



Тумбовый распашной турникет

Руководство пользователя

Руководство пользователя

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

Это руководство относится к тумбовым распашным турникетам.

Название продукта	Модель	Описание
Тумбовый распашной турникет	DS-K3B601-L серия	Левая тумба
	DS-K3B601-M серия	Центральная тумба
	DS-K3B601-R серия	Правая тумба
	DS-K3B601A-L серия	Левая тумба
	DS-K3B601A-M серия	Центральная тумба
	DS-K3B601A-R серия	Правая тумба

Примечание: Маркировка «L» используется для левой тумбы, маркировка «M» используется для центральной тумбы и маркировка «R» используется для правой тумбы.

Руководство содержит инструкции по использованию Продукта. Программное обеспечение, включенное в Продукт, регулируется пользовательским лицензионным соглашением этого Продукта.

О руководстве

Вся информация, включая текст, изображения и графики является интеллектуальной собственностью Hikvision Digital Technology Co., Ltd. или ее дочерних компаний (далее «Hikvision»). Данное руководство пользователя (далее «Руководство») не подлежит воспроизведению, изменению, переводу или распространению, частично или целиком, без предварительного разрешения Hikvision.

Торговые марки

HIKVISION и другие торговые марки Hikvision и логотипы являются интеллектуальной собственностью Hikvision в различных юрисдикциях. Другие торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев. Права на использование таких товарных знаков без явного разрешения не предоставляются.

Правовая информация

ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, HIKVISION НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЯ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ И ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ, В ОТНОШЕНИИ ДАННОГО РУКОВОДСТВА. HIKVISION НЕ РУЧАЕТСЯ, НЕ ГАРАНТИРУЕТ И НЕ ДЕЛАЕТ НИКАКИХ ЗАЯВЛЕНИЙ ОТНОСИТЕЛЬНО ИСПОЛЬЗОВАНИЯ РУКОВОДСТВА, А ТАКЖЕ ПРАВИЛЬНОСТИ, ТОЧНОСТИ ИЛИ НАДЕЖНОСТИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В НЕМ. ВЫ ИСПОЛЬЗУЕТЕ ДАННОЕ РУКОВОДСТВО И ПОЛНОСТЬЮ ПОЛАГАЕТЕСЬ НА НЕГО НА СВОЙ СТРАХ И РИСК.

ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ; НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, НАША КОМПАНИЯ ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.

ЗАКОНЫ, РЕГУЛИРУЮЩИЕ ВИДЕОНАБЛЮДЕНИЕ, ВАРЬИРУЮТСЯ В ЗАВИСИМОСТИ ОТ СТРАНЫ. ПОЖАЛУЙСТА, ПРОВЕРЬТЕ ВСЕ СООТВЕТСТВУЮЩИЕ ЗАКОНЫ ВАШЕЙ СТРАНЫ ПЕРЕД ИСПОЛЬЗОВАНИЕМ ОБОРУДОВАНИЯ. НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА

ИСПОЛЬЗОВАНИЕ ОБОРУДОВАНИЯ В НЕЗАКОННЫХ ЦЕЛЯХ.

В СЛУЧАЕ КОНФИЛИКТОВ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.

Поддержка

Если у вас есть какие-либо вопросы, пожалуйста, не стесняйтесь обращаться к местному дилеру.

Регулирующая информация

Информация о FCC

Пожалуйста, обратите внимание, что изменения или модификации, явно не утвержденные стороной, ответственной за соответствие, могут привести к лишению пользователя права на эксплуатацию данного оборудования.

Соответствие FCC: Это оборудование было проверено и найдено соответствующим регламенту для цифрового устройства Класа В, применительно к части 15 Правил FCC. Данный регламент разработан для того, чтобы обеспечить достаточную защиту от вредных эффектов, возникающих при использовании оборудования в жилых помещениях. Это оборудование генерирует, использует, и может излучать радиоволны на разных частотах, и если не установлено и не используется в соответствии с инструкциями, может создавать помехи для радиосвязи. Тем не менее, нет никакой гарантии, что помехи не возникнут в каких-либо конкретных случаях установки. Если данное оборудование вызывает помехи радио- или телевизионного приема, что можно определить путем выключения оборудования и включения, пользователю рекомендуется попытаться устранить помехи одним или несколькими из следующих способов:

- Изменить ориентацию или местоположение приемной антенны.
- Увеличить расстояние между оборудованием и приемником.
- Подключить оборудование к розетке в цепи, отличной от той, к которой подключен приемник.
- Обратитесь к дилеру или опытному радио/телемастеру.

Это оборудование следует устанавливать и эксплуатировать на расстоянии не менее 20 см между излучателем и вашим телом.

Условия FCC

Это устройство соответствует регламенту для цифрового устройства применительно к части 15 Правил FCC. При работе необходимо выполнение следующих двух условий:

1. Данное устройство не должно создавать вредных помех.
2. Устройство должно выдерживать возможные помехи, включая и те, которые могут привести к выполнению нежелательных операций.

Соответствие стандартам ЕС



Данный продукт и, если применимо, также поставляемые принадлежности отмечены знаком "CE" и, следовательно, согласованны с европейскими стандартами, перечисленными под директивой RE 2014/53/EU, директивой

EMC 2014/30/EU, директивой RoHS 2011/65/EU.



2012/19/EU (директива WEEE): Продукты, отмеченные данным знаком, запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Для надлежащей утилизации верните продукт поставщику при покупке эквивалентного нового оборудования, либо избавьтесь от него в

специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info



2006/66/ЕС (директива о батареях): Данный продукт содержит батарею, которую запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Подробная информация о батарее изложена в документации продукта. Батарея отмечена данным значком, который может включать наименования, обозначающие содержание кадмия (Cd), свинца (Pb)

или ртути (Hg). Для надлежащей утилизации возвратите батарею своему поставщику, либо избавьтесь от неё в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info

Инструкция по технике безопасности

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

Меры предосторожности разделены на "Предупреждения" и "Предостережения".

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



Предупреждения

- Использование продукта должно соответствовать нормам электробезопасности, правилам пожарной безопасности и другим связанным нормам страны и региона.
- Пожалуйста, используйте качественный адаптер питания. Напряжение блока питания не должно быть меньше требуемого значения.
- Не подключайте несколько устройств к одному блоку питания, перегрузка адаптера может привести к перегреву или возгоранию.

- Пожалуйста, убедитесь, что питание отключено перед подключением, установкой или демонтажем устройства.
- Если устройство устанавливается на стену или потолок, оно должно быть надежно закреплено.
- Если из устройства идет дым или доносится шум – отключите питание, извлеките кабель и свяжитесь с сервисным центром.
- Если продукт не работает должным образом, обратитесь к дилеру или в ближайший сервисный центр. Не пытайтесь самостоятельно разобрать устройство. (Мы не несем ответственность за проблемы, вызванные несанкционированным ремонтом или техническим обслуживанием.)



Предостережения

- В некоторых ситуациях нержавеющая сталь может быть подвержена коррозии. Вам необходимо чистить и ухаживать за устройством, используя очиститель для нержавеющей стали. Рекомендуется чистить устройство каждый месяц.
- Не бросайте устройство и не подвергайте его ударам, воздействию сильных электромагнитных излучений. Избегайте установки на поверхности, подверженные вибрациям и встряскам (игнорирование этого условия может привести к поломке оборудования).
- Не устанавливайте устройство в условиях экстремально высоких/низких температур (обратитесь к спецификации устройства за подробной информацией), в пыльной или влажной среде, не подвергайте его воздействию сильного электромагнитного излучения.
- Устройство, предназначенное для использования в помещении, не должно подвергаться воздействию дождя или влажности.
- Запрещено использование устройства под воздействием прямых солнечных лучей, в условиях недостаточной вентиляции и рядом с источниками тепла, такими как обогреватели и другие нагревательные устройства (игнорирование этого условия может привести к возгоранию).
- Не направляйте устройство на солнце или другие яркие источники света, так как это может вызвать блики (которые не являются неисправностью), но влияют на продолжительность работы датчика.
- Пожалуйста, используйте перчатки 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 чистки внешних и внутренних поверхностей устройства, пожалуйста, используйте мягкую и сухую ткань, не используйте щелочные моющие средства.
- Пожалуйста, сохраняйте упаковку для последующей транспортировки устройства. В случае неполадок устройства, Вам необходимо будет вернуть оборудование производителю в оригинальной упаковке. Транспортировка без оригинальной упаковки может привести к повреждению устройства и дополнительным расходам.
- Неправильное использование или замена батареи может привести к опасности взрыва. Проводите замену на такие же батареи или аналогичные. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем батарей.

Содержание

Глава 1	Обзор	8
1.1	Представление.....	8
1.2	Основные особенности.....	8
Глава 2	Установка	10
2.1	Разборка турникетов.....	10
2.2	Установка тумб.....	10
Глава 3	Подключение.....	12
3.1	Представление компонентов	12
3.2	Подключение питания	13
3.3	Подключение соединительного кабеля	14
3.4	Описание клемм.....	15
3.4.1	Описание клемм ведущей платы управления проходом	15
3.4.2	Описание клемм подчиненной платы управления проходом	16
3.4.3	Описание клемм основной платы управления	17
3.4.4	Описание ID последовательного порта основной платы управления.....	20
3.4.5	Подключение по RS-485.....	21
3.4.6	Подключение по RS-232.....	22
3.4.7	Подключение по Wiegand	23
3.4.8	Подключение платы управления турникетом	24
3.4.9	Подключение тревожного выхода.....	25
3.5	Подключение литиевой батареи (Опционально).....	25
Глава 4	Настройки устройства.....	27
4.1	Установка закрытого положения	27
4.2	Сопряжение пульта дистанционного управления (Опционально)	28
4.3	Инициализация устройства	29
4.4	Переключение режимов RS-485/RS-232	29
4.5	Переключение режима релейного выхода (НО/НЗ)	30
4.5.1	Режим вывода реле управления турникетом	30
4.5.2	Режим вывода реле тревоги (НО/НЗ)	30
Глава 5	Активация устройства	31
5.1	Активация через ПО SADP.....	31
5.2	Активация при помощи клиентского ПО.....	32
Глава 6	Операции в клиентском ПО	35
6.1	Функциональный модуль	35

6.2	Регистрация пользователей и вход в систему	35
6.3	Конфигурация системы.....	37
6.4	Управление контролем доступа.....	37
6.4.1	Добавление устройства контроля доступа	39
6.4.2	Просмотр состояния устройства	52
6.4.3	Редактирование основной информации	53
6.4.4	Настройки RS-485	54
6.4.5	Аутентификация с шифрованием карт M1.....	55
6.4.6	Удаленная конфигурация.....	56
6.5	Управление организацией.....	68
6.5.1	Добавление организации.....	68
6.5.2	Изменение и удаление организации	68
6.6	Управление людьми.....	69
6.6.1	Добавление людей.....	69
6.6.2	Управление людьми.....	82
6.6.3	Выдача карт в пакетном режиме	82
6.7	Конфигурация разрешений	85
6.7.1	Добавление разрешений.....	85
6.7.2	Применение разрешений.....	86
6.8	Расширенные функции	87
6.8.1	Параметры контроля доступа	88
6.8.2	Аутентификация считывателя карт	92
6.8.3	Многократная аутентификация.....	94
6.8.4	Открытие двери при помощи первой карты	97
6.8.5	Запрет обратного прохода.....	99
6.8.6	Межконтроллерный запрет обратного прохода	100
6.9	Поиск событий контроля доступа	104
6.9.1	Поиск локальных событий контроля доступа	105
6.9.2	Поиск удаленных событий контроля доступа.....	105
6.10	Конфигурация событий контроля доступа	105
6.10.1	Привязка событий контроля доступа	106
6.10.2	Связанные действия тревожного входа контроля доступа	107
6.10.3	Привязка карт/событий	108
6.10.4	Межустройственная привязка	111
6.11	Управление состоянием двери	113
6.11.1	Управление группой контроля доступа	113

6.11.2	Анти-контроль точки контроля доступа (Дверь).....	115
6.11.3	Конфигурация длительности состояния.....	116
6.11.4	Запись проводки карты в реальном времени	118
6.11.5	Тревога контроля доступа в реальном времени	118
6.12	Управление охраной	120
6.13	Время и посещаемость	120
6.13.1	Управление расписанием смены.....	121
6.13.2	Обработка посещаемости	128
Приложение А	Рекомендации по сканированию отпечатков пальцев	131
Приложение В	Описание DIP-переключателей.....	132
	Представление DIP-переключателей.....	132
	Соответствующие DIP-переключателям функции	132
Приложение С	Таблица значений аудио индексов.....	134
Приложение D	Описание кодов ошибок	135

Глава 1 Обзор

1.1 Представление

Тумбовый распашной турникет с двумя створками и 12 ИК-детекторами предназначен для обнаружения несанкционированного входа или выхода. При использовании распашного турникета, интегрированного с системой контроля доступа, человек должен аутентифицироваться для прохождения через него при помощи IC или ID-карты, сканирования QR-кода и т.д. Такие турникеты широко используются на аттракционах, стадионах, строительных площадках, в жилых домах и т. д.

1.2 Основные особенности

- 32-х битный высокоскоростной процессор
- Передача данных по TCP/IP сети
Данные специально зашифрованы, чтобы устранить проблему утечки конфиденциальной информации.
- Проверка разрешений и предотвращение несоблюдения дистанции при прохождении турникета
- Доступны режимы: «оставить открытым»/«оставить закрытым»
- Двухнаправленный проход (Вход/Выход)
Скорость открытия и закрытия турникета может быть настроена в соответствии с потоком посетителей.
- При защемлении человека турникет будет заблокирован или перестанет работать
- Противодействие принудительному доступу
Турникет будет автоматически заблокирован, если не был подан сигнал открытия турникета. Он может выдержать усилие до 120 Нм.
- Самоконтроль, самодиагностика и автоматическая тревога
- Запуск аудио и визуальной тревоги при детекции вторжения, несоблюдения дистанции при прохождении турникета, обратного прохода и перепрыгивания турникета.
- Удаленный контроль и управление
- Онлайн/офлайн работа
- Светодиод показывает состояние входа/выхода и прохождения через турникет
- Турникет находится в состоянии свободного доступа при отключении питания; Если в устройстве установлена литиевая батарея (Опционально), турникет останется в открытом состоянии при отключении питания
- Прохождение при пожаре
Когда срабатывает пожарная сигнализация, турникет автоматически открывается для аварийной эвакуации.
- Настройка действительного времени прохождения

Система отменит разрешение на прохождение через турникет, если человек не пройдет через него в течение заданного действительного времени прохода.

- Открытие/закрытие турникета в соответствии с шаблоном расписания.
- Можно добавить до 3000 карт посетителей и до 60 000 других карт, кроме карт посетителей

Глава 2 Установка

2.1 Разборка турникетов

Цель:

Перед установкой вы должны использовать ключ, чтобы открыть турникеты.

Посмотрите изображения ниже, чтобы ознакомиться с местоположением замков и монтажного отверстия.



2.2 Установка тумб

Перед началом:

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

Примечания:

- Устройство должно быть установлено на бетонную поверхность или на другие негорючие поверхности.
- Если область установки находится слишком близко к стене, убедитесь, что расстояние между тумбой и стеной не превышает 120 мм, иначе вы не сможете открыть верхнюю панель тумбы.

Шаги:

1. Нарисуйте центральную линию на установочной поверхности для установки центральной тумбы.
2. Нарисуйте еще две параллельные линии с каждой стороны от центральной линии для установки двух других тумб.

Примечание: Расстояние между двумя ближайшими линиями составляет $L + 200$ мм, где L - ширина прохода.

3. Просверлите отверстия на поверхности установки в соответствии с монтажными отверстиями на тумбах и вставьте расширительные элементы.

4. Проложите соединительные кабели для осуществления связи между тумбами турникета.

Примечание: Для получения подробной информации о прокладке и подключении соединительных кабелей смотрите *Раздел **Ошибка! Источник ссылки не найден.** Подключение соединительного кабеля.*

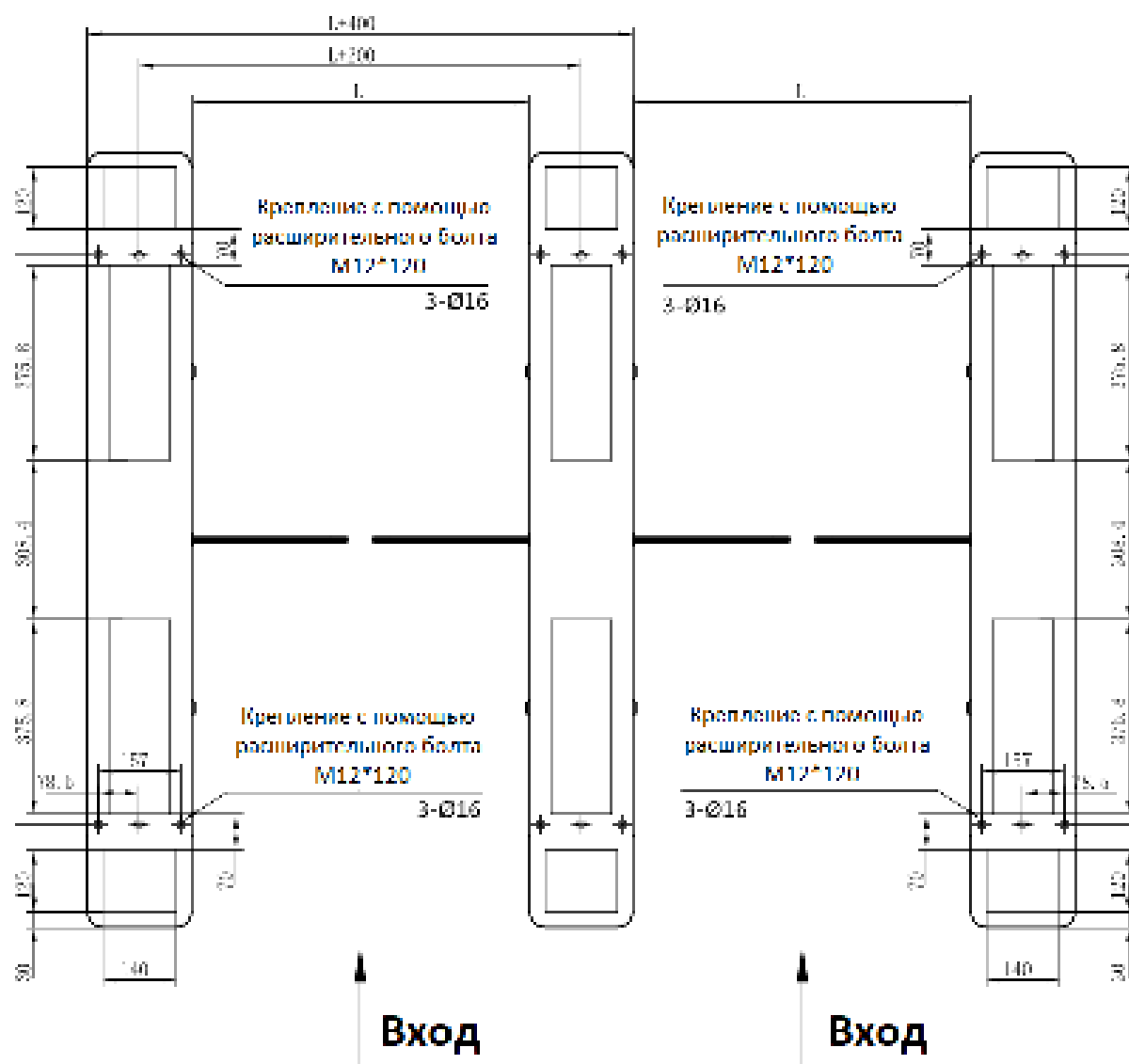
5. В соответствии с отметками **Entrance** («вход») и **Exit** («выход») на тумбах переместите их на соответствующие позиции.

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

6. Закрепите тумбы при помощи расширительных болтов.

Примечание: Не погружайте тумбы в воду. В особых случаях высота погружения должна быть не более 10 мм.

Схема установки представлена ниже:



Глава 3 Подключение

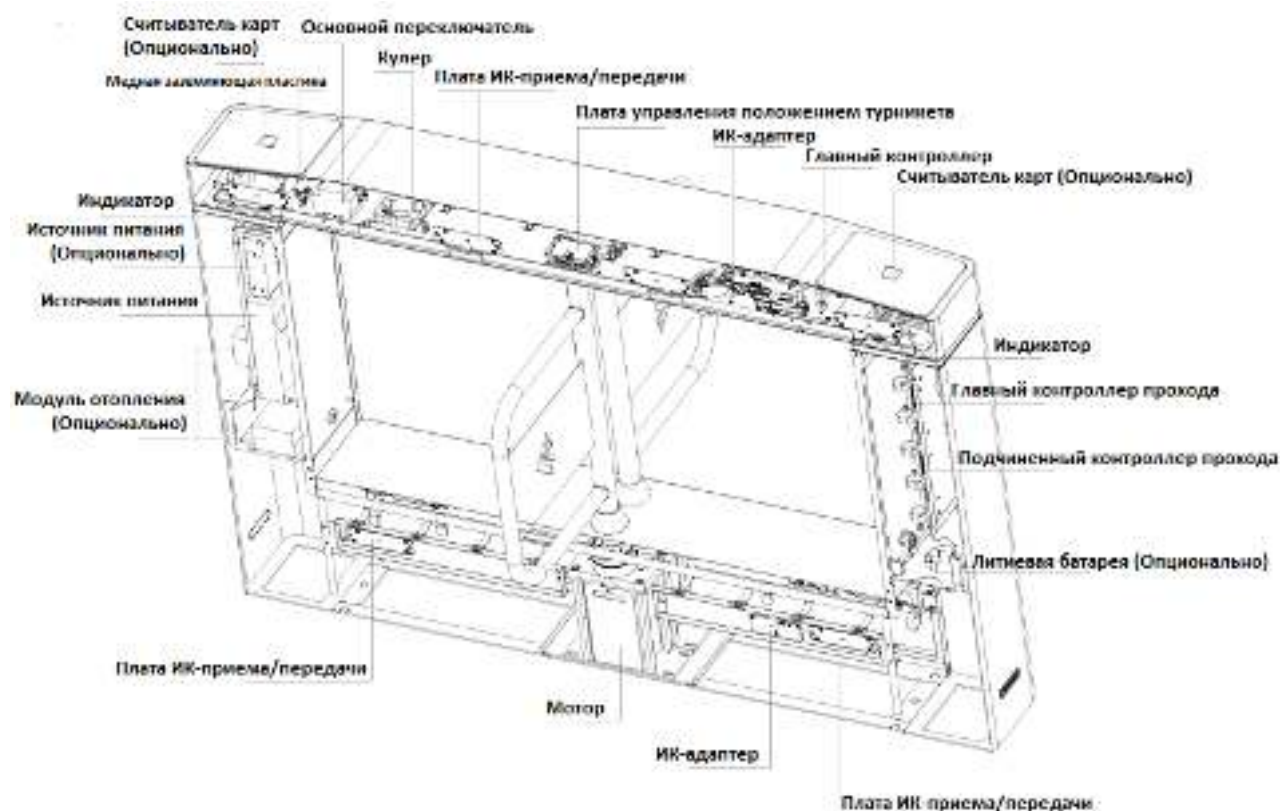
3.1 Представление компонентов

Цель:

По умолчанию основные компоненты распашного турникета хорошо соединены. Вы должны соединить турникеты вместе для связи и соединить турникет с источником переменного тока.

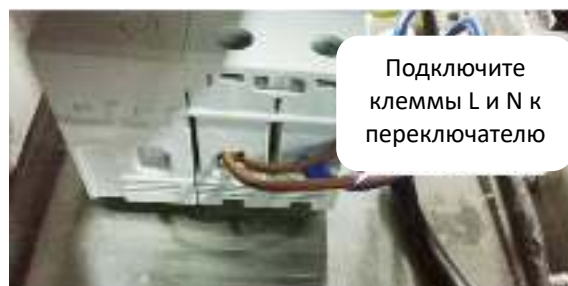
Примечание: Колебание напряжения электропитания составляет AC от 100 до 220 В, от 50 до 60 Гц.

Изображение, показанное ниже, описывает положение каждого компонента в тумбе распашного турникета.



3.2 Подключение питания

Подключите источник питания к переключателю в тумбе турникета. Клемма L и клемма N находятся на переключателе, а клемма PE должна подключаться к заземляющему проводу (желтый и зеленый провода).

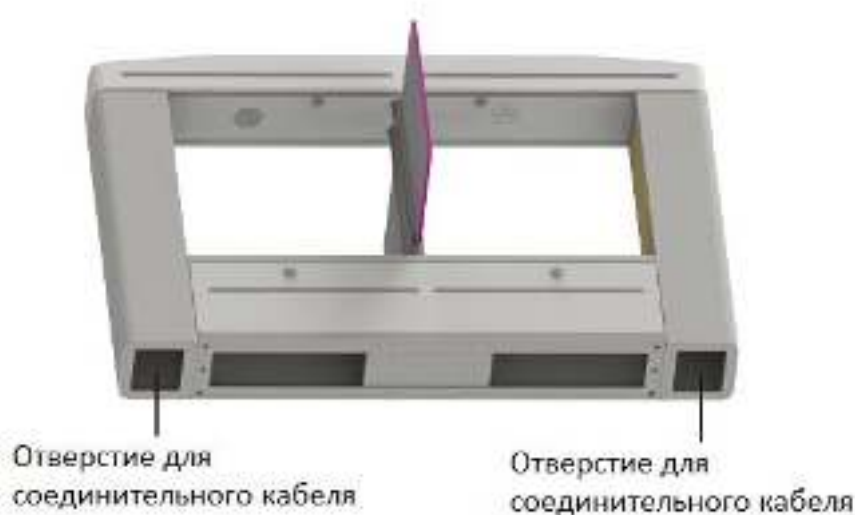


3.3 Подключение соединительного кабеля

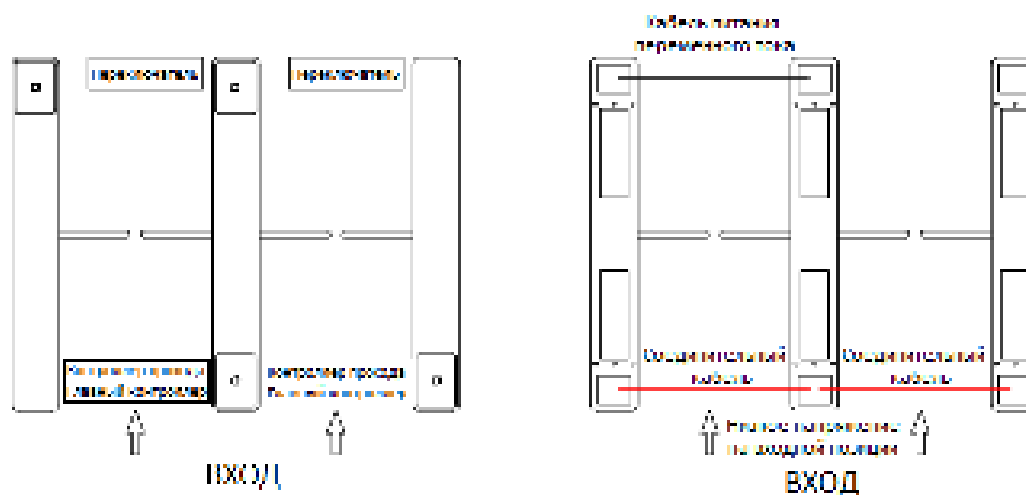
Цель:

Вы должны использовать соединительные кабели, чтобы соединить ведущую плату прохода и подчиненную плату прохода для связи компонентов.

На изображении ниже показано положение отверстий для соединительного кабеля на тумбах турникетов.



Изображение, показанное ниже, описывает схему подключения соединительного кабеля.



Примечания:

- Длина поставляемого соединительного кабеля составляет 3,75 м. Если вам нужен более длинный кабель, обратитесь в нашу службу технической поддержки или в отдел продаж и приобретите 5,5 м соединительные кабели.
- Внутренние диаметры кабелепровода низкого напряжения и кабелепровода высокого напряжения должны быть больше 30 мм. Если на левой тумбе установлено периферийное устройство большой мощности (для аутентификации) (в соответствии с изображением, показанным выше), следует увеличить внутренний диаметр

кабелепровода высокого напряжения.

