SmartPSS-AC

Посібник користувача

V1.0.3

Передмова

Генерал

Цей посібник знайомить із загальними функціями та операціями SmartPSS-AC (далі - "SmartPSS-AC").

Інструкції з техніки безпеки

У посібнику можуть з'являтися такі сигнальні слова.

Сигнальні слова	Це означає.
 **НЕБЕЗПЕКА**	Вказує на високу потенційну небезпеку, яка, якщо її не уникнути, може призвести до смерті або серйозних травм.
 **ПОПЕРЕДЖЕННЯ**	Вказує на середню або низьку потенційну небезпеку, яка, якщо її не уникнути, може призвести до травм легкого або середнього ступеня тяжкості.
 **ПОПЕРЕДЖЕННЯ**	Вказує на потенційний ризик, який, якщо його не уникнути, може призвести до пошкодження майна, втрата даних, зниження продуктивності або непередбачувані результати.
 **ПОРАДИ**	Надає методи, які допоможуть вам вирішити проблему або заощадити час.
 **ПРИМІТКА**	Надає додаткову інформацію як доповнення до тексту.

Історія ревізій

Версія	Зміст ревізії	Час випуску
V1.0.3	• Оновлена функція ініціалізації. • Оновлена функція налаштування подій.	Серпень 2021 року
V1.0.2	Додано план взаємодії з користувачем, зворотній зв'язок та п'ять час бали в **Система Конфігурація > Керування даними**.	Серпень 2020 року
V1.0.1	Модифіковано функцію запиту до журналу.	Червень 2020
V1.0.0	Перший випуск.	Травень 2020

Повідомлення про захист персональних даних

Як користувач пристрою або контролер даних, ви можете збирати персональні дані інших людей, такі як їхні обличчя, відбитки пальців і номер автомобіля. Ви повинні дотримуватися місцевих законів і нормативних актів про захист персональних даних, щоб захистити законні права та інтереси інших людей шляхом вжиття заходів, які включають, але не обмежуються ними: Забезпечення чіткої та видимої ідентифікації для інформування людей про існування зони спостереження та надання необхідної контактної інформації.

Про Посібник

- Посібник призначений лише для ознайомлення. Між інструкцією та виробом можуть бути незначні відмінності.
- Ми не несемо відповідальності за збитки, понесені внаслідок експлуатації виробу, що не відповідає вимогам посібника.
- Посібник буде оновлюватися відповідно до останніх законів і нормативних актів відповідних юрисдикцій. Для отримання детальної інформації дивіться паперовий посібник користувача, використовуйте наш CD-ROM, відскануйте QR-код або відвідайте наш офіційний веб-сайт. Посібник призначений лише для ознайомлення. Між електронною та паперовою версіями можуть бути незначні відмінності.
- Усі конструкції та програмне забезпечення можуть бути змінені без попереднього письмового повідомлення. Оновлення продукту можуть призвести до появи деяких відмінностей між фактичним продуктом та інструкцією. Будь ласка, зверніться до служби підтримки для отримання останньої версії програми та додаткової документації.
- Можливі помилки в друці або відхилення в описі функцій, операцій і технічних даних. У разі виникнення будь-яких сумнівів або суперечок ми залишаємо за собою право на остаточне роз'яснення.
- Оновіть програмне забезпечення для читання або спробуйте інше основне програмне забезпечення для читання, якщо посібник (у форматі PDF) не відкривається.
- Усі торгові марки, зареєстровані торгові марки та назви компаній у цьому посібнику є власністю відповідних власників.
- Якщо під час використання пристрою виникають проблеми, відвідайте наш веб-сайт, зв'яжіться з постачальником або службою підтримки.
- У разі виникнення будь-яких неясностей або суперечностей, ми залишаємо за собою право на остаточне роз'яснення.

Зміст

1 Огляд

SmartPSS-AC - це клієнтське програмне забезпечення, розроблене для малих і середніх рішень. Ви можете завантажити різні рішення за потреби. Цей посібник знайомить з основними функціями та операціями.

2 Встановлення та вхід

2.1 Встановлення

Зверніться до технічної підтримки або завантажте ToolBox, щоб отримати SmartPSS-AC. Завантажити ToolBox можна на офіційному сайті Dahua.

- Якщо ви отримали пакет програмного забезпечення SmartPSS-AC, встановіть і запустіть програмне забезпечення відповідно до інструкцій інтерфейсу.
- Якщо ви отримали програмне забезпечення через панель інструментів, запустіть SmartPSS-AC відповідно до інструкцій інтерфейсу.

2.2 Логін

2.2.1 Ініціалізація

Ініціалізуйте SmartPSS-AC під час першого входу, включаючи встановлення пароля та захисних запитань. Пароль призначений для входу в систему, а захисні питання - для зміни пароля.

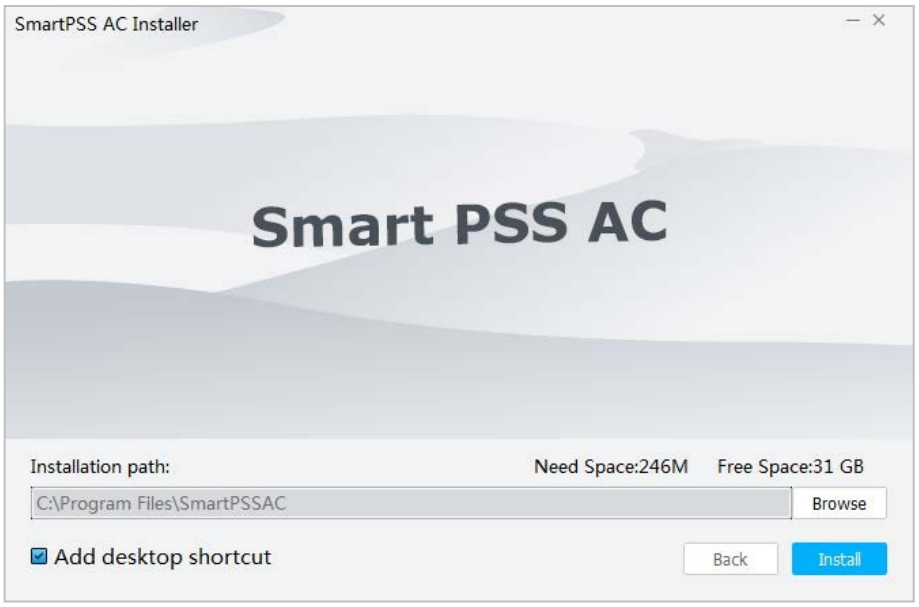
Крок 1 Двічі клацніть SmartPSSAC.exe або натисніть кнопку **Відкрити** поруч із піктограмою програми на панелі інструментів.

Крок 2 Виберіть мову зі спадного списку, виберіть **Я прочитав і погоджуюсь з угодою про використання програмного забезпечення,** а потім натисніть **Далі**.

Рисунок 2-1 Вибір мови

Крок 3 Натисніть **Огляд,** щоб вибрати шлях до інсталяції, а потім натисніть **Встановити**.

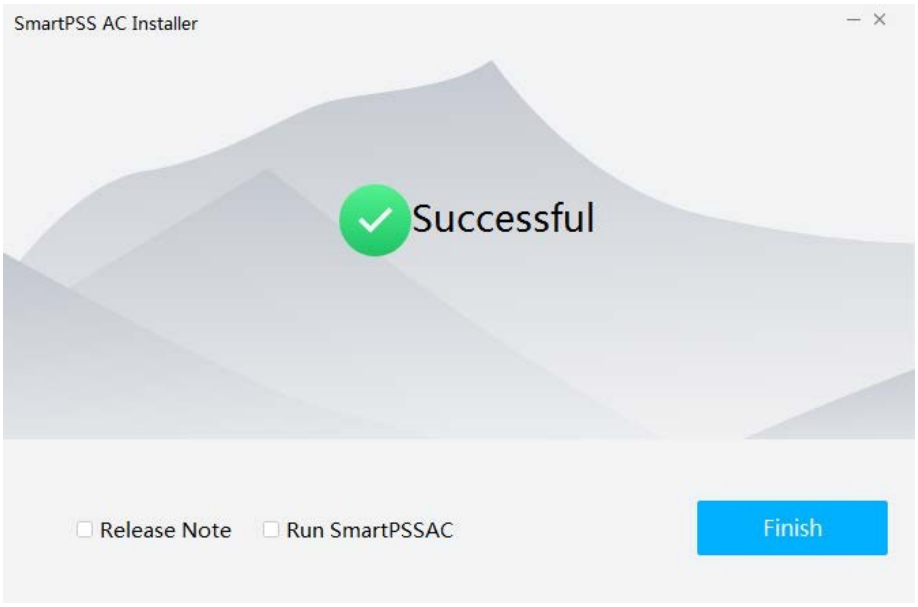
Рисунок 2-2 Вибір шляху встановлення



Крок 4 Натисніть **Готово,** щоб завершити встановлення.

Виберіть **Запустити SmartPSSAC,** щоб запустити SmartPSS-AC.

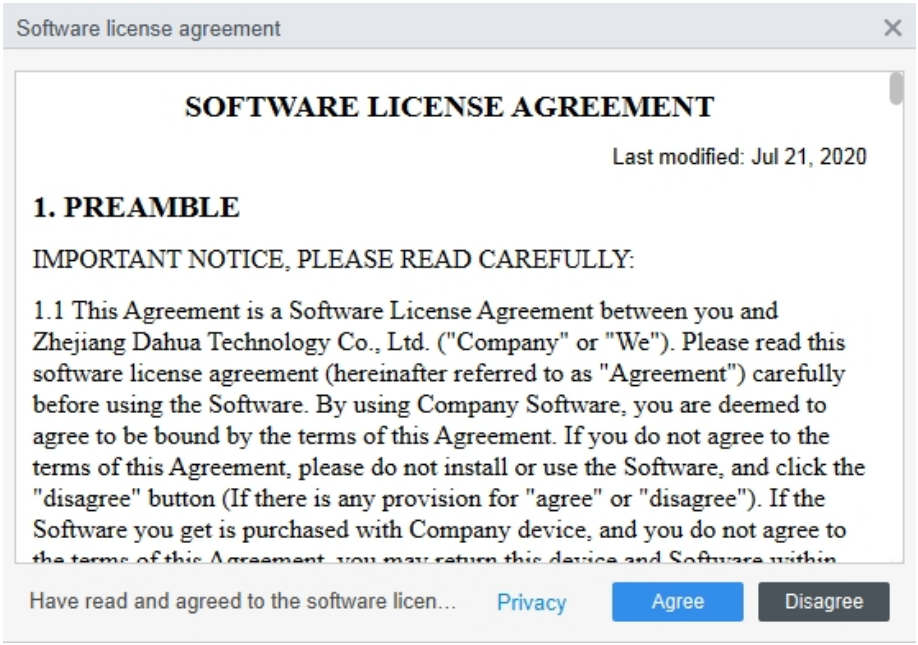
Рисунок 2-3 Встановлення завершено



Крок 5 Натисніть кнопку "**Згоден",** щоб погодитися з ліцензійною угодою на програмне забезпечення.

