

Контроллер доступа

Руководство пользователя

Правовая информация

Информация о документе

- Документ содержит инструкции для использования и управления продуктом. Изображения, графики и вся другая информация предназначены только для ознакомления.
- Этот документ может быть изменен без уведомления, в связи с обновлением прошивки и по другим причинам. Актуальная версия настоящего документа представлена на веб-сайте компании. Если не оговорено иное, компания не предоставляет никаких гарантий, явных или подразумеваемых.
- Используйте этот документ под руководством профессионалов, обученных работе с продуктом.

О продукте

Послепродажное обслуживание данного продукта возможно только в той стране или регионе, где была совершена покупка.

Торговая марка

Торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

ПРАВОВАЯ ИНФОРМАЦИЯ

- ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ДАННОЕ РУКОВОДСТВО, ПРОДУКТ, АППАРАТУРА, ПРОГРАММНОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», СО ВСЕМИ ОШИБКАМИ И НЕТОЧНОСТЯМИ. НАША КОМПАНИЯ НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, КАСАТЕЛЬНО УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ. ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА НЕСЕТ ПОЛЬЗОВАТЕЛЬ. НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД ПОТРЕБИТЕЛЕМ ЗА КАКОЙ-ЛИБО СЛУЧАЙНЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ, ВКЛЮЧАЯ УБЫТКИ ИЗ-ЗА ПОТЕРИ ПРИБЫЛИ, ПЕРЕРЫВА В ДЕЯТЕЛЬНОСТИ ИЛИ ПОТЕРИ ДАННЫХ ИЛИ ДОКУМЕНТАЦИИ, ПО ПРИЧИНЕ НАРУШЕНИЯ УСЛОВИЙ КОНТРАКТА, ТРЕБОВАНИЙ (ВКЛЮЧАЯ ХАЛАТНОСТЬ), УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ ИНОГО, В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ НАШЕЙ КОМПАНИИ БЫЛО ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.
- ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ; НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, НАША КОМПАНИЯ ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.

- ВЫ СОГЛАШАЕТЕСЬ ИСПОЛЬЗОВАТЬ ДАННЫЙ ПРОДУКТ В СООТВЕТСТВИИ СО ВСЕМИ ПРИМЕНИМЫМИ ЗАКОНАМИ, И ВЫ НЕСЕТЕ ЕДИНОЛИЧНУЮ ОТВЕТСТВЕННОСТЬ ЗА ОБЕСПЕЧЕНИЕ ТОГО, ЧТОБЫ ВАШЕ ИСПОЛЬЗОВАНИЕ СООТВЕТСТВОВАЛО ПРИМЕНИМЫМ ЗАКОНАМ. В ЧАСТНОСТИ, ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ДАННОГО ПРОДУКТА ТАКИМ ОБРАЗОМ, КОТОРЫЙ НЕ НАРУШАЕТ ПРАВА ТРЕТЬИХ ЛИЦ, ВКЛЮЧАЯ, БЕЗ ОГРАНИЧЕНИЙ, ПРАВА НА ПУБЛИЧНОСТЬ, ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ ИЛИ ПРАВА НА ЗАЩИТУ ДАННЫХ И ДРУГИЕ ПРАВА НА КОНФИДЕНЦИАЛЬНОСТЬ. ВЫ ОБЯЗУЕТЕСЬ НЕ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В ЗАПРЕЩЕННЫХ ЦЕЛЯХ, ВКЛЮЧАЯ РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ, РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ХИМИЧЕСКОГО ИЛИ БИОЛОГИЧЕСКОГО ОРУЖИЯ, ЛЮБУЮ ДЕЯТЕЛЬНОСТЬ, СВЯЗАННУЮ С ЯДЕРНЫМИ ВЗРЫВЧАТЫМИ ВЕЩЕСТВАМИ, НЕБЕЗОПАСНЫМ ЯДЕРНЫМ ТОПЛИВНЫМ ЦИКЛОМ ИЛИ НАРУШАЮЩУЮ ПРАВА ЧЕЛОВЕКА.
- В СЛУЧАЕ КАКИХ-ЛИБО КОНФЛИКТОВ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.

Защита данных

- При разработке устройств соблюдаются принципы конфиденциальности в целях защиты данных. Например, устройства с функциями распознавания лиц разработаны таким образом, что сохраняемые биометрические данные защищены шифрованием; в устройствах с функцией идентификации по отпечатку пальца будут сохранены только шаблоны отпечатка пальца и, таким образом, изображение отпечатка пальца не подлежит реконструкции.
- Поскольку данные находятся под вашим контролем, сбор, хранение, обработку и передачу данных необходимо выполнять в соответствии с применимыми законами и требованиями по защите данных. Также необходимо выполнять действия по безопасности для защиты личных данных, такие как разумный административный и физический контроль безопасности, периодические обзоры и оценки эффективности мер безопасности.

Доступные модели

Наименование	Описание
Контроллер доступа	Контроллер доступа на 1 дверь
	Контроллер доступа на 2 двери
	Контроллер доступа на 4 двери
	Контроллер доступа для 8 дверей
Модуль доступа	Модуль доступа

Регулирующая информация

Информация о FCC

Обратите внимание, что изменения или модификации, не одобренные явно стороной, ответственной за соответствие, могут привести к аннулированию полномочий пользователя по работе с данным оборудованием.
Соответствие FCC. Это оборудование прошло испытания и соответствует регламенту для цифрового устройства класса B, применительно к части 15 Правил FCC. Данный регламент разработан для того, чтобы обеспечить достаточную защиту от вредных помех, возникающих при использовании оборудования в коммерческой среде. Это оборудование генерирует, использует и может излучать радиоволны на разных частотах и, если устройство установлено и используется не в соответствии с инструкцией, оно может создавать помехи для радиосигналов. Тем не менее, нет никакой гарантии, что помехи не возникнут в каких-либо конкретных случаях установки. Если оборудование создает вредные помехи для приема радио- или телевизионных сигналов, что может быть определено путем включения и выключения оборудования, пользователю рекомендуется попытаться устранить помехи одним или несколькими способами, а именно:
— изменить ориентацию или местоположение приемной антенны;
— увеличить расстояние между оборудованием и приемником;
— подключить оборудование к розетке в цепи, отличной от той, к которой подключен приемник;
— обратиться к дилеру или опытному радио / телемастеру.
Данное оборудование следует устанавливать и использовать на расстоянии не менее 20 см между источником излучения и пользователем.
Условия FCC
Это устройство соответствует регламенту для цифрового устройства применительно к части 15 Правил FCC. Эксплуатация допускается при соблюдении следующих двух условий.
1. Данное устройство не должно создавать вредных помех.
2. Данное устройство должно выдерживать возможные помехи, включая те, которые могут привести к выполнению нежелательных операций.

Соответствие стандартам ЕС

CE

Данный продукт и — если применимо — также и поставляемые принадлежности отмечены знаком «CE» и, следовательно, согласованы с европейскими стандартами, перечисленными под директивами 2014/30/EC EMC, 2014/53/EC и 2011/65/EC RoHS.



2012/19/EC (директива WEEE). Продукты, отмеченные данным знаком, запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Для надлежащей переработки верните этот продукт своему местному поставщику при покупке эквивалентного нового оборудования или утилизируйте его в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info



2006/66/EC (директива о батареях). Данный продукт оснащен батареей, которую запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Подробная информация о батарее изложена в документации продукта. Батарея отмечена значком, который может включать наименования, обозначающие содержание кадмия (Cd), свинца (Pb) или ртути (Hg). Для надлежащей утилизации возвратите батарею своему поставщику либо избавьтесь от нее в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info

Инструкция по технике безопасности

Эта инструкция предназначена для того, чтобы пользователь мог использовать продукт правильно и избежать опасности или причинения вреда имуществу.
Меры предосторожности разделены на «Предупреждения» и «Предостережения».
Предупреждение: игнорирование любого из предупреждений может привести к серьезным травмам или смерти.
Предостережение: игнорирование любого из предостережений может привести к травмам или порче оборудования.

⚠	⚠
Предупреждение: следуйте данным правилам для предотвращения серьезных травм и смертельных случаев.	**Предостережение:** следуйте мерам предосторожности, чтобы предотвратить возможные повреждения или материальный ущерб.

⚠Предупреждения:

- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в регионе эксплуатации.
- Используйте адаптер питания соответствующей компании. Потребляемая мощность не может быть меньше требуемого значения.
- Не подключайте несколько устройств к одному блоку питания, перегрузка адаптера может привести к перегреву или возгоранию.
- Прежде чем подключать, устанавливать или разбирать устройство, убедитесь, что питание отключено.
- Если устройство устанавливается на потолок или стену, убедитесь, что оно надежно закреплено.
- Если из устройства идет дым или доносится шум — отключите питание, извлеките кабель и свяжитесь с сервисным центром.
- Избегайте проглатывания батареи, существует опасность химического ожога.
  Данное устройство оснащено батареей таблеточного типа. Проглатывание батареи таблеточного типа может вызвать серьезные внутренние ожоги всего за 2 часа и привести к смерти.
  Храните новые и использованные батареи в недоступном для детей месте. Если отсек для батареи закрывается ненадежно, прекратите использование продукта и храните его в недоступном для детей месте. В случае проглатывания батареи или ее перемещения в какую-либо часть тела, немедленно обратитесь за медицинской помощью.

- Если продукт не работает должным образом, необходимо обратиться к дилеру или в ближайший сервисный центр. Не пытайтесь самостоятельно разобрать устройство. (Компания не несет ответственность за проблемы, вызванные несанкционированным ремонтом или техническим обслуживанием.)

⚠ Предостережения

- Запрещено ронять устройство и подвергать воздействию сильных электромагнитных помех. Избегайте установки устройства на вибрирующую поверхность или в местах, подверженных ударам (пренебрежение этим предостережением может привести к повреждению устройства).
- Запрещено размещать устройство в местах с чрезвычайно высокой или низкой температурой окружающей среды (подробная информация о рабочей температуре представлена в спецификации устройства), в пыльной или влажной среде, запрещено подвергать устройство воздействию сильных электромагнитных помех.
- Не подвергайте крышку устройства, предназначенного для использования внутри помещения, воздействию дождя или влаги.
- Не подвергайте устройство воздействию прямых солнечных лучей, не устанавливайте в местах с плохой вентиляцией или рядом с источником тепла таким, как обогреватель или радиатор (пренебрежение этим предостережением может привести к пожару).
- Запрещено направлять устройство на солнце или очень яркие источники света. Яркий свет может вызвать размытие или потерю четкости изображения (что не является признаком неисправности), а также повлиять на срок службы матрицы.
- Используйте прилагаемую перчатку во время демонтажа крышки устройства, избегайте прямого контакта с крышкой устройства, так как пот и жир с пальцев могут стать причиной разрушения защитного покрытия на поверхности устройства.
- Для очистки внутренних и внешних поверхностей крышки устройства используйте мягкую и сухую ткань, не используйте щелочные моющие средства.
- Сохраните упаковку после распаковки для использования в будущем. В случае сбоя работы устройство необходимо вернуть на завод (с оригинальной упаковкой). Транспортировка без оригинальной упаковки может привести к повреждению устройства и к дополнительным расходам.
- Неправильное использование или замена батареи может привести к опасности взрыва. Проводите замену на такие же батареи или аналогичные. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем батарей.

Содержание

Раздел 1 Внешний вид 1

1.1 Внешний вид и интерфейсы контроллера доступа для 1 двери / 2 дверей / 4 дверей / 8 дверей 1

1.2 Внешний вид модуля доступа 6

1.3 Описание индикаторов 6

Раздел 2 Подключение 8

2.1 Описание подключения 8

2.2 Подключение считывателя карт Wiegand 10

2.3 Подключение считывателя карт RS-485 11

2.4 Подключение дверного замка 11

2.5 Подключение тревожных интерфейсов 12

2.6 Подключение кнопки выхода 12

2.7 Подключение дверного контакта 13

2.8 Подключение модуля обнаружения возгораний 13

Раздел 3 Установка 14

3.1 Установка контроллера лифта 14

3.2 Установка контроллера лифта (с шасси) 16

Глава 4 Настройки 17

Раздел 5 Активация устройства 18

5.1 Активация через веб-интерфейс 18

5.2 Активация через ПО SADP 19

Раздел 6 Сценарии применения 21

Раздел 7 Быстрые операции через веб-интерфейс 22

7.1 Настройка контрольного вопроса 22

7.2 Выбор языка 22

7.3 Настройка времени 22

Глава 8 Работа через веб-интерфейс 24

8.1 Вход в систему 24

8.2 Забыть пароль 24

8.3 Описание модулей 25
8.4 Управление контролем доступа 25
8.4.1 Обзор 25
8.4.2 Поиск событий 26
8.4.3 Управление точкой доступа 26
8.4.4 Управление разрешениями 31
8.4.5 Приложения контроля доступа 35
8.5 Управление пользователями 43
8.5.1 Добавление организации 43
8.5.2 Добавление пользователя 43
8.6 Управление устройством 47
8.6.1 Поиск недобавленных устройств 47
8.6.2 Добавление модуля доступа 48
8.6.3 Добавление модуля ввода-вывода 51
8.6.4 Управление областью 52
8.7 Система и обслуживание 52
8.7.1 Отображение информации об устройстве 52
8.7.2 Настройка времени 53
8.7.3 Настройка параметров перехода на летнее время 53
8.7.4 Изменение пароля администратора 53
8.7.5 Настройки безопасности учетной записи 54
8.7.6 Просмотр пользователей в сети 54
8.7.7 Просмотр лицензии на ПО с открытым исходным кодом в веб-интерфейсе ПК 55
8.7.8 Просмотр информации о постановке на охрану / снятии с охраны 55
8.7.9 Настройка сетевых параметров 55
8.7.10 Настройки событий 60
8.7.11 Конфигурация доступа 63
8.7.12 Настройки параметров карты 66
8.7.13 ТО и безопасность 67
8.7.14 Управление сертификатами 72
8.7.15 Разблокировка 73

Раздел 9 Настройка устройства через мобильный веб-интерфейс 74
9.1 Вход в систему 74
9.2 Обзор 74
9.3 Забыли пароль 75
9.4 Конфигурация 75
9.4.1 Отображение информации об устройстве 75
9.4.2 Настройки времени 76
9.4.3 Настройка параметров DST 76
9.4.4 Управление пользователями 77
9.4.5 Настройка сетевых параметров 77
9.4.6 Настройки параметров тревоги 82
9.4.7 Конфигурация доступа 83
9.4.8 Управление организацией и пользователями 84
9.4.9 Управление устройством 86
9.4.10 Настройка параметров контроля доступа 89
9.4.11 Поиск событий 94
9.4.12 Обновление и техническое обслуживание 94
9.4.13 Просмотр руководства пользователя 96
9.4.14 Просмотр лицензии на ПО с открытым исходным кодом 96
A. Размеры 97

Раздел 1 Внешний вид

1.1 Внешний вид и интерфейсы контроллера доступа для 1 двери / 2 дверей / 4 дверей / 8 дверей

Описание внешнего вида и интерфейсов контроллера доступа для 1 двери / 2 дверей / 4 дверей / 8 дверей.

Внешний вид и интерфейсы контроллера доступа для 1 двери

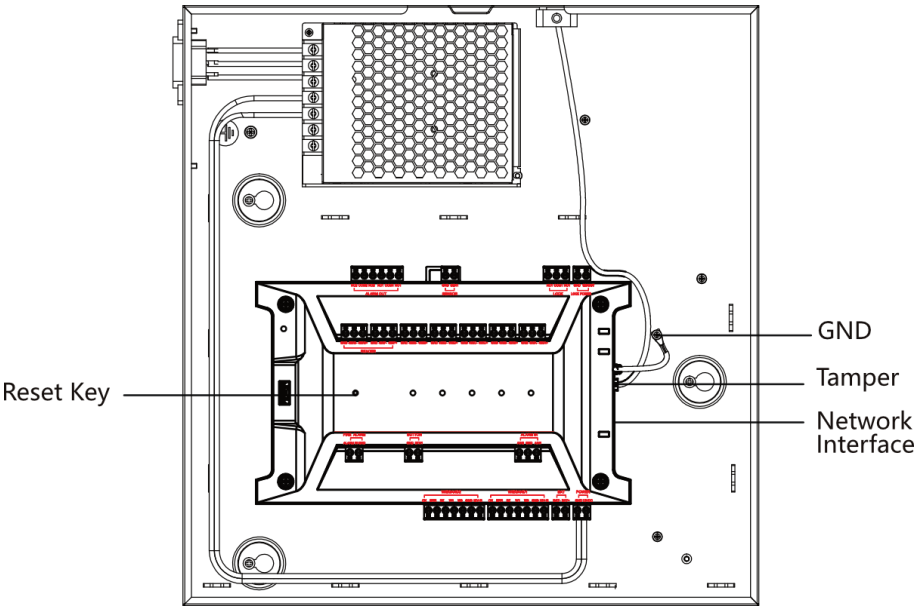


Рисунок 1-1 Внешний вид и интерфейсы контроллера доступа для 1 двери

Английский язык	Русский язык
Reset key	Кнопка сброса
GND	Заземление
Tamper	Тампер
Network interface	Сетевой интерфейс

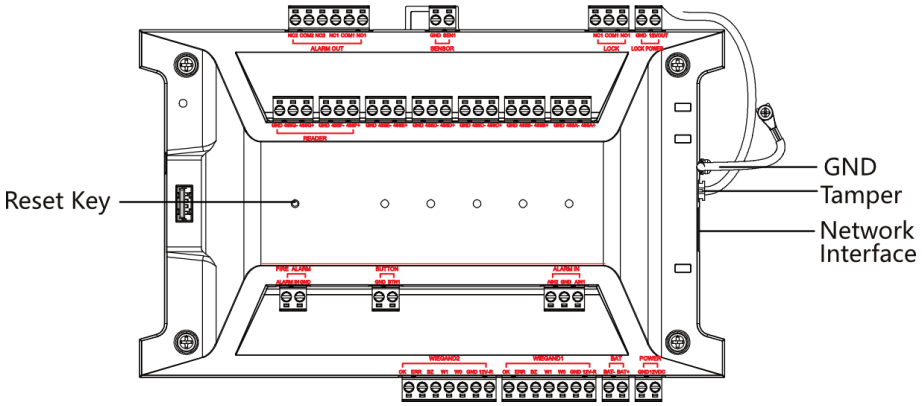


Рисунок 1-2 Внешний вид и интерфейсы основной платы контроллера доступа для 1 двери

Английский язык	**Русский язык**
Reset key	Кнопка сброса
GND	Заземление
Tamper	Тампер
Network interface	Сетевой интерфейс

Внешний вид и интерфейсы контроллера доступа для 2 дверей

Примечание

- Только некоторые модели поддерживают функции Wi-Fi и PoE.
- При использовании устройств с PoE необходимо учитывать следующее:
  1. Мощность коммутатора составляет 30 Вт.
  2. Функции PoE и Wi-Fi не могут использоваться одновременно.
  3. Если общая мощность входящих замков превышает 10 Вт, для одного из замков требуется дополнительный отдельный источник питания.
  4. Поддержка доступа до 4 считывателей карт.

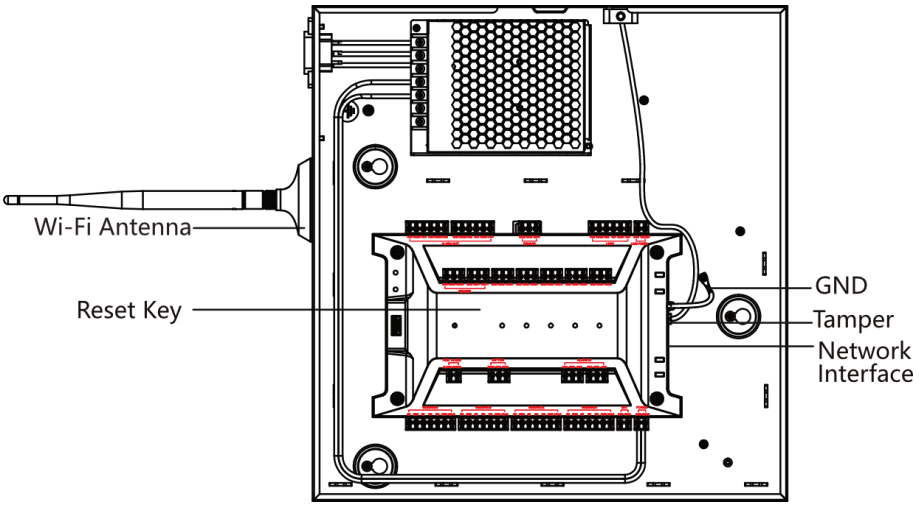


Рисунок 1-3 Внешний вид и интерфейсы контроллера доступа для 2 дверей

Английский язык	**Русский язык**
Reset key	Кнопка сброса
GND	Заземление
Tamper	Тампер
Network interface	Сетевой интерфейс
Wi-Fi antenna	Антенна Wi-Fi

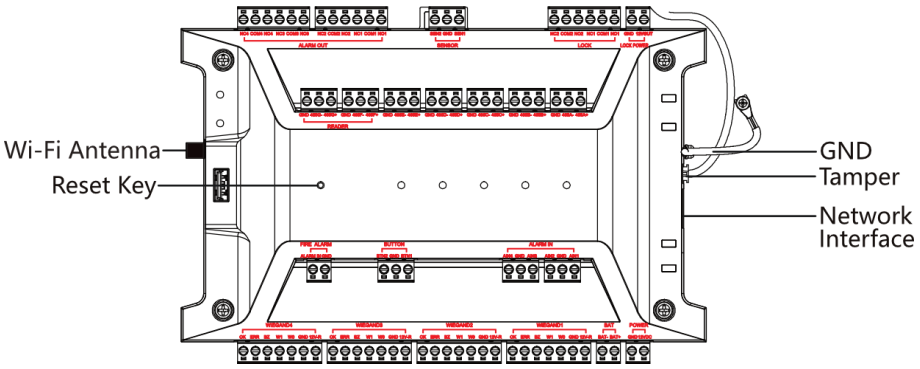


Рисунок 1-4 Внешний вид и интерфейсы основной платы контроллера доступа для 2 дверей

Английский язык	**Русский язык**
Reset key	Кнопка сброса
GND	Заземление
Tamper	Тампер
Network interface	Сетевой интерфейс
Wi-Fi antenna	Антенна Wi-Fi

Внешний вид и интерфейсы контроллера доступа для 4 дверей

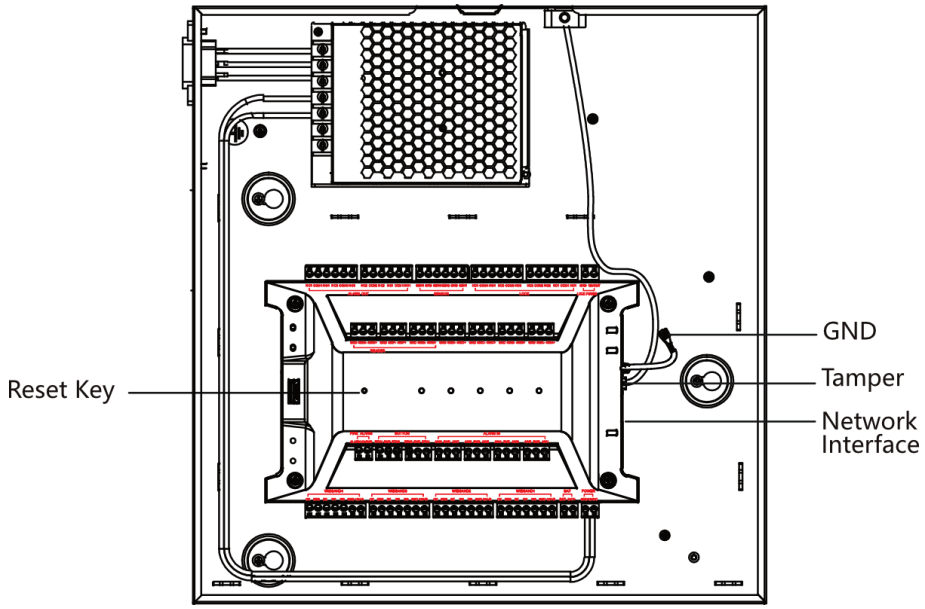


Рисунок 1-5 Внешний вид и интерфейсы контроллера доступа для 4 дверей

Английский язык	**Русский язык**
Reset key	Кнопка сброса
GND	Заземление
Tamper	Тампер
Network interface	Сетевой интерфейс

