Контроллер доступа с распознаванием лиц

Руководство пользователя

Версия 1.0.0

Предисловие

Общий

В этом руководстве описываются функции и операции Контроллера доступа с распознаванием лиц (далее именуемого «Контроллер доступа»). Внимательно прочтите перед использованием устройства и сохраните руководство для дальнейшего использования.

Инструкции по технике безопасности

В руководстве могут встречаться следующие сигнальные слова.

Сигнальные слова	Значение
DANGER	Указывает на высокую потенциальную опасность, которая, если ее не предотвратить, приведет к смерти или серьезным травмам.
WARNING	Указывает на среднюю или низкую потенциальную опасность, которая, если ее не избежать, может привести к легкой или средней травме.
CAUTION	Указывает на потенциальный риск, который, если его не предотвратить, может привести к повреждению имущества, потере данных, снижению производительности или непредсказуемым результатам.
TIPS	Предоставляет методы, которые помогут вам решить проблему или сэкономить время.
NOTE	Предоставляет дополнительную информацию в качестве дополнения к тексту.

История изменений

Версия	Содержание пересмотра	Время выпуска
Версия 1.0.0	Первый выпуск.	Июнь 2023 г.

Уведомление о защите конфиденциальности

Как пользователь устройства или контроллер данных, вы можете собирать персональные данные других лиц, такие как их лицо, отпечатки пальцев и номерной знак. Вам необходимо соблюдать местные законы и правила о защите конфиденциальности, чтобы защищать законные права и интересы других лиц, реализуя меры, которые включают, но не ограничиваются: предоставление четкой и видимой идентификации для информирования людей о существовании зоны наблюдения и предоставление необходимой контактной информации.

О руководстве

- Руководство носит исключительно справочный характер. Между руководством и продуктом могут быть обнаружены незначительные различия.
- Мы не несем ответственности за убытки, возникшие в результате эксплуатации изделия способами, не соответствующими руководству.
- Руководство будет обновляться в соответствии с последними законами и правилами соответствующих юрисдикций. Для получения подробной информации см. бумажное руководство пользователя, используйте наш CD-ROM, отсканируйте QR-код или посетите наш официальный веб-сайт. Руководство предназначено только для справки. Между электронной и бумажной версиями могут быть обнаружены незначительные различия.
- Все проекты и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта

может привести к некоторым различиям между фактическим продуктом и руководством. Пожалуйста, свяжитесь со службой поддержки клиентов для получения последней версии программы и дополнительной документации.

- Могут быть ошибки в печати или отклонения в описании функций, операций и технических данных. В случае возникновения сомнений или споров мы оставляем за собой право окончательного объяснения.
- Обновите программное обеспечение считывателя или попробуйте другое популярное программное обеспечение считывателя, если руководство (в формате PDF) не открывается.
- Все товарные знаки, зарегистрированные товарные знаки и названия компаний в руководстве являются собственностью их владельцев.
- Пожалуйста, посетите наш веб-сайт, обратитесь к поставщику или в службу поддержки клиентов, если при использовании устройства возникли какие-либо проблемы.
- В случае возникновения каких-либо неопределенностей или разногласий мы оставляем за собой право окончательного разъяснения.

Важные меры предосторожности и предупреждения

В этом разделе представлен контент, охватывающий правильное обращение с контроллером доступа, предотвращение опасностей и предотвращение повреждения имущества. Внимательно прочтите перед использованием контроллера доступа и следуйте инструкциям при его использовании.

Требования к транспортировке

Транспортируйте, используйте и храните контроллер доступа при допустимых условиях влажности и температуры.

Требования к хранению

Храните контроллер доступа при допустимых условиях влажности и температуры.

Требования к установке

- Не подключайте адаптер питания к контроллеру доступа, когда адаптер включен.
- Строго соблюдайте местные правила и стандарты электробезопасности. Убедитесь, что напряжение окружающей среды стабильно и соответствует требованиям к электропитанию контроллера доступа.
- Не подключайте контроллер доступа к двум или более типам источников питания, чтобы избежать повреждения контроллера доступа.
- Неправильное использование аккумулятора может привести к возгоранию или взрыву.

- Персонал, работающий на высоте, должен принимать все необходимые меры для обеспечения личной безопасности, включая ношение каски и ремней безопасности.
- Не размещайте контроллер доступа в местах, подверженных воздействию солнечного света или вблизи источников тепла.
- Берегите контроллер доступа от влаги, пыли и копоти.
- Установите контроллер доступа на устойчивую поверхность, чтобы предотвратить его падение.
- Устанавливайте контроллер доступа в хорошо проветриваемом месте и не блокируйте его вентиляцию.
- Используйте адаптер или блок питания для шкафа, предоставленный производителем.
- Используйте шнуры питания, рекомендованные для вашего региона и соответствующие номинальным характеристикам мощности.
- Источник питания должен соответствовать требованиям ES1 в стандарте IEC 62368-1 и быть не выше PS2. Обратите внимание, что требования к источнику питания зависят от этикетки контроллера доступа.
- Контроллер доступа — это электроприбор класса I. Убедитесь, что источник питания контроллера доступа подключен к розетке с защитным заземлением.

Требования к эксплуатации

- Перед использованием проверьте правильность электропитания.

- Не отсоединяйте шнур питания сбоку контроллера доступа, пока адаптер включен.

- Эксплуатируйте контроллер доступа в пределах номинального диапазона входной и выходной мощности.
- Используйте контроллер доступа при допустимых условиях влажности и температуры.
- Не допускайте попадания жидкости на контроллер доступа и не допускайте ее попадания на него. Убедитесь, что на контроллере доступа нет предметов, наполненных жидкостью, чтобы предотвратить попадание жидкости в контроллер.
- Не разбирайте контроллер доступа без профессиональных инструкций.
- Данный продукт является профессиональным оборудованием.
- Контроллер доступа не подходит для использования в местах, где вероятно присутствие детей.

Оглавление

Предисловие.....я

Важные меры предосторожности и предупреждения..... III

1 Обзор..... 1

2 локальных операции.....2

2.1 Базовая процедура настройки..... 2

2.2 Общие значки..... 2

2.3 Экран ожидания..... 3

2.4 Инициализация.....4

2.5 Вход в систему..... 4

2.6 Методы разблокировки.....5

2.6.1 Разблокировка картами..... 5

2.6.2 Разблокировка по лицу.....5

2.6.3 Разблокировка с помощью пароля пользователя..... 5

2.6.4 Разблокировка с помощью пароля администратора..... 5

2.6.5 Разблокировка по QR-коду.....6

2.6.6 Разблокировка по отпечатку пальца..... 6

2.6.7 Разблокировка временным паролем..... 6

2.7 Управление пользователями.....6

2.7.1 Добавление пользователей..... 6

2.7.2 Просмотр информации о пользователе.....9

2.7.3 Настройка пароля разблокировки администратора.....10

2.8 Управление доступом.....10

2.8.1 Настройка комбинаций разблокировки.....10

2.8.2 Настройка будильников.....11

2.8.3 Настройка статуса двери.....13

2.9 Управление посещаемостью.....14

2.9.1 Настройка отделов.....14

2.9.2 Настройка смен.....15

2.9.3 Настройка планов на праздники.....17

2.9.4 Настройка графиков работы.....18

2.9.5 Настройка интервала времени проверки.....21

2.9.6 Настройка режимов присутствия.....21

2.10 Сетевое взаимодействие.....24

2.10.1 Настройка IP-адреса.....25

2.10.2 Настройка активной регистрации.....26

2.10.3 Настройка Wi-Fi....27
2.10.4 Настройка последовательного порта....27
2.10.5 Настройка Wiegand....28
2.11 Системные настройки....29
2.11.1 Настройка времени....29
2.11.2 Настройка параметров лица....31
2.11.3 Настройка громкости....33
2.11.4 Настройка языка....33
2.11.5 Настройки экрана....33
2.11.6 (Необязательно) Настройка параметров отпечатков пальцев....34
2.11.7 Восстановление заводских настроек....34
2.11.8 Перезагрузка устройства....34
2.12 Настройки функций....34
2.13 Управление USB-устройствами....38
2.13.1 Экспорт на USB....38
2.13.2 Импорт с USB....39
2.13.3 Обновление системы....39
2.14 Управление записями....39
2.15 Системная информация....39
2.15.1 Просмотр емкости данных....39
2.15.2 Просмотр версии устройства....39
3 веб-операции....40
3.1 Инициализация....40
3.2 Вход в систему....40
3.3 Сброс пароля....41
3.4 Домашняя страница....42
3.5 Добавление пользователей....42
3.6 Настройка интеркома....46
3.6.1 Использование устройства в качестве SIP-сервера....46
3.6.1.1 Настройка SIP-сервера....46
3.6.1.2 Настройка локальных параметров....47
3.6.1.3 Добавление VTO....48
3.6.1.4 Добавление VTH....49
3.6.1.5 Добавление СУДС....52
3.6.2 Использование VTO в качестве SIP-сервера....53
3.6.2.1 Настройка SIP-сервера....53
3.6.2.2 Настройка локальных параметров....54
3.6.3 Использование платформы в качестве SIP-сервера....55

3.6.3.1 Настройка SIP-сервера.....55
3.6.3.2 Настройка локальных параметров.....57
3.7 Настройка контроля доступа.....58
3.7.1 Настройка основных параметров.....58
3.7.2 Настройка методов разблокировки.....59
3.7.3 Настройка будильников.....61
3.7.4 Настройка глобальных связей тревог (необязательно).....63
3.7.5 Настройка распознавания лиц.....65
3.7.6 Настройка параметров карты.....68
3.7.7 Настройка QR-кода.....69
3.7.8 Настройка расписаний.....69
3.7.8.1 Настройка периодов времени.....69
3.7.8.2 Настройка планов на праздники.....70
3.7.9 Настройка модулей расширения.....72
3.7.10 Настройка функций порта.....72
3.8 Настройка аудио и видео.....73
3.8.1 Настройка видео.....73
3.8.1.1 Настройка канала 1.....73
3.8.1.2 Настройка канала 2.....77
3.8.2 Настройка звуковых подсказок.....80
3.8.3 Настройка обнаружения движения.....80
3.8.4 Настройка локального кодирования.....81
3.9 Настройка сети.....82
3.9.1 Настройка TCP/IP.....82
3.9.2 Настройка Wi-Fi.....84
3.9.3 Настройка порта.....84
3.9.4 Настройка базовой службы.....85
3.9.5 Настройка облачного сервиса.....87
3.9.6 Настройка активной регистрации.....88
3.10 Настройка RS-485.....89
3.11 Настройка Wiegand.....91
3.12 Настройка системы.....92
3.12.1 Управление пользователями.....92
3.12.1.1 Добавление администраторов.....92
3.12.1.2 Добавление пользователей ONVIF.....93
3.12.1.3 Сброс пароля.....94
3.12.1.4 Просмотр пользователей онлайн.....94
3.12.2 Настройка времени.....95

3.12.3 Техническое обслуживание....96
3.12.4 Управление конфигурацией....96
3.12.4.1 Экспорт и импорт файлов конфигурации....96
3.12.4.2 Восстановление заводских настроек по умолчанию....97
3.12.5 Обновление системы....98
3.12.5.1 Обновление файла....98
3.12.5.2 Онлайн-обновление....98
3.12.6 Просмотр информации о версии....98
3.12.7 Просмотр емкости данных....99
3.12.8 Просмотр юридической информации....99
3.13 Персонализация....99
3.13.1 Добавление ресурсов....99
3.13.2 Настройка тем....100
3.13.3 Настройка сочетаний клавиш....103
3.14 Просмотр журналов....105
3.14.1 Системные журналы....105
3.14.2 Журналы администратора....105
3.14.3 Разблокировка журналов....106
3.14.4 Журналы тревог....106
3.14.5 Журналы вызовов....106
3.14.6 Управление USB-устройствами....106
3.15 Емкость данных....107
3.16 Настройки безопасности (необязательно)....107
3.16.1 Статус безопасности....107
3.16.2 Настройка HTTPS....108
3.16.3 Атака и защита....108
3.16.3.1 Настройка брандмауэра....108
3.16.3.2 Настройка блокировки учетной записи....109
3.16.3.3 Настройка защиты от DoS-атак....110
3.16.4 Установка сертификата устройства....111
3.16.4.1 Создание сертификата....111
3.16.4.2 Подача заявки на получение и импорт сертификата CA....112
3.16.4.3 Установка существующего сертификата....113
3.16.5 Установка доверенного сертификата CA....114
3.16.6 Шифрование данных....115
3.16.7 Предупреждение о безопасности....116
4. Упрощенная конфигурация Smart PSS....117
4.1 Установка и вход в систему....117

4.2 Добавление устройств.....117

4.2.1 Добавление по одному..... 117

4.2.2 Добавление партиями..... 118

4.3 Управление пользователями.....119

4.3.1 Настройка типа карты..... 119

4.3.2 Добавление пользователей..... 120

4.3.2.1 Добавление по одному..... 120

4.3.2.2 Добавление партиями..... 121

4.3.3 Назначение разрешения на доступ.....122

4.3.4 Назначение разрешений на посещение.....124

4.4 Управление доступом.....126

4.4.1 Дистанционное открытие и закрытие двери.....126

4.4.2 Настройка «Всегда открыто» и «Всегда закрыто».....127

4.4.3 Мониторинг состояния двери..... 127

Приложение 1. Важные моменты регистрации лица..... 129

Приложение 2. Важные моменты эксплуатации домофона..... 132

Приложение 3. Важные моменты инструкции по регистрации отпечатков пальцев.....133

Приложение 4. Важные моменты сканирования QR-кода..... 135

Приложение 5 Рекомендации по кибербезопасности..... 136

1 Обзор

Контроллер доступа — это панель управления доступом, которая поддерживает разблокировку с помощью лиц, паролей, отпечатков пальцев, карт, QR-кодов и их комбинаций. Благодаря алгоритму глубокого обучения он отличается более быстрым распознаванием и более высокой точностью. Может работать с платформой управления, которая отвечает различным потребностям клиентов.

Он широко используется в парках, жилых районах, бизнес-центрах и на фабриках, а также идеально подходит для таких мест, как офисные здания, правительственные здания, школы и стадионы.

- Конфигурации могут отличаться в зависимости от модели продукта, пожалуйста, обратитесь к фактическому продукту.

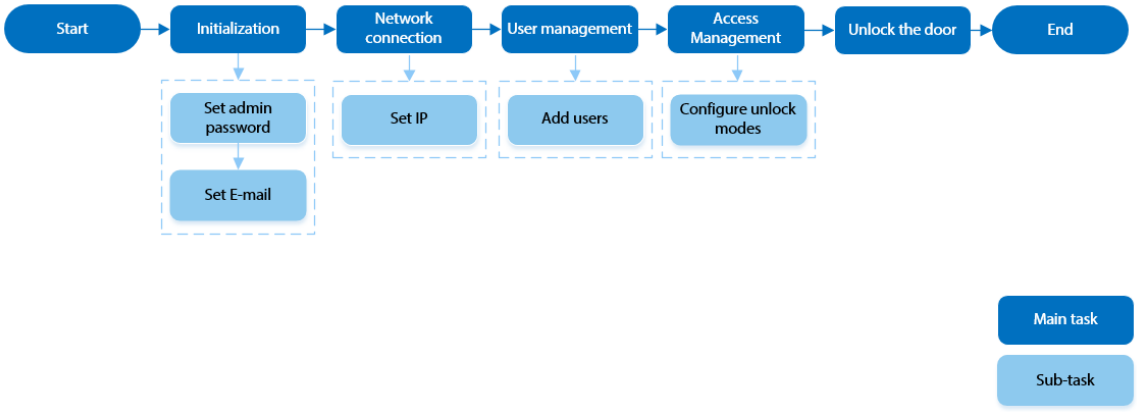
- Устройства с несенсорным экраном должны подключаться к мыши для выполнения конфигураций. В этом руководстве в качестве примера используется устройство с сенсорным экраном.
- Некоторые модели поддерживают подключение модулей расширения, таких как модуль QR-кода, модуль отпечатков пальцев и т. д. Тип модулей расширения, поддерживаемых контроллером доступа, может отличаться, см. фактический продукт.

2 локальных операции

- Конфигурации могут отличаться в зависимости от конкретного продукта.
- Модели с сенсорным экраном не требуют подключения проводной USB-мыши. В этом разделе в качестве примера используются модели с сенсорным экраном.
- Внешние модули расширения доступны только для некоторых моделей.
- Вы можете увидеть, что некоторые тексты пользовательского интерфейса не отображаются из-за ограниченного пространства. Долго нажмите на текст в течение 3 секунд, и он отобразится.

2.1 Базовая процедура настройки

Рисунок 2-1 Базовая процедура настройки



2.2 Общие значки

Таблица 2-1 Описание иконок

Икона	Описание
	Значок главного меню.
	Значок подтверждения.
	Откройте первую страницу списка.
	Откройте последнюю страницу списка.
или	Перейти на предыдущую страницу списка.
или	Перейдите на следующую страницу списка.
	Вернуться в предыдущее меню.
	Включено.
	Выключено.
	Удалить
	Поиск

2.3 Экран ожидания

Вы можете разблокировать дверь с помощью лиц, карты, паролей и QR-кода. Вы также можете совершать звонки через функцию домофона. Методы разблокировки могут различаться в зависимости от модели продукта.

- Если в течение 30 секунд не будет выполнено никаких действий, контроллер доступа перейдет в режим ожидания.
- Это руководство предназначено только для справки. Небольшие различия могут быть обнаружены между экраном ожидания в данном руководстве и на самом устройстве.

Рисунок 2-2 Экран режима ожидания

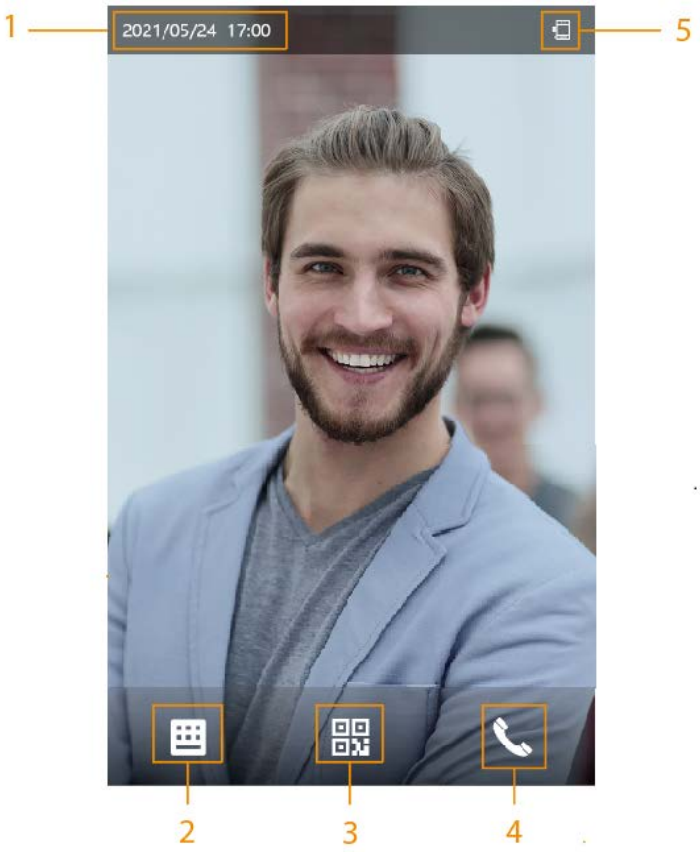


Таблица 2-2 Описание главного экрана

Нет.	Имя	Описание
1	Дата и время	Текущая дата и время.
2	Пароль	Введите пароль пользователя, пароль администратора или временный пароль, чтобы разблокировать дверь.

Нет.	Имя	Описание
3	QR-код	Нажмите на значок QR-кода и отсканируйте QR-код, чтобы разблокировать дверь. Для моделей, которые имеют автономный модуль QR-кода или подключают модуль расширения QR. Значок не будет отображаться. Вы можете просто поместить свой код QR перед линзой контроллера доступа или модуля расширения, он будет автоматически отсканирован.
4	Интерком	● Когда контроллер доступа функционирует как сервер, он может вызывать VTO и VTH. ● Когда платформа управления функционирует как сервер, контроллер доступа может вызывать VTO, VTS и платформу управления. ● При работе с DMSS он может вызывать DMSS.
5	Отображение статуса	Отображает состояние Wi-Fi, сети, модуля расширения, USB и т. д. Wi-Fi и модули расширения доступны только в некоторых моделях.

2.4 Инициализация

При первом использовании или после восстановления заводских настроек вам необходимо выбрать язык на Access Controller, а затем задать пароль и адрес электронной почты для учетной записи администратора. Вы можете использовать учетную запись администратора для входа в главное меню Access Controller и его веб-страницу.

- Если вы забыли пароль администратора, отправьте запрос на сброс на ваш зарегистрированный адрес электронной почты.
- Пароль должен состоять из 8–32 непустых символов и содержать не менее двух типов символы верхнего регистра, строчные буквы, цифры и специальные символы (за исключением ' " ; : &).

2.5 Вход в систему

Войдите в главное меню, чтобы настроить контроллер доступа. Только учетная запись администратора и учетная запись администратора могут войти в главное меню контроллера доступа. При первом использовании используйте учетную запись администратора для входа в экран главного меню, а затем вы сможете создать другие учетные записи администраторов.

Справочная информация

- Учетная запись администратора: может войти в главное меню контроллера доступа, но не имеет прав доступа к двери.
- Учетная запись администратора: может входить в главное меню контроллера доступа и имеет разрешения на доступ к двери.

Процедура

Шаг 1 Нажмите и удерживайте экран ожидания в течение 3 секунд.

Шаг 2 Выберите метод проверки, чтобы войти в главное меню.

- Лицо: Вход в главное меню с помощью распознавания лица.
- Отпечаток пальца: войдите в главное меню, используя отпечаток пальца.

  Функция сканера отпечатков пальцев доступна только в некоторых моделях.
- Перфорация карты: войдите в главное меню, проведя картой по считывателю.
- PWD: Введите идентификатор пользователя и пароль учетной записи администратора.
- admin: Введите пароль администратора для входа в главное меню.

2.6 Методы разблокировки

Вы можете открыть дверь с помощью лица, пароля, отпечатка пальца, карты и других средств.

2.6.1 Разблокировка картами

Приложите карту к зоне считывания, чтобы отпереть дверь.

2.6.2 Разблокировка по лицу

Проверьте личность человека, распознав его лицо. Убедитесь, что лицо находится в центре рамки распознавания лиц.

2.6.3 Разблокировка с помощью пароля пользователя

Введите идентификатор пользователя и пароль, чтобы разблокировать дверь.

Процедура

Шаг 1 Кран  на экране в режиме ожидания.

Шаг 2 Кран**Разблокировать паролем**, а затем введите идентификатор пользователя и пароль. Нажмите

Шаг 3 **хорошо**.

2.6.4 Разблокировка с помощью пароля администратора

Введите только пароль администратора, чтобы разблокировать дверь. Дверь можно разблокировать с помощью пароля администратора, за исключением нормально закрытой двери. Одно устройство допускает только один пароль администратора.

Предпосылки

Пароль администратора был настроен. Подробности см. в разделе "2.7.3 Настройка пароля разблокировки администратора".

Процедура

Шаг 1 Кран  на экране в режиме ожидания.

Шаг 2 Кран**Разблокировать с помощью пароля администратора**, а затем введите пароль администратора.

Шаг 3 Нажми 

Пароль администратора не может быть использован для разблокировки, если статус двери установлен на «всегда» статус закрыт.

2.6.5 Разблокировка по QR-коду

Процедура

Шаг 1 На экране ожидания нажмите .

Шаг 2 Поместите QR-код перед объективом.

2.6.6 Разблокировка по отпечатку пальца

Приложите палец к сканеру отпечатков пальцев. Эта функция доступна только в некоторых моделях.

2.6.7 Разблокировка временным паролем

Откройте дверь временным паролем.

Процедура

Шаг 1 Добавьте контроллер доступа в DMSS.

DMSS сгенерирует временный пароль, который позволит вам разблокировать дверь до истечения срока его действия.

Шаг 2 На главном экране нажмите , а затем нажмите**Разблокировать временным паролем**.

Шаг 3 Введите временный пароль, а затем нажмите

2.7 Управление пользователями

Вы можете добавлять новых пользователей, просматривать список пользователей/администраторов и редактировать информацию о пользователях.

Изображения в данном руководстве приведены только для справки и могут отличаться от фактического продукта.

2.7.1 Добавление пользователей

Процедура

Шаг 1 На**Главное меню**, выбирать**Управление персоналом**>**Создать**

Шаг 2 **пользователя**. Настройте параметры интерфейса.

Рисунок 2-3 Добавить нового пользователя

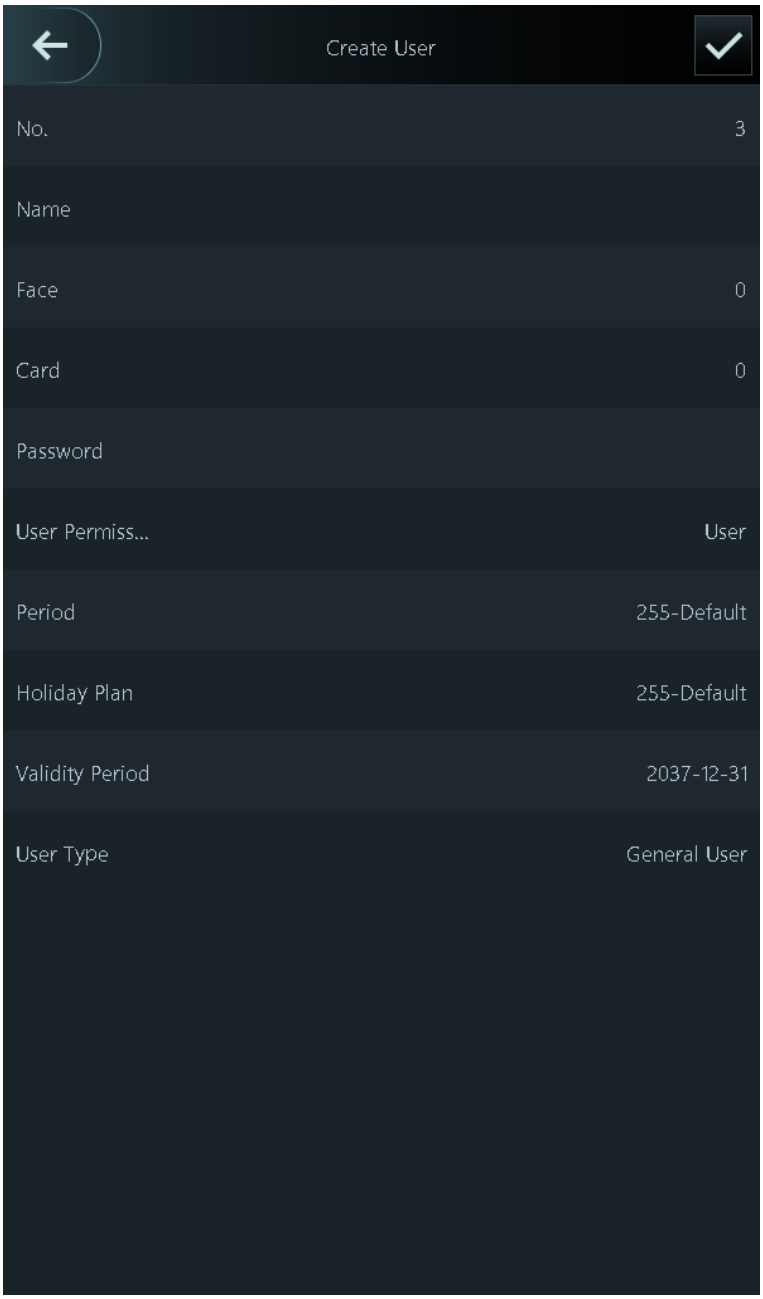


Таблица 2-3 Описание параметров

Параметр	Описание
Нет.	Номер похож на идентификатор сотрудника и может состоять из цифр, букв и их комбинаций, а максимальная длина номера составляет 32 символа.
Имя	Имя может содержать до 30 символов (включая цифры, символы и буквы).

Параметр	Описание
ФП	Регистрация отпечатков пальцев. Пользователь может зарегистрировать до 3 отпечатков пальцев, и вы можете установить отпечаток пальца для отпечатка пальца принуждения. Сигнализация сработает, если отпечаток пальца принуждения будет использован для разблокировки двери.  ● Функция отпечатков пальцев доступна только на некоторых модели. ● Мы не рекомендуем вам устанавливать первый отпечаток пальца в качестве отпечатка пальца под принуждением. ● Один пользователь может установить только один отпечаток пальца под принуждением. ● Функция распознавания отпечатков пальцев доступна, если контроллер доступа поддерживает подключение модуля расширения для распознавания отпечатков пальцев.
Лицо	Поместите свое лицо в рамку, и изображение лица будет захвачено автоматически. Вы можете зарегистрироваться снова, если вы не удовлетворены результатом.
Карточка	Пользователь может зарегистрировать максимум до 5 карт. Введите номер своей карты или проведите ею по считывателю, после чего данные карты будут считаны контроллером доступа. Вы можете включить**Карта принуждения**функция. Сигнализация сработает, если для разблокировки двери будет использована карта принуждения.  Один пользователь может установить только одну карту принуждения.
Пароль	Введите пароль пользователя. Максимальная длина пароля — 8 цифр. Пароль принуждения — это пароль разблокировки + 1. Например, если пароль пользователя — 12345, пароль принуждения будет 12346. Сигнализация принуждения сработает, если для разблокировки двери будет использован пароль принуждения.
Разрешение пользователя	● **Пользователь**: Пользователи имеют только разрешение на доступ к двери или учет рабочего времени. ● **Админ**: Администраторы могут настраивать контроллер доступа, помимо разрешений на доступ к двери и посещаемость.
Период	Люди могут открывать дверь или принимать посетителей в течение определенного периода. Подробнее о настройке периодов см. в разделе "3.7.8.1 Настройка периодов времени".
План отпуска	Люди могут открывать дверь или принимать посетителей во время определенного праздника. Подробнее о настройке периодов см. в разделе "3.7.8.2 Настройка планов праздников".
Срок действия	Установите дату, когда истекает срок действия разрешений на доступ к двери и присутствие человека.

Параметр	Описание
Тип пользователя	● **Обычный пользователь**: Обычные пользователи могут разблокировать дверь. ● **Черный список пользователей**: Когда пользователи из черного списка открывают дверь, срабатывает сигнализация черного списка. ● **Гость Пользователь**: Гости могут разблокировать дверь в течение определенного периода или определенное количество раз. После истечения определенного периода или времени разблокировки они не смогут разблокировать дверь. ● **Патрульный пользователь**: Патрульные пользователи могут регистрировать присутствие на контроллере доступа, но у них нет доступа к двери разрешения. ● **VIP-пользователь**: Когда VIP откроет дверь, обслуживающий персонал получит уведомление. ● **Другой пользователь**: Когда они отпирают дверь, она остается открытой еще 5 секунд. ● **Пользовательский пользователь 1/Пользовательский пользователь 2**: То же самое и с обычными пользователями.
Отделение	Выберите отделы, что полезно при настройке расписаний отделов. О том, как создавать отделы, см. в разделе "2.9.1 Настройка отделов". Эта функция доступна только в некоторых моделях.
Режим расписания	● Расписание работы отдела: применение расписаний работы отдела к пользователю. ● Персональное расписание: применение персональных расписаний к пользователю. О том, как настроить личные или отдельные расписания, см. в разделе «2.9.4 Настройка рабочих расписаний». ◇ Эта функция доступна только в некоторых моделях. ◇ Если вы установите режим расписания на отдел расписание здесь, личное расписание у вас есть настроено для пользователя в**Посещаемость**>**Расписание Конфигурации**>**Личное расписание**становятся недействительными.

Шаг 3 Кран.

2.7.2 Просмотр информации о пользователе

Процедура

Шаг 1 На**Главное меню**, выбирать**Управление персоналом**>**Список пользователей**, или выберите**Пользователь**>**Список администраторов**. Просмотреть всех

Шаг 2 добавленных пользователей и учетные записи администраторов.

- : Разблокировать с помощью пароля.
- : Разблокировка путем считывания карты.

- : Разблокировка с помощью распознавания лица.
- : Разблокировка с помощью отпечатка пальца.

Связанные операции

На**Пользователь**экране вы можете управлять добавленными пользователями.

- Поиск пользователей: нажмите и введите имя пользователя.
- Редактировать пользователей: нажмите на пользователя, чтобы изменить информацию о нем.
- Удалить пользователей
  - ◇ Удалить по одному: выберите пользователя, а затем нажмите .
  - ◇ Удалять партиями:
    - ○ На**Список пользователей**экран, нажмите для удаления всех пользователей.
    - ○ На**Список администраторов**экран, нажмите для удаления всех пользователей-администраторов.

2.7.3 Настройка пароля разблокировки администратора

Вы можете разблокировать дверь, введя только пароль администратора. Пароль не ограничен типами пользователей. Для одного устройства разрешен только один пароль разблокировки администратора.

Процедура

Шаг 1 На**Главное меню**экран, выберите**Пользователь**>**Пароль разблокировки администратора**.

Шаг 2 Кран**Пароль разблокировки администратора**, а затем введите пароль. Включите функцию

Шаг 3 разблокировки администратора.

2.8 Управление доступом

Вы можете настроить параметры для дверей, такие как режим разблокировки, связь с сигнализацией и расписания дверей. Доступные режимы разблокировки могут отличаться в зависимости от модели продукта.

2.8.1 Настройка комбинаций разблокировки

Используйте карту, отпечаток пальца, лицо или пароль или их комбинации для разблокировки двери. Доступные режимы разблокировки могут различаться в зависимости от модели продукта.

Процедура

Шаг 1 Выбирать**Управление контролем доступа**>**Разблокировать комбинацию**.

Шаг 2 Выберите методы разблокировки.

Чтобы отменить выбор, коснитесь выбранного метода еще раз.

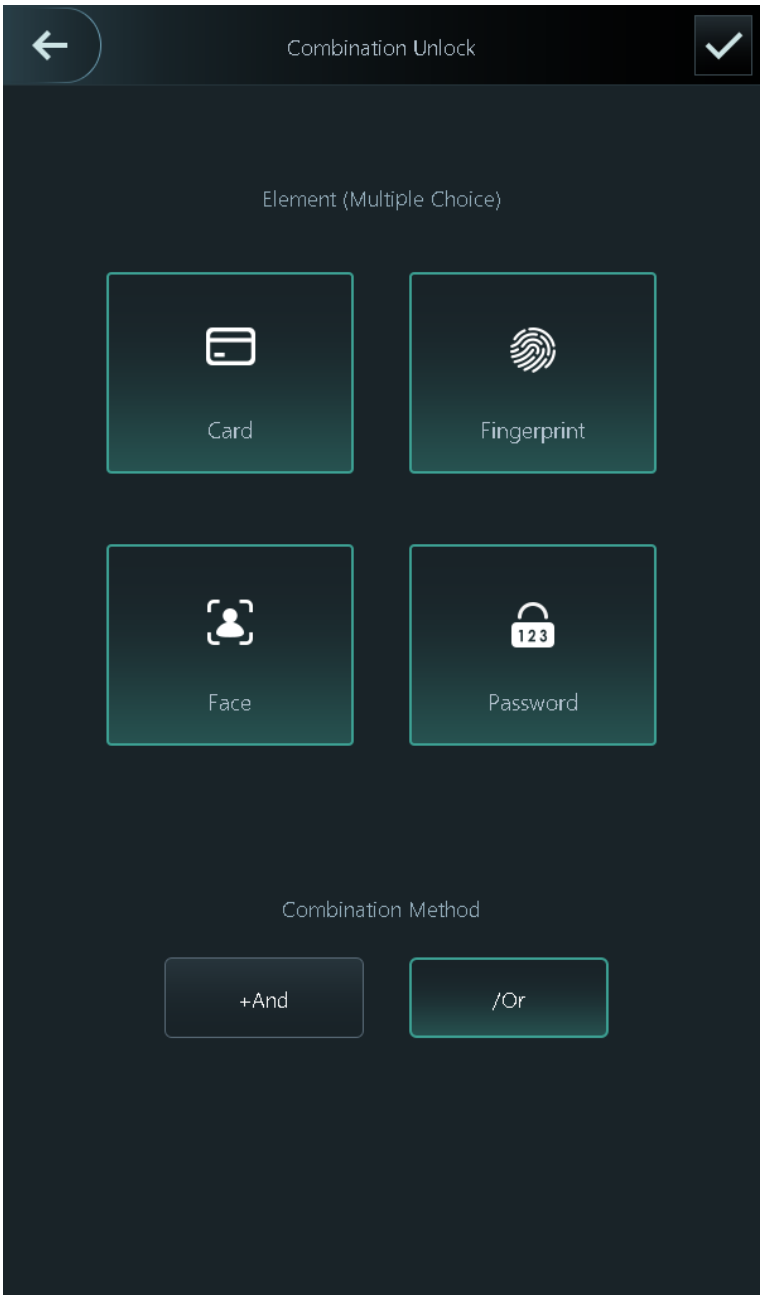
Шаг 3 Нажмите +**И**или**/Или**для настройки комбинаций.

- **+И**: Проверьте все выбранные методы разблокировки, чтобы открыть дверь.

  Людям необходимо пройти проверку в следующем порядке: карта, отпечатки пальцев, лицо и пароль.

- **/Или**: Подтвердите один из выбранных методов разблокировки, чтобы открыть дверь.

Рисунок 2-4 Элемент (множественный выбор)



Шаг 4 Кран для сохранения изменений.

2.8.2 Настройка будильников

При несанкционированном доступе к входу или выходу сработает сигнализация.

Процедура

Шаг 1 Выбирать**Управление контролем доступа**>**Тревога**.

Шаг 2 Включите тип будильника.

Типы сигналов тревоги могут различаться в зависимости от модели продукта.

Рисунок 2-5 Сигнализация

Таблица 2-4 Описание параметров сигнализации

Параметр	Описание
Антипассбэк	Пользователи должны подтвердить свою личность как для входа, так и для выхода; в противном случае сработает сигнализация. Это помогает предотвратить передачу держателями карт своих карт другим лицам для предоставления им доступа. Когда включена функция anti-passback, держатель карты должен покинуть защищенную зону через выходной считыватель, прежде чем система снова предоставит ему доступ. Людям нужно провести картой по считывателю "in", чтобы войти в защищенную зону, и провести ее по считывателю "out", чтобы выйти из нее. Пока последовательность "in, out, in, out и т. д.", система будет работать нормально. ● Если человек войдет после верификации, но выйдет, не пройдя верификацию, при повторной попытке входа сработает сигнализация, и в доступе ему будет отказано. ● Если человек войдет без проверки, но выйдет после проверки, при повторной попытке входа сработает сигнализация, и в доступе ему будет отказано. Если контроллер доступа может подключить только один замок, проверка на Контроллер доступа означает направление "вход", а проверка на внешнем считывателе карт означает направление "выход" по умолчанию. Вы можете изменить настройки на платформе управления.
Принуждение	Сигнализация сработает, если для разблокировки двери будет использована карта принуждения, пароль принуждения или отпечаток пальца принуждения.

Параметр	Описание
Вторжение	Если датчик двери включен, при ненормальном открытии двери сработает сигнализация о вторжении.
Дверь заперта	Сигнализация сработает, если дверь останется открытой дольше определенного времени. Оно может быть от 1 до 9999 секунд.

2.8.3 Настройка статуса двери

Процедура

Шаг 1 На**Главное меню**экран, выберите**Управление контролем доступа**>**Блокировка статуса конфигурации**.

Шаг 2 Установить статус двери.

Рисунок 2-6 Состояние блокировки

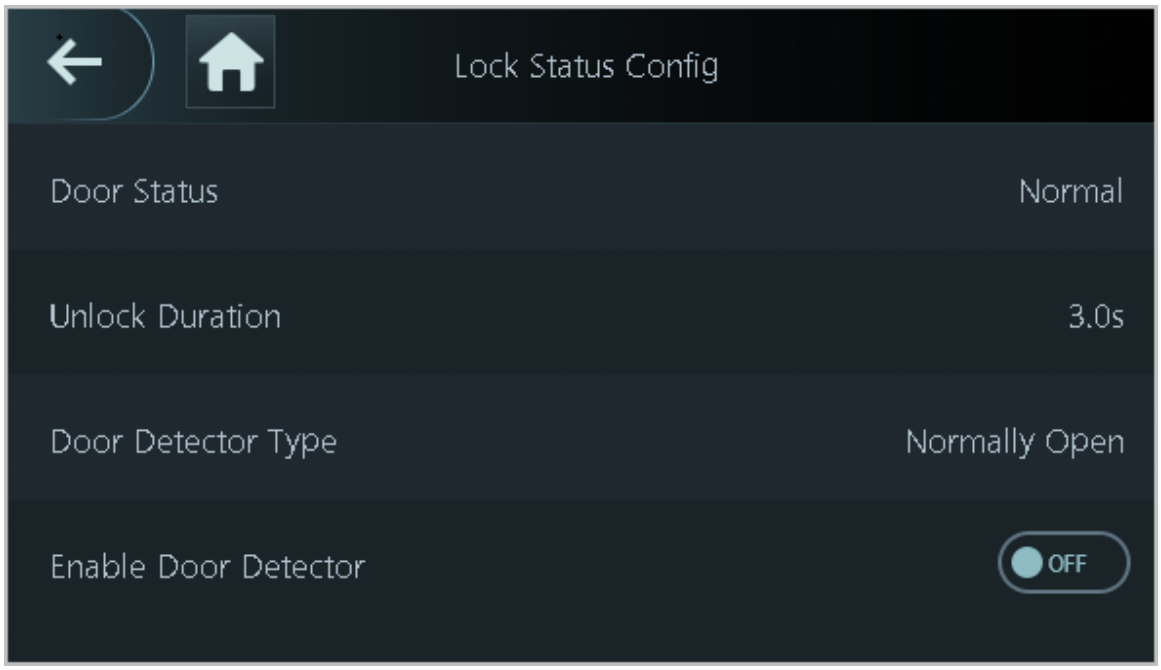


Таблица 2-5 Описание параметров

Параметр	Описание
Состояние двери	● **Нормально открытый**: Дверь все время остается незапертой. ● **Нормально закрытый**: Дверь все время остается запертой. ● **Нормальный**: Если**Нормальный**Если выбран этот параметр, дверь будет запираться и отпираться в соответствии с вашими настройками.
Продолжительность разблокировки	После того, как человеку предоставлен доступ, дверь останется открытой в течение определенного времени, чтобы он мог пройти.
Тип дверного детектора	С дверным детектором, подключенным к вашему устройству, сигналы тревоги могут срабатывать при ненормальном открытии или закрытии дверей. Дверной детектор включает 2 типа, включая NC-детектор и NO-детектор. ● Нормально закрытый: датчик находится в замкнутом положении, когда дверь или окно закрыты. ● Нормально открытый: Разомкнутая цепь создается, когда окно или дверь фактически закрыты.

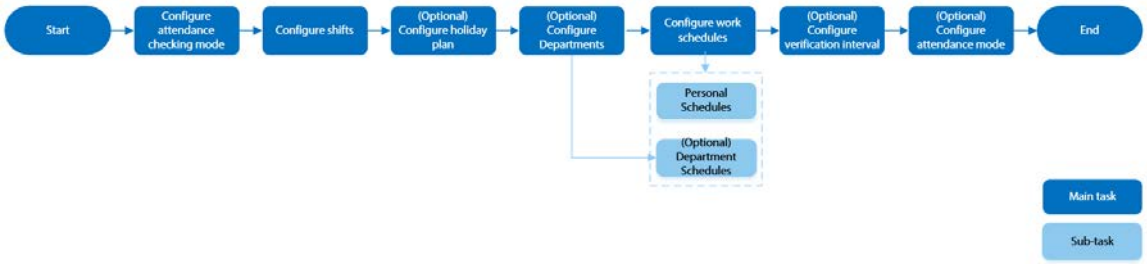
Параметр	Описание
Включить детектор двери	Сигнализация о вторжении и истечении времени выхода из дома вступит в силу только после включения этой функции.

2.9 Управление посещаемостью

Посещаемость времени поддерживает управление посещаемостью как на локальном устройстве, так и на Smart PSS Lite. В этом разделе в качестве примера используется только настройка посещаемости на локальном устройстве.

Эта функция доступна только на некоторых моделях серии 4,3 дюйма.

Рисунок 2-7 Схема конфигурации учета рабочего времени



2.9.1 Настройка отделов

Процедура

Шаг 1 Выбирать**Посещаемость**>**Настройки отдела**.

Шаг 2 Выберите отдел, а затем переименуйте его.

Есть 20 департаментов по умолчанию. Мы рекомендуем вам переименовать их.

Рисунок 2-8 Создание отделов

Шаг 3 Кран.

2.9.2 Настройка смен

Настройте смены, чтобы определить правила посещения рабочего времени. Сотрудники должны приходить на работу в запланированное время начала смены и уходить в назначенное время окончания, за исключением случаев, когда они решают поработать сверхурочно.

Процедура

Шаг 1 Выбирать**Посещаемость**>**Конфигурация смены**.

Шаг 2 Выберите смену.

Нажмите, чтобы просмотреть больше смен. Вы можете настроить до 24

Шаг 3 смен. Настройте параметры смены.

Рисунок 2-9 Создание смен

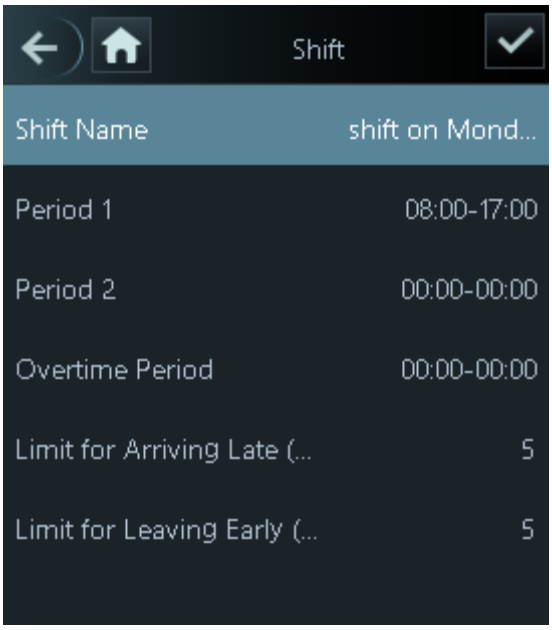
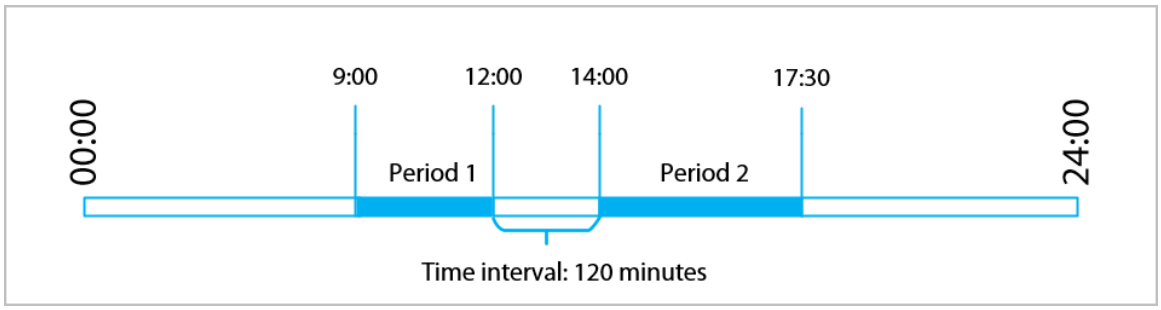


Таблица 2-6 Описание параметров сдвига

Параметр	Описание
Название смены	Введите название смены.
Период 1	Укажите временной диапазон, в течение которого сотрудники могут отмечать начало и конец рабочего дня. Если вы устанавливаете только один период посещения, сотрудники должны отмечать приход и уход в назначенное время, чтобы избежать аномалии в их записях о посещении. Например, если вы устанавливаете период с 08:00 до 17:00, сотрудники должны отмечать приход до 08:00 и уход с 17:00 и далее. Если вы установите 2 периода присутствия, эти 2 периода не могут пересекаться. Сотрудники должны отмечать приход и уход для обоих периодов.
Период 2	
Период сверхурочной работы	Сотрудники, которые приходят на работу или уходят с работы в течение определенного периода, будут считаться работающими сверх обычного рабочего времени.
Лимит опоздания (мин)	Определенное количество времени может быть предоставлено сотрудникам, чтобы они могли приходить на работу немного позже и уходить немного раньше. Например, если обычное время прихода на работу — 08:00, то допустимый период может быть установлен в 5 минут для сотрудников, которые приходят к 08:05, чтобы не считаться опоздавшими.
Лимит раннего ухода (мин)	

- Если интервал времени между двумя периодами является четным числом, вы можете разделить интервал времени на 2 и назначить первую половину интервала первому периоду, что будет временем выхода. Вторую половину интервала следует назначить второму периоду как время прихода.

Рисунок 2-10 Временной интервал (четное число)

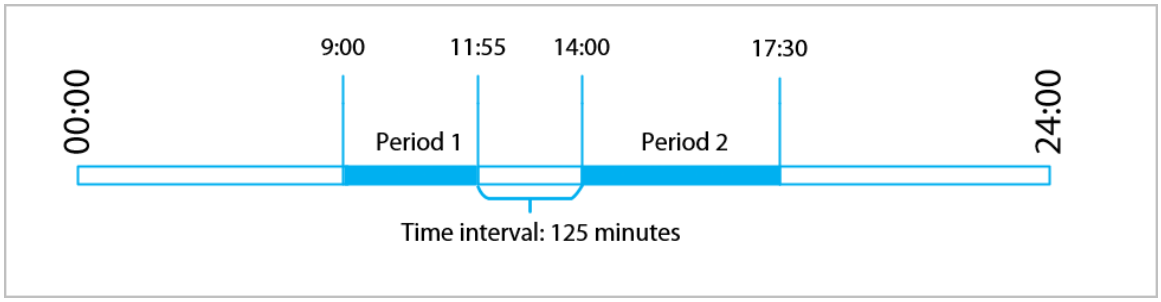


Например: если интервал составляет 120 минут, то время ухода с работы для периода 1 составляет с 12:00 до 12:59, а время прихода для периода 2 составляет с 13:00 до 14:00.

