

Контроллер доступа

Руководство пользователя



V1.0.0

Предисловие

Общий

В данном руководстве описаны функции и принцип работы устройства (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.
 ESD	Электростатически чувствительные устройства. Указывает на устройство, чувствительное к электростатическому разряду.
 ELECTRIC SHOCK	Указывает на опасно высокое напряжение. Будьте осторожны, избегайте контакта с электричеством.
 LASER RADIATION	Указывает на опасность лазерного излучения. Будьте осторожны и избегайте воздействия лазерного луча.
 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.	Ноябрь 2023 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 см. бумажное руководство пользователя, воспользуйтесь нашим CD-ROM, отсканируйте QR-код или посетите наш официальный сайт. Руководство предназначено только для ознакомления. Между электронной и бумажной версиями могут быть незначительные различия.

- Все дизайнерские решения 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.

Оглавление

Предисловие.....	Я
1 Обзор.....	1
2. Веб-операции.....	2
2.1 Инициализация.....	2
2.2 Вход в систему.....	2
2.3 Сброс пароля.....	3
2.4 Главная страница.....	4
2.5 Управление персоналом.....	4
2.5.1 Добавление человека.....	4
2.5.2 Режим проверки.....	7
2.6 Настройка контроля доступа.....	8
2.6.1 Настройка общих планов.....	8
2.6.2 Настройка планов на время праздников.....	9
2.6.3 Настройка параметров дверей.....	11
2.6.4 Настройка дополнительных параметров.....	16
2.6.5 Настройка способов разблокировки.....	21
2.6.6 Настройка параметров карты.....	22
2.6.7 Настройка сравнения на стороне сервера.....	23
2.6.8 Настройка параметров правил для карт доступа.....	23
2.7 Мониторинг доступа.....	25
2.8 Сетевые настройки.....	26
2.8.1 Настройка TCP/IP.....	26
2.8.2 Настройка порта.....	27
2.8.3 Настройка базовой услуги.....	28
2.8.4 Настройка облачной услуги.....	30
2.8.5 Настройка автоматической регистрации.....	31
2.8.6 Настройка автоматической регистрации CGI.....	32
2.8.7 Настройка автоматической загрузки.....	34
2.9 Настройка системы.....	34
2.9.1 Настройка связи с сигнализацией.....	35
2.9.2 Настройка сигнализации.....	38
2.9.3 Управление пользователями.....	38
2.9.4 Просмотр пользователей в сети.....	41
2.9.5 Настройка времени.....	41
2.10 Настройки безопасности (необязательно)	43
2.10.1 Статус безопасности.....	43
2.10.2 Настройка HTTPS.....	44

2.10.3 Атака Защита.....	44
2.10.4 Установка сертификата устройства.....	47
2.10.5 Установка сертификата доверенного центра сертификации.....	50
2.10.6 Предупреждение безопасности.....	51
2.10.7 Аутентификация безопасности.....	52
2.11 Центр технического обслуживания.....	52
2.11.1 Диагностика одним щелчком мыши.....	52
2.11.2 Информация о системе.....	53
2.11.3 Объем данных.....	53
2.11.4 Журналы просмотра.....	53
2.11.5 Управление техническим обслуживанием.....	54
2.11.6 Обновление системы.....	57
2.11.7 Расширенное техническое обслуживание.....	57
Приложение 1. Важные моменты инструкции по регистрации отпечатков пальцев.....	59
Приложение 2 Рекомендации по безопасности.....	61

1. Обзор

Гибкий и удобный контроллер доступа имеет простую в использовании систему, позволяющую управлять правами доступа на веб-странице через IP-адрес устройства при использовании с считывателем карт.

Он поддерживает функции разблокировки для нескольких пользователей, защиты от повторного прохода и разблокировки первой картой.

Он широко используется в жилых комплексах, деловых центрах, на объектах групп компаний и в коммерческих зданиях.

2. Веб-операции

На веб-странице вы можете настраивать и управлять устройством, включая настройку сетевых параметров, параметров доступа и других операций. Вы также можете обслуживать и обновлять устройство.

В этой главе в качестве примера используется контроллер доступа (четыре двери).



Настройки веб-браузера различаются в зависимости от модели устройства.

2.1 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.

Шаг 3 (необязательно) Ознакомьтесь с соглашением и заявлением и примите их.

Шаг 4. Настройка часового пояса.

Шаг 5. 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. •
- Храните пароль в безопасном месте после инициализации и регулярно меняйте его для повышения безопасности. • Для сброса пароля потребуется адрес электронной почты. Код безопасности будет отправлен на указанный адрес электронной почты.

Шаг 6 (необязательно) Выберите «Автоматическая проверка обновлений».

После выбора функции вы получите уведомление об обнаружении обновления версии.

Шаг 7. Нажмите «Завершено», чтобы завершить инициализацию.

2.2 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».

2.3 Сброс пароля

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

Процедура

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

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

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

Рисунок 2-1. 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 OK.

2.4 Главная страница

Главная страница отображается после успешного входа в систему.

Рисунок 2-2 Главная страница

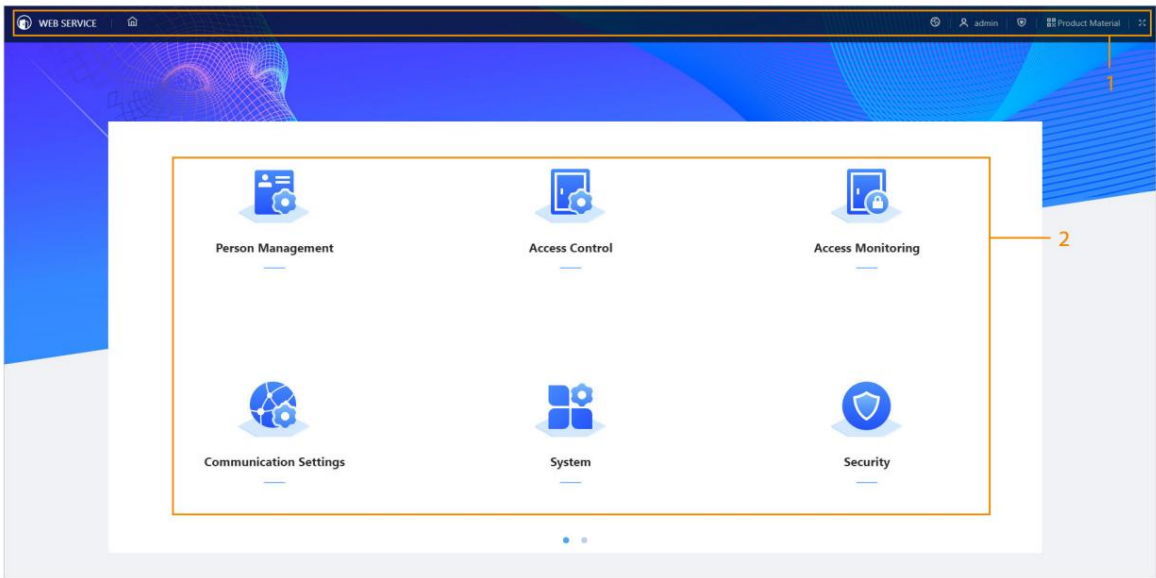


Таблица 2-1. Описание главной страницы

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

2.5 Управление персоналом

2.5.1 Добавление человека

Процедура

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

Шаг 2. Настройка информации о пользователе.

Рисунок 2-3. Добавление пользователей.

Add

Basic Info

* No.

1

Name

* User Type

General User

* Times Used

Unlimited

Validity Period

2037-12-31 23:59:59

Verification Mode

▼ Password

Not Added

Add

> Card

Not Added

> Fingerprint

Not Added

Permission

Type

Use the Same Time Template for All Channels

Channel Permission...

☐ 1 ☐ 2

* General Plan

255-Default x

* Holiday Plan

255-Default x

Add

Add More

Cancel

Таблица 2-2. Описание параметров.

Параметр		Описание
Основная информация	Нет.	Идентификатор пользователя похож на идентификатор сотрудника и может состоять из цифр, букв и символов. их комбинации, а максимальная длина числа составляет 30. персонажей.
	Имя	Имя может содержать до 32 символов (включая цифры, символы, и письма).

Параметр		Описание
	Тип пользователя	- Обычный пользователь : Обычные пользователи могут подтвердить свою личность в соответствии с настроенными методами разблокировки. • - VIP-пользователь : VIP-пользователи могут разблокировать дверь независимо от... Настройки методов разблокировки, периодов разблокировки и разблокировки для нескольких пользователей. - Гостевой пользователь : Гости могут открывать дверь в течение определенного периода времени или определенное количество раз. По истечении определенного периода или времени разблокировки они не могут открыть дверь. • Патрульный пользователь : Патрульные пользователи могут отмечать посещаемость на устройстве, но у них нет разрешения на вход. - Пользователи из черного списка : Если пользователи из черного списка попытаются открыть дверь, они не смогут этого сделать, и будет срабатывать сигнализация. - Другой пользователь : Когда он откроет дверь, она останется открытой. Разблокировано ещё на 5 секунд. - Пользователь 1/Пользователь 2: То же самое, что и для обычных пользователей.
	Количество использований	Установите лимит времени разблокировки для гостевых пользователей. После истечения этого лимита они не смогут открыть дверь.
	Валидность Период	Укажите дату, когда истечет срок действия прав доступа к двери для данного лица.
Проверка Режим	Пароль	Подробности см. в разделе "2.5.2 Режим проверки".
	Карта	
	Отпечаток пальца	
Разрешение	Тип	- Используйте один и тот же шаблон времени для всех каналов: настройте один и тот же общий план и план на случай праздников для всех каналов. • - Используйте разные шаблоны времени для разных каналов: настройте разные общие планы и планы на случай праздников для разных каналов.  Параметр не отображается для контроллера доступа (одна дверь).
	Канал Разрешения	Цифры обозначают соответствующую дверь. Например, 1 означает дверь 1. Выберите канал, которому вы предоставите права доступа.  - Параметр не отображается для контроллера доступа (одиночного) дверь). - Число может отличаться в зависимости от фактической модели устройства.
	Общий план. Люди	могут открыть дверь в течение установленного временного промежутка.
	План на отпуск	В дни установленных праздников люди могут открывать дверь. По умолчанию праздников нет.

Шаг 3. Нажмите «Добавить».

Связанные операции

- Импорт информации о пользователе: Нажмите «Экспорт шаблона» , загрузите шаблон и введите в него информацию о пользователе.
Поместите изображения лиц и шаблон в одну папку, а затем нажмите «Импорт информации о пользователе» , чтобы импортировать папку.

За один раз можно импортировать до 10 000 пользователей.
 - Очистить: Удалить всех пользователей.
 - Обновить: Обновить список пользователей. •
- Поиск: Поиск по имени пользователя или идентификатору пользователя.

2.5.2 Режим проверки

Пароль

Настройте пароль пользователя. Максимальная длина пароля — 8 цифр.

Введите номер пользователя + пароль , чтобы открыть дверь.

Пароль принуждения равен паролю разблокировки + 1. Например, если пароль пользователя — 12345, то пароль принуждения будет 12346. Сигнализация принуждения сработает, если для разблокировки двери будет использован пароль принуждения.

1. Нажмите «Добавить».
2. Введите пароль и подтвердите его.
3. Нажмите ОК.

Карта

Соберите информацию о карте с помощью внешних устройств или введите номер карты вручную.

- Введите номер карты вручную.

1. Нажмите «Добавить».
2. Введите номер карты и нажмите «Добавить».

- Автоматическое считывание номера с помощью считывателей регистрационных карт (IC-карт или удостоверений личности).

1. Нажмите , а затем нажмите «Изменить» , чтобы выбрать устройство для чтения регистрационных данных, подключенное к...
«Добавить контроллер доступа». Выберите из вариантов «IC-карта» и «ID-карта».
2. Нажмите «Прочитать карту», а затем проведите картой по считывающему устройству для регистрации.

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.

3. Нажмите «Добавить».

- Автоматическое считывание номера с помощью регистрационных считывателей (карта Desfire).

1. Нажмите «Добавить» , Затем нажмите «Изменить» , чтобы выбрать карту Desfire , подключенную к устройству доступа.
контроллер.
2. Поместите карту в устройство для считывания регистрационных данных, а затем нажмите «Прочитать карту».

Если на карту Desfire был записан номер карты, он будет считан и отображен здесь.

Если карта пуста, сначала необходимо вписать в нее номер. Номер карты будет автоматически сгенерирован на компьютере и записан на карту.

