

Доступ по распознаванию лиц Контроллер

Руководство пользователя



V1.0.0

Предисловие

Общий

В данном руководстве описаны функции и работа контроллера доступа с распознаванием лиц (далее именуемого «устройство»). Внимательно прочтите руководство перед использованием устройства и сохраните его для дальнейшего использования.

Инструкции по технике безопасности

В руководстве могут встречаться следующие сигнальные слова.

Сигнальные слова	Значение:
 DANGER	Указывает на высокую потенциальную опасность, которая, если ее не 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
V1.0.0	Первый релиз.	Январь 2026 г.

Уведомление о защите конфиденциальности

Как пользователь устройства или оператор данных, вы можете собирать персональные данные других лиц, такие как их лицо, аудиозаписи, отпечатки пальцев и номерные знаки автомобилей. Вам необходимо соблюдать местные законы и правила защиты конфиденциальности, чтобы защитить законные права и интересы других людей, внедряя меры, которые включают, помимо прочего: предоставление четкой и видимой идентификации для информирования людей о наличии зоны видеонаблюдения и предоставление необходимой контактной информации.

О руководстве пользователя

- Данное руководство носит исключительно справочный характер. Между руководством и другими документами могут быть обнаружены незначительные различия. продукт.
- Мы не несем ответственности за убытки, понесенные в результате эксплуатации продукта способами, не предусмотренными законом.
 - Соблюдение требований руководства. •

Руководство будет обновляться в соответствии с последними законами и нормативными актами соответствующих юрисдикций.

Для получения подробной информации ознакомьтесь с бумажным руководством пользователя, воспользуйтесь нашим CD-ROM, отсканируйте QR-код или посетите наш сайт.

Наш официальный сайт. Руководство предназначено только для ознакомления. Между электронной и бумажной версиями могут быть незначительные различия. • Все дизайн-проекты и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта

Возможно, будут некоторые расхождения между фактическим продуктом и руководством. Пожалуйста, свяжитесь со службой поддержки клиентов для получения последней версии программы и дополнительной документации. • Возможны ошибки в печати или расхождения в описании функций, операций и технических данных. В случае возникновения каких-либо сомнений или споров мы оставляем за собой право окончательного толкования. • Если руководство (в формате PDF) не открывается, обновите программное обеспечение для чтения или попробуйте другое распространенное программное обеспечение для чтения. • Все товарные знаки, зарегистрированные товарные знаки и названия компаний, упомянутые в руководстве, являются собственностью их владельцев.

соответствующих владельцев.

• В случае возникновения каких-либо проблем, пожалуйста, посетите наш веб-сайт, свяжитесь с поставщиком или службой поддержки клиентов. с использованием

устройства. • В случае возникновения каких-либо неясностей или разногласий мы оставляем за собой право окончательного разъяснения.

Важные меры предосторожности и предупреждения

В этом разделе представлена информация о правильном обращении с устройством, предотвращении опасностей и предотвращении повреждения имущества. Внимательно прочтите перед использованием устройства и соблюдайте инструкции по его использованию.

Требования к транспорту



Транспортировка, использование и хранение устройства должны осуществляться в пределах допустимых условий влажности и температуры.

Требования к хранению



Храните устройство в условиях допустимой влажности и температуры.

Требования к установке



- Не подключайте адаптер питания к устройству, когда адаптер включен. • Строго соблюдайте местные правила и стандарты электробезопасности. Убедитесь, что напряжение окружающей среды соответствует нормам. Стабильна и соответствует требованиям к электропитанию устройства.
- Не подключайте устройство к двум или более типам источников питания во избежание его повреждения. Устройство.
- Неправильное использование батареи может привести к возгоранию или взрыву. • Пожалуйста, соблюдайте требования к электропитанию устройства.
- ◇ Ниже приведены требования к выбору адаптера питания. • Источник питания должен соответствовать требованиям IEC 60950-1 и IEC 62368-1. стандарты.
- Напряжение должно соответствовать требованиям SELV (Safety Extra Low Voltage) и не превышать стандарты ES-1.
- Если мощность устройства не превышает 100 Вт, блок питания должен соответствовать требованиям LPS и быть не выше PS2.
- ◇ Мы рекомендуем использовать адаптер питания, входящий в комплект поставки устройства.
- ◇ При выборе адаптера питания необходимо учитывать требования к источнику питания (например, номинальное напряжение), указанные на этикетке устройства.



- Персонал, работающий на высоте, должен принимать все необходимые меры для обеспечения личной безопасности, включая ношение каски и страховочных ремней.
- Не размещайте устройство в местах, подверженных воздействию солнечных лучей или вблизи источников тепла. • Берегите устройство от влаги, пыли и саж. • Установите устройство на устойчивую поверхность, чтобы предотвратить его падение. • Установите устройство в хорошо проветриваемом месте и не препятствуйте его вентиляции.

- Используйте адаптер или блок питания, предоставленный производителем. • Используйте сетевые кабели, рекомендованные для данного региона и соответствующие номинальной мощности.

технические характеристики.

- Устройство относится к электроприборам класса I. Убедитесь, что источник питания устройства соответствует требованиям.

- Подключается к розетке с защитным заземлением. • Устройство должно быть установлено на высоте не более 2 метров. • Если изделие имеет металлический корпус, рекомендуется устанавливать его в помещении с...

Температура должна быть ниже 40°C (104°F), чтобы избежать перегрева и ухудшения качества использования.

Эксплуатационные требования



- Перед использованием проверьте правильность подключения блока питания. • Перед включением устройства заземлите его на защитный контакт. • Не отключайте шнур питания сбоку устройства, пока адаптер включен. • Эксплуатируйте устройство в пределах номинального диапазона входной и выходной мощности. • Используйте устройство при допустимых условиях влажности и температуры. • Не допускайте попадания жидкости на устройство и убедитесь, что на нем нет предметов, наполненных жидкостью.

- Не разбирайте устройство без инструкции специалиста. • Данное изделие является профессиональным оборудованием. • Устройство не подходит для использования в местах, где могут находиться дети.

Оглавление

Предисловие.....	Я
Важные меры предосторожности и предупреждения.....	III
1 Обзор.....	1
2 Локальные операции.....	2
2.1 Включение питания.....	2
2.2 Методы разблокировки.....	2
2.2.1 Разблокировка с помощью карт.....	2
2.2.2 Разблокировка по лицу.....	2
2.2.3 Разблокировка по отпечатку пальца.....	2
2.2.4 Разблокировка по паролю пользователя.....	2
2.2.5 Разблокировка по Bluetooth.....	2
2.2.6 Разблокировка с помощью QR-кода.....	2
2.3 Восстановление заводских настроек.....	3
3. Веб-операции.....	4
3.1 Инициализация.....	4
3.2 Вход в систему.....	4
3.3 Сброс пароля.....	5
3.4 Мониторинг доступа.....	5
3.5 Домашняя страница.....	7
3.6 Управление персоналом.....	8
3.7 Настройка домофона.....	12
3.7.1 Использование устройства в качестве SIP-сервера.....	13
3.7.2 Использование VTO в качестве SIP-сервера.....	19
3.7.3 Использование платформы в качестве SIP-сервера.....	21
3.7.4 Настройка параметров вызова.....	24
3.8 Настройка контроля доступа.....	25
3.8.1 Параметры контроля доступа.....	25
3.8.2 Сигнализация.....	29
3.8.3 Настройка параметров распознавания лица.....	35
3.8.4 Настройки карты.....	37
3.8.5 Настройка QR-кода.....	42
3.8.6 Настройка периодов.....	43
3.8.7 Настройки конфиденциальности.....	46
3.8.8 Настройка функций выходного порта.....	47
3.8.9 Настройка сравнения на стороне сервера.....	47
3.8.10 Настройка разблокировки от первого лица.....	48
3.9 Настройка аудио и видео.....	49

3.9.1 Настройка видео.....	49
3.9.2 Настройка звуковых подсказок.....	54
3.9.3 Настройка локального кода.....	55
3.10 Настройки связи.....	56
3.10.1 Сетевые настройки.....	56
3.10.2 Настройки Bluetooth.....	67
3.10.3 Настройка RS-485.....	68
3.10.4 Настройка Wiegand.....	69
3.11 Центр управления.....	71
3.11.1 Диагностика одним щелчком мыши.....	71
3.11.2 Информация о системе.....	71
3.11.3 Объем данных.....	72
3.11.4 Журналы просмотра.....	72
3.11.5 Центр технического обслуживания.....	73
3.11.6 Обновление системы.....	75
3.11.7 Расширенное техническое обслуживание.....	75
3.12 (Необязательно) Настройки безопасности.....	77
3.12.1 Состояние безопасности.....	77
3.12.2 Настройка HTTPS.....	78
3.12.3 Атака Защита.....	78
3.12.4 Установка сертификата устройства.....	81
3.12.5 Установка сертификата доверенного центра сертификации.....	84
3.12.6 Шифрование данных.....	85
3.12.7 Предупреждение о безопасности.....	86
3.12.8 Безопасность. Аутентификация.....	86
4. Работа с телефоном.....	88
4.1 Инициализация.....	88
4.2 Вход на веб-страницу.....	88
4.3 Главная страница.....	89
4.4 Управление персоналом.....	91
4.5 Настройка системы.....	94
4.5.1 Просмотр информации о версии.....	94
4.5.2 Управление конфигурацией.....	94
4.5.3 Техническое обслуживание.....	95
4.5.4 Настройка времени.....	95
4.5.5 Объем данных.....	97
4.5.6 Язык.....	97
4.6 Настройка контроля доступа.....	97
4.6.1 Настройка методов разблокировки.....	97
4.6.2 Настройка параметров поверхности.....	98

4.6.3 Настройка параметров контроля доступа.....	100
4.6.4 Настройка сигналов тревоги.....	103
4.6.5 Настройка связи сигналов тревоги (необязательно).....	106
4.6.6 Настройка связи событий тревоги.....	107
4.6.7 Настройка параметров карты.....	108
4.6.8 Настройка конфиденциальности.....	110
4.6.9 Настройка функций выходного порта.....	111
4.7 Настройки связи.....	112
4.7.1 Настройка TCP/IP.....	112
4.7.2 Настройка Wi-Fi.....	114
4.7.3 Настройка точки доступа Wi-Fi.....	114
4.7.4 Настройка облачного сервиса.....	115
4.7.5 Настройка автоматической регистрации.....	115
4.7.6 Настройки Bluetooth.....	116
4.7.7 Настройка Wiegand.....	117
4.7.8 Настройка RS-485.....	118
4.8 Настройка аудиоподсказок.....	120
4.9 Журналы просмотров.....	121
4.9.1 Системные журналы.....	121
4.9.2 Разблокировка записей.....	122
4.9.3 История звонков.....	122
4.9.4 Журналы тревог.....	122
5 Настройка Smart PSS Lite.....	124
5.1 Установка.....	124
5.2 Инициализация и вход в систему.....	124
5.3 Добавление устройств.....	125
5.3.1 Добавление устройства путем поиска.....	125
5.3.2 Добавление устройства по одному.....	126
Приложение 1 Важные моменты регистрации лица.....	127
Приложение 2. Важные моменты сканирования QR-кода.....	130
Приложение 3 Рекомендации по безопасности.....	131

1. Обзор

Данное устройство представляет собой контроллер доступа, поддерживающий разблокировку по лицу, с помощью карт, Bluetooth и их комбинаций. Кроме того, к нему можно подключить внешний сканер паролей или отпечатков пальцев для поддержки дополнительных методов аутентификации.

Благодаря алгоритму глубокого обучения, система отличается более быстрым распознаванием и более высокой точностью. Она может работать с платформой управления, что удовлетворяет различным потребностям клиентов.

Он широко используется в парках, жилых комплексах, деловых центрах и на заводах, а также идеально подходит для таких мест, как офисные здания, правительственные здания, школы и стадионы.

2 Локальные операции

2.1 Включение питания

После включения устройства синий индикатор медленно мигает. После успешного включения устройства зеленый индикатор горит 3 секунды, после чего загорается синий индикатор, имитирующий дыхание. При деинициализации устройства красный индикатор медленно мигает.

2.2 Методы разблокировки

2.2.1 Разблокировка с помощью карт

Вставьте карту в зону считывания, чтобы разблокировать дверь.

2.2.2 Разблокировка по лицу

Для разблокировки двери необходимо подтвердить личность человека, распознав его лицо.

2.2.3 Разблокировка по отпечатку пальца

Подключите внешний сканер отпечатков пальцев к контроллеру доступа, а затем приложите палец к сканеру.

2.2.4 Разблокировка с помощью пароля пользователя

Подключите внешнее устройство к контроллеру доступа, а затем введите идентификатор пользователя и пароль на внешнем устройстве, чтобы разблокировать дверь.

2.2.5 Разблокировка по Bluetooth

Дверь можно разблокировать через Bluetooth с помощью приложения DMSS.



Данная функция поддерживается на некоторых моделях.

Подготовьте следующие вещи.

- Функция Bluetooth включена на веб-странице. Подробности см. в разделе "3.10.2 Bluetooth". Настройки".
- Устройство добавлено в приложение DMSS. Подробности см. в соответствующем руководстве пользователя.

Откройте дверь через приложение DMSS.

Голосовое сообщение "Успешно разблокировано" означает, что дверь открывается, и вы можете войти.

2.2.6 Разблокировка с помощью QR-кода

Воспользуйтесь QR-кодом, чтобы открыть дверь.



Метод использования QR-кода доступен при использовании устройства с модулем для посетителей системы поддержки принятия решений (DSS).

2.3 Восстановление заводских настроек

В течение 5 минут после включения устройства нажмите кнопку защиты от вскрытия пять раз подряд в течение 8 секунд. Индикатор загорится зеленым, затем нажмите и удерживайте кнопку защиты от вскрытия более 3 секунд, чтобы восстановить заводские настройки устройства.

3 Веб-операции

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 на устройстве.

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.

3.2 Вход в систему

Процедура

Шаг 1. Откройте браузер, введите IP-адрес устройства в адресную строку и нажмите кнопку.

Нажмите клавишу Enter.

Шаг 2. Введите имя пользователя и пароль.



- Имя администратора по умолчанию — admin, а пароль — тот, который вы установили во время инициализации. Мы рекомендуем регулярно менять пароль администратора для повышения безопасности. • Если вы забыли пароль для входа в систему администратора, вы можете нажать «Забыли пароль?» Сбросить пароль.

Шаг 3. Нажмите «Войти».

3.3 Сброс пароля

Если вы забыли пароль администратора, сбросьте его через связанный адрес электронной почты. Если адрес электронной почты для сброса пароля не был указан, вам необходимо связаться с местным дилером или службой технической поддержки.

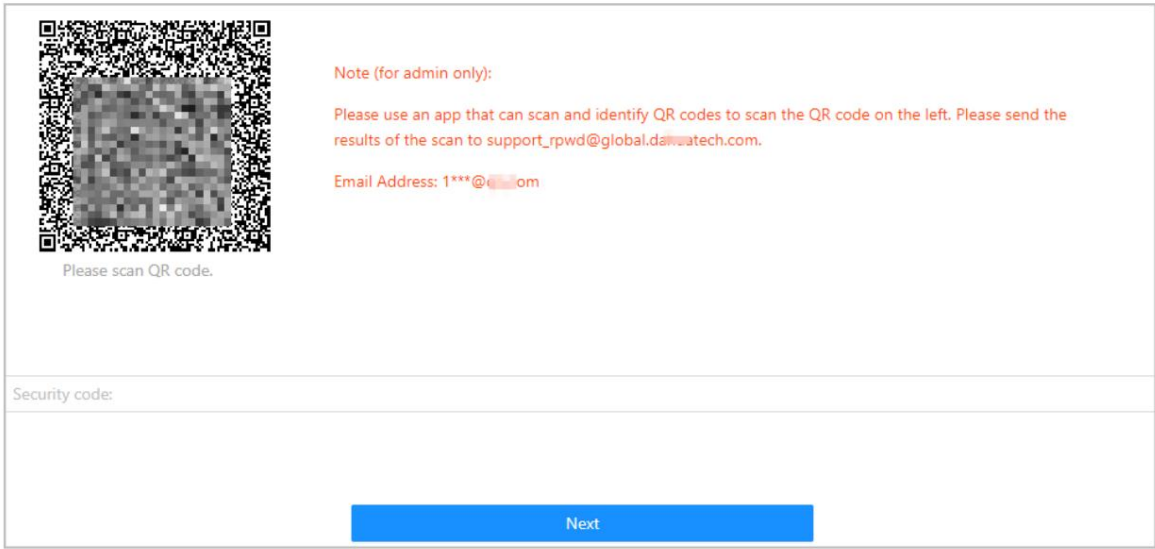
Процедура

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 3-1. Сброс пароля.




- 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.

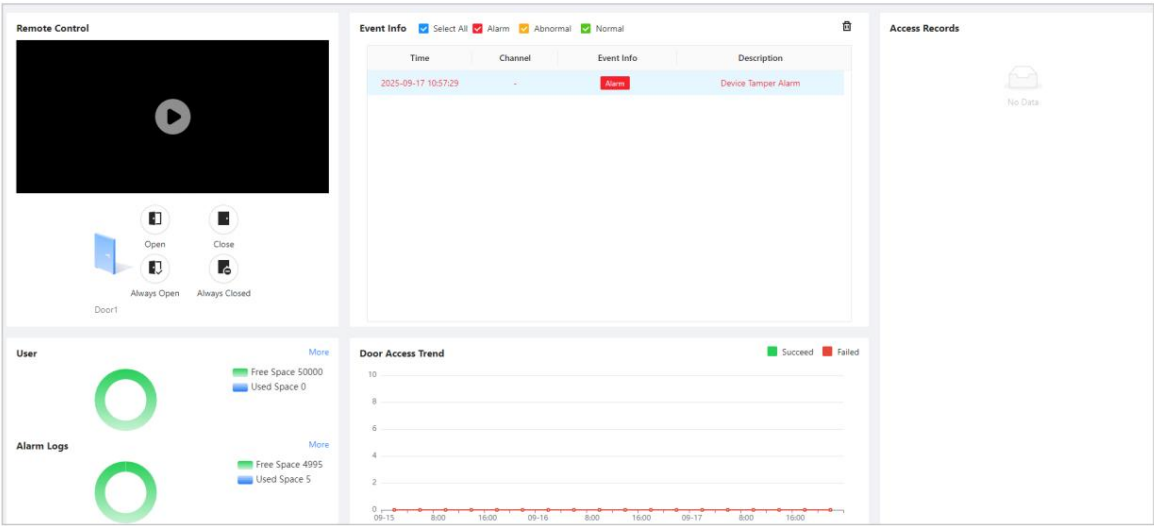
3.4 Мониторинг доступа

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



- Для первого использования, пожалуйста, 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 3-2. 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.
- Нажмите  для предварительного просмотра изображения на экране и выполнения соответствующих операций.

Таблица 3-1. Описание значков на экране пульта дистанционного управления.

Иконки	Описание
	Сделайте снимок.
	Начните запись видео.
	Включите звук в видео.
	Включите функцию внутренней связи.
	Увеличьте изображение.

Тенденция в сфере доступа к дверям

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

Доступ к записям

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

Информация о мероприятии

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

Журналы действий пользователей и тревожных сигналов

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

3.5 Главная страница

 Чтобы перейти на главную страницу, нажмите на кнопку в верхнем левом углу веб-страницы.

Рисунок 3-3 Главная страница

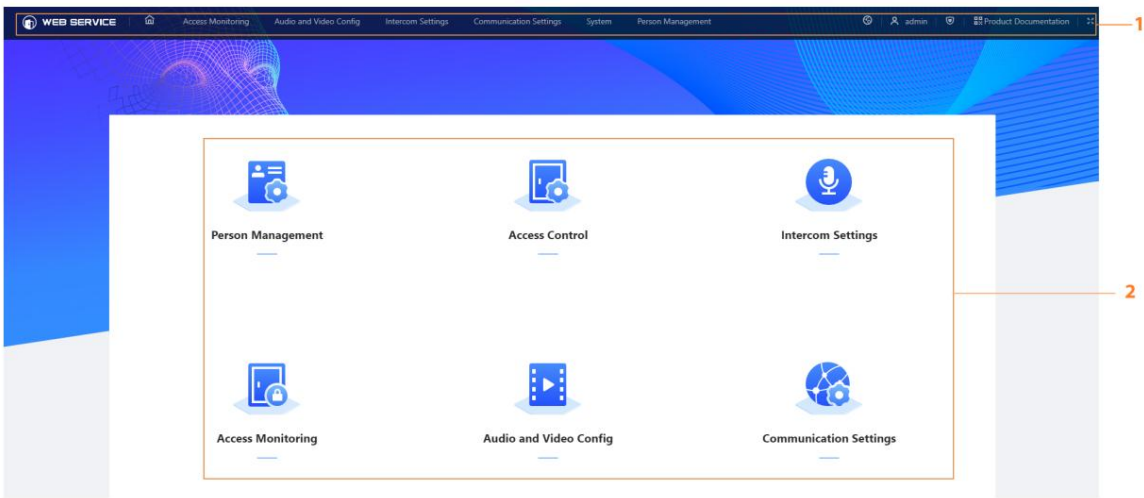


Таблица 3-2. Описание главной страницы

Нет.	Описание
1	Главное меню.

Нет.	Описание
2	• : Перейдите на главную страницу. • : Выберите язык на устройстве. • : admin Выйдите из системы или перезагрузите устройство. • : Перейдите на страницу «Безопасность» . • : Product Documentation Отсканируйте QR-код с помощью телефона, чтобы посмотреть товар. документы. Эта функция доступна только на некоторых моделях. • : Отображение в полноэкранном режиме.

3.6 Управление персоналом

Процедура

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

Шаг 2. Настройка информации о пользователе.

Рисунок 3-4. Основная информация.

Basic Info

* ID

Name

* User Type

General User

▼

* Times Used

Unlimited

* General Plan

255-Default x

* Holiday Plan

255-Default x

Email

Validity Period

Forever

▼

Verification Mode

☐ Same as Device

☒ Custom

Combination Meth...

☐ And

☒ Or

* Unlock Method

Card x

Face x

Password x

Fingerprint x

Bluetooth Card x

Таблица 3-3. Описание основной информации.

Параметр	Описание
Идентификатор	Идентификатор пользователя подобен идентификатору сотрудника и может состоять из цифр, букв и их символов. комбинации, максимальная длина числа составляет 30 символов.
Имя	Имя может содержать до 32 символов (включая цифры, символы и т. д.). буквы).
Срок действия	Выберите один из вариантов: «Навсегда» или «Пользовательский». Если вы выберете «Пользовательский», вам нужно будет установить... дата, когда истекает срок действия прав доступа к двери для данного лица.

Параметр	Описание
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 открыть дверь в течение определенного периода времени или на определенное количество раз. По истечении установленного периода или времени разблокировки они не смогут открыть дверь. • Патрульный пользователь : Патрульные пользователи не имеют доступа к двери. • VIP-пользователь : При разблокировке двери VIP-пользователем обслуживающий персонал получит уведомление. - уведомление. • Другой пользователь : После открытия двери она останется открытой еще на 5 секунд. • Пользователь 1 / Пользователь 2: Аналогично обычным пользователям.
Количество использований	Установите лимит времени разблокировки для гостевых пользователей. После истечения этого лимита они не смогут открыть дверь.
Генеральный план	Люди могут открыть дверь в течение установленного периода времени.  Вы можете выбрать несколько тарифных планов.
План на отпуск	В дни установленных праздников люди могут открывать дверь.  Вы можете выбрать более одного праздника.
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 «Пользовательский» отобразятся «Метод комбинации» и «Метод разблокировки» . Выберите необходимый метод комбинации и методы разблокировки. ◇ 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. Он не может использоваться во внешних считывателях карт. ◇ Если пользовательский режим проверки отличается от режима устройства, приоритет отдается пользовательскому режиму.
Способ разблокировки. Выберите способ(ы) в соответствии с вашими потребностями.	