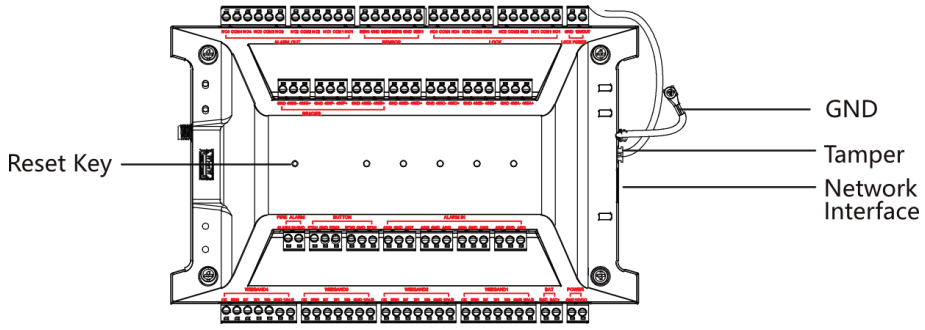


Рисунок 1-6 Внешний вид и интерфейсы основной платы контроллера доступа для 4 дверей

Английский язык	**Русский язык**
Reset key	Кнопка сброса
GND	Заземление
Tamper	Тампер
Network interface	Сетевой интерфейс

Внешний вид и интерфейсы контроллера доступа для 8 дверей

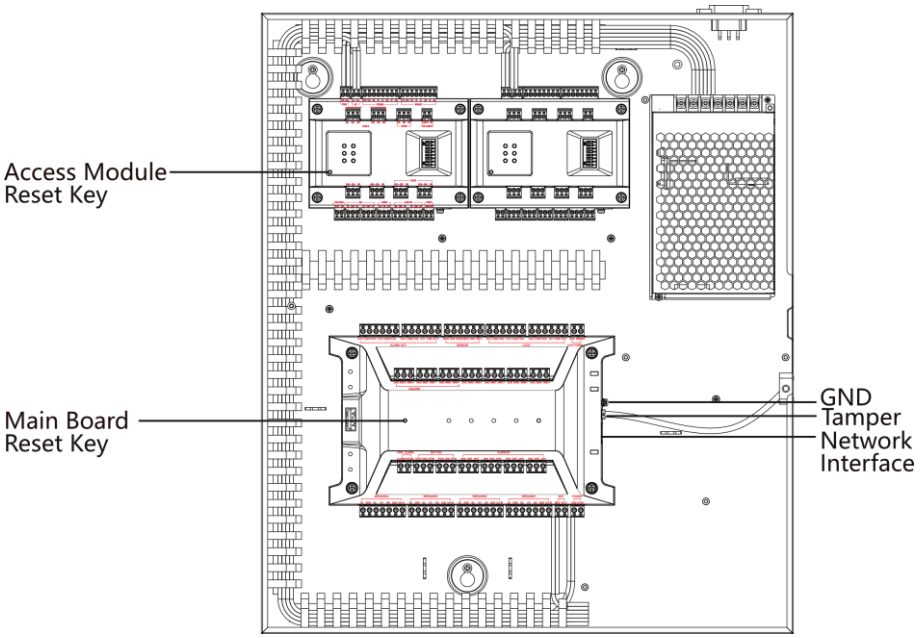


Рисунок 1-7 Внешний вид и интерфейсы основной платы контроллера доступа для 8 дверей

Английский язык	**Русский язык**
Access module reset key	Кнопка сброса модуля доступа
Main board reset key	Кнопка сброса основной панели
GND	Заземление
Tamper	Тампер
Network interface	Сетевой интерфейс

1.2 Внешний вид модуля доступа

Ниже представлено изображение модуля доступа.

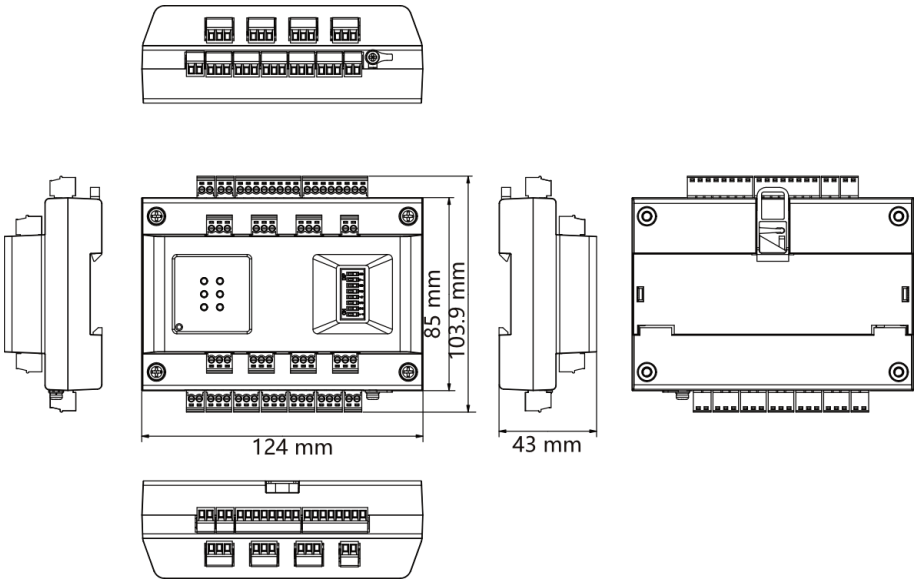


Рисунок 1-8 Внешний вид модуля доступа

1.3 Описание индикаторов

Ниже приведено описание индикаторов контроллера доступа для 1 / 2 / 4 / 8 дверей и модуля доступа.

Контроллер доступа для 1 двери

Всего 9 индикаторов: индикатор питания, индикатор рабочего состояния, индикатор сети, индикатор состояния двери и 5 индикаторов состояния RS-485.

Контроллер доступа для 2 дверей

Всего 11 индикаторов: индикатор питания, индикатор рабочего состояния, индикатор сети, индикатор Wi-Fi, 5 индикаторов состояния RS-485 и 2 индикатора состояния дверей.

Примечание. Некоторые модели не поддерживают индикаторы Wi-Fi.

Контроллер доступа для 4 дверей

Всего 12 индикаторов: индикатор питания, индикатор рабочего состояния, индикатор сети, 5 индикаторов состояния RS-485 и 4 индикатора состояния дверей.

Контроллер доступа для 8 дверей

Всего 12 индикаторов: индикатор питания, индикатор рабочего состояния, индикатор сети, 5 индикаторов состояния RS-485 и 4 индикатора состояния двери.

Модуль доступа

Всего 6 индикаторов: индикатор питания, индикатор рабочего состояния, 2 индикатора состояния связи и 2 индикатора состояния двери.

Примечание

Когда индикатор рабочего состояния горит красным, это означает, что устройство включено; когда индикатор рабочего состояния мигает зеленым, это означает, что устройство добавлено на платформу. Когда индикатор состояния двери горит, это означает, что дверь открыта, а когда индикатор выключен, это означает, что дверь закрыта. Если другие индикаторы состояния горят, значит устройство подключено; если индикаторы выключены, значит устройство не подключено.

Примечание

Раздел 2 Подключение

Описание подключения контроллера доступа.

2.1 Описание подключения

Ниже приведено описание подключения контроллера доступа для 1 / 2 / 4 / 8 дверей.

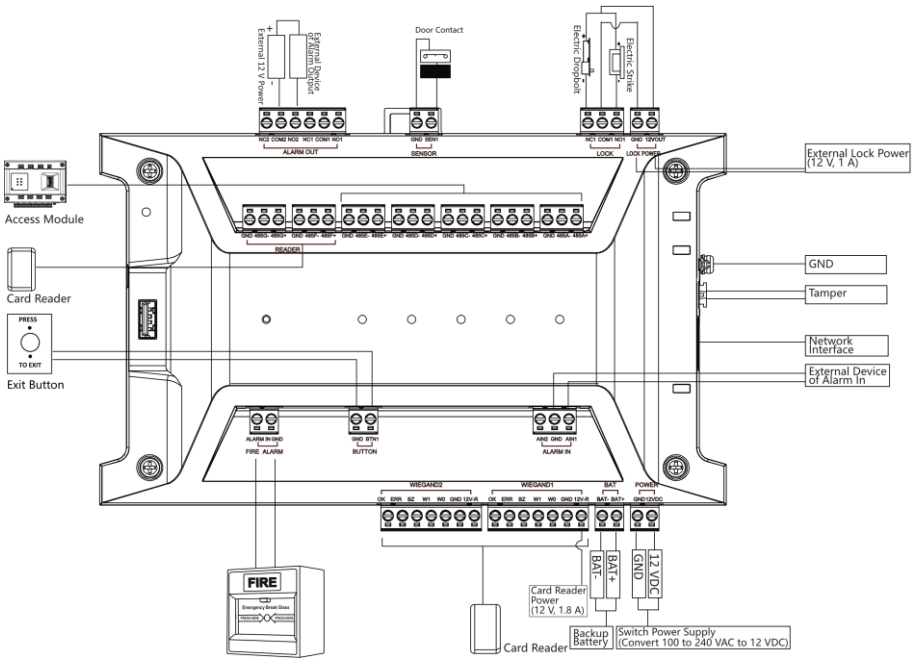


Рисунок 2-1 Подключение контроллера доступа для 1 двери

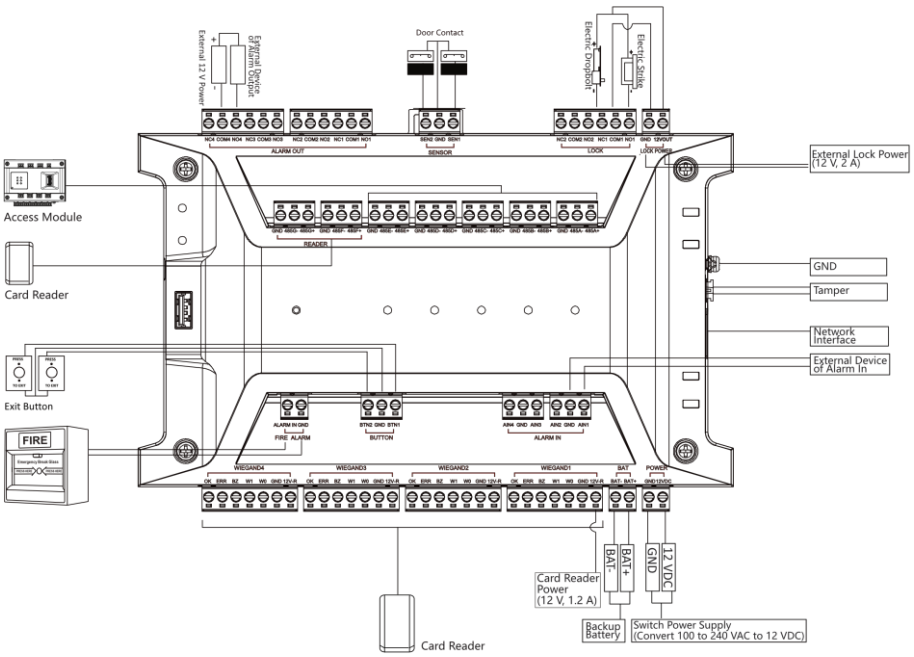


Рисунок 2-2 Подключение контроллера доступа для 2 дверей

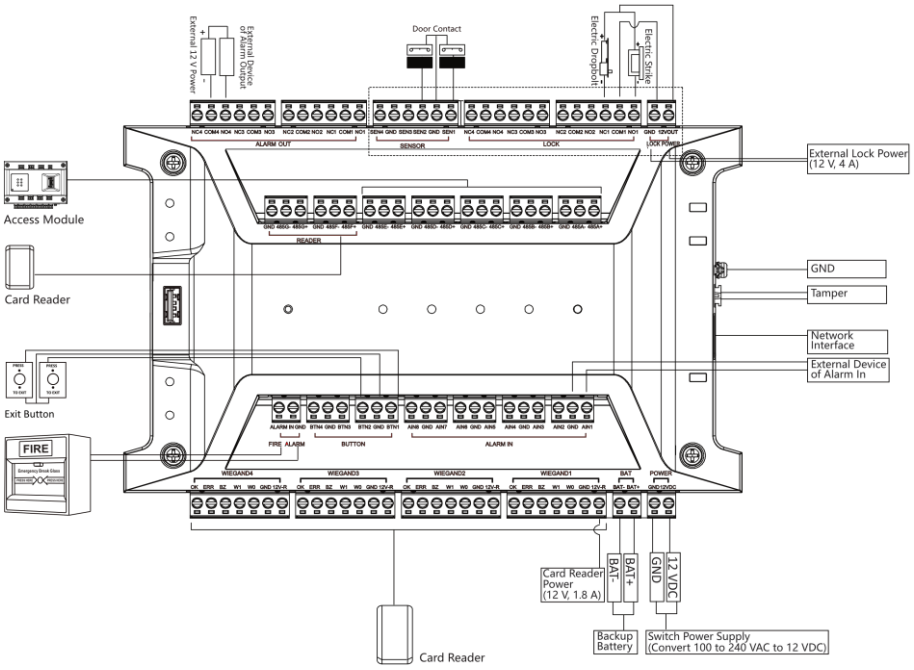


Рисунок 2-3 Подключение контроллера доступа для 4 дверей

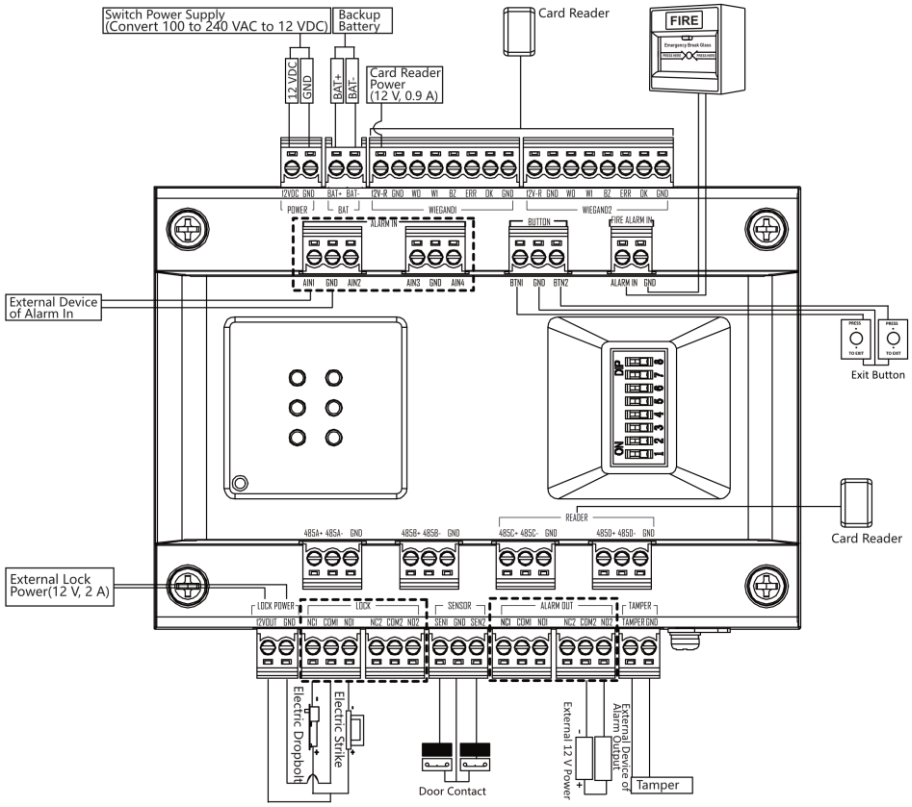


Рисунок 2-4 Подключение модуля доступа

2.2 Подключение считывателя карт Wiegand

Далее представлена схема подключения считывателя карт Wiegand.

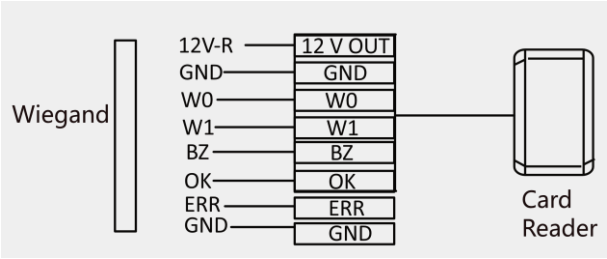


Рисунок 2-5 Схема подключения считывателя карт Wiegand

Примечание

При использовании контроллера доступа для управления светодиодом и бипером считывателя карт Wiegand необходимо подключить разъемы OK / ERR / BZ.

2.3 Подключение считывателя карт RS-485

Далее представлена схема подключения считывателя карт RS-485.

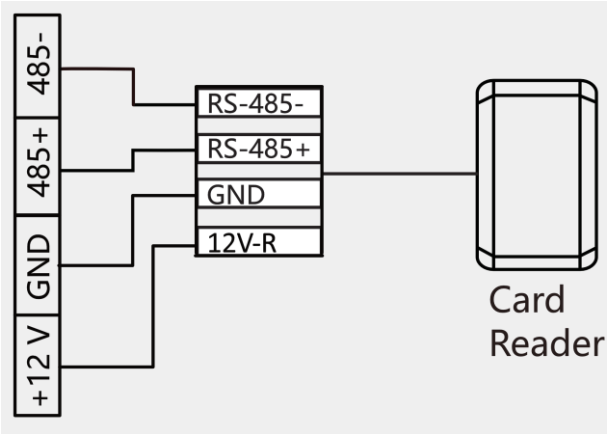


Рисунок 2-6 Схема подключения считывателя карт RS-485

Примечание

- Если считыватель карт установлен слишком далеко от контроллера доступа, можно использовать внешний источник питания.
- Рекомендуется использовать гирляндное подключение при установке считывателя карт RS-485.

2.4 Подключение дверного замка

Ниже представлена схема подключения дверного замка.

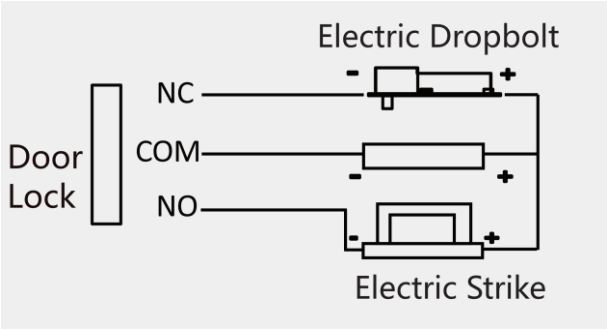


Рисунок 2-7 Схема подключения дверного замка

2.5 Подключение тревожных интерфейсов

Ниже представлена схема подключения тревожных интерфейсов.

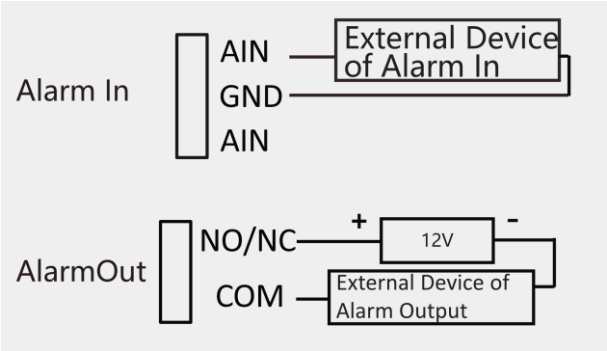


Рисунок 2-8 Подключение тревожных интерфейсов

2.6 Подключение кнопки выхода

Далее представлена схема подключения кнопки выхода.

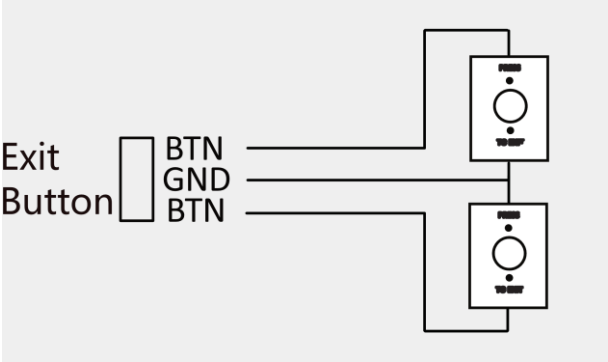


Рисунок 2-9 Подключение кнопки выхода

2.7 Подключение дверного контакта

Далее представлена схема подключения дверного контакта.

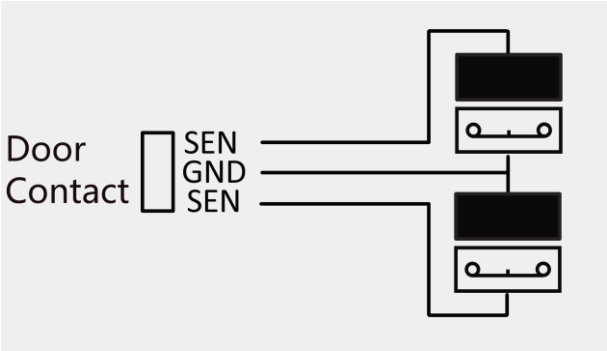


Рисунок 2-10 Подключение дверного контакта

2.8 Подключение модуля обнаружения возгораний

Далее представлена схема подключения модуля обнаружения возгораний.

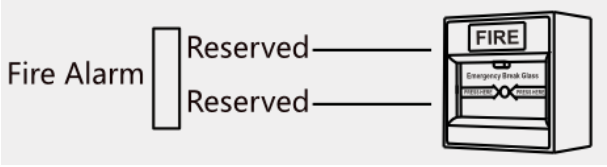


Рисунок 2-11 Подключение модуля обнаружения возгораний

Раздел 3 Установка

3.1 Установка контроллера лифта

Шаги

Примечание

Стена или другое место монтажа должно выдерживать массу втрое больше массы устройства.

1. На стене или в других местах установки оборудования просверлите отверстия, расположение которых будет совпадать с отверстиями на направляющей рейке.

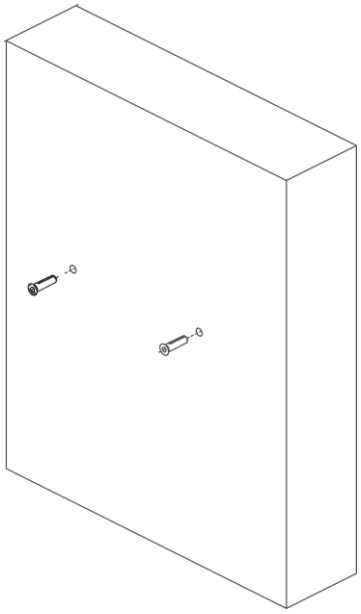


Рисунок 3-1 Отверстия для установки

2. Вставьте в просверленные отверстия дюбели для установочных винтов (входят в комплект поставки).

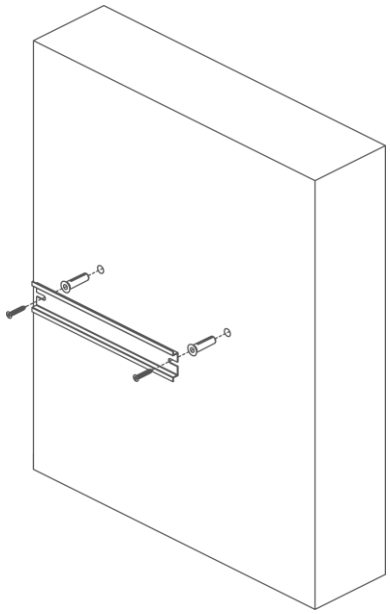


Рисунок 3-2 Вставка винтов

3. Смонтируйте устройство на направляющей рейке и и завершите установку.

