Турникет с тремя штангами серии DS-K3G200(L)X

Правовая информация

О руководстве

Руководство 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. Последнюю версию настоящего документа можно найти на веб-сайте (***https:// www.hikvision.com/***).
Используйте этот документ под руководством профессионалов, обученных работе с продуктом.

Торговые марки

HIKVISION и другие торговые марки Hikvision и логотипы являются интеллектуальной собственностью Hikvision в различных юрисдикциях.
Другие 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. HIKVISION НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, КАСАТЕЛЬНО УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ. ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА НЕСЕТ ПОЛЬЗОВАТЕЛЬ.
HIKVISION 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 HIKVISION БЫЛО ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.
ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ; HIKVISION НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, HIKVISION ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.
ВЫ ОБЯЗУЕТЕСЬ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В СООТВЕТСТВИИ С ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, А ТАКЖЕ НЕСЕТЕ ПОЛНУЮ ОТВЕТСТВЕННОСТЬ ЗА ЕГО СОБЛЮДЕНИЕ. В ЧАСТНОСТИ, ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ДАННОГО ПРОДУКТА ТАКИМ ОБРАЗОМ, ЧТОБЫ НЕ НАРУШАТЬ ПРАВА ТРЕТЬИХ ЛИЦ, ВКЛЮЧАЯ ПРАВА НА ПУБЛИЧНОСТЬ, ПРАВА НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ, ЗАЩИТУ ДАННЫХ И ДРУГИЕ ПРАВА КАСАТЕЛЬНО НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ.

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.

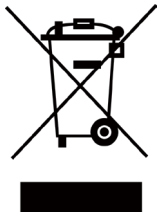
Защита данных

Во время использования устройства личные данные будут собираться, храниться и обрабатываться. При разработке устройств Hikvision 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.

Регулирующая информация

Соответствие стандартам ЕС

Данный продукт и (если применимо) поставляемые принадлежности отмечены знаком «CE» и, следовательно, согласованы с европейскими стандартами, перечисленными под директивой 2014/30/EC EMC, директивой 2014/53/EC RE, директивой 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 содержит батарею, 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 предупреждений может привести к тяжелым 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.

⚠ Предупреждение:

- 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 для технического обслуживания необходимо открыть верхние крышки и включить устройство, то:
  1. Отключите кулер, чтобы оператор не получил травму.
  2. Не прикасайтесь к оголенным компонентам под высоким напряжением.
  3. После технического обслуживания проверьте правильность последовательности подключений коммутатора.
- 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 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.)

⚠ Предостережение:

- В некоторых случаях нержавеющая сталь может подвергаться действию коррозии. Чистить и ухаживать за устройством необходимо чистящим средством для нержавеющей стали. Устройство необходимо чистить каждый месяц.
- Не бросайте устройство и не подвергайте его ударам или 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.
- Продукты с биометрическим распознаванием не на 100 % применимы для защиты от подделки биометрических данных. Используйте несколько режимов аутентификации, если требуется более высокий уровень безопасности.
- Во время перезагрузки устройства запрещено находиться в проходе турникета.

- Если при замене батареи используют батарею несоответствующего типа, существует риск взрыва. Использованные батареи необходимо утилизировать в соответствии с инструкциями.
- Устройство необходимо устанавливать на бетонную поверхность или на другие поверхности, не подвергаемые воспламенению.
- Необходимо подключить провод защитного заземления оборудования к проводу защитного заземления установки.

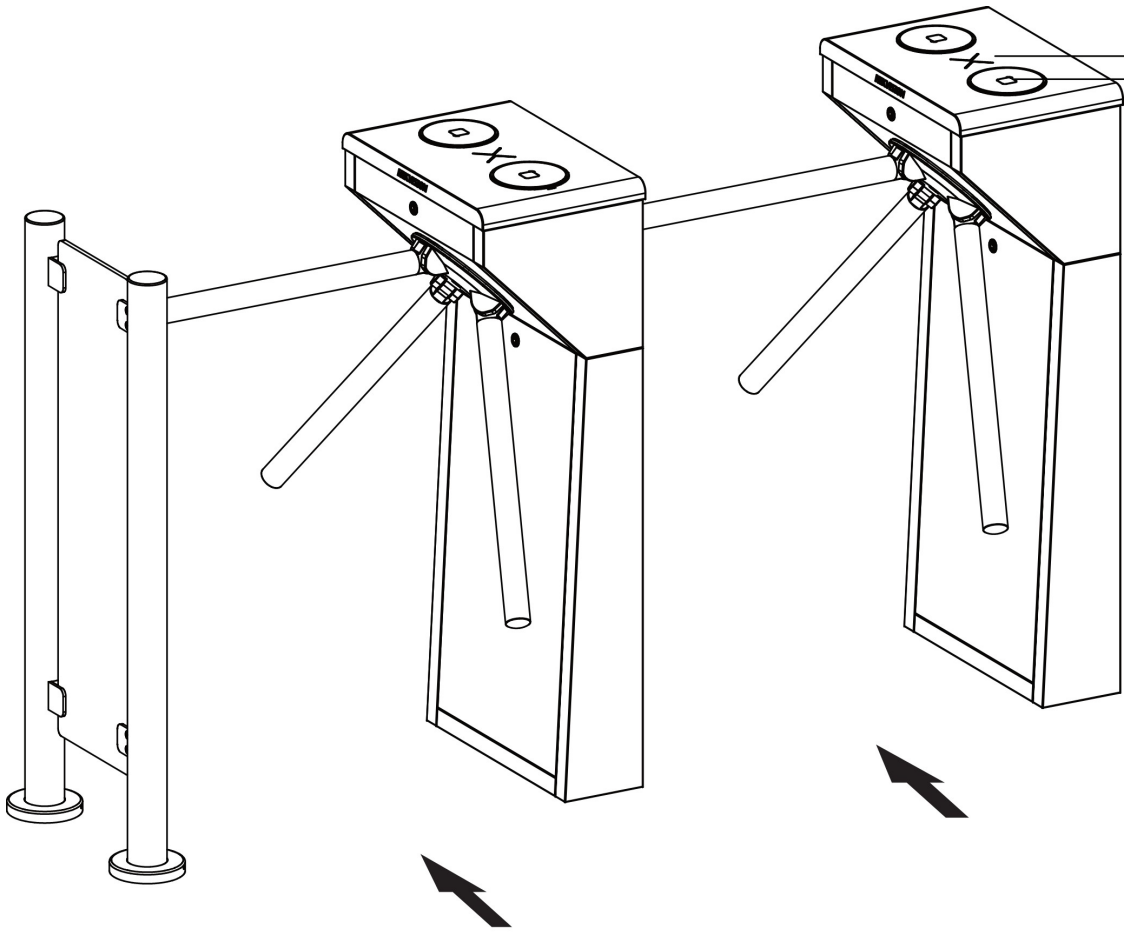
Доступные модели

Наименование продукта	Модель
Турникет с тремя штангами	DS-K3G200(L)X

Содержание

Раздел 1 Представление продукта

1.1 Представление



Entrance

Английский язык	Русский язык
Entrance	Вход

Турникет можно использовать в составе СКУД с аутентификацией при входе / выходе по картам, лицу или QR-коду. Турникет широко используется в парках аттракционов, в офисах, на строительных площадках, в жилых домах и т. д.

1.2 Основные характеристики

- Двунаправленный проход (вход / выход).
- Удаленный контроль и управление через HCP.
- Использование LED-индикатора высокой яркости для отображения состояния «Открыто» / «Закрыто» и направления движения через турникет, за исключением типа «Pg».

- Пропуск при сигнале пожарной тревоги: при запуске тревоги турникет автоматически открывается для аварийной эвакуации.
- Настройка через веб-интерфейс ПК.
- Поддержка протокола ISAPI для интеграции со сторонними системами.

Раздел 2. Подключение системы

Подготовка перед установкой и основные подключения.

Шаги

1. Нарисуйте линию с внешней стороны левой или правой тумбы.
2. Нарисуйте параллельные линии с каждой стороны от центральной линии для установки других тумб.

Примечание

Расстояние между двумя ближайшими линиями должно составлять 836 мм.

3. Пробейте пазы на монтажной поверхности и просверлите установочные отверстия в соответствии со схемой расположения отверстий. Вставьте 4 дюбеля для каждой тумбы.
4. Проложите кабели. Для каждого прохода прокладывают 1 высоковольтный кабель. Более подробная информация представлена далее в схеме подключения компонентов системы.

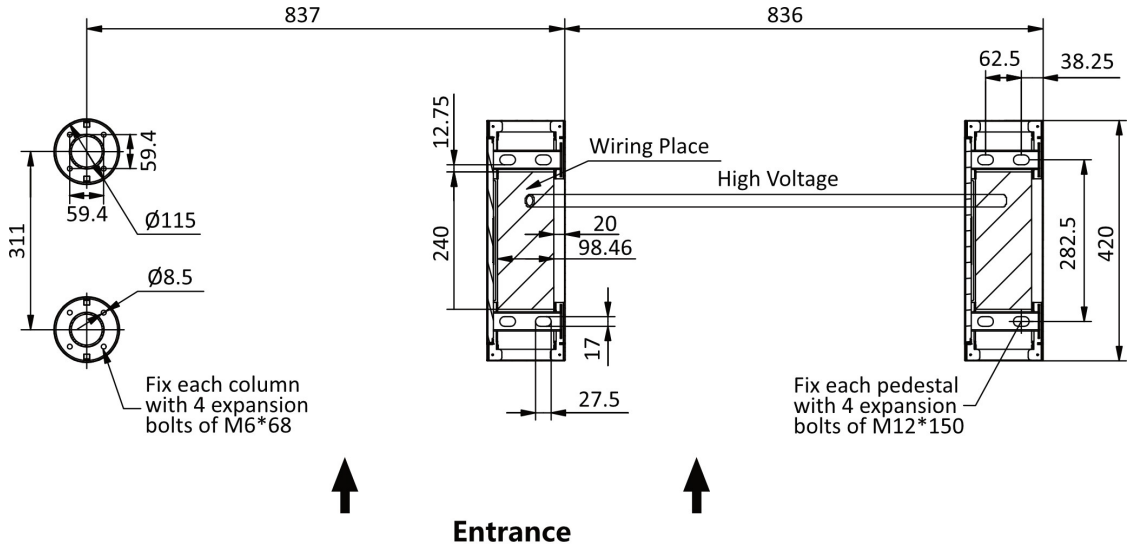


Рисунок 2-1. Схема подключения компонентов системы

Английский язык	Русский язык
Wiring Place	Место проводки
High Voltage	Высокое напряжение
Fix each column with 4 expansion bolts of M6 × 68	Закрепите каждую стойку 4 дюбелями M6 × 68.
Fix each pedestal with 4 expansion bolts of M12 × 150	Закрепите каждую тумбу 4 дюбелями M12 × 150.

Примечание

- Высокое напряжение: питание AC
- Рекомендуемый внутренний диаметр высоковольтного кабеля: больше 30 мм.

- Шнур внешнего источника переменного тока должен быть оснащен двойной изоляцией.
- Прежде просверливать отверстия необходимо проверить толщину установочной поверхности, чтобы избежать пробитий.
- Необходимо использовать сетевой кабель CAT5e или сетевой кабель с более мощными рабочими характеристиками.
- Если устройство будет применяться в детском саду и начальной школе, рекомендуется разработать специальные турникеты для детей младшего возраста и учащихся младших классов, чтобы снизить риски.

  Если дети проходят через турникет без сопровождения взрослых, рекомендуется использовать специальный кронштейн для установки терминала распознавания лиц для детей. При установке рекомендуется выбирать установку с малым углом или внешний вертикальный кронштейн. Такой кронштейн рекомендуется устанавливать на расстоянии около 0.5 метра перед турникетом.

Раздел 3 Установка

3.1 Демонтаж тумб

Перед установкой необходимо разобрать тумбу при помощи определенного ключа.
Замки и отверстия для установки представлены на рисунке ниже.

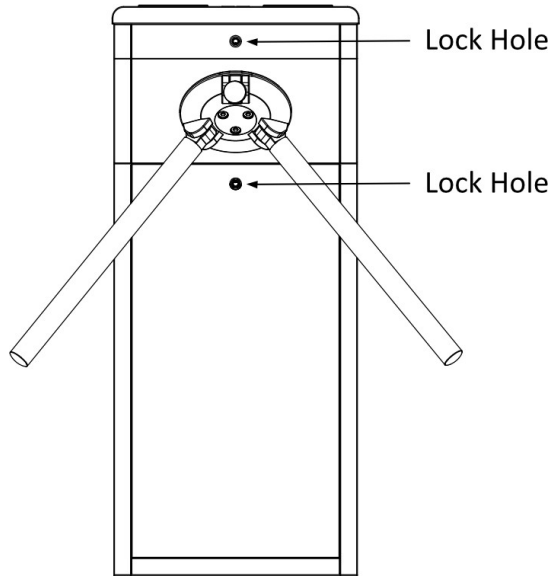


Рисунок 3-1. Отверстия для установки

Английский язык	Русский язык
Lock Hole	Отверстие для установки

3.2 Установка тумб

Перед началом
Подготовьте инструменты для установки, проверьте устройство и аксессуары и очистите основание для установки

Шаги

Примечание

- Устройство необходимо устанавливать на бетонную поверхность или на другие поверхности, устойчивые к воспламенению.
- Для предотвращения распространения ржавчины рекомендуется снять защитную пленку после завершения монтажа. В месте снятия пленки возможны остатки клея. После снятия пленки рекомендуется протереть поверхность защитной жидкостью WD-40.

- Далее представлена информация по размерам.

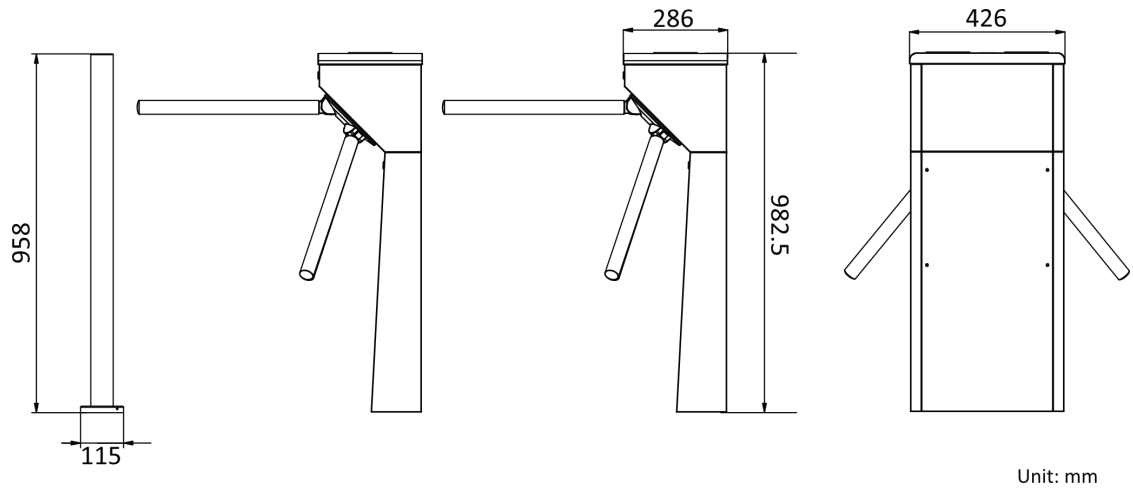


Рисунок 3-2. Размеры

1. Подготовьте инструменты для установки, проверьте устройство и компоненты и подготовьте основание для установки.
2. Герметично зафиксируйте основание турникета, чтобы защитить устройство от попадания воды внутрь.
3. Разместите кабели в соответствии с отметками **Entrance** («Вход») и **Exit** («Выход») на тумбах.

Примечание

Убедитесь, что монтажные отверстия на тумбах и основании совмещены друг с другом.

4. Зафиксируйте тумбы при помощи дюбелей.

Примечание

- Запрещено погружать тумбы в воду. В особых случаях глубина погружения должна составлять не более 150 мм.

5. Установите штанги.

Раздел 4. Основные подключения

Примечание

- После технического обслуживания необходимо закрыть водонепроницаемую крышку высоковольтного модуля.
- При обслуживании или демонтаже высоковольтных модулей следует демонтировать все высоковольтные модули целиком и обслуживать их снаружи турникета. Перед обслуживанием необходимо отключить кабели подключения к периферийным устройствам, чтобы избежать повреждения устройств.

4.1 Компоненты

По умолчанию основные компоненты турникета хорошо соединены. Связь между тумбами реализуется посредством подключения соединительных кабелей. Турникет можно подключить к источнику переменного тока для питания всей системы.

Примечание

Колебание напряжения электропитания составляет AC от 100 до 220 В, от 50 до 60 Гц.

На изображении ниже представлен серийный интерфейс для входа и выхода.

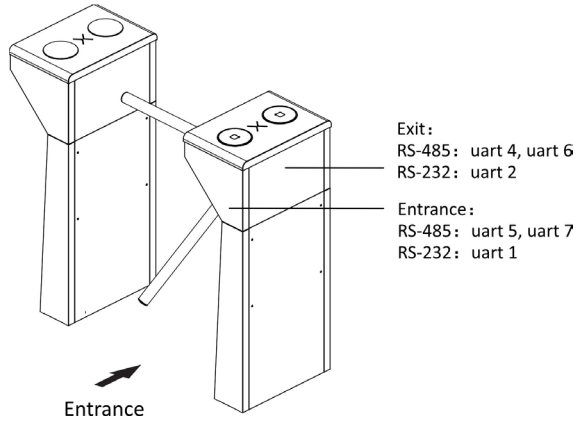


Рисунок 4-1. Серийный интерфейс

Английский язык	Русский язык
Entrance	Вход
Exit	Выход

На представленном далее изображении показано положение каждого компонента турникета.

Примечание

Схема содержит только справочную информацию.