Рисунок 3-5. Учетные данные доступа.

Access Credentials

Face

Not Added

Upload

Local Collec...

Supports jpg,jpeg,png image formats.

> Password

Not Added

> Card

Not Added

> Fingerprint

Not Added

> Bluetooth Card

No email was configured. You cannot request a Bluetooth card through email.

Not Added

Таблица 3-4. Описание учетных данных доступа.

Параметр	Описание
Лицо	- Загрузка: Нажмите «Загрузить», чтобы загрузить изображение лица. Каждый пользователь может добавить не более 2 изображений лица. После загрузки вы можете просмотреть или удалить изображение лица. - Локальный сбор: Используйте камеру устройства или USB-камеру для сбора изображений лиц. После создания снимка вы можете просмотреть или удалить изображение лица. - Нажмите «Локальная коллекция». - Нажмите «Изменить», чтобы выбрать устройство сбора данных. - Нажмите «Начать создание снимка», чтобы получить изображение лица. - Нажмите «Добавить».
Пароль	Вам необходимо подключить внешнее устройство, способное вводить пароль. Введите пароль пользователя. Максимальная длина пароля — 8 цифр. Пароль принудительного вызова — это пароль разблокировки + 1. Например, если пароль пользователя — 12345, то пароль принудительного вызова будет 12346. Сигнализация принудительного вызова сработает при использовании пароля принудительного вызова для разблокировки двери.

Параметр	Описание
Карта	- Введите номер карты вручную. - Нажмите «Добавить». - Введите номер карты и нажмите «Добавить». - Считывание номера происходит автоматически через устройство считывания регистрационных данных или Устройство. - Нажмите «Добавить» , а затем нажмите «Изменить» , чтобы выбрать устройство для чтения регистрационных данных 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». 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.  : Установить карту принуждения.  : 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. - Нажмите «Добавить» , а затем нажмите «Изменить» , чтобы выбрать устройство для чтения регистрационных данных или устройство». - Прижмите палец к сканеру в соответствии с инструкциями на экране. - Нажмите «Добавить».  - Мы не рекомендуем устанавливать первый отпечаток пальца в качестве отпечатка для принудительного снятия. Отпечаток пальца. • Один пользователь может установить только один принудительный отпечаток пальца. • Функция отпечатка пальца доступна, если устройство поддерживает подключение модуля отпечатков пальцев.

Параметр	Описание
Bluetooth-карта	Вы можете выбрать вариант «Запрос по электронной почте» или «Запрос с помощью регистрационного кода». - Запрос по электронной почте : подходит для тех, кто впервые использует Bluetooth-карту. Запрос. 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 получить Bluetooth-карты. по запросу. - Запрос через регистрационный код : 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 ОК.

Шаг 3. Нажмите «Добавить».

Вы можете нажать кнопку «Добавить ещё», чтобы добавить других пользователей.

Связанные операции

• Очистить: Удалить всех пользователей.

• Обновить: Обновить список пользователей. •

Поиск: Поиск по имени пользователя или идентификатору пользователя. • Пакетная выдача карт:

Выберите пользователей, а затем нажмите «Выдать карточки выбранным пользователям» или « Выдать карточки всем пользователям».

- ◇ 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. • Нажмите «Записи о

картах Bluetooth», чтобы просмотреть записи о картах Bluetooth. Для пользователей, которым не удалось выдать карты, вы можете перевыпустить карты здесь.

3.7 Настройка домофона

Устройство может функционировать как дверная станция для реализации видеодомофонной системы.



Функция внутренней связи доступна только на некоторых моделях.

3.7.1 Использование устройства в качестве SIP-сервера

3.7.1.1 Настройка SIP-сервера

Когда устройство функционирует как SIP-сервер, оно может подключать до 500 VTN.

Процедура

Шаг 1. Выберите «Настройки домофона» > «SIP-сервер».

Шаг 2. Включите SIP-сервер.



При изменении состояния SIP-сервера настройки устройства будут автоматически восстановлены до заводских значений.

Рисунок 3-6 SIP-сервер

Шаг 3. Нажмите «Применить».

3.7.1.2 Настройка локальных параметров

Если устройство функционирует как SIP-сервер, настройте параметры устройства.

Процедура

Шаг 1. Выберите «Настройки домофона» > «Конфигурация локального устройства».

Шаг 2. Настройте параметры.

Рисунок 3-7. Основные параметры

Таблица 3-5. Описание основных параметров.

Параметр	Описание
Тип устройства	Выберите дверную станцию.
Нет.	Невозможно установить.
Групповой звонок	При включении функции группового вызова дверной пульт одновременно звонит на главный VTN и на внутренние номера. Настройка вступает в силу после перезагрузки дверного пульта.
Центр управления	Номер телефона центра управления по умолчанию: 888888 + номер VTS. Чтобы узнать номер VTS, перейдите в раздел «Настройки проекта» > «Общие» в центре управления.

Шаг 3. Нажмите «Применить».

3.7.1.3 Добавление ВТО

Когда устройство функционирует как SIP-сервер, необходимо добавить дверную станцию к SIP-серверу, чтобы обеспечить возможность связи между ними.

Процедура

Шаг 1. На веб-странице устройства выберите «Настройки домофона» > «Настройки устройства».

Шаг 2. Нажмите «Добавить», а затем настройте дверную станцию.

Рисунок 3-8 Добавить VTO

Таблица 3-6. Добавление конфигурации VTO.

Параметр	Описание
Тип устройства	Выберите VTO.
Нет.	Чтобы посмотреть номер дверной станции, перейдите на экран «Устройство». Затем введите номер дверной станции на этой странице.
Регистрация Пароль	Оставьте значения по умолчанию.
Здание №	Невозможно настроить.
Номер блока	
IP-адрес	IP-адрес добавленной дверной станции.
Имя пользователя	Имя пользователя и пароль, используемые для входа на веб-страницу Добавлена дверная станция.
Пароль	

Шаг 3. Нажмите OK.

3.7.1.4 Добавление VTH

Когда устройство функционирует как SIP-сервер, вы можете добавить все VTH в одном блоке на SIP-сервер, чтобы обеспечить возможность их связи друг с другом.

Справочная информация



- При наличии основного VTH и дополнительных линий необходимо сначала включить функцию группового вызова. Затем добавьте основной VTH и дополнительный VTH на странице управления VTH.
- Добавление расширения невозможно, если не добавлены основные VTH.

Процедура

Шаг 1. На главной странице выберите «Настройки домофона» > «Настройки устройства».

Шаг 2. Добавьте VTH.

- Добавляйте по одному.
 1. Нажмите «Добавить».
 2. Настройте параметры, а затем нажмите ОК.

Рисунок 3-9. Складывайте по одному.

Add X

Device Type VTH

Add Mode Add One by One

First Name Please enter

Last Name Please enter

Alias Please enter

* Room No. Please enter

Registration Mode Public

* Registration Password 🔒

OK Cancel

Таблица 3-7 Информация о номере

Параметр	Описание
Имя	Введите название VTH, чтобы вам было проще различать VTH.
Фамилия	
Псевдоним	
Номер комнаты.	Введите номер комнаты ветеринарной клиники. ◇ Номер комнаты состоит из 1-5 цифр и должен соответствовать номеру комнаты, указанному в настройках VTH. ◇ Если есть основной виртуальный домофон (VTH) и его филиалы, то номер комнаты основного VTH заканчивается на -0, а номер комнаты филиала — на -1, -2 или -3. Например, основной VTH — 101-0, а номер комнаты филиала — 101-1, 101-2 и т.д. ◇ Если функция группового вызова не включена, номер комнаты в формате 9901-xx установить невозможно.
Режим регистрации	Оставьте их по умолчанию.
Пароль для регистрации	

• Добавляйте партиями.

1. Нажмите «Добавить в пакетном режиме».

2. Настройте параметры.

3. Нажмите «Добавить».

Рисунок 3-10. Пакетное добавление.

Таблица 3-8. Добавлять партиями.

Параметр	Описание
Этажи в квартире	Количество этажей в здании варьируется от 1 до 99.
Комнаты на каждом этаже	Количество комнат на каждом этаже варьируется от 1 до 99.
Комната номер один на 1-м этаже	Первая комната на первом этаже.
Комната номер один на 2-м этаже	Номер первой комнаты на 2-м этаже равен первой цифре номера первой комнаты на 1-м этаже плюс 1. Например, если номер первой комнаты на первом этаже — 101, то номер первой комнаты на 2-м этаже должен быть 201.

3.7.1.5 Добавление системы VTS

Когда устройство функционирует как SIP-сервер, вы можете добавить VTS к SIP-серверу, чтобы обеспечить возможность совершения звонков друг другу.

Процедура

Шаг 1. На главной странице выберите «Настройки домофона» > «Настройки устройства».

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

Рисунок 3-11. Управление VTS.

Add

Device Type

VTS

Alias

Please enter

* VTS No.

Please enter

* IP Address

1

.

1

.

1

.

1

.

1

* Registration Password

.....

OK

Cancel

Таблица 3-9 Параметры VTS

Параметр	Описание
Псевдоним	Введите название системы управления движением (VTS).
Номер ВТС.	Введите 888888+ номер VTS, который может содержать до 9 цифр. Нет, перейдите на экран «Устройство» в системе VTS.
IP-адрес	IP-адрес системы VTS.
Пароль для регистрации	Оставьте значение по умолчанию.

Шаг 3. Нажмите OK.

3.7.2 Использование VTO в качестве SIP-сервера

3.7.2.1 Настройка SIP-сервера

Используйте другой VTO в качестве SIP-сервера.

Процедура

Шаг 1. Выберите «Настройки домофона» > «SIP-сервер».

Шаг 2. Выберите устройство в поле «Тип сервера».



Не включайте локальный SIP-сервер.

Шаг 3. Настройте параметры, а затем нажмите OK.

Рисунок 3-12. Использование VTO в качестве SIP-сервера.

Local SIP Server

Server Type

Device

Server Address

Port

5060

SIP No.

8001

Registration Password

SIP Domain

VDP

SIP Server Username

SIP Server Password

Apply

Refresh

Default

Таблица 3-10. Конфигурация SIP-сервера.

Параметр	Описание
Адрес сервера	IP-адрес или доменное имя VTO.
Порт	По умолчанию используется код 5060, когда VTO работает в качестве SIP-сервера.
Номер SIP.	Оставьте их по умолчанию.
Пароль для регистрации	
Домен SIP	ВДП.
Имя пользователя SIP-сервера	Имя пользователя и пароль для входа на SIP-сервер.
Пароль SIP-сервера	

Шаг 4. Нажмите «Применить».

3.7.2.2 Настройка локальных параметров

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

Процедура

Шаг 1. Выберите «Настройки домофона» > «Конфигурация локального устройства».

Шаг 2. Настройте параметры.

Рисунок 3-13. Настройка параметров.

Device Type

Door Station

No.

8001

Group Call

☐

Management Center

888888

Apply

Refresh

Default

Таблица 3-11. Описание параметров.

Параметр	Описание
Тип устройства	Выберите дверную станцию.
Нет.	Номер ВТО. • Номер должен состоять из 4 цифр. Первые 2 цифры должны быть 80, а последние 2 цифры начинаются с 01. Например, 8001. • Если в одном подразделении существует несколько регистрационных номеров транспортных средств (ВТО), номер ВТО не может повторяться.
Групповой звонок	Возможна организация связи между дверными станциями.
Центр управления	Номер телефона для связи с центром управления — 888888. Оставьте его значением по умолчанию.

Шаг 3. Нажмите «Применить».

3.7.3 Использование платформы в качестве SIP-сервера

3.7.3.1 Настройка SIP-сервера

Платформа управления используется в качестве SIP-сервера.

Процедура

Шаг 1. Выберите «Настройки домофона» > «SIP-сервер».

Шаг 2. В поле «Тип сервера» выберите «Частный SIP-сервер» .



Не включайте SIP-сервер.

Рисунок 3-14. Альтернативный сервер.

Local SIP Server

Server Type

Private SIP Server

Server Address

192.168.1.111

Port

5080

SIP No.

8001

Registration Password

.....

SIP Domain

VDP

Device as Alternate Server

Alternate IP

Alternate Server Username

admin

Alternate Server Password

.....

Alternate VTS IP

0 . 0 . 0 . 0

Таблица 3-12. Конфигурация SIP-сервера.

Параметр	Описание
Адрес сервера	IP-адрес платформы.
Порт	По умолчанию используется порт 5080, когда платформа работает в режиме SIP-сервера.
Пароль для регистрации. Оставьте значения по умолчанию.	
Домен SIP	Оставьте значение по умолчанию.
Альтернативный IP-адрес	В случае, если платформа не отвечает, в качестве SIP-сервера будет использоваться альтернативный сервер. • Если вы включите функцию «Дополнительный сервер» , вы настроите устройство. в качестве альтернативного сервера. • Если вы хотите, чтобы другой VTO функционировал в качестве альтернативного сервера, вам необходимо ввести IP-адрес, имя пользователя и пароль этого VTO. В этом случае не включайте функцию «Альтернативный сервер» . • Мы рекомендуем установить основной VTO в качестве резервного сервера.
Альтернативный сервер	После настройки альтернативного сервера, если платформа управления не отвечает, альтернативный сервер будет активирован, чтобы обеспечить взаимодействие VTO и VTH. • Если включена опция «Альтернативный сервер» , устройство устанавливается в качестве альтернативного сервера. • Если опция «Альтернативный сервер» не включена, введите IP-адрес альтернативного сервера. укажите сервер, его имя пользователя и пароль, чтобы установить VTO в качестве альтернативного сервера. Мы рекомендуем установить основной VTO в качестве резервного сервера.
Имя пользователя	
Пароль	
Альтернативный сервер	
Альтернативный VTS IP	Введите IP-адрес альтернативного VTS. Если платформа управления не отвечает, будет активирован альтернативный VTS, чтобы обеспечить взаимодействие VTO, VTH и VTS.

Шаг 3. Нажмите «Применить».

3.7.3.2 Настройка локальных параметров

Настройте параметры устройства, если платформа используется в качестве SIP-сервера.

Процедура

Шаг 1. Выберите «Настройки домофона» > «Конфигурация локального устройства».

Шаг 2. Настройте параметры.

Рисунок 3-15. Основной параметр

Device Type

Door Station

Building No.

0

☐

Unit No.

0

☐

No.

8001

Management Center

888888

Apply

Refresh

Default

Таблица 3-13. Описание параметров.

Параметр	Описание
Тип устройства	Выберите станцию ограждения или дверную станцию в зависимости от места установки.
Здание №	Установите флажок и введите номер здания, в котором установлен дверной блок.
Номер блока	Установите флажок, а затем введите номер устройства, в котором установлена дверная станция.
Нет.	• Номер должен состоять из 4 цифр. Первые 2 цифры должны быть 80, а последние 2 цифры начинаются с 01. Например, 8001. • Если в одном подразделении существует несколько ВТО, номер ВТО не может быть повторено.
Центр управления	Номер телефона по умолчанию при звонке оператора ВТО в службу ВТС — 888888. Оставьте значение по умолчанию.

Шаг 3. Нажмите «Применить».

После настройки имя пользователя на странице «Домофон > SIP-сервер» автоматически обновляется.
При добавлении устройства на платформу управления убедитесь, что имя пользователя совпадает с номером вызова.

3.7.4 Настройка параметров вызова

Вы можете настроить функции вызова и дверного звонка.

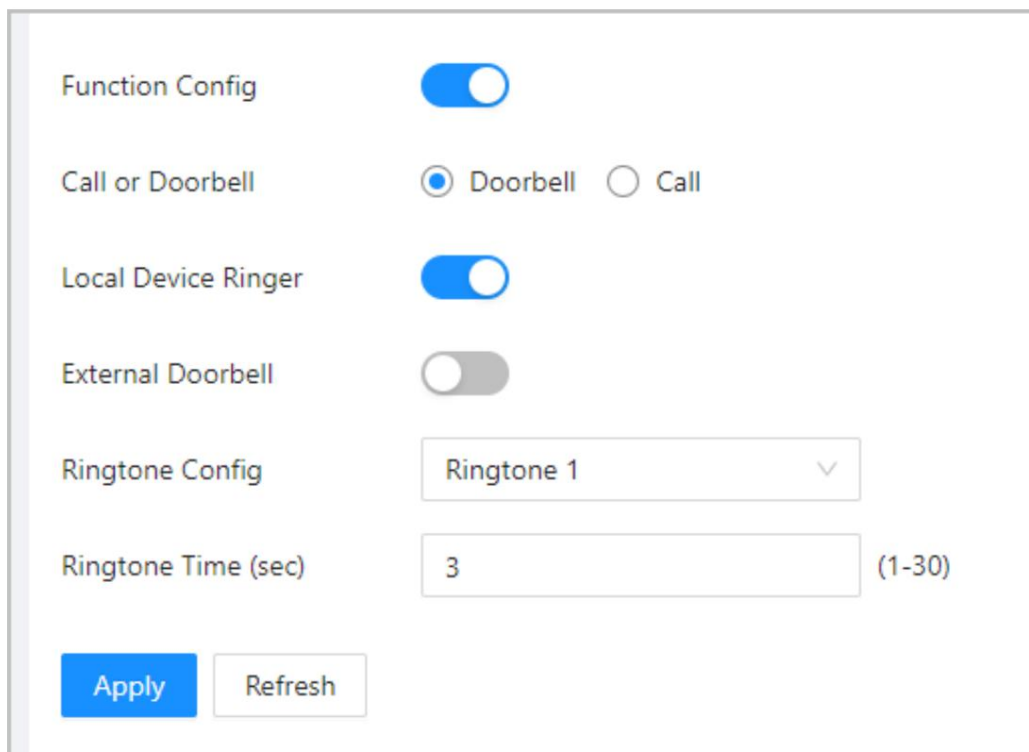
Процедура

Шаг 1. Выберите «Настройки домофона» > «Настройка вызовов».

Шаг 2. Включить настройку функций.

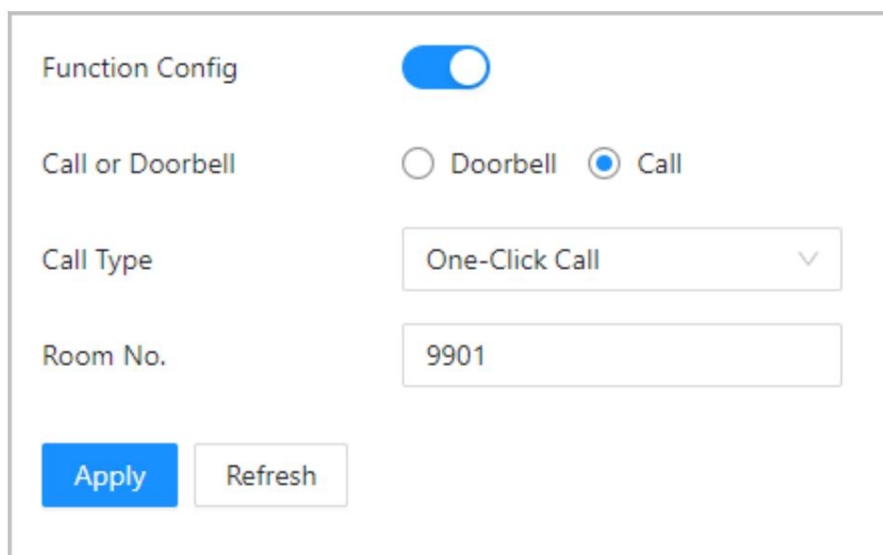
Шаг 3. Выберите «Вызов» или «Дверной звонок», а затем настройте параметры.

Рисунок 3-16. Настройка дверного звонка.



The screenshot shows a configuration window titled 'Function Config' with a blue toggle switch turned on. Below it, the 'Call or Doorbell' section has two radio buttons: 'Doorbell' (selected) and 'Call'. The 'Local Device Ringer' section has a blue toggle switch turned on. The 'External Doorbell' section has a grey toggle switch turned off. The 'Ringtone Config' section features a dropdown menu currently showing 'Ringtone 1'. The 'Ringtone Time (sec)' section has a text input field containing the number '3', with '(1-30)' indicating the valid range. At the bottom, there are two buttons: 'Apply' (blue) and 'Refresh' (white).

Рисунок 3-17. Настройка вызова.



The screenshot shows a configuration window titled 'Function Config' with a blue toggle switch turned on. Below it, the 'Call or Doorbell' section has two radio buttons: 'Doorbell' and 'Call' (selected). The 'Call Type' section features a dropdown menu currently showing 'One-Click Call'. The 'Room No.' section has a text input field containing the number '9901'. At the bottom, there are two buttons: 'Apply' (blue) and 'Refresh' (white).

Таблица 3-14. Описание параметров вызова и дверного звонка.

Параметр	Описание
Вызов	• Тип вызова : Вы можете выбрать «Вызов в один клик» или «Управление вызовом». Центр. • Номер комнаты : Если вы выберете «Звонок в один клик», вам необходимо указать номер комнаты.
Дверной звонок	• Локальный звонок : управляет воспроизведением мелодии звонка через встроенный динамик устройства. • Внешний дверной звонок : управляет отправкой сигнала звонка на внешний дверной звонок. Необходимо переключить выходной порт сигнализации на порт дверного звонка. • Настройка мелодии звонка : выбирает мелодию звонка, воспроизводимую при нажатии кнопки. Устройство сработало. • Время воспроизведения мелодии звонка (сек) : Настройте продолжительность воспроизведения мелодии звонка.

Шаг 4. Нажмите «Применить».

3.8 Настройка контроля доступа

3.8.1 Параметры контроля доступа

3.8.1.1 Настройка основных параметров

Процедура

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

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

Рисунок 3-18. Основные параметры

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

☐

Таблица 3-15. Описание основных параметров.

Параметр	Описание
Имя	Название двери.

Параметр	Описание
Состояние двери	Установите статус двери. - Обычный режим: Дверь будет запирается и отпираться в соответствии с вашими настройками. - 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.  Если период работы обычно открыт и период закрытия конфликтуют, то период работы обычно открыт имеет приоритет над периодом закрытия. • Если генеральный план конфликтует с планом праздников, то план праздников имеет приоритет над генеральным планом.
Обычно закрытый период	
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 дверь обычно открывается, и создаются записи. В течение заданного периода, если вы повторно проведете картой для проверки, дверь открыться не удастся, и записи не будут созданы. 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.

Шаг 3. Нажмите «Применить».

3.8.1.2 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 3-19. Комбинированная разблокировка.

