім'я сервера.
Порт	Порт сервера, який використовується для автоматичної реєстрації.
Реєстраційний ідентифікатор	Реєстраційний ідентифікатор (визначається користувачем) пристрою. Додавання пристрої управління шляхом введення реєстраційного ідентифікатора на платформі.

Крок 3 Натисніть**Застосовувати**.

3.10 Налаштування RS-485

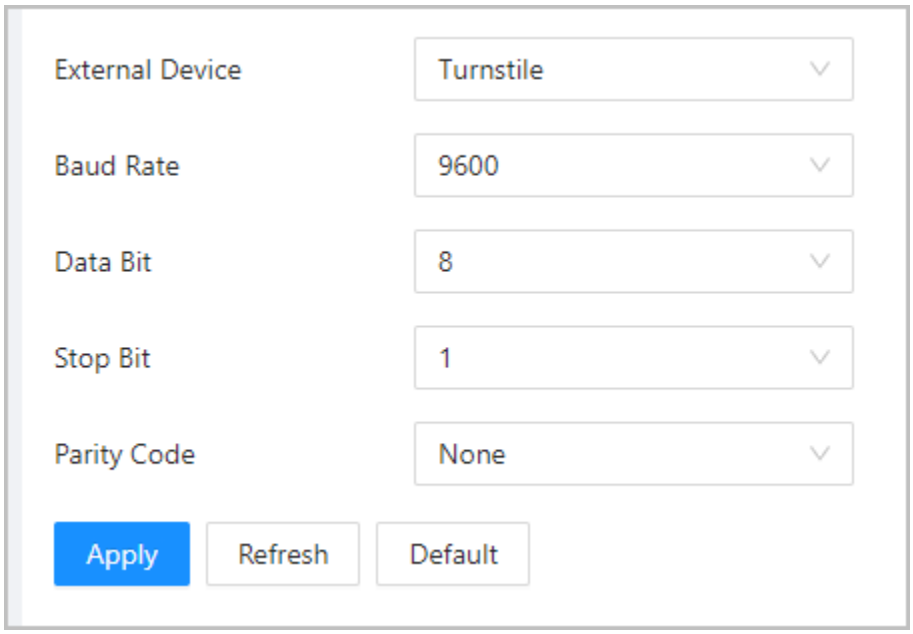
Налаштуйте параметри RS-485, якщо ви підключаєте зовнішній пристрій до порту RS-485.

Процедура

Крок 1 Вибирати**Налаштування зв'язку**>**Установки RS-485**.

Крок 2 Налаштуйте параметри.

Малюнок 3-44 Налаштування параметрів



Таблиця 3-31 Налаштування формату Wiegand

Параметр	Опис
Зовнішній пристрій	● Контролер доступу: Вибрати**Контролер доступу**коли контролер доступу функціонує як зчитувач карт, так і контролер доступу буде надсилати дані контролеру доступу для керування доступом. Тип вихідних даних: ◇ Номер картки: виводить дані на основі номера картки, коли користувачі проводять картою, щоб відімкнути двері; виводить дані на основі номера першої карти користувача, коли вони використовують інші методи розблокування. ◇ Ні: Виводить дані на основі ідентифікатора користувача. ● Пристрій для читання карт: Контролер доступу підключається до пристрою читання карт. ● Зчитувач (OSDP): Контролер доступу підключається до зчитувачу карток на основі протоколу OSDP. ● Модуль безпеки керування дверима: кнопка виходу з дверей, замок та пожежний зв'язок не працюють після включення модуля безпеки. ● Турнікет: Коли контролер доступу підключається до турнікету, а плата контролера доступу турнікета підключається до зовнішнього модулю QR-коду чи модулю зчитування карток, плата передає дані перевірки турнікету.
Біт даних	Число біт, що використовуються для передачі фактичних даних у послідовному зв'язку. Воно являє собою двійкові цифри, що несуть інформацію, що передається.

Параметр	Опис
Стоп-біт	Біт, що відправляється після даних та необов'язкових бітів парності, щоб вказати кінець передачі. Він дозволяє приймачеві підготуватися до наступного байта даних та забезпечує синхронізація у протоколі зв'язку.
Код парності	Додатковий біт, що надсилається після бітів даних для виявлення помилок передачі. Він допомагає перевірити цілісність даних, що передаються, гарантуючи певну кількість логічних високих чи низьких бітів.

Крок 3 Натисніть**Застосовувати**.

3.11 Налаштування Wiegand

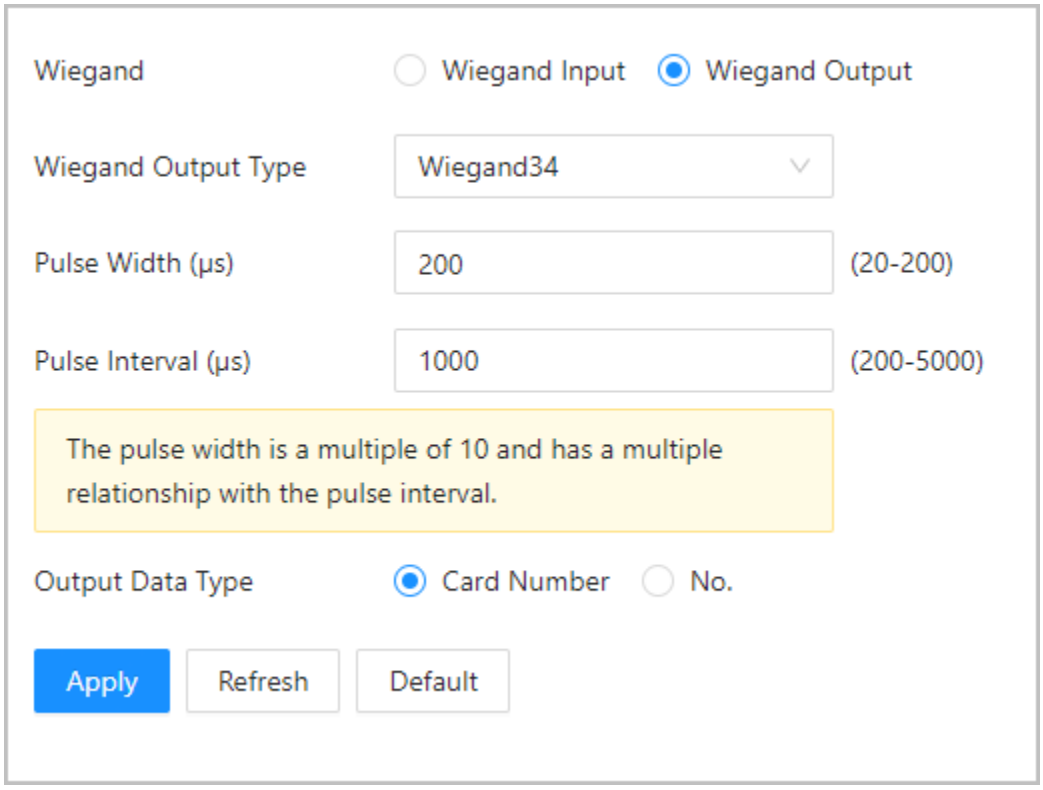
Налаштуйте параметри RS-485, якщо ви підключаєте зовнішній пристрій до порту RS-485.

Процедура

Крок 1 Вибирати**Налаштування зв'язку**>**Віганд**.

Крок 2 Налаштуйте параметри.

Малюнок 3-45 Налаштування параметрів



Таблиця 3-32 Опис виходу Wiegand

Параметр	Опис
Тип виходу Wiegand	Виберіть формат Wiegand, щоб прочитати номери карт або ідентифікаційні номери. ● **Віганд26**: Зчитує 3 байти або 6 цифр ● **Віганд34**: Зчитує 4 байти або 8 цифр ● **Вігандб6**: Зчитує 8 байт або 16 цифр

Параметр	Опис
Ширина імпульсу	Введіть ширину імпульсу та інтервал виходу Wiegand.
Інтервал імпульсу	
Тип вихідних даних	Виберіть тип вихідних даних. ● **Hi.**: Виводить дані на основі ідентифікатора користувача. Формат даних - шістнадцятковий або десятковий. ● **Номер картки**: Виводить дані на основі номера першої картки користувача.

Крок 3 Натисніть**Застосовувати**.

3.12 Налаштування системи

3.12.1 Управління користувачами

Ви можете додавати або видаляти користувачів, змінювати паролі користувачів та вводити електронну адресу. пошти для скидання пароля, якщо ви забудете його.

3.12.1.1 Додавання адміністраторів

Ви можете додавати нові облікові записи адміністраторів, після чого вони можуть входити на веб-сторінку контролера доступу.

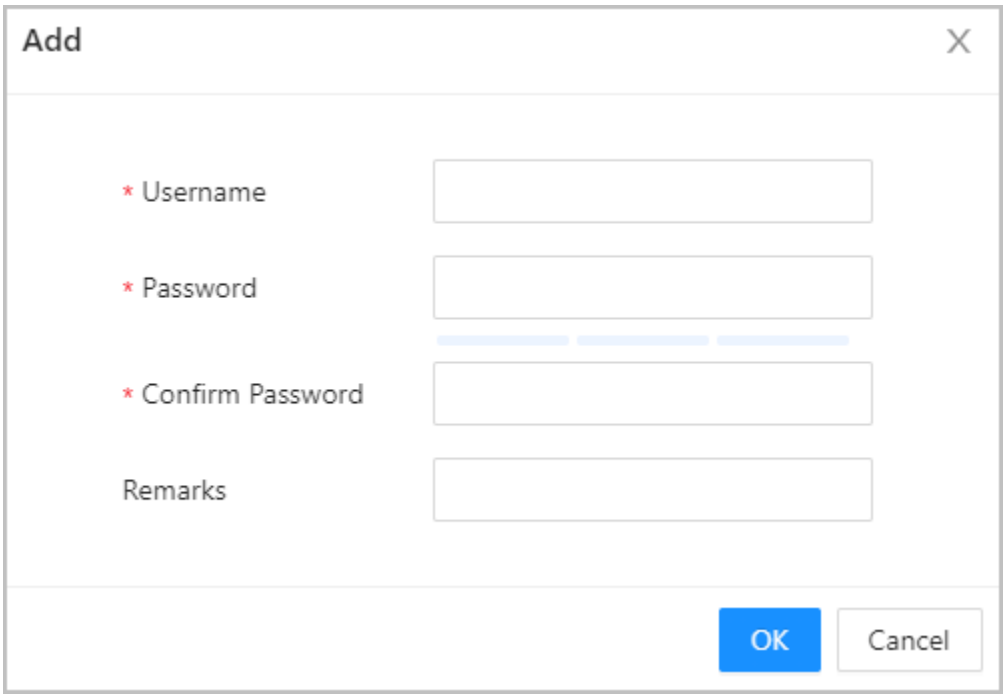
Процедура

Крок 1 На головній сторінці виберіть**Система**>**Рахунок**. Натисніть

Крок 2 **Додавати**та введіть інформацію про користувача.

- Ім'я користувача не може збігатися з існуючим обліковим записом. Ім'я користувача складається з до 31 символу і допускає лише цифри, літери, підкреслення, середні лінії, крапки або @.
- Пароль повинен складатися з 8–32 непустих символів та містити не менше двох типи наступних символів: великі літери, малі літери, цифри та спеціальні символи символи (за винятком ' " ; : &). Встановіть пароль високого ступеня безпеки за паролем. підказка за силою.

Малюнок 3-46 Додати адміністраторів



Крок 3 Натисніть**ДОБРЕ**.

Змінити пароль може лише обліковий запис адміністратора, і обліковий запис адміністратора не можна видалити.

3.12.1.2 Додавання користувачів ONVIF

Довідкова інформація

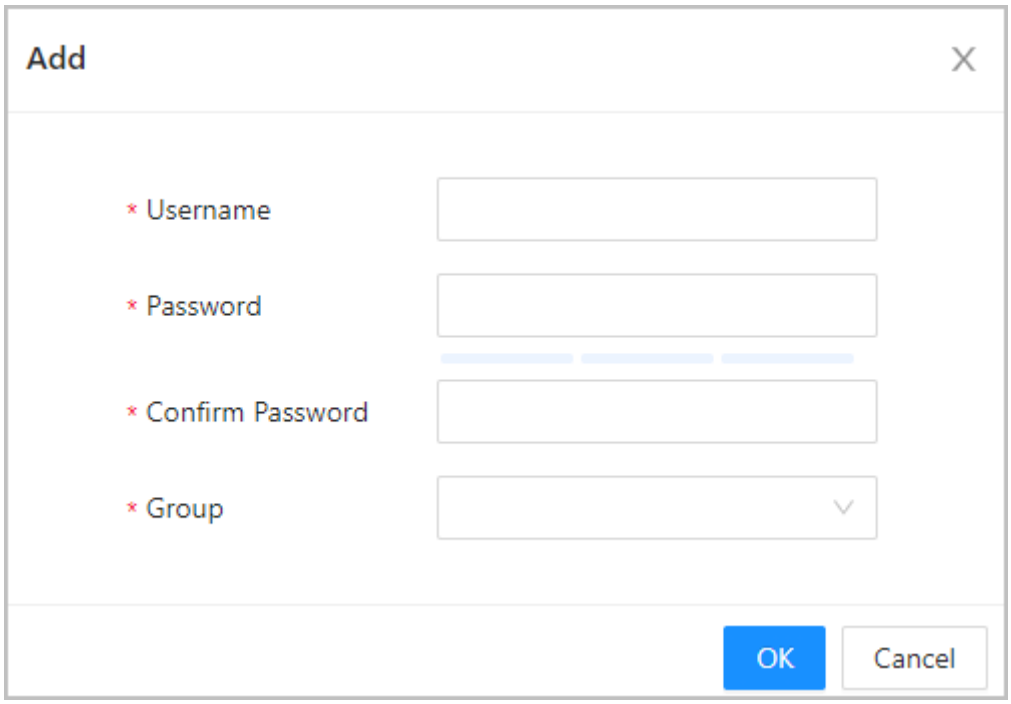
Open Network Video Interface Forum (ONVIF), глобальний та відкритий галузевий форум, створений для розробки глобального відкритого стандарту для інтерфейсу фізичних продуктів безпеки на основі IP, який забезпечує сумісність із продуктами різних виробників. Користувачі ONVIF перевіряють свою особу за допомогою протоколу ONVIF. За замовчуванням ONVIF — адміністратор.

Процедура

Крок 1 На головній сторінці виберіть**Система**>**Рахунок**>**Користувач ONVIF**.

Крок 2 Натисніть**Додавати**, а потім налаштуйте параметри.

Рисунок 3-47 Додати користувача ONVIF



Крок 3 Натиснітьдобре.

3.12.1.3 Скидання пароля

Якщо ви забули пароль, скиньте його, скориставшись посиланням на електронний лист.

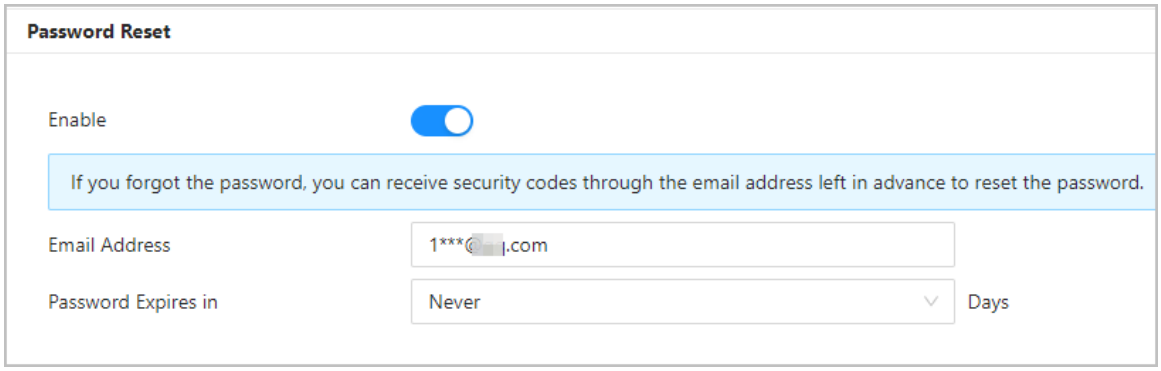
Процедура

Крок 1 Вибирати**Система**>**Рахунок**.

Крок 2 Введіть адресу електронної пошти та встановіть термін дії

Крок 3 пароля. Увімкніть функцію скидання пароля.

Малюнок 3-48 Скидання пароля



Якщо ви забули пароль, ви можете отримати код безпеки за вказаною адресою електронної пошти.

адресу для скидання пароля.

Крок 4 Натиснітьзастосовувати.

3.12.1.4 Перегляд користувачів онлайн

Ви можете переглядати онлайн-користувачів, які зараз заходять на веб-сторінку. На домашній сторінці виберіть**Система**>

Користувач онлайн.