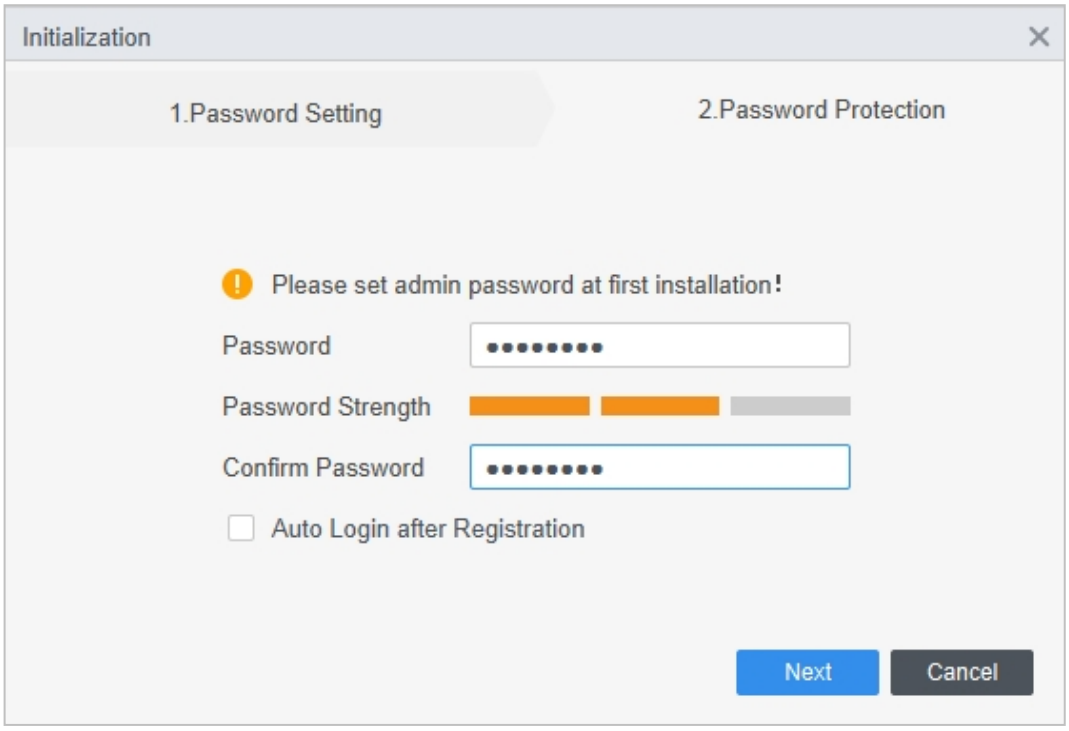
Натисніть "**Конфіденційність",** щоб переглянути конкретний вміст.

Рисунок 2-4 Погодьтеся з ліцензійною угодою на програмне забезпечення



Крок 6 Встановіть пароль в інтерфейсі **Ініціалізація,** а потім натисніть **Далі**.

Рисунок 2-5 Встановлення пароля



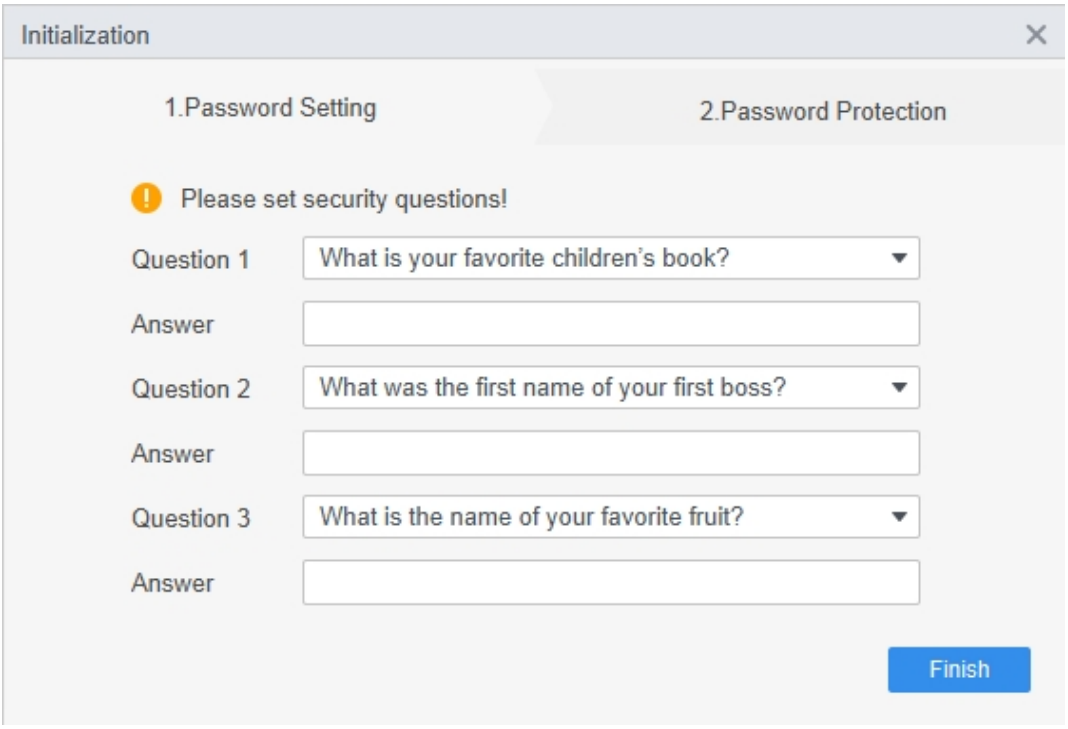
Таблиця 2-1 Параметри ініціалізації

Параметр	Опис
Пароль	Пароль повинен складатися з 8-32 непустих символів і містити принаймні два типи символів: великі, малі, цифри та спеціальні символи (за винятком символів ' " ; : &).
Надійність пароля	Відображення ефективності пароля проти вгадування або грубого перебору атаки. Зелений колір означає, що пароль достатньо надійний, червоний -

	менш надійний. Встановіть пароль високого рівня безпеки відповідно до пароля
Параметр	**Опис**
	підказка про силу.
Підтвердити пароль	Введіть пароль ще раз, щоб підтвердити його.
Автоматичний вхід після реєстрації	Увімкніть **Автоматичний вхід після реєстрації,** щоб SmartPSS-AC автоматично входив в систему після ініціалізації; в іншому випадку відображається інтерфейс входу в систему.

Крок 7 Задайте питання безпеки та натисніть **Готово**.

Рисунок 2-6 Встановіть питання безпеки

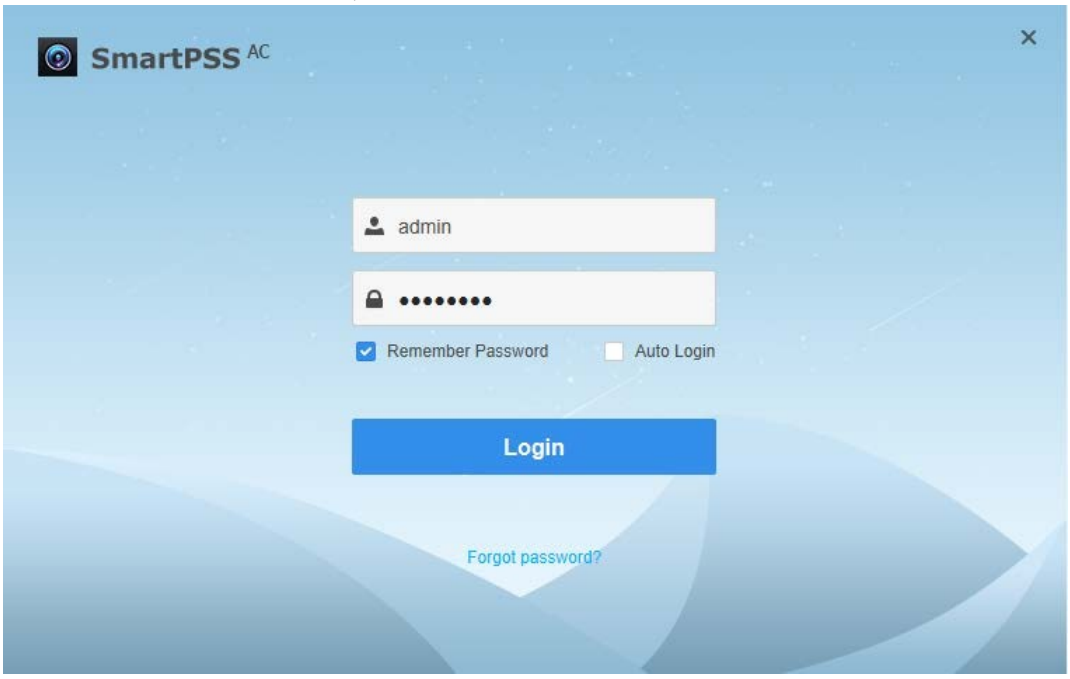


2.2.2 Щоденний вхід

Крок 1 Двічі клацніть на SmartPSSAC.exe або натисніть кнопку **Відкрити** поруч з піктограмою програми на панелі інструментів. Введіть ім'я користувача та пароль, а потім натисніть **Увійти**.

Крок 2

Рисунок 2-7 Вхід до системи



Таблиця 2-2 Параметри входу в систему

Параметр	Опис
Запам'ятати пароль	Увімкніть опцію **Запам'**ятати **пароль,** щоб вам не потрібно було повторно вводити пароль при наступному вході.
Автоматичний вхід	Увімкніть **Автоматичний вхід,** щоб SmartPSS-AC автоматично входив в систему наступного разу, коли ви використовуєте той самий обліковий запис користувача.
Забули пароль?	Натисніть **Забули пароль,** щоб відновити пароль за допомогою захисних запитань, якщо ви забули пароль.

2.3 Скидання пароля

Ви можете відновити пароль, відповівши на питання безпеки.

