



Турникет с тремя штангами серии F-TG-330

Руководство пользователя

Инструкция по технике безопасности

Эта инструкция предназначена для того, чтобы пользователь мог использовать продукт правильно и избежать опасности или причинения вреда имуществу.

Меры предосторожности разделены на «Предупреждения» и «Предостережения».

Предупреждение: игнорирование любого из предупреждений может привести к серьезным травмам или смерти.

Предостережение: игнорирование любого из предостережений может привести к травмам или порче оборудования.

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

Предупреждения:

- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в регионе эксплуатации.
- Используйте адаптер питания соответствующей компании. Потребляемая мощность не может быть меньше требуемого значения.
- Не подключайте несколько устройств к одному блоку питания, перегрузка адаптера может привести к перегреву или возгоранию.
- Прежде чем подключать, устанавливать или разбирать устройство, убедитесь, что питание отключено.
Если для технического обслуживания необходимо открыть верхние крышки и включить устройство, то:
 - Отключите кулер, чтобы оператор не получил травму.
 - Не прикасайтесь к оголенным компонентам под высоким напряжением.
 - 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 или ее перемещения в какую-либо часть тела, немедленно обратитесь за медицинской помощью.

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

Предостережения

- 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. Если требуется более высокий уровень безопасности, используйте несколько режимов аутентификации.
 - 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 УСТАНОВЛИВАТЬ НА БЕТОННУЮ ПОВЕРХНОСТЬ ИЛИ НА ДРУГИЕ ПОВЕРХНОСТИ, НЕ ПОДВЕРГАЕМЫЕ ВОСПЛАМЕНЕНИЮ.
 - Необходимо подключить провод защитного заземления оборудования к проводу защитного заземления установки.

Содержание

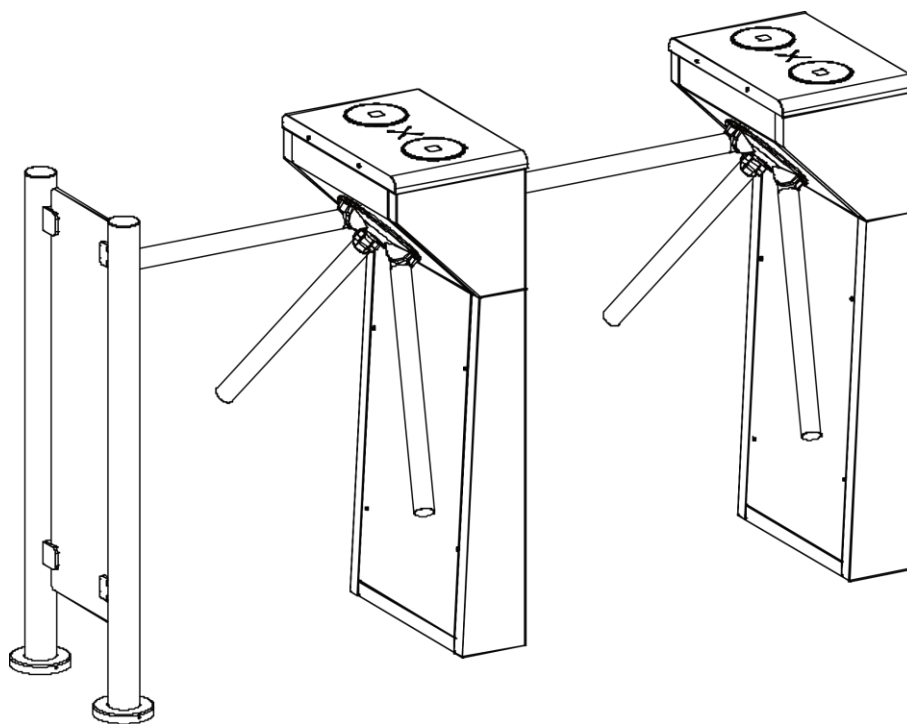
Раздел 1 Представление продукта	1
1.1 Введение.....	1
1.2 Основные функции	1
Раздел 2 Подключение системы.....	2
Раздел 3 Установка тумб	4
Раздел 4 Основные подключения	6
4.1 Компоненты	6
4.2 Подключение питания	7
Раздел 5 Описание разъемов	9
5.1 Общая схема подключения	9
5.2 Описание разъемов платы управления полосой движения	10
5.3 Описание разъемов платы контроля доступа (опционально)	12
5.4 Описание разъемов основной дополнительной платы (опционально)	14
5.5 Считыватель карт.....	15
5.6 Подключение RS-485.....	15
5.7 Подключение тревожного входа	16
5.8 Подключение кнопки выхода.....	17
Раздел 6 Настройка устройства с помощью кнопки	18
6.1 Конфигурация с помощью кнопки.....	18
6.2 Инициализация устройства	20
Раздел 7 Активация	22
7.1 Активация через веб-интерфейс	22
7.2 Активация через мобильный веб-интерфейс.....	23
7.3 Активация через ПО SADP	23
7.4 Активация устройства при помощи клиентского ПО iVMS-4200	25
Глава 8 Работа через веб-интерфейс	26
8.1 Вход в систему	26
8.2 Забыть пароль.....	26
8.3 Быстрые операции через веб-интерфейс.....	27

8.3.1 Настройка времени	27
8.4 Управление пользователями	27
8.5 Турникет.....	29
8.5.1 Обзор.....	29
8.5.2 Поиск событий	29
8.5.3 Настройки параметров контроля доступа	30
8.5.4 Турникет	36
8.6 Система и обслуживание.....	39
8.6.1 Отображение информации об устройстве.....	39
8.6.2 Настройка времени	40
8.6.3 Изменение пароля администратора	41
8.6.4 Пользователи онлайн	41
8.6.5 Просмотр информации о постановке / снятии устройства с охраны через веб-интерфейс ПК	41
8.6.6 Сетевые настройки	42
8.6.7 Настройка параметров звука через веб-интерфейс ПК.....	45
8.6.8 Настройка параметров Wiegand через веб-интерфейс ПК	46
8.6.9 Настройки серийного интерфейса	46
8.6.10 Настройка голосовых предупреждений	48
8.6.11 Обновление и ТО	49
8.6.12 Отладка устройства	51
8.6.13 Тестирование протокола через веб-интерфейс ПК.....	52
8.6.14 Настройка службы проверки на проникновение в сеть через веб-интерфейс ПК.....	52
8.6.15 Состояние компонентов	53
8.6.16 Просмотр журнала через веб-интерфейс ПК.....	54
8.6.17 Управление сертификатами	54
Раздел 9 Настройка устройства через мобильный веб-интерфейс.....	56
9.1 Вход в систему	56
9.2 Обзор.....	56
9.3 Конфигурация	58
9.3.1 Основные параметры турникета.....	58

9.3.2 Управление пользователями	58
9.3.3 Просмотр основной информации об устройстве	60
9.3.4 Настройка времени устройства	60
9.3.5 Управление пользователями	62
9.3.6 Сеть	62
9.3.7 Поиск событий	65
9.3.8 Настройка параметров аудио	65
9.3.9 Настройки параметров контроля доступа	66
9.3.10 Настройки подсчета людей	71
9.3.11 Другие настройки	72
9.3.12 Обновление и техническое обслуживание	73
9.3.13 Выход из системы	73
9.3.14 Лицензия на ПО с открытым исходным кодом	74
9.3.15 Просмотр документации пользователя	74
Раздел 10 Другие платформы	75
А. Событие и тип тревоги	76
В. Описание ошибок	77

Раздел 1 Представление продукта

1.1 Введение



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 функции

- Двухнаправленный проход (вход / выход).
- Поддержка удаленного управления и контроля с помощью ПО НСР.
- Использование LED-индикатора высокой яркости для отображения состояния «Открыто» / «Закрыто» и направления движения через турникет.
- Пропуск при сигнале пожарной тревоги: при запуске тревоги турникет автоматически открывается для аварийной эвакуации.
- Поддержка конфигурации через веб-интерфейс на ПК.
- Поддержка протокола ISAPI для интеграции со сторонними системами.

Раздел 2 Подключение системы

Подготовка перед установкой и основные подключения.

Шаги

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



Примечание

Расстояние между двумя ближайшими линиями составляет 836 мм.

3. Пробейте пазы на монтажной поверхности и просверлите установочные отверстия в соответствии со схемой расположения отверстий. Вставьте по 4 распорных болта M12 × 150 в каждую тумбу.
4. Проложите кабели. Для каждого прохода прокладывают по 1 высоковольтному кабелю. Более подробная информация представлена далее в схеме подключения компонентов системы.

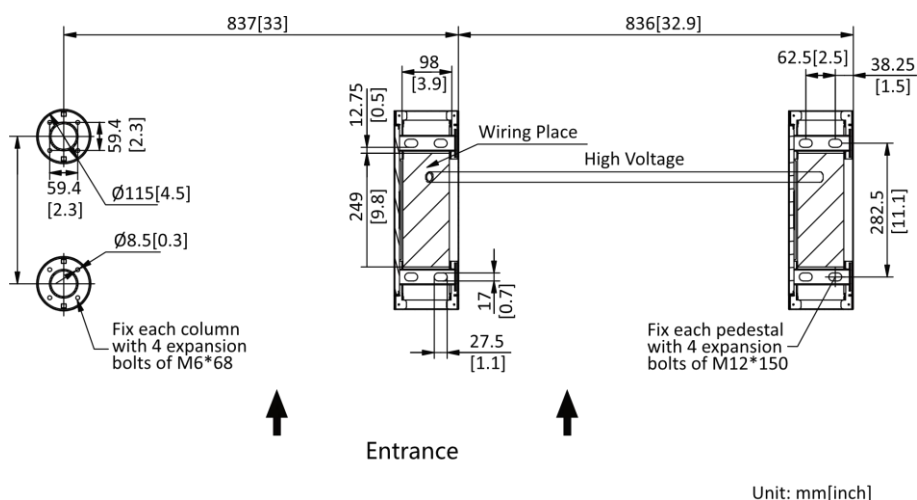


Рисунок 2-1 Подключение системы

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.
Entrance	Вход



Примечание

- Высокое напряжение: вход переменного тока
- Рекомендуемый внутренний диаметр высоковольтного кабеля должен превышать 30 мм.
- Внешний шнур питания переменного тока должен быть оснащен двойной изоляцией.
- Перед тем как начать копать, необходимо измерить толщину монтажной поверхности, чтобы не допустить ошибок.
- Необходимо использовать сетевой кабель CAT5e или сетевой кабель с более мощными рабочими характеристиками.
- Если сценарии использования оборудования включают детский сад или начальную школу, рекомендуется устанавливать специальные турникеты для детей, чтобы снизить риски для безопасности.

Если предполагается самостоятельный проход детей через турникет, рекомендуется использовать специальный кронштейн для установки терминала доступа с функцией распознавания лиц. При установке рекомендуется выбирать установку под небольшим углом или вертикальный кронштейн для детей. Вертикальный детский кронштейн рекомендуется устанавливать примерно в 0.5 метрах перед турникетом.

Раздел 3 Установка тумб

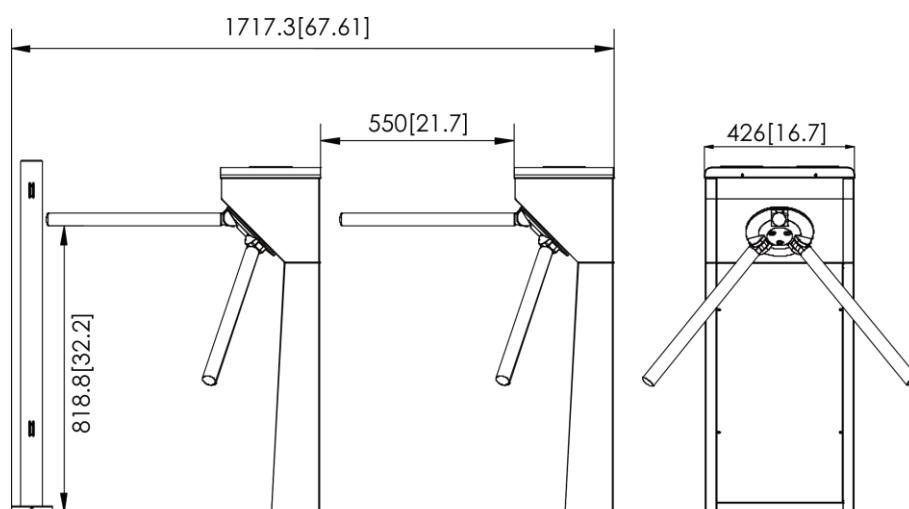
Перед началом

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

Шаги

Примечание

- Убедитесь, что устройство установлено на ровной поверхности. Основание должно быть твердым, а его толщина должна превышать длину анкерного болта.
 - Убедитесь, что устройство выключено во время установки и других операций.
 - Инструменты для установки находятся внутри упаковки тумбы.
 - Для предотвращения распространения ржавчины рекомендуется снять защитную пленку после установки устройства.
 - После снятия пленки рекомендуется протереть поверхность защитной жидкостью WD-40.
 - Только для использования внутри помещений. Запрещено погружать тумбы в воду.
 - Если место установки расположено близко к стене, убедитесь, что расстояние между тумбой и стеной составляет более 20 мм (60 мм при использовании терминалов доступа с функцией распознавания лиц), в противном случае это может привести к повреждению устройства или невозможности снять верхнюю панель тумбы.
 - Не превышайте нагрузку на штангу в 50 км.
-



Unit: mm[inch]

Рисунок 3-1 Размеры (ед. изм.: мм (дюймы))

-
1. Подготовьте инструменты для установки, проверьте компоненты и очистите монтажное основание.
 2. Герметично зафиксируйте основание турникета, чтобы защитить устройство от попадания воды внутрь.
 3. Правильно установите тумбы на основание и закрепите их с помощью расширительных болтов.