3. Нажмите «Добавить».

- Автоматическое считывание номера через устройство чтения карт, подключенное к устройству.

1. Нажмите «Добавить», , Затем нажмите «Изменить», чтобы выбрать устройство чтения карт. Выберите «Устройство», а затем выберите конкретное устройство чтения.

2. Нажмите «Прочитать карту», а затем проведите картой по внешнему устройству.

На экране отображается 60-секундный обратный отсчет, напоминающий о необходимости провести картой, после чего система автоматически считает номер карты. Если 60-секундный отсчет истек, нажмите кнопку «Считать карту» еще раз, чтобы начать новый отсчет.

3. Нажмите «Добавить».

Пользователь может зарегистрировать максимум 5 карт. Введите номер карты или проведите картой по считывателю, после чего будет считана информация 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 через считыватель карт, подключенный к компьютеру, или через внешний считыватель карт, подключенный к контроллеру доступа.

1. Нажмите , а затем нажмите «Изменить», чтобы выбрать устройство для считывания регистрационных данных или устройство для считывания карт. «Добавить», чтобы подключиться к контроллеру доступа.

2. Прижмите палец к сканеру в соответствии с инструкциями на экране.

3. Нажмите «Добавить».



• Функция распознавания отпечатков пальцев доступна только на некоторых моделях. • Не рекомендуется устанавливать первый отпечаток пальца в качестве отпечатка для принудительного снятия. • Один пользователь может установить только один отпечаток пальца для принудительного снятия.

2.6 Настройка контроля доступа

2.6.1 Настройка общих планов

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

Процедура

Шаг 1. Войдите на веб-страницу.

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

Шаг 3. Нажмите +.

1. Укажите название и номер тарифного плана.

2. Перетащите ползунок времени, чтобы настроить время для каждого дня.

3. (Необязательно) Нажмите «Копировать», чтобы скопировать конфигурацию на оставшиеся дни.

Рисунок 2-4. Настройка общего плана.

The screenshot displays a web interface for configuring a 'General Plan 1'. At the top, there is a text input field for the name, a dropdown for the number (set to 0), and a 'Time Plan' dropdown. Below these is a time selection dialog showing a range from 09:00:00 to 23:59:59, with 'OK' and 'Delete' buttons. The main area is a grid representing a week's schedule. The columns are labeled 0 through 9, and the rows are labeled Sun through Sat. The grid is filled with blue blocks, indicating a continuous schedule. To the right of each row is a 'Copy' button. At the bottom of the interface are 'Apply' and 'Cancel' buttons.

Шаг 4. Нажмите «Применить».

2.6.2 Настройка планов отпусков

Вы можете настроить до 128 групп праздников (от №0 до №127), и в каждую группу праздников можно добавить до 16 праздников.

После этого вы можете назначить настроенные группы праздников плану праздников. Пользователи могут открывать дверь только в течение времени, указанного в плане праздников.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «План на случай праздников».

Шаг 3. Нажмите +.

1. Укажите название и номер тарифного плана.

Рисунок 2-5. Добавить план отпуска.

* Name

Holiday Plan 1

No.

0

Time Plan

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Holiday

Holiday List

Add

No.	Holiday Name	Start Time	End Time	Operation
1	National Day	2024-10-01	2024-10-07	  

Apply

Cancel

2. Перетащите ползунок времени, чтобы установить время для праздника.
- Вы можете настроить до 4 периодов.
3. Нажмите «Добавить», укажите название и период, а затем нажмите «ОК», чтобы добавить праздник в список праздников.

Рисунок 2-6. Добавить праздник.

Add

X

Holiday Name

National Day

* Period

2024-10-01 → 2024-10-07



OK

Cancel

4. Нажмите ОК.

Шаг 4. Нажмите «Применить».

Связанные операции

Скопируйте настроенный праздник в другие планы праздничных дней.

Рисунок 2-7 Список праздников

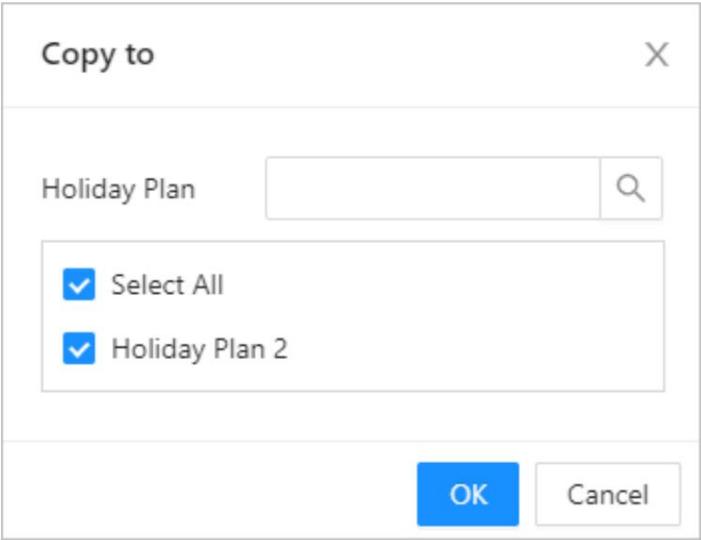
Holiday List

Add

No.	Holiday Name	Start Time	End Time	Operation
1	National Day	2024-10-01	2024-10-07	  

1. Нажмите  , Выберите добавленный план отдыха, а затем нажмите ОК.

Рисунок 2-8. Скопируйте праздник.



2. Нажмите «Применить».

2.6.3 Настройка параметров двери

Настройте состояние двери, способы разблокировки и другие параметры двери.

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите «Контроль доступа» > «Параметры двери».
- Шаг 3. В разделе «Основные настройки» настройте основные параметры контроля доступа.

Рисунок 2-9. Основные параметры

Basic Settings

Name

Door1

Door Status

☒ Normal

☐ Always Closed

☐ Always Open

Normally Open Period

General Plan

0-General Plan 1

Holiday Plan

0-Holiday Plan 1

Normally Closed Period

General Plan

0-General Plan 1

Holiday Plan

0-Holiday Plan 1

Holiday Plan Authentication

0-Holiday Plan 1

Admin Unlock Password

☒

Таблица 2-3. Описание основных параметров.

Параметр	Описание
Имя	Название двери.

Параметр	Описание
Состояние двери	Установите статус двери. - Обычный режим: Дверь будет открываться и закрываться в соответствии с вашими настройками. - Всегда закрыто: Дверь постоянно заперта. • Всегда открыто: Дверь постоянно открыта.
Обычно открытый период	При выборе «Обычный» вы можете выбрать временной шаблон из выпадающего списка. Дверь остается открытой или закрытой в течение заданного времени. Сначала необходимо настроить общий план и план на случай праздников.
Период обычного закрытия	 - Если период открытого состояния конфликтует с периодом закрытого состояния, то период открытого состояния имеет приоритет над периодом закрытого состояния. - Если периоды совпадают с планами на отпуск, планы на отпуск переносятся на более поздний срок. приоритет над периодами.
План на отпуск Аутентификация	В соответствии с установленным планом на праздничные дни разрешен доступ только при постоянно закрытой двери.
Разблокировка пароля администратора	После включения этой функции вы сможете разблокировать дверь, используя пароль администратора. Введите пароль администратора напрямую, без ввода идентификатора пользователя, чтобы разблокировать дверь, независимо от типа пользователя, способа разблокировки, общего плана, плана на время отпуска и прав на защиту от повторного ввода пароля. Только когда дверь находится в нормально закрытом состоянии, пароль администратора нельзя использовать для её разблокировки.

Шаг 4. В разделе «Настройки разблокировки» настройте способ разблокировки и соответствующие параметры.

• Разблокировка комбинации

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

Рисунок 2-10. Настройки разблокировки.

Unlock Settings

Unlock Method

Combination Unlock

Combination Method

☒ Or ☐ And

Unlock Method (Multi-select)

☒ Card ☒ Fingerprint ☒ Password

Door Unlocked Duration

3.0

s (0.2-600)

Unlock Timeout

60

s (1-9999)

Remote Verification

☐

Таблица 2-4. Описание настроек разблокировки.

Параметр	Описание
Способ разблокировки (множественный выбор)	Способы разблокировки могут различаться в зависимости от модели продукта.
Продолжительность открытия двери	После того, как человеку будет предоставлен доступ, дверь останется незапертой в течение определенного времени, чтобы он мог пройти. Это время варьируется от 0,2 до 600 секунд.
Тайм-аут разблокировки	Если включены датчик открытия двери и сигнализация о превышении времени разблокировки, то сработает сигнализация о превышении времени разблокировки, если дверь останется незапертой дольше заданного времени.
Удалённая проверка	Откройте дверь дистанционно.

• 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 комбинации и способ разблокировки на определенный период времени, а затем настройте остальные параметры.

Рисунок 2-11. Разблокировка по периодам.

• Разблокируется несколькими пользователями.

1. В списке «Способ разблокировки» выберите «Разблокировано несколькими пользователями».
2. Нажмите «Добавить», чтобы добавить группы.
3. Выберите способ разблокировки, действительный номер и количество пользователей.
 - ◇ 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.
4. Настройте время ожидания проверки разблокировки для нескольких пользователей.



- ◇ Вы можете добавить до 4 групп.
- ◇ 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.
- ◇ Если вы настроили разблокировку первой карты, и пользователь, которому принадлежит первая карта, входит в группу пользователей, то ему сначала необходимо подтвердить свою личность.

Шаг 5

В разделе «Аварийные сигналы» настройте параметры аварийных сигналов.

Рисунок 2-12. Настройки сигнализации.

Alarm

Door Detector

NO

NC

Intrusion Alarm

Link Local Buzzer

Unlock Timeout Alarm

Link Local Buzzer

Controller Buzzer Mode

Custom Time

Duration

15

s (1-1800)

Link Buzzer of Card Reader Bound t...

Card Reader Buzzer Mode

Custom Time

Duration

15

s (1-255)

Duress Alarm

Таблица 2-5. Описание параметров тревоги.

Параметр	Описание
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. • НЕТ: Разомкнутая цепь образуется, когда дверь фактически открыта. закрыто. • NC: Датчик находится в закороченном состоянии, когда дверь открыта. закрыто.
охранная сигнализация	После включения как датчика открытия двери, так и охранной сигнализации, в случае несанкционированного открытия двери сработает охранная сигнализация, которая будет действовать в течение заданного времени. Функция «Локальный зуммер» : при срабатывании сигнализации устройство издает звуковой сигнал, продолжительность которого по умолчанию составляет 15 секунд.

Параметр	Описание
Сигнализация об истечении времени разблокировки	После включения датчика открытия двери и сигнализации о превышении времени разблокировки, если дверь остается открытой дольше заданного времени, сработает сигнализация о превышении времени разблокировки, которая будет действовать в течение заданного времени. • Привязка локального звукового сигнала : При срабатывании сигнализации... Устройство издает звуковой сигнал. Вы можете настроить режим и продолжительность звукового сигнала. • Звуковой сигнал устройства чтения карт, привязанного к этому каналу : При срабатывании сигнализации подключенный к этому каналу считыватель карт RS-485 издает звуковой сигнал. Вы можете настроить режим и продолжительность звукового сигнала.  Эта функция доступна на некоторых моделях. В режиме звукового сигнала поддерживаются 2 способа. • Пользовательское время: Если время превышает заданное значение В течение определенного времени устройство перестает издавать звуковые сигналы. • До закрытия двери: Когда дверь закрывается, устройство останавливается. пищат.
Сигнал тревоги	Сигнализация сработает при использовании карты принудительного вызова, пароля принудительного вызова или отпечатка пальца для разблокировки двери.

Шаг 6. Нажмите «Применить».

2.6.4 Настройка расширенных параметров

2.6.4.1 Настройка разблокировки первой карты

Определите определенных лиц как первых владельцев карт; другие пользователи смогут подтвердить свою личность и открыть дверь только после того, как первые владельцы карт подтвердят свою личность.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Дополнительные параметры контроля доступа» > «Разблокировка первой карты».

Шаг 3. Выберите дверь, а затем нажмите.



Рисунок 2-13. Назначение пользователям разрешения на доступ к первой карте.

Шаг 4. Выберите общий план и план отдыха.

Первая карта действительна только в течение установленного периода времени. В каждом периоде действия плана, после того как владельцы первой карты подтвердят свою личность, другие пользователи смогут подтвердить свою личность.

Шаг 5. Выберите состояние двери.