Если человек уходит с работы несколько раз в течение периода 1, то действительным будет последнее время, а если они регистрируются несколько раз в течение периода 2, наиболее раннее время будет считаться действительным.

- Когда интервал времени между двумя периодами является нечетным числом, наименьшая часть интервала будет отнесена к первому периоду, что будет временем выхода. Наибольшая часть интервала будет отнесена ко второму периоду как время прихода.

Рисунок 2-11 Временной интервал (четное число)



Например: если интервал составляет 125 минут, то время ухода с работы для периода 1 — с 11:55 до 12:57, а время прихода с работы для периода 2 — с 12:58 до 14:00. Период 1 длится 62 минуты, а период 2 — 63 минуты.

Если человек уходит с работы несколько раз в течение периода 1, то действительным будет последнее время, а если они регистрируются несколько раз в течение периода 2, наиболее раннее время будет считаться действительным.

Все время посещения точное до секунды. Например, если обычное время прихода время установлено на 8:05 утра, сотрудник, который придет на работу в 8:05:59 утра, не будет считаться опоздание. Но сотрудник, прибывший в 8:06 утра, будет отмечен как опоздавший на 1 минуту.

Шаг 4 Кран.

2.9.3 Настройка планов на праздники

Настройте планы праздников, чтобы установить периоды, в течение которых посещаемость не будет отслеживаться.

Процедура

Шаг 1 Выбирать**Посещаемость**>**Конфигурация смены**>**Праздничный день**.

Шаг 2 Нажмите, чтобы добавить планы на отпуск.

Шаг 3 Настройте параметры.

Рисунок 2-12 Создание планов отпуска

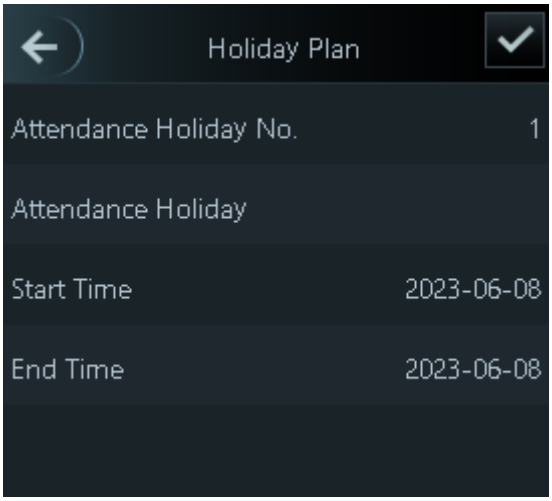


Таблица 2-7 Описание параметров

Параметр	Описание
Посещаемость Праздник №	Число праздника.
Посещаемость праздника	Название праздника.
Время начала	Время начала и окончания праздника.
Время окончания	

Шаг 4 Кран.

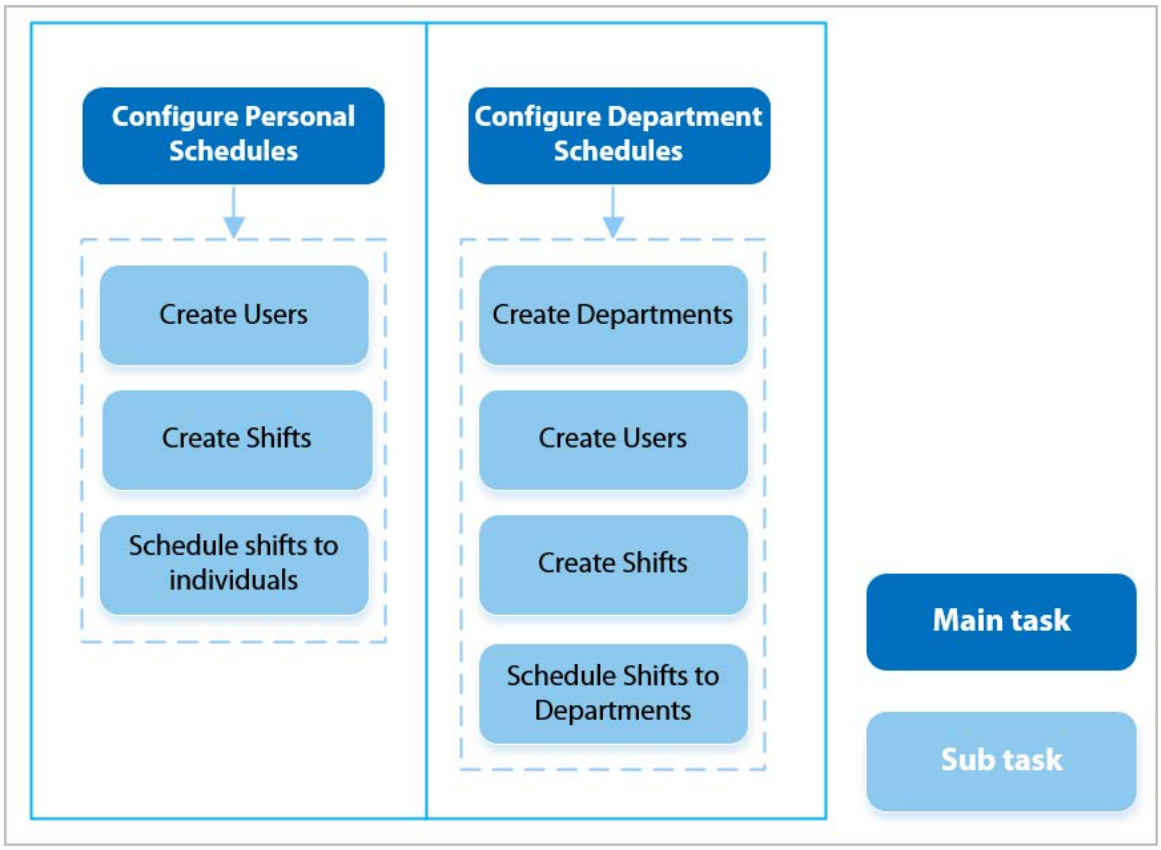
2.9.4 Настройка графиков работы

График работы обычно относится к дням в месяце и часам в день, которые сотрудник должен находиться на своей работе. Вы можете создать различные типы графиков работы на основе разных лиц или отделов, а затем сотрудники должны будут следовать установленным графикам работы.

Справочная информация

Воспользуйтесь блок-схемой для настройки личных графиков или графиков отделов.

Рисунок 2-13 Настройка графиков работы



Процедура

Шаг 1 Выбирать**Посещаемость**>**Расписание Конфигурации**.

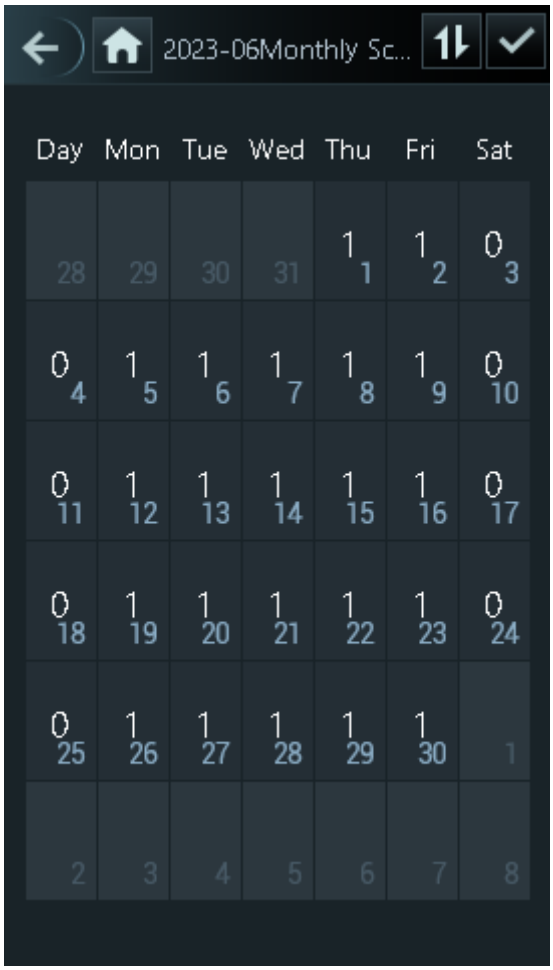
Шаг 2 Установите графики работы для отдельных лиц.

1. Нажмите**Личное расписание**.
2. Введите идентификатор пользователя, а затем нажми
3. В календаре выберите день, а затем смену. Смена запланирована на этот день.

Вы можете установить графики работы только на текущий и следующий месяц.

- 0 указывает на перерыв.
- От 1 до 24 указывает количество определенных смен. О том, как настроить смены, см. «2.9.2 Настройка смен».
- 25 указывает на командировку.
- 26 указывает на отпуск.

Рисунок 2-14 График смен для отдельных лиц



4. Нажмит

Шаг 3 Установите графики работы для отделов. 1.

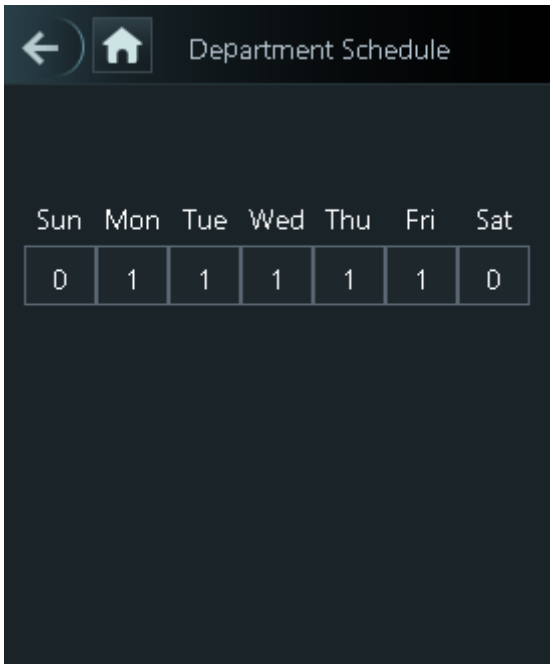
Нажмите**Расписание работы отдела**.

2. Нажмите на отдел, а затем выберите смены на неделю.

Смены планируются на неделю.

- 0 указывает на покой.
- 1–24 указывает количество определенных смен. О том, как настроить смены, см. в разделе «2.9.2 Настройка смен».
- 25 указывает на командировку.
- 26 указывает на отпуск.

Рисунок 2-15 Планирование смен в отделе



Определенный график работы составляется на недельный цикл и будет применяться ко всем сотрудникам в отделение.

Шаг 4 Кран.

2.9.5 Настройка интервала времени проверки

Если сотрудник отмечает приход и уход с работы несколько раз в течение установленного периода, действительным будет считаться самое раннее время.

Процедура

Шаг 1 Выбирать**Посещаемость**>**Интервал проверки (сек)**.

Шаг 2 Введите временной интервал, а затем нажмите.

2.9.6 Настройка режимов присутствия

При регистрации прихода или ухода с работы вы можете установить режимы учета посещаемости, чтобы определить статус посещаемости.

Процедура

Шаг 1 На экране главного меню выберите**Посещаемость**>**Настройки режима**. Давать

Шаг 2 возможность**Локальный или удаленный**, а затем установите режим присутствия.

Записи о посещаемости также будут синхронизированы с платформой управления.

Рисунок 2-16 Режим присутствия

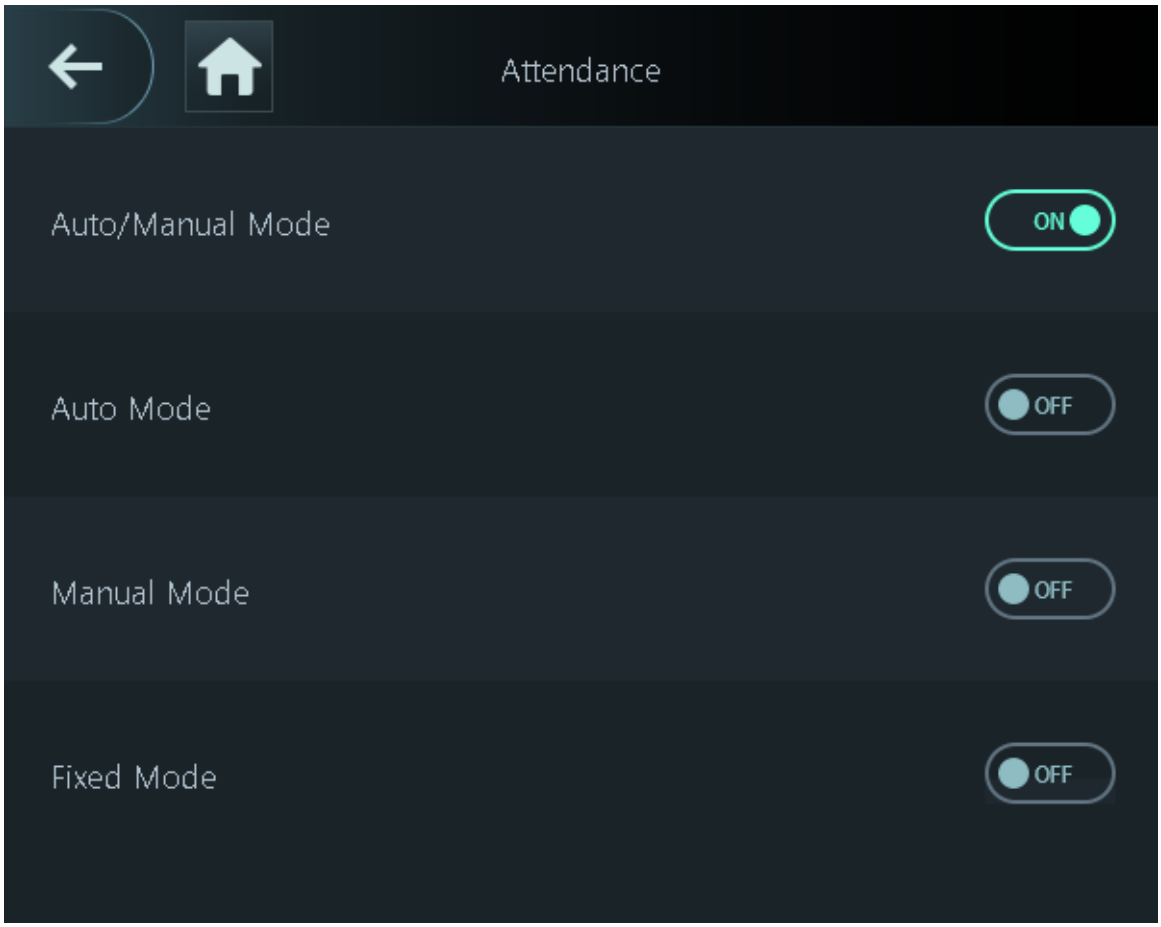


Таблица 2-8 Режим посещаемости

Параметр	Описание
Автоматический/ручной режим	Статус посещаемости отображается на экране автоматически после того, как вы зарегистрировались на работе или ушли с работы, но вы также можете вручную изменить свой статус посещаемости.
Автоматический режим	На экране автоматически отображается статус вашего посещения после того, как вы зарегистрировались на работе или ушли с работы.
Ручной режим	Выберите вручную свой статус посещения при регистрации прихода или ухода.
Фиксированный режим	При регистрации вашего прихода или ухода на экране все время будет отображаться заданный статус посещаемости.

Шаг 3 Выберите режим посещения.

Шаг 4 Настройте параметры режима присутствия.

Рисунок 2-17 Автоматический режим/ручной режим

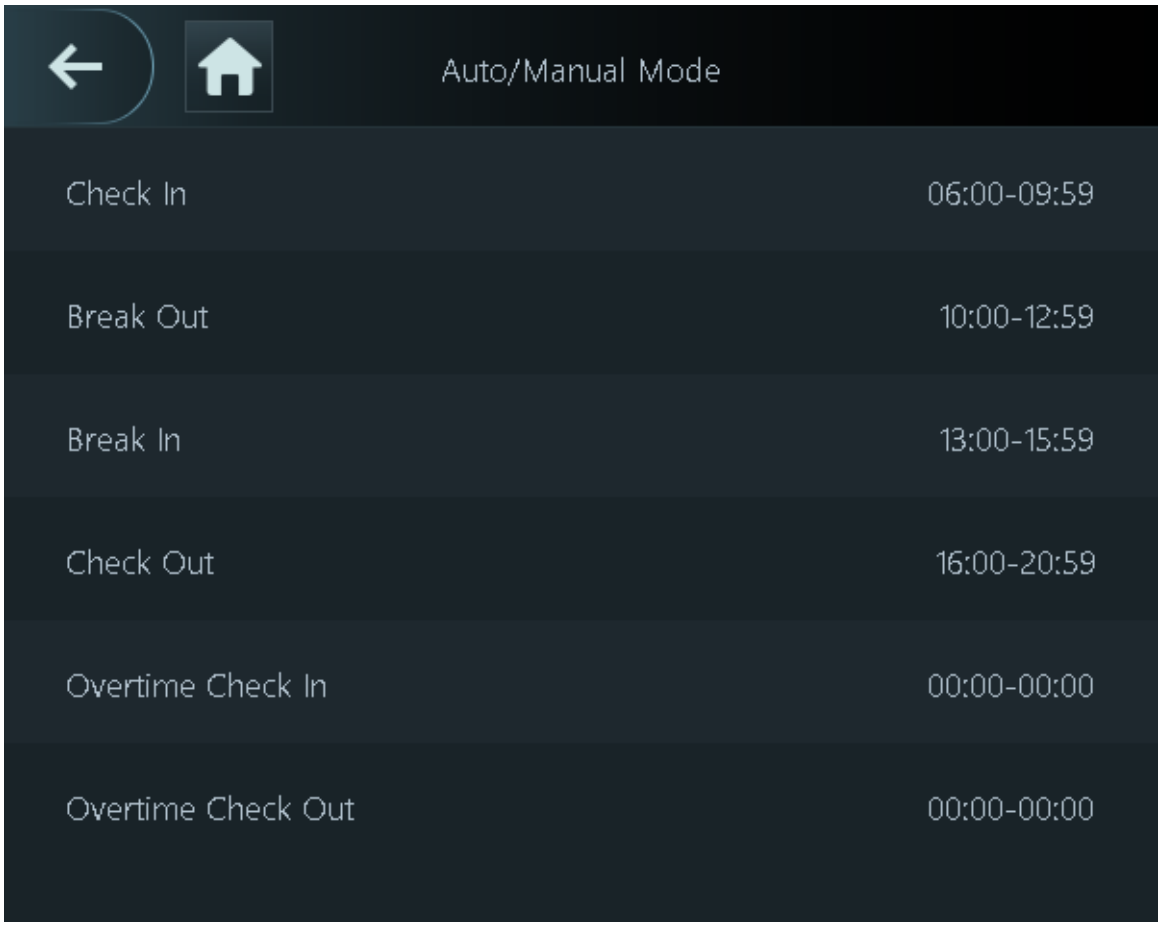


Рисунок 2-18 Фиксированный режим

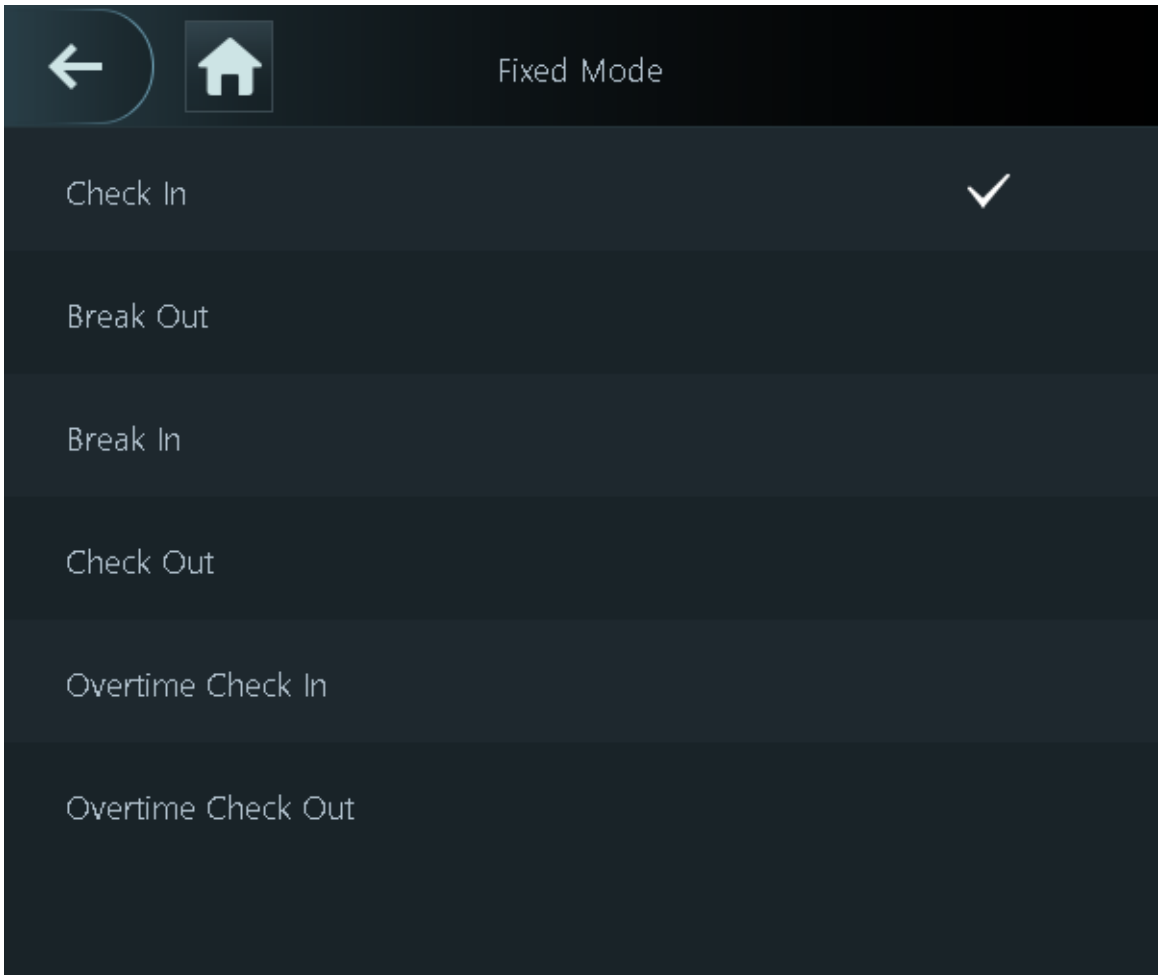


Таблица 2-9 Параметры режима посещаемости

Параметры	Описание
Регистрироваться	Зарегистрируйтесь, когда начинается ваш обычный рабочий день.
Разразиться	Отметьте время ухода с работы, когда начнется перерыв.
Вламываться	Отметьте время окончания перерыва.
Проверить	Отметьте время ухода с работы в начале вашего обычного рабочего дня.
Сверхурочная регистрация	Отметьте начало сверхурочной работы.
Сверхурочная проверка	По окончании сверхурочной работы отмечайте свой уход с работы.

2.10 Сетевое взаимодействие

Настройте сеть, последовательный порт и порт Wiegand для подключения контроллера доступа к сети.

Последовательный порт и порт Wiegand могут отличаться в зависимости от модели контроллера доступа.

2.10.1 Настройка IP-адреса

Установите IP-адрес для контроллера доступа, чтобы подключить его к сети. После этого вы можете войти на веб-страницу и платформу управления, чтобы управлять контроллером доступа.

Процедура

Шаг 1 На**Главное меню**, выбирать**Настройки связи**>**Сеть**>**IP-адрес**.

Шаг 2 Установите IP-адрес.

Рисунок 2-19 Конфигурация IP-адреса

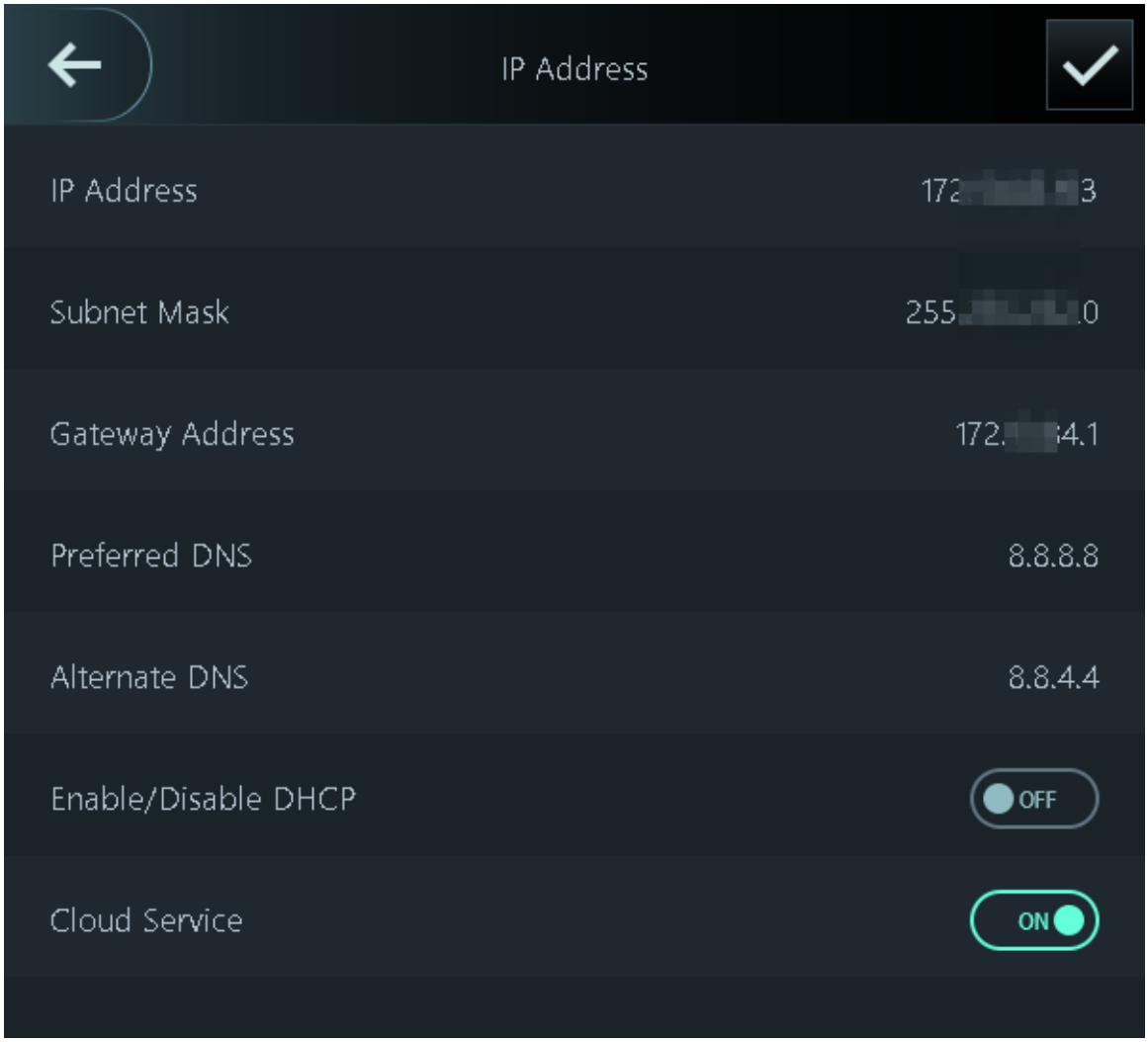


Таблица 2-10 Параметры конфигурации IP

Параметр	Описание
IP-адрес/Маска подсети/Адрес шлюза	IP-адрес, маска подсети и IP-адрес шлюза должны находиться в одном сегменте сети.
Предпочтительный DNS	IP DNS-сервера.
Альтернативный DNS	Альтернативный IP-адрес DNS-сервера.

Параметр	Описание
Включить/выключить DHCP	Это сокращение от Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста). При включении DHCP контроллеру доступа автоматически назначаются IP-адрес, маска подсети и шлюз.
Облачный сервис	Управляйте устройствами без использования DDNS, настраивайте сопоставление портов и развертывайте транзитные серверы.

2.10.2 Настройка активной регистрации

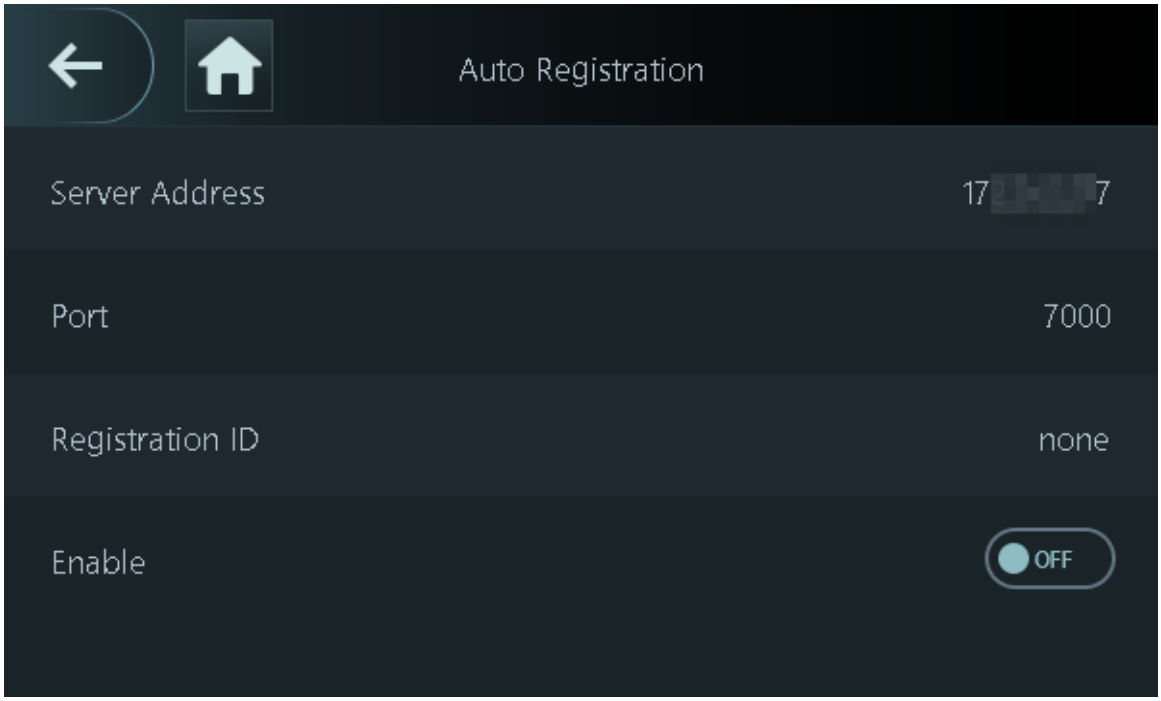
Добавьте устройство на платформу управления, чтобы вы могли управлять им с этой платформы.

Процедура

Шаг 1 На**Главное меню**, выбирать**Коммуникация**>**Сеть**>**Автоматическая регистрация**.

Чтобы не подвергать систему рискам безопасности и потере данных, контролируйте управление разрешения платформы.

Рисунок 2-20 Активная регистрация



Шаг 2 Включите функцию автоматической регистрации и задайте параметры.

Таблица 2-11 Автоматическая регистрация

Параметр	Описание
Адрес сервера	IP-адрес платформы управления.
Порт	Номер порта платформы управления.

Параметр	Описание
Регистрационный идентификатор	Введите идентификатор устройства (определяется пользователем). При добавлении контроллера доступа к платформе управления регистрационный идентификатор, который вы вводите на платформе управления, должен соответствовать определенному регистрационному идентификатору на контроллере доступа.

Шаг 3 Включите функцию.

2.10.3 Настройка Wi-Fi

Вы можете подключить контроллер доступа к сети через сеть Wi-Fi.

Процедура

Шаг 1 На**Главное меню**, выбирать**Коммуникация**>**Сеть**>**Wi-Fi**.

Шаг 2 Включите Wi-Fi.

Функция Wi-Fi доступна только в некоторых моделях.

Шаг 3 Кран для поиска доступных беспроводных сетей.

Шаг 4 Выберите беспроводную сеть и введите пароль.

Если система не находит сеть Wi-Fi, нажмите**SSID**чтобы ввести имя Wi-Fi.

Шаг 5 Нажмите .

2.10.4 Настройка последовательного порта

Процедура

Шаг 1 На**Главное меню**, выбирать**Настройки связи**>**Последовательный порт**.

Шаг 2 Выберите тип порта.

Таблица 2-12 Описание порта

Внешнее устройство	Описание
Контроллер доступа	Выбирать**Контроллер доступа**когда контроллер доступа функционирует как считыватель карт, и контроллер доступа будет отправлять данные контроллеру доступа для управления доступом. Тип выходных данных: ● Номер карты: выводит данные на основе номера карты, когда пользователи проводят своей картой, чтобы отпереть двери; выводит данные на основе номера первой карты пользователя, когда пользователи используют другие методы разблокировки. ● Нет.: Выводит данные на основе идентификатора пользователя.
Кардридер	Контроллер доступа подключается к считывателю карт.
Читатель (ОСДП)	Контроллер доступа подключается к считывателю карт по протоколу OSDP.

Внешнее устройство	Описание
Модуль безопасности управления дверью	Кнопка выхода из двери, управление замком и пожарная связь становятся неэффективными после включения модуля безопасности.
Турникет	Когда контроллер доступа подключен к турникету, а плата контроллера доступа турникета подключена к внешнему модулю QR-кода или модулю считывания карт, плата будет передавать данные проверки на турникет.

2.10.5 Настройка Wiegand

Контроллер доступа поддерживает как режим ввода, так и режим вывода Wiegand.

Процедура

Шаг 1 На веб-странице выберите**Настройки связи**>**Виганд**.

Шаг 2 Выберите Wiegand.

- Выбирать**Вход Wiegand**при подключении внешнего считывателя карт к контроллеру доступа.
- Выбирать**Выход Виганда**когда контроллер доступа функционирует как считыватель карт, и вам необходимо подключить его к контроллеру или другому терминалу доступа.

Рисунок 2-21 Выход Wiegand

Таблица 2-13 Описание выхода Wiegand

Параметр	Описание
Тип выхода Wiegand	Выберите формат Wiegand для считывания номеров карт или идентификационных номеров. ● **Виганд26**: Считывает 3 байта или 6 цифр. ● **Виганд34**: Считывает 4 байта или 8 цифр. ● **Виганд66**: Считывает 8 байт или 16 цифр.
Ширина импульса	Введите ширину импульса и интервал импульса выхода Wiegand.

Параметр	Описание
Интервал импульса	
Тип выходных данных	Выберите тип выходных данных. ● **Нет.**: Система выводит данные на основе идентификатора пользователя. Формат данных — шестнадцатеричный или десятичный. ● **Номер карты**: Система выводит данные на основе номера первой карты пользователя.

Шаг 3 Нажмите**Применять**.

2.11 Системные настройки

2.11.1 Настройка времени

Настройте системное время, такое как дата, время и NTP.

Процедура

Шаг 1 На**Главное меню**, выбирать**Системные настройки**>**Время**.

Шаг 2 Настройте системное время.

Рисунок 2-22 Время

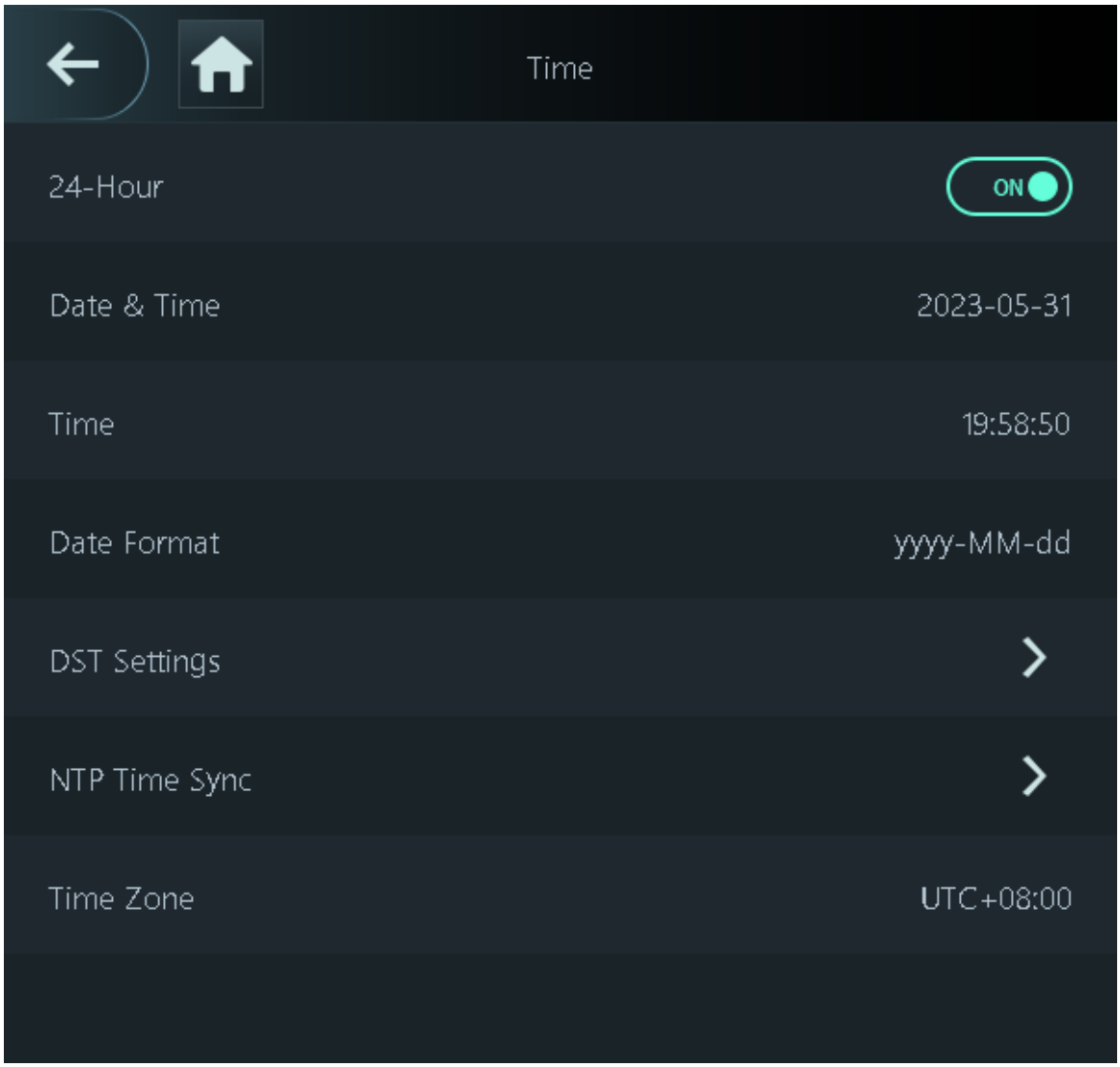


Таблица 2-14 Описание временных параметров

Параметр	Описание
24-часовая система	Время отображается в 24-часовом формате.
Дата и время	Назначьте дату.
Время	Установите время.
Формат даты	Выберите формат даты.
Настройка летнего времени	1. Нажмите**Настройка летнего времени**и включите его. 2. Выбрать**Дата**или**Неделя**из**летнее время**Список типов. 3. Введите время начала и время окончания. 4. Нажмит

Параметр	Описание
Синхронизация времени NTP	Сервер сетевого протокола времени (NTP) — это машина, выделенная в качестве сервера синхронизации времени для всех клиентских компьютеров. Если ваш компьютер настроен на синхронизацию с сервером времени в сети, ваши часы будут показывать то же время, что и сервер. Когда администратор меняет время (на летнее время), все клиентские машины в сети также будут обновлены. 1. Нажмите**Проверка НТП**, а затем включите его. 2. Настройте параметры. ● **Адрес сервера**: Введите IP-адрес NTP-сервера, и контроллер доступа автоматически синхронизирует время с NTP-сервером. ● **Порт**: Введите порт NTP-сервера. ● **Интервал**: Введите интервал синхронизации времени.
Часовой пояс	Выберите часовой пояс.

2.11.2 Настройка параметров лица

Процедура

Шаг 1 В главном меню выберите**Системные настройки**>**Конфигурация параметров**

Шаг 2 **лица**. Настройте параметры лица, а затем нажмите .

Рисунок 2-23 Параметр лица (01)

Таблица 2-15 Описание параметров лица

Имя	Описание
Порог распознавания лица	Отрегулируйте уровень точности распознавания лиц. Более высокий порог означает более высокую точность и меньший уровень ложного распознавания.
Максимальное отклонение угла распознавания лица	Установите наибольший угол, под которым лицо может быть расположено для обнаружения лица. Чем больше значение, тем больше диапазон для угла лица. Если угол, под которым расположено лицо, не входит в заданный диапазон, оно может быть обнаружено неправильно.
Расстояние между зрачками	Для успешного распознавания требуется определенное количество пикселей между глазами, называемое зрачковым расстоянием. Значение по умолчанию — 45 пикселей. Это число меняется в зависимости от размера лица и расстояния между лицом и линзой. Если взрослый человек находится на расстоянии 1,5 метра от линзы, зрачковое расстояние обычно составляет 50–70 пикселей.
Действительный интервал лиц (сек)	Если лицо человека успешно верифицировано слишком много раз, контроллер доступа выдает запрос об успешной верификации в течение определенного интервала времени.
Недействительный интервал лиц (сек)	Если человеку не удается пройти верификацию лица слишком много раз, контроллер доступа выдает сообщение о неудачной верификации в течение определенного промежутка времени.
Включить антиспуфинг	Это не позволяет людям использовать фотографии, видео, маски и другие заменители для получения несанкционированного доступа.
Включить Beautifier	Украсьте сделанные снимки лиц.
Включить обнаружение шлема	Обнаруживает защитные каски. Дверь не будет разблокирована для людей, которые не носят каску.
Параметры маски	● Режим маски: ◇ **Не обнаруживать**: Маска не обнаруживается при распознавании лица. ◇ **Напоминание о маске**: Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, но доступ ему все равно будет разрешен. ◇ **Без маски вход не разрешен**: Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, и доступ будет запрещен. ● Порог распознавания маски: чем выше порог, тем точнее будет распознавание лица человека в маске и тем ниже будет уровень ложного распознавания.

Имя	Описание
Распознавание нескольких лиц	Распознает от 4 до 6 изображений лиц одновременно. Комбинированная разблокировка не может быть использована с этим, и дверь будет разблокирована, когда один из людей успешно пройдет проверку.  Количество поддерживаемых изображений лиц может различаться в зависимости от модели продукта.
Режим осветителя	● Авто: Подсветка включается в условиях низкой освещенности. ● Отключить: осветитель постоянно выключен.  Эта функция доступна только в некоторых моделях.

2.11.3 Настройка громкости

Вы можете отрегулировать громкость динамика и микрофона.

Процедура

Шаг 1 На**Главное меню**, выбирать**Системные настройки**>**Настройки громкости**.

Шаг 2 Выбирать**Громкость звукового сигнала**или**Громкость микрофона**, а затем нажмите+или− чтобы настроить громкость.

2.11.4 Настройка языка

Измените язык на контроллере доступа.**Главное меню**, выбирать**Системные настройки**> **Язык**, выберите язык для контроллера доступа.

2.11.5 Настройки экрана

Настройте время отключения дисплея и время выхода из системы.

Процедура

Шаг 1 На**Главное меню**, выбирать**Система**>**Настройки экрана**. Кран**Время выхода**

Шаг 2 **из системы**или**Настройки выключения экрана**, а затем нажмите + или− для настройки времени.

- Время выхода из системы: система возвращается в режим ожидания после определенного времени бездействия.
- Настройки выключения экрана: система возвращается к экрану ожидания, а затем экран выключается после определенного времени бездействия. Например, если время выхода из системы установлено на 15 секунд, а время выключения экрана установлено на 30 секунд, система возвращается к экрану ожидания через 15 секунд, а затем экран выключается еще через 15 секунд.

Время выхода из системы должно быть меньше времени выключения экрана.

2.11.6 (Необязательно) Настройка параметров отпечатков пальцев

Настройте точность обнаружения отпечатков пальцев. Чем выше значение, тем выше порог схожести и точность.

Справочная информация

Эта функция доступна только на некоторых моделях, а некоторые поддерживают подключение к отпечатку пальца. модуль расширения.

Процедура

Шаг 1 На**Главное меню**, выбирать**Системные настройки**>**Настройки параметров отпечатков пальцев**.

Шаг 2 Нажмите или , чтобы настроить значение.

2.11.7 Восстановление заводских настроек

Процедура

Шаг 1 На**Главное меню**, выбирать**Системные настройки**>**Заводские настройки по умолчанию**.

Шаг 2 Восстановите заводские настройки, если необходимо. Восстановите заводские настройки, если необходимо.

- **Заводские настройки по умолчанию**: Сбрасывает все конфигурации и данные, за исключением настроек IP и типа модуля расширения.
- **Восстановить настройки по умолчанию (за исключением информации о пользователе и журналов)**: Сбрасывает все конфигурации, за исключением информации о пользователе и журналов.

2.11.8 Перезагрузка устройства

На**Главное меню**, выбирать**Системные настройки**>**Перезапуск**, и контроллер доступа будет перезапущен.

2.12 Настройки функций

На**Главное меню**экран, выберите**Функции**.

Функции могут отличаться в зависимости от модели продукта.

Рисунок 2-24 Функции

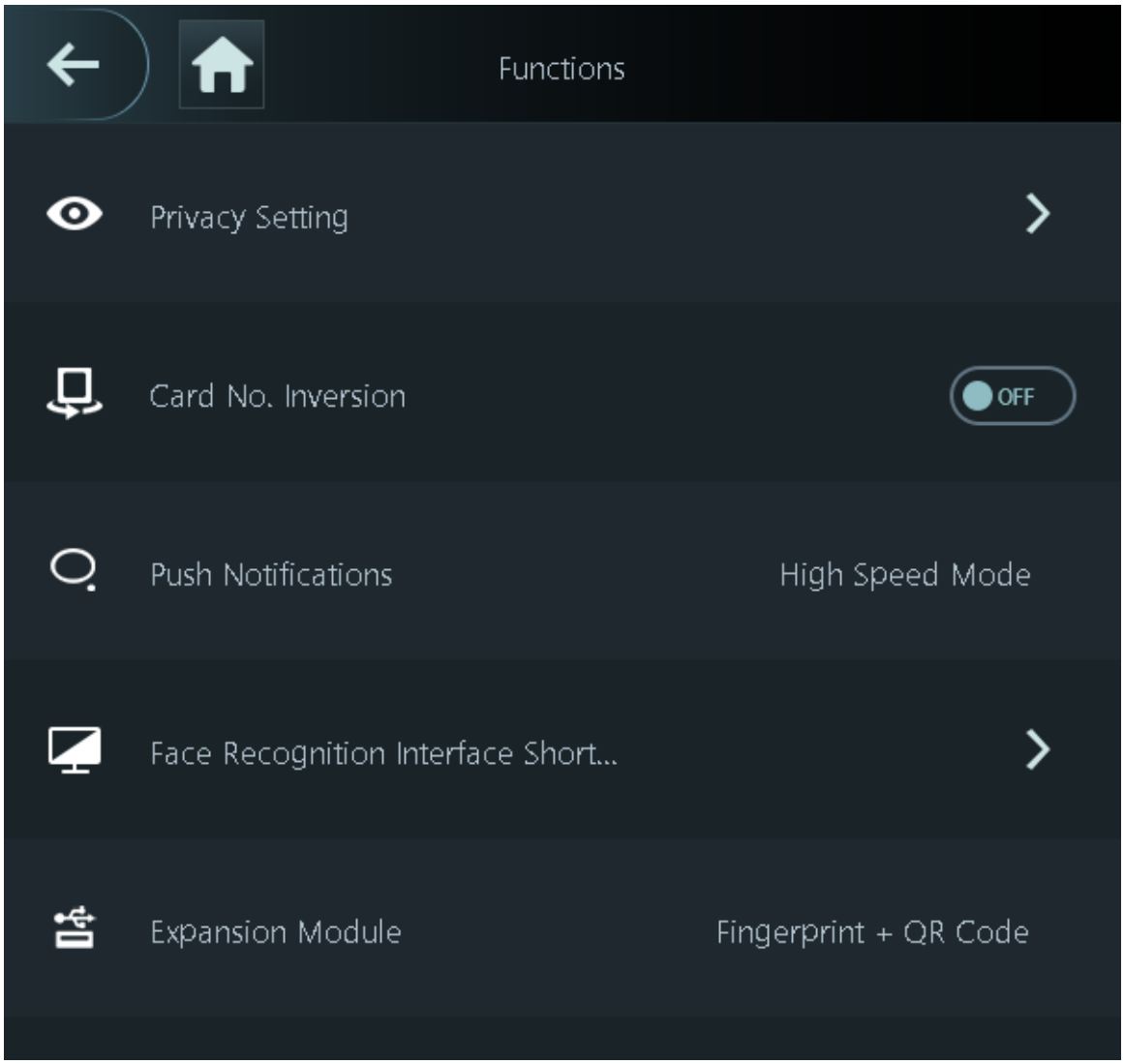


Таблица 2-16 Описание функции

Параметр	Описание
Частная обстановка	● Сброс пароля: пароль можно сбросить, включив эту функцию. ● Включить HTTPS: Hypertext Transfer Protocol Secure (HTTPS) — это протокол для безопасной связи по компьютерной сети. Если включен HTTPS, для доступа к командам CGI будет использоваться HTTPS; в противном случае будет использоваться HTTP.  При включении HTTPS контроллер доступа автоматически перезапустится. ● Включить CGI: Common Gateway Interface (CGI) предлагает стандартный протокол для веб-серверов для выполнения программ, аналогичных тому, как консольные приложения работают на сервере, который динамически генерирует веб-страницы. CG I включен по умолчанию. ● Включить SSH: Secure Shell (SSH) — это криптографический сетевой протокол для безопасной работы сетевых служб в незащищенной сети. Передаваемые данные будут зашифрованы после включения этой функции. ● Изображение отпечатка пальца: Изображение отпечатка пальца отображается при разблокировке с помощью отпечатка пальца.  Эта функция доступна только в некоторых моделях. ● Захват: изображения лиц будут захватываться автоматически, когда люди открывают дверь. Функция включена по умолчанию. ● Очистить все снимки: удалить все автоматически сделанные фотографии.
Номер карты. Инверсия	Когда контроллер доступа подключается к стороннему устройству через входной порт Wiegand, а номер карты, считываемый контроллером доступа, находится в обратном порядке от фактического номера карты. В этом случае вы можете включить эту функцию.