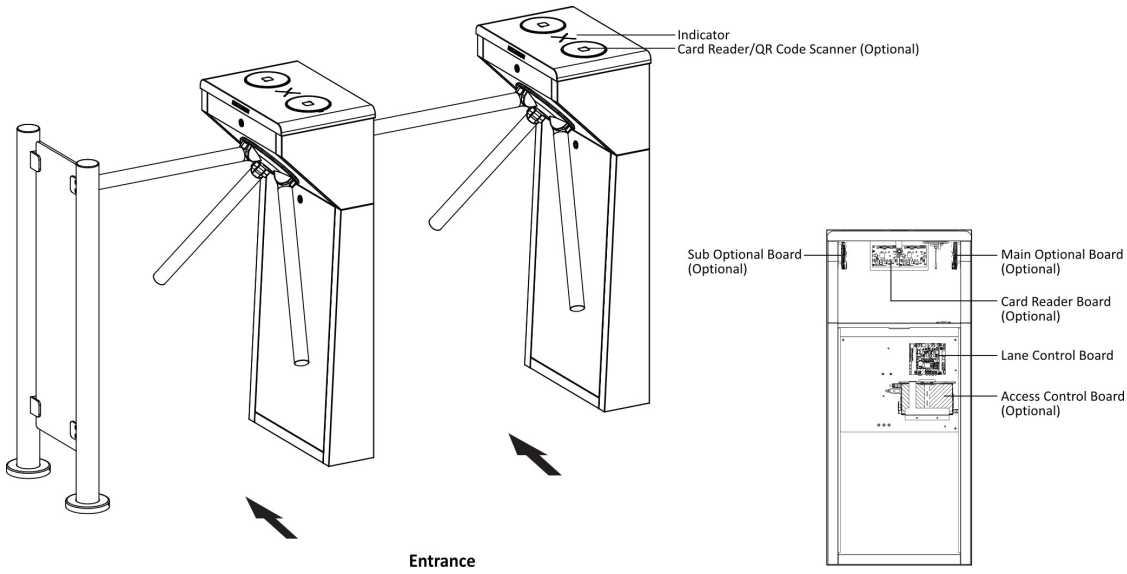


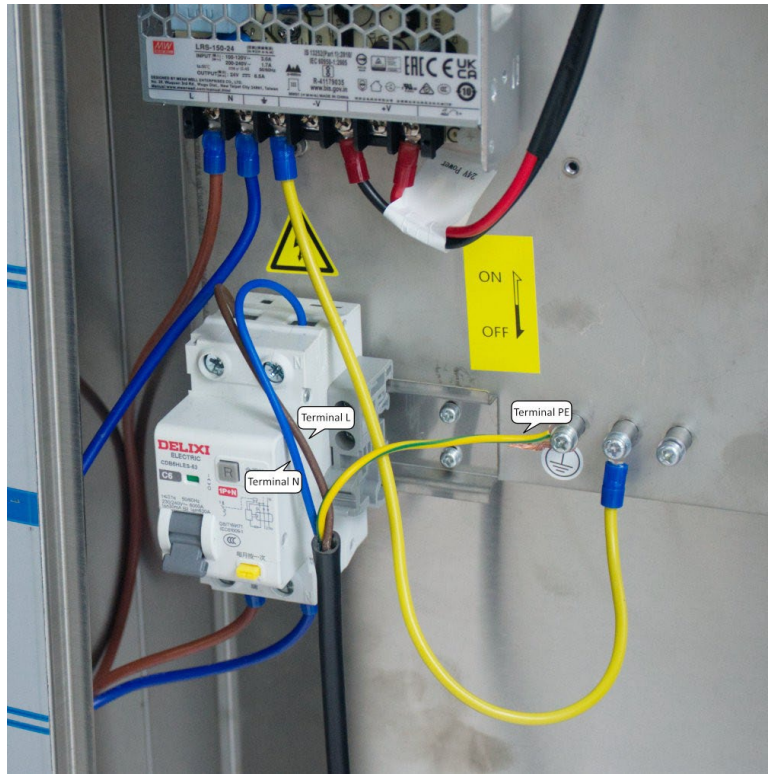
Рисунок 4-2. Схема подключения компонентов 1

Английский язык	**Русский язык**
Indicator	Индикатор
Card Reader / QR Code Scanner (Optional)	Считыватель карт / Сканер QR-кода (опционально)
Sub Optional Board (Optional)	Вспомогательная дополнительная плата (опционально)
Main Optional Board (Optional)	Основная дополнительная плата (опционально)
Card Reader Board (Optional)	Плата считывателя карт (опционально)
Lane Control Board	Плата контроля прохода
Access Control Board (Optional)	Плата контроля доступа (опционально)

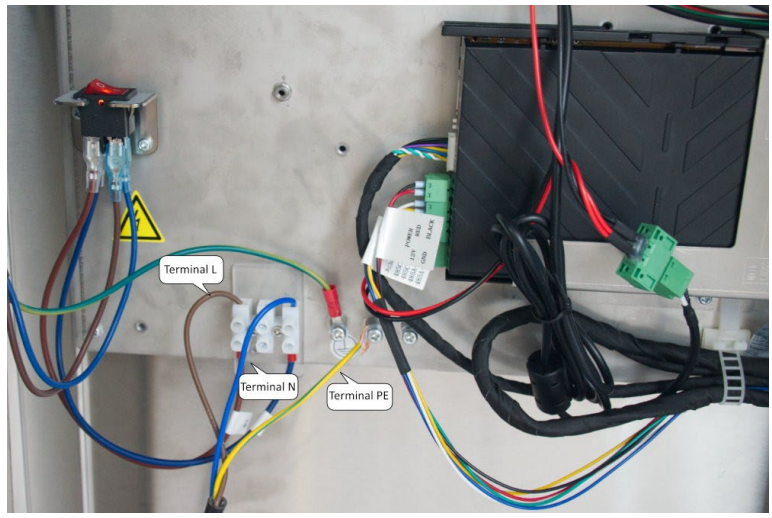
4.2 Подключение питания

Подключите источник питания к переключателю питания или адаптеру питания в тумбе турникета. Разъем L (коричневый) и разъем N (синий) расположены на переключателе, а разъем PE должен подключаться к заземляющему проводу (желто-зеленый провод).

Для турникета с переключателем питания схема подключения выглядит следующим образом:



Для турникета с адаптером питания схема подключения выглядит следующим образом:



Предупреждение

Разъем PE должен подключаться к заземляющему проводу, чтобы избежать опасности при прикосновении к устройству.

Примечание

- Длина оголенной части кабеля не должна превышать 8 мм. Если возможно, наденьте изоляционный колпачок на конец оголенного кабеля. Убедитесь, что после подключения всех кабелей отсутствует оголенная медь или оголенный кабель.
- Разъем L и разъем N не могут быть подключены в обратном порядке. Не подключайте входной и выходной разъемы в обратном порядке.
- Во избежание травм и повреждения устройства при испытании сопротивление заземления эквипотенциальных точек не должно превышать 2 Ом.

4.3 Подключение

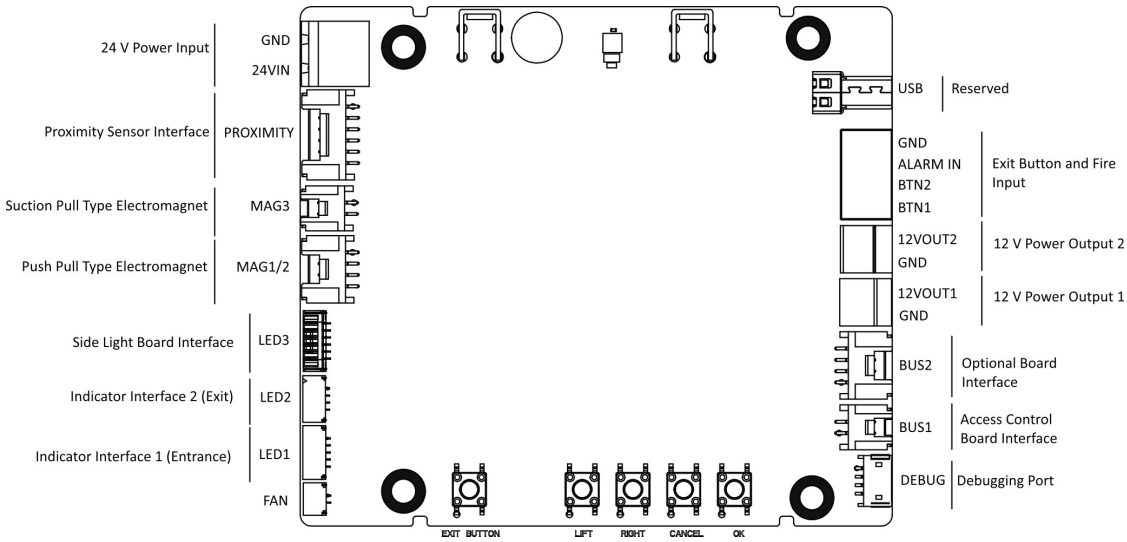
Сканируйте QR-код, чтобы просмотреть видео-руководство по подключению.

4.4 Описание разъемов

4.4.1 Описание разъемов платы контроля прохода

Плата контроля прохода содержит интерфейс питания, кнопку выхода и интерфейс пожарной тревоги, интерфейс платы контроля доступа, порт отладки, интерфейс индикатора и т. д.

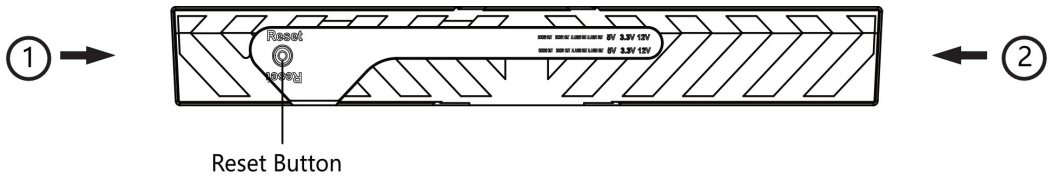
На представленном далее рисунке изображена схема платы контроля прохода.

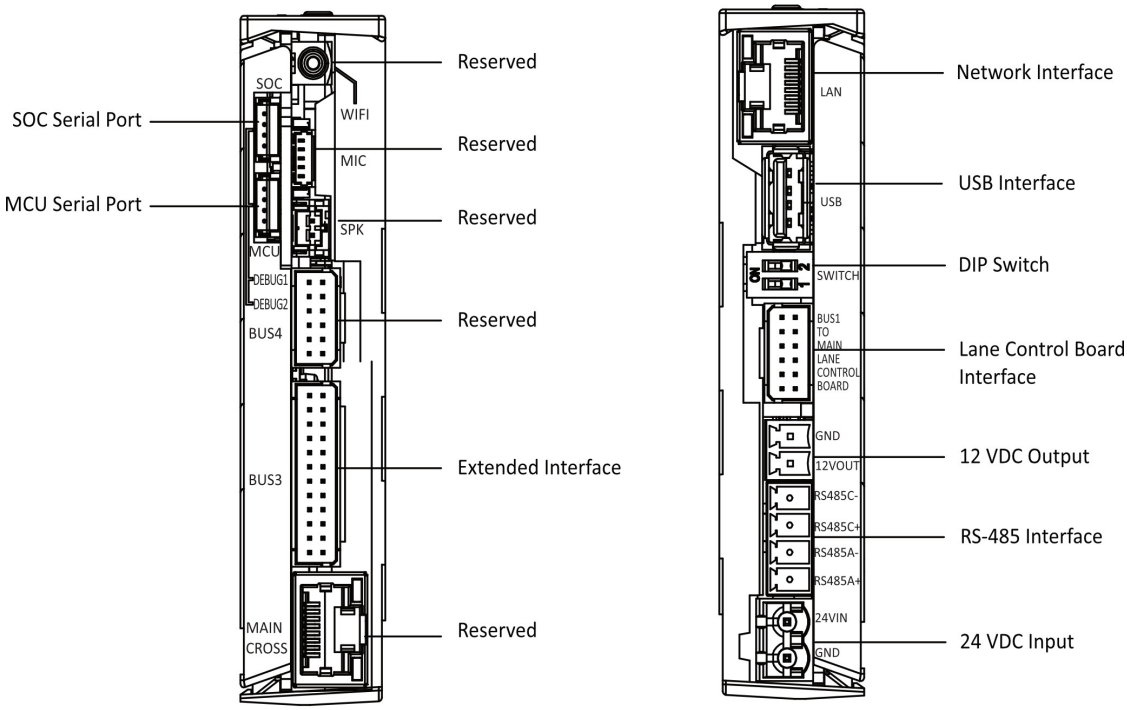


Английский язык	**Русский язык**
24 V Power Input	Вход питания 12 В
Proximity Sensor Interface	Интерфейс встроенного считывателя
Suction Pull Type Electromagnet	Электромагнит втягивающего типа
Push Pull Type Electromagnet	Электромагнит толкающего типа
Side Light Board Interface	Интерфейс платы управления световыми индикаторами
Indicator Interface 2 (Exit)	Интерфейс индикатора 2 (выход)
Indicator Interface 1 (Entrance)	Интерфейс индикатора 1 (вход)
Reserved	Зарезервировано
Exit Button and Fire Input	Кнопка выхода и вход противопожарной системы
12 V Power Output 2	Выход питания 2 (12 В)
12 V Power Output 1	Выход питания 1 (12 В)
Optional Board Interface	Интерфейс дополнительной платы
Access Control Board Interface	Интерфейс платы контроля доступа
Debugging Port	Порт отладки

4.4.2 Описание разъемов платы контроля доступа (опционально)

Плата контроля доступа в основном используется для идентификации уровня доступа в местах с высоким уровнем безопасности (таких как государственные учреждения и суды) посредством подключения к внешним устройствам и связи с контроллером прохода.





Английский язык	**Русский язык**
Reset Button	Кнопка сброса
SOC Serial Port	Серийный интерфейс SOC
MCU Serial Port	Серийный интерфейс MCU
Reserved	Зарезервировано
Extended Interface	Расширенный интерфейс
Network Interface	Сетевой интерфейс
USB Interface	USB
DIP Switch	DIP-переключатель
Lane Control Board Interface	Интерфейс платы контроля прохода
12 VDC Output	Выход DC 12 В
RS-485 Interface	RS-485
24 VDC Input	Вход DC 24 В

Примечание

- RS-485A соответствует UART 5 и по умолчанию предназначен для подключения сканера QR-кода на входе; RS-485C соответствует UART 7 и по умолчанию предназначен для подключения считывателя на входе.
- Серийные интерфейсы SOC и MCU предназначены только для обслуживания и отладки.
- Нажмите кнопку Reset («Сброс») на 5 секунд, и устройство начнет восстанавливать заводские настройки.
- DIP-переключатель предназначен для настройки в режиме обучения. Подробная информация о DIP-переключателе представлена в разделе *DIP-переключатель.*

Схема подключения расширенного интерфейса платы контроля доступа показана ниже.

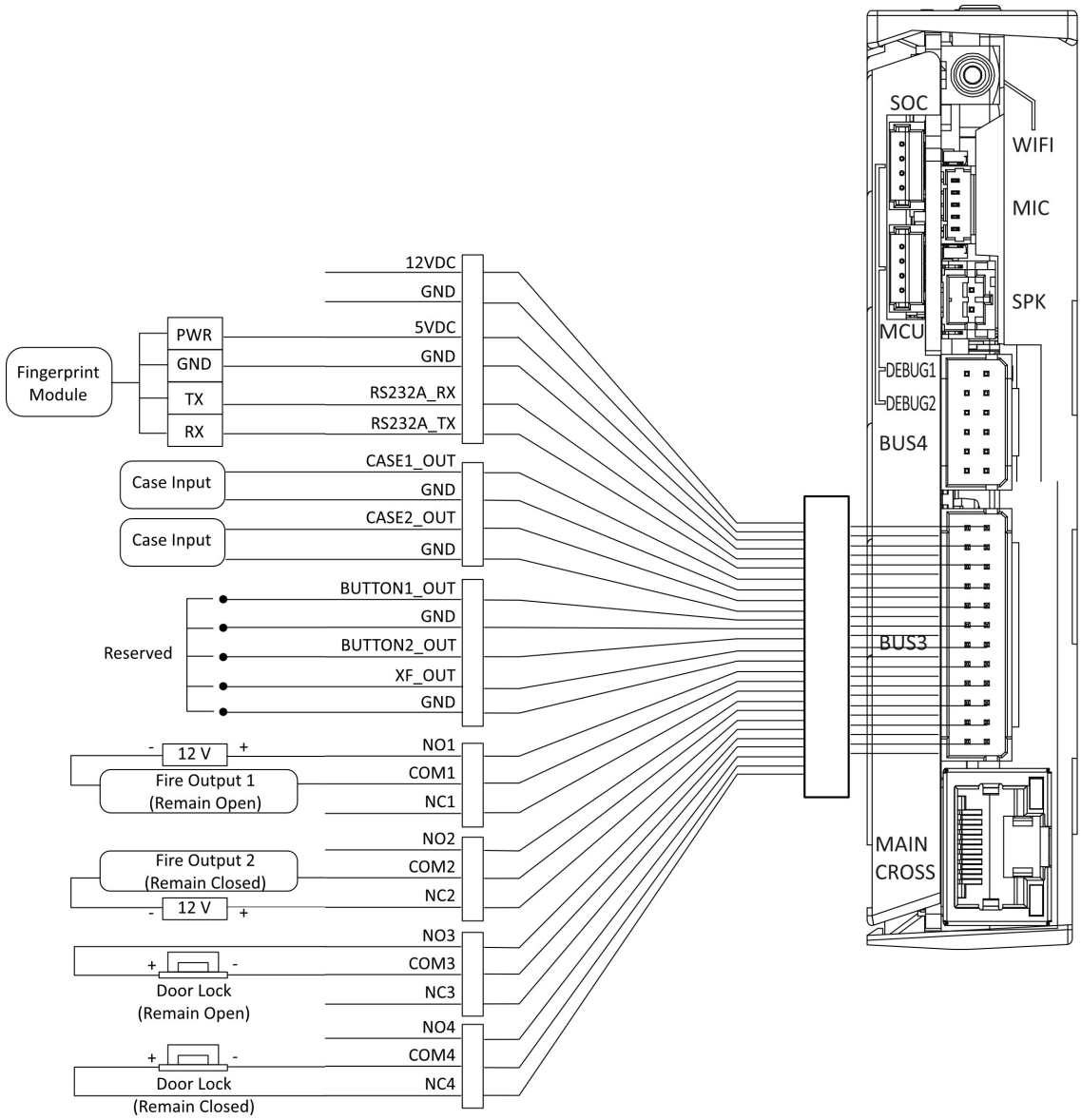


Рисунок 4-3. Схема подключения интерфейса BUS 3

Английский язык	Русский язык
Fingerprint Module	Модуль считывателя отпечатков пальцев
Case Input	Вход событий
Reserved	Зарезервировано
Fire Output 1 (Remain Open)	Выход противопожарной системы 1 (оставить открытым)
Fire Output 2 (Remain Closed)	Выход противопожарной системы 2 (оставить закрытым)
Door Lock (Remain Open)	Дверной замок (оставить открытым)
Door Lock (Remain Closed)	Дверной замок (оставить закрытым)

Примечание

RS-232A соответствует UART 1.

4.4.3 Описание разъемов основной дополнительной платы (опционально)

Основная дополнительная плата содержит интерфейс антенны sub-1G, интерфейс динамика, порт отладки, интерфейс Wiegand / кнопки выхода, выход DC 5 В и интерфейс связи.

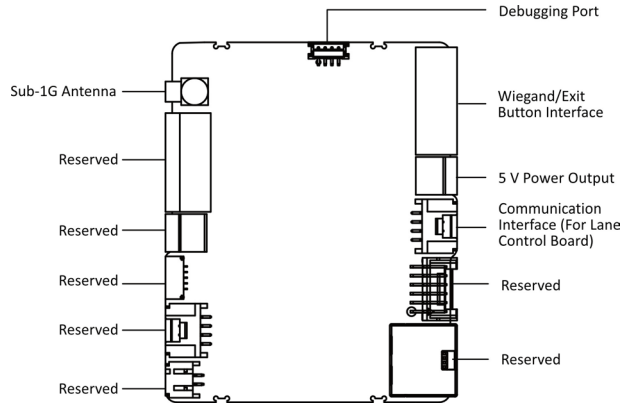


Рисунок 4-4. Разъемы основной дополнительной платы

Английский язык	Русский язык
Sub-1G Antenna	Антенна Sub-1G
Reserved	Зарезервировано
Debugging Port	Порт отладки
Wiegand/Exit Button Interface	Wiegand / интерфейс кнопки выхода
5 V Power Output	Выход питания 5 В
Communication Interface (for lane control board)	Интерфейс связи (для платы контроля прохода)

4.4.4 Описание разъемов вспомогательной дополнительной платы (опционально)

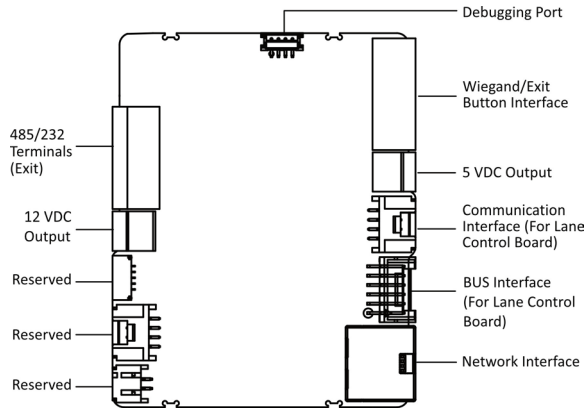


Рисунок 4-5. Разъемы вспомогательной дополнительной платы

Английский язык	**Русский язык**
485/232 Terminals (Exit)	Антенна Sub-1G
12 VDC Output	Выход DC 12 В
Reserved	Зарезервировано
Debugging Port	Порт отладки
Wiegand/Exit Button Interface	Wiegand / интерфейс кнопки выхода
5 V Power Output	Выход питания 5 В
Communication Interface (for lane control board)	Интерфейс связи (для платы контроля прохода)
BUS Interface (for lane control board)	Интерфейс шины (для платы контроля прохода)
Network Interface	Сетевой интерфейс

Примечание

- RS-485B соответствует порту 6 и по умолчанию предназначен для подключения сканера QR-кода.
- RS-485D соответствует порту 4 и по умолчанию предназначен для подключения считывателя карт.
- RS-232B соответствует порту 2 и по умолчанию используется для подключения считывателя отпечатков пальцев.