Крок 1 Двічі клацніть SmartPSSAC.exe або натисніть кнопку **Відкрити** поруч із піктограмою програми на панелі інструментів.

Крок 2 Натисніть **Забули пароль?** в інтерфейсі входу.

Крок 3 Дайте відповідь на питання безпеки, а потім натисніть **Далі**. Відновіть пароль відповідно до інструкцій інтерфейсу.

Крок 4

2.4 План взаємодії з користувачем

Ви можете вибрати "**Приєднатися",** щоб приєднатися до плану, або "**Не приєднуватися",** щоб продовжити. Якщо ви приєдналися до плану, інформація про ваші операції буде збиратися; в іншому випадку інформація про ваші операції збиратися не буде.

- Якщо ви хочете вийти з плану, у верхньому правому куті інтерфейсу ви можете **вибрати>**

Конфігурація системи> Базові налаштування, щоб зняти позначку з **Плану користувацького досвіду.**

- Натисніть **Переглянути політику конфіденційності,** щоб переглянути конкретний зміст.

Рисунок 2-8 План взаємодії з користувачем

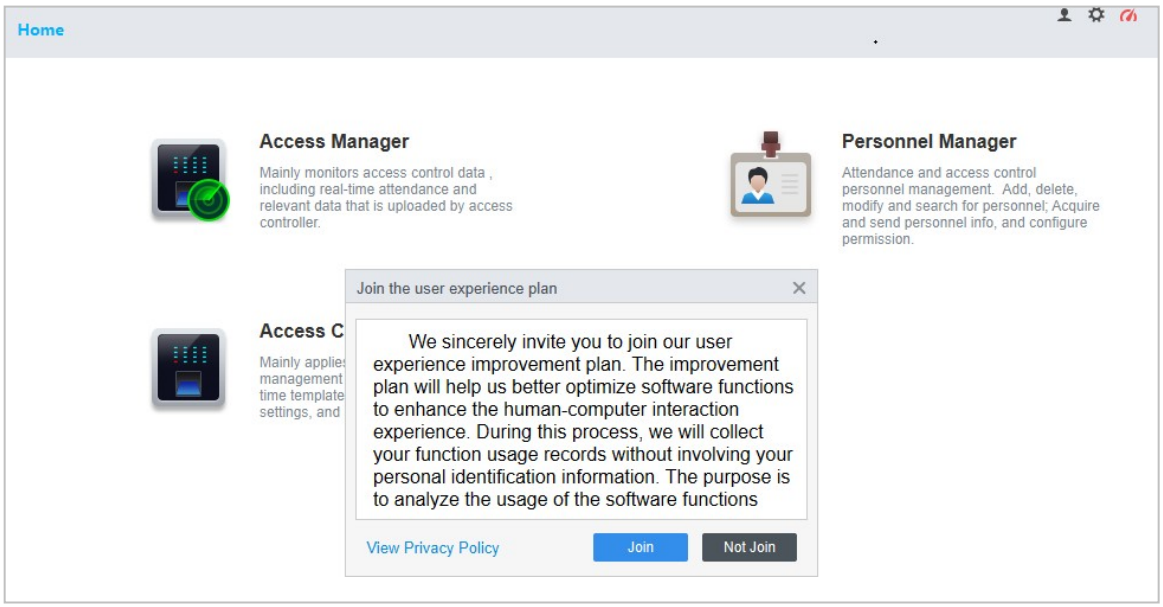
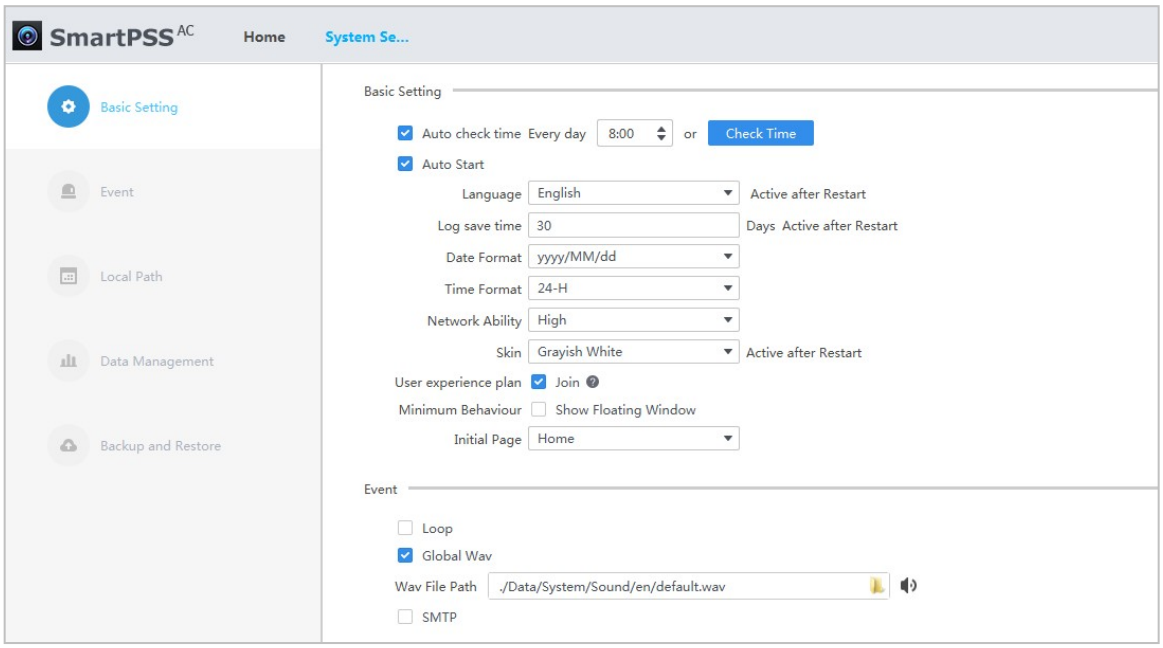


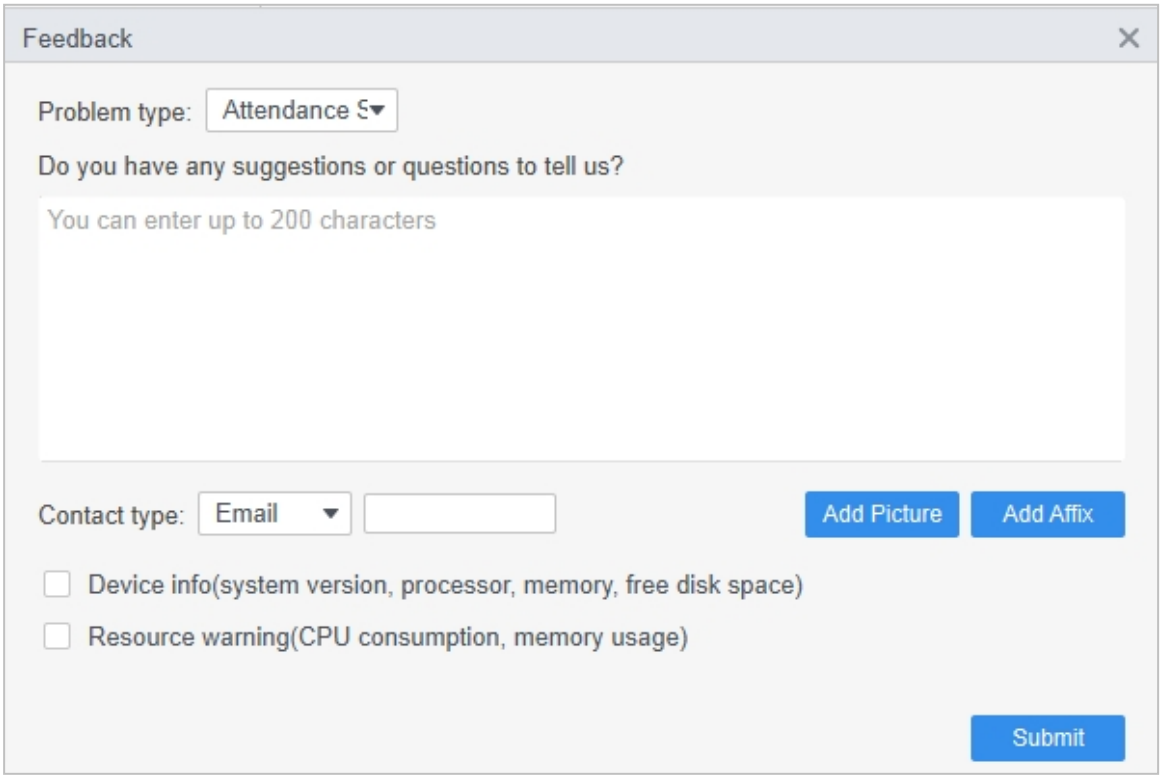
Рисунок 2-9 Виберіть або скасуйте вибір плану взаємодії з користувачем



2.5 Зворотній зв'язок

Якщо у вас є якісь пропозиції, у верхньому правому куті інтерфейсу виберіть > **Зворотній зв'язок, після** чого ви можете ввести пропозиції (слова), завантажити фотографії та вкладення, а потім натиснути кнопку "**Надіслати**".

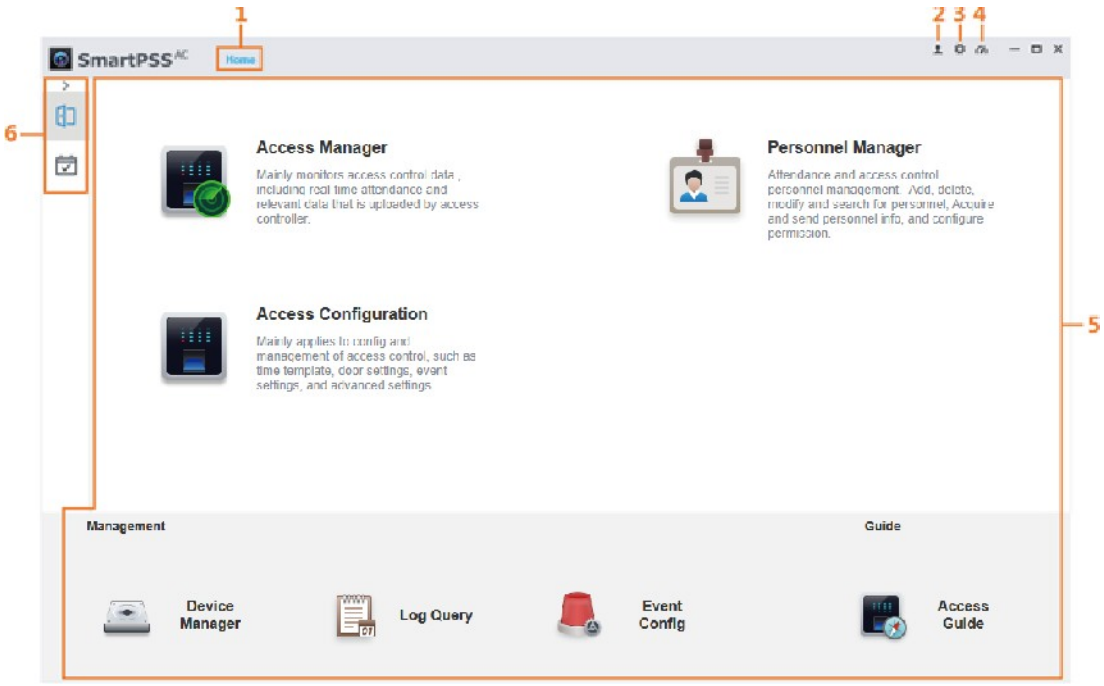
Рисунок 2-10 Зворотній зв'язок



3 Головна сторінка

Головна сторінка складається з 6 частин.