The screenshot shows the 'Unlock Settings' window with the following configurations:

- Unlock Method:** Combination Unlock
- Combination Method:** Or (selected)
- Unlock Method (Multi-select):** Card, Fingerprint, Face, Password, Bluetooth Card (all checked)
- Bluetooth Mode:** Long-range (selected)
- PIN Code Authentication:** Enabled (toggle)
- Door Unlocked Duration:** 3.0 s (range 0.2-600)
- Remote Verification:** Enabled (toggle)
- Remote Verification Unlock Period:** General Plan, Disabled
- Holiday Plan:** Disabled
- Unlock Code:** [Empty field with copy icon]

• 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 3-20 Добавить группу

Add

No.1

Unlock Method ...Card x

Valid No.1

Select PersonUser ID/Name

No.	User ID	Name
☒	1	1000... 10000001
☒	2	1000... 10000002
☐	3	1000... 10000003
☐	4	1000... 10000004
☐	5	1000... 10000005

Selected PeopleClear

No.	User ID	Name	Operation
1	100000...	100000...	
2	100000...	100000...	

OK

Cancel

Рисунок 3-21. Разблокировка несколькими пользователями.

Unlock Settings

Unlock MethodUnlock 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 Duration20s (10-60)

Bluetooth Mode

Short-range

Long-range

PIN Code Authentication

Door Unlocked Duration

3.0s (0.2-600)

Remote Verification

Remote Verification Unlock Period

General PlanDisabled

Holiday PlanDisabled

Unlock Code

Таблица 3-16. Описание настроек разблокировки.

Параметр	Описание
Проверка нескольких человек Длительность тайм-аута разблокировки	В процессе проверки интервал между каждыми двумя проверяющими должен находиться в пределах этого временного периода.

28

Параметр	Описание
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.
Режим Bluetooth	Выберите радиус действия Bluetooth. Вы можете выбрать дальний или ближний радиус действия. Режим Bluetooth поддерживается только для моделей, оснащенных функцией Bluetooth.
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 с помощью соответствующих параметров пульта дистанционного управления.
Удалённая проверка разблокировки Период	

• Разблокировка по периодам

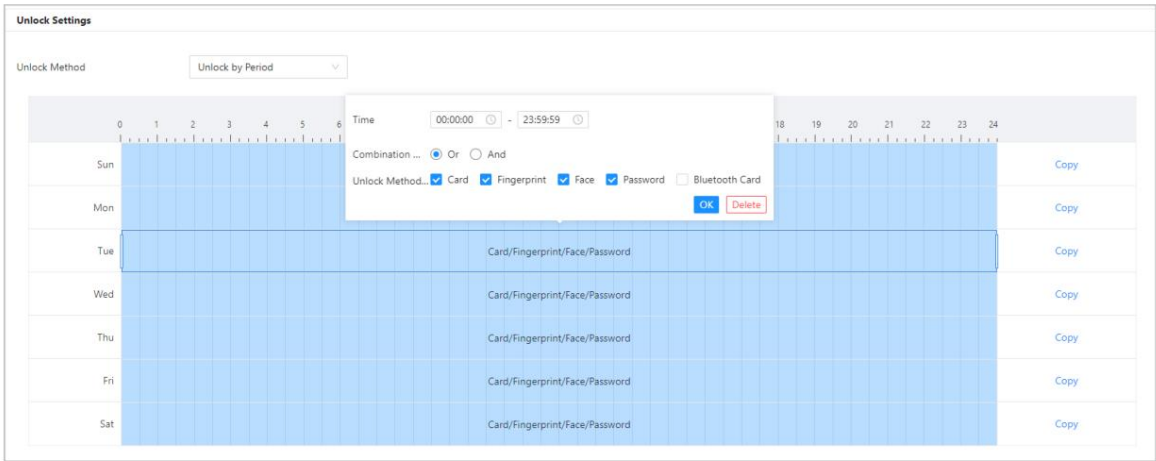
- 1. В списке «Способ разблокировки» выберите «Разблокировка по периоду».
- 2. Перетащите ползунок, чтобы отрегулировать временной период для каждого дня.



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 3-22. Разблокировка по периодам.



Шаг 3. Нажмите «Применить».

3.8.2 Сигнализация

3.8.2.1 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 3-23. Выберите канал.

Door Channel

1

Шаг 3. Настройка параметров сигнализации.

Рисунок 3-24 Сигнал тревоги

Duress Alarm

Anti-passback

Door Detector

NCNO

Intrusion Alarm

Unlock Timeout Alarm

Unlock Timeout

60

s (1-9999)

Excessive Attempts Ala...

Apply

Refresh

Default

Таблица 3-17. 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.
Сигнал тревоги о чрезмерном количестве попыток	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании нелегальной карты, которая будет гореть в течение определенного времени.

Шаг 4. Нажмите «Применить».

3.8.2.2 Настройка связи между сигналами тревоги (необязательно)

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 сигнализации.

Рисунок 3-25. Связь сигналов тревоги.

Modify

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

When the heat alarm signal disappears, the door will automatically return to the normal authentication mode.

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.

- 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 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.

- **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 7. Выберите тип канала.

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

Шаг 8. Нажмите ОК.

3.8.2.3 Настройка связи между событиями тревоги

Процедура

Шаг 1. Выберите «Контроль доступа» > «Сигнализация» > «Связывание событий тревоги».

Шаг 2. Настройте связи между событиями тревоги, а затем нажмите «Применить».

Рисунок 3-26. Связь событий тревоги.

Intrusion Alarm Linkage ☒ **Please enable Intrusion Alarm.**

Buzzer ☒ Enable Duration 15 s (1-1800)

Link Alarm Output ☒ Enable Duration 15 s (1-1800)

Unlock Timeout Alarm Linkage ☒ **Please enable Unlock Timeout Alarm.**

Buzzer ☒ Enable Duration Custom Time 15 s (1-1800)

Link Alarm Output ☒ Enable Duration Custom Time 15 s (1-1800)

Max Use Alarm Link ☒

Buzzer ☒ Enable Duration 15 s (1-1800)

Link Alarm Output ☒ Enable Duration 15 s (1-1800)

Tamper Alarm Linkage ☒

Buzzer ☒ Enable Duration 3 s (1-1800)

Link Alarm Output ☐ Enable Duration 15 s (1-1800)

Buttons: Apply Refresh Default

Таблица 3-18. Связь событий тревоги.

Параметр	Описание
Связь с охранной сигнализацией	Если дверь откроется ненормально, сработает охранная сигнализация. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении вторжения. Вы можете настроить продолжительность сигнала тревоги. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает охранная сигнализация. Вы можете настроить продолжительность тревоги.
Сигнализация об истечении времени разблокировки Связь	Если дверь остается незапертой дольше заданного времени, сработает сигнализация об истечении времени ожидания, которая будет действовать в течение заданного времени. • Звуковой сигнал: Звуковой сигнал срабатывает, когда истекает время ожидания разблокировки. Сработало. Длительность поддерживает пользовательское время и устанавливается до блокировки двери. ◇ До закрытия двери: Звук сигнализации прекращается после закрытия двери. ◇ Настраиваемое время: Вы можете установить продолжительность. • Локальный вывод сигналов тревоги: Внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнал тревоги об истечении времени разблокировки. Поддерживается установка пользовательского времени и установка параметра «До блокировки двери». ◇ До закрытия двери: После закрытия двери звуковой сигнал тревоги прекращается. ◇ Настраиваемое время: Вы можете указать продолжительность.
Ссылка на оповещение о максимальном использовании	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. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении чрезмерного использования. Длительность срабатывания сигнала можно настроить. • Выходной сигнал тревоги: Внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнал тревоги об истечении времени разблокировки. Вы можете настроить продолжительность сигнала тревоги.
Связь сигнализации о несанкционированном доступе	Сигнализация о попытке взлома срабатывает, когда кто-то пытается физически повредить устройство. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении попытки взлома. Вы можете настроить продолжительность сигнала тревоги. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнализация о несанкционированном доступе. Вы можете настроить продолжительность срабатывания сигнализации.

3.8.3 Настройка параметров лица

Настройте параметры распознавания лиц. Параметры распознавания лиц могут различаться в зависимости от модели устройства.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Параметры распознавания лиц».

Рисунок 3-27 Параметры обнаружения лиц



Recognition

Exposure

Face Recognition Threshold85(0-100)

Max Face Recognition Angl...30(0-90)

Anti-spoofing Level

Close

General

High

Ultra High

Valid Face Interval (sec)3(1-60)

Invalid Face Interval (sec)10(0-60)

Recognition Distance1.5m

Mask modeNot Detect

Mask Recognition Threshold75(0-100)

Snapshot Mode

Face Snapshot Enhancement

Beautifier

Enable Helmet Detection

Target Filter

Min Size256 * 256

Draw TargetClear

Detection Area

Detection AreaClear

ApplyRefreshDefault

Шаг 3. Настройте параметры.

Таблица 3-19. Описание параметров лица.

Имя	Описание
Порог распознавания лиц	Настройте уровень точности распознавания лиц. Более высокий порог означает более высокую точность и меньший процент ложных срабатываний.  Если пороговое значение слишком низкое, например, равно 0, то частота ложных срабатываний будет чрезвычайно высокой. Обратите внимание.
Максимальный угол распознавания лиц Отклонение	Задайте максимальный угол, под которым можно расположить лицо для распознавания. Чем больше значение, тем шире диапазон углов наклона грани. Если угол наклона грани выходит за пределы заданного диапазона, она может быть обнаружена неправильно.
Уровень защиты от подделки	После включения эта функция предотвращает использование фотографий, видео, масок и других заменителей для получения несанкционированного доступа. После включения этой функции рамка с лицом не отображается при проверке подлинности неживого объекта.

Имя	Описание
Интервал между полями для заполнения (сек)	Если после первого успешного распознавания перед объективом остается то же лицо, устройство повторно выполнит распознавание лица через определенный промежуток времени.
Неверный интервал между предъявлениями лиц (сек)	Если после первой неудачной попытки распознавания перед объективом остается то же лицо, устройство повторно выполнит распознавание лица через определенный промежуток времени. Если вы укажете 0, лицо не будет распознано, и записи о разблокировке не будут созданы.
Расстояние распознавания	Расстояние между лицом и линзой.
Режим маски	• Не обнаружено : Маска не обнаружена во время распознавания лица. • Предупреждение о маске : Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, но доступ будет разрешен. • Требуется маска : Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, и доступ будет запрещен.
Порог распознавания маски	Чем выше пороговое значение, тем точнее будет распознавание лица, когда человек носит маску, и тем ниже будет частота ложных срабатываний.
Режим моментального снимка	После включения этой функции можно отфильтровать снимки низкого качества из записей о разблокировке.
Улучшение снимков лица	После включения этой функции снимки в записях разблокировки отображаются в улучшенном виде.
Украшение	Улучшите качество захваченных изображений лиц.
Включить обнаружение шлема	Обнаруживает защитные каски. Дверь не откроется, если человек не в каске.

Шаг 4. Настройте параметры экспозиции.

Рисунок 3-28 Параметры экспозиции

Recognition

Exposure

Face Exposure ☒

Face Target Brightness (0-100)

Face Exposure Interval Dete... s (1-28800)

Таблица 3-20. Описание параметров воздействия.

Параметр	Описание
Открытое лицо	После включения функции экспозиции лица, лицо будет экспонироваться с заданной яркостью для четкого отображения изображения.
Яркость мишени лица	
Обнаружение интервала экспозиции лица	Лицо будет показано лишь один раз в течение определенного промежутка времени.

Шаг 5. Нарисуйте область обнаружения лица.

1. Область обнаружения кликов .
2. Щелкните правой кнопкой мыши, чтобы нарисовать область обнаружения, а затем отпустите левую кнопку мыши, чтобы завершить рисование.

Лицо в заданной области будет обнаружено.

Шаг 6. Нарисуйте целевой размер.

1. Нажмите «Нарисовать цель».
2. Нарисуйте прямоугольник распознавания лица, чтобы определить минимальный размер обнаруженного лица.

Только если размер лица превышает заданный размер, устройство может его распознать.

Шаг 7. Нарисуйте область обнаружения.

Шаг 8. Нажмите ОК.

3.8.4 Настройки карты

3.8.4.1 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 3-29 Параметры карты

Card Settings

M1 Card

M1 Card Encryption & Verification

ID Card

Block NFC Cards

DESFire Card

DESFire Card Decryption

Apply

Refresh

Default

Card No. System

After the number system is changed, the card numbers will become invalid.

Card No. System

Hexadecimal

Decimal

Apply

Refresh

Default

DESFire Card Write

Acquisition De...

Device

Please place the card on the swiping area and enable DESFire card and DESFire Card Decryption.

Card Number

Write

Таблица 3-21. Описание параметров карты.

Элемент	Параметр	Описание
Настройки карты	Карта M1	При использовании этой функции карту M1 можно считать. включено.

38

Элемент	Параметр	Описание
	Шифрование карты M1 и Проверка	При включении этой функции можно считать только зашифрованную IC-карту.  Убедитесь, что карта M1 активирована.
	Удостоверение личности	При включении этой функции удостоверение личности можно считать.  Эта функция доступна только на некоторых моделях.
	Блокировка NFC-карт	После включения этой функции разблокировка с помощью дубликата NFC-карты будет исключена.  • Убедитесь, что карта M1 активирована. • Функция NFC доступна только на некоторых моделях телефонов.
	Карта Defire	При включении этой функции устройство может считывать номер карты Defire.  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» .  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».

3.8.4.2 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 3-30. 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 3-22. 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 ведущий ноль к фиксированной длине числа. Например, если введенный вами 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 добавляется в качестве кода объекта. Таким образом, окончательный номер карты будет 000056.

3.8.4.3 Настройка пользовательского преобразования

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 3-31. 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	1A2B3C4D	1A2B3C4D	1A2B3C4D	4D3C2B1A
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 3-32. Правило конвертации импорта.

Enable ☒

Matching Mode ☐ Auto Match ☒ Import Conversion Rule

Version 2025-03-31

Upload File

Default

You can only upload files in zip format and the size must not exceed 1 MB.

3.8.5 Настройка QR-кода

Процедура

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

Рисунок 3-33 QR-код

Enable QR Code Exposure

QR Code Brightness

50

QR Code Exposure Interval (sec)

2

(1-28800)

QR Code Validity Period (sec)

600

(0-86400)

Apply

Refresh

Default

Таблица 3-23 Параметры QRR-кода

Параметры	Описание
Включить отображение QR-кода	QR-код будет отображаться с заданной яркостью, и его можно будет распознать и четко прочитать.
Яркость QR-кода	
Интервал показа QR-кода (сек)	QR-код будет показан только один раз в течение заданного интервала времени.
Срок действия QR-кода (мин)	После генерации QR-кода срок его действия будет определяться в течение определенного времени, после чего он истечет.  Сроки действия QR-кодов в QR Code Validity Period, DSS Pro и Dolyнк имеют приоритет друг над другом. Это означает, что платформа, которая последней внесла изменения во время действия кода, будет иметь приоритет над своей последней конфигурацией, а первоначальный срок действия будет аннулирован.

3.8.6 Настройка периодов

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

3.8.6.1 Настройка общего плана

Вы можете настроить до 128 периодов времени (от №0 до №127). В каждом периоде необходимо настроить расписание доступа к двери 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».

Add

X

No.

0

General Plan Name

Plan 1

Time Plan

Time

12:30:00

-

23:59:59

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

3.8.6.2 Настройка плана отпусков

Процедура

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

Рисунок 3-35. 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 ОК.

Рисунок 3-36. Добавить праздник в группу праздников.

Edit

Holiday Name

* Period →

Шаг 4. Нажмите ОК.

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 течение дня.

Рисунок 3-37. Добавить план отпуска.

Шаг 6. Нажмите OK.

3.8.7 Настройки конфиденциальности

Процедура

Шаг 1. На веб-странице выберите «Контроль доступа» > «Настройки конфиденциальности».

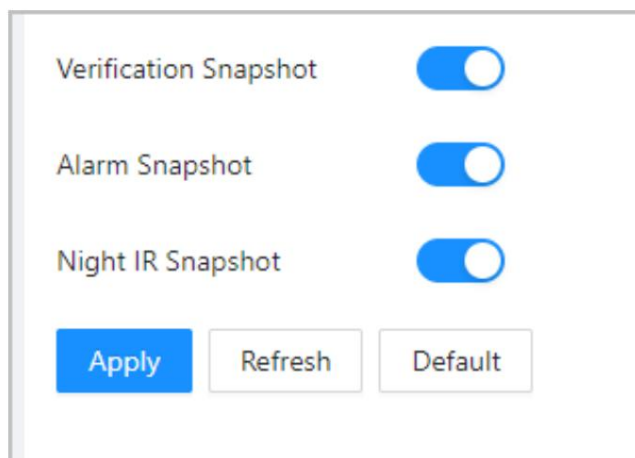
Шаг 2. Включите необходимую функцию.

- Снимок лица для проверки: изображения лиц будут автоматически считываться при разблокировке устройства. дверь.
- Снимок тревоги: При включении этой функции снимки будут создаваться при срабатывании сигнализации. Обратная передача данных, принуждение, черный список и несанкционированные чрезмерные попытки. По умолчанию отключено.
- Ночные ИК-снимки: четкие изображения можно получить при слабом освещении или в полной темноте.



- Если включена функция «Проверочный снимок», функция «Ночной ИК-снимок» будет включена автоматически. Днём функция «Проверочный снимок» использует захват белого света, а ночью — ИК-снимок. Если отключена только функция «Ночной ИК-снимок», функция «Проверочный снимок» будет использовать захват белого света как днём, так и ночью.
- При включении функции «Снимок тревоги» функция «Ночной ИК-снимок» будет включена автоматически. В дневное время функция «Снимок тревоги» использует захват белого света, а ночью — ИК-излучение. Если отключен только «Ночной ИК-снимок», функция «Снимок тревоги» будет использовать захват белого света как днем, так и ночью. • Если включены функции «Проверочный снимок», «Снимок тревоги» и «Ночной ИК-снимок», и обе функции отключены, функция «Ночной ИК-снимок» будет автоматически скрыта.

Рисунок 3-38 Настройки конфиденциальности



Шаг 3. Нажмите «Применить».

3.8.8 Настройка функций выходного порта

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



• 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 выходного порта».

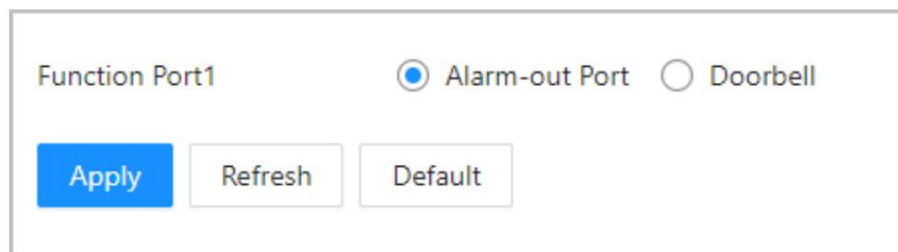
Шаг 2. Выберите тип порта.



Если кабель сигнализации и кабель дверного звонка используются совместно, настройте интерфейс на подключение к дверному звонку, чтобы гарантировать срабатывание звонка.

Шаг 3. Нажмите «Применить».

Рисунок 3-39. Настройка портов.



3.8.9 Настройка сравнения на стороне бэкэнда

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.

Выберите «Контроль доступа» > «Сравнение серверных частей».

Рисунок 3-40. Сравнение бэкэндов.

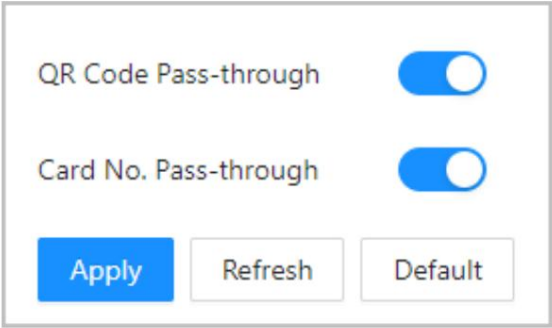


Таблица 3-24. Сравнение бэкэндов.

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.

3.8.10 Настройка разблокировки режима от первого лица

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

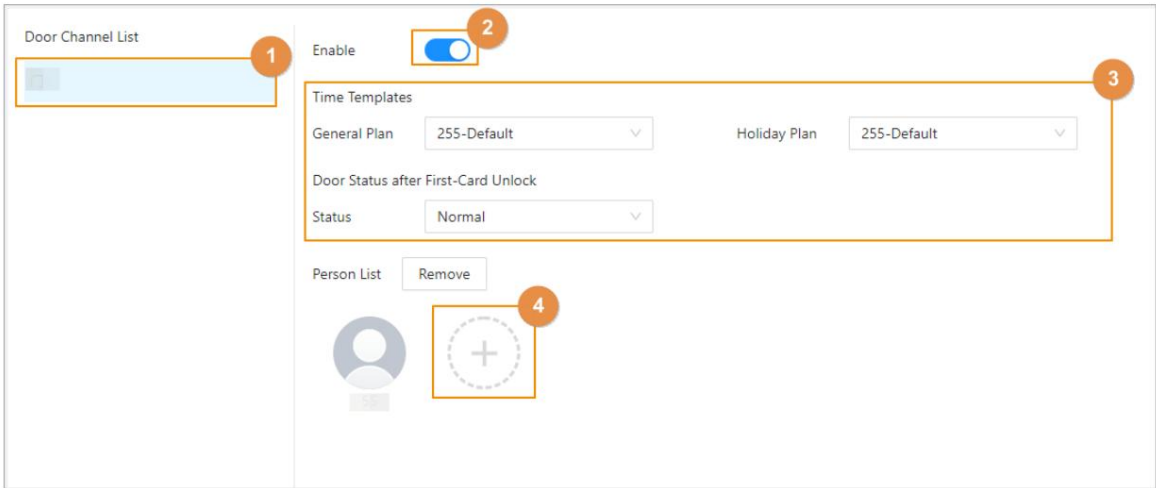
Предварительные требования

- Персонажей можно назначать в качестве персонажей от первого лица только в том случае, если у них есть права доступа к дверям.
- В качестве первого пользователя могут быть назначены только обычные пользователи.
 - После подтверждения личности первым пользователем, если устройство перезагрузится, первому пользователю необходимо будет пройти повторную проверку. Идентификация снова.
 - После включения этой функции сотрудники патрульной службы могут в обычном режиме отмечать время начала и окончания работы.

Процедура

- Шаг 1. Выберите «Контроль доступа» > «Разблокировка от первого лица».
- Шаг 2. Выберите дверной канал, а затем активируйте функцию.

Рисунок 3-41. Разблокировка от первого лица.



Шаг 3. Настройте параметры.

Таблица 3-25. 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».

3.9 Настройка аудио и видео

3.9.1 Настройка видео

Процедура

Шаг 1. Выберите «Настройка аудио и видео» > «Видео».

Шаг 2. Настройте битрейт.

Рисунок 3-42. Битрейт

Bit Rate

Status

Exposure

Image

Main Stream

Resolution720P

Frame Rate (FPS)30

Bit Rate1024Kbps

CompressionH.264

Sub Stream

ResolutionVGA

Frame Rate (FPS)30

Bit Rate1024Kbps

CompressionH.264

Default

Snapshot

Таблица 3-26. Описание скорости передачи данных.

