

Доступ к автономной версии

Руководство пользователя



V1.0.3

Предисловие

Общий

В данном руководстве описаны функции и работа автономного устройства доступа (далее именуемого «Устройство»). Внимательно прочтите руководство перед использованием устройства и сохраните его для дальнейшего использования.

Символы

В руководстве могут встречаться следующие символы.

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

История изменений

Версия	Содержание для пересмотра	Время выпуска
V1.0.3	- Добавлена функция QR-кода. - Добавлена функция Bluetooth. - Переработаны функции настройки будильника. - Добавлена функция сравнения данных в бэкенде. - Добавлена функция воспроизведения звука.	Июль 2026 г.
V1.0.2	Пересмотренное содержание.	Декабрь 2025 г.
V1.0.1	Добавлено описание инициализации.	Декабрь 2024 г.
V1.0.0	Первый релиз.	Август 2024 г.

Уведомление о защите конфиденциальности

Как пользователь устройства, вы можете собирать персональные данные физических лиц, такие как их имена, адреса электронной почты, изображения лиц, аудиозаписи и отпечатки пальцев. Вы несете полную ответственность за любые действия, связанные с обработкой персональных данных. Вы обязуетесь соблюдать местные законы и правила защиты конфиденциальности для защиты законных прав и интересов физических лиц и принимать меры, требуемые действующим законодательством, включая, помимо прочего, предоставление четкой и исчерпывающей информации физическим лицам до обработки их персональных данных, получение согласия от физических лиц, когда это необходимо, информирование физических лиц о наличии зоны наблюдения и предоставление необходимой контактной информации.

Заявление об использовании интеллектуального продукта

Интеллектуальные продукты используют технологии искусственного интеллекта для эффективного повышения уровня безопасности. На работу функций интеллектуального распознавания и оповещения могут влиять такие факторы, как освещение окружающей среды, ракурсы камеры, препятствия и задержки в сети, что потенциально может привести к ложным срабатываниям, пропущенным оповещениям или задержкам реагирования. Данный интеллектуальный продукт предназначен исключительно для использования в качестве вспомогательного инструмента обеспечения безопасности. Результаты идентификации носят исключительно справочный характер и не являются абсолютной гарантией личной безопасности или безопасности имущества. Пользователям необходимо сочетать эти продукты с необходимыми мерами физической защиты для повышения общей безопасности. За исключением случаев, предусмотренных законом, или в случае умышленной или грубой халатности со стороны компании, компания не несет ответственности за любые убытки, вызванные вышеупомянутыми факторами, не зависящими от компании.

Объявление интерфейса

Данное руководство в основном описывает основные функции устройства. Интерфейсы, используемые при его производстве, процедуры возврата устройства на завод для проверки и выявления неисправностей в данном руководстве не описаны. Для получения информации об этих интерфейсах обратитесь в службу технической поддержки.

О руководстве пользователя

- Данное руководство предназначено только для общего ознакомления. Возможны расхождения между версиями.

продукт и данное руководство, включая, помимо прочего, печатные, электронные и любые другие издания. • Руководство будет обновляться в соответствии с последними законами и правилами соответствующих юрисдикций.

Технические характеристики и документация могут быть изменены без предварительного уведомления. Для получения актуальной информации, а также юридических уведомлений, обратитесь к печатному руководству, странице продукта на нашем официальном сайте или отсканируйте QR-код для доступа к электронной версии.

- Руководство будет обновляться по мере необходимости с учетом изменений в продукте и применимого законодательства.

требования. Эти обновления не уменьшат ваши законные права и не удалят и не ослабят информацию о безопасности или основные инструкции, предоставленные во время покупки. • Хотя мы прилагаем все усилия для обеспечения точности, ошибки или отклонения в описаниях могут

быть незначительными.

Возможны несоответствия в функциях, операциях или технических данных. В случае возникновения каких-либо неясностей или разногласий мы оставляем за собой право окончательного разъяснения. • Все

товарные знаки, зарегистрированные товарные знаки и названия компаний, упомянутые в данном руководстве, являются собственностью [название компании].
собственность их соответствующих владельцев.

Оглавление

Предисловие.....	Я
1 Обзор.....	1
2 Локальные операции.....	2
2.1 Инициализация.....	2
2.2 Главное меню.....	3
2.3 Управление пользователями.....	4
2.3.1 Добавление пользователя.....	4
2.3.2 Удаление пользователя.....	5
2.4 Настройка режима разблокировки двери.....	5
2.5 Настройка продолжительности разблокировки.....	6
2.6 Настройка датчика двери.....	6
2.7 Управление паролями.....	6
2.7.1 Изменение пароля администратора.....	6
2.7.2 Добавление публичного пароля.....	7
2.7.3 Удаление публичного пароля.....	7
2.8 Управление основной картой.....	7
2.8.1 Добавление основной карты.....	7
2.8.2 Удаление основной карты.....	8
2.8.3 Управление пользовательскими картами через основную карту.....	8
2.9 Настройка периода ожидания двери.....	8
2.10 Восстановление заводских настроек.....	9
3. Операции с веб-страницами.....	10
3.1 Инициализация.....	10
3.2 Сброс пароля.....	11
3.3 Главная страница.....	12
3.4 Управление персоналом.....	13
3.5 Мониторинг доступа.....	18
3.6 Настройка контроля доступа.....	20
3.6.1 Настройка параметров контроля доступа.....	20
3.6.2 Сигнализация.....	25
3.6.3 Настройки карты.....	29
3.6.4 Настройка периодов.....	34
3.6.5 Настройка QR-кода.....	37
3.6.6 Настройка сравнения на стороне сервера.....	38
3.6.7 Настройка функций порта.....	38
3.6.8 Настройка разблокировки паролем.....	39
3.6.9 Настройка разблокировки режима от первого лица.....	39

3.6.10 Настройка защиты от обратной передачи.....	40	3.7
Настройка звука.....	42	
3.8 Настройки связи.....	43	
3.8.1 Сетевые настройки.....	43	
3.8.2 Настройки режима.....	54	
3.8.3 Настройка параметров Bluetooth.....	58	3.9 Настройка
системы.....	59	
3.9.1 Управление пользователями.....	59	
3.9.2 Просмотр онлайн-пользователей.....	62	
3.9.3 Настройка времени.....	62	
3.10 Центр технического обслуживания.....	63	
3.10.1 Диагностика одним щелчком мыши.....	63	
3.10.2 Информация о системе.....	64	3.10.3 Объем
данных.....	64	
3.10.4 Журналы просмотра.....	64	
3.10.5 Управление техническим обслуживанием.....	65	
3.10.6 Обновление системы.....	67	
3.10.7 Расширенное техническое обслуживание.....	68	
3.11 (Необязательно) Настройки безопасности.....	68	
3.11.1 Состояние безопасности.....	68	
3.11.2 Настройка системной службы.....	69	
3.11.3 Атака Защита.....	70	
3.11.4 Установка сертификата устройства.....	73	3.11.5
Установка сертификата доверенного центра сертификации.....	76	
3.11.6 Предупреждение о безопасности.....	77	
3.11.7 Аутентификация безопасности.....	78	
4. Работа с телефоном.....	79	
4.1 Инициализация.....	79	
4.2 Вход на веб-страницу.....	80	
4.3 Главная страница.....	81	
4.4 Управление персоналом.....	83	
4.5 Настройка системы.....	86	4.5.1 Просмотр
информации о версии.....	86	
4.5.2 Техническое обслуживание.....	86	
4.5.3 Настройка времени.....	87	
4.5.4 Объем данных.....	89	4.5.5
Язык.....	89	4.6 Настройка контроля
доступа.....	89	4.6.1 Настройка методов
разблокировки.....	89	
4.6.2 Настройка параметров контроля доступа.....	90	

4.6.3 Настройка сигналов тревоги.....	93
Настройка связи сигналов тревоги.....	95
Настройка параметров карты.....	96
связи.....	98
4.7.1 Настройка TCP/IP.....	98
4.7.2 Настройка Wi-Fi.....	100
точки доступа Wi-Fi.....	100
облачного сервиса.....	101
автоматической регистрации.....	102
4.7.6 Режим настройки.....	102
4.7.7 Настройка Bluetooth.....	106
звука.....	107
4.9 Журналы просмотров.....	107
4.9.1 Системные журналы.....	107
4.9.2 Разблокировка записей.....	108
4.9.3 Журналы аварийных сигналов.....	
108 5 Конфигурация Smart PSS Lite.....	109
5.1 Установка.....	109
5.2 Добавление устройств по одному.....	109
5.3 Добавление пользователей.....	110
Приложение 1. Важные моменты инструкции по регистрации отпечатков пальцев.....	111
Приложение 2. Рекомендации по безопасности.....	113

1. Обзор

Данное изделие представляет собой устройство контроля доступа, объединяющее считывание карт, настройку и управление. Изделие имеет простой и модный внешний вид и подходит для офисных зданий, школ, парков, жилых комплексов, заводов, общественных мест, бизнес-центров, правительственных зданий и других мест применения.

2 Локальные операции

2.1 Инициализация

После первого включения устройства необходимо установить пароль администратора. Пароль администратора используется для входа в главное меню устройства.

Процедура

Шаг 1. Включите устройство, индикатор начнет медленно мигать красным. Введите пароль

Шаг 2 Нажимать # , администратора, затем нажмите #.

Пароль должен состоять из 1–8 символов.

Если индикатор горит синим цветом, это означает, что устройство инициализировано.



После инициализации вы сможете использовать только функции устройства. Чтобы войти на веб-страницу устройства, инициализируйте устройство на его веб-странице или через ConfigTool.

Связанные операции • При

инициализации через устройство в качестве пароля учетной записи администратора можно установить только цифры. • При инициализации в качестве пароля учетной записи администратора можно установить цифры, буквы и другие символы. через платформу ConfigTool.

После завершения инициализации устройства вы сможете выполнять операции только с самим устройством. Если вам необходимо подключить устройство к сети, используйте ConfigTool или платформу для инициализации устройства.

При использовании ConfigTool или платформы для инициализации устройства после настройки сетевой учетной записи и пароля устройство автоматически завершит инициализацию и перейдет в режим ожидания. Пароль локального администратора преобразуется из сетевого пароля. Если пароль превышает 8 символов, сохраняются только первые 8 символов. Буквы преобразуются в цифры в соответствии со стандартом E.161. Преобразование пароля нечувствительно к регистру, а все остальные символы преобразуются в 0.



• После инициализации, если вы измените сетевой пароль, пароль локального администратора останется неизменным. • Если вы сначала инициализируете устройство, а затем — ConfigTool или платформу, пароль локального администратора останется неизменным. Пароль администратора останется без изменений.

Рисунок 2-1 Е.161 (клавиатура Т9)

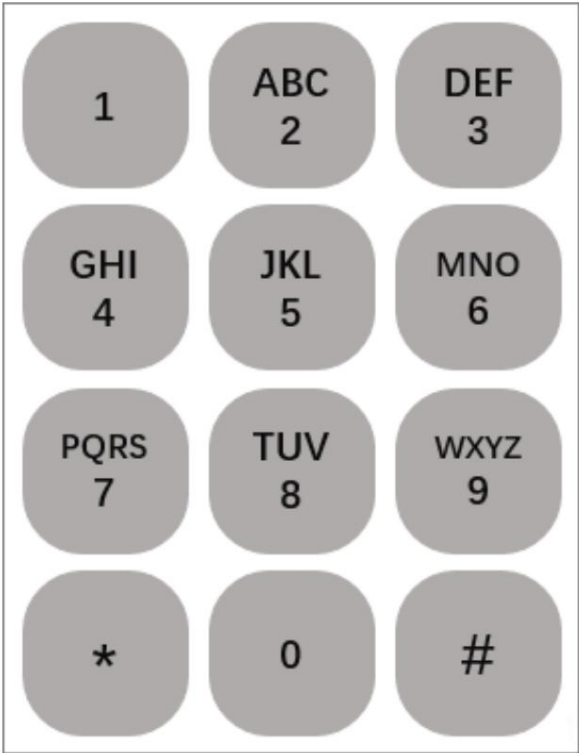


Таблица 2-1. Пример преобразования.

Пароль сети	Пароль локального администратора
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

2.2 Главное меню

Вход в главное меню

Нажимать # , Введите пароль администратора, а затем нажмите #.

- Индикатор мигает синим цветом, это означает, что вы вошли в главное меню.
- Индикатор один раз мигает красным, раздается 3 звуковых сигнала, после чего индикатор загорается синим цветом и горит постоянно. Это значит, что пароль неверный.

Похожие вопросы

- Индикатор мигает зеленым один раз, и раздается один звуковой сигнал, что означает, что операция завершена. Проверка контроля доступа прошла успешно.
- Индикатор мигает красным один раз, и раздается 3 звуковых сигнала, что означает, что операция завершена. Проверка контроля доступа не удалась.
- Если индикатор медленно мигает красным, это означает, что устройство не инициализировано.

- Если индикатор горит синим цветом, это означает, что устройство находится в режиме ожидания.
- Если индикатор мигает синим цветом, это означает, что устройство перешло в главное меню.
- Клавиатура белая при работе с устройством. Если в течение 10 секунд не выполняются никаких действий, Индикатор гаснет, и устройство выходит из текущего экрана.

2.3 Управление пользователями

2.3.1 Добавление пользователя



- Для одного пользователя можно добавить только одну карту, один пароль или один отпечаток пальца. Необходимо добавить как минимум один способ оплаты: карту, пароль и отпечаток пальца.
- Функция распознавания отпечатков пальцев доступна в некоторых моделях.

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 1 и # , чтобы добавить пользователей.

Шаг 3 Введите идентификатор пользователя, а затем нажмите #.

- Если индикатор не загорается и устройство издает звуковой сигнал, идентификатор пользователя добавляется успешно.
- Если индикатор мигает красным и устройство издает звуковой сигнал, добавление идентификатора пользователя не удается.
Возможная причина в том, что данный идентификатор уже существует. Пожалуйста, попробуйте другой идентификатор.



В качестве идентификатора устройства можно вводить только цифры.

Шаг 4. После проведения карты через считывающее устройство нажмите # , чтобы добавить карту.

Если добавлять карту не нужно, нажмите # , чтобы пропустить этот шаг.

Шаг 5. Введите пароль пользователя, а затем нажмите #.

Если вам не нужно устанавливать пароль пользователя, нажмите #, чтобы пропустить этот шаг.



Пароль может состоять из 1–8 символов.

Шаг 6. Добавьте отпечаток пальца, а затем нажмите #.

Если вам не нужно устанавливать отпечаток пальца, нажмите #, чтобы пропустить этот шаг.



Эта функция доступна на некоторых моделях.

Шаг 7. Повторите шаги со 2 по 6, чтобы добавить больше пользователей.

После добавления пользователя нажмите * для возврата в главное меню, а затем нажмите * для возврата в режим ожидания.

2.3.2 Удаление пользователя

Процедура

- Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.
- Войдите в главное меню, и индикатор начнет мигать синим цветом.
- Шаг 2 Нажмите 2 и #.
- Шаг 3 Удалить пользователя.
- Проведите картой по считывающему устройству, затем нажмите #.
- 
- Если вы проведете картой, которая еще не добавлена, удаление не удастся.
- Введите идентификатор пользователя и нажмите #.
- 
- Если ввести идентификатор, который еще не был добавлен, удаление не удастся.
- Введите 0000, а затем нажмите # , чтобы удалить всех пользователей.
- После удаления нажмите * для возврата в главное меню, а затем нажмите * для выхода из главного меню.
- меню.

2.4 Настройка режима разблокировки двери

Справочная информация



Функция распознавания отпечатков пальцев доступна на некоторых моделях.

Процедура

- Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.
- Войдите в главное меню, и индикатор начнет мигать синим цветом.
- Шаг 2 Нажмите 3 и #.
- Шаг 3 Выберите режим разблокировки.
- Нажмите 0 и # , чтобы настроить разблокировку по карте, паролю, Bluetooth или отпечатку пальца.
- Проведите картой, введите пароль или используйте отпечаток пальца, чтобы открыть дверь.
- Пароль может быть получен следующими способами.
- ◇ На экране ожидания введите идентификатор пользователя, нажмите Устройство издает один звуковой сигнал. Введите # для ввода пароля, а затем нажмите # для подтверждения личности.
 - ◇ На экране ожидания введите публичный пароль, а затем нажмите # для подтверждения личности.
 - ◇ Если на веб-странице устройства включена аутентификация по PIN-коду , Люди могут подтвердить свою личность, просто введя пароль.
 - ◇ При использовании устройства с приложением DMSS поддерживается временный пароль. и может быть настроен в приложении.
- Нажмите 1 и # , чтобы установить разблокировку по карте и паролю пользователя.
- Сначала проведите картой. После того, как устройство издает один звуковой сигнал, введите пароль, а затем нажмите # для подтверждения личности.
- Нажмите 2 и # , чтобы настроить разблокировку по карте и отпечатку пальца.

Сначала проведите картой. После того, как устройство издаст один звуковой сигнал, нажмите на отпечаток пальца для подтверждения личности.

- Нажмите 3 и # , чтобы настроить разблокировку с помощью карты, пароля и отпечатка пальца.

Сначала проведите картой. После того, как устройство издаст один звуковой сигнал, приложите отпечаток пальца. Устройство снова раздаётся звуковой сигнал. Введите пароль, а затем нажмите # для подтверждения личности.

Шаг 4. Нажмите * для выхода из главного меню.

2.5 Настройка продолжительности разблокировки

После разблокировки дверь остается открытой в течение определенного времени, что позволяет людям проходить через нее.

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 4 и #.

Шаг 3 Введите время, а затем нажмите #.

Значение варьируется от 1 секунды до 600 секунд. Значение по умолчанию — 3 секунды.

Шаг 4. Нажмите * для выхода из главного меню.

2.6 Настройка дверного датчика

После включения датчика двери по умолчанию одновременно включается и сигнализация о тайм-ауте двери. Если

Если дверь остается открытой после истечения установленного времени ожидания, звуковой сигнал устройства подает сигнал тревоги.

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 5 и #.

Шаг 3 Включите или выключите датчик двери.

Датчик двери по умолчанию отключен.

- Нажмите 0 и # , чтобы выключить датчик двери.
- Нажмите 1 и # , чтобы включить датчик двери.

Шаг 4. Нажмите * для выхода из главного меню.

2.7 Управление паролями

- Пароль администратора: используется для входа в главное меню устройства.

- Открытый пароль: Используется для подтверждения подлинности при разблокировке двери.

2.7.1 Изменение пароля администратора

Для обеспечения безопасности устройства мы рекомендуем периодически менять пароль администратора со временем.

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 0 и #.

Шаг 3 Введите новый пароль, а затем нажмите #.

Шаг 4. Снова введите новый пароль, а затем нажмите #.

- Мигающий зеленый индикатор означает, что пароль успешно изменен.
- Мигающий красный индикатор означает, что вам не удалось изменить пароль.
- После внесения изменений устройство автоматически выходит из главного меню, и индикатор...
Становится сплошным синим цветом. Войдите в главное меню, используя новый пароль, если вы его изменили.
Пароль успешно введен. Если не удалось войти в главное меню, используйте исходный пароль.
Изменить пароль.

2.7.2 Добавление публичного пароля

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 6 и #.

Шаг 3 Введите публичный пароль, а затем нажмите #.

Пароль может состоять из 1–8 символов.



Вы можете добавить только один публичный пароль. Если вы повторите операцию, новый пароль будет изменен. заменит оригинальный.

Шаг 4. Нажмите * для выхода из главного меню.

2.7.3 Удаление открытого пароля

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 7 и #.

Шаг 3 Введите публичный пароль и нажмите #.

Шаг 4. Нажмите * для выхода из главного меню.

2.8 Управление основной картой

2.8.1 Добавление основной карты

После добавления основной карточки вы можете быстро добавлять и удалять другие карточки пользователей через основную карточку.

Справочная информация



Для разблокировки двери основная карта недоступна.

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 8 и #.

Шаг 3 Проведите картой, затем нажмите #.

- Если индикатор мигает зеленым и устройство издает звуковой сигнал, это означает, что карта добавлена в качестве...
главная карта.
- Если индикатор мигает красным и устройство издает звуковой сигнал, это означает, что вам не удалось добавить карту.
Главная карта.



- Добавленные карточки пользователей также можно установить в качестве основной карточки.
- Если пользовательская карта назначена основной, она не сможет открыть дверь.
- Поддерживается только одна основная карта. Если добавлена новая основная карта, будет использоваться старая.
перезаписано.

Шаг 4. Нажмите * для выхода из главного меню.

2.8.2 Удаление основной карты

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 9 и #.

Шаг 3 Проведите картой и нажмите #.

Шаг 4. Нажмите * для выхода из главного меню.

2.8.3 Управление пользовательскими карточками через основную карточку

Если в течение 3 секунд после считывания основной карты не будет выполнено никаких действий, устройство перейдет в основной режим. В режиме карты устройство определит соответствующую функцию в зависимости от количества проведений пальцем по экрану. основной карты. В режиме основной карты индикатор попеременно мигает красным и синим цветом, и если есть

Если в течение 10 секунд не выполняется никаких действий или вы повторно проводите основной картой один раз, она возвращается в исходное положение. статус ожидания.

- Добавление карты пользователя: проведите основной картой один раз, а затем проведите картой пользователя, чтобы добавить ее. Карты пользователей могут добавляться непрерывно.
- Удаление карты пользователя: проведите основной картой дважды, а затем проведите картой пользователя, чтобы удалить ее. Пользователь Карты можно удалять непрерывно.
- Очистить все пользовательские карточки: проведите основной карточкой 5 раз подряд.

2.9 Настройка периода ожидания двери

После активации дверного датчика, если дверь остается открытой по истечении заданного времени, срабатывает звуковой сигнал устройства. поднимет тревогу.

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 10 и #.

Шаг 3 Введите период ожидания открытия двери, а затем нажмите #.

Диапазон значений — от 1 секунды до 9999 секунд. Значение по умолчанию — 60 секунд.

Шаг 4. Нажмите * для выхода из главного меню.

2.10 Восстановление заводских настроек

Процедура

Шаг 1 Нажимать # , Введите пароль администратора, а затем нажмите #.

Войдите в главное меню, и индикатор начнет мигать синим цветом.

Шаг 2 Нажмите 11 и #.

Шаг 3 Восстановите заводские настройки устройства.

- Нажмите 00 и # для восстановления заводских настроек (с сохранением информации о пользователе).
- Нажмите 000 и # для восстановления заводских настроек (восстановления всей информации).

Связанные операции

С помощью кнопки сброса вы можете восстановить заводские настройки устройства.

3. Операции с веб-страницами

На веб-странице вы также можете настроить и обновить устройство.



Настройки веб-браузера различаются в зависимости от модели устройства.

3.1 Инициализация

Инициализируйте устройство при первом входе на веб-страницу или после сброса устройства до заводских настроек.

Предварительные требования

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

Процедура

Шаг 1. Откройте браузер и перейдите по IP-адресу устройства (адрес по умолчанию — 192.168.1.108).



Мы рекомендуем использовать последнюю версию Chrome или Firefox.

Шаг 2. Выберите язык для устройства.

Шаг 3. Установите пароль и адрес электронной почты в соответствии с инструкциями на экране.



- Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа следующих символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' '). ; : &). Установите надежный пароль, следуя подсказкам о его надежности. • Сохраните пароль в безопасном месте после инициализации и регулярно меняйте его для повышения уровня безопасности.

Связанные операции

- В качестве пароля учетной записи администратора можно установить только цифры, если инициализировать ее через... Устройство.
- Вы можете установить цифры, буквы и другие символы в качестве пароля учетной записи администратора. Инициализируйте его через платформу ConfigTool.

После завершения инициализации устройства вы сможете выполнять операции только с самим устройством. Если вам необходимо подключить устройство к сети, используйте ConfigTool или платформу для инициализации устройства.

При использовании ConfigTool или платформы для инициализации устройства после настройки сетевой учетной записи и пароля устройство автоматически завершит инициализацию и перейдет в режим ожидания. Пароль локального администратора преобразуется из сетевого пароля. Если пароль превышает 8 символов, сохраняются только первые 8 символов. Буквы преобразуются в цифры в соответствии со стандартом E.161. Преобразование пароля нечувствительно к регистру, а все остальные символы преобразуются в 0.



- После инициализации, если вы измените сетевой пароль, пароль локального администратора не будет изменен. быть затронуты.
- Если сначала выполнить инициализацию через устройство, а затем через ConfigTool или платформу, пароль локального администратора останется неизменным.

Рисунок 3-1 Е.161 (клавиатура Т9)

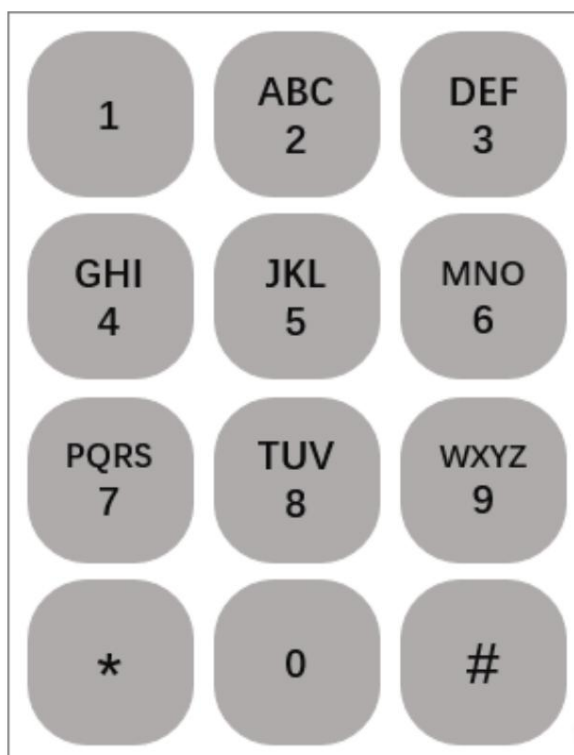


Таблица 3-1. Пример преобразования.

Пароль сети	Пароль локального администратора
ABC12345	22212345
admin123	23646123
admin12!	23646120
admin123456	23646123

3.2 Сброс пароля

Если вы забыли пароль администратора, сбросьте его через указанный адрес электронной почты.