4.4.5 Описание разъемов платы считывателя карт

Плата считывателя карт может быть подключена к плате контроля доступа по интерфейсу RS-485.

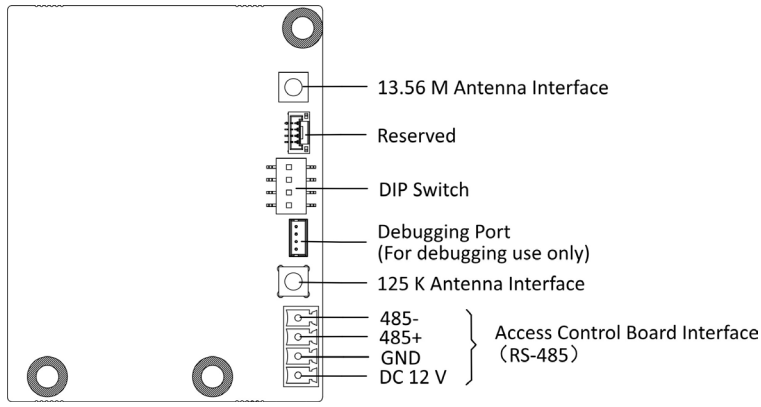


Рисунок 4-6. Плата считывателя карт

Английский язык	**Русский язык**
13.56 M Antenna Interface	Интерфейс антенны 13.56 M
Reserved	Зарезервировано
DIP Switch	DIP-переключатель
Debugging Port (for debugging use only)	Порт отладки (только для отладки)
125 K Antenna Interface	Интерфейс антенны 125 K
Access Control Board Interface	Интерфейс платы контроля доступа

4.4.6 Подключение по RS-485

Для подключения к модулю распознавания лиц или считывателю карт рекомендуется использовать интерфейсы RS-485 на плате контроля доступа и дополнительной плате. В качестве примера используется подключение к считывателю карт.

Примечание

- Если есть другие устройства, подключенные к RS-485, убедитесь в отсутствии конфликтов ID RS-485.
- Подключенный интерфейс питания 12 В для терминала распознавания лиц нельзя подключать к другим устройствам на 12 В.

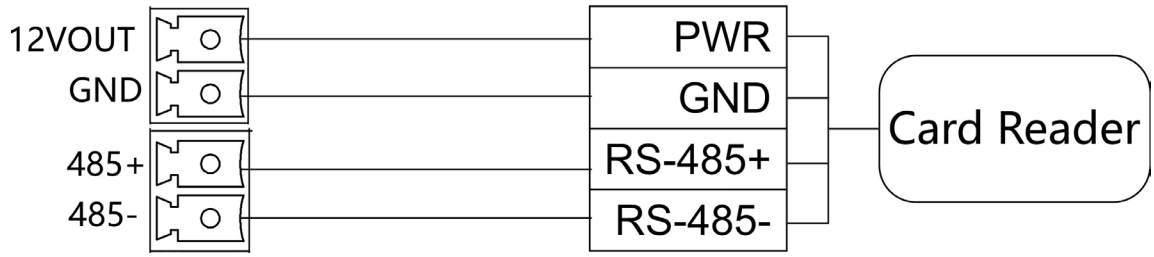


Рисунок 4-7. Подключение по RS-485

Английский язык	Русский язык
Card Reader	Считыватель карт

4.4.7 Подключение по RS-232

Примечание

- На расширенной плате контроля доступа расположен 1 интерфейс RS-232. Подробная информация представлена в разделе ***Описание разъемов платы контроля доступа (опционально).*** RS-232A соответствует UART 1.
- На расширенной вспомогательной плате контроля доступа расположен 1 интерфейс RS-232. Подробная информация представлена в разделе ***Описание разъемов вспомогательной дополнительной платы (опционально)*** RS-232B соответствует UART 2. Интерфейс RS-232C зарезервирован.

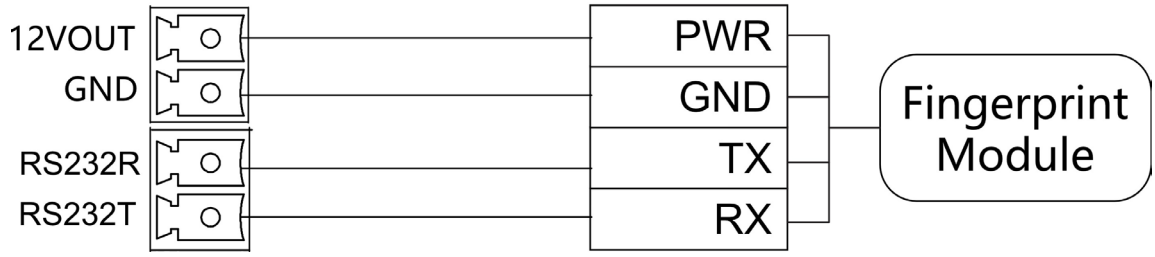
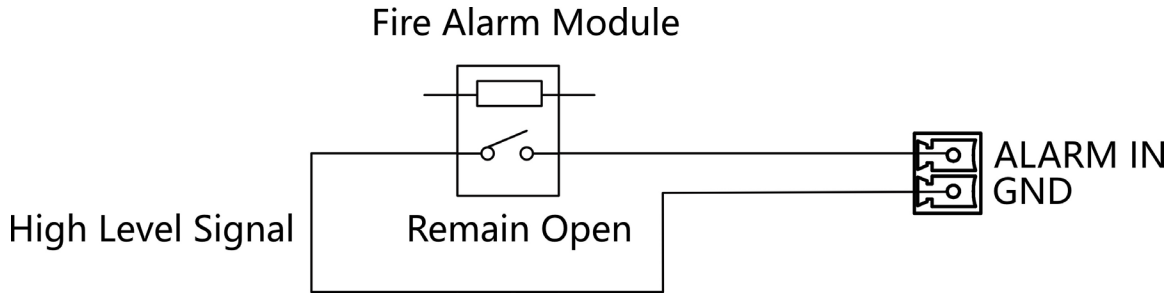


Рисунок 4-8. Подключение по RS-232

Английский язык	Русский язык
Fingerprint Module	Модуль считывания отпечатков пальцев

4.4.8 Подключение тревожного входа



К плате контроля прохода можно подключить входной интерфейс пожарной сигнализации.

Английский язык	**Русский язык**
Fire Alarm Module	Модуль противопожарной системы
High Level Signal	Сигнал высокого уровня
Remain Open	Оставить открытым

Рисунок 4-9. Режим «Оставить открытым»

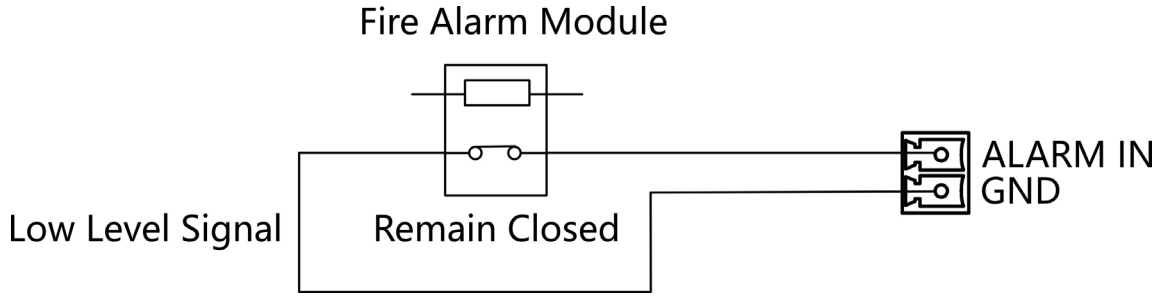


Рисунок 4-10. Режим «Оставить закрытым»

Английский язык	**Русский язык**
Fire Alarm Module	Модуль противопожарной системы
Low Level Signal	Сигнал низкого уровня
Remain Closed	Оставить закрытым

4.4.9 Подключение кнопки выхода

На основной и вспомогательной плате контроля расположено по 1 интерфейсу кнопки, который можно подключить к кнопке выхода или устройству распознавания лиц.

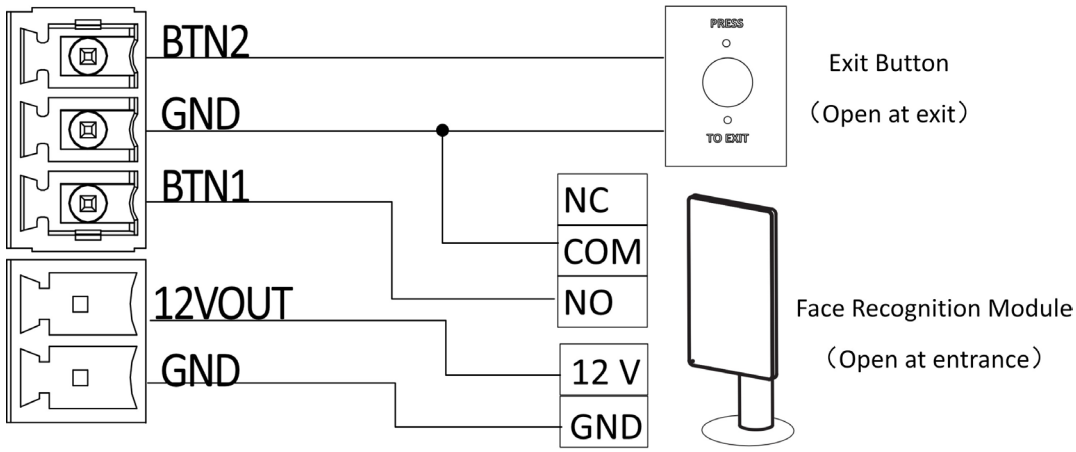


Рисунок 4-11. Подключение кнопки выхода

Английский язык	Русский язык
Exit Button (Open at exit)	Кнопка выхода (открытие при выходе)
Face Recognition Module (Open at entrance)	Модуль распознавания лиц (открытие при входе)

Примечание

- Устройства распознавания лиц питаются от выходного интерфейса питания DC 12 В основной и вспомогательной платы контроля прохода.
- Открытие турникета на входе: подключить к BTN1 и GND.
- Открытие турникета на выходе: подключить к BTN2 и GND.

4.5 Настройка устройства с помощью кнопки

Можно настроить устройство с помощью кнопки на плате контроля прохода.

4.5.1 Настройка с помощью кнопки

Описание кнопок

Кнопки расположены на плате контроля прохода.

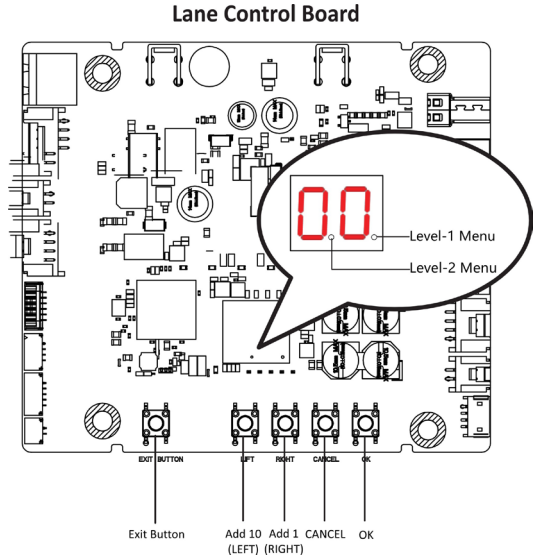


Рисунок 4-12. Кнопка

Английский язык	Русский язык
Lane Control Board	Плата контроля прохода
Level 1 Menu	Меню 1 уровня
Level 2 Menu	Меню 2 уровня
Exit Button	Кнопка выхода
Add 10 (Left)	Добавить 10 (влево)
Add 1 (right)	Добавить 1 (вправо)
Cancel	Отмена
OK	ОК

Кнопка выхода

- Нажмите один раз, чтобы открыть турникет из положения входа.
- Дважды нажмите, чтобы открыть турникет из положения выхода.

Кнопка настройки параметров

- **LEFT** («Влево»): нажмите, чтобы добавить десять к параметрам.
- **RIGHT** («Вправо»): нажмите, чтобы добавить один к параметрам.
- **CANCEL** («Отмена»): возврат в меню уровня 1 или выход из меню настроек.
- **OK**. Подтверждение данных или вход в режим настроек, или вход в дополнительное меню.

Примечание

- Параметры отображаются двумя цифрами.
- Меню 1 уровня: десятичная точка справа указывает на меню уровня 1. Число представляет собой номер элемента настройки.
- Меню уровня 2: десятичная точка посередине указывает на меню уровня 2. Число представляет параметры элемента настройки.

Процедура настройки при помощи кнопки

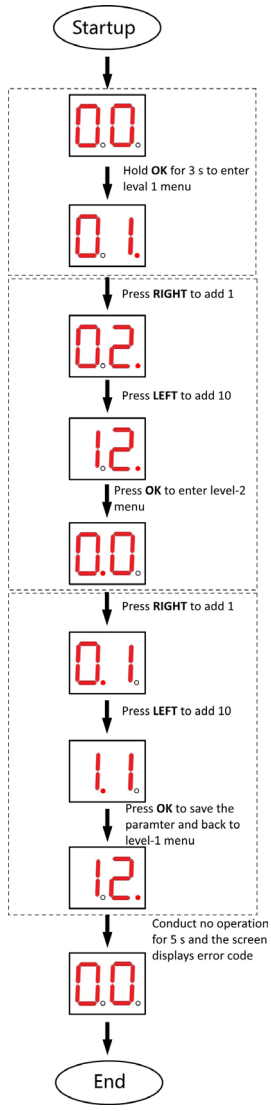


Рисунок 4-13. Процедура

Английский язык	**Русский язык**
Start up	Запуска
Hold OK for 3 s to enter level 1 menu	Удерживайте кнопку OK в течение 3 секунд, чтобы войти в меню уровня 1
Press RIGHT to add 1	Нажмите RIGHT («Вправо»), чтобы добавить 1
Press LEFT to add 10	Нажмите LEFT («Влево»), чтобы добавить 10
Press OK to enter level 2 menu	Нажмите OK, чтобы пойти в меню уровня 2
Press OK to save the parameter and back to level 1 menu	Нажмите OK, чтобы сохранить параметр и вернуться в меню уровня 1
Conduct no operation for 5 s and the screen display error code	Не выполняйте никаких действий в течение 5 с, и на экране отобразится код ошибки
End	Конец

Шаги

1. Войдите в режим настройки. Число 1 появится в правой части экрана, устройство готово к настройке.
2. Нажмите **LEFT** («Влево») и **RIGHT** («Вправо»), чтобы установить номер параметра настройки. Нажмите **OK**, чтобы войти в меню уровня 2 и просмотреть параметры. Нажмите **CANCEL** («Отмена») или не выполняйте никаких действий в течение 5 с, чтобы отменить настройку.
3. Нажмите **LEFT** («Влево») и **RIGHT** («Вправо»), чтобы установить параметры в соответствии с требованиями. Нажмите **OK**, чтобы сохранить изменения, или нажмите **CANCEL** («Отмена»), чтобы вернуться к настройке номера параметра без сохранения изменений. Не выполняйте никаких действий в течение 5 с, чтобы отменить настройку.

4.5.2 Инициализация устройства

Шаги

1. Удерживайте кнопку инициализации на плате контроля доступа в течение 5 с.

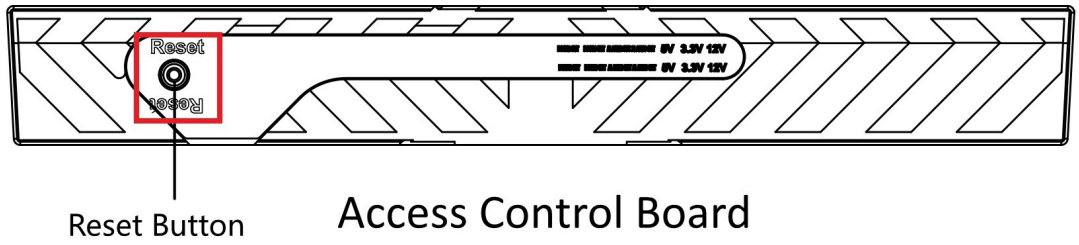


Рисунок 4-14. Положение кнопки инициализации

Английский язык	**Русский язык**
Reset Button	Кнопка сброса
Access Control Board	Плата контроля доступа

2. Устройство начнет восстановление заводских настроек.

3. Когда процесс завершится, устройство будет подавать звуковой сигнал в течение 3 с.

Предостережения

Инициализация устройства восстановит все параметры до значений по умолчанию, и все события устройства будут удалены.

Примечание

При включении устройства убедитесь, что в проходе нет людей.

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
- № порта по умолчанию: 8000
- Имя пользователя по умолчанию: admin

5.1 Активация через SADP

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

Перед началом

- ПО SADP загружено на диск, поставляемый в комплекте, также его можно скачать с официального сайта ***http:// www.hikvision.com/en/*** . Установите ПО SADP в соответствии с инструкцией.
- Устройство и ПК, на котором запущено ПО SADP, должны находиться в одной подсети.

Следующие шаги показывают, как активировать устройство и изменить его IP-адрес. Для получения подробной информации о пакетной активации и изменении IP-адресов смотрите ***Руководство 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.

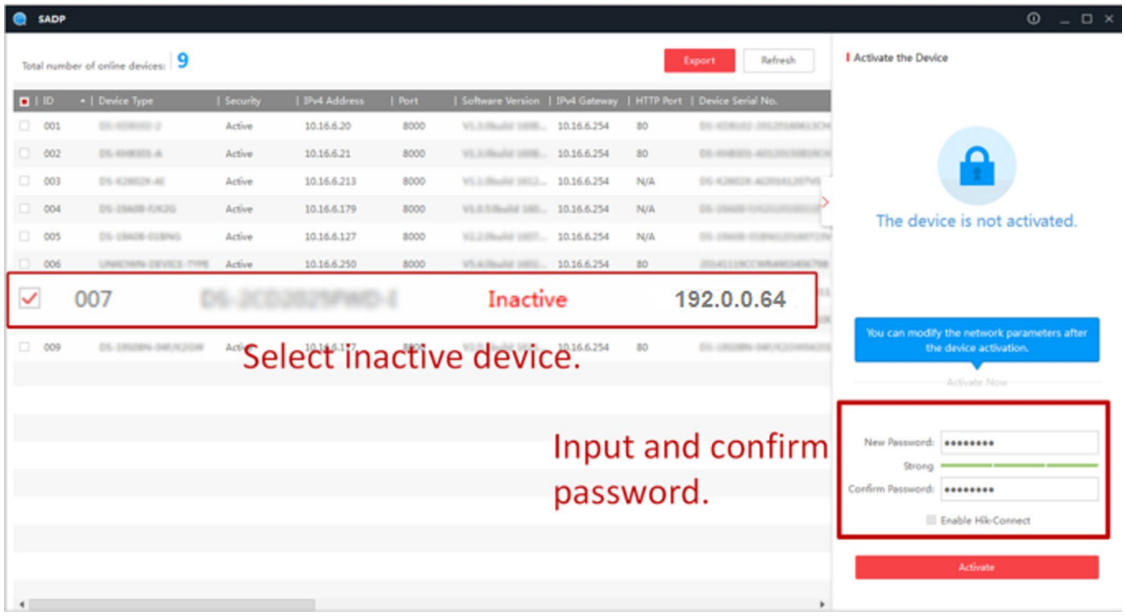
Предостережения

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 IP-адреса.