- Общий способ прокладки: Проложите один сетевой кабель и один кабель питания переменного тока для правой тумбы и проложите один сетевой кабель и один кабель питания переменного тока для центральной тумбы перед установкой. Если нет кабеля питания переменного тока проложенного независимо, то вы должны проложить кабель питания переменного тока между правой и центральной тумбами.
- Если вы хотите проложить кабель питания переменного тока и низковольтный кабель на стороне входа, то оба кабеля должны находиться в отдельных кабелепроводах, чтобы избежать помех.
- Если все соединительные кабели подключены к периферийным устройствам, и требуется подключить больше периферийных устройств, следует увеличить диаметр кабелепровода или проложить другой кабелепровод для внешнего кабеля.
- Внешний кабель питания переменного тока должен быть с двойной изоляцией.

3.4 Описание клемм

Цель:

Контроллер прохода содержит ведущий контроллер прохода и подчиненный контроллер прохода, который контролирует работу ИК-лучей, двигателя и других компонентов.

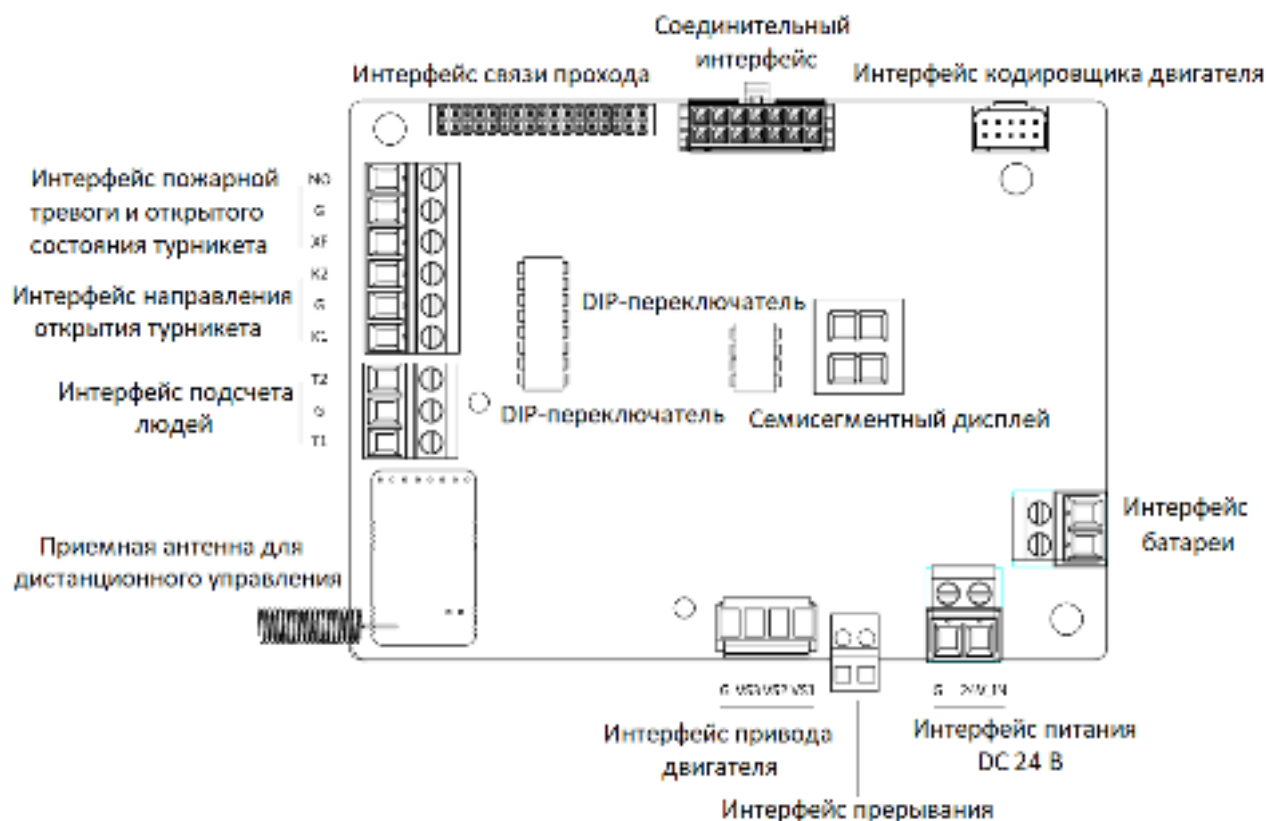
3.4.1 Описание клемм ведущей платы управления проходом

Цель:

Ведущая плата управления проходом содержит интерфейсы связи прохода, соединительный интерфейс, интерфейс кодировщика двигателя, интерфейс пожарной тревоги и открытого состояния турникета, интерфейс направления открытия турникета, интерфейс подсчета людей, приемную антенну для дистанционного управления, интерфейс привода двигателя, интерфейс прерывания, интерфейс питания, интерфейс батареи, DIP-переключатели и семисегментный дисплей (SSD).

Примечание: Для получения подробной информации о значениях DIP-переключателей и их назначении смотрите *Приложение В Описание Описание DIP-переключателей*.

Изображение, показанное ниже, является схемой ведущей платы управления проходом.

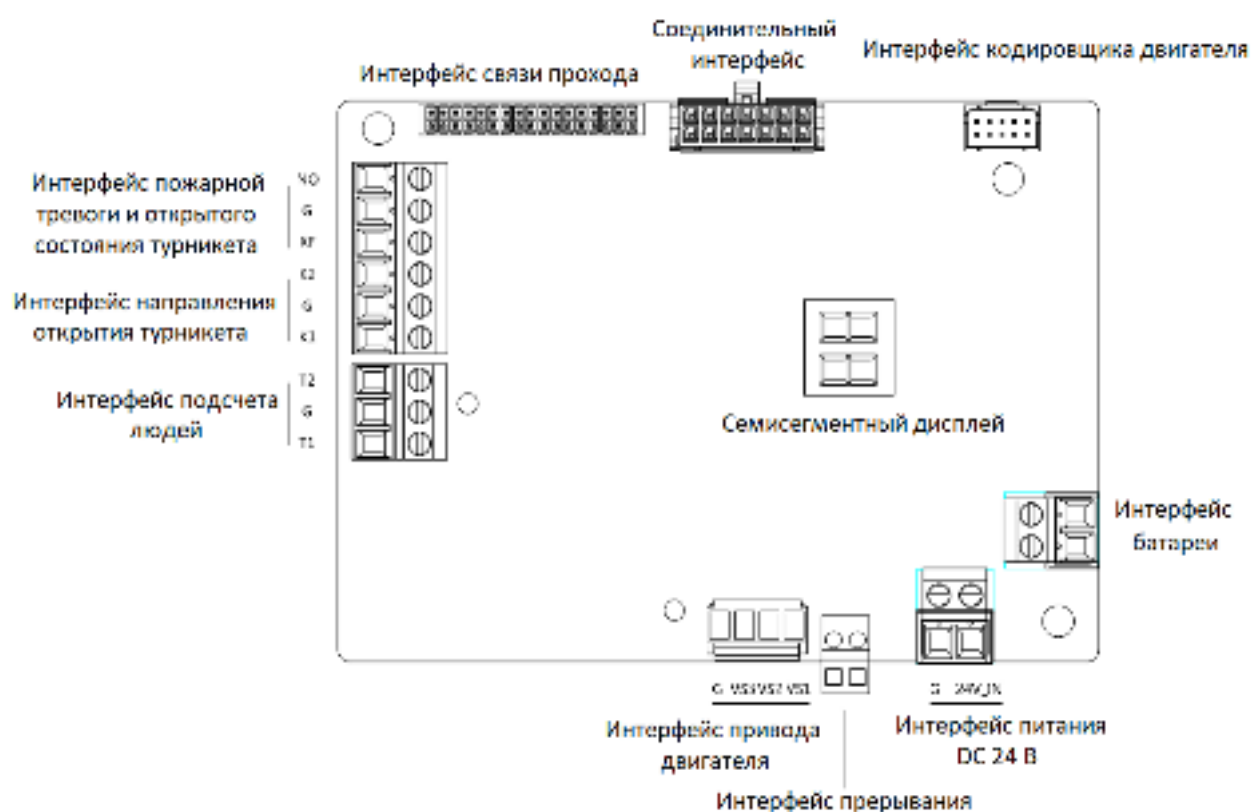


3.4.2 Описание клемм подчиненной платы управления проходом

Цель:

Подчиненная плата управления проходом содержит интерфейсы связи прохода, соединительный интерфейс, интерфейс кодировщика двигателя, интерфейс пожарной тревоги и открытого состояния турникета, интерфейс направления открытия турникета, интерфейс подсчета людей, интерфейс привода двигателя, интерфейс прерывания, интерфейс питания, интерфейс батареи и семисегментный дисплей.

Изображение, показанное ниже, является схемой подчиненной платы управления проходом.



3.4.3 Описание клемм основной платы управления

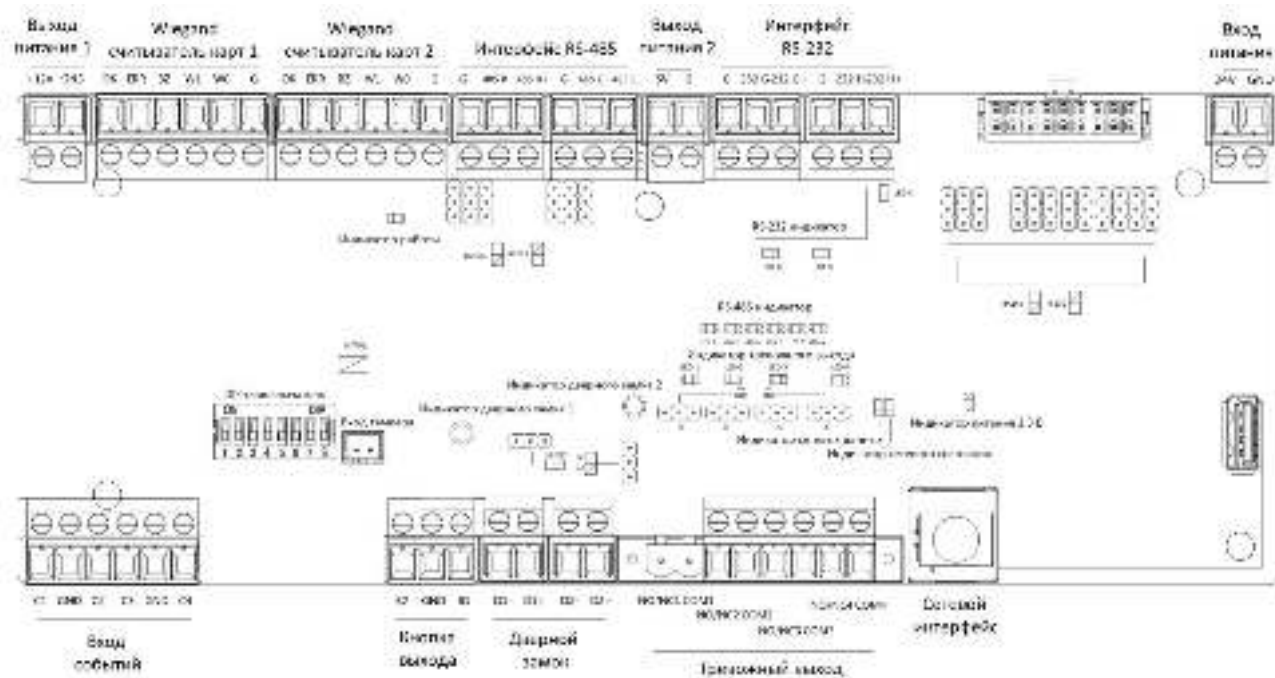


Таблица 3-1 Описание клемм основной платы управления

Описание клемм основной платы управления		
Выход питания 1	+12V	Заземление
	GND	Выход питания
Wiegand считыватель карт 1	OK	Индикатор управляющего выхода считывателя карт (Выход недействительной карты)
	ERR	Индикатор управляющего выхода считывателя карт (Выход действительной карты)
	BZ	Выход управления зуммером считывателя карт
	W1	Интерфейс подключения Wiegand Data1
	W0	Интерфейс подключения Wiegand Data0
	GND	Заземление
Wiegand считыватель карт 2	OK	Индикатор управляющего выхода считывателя карт (Выход недействительной карты)
	ERR	Индикатор управляющего выхода считывателя карт (Выход действительной карты)
	BZ	Выход управления зуммером считывателя карт
	W1	Интерфейс подключения Wiegand Data1
	W0	Интерфейс подключения Wiegand Data0
	GND	Заземление
Интерфейс RS-485	GND	Заземление
	RS-485 B-	Подключение к считывателю карт RS485-
	RS-485 B+	Подключение к считывателю карт RS485+
	GND	Заземление
	RS-485 C-	Подключение к считывателю карт RS485-
	RS-485 C+	Подключение к считывателю карт RS485+
Выход питания 2	5V	Выход питания DC 5 В
	GND	Заземление DC 5 В
Интерфейс RS-232	GND	Заземление
	RS-232 G-	Подключение к считывателю карт RS232-
	RS-232 G+	Подключение к считывателю карт RS232+
	GND	Заземление
	RS-232 H-	Подключение к считывателю карт RS232-
	RS-232 H+	Подключение к считывателю карт RS232+
Вход питания	+12V	Вход питания DC 12 В
	GND	Заземление DC 12 В
Вход событий	C1	Тревожный вход событий 4
	GND	Заземление
	C2	Тревожный вход событий 3
	C3	Тревожный вход событий 2

Описание клемм основной платы управления		
	GND	Заземление
	C4	Тревожный вход событий 1
Кнопка выхода	B2	Дверь 2 Сигнальный вход
	GND	Заземление
	B1	Дверь 1 Сигнальный вход
Дверной замок (Реле)	D1-	Дверь 1 Релейный выход (сухой контакт)
	D1+	
	D2-	Дверь 2 Релейный выход (сухой контакт)
	D2+	
Тревожный выход	NO/NC1	Реле тревожного выхода 1 (сухой контакт)
	COM1	
	NO/NC2	Реле тревожного выхода 2 (сухой контакт)
	COM2	
	NO/NC3	Реле тревожного выхода 3 (сухой контакт)
	COM3	
	NO/NC4	Реле тревожного выхода 4 (сухой контакт)
	COM4	
Сетевой интерфейс	LAN	Сетевой доступ

Примечания:

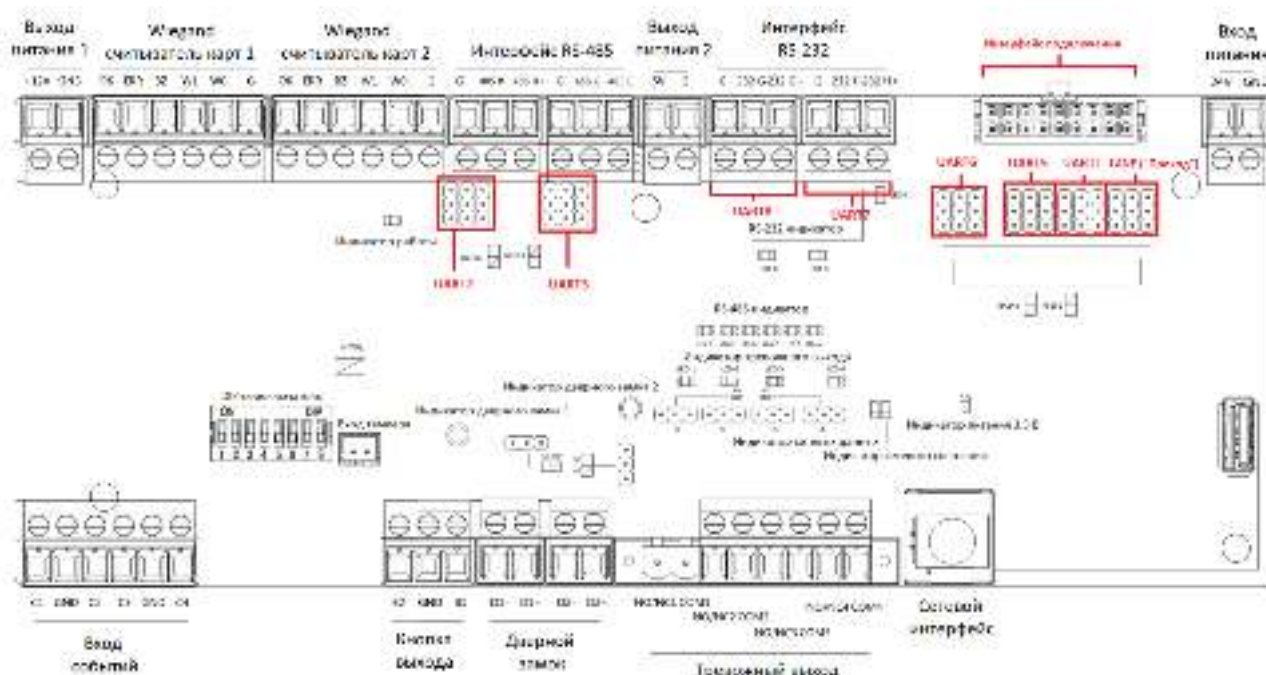
- Аппаратный интерфейс тревожного входа обычно открыт по умолчанию. Поэтому допускается только нормально открытый сигнал. Он может быть связан с зуммером считывателя карт и контроллером доступа, релейным выходом тревоги и релейным выходом открытой двери.
- На DIP-переключателе RS485 считывателя ID карт по умолчанию установлено значение «1» или «4». «1» - для входа, «4» - для выхода. Установите на DIP-переключателе «3» для подключения считывателя карт посетителей.
- Wiegand считыватели карт 1 и 2 соответственно относятся к считывателям карт для входа и выхода.
- Тревожный выход поддерживает доступ к сетевой камере.
- При необходимости дверной замок может контролировать состояние стороннего турникета. D1 управляет открытием турникета для входа, а D2 управляет открытием турникета для выхода. Для получения подробной информации смотрите *Раздел 4.5.1 Режим вывода реле управления турникетом*.
- C3 и C4 во входе событий могут также быть интерфейсами подсчета людей. C3 контролирует подсчет людей на входе, а C4 контролирует подсчет людей на выходе. Когда главная плата управления обнаруживает сигналы на C3 и C4, количество людей будет увеличиваться. Для получения подробной информации о подсчете людей и их количестве

смотрите пункт *Конфигурация параметров подсчета людей* в Разделе **Ошибка!**
Источник ссылки не найден. Удаленная конфигурация.

3.4.4 Описание ID последовательного порта основной платы управления

Цель:

Вы можете использовать колпачковую перемычку на основной плате управления для переключения режима интерфейса связи. Для получения подробной информации о переключении между RS-232 и RS-485 смотрите *Раздел 4.4 Переключение режимов RS-485/RS-232*.



Согласно изображению выше, последовательный порт RS-485 соответствует UART2 и UART3. Последовательный порт RS-232 соответствует UART7 и UART8. Интерфейс подключения соответствует UART1, UART4, UART5, UART6 и Lane («Проход»).

Описание основной панели управления представлено ниже:

Колпачковая перемычка UART2/UART3:

Зарезервированный последовательный порт. Используйте колпачковую перемычку для переключения режима связи последовательного порта. Вы можете переключаться между режимом связи RS-485 и режимом связи RS-232. По умолчанию выбран режим связи RS-485.

Колпачковая перемычка UART6:

Используйте колпачковую перемычку для переключения режима связи последовательного порта с подчиненным контроллером прохода. Вы можете переключаться между режимом связи RS-485 и режимом связи RS-232. По умолчанию выбран режим связи RS-232.

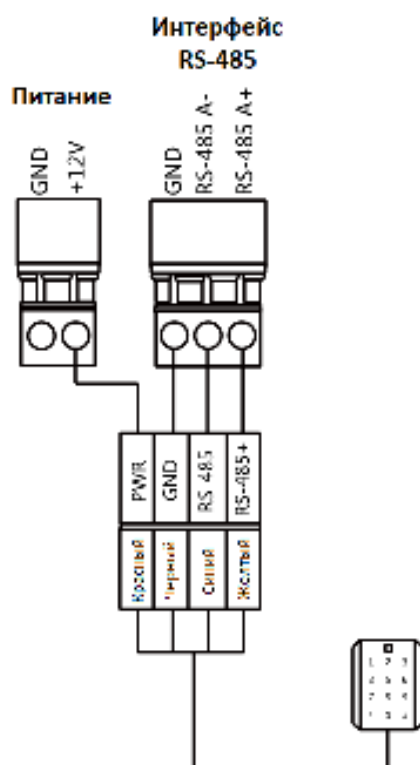
Колпачковая перемычка UART5:	Используйте колпачковую перемычку для переключения режима связи последовательного порта с подчиненным контроллером прохода. Вы можете переключаться между режимом связи RS-485 и режимом связи RS-232. По умолчанию выбран режим связи RS-485.
Колпачковая перемычка UART1:	Используйте колпачковую перемычку для переключения режима связи последовательного порта с ведущим контроллером прохода. Вы можете переключаться между режимом связи RS-485 и режимом связи RS-232. По умолчанию выбран режим связи RS-485.
Lane («Проход»):	Используйте колпачковую перемычку для переключения режима связи последовательного порта с контроллером прохода. По умолчанию интерфейс является проводным и находится в режиме связи RS-485. При подключении других контроллеров (совместимых с протоколом связи Hikvision) используйте колпачковую перемычку для переключения между режимами связи RS-485 и RS-232.
UART4:	Последовательный порт находится в интерфейсе подключения в соответствии с рисунком выше, который имеет фиксированный режим связи RS-232 для связи с ведущим контроллером прохода. Он не содержит колпачковых перемычек и не может изменить режим связи.
UART7/UART8:	Зарезервированный последовательный порт. Последовательный порт имеет фиксированный режим связи RS-232. Он не содержит колпачковых перемычек и не может изменить режим связи. К нему можно подключить сканер QR-кода, устройство переработки карт и текстовый экран.

3.4.5 Подключение по RS-485

Примечания:

- Имеется пять интерфейсов RS-485, которые предназначены для подключения считывателя ID-карт, считывателя IC-карт, сканера QR-кода, считывателя отпечатков пальцев и карт, устройства переработки карт, текстового экрана, считывателя отпечатков пальцев и терминала распознавания лиц. Возьмем в качестве примера подключение считывателя карт по RS-485.

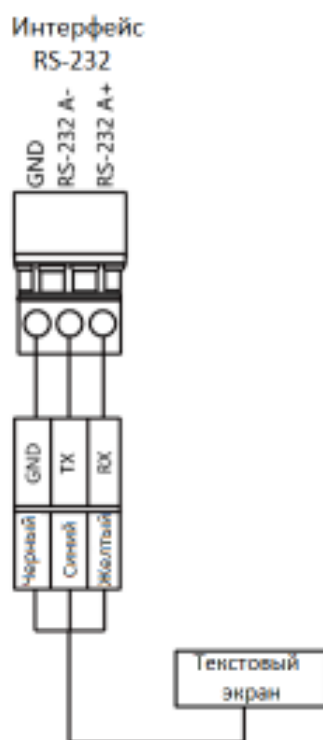
- Для получения подробной информации о текстовом экране смотрите пункт *Конфигурация параметров экрана* в Разделе **Ошибка! Источник ссылки не найден.** Удаленная конфигурация.



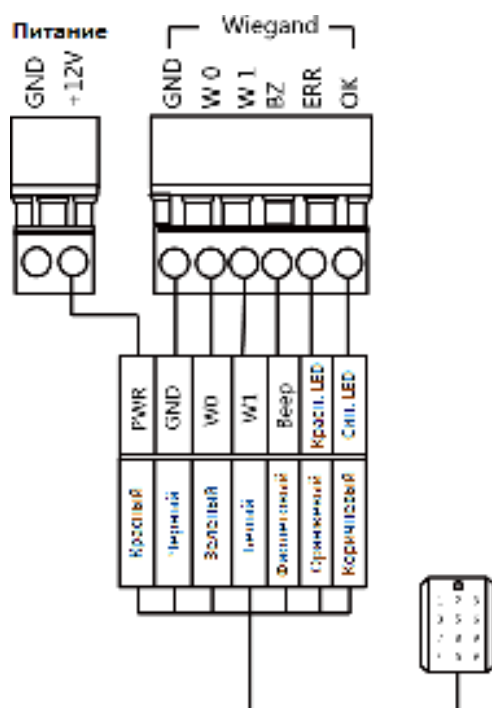
3.4.6 Подключение по RS-232

Примечание: Имеется три RS-232 интерфейса (UART4, UART7 и UART8). К UART7 и UART8 можно подключать сканер QR-кодов, устройство переработки карт и текстовый экран, в то время как к UART4 можно подключать сканер QR-кодов, устройство переработки карт, текстовый экран и терминал распознавания лиц. Для получения подробной информации о текстовом экране смотрите пункт *Конфигурация параметров экрана* в Разделе **Ошибка! Источник ссылки не найден.** Удаленная конфигурация.

Возьмем в качестве примера подключение текстового экрана.



3.4.7 Подключение по Wiegand

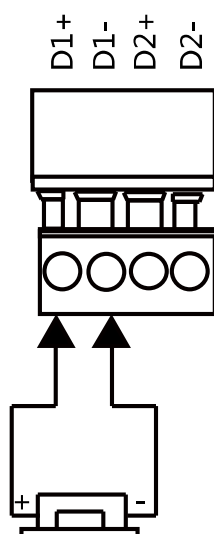
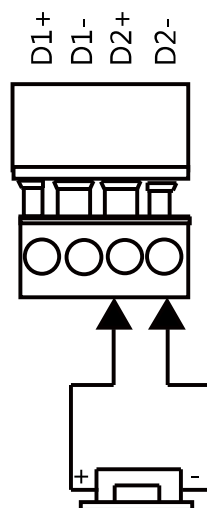


Примечание: Вы должны подключить клеммы OK/ERR/BZ, если используете контроллер доступа для управления светодиодом и зуммером Wiegand считывателя карт.

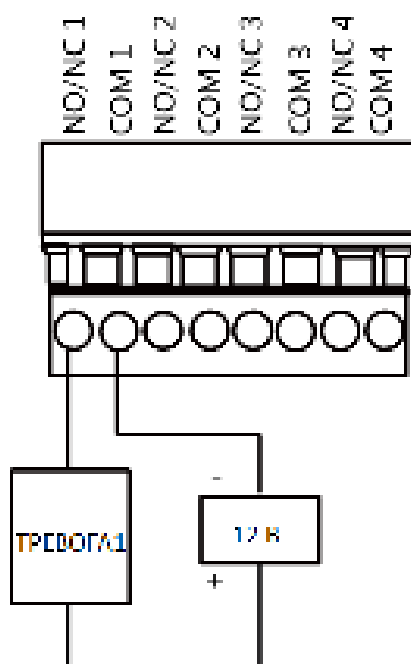
3.4.8 Подключение платы управления турникетом

Цель:

По умолчанию турникет связан с основной платой управления. Плата управления проходом может контролировать состояние турникета. Если необходимо, устройство может соединяться со сторонней платой управления проходом для управления сторонними турникетами. Интерфейс D1 управляет открытием турникета для входа, а интерфейс D2 управляет открытием турникета для выхода.

Подключение входа**Подключение выхода**

3.4.9 Подключение тревожного выхода



Примечание: Для получения подробной информации об изменении состояния релейного выхода через колпачковую перемычку смотрите *Раздел 4.5.2 Режим вывода реле тревоги (НО/НЗ)*.

3.5 Подключение литиевой батареи (Опционально)

Цель:

Литиевая батарея обеспечивает питание для ведущей платы управления проходом и подчиненной платы управления проходом, когда устройство выключено.