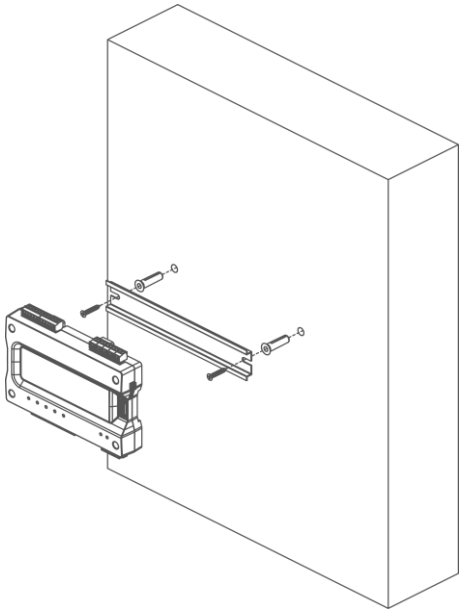


Рисунок 3-3 Фиксация устройства

3.2 Установка контроллера лифта (с шасси)

Шаги

Примечание

Стена или другое место монтажа должно выдерживать массу втрое больше массы устройства.

1. Просверлите отверстия в стене в соответствии с отверстиями для винтов в корпусе и вставьте в них дюбеля.
2. Используйте винты, входящие в комплект, чтобы выровнять положение дюбелей, зафиксируйте корпус в монтажном положении и завершите установку.

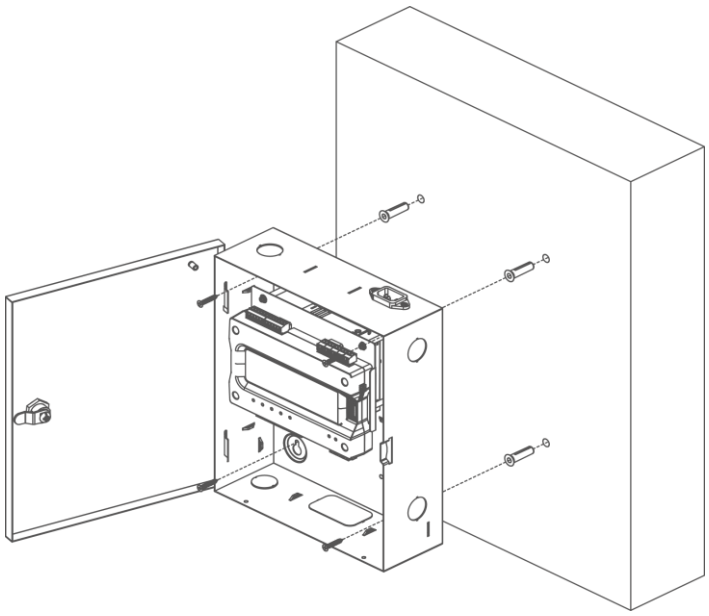


Рисунок 3-4 Фиксация устройства

Глава 4 Настройки

Инициализация оборудования

Удерживайте кнопку восстановления настроек в течение 5 секунд для инициализации оборудования.

Реле пожарной тревоги NO/NC

Положение противопожарной перемычки и соответствующее состояние NO/NC указаны ниже.

Примечание

Для выполнения этой операции необходимо разобрать верхнюю и нижнюю части устройства, что рекомендуется делать специалистам.

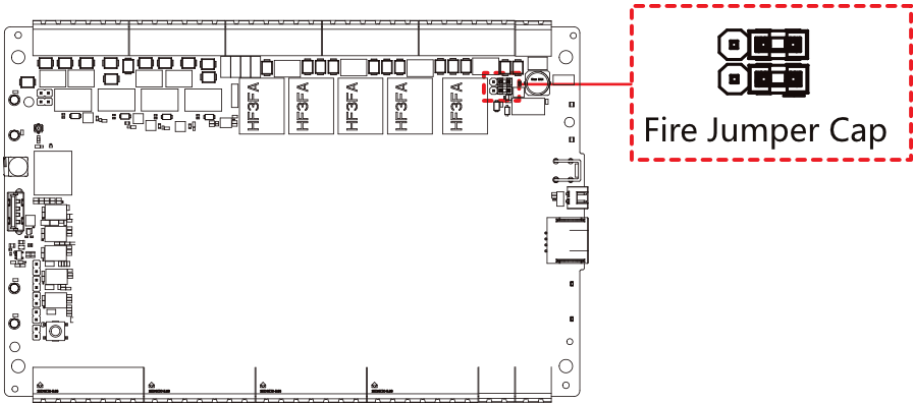
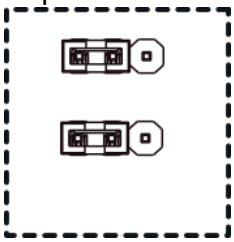
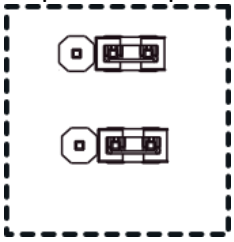


Рисунок 4-1 Описание положения противопожарной перемычки

Нормально замкнутый контакт



Нормально разомкнутый контакт



Раздел 5 Активация устройства

Перед первым входом в систему необходимо активировать устройство. После включения устройства система переключится на страницу активации устройства.
Поддерживается активация через само устройство, активация при помощи ПО SADP и при помощи клиентского ПО.
Значения по умолчанию для устройства следующие:

- IP-адрес по умолчанию: 192.0.0.64
- Доступ к устройству осуществляется через веб-интерфейс с использованием порта 443.
- Имя пользователя по умолчанию: admin

5.1 Активация через веб-интерфейс

Можно активировать устройство через веб-интерфейс.

Шаги

1. Введите IP-адрес устройства по умолчанию (192.0.0.64) в адресную строку веб-интерфейса и нажмите **Enter** («Ввод»).

Примечание

IP-адреса устройства и компьютера должны находиться в одном IP-сегменте.

2. Создайте новый пароль (пароль администратора) и подтвердите его.

Предостережение

- Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопаснее.
- Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг и / или конечного пользователя.
- В пароле не должны содержаться следующие символы: имя пользователя, 123, admin (без учета регистра), 4 или более непрерывно увеличивающихся или уменьшающихся цифр или 4 или более последовательно повторяющихся символов.

3. Нажмите **Activate** («Активировать»).
4. Изменение IP-адреса устройства. IP-адрес можно редактировать с помощью инструмента SADP, устройства и клиентского программного обеспечения.

5.2 Активация через ПО SADP

Программное обеспечение SADP — это инструмент для обнаружения, активации и изменения IP-адреса устройства через локальную сеть.

Перед началом

- ПО SADP доступно на диске, входящем в комплект или на официальном сайте; установите ПО SADP согласно инструкции.
- Устройство и ПК, на котором запущено ПО SADP, должны находиться в одной подсети.

Следующие шаги показывают, как активировать устройство и изменить его IP-адрес. Подробная информация о пакетной активации и изменении IP-адресов представлена в ***Руководстве пользователя ПО SADP***.

Шаги

1. Запустите ПО SADP для поиска онлайн устройств.
2. Найдите и выберите устройство в списке онлайн устройств.
3. Введите новый пароль (пароль администратора) и подтвердите его.

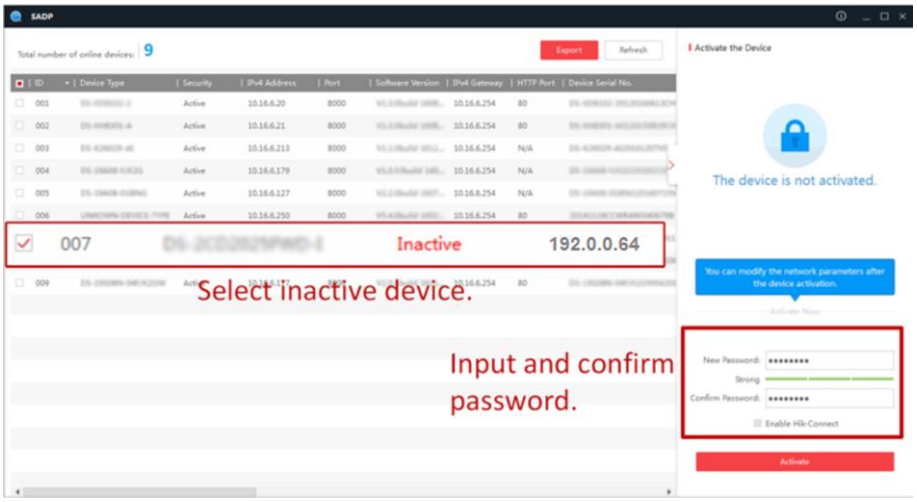
Предостережение

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

Примечание

Символы, содержащие admin и nimda, не могут быть использованы для активации пароля.

4. Нажмите **Activate** («Активировать») для начала активации.



После успешной активации статус устройства изменится на **Active** («Активно»).

5. Измените IP-адрес устройства.
   1) Выберите устройство.
   2) Измените IP-адрес устройства на адрес в той же подсети, к которой подключен компьютер вручную или поставив галочку **Enable DHCP** («Включить DHCP»).
   3) Введите пароль администратора и нажмите **Modify** («Изменить») для изменения вашего IP-адреса.

Раздел 6 Сценарии применения

Описание стандартных сценариев применения контроллера доступа, модуля доступа, замка и платформы.

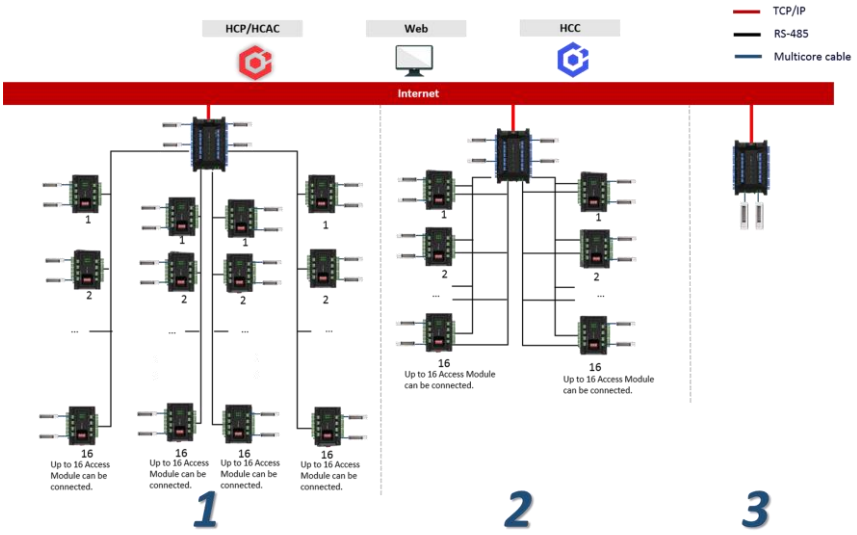


Рисунок 6-1 Стандартные сценарии применения

1. Без резервной защиты RS-485 макс. 128 дверей.
2. С резервной защитой RS-485 макс. 64 дверей.
3. Макс. 4 двери.

Раздел 7 Быстрые операции через веб-интерфейс

7.1 Настройка контрольного вопроса

Если вы забыли пароль активации устройства, можно изменить его с помощью контрольных вопросов и электронной почты. Настройте контрольные вопросы.
Нажмите в верхнем правом углу веб-страницы для перехода на страницу **Change Password** («Изменить пароль»).

Проверка по контрольным вопросам

Ответьте на контрольные вопросы.

Подтверждение по электронной почте

1. Экспортируйте QR-код и отправьте его на адрес сервера электронной почты во вложении.
2. Проверочный код будет отправлен на зарезервированный адрес электронной почты в течение 5 минут.
3. Введите проверочный код в поле проверочного кода для подтверждения идентификации.

Нажмите **Next** («Далее»). Или нажмите **Skip** («Пропустить»), чтобы пропустить этот шаг.

7.2 Выбор языка

Можно выбрать язык системы устройства.
Нажмите в верхнем правом углу веб-страницы для перехода на страницу **Device Language Settings** («Настройка языка устройства»). Можно выбрать язык для системы устройства из выпадающего списка.
По умолчанию языком системы выбран английский.

Примечание

После изменения языка системы устройство автоматически перезагрузится.

7.3 Настройка времени

Нажмите в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек.

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

NTP

Необходимо задать IP-адрес NTP-сервера, номер порта и интервал.

Вручную

По умолчанию время устройства должно быть синхронизировано вручную. Можно установить время устройства вручную или нажать **Sync. with Computer Time** («Синхронизировать со временем компьютера»), чтобы синхронизировать время устройства со временем компьютера.

Адрес сервера / Порт NTP / Интервал

Можно настроить адрес сервера, порт NTP, интервал.

Переход на летнее время (DST)

Установите время начала и окончания перехода на летнее время (DST), а также смещение.

Глава 8 Работа через веб-интерфейс

8.1 Вход в систему

В систему можно войти через веб-интерфейс или удаленную настройку клиентского программного обеспечения.

Примечание

- Устройство должно быть активировано. Подробная информация представлена в разделе Активация.
- Рекомендуется входить в систему через браузер Chrome.

Вход в систему через веб-интерфейс

Введите IP-адрес устройства в адресной строке веб-интерфейса и нажмите **Enter** («Ввод») для того, чтобы войти в систему.
Введите имя пользователя и пароль. Нажмите **Login** («Вход»).

Вход в систему через удаленную настройку клиентского программного обеспечения

Загрузите и откройте клиентское программное обеспечение. После добавления устройства нажмите , чтобы перейти на страницу настройки.

8.2 Забыть пароль

Если вы забыли пароль для входа в систему, пароль можно поменять с помощью адреса электронной почты или контрольных вопросов.
На странице входа в систему нажмите **Forget Password** («Забыть пароль»).
Выберите **Verification Mode** («Режим проверки»).

Проверка по контрольным вопросам

Ответьте на контрольные вопросы.

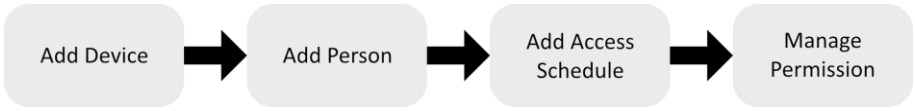
Подтверждение по электронной почте

1. Экспортируйте QR-код и отправьте его на адрес сервера электронной почты во вложении.
2. Проверочный код будет отправлен на зарезервированный адрес электронной почты в течение 5 минут.
3. Введите проверочный код в поле проверочного кода для подтверждения идентификации.

Создайте новый пароль и подтвердите его.

8.3 Описание модулей

Можно настроить параметры управления сотрудниками / посетителями, управления устройствами, контроля доступа, системы и технического обслуживания.
Нажмите в правой части экрана, чтобы открыть страницу описания модуля и просмотреть описание каждого модуля. Нажмите на каждую гиперссылку, чтобы перейти на соответствующую страницу настроек.
Описание процесса конфигурации.



Английский язык	**Русский язык**
Add device	Добавление устройства
Add person	Добавление пользователя
Add access schedule	Добавление расписания доступа
Manage permission	Управление разрешением

8.4 Управление контролем доступа

8.4.1 Обзор

Можно выбрать область и управлять состоянием двери, просматривать состояние устройства, просматривать события, просматривать данные тревоги, просматривать информацию о человеке, состояние сети, основную информацию и емкость устройства. Также можно перейти на страницу из раздела быстрого запуска
Войдите в веб-интерфейс и перейдите в раздел **Access Control** → **Overview** («Контроль доступа → Обзор»).

Состояние двери

Нажмите **View More** («Дополнительно»), чтобы просматривать и управлять состоянием всех дверей.

/ / /

Установите состояние двери: открыта / закрыта / оставить открытой / оставить закрытой.

Быстрый запуск

Нажмите **Add Person** («Добавить пользователя»), **Add Device** («Добавить устройство»), **System Settings** («Системные настройки») или **System and Maintenance** («Система и обслуживание») в правом верхнем углу страницы, чтобы быстро перейти на страницу настройки параметров.

Событие

Можно просмотреть идентификатор сотрудника, имя, номер карты, тип события, время и операции.
Можно нажать **View More** («Просмотреть больше») и ввести условия поиска, включая идентификатор сотрудника / посетителя, имя, номер карты, время начала и время окончания доступа, затем нажать **Search** («Поиск»). После этого на панели справа появятся результаты поиска.

Данные тревоги

Можно просмотреть данные о тревоге.

Состояние устройства

Просмотрите состояние других подключенных устройств.

Информация о пользователе

Просмотрите номер сотрудника / посетителя, номер карты, номер отпечатка пальца.

Состояние сети

Можно просмотреть состояние подключения и регистрации проводной сети, беспроводной сети, ISUP и облачного сервиса.

Основная информация

Можно просмотреть модель, серийный номер и версию прошивки.

Емкость устройства

Можно просмотреть количество людей, карт, отпечатков пальцев и событий.

8.4.2 Поиск событий

Нажмите **Access Control → Event Search** («Контроль доступа → Поиск события») для перехода на страницу поиска.
Введите условия поиска, включая идентификатор сотрудника / посетителя, имя, номер карты, время начала и время окончания доступа и нажмите **Search** («Поиск»).

Примечание

Название для поиска должно быть не более 32 бит.

После этого на панели справа появятся результаты поиска.

8.4.3 Управление точкой доступа

Нажмите **Access Control** → **Access Point Management** («Контроль доступа → Управление точкой доступа»), чтобы просмотреть двери, связанные с контроллером доступа, и считыватели карт, связанные с этими дверями.
Наведите курсор мыши на дверь или считыватель карт в правой части интерфейса и нажмите, чтобы настроить параметры двери и параметры аутентификации считывателя карт.

Настройка параметров двери

Настройте параметры двери.
Можно перейти на страницу параметров двери двумя способами.
1. Нажмите **Access Control** → **Access Point Management** («Контроль доступа → Управление точкой доступа»). Наведите курсор мыши на дверь и нажмите , чтобы перейти на страницу параметров двери.
2. Нажмите **Access Control → Parameter Settings → Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»).
Нажмите **Save** («Сохранить»), чтобы сохранить настройки. Нажмите **Copy to** («Копировать в»), чтобы скопировать параметры двери на другие двери.

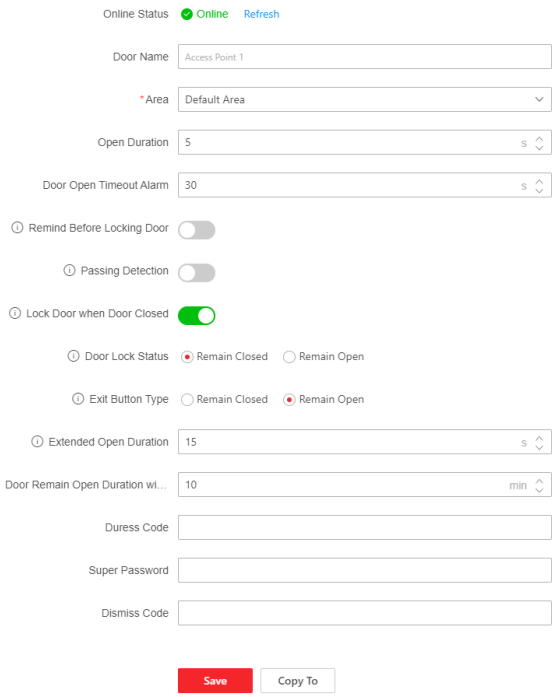


Рисунок 8-1 Настройка параметров двери

Наименование двери

Можно задать имя двери.

Область

Выберите добавленную область или нажмите **Add Area** («Добавить область»), чтобы добавить новую область для двери.

Длительность открытого состояния

Укажите длительность открытого состояния двери. Дверь будет заблокирована, если движение отсутствует в течение установленного времени.

Напоминание перед блокировкой двери

Напоминание сопровождается звуковым сигналом считывателя карт, а также может мигать индикатор.

Детекция прохода

Если функция включена и дверь не открывается в течение времени разблокировки, событие будет записано как **Passing Allowed (Door Not Used)** («Проход разрешен (Дверь не используется)»).

Блокировка двери при закрытии

Относится к состоянию двери при включении дверного замка. Если дверной замок не катодный, выберите **Remain Closed** («Оставить закрытым»). В противном случае выберите **Remain Open** («Оставить открытым»).

Тревога тайм-аута открытой двери

Тревога сработает, если дверь не будет закрыта в течение заданного периода времени.

Состояние дверного замка

Можно установить состояние дверного замка: **Remain Open** («Оставить открытым») или **Remain Closed** («Оставить закрытым»). По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).

Тип кнопки выхода

Можно установить параметры кнопки выхода как **Remain Open** («Оставить открытым») или **Remain Closed** («Оставить закрытым»). По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).

Увеличение длительности открытого состояния

Дверной контакт может быть активирован с установленной задержкой после считывания карты пользователя с расширенным доступом.

Дверь остается открытой после авторизации первого сотрудника

Установите продолжительность открытия двери после авторизации первого сотрудника. После авторизации первого пользователя несколько других пользователей получат доступ к дверям и разрешения на другие действия.

Код принуждения

Дверь может быть открыта при помощи кода принуждения. При этом клиент может создает уведомление о событии принуждения.

Суперпароль

Пользователь может открыть дверь с помощью суперпароля.

Код отклонения

При срабатывании тревоги можно ввести код отклонения, чтобы отключить тревогу.

Примечание

Суперпароль должен отличаться от кода принуждения.

Настройка параметров аутентификации

Можно перейти на страницу параметров аутентификации двумя способами.
1. Нажмите **Access Control → Access Point Management** («Контроль доступа → Управление точкой доступа»). Наведите курсор мыши на считыватель карт и нажмите ⚙, чтобы перейти на страницу параметров аутентификации.
2. Нажмите **Access Control** → **Parameter Settings** → **Authentication Parameters** («Контроль доступа → Настройки параметров → Параметры аутентификации»).
Нажмите **Save** («Сохранить»), чтобы сохранить настройки. Нажмите **Copy to** («Копировать в»), чтобы скопировать параметры считывателя карт на другие считыватели карт.

Примечание

Функционал устройств может различаться в зависимости от модели. Проверьте функционал фактического устройства.

Конфигурация параметров считывателя карт

Название считывателя карт

Придумайте название для считывателя карт.

Тип считывателя карт/описание считывателя карт

Просмотрите тип и описание считывателя карт.

Включить устройство с функцией аутентификации

Включить функцию аутентификации.

Интервал аутентификации

Можно установить интервал аутентификации одного и того же сотрудника во время аутентификации. Один сотрудник может пройти аутентификацию только один раз в заданный интервал. Вторая аутентификация будет невозможна.

Запуск тревоги при достижении максимального количества неудачных попыток считывания карты

Можно включить функцию сообщения о тревоге при достижении максимального количества неудачных попыток считывания карты.

Достижение макс. количества неудачных попыток аутентификации

Можно включить функцию сообщения о тревоге при достижении максимального количества неудачных попыток считывания карты.

Связь с контроллером

Если устройство контроля доступа не может подключиться к считывателю карт в течение установленного времени, считыватель карт отключится автоматически.

Максимальный интервал времени при вводе пароля

Если при вводе пароля в устройство для считывания карт интервал между нажатием двух цифр больше установленного значения, цифры, которые пользователь нажал до этого, будут автоматически удалены.

Правильная полярность светодиода / Ошибочная полярность светодиода / Полярность бипера

Настройте **OK LED Polarity** («Полярность светодиода при нормальном состоянии») / **Error LED Polarity** («Полярность светодиода при ошибке») / **Buzzer Polarity** («Полярность бипера») устройства контроля доступа в соответствии с параметрами считывателя карт. Как правило, устройство получает настройки по умолчанию.

Тревога тампера

Включите детектор саботажа на считывателе карт.

QR-код

Включите функцию, и считыватель карт сможет распознавать QR-код для аутентификации.

Примечание

Функция должна поддерживаться считывателем карт.

Конфигурация параметров Bluetooth

Включить Bluetooth

Включите функцию Bluetooth, чтобы использовать ее на считывателе карт (например, для открытия двери).

Название устройства / Мощность передачи

Измените название считывателя карт и его мощность передачи.

Открытие двери с помощью Bluetooth

Включите функцию, чтобы открывать дверь через Bluetooth с помощью приложения. Перед использованием функции необходимо добавить устройство в приложение.

Открытие двери жестом / Перекрытие / Длительность перекрытия / Дальность обнаружения перекрытия

После включения дверь можно будет открывать жестом. Необходимо установить длительность и дальность обнаружения перекрытия.

Примечание

Непрерывное перекрытие датчика не допускается. Продолжительность каждого перекрытия не должна превышать 5 секунд.

Конфигурация плана аутентификации

Установите расписание аутентификации для считывателя карт.