5.2 Активация устройства через клиентское ПО iVMS-4200

Для некоторых устройств необходимо создать пароль для их активации, прежде чем их можно будет добавить в программное обеспечение iVMS-4200, и они будут работать надлежащим образом.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Перейдите на страницу **Device Management** («Управление устройством»).
2. Нажмите в правой части экрана на странице **Device Management** («Управление устройством») и выберите **Device** («Устройство»).
3. Нажмите **Online Device** («Онлайн устройства»), чтобы отобразить область онлайн устройств. Искомые онлайн устройства отобразятся в списке.
4. Проверьте состояние устройства (отображено в столбце **Security Level** («Уровень безопасности»)) и выберите неактивное устройство.
5. Нажмите **Activate** («Активировать»), чтобы открыть окно активации.
6. Создайте и введите новый пароль в поле **Password** («Пароль») и подтвердите его в поле **Confirm Password** («Подтвердить пароль»).

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 безопасным. Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг или конечного пользователя.

Примечание

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

7. Для активации устройства нажмите **OK**.

5.3 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** («Войти»).

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

2. Создайте 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.

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

4. Изменение IP-адреса устройства. IP-адрес можно редактировать с помощью инструмента SADP, устройства и клиентского программного обеспечения.

Раздел 6 Операции через веб-интерфейс

6.1 Вход в систему

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

Примечание

программного обеспечения.

Устройство должно быть активировано. Подробная информация представлена в разделе ***Активация***.

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.

6.2 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 по адресу ***pw_recovery@hikvision.com*** в качестве вложения.
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.

6.3 Обзор

Можно просматривать состояние компонентов устройства, события в режиме реального времени, информацию о пользователях, состояние сети, основную информацию и емкость устройства. Также можно удаленное управлять турникетом.

Описание функций:

Состояние компонентов устройства

Проверьте корректность работы устройства. Нажмите **View More** («Подробная информация»), чтобы просмотреть состояние компонента.

Удаленное управление

/ / /

Состояние: открыт / закрыт / оставить открытым / оставить закрытым.

События в режиме реального времени

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

Информация о пользователе

Можно просмотреть добавленные изображения и карты.

Состояние сети

Отображение состояния сетевого подключения.

Основная информация

Можно просмотреть модель, серийный номер и версию прошивки.

Емкость устройства

Можно просмотреть емкость библиотек пользователей, карт и событий.

6.4 Управление пользователями

Нажмите **Add** («Добавить»), чтобы добавить информацию о пользователе, включая основную информацию, сертификат и метод аутентификации.

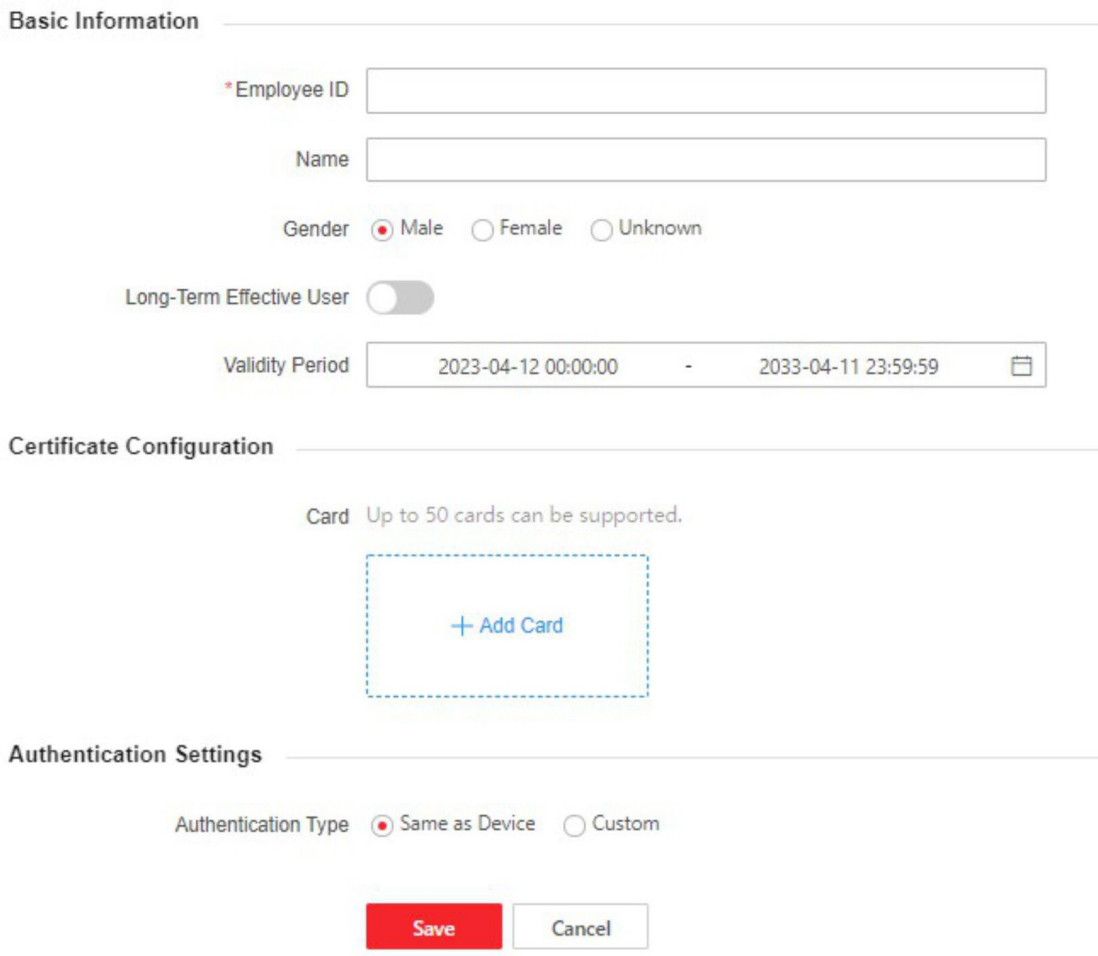


Рисунок 6-1. Управление пользователями

Добавление основной информации

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления пользователя.
Добавьте основную информацию пользователя, включая идентификатор, имя и т. д.
Затем нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Настройка периода разрешения

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления пользователя.
Нажмите **Long-Term Effective User** («Долгосрочное разрешение пользователя») или настройте время начала и время окончания. Разрешение пользователя будет действительно только в течение настроенного периода времени в соответствии с требованиями проекта.
Нажмите **Save** («Сохранить») для сохранения настроек.

Настройки параметров аутентификации

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления пользователя. Выберите тип аутентификации.

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

Добавление карты

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления пользователя.
Нажмите **Add Card** («Добавление карты»), введите **Card No.** («Номер карты»), выберите **Property** («свойство») и нажмите **Save** («Сохранить»), чтобы добавить карту. Нажмите **Save** («Сохранить») для сохранения настроек.

Импорт и экспорт информации о пользователе

Экспорт информации о пользователе

Можно экспортировать данные о добавленных пользователях для резервного копирования или импорта на другие устройства. Нажмите **Export Person Data** («Экспортировать данные пользователя»), установите пароль шифрования и подтвердите его. Нажмите **OK**.

Примечание

- Данные будут загружены на ваш компьютер.
- Для импорта файла данных потребуется ввести установленный пароль.

Импорт информации о пользователе

Нажмите **Importing Person Data** («Импортировать данные пользователя») и выберите файл. Нажмите **Import** («Импорт»).

Введите пароль шифрования, чтобы импортировать данные пользователя на устройства.

Примечание

- Убедитесь, что имя импортируемого файла — UserDataFile.

6.5 Поиск событий

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

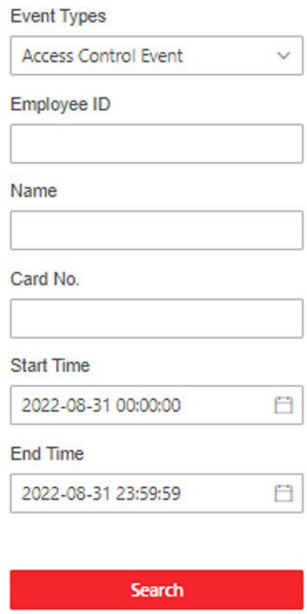


Рисунок 6-2. Поиск событий

Выберите тип события и введите условия поиска, включая идентификатор сотрудника / посетителя, имя, номер карты, время начала и время окончания доступа и нажмите **Search** («Поиск»).

После этого на панели справа появятся результаты поиска.

6.6 Настройка

6.6.1 Просмотр информации об устройстве

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

Можно просмотреть имя устройства, язык, модель, серийный номер, версию, интерфейсы входа и выхода и номер RS-485.

Можно изменить **Device Name** («Имя устройства») и нажать **Save** («Сохранить»).

Можно просмотреть емкость устройства, включая емкость библиотек пользователей, карт и событий.

6.6.2 Настройка времени

Настройте время устройства, часовой пояс, режим синхронизации, адрес сервера, порт NTP и интервал. Нажмите **Configuration → System → System Settings → Time Settings** («Настройки → Система → Настройки системы → Настройки времени»).

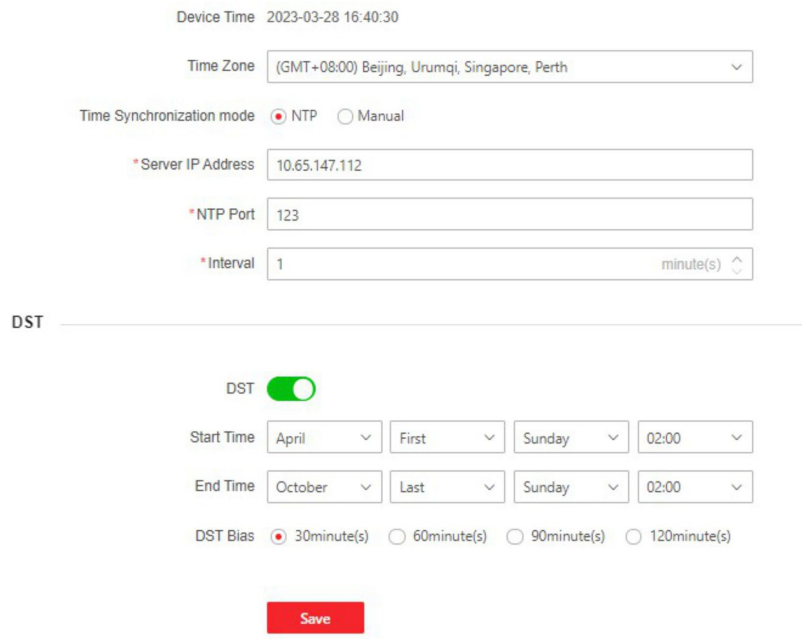


Рисунок 6-3. Настройка времени

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

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

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 настроить IP-адрес сервера, порт NTP, интервал.

6.6.3 Настройка перехода на летнее время (DST)

Шаги

1. Нажмите **Configuration → System → System Settings → Time Settings** («Настройки → Система → Настройки системы → Настройки времени»).

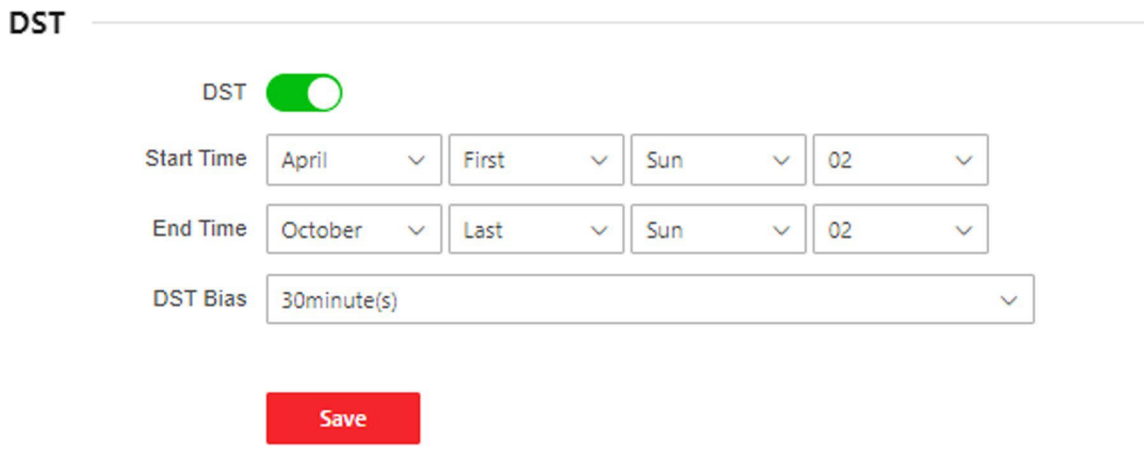


Рисунок 6-4. Страница перехода на летнее время

2. Включите **DST**.
3. Установите время начала и окончания DST, а также смещение DST.
4. Нажмите **Save** («Сохранить») для сохранения настроек.

6.6.4 Изменение пароля администратора

Шаги

1. Нажмите **Configuration → User Management** («Настройки → Управление пользователями»).
2. Нажмите .
3. Введите старый пароль и создайте новый пароль.
4. Подтвердите новый пароль.
5. Нажмите **OK**.

Предостережения

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 безопасным. Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг или конечного пользователя.

6.6.5 Онлайн пользователи

Отображается информация о пользователях, выполняющих вход в устройство.

Перейдите в меню **Configuration → User Management → Online Users** («Настройки → Управление пользователями → Онлайн пользователи») для просмотра списка онлайн пользователей.

6.6.6 Просмотр информации о постановке / снятии с охраны

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

Нажмите **Configuration → User Management → Arming/Disarming Information** («Настройки → Управление пользователями → Информация о постановке / снятии с охраны»).

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

6.6.7 Параметры сети

Настройка основных сетевых параметров

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

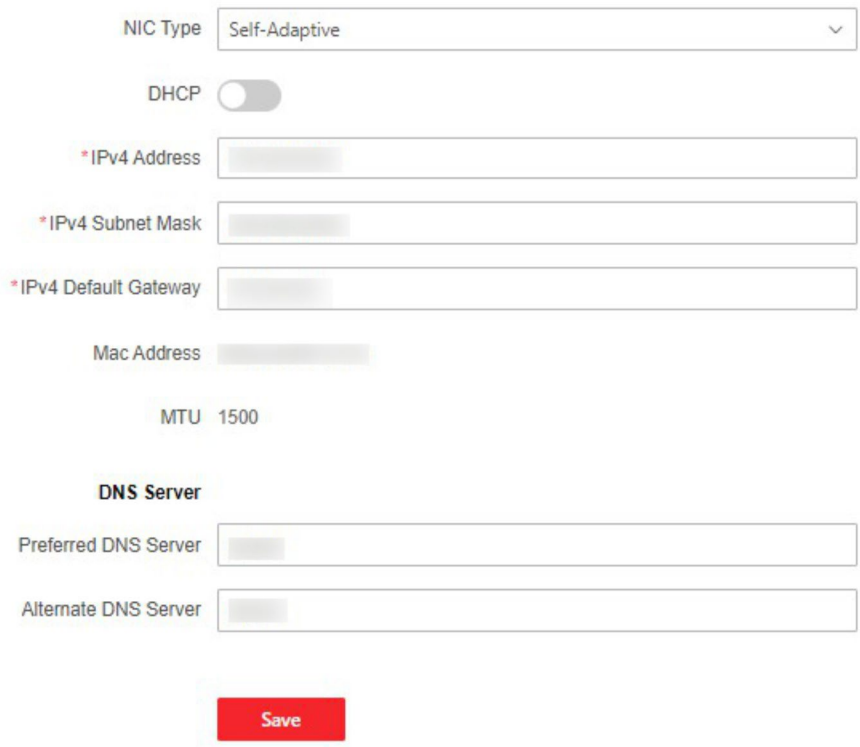


Рисунок 6-5. Страница настройки TCP/IP

Также можно посмотреть MAC-адрес и MTU.

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

Тип NIC

Выберите тип NIC из выпадающего списка. По умолчанию выбрано значение **Self-Adaptive** («Автоматическая адаптация»).

DHCP

При отключении DHCP необходимо вручную настроить адрес IPv4, маску подсети IPv4, шлюз IPv4 по умолчанию, предпочитаемый DNS-сервер и альтернативный DNS-сервер.

При включении DHCP система автоматически назначит IPv4-адрес, маску подсети IPv4, шлюз IPv4 по умолчанию, предпочитаемый DNS-сервер и альтернативный DNS-сервер.

DNS-сервер

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

Настройка параметров порта

Настройте параметры HTTP, HTTPS, параметры прослушивания HTTP.

Нажмите **Configuration → Network → Network Service → HTTP(S)** («Настройки → Сеть → Сетевая служба → HTTP(S)»).

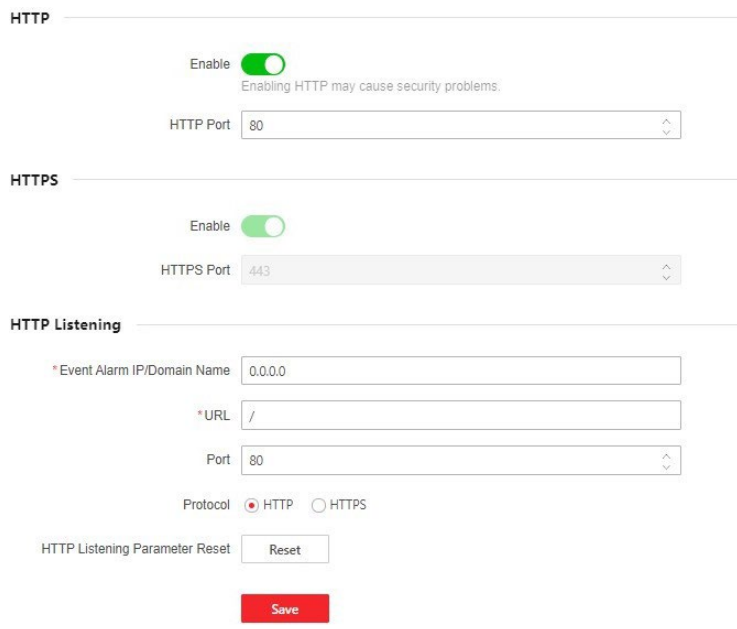


Рисунок 6-6. Сетевая служба

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.

6.6.8 Привязка события

Настройте привязку действий и событий.

Шаги

1. Нажмите **Configuration → Event → Event Detection → Linkage Settings** («Настройка → События → События обнаружения → Настройка привязки») для перехода на страницу настроек.