Отсканируйте QR-код, чтобы просмотреть видео-инструкцию по установке и подключению.

Раздел 4 Основные подключения

Примечание

- После ТО необходимо закрыть высоковольтный модуль водонепроницаемой крышкой.
 - При проведении технического обслуживания или разборки высоковольтных модулей следует извлечь все высоковольтные модули и разместить их вне турникета. Перед проведением технического обслуживания следует отсоединить кабели, подключенные к периферийным устройствам, чтобы избежать их повреждения.
-

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 АС от 100 до 240 В, от 50 до 60 Гц.

На представленном далее изображении показано положение каждого компонента турникета.

Примечание

Схема содержит только справочную информацию.

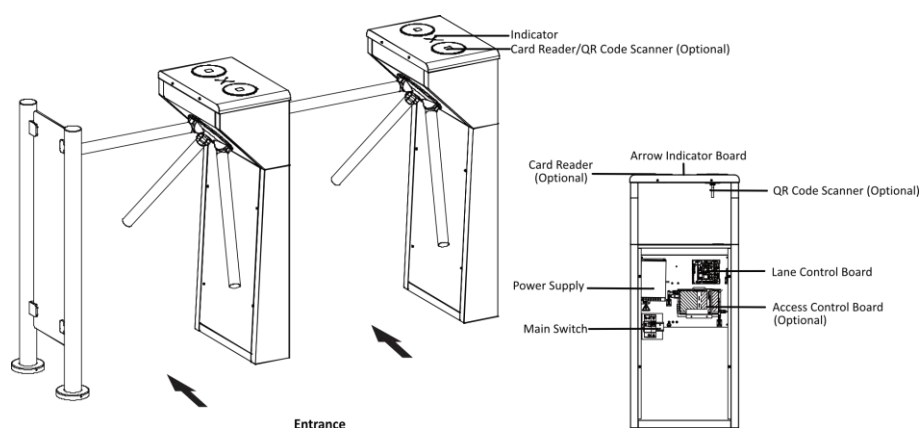
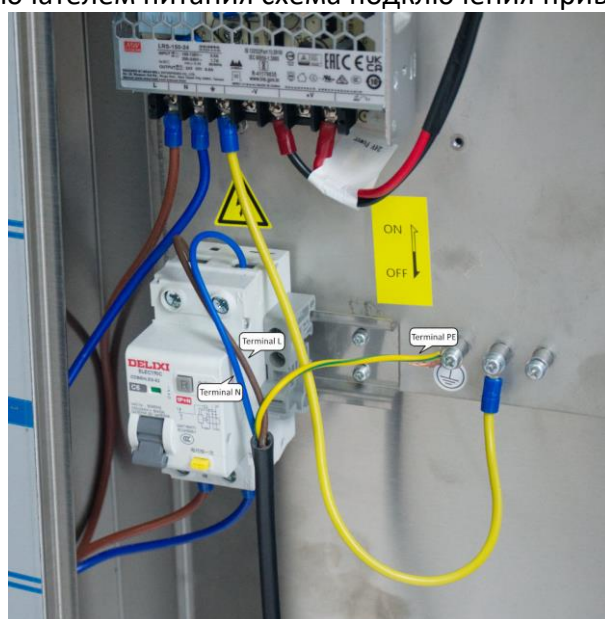


Рисунок 4-1 Компоненты

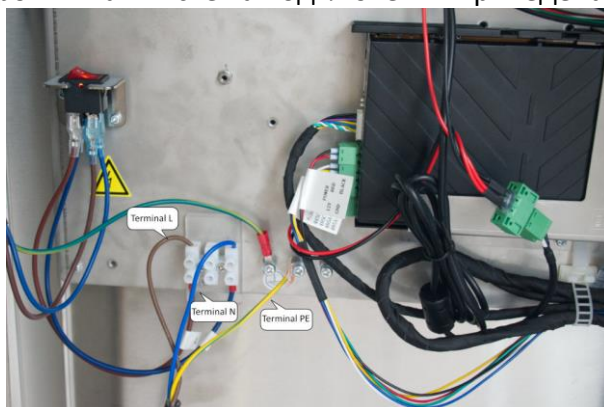
Английский язык	Русский язык
Indicator	Индикатор
Card Reader / QR Code Scanner (Optional)	Считыватель карт / Сканер QR-кода (опционально)
Card Reader (Optional)	Считыватель карт (опционально)
Arrow Indicator Board	Плата индикатора со стрелками
QR Code Scanner (Optional)	Сканер QR-кода (опционально)
Lane Control Board	Плата контроля прохода
Access Control Board (Optional)	Плата контроля доступа (опционально)
Power supply	Питание
Main switch	Основной переключатель

4.2 Подключение питания

Подключите источник питания к переключателю питания или адаптеру питания на тумбе. Разъем L (коричневый) и разъем N (синяя) расположены на переключателе, а разъем PE должен подключаться к заземляющему проводу (желтый и зеленый провода). Для устройства с переключателем питания схема подключения приведена ниже:



Для устройства с адаптером питания схема подключения приведена ниже:



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.
-

Таблица 5-1 Подключение RS-485

ID RS-485	ID порта в веб-интерфейсе	Подключение по умолчанию
RS-485A	Порт 3	Сканер QR-кодов (вход)
RS-485B	Порт 4	Сканер QR-кодов (выход)
RS-485C	Порт 5	Считыватель карт (вход)
RS-485D	Порт 6	Считыватель карт (выход)

5.2 Описание разъемов платы управления полосой движения

Плата управления полосой движения содержит интерфейс питания, интерфейс кнопки выхода и входа пожарной тревоги, интерфейс платы управления доступом, порт отладки, интерфейс индикатора и т. д.

На изображении ниже представлена схема платы управления полосой движения.

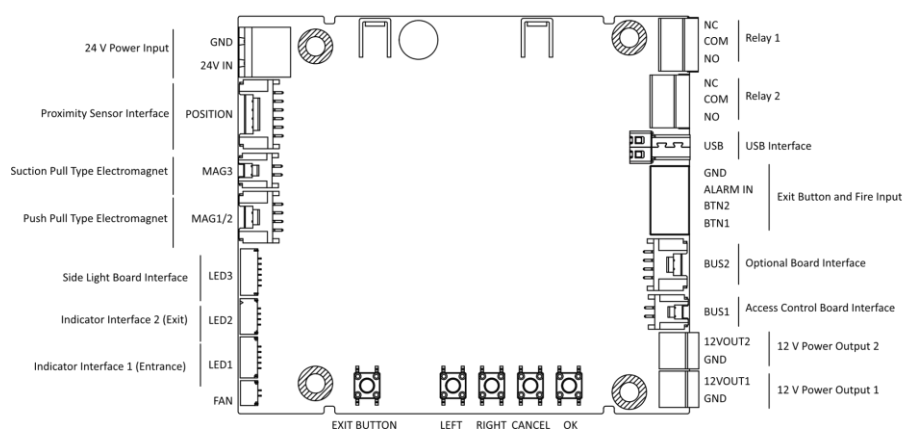


Рисунок 5-2 Плата управления полосой движения (спереди)

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)
Relay 1	Реле
USB Interface	USB-интерфейс
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

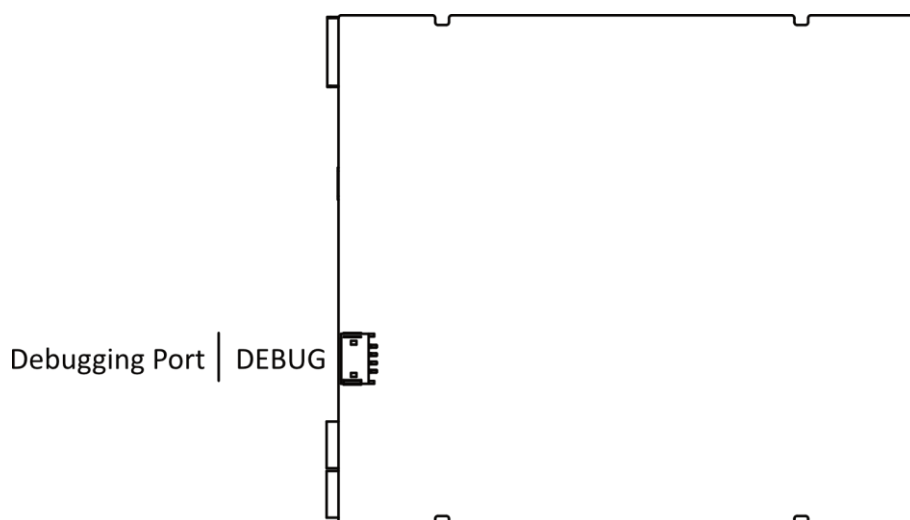
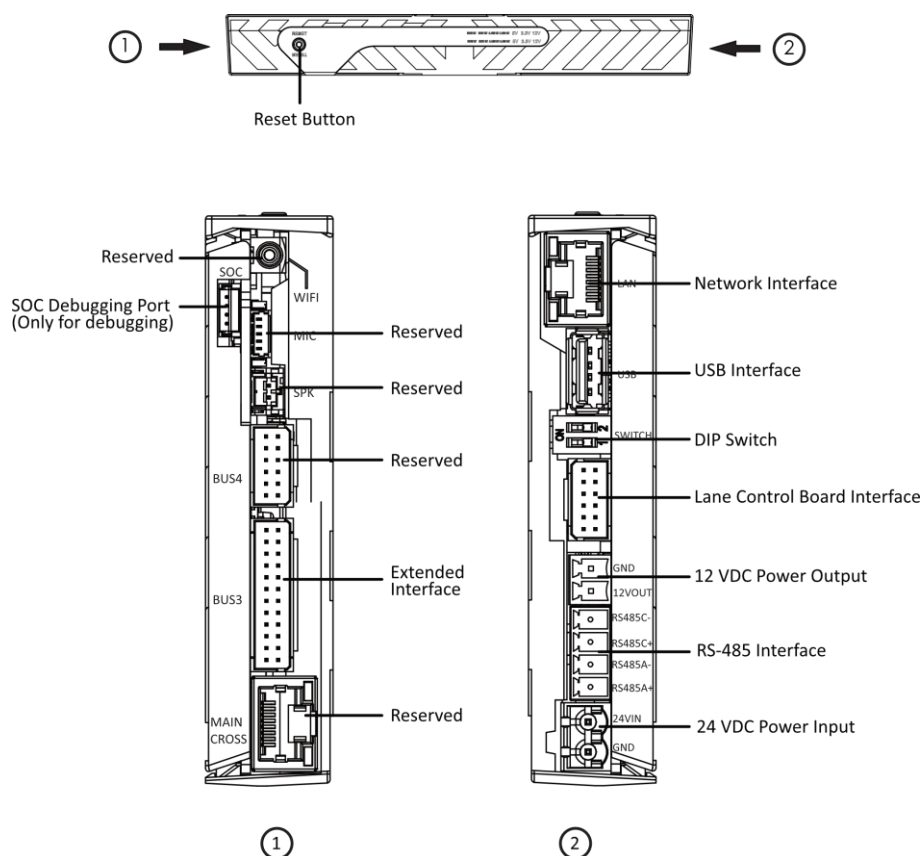


Рисунок 5-3 Плата управления полосой движения (сзади)

Английский язык	Русский язык
Debugging port	Порт отладки

5.3 Описание разъемов платы контроля доступа (опционально)

Плата контроля доступа в основном используется для аутентификации сотрудников в зонах с повышенными требованиями к безопасности, например, в органах внутренних дел или судах. Она также позволяет контролировать доступ к внешним устройствам и обеспечивает связь с вышестоящей платформой и контроллером полосы движения.



Английский язык	Русский язык
Reset Button	Кнопка сброса
SOC Debugging Port (Only for debugging)	Порт отладки SOC (только для отладки)
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 Power Input	Вход питания DC 24 В



Примечание

- Серийные интерфейсы SOC и MCU предназначены только для ТО и отладки.
- Удерживайте кнопку сброса настроек в течение 5 секунд, и устройство начнет процесс восстановления заводских настроек.