Перед началом:

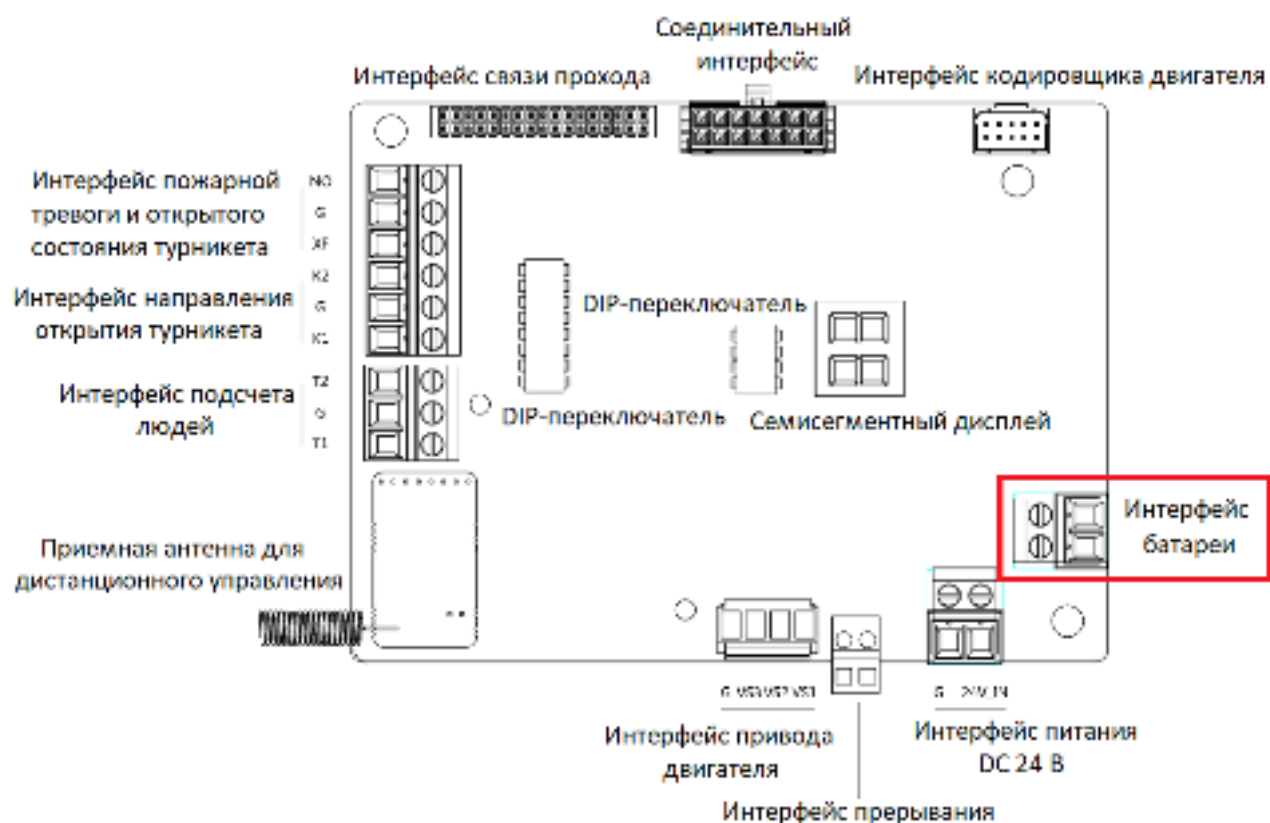
Обратитесь к нашим специалистам технической поддержки или в отдел продаж для приобретения литиевой батареи.

Шаги:

1. Установите литиевую батарею.
 - 1) Удалите винты на составном элементе батареи, чтобы разобрать его.
 - 2) Поместите литиевую батарею внутрь составного элемента.
 - 3) Закрепите составные элементы на устройстве с помощью винтов.
2. Вставьте разъем батареи в интерфейс батареи на плате управления проходом.

Примечание: Батарейные интерфейсы есть на ведущей плате управления и на подчиненной плате управления проходом.

Положение интерфейса батареи представлено на рисунке ниже:



Глава 4 Настройки устройства

После завершения монтажа и подключения необходимо установить закрытое положение турникетов (режим обучения) перед переходом в рабочий режим.

Вы также можете установить режим прохода и режим памяти, выполнить сопряжение пульта ДУ, инициализировать аппаратное обеспечение, переключиться между режимом связи RS-485 и режимом связи RS-232, а также просмотреть схему НО/НЗ (NO/NC) релейного выхода, установив DIP-переключатели.

- **Study Mode** («Режим обучения»): Турникет выучит закрытое положение.
- **Normal Mode** («Нормальный режим»): Устройство будет работать должным образом. Положение турникета, сконфигурированное в режиме обучения, является закрытой позицией, когда устройство работает нормально.
- **Passing Mode** («Режим прохода»): Есть 9 режимов прохода, включая контролируемое двунаправленное движение, контролируемый вход и запрещенный выход, контролируемый вход и свободный выход, свободное двунаправленное движение, свободный вход и контролируемый выход, свободный вход и запрещенный выход, запрещенное двунаправленное движение, запрещенный вход и свободный выход.
- **Memory Mode** («Режим памяти»): По умолчанию режим памяти включен. Когда выполняется проводка нескольких карт и их успешная аутентификация, нескольким людям разрешается пройти через турникет. Когда турникет подсчитывает, что количество прошедших людей равно числу проводок карт, или если никто не проходит через турникет после последнего прошедшего человека, тогда турникет закрывается.

Примечание: Вы также можете установить DIP-переключатель для управления действием проводки карты для открытия турникета в зоне тревоги, для выбора типа управления входом и выходом, для сопряжения с пультом дистанционного управления и т. д. Для получения подробной информации о значениях DIP-переключателей и их назначении смотрите Приложение В Описание Описание DIP-переключателей.

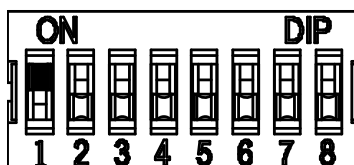
4.1 Установка закрытого положения

Цель:

Войдите в режим обучения с помощью DIP-переключателей, чтобы установить закрытое положение турникета.

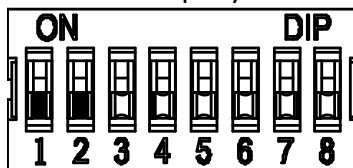
Шаги:

1. Установите переключатели №1 и №2 8-значного DIP-переключателя на ведущей плате управления проходом так, как показано на рисунке ниже, для перехода в режим обучения.



2. Отрегулируйте закрытое положение турникета.
3. Включите устройство.
Устройство запомнит текущую позицию (закрытую позицию) автоматически.

4. Выключите устройство.
5. Установите переключатели №1 и №2 8-значного DIP-переключателя на ведущей плате управления проходом так, как показано на рисунке ниже.



6. Снова включите устройство.
Турникет откроется автоматически и вернется в закрытое положение. В этих обстоятельствах устройство переходит в обычный режим.

Примечание: Для получения подробной информации о значениях DIP-переключателей и их назначении смотрите *Приложение В Описание Описание DIP-переключателей*.

4.2 Сопряжение пульта дистанционного управления (Опционально)

Цель:

Выполните сопряжение пульта дистанционного управления с устройством с помощью DIP-переключателей для дистанционного открытия/закрытия турникета.

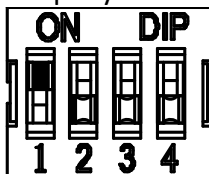
Примечание: Подробности о работе пульта дистанционного управления смотрите в соответствующем руководстве пользователя.

Перед началом:

Обратитесь к нашим специалистам технической поддержки или в отдел продаж для приобретения пульта ДУ.

Шаги:

1. Выключите распашной турникет.
2. Установите переключатель №1 4-значного DIP-переключателя на ведущей плате управления проходом в соответствии с рисунком ниже.



3. Включите распашной турникет, и он войдет в режим сопряжения.
4. Удерживайте кнопку **Close** («Закрыть») более 10 секунд.
Индикатор пульта дистанционного управления мигнет дважды, если сопряжение выполнено успешно.
5. Установите DIP-переключатель в положение **OFF** («Выкл.»), а затем перезагрузите турникет для вступления настроек в силу.

Примечания:

- Вы также можете выполнить сопряжение пульта ДУ при помощи клиентского ПО. Для получения подробной информации смотрите пункт *Управление при помощи пульта ДУ* в Разделе **Ошибка! Источник ссылки не найден. Ошибка! Источник ссылки не найден..**

- Только один распашной турникет может быть сопряжен с пультом дистанционного управления. Если в режиме сопряжения находятся несколько распашных турникетов, пульт дистанционного управления выберет только один из них для сопряжения.
- Для получения подробной информации о значениях DIP-переключателей и их назначении смотрите *Приложение В Описание DIP-переключателей*.

4.3 Инициализация устройства

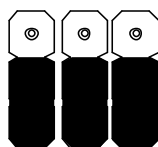
Шаги:

1. Удалите колпачковую перемычку JP11.
2. Отключите питание и перезагрузите устройство. Зуммер устройства издаст длинный гудок.
3. Когда звуковой сигнал прекратится, вставьте колпачковую перемычку обратно.
4. Отключите питание и перезагрузите устройство.

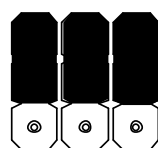
Примечание: Инициализация устройства восстановит все параметры до значений по умолчанию, и все события устройства будут удалены.

4.4 Переключение режимов RS-485/RS-232

В качестве примера возьмем UART2 и UART3 на основной плате управления. Если колпачковая перемычка находится в положении, представленном на рисунке ниже, то последовательный порт находится в режиме связи RS-485. (Черная часть - это колпачковая перемычка)



Если колпачковая перемычка находится в положении, представленном на рисунке ниже, то последовательный порт находится в режиме связи RS-232. (Черная часть - это колпачковая перемычка)



4.5 Переключение режима релейного выхода (НО/НЗ)

4.5.1 Режим вывода реле управления турникетом

Контакты реле управления турникетом на основной плате управления представлены ниже:



Положение колпачковой перемычки открытия турникета для входа (НО) представлено ниже:



Положение колпачковой перемычки открытия турникета для выхода (НО) представлено ниже:



Положение колпачковой перемычки закрытия турникета для входа (НЗ) представлено ниже:

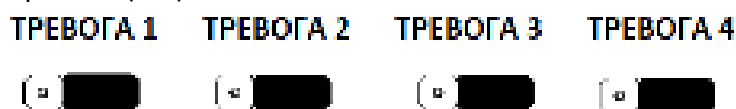


Положение колпачковой перемычки закрытия турникета для выхода (НЗ) представлено ниже:



4.5.2 Режим вывода реле тревоги (НО/НЗ)

Режим вывода реле тревоги (НО):



Режим вывода реле тревоги (НЗ):



Глава 5 Активация устройства

Цель:

Вам необходимо активировать устройство перед его использованием.

Поддерживается активация при помощи ПО SADP и при помощи клиентского ПО.

Значения по умолчанию для терминала управления следующие.

- IP-адрес по умолчанию: 192.0.0.64.
- № порта по умолчанию: 8000.
- Имя пользователя по умолчанию: admin.

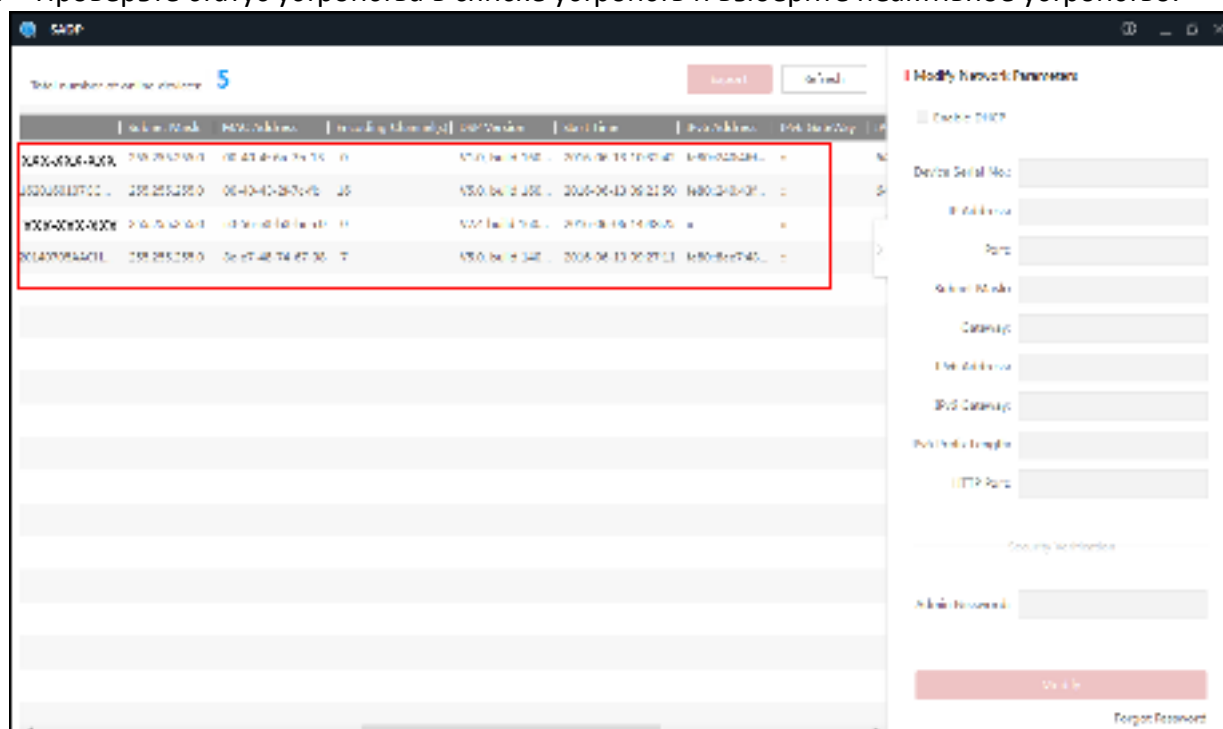
5.1 Активация через ПО SADP

Программное обеспечение SADP используется для обнаружения онлайн-устройств, активации устройств и сброса пароля.

Получите программное обеспечение SADP с прилагаемого диска или официального сайта и установите SADP в соответствии с подсказками. Выполните следующие шаги для активации устройства.

Шаги:

1. Запустите ПО SADP для поиска онлайн-устройств.
2. Проверьте статус устройства в списке устройств и выберите неактивное устройство.



3. Создайте пароль, введите его в поле **Password** («пароль») и подтвердите пароль в поле **Confirm** («подтверждение»).



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 активации устройства.
5. Проверьте активированное устройство. Вы можете изменить IP-адрес устройства так, чтобы он был в той же подсети, к которой подключен Ваш компьютер, вручную или, поставив галочку **Enable DHCP** («Включить DHCP»).

6. Введите пароль и нажмите кнопку **Modify** («Изменить») для сохранения IP-адреса.

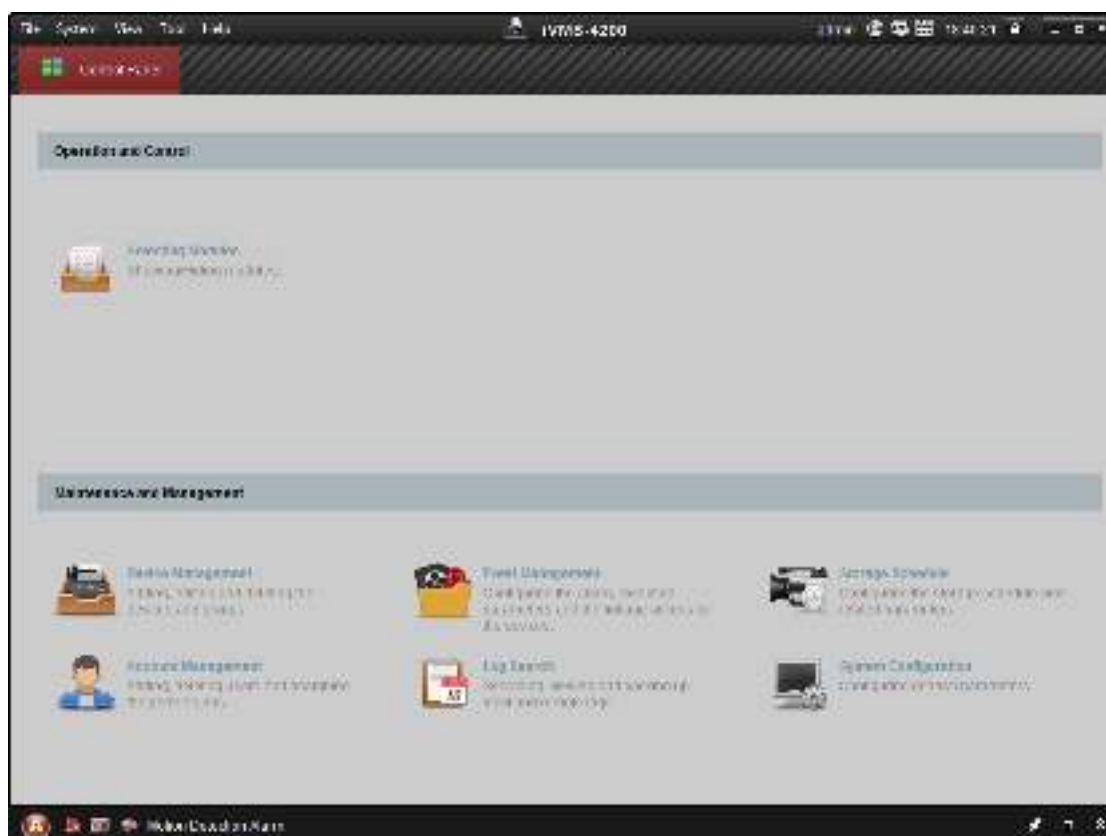
5.2 Активация при помощи клиентского ПО

Клиентское программное обеспечение является универсальным программным обеспечением для управления видеонаблюдением для нескольких видов устройств.

Получите клиентское программное обеспечение с прилагаемого диска или на официальном сайте и установите программное обеспечение в соответствии с подсказками. Выполните следующие действия для активации устройства.

Шаги:

1. Запустите клиентское программное обеспечение, появится панель управления программным обеспечением, как показано на рисунке ниже.



2. Нажмите **Device Management** («Управление устройствами») для перехода в меню управления устройствами.
3. Проверьте статус устройства в списке устройств и выберите неактивное устройство.

IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.	Start Time
192.0.0.64			Active	8000		2017-01
192.168.1.64			Inactive	8000		2017-01

4. Нажмите **Activate** («Активировать») для появления всплывающего окна активации.
5. Во всплывающем окне создайте пароль и введите его в поле **Password** («пароль») и **Confirm** («подтверждение»).



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.



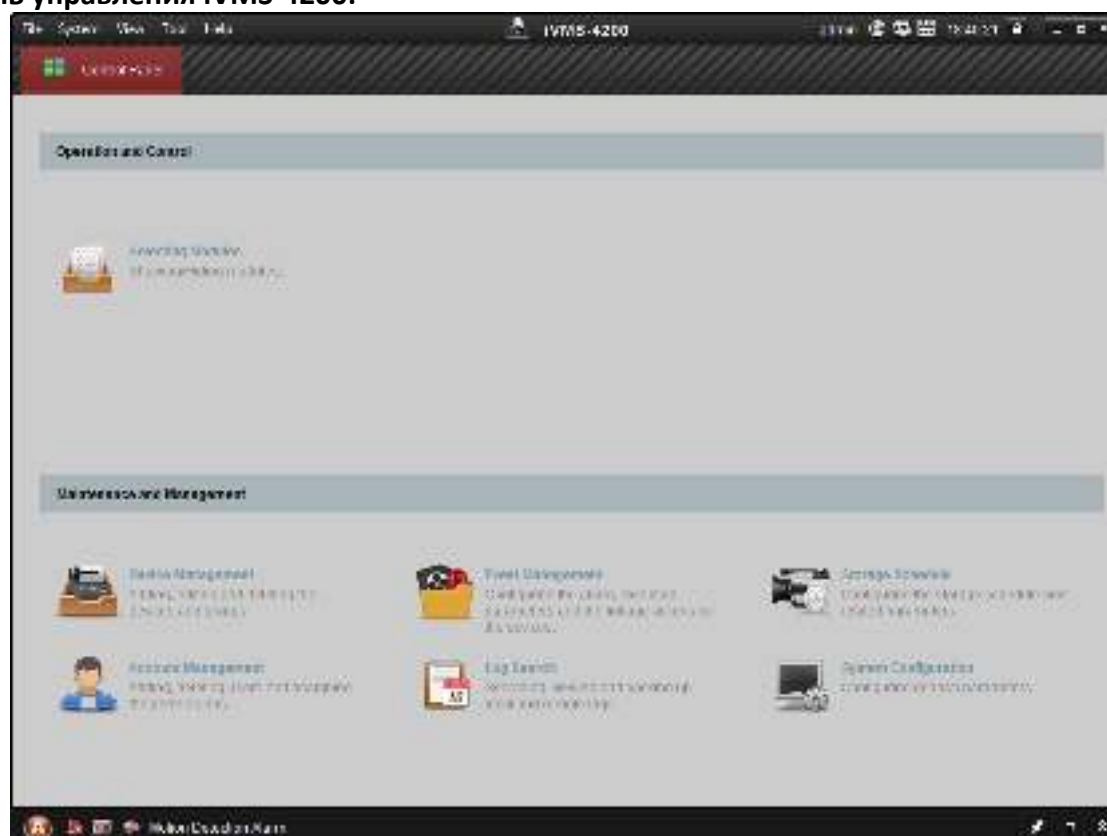
6. Нажмите кнопку **OK** для начала активации.
7. Нажмите кнопку **Modify Netinfo** («Изменить сетевую информацию») для появления всплывающего окна изменения сетевых параметров.
8. Измените вручную IP-адрес устройства так, чтобы он был в той же подсети, к которой подключен Ваш компьютер.
9. Введите пароль и нажмите **OK** для сохранения настроек.

Глава 6 Операции в клиентском ПО

Вы можете настраивать и управлять устройствами контроля доступа через клиентское программное обеспечение. В этой главе будут представлены операции, связанные с управлением доступом в клиентском программном обеспечении. Для получения подробной информации смотрите *Руководство пользователя Клиентского ПО iVMS-4200*.

6.1 Функциональный модуль

Панель управления iVMS-4200:



6.2 Регистрация пользователей и вход в систему

Для первого использования клиентского ПО iVMS-4200 вам необходимо зарегистрировать супер пользователя для входа в систему.

Шаги:

1. Введите **Super User Name** («имя супер пользователя») и **Password** («пароль»). Программное обеспечение автоматически оценит надежность пароля, и мы настоятельно рекомендуем использовать надежный пароль для обеспечения безопасности данных.
2. Введите пароль снова в поле **Confirm Password** («Подтверждение пароля»).
3. Опционально, поставьте галочку **Enable Auto-login** («Включить автоматический вход») для входа в систему автоматически.
4. Нажмите **Register** («Зарегистрировать»). Теперь вы можете войти в систему в качестве супер пользователя.



- ◆ Имя пользователя не может содержать любой из следующих символов: / \ : * ? " < > | .
А длина пароля не может быть меньше 6-ти символов.
- ◆ Для вашей безопасности, мы настоятельно рекомендуем изменить пароль на ваш собственный (используя как минимум 8 символов, включая символы верхнего или нижнего регистра, числа и специальные символы) с целью повышения безопасности вашего продукта.
- ◆ Правильная настройка всех паролей и других параметров безопасности является обязанностью установщика и/или конечного пользователя.

Когда ПО iVMS-4200 открыто после регистрации, вы можете войти в клиентское ПО с зарегистрированным именем и паролем.

Шаги:

1. Введите **User Name** («имя пользователя») и **Password** («пароль»), которые вы зарегистрировали.
- Примечание:** Если вы забыли ваш пароль, пожалуйста, нажмите **Forgot Password** («Забыл пароль») и запомните зашифрованную строку во всплывающем окне. Свяжитесь с вашим дилером и отправьте ему зашифрованную строку для сброса пароля.
2. Опционально, поставьте галочку **Enable Auto-login** («Включить авто вход») для автоматического входа в программу.
 3. Нажмите **Login** («Вход»).



После запуска клиентского ПО вы можете открыть программы-помощники (включая видео помощника, помощника настройки видеостены, помощника настройки панели управления безопасностью, помощника контроля доступа и видеодомофонии, помощника настройки посещаемости) для помощи в добавлении устройств и выполнения настройки и различных операций. Для получения подробной информации о помощниках смотрите *Краткое руководство пользователя iVMS-4200*.

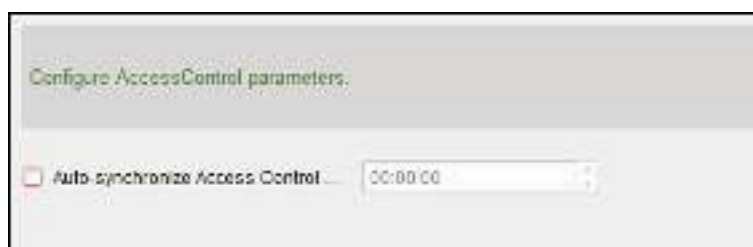
6.3 Конфигурация системы

Цель:

Вы можете синхронизировать пропущенные события контроля доступа с клиентом.

Шаги:

1. Нажмите **Tool – System Configuration** («Инструменты – Конфигурация системы»).
2. В окне конфигурации системы поставьте галочку **Auto-synchronize Access Control Event** («Автоматическая синхронизация событий контроля доступа»).
3. Установите время синхронизации.
Клиент будет автоматически синхронизировать события контроля доступа в заданное время.



6.4 Управление контролем доступа

Цель:

Модуль контроля доступа применим к устройствам контроля доступа и видеодомофонам. Он обеспечивает множество функций, включая управление людьми и карточками, конфигурацию разрешений, управление статусом контроля доступа, видеодомофонию и другие расширенные функции.

Вы также можете настроить конфигурацию событий для контроля доступа и отображение точек и зон контроля доступа на Е-карте.

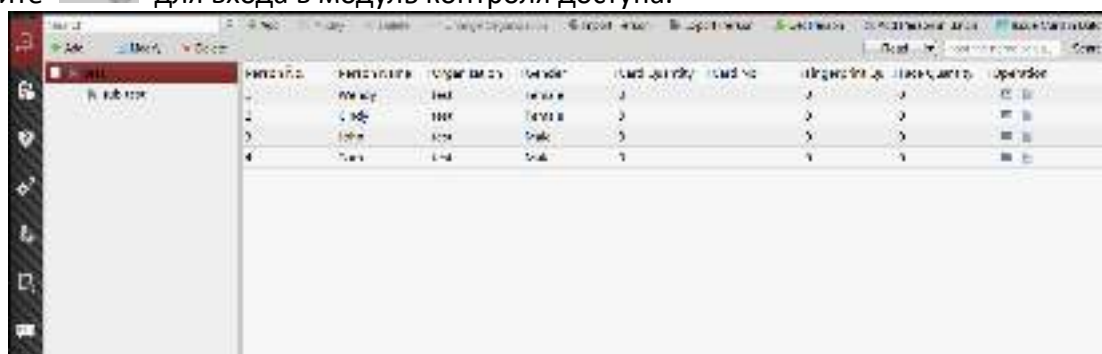
Примечание: Пользователь с разрешениями модуля контроля доступа может войти в модуль контроля доступа и настроить параметры управления доступом.



Нажмите  на панели управления и отметьте **Access Control** («Контроль доступа») для добавления модуля контроля доступа на панель управления.



Нажмите  для входа в модуль контроля доступа.



Перед началом:

При первом открытии модуля контроля доступа появится следующее диалоговое окно, и вы

должны выбрать сцену в соответствии с фактическими потребностями.

Non-residence («Нежилой комплекс»): Вы можете установить правило посещаемости при добавлении человека, задав параметры контроля доступа.

Residence («Жилой комплекс»): Вы не можете установить правило посещаемости при добавлении человека.



Примечание: После того как сцена настроена, вы не сможете изменить ее позже.

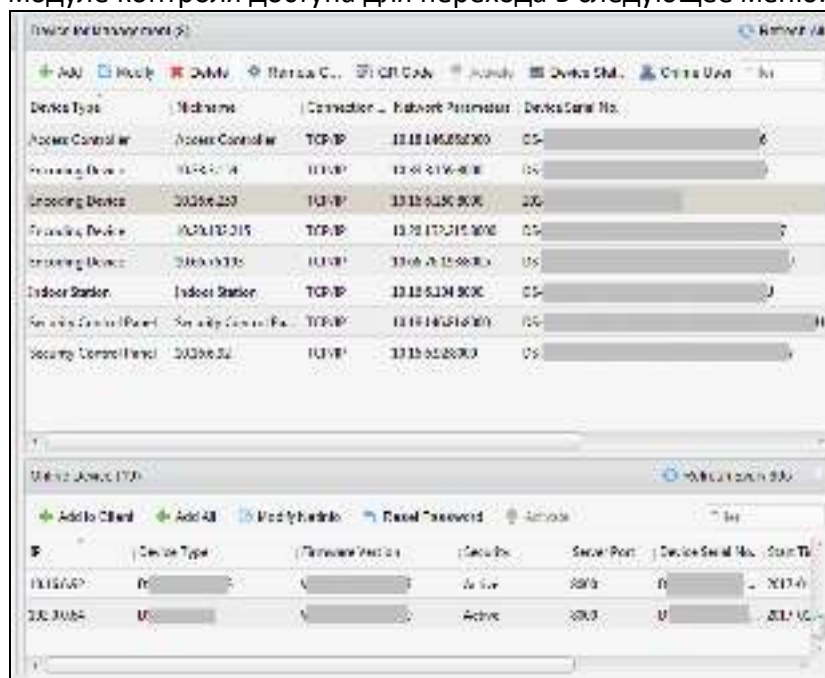
Модуль контроля доступа состоит из следующих подмодулей

	Person and Card («Люди и карты»)	Управление организациями, людьми и присвоение карточек людям.
	Schedule and Template («Расписание и шаблоны»)	Настройка недельного расписания, группы выходных и настройка шаблона.
	Permission («Разрешения»)	Назначение разрешений контроля доступа людям и применение к устройствам.
	Advanced Function («Расширенные функции»)	Предоставление расширенных функций, включая настройку параметров контроля доступа, аутентификацию считывателя карт, открытие двери при помощи первой карты, защиту от обратного прохода, блокировку нескольких дверей и пароль аутентификации.
	Video Intercom («Видеодомофония»)	Видеодомофония между клиентом и жильцом, поиск в журнале набора номеров и выдача уведомлений.
	Search («Поиск»)	Поиск в истории событий контроля доступа; Поиск по журналу вызовов, журналу разблокировки дверей и выдача уведомлений.
	Device Management («Управление устройством»)	Управление устройствами контроля доступа и видеодомофонами.