Параметр		Описание
Основной формат	Разрешение	Когда устройство функционирует как VTO и подключается к VTH, ограничение на размер получаемого потока VTH составляет 720р. При изменении разрешения на 1080р это может повлиять на работу функций вызова и мониторинга.
	Частота кадров (FPS)	Количество кадров (или изображений) в секунду.
	Битрейт	Объем данных, передаваемых по интернет-соединению за определенный промежуток времени. Выберите подходящее значение в зависимости от скорости вашей сети.
	Сжатие	Стандарт сжатия видео, обеспечивающий хорошее качество видео при более низких битрейтах.
Подпоток	Разрешение	Дополнительный поток поддерживает D1, VGA и QVGA.
	Частота кадров (FPS)	Количество кадров (или изображений) в секунду.
	Битрейт	Это указывает на объем передаваемых данных. через интернет-соединение за определенный промежуток времени.
	Сжатие	Стандарт сжатия видео, обеспечивающий хорошее качество видео при более низких битрейтах.

Шаг 3. Настройте статус.

Рисунок 3-43. Статус

The screenshot shows a settings interface with a sidebar on the left containing 'Bit Rate', 'Status' (highlighted), 'Exposure', and 'Image'. The main panel displays the following settings:

- Scene Mode: Auto
- Day/Night: Color
- Compensation Mode: WDR
- Brightness slider: Set to 30
- Video Standard: NTSC

Таблица 3-27. Описание параметров состояния.

Параметр	Описание
Режим сцены	Оттенок изображения различается в зависимости от режима съемки. • Закрыть : Функция режима сцены отключена. • Авто : Система автоматически регулирует режим сцены в зависимости от... на основе фоточувствительности. • Солнечный : В этом режиме оттенок изображения будет уменьшен. • Ночной : В этом режиме оттенок изображения будет увеличен.
День/Ночь	Режим «День/Ночь» влияет на компенсацию освещенности в разных ситуациях. • Авто : Система автоматически регулирует дневной/ночной режим в зависимости от светочувствительности. • Цветной : В этом режиме изображения получают цветными. • Черно-белый : В этом режиме изображения отображаются в черно-белом цвете.
Режим компенсации	• Отключить : Компенсация выключена. • BLC : Компенсация подсветки автоматически увеличивает освещенность темных участков изображения, когда яркий свет, падающий сзади, заслоняет их. • WDR : Система затемняет светлые участки и компенсирует темные, создавая баланс для улучшения общего качества изображения. • HLC : Компенсация подсветки (HLC) — это технология, используемая в Камеры видеонаблюдения/IP-камеры предназначены для обработки изображений, снятых при освещении, например, фарами или прожекторами. Датчик изображения камеры обнаруживает яркие источники света в видео и уменьшает экспозицию в этих местах для повышения общего качества изображения.
Видеостандарт	Выберите один из стандартов: PAL или NTSC.

Шаг 4. Настройте параметры экспозиции.

Рисунок 3-44. Воздействие

Bit Rate

Status

Exposure

Image

Anti-flicker

Outdoor

Exposure Mode

Manual

Shutter

Custom Range

Shutter Range

0

-

20

(0-40)ms

Gain

0

-

80

(0-100)

Exposure Compensation

-

+

50

3D NR

NR Level

-

+

50

Таблица 3-28. Описание параметров воздействия.

Параметр	Описание
Защита от мерцания	Установите функцию подавления мерцания, чтобы уменьшить мерцание и снизить неравномерность цветопередачи. контакт. • 50 Гц : При частоте электросети 50 Гц воздействие составляет Автоматическая регулировка в зависимости от яркости окружающей среды для предотвращения появления горизонтальных линий. • 60 Гц : При частоте электросети 60 Гц экспозиция Автоматическая регулировка в зависимости от яркости окружающего освещения для уменьшения появления горизонтальных линий. • На улице : При выборе режима «На улице» можно выбрать режим экспозиции. переключилось.

Параметр	Описание
Режим экспозиции	Вы можете настроить экспозицию для регулировки яркости изображения. • Автоматический режим : Устройство автоматически регулирует яркость изображений, исходя из окружающей обстановки. • Приоритет выдержки : Устройство регулирует яркость изображения в соответствии с заданным диапазоном выдержки. Если изображение недостаточно яркое, но значение выдержки достигло верхнего или нижнего предела, устройство автоматически отрегулирует значение усиления для достижения оптимального уровня яркости. • Ручной режим : Вы можете вручную отрегулировать усиление и значение выдержки для регулировки яркости изображения.  ◇ При выборе пункта «На открытом воздухе» в списке «Защита от мерцания» можно выбрать режим приоритета выдержки . ◇ Режим экспозиции может отличаться в зависимости от модели устройства.
Затвор	Затвор — это элемент, пропускающий свет в течение определенного времени. Чем больше выдержка, тем короче время экспозиции и тем темнее изображение. Вы можете выбрать диапазон выдержек или добавить собственный диапазон.
Прирост	При установке диапазона значений усиления качество видео улучшится.
Контакт Компенсация	Видео станет ярче, если отрегулировать значение компенсации экспозиции.
3D NR	При включении функции 3D-шумоподавление (RD) можно уменьшить видеосум, чтобы обеспечить более высокое разрешение видео.
Уровень NR	При включении этой функции можно установить уровень детализации изображения. Более высокий уровень детализации означает более четкое изображение.

Шаг 5. Настройте образ.

Рисунок 3-45 Изображение

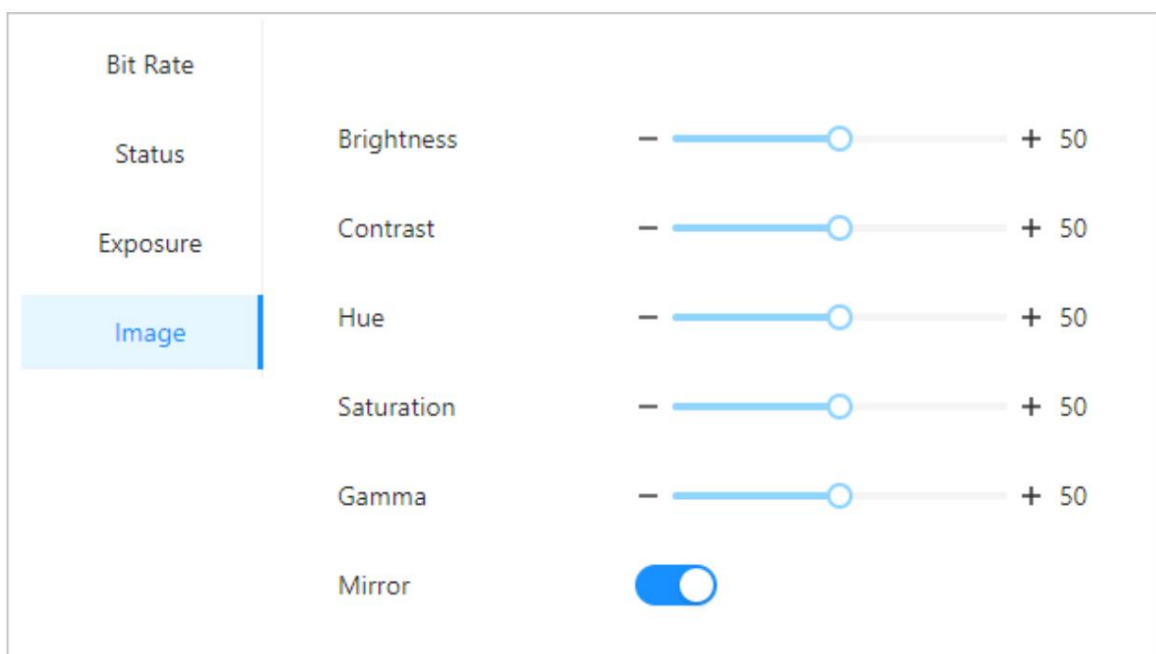


Таблица 3-29. Описание изображения.

Параметр	Описание
Яркость	Яркость изображения. Чем выше значение, тем ярче изображение.
Контраст	Контраст — это разница в яркости или цвете, которая позволяет различить объект. Чем выше значение контраста, тем больше будет цветовой контраст.
Оттенок	Относится к интенсивности или насыщенности цвета. Описывает яркость цвета или его чистоту.
Насыщенность	Насыщенность цвета указывает на интенсивность цвета в изображении. Чем выше насыщенность, тем насыщеннее цвет, например, тем больше в нем красного или синего.  Значение насыщенности не изменяет яркость изображения.
Гамма	Изменяйте яркость и контрастность изображения нелинейным способом. Чем выше значение, тем ярче изображение.
Зеркало	При включении этой функции изображения будут отображаться с перевернутыми левой и правой сторонами. Экран устройства не поддерживает настройку и всегда отображает зеркальное изображение.

Связанные операции

- По умолчанию: Нажмите «По умолчанию», и параметры на этой странице будут восстановлены до значений по умолчанию.
- Снимок экрана: Нажмите «Снимок экрана», чтобы сделать снимок экрана текущего устройства.

3.9.2 Настройка аудиоподсказок

Настройте звуковые подсказки во время подтверждения личности.

Процедура

Шаг 1. Выберите «Настройка аудио и видео» > «Аудио».

Шаг 2. Настройте параметры звука.

Рисунок 3-46. Настройка параметров звука.

Audio Config

Speaker Volume

80

(0-100) ?

Microphone Volume

90

(0-100) ?

Audio Collection

Enable

▼

Only supports MP3 files that are less than 100 KB with a sampling rate of 16K.

Audio File

Audio Type	Audio File	Modify
Successfully verified.	-	⬆️
Failed to verify.	-	⬆️
Not wearing face mask.	-	⬆️

DND Mode

Apply

Refresh

Default

Таблица 3-30. Описание параметров.

Параметры	Описание
Громкость динамика	Установите громкость динамика.
Громкость микрофона	Установите громкость микрофона.
Аудиоколлекция	Если эта функция включена, звук из микрофона устройства будет Запись производилась в режиме реального времени и во время видеозаписи.
Аудиофайл	Вы можете загружать аудиофайлы на устройство.
Режим «Не беспокоить»	В течение установленного времени при подтверждении вашей учетной записи голосовые подсказки не звучат. Идентификатор устройства. Можно установить до 4 периодов.

Шаг 3. Нажмите, чтобы загрузить аудиофайлы на платформу для каждого типа аудио.



Поддерживаются только MP3-файлы размером менее 100 КБ с частотой дискретизации 16 кГц.

Шаг 4. Нажмите «Применить».

3.9.3 Настройка локального кода

Настройте область просмотра в видеообращении и предварительном просмотре.

Справочная информация



Эта функция включена по умолчанию при работе с VTH. Предварительный просмотр может быть недоступен, когда эта функция отключена.

Процедура

Шаг 1. Войдите на веб-страницу.

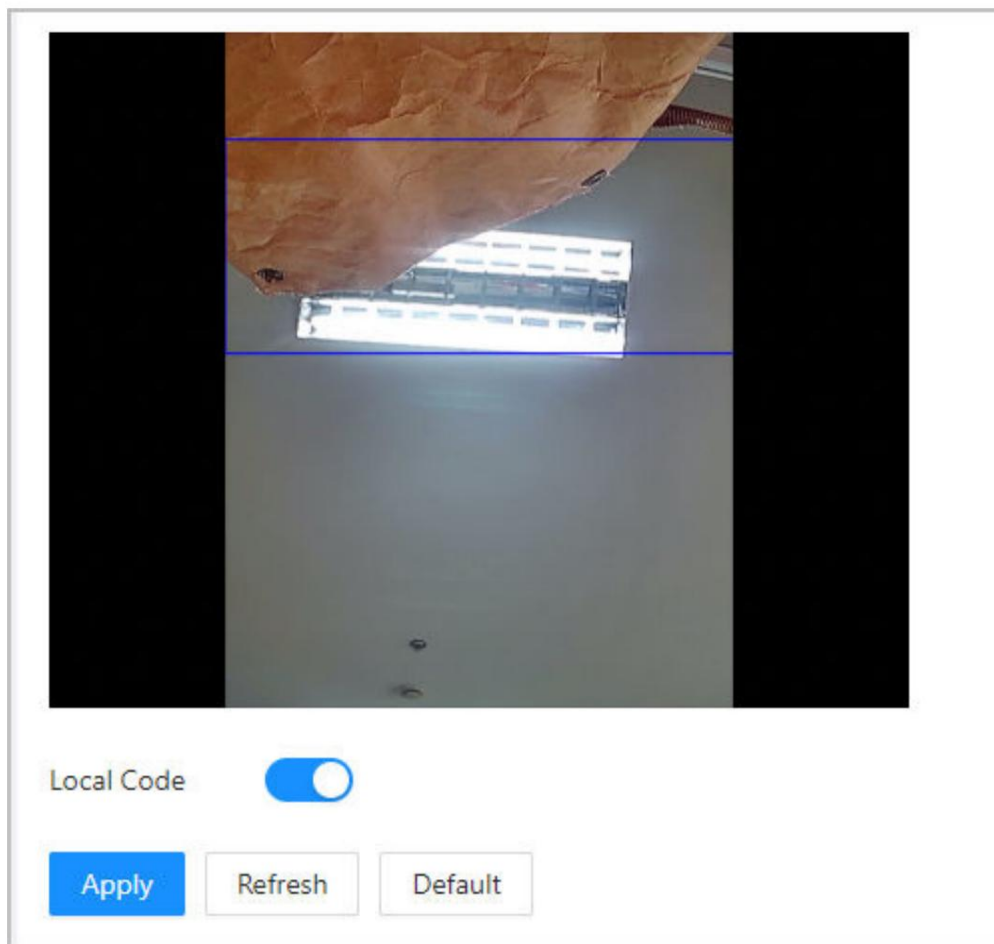
Шаг 2. Выберите «Настройка аудио и видео» > «Локальный код».

Шаг 3. Выберите «Включить», чтобы активировать функцию.

Шаг 4. Перетащите прямоугольник в указанное место.

В рамке указана область предварительного просмотра во время видеоконференции.

Рисунок 3-47 Локальное кодирование



Шаг 5. Нажмите «Применить».

3.10 Настройки связи

3.10.1 Сетевые настройки

3.10.1.1 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 3-48 TCP/IP

NIC

NIC 1

Mode

DHCP

Static

MAC Address

90 : 02 : : 51 : 9f

IP Version

IPv4

IP Address

172 . . 103

Subnet Mask

255 . . 0

Default Gateway

172 . . 1

Preferred DNS

8 . . 8

Alternate DNS

8 . . 4

MTU

1500

Transmission Mode

Multicast

Unicast

Apply

Refresh

Default

Таблица 3-31. 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.

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. • Для версий IPv6 не требуется установка 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, которые могут быть переданы в одном сетевом пакете в компьютерных сетях. По умолчанию он равен 1500.
Режим передачи	• Многоадресная рассылка: идеально подходит для видеозвонков. • Одноадресная передача: идеально подходит для групповых звонков.

Шаг 3. Нажмите OK.

3.10.1.2 Настройка Wi-Fi



• Функция Wi-Fi доступна только на некоторых моделях. • Wi-Fi и точка доступа Wi-Fi могут быть включены одновременно, при этом функция Wi-Fi включена по умолчанию.

Процедура

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

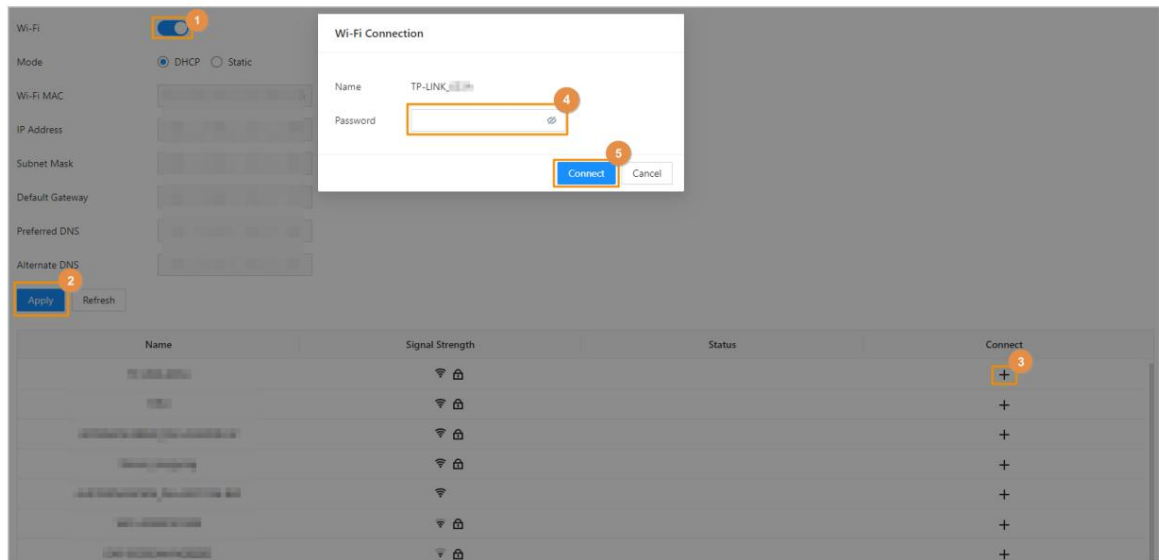
Шаг 2. Включите Wi-Fi, а затем нажмите «Применить».

Отображаются все доступные сети Wi-Fi.

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

Wi-Fi подключен.

Рисунок 3-49 Wi-Fi



Связанные операции

- DHCP: Включите эту функцию и нажмите «Применить», устройству 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.

3.10.1.3 Настройка точки доступа Wi-Fi



Wi-Fi и точка доступа Wi-Fi могут быть включены одновременно, при этом функция Wi-Fi включена по умолчанию.

Процедура

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

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

Рисунок 3-50 Точка доступа Wi-Fi

The screenshot shows a configuration page for a Wi-Fi access point. It features the following elements:

- Enable:** A toggle switch that is currently turned off.
- SSID:** A text input field containing a masked string.
- Security:** A dropdown menu showing a selected security protocol.
- Password:** A text input field with a masked password.
- IP Address:** A text input field with a masked IP address.
- QR Code:** A large QR code positioned below the IP address field, likely for quick configuration via a mobile app.
- Buttons:** Three buttons at the bottom: 'Apply' (blue), 'Refresh' (white), and 'Default' (white).

Результаты

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

3.10.1.4 Настройка порта

Вы можете одновременно ограничить доступ к устройству через веб-страницу, настольное приложение и мобильное приложение.

Процедура

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

Шаг 2. Настройте порты.



За исключением параметров Max Connection и RTSP Port, для вступления изменений в силу после изменения остальных параметров необходимо перезагрузить устройство.

Рисунок 3-51. Настройка портов.

Max Connection

50

(1-50)

TCP Port

37777

(1025-65535)

HTTP Port

80

HTTPS Port

443

RTSP Port

554

Apply

Refresh

Default

Таблица 3-32. 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.
Порт RTSP	Значение по умолчанию — 554.

Шаг 3. Нажмите «Применить».

3.10.1.5 Настройка основных служб

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

Процедура

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

Шаг 2. Настройка основных служб.

Рисунок 3-52. Базовое обслуживание.

SSH

Multicast/Broadcast Search

CGI

ONVIF

Outbound Protection of Service Pass...

There might be data leakage risk if this service is disabled.

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 3-33. 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.
Защита исходящих услуг Пароль	Убедитесь, что устройства и программное обеспечение, совместимые с VTO, могут оказывать свои услуги при включенной защите исходящих паролей сервиса . При отключении этой службы может возникнуть риск утечки данных.
Аварийное техническое обслуживание	Она включена по умолчанию.

Параметр	Описание
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.
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».

3.10.1.6 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.

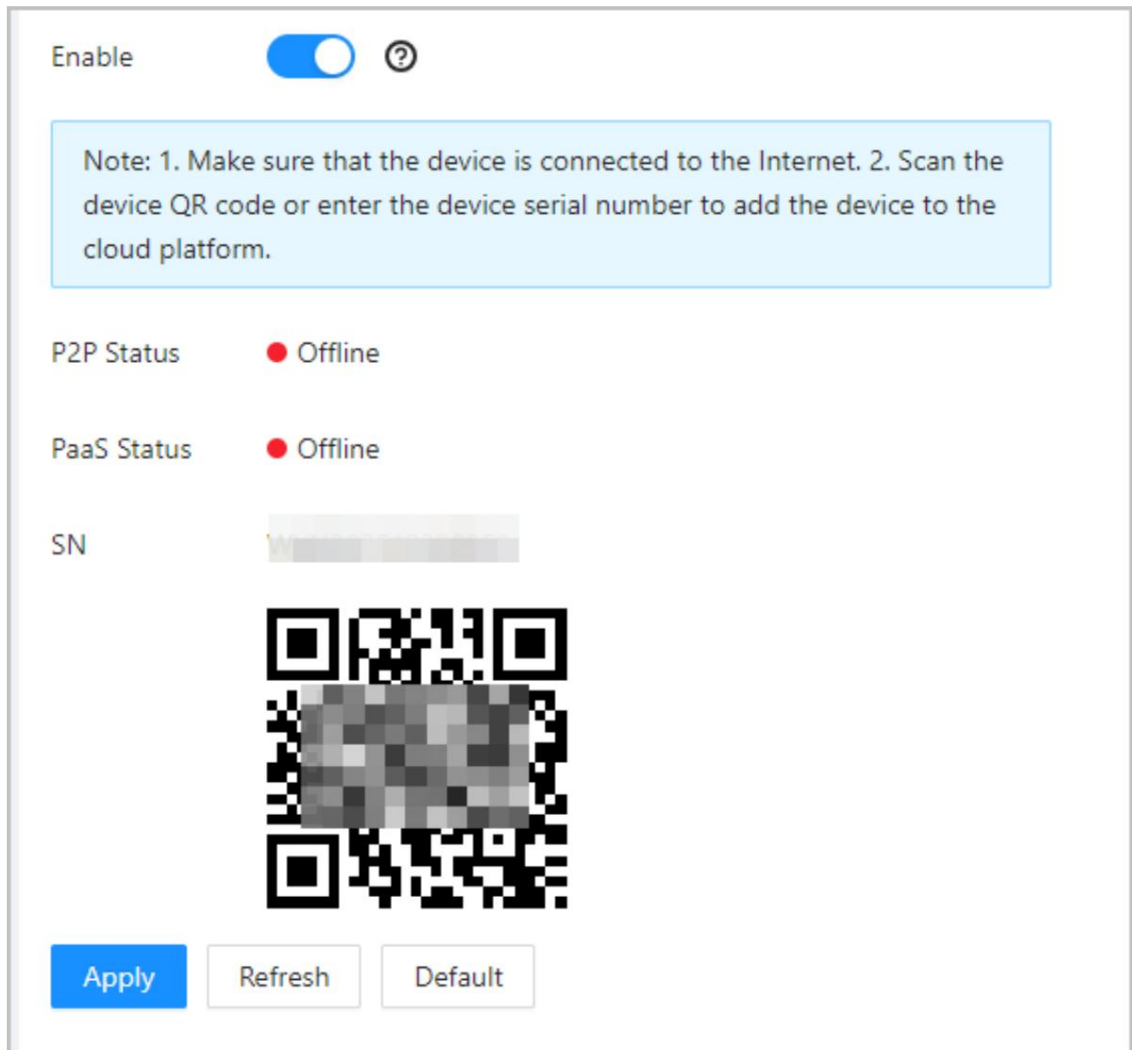
Процедура

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 3-53. Облачный сервис.



Шаг 3. Нажмите «Применить».

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

3.10.1.7 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 сети» > «Автоматическая регистрация SDK».

Шаг 2. Включите функцию автоматической регистрации и настройте параметры.

Рисунок 3-54. Регистрация автомобиля.