- Обычный режим: Пользователи, не имеющие первой карты, должны подтвердить свою личность, чтобы открыть дверь после первой карты. Пользователи карт предоставляют доступ через контроллер доступа.
- Всегда открыто: Дверь остается открытой после того, как первый пользователь карты предоставит доступ через систему доступа. Контроллер.

Шаг 6. Нажмите



Чтобы добавить пользователей с первой карточкой, нажмите кнопку ОК.



- Вы можете выбрать только пользователя, тип пользователя которого — «Обычный пользователь».
- В качестве первого пользователя карты можно назначить до 100 пользователей.

Рисунок 2-14. Добавление пользователей первой карты.

Add User

Select Person

User ID/Name

	No.	User ID	Name
☒	1	1	

Selected People

Clear

No.	User ID	Name	Operation
1	1		

OK

Cancel

Шаг 7. Нажмите «Применить».

2.6.4.2 Настройка защиты от повторного прохода

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

Справочная информация

- Если человек имеет право войти, но выходит без проверки, сработает сигнализация. Если они попытаются войти снова, доступ будет заблокирован.
- Если человек войдет, следуя за другим без подтверждения личности, при попытке выхода сработает сигнализация, и доступ будет заблокирован.

Процедура

- Шаг 1. Войдите на веб-страницу.
- Шаг 2. Выберите «Контроль доступа» > «Дополнительные параметры контроля доступа» > «Группа защиты от повторного прохода».
- Конфигурация.
- Шаг 3. Нажмите + , настройте параметры, а затем нажмите Применить.

Рисунок 2-15. Защита от обратного прохода.

Anti-passback Group

+

🗑

1

☐

 Anti-passback Group 1

🗑

Reset Time

30

 min (5-300)

Time Templates

General Plan

255-Default

▼

Holiday Plan

255-Default

▼

Anti-passback Group Config

?

Entry Group(0/4)

+

 Add

🗑

 Clear

No data

Exit Group(0/4)

+

 Add

🗑

 Clear

No data

3

Apply

Cancel

Таблица 2-6. Описание параметров группы защиты от повторного прохода.

Параметр	Описание
Сбросить время	Настройте время срабатывания сигнализации о невозможности повторного прохода после проверки при входе или время для повторной проверки и входа после срабатывания сигнализации о невозможности повторного прохода. Например, если установить время в 30 минут, то если человек войдет после проверки и выйдет без проверки, сработает сигнализация, если он попытается войти снова в течение 30 минут. После срабатывания сигнализации человек сможет пройти проверку и войти снова через 30 минут.
Генеральный план	Выберите недельный и праздничный тарифы. Функция предотвращения повторного прохода действует в течение указанного времени.
План на отпуск	
Вступительная группа	Нажмите «Добавить», а затем выберите считыватели карт для входа и выхода.
Выходная группа	📖 Необходимо добавить как минимум 2 группы.

Шаг 4. Нажмите «Применить».

Шаг 5. Нажмите

☐

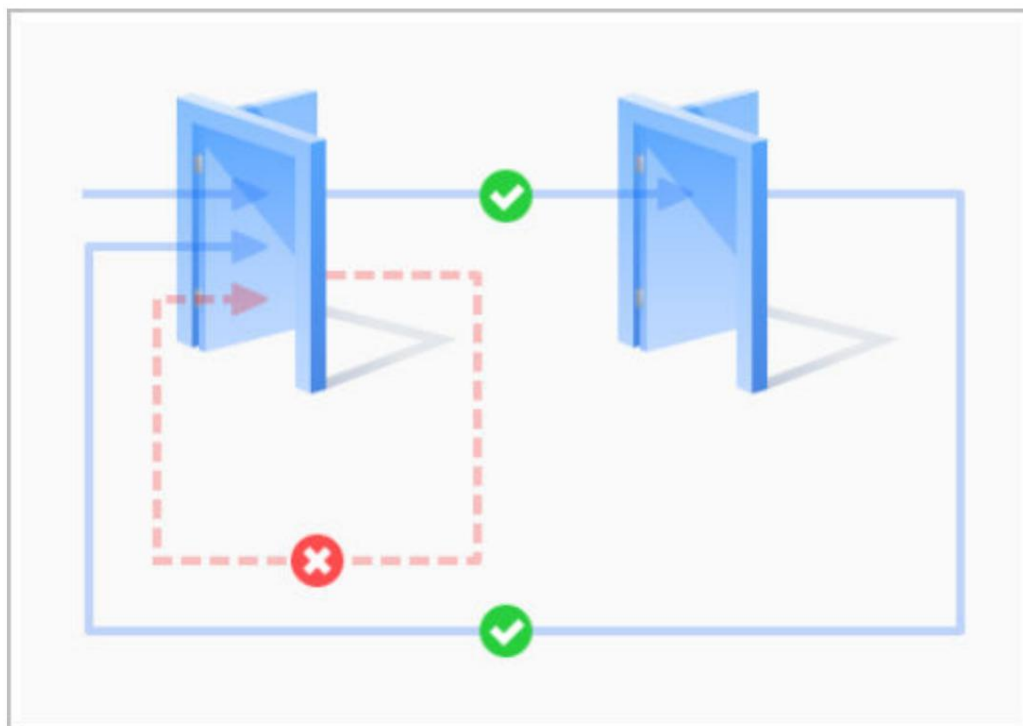
 для включения этой функции.

Результаты

Номер группы указывает последовательность считывания карт. Карту необходимо использовать в соответствии с указанной последовательностью групп. Например, необходимо провести картой через считыватель в группе 1, а затем через другой считыватель.

Сначала считыватель для группы 2, затем считыватель для группы 3 и так далее. Пока вы проводите карту, следуя установленной последовательности, система работает исправно.

Рисунок 2-16. Функция защиты от повторного прохода.



2.6.4.3 Настройка блокировки нескольких дверей

Блокировка нескольких дверей позволяет запирает две или более дверей. Если одна дверь разблокирована, доступ к остальным дверям будет запрещен. Одно устройство поддерживает настройку двух дверей, и две двери не влияют друг на друга.



Эта функция доступна в некоторых моделях, поддерживающих несколько дверей.

- Если вы настроили блокировку нескольких дверей для дополнительных контроллеров через главный контроллер и планируете восстановить заводские настройки главного контроллера, мы рекомендуем одновременно восстановить заводские настройки и дополнительного контроллера.
- При использовании правила блокировки нескольких дверей в условиях нестабильной сети дверь может открыться после проверки личности, но при этом может сработать сигнализация по истечении времени ожидания на считывателе карт. Пожалуйста, убедитесь в стабильности вашей сети.

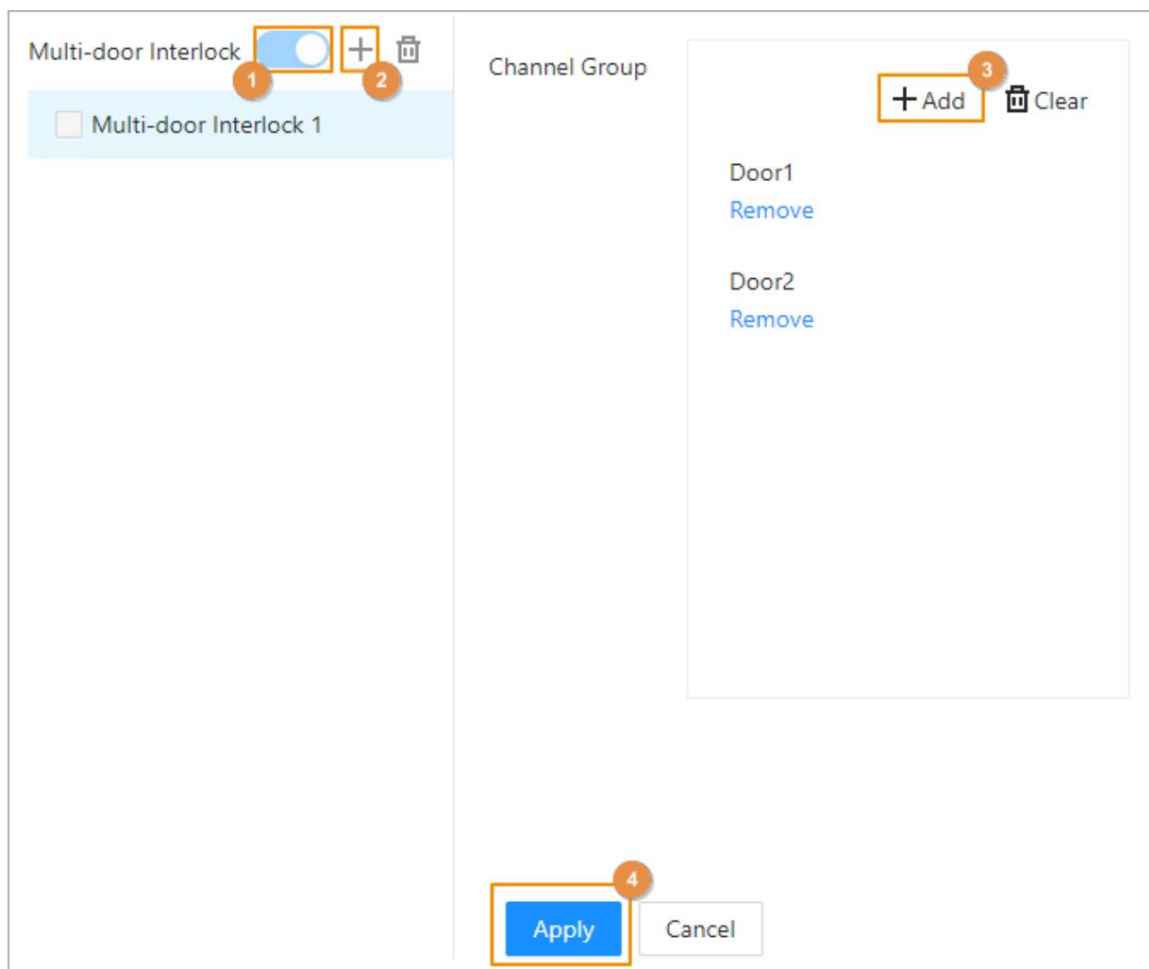
Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Дополнительные настройки контроля доступа» > «Блокировка нескольких дверей».

Шаг 3 Нажмите ☐ Чтобы включить эту функцию, нажмите +.

Рисунок 2-17. Многодверная блокировка.



Шаг 4. Нажмите «Добавить», Выберите дверь, а затем нажмите ОК.

Шаг 5. Нажмите «Применить».

2.6.5 Настройка методов разблокировки

Процедура

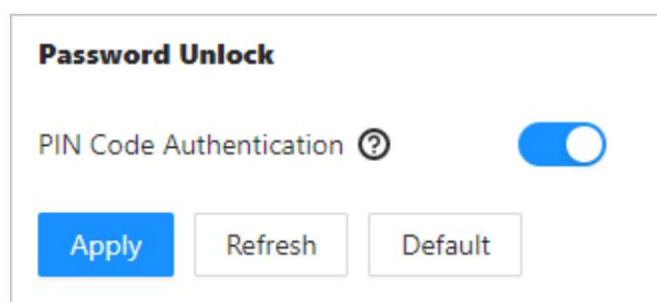
Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройка метода разблокировки».

Шаг 3. Включите или выключите аутентификацию по PIN-коду.

При включенной аутентификации по PIN-коду вы можете открыть дверь, используя только пароль.

Рисунок 2-18. Аутентификация по ПИН-коду.



Шаг 4. Нажмите «Применить».

2.6.6 Настройка параметров карты

Справочная информация



Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. Войдите на веб-страницу.

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

Шаг 3. Настройте параметры карты.

Рисунок 2-19 Параметры карты

The image shows two screenshots of a web interface for card configuration.

The top screenshot is titled "Card No. System". It contains a light blue warning box that says "After the number system is changed, the card numbers will become invalid." Below this, there are two radio buttons: "Hexadecimal" (which is selected) and "Decimal". At the bottom of this section are three buttons: "Apply" (in blue), "Refresh", and "Default".

The bottom screenshot is titled "DESFire Card Write". It features a dropdown menu labeled "Acquisition De..." with "Enrollment Reader" selected. Below this is another light blue instruction box: "Please place the card on the swiping area of the device." Underneath is a text input field labeled "Card Number". At the bottom left of this section is a blue "Write" button.

Таблица 2-7. Описание параметров карты.