Примечание: В этой главе мы представим только операции контроля доступа.

6.4.1 Добавление устройства контроля доступа

Нажмите  в модуле контроля доступа для перехода в следующее меню.



Примечание: После добавления устройства вы должны проверить статус постановки устройства на охрану в меню **Tool – Device Arming Control** («Инструменты – Контроль постановки устройств на охрану»). Если устройство не поставлено на охрану, вы должны поставить его на охрану, иначе оно не будет получать события в реальном времени при помощи клиентского ПО. Для получения подробной информации о постановке устройств на охрану смотрите *Раздел **Ошибка! Источник ссылки не найден.** Управление охраной.*

Создание пароля

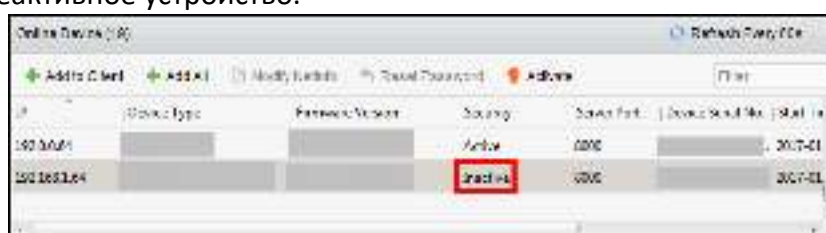
Цель:

Для некоторых устройств вам необходимо создать пароль для их активации, перед тем как они смогут быть добавлены в ПО и смогут работать должным образом.

Примечание: Эта функция должна поддерживаться устройством.

Шаги:

1. Войдите на страницу **Device Management** («Управление устройствами»).
2. В области **Device for Management** («Устройства для управления») или **Online Device** («Онлайн устройства») проверьте статус устройств (в столбце **Security** («Безопасность»)) и выберите неактивное устройство.



3. Нажмите кнопку **Activate** («Активировать») для появления всплывающего меню активации.
4. Создайте пароль в поле **Password** («пароль») и подтвердите его в поле **Confirm** («подтверждение»).



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.



5. (Опционально) Включите службу Hik-Connect при активации устройства, если оно поддерживает данную службу.
 - 1) Поставьте галочку **Enable Hik-Connect** («Включить Hik-Connect») для появления следующего всплывающего окна.

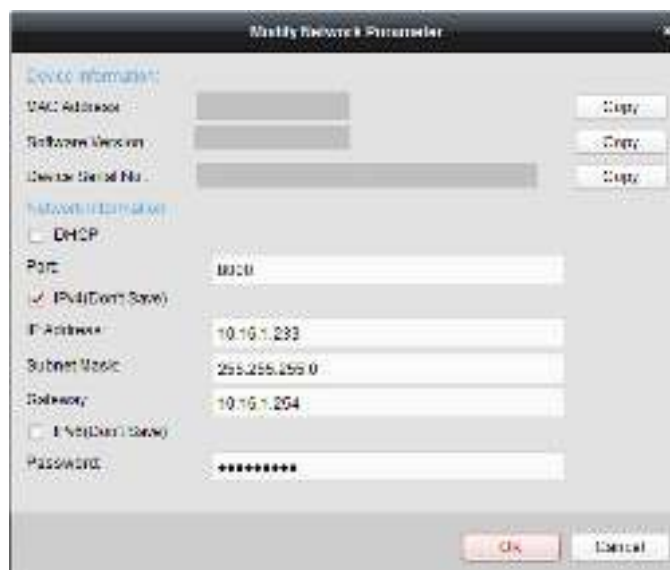


- 2) Создайте **Verification Code** («проверочный код»).
 - 3) Подтвердите проверочный код в поле **Confirm Verification Code** («Подтверждение проверочного кода»).
 - 4) Нажмите **Terms of Service** («Условия предоставления услуг») и **Privacy Policy** («Политика конфиденциальности») для ознакомления с соответствующими документами.
 - 5) Нажмите **OK** для включения службы Hik-Connect.
 6. Нажмите **OK** для активации устройства.
- При успешной установке пароля появится надпись **“The device is activated.”** («Устройство активировано»).

- Нажмите кнопку **Modify Netinfo** («Изменить сетевую информацию») для появления всплывающего окна изменения сетевых параметров.

Примечание: Эта функция доступна только в области **Online Device** («Онлайн устройства»). Вы можете изменить IP-адрес устройства на адрес в той же подсети, что и ваш компьютер, если вам необходимо добавить устройство к программе.

- Измените IP-адрес устройства на адрес в той же подсети, что и ваш компьютер, вручную или поставив галочку напротив **DHCP**.
- Введите пароль, установленный в шаге 4, и нажмите **OK** для завершения сетевых настроек.

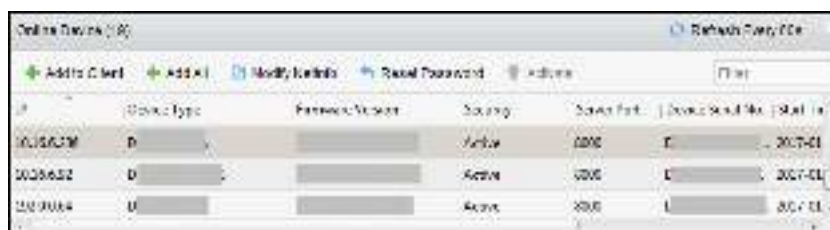


Добавление онлайн устройств

Цель:

Активные онлайн устройства в той же локальной подсети, что и клиентское ПО будут отображаться в области **Online Device** («Онлайн устройства»). Вы можете нажать кнопку **Refresh Every 60s** («Обновлять каждые 60 сек») для обновления информации в области **Online Device** («Онлайн устройства»).

Примечание: Вы можете нажать , чтобы скрыть область **Online Device** («Онлайн устройства»).



Шаги:

- Выберите устройства, которые вы хотите добавить из списка.

Примечание: Для неактивных устройств, вам необходимо создать пароль для них, перед тем как вы сможете добавить устройство.

- Нажмите **Add to Client** («Добавить к клиенту») для открытия диалогового окна добавления устройств.

3. Введите необходимую информацию.

Nickname («Псевдоним»): Измените название устройства по вашему желанию.

Address («Адрес»): Введите IP-адрес устройства. IP-адреса устройств получаются автоматически в данном режиме добавления.

Port («Порт»): Введите № порта устройства. Значение по умолчанию 8000.

User Name («Имя пользователя»): Введите имя пользователя устройства. По умолчанию имя пользователя - *admin*.

Password («Пароль»): Введите пароль устройства.



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. Опционально, вы можете поставить галочку **Export to Group** («Экспортировать в группу») для создания группы соответствующей имени устройства.

Все каналы устройства будут импортированы в соответствующую группу по умолчанию.

Примечание: iVMS-4200 так же предоставляет метод добавления офлайн устройств.

1) Поставьте галочку **Add Offline Device** («Добавить офлайн устройство»).

2) Введите необходимую информацию, включая количество каналов устройства и количество тревожных входов.

3) Нажмите **Add** («Добавить»).

Когда устройство из офлайн режима перейдет в онлайн режим, программа подключится к нему автоматически.

5. Нажмите **Add** («Добавить») для добавления устройства.

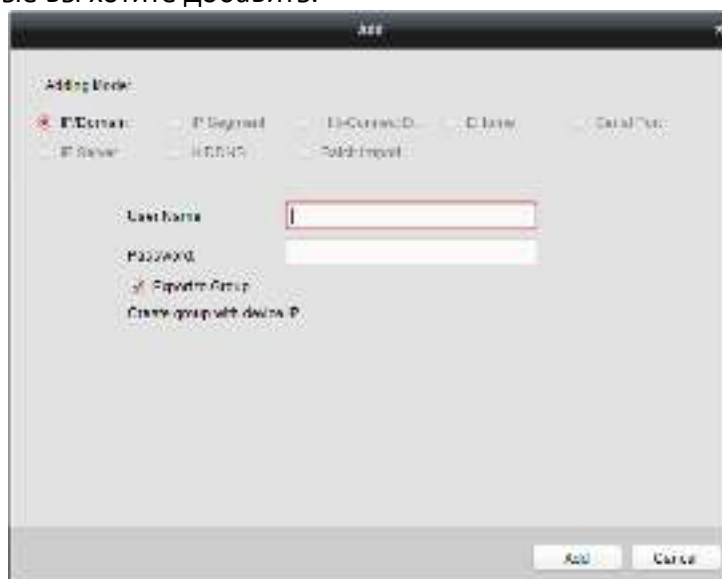
➤ **Добавление нескольких онлайн устройств**

Если вы хотите добавить несколько онлайн устройств в клиентское ПО, нажмите и

удерживайте клавишу *Ctrl* для выбора нескольких устройств, и нажмите **Add to Client** («Добавить к клиенту») для открытия диалогового окна добавления устройств. Во всплывающем окне введите имя пользователя и пароль устройств, которые вы хотите добавить.

➤ Добавление всех онлайн устройств

Если вы хотите добавить все онлайн устройства в ПО, нажмите **Add All** («Добавить все»), а затем нажмите **OK** во всплывающем окне. Затем введите имя пользователя и пароль устройств, которые вы хотите добавить.



Добавление устройств по IP или доменному имени

Шаги:

1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.
2. Выберите **IP/Domain** («IP/Домен») в поле **Adding Mode** («режим добавления»).
3. Введите необходимую информацию.

Nickname («Имя устройства»): Измените имя устройства по вашему желанию.

Address («Адрес»): Введите IP-адрес устройства или доменное имя устройства.

Port («Порт»): Введите № порта устройства. Значение по умолчанию - 8000.

User Name («Имя пользователя»): Введите имя пользователя устройства. По умолчанию имя пользователя - *admin*.

Password («Пароль»): Введите пароль устройства.



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. Опционально, вы можете поставить галочку **Export to Group** («Экспортировать в группу») для создания группы соответствующей имени устройства.

Все каналы устройства будут импортированы в соответствующую группу по умолчанию.

Примечание: iVMS-4200 так же предоставляет метод добавления офлайн устройств.

- 1) Поставьте галочку **Add Offline Device** («Добавить офлайн устройство»).
- 2) Введите необходимую информацию, включая количество каналов устройства и количество тревожных входов.
- 3) Нажмите **Add** («Добавить»).

Когда устройство из офлайн режима перейдет в онлайн режим, программа подключится к нему автоматически.

5. Нажмите **Add** («Добавить») для добавления устройства.

Добавление устройств по IP сегменту

Шаги:

1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.
2. Выберите **IP Segment** («IP сегмент») в поле **Adding Mode** («режим добавления»).
3. Введите необходимую информацию.

Start IP («Начальный IP»): Введите начальный IP-адрес.

End IP («Конечный IP»): Введите конечный IP-адрес из того же сегмента сети, что и начальный IP-адрес.

Port («Порт»): Введите № порта устройства. Значение по умолчанию - 8000.

User Name («Имя пользователя»): Введите имя пользователя устройства. По умолчанию имя пользователя - *admin*.

Password («Пароль»): Введите пароль устройства.



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.

- Опционально, вы можете поставить галочку **Export to Group** («Экспортировать в группу») для создания группы соответствующей имени устройства.

Все каналы устройства будут импортированы в соответствующую группу по умолчанию.

Примечание: iVMS-4200 так же предоставляет метод добавления офлайн устройств.

- Поставьте галочку **Add Offline Device** («Добавить офлайн устройство»).
- Введите необходимую информацию, включая количество каналов устройства и количество тревожных входов.
- Нажмите **Add** («Добавить»).

Когда устройство из офлайн режима перейдет в онлайн режим, программа подключится к нему автоматически.

- Нажмите **Add** («Добавить»).

Устройство, чей IP-адрес находится между начальным IP-адресом и конечным IP-адресом будет добавлено в список устройств.



Добавление устройств при помощи Hik-Connect домена

Цель:

Вы можете добавлять устройства, подключенные при помощи Hik-Connect, войдя в учетную запись Hik-Connect.

Перед началом:

Добавьте устройства в учетную запись Hik-Connect при помощи iVMS-4200, Мобильного клиента iVMS-4500 или Hik-Connect. Для получения информации о добавлении устройств в Hik-Connect при помощи iVMS-4200, обратитесь к *Руководству пользователя Клиентского ПО iVMS-4200*.

➤ Добавление одиночного устройства

Шаги:

- Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.
- Выберите **Hik-Connect Domain** («Hik-Connect домен») в поле **Adding Mode** («режим добавления»).

3. Выберите **Single Adding** («Одиночное добавление»).

4. Введите необходимую информацию.

Nickname («Имя устройства»): Измените имя устройства по вашему желанию.

Device Serial No. («Серийный номер устройства»): Введите серийный номер устройства.

User Name («Имя пользователя»): Введите имя пользователя устройства. По умолчанию имя пользователя - *admin*.

Password («Пароль»): Введите пароль устройства.



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.

Hik-Connect Account («Учетная запись Hik-Connect»): Введите имя пользователя учетной записи Hik-Connect.

Hik-Connect Password («Пароль Hik-Connect»): Введите пароль учетной записи Hik-Connect.

5. Опционально, вы можете поставить галочку **Export to Group** («Экспортировать в группу») для создания группы соответствующей имени устройства.

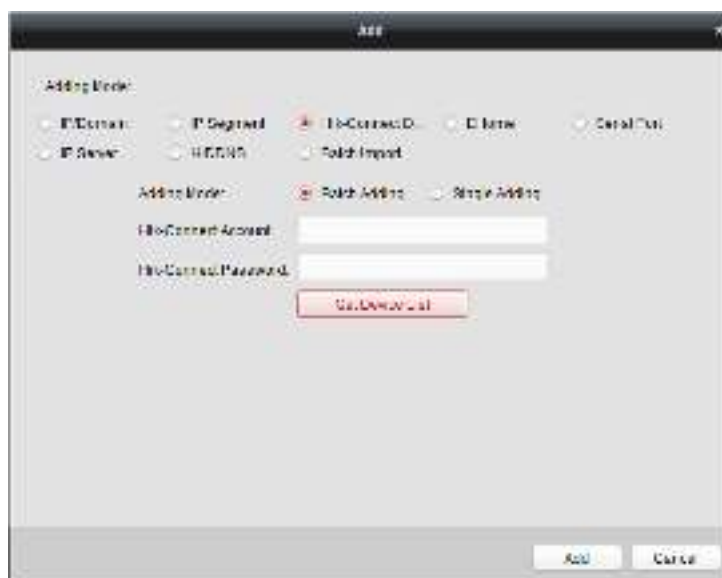
Все каналы устройства будут импортированы в соответствующую группу по умолчанию.

6. Нажмите **Add** («Добавить») для добавления устройства.

Пакетное добавление устройств

Шаги:

1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.



2. Выберите **Hik-Connect Domain** («Hik-Connect домен») в поле **adding mode** («режим добавления»).
3. Выберите **Batch Adding** («Пакетное добавление»).
4. Введите необходимую информацию.
Hik-Connect Account («Учетная запись Hik-Connect»): Введите имя пользователя учетной записи Hik-Connect.
Hik-Connect Password («Пароль Hik-Connect»): Введите пароль учетной записи Hik-Connect.
5. Нажмите **Get Device List** («Получить список устройств») для отображения устройств, добавленных в учетную запись Hik-Connect.



6. Поставьте галочки напротив устройств, которые вы хотите добавить.
7. Введите имя пользователя и пароль для устройств, которые вы собираетесь добавить.
8. Опционально, вы можете поставить галочку **Export to Group** («Экспортировать в группу») для создания группы соответствующей имени устройства.
 Все каналы устройства будут импортированы в соответствующую группу по умолчанию.

9. Нажмите **Add** («Добавить») для добавления устройств.

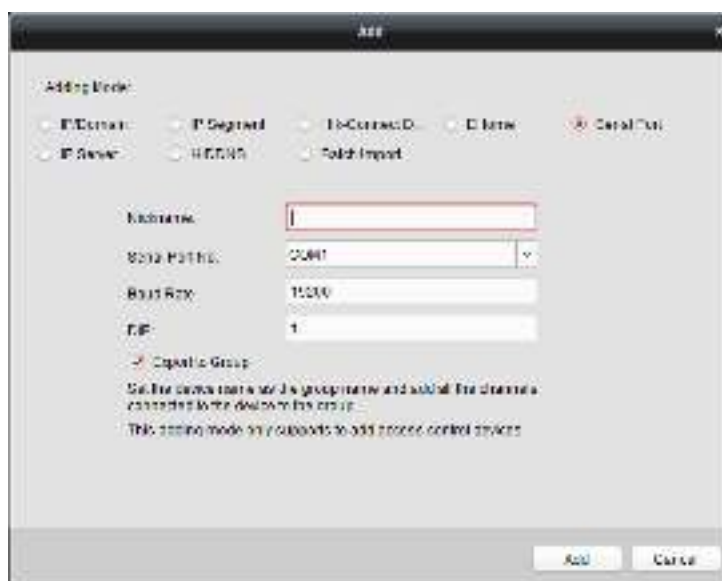
Добавление устройств при помощи последовательного порта

Цель:

Вы можете добавить устройство контроля доступа, подключенное через последовательный порт.

Шаги:

1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.
2. Выберите **Serial Port** («Последовательный порт») в поле **Adding Mode** («режим добавления»).



3. Введите необходимую информацию.

Nickname («Имя устройства»): Измените имя устройства по вашему желанию.

Serial Port No. («№ последовательного порта»): Выберите последовательный порт, при помощи которого подключено устройство.

Baud Rate («Скорость передачи данных (в бодах)»): Введите скорость передачи данных устройства контроля доступа.

DIP: Введите DIP-адрес устройства.

4. Опционально, вы можете поставить галочку **Export to Group** («Экспортировать в группу») для создания группы соответствующей имени устройства.

Все каналы устройства будут импортированы в соответствующую группу по умолчанию.

Примечание: iVMS-4200 так же предоставляет метод добавления офлайн устройств.

1) Поставьте галочку **Add Offline Device** («Добавить офлайн устройство»).

2) Введите необходимую информацию, включая количество каналов устройства и количество тревожных входов.

3) Нажмите **Add** («Добавить»).

Когда устройство из офлайн режима перейдет в онлайн режим, программа подключится к нему автоматически.

5. Нажмите **Add** («Добавить») для добавления устройства.

Добавление устройств при помощи IP сервера

Шаги:

1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.
2. Выберите **IP Server** («IP сервер») в поле **Adding Mode** («режим добавления»).

3. Введите необходимую информацию.

Nickname («Имя устройства»): Измените имя устройства по вашему желанию.

Server Address («Адрес сервера»): Введите IP-адрес ПК, на котором установлен IP сервер.

Device ID («ID устройства»): Введите ID устройства, зарегистрированный в IP сервере.

User Name («Имя пользователя»): Введите имя пользователя устройства. По умолчанию имя пользователя - *admin*.

Password («Пароль»): Введите пароль устройства.



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. Опционально, вы можете поставить галочку **Export to Group** («Экспортировать в группу») для создания группы соответствующей имени устройства.

Все каналы устройства будут импортированы в соответствующую группу по умолчанию.

Примечание: iVMS-4200 так же предоставляет метод добавления офлайн устройств.

- 1) Поставьте галочку **Add Offline Device** («Добавить офлайн устройство»).
- 2) Введите необходимую информацию, включая количество каналов устройства и количество тревожных входов.
- 3) Нажмите **Add** («Добавить»).

Когда устройство из офлайн режима перейдет в онлайн режим, программа подключится к нему автоматически.

5. Нажмите **Add** («Добавить») для добавления устройства.

Импорт устройств в пакетном режиме

Цель:

Устройства могут быть добавлены в программу в пакетном режиме путем внесения информации об устройствах в специальный CSV файл.

Шаги:

1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.
2. Выберите **Batch Import** («Пакетный импорт») в поле **Adding Mode** («режим добавления»).



3. Нажмите **Export Template** («Экспортировать шаблон») и сохраните предустановленный шаблон (CSV файл) на ваш ПК.
4. Откройте экспортированный файл шаблона и введите необходимую информацию об устройстве в соответствующие поля.
 - **Nickname** («Имя устройства»): Измените имя устройства по вашему желанию.
 - **Adding Mode** («Режим добавления»): Вы можете ввести «0», «2», «3», «4», «5» или «6», что соответствует различным режимам добавления. «0» обозначает, что устройство добавлено при помощи IP-адреса или доменного имени; «2» обозначает, что устройство добавлено при помощи IP сервера; «3» обозначает, что устройство добавлено при помощи HiDDNS; «4» обозначает, что устройство добавлено при помощи EHome протокола; «5» обозначает, что устройство добавлено при помощи последовательного порта; «6» обозначает, что устройство добавлено при помощи домена Hik-Connect.
 - **Address** («Адрес»): Измените адрес устройства. Если вы установили «0» в качестве режима добавления, вы должны ввести IP-адрес или доменное имя устройства; если вы установили «2» в качестве режима добавления, вы должны ввести IP-адрес ПК, на котором установлен IP сервер; если вы установили «3» в качестве режима добавления, вы должны ввести www.hik-online.com.
 - **Port** («Порт»): Введите № порта устройства. Значение по умолчанию - 8000.
 - **Device Information** («Информация устройства»): Если вы установили «0» в качестве

режима добавления, это поле заполнять не требуется; если вы установили «2» в качестве режима добавления, введите ID устройства зарегистрированного на IP сервере; если вы установили «3» в качестве режима добавления, введите доменное имя устройства зарегистрированного на HiDDNS сервере; если вы установили «4» в качестве режима добавления, введите данные учетной записи EHome; если вы установили «6» в качестве режима добавления, введите серийный номер устройства.

- **User Name** («Имя пользователя»): Введите имя пользователя устройства. По умолчанию имя пользователя - *admin*.
- **Password** («Пароль»): Введите пароль устройства.



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.

- **Add Offline Device** («Добавить офлайн устройство»): Вы можете поставить «1» для включения добавления офлайн устройств, и затем программа будет автоматически подключать устройства, когда они будут онлайн. Поставьте «0» в данном поле для отключения данной функции.
- **Export to Group** («Экспорт в группу»): Вы можете ввести «1» для создания группы по имени устройства (прозвищу). Все каналы устройства будут импортированы в соответствующую группу по умолчанию. «0» в данном поле обозначает отключение данной функции.
- **Channel Number** («Количество каналов»): Если вы установили «1» в поле **Add Offline Device** («Добавить офлайн устройство»), введите количество каналов устройства. Если вы установили «0» в поле **Add Offline Device** («Добавить офлайн устройство»), заполнять это поле не нужно.
- **Alarm Input Number** («Количество тревожных входов»): Если вы установили «1» в поле **Add Offline Device** («Добавить офлайн устройство»), введите количество тревожных входов устройства. Если вы установили «0» в поле **Add Offline Device** («Добавить офлайн устройство»), заполнять это поле не нужно.
- **Serial Port No.** («№ последовательного порта»): Если вы установили «5» в качестве режима добавления, введите № последовательного порта для устройства контроля доступа.
- **Serial Port No.** («№ последовательного порта»): Если вы установили «5» в качестве режима добавления, введите № последовательного порта для устройства контроля доступа.
- **DIP**: Если вы установили «5» в качестве режима добавления, введите DIP-адрес устройства контроля доступа.
- **Hik-Connect Account** («Учетная запись Hik-Connect»): Если вы установили «6» в качестве режима добавления, введите имя пользователя учетной записи Hik-Connect.
- **Hik-Connect Password** («Пароль Hik-Connect»): Если вы установили «6» в качестве

режима добавления, введите пароль учетной записи Hik-Connect.

5. Нажмите  и выберите файл шаблона.

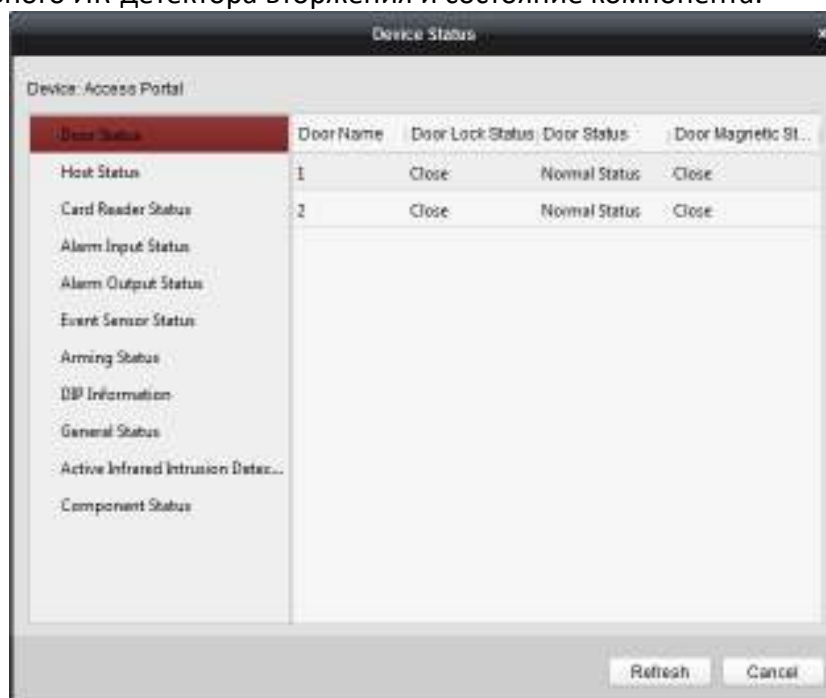
6. Нажмите **Add** («Добавить») для импорта устройств.

Устройства будут отображаться в списке устройств для управления после успешного добавления. Вы можете проверить использование ресурсов, состояние HDD, состояние записи и другую информацию о добавленных устройствах.

Нажмите **Refresh All** («Обновить все») для обновления информации всех добавленных устройств. Вы так же можете ввести имя устройства в поле **Filter** («Фильтр») для поиска.

6.4.2 Просмотр состояния устройства

В списке устройств вы можете выбрать устройство, а затем нажать кнопку **Device Status** («Состояние устройства») для просмотра его состояния. Вы можете просмотреть состояние двери, состояние хоста, состояние считывателя карт, состояние тревожного входа, состояние тревожного выхода, состояние постановки на охрану, DIP информацию, общее состояние, состояние активного ИК-детектора вторжения и состояние компонента.



Примечание: Интерфейс может отличаться от изображения выше. При использовании этой функции обратитесь к фактическому интерфейсу.

Название состояния	Описание
Door Status («Состояние двери»)	Просмотр состояния подключенной двери.
Host Status («Состояние хоста»)	Просмотр состояния хоста, включая состояние источника питания устройства, состояние запрета обратного прохода, состояние тамперинга хоста и т.д.
Card Reader Status («Состояние считывателя»)	Просмотр состояния считывателя карт, включая онлайн состояние, состояние тамперинга и метод аутентификации.

карт»)	
Alarm Input Status («Состояние тревожного входа»)	Просмотр состояния тревожного входа.
Alarm Output Status («Состояние тревожного выхода»)	Просмотр состояния тревожного выхода.
Event Sensor Status («Состояние датчика событий»)	Просмотр состояния датчика события.
Arming Status («Состояние постановки на охрану»)	Просмотр IP-адреса устройства, находящегося под охраной, и его типа постановки на охрану.
DIP Information («DIP информация»)	Просмотр локальной DIP информации устройства.
General Status («Общее состояние»)	Просмотр общего состояния устройства, в том числе состояния синхронизации шины, ИК подсчета посетителей для входа, подсчета аутентифицированных людей для входа и т. д.
Active Infrared Intrusion Detector Status («Состояние активного ИК-детектора вторжения»)	Просмотр состояния активного ИК-детектора вторжения, приемной платы и т. д.
Component Status («Состояние компонента»)	Просмотр состояния компонентов устройства, включая состояние датчика двигателя, состояние тормоза и т. д.

6.4.3 Редактирование основной информации

Цель:

После добавления устройства контроля доступа вы можете изменить основную информацию устройства.