Рисунок 3-1 Домашня сторінка



Таблиця 3-1 Параметри домашньої сторінки

Ні.	Параметр	Опис
1	Вкладка "Функції	Відображати домашню сторінку за замовчуванням. Коли ви натискаєте на функцію вперше, тут з'являється вкладка функції.
2	Керування користувачами	• Перейдіть за посиланням і виберіть **Менеджер користувачів,** щоб керувати користувачами, наприклад, додавати ролі/користувачів, видаляти ролі/користувачів і встановлювати дозволи. • Натисніть і виберіть **Блокувати екран,** щоб заблокувати екран. Введіть пароль облікового запису, коли хочете розблокувати. • Натисніть і виберіть "Змінити **користувача",** щоб повернутися до інтерфейсу входу. Ви можете увійти під новим обліковим записом. • Перейдіть за посиланням і виберіть **Help Manual**, щоб отримати посібник користувача. • Натисніть і виберіть **Про** систему, щоб переглянути версію і дату системи. Увімкніть **Відкрити журнал налагодження,** щоб журнали налагодження автоматично зберігалися у локальному каталозі для

		пошуку та вирішення проблем.
3	Конфігурація системи	• Базове налаштування ◇ Хронометраж: Увімкніть **автоматичну перевірку часу кожного дня** та встановіть **час перевірки** щоб пристрої автоматично перевіряли час за встановленим значенням у час.
Ні.	**Параметр**	**Опис**

◇ Мова: Відображати мову, яка буде активована після перезапуску.

◇ Час збереження журналу: Встановити час збереження журналу, а потім журналів з сьогоднішнього дня до встановленого часу буде збережено. Ця функція активується після перезапуску. Наприклад, встановіть час збереження 30, і тоді будуть збережені журнали за останні 30 днів.

◇ Формат даних: Виберіть формат відображення даних.

◇ Формат часу: Виберіть формат відображення часу.

◇ Мережеві можливості: Виберіть мережеві можливості відповідно до вашої мережі стан мережі. Наприклад, якщо стан мережі вільний, рекомендується вибрати **Високий**.

◇ Обличчя: Виберіть стиль, який буде активовано після перезапуску. За замовчуванням сірувато-білого кольору.

- Подія
  - ◇ Увімкніть цикл відтворення звуку події.
  - ◇ Вибрати звук події. Ви можете вибрати потрібний звук або додати кастомізовані звуки в доріжці.
  - ◇ Увімкніть та налаштуйте SMTP.
- Локальний шлях

  Шляхи зберігання.
- Управління даними
  - ◇ Витягувати регулярно: Встановіть час регулярного вилучення, щоб дані про відвідування пристроїв вилучалися у визначений час.
  1. Якщо ви виберете "**Щодня"**, ви зможете вибрати п'ять часових точок.
  2. Якщо ви виберете "**Щотижня",** ви зможете вибрати певний часовий проміжок у певний день.

     Для пристроїв обліку відвідуваності витягніть дані безпосередньо. Для контролерів доступу встановіть пристрій як точку відвідування, а потім витягніть дані відвідування.
  - ◇ Регулярно очищайте: Встановіть час збереження даних і зображень. SmartPSS-AC автоматично очищає дані та зображення, які перевищують час збереження. Вона запускається о 00:00 кожного дня або під час запуску програми.
- Резервне копіювання: Підтримка автоматичного та ручного резервного копіювання.
  - ◇ Вручну: Виберіть шлях до резервної копії та натисніть кнопку "Створити **резервну копію вручну"**.
  - ◇ Авто: Виберіть шлях до резервної копії та увімкніть **автоматичне резервне копіювання**.
- Відновити: Натисніть **Відновити** і виберіть потрібний файл

		резервної копії. Configurations відновить конфігурації файлів.
4	Стан системи	Натисніть  , щоб переглянути стан використання процесора та оперативної пам'яті. Якщо завантаження процесора високе, іконка стає червоною.
5	Функціо нальний модуль	Натисніть на іконку функції, щоб перейти до інтерфейсу функції.
6	Модуль рішення	Виберіть потрібне рішення. Натисніть >, щоб відобразити або приховати рішення.

4 Керування пристроями

SmartPSS-AC дозволяє додавати пристрої. Ви можете віддалено налаштовувати та керувати пристроями після додавання за допомогою SmartPSS-AC.

4.1 Додавання пристрою

Існує кілька способів додавання пристроїв. Виберіть найбільш підходящий метод відповідно до ситуації, наприклад, IP-адреси та сегмента мережі.

- Автоматичний пошук
- Додавання вручну
- Імпорт партіями

4.1.1 Додавання пристрою за допомогою автопошуку

Закривайте ConfigTool і DSS, коли налаштовуєте пристрої, інакше ви не зможете виконати пошук на всіх пристроях.

Рекомендується додавати пристрої за допомогою автопошуку, коли вам потрібно додавати пристрої групами в межах одного сегмента мережі, або коли сегмент мережі відомий, але IP-адреса пристрою невідома.

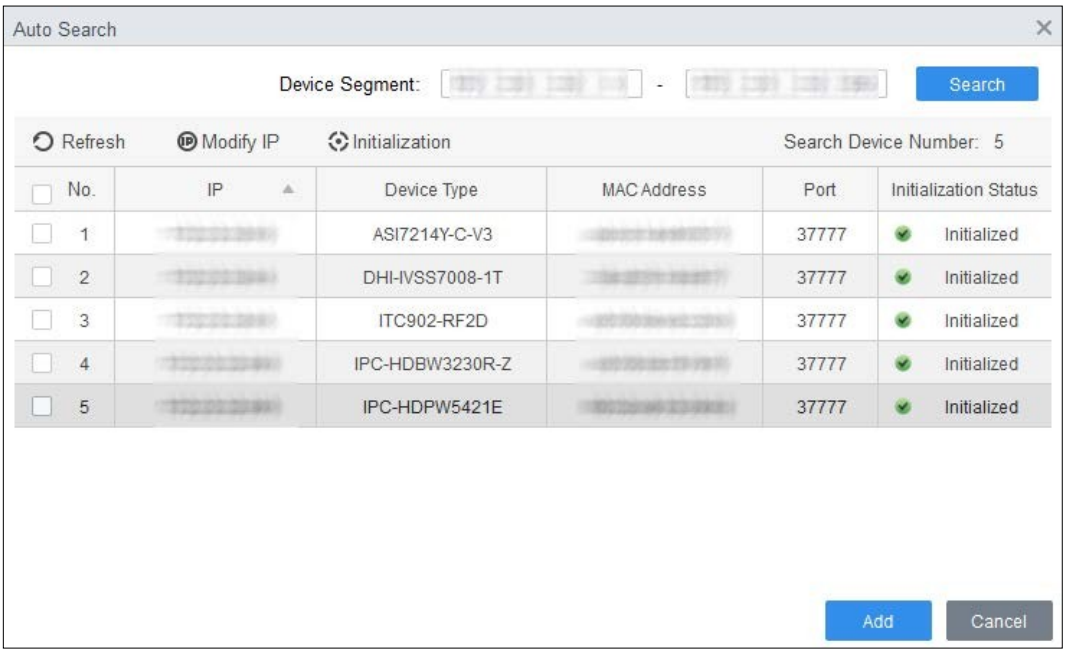
Крок 1 Натисніть **Автопошук** в інтерфейсі **Диспетчера пристроїв.**

Задайте діапазон сегмента мережі і натисніть **Пошук**.

Крок 2 Відобразиться список знайдених пристроїв.

- Натисніть **Оновити,** щоб оновити результати пошуку.
- Виберіть потрібний пристрій, а потім натисніть **Змінити IP,** щоб змінити IP-адресу, маску підмережі та шлюз. Докладні відомості див. у розділі "4.4.3 Зміна IP-адреси".
- Виберіть один неініціалізований пристрій, а потім натисніть **Ініціалізація**. Ви можете відновити IP-адресу, маску підмережі, шлюз і пароль для входу. Докладні відомості див. у розділі "4.4.2 Ініціалізація".

Рисунок 4-1 Результати пошуку



Крок 3 Виберіть потрібні пристрої, а потім натисніть **Додати**.

Крок 3 Введіть ім'я користувача та пароль для входу, а потім натисніть **ОК** для підтвердження.

Крок 4

- Після додавання пристроїв все ще відображається інтерфейс **автоматичного пошуку.** Ви можете продовжити додавання або натиснути **Скасувати,** щоб вийти.
- Пристрої будуть авторизовані автоматично після додавання. Якщо вхід пройшов успішно, статус відображається як "онлайн", інакше - "офлайн".