Элемент	Параметр	Описание
Система номеров карт	Система номеров карт	Выберите десятичный или шестнадцатеричный формат. формат номера карты при использовании Wiegand Считыватель карт подключен. Номер карты. Система одинакова для обоих номеров карт. ввод и вывод.
DESFire Card Write	Устройство сбора данных	Выберите устройство, поместите карту на считыватель, введите номер карты, а затем Нажмите «Записать» , чтобы записать номер карты.  • Поддерживается только шестнадцатеричный формат. • Поддерживает до 8 символов.
	Номер карты	

2.6.7 Настройка сравнения на бэкэнде

Передайте данные, такие как QR-код или номер карты, напрямую на стороннюю платформу для проверки данных. вместо проверки данных на устройстве.

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

Рисунок 2-20. Сравнение бэкэндов.

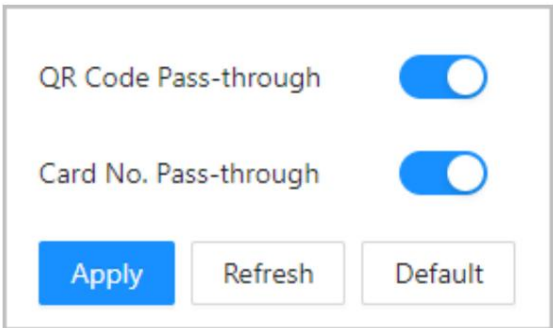


Таблица 2-8. Сравнение бэкэндов.

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 третьей стороне. платформа для проверки данных.

2.6.8 Настройка параметров правил использования карт доступа

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

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройка правил использования карт доступа».

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

Рисунок 2-21. 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 2-9. Описание формата Wiegand.

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

Шаг 4. Нажмите ОК.

Связанные операции

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

- ◆ Номер карты должен состоять из 5 символов, а код объекта — не более чем из 3 символов.
При ручном вводе номера карты система автоматически добавляет ведущий ноль к фиксированной длине числа. Например, если введенный вами номер карты содержит менее 5 символов, например, 56, к нему добавляется ведущий ноль, чтобы зафиксировать длину числа в 5 символов, например, 00056, а также еще один ноль, выполняющий функцию кода объекта. Таким образом, окончательный номер карты будет 000056.

2.7 Мониторинг доступа

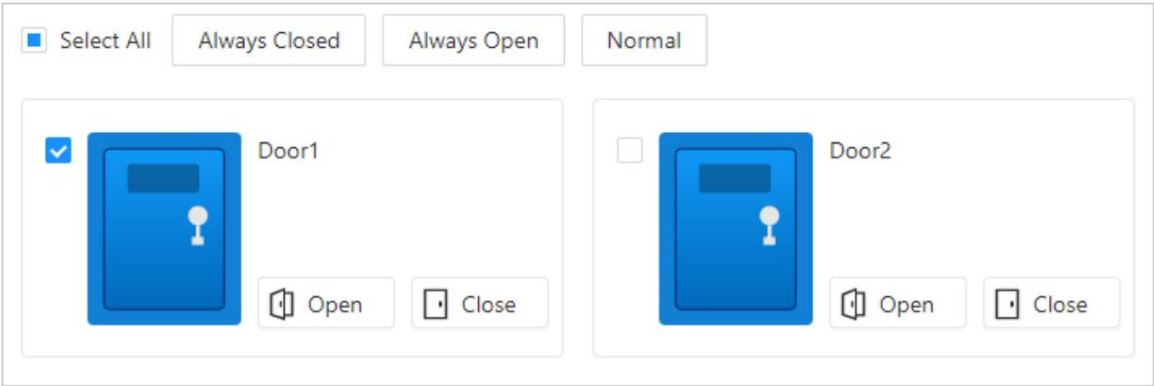
Войдите на веб-страницу, выберите «Мониторинг доступа», и отобразятся все подключенные двери.

Операции по управлению дверью

- Нажмите «Открыть» или «Закрыть» рядом с дверью, чтобы дистанционно управлять ею. •
Выберите дверь, а затем нажмите «Всегда открыта» или «Всегда закрыта», чтобы дистанционно управлять ею.

Дверь будет оставаться открытой или закрытой постоянно. Вы можете выбрать дверь, а затем нажать «Нормальный», чтобы восстановить работу системы контроля доступа в обычном режиме, и дверь будет открываться или закрываться в зависимости от настроенных методов проверки.

Рисунок 2-22. Действия по управлению дверью.



Информация о мероприятии

В разделе «Информация о событии» выберите тип события, чтобы просмотреть события. Нажмите на  чтобы завершить все события.
ссылку «Информация о событии» (Рисунок 2-23).

Event Info ☒ Select All ☒ Alarm ☒ Abnormal ☒ Normal 			
Time	Camera Name	Event Info	Description
2024-07-30 00:32:00	Door1	Alarm	Unlock Timeout Alarm
2024-07-30 00:32:00	Door1	Alarm	Unlock Timeout Alarm

Подробности

Отображаются подробные сведения об устройстве. Здесь вы можете просмотреть IP-адрес, тип устройства и модель устройства.

2.8 Сетевые настройки

2.8.1 Настройка TCP/IP

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

Процедура

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

Шаг 2. Настройте параметры.

Рисунок 2-24 TCP/IP

The image shows a network configuration window for TCP/IP. It contains the following fields and controls:

- NIC:** A dropdown menu showing "NIC 1".
- Mode:** Two radio buttons: "DHCP" (unselected) and "Static" (selected).
- MAC Address:** A text field with a blurred placeholder.
- IP Version:** A dropdown menu showing "IPv4".
- IP Address:** A text field with a blurred placeholder.
- Subnet Mask:** A text field with a blurred placeholder.
- Default Gateway:** A text field with a blurred placeholder.
- Preferred DNS:** A text field with a blurred placeholder.
- Alternate DNS:** A text field with a blurred placeholder.
- MTU:** A text field containing the value "1500".
- Buttons:** At the bottom, there are three buttons: "Apply" (blue), "Refresh", and "Default".

Таблица 2-10. Описание TCP/IP.

Параметр	Описание
Режим	• Статический: Введите IP-адрес, маску подсети и шлюз вручную. • DHCP: Расшифровывается как Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста). При включении DHCP устройству автоматически будут присвоены IP-адрес, маска подсети и шлюз.
MAC-адрес	MAC-адрес устройства.
IP-версия	IPv4 или IPv6.
IP-адрес	Если вы установите режим «Статический», настройте IP-адрес, маску подсети и шлюз.  • IPv6-адрес представляется в шестнадцатеричном формате. • Для версий IPv6 не требуется установка масок подсети. • IP-адрес и шлюз по умолчанию должны совпадать. • сегмент сети.
Маска подсети	
Шлюз по умолчанию	
Предпочитаемый DNS	Укажите IP-адрес предпочтительного DNS-сервера.
Альтернативный DNS	Укажите IP-адрес альтернативного DNS-сервера.
MTU	MTU (Maximum Transmission Unit) — это максимальный размер данных, который может быть передан в одном сетевом пакете в компьютерных сетях. Более высокое значение MTU может повысить эффективность передачи данных по сети за счет уменьшения количества пакетов и связанных с этим сетевых накладных расходов. Если устройство на пути следования по сети не может обрабатывать пакеты определенного размера, это может привести к фрагментации пакетов или ошибкам передачи. В сетях Ethernet обычно используется значение MTU 1500 байт. Однако в некоторых случаях, например, при использовании PPPoE или VPN, могут потребоваться меньшие значения MTU для соответствия требованиям конкретных сетевых протоколов или служб. Ниже приведены рекомендуемые значения MTU для справки: • 1500: Максимальное значение для пакетов Ethernet, также является значением по умолчанию. Это типичная настройка для сетевых подключений без PPPoE и VPN, некоторых маршрутизаторов, сетевых адаптеров и коммутаторов. • 1492: Оптимальное значение для PPPoE • 1468: Оптимальное значение для DHCP. • 1450: Оптимальное значение для VPN.

Шаг 3. Нажмите «Применить».

2.8.2 Настройка порта

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

Процедура

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

Шаг 2. Настройте порты.

Рисунок 2-25. Настройка портов.

Max Connection

50

(1-50)

TCP Port

37777

(1025-65535)

HTTP Port

80

HTTPS Port

443

Apply

Refresh

Default



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

Таблица 2-11. Описание портов.

Параметр	Описание
Максимальное соединение	Вы можете установить максимальное количество клиентов (например, веб-страниц, настольных компьютеров и мобильных устройств), которые могут одновременно получать доступ к устройству.
TCP-порт	Значение по умолчанию — 37777.
HTTP-порт	Значение по умолчанию — 80. Если вы изменили номер порта, добавьте номер порта после IP-адреса при доступе к веб-странице.
Порт HTTPS	Значение по умолчанию — 443.

Шаг 3. Нажмите «Применить».

2.8.3 Настройка базовой службы

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

Процедура

Шаг 1. Выберите «Настройки связи» > «Основные услуги».

Шаг 2. Настройка базовой службы.

Рисунок 2-26. Базовое обслуживание.

SSH

Multicast/Broadcast Search

CGI

ONVIF

Emergency Maintenance

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

Private Protocol Authentication Mode

Security Mode (Recommended)

Private Protocol

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

TLSv1.1

Apply

Refresh

Default

Таблица 2-12. Описание основных параметров обслуживания.

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

Параметр	Описание
TLSv1.1	TLSv1.1 означает Transport Layer Security версии 1.1. TLS — это криптографический протокол, предназначенный для обеспечения безопасной и аутентифицированной связи в компьютерной сети.  При включении протокола TLSv1.1 могут возникнуть риски безопасности. Просим принять это к сведению.

Шаг 3. Нажмите «Применить».

2.8.4 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.

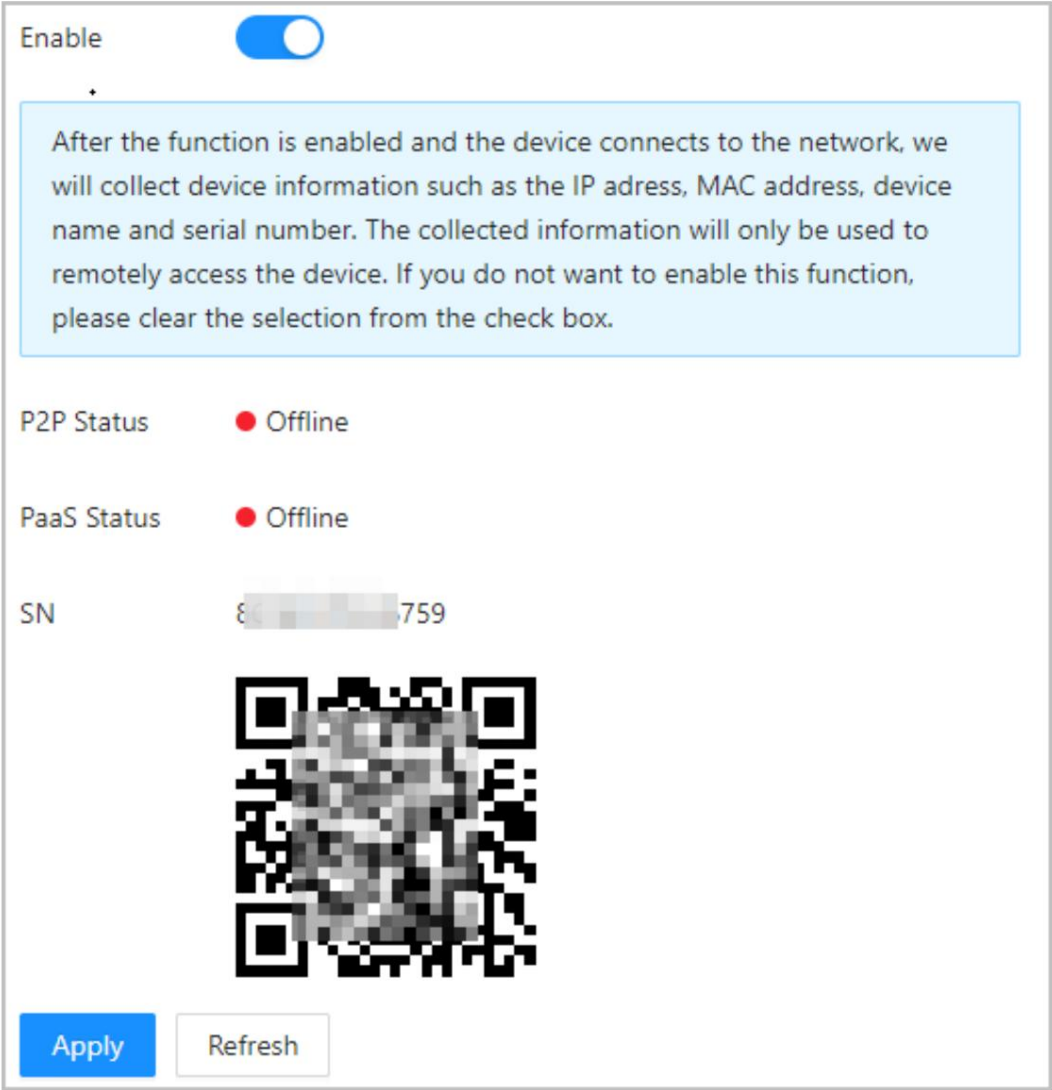
Процедура

Шаг 1. На главной странице выберите «Настройки связи» > «Облачный сервис».