Enable

Status

Offline

Server Address

172.5.2.7

Port

7000

(1-65535)

Registration ID

none

Apply

Refresh

Default

Таблица 3-34. 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). Добавление устройства в систему. для управления путем ввода регистрационного идентификатора на платформе.

Шаг 3. Нажмите «Применить».

3.10.1.8 Настройка автоматических регистров CGI

Подключитесь к сторонней платформе через протокол CGI.

Справочная информация



Поддерживается только IPv4.

Процедура

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

Регистрация.

Шаг 2. Включите эту функцию, а затем настройте параметры.



Шаг 3 Нажмите , а затем настройте параметры.

Рисунок 3-55 Автоматическая регистрация CGI

Edit

X

Enable

☐

Device ID

none

Address Type

Host IP

▼

Host IP

10.0.0.1

Port

60005

HTTPS

☐

Username

Password

OK

Cancel

Таблица 3-35. Описание автоматической регистрации.

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

Шаг 4. Нажмите OK.

3.10.1.9 Настройка автоматической загрузки

Передавайте 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 3-56 Автоматическая загрузка

Push Person Info

Upload Mode

HTTP

Enable

Add

Delete

☐	No.	IP/Domain Name	Port	HTTPS	Path	Authenti- cation	Event Type	Test	Delete
☐	1	192.168.1.108	80		/		Person Info, Unlock Reco...	Test	

Apply

Refresh

Default

Таблица 3-36. 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 в систему необходимы имя пользователя и пароль.
Тип события	Выберите тип события, которое будет отправлено на платформу управления. • Перед использованием этой функции включите функцию «Передача информации о человеке». • Информация о человеке может быть передана только на одну платформу управления, а записи о разблокировке — на несколько платформ управления.

Шаг 5. Нажмите «Применить».

3.10.2 Настройки Bluetooth

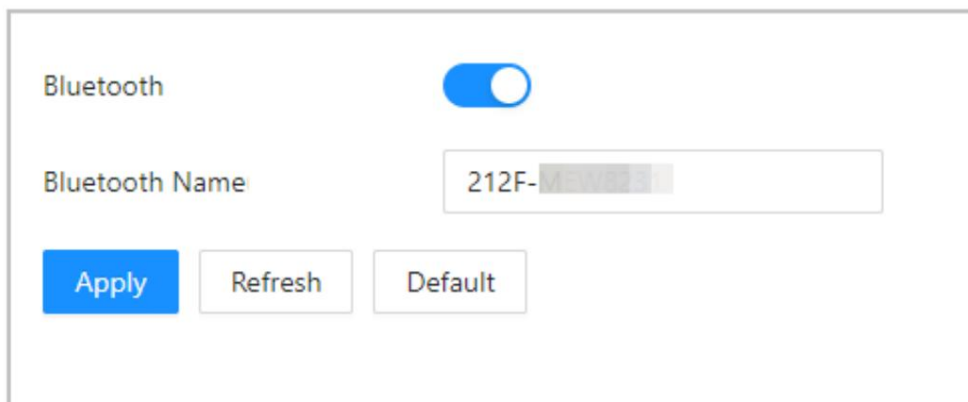
Настройте функцию Bluetooth устройства. Эта функция доступна только на некоторых моделях.

Процедура

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

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

Рисунок 3-57 Bluetooth



Шаг 3. Нажмите «Применить».

Результаты

Разблокировать дверь можно через Bluetooth с помощью приложения DMSS. Подробнее см. раздел "2.2.5 Разблокировка через Bluetooth".

3.10.3 Настройка RS-485

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

Процедура

Шаг 1. Выберите «Настройки связи» > «Настройки RS-485».

Шаг 2. Настройте параметры.

Рисунок 3-58. Настройка параметров.

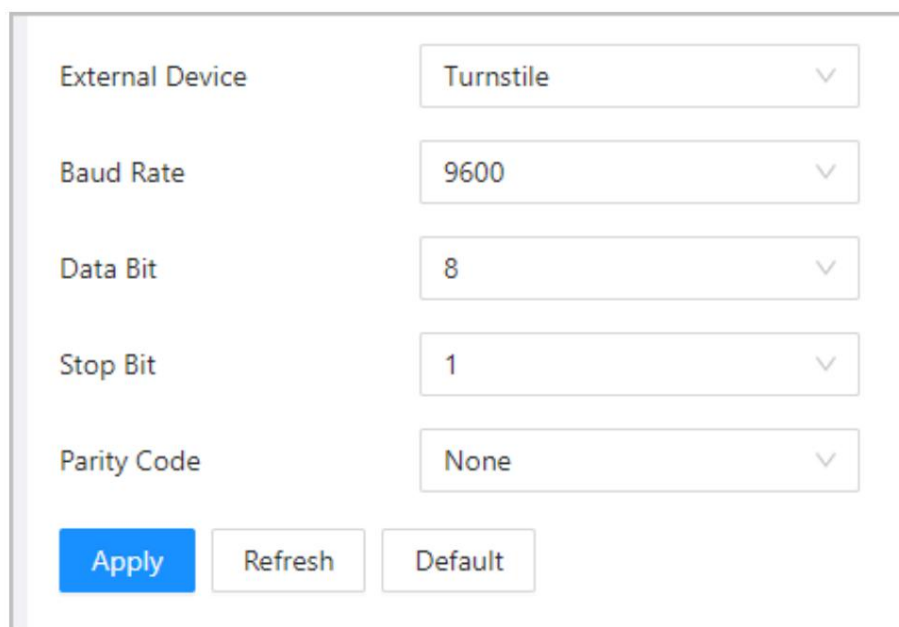


Таблица 3-37. Настройка параметров RS-485.

Параметр	Описание
Внешнее устройство	• 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. ◇ Нет: Выводит данные на основе идентификатора пользователя. • Считыватель карт: Устройство функционирует как контроллер доступа и подключается к внешнему считывателю карт. • Считыватель (OSDP): Устройство подключается к считывателю карт на основе протокола OSDP. протокол. • Модуль безопасности управления дверью: После включения модуля безопасности кнопка выхода, замок и функция пожарной сигнализации не работают. • Турникет: Когда устройство подключается к турникету, происходит доступ. Контроллерная плата турникета подключается к внешнему модулю QR-кода или модулю считывания карт, после чего плата передает данные для проверки на турникет. • Режим расширения замка: Если контроллер доступа подключен к внешнему модулю расширения замка и выбран режим «Модуль расширения замка», локальный замок разблокируется после подтверждения идентификации на локальном устройстве, а дополнительный замок — после подтверждения 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.
Бит данных	Количество бит, используемых для передачи фактических данных в последовательном канале связи. Это двоичные цифры, несущие передаваемую информацию.
Стоп Бит	После данных передается бит, а также необязательные биты четности, указывающие на конец передачи данных. Это позволяет приемнику подготовиться к передаче следующего байта данных и обеспечивает синхронизацию в протоколе связи.
Код четности	После битов данных отправляется дополнительный бит для обнаружения ошибок передачи. Он помогает проверить целостность передаваемых данных, обеспечивая наличие определенного количества логических старших или младших битов.

Шаг 3. Нажмите «Применить».

3.10.4 Настройка Wiegand

Поддерживает доступ к устройствам Wiegand. Настройте режим и режим передачи в соответствии с вашими реальными устройствами.

Процедура

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

Шаг 2. Выберите тип Wiegand, а затем настройте параметры.

- При подключении внешнего считывателя карт к устройству выберите вход Wiegand .



Если устройство подключается к стороннему устройству через входной порт Wiegand, и номер карты, считываемый устройством, отображается в обратном порядке по отношению к фактическому номеру карты, в этом случае можно включить функцию инверсии номера карты .

- Выберите выход Wiegand, если устройство функционирует как считыватель карт и вам необходимо подключить его к другому контроллеру доступа.

Рисунок 3-59. Выход Wiegand.

Wiegand

☐ Wiegand Input ☒ Wiegand Output

Wiegand Output Type

Wiegand34

▼

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.

Output Data Type

☒ Card Number ☐ No.

Apply

Refresh

Default

Таблица 3-38. Описание выходных данных Wiegand.

Параметр	Описание
Тип выходного сигнала Wiegand	Выберите формат Wiegand для считывания номеров карт или идентификационных номеров. • Wiegand26 : считывает 3 байта или 6 цифр. • Wiegand34 : считывает 4 байта или 8 цифр. • Wiegand66 : считывает 8 байтов или 16 цифр.
Ширина импульса	Введите ширину импульса и интервал между импульсами на выходе Wiegand.
Интервал пульса	
Тип выходных данных	Выберите тип выходных данных. • Нет .: Выводит данные на основе идентификатора пользователя. Формат данных — шестнадцатеричный или десятичный. • Номер карты : Выводит данные на основе первой карты пользователя. число.

Шаг 3. Нажмите «Применить».

3.11 Центр управления

3.11.1 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.

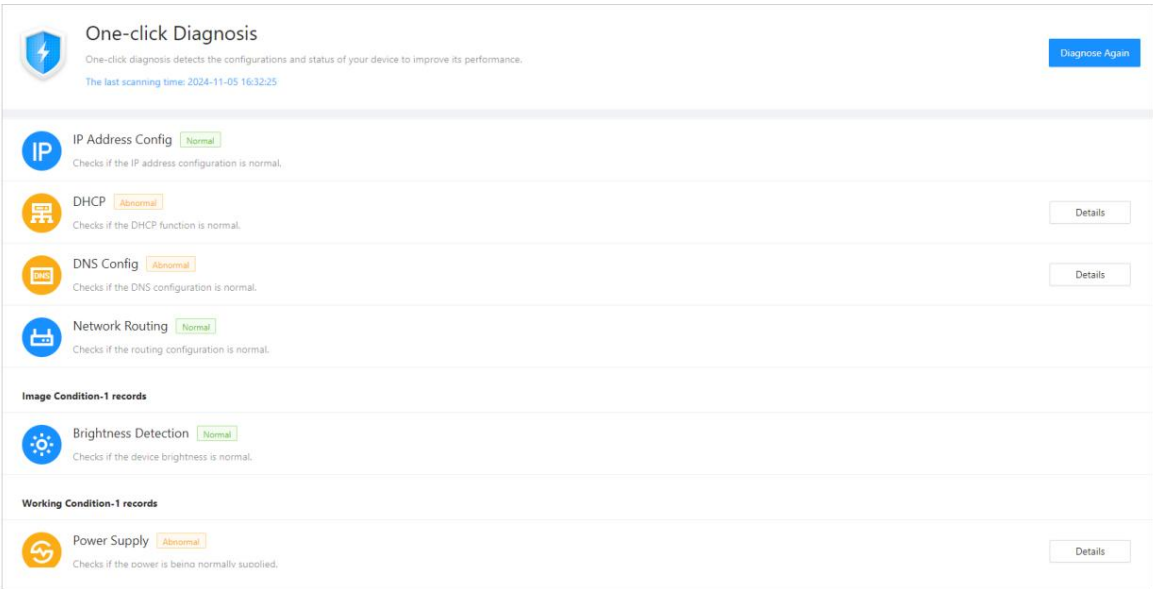
Шаг 2. Нажмите «Диагностика».

Система автоматически диагностирует конфигурацию и состояние устройства 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 3-60. Диагностика одним щелчком мыши.



3.11.2 Информация о системе

3.11.2.1 Просмотр информации о версии

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

3.11.2.2 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.

3.11.3 Объем данных

Вы можете увидеть, сколько пользователей, карточек и изображений лиц может хранить устройство.

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

3.11.4 Журналы просмотров

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

3.11.4.1 Системные журналы

Поиск и просмотр 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, чтобы

просмотреть  подробную информацию о журнале.

3.11.4.2 Разблокировка записей

Найдите записи о разблокировке и экспортируйте их.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр обслуживания > Журнал > Разблокировать записи.

Функция «Сохранять записи разблокировки» включена по умолчанию. После её отключения записи разблокировки не могут быть сохранены на устройстве.

Шаг 3. Выберите временной диапазон и тип, а затем нажмите «Поиск».

Для загрузки журнала нажмите кнопку «Экспорт».

Связанные операции

• Нажмите «Экспорт», чтобы экспортировать записи о разблокировке на свой компьютер.

• Нажмите  для просмотра собранного изображения лица.

• Нажмите  для просмотра изображения лица, полученного в ходе верификации.

3.11.4.3 История звонков

Просмотреть журналы звонков.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр технического обслуживания > Журнал > История обращений.

3.11.4.4 Журналы аварийных сигналов

Просмотреть журналы тревожных сообщений.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр технического обслуживания > Журнал > Журнал аварийных сигналов.

Шаг 3. Выберите тип и временной диапазон.

Шаг 4. Введите идентификатор администратора, а затем нажмите «Поиск».

3.11.4.5 Управление USB

Экспорт пользовательской информации с/на USB-накопитель.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр обслуживания > Журнал > Управление USB.



- Перед экспортом данных или обновлением системы убедитесь, что USB-накопитель вставлен в устройство. Во избежание сбоев не извлекайте USB-накопитель и не выполняйте никаких операций с устройством во время процесса.
- Для экспорта информации с устройства на другие устройства необходимо использовать USB-накопитель. Импорт изображений лиц через USB-накопитель запрещен.

Шаг 3. Выберите тип данных, а затем нажмите «Импорт с USB» или «Экспорт с USB», чтобы импортировать или экспортировать данные.

3.11.5 Центр технического обслуживания

3.11.5.1 Управление конфигурацией

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

3.11.5.1.1 Экспорт и импорт конфигурационных файлов

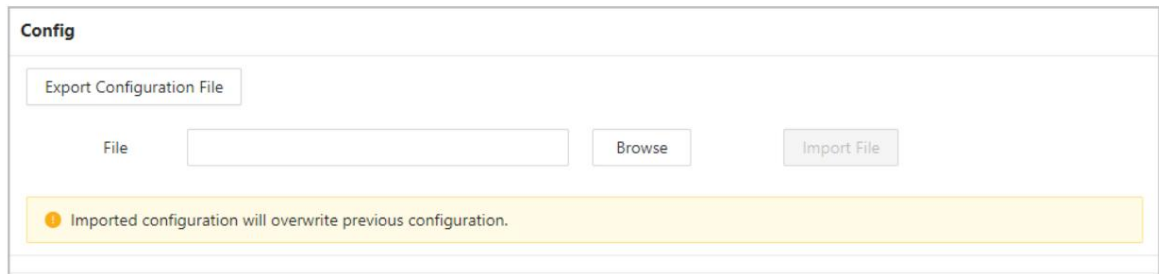
Вы можете импортировать и экспортировать файл конфигурации устройства. Если вы хотите применить одни и те же настройки к нескольким устройствам, вы можете импортировать файл конфигурации на них.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Управление техническим обслуживанием» > «Конфигурация».

Рисунок 3-61. 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.

3.11.5.1.2 Восстановление заводских настроек по умолчанию

Процедура

Шаг 1. Выберите «Управление техническим обслуживанием» > «Конфигурация».



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

Шаг 2. При необходимости восстановите заводские настройки по умолчанию.

- Восстановление заводских настроек (с сохранением сетевой конфигурации): Сбрасывает все настройки.
За исключением сетевой конфигурации устройства.
- Восстановление настроек по умолчанию (сохраняет журналы, информацию о пользователе и сетевую конфигурацию): Сбрасывает настройки устройства.
удаляет все данные, кроме информации о пользователе, журналов и сетевых конфигураций, и вносит изменения в настройки устройства.

3.11.5.2 Техническое обслуживание

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

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «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.

3.11.6 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.

3.11.6.1 Обновление файла

Процедура

Шаг 1. На главной странице выберите Система > 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.

3.11.6.2 Онлайн-обновление

Процедура

Шаг 1. На главной странице выберите Система > Обновление.

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

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

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

3.11.7 Расширенное техническое обслуживание

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

3.11.7.1 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.

3.11.7.2 Захват пакетов

Захват пакетов

1. На главной странице выберите Центр обслуживания > Расширенное обслуживание > Захват пакетов.

Рисунок 3-62. Захват пакетов.

Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	1 156	Optional	Optional	Optional	Optional	0.00MB	►
eth2	1 101	Optional	Optional	Optional	Optional	0.00MB	►

2. Введите IP-адрес, нажмите ►.

► изменения в . ||

3. После того, как вы соберете достаточно данных, нажмите || .

Захваченные пакеты автоматически загружаются на ваш локальный компьютер.

Тестирование сети

- 1. На главной странице выберите Центр обслуживания > Расширенное обслуживание > Захват пакетов.
- 2. В области «Тестирование сети» введите адрес назначения, а затем настройте размер пакета данных.

Рисунок 3-63. Тест сети.

Network Test

Destination Address

Test

Data Packet Size

64

Byte (64-4096)

Test Result

Copy

3. Нажмите «Тест».

Результат отображается в области «Результаты теста» . Вы можете скопировать результат.

3.12 (Необязательно) Настройки безопасности

3.12.1 Состояние безопасности

Просканируйте модули пользователей, служб и безопасности, чтобы проверить состояние безопасности устройства.

Справочная информация

- Проверка пользователей и служб: проверка соответствия текущей конфигурации рекомендациям.
- Сканирование модулей безопасности: сканирует состояние работы модулей безопасности, таких как передача аудио- и видеосигнала, доверенная защита, система предупреждения об угрозах и защита от атак, не определяя, включены ли они.

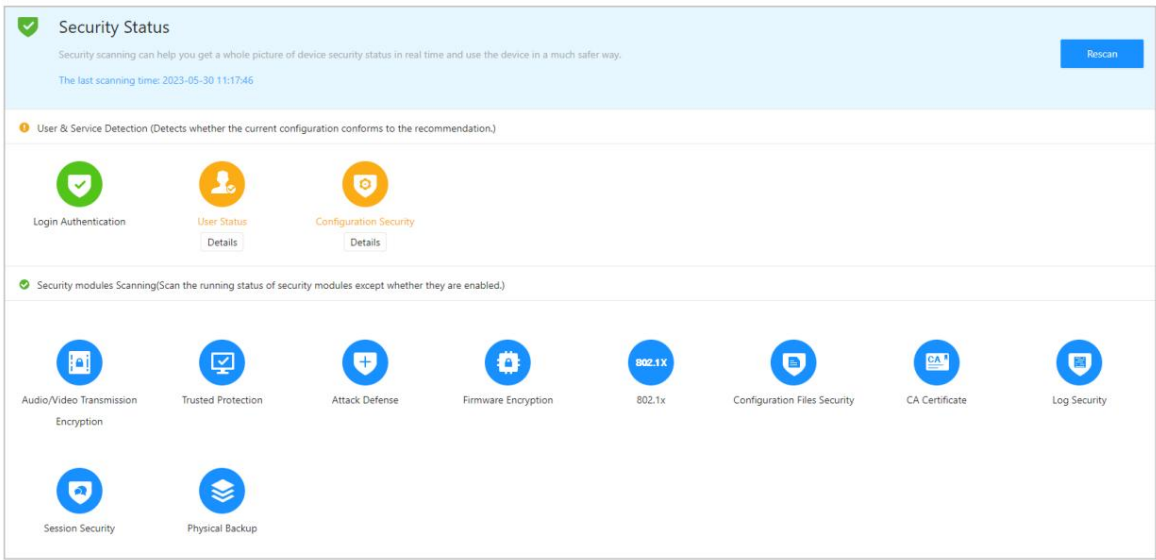
Процедура

- 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 3-64. 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 она не будет сканироваться. Обнаруженная аномалия «Игнорируется» будет выделено серым цветом.
- Нажмите «Оптимизировать», чтобы устранить проблему.

3.12.2 Настройка HTTPS

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 > Система > Служба > HTTPS.

Шаг 2. Включите службу HTTPS.



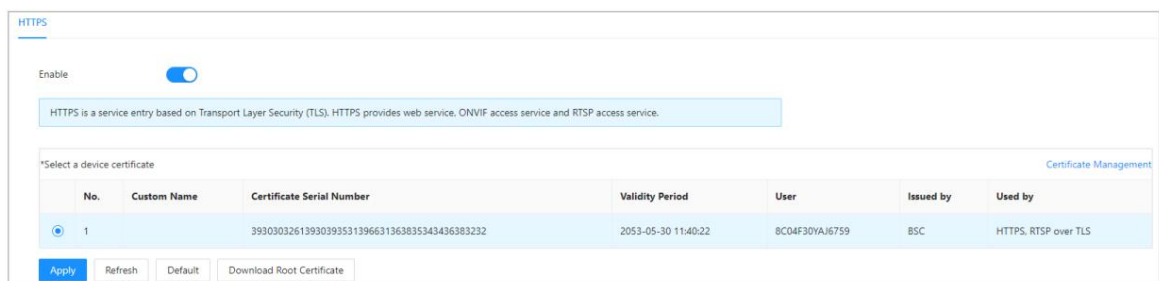
Если включить параметр "Совместимость с TLS v1.1 и более ранними версиями", могут возникнуть риски для безопасности. Обращаем ваше внимание.

Шаг 3. Выберите сертификат.



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

Рисунок 3-65 HTTPS



Шаг 4. Нажмите «Применить».

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

3.12.3 Атака Защита

3.12.3.1 Настройка брандмауэра

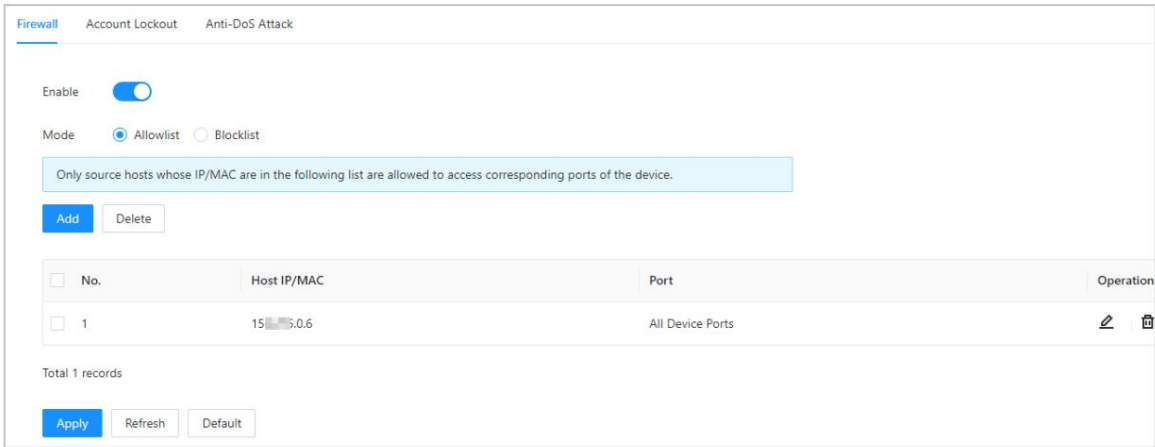
Настройте брандмауэр для ограничения доступа к устройству.

Процедура

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

Шаг 2. Нажмите, чтобы включить функцию брандмауэра.