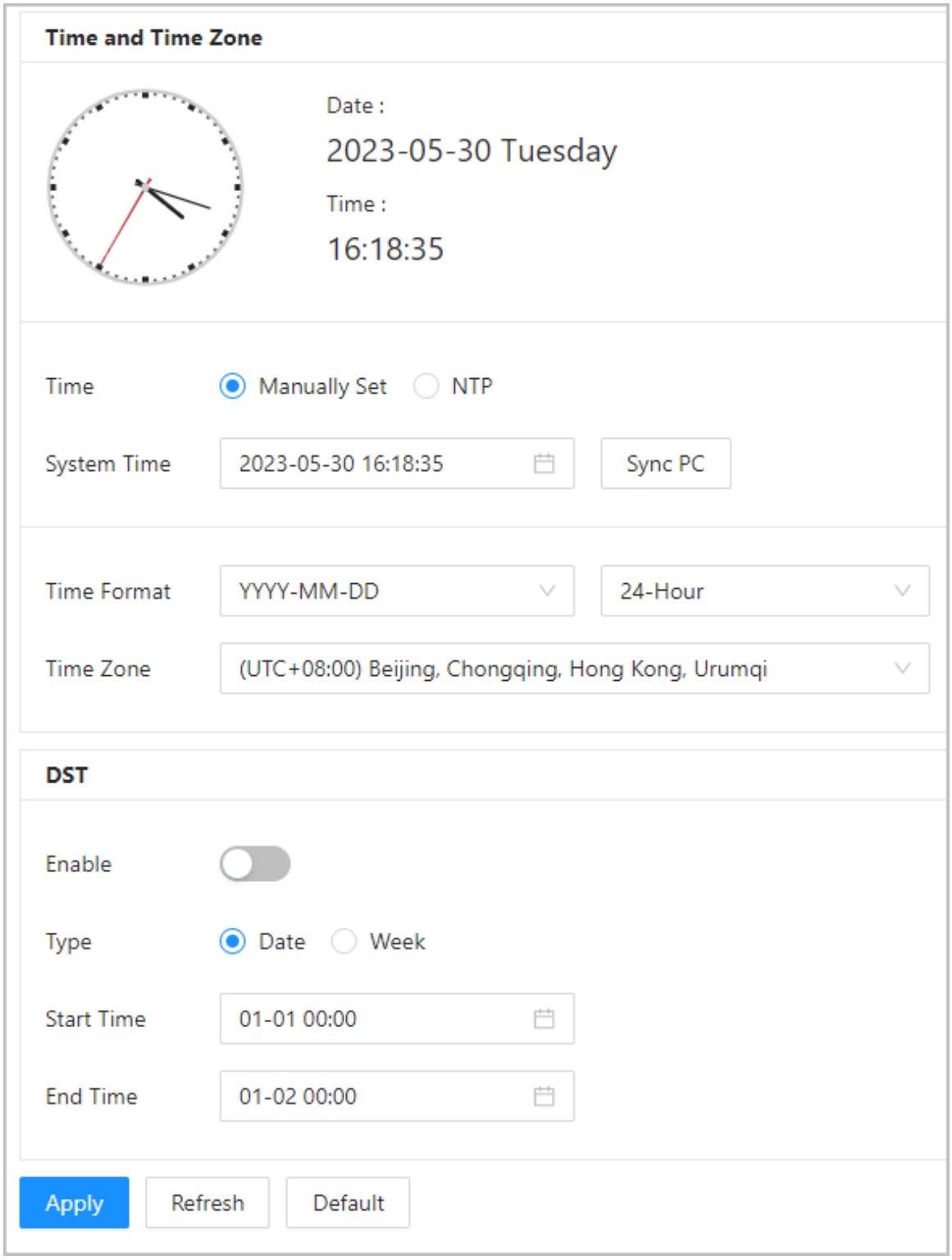
3.12.2 Налаштування часу

Процедура

Крок 1 На головній сторінці виберіть**Система**>

Крок 2 **Час**. Налаштуйте час платформи.

Малюнок 3-49 Налаштування дати



Таблиця 3-34 Опис налаштувань часу

Параметр	Опис
Час	● Ручне встановлення: введіть час вручну або натисніть**Синхронізувати час**для синхронізація часу з комп'ютером. ● NTP: Контролер доступу автоматично синхронізує час із сервером NTP. ◇ **Сервер**: Введіть домен сервера NTP. ◇ **Порт**: Введіть порт NTP-сервера. ◇ **Інтервал**: Введіть час із інтервалом синхронізації.
Формат часу	Виберіть формат часу.
Часовий пояс	Введіть часовий пояс.
літній час	1. (Необов'язково) Увімкніть літній час. 2. Вибрати**Дата**або**Тиждень**з**Тип**. 3. Налаштуйте час початку та закінчення літнього часу.

Крок 3 Натисніть**Застосовувати**.

3.12.3 Технічне обслуговування

Регулярно перезапускайте контролер доступу під час його простою, щоб підвищити його продуктивність.

Процедура

Крок 1 Увійти на веб-сторінку. Вибрати**Система**>

Крок 2 **Обслуговування**. Встановіть час, а потім

Крок 3 натисніть**Застосовувати**.

Контролер доступу перезапуститься у запланований час, або ви можете натиснути**Перезапуск**щоб перезапустити його негайно.

3.12.4 Управління конфігурацією

Якщо кільком контролерам доступу потрібні однакові конфігурації, ви можете налаштувати для них параметри, імпортувавши або експортувавши файли конфігурації.

3.12.4.1 Експорт та імпорт файлів конфігурації

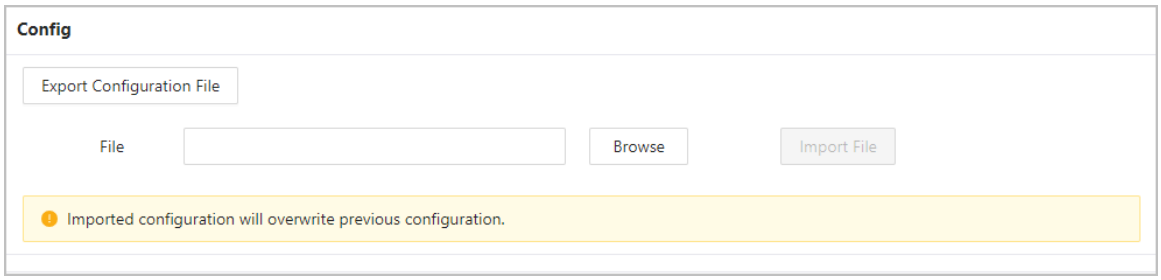
Ви можете імпортувати та експортувати конфігураційний файл для контролера доступу. Коли ви хочете застосувати ті ж конфігурації до кількох пристроїв, можна імпортувати файл конфігурації на них.

Процедура

Крок 1 Увійти на веб-сторінку. Вибрати

Крок 2 **Система**>**Конфігурація**.

Малюнок 3-50 Керування конфігурацією



Крок 3 Експорт або імпорт конфігураційних файлів.

- Експортуйте конфігураційний файл.

  Натисніть**Експортувати конфігураційний файл**для завантаження файлу на локальний комп'ютер.

  IP не буде експортовано.

- Імпортуйте конфігураційний файл.

  1. Натисніть**Переглядати**для вибору конфігураційного файлу.

  2. Натисніть**Імпорт конфігурації**.

  Файли конфігурації можна імпортувати лише на пристрої тієї ж моделі.

3.12.4.2 Відновлення заводських налаштувань за умовчанням

Процедура

Крок 1 Вибирати**Система**>**Конфігурація**.

Відновлення**Контролер доступу**до його налаштувань за умовчанням призведе до втрати даних. Будь ласка будьте обережні.

Крок 2 У разі потреби відновіть заводські установки за промовчанням.

- **Заводські налаштування за замовчуванням**: Скидає всі конфігурації контролера доступу та видаляє всі дані.
- **Відновити параметри за замовчуванням (за винятком інформації про користувача та журналів)**: Скидає налаштування контролера доступу та видаляє всі дані, за винятком інформації про користувачів та журналів.

Підтримує лише основний контролер**Відновити параметри за замовчуванням (за винятком інформації про користувача та журналів)**.

3.12.5 Оновлення системи

- Використовуйте правильний файл оновлень. Переконайтеся, що ви отримали правильний файл оновлень від технічної підтримки.
- Не вимикайте живлення або мережу, не перезавантажуйте та не вимикайте Access. Контролер під час оновлення.

3.12.5.1 Оновлення файлу

Процедура

Крок 1 На головній сторінці виберіть**Система**>**Оновлювати**.

Крок 2 У**Оновлення файлу**, натисніть**Переглядати**, а потім завантажте файл оновлень.

Файл поновлення повинен мати розширення .bin.

Крок 3 Натисніть**Оновлювати**.

Контролер доступу перезавантажиться після завершення оновлення.

3.12.5.2 Онлайн-оновлення

Процедура

Крок 1 На головній сторінці виберіть**Система**>**Оновлювати**.

Крок 2 У**Онлайн-оновлення**Виберіть спосіб оновлення.

- Вибирати**Автоматична перевірка оновлень**, та контролер доступу автоматично перевірить наявність останньої версії оновлення.
- Вибирати**Ручна перевірка**, і ви можете відразу ж перевірити, чи доступна остання версія.

Крок 3 (Необов'язково) Натисніть**Оновити зараз**негайно оновити контролер доступу.

3.12.6 Перегляд інформації про версію

На веб-сторінці виберіть**Система**>**Версія**, і ви можете переглянути інформацію про версію контролера доступу.

3.12.7 Перегляд ємності даних

На веб-сторінці виберіть**Система**>**Місткість даних**, перегляньте ємність даних контролера доступу.

3.12.8 Перегляд юридичної інформації

На головній сторінці виберіть**Система**>**Юридична інформація**, а також ви можете ознайомитися з ліцензійною угодою щодо програмного забезпечення, політикою конфіденційності та повідомлення про програмне забезпечення з відкритим вихідним кодом.

3.13 Персоналізація

Налаштуйте теми та додайте відео- або графічні ресурси до контролера доступу.

3.12.1 Додавання ресурсів

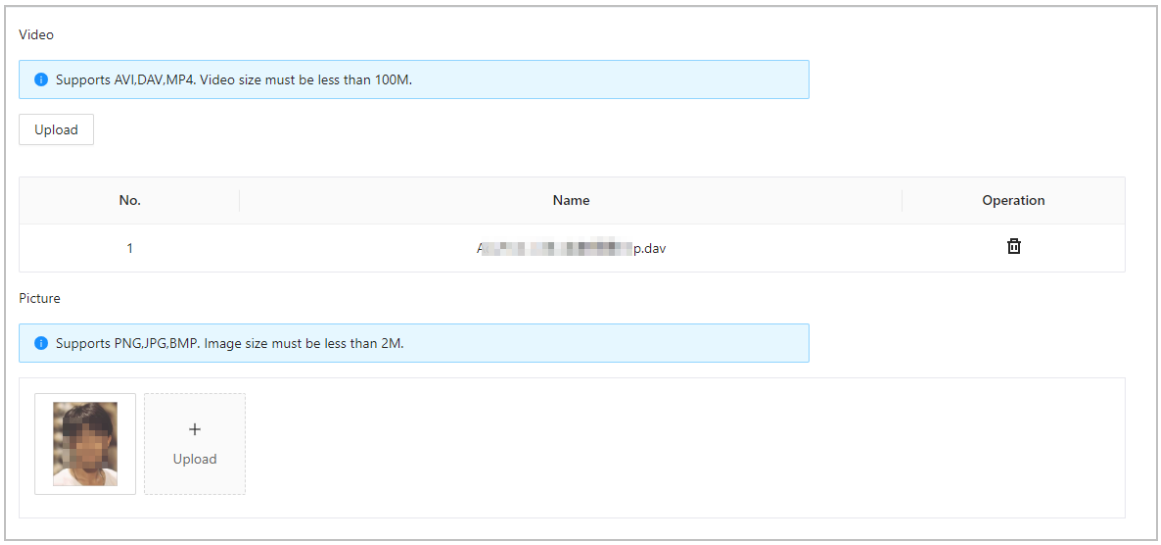
Додайте зображення або відео, які відображатимуться на екрані очікування контролера доступу.

Процедура

Крок 1 На головній сторінці виберіть**Персоналізація**>**Реклама**>**Рекламні ресурси**. Додати відео

Крок 2 або зображення.

Малюнок 3-51 Додати відео чи зображення



- Додати відео.

  1. Натисніть**Завантажити**.

  2. Натисніть**Переглядати**, виберіть відеофайл, а потім натисніть**Наступний**.

     Відео автоматично завантажується на платформу після перекодування.

     - Ви можете завантажити до 5 відеофайлів.
     - Підтримує DAV, AVI, MP4. Розмір відео має бути меншим за 100 МБ.
     - Для завантаження відео підтримуються лише останні версії FireFox та Chrome.

- Додати зображення.

  1. Натисніть.

2. Виберіть зображення з локального сховища та завантажте його.

Підтримує PNG, JPG, BMP. Розмір зображення має бути меншим за 2 Мб.

Пов'язані операції

Натисніть для видалення завантажених зображень або відео.

Відео та зображення не можна видалити.

3.13.2 Налаштування тем

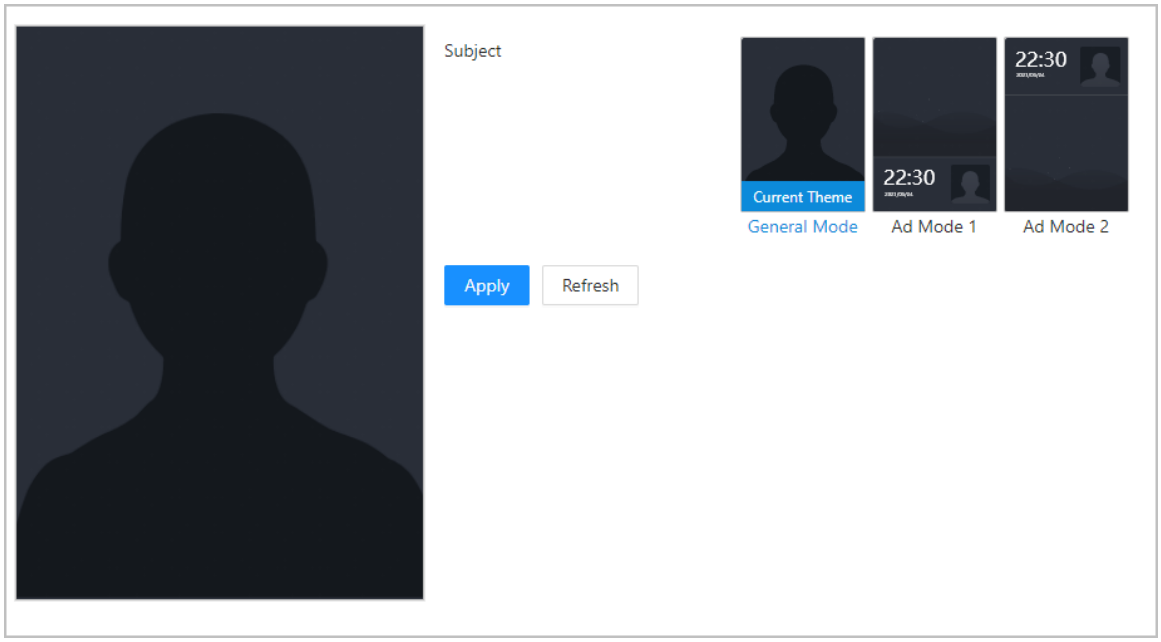
Процедура

Крок 1 На головній сторінці виберіть**Персоналізація**>**Реклама**>**Предмет**.

Крок 2 Виберіть тему.

- Загальна тема: Показує зображення обличчя на весь екран.
- Режим реклами1: у верхній області відображається реклама, а в нижній – час та поле розпізнавання облич.
- Режим реклами2: у верхній області відображається час і поле розпізнавання облич, а в нижній області відображається реклама.

Малюнок 3-52 Тема

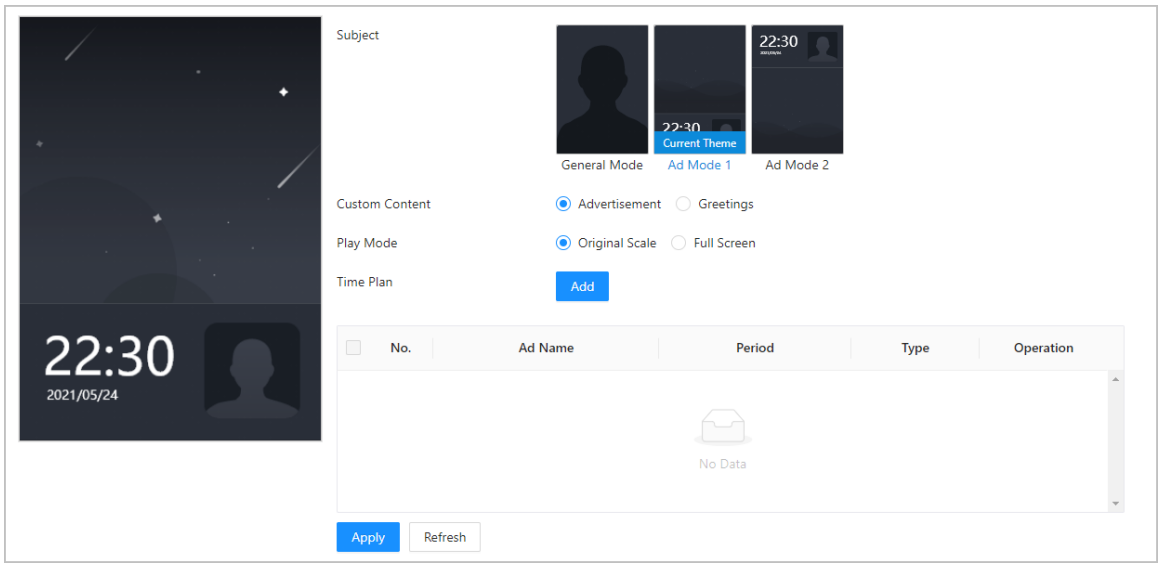


Крок 3 Виберіть голосову підказку для успішної перевірки особистості.

Крок 4 Встановіть показ реклами.

1. Виберіть режим реклами 1 або режим реклами 2, а потім виберіть**Реклама**.