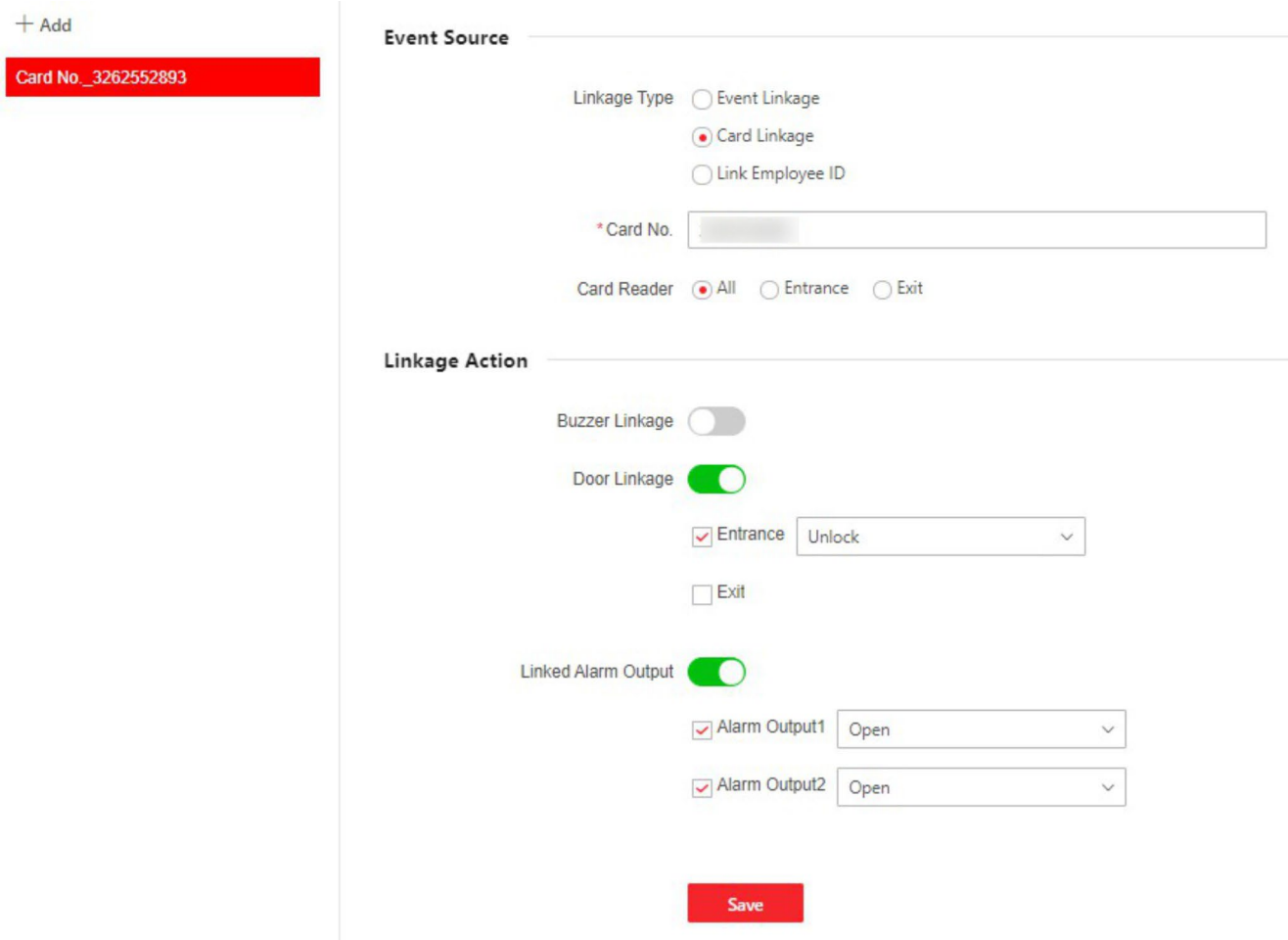


Рисунок 6-7. Привязка событий

2. Настройте источник события.
   - При настройке **Linkage Type** («Тип привязки») выберите **Event Linkage** («Привязка события»).
   - При выборе **Card Linkage** («»Привязка карты») в **Linkage Type** («Тип привязки») введите № карты и выберите считыватель карт.
   - При выборе **Employee ID Linkage** («Привязка ID сотрудника») в **Linkage Type** («Тип привязки») введите ID сотрудника и выберите считыватель карт.
3. Настройте действие привязки.

Привязка бипера

Нажмите **Buzzer Linkage** («Привязка бипера») и выберите **Start Buzzing** («Запуск бипера») или **Stop Buzzing** («Остановка бипера») для целевого события.

Привязка двери

Нажмите **Door Linkage** («Привязка двери»), выберите **Entrance** («Вход») или **Exit («**Выезд») и настройте состояние двери для события.

Привязка тревожного выхода

Нажмите **Linked Alarm Output** («Привязка тревожного выхода»), выберите **Alarm Output 1** («Тревожный выход 1») или **Alarm Output 2** («Тревожный выход 2») и настройте состояние тревожного выхода для события.

6.6.9 Настройки контроля доступа

Настройка параметров контроля доступа

Нажмите **Configuration → Access Control → Authentication Settings** («Настройки → Контроль доступа → Параметры аутентификации»).

Примечание

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

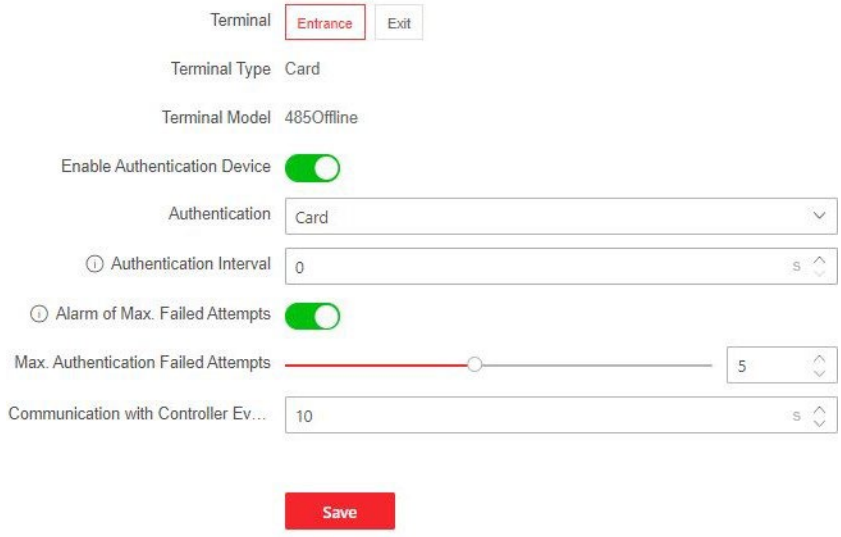


Рисунок 6-8. Настройка параметров аутентификации

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

Терминал

Выберите **Entrance** («Вход») или **Exit** («Выход»).

Тип терминала / режим терминала

Представлена дополнительная информация. Доступно только для чтения.

Включить устройство с функцией аутентификации

Включить функцию аутентификации.

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.

Достижение максимального 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.

Примечание

Значение интервала аутентификации находится в диапазоне от 2 с до 255 с.

6.6.10 Настройка параметров двери

Нажмите **Configuration → Access Control → Door Parameters** («Настройки → Контроль доступа → Параметры двери»). Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Номер двери

Выберите **Entrance** («Вход») или **Exit** («Выход») для настройки.

Наименование двери

Можно задать имя двери.

Длительность открытого состояния

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

Примечание

Состояние «открыто» длится от 5 до 60 с.

Тип кнопки выхода

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

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.

6.6.11 Настройки серийного интерфейса

Настройка параметров серийного интерфейса.

Шаги

1. Нажмите **Configuration → Access Control → Serial Port Settings** («Настройки → Контроль доступа → Настройка серийного интерфейса»).

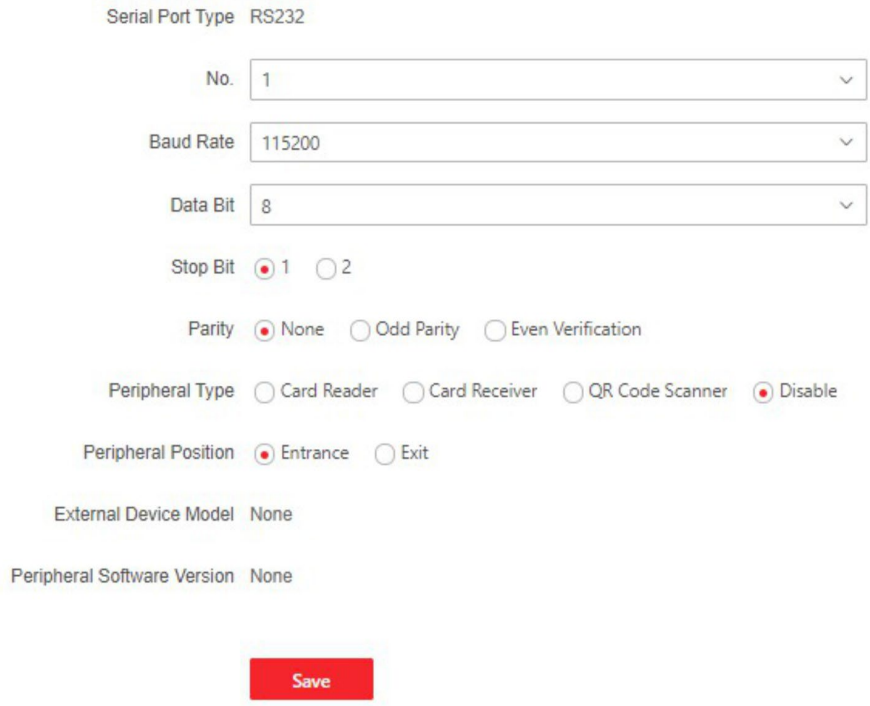


Рисунок 6-9. Настройки серийного интерфейса

2. Настройте значение **No.** («Номер»), **Baud Rate** («Скорость передачи данных»), **Data Bit** («Бит данных»), **Stop Bit** («Стоповый бит») и **Parity** («Четность»).
3. Настройте **Peripheral Type** («Тип периферийного устройства»), выбрав **Card Reader** («Считыватель карт»), **Card Receiver** («Картоприемник»), **QR Code Scanner** («Сканер QR-кода») или **Disable** («Отключить»).
4. Настройте **Peripheral Position** («Положение периферийного устройства»), выбрав **Entrance** («Вход») или **Exit** («Выход»).
5. Можно просмотреть тип серийного порта, модель устройства и версию программного обеспечения периферийного устройства.

6. Нажмите **Save** («Сохранить»).

6.6.12 Настройка параметров терминала

Можно настроить параметры терминала для получения доступа.

Нажмите **Configuration → Access Control → Terminal Parameters** («Настройка → Контроль доступа → Параметры терминала»).

Настройте **Working Mode** («Режим работы»), выбрав **Permission Free Mode** («Режим свободного доступа») или **Access Control Mode** («Режим контроля доступа»).

Режим свободного доступа

Устройство определяет срок действия учетных данных, но не выполняет аутентификацию разрешений.

Нажмите **Verify Credential Locally** («Верификация учетных данных локально»), устройство будет проверять разрешения без проверки шаблона.

Режим контроля доступа

Режим контроля доступа является нормальным режимом работы устройства. Для получения доступа необходимо пройти аутентификацию с использованием учетных данных.

Можно включить **Remote Verification** («Удаленная верификация»). После включения можно выполнять верификацию удаленно. Можно включить **Verify Credential Locally** («Верификация учетных данных локально») в соответствии с требованиями проекта.

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

6.6.13 Основные параметры турникета

Настройте основные параметры турникета.

Шаги

1. Чтобы войти на страницу, нажмите **Configuration → Turnstile Configuration → Basic Settings** («Настройки → Настройка турникета → Основные настройки»).

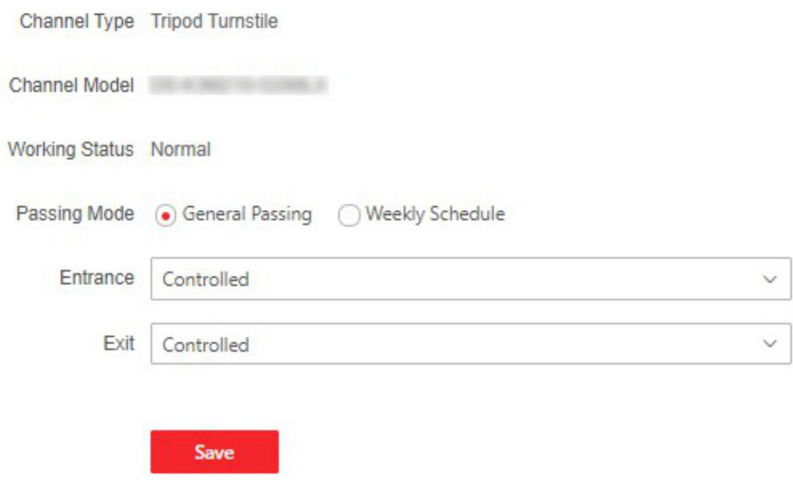


Рисунок 6-10. Основные настройки

2. Возможность просмотра **Channel Type** («Типа канала»), **Channel Model** («Модели канала») и **Working Status** («Рабочего состояния»).
3. Настройте режим прохода.
   - При выборе **General Passing** («Обычный проход») можно выбрать состояние турникета для входа и выхода из выпадающего списка.
   - При выборе **Weekly Schedule** («Расписание на неделю») можно установить еженедельное расписание для входа и выхода.
4. Нажмите **Save** («Сохранить»).

6.6.14 Подсчет сотрудников / посетителей

Настройка подсчета сотрудников / посетителей.

Шаги

1. Чтобы войти на страницу, нажмите **Configuration → Turnstile Configuration → People Counting Settings** («Настройки → Настройка турникета → Настройка подсчета сотрудников / посетителей»).

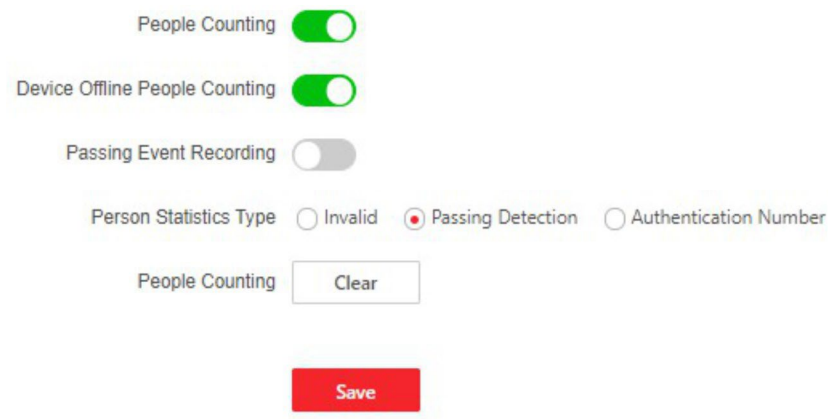


Рисунок 6-11. Подсчет сотрудников / посетителей

2. Нажмите **People Counting** («Подсчет сотрудников / посетителей»).
3. Нажмите **Device Offline People Counting** («Подсчет сотрудников / посетителей в режиме офлайн»), если необходимо.

Примечание

Функция **Passing Event Recording** («Запись события прохода») зарезервирована.

4. Настройте **Person Statistics Type** («Тип статистики»), выбрав **Invalid** («Недействительно»), **Passing Detection** («Детекция прохода») или **Authentication Number** («Номер аутентификации»).
5. **Опционально.** Нажмите **Clear** («Очистить»), чтобы удалить всю информацию о подсчете.

6.6.15 Прочие настройки

Настройте другие параметры.

Шаги

1. Чтобы войти на страницу, нажмите **Configuration → Turnstile Configuration → Other Settings** («Настройки → Настройка турникета → Другие настройки»).
2. Настройте **Alarm Output Duration** («Продолжительность работы тревожного выхода»).

   Примечание

   Длительность сигнала тревоги настроена в диапазоне от 0 с до 3599 с.
3. Настройте **Temperature Unit** («Единицы измерения температуры»).
4. Перетащите блок или введите значение, чтобы отрегулировать параметры.
5. Настройте длительность работы бипера.
6. Включите режим памяти, если необходимо.

   Примечание

   При включении режима памяти допускается предъявление нескольких карт для прохождения нескольких сотрудников / посетителей. Когда количество проходящих сотрудников / посетителей превышает количество предъявленных карт или после того, как последний сотрудник / посетитель проходит, а другие люди не проходят в течение времени открытия, турникет закроется автоматически.
7. Настройте **Fire Input Type** («Тип входа модуля обнаружения возгораний»).
8. Нажмите **Save** («Сохранить»).

6.6.16 Настройки параметров карты

Настройка безопасности карты

Нажмите **Configuration → Card Settings → Card Type** («Настройка → Настройка параметров карты → Тип карты») для перехода на страницу настроек. Настройте параметры и нажмите **Save** («Сохранить»).

Включение распознавания NFC-карты

Зарезервировано.

Включение распознавания M1-карты

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

Сектор шифрования M1-карты

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.

Чтение DESfire-карт

Устройство может считывать данные с DESfire-карты при включении соответствующей функции.

Чтение DESFire-карт

После включения функции чтения DESFire-карт устройство может считывать содержимое DESFire-карты.

Чтение FeliCa-карт

Устройство может считывать данные с FeliCa-карты при включении соответствующей функции.

6.6.17 Настройка параметров аутентификации номера карты

Настройте параметры карты при аутентификации через карту на устройстве. Нажмите

Configuration → Card Settings → Card No. Settings («Настройки → Настройки карты → →

Настройка параметров аутентификации номера карты»).

Выберите режим аутентификации карты и включите обратный порядок номера карты, если необходимо. Нажмите **Save** («Сохранить»).

6.6.18 Настройка параметров конфиденциальности

Задайте тип хранения событий.

Перейдите в **Configuration → Security → Privacy Settings** («Настройка → Безопасность → Настройка параметров конфиденциальности»).

Тип хранения событий по умолчанию — перезапись. Самые ранние 5 % событий будут удалены, когда система обнаружит, что сохраненные события занимают более 95 % заполненного пространства.

6.6.19 Обновление и техническое обслуживание

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

Перезагрузка устройства

Нажмите **Maintenance and Security → Maintenance → Restart** («Техническое обслуживание и безопасность → Техническое обслуживание → Перезагрузка»). Нажмите **Restart** («Перезагрузка») для перезагрузки устройства.

Обновление

Нажмите **Maintenance and Security → Maintenance → Upgrade** («Техническое обслуживание и безопасность → Техническое обслуживание → Обновление»).
Выберите тип обновления из выпадающего списка. Нажмите и выберите файл обновления с локального ПК. Нажмите **Upgrade** («Обновить») для начала обновления.

Примечание
Не выключайте устройство во время обновления.

Восстановление параметров

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

Восстановить все

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

Восстановление

Настройки устройства будут восстановлены до настроек по умолчанию, за исключением параметров сети и информации о пользователе.

Параметры импорта и экспорта

Нажмите **Maintenance and Security → Maintenance → Backup and Reset** («Техническое обслуживание и безопасность → 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.

6.6.20 Отладка устройства

Можно настроить параметры отладки устройства.

Шаги

1. Нажмите **Maintenance and Security → Maintenance → Device Debugging** («Техническое обслуживание и безопасность → 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.

Печать журнала

Можно выбрать компонент из раскрывающегося списка и нажать **Export** («Экспорт»), чтобы экспортировать журнал.

Захват сетевого пакета

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

6.6.21 Состояние компонентов

Можно просмотреть состояние прохода и состояния других компонентов.