Параметр	Описание
Push-уведомления	Отображает уведомление на экране, когда человек проверяет свою личность на контроллере доступа. ● Режим высокой скорости: система предлагает**Успешно проверено**или**Не авторизовано**на экране. ● Простой режим: отображает идентификатор пользователя, имя и время проверки после предоставления доступа, а также отображает**Не авторизовано**и время авторизации после отказа в доступе. ● Стандарт: отображает зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время проверки после предоставления доступа, а также отображает**Не авторизовано**и время проверки после отказа в доступе. ● Контрастный режим: отображает захваченное изображение лица и зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время авторизации после предоставления доступа, а также отображает**Не авторизовано**после отказа в доступе.
Ярлык интерфейса распознавания лиц	Выберите методы проверки личности на экране ожидания. ● Пароль: его значок отображается на экране в режиме ожидания. ● QR-код: его значок отображается на экране в режиме ожидания. ● Дверной звонок: его значок отображается на экране в режиме ожидания. ◇ Звонок: нажмите значок звонка на экране режима ожидания, и контроллер доступа зазвонит. ◇ Будильник: нажмите на значок колокольчика, и внешнее устройство сигнализации зазвонит. Эта функция доступна только в некоторых моделях. ◇ Настройка рингтона: выберите рингтон ◇ Время рингтона (сек): Установите время звонка (1-30 секунд). Значение по умолчанию — 3. ● Вызов: его значок отображается на экране в режиме ожидания. ● Тип вызова: ◇ Вызов комнаты: нажмите значок вызова в режиме ожидания и введите номер комнаты, чтобы совершить звонок. ◇ Центр управления вызовами: нажмите значок вызова в режиме ожидания, а затем позвоните в центр управления. ◇ Пользовательская комната для звонков: нажмите значок звонка на экране ожидания, чтобы позвонить в заранее определенную комнату. Убедитесь, что контроллер доступа добавлен в DMSS. ● Включить SIP: вы можете включить SIP, чтобы настроить контроллер доступа на SIP-сервер.

Параметр	Описание
Модуль расширения	Выберите модуль расширения, и контроллер доступа перезагрузится. ● отображается в правом углу экрана в режиме ожидания, что означает, что настройка прошла успешно. ● отображается в правом углу экрана ожидания, что означает сбой настройки. ● Модуль расширения доступен только в некоторых моделях. ● Модуль расширения не поддерживает горячую замену. ● Конфигурация для модуля расширения остается не изменится даже после восстановления заводских настроек системы.

2.13 Управление USB-устройствами

Вы можете использовать USB для обновления контроллера доступа, а также экспортировать или импортировать информацию о пользователях или записи о посещаемости через USB.

- Перед экспортом данных или обновлением убедитесь, что USB-накопитель вставлен в контроллер доступа. система. Чтобы избежать сбоя, не вытаскивайте USB и не выполняйте никаких операций Access Контролер во время процесса.
- Для экспорта информации с контроллера доступа на другие устройства необходимо использовать USB-накопитель. Лицо Импорт изображений через USB не допускается.
- Импорт/экспорт записей о посещаемости доступен только на некоторых моделях.

2.13.1 Экспорт на USB

Вы можете экспортировать данные из контроллера доступа на USB. Экспортированные данные зашифрованы и не могут быть отредактированы.

Процедура

Шаг 1 На**Главное меню**, выбирать**USB-управление**>**USB-экспорт**. Выберите тип

Шаг 2 данных, который вы хотите экспортировать, а затем нажмите**ХОРОШО**.

- После экспорта данных в Excel их можно редактировать.
- USB-диск поддерживает формат FAT32, а емкость хранилища составляет 4 ГБ—128 ГБ.

2.13.2 Импорт с USB

Вы можете импортировать данные с USB-накопителя в контроллер доступа.

Процедура

Шаг 1 На**Главное меню**, выбирать**USB-управление**>**USB-импорт**. Выберите тип

Шаг 2 данных, который вы хотите экспортировать, а затем нажмите**ХОРОШО**.

2.13.3 Обновление системы

Обновите систему контроллера доступа через USB.

Процедура

Шаг 1 Переименуйте файл обновления в «update.bin», поместите его в корневой каталог USB-накопителя, а затем вставьте USB-накопитель в контроллер доступа.

Шаг 2 На**Главное меню**, выбирать**USB-управление**>**Обновление через USB**. Кран

Шаг 3 **ХОРОШО**.

Контроллер доступа перезагрузится после завершения обновления.

Не выключайте контроллер доступа во время обновления.

2.14 Управление записями

В главном меню выберите**Управление записями**>**Поиск записей разблокировки**. Отображаются записи разблокировки. Вы можете искать записи по идентификатору пользователя.

2.15 Системная информация

Вы можете просмотреть объем данных и версию устройства.

2.15.1 Просмотр емкости данных

На**Главное меню**, выбирать**Системная информация**>**Емкость данных**, вы можете просмотреть емкость хранилища каждого типа данных.

2.15.2 Просмотр версии устройства

На**Главное меню**, выбирать**Системная информация**>**Версия устройства**, вы можете просмотреть версию устройства, такую как серийный номер, версию программного обеспечения и многое другое.

3 веб-операции

На веб-странице вы также можете настроить и обновить контроллер доступа.

Веб-конфигурации различаются в зависимости от модели контроллера доступа.

3.1 Инициализация

Инициализируйте контроллер доступа при первом входе на веб-страницу или после восстановления заводских настроек контроллера доступа.

Предпосылки

Убедитесь, что компьютер, используемый для входа на веб-страницу, находится в той же локальной сети, что и контроллер доступа.

Процедура

Шаг 1 Откройте браузер, перейдите по IP-адресу (адрес по умолчанию — 192.168.1.108) контроллера доступа.

Мы рекомендуем вам использовать последнюю версию Chrome или Firefox.

Шаг 2 Выберите язык на контроллере доступа.

Шаг 3 Установите пароль и адрес электронной почты, следуя инструкциям на экране.

- Пароль должен состоять из 8–32 непустых символов и содержать не менее двух типы следующих символов: заглавные, строчные, цифры и специальные символы (исключая ' " ; : &). Установите пароль высокой степени безопасности, следуя паролю подсказка по силе.
- Сохраняйте пароль в безопасности после инициализации и регулярно меняйте его, чтобы повысить безопасность.

3.2 Вход в систему

Процедура

Шаг 1 Откройте браузер, введите IP-адрес контроллера доступа в поле**Адрес**и нажмите клавишу Enter.

Шаг 2 Введите имя пользователя и пароль.

- Имя администратора по умолчанию — admin, а пароль — тот, который вы установили. во время инициализации. Мы рекомендуем вам регулярно менять пароль администратора для повышения безопасности.
- Если вы забыли пароль администратора, вы можете нажать**Забыли пароль?**Для подробности,

Шаг 3 Нажмите**Авторизоваться**.

3.3 Сброс пароля

Если вы забыли пароль администратора, сбросьте пароль с помощью электронного письма, отправленного по ссылке.

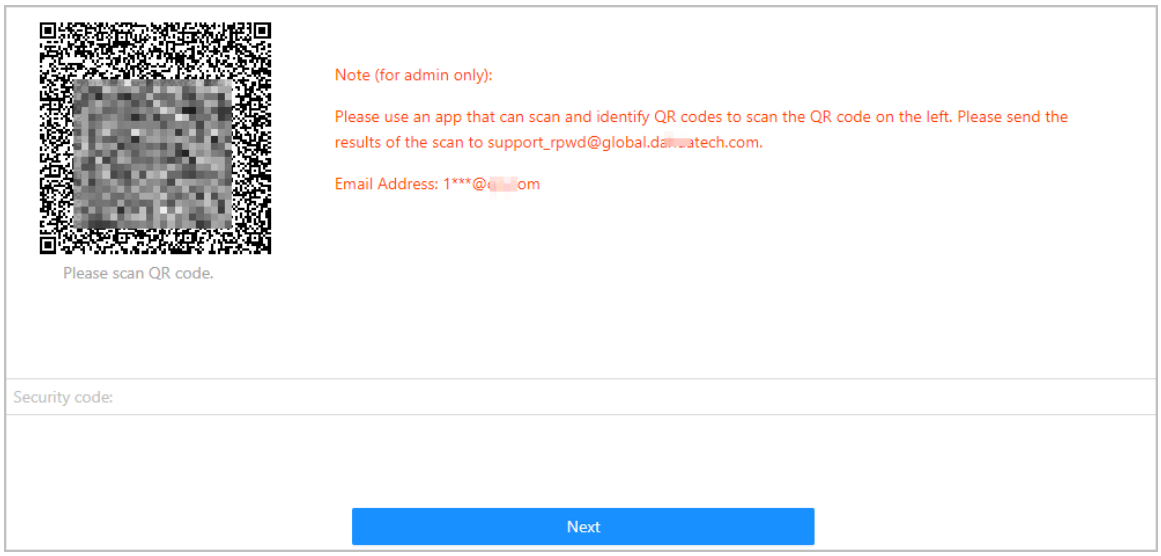
Процедура

Шаг 1 На странице входа нажмите**Забыли пароль**.

Шаг 2 Внимательно прочитайте подсказку на экране, а затем нажмите

Шаг 3 **ХОРОШО**. Отсканируйте QR-код, и вы получите код безопасности.

Рисунок 3-1 Сброс пароля



- При сканировании одного и того же QR-кода будет сгенерировано до двух кодов безопасности. Если код безопасности стал недействительным, обновите QR-код и отсканируйте снова.
- После сканирования QR-кода вы получите код безопасности на указанный вами адрес электронной почты. адрес. Используйте код безопасности в течение 24 часов после его получения. В противном случае он будет становятся недействительными.
- Если неправильный код безопасности будет введен 5 раз подряд, учетная запись администратора будет заблокирована. заморожено на 5 минут.

Шаг 4 Введите код безопасности.

Шаг 5 Нажмите**Следующий**.

Шаг 6 Сбросьте и подтвердите пароль.

Пароль должен состоять из 8–32 непустых символов и содержать не менее двух из следующих символов: следующие типы символов: заглавные буквы, строчные буквы, цифры и специальные символы (исключая ' " ; : &).

Шаг 7 Нажмите**ХОРОШО**.

3.4 Домашняя страница

Домашняя страница отображается после успешного входа в систему.

Рисунок 3-2 Домашняя страница

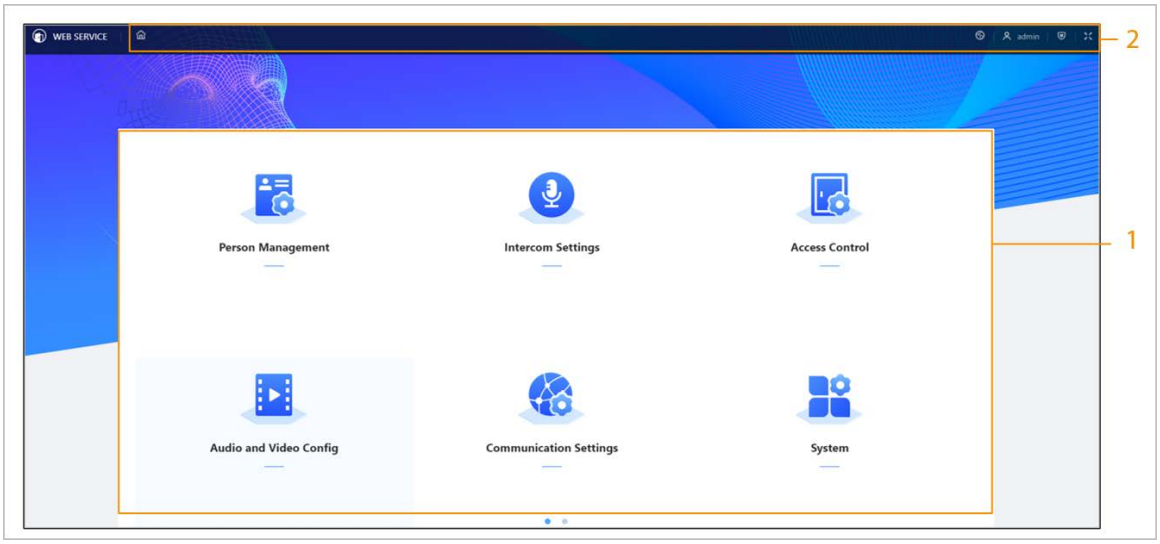


Таблица 3-1 Описание домашней страницы

Нет.	Описание
1	Главное меню.
2	• : Войдите на домашнюю страницу. • : Отображение на весь экран. • : Введите**Безопасность**страница. • admin: Выйдите из системы или перезагрузите устройство. • : Выберите язык на устройстве.

3.5 Добавление пользователей

Процедура

Шаг 1 На главной странице выберите**Управление персоналом**, а затем нажмите**Добавлять**.

Шаг 2 Настройте информацию о пользователе.

Рисунок 3-3 Добавление пользователей

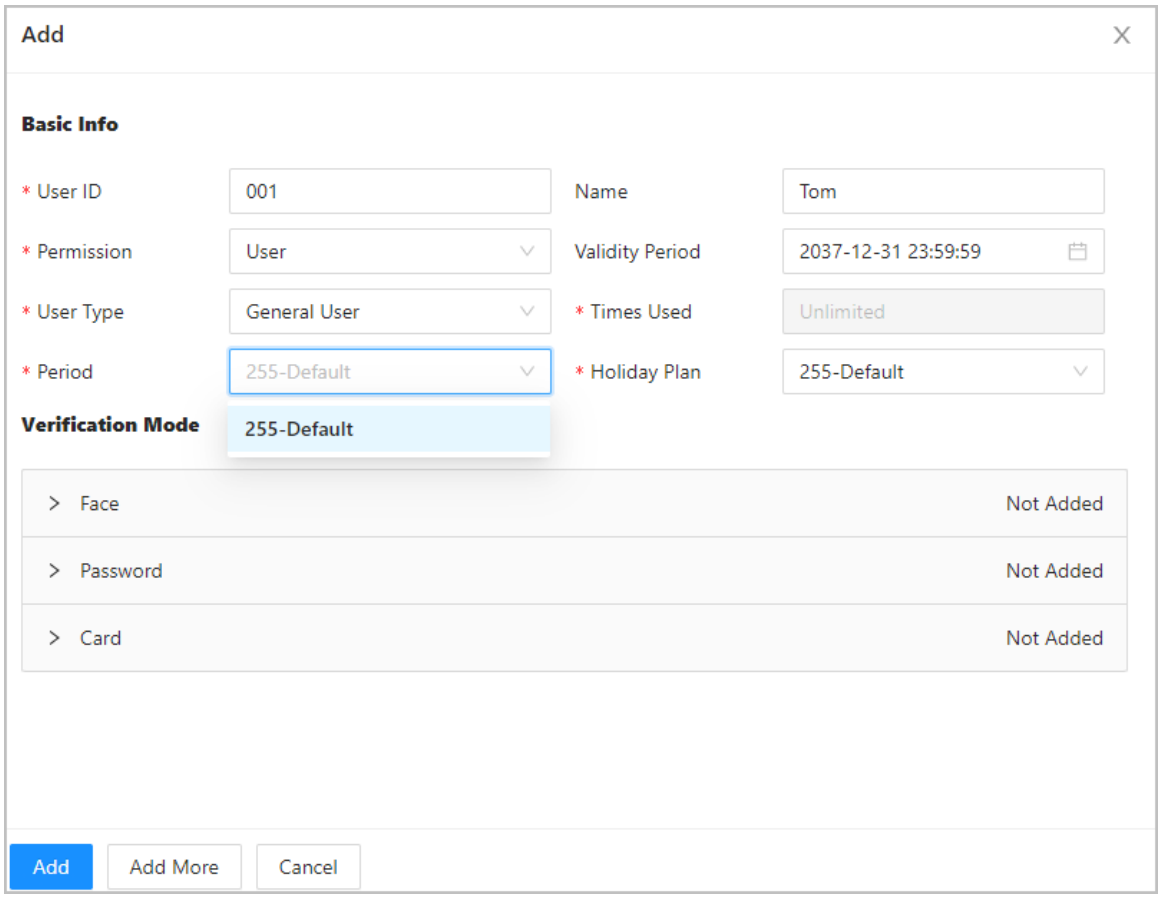


Таблица 3-2 Описание параметров

Параметр	Описание
ID пользователя	Идентификатор пользователя похож на идентификатор сотрудника и может состоять из цифр, букв и их комбинаций, а максимальная длина номера составляет 32 символа.
Имя	Имя может содержать до 30 символов (включая цифры, символы и буквы).
Разрешение	● **Пользователь**: Пользователи имеют только разрешение на доступ к двери или учет рабочего времени. ● **Админ**: Администраторы могут настраивать контроллер доступа, помимо разрешений на доступ к двери и посещаемость.
Срок действия	Установите дату, когда истекает срок действия разрешений на доступ к двери и присутствие человека.

Параметр	Описание
Тип пользователя	● **Обычный пользователь**: Обычные пользователи могут разблокировать дверь. ● **Черный список пользователей**: Когда пользователи из черного списка открывают дверь, обслуживающий персонал получает уведомление. ● **Гость Пользователь**: Гости могут разблокировать дверь в течение определенного периода или определенное количество раз. После истечения определенного периода или времени разблокировки они не смогут разблокировать дверь. ● **Патрульный пользователь**: Патрульные пользователи могут регистрировать присутствие на контроллере доступа, но у них нет доступа к двери разрешения. ● **VIP-пользователь**: Когда VIP-клиент откроет дверь, обслуживающий персонал получит уведомление. ● **Другой пользователь**: Когда они отпирают дверь, она остается открытой еще 5 секунд. ● Пользовательский пользователь 1/Пользовательский пользователь 2: То же, что и у обычных пользователей.
Время использования	Установите лимит разблокировки для гостевых пользователей. После того, как время разблокировки истечет, они не смогут разблокировать дверь.
Период	Люди могут открывать дверь или принимать посетителей в течение определенного периода.
План отпуска	Люди могут открывать дверь или принимать посетителей в течение определенного периода.
Лицо	Нажмите**Загрузить**загрузить изображение лица. Каждый человек может добавить только до 2 изображений лица. Вы можете просмотреть или удалить изображение лица после его загрузки.  Изображение лица должно быть в формате jpg и иметь размер менее 100 КБ.

Параметр	Описание
Карточка	● Введите номер карты вручную. 1. Щелкните**Добавлять**. 2. Введите номер карты, а затем нажмите**Добавлять**. ● Автоматически считывает номер через считыватель карт. 1. Убедитесь, что кард-ридер подключен к вашему компьютеру. 2. Щелкните**Прочитать карту**, а затем проведите картой по считывателю. Отображается 60-секундный обратный отсчет, чтобы напомнить вам о необходимости провести карты, и система автоматически считает номер карты. Если 60-секундный обратный отсчет истек, нажмите**Прочитать карту**еще раз, чтобы начать новый отсчет. 3. Щелкните**Добавлять**. Пользователь может зарегистрировать максимум до 5 карт. Введите номер своей карты или проведите ею по считывателю, после чего данные карты будут считаны контроллером доступа. Вы можете включить**Карта принуждения**функция. Сигнализация сработает, если для разблокировки двери будет использована карта принуждения. ● : Установить карту принуждения. ● : Изменить номер карты. Один пользователь может установить только одну карту принуждения.
Пароль	Введите пароль пользователя. Максимальная длина пароля — 8 цифр. Пароль принуждения — это пароль разблокировки + 1. Например, если пароль пользователя — 12345, пароль принуждения будет 12346. Сигнализация принуждения сработает, если для разблокировки двери будет использован пароль принуждения.
ФП	Регистрация отпечатков пальцев. Пользователь может зарегистрировать до 3 отпечатков пальцев, и вы можете установить отпечаток пальца для отпечатка пальца принуждения. Сигнализация сработает, если отпечаток пальца принуждения будет использован для разблокировки двери. ● Функция отпечатков пальцев доступна только на некоторых модели. ● Мы не рекомендуем вам устанавливать первый отпечаток пальца в качестве отпечаток пальца под принуждением. ● Один пользователь может установить только один отпечаток пальца под принуждением. ● Функция отпечатков пальцев доступна, если Access Контроллер поддерживает подключение модуля считывателя отпечатков пальцев.
Отделение	Добавить пользователей в отдел. Если расписание отдела

Параметр	Описание
Режим расписания	назначенные человеку, они будут следовать установленному графику отдела. О том, как создать отдел, см. в разделе "2.9.1 Настройка отделов". ● Расписание отдела: Назначьте расписание отдела пользователю. Подробнее см. в разделе "2.9.4 Настройка расписаний работы". ● Персональный график: Назначьте персональный график пользователю. Подробнее см. в разделе "2.9.4 Настройка рабочих графиков".  ◇ Эта функция доступна только в некоторых моделях. ◇ Если вы установите режим расписания на отдел расписание здесь, личное расписание у вас есть настроено для пользователя в**Посещаемость**>**Расписание Конфигурации**>**Личное расписание**недействительно.

Шаг 3 Нажмите**ХОРОШО**.

Связанные операции

- Импортировать информацию о пользователе: Нажмите**Экспортировать шаблон**, и загрузите шаблон и введите в него информацию о пользователе. Поместите изображения лиц и шаблон в один и тот же путь к файлу, а затем нажмите**Импорт информации о пользователе** для импорта папки.

  Одновременно можно импортировать до 10 000 пользователей.
- Очистить: Очистить всех пользователей.

3.6 Настройка интеркома

Контроллер доступа может функционировать как дверная станция для реализации видеодомофона.

Функция внутренней связи доступна только в некоторых моделях.

3.6.1 Использование устройства в качестве SIP-сервера

3.6.1.1 Настройка SIP-сервера

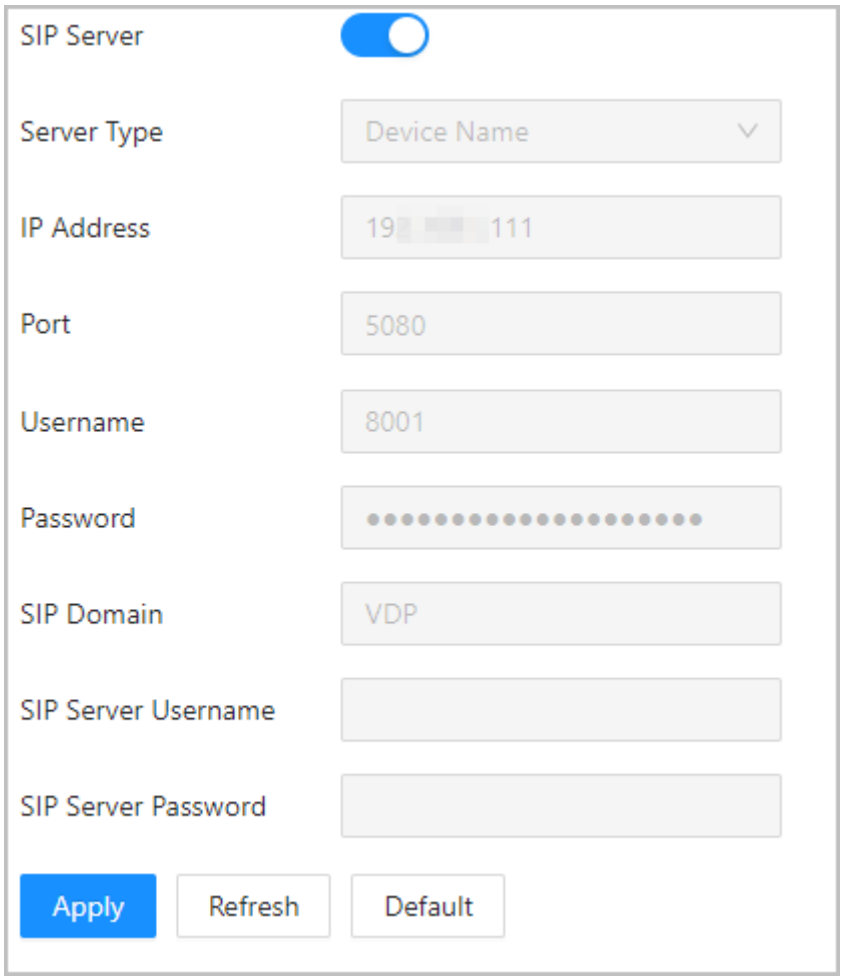
Когда контроллер доступа функционирует как SIP-сервер, он может подключать до 500 устройств контроля доступа и видеодомофонов.

Процедура

Шаг 1 Выбирать**Настройки домофона**>**SIP-сервер**.

Шаг 2 Включать**SIP-сервер**.

Рисунок 3-4 Использование контроллера доступа в качестве SIP-сервера



Шаг 3 Нажмите**Применять**.

3.6.1.2 Настройка локальных параметров

Когда Устройство функционирует как SIP-сервер, настройте параметры Устройства.

Процедура

Шаг 1 Выбирать**Настройки домофона**>**Конфигурация локального**

Шаг 2 **устройства**. Настройте параметры.

Рисунок 3-5 Основной параметр

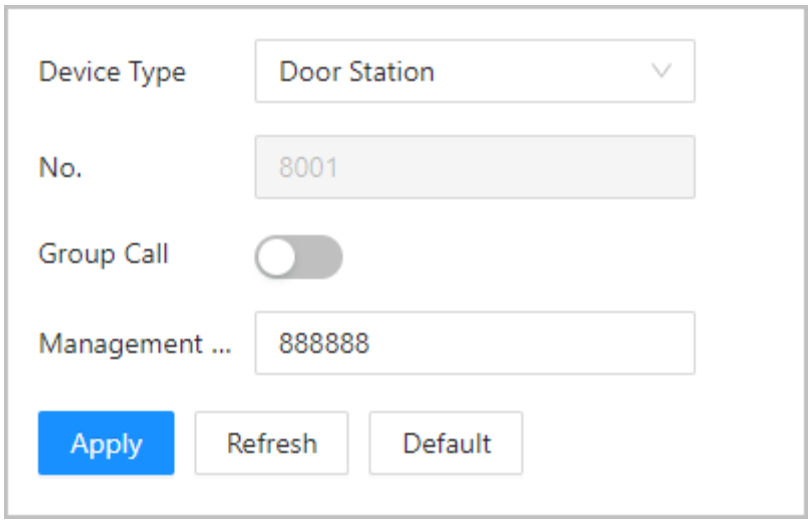


Таблица 3-3 Описание основных параметров

Параметр	Описание
Тип устройства	Выбирать**Дверная станция**.
Нет	Невозможно установить.
Групповой вызов	При включении функции группового вызова дверная станция одновременно вызывает основной VTH и расширения. Настройка вступает в силу после перезапуска дверной станции.
Центр управления	Номер вызова центра управления по умолчанию — 888888+VTS No. Чтобы узнать VTS No, перейдите на страницу**Проект Настройка**>**Общий**центра управления.

Шаг 3 Нажмите**Применять**.

3.6.1.3 Добавление VTO

Когда контроллер доступа функционирует как SIP-сервер, вам необходимо добавить VTO к SIP-серверу, чтобы они могли звонить друг другу.

Процедура

Шаг 1 На веб-странице контроллера доступа выберите**Настройки домофона**>**Настройка устройства**.

Шаг 2 Нажмите**Добавлять**, а затем настройте VTO.

Рисунок 3-6 Добавить VTO

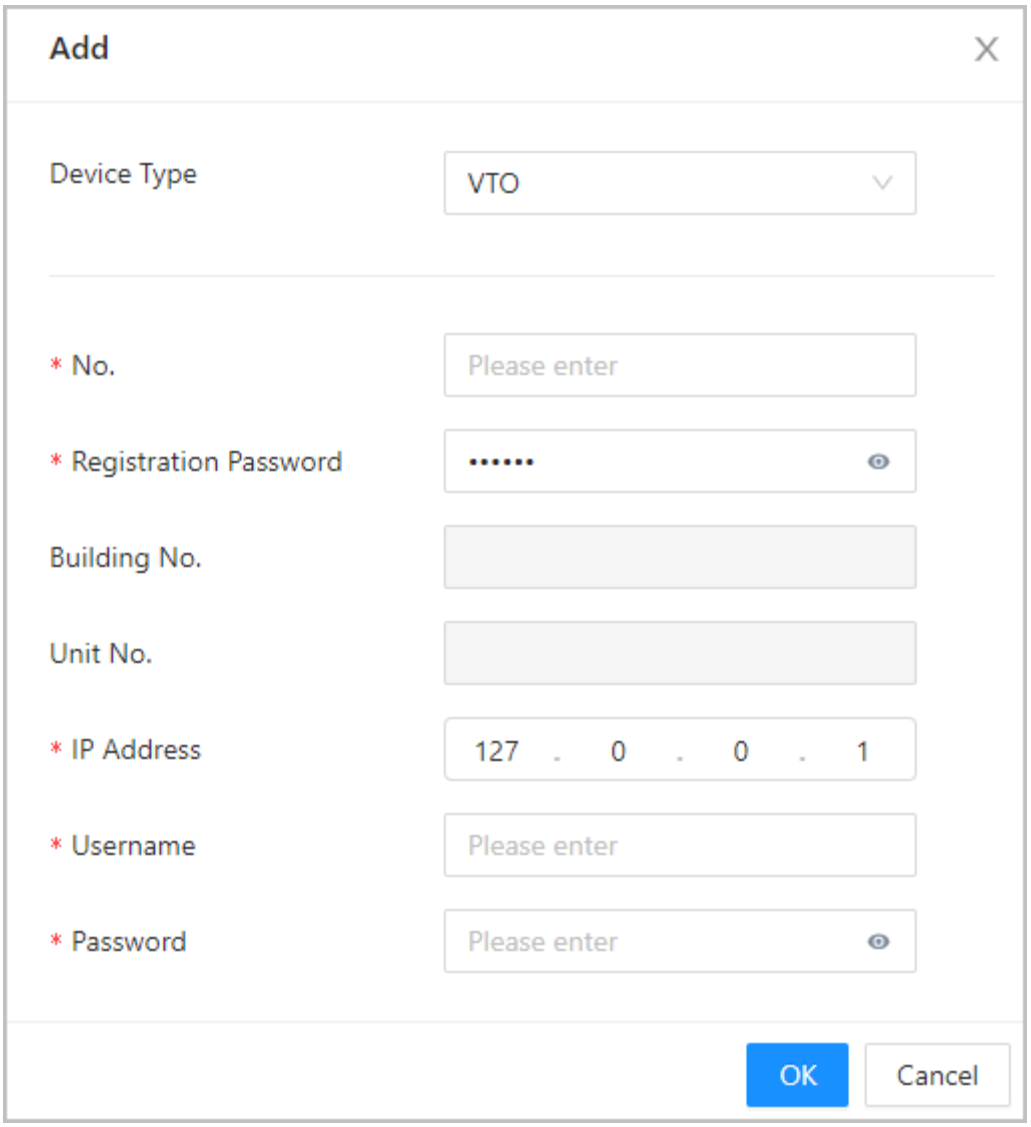


Таблица 3-4 Добавить конфигурацию VTO

Параметр	Описание
Тип устройства	Выбирать**ВТО**.
Нет.	Введите номер VTO. Чтобы узнать номер VTO, перейдите на страницу**Устройство**экран ВТО.
Регистрация Пароль	Оставьте значение по умолчанию.
Номер здания	Невозможно настроить.
Номер блока	
IP-адрес	IP-адрес добавленного VTO.
Имя пользователя	Имя пользователя и пароль, которые используются для входа на веб-страницу добавленного VTO.
Пароль	

Шаг 3 Нажмите**ХОРОШО**.

3.6.1.4 Добавление VTH

Когда устройство функционирует как SIP-сервер, вы можете добавить все VTH в одном устройстве к SIP-серверу.

чтобы убедиться, что они могут звонить друг другу.

Справочная информация

- При наличии основного VTH и добавочного номера сначала необходимо включить функцию группового вызова, а затем затем добавьте основной VTH и расширение на**Управление ВТХ**страница. Как включить группу вызов функции, см. «3.6.1.2 Настройка локальных параметров».
- Расширение не может быть добавлено, если не добавлены основные видеодомофоны.

Процедура

Шаг 1 На главной странице выберите**Настройки домофона**>**Настройка устройства**.

Шаг 2 Добавьте VTH.

- Добавляйте по одному.

  1. Щелкните**Добавлять**.

  2. Настройте параметры, а затем нажмите**ХОРОШО**.

Рисунок 3-7 Добавляйте по одному

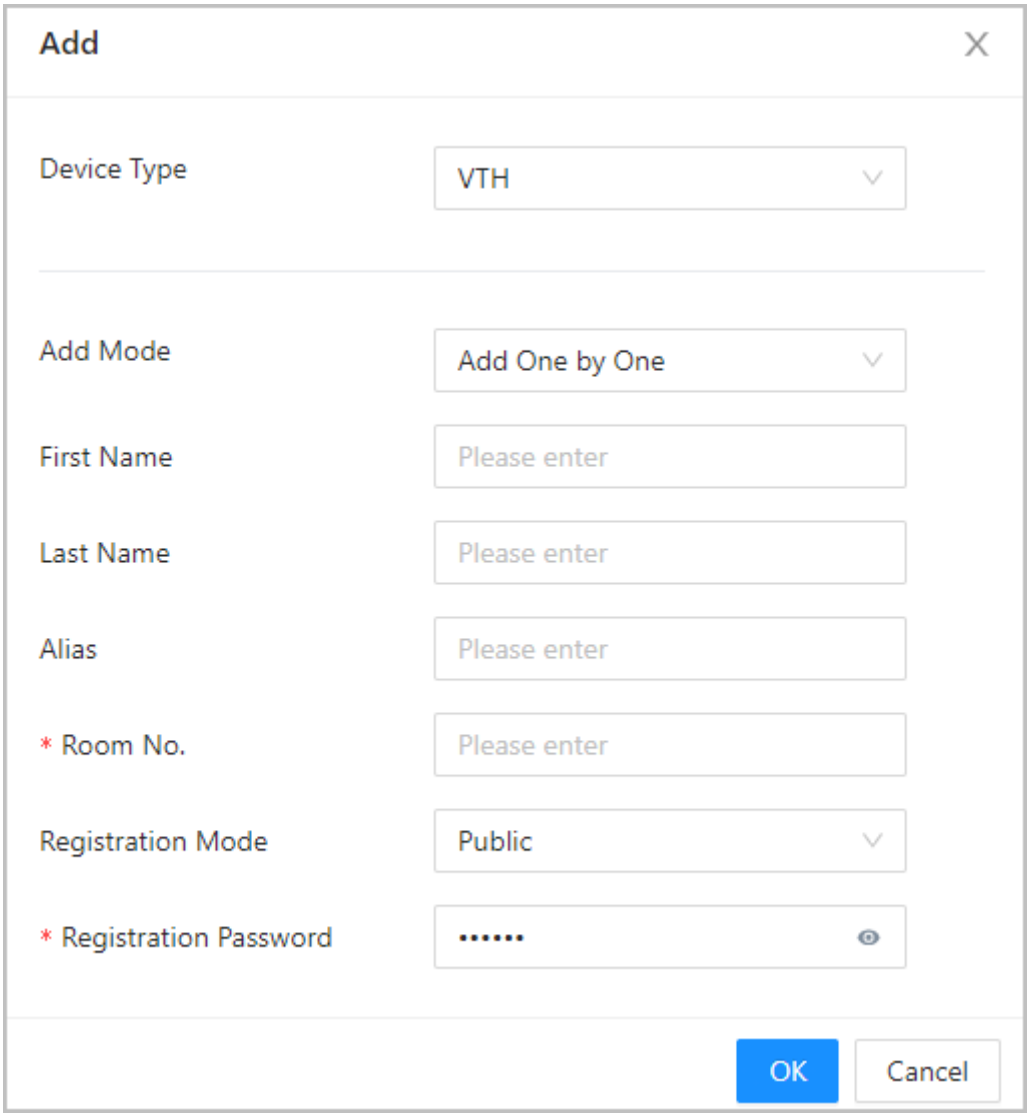


Таблица 3-5 Информация о номере

Параметр	Описание
Имя	Введите название VTH, чтобы вам было легче различать VTH.
Фамилия	
Псевдоним	
Номер комнаты	Введите номер комнаты VTH. ● Номер комнаты состоит из 1–5 цифр и должен соответствовать настроенному номеру комнаты на видеодомофоне. ● Когда есть основной VTH и расширения, номер комнаты основного VTH заканчивается на -0, а номер комнаты расширения заканчивается на -1, -2 или -3. Например, основной VTH - 101-0, а номер комнаты расширения - 101-1, 101-2... ● Если функция группового вызова не включена, номер комнаты в формате 9901-xx установить невозможно.
Номер комнаты	Введите номер комнаты VTH. ● Номер комнаты состоит из 1–5 цифр и должен соответствовать настроенному номеру комнаты на видеодомофоне. ● Когда есть основной VTH и расширения, номер комнаты основного VTH заканчивается на -0, а номер комнаты расширения заканчивается на -1, -2 или -3. Например, основной VTH - 101-0, а номер комнаты расширения - 101-1, 101-2... ● Если функция группового вызова не включена, номер комнаты в формате 9901-xx установить невозможно.
Режим регистрации	Оставьте их как значения по умолчанию.
Пароль регистрации	

- Добавляйте порциями.

  1. Щелкните**Добавить партиями**.
  2. Настройте параметры.
  3. Щелкните**Добавлять**.

Рисунок 3-8 Пакетное добавление

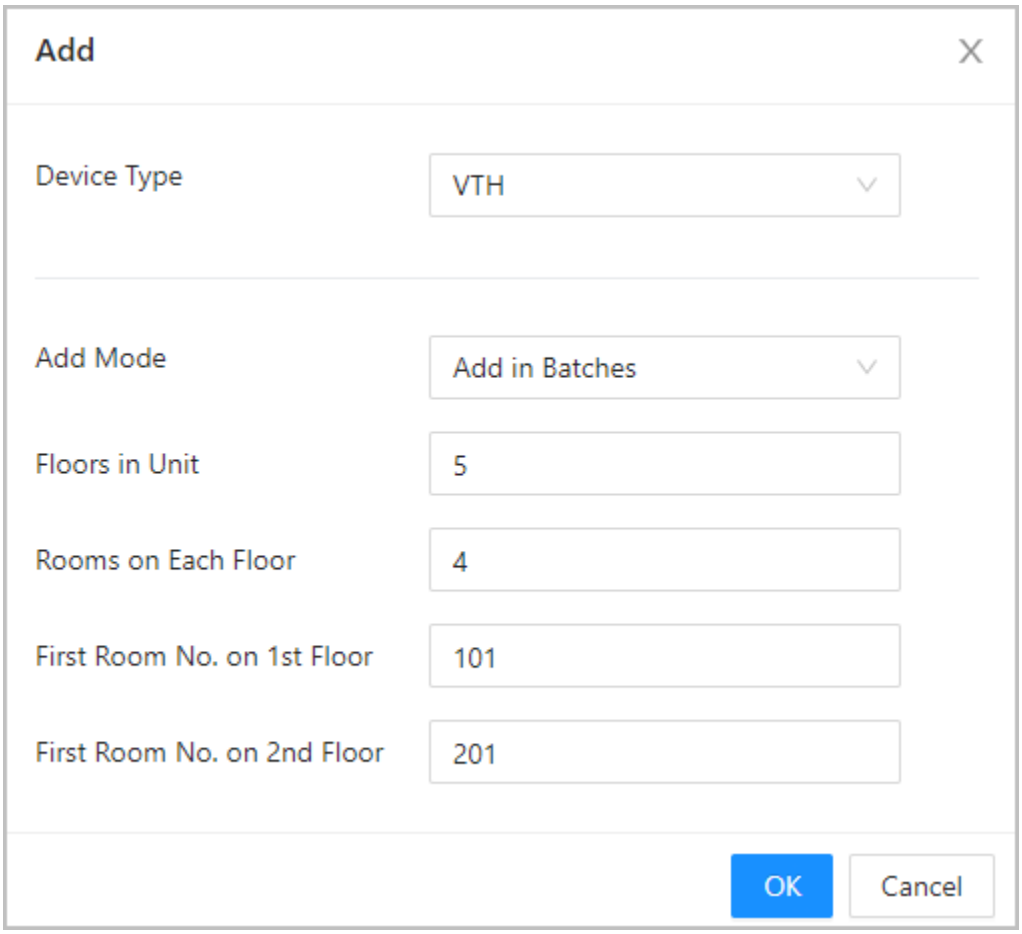


Таблица 3-6 Добавить партиями

Параметр	Описание
Этажи в блоке	Количество этажей здания, которое варьируется от 1 до 99.
Комнаты на каждом этаже	Количество комнат на каждом этаже варьируется от 1 до 99.
Номер первой комнаты на 1 этаже	Первая комната на первом этаже.
Номер первой комнаты на 2 этаже	Номер первой комнаты на 2-м этаже = Первая цифра номера первой комнаты на 1-м этаже плюс 1. Например, если номер первой комнаты на первом этаже — 101, номер первой комнаты на 2-м этаже должен быть 201.

3.6.1.5 Добавление СУДС

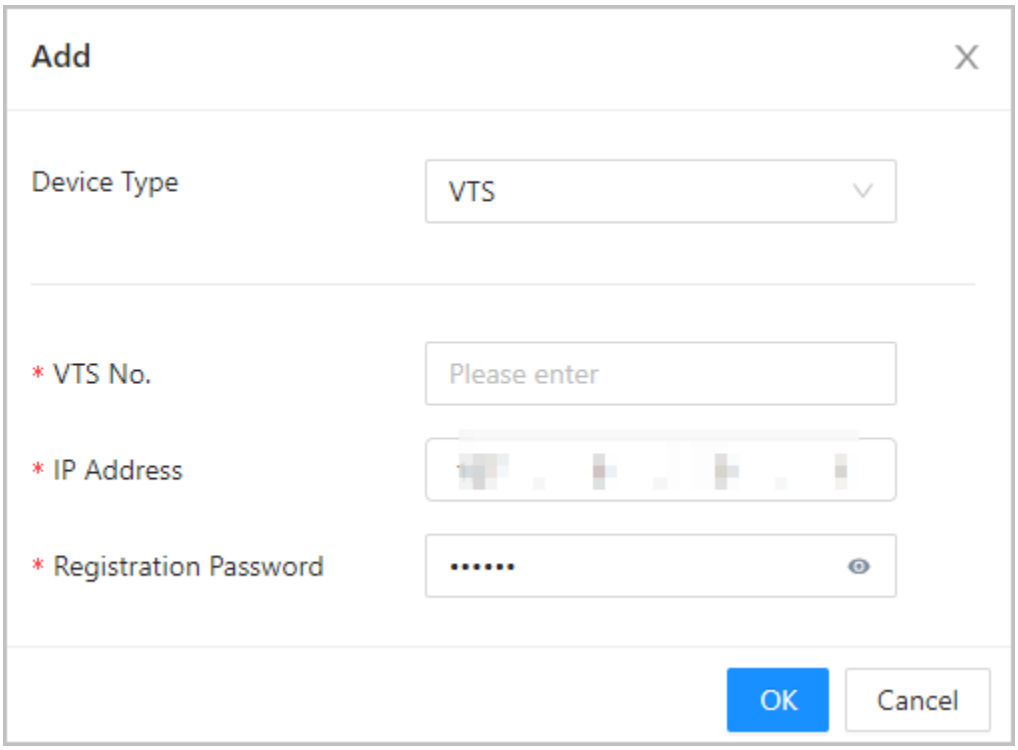
Когда устройство функционирует как SIP-сервер, вы можете добавить VTS к SIP-серверу, чтобы убедиться, что они могут звонить друг другу.

Процедура

Шаг 1 На главной странице выберите**Настройки домофона**>**Настройка устройства**.

Шаг 2 Нажмите**Добавлять**, а затем задайте параметры.

Рисунок 3-9 Управление СУДС



Шаг 3 НажмитеХОРОШО.

3.6.2 Использование VTO в качестве SIP-сервера

3.6.2.1 Настройка SIP-сервера

Используйте другой VTO в качестве SIP-сервера.

Процедура

Шаг 1 Выбирать**Настройки домофона**>**SIP-сервер**.

Шаг 2 Выбирать**Устройство**из**Тип сервера**.

Не включать**SIP-сервер**.

Шаг 3 Настройте параметры, а затем нажмите**ХОРОШО**.

Рисунок 3-10 Использование VTO в качестве SIP-сервера

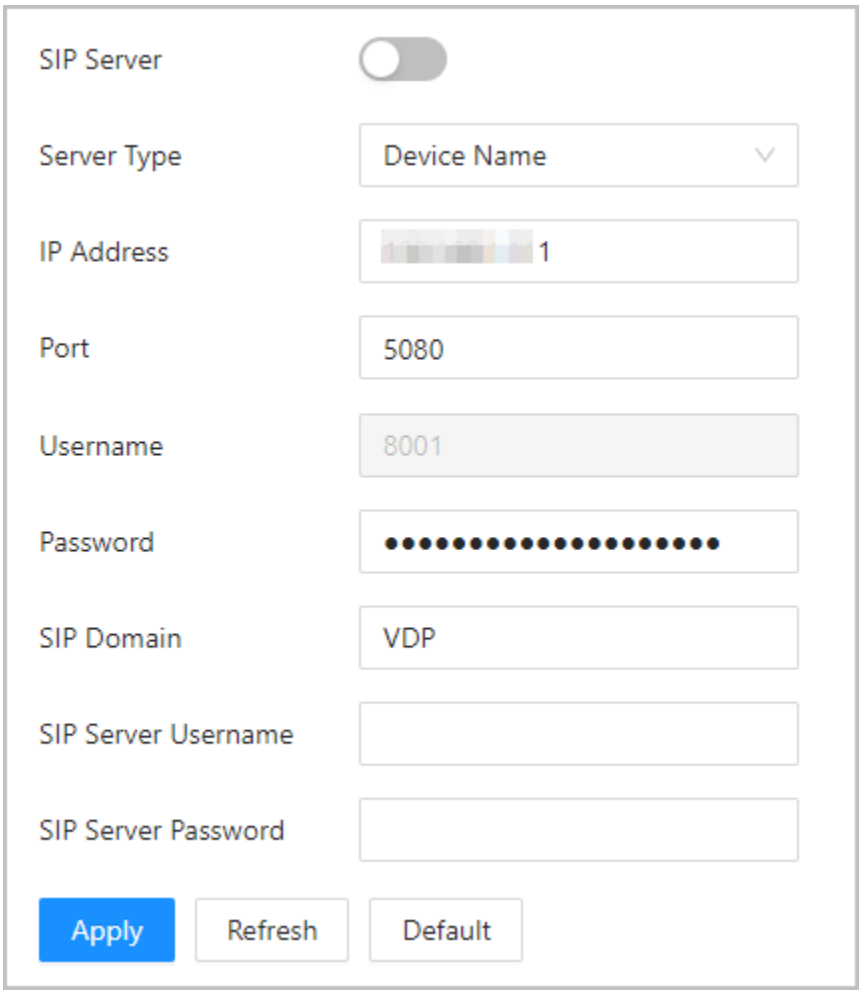


Таблица 3-8 Конфигурация SIP-сервера

Параметр	Описание
IP-адрес	IP-адрес ВТО.
Порт	5060 по умолчанию, когда VTO работает как SIP-сервер.
Имя пользователя	Оставьте их по умолчанию.
Пароль	
SIP-домен	ВДП.
Имя пользователя SIP-сервера	Имя пользователя и пароль для входа на SIP-сервер.
Пароль SIP-сервера	

Шаг 4 Нажмите**Применять**.

3.6.2.2 Настройка локальных параметров

Настройте параметры устройства при использовании другого VTO в качестве SIP-сервера.

Процедура

Шаг 1 Выбирать**Настройки домофона**>**Конфигурация локального**

Шаг 2 **устройства**. Настройте параметры.

Рисунок 3-11 Настройка параметров

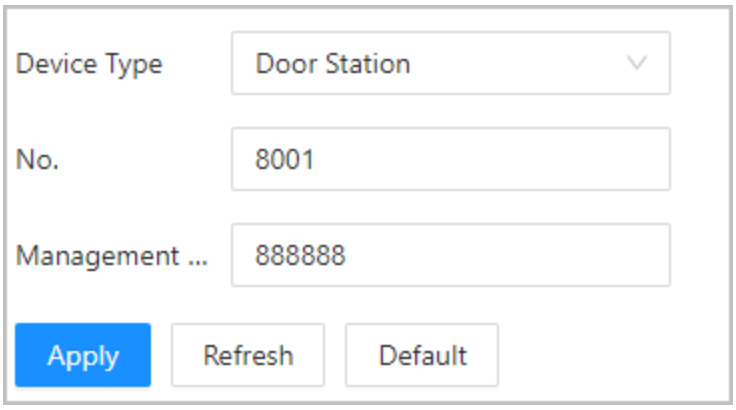


Таблица 3-9 Описание параметров

Параметр	Описание
Тип устройства	Выбирать**Дверная станция**.
Нет.	Номер ВТО. ● Номер должен состоять из 4 цифр. Первые 2 цифры должны быть 80, а последние 2 цифры начинаются с 01. Например, 8001. ● Если в одном подразделении имеется несколько VTO, номер VTO не может повторяться.
Центр управления	Номер вызова центра управления — 888888. Оставьте его по умолчанию.

Шаг 3 Нажмите**Применять**.

3.6.3 Использование платформы в качестве SIP-сервера

3.6.3.1 Настройка SIP-сервера

Платформа управления используется в качестве SIP-сервера.

Процедура

Шаг 1 Выбирать**Настройки домофона**>**Частный SIP-сервер**.

Шаг 2 Выбирать**Частный SIP-сервер**из**Тип сервера**.

Не включать**SIP-сервер**.