Рисунок 3-66 Межсетевой экран

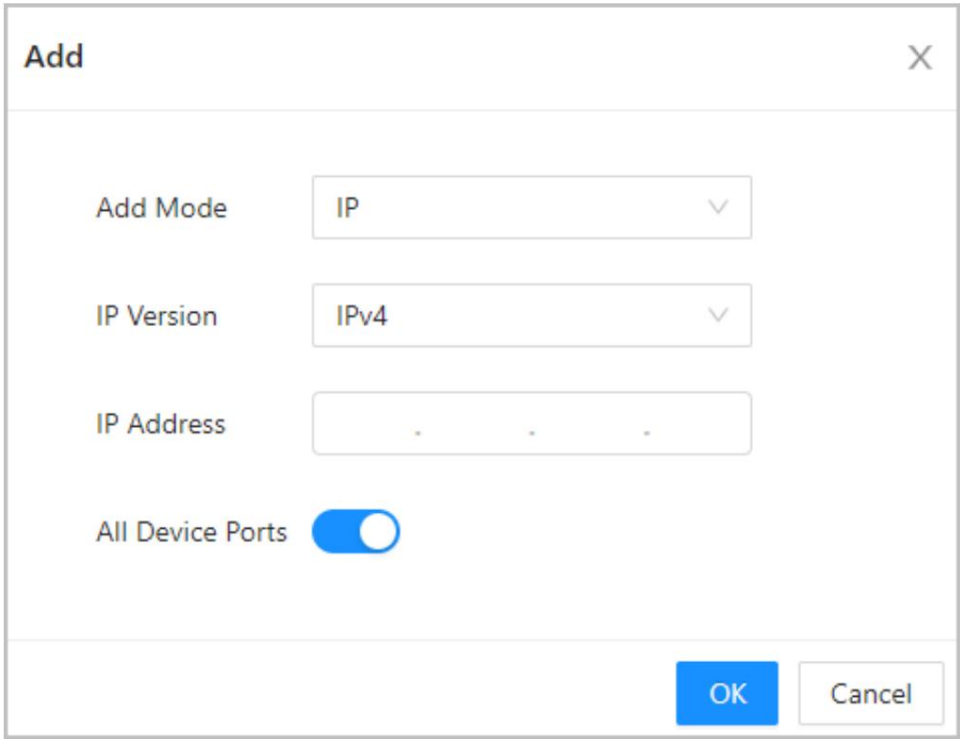


Шаг 3. Выберите режим: Список разрешенных и Список заблокированных.

- 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 3-67. Добавить информацию об IP-адресе.



Шаг 5. Нажмите OK.

Связанные операции

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

3.12.3.2 Настройка блокировки учетной записи

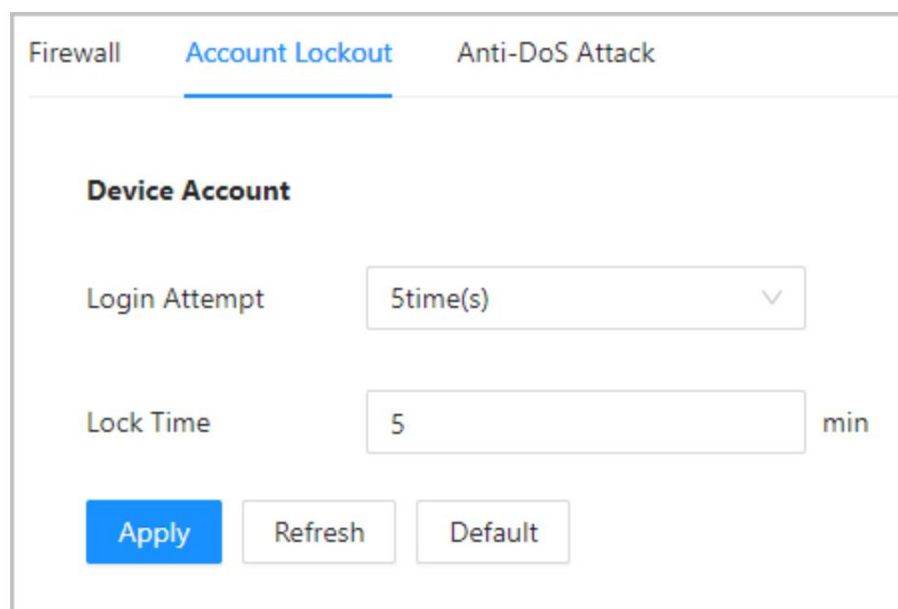
Если неверный пароль будет введен заданное количество раз, учетная запись будет заблокирована.

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 3-68 Блокировка учетной записи



- 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».

3.12.3.3 Настройка защиты от DoS-атак

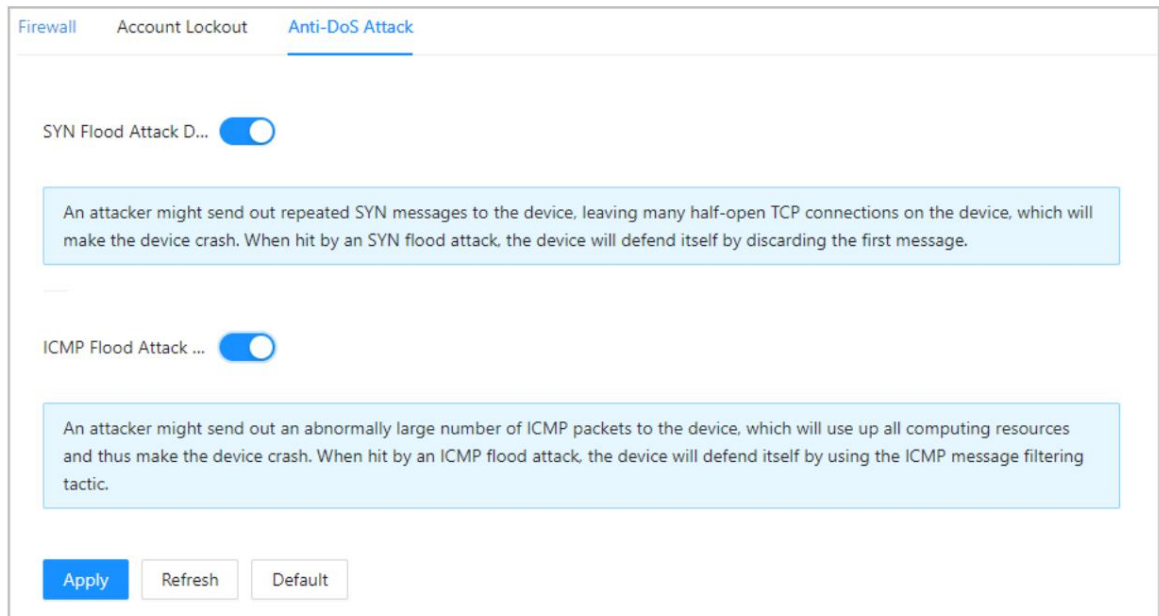
Для защиты устройства от DoS-атак можно включить защиту от SYN-флуд-атак и защиту от ICMP-флуд-атак .

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-атаки.

Рисунок 3-69. Защита от DoS-атаки.



Шаг 3. Нажмите «Применить».

3.12.4 Сертификат на устанавливаемое устройство

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

3.12.4.1 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 3-70. 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.

3.12.4.2 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 3-71 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 "172.16.0.03".
- 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.

3.12.4.3 Установка существующего сертификата

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

Процедура

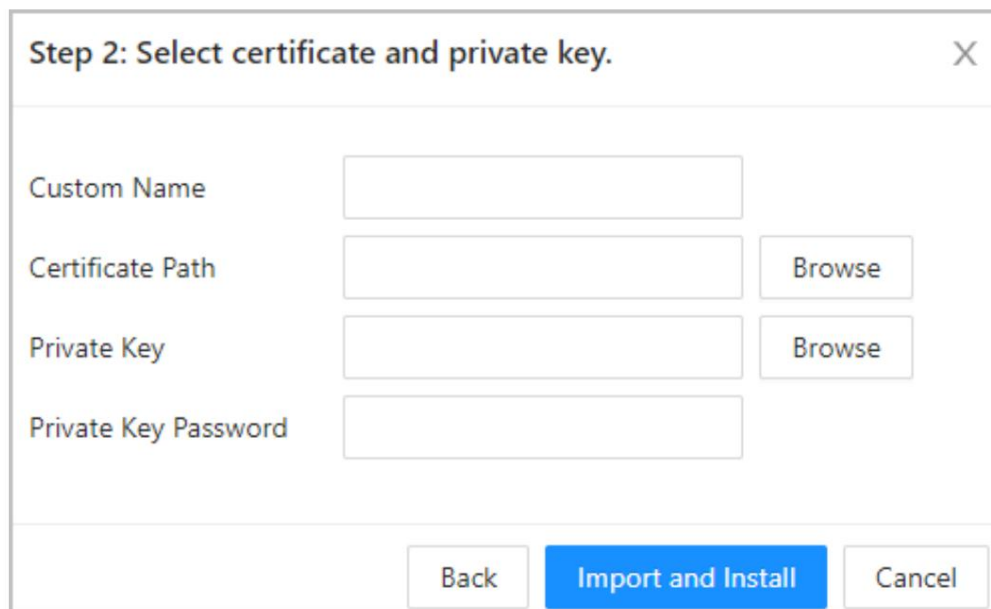
Шаг 1. Выберите Безопасность > Сертификат центра сертификации > Сертификат устройства.

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 3-72. 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.

3.12.5 Установка сертификата доверенного 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 подтверждает личность пользователя и предоставляет ему доступ к сети.

Процедура

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

Шаг 2. Выберите «Установить доверенный сертификат».

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

Рисунок 3-73. Установите доверенный сертификат.

Install Trusted Certificate

Custom Name

Certificate Path

Browse

OK

Cancel

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 скачать сертификат.
- Нажмите  чтобы удалить сертификат.

3.12.6 Шифрование данных

Процедура

Шаг 1. Выберите > Шифрование данных.

Шаг 2. Настройте параметры.

Рисунок 3-74 Шифрование данных

Encrypted Transmission

Private Protocol

Enable

Stream transmission is encrypted by using private protocol.

*Please make sure that the corresponding device or software supports video decryption.

Encryption Type

AES256-OFB

Update Period...

12

hr (0-720)

RTSP over TLS

Enable

RTSP stream is encrypted by using TLS tunnel before transmission.

*Please make sure that the corresponding device or software supports video decryption.

*Select a device certificate

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		393030313233343436383232	2053-05-30 11:40:22	8C04F30YA6759	BSC	HTTPS, RTSP over TLS

Certificate Management

Apply

Refresh

Default

Таблица 3-39. Описание шифрования данных.

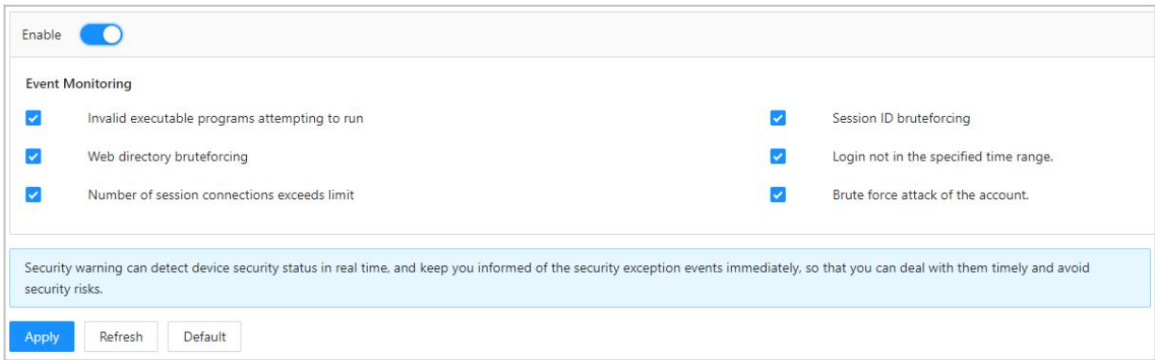
	Параметр	Описание
Частный протокол	Давать возможность	Передача потоков данных осуществляется с использованием частного протокола и шифруется во время передачи.
	Тип шифрования	Оставьте значение по умолчанию.
	Период обновления секретности Ключ	Диапазон значений от 0 ч до 720 ч. 0 означает, что секретный ключ никогда не будет обновляться.
RTSP поверх TLS	Давать возможность	Поток RTSP шифруется во время передачи через туннель TLS.
	Управление сертификатами: создание или импорт сертификата.	

3.12.7 Предупреждение о безопасности

Процедура

- Шаг 1. Выберите > Предупреждение безопасности.
- Шаг 2. Включите функцию предупреждения системы безопасности.
- Шаг 3. Выберите элементы мониторинга.

Рисунок 3-75. Предупреждение о безопасности.



- Шаг 4. Нажмите «Применить».

3.12.8 Аутентификация безопасности

Процедура

- Шаг 1. Выберите Безопасность > Аутентификация безопасности.
- Шаг 2. Выберите алгоритм хэширования сообщения.
- Шаг 3. Нажмите «Применить».

Рисунок 3-76. Аутентификация безопасности.

Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☒ MD5 ☐ SHA256

Digest Algorithm for ONVIF User Authentication ☒ MD5 ☐ SHA256

4. Работа с телефоном

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. В этом разделе рассматривается инициализация телефона через точку доступа Wi-Fi.

Процедура

Шаг 1. Включите контроллер доступа.

Шаг 2. Точка доступа Wi-Fi включена по умолчанию, если устройство не инициализировано. Через 30 минут после перехода устройства в режим инициализации точка доступа Wi-Fi на вашем телефоне автоматически выключится. Имя точки доступа: DAP + серийный номер продукта.

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. Выберите язык.

Шаг 6. Введите и подтвердите пароль, укажите адрес электронной почты, а затем нажмите «Далее».



- 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.
- Храните пароль в безопасности после инициализации и регулярно меняйте его для повышения уровня безопасности.
- Если вы хотите сбросить пароль администратора, отсканировав QR-код, вам потребуется указанный адрес электронной почты для получения кода безопасности.

Шаг 7. При необходимости включите автоматическую проверку, а затем нажмите «Выполнено».

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.

Вы можете войти на веб-страницу тремя следующими способами:

- Телефон и устройство находятся в одной локальной сети. Откройте браузер на телефоне и введите IP-адрес.
- Телефон и устройство находятся в одной локальной сети. Отсканируйте QR-код.
Настройки связи > Сетевые настройки > Wi-Fi на веб-странице вашего телефона.
- Вы также можете выбрать «Настройки связи» > «Сетевые настройки» > «Точка доступа Wi-Fi», чтобы перейти в главное меню.

Шаг 2. Введите имя пользователя и пароль.

Нажмите рядом с паролем, чтобы просмотреть его.



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

Рисунок 4-1 Страница входа

Шаг 3. Нажмите «Войти».

4.3 Главная страница

Главная страница отображается после успешного входа в систему.

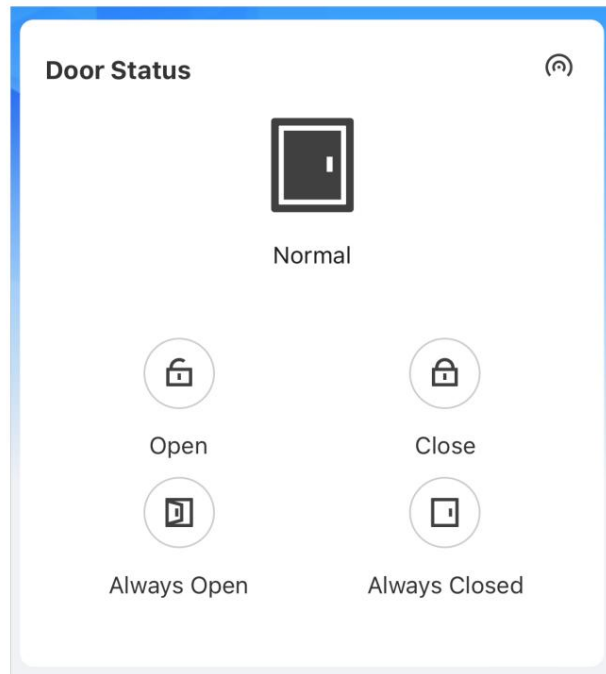
- Нажмите  в правом верхнем углу веб-страницы, а затем нажмите на QR-код «Документация по продукту». «Код», чтобы отсканировать QR-код и получить информацию о продукте, или нажмите «Выход», чтобы выйти из учетной записи.



Документация по продукту доступна для некоторых моделей.

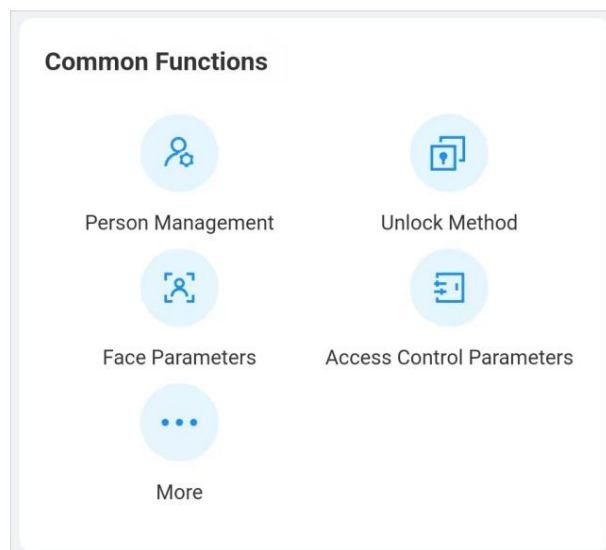
- В разделе «Состояние двери» отображается состояние двери. Вы можете дистанционно открывать или закрывать дверь. Вы также можете настроить статус двери как «Всегда открыта» или «Всегда закрыта».

Рисунок 4-2. Состояние двери.



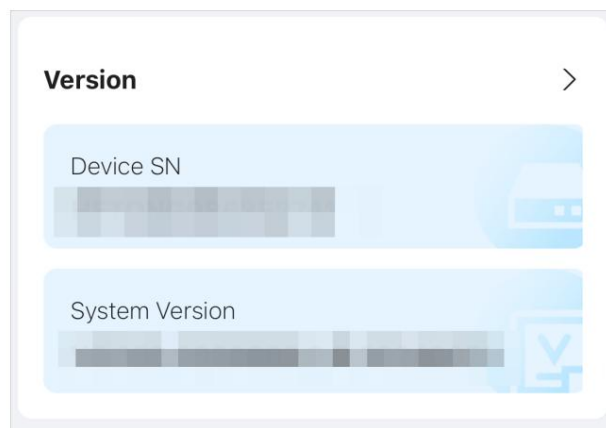
- В разделе «Общие функции» отображается меню настроек устройства. Нажмите «Подробнее», чтобы просмотреть все меню настроек.

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, а затем

Шаг 2. Нажмите «Управление персоналом» и нажмите +.

Шаг 3. Настройте информацию о пользователе.

Рисунок 4-5. Добавить человека (1)

Basic Info

* ID

Name

Access Credentials

Face0 >

PasswordNot Added >

Card0 >

Bluetooth Card
No email was configured. You cannot request a Bluetooth card through email.0 >

Рисунок 4-6. Добавить человека (2)

Verification Mode

Same as Device >

Validity Period

Forever >

Email

General Plan

255-Default >

Holiday Plan

255-Default >

User Type

General User >

Times Used

Unlimited

Add

Таблица 4-1. Описание параметров.

Параметр	Описание
—	Идентификатор пользователя аналогичен идентификатору сотрудника и может состоять из цифр, букв и их комбинаций, при этом максимальная длина числа составляет 30 символов.
Имя	Имя может содержать до 32 символов (включая цифры, символы и буквы).
Лицо	Поддерживается загрузка изображения лица или создание фотографии. Каждый пользователь может добавить не более 2 изображений лица. После загрузки изображение лица можно просмотреть или удалить.  Изображение лица представлено в форматах jpg, jpeg, png.
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.  Для использования этой функции необходимо подключить внешний коллектор.

Параметр	Описание
Карта	Нажмите «Добавить», введите номер карты вручную или проведите карту через специальное считывающее устройство. Пользователь может зарегистрировать максимум 5 карт. После успешного добавления нажмите на добавленную карту, вы сможете изменить номер карты, настроить карту как карту принуждения или удалить карту. Если вы включите тревожную сигнализацию, то при использовании карты вызова помощи для разблокировки двери сработает сигнализация.  Один пользователь может установить только одну принудительную карту.
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 тех, кто впервые использует Bluetooth-карту. Запрос. 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 получить Bluetooth-карты по запросу. - Запрос через регистрационный код : 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 идентичен режиму работы устройства. • Пользовательский : После выбора пользовательского режима отобразятся «Метод комбинации» и «Метод разблокировки». Выберите необходимый метод комбинации и метод разблокировки. - 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. Он не может использоваться во внешних считывателях карт. - Если пользовательский режим проверки отличается от режима устройства, приоритет отдается пользовательскому режиму.
Срок действия	Выберите один из вариантов: «Пользовательский» или «Бессрочный». Если вы выберете «Пользовательский», вам нужно будет указать дату, когда права доступа к двери для данного пользователя истекнут.

Параметр	Описание
Электронная почта	Введите адрес электронной почты этого человека.
Генеральный план	Люди могут открыть дверь в течение установленного периода времени.  Вы можете выбрать несколько тарифных планов.
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 открыть дверь в течение определенного периода времени или на определенное количество раз. По истечении установленного периода или времени разблокировки они не смогут открыть дверь. • Патрульный пользователь : Патрульные пользователи не имеют доступа к двери. • VIP-пользователь : При разблокировке двери VIP-пользователем обслуживающий персонал получит уведомление. - уведомление. • Другой пользователь : Когда он откроет дверь, она останется открытой в течение 5 минут. ещё несколько 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 Управление конфигурацией

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Система > Конфигурация.

Шаг 3. При необходимости восстановите заводские настройки по умолчанию.

- Восстановление заводских настроек (с сохранением сетевой конфигурации) : Сбрасывает все настройки.

За исключением сетевой конфигурации устройства. • Восстановление настроек

по умолчанию (сохраняет журналы, информацию о пользователе и сетевую конфигурацию) : Сбрасывает настройки устройства.

удаляет все данные, кроме информации о пользователе, журналов и сетевых конфигураций, и вносит изменения в настройки устройства.

4.5.3 Техническое обслуживание

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

Процедура

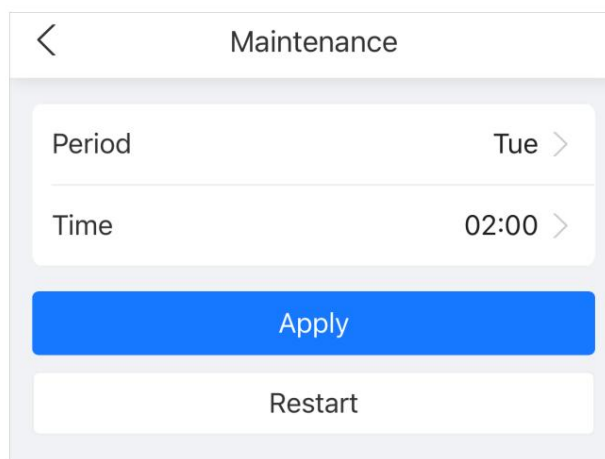
Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Система > Обслуживание.

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

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

Рисунок 4-7. Техническое обслуживание.



4.5.4 Настройка времени

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Система > Время.

Шаг 3. Настройте время.

Рисунок 4-8. Настройка параметров времени.