Состояние прохода

Компоненты устройства

Можно просмотреть состояние платы контроля доступа, платы контроля прохода, платы с расширенными интерфейсами.

Периферийные устройства

Можно просмотреть состояние считывателя карт RS-485.

Другое

Режим прохода

Можно просмотреть состояние режима входа и выхода.

Состояние входа и выхода

Можно просмотреть состояние входа события, тревожного выхода и пожарной тревоги.

Другие состояния

Можно просмотреть состояние турникета.

6.6.22 Управление записями в журналах

Можно искать и просматривать журналы устройства.

Перейдите в **Maintenance and Security → Maintenance → Log** («Техническое обслуживание и безопасность → Техническое 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.

6.6.23 Управление сертификатами

Помогает управлять сертификатами сервера / клиента и сертификатом CA.

Примечание

Данная функция поддерживается только у определенных моделей устройств.

Создание и установка самозаверенного сертификата

Шаги

1. Перейдите в меню **Maintenance and Security → Security → Certificate Management** («Техническое обслуживание и безопасность → Безопасность → Управление сертификатами»).
2. В области **Certificate Files** («Файлы сертификатов») выберите тип сертификата из выпадающего списка.
3. Нажмите **Create** («Создать»).
4. Введите информацию о сертификате.
5. Нажмите **OK**, чтобы сохранить и установить сертификат.

   Созданный сертификат отображается в области **Certificate Details** («Сведения о сертификате»). Сертификат будет сохранен автоматически.
6. Загрузите сертификат и сохраните его в запрашиваемом файле на локальном компьютере.
7. Отправьте запрашиваемый файл в центр сертификации на подпись.
8. Импортируйте подписанный сертификат.
   1) Выберите тип сертификата в области **Import Passwords** («Импорт паролей»), выберите сертификат на локальном компьютере и нажмите **Install** («Установить»).
   2) Выберите тип сертификата в области **Import Communication Certificate** («Импорт сертификата связи»), затем выберите сертификат на локальном компьютере и нажмите **Install** («Установить»).

Установка другого авторизованного сертификата

Если есть авторизованный сертификат (не созданный устройством), можно импортировать его напрямую на устройство.

Шаги

1. Перейдите в меню **Maintenance and Security → Security → Certificate Management** («Техническое обслуживание и безопасность → Безопасность → Управление сертификатами»).
2. В областях **Import Passwords** («Импорт паролей») и **Import Communication Certificate** («Импорт сертификата связи») выберите тип сертификата и загрузите сертификат.
3. Нажмите **Install** («Установить»).

Установка 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 **Import CA Certificate** («Импорт сертификата CA»).

   Примечание

   Идентификатор сертификата не может совпадать с идентификатором уже существующих сертификатов.
3. Загрузите файл сертификата с локального ПК.
4. Нажмите **Install** («Установить»).

Раздел 7 Настройка клиентского ПО

Можно позвонить на горячую линию, чтобы получить установочный пакет клиентского ПО iVMS-4200.

7.1 Схема настройки клиентского ПО

Следуйте приведенной ниже схеме для настройки клиентского ПО.

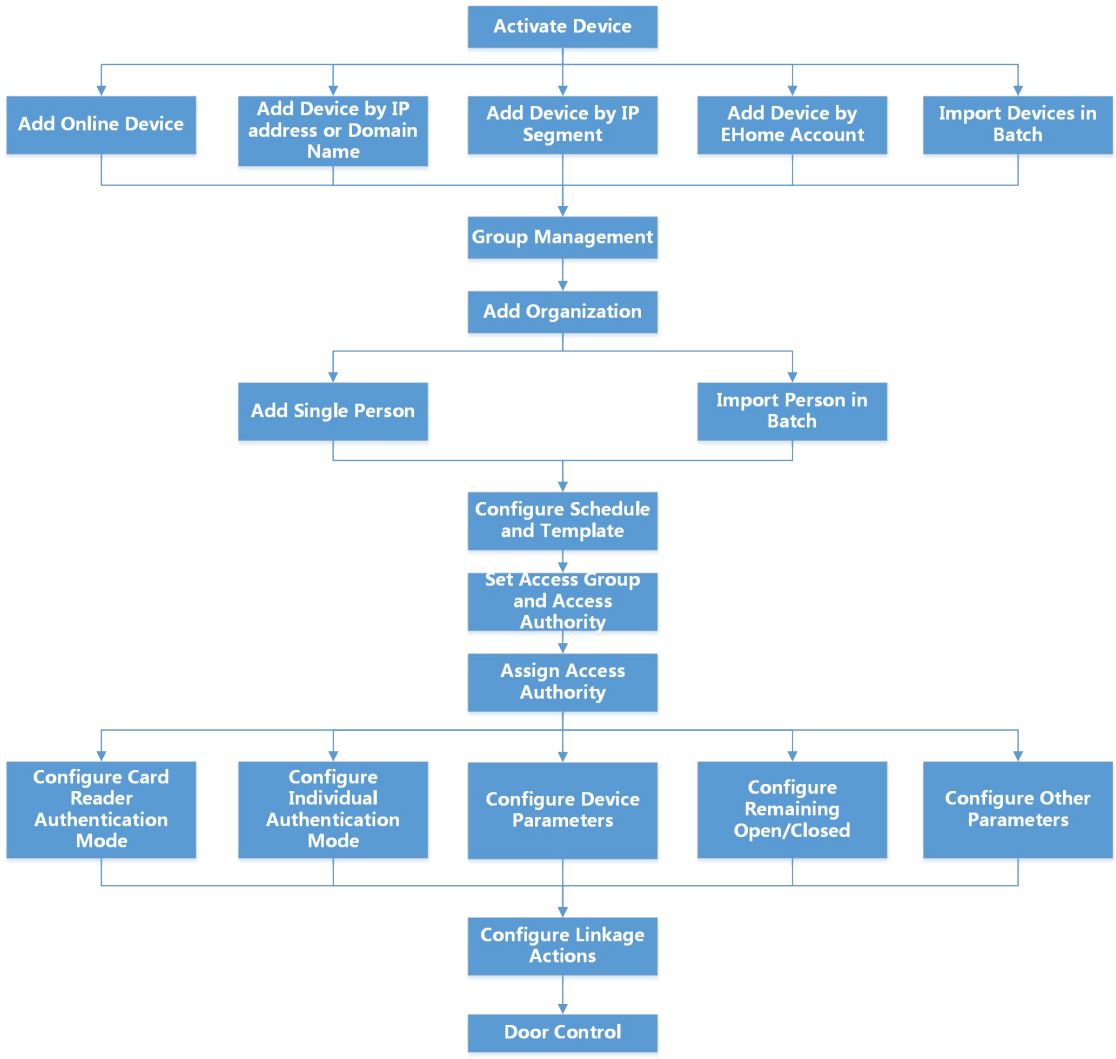


Рисунок 7-1 Схема настройки клиентского ПО

Английский язык	Русский язык
Activate Device	Активировать устройство
Add Online Device	Добавить устройство онлайн
Add Device by IP Address or Domain Name	Добавить устройство по IP-адресу или доменному имени
Add Device by IP Segment	Добавить устройство по сегменту IP-адреса
Add Device by EHome Account	Добавить устройство по учетной записи EHome
Import Devices in Batch	Импортировать устройства в пакетном режиме
Group Management	Управление группами
Add Organization	Добавить организацию
Add Single Person	Добавить одного пользователя
Import Person in Batch	Импорт пользователя в пакетном режиме
Configure Schedule and Template	Настроить расписание и шаблон
Set Access Group and Access Authority	Настроить группу доступа и права доступа
Assign Access Authority	Назначить права доступа
Configure Card Reader Authentication Mode	Настроить считыватель карт
Configure Individual Authentication Mode	Настроить индивидуальный режим аутентификации
Configure Device Parameters	Настроить параметры устройства
Configure Remaining Open / Closed	Настроить состояние «Оставить открытым / закрытым»
Configure Other Parameters	Настроить другие параметры
Configure Linkage Actions	Настроить действия привязки
Door Control	Управление дверью

7.2 Управление устройством

Поддержка устройств контроля доступа и устройств видеодомофонии.

Пример
После добавления устройств контроля доступа в клиентское ПО доступно управление въездом и выездом, управление УРВ, видеодомофония с использованием вызывной панели, установленной внутри или снаружи помещений.

7.2.1 Добавление устройства

Клиент предоставляет три режима добавления устройств, в том числе по IP, домену и сегменту IP. Также поддерживается импорт нескольких устройств в пакетном режиме, когда требуется добавить большое количество устройств.

Добавление устройства по IP-адресу или доменному имени

Если IP-адрес или доменное имя устройства известны, можно добавить устройство в клиентское ПО, указав IP-адрес (или доменное имя), имя пользователя, пароль и т. д.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. В верхней части правой панели нажмите вкладку **Device** («Устройство»).

   Добавленные устройства отображаются на панели справа.
3. Нажмите кнопку **Add** («Добавить»), чтобы открыть окно добавления устройства. Выберите режим добавления **IP/Domain** («IP-адрес / доменное имя»).
4. Введите необходимую информацию.

   Имя

   Создайте описательное название для устройства. Например, можно использовать название, которое отображает местоположение или функцию устройства.

   Адрес

   IP-адрес или доменное имя устройства.

   Порт

   Добавляемые устройства имеют одинаковый номер порта. Значение по умолчанию - **80**.

   Имя пользователя

   Введите имя пользователя устройства. По умолчанию имя пользователя — **Admin** («Администратор»).

   Пароль

   Введите пароль устройства.

   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 безопасным. Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг или конечного пользователя.
5. **Опционально.** Нажмите **Transmission Encryption (TLS)** («Шифрование передачи») для включения шифрования передачи, защищенной протоколом TLS (безопасность на транспортном уровне).

   Примечание

   - Устройство должно поддерживать данную функцию.
   - Если функция **Certificate Verification** («Проверка сертификата») включена, нажмите **Open Certificate Directory** («Открыть каталог сертификатов»), чтобы открыть папку по умолчанию, затем скопируйте файл сертификата, экспортированный с устройства, в этот каталог по умолчанию для повышения уровня безопасности.
   - Войдите в устройство, чтобы загрузить файл сертификата через веб-интерфейс.
6. Установите флажок **Synchronize Time** («Синхронизировать время»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО, после добавления устройства в клиентское ПО.

7. **Опционально.** Поставьте галочку в пункте **Import to Group** («Импортировать в группу»), чтобы создать группу по названию устройства. Также можно импортировать все каналы устройства в соответствующую группу.

   Пример

   Точки доступа, тревожные входы / выходы и каналы кодирования (при наличии) устройства контроля доступа будут импортированы в эту группу.
8. Завершите добавление устройства.
   - Нажмите **Add** («Добавить») для добавления устройств и возврата на страницу списка устройств.
   - Нажмите **Add and New** («Добавить и продолжить») для сохранения настроек и продолжения добавления других устройств.

Импорт устройств в пакетном режиме

Устройства можно добавлять в программное обеспечение в пакетном режиме, введя информацию о них в предварительно заданный файл CSV.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. В верхней части правой панели нажмите вкладку **Device** («Устройство»).
3. Нажмите кнопку **Add** («Добавить»), чтобы открыть окно добавления устройства. Выберите режим добавления **Batch Import** («Добавить в пакетном режиме»).
4. Нажмите **Export Template** («Скачать шаблон») и сохраните предварительно выбранный шаблон (файл CSV) на компьютере.
5. Откройте экспортированный файл шаблона и введите необходимую информацию об устройствах, подлежащих добавлению, в соответствующие столбцы.

Примечание

Более подробное описание обязательных полей представлено во введении.

Режим добавления

Введите ***0*** или ***1*** или ***2***.

Адрес

Измените адрес устройства.

Порт

Введите номер порта устройства. Номер порта по умолчанию: ***8000***.

Имя пользователя

Введите имя пользователя устройства. По умолчанию имя пользователя — **Admin** («Администратор»).

Пароль

Введите пароль устройства.

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 безопасным. Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг или конечного пользователя.

Импорт в группу

Введите ***1,*** чтобы создать группу по названию устройства. Все каналы устройства будут импортированы в соответствующую группу по умолчанию. Введите ***0***, чтобы отключить функцию.

6. Нажмите … и выберите файл шаблона.
7. Нажмите **Add** («Добавить»), чтобы импортировать устройства.

7.2.2 Сброс пароля устройства

Если пользователь забыл пароль обнаруженных онлайн устройств, пароль устройства можно сбросить через клиентское ПО.

Шаги

1. Откройте страницу **Device Management** («Управление устройством»).
2. Нажмите **Online Device** («Онлайн устройства»), чтобы отобразить область онлайн устройств.
   Все онлайн устройства, находящиеся в одной подсети, будут отображены в списке.
3. Выберите устройство из списка и нажмите в столбце **Operation** («Операции»).
4. Сбросьте пароль устройства.
   Нажмите **Generate** («Создать»), чтобы открыть окно QR-кода, затем нажмите **Download** («Загрузить»), чтобы сохранить QR-код на компьютере. Также можно сфотографировать QR-код и сохранить его на телефон. Отправьте изображение в нашу службу технической поддержки.

Примечание

Для выполнения следующих операций по сбросу пароля обратитесь в службу технической поддержки.

Предостережения

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 безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг или конечного пользователя.

7.2.3 Управление добавленными устройствами

После добавления устройств вы можете управлять добавленными устройствами, в том числе: редактировать параметры устройства, выполнять удаленную настройку устройства, просмотреть состояние устройства и т. д.

Таблица 7-1. Управление добавленными устройствами

Изменение устройства	Нажмите , чтобы изменить информацию устройства, включая имя устройства, адрес, имя пользователя, пароль и т. д.
Удаление устройства	Выберите одно или несколько устройств, нажмите **Delete** («Удалить») для удаления выбранных устройств.
Удаленная настройка	Нажмите , чтобы выполнить удаленную настройку соответствующего устройства. Подробная информация представлена в руководстве пользователя устройства.
Просмотр состояния устройства	Нажмите , чтобы просмотреть состояние устройства, включая наименование двери, номер, статус и т. д. **Примечание** Доступная информация о состоянии устройства зависит от модели фактического устройства.
Просмотр пользователей в сети	Нажмите , чтобы просмотреть подробную информацию о пользователях в сети, которые имеют доступ к устройству, включая имя пользователя, тип пользователя, IP-адрес и время входа в систему.
Обновление информации об устройстве	Нажмите , чтобы обновить и получить последнюю информацию об устройстве.

7.3 Управление группами

Клиентское ПО предоставляет области для управления добавленными ресурсами в разных группах. Ресурсы можно сгруппировать в разные группы в зависимости от расположения ресурсов.

Пример
Например, на первом этаже установлено 16 дверей, 64 тревожных входа и 16 тревожных выходов. Эти ресурсы можно организовать в одну группу (с именем «1-й этаж») для удобного управления. Можно контролировать состояние двери и выполнять другие операции с устройствами, объединив ресурсы по группам.

7.3.1 Добавление группы

Добавьте группы для удобного управления устройствами.

Шаги
1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device Management → Group** («Управление устройством→ Группа») для перехода на страницу управления группами.
3. Создайте группу.
   - Нажмите **Add Group** («Добавить группу») и введите желаемое название группы.
   - Нажмите **Create Group by Device Name** («Создать группу по названию устройства») и выберите добавленное устройство, чтобы создать новую группу по имени выбранного устройства.

   Примечание
   Ресурсы (такие как тревожные входы / выходы, точки доступа и т. д.) устройства будут импортированы в группу по умолчанию.

7.3.2 Добавление ресурсов в группу

Импортируйте ресурсы устройства (такие как тревожные входы / выходы, точки доступа и т. д.) в добавленную группу в пакетном режиме.

Перед началом
Добавьте группу для управления устройствами. Подробная информация представлена в разделе ***Добавление группы***.

Шаги
1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device Management → Group** («Управление устройством→ Группа») для перехода на страницу управления группами.
3. Выберите группу и тип ресурса из списка: **Access Point** («Точка доступа»), **Alarm Input** («Тревожный вход»), **Alarm Output** («Тревожный выход») и т. д.
4. Нажмите **Import** («Импорт»).
5. Выберите миниатюры / названия ресурсов для отображения в списке.

Примечание

Нажимайте и , чтобы переключать режим просмотра миниатюр или списка.

6. Нажмите **Import** («Импорт») для импорта выбранных ресурсов в группу.

7.4 Управление сотрудниками / посетителями

Добавьте информацию о сотруднике / посетителе в систему для дальнейших операций, таких как контроль доступа, видеодомофония, настройка времени, УРВ и т. д. Здесь можно управлять добавленными пользователями, например, выпускать карточки в пакетном режиме, импортировать и экспортировать информацию пользователя в пакетном режиме и т. д.

7.4.1 Добавление организации

Добавьте организацию и импортируйте информацию о сотруднике/посетителе в организацию для эффективного управления персоналом. Также можно добавить подчиненную организацию для добавленной организации.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Выберите головную организацию в левом столбце и нажмите **Add** («Добавить») в верхнем левом углу, чтобы добавить организацию.
3. Создайте имя для добавленной организации.

Примечание

Можно добавить до 10 уровней организаций.

4. **Опционально.** Выполните следующие операции.

Изменение организации

Наведите указатель мыши на добавленную организацию и нажмите , чтобы изменить ее название.

Удаление организации

Наведите указатель мыши на добавленную организацию и нажмите , чтобы удалить ее.

Примечание

- Организации нижнего уровня будут удалены, если удалить организацию верхнего уровня.
- Организация не может быть удалена, если ранее добавлены сотрудники.

Отображение персонала подчиненной организации

Нажмите **Show Persons in Sub Organization** («Отображение персонала подчиненной организации») и выберите организацию, чтобы показать персонал подчиненной организации.

7.4.2 Импорт и экспорт информации о сотруднике / посетителе

Можно импортировать информацию о нескольких пользователях в клиентское ПО в пакетном режиме. Также информацию о пользователях можно экспортировать и сохранить на компьютере.

Импорт информации о сотруднике / посетителе

Введите информацию о нескольких пользователях в предварительно настроенный шаблон (файл CSV / Excel) и импортируйте информацию в клиентское ПО в пакетном режиме.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Выберите добавленную организацию из списка и нажмите **Add** («Добавить») в верхнем левом углу, чтобы добавить организацию, затем выберите эту организацию.
3. Нажмите Import («Импорт»), чтобы открыть соответствующую панель.
4. Выберите значение **Person Information** («Информация о сотруднике / посетителе») в поле Importing Mode («Режим импортирования»).
5. Нажмите **Download Template for Importing Person** («Скачать шаблон для импорта данных сотрудника / посетителя»), чтобы скачать шаблон.
6. Введите информацию о пользователе в загруженный шаблон.

Примечание

- Если у пользователя несколько карт, отделите каждый номер карты точкой с запятой.
- Поля, отмеченные звездочкой, являются обязательными.
- По умолчанию **Hire Date** («Дата найма») является текущей датой.

- Нажмите , чтобы выбрать файл CSV / Excel с информацией о пользователе с локального ПК.

7. Нажмите **Import** («Импорт») для начала импорта.

Примечание

- Если номер пользователя уже существует в базе данных клиента, удалите существующую информацию перед импортом.
- Можно импортировать информацию не более 2000 пользователей.

Импорт изображений сотрудников / посетителей

После импорта изображений лиц в клиентское ПО, пользователи на изображениях могут быть идентифицированы с помощью терминала доступа с функцией распознавания лиц. Можно импортировать изображения пользователей по одному или импортировать несколько изображений одновременно.