Схема подключения расширенного интерфейса платы контроля доступа показана ниже.

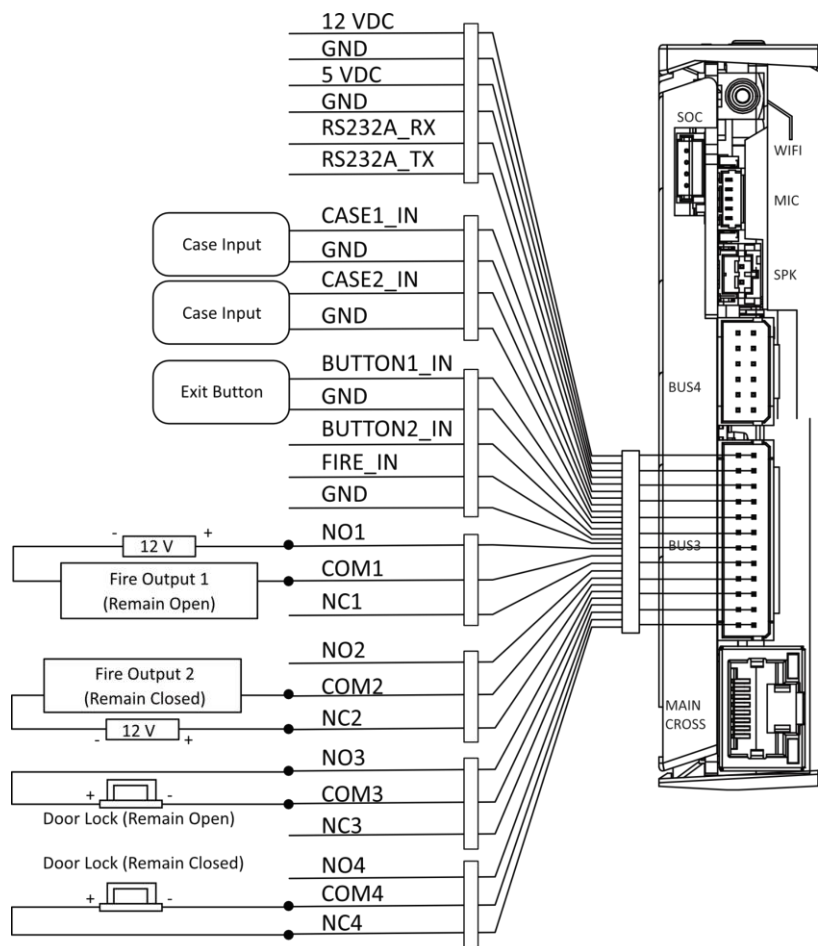


Рисунок 5-4 Схема подключения интерфейса BUS3

Английский язык	Русский язык
Exit Button	Кнопка выхода
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)

5.4 Описание разъемов основной дополнительной платы (опционально)

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

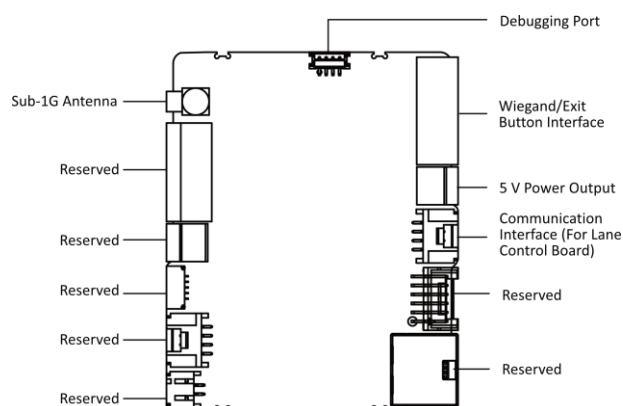


Рисунок 5-5 Разъемы основной дополнительной платы

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)

5.5 Считыватель карт

Считыватель карт может быть подключен к BUS4 платы контроля доступа.

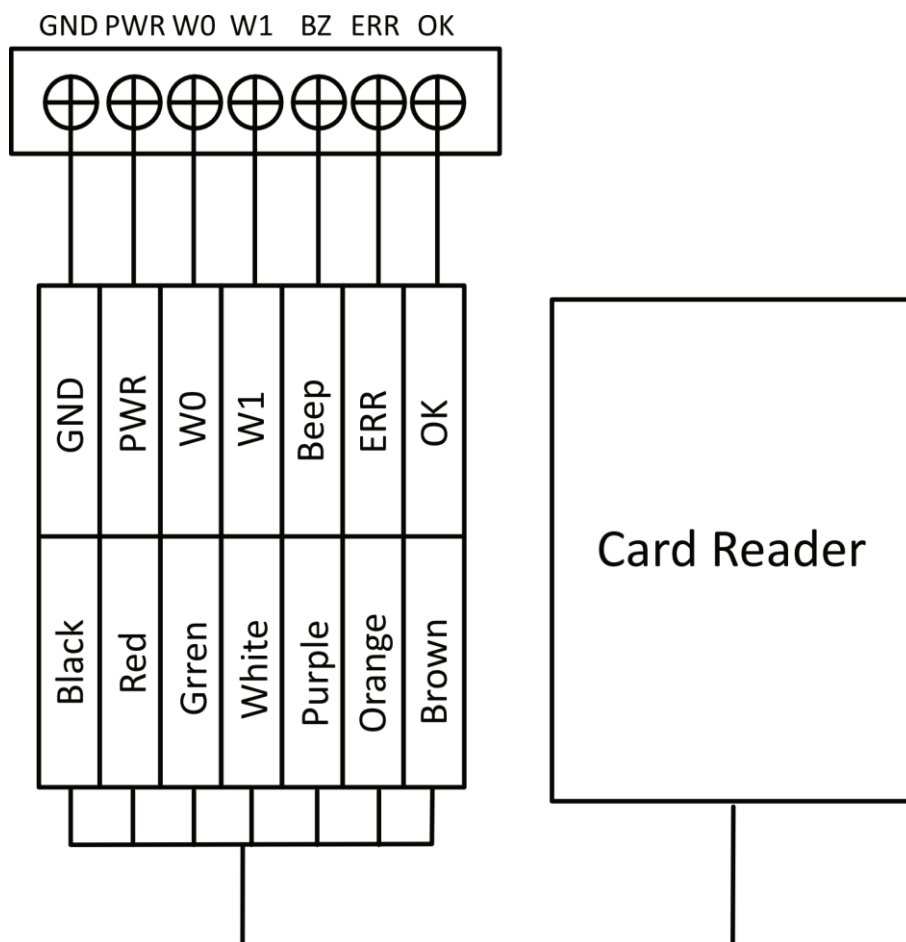


Рисунок 5-6 Считыватель карт

5.6 Подключение RS-485

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



Примечание

- Если к RS-485 подключаются другие устройства, идентификатор RS-485 не может быть изменен.
 - Если к интерфейсу питания 12 В подключен терминал доступа с функцией распознавания лиц, другие устройства подключить нельзя.
-

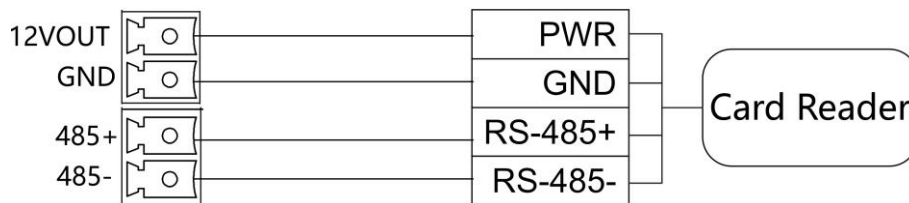


Рисунок 5-7 Подключение RS-485

Английский язык	Русский язык
Card Reader	Считыватель карт

5.7 Подключение тревожного входа

На главной плате управления можно подключить тревожный вход системы обнаружения возгораний.

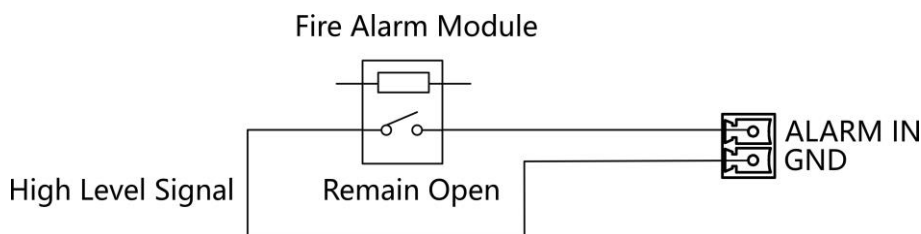


Рисунок 5-8 Оставить открытым

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

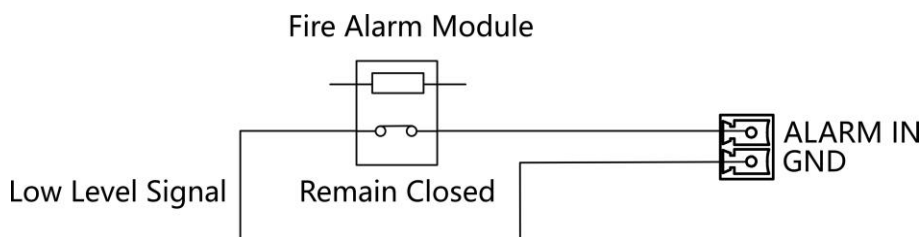


Рисунок 5-9 Оставить закрытым

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

5.8 Подключение кнопки выхода

Главная и дополнительная платы управления оснащены интерфейсом одной кнопки, к которому можно подключить кнопку выхода или устройство распознавания лиц.

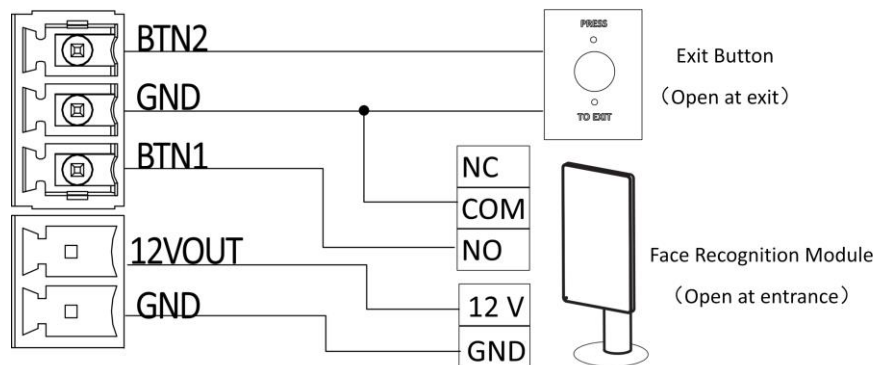


Рисунок 5-10 Подключение кнопки выхода

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 интерфейса питания 12 В постоянного тока главной и дополнительной плат управления.
- Открытие турникета на входе: подключение к BTN1 и GND.
- Закрытие турникета на выходе: подключение к BTN2 и GND.

Раздел 6 Настройка устройства с помощью КНОПКИ

6.1 Конфигурация с помощью кнопки

Описание кнопок

Кнопки находятся на плате управления полосой движения.

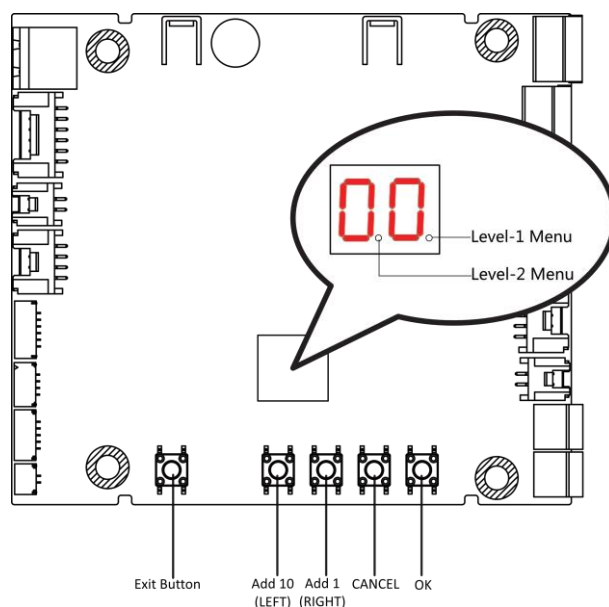


Рисунок 6-1 Кнопка

Английский язык	Русский язык
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

- Одно нажатие открывает турникет из положения для входа.
- Двойное нажатие открывает турникет из положения для выхода.

Кнопка конфигурации параметров

- ВЛЕВО: нажмите, чтобы добавить 10 единиц к данным конфигурации
- ВПРАВО: нажмите, чтобы добавить 1 единицу к данным конфигурации

- ОТМЕНА: вернуться в меню первого уровня или выйти из меню первого уровня
- ОК: подтвердить настройки, войти в режим конфигурации или в меню второго уровня

Примечание

- Номер конфигурации отображается двумя цифровыми индикаторами.
- Меню 1 уровня: если десятичная точка справа включена, это означает, что отображается меню первого уровня. Число обозначает номер конфигурации.
- Меню 2 уровня: если десятичная точка посередине включена, это означает, что отображается меню второго уровня. Число обозначает параметры элемента конфигурации.