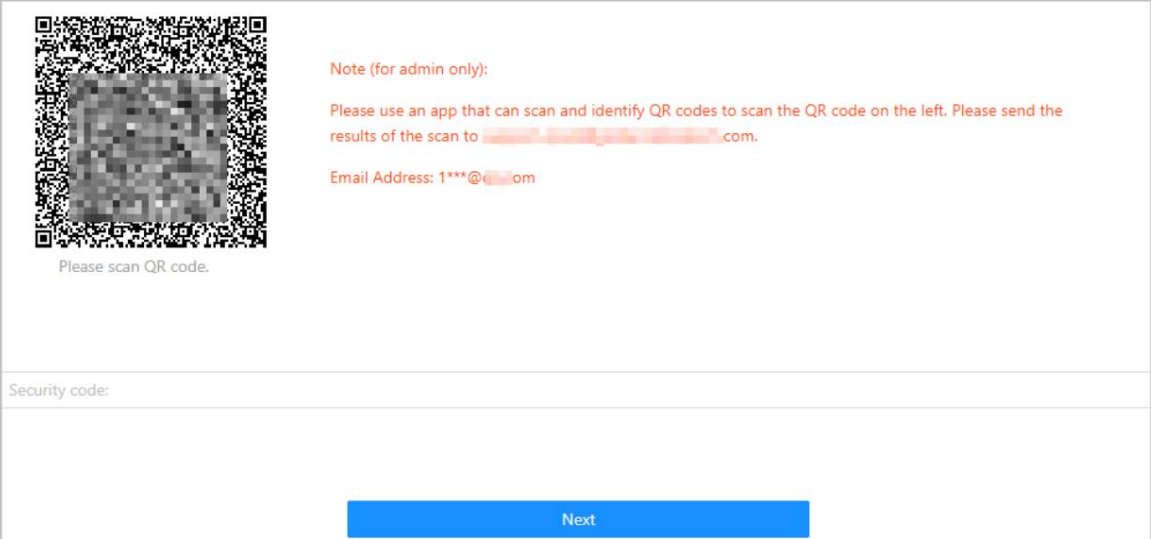
Процедура

Шаг 1. На странице входа нажмите «Забыли пароль».

Шаг 2. Внимательно прочтите подсказку на экране, а затем нажмите ОК.

Шаг 3. Отсканируйте QR-код, и вы получите защитный код.

Рисунок 3-2. Сброс пароля.



Please scan QR code.

Note (for admin only):

Please use an app that can scan and identify QR codes to scan the QR code on the left. Please send the results of the scan to [redacted] com.

Email Address: 1***@[redacted].com

Security code:

Next



- При сканировании одного и того же QR-кода будет сгенерировано до двух защитных кодов. Если защитный код недействителен, обновите QR-код и отсканируйте его снова.
- После сканирования QR-кода вы получите защитный код на связанный с ним адрес электронной почты. Адрес. Используйте защитный код в течение 24 часов после его получения. В противном случае он станет недействительным.
- Если неверный код безопасности будет введен 5 раз подряд, учетная запись администратора будет заблокирована на 5 минут.

Шаг 4. Введите защитный код.

Шаг 5. Нажмите «Далее».

Шаг 6. Сбросьте и подтвердите пароль.



Пароль должен состоять из 8–32 непустых символов и содержать как минимум два из следующих типов символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; : &).

Шаг 7. Нажмите ОК.

3.3 Главная страница

Главная страница отображается после успешного входа в систему.

Рисунок 3-3 Главная страница

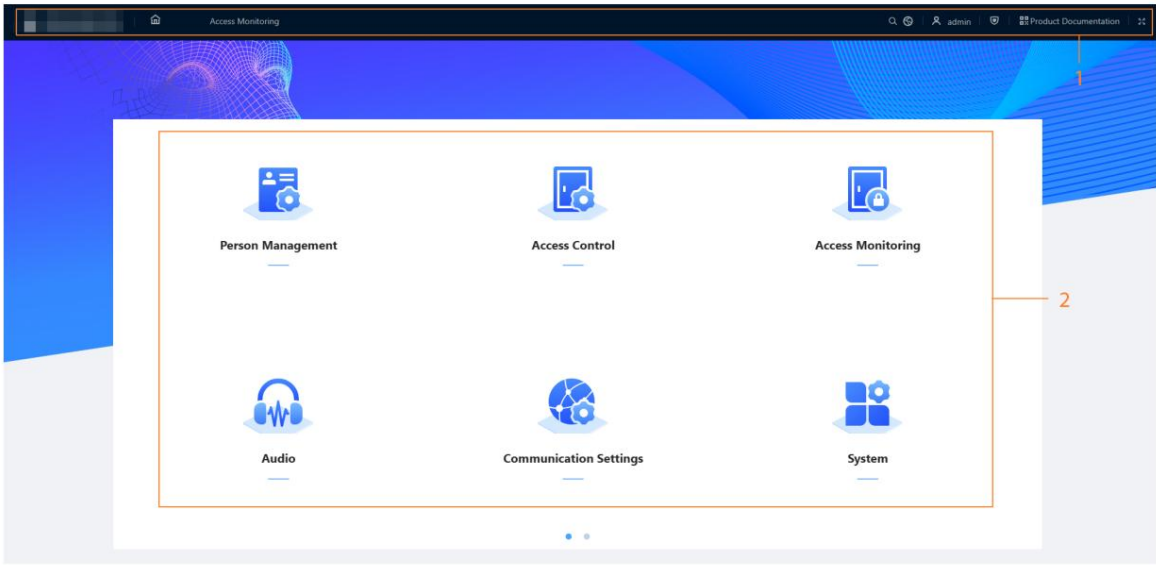


Таблица 3-2. Описание главной страницы

Нет.	Описание
1	• : Перейдите на главную страницу. • Поиск функциональных меню по ключевым словам. • Выберите язык на устройстве. • Выйдите из системы или перезагрузите устройство. • Перейдите на страницу «Безопасность» . • Отсканируйте QR-код, чтобы посмотреть материалы, представленные на упаковке. Эта функция доступна на некоторых моделях. • Отображение в полноэкранном режиме.
2	Главное меню.

3.4 Управление персоналом

Процедура

Шаг 1. На главной странице выберите «Управление персоналом» , а затем нажмите «Добавить».

Шаг 2. Настройка информации о пользователе.

Рисунок 3-4. Добавление пользователей.

Basic Info

* ID

Name

* User Type

General User

▼

* Times Used

Unlimited

* General Plan

255-Default

×

* Holiday Plan

255-Default

×

Email

Validity Period

Forever

▼

Verification Mode

☐ Same as Device

☒ Custom

Combination Meth...

☐ And

☒ Or

* Unlock Method

Card

×

Password

×

Таблица 3-3. Описание параметров.

Параметр	Описание
	Идентификатор может состоять из цифр, букв и их комбинаций, а максимальная длина числа составляет 30 символов.
Имя	Имя может содержать до 32 символов (включая цифры, символы и буквы).
Тип пользователя	• Обычный пользователь : Обычные пользователи могут открыть дверь. • Пользователь из черного списка : Когда пользователи из черного списка открывают дверь, обслуживающий персонал получает уведомление. • Гостевой пользователь : Гости могут открыть дверь в течение определенного времени. В течение определенного периода времени или на определенное количество раз. После истечения определенного периода или окончания времени разблокировки, открыть дверь уже невозможно. • Патрульный пользователь : Патрульные пользователи могут отмечать посещаемость. Устройство, но у них нет прав доступа к двери. • VIP-пользователь : Когда VIP-пользователь открывает дверь, на него не распространяются ограничения режимов разблокировки, таких как «Многокарточный доступ» и «Временной интервал». • Другой пользователь : После разблокировки двери она останется незапертой еще на 5 секунд. • Пользователь 1/Пользователь 2 : Аналогично обычным пользователям.
Электронная почта	Введите адрес электронной почты пользователя.
Количество использований	Установите лимит времени разблокировки для гостевых пользователей. После истечения этого лимита они не смогут открыть дверь.
Генеральный план	В течение установленного периода люди могут открывать дверь или отмечать присутствие.  Вы можете выбрать несколько тарифных планов.

Параметр	Описание
План на отпуск	В дни установленных праздников посетители могут открывать двери или отмечать присутствие.  Вы можете выбрать более одного праздника.
Срок действия	Укажите дату, когда истекает срок действия разрешений на доступ к двери и учет рабочего времени данного лица.
Пароль	Введите пароль пользователя. Максимальная длина пароля — 8 цифр. Пароль принуждения — это пароль разблокировки + 1. Например, если пароль пользователя — 12345, то пароль принуждения будет 12346. В особых случаях, если последняя цифра пароля — 9, например, пароль пользователя — 12349, то пароль принуждения будет 12340. Сигнализация сработает при использовании пароля для разблокировки двери.

Параметр	Описание
Карта	Пользователь может зарегистрировать максимум 5 карт. Введите номер своей карты или проведите картой по устройству или внешнему считывателю карт, после чего устройство считывает информацию о карте. - Введите номер карты вручную. - Нажмите «Добавить». - Введите номер карты, затем нажмите «Добавить». • Номер будет считан автоматически с помощью считывателя регистрации или устройства. - Нажмите , а затем нажмите «Изменить» , чтобы выбрать «Добавить устройство для регистрации» или «Устройство». - Прочитайте карточку. - Для считывания удостоверений личности и идентификационных карт нажмите «Считать карту», а затем проведите картой по считывателю. На экране отображается 60-секундный обратный отсчет, напоминающий о необходимости провести картой, после чего система автоматически считывает номер карты. Если 60-секундный отсчет истек, нажмите кнопку «Считать карту» еще раз, чтобы начать новый отсчет. - Для считывания карты Desfire поместите карту на устройство, а затем нажмите кнопку «Считать карту». Если на карту Desfire уже записан номер карты, он будет считан и отображен здесь. Если карта пуста, то сначала необходимо записать номер карты. Номер карты будет автоматически сгенерирован на компьютере и записан на карту. - Нажмите «Добавить». Вы можете включить функцию «Карта принуждения». Сигнализация сработает, если для разблокировки двери будет использована карта принуждения.  : Установить карту принуждения.  : Изменить номер карты.  Один пользователь может установить только одну принудительную карту.

Параметр	Описание
Отпечаток пальца	Регистрация отпечатков пальцев. Пользователь может зарегистрировать до 3 отпечатков пальцев, и вы можете назначить один из них в качестве отпечатка для вызова помощи. Сигнализация сработает, когда отпечаток пальца будет использован для разблокировки двери. Регистрация отпечатков пальцев осуществляется с помощью считывателя отпечатков или самого устройства. 1. Нажмите  , а затем нажмите «Изменить» , чтобы выбрать «Добавить устройство для регистрации» или «Устройство». 2. Приложите палец к сканеру в соответствии с инструкциями на экране. 3. Нажмите «Добавить».  • Функция распознавания отпечатков пальцев доступна только на некоторых моделях. • Не рекомендуется устанавливать первый отпечаток пальца в качестве принудительных. • Один пользователь может установить только один принудительный отпечаток пальца. • Функция распознавания отпечатков пальцев доступна, если устройство поддерживает подключение модуля распознавания отпечатков пальцев.
Bluetooth-карта	 Функция Bluetooth доступна только на некоторых моделях. Вы можете выбрать вариант «Запрос по электронной почте» или «Запрос с помощью регистрационного кода». • Запрос по электронной почте : Подходит для первого запроса Bluetooth-карты. Вы можете запросить до 5 Bluetooth-карт, используя адрес электронной почты, зарегистрированный в DMSS.  Перед использованием этой функции необходимо ввести зарезервированный адрес электронной почты. 1. Настройте адрес электронной почты, зарегистрированный в DMSS. 2. Нажмите «Запрос по электронной почте», после чего можно будет запросить карты Bluetooth. • Запрос с помощью регистрационного кода : подходит, если у вас уже есть карта Bluetooth, и вы хотите использовать ее на другом контроллере доступа, поддерживающем функцию Bluetooth. 1. Скопируйте код регистрации Bluetooth из ДМС. 2. Нажмите «Запросить с помощью регистрационного кода», а затем введите код. 3. Нажмите ОК.

Шаг 3. Нажмите ОК.

Связанные операции

- Импорт информации о пользователях: Нажмите «Экспорт» , скачайте шаблон и введите в него информацию о пользователях.

Нажмите «Импорт» , чтобы импортировать папку.



За один раз можно импортировать до 10 000 пользователей.

- Очистить: Удалить всех пользователей.

- Обновить: Обновить список пользователей.

- Нажмите  Чтобы отредактировать информацию о

пользователе: • Выберите пользователей, затем нажмите «Удалить» , чтобы удалить их.

- Поиск: поиск по имени пользователя или идентификатору

пользователя. • Нажмите «Записи о картах Bluetooth», чтобы просмотреть записи о картах Bluetooth. Для пользователей, которым не удалось выпустить карты, вы можете перевыпустить карты здесь.



Вы можете выпускать карты партиями на устройствах, поддерживающих функцию Bluetooth.

- Нажмите « Выдать карты всем пользователям » , а затем выберите «Выдать карты выбранным пользователям» или «Выдать карты выбранным пользователям».
- пакетным способом».

- ◇ На вкладке «Доступные для запроса» вы можете просмотреть всех пользователей, которым могут быть выданы Bluetooth-карты, а затем нажать «Запросить по электронной почте» , чтобы выдать Bluetooth-карты партиями.



- Bluetooth-карты можно создавать только партиями по электронной почте. • Облачный сервис должен быть подключен к сети.

- ◇ На вкладке «Не запрашиваемые» вы можете просмотреть пользователей без адреса электронной почты, которым не могут быть выданы карты.

- Нажмите «Экспорт пользователей, у которых отсутствуют адреса электронной почты» , чтобы загрузить список пользователей на локальный компьютер, а затем введите адрес электронной почты.

- Нажмите «Импорт» , чтобы импортировать список пользователей и выдать им карты.

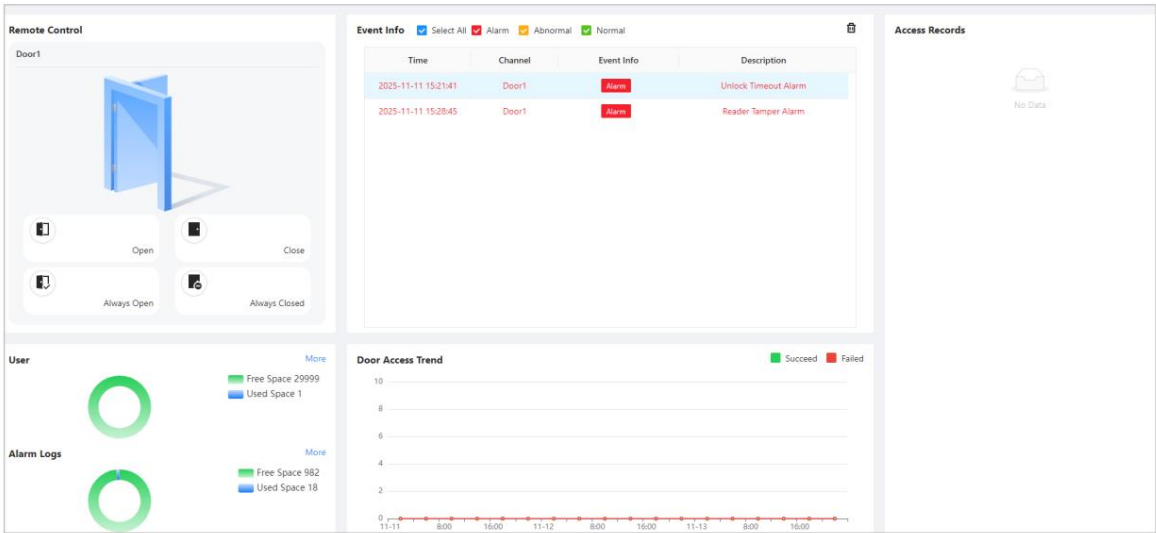
3.5 Мониторинг доступа

Войдите на веб-страницу, и система автоматически перейдет на страницу мониторинга доступа .



- Для первого использования загрузите и установите плагин в соответствии с инструкциями. • Вы также можете щелкнуть значок веб-сервиса в верхнем левом углу, чтобы просмотреть мониторинг доступа.
- страница.

Рисунок 3-5. Мониторинг доступа.



Пульт дистанционного управления

- Нажмите «Открыть» или «Закрыть» рядом с дверью, чтобы дистанционно управлять ею.
- Нажмите «Всегда открыто» или «Всегда закрыто», чтобы дистанционно управлять дверью. Нажмите «Восстановить», чтобы вернуть дверь в нормальное состояние.

Тенденция в сфере доступа к дверям

Отображается динамика доступа за последние 3 дня. Зеленый цвет означает успешный доступ, красный — неудачный.

Доступ к записям

Отображаются записи о доступе в режиме реального времени, включая изображения, информацию о пользователе, метод проверки и время проверки.

Информация о мероприятии

В разделе «Информация о событии» выберите тип события, чтобы просмотреть события. Нажмите  чтобы завершить все события.

Журналы действий пользователей и тревожных сигналов

Просмотрите информацию о помещениях пользователей и журналы аварийных сигналов. Нажмите «Подробнее», чтобы просмотреть подробную информацию.

3.6 Настройка контроля доступа

3.6.1 Настройка параметров контроля доступа

3.6.1.1 Настройка основных параметров

Процедура

Шаг 1. Выберите «Контроль доступа» > «Параметры контроля доступа».

Шаг 2 В разделе «Основные настройки» укажите основные параметры контроля доступа.

Рисунок 3-6. Основные параметры

Basic Settings

Name

Door1

Door Status

☒ Normal ☐ Always Closed ☐ Always Open

Normally Open Period

General Plan Disabled

Holiday Plan Disabled

Normally Closed Period

General Plan Disabled

Holiday Plan Disabled

Verification Interval

0

s (0-180)

Card Swiping Interval

0

s (0-86400)

Public Password

☐

Tamper Reset

☐

Таблица 3-4. Описание основных параметров.

Параметр	Описание
Имя	Название двери.
Состояние двери	Установите статус двери. • Обычный режим: Дверь будет открываться и закрываться в соответствии с вашими настройками. настройки. • Всегда открыта: дверь всегда остается незапертой. • Всегда закрыта: дверь всегда остается запертой.
Обычно открытый период	При выборе режима «Обычный» вы можете выбрать временной шаблон из выпадающего списка. Дверь остается открытой или закрытой в течение заданного времени.
Обычно закрытый период	• Если период открытого состояния конфликтует с периодом закрытого состояния, то период открытого состояния имеет приоритет над периодом закрытого состояния. • Если период совпадает с планами на отпуск, планы на отпуск переносятся на более поздний срок. приоритет над периодами.

Параметр	Описание
Интервал проверки	Если вы подтверждаете свою личность несколько раз в течение определенного периода времени, действительной будет считаться только самая ранняя проверка, и дверь не откроется после второй или последующих проверок. С момента, когда дверь не открывается, вам необходимо дождаться истечения заданного интервала времени проверки, прежде чем пытаться подтвердить свою личность снова.
Интервал считывания карты	При первой проверке с помощью карты вы, как правило, можете открыть дверь или отметить присутствие, и записи будут сгенерированы. В течение заданного периода, если вы повторно проведете картой для проверки, вы не сможете открыть дверь или отметить присутствие, и записи не будут сгенерированы. Пожалуйста, подтвердите свою личность по истечении заданного периода.  Интервал считывания карты имеет приоритет над интервалом проверки.
Открытый пароль	После включения функции публичного пароля настройте пароль. Вы можете использовать публичный пароль для разблокировки двери без ввода идентификатора пользователя. Для одного устройства поддерживается только один публичный пароль.
Сброс защиты от несанкционированного доступа	При включении этой функции можно восстановить заводские настройки с помощью кнопки защиты от взлома на задней панели устройства. Операция сброса настроек после вскрытия: В течение 5 минут после включения устройства нажмите кнопку защиты от вскрытия 5 раз подряд в течение 8 секунд. На экране ожидания устройства отобразится запрос на сброс к заводским настройкам. Нажмите «Подтвердить» или нажмите и удерживайте кнопку защиты от вскрытия в течение 3 секунд или дольше. Устройство перезагрузится. Все настройки и информация будут восстановлены до заводских значений по умолчанию.

Шаг 3. Нажмите «Применить».

3.6.1.2 Настройка методов разблокировки

Для разблокировки двери можно использовать несколько способов, таких как отпечаток пальца, карта и пароль.

Вы также можете комбинировать их, чтобы создать свой собственный способ разблокировки.

Процедура

Шаг 1. Выберите «Контроль доступа» > «Параметры контроля доступа».

Шаг 2. В разделе «Настройки разблокировки» выберите способ разблокировки.

• Разблокировка комбинации

1. Выберите «Разблокировка комбинацией» из списка способов разблокировки.
2. Выберите «Или» или «И».
 - ◇ Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы открыть дверь.
 - ◇ И ещё: используйте все выбранные способы разблокировки, чтобы открыть дверь.
3. Выберите способы разблокировки, а затем настройте остальные параметры.

Рисунок 3-7. Комбинированная разблокировка.

Unlock Settings

Unlock Method: Combination Unlock

Combination Method: ☒ Or ☐ And

Unlock Method (Multi-select): ☒ Card ☒ Password ☒ Bluetooth Card

Bluetooth Mode: ☐ Short-range ☒ Long-range

PIN Code Authentication: ☐

Door Unlocked Duration: s (0.2-600)

Remote Verification: ☒

Remote Verification Unlock Period: General Plan Disabled Holiday Plan Disabled

Apply Refresh Default

Таблица 3-5. Описание настроек разблокировки.

Параметр	Описание
Способ разблокировки (выбор нескольких вариантов)	Способы разблокировки могут различаться в зависимости от модели продукта.
Аутентификация по ПИН-коду	При включенной аутентификации по ПИН-коду вы можете открыть дверь, используя только пароль.
Продолжительность открытия двери	После того, как человеку будет предоставлен доступ, дверь останется открытой в течение определенного времени, чтобы он мог пройти. Это время варьируется от 0,2 до 600 секунд.
Удалённая проверка	Откройте дверь дистанционно. После включения функции выберите общий тарифный план и тарифный план для отдыха.
Режим Bluetooth	Выберите радиус действия Bluetooth. Вы можете выбрать дальний или ближний радиус действия.  Эта функция доступна только для устройств с поддержкой Bluetooth.

• Разблокируется несколькими пользователями.

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

1. В списке «Режим разблокировки» выберите «Разблокировка для нескольких пользователей».
2. Нажмите «Добавить», чтобы добавить группы.
3. Выберите способ разблокировки и пользователей, укажите допустимый номер, а затем нажмите ОК.

- ◇ Вы можете добавить до 4 групп.
- ◇ Методы разблокировки поддерживают только связь «или».

- Указанное число означает количество людей в каждой группе, которым необходимо подтвердить свою личность на устройстве, прежде чем дверь откроется. Например, если для группы установлено число 3, то для открытия двери необходимо, чтобы любые 3 человека из этой группы подтвердили свою личность.

Допустимое число не может превышать количество пользователей в списке пользователей.

Рисунок 3-8 Добавить группу

Add

No.1

Unlock Method ...Card

Valid No.1(1-50)

Select PersonUser ID/Name

	No.	User ID	Name
☒	1	1	
☒	2	1000...	10000002
☐	3	1000...	10000003
☐	4	1000...	10000004
☐	5	1000...	10000005

Selected PeopleClear

>

No.	User ID	Name	Operation
1	1		
2	10000...	10000...	

OK

Cancel

Рисунок 3-9. Разблокировка несколькими пользователями.

Unlock Settings

Unlock Method

Unlock by Multiple Users

You can add up to 4 multi-person unlock groups.

Add

No.	User List	Unlock Method	Valid No.	Operation
No data				

Verification of Multi-person Unlock Timeout Duration

20

s (10-60)

Bluetooth Mode

Short-range

Long-range

PIN Code Authentication

Door Unlocked Duration

3.0

s (0.2-600)

Remote Verification

Remote Verification Unlock Period

General Plan

Disabled

Holiday Plan

Disabled

Apply

Refresh

Default

Таблица 3-6. Описание настроек разблокировки.

Параметр	Описание
Способ разблокировки (выбор нескольких вариантов)	Способы разблокировки могут различаться в зависимости от модели продукта.
Проверка нескольких человек Длительность тайм-аута разблокировки	В процессе проверки интервал между каждыми двумя проверяющими должен находиться в пределах этого временного периода.
Аутентификация по ПИН-коду	Если включена аутентификация по PIN-коду и вы выбираете пароль пользователя для разблокировки, вам нужно ввести только пароль пользователя, без идентификатора пользователя. При включенной аутентификации по PIN-коду удаленная проверка не поддерживается при использовании пароля пользователя для разблокировки.
Продолжительность открытия двери	После того, как человеку будет предоставлен доступ, дверь останется открытой в течение определенного времени, необходимого для прохода. Это время варьируется от 0,2 до 600 секунд.
Удалённая проверка	Если эта функция включена, вы можете управлять дверью на соответствующей платформе.
Режим Bluetooth	Выберите радиус действия Bluetooth. Вы можете выбрать дальний или ближний радиус действия. Эта функция доступна только для устройств с поддержкой Bluetooth.

• Разблокировка по периодам

1. В списке «Способ разблокировки» выберите «Разблокировка по периоду».
2. Перетяните ползунок, чтобы отрегулировать временной период для каждого дня.



Вы также можете нажать кнопку «Копировать», чтобы применить настроенный период времени к другим дням.

3. Выберите способ разблокировки на указанный период времени, а затем настройте остальные параметры.

Рисунок 3-10. Разблокировка по периодам.

Unlock Settings

Unlock Method: Unlock by Period

Time: 00:00:00 - 23:59:59

Combination: ☒ Or ☐ And

Unlock Method: ☒ Card ☒ Password ☐ Bluetooth Card

Bluetooth Mode: ☐ Short-range ☒ Long-range

PIN Code Authentication: ☐

Door Unlocked Duration: 3.0 s (0.2-600)

Шаг 3. Нажмите «Применить».

3.6.2 Сигнализация

3.6.2.1 Настройка сигнализации

Сигнал тревоги сработает при возникновении нештатной ситуации доступа.

Процедура

Шаг 1. Выберите «Контроль доступа» > «Сигнализация» > «Сигнализация».

Шаг 2 (необязательно) Выберите направляющую двери.

Если в настройках связи > Настройки RS-485 на контроллере доступа вы выбрали модуль расширения замка в качестве внешнего устройства, вы можете выбрать канал здесь.

Рисунок 3-11. Выберите канал.

Door Channel: 1

Шаг 3. Настройка параметров сигнализации.