Шаг 2. Включите функцию облачного сервиса.

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

Рисунок 2-27. Облачный сервис.



Шаг 3. Нажмите «Применить».

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

2.8.5 Настройка автоматической регистрации

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

Справочная информация



Автоматическая регистрация поддерживает только SDK.

Процедура

Шаг 1. На главной странице выберите «Настройки связи» > «Автоматическая регистрация».

Шаг 2. Включите функцию автоматической регистрации и настройте параметры.

Рисунок 2-28. Регистрация автомобиля.

Enable

Server Address

Port

7000

(1-65535)

Registration ID

none

Apply

Refresh

Default

Таблица 2-13. Описание автоматической регистрации.

Параметр	Описание
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».

2.8.6 Настройка автоматической регистрации CGI

Подключитесь к сторонней платформе через протокол CGI.

Справочная информация



Поддерживается только IPv4.

Процедура

Шаг 1. На главной странице выберите «Настройки связи» > «Автоматическая регистрация CGI».

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

Шаг 3 Нажмите  , а затем настройте параметры.

Рисунок 2-29 Автоматическая регистрация CGI

Edit

Enable

Device ID

none

Address Type

Host IP

Host IP

Port

60005

HTTPS

Username

Password

OK

Cancel

Таблица 2-14. Описание автоматической регистрации.

Параметр	Описание
Идентификатор устройства	Поддерживает до 32 байт, включая китайские иероглифы, цифры, буквы и специальные символы.
Тип адреса	Поддерживаются 2 способа регистрации.
IP-адрес хоста	• 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 передачи данных по компьютерной сети.
Имя пользователя	Введите имя пользователя и пароль устройства.
Пароль	

Шаг 4. Нажмите «Применить».

2.8.7 Настройка автоматической загрузки

Передавайте информацию о пользователях и разблокируйте записи через платформу управления.

Процедура

Шаг 1. На главной странице выберите «Настройки связи» > «Автоматическая загрузка».

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 2-30 Автоматическая загрузка

Таблица 2-15. Описание параметров.

Параметр	Описание
IP-адрес/доменное имя	IP-адрес или доменное имя платформы управления.
Порт	Порт платформы управления.
HTTPS	Доступ к платформе управления осуществляется через HTTPS. HTTPS обеспечивает безопасность связи в компьютерной сети.
Аутентификация	Включите аутентификацию учетной записи при доступе к платформе управления. Для входа потребуется имя пользователя и пароль.
Чётный тип	Выберите тип события, которое будет отправлено на платформу управления. • Перед использованием этой функции включите функцию «Отправка информации о человеке». • Информация о человеке может быть отправлена только одному человеку. Платформа управления и записи о разблокировке могут передаваться на несколько платформ управления.

Шаг 5. Нажмите «Применить».

2.9 Настройка системы

2.9.1 Настройка связи между сигналами тревоги



- Если устройство добавлено в платформу управления, настройки оповещений будут синхронизированы с ним. платформа.
 - Эта функция доступна только на моделях, имеющих входные и выходные порты для сигнализации. •
- Количество входных и выходных портов для сигнализации различается в зависимости от модели изделия.

2.9.1.1 Настройка канала ввода сигнала тревоги

Вы можете настроить связь между сигналами тревоги.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Система > Настройка связи с сигнализацией > Сигнализация.

Шаг 3 Нажмите  Рядом с входным каналом сигнализации можно настроить параметры.

Рисунок 2-31. Связь между сигналами тревоги.

Enable ☒

Alarm Input Cha...1

Alarm Input Na...Zone1

Alarm Input TypeNO

Link Fire Safety ...☐

Number of EOLs0EOL

ResistanceOK

Module TypeLocal

Address--

Channel No.--

Alarm-out Port☐

Duration30s (1-300)

Alarm Output Channel

1

2

3

4

5

6

7

8

9

10

11

12

Access Control L...☐

Link Local Buzzer☐

Таблица 2-16. Описание входного сигнала тревоги.

Параметр	Описание
Название входного сигнала	тревоги. Настройте название.
Тип входного сигнала тревоги	Выберите «Нет» или «НЗ» в зависимости от типа внешнего устройства ввода сигнала тревоги. • NO: Входное устройство сигнализации находится в нормально разомкнутом (NO) состоянии, когда сигнал тревоги не сработал. Замыкание цепи приводит к срабатыванию сигнализации. • NC: Входное устройство сигнализации находится в нормально замкнутом (NC) состоянии, когда Сигнализация не сработала. Срабатывание сигнализации происходит при размыкании нормально замкнутой цепи.
Пожарная безопасность Link Контроль	После включения этой функции по умолчанию открываются все каналы вывода сигналов тревоги и каналы контроля доступа.
Количество смертей	• Локальный вход для сигнализации: можно выбрать один из вариантов: 0EOL (сигнал тревоги и нормальный режим) или 1EOL (аварийный сигнал, нормальный режим и обрыв цепи) и 2EOL (аварийный сигнал, нормальный режим, обрыв цепи и короткое замыкание). • Внешний модуль расширения: Вы можете выбрать один из следующих вариантов: 0EOL (сигнализация и нормальный режим), 1EOL NC (сигнализация, нормальный режим и короткое замыкание), 1EOL NO (сигнализация, нормальный режим и обрыв цепи), 2EOL (сигнализация, нормальный режим, обрыв цепи и короткое замыкание) и 3EOL (нормальный режим, сигнализация, обрыв цепи, короткое замыкание и блокировка). При подключении внешних устройств тревожного сигнала, для состояния 0EOL резисторная конфигурация не требуется, в то время как для состояний 1EOL, 2EOL и 3EOL требуется конфигурация из 1, 2 и 3 резисторов соответственно. Значения напряжения для каждого состояния тревоги изменяются в зависимости от различных комбинаций количества резисторов и их значений сопротивления, поэтому выбор следует делать гибко, исходя из фактически используемых внешних устройств тревожного сигнала.  • Контроллер доступа модели C поддерживает полиморфную сигнализацию только для первых двух входных каналов сигнализации. • Контроллер доступа модели B не поддерживает полиморфную сигнализацию.
Сопротивление	• Для локального входа сигнализации этот параметр настраивать не требуется. • Выберите сопротивление в соответствии с фактически подключенным сигнальным устройством.
Тип модуля	Поддерживает подключение модулей RS-708 и RS-808.
Адрес	Выберите тип, адрес и номер канала в соответствии с фактически подключенными модулями.
Номер канала	-- неверный номер канала.  Для локального ввода сигналов тревоги этот параметр настраивать не нужно.
Порт выхода тревоги	Включите порт выхода тревоги, а затем выберите каналы вывода тревоги. При срабатывании тревоги выбранный выходной сигнал тревоги срабатывает, продолжительность срабатывания по умолчанию составляет 30 секунд.
Продолжительность	
Выходной сигнал тревоги Канал	

Параметр	Описание
Контроль доступа Связь	После включения этой функции, при срабатывании сигнализации, дверь переходит в заданное состояние. - Автоматический режим: Дверь сохраняет состояние, в котором она находилась до срабатывания сигнализации. Если до срабатывания сигнализации состояние двери было нормальным (разрешенная разблокировка), то после срабатывания сигнализации дверь останется в нормальном состоянии. - НЕТ: Дверь автоматически открывается при срабатывании пожарной сигнализации. - НЕТ: Дверь автоматически закрывается при срабатывании пожарной сигнализации. Режим соединения: При выборе состояния двери (NO или NC) настройте режим соединения. - Надежное исполнение: Когда сигнал пожарной тревоги исчезает, дверь остается в текущем состоянии. При желании вы можете вручную изменить ее состояние на предыдущее. - Недостаточное исполнение: Когда сигнал пожарной тревоги исчезает, дверь автоматически возвращается в предыдущее состояние.
Ссылка на локальный звонок	После включения этой функции при срабатывании сигнализации устройство издает звуковой сигнал, продолжительность которого по умолчанию составляет 15 секунд.

Шаг 4. Нажмите OK.

2.9.1.2 Настройка канала вывода сигнала тревоги

Настройте адрес, номер канала и другие параметры при подключении внешних модулей расширения выходного сигнала тревоги.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Система > Настройка связи с сигнализацией > Выходной канал сигнализации.

Шаг 3 Нажмите



Рядом с каналом вывода сигнала тревоги можно настроить параметры.

Рисунок 2-32. Выходной канал сигнализации.

Шаг 4. Нажмите OK.

2.9.2 Настройка сигнализации

Справочная информация



Эта функция доступна на некоторых моделях.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Система > Настройки сигнализации.

Шаг 3. Настройте сигнализацию и связь в соответствии с необходимостью.

Включите или выключите сигнализацию о пониженном напряжении батареи и сигнализацию об отключении электросети. Вы можете включить локальный звуковой сигнал и настроить его продолжительность. После срабатывания сигнализации устройство будет издавать звуковой сигнал в течение заданного периода времени.

Шаг 4. Настройте тип входного сигнала пожарной сигнализации.

Убедитесь, что переключатель пожарной сигнализации на устройстве установлен в положение «НЕТ». Для выбора типа входного сигнала пожарной сигнализации выберите NO или NC.

Шаг 5. Нажмите «Применить».

2.9.3 Управление пользователями

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

2.9.3.1 Добавление администраторов

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

Процедура

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

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



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

Установите надежный пароль, следуя подсказкам по проверке уровня защиты.

Рисунок 2-33. Добавление администраторов.

The screenshot shows a web-based 'Add' dialog box. It has a title bar with the word 'Add' and a close button 'X'. Inside the dialog, there are four input fields arranged vertically. The first three fields are labeled 'Username', 'Password', and 'Confirm Password', each preceded by a red asterisk indicating they are required. The fourth field is labeled 'Remarks'. Below the input fields, there are two buttons: 'OK' (in a blue box) and 'Cancel' (in a white box with a grey border).

Шаг 3. Нажмите OK.



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

2.9.3.2 Сброс пароля

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

Процедура

Шаг 1. Выберите Система > Учетная запись.

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

Шаг 3. Включите функцию сброса пароля.

Рисунок 2-34 Сброс пароля

Password Reset

Enable

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

Email Address

1***@.com

Password Expires in

Never

Days



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

Шаг 4. Нажмите «Применить».

2.9.3.3 Добавление пользователей ONVIF

Справочная информация

Форум открытых сетевых видеоинтерфейсов (ONVIF) — это глобальный открытый отраслевой форум, созданный для разработки глобального открытого стандарта для интерфейса физических IP-устройств безопасности, обеспечивающего совместимость с продукцией различных производителей. Идентификация пользователей ONVIF проверяется с помощью протокола ONVIF. Пользователем ONVIF по умолчанию является администратор.

Процедура

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

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

Рисунок 2-35. Добавить пользователя ONVIF.

Add

* Username

* Password

* Confirm Password

* Group

Please select

OK

Cancel

Таблица 2-17. Описание пользователя ONVIF.

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

Шаг 3. Нажмите ОК.

2.9.4 Просмотр пользователей онлайн

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

2.9.5 Настройка времени

Процедура

Шаг 1. На главной странице выберите Система > Время.

Шаг 2. Настройте время на платформе.

Рисунок 2-36. Настройки даты.

Time and Time Zone



Date :

2024-10-25 Friday

Time :

15:59:29

Time

☒ Manually Set

☐ NTP

System Time

2024-10-25 15:59:29



Sync PC

Time Format

YYYY-MM-DD



24-Hour



Time Zone

(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi



DST

Enable

☐

Type

☒ Date

☐ Week

Start Time

Jan



1



00:00



End Time

Jan



2



00:00



Apply

Refresh

Default

Таблица 2-18. Описание настроек времени.