Процедура настройки

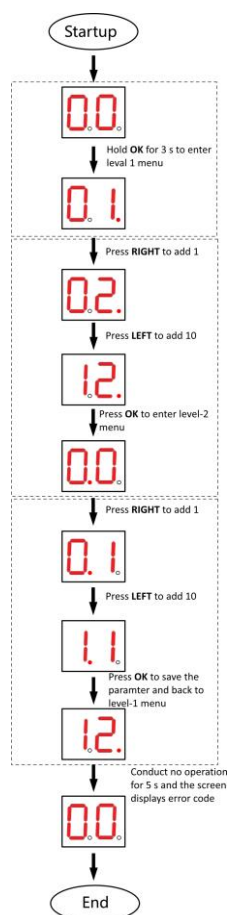


Рисунок 6-2 Процедура

Английский язык	Русский язык
Start up	Запуска
Hold OK for 3 s to enter level 1 menu	Удерживайте кнопку ОК 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 ОК, чтобы пойти в меню уровня 2
Press OK to save the parameter and back to level 1 menu	Нажмите ОК, 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: войдите в режим конфигурации. В правой части экрана отобразится цифра 1, и устройство будет готово к настройке.
- Нажмите **Left** («Влево») или **Right** («Вправо»), чтобы настроить номер конфигурации. Нажмите **OK**, чтобы войти в меню уровня 2 и просмотреть параметры. Нажмите **Cancel** («Отмена») или не выполняйте никаких операций в течение 5 секунд, чтобы отменить настройку.
- Нажмите **Left** («Влево») или **Right** («Вправо»), чтобы задать необходимые параметры. Нажмите **OK**, чтобы сохранить изменения, или нажмите **Cancel** («Отмена»), чтобы вернуться к настройке номера конфигурации без сохранения изменений. В течение 5 секунд не выполняйте никаких операций для отмены настройки.

6.2 Инициализация устройства

Шаги

- Удерживайте кнопку инициализации на плате контроля доступа в течение 5 секунд.

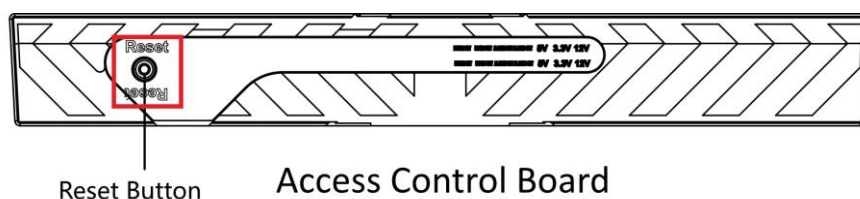


Рисунок 6-3 Положение кнопки инициализации

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

- Устройство начнет восстановление заводских настроек.
- По завершении процесса устройство будет подавать звуковой сигнал в течение 3 секунд.



Предостережение

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 7 Активация

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

7.1 Активация через веб-интерфейс

Можно активировать устройство через веб-интерфейс.

Шаги

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



Примечание

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

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



Предостережение

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.

7.2 Активация через мобильный веб-интерфейс

Можно активировать устройство через мобильный веб-интерфейс.

Шаги

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



Примечание

- Для неактивных устройств точка доступа включена по умолчанию.
- Паролем точки доступа по умолчанию является серийный номер устройства.

Всплывет страница входа в систему.

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.

7.3 Активация через ПО SADP

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

Перед началом

- ПО SADP доступно на диске, входящем в комплект или на официальном сайте <http://www.hikvision.com/en/>, <https://iflow-tech.ru/images/faq/>
Инструкция_по_сбросу_пароля_iFLOW.pdf установите ПО SADP согласно инструкции.
- Устройство и ПК, на котором запущено ПО SADP, должны находиться в одной подсети. Следующие шаги показывают, как активировать устройство и изменить его IP-адрес.

Подробная информация о пакетной активации и изменении IP-адресов представлена в **Руководстве пользователя ПО SADP**.

Шаги

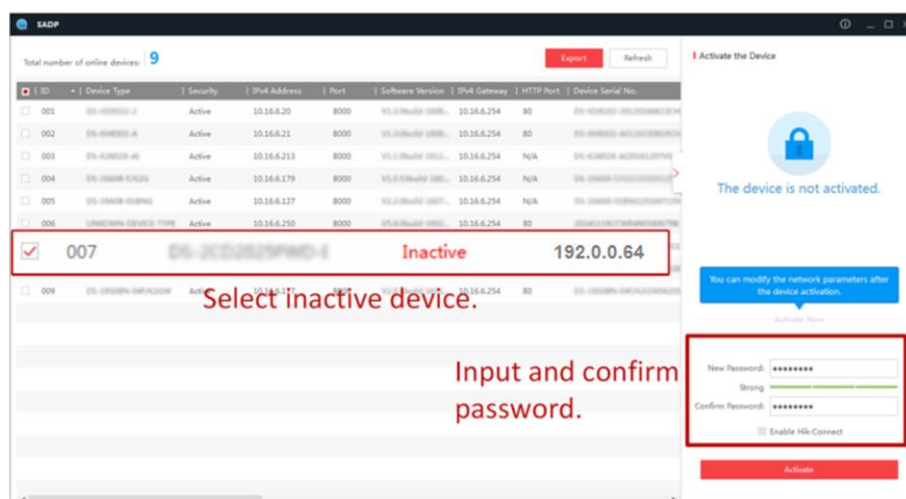
1. Запустите ПО SADP для поиска онлайн устройств.
2. Найдите и выберите устройство в списке онлайн устройств.
3. Введите новый пароль (пароль администратора) и подтвердите его.



Предостережение

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

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



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

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

7.4 Активация устройства при помощи клиентского ПО iVMS-4200

Для исправной работы некоторых устройств необходимо создать пароль активации, прежде чем добавлять их в систему iVMS-4200.

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 устройство»), 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. 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 безопаснее.
Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг и / или конечного пользователя.



Примечание

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

7. Нажмите **ОК** для активации устройства.

Глава 8 Работа через веб-интерфейс

8.1 Вход в систему

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



Примечание

Устройство должно быть активировано. Подробная информация об активации представлена в разделе **Активация 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»).



Примечание

После 5 неудачных попыток ввода пароля устройство будет заблокировано. Повторите попытку через 30 минут.

8.2 Забыть пароль

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

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

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

Проверка по контрольным вопросам

Также вы можете обратиться за сбросом пароля https://iflow-tech.ru/images/faq/Инструкция_по_сбросу_пароля_iFLOW.pdf

8.3 Быстрые операции через веб-интерфейс

8.3.1 Настройка времени

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

Время устройства

Отображение времени устройства в режиме реального времени.

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Режим синхронизации времени

NTP

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

Вручную

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

Переход на летнее время (DST)

Можно включить летнее время, установить и просмотреть время начала и окончания летнего времени, а также время смещения.

Нажмите **Complete** («Завершить») для сохранения настроек.

8.4 Управление пользователями

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

Добавление основной информации

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

Добавьте основную информацию о пользователе, включая идентификатор, имя и тип пользователя.

При выборе роли пользователя **Visitor** («Посетитель») можно установить количество посещений.

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

Настройка длительности разрешения

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

Включите **Long-Term Effective User** («Пользователь с длительным разрешением») или настройте **Validity Period** («Период действия»), и пользователь сможет получить разрешение только в течение настроенного периода времени.

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

Добавление карты

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

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



Примечание

Для добавления доступно до 50 карт.

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

Настройки параметров аутентификации

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

Выберите для параметра **Authentication Type** («Тип аутентификации»): **Same as Device** («Тот же, что и у устройства») или **Custom** («Пользовательский»).

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

Импорт / экспорт данных о пользователе

Экспорт данных о пользователе

Можно экспортировать добавленные данные для резервного копирования или импорта на другие устройства.

Нажмите **Export** → **Export Person Data (Database)** («Экспорт → Экспорт данных о пользователях (база данных)'), установите пароль шифрования и подтвердите его.

Нажмите **OK**.



Примечание

- Данные о пользователе будут загружены на ПК.
 - Настроенный пароль потребуется для импорта файла данных.
-

Импорт данных о пользователе

Нажмите **Import** → **Import Person Data** («Импорт → Импорт данных о пользователе») и выберите файл.

Введите пароль шифрования для импорта и синхронизации персональных данных с устройствами.

8.5 Турникет

8.5.1 Обзор

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

Описание функций:

Состояние компонентов устройства

Проверьте корректность работы устройства. Нажмите **View More** («Дополнительно»), чтобы просмотреть подробную информацию о состоянии компонента.

Удаленное управление

 /  /  / 

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

Событие в режиме реального времени

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

Информация о пользователе

Можно просмотреть добавленную и недобавленную информацию о пользователе и карте.

Состояние сети

Можно просмотреть состояние сетевого подключения.

Основная информация

Можно просмотреть модель, серийный номер и версию прошивки.

Емкость устройства

Можно просмотреть емкость хранения записей пользователей, карт и событий.

8.5.2 Поиск событий

Нажмите **Turnstile** → **Event Search** («Турникет → Поиск события»), чтобы перейти на соответствующую страницу.

Event Types

Access Control Event

Major Type

All Type

Sub Type

All Type

Employee ID

Name

Card No.

Start Time

2024-06-17 00:00:00

End Time

2024-06-17 23:59:59

Yes...

Today

Cur...

Cur...

Search

Рисунок 8-1 Поиск событий

Введите условия поиска, включая тип события, основной тип, подтип, идентификатор сотрудника, имя, номер карты, время начала и время окончания, и нажмите **Search** («Поиск»).

После этого на панели справа появятся результаты поиска.

8.5.3 Настройки параметров контроля доступа

Настройка параметров двери

Нажмите **Turnstile** → **Parameter Settings** → **Door Parameters** («Турникет → Настройки параметров → Параметры двери»).

Door No.

Entrance

Exit

Door Name

Access Point 1

Open Duration

8

s

☐ Exit Button Type

☐ Remain Closed

☒ Remain Open

Door Remain Open Duration wi...

10

min

Рисунок 8-2 Настройка параметров двери

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

Номер двери

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

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

Длительность открытия составляет от 5 до 60 секунд.

Тип кнопки выхода

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

Дверь остается открытой после авторизации первого сотрудника

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

Настройка параметров аутентификации

Нажмите **Turnstile** → **Parameter Settings** → **Authentication Settings** («Турникет → Настройки параметров → Настройки аутентификации»).



Примечание

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

Card Reader Parameter Configuration

Terminal

Entrance

Exit

Terminal Type Card

Terminal Model 485Offline

Enable Authentication Device

① Authentication Interval

0

s

① Alarm of Max. Failed Attem...

Communication with Controller ...

10

s

Authentication Plan Configuration

Authentication

Card

Clear

Sun	00	02	04	06	08	10	12	14	16	18	20	22	24
Mon													
Tue													
Wed													
Thu													
Fri													
Sat													

00 02 04 06 08 10 12 14 16 18 20 22 24

The selected authentication mode should be supported by card reader.

Save

Рисунок 8-3 Параметры аутентификации

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

Терминал

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

Тип терминала / режим терминала

Получение описания терминалов. Доступно только для чтения.

Включить устройство с функцией аутентификации

Включить функцию аутентификации.

Интервал аутентификации

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

Запуск тревоги при достижении максимального количества неудачных попыток считывания карты

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

Макс. кол-во 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

Интервал аутентификации варьируется от 2 до 255 секунд.

Настройки параметров карты

Настройка типа карты

Нажмите **Turnstile** → **Parameter Settings** → **Card Settings** («Турникет → Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.

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

Включение распознавания NFC-карты

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

Включение распознавания M1-карты

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

Шифрование M1-карты

Сектор

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

Активация распознавания EM-карты

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



Примечание

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

Включение карты DESFire

Устройство может считывать данные с DESfire-карты.

Чтение DESFire-карт

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

Активация распознавания FeliCa-карты

Устройство может считывать данные с FeliCa-карты.

Настройка параметров аутентификации № карты

Настройте параметры карты при аутентификации через карту на устройстве.

Перейдите **Turnstile** → **Parameter Settings** → **Card Settings** («Турникет → Настройки параметров → Настройки карты»).

Выберите режим аутентификации по карте и нажмите **Save** («Сохранить»).

Режим аутентификации карты

Полный номер карты

Будет прочитан полный номер карты.

Wiegand 26 (3 байта)

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

Wiegand 34 (4 байта)

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

Corporate1000_35/Corporate1000_48/H10302_37/10304_37/H103130_332CSN/Wiegand_56 CSN/Wiegand_58

Устройство будет считывать данные с карты в другом режиме.

Включение считывания номера карты в обратной последовательности

После включения функции номер карты будет считываться в обратной последовательности.