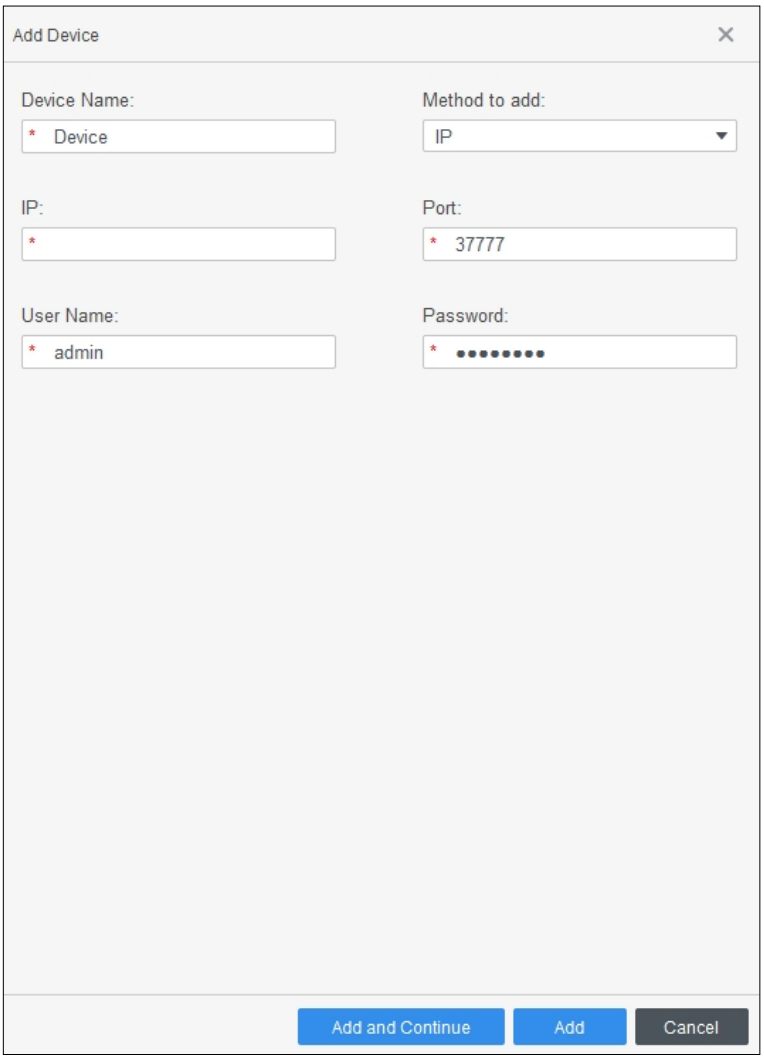
4.1.2 Додавання пристрою вручну

Рекомендується додавати пристрої вручну, якщо вам потрібно додати один пристрій з певною IP-адресою або доменним ім'ям.

Крок 1 Виберіть **Додати** в інтерфейсі **Диспетчера пристроїв.** Налаштуйте параметри

Крок 2 пристрою.

Рисунок 4-2 Додавання пристрою вручну



Таблиця 4-1 Параметри додавання вручну

Параметр	**Опис**
Назва пристрою	Рекомендується присвоювати пристроям імена із зазначенням зони моніторингу для легкої ідентифікації.
Спосіб додавання	Виберіть метод для додавання.
IP	Введіть тут IP-адресу пристрою, коли ви виберете IP як метод додавання.
Порт	Введіть номер порту, за замовчуванням він дорівнює 37777. Фактичний номер порту має перевагу.
Ім'я користувача	Введіть ім'я користувача для входу.
Пароль	Введіть пароль для входу.

Крок 3 Натисніть **Додати,** щоб додати пристрій і закрити інтерфейс **Додати пристрій**; або натисніть **Додати і продовжити,** щоб додати пристрій і залишитися в інтерфейсі **Додати пристрій, щоб можна було** зручно додати інший пристрій.

4.1.3 Імпорт пристрою партіями

Рекомендується додавати пристрої за допомогою імпорту, якщо вам потрібно додати кілька пристроїв, але вони знаходяться в різних сегментах мережі. Організуйте інформацію про пристрої у вигляді файлу у форматі .xml, а потім імпортуйте файл.

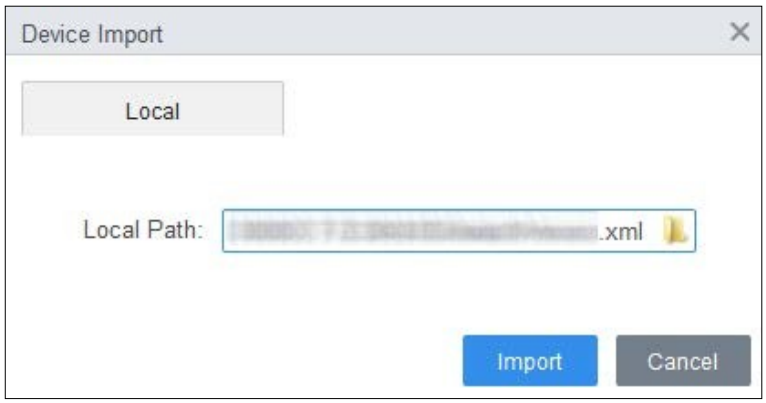
Ви можете експортувати шаблон інформації про пристрій. Виберіть пристрій і натисніть **Експортувати**.

Крок 1 Натисніть Диспетчер пристроїв > Імпорт.

Крок 2 Виберіть інформаційний файл і натисніть кнопку "**Імпортувати**".

Пристрої будуть авторизовані автоматично після додавання. Якщо вхід пройшов успішно, статус відображається як "онлайн", інакше - "офлайн".

Рисунок 4-3 Імпорт інформації про пристрій у форматі .xml



4.2 Видалення пристрою

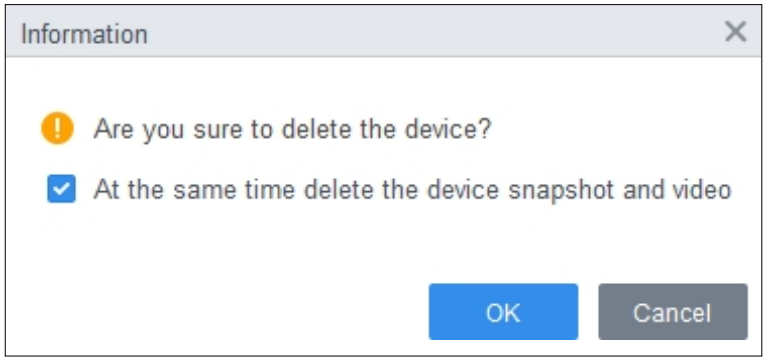
Крок 1 Виберіть Диспетчер **пристроїв** на головній сторінці.

Крок 2 Виберіть пристрій, який вам більше не потрібен, а потім натисніть **Видалити** або , що знаходиться праворуч від пристрою.

(Необов'язково) виберіть **Одночасно видалити знімок пристрою та відео,** якщо ви цього не зробите потрібні ці знімки та відео, інакше не перевіряйте.

Рисунок 4-4 Видалення пристрою

Крок 3



Крок 4 Натисніть **OK**.

4.3 Пристрій для експорту

Ви можете експортувати інформацію про пристрій до локальної пам'яті.

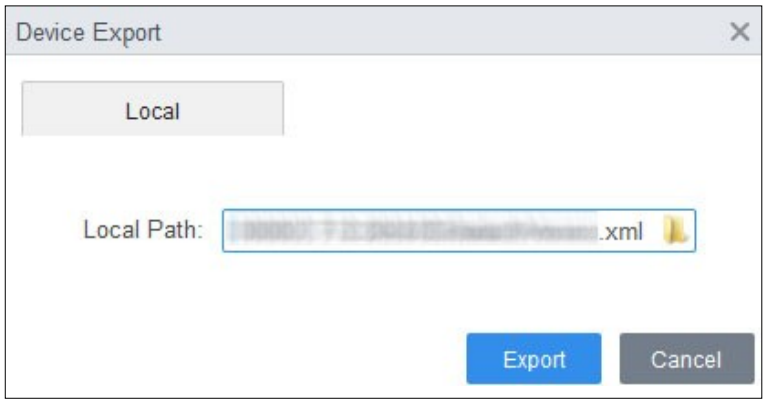
Крок 1 Виберіть Диспетчер **пристроїв** на домашній сторінці.

Крок 2 Виберіть пристрій, який потрібно експортувати, а потім натисніть **Експортувати** в інтерфейсі **Диспетчера пристроїв.**

Виберіть локальний шлях експорту, а потім натисніть **Експортувати**.

Рисунок 4-5 Експорт інформації про пристрій

Крок 3



4.4 Пристрій для редагування

4.4.1 Редагування інформації про пристрій

Ви можете змінити інформацію про доданий пристрій, таку як назва, ім'я користувача та пароль для входу.

Крок 1 Виберіть Диспетчер **пристроїв** на домашній сторінці.

Крок 2 Натисніть праворуч від обраного пристрою або двічі клацніть пристрій у списку пристроїв.

Відредагуйте інформацію про пристрій. Натисніть "**Зберегти**".

Крок 3

Крок 4

4.4.2 Ініціалізація

Підтримує ініціалізацію лише тих пристроїв, які знаходяться в тому ж сегменті мережі, що і ПК.

Крок 1 2

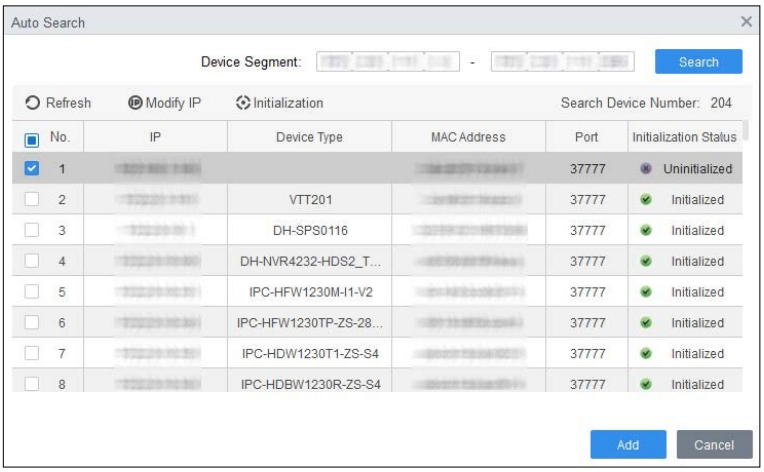
Крок

Клацніть Диспетчер пристроїв > Автоматичний пошук.

ть **Пошук**. Відобразиться список знайдених пристроїв.