Шаги:

1. Выберите устройство в списке устройств.
2. Нажмите **Modify** («Изменить») для появления всплывающего окна изменения информации устройства.
3. Нажмите вкладку **Basic Information** («Основная информация») для перехода в меню основной информации.



- Измените информацию устройства, включая **Adding Mode** («режим добавления»), **Device Name** («имя устройства»), **Device IP Address** («IP-адрес устройства»), **port No.** («№ порта»), **User name** («имя пользователя») и **Password** («пароль»).

6.4.4 Настройки RS-485

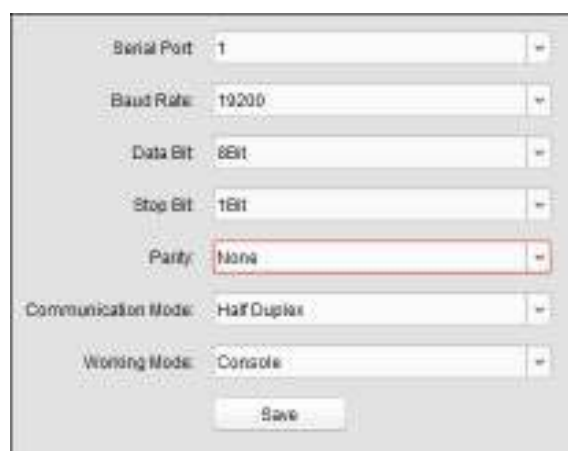
Цель:

Вы можете установить параметры RS-485, включая последовательный порт, скорость передачи (в бодах), бит данных, стоповый бит, тип четности, режим связи, рабочий режим и режим соединения.

Примечание: Настройки RS-485 должны поддерживаться устройством.

Шаги:

- Выберите устройство в списке устройств и нажмите **Modify** («Изменить») для появления всплывающего окна изменения информации устройства.
- Нажмите вкладку **RS-485 Settings** («Настройки RS-485») для перехода в меню настройки RS-485.



- Выберите **Serial Port** («Последовательный порт») из выпадающего списка для установки

параметров RS-485.

3. Установите **Baud Rate** («скорость передачи в бодах»), **Data Bit** («бит данных»), **Stop Bit** («стоповый бит»), **Parity** («четность»), **Flow Control** («управление потоком»), **Communication Mode** («режим связи»), **Working Mode** («рабочий режим») и **Connection Mode** («режим подключения»).
4. Нажмите **Save** («Сохранить») для сохранения настроек, и сконфигурированные параметры будут применены к устройству автоматически.

Примечание: После изменения рабочего режима устройство будет перезагружено. После изменения рабочего режима появится соответствующая подсказка.

6.4.5 Аутентификация с шифрованием карт M1

Перед началом:

Вы должны использовать определенный настольный считыватель карт Hikvision для выдачи карт. Для получения подробной информации смотрите пункт *Добавление человека (Карта)* в Разделе **Ошибка! Источник ссылки не найден. Добавление людей.**

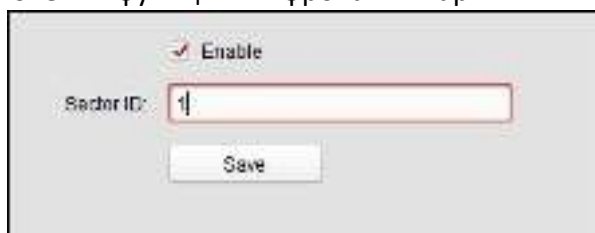
Цель:

Функция шифрования карт M1 повышает уровень безопасности аутентификации, она должна применяться совместно с настольным считывателем карт нашей компании через клиентское программное обеспечение или веб-клиент. После выдачи карты вы можете установить функцию шифрования карт M1 на контроллере.

Примечание: Функция должна поддерживаться устройством контроля доступа и считывателем карт.

Шаги:

1. Выберите устройство в списке устройств, нажмите **Modify** («Изменить») для появления всплывающего окна изменения информации устройства.
2. Нажмите вкладку **M1 Card Encryption** («Шифрование карт M1») для перехода в соответствующий интерфейс.
3. В интерфейсе **M1 Card Encryption** («Шифрование карт M1») поставьте галочку **Enable** («Включить») для включения функции шифрования карт M1.



4. Задайте значение **Sector ID** («ID сектора»).
5. Нажмите **Save** («Сохранить») для сохранения настроек.

Примечание: ID сектора может быть в диапазоне от 1 до 100.

6.4.6 Удаленная конфигурация

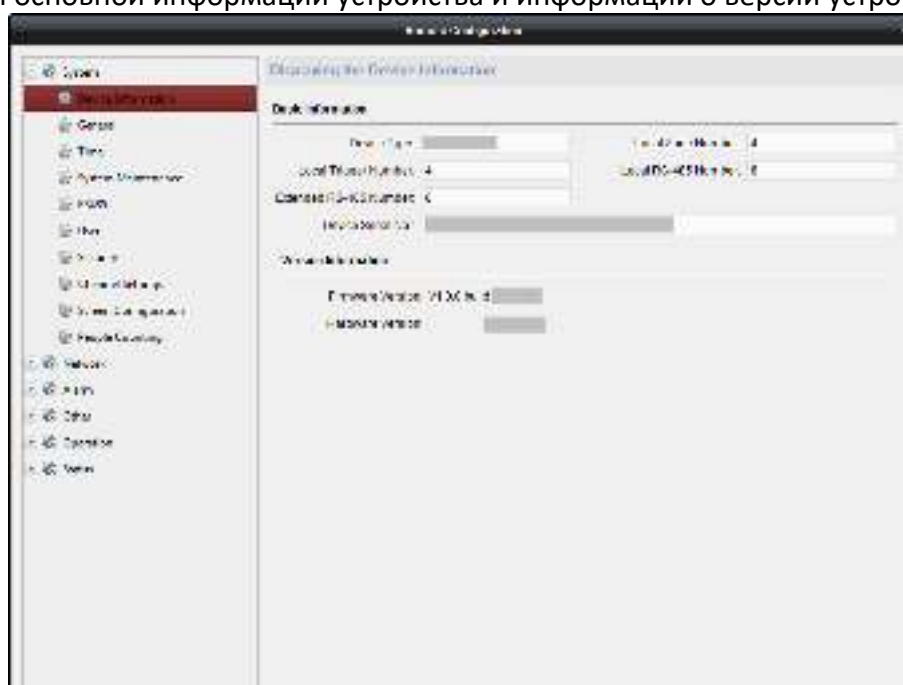
Цель:

В списке устройств выберите устройство и нажмите кнопку **Remote Configuration** («Удаленная конфигурация») для перехода в меню удаленной конфигурации. Вы можете установить параметры выбранного устройства.

Проверка информации устройства

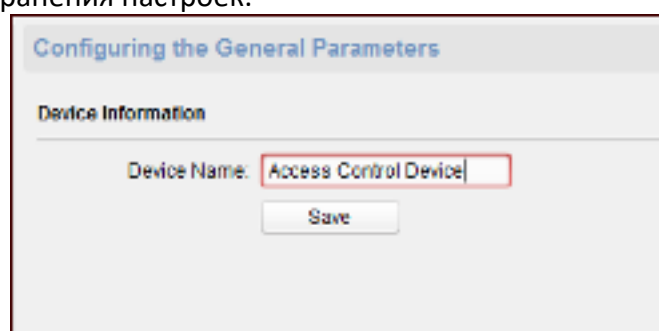
Шаги:

1. В списке устройств вы можете нажать **Remote Configuration** («Удаленная конфигурация») для перехода в меню удаленной конфигурации.
2. Нажмите **System -> Device Information** («Система -> Информация устройства») для проверки основной информации устройства и информации о версии устройства.



Изменение имени устройства

В меню удаленной конфигурации нажмите **System -> General** («Система -> Общие») для конфигурации имени устройства и перезаписи параметра файлов записи. Нажмите **Save** («Сохранить») для сохранения настроек.



Редактирование времени

Шаги:

1. В меню удаленной конфигурации нажмите **System -> Time** («Система -> Время») для конфигурации временной зоны.
2. (Опционально) Поставьте галочку **Enable NTP** («Включить NTP») и настройте **NTP Server Address** («адрес NTP сервера»), **NTP Port** («NTP порт») и **Synchronization Interval** («интервал синхронизации»).
3. (Опционально) Поставьте галочку **Enable DST** («Включить DST») и настройте **DST Start Time** («время начала DST»), **DST End Time** («время окончания DST») и **Bias** («смещение»).
4. Нажмите **Save** («Сохранить») для сохранения настроек.

Настройка обслуживания системы

Цель:

Вы можете перезагрузить устройство удаленно, восстановить настройки устройства по умолчанию, импортировать файл конфигурации, обновить устройство и т. д.

Шаги:

1. В меню удаленной конфигурации нажмите **System -> System Maintenance** («Система -> Обслуживание системы»).
2. Нажмите **Reboot** («Перезагрузить») для перезагрузки устройства.
Или нажмите **Restore Default Settings** («Восстановить настройки по умолчанию») для восстановления настроек устройства до настроек по умолчанию, кроме IP-адреса.
Или нажмите **Restore All** («Восстановить все») для восстановления всех параметров до настроек по умолчанию. Устройство необходимо будет активировать заново.

Примечание: Файл конфигурации содержит параметры устройства.

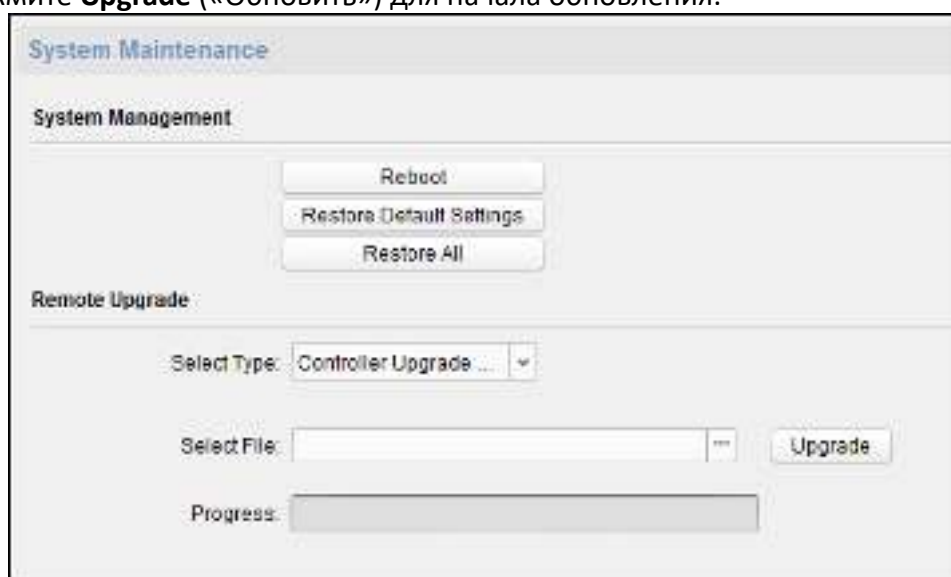
3. Вы также можете удаленно обновить устройство.
 - 1) В поле **Remote Upgrade** («Удаленное обновление») выберите тип обновления из выпадающего списка: **Controller Upgrade File** («Файл обновления контроллера»), **Card Reader Upgrade File** («Файл обновления считывателя карт») или **Upgrade File of Lane Controller** («Файл обновления контроллера прохода»).

Controller Upgrade File («Файл обновления контроллера»): Обновить контроллер доступа.

Card Reader Upgrade File («Файл обновления считывателя карт»): Обновить считыватель карт. Только считыватели карт, подключенные через RS-485, могут быть обновлены удаленно.

Upgrade File of Lane Controller («Файл обновления контроллера прохода»): Выберите ведущий контроллер прохода или подчиненный контроллер прохода для обновления.

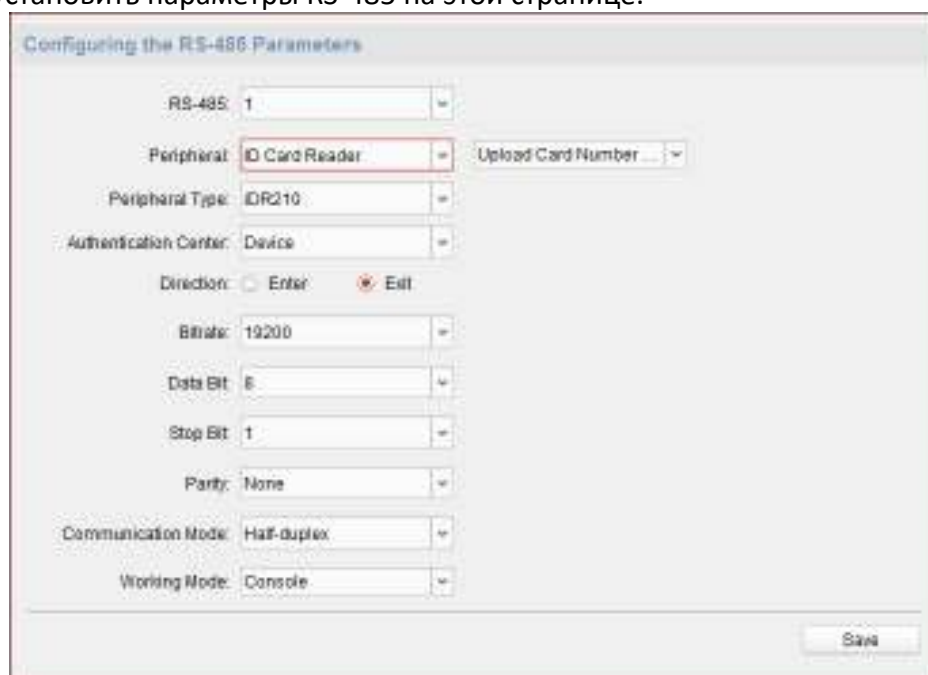
- 2) Нажмите  для выбора файла обновления.
- 3) Нажмите **Upgrade** («Обновить») для начала обновления.



The screenshot shows the 'System Maintenance' window. Under the 'System Management' tab, there are buttons for 'Reboot', 'Restore Default Settings', and 'Restore All'. Below this is the 'Remote Upgrade' section. It includes a 'Select Type' dropdown menu currently set to 'Controller Upgrade ...'. Below that is a 'Select File' text field with a browse icon (three dots) to its right. To the right of the text field is an 'Upgrade' button. At the bottom of the section is a 'Progress' label followed by a progress bar.

Настройка параметров RS-485

Вы можете установить параметры RS-485 на этой странице.



The screenshot shows the 'Configuring the RS-485 Parameters' window. It contains several configuration fields:

- RS-485:** A dropdown menu set to '1'.
- Peripheral:** A dropdown menu set to 'ID Card Reader'. To its right is an 'Upload Card Number ...' dropdown menu.
- Peripheral Type:** A dropdown menu set to 'IDR210'.
- Authentication Center:** A dropdown menu set to 'Device'.
- Direction:** Radio buttons for 'Enter' and 'Exit', with 'Exit' selected.
- Baudrate:** A dropdown menu set to '19200'.
- Data Bit:** A dropdown menu set to '8'.
- Stop Bit:** A dropdown menu set to '1'.
- Parity:** A dropdown menu set to 'None'.
- Communication Mode:** A dropdown menu set to 'Half-duplex'.
- Working Mode:** A dropdown menu set to 'Console'.

 A 'Save' button is located at the bottom right of the window.

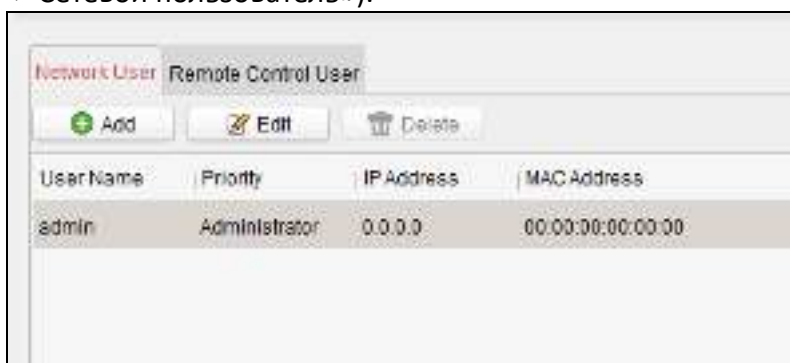
Примечания:

- Поддерживает 9 периферийных устройств: считыватель ID-карт, считыватель IC-карт, сканер QR-кодов, считыватель отпечатков пальцев и карт, текстовый экран, устройство переработки карт, считыватель отпечатков пальцев и терминал идентификации ID-карт.
- Если в качестве периферийного устройства выбраны считыватель ID-карт, сканер QR-кодов, устройство переработки карт, текстовый экран или считыватель отпечатков пальцев, вам следует указать направление доступа.
- Если в качестве внешнего устройства выбран считывать IC-карт или считыватель отпечатков пальцев, вам следует установить направление доступа, установив DIP-переключатель.
- Система поддерживает 3 центра аутентификации: **Device** («Устройство»), **Client** («Клиент») и **Swipe Card** («Проводка карты»). Если вы выберете **Swipe Card** («Проводка карты»), то турникет откроет створки немедленно без оценки разрешений после аутентификации пользователя при помощи сконфигурированных периферийных устройств.
- Тип центра аутентификации **Client** («Клиент») в основном используется разработчиками стороннего программного обеспечения.

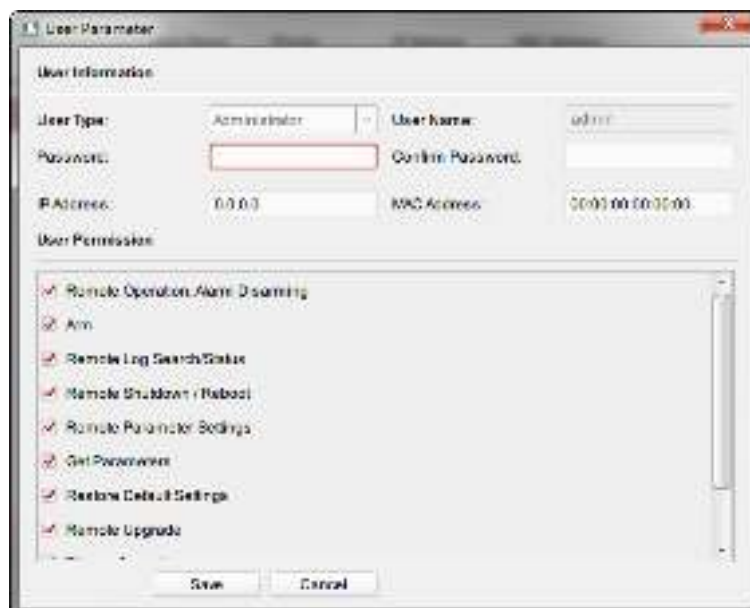
Управление сетевыми пользователями

Шаги:

1. В меню удаленной конфигурации нажмите **System -> User -> Network User** («Система -> Пользователь -> Сетевой пользователь»).



2. Нажмите **Add** («Добавить») для добавления пользователя (Не поддерживается контроллером лифта.).
Или выберите пользователя из списка и нажмите **Edit** («Редактировать») для изменения пользователя. Вы можете изменить пароль пользователя, IP-адрес, MAC-адрес и разрешения пользователя. Нажмите **OK** для подтверждения изменений.



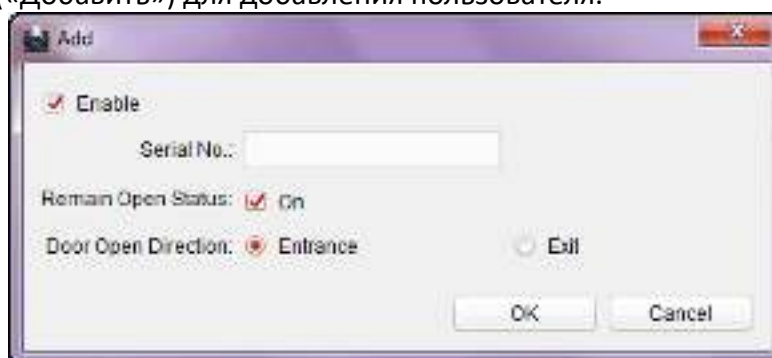
Управление при помощи пульта ДУ

Цель:

Вы можете выполнить сопряжение кода пульта ДУ с устройством. После сопоставления кода вы сможете управлять устройством с помощью пульта дистанционного управления.

Шаги:

1. В меню удаленной конфигурации нажмите **System -> User -> Remote Control User** («Система -> Пользователь -> Пользователь пульта ДУ»).
2. Нажмите **Add** («Добавить») для добавления пользователя.



3. Поставьте галочку **Enable** («Включить») во всплывающем окне и задайте серийный номер пульта ДУ в поле **Serial No** («Серийный номер»).
4. (Опционально) Поставьте галочку **Remain Open Status** («Состояние: Оставить открытым») для распашного турникета.

Примечание: Если эта функция включена, то вы сможете управлять турникетом в состоянии «Оставить открытым» при помощи пульта дистанционного управления (после его сопряжения).

5. Установите **Door Open Direction** («направление открытия двери»).
6. Нажмите **OK** для сохранения настроек.

Примечание: Вы можете добавить до 32 пользователей удаленного управления.

Настройка безопасности

Цель:

Вы можете установить параметры безопасности при входе в устройство.

Шаги:

1. Нажмите **System -> Security** («Система -> Безопасность»).



2. Выберите **Encryption Mode** («режим шифрования») из выпадающего списка. Вы можете выбрать **Compatible Mode** («Совместимый режим») или **Encryption Mode** («Режим шифрования»).
3. Нажмите **Save** («Сохранить») для сохранения настроек.

Конфигурация параметров прохода

Цель:

Вы можете установить параметры прохода для человека, проходящего через устройство, включая задержку срабатывания тревоги и период тайм-аута запуска ИК-лучей.

Нажмите **System -> Passing Settings** («Система -> Настройки прохода») и установите параметры. Нажмите **Save** («Сохранить») для сохранения настроек.

Описание параметров представлено ниже:

Valid Passing Duration

(«Действительное время прохождения»):

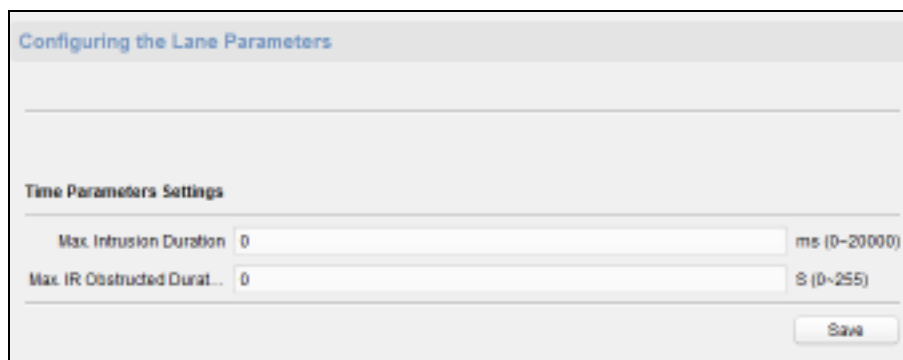
Если человек находится в проходе или проходит через него в течение времени, превышающего заданный промежуток времени, будет запущена тревога. Если установлено значение «0», то функция отключена.

Примечание: Рекомендуемая минимальная продолжительность обнаружения составляет 2 сек.

Max. IR Obstructed Duration

(«Макс. продолжительность времени прерывания ИК-лучей»):

Установите максимальную продолжительность времени для прерывания ИК-лучей. Если ИК-подсветка перекрыта на больший промежуток времени, чем заданный промежуток времени, то сработает сигнализация. Если установлено значение «0», то функция отключена.



Конфигурация параметров экрана

Цель:

Устройство может подключаться к текстовому экрану. Вы можете установить параметры отображения на этой странице.

Нажмите **System -> Screen Configuration** («Система -> Конфигурация экрана») и установите параметры. Нажмите **Save** («Сохранить») для сохранения настроек.

Примечание: Для лучшей производительности мы предлагаем вам использовать параметры по умолчанию.

Описание параметров представлено ниже:

Screen Position («Положение экрана»):	Выберите положение экрана. Если из выпадающего списка выбрано значение Exit («Выход»), экран будет установлен на выходе.
Screen Model («Модель экрана»):	Выберите модель экрана из выпадающего списка.
Font Size («Размер шрифта»):	Выберите размер шрифта текста на экране.
Text Orientation («Ориентация текста»):	Выберите ориентацию текста на экране.
Line Spacing («Межстрочный интервал»):	Установите расстояние между двумя строками.
Word Spacing («Интервал между словами»):	Установите расстояние между двумя словами.
Initial Position («Начальная позиция»):	Установите позицию первого символа, отображаемого на экране.



Конфигурация подсчета людей

Цель:

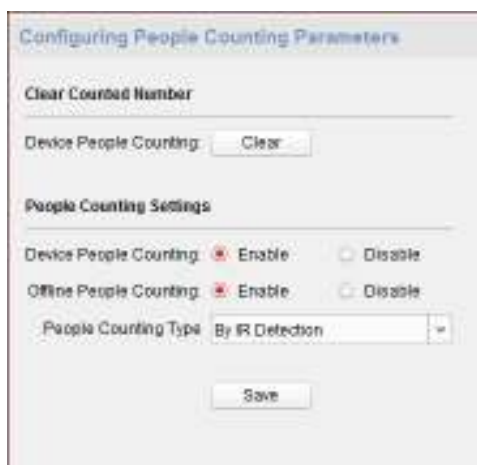
Вы можете установить параметры подсчета людей.

Нажмите **System -> People Counting** («Система -> Подсчет людей») и установите параметры.

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

Описание параметров представлено ниже:

Clear People Number («Очистить число людей»):	Нажмите Clear («Очистить») и подсчитанное количество людей будет сброшено до нуля.
Device People Counting («Подсчет людей на устройстве»):	Нажмите Enable («Включить») или Disable («Отключить») для включения или отключения функции подсчета людей.
Offline People Counting on Client («Офлайн подсчет людей в клиенте»):	Нажмите Enable («Включить») или Disable («Отключить») для включения или отключения функции офлайн подсчета людей в клиенте. Если эта функция включена и устройство находится в офлайн режиме, устройство продолжит подсчет людей, и их число будет сохранено в устройстве. Когда устройство перейдет в онлайн режим, клиент автоматически выполнит считывание обновленного числа людей с устройства.
People Counting Type («Тип подсчета людей»):	Вы можете выбрать значения: None («Никакой»), By IR Detection («При помощи ИК-детекции») и By Authentication Number («По числу аутентификаций»). None («Никакой»): Устройство не будет считать людей. Если функция подсчета людей на устройстве включена, функция подсчета людей все равно будет отключена. By IR Detection («При помощи ИК-детекции»): Устройство будет подсчитывать количество людей, проходящих через устройство, на основе ИК-детекции. By Authentication Number («По числу аутентификаций»): Устройство будет подсчитывать людей, которые проходят аутентификацию на устройстве. Неудачная аутентификация тоже будет считаться за 1.



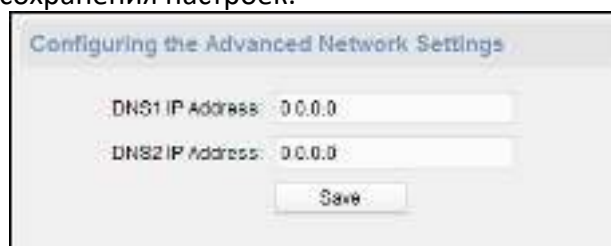
Конфигурация сетевых параметров

Нажмите **Network -> General** («Сеть -> Общие»). Вы можете настроить NIC, тип NIC, IPv4 адрес, маску подсети (IPv4), шлюз по умолчанию (IPv4), MAC-адрес, MTU и порт устройства. Нажмите **Save** («Сохранить») для сохранения настроек.



Настройка расширенных сетевых параметров

Нажмите **Network -> Advanced Settings** («Сеть -> Расширенные настройки»). Вы можете настроить **DNS IP address 1** («IP-адрес DNS 1»), **DNS IP address 2** («IP-адрес DNS 2»). Нажмите **Save** («Сохранить») для сохранения настроек.



Конфигурация параметров зоны

Шаги:

1. Нажмите **Alarm -> Zone** («Тревога -> Зона»).
Вы можете просмотреть параметры зоны.



Zone	Name	Zone Type	Sensitivity	Settings
1		24-hour Voiced ...	250ms	
2		24-hour Voiced ...	250ms	
3		24-hour Voiced ...	250ms	
4		24-hour Voiced ...	250ms	

- Нажмите  для появления всплывающего окна **Zone Settings** («Настройки зоны»).
- Задайте **Zone Name** («имя зоны»), **Zone Detector Type** («тип детектора зоны»), **Zone Type** («тип зоны»), **Sensitivity Value** («значение чувствительности»), **Linked Trigger** («связанный триггер») и другие параметры.
- Нажмите **Save** («Сохранить») для сохранения параметров.
Или нажмите **Copy to...** («Копировать в») для копирования информации зоны в другие зоны.