Выберите тип аутентификации и перетащите временной интервал в таблице расписания, чтобы задать продолжительность аутентификации.
Нажмите **Clear** («Очистить») и перетащите временной интервал для удаления или нажмите ··· → **Clear All** («Очистить все»), чтобы удалить все временные интервалы.

Настройка интеллектуальных параметров

Нажмите **Access Control** → **Parameter Settings** → **Smart** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции → Интеллектуальные функции»).

Примечание

- Функционал устройств может различаться в зависимости от модели. Проверьте функционал фактического устройства.
- После настройки общих параметров все считыватели карт начнут работать.

Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Распознавание отпечатков пальцев

После включения функции распознавания отпечатков пальцев устройство будет поддерживать эту функцию.

Уровень безопасности отпечатков пальцев

Выберите уровень безопасности отпечатков пальцев.
Чем выше уровень безопасности, тем ниже вероятность ошибочного предоставления доступа.

8.4.4 Управление разрешениями

Можно установить шаблон расписания для разрешений на доступ, шаблон расписания на праздничные дни и настроить разрешение на доступ.

Конфигурация шаблона расписания

Добавление шаблона расписания доступа

Шаблон расписания доступа используется для установки разрешенного времени входа и выхода людей. На системном диске доступны 3 шаблона расписания доступа по умолчанию: **All-day Template** («Шаблон всего дня»), **Workday Template** («Шаблон рабочего дня») и **Weekend Template** («Шаблон нерабочего дня»). Также можно добавить пользовательский шаблон в соответствии с текущими потребностями.

Шаги

1. Нажмите **Access control** → **Permission Management** → **Access Plan Management** → **+Add** («Контроль доступа → Управление разрешениями → Управление расписанием доступа → +Добавить»).

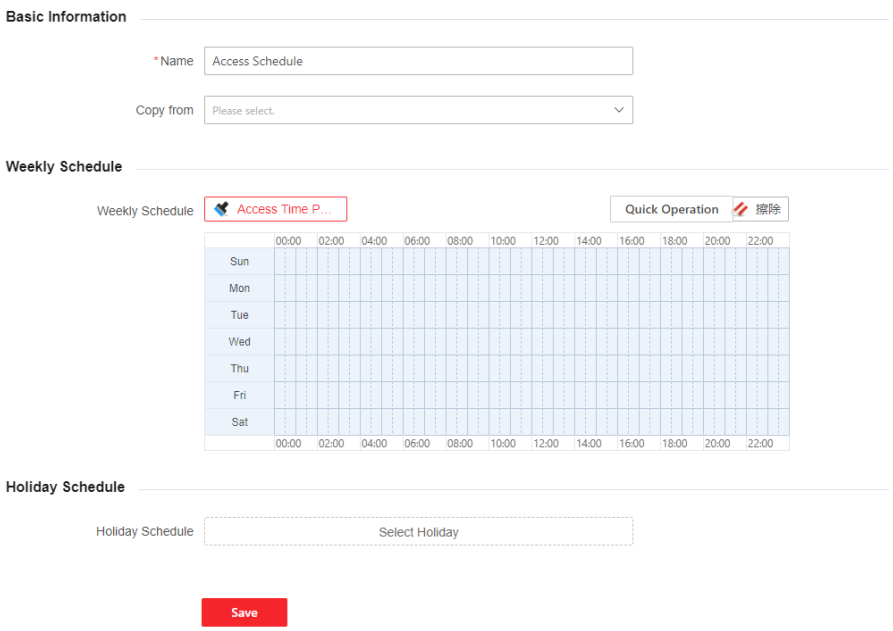


Рисунок 8-2 Добавление шаблона расписания для доступа

2. Укажите основную информацию.

Название

Укажите основную информацию.

Копировать из

Пользователь может выбрать существующий шаблон. После выбора шаблон будет скопирован в текущий шаблон. Пользователь может вносить изменения на основе выбранного шаблона.

3. В разделе **Weekly Schedule** («Еженедельное расписание») нажмите **Access Time Period** («Период доступа»), затем перетащите курсор по временной шкале, чтобы установить время доступа. Можно включить и установить время аутентификации.

Примечание

Максимальное количество периодов в день – 8.

4. Опционально. Нажмите **Clear** («Очистить»), затем перетащите курсор. Пересекающуюся часть можно удалить. Также можно выбрать определенный период времени и настроить его вручную.
5. Опционально. Выберите **Holiday Schedule** («Расписание праздников»).

Примечание

Если выбранное расписание праздников противоречит еженедельному расписанию, приоритет будет отдан еженедельному расписанию.

1) Нажмите **Select Holiday** («Выбрать праздники»).

2) Выберите существующее расписание праздников или нажмите **Add** («Добавить»). Введите название праздника, дату и период доступа.

Примечание

Максимальное количество периодов в день – 8.

3) Нажмите **OK**.
4) Затем пользователь может проверить разрешенный период доступа во время праздников.

6. Нажмите **Save** («Сохранить»).

Шаблон расписания выходных

Установите официальные праздники или указанные даты в качестве праздников. Уровень доступа для установленных праздников выше, чем для других базовых уровней доступа.

Шаги

1. Нажмите **Access control** → **Permission Management** → **Access Plan Management** → **+Add** («Контроль доступа → Управление разрешениями → Управление расписанием доступа → +Добавить»).
2. Введите название праздника в правом столбце.
3. Опционально. Включите параметр **Repeat Annually** («Повторять ежегодно»), если необходимо. После включения шаблон будет действовать каждый год. Повторная настройка не требуется. Применимо для установки официальных праздников.
4. Установите дату начала и дату окончания периода.
5. Перетащите курсор на соответствующую временную шкалу, чтобы отобразить допустимый период доступа. Пользователи могут получить доступ в течение допустимого периода доступа. Можно включить и установить время аутентификации.
6. Опционально. Нажмите **Clear** («Очистить»), чтобы настроить выбранный период времени. Также можно выбрать определенный период времени и настроить его вручную.
7. Нажмите **Save** («Сохранить»).

Управление контролем доступа

Права доступа можно настраивать или классифицировать в зависимости от точки доступа.

Шаги

1. Нажмите **Access control** → **Permission Management** → **+Add** («Контроль доступа → Управление разрешениями → +Добавить»).

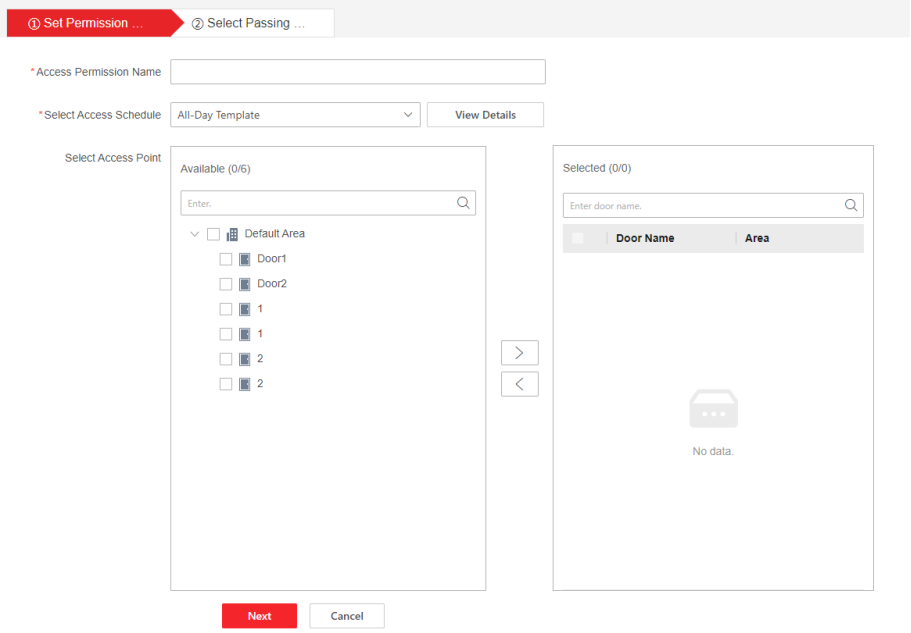


Рисунок 8-3 Управление контролем доступа

2. Введите **Access Permission Name** («Название разрешения доступа»).
3. Выберите шаблон **Access Schedule** («Расписание доступа»). Нажмите **View Licenses** («Просомтр лицензий») справа, чтобы проверить периоды доступа для различных шаблонов.
4. Нажмите **+Add** («Добавить»). Выберите точку доступа.
5. Нажмите **Next** («Далее»), введите или отметьте название организации или имя пользователя.
6. Нажмите **Complete** («Завершить»).
7. Опционально. Можно нажать **Batch Add Passing Persons** («Добавление проходящих людей в пакетном режиме»), выбрать разрешение для добавляемого лица, организации и человека.

Установка разрешения на прохождение в автономном режиме

Когда модуль доступа отключается от контроллера доступа, модуль доступа может блокировать или разблокировать дверь в зависимости от настроенного разрешения на проход.

Шаги

1. Нажмите **Access control** → **Permission Management** → **Offline Passing Permission** («Контроль доступа → Управление разрешениями → Разрешение на проход в автономном режиме»).
2. Настройте разрешение на проход в автономном режиме. Выберите устройство. Можно включить или отключить **Allow Offline Passing** («Разрешение на проход в автономном режиме»).

3. Настройте параметры аутентификации. Нажмите → **Add** («Добавить»), введите название организации, выберите пользователя или включите **Quick Select** («Быстрый выбор»), выберите пользователей в пакетном режиме и нажмите **OK**.
4. Опционально. Можно выбрать несколько устройств и нажать **Batch Enable Offline Passing** («Включить автономный доступ в пакетном режиме»), **Batch Disable Offline Passing** («Отключить автономный доступ в пакетном режиме»), **Enable All** («Включить все») или **Disable All** («Отключить все»), чтобы установить разрешение на автономный доступ.

8.4.5 Приложения контроля доступа

Открытие двери первой картой

После того, как указанный человек (первый человек) пройдет проверку с помощью учетных данных (например, карты, отпечатка пальца, лица), остальные могут войти напрямую или пройти, используя учетные данные. Обычно это применяется в сценариях с общественным транспортом.

Шаги

1. Нажмите **Access Control** → **Access Control Application** → **Open Door with First Person** → **Settings** → **+Add** («Контроль доступа → Приложение контроля доступа → Открытие двери первой картой → Настройки → +Добавить»).

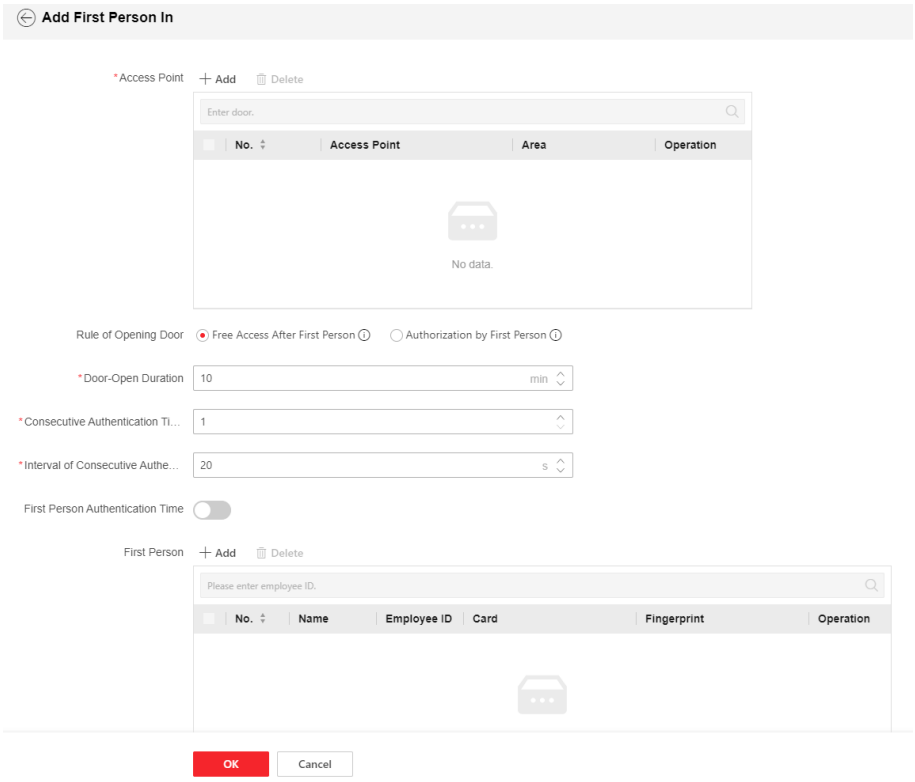


Рисунок 8-4 Открытие двери первой картой

2. Нажмите **+Add** («Добавить»). Выберите точку доступа.

3. Настройте параметры для открытия двери первой картой.

Правила открытия двери

Свободный доступ после первого человека

Этот режим применим для прохождения групп людей, например, посетителей, посещающих живописные места. После прохождения указанного человека дверь откроется на заданное время, и другие люди смогут пройти без аутентификации. Длительность открытого состояния двери

Авторизация после первого лица

Этот режим применим в местах с высокими требованиями к безопасности. Только после того, как пользователь, у которого настроены права доступа, пройдет проверку подлинности с использованием учетных данных, другие пользователи смогут пройти проверку подлинности с использованием учетных данных.

Количество последовательных аутентификаций

Количество успешных последовательных аутентификаций.

Интервал последовательной аутентификации

Допустимая продолжительность интервала последовательной аутентификации для одного и того же человека. Повторная аутентификация одного и того же человека в течение интервала недопустима.

Время первой аутентификации пользователя

Установите **Rules Takes Effect at** («Правила вступают в силу») и **Authentication Period** («Период аутентификации»).

4. Для выбора первого пользователя нажмите **+Add** («Добавить»).
   1) Нажмите **+Add** («Добавить»).
   2) Выберите пользователя.
   3) Нажмите **OK**.
5. Нажмите **OK**.
6. Опционально. Выберите пользователей, которых вы хотите удалить из списка. Нажмите **Delete** («Удалить»).

Параметры многофакторной аутентификации

Пользователи, входящие в группу многофакторной аутентификации, могут открывать дверь только после аутентификации в соответствии с правилом многофакторной аутентификации.

Перед началом

- Подробная информация о конфигурации и ее способах представлена в разделе ***Управление разрешениями***.

Шаги

1. Нажмите **Access Control** → **Access Control Application** → **Multi-Factor Authentication** → **Set** («Контроль доступа → Приложение контроля доступа → Многофакторная аутентификация → Установка»).

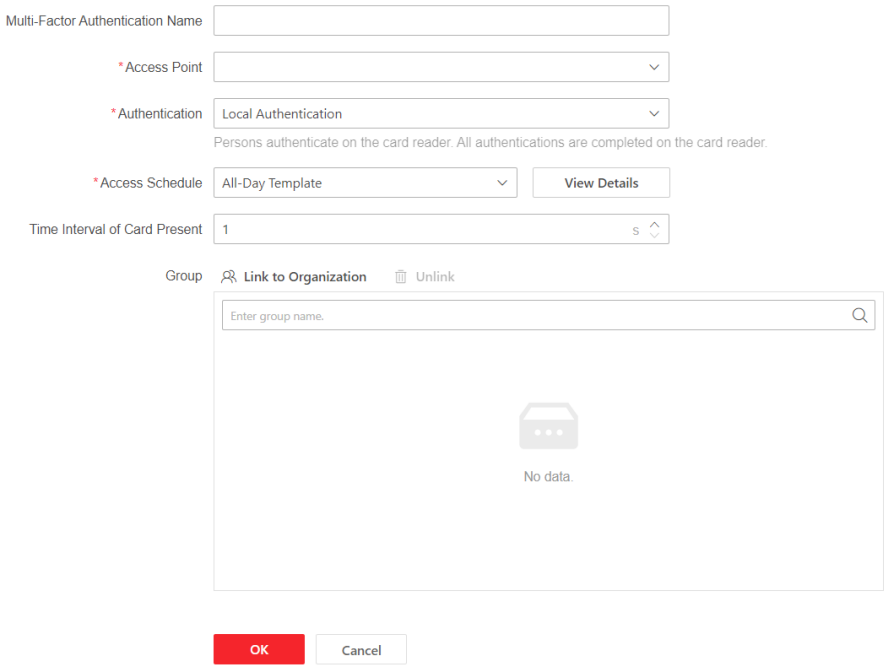


Рисунок 8-5 Настройки многофакторной аутентификации

2. Нажмите **Group Management** («Управление группами»), чтобы настроить группу.
   1) Нажмите **+** слева, затем введите название группы.
   2) Нажмите **+Add** («+Добавить») и выберите пользователей, которых необходимо добавить в эту группу. Нажмите **OK**.
   3) Нажмите **OK**. Добавленные группы будут отображаться в левой колонке. Информация о членах группы будет отображаться в правой части страницы.
   4) Опционально. Выберите одну группу, затем нажмите **+Add** («+Добавить») справа, чтобы добавить больше членов группы. Выберите и нажмите **OK**.
3. Добавьте правило многофакторной аутентификации.
   1) Нажмите **+Add** («+Добавить») в интерфейсе многофакторной аутентификации.
   2) Установите параметры распознавания лиц.

Название многофакторной аутентификации

Введите название многофакторной аутентификации.

Точка доступа

Выберите из выпадающего списка точку доступа, для которой требуется многофакторная аутентификация.

Режим аутентификации

Локальная аутентификация

Пользователи могут открыть дверь только после того, как они завершат аутентификацию в соответствии с правилами на считывателе карт.

Локальная аутентификация + Удаленное открытие двери

Пользователи должны сначала пройти аутентификацию на устройстве, и аутентификация будет подтверждена удаленно на клиенте.

Локальная аутентификация + Учетные данные суперпользователя

Аутентификация на считывателе карт. Если считыватель карт не в сети, аутентификация выполняется с помощью учетных данных суперпользователя.

Расписание доступа

Выберите расписание доступа, требующее многофакторной аутентификации. Нажмите **View Licenses** («Просомтр лицензий»), чтобы более подробно ознакомиться с выбранным шаблоном расписания.

Интервал времени предъявления карты

Интервал времени между конфигурацией для двух разных пользователей.

Группа

Нажмите **Link to Organization** («Привязка к организации»), чтобы выбрать группу. Настройте последовательность выбранных групп, перетаскивая на панели действий. Перед открытием двери, сверьтесь с последовательностью в списке и количеством людей, которых необходимо проверить, для фактической проверки.

3) **OK**.

4. Опционально. Выберите параметр («Многофакторная аутентификация не требуется»), затем нажмите **Delete** («Удалить»).
5. Нажмите , чтобы подробнее ознакомиться с расписанием доступа.

Настройки блокировка нескольких дверей

Можно установить блокировку нескольких дверей для нескольких дверей одного контроллера доступа. Чтобы открыть одну из дверей, другие двери должны оставаться закрытыми.

Шаги

1. Нажмите **Access Control** → **Access Control Application** → **Multi-Door Interlocking** → **Set** («Контроль доступа → Приложение контроля доступа → Блокировка нескольких дверей → Установка»).

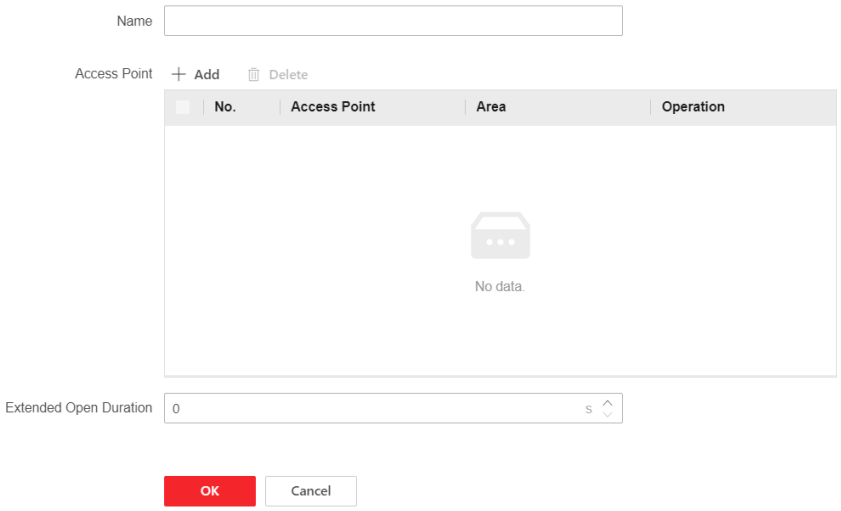


Рисунок 8-6 Настройки блокировки нескольких дверей

2. Введите название.
3. Нажмите **+Add** («Добавить»), выберите точку доступа, чтобы сформировать группу блокировки нескольких дверей.
4. Рекомендуется удалить ненужные точки доступа в зоне.
   – Выберите точки доступа, которые не нужны. Нажмите **Delete** («Удалить»), чтобы удалить в пакетном режиме.
   – Нажмите , чтобы удалить одну точку доступа.
5. Нажмите **OK**.
6. Удаление или изменение параметров блокировки нескольких дверей.
   – Выберите одну блокировку нескольких дверей. Нажмите для редактирования.
   – Выберите одну блокировку нескольких дверей. Нажмите , чтобы удалить.
   – Выберите несколько блокировок дверей. Нажмите **Delete** («Удалить»), чтобы удалить в пакетном режиме.

Настройки запрета двойного прохода

Проход через точки доступа возможен только в заданной последовательности. Если не следовать заданному пути, дверь не откроется. Если пользователь проведет картой, не пройдя через систему, его вход будет заблокирован при следующем проходе. И наоборот.

Шаги

1. Нажмите **Access Control** → **Access Control Application** → **Anti-Passback** («Контроль доступа → Приложение контроля доступа → Запрет двойного прохода»).
2. Добавьте маршрут для запрета двойного прохода.
   1) Введите название параметра для запрета двойного прохода. Нажмите **Next** («Далее»).
   2) Порядок считывателей карт. Нажмите **Add** («Добавить»). Выберите нужный считыватель карт.
   3) Нажмите , чтобы добавить следующий считыватель карт.
   4) Повторите подпункт 3, чтобы добавить другие считыватели карт.

5) Опционально. Нажмите на считыватель карт, чтобы заменить или удалить его.
6) Нажмите **Next Step** («Следующий шаг»).
7) Первый считыватель карт

Отключить

- Если считыватель карт, через который проходил пользователь в прошлый раз, не имеет защиты от повторного прохода, или пользователь является новым пользователем, доступ с защитой от повторного прохода предоставляется.
- Если считыватель карт, через который проходил пользователь в прошлый раз, имеет защиту от повторного прохода, и текущий считыватель карт является следующим за ним считывателем в маршруте защиты от повторного прохода, доступ с защитой от повторного прохода предоставляется; если текущий считыватель карт не является следующим за ним считывателем карт, доступ с защитой от повторного прохода запрещен.

Выбор одного считывателя карт в качестве первого

- Доступ предоставляется каждый раз, когда пользователь проводит своей картой через первый считыватель карт.
- Если считыватель карт, через который проходил пользователь в прошлый раз, имеет функцию защиты от повторного прохода, и текущий считыватель карт является следующим за ним в этом же маршруте защиты от повторного прохода, доступ с защитой от повторного прохода предоставляется; если текущий считыватель карт не является следующим за ним, доступ с защитой от повторного прохода запрещен.

Примечание

- Если нарушить правило запрета двойного прохода, необходимо повторно считать карту через первый считыватель карт.
- Исключением являются суперпользователи.
- На маршруте запрета двойного прохода может быть не более 64 дверей.

3. Опционально. Параметры запрета двойного прохода.
1) Нажмите **Anti-Passback Parameter** («Параметр запрета двойного прохода»).
2) Выберите режим оценки состояния прохождения человека.

По состоянию аутентификации

Процесс запрета двойного прохода определяется аутентификацией по карте.

По фактическому состоянию потока

Процесс запрета двойного прохода определяется фактическим открытием с помощью карты.

3) Включите **Forgive Anti-Passback** («Отключение запрета двойного прохода»), чтобы настроить расписание.

Режим отключения

Регулярное отключение запрета двойного прохода

Настройте время для **Forgive Anti-Passback Regularly** («Регулярное отключение запрета двойного прохода»). Система автоматически отключит запрет двойного прохода. Затем пользователю необходимо следовать по маршруту запрета двойного прохода, начиная с первого считывателя карт.