Привязка события

Настройте действия привязки для событий.

Шаги

1. Нажмите **Turnstile** → **Parameter Settings** → **Linkage Settings** («Турникет → Настройки параметров → Настройки привязки»), чтобы перейти на страницу настроек.

Рисунок 8-4 Привязка события

2. Нажмите +, чтобы задать источник события.
 - При выборе **Event Linkage** («Привязка события»), как **Linkage Type** («Тип привязки»), из выпадающего списка выберите тип события.
 - При выборе **Card Linkage** («Привязка карты»), как **Linkage Type** («Тип привязки»), введите № карты и выберите считыватель карт.
 - При выборе **Employee ID Linkage** («Привязка ID сотрудника»), как **Linkage Type** («Тип привязки»), введите ID сотрудника и выберите считыватель карт.
3. Настройте действия привязки.

Привязка двери

Включите **Door Linkage** («Привязка двери») и установите состояние двери **Entrance** («Вход») и **Exit** («Выход») для целевого события.

Linked Alarm Output («Привязанный тревожный выход»)

Включите **Linked Alarm Output** («Привязанный тревожный выход»), выберите **Alarm Output 1** или **Alarm Output 2** и настройте состояние тревожного выхода для события.

Привязанное голосовое предупреждение

Включите **Linked Audio Prompt** («Привязанное голосовое предупреждение») и выберите режим воспроизведения.

- При выборе **TTS** необходимо задать язык и ввести содержимое предупреждения.
- При выборе параметра **Audio File** («Аудиофайл») необходимо добавить доступный аудиофайл из выпадающего списка или нажать **General Linkage Settings** («Общие настройки привязки»), чтобы добавить новый аудиофайл.

Привязка захвата

Включите **Linked Capture** («Привязка захвата») и выберите вход или выход для захвата события.

Настройка параметров терминала

Можно настроить параметры терминала для получения доступа.

Нажмите **Turnstile** → **Parameter Settings** → **Terminal Parameters** («Турникет → Настройки параметров → Параметры терминала»).

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

Режим без разрешений

Устройство проверяет только действительность учетных данных и не выполняет аутентификацию разрешений.

Перейдите **Remote Verification** → **Verify Credential Locally** («Удаленная проверка → Локальная проверка учетных данных»). Устройство проверит разрешения, но не будет оценивать шаблон плана.

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 проверка») в соответствии с фактическими потребностями. После включения можно выполнить проверку удаленно. И можно включить **Verify Credential Locally** («Локальная проверка учетных данных»), если необходимо.

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

Настройка параметров конфиденциальности

Задайте тип хранения событий.

Перейдите **Turnstile** → **Parameter Settings** → **Privacy Settings** («Турникет → Настройки параметров → Настройки конфиденциальности»).

По умолчанию тип хранения событий – перезапись. Самые ранние 5 % событий будут удалены, когда система обнаружит, что сохраненные события занимают более 95 % заполненного пространства.

8.5.4 Турникет

Основные параметры

Установите основные параметры турникета.

Шаги

1. Нажмите **Turnstile** → **Turnstile Configuration** → **Basic Settings** («Турникет → Конфигурация турникета → Основные настройки»), чтобы перейти на страницу.

Channel Type Tripod Turnstile

Channel Model

Working Status Normal

Passing Mode ☒ General Passing ☐ Weekly Schedule

Entrance Controlled

Exit Controlled

Рисунок 8-5 Основные параметры

- Просмотрите **Channel Type** («Тип канала»), **Channel Model** («Модель канала») и **Working Status** («Состояние режима работы»).
- Установите режим для прохода.

Общий проход

При выборе **General Passing** («Общий проход») можно выбрать состояние турникета из выпадающего списка для входа и выхода.

Расписание на неделю

При выборе **Weekly Schedule** («Расписание на неделю») можно установить еженедельный график для входа и выхода.

- Нажмите **Save** («Сохранить»).

Подсчет людей

Задайте параметры подсчета людей.

Шаги

- Нажмите **Turnstile** → **Turnstile Configuration** → **People Counting Settings** («Турникет → Конфигурация турникета → Настройка подсчета людей»), чтобы перейти на страницу.

People Counting ☒

Device Offline People Counting ☒

Passing Event Record ☒

Person Statistics Type ☒ Invalid ☐ Passing Detection ☐ Authentication Number

People Counting Clear

Save

Рисунок 8-6 Подсчет людей

- Включите **People Counting** («Подсчет людей»).

-
3. Включите **Device Offline People Counting** («Автономный подсчет людей на устройстве»), устройство будет подсчитывать количество людей, даже если оно находится в автономном режиме.
 4. Включите **Passing Event Record** («Запись о проходящих людях»), устройство будет сообщать о событии, когда люди будут проходить мимо.
 5. Выберите **People Statistics Type** («Тип статистики по людям»).

Недействительно

Отключение функции подсчета пассажиров.

Детекция прохода

Количество всех проходящих людей.

Номер аутентификации

Количество прошедших людей, проверенных с помощью считывателя карт и т. д.

6. Опционально. Нажмите **Clear** («Очистить»), чтобы удалить всю информацию о подсчете людей.

Прочие настройки

Настройте другие параметры.

Шаги

1. Нажмите **Turnstile** → **Turnstile Configuration** → **Other Settings** («Турникет → Конфигурация турникета → Другие настройки»), чтобы перейти на страницу.
2. Настройте параметры.

Длительность запуска тревоги

Длительность запуска тревоги варьируется от 0 до 3599 с. 0 означает непрерывную подачу сигнала.

Яркость световой панели

Перетащите указатель или введите значение, чтобы настроить яркость. Чем больше значение, тем ярче становится индикатор.

Длительность звукового сигнала тревоги

Установите продолжительность звукового сигнала тревоги.

Правило запрета двойного прохода

Установите правило запрета двойного прохода: **Authentication Status** («Состояние аутентификации») или **By Passing Status** («Состояние прохождения»).

По состоянию аутентификации

Пользователь должен пройти аутентификацию, в противном случае функция запрета двойного прохода не будет активирована.

Состояние прохождения

Пользователь не может пройти аутентификацию, и запрет двойного прохода будет выполнен.

Режим памяти

При включении режима памяти допускается предъявление нескольких карт для одновременного прохода нескольких человек. Когда количество проходящих людей превышает количество предъявленных карт, или после того, как последний прошедший человек не прошел, и в течение времени открытия двери не прошло ни одного другого человека, дверь автоматически закроется.

По умолчанию функция отключена.

Тип входа пожарной тревоги

В нормально разомкнутом состоянии закрытие активирует противопожарную защиту. В нормально замкнутом состоянии открытие активирует противопожарную защиту.

3. Нажмите **Save** («Сохранить»).

8.6 Система и обслуживание

Можно просмотреть системную информацию и емкость. Кроме того, можно обновить устройство, восстановить заводские настройки, восстановить настройки по умолчанию и перезагрузить устройство.

8.6.1 Отображение информации об устройстве

Просмотр названия устройства, языка, модели, серийного номера, версии, количества каналов, количества интерфейсов входа, количества интерфейсов выхода, числа тревожных входов, числа тревожных выходов, емкости устройства и т. д.

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

Можно просмотреть язык, модель, серийный номер, версию, количества интерфейсов входа, количества интерфейсов выхода, числа тревожных входов, числа тревожных выходов.

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

Нажмите **Upgrade** («Обновить»), чтобы обновить версию встроенного ПО.

Можно просмотреть емкость устройства, включая данные о пользователе, изображение лица, карту и событие.

8.6.2 Настройка времени

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

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

Device Time 2024-06-17 19:57:14

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Synchronization mode ☐ NTP ☒ Manual

Set Time 2024-06-17 19:56:52 Sync With Com...

DST

DST

Рисунок 8-7 Настройка времени

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

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

NTP

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

Вручную

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

Переход на летнее время (DST)

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

8.6.3 Изменение пароля администратора

Шаги

1. Перейдите на страницу смены пароля.
 - Перейдите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **User Management** («Система и обслуживание → Конфигурация системы → Система → Управление пользователем → Управление пользователем») и нажмите .
 - Нажмите **admin** → **Modify Password** («Администратор → Изменить пароль») в правом верхнем углу страницы.
2. Введите старый пароль и создайте новый пароль.
3. Подтвердите новый пароль.
4. Нажмите **Save** («Сохранить»).



Предостережение

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

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

8.6.4 Пользователи онлайн

Отображается информация о пользователях, выполняющих вход в устройство.

Перейдите в меню **System and Maintenance** → **System Configuration** → **System** → **User Management** → **Online Users** («Система и обслуживание → Конфигурация системы → Система → Управление пользователями → Онлайн пользователи») для просмотра списка онлайн пользователей.

8.6.5 Просмотр информации о постановке / снятии устройства с охраны через веб-интерфейс ПК

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

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

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

8.6.6 Сетевые настройки

Настройка основных сетевых параметров

Нажмите **System and Maintenance** → **System Configuration** → **System** → **Network** → **Network Settings** → **TCP/IP** («Система и обслуживание» → Конфигурация системы → Система → Сеть → Сетевые настройки → TCP / IP»).

Можно просмотреть MAC-адрес и MTU.

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

NIC Type: Self-Adaptive

DHCP: ☐

* IPv4 Address:

* IPv4 Subnet Mask:

* IPv4 Default Gateway:

IPv6 Mode: ☒ Manual ☐ DHCP ☐ Route Advertisement

* IPv6 Address:

* IPv6 Subnet Prefix Length:

* IPv6 Default Gateway:

Mac Address:

MTU: 1500

DNS Server

DHCP: ☐

Preferred DNS Server:

Alternate DNS Server:

Save

Рисунок 8-8 Настройка TCP / IP

Тип NIC

Выберите тип NIC из выпадающего списка. По умолчанию задан параметр **Auto** («Автоматич.»).

DNCP

При отключении этой функции необходимо настроить IPv4-адрес, IPv4-маску подсети, IPv4-шлюз по умолчанию, Мас-адрес и MTU.

При включении этой функции система автоматически задаст IPv4-адрес, IPv4-маску подсети и IPv4-шлюз.

Режим IPv6

Вручную

Установите IPv6-адрес, длину префикса подсети IPv6 и шлюз по умолчанию IPv6 вручную.

DNCP

Система автоматически выделит IPv6-адрес, длину префикса подсети IPv6 и шлюз по умолчанию IPv6.

Анонс маршрутизатора

Механизм автоматической настройки адресов в стеке протоколов IPv6. Устройство может выполнить настройку IPv6-адреса, если в среде есть маршрутизаторы, которые могут предоставлять уведомления о маршрутизации.

Нажмите **View Route Advertisement** («Просмотреть анонс маршрутизатора»), чтобы просмотреть список IPv6-адресов.

DNS-сервер



Примечание

Настроить DNS-сервер можно только при включенном DNCP.

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

Настройка порта через веб-интерфейс ПК

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** («Система и обслуживание» → Конфигурация системы → Сеть → 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.

Настройка OTAP через веб-интерфейс ПК

Подключите устройство к платформе по протоколу OTAP, чтобы получить информацию об устройстве, загрузить информацию о состоянии работы и тревогах, перезагрузить и обновить устройство.

Шаги

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

Enable ☒

* Server IP Address

* Port

* Device ID

* Encryption Key

Register Status ✖ Offline

[More](#) ▾

Рисунок 8-9 Настройка OTAP

2. Выберите центральную группу.
3. Нажмите **Enable** («Включить»), чтобы включить OTAP.
4. Установите **Server IP Address** («IP-адрес сервера»), **Port** («Порт»), **Device ID** («ID-устройства») и **Encryption Key** («Ключ шифрования»).
5. Нажмите **More** («Дополнительно»), чтобы просмотреть тип сети и приоритет доступа. Перетащите значок операции вверх или вниз, чтобы отрегулировать приоритет сети.
6. Нажмите **Test** («Диагностика»), чтобы убедиться, что устройство может подключиться к серверу и успешно зарегистрироваться. Обновите страницу или перезагрузите устройство, чтобы увидеть **Register Status** («Состояние регистрации»).
7. Нажмите **Save** («Сохранить»).

Доступ к платформе через веб-интерфейс ПК

Устройствами можно управлять с помощью платформы доступа.

Шаги

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



Примечание

Hik-Connect — это приложение для мобильных устройств. С помощью приложения можно просматривать видео в реальном времени с устройства, получать тревожные уведомления и т. д.

2. Поставьте **Enable** («Включить») для включения соответствующей функции.
3. Опционально. Поставьте галочку возле **Custom** («Пользовательская настройка»), чтобы настроить адрес сервера самостоятельно.
4. Введите проверочный код.
5. Опционально. Нажмите **Enable** («Включить»), чтобы включить шифрование видео, установить пароль шифрования и подтвердить его.
6. Нажмите **More** («Дополнительно»), чтобы просмотреть тип сети и приоритет доступа. Перетащите значок операции вверх или вниз, чтобы отрегулировать приоритет сети.
7. Нажмите **View** («Просмотр»), чтобы просмотреть QR-код устройства. Сканируйте QR-код, чтобы выполнить привязку учетной записи.