Рисунок 3-12 Использование платформы управления в качестве SIP-сервера

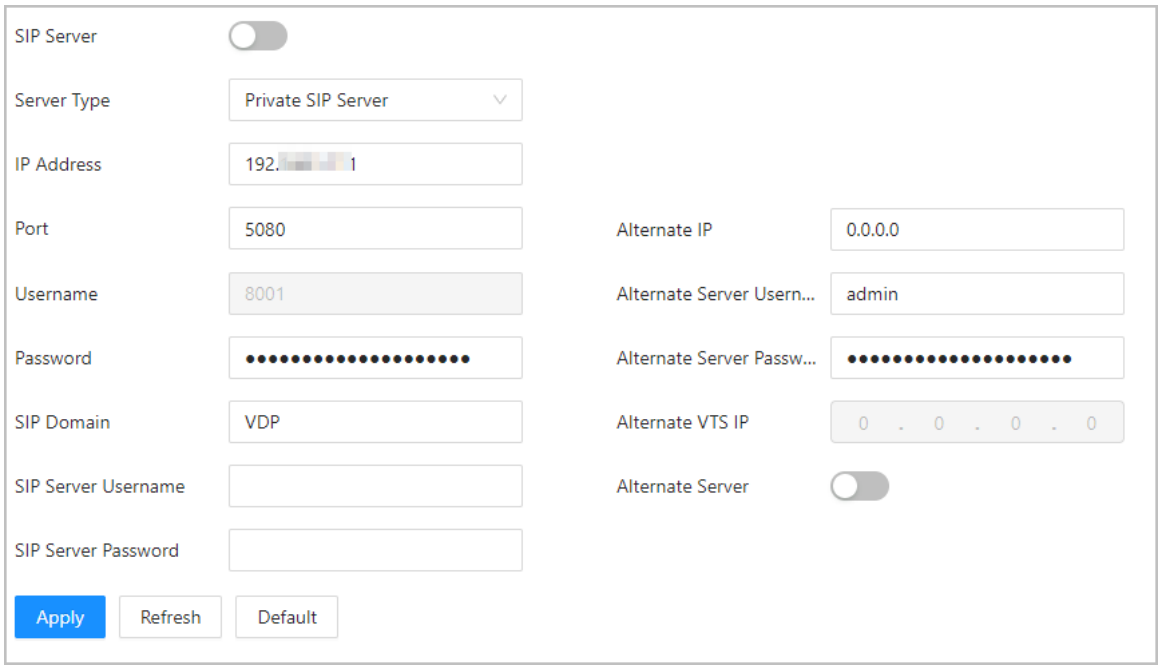


Таблица 3-10 Конфигурация SIP-сервера

Параметр	Описание
IP-адрес	IP-адрес платформы.
Порт	5080 по умолчанию, когда платформа работает как SIP-сервер.
Имя пользователя Пароль	Оставьте их по умолчанию.
SIP-домен	Оставьте значение по умолчанию.
Имя пользователя SIP-сервера Пароль SIP-сервера	Имя пользователя и пароль для входа на платформу.
Альтернативный IP-адрес	Альтернативный сервер будет использоваться в качестве SIP-сервера, если платформа не отвечает. ● Если вы включите**Альтернативный сервер**этой функции вы установите контроллер доступа в качестве альтернативного сервера. ● Если вы хотите, чтобы другой VTO функционировал как альтернативный сервер, вы необходимо ввести IP-адрес, имя пользователя, пароль VTO. Делать не включить**Альтернативный сервер**в этом случае. ● Мы рекомендуем вам установить основной VTO в качестве альтернативного сервера.
Альтернативный сервер Имя пользователя Альтернативный сервер Пароль	Используется для входа на альтернативный сервер.

Параметр	Описание
Альтернативный IP-адрес VTS	Введите IP-адрес альтернативного VTS. Если платформа управления не отвечает, будет активирован альтернативный VTS, чтобы убедиться, что VTO, VTH и VTS могут друг друга.

Шаг 3 НажмитеПрименять.

3.6.3.2 Настройка локальных параметров

Настройте параметры контроллера доступа при использовании платформы в качестве SIP-сервера.

Процедура

Шаг 1 Выбирать**Настройки домофона**>**Конфигурация локального**

Шаг 2 **устройства**. Настройте параметры.

Рисунок 3-13 Основной параметр

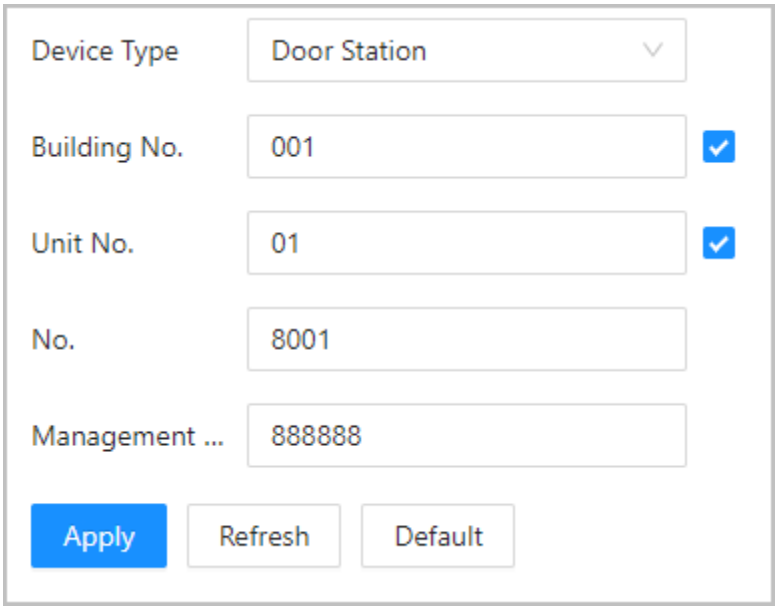


Таблица 3-11 Описание параметров

Параметр	Описание
Тип устройства	Выберите станцию ограждения или дверную станцию в зависимости от места ее установки.
Номер здания	Установите флажок, а затем введите номер здания, в котором установлена вызывная панель.
Номер блока	Установите флажок, а затем введите номер блока, в котором установлена вызывная панель.
Нет.	● Номер должен состоять из 4 цифр. Первые 2 цифры должны быть 80, а последние 2 цифры должны начинаться с 01. Например, 8001. ● Если в одном подразделении имеется несколько VTO, номер VTO не может повторяться.
Центр управления	Номер телефона по умолчанию — 888888, когда VTO звонит в VTS. Оставьте его по умолчанию.

Шаг 3 НажмитеПрименять.

После настроек имя пользователя в**Интерком**>**ГЛОТОК**страница автоматически обновляется. Убедитесь, что имя пользователя совпадает с номером вызова, когда вы добавляете устройство в управление

платформа.

3.7 Настройка контроля доступа

3.7.1 Настройка основных параметров

Процедура

Шаг 1 Выбирать**Контроль доступа**>**Параметры контроля доступа**.

Шаг 2 В**Основные настройки**, настроить основные параметры контроля доступа.

Рисунок 3-14 Основные параметры

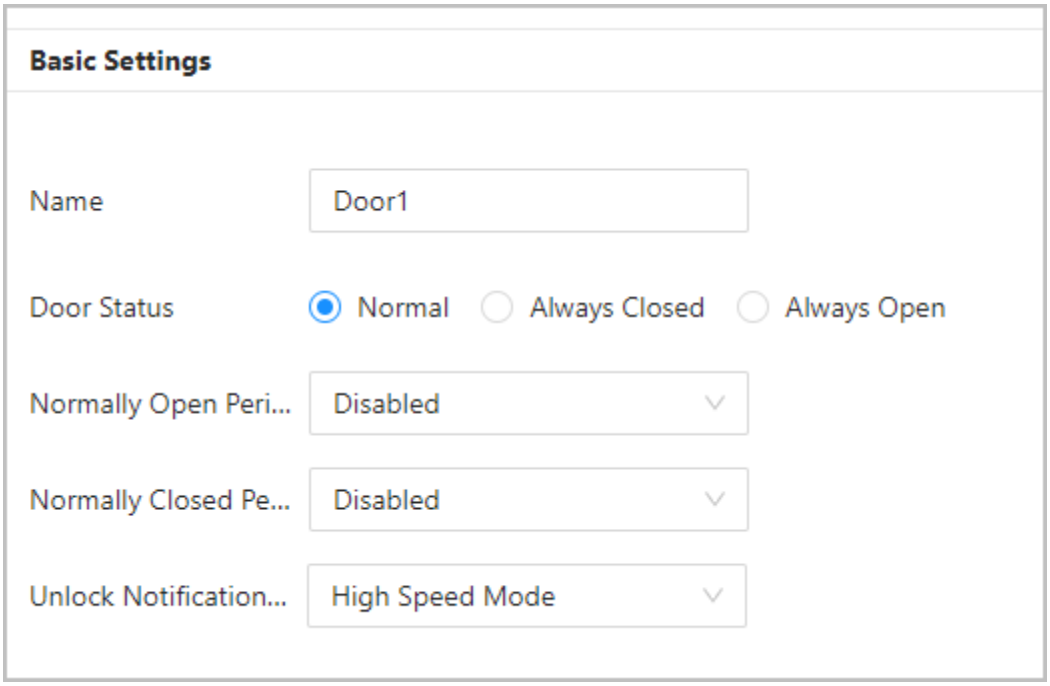


Таблица 3-12 Описание основных параметров

Параметр	Описание
Имя	Название двери.
Состояние двери	Установите статус двери. ● Нормальный режим: Дверь будет разблокирована и заблокирована в соответствии с вашими настройками. ● Всегда открыто: дверь все время остается открытой. ● Всегда закрыто: дверь все время остается запертой.
Нормально открытый период	Когда вы выбираете**Нормальный**, вы можете выбрать шаблон времени из выпадающего списка. Дверь остается открытой или закрытой в течение определенного времени.
Период нормального закрытия	

Параметр	Описание
Уведомление о разблокировке	Отображает уведомление на экране, когда человек подтверждает свою личность на контроллере доступа. ● Режим высокой скорости: система предлагает**Успешно проверено**или **Не авторизовано**на экране. ● Простой режим: отображает идентификатор пользователя, имя и время проверки после предоставления доступа; отображает**Не авторизовано**и время авторизации после отказа в доступе. ● Стандарт: отображает зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время проверки после предоставления доступа; отображает**Не авторизовано**и время проверки после отказа в доступе. ● Контрастный режим: отображает захваченное изображение лица и зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время авторизации после предоставления доступа; отображает**Не авторизовано**и время авторизации после отказа в доступе.

Шаг 3 Нажмите**Применять**.

3.7.2 Настройка методов разблокировки

Вы можете использовать несколько методов разблокировки, чтобы разблокировать дверь, например, Bluetooth-карту, отпечаток пальца, карту и пароль. Вы также можете объединить их, чтобы создать свой собственный метод разблокировки.

Процедура

Шаг 1 Выбирать**Контроль доступа**>**Параметры контроля доступа**. В

Шаг 2 **Разблокировать настройки**, выберите режим разблокировки.

- Комбинированная разблокировка
  1. Выбрать**Комбинация разблокировки**из**Режим разблокировки**список.
  2. Выбрать**Или**или**И**.
     - ◇ Или: используйте один из выбранных методов разблокировки, чтобы открыть дверь.
     - ◇ И: Используйте все выбранные методы разблокировки, чтобы открыть дверь.
  3. Выберите методы разблокировки, а затем настройте другие параметры.

Рисунок 3-15 Настройки разблокировки

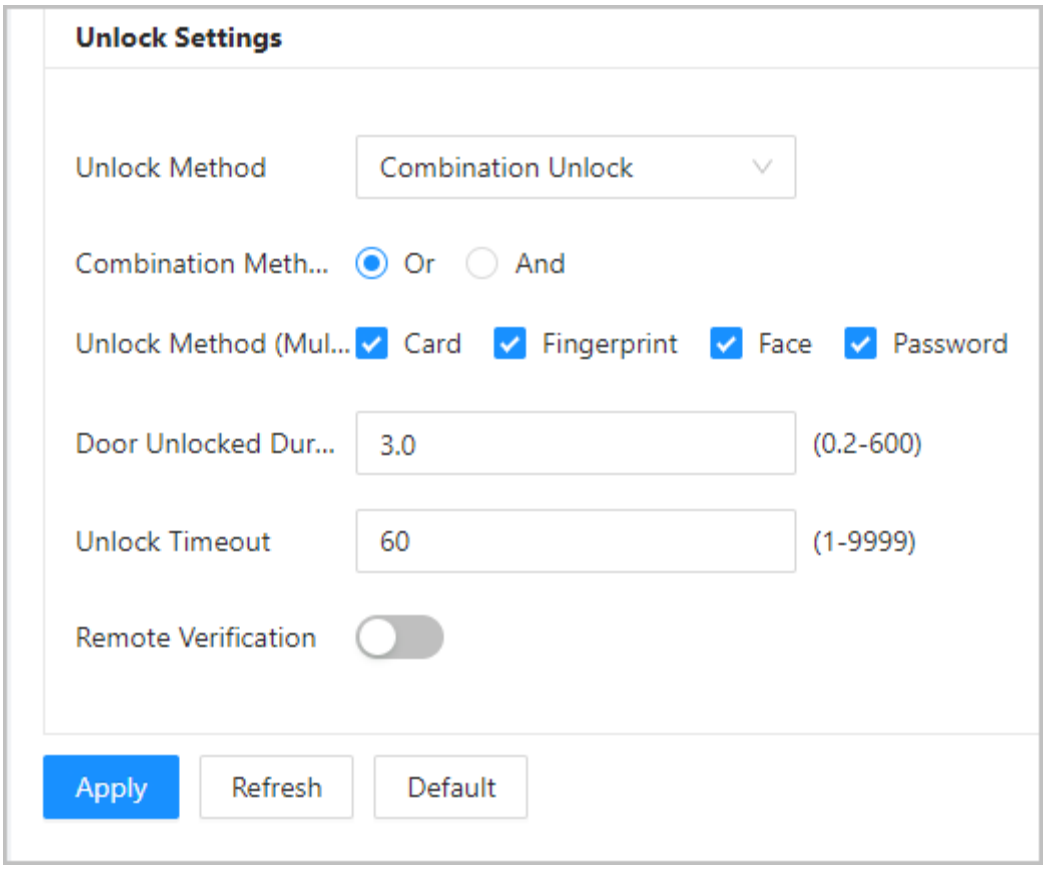


Таблица 3-13 Описание настроек разблокировки

Параметр	Описание
Метод разблокировки (множественный выбор)	Методы разблокировки могут различаться в зависимости от модели продукта.
Продолжительность разблокировки двери	После того, как человеку предоставлен доступ, дверь останется открытой в течение определенного времени, чтобы он мог пройти. Оно варьируется от 0,2 с до 600 секунд.
Тайм-аут разблокировки	Если включены детектор двери и сигнализация тайм-аута разблокировки, сработает сигнализация тайм-аута, если дверь останется разблокированной дольше заданного времени разблокировки.
Удаленная проверка	Откройте дверь дистанционно.

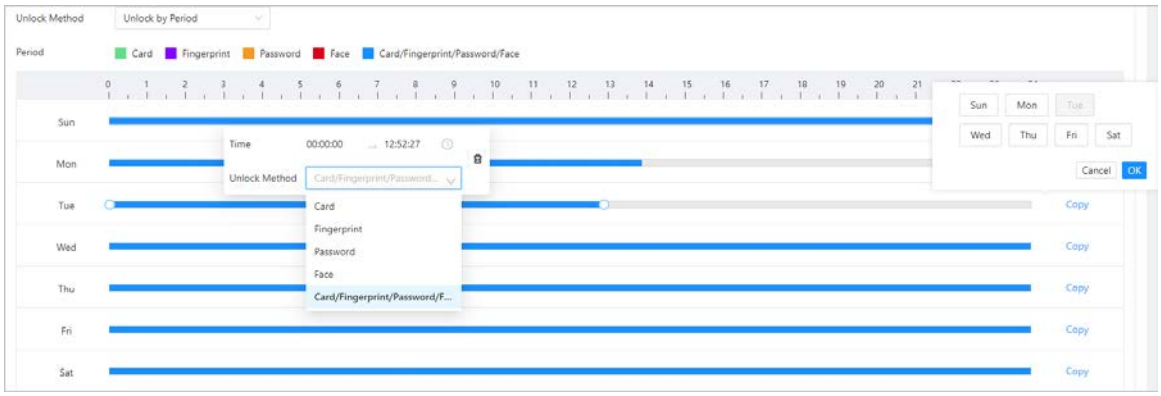
- Разблокировать по периоду

1. В**Режим разблокировки**список, выбрать**Разблокировать по периоду**.
2. Перетащите ползунок, чтобы настроить период времени для каждого дня.

Вы также можете нажать**Копировать**для применения настроенного периода времени к другим дням.

3. Выберите метод разблокировки для указанного периода времени, а затем настройте другие параметры.

Рисунок 3-16 Разблокировка по периоду



- Разблокировка несколькими пользователями.

  1. В**Режим разблокировки**список, выбрать**Разблокировка несколькими пользователями**.

  2. Щелкните**Добавлять**для добавления групп.

  3. Выберите метод разблокировки, действительный номер и список пользователей.

     - ◇ Если добавлена только одна группа, дверь разблокируется только после того, как количество людей в группе, предоставляющих доступ, сравняется с указанным допустимым числом.
     - ◇ Если добавлено более одной группы, дверь разблокируется только после того, как количество людей в каждой группе, предоставивших доступ, сравняется с указанным допустимым числом.

  - ◇ Вы можете добавить до 4 групп.
  - ◇ Действительный номер указывает количество людей в каждой группе, которым необходимо подтвердить свои данные. идентификаторы на контроллере доступа до того, как дверь откроется. Например, если действительный Количество установлено на 3 для группы, любые 3 человека в группе должны подтвердить свою личность, чтобы отоприте дверь.

Шаг 3 Нажмите**Применять**.

3.7.3 Настройка будильников

При возникновении нештатного события доступа срабатывает сигнализация.

Процедура

Шаг 1 Выбирать**Контроль доступа**>**Тревога**>**Тревога**.

Шаг 2 Настройте параметры сигнализации.

Рисунок 3-17 Сигнализация

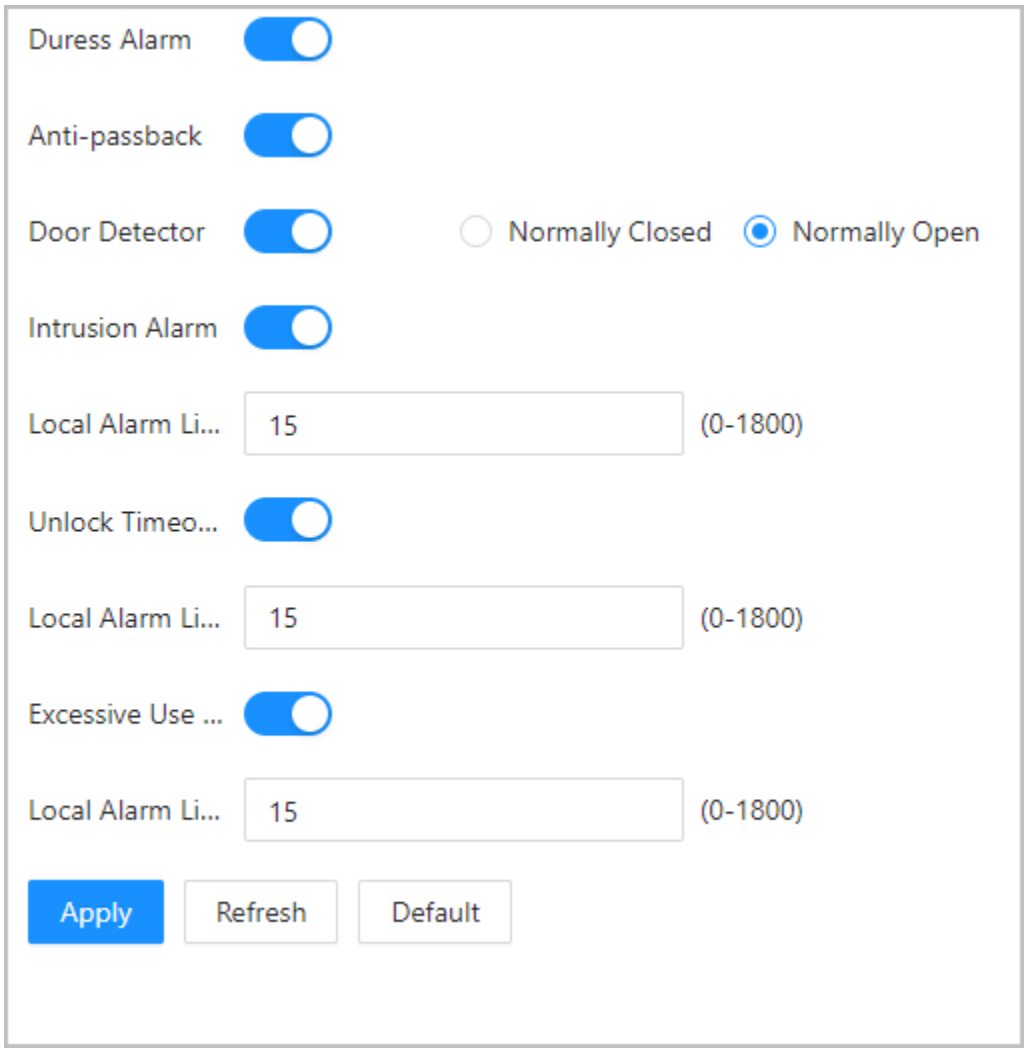


Таблица 3-14 Описание параметров сигнализации

Параметр	Описание
Сигнализация принуждения	Сигнализация сработает, если для разблокировки двери будет использована карта принуждения, пароль принуждения или отпечаток пальца принуждения.

Параметр	Описание
Антипассбэк	Пользователи должны подтвердить свою личность как для входа, так и для выхода; в противном случае сработает сигнализация. Это помогает предотвратить передачу карты доступа держателем карты другому человеку для входа. Когда включена защита от повторного прохода, держатель карты должен покинуть защищенную зону через считыватель на выходе, прежде чем система предоставит другой вход. ● Если человек войдет после авторизации и выйдет без авторизации, при повторной попытке входа сработает сигнализация, и доступ будет запрещен. ● Если человек войдет без разрешения и выйдет после получения разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен.  Если контроллер доступа может подключить только один замок, проверка на контроллере доступа означает направление входа, и проверка на внешнем считывателе карт означает направление выхода по умолчанию. Вы можете изменить настройки на платформе управления.
Детектор двери	С дверным детектором, подключенным к вашему устройству, сигнализация может срабатывать при ненормальном открытии или закрытии дверей. Дверной детектор включает 2 типа, включая NC-детектор и NO-детектор. ● Нормально замкнутый: датчик находится в замкнутом положении, когда дверь или окно закрыты. ● Нормально открытый: Разомкнутая цепь создается, когда окно или дверь фактически закрыты.
Сигнализация вторжения	Если включены детектор двери и сигнализация вторжения, при ненормальном открытии двери сработает сигнализация вторжения.
Разблокировать сигнализацию тайм-аута	Если включены детектор двери и сигнализация тайм-аута разблокировки, сработает сигнализация тайм-аута, если дверь останется разблокированной дольше заданного времени разблокировки.
Сигнализация чрезмерного использования	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании нелегальной карты, которая по умолчанию длится 15 секунд.
Локальная связь с сигнализацией	Длительность сигнала будильника. По умолчанию 15 с.

Шаг 3 Нажмите**Применять**.

3.7.4 Настройка глобальных связей тревог (необязательно)

Вы можете настроить глобальные связи тревог.

Процедура

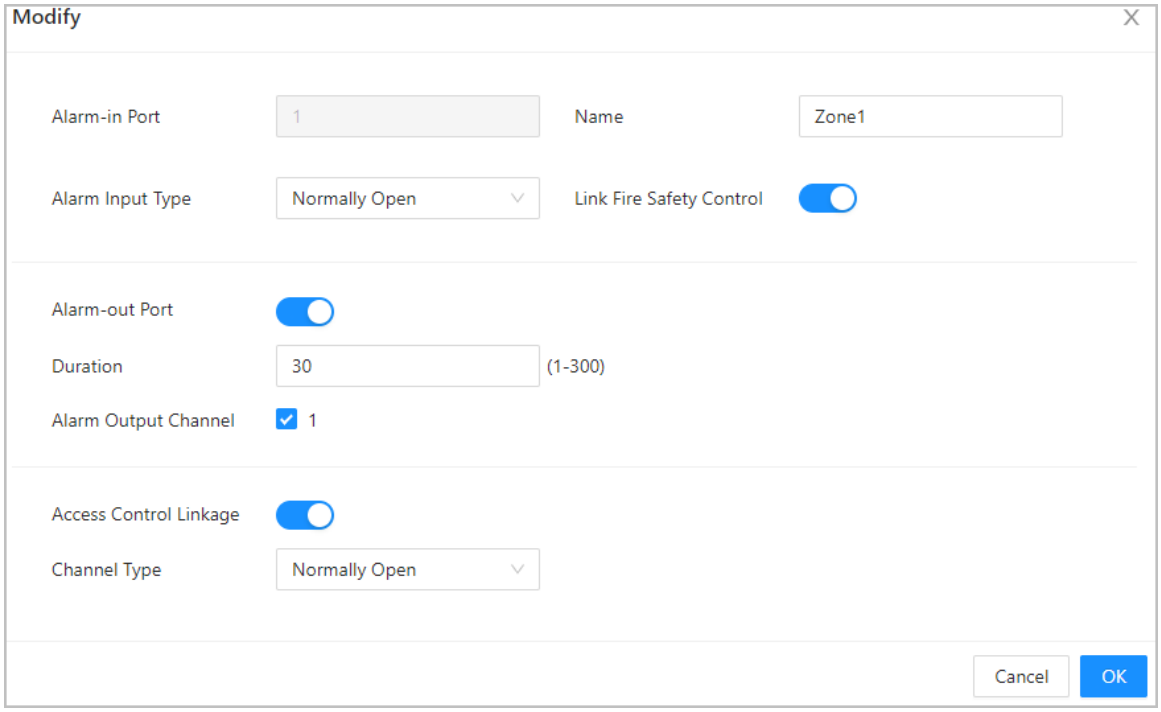
Шаг 1 Выбирать**Контроль доступа**>**Тревога**>**Настройка связи с сигналом тревоги**.

- Если контроллер доступа добавлен в качестве платформы управления, настройки сигнализации будут синхронизировано с платформой.
- Эта функция доступна только в моделях, имеющих порты входа и выхода тревоги.
- Количество входных и выходных портов сигнализации различается в зависимости от модели продукт.

Шаг 2 Настройте вход тревоги. 1.

Нажмите .

Рисунок 3-18 Глобальная связь тревог



2. Настройте имя для будильника.

3. Выберите тип устройства входа тревоги.

- Нормально замкнутый: Вход сигнализации находится в состоянии нормально замкнутой цепи (NC), когда сигнализация не сработала. Размыкание нормально замкнутой цепи активирует сигнализацию.
- Нормально разомкнутый: Устройство входа сигнализации находится в состоянии нормально разомкнутой цепи (НО), когда сигнализация не сработала. Замыкание цепи включает сигнализацию.

4. Щелкните**Давать возможность**для включения функции присоединения двери.

Если вы включите управление пожарной безопасностью, выход сигнализации и все дверные соединения будут отключены. автоматически включено изменение на**Всегда открыто**статус, и все двери откроются, когда срабатывает пожарная сигнализация.

1. Выберите вход сигнала тревоги из списка каналов входа сигнала тревоги, а затем нажмите**Выход сигнала тревоги**.

2. Щелкните**Добавлять**, выберите канал выхода тревоги, а затем нажмите**ХОРОШО**.

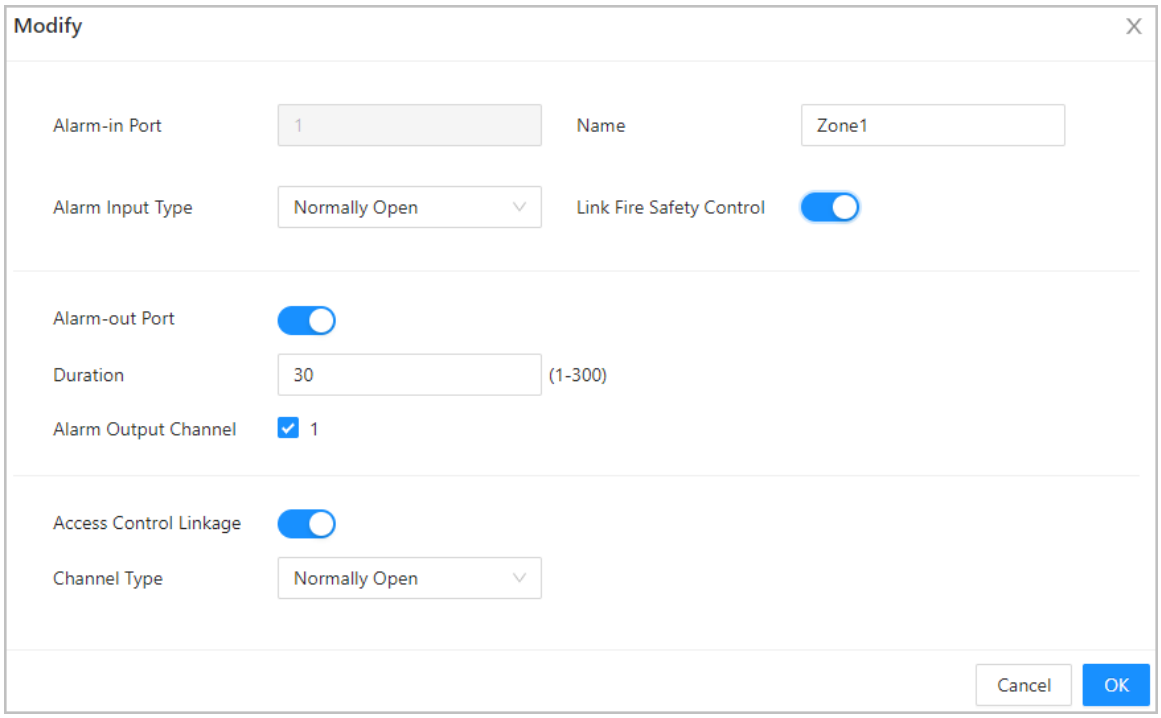
3. Щелкните**Применять**.

Шаг 3 Включите функцию выхода тревоги, а затем введите длительность сигнала тревоги.

Шаг 4 Включите связь электронного управления доступом, а затем выберите статус двери.

- Нормально закрытый: дверь автоматически запирается при срабатывании сигнализации.
- Нормально открытый: дверь автоматически разблокируется при срабатывании сигнализации.

Рисунок 3-19 Выход сигнала тревоги



3.7.5 Настройка распознавания лиц

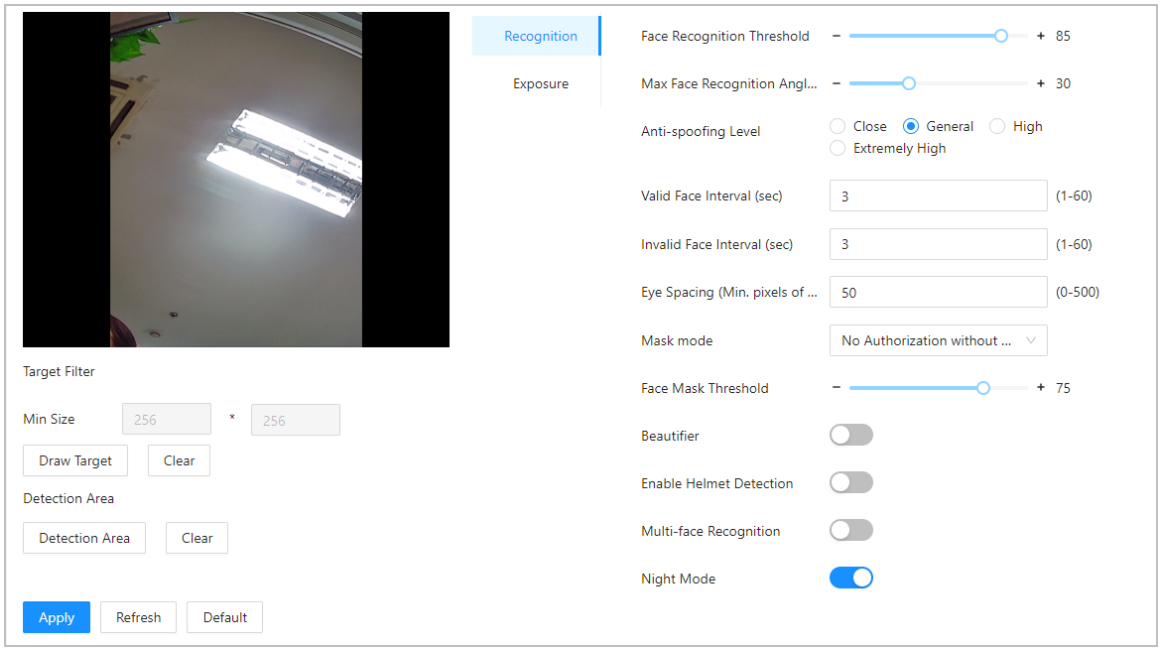
Настройте параметры обнаружения лиц.

Процедура

Шаг 1 Войдите на веб-страницу.

Шаг 2 Выбирать**Контроль доступа**>**Распознавание лиц**.

Рисунок 3-20 Параметры обнаружения лиц



Шаг 3 Настройте параметры.

Таблица 3-15 Описание параметров лица

Имя	Описание
Порог распознавания лица	Отрегулируйте уровень точности распознавания лиц. Более высокий порог означает более высокую точность и меньший уровень ложного распознавания.
Максимальное отклонение угла распознавания лица	Установите наибольший угол, под которым лицо может быть расположено для обнаружения лица. Чем больше значение, тем больше диапазон для угла лица. Если угол, под которым расположено лицо, не входит в заданный диапазон, оно может быть обнаружено неправильно.
Уровень защиты от подделки	Это не позволяет людям использовать фотографии, видео, маски и другие заменители для получения несанкционированного доступа.
Действительный интервал лиц (сек)	Если лицо человека успешно верифицировано слишком много раз, контроллер доступа выдает запрос об успешной верификации в течение определенного интервала времени.
Неверный интервал лиц (сек)	Если человеку не удается пройти верификацию лица слишком много раз, контроллер доступа выдает сообщение о неудачной верификации в течение определенного промежутка времени.
Расстояние между глазами (мин. пиксели расстояния между глазами)	Для успешного распознавания требуется определенное количество пикселей между глазами, называемое зрачковым расстоянием. Значение по умолчанию — 45 пикселей. Это число меняется в зависимости от размера лица и расстояния между лицом и линзой. Если взрослый человек находится на расстоянии 1,5 метра от линзы, зрачковое расстояние обычно составляет 50–70 пикселей.
Режим маски	● Режим маски: ◇ **Не обнаруживать**: Маска не обнаруживается при распознавании лица. ◇ **Напоминание о маске**: Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, но доступ ему все равно будет разрешен. ◇ **Без маски вход не разрешен**: Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, и доступ будет запрещен. ● Порог распознавания маски: чем выше порог, тем точнее будет распознавание лица человека в маске и тем ниже будет уровень ложного распознавания.
Украшатель	Украсьте сделанные снимки лиц.
Включить обнаружение шлема	Обнаруживает защитные каски. Дверь не откроется, если человек не носит каску.

Имя	Описание
Распознавание нескольких лиц	Распознает от 4 до 6 изображений лиц одновременно. Комбинированная разблокировка не может быть использована с этим, и дверь будет разблокирована, когда один из людей успешно пройдет проверку. Количество поддерживаемых изображений лиц может различаться в зависимости от модели продукта.
Ночной режим	В темных условиях на экране в режиме ожидания отображается белое фоновое изображение для повышения яркости при распознавании лица или QR-кода.
Режим осветителя	● Авто: Подсветка включается в условиях низкой освещенности. ● Отключить: осветитель постоянно выключен. Эта функция доступна только в некоторых моделях.

Шаг 4 Настройте параметры экспозиции.

Рисунок 3-21 Параметры экспозиции

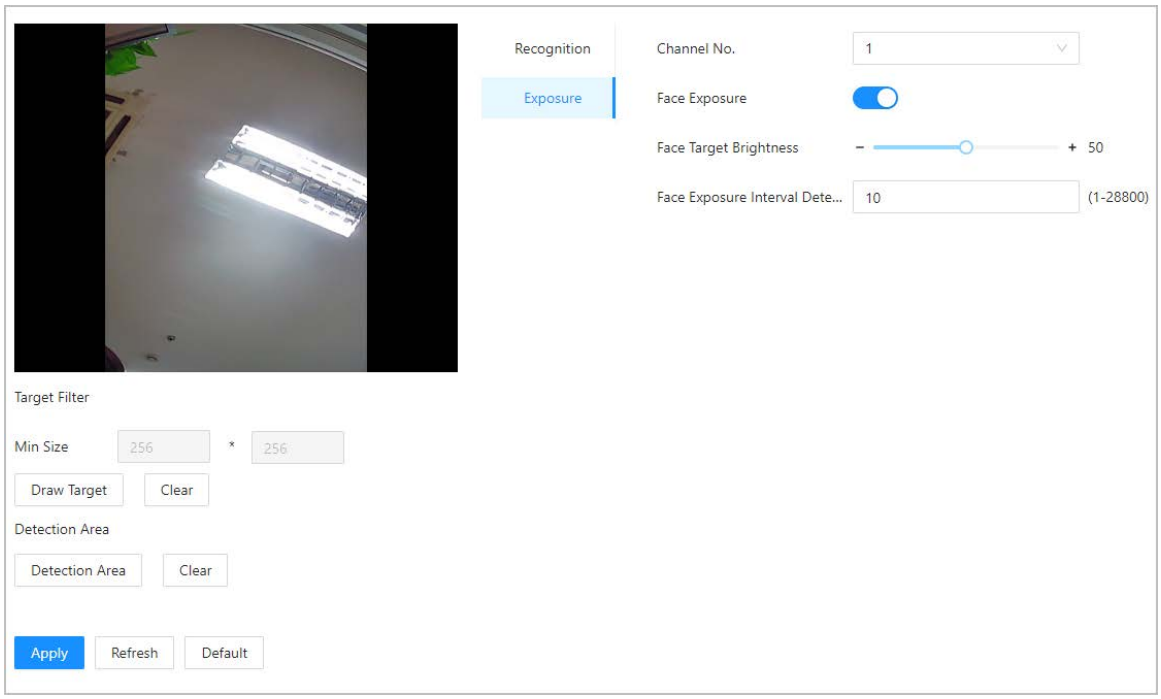


Таблица 3-16 Описание параметров воздействия

Параметр	Описание
Номер канала	● Канал 1 — режим белого света. ● Канал 2 — режим инфракрасного света.
Лицо экспонирование	После включения функции экспозиции лица лицо будет экспонироваться с заданной яркостью для четкого обнаружения изображения лица.
Определение интервала экспозиции лица	Лицо будет обнажаться только один раз в определенный промежуток времени.

Шаг 5 Нарисуйте область обнаружения лица. 1)

Нажмите**Определить регион**.

2) Щелкните правой кнопкой мыши, чтобы нарисовать область обнаружения, а затем отпустите левую кнопку мыши, чтобы

полный рисунок.

Лицо в указанной области будет обнаружено.

Шаг 6 Нарисуйте целевой размер.

1) Щелкните**Нарисуйте цель**

2) Нарисуйте рамку распознавания лиц, чтобы определить минимальный размер обнаруженного лица.

Контроллер доступа может обнаружить лицо только в том случае, если его размер превышает заданный размер.

Шаг 7 Нарисуйте зону обнаружения. Нажмите

Шаг 8 **хорошо**.

3.7.6 Настройка параметров карты

Справочная информация

Эта функция доступна только в некоторых моделях.

Процедура

Шаг 1 Войдите на веб-страницу.

Шаг 2 Выбирать**Контроль доступа**>**Настройки**

Шаг 3 **карты**. Настройте параметры карты.

Рисунок 3-22 Параметры карты

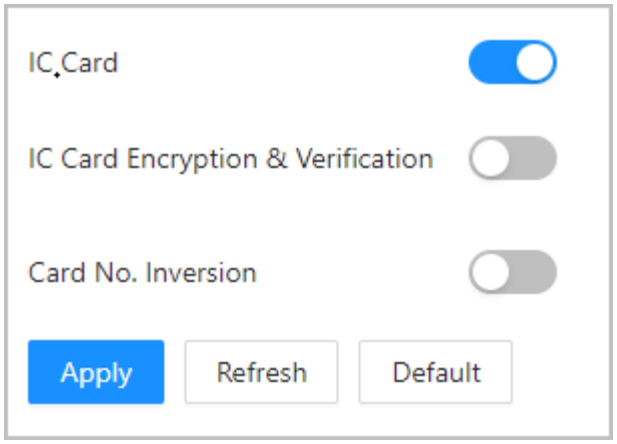


Таблица 3-17 Описание параметров карты

Параметр	Описание
IC-карта	При включении этой функции можно считать карту IC. Эта функция доступна только в некоторых моделях.
Шифрование и проверка IC-карт	Зашифрованную карту можно считать, если эта функция включена.
Номер карты. Инверсия	Когда контроллер доступа подключается к стороннему устройству через вход Wiegand, а номер карты, считываемый контроллером доступа, находится в обратном порядке от фактического номера карты. В этом случае вы можете включить эту функцию.

3.7.7 Настройка QR-кода

Процедура

Шаг 1 На веб-странице выберите**Контроль доступа**>**Настройки карты**.

Рисунок 3-23 QR-код

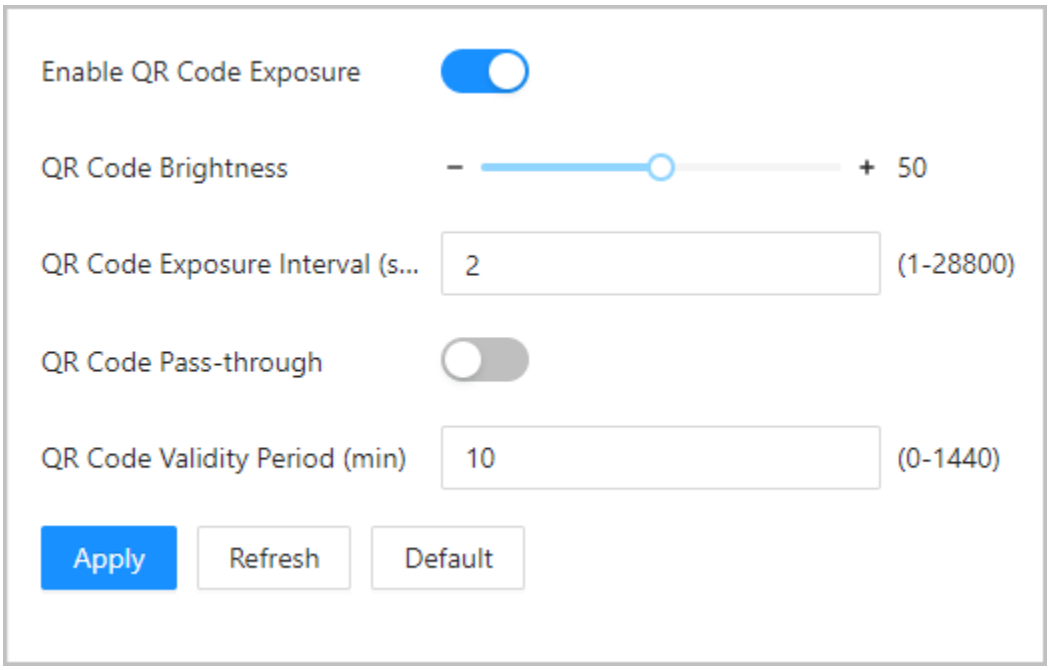


Таблица 3-18 Параметры QRR-кода

Параметры	Описание
Включить отображение QR-кода	QR-код будет экспонироваться с заданной яркостью, и его можно будет четко обнаружить и прочитать.
Яркость QR-кода	
Интервал экспозиции QR-кода (сек)	QR-код будет показан только один раз в течение определенного интервала времени.
Проход QR-кода	QR-код, считанный сторонней платформой.
Срок действия QR-кода (мин)	После того, как QR-код будет сгенерирован, срок действия ваших QR-кодов будет длиться в течение определенного времени, прежде чем истечет.

3.7.8 Настройка расписаний

Настройте временные интервалы и планы на праздничные дни, а затем определите, когда пользователь имеет право открывать двери.

3.7.8.1 Настройка периодов времени

Вы можете настроить до 128 групп (от № 0 до № 127) временных периодов. В каждом периоде вам необходимо настроить расписания доступа к двери на целую неделю. Люди могут открывать дверь только в течение запланированного времени.

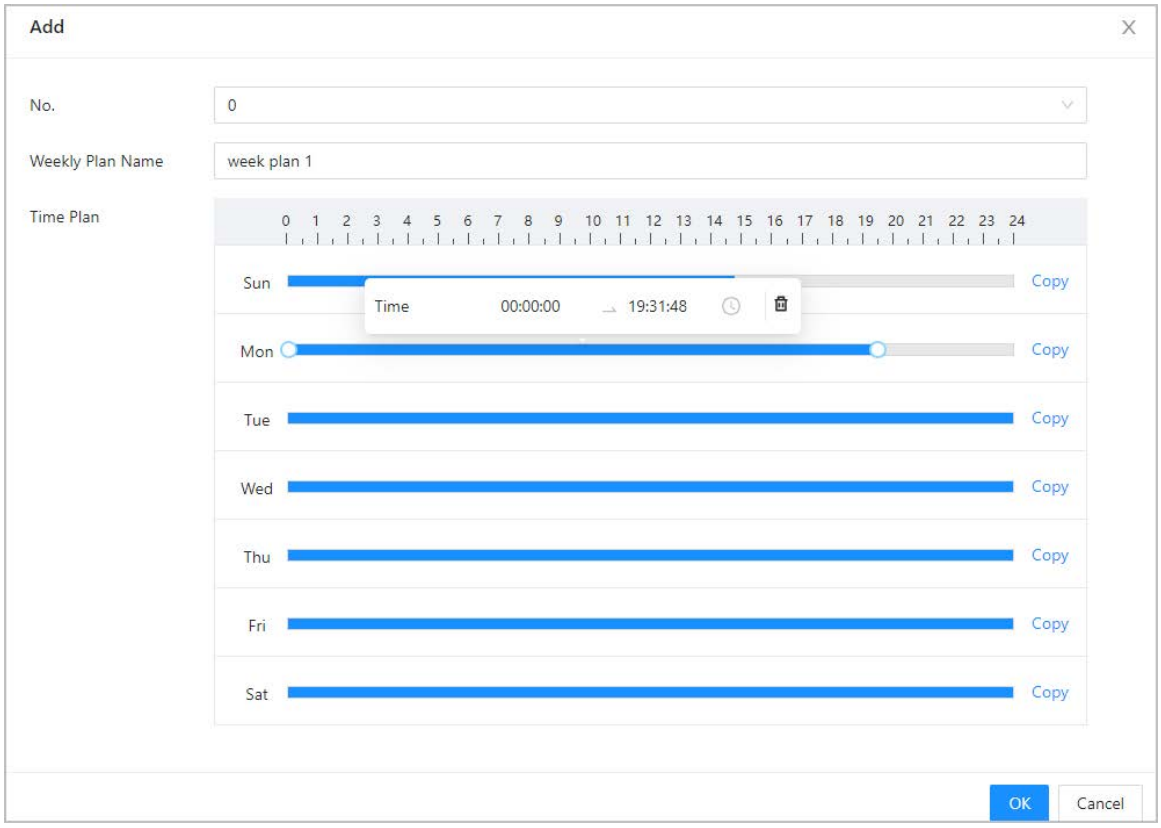
Процедура

Шаг 1 Войдите на веб-страницу.

Шаг 2 Выбирать**Контроль доступа**>**Конфигурация периода**>**Еженедельный план**. Нажмите

Шаг 3 **Добавлять**.

Рисунок 3-24 Настройка периодов времени



Шаг 4 Перетащите ползунок времени, чтобы настроить время для каждого дня.

Шаг 5 (Необязательно) Нажмите**Копировать**чтобы скопировать конфигурацию на остальные дни. Нажмите

Шаг 6 **ХОРОШО**.

3.7.8.2 Настройка планов на праздники

Вы можете настроить до 128 групп праздников (от № 0 до № 127), и для каждой группы праздников вы можете добавить до 16 праздников. После этого вы можете назначить настроенные группы праздников плану праздников. Пользователи могут открывать дверь только в определенное время в плане праздников.

Процедура

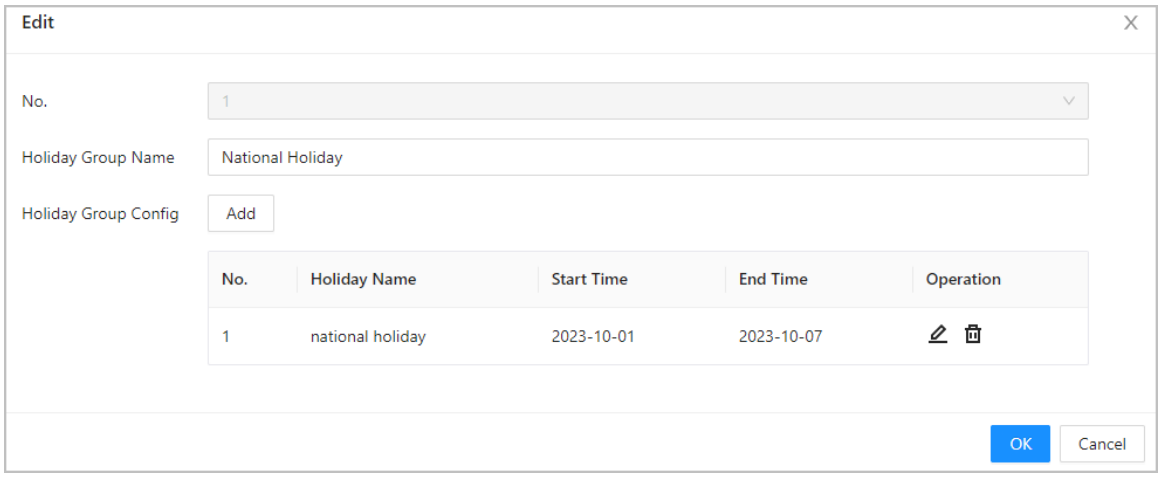
Шаг 1 Войдите на веб-страницу.