Параметр	Описание
Время	• Ручная настройка: Введите время вручную или нажмите «Синхронизировать время» , чтобы синхронизировать время с компьютером. • 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 времени	Выберите формат времени.
Часовой пояс	Введите часовой пояс.

Параметр	Описание
летнее время	1. (Необязательно) Включите летнее время. 2. В поле «Тип» выберите «Дата» или «Неделя» . 3. Настройте время начала и окончания перехода на летнее время.

Шаг 3. Нажмите «Применить».

2.10 Настройки безопасности (необязательно)

2.10.1 Состояние безопасности

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

Справочная информация •

Определение пользователей и служб: Проверьте, соответствует ли текущая конфигурация 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

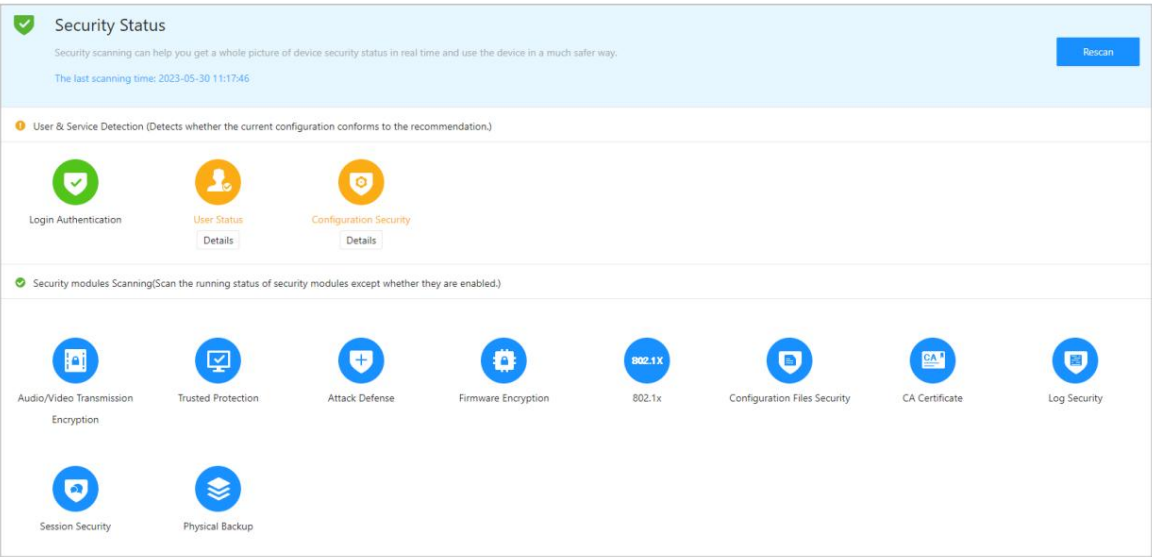
Шаг 1. Выберите «Безопасность» > «Состояние безопасности».

Шаг 2. Нажмите «Повторное сканирование» , чтобы выполнить проверку безопасности устройства.



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

Рисунок 2-37. 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

Игнорируемые элементы будут выделены серым цветом.

• Нажмите «Оптимизировать» , чтобы устранить неполадку.

2.10.2 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 Безопасность > Системные службы > HTTPS.

Шаг 2. Включите службу HTTPS.



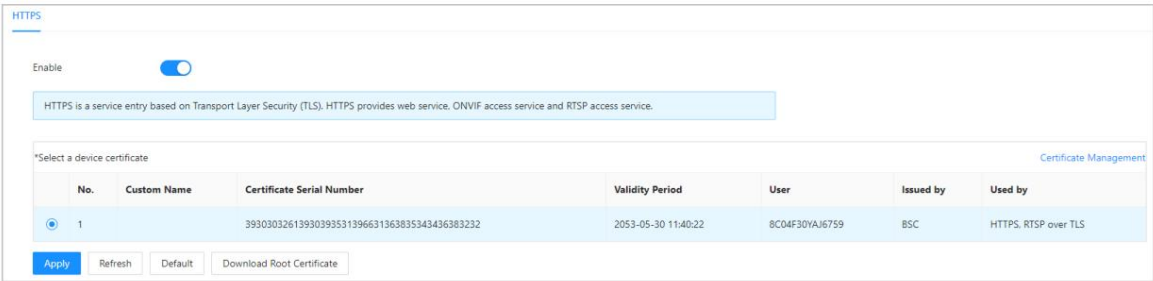
Если включить параметр "Совместимость с TLS v1.1 и более ранними версиями", могут возникнуть риски для безопасности. Обращаем ваше внимание.

Шаг 3. Выберите сертификат.



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

Рисунок 2-38 HTTPS



Шаг 4. Нажмите «Применить».

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

2.10.3 Атака Защита

2.10.3.1 Настройка брандмауэра

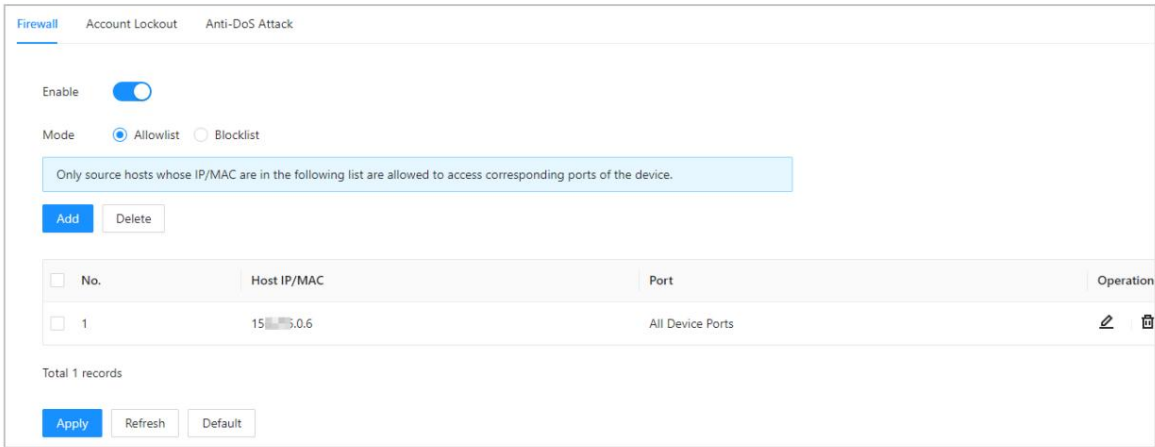
Настройте брандмауэр для ограничения доступа к устройству.

Процедура

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

Шаг 2. Нажмите, чтобы включить функцию брандмауэра.

Рисунок 2-39 Межсетевой экран

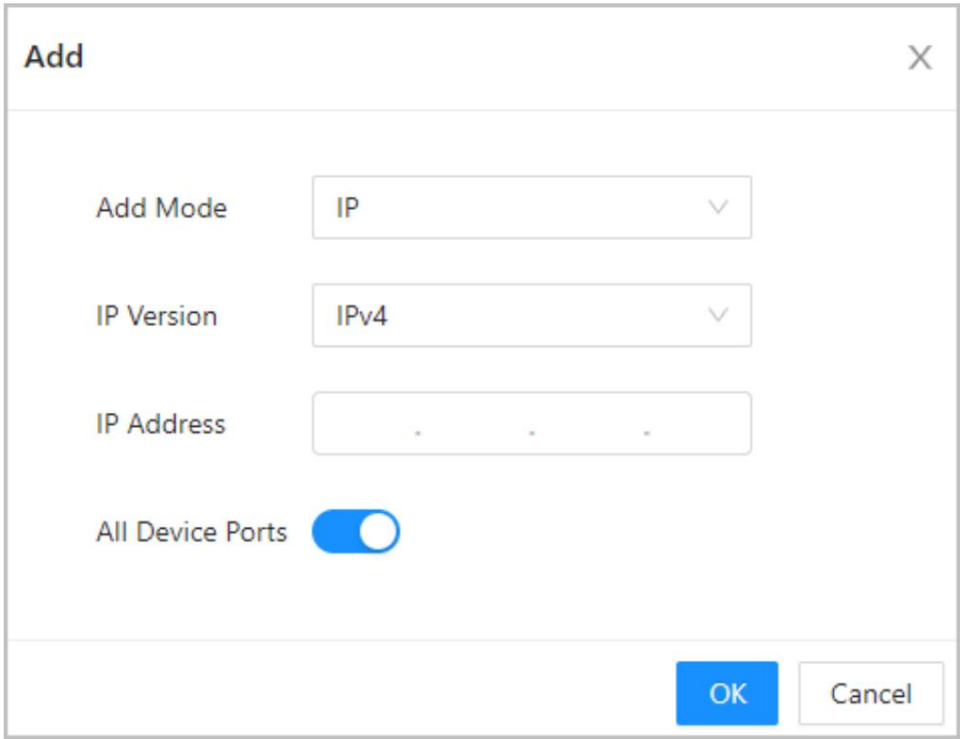


Шаг 3. Выберите режим: Список разрешенных и Список заблокированных.

- 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 2-40. Добавить информацию об IP-адресе.



Шаг 5. Нажмите OK.

Связанные операции

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

2.10.3.2 Настройка блокировки учетной записи

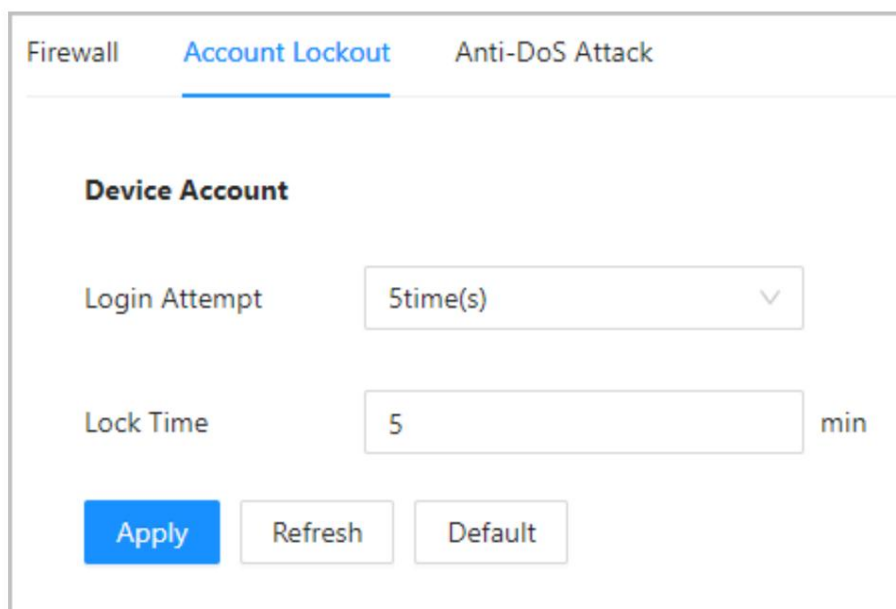
Если неверный пароль будет введен заданное количество раз, учетная запись будет заблокирована.

Процедура

Шаг 1. Выберите Безопасность > 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 2-41 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».

2.10.3.3 Настройка защиты от DoS-атак

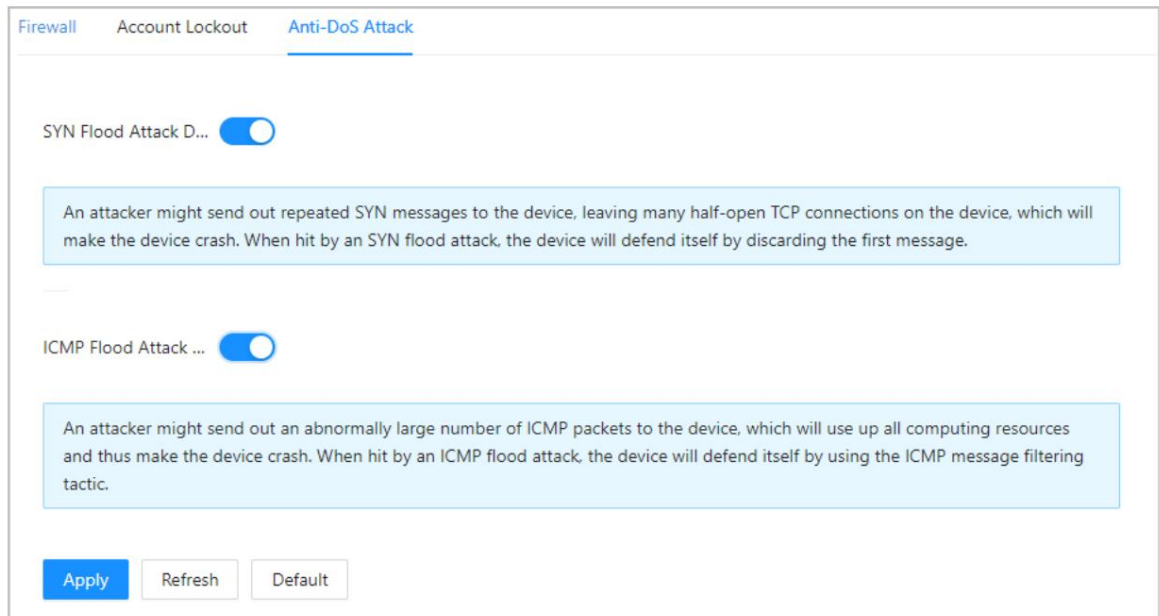
Для защиты устройства от DoS-атак можно включить защиту от SYN-флуд-атак и защиту от ICMP-флуд-атак .