Малюнок 3-53 Режим реклами



2. Виберіть режим відображення.

- Вихідний масштаб: відтворює зображення та відео у вихідному розмірі.
- Повний екран: відтворює зображення та відео на весь екран.

3. Натисніть**Додавати**для додавання розкладу.

Ви можете додати до 10 розкладів.

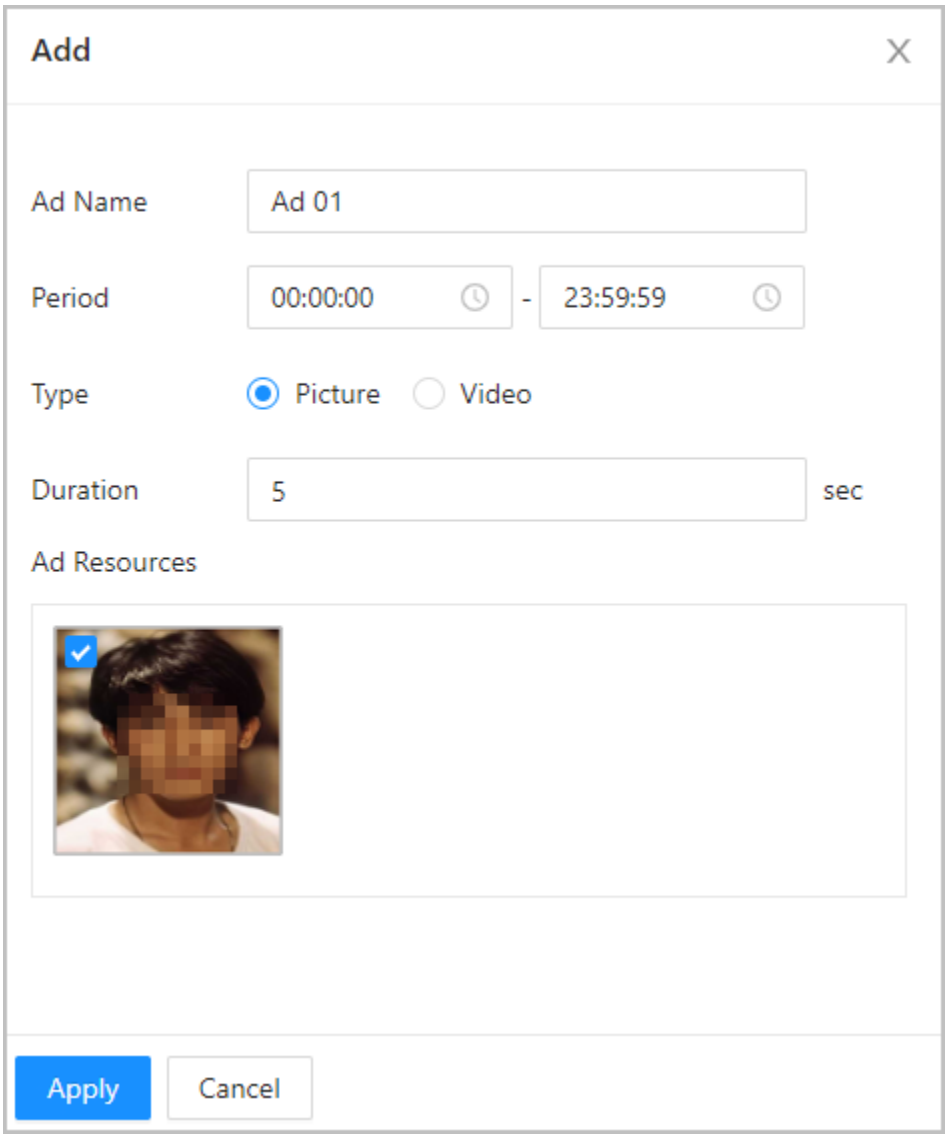
4. Введіть назву оголошення.

5. Виберіть часовий відрізок, тип файлу та файл.

6. Введіть тривалість, а потім натисніть**Застосовувати**.

Встановіть тривалість одного зображення, коли зображення відтворюються в циклі. Тривалість варіюється від 1 до 20 с і за замовчуванням становить 5 с.

Малюнок 3-54 Додати розклад



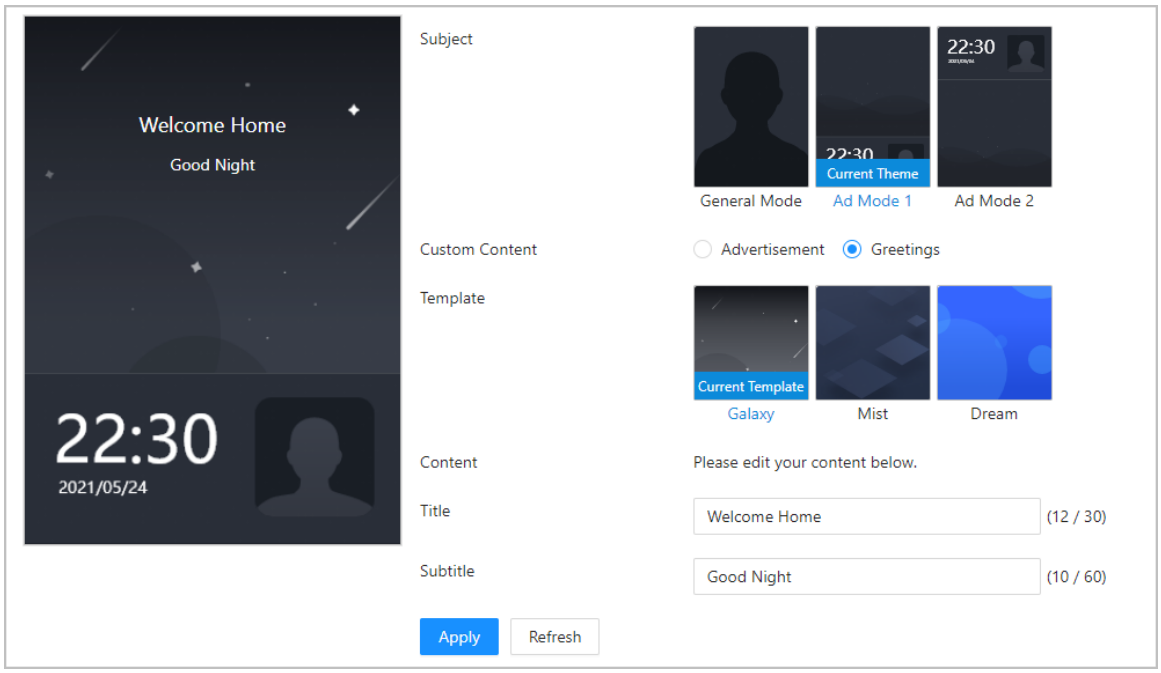
Крок 5 Налаштуйте привітання.

1. Вибрати**Привіт**з**Контент користувача**.

2. Виберіть шаблон.

3. Введіть заголовок та підзаголовок.

Малюнок 3-55 Вітання



4. Натисніть**Застосовувати**.

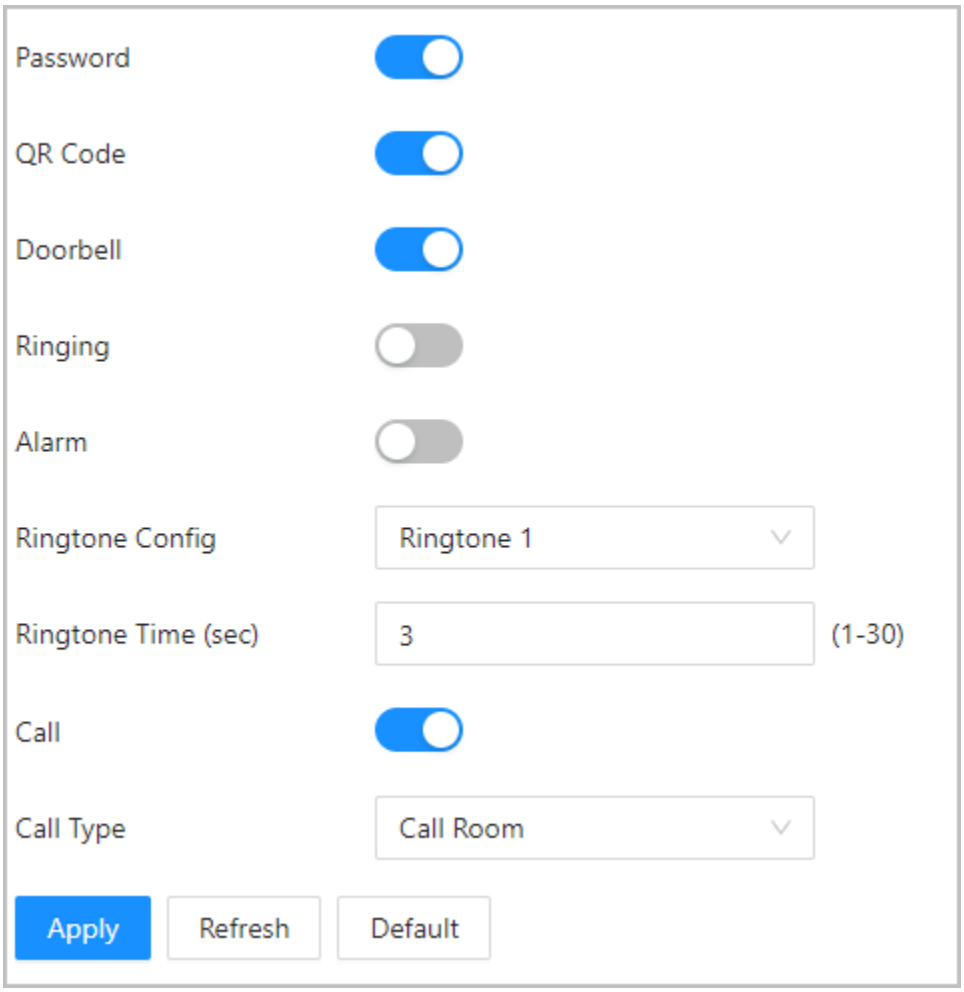
3.13.3 Налаштування клавіш.

Процедура

Крок 1 На веб-сторінці контролера доступу виберіть**Персоналізація**>**Налаштування клавіш**.

Крок 2 Налаштуйте параметри комбінації клавіш.

Рисунок 3-56 Налаштування клавіш.



Таблиця 3-35 1

Параметр	Опис
Пароль	Значок методу розблокування пароля відображається на екрані очікування.
QR-код	QR-код відображається на екрані очікування. Ця функція недоступна для контролера доступу з автономним модулем QR-коду.
Дверний дзвінок	Після активації дверцят на екрані режиму очікування відображається дверний дзвінок значок. ● Дзвінок: натисніть піктограму дзвінка на екрані режиму очікування та контролер доступу задзвонить. ● Сигналізація: увімкніть функцію зв'язку з сигналізацією, після чого пролунає дзвінок у двері. Ця функція доступна лише в деяких моделях. ● Настроювання рінгтону: виберіть дзвінок. ● Ringtone Times (sec): Встановіть час дзвінка (1-30 секунд). Значення за замовчуванням – 3.
Виклик	Значок дзвінка з'являється на екрані в режимі очікування.

Параметр	Опис
Тип виклику	● Кімната для дзвінків: натисніть піктограму дзвінка в режимі очікування та введіть номер кімнати для здійснення дзвінків. ● Центр керування дзвінками: натисніть піктограму дзвінка в режимі очікування, а потім зателефонуйте до центру керування. ● Номер дзвінка: введіть номер кімнати, а потім натисніть значок дзвінка на екрані очікування, щоб зателефонувати на попередньо заданий номер кімнати.  Переконайтеся, що контролер доступу додано до DMSS.

3.14 Перегляд журналів

Переглядайте журнали, такі як системні журнали, журнали адміністратора та записи розблокування.

3.14.1 Системні журнали

Перегляд та пошук системних журналів.

Процедура

Крок 1 Увійти на веб-сторінку.

Крок 2 Вибрати**Колода**>**Колода**.

Крок 3 Виберіть часовий діапазон та тип журналу, а потім натисніть**Пошук**.

Пов'язані операції

- натисніть**Експорт**для експорту журналів на локальний комп'ютер.
- Натисніть**Зашифрувати резервну копію журналу**, а потім введіть пароль. Експортований файл можна відкрити лише після введення пароля.
- Натисніть, щоб переглянути відомості про журнал.

3.14.2 Журнали адміністратора

Знайдіть журнали адміністратора за допомогою ідентифікатора адміністратора.

Процедура

Крок 1 Увійти на веб-сторінку. Вибрати

Крок 2 **Колода**>**Журнал адміністратора**.

Крок 3 Введіть ідентифікатор адміністратора та натисніть**Пошук**.

Натисніть**Експорт**для експорту журналів адміністратора.

3.14.3 Розблокування журналів

Знайдіть записи розблокування та експортуйте їх.

Процедура

Крок 1 Увійти на веб-сторінку. Вибрати**Колода**

Крок 2 >**Розблокувати записи**.

Крок 3 Виберіть тимчасовий діапазон і тип, а потім натисніть**Пошук**. Ви можете натиснути**Експорт**щоб завантажити журнал.

3.14.4 Журнали тривог

Перегляд журналів тривог.

Процедура

Крок 1 Увійти на веб-сторінку. Вибрати**Колода**>**Журнал тривог**

Крок 2 . Виберіть тип та часовий діапазон. Введіть

Крок 3 ідентифікатор адміністратора, а потім натисніть**Пошук**.

Крок 4

3.14.5 Журнали дзвінків

Перегляд журналів дзвінків.

Процедура

Крок 1 Увійти на веб-сторінку. Вибрати

Крок 2 **Колода**>**Історія дзвінків**.

3.14.6 Керування USB-пристроями

Експорт інформації про користувача з/на USB.

Процедура

Крок 1 Увійти на веб-сторінку. Вибрати

Крок 2 **Колода**>**USB-керування**.

- Перед експортом даних або оновити систему. Щоб уникнути збою, не витягуйте USB та не виконуйте жодних операцій Контролер доступу під час процесу.
- Вам необхідно використовувати USB для експорту інформації з контролера доступу до іншого пристрої. Зображення осіб не можна імпортувати через USB.

Крок 3 Виберіть тип даних, а потім натисніть**USB-імпорт**або**USB-експорт**імпортувати чи експортувати дані.

3.15 Місткість даних

Ви можете побачити, скільки користувачів, карт та зображень осіб може зберігати контролер доступу.

Увійдіть на веб-сторінку та виберіть**Місткість даних**.

3.16 Налаштування безпеки (необов'язково)

3.16.1 Статус безпеки

Скануйте користувачів, служби та модулі безпеки, щоб перевірити стан безпеки контролера доступу.

Довідкова інформація

- Виявлення користувачів та служб: перевірте, чи поточна конфігурація відповідає рекомендацій.
- Сканування модулів безпеки: сканування поточного стану модулів безпеки, таких як передача аудіо та відео, надійний захист, попередження про безпеку та захист від атак, а не визначення того, чи включені вони.

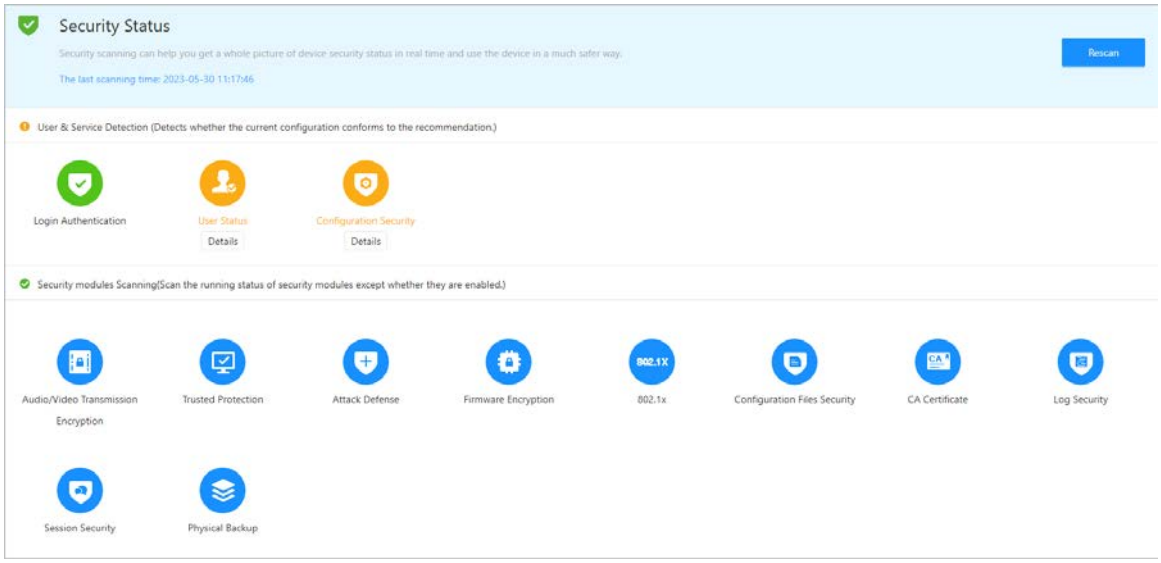
Процедура

Крок 1 Вибирати**Безпека**>**Статус безпеки**.

Крок 2 Натисніть**Повторне сканування**для сканування безпеки контролера доступу.

Наведіть курсор на піктограми модулів безпеки, щоб побачити їхній стан роботи.

Малюнок 3-57 Стан безпеки



Пов'язані операції

Після виконання сканування результати відображатимуться різними кольорами. Жовтий колір означає, що модулі безпеки несправні, а зелений колір означає, що модулі безпеки в нормі.