Шаг 2 Выбирать**Контроль доступа**>**Конфигурация периода**>**План отпуска**.

Шаг 3 Нажмите**Управление праздниками**, а затем нажмите**Добавлять**.

Шаг 4 Выберите номер для группы праздников, а затем введите название группы.

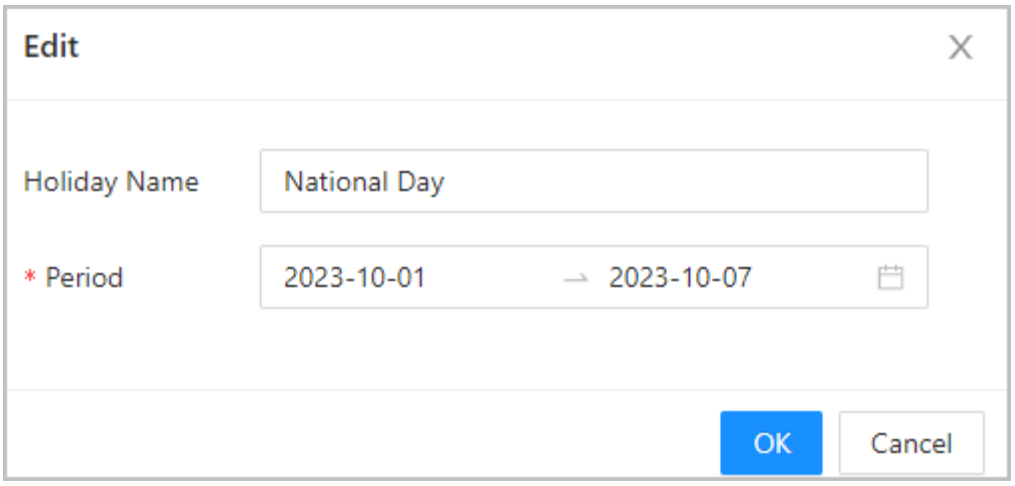
Рисунок 3-25 Добавить группу праздников



Шаг 5 Нажмите**Добавлять**, а затем добавьте праздник в группу праздников.

Шаг 6 Нажмите**ХОРОШО**.

Рисунок 3-26 Добавить праздник в группу праздников



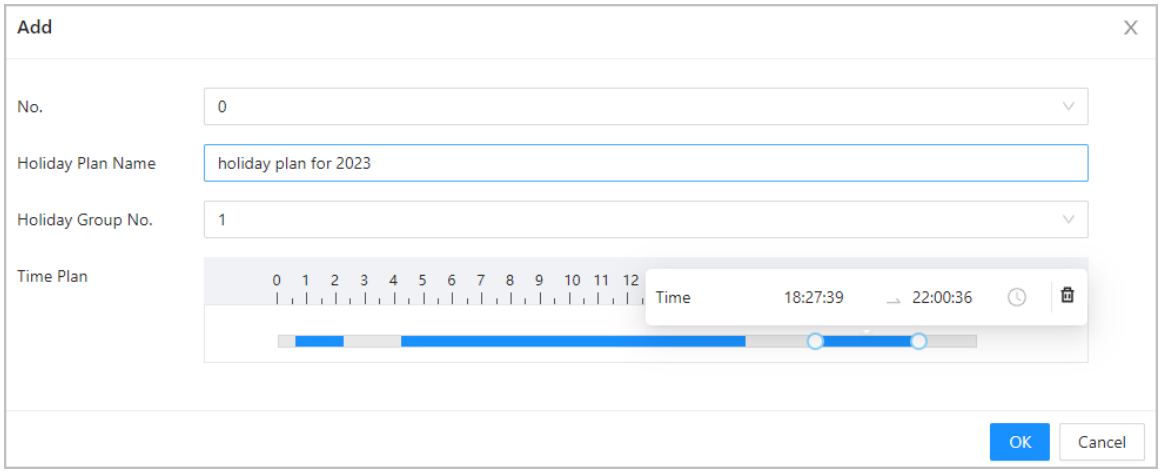
Шаг 7 Нажмите**План управления**, а затем нажмите**Добавлять**.

Шаг 8 Выберите номер для плана отпуска, а затем введите его название.

Шаг 9 Выберите группу праздников, а затем перетащите ползунок, чтобы настроить время для каждого дня.

Поддерживает добавление до 4 временных разделов в день.

Рисунок 3-27 Добавить план отпуска



Шаг 10 Нажмите**ХОРОШО**.

3.7.9 Настройка модулей расширения

Для контроллера доступа, поддерживающего подключение модулей расширения, настройте тип модуля, поддерживаемого контроллером доступа.

Справочная информация

- Тип модуля расширения может отличаться в зависимости от модели контроллера доступа.
- Настройки модуля расширения сохраняются после восстановления заводских настроек контроллера доступа.

Процедура

Шаг 1 На веб-странице выберите**Контроль доступа**>**Модуль расширения**.

Шаг 2 Выберите тип модуля, который поддерживает Access Controller. Нажмите

Шаг 3 **Применять**.

Конфигурации вступают в силу после перезапуска контроллера доступа.

- отображается в правом углу контроллера доступа, если настройка вступила в силу.
- отображается в правом углу контроллера доступа, что означает, что тип настроенного вами модуля расширения не соответствует фактическому модулю расширения, подключенному к контроллеру доступа.
- Если**Никто**выбран и к контроллеру доступа не подключен модуль расширения, значок модуля расширения отображаться не будет.

3.7.10 Настройка функций порта

Некоторые порты могут функционировать как разные порты, вы можете настроить их на разные порты в зависимости от фактических потребностей.

Справочная информация

- Эта функция доступна только в некоторых моделях.
- Порты могут отличаться в зависимости от модели продукта.

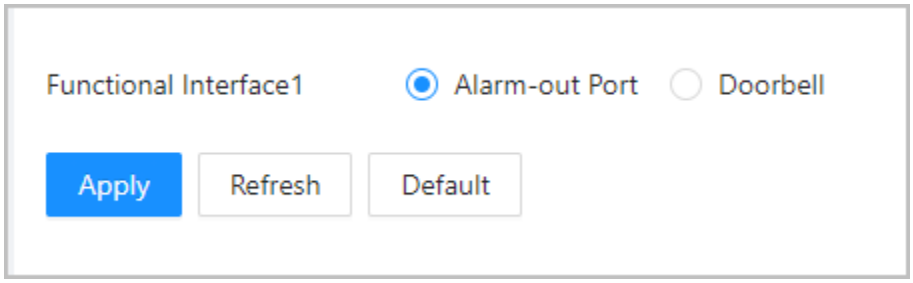
Процедура

Шаг 1 На веб-странице выберите**Контроль доступа**>**Конфигурация**

Шаг 2 **порта**. Выберите тип порта.

Шаг 3 Нажмите**Применять**.

Рисунок 3-28 Настройка портов



3.8 Настройка аудио и видео

3.8.1 Настройка видео

На главной странице выберите**Видео Настройка**, а затем настройте видеопоток, статус, изображение и экспозицию.

Справочная информация

- Стандарт видео: Выбрать**НТСК**.
- Идентификатор канала: Канал 1 предназначен для конфигураций изображения в видимом свете. Канал 2 предназначен для конфигураций изображения в инфракрасном свете.
- По умолчанию: восстановить настройки по умолчанию.
- Захват: сделать снимок текущего изображения.

Стандарт видео PAL — 25 кадров в секунду, а стандарт видео NTSC — 30 кадров в секунду.

3.8.1.1 Настройка канала 1

Процедура

Шаг 1 Выбирать**Конфигурация аудио и видео**>**Видео**.

Шаг 2 Выбирать**1**из**Номер канала**список. Настройте скорость

Шаг 3 передачи данных.

Рисунок 3-29 Скорость передачи данных

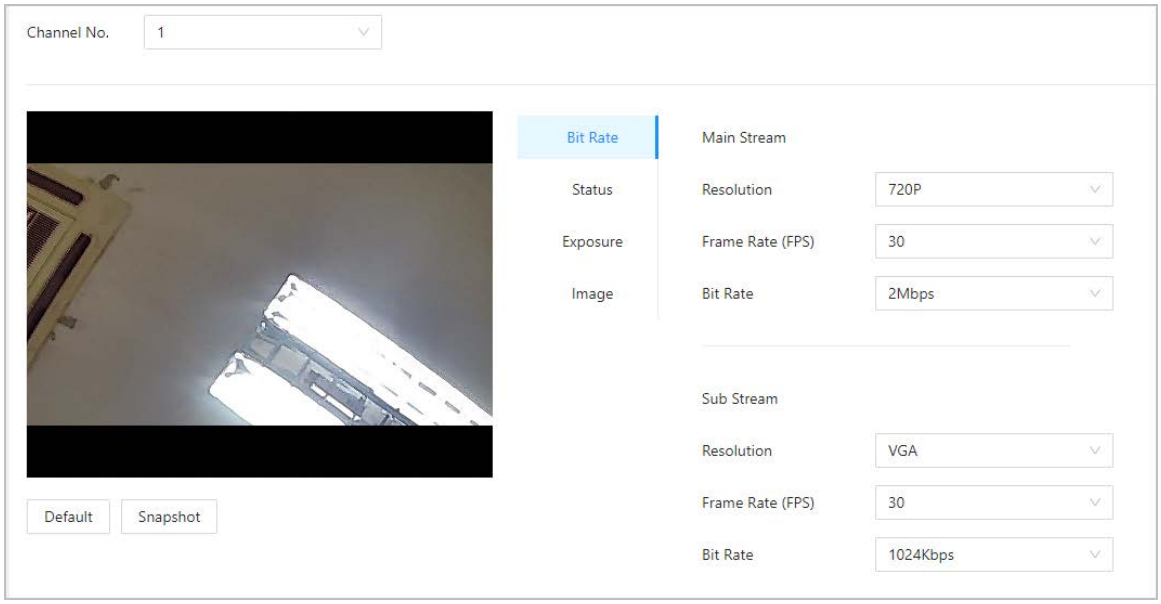


Таблица 3-19 Описание скорости передачи данных

Параметр		Описание
Основной формат	Разрешение	Когда контроллер доступа функционирует как VTO и подключается к VTH, Полученный предел потока VTH составляет 720p. При изменении разрешения на 1080p вызов и функционирование монитора может быть нарушено.
	Частота кадров (кадров в секунду)	Количество кадров (или изображений) в секунду.
	Скорость передачи данных	Объем данных, переданных через интернет-соединение за определенное время. Выберите подходящую пропускную способность в зависимости от скорости вашей сети.
Дополнительный поток	Разрешение	Дополнительный поток поддерживает D1, VGA и QVGA.
	Частота кадров (кадров в секунду)	Количество кадров (или изображений) в секунду.
	Скорость передачи данных	Он показывает объем данных, переданных через интернет-соединение за определенный промежуток времени.

Шаг 4 Настройте статус.

Рисунок 3-30 Статус

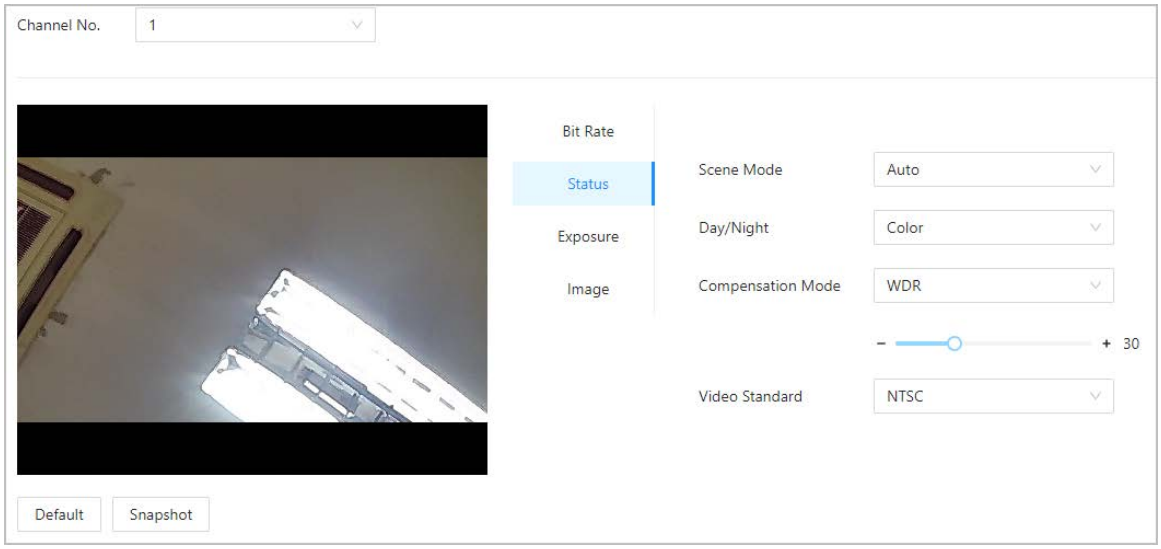


Таблица 3-20 Описание изображения

Параметр	Описание
Режим сцены	Оттенок изображения отличается в разных режимах сцены. ● **Закрывать**: Функция режима сцены отключена. ● **Авто**: Система автоматически настраивает режим сцены на основе фотографической чувствительности. ● **Солнечно**: В этом режиме оттенок изображения будет уменьшен. ● **Ночь**: В этом режиме оттенок изображения будет увеличен.

Параметр	Описание
День/Ночь	Режим «День/Ночь» влияет на компенсацию освещенности в различных ситуациях. ● **Авто**: Система автоматически настраивает режим «день/ночь» на основе фотографической чувствительности. ● **Красочный**: В этом режиме изображения цветные. ● **Черно-белый**: В этом режиме изображения черно-белые.
Режим компенсации	● **Запрещать**: Компенсация отключена. ● **БЛК**: Компенсация контрового света автоматически добавляет больше света в темные области изображения, когда яркий свет сзади затмевает их. ● **ВДР**: Система затемняет яркие области и компенсирует темные области, создавая баланс для улучшения общего качества изображения. ● **КЛК**: Компенсация засветки (HLC) — это технология, используемая в камерах видеонаблюдения/IP-камерах безопасности для обработки изображений, которые подвергаются воздействию света, например, фар или прожекторов. Датчик изображения камеры обнаруживает сильные световые пятна на видео и уменьшает экспозицию в этих точках, чтобы улучшить общее качество изображения.

Шаг 5 Настройте параметры экспозиции.

Рисунок 3-31 Экспозиция

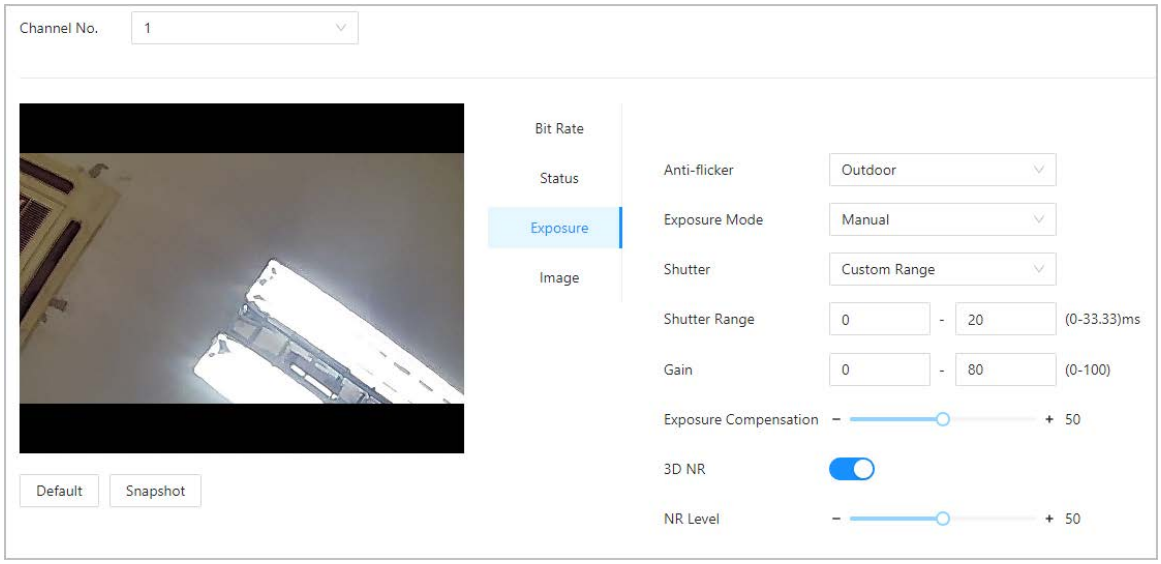


Таблица 3-21 Описание параметров экспозиции

Параметр	Описание
Антимерцание	Установите функцию «Антимерцание», чтобы уменьшить мерцание и уменьшить неравномерность цветов или экспозиции. ● **50 Гц**: Если частота электросети составляет 50 Гц, экспозиция автоматически регулируется в зависимости от яркости окружающей среды, чтобы предотвратить появление горизонтальных линий. ● **60 Гц**: Если частота электросети составляет 60 Гц, экспозиция автоматически регулируется в зависимости от яркости окружающей среды, чтобы уменьшить появление горизонтальных линий. ● **На открытом воздухе**: Когда**На открытом воздухе**выбран, можно переключить режим экспозиции.

Параметр	Описание
Режим экспозиции	Вы можете настроить экспозицию, чтобы отрегулировать яркость изображения. ● **Авто**: Контроллер доступа автоматически регулирует яркость изображений в зависимости от окружающей обстановки. ● **Приоритет выдержки**: Контроллер доступа регулирует яркость изображения в соответствии с установленным диапазоном затвора. Если изображение недостаточно яркое, но значение затвора достигло своего верхнего или нижнего предела, контроллер доступа автоматически отрегулирует значение усиления для идеального уровня яркости. ● **Руководство**: Вы можете вручную отрегулировать усиление и значение затвора, чтобы отрегулировать яркость изображения. ◇ Когда вы выбираете**На открытом воздухе**из**Антимерцание**список, вы можете выбрать**Приоритет выдержки**как режим экспозиции. ◇ Режим экспозиции может отличаться в зависимости от модели контроллера доступа.
Затвор	Затвор — это компонент, который позволяет свету проходить в течение определенного периода. Чем выше скорость затвора, тем короче время экспозиции и тем темнее изображение.
Прирост	При установке диапазона значений усиления качество видео улучшится.
Контакт Компенсация	Видео станет ярче за счет регулировки значения компенсации экспозиции.
3D NR	При включении функции 3D-шумоподавление (RD) можно снизить уровень видеошума, чтобы обеспечить более высокую четкость видео. Вы можете установить его оценку, когда эта функция включена. Более высокая оценка означает более четкое изображение.
Оценка	

Шаг 6 Настройте изображение.

Рисунок 3-32 Изображение

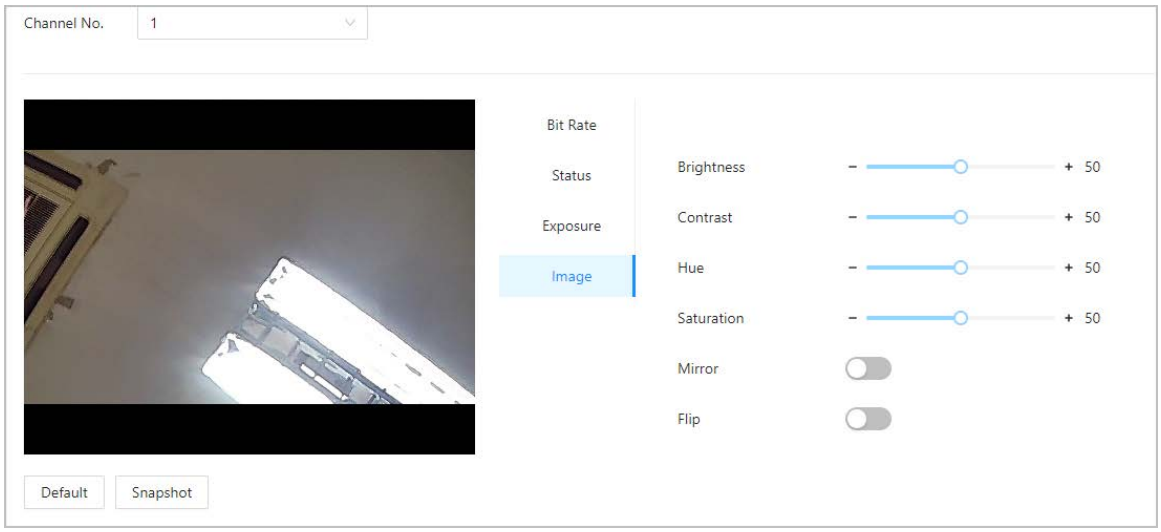


Таблица 3-22 Описание изображения

Параметр	Описание
Яркость	Яркость изображения. Более высокое значение означает более яркие изображения.
Контраст	Контрастность — это разница в яркости или цвете, которая делает объект различимым. Чем больше значение контрастности, тем больше будет цветовой контраст.
Оттенок	Относится к силе или насыщенности цвета. Описывает интенсивность цвета или его чистоту.
Насыщенность	Насыщенность цвета указывает на интенсивность цвета на изображении. По мере увеличения насыщенности цвета кажутся сильнее, например, более красными или более синими. Значение насыщенности не изменяет яркость изображения.
Зеркало	При включении функции изображения будут отображаться с перевернутыми левой и правой сторонами.
Подбросить	При включении этой функции изображения можно переворачивать.

3.8.1.2 Настройка канала 2

Процедура

Шаг 1 Выбирать**Конфигурация аудио и видео**>

Шаг 2 **Видео**. Выбирать**2**из**Номер канала**список.

Шаг 3 Выберите 2 из**Номер канала**. Настройте

Шаг 4 статус видео.

Мы рекомендуем включать функцию WDR, когда лицо находится в контровом свете.

Рисунок 3-33 Настройка статуса

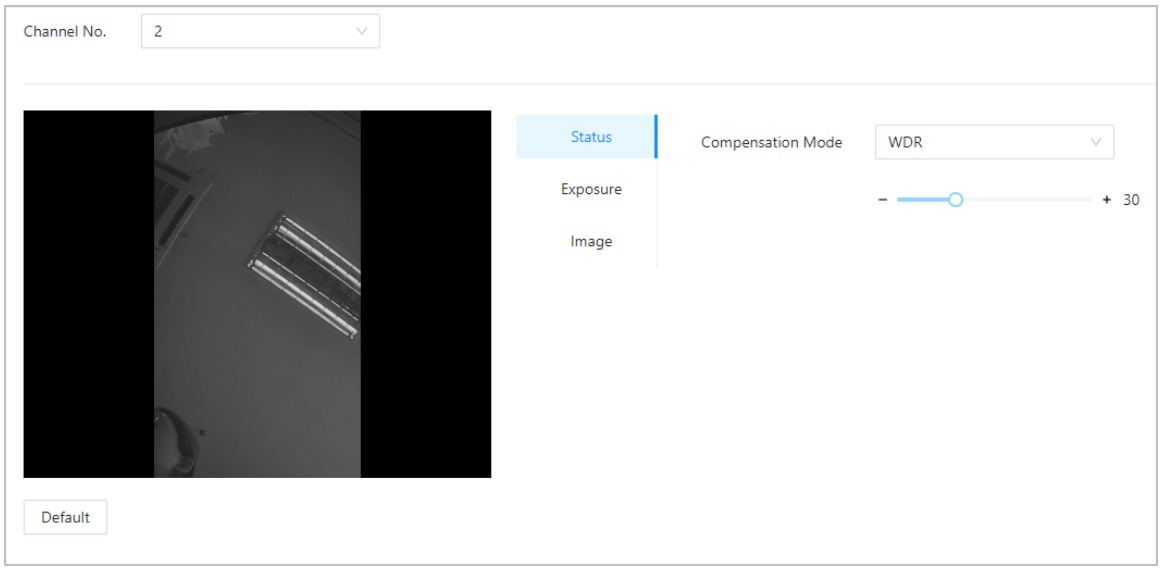


Таблица 3-23 Описание статуса

Параметр	Описание
Режим компенсации	● **Запрещать**: Компенсация отключена. ● **БЛК**: Компенсация контрового света автоматически добавляет больше света в темные области изображения, когда яркий свет сзади затмевает их. ● **ВДР**: Система затемняет яркие области и компенсирует темные области, создавая баланс для улучшения общего качества изображения. ● **КЛК**: Компенсация засветки (HLC) — это технология, используемая в камерах видеонаблюдения/IP-камерах безопасности для обработки изображений, которые подвергаются воздействию света, например, фар или прожекторов. Датчик изображения камеры обнаруживает сильные световые пятна на видео и уменьшает экспозицию в этих точках, чтобы улучшить общее качество изображения.

Шаг 5 Настройте параметры экспозиции.

Рисунок 3-34 Параметр экспозиции

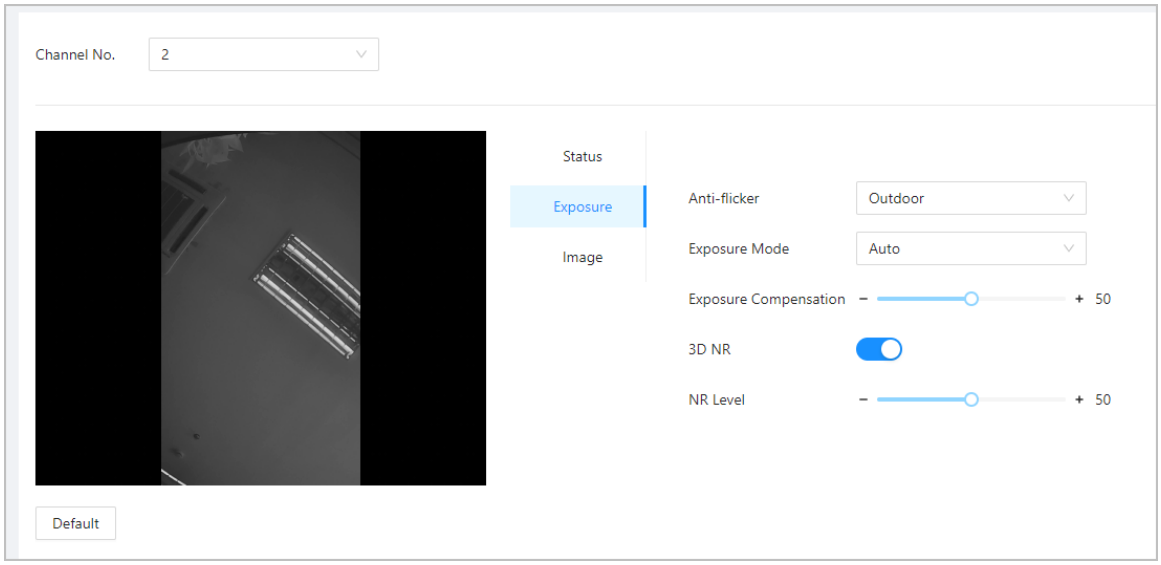


Таблица 3-24 Описание параметров экспозиции

Параметр	Описание
Антимерцание	Установите функцию «Антимерцание», чтобы уменьшить мерцание и уменьшить неравномерность цветов или экспозиции. ● **50 Гц**: Если частота электросети составляет 50 Гц, экспозиция автоматически регулируется в зависимости от яркости окружающей среды, чтобы предотвратить появление горизонтальных линий. ● **60 Гц**: Если частота электросети составляет 60 Гц, экспозиция автоматически регулируется в зависимости от яркости окружающей среды, чтобы уменьшить появление горизонтальных линий. ● **На открытом воздухе**: Когда**На открытом воздухе**выбран, можно переключить режим экспозиции.

Параметр	Описание
Режим экспозиции	Вы можете настроить экспозицию, чтобы отрегулировать яркость изображения. ● **Авто**: Контроллер доступа автоматически регулирует яркость изображений в зависимости от окружающей обстановки. ● **Приоритет выдержки**: Контроллер доступа регулирует яркость изображения в соответствии с установленным диапазоном затвора. Если изображение недостаточно яркое, но значение затвора достигло своего верхнего или нижнего предела, контроллер доступа автоматически отрегулирует значение усиления для идеального уровня яркости. ● **Руководство**: Вы можете вручную отрегулировать усиление и значение затвора, чтобы отрегулировать яркость изображения. ◇ Когда вы выбираете**На открытом воздухе**из**Антимерцание**список, вы можете выбирать**Приоритет выдержки**как режим экспозиции. ◇ Режим экспозиции может отличаться в зависимости от модели контроллера доступа.
Контакт Компенсация	Видео станет ярче за счет регулировки значения компенсации экспозиции.
3D NR	При включении функции 3D-шумоподавление (RD) можно снизить уровень видеошума, чтобы обеспечить более высокую четкость видео.
Уровень HP	Вы можете установить его оценку, когда эта функция включена. Более высокая оценка означает более четкое изображение.

Шаг 6 Настройте параметры изображения.

Рисунок 3-35 Параметры изображения

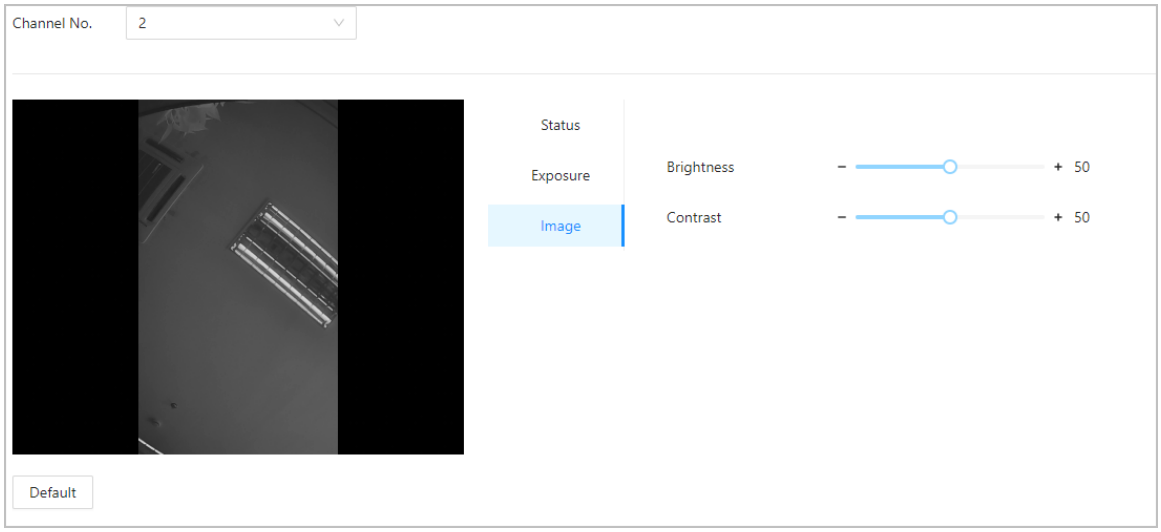


Таблица 3-25 Описание изображения

Параметр	Описание
Яркость	Яркость изображения. Более высокое значение означает более яркие изображения.
Контраст	Контрастность — это разница в яркости или цвете, которая делает объект различимым. Чем больше значение контрастности, тем больше будет цветовой контраст.

3.8.2 Настройка звуковых подсказок

Установите звуковые подсказки при проверке личности.

Процедура

Шаг 1 Выбирать**Конфигурация аудио и видео**>

Шаг 2 **Аудио**. Настройте параметры звука.

Рисунок 3-36 Настройка параметров звука

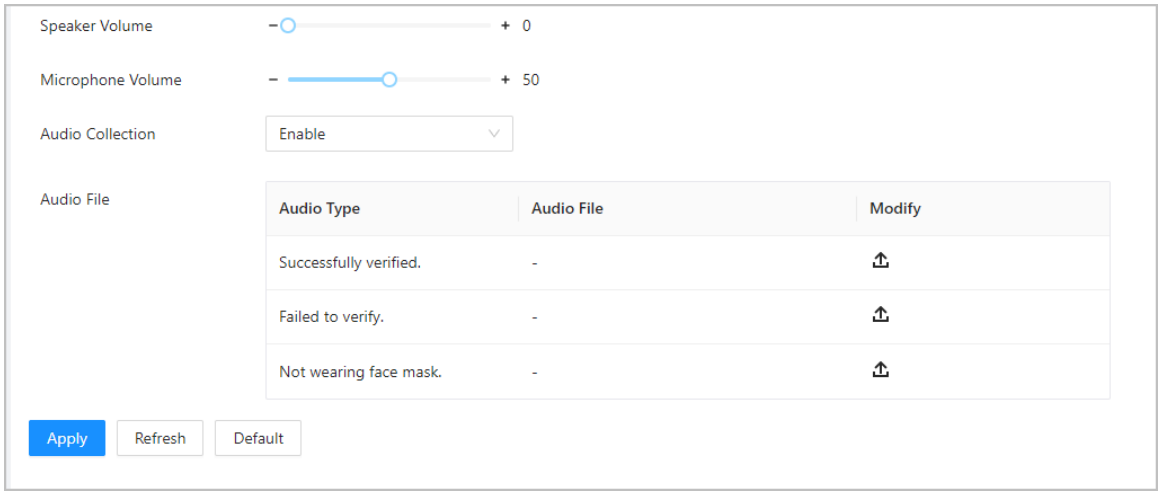


Таблица 3-26 Описание параметров

Параметры	Описание
Спикер	Перетащите ползунок, чтобы отрегулировать громкость динамика.
Громкость микрофона	Перетащите ползунок, чтобы отрегулировать громкость микрофона.
Аудио Коллекция	Если эта функция не включена, во время видеоразговора звук записываться не будет.
Аудиофайл	Нажмите Загрузить аудиофайлы на платформу.

Шаг 3 Нажмите для загрузки аудиофайлов на платформу для каждого типа аудио.

Формат — MP3, размер — менее 20 КБ.

Шаг 4 Нажмите**Применять**.

3.8.3 Настройка обнаружения движения

При обнаружении движущихся объектов и достижении установленного порогового значения экран активируется.

Процедура

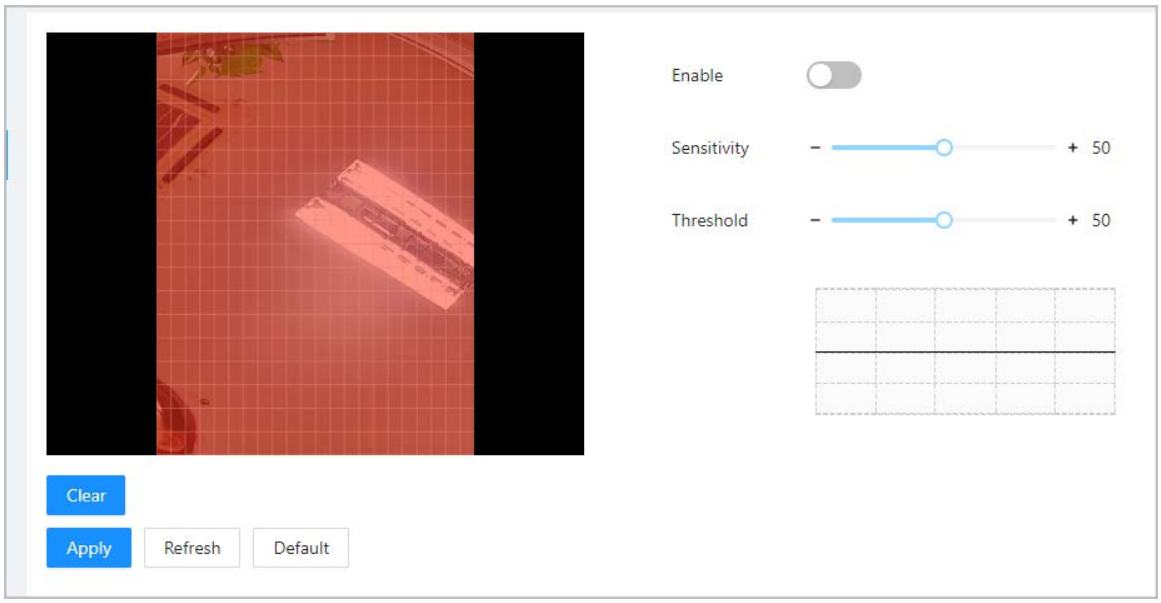
Шаг 1 Выбирать**Конфигурация аудио и видео**>**Настройки обнаружения движения**.

Шаг 2 Включите функцию обнаружения движения.

Шаг 3 Нажмите и удерживайте левую кнопку мыши, а затем нарисуйте область обнаружения в красной области.

- Зона обнаружения движения отображается красным цветом.
- Чтобы удалить существующую область обнаружения движения, нажмите**Прозрачный**.
- Нарисованная вами область обнаружения движения не будет областью обнаружения движения, если вы нарисуете область обнаружения движения по умолчанию.

Рисунок 3-37 Зона обнаружения движения



Шаг 4 Настройте параметры.

- Чувствительность: Чувствительность к окружающей среде. Более высокая чувствительность означает более легкое срабатывание сигнализации.
- Порог: процент площади движущегося объекта в зоне обнаружения движения. Более высокий порог означает более легкое срабатывание тревоги.

Шаг 5 Нажмите**Применять**.

Обнаружение движения срабатывает, когда отображаются красные линии; зеленые линии отображаются, когда обнаружение движения не срабатывает.

3.8.4 Настройка локального кодирования

Установите область просмотра в видеообсуждении и предварительном просмотре.

Справочная информация

- Эта функция доступна только в некоторых моделях.
- Эта функция включена по умолчанию при работе с VTH. Предварительный просмотр может быть не доступно, когда эта функция отключена.

Процедура

Шаг 1 Войдите на веб-страницу.

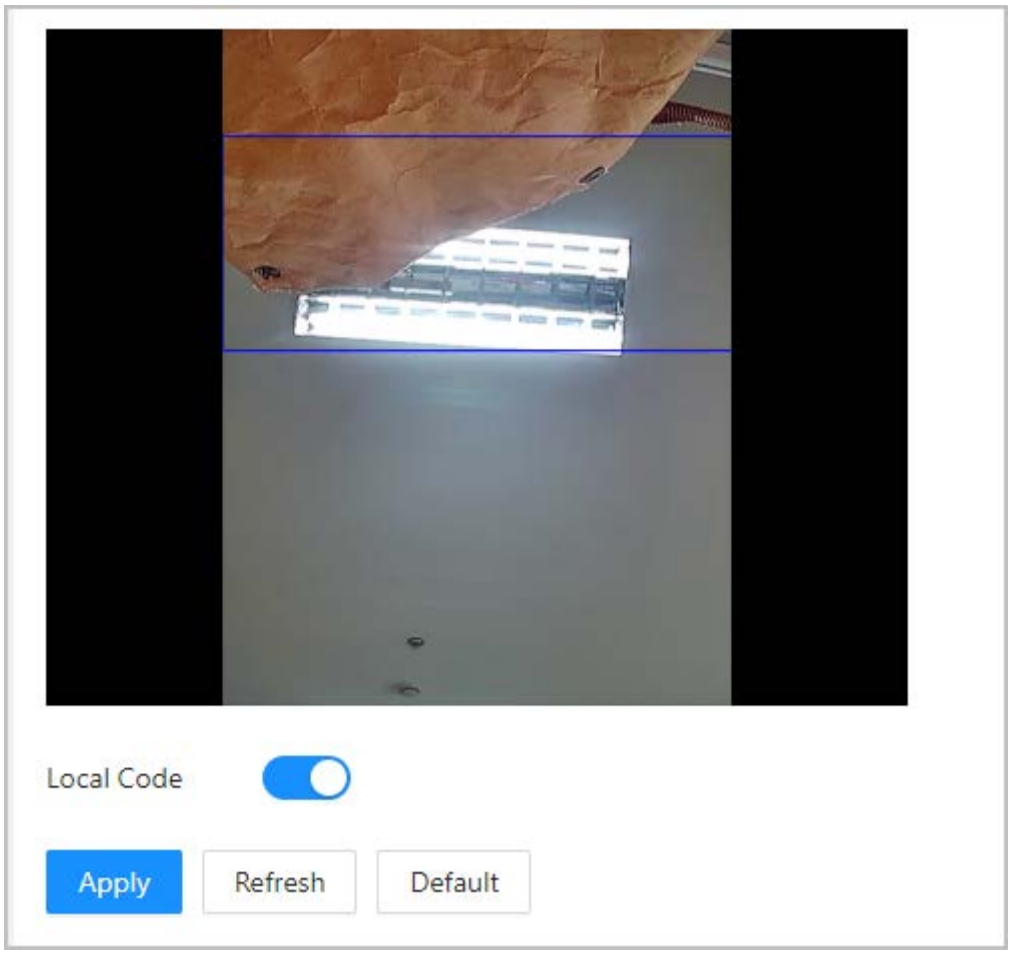
Шаг 2 Выбирать**Конфигурация аудио и видео**>**Настройки обнаружения движения**.

Шаг 3 Выбирать**Давать возможность**Чтобы включить функцию, перетащите поле в

Шаг 4 указанное место.

Поле обозначает область предварительного просмотра во время видеоконференции.

Рисунок 3-38 Локальное кодирование



Шаг 5 Нажмите**Применять**.

3.9 Настройка сети

3.9.1 Настройка TCP/IP

Вам необходимо настроить IP-адрес контроллера доступа, чтобы убедиться, что он может взаимодействовать с другими устройствами.

Процедура

Шаг 1 Выбирать**Настройки связи**>**TCP/IP**.

Шаг 2 Настройте параметры.

Рисунок 3-39 TCP/IP

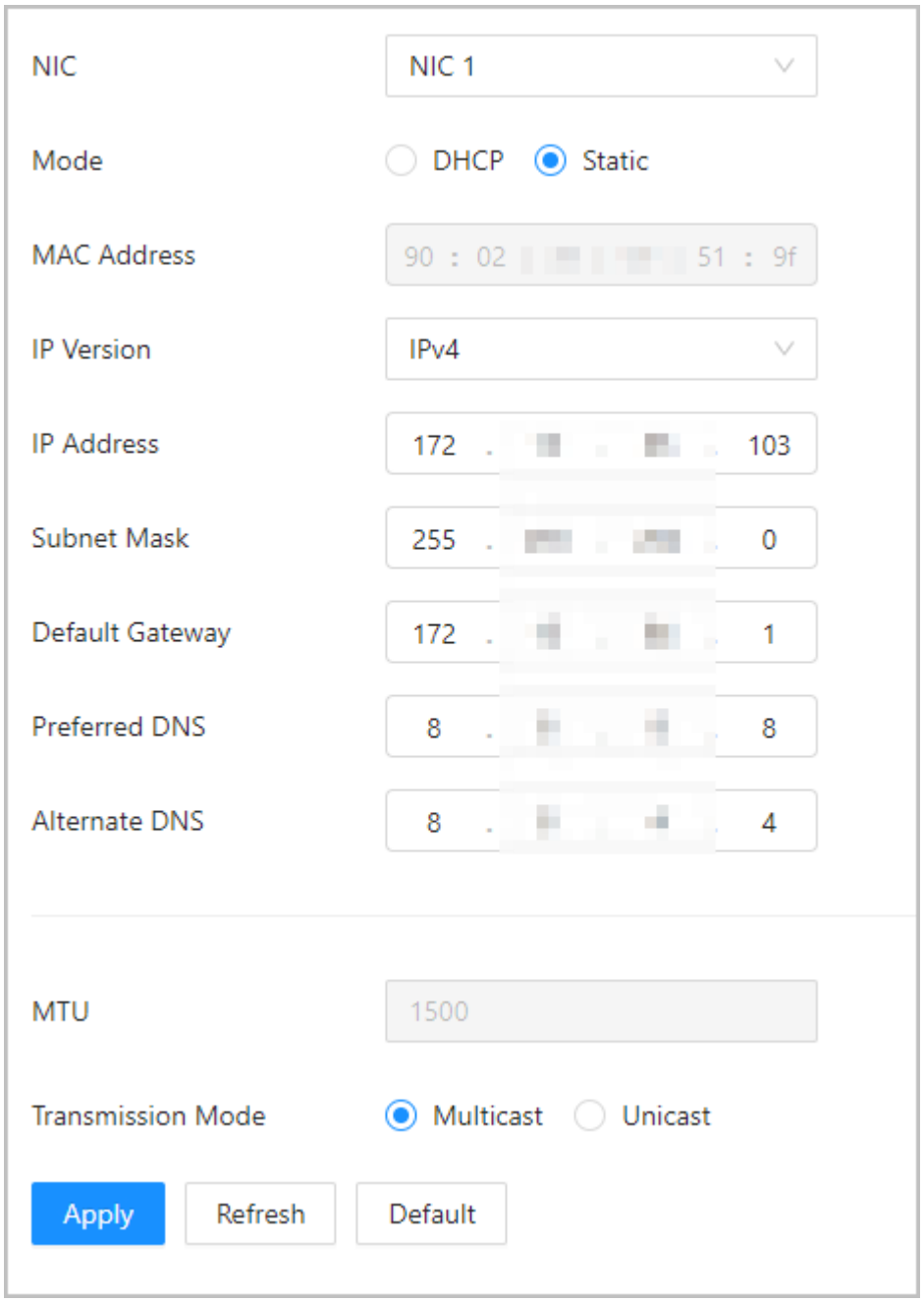


Таблица 3-27 Описание TCP/IP

Параметр	Описание
Режим	● **Статичный**: Введите вручную IP-адрес, маску подсети и шлюз. ● **DHCP**: Это означает Dynamic Host Configuration Protocol. При включении DHCP контроллеру доступа автоматически назначаются IP-адрес, маска подсети и шлюз.
MAC-адрес	MAC-адрес контроллера доступа.
IP-версия	IPv4 или IPv6.
IP-адрес	Если вы установите режим**Статичный**, настройте IP-адрес, маску подсети и шлюз.
Маска подсети	

Параметр	Описание
Шлюз по умолчанию	 ● Адрес IPv6 представлен в шестнадцатеричном формате. ● Версия IPv6 не требует установки масок подсети. ● IP-адрес и шлюз по умолчанию должны находиться в одном сегменте сети.
Предпочтительный DNS	Установите IP-адрес предпочитаемого DNS-сервера.
Альтернативный DNS	Установите IP-адрес альтернативного DNS-сервера.
МТУ	MTU (Maximum Transmission Unit) относится к максимальному размеру данных, которые могут быть переданы в одном сетевом пакете в компьютерных сетях. Большее значение MTU может повысить эффективность передачи данных в сети за счет сокращения количества пакетов и связанных с ними сетевых издержек. Если устройство на сетевом пути не может обрабатывать пакеты определенного размера, это может привести к фрагментации пакетов или ошибкам передачи. В сетях Ethernet общее значение MTU составляет 1500 байт. Однако в некоторых случаях, таких как использование PPPoE или VPN, могут потребоваться меньшие значения MTU для удовлетворения требований определенных сетевых протоколов или служб. Ниже приведены рекомендуемые значения MTU для справки: ● 1500: Максимальное значение для пакетов Ethernet, также значение по умолчанию. Это типичная настройка для сетевых подключений без PPPoE и VPN, некоторых маршрутизаторов, сетевых адаптеров и коммутаторов. ● 1492: Оптимальное значение для PPPoE ● 1468: Оптимальное значение для DHCP. ● 1450: Оптимальное значение для VPN.
Режим передачи	● Многоадресная передача: идеально подходит для видеоконференций. ● Unicast: идеально подходит для групповых звонков.

Шаг 3 Нажмите**ХОРОШО**.

3.9.2 Настройка Wi-Fi

Процедура

Шаг 1 Выбирать**Настройки связи**>**TCP/IP**.

Шаг 2 Включите Wi-Fi.

Отображаются все доступные сети Wi-Fi.

Функция Wi-Fi доступна только в некоторых моделях.

Шаг 3 Кран+, а затем введите пароль Wi-Fi.

3.9.3 Настройка порта

Вы можете ограничить доступ к контроллеру доступа одновременно через веб-страницу, настольный клиент и

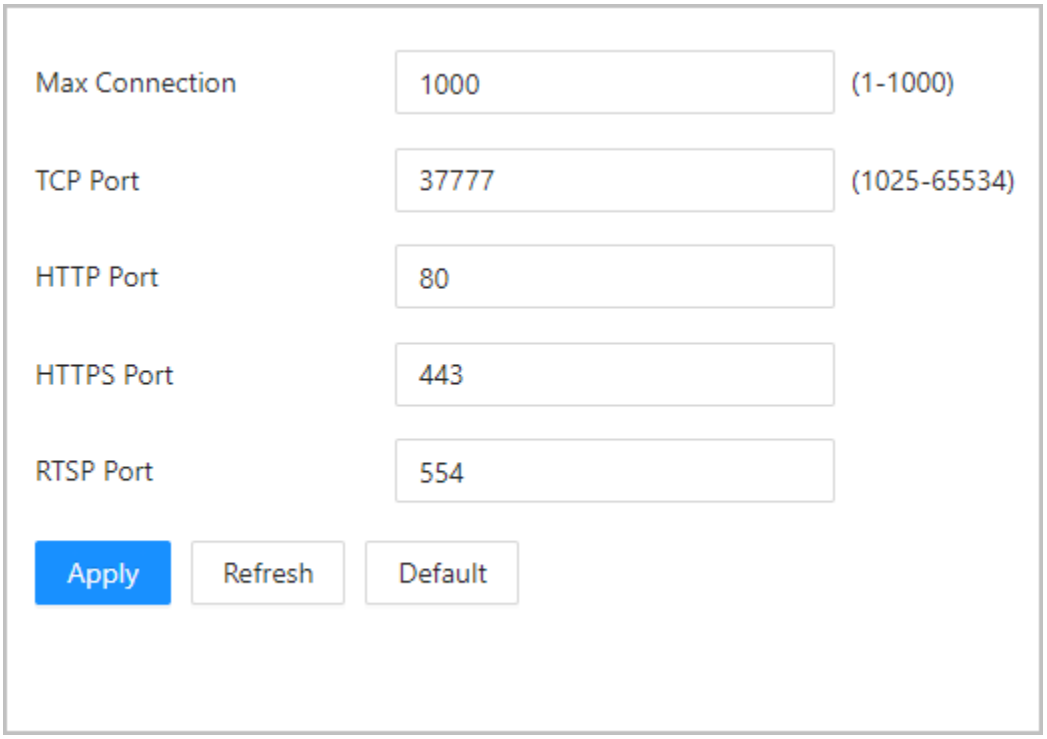
мобильный клиент.