Рисунок 3-12 Сигнализация

Duress Alarm

Anti-passback

Door Detector

NC NO

Intrusion Alarm

Unlock Timeout Alarm

Excessive Attempts Ala...

Buzzer

Enable

Duration

15

s (1-1800)

Link Alarm Output

Enable

Duration

15

s (1-1800)

Tamper Alarm

Buzzer

Enable

Duration

3

s (1-1800)

Link Alarm Output

Enable

Duration

15

s (1-1800)

Apply

Refresh

Default

Таблица 3-7. Описание параметров тревоги.

Параметр	Описание
Сигнал тревоги	Сигнализация сработает при срабатывании карты принудительного вызова. Для разблокировки двери используется пароль или отпечаток пальца принуждения.

Параметр	Описание
Защита от повторного прохода	Пользователи должны подтвердить свою личность как при входе, так и при выходе; в противном случае сработает сигнализация. Это помогает предотвратить передачу карты доступа другому лицу для входа. При включенной функции защиты от повторного прохода владелец карты должен покинуть охраняемую зону через считыватель на выходе, прежде чем система предоставит доступ другому лицу. - Если человек входит после получения разрешения, а выходит без разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен. - Если человек входит без разрешения и выходит после получения разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен.  Если к устройству можно подключить только один замок, проверка на самом устройстве по умолчанию означает направление входа, а проверка на внешнем считывателе карт — направление выхода. Вы можете изменить эту настройку на платформе управления.
Детектор двери	При подключении дверного датчика к вашему устройству сигнализация может срабатывать при ненормальном открытии или закрытии дверей. Существует два типа дверных датчиков: нормально замкнутый (NC) и нормально разомкнутый (NO) датчик. - NC: Датчик находится в закороченном состоянии, когда дверь или Окно закрыто. - NET: Разомкнутая цепь образуется, когда окно или дверь фактически закрыты.
охранная сигнализация	Если дверь открывается ненормально, сработает охранная сигнализация, которая будет гореть в течение определенного времени.  Датчик открытия двери и система охранной сигнализации должны быть включены одновременно.
Сигнализация об истечении времени разблокировки	Если дверь остается незапертой дольше заданного времени, сработает сигнализация об истечении времени ожидания, которая будет действовать в течение заданного времени.
Тайм-аут разблокировки	 Датчик открытия двери и функция автоматического закрытия двери должны быть включены одновременно.
Сигнализация о чрезмерном употреблении	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании неlegalной карты, которая будет гореть в течение определенного времени.
Сигнализация о несанкционированном доступе	Сигнализация о попытке взлома срабатывает при нажатии кнопки обнаружения взлома.

Шаг 4. Нажмите «Применить».

3.6.2.2 (Необязательно) Настройка связи между сигналами тревоги

Вы можете настроить связь между сигналами тревоги.

Процедура

Шаг 1. Выберите «Контроль доступа» > «Сигнализация» > «Настройки связи с сигнализацией».



- Если устройство добавлено в платформу управления, настройки сигнализации будут изменены. синхронизировано с платформой.
- Эта функция доступна только на моделях, имеющих вход и выход для сигнализации. порты.
- Количество входных и выходных портов сигнализации различается в зависимости от модели. продукт.

Шаг 2. Нажмите  для настройки оповещений.

Рисунок 3-13. Связь между сигналами тревоги.

Alarm-in Port	1	Name	Zone1
Alarm Input Type	NO	Link Fire Safety Control	☐
Alarm-out Port	☐		
Duration	30 s (1-300)		
Alarm Output Channel	☒ 1		
Access Control Linkage	☐		
<i>! When the heat alarm signal disappears, the door will automatically return to the normal authentication mode.</i>			
Linkage Mode	Weak Execution		
Channel Type	NO		
OK Cancel			

Шаг 3. Придумайте название для зоны тревоги.

Шаг 4. Включите функцию Link Fire Safety Control и выберите тип устройства ввода сигнала тревоги.

- Нормально замкнутый: Когда сигнализация не сработала, входной сигнал тревоги находится в нормально замкнутом (НЗ) состоянии. Размыкание нормально замкнутой цепи приводит к срабатыванию сигнализации.
- Нормально разомкнутый: Когда сигнализация не сработала, входное устройство сигнализации находится в нормально разомкнутом (НО) состоянии. Замыкание цепи приводит к срабатыванию сигнализации.

Шаг 5 Если вы хотите связать контроль доступа с моментом срабатывания пожарной сигнализации, включите функцию «Связывание контроля доступа».



Эта функция вступает в силу только после включения функции Link Fire Safety Control .

Шаг 6. Выберите режим соединения.

- Надежное исполнение: Когда сигнал пожарной тревоги исчезает, дверь остается в закрытом положении. Текущий статус. При желании вы можете вручную вернуть предыдущий статус двери.
- Недостаточное исполнение: Когда сигнал пожарной тревоги исчезает, дверь автоматически возвращается в предыдущее состояние.

Шаг 7. Выберите тип канала.

- НЕТ: Дверь автоматически открывается при срабатывании пожарной сигнализации.
- НЕТ: Дверь автоматически закрывается при срабатывании пожарной сигнализации.

Шаг 8. Нажмите OK.

3.6.3 Настройки карты

3.6.3.1 Настройка параметров карты



Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройки карты» > «Настройки карты».

Шаг 3. Настройте параметры карты.

Рисунок 3-14. Параметры карты.

Card Settings

M1 Card

M1 Card Encryption & Verification

FeliCa Card

Block NFC Cards

DESFire Card

DESFire Card Decryption

Apply

Refresh

Default

Таблица 3-8. Описание параметров карты.

Элемент	Параметр	Описание
Настройки карты	Карта M1	При включении этой функции карту M1 можно считать. Эта функция доступна только на некоторых моделях.
	Шифрование карты M1 и Проверка	При включении этой функции можно считать только зашифрованную IC-карту. Убедитесь, что карта M1 активирована.
	FeliCa Card	При включении этой функции карту FeliCa можно считать. Эта функция доступна только на некоторых моделях.

Элемент	Параметр	Описание
	Блокировка NFC-карт	После включения этой функции разблокировка с помощью дубликата NFC-карты будет исключена.  - Эта функция доступна только на моделях. - Убедитесь, что карта M1 включена. - Функция NFC доступна только на некоторых моделях телефонов.
	Карта DESFire	При включении этой функции устройство может считывать номер карты Desfire.  - Эта функция доступна только на моделях - Поддерживаются только IC-карты. - Поддерживается только шестнадцатеричный формат.
	Расшифровка карты DESFire	Информация на карте DESFire может быть прочитана, если одновременно включены функции «Включить карту DESFire» и «Расшифровка карты DESFire» .  - Эта функция доступна только на моделях, которые поддерживают IC-карты. - Убедитесь, что карта DESFire включена.
Система номеров карт	Система номеров карт	При подключении считывателя карт Wiegand выберите десятичный или шестнадцатеричный формат для номера карты. Система нумерации карт одинакова как для ввода, так и для вывода номера карты.
DESFire Card Write	Устройство сбора данных	Выберите устройство, поместите карту в считыватель, введите номер карты, а затем нажмите «Записать» , чтобы записать номер карты на карту.  - Необходимо включить функцию карты Desfire и функцию расшифровки карты Desfire. - Поддерживается только шестнадцатеричный формат. • Поддерживается до 8 символов.
	Номер карты	

Шаг 4. Нажмите «Применить».

3.6.3.2 Настройка параметров правил использования карт доступа

Платформа по умолчанию поддерживает 5 типов форматов Wiegand. Вы также можете добавить собственные форматы Wiegand.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройки карт» > «Настройки правил доступа по картам».

Шаг 3. Нажмите «Добавить», а затем настройте новые форматы Wiegand.

Рисунок 3-15. Добавление новых форматов Wiegand.

Add

Wiegand Format

Wiegand88

Total Bits

88

(1-128)

Facility Code

Add

No.	Start Bit	End Bit	Total Bits	Operation
FC	2	33	32	

Card Number

Add

No.	Start Bit	End Bit	Total Bits	Operation
ID0	34	87	54	

Parity Code

Add

Parity Code	Type	Start Bit	End Bit	Total Bits	Operation
1	Odd	2	33	32	
88	Even	34	87	54	

OK

Cancel

Таблица 3-9. Описание формата Wiegand.

Параметр	Описание
Формат Виганда	Название формата Wiegand.
Всего бит	Введите общее количество битов.
Код объекта	Нажмите кнопку «Добавить», а затем введите начальный и конечный биты кода объекта.
Номер карты	Нажмите кнопку «Добавить», а затем введите начальный и конечный биты номера карты.
Код четности	1. Нажмите «Добавить». 2. Введите бит начала и бит конца четности. 3. Введите бит начала и бит конца нечетной четности.

Шаг 4. Нажмите ОК.

Связанные операции

- Вы также можете нажать «Добавить протокол» , чтобы импортировать файл Wiegand на платформу.
- Код учреждения: Если эта функция включена, и на странице «Управление персоналом» для системы номеров карт установлен десятичный формат , код учреждения и номер карты преобразуются в десятичный формат отдельно, а затем объединяются.
- HID26: Если функция включена:
 - ◇ Поддерживается только Wiegand 26.
 - ◇ Платформа поддерживает отображение данных карты только в десятичном формате.

- ◆ Номер карты должен состоять из 5 символов, а код объекта — не более чем из 3 символов. При ручном вводе номера карты система автоматически добавляет ведущие нули к фиксированной длине числа. Например, если введенный номер карты короче 5 символов, например, 56, к нему добавляется ведущий ноль, чтобы зафиксировать длину числа в 5 символов, например, 00056, и еще один ноль, который служит кодом объекта. Таким образом, окончательный номер карты будет 000056.

3.6.3.3 Настройка пользовательской конверсии

При считывании карт сторонних производителей с помощью встроенного считывателя устройства, внешнего считывателя карт RS-485 или внешнего считывателя карт Wiegand, если фактический номер карты не совпадает ни с одним номером карты в системе, можно настроить пользовательское преобразование номера карты, чтобы гарантировать, что преобразованный номер карты будет соответствовать номеру карты в системе.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройки карты» > «Пользовательская конверсия».

Шаг 3. Включите функцию преобразования, а затем выберите режим сопоставления.

- Автоматическое сопоставление: Используйте встроенное правило преобразования устройства для конвертации номера карты.

1. Выберите тип ввода.
 - ◆ Ввод с устройства: проведите картой по устройству, чтобы считать карту.
 - ◆ Вход RS-485: Проведите картой по подключенному считывателю карт RS-485, чтобы считать карту.
 - ◆ Ввод Wiegand: Проведите картой по подключенному считывателю карт Wiegand, чтобы считать карту.
2. Считайте номер карты через устройство или введите номер карты до конвертации, а затем введите номер карты после конвертации.
3. Нажмите «Автоматический поиск».
 - ◆ Если номера карт успешно совпали, вы можете нажать кнопку «Экспорт», чтобы экспортировать правило и импортировать его на другое устройство для быстрого переключения правил сопоставления.
 - ◆ Если номера карт не совпадают, это означает, что в системе отсутствует правило сопоставления. Вам необходимо настроить скрипт правила сопоставления и выбрать «Импорт правила преобразования», чтобы импортировать правило на устройство.
 - ◆ Если вам необходимо изменить правило сопоставления, нажмите «Изменить правило сопоставления».

Рисунок 3-16. Автоматическое сопоставление (сопоставление успешно выполнено).

Enable ☒

Matching Mode ☒ Auto Match ☐ Import Conversion Rule

Status ☒ Applied ☐ Default

* Input Type ☒ Device Input ☒ RS-485 Input ☒ Wiegand Input

No.	Card No. Before Conversion (Device Input)	Card No. Before Conversion (RS-485 Input)	Card No. Before Conversion (Wiegand Input)	Card No. After Conversion
1	1A283C4D	1A283C4D	1A283C4D	4D3C281A
2				
3				

Successfully Matched

This rule will automatically apply to this device.

Change Matching Rule

Export

- Импорт правила преобразования: Импортируйте другие правила для преобразования номера карты.

Нажмите «Загрузить файл», , Выберите файл с правилами, а затем нажмите «Открыть».

Рисунок 3-17. Правило конвертации импорта.

The screenshot shows a configuration window for an import conversion rule. At the top, there is a toggle switch labeled 'Enable' which is currently turned on. Below this, there is a section for 'Matching Mode' with two radio buttons: 'Auto Match' and 'Import Conversion Rule', with the latter being selected. Underneath, there is a 'Version' field displaying '2025-03-31' and two buttons: 'Upload File' and 'Default'. At the bottom, a light blue box contains a warning message: 'You can only upload files in zip format and the size must not exceed 1 MB.'

3.6.4 Настройка периодов

Настройте общие планы и планы на случай праздников, а затем определите, когда пользователь имеет право открывать двери.

3.6.4.1 Настройка общего плана

Вы можете настроить до 128 периодов (от №0 до №127) общих планов. В каждом периоде необходимо настроить расписание доступа к дверям на целую неделю. Люди могут открыть дверь только в запланированное время.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройка периода» > «Общий план».

Шаг 3. Нажмите «Добавить».

1. Укажите номер тарифного плана и название тарифного плана.
2. Перетащите ползунок времени, чтобы настроить время для каждого дня.
3. (Необязательно) Нажмите «Копировать» , чтобы скопировать конфигурацию на остальные дни.

Рисунок 3-18. Настройка общего плана.

Add [X]

No.

General Plan Name

Time Plan

Time - [OK] [Delete]

	0	1	2	3	4	5	6	7	8	9	10	11	
Sun													Copy
Mon													Copy
Tue													Copy
Wed													Copy
Thu													Copy
Fri													Copy
Sat													Copy

[OK] [Cancel]

Шаг 4. Нажмите OK.

3.6.4.2 Настройка плана отпусков

Вы можете настроить до 128 групп праздников (от №0 до №127), и в каждую группу праздников можно добавить до 16 праздников. После этого вы можете назначить настроенные группы праздников плану праздников. Пользователи могут открывать дверь только в течение времени, указанного в плане праздников.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройка периода» > «План отпусков».

Шаг 3. Нажмите «Управление праздниками», а затем нажмите «Добавить».

1. Выберите номер для группы праздников, а затем введите название группы.

Рисунок 3-19. Добавить группу праздников.

Add

No.

Holiday Group Name

Holiday Group Config

No.	Holiday Name	Start Time	End Time	Operation
1	National Day	2023-10-01	2023-10-07	

2. Нажмите «Добавить», , Добавьте праздник в группу праздников, а затем нажмите OK.

Рисунок 3-20. Добавление праздника в группу праздников.

Edit

Holiday Name

* Period →

Шаг 4. Нажмите OK.

Шаг 5. Нажмите «Управление планами», а затем нажмите «Добавить».

1. Выберите номер для плана отдыха, а затем введите для него название.
2. Выберите группу праздников, а затем перетащите ползунок, чтобы настроить время для каждого дня.

Поддерживается добавление до 4 временных интервалов в день.

Рисунок 3-21. Добавить план отпуска.

Edit

No.

Holiday Plan Name

Holiday Group No.

Time Plan

Time -

OK Delete

0 1 2 3 4 5 6 7 8 24

Holid Copy

OK Cancel

Шаг 6. Нажмите OK.

3.6.5 Настройка QR-кода

Процедура

Шаг 1. На веб-странице выберите «Контроль доступа» > «QR-код».

Шаг 2. Настройте режим подсветки и срок действия QR-кода, а затем нажмите «Применить».

- Всегда включено: Подсветка всегда включена.
- Закрыто: Подсветка закрыта.
- Автоматическое определение: подсветка загорается при обнаружении объекта и выключается после сканирования прошло успешно. Автоматическое определение выбрано по умолчанию.

Рисунок 3-22. Настройка осветителя.

Illuminator Mode

QR Code Validity Period (sec) (0-86400)

Apply Refresh Default

3.6.6 Настройка сравнения на бэкэнде

Перед настройкой убедитесь, что устройство подключено к сторонней платформе через SDK. Вы можете напрямую передавать данные, такие как QR-код или номер карты, на стороннюю платформу для проверки данных, вместо проверки данных на самом устройстве.

Процедура

- Шаг 1. Войдите на веб-страницу устройства.
- Шаг 2. Выберите «Контроль доступа» > «Сравнение внутренних систем».

Рисунок 3-23. Сравнение бэкэндов.

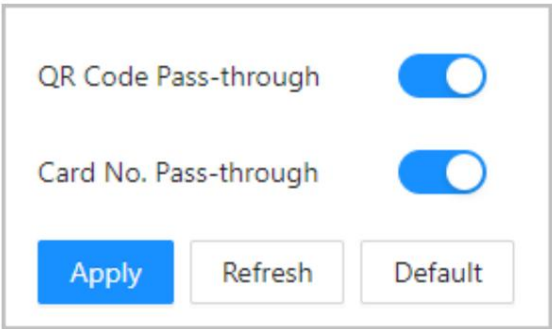


Таблица 3-10. Сравнение бэкэндов.

Параметры	Описание
Пропуск QR-кода	После активации отсканированный QR-код передается на стороннюю платформу для проверки данных.
Номер карты. Передача данных.	После активации номер карты передается на стороннюю платформу для проверки данных.

3.6.7 Настройка функций порта

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

Справочная информация



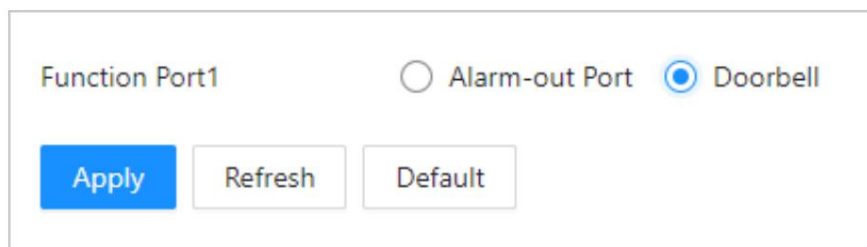
- Эта функция доступна только на некоторых моделях. •
- Расположение портов может отличаться в зависимости от модели изделия.

Процедура

- Шаг 1. На веб-странице выберите «Контроль доступа» > «Настройка портов».
- Шаг 2. Выберите тип порта.

По умолчанию это дверной звонок .
- Шаг 3. Нажмите «Применить».

Рисунок 3-24. Настройка портов.



3.6.8 Настройка разблокировки паролем

При включении аутентификации по PIN-коду пользователи могут открыть дверь, просто введя пароль.

Справочная информация



- Если аутентификация по PIN-коду не включена, вы можете разблокировать дверь, введя код разблокировки. Пароль в формате идентификатор пользователя#пароль#. Например, если идентификатор пользователя — 123, то установленный вами пароль — 12345, и затем для разблокировки двери необходимо ввести 123#12345#.
- Если включена аутентификация по PIN-коду, вы можете разблокировать дверь, введя пароль разблокировки в формате пароль#. Например, если идентификатор пользователя — 123, а установленный вами пароль — 12345, то для разблокировки двери необходимо ввести 12345#.

Процедура

Шаг 1. На главной странице выберите «Контроль доступа» > «Настройка метода разблокировки».

Шаг 2. Включите аутентификацию по PIN-коду. , а затем нажмите «Применить».



Включение аутентификации по PIN-коду сопряжено с определенными рисками для безопасности. При ее включении типы пользователей и роли становятся недействительными, и возникают следующие ситуации.

- Владелец первой карты и пользователи в группах разблокировки для нескольких человек должны подтвердить свою личность с помощью определенных методов разблокировки, за исключением пароля. Если они подтвердят свою личность с помощью пароля, функция разблокировки первой карты или разблокировки для нескольких человек станет неэффективной.
- Пользователям необходимо подтвердить свою личность с помощью определенных методов разблокировки, за исключением пароля. Если доступ будет получен через пароль, функция защиты от повторного ввода пароля станет неэффективной.
- Пользователи патрульной службы и пользователи из заблокированных списков могут просто ввести свой пароль для разблокировки двери. • Заблокированные и просроченные учетные записи по-прежнему могут разблокировать двери, просто введя свой пароль. • При одновременном отключении метода разблокировки по паролю все типы пользователей могут разблокировать дверь. Не могут открыть дверь, используя свой пароль.

3.6.9 Настройка разблокировки режима от первого лица

Доступ к дверям возможен только после того, как через них пройдут указанные вами лица. Если указано несколько лиц, доступ к дверям возможен после того, как через них пройдет любое из указанных лиц.

Предварительные требования

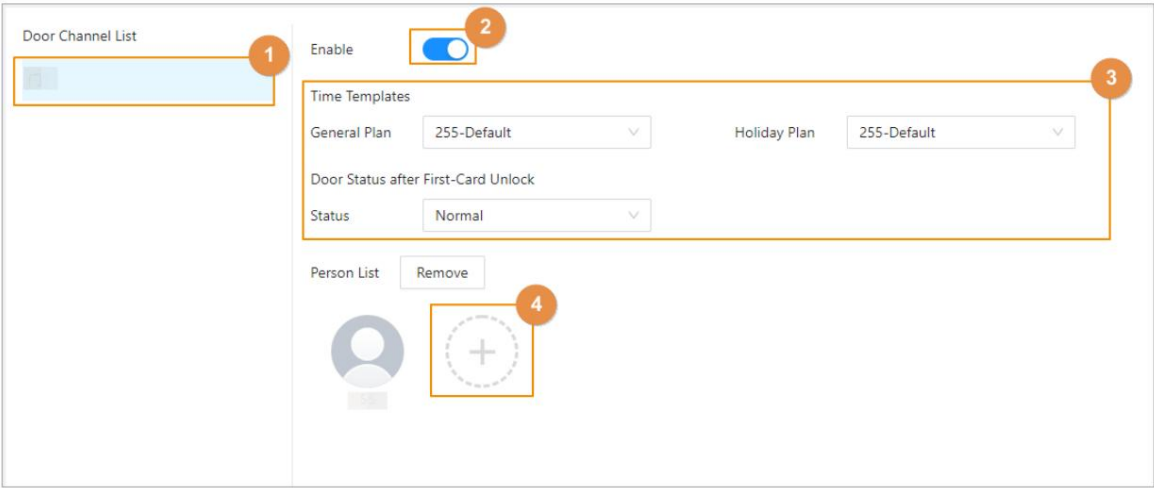
Персонажей можно назначать в качестве персонажей от первого лица только в том случае, если у них есть права доступа к дверям.

Процедура

Шаг 1. На главной странице выберите «Контроль доступа» > «Разблокировка от первого лица».

Шаг 2. Выберите дверной канал, а затем активируйте функцию.

Рисунок 3-25. Разблокировка от первого лица.



Шаг 3. Настройте параметры.

Таблица 3-11. Описание параметров.

Параметр	Описание
Временные шаблоны	Выберите период действия этого правила.
Состояние двери после первой карты Разблокировать	- Обычный режим : Другие лица должны подтвердить свою личность. проходить. - Круглосуточно открыто : любой желающий может пройти без проверки документов, удостоверяющих личность.
Список лиц	Нажмите кнопку «+» , чтобы выбрать одного или нескольких человек, и они получат доступ к дверям.

Шаг 4. Нажмите «Применить».

3.6.10 Настройка защиты от повторной передачи

Пользователи должны подтвердить свою личность как при входе, так и при выходе; в противном случае сработает сигнализация о невозможности повторной передачи карты. Это предотвращает передачу карты доступа другому лицу для обеспечения доступа. При включении функции предотвращения повторной передачи карты владелец карты должен покинуть охраняемую зону, прежде чем система предоставит доступ другому лицу.

- Если человек входит после получения разрешения и выходит без разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен.
- Если человек входит без разрешения и выходит после получения разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен.



- Если вы настроили защиту от повторного прохода для подконтроллеров через главный контроллер, и Если вы планируете восстановить заводские настройки основного контроллера, мы рекомендуем одновременно восстановить заводские настройки и дополнительного контроллера.

- Если правило предотвращения повторного прохода используется при нестабильной сети, дверь может открыться после Подтверждение личности пройдено, но на считывателе карт может сработать предупреждение о превышении времени ожидания. Пожалуйста, убедитесь в стабильности вашей сети.

Процедура

Шаг 1. На главной странице выберите «Контроль доступа» > «Настройка групп защиты от повторного прохода».

Шаг 2. Включите эту функцию, а затем настройте время сброса.

Укажите время, когда будет сброшен статус защиты от повторного прохода для всего персонала.

Шаг 3. Выберите общий план и план отдыха.

Система предотвращения повторного прохода действует в течение установленного времени.

Шаг 4. В группе устройств нажмите «Добавить», а затем выберите устройство для чтения карт.

Шаг 5 В группе выхода нажмите «Добавить», а затем выберите устройство чтения карт.

Рисунок 3-26. Защита от обратного прохода.

Enable ☒

Reset Time min (5-300)

Time Templates

General Plan Holiday Plan

Anti-passback Group Config [?]

Entry Group

/Reader 1
[Remove](#)

Exit Group

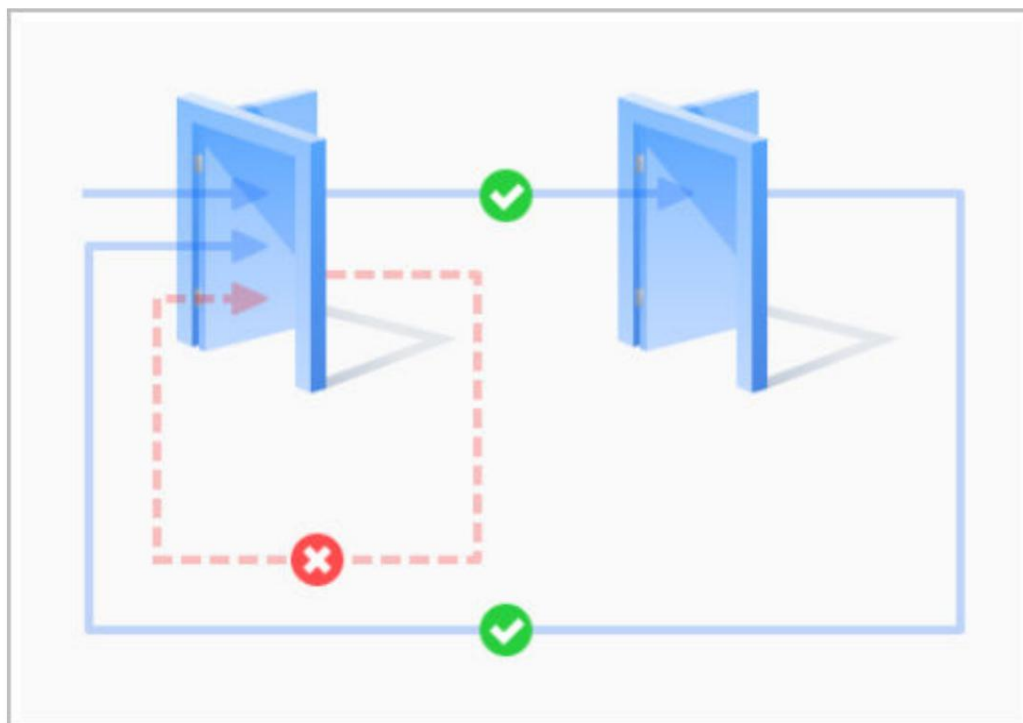
/Reader 2
[Remove](#)

Шаг 6. Нажмите «Применить».