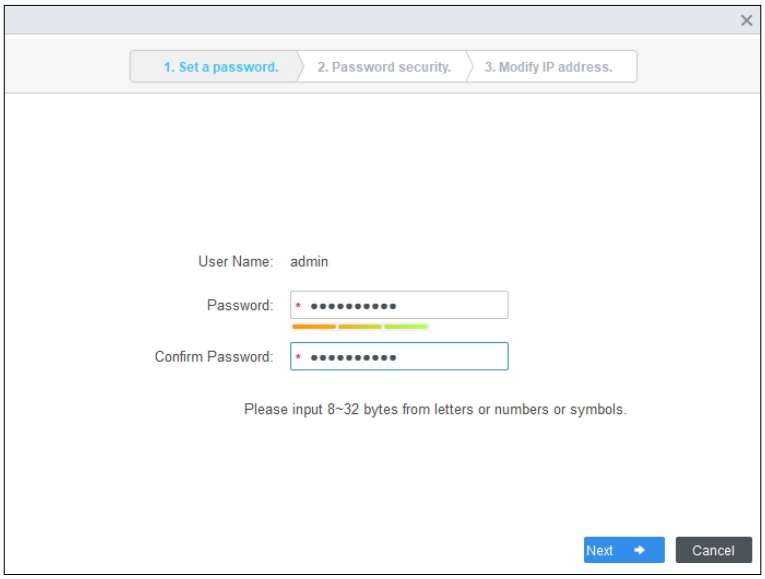
Задайте діапазон сегмента мережі і натисніть

Рисунок 4-6 Список пристроїв



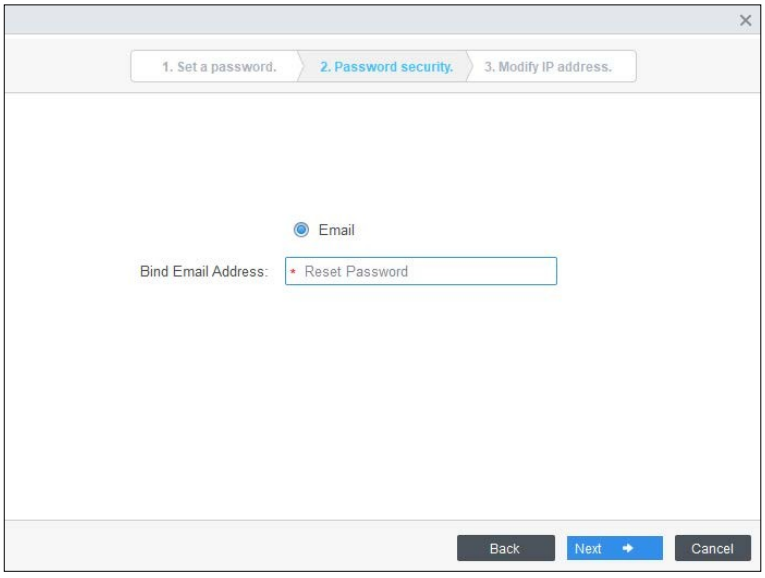
Крок 3 Виберіть неініціалізований пристрій і натисніть **Ініціалізація**. Встановіть пароль і натисніть **Далі**.

Рисунок 4-7 Встановлення пароля



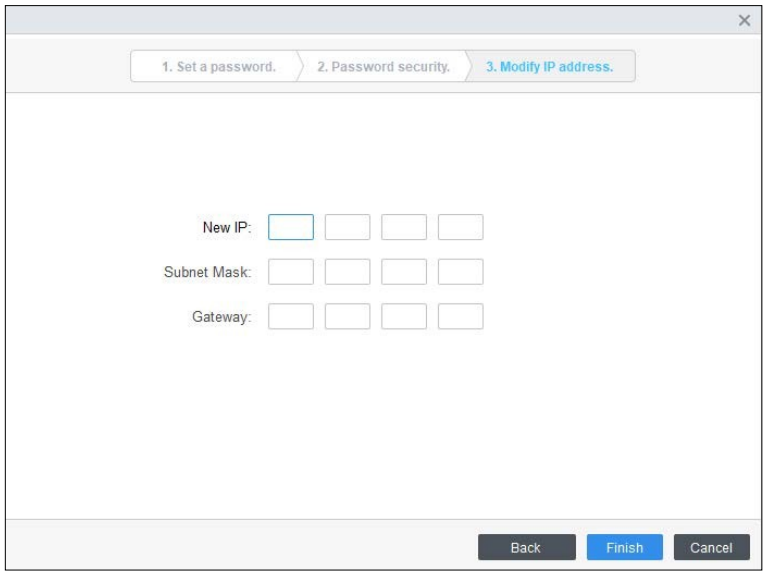
Крок 5 Введіть адресу електронної пошти для скидання пароля.

Рисунок 4-8 Резервна адреса електронної пошти



Крок 6 Введіть нову IP-адресу, маску підмережі та шлюз, а потім натисніть **Готово**. Якщо їх не буде введено, ці три параметри буде використано за замовчуванням.

Рисунок 4-9 Зміна IP-адреси



4.4.3 Зміна IP-адреси

Після ініціалізації віддаленого пристрою ви можете змінити його IP-адресу.

Крок 1 Натисніть **Автопошук** в інтерфейсі **Диспетчера пристроїв.**

Крок 2 Задайте діапазон сегмента мережі та натисніть **Пошук**.

Крок 3 Виберіть потрібні пристрої і натисніть **Змінити IP**.

Крок 4 Змініть IP-адресу, маску підмережі та шлюз пристрою і натисніть **OK**. Ви можете змінити IP-адресу одного пристрою або декількох пристроїв одночасно.

- При пакетній зміні новий IP буде присвоєно пристрою, що знаходиться зверху, а інші IP-адреси будуть збільшуватися на 1 зверху донизу. Наприклад, якщо ви виберете два пристрої і встановите нову IP-адресу 192.168.1.10, то IP-адресу верхнього пристрою в списку буде змінено на 192.168.1.10, а наступного пристрою - на 192.168.1.11.
- У разі пакетної зміни маска підмережі та шлюз будуть призначені всім вибраним пристроям.

Рисунок 4-10 Зміна IP-адреси одного пристрою

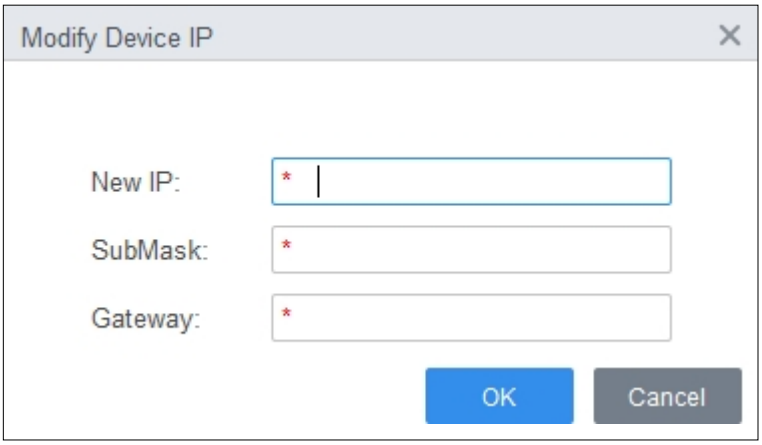


Рисунок 4-11 Зміна IP-адреси пристроїв у пакетах

Крок 5 Введіть ім'я користувача та пароль для входу, а потім натисніть **OK** для підтвердження.

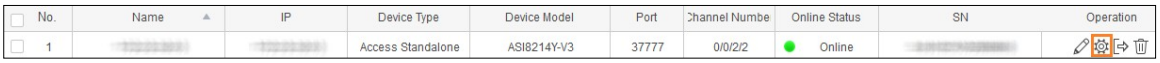
4.4.4 Конфігурація пристрою

Для деяких пристроїв ви можете виконати конфігурацію, включаючи встановлення часу, оновлення прошивки, перезавантаження пристрою, вилучення персоналу та вилучення записів відвідуваності.

Крок 1Виберіть диспетчер пристроїв.

Крок 2 Натисніть .

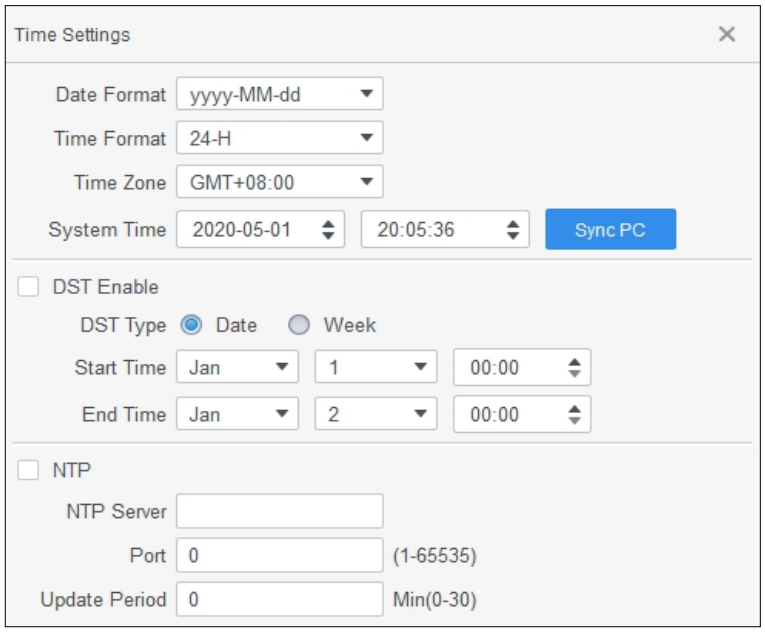
Рисунок 4-12 Налаштування пристрою



Крок 3 Налаштувати пристрій.

- Налаштування часу

Рисунок 4-13 Зміна IP-адреси пристроїв у пакетах



Таблиця 4-2 Параметри налаштування часу

Параметр	Опис
Формат дати	Налаштуйте формат відображення дати.
Формат часу	Встановіть формат відображення часу.
Часовий пояс	Встановіть часовий пояс.
Системний час	Встановіть системний час. Ви також можете натиснути кнопку **Синхронізувати з ПК**, щоб встановити системний час таким самим, як і час ПК.
DST	Увімкніть перехід на літній час за потреби. Встановіть тип переходу на літній час, час початку та час закінчення.
НТП	Увімкніть сервер NTP, якщо вам потрібно синхронізувати системний час з часом NTP. Введіть адресу сервера, порт і період оновлення.

- Оновлення прошивки

  Виберіть кошик для оновлення і дійте відповідно до інструкцій.
- Перезавантажити

  Натисніть, щоб перезавантажити пристрій.
- Евакуювати особовий склад

  Виберіть потрібний персонал і витягніть інформацію про нього з пристрою на локальну пам'ять.
- Витягніть записи про відвідування.

  Встановіть період часу та витягніть записи відвідувань вручну.