- Натисніть**Подробиці**для перегляду подробиць про результати сканування.
- Натисніть**Ігнорувати**ігнорувати аномалію, і вона не скануватиметься. Аномалія, яка була

проігноровані будуть виділені сірим кольором.

- Натисніть**Оптимізувати**для усунення несправності.

3.16.2 Налаштування HTTPS

Створіть сертифікат або завантажте автентифікований сертифікат, і тоді ви зможете увійти на веб-сайт сторінку через HTTPS на вашому комп'ютері. HTTPS захищає зв'язок через мережу комп'ютера.

Процедура

Крок 1 Вибирати**Безпека**>**Системна служба**>

Крок 2 **HTTPS**. Увімкніть HTTPS.

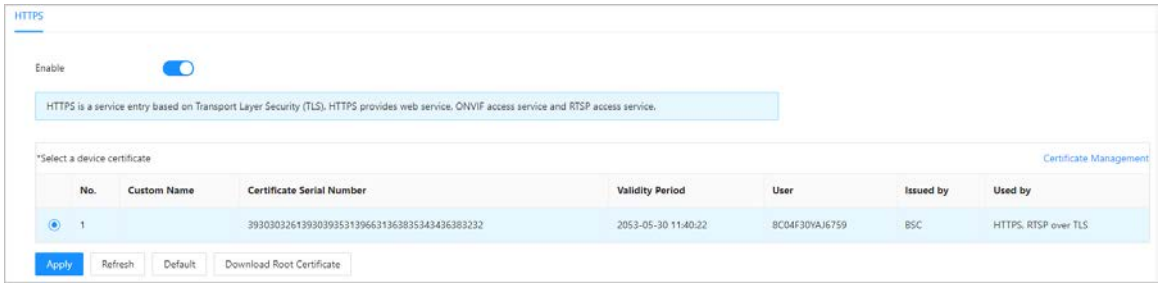
Якщо ви увімкнете сумісність з TLS v1.1 та попередніми версіями, можуть виникнути загрози безпеці.

Будь ласка, візьміть до уваги.

Крок 3 Виберіть сертифікат.

Якщо у списку немає сертифікатів, натисніть**Управління сертифікатами**для завантаження сертифіката.

Малюнок 3-58 HTTPS



Крок 4 Натисніть**Застосовувати**.

Введіть "https://"*IP-адреса*:*httpsпорт*" у веб-браузері. Якщо сертифікат встановлено, ви зможете успішно увійти на веб-сторінку. Якщо ні, веб-сторінка відобразить сертифікат як неправильний або ненадійний.

3.16.3 Атака та захист

3.16.3.1 Налаштування брандмауера

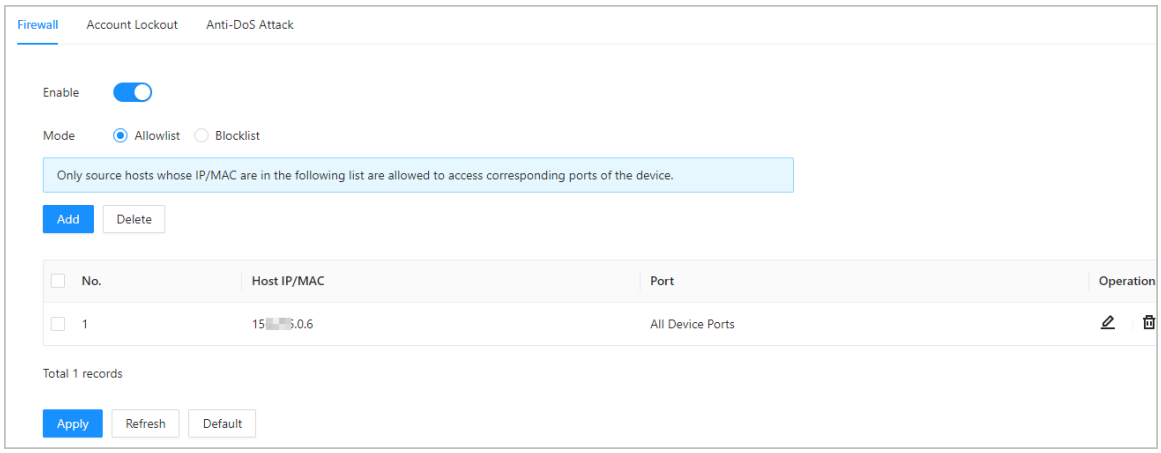
Налаштуйте брандмауер для обмеження доступу до контролера доступу.

Процедура

Крок 1 Вибирати**Безпека**>**Атака Захист**>**Брандмауер**.

Крок 2 Натисніть, щоб увімкнути брандмауер.

Малюнок 3-59 Брандмауер

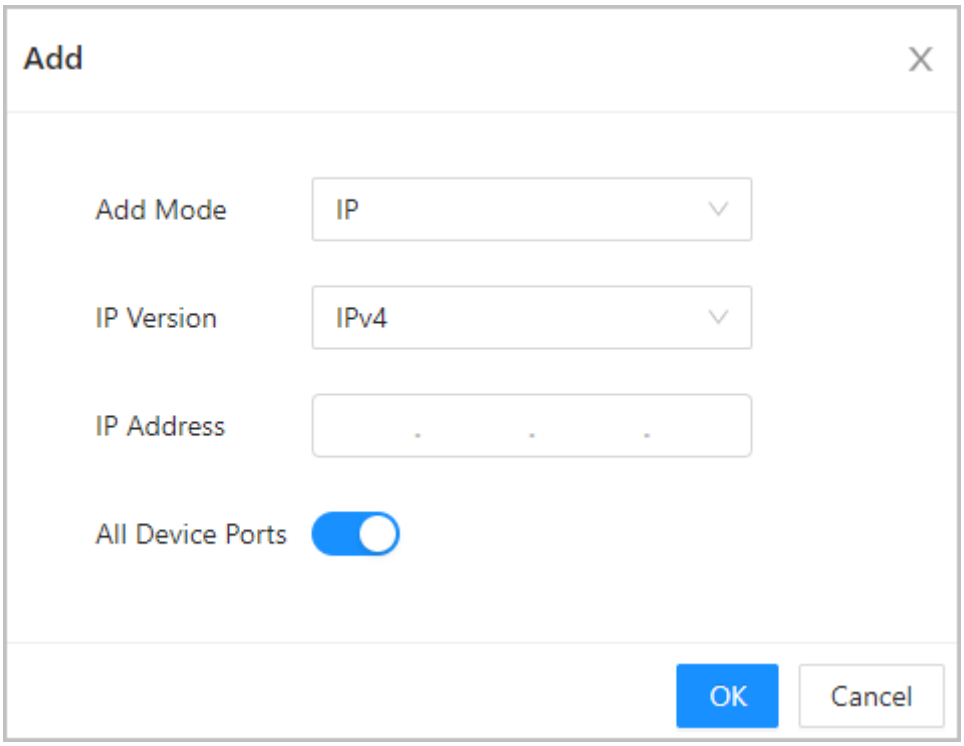


Крок 3 Виберіть режим:**Білий список**і**Чорний список**.

- **Білий список**: Доступ до контролера доступу можуть отримати лише IP/MAC-адреси з дозволеного списку.
- **Чорний список**: IP/MAC-адреси з чорного списку не можуть отримати доступ до контролера доступу.

Крок 4 Натисніть**Додавати**для введення інформації IP.

Малюнок 3-60 Додати інформацію про IP



Крок 5 Натисніть**ДОБРЕ**.

Пов'язані операції

- Натисніть для редагування інформації про
- Натисніть IP-адреса. для видалення IP-адреси.

3.16.3.2 Налаштування блокування облікового запису

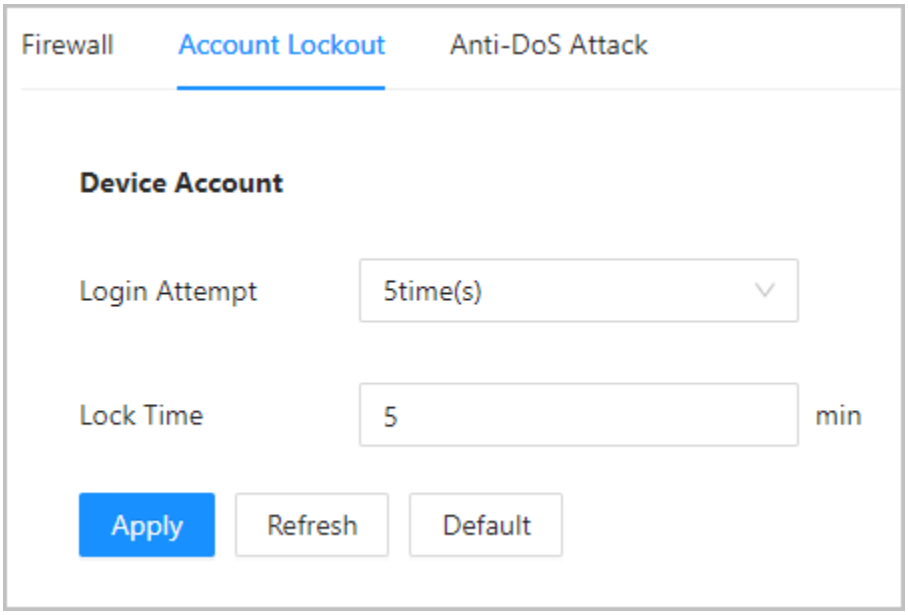
Якщо неправильний пароль буде введено кілька разів, обліковий запис буде заблоковано.

Процедура

Крок 1 Вибирати**Безпека**>**Атака Захист**>**Блокування облікового запису**.

Крок 2 Введіть кількість спроб входу в систему та час, на який буде заблоковано обліковий запис адміністратора та користувача ONVIF.

Малюнок 3-61 Блокування облікового запису



- Спроба входу: Ліміт спроб входу. Якщо неправильний пароль буде введено певне кількість разів, обліковий запис буде заблоковано.
- Час блокування: Інтервал, протягом якого ви не можете увійти до системи після блокування облікового запису.

Крок 3 Натисніть**Застосовувати**.

3.16.3.3 Налаштування захисту від DoS-атак

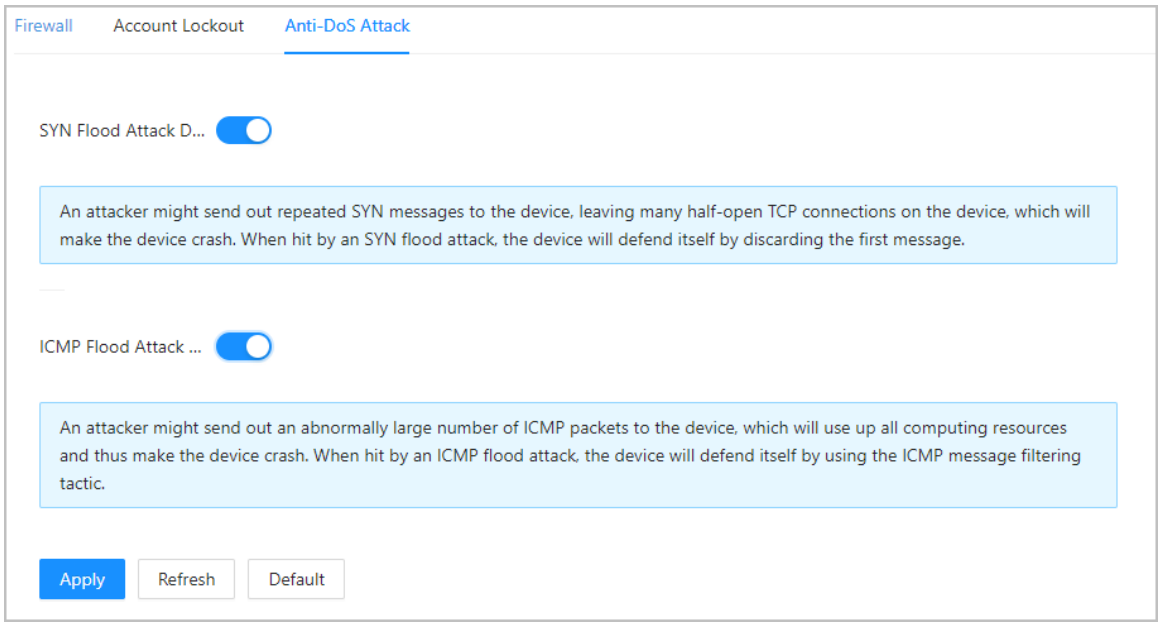
Ви можете увімкнути**Захист від атак SYN-потоку**і**Захист від атак ICMP Flood**для захисту контролера доступу від DoS-атак.

Процедура

Крок 1 Вибирати**Безпека**>**Атака Захист**>**Анти-DoS-атака**.

Крок 2 Вмикати**Захист від атак SYN-потоку**або**Захист від атак ICMP Flood**для захисту контролера доступу від DoS-атак.

Малюнок 3-62 Анти-DoS-атака



Крок 3 Натиснітьтаку.

3.16.4 Встановлення сертифіката пристрою

Створіть сертифікат або завантажте автентифікований сертифікат, після чого ви зможете увійти до системи через HTTPS на своєму комп'ютер.

3.16.4.1 Створення сертифіката

Створіть сертифікат для контролера доступу.

Процедура

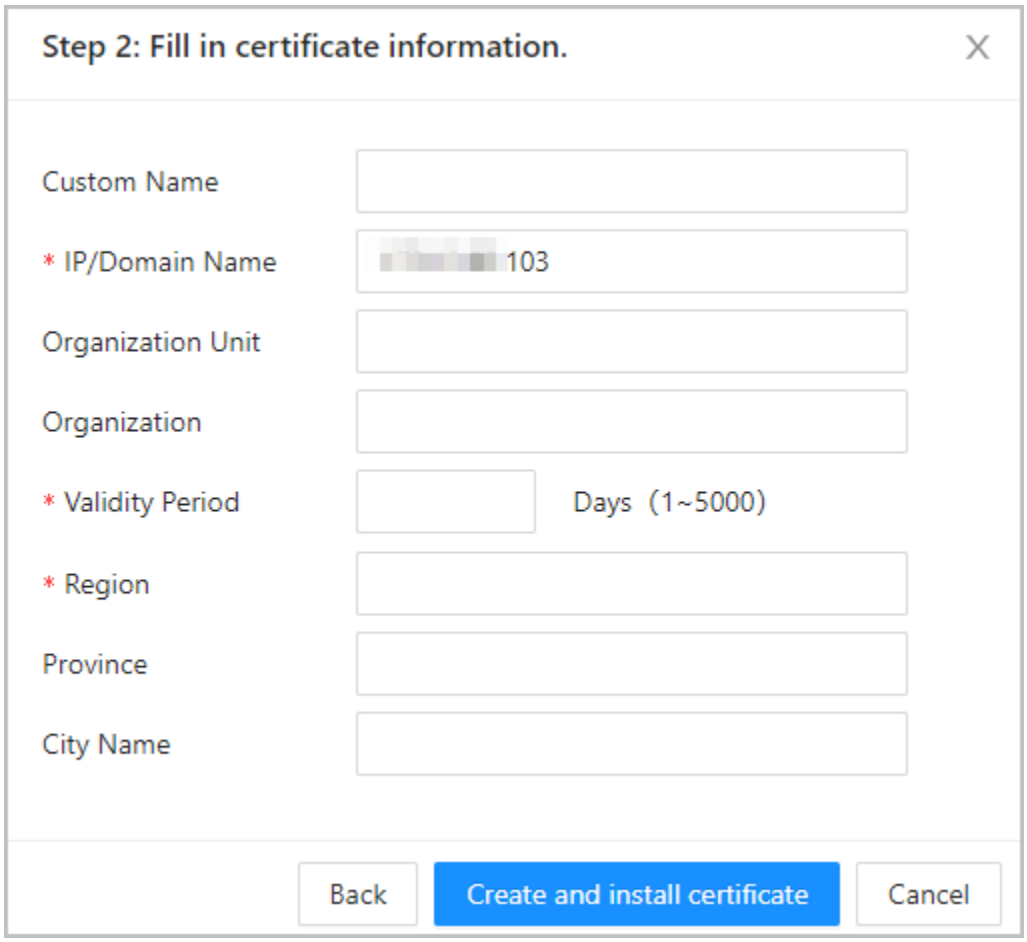
Крок 1 ВибиратиБезпека>Сертифікат CA>Сертифікат пристрою.

Крок 2 ВибиратиВстановити сертифікат пристрою. ВибиратиСтворити

Крок 3 сертифікатта натиснітьНаступний. Введіть інформацію про

Крок 4 сертифікат.

Малюнок 3-63 Інформація про сертифікат



Назва регіону не може перевищувати 2 символи. Рекомендуємо ввести абревіатуру від назви регіону.

Крок 5 Натисніть**Створити та встановити сертифікат**.

Нещодавно встановлений сертифікат відображається на**Сертифікат пристрою**сторінка після успішного встановлення сертифіката.

Пов'язані операції

- Натисніть**Увійти в режим редагування**на**Сертифікат пристрою**сторінка для редагування імені сертифіката.
- Натисніть завантажити сертифікат.
- Натисніть видалити сертифікат.

3.16.4.2 Подання заявки на отримання та імпорт сертифіката CA

Імпортуйте сертифікат стороннього центру сертифікації до контролера доступу.

Процедура

Крок 1 Вибирати**Безпека**>**Сертифікат CA**>**Сертифікат пристрою**. Натисніть

Крок 2 **Встановити сертифікат пристрою**.