Результаты

Номер группы указывает последовательность считывания карт. Карты необходимо использовать в соответствии с определенной последовательностью групп. Например, в группе входа необходимо провести карту через считыватель, а затем через считыватель в группе выхода. Пока вы проводите карту в соответствии с установленной последовательностью, система работает корректно.

Рисунок 3-27. Функция защиты от повторного прохода.



3.7 Настройка звука

Процедура

Шаг 1. Войдите на веб-страницу устройства.

Шаг 2. Выберите аудио.

Шаг 3. Включите звук нажатия клавиш или режим «Не беспокоить» в зависимости от ваших потребностей.

Рисунок 3-28 Аудио

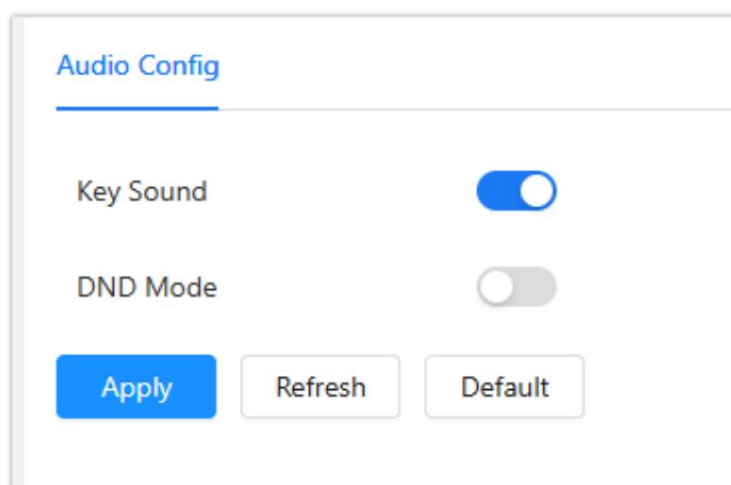


Таблица 3-12. Описание параметров звука.

Параметры	Описание
Ключевой звук	При включении этой функции устройства с сенсорным экраном будут издавать звуковой сигнал при локальных сенсорных операциях, а устройства без сенсорного экрана — при операциях с клавишами/кнопками.
Режим «Не беспокоить»	При включении этой функции в течение заданных периодов времени не будут воспроизводиться звуковые сигналы для локальной проверки (например, доступа к двери или учета присутствия). Поддерживает до 4 временных периодов.

Шаг 4. Нажмите «Применить».

3.8 Настройки связи

3.8.1 Сетевые настройки

3.8.1.1 Настройка TCP/IP

Необходимо настроить IP-адрес устройства, чтобы обеспечить его связь с другими устройствами.

Процедура

Шаг 1. Выберите «Настройки связи» > «Настройки сети» > «TCP/IP».

Шаг 2. Настройте параметры.

Рисунок 3-29 TCP/IP

NIC

NIC 1

Mode

DHCP

Static

MAC Address

IP Version

IPv4

IP Address

Subnet Mask

Default Gateway

Preferred DNS

Alternate DNS

MTU

1500

Apply

Refresh

Default

Таблица 3-13. Описание TCP/IP.

Параметр	Описание
Режим	• Статический режим: Введите IP-адрес, маску подсети и шлюз вручную. • DHCP: расшифровывается как Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста). При включении DHCP устройство будет автоматически Назначается с указанием IP-адреса, маски подсети и шлюза.
MAC-адрес	MAC-адрес устройства.
IP-версия	IPv4 или IPv6.

Параметр	Описание
IP-адрес	Если вы установите режим «Статический», настройте IP-адрес, маску подсети и шлюз.
Маска подсети	
Шлюз по умолчанию	 - IPv6-адрес представляется в шестнадцатеричном формате. - Версия IPv6 не требует установки масок подсети. - IP-адрес и шлюз по умолчанию должны совпадать. - сегмент сети.
Предпочитаемый DNS	Укажите IP-адрес предпочтительного DNS-сервера.
Альтернативный DNS	Укажите IP-адрес альтернативного DNS-сервера.
MTU	MTU (Maximum Transmission Unit) — это максимальный размер данных, который может быть передан в одном сетевом пакете в компьютерных сетях. Более высокое значение MTU может повысить эффективность передачи данных по сети за счет уменьшения количества пакетов и связанных с этим сетевых накладных расходов. Если устройство на пути следования по сети не может обрабатывать пакеты определенного размера, это может привести к фрагментации пакетов или ошибкам передачи. В сетях Ethernet обычно используется значение MTU 1500 байт. Однако в некоторых случаях, например, при использовании PPPoE или VPN, могут потребоваться меньшие значения MTU для соответствия требованиям конкретных сетевых протоколов или служб. Ниже приведены рекомендуемые значения MTU для справки: 1500: Максимальное значение для пакетов Ethernet, также является значением 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.

Шаг 3. Нажмите «Применить».

3.8.1.2 Настройка Wi-Fi



- Функция Wi-Fi доступна на некоторых моделях.
- Wi-Fi и точка доступа Wi-Fi не могут быть включены одновременно.

Процедура

Шаг 1. Выберите «Настройки связи» > «Настройки сети» > «Wi-Fi».

Шаг 2. Включите Wi-Fi.

Отображаются все доступные сети Wi-Fi.

Рисунок 3-30 Wi-Fi



- Одновременное включение Wi-Fi и точек доступа Wi-Fi невозможно.
- Функция Wi-Fi доступна только в некоторых моделях.

Шаг 3. Нажмите кнопку «+», а затем введите пароль от сети Wi-Fi.

Wi-Fi подключен.

Связанные операции

- DHCP: Включите эту функцию и нажмите «Применить». Устройство автоматически будет назначена сеть Wi-Fi. адрес.
- Статический режим: Включите эту функцию, вручную введите Wi-Fi-адрес, затем нажмите «Применить», и устройство подключится к Wi-Fi.

3.8.1.3 Настройка точки доступа Wi-Fi



- Функция Wi-Fi доступна в некоторых моделях.
- Wi-Fi и точка доступа Wi-Fi не могут быть включены одновременно.

Процедура

Шаг 1. Выберите «Настройки связи» > «Настройки сети» > «Точка доступа Wi-Fi».

Шаг 2. Включите функцию, а затем нажмите «Применить».

Рисунок 3-31 Точка доступа Wi-Fi

The image shows a configuration window for a Wi-Fi access point. At the top, there is a toggle switch labeled 'Enable' which is currently turned off. Below it are three input fields: 'SSID' with a blurred text entry, 'Security' with a dropdown menu showing 'None', and 'IP Address' with a blurred IP address. A large QR code is displayed in the center of the window. At the bottom, there are three buttons: 'Apply' (blue), 'Refresh' (white), and 'Default' (white).

Результаты

После включения этой функции вы сможете подключиться к Wi-Fi устройства через свой телефон и войти на веб-страницу устройства на своем телефоне.

3.8.1.4 Настройка порта

Вы можете одновременно ограничить доступ к устройству через веб-страницу, настольный клиент и мобильный клиент.

Процедура

Шаг 1. Выберите «Настройки связи» > «Настройки сети» > «Порт».

Шаг 2. Настройте порты.

Рисунок 3-32. Настройка портов.

Max Connection

50

(1-50)

TCP Port

37777

(1025-65535)

HTTP Port

80

HTTPS Port

443

Apply

Refresh

Default



Для вступления в силу настроек после их установки необходимо перезагрузить устройство.

Таблица 3-14. Описание портов.

Параметр	Описание
Максимальное соединение	Вы можете установить максимальное количество клиентов (например, веб-страниц, настольных компьютеров и мобильных устройств), которые могут одновременно получать доступ к устройству.
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.
Порт HTTPS	Значение по умолчанию — 443.

Шаг 3. Нажмите «Применить».

3.8.1.5 Настройка базового сервиса

Для подключения устройства к сторонней платформе включите функции CGI и ONVIF.

Процедура

Шаг 1. Выберите «Настройки связи» > «Сетевые настройки» > «Основные службы».

Шаг 2. Настройка базовой службы.

Рисунок 3-33. Базовое обслуживание.

SSH

Multicast/Broadcast Search

CGI

ONVIF

Emergency Maintenance

For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.

Private Protocol Authentication Mode

Security Mode (Recommended)

Private Protocol

*Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.

TLSv1.1

LLDP

Apply

Refresh

Default

Таблица 3-15. Описание основных параметров обслуживания.

Параметр	Описание
SSH	SSH, или протокол Secure Shell, — это протокол удалённого администрирования, позволяющий пользователям получать доступ к удалённым серверам, управлять ими и изменять их через Интернет.
Поиск по многоканальной/широковещательной рассылке	Поиск устройств с использованием многоадресного или широковещательного протокола.
CGI	Общий интерфейс шлюза (CGI) представляет собой точку пересечения между веб-серверами, через которую возможен стандартизированный обмен данными между внешними приложениями и серверами.
ОНВИФ	ONVIF расшифровывается как Open Network Video Interface Forum (Форум открытых сетевых видеоинтерфейсов). Его цель — обеспечить стандарт для взаимодействия между различными IP-устройствами безопасности. Эти стандартизированные спецификации ONVIF представляют собой своего рода общий язык, который все устройства могут использовать для обмена данными.
Аварийное техническое обслуживание	Она включена по умолчанию.
Аутентификация по частному протоколу Режим	Установите режим аутентификации, включая безопасный режим и режим совместимости. Рекомендуется выбрать режим безопасности. • Режим безопасности (рекомендуемый): не поддерживает доступ к устройству с использованием методов аутентификации Digest, DES и открытого текста, что повышает безопасность устройства. • Совместимый режим: поддерживает доступ к устройству с использованием методов аутентификации Digest, DES и открытого текста, но с пониженным уровнем безопасности.
Частный протокол	Платформа добавляет устройства по частному протоколу.

Параметр	Описание
TLSv1.1	TLSv1.1 означает Transport Layer Security версии 1.1. TLS — это криптографический протокол, предназначенный для обеспечения безопасной и аутентифицированной связи в компьютерной сети.  При включении протокола TLSv1.1 могут возникнуть риски безопасности. Просим принять это к сведению.
ЛЛДП	LLDP — это аббревиатура от Link Layer Discovery Protocol (протокол обнаружения канального уровня), протокола канального уровня. Он позволяет сетевым устройствам, таким как коммутаторы, маршрутизаторы или серверы, обмениваться информацией о своих идентификационных данных и возможностях друг с другом. Протокол LLDP помогает сетевым администраторам лучше понимать топологию сети и предоставляет стандартизированный способ автоматизации обнаружения и сопоставления соединений между сетевыми устройствами. Это упрощает настройку сети, устранение неполадок и оптимизацию производительности.

Шаг 3. Нажмите «Применить».

3.8.1.6 Настройка облачного сервиса

Облачный сервис предоставляет услугу NAT-проникновения. 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 «Настройки связи» > «Настройки сети» > «Облако».

Услуга.

Шаг 2. Включите функцию облачного сервиса.

Облачный сервис становится доступным, если P2P-сети и PaaS-платформы подключены к сети.

Рисунок 3-34. Облачный сервис.



Enable ☒

After the function is enabled and the device connects to the network, we will collect device information such as the IP address, MAC address, device name and serial number. The collected information will only be used to remotely access the device. If you do not want to enable this function, please clear the selection from the check box.

P2P Status ● Offline

PaaS Status ● Offline

SN 8[redacted]759



Шаг 3. Нажмите «Применить».

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

3.8.1.7 Настройка автоматической регистрации SDK

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

Справочная информация



Автоматическая регистрация поддерживает только SDK.

Процедура

Шаг 1. На главной странице выберите «Настройки связи» > «Сетевые настройки» > «Авто».

Регистрация > Автоматическая регистрация SDK.

Шаг 2. Включите функцию автоматической регистрации и настройте параметры.

Рисунок 3-35. Регистрация автомобиля.

Enable

Status

Offline

Server Address

172.52.2.7

Port

7000

(1-65535)

Registration ID

none

Apply

Refresh

Default

Таблица 3-16. Описание автоматической регистрации.

Параметр	Описание
Статус	Отображает статус подключения автоматической регистрации.
Адрес сервера	IP-адрес или доменное имя сервера.
Порт	Порт сервера, используемого для автоматической регистрации.
Идентификатор регистрации	Идентификатор регистрации устройства (определяется пользователем). Вы можете добавить... Для подключения устройства к платформе управления необходимо войти на платформу.

Шаг 3. Нажмите «Применить».

3.8.1.8 Настройка автоматической регистрации CGI

Подключитесь к сторонней платформе через протокол CGI.

Справочная информация



Поддерживается только IPv4.

Процедура

Шаг 1. На главной странице выберите «Настройки связи» > «Сетевые настройки» > «Авто».

Регистрация > Автоматическая регистрация CGI.

Шаг 2. Включите эту функцию, а затем нажмите



для настройки параметров.

Таблица 3-17. Описание автоматической регистрации.

Параметр	Описание
Идентификатор устройства	Поддерживает до 32 байт, включая китайские иероглифы, цифры, буквы и специальные символы.
Тип адреса	Поддерживаются 2 способа регистрации. • IP-адрес хоста: Введите IP-адрес сторонней платформы. • Доменное имя: Введите доменное имя сторонней платформы.
IP-адрес хоста	
Доменное имя	
HTTPS	Доступ к сторонней платформе осуществляется через HTTPS. HTTPS обеспечивает безопасность передачи данных по компьютерной сети.

Шаг 3. Нажмите ОК.

3.8.1.9 Настройка автоматической загрузки

Отправляйте информацию о пользователях и разблокируйте записи через платформу управления.

Процедура

Шаг 1. На главной странице выберите «Настройки связи» > «Сетевые настройки» > «Авто». Загрузить.

Шаг 2 (необязательно) Включите отправку информации о пользователе.

При обновлении информации о пользователе или добавлении новых пользователей устройство автоматически передаст информацию о пользователе на платформу управления.

Шаг 3. Включите режим загрузки по протоколу HTTP.

Шаг 4. Нажмите «Добавить», а затем настройте параметры.

Рисунок 3-36 Автоматическая загрузка



Таблица 3-18. Описание параметров.

Параметр	Описание
IP-адрес/доменное имя	IP-адрес или доменное имя платформы управления.
Порт	Порт платформы управления.
HTTPS	Доступ к платформе управления осуществляется через HTTPS. HTTPS обеспечивает безопасность связи в компьютерной сети.
Аутентификация	Включите аутентификацию учетной записи при доступе к платформе управления. Для входа потребуется имя пользователя и пароль.

Параметр	Описание
Тип события	Выберите тип события, которое будет отправлено на платформу управления.  • Перед использованием этой функции включите функцию «Отправка информации о человеке». • Информация о человеке может быть отправлена только одному человеку. Платформа управления и записи о разблокировке могут передаваться на несколько платформ управления.

Шаг 5. Нажмите «Применить».

3.8.2 Настройки режима

Войдите в веб-браузер и выберите «Настройки связи» > «Настройки режима».

Режим считывания карт

Выберите режим «Считыватель карт». Устройство служит в качестве считывателя карт, подключенного к контроллеру контроля доступа извне. Оно не выполняет аутентификацию, а напрямую передает информацию о контроле доступа (например, карту, пароль, отпечаток пальца) на контроллер контроля доступа, который затем выполняет аутентификацию и открывает дверь.

Рисунок 3-37 Режим считывания карт

Mode

☒ Card Reader ☐ Access Controller

RS-485 Settings

Baud Rate

9600

▼

Data Bit

8

▼

Stop Bit

1

▼

Parity Code

None

▼

Wiegand Settings

Wiegand Output Type

Wiegand 34

▼

Pulse Width (µs)

200

(20-200)

Pulse Interval (µs)

1000

(200-5000)

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Apply

Refresh

Default

Режим контроллера доступа

Установите режим «Контроллер доступа».

Рисунок 3-38 Режим контроллера доступа

Mode

☐ Card Reader ☒ Access Controller

RS-485 Settings

External Device

Card Reader

?

Baud Rate

9600

Data Bit

8

Stop Bit

1

Parity Code

None

Wiegand Settings

Wiegand Settings

☒ Wiegand Input ☐ Wiegand Output

Card No. Inversion

☒

Apply

Refresh

Default

Таблица 3-19. Описание RS-485.

Внешнее устройство	Описание
Контроллер доступа	Выберите «Контроллер доступа», если устройство функционирует как считыватель карт и отправляет данные другим внешним контроллерам доступа для управления доступом. Тип выходных данных: • Номер карты: Выводит данные на основе номера карты, когда пользователь проводит картой для разблокировки двери; выводит данные на основе первого номера карты пользователя при использовании других способов разблокировки. • ID: Выводит данные на основе ID пользователя.  • В случае успешной аутентификации соответствующая информация передается контроллеру доступа. В этом случае отображаемый результат аутентификации соответствует результату аутентификации контроллера доступа. • При сбое аутентификации соответствующая информация не передается. Данные передаются контроллеру доступа, но отображаемый результат аутентификации по-прежнему отображается как "неудачная попытка".
Считыватель карт	Устройство подключается к внешнему считывателю карт и передает информацию о картах контроля доступа на контроллер доступа или платформу управления.
Устройство чтения карт (OSDP)	Устройство подключается к внешнему считывателю карт OSDP и передает информацию о картах контроля доступа на контроллер доступа или платформу управления.
Модуль безопасности двери	Кнопка выхода, замок и противопожарная система не работают после включения модуля безопасности. Поддерживается аутентификация по лицу, карте, отпечатку пальца. пароль и другие методы управления модулем безопасности двери для ее разблокировки. • Поддерживает разблокировку через внешний интерфейс RS-485. Считыватель карт или кнопка открытия, подключенная к модулю безопасности управления дверью.  Дистанционная разблокировка внешнего дверного замка через модуль безопасности двери не поддерживается.
Модуль расширения замка	Когда контроллер доступа подключен к внешнему модулю расширения замка, при выборе опции «Модуль расширения замка» локальный замок разблокируется после проверки идентификации на локальном устройстве, а дополнительный замок — после проверки идентификации на внешнем считывателе карт. После выбора модуля расширения замка вы можете выбрать канал 2 на странице «Параметры контроля доступа и сигналы тревоги» на веб-странице контроллера доступа.

Таблица 3-20. Описание Виганда.

Параметр		Описание
Настройки Wiegand		• При подключении внешнего устройства чтения карт выберите Wiegand. Ввод . • Если устройство функционирует как считыватель карт и вам необходимо подключить его к другому контроллеру доступа, выберите параметр «Конфигурация вывода Wiegand».
Виганд Вход	Номер карты. Инверсия	Если последовательность номеров карт, полученная через вход Wiegand, не совпадает с фактической последовательностью номеров карт при взаимодействии с устройствами сторонних производителей, включите эту функцию.
Виганд Выход	Виганд Тип вывода	Длина битов номеров карт или идентификаторов, которые устройство может распознать и вывести. • Wiegand 26: считывает 3 байта или 6 цифр. • Wiegand 34: считывает 4 байта или 8 цифр. • Wiegand 66: считывает 8 байтов или 16 цифр.
	Ширина импульса	Настройте ширину импульса и интервал для вывода сигнала Wiegand.
	Интервал пульса	
	Выходные данные Тип	Выберите формат Wiegand для считывания номеров карт или идентификационных номеров. • Идентификатор пользователя: Выводит данные на основе идентификатора пользователя. • Карта: Выводит данные на основе первого номера карты пользователя.
	Виганд Формат	Если в качестве типа выходных данных выбран ID, можно выбрать десятичный или шестнадцатеричный формат вывода.

3.8.3 Настройка параметров Bluetooth

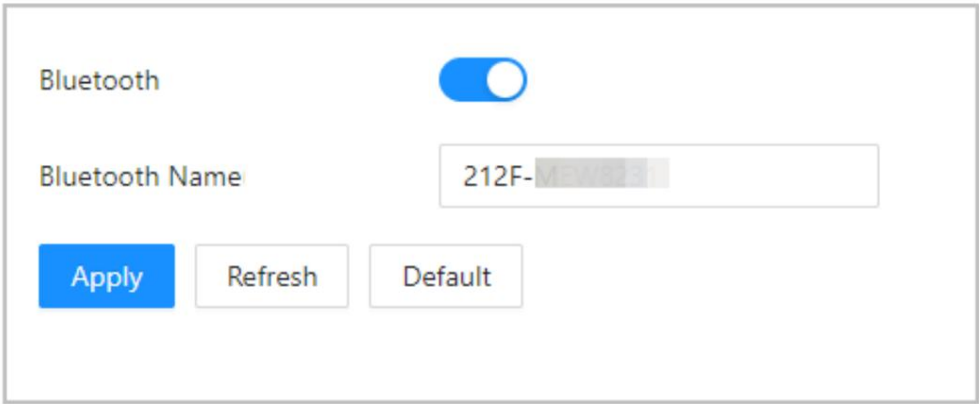
Настройте функцию Bluetooth устройства. Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. Выберите «Настройки связи» > «Настройки Bluetooth».

Шаг 2. Включите или выключите Bluetooth, а затем настройте имя Bluetooth.

Рисунок 3-39 Bluetooth



Шаг 3. Нажмите «Применить».

Результаты

Дверь можно разблокировать через Bluetooth с помощью приложения DMSS.

3.9 Настройка системы

3.9.1 Управление пользователями

Вы можете добавлять или удалять пользователей, изменять пароли пользователей, а также указывать адрес электронной почты для сброса пароля в случае его забывания.

3.9.1.1 Добавление администраторов

Вы можете добавить новые учетные записи администраторов, после чего они смогут войти на веб-страницу устройства.

Процедура

Шаг 1. На главной странице выберите Система > Учетная запись > Учетная запись.

Шаг 2. Нажмите «Добавить» и введите информацию о пользователе.



- Имя пользователя не может совпадать с именем существующей учетной записи. Имя пользователя может содержать до 31 символа и допускает только цифры, буквы, подчеркивания, символы середины строки, точки или символ @.
- Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа следующих символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; : &).

Установите надежный пароль, следуя подсказкам по проверке уровня защиты.

Рисунок 3-40. Добавление администраторов.

Add [X]

* Username

* Password

* Confirm Password

Remarks

OK Cancel

Шаг 3. Нажмите OK.



Изменить пароль может только администратор, и удалить учетную запись администратора невозможно.

3.9.1.2 Сброс пароля

Если вы забыли пароль, восстановите его через указанный адрес электронной почты.

Процедура

Шаг 1. Выберите Система > Учетная запись > Учетная запись.

Шаг 2. Введите адрес электронной почты и установите время истечения срока действия пароля.

Шаг 3. Включите функцию сброса пароля.

Рисунок 3-41 Сброс пароля

Password Reset

Enable ☒

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Email Address

Password Expires in Days



Если вы забыли пароль, вы можете получить коды безопасности на привязанный адрес электронной почты для его сброса.

Шаг 4. Нажмите «Применить».

3.9.1.3 Добавление пользователей ONVIF

Справочная информация

Форум открытых сетевых видеоинтерфейсов (ONVIF) — это глобальный открытый отраслевой форум, созданный для разработки глобального открытого стандарта для интерфейса физических IP-устройств безопасности, обеспечивающего совместимость между различными производителями. Идентификация пользователей ONVIF проверяется с помощью протокола ONVIF.

Пользователем ONVIF по умолчанию является администратор.

Процедура

Шаг 1. На главной странице выберите Система > Учетная запись > Пользователь ONVIF.

Шаг 2. Нажмите «Добавить», а затем настройте параметры.

Рисунок 3-42. Добавить пользователя ONVIF.

Add

*

Username

*

Password

*

Confirm Password

*

Group

OK

Cancel

Таблица 3-21. Описание пользователя ONVIF.

Параметр	Описание
Имя пользователя	Имя пользователя не может совпадать с именем существующей учетной записи. Имя пользователя может содержать до 31 символа и допускает только цифры, буквы, подчеркивания, символы середины строки, точки или символ @.
Пароль	Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа следующих символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; &).
Группа	Существует три группы разрешений, представляющие разные уровни доступа. • Администратор: Вы можете просматривать и управлять другими учетными записями пользователей в диспетчере устройств ONVIF. • Оператор: Вы не можете просматривать или управлять другими учетными записями пользователей в диспетчере устройств ONVIF. • Пользователь: Вы не можете просматривать или управлять учетными записями других пользователей и системными журналами в диспетчере устройств ONVIF.

Шаг 3. Нажмите OK.

3.9.2 Просмотр пользователей онлайн

Вы можете просмотреть список пользователей, которые в данный момент авторизованы на веб-странице. На главной странице выберите Система > Пользователи онлайн.

3.9.3 Настройка времени

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите Система > Время.
- Шаг 3. Настройте время на платформе.

Рисунок 3-43. Настройки времени.

Time and Time Zone

Date :

2024-08-05 Monday

Time :

18:50:31

Time

☒ Manually Set

☐ NTP

System Time

2024-08-05 18:50:31

Sync PC

Time Format

YYYY-MM-DD

24-Hour

Time Zone

(UTC+09:30)

DST

Enable

☐

Type

☒ Date

☐ Week

Start Time

Jan

1

00:00

End Time

Jan

2

00:00

Apply

Refresh

Default

Таблица 3-22. Описание настроек времени.

Параметр	Описание
Время	• Ручная настройка: Введите время вручную или нажмите «Синхронизировать ПК», чтобы синхронизировать время с компьютером. • NTP: Устройство автоматически синхронизирует время с NTP-сервером. ◇ Сервер : Введите домен NTP-сервера. ◇ Порт : Введите порт NTP-сервера. ◇ Интервал : Введите временной интервал для синхронизации.
Формат времени	Выберите формат времени.
Часовой пояс	Выберите часовой пояс.
летнее время	1. (Необязательно) Включите летнее время. 2. В поле «Тип» выберите «Дата» или «Неделя» . 3. Настройте время начала и окончания перехода на летнее время.