Процедура

Шаг 1 Выбирать**Настройки связи**>**Порт**.

Шаг 2 Настройте порты.

Рисунок 3-40 Настройка портов



За исключением**Макс. соединение**и**RTSP-порт**, вам необходимо перезапустить контроллер доступа, чтобы вступайте в силу после изменения других параметров.

Таблица 3-28 Описание портов

Параметр	Описание
Макс. соединение	Вы можете установить максимальное количество клиентов (например, веб-страница, настольный клиент и мобильный клиент), которые могут получить доступ к контроллеру доступа одновременно.
TCP-порт	Значение по умолчанию — 37777.
HTTP-порт	Значение по умолчанию — 80. Если вы изменили номер порта, добавьте номер порта после IP-адреса при доступе к веб-странице.
HTTPS-порт	Значение по умолчанию — 443.
RTSP-порт	Значение по умолчанию — 554.

Шаг 3 Нажмите**Применять**.

3.9.4 Настройка базовой службы

Если вы хотите подключить контроллер доступа к сторонней платформе, включите CGI и

Функции ONVIF.

Процедура

Шаг 1 Выбирать**Настройки сети**>**Базовые услуги**.

Шаг 2 Настройте базовую услугу.

Рисунок 3-41 Базовая услуга

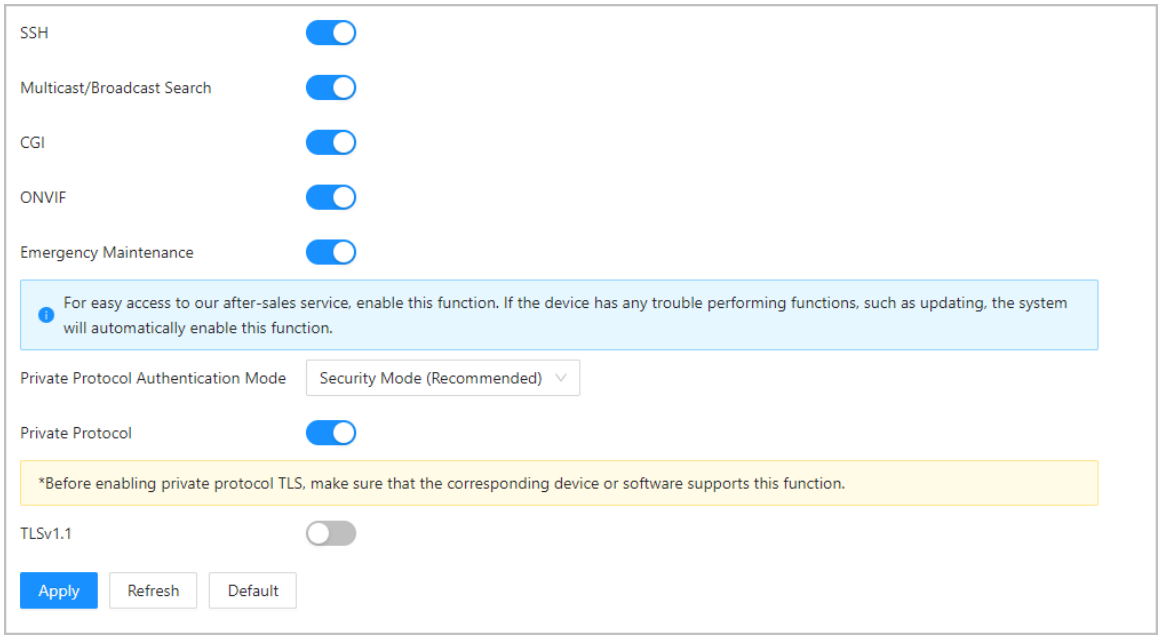


Таблица 3-29 Описание основных параметров сервиса

Параметр	Описание
SSH	SSH (Secure Shell Protocol) — это протокол удаленного администрирования, который позволяет пользователям получать доступ к своим удаленным серверам, управлять ими и изменять их через Интернет.
Поиск Multicast/Broadcast	Поиск устройств по протоколу многоадресной или широковещательной передачи.
CGI	Интерфейс общего шлюза (CGI) представляет собой точку пересечения веб-серверов, через которую возможен стандартизированный обмен данными между внешними приложениями и серверами.
ONVIF	ONVIF означает Open Network Video Interface Forum (Форум открытого сетевого видеоинтерфейса). Его цель — предоставить стандарт для интерфейса между различными устройствами безопасности на базе IP. Эти стандартизированные ONVIF Спецификации подобны общему языку, который могут использовать все устройства для общения.
Аварийное обслуживание	По умолчанию эта функция включена.
Частный протокол Режим аутентификации	Установите режим аутентификации, включая безопасный режим и режим совместимости. Рекомендуется выбрать**Режим безопасности**. ● Режим безопасности (рекомендуется): не поддерживает доступ к устройству с помощью методов аутентификации Digest, DES и открытого текста, что повышает безопасность устройства. ● Совместимый режим: поддерживает доступ к устройству с помощью методов аутентификации Digest, DES и открытого текста с пониженной безопасностью.

Параметр	Описание
Частный протокол	Платформа добавляет устройства по протоколу TLSv1.1.  При включении TLSv1.1 могут возникнуть риски безопасности. Обратите внимание.

Шаг 3 Нажмите**Применять**.

3.9.5 Настройка облачного сервиса

Облачный сервис предоставляет услугу проникновения NAT. Пользователи могут управлять несколькими устройствами через DMSS.

Вам не нужно подавать заявку на динамическое доменное имя, настраивать сопоставление портов или развертывать сервер.

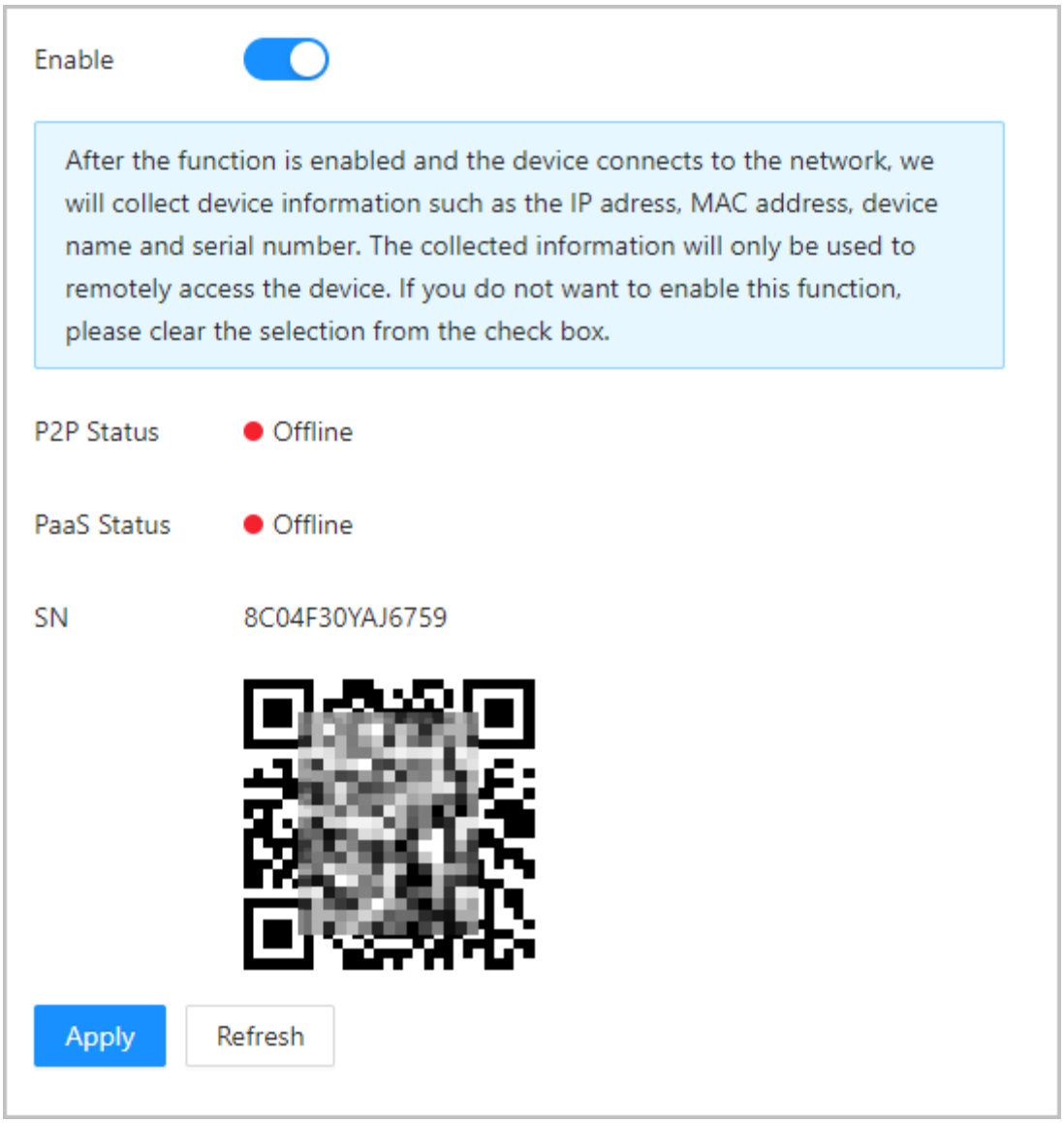
Процедура

Шаг 1 На главной странице выберите**Настройка сети**>**Облачный сервис**.

Шаг 2 Включите функцию облачного сервиса.

Облачный сервис переходит в режим онлайн, если P2P и PaaS находятся в режиме онлайн.

Рисунок 3-42 Облачный сервис



Шаг 3 Нажмите**Применять**.

Шаг 4 Отсканируйте QR-код с помощью DMSS, чтобы добавить устройство.

3.9.6 Настройка активной регистрации

Активная регистрация позволяет добавлять устройства на платформу управления без ручного ввода информации об устройстве, такой как IP-адрес и порт.

Процедура

Шаг 1 На главной странице выберите**Настройка сети**>**Автоматическая регистрация**.

Шаг 2 Включите функцию автоматической регистрации и настройте параметры.

Рисунок 3-43 Автоматическая регистрация

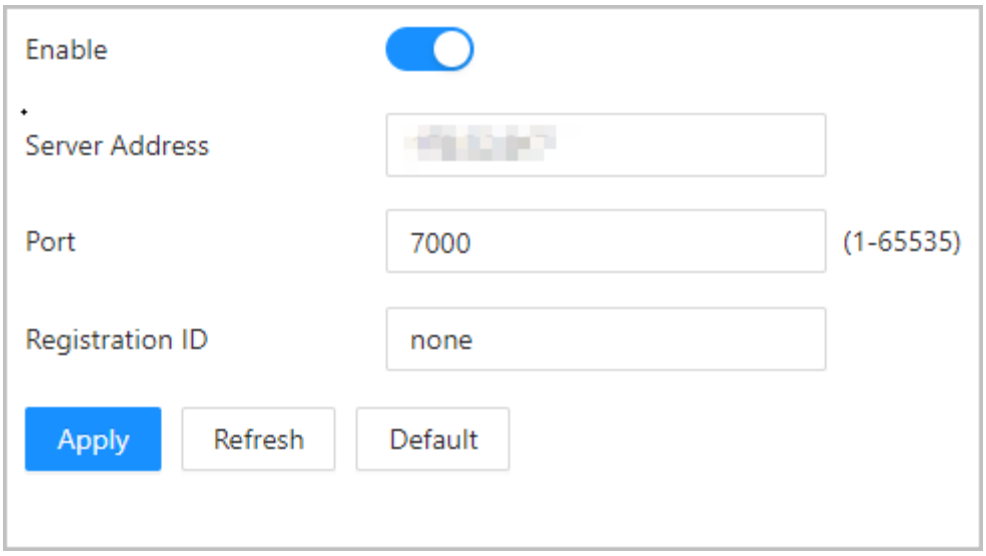


Таблица 3-30 Описание автоматической регистрации

Параметр	Описание
Адрес сервера	IP-адрес или доменное имя сервера.
Порт	Порт сервера, который используется для автоматической регистрации.
Регистрационный идентификатор	Регистрационный идентификатор (определяется пользователем) устройства. Добавление устройства в управление путем ввода регистрационного идентификатора на платформе.

Шаг 3 Нажмите**Применять**.

3.10 Настройка RS-485

Настройте параметры RS-485, если вы подключаете внешнее устройство к порту RS-485.

Процедура

Шаг 1 Выбирать**Настройки связи**>**Настройки RS-485**.

Шаг 2 Настройте параметры.

Рисунок 3-44 Настройка параметров

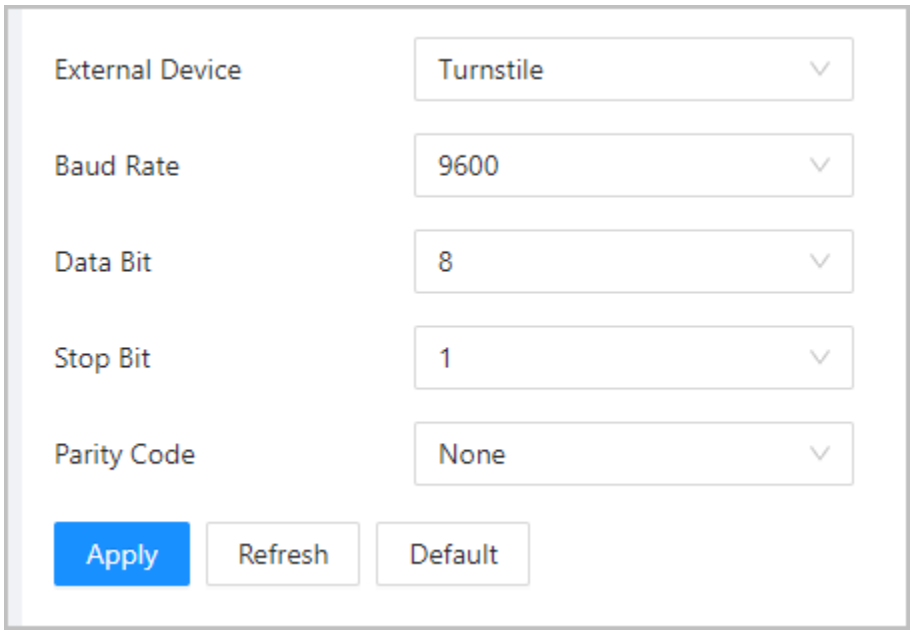


Таблица 3-31 Настройка формата Wiegand

Параметр	Описание
Внешнее устройство	● Контроллер доступа: Выбрать**Контроллер доступа**когда контроллер доступа функционирует как считыватель карт, и контроллер доступа будет отправлять данные контроллеру доступа для управления доступом. Тип выходных данных: ◇ Номер карты: выводит данные на основе номера карты, когда пользователи проводят картой, чтобы отпереть дверь; выводит данные на основе номера первой карты пользователя, когда они используют другие методы разблокировки. ◇ Нет.: Выводит данные на основе идентификатора пользователя. ● Устройство чтения карт: Контроллер доступа подключается к устройству чтения карт. ● Считыватель (OSDP): Контроллер доступа подключается к считывателю карт на основе протокола OSDP. ● Модуль безопасности управления дверью: кнопка выхода из двери, замок и пожарная связь не работают после включения модуля безопасности. ● Турникет: Когда контроллер доступа подключается к турникету, а плата контроллера доступа турникета подключается к внешнему модулю QR-кода или модулю считывания карт, плата передает данные проверки на турникет.
Бит данных	Число бит, используемых для передачи фактических данных в последовательной связи. Оно представляет собой двоичные цифры, несущие передаваемую информацию.

Параметр	Описание
Стоп-бит	Бит, отправляемый после данных и необязательных битов четности, чтобы указать конец передачи данных. Он позволяет приемнику подготовиться к следующему байту данных и обеспечивает синхронизация в протоколе связи.
Код четности	Дополнительный бит, отправляемый после битов данных для обнаружения ошибок передачи. Он помогает проверить целостность передаваемых данных, гарантируя определенное количество логических высоких или низких битов.

Шаг 3 Нажмите**Применять**.

3.11 Настройка Wiegand

Настройте параметры RS-485, если вы подключаете внешнее устройство к порту RS-485.

Процедура

Шаг 1 Выбирать**Настройки связи**>**Виганд**.

Шаг 2 Настройте параметры.

Рисунок 3-45 Настройка параметров

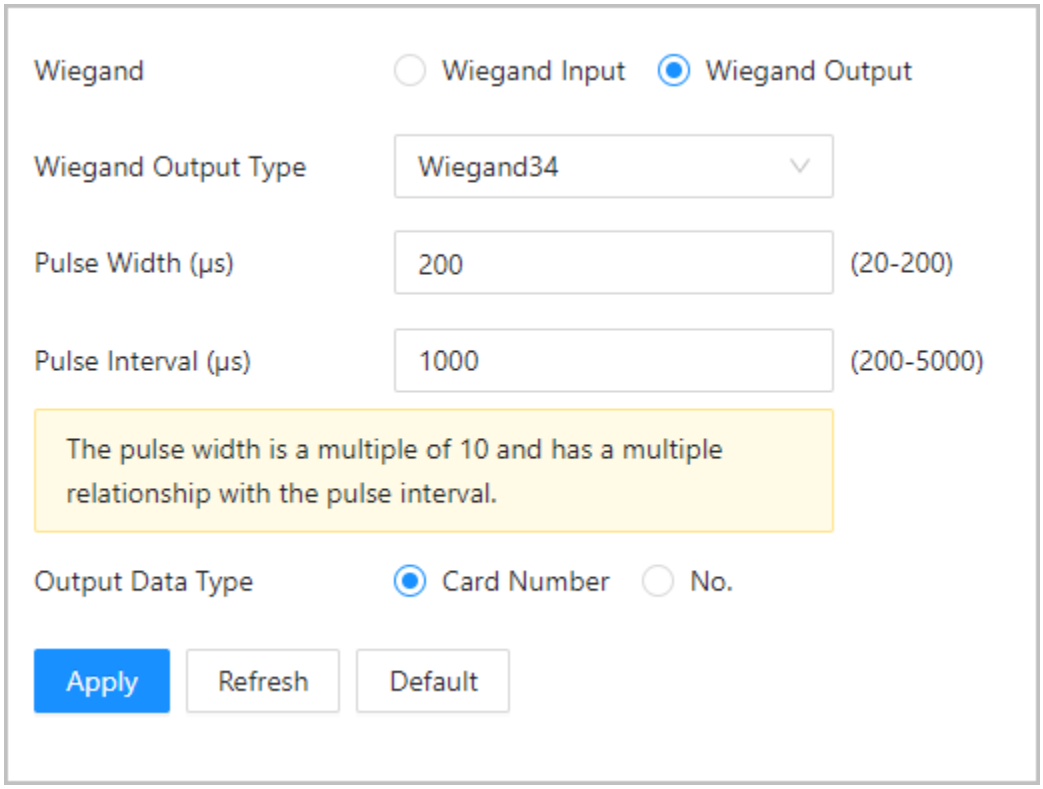


Таблица 3-32 Описание выхода Wiegand

Параметр	Описание
Тип выхода Wiegand	Выберите формат Wiegand для считывания номеров карт или идентификационных номеров. ● **Виганд26**: Считывает 3 байта или 6 цифр. ● **Виганд34**: Считывает 4 байта или 8 цифр. ● **Виганд66**: Считывает 8 байт или 16 цифр.

Параметр	Описание
Ширина импульса	Введите ширину импульса и интервал импульса выхода Wiegand.
Интервал импульса	
Тип выходных данных	Выберите тип выходных данных. ● **Нет.**: Выводит данные на основе идентификатора пользователя. Формат данных — шестнадцатеричный или десятичный. ● **Номер карты**: Выводит данные на основе номера первой карты пользователя.

Шаг 3 Нажмите**Применять**.

3.12 Настройка системы

3.12.1 Управление пользователями

Вы можете добавлять или удалять пользователей, изменять пароли пользователей и вводить адрес электронной почты для сброса пароля, если вы его забудете.

3.12.1.1 Добавление администраторов

Вы можете добавлять новые учетные записи администраторов, после чего они смогут входить на веб-страницу контроллера доступа.

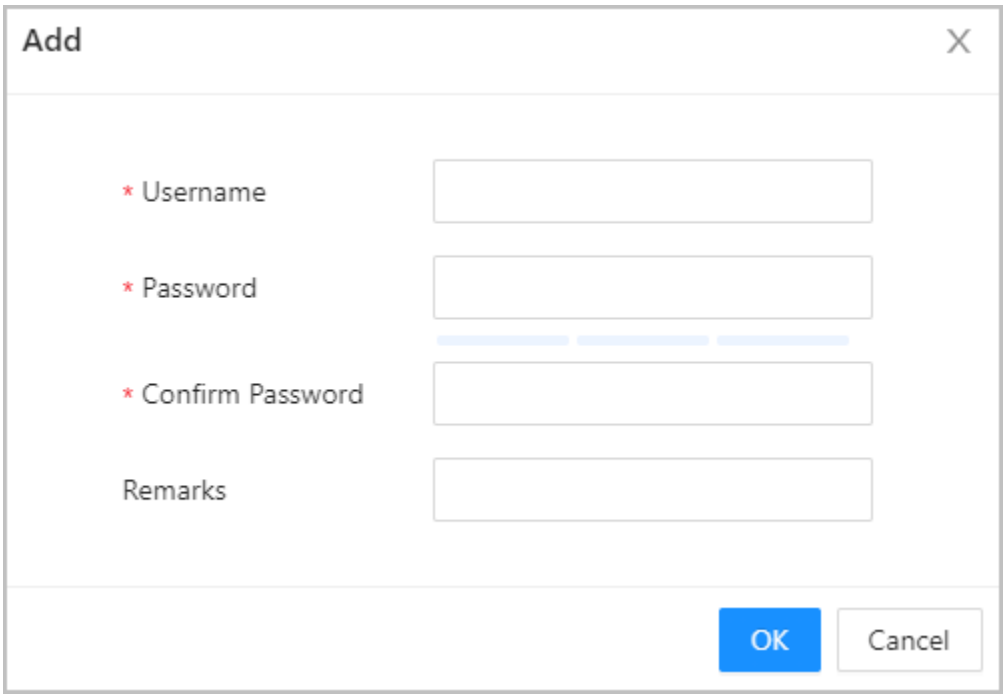
Процедура

Шаг 1 На главной странице выберите**Система**>**Счет**. Нажмите

Шаг 2 **Добавлять**и введите информацию о пользователе.

- Имя пользователя не может совпадать с существующим аккаунтом. Имя пользователя состоит из до 31 символа и допускает только цифры, буквы, подчеркивания, средние линии, точки или @.
- Пароль должен состоять из 8–32 непустых символов и содержать не менее двух типы следующих символов: заглавные буквы, строчные буквы, цифры и специальные символы символы (исключая ' " ; : &). Установите пароль высокой степени безопасности, следуя паролю подсказка по силе.

Рисунок 3-46 Добавить администраторов



Шаг 3 Нажмите**ХОРОШО**.

Изменить пароль может только учетная запись администратора, и учетная запись администратора не может быть удалена.

3.12.1.2 Добавление пользователей ONVIF

Справочная информация

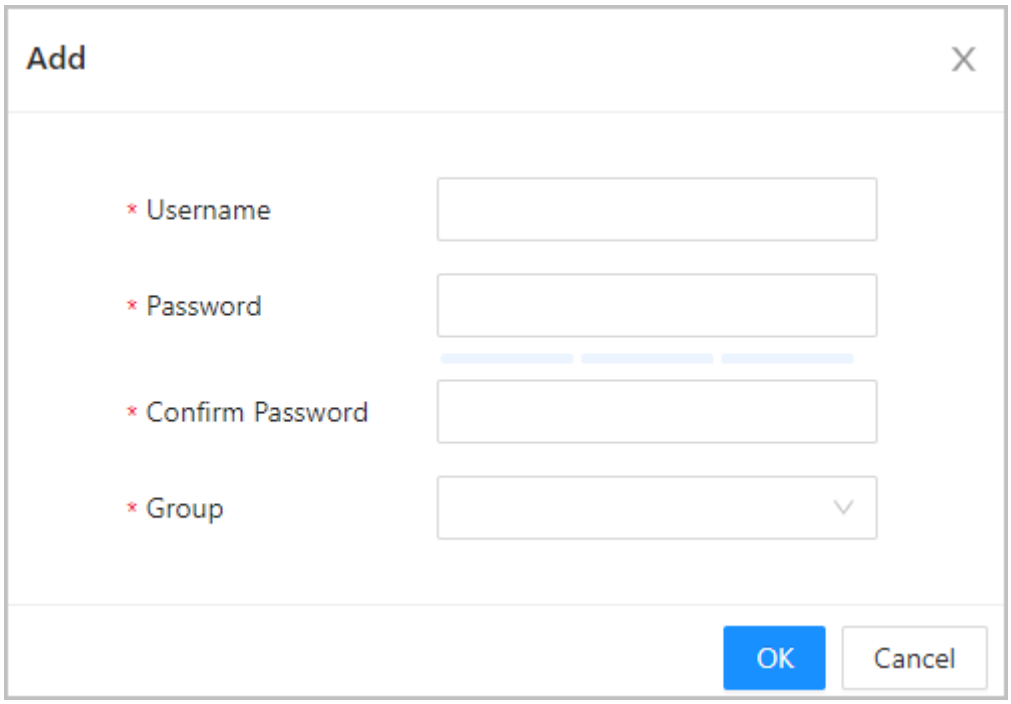
Open Network Video Interface Forum (ONVIF), глобальный и открытый отраслевой форум, созданный для разработки глобального открытого стандарта для интерфейса физических продуктов безопасности на основе IP, который обеспечивает совместимость с продуктами разных производителей. Пользователи ONVIF проверяют свою личность с помощью протокола ONVIF. Пользователь ONVIF по умолчанию — администратор.

Процедура

Шаг 1 На главной странице выберите**Система**>**Счет**>**Пользователь ONVIF**.

Шаг 2 Нажмите**Добавлять**, а затем настройте параметры.

Рисунок 3-47 Добавить пользователя ONVIF



Шаг 3 Нажмите**ХОРОШО**.

3.12.1.3 Сброс пароля

Если вы забыли пароль, сбросьте его, воспользовавшись ссылкой на электронное письмо.

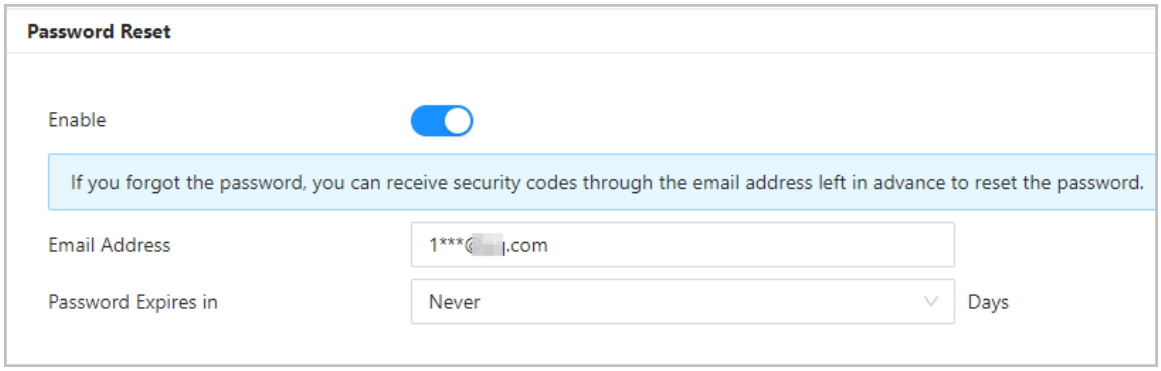
Процедура

Шаг 1 Выбирать**Система**>**Счет**.

Шаг 2 Введите адрес электронной почты и установите срок действия

Шаг 3 пароля. Включите функцию сброса пароля.

Рисунок 3-48 Сброс пароля



Если вы забыли пароль, вы можете получить коды безопасности по указанному адресу электронной почты.

адрес для сброса пароля.

Шаг 4 Нажмите**Применять**.

3.12.1.4 Просмотр пользователей онлайн

Вы можете просматривать онлайн-пользователей, которые в настоящее время заходят на веб-страницу. На домашней странице выберите**Система**>

Пользователь онлайн.

3.12.2 Настройка времени

Процедура

Шаг 1 На главной странице выберите**Система**>

Шаг 2 **Время**. Настройте время платформы.

Рисунок 3-49 Настройки даты

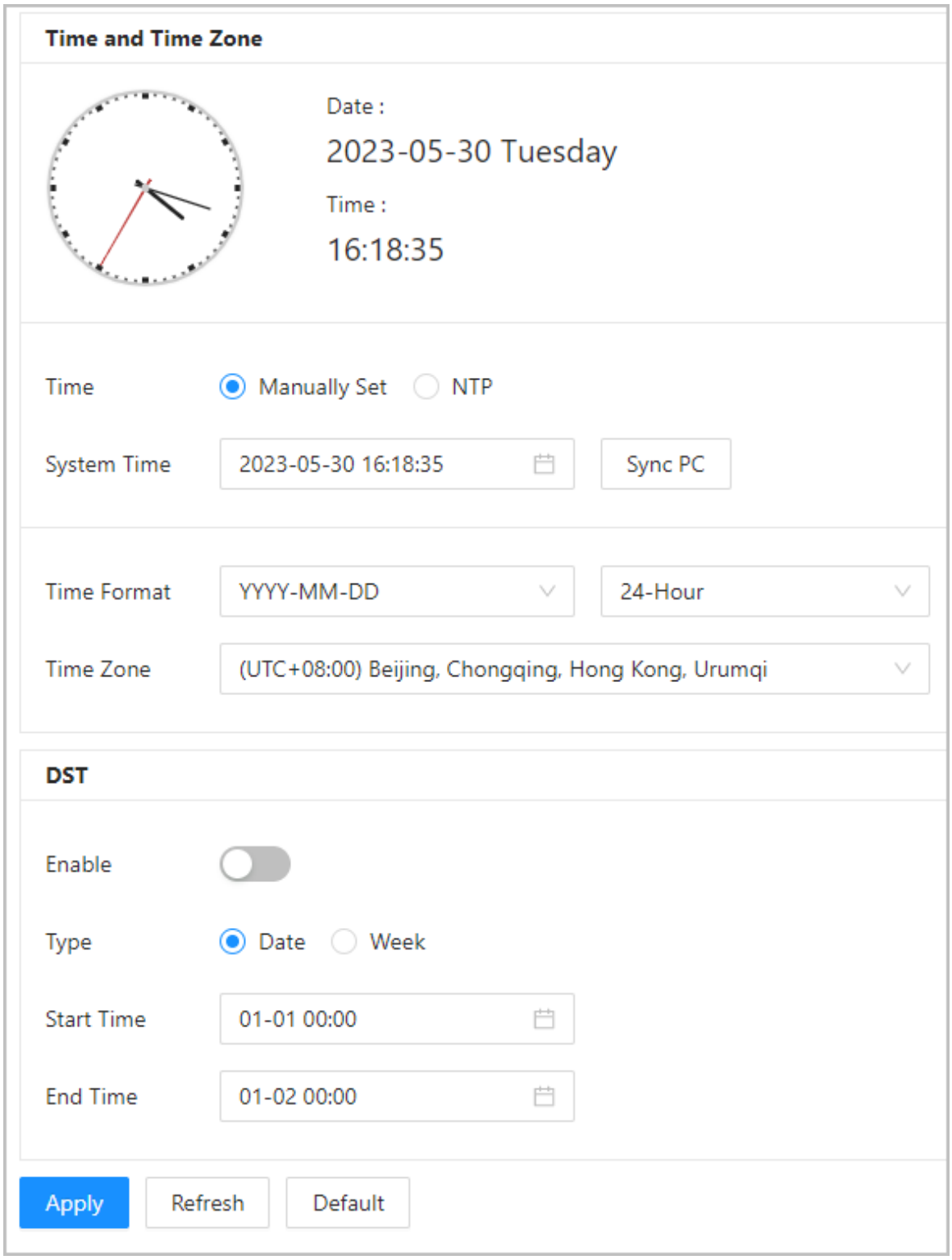


Таблица 3-34 Описание настроек времени

Параметр	Описание
Время	● Ручная установка: введите время вручную или нажмите**Синхронизировать время**для синхронизации времени с компьютером. ● NTP: Контроллер доступа автоматически синхронизирует время с сервером NTP. ◇ **Сервер**: Введите домен NTP-сервера. ◇ **Порт**: Введите порт NTP-сервера. ◇ **Интервал**: Введите время с интервалом синхронизации.
Формат времени	Выберите формат времени.
Часовой пояс	Введите часовой пояс.
летнее время	1. (Необязательно) Включите летнее время. 2. Выбрать**Дата**или**Неделя**из**Тип**. 3. Настройте время начала и окончания летнего времени.

Шаг 3 Нажмите**Применять**.

3.12.3 Техническое обслуживание

Регулярно перезапускайте контроллер доступа во время его простоя, чтобы повысить его производительность.

Процедура

Шаг 1 Войти на веб-страницу. Выбрать**Система**>

Шаг 2 **Обслуживание**. Установите время, а затем

Шаг 3 нажмите**Применять**.

Контроллер доступа перезапустится в запланированное время, или вы можете нажать**Перезапуск**чтобы перезапустить его немедленно.

3.12.4 Управление конфигурацией

Если нескольким контроллерам доступа требуются одинаковые конфигурации, вы можете настроить для них параметры, импортировав или экспортировав файлы конфигурации.

3.12.4.1 Экспорт и импорт файлов конфигурации

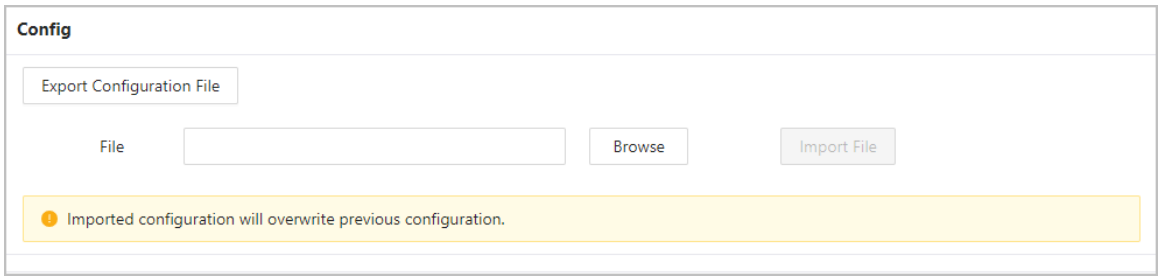
Вы можете импортировать и экспортировать файл конфигурации для контроллера доступа. Когда вы хотите применить те же конфигурации к нескольким устройствам, вы можете импортировать файл конфигурации на них.

Процедура

Шаг 1 Войти на веб-страницу. Выбрать

Шаг 2 **Система**>**Конфигурация**.

Рисунок 3-50 Управление конфигурацией



Шаг 3 Экспорт или импорт файлов конфигурации.

- Экспортируйте файл конфигурации.

  Нажмите**Экспортировать файл конфигурации**для загрузки файла на локальный компьютер.

  IP не будет экспортирован.

- Импортируйте файл конфигурации.

  1. Щелкните**Просматривать**для выбора файла конфигурации.

  2. Щелкните**Импорт конфигурации**.

  Файлы конфигурации можно импортировать только на устройства той же модели.

3.12.4.2 Восстановление заводских настроек по умолчанию

Процедура

Шаг 1 Выбирать**Система**>**Конфигурация**.

Восстановление**Контроллер доступа**к его настройкам по умолчанию приведет к потере данных. Пожалуйста будьте осторожны.

Шаг 2 При необходимости восстановите заводские настройки по умолчанию.

- **Заводские настройки по умолчанию**: Сбрасывает все конфигурации контроллера доступа и удаляет все данные.
- **Восстановить настройки по умолчанию (за исключением информации о пользователе и журналов)**: Сбрасывает настройки контроллера доступа и удаляет все данные, за исключением информации о пользователях и журналов.

Поддерживает только основной контроллер**Восстановить настройки по умолчанию (за исключением информации о пользователе и журналов)**.

3.12.5 Обновление системы

- Используйте правильный файл обновления. Убедитесь, что вы получили правильный файл обновления от технической поддержки.
- Не отключайте питание или сеть, не перезагружайте и не выключайте Access. Контроллер во время обновления.

3.12.5.1 Обновление файла

Процедура

Шаг 1 На главной странице выберите**Система**>**Обновлять**.

Шаг 2 В**Обновление файла**, нажмите**Просматривать**, а затем загрузите файл обновления.

Файл обновления должен иметь расширение .bin.

Шаг 3 Нажмите**Обновлять**.

Контроллер доступа перезагрузится после завершения обновления.

3.12.5.2 Онлайн-обновление

Процедура

Шаг 1 На главной странице выберите**Система**>**Обновлять**.

Шаг 2 В**Онлайн-обновление**выберите способ обновления.

- Выбирать**Автоматическая проверка обновлений**, и контроллер доступа автоматически проверит наличие последней версии обновления.
- Выбирать**Ручная проверка**, и вы можете сразу же проверить, доступна ли последняя версия.

Шаг 3 (Необязательно) Нажмите**Обновить сейчас**немедленно обновить контроллер доступа.

3.12.6 Просмотр информации о версии

На веб-странице выберите**Система**>**Версия**, и вы можете просмотреть информацию о версии контроллера доступа.

3.12.7 Просмотр емкости данных

На веб-странице выберите**Система**>**Емкость данных**, просмотрите емкость данных контроллера доступа.

3.12.8 Просмотр юридической информации

На главной странице выберите**Система**>**Юридическая информация**, а также вы можете ознакомиться с лицензионным соглашением по программному обеспечению, политикой конфиденциальности и уведомлением о программном обеспечении с открытым исходным кодом.

3.13 Персонализация

Настройте темы и добавьте видео- или графические ресурсы в контроллер доступа.

3.13.1 Добавление ресурсов

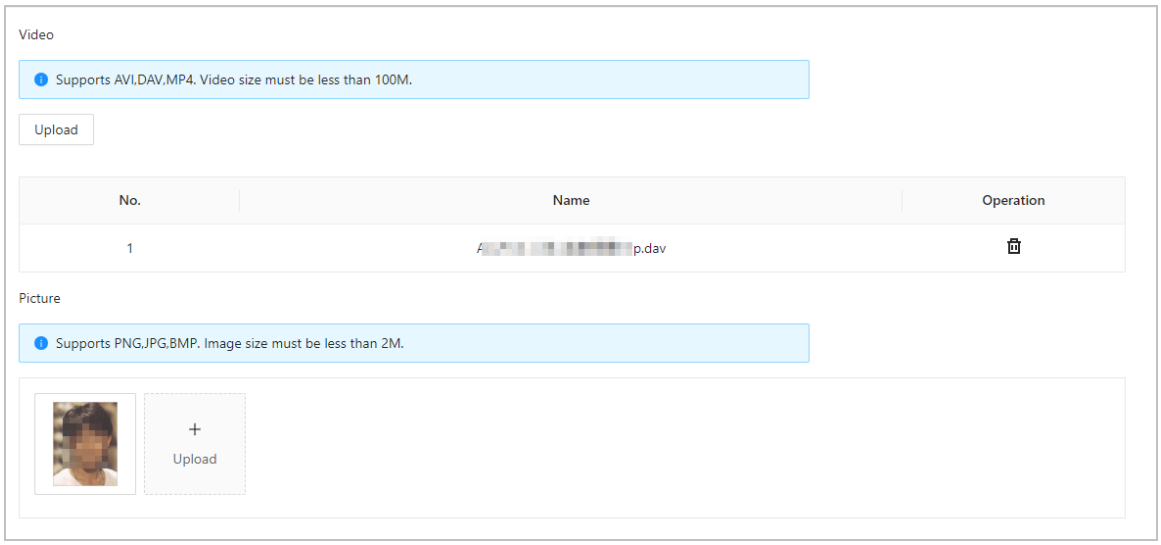
Добавьте изображения или видео, которые будут отображаться на экране ожидания контроллера доступа.

Процедура

Шаг 1 На главной странице выберите**Персонализация**>**Реклама**>**Рекламные ресурсы**. Добавьте видео

Шаг 2 или изображения.

Рисунок 3-51 Добавить видео или изображения



- Добавьте видео.

  1. Щелкните**Загрузить**.

  2. Щелкните**Просматривать**, выберите видеофайл, а затем нажмите**Следующий**.

     Видео автоматически загружается на платформу после перекодирования.

     - Вы можете загрузить до 5 видеофайлов.
     - Поддерживает DAV, AVI, MP4. Размер видео должен быть менее 100 МБ.
     - Для загрузки видеофайлов поддерживаются только последние версии FireFox и Chrome.

- Добавьте изображения.

  1. Нажмите.

2. Выберите изображение из локального хранилища и загрузите его.

Поддерживает PNG, JPG, BMP. Размер изображения должен быть менее 2 Мб.

Связанные операции

Нажмите для удаления загруженных изображений или видео.

Используемые видео и изображения не могут быть удалены.

3.13.2 Настройка тем

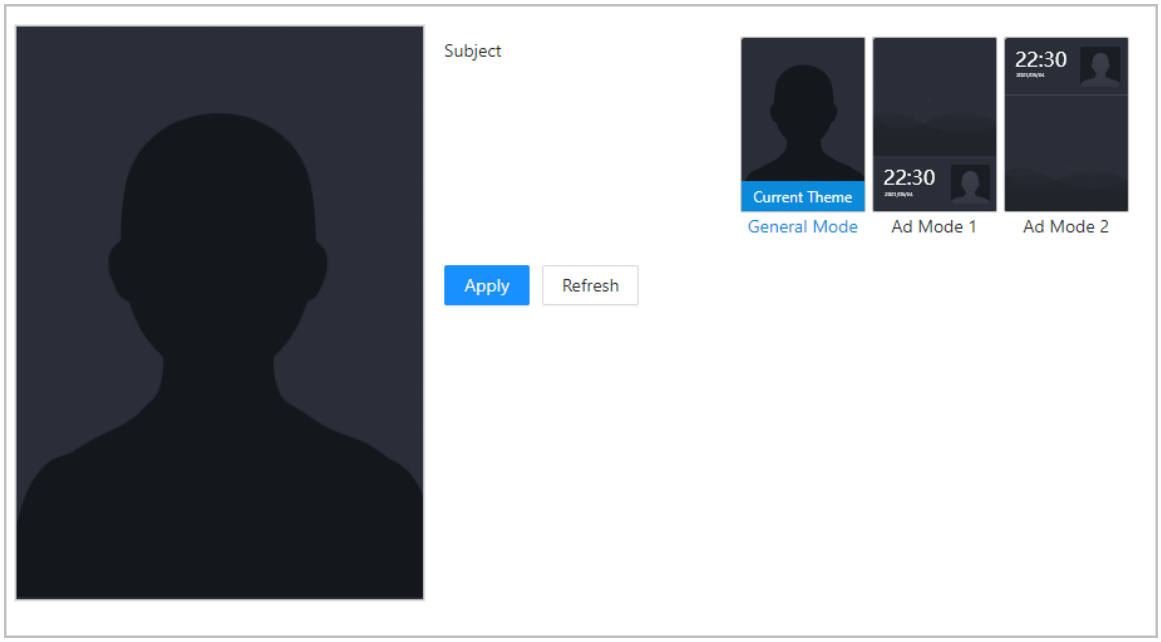
Процедура

Шаг 1 На главной странице выберите**Персонализация**>**Реклама**>**Предмет**.

Шаг 2 Выберите тему.

- Общая тема: отображает изображение лица на весь экран.
- Режим рекламы 1: в верхней области отображается реклама, а в нижней — время и поле распознавания лиц.
- Режим рекламы 2: в верхней области отображается время и поле распознавания лиц, а в нижней области отображается реклама.

Рисунок 3-52 Тема

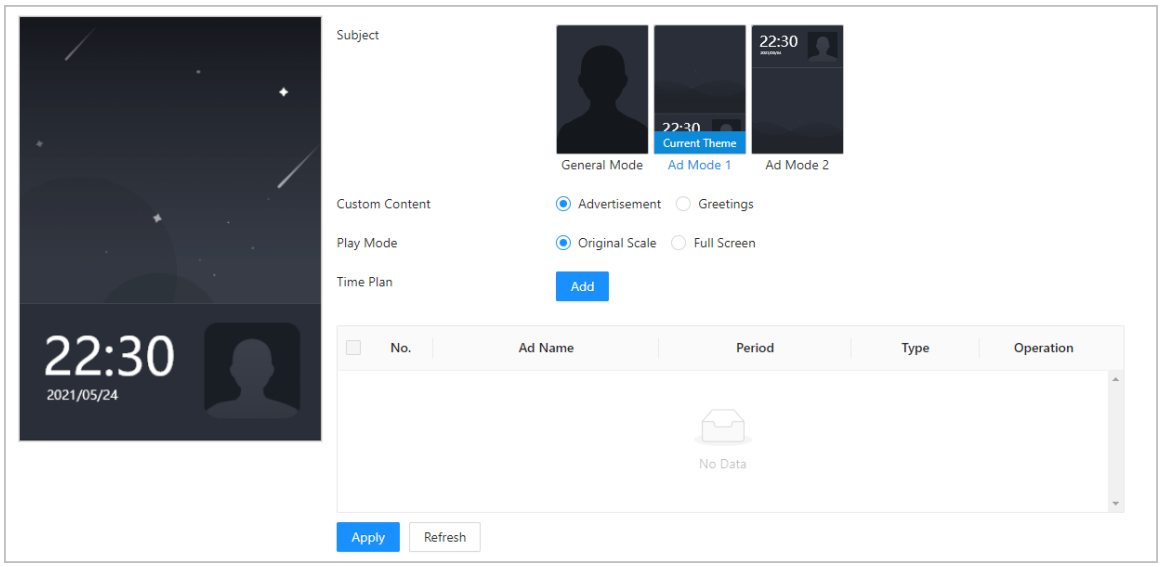


Шаг 3 Выберите голосовую подсказку для успешной проверки личности.

Шаг 4 Установите показ рекламы.

1. Выберите режим рекламы 1 или режим рекламы 2, а затем выберите**Реклама**.

Рисунок 3-53 Режим рекламы



2. Выберите режим отображения.

- Исходный масштаб: воспроизводит изображение и видео в исходном размере.
- Полный экран: воспроизводит изображение и видео на весь экран.

3. Щелкните**Добавлять**для добавления расписаний.

Вы можете добавить до 10 расписаний.

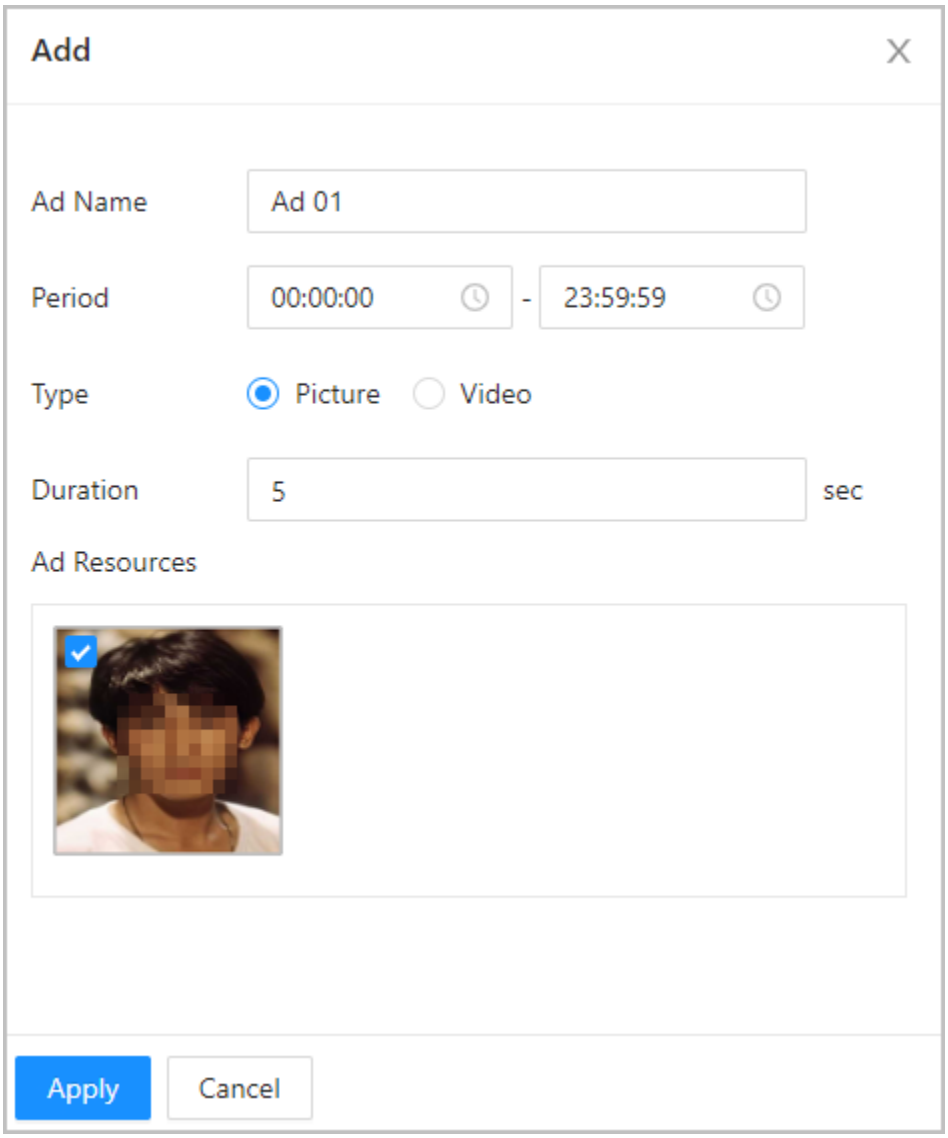
4. Введите название объявления.

5. Выберите временной отрезок, тип файла и файл.

6. Введите продолжительность, а затем нажмите**Применять**.

Установите длительность для одного изображения, когда изображения воспроизводятся в цикле. Длительность варьируется от 1 с до 20 с и по умолчанию составляет 5 с.