Примечание

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

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

8.6.7 Настройка параметров звука через веб-интерфейс ПК

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Video/Audio** → **Audio** («Система и обслуживание → Конфигурация системы → Видео / аудио → Аудио»).
2. Выберите **Enable Voice Prompt** («Включить голосовое предупреждение»), и голосовые предупреждения будут включены на устройстве.
3. Установите громкость выхода.

8.6.8 Настройка параметров Wiegand через веб-интерфейс ПК

Можно настроить направление передачи данных интерфейса Wiegand.

Шаги



Примечание

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

1. Нажмите **System and Maintenance** → **System Configuration** → **Access Configuration** → **Wiegand Settings** («Система и обслуживание» → Конфигурация системы → Конфигурация доступа → Настройки Wiegand»).

No. Entrance Exit

Wiegand ☒

Wiegand Direction Input

Wiegand Mode Wiegand34

Рисунок 8-10 Страница настройки Wiegand

2. Выберите **Entrance** («Вход») или **Exit** («Выход») в качестве направления считывателя карт.
3. Нажмите **Wiegand**, чтобы включить функцию Wiegand.
4. Установите направление передачи данных.

Вход

Устройство можно подключать к считывателю карт Wiegand.

5. Выберите режим Wiegand из раскрывающегося списка.
6. Нажмите **Save** («Сохранить»).



Примечание

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

8.6.9 Настройки серийного интерфейса

Настройте параметры серийного интерфейса.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Access Configuration** → **Serial Port Configuration** («Система и обслуживание» → Конфигурация системы → Конфигурация доступа → Конфигурация серийного интерфейса»).

Serial Port Type RS232

No. 1

Baud Rate 115200

Data Bit 8

Stop Bit ☒ 1 ☐ 2

Parity ☒ None ☐ Odd Parity ☐ Even Verification

Peripheral Type ☐ QR Code Scanner ☒ Disable

Peripheral Position ☒ Entrance ☐ Exit

External Device Model None

Save

Рисунок 8-11 Конфигурация серийного интерфейса

2. Выберите номер серийного интерфейса, и соответствующий тип серийного интерфейса отобразится автоматически.
3. Настройте параметры серийного интерфейса.

Скорость передачи данных

Настройте скорость передачи данных.

Бит данных

Настройте количество битов для передачи данных.

Стоповый бит

Выберите конечную точку для одного кадра данных.

Четность

Выберите принцип обнаружения ошибок связи серийного интерфейса. Можно выбрать, нужно ли определить, является ли один из битов данных и контрольных цифр нечетным или четным, или же контрольная цифра отсутствует.

4. Установите **Peripheral Type** («Тип периферийного устройства»).
5. Выберите параметр для **Peripheral Position** («Положение периферийного устройства»): **Entrance** («Вход») или **Exit** («Выход»).
6. Можно просмотреть модель внешнего устройства.
7. Нажмите **Save** («Сохранить»).

8.6.10 Настройка голосовых предупреждений

Настройте голосовые предупреждения для случаев успешной аутентификации и сбоев аутентификации.

Шаги

1. Перейдите **System and Maintenance** → **Preference** → **Prompt Schedule** («Система и обслуживание → Пользовательская настройка → Расписание подсказок»).

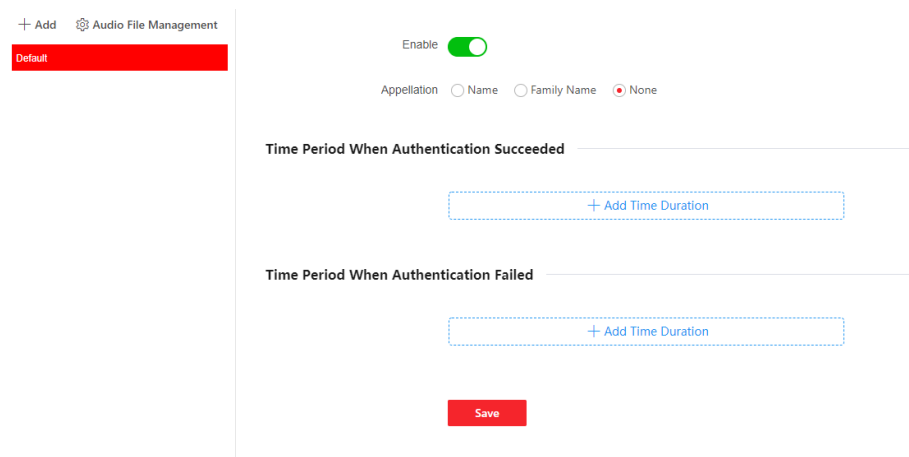


Рисунок 8-12 Настройка голосовых предупреждений

2. Включите функцию.
3. Укажите наименование.
4. Настройте период предупреждения при успешной аутентификации.
 - 1) Нажмите **Add Time Duration** («Добавить продолжительность»).
 - 2) Установите продолжительность времени.



Примечание

Если аутентификация прошла успешно, устройство будет транслировать настроенное предупреждение в течение заданного времени.

- 3) Выберите тип голосового предупреждения.
- 4) Введите содержимое голосового предупреждения или выберите аудиофайл.



Примечание

Можно нажать + **Audio File** («Аудиофайл») или **Audio File Management** («Управление аудиофайлами»), чтобы добавить аудиофайлы.

- 5) Опционально. Повторите шаги от 1 до 3.
- 6) Опционально. Нажмите , чтобы сбросить настроенную продолжительность предупреждения.
5. Установите продолжительность предупреждения при сбое аутентификации.
 - 1) Нажмите **Add Time Duration** («Добавить продолжительность»).

2) Установите продолжительность времени.



Примечание

При сбое аутентификации устройство будет транслировать настроенное предупреждение в течение заданного времени.

3) Выберите тип голосового предупреждения.

4) Введите содержимое голосового предупреждения или выберите аудиофайл.



Примечание

Можно нажать + **Audio File** («Аудиофайл») или **Audio File Management** («Управление аудиофайлами»), чтобы добавить аудиофайлы.

5) Опционально. Повторите шаги от 1 до 3.

6) Опционально. Нажмите , чтобы сбросить настроенную продолжительность предупреждения.

6. Нажмите **Save** («Сохранить»).

8.6.11 Обновление и ТО

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

Перезагрузка устройства

Нажмите **System and Maintenance** → **Maintenance** → **Restart** («Система и обслуживание → Техническое обслуживание → Перезагрузка»).

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

Обновление

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

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



Примечание

Не выключайте устройство во время обновления.

Восстановление параметров

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

Восстановление всех настроек

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

Восстановить

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

Параметры импорта и экспорта

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

Экспорт

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



Примечание

Можно импортировать экспортированные параметры устройства на другое устройство.

Импорт

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

Отладка устройства

Можно настроить параметры отладки устройства.

Шаги

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

Включить SSH

Чтобы повысить безопасность сети, отключите службу SSH. Данная настройка используется профессионалами только для отладки устройства.

Печать журнала

Можно нажать **Export** («Экспорт») для экспорта результатов.

Захват сетевого пакета

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

Управление командами отладки

Выберите тип команды **Quick Command** («Быстрая команда») или добавьте информацию в **Custom Command** («Настраиваемая команда»).

Выберите тип платы из выпадающего списка, нажмите **Send** («Отправить»), чтобы отправить команду отладки. Можно просмотреть информацию о полученной команде устройства в разделе **Execution Result** («Результаты выполнения»).

Нажмите **End Debugging** («Завершить отладку»), и устройство вернется в нормальное рабочее состояние.



Примечание

- Для обеспечения работоспособности устройства, нажмите **End Debugging** («Завершить отладку»), чтобы закрыть режим отладки.
 - Если не нажать **End Debugging** («Завершить отладку»), устройство автоматически выйдет из режима отладки через 7 суток.
-

8.6.12 Отладка устройства

Можно настроить параметры отладки устройства.

Шаги

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

Включить SSH

Чтобы повысить безопасность сети, отключите службу SSH. Данная настройка используется профессионалами только для отладки устройства.

Печать журнала

Можно нажать **Export** («Экспорт») для экспорта результатов.

Захват сетевого пакета

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

Управление командами отладки

Выберите тип команды **Quick Command** («Быстрая команда») или добавьте информацию в **Custom Command** («Настраиваемая команда»).

Выберите тип платы из выпадающего списка, нажмите **Send** («Отправить»), чтобы отправить команду отладки. Можно просмотреть информацию о полученной команде устройства в разделе **Execution Result** («Результаты выполнения»).

Нажмите **End Debugging** («Завершить отладку»), и устройство вернется в нормальное рабочее состояние.



Примечание

- Для обеспечения работоспособности устройства, нажмите End Debugging («Завершить отладку»), чтобы закрыть режим отладки.
 - Если не нажать **End Debugging** («Завершить отладку»), устройство автоматически выйдет из режима отладки через 7 суток.
-

8.6.13 Тестирование протокола через веб-интерфейс ПК

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

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

Рисунок 8-13 Тестирование протокола

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

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

8.6.14 Настройка службы проверки на проникновение в сеть через веб-интерфейс ПК

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

Шаги

1. Перейдите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Network Penetration Service** («Система и обслуживание → Обслуживание → Отладка устройства → Служба проверки на проникновение в сеть»).

-
2. Переведите ползунок **Enable Penetration Service** («Включить службу проверки на проникновение»).
 3. Установите **Server IP Address** («IP-адрес сервера») и **Server Port** («Порт сервера»). Создайте **User Name** («Имя пользователя») и **Password** («Пароль»)
 4. Опционально. Можно настроить **Heartbeat Timeout** («Период цикла Heartbeat»). Диапазон значений: от 1 до 6000.
 5. Опционально. Можно посмотреть состояние службы проверки на проникновение. Нажмите **Refresh** («Обновить»), чтобы обновить состояние.
 6. Нажмите **Save** («Сохранить»).
-



Примечание

Служба проверки на проникновение будет автоматически отключена через 48 часов.

8.6.15 Состояние компонентов

Можно просматривать состояние различных компонентов.

Состояние главной полосы

Компонент устройства

Можно просматривать состояние платы контроля доступа, платы управления полосой движения и т. д.

Периферийные устройства

Можно просматривать состояние считывателя карт RS-485.

Температура

Можно просмотреть температуру тумбы.

Движение

Можно просмотреть рабочее состояние датчика двигателя.

Другое

Режим прохода

Можно просмотреть режим входа и выхода.

Состояние входа и выхода

Можно просмотреть состояние входа событий, тревожного выхода и тревоги обнаружения возгорания.

Другое состояние

Можно просмотреть состояние турникета.

8.6.16 Просмотр журнала через веб-интерфейс ПК

Можно искать и просматривать журналы устройства.

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

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

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

8.6.17 Управление сертификатами

Помогает управлять сертификатами сервера/клиента и сертификатом CA.

Примечание

Данная функция поддерживается только у определенных моделей устройств.

Создание и импорт сертификата HTTPS

Шаги

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

Создание и импорт сертификата SYSLOG

Шаги

1. Перейдите **System and Maintenance** → **Safe** → **Certificate Management** («Система и обслуживание → Безопасность → Управление сертификатами»).

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

Импорт сертификата CA

Перед началом

Заранее подготовьте сертификат CA.

Шаги

1. Перейдите **System and Maintenance** → **Safe** → **Certificate Management** («Система и обслуживание → Безопасность → Управление сертификатами»).
2. Создайте идентификатор в области **CA Certificate ID** («Идентификатор сертификата CA»).



Примечание

Идентификатор сертификата не может совпадать с идентификатором уже существующих сертификатов.

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

Раздел 9 Настройка устройства через мобильный веб-интерфейс

9.1 Вход в систему

В систему можно войти через мобильный интерфейс.



Примечание

Устройство должно быть активировано.

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

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

9.2 Обзор

Можно просмотреть состояние устройства, выполнить дистанционное управление и т. д.

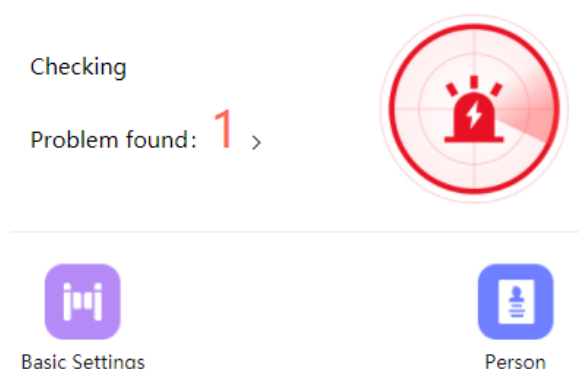


Рисунок 9-1 Состояние и быстрые настройки

Можно просмотреть состояние устройства. В случае возникновения исключения, можно нажать, чтобы просмотреть подробную информацию о компоненте.