Шаг 4. Нажмите «Применить».

3.10 Центр технического обслуживания

3.10.1 Диагностика одним щелчком мыши

Система автоматически диагностирует конфигурацию и состояние устройства для повышения его производительности.

Процедура

Шаг 1. На главной странице выберите Центр обслуживания > Диагностика в один клик.

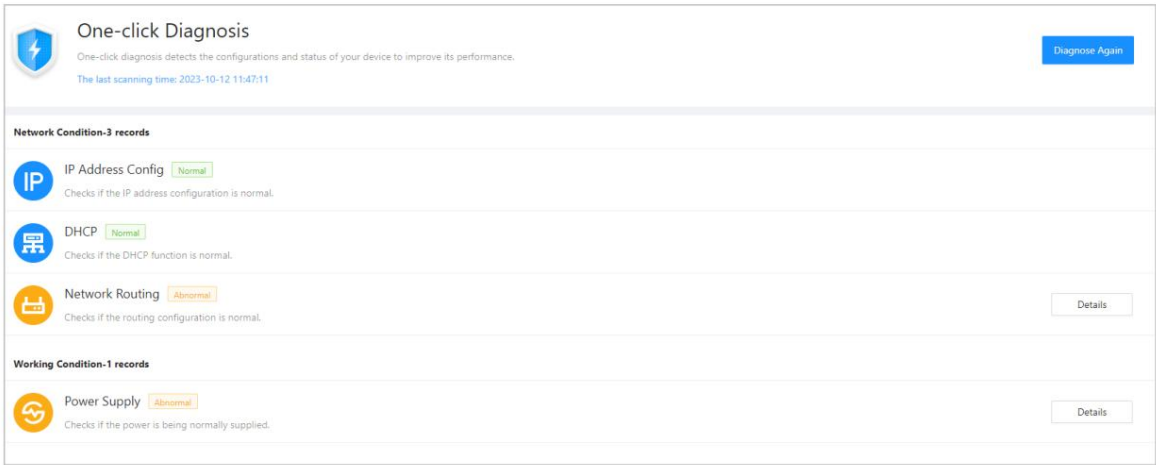
Шаг 2. Нажмите «Диагностика».

Система автоматически диагностирует конфигурации и отображает результаты диагностики после ее завершения.

Шаг 3 (необязательно) Нажмите «Подробности», чтобы просмотреть сведения об аномальных элементах.

Вы можете проигнорировать отклонение или оптимизировать его. Вы также можете нажать «Провести повторную диагностику», чтобы повторно выполнить автоматическую диагностику.

Рисунок 3-44. Диагностика одним щелчком мыши.



3.10.2 Информация о системе

3.10.2.1 Просмотр информации о версии

На веб-странице выберите Центр обслуживания > Информация о системе > Версия, и вы сможете просмотреть информацию о версии устройства.

3.10.2.2 Просмотр юридической информации

На главной странице выберите Центр обслуживания > Информация о системе > Юридическая информация, и вы сможете ознакомиться с лицензионным соглашением на программное обеспечение, политикой конфиденциальности и уведомлением об использовании программного обеспечения с открытым исходным кодом.

3.10.3 Объем данных

Вы можете увидеть, сколько используемого/неиспользуемого пространства устройство может хранить для пользователей, карт и Bluetooth-карт.

Войдите на веб-страницу и выберите Центр обслуживания > Емкость хранилища данных.

3.10.4 Просмотр журналов

Просматривайте журналы, такие как системные журналы, журналы администратора и записи о разблокировке.

3.10.4.1 Системные журналы

Просмотр и поиск системных журналов.
Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите Центр технического обслуживания > Журнал > Журнал.
- Шаг 3. Выберите временной диапазон и тип журнала, а затем нажмите «Поиск».

Связанные операции

- Нажмите «Экспорт» , чтобы экспортировать найденные журналы на локальный компьютер. •
- Нажмите «Зашифровать резервную копию журнала», а затем введите пароль. Экспортированный файл можно будет открыть только после ввода пароля.
- Нажмите  для просмотра подробностей журнала.

3.10.4.2 Разблокировка записей

Найдите записи о разблокировке и экспортируйте их.

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите Центр обслуживания > Журнал > Разблокировать записи.
- Шаг 3. Выберите временной диапазон и тип, а затем нажмите «Поиск».

Вы можете нажать кнопку «Экспорт» , чтобы загрузить записи о разблокировке.

3.10.4.3 Журналы аварийных сигналов

Просмотреть журналы тревожных сообщений.

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите Центр технического обслуживания > Журнал > Журналы аварийных сигналов.
- Шаг 3. Выберите тип и временной диапазон.
- Шаг 4. Введите идентификатор администратора, а затем нажмите «Поиск».

3.10.5 Управление техническим обслуживанием

Если для нескольких устройств требуются одинаковые настройки, вы можете задать для них параметры, импортировав или экспортировав файлы конфигурации.

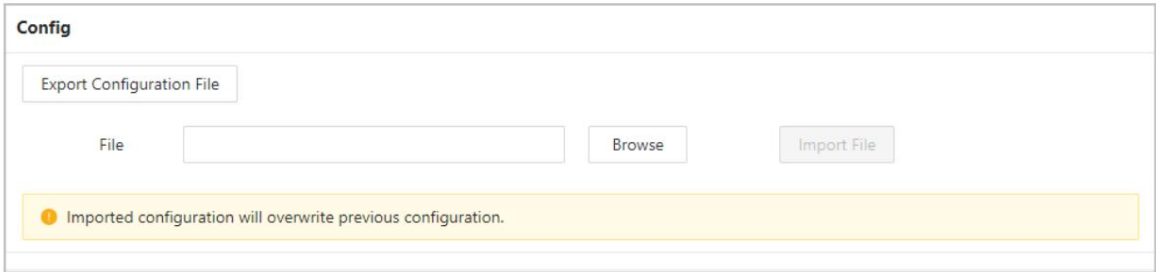
3.10.5.1 Экспорт и импорт конфигурационных файлов

Вы можете импортировать и экспортировать файл конфигурации устройства. Если вы хотите применить одни и те же настройки к нескольким устройствам, вы можете импортировать файл конфигурации на каждое из них.

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите Центр технического обслуживания > Управление техническим обслуживанием > Конфигурация.

Рисунок 3-45. Управление конфигурацией.



Шаг 3. Экспорт или импорт конфигурационных файлов.

- Экспортируйте файл конфигурации.

Нажмите «Экспорт файла конфигурации», чтобы загрузить файл на локальный компьютер.



IP-адрес экспортироваться не будет.

- Импортируйте файл конфигурации.

1. Нажмите кнопку «Обзор», чтобы выбрать файл конфигурации.

2. Нажмите «Импорт конфигурации».



Файлы конфигурации можно импортировать только на устройства одной и той же модели.

3.10.5.2 Настройка порога сходства отпечатков пальцев

Настройте пороговое значение сходства отпечатков пальцев. Чем выше значение, тем выше точность и ниже процент прохождения проверки.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр технического обслуживания > Управление техническим обслуживанием > Конфигурация.

Шаг 3. Введите пороговое значение сходства, а затем нажмите «Применить».



- Этот параметр доступен на модульном контроллере доступа с использованием отпечатка пальца. модуль.
- Этот параметр доступен на контроллере доступа с функцией распознавания отпечатков пальцев.

Рисунок 3-46. Порог сходства отпечатков пальцев.

3.10.5.3 Восстановление заводских настроек по умолчанию

Процедура

Шаг 1. Выберите Центр технического обслуживания > Управление техническим обслуживанием > Конфигурация.



Восстановление устройства до заводских настроек приведет к потере данных. Обратите внимание.

Шаг 2. При необходимости восстановите заводские настройки по умолчанию.

- Сброс к заводским настройкам : Сбрасывает все параметры устройства и удаляет все данные.

- Восстановить настройки по умолчанию (за исключением информации о пользователе и журналов) : Сбрасывает конфигурацию устройства, удаляет все данные, кроме информации о пользователе и журналов.

3.10.5.4 Техническое обслуживание

Для повышения производительности устройства рекомендуется регулярно перезагружать его в режиме ожидания.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр технического обслуживания > Управление техническим обслуживанием > Техническое обслуживание.

Шаг 3. Установите время, а затем нажмите «Применить».

Устройство перезагрузится в запланированное время, или вы можете нажать кнопку «Перезагрузить» , чтобы перезагрузить его немедленно.

3.10.6 Обновление системы



- Используйте правильный файл обновления. Убедитесь, что вы получили правильный файл обновления от технической поддержки.
- Не отключайте источник питания или сеть, а также не перезагружайте и не выключайте устройство во время обновления.
- Обновление до более старой версии может повлечь за собой потенциальные риски. Обратите внимание. • При первом включении устройства или восстановлении заводских настроек устройства могут возникнуть следующие проблемы:
 - Устройство автоматически создает резервные копии системных файлов в течение первых 10 минут. Пожалуйста, не обновляйте систему в этот период.

3.10.6.1 Обновление файла

Процедура

Шаг 1. На главной странице выберите Центр обслуживания > Обновление.

Шаг 2. В разделе «Обновление файла» нажмите «Обзор», а затем загрузите файл обновления.



Файл обновления должен быть файлом с расширением .bin.

Шаг 3. Нажмите «Обновить».

После завершения обновления устройство перезагрузится.

3.10.6.2 Онлайн-обновление

Процедура

Шаг 1. На главной странице выберите Центр обслуживания > Обновление.

Шаг 2 В разделе «Онлайн-обновление» выберите способ обновления.

- Выберите опцию «Автоматическая проверка обновлений», и устройство автоматически проверит наличие последних версий. Обновление версии.
- Выберите «Ручная проверка», и вы сразу сможете проверить, установлена ли последняя версия. Доступный.

Шаг 3 (необязательно) Нажмите «Обновить сейчас» , чтобы немедленно обновить устройство.

3.10.7 Расширенное техническое обслуживание

Получение информации об устройстве и захват пакетов данных упростит работу обслуживающего персонала по устранению неполадок.

3.10.7.1 Экспорт

Процедура

- Шаг 1. На главной странице выберите Центр обслуживания > Расширенное обслуживание > Экспорт.
- Шаг 2. Нажмите «Экспорт» , чтобы экспортировать серийный номер, версию микропрограммы, журналы работы устройства и информацию о конфигурации.

3.10.7.2 Захват пакетов

Процедура

- Шаг 1. На главной странице выберите Центр обслуживания > Расширенное обслуживание > Пакет.
Захватывать.

Рисунок 3-47. Захват пакетов.

Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	1 166	Optional	Optional	Optional	Optional	0.00MB	▶
eth2	1 101	Optional	Optional	Optional	Optional	0.00MB	▶

- Шаг 2. Введите IP-адрес, нажмите  .
-  изменения в .  .
- Шаг 3. После того, как вы собрали достаточно данных, нажмите  .

Захваченные пакеты автоматически загружаются на ваш локальный компьютер.

3.11 (Необязательно) Настройки безопасности

3.11.1 Состояние безопасности

Для проверки состояния безопасности устройства выполните сканирование модулей пользователя, службы и безопасности.

Справочная информация

- Проверка пользователей и служб: проверьте, соответствует ли текущая конфигурация рекомендациям.
- Сканирование модулей безопасности: сканирование текущего состояния модулей безопасности, таких как аудиомодули и Передача видео, надежная защита, предупреждение о безопасности и защита от атак — не определяется, включены ли они.

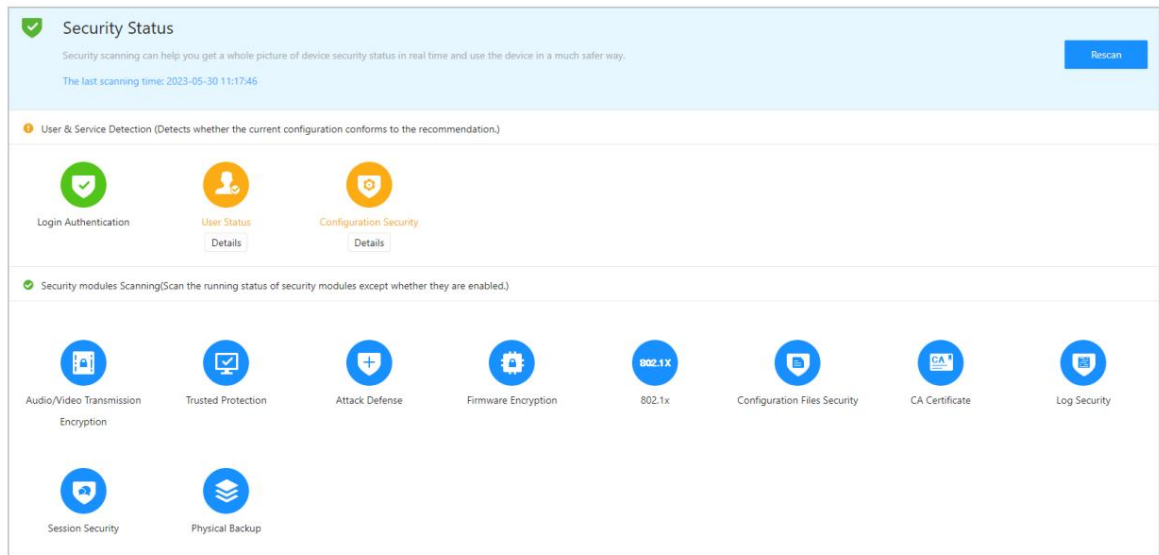
Процедура

- Шаг 1. Выберите >  Состояние безопасности.
- Шаг 2. Нажмите «Повторное сканирование» , чтобы выполнить проверку безопасности устройства.



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

Рисунок 3-48. Состояние безопасности.



Связанные операции

После выполнения сканирования результаты будут отображены разными цветами. Жёлтый цвет указывает на неисправность модулей безопасности, а зелёный — на их исправность.

- Нажмите «Подробности», чтобы просмотреть подробную информацию о результатах сканирования.
- Нажмите «Игнорировать», чтобы проигнорировать обнаруженную аномалию, и сканирование не будет выполнено. Обнаруженная аномалия «Игнорируется» будет выделено серым цветом.
- Нажмите «Оптимизировать», чтобы устранить проблему.

3.11.2 Настройка системной службы

Создайте сертификат или загрузите аутентифицированный сертификат, после чего вы сможете войти на веб-страницу через HTTPS на своем компьютере. HTTPS обеспечивает безопасность передачи данных по компьютерной сети.

Процедура

Шаг 1. Выберите > Системная служба > Системная служба.

Шаг 2. Включите службу HTTPS.



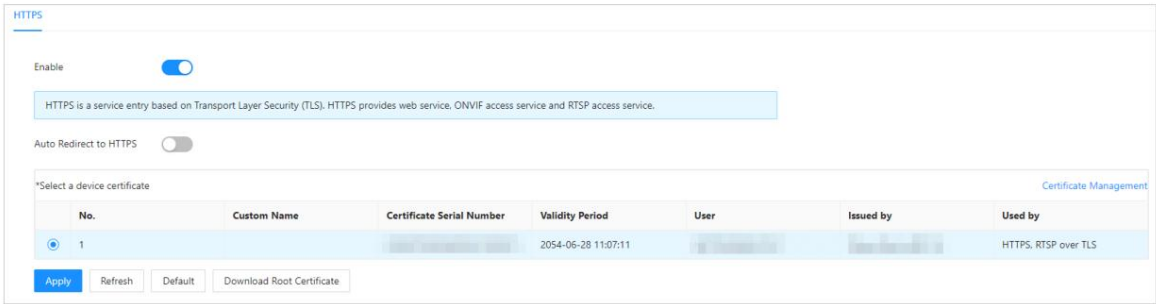
Включение совместимости с TLS версии 1.1 и более ранними версиями может привести к возникновению угроз безопасности. Обращаем ваше внимание на это.

Шаг 3. Выберите сертификат.



Если в списке нет сертификатов, нажмите «Управление сертификатами», чтобы загрузить сертификат.

Рисунок 3-49. Системное обслуживание.



Шаг 4. Нажмите «Применить».

Введите в веб-браузере «https://IP-адрес: httpsport». Если сертификат установлен, вы сможете успешно войти на веб-страницу. В противном случае веб-страница отобразит сертификат как недействительный или ненадежный.

3.11.3 Нападение Защита

3.11.3.1 Настройка брандмауэра

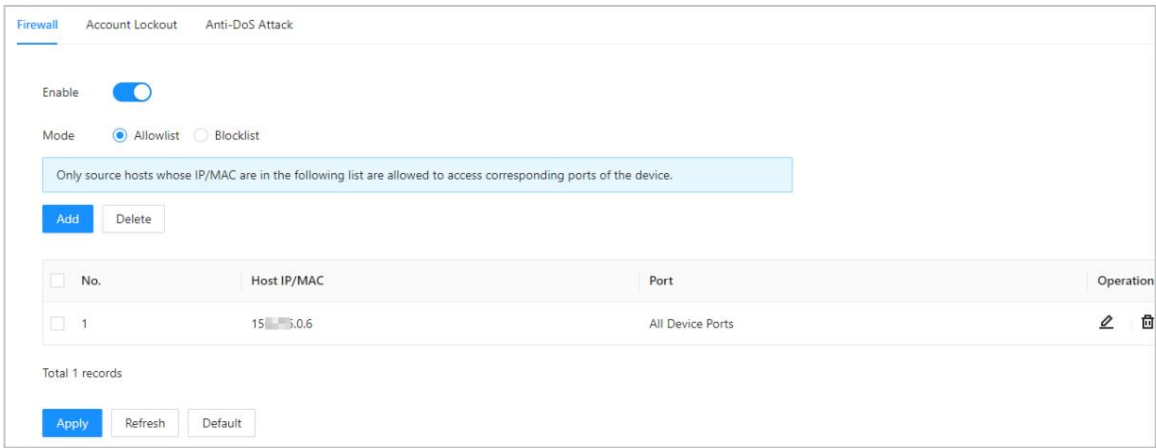
Настройте брандмауэр для ограничения доступа к устройству.

Процедура

Шаг 1. Выберите > Защита от атак > Межсетевой экран.

Шаг 2. Нажмите, чтобы включить функцию брандмауэра.

Рисунок 3-50 Межсетевой экран

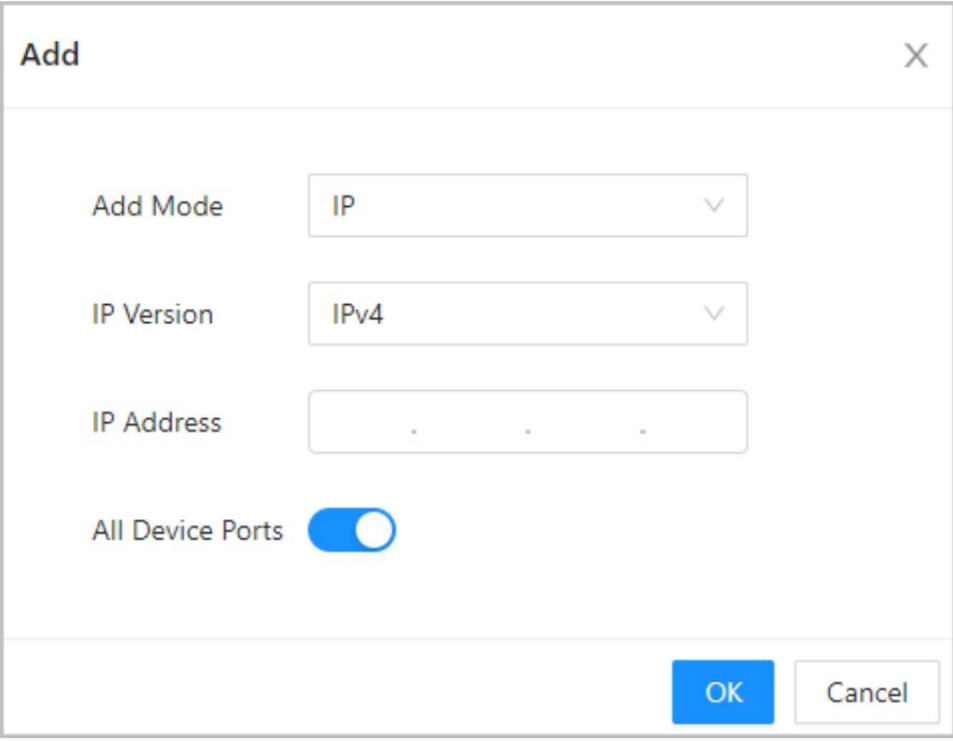


Шаг 3. Выберите режим: Список разрешенных или Список заблокированных.

- Список разрешенных адресов : Доступ к устройству разрешен только для IP-адресов/MAC-адресов из списка разрешенных адресов.
- Список заблокированных адресов : Доступ к устройству запрещен для IP-адресов/MAC-адресов из списка заблокированных адресов.

Шаг 4. Нажмите «Добавить» , чтобы ввести IP-адрес.

Рисунок 3-51. Добавить информацию об IP-адресе.



The image shows a dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there are four fields: "Add Mode" with a dropdown menu showing "IP", "IP Version" with a dropdown menu showing "IPv4", "IP Address" with a text input field containing three dots, and "All Device Ports" with a toggle switch that is currently turned on. At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Шаг 5. Нажмите OK.

Связанные операции

- Нажмите, чтобы отредактировать информацию об IP-адресе.
- Нажмите, чтобы удалить IP-адрес.

3.11.3.2 Настройка блокировки учетной записи

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

Процедура

Шаг 1. Выберите > Защита от атак > Блокировка учетной записи.

Шаг 2. Введите количество попыток входа в систему и время, указанное для учетной записи администратора и ONVIF.
Пользователь будет заблокирован.

Рисунок 3-52 Блокировка учетной записи

Firewall **Account Lockout** Anti-DoS Attack

Device Account

Login Attempt 5time(s) ▾

Lock Time 5 min

Apply Refresh Default

- Количество попыток входа: Лимит попыток входа. Если неверный пароль будет введен определенное количество раз, учетная запись будет заблокирована.
- Время

блокировки: Период времени, в течение которого вы не сможете войти в систему после блокировки учетной записи.

Шаг 3. Нажмите «Применить».

3.11.3.3 Настройка защиты от DoS-атак

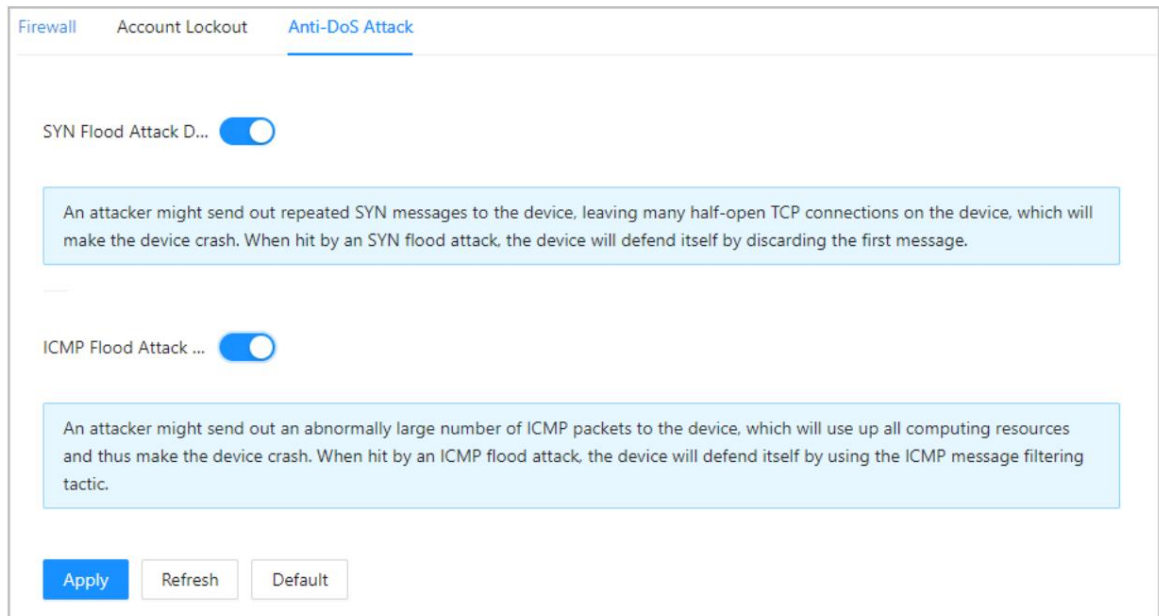
Для защиты устройства от DoS-атак можно включить защиту от SYN-флуд-атак и защиту от ICMP-флуд-атак .

Процедура

Шаг 1. Выберите >  Защита от атак > Защита от DoS-атак.

Шаг 2. Включите защиту от SYN-флуд-атак или ICMP-флуд-атак , чтобы защитить устройство от DoS-атак.

Рисунок 3-53 Защита от DoS-атаки



Шаг 3. Нажмите «Применить».

3.11.4 Сертификат на устанавливаемое устройство

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

3.11.4.1 Создание сертификата

Создайте сертификат для устройства.

Процедура

Шаг 1. Выберите > Сертификат центра сертификации > Сертификат устройства.

Шаг 2. Выберите «Установить сертификат устройства».

Шаг 3. Выберите «Создать сертификат». Шаг 4. , и нажмите «Далее».

Введите информацию о сертификате.

Рисунок 3-54. Информация о сертификате.



Название региона не может превышать 2 символов. Рекомендуется вводить сокращенное название региона.

Шаг 5. Нажмите «Создать и установить сертификат».

После успешной установки сертификата он отобразится на странице «Сертификаты устройства».

Связанные операции

- На странице «Сертификат устройства» нажмите «Войти в режим редактирования», чтобы изменить имя сертификата.
- Нажмите, чтобы загрузить сертификат.
- Нажмите, чтобы удалить сертификат.

3.11.4.2 Подача заявки на получение и импорт сертификата CA

Импортируйте сертификат стороннего центра сертификации на устройство.

Процедура

Шаг 1. Выберите > Сертификат центра сертификации > Сертификат устройства.

Шаг 2. Нажмите «Установить сертификат устройства».

Шаг 3. Выберите «Подать заявку на получение сертификата CA и импорт (рекомендуется)», и нажмите «Далее».

Шаг 4. Введите информацию о сертификате.