Рисунок 3-54 Добавить расписания



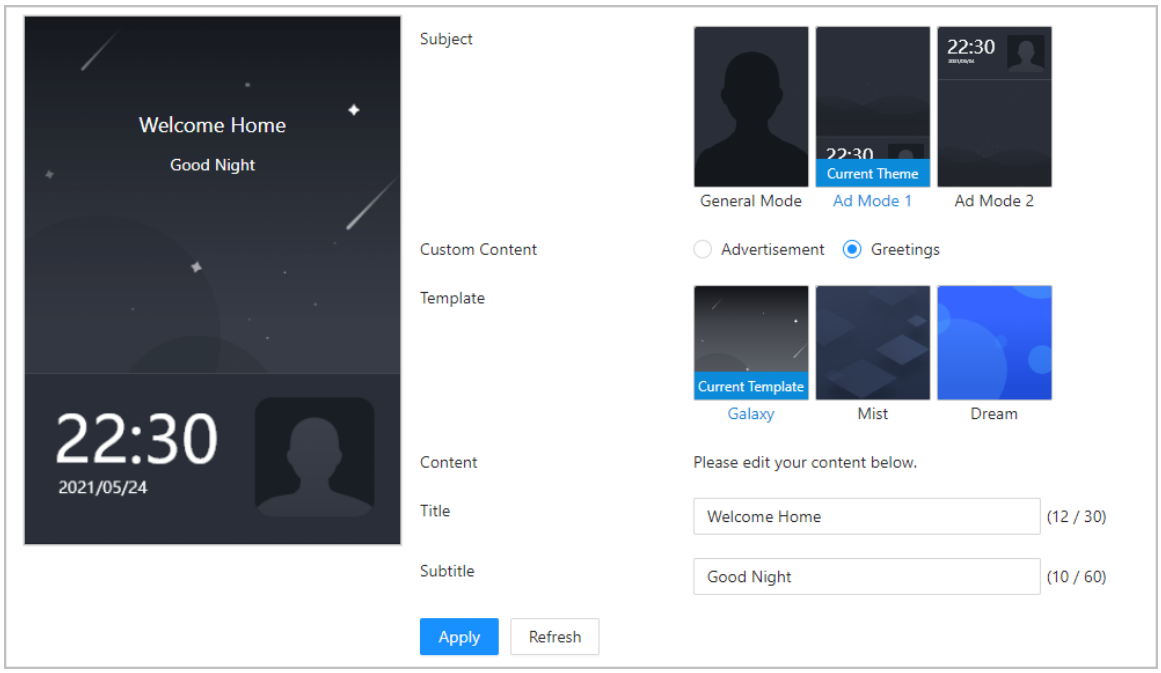
Шаг 5 Настройте приветствия.

1. Выбрать**Привет**из**Пользовательский контент**.

2. Выберите шаблон.

3. Введите заголовок и подзаголовок.

Рисунок 3-55 Приветствия



4. Щелкните**Применять**.

3.13.3 Настройка сочетаний клавиш

Процедура

Шаг 1 На веб-странице контроллера доступа выберите**Персонализация**>**Настройки сочетания клавиш**.

Шаг 2 Настройте параметры сочетания клавиш.

Рисунок 3-56 Настройки сочетания клавиш

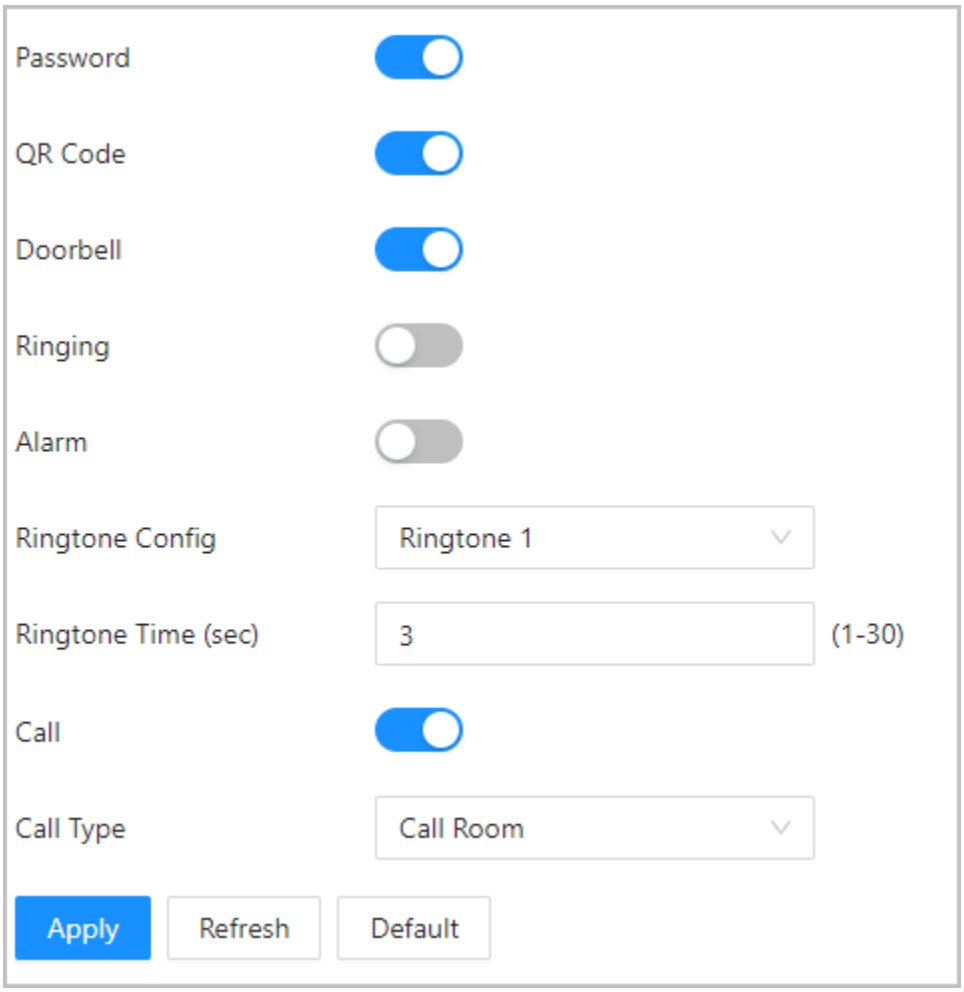


Таблица 3-35 1

Параметр	Описание
Пароль	Значок метода разблокировки пароля отображается на экране ожидания.
QR-код	Значок QR-кода отображается на экране ожидания. Эта функция недоступна для контроллера доступа с автономным модулем QR-кода.
Дверной звонок	После включения функции дверного звонка на экране режима ожидания отображается значок дверного звонка. ● Звонок: нажмите значок звонка на экране режима ожидания, и контроллер доступа зазвонит. ● Сигнализация: включите функцию связи с сигнализацией, после чего раздастся звонок в дверь. Эта функция доступна только в некоторых моделях. ● Настройка рингтона: выберите звонок. ● Ringtone Times (sec): Установите время звонка (1-30 с). Значение по умолчанию — 3.
Вызов	Значок вызова отображается на экране в режиме ожидания.

Параметр	Описание
Тип вызова	● Комната для звонков: нажмите значок вызова в режиме ожидания и введите номер комнаты для совершения звонков. ● Центр управления вызовами: нажмите значок вызова в режиме ожидания, а затем позвоните в центр управления. ● Пользовательский номер вызова: введите номер комнаты, а затем нажмите значок вызова на экране ожидания, чтобы позвонить на предварительно заданный номер комнаты.  Убедитесь, что контроллер доступа добавлен в DMSS.

3.14 Просмотр журналов

Просматривайте журналы, такие как системные журналы, журналы администратора и записи разблокировки.

3.14.1 Системные журналы

Просмотр и поиск системных журналов.

Процедура

Шаг 1 Войти на веб-страницу.

Шаг 2 Выбрать**Бревно**>**Бревно**.

Шаг 3 Выберите временной диапазон и тип журнала, а затем нажмите**Поиск**.

Связанные операции

- нажмите**Экспорт**для экспорта найденных журналов на локальный компьютер.
- Нажмите**Зашифровать резервную копию журнала**, а затем введите пароль. Экспортированный файл можно открыть только после ввода пароля.
- Нажмите, чтобы просмотреть сведения о журнале.

3.14.2 Журналы администратора

Найдите журналы администратора, используя идентификатор администратора.

Процедура

Шаг 1 Войти на веб-страницу. Выбрать

Шаг 2 **Бревно**>**Журнал администратора**.

Шаг 3 Введите идентификатор администратора и нажмите**Поиск**.

Нажмите**Экспорт**для экспорта журналов администратора.

3.14.3 Разблокировка журналов

Найдите записи разблокировки и экспортируйте их.

Процедура

Шаг 1 Войти на веб-страницу. Выбрать**Бревно**

Шаг 2 >**Разблокировать записи**.

Шаг 3 Выберите временной диапазон и тип, а затем нажмите**Поиск**. Вы можете нажать**Экспорт**чтобы загрузить журнал.

3.14.4 Журналы тревог

Просмотр журналов тревог.

Процедура

Шаг 1 Войти на веб-страницу. Выбрать**Бревно**>**Журнал тревог**

Шаг 2 . Выберите тип и временной диапазон. Введите

Шаг 3 идентификатор администратора, а затем нажмите**Поиск**.

Шаг 4

3.14.5 Журналы вызовов

Просмотр журналов вызовов.

Процедура

Шаг 1 Войти на веб-страницу. Выбрать

Шаг 2 **Бревно**>**История звонков**.

3.14.6 Управление USB-устройствами

Экспорт информации о пользователе с/на USB.

Процедура

Шаг 1 Войти на веб-страницу. Выбрать

Шаг 2 **Бревно**>**USB-управление**.

- Перед экспортом данных или обновить систему. Чтобы избежать сбоя, не вытаскивайте USB и не выполняйте никаких операций Контроллера доступа во время процесса.
- Вам необходимо использовать USB для экспорта информации с контроллера доступа на другой устройства. Изображения лиц не могут быть импортированы через USB.

Шаг 3 Выберите тип данных, а затем нажмите**USB-импорт**или**USB-экспорт**импортировать или экспортировать данные.

3.15 Емкость данных

Вы можете увидеть, сколько пользователей, карт и изображений лиц может хранить контроллер доступа.

Войдите на веб-страницу и выберите**Емкость данных**.

3.16 Настройки безопасности (необязательно)

3.16.1 Статус безопасности

Сканируйте пользователей, службы и модули безопасности, чтобы проверить состояние безопасности контроллера доступа.

Справочная информация

- Обнаружение пользователей и служб: проверьте, соответствует ли текущая конфигурация рекомендациям.
- Сканирование модулей безопасности: сканирование текущего состояния модулей безопасности, таких как передача аудио и видео, надежная защита, предупреждение о безопасности и защита от атак, а не определение того, включены ли они.

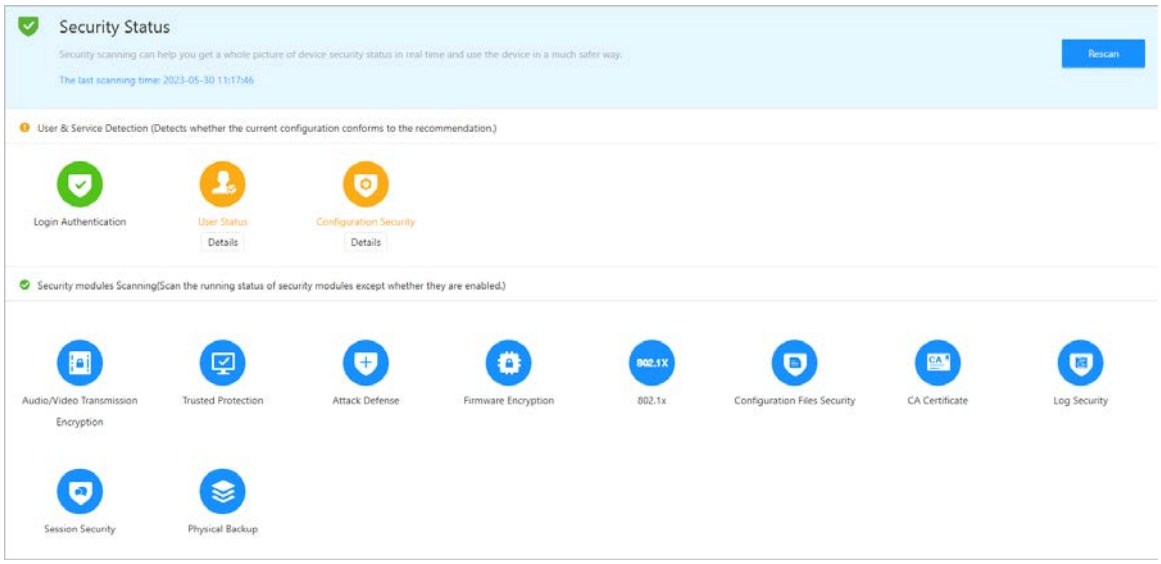
Процедура

Шаг 1 Выбирать**Безопасность**>**Статус безопасности**.

Шаг 2 Нажмите**Повторное сканирование**для выполнения сканирования безопасности контроллера доступа.

Наведите курсор на значки модулей безопасности, чтобы увидеть их состояние работы.

Рисунок 3-57 Состояние безопасности



Связанные операции

После выполнения сканирования результаты будут отображаться разными цветами. Желтый цвет означает, что модули безопасности неисправны, а зеленый цвет означает, что модули безопасности в норме.

- Нажмите**Подробности**для просмотра подробностей о результатах сканирования.
- Нажмите**Игнорировать**игнорировать аномалию, и она не будет сканироваться. Аномалия, которая была

проигнорированные будут выделены серым цветом.

- Нажмите**Оптимизировать**для устранения неисправности.

3.16.2 Настройка HTTPS

Создайте сертификат или загрузите аутентифицированный сертификат, и тогда вы сможете войти на веб-страницу через HTTPS на вашем компьютере. HTTPS защищает связь через компьютерную сеть.

Процедура

Шаг 1 Выбирать**Безопасность**>**Системная служба**>

Шаг 2 **HTTPS**. Включите службу HTTPS.

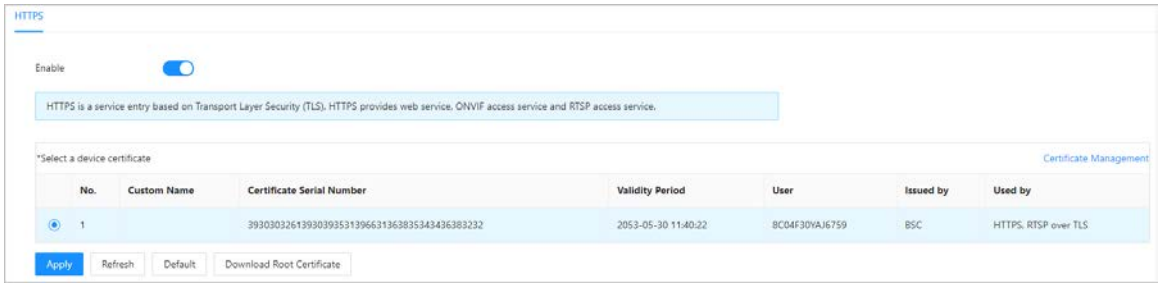
Если вы включите совместимость с TLS v1.1 и более ранними версиями, могут возникнуть угрозы безопасности.

Пожалуйста, примите во внимание.

Шаг 3 Выберите сертификат.

Если в списке нет сертификатов, нажмите**Управление сертификатами**для загрузки сертификата.

Рисунок 3-58 HTTPS



Шаг 4 Нажмите**Применять**.

Введите «https://»*IP-адрес*:*httpsспорт*" в веб-браузере. Если сертификат установлен, вы сможете успешно войти на веб-страницу. Если нет, веб-страница отобразит сертификат как неправильный или ненадежный.

3.16.3 Атака и защита

3.16.3.1 Настройка брандмауэра

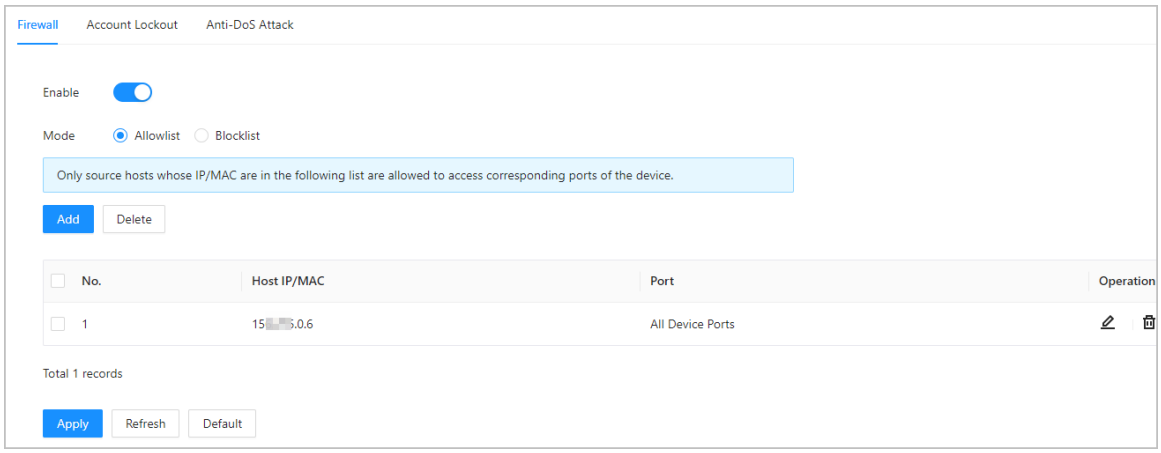
Настройте брандмауэр для ограничения доступа к контроллеру доступа.

Процедура

Шаг 1 Выбирать**Безопасность**>**Атака Защита**>**Брандмауэр**.

Шаг 2 Нажмите, чтобы включить функцию брандмауэра.

Рисунок 3-59 Брандмауэр

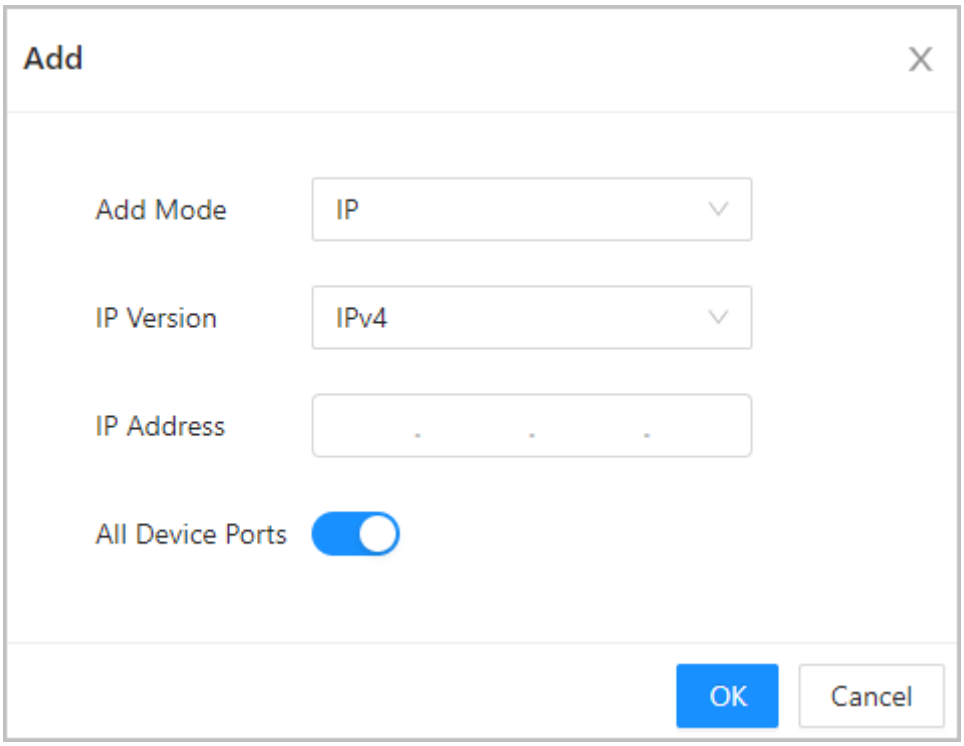


Шаг 3 Выберите режим:**Белый список**и**Черный список**.

- **Белый список**: Доступ к контроллеру доступа могут получить только IP/MAC-адреса из разрешенного списка.
- **Черный список**: IP/MAC-адреса из черного списка не могут получить доступ к контроллеру доступа.

Шаг 4 Нажмите**Добавлять**для ввода информации об IP.

Рисунок 3-60 Добавить информацию об IP



Шаг 5 Нажмите**ХОРОШО**.

Связанные операции

- Нажмите для редактирования информации об
- Нажмите IP-адресе. для удаления IP-адреса.

3.16.3.2 Настройка блокировки учетной записи

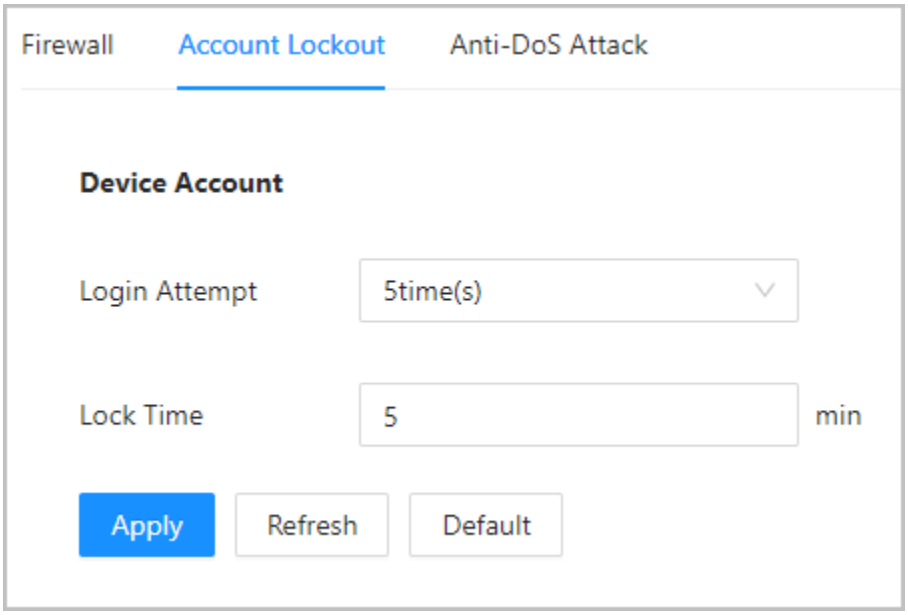
Если неверный пароль будет введен определенное количество раз, учетная запись будет заблокирована.

Процедура

Шаг 1 Выбирать**Безопасность**>**Атака Защита**>**Блокировка аккаунта**.

Шаг 2 Введите количество попыток входа в систему и время, на которое будет заблокирована учетная запись администратора и пользователя ONVIF.

Рисунок 3-61 Блокировка учетной записи



- Попытка входа: Лимит попыток входа. Если неверный пароль будет введен определенное количество раз, учетная запись будет заблокирована.
- Время блокировки: Интервал, в течение которого вы не можете войти в систему после блокировки учетной записи.

Шаг 3 Нажмите**Применять**.

3.16.3.3 Настройка защиты от DoS-атак

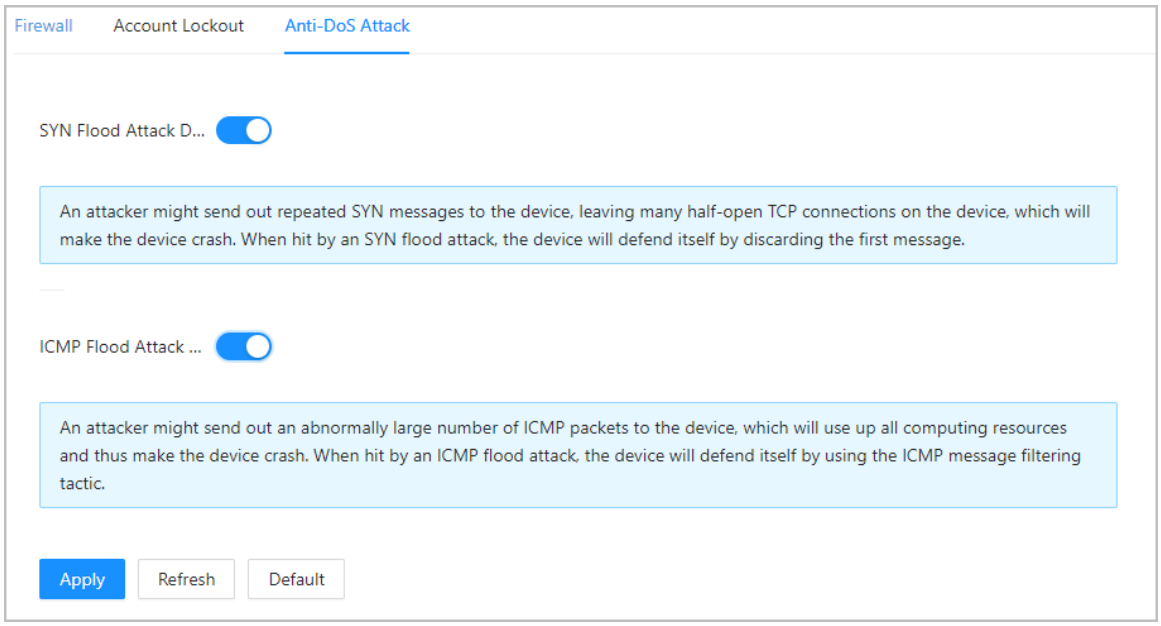
Вы можете включить**Защита от атак SYN-потока**и**Защита от атак ICMP Flood**для защиты контроллера доступа от DoS-атак.

Процедура

Шаг 1 Выбирать**Безопасность**>**Атака Защита**>**Анти-DoS-атака**.

Шаг 2 Включать**Защита от атак SYN-потока**или**Защита от атак ICMP Flood**для защиты контроллера доступа от DoS-атак.

Рисунок 3-62 Анти-DoS-атака



Шаг 3 Нажмите**Применять**.

3.16.4 Установка сертификата устройства

Создайте сертификат или загрузите аутентифицированный сертификат, после чего вы сможете войти в систему через HTTPS на своем компьютере.

3.16.4.1 Создание сертификата

Создайте сертификат для контроллера доступа.

Процедура

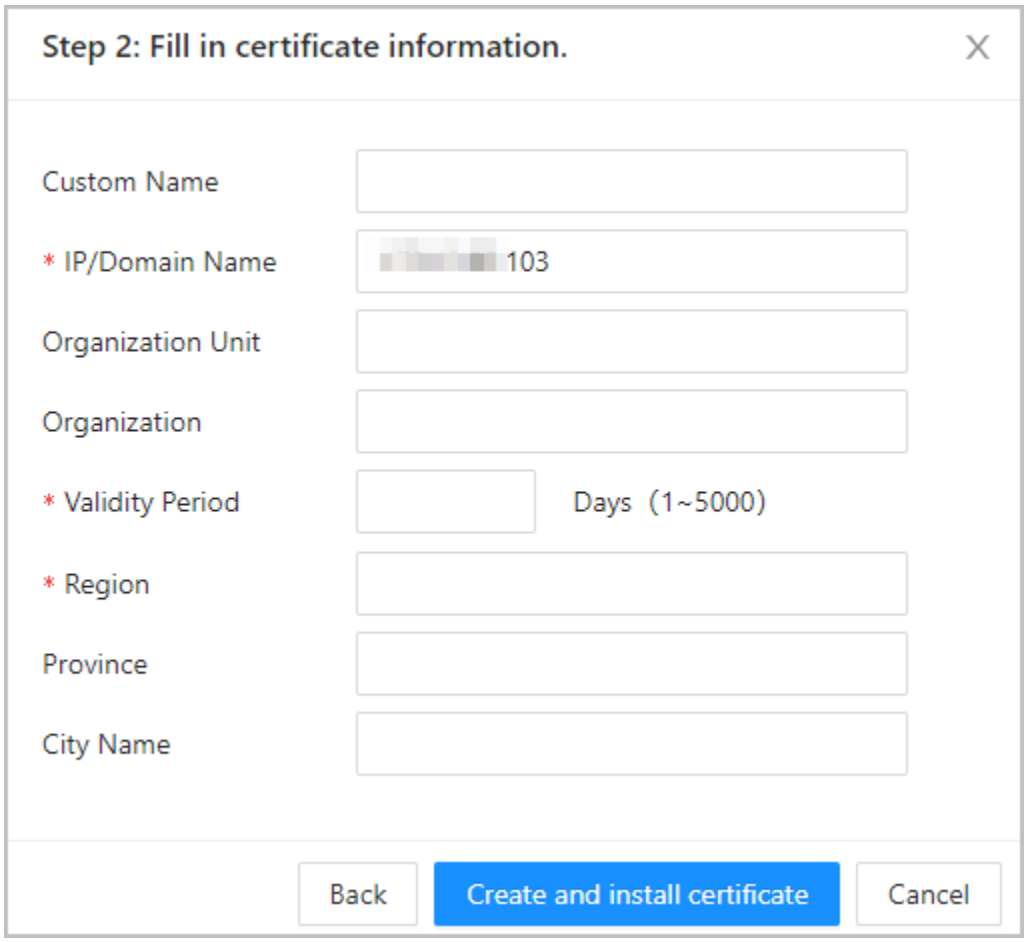
Шаг 1 Выбирать**Безопасность**>**Сертификат CA**>**Сертификат устройства**.

Шаг 2 Выбирать**Установить сертификат устройства**. Выбирать**Создать**

Шаг 3 **сертификат**и нажмите**Следующий**. Введите информацию о

Шаг 4 сертификате.

Рисунок 3-63 Информация о сертификате



Название региона не может превышать 2 символа. Рекомендуем ввести аббревиатуру от названия региона.

Шаг 5 Нажмите**Создать и установить сертификат**.

Недавно установленный сертификат отображается на**Сертификат устройства**страница после успешной установки сертификата.

Связанные операции

- Нажмите**Войти в режим редактирования**на**Сертификат устройства**страница для редактирования имени сертификата.
- Нажмите загрузить сертификат.
- Нажмите удалить сертификат.

3.16.4.2 Подача заявки на получение и импорт сертификата CA

Импортируйте сертификат стороннего центра сертификации в контроллер доступа.

Процедура

Шаг 1 Выбирать**Безопасность**>**Сертификат CA**>**Сертификат устройства**. Нажмите

Шаг 2 **Установить сертификат устройства**.

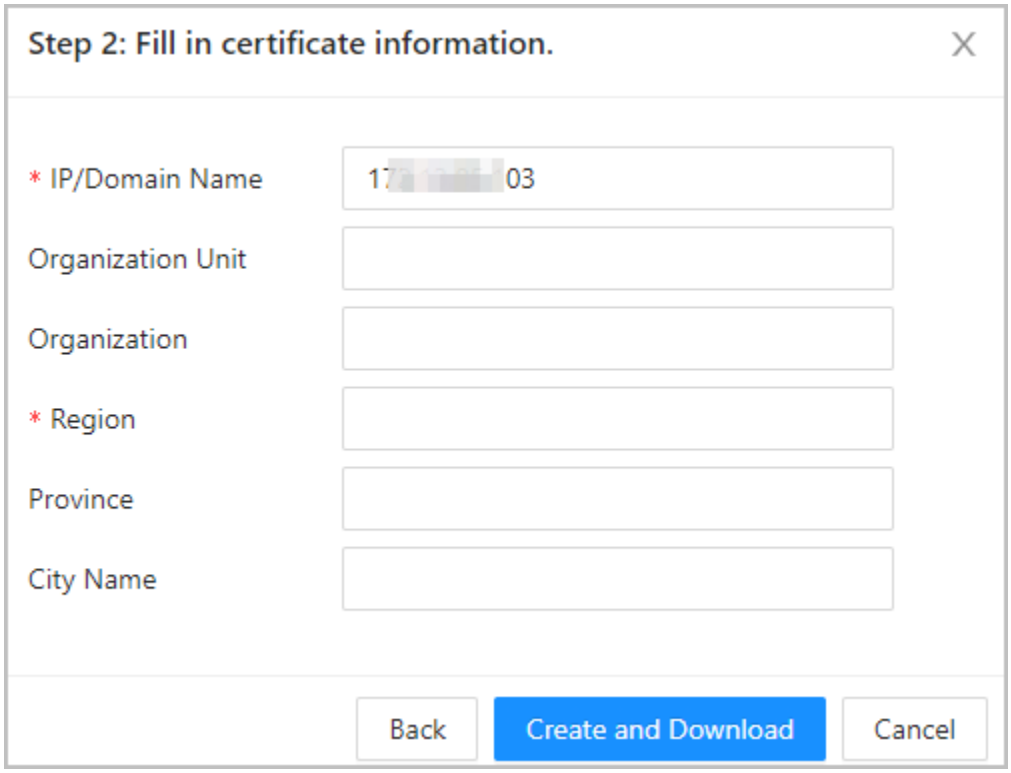
Шаг 3 Выбирать**Подать заявку на получение сертификата CA и импорт (рекомендуется)**и нажмите**Следующий**.

Шаг 4 Введите информацию о сертификате.

- IP/доменное имя: IP-адрес или доменное имя контроллера доступа.
- Регион: Название региона не должно превышать 3 символов. Рекомендуем ввести

аббревиатура названия региона.

Рисунок 3-64 Информация о сертификате (2)



Шаг 5 Нажмите**Создать и скачать**.

Сохраните файл запроса на своем компьютере.

Шаг 6 Подайте заявку на сертификат в сторонний центр сертификации, используя файл запроса. Импортируйте

Шаг 7 подписанный сертификат центра сертификации.

1) Сохраните сертификат CA на своем компьютере.

2) Щелкните**Установка сертификата устройства**.

3) Щелкните**Просматривать**для выбора сертификата CA.

4) Щелкните**Импорт и установка**.

Недавно установленный сертификат отображается на**Сертификат устройства**страница после успешной установки сертификата.

- Нажмите**Воссоздать**чтобы заново создать файл запроса.
- Нажмите**Импортировать позже**для импорта сертификата в другое время.

Связанные операции

- Нажмите**Войти в режим редактирования**на**Сертификат устройства**страница для редактирования имени сертификата.
- Нажмите загрузить сертификат.
- Нажмите удалить сертификат.

3.16.4.3 Установка существующего сертификата

Если у вас уже есть файл сертификата и закрытого ключа, импортируйте файл сертификата и закрытого ключа.

Процедура

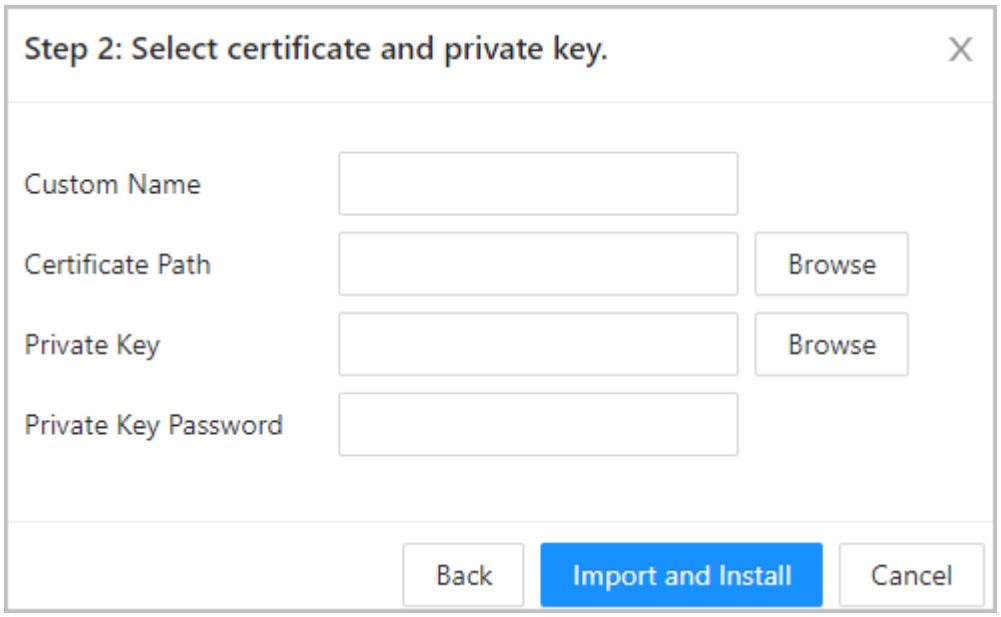
Шаг 1 Выбирать**Безопасность**>**Сертификат CA**>**Сертификат устройства**. Нажмите

Шаг 2 **Установить сертификат устройства**.

Шаг 3 Выбирать**Установить существующий сертификат**и нажмите**Следующий**.

Шаг 4 Нажмите**Просматривать**чтобы выбрать файл сертификата и закрытого ключа, а также ввести пароль закрытого ключа.

Рисунок 3-65 Сертификат и закрытый ключ



Шаг 5 Нажмите**Импорт и установка**.

Недавно установленный сертификат отображается на**Сертификат устройства**страница после успешной установки сертификата.

Связанные операции

- Нажмите**Войти в режим редактирования**на**Сертификат устройства**страница для редактирования имени сертификата.
- Нажмите загрузить сертификат.
- Нажмите удалить сертификат.

3.16.5 Установка доверенного сертификата CA

Доверенный сертификат CA — это цифровой сертификат, который используется для проверки подлинности веб-сайтов и серверов. Например, при использовании протокола 802.1x сертификат CA для коммутаторов требуется для аутентификации его подлинности.

Справочная информация

802.1X — это протокол сетевой аутентификации, который открывает порты для доступа к сети, когда организация проверяет подлинность личности пользователя и разрешает ему доступ к сети.

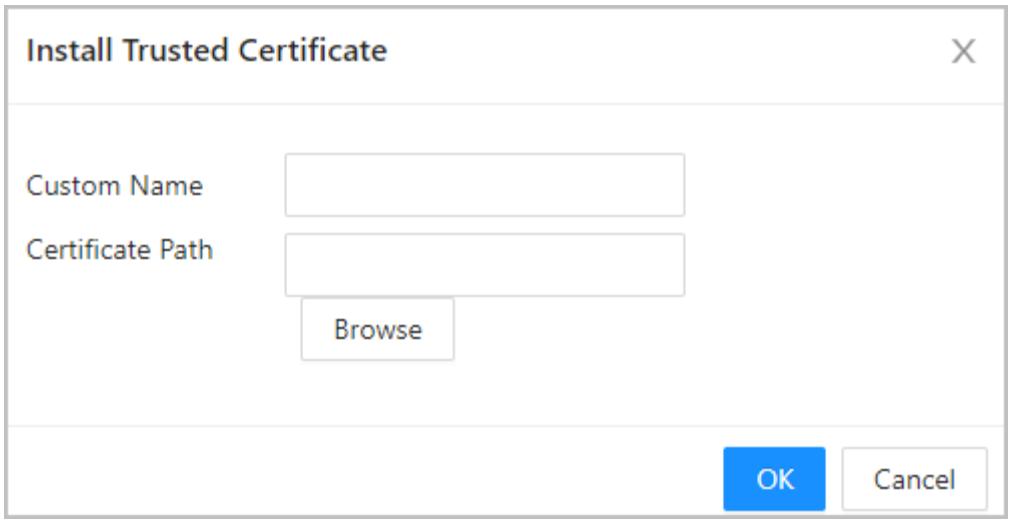
Процедура

Шаг 1 Выбирать**Безопасность**>**Сертификат CA**>**Доверенные сертификаты CA**.

Шаг 2 Выбирать**Установить доверенный сертификат**.

Шаг 3 Нажмите**Просматривать**для выбора доверенного сертификата.

Рисунок 3-66 Установка доверенного сертификата



Шаг 4 НажмитеХОРОШО.

Недавно установленный сертификат отображается на**Доверенные сертификаты CA**страница после успешной установки сертификата.

Связанные операции

- Нажмите**Войти в режим редактирования**на**Сертификат устройства**страница для редактирования имени сертификата.
- Нажмите загрузить сертификат.
- Нажмите удалить сертификат.

3.16.6 Шифрование данных

Процедура

Шаг 1 Выбирать**Безопасность**>**Шифрование**

Шаг 2 **данных**. Настройте параметры.

Рисунок 3-67 Шифрование данных

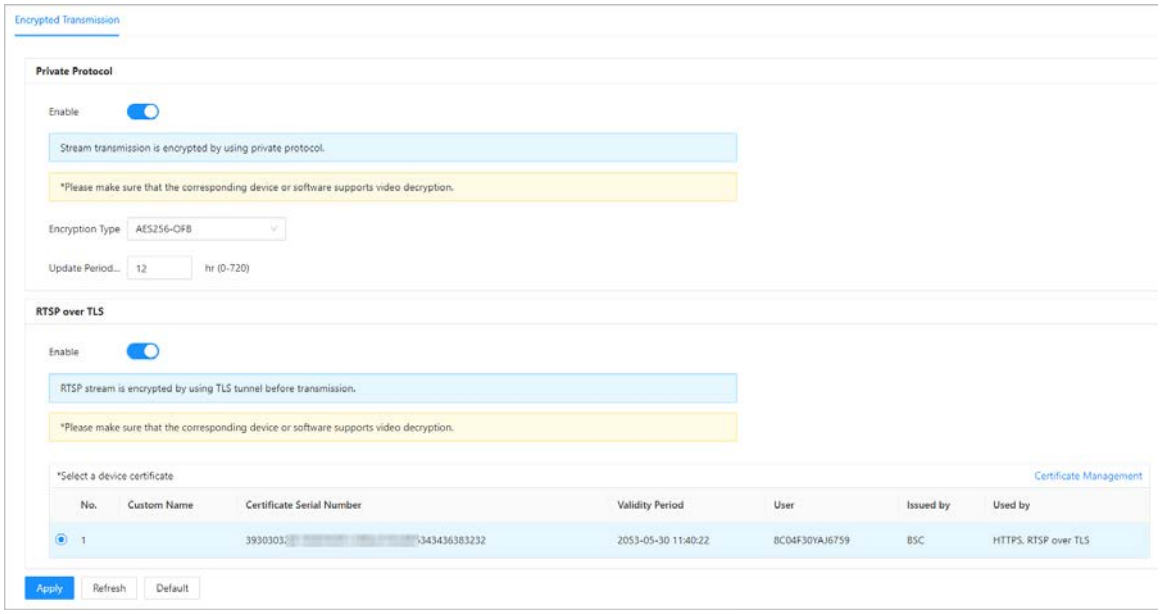


Таблица 3-36 Описание шифрования данных

	Параметр	Описание
Частный протокол	Давать возможность	Потоки шифруются во время передачи по закрытому протоколу.
	Тип шифрования	Оставьте его по умолчанию.
	Период обновления Секретный ключ	Диапазон значений: 0 ч - 720 ч. 0 означает, что секретный ключ никогда не обновляется.
RTSP через TLS	Давать возможность	Поток RTSP шифруется при передаче через туннель TLS.
	Сертификат Управление	Создать или импортировать сертификат. Подробности см. в разделе "3.16.4 Установка сертификата устройства". Установленные сертификаты отображаются в списке.

3.16.7 Предупреждение о безопасности

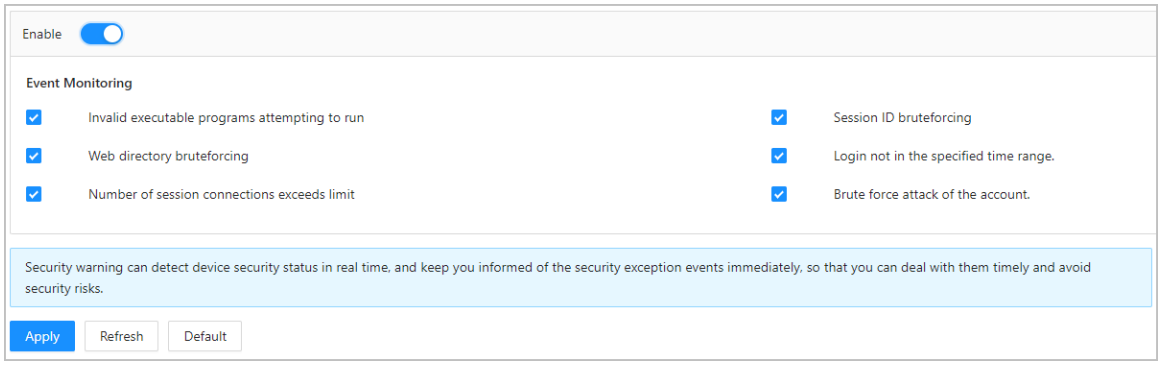
Процедура

Шаг 1 Выбирать**Безопасность**>**Предупреждение о**

Шаг 2 **безопасности**. Включить функцию предупреждения

Шаг 3 безопасности. Выберите элементы мониторинга.

Рисунок 3-68 Предупреждение безопасности



Шаг 4 Нажмите**Применять**.

4. Упрощенная конфигурация Smart PSS

В этом разделе описывается, как управлять и настраивать контроллер доступа через Smart PSS Lite. Подробности см. в руководстве пользователя Smart PSS Lite.

4.1 Установка и вход в систему

Установите и войдите в Smart PSS Lite. Подробности см. в руководстве пользователя Smart PSS Lite.

Процедура

Шаг 1 Получите пакет программного обеспечения Smart PSS Lite в службе технической поддержки, а затем установите и запустите программное обеспечение согласно инструкциям.

Шаг 2 При первом входе в систему выполните инициализацию Smart PSS Lite, включая установку пароля и контрольных вопросов.

Установите пароль для первого использования, а затем задайте контрольные вопросы, чтобы сбросить пароль. пароль, если вы его забыли.

Шаг 3 Введите имя пользователя и пароль для входа в Smart PSS Lite.

4.2 Добавление устройств

Вам необходимо добавить контроллер доступа в Smart PSS Lite. Вы можете добавлять их партиями или по отдельности.

4.2.1 Добавление по одному

Вы можете добавлять контроллеры доступа по одному, вводя их IP-адреса или доменные имена.

Процедура

Шаг 1 Войдите в Smart PSS Lite.

Шаг 2 Нажмите **Диспетчер устройств** и нажмите **Добавлять**.

Шаг 3 Введите информацию об устройстве.

Рисунок 4-1 Информация об устройстве

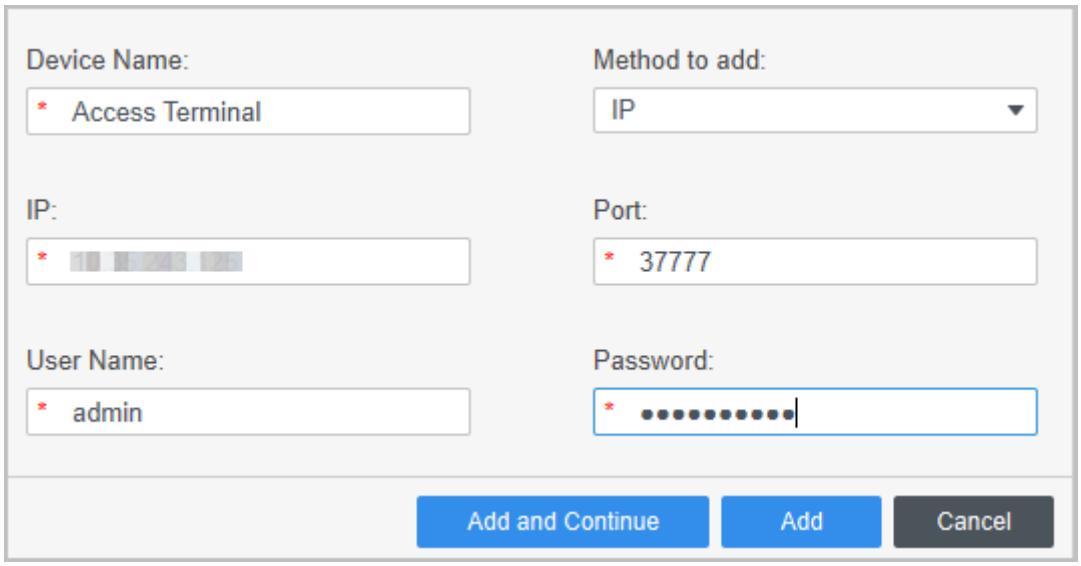


Таблица 4-1 Описание параметров устройства

Параметр	Описание
Имя устройства	Введите имя контроллера доступа. Мы рекомендуем назвать его по месту установки.
Метод добавления	Выбирать**ИС**чтобы добавить терминал доступа, введя его IP-адрес.
ИС	Введите IP-адрес контроллера доступа.
Порт	Номер порта по умолчанию — 37777.
Имя пользователя/Пароль	Введите имя пользователя и пароль терминала доступа.

Шаг 4 Нажмите**Добавлять**.

Добавленный контроллер доступа отображается на**Устройства**странице. Вы можете нажать**Добавить и продолжить** для добавления дополнительных контроллеров доступа.

4.2.2 Добавление партиями

Мы рекомендуем вам использовать функцию автопоиска, когда вы добавляете контроллеры доступа партиями. Убедитесь, что добавляемые вами контроллеры доступа должны находиться в одном сегменте сети.