Можно нажать, чтобы быстро перейти на страницу основных настроек и страницу пользователя.

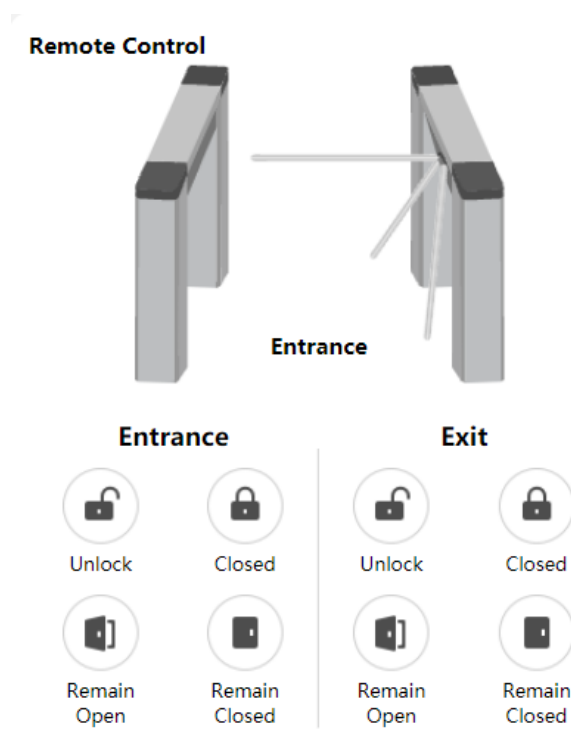


Рисунок 9-2 Дистанционное управление

Можно дистанционно управлять турникетом, нажимая на значок.

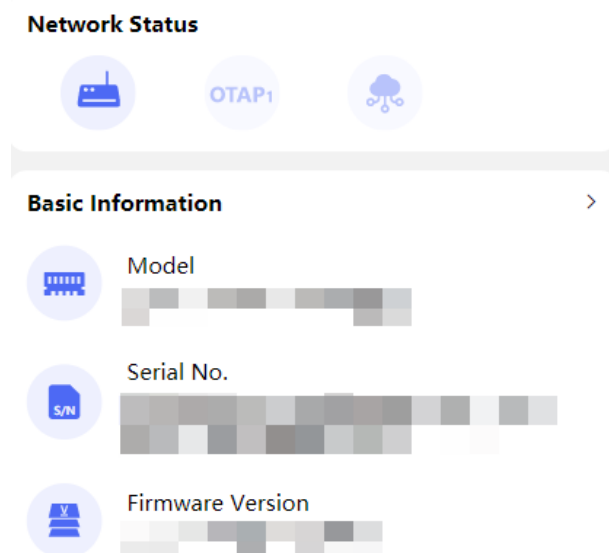


Рисунок 9-3 Состояние сети и основная информация

Можно просмотреть состояние сети, модель, серийный номер и версию прошивки, а также быстро перейти на страницу с основной информацией, нажав на соответствующую кнопку.

9.3 Конфигурация

9.3.1 Основные параметры турникета

Можно настроить основные параметры турникета.

На странице обзора нажмите **Basic Settings** («Основные настройки») в соответствующем поле или нажмите  → **System Settings** → **Basic Information** («Настройки системы → Основная информация»).

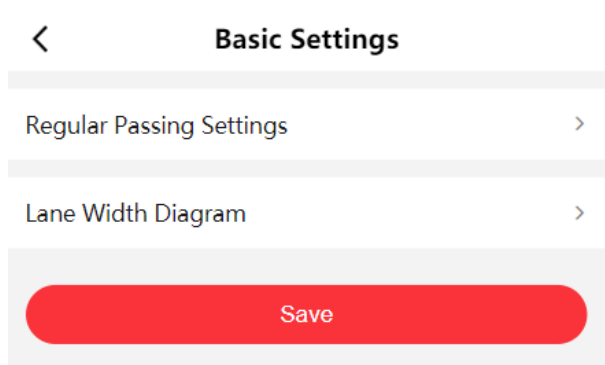


Рисунок 9-4 Основные параметры турникета

Нажмите **Regular Passing Settings** («Настройки обычного прохода»), чтобы задать режим прохода на входе и выходе.

Нажмите **Lane Width Diagram** («Схема ширины полосы»), чтобы просмотреть схему устройства.

Нажмите **Save** («Сохранить»).

9.3.2 Управление пользователями

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

Шаги

1. Нажмите **User** («Пользователь») в записи быстрого доступа или нажмите  → **Person Management** («Управление пользователями»), чтобы перейти на страницу настроек.

< Add Person Save

*Employee ID Please enter.

Name Please enter.

Long-Term Effective User ☐

Start Date 2024-01-23 00:00:00 >

End Date 2034-01-22 23:59:59 >

User Role Normal User >

Card Not added. >

Рисунок 9-5 Добавление пользователя

2. Добавьте пользователя.

- 1) Нажмите +.
- 2) Настройте следующие параметры.

ID сотрудника

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

Имя

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

Пользователь с длительным разрешением

Настройте долгосрочное разрешение для пользователя.

Дата начала / Дата окончания

Настройте **Start Date** («Дата начала») и **End Date** («Дата окончания») разрешения пользователя.

Роль пользователя

Выберите роль пользователя.

Карта

Добавление карты. Нажмите +. Введите **Card No.** («№ карты») и выберите **Card Type** («Тип карты»). Нажмите **Save** («Сохранить»), чтобы добавить карту.

-
- 3) Нажмите **Save** («Сохранить»).
3. Нажмите на пользователя в списке, чтобы изменить информацию о нем.
4. Можно осуществлять поиск по идентификатору сотрудника в поле поиска.

9.3.3 Просмотр основной информации об устройстве

Здесь можно посмотреть название устройства, язык, модель, серийный номер, версию, MAC-адрес и т. д.

Нажмите  → **System Settings** → **Basic Information** («Системные настройки → Основная информация»).

Можно изменить название устройства.

Можно посмотреть язык устройства, модель, серийный номер, версию, локальный номер RS-485, количество тревожных входов и выходов, MAC-адрес, заводскую информацию и т. д.

Нажмите **Device Capacity** («Емкость устройства»), чтобы посмотреть количество и емкость устройств (людей, карт и событий).

Нажмите **Save** («Сохранить»).

9.3.4 Настройка времени устройства

Установите часовой пояс и текущее время устройства.

Нажмите  → **System Settings** → **Time Settings** («Системные настройки → Настройки

времени»).

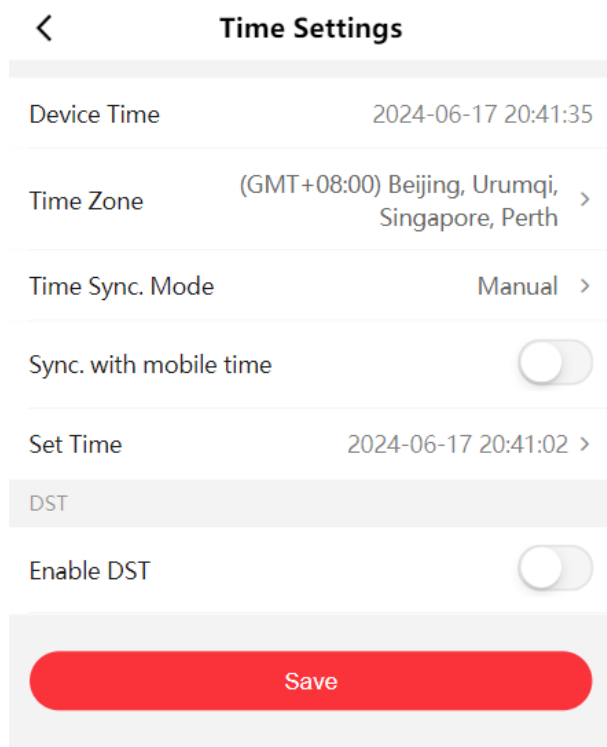


Рисунок 9-6 Настройка времени

Часовой пояс

Нажмите, чтобы выбрать часовой пояс для устройства.

Синхронизация времени Режим

Вручную

По умолчанию включена синхронизация вручную. Можно установить время на устройстве вручную.

NTP

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

Включение DST

Можно включить DST и установить время начала и окончания. А также установить смещение.

Нажмите **Save** («Сохранить»).

9.3.5 Управление пользователями

Можно изменить пароль пользователя.

На главной странице нажмите  → **User Management** («Управление пользователями»).

Нажмите на пользователя, введите старый пароль, создайте новый пароль и подтвердите пароль.

Нажмите **Save** («Сохранить»).

9.3.6 Сеть

Проводная сеть

Настройка проводной сети.

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

Тип NIC

Выберите тип NIC из выпадающего списка.

DHCP

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

При включении этой функции система автоматически задаст IPv4-адрес, IPv4-маску подсети и IPv4-шлюз.

MAC-адрес и MTU

Можно просмотреть MAC-адрес и MTU по умолчанию.

Режим IPv6

Анонс маршрутизатора

IPv6 адрес создается путем объединения анонса маршрутизатора и MAC-адреса устройства.



Примечание

Маршрутизатор, подключенный к устройству, должен поддерживать режим анонса.

Вручную

Введите **IPv6 Address** («IPv6-адрес»), **IPv6 Subnet Mask** («IPv6-маска подсети») и **IPv6 Default Gateway** («IPv6-шлюз по умолчанию»). Для получения подробной информации свяжитесь с сетевым администратором.

DHCP

IPv6 адрес назначается сервером, маршрутизатором или шлюзом.

DNS-сервер



Примечание

Настроить DNS-сервер можно только при включенном DHCP.

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

Настройка параметров порта

Можно настроить HTTP и HTTPS при доступе к устройству через сеть.

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

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.

Доступ к платформе

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите → **Device Access** → **Hik-Connect** («Доступ устройств → Hik-Connect») для перехода на страницу настроек.



Примечание

Hik-Connect — это приложение для мобильных устройств. С помощью приложения можно просматривать видео в реальном времени с устройства, получать тревожные уведомления и т. д.

2. Сдвиньте ползунок для включения функции.
3. Можно включить **Custom** («Пользовательская настройка») для ввода адреса сервера.



Примечание

- От 6 до 12 букв (от а до z, от А до Z) или цифры (от 0 до 9), с учетом регистра. Рекомендуется использовать комбинацию не менее 8 букв или цифр.

4. Можно просмотреть **Register Status** («Состояние регистрации») и **Binding Status** («Состояние привязки»).
5. Можно нажать **Bind An Account → View QR Code** («Привязка учетной записи → Просмотр QR-кода») и сканировать QR-код, чтобы привязать учетную запись.
6. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Настройка протокола OTAP

Можно получить доступ к платформе обслуживания устройства по протоколу OTAP для поиска и получения информации об устройстве, загрузки состояния работы устройства и исключений, перезагрузки и обновления.

Шаги

1. Нажмите → **Device Access** → **OTAP** («Доступ к устройству → OTAP»).

< OTAP

Enable

* Server Address 0.0.0.0

* Port

* Device ID

* Encryption Key

Register Status Offline

Test

Save

Рисунок 9-7 OTAP

2. Сдвиньте ползунок **Enable** («Включить»).
3. Установите адрес сервера, порт, идентификатор устройства и ключ шифрования.
4. Нажмите **Test** («Тест») и убедитесь, что устройство может подключиться к серверу и регистрация завершена.

5. Нажмите **Save** («Сохранить»).

Результат

Обновите веб-страницу или перезагрузите устройство, чтобы убедиться, что параметр **Register Status** («Состояние регистрации») для ОТАР изменился на «в сети».

Настройка службы проверки на проникновение в сеть

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

Шаги

1. Нажмите  → **Device Access** → **Network Penetration Settings** («Доступ к устройству → Настройки проверки на проникновение в сеть»), чтобы перейти на страницу конфигурации.
2. Выберите **Enable Penetration Service** («Включить службу проверки на проникновение»).
3. Введите **Server IP Address** («IP-адрес сервера») и **Server Port** («Порт сервера»).
4. Введите **User** («Имя пользователя») и **Password** («Пароль») для входа в систему.
5. Установите **Heartbeat Timeout** («Период цикла Heartbeat»). Диапазон: от 1 до 6000.
6. Можно просмотреть **Online Status** («Состояние онлайн»). Нажмите **Refresh** («Обновить»), чтобы просмотреть последнее состояние.
7. Нажмите **Save** («Сохранить»).

9.3.7 Поиск событий

Нажмите  → **Event Search** («Поиск событий»).

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



Примечание

Поддерживает поиск по имени до 32 символов.

Информация будет отображена в виде списка.

9.3.8 Настройка параметров аудио

Установите громкость устройства.

Шаги

1. Нажмите  → **Audio** («Аудио»), чтобы перейти на страницу настроек.
2. Можно отрегулировать громкость устройства в соответствии с потребностями.
3. Можно включить голосовые предупреждения в соответствии с потребностями.