- IP-адрес/доменное имя: IP-адрес или доменное имя устройства.

- Регион: Название региона не должно превышать 3 символов. Рекомендуем ввести...
Сокращенное название региона.

Рисунок 3-55 Информация о сертификате (2)

The screenshot shows a web form titled "Step 2: Fill in certificate information." with a close button (X) in the top right corner. The form contains the following fields and labels:

- * IP/Domain Name**: A text input field containing "17" followed by a blurred area and "03".
- Organization Unit**: A text input field.
- Organization**: A text input field.
- * Region**: A text input field.
- Province**: A text input field.
- City Name**: A text input field.

At the bottom of the form, there are three buttons: "Back", "Create and Download" (highlighted in blue), and "Cancel".

Шаг 5. Нажмите «Создать и загрузить».

Сохраните файл запроса на свой компьютер.

Шаг 6. Обратитесь в сторонний центр сертификации за сертификатом, используя файл запроса.

Шаг 7. Импортируйте подписанный сертификат центра сертификации.

1. Сохраните сертификат центра сертификации на свой компьютер.
2. Нажмите «Установка сертификата устройства».
3. Нажмите кнопку «Обзор», чтобы выбрать сертификат центра сертификации.
4. Нажмите «Импорт и установка».

После успешной установки сертификата он отобразится на странице «Сертификаты устройства».

- Нажмите «Создать заново», чтобы повторно создать файл запроса.
- Нажмите «Импортировать позже», чтобы импортировать сертификат позже.

Связанные операции

- На странице «Сертификат устройства» нажмите «Войти в режим редактирования», чтобы изменить имя сертификата. • Нажмите, чтобы загрузить сертификат.
- Нажмите, чтобы удалить сертификат.

3.11.4.3 Установка существующего сертификата

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

Процедура

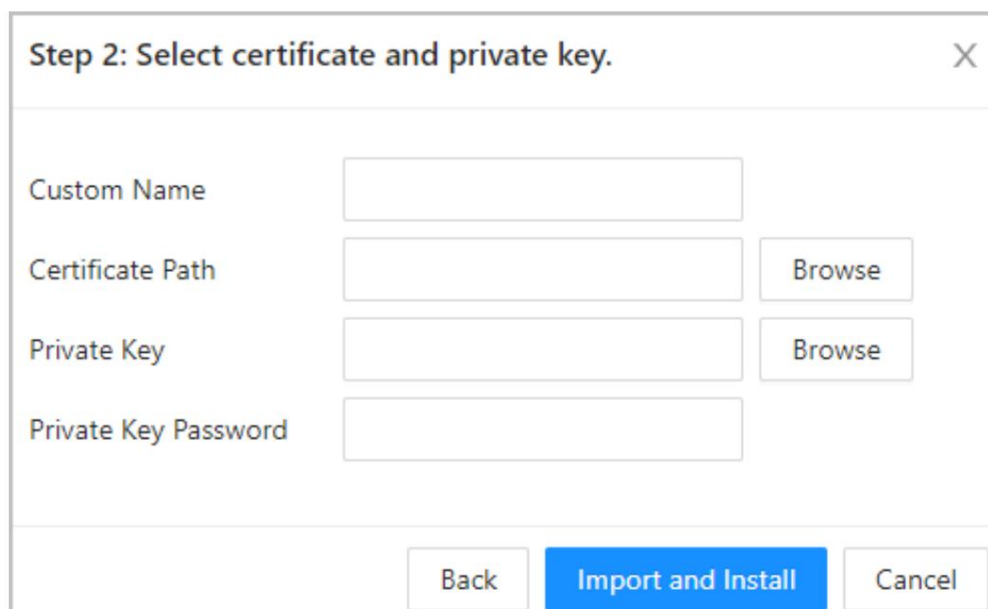
Шаг 1. Выберите Безопасность > Сертификат центра сертификации > Сертификат устройства.

Шаг 2. Нажмите «Установить сертификат устройства».

Шаг 3. Выберите «Установить существующий сертификат». , и нажмите «Далее».

Шаг 4. Нажмите «Обзор» , чтобы выбрать файл сертификата и закрытого ключа, и введите закрытый ключ. пароль.

Рисунок 3-56. Сертификат и закрытый ключ.



Step 2: Select certificate and private key.

Custom Name

Certificate Path Browse

Private Key Browse

Private Key Password

Back Import and Install Cancel

Шаг 5. Нажмите «Импорт и установка».

После успешной установки сертификата он отобразится на странице «Сертификаты устройства» .

Связанные операции

- На странице «Сертификат устройства» нажмите «Войти в режим редактирования» , чтобы изменить имя сертификата.
- Нажмите, чтобы скачать сертификат.
- Нажмите, чтобы удалить сертификат.

3.11.5 Установка доверенного сертификата центра сертификации

Доверенный сертификат центра сертификации (ЦС) — это цифровой сертификат, используемый для проверки подлинности веб-сайтов и серверов. Например, при использовании протокола 802.1X для коммутаторов требуется сертификат ЦС для подтверждения их подлинности.

Справочная информация.

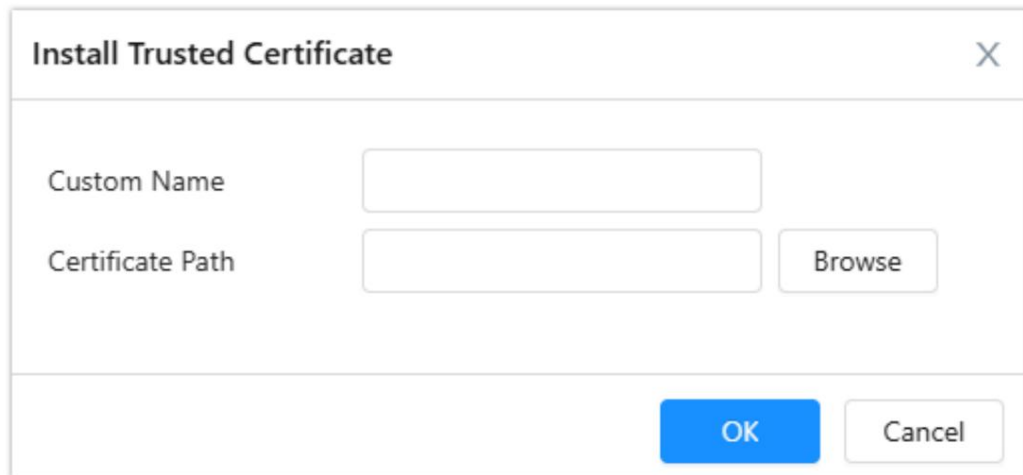
802.1X — это протокол сетевой аутентификации, который открывает порты для доступа к сети, когда организация разрешает ей это делать. Процедура.

Шаг 1. Выберите > Сертификат центра сертификации > Доверенные сертификаты центра сертификации.

Шаг 2. Выберите «Установить доверенный сертификат».

Шаг 3. Нажмите кнопку «Обзор» , чтобы выбрать доверенный сертификат.

Рисунок 3-57. Установите доверенный сертификат.



Шаг 4. Нажмите OK.

После успешной установки сертификата он отображается на странице «Доверенные сертификаты центра сертификации».

Связанные операции

- На странице «Сертификат устройства» нажмите «Войти в режим редактирования», чтобы изменить имя сертификата.
- Нажмите , чтобы загрузить сертификат.
- Нажмите , чтобы удалить сертификат.

3.11.6 Предупреждение о безопасности

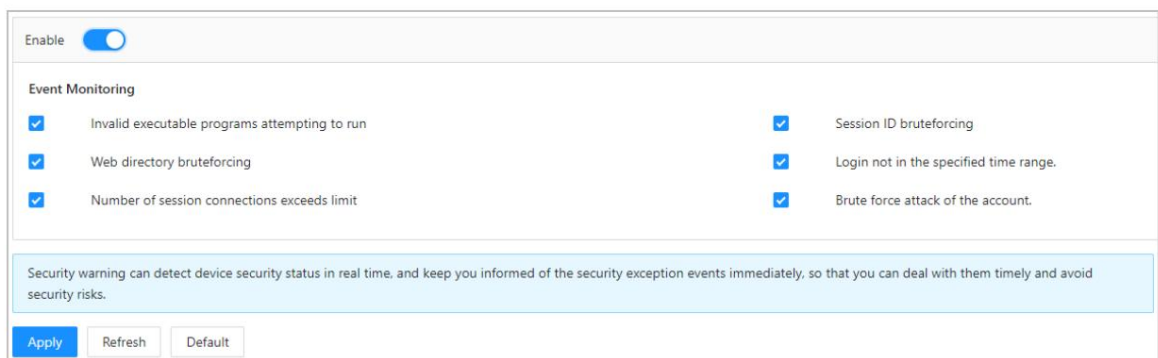
Процедура

Шаг 1. Выберите > Предупреждение безопасности.

Шаг 2. Включите функцию предупреждения системы безопасности.

Шаг 3. Выберите элементы мониторинга.

Рисунок 3-58. Предупреждение о безопасности.



Шаг 4. Нажмите «Применить».

3.11.7 Аутентификация безопасности

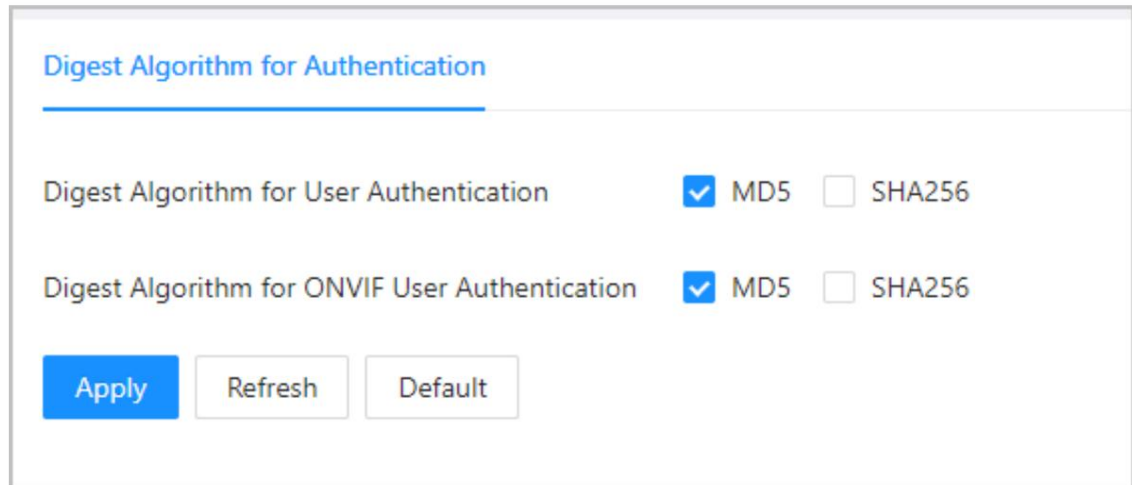
Процедура

Шаг 1. Выберите Безопасность > Аутентификация безопасности.

Шаг 2. Выберите алгоритм хэширования сообщения.

Шаг 3. Нажмите «Применить».

Рисунок 3-59. Аутентификация безопасности.



Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☒ MD5 ☐ SHA256

Digest Algorithm for ONVIF User Authentication ☒ MD5 ☐ SHA256

Apply Refresh Default

4. Работа с телефоном

Перед входом в веб-страницу устройства на телефоне убедитесь, что вы инициализировали устройство через веб-страницу на компьютере.

Мы рекомендуем использовать телефон в портретном и дневном режимах. Вы можете войти на веб-страницу устройства на телефоне следующими способами.

- Подключите устройство к сети с помощью сетевого кабеля. Убедитесь, что телефон и устройства находятся в одной сети. Откройте браузер на телефоне и введите IP-адрес устройства.
- Подключите устройство и телефон к одной и той же сети Wi-Fi. Откройте браузер на телефоне и введите IP-адрес подключенной сети Wi-Fi.
- Подключите телефон к сети через Wi-Fi устройства. Откройте браузер на телефоне и введите IP-адрес точки доступа Wi-Fi на устройстве (по умолчанию это 192.168.3.1).



Название сети Wi-Fi устройства отображается в режиме «Серийный номер устройства + Модель устройства».



- Wi-Fi и точки доступа Wi-Fi доступны на некоторых моделях.
- При входе на веб-страницу с телефона поддерживается только английский язык.

4.1 Инициализация

Если телефон находится в той же локальной сети, что и контроллер доступа, инициализацию контроллера доступа можно выполнить в первый раз или после восстановления заводских настроек устройства через веб-страницу телефона.

Предварительные требования

Убедитесь, что контроллер доступа не подключен к сети Wi-Fi или 4G.

Существует три основных способа подключения устройства и телефона к одной и той же сети. В этом разделе рассматривается инициализация телефона через точку доступа Wi-Fi.

- Подключите устройство к сети с помощью сетевого кабеля. Убедитесь, что телефон и устройства находятся в одной сети. Откройте браузер на телефоне и введите IP-адрес устройства.
- Подключите устройство и телефон к одной и той же сети Wi-Fi. Откройте браузер на телефоне и введите IP-адрес подключенной сети Wi-Fi.
- Подключите телефон к сети через Wi-Fi устройства. Откройте браузер на телефоне и введите IP-адрес точки доступа Wi-Fi на устройстве (по умолчанию это 192.168.3.1).



Wi-Fi и точки доступа Wi-Fi доступны на некоторых моделях.

Процедура

Шаг 1. Включите контроллер доступа.

Шаг 2. Подключитесь к точке доступа Wi-Fi на своем телефоне. Название точки доступа — серийный номер продукта + модель устройства.

Если вы не подключились к точке доступа Wi-Fi в течение 30 минут, точка доступа будет отключена.

Шаг 3. Откройте браузер на своем телефоне и перейдите по IP-адресу точки доступа (адрес по умолчанию — 192.168.3.1).

Шаг 4. Нажмите «Начать инициализацию».

Шаг 5. Введите и подтвердите пароль, а также укажите адрес электронной почты.



- Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа следующих символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' ').
- ; : &). Установите надежный пароль, следуя подсказкам о его надежности.
- Сохраните пароль в безопасном месте после инициализации и регулярно меняйте его для повышения уровня безопасности.

Шаг 6 (необязательно) Включите адрес электронной почты, а затем настройте его.



Если вы хотите сбросить пароль администратора, отсканировав QR-код, вам необходимо включить функцию отправки по электронной почте и указать адрес электронной почты, на который будет приходить код безопасности.

Шаг 7 (необязательно) Выберите «Я прочитал и согласен с Лицензионным соглашением на программное обеспечение и Политикой конфиденциальности».

Шаг 8. Нажмите «Далее».

Шаг 9. Включите автоматическую проверку обновлений по мере необходимости, а затем нажмите «Выполнено».

Отображается страница входа.

4.2 Вход на веб-страницу

Предварительные требования

Убедитесь, что телефон, используемый для входа на веб-страницу, находится в той же локальной сети, что и устройство.

Процедура

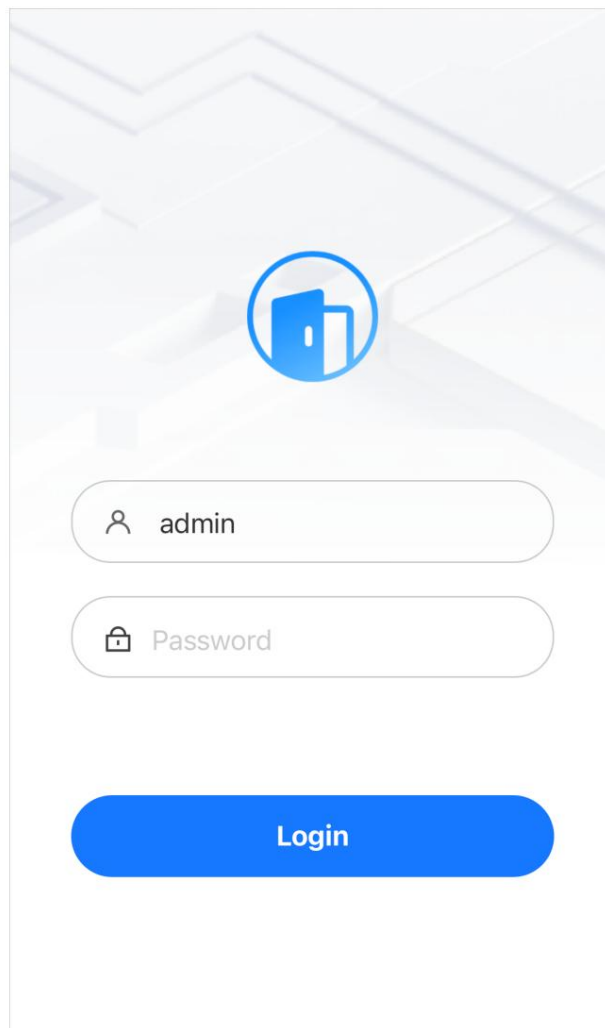
Шаг 1. Откройте браузер и введите IP-адрес устройства.

Шаг 2. Введите имя пользователя и пароль.



- Имя по умолчанию — admin, а пароль — тот, который вы установили во время настройки.
- инициализация. Мы рекомендуем регулярно менять пароль администратора для повышения безопасности.
- Если вы забыли пароль для входа в систему администратора, вы можете сбросить его через веб-страницу на компьютере.

Рисунок 4-1 Страница входа

The image shows a login page with a light gray background featuring a subtle geometric pattern of overlapping planes. At the top center is a blue circular icon containing a white door symbol. Below this icon are two input fields: the first contains the text 'admin' preceded by a small person icon, and the second contains the text 'Password' preceded by a small lock icon. At the bottom center is a large, rounded blue button with the word 'Login' in white text.

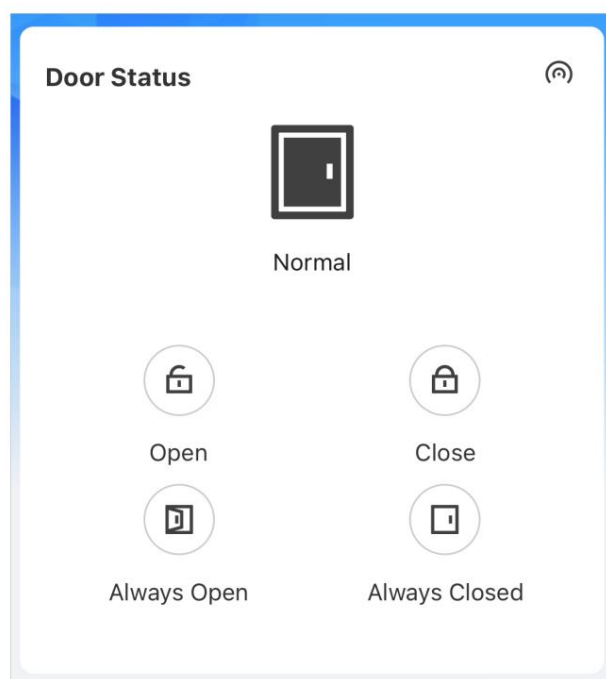
Шаг 3. Нажмите «Войти».

4.3 Главная страница

Главная страница отображается после успешного входа в систему.

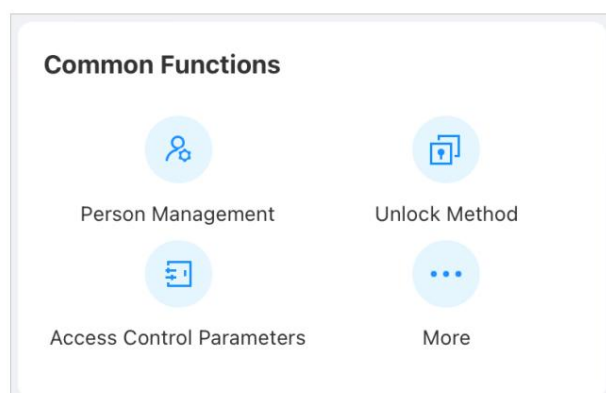
- В разделе «Состояние двери» отображается состояние двери. Вы можете дистанционно открывать или закрывать дверь. Вы также можете настроить статус двери как «Всегда открыта» или «Всегда закрыта».

Рисунок 4-2. Состояние двери.



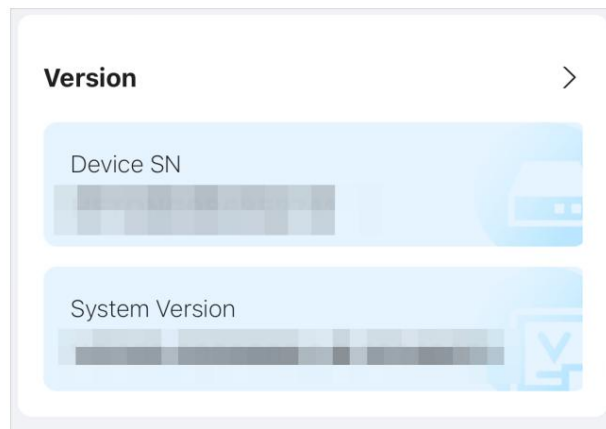
- В области «Общие функции» отображается меню настроек устройства. Нажмите «Подробнее», чтобы просмотреть все меню настроек.

Рисунок 4-3. Общие функции



- В разделе «Версия» можно просмотреть серийный номер и информацию о версии. Нажмите > для просмотра. Подробности о версии.

Рисунок 4-4. Версия



4.4 Управление персоналом

Добавьте пользователя и настройте права доступа.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Нажмите «Управление персоналом», а затем нажмите «+».

Шаг 3. Настройка информации о пользователе.

Рисунок 4-5. Добавить человека (1)

A screenshot of a mobile application form titled 'Basic Info'. It contains several input fields and sections: 'ID' (marked with a red asterisk), 'Name', 'Access Credentials' (a section header), 'Password' (with 'Not Added' and a right arrow), 'Card' (with '0' and a right arrow), 'Fingerprint' (with '0' and a right arrow), 'Bluetooth Card' (with a note 'No email was configured. You cannot request a Bluetooth card through email.' and '0' with a right arrow), 'Verification Mode' (with 'Same as Device' and a right arrow), and 'Permission' (with 'User' and a right arrow).

Таблица 4-1. Описание параметров.

Параметр	Описание
Имя	Идентификатор может состоять из цифр, букв и их комбинаций, а максимальная длина числа составляет 30 символов.
Пароль	Имя может содержать до 32 символов (включая цифры, символы и буквы).
Пароль	Настройте пароль пользователя. Максимальная длина пароля — 8 цифр. Пароль принуждения — это пароль разблокировки + 1. Например, если пароль пользователя — 12345, то пароль принуждения будет 12346. Сигнализация принуждения сработает при использовании пароля принуждения для разблокировки двери.
Карта	- Введите номер карты вручную. - Нажмите «Добавить». - Введите номер карты и нажмите «Добавить». - Автоматическое считывание номера устройством. - Нажмите «Добавить». - Проведите картой по считывателю карт. На экране отображается 60-секундный обратный отсчет, напоминающий о необходимости провести картой, после чего система автоматически считывает номер карты. Если 60-секундный отсчет истек, нажмите кнопку «Считать карту» еще раз, чтобы начать новый отсчет. - Нажмите ОК. Пользователь может зарегистрировать максимум 5 карт. Введите номер карты или проведите картой по считывателю, после чего устройство считывает информацию о карте. Вы можете включить функцию «Карта принуждения». Сигнализация сработает, если для разблокировки двери будет использована карта принуждения. - Карта принуждения : Нажмите, чтобы установить карту принуждения. - Изменить номер карты : Нажмите, чтобы изменить номер карты.  Один пользователь может установить только одну принудительную карту.
Отпечаток пальца	Регистрация отпечатков пальцев. Пользователь может зарегистрировать до 3 отпечатков пальцев, и вы можете назначить один из них в качестве отпечатка для вызова помощи. Сигнализация сработает, когда отпечаток пальца будет использован для разблокировки двери. Регистрация отпечатков пальцев осуществляется с помощью считывателя отпечатков или самого устройства. - Нажмите «Добавить». - Прижмите палец к сканеру в соответствии с инструкциями на экране. - Нажмите ОК.  - Функция сканирования отпечатков пальцев доступна только на некоторых моделях. • Мы не рекомендуем устанавливать первый отпечаток пальца в качестве принудительных отпечатков пальца. • Один пользователь может установить только один принудительный отпечаток пальца.

Параметр	Описание
Bluetooth-карта	 Функция Bluetooth доступна только на некоторых моделях. Вы можете выбрать вариант «Запрос по электронной почте» или «Запрос с помощью регистрационного кода». - Запрос по электронной почте : Подходит для первого запроса Bluetooth-карты. Вы можете запросить до 5 Bluetooth-карт, используя адрес электронной почты, зарегистрированный в DMSS.  Перед использованием этой функции необходимо ввести зарезервированный адрес электронной почты. - Настройте адрес электронной почты, зарегистрированный в DMSS. - Нажмите «Запрос по электронной почте», после чего можно будет запросить карты Bluetooth. • Запрос с помощью регистрационного кода : подходит, если у вас уже есть карта Bluetooth, и вы хотите использовать ее на другом контроллере доступа, поддерживающем функцию Bluetooth. - Скопируйте код регистрации Bluetooth из DMSS. - Нажмите «Запросить с помощью регистрационного кода», а затем введите... код. - Нажмите OK.
Режим проверки	Настройте режим проверки для пользователя. Вы можете использовать режим, совпадающий с режимом устройства, или настроить свой собственный. - Аналогично устройству : Режим работы совпадает с режимом работы устройства. • Пользовательский : После выбора пользовательского режима, метода комбинации и Отображаются способы разблокировки . Выберите комбинацию способов и разблокируйте способы по мере необходимости. - Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы открыть дверь. - И ещё: используйте все выбранные способы разблокировки, чтобы открыть дверь.  - Настраиваемый режим проверки действителен только для локального устройства. Его нельзя использовать во внешних считывателях карт. - Если пользовательский режим проверки отличается от режима устройства, приоритет отдается пользовательскому режиму.
Срок действия	Укажите дату, когда истекает срок действия разрешений на доступ к двери и учет рабочего времени данного лица.
Генеральный план	В течение установленного периода люди могут открывать дверь или отмечать присутствие.  Вы можете выбрать несколько тарифных планов.