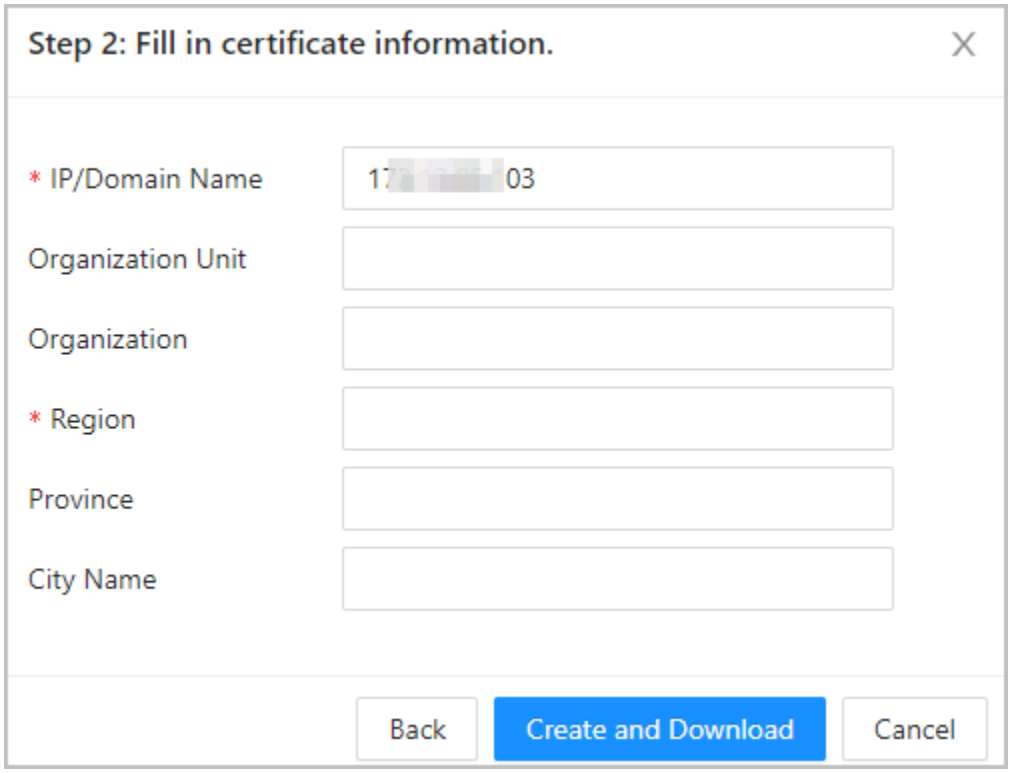
Крок 3 Вибирати**Подати заявку на отримання сертифіката CA та імпорт (рекомендується)**та натисніть**Наступний**.

Крок 4 Введіть інформацію про сертифікат.

- IP/доменне ім'я: IP-адреса або доменне ім'я контролера доступу.
- Регіон: Назва регіону не повинна перевищувати3 символи. Рекомендуємо ввести

абревіатура назви регіону.

Малюнок 3-64 Інформація про сертифікат (2)



Крок 5 Натисніть**Створити та завантажити**.

Збережіть файл запиту на комп'ютері.

Крок 6 Подайте заявку на сертифікат до стороннього центру сертифікації, використовуючи файл запиту. Імпортуйте

Крок 7 підписаний сертифікат центру сертифікації.

1) Збережіть сертифікат CA на своєму комп'ютері.

2) Клацніть**Встановлення сертифіката пристрою**.

3) Клацніть**Переглядати**для вибору сертифіката CA.

4) Клацніть**Імпорт та встановлення**.

Нещодавно встановлений сертифікат відображається на**Сертифікат пристрою**сторінка після успішного встановлення сертифіката.

- Натисніть**Відтворити**щоб наново створити файл запиту.
- Натисніть**Імпортувати пізніше**для імпорту сертифіката в інший час.

Пов'язані операції

- Натисніть**Увійти в режим редагування**на**Сертифікат пристрою**сторінка для редагування імені сертифіката.
- Натисніть завантажити сертифікат.
- Натисніть видалити сертифікат.

3.16.4.3 Встановлення існуючого сертифіката

Якщо у вас є файл сертифіката та закритого ключа, імпортуйте файл сертифіката та закритого ключа.

Процедура

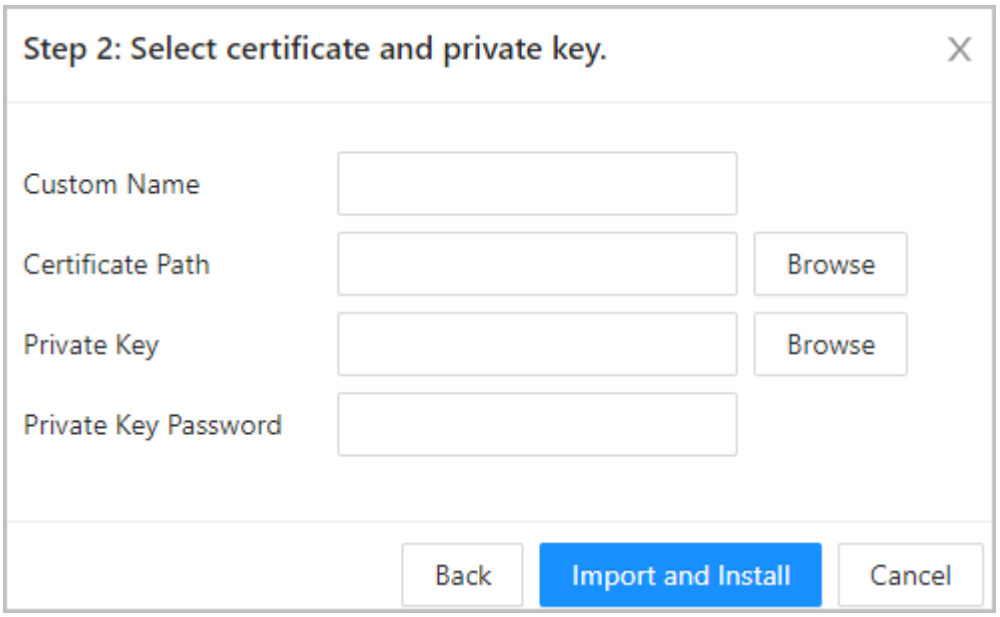
Крок 1 Вибирати**Безпека**>**Сертифікат CA**>**Сертифікат пристрою**. Натисніть

Крок 2 **Встановити сертифікат пристрою**.

Крок 3 Вибирати**Встановити існуючий сертифікат**та натисніть**Наступний**.

Крок 4 Натисніть**Переглядати**щоб вибрати файл сертифіката та закритого ключа, а також ввести пароль закритий ключ.

Малюнок 3-65 Сертифікат та закритий ключ



Крок 5 Натисніть**Імпорт та встановлення**.

Нещодавно встановлений сертифікат відображається на**Сертифікат пристрою**сторінка після успішного встановлення сертифіката.

Пов'язані операції

- Натисніть**Увійти в режим редагування**на**Сертифікат пристрою**сторінка для редагування імені сертифіката.
- Натисніть завантажити сертифікат.
- Натисніть видалити сертифікат.

3.16.5 Встановлення довіреного сертифіката CA

Довірений сертифікат CA — це цифровий сертифікат, який використовується для автентифікації веб-сайтів і серверів. Наприклад, при використанні протоколу 802.1x сертифікат CA для комутаторів потрібний для автентифікації його справжності.

Довідкова інформація

802.1X — це протокол мережної автентифікації, який відкриває порти для доступу до мережі, коли організація перевіряє справжність особи користувача дозволяє йому доступом до мережі.

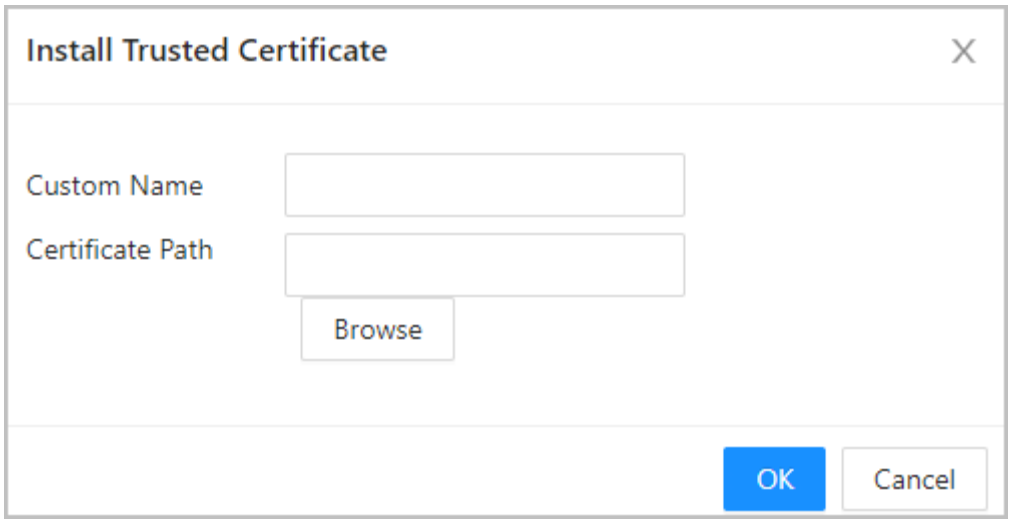
Процедура

Крок 1 Вибирати**Безпека**>**Сертифікат CA**>**Довірені сертифікати CA**.

Крок 2 Вибирати**Встановити довірений сертифікат**.

Крок 3 Натисніть**Переглядати**вибір довіреного сертифіката.

Малюнок 3-66 Встановлення довіреного сертифіката



Крок 4 Натиснітьдобре.

Нещодавно встановлений сертифікат відображається на**Довірені сертифікати СА**сторінка після успішного встановлення сертифіката.

Пов'язані операції

- Натисніть**Увійти в режим редагування**на**Сертифікат пристрою**сторінка для редагування імені сертифіката.
- Натисніть завантажити сертифікат.
- Натисніть видалити сертифікат.

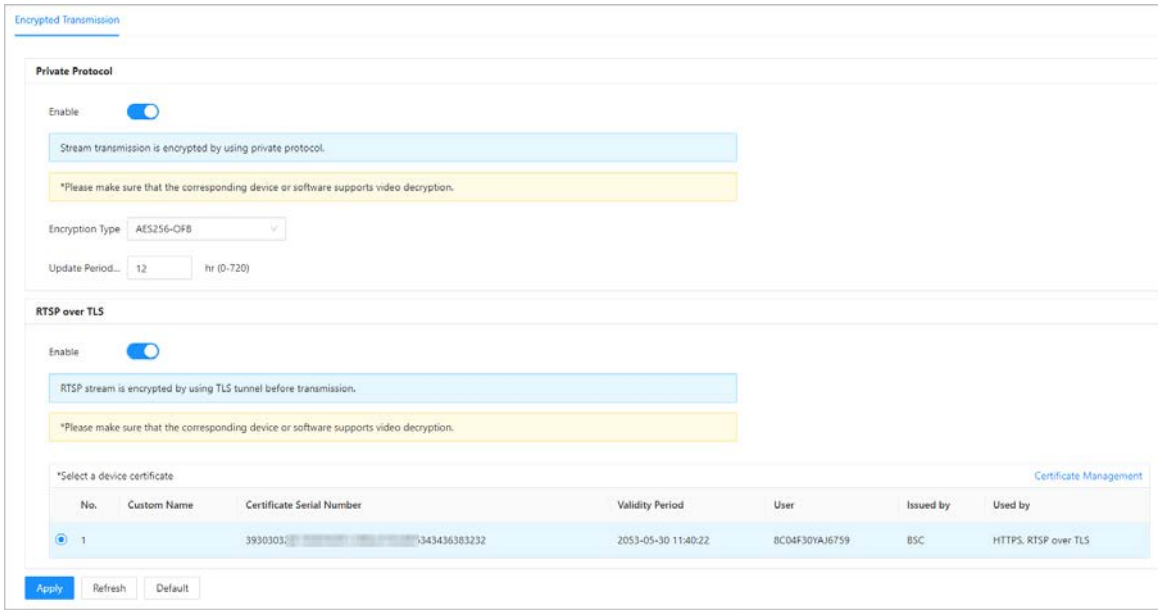
3.16.6 Шифрування даних

Процедура

Крок 1 Вибирати**Безпека**>**Шифрування**

Крок 2 **даних**. Налаштуйте параметри.

Малюнок 3-67 Шифрування даних



Таблиця 3-36 Опис шифрування даних

	Параметр	Опис
Приватний протокол	Давати можливість	Потоки шифруються під час передачі за закритим протоколом.
	Тип шифрування	Залишіть його за промовчанням.
	Період оновлення Секретний ключ	Діапазон значень: 0 год - 720 год. 0 означає, що секретний ключ ніколи не оновлюється.
RTSP через TLS	Давати можливість	Потік RTSP шифрується під час передачі через тунель TLS.
	Сертифікат Управління	Створити чи імпортувати сертифікат. Подробиці див. у розділі "3.16.4 Встановлення сертифіката пристрою". Встановлені сертифікати відображаються у списку.

3.16.7 Попередження про безпеку

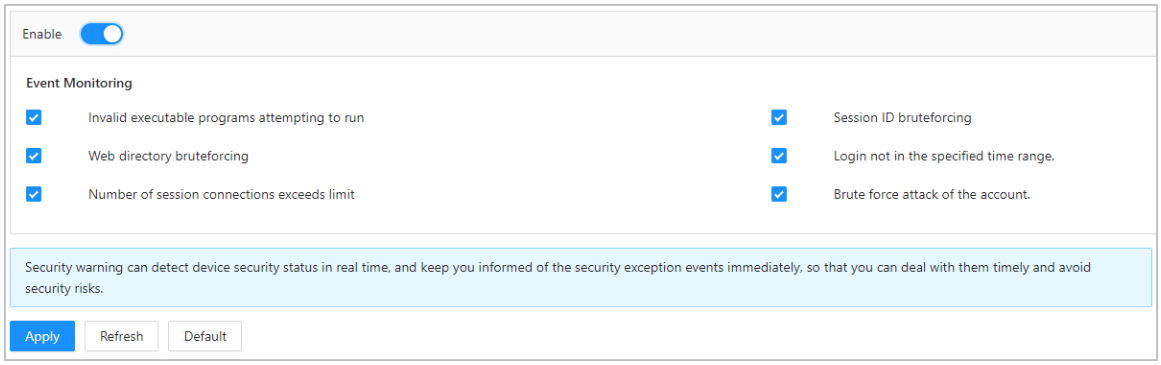
Процедура

Крок 1 Вибирати**Безпека**>**Попередження про**

Крок 2 **безпеки**. Увімкнути функцію попередження

Крок 3 безпеки. Виберіть елементи моніторингу.

Малюнок 3-68 Попередження безпеки



Крок 4 Натиснітьзастосовувати.

4. Спрощена конфігурація Smart PSS

У цьому розділі описано, як керувати та налаштовувати контролер доступу через Smart PSS Lite.

Докладнішу інформацію див. у посібнику користувача Smart PSS Lite.

4.1 Встановлення та вхід до системи

Встановіть та увійдіть до Smart PSS Lite. Докладнішу інформацію див. у посібнику користувача Smart PSS Lite.

Процедура

Крок 1 Отримайте пакет програмного забезпечення Smart PSS Lite у службі технічної підтримки, а потім установіть та запустіть програмне забезпечення згідно з інструкціями.

Крок 2 Під час першого входу в систему виконайте ініціалізацію Smart PSS Lite, включаючи встановлення пароля та контрольних питань.

Встановіть пароль для першого використання, а потім поставте контрольні питання, щоб скинути пароль.

пароль, якщо ви забули його.

Крок 3 Введіть ім'я користувача та пароль для входу до Smart PSS Lite.

4.2 Додавання пристроїв

Вам необхідно додати контролер доступу до Smart PSS Lite. Ви можете додавати їх партіями або по окремо.

4.2.1 Додавання по одному

Ви можете додавати контролери доступу по одному, вводячи IP-адреси або доменні імена.

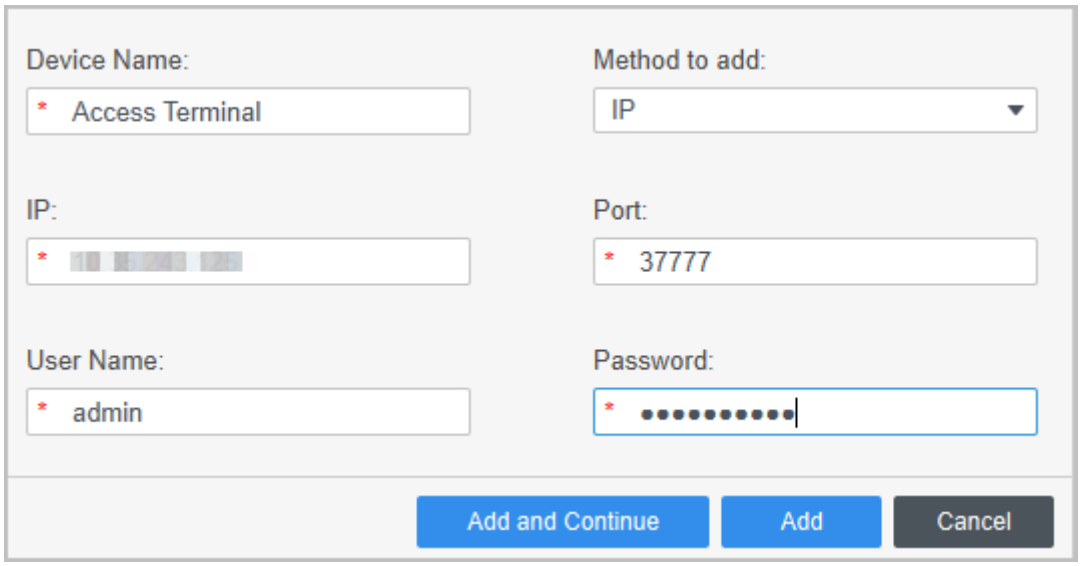
Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 Натисніть**Диспетчер пристроїв**та натисніть**Додавати**.