Задержка отключения запрета двойного прохода

Настройте время для **Delay Forgive Anti-Passback** («Задержка отключения запрета двойного прохода»). Система начнет отсчет времени и отключит запрет двойного прохода, как только будет достигнуто установленное время задержки. Затем необходимо следовать правилу запрета двойного прохода и начать заново с первого считывателя карт.

Период без запрета двойного прохода

Выберите **Effective Time** («Время действия»), затем перетащите курсор по временной шкале, чтобы отметить период без запрета двойного прохода. Запрет двойного прохода недействителен в течение выбранного периода.
Нажмите **Clear** («Очистить») и перетащите курсор по метке времени, чтобы удалить определенный период времени.
Нажмите ··· → **Clear All** («Очистить все»), чтобы удалить все выбранные периоды времени.

4) Нажмите **Save** («Сохранить»).

4. Изменение или удаление настроенных запретов двойного прохода.
   – Нажмите на запрет двойного прохода. Нажмите для редактирования.
   – Нажмите на запрет двойного прохода. Нажмите , чтобы удалить.
   – Выберите несколько запретов двойного прохода. Нажмите **Delete** («Удалить»), чтобы удалить в пакетном режиме.
   – Нажмите на запрет двойного прохода. Нажмите , чтобы просмотреть маршрут запрета двойного прохода.

Настройка состояния двери: оставить открытой / закрытой

Установите период времени по неделям, в течение которого дверь остается закрытой / открытой.

Шаги

1. Нажмите **Access Control** → **Access Control Application** → **Remain Open or Closed** → **Set** («Контроль доступа → Приложение контроля доступа → Оставить дверь открытой / закрытой → Установка»).

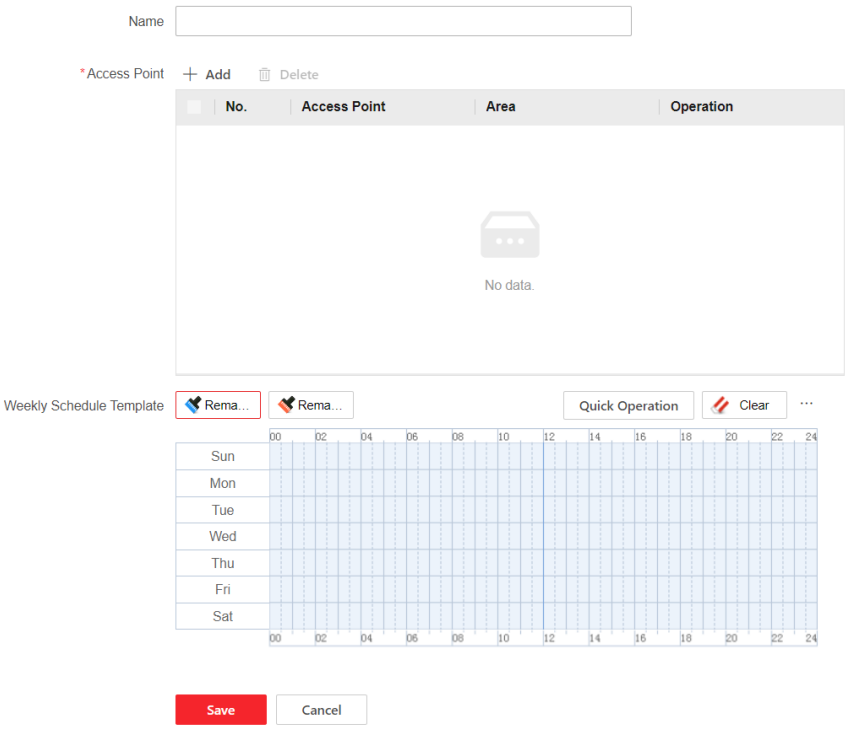


Рисунок 8-7 Оставить открытой / закрытой

2. Нажмите **+Add** («Добавить»).
3. Добавьте точку доступа.
   1) Нажмите **+Add** («Добавить»).
   2) Выберите точку доступа во всплывающем окне справа. Нажмите **OK**.
   3) Нажмите , чтобы удалить одну точку доступа, или выберите несколько точек доступа, а затем нажмите **Delete** («Удалить»), чтобы удалить их в пакетном режиме.
4. Шаблон расписания на неделю.
   1) Укажите период времени для параметров **Remain Open** («Оставить отрытой») или **Remain Closed** («Оставить закрытой»).
   – Нажмите **Remain Open** («Оставить открытой») или **Remain Closed** («Оставить закрытой»). Перетащите курсор по метке времени, чтобы указать необходимый период.
   – Нажмите **Remain Open** («Оставить открытой») или **Remain Closed** («Оставить закрытой»), затем нажмите **Quick Operation** («Быстрая операция»). Выберите **All-Day Schedule** («Расписание на весь день»), **Workday Schedule** («Расписание рабочего дня») или **Weekend Schedule** («Расписание выходного дня»). Система автоматически выберет соответствующий временной период.
   1) Опционально. Нажмите **Clear** («Очистить») и перетащите курсор по метке времени, чтобы удалить определенный период времени. Нажмите ··· → **Clear All** («Очистить все»), чтобы удалить все выбранные периоды времени.
5. Нажмите **Save** («Сохранить»).

8.5 Управление пользователями

8.5.1 Добавление организации

После добавления организации к ней можно привязать людей.

Шаги

1. Нажмите **Person Management** («Управление пользователями»), чтобы перейти на страницу настроек.
2. Нажмите кнопку **+** в левой части страницы и выберите главную организацию.
3. Введите название организации.
4. Нажмите **Save** («Сохранить»).
   Добавленная организация будет отображаться в списке выбранной главной организации.
5. Опционально. изменение / удаление
   – Нажмите на организацию, а затем нажмите , чтобы отредактировать информацию об организации.
   Выберите пользователей и нажмите **Delete** («Удалить»), чтобы удалить информацию в пакетном режиме.
   Нажмите **Clear All** («Очистить все»), и вся информация о сотрудниках будет удалена.
   – Выберите организацию и нажмите , чтобы удалить информацию о ней.

8.5.2 Добавление пользователя

Добавьте информацию о пользователе, включая основные данные, сертификат, аутентификацию и настройки.

Добавление основной информации

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Добавьте основные данные о пользователе, включая идентификационный номер сотрудника, имя, организацию, пол и тип пользователя.

Примечание

- При выборе роли пользователя **Visitor** («Посетитель») можно установить количество посещений.
- В идентификационном номере сотрудника допускаются буквы. Допускается до 32 бит.
- В имени допускается до 128 бит.

Нажмите **Add** («Добавить») для сохранения настроек.

Нажмите **Save and Continue** («Сохранить и продолжить»), чтобы сохранить настройки и продолжить добавление следующего пользователя.

Установка времени разрешения

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Включите **Long-Term Effective User** («Пользователь с длительным разрешением») или настройте **Start Time** («Время начала») и **End Time** («Время окончания»), и пользователь сможет получить разрешение только в течение настроенного периода времени.

Нажмите **Add** («Добавить») для сохранения настроек.

Нажмите **Save and Continue** («Сохранить и продолжить»), чтобы сохранить настройки и продолжить добавление следующего пользователя.

Добавление карты

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Нажмите на кнопку **Configuration** («Настройки»). Если в качестве устройства сбора данных выбран **Card Enrollment Station** («Настольный считыватель карт»), необходимо выбрать модель устройства, тип карты, установить бипер, шифрование карты M1 и сектор. Нажмите **OK** для сохранения настроек.

Примечание

Если в качестве устройства сбора данных выбран **Card Enrollment Station** («Настольный считыватель карт»), нажмите **Download** («Загрузить»), чтобы загрузить плагин и просмотреть состояние устройства. Во время установки следует закрыть веб-страницу.

Если в качестве устройства сбора данных установлен **Card Reader** («Считыватель карт»), выберите считыватель карт из выпадающего списка. Нажмите **OK** для сохранения настроек.

Нажмите **Add Card** («Добавление карты»), введите **Card No.** («Номер карты») и выберите **Property** («Свойства»), нажмите **OK**, чтобы добавить карту.

Нажмите **Add** («Добавить») для сохранения настроек.

Нажмите **Save and Continue** («Сохранить и продолжить»), чтобы сохранить настройки и продолжить добавление следующего пользователя.

Добавление отпечатка пальца

Примечание

Только устройства с поддержкой функции считывания отпечатков пальцев могут добавлять считывание отпечатков пальцев.

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Нажмите на кнопку **Configuration** («Настройки»). Если выбран **USB Fingerprint Recorder** («USB-считыватель отпечатков пальцев»), нажмите **Download** («Загрузить»), чтобы загрузить плагин и просмотреть его состояние. Или установите **Fingerprint and Card Reader** («Считыватель отпечатков пальцев и карт») и выберите считыватель карт из выпадающего списка. Нажмите **OK** для сохранения настроек.

Примечание

Во время установки следует закрыть веб-страницу.

Нажмите **Add Fingerprint** («Добавить отпечатки пальцев») и приложите палец к модулю отпечатков пальцев, чтобы добавить отпечаток пальца.

Нажмите **Add** («Добавить») для сохранения настроек.

Нажмите **Save and Continue** («Сохранить и продолжить»), чтобы сохранить настройки и продолжить добавление следующего пользователя.

Примечание

Плагин для добавления карты или отпечатка пальца через USB доступен только для Windows.

Добавление PIN-кода

Перед настройкой PIN-кода необходимо уточнить, через что настроен PIN-код: через устройство или через платформу. Если PIN-код настроен через устройство, его можно создать или изменить через устройство или веб-интерфейс, его нельзя настроить через другие платформы. Если PIN-код настроен через платформу, его можно создать или изменить через платформу, его нельзя настроить через устройство или веб-интерфейс.

Убедитесь, что для режима PIN-кода выбран параметр **Device-Set Personal PIN** («Персональный PIN-код, настраиваемый через устройство») в разделе ***Set Password Mode*** («Установка режима пароля»). Нажмите **PIN Mode** («Режим PIN-кода») на странице, чтобы перейти к настройке.

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Установите PIN-код. Или нажмите **Auto Generate** («Автоматическая генерация»), чтобы автоматически сгенерировать PIN-код.

Нажмите **Add** («Добавить») для сохранения настроек.

Нажмите **Save and Continue** («Сохранить и продолжить»), чтобы сохранить настройки и продолжить добавление следующего пользователя.

Настройки параметров аутентификации

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Выберите тип аутентификации.

Нажмите **Add** («Добавить») для сохранения настроек.

Нажмите **Save and Continue** («Сохранить и продолжить»), чтобы сохранить настройки и продолжить добавление следующего пользователя.

Управление разрешениями

Перед началом

- Устройство уже добавлено. Подробная информация представлена в разделе ***Управление устройством***.
- Управление точкой доступа уже завершено. Подробная информация представлена в разделе ***Управление точкой доступа***.
- Управление правами доступа уже завершено. Подробная информация представлена в разделе ***Управление разрешениями***.

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Установите параметры разрешений.

Тип разрешения

По группе разрешений

Нажмите **Allocate** («Назначить») и выберите добавленное разрешение доступа. Для каждого человека будут указаны отмеченные разрешения доступа. Чтобы добавить разрешения, нажмите кнопку **Add Access Permission** («Добавить разрешения»). Подробная информация представлена в разделе ***Управление разрешениями***. Нажмите **ОК**.

По точке доступа

Нажмите **Allocate** («Назначить») и выберите расписание доступа. Нажмите **Add** («Добавить»), чтобы добавить точки доступа. Для каждого пользователя будут указаны права доступа к точке доступа в соответствии с расписанием доступа. Нажмите **ОК**.

Увеличенная продолжительность открытия двери

Дверь, связанная с пользователем, закроется по истечении заданного времени. Для установки увеличенной длительности открытого состояния двери перейдите в раздел ***Настройка параметров двери***. Нажмите **Door Parameters** («Параметры двери»), чтобы перейти на страницу конфигурации.

Нажмите **Add** («Добавить») для сохранения настроек.

Нажмите **Save and Configure** («Сохранить и настроить»), чтобы сохранить настройки и продолжить добавление следующего пользователя.

Изменение / Удаление / Поиск пользователя

Нажмите **Person Management** («Управление сотрудниками / посетителями»), чтобы перейти на страницу.

Выберите человека и нажмите , чтобы отредактировать информацию о нем.

Выберите человека и нажмите , чтобы удалить информацию о нем.

Выберите несколько человек, нажмите **Delete** («Удалить»), чтобы удалить пользователей в пакетном режиме.

Нажмите **Import** («Импорт») или **Export** («Экспорт»).

Нажмите **Clear All** («Очистить все»), чтобы удалить всю информацию о сотрудниках.

Нажмите или , чтобы переключить способ просмотра.

Введите идентификатор сотрудника, выберите состояние учетных данных и нажмите **Filter** («Фильтр») для поиска. Нажмите **Reset** («Сбросить»), чтобы сбросить все условия.

Выберите **Show Sub Organization** («Показать дополнительные организации»), чтобы отобразить всех сотрудников в подразделениях.

8.6 Управление устройством

8.6.1 Поиск недобавленных устройств

Система может автоматически искать недобавленные модули, которые были подключены к контроллеру доступа.

Нажмите **Device Management** → **Search Not Added Device** («Управление устройством → Поиск недобавленного устройства»). Найденные недобавленные модули отобразятся в списке на странице.

Нажмите + на панели действий, чтобы добавить модуль к контроллеру доступа.

8.6.2 Добавление модуля доступа

Добавьте модуль доступа вручную.

Перед началом

Убедитесь, что область была добавлена. Подробная информация представлена в разделе ***Управление областью***.

Шаги

1. Нажмите **Device Management** («Управление устройством») для перехода на страницу настроек.

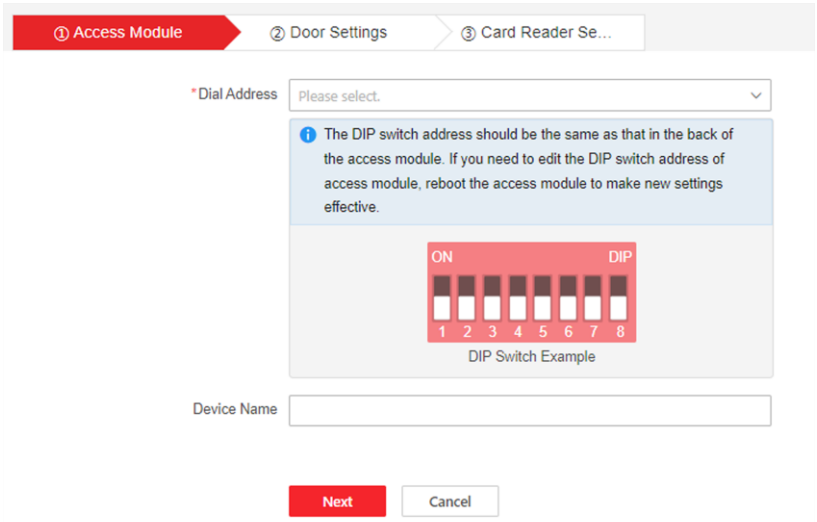


Рисунок 8-8 Добавление модуля доступа

2. Выберите модуль ввода-вывода.
3. Выберите адрес набора номера модуля доступа и установите DIP-переключатель модуля доступа в соответствии с показанным на рисунке.

Примечание

После добавления или изменения адреса набора номера модуля доступа необходимо перезагрузить модуль доступа, чтобы изменения вступили в силу.

4. Задайте параметры двери и нажмите **Next** («Далее»).

Выберите дверь модуля доступа

В зависимости от того, какая дверь фактически контролируется модулем доступа, выберите **1** или **2**.

Наименование двери

Введите название двери, связанное с модулем доступа.

Область

Выберите область из выпадающего списка. Если привязанная область еще не создана, нажмите **Add Area** («Добавить область»), чтобы создать ее.

Длительность открытого состояния

Установите время срабатывания после разблокировки привязанной двери. Если дверь не будет открыта в течение установленного времени, она автоматически заблокируется. Диапазон значений можно установить от 1 до 255 с.

Состояние дверного замка

Можно установить состояние дверного замка: **Remain Open** («Оставить открытым») или **Remain Closed** («Оставить закрытым»). По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).

Тип кнопки выхода

В обычных условиях дверь остается открытой (за исключением особых случаев).

Увеличение длительности открытого состояния

Для пожилых людей или людей с ограниченной подвижностью можно установить параметр **Extended Open Duration** («Увеличенная длительность открытого состояния»), чтобы отложить время открытия двери после считывания карты магнитным датчиком.

5. Настройте параметры считывателя карт, связанного с модулем доступа.

Выберите дверь модуля доступа

В зависимости от того, какая дверь фактически контролируется модулем доступа, выберите **1** или **2**.

Выбор считывателя карт

Выберите вход или выход в зависимости от фактического расположения считывателя карт.

Имя считывателя карт

Введите название считывателя карт.

Описание считывателя карт

Просмотрите описание считывателя карт.

QR-код

Если считыватель карт поддерживает функцию аутентификации по QR-коду, эту функцию можно включить, после чего считыватель карт сможет осуществлять аутентификацию посредством QR-кода.

Включить Bluetooth

Если считыватель карт поддерживает функцию открытия двери через Bluetooth, эту функцию можно включить, после чего дверь можно будет открыть через Bluetooth на считывателе карт.

Конфигурация плана аутентификации

Настройте план аутентификации для различных типов аутентификации. Можно установить разные типы аутентификации на разные периоды времени.
Выберите тип аутентификации (можно выбрать несколько) и настройте необходимый период времени на шкале ниже, в течение которого можно выполнять выбранный тип аутентификации.
Нажмите **Clear** («Очистить») и выберите период времени, нарисованный на временной шкале, чтобы очистить план.
Нажмите ··· → **Clear All** («Очистить все»), чтобы очистить все периоды времени.

6. Настройте параметры тревожного входа и выхода.

Тревожный вход

Установите номер и название тревожного входа.

Тревожный выход

Установите номер и название тревожного выхода. Можно установить **Alarm Duration** («Длительность тревоги»).

Непрерывная тревога

Устройство тревожного выхода будет постоянно находиться в состоянии тревоги.

Настройка длительности тревоги

Необходимо установить длительность. Устройство тревожного выхода будет находиться в состоянии тревоги в течение заданного времени.

Примечание

Диапазон: от 1 до 5999 секунд.

7. Нажмите **ОК**.
8. Нажмите **Import** («Импорт»), чтобы импортировать модуль доступа.
9. Опционально. Другие операции

Значок	Описание
	Можно редактировать модуль доступа.
	Можно удалить модуль доступа.
	Можно перезапустить модуль доступа.
	Можно восстановить модуль доступа до заводских настроек.
	Можно обновить модуль доступа. Выберите локальный пакет обновления для обновления.

8.6.3 Добавление модуля ввода-вывода

Добавьте модуль ввода-вывода вручную.

Шаги

Примечание

Доступно до 26 модулей ввода-вывода.

1. Нажмите **Device Management** («Управление устройством») для перехода на страницу настроек.
2. Выберите модуль ввода-вывода.
3. Выберите адрес набора номера модуля ввода-вывода и установите DIP-переключатель модуля ввода-вывода в соответствии с показанным на рисунке.

Примечание

После добавления или изменения адреса набора номера модуля ввода-вывода необходимо перезагрузить модуль ввода-вывода, чтобы изменения вступили в силу.

4. Настройте параметры тревожного входа и выхода.

Тревожный вход

Установите номер и название тревожного входа.

Тревожный выход

Установите номер и название тревожного выхода. Можно установить **Alarm Duration** («Длительность тревоги»).

Непрерывная тревога

Устройство тревожного выхода будет постоянно находиться в состоянии тревоги.

Настройка длительности тревоги

Необходимо установить длительность. Устройство тревожного выхода будет находиться в состоянии тревоги в течение заданного времени.

Примечание

Диапазон: от 1 до 5999 секунд.

5. Нажмите **ОК**.

6. Опционально. Другие операции

Значок	Описание
	Можно отредактировать модуль ввода-вывода.
	Можно удалить модуль ввода-вывода.
	Можно перезапустить модуль ввода-вывода.
	Можно обновить модуль ввода-вывода. Выберите локальный пакет обновления для обновления.

8.6.4 Управление областью

После создания области можно добавить в нее точки контроля доступа, чтобы управлять ими в разделе.

Шаги

1. Нажмите **Device Management** → **Area Management** («Управление устройством → Управление областью»).
2. Нажмите **+** в левой части страницы, выберите главную область и задайте имя области.
3. Нажмите **Save** («Сохранить»).
   Добавленная область будет отображаться в выбранной главной области.
4. Опционально. изменение / удаление
   – Выберите область и нажмите , чтобы отредактировать информацию о ней.
   Выберите несколько пользователей и нажмите **Delete** («Удалить»), чтобы удалить информацию о сотрудниках в пакетном режиме.
   Нажмите **Clear All** («Очистить все»), чтобы удалить информацию обо всех сотрудниках.
   – Выберите область и нажмите , чтобы удалить информацию об области.

8.7 Система и обслуживание

8.7.1 Отображение информации об устройстве

Просмотрите название устройства, язык, модель, серийный номер, версию, количество интерфейсов входа, количество интерфейсов выхода, RS-485, тревожный вход, тревожный выход, емкость устройства и т. д.

Нажмите **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Basic Information** («Система и обслуживание → Конфигурация системы → Система → Настройки системы → Основная информация»), чтобы перейти на соответствующую страницу.

Можно просмотреть название устройства, язык, модель, серийный номер, версию, RS-485, тревожный вход, тревожный выход, емкость устройства и т. д.

8.7.2 Настройка времени

Установите часовой пояс, режим синхронизации, адрес сервера, порт NTP и интервал.

Нажмите **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Time Settings** («Система и обслуживание → Конфигурация системы → Система → Настройки системы → Настройка времени»).

Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Режим синхронизации времени

NTP

Необходимо задать IP-адрес NTP-сервера, номер порта и интервал.

Вручную

По умолчанию время устройства должно быть синхронизировано вручную. Можно установить время устройства вручную или нажать **Sync. with Computer Time** («Синхронизировать со временем компьютера»), чтобы синхронизировать время устройства со временем компьютера.

IP-адрес сервера / Порт NTP / Интервал

Можно установить IP-адрес сервера, порт NTP и интервал.

8.7.3 Настройка параметров перехода на летнее время

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Time Settings** («Система и обслуживание → Конфигурация системы → Система → Настройки системы → Настройка времени»).
2. Включите переход на летнее время.
3. Настройте время перехода на летнее время, время окончания и смещения.
4. Нажмите **Save** («Сохранить») для сохранения настроек.

8.7.4 Изменение пароля администратора

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **System** → **User Management** («Система и обслуживание → Конфигурация системы → Система → Управление пользователем»).

2. Нажмите .
3. Введите старый пароль и создайте новый пароль.
4. Подтвердите новый пароль.
5. Нажмите **Save** («Сохранить»).

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопаснее.
Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг и / или конечного пользователя.

8.7.5 Настройки безопасности учетной записи

Можно изменить контрольные вопросы и ответы или адрес электронной почты для устройства. Если после изменения настроек вы забыли пароль устройства, необходимо ответить на новые вопросы или использовать новый адрес электронной почты для сброса пароля устройства.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **Account Security Settings** («Система и обслуживание → Конфигурация системы → Система → Управление пользователем → Настройки безопасности учетной записи»).
2. Установите контрольные вопросы и адрес электронной почты.
3. Введите пароль устройства и нажмите **OK** для подтверждения изменений.

8.7.6 Просмотр пользователей в сети

Можно просмотреть пользователей в сети.

Нажмите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **Online Users** («Система и обслуживание → Конфигурация системы → Система → Управление пользователем → Онлайн пользователи»).

Можно просмотреть информацию о пользователях в сети, включая имя, тип, IP-адрес и время работы. Для обновления нажмите кнопку **Refresh** («Обновить»).

8.7.7 Просмотр лицензии на ПО с открытым исходным кодом в веб-интерфейсе ПК

На главной странице веб-интерфейса устройства нажмите → **Open Source Software Statement** («Лицензия на ПО с открытым исходным кодом»), чтобы просмотреть лицензию устройства.