Конфигурация параметров реле

Цель:

Установите параметры реле тревожного выхода основного контроллера.

Шаги:

- Нажмите **Alarm -> Trigger** («Тревога -> Триггер»).
- Вы можете просмотреть параметры триггера.



Relay	Name	Output Delay(s)	Zone Linkage	Settings
1		0	None	
2		0	None	
3		0	None	
4		0	None	

- Нажмите  для появления всплывающего окна настройки параметров триггера.
- Настройте значения в полях **Relay Name** («имя реле») и **Output Delay** («задержка вывода»).
- Нажмите **Save** («Сохранить») для сохранения параметров.
Или нажмите **Copy to...** («Копировать в») для копирования информации реле в другие реле.

Конфигурация аудио файла

Цель:

Вы можете связать аудио файл с соответствующей воспроизводимой сценой. Вы также можете экспортировать аудио файл из системы и импортировать аудио файл из локального ПК.

Шаги:

1. Нажмите **Other -> Audio File** («Другие -> Аудио файл») для перехода на страницу аудио файлов.

Примечание: По умолчанию система содержит аудиоконтент. Для получения подробной информации об аудио индексах смотрите Приложение С Таблица значений аудио индексов.

The screenshot shows the 'Audio File' window. At the top, there is a section 'Add Audio File:' with a file input field, an 'Import' button, and an 'Export' button. Below this is a 'Play Sence:' section with a 'Save Param...' button and a dropdown menu. The main part of the window is a table with three columns: 'Index', 'Play Sence', and 'Descriptions'. The table contains 13 rows of data. The 'Play Sence' column has a dropdown arrow next to each entry. The entry 'Authenticated' in row 8 is highlighted with a red box.

Index	Play Sence	Descriptions
1	Do Not Play	audio1
2	Authentication Failed	audio1
3	Do Not Play	audio 2
4	Do Not Play	audio 2
5	Do Not Play	audio 2
6	Do Not Play	audio 2
7	Authentication Failed	audio1
8	Authenticated	audio1
9	Authentication Failed	audio1
10	Do Not Play	audio 2
11	Do Not Play	audio 2
12	Authentication Failed	audio1
13	Authentication Failed	audio1

2. Выберите индекс (воспроизводимый контент) соответствующий сцене.
3. (Опционально) Введите описание сцены.
4. Нажмите **Save Parameters** («Сохранить параметры») для сохранения связи между индексом (воспроизводимым контентом) и сценой воспроизведения.
5. (Опционально) Нажмите **Export** («Экспорт») для экспорта аудио файла по умолчанию на локальный компьютер.
6. (Опционально) Нажмите  и выберите аудио файл с локального компьютера. Нажмите **Import** («Импорт») для импорта файла в устройство.

Примечания:

- Импортированный аудио файл должен быть в формате MEM.
- Для получения дополнительной информации о преобразовании другого формата аудио файла в формат MEM смотрите Руководство по преобразованию аудио.
- Если вы используете стороннее программное обеспечение для создания или редактирования аудио файлов, громкость аудио файла должна быть не менее 0 x 68. Если громкость меньше этого значения, будет превышено энергопотребление динамика, что приведет к его повреждению.

Операции с зоной

Цель:

Вы можете устанавливать на охрану/снимать с охраны зону.

Нажмите **Operation** -> **Zone** («Операции -> Зона») для перехода в соответствующее меню. Поставьте галочку напротив зоны и нажмите кнопку **Arm** («Поставить на охрану») или **Disarm** («Снять с охраны»).

Zone No.	Name	Partition	Status of Alarm	Status of Guard	Fault Status
☐ 1		None	Alarm	Disarm	Normal
☐ 2		None	Alarm	Disarm	Normal
☐ 3		None	Alarm	Disarm	Normal
☐ 4		None	Alarm	Disarm	Normal

Операции с реле

Цель:

Откройте или закройте реле тревожного выхода основного контроллера устройства.

Шаги:

1. Нажмите **Operation** -> **Relay** («Операции -> Реле»).
2. Вы можете просмотреть состояние реле.
3. Поставьте галочку напротив реле.
4. Нажмите **Open** («Открыть») или **Close** («Закрыть») для открытия или закрытия реле.
4. (Опционально) Нажмите **Refresh** («Обновить») для обновления статуса реле.

Relay No.	Name	Status
☐ 1		Close
☐ 2		Close
☐ 3		Close
☐ 4		Close

Просмотр статуса реле

Нажмите **Status** -> **Relay** («Статус -> Реле») для просмотра статуса реле.

Relay	Status
Relay1	Close
Relay2	Close
Relay3	Close
Relay4	Close

6.5 Управление организацией

Вы можете добавлять, изменять или удалять организации по вашему желанию.

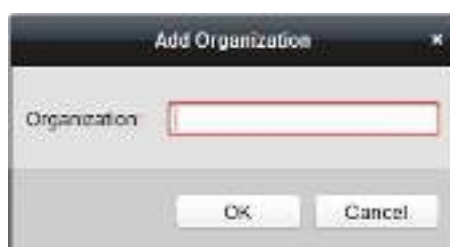
Нажмите иконку  для перехода в меню управления людьми и картами.

6.5.1 Добавление организации

Шаги:

1. В списке организаций слева вы должны добавить верхнюю организацию как головную организацию для всех организаций.

Нажмите кнопку **Add** («Добавить») для появления всплывающего окна добавления организации.



2. Введите **Organization Name** («Имя организации») по вашему усмотрению.
 3. Нажмите **OK** для подтверждения добавления.
 4. Вы можете добавить несколько уровней организаций в соответствии с фактическими потребностями.
Чтобы добавить дочернюю организацию, выберите родительскую организацию и нажмите **Add** («Добавить»).
- Повторите *Шаг 2* и *3* для добавления дочерней организации.
- Тогда добавленная организация станет дочерней для организации верхнего уровня.

Примечание: Можно создать до 10 уровней организаций.

6.5.2 Изменение и удаление организации

Вы можете выбрать добавленную организацию и нажать **Modify** («Изменить») для изменения ее имени.

Вы можете выбрать добавленную организацию и нажать **Delete** («Удалить») для ее удаления.

Примечания:

- Организации нижнего уровня будут удалены, если вы удалите организацию верхнего уровня.
- Убедитесь, что в организацию не добавлены люди, иначе организация не сможет быть удалена.

6.6 Управление людьми

После добавления организации вы можете добавить человека в организацию и управлять добавленными людьми, например, выпускать карточки в пакетном режиме, импортировать и экспортировать информацию пользователя в пакетном режиме и т. д.

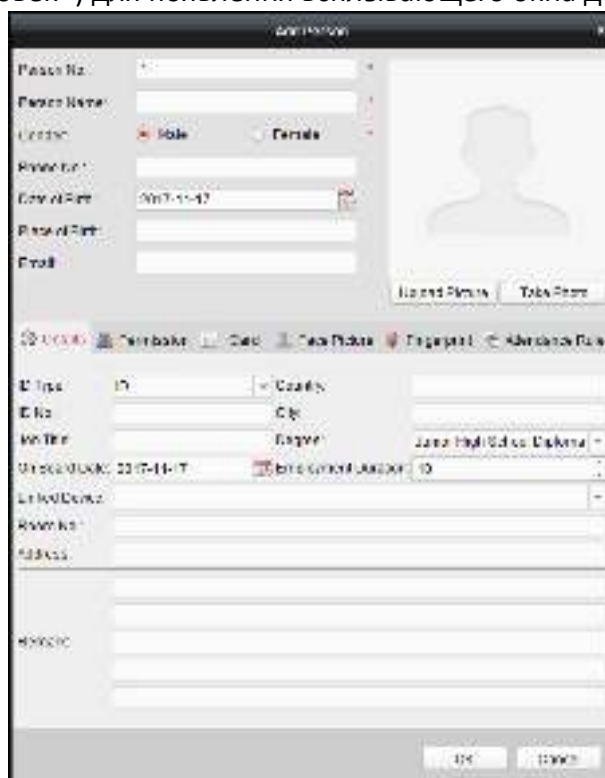
Примечание: Может быть добавлено до 10,000 человек или карт.

6.6.1 Добавление людей

Добавление человека (Основная информация)

Шаги:

1. Выберите организацию в списке организаций и нажмите кнопку **Add** («Добавить») на панели **Person** («Человек») для появления всплывающего окна добавления людей.

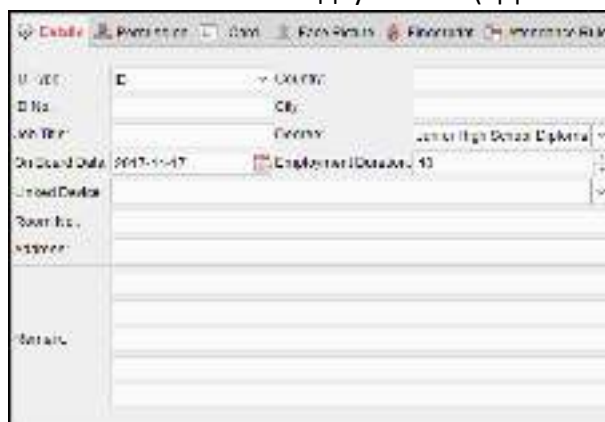
The image shows a 'Add Person' window with the following fields: Person No. (auto-generated), Person Name, Gender (radio buttons for Male and Female), Phone No., Birthday (Month, Day, Year), Email, ID Type (dropdown), ID No., ID Photo (button), and a section for Address. There are also buttons for 'Upload Picture' and 'Take Photo'.

2. **Person No.** («№ человека») будет сгенерирован автоматически и не может быть изменен.
3. Введите основную информацию, включая **Person Name** («имя человека»), **Gender** («пол»), **Phone No.** («№ телефона»), **Birthday Details** («детали рождения») и **email**.
4. Нажмите **Upload Picture** («Загрузить изображение») для выбора изображения человека из папки на локальном ПК и загрузки в клиент.
Примечание: Изображение должно быть в формате *.jpg.
5. (Опционально) Вы также можете нажать **Take Photo** («Сделать фото») для того, чтобы сделать фото человека при помощи камеры ПК.
6. Нажмите **OK** для завершения добавления.

Добавление человека (Подробная информация)

Шаги:

1. В меню добавления человека нажмите вкладку **Details** («Детали»).



2. Введите подробную информацию о человеке, включая **ID Type** («тип ID»), **ID No.** («ID номер»), **Country** («страна») и другие.
 - **Linked Device** («Связанные устройства»): Вы можете привязать видеодомофон к человеку.
Примечание: Если вы выбрали значение **Analog Indoor Station** («Аналоговый видеодомофон») в поле **Linked Device** («Связанные устройства»), тогда будет отображено поле **Door Station** («Вызывная панель»), и вам необходимо будет выбрать вызывную панель для связи с аналоговым видеодомофоном.
 - **Room No.** («№ кабинета»): Вы можете ввести номер кабинета для человека.
3. Нажмите **OK** для сохранения настроек.

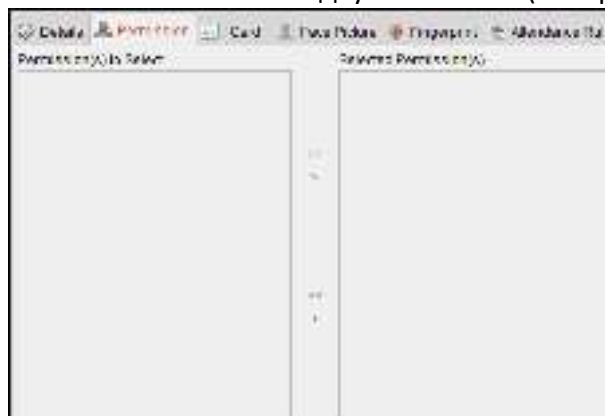
Добавление человека (Разрешения)

Вы можете назначать разрешения (включая разрешения на операции устройства контроля доступа и разрешения контроля доступа) человеку при его добавлении.

Примечание: Для получения подробной информации о разрешениях контроля доступа смотрите Раздел **Ошибка! Источник ссылки не найден. Конфигурация разрешений.**

Шаги:

1. В меню добавления человека нажмите вкладку **Permission** («Разрешения»).



2. В поле **Device Operation Role** («Роль для работы с устройством») выберите роль для

работы с устройством контроля доступа.

Normal User («Обычный пользователь»): Человек имеет разрешение на отметку о входе/выходе в устройстве, на проход через контрольные точки доступа и др.

Administrator («Администратор»): У администратора есть разрешения обычного пользователя, а также разрешение на конфигурацию устройства, включая добавление обычных пользователей и др.

3. В списке **Permission(s) to Select** («Разрешения для выбора») отображаются все сконфигурированные разрешения.

Поставьте галочку (-и) напротив разрешений и нажмите > для их добавления в список **Selected Permission(s)** («Выбранные разрешения»).

(Опционально) Вы можете нажать >> для добавления всех отображенных разрешений в список **Selected Permission(s)** («Выбранные разрешения»).

(Опционально) В списке **Selected Permission(s)** («Выбранные разрешения») выберите разрешения и нажмите кнопку < для их удаления из данного списка. Вы также можете нажать << для удаления всех выбранных разрешений.

4. Нажмите **ОК** для сохранения настроек.

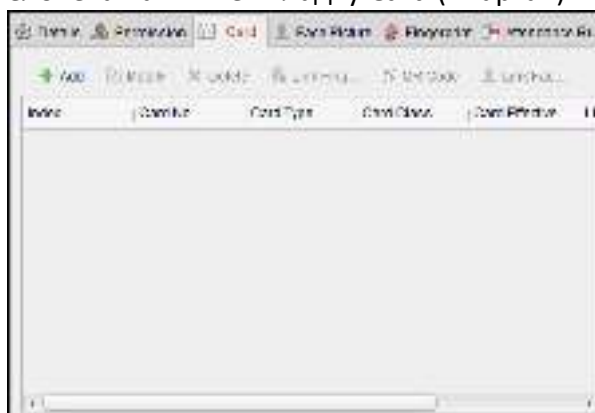
Добавление человека (Карта)

Вы можете добавлять карты и выдавать их людям.

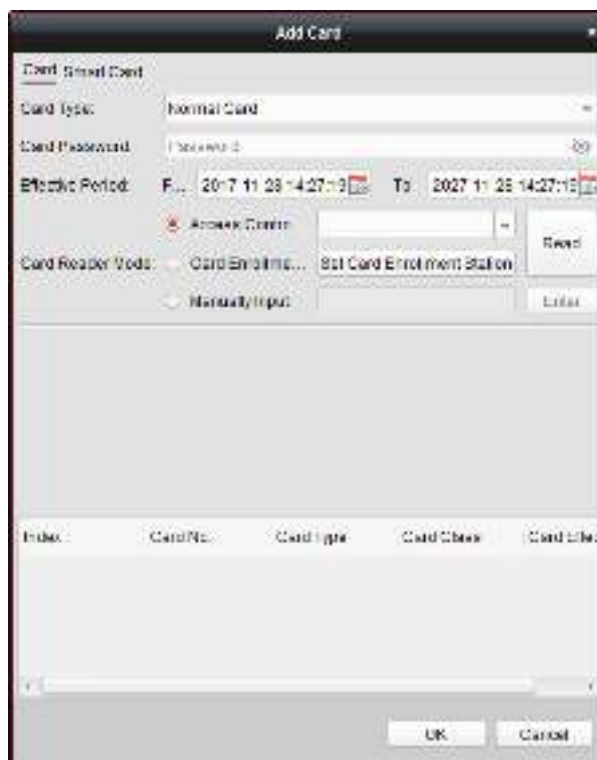
➤ Добавление обычной карты

Шаги:

1. В меню добавления человека нажмите вкладку **Card** («Карта»).



2. Нажмите **Add** («Добавить») для появления всплывающего окна добавления карты
3. Нажмите вкладку **Card** («Карта»).



4. Выберите необходимый вам тип карты.

- **Normal Card** («Обычная карта»)
- **Card for Disabled Person** («Карта для инвалидов»): Дверь останется открытой в течение заданного периода времени для владельца данной карты.
- **Card in Blacklist** («Карта в черном списке»): Действие проводки карты будет загружено в систему и дверь не будет открыта.
- **Patrol Card** («Патрульная карта»): Действие проводки карты может использоваться для проверки состояния персоналом инспектирования. Разрешения доступа для персонала инспектирования могут быть настроены по вашему усмотрению.
- **Duress Card** («Принудительная карта»): Дверь может быть открыта при помощи проводки принудительной карты. В тоже время клиент создает уведомление о событии принуждения.
- **Super Card** («Супер карта»): Карта действительна для всех дверей контроллера в течение заданного в расписании времени.
- **Visitor Card** («Карта посетителя»): Карта, предназначенная для посетителей. Для карты посетителя вы можете установить параметр **Max. Swipe Times** («Макс. число проводок»).

Примечания:

- Параметр **Max. Swipe Times** («Макс. число проводок») должен быть в промежутке от 0 до 255. При установке значения «0» количество проводок карты не ограничено.
- Может быть добавлено до 3000 карт посетителей.

5. Введите пароль от самой карты в поле **Card Password** («Пароль карты»). Пароль карты должен содержать от 4 до 8 цифр.

Примечание: Пароль будет необходим, когда держатель карты проведет картой для входа или выхода через дверь, если включены такие режимы аутентификации считывателя карт как **Card and Password** («Карта и Пароль»), **Password and Fingerprint** («Пароль и Отпечаток пальца»), **Card** («Карта»), **Password** («Пароль») и **Fingerprint** («Отпечаток пальца»). Для получения подробной информации смотрите *Раздел Ошибка! Источник ссылки не найден. Ошибка! Источник ссылки не найден..*

6. Нажмите  для установки времени действия и истечения действия карты.
7. Выберите **Card Reader Mode** («Режим считывателя карт») для считывания номера карты.
 - **Access Controller Reader** («Считыватель карт контроллера доступа»): Поместите карту на считыватель контроллера доступа и нажмите **Read** («Считать») для получения номера карты.
 - **Card Enrollment Station** («Настольный считыватель карт»): Поместите карту на настольный считыватель карт и нажмите **Read** («Считать») для получения номера карты.

Примечание: Настольный считыватель карт должен быть подключен к ПК с запущенным клиентом. Вы можете нажать **Set Card Enrollment Station** («Установить настольный считыватель карт») для перехода в следующее меню.



- 1) Выберите тип настольного считывателя карт.

Примечание: В настоящее время поддерживаемые типы считывателей карт включают в себя: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

- 2) Установите **Serial Port No.** («№ последовательного порта»), **Baud Rate** («скорость передачи в бодах»), **Timeout Value** («значение тайм-аута»), **Buzzing** («звонок») и **Card No. Type** («Тип номера карты»).

Если карта является M1 картой и вам необходимо включить функцию шифрования M1 карт, вы должны поставить галочку **Enable** («Включить») напротив **M1 Card Encryption** («Шифрование карт M1») и нажать **Modify** («Изменить») для выбора сектора.

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

Вы можете нажать кнопку **Restore Default Value** («Восстановить значение по умолчанию») для восстановления настроек по умолчанию.

- **Manually Input** («Ввод вручную»): Введите номер карты и нажмите **Enter** для внесения номера карты.

8. Нажмите **OK** и карта (-ы) будет выдана человеку.
9. (Опционально) Вы можете выбрать добавленную карту и нажать **Modify** («Изменить») или **Delete** («Удалить») для редактирования или удаления карты.
10. (Опционально) Вы можете сгенерировать и сохранить QR-код карты для аутентификации при помощи QR-кода.
 - 1) Выберите добавленную карту и нажмите **QR Code** («QR-код») для генерации QR-кода карты.
 - 2) Во всплывающем окне QR-кода нажмите **Download** («Скачать») для его сохранения на локальном ПК.

Вы можете распечатать QR-код для аутентификации на указанном устройстве.

Примечание: Устройство должно поддерживать функцию аутентификации при помощи QR-кода. Подробнее о настройке функции аутентификации при помощи QR-кода смотрите в руководстве пользователя данного устройства.
11. (Опционально) Вы можете нажать **Link Fingerprint** («Привязать отпечаток пальца») для привязки карты к отпечатку пальца человека, таким образом, человек сможет поместить палец на сканер вместо проводки карты для открытия двери.
12. (Опционально) Вы можете нажать **Link Face Picture** («Привязать изображение лица») для привязки карты к изображению лица человека, таким образом, человек сможет пройти через дверь при помощи сканирования лица вместо проводки карты.
13. Нажмите **OK** для сохранения настроек.

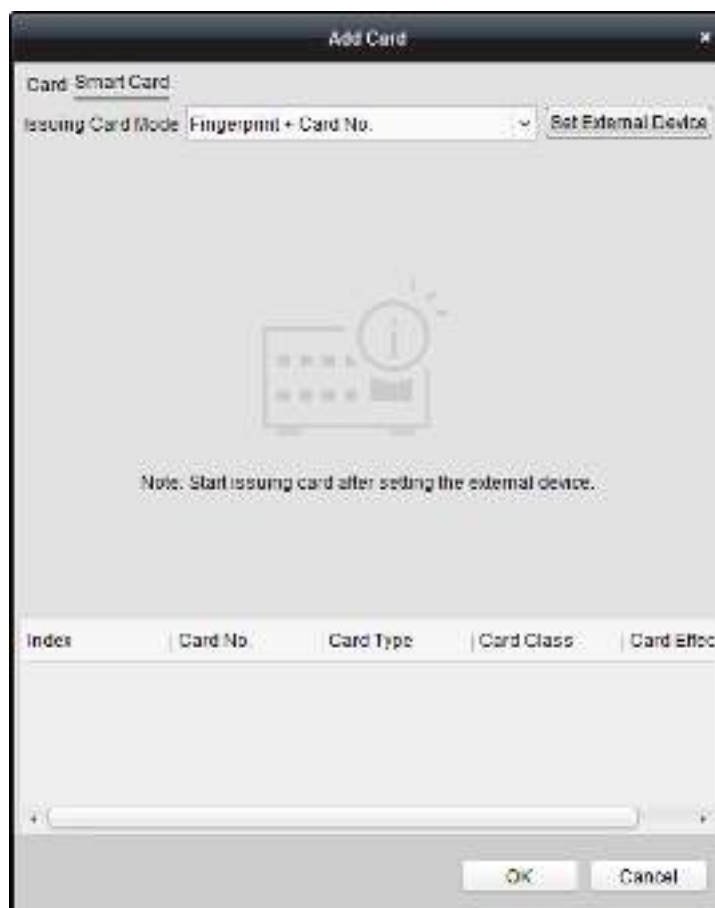
➤ **Добавление смарт карты**

Цель:

Вы можете хранить отпечатки пальцев и информацию ID-карты в смарт карте. При аутентификации после проводки смарт карты через устройство, вы можете отсканировать ваш отпечаток пальца или провести вашей ID-картой через устройство. Устройство сравнит отпечаток пальца или информацию ID-карты в смарт карте с полученными только что. Если вы используете смарт карту для аутентификации, нет необходимости заранее хранить отпечатки пальцев или информацию ID-карты в устройстве.

Шаги:

1. На странице **Add Person** («Добавить человека») установите основную информацию о человеке.
2. Нажмите **Card** («Карта») для перехода на вкладку карт.
3. Нажмите **Add** («Добавить») для появления всплывающего окна добавления карт.
4. Нажмите **Smart Card** («Смарт карта») для перехода на вкладку Смарт карт.



5. Выберите **Issuing Card Mode** («режим выдачи карт») из выпадающего списка.
6. Установите внешнее устройство.
 - 1) Нажмите **Set External Device** («Установить внешнее устройство») для перехода на страницу установки внешнего устройства.
 - 2) (Опционально) Выберите снова **Issuing Card Mode** («режим выдачи карт»).
 - 3) Установите настольный считыватель карт.
 - 4) Если вы выбрали **“Fingerprint + Card No.”** («Отпечаток пальца + № карты») в качестве режима выдачи карт, установите модель регистратора отпечатков пальцев. Если вы выбрали **“ID Card No. + Card No.”** («№ ID карты + № карты») в качестве режима выдачи карт, установите модель считывателя ID карт. Если вы выбрали **“Fingerprint + ID Card No. + Card No.”** («Отпечаток пальца + № ID карты + № карты») в качестве режима выдачи карт, установите модель регистратора отпечатков пальцев и модель считывателя ID карт.
 - 5) Нажмите **OK** для сохранения настроек.
7. Выберите тип для Смарт карты.
 - **Normal Card** («Обычная карта»)
 - **Card for Disabled Person** («Карта для инвалидов»): Дверь останется открытой в течение заданного периода времени для владельца данной карты.
 - **Card in Blacklist** («Карта в черном списке»): Действие проводки карты будет загружено в систему и дверь не будет открыта.

- **Patrol Card** («Патрульная карта»): Действие проводки карты может использоваться для проверки состояния персоналом инспектирования. Разрешения доступа для персонала инспектирования могут быть настроены по вашему усмотрению.
- **Duress Card** («Принудительная карта»): Дверь может быть открыта при помощи проводки принудительной карты. В тоже время клиент создает уведомление о событии принуждения.
- **Super Card** («Супер карта»): Карта действительна для всех дверей контроллера в течение заданного в расписании времени.
- **Visitor Card** («Карта посетителя»): Карта, предназначенная для посетителей. Для карты посетителя вы можете установить параметр **Max. Swipe Times** («Макс. число проводок»).

Примечания:

- Параметр **Max. Swipe Times** («Макс. число проводок») должен быть в промежутке от 0 до 255. При установке значения «0» количество проводок карты не ограничено.
- Может быть добавлено до 3000 карт посетителей.
- **Dismiss Card** («Карта прекращения»): Проведите картой для прекращения тревоги.

8. Установите другие параметры карты.

- 1) Установите пароль карты.
- 2) Установите срок действия карты.
- 3) Отсканируйте свой отпечаток пальца и проведите ID картой в соответствии с приглашением.
- 4) Проведите Смарт картой.

Добавленная информация карты будет отображаться в списке ниже.

9. Нажмите **OK** и карта (-ы) будет выдана человеку.

10. (Опционально) Вы можете выбрать добавленную карту и нажать **Modify** («Изменить») или **Delete** («Удалить») для редактирования или удаления карты.

11. (Опционально) Вы можете сгенерировать и сохранить QR-код карты для аутентификации при помощи QR-кода.

- 1) Выберите добавленную карту и нажмите **QR Code** («QR-код») для генерации QR-кода карты.
- 2) Во всплывающем окне QR-кода нажмите **Download** («Скачать») для его сохранения на локальном ПК.

Вы можете распечатать QR-код для аутентификации на указанном устройстве.

Примечание: Устройство должно поддерживать функцию аутентификации при помощи QR-кода. Подробнее о настройке функции аутентификации при помощи QR-кода смотрите в руководстве пользователя данного устройства.

12. (Опционально) Вы можете нажать **Link Fingerprint** («Привязать отпечаток пальца») для привязки карты к отпечатку пальца человека, таким образом, человек сможет поместить палец на сканер вместо проводки карты для открытия двери.

13. (Опционально) Вы можете нажать **Link Face Picture** («Привязать изображение лица») для привязки карты к изображению лица человека, таким образом, человек сможет пройти через дверь при помощи сканирования лица вместо проводки карты.

14. Нажмите **OK** для сохранения настроек.

Добавление человека (Изображение лиц)

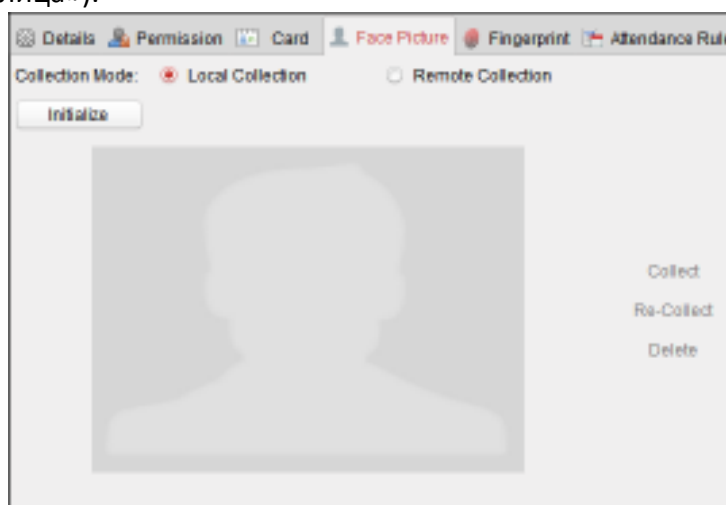
Вы можете собрать изображения лиц двумя способами: **Local Collection** («Локальный сбор») и **Remote Collection** («Удаленный сбор»).