Крок 3 Введіть інформацію про пристрій.

Малюнок 4-1 Інформація про пристрій



Таблиця 4-1 Опис параметрів пристрою

Параметр	Опис
Ім'я пристрою	Введіть ім'я контролера доступу. Ми рекомендуємо назвати його за місцем встановлення.
Метод додавання	Вибирати**IC**щоб додати термінал доступу, ввівши його IP-адресу.
IC	Введіть IP-адресу контролера доступу.
Порт	Номер порту за замовчуванням – 37777.
Ім'я користувача/Пароль	Введіть ім'я користувача та пароль терміналу доступу.

Крок 4 Натисніть**Додавати**.

Доданий контролер доступу відображається на**Пристрої**сторінку. Ви можете натиснути**Додати та продовжити** додавання додаткових контролерів доступу.

4.2.2 Додавання партіями

Ми рекомендуємо використовувати функцію автопошуку, коли ви додаєте контролери доступу партіями. Переконайтеся, що контролери доступу, які ви додаєте, повинні знаходитися в одному сегменті мережі.

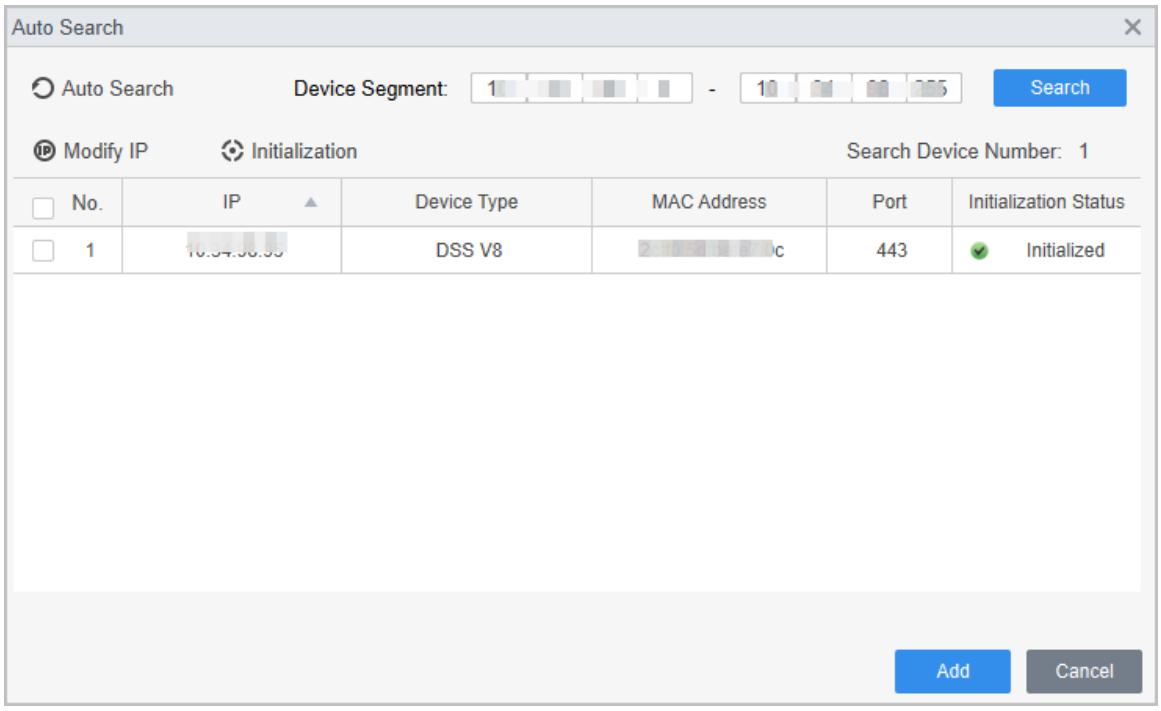
Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 Натисніть**Диспетчер пристроїв**та пошук пристроїв.

- Натисніть**Автоматичний пошук**, щоб знайти пристрої в тій же локальній мережі.
- Введіть діапазон сегмента мережі, а потім натисніть**Пошук**.

Малюнок 4-2 Автоматичний пошук



Буде відображено список пристроїв.

Виберіть пристрій та натисніть**Змінити IP-адресу**змінити свою IP-адресу.

Крок 3 Виберіть контролер доступу, який потрібно додати до Smart PSS Lite, а потім натисніть

Крок 4 **Додавати**. Введіть ім'я користувача та пароль контролера доступу.

Ви можете переглянути доданий контролер доступу на**Пристрої**сторінка.

Контролер доступу автоматично входить до Smart PSS Lite після додавання.**Онлайн**є відображається після успішного входу до системи.

4.3 Керування користувачами

Додайте користувачів, призначте їм карти та налаштуйте їх права доступу.

4.3.1 Налаштування типу картки

Встановіть тип картки, перш ніж призначати карти користувачам. Наприклад, якщо призначена картка — це посвідчення особи, встановіть тип картки на посвідчення особи.

Процедура

Крок 1 Увійдіть до Smart PSS Lite.

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

Крок 3 **Користувач**. на**Тип випуску картки**а потім виберіть тип картки.

Переконайтеся, що тип картки збігається з фактично призначеною карткою; в іншому випадку карта Номер не може бути прочитаний.

Крок 4 Натисніть**ДОБРЕ**.

4.3.2 Додавання користувачів

4.3.2.1 Додавання по одному

Ви можете додавати користувачів по одному.

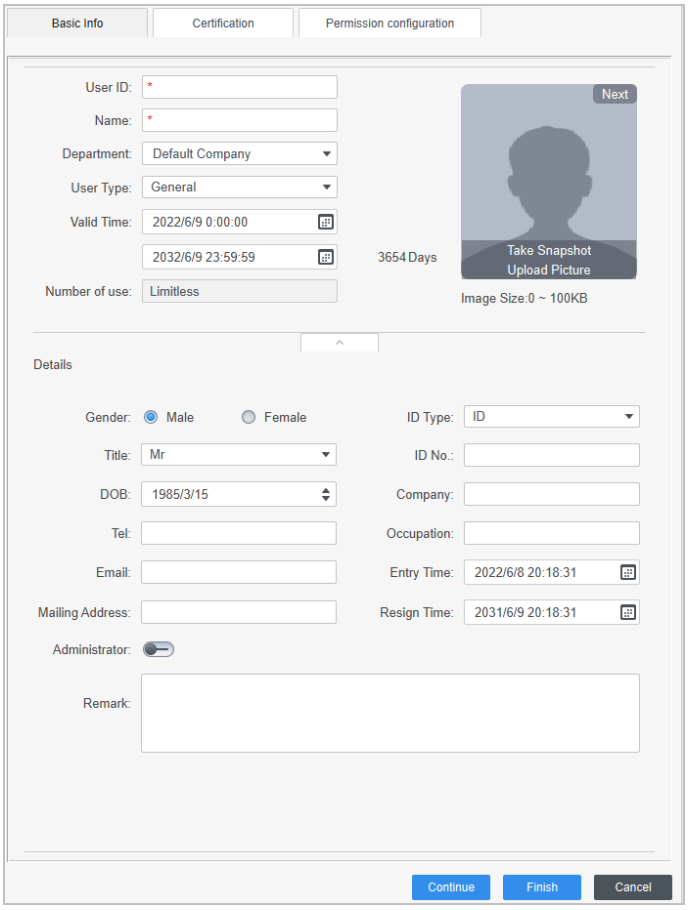
Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 Натисніть**Доступ до рішення**>**Менеджер з персоналу**>**Користувач**>**Додавати**.

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

Малюнок 4-3 Додати основну інформацію



Крок 4 Натисніть на**Сертифікація**вкладка, щоб додати інформацію про сертифікацію користувача.

- Налаштуйте пароль: Пароль повинен складатися з6-8 цифр.
- Налаштуйте картку: Номер картки може бути рахований автоматично або введений вручну. Щоб автоматично рахувати номер картки, виберіть пристрій для зчитування карт, а потім помістіть картку в пристрій зчитування карток.

  1. На**Картка**область, клацніть та виберіть**Емітент карти**, а потім натисніть**ДОБРЕ**.

2. Натисніть**Додавати**, проведіть карткою по зчитувачу карток. Відобразиться номер картки.

3. Натисніть**ДОБРЕ**.

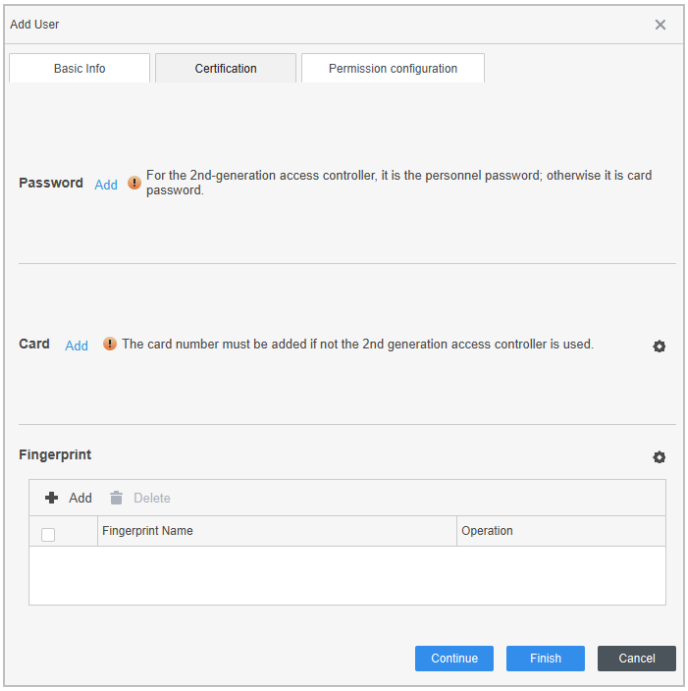
Після додавання картки ви можете зробити її основною або примусовою карткою, замінити картку на нову або видалити картку.

- Налаштуйте відбиток пальця.

1. На**Відбиток пальця**область, клацніть та виберіть**Сканер відбитків пальців**, а потім натисніть**ДОБРЕ**.

2. Натисніть**Додати відбиток пальця**натисніть пальцем на сканер тричі поспіль.

Малюнок 4-4 Додати пароль, карту та відбиток пальця



Крок 5 Налаштуйте дозволи користувача. Докладніше див. у розділі "4.3.3 Призначення дозволу на доступ". Натисніть

Крок 6 **Закінчувати**.

4.3.2.2 Додавання партіями

Ви можете додавати користувачів партіями.

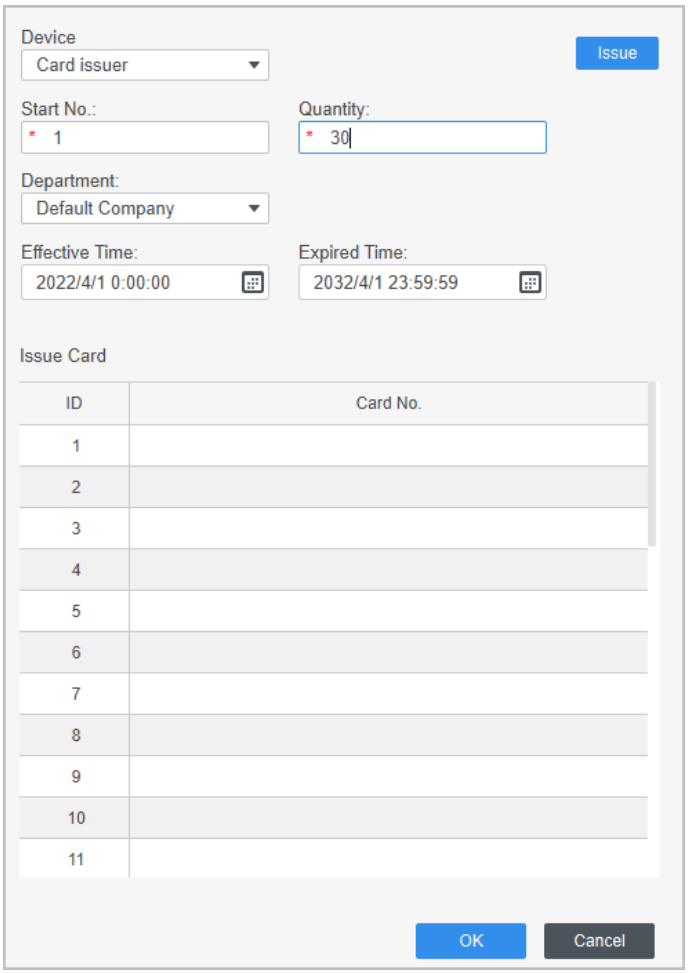
Процедура

Крок 1 Увійдіть до Smart PSS Lite.

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

Крок 3 Вибирати**Емітент карти**з**Пристрій**список, а потім налаштуйте параметри.

Рисунок 4-5 Додавання користувачів партіями



Таблиця 4-2 Параметри додавання користувачів до пакетів

Параметр	Опис
Стартовий номер	Ідентифікатор користувача починається із зазначеного вами числа.
Кількість	Кількість користувачів, яких потрібно додати.
Відділення	Виберіть відділ, до якого належить користувач.
Ефективний час / час, що минув	Користувачі можуть розблокувати двері протягом певного періоду часу.

Крок 4 Натисніть**Проблема**.

Номер картки буде рахований автоматично. Натисніть

Крок 5 **ДОБРЕ**.

Крок 6 на**Користувач**сторінка, натисніть для заповнення інформації про користувача.

4.3.3 Призначення дозволу на доступ

Створіть групу дозволів, яка є набором дозволів на доступ до дверей, а потім зв'яжіть користувачів з групою, щоб вони могли відчиняти відповідні двері.

Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 Натисніть**Доступ до рішення**>**Менеджер з персоналу**>**Конфігурація дозволів**

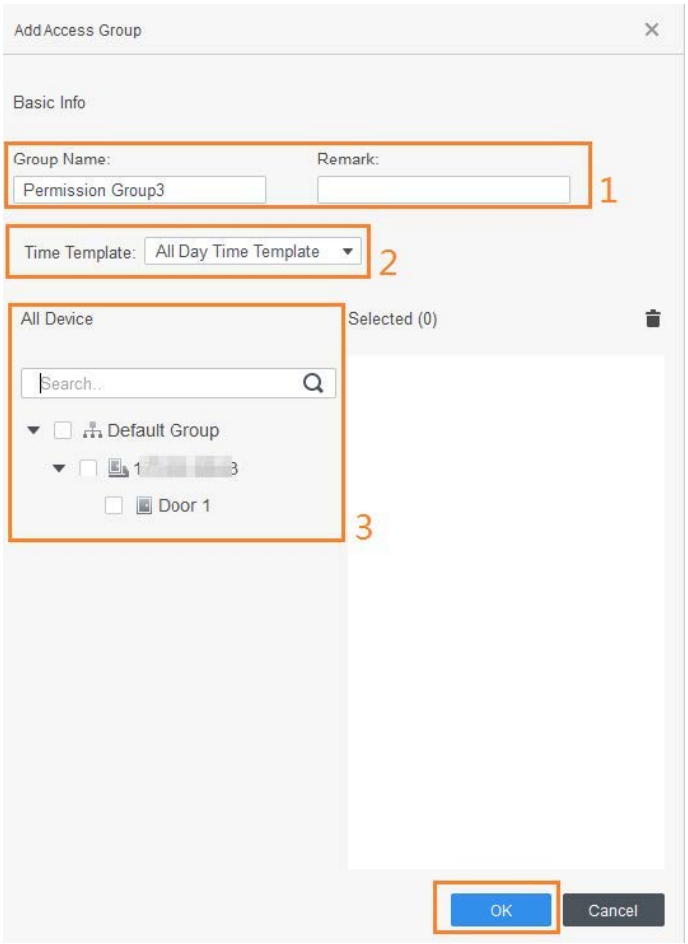
Крок 3 Натисніть кнопку .

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

Крок 5 Виберіть пристрій контролю доступу.

Крок 6 Натисніть**ДОБРЕ**.

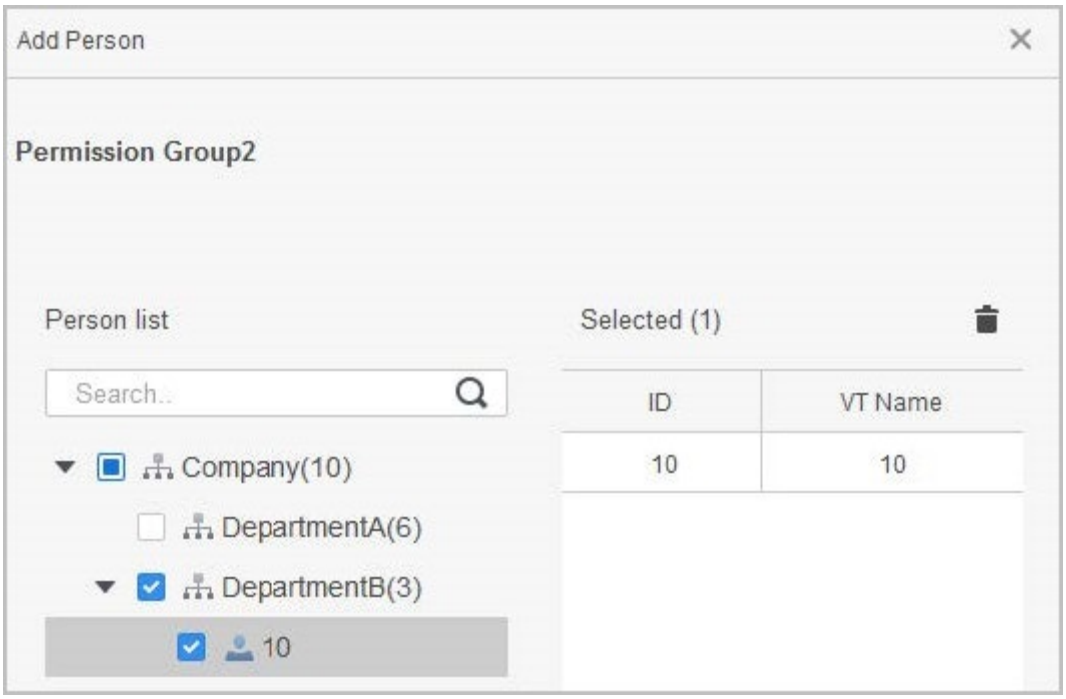
Малюнок 4-6 Створення групи дозволів



Крок 7 Натисніть доданої вами групи дозволів.