Параметр	Описание
План на отпуск	В дни установленных праздников посетители могут открывать двери или отмечать присутствие.  Вы можете выбрать более одного праздника.
Тип пользователя	• Обычный пользователь : Обычные пользователи могут открыть дверь. • Пользователь из черного списка : Когда пользователи из черного списка открывают дверь, служба Персонал получит уведомление. • Гостевой пользователь : Гости могут открывать дверь в течение определенного периода времени или определенное количество раз. По истечении определенного периода или времени разблокировки они не могут открыть дверь. • Патрульный пользователь : Патрульные пользователи могут отмечать посещаемость на устройстве, но у них нет прав доступа к двери. • VIP-пользователь : При разблокировке двери VIP-пользователями на них не распространяются режимы разблокировки, такие как «Многокарточный» и «Временной интервал». • Другой пользователь : После открытия двери она останется открытой еще на 5 секунд. • Пользователь 1/Пользователь 2: То же самое, что и для обычных пользователей.
Затраченное время	Установите лимит времени разблокировки для гостевых пользователей. После истечения этого лимита они не смогут открыть дверь.

Шаг 4. Нажмите «Добавить».

4.5 Настройка системы

4.5.1 Просмотр информации о версии

На веб-странице выберите «Дополнительно» > «Система» > «Версия», и вы сможете просмотреть информацию о версии устройства.

4.5.2 Техническое обслуживание

Для повышения производительности устройства рекомендуется регулярно перезагружать его в режиме ожидания.

Процедура

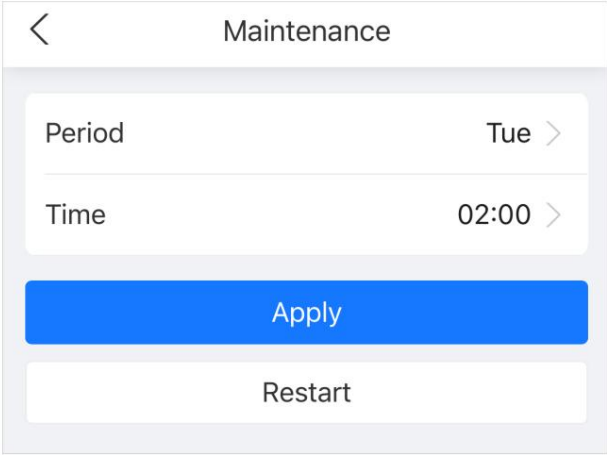
Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Система > Обслуживание.

Шаг 3. Установите время, а затем нажмите «Применить».

Устройство перезагрузится в запланированное время, или вы можете нажать кнопку «Перезагрузить» , чтобы перезагрузить его немедленно.

Рисунок 4-6. Техническое обслуживание.



< Maintenance

Period Tue >

Time 02:00 >

Apply

Restart

4.5.3 Настройка времени

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Система > Время.

Шаг 3. Настройте время.

Рисунок 4-7. Настройка параметров времени.

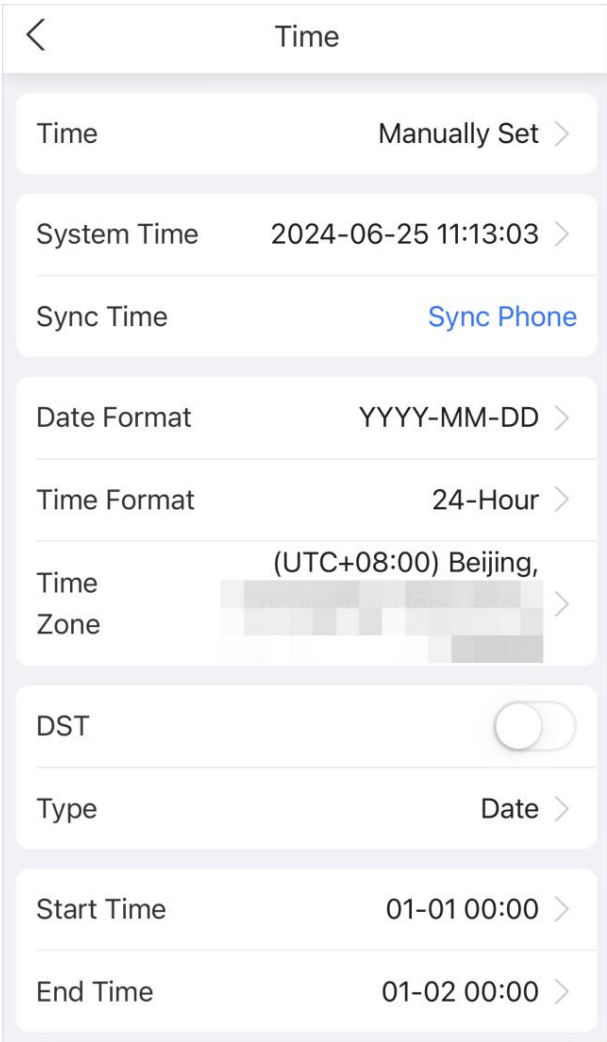


Таблица 4-2. Описание настроек времени.

Параметр	Описание
Время	• Ручная настройка: Введите время вручную или нажмите «Синхронизировать телефон», чтобы синхронизировать время с телефоном. • NTP: Устройство автоматически синхронизирует время с NTP-сервером. сервер. ◇ Сервер : Введите домен NTP-сервера. ◇ Порт : Введите порт NTP-сервера. ◇ Интервал : Введите интервал синхронизации времени.
Формат даты	Выберите формат даты и формат времени.
Формат времени	
Часовой пояс	Выберите часовой пояс.
летнее время	1. (Необязательно) Включите летнее время. 2. Выберите «Дата» или «Неделя» в качестве типа. 3. Настройте время начала и окончания перехода на летнее время.

Шаг 4. Нажмите «Применить».

4.5.4 Объем данных

Вы можете увидеть, сколько используемого/неиспользуемого пространства устройство может хранить для пользователей, карт и Bluetooth-карт.

Войдите на веб-страницу и выберите «Дополнительно» > «Система» > «Объем данных».

4.5.5 Язык

Войдите на веб-страницу, выберите «Дополнительно» > «Система» > «Язык». Измените язык, а затем нажмите «Применить».

4.6 Настройка контроля доступа

4.6.1 Настройка методов разблокировки

Для разблокировки двери можно использовать несколько способов, таких как отпечаток пальца, карта и пароль.

Вы также можете комбинировать их, чтобы создать свой собственный способ разблокировки.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. В главном меню нажмите «Способ разблокировки» или выберите «Дополнительно» > «Контроль доступа» > «Разблокировать».

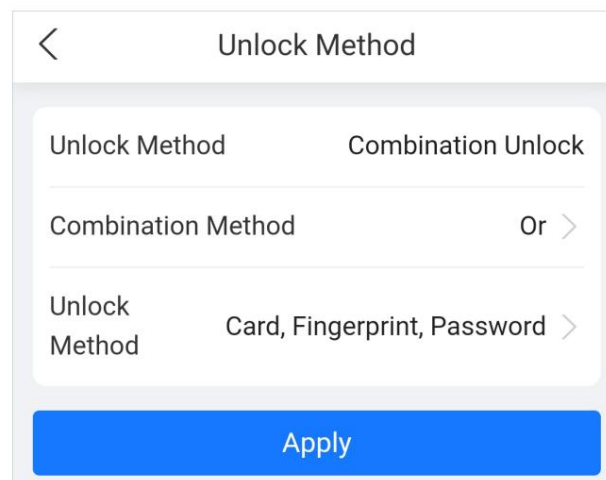
Метод.

Шаг 3 (необязательно) Настройте способ ввода комбинации клавиш и способ разблокировки, а затем нажмите Применять.

- Комбинированный метод
 - ◇ Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы открыть дверь.
 - ◇ И ещё: используйте все выбранные способы разблокировки, чтобы открыть дверь.
- Способ разблокировки

Выберите способ разблокировки в соответствии с поддерживаемыми возможностями устройства.

Рисунок 4-8. Способ разблокировки.



4.6.2 Настройка параметров контроля доступа

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. В главном меню нажмите «Параметры контроля доступа» или выберите «Дополнительно» > «Контроль доступа» > «Параметры контроля доступа».

Шаг 3. Настройте основные параметры контроля доступа, а затем нажмите «Применить».

Рисунок 4-9 Параметры контроля доступа (1)

Name	Door1
Door Status	Normal >
Verification Interval	0 s
Card Swiping Interval	0 s (0-86400)
Public Password	☐
Normally Open Period	
General Plan	Disabled >
Holiday Plan	Disabled >
Normally Closed Period	
General Plan	Disabled >
Holiday Plan	Disabled >

Рисунок 4-10 Параметры контроля доступа (2)

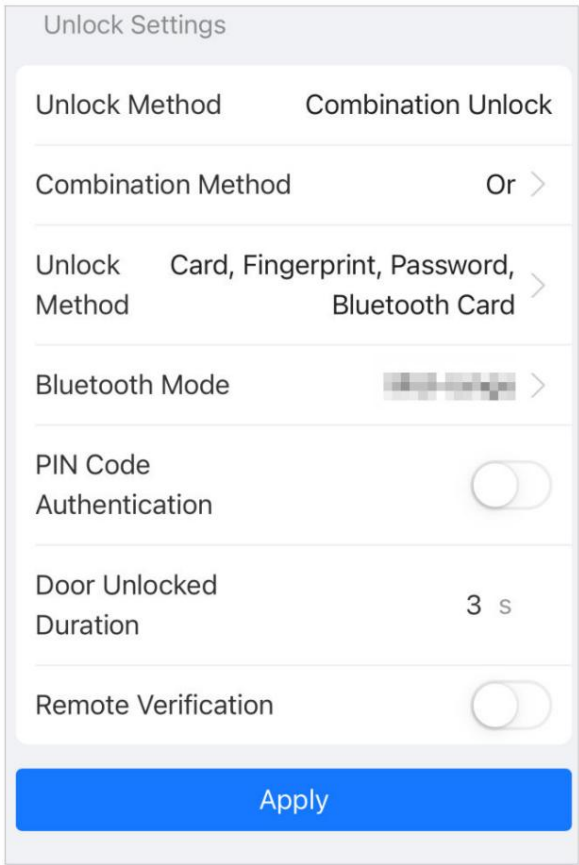


Таблица 4-3. Описание параметров контроля доступа.

Параметр		Описание
Основные настройки	Имя	Название двери.
	Состояние двери	Установите статус двери. • Нормальный режим: Дверь будет открыта и закрыта в соответствии с вашими настройками. • Всегда открыто: Дверь остается незапертой все время. • Всегда закрыто: Дверь остается запертой все время.
	Интервал проверки	Если вы подтверждаете свою личность несколько раз в течение установленного периода, действительной будет считаться только самая ранняя проверка, и дверь не откроется после второй или последующих проверок. С момента, когда дверь не открывается, вам необходимо дождаться истечения заданного интервала времени проверки, прежде чем пытаться подтвердить свою личность снова.

Параметр		Описание
	Проведение картой Интервал	При первой проверке с помощью карты вы, как правило, можете открыть дверь или отметить присутствие, и записи будут сгенерированы. В течение заданного периода, если вы повторно проведете картой для проверки, вы не сможете открыть дверь или отметить присутствие, и записи не будут сгенерированы. Пожалуйста, проверьте идентификацию по истечении заданного периода.  Интервал считывания карты имеет приоритет над интервалом проверки.
	Открытый пароль	После включения функции публичного пароля настройте пароль. Вы можете использовать публичный пароль для разблокировки двери без ввода идентификатора пользователя. Для одного устройства поддерживается только один публичный пароль.
Обычно открыто Период	Период/Праздничный план	При выборе режима «Обычный» вы можете выбрать временной шаблон из выпадающего списка. Дверь остается открытой или закрытой в течение заданного времени.
Обычно закрыто Период	Период/Праздничный план	 • Когда обычно открытый период конфликтует с - В периоды, обычно закрытые, периоды, обычно открытые, имеют приоритет над периодами, обычно закрытыми. • Если периоды совпадают с планами на отпуск, планы на отпуск имеют приоритет над периодами.
Разблокировать настройки	Способ разблокировки	Комбинированная разблокировка по умолчанию.
	Комбинация Метод	• Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы - Откройте дверь. • И: Используйте все выбранные способы разблокировки, чтобы открыть дверь.
	Способ разблокировки	Выберите способ разблокировки в соответствии с поддерживаемыми возможностями устройства.
	Дверь открыта Продолжительность	Настройте продолжительность открытия двери. По умолчанию — 3 секунды. Если дверь открыта дольше заданного времени, она закрывается.
	Режим Bluetooth	Выберите режим Bluetooth в соответствии с вашими потребностями.  Эта функция отображается только после выбора карты Bluetooth в качестве способа разблокировки.
	ПИН-код Аутентификация	При включенной аутентификации по PIN-коду вы можете открыть дверь, используя только пароль.  Если эта функция включена, вводить идентификатор пользователя не требуется. Удаленная проверка не поддерживается.

Параметр	Описание
	Удалённая проверка. Откройте дверь дистанционно.

Шаг 4. Нажмите «Применить».

4.6.3 Настройка сигналов тревоги

Сигнал тревоги сработает при возникновении нештатной ситуации доступа.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Контроль доступа > Сигнализация.

Шаг 3. Настройте параметры сигнализации, а затем нажмите «Применить».

Рисунок 4-11. Настройки сигнализации.

The image shows a mobile application interface for configuring alarm settings. At the top, there are three toggle switches: 'Duress Alarm', 'Anti-passback', and 'Door Detector', all of which are currently turned on (blue). Below these are five expandable sections, each with a title and a status indicator with a chevron arrow. 1. 'Door Detector Status' is set to 'NO'. 2. 'Intrusion Alarm' is 'Disabled', with sub-statuses 'Buzzer: Disabled' and 'Link Alarm Output: Disabled'. 3. 'Unlock Timeout Alarm' is 'Disabled', with sub-statuses 'Buzzer: Disabled' and 'Link Alarm Output: Disabled'. 4. 'Excessive Attempts Alarm' is 'Enable', with sub-statuses 'Buzzer: Disabled' and 'Link Alarm Output: Disabled'. 5. 'Tamper Alarm' is 'Enable', with sub-statuses 'Buzzer: Enable, Duration: 3 s' and 'Link Alarm Output: Disabled'. At the bottom of the screen is a large blue button labeled 'Apply'.

Таблица 4-4. Описание параметров тревоги.

Параметр	Описание
Сигнал тревоги	Сигнализация сработает при использовании карты принудительного вызова, пароля принудительного вызова или отпечатка пальца для разблокировки двери.

Параметр	Описание
Защита от повторного прохода	Пользователи должны подтвердить свою личность как при входе, так и при выходе; в противном случае сработает сигнализация. Это помогает предотвратить передачу карты доступа другому лицу для входа. При включенной функции защиты от повторного прохода владелец карты должен покинуть охраняемую зону через считыватель на выходе, прежде чем система предоставит доступ другому лицу. - Если человек входит после получения разрешения, а выходит без разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен. - Если человек входит без разрешения и выходит после получения разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен.  Если к устройству можно подключить только один замок, проверка на самом устройстве по умолчанию означает направление входа, а проверка на внешнем считывателе карт — направление выхода. Вы можете изменить эту настройку на платформе управления.
Детектор двери	При подключении дверного датчика к вашему устройству сигнализация может срабатывать при ненормальном открытии или закрытии дверей. Существует два типа дверных датчиков: нормально замкнутый (NC) и нормально разомкнутый (NO) датчик. - NC: Датчик находится в закороченном состоянии, когда дверь или Окно закрыто. - NET: Разомкнутая цепь образуется, когда окно или дверь фактически закрыты.
охранная сигнализация	Если дверь открывается ненормально, сработает охранная сигнализация, которая будет гореть в течение определенного времени.  Датчик открытия двери и система охранной сигнализации должны быть включены одновременно.
Сигнализация об истечении времени разблокировки	Если дверь остается незапертой дольше заданного времени, сработает сигнализация об истечении времени ожидания, которая будет действовать в течение заданного времени.
Тайм-аут разблокировки	 Датчик открытия двери и функция автоматического закрытия двери должны быть включены одновременно.
Сигнализация о чрезмерном употреблении	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании неlegalной карты, которая будет гореть в течение определенного времени.
Сигнализация о несанкционированном доступе	Сигнализация о попытке взлома срабатывает при нажатии кнопки обнаружения взлома.

4.6.4 Настройка связи между сигналами тревоги

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Контроль доступа > Настройка связи с сигнализацией.

Шаг 3. Выберите зону для настройки сигнализации.

Рисунок 4-12. Связь сигналов тревоги.

Alarm-in Port	1
Name	Zone1
Alarm Input Type	NO >
Link Fire Safety Control	☐
Alarm-out Port	☐
Duration	30 s
Alarm Output Channel	1 >
Access Control Linkage	☐
Linkage Mode	Weak Execution >
When the fire alarm signal disappears, the door will automatically return to the normal authentication mode.	
Channel Type	NC >
OK	

Шаг 4. Придумайте название для зоны тревоги.

Шаг 5. Включите функцию Link Fire Safety Control и выберите тип устройства ввода сигнала тревоги.

- NC: Вход сигнализации находится в нормально замкнутом (NC) состоянии, когда сигнал тревоги не сработал. Сработала сигнализация. Размыкание нормально замкнутой цепи приводит к срабатыванию сигнализации.
- НЕТ: Когда сигнализация не сработала, входное устройство сигнализации находится в нормально разомкнутом (НО) состоянии. Замыкание цепи приводит к срабатыванию сигнализации.

Шаг 6. Если вы хотите связать управление доступом с срабатыванием пожарной сигнализации, включите функцию «Управление доступом». Связь.



Эта функция вступает в силу только после включения функции Link Fire Safety Control .

Шаг 7. Выберите режим соединения.

- Интенсивное выполнение: Когда сигнал пожарной тревоги исчезает, дверь остается в текущем состоянии. При желании вы можете вручную изменить ее состояние на предыдущее.
- Слабое выполнение: Когда сигнал пожарной тревоги исчезает, дверь автоматически возвращается в предыдущее состояние.

Шаг 8. Выберите тип канала.

- НЕТ: Дверь автоматически открывается при срабатывании пожарной сигнализации.
- НЕТ: Дверь автоматически закрывается при срабатывании пожарной сигнализации.

Шаг 9. Нажмите OK.

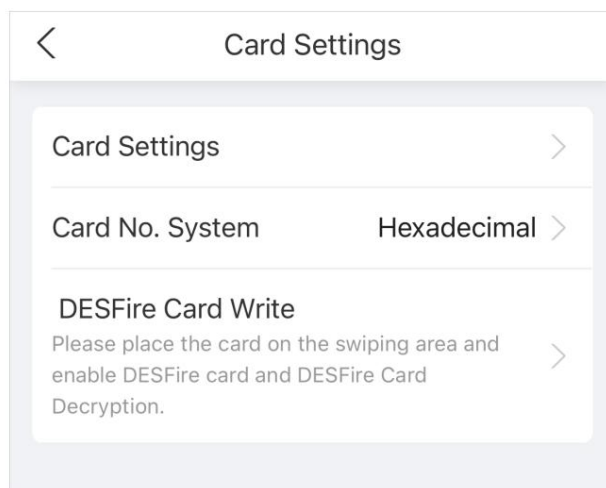
4.6.5 Настройка параметров карты

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Контроль доступа > Настройки карты.

Рисунок 4-13 Настройки карты



Шаг 3. Нажмите «Настройки карты» , настройте параметры карты, а затем нажмите «Применить».

Рисунок 4-14. Параметры карты.

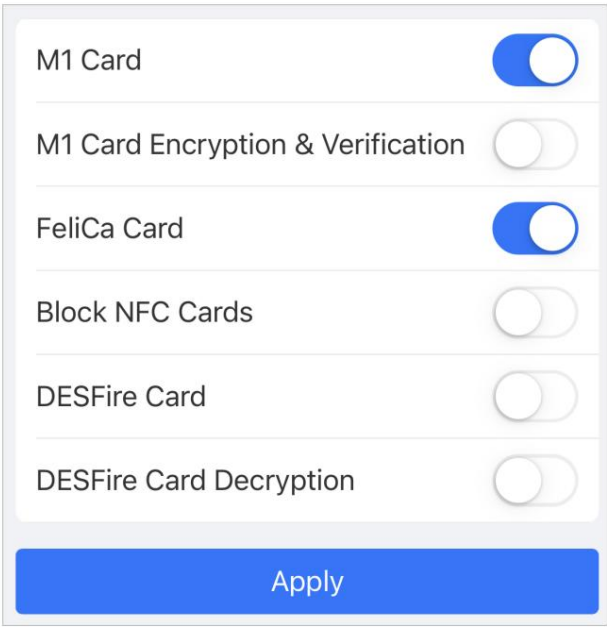


Таблица 4-5. Описание параметров карты.

Параметр	Описание
Карта M1	При включении этой функции карту M1 можно считать.  Эта функция доступна только на некоторых моделях.
Шифрование и проверка карт M1	При включении этой функции можно считать только зашифрованную IC-карту.  Убедитесь, что карта M1 активирована.
FeliCa Card	При включении этой функции карту FeliCa можно считать.  Эта функция доступна только на некоторых моделях.
Блокировка NFC-карт	После включения этой функции разблокировка с помощью дубликатов NFC-карт будет исключена.  • Эта функция доступна только в моделях, поддерживающих IC-карты. • Убедитесь, что карта M1 активирована. • Функция NFC доступна только на некоторых моделях телефонов.

Параметр	Описание
Карта Defire	При включении этой функции устройство может считывать номер карты Desfire.  • Эта функция доступна только в моделях, поддерживающих IC. карты. • Поддерживается только шестнадцатеричный формат.
Расшифровка карты Desfire	Информация на карте Desfire может быть прочитана, если одновременно включены функции «Включить карту Desfire» и «Расшифровка карты Desfire» .  • Эта функция доступна только в моделях, поддерживающих IC. карты. • Убедитесь, что карта Desfire включена.

Шаг 4. Нажмите «Система номеров карт» , выберите формат, а затем нажмите «Применить».

При подключении считывателя карт Wiegand выберите десятичный или шестнадцатеричный формат для номера карты. Система нумерации карт одинакова как для ввода, так и для вывода номера карты.

Шаг 5. Нажмите кнопку «Записать на карту DESFire».

Поместите карту в считывающее устройство, введите номер карты, а затем нажмите кнопку «Записать» , чтобы записать номер карты на карту.



- Необходимо включить функцию карты Desfire и функцию расшифровки карты Desfire. • Поддерживается только шестнадцатеричный формат. • Поддерживается до 8 символов.

4.7 Настройки связи

4.7.1 Настройка TCP/IP

Необходимо настроить IP-адрес устройства, чтобы обеспечить его связь с другими устройствами.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройки связи > TCP/IP.

Шаг 3. Настройте параметры, а затем нажмите «Применить».

Рисунок 4-15 TCP/IP

TCP/IP

NIC

NIC 1 >

Mode

Static >

MAC Address

IP Version

IPv4 >

* IP Address

* Subnet Mask

* Default Gateway

* Preferred DNS

* Alternate DNS

MTU

1500

Apply

Таблица 4-6. Описание TCP/IP.

Параметр	Описание
Режим	• Статический: Введите IP-адрес, маску подсети и шлюз вручную. • DHCP: Расшифровывается как Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста). При включении DHCP устройству автоматически будут присвоены IP-адрес, маска подсети и шлюз.
MAC-адрес	MAC-адрес устройства.
IP-версия	IPv4 или IPv6.
IP-адрес	Если вы установите режим «Статический», настройте IP-адрес, маску подсети и шлюз. • IPv6-адрес представляется в шестнадцатеричном формате. • Версия IPv6 не требует установки масок подсети. • IP-адрес и шлюз по умолчанию должны совпадать. сегмент сети.
Маска подсети	
Шлюз по умолчанию	

Параметр	Описание
Предпочитаемый DNS	Укажите IP-адрес предпочтительного DNS-сервера.
Альтернативный DNS	Укажите IP-адрес альтернативного DNS-сервера.
MTU	MTU (Maximum Transmission Unit) — это максимальный размер данных, который может быть передан в одном сетевом пакете в компьютерных сетях. Более высокое значение MTU может повысить эффективность передачи данных по сети за счет уменьшения количества пакетов и связанных с этим сетевых накладных расходов. Если устройство на пути следования по сети не может обрабатывать пакеты определенного размера, это может привести к фрагментации пакетов или ошибкам передачи. В сетях Ethernet обычно используется значение MTU 1500 байт. Однако в некоторых случаях, например, при использовании PPPoE или VPN, могут потребоваться меньшие значения MTU для соответствия требованиям конкретных сетевых протоколов или служб. Ниже приведены рекомендуемые значения MTU для справки: • 1500: Максимальное значение для пакетов Ethernet, также является значением 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.

4.7.2 Настройка Wi-Fi

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Дополнительно» > «Настройки связи» > «Wi-Fi».

Шаг 3. Включите Wi-Fi.

Отображаются все доступные сети Wi-Fi.



• Функция Wi-Fi доступна на некоторых моделях. • Wi-Fi и точка доступа Wi-Fi не могут быть включены одновременно.

Шаг 4. Щелкните по сети Wi-Fi, а затем введите пароль.

Wi-Fi подключен.

Связанные операции

- DHCP: Выберите режим DHCP и нажмите «Применить». Устройство автоматически будет назначена сеть Wi-Fi. адрес.
- Статический режим: Выберите статический режим, вручную введите Wi-Fi-адрес, затем нажмите «Применить». Устройство Подключится к Wi-Fi.

4.7.3 Настройка точки доступа Wi-Fi



- Функция Wi-Fi доступна в некоторых моделях.
- Wi-Fi и точка доступа Wi-Fi не могут быть включены одновременно.