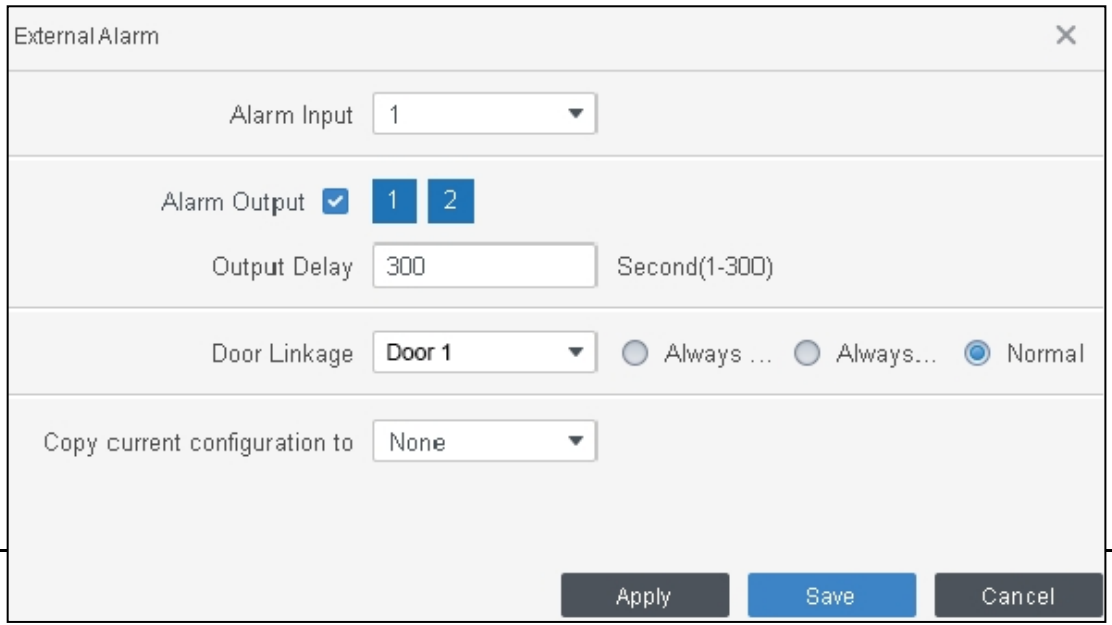
  Перед витяганням переконайтеся, що ви встановили контролери доступу як точки відвідування. Для отримання детальної інформації про налаштування точки відвідування див. *Посібник користувача SmartPSS-AC_Attendance Solution_User's Manual*.

4.4.5 Конфігурація тривоги

Пристрої з моделлю ASC2202B-D можна підключати до зовнішніх пристроїв сигналізації. Перейдіть до розділу

Зовнішній інтерфейс **тривоги,** а потім налаштуйте параметри.

Рисунок 4-14 Зовнішня тривога



Таблиця 4-3 Параметри налаштування часу

Параметр	**Опис**
Тривожний вхід	За потреби виберіть номер вхідного каналу тривоги.
Вихід тривоги	За потреби оберіть номер вихідного каналу тривоги.
Затримка на виході	Сигнали тривоги будуть виводитися після встановленої вами тривалості.
Дверна фурнітура	Після спрацьовування тривог ви можете вибрати режим "Завжди відчинені", "Завжди зачинені" або "Нормальний" для різних дверей.
Скопіювати поточну конфігурацію до	Ви можете скопіювати поточну конфігурацію на інші пристрої за потреби.

5 Запит до журналу

Ви можете робити запити до журналів клієнта і пристроїв. Ці два методи схожі, і тут розглянуто запит до системних журналів клієнта як приклад.

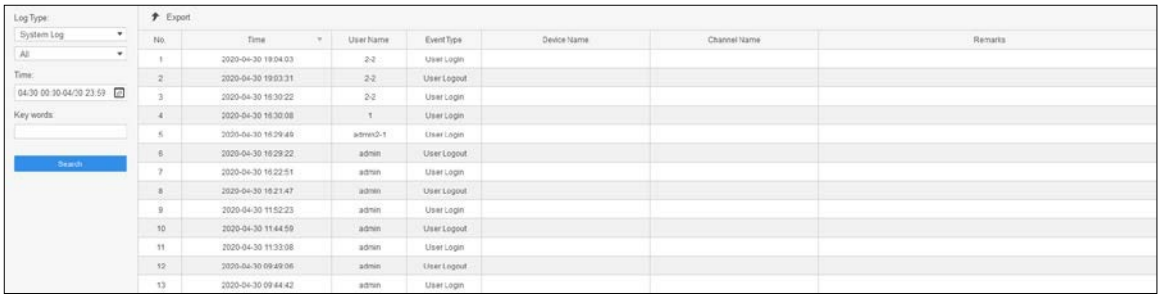
Крок 1 Виберіть Запит до журналу.

Крок 2 Виберіть тип журналу та час запису, а також введіть ключові слова, якщо потрібно. Натисніть **Пошук**. Результати відображаються в правій частині інтерфейсу.

Крок 3 (Необов'язково) Натисніть **Експортувати,** щоб експортувати журнали на локальний пристрій.

Крок 4

Рисунок 5-1 Запит до журналів



6 Конфігурація подій

Налаштувавши подію, ви можете створити програмні зв'язки, такі як звуковий сигнал тривоги, надсилання електронної пошти та зв'язки з будильниками.

- Налаштуйте зовнішні сигналізації, підключені до контролерів доступу (наприклад, димову сигналізацію), камер і пристроїв зберігання даних.
- Налаштуйте зв'язки подій контролера доступу.
  - Тривожна подія
  - Аномальна подія
  - Звичайна подія

- Для функції антипасажу встановіть режим антипасажу в пункті **Abnormal** у розділі **Event Config,** а потім налаштуйте параметри в розділі **Advanced Config**.
- У **групі за замовчуванням** відображаються лише пристрої контролю доступу та відвідування.

Крок 1 Натисніть Конфігурація **подій** на головній сторінці.

Крок 2 Виберіть потрібні двері та виберіть **Тривожна подія > Подія вторгнення**. Натисніть праворуч від тривоги **вторгнення,** щоб увімкнути функцію. Налаштуйте дії прив'язки тривоги вторгнення.

Крок 3
- Увімкнути сигнал тривоги.

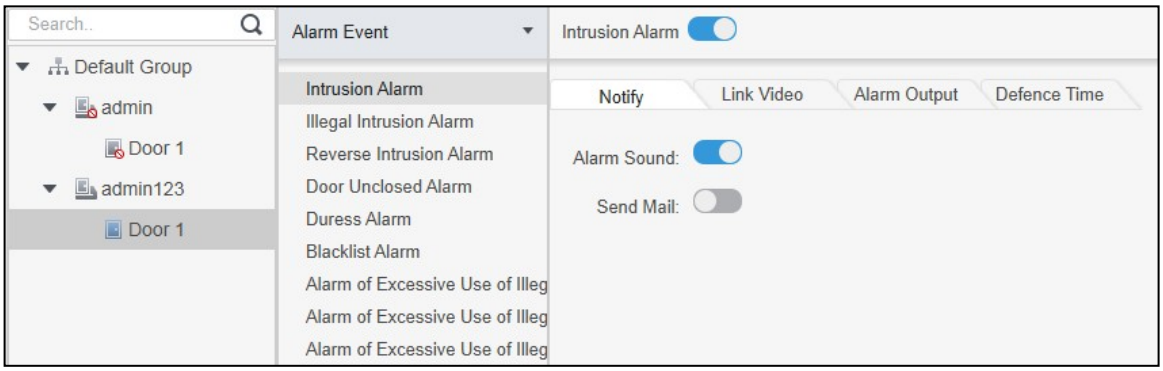
Крок 4 Перейдіть на вкладку Сповіщення та натисніть праворуч від пункту **Звук тривоги**. При виникненні події вторгнення контролер доступу сповіщає про це звуковим сигналом тривоги.

- Надішліть тривожний імейл.

1) Увімкніть **Надіслати пошту** і підтвердіть налаштування SMTP, ви автоматично перейдете до інтерфейсу **налаштувань системи.**
2) Налаштуйте параметри SMTP, такі як адреса сервера, номер порту та режим шифрування.

При виникненні події вторгнення система автоматично надсилає тривожні повідомлення на вказаний адресат.

Рисунок 6-1 Налаштування тривоги вторгнення



- Налаштуйте відео з прив'язкою.

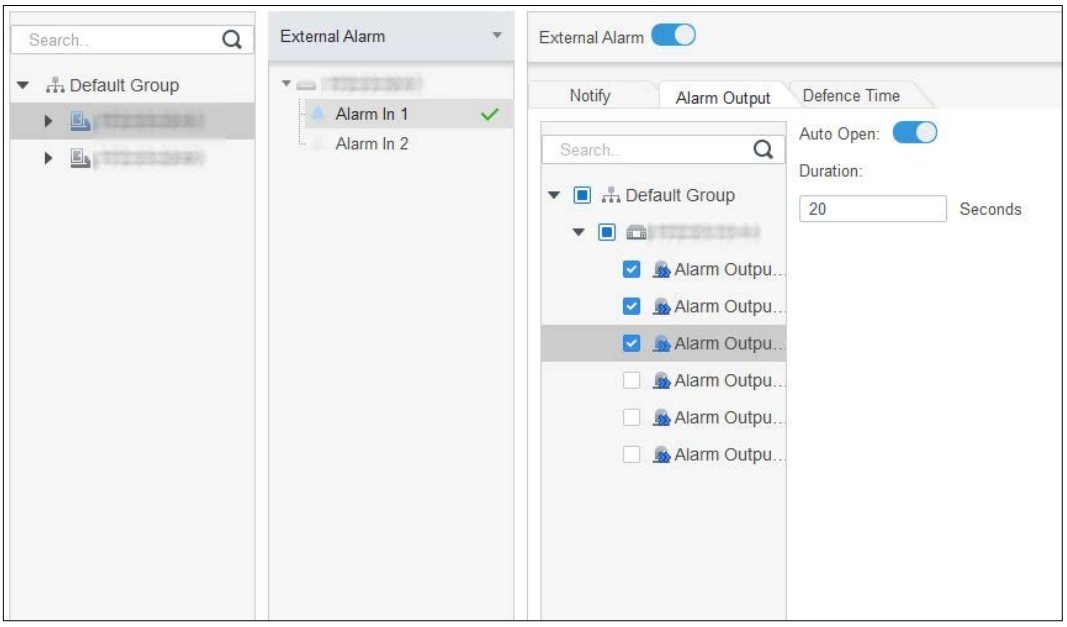
1) Натисніть "**Приєднати відео"**, виберіть потрібний макет відео. Щойно спрацює тривога вторгнення, відео автоматично відобразиться на інтерфейсі.