Крок 8 Виберіть користувачів, щоб зв'язати їх із групою дозволів.

Рисунок 4-7 Додавання користувачів до групи дозволів



Крок 9 Натисніть**ДОБРЕ**.

Користувачі групи дозволів можуть розблокувати двері після дійсної перевірки особи.

4.3.4 Призначення дозволів на відвідування

Створіть групу дозволів, яка є набором дозволів на відвідування робочого часу, а потім зв'яжіть працівників з цією групою, щоб вони могли відзначати прихід/догляд з роботи за допомогою певних методів перевірки.

Процедура

Крок 1 Увійдіть до Smart PSS Lite.

Крок 2 Натисніть**Доступ до рішення**>**Менеджер з персоналу**>**Конфігурація дозволів**

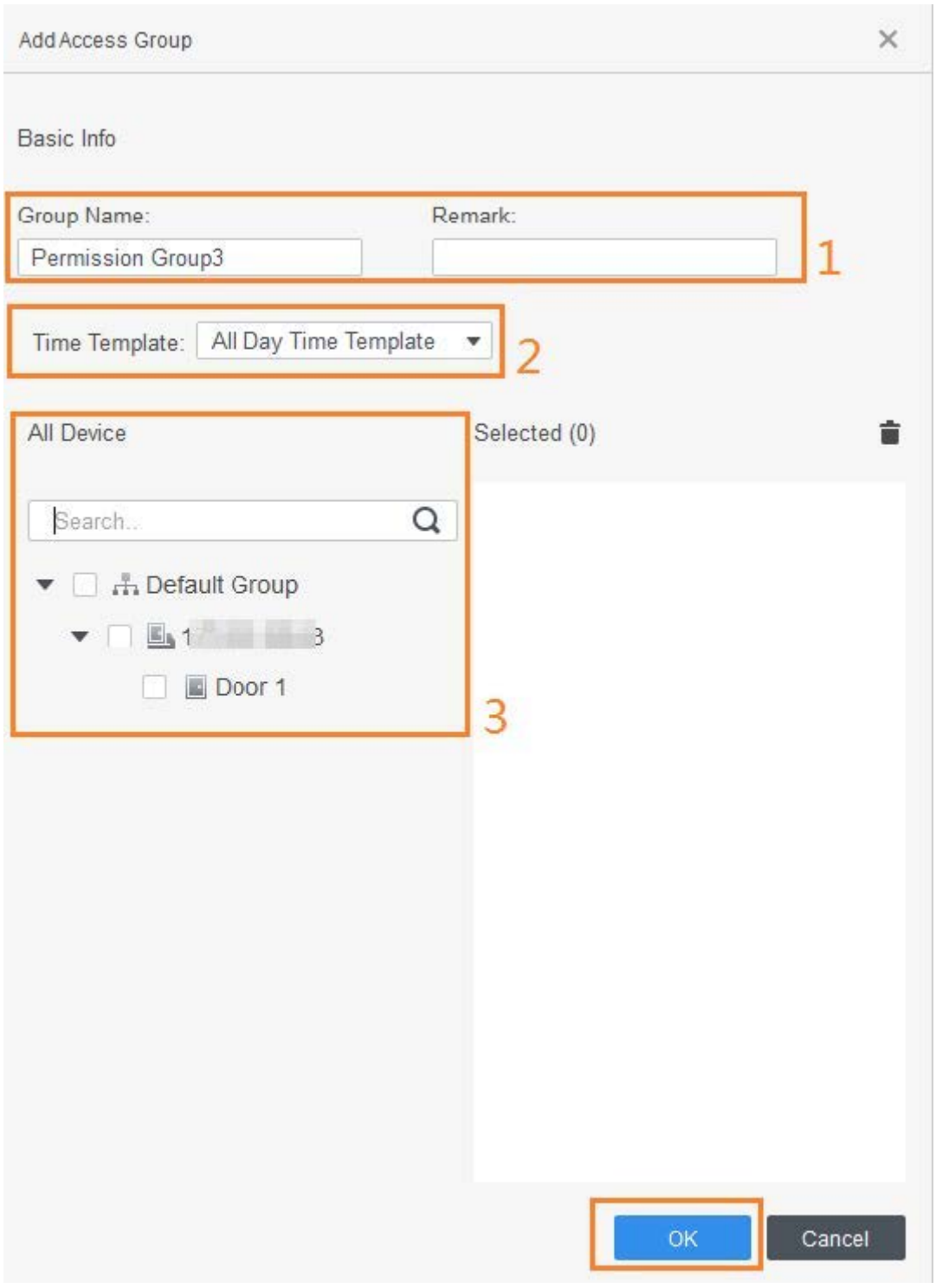
Крок 3 Натисніть кнопку .

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

Крок 5 Виберіть пристрій контролю доступу.

Крок 6 Натисніть**ДОБРЕ**.

Малюнок 4-8 Створення групи дозволів



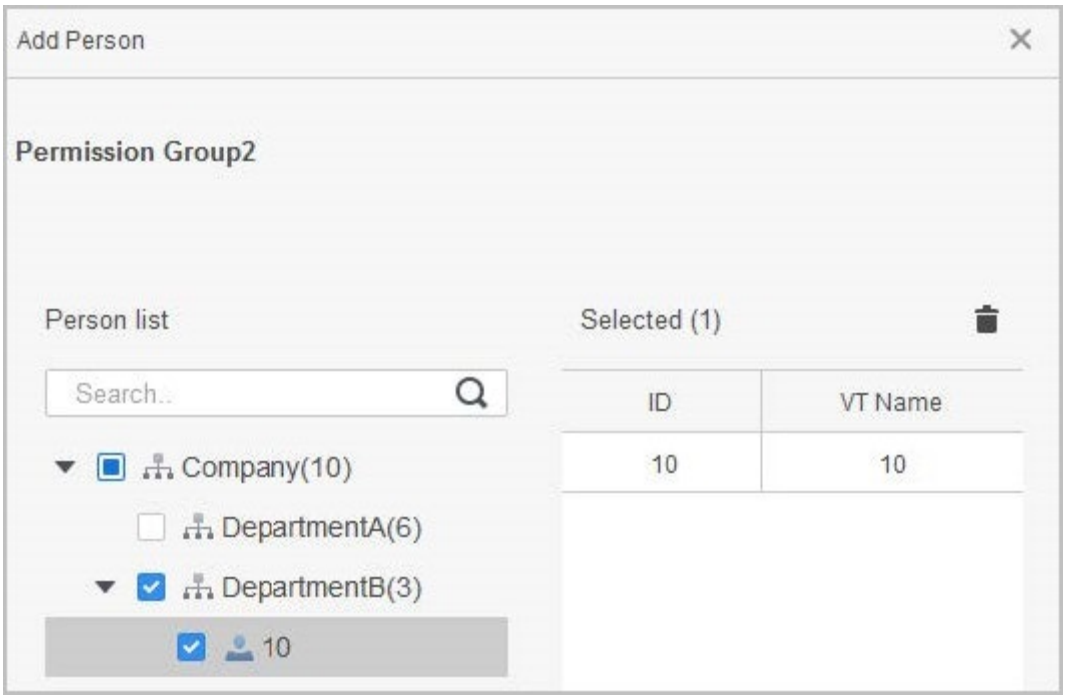
Система обліку робочого часу підтримує лише вхід/вихід за допомогою пароля та розпізнавання обличчя.

відвідуваність.

Крок 7 Натисніть доданої вами групи дозволів.

Крок 8 Виберіть користувачів, щоб зв'язати їх із групою дозволів.

Рисунок 4-9 Додавання користувачів до групи дозволів



Крок 9 Натисніть**ДОБРЕ**.

4.4 Управління доступом

4.4.1 Дистанційне відкриття та закриття дверей

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

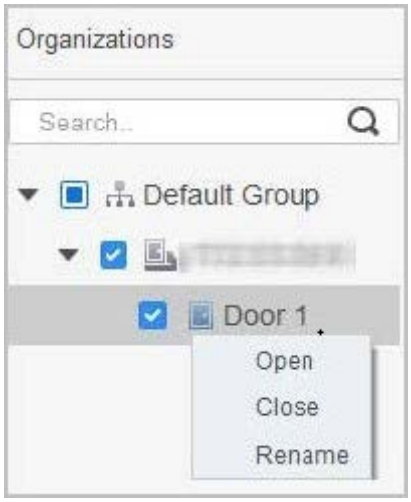
Процедура

Крок 1 Натисніть**Доступ до рішення**>**Менеджер доступу**на головній сторінці.

Крок 2 Віддалене керування дверима.

- Виберіть двері, клацніть правою кнопкою миші та виберіть**Відкрити**або**Закривати**.

Малюнок 4-10 Відчинені двері



- Натисніть або , щоб відкрити або закрити двері.

Пов'язані операції

- Фільтрування подій: виберіть тип події в**Інформація про подію**, а у списку подій відображається вибраний тип подій, наприклад, тривожні події та аномальні події.
- Блокування оновлень подій: Натисніть, щоб заблокувати список подій, після чого список подій перестане оновлюватися. Натисніть щоб розблокувати.
- Видалення події: Натисніть, щоб очистити всі події у списку подій.

4.4.2 Налаштування «Завжди відкрито» та «Завжди закрито»

Після встановлення "Завжди відкрито" або "Завжди закрито" двері залишаються відкритими або закритими весь час.

Процедура

Крок 1 Натисніть**Доступ до рішення**>**Менеджер доступу**на головній сторінці. Натисніть

Крок 2 **Завжди відкрито**або**Завжди близько**щоб відкрити або зачинити двері.

Малюнок 4-11 Завжди відкрито чи закрито

Двері будуть залишатися відкритими або закритими весь час. Ви можете натиснути**Нормальний**для відновлення нормального стану контролю доступу, після чого двері будуть відчинені або зачинені в Залежно від налаштованих методів перевірки.

4.4.3 Моніторинг стану дверей

Процедура

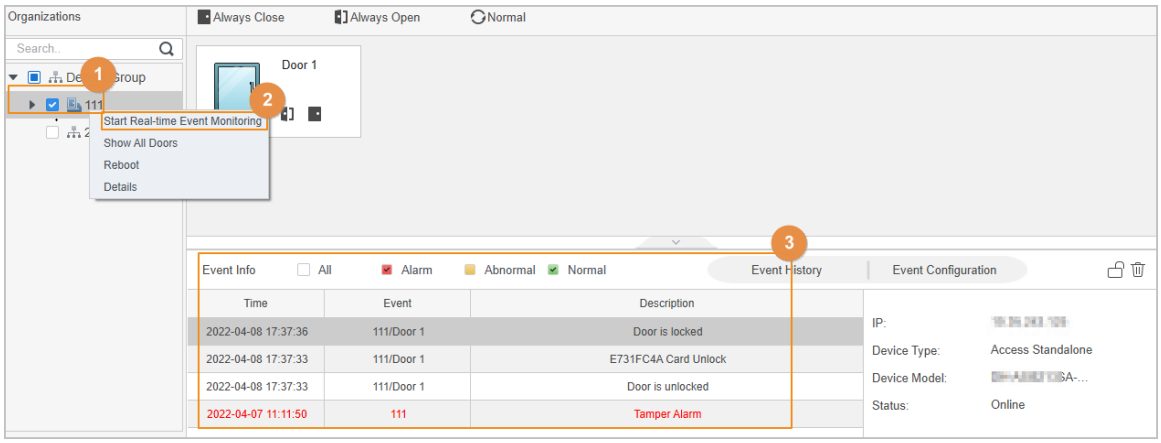
Крок 1 Натисніть**Доступ до рішення**>**Менеджер доступу**на головній сторінці.

Крок 2 Виберіть контролер доступу у дереві пристроїв, клацніть правою кнопкою миші контролер доступу та виберіть **Розпочати моніторинг подій у реальному часі**.

Події контролю доступу в реальному часі відображатимуться у списку подій.

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

Малюнок 4-12 Стан дверей монітора



Пов'язані операції

- Показати всі двері: відображає всі двері, які контролює контролер доступу.
- Перезавантаження: перезапустіть контролер доступу.
- Подробиці: переглянути відомості про пристрій, наприкладIP-адреса, модель та статус.

Додаток 1. Важливі моменти особи

Реєстрація

Перед реєстрацією

- Окуляри, капелюхи та бороди можуть вплинути на ефективність розпізнавання осіб.
- Не закривайте брови, надягаючи капелюх.
- Не змінюйте стиль бороди, якщо використовуєте контролер доступу, інакше розпізнавання обличчя може виявитися неможливим.
- Тримайте обличчя у чистоті.
- Розташовуйте контролер доступу на відстані щонайменше2 метри від джерела світла і не менше 3 метрів від вікон або дверей; в іншому випадку підсвічування та прямі сонячні промені можуть вплинути на ефективність розпізнавання облич контролером доступу.

Під час реєстрації

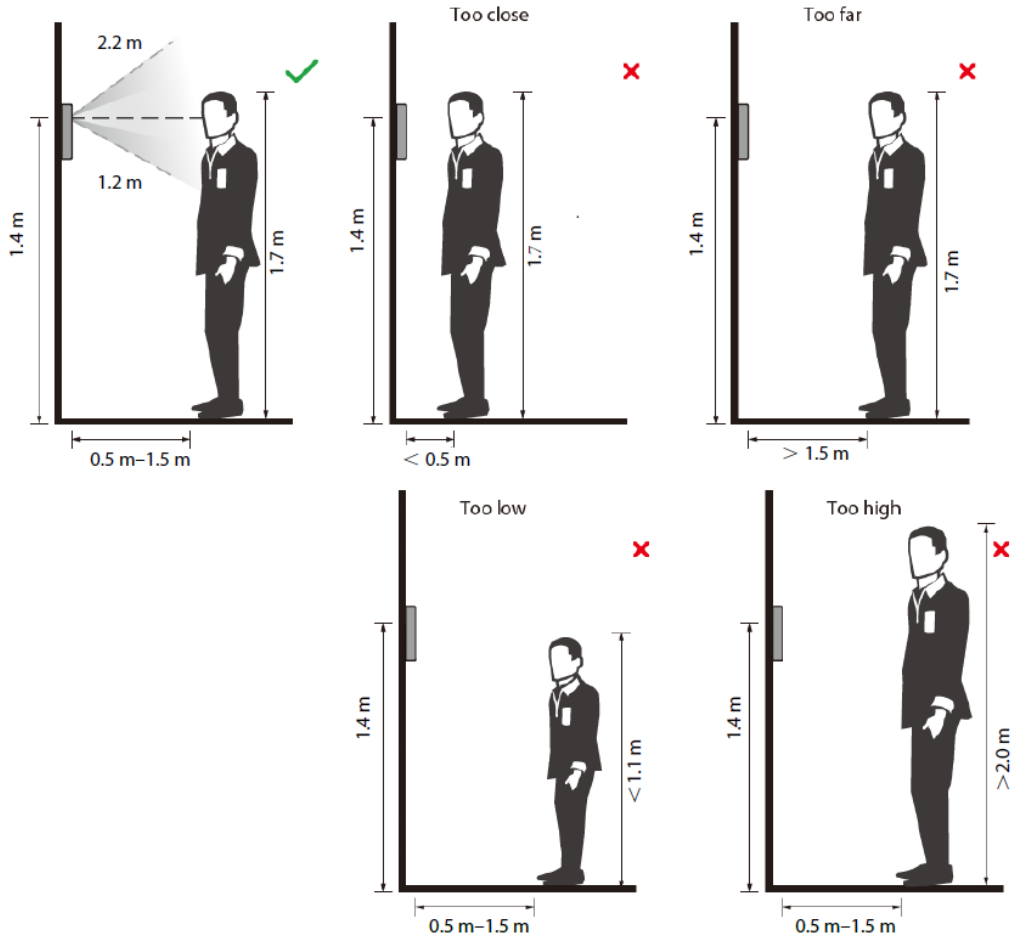
- Ви можете реєструвати особи через контролер доступу або через платформу. Для реєстрації через платформу див. посібник користувача платформи.
- Помістіть голову до центру фотозйомки. Зображення обличчя буде захоплено автоматично.

- Не трясіть головою і тілом, інакше реєстрація може бути не вдалася.
- Уникайте одночасної появи у кадрі двох осіб.

Положення особи

Якщо ваша особа знаходиться в неправильному положенні, точність розпізнавання обличчя може бути знижена.