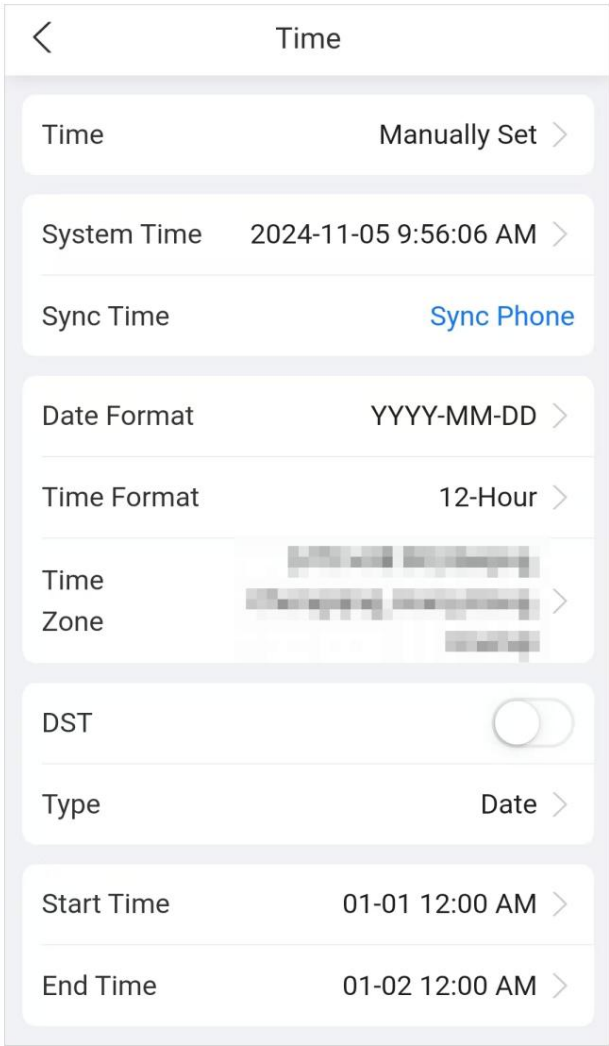


Таблица 4-2. Описание настроек времени.

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 время с указанием интервала синхронизации.
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».

4.5.5 Объем данных

Вы можете увидеть, сколько пользователей, карт, изображений лиц, отпечатков пальцев, журналов, записей разблокировки и другой информации может хранить устройство.

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

4.5.6 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. Нажмите «Способ разблокировки» в главном меню или выберите «Дополнительно» > «Контроль доступа» > «Разблокировать».

Метод.

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

Применять.

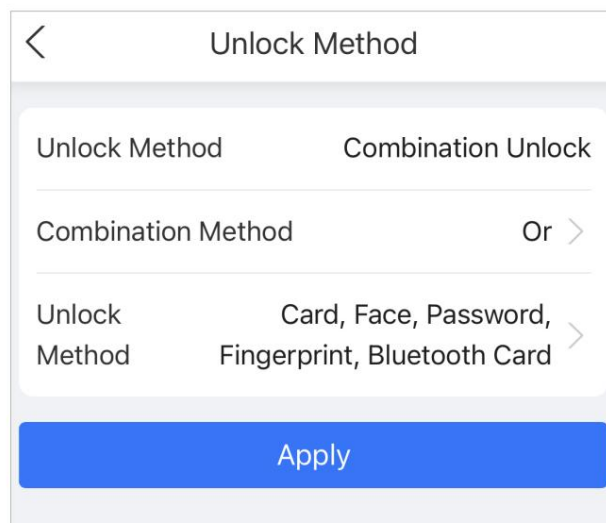
• Комбинированный метод

- ◇ 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 4-9. Способ разблокировки.



4.6.2 Настройка параметров лицевой панели

Настройте параметры распознавания лиц. Параметры распознавания лиц могут различаться в зависимости от модели устройства.

Процедура

Шаг 1. Войдите на веб-страницу.

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

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

Рисунок 4-10. Настройка параметров лица (1)

Face Parameters	
Face Recognition Threshold	85
Max Face Recognition Angle Deviation	30
Anti-spoofing Level	General >
Valid Face Interval (sec)	3
Invalid Face Interval (sec)	10
Recognition Distance	1.5m >
Mask mode	Not Detect >
Mask Recognition Threshold	75

Рисунок 4-11 Настройка параметров лица (2)

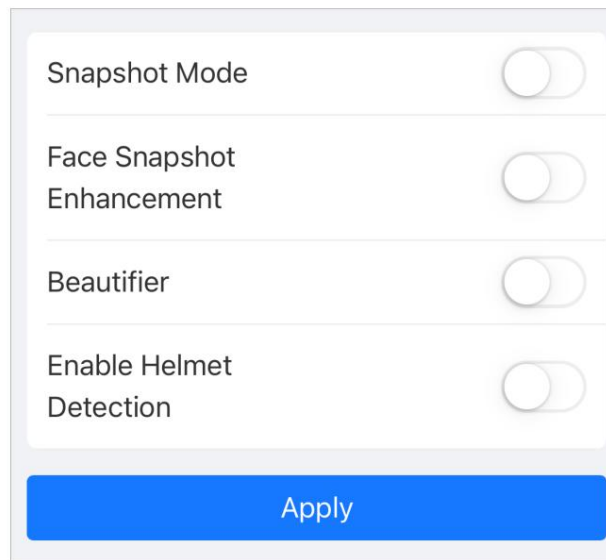


Таблица 4-3. Описание параметров лица.

Имя	Описание
Порог распознавания лиц	Настройте уровень точности распознавания лиц. Более высокий порог означает более высокую точность и меньший процент ложных срабатываний.  Если пороговое значение слишком низкое, например, равно 0, то частота ложных срабатываний будет чрезвычайно высокой. Обратите внимание.
Максимальный угол распознавания лиц Отклонение	Задайте максимальный угол, под которым можно расположить лицо для распознавания. Чем больше значение, тем шире диапазон углов наклона грани. Если угол наклона грани выходит за пределы заданного диапазона, она может быть обнаружена неправильно.
Уровень защиты от подделки	После включения эта функция предотвращает использование фотографий, видео, масок и других заменителей для получения несанкционированного доступа. После включения этой функции рамка с лицом не отображается при проверке подлинности неживого объекта.
Интервал между полями для заполнения (сек)	Если после первого успешного распознавания перед объективом остается то же лицо, устройство повторно выполнит распознавание лица через определенный промежуток времени.
Неверный интервал между предъявлениями лиц (сек)	Если после первой неудачной попытки распознавания перед объективом остается то же лицо, устройство повторно выполнит распознавание лица через определенный промежуток времени. Если вы укажете 0, лицо не будет распознано, и записи о разблокировке не будут созданы.
Расстояние распознавания	Расстояние между лицом и линзой.

Имя	Описание
Режим маски	• Не обнаружено : Маска не обнаружена во время распознавания лица. • Предупреждение о маске : Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, но доступ будет разрешен. • Требуется маска : Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, и доступ будет запрещен.
Порог распознавания маски	Чем выше пороговое значение, тем точнее будет распознавание лица, когда человек носит маску, и тем ниже будет частота ложных срабатываний.
Режим моментального снимка	После включения этой функции можно отфильтровать снимки низкого качества из записей о разблокировке.
Улучшение снимков лица	После включения этой функции снимки в записях разблокировки отображаются в улучшенном виде.
Украшение	Улучшите качество захваченных изображений лиц.
Включить обнаружение шлема	Обнаруживает защитные каски. Дверь не откроется, если человек не в каске.

4.6.3 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 4-12 Параметры контроля доступа (1)

Basic Settings

NameDoor1

Door StatusNormal >

Verification Interval0 s

Card Swiping Interval0 s (0-86400)

Public Password

Рисунок 4-13 Параметры контроля доступа (2)

Normally Open Period

General Plan

Disabled >

Holiday Plan

Disabled >

Normally Closed Period

General Plan

Disabled >

Holiday Plan

Disabled >

Рисунок 4-14 Параметры контроля доступа (3)

Unlock Settings

Unlock Method

Combination Unlock

Combination Method

Or >

Unlock Method

Card, Face, Password, Bluetooth Card >

Bluetooth Mode

Long-range >

PIN Code Authentication

☐

Door Unlocked Duration

3 s

Remote Verification

☐

Apply

Таблица 4-4. Описание параметров контроля доступа.

Параметр		Описание
Основные настройки	Имя	Название двери.

Параметр		Описание
	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.
	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	Генеральный план/ План на отпуск	При выборе режима «Обычный» вы можете выбрать временной шаблон из выпадающего списка. Дверь остается открытой или закрытой в течение заданного времени.
Обычно закрыто Период	Генеральный план/ План на отпуск	 • Когда обычно открытый период конфликтует с В период, обычно закрытый, период, обычно открытый, имеет приоритет над периодом, обычно закрытым. • В случае конфликта генерального плана с планом праздников, план праздников имеет приоритет над генеральным планом.
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.

Параметр		Описание
	Способ разблокировки	Способы разблокировки могут различаться в зависимости от модели продукта.
	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.
	Выберите режим Bluetooth в соответствии с вашими потребностями.	
	Дверь открыта Продолжительность	После того, как человеку будет предоставлен доступ, дверь останется открытой в течение определенного времени, чтобы он мог пройти. Его продолжительность варьируется от 0,2 до 600 секунд.
	Удаленная проверка. Откройте дверь дистанционно.	

Шаг 4. Нажмите «Применить».

4.6.4 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 (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.

Шаг 4. Настройте параметры сигнализации, а затем нажмите «Применить».

Рисунок 4-15. Настройки сигнализации.

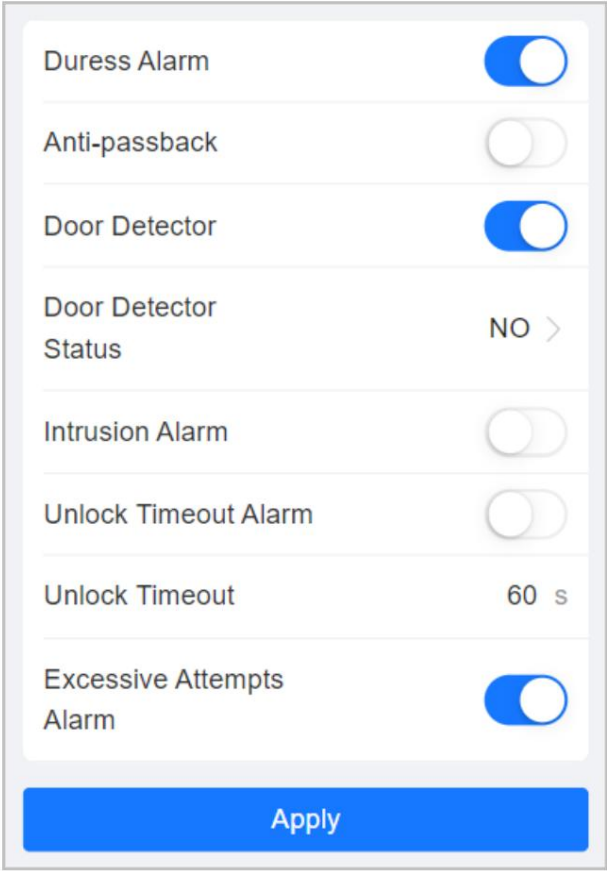


Таблица 4-5. Описание параметров тревоги.

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.
Сигнал тревоги о чрезмерном количестве попыток	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании нелегальной карты, которая будет гореть в течение определенного времени.

4.6.5 Настройка связи между системами сигнализации (необязательно)

Вы можете настроить связь 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 4-16. Связь сигналов тревоги.

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 блокировки: локальная или внешняя.

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

Шаг 9. Нажмите OK.

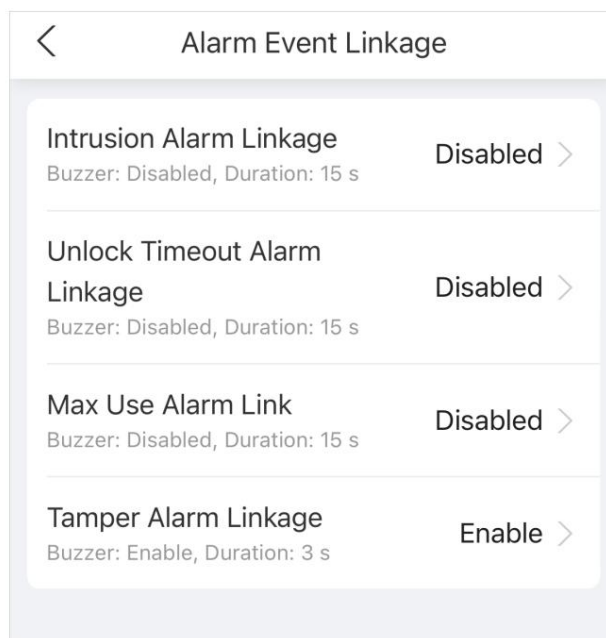
4.6.6 Настройка связи между событиями тревоги

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Контроль доступа > Связывание событий тревоги.

Рисунок 4-17. Связь событий тревоги.



Шаг 3. Коснитесь ссылки, чтобы настроить связь с тревожной системой, а затем нажмите OK.

Таблица 4-6. Связь событий тревоги.

Параметр	Описание
Связь с охранной сигнализацией	Если дверь откроется ненормально, сработает охранная сигнализация. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении вторжения. Вы можете настроить продолжительность сигнала тревоги. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает охранная сигнализация. Вы можете настроить продолжительность тревоги.
Сигнализация об истечении времени разблокировки Связь	Если дверь остается незапертой дольше заданного времени ожидания, сработает сигнализация об истечении времени ожидания, которая будет действовать в течение заданного времени. • Звуковой сигнал: Звуковой сигнал срабатывает, когда истекает время ожидания разблокировки. Сработало. Длительность поддерживает пользовательское время и устанавливается до блокировки двери. ◇ До закрытия двери: Звук сигнализации прекращается после закрытия двери. ◇ Настраиваемое время: Вы можете установить продолжительность. • Локальный вывод сигналов тревоги: Внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнал тревоги об истечении времени разблокировки. Поддерживается установка пользовательского времени и установка параметра «До блокировки двери». ◇ До закрытия двери: После закрытия двери звуковой сигнал тревоги прекращается. ◇ Настраиваемое время: Вы можете указать продолжительность.
Ссылка на оповещение о максимальном использовании	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании нелегальной карты, которая будет гореть в течение определенного времени. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении чрезмерного использования. Длительность срабатывания сигнала можно настроить. • Выходной сигнал тревоги: Внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнал тревоги об истечении времени разблокировки. Вы можете настроить продолжительность сигнала тревоги.
Связь сигнализации о несанкционированном доступе	Сигнализация о попытке взлома срабатывает, когда кто-то пытается физически повредить устройство. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении попытки взлома. Вы можете настроить продолжительность сигнала тревоги. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнализация о несанкционированном доступе. Вы можете настроить продолжительность срабатывания сигнализации.

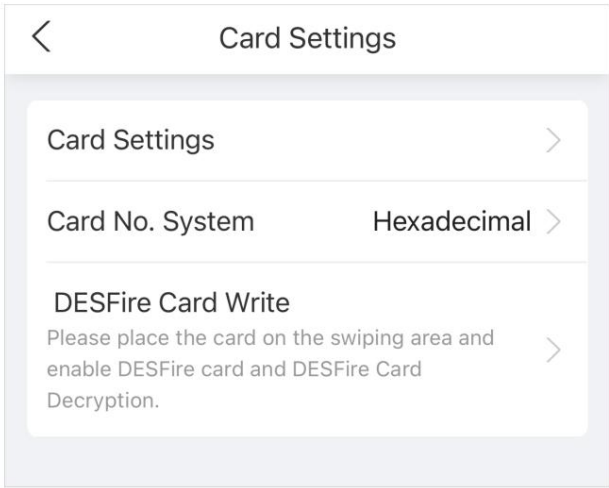
4.6.7 Настройка параметров карты

Процедура

Шаг 1. Войдите на веб-страницу.

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

Рисунок 4-18 Настройки карты



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

Рисунок 4-19 Параметры карты

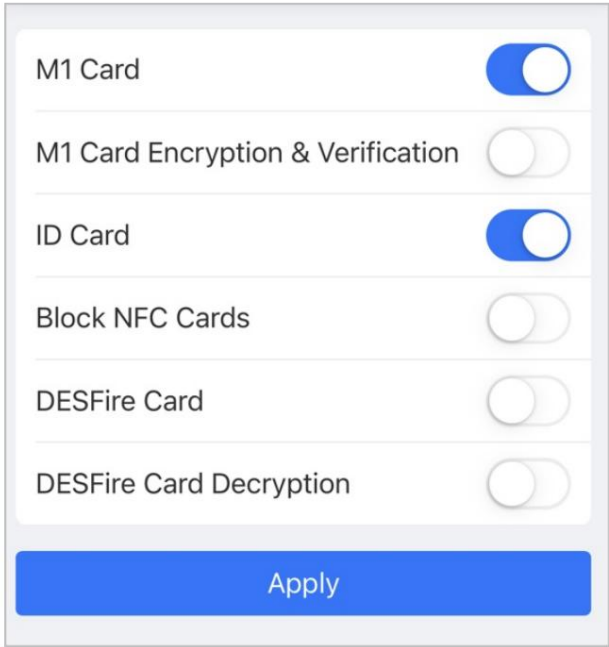


Таблица 4-7. Описание параметров карты.

Параметр	Описание
Карта M1	При включении этой функции карту M1 можно считать.
Шифрование и проверка карт M1	При включении этой функции можно считать только зашифрованную IC-карту.  Убедитесь, что карта M1 активирована.

Параметр	Описание
Удостоверение личности	При включении этой функции удостоверение личности можно считать.  Эта функция доступна только на некоторых моделях.
Блокировка NFC-карт	После включения этой функции разблокировка с помощью дубликата NFC-карты будет исключена.  • Эта функция доступна только в моделях, поддерживающих IC-карты. • Убедитесь, что карта M1 активирована. Функция NFC доступна только на некоторых моделях телефонов.
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.

4.6.8 Настройки конфиденциальности

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Дополнительно» > «Контроль доступа» > «Настройки конфиденциальности».

Шаг 3. Включите необходимую функцию.

- Снимок лица для проверки: изображения лиц будут автоматически считываться при разблокировке устройства. дверь.
- Снимок тревоги: При включении этой функции снимки будут создаваться при срабатывании сигнализации. Обратная передача данных, принуждение, черный список и несанкционированные чрезмерные попытки. По умолчанию отключено.
- Ночные ИК-снимки: четкие изображения можно получить при слабом освещении или в полной темноте.



- Если включена функция «Проверочный снимок», функция «Ночной ИК-снимок» будет включена автоматически. Днём функция «Проверочный снимок» использует захват белого света, а ночью — ИК-снимок. Если отключена только функция «Ночной ИК-снимок», функция «Проверочный снимок» будет использовать захват белого света как днём, так и ночью.
- При включении функции «Снимок тревоги» функция «Ночной ИК-снимок» будет включена автоматически. В дневное время функция «Снимок тревоги» использует захват белого света, а ночью — захват ИК-излучения. Если отключена только функция «Ночной ИК-снимок», функция «Снимок тревоги» будет использовать захват белого света как днем, так и ночью.
- Когда включены функции «Снимок проверки», «Снимок тревоги» и «Ночной ИК-снимок». Если функция включена, а функции «Проверочный снимок» и «Снимок тревоги» отключены, то ночной ИК-снимок будет автоматически скрыт.

Шаг 4. Нажмите «Применить».

4.6.9 Настройка функций выходного порта

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



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

Процедура

Шаг 1. Войдите на веб-страницу.

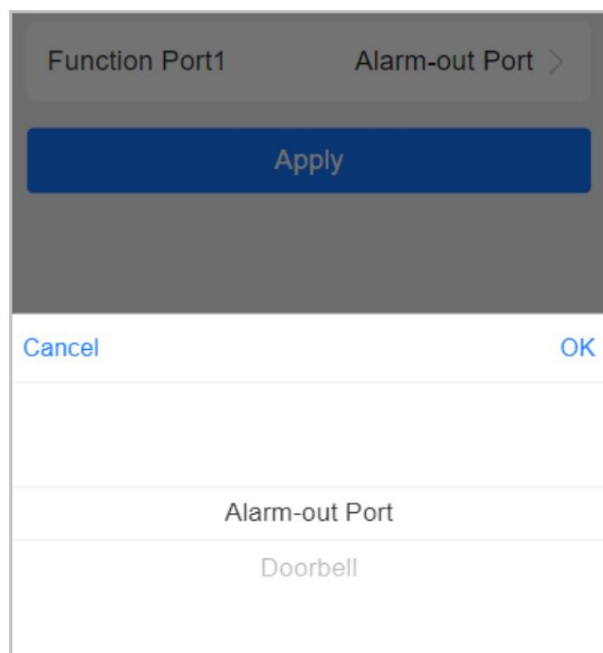
Шаг 2. Выберите Дополнительно > Контроль доступа > Настройка выходного порта.

Шаг 3. Выберите тип порта.



Если кабель сигнализации и кабель дверного звонка используются совместно, настройте интерфейс на подключение к дверному звонку, чтобы гарантировать срабатывание звонка.

Рисунок 4-20. Настройка портов.



Шаг 4. Нажмите «Применить».

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 > Сетевые настройки > TCP/IP.

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

Рисунок 4-21 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

Transmission Mode

Multicast >

Таблица 4-8. 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.
Маска подсети	
Шлюз по умолчанию	• IPv6-адрес представляется в шестнадцатеричном формате. • Для версий IPv6 не требуется установка масок подсети. • IP-адрес и шлюз по умолчанию должны совпадать. сегмент сети.

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, которые могут быть переданы в одном сетевом пакете в компьютерных сетях. По умолчанию он равен 1500.
Режим передачи	• Многоадресная рассылка: идеально подходит для видеозвонков. • Одноадресная рассылка: идеально подходит для групповых звонков.

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 только на некоторых моделях. • Wi-Fi и точка доступа Wi-Fi могут быть включены одновременно, при этом функция Wi-Fi включается автоматически по умолчанию.

Шаг 4. Нажмите на Wi-Fi, а затем введите пароль.

Wi-Fi подключен.

Связанные операции

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

4.7.3 Настройка точки доступа Wi-Fi



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

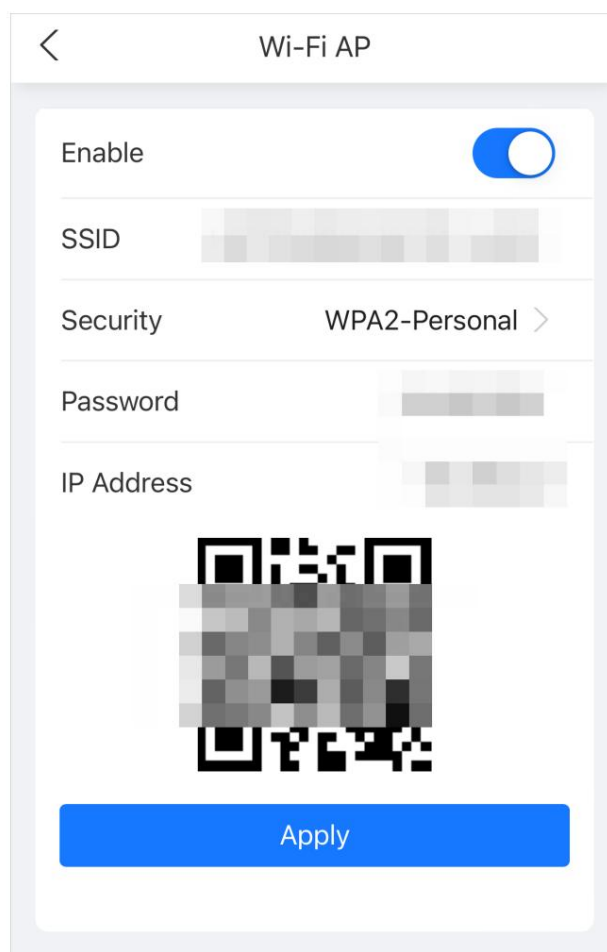
Процедура

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 4-22 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 4-23. Автоматическая регистрация.