- **Local Collection** («Локальный сбор»): Сбор изображений лиц с помощью сканера изображений лиц.
- **Remote Collection** («Удаленный сбор»): Сбор изображений лиц с помощью терминала контроля доступа.

Примечание: Терминал контроля доступа должен поддерживать функцию распознавания лиц.

Шаги:

1. В меню **Add Person** («Добавление человека») нажмите вкладку **Face Picture** («Изображение лица»).



2. Для получения изображения лица с помощью сканера изображений лиц:
 - 1) Выберите **Local Collection** («Локальный сбор»).
 - 2) Подключите сканер изображений лиц к ПК, на котором запущен клиент.
 - 3) Выберите тип устройства.

Примечание: В настоящее время поддерживается сканер изображений лиц DS2CS5432B-S.

 - 4) (Опционально) Вы можете нажать **Initialize** («Инициализировать») для инициализации сканера изображений лиц.
3. Для получения изображения лица с помощью терминала контроля доступа:
 - 1) Выберите **Remote Collection** («Удаленный сбор»).
 - 2) Нажмите **Select Device** («Выбор устройства») для выбора терминала контроля доступа, который поддерживает функцию распознавания лиц.
4. Нажмите **Collect** («Собрать») для захвата изображения лица.
 Вы можете нажать **Re-Collect** («Повторный сбор») для захвата изображения снова.
 Вы можете нажать **Delete** («Удалить») для удаления захваченного изображения.
5. Нажмите **OK** для сохранения настроек.

Добавление человека (Отпечатки пальцев)

Шаги:

1. В меню добавления человека нажмите вкладку **Fingerprint** («Отпечатки пальцев»).



2. Выберите **Local Collection** («Локальный сбор»).
3. Прежде чем вводить в систему отпечаток пальца, вы должны подключить устройство считывания отпечатков пальцев к ПК и настроить его параметры. Нажмите **Set Fingerprint Machine** («Установить устройство считывания отпечатков пальцев») для перехода в следующее диалоговое окно.



- 1) Выберите **Device Type** («тип устройства»).
В настоящее время поддерживаемые типы устройств считывания отпечатков пальцев: DS-K1F800-F, DS-K1F810-F, DS-K1F820-F и DS-K1F181-F.
- 2) Для устройства считывания отпечатков пальцев типа DS-K1F800-F, вы можете установить **Serial Port No.** («№ последовательного порта»), **Baud Rate** («скорость передачи в бодах») и **Timeout Value** («значение тайм-аута»).
- 3) Нажмите кнопку **Save** («Сохранить») для сохранения настроек.
Вы можете нажать кнопку **Restore Default Value** («Восстановить значение по умолчанию») для восстановления настроек по умолчанию.

Примечания:

- Номер последовательного порта должен соответствовать номеру последовательного порта ПК. Вы можете проверить номер последовательного порта в Диспетчере устройств на ПК.
- Скорость передачи должна устанавливаться в соответствии с внешним устройством считывания отпечатков пальцев. Значение по умолчанию - 19200.
- Поле **Timeout after** («Тайм-аут после») относится ко времени сбора отпечатка пальца.

Если пользователь не вводит отпечаток пальца или неудачно вводит отпечаток пальца, устройство укажет, что сбор отпечатка пальца прекращен.

4. Нажмите кнопку **Start** («Старт») для начала получения отпечатка пальца.
5. Поднимите и приложите необходимый палец к сканеру отпечатков пальцев дважды, чтобы клиент смог получить ваш отпечаток пальца.
6. (Опционально) Вы также можете нажать **Remote Collection** («Удаленный сбор») для получения отпечатков пальцев из устройства.

Примечание: Функция должна поддерживаться устройством.

7. (Опционально) Вы можете выбрать зарегистрированный отпечаток пальцев и нажать кнопку **Delete** («Удалить»).
- Вы можете нажать **Clear** («Очистить») для очистки всех отпечатков пальцев.
8. Нажмите **OK** для сохранения отпечатков пальцев.

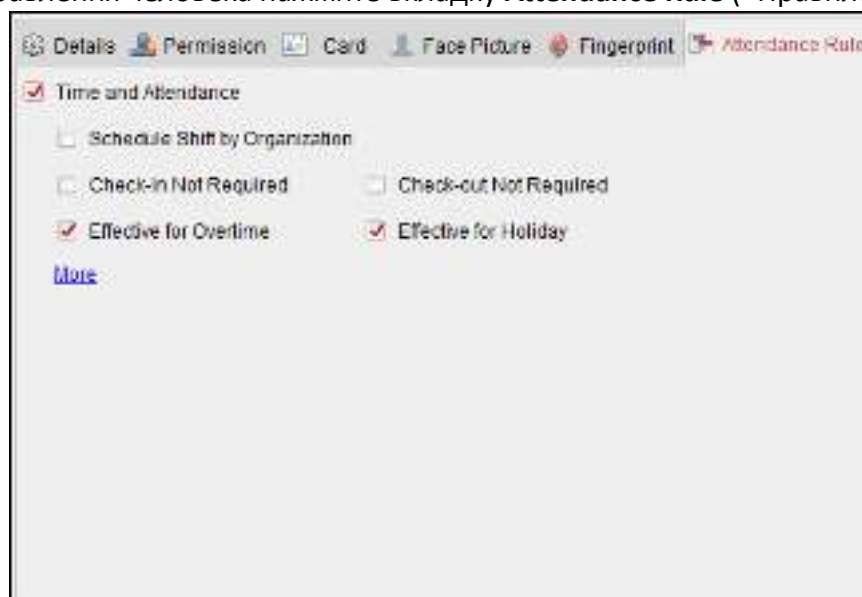
Добавление человека (Правило посещения)

Вы можете установить правило посещения для человека.

Примечание: Эта вкладка будет отображаться, когда вы выбираете режим **Non-residence** («Нежилой комплекс») в сцене приложения при первом запуске программного обеспечения.

Шаги:

1. В меню добавления человека нажмите вкладку **Attendance Rule** («Правило посещения»).



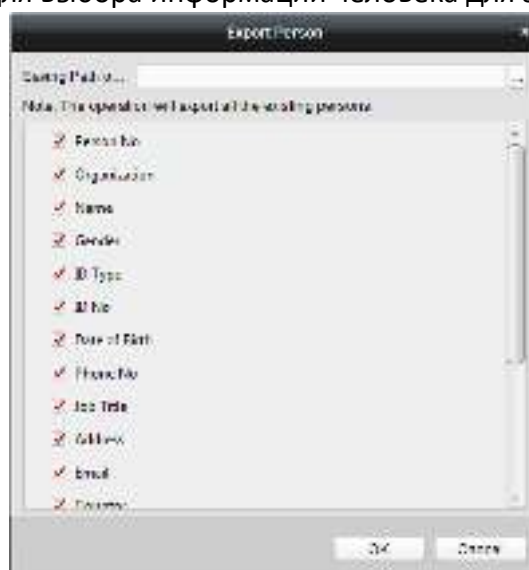
2. Если человека необходимо присоединить ко времени и посещаемости, поставьте галочку **Time and Attendance** («Время и посещаемость») для включения этой функции для человека. Тогда записи проводок карты человека будут сохраняться, и будут анализироваться для учета в посещаемости.
Для получения подробной информации о времени и посещаемости нажмите **More** («Больше») для перехода в модуль **Time and Attendance** («Время и посещаемость»).
3. Нажмите **OK** для сохранения настроек.

Импорт и экспорт информации человека

Информация человека может быть импортирована и экспортирована в пакетном режиме.

Шаги:

1. **Exporting Person** («Экспорт человека»): Вы можете экспортировать информацию добавленных людей в файл в формате Excel на локальный ПК.
 - 1) После добавления человека вы можете нажать кнопку **Exporting Person** («Экспорт человека») на вкладке **Person and Card** («Человек и Карта») для появления следующего всплывающего окна.
 - 2) Нажмите  для выбора пути сохранения экспортируемого Excel файла.
 - 3) Поставьте галочки для выбора информации человека для экспорта.



- 4) Нажмите **OK** для начала экспорта.
2. **Importing Person** («Импорт человека»): Вы можете импортировать Excel файл с информацией о людях в пакетном режиме с локального ПК.
 - 1) Нажмите кнопку **Importing Person** («Импорт человека») на вкладке **Person and Card** («Человек и Карта»).



- 2) Вы можете нажать **Download Template for Importing Person** («Скачать шаблон для импорта человека») для скачивания шаблона.
- 3) Введите информацию человека в скаченный шаблон.
- 4) Нажмите  для выбора Excel файла с информацией человека.
- 5) Нажмите **OK** для начала импорта.

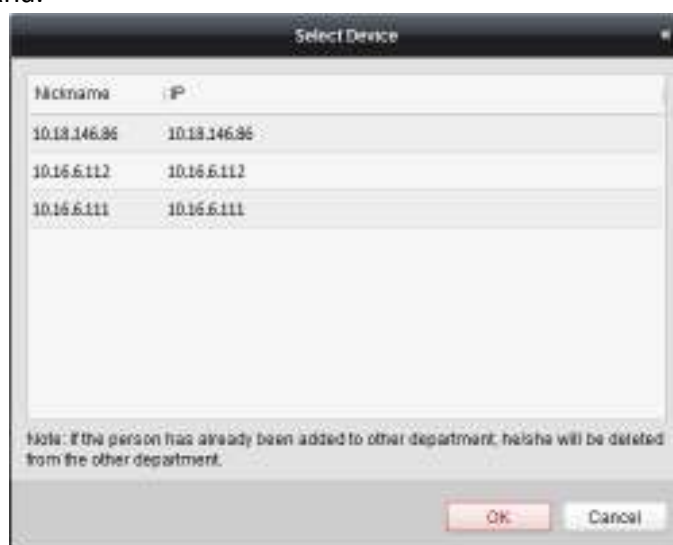
Получение информации о человеке с устройства контроля доступа

Если в добавленном устройстве контроля доступа уже сконфигурирована информация о человеке (включая данные о человеке, отпечаток пальца, информацию о выпущенной карте), вы можете получить эту информацию о пользователе от устройства и импортировать в клиент для дальнейшей работы.

Примечание: Эта функция поддерживается только устройством, методом подключения которого является TCP/IP.

Шаги:

1. В списке организации слева нажмите на организацию, чтобы выбрать ее для импорта людей.
2. Нажмите кнопку **Get Person** («Получить человека») для появления следующего всплывающего окна.



3. Добавленное устройство контроля доступа будет отображено.
4. Щелкните для выбора устройства и нажмите **OK** для начала получения информации о человеке с устройства.
Вы также можете дважды нажать на имя устройства для начала получения информации о человеке.

Примечания:

- Информация о человеке, включая подробные сведения о человеке, данные об отпечатке пальца человека (если он был настроен) и связанная карта (если она настроена), будут импортированы в выбранную организацию.
- Если имя человека, хранящееся на устройстве, не было заполнено изначально, то после импорта в клиент имя человека будет соответствовать номеру выданной карты.
- Пол человека по умолчанию - **Male** («Мужской»).
- Может быть импортировано до 10000 людей.

6.6.2 Управление людьми

Изменение и удаление людей

Для изменения информации человека и его правила посещаемости нажмите  или  в столбце **Operation** («Операция»), или выберите человека и нажмите кнопку **Modify** («Изменить») для открытия диалогового окна редактирования информации человека.

Вы можете нажать  для просмотра записей проводок карты человека.

Для удаления человека, выберите его и нажмите **Delete** («Удалить»).

Примечание: Если карта выдается текущему человеку, привязка будет недействительной после удаления человека.

Перемещение человека в другую организацию

Вы можете переместить человека в другую организацию, если это необходимо.

Шаги:

1. Выберите человека в списке людей и нажмите кнопку **Change Organization** («Сменить организацию»).



2. Выберите организацию, в которую вы хотите переместить человека.
3. Нажмите **OK** для сохранения настроек.

Поиск людей

Вы можете ввести ключевое слово номера карты или имени человека в поле поиска, а затем нажать кнопку **Search** («Поиск») для поиска человека.

Вы можете ввести № карты, нажав кнопку **Read** («Считать») для получения номера карты при помощи подключенного настольного считывателя карт.

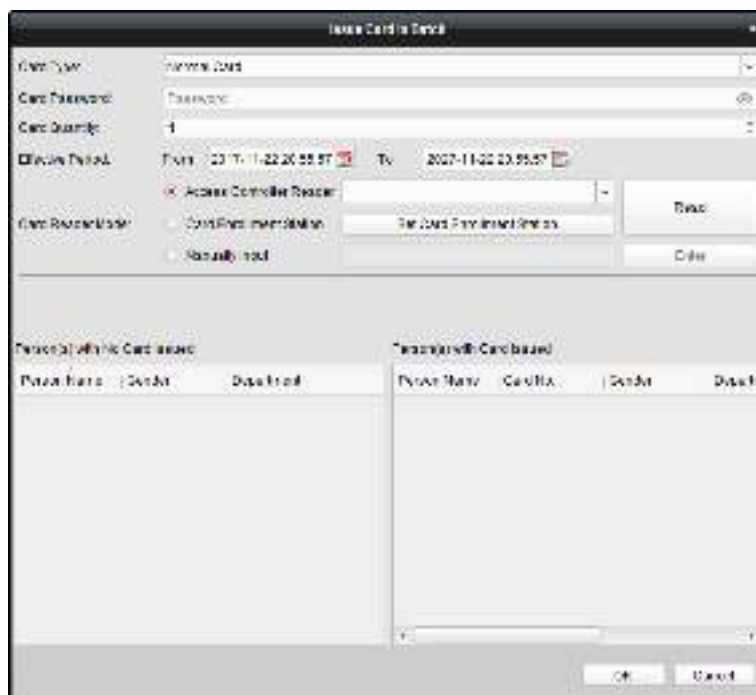
Вы можете нажать **Set Card Enrollment Station** («Установить настольный считыватель карт») для установки параметров настольного считывателя карт.

6.6.3 Выдача карт в пакетном режиме

Вы можете выдавать несколько карт для лица, у которого нет карты.

Шаги:

1. Нажмите кнопку **Issue Card in Batch** («Пакетная выдача карт») для перехода в следующее меню.
Все добавленные люди, которым не были выданы карты, будут отображены в списке **Person(s) with No Card Issued** («Люди, которым не выданы карты»).



2. Выберите **Card Type** («тип карты») по вашему усмотрению.

Примечание: Для получения подробной информации о типах карт, обратитесь к разделу *Добавление людей*.

3. Введите пароль от самой карты в поле **Card Password** («Пароль карты»). Пароль карты должен содержать от 4 до 8 цифр.

Примечание: Пароль будет необходим, когда держатель карты проведет картой для входа или выхода через дверь, если включены такие режимы аутентификации считывателя карт как **Card and Password** («Карта и Пароль»), **Password and Fingerprint** («Пароль и Отпечаток пальца»), **Card** («Карта»), **Password** («Пароль») и **Fingerprint** («Отпечаток пальца»). Для получения подробной информации смотрите *Раздел Ошибка! Источник ссылки не найден. Ошибка! Источник ссылки не найден..*

4. Введите количество карт, выданных для каждого человека.
Например, если **Card Quantity** («Количество карт») равно 3, вы можете считать номера трех карт или ввести их вручную для каждого человека.
5. Нажмите  для установки времени действия и истечения действия карты.
6. В списке **Person(s) with No Card Issued** («Люди, которым не выданы карты») слева выберите человека, которому необходимо выдать карту.

Примечание: Вы можете нажать на заголовок столбцов **Person Name** («Имя человека»), **Gender** («Пол») или **Department** («Отдел») для сортировки людей по соответствующему параметру.

7. Выберите **Card Reader Mode** («Режим считывателя карт») для считывания номера карты.
 - **Access Controller Reader** («Считыватель карт контроллера доступа»): Поместите карту на считыватель контроллера доступа и нажмите **Read** («Считать») для получения номера карты.
 - **Card Enrollment Station** («Настольный считыватель карт»): Поместите карту на настольный считыватель карт и нажмите **Read** («Считать») для получения номера

карты.

Примечание: Настольный считыватель карт должен быть подключен к ПК с запущенным клиентом. Вы можете нажать **Set Card Enrollment Station** («Установить настольный считыватель карт») для перехода в следующее меню.



- 1) Выберите тип настольного считывателя карт.

Примечание: В настоящее время поддерживаемые типы считывателей карт включают в себя: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

- 2) Установите параметры для подключенного настольного считывателя карт.

Если карта является M1 картой и вам необходимо включить функцию шифрования M1 карт, вы должны поставить галочку **Enable** («Включить») напротив **M1 Card Encryption** («Шифрование карт M1») и нажать **Modify** («Изменить») для выбора сектора.

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

Вы можете нажать кнопку **Restore Default Value** («Восстановить значение по умолчанию») для восстановления значений по умолчанию.

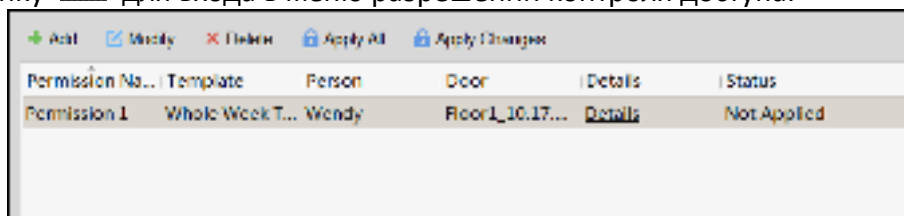
- **Manually Input** («Ввод вручную»): Введите номер карты и нажмите **Enter** для внесения номера карты.

8. После выдачи карты человеку информация о нем и о карте будет отображаться в списке **Person(s) with Card Issued** («Люди, которым выданы карты»).
9. Нажмите **OK** для сохранения настроек.

6.7 Конфигурация разрешений

В модуле конфигурации разрешений вы можете добавлять, изменять и удалять разрешения контроля доступа, и затем применять настройки разрешений к устройству.

Нажмите иконку для входа в меню разрешений контроля доступа.



6.7.1 Добавление разрешений

Цель:

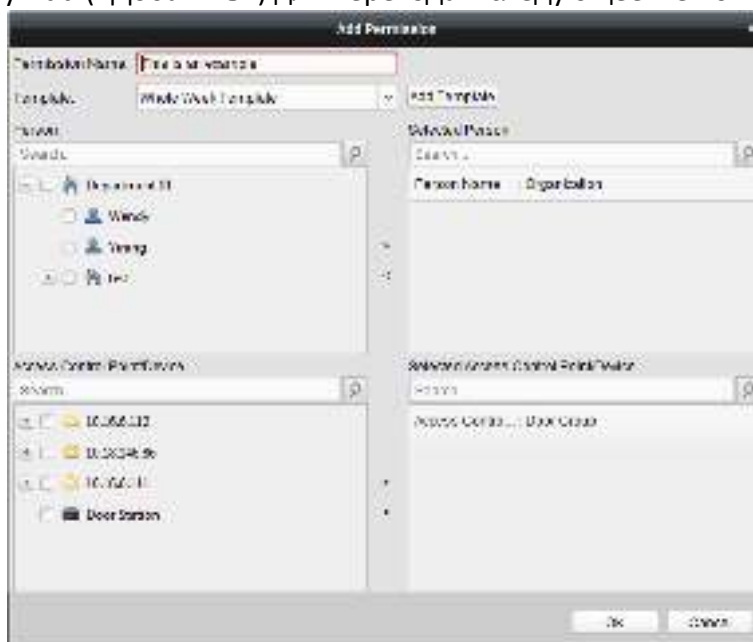
Вы можете назначать разрешения для людей на вход/выход через контрольные точки (двери) в этой секции.

Примечания:

- Вы можете добавить до 4 разрешений на одну контрольную точку доступа на одном устройстве.
- Вы можете добавить до 128 разрешений всего.

Шагу:

1. Нажмите иконку **Add** («Добавить») для перехода в следующее меню.



- В поле **Permission Name** («Имя разрешения») введите имя для разрешения по вашему желанию.
- Нажмите на выпадающий список в поле **Template** («шаблон») для выбора шаблона для разрешения.

Примечание: Вы должны настроить шаблон перед конфигурацией разрешений. Вы можете нажать кнопку **Add Template** («Добавить шаблон») для добавления шаблона.

4. В поле **Person List** («Список людей») отображаются все добавленные люди. Поставьте галочки для выбора людей и нажмите «>» для добавления в список **Selected Person** («Выбранные люди»).
(Опционально) Вы можете выбрать человека в списке **Selected Person** («Выбранные люди») и нажать «<» для отмены выбора человека.
5. В списке **Access Control Point/Device** («Точка контроля доступа/Устройство») будут отображены все добавленные точки контроля доступа (двери) и вызывные панели. Поставьте галочки для выбора дверей или вызывных панелей нажмите «>» для добавления в список выбранных устройств.
(Опционально) Вы можете выбрать дверь или вызывную панель в списке выбранных устройств и нажать «<» для отмены выбора.
6. Нажмите кнопку **OK** для завершения добавления разрешений. Выбранные люди будут иметь разрешения на вход/выход через выбранные двери/вызывные панели при помощи привязанных карт или отпечатков пальцев.
7. (Опционально) После добавления разрешения, вы можете нажать **Details** («Детали») просмотра деталей. Или вы можете выбрать разрешение и нажать **Modify** («Изменить») для изменения.
Вы можете выбрать добавленное разрешение из списка и нажать **Delete** («Удалить») для его удаления.

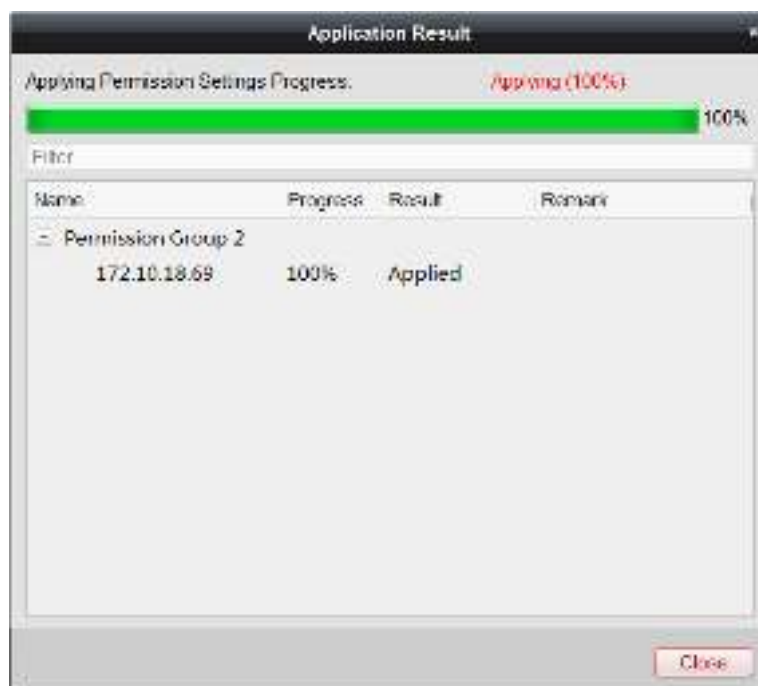
6.7.2 Применение разрешений

Цель:

После конфигурации разрешений вы должны применить добавленные разрешения к устройствам контроля доступа.

Шаги:

1. Выберите разрешения, которые вы хотите применить к устройству контроля доступа.
Для выбора нескольких разрешений вы можете удерживать кнопки *Ctrl* или *Shift*.
2. Нажмите **Apply All** («Применить все») для начала применения всех выбранных разрешений к устройству контроля доступа или вызывной панели.
Вы можете также нажать **Apply Changes** («Применить изменения») для применения измененной части выбранных разрешений к устройству.
3. Появится следующее всплывающее окно, показывающее результат применения разрешений.

**Примечания:**

- Когда настройки разрешений будут изменены, появится следующий экран с подсказками.



Вы можете нажать **Apply Now** («Применить сейчас») для применения измененных разрешений к устройству.

Или вы можете нажать **Apply Later** («Применить позже») для того, чтобы применить изменения позже в меню разрешений.

- Изменения разрешений включают в себя изменения расписания и шаблона, настроек разрешений, настроек разрешений людей и настроек связанных людей (включая № карты, отпечатки пальцев, изображения лиц, связь между № карты и отпечатком пальцев, пароль карты, срок действия карты и др.).

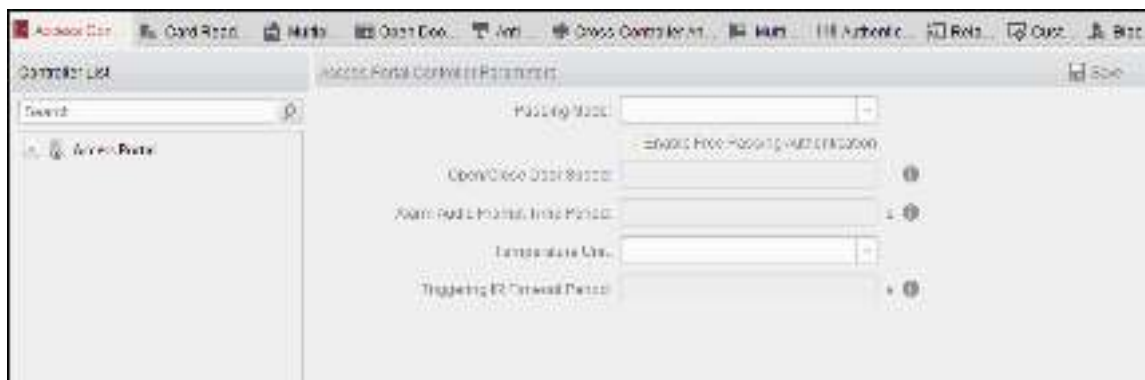
6.8 Расширенные функции

Цель:

После конфигурации людей, шаблонов, разрешений контроля доступа, вы можете настроить расширенные функции контроля доступа, такие как параметры контроля доступа, пароль аутентификации, открытие двери при помощи первой карты, запрет обратного прохода и т.д.

Примечание: Расширенные функции должны поддерживаться устройством.

Нажмите иконку  для перехода в следующее меню.



6.8.1 Параметры контроля доступа

Цель:

После добавления устройства контроля доступа вы можете настроить параметры его точки контроля доступа (двери) и параметры его считывателя карт.

Нажмите вкладку **Access Control Parameters** («Параметры контроля доступа») для перехода в меню настройки параметров.

Параметры двери

Шаги:

1. В области **Controller List** («список контроллеров») слева нажмите , чтобы развернуть устройство контроля доступа, выберите дверь (точку контроля доступа), и вы сможете изменить информацию выбранной двери справа.



2. Вы можете настроить следующие параметры:
 - **Door Magnetic** («Магнитная дверь»): Магнитная дверь находится в состоянии **Remain Closed** («Оставить закрытой») (Исключая особые условия).
 - **Exit Button Type** («Тип кнопки выхода»): Кнопка выхода находится в состоянии **Remain Open** («Оставить открытой») (Исключая особые условия).
 - **Door Locked Time(s)** («Время блокировки двери (с)»): После проводки обычной карты или действия реле, таймер для блокировки двери начнет работу.
 - **Door Open Timeout Alarm** («Тревога тайм-аута открытого состояния двери»): Может быть запущена тревога, если дверь не была закрыта.
 - **Enable Locking Door when Door Closed** («Включить блокировку двери при закрытии

двери»): Дверь может быть заблокирована после закрытия, даже если время блокировки двери не достигнуто.

- **Duress Code** («Принудительный код»): Дверь может быть открыта при помощи ввода принудительного кода. В тоже время клиент может сообщить о принудительном событии.
- **Super Password** («Супер пароль»): Конкретный человек может открыть дверь, введя супер пароль.
- **Dismiss Code** («Код отклонения»): Введите код отклонения, чтобы остановить зуммер считывателя карт.