8.7.8 Просмотр информации о постановке на охрану / снятии с охраны

Просмотр информации о постановке устройства на охрану и IP-адреса постановки на охрану.

Перейдите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **Arming/Disarming Information** («Система и обслуживание → Конфигурация системы → Система → Управление пользователями → Информация о постановке на охрану / снятии с охраны»).

Можно просмотреть информацию о постановке на охрану/снятии с охраны. Для обновления нажмите кнопку **Refresh** («Обновить»).

8.7.9 Настройка сетевых параметров

Настройка основных сетевых параметров

Нажмите **Configuration → Network → Network Settings → TCP/IP** («Настройки → Сеть → Настройки сети → TCP / IP»).

Задайте параметры и нажмите **Save** («Сохранить») для сохранения настроек.

Тип NIC

Выберите тип NIC из выпадающего списка.

DHCP

При выключении функции необходимо настроить адрес IPv4, маску подсети IPv4, шлюз IPv4 по умолчанию, режим IPv6, адрес IPv6, длину префикса подсети IPv6, шлюз IPv6 по умолчанию, MAC-адрес и MTU.

При включении функции система автоматически назначит адрес IPv4, маску подсети IPv4, шлюз IPv4 по умолчанию, режим IPv6, адрес IPv6, длину префикса подсети IPv6 и шлюз IPv6 по умолчанию.

DNS-сервер

Установите предпочтительный DNS-сервер и альтернативный DNS-сервер в соответствии с фактическими потребностями.

Настройка параметров Wi-Fi

Задайте параметры Wi-Fi для беспроводного подключения устройства.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **Wi-Fi** («Система и обслуживание → Конфигурация системы → Сеть → Настройки сети → Wi-Fi»).
2. Нажмите **Wi-Fi** («Wi-Fi»).
3. Выберите Wi-Fi
   – Нажмите и введите пароль Wi-Fi для подключения.
   – Нажмите **Add** («Добавить») и введите имя, пароль и тип шифрования Wi-Fi. Нажмите **Connect** («Подключить»). Когда Wi-Fi подключен, нажмите **ОК**.
4. Опционально. Настройте параметры WLAN.
   1) Настройте IP-адрес, маску подсети и шлюз по умолчанию. Или включите DHCP, и система автоматически задаст IP-адрес, маску подсети и по умолчанию шлюз.
5. Нажмите **Save** («Сохранить»).

Точка доступа устройства

После включения точки доступа на устройстве можно использовать свой телефон для подключения к ней и ее настройки.

Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **Device Hotspot** («Система и обслуживание → Конфигурация системы → Сеть → Настройки сети → Точка доступа устройства»).

Нажмите **Enable Device Hotspot** («Включить точку доступа устройства»), чтобы включить функцию и просмотреть имя точки доступа устройства.

Нажмите **Save** («Сохранить»).

Чтобы включить точку доступа, выполните следующие действия.

1. Подключитесь к точке доступа устройства с помощью мобильного телефона, введя пароль точки доступа. Откроется страница активации.

Примечание

- Если всплывающее окно не появилось автоматически. Введите IP-адрес устройства по умолчанию или введите www.acsvis.com в браузере, чтобы перейти на страницу активации.
- Для неактивных устройств имя точки доступа устройства — AP_Serial Number, а пароль точки доступа — серийный номер устройства.

- По умолчанию устройство находится в режиме точки доступа. Режим точки доступа будет отключен через 30 минут. Удерживайте кнопку 5 в течение 10 секунд, чтобы снова войти в режим точки доступа.
- После активации устройства пароль точки доступа будет изменен на пароль активации устройства.

2. Создайте новый пароль (пароль администратора) и подтвердите его.

Примечание

Символы, содержащие admin и nimda, не могут быть использованы для активации пароля.

Предостережение

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

3. Нажмите **Activate** («Активировать»).

4. Нажмите **Configuration → Communication Settings → Wi-Fi** («Настройки → Настройка связи → Wi-Fi») и подключитесь к сети Wi-Fi. Или измените IP-адрес через мобильный веб-интерфейс, веб-интерфейс ПК и клиентское программное обеспечение. Изменение IP-адреса устройства. IP-адрес можно редактировать с помощью инструмента SADP, ПК и клиентского программного обеспечения.

Настройка параметров порта

Установите параметры HTTP, HTTPS, прослушивания HTTP, RTSP, HTTPS и порта сервера.

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **HTTP(S)** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба → HTTP(S)»).

HTTP

Через этот порт веб-интерфейс получает доступ к устройству. Например, если **HTTP Port** («Порт HTTP») изменен на 81, необходимо ввести ***http://192.168.1.64:81*** для входа в веб-интерфейс.

HTTPS

Задайте HTTPS для доступа к браузеру. Для доступа необходим сертификат.

Прослушивание HTTP

Устройство может отправлять информацию о тревоге по IP-адресу или доменному имени по протоколу HTTP или HTTPS. Настраивайте IP-адрес или доменное имя, URL-адрес, порт, и протокол информации о тревоге.

Примечание

Для получения информации о тревоге IP-адрес или доменное имя должны поддерживать протокол HTTP или HTTPS.

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **WebSocket(s)** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба → WebSocket(s)»).

Просмотрите порт WebSocket и WebSockets.

Порт 53

DNS.

Порт 80

Порт связи HTTP (доступ к устройству через HTTP).

Порт 443

Порт связи HTTPPS (доступ к устройству через HTTPS).

Порт 7681

Порт связи WebSocket (используется для отправки событий при управлении устройством через веб-интерфейс).

Порт 7682

Порт связи WebSockets (используется для отправки событий при управлении устройством через веб-интерфейс).

Настройка параметров ISUP

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **ISUP** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → ISUP»).

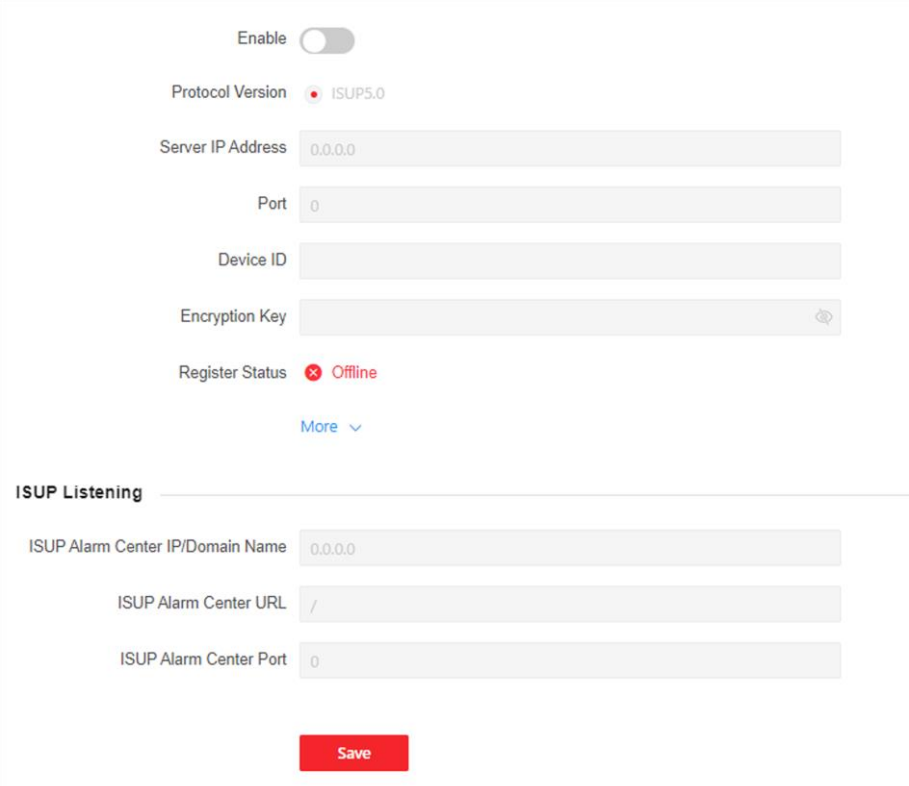


Рисунок 8-9 Настройка параметров ISUP

2. Нажмите **Enable** («Включить»).
3. Просмотр версии ISUP, установка IP-адреса сервера, порта, идентификатора устройства, ключа шифрования и просмотр состояния ISUP.
4. Опционально. Нажмите **More** («Больше»), чтобы настроить приоритет сетевого подключения.
   1) Включите **WLAN** или **Wired Network** («Проводная сеть») в соответствии с требованиями проекта.
   1) Удерживайте и перемещайте ☰, чтобы настроить приоритет доступа.
5. Настройте параметры прослушивания ISUP, в том числе IP-адрес устройства / доменное имя центра тревог ISUP, URL-адрес центра тревог ISUP и порт центра тревог ISUP.
6. Нажмите **Save** («Сохранить»).

Доступ к платформе

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **Hik-Connect** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → Hik-Connect») для перехода на страницу настроек.

Примечание

Guarding Vision является приложением для мобильных устройств. С помощью приложения можно просматривать видео в реальном времени с устройства, получать тревожные уведомления и т. д.

2. Поставьте **Enable** («Включить») для включения соответствующей функции.
3. Опционально. Выберите **Custom** («Пользовательская настройка»), чтобы настроить адрес сервера самостоятельно.
4. Введите проверочный код.
5. Опционально. Просмотрите состояние регистрации. Нажмите **Refresh** («Обновить»), чтобы обновить состояние.
6. Опционально. Нажмите **More** («Больше»), чтобы настроить приоритет сетевого подключения.
   1) Включите **WLAN** или **Wired Network** («Проводная сеть») в соответствии с требованиями проекта.
   1) Удерживайте и перемещайте ☰, чтобы настроить приоритет доступа.
7. Нажмите **View** («Просмотр»), чтобы просмотреть QR-код устройства. Сканируйте QR-код, чтобы выполнить привязку учетной записи.

Примечание

От 8 до 32 букв (от a до z, от A до Z) или цифр (от 0 до 9), с учетом регистра. Рекомендуется использовать комбинацию не менее 8 букв или цифр.

8. Нажмите **Save** («Сохранить») для сохранения настроек.
9. Опционально. Нажмите **Refresh** («Обновить»), чтобы обновить состояние привязки.
10. Нажмите **Save** («Сохранить»).

8.7.10 Настройки событий

Установите параметры привязки событий и тревожного выхода.

Привязка события

Настройте действия привязки для событий.

Шаги

1. Нажмите **Access Control** → **Parameters Settings** → **Linkage Settings** («Контроль доступа → Настройки параметров → Настройки привязки»), чтобы перейти на соответствующую страницу.
2. Нажмите ＋
3. Настройте источник события.
   – При выборе **Event Linkage** («Привязка события»), как **Linkage Type** («Тип привязки»), из выпадающего списка выберите тип события.

– При выборе **Card Linkage** («Привязка карты»), как **Linkage Type** («Тип привязки»), введите № карты и выберите считыватель карт.
– При выборе **Link Employee ID** («Привязка ID сотрудника»), как **Linkage Type** («Тип привязки»), введите ID сотрудника и выберите считыватель карт.

4. Настройте действие привязки.

Бипер привязанного контроллера доступа

Включите **Linked Access Controller Buzzing** («Бипер привязанного контроллера доступа») и выберите **Start Buzzing** («Включить бипер») или **Stop Buzzing** («Выключить бипер») для целевого события.

Привязка считывателя карт

Включите **Card Reader Linkage** («Привязка считывателя карт») и нажмите **Add** («Добавить»), чтобы выбрать считыватель карт, который будет издавать звуковой сигнал. Нажмите **Save** («Сохранить»).
Настройте действие бипера для считывателя карт.
Нажмите , чтобы удалить отдельный считыватель карт. Выберите считыватели карт и нажмите **Delete** («Удалить»), чтобы удалить их в пакетном режиме. Нажмите **Batch Configure** («Конфигурация в пакетном режиме»), чтобы настроить все считыватели карт в списке.

Привязка двери

Включите **Door Linkage** («Привязка двери») и нажмите **Add** («Добавить»), чтобы выбрать считыватель карт, который будет издавать звуковой сигнал. Нажмите **Save** («Сохранить»).
Настройте действие точки доступа.
Нажмите , чтобы удалить отдельный считыватель карт. Выберите считыватели карт и нажмите **Delete** («Удалить»), чтобы удалить их в пакетном режиме.

Привязанный тревожный выход

Если тип подключения в источнике событий – **Card Linkage** («Привязка карты»), то при включении **Linked Alarm Output** («Привязанный тревожный выход») можно настроить **Triggering Times Configuration** («Конфигурация времени запуска»), **Triggering Times (Enable)** («Время запуска (включено)») и **Triggering Times (Disable)** («Время запуска (выключено)»).
Если для **Triggering Times (Enable)** («Время запуска (включено)») и **Triggering Times (Disable)** («Время запуска (выключено)») установить значение 3, то для отключения тревоги, когда тревожный выход из списка будет находиться в открытом состоянии, достаточно трижды поднести карту, настроенную в источнике событий. Если тревожный выход отключен, можно трижды поднести карту к устройству, чтобы активировать тревогу.
Настройте тревожный выход. Нажмите **Add** («Добавить»), выберите тревожные выходы из списка и нажмите **Save** («Сохранить»).
Нажмите , чтобы установить продолжительность тревоги. Нажмите **Save** («Сохранить»).

Примечание

После завершения настройки конфигурация того же выхода, связанного с другими действиями, также будет изменена.

Непрерывная тревога

Устройство тревожного выхода будет постоянно находиться в состоянии тревоги.

Настройка длительности тревоги

Необходимо установить длительность. Устройство тревожного выхода будет находиться в состоянии тревоги в течение заданного времени.

Примечание

Диапазон: от 0 до 5999 с.

5. Нажмите **Save** («Сохранить»).
6. Чтобы сопоставить режим связи модуля с другими модулями, нажмите кнопку **Copy To** («Копировать в»), выберите или введите имя устройства и нажмите кнопку **ОК**.

Alarm Output Settings («Настройка тревожного выхода»)

Установите параметры тревожного выхода устройства.

Нажмите **System and Maintenance** → **System Configuration** → **Event** → **Alarm Settings** → **Alarm Output** («Система и обслуживание → Конфигурация системы → Событие → Настройки тревоги → Тревожный выход») для перехода на страницу настроек.

Выберите точку доступа из списка слева. Выберите номер тревожного выхода. Введите название тревожного выхода и установите продолжительность тревоги. Нажмите **Save** («Сохранить»). Нажмите **Copy to** («Копировать в...»), чтобы скопировать параметры.

Непрерывная тревога

Устройство тревожного выхода будет постоянно находиться в состоянии тревоги.

Настройка длительности тревоги

Необходимо установить длительность. Устройство тревожного выхода будет находиться в состоянии тревоги в течение заданного времени.

Примечание

Диапазон: от 1 до 5999 секунд.

Настройки тревожного входа

Установите параметры тревожного входа устройства.

Нажмите **System and Maintenance** → **System Configuration** → **Event** → **Alarm Settings** → **Alarm Input** («Система и обслуживание → Конфигурация системы → Событие → Настройки тревоги → Тревожный вход») для перехода на страницу настроек.

Выберите устройство, задайте номер и название. Нажмите **Save** («Сохранить»).

8.7.11 Конфигурация доступа

Можно установить параметры RS-485, Wiegand и хоста.

Настройка параметров RS-485

Можно установить параметры RS-485, параметры периферийных устройств, адрес, скорость передачи и т. д.

Нажмите **System and Maintenance** → **System Configuration** → **Access Configuration** → **RS-485** («Система и обслуживание → Конфигурация системы → Конфигурация доступа → RS-485») для перехода на страницу настроек.

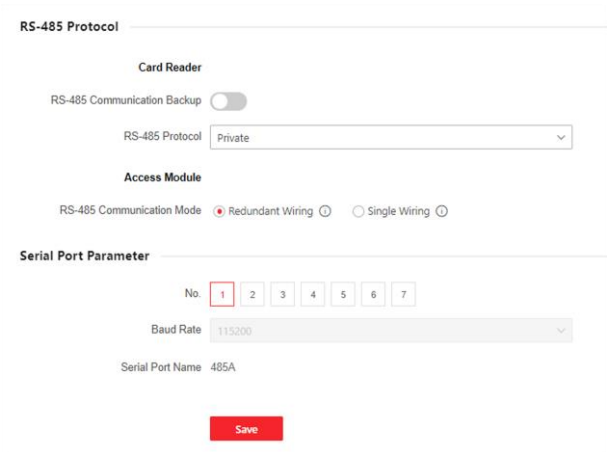


Рисунок 8-10 Настройка параметров RS-485

Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Резервная линия связи RS-485

При включении этой функции будет использоваться резервная линия при передаче данных считывателем по протоколу RS-485.

Протокол RS-485

Выберите протокол RS-485 из выпадающего списка.

Режим связи RS-485

Различные способы подключения

Когда контроллер доступа подключается к терминалу (RS-485A/RS-485B/RS-485C/RS-485D) модуля доступа, RS-485A и RS-485B представляют собой пару, использующую резервную проводку, а RS-485C и RS-485D представляют собой другую пару. При отключении одного из каналов контроллер доступа может взаимодействовать с другим каналом. К контроллеру доступа можно подключить не более 32 модулей доступа.

Подключение по одному кабелю

RS-485A и RS-485D – это терминалы связи модуля доступа. Терминал RS-485E на контроллере доступа может быть подключен к терминалам RS-485A и RS-485D через один провод для передачи данных. К контроллеру доступа можно подключить не более 62 модулей доступа.

Номер

Выберите номер RS-485.

Скорость передачи данных

Скорость передачи при обмене данными по протоколу RS-485.

Название серийного интерфейса

Просмотр названия серийного интерфейса.

Настройка параметров интерфейса Wiegand

Можно настроить направление передачи данных интерфейса Wiegand.

Шаги

Примечание

Некоторые модели устройств не поддерживают данную функцию. Настройка параметров зависит от фактического функционала устройства.

1. Нажмите **System and Maintenance** → **System Configuration** → **Access Configuration** → **Wiegand Settings** («Система и обслуживание → Конфигурация системы → Конфигурация доступа → Настройки Wiegand»).
2. Выберите точку доступа из списка слева.
3. Настройка параметров интерфейса Wiegand.

Номер

Выберите номер Wiegand для настройки параметров.

Wiegand

Выберите, чтобы включить функцию Wiegand считывателя карт.

Направление Wiegand

По умолчанию установлено значение **Input** («Вход»).

Режим Wiegand

Выберите режим Wiegand, и считыватель карт сможет взаимодействовать с контроллером по протоколу Wiegand 26/34 или другому протоколу.
Нажмите **Auto Recognize** («Автоматическое распознавание»), введите номер карты для распознавания в режиме Wiegand. Введите номер карты и нажмите **Start to Recognize** («Начать распознавание»). Поднесите карту к соответствующему считывателю карт. Система отобразит режим Wiegand. Нажмите **OK**.
Если выбран режим **Custom** («Пользовательская настройка»), необходимо установить пользовательские параметры Wiegand. Нажмите **Custom Wiegand Settings** («Пользовательские настройки Wiegand») и задайте имя, тип четности, общую длину и правило Wiegand. Нажмите **OK**.

Сопоставление считывателя карт Wiegand

Выберите дверь и направление считывателя карт, к которым относится считыватель карт Wiegand.

4. Нажмите **Save** («Сохранить») для сохранения настроек.

Примечание

При изменении и сохранении параметров периферийных устройств произойдет автоматическая перезагрузка устройства.

Настройки магнитоконтактного датчика

Установите состояние открытия и закрытия двери с магнитоконтактным датчиком в соответствии с фактическим способом подключения.

Перед началом

Контроллер доступа подключен к магнитоконтактному датчику двери.

Шаги

1. Нажмите **System and Maintenance** → **Maintenance** → **Device Access** → **Host Parameter** («Система и обслуживание → Обслуживание → Доступ к устройству → Параметр хоста») для перехода на страницу настроек.
2. Выберите состояние магнитоконтактного датчика.

Открыто (по умолчанию)

По умолчанию магнитоконтактный датчик открыт. Контроллер доступа подключен к магнитоконтактному датчику через NO.

Дверь закрыта

По умолчанию магнитоконтактный датчик находится в замкнутом состоянии. Контроллер доступа подключен к магнитоконтактному датчику с помощью NC.

8.7.12 Настройки параметров карты

Настройка параметров безопасности карты

Нажмите **System and Maintenance** → **System Configuration** → **Card Settings** → **Card Type** («Система и обслуживание → Конфигурация системы → Настройки параметров карты → Тип карты») для перехода на страницу настроек.

Настройте параметры и нажмите **Save** («Сохранить»).

Включение распознавания NFC-карты

Чтобы на мобильный телефон не передавались данные контроля доступа, можно включить распознавание NFC-карты и повысить уровень безопасности данных.

Включение распознавания M1-карты

При активации распознавания M1-карты становится доступна аутентификация путем считывания M1-карты.

Шифрование M1-карты

Сектор

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации. Активируйте функцию и установите сектор шифрования. По умолчанию сектор 13 зашифрован. Рекомендуется зашифровать сектор 13.

Активация распознавания EM-карты

При активации распознавания EM-карты становится доступна аутентификация путем считывания EM-карты.

Примечание

Если периферийный считыватель карт поддерживает распознавание EM-карты, то также поддерживается функция включения / выключения распознавания EM-карты.

Активация распознавания DESfire-карты

Устройство может считывать данные с DESfire-карты.

Чтение DESFire-карт

Устройство может считывать информацию с карты DESFire.

Активация распознавания FeliCa-карты

Устройство может считывать данные с FeliCa-карты.

Настройка параметров аутентификации № карты

Настройте параметры карты при аутентификации через карту на устройстве.

Перейдите **System and Maintenance** → **System Configuration** → **Card Settings** → **Card No. Auth. Settings** («Система и обслуживание → Конфигурация системы → Настройки карты → Настройки аутентификации по номеру карты»).

Выберите режим аутентификации карты, задайте обратный номер карты и нажмите **Save** («Сохранить»).

Полный номер карты

Будет прочитан полный номер карты.

3 байта

Устройство будет считывает карту по протоколу Wiegand 26 (считывание трех байтов).

4 байта

Устройство будет считывает карту по протоколу Wiegand 34 (считывание четырех байтов).

Включение считывания номера карты в обратной последовательности

После включения функции номер карты будет считываться в обратной последовательности.

8.7.13 ТО и безопасность

Настройка параметров конфиденциальности

Задайте тип хранения событий, параметры загрузки и хранения изображений, а также параметры очистки изображений.

Перейдите в **System and Maintenance** → **System Configuration** → **Security** → **Privacy Settings** («Система и обслуживание → Конфигурация системы → Безопасность → Настройки конфиденциальности»).

Выберите способ удаления события. Можно выбрать **Delete Old Events Periodically** («Периодическое удаление старых событий»), **Delete Old Events by Specified Time** («Удаление старых событий в заданное время») или **Overwriting** («Перезапись»). Нажмите **Save** («Сохранить») после настройки.

Периодическое удаление старых событий

Переместите курсор мыши или введите число, чтобы установить период для удаления событий. Все события будут удалены в соответствии с настроенным периодом времени.

Удаление старых событий в заданное время

Установите время, и все события будут удалены в указанное время.

Перезапись

Самые ранние 5 % событий будут удалены, когда система обнаружит, что сохраненные события занимают более 95 % заполненного пространства.

Настройка режима пароля

Перед настройкой паролей необходимо уточнить, через что настроен PIN-код: через устройство или через платформу. Если PIN-код настроен через устройство, его можно создать или изменить через устройство или веб-интерфейс, его нельзя настроить через другие платформы. Если PIN-код настроен через платформу, его можно создать или изменить через платформу, его нельзя настроить через устройство или веб-интерфейс.

Шаги

1. Перейдите в **System and Maintenance** → **System Configuration** → **Security** → **PIN Mode** («Система и обслуживание → Конфигурация системы → Безопасность → Режим PIN-кода»).

   Персональный PIN-код, настраиваемый через устройство

   PIN-код можно создать или изменить через устройство или веб-интерфейс, его нельзя настроить через другие платформы.

   Персональный PIN-код, настраиваемый через платформу

   PIN-код можно создать или изменить через платформу, его нельзя настроить через устройство или веб-интерфейс.
2. Нажмите **Save** («Сохранить»).