Auto Registration

Enable

Status

Offline

Server Address

Port

7000

Registration ID

none

Apply

Таблица 4-9. 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). Добавление устройства в систему для управления путем ввода регистрационного идентификатора на платформе.

4.7.6 Настройки Bluetooth

Процедура

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

Рисунок 4-24 Bluetooth

Bluetooth

Bluetooth Name

212F-ME118237

Save

- Шаг 4. Нажмите «Сохранить».

Результаты

Разблокировать дверь можно через Bluetooth с помощью приложения DMSS. Подробности см. в разделе "2.2.5 Разблокировка через Bluetooth".

4.7.7 Настройка Wiegand

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройки связи > Wiegand.

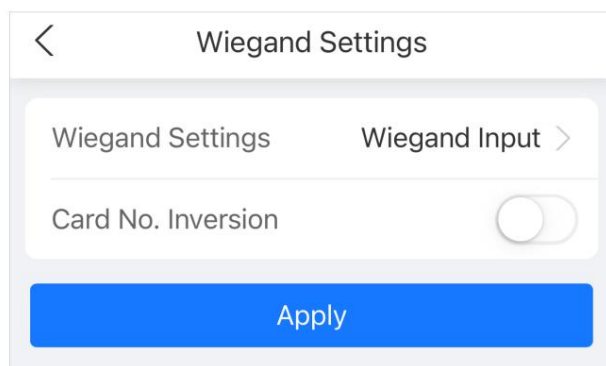
Шаг 3. Выберите тип Wiegand, настройте параметры, а затем нажмите «Применить».

- При подключении внешнего считывателя карт к устройству выберите вход Wiegand .



Если устройство подключается к стороннему устройству через входной порт Wiegand, и номер карты, считываемый устройством, отображается в обратном порядке по отношению к фактическому номеру карты, в этом случае можно включить функцию инверсии номера карты .

Рисунок 4-25. Вход Wiegand.



- Выберите выход Wiegand, если устройство функционирует как считыватель карт и вам необходимо подключить его к другому контроллеру доступа.

Рисунок 4-26. Выход Wiegand.

Wiegand Settings

Wiegand Settings

Wiegand Output >

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.

Output Data Type

No. >

Output Format

Decimal >

Apply

Таблица 4-10. Описание выходных данных Wiegand.

Параметр	Описание
Тип выходного сигнала Wiegand	Выберите формат Wiegand для считывания номеров карт или идентификационных номеров. - Wiegand26 : считывает 3 байта или 6 цифр. - Wiegand34 : Считывает 4 байта или 8 цифр. - Wiegand66 : Считывает 8 байтов или 16 цифр.
Ширина импульса	Введите ширину импульса и интервал между импульсами на выходе Wiegand.
Интервал пульса	
Тип выходных данных	Выберите тип выходных данных. - Нет.: Выводит данные на основе идентификатора пользователя. Формат данных — шестнадцатеричный или десятичный. - Номер карты : Выводит данные на основе первого номера карты пользователя.

4.7.8 Настройка RS-485

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

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройки связи > Настройки RS-485.

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

Параметры могут различаться в зависимости от типа внешнего устройства. На следующем рисунке в качестве примера используется контроллер доступа .

Рисунок 4-27 Настройки RS-485

< RS-485 Settings

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 >

Apply

Таблица 4-11. Настройка параметров RS-485.

Параметр	Описание
Внешнее устройство	• 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. ◇ Нет: Выводит данные на основе идентификатора пользователя. • Считыватель карт: Устройство функционирует как контроллер доступа и подключается к внешнему считывателю карт. • Считыватель (OSDP): Устройство подключается к считывателю карт на основе протокола OSDP. протокол. • Модуль безопасности управления дверью: После включения модуля безопасности кнопка выхода, замок и функция пожарной сигнализации не работают. • Турникет: Когда устройство подключается к турникету, происходит доступ. Контроллерная плата турникета подключается к внешнему модулю QR-кода или модулю считывания карт, после чего плата передает данные для проверки на турникет. • Режим расширения замка: Если контроллер доступа подключен к внешнему модулю расширения замка и выбран режим «Модуль расширения замка», локальный замок разблокируется после подтверждения идентификации на локальном устройстве, а дополнительный замок — после подтверждения 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.
Бит данных	Количество бит, используемых для передачи фактических данных в последовательном канале связи. Это двоичные цифры, несущие передаваемую информацию.
Стоп Бит	После данных передается бит, а также необязательные биты четности, указывающие на конец передачи данных. Это позволяет приемнику подготовиться к передаче следующего байта данных и обеспечивает синхронизацию в протоколе связи.
Код четности	После битов данных отправляется дополнительный бит для обнаружения ошибок передачи. Он помогает проверить целостность передаваемых данных, обеспечивая наличие определенного количества логических старших или младших битов.

4.8 Настройка аудиоподсказок

Настройте звуковые подсказки во время подтверждения личности.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройки аудио и видео > Аудио.

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

Рисунок 4-28. Настройка параметров звука.

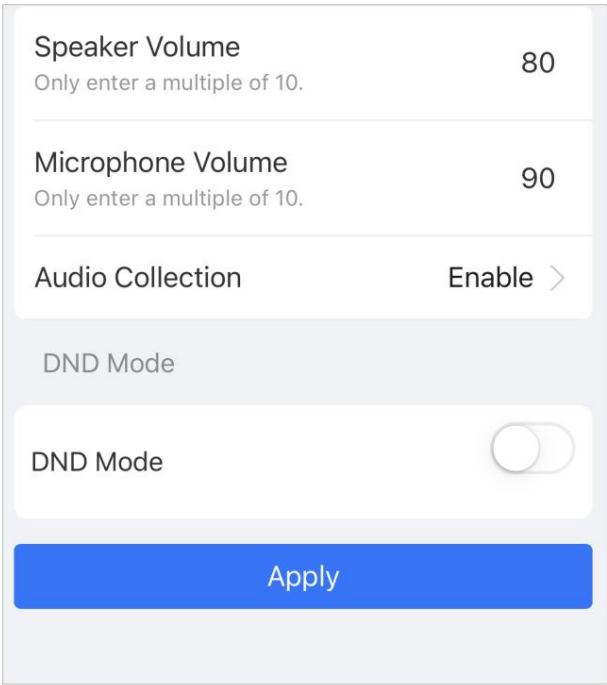


Таблица 4-12. Описание параметров.

Параметры	Описание
Громкость динамика	Установите громкость динамика.
Громкость микрофона	Установите громкость микрофона.
Аудиоколлекция	Если эта функция включена, звук из микрофона устройства будет записываться в режиме реального времени и во время видеозаписи.
Режим «Не беспокоить»	В течение установленного времени при подтверждении вашей учетной записи голосовые подсказки не звучат. Идентификатор устройства. Можно установить до 4 периодов.

4.9 Журналы просмотров

Просматривайте журналы, такие как системные журналы, записи о разблокировке и журналы тревожных сигналов.

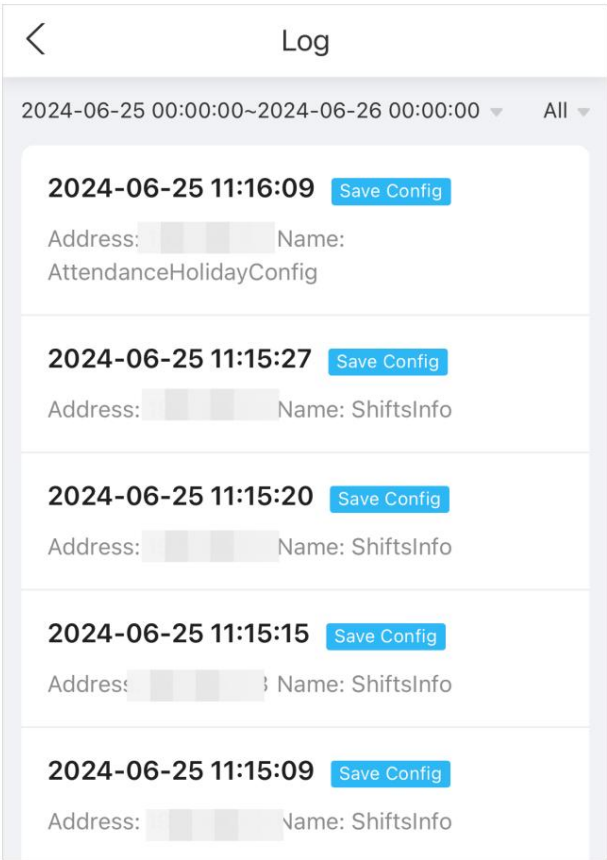
4.9.1 Системные журналы

Просмотр и поиск системных журналов.

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите Дополнительно > Журнал > Журнал.
- Шаг 3. Выберите время и тип записи.

Рисунок 4-29. 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. Выберите время и тип записи.
- Шаг 4. Нажмите на запись, чтобы просмотреть подробности.

4.9.3 История звонков

Найдите историю звонков.

Процедура

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

4.9.4 Журналы аварийных сигналов

Просмотреть журналы тревожных сообщений.

Процедура

- Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Журнал > Журнал тревог.

Шаг 3. Выберите время и тип записи.

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 SmartPSS 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 Инициализация и вход в систему

При первом входе в систему выполните инициализацию SmartPSS Lite, включая установку пароля для входа и контрольных вопросов для сброса пароля.

Процедура

- Шаг 1

Дважды щелкните файл SmartPSSLite.exe.
- Шаг 2

Выберите язык из выпадающего списка, затем выберите «Я прочитал и согласен с условиями использования программного обеспечения». Соглашение , а затем нажмите «Далее».
- Шаг 3

Нажмите «Обзор» , чтобы выбрать путь установки, а затем нажмите «Установить».
- Шаг 4

Нажмите «Готово» , чтобы завершить установку.
- 

Выберите «Запустить SmartPSSLite» , чтобы запустить SmartPSS Lite.
- Шаг 5

Выберите сцены приложения, которые хотите добавить, и нажмите ОК.
- Шаг 6

Нажмите «Я прочитал и согласен с условиями лицензионного соглашения на программное обеспечение» , чтобы принять ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.
- Шаг 7

Нажмите «Я прочитал(а) и согласен(на) с условиями политики конфиденциальности программного обеспечения» , чтобы принять Политику конфиденциальности продукта.
- Шаг 8

Установите пароль на странице «Инициализация» , а затем нажмите «Далее».

Таблица 5-1. Параметры установки пароля.

Параметр	Описание
Пароль	Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; : &).
Надежность пароля	Отображает эффективность пароля против попыток подбора или перебора. Зеленый цвет означает, что пароль достаточно надежен, красный — менее надежен. Установите пароль высокого уровня безопасности в соответствии с подсказкой о надежности пароля.
Подтвердите пароль	Введите пароль еще раз для подтверждения.
Автоматический вход в систему после регистрации	Включите функцию автоматического входа после регистрации , чтобы SmartPSS Lite автоматически входил в систему после инициализации; в противном случае будет отображаться страница входа.

- Шаг 9

Установите контрольные вопросы безопасности, а затем нажмите «Завершить».
- Шаг 10

Дважды щелкните файл SmartPSSLite.exe.
- Шаг 11

Введите имя пользователя и пароль, а затем нажмите «Войти».

Если на вашем компьютере доступно несколько сетей, вы можете выбрать одну из них.

5.3 Добавление устройств

Существует 3 доступных способа добавления устройств.

• Автоматический поиск •

Добавление вручную •

Пакетный импорт

5.3.1 Добавление устройства путем поиска

Вы можете добавить несколько устройств, выполнив поиск по ним в текущем сегменте сети или в других сегментах сети.



Мы рекомендуем добавлять устройства через поиск, если устройства находятся в одном сетевом сегменте или если вы хотите добавить устройства из известного сетевого сегмента, но не знаете точный IP-адрес устройств.

Процедура

Шаг 1. На главной странице нажмите «Устройства».

Шаг 2. Выберите метод поиска.

- Нажмите «Автопоиск», чтобы автоматически выполнить поиск устройств, находящихся в той же сети.
- Введите начальный и конечный

IP-адреса рядом с полем «Сетевой сегмент устройства», нажмите «Поиск», и система автоматически выполнит поиск устройств в этом диапазоне IP-адресов.

Шаг 3. Выберите устройства, а затем нажмите «Добавить».

Шаг 4. Введите имя пользователя и пароль для входа в систему, а затем нажмите ОК.

Устройства будут добавлены на платформу.

-  : Изменить информацию об устройстве.
-  : Переходит в модуль «Конфигурация устройства» на платформе.
-  : Переходит на веб-страницу устройства.
-  Выйдите из системы на устройстве, и его статус изменится на «Офлайн».
-  Войдите в систему устройства, и его статус изменится на «В сети».
-  Удалите устройство.

Связанные операции

- Изменение IP-адреса по одному: выберите устройство и нажмите «Изменить IP-адрес», чтобы изменить IP-адрес устройства.
- Изменение IP-адреса группами: выберите несколько устройств и нажмите «Изменить», чтобы изменить их IP-адреса.

адреса.



Введите начальный IP-адрес, и система автоматически назначит устройствам IP-адреса, увеличивая их на 1 в зависимости от начального IP-адреса. Например, если начальный IP-адрес — 10.XX.XXX.52, то IP-адреса последующих устройств будут 10.XX.XXX.53, 10.XX.XXX.54 и так далее.

- Инициализация устройств: Нажмите «Инициализировать» , чтобы инициализировать устройства.



Поддерживается активация только устройств, находящихся в том же сетевом сегменте, что и ваш компьютер.

5.3.2 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.

Шаг 3. Нажмите «Добавить».

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

Приложение 1. Важные особенности лица. Регистрация

Перед регистрацией

- Очки, головные уборы и борода могут повлиять на эффективность распознавания лиц. • Не закрывайте брови, когда носите головной убор. • Не меняйте сильно форму бороды во время использования устройства; в противном случае распознавание лиц может быть нарушено.

неудача.

- Держите лицо в чистоте. •

Держите устройство на расстоянии не менее 2 метров от источника света и не менее 3 метров от других источников света. окна или двери; в противном случае подсветка и прямые солнечные лучи могут повлиять на эффективность распознавания лиц контроллером доступа.

Во время регистрации

- Вы можете зарегистрировать лица через устройство или через платформу. Для регистрации через
 - Расположите голову по центру рамки для фотосъемки. Будет сделано фотоизображение лица. автоматически.



- Не трясите головой или телом, иначе регистрация может не удался. • Избегайте одновременного появления двух лиц в кадре.

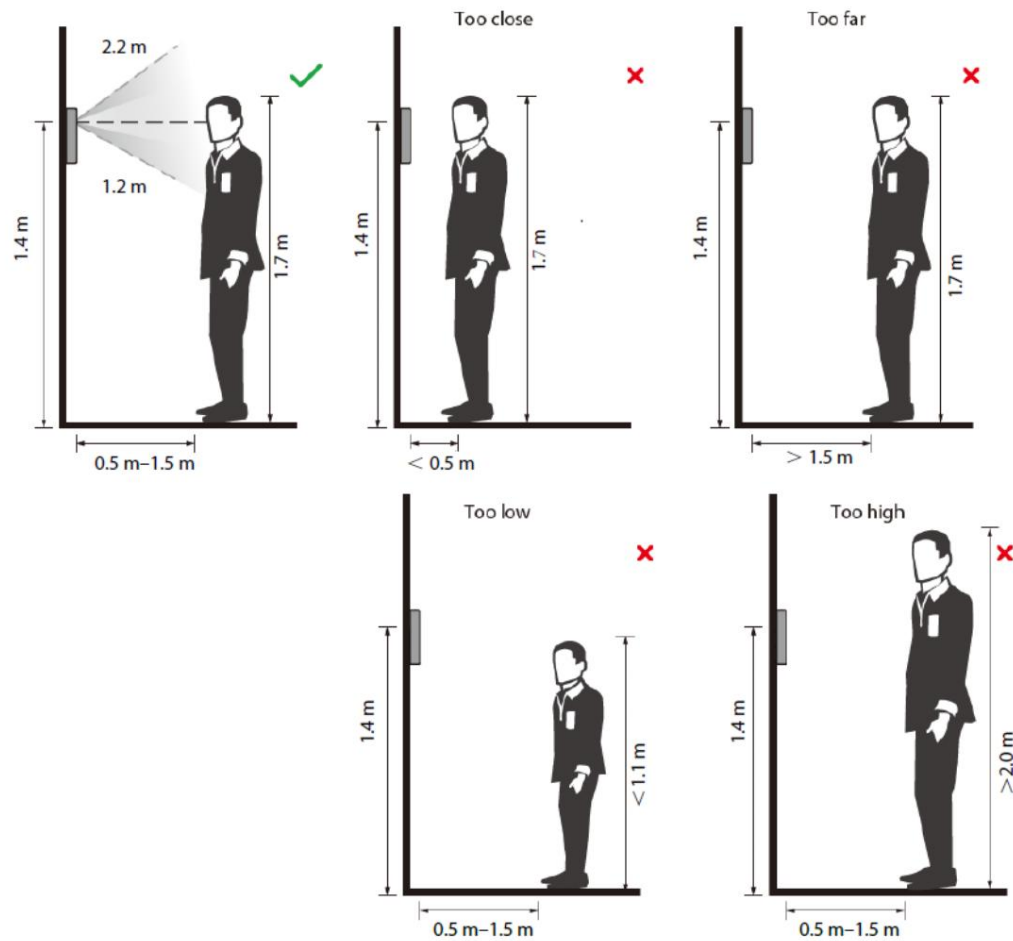
Положение лица

Если ваше лицо находится не в правильном положении, точность распознавания лиц может снизиться.



Положение лица, показанное ниже, приведено только для справки и может отличаться от фактического.

Приложение, Рисунок 1-1. Правильное положение лица.



Требования к лицам

- Убедитесь, что лицо чистое, а лоб не закрыт волосами. • Не носите очки, шляпы, густую бороду или другие украшения для лица, которые влияют на внешний вид лица. запись.
- Смотрите на экран с открытыми глазами, без мимики, и направьте лицо в центр камеры. • При записи лица или распознавании лиц не располагайте лицо слишком близко или слишком далеко от камеры.

Приложение, Рисунок 1-2. Положение головы.



Приложение, Рисунок 1-3 Расстояние между границами



- При импорте изображений лиц через платформу управления убедитесь, что изображение разрешение находится в диапазоне от 150 × 300 пикселей до 600 × 1200 пикселей. Рекомендуется, чтобы разрешение было больше 500 × 500 пикселей, размер изображения был меньше 100 КБ, а имя изображения и идентификатор человека совпадали. • Убедитесь, что лицо занимает более 1/3, но не более 2/3 всей площади изображения, а соотношение сторон не превышает 1:2.

Приложение 2. Важные моменты, касающиеся QR-кода.

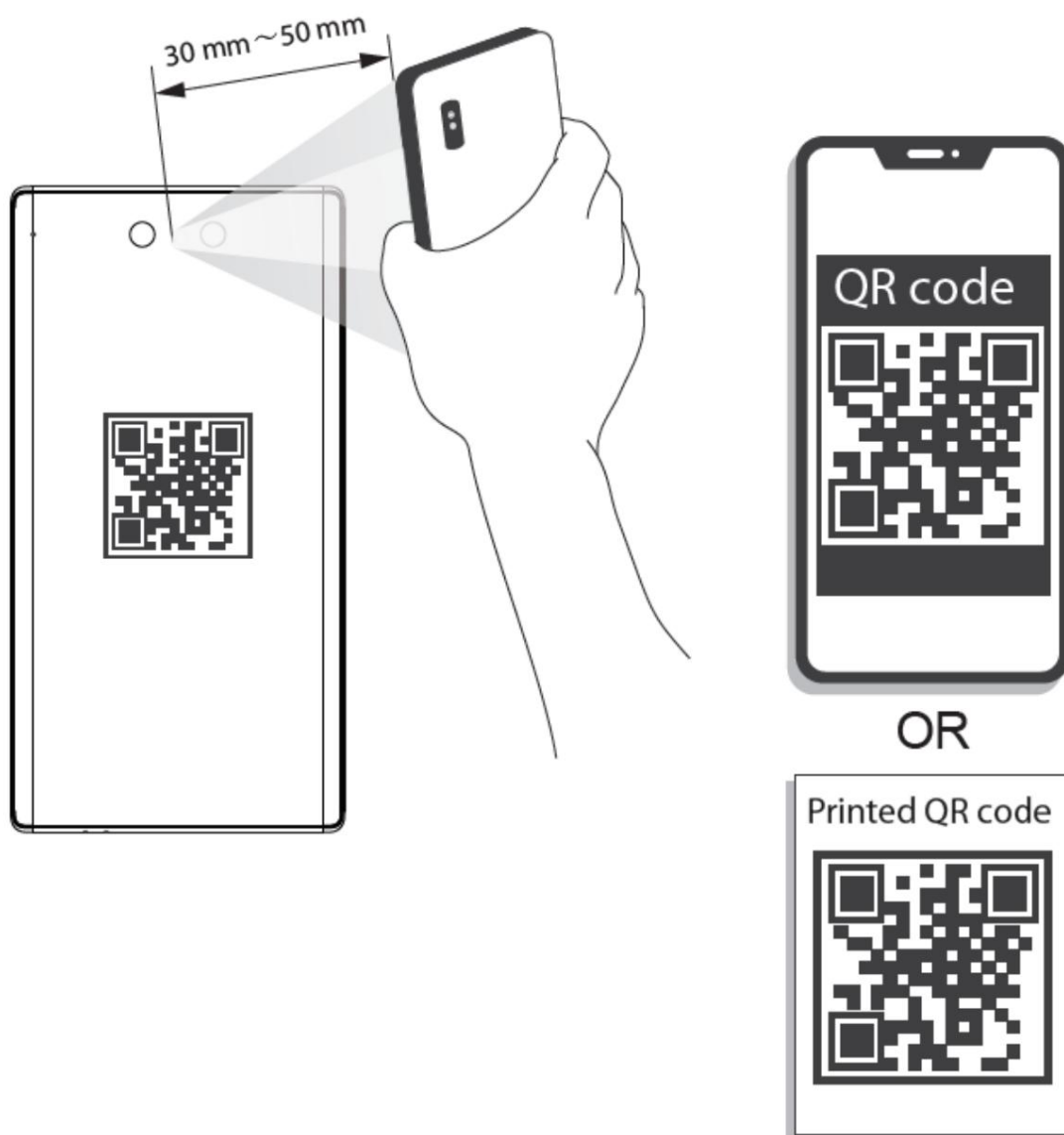
Сканирование

Разместите QR-код на телефоне на расстоянии 30–50 мм от сканирующего объектива. Поддерживаются QR-коды размером более 30 мм × 30 мм и размером менее 128 байт.



- Расстояние обнаружения QR-кода зависит от количества байтов и размера QR-кода. • Убедитесь, что QR-код выровнен относительно объектива, и избегайте попадания прямых солнечных лучей.

Приложение, Рисунок 2-1. Сканирование QR-кода.



Приложение 3. 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. Включить 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 совместимого 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.