Примечания:

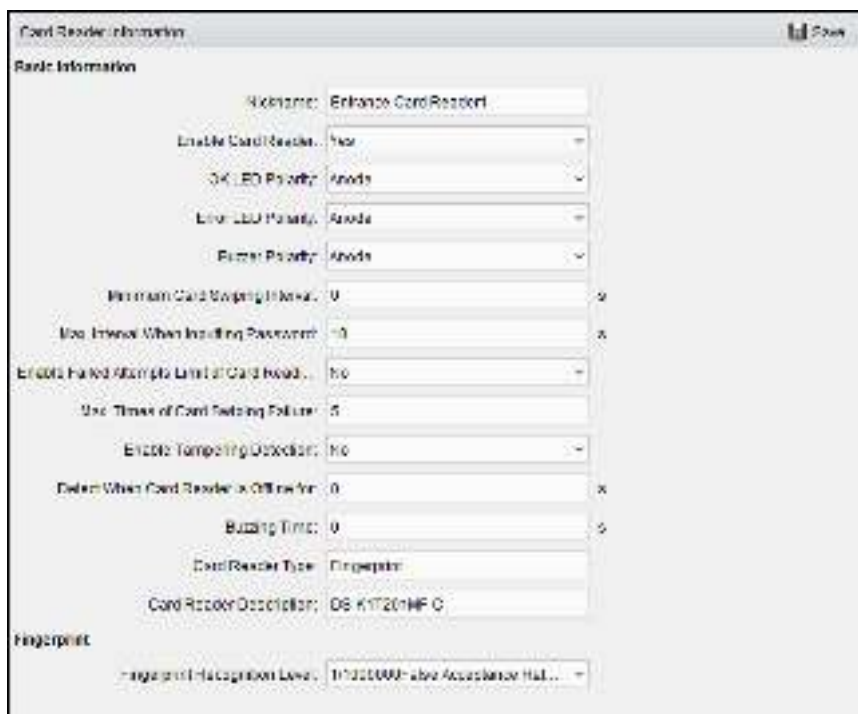
- Принудительный код, супер пароль и код отклонения должны быть разными.
- Принудительный код, супер пароль и код отклонения должны отличаться от пароля аутентификации.
- Принудительный код, супер пароль и код отклонения должны содержать от 4 до 8 цифр.

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

Параметры считывателя карт

Шаги:

1. В списке устройств слева нажмите , чтобы развернуть дверь, выберите имя считывателя карт, а затем вы сможете изменить информацию выбранного считывателя карт справа.



The screenshot shows a configuration window titled 'Card Reader Information'. It contains two main sections: 'Basic Information' and 'Fingerprint'. The 'Basic Information' section includes fields for 'Nickname' (set to 'Entrance Card Reader'), 'Enable Card Reader' (set to 'Yes'), 'OK LED Priority' (set to 'Anode'), 'Error LED Priority' (set to 'Anode'), 'Buzzer Priority' (set to 'Anode'), 'Minimum Card Swiping Interval' (set to '0'), 'Max. Interval When Issuing Password' (set to '10'), 'Enable Failed Attempts Limit of Card Reader' (set to 'No'), 'Use Times of Card Swiping Failure' (set to '5'), 'Enable Tampering Detection' (set to 'No'), 'Detect When Card Reader is Offline for' (set to '0'), 'Buzzer Time' (set to '0'), 'Card Reader Type' (set to 'Fingerprint'), and 'Card Reader Description' (set to 'DS-K1T201MF-C'). The 'Fingerprint' section includes a 'Fingerprint Recognition Level' (set to '1:1024000: also Acceptance Rate...').

2. Вы можете изменить следующие параметры:

- **Nickname** («Название»): Измените имя считывателя карт по вашему усмотрению.
- **Enable Card Reader** («Включить считыватель карт»): Выберите **Yes** («Да») для включения считывателя карт.

- **OK LED Polarity** («Полярность светодиода ОК»): Выберите полярность светодиода ОК для системной платы считывателя карт.
- **Error LED Polarity** («Полярность светодиода ошибки»): Выберите полярность светодиода ошибки для системной платы считывателя карт.
- **Buzzer Polarity** («Полярность зуммера»): Выберите полярность зуммера для системной платы считывателя карт.
- **Minimum Card Swiping Interval** («Минимальный интервал проводки карты»): Если интервал между проводками одной и той же карты меньше установленного значения, проводка карты недействительна. Вы можете установить значение от 0 до 255.
- **Max. Interval When Inputting Password** («Макс. интервал ввода пароля»): При вводе пароля в устройство считывания карт, если интервал между нажатием двух цифр больше установленного значения, цифры, которые вы нажали до этого, будут автоматически сброшены.
- **Enable Failed Attempts Limit of Card Reading** («Включить ограничение неудачных попыток считывания карты»): Включить отправку сообщения о тревоге, когда количество попыток считывания карты достигает установленного значения.
- **Max. Times of Card Swiping Failure** («Макс. число неудачных считываний карты»): Установите максимальное количество неудачных попыток считывания карты.
- **Enable Tampering Detection** («Включить детекцию тамперинга»): Включить детекцию тамперинга для считывателя карт.
- **Detect When Card Reader is Offline for** («Детекция офлайн состояния считывателя карт»): Когда устройство контроля доступа не может подключиться к считывателю карт дольше, чем установленное время, считыватель карт перейдет в офлайн состояние автоматически.
- **Buzzing Time** («Время работы зуммера»): Установите время работы зуммера считывателя карт. Доступное время составляет от 0 до 5999 секунд. 0 - непрерывный звон.
- **Card Reader Type** («Тип считывателя карт»): Получить тип считывателя карт.
- **Card Reader Description** («Описание считывателя карт»): Получить описание считывателя карт.
- **Fingerprint Recognition Level** («Уровень распознавания отпечатков пальцев»): Выберите уровень распознавания отпечатков пальцев из выпадающего списка. По умолчанию значение **Low** («Низкий»).

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

Параметры контроллера прохода

Шаги:

1. В списке устройств слева нажмите , чтобы развернуть дверь, выберите контроллер прохода, а затем вы сможете изменить параметры контроллера прохода на панели справа.



2. Вы можете изменить следующие параметры:

- **Passing Mode** («Режим прохода»): Выберите контроллер, который будет контролировать состояние турникета.

Если выбрано значение **According to Lane Controller's DIP Settings** («В соответствии с настройками DIP-переключателей контроллера прохода»), устройство будет следовать настройкам DIP-переключателей контроллера прохода для управления турникетом. Настройки в ПО системы будут недействительны.

Если выбрано значение **According to Main Controller's Settings** («В соответствии с настройками главного контроллера»), устройство будет следовать настройкам ПО системы для управления турникетом. Настройки DIP-переключателей контроллера прохода будут недействительны.

Примечание: Для получения подробной информации об установке состояния турникета смотрите *Раздел Ошибка! Источник ссылки не найден. Ошибка! Источник ссылки не найден.*

- **Enable Free Passing Authentication** («Включить аутентификацию при свободном проходе»): Если установлена галочка в этом поле, то когда в качестве режима входного и выходного турникетов установлено значение **Remain Open** («Оставить открытым»), пешеходы должны будут проходить аутентификацию каждый раз, когда проходят через турникет. Иначе будет запущена тревога.
- **Open/Close Door Speed** («Скорость открытия/закрытия двери»): Установите скорость открытия и закрытия прохода. Вы можете выбрать значение от 1 до 10. Чем больше значение, тем выше скорость.

Примечание: Рекомендуемое значение - 6.

- **Alarm Audio Prompt Time Duration** («Длительность звукового уведомления о тревоге»): Установите продолжительность воспроизведения звукового уведомления о тревоге.

Примечание: «0» обозначает, что звуковое уведомление о тревоге будет воспроизводиться до тех пор, пока тревога не закончится.

- **Temperature Unit** («Единица измерения температуры»): Выберите единицу измерения температуры, которая отображается в поле состояния устройства.

Примечание: Для получения информации о просмотре состояния устройства смотрите *Раздел Ошибка! Источник ссылки не найден. Просмотр состояния устройства.*

3. Нажмите **Save** («Сохранить») для сохранения параметров контроллера прохода.

6.8.2 Аутентификация считывателя карт

Цель:

Вы можете установить правила прохода для считывателя карт устройства контроля доступа.

Шаги:

1. Нажмите вкладку **Card Reader Authentication** («Аутентификация считывателя карт») и выберите считыватель карт слева.
2. Нажмите кнопку **Configuration** («Конфигурация») для выбора режимов аутентификации считывателя карт для настройки расписания.

Примечания:

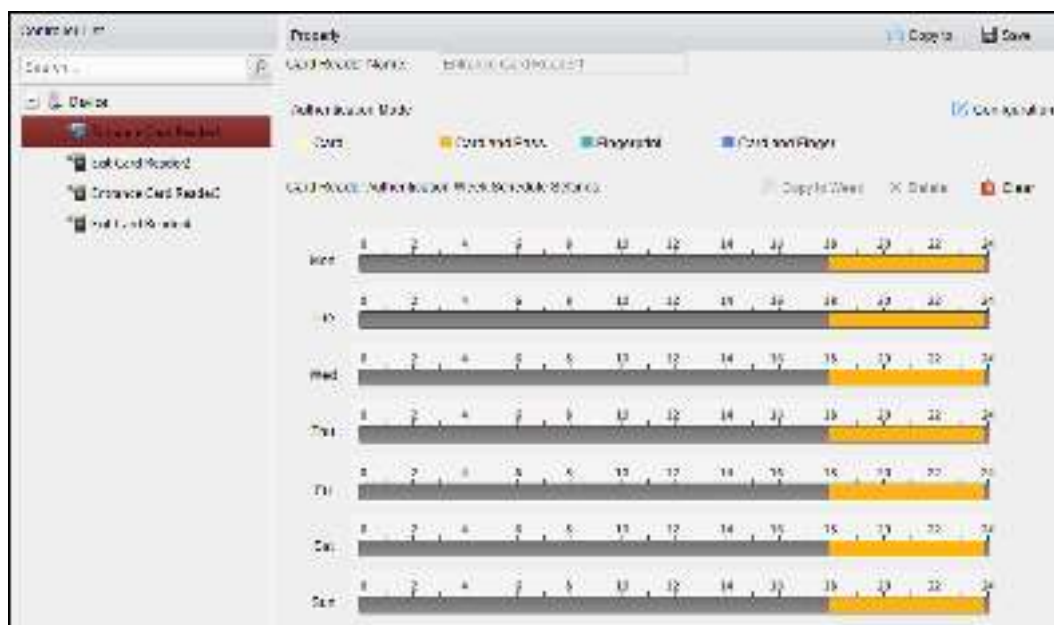
- Доступные режимы аутентификации зависят от типа устройства.
- Пароль относится к паролю карты, установленному при выдаче карты человеку, подробности смотрите в *Разделе **Ошибка! Источник ссылки не найден. Управление людьми.***

- 1) Выбирайте режимы в поле слева и нажимайте  для добавления в список выбранных режимов.

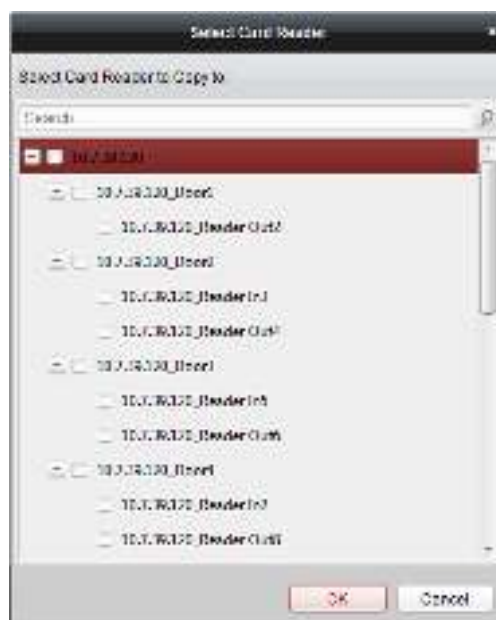
Вы можете нажимать иконки  или  для регулировки порядка отображения.



- 2) Нажмите **OK** для подтверждения выбора.
3. После выбора режимов, они будут отображены в виде иконок. Нажмите на иконку для выбора режима аутентификации считывателя карт.
4. Нажмите и потяните указатель мыши вдоль одного дня, чтобы нарисовать цветную полосу в расписании, что означает, что в этот период времени аутентификация считывателя карт действительна.



5. Повторите вышеуказанные шаги, чтобы установить другие периоды времени.
Или вы можете выбрать сконфигурированный день и нажать кнопку **Copy to Week** («Копировать на неделю») для копирования всех настроек на другие дни целой недели.
(Опционально) Вы можете нажать кнопку **Delete** («Удалить») для удаления выбранного периода времени или нажать кнопку **Clear** («Очистить») для удаления всех настроенных периодов времени.
6. (Опционально) Нажмите кнопку **Copy to** («Копировать в») для копирования настроек в другие считыватели карт.



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

6.8.3 Многократная аутентификация

Цель:

Вы можете управлять картами по группам и устанавливать аутентификацию для нескольких карт для одной точки контроля доступа (двери).

Примечание: Пожалуйста, установите разрешения карты и примените настройки разрешений к устройству контроля доступа. Для получения подробной информации смотрите *Раздел **Ошибка! Источник ссылки не найден.** Конфигурация разрешений.*

Шаги:

1. Нажмите вкладку **Multiple Authentication** («Многократная аутентификация») для перехода в соответствующее меню.



2. Выберите устройство контроля доступа из списка слева.
3. На панели **Set Card Group** («Установка группы карт») нажмите кнопку **Add** («Добавить») для появления следующего всплывающего окна:



- 1) В поле **Card Group Name** («Имя группы карт») введите имя для группы карт по вашему усмотрению.
- 2) Нажмите  для установки времени начала действия и окончания действия группы карт.
- 3) Поставьте галочки для выбора карт, которые вы хотите добавить в группу карт.
- 4) Нажмите **OK** для сохранения группы карт.
4. На панели **Set Authentication Group** («Установка группы аутентификации») выберите точку контроля доступа (дверь) устройства для множественной аутентификации.
5. Введите **Time Interval** («интервал времени») для проводок карт.
6. Нажмите **Add** («Добавить») для появления следующего всплывающего окна.



- 1) Выберите **Template** («шаблон») для группы аутентификации из выпадающего списка.
- 2) Выберите **Authentication Type** («тип аутентификации») для группы аутентификации из выпадающего списка.

- **Local Authentication** («Локальная аутентификация»): Аутентификация устройством контроля доступа.
- **Local Authentication and Remotely Open Door** («Локальная аутентификация и удаленное открытие двери»): Аутентификация устройством контроля доступа и клиентом.

Для типа **Local Authentication and Remotely Open Door** («Локальная аутентификация и удаленное открытие двери») вы можете поставить галочку для включения аутентификации по супер паролю, когда устройство контроля доступа отключено от клиента.

- **Local Authentication and Super Password** («Локальная аутентификация и супер пароль»): Аутентификация устройством контроля доступа и супер паролем.
- 3) В списке слева появится добавленная группа карт. Вы можете нажать на группу карт и нажать **+** для добавления группы в группу аутентификации.

Вы можете нажать на добавленную группу карт и нажать **X** для удаления ее из группы аутентификации.

Вы также можете нажимать кнопку **+** или **↓** для установки порядка проводок карт.

- 4) Введите **Card Swiping Times** («Число проводок карт») для выбранной группы карт.

Примечания:

- **Card Swiping Times** («Число проводок карт») должно быть больше 0 и меньше количества добавленных карт в группе карт.
- Верхний предел числа проводок карт - 16.

5) Нажмите **OK** для сохранения настроек.

7. Нажмите **Save** («Сохранить») для сохранения и вступления в силу настроек.

Примечания:

- Для каждой точки контроля доступа (двери) может быть добавлено до 20 групп аутентификации.
- Для группы аутентификации, тип сертификата которой **Local Authentication** («Локальная аутентификация»), в группу аутентификации можно добавить до 8 групп карт.
- Для группы аутентификации, тип сертификата которой является **Local Authentication and Super Password** («Локальная аутентификация и супер пароль») или **Local Authentication and Remotely Open Door** («Локальная аутентификация и удаленное открытие двери»), в группу аутентификации можно добавить до 7 групп карт.

6.8.4 Открытие двери при помощи первой карты

Цель:

Вы можете установить несколько первых карт для одной контрольной точки доступа. После проводки первой карты, разрешается доступ к двери другим людям или другие действия аутентификации. Режимы первой карты: **Remain Open with First Card** («Оставить открытой после проводки первой карты»), **Disable Remain Open with First Card** («Отключить открытое состояние запущенное первой картой») и **First Card Authorization** («Авторизация первой карты»).

- **Remain Open with First Card** («Оставить открытой после проводки первой карты»): Дверь остается открытой в течение заданной продолжительности времени после проводки первой карты до тех пор, пока не закончится продолжительность открытого состояния.
- **Disable Remain Open with First Card** («Отключить открытое состояние запущенное первой картой»): Отключение функции.
- **First Card Authorization** («Авторизация первой карты»): Все аутентификации (кроме аутентификации супер карты, супер пароля, принудительной карты и принудительного пароля) разрешены только после авторизации первой карты.

Примечания:

- Авторизация первой карты действует только в текущий день. Срок действия разрешения истекает после 24:00 в текущий день.
- Вы можете провести первой картой снова, чтобы отключить режим первой карты.

Шаги:

1. Нажмите вкладку **Open Door with First Card** («Открыть дверь при помощи первой карты») для перехода в соответствующее меню.



2. Выберите устройство контроля доступа из списка слева.
3. Выберите **First Card Mode** («режим первой карты») из выпадающего списка для контрольной точки доступа.
4. (Опционально) Если вы выбрали значение **Remain Open with First Card** («Оставить открытой после проводки первой карты») вы должны установить длительность открытого состояния.

Примечания:

- **Remain Open Duration** («Длительность открытого состояния») должна быть от 0 до 1440 минут. По умолчанию это 10 минут.
 - Вы можете провести первой картой снова, чтобы отключить режим первой карты.
5. В области **First Card List** («Список первых карт») нажмите **Add** («Добавить») для появления следующего всплывающего окна.



- 1) Выберите карты для добавления в качестве первых карт для двери.

Примечание: Установите разрешения карты и примените настройки разрешения к устройству контроля доступа. Для получения подробной информации смотрите Раздел **Ошибка! Источник ссылки не найден. Конфигурация разрешений.**

- 2) Нажмите кнопку **OK** для подтверждения добавления карты.
6. Вы можете нажать кнопку **Delete** («Удалить») для удаления карты из списка первых карт.
7. Нажмите **Save** («Сохранить») для сохранения и вступления в силу настроек.

6.8.5 Запрет обратного прохода

Цель:

Вы можете установить только проход в одном направлении через контрольную точку в соответствии с заданным путем, и только один человек может пройти контрольную точку доступа после проводки карты.

Примечания:

- Можно одновременно настроить функцию защиты от обратного прохода или функцию многодверной блокировки для устройства контроля доступа.
- В первую очередь вы должны включить функцию запрета обратного прохода на устройстве контроля доступа.

Шаги:

1. Нажмите вкладку **Anti-passing Back** («Запрет обратного прохода») для перехода в соответствующее меню.



2. Выберите устройство контроля доступа из списка устройств слева.
3. В поле **First Card Reader** («Первый считыватель карт») выберите считыватель карт в качестве начала пути.
4. В списке нажмите на текстовое поле **Card Reader Afterward** («Последующий считыватель карт») и выберите связанные считыватели карт.

Пример: Если выбрали *Reader In_01* в качестве начального считывателя карт и выбрали *Reader In_02*, *Reader Out_04* в качестве связанных считывателей карт, тогда вы можете пройти через контрольную точку доступа, выполнив проводку карты в порядке: *Reader In_01*, *Reader In_02* и *Reader Out_04*.



Примечание: До четырех последующих считывателей карт можно добавить для одного считывателя карт.

5. (Опционально) Вы можете снова войти в диалоговое окно **Select Card Reader** («Выбор считывателя карт»), чтобы изменить его считыватели.
6. Нажмите **Save** («Сохранить») для сохранения и вступления в силу настроек.

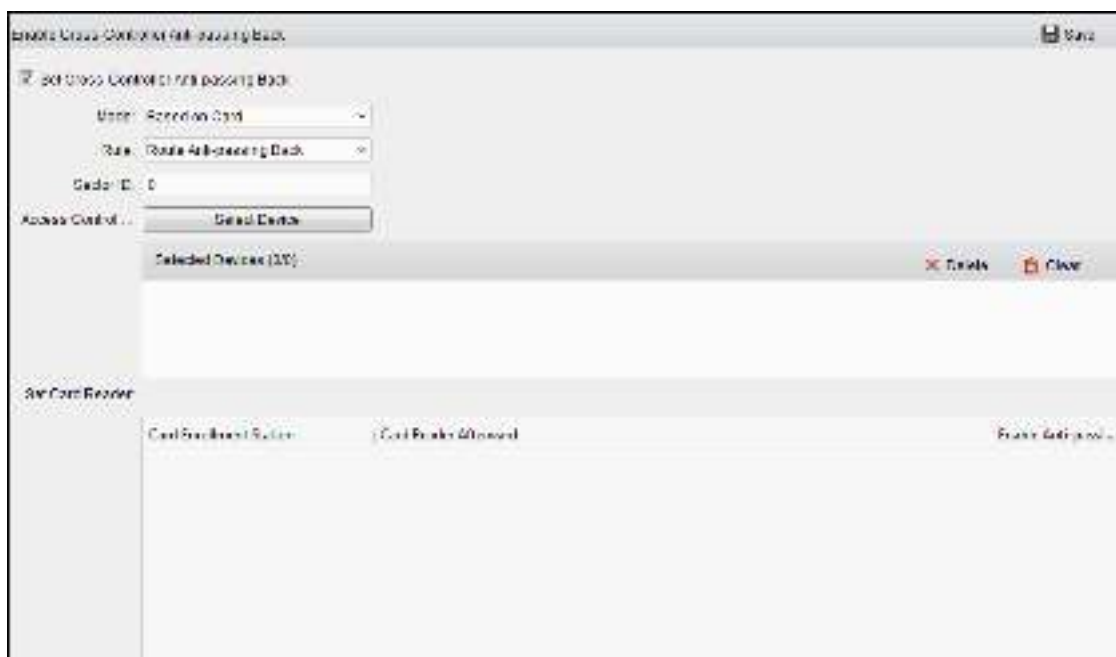
6.8.6 Межконтроллерный запрет обратного прохода

Цель:

Вы можете установить запрет обратного прохода для считывателей карт в нескольких устройствах контроля доступа. Вы должны выполнять считывания карты в соответствии с настроенным маршрутом проводок карт. И только один человек может пройти через точку контроля доступа после проводки карты.

Примечание: Функция должна поддерживаться устройством.

Нажмите **Cross-Controller Anti-passing Back** («Межконтроллерный запрет обратного прохода») для перехода соответствующее меню.



Настройка маршрута для запрета обратного прохода

Цель:

Маршрут запрета обратного прохода зависит от маршрута считывания карты. Вы должны установить первый считыватель карт и последующие считыватели карт.

Шаги:

1. Поставьте галочку **Enable Cross-Controller Anti-passing Back** («Включить межконтроллерный запрет обратного прохода») для включения соответствующей функции.
2. Задайте параметры запрета обратного прохода.

➤ На основе карты

Примечание: Система будет оценивать необходимость срабатывания запрета обратного прохода в соответствии с записями входа и выхода на карте.

- 1) Выберите **Based on Card** («На основе карты») из выпадающего списка в поле **Anti-passing Back Mode** («режим запрета обратного прохода»).
- 2) Выберите **Route Anti-passing Back** («Маршрут запрета обратного прохода») в поле **Rule** («Правило»).
- 3) Задайте значение **Sector ID** («ID сектора»).
- 4) Нажмите **Select Access Controller** («Выбрать контроллер доступа») для выбора устройства во всплывающем окне.
- 5) В области **Card Reader** («Считыватель карт») нажмите на иконку слева от колонки считывателя карт для выбора первого считывателя карт. Иконка сменится на .
- 6) Нажмите на поле **Card Reader Afterward** («Последующий считыватель карт») для выбора последующих считывателей карт во всплывающем окне.
- 7) Поставьте галочку в столбце **Enable Anti-passing Back** («Включить запрет обратного прохода») для включения функции запрета обратного прохода.

Примечания:

- Отображаемые считыватели карт в поле **Card Reader Afterward** («Последующий считыватель карт») должны быть расположены в порядке аутентификации.
- Может быть добавлено до 64 устройств с функцией запрета обратного прохода.
- Для каждого считывателя карт может быть добавлено до 16 последующих считывателей карт.
- В настоящее время поддерживается карта M1, и сектор не может быть зашифрован.

➤ **На основе сети**

Примечание: Оценка необходимости срабатывания запрета обратного прохода в соответствии с информацией о входе и выходе в считывателе карт.

- 1) Выберите **Based on Network** («На основе сети») из выпадающего списка в поле **Anti-passing Back Mode** («режим запрета обратного прохода»).
- 2) Выберите **Route Anti-passing Back** («Маршрут запрета обратного прохода») в поле **Rule** («Правило»).
- 3) Выберите сервер из выпадающего списка для оценки необходимости срабатывания запрета обратного прохода.
- 4) (Опционально) Вы можете нажать **Delete Record** («Удалить запись») и выбрать карту во всплывающем окне для удаления информации о проводках карты на всех устройствах.
Пользователь должен снова начать выполнять проводки карты с первого считывателя карт.
- 5) Нажмите **Select Access Controller** («Выбрать контроллер доступа») для выбора устройства во всплывающем окне.
- 6) В области **Card Reader** («Считыватель карт») нажмите на иконку слева от колонки считывателя карт для выбора первого считывателя карт. Иконка сменится на .
- 7) Нажмите на поле **Card Reader Afterward** («Последующий считыватель карт») для выбора последующих считывателей карт во всплывающем окне.
- 8) Поставьте галочку в столбце **Enable Anti-passing Back** («Включить запрет обратного прохода») для включения функции запрета обратного прохода.

Примечания:

- Отображаемые считыватели карт в поле **Card Reader Afterward** («Последующий считыватель карт») должны быть расположены в порядке аутентификации.
- Может быть добавлено до 64 устройств с функцией запрета обратного прохода.
- Для каждого считывателя карт может быть добавлено до 16 последующих считывателей карт.
- На выбранном сервере может быть сохранено до 5000 записей проводок карт.

Настройка запрета обратного прохода для входа/выхода

Цель:

Вы можете настроить считыватель карт на входе и считыватель карт на выходе таким образом, чтобы они были предназначены только для входа и выхода соответственно, без настройки первого считывателя карт и последующего считывателя карт.

Шаги:

1. Во вкладке **Cross-Controller Anti-passing Back** («Межконтроллерный запрет обратного прохода») поставьте галочку **Enable Cross-Controller Anti-passing Back** («Включить межконтроллерный запрет обратного прохода») для включения соответствующей функции.
2. Задайте параметры запрета обратного прохода.

➤ На основе карты

Примечание: Система будет оценивать необходимость срабатывания запрета обратного прохода в соответствии с записями входа и выхода на карте.

- 1) Выберите **Based on Card** («На основе карты») из выпадающего списка в поле **Anti-passing Back Mode** («режим запрета обратного прохода»).
- 2) Выберите **Entrance/Exit Anti-passing Back** («Запрет обратного прохода для входа/выхода») в поле **Rule** («Правило»).
- 3) Задайте значение **Sector ID** («ID сектора»).
- 4) Нажмите **Select Access Controller** («Выбрать контроллер доступа») для выбора устройства во всплывающем окне.
- 5) В области **Card Reader** («Считыватель карт») поставьте галочки в столбце **Enable Anti-passing Back** («Включить запрет обратного прохода») для выбора считывателя карт входа и считывателя карт выхода.
- 6) Нажмите **Save** («Сохранить») для сохранения настроек.

Примечания:

- Необходимо выбрать один считыватель карт входа и один считыватель карт выхода.
- Может быть добавлено до 64 устройств с функцией запрета обратного прохода.
- В настоящее время поддерживается карта M1, и сектор не может быть зашифрован.

➤ На основе сети

Примечание: Оценка необходимости срабатывания запрета обратного прохода в соответствии с информацией о входе и выходе в считывателе карт.

- 1) Выберите **Based on Network** («На основе сети») из выпадающего списка в поле **Anti-passing back mode** («режим запрета обратного прохода»).
- 2) Выберите **Entrance/Exit Anti-passing Back** («Запрет обратного прохода для входа/выхода») в поле **Rule** («Правило»).
- 3) Выберите сервер из выпадающего списка для оценки необходимости срабатывания запрета обратного прохода.
- 4) (Опционально) Вы можете нажать **Delete Record** («Удалить запись») и выбрать

карту во всплывающем окне для удаления информации о проводках карты на всех устройствах.

- 5) Нажмите **Select Access Controller** («Выбрать контроллер доступа») для выбора устройства во всплывающем окне.
- 6) В области **Card Reader** («Считыватель карт») поставьте галочки в столбце **Enable Anti-passing Back** («Включить запрет обратного прохода») для выбора считывателя карт входа и считывателя карт выхода.
- 7) Нажмите **Save** («Сохранить») для сохранения настроек.

Примечания:

- Необходимо выбрать один считыватель карт входа и один считыватель карт выхода.
- Может быть добавлено до 64 устройств с функцией запрета обратного прохода.
- На выбранном сервере может быть сохранено до 5000 записей проводок карт.

6.9 Поиск событий контроля доступа