Додаток Малюнок 1-1 Відповідне положення особи



Вимоги до осіб

- Переконайтеся, що обличчя чисте та чоло не закрите волоссям.
- Не надягайте окуляри, капелюхи, густу бороду або інші прикраси на обличчі, які можуть вплинути на запис зображення обличчя.
- З відкритими очима, без обличчя, поверніть обличчя до центру камери.
- Під час запису вашої особи або під час розпізнавання облич не тримайте обличчя надто близько або надто далеко від камери.

Додаток Малюнок 1-2 Положення голови

Додаток Малюнок 1-3 Відстань до особи

- При імпорті зображень осіб через платформу керування переконайтеся, що зображення роздільна здатність в діапазоні 150 × 300 пікселів – 600 × 1200 пікселів; пікселі зображення понад 500 × 500 пікселів; розмір зображення менше 100 КБ, ім'я зображення та ідентифікатор людини збігаються.
- Переконайтеся, що особа займає більше 1/3, але не більше 2/3 усієї площі зображення, та співвідношення сторін не перевищує 1:2.

Додаток 2. Важливі моменти внутрішнього зв'язку

Операція

Контролер доступу може функціонувати як VTO для реалізації функції домофону.

Передумови

Функція внутрішнього зв'язку налаштовується на контролері доступу та VTO.

Процедура

Крок 1 На екрані очікування натисніть «Введіть.

Крок 2 номер кімнати», а потім натисніть .

Додаток 3. Важливі моменти відбитків пальців

Інструкції з реєстрації

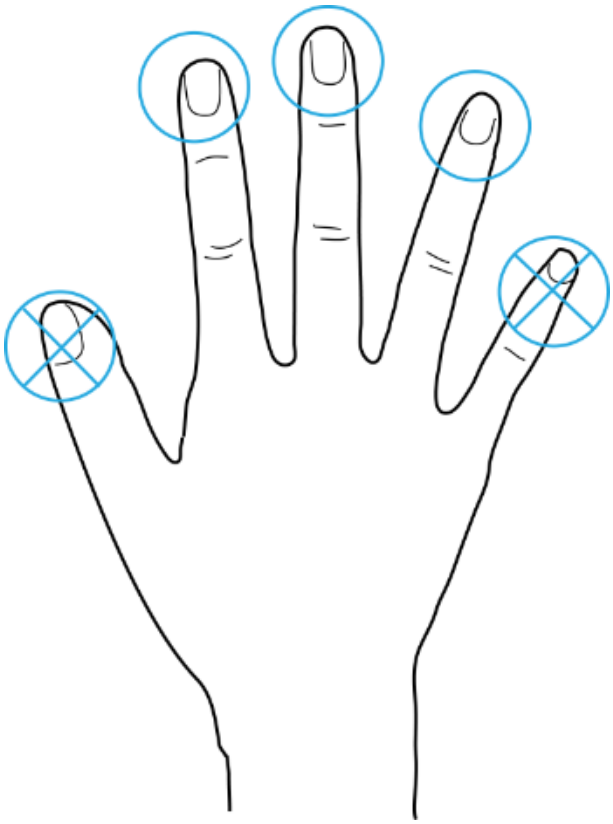
При реєстрації відбитка пальця зверніть увагу на такі моменти:

- Переконайтеся, що ваші пальці та поверхня сканера чисті та сухі.
- Натисніть пальцем на центр сканера відбитків пальців.
- Не розміщуйте сканер відбитків пальців у місцях з яскравим освітленням, високою температурою та високою вологістю.
- Якщо ваші відбитки пальців нечіткі, скористайтеся іншими способами розблокування.

Пальці рекомендуються

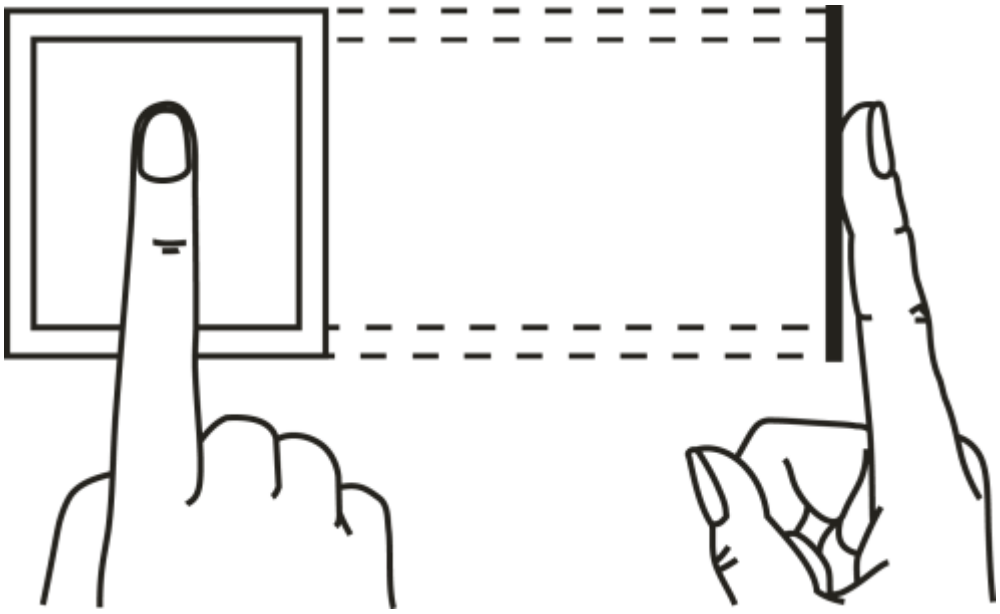
Рекомендуються вказівні, середні та безіменні пальці. Великі пальці та мізинці не можуть бути легко поміщені до центру запису.

Додаток Малюнок 3-1 Рекомендовані пальці

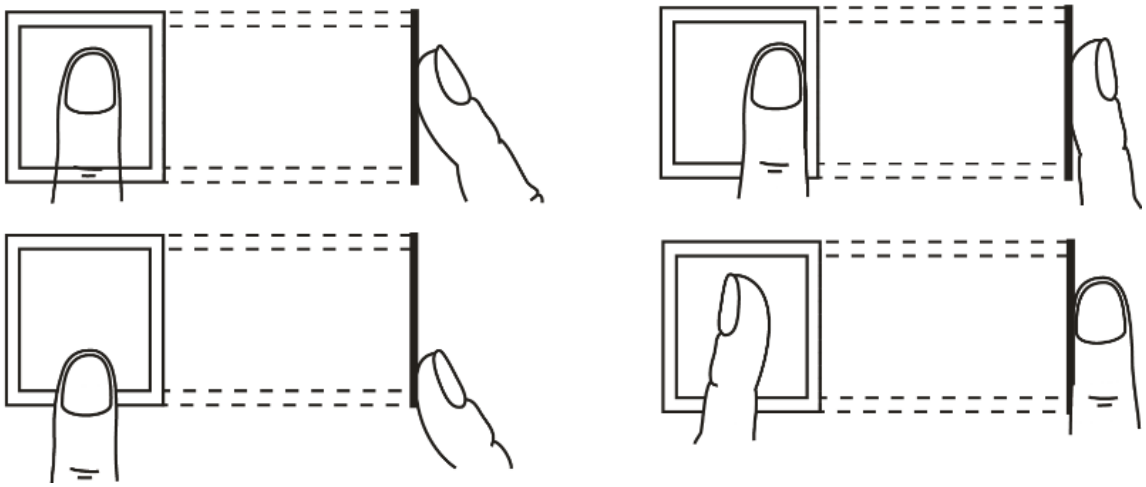


Як прикласти відбиток пальця до сканера

Додаток Малюнок 3-2 Правильне розміщення



Додаток Малюнок 3-3 Неправильне розміщення



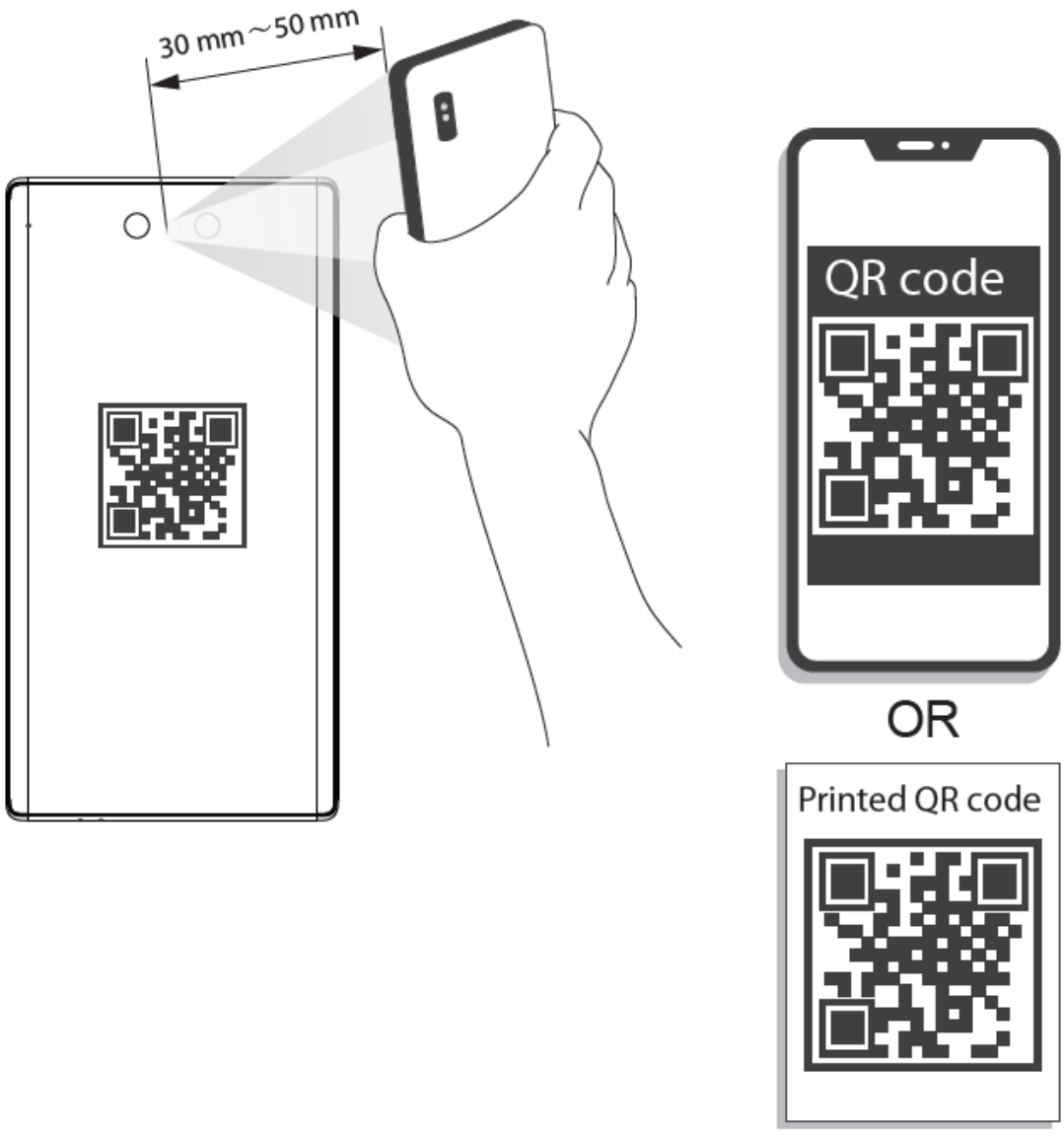
Додаток 4. Важливі моменти QR-коду

Сканування

Контролер доступу: Розмістіть QR-код на телефоні на відстані 30–50 мм від лінзи сканера QR-коду. Він підтримує QR-код, який має бути більше 30 мм × 30 мм і розміром менше 128 байт.

Відстань виявлення QR-коду залежить від байтів і розміру QR-коду.

Додаток Малюнок 4-1 Сканування QR-коду



Додаток 5 Рекомендації щодо кібербезпеки

Обов'язкові дії, які необхідно вжити для забезпечення безпеки базової мережі пристрою:

1.**Використовуйте надійні паролі**

Будь ласка, скористайтеся наступними рекомендаціями щодо встановлення паролів:

- Довжина не повинна бути меншою8 символів.
- Увімкніть щонайменше два типи символів; типи символів включають великі та малі літери, цифри та символи.
- Не використовуйте ім'я облікового запису або обліковий запис у зворотному порядку.
- Не використовуйте безперервні символи, такі як123, abc і т.д.
- Не використовуйте символи, що перетинаються, такі як111, aaa і т.д.

2.**Вчасно оновлюйте прошивку та клієнтське програмне забезпечення**

- Відповідно до стандартної процедури у технологічній галузі, ми рекомендуємо підтримувати прошивку вашого пристрою (наприклад, NVR, DVR, IP-камери тощо) в актуальному стані, щоб гарантувати, що система оснащена останніми виправленнями та патчами безпеки. Якщо пристрій підключено до загальнодоступної мережі, рекомендується увімкнути функцію «автоматичної перевірки оновлень», щоб отримувати своєчасну інформацію про оновлення прошивки, випущених виробником.
- Ми рекомендуємо вам завантажити та використовувати останню версію клієнтського програмного забезпечення.

Корисні рекомендації щодо покращення мережевої безпеки вашого пристрою:

1.**Фізичний захист**

Ми пропонуємо вам виконати фізичний захист пристрою, особливо пристроїв для зберігання даних. Наприклад, помістіть пристрій у спеціальну комп'ютерну кімнату та шафу, а також впровадьте добре організований контроль доступу та управління ключами, щоб запобігти несанкціонованому персоналу від здійснення фізичних контактів, таких як пошкодження обладнання, несанкціоноване підключення знімного пристрою (наприклад, USB-флеш-диска, послідовного порту) і т.д.

2.**Регулярно змінюйте паролі**

Ми рекомендуємо вам регулярно змінювати паролі, щоб знизити ризик їхнього вгадування або злому.

3.**Встановлення та оновлення паролів. Своєчасне скидання інформації.**

Пристрій підтримує функцію скидання пароля. Будь ласка, налаштуйте відповідну інформацію для скидання пароля вчасно, включаючи поштову скриньку кінцевого користувача та питання захисту пароля. Якщо інформація зміниться, будь ласка, змініть її вчасно. При встановленні питань захисту пароля рекомендується не використовувати ті, які можна легко вгадати.

4.**Увімкнути блокування облікового запису**

Функція блокування облікового запису увімкнена за замовчуванням, і ми рекомендуємо вам залишити її увімкненою, щоб гарантувати безпеку облікового запису. Якщо зловмисник спробує увійти до системи з неправильним паролем кілька разів, відповідний обліковий запис та вихідна IP-адреса будуть заблоковані.

5.**Змінити порти HTTP та інші сервісні порти за промовчанням**

Ми пропонуємо вам змінити порти HTTP та інших стандартних служб на будь-який набір чисел в діапазоні 1024–65535, щоб знизити ризик того, що сторонні зможуть вгадати, які порти ви використовуєте.

6.**Увімкнути HTTPS**

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

7.**Прив'язка MAC-адреси**

Ми рекомендуємо вам прив'язати IP і MAC адресу шлюзу до пристрою, тим самим зменшивши

ризик заміни ARP.

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

Відповідно до вимог бізнесу та управління розумно додавайте користувачів та призначайте їм мінімальний набір дозволів.

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

Якщо в них немає необхідності, рекомендується вимкнути деякі служби, такі як SNMP, SMTP, UPnP і т.д. зменшити ризики.

При необхідності рекомендується використовувати безпечні режими, включаючи, крім іншого, такі служби:

- SNMP: виберіть SNMP v3 та встановіть надійні паролі шифрування та паролі автентифікації.
- SMTP: виберіть TLS, щоб отримати доступ до сервера поштових скриньок.
- FTP: виберіть SFTP та встановіть надійні паролі.
- Точка доступу: виберіть режим шифруванняWPA2-PSK та встановіть надійні паролі.

10.**Зашифрована передача аудіо та відео**

Якщо ваші аудіо- та відеодані дуже важливі або конфіденційні, ми рекомендуємо вам використовувати функцію зашифрованої передачі, щоб знизити ризик крадіжки аудіо- та відеоданих у час передачі.

Нагадування: зашифрована передача даних призведе до втрати ефективності передачі.

11.**Безпечний аудит**

- Перевіряйте користувачів у мережі: ми рекомендуємо вам регулярно перевіряти користувачів у мережі, щоб переконатися, що пристрій не авторизований.
- Перевірте журнал пристрою: переглядаючи журнали, ви можете дізнатисяIP-адреси, які використовувалися для входу на ваші пристрої та їх основні операції.

12.**Мережевий журнал**

Через обмежену ємність пристрою збережений журнал обмежений. Якщо вам потрібно зберегти журнал протягом тривалого часу, рекомендується ввімкнути функцію мережевого журналу, щоб гарантувати синхронізацію критичних журналів із сервером мережевого журналу для трасування.

13.**Побудуйте безпечне мережеве середовище**

Щоб краще забезпечити безпеку пристрою та знизити потенційні кіберриски, ми рекомендуємо:

- Вимкніть функцію зіставлення портів маршрутизатора, щоб уникнути прямого доступу до пристроїв. інтрамережі із зовнішньої мережі.
- Мережа повинна бути розділена та ізольована відповідно до реальних потреб мережі. Якщо між двома підмережами немає вимог до комунікації, пропонується використати VLAN, мережевий GAP та інші технології для поділу мережі, щоб досягти ефекту ізоляції мережі.
- Введіть систему автентифікації доступу802.1x для зниження ризику несанкціонованого доступу до приватних мереж.
- Увімкніть функцію фільтраціїIP/MAC-адрес, щоб обмежити коло хостів, яким дозволено доступ до влаштування.