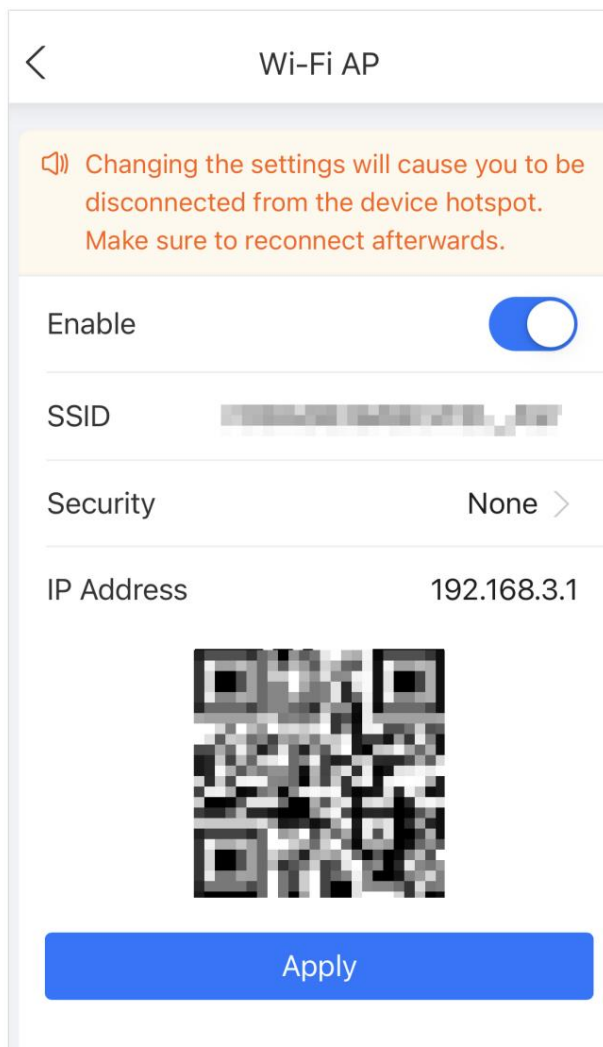
Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Дополнительно» > «Настройки связи» > «Точка доступа Wi-Fi».

Шаг 3. Включите функцию, а затем нажмите «Применить».

Рисунок 4-16. Точка доступа Wi-Fi.



4.7.4 Настройка облачного сервиса

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройки связи > Облачный сервис.

Шаг 3. Включите функцию облачного сервиса.

Облачный сервис становится доступным, если P2P-сети и PaaS-платформы подключены к сети.

Шаг 4. Нажмите «Применить».

4.7.5 Настройка автоматической регистрации

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите Дополнительно > Настройки сети > Автоматическая регистрация.
- Шаг 3. Включите функцию автоматической регистрации, настройте параметры, а затем нажмите «Применить».

Рисунок 4-17. Автоматическая регистрация.

<

Auto Registration

Enable

☐

Status

●

Offline

Server Address

Port

7000

Registration ID

none

Apply

Таблица 4-7. Описание автоматической регистрации.

Параметр	Описание
Статус	Отображает статус подключения автоматической регистрации.
Адрес сервера	IP-адрес или доменное имя сервера.
Порт	Порт сервера, используемого для автоматической регистрации.
Идентификатор регистрации	Идентификатор регистрации устройства (определяемый пользователем). Добавление устройства в систему управления осуществляется путем ввода идентификатора регистрации на платформе.

4.7.6 Режим настройки

Войдите на веб-страницу и выберите «Настройки связи» > «Настройки режима».

Режим считывания карт

Выберите режим «Считыватель карт». Устройство служит в качестве считывателя карт, подключенного к контроллеру контроля доступа извне. Оно не выполняет аутентификацию, а напрямую передает информацию о контроле доступа (например, карту, пароль, отпечаток пальца) на контроллер контроля доступа, который затем выполняет аутентификацию и открывает дверь.

Рисунок 4-18. Режим считывания карт.

Mode

Card Reader >

RS-485 Settings

Baud Rate

9600 >

Data Bit

8 >

Stop Bit

1 >

Parity Code

None >

Wiegand Settings

Wiegand Output Type

Wiegand 34 >

Pulse Width (µs)

200

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Pulse Interval (µs)

1000

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Apply

Режим контроллера доступа

Установите режим «Контроллер доступа ».

103

Рисунок 4-19 Режим контроллера доступа

External Device

Access Controller >

Access controller: This device acts as a card reader, and connects to an access controller, which manages the opening of doors.

Baud Rate

9600 >

Data Bit

8 >

Stop Bit

1 >

Parity Code

None >

Output Data Type

Card Number >

Wiegand Settings

Wiegand Settings

Wiegand Input >

Card No. Inversion

☒

Таблица 4-8. Описание RS-485.

Внешнее устройство	Описание
Контроллер доступа	Выберите «Контроллер доступа», если устройство функционирует как считыватель карт и отправляет данные другим внешним контроллерам доступа для управления доступом. Тип выходных данных: • Номер карты: Выводит данные на основе номера карты, когда пользователь проводит картой для разблокировки двери; выводит данные на основе первого номера карты пользователя при использовании других способов разблокировки. • ID: Выводит данные на основе ID пользователя.  • В случае успешной аутентификации соответствующая информация передается контроллеру доступа. В этом случае отображаемый результат аутентификации соответствует результату аутентификации контроллера доступа. • При сбое аутентификации соответствующая информация не передается. Данные передаются контроллеру доступа, но отображаемый результат аутентификации по-прежнему отображается как "неудачная попытка".
Считыватель карт	Устройство подключается к внешнему считывателю карт и передает информацию о картах контроля доступа на контроллер доступа или платформу управления.
Устройство чтения карт (OSDP)	Устройство подключается к внешнему считывателю карт OSDP и передает информацию о картах контроля доступа на контроллер доступа или платформу управления.
Модуль безопасности двери	Кнопка выхода, замок и противопожарная система не работают после включения модуля безопасности. Поддерживается аутентификация по лицу, карте, отпечатку пальца. пароль и другие методы управления модулем безопасности двери для ее разблокировки. • Поддерживает разблокировку через внешний интерфейс RS-485. Считыватель карт или кнопка открытия, подключенная к модулю безопасности управления дверью.  Дистанционная разблокировка внешнего дверного замка через модуль безопасности двери не поддерживается.
Модуль расширения замка	Когда контроллер доступа подключен к внешнему модулю расширения замка, при выборе опции «Модуль расширения замка» локальный замок разблокируется после проверки идентификации на локальном устройстве, а дополнительный замок — после проверки идентификации на внешнем считывателе карт. После выбора модуля расширения замка вы можете выбрать канал 2 на странице «Параметры контроля доступа и сигналы тревоги» на веб-странице контроллера доступа.

Таблица 4-9. Описание Виганда.

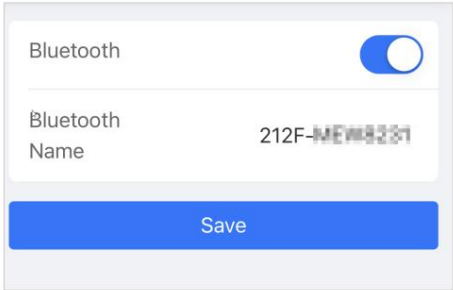
Параметр		Описание
Настройки Wiegand		• При подключении внешнего устройства чтения карт выберите Wiegand. Ввод . • Если устройство функционирует как считыватель карт и вам необходимо подключить его к другому контроллеру доступа, выберите параметр «Конфигурация вывода Wiegand».
Виганд Вход	Номер карты. Инверсия	Если последовательность номеров карт, полученная через вход Wiegand, не совпадает с фактической последовательностью номеров карт при взаимодействии с устройствами сторонних производителей, включите эту функцию.
Виганд Выход	Виганд Тип вывода	Длина битов номеров карт или идентификаторов, которые устройство может распознать и вывести. • Wiegand 26: считывает 3 байта или 6 цифр. • Wiegand 34: считывает 4 байта или 8 цифр. • Wiegand 66: считывает 8 байтов или 16 цифр.
	Ширина импульса	Настройте ширину и интервал импульса для выхода Wiegand.
	Интервал пульса	
	Выходные данные Тип	Выберите формат Wiegand для считывания номеров карт или идентификационных номеров. • Идентификатор пользователя: Выводит данные на основе идентификатора пользователя. • Карта: Выводит данные на основе первого номера карты пользователя.
	Виганд Формат	Если в качестве типа выходных данных выбран ID, можно выбрать десятичный или шестнадцатеричный формат вывода.

4.7.7 Настройка Bluetooth

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите «Связь» > «Настройки Bluetooth».
- Шаг 3. Включите или выключите Bluetooth.

Рисунок 4-20 Bluetooth



- Шаг 4. Нажмите «Сохранить».

Результаты

Разблокировать дверь можно через Bluetooth с помощью приложения DMSS.

4.8 Настройка звука

Процедура

- Шаг 1. Войдите на веб-страницу устройства.
- Шаг 2. Выберите аудио.
- Шаг 3. Включите звук нажатия клавиш или режим «Не беспокоить» в зависимости от ваших потребностей.

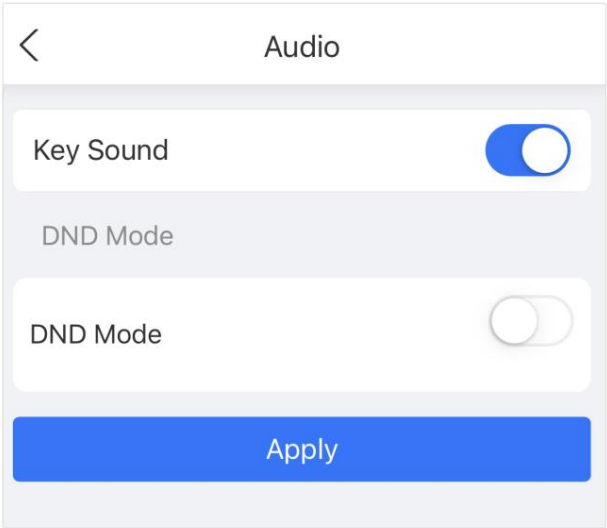


Таблица 4-10. Описание параметров звука.

Параметры	Описание
Ключевой звук	При включении этой функции устройства с сенсорным экраном будут издавать звуковой сигнал при локальных сенсорных операциях, а устройства без сенсорного экрана — при операциях с клавишами/кнопками.
Режим «Не беспокоить»	При включении этой функции в течение заданных периодов времени не будут воспроизводиться звуковые сигналы для локальной проверки (например, доступа к двери или учета присутствия). Поддерживает до 4 временных периодов.

- Шаг 4. Нажмите «Применить».

4.9 Журналы просмотров

Вы можете просматривать такие журналы, как системные журналы, записи о разблокировке и журналы тревожных событий.

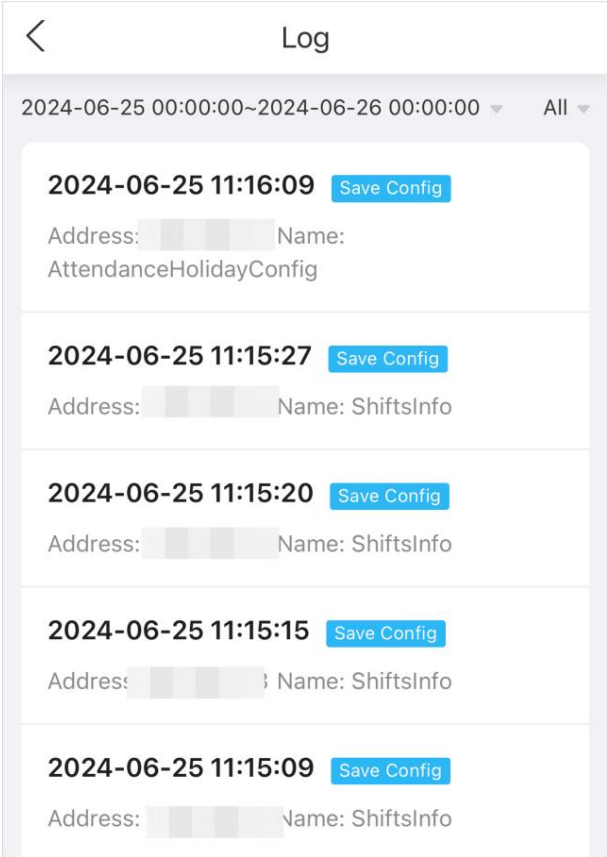
4.9.1 Системные журналы

Просмотр и поиск системных журналов.

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите Дополнительно > Журнал > Журнал.

Рисунок 4-21. Журналы



4.9.2 Разблокировка записей

Найдите записи о разблокировке.

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите «Дополнительно» > «Журнал» > «Разблокировать записи».
- Шаг 3. Щелкните запись, чтобы просмотреть подробности.

4.9.3 Журналы аварийных сигналов

Просмотреть журналы тревожных сообщений.

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите Дополнительно > Журнал > Журнал тревог.

5 конфигураций Smart PSS Lite

В этом разделе описывается, как управлять устройством и настраивать его с помощью Smart PSS Lite. Подробную информацию см. в руководстве пользователя Smart PSS Lite.

5.1 Установка

Для получения Smart PSS Lite обратитесь в службу технической поддержки или посетите официальный сайт. Если вы приобрели программный пакет SmartPSS Lite, установите и запустите программу в соответствии с инструкциями на странице.

5.2 Добавление устройств по одному

Если вам уже известен IP-адрес устройства, вы можете добавить его на платформу вручную.

Процедура

Шаг 1. На главной странице нажмите «Устройства».

Шаг 2. Нажмите «Добавить», а затем введите информацию об устройстве.

Рисунок 5-1. Добавление устройств.

Add Device

Device Name:

*

Add Mode:

IP/Domain Name

IP/Domain Name:

*

Port No.:

*

37777

Username:

*

Password:

*

Add and Continue

Add

Cancel

Таблица 5-1. Параметры добавления IP-блоков.

Параметр	Описание
Название устройства	Название устройства.
Добавить режим	• IP-адрес/доменное имя: добавление устройств по IP-адресу. • Серийный номер (доступен на устройствах, поддерживающих P2P): добавление устройств по их серийному номеру. • Автоматическая регистрация: добавление устройств посредством автоматической регистрации.

Параметр	Описание
IP-адрес/доменное имя	Введите IP-адрес или доменное имя устройства.
Номер порта	Введите номер порта (по умолчанию 37777).
Имя пользователя	Введите имя пользователя и пароль устройства.
Пароль	

Шаг 3. Нажмите «Добавить».

Вы также можете нажать «Добавить и продолжить» , чтобы добавить больше устройств.

5.3 Добавление пользователей

Вы можете добавлять пользователей и предоставлять им права доступа к меню.

Процедура

Шаг 1. Войдите на платформу.

Шаг 2 Выберите  > Управление пользователями.

Шаг 3. Нажмите. Шаг  .

4. Введите основную информацию о пользователе, выберите роли пользователя и подтвердите.
права доступа пользователя.

Рисунок 5-2. Добавление пользователей.

User Info

Username:

Roles:

admin

Password:

••••••••

Confirm Password:

••••••••

Remarks:

Channel Permissions:

Device Right

Search...

▼ Default Group

10.0.0.1

10.0.0.2

10.0.0.3

10.0.0.4

10.0.0.5

10.0.0.6

10.0.0.7

10.0.0.8

10.0.0.9

10.0.0.10

10.0.0.11

10.0.0.12

10.0.0.13

10.0.0.14

10.0.0.15

10.0.0.16

10.0.0.17

10.0.0.18

10.0.0.19

10.0.0.20

Menu Permissions:

Live View

Playback

Access Control Config

Attendance

Event Center

Log Search

Devices

Device Config

Event Config

Person

Attendance Monitor

User Management

System

Save

Cancel

Шаг 5. Нажмите «Сохранить».

Приложение 1. Важные моменты, касающиеся снятия отпечатков пальцев.

Инструкции по регистрации

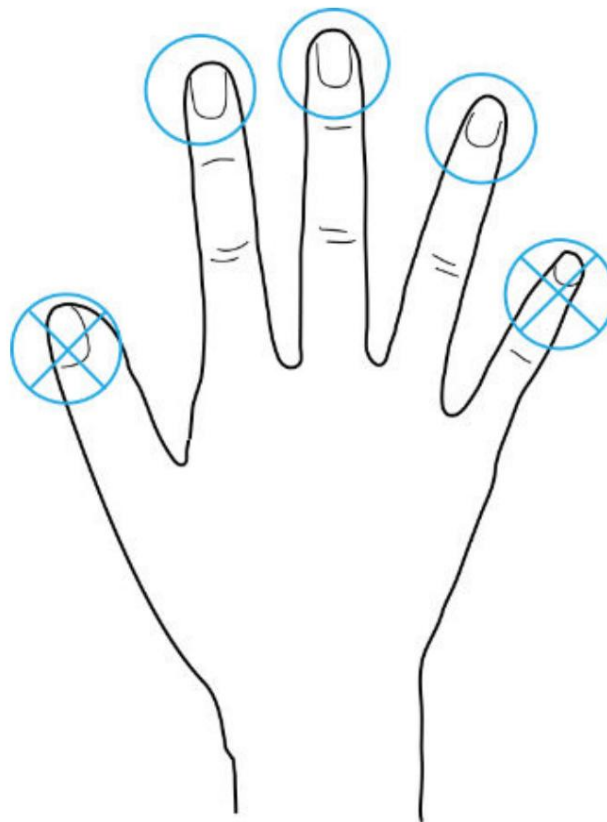
При регистрации отпечатков пальцев обратите внимание на следующие моменты:

- Убедитесь, что ваши пальцы и поверхность сканера чистые и сухие.
- Прижмите палец к центру сканера отпечатков пальцев.
- Не размещайте датчик отпечатков пальцев в местах с интенсивным освещением, высокой температурой и высокой температурой. влажность.
- Если отпечатки пальцев нечеткие, используйте другие способы разблокировки.

Рекомендуется использовать пальцы.

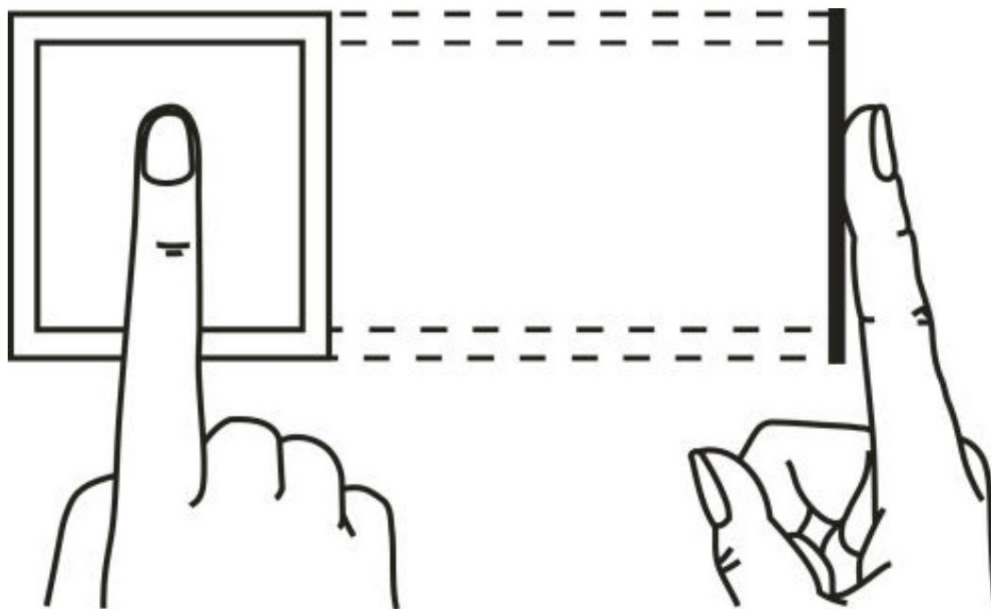
Рекомендуется использовать указательные, средние и безымянные пальцы. Большие пальцы и мизинцы будет сложно разместить в центре записи.

Приложение, Рисунок 1-1. Рекомендуемые пальцы.

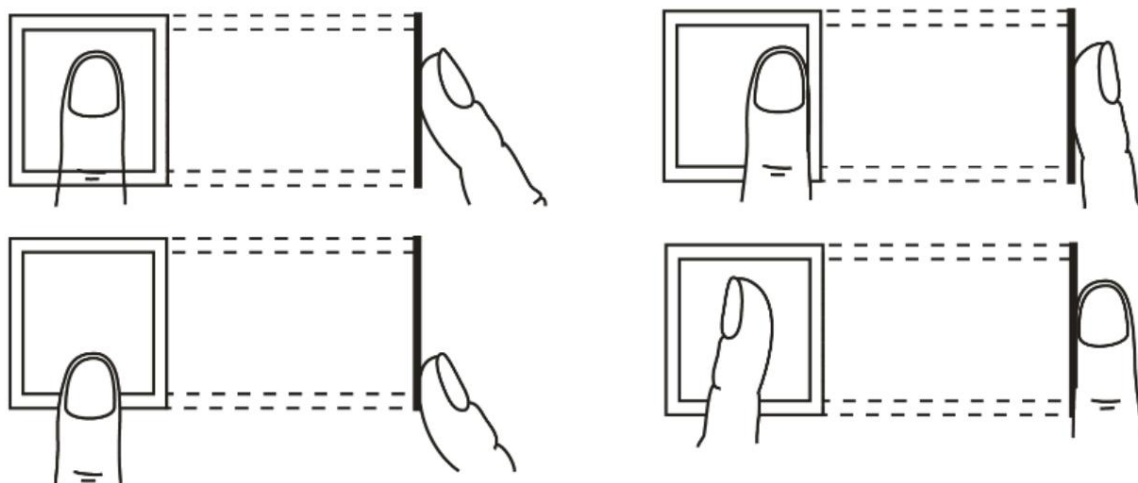


Как приложить отпечаток пальца к сканеру

Приложение, Рисунок 1-2. Правильное размещение.



Приложение, Рисунок 1-3. Неправильное размещение.



Приложение 2. Рекомендации по безопасности.

Управление учетными записями

1. Используйте сложные пароли.

Для установки паролей воспользуйтесь следующими рекомендациями:

- Длина не должна быть меньше 8 символов;
- Включать как минимум два типа символов: прописные и строчные буквы, цифры и символы;
- Не содержать название счета или название счета в обратном порядке;
- Не использовать непрерывные символы, такие как 123, abc и т. д.;
- Не использовать повторяющиеся символы, такие как 111, aaa и т. д.

2. Периодически меняйте пароли.

Рекомендуется периодически менять пароль устройства, чтобы снизить риск его угадывания или взлома.

3. Распределите учетные записи и права доступа надлежащим образом.

Добавляйте пользователей в соответствии с требованиями к обслуживанию и управлению и назначайте им минимальные наборы прав доступа.

4. Включите функцию блокировки учетной записи.

Функция блокировки учетной записи включена по умолчанию. Рекомендуется оставить ее включенной для защиты безопасности учетной записи. После нескольких неудачных попыток ввода пароля соответствующая учетная запись и исходный IP-адрес будут заблокированы.

5. Своевременно устанавливайте и обновляйте информацию для сброса пароля.

Устройство поддерживает функцию сброса пароля. Чтобы снизить риск использования этой функции злоумышленниками, при изменении информации, пожалуйста, своевременно вносите необходимые корректировки. При настройке контрольных вопросов рекомендуется не использовать легко угадываемые ответы.

Конфигурация службы

1. Включите HTTPS.

Рекомендуется включить протокол HTTPS для доступа к веб-сервисам через защищенные каналы.

2. Зашифрованная передача аудио и видео.

Если ваши аудио- и видеоданные очень важны или конфиденциальны, рекомендуется использовать функцию зашифрованной передачи, чтобы снизить риск перехвата ваших аудио- и видеоданных во время передачи.

3. Отключите некритичные службы и используйте безопасный режим.

Если в этом нет необходимости, рекомендуется отключить некоторые службы, такие как SSH, SNMP, SMTP, UPnP, точки доступа и т. д., чтобы уменьшить поверхность атаки.

При необходимости настоятельно рекомендуется выбирать безопасные режимы, включая, помимо прочего, следующие сервисы:

- SNMP: Выберите SNMP v3 и настройте надежное шифрование и пароли аутентификации.
- SMTP: Выберите TLS для доступа к серверу почтовых ящиков.
- FTP: Выберите SFTP и настройте сложные пароли.
- Точка доступа: Выберите режим шифрования WPA2-PSK и настройте сложные пароли.

4. Измените порты HTTP и других служб по умолчанию.

Рекомендуется изменить порт по умолчанию для HTTP и других служб на любой порт в диапазоне от 1024 до 65535, чтобы снизить риск его подбора злоумышленниками.

Сетевая конфигурация

1. Включите список разрешенных .

Рекомендуется включить функцию списка разрешенных IP-адресов и разрешить доступ к устройству только IP-адресам из этого списка. Поэтому обязательно добавьте IP-адрес вашего компьютера и IP-адрес вашего устройства в список разрешенных.

2. Привязка MAC-адреса

Рекомендуется привязать IP-адрес шлюза к MAC-адресу устройства, чтобы снизить риск подмены ARP-адреса.

3. Создайте безопасную сетевую среду.

Для повышения уровня безопасности устройств и снижения потенциальных киберрисков рекомендуется следующее:

- Отключите функцию переадресации портов маршрутизатора, чтобы избежать прямого доступа к устройствам внутренней сети из внешней сети;
- Разделите сеть в соответствии с фактическими потребностями: если между двумя подсетями нет потребности в обмене данными, рекомендуется использовать VLAN, шлюзы и другие методы для разделения сети с целью достижения сетевой изоляции;
- Внедрить систему аутентификации доступа 802.1x для снижения риска несанкционированного доступа терминалов к частной сети.

Аудит безопасности

1. Проверьте пользователей сети.

Рекомендуется регулярно проверять пользователей в сети, чтобы выявлять нелегальных пользователей.

2. Проверьте журнал устройства.

Просмотрев журналы, вы можете узнать об IP-адресах, которые пытались войти в систему устройства, и о ключевых операциях авторизованных пользователей.

3. Настройка сетевого журнала

Из-за ограниченной емкости памяти устройств объем сохраняемых журналов ограничен. Если вам необходимо сохранять журналы в течение длительного времени, рекомендуется включить функцию сетевого журнала, чтобы обеспечить синхронизацию критически важных записей с сервером сетевого журнала для трассировки.

Безопасность программного обеспечения

1. Своевременно обновляйте прошивку.

В соответствии со стандартными отраслевыми требованиями, для обеспечения актуальности функций и безопасности устройства необходимо своевременно обновлять его прошивку до последней версии. Если устройство подключено к общедоступной сети, рекомендуется включить функцию автоматического обнаружения онлайн-обновлений, чтобы своевременно получать информацию об обновлениях прошивки, выпущенных производителем.

2. Своевременно обновляйте клиентское программное обеспечение.

Рекомендуется загрузить и использовать последнюю версию клиентского программного обеспечения.

Физическая защита

Рекомендуется обеспечить физическую защиту устройств (особенно устройств хранения данных), например, разместить устройство в специально отведенном машинном помещении и шкафу, а также установить систему контроля доступа.

а также внедрена система управления ключами для предотвращения повреждения оборудования и других периферийных устройств (например, USB-накопителей, последовательных портов) посторонними лицами.