Перед началом

Не забудьте заранее импортировать информацию о пользователе в клиентское ПО.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Выберите добавленную организацию из списка и нажмите **Add** («Добавить») в верхнем левом углу, чтобы добавить организацию, затем выберите эту организацию.
3. Нажмите **Import** («Импорт»), чтобы открыть соответствующую панель, затем выберите **Face** («Лицо»).
4. **Опционально.** Включите функцию **Verify by Device** («Проверка устройством»), чтобы проверить способность устройства распознавания лиц на клиентском ПО распознать лицо на фотографии.
5. Нажмите , чтобы выбрать файл с изображением лица.

Примечание

- Папка с изображениями лиц должна быть в формате ZIP.
- Изображение должно быть в формате JPG. Размер изображения не должен превышать 200 КБ.
- Название файла изображения должно формироваться в соответствии со следующим правилом: «Идентификатор сотрудника_Имя». Идентификатор пользователя должен совпадать с идентификатором импортированного пользователя.

6. Нажмите **Import** («Импорт») для начала импорта.
   Прогресс и результат импорта будут отображены на экране.

Экспорт информации о сотруднике / посетителе

Экспортируйте данные о добавленном пользователе на локальный ПК в формате CSV/Excel.

Перед началом

- Убедитесь, что пользователь добавлен в организацию.
- Убедитесь, что функция **Export Person Information** («Экспорт информации о сотруднике / посетителе») включена, тогда будет отображена кнопка **Export** («Экспорт»).
  Подробная информация представлена в соответствующем разделе.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. **Опционально.** Выберите организацию из списка.

Примечание

Если не выбрать конкретную организацию, будет экспортирована информация обо всех пользователях.

3. Нажмите **Export** («Экспорт»).
4. Введите имя суперпользователя и пароль для проверки. Отобразится панель экспорта.
5. Выберите **Person Information** («Информация о сотруднике / посетителе») для экспорта.
6. Выберите параметры, которые необходимо экспортировать.
7. Нажмите **Export** («Экспорт»), чтобы сохранить экспортированный файл в формате CSV/Excel на ПК.

Экспорт изображений сотрудников / посетителей

Экспортируйте файл с изображением лиц добавленных сотрудников и сохраните его на компьютере.

Перед началом

- Убедитесь, что пользователи и изображения их лиц добавлены в организацию.
- Убедитесь, что функция **Export Person Information** («Экспорт информации о сотруднике / посетителе») включена, тогда будет отображена кнопка **Export** («Экспорт»). Подробная информация представлена в соответствующем разделе.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. **Опционально.** Выберите организацию из списка.

   Примечание

   Если не выбрать конкретную организацию, будут экспортированы изображения лиц всех пользователей.
3. Нажмите **Export** («Экспорт») в главном меню.
4. Введите имя суперпользователя и пароль для проверки. Отобразится панель экспорта.
5. Выберите **Face** («Изображение лица») для экспорта.
6. Нажмите **Export** («Экспорт») и настройте ключ шифрования для шифрования экспортируемого файла.

   Примечание

   - Файл будет экспортирован в формате ZIP.
   - Название файла экспортированного изображения должно формироваться в соответствии со следующим правилом: «Идентификатор сотрудника_имя_0» («0» — для лица, видимого во всех деталях).

7.4.3 Получение информации о пользователе с устройства контроля доступа

Если устройство контроля доступа было дополнено информацией о пользователе (включая подробную информацию о пользователе, об отпечатках пальцев и выданной карте), данную информацию можно получить с устройства и импортировать ее в клиент для дальнейшей работы.

Шаги

Примечание

- Если в информации о пользователе, хранящейся на устройстве, в поле **Name** («Имя») не указаны данные, то это поле будет заполнено номером выданной карты после импорта в клиентское ПО.
- Если номер карты или идентификатор пользователя (идентификатор сотрудника), который хранится на устройстве, уже существует в клиентской базе данных, пользователь с таким номером карты или идентификатором не будет импортирован в клиентское ПО.

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Выберите организацию для импорта сотрудников.
3. Нажмите **Get from Device** («Получить из устройства»).
4. Выберите добавленное устройство контроля доступа или настольный считыватель карт из выпадающего списка.

Примечание

При выборе настольного считывателя карт, нажмите **Login** («Войти»), затем установите IP-адрес, номер порта, имя пользователя и пароль.

5. Выберите **Getting Mode** («Режим получения»).

Примечание

Режим получения может различаться в зависимости от устройства. Устройство контроля доступа поддерживает получение личной информации о пользователе с помощью ID сотрудника. Могут быть указаны до 5 ID сотрудников.

6. Нажмите **Import** («Импорт») для начала импорта информации о пользователе в клиент.

Примечание

Можно импортировать до 2000 пользователей и до 5000 карт.

Информация пользователя, включая подробную информацию, информацию об отпечатках пальцев (если настроены) и связанных картах (если настроены), будет импортирована в выбранную организацию.

7.4.4 Выдача карт сотрудникам в пакетном режиме

В клиентском ПО предусмотрена возможность выпустить сразу несколько карт в пакетном режиме.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. **Опционально.** Выберите группу пользователей и выберите пользователей, которым не выдана карта.
   - Выбранные пользователи без карт в группе будут отображаться на правой панели.
   - Если не выбирать пользователей без карты в группе, все добавленные пользователи без карт будут отображаться на правой панели.
3. Нажмите **Batch Issue Cards** («Выпуск карт в пакетном режиме»).
4. **Опционально.** Введите ключевое слово (имя или идентификатор пользователя) в поле ввода информации, чтобы выделить пользователей, для которых необходимо выпустить карты.
5. **Опционально.** Нажмите **Settings** («Настройки»), чтобы установить параметры выпуска карт. Подробная информация представлена в соответствующем разделе.
6. Нажмите **Initialize** («Инициализировать»), чтобы инициализировать считыватель карт и подготовить его к выдаче карт.
7. Нажмите на колонку **Card No.** («Номер карты») и введите номер карты.
   - Поместите карту на настольный считыватель.

- Считайте карту через считыватель карт.
- Вручную введите номер карты и нажмите клавишу ввода **Enter**. Карты будут выпущены для пользователей, отображаемых в списке.

7.4.5 Рапорт о потере карты

В случае утери карты необходимо сообщить о потере для деактивации доступа с помощью утерянной карты.

Шаги

1. Войдите в модуль **Person** («Сотрудник / посетитель»).
2. Выберите сотрудника, о потере карты которого необходимо сообщить, и нажмите **Edit** («Редактировать»), чтобы открыть соответствующее окно.
3. На панели **Credential → Card** («Учетные данные → Карта»), нажмите  на добавленную карту, чтобы изменить ее статус на **Lost card** («Утерянная карта»).

   После уведомления об утере карты авторизация доступа по этой карте будет недействительной и неактивной. Если картой решит воспользоваться другой пользователь, он не сможет получить доступ к дверям, используя утерянную карту.
4. **Опционально.** Нажмите  , чтобы отменить уведомление о потере карты, если карта найдена.

   После отмены уведомления об утере карты, авторизация доступа по этой карте будет действительной и активной.
5. Если утерянная карта добавлена в группу доступа, которая применена к устройству, после сообщения об утере карты или отмене уведомления об утере карты появится окно с уведомлением о необходимости применить изменения к устройству. После применения к устройству эти изменения будут задействованы на устройстве.

7.4.6 Настройка параметров выпуска карт

Предусмотрено два режима считывания номера карты: с помощью настольного считывателя карт или считывателя карт устройства контроля доступа. Подключите настольный считыватель карт к ПК, на котором работает клиент, через USB или COM-интерфейс, затем поместите карту на настольный считыватель карт. При отсутствии настольного считывателя карт считайте карту через считыватель карт добавленного устройства контроля доступа, чтобы получить номер карты. Перед выпуском карты для пользователя необходимо установить параметры выпуска карты, в том числе режим выпуска карт и сопутствующие параметры.

При добавлении карточки нажмите **Settings** («Настройки»), чтобы открыть соответствующее окно.

Локальный режим: выпуск карт с помощью настольного считывателя карт

Подключите настольный считыватель карт к ПК, на котором работает клиент. Поместите карту на настольный считыватель для получения номера карты.

Настольный считыватель карт

Выберите модель подключенного настольного считывателя карт.

Примечание

В настоящее время поддерживаются следующие модели считывателя карт: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

Тип карты

Это поле доступно только для моделей считывателя карт DS-K1F100-D8E или DS-K1F180-D8E.

Выберите тип карты: EM-карта или IC-карта в соответствии с фактическим типом карты.

Серийный интерфейс

Это поле доступно только для модели считывателя карт DS-K1F100-M. Выберите COM-интерфейс, к которому будет подключен настольный считыватель карт.

Бипер

После успешного считывания номера карты включите или выключите бипер.

Тип номера карты

Выберите необходимый тип номера карты.

Шифрование M1-карты

Это поле доступно только для моделей считывателя карт DS-K1F100-D8, DS-K1F100-D8E или DS-K1F180-D8E.

Если используется карта M1 и нужно активировать функцию ее шифрования, выберите соответствующий сектор.

Удаленный режим: выпуск карт с помощью считывателя карт

Выберите устройство контроля доступа, добавленное в клиент, и считайте карту через считыватель карт, чтобы получить ее номер.

7.5 Настройка графиков и шаблонов

Настройте шаблон, в том числе недельный график работы и график выходных дней. После настройки шаблона, его можно использовать для настройки групп доступа, чтобы настройки указанной группы доступа были действительны во время действия шаблона.

Примечание

Подробная информация о настройке группы контроля доступа представлена в разделе ***Настройка группы контроля доступа для назначения разрешений на доступ***.

7.5.1 Добавление выходного дня

Здесь можно установить выходные дни и настроить параметры выходных дней, в том числе дату начала, дату окончания и продолжительность указанного периода.

Шаги

Примечание

Можно добавить до 64 групп выходных дней.

1. Нажмите **Access Control → Schedule → Holiday** («Контроль доступа → Графики → Выходные дни»), чтобы перейти на соответствующую страницу.
2. На панели слева нажмите **Add** («Добавить»).
3. Создайте название для выходного дня.
4. **Опционально.** Введите описание или уведомления об этом выходном дне в поле **Remark** («Замечания»).
5. Добавьте период и настройте продолжительность выходных дней.

   Примечание

   Для одной группы выходного дня можно добавить до 16 периодов.

   1) Нажмите **Add** («Добавить») в поле списка выходных дней.
   2) Двигайте курсор, чтобы указать временной интервал. Для данного периода времени будет активировано настроенное разрешение.

      Примечание

      Для одного периода выходных может быть установлено до 8 временных интервалов.

   3) **Опционально.** Для изменения временных интервалов выполните следующие действия.
      - Когда вид курсора изменится на  , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.
      - Наведите курсор на временную шкалу и измените время начала / окончания периода в появившемся диалоговом окне.
      - Когда вид курсора изменится на  , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
   4) **Опционально.** Выберите отрезок времени, который необходимо удалить, а затем нажмите  в столбце **Operation** («Операции»), чтобы удалить его.
   5) **Опционально.** Нажмите  , чтобы удалить все отрезки времени нерабочих дней.
   6) **Опционально.** Нажмите  , чтобы удалить конкретный нерабочий день.
6. Нажмите **Save** («Сохранить»).

7.5.2 Добавление шаблона

Шаблон может содержать недельный график работы и график выходных дней. Установите недельный график работы и назначьте время авторизации доступа для конкретного пользователя или группы. Также можно выбрать добавленные выходные дни и включить их в шаблон.

Шаги

Примечание

Можно добавить до 255 шаблонов.

1. Нажмите **Access Control → Schedule → Template** («Контроль доступа → Графики → Шаблон»), чтобы перейти на соответствующую страницу.

Примечание

По умолчанию предусмотрено два вида шаблонов: **All-Day Authorized** («Авторизован в течение всего дня») и **All-Day Denied** («Доступ запрещен в течение всего дня»). Указанные шаблоны не подлежат редактированию или удалению.

Авторизован в течение всего дня

Авторизация действует в каждый день недели и не предусматривает выходных дней.

Доступ запрещен в течение всего дня

Авторизация не действует в течение недели и не предусматривает выходных дней.

2. На панели слева нажмите **Add** («Добавить»), чтобы создать новый шаблон.
3. Создайте имя для шаблона.
4. Введите описание или уведомления об этом шаблоне в поле **Remark** («Замечания»).
5. Внесите изменения в недельный график и примените их к шаблону.
   1) Перейдите на вкладку **Week Schedule** («Недельный график работы») на панели снизу.
   2) Выберите день недели и укажите продолжительность на шкале времени.

Примечание

Для каждого дня в недельном графике может быть установлено до 8 временных интервалов.

   3) **Опционально.** Для изменения временных интервалов выполните следующие действия.
      - Когда вид курсора изменится на  , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.
      - Наведите курсор на временную шкалу и измените время начала / окончания периода в появившемся диалоговом окне.
      - Когда вид курсора изменится на  , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
   4) Повторите два последних действия выше, чтобы задать несколько временных интервалов в другие дни недели.
6. Добавьте выходной день и примените его к шаблону.

Примечание

В один шаблон можно добавить до 4 выходных дней.

   1) Нажмите на вкладку **Holiday** («Выходной день»).
   2) Выберите выходной день из списка слева, чтобы добавить его в выбранный список на панели справа.
   3) **Опционально.** Нажмите **Add** («Добавить») для добавления нового выходного.

Примечание

Подробная информация о добавлении выходного дня представлена в разделе ***Добавление выходного дня***.

   4) **Опционально.** Выберите выходной день и нажмите  , чтобы удалить его, или нажмите **Clear** («Очистить»), чтобы удалить все выбранные выходные дни из списка справа.

7. Нажмите **Save** («Сохранить») для сохранения настроек и завершите добавление шаблона.

7.6 Настройка группы контроля доступа для назначения разрешений на доступ

После добавления пользователя и настройки его учетных данных можно создать группы контроля доступа, чтобы предоставить доступ к дверям для определенных пользователей. После этого необходимо применить группу контроля доступа к устройству контроля доступа, чтобы измененные настройки были задействованы.

Шаги

После изменения настроек группы доступа необходимо снова применить эти группы доступа к устройствам, чтобы изменения вступили в силу. Изменения в группе доступа включают в себя изменения шаблона, настроек группы доступа, настроек группы доступа пользователя и сведений о связанных лицах (включая № карты, отпечатки пальцев, изображения лиц, привязку № карты и отпечатков пальцев, пароль карты, срок действия карты и др.).

1. Нажмите **Access Control → Authorization → Access Group** («Контроль доступа → Авторизация → Группа доступа»), чтобы перейти на соответствующую страницу.

2. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.

3. В текстовом поле **Name** («Имя») введите имя для группы доступа по своему выбору.

4. Выберите шаблон для группы доступа.

Примечание

Необходимо настроить шаблон перед настройкой группы доступа. Подробная информация представлена в разделе ***Настройка графиков и шаблонов.***

5. В списке слева поля **Select Person** («Выбрать пользователя») выберите пользователей, которым необходимо назначить разрешения на доступ.

6. В списке слева поля **Select Person** («Выбрать пользователя») выберите двери, вызывные панели и этажи, к которым будут иметь доступ выбранные пользователи.

7. Нажмите **Save** («Сохранить»).

Выбранные пользователи и точки доступа отображаются в правой части экрана.

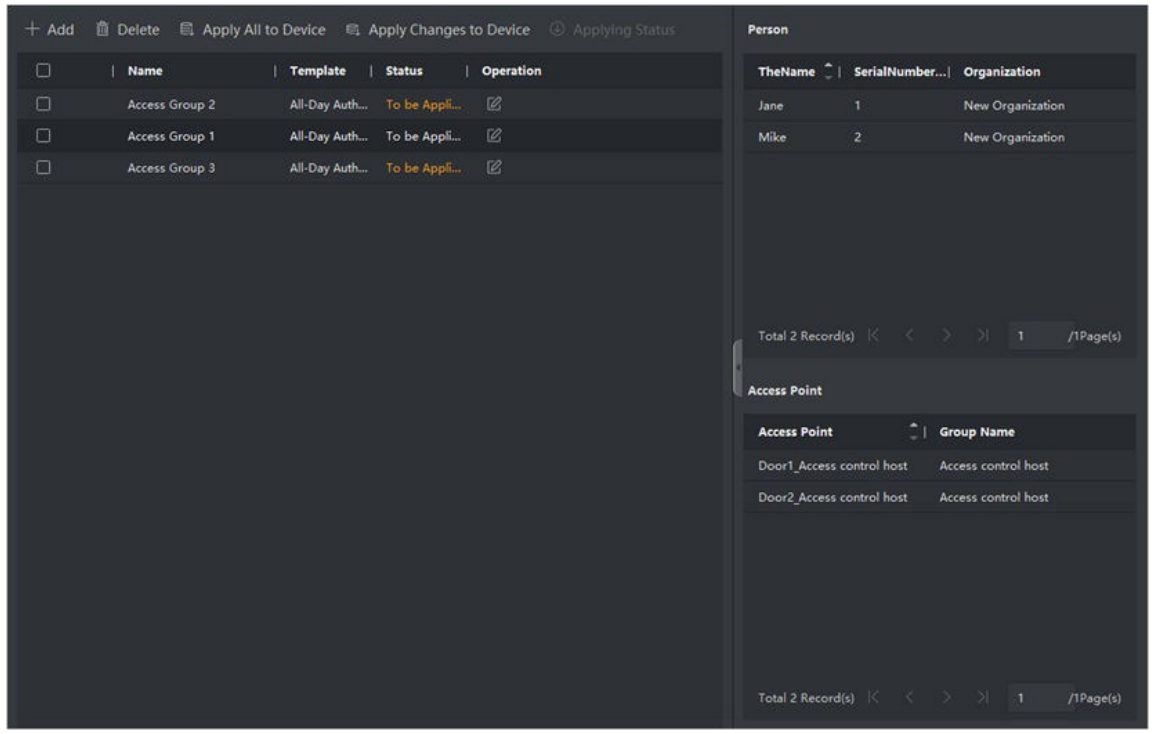


Рисунок 7-2. Отображение выбранных пользователей и точек доступа

8. После добавления группы доступа необходимо применить их к устройству контроля доступа, чтобы изменения были задействованы.

1) Выберите группы доступа, которые необходимо применить к устройству контроля доступа.
2) Нажмите **Apply to Devices** («Применить к устройствам») для начала применения выбранных групп доступа к устройству контроля доступа или вызывной панели.
3) Нажмите **Apply to Devices** («Применить к устройствам») или **Apply Changes to Devices** («Применить изменения к устройствам»).

   Применить к устройствам

   Операция очистит все группы доступа, привязанные к выбранным устройствам, а затем задаст новую группу доступа.

   Применить изменения к устройствам

   Операция не очистит группы доступа, привязанные к выбранным устройствам, и применит только измененную часть выбранных групп доступа к устройству.
4) Присвоенный статус отображается в столбце Status («Статус»). Также можно нажать **Applying Status** («Присвоенный статус»), чтобы просмотреть все примененные группы доступа.

Примечание

Выберите **Display Failure Only** («Отображать только ошибки») для фильтрации примененных изменений.

Выбранные пользователи будут иметь разрешения на вход/выход через выбранные двери/вызывные панели при помощи привязанных карт.

9. Опционально. При необходимости нажмите для редактирования групп доступ.

Примечание

При изменении информации о доступе пользователя или другой связанной информации появится предупреждение **Access Group to Be Applied** («Применить группу доступа») в правом углу.
Нажмите на подсказку для применения изменений к устройству. Выберите **Apply Now** («Применить сейчас») или **Apply Later** («Применить позже»).