- Налаштуйте вхід/вихід тривоги.

1) Перейдіть на вкладку **Вихід тривоги.**
2) Виберіть пристрій, який підтримує вхід тривоги, виберіть канал входу тривоги, а потім увімкніть **Зовнішню тривогу**.

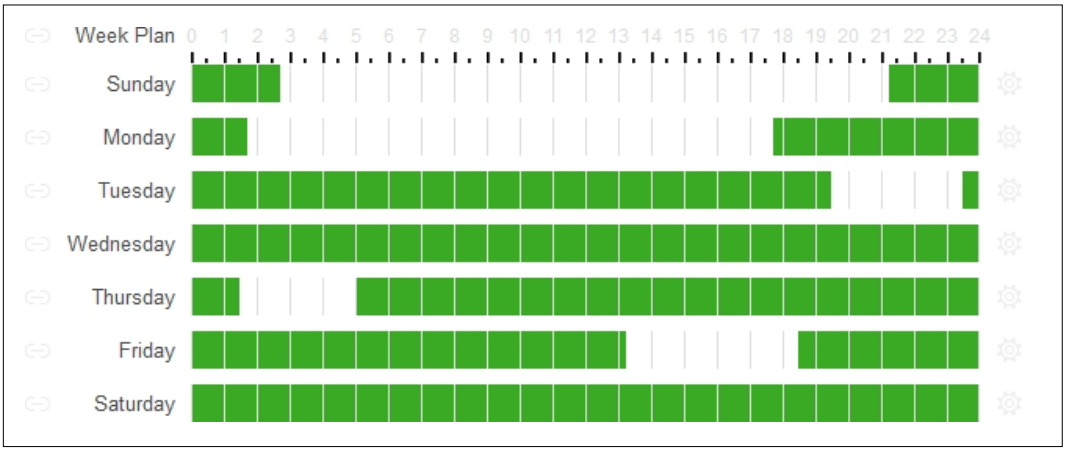
3) Виберіть пристрій, який підтримує тривожний вихід, а потім виберіть інтерфейс тривожного виходу.
4) Увімкніть **автоматичне відкриття** для прив'язки будильника.
5) Встановіть тривалість.

Рисунок 6-2 Налаштування прив'язки тривог



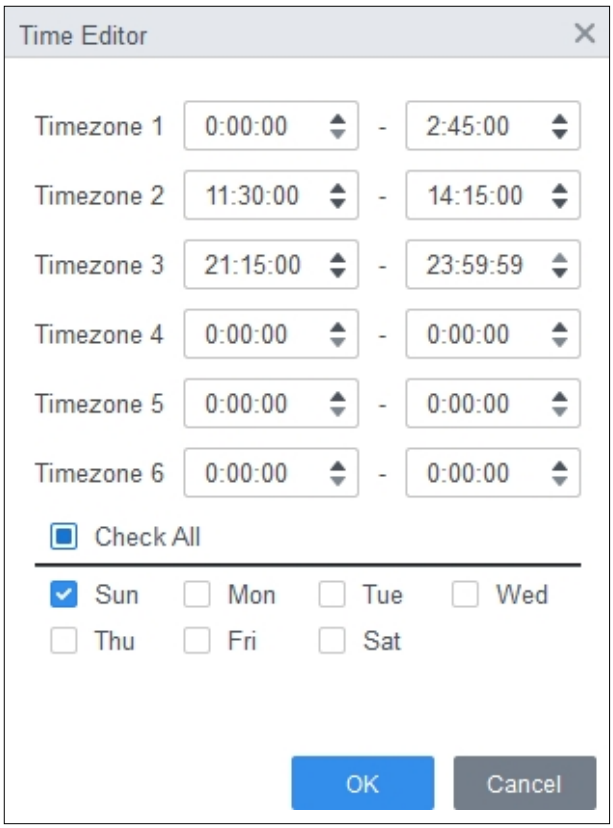
- Встановіть періоди постановки на охорону. Є два способи.
  - ◇ Спосіб 1: Перемістіть курсор, щоб встановити періоди часу. Коли курсор перетвориться на олівець, клацніть, щоб додати періоди; коли курсор перетвориться на гумку, клацніть, щоб відняти періоди. Періоди в зеленій області є активними.

Рисунок 6-3 Встановлення періодів встановлення під охорону (спосіб 1)



  - ◇ Спосіб 2: Перейдіть за посиланням , щоб встановити періоди, а потім натисніть **OK**.

Рисунок 6-4 Встановлення періодів встановлення під охорону (спосіб 2)



Крок 5 (Необов'язково) Натисніть **Копіювати до**, виберіть контролер доступу, до якого потрібно застосувати, а потім натисніть **OK**. Натисніть **Зберегти**.

Крок 6

Додаток 1 Рекомендації з кібербезпеки

Кібербезпека - це не просто модне слово: це те, що стосується кожного пристрою, підключеного до інтернету. IP-відеоспостереження не застраховане від кібер-ризиків, але прийняття базових заходів для захисту і зміцнення мереж і мережевих пристроїв зробить їх менш вразливими до атак. Нижче наведено кілька порад і рекомендацій щодо створення більш захищеної системи безпеки.

Обов'язкові дії, які необхідно виконати для забезпечення мережевої безпеки базового пристрою:

1. **Використовуйте надійні паролі**

   Будь ласка, зверніться до наступних рекомендацій щодо встановлення паролів:

   - Довжина не повинна бути менше 8 символів;
   - Містити принаймні два типи символів; типи символів включають великі та малі літери, цифри та символи;
   - Не містити ім'я облікового запису або ім'я облікового запису в зворотному порядку;
   - Не використовуйте безперервні символи, такі як 123, abc тощо;
   - Не використовуйте символи, що перекриваються, такі як 111, aaa тощо;

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

   - Відповідно до стандартної процедури в технічній галузі, ми рекомендуємо постійно оновлювати прошивку вашого пристрою (наприклад, NVR, DVR, IP-камери тощо), щоб гарантувати, що в системі встановлені найновіші патчі та виправлення безпеки. Коли пристрій підключено до публічної мережі, рекомендується увімкнути функцію "автоперевірки оновлень", щоб своєчасно отримувати інформацію про оновлення прошивки, випущені виробником.
   - Ми рекомендуємо вам завантажити та використовувати останню версію клієнтського програмного забезпечення.

"Корисні" рекомендації щодо покращення мережевої безпеки вашого пристрою:

1. **Фізичний захист**

   Ми рекомендуємо вам забезпечити фізичний захист пристрою, особливо пристроїв зберігання даних. Наприклад, розмістіть пристрій у спеціальній комп'ютерній кімнаті або шафі, а також запровадьте добре продуманий контроль доступу та управління ключами, щоб запобігти фізичним контактам несанкціонованого персоналу, таким як пошкодження обладнання, несанкціоноване підключення знімного пристрою (наприклад, USB-флешки, послідовного порту) тощо.

2. **Регулярно змінюйте паролі**

   Ми рекомендуємо регулярно змінювати паролі, щоб зменшити ризик того, що їх вгадають або зламають.

3. **Вчасно встановлюйте та оновлюйте паролі Скидайте інформацію**

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

4. **Увімкнути блокування облікового запису**

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

5. Зміна стандартних портів HTTP та інших службових портів

Ми рекомендуємо вам змінити стандартні HTTP та інші службові порти на будь-який набір чисел між 1024~65535, щоб зменшити ризик того, що сторонні особи зможуть здогадатися, які порти ви використовуєте.

6. **Увімкнути HTTPS**

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

7. **Прив'язка MAC-адрес**

   Ми рекомендуємо прив'язати IP і MAC-адреси шлюзу до пристрою, щоб зменшити ризик підміни ARP.

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

   Відповідно до бізнес-вимог та вимог керівництва, розумно додавайте користувачів і призначайте їм мінімальний набір дозволів.

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

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

   У разі необхідності настійно рекомендується використовувати безпечні режими, включаючи, але не обмежуючись наступними послугами:

   - SNMP: Виберіть SNMP v3 і налаштуйте надійні паролі шифрування та автентифікації.
   - SMTP: Виберіть TLS для доступу до сервера поштових скриньок.
   - FTP: Виберіть SFTP і встановіть надійні паролі.
   - Точка доступу: Виберіть режим шифрування WPA2-PSK і встановіть надійні паролі.

10. **Зашифрована передача аудіо та відео**

    Якщо вміст ваших аудіо- та відеоданих є дуже важливим або конфіденційним, ми рекомендуємо використовувати функцію шифрування, щоб зменшити ризик викрадення аудіо- та відеоданих під час передачі.

    Нагадуємо, що зашифрована передача може призвести до певної втрати ефективності передачі.

11. **Безпечний аудит**

    - Перевіряйте користувачів в Інтернеті: ми рекомендуємо регулярно перевіряти користувачів в Інтернеті, щоб дізнатися, чи не ввійшли вони в систему без дозволу.
    - Перевірте журнал пристрою: Переглядаючи журнали, ви можете дізнатися IP-адреси, які використовувалися для входу на ваші пристрої та їхні ключові операції.

12. **Журнал мережі**

    Через обмежений обсяг пам'яті пристрою обсяг збереженого журналу обмежений. Якщо вам потрібно зберігати журнал протягом тривалого часу, рекомендується увімкнути функцію мережевого журналу, щоб забезпечити синхронізацію критично важливих журналів з мережевим сервером журналів для трасування.

13. **Побудова безпечного мережевого середовища**

    Для того, щоб краще забезпечити безпеку пристрою та зменшити потенційні кібер-ризики, ми рекомендуємо:

    - Вимкніть функцію мапування портів маршрутизатора, щоб уникнути прямого доступу до пристроїв інтрамережі із зовнішньої мережі.
    - Мережа повинна бути розділена та ізольована відповідно до фактичних потреб мережі. Якщо між двома підмережами немає вимог до зв'язку, рекомендується використовувати VLAN, мережевий розрив та інші технології для розділення мережі, щоб досягти ефекту ізоляції мережі.
    - Встановіть систему автентифікації доступу 802.1x, щоб зменшити ризик несанкціонованого доступу до приватних мереж.
    - Увімкніть функцію фільтрації IP/MAC-адрес, щоб обмежити коло хостів, яким дозволено доступ до пристрою.