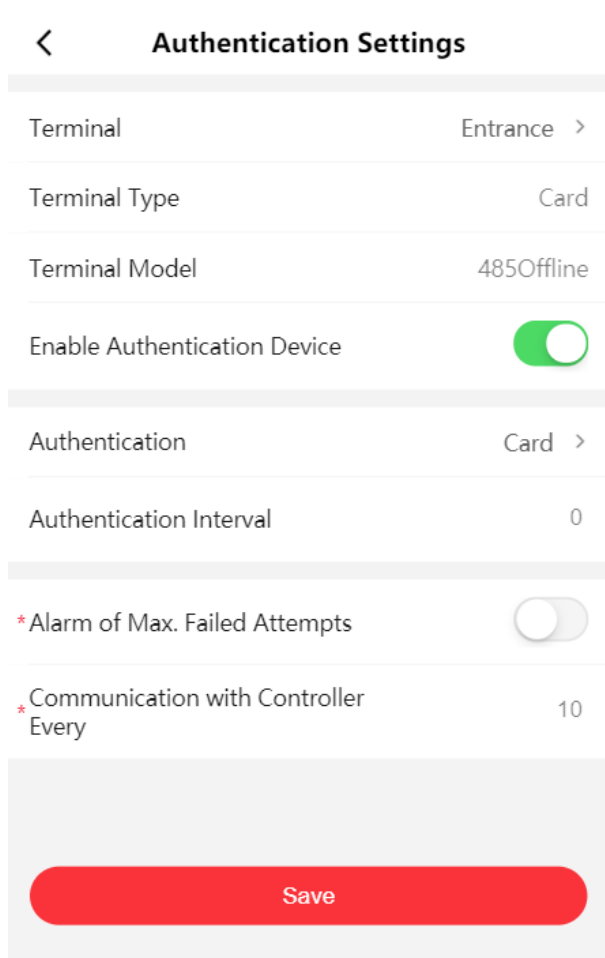
9.3.9 Настройки параметров контроля доступа

Настройка параметров аутентификации

Настройка параметров аутентификации.

Шаги

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



Authentication Settings	
Terminal	Entrance >
Terminal Type	Card
Terminal Model	485Offline
Enable Authentication Device	☒
Authentication	Card >
Authentication Interval	0
* Alarm of Max. Failed Attempts	☐
* Communication with Controller Every	10
Save	

Рисунок 9-8 Настройка аутентификации

2. Нажмите **Save** («Сохранить») после настройки.

Терминал

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

Тип / модель терминала

Можно просмотреть текущие тип и модель терминала.

Включить устройство с функцией аутентификации

Терминал можно использовать для считывания карт в обычном режиме, если эта функция включена.

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. Если другой пользователь пройдет аутентификацию в течение заданного интервала, он сможет пройти аутентификацию повторно.



Примечание

Диапазон настройки от 0 до 255 с.

Запуск тревоги при достижении максимального количества неудачных попыток считывания карты

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



Примечание

Диапазон настройки от 1 до 10.

Связь с контроллером

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

Настройка параметров двери

Можно задать название двери, продолжительность открытия и параметры кнопки выхода.

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

Door Parameters	
Door No.	Entrance >
Name	
*Open Duration	8
Exit Button Type	Remain Open >
*Door Remain Open Duration with First Person (min)	10
Save	

Рисунок 9-9 Параметры двери

Выберите вход или выход для настройки, задайте имя и продолжительность открытия, а также выберите тип кнопки выхода.

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

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

Настройки терминала

Установите режим работы.

Нажмите  → **Access Control** → **Terminal Parameters** («Контроль доступа → Параметры терминала»), чтобы перейти на страницу настроек.

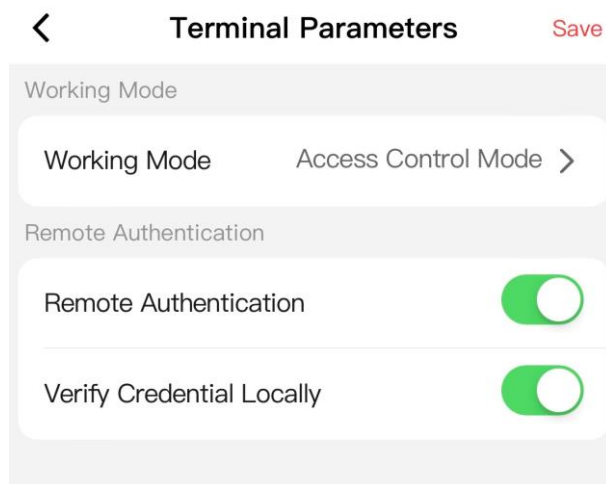


Рисунок 9-10 Параметры терминала

Режим без разрешений

Устройство не будет проверять разрешение пользователя, а только срок действия его данных. Если срока действия данных пользователя еще активен, турникет откроется. Можно включить функцию **Verify Credential Locally** («Локальная проверка учетных данных»). После включения функции устройство будет проверять только разрешение пользователя без шаблона расписания и т. д.

Режим контроля доступа

Устройство будет работать в обычном режиме и проверять разрешение пользователя на открытие.

Удаленная аутентификация

Устройство загрузит на платформу информацию для аутентификации пользователя. Платформа определит, открывать турникет или нет.

Локальная проверка учетных данных

Устройство будет проверять только разрешение пользователя без шаблона расписания и т. д.

Настройка параметров безопасности карты

Настройте карты для устройства.

Нажмите  → **Access Control** → **Card Security** («Контроль доступа → Безопасность карты»).

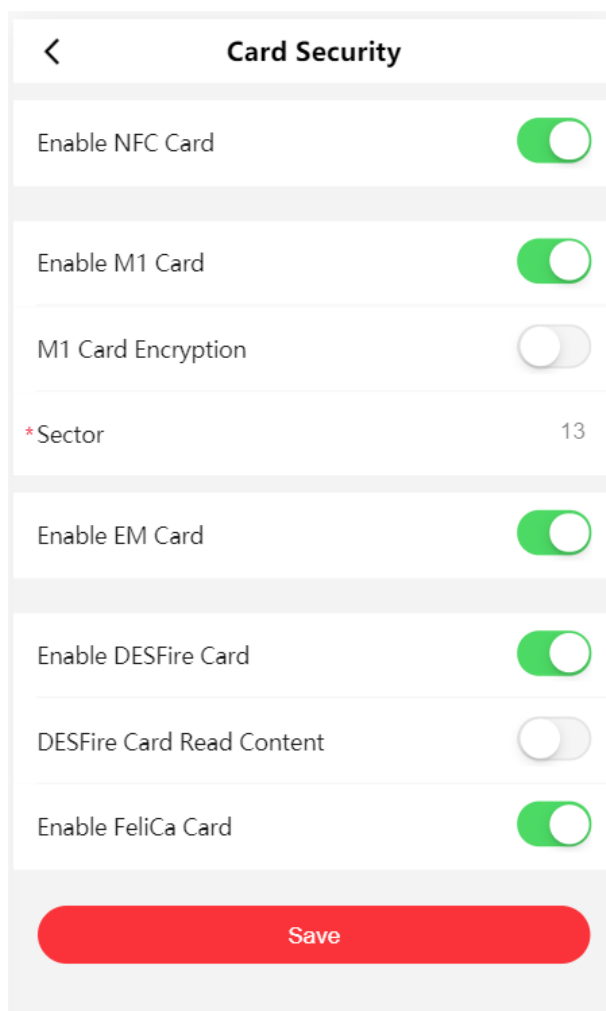


Рисунок 9-11 Безопасность карты

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

Включение распознавания NFC-карты

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

Включение распознавания M1-карты

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

Шифрование M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

Сектор

Активируйте функцию и установите сектор шифрования.



Примечание

Рекомендуется зашифровать сектор 13.

Активация распознавания EM-карты

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



Примечание

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

Активация распознавания DESfire-карты

Устройство может считывать данные с DESfire-карты.

Чтение DESFire-карт

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

Активация распознавания FeliCa-карты

Устройство может считывать данные с FeliCa-карты.

9.3.10 Настройки подсчета людей

Настройте подсчет людей.

Шаги

1. Нажмите  → **People Counting Settings** («Настройки подсчета людей»), чтобы перейти на страницу конфигурации.
2. Включите **People Counting** («Подсчет людей»), и устройство будет подсчитывать количество проходящих мимо людей.
3. Включите **Device Offline People Counting** («Автономный подсчет людей на устройстве»), устройство будет подсчитывать количество людей, даже если оно находится в автономном режиме.
4. Включите **Passing Event Record** («Запись о проходящих людях»), устройство будет загружать события, когда люди проходят мимо.
5. Установите **Person Statistics Type** («Тип статистики по людям»).

Недействительно

Отключите функцию подсчета людей.

Детекция прохода

Количество всех проходящих людей.

Номер аутентификации

Количество прошедших людей, проверенных с помощью считывания карт, распознавания лиц и т. д.

6. Настройте **Passing Direction** («Направление прохода») на устройстве.
7. Нажмите **Clear** («Очистить»), чтобы удалить всю информацию о подсчете людей.
8. Нажмите **Save** («Сохранить»).

9.3.11 Другие настройки

Нажмите  → **Other Settings** («Другие настройки»), чтобы перейти на страницу конфигурации.

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

Длительность тревожного выхода

Длительность тревожного выхода варьируется от 0 до 3599 секунд. 0 означает непрерывный выход.

Яркость световой панели

Перетащите указатель или введите значение, чтобы настроить яркость. Чем больше значение, тем ярче становится индикатор.

Правило запрета двойного прохода

Установите правило запрета двойного прохода: **Authentication Status** («Состояние аутентификации») или **By Passing Status** («Состояние прохождения»).

По состоянию аутентификации

Пользователь должен пройти аутентификацию, в противном случае функция запрета двойного прохода не будет активирована.

Состояние прохождения

Пользователь не может пройти аутентификацию, и запрет двойного прохода будет выполнен.

Режим памяти

При включении режима памяти допускается предъявление нескольких карт для одновременного прохода нескольких человек. Когда количество проходящих людей превышает количество предъявленных карт, или после того, как последний прошедший человек не прошел, и в течение времени открытия двери не прошло ни одного другого человека, дверь автоматически закроется.

По умолчанию функция отключена.

Тип входа пожарной тревоги

В нормально разомкнутом состоянии закрытие активирует противопожарную защиту. В нормально замкнутом состоянии открытие активирует противопожарную защиту.

9.3.12 Обновление и техническое обслуживание

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

Перезагрузка устройства

Нажмите  → **Restart** («Перезагрузить»).

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

Обновление

Нажмите  → **Upgrade** («Обновление»).

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

Примечание

Не выключайте устройство во время обновления.

Восстановление параметров

Нажмите  → **Default** («По умолчанию»).

Восстановление настроек по умолчанию

Нажмите **Restore to Default Settings** («Восстановление настроек по умолчанию»), введите пароль администратора и нажмите **OK**. Настройки устройства будут восстановлены до настроек по умолчанию, за исключением IP-адреса устройства и информации о пользователе.

Восстановление настроек изготовителя

Нажмите **Restore to Factory Settings** («Восстановление заводских настроек»), введите пароль администратора и нажмите **OK**. Все параметры будут сброшены до заводских настроек. Перед первым входом в систему необходимо активировать устройство.

Экспорт журнала

Нажмите  → **Log Export** («Экспорт журнала»).

Выберите тип журнала и нажмите **Export** («Экспорт»), чтобы загрузить журнал технического обслуживания.

9.3.13 Выход из системы

Выйдите из страницы настроек.

Нажмите  → **Logout** («Выход из системы»), нажмите **OK**.

Если нужно перейти на страницу настроек, необходимо снова ввести имя пользователя и пароль.

9.3.14 Лицензия на ПО с открытым исходным кодом

Можно просмотреть лицензии на ПО с открытым исходным кодом.

Нажмите , чтобы перейти на страницу.

Нажмите **Open Source Software Licenses** («Лицензии на ПО с открытым исходным кодом»).

9.3.15 Просмотр документации пользователя

Просмотр документации пользователя.



Примечание

Просмотр документации возможен только при входе в мобильный веб-интерфейс по IP-адресу. При входе через точку доступа данная функция не поддерживается.

Нажмите , чтобы перейти на страницу.

Нажмите **View Online Document** («Просмотр документации онлайн»), чтобы открыть руководство пользователя.

Раздел 10 Другие платформы

Также можно настроить устройство с помощью клиентского программного обеспечения iVMS-4200 или HikCentral Access Control. Подробная информация представлена в соответствующих руководствах.

Клиентское ПО iVMS-4200

Нажмите ссылку, чтобы просмотреть руководство пользователя клиентского программного обеспечения.

<http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247>

A. Событие и тип тревоги

Событие	Тип тревоги
Время прохода истекло	—

В. Описание ошибок

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

Причина ошибки	Код
Дополнительная плата отключена (если плата не установлена, появится код ошибки «49» или «59», но устройство будет работать нормально).	49/59