Процедура

Шаг 1. Выберите Безопасность > 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 2-42. Защита от DoS-атаки.



Шаг 3. Нажмите «Применить».

2.10.4 Сертификат на устанавливаемое устройство

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

2.10.4.1 Создание сертификата

Создайте сертификат для устройства.

Процедура

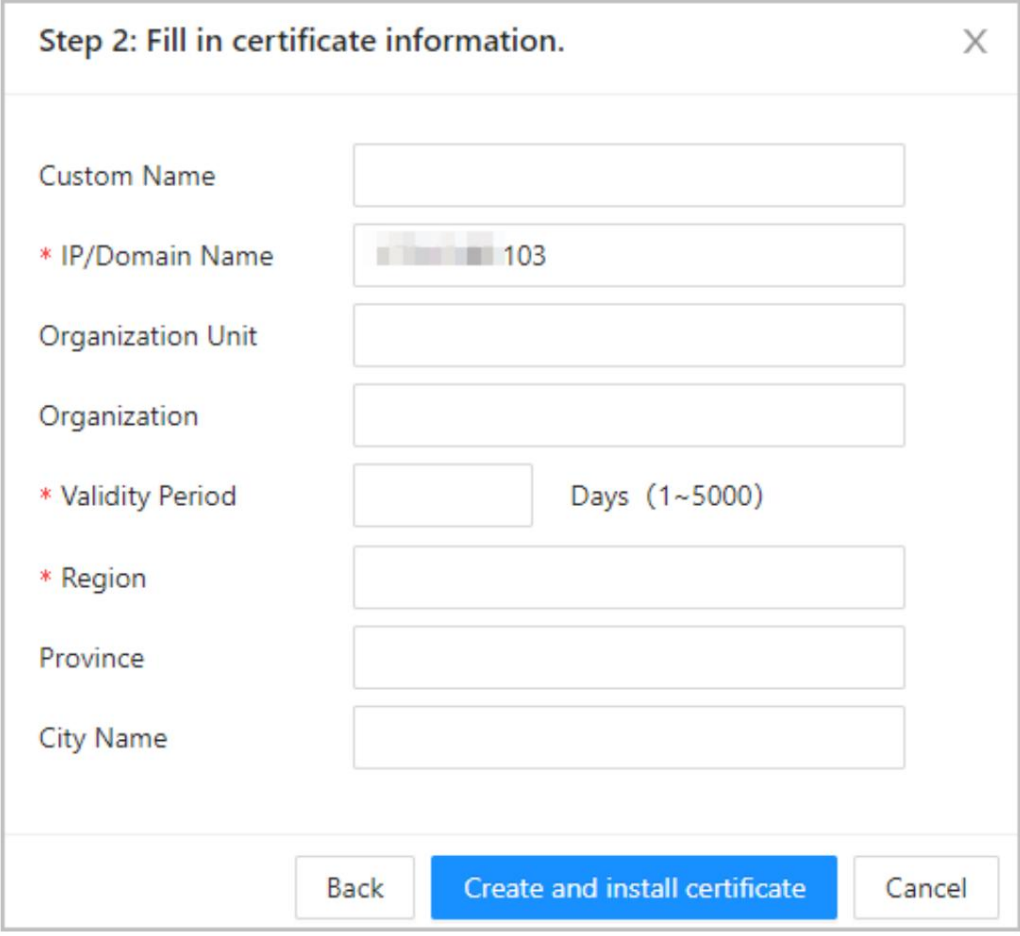
Шаг 1. Выберите Безопасность > Сертификат центра сертификации > Сертификат устройства.

Шаг 2. Выберите «Установить сертификат устройства».

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

Введите информацию о сертификате.

Рисунок 2-43. Информация о сертификате.



Step 2: Fill in certificate information.

Custom Name

* IP/Domain Name

Organization Unit

Organization

* Validity Period Days (1~5000)

* Region

Province

City Name

Back Create and install certificate Cancel



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.

2.10.4.2 Подача заявки на получение и импорт сертификата CA

Импортируйте сертификат стороннего центра сертификации на устройство.

Процедура

Шаг 1. Выберите Безопасность > 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 2-44 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.

2.10.4.3 Установка существующего сертификата

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

Процедура

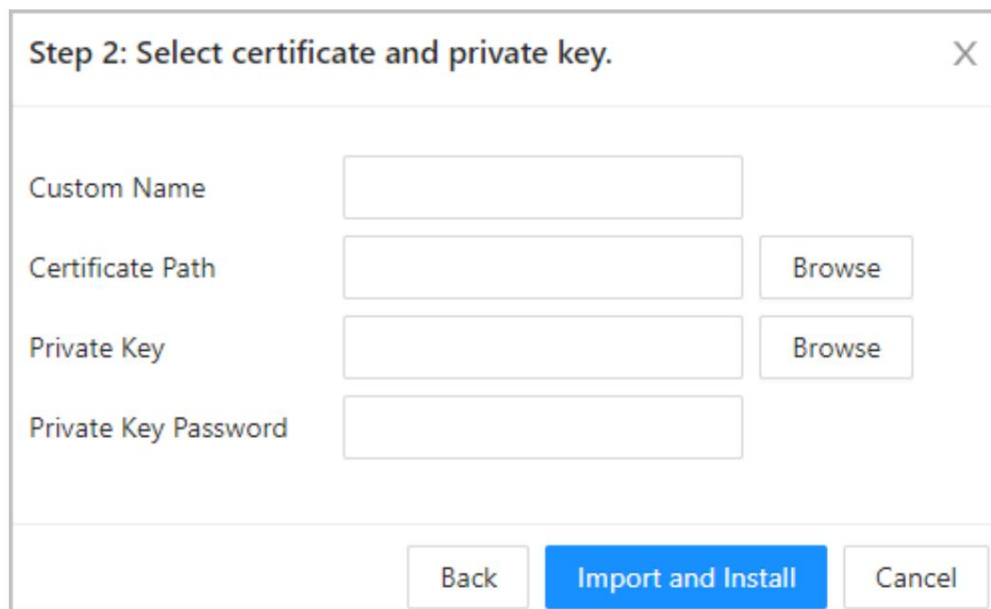
Шаг 1. Выберите Безопасность > Сертификат центра сертификации > Сертификат устройства.

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 2-45. Сертификат и закрытый ключ.



The image shows a Windows-style dialog box titled "Step 2: Select certificate and private key." with a close button (X) in the top right corner. Inside the dialog, there are four labeled input fields arranged vertically: "Custom Name", "Certificate Path", "Private Key", and "Private Key Password". To the right of the "Certificate Path" and "Private Key" fields are "Browse" buttons. At the bottom of the dialog, there are three buttons: "Back", "Import and Install" (which is highlighted in blue), and "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.

2.10.5 Установка доверенного сертификата центра сертификации

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

Справочная информация: 802.1X — это

протокол сетевой аутентификации, который открывает порты для доступа к сети, когда организация подтверждает личность пользователя и предоставляет ему доступ к сети.

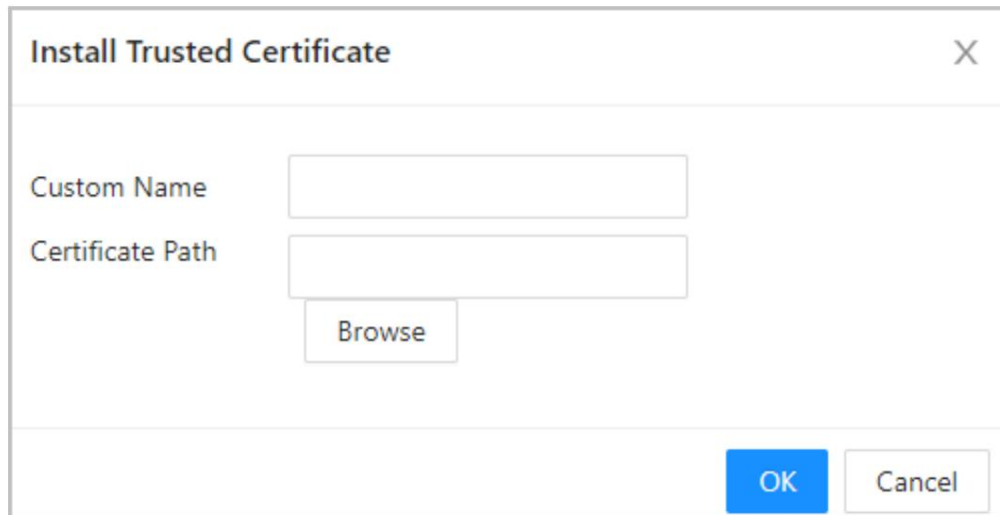
Процедура

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

Шаг 2. Выберите «Установить доверенный сертификат».

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

Рисунок 2-46. Установите доверенный сертификат.



Шаг 4. Нажмите OK.

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

Связанные операции

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

2.10.6 Предупреждение о безопасности

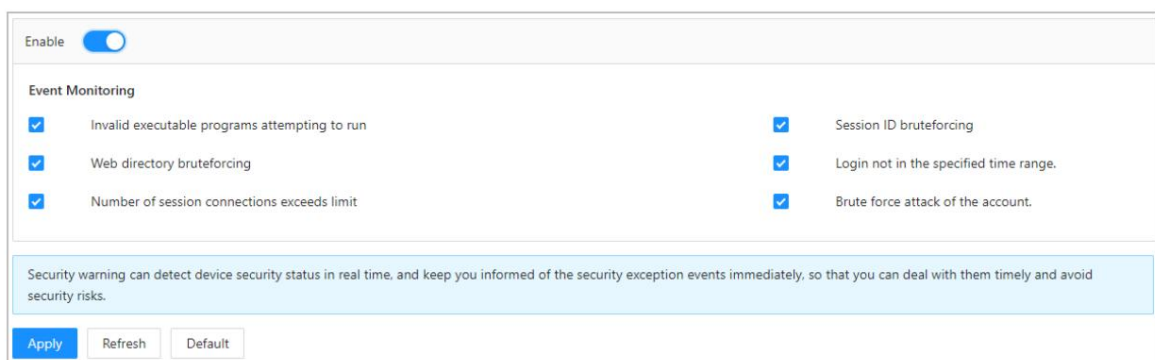
Процедура

Шаг 1. Выберите Безопасность > Предупреждение безопасности.

Шаг 2. Включите функцию предупреждения системы безопасности.

Шаг 3. Выберите элементы мониторинга.

Рисунок 2-47. Предупреждение о безопасности.



Шаг 4. Нажмите «Применить».

2.10.7 Аутентификация безопасности

Процедура

Шаг 1. Выберите Безопасность > Аутентификация безопасности.

Шаг 2. Выберите алгоритм хэширования сообщения.

Шаг 3. Нажмите «Применить».

Рисунок 2-48. Аутентификация безопасности.

2.11 Центр технического обслуживания

2.11.1 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.

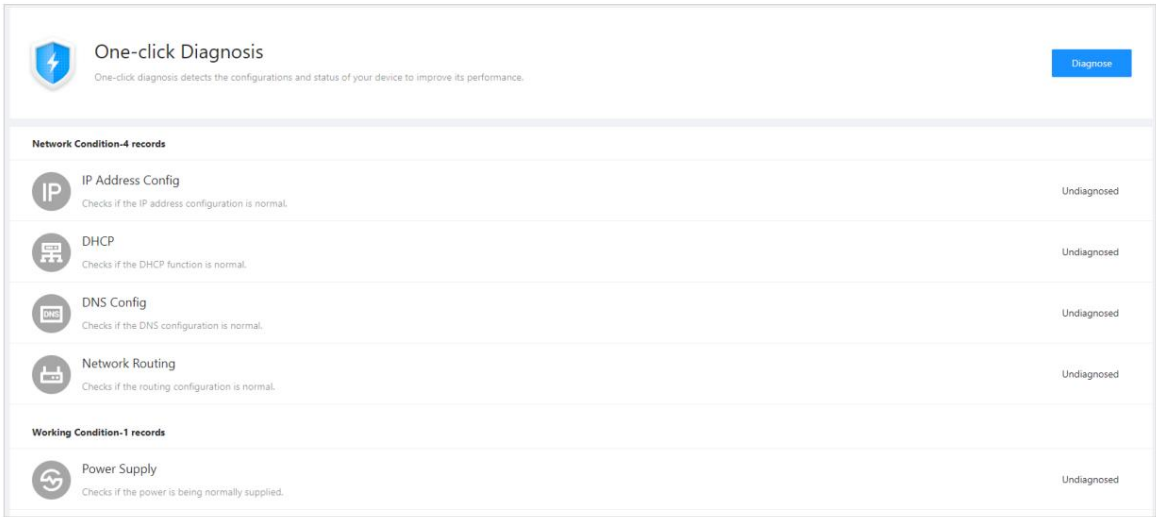
Шаг 2. Нажмите «Диагностика».

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 2-49. Диагностика одним щелчком мыши.



2.11.2 Информация о системе

2.11.2.1 Просмотр информации о версии

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

2.11.2.2 Просмотр юридической информации

На главной странице выберите «Система» > «Юридическая информация», и вы сможете ознакомиться с лицензионным соглашением на программное обеспечение, политикой конфиденциальности и уведомлением об открытом исходном коде.

2.11.3 Объем данных

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

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

2.11.4 Журналы просмотров

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

2.11.4.1 Системные журналы

Просмотр и поиск системных журналов.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите 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  подробности журнала.

2.11.4.2 Разблокировка записей

Найдите записи о разблокировке и экспортируйте их.

Процедура

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

Для загрузки журнала нажмите кнопку «Экспорт» .

2.11.4.3 Журналы аварийных сигналов

Просмотреть журналы тревожных сообщений.

Процедура

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

2.11.5 Управление техническим обслуживанием

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

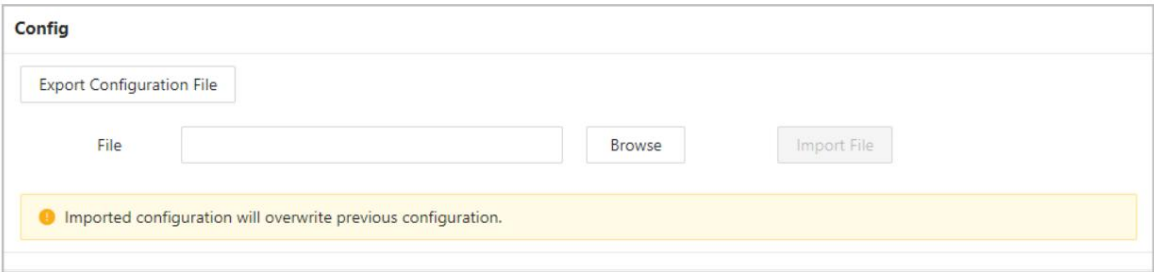
2.11.5.1 Экспорт и импорт конфигурационных файлов

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

Процедура

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

Рисунок 2-50 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.

2.11.5.2 Настройка считывателя карт

Процедура

Шаг 1. Войдите на веб-страницу.

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

Шаг 3. В разделе «Настройки считывателя карт» настройте параметры считывателя карт, а затем нажмите «Применить».

1. Выберите дверной канал, а затем включите или выключите функцию инверсии карты №.
2. Выберите устройство считывания, затем выберите протокол и скорость передачи данных.

Рисунок 2-51 Настройки считывателя карт

Card Reader Settings

Door Channel

1

Card No. Inver...

☐ Enable

☒ Close

Reader

Reader 1

Card Reader P...

☒ RS-485

☐ OSDP

Baud Rate

☒ 9600

☐ 115200

Apply

Refresh

Default

2.11.5.3 Настройка порога сходства отпечатков пальцев

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

Процедура

Шаг 1. Войдите на веб-страницу.

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

Шаг 3 В поле «Отпечаток пальца» введите пороговое значение сходства, а затем нажмите «Применить».



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

Рисунок 2-52. Порог сходства отпечатков пальцев.

2.11.5.4 Восстановление заводских настроек по умолчанию

Процедура

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



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

Шаг 2. При необходимости восстановите заводские настройки по умолчанию.

- Сброс к заводским настройкам : Сбрасывает все параметры устройства и удаляет все данные. • Восстановление настроек по умолчанию (кроме информации о пользователе и журналов) : Сбрасывает параметры устройства.

Устройство удаляет все данные, кроме информации о пользователе и журналов.

2.11.5.5 Техническое обслуживание

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

Процедура

Шаг 1. Войдите на веб-страницу.

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

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

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

2.11.6 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.

Обновление файла 2.11.6.1

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.

2.11.6.2 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.

2.11.7 Расширенное техническое обслуживание

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

2.11.7.1 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.

2.11.7.2 Захват пакетов

Захват пакетов

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

Рисунок 2-53. Захват пакетов.

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

- 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 2-54. 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.

Приложение 1. Важные моменты, касающиеся снятия отпечатков пальцев.

Инструкции по регистрации

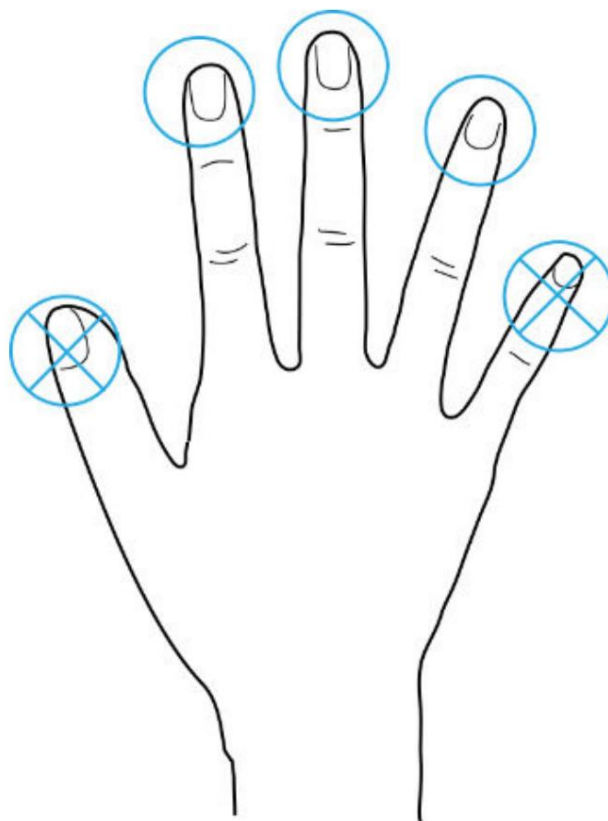
При регистрации отпечатков пальцев обратите внимание на следующие моменты:

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

Рекомендуется использовать пальцы.

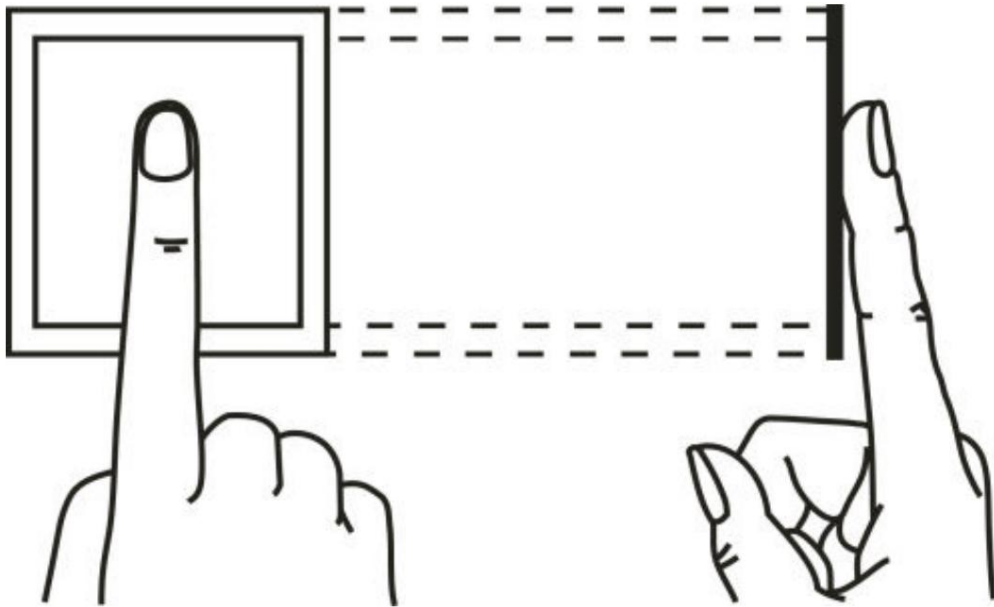
Рекомендуется использовать указательные, средние и безымянные пальцы. Большие пальцы и мизинцы будет сложно разместить в центре записи.

Приложение, Рисунок 1-1. Рекомендуемые пальцы.

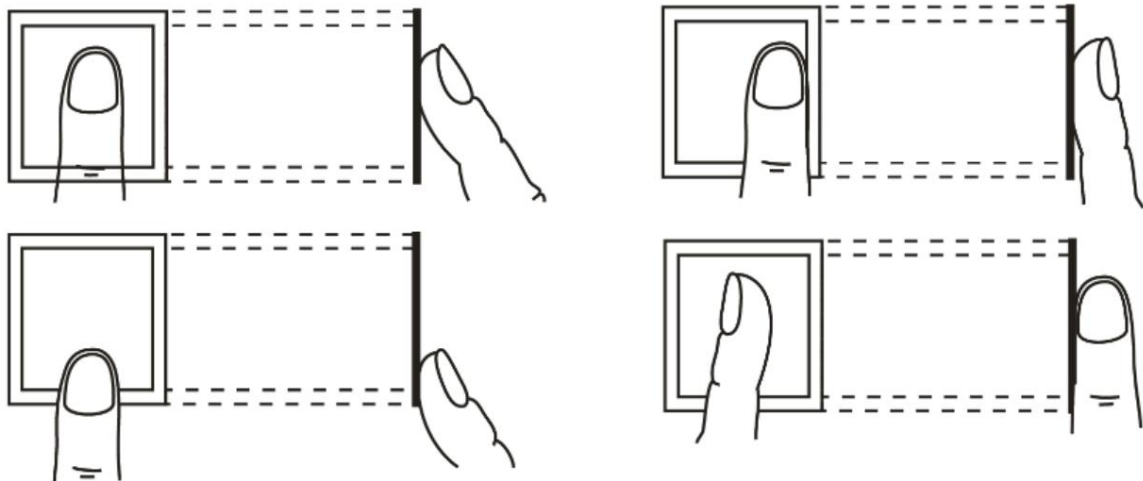


Как приложить отпечаток пальца к сканеру

Приложение, Рисунок 1-2. Правильное размещение.



Приложение, Рисунок 1-3. Неправильное размещение.



Приложение 2. Рекомендации по безопасности.

Управление учетными записями

1. Используйте сложные пароли.

Для установки паролей воспользуйтесь следующими рекомендациями:

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

2. Периодически меняйте пароли.

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

3. Распределите учетные записи и права доступа надлежащим образом.

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

4. Включите функцию блокировки учетной записи.

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

5. Своевременно устанавливайте и обновляйте информацию для сброса пароля.

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

Конфигурация службы

1. Включите HTTPS.

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

2. Зашифрованная передача аудио и видео.

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

3. Отключите некритичные службы и используйте безопасный режим.

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

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

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

4. Измените порты HTTP и других служб по умолчанию.

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

Сетевая конфигурация

1. Включите список разрешенных .

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

2. Привязка MAC-адреса

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

3. Создайте безопасную сетевую среду.

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

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

Аудит безопасности

1. Проверьте пользователей сети.

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

2. Проверьте журнал устройства.

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

3. Настройка сетевого журнала

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

Безопасность программного обеспечения

1. Своевременно обновляйте прошивку.

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

2. Своевременно обновляйте клиентское программное обеспечение.

Рекомендуется загрузить и использовать последнюю версию клиентского программного обеспечения.

Физическая защита

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

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