Обновление и техническое обслуживание

Можно выполнить перезагрузку устройства, восстановление параметров устройства и обновление версии устройства.

Перезагрузка устройства

Нажмите **System and Maintenance → Maintenance → Host** («Система и обслуживание → Обслуживание → Хост»).

Нажмите **Restart** («Перезагрузка») для перезагрузки устройства.

Перезагрузка дополнительного устройства

Нажмите **System and Maintenance → Maintenance → Sub-Device** («Система и обслуживание → Обслуживание → Дополнительное устройство»).

Настройте устройство и нажмите **Restart** («Перезагрузить»).

Обновление

Нажмите **System and Maintenance → Maintenance → Upgrade** («Система и обслуживание → Обслуживание → Обновление»).

Выберите тип обновления из выпадающего списка. Нажмите и выберите файл обновления с локального ПК. Нажмите **Upgrade** («Обновить»), чтобы начать обновление.

Если устройство было подключено к Guarding Vision и сети, когда доступен новый установочный пакет Guarding Vision, нажмите **Upgrade** («Обновить») для обновления системы устройства.

Примечание

Не выключайте устройство во время обновления.

Обновление дополнительного устройства

Нажмите **System and Maintenance → Maintenance → Upgrade** («Система и обслуживание → Обслуживание → Обновление»).

Выберите тип обновления из выпадающего списка. Нажмите , выберите файл обновления с локального ПК и нажмите **Next** («Далее»). Нажмите **Upgrade** («Обновить»), чтобы начать обновление.

Восстановление параметров

Нажмите **System and Maintenance → Maintenance → Backup and Reset → Host** («Система и обслуживание → Техническое обслуживание → Резервное копирование и сброс → Хост»).

Восстановить все

Все параметры будут сброшены до заводских настроек. Перед первым входом в систему необходимо активировать устройство.

Восстановить

Настройки устройства будут восстановлены до настроек по умолчанию, за исключением IP-адреса устройства и информации о пользователе.

Восстановление параметров дополнительного устройства

Нажмите **System and Maintenance → Maintenance → Backup and Reset → Sub-Device** («Система и обслуживание → Техническое обслуживание → Резервное копирование и сброс → Дополнительное устройство»).

Выберите устройство и нажмите **Restore to Factory Settings** («Восстановление заводских настроек»).

Параметры импорта и экспорта

Нажмите **System and Maintenance → Maintenance → Backup and Reset** («Система и обслуживание → Техническое обслуживание → Резервное копирование и сброс»).

Экспорт

Нажмите **Export** («Экспорт») для экспорта параметров устройства.

Примечание

Можно импортировать экспортированные параметры устройства на другое устройство.

Импорт

Нажмите и выберите файлы для импорта. Нажмите **Import** («Импорт») для начала импорта файла настройки.

Отладка устройства

Можно настроить параметры отладки устройства.

Шаги

1. Нажмите **System and Maintenance → Maintenance → Device Debugging** («Система и обслуживание → Техническое обслуживание → Отладка устройства»).
2. Можно настроить следующие параметры.

Включить SSH

Чтобы повысить безопасность сети, отключите службу SSH. Данная настройка используется профессионалами только для отладки устройства. Нажмите **Debug** («Отладка») для отладки SSH.

Захват сетевого пакета

Можно настроить **Capture Packet Duration** («Длительность захвата пакета») и **Capture Packet Size** («Размер захвата пакета»), затем нажмите **Start** («Начать») для захвата.

Управление записями в журналах

Можно искать и просматривать журналы устройства.

Перейдите **System and Maintenance** → **Maintenance** → **Log** («Система и обслуживание → Обслуживание → Журнал»).

Установите основной и второстепенный тип журнала. Установите время начала и время окончания поиска и нажмите **Search** («Поиск»).

Результаты будут отображаться ниже, включая номер, время, основной тип, второстепенный тип, номер канала, информацию о локальном/удаленном пользователе, IP-адрес удаленного хоста и т. д.

Тестирование протокола через веб-интерфейс ПК

Выберите адрес протокола и введите протокол для тестирования. Можно выполнять отладку устройства в соответствии с заголовком ответа и полученным результатом.

Нажмите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Protocol Testing** («Система и обслуживание → Обслуживание → Отладка устройства → Тестирование протокола»).

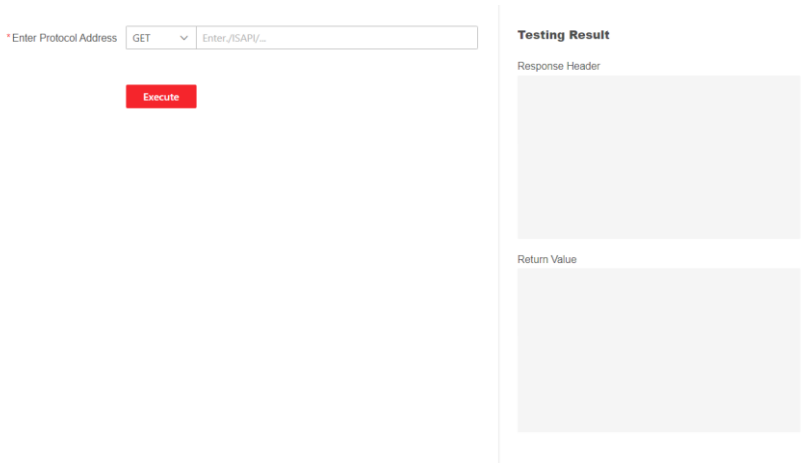


Рисунок 8-11 Тестирование протокола

Выберите адрес протокола и введите протокол. Нажмите **Execute** («Выполнить»).

Выполняйте отладку устройства в соответствии с заголовком ответа и полученным результатом.

Настройка сетевой диагностики

Введите IP-адрес устройства или доменное имя, чтобы выполнить настройку PING. Выполните отладку сети в соответствии с результатом PING.

Перейдите **Maintenance and Security → Maintenance → Network Diagnosis** («Техническое обслуживание и безопасность → Техническое обслуживание → Сетевая диагностика»).

Введите IP-адрес устройства для выполнения операции PING, выберите режим сетевого подключения, продолжительность PING и размер пакета данных PING (рекомендуется использовать параметры по умолчанию). Нажмите **Diagnose** («Диагностика»). Результат будет отображен в разделе **PING Result** («Результаты PING»).

Настройка службы проверки на проникновение в сеть

При развертывании устройства в локальной сети можно включить службу тестирования на проникновение для удаленного управления устройством.

Шаги

1. Нажмите **Configuration → Network → Network Service → Network Penetration Service** («Настройка → Сеть → Сетевая служба → Служба проверки на проникновение в сеть»).
2. Нажмите **Enable Penetration Service** («Включение службы проверки на проникновение»).
3. Введите **Server IP Address** («IP-адрес сервера») и **Server Port** («Порт сервера»).
4. Введите **User Name** («Имя пользователя») и **Password** («Пароль») для входа в систему.
5. Установите **Heartbeat Timeout** («Период цикла Heartbeat»). Диапазон: от 1 до 6000.
6. Нажмите **Save** («Сохранить»).

7. Можно просмотреть **Online Status** («Состояние онлайн»). Нажмите **Refresh** («Обновить»), чтобы просмотреть последнее состояние.

8.7.14 Управление сертификатами

Помогает управлять сертификатами сервера/клиента и сертификатом CA.

Примечание

Данная функция поддерживается только у определенных моделей устройств.

Создание и импорт сертификата HTTPS

Шаги

1. Перейдите в меню **Maintenance and Security → Security → Certificate Management** («Техническое обслуживание и безопасность → Безопасность → Управление сертификатами»).
2. В области **HTTPS Certificate** («Сертификат HTTPS») нажмите **Create Certificate Request** («Создать запрос сертификата»).
3. Введите информацию о сертификате и нажмите **Save** («Сохранить»).
   - Нажмите **View** («Просмотр»), и отобразится созданный сертификат.
   - Сертификат будет сохранен автоматически.
4. Загрузите сертификат и сохраните его в запрашиваемом файле на локальном компьютере.
5. Отправьте запрашиваемый файл в центр сертификации на подпись.
6. Импортируйте подписанный сертификат.
   1) В области **Import Key** («Ключ импорта») выберите сертификат из локального хранилища и нажмите **Import** («Импорт»).
   2) В области **Import Communication Certificate** («Импорт сертификата связи») выберите сертификат на локальном компьютере и нажмите **Import** («Импорт»).

Создание и импорт сертификата SYSLOG

Шаги

1. Перейдите в меню **Maintenance and Security → Security → Certificate Management** («Техническое обслуживание и безопасность → Безопасность → Управление сертификатами»).
2. В области **SYSLOG Certificate** («Сертификат SYSLOG») нажмите **Create Certificate Request** («Создать запрос сертификата»).
3. Введите информацию о сертификате и нажмите **Save** («Сохранить»).
   - Нажмите **View** («Просмотр»), и отобразится созданный сертификат.
   - Сертификат будет сохранен автоматически.
4. Загрузите сертификат и сохраните его в запрашиваемом файле на локальном компьютере.
5. Отправьте запрашиваемый файл в центр сертификации на подпись.

6. Импортируйте подписанный сертификат.
   1) В области **Import Key** («Ключ импорта») выберите сертификат из локального хранилища и нажмите **Import** («Импорт»).
   2) В области **Import Communication Certificate** («Импорт сертификата связи») выберите сертификат на локальном компьютере и нажмите **Import** («Импорт»).

Импорт сертификата CA

Перед началом

Заранее подготовьте сертификат CA.

Шаги

1. Перейдите в меню **Maintenance and Security → Security → Certificate Management** («Техническое обслуживание и безопасность → Безопасность → Управление сертификатами»).
2. Создайте идентификатор в области **CA Certificate ID** («Идентификатор сертификатов CA»).

Примечание

Идентификатор сертификата не может совпадать с идентификатором уже существующих сертификатов.

3. Загрузите файл сертификата с локального ПК.
4. Нажмите **Import** («Импорт»).

8.7.15 Разблокировка

Если карты заблокированы, можно нажать кнопку, чтобы разблокировать все карты.

Перейдите **System and Maintenance** → **Safe** → **Unlock** («Система и обслуживание → Безопасность → Разблокировка») и нажмите **Unlock** («Разблокировать»).

Раздел 9 Настройка устройства через мобильный веб-интерфейс

9.1 Вход в систему

В систему можно войти через мобильный интерфейс.

Примечание

- Некоторые модели поддерживают настройку Wi-Fi.
- Устройство должно быть активировано.
- Убедитесь, что устройство и смартфон находятся в одной сети Wi-Fi.

Введите IP-адрес устройства в адресной строке мобильного интерфейса и нажмите **Enter** («Ввод») для того, чтобы войти в систему.

Введите имя пользователя и пароль. Нажмите **Login** («Войти»).

9.2 Обзор

С помощью ярлыка можно просмотреть основную информацию, состояние двери, события в режиме реального времени, состояние устройства, состояние сети, а также настроить управление персоналом, управление устройством, поиск событий, параметры контроля доступа, параметры двери и т. д.

Описание функций:

Состояние двери

/ / /

Состояние двери: открыта / закрыта / оставить открытой / оставить закрытой. Можно нажать, чтобы выбрать состояние двери «открыта / закрыта / оставить открытой / оставить закрытой».

Ярлык быстрого доступа

С помощью ярлыка можно настроить управление пользователями, управление устройством, поиск событий, параметры контроля доступа, параметры двери и т. д.

Состояние сети

Можно просмотреть состояние подключения и регистрации в сети.

События в режиме реального времени

Можно просмотреть события в режиме реального времени.

Состояние устройства

Можно просмотреть состояние устройства.

9.3 Забыли пароль

Если вы забыли пароль для входа в систему, пароль можно поменять с помощью адреса электронной почты или контрольных вопросов.

На странице входа в систему нажмите **Forget Password** («Забыли пароль»).

Выберите **Verification Mode** («Режим проверки»).

Проверка по контрольным вопросам

Ответьте на контрольные вопросы.

Подтверждение по электронной почте

1. Экспортируйте QR-код и отправьте его на адрес сервера электронной почты во вложении.
2. Проверочный код будет отправлен на зарезервированный адрес электронной почты в течение 5 минут.
3. Введите проверочный код в поле проверочного кода для подтверждения идентификации.

Нажмите **Next** («Далее»), создайте новый пароль и подтвердите его.

9.4 Конфигурация

9.4.1 Отображение информации об устройстве

Просмотр имени устройства, языка, модели, серийного номера, версии, MAC-адреса, локального номера RS-485, номера тревожного входа, номера тревожного выхода, емкости устройства и т. д.

На главной странице нажмите → **System Settings** → **Basic Information** («Настройки системы → Основная информация»).

Просмотр имени устройства, языка, модели, серийного номера, версии, MAC-адреса, локального номера RS-485, номера тревожного входа, номера тревожного выхода, емкости устройства и т. д.

Нажмите **Save** («Сохранить»).

9.4.2 Настройки времени

Установите часовой пояс, режим синхронизации времени и отображаемое время.

Нажмите → **System Settings → Time Settings** («Настройки системы → Настройки времени») для перехода на соответствующую страницу.

Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Часовой пояс

Выберите часовой пояс, в котором находится устройство.

Синхронизация времени Режим

Вручную

По умолчанию время устройства должно быть синхронизировано вручную. Можно установить время устройства вручную.

NTP

Задайте IP-адрес NTP-сервера, номер порта и интервал.

9.4.3 Настройка параметров DST

Шаги

1. Нажмите → **System Settings → Time Settings** («Настройки системы → Настройки времени») для перехода на соответствующую страницу.

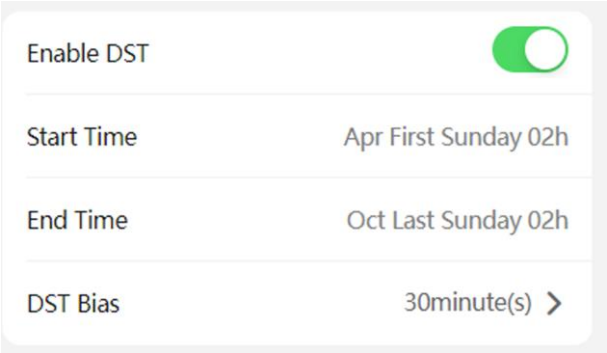


Рисунок 9-1 Переход на летнее время (DST)

2. Нажмите **Enable DST** («Включить переход на летнее время»).
3. Настройте время перехода на летнее время, время окончания и смещения.
4. Нажмите **Save** («Сохранить»).

9.4.4 Управление пользователями

Шаги

1. Нажмите → **User Management → User Management → admin** («Управление пользователями → Управление пользователями → Администратор»), чтобы перейти на соответствующую страницу.
2. Введите старый пароль и создайте новый пароль.
3. Подтвердите новый пароль.
4. Нажмите **Save** («Сохранить»).

Примечание

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя от 8 до 16 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопаснее.

9.4.5 Настройка сетевых параметров

Проводная сеть

Настройка проводной сети.

Нажмите → **Network Settings → TCP/IP** («Сетевые настройки → TCP / IP») для перехода на соответствующую страницу.

DHCP

При выключении функции необходимо настроить адрес IPv4, маску подсети IPv4, шлюз IPv4 по умолчанию, режим IPv6, адрес IPv6, длину префикса подсети IPv6, шлюз IPv6 по умолчанию, MAC-адрес и MTU.
При включении функции система автоматически назначит адрес IPv4, маску подсети IPv4, шлюз IPv4 по умолчанию, режим IPv6, адрес IPv6, длину префикса подсети IPv6 и шлюз IPv6 по умолчанию.

DNS-сервер

Установите предпочтительный DNS-сервер и альтернативный DNS-сервер в соответствии с фактическими потребностями.

Настройка параметров Wi-Fi

Задайте параметры Wi-Fi для беспроводного подключения устройства.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите → **Network Settings** → **Wi-Fi** («Настройки сети → Wi-Fi»), чтобы перейти на страницу настроек.
2. Включите **Wi-Fi**.

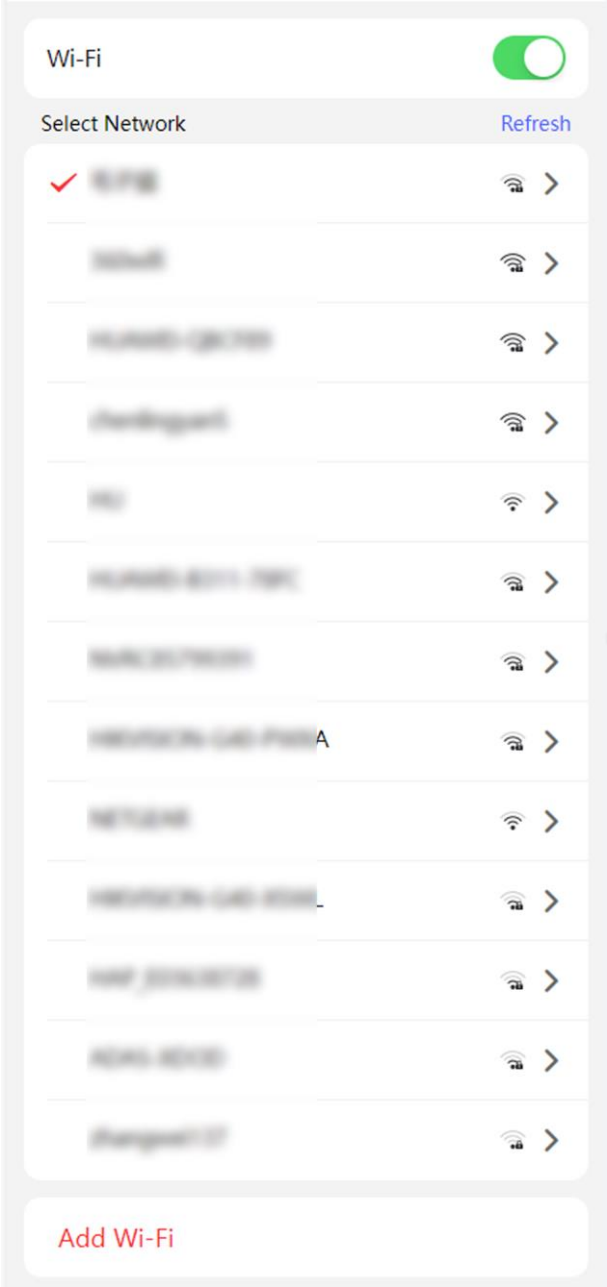


Рисунок 9-2 Wi-Fi

3. Добавьте Wi-Fi.
   1) Нажмите **Add Wi-Fi** («Добавить Wi-Fi»).
   2) Введите **Wi-Fi Name** («Имя Wi-Fi») и **Wi-Fi Password** («Пароль Wi-Fi») и выберите **Encryption Type** («Тип шифрования»).
   3) Нажмите **Save** («Сохранить»).
4. Выберите имя Wi-Fi и нажмите **Connect** («Подключиться»).
5. Введите пароль и нажмите **Save** («Сохранить»).

Настройка точки доступа устройства

Настройте точку доступа устройства, и мобильный телефон сможет подключиться к устройству для входа в мобильный браузер.

Шаги

1. Нажмите → **Network Settings** → **Device Hotspot** («Настройки сети → Точка доступа устройства»).
2. Можно включить точку доступа устройства и просмотреть имя точки доступа.

Примечание

По умолчанию именем точки доступа является серийный номер устройства.

3. Нажмите **Save** («Сохранить»).

Настройка параметров порта

Можно настроить HTTP, HTTPS и WebSocket(s) при доступе к устройству через сеть согласно текущим потребностям.

Нажмите → **Network Service** → **HTTP(S)** («Сетевая служба → HTTP(S)»), чтобы перейти на соответствующую страницу.

HTTP

Через этот порт веб-интерфейс получает доступ к устройству. Например, если **HTTP Port** («Порт HTTP») изменен на 81, необходимо ввести ***http://192.168.1.64:81*** для входа в веб-интерфейс.

HTTPS

Задайте HTTPS для доступа к браузеру. Для доступа необходим сертификат.

Нажмите → **Network Service** → **Websocket(s)** («Сетевая служба → Websocket(s)»), чтобы перейти на соответствующую страницу.

Можно просмотреть номер порта Websocket(s).

Доступ к платформе

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите → **Device Access** → **Guarding Vision** («Доступ устройств → Guarding Vision») для перехода на страницу настроек.

Примечание

Guarding Vision является приложением для мобильных устройств. С помощью приложения можно просматривать видео в реальном времени с устройства, получать тревожные уведомления и т. д.

2. Поставьте **Enable** («Включить») для включения соответствующей функции.
3. Можно включить **Custom** («Пользовательская настройка») для ввода адреса сервера.

Примечание

- От 6 до 12 букв (от a до z, от A до Z) или цифры (от 0 до 9), с учетом регистра. Рекомендуется использовать комбинацию не менее 8 букв или цифр.
- Код подтверждения не может быть ***123456*** или ***abcdef*** (без учета регистра).

4. Можно просмотреть **Network Connection Status** («Состояние сетевого подключения») и **Binding Status** («Состояние привязки»).
5. Можно настроить **Network Connection Priority** («Приоритет сетевого подключения»).
6. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Настройка параметров ISUP

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите → **Device Access** → **ISUP** («Доступ устройств → ISUP») для перехода на страницу настроек.
2. Включите **ISUP**.
3. Настройте версию ISUP, адрес сервера, порт, идентификатор устройства и код шифрования.

Примечание

Если выбрана версия 5.0, необходимо также установить ключ шифрования.

4. Можно просмотреть **Registration Status** («Состояние регистрации»).
5. Можно настроить **Network Connection Priority** («Приоритет сетевого подключения»).
6. Настройте параметры прослушивания ISUP, в том числе IP-адрес устройства / доменное имя центра тревог ISUP, URL-адрес центра тревог ISUP и порт центра тревог ISUP.
7. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Настройка службы проверки на проникновение в сеть

После развертывания устройства в локальной сети можно включить службу проверки на проникновение для удаленного управления устройством.

Шаги

1. Нажмите → **Device Access** → **Network Penetration Service** («Доступ к устройству → Служба проверки на проникновение в сеть») для перехода на страницу настроек.
2. Нажмите **Enable Penetration Service** («Включить службу проверки на проникновение»).
3. Установите **Server IP Address** («IP-адрес сервера») и **Server Port** («Порт сервера»). Создайте **User Name** («Имя пользователя») и **Password** («Пароль»)
4. Опционально. Можно настроить **Heartbeat Timeout** («Период цикла Heartbeat»). Диапазон значений: от 1 до 6000.
5. Опционально. Можно посмотреть состояние службы проверки на проникновение. Нажмите **Refresh** («Обновить»), чтобы обновить состояние.
6. Нажмите **Save** («Сохранить»).

Примечание

Служба проверки на проникновение будет автоматически отключена через 48 часов.

9.4.6 Настройки параметров тревоги

Настройки тревожного входа

Установите параметры тревожного входа устройства.

Нажмите → **Alarm Settings** → **Alarm Input** («Настройки тревоги → Тревожный вход»).

Выберите устройство, задайте название тревоги. Нажмите **Save** («Сохранить»).

Настройка тревожного выхода

Установите параметры тревожного выхода устройства.

Нажмите → **Alarm Settings** → **Alarm Output** («Настройки тревоги → Тревожный выход»).

Выберите устройство. Выберите номер тревожного выхода. Введите название тревожного выхода и установите продолжительность тревоги. Нажмите **Save** («Сохранить»).

Непрерывная тревога

Устройство тревожного выхода будет постоянно находиться в состоянии тревоги.

Настройка длительности тревоги

Необходимо установить длительность. Устройство тревожного выхода будет находиться в состоянии тревоги в течение заданного времени.

Примечание

Диапазон: от 1 до 5999 секунд.

9.4.7 Конфигурация доступа

Настройка параметров интерфейса Wiegand

Можно настроить направление передачи данных интерфейса Wiegand.

Шаги

Примечание

Некоторые модели устройств не поддерживают данную функцию. Настройка параметров зависит от фактического функционала устройства.

1. Нажмите → **Access Configuration** → **Wiegand Settings** («Настройки контроля доступа → Настройки Wiegand»).
2. Выберите точку доступа из списка.
3. Настройка параметров интерфейса Wiegand.