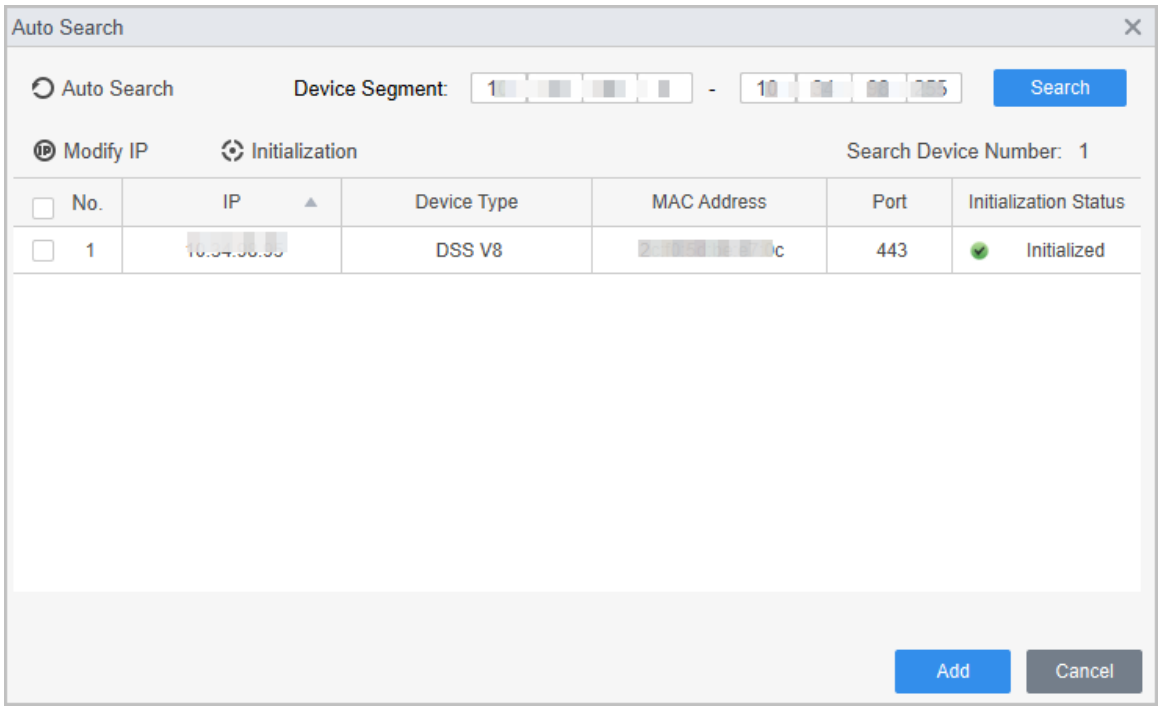
Процедура

Шаг 1 Войдите в Smart PSS Lite.

Шаг 2 Нажмите**Диспетчер устройств**и поиск устройств.

- Нажмите**Автоматический поиск**, для поиска устройств в той же локальной сети.
- Введите диапазон сегмента сети, а затем нажмите**Поиск**.

Рисунок 4-2 Автоматический поиск



Будет отображен список устройств.

Выберите устройство и нажмите**Изменить IP-адрес**изменить свой IP-адрес.

Шаг 3 Выберите контроллер доступа, который вы хотите добавить в Smart PSS Lite, а затем нажмите

Шаг 4 **Добавлять**. Введите имя пользователя и пароль контроллера доступа.

Вы можете просмотреть добавленный контроллер доступа на**Устройства**страница.

Контроллер доступа автоматически входит в Smart PSS Lite после добавления.**Онлайн**является отображается после успешного входа в систему.

4.3 Управление пользователями

Добавьте пользователей, назначьте им карты и настройте их права доступа.

4.3.1 Настройка типа карты

Установите тип карты, прежде чем назначать карты пользователям. Например, если назначенная карта — это удостоверение личности, установите тип карты на удостоверение личности.

Процедура

Шаг 1 Войдите в Smart PSS Lite.

Шаг 2 Нажмите**Доступ к решению**>**Менеджер по персоналу**>

Шаг 3 **Пользователь**. На**Тип выпуска карты**и затем выберите тип карты.

Убедитесь, что тип карты совпадает с фактически назначенной картой; в противном случае карта Номер не может быть прочитан.

Шаг 4 Нажмите**ХОРОШО**.

4.3.2 Добавление пользователей

4.3.2.1 Добавление по одному

Вы можете добавлять пользователей по одному.

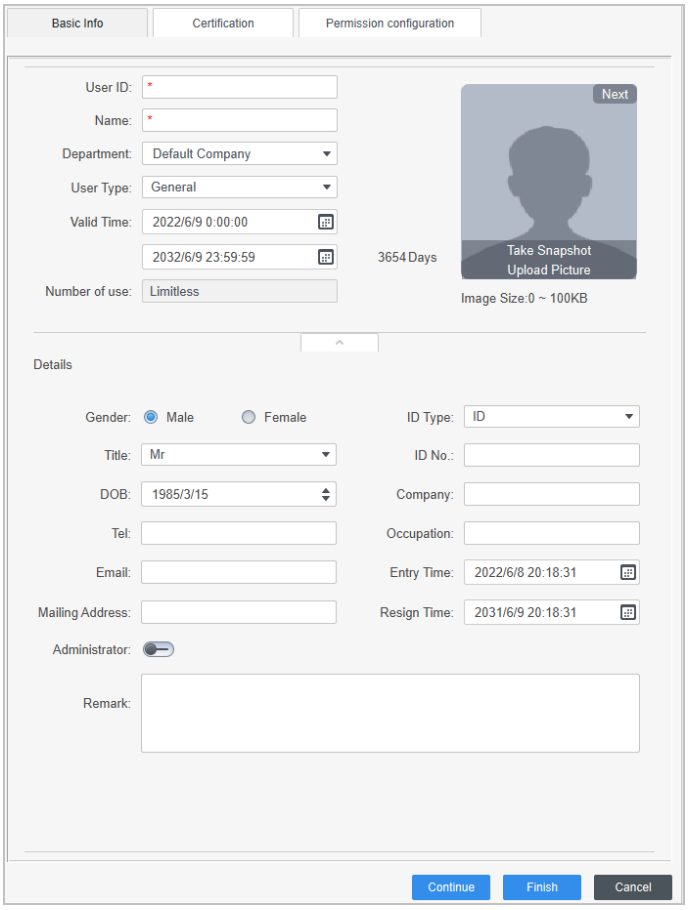
Процедура

Шаг 1 Войдите в Smart PSS Lite.

Шаг 2 Нажмите**Доступ к решению**>**Менеджер по персоналу**>**Пользователь**>**Добавлять**.

Шаг 3 Нажмите**Основная информация**и введите основную информацию о пользователе, а затем импортируйте изображение лица.

Рисунок 4-3 Добавьте основную информацию



Шаг 4 Нажмите на**Сертификация**вкладка для добавления информации о сертификации пользователя.

- Настройте пароль: Пароль должен состоять из 6–8 цифр.
- Настройте карту: Номер карты может быть считан автоматически или введен вручную. Чтобы автоматически считать номер карты, выберите устройство для считывания карт, а затем поместите карту в устройство для считывания карт.

  1. На**Карточка**область, щелкните и выберите**Эмитент карты**, а затем нажмите**ХОРОШО**.

2. Щелкните**Добавлять**, проведите картой по считывателю карт. Отобразится номер карты.

3. Щелкните**ХОРОШО**.

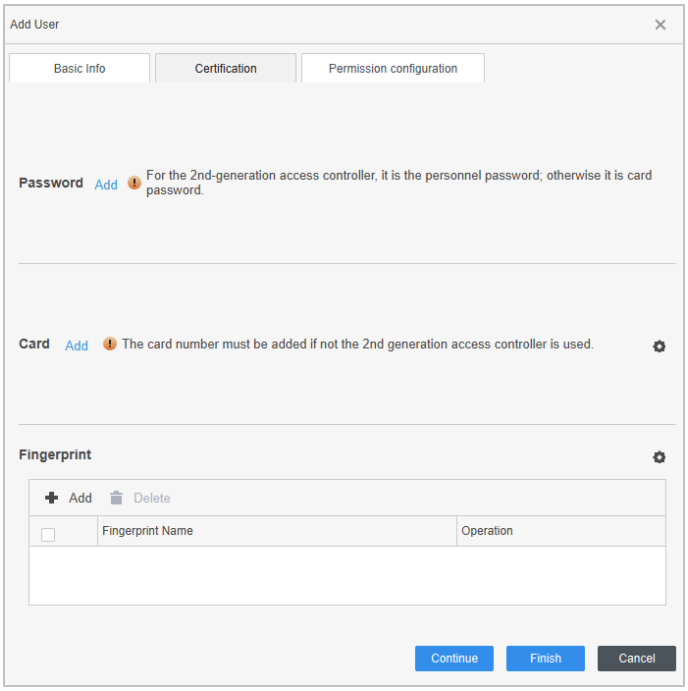
После добавления карты вы можете сделать ее основной или картой принуждения, заменить карту на новую или удалить карту.

- Настройте отпечаток пальца.

1. На**Отпечаток пальца**область, щелкните и выберите**Сканер отпечатков пальцев**, а затем нажмите **ХОРОШО**.

2. Щелкните**Добавить отпечаток пальца**нажмите пальцем на сканер три раза подряд.

Рисунок 4-4 Добавьте пароль, карту и отпечаток пальца



Шаг 5 Настройте разрешения для пользователя. Подробности см. в разделе "4.3.3 Назначение разрешения на доступ". Нажмите

Шаг 6 **Заканчивать**.

4.3.2.2 Добавление партиями

Вы можете добавлять пользователей партиями.

Процедура

Шаг 1 Войдите в Smart PSS Lite.

Шаг 2 Нажмите**Менеджер по персоналу**>**Пользователь**>**Пакетное добавление**.

Шаг 3 Выбирать**Эмитент карты**из**Устройство**список, а затем настройте параметры.

Рисунок 4-5 Добавление пользователей партиями

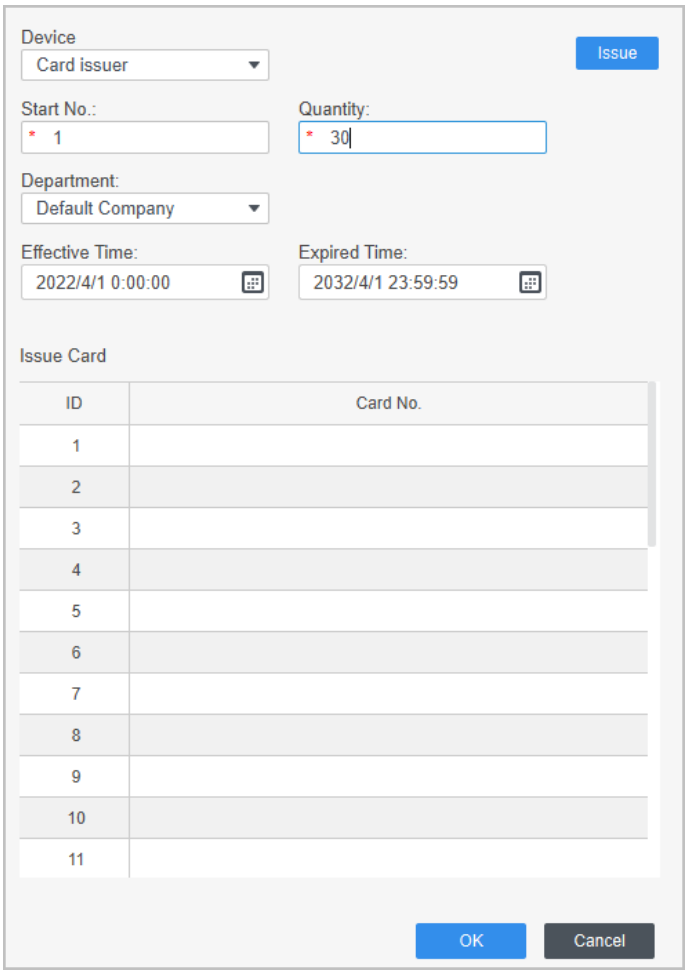


Таблица 4-2 Параметры добавления пользователей в пакеты

Параметр	Описание
Стартовый номер	Идентификатор пользователя начинается с указанного вами числа.
Количество	Количество пользователей, которых вы хотите добавить.
Отделение	Выберите отдел, к которому принадлежит пользователь.
Эффективное время/истекшее время	Пользователи могут разблокировать дверь в течение определенного периода времени.

Шаг 4 Нажмите**Проблема**.

Номер карты будет считан автоматически. Нажмите

Шаг 5 **ХОРОШО**.

Шаг 6 На**Пользователь**странице, нажмите для заполнения информации о пользователе.

4.3.3 Назначение разрешения на доступ

Создайте группу разрешений, которая представляет собой набор разрешений на доступ к дверям, а затем свяжите пользователей с группой, чтобы они могли открывать соответствующие двери.

Процедура

Шаг 1 Войдите в Smart PSS Lite.

Шаг 2 Нажмите**Доступ к решению**>**Менеджер по персоналу**>**Конфигурация разрешений**

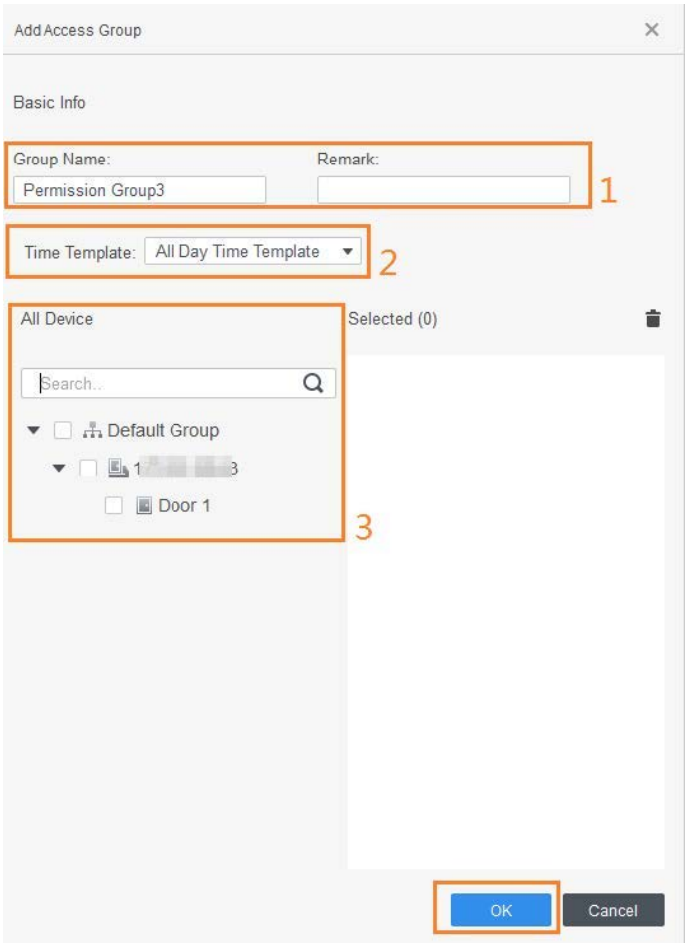
Шаг 3 Щелкните .

Шаг 4 Введите имя группы, примечания (необязательно) и выберите шаблон времени.

Шаг 5 Выберите устройство контроля доступа.

Шаг 6 Нажмите**ХОРОШО**.

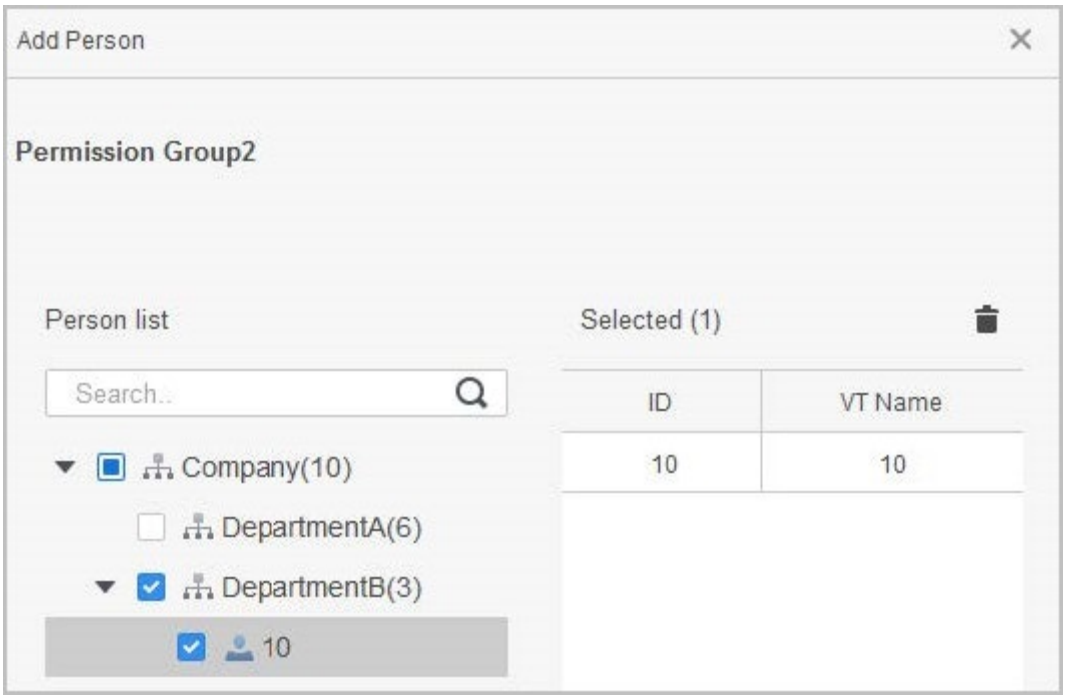
Рисунок 4-6 Создание группы разрешений



Шаг 7 Нажмите добавленной вами группы разрешений.

Шаг 8 Выберите пользователей, чтобы связать их с группой разрешений.

Рисунок 4-7 Добавление пользователей в группу разрешений



Шаг 9 Нажмите**ХОРОШО**.

Пользователи в группе разрешений могут разблокировать дверь после действительной проверки личности.

4.3.4 Назначение разрешений на посещение

Создайте группу разрешений, которая представляет собой набор разрешений на посещение рабочего времени, а затем свяжите сотрудников с этой группой, чтобы они могли отмечать приход/уход с работы с помощью определенных методов проверки.

Процедура

Шаг 1 Войдите в Smart PSS Lite.

Шаг 2 Нажмите**Доступ к решению**>**Менеджер по персоналу**>**Конфигурация разрешений**

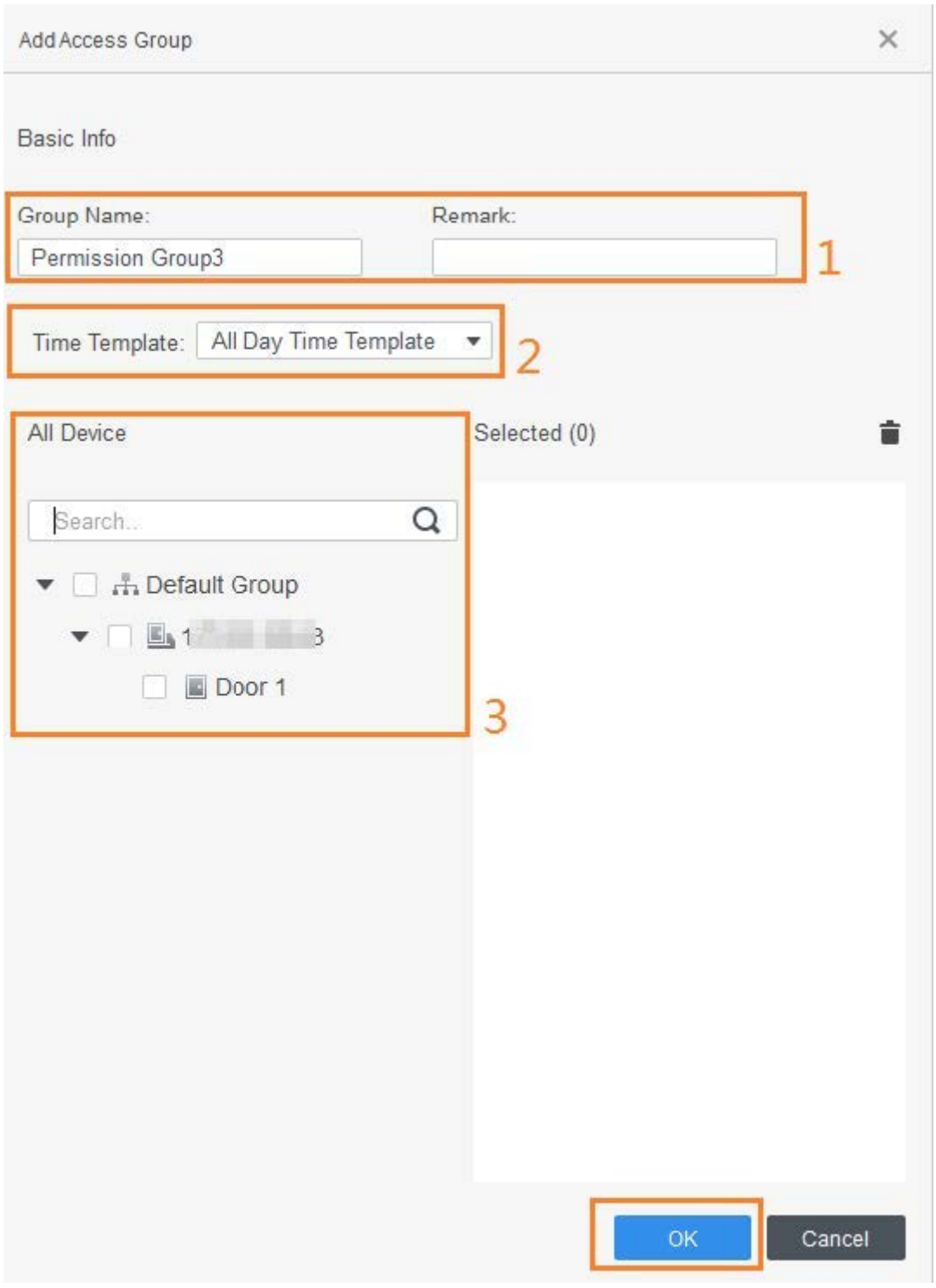
Шаг 3 Щелкните .

Шаг 4 Введите имя группы, примечания (необязательно) и выберите шаблон времени.

Шаг 5 Выберите устройство контроля доступа.

Шаг 6 Нажмите**ХОРОШО**.

Рисунок 4-8 Создание группы разрешений



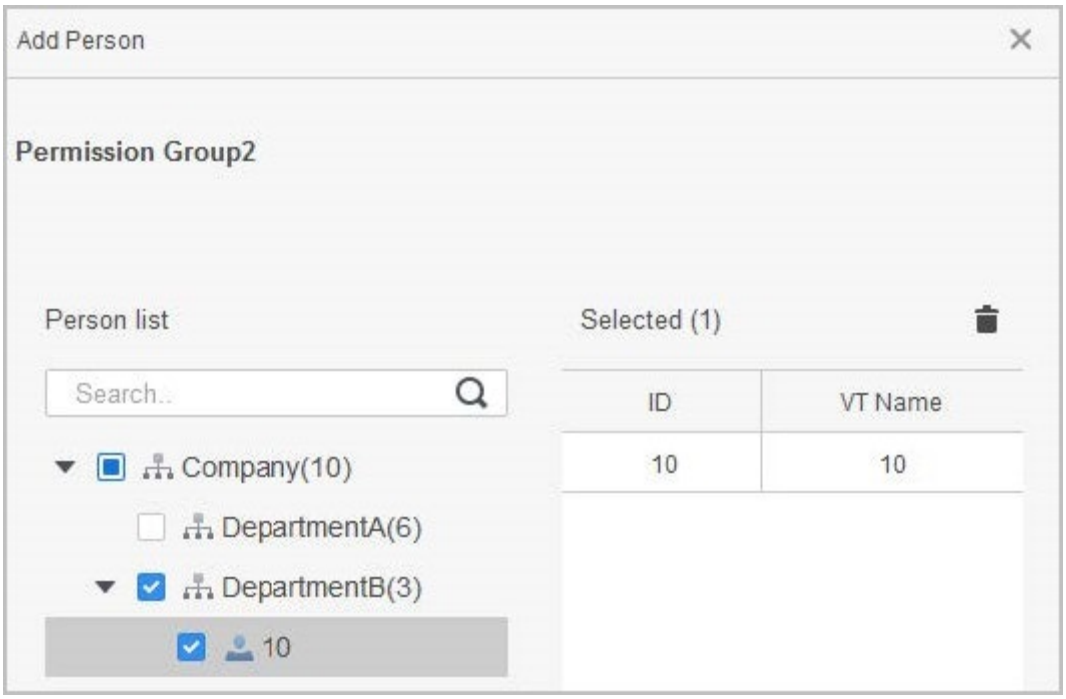
Система учета рабочего времени поддерживает только вход/выход с помощью пароля и распознавания лица.

посещаемость.

Шаг 7 Нажмите добавленной вами группы разрешений.

Шаг 8 Выберите пользователей, чтобы связать их с группой разрешений.

Рисунок 4-9 Добавление пользователей в группу разрешений



Шаг 9 Нажмите**ХОРОШО**.

4.4 Управление доступом

4.4.1 Дистанционное открытие и закрытие двери

Вы можете удаленно контролировать и управлять дверью через Smart PSS Lite. Например, вы можете удаленно открывать или закрывать дверь.

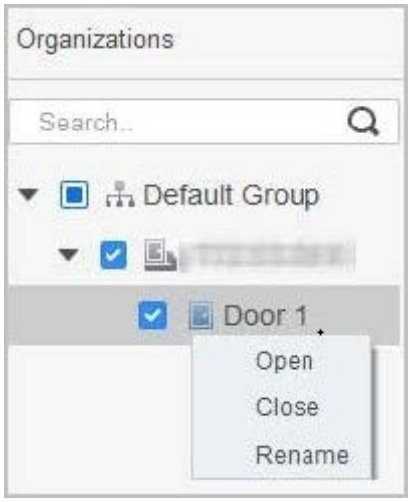
Процедура

Шаг 1 Нажмите**Доступ к решению**>**Менеджер доступа**на главной странице.

Шаг 2 Удаленное управление дверью.

- Выберите дверь, щелкните правой кнопкой мыши и выберите**Открыть**или**Закрывать**.

Рисунок 4-10 Открытая дверь



- Нажмите или , чтобы открыть или закрыть дверь.

Связанные операции

- Фильтрация событий: выберите тип события в**Информация о событии**, а в списке событий отображается выбранный тип событий, например, тревожные события и аномальные события.
- Блокировка обновления событий: Нажмите, чтобы заблокировать список событий, после чего список событий перестанет обновляться. Нажмите, чтобы разблокировать.
- Удаление события: Нажмите, чтобы очистить все события в списке событий.

4.4.2 Настройка «Всегда открыто» и «Всегда закрыто»

После установки «Всегда открыто» или «Всегда закрыто» дверь остается открытой или закрытой все время.

Процедура

Шаг 1 Нажмите**Доступ к решению**>**Менеджер доступа**на главной странице. Нажмите

Шаг 2 **Всегда открыто**или**Всегда близко**чтобы открыть или закрыть дверь.

Рисунок 4-11 Всегда открыто или закрыто

Дверь будет оставаться открытой или закрытой все время. Вы можете нажать**Нормальный**для восстановления нормального состояния контроля доступа, после чего дверь будет открыта или закрыта в зависимости от настроенных методов проверки.

4.4.3 Мониторинг состояния двери

Процедура

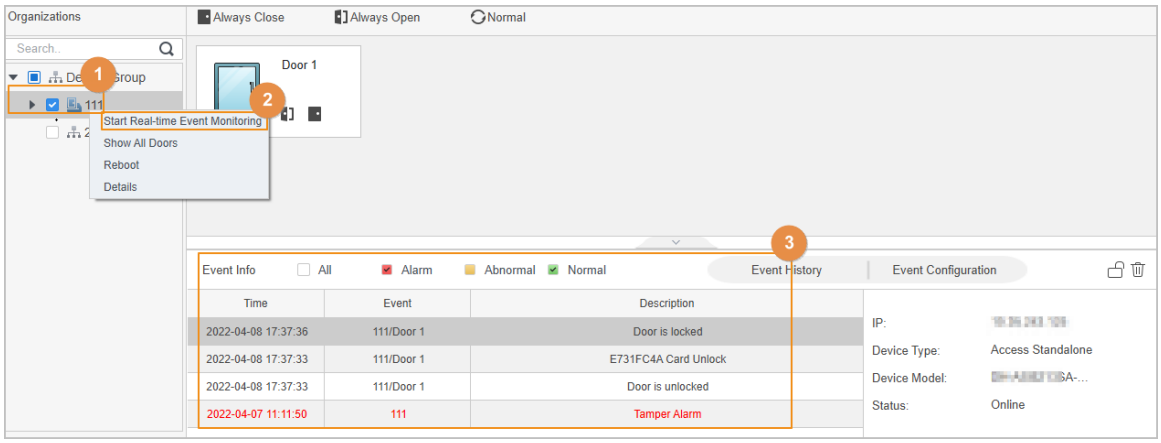
Шаг 1 Нажмите**Доступ к решению**>**Менеджер доступа**на главной странице.

Шаг 2 Выберите контроллер доступа в дереве устройств, щелкните правой кнопкой мыши контроллер доступа и выберите **Начать мониторинг событий в реальном времени**.

События контроля доступа в реальном времени будут отображаться в списке событий.

Нажмите**Остановить монитор**, события контроля доступа в реальном времени отображаться не будут.

Рисунок 4-12 Состояние двери монитора



Связанные операции

- Показать все двери: отображает все двери, контролируемые контроллером доступа.
- Перезагрузка: перезапустите контроллер доступа.
- Подробности: просмотр сведений об устройстве, таких как IP-адрес, модель и статус.

Приложение 1. Важные моменты лица

Регистрация

Перед регистрацией

- Очки, шляпы и бороды могут повлиять на эффективность распознавания лиц.
- Не закрывайте брови, надевая шляпу.
- Не меняйте сильно стиль бороды, если используете контроллер доступа, в противном случае распознавание лица может оказаться невозможным.
- Держите лицо в чистоте.
- Располагайте контроллер доступа на расстоянии не менее 2 метров от источника света и не менее 3 метров от окон или дверей; в противном случае подсветка и прямые солнечные лучи могут повлиять на эффективность распознавания лиц контроллером доступа.

Во время регистрации

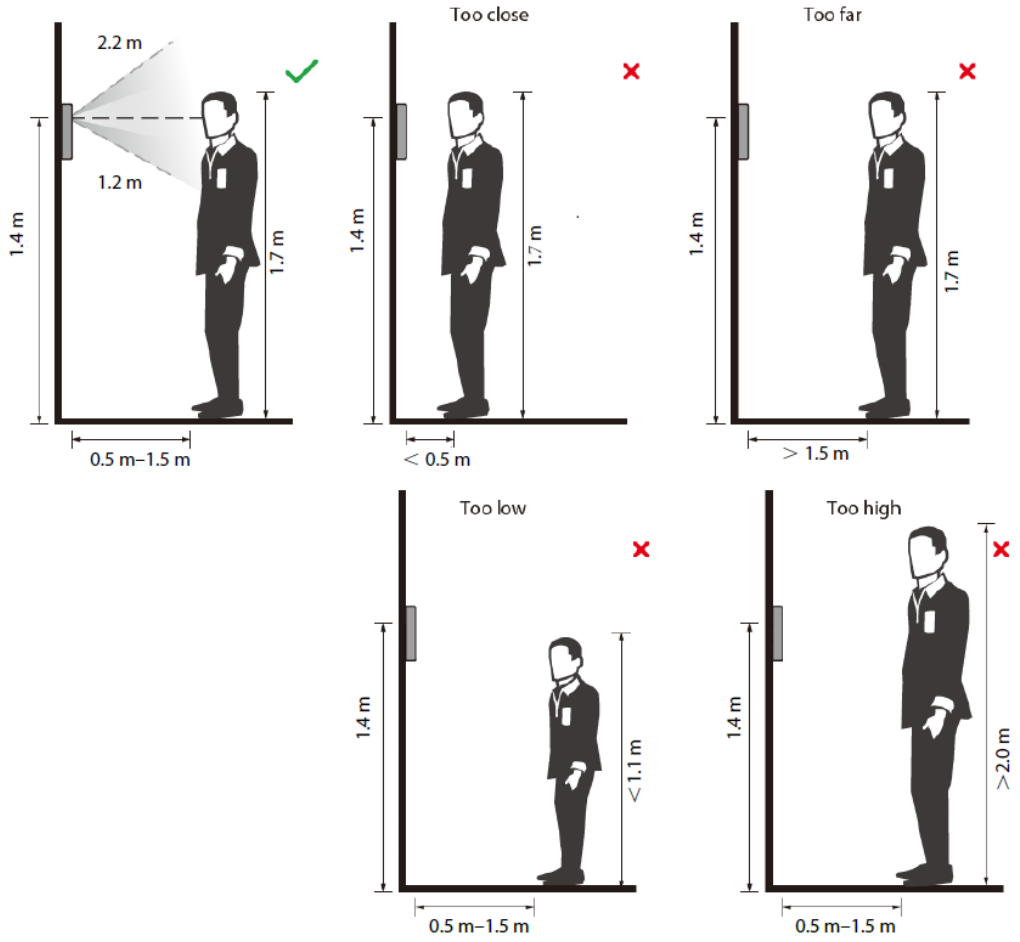
- Вы можете регистрировать лица через контроллер доступа или через платформу. Для регистрации через платформу см. руководство пользователя платформы.
- Поместите голову в центр рамки фотосъемки. Изображение лица будет захвачено автоматически.

- Не трясите головой и телом, иначе регистрация может быть не удалась.
- Избегайте одновременного появления в кадре двух лиц.

Положение лица

Если ваше лицо находится в неправильном положении, точность распознавания лица может быть снижена.

Приложение Рисунок 1-1 Соответствующее положение лица



Требования к лицам

- Убедитесь, что лицо чистое и лоб не закрыт волосами.
- Не надевайте очки, шляпы, густую бороду или другие украшения на лице, которые могут повлиять на запись изображения лица.
- С открытыми глазами, без выражения лица, поверните лицо к центру камеры.
- Во время записи вашего лица или во время распознавания лиц не держите лицо слишком близко или слишком далеко от камеры.

Приложение Рисунок 1-2 Положение головы

Приложение Рисунок 1-3 Расстояние до лица

- При импорте изображений лиц через платформу управления убедитесь, что изображение разрешение в диапазоне 150 × 300 пикселей–600 × 1200 пикселей; пиксели изображения более 500 × 500 пикселей; размер изображения менее 100 КБ, имя изображения и идентификатор человека совпадают.
- Убедитесь, что лицо занимает более 1/3, но не более 2/3 всей площади изображения, и соотношение сторон не превышает 1:2.

Приложение 2. Важные моменты внутренней связи

Операция

Контроллер доступа может функционировать как VTO для реализации функции домофона.

Предпосылки

Функция внутренней связи настраивается на контроллере доступа и VTO.

Процедура

Шаг 1 На экране ожидания нажмите «Введите».

Шаг 2 номер комнаты», а затем нажмите .

Приложение 3. Важные моменты отпечатков пальцев

Инструкции по регистрации

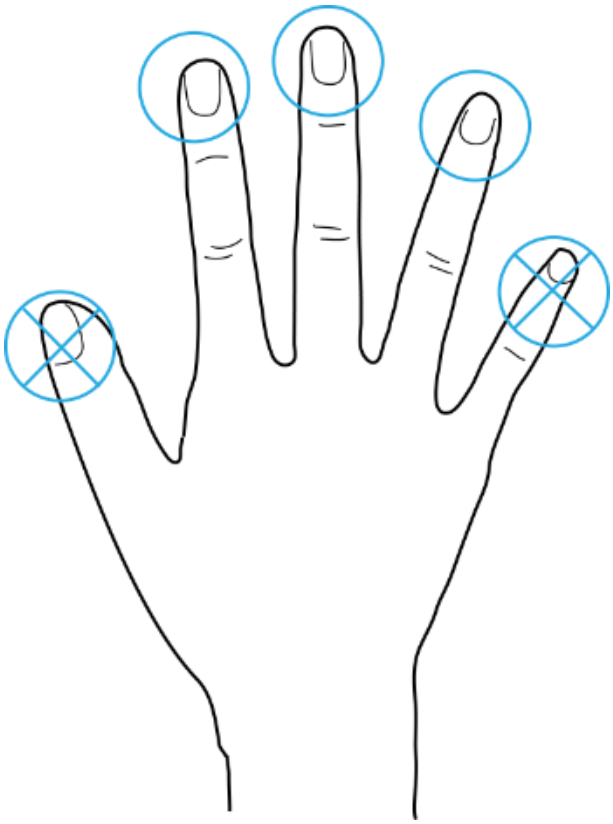
При регистрации отпечатка пальца обратите внимание на следующие моменты:

- Убедитесь, что ваши пальцы и поверхность сканера чистые и сухие.
- Нажмите пальцем на центр сканера отпечатков пальцев.
- Не размещайте сканер отпечатков пальцев в местах с ярким освещением, высокой температурой и высокой влажностью.
- Если ваши отпечатки пальцев нечеткие, воспользуйтесь другими методами разблокировки.

Пальцы рекомендуются

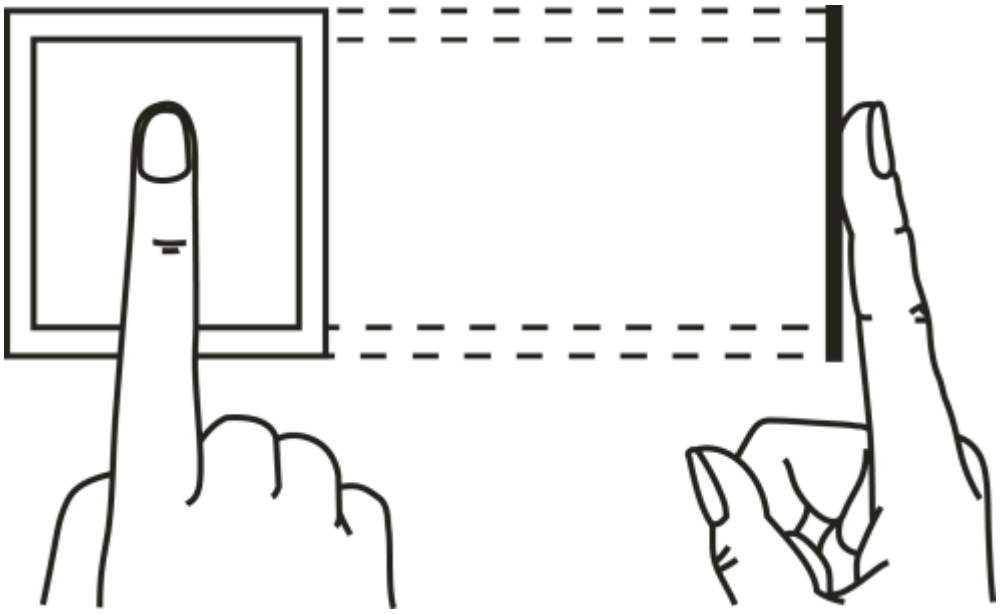
Рекомендуются указательные, средние и безымянные пальцы. Большие пальцы и мизинцы не могут быть легко помещены в центр записи.

Приложение Рисунок 3-1 Рекомендуемые пальцы

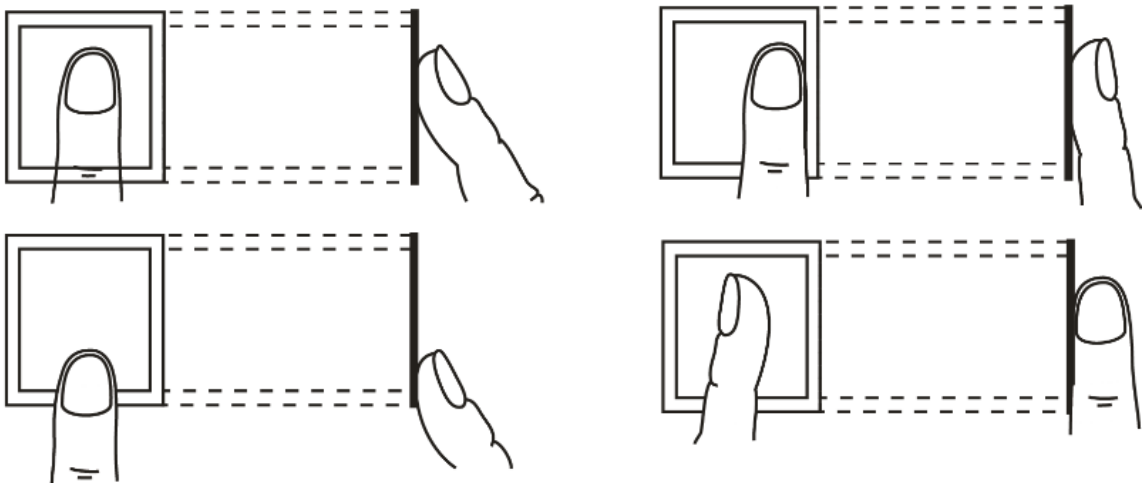


Как приложить отпечаток пальца к сканеру

Приложение Рисунок 3-2 Правильное размещение



Приложение Рисунок 3-3 Неправильное размещение



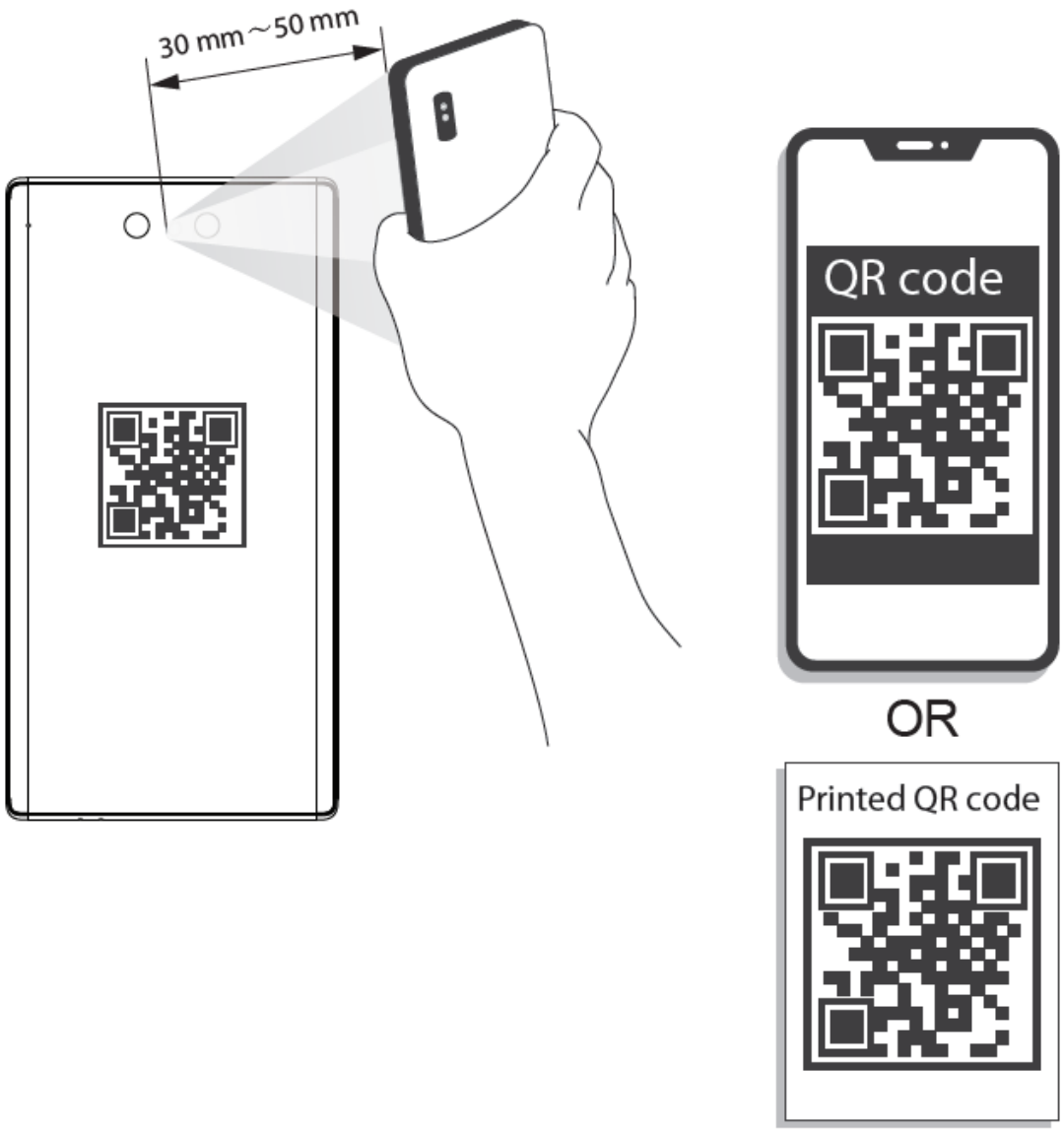
Приложение 4. Важные моменты QR-кода

Сканирование

Контроллер доступа: Разместите QR-код на телефоне на расстоянии 30–50 мм от линзы сканера QR-кода. Он поддерживает QR-код, который должен быть больше 30 мм × 30 мм и размером менее 128 байт.

Расстояние обнаружения QR-кода различается в зависимости от байтов и размера QR-кода.

Приложение Рисунок 4-1 Сканирование QR-кода



Приложение 5 Рекомендации по кибербезопасности

Обязательные действия, которые необходимо предпринять для обеспечения безопасности базовой сети устройства:

1.**Используйте надежные пароли**

Пожалуйста, воспользуйтесь следующими рекомендациями по установке паролей:

- Длина не должна быть менее 8 символов.
- Включите не менее двух типов символов; типы символов включают заглавные и строчные буквы, цифры и символы.
- Не используйте имя учетной записи или имя учетной записи в обратном порядке.
- Не используйте непрерывные символы, такие как 123, abc и т. д.
- Не используйте пересекающиеся символы, такие как 111, aaa и т. д.

2.**Своевременно обновляйте прошивку и клиентское программное обеспечение**

- Согласно стандартной процедуре в технологической отрасли, мы рекомендуем поддерживать прошивку вашего устройства (например, NVR, DVR, IP-камеры и т. д.) в актуальном состоянии, чтобы гарантировать, что система оснащена последними исправлениями и патчами безопасности. Когда устройство подключено к общедоступной сети, рекомендуется включить функцию «автоматической проверки обновлений», чтобы получать своевременную информацию об обновлениях прошивки, выпущенных производителем.
- Мы рекомендуем вам загрузить и использовать последнюю версию клиентского программного обеспечения.

Полезные рекомендации по улучшению сетевой безопасности вашего устройства:

1.**Физическая защита**

Мы предлагаем вам выполнить физическую защиту устройства, особенно устройств хранения данных. Например, поместите устройство в специальную компьютерную комнату и шкаф, а также внедрите хорошо организованный контроль доступа и управление ключами, чтобы предотвратить несанкционированный персонал от осуществления физических контактов, таких как повреждение оборудования, несанкционированное подключение съемного устройства (например, USB-флеш-диска, последовательного порта) и т. д.

2.**Регулярно меняйте пароли**

Мы рекомендуем вам регулярно менять пароли, чтобы снизить риск их угадывания или взлома.

3.**Установка и обновление паролей. Своевременный сброс информации.**

Устройство поддерживает функцию сброса пароля. Пожалуйста, настройте соответствующую информацию для сброса пароля вовремя, включая почтовый ящик конечного пользователя и вопросы защиты пароля. Если информация изменится, пожалуйста, измените ее вовремя. При установке вопросов защиты пароля рекомендуется не использовать те, которые можно легко угадать.

4.**Включить блокировку учетной записи**

Функция блокировки учетной записи включена по умолчанию, и мы рекомендуем вам оставить ее включенной, чтобы гарантировать безопасность учетной записи. Если злоумышленник попытается войти в систему с неправильным паролем несколько раз, соответствующая учетная запись и исходный IP-адрес будут заблокированы.

5.**Изменить HTTP-порты и другие сервисные порты по умолчанию**

Мы предлагаем вам изменить порты HTTP и других служб по умолчанию на любой набор чисел в диапазоне 1024–65535, чтобы снизить риск того, что посторонние смогут угадать, какие порты вы используете.

6.**Включить HTTPS**

Мы предлагаем вам включить HTTPS, чтобы вы могли посещать веб-сервис через защищенный канал связи.

7.**Привязка MAC-адреса**

Мы рекомендуем вам привязать IP и MAC адрес шлюза к устройству, тем самым уменьшив

риск подмены ARP.

8.**Разумно назначайте учетные записи и привилегии**

В соответствии с требованиями бизнеса и управления разумно добавляйте пользователей и назначайте им минимальный набор разрешений.

9.**Отключите ненужные службы и выберите безопасные режимы**

Если в них нет необходимости, рекомендуется отключить некоторые службы, такие как SNMP, SMTP, UPnP и т. д., чтобы снизить риски.

При необходимости настоятельно рекомендуется использовать безопасные режимы, включая, помимо прочего, следующие службы:

- SNMP: выберите SNMP v3 и установите надежные пароли шифрования и пароли аутентификации.
- SMTP: выберите TLS для доступа к серверу почтовых ящиков.
- FTP: выберите SFTP и установите надежные пароли.
- Точка доступа: выберите режим шифрования WPA2-PSK и установите надежные пароли.

10.**Зашифрованная передача аудио и видео**

Если ваши аудио- и видеоданные очень важны или конфиденциальны, мы рекомендуем вам использовать функцию зашифрованной передачи, чтобы снизить риск кражи аудио- и видеоданных во время передачи.

Напоминание: зашифрованная передача данных приведет к некоторой потере эффективности передачи.

11.**Безопасный аудит**

- Проверяйте пользователей в сети: мы рекомендуем вам регулярно проверять пользователей в сети, чтобы убедиться, что устройство не авторизовано.
- Проверьте журнал устройства: просматривая журналы, вы можете узнать IP-адреса, которые использовались для входа на ваши устройства, а также их основные операции.

12.**Сетевой журнал**

Из-за ограниченной емкости устройства, сохраненный журнал ограничен. Если вам необходимо сохранить журнал в течение длительного времени, рекомендуется включить функцию сетевого журнала, чтобы гарантировать синхронизацию критических журналов с сервером сетевого журнала для трассировки.

13.**Постройте безопасную сетевую среду**

Чтобы лучше обеспечить безопасность устройства и снизить потенциальные киберриски, мы рекомендуем:

- Отключите функцию сопоставления портов маршрутизатора, чтобы избежать прямого доступа к устройствам интрасети из внешней сети.
- Сеть должна быть разделена и изолирована в соответствии с реальными потребностями сети. Если между двумя подсетями нет требований к коммуникации, предлагается использовать VLAN, сетевой GAP и другие технологии для разделения сети, чтобы достичь эффекта изоляции сети.
- Внедрите систему аутентификации доступа 802.1x для снижения риска несанкционированного доступа к частным сетям.
- Включите функцию фильтрации IP/MAC-адресов, чтобы ограничить круг хостов, которым разрешен доступ к устройству.