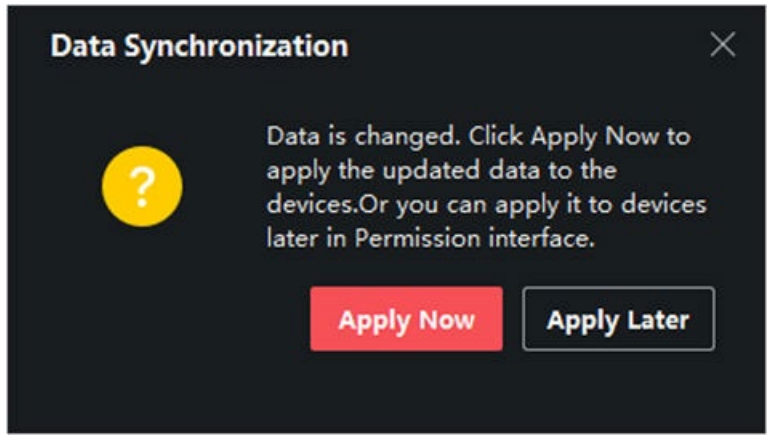


Рисунок 7-4. Синхронизация данных

7.7 Настройка расширенных функций

Настройте расширенные функции контроля доступа в соответствии со сценой наблюдения.

Примечание

- При использовании функций, связанных с картами (с картами контроля доступа), во время добавления карт будут перечислены только карты с примененной группой доступа.
- Устройство должно поддерживать возможность использования расширенных функций.
- Наведите курсор на **Advanced Function** («Расширенные функции»), затем нажмите для настройки расширенной функции.

7.7.1 Настройка параметров

После добавления устройства контроля доступа можно настроить параметры устройства контроля доступа и точки управления доступом.

Настройка параметров устройства контроля доступа

После добавления устройства контроля доступа можно настроить его параметры, в том числе наложить пользовательскую информацию на изображение, загрузить изображения после захвата, сохранить захваченные изображения и т. д.

Перед началом
Добавьте устройство контроля доступа в клиент.

Шаги
1. Нажмите **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»).

Примечание
Выберите **Device Parameter** («Параметры устройства») в списке расширенных функций, наведите курсор, а затем отобразите параметры устройства.

2. Выберите устройство контроля доступа, чтобы отобразить его параметры на странице справа.
3. Нажмите **ON** («Вкл.»), чтобы включить соответствующую функцию.

Примечание
- Отображаемые параметры могут различаться в зависимости от устройства контроля доступа.
- Некоторые из следующих параметров не перечислены на странице **Basic Information** («Основная информация»), нажмите **More** («Дополнительная информация»), чтобы изменить параметры.

Включение распознавания NFC-карт

После активации этой функции устройство сможет распознавать NFC-карты. Поднесите NFC-карту к устройству.

Включение распознавания M1-карт

После активации этой функции устройство сможет распознавать M1-карты. Поднесите M1-карту к устройству.

Включение распознавания EM-карт

После активации этой функции устройство сможет распознавать EM-карты. Поднесите EM-карту к устройству.

4. Нажмите **OK**.
5. **Опционально.** Нажмите **Copy to** («Копировать в...») и выберите устройство контроля доступа, чтобы копировать параметры, указанные на странице, на выбранное устройство.

Настройка параметров дверей / лифтов

После добавления устройства контроля доступа можно настроить параметры точек доступа (дверь или этаж).

Перед началом
Добавьте устройство контроля доступа в клиент.

Шаги

1. Нажмите **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»).
2. Выберите устройство контроля доступа на панели слева, а затем нажмите , чтобы показать двери или этажи выбранного устройства.
3. Выберите дверь или этаж, чтобы отобразить его параметры в правой части экрана.
4. Измените параметры двери или этажа.

Примечание

- Отображаемые параметры могут различаться в зависимости от устройства контроля доступа.
- Некоторые из следующих параметров не перечислены на странице **Basic Information** («Основная информация»), нажмите **More** («Дополнительная информация»), чтобы изменить параметры.

Имя

Выберите наименование считывателя карт по своему выбору.

Тип кнопки выхода

Установите кнопку выхода в режим **Remaining closed** («Оставить открытым») или **Remaining open** («Оставить закрытым»). По умолчанию активирован режим **Remaining open** («Оставить закрытым»).

Длительность открытого состояния

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

5. Нажмите **OK**.
6. **Опционально.** Нажмите **Copy to** («Копировать в...») и выберите двери / этажи, чтобы копировать параметры, указанные на странице, и применить их к выбранным дверям / этажам.

Примечание

Настройки состояния двери и этажа будут также применены к выбранной двери.

Настройка параметров считывателя карт

После добавления устройства контроля доступа можно настроить параметры его считывателя карт.

Перед началом

Добавьте устройство контроля доступа в клиент.

Шаги

1. Нажмите **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»).
2. Нажмите кнопку ▶ в списке устройств, расположенном слева, чтобы развернуть на экране информацию о двери, и выберите название устройства для считывания карт.
3. Затем измените основные параметры данного устройства, приведенные на соответствующей странице.

Примечание

- Отображаемые параметры могут различаться в зависимости от устройства контроля доступа. Ниже приведены некоторые параметры. Подробная информация представлена в руководстве пользователя устройства.
- Некоторые из следующих параметров не перечислены на странице **Basic Information** («Основная информация»), нажмите **More** («Дополнительная информация»), чтобы изменить параметры.

Имя

Выберите наименование считывателя карт по своему выбору.

Интервал аутентификации карты

Временной интервал между двумя циклами распознавания карты при непрерывной работе.

Интервал повторной аутентификации

В течение указанного интервала повторная аутентификация одного и того же номера карты (загруженной с разных устройств) недействительна. Выполняется только одна аутентификация.

Активировать предел неудачных попыток аутентификации / достижение максимального количества неудачных попыток аутентификации

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

Тип считывателя карт / Описание считывателя карт

Просмотр типа и описания считывателя карт. Доступны только для чтения.

4. Нажмите **OK**.
5. **Опционально.** Нажмите **Copy to** («Копировать в...») и выберите считыватель карт, чтобы копировать параметры, указанные на странице, на выбранное устройство.

Настройка параметров тревожного выхода

Настройте параметры тревожного выхода после добавления устройства контроля доступа.

Перед началом

Добавьте устройство контроля доступа в клиент и убедитесь, что устройство поддерживает тревожный выход.

Шаги

1. Нажмите **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»), чтобы перейти на соответствующую страницу.
2. Нажмите кнопку в списке устройств, расположенном слева, чтобы развернуть на экране информацию о двери, выберите тревожный вход и настройте его параметры на панели справа.
3. Настройте параметры тревожного выхода.

   Имя

   Выберите наименование считывателя карт по своему выбору.

   Время работы тревожного выхода

   Время работы тревожного выхода после активации.
4. Нажмите **OK**.
5. **Опционально.** Установите переключатель в верхнем правом углу в положение ON («Вкл.»), чтобы активировать тревожный выход.

Настройка параметров контроллера турникета

После добавления контроллера турникета в клиент, можно настроить его параметры для прохождения турникета.

Перед началом
Добавьте устройство контроля доступа в клиент.

Шаги

1. Перейдите на вкладку **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Дополнительные функции → Параметр устройства»), чтобы перейти на страницу настроек параметров.
2. Нажмите кнопку в списке устройств слева, выберите считыватель карт и измените его параметры справа.
3. Измените параметры.

   Режим прохода

   Выберите контроллер, который будет контролировать состояние турникета.

   Длительность звукового предупреждения

   Настройка длительности звукового предупреждения при тревоге.

   Примечание

   Если установлено значение 0, звук тревоги будет воспроизводиться до отключения тревоги.

   Единица измерения температуры

   Выберите единицу измерения температуры, отображаемую в статусе устройства.

   Яркость световой панели

   Настройте яркость подсветки устройства.

Режим памяти

При включении режима памяти допускается предъявление нескольких карт для прохождения нескольких сотрудников / посетителей. Когда количество проходящих сотрудников / посетителей превышает количество предъявленных карт или после того, как последний сотрудник / посетитель проходит, а другие люди не проходят в течение времени открытия, турникет закроется автоматически.

4. Нажмите **OK**.

7.7.2 Настройка дополнительных параметров

После добавления устройства контроля доступа можно настроить параметры его сети.

Настройка параметров RS-485

Установите параметры RS-485 устройства контроля доступа, включая скорость передачи данных, бит данных, стоповый бит, тип контроля четности, тип управления потоком, режим связи, режим работы и режим соединения.

Перед началом
Добавьте устройство контроля доступа в клиент и убедитесь, что устройство поддерживает RS-485.

Шаги

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа в списке устройств и нажмите **RS-485**, чтобы открыть страницу настроек RS-485.
4. Из выпадающего списка выберите номер серийного интерфейса, чтобы настроить параметры RS-485.
5. Настройте скорость передачи данных, бит данных, стоповый бит, тип четности и режим соединения из всплывающего списка.
6. Нажмите **Save** («Сохранить»).
   - Настроенные параметры будут автоматически применены к устройству.
   - При изменении режима подключения устройство автоматически перезагрузится.

Включить шифрование M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

Шаги

Примечание
Устройство контроля доступа и считыватель карт должны поддерживать данную функцию.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).

Примечание

3. Выберите устройство контроля доступа в списке устройств и нажмите **M1 Card Encryption** («Шифрование карты M1»), чтобы открыть страницу «Шифрование карты M1».
4. Установите переключатель в положение **On** («Вкл.»), чтобы включить функцию шифрования M1-карты.
5. Установите идентификатор сектора.

   Диапазон яркости от 1 до 100.
6. Нажмите **Save** («Сохранить») для сохранения настроек.

7.8 Управление состоянием двери

Состояние двери добавленного устройства контроля доступа будет отображаться в режиме реального времени в модуле **Monitoring** («Мониторинг») добавленного устройства контроля доступа. Также можно управлять дверьми, например, открывать / закрывать дверь или оставлять дверь открытой / закрытой удаленно через клиентское ПО. События доступа отображаются в этом модуле в режиме реального времени. Здесь можно просматривать информацию о допуске и данные пользователей.

Примечание

Пользователь с разрешением на управление дверью может войти в модуль мониторинга и осуществлять управление дверьми. Для других пользователей панель управления устройством отображаться не будет. Подробная информация о настройке разрешения пользователя представлена в разделе ***Управление пользователями*** .

7.8.1 Управление состоянием двери

Можно контролировать состояние двери (дверей): разблокировать / заблокировать, оставить дверь разблокированной / заблокированной, оставить все двери разблокированными и т. д.

Перед началом

- Добавьте сотрудника / посетителя и назначьте уровень доступа, тогда у сотрудника / посетителя будет право доступа к точкам доступа (дверям). Подробная информация представлена в разделах ***Управление сотрудниками*** и ***Настройка группы доступа для назначения разрешений на доступа***.
- Убедитесь, что у пользователя есть разрешение выполнять операции с точками доступа (двери).

Шаги

1. Нажмите **Monitoring** («Мониторинг») для перехода на соответствующую страницу.
2. В правом верхнем углу выберите группу точки доступа.

   Примечание

   Подробная информация об управлении группой точек доступа представлена в разделе ***Управление группами***.

   На экране будут отображены двери в выбранной группе контроля доступа.

3. Нажмите значок двери, чтобы выбрать ее, или нажмите **Ctrl** и выберите несколько дверей.

При активированных опциях **Remain All Unlocked** («Оставить все двери разблокированными») и **Remain All Locked** («Оставить все двери заблокированными») этот шаг пропускают.

4. Нажимайте следующие кнопки, чтобы управлять дверью.

Разблокировка двери

Разблокируйте дверь, чтобы открыть ее на определенный промежуток времени. По истечении заданного времени дверь будет автоматически заблокирована.

Блокировка двери

Когда дверь открыта, заблокируйте ее. Пользователь с соответствующим разрешением может получить доступ к двери с помощью учетных данных.

Оставить разблокированной

Дверь будет разблокирована (из открытого или закрытого состояния). Для доступа к двери не требуется предъявление учетных данных.

Оставить заблокированной

Дверь будет закрыта и заблокирована. Дверь будет недоступна даже для пользователей с соответствующими разрешениями, за исключением суперпользователей.

Все двери остаются разблокированными

Все двери из группы будут разблокированы (из открытого или закрытого состояния). Для доступа к двери не требуется предъявление учетных данных.

Все двери остаются заблокированными

Все двери из группы будут закрыты и заблокированы (из открытого или закрытого состояния). Дверь будет недоступна даже для пользователей с соответствующими разрешениями, за исключением суперпользователей.

Захват

Захват изображения вручную.

Примечание

Кнопка **Capture** («Захват») доступна, когда устройство поддерживает функцию захвата изображений. Изображение сохраняется на компьютере, на котором работает клиентское ПО.

Удаленное открытие через вызывную панель

Если в группу входят вызывные панели, можно выбрать **Lock1** («Замок 1») или **Lock2** («Замок 2»), а затем нажать **Unlock Door** («Разблокировать дверь»), чтобы разблокировать дверь через вызывную панель.

По умолчанию **Lock1** («Замок 1») выбран для вызывных панелей.

Обновление состояния

Нажмите **Refresh Status** («Обновить состояние»), чтобы узнать актуальное состояние двери.

Результат

Иконки дверей изменятся в режиме реального времени, если операция завершена успешно.

7.8.2 Проверка записей о считывании карт в режиме реального времени

Информация о считывании карт в режиме реального времени, распознавании лиц, поверхностной температуре тела и другое будет отображаться в клиенте. Кроме того, можно просматривать личную информацию пользователя и изображение, захваченное во время доступа.

Перед началом

В клиент добавлен сотрудник и устройство контроля доступа. Подробная информация представлена в разделах ***Управление пользователями*** и ***Добавление устройства***.

Шаги

1. Нажмите **Monitoring** («Мониторинг») для перехода в соответствующий модуль.

   Записи доступа в режиме реального времени отображаются внизу страницы. Можно посмотреть записанные сведения, включая номер карты, имя сотрудника, время события, местоположение двери, температуру, тип аутентификации и т. д.

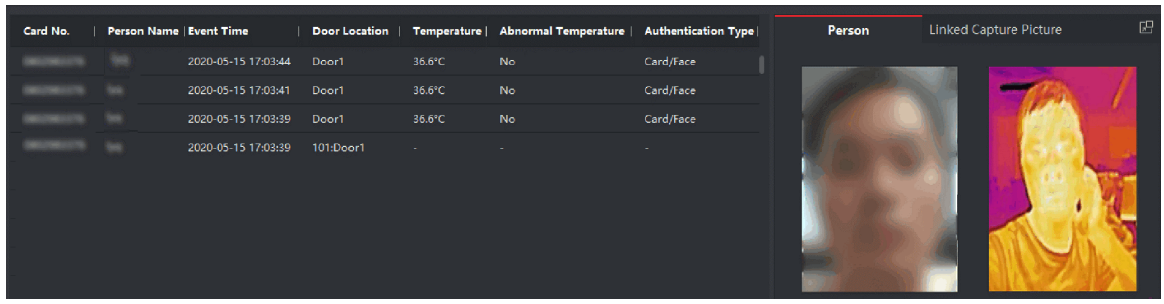


Рисунок 7-5. Записи доступа в режиме реального времени

Примечание

Нажмите правой кнопкой мыши на название колонки события доступа в таблице, чтобы отобразить или скрыть колонку.

2. **Опционально.** Выберите группу записей доступа из раскрывающегося списка в правом верхнем углу, чтобы отобразить записи доступа в режиме реального времени для выбранной группы.
3. **Опционально.** Проверьте тип и состояние события.

   Обнаруженные события, тип и состояние которых не установлены, не будут отображаться в списке.
4. **Опционально.** Поставьте галочку **Show Latest Event** («Показать последнее событие»), чтобы посмотреть последнюю запись доступа. Список записей будет указан в обратном хронологическом порядке.
5. **Опционально.** Поставьте галочку **Enable Abnormal Temperature Prompt** («Включить предупреждение об аномальной температуре»), чтобы включить предупреждение об аномальной поверхностной температуре тела.

Примечание

Если этот параметр включен, при появлении информации об аномальной температуре при входе в модуль мониторинга появляется всплывающее окно, в котором отображается фотография человека, температура поверхности тела, номер карты, имя человека и т. д.

6. **Опционально.** Нажмите на событие, чтобы посмотреть фотографии сотрудников (включая захваченное изображение и профиль).

Примечание

В поле **Linked Capture Picture** («Привязанные захваченные изображения») двойным нажатием можно увеличить захваченное изображение.

7. **Опционально.** Можно посмотреть детали (включая подробную информацию о сотруднике и захваченное изображение).

Примечание

Во всплывающем окне можно просмотреть сведения в полноэкранном режиме

Приложение A. DIP-переключатели

A.1 Описание DIP-переключателя

DIP-переключатель расположен на плате контроля доступа. Расположение переключателей № 1 и № 2 означает расположение от младшего бита к старшему.

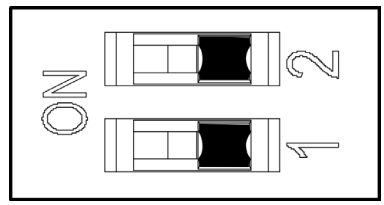


Рисунок A-1. DIP-переключатель

Когда переключатель находится в положении **ON** («ВКЛ.»), это означает, что переключатель включен, в противном случае переключатель выключен.

Приложение B. Описание конфигурации кнопок

Подробная информация о настройке устройства с помощью кнопки платы контроля прохода представлена в таблице ниже.

Номер конфигурации уровня 1	Описание	Номер конфигурации уровня 1 и функции
3	Режим прохода	1-Контроль обеих сторон. **Примечание** По умолчанию на экране будет отображаться 1. 2-Контролируемый вход; выход запрещен 3-Контролируемый вход; выход свободный 4-Свободный проход с обеих сторон 5-Вход свободный; контролируемый выход 6-Вход свободный; выход запрещен 7 Проход с обеих сторон запрещен 8-Вход запрещен; контролируемый выход 9-Вход запрещен; свободный выход
4	Режим памяти	1 Выключить 2 Включить **Примечание** По умолчанию на экране будет отображаться 2.
9	Продолжительность входа	От 5 до 5 с, от 6 до 6 с, от 7 до 7 с ... от 60 до 60 с **Примечание** По умолчанию на экране будет отображаться 5.
10	Продолжительность выхода	От 5 до 5 с, от 6 до 6 с, от 7 до 7 с ... от 60 до 60 с

Номер конфигурации уровня 1	Описание	Номер конфигурации уровня 1 и функции
		Примечание По умолчанию на экране будет отображаться 5.
39	Яркость подсветки	От 0 до 0, от 1 до 1, от 2 до 2 … от 10 до 10 **Примечание** По умолчанию на экране будет отображаться 6.
42	Очищение подсчета сотрудников / посетителей	1 Выключить 2 Включить **Примечание** По умолчанию на экране будет отображаться 1.
43	Тип противопожарной защиты	1 Оставить закрытым 2 Оставить открытым **Примечание** По умолчанию на экране будет отображаться 2.
99	Восстановление настроек по умолчанию	1 Выключить 2 Включить **Примечание** По умолчанию на экране будет отображаться 1.

Приложение C. Событие и тип тревоги

Событие	Тип тревоги
Время прохода истекло	—

Приложение D. Описание ошибок

При возникновении ошибки турникет отобразит код ошибки на семисегментном дисплее. В представленной ниже таблице описан каждый код ошибки.

Причина ошибки	Код	Причина ошибки	Код
Дополнительная плата в автономном режиме (если плата не установлена, появится код ошибки «49» или «59», но устройство работает нормально)	49/59	Препятствие	55
Исключение кодера	57	Исключение привода	58


See Far, Go Further