Номер

Выберите номер Wiegand для настройки параметров.

Wiegand

Выберите, чтобы включить функцию Wiegand считывателя карт.

Направление Wiegand

По умолчанию установлено значение **Input** («Вход»).

Режим Wiegand

Выберите режим Wiegand, и считыватель карт сможет взаимодействовать с контроллером по протоколу Wiegand 26/34 или другому протоколу.
Нажмите **Auto Recognize** («Автоматическое распознавание»), введите номер карты для распознавания в режиме Wiegand. Введите номер карты и нажмите **Start to Recognize** («Начать распознавание»). Поднесите карту к соответствующему считывателю карт. Система отобразит режим Wiegand. Нажмите **OK**.
Если выбран режим **Custom** («Пользовательская настройка»), необходимо установить пользовательские параметры Wiegand. Нажмите **Custom Wiegand Settings** («Пользовательские настройки Wiegand») и задайте имя, тип четности, общую длину и правило Wiegand. Нажмите **OK**.

Сопоставление считывателя карт Wiegand

Выберите дверь и направление считывателя карт, к которым относится считыватель карт Wiegand.

4. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Примечание

При изменении и сохранении параметров периферийных устройств произойдет автоматическая перезагрузка устройства.

Настройки магнитоконтактного датчика

Установите состояние открытия и закрытия двери с магнитоконтактным датчиком в соответствии с фактическим способом подключения.

Перед началом

Контроллер доступа подключен к магнитоконтактному датчику двери.

Шаги

1. Нажмите → **Access Configuration** → **Host Parameter** («Конфигурация доступа → Параметры хоста»), чтобы перейти на страницу настроек.
2. Выберите состояние магнитоконтактного датчика.

Шлагбаум открыт (по умолчанию)

По умолчанию магнитоконтактный датчик открыт. Контроллер доступа подключен к магнитоконтактному датчику двери с помощью NO.

Дверь закрыта

По умолчанию магнитоконтактный датчик находится в замкнутом состоянии. Контроллер доступа подключен к магнитоконтактному датчику с помощью NC.

9.4.8 Управление организацией и пользователями

Можно добавлять, редактировать, удалять и искать организации и пользователей через мобильный веб-интерфейс.

Шаги

1. Нажмите → **Person Management** («Управление пользователями») для перехода на страницу настроек.
2. Добавьте организацию.
   1) Нажмите **Add** («Добавить») и выберите **Add Organization** («Добавить организацию»).
   2) Введите **Organization Name** («Название организации»).
   3) Выберите **Upper-Level Organization** («Организация верхнего уровня»).
   4) Нажмите **Save** («Сохранить»).
3. Добавление пользователя.
   1) Нажмите **Add** («Добавить») и выберите **Add Person** («Добавить пользователя»).

2) Настройте следующие параметры.

ID сотрудника

Введите ID сотрудника. ID сотрудника не может быть 0 или превышать 32 символа. Он может состоять из букв верхнего / нижнего регистра и цифр.

Имя

Введите ваше имя. Имя поддерживает числа, буквы верхнего / нижнего регистра и символы. Рекомендуется вводить имя в пределах 32 символов.

Тип пользователя

Выберите **User Type** («Тип пользователя»).

Организация

Выберите организацию.

Тип разрешения / группа разрешений

Тип разрешения

По группе разрешений

Нажмите **Allocate** («Назначить») и выберите добавленное разрешение доступа. Для каждого человека будут указаны отмеченные разрешения доступа. Чтобы добавить разрешения, нажмите кнопку **Add Access Permission** («Добавить разрешения»). Подробная информация представлена в разделе Управление разрешениями. Нажмите **OK**.

По точке доступа

Нажмите Allocate («Назначить») и выберите расписание доступа. Нажмите **Add** («Добавить»), чтобы добавить точки доступа. Для каждого пользователя будут указаны права доступа к точке доступа в соответствии с расписанием доступа. Нажмите **OK**.

Отпечаток пальца

Добавьте отпечатки пальцев. Нажмите **Fingerprint** («Отпечаток пальца»), затем нажмите **+**, чтобы добавить отпечатки пальцев с помощью модуля считывания отпечатков пальцев.

Карта

Добавление карты. Нажмите **Card** («Карта»), затем нажмите «+», введите номер карты и выберите тип карты.

PIN-код

Просмотр и изменение PIN-кода.

Примечание

Перед настройкой PIN-кода необходимо уточнить, через что настроен PIN-код: через устройство или через платформу. Если PIN-код настроен через устройство, его можно создать или изменить через устройство или веб-интерфейс, его нельзя настроить через другие платформы. Если PIN-код настроен через платформу, его можно создать или изменить через платформу, его нельзя настроить через устройство или веб-интерфейс.

3) Нажмите **Save** («Сохранить»).

4. Нажмите **More** («Дополнительно»).
   1) Выберите **Gender** («Пол»).
   2) Настройте следующие параметры.

Пользователь с длительным разрешением

Настройте долгосрочное разрешение для пользователя.

Дата выдачи / Дата истечения срока

Установите дату выдачи и дату истечения срока действия разрешения пользователя.

Увеличение длительности открытого состояния

После включения режима увеличенной длительности открытого состояния двери необходимо настроить время ее закрытия в разделе параметров двери.

Тип аутентификации

Выберите тип аутентификации.

5. Нажмите **Save** («Сохранить»).

9.4.9 Управление устройством

Автоматический поиск устройства

Система может автоматически искать недобавленные модули, которые были подключены к контроллеру доступа.

Нажмите → **Device Management** → **Add** → **Auto Search Device** («Управление устройством → Добавить → Автоматический поиск устройства»). Найденные недобавленные модули отобразятся в списке на странице.

Добавление модуля доступа

Добавьте модуль доступа вручную.

Шаги

1. Нажмите → **Device Management** → **Add** → **Add Access Module** («Управление устройством → Добавить → Добавить модуль доступа»), чтобы перейти на страницу настроек.

2. Выберите адрес набора номера модуля доступа и установите DIP-переключатель модуля доступа в соответствии с показанным на рисунке. Задайте **Device Name** («Название устройства»). Нажмите **Next** («Далее»).

Примечание

После добавления или изменения адреса набора номера модуля доступа необходимо перезагрузить модуль доступа, чтобы изменения вступили в силу.

3. Выберите дверь, задайте параметры двери и нажмите **Next** («Далее»).

Выберите дверь модуля доступа

Выберите дверь в зависимости от того, какая фактически контролируется модулем доступа.

Наименование двери

Введите название двери, связанное с модулем доступа.

Область

Выберите область из выпадающего списка. Если привязанная область еще не создана, нажмите **Add Area** («Добавить область»), чтобы создать ее.

Длительность открытого состояния

Установите время срабатывания после разблокировки привязанной двери. Если дверь не будет открыта в течение установленного времени, она автоматически заблокируется. Диапазон значений можно установить от 1 до 255 с.

Тип магнитоконтактного датчика двери

Можно установить параметры магнитоконтактного датчика как **Remain Open** («Оставить открытым») или **Remain Closed** («Оставить закрытым»). По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).

Тип кнопки выхода

В обычных условиях дверь остается открытой (за исключением особых случаев).

Увеличение длительности открытого состояния

Для пожилых людей или людей с ограниченной подвижностью можно установить параметр **Extended Open Duration** («Увеличенная длительность открытого состояния»), чтобы отложить время открытия двери после считывания карты магнитным датчиком.

4. Выберите точку доступа, задайте параметры считывателя карт, связанные с модулем, и нажмите **Next** («Далее»).

Выберите точку доступа

В соответствии с дверью, фактически управляемой модулем доступа, выберите точку доступа.

Выбор считывателя карт

Выберите вход или выход в зависимости от фактического расположения считывателя карт.

Имя считывателя карт

Введите название считывателя карт.

Описание считывателя карт

Просмотрите описание считывателя карт.

QR-код

Если считыватель карт поддерживает функцию аутентификации по QR-коду, эту функцию можно включить, после чего считыватель карт сможет осуществлять аутентификацию посредством QR-кода.

Включить Bluetooth

Если считыватель карт поддерживает функцию открытия двери через Bluetooth, эту функцию можно включить, после чего дверь можно будет открыть через Bluetooth на считывателе карт.

5. Задайте параметры тревожного входа и выхода.

Тревожный вход

Выберите номер тревожного входа и задайте имя.

Тревожный выход

Выберите номер тревожного выхода и задайте имя. Можно установить **Alarm Duration** («Длительность тревоги»).

Непрерывная тревога

Устройство тревожного выхода будет постоянно находиться в состоянии тревоги.

Настройка длительности тревоги

Необходимо установить длительность. Устройство тревожного выхода будет находиться в состоянии тревоги в течение заданного времени.

Примечание

Диапазон: от 1 до 5999 секунд.

6. Нажмите **Save** («Сохранить»).

Добавление модуля ввода-вывода

Добавьте модуль ввода-вывода вручную.

Шаги

1. Нажмите → **Device Management** → **Add** → **Add I/O Module** («Управление устройством → Добавить → Добавить модуль ввода-вывода»), чтобы перейти на страницу настроек.

2. Выберите адрес набора номера модуля и установите DIP-переключатель модуля в соответствии с показанным на рисунке. Задайте **Device Name** («Название устройства»). Нажмите **Next** («Далее»).

Примечание

После добавления или изменения адреса набора номера модуля необходимо перезагрузить модуль, чтобы изменения вступили в силу.

3. Задайте параметры тревожного входа и выхода.

Тревожный вход

Выберите номер тревожного входа и задайте имя.

Тревожный выход

Выберите номер тревожного выхода и задайте имя. Можно установить **Alarm Duration** («Длительность тревоги»).

Непрерывная тревога

Устройство тревожного выхода будет постоянно находиться в состоянии тревоги.

Настройка длительности тревоги

Необходимо установить длительность. Устройство тревожного выхода будет находиться в состоянии тревоги в течение заданного времени.

Примечание

Диапазон: от 1 до 5999 с.

4. Нажмите **Save** («Сохранить»).

9.4.10 Настройка параметров контроля доступа

Настройка параметров двери

Нажмите → **Access Control** → **Door Parameters** («Контроль доступа → Параметры двери»).

Выберите дверь и измените параметры двери. Нажмите **Save** («Сохранить»), чтобы сохранить настройки. Нажмите **Save and Sync. to All** («Сохранить и синхронизировать со всеми устройствами»).

Наименование двери

Можно задать имя двери.

Область

Выберите область.

Длительность открытого состояния

Укажите длительность открытого состояния двери. Дверь будет заблокирована, если движение отсутствует в течение установленного времени.

Пороговое значение тревоги тайм-аута открытой двери

Тревога сработает, если дверь не будет закрыта в течение заданного периода времени.

Тип кнопки выхода

Можно установить параметры кнопки выхода как **Remain Open** («Оставить открытым») или **Remain Closed** («Оставить закрытым»). По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).

Дверь остается открытой после авторизации первого сотрудника (мин)

Установите продолжительность открытия двери после авторизации первого сотрудника. После авторизации первого пользователя несколько других пользователей получат доступ к дверям и разрешения на другие действия.

Суперпароль

Пользователь может открыть дверь с помощью суперпароля.

Примечание

Суперпароль должен отличаться от кода принуждения. Содержит от 4 до 8 цифр.

Настройка параметров аутентификации

Настройка параметров аутентификации.

Шаги

1. Нажмите → **Access Control** → **Authentication Settings** («Контроль доступа → Настройки аутентификации»).
2. Выберите соответствующий считыватель карт и отредактируйте параметры аутентификации.

Считыватель карт

Выберите считыватель карт для настройки.

Тип считывателя карт/описание считывателя карт

Просмотр описания считывателя карт. Доступно только для чтения.

Аутентификация

В выпадающем списке выберите режим аутентификации в соответствии с потребностями.

Интервал аутентификации

Можно установить интервал аутентификации одного и того же сотрудника во время аутентификации. Один сотрудник может пройти аутентификацию только один раз в заданный интервал. Вторая аутентификация будет невозможна.

Запуск тревоги при достижении максимального количества неудачных попыток считывания карты

Можно включить функцию сообщения о тревоге при достижении максимального количества неудачных попыток считывания карты.

Блокировка при превышении лимита / макс. кол-ва неудачных попыток считывания карты

Можно включить функцию сообщения о тревоге при достижении установленного максимального количества неудачных попыток считывания карты.

QR-код

Включите функцию, и считыватель карт сможет распознавать QR-код для аутентификации.

Примечание

Функция должна поддерживаться считывателем карт.

Включить Bluetooth

Включите функцию Bluetooth, чтобы использовать ее на считывателе карт (например, для открытия двери).

Название устройства / Мощность передачи

Измените название считывателя карт и его мощность передачи.

Открытие двери с помощью Bluetooth

Включите функцию, чтобы открывать дверь через Bluetooth с помощью приложения. Перед использованием функции необходимо добавить устройство в приложение.

Расширенные настройки

Включить устройство с функцией аутентификации

Включить функцию аутентификации.

Связь с контроллером

Если устройство контроля доступа не может подключиться к считывателю карт в течение установленного времени, считыватель карт отключится автоматически.

Максимальный интервал времени при вводе пароля

Если при вводе пароля в устройство для считывания карт интервал между нажатием двух цифр больше установленного значения, цифры, которые пользователь нажал до этого, будут автоматически удалены.

Включение тревоги тампера

Включите детектор саботажа на считывателе карт.

Правильная полярность светодиода / Ошибочная полярность светодиода / Полярность бипера

Настройте **OK LED Polarity** («Полярность светодиода при нормальном состоянии») / **Error LED Polarity** («Полярность светодиода при ошибке») / **Buzzer Polarity** («Полярность бипера») устройства контроля доступа в соответствии с параметрами считывателя карт. Как правило, устройство получает настройки по умолчанию.

3. Нажмите **Save** («Сохранить»). Нажмите **Save and Sync. to All** («Сохранить и синхронизировать со всеми устройствами»).

Интеллектуальные настройки

Настройка интеллектуальных параметров.

Параметры отпечатков пальцев

Нажмите → **Smart** → **Fingerprint Parameters** («Интеллектуальные функции → Параметры отпечатков пальцев»).

Распознавание отпечатков пальцев

Включите **Fingerprint Recognition** («Распознавание отпечатков пальцев»).

Уровень безопасности отпечатков пальцев

Можно настроить уровень безопасности отпечатков пальцев. Чем выше настроенный уровень безопасности, тем ниже вероятность ошибочного предоставления доступа (FAR). Чем выше настроенный уровень безопасности, тем ниже вероятность ошибочного отказа в доступе (FRR).

Настройка параметров конфиденциальности

Настройте параметры хранения.

Нажмите → **Access Control** → **Privacy Settings** («Контроль доступа → Настройки конфиденциальности»).

Настройки хранения событий

Периодическое удаление старых событий

Введите число, чтобы установить период для удаления событий. Все события будут удалены в соответствии с настроенным периодом времени.

Удаление старых событий в заданное время

Установите время, и все события будут удалены в указанное время.

Перезапись

Самые ранние 5 % событий будут удалены, когда система обнаружит, что сохраненные события занимают более 95 % заполненного пространства.

Режим пароля

Перед настройкой паролей необходимо уточнить, через что настроен PIN-код: через устройство или через платформу. Если PIN-код настроен через устройство, его можно создать или изменить через устройство или веб-интерфейс, его нельзя настроить через другие платформы. Если PIN-код настроен через платформу, его можно создать или изменить через платформу, его нельзя настроить через устройство или веб-интерфейс.

Шаги

1. Нажмите → **Access Control** → **Privacy Settings** → **PIN Mode** («Контроль доступа → Настройки конфиденциальности → Режим PIN-кода»).

   Персональный PIN-код, настраиваемый через устройство

   PIN-код можно создать или изменить через устройство или веб-интерфейс, его нельзя настроить через другие платформы.

   Персональный PIN-код, настраиваемый через платформу

   PIN-код можно создать или изменить через платформу, его нельзя настроить через устройство или веб-интерфейс.
2. Нажмите **Save** («Сохранить»).

Настройка параметров безопасности карты

Нажмите → **Access Control** → **Card Settings** («Контроль доступа → Настройки карты»), чтобы перейти на страницу конфигурации.

Настройте параметры и нажмите **Save** («Сохранить»).

Включение распознавания NFC-карты

Чтобы на мобильный телефон не передавались данные контроля доступа, можно включить распознавание NFC-карты и повысить уровень безопасности данных.

Включение шифрования NFC-защиты

При включении этой функции считыватель карт может распознавать только NFC-код, сгенерированный Guarding Vision.

Включение распознавания M1-карты

При активации распознавания M1-карты становится доступна аутентификация путем считывания M1-карты.

Шифрование M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

Сектор

Активируйте функцию и установите сектор шифрования. По умолчанию сектор 13 зашифрован. Рекомендуется зашифровать сектор 13.

Активация распознавания EM-карты

При активации распознавания EM-карты становится доступна аутентификация путем считывания EM-карты.

Примечание

EM-карта поддерживается, если к устройству подключен периферийный считыватель карт, поддерживающий распознавание EM-карты.

Активация распознавания DESfire-карты

Устройство может считывать данные с DESfire-карты.

Активация распознавания FeliCa-карты

Устройство может считывать данные с FeliCa-карты.

Режим аутентификации карты

Выберите режим аутентификации карты.

Включение считывания номера карты в обратной последовательности

После включения функции номер карты будет считываться в обратной последовательности.

9.4.11 Поиск событий

Нажмите → **Event Search** («Поиск событий») для перехода на соответствующую страницу.

Введите условия поиска и нажмите **Search** («Поиск»).

Примечание

Поддерживает поиск по имени до 32 символов.

9.4.12 Обновление и техническое обслуживание

Можно выполнить перезагрузку устройства, восстановление параметров устройства и обновление версии устройства.

Просмотр рекомендаций по обращению

Нажмите → **Maintenance** → **Restart** («Техническое обслуживание → Перезагрузка»).

Можно просмотреть записи об исключениях в элементах и ознакомиться с рекомендациями по их обработке.

Перезагрузка устройства

Нажмите → **Maintenance** → **Restart** («Техническое обслуживание → Перезагрузка»).

Нажмите **Restart** («Перезагрузить»), чтобы перезагрузить устройство.

Обновление

Нажмите → **Maintenance** → **Upgrade** («Техническое обслуживание → Обновление»).

Нажмите **Upgrade** («Обновить»), чтобы обновить устройство.

Примечание

Не выключайте устройство во время обновления.

Восстановление параметров

Нажмите → **Maintenance** → **Default** («Техническое обслуживание → Параметры по умолчанию»).

Восстановить

Настройки устройства будут восстановлены до настроек по умолчанию, за исключением IP-адреса устройства и информации о пользователе.

Восстановить все настройки

Все параметры будут сброшены до заводских настроек. Перед первым входом в систему необходимо активировать устройство.

Отладка устройства

Нажмите → **Maintenance** → **Device Debugging** («Техническое обслуживание → Отладка устройства»).

Можно включить **SSH** для отладки.

Просмотр информации журнала

Нажмите → **Maintenance** → **Log** («Техническое обслуживание → Журнал»).

Укажите тип и время записи в журнале, а затем нажмите **Search** («Поиск»), чтобы выполнить поиск по записям.

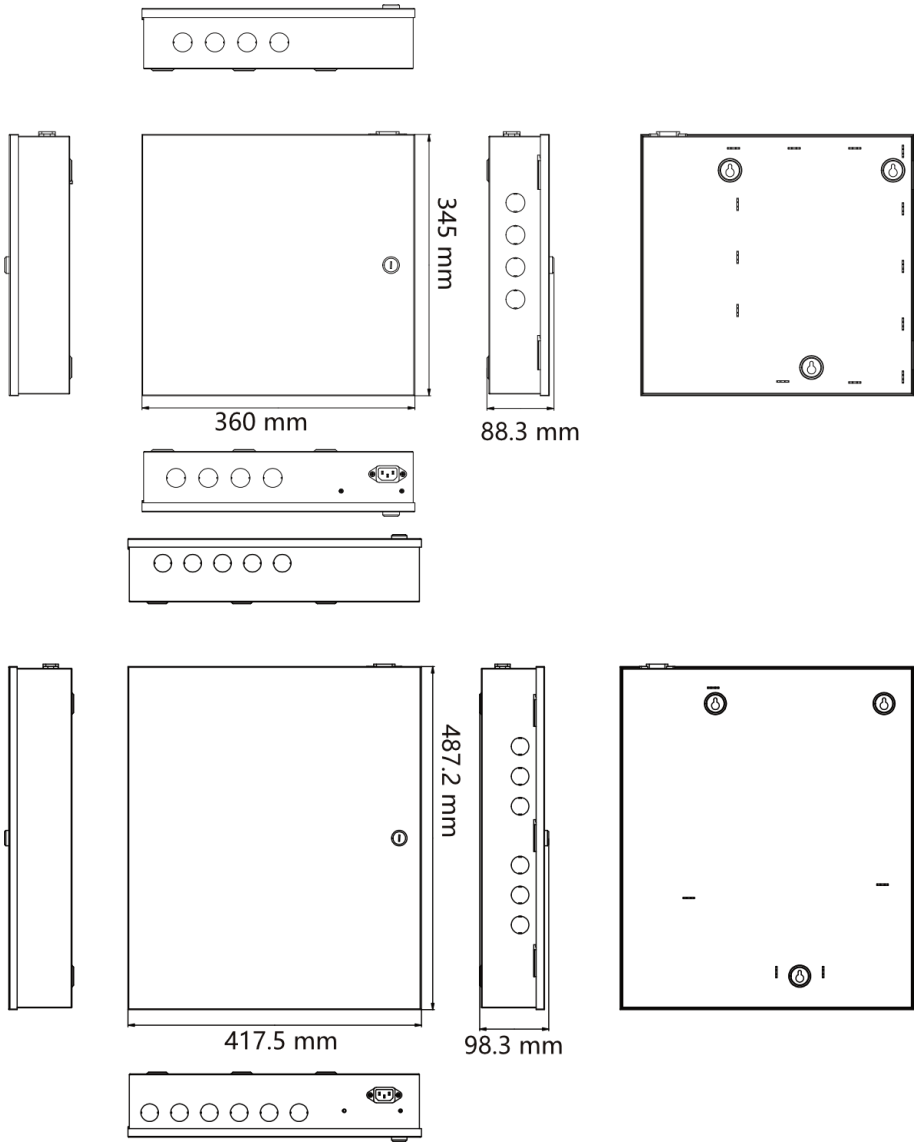
9.4.13 Просмотр руководства пользователя

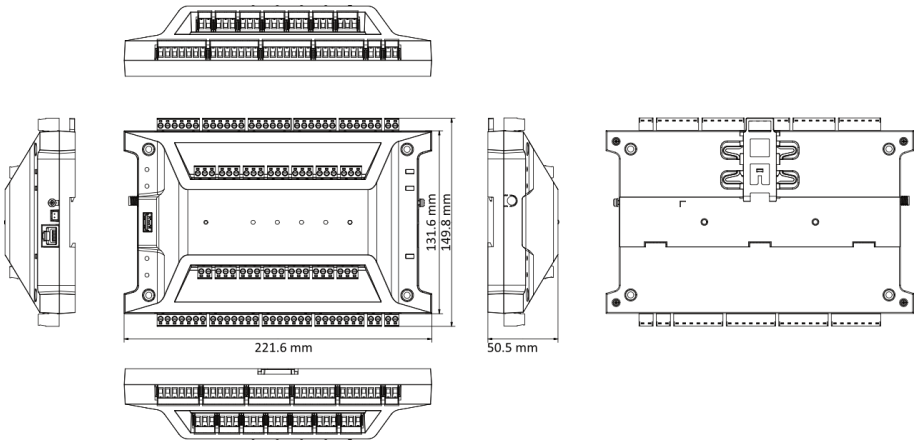
Нажмите → **View User Manual** («Просмотр руководства пользователя»). Можно сканировать QR-код с помощью мобильного телефона для получения подробной информации.

9.4.14 Просмотр лицензии на ПО с открытым исходным кодом

Нажмите → **Open Source Software Statement** («Лицензия на ПО с открытым исходным кодом»), чтобы просмотреть лицензию.

A. Размеры




131.6 mm
149.8 mm
221.6 mm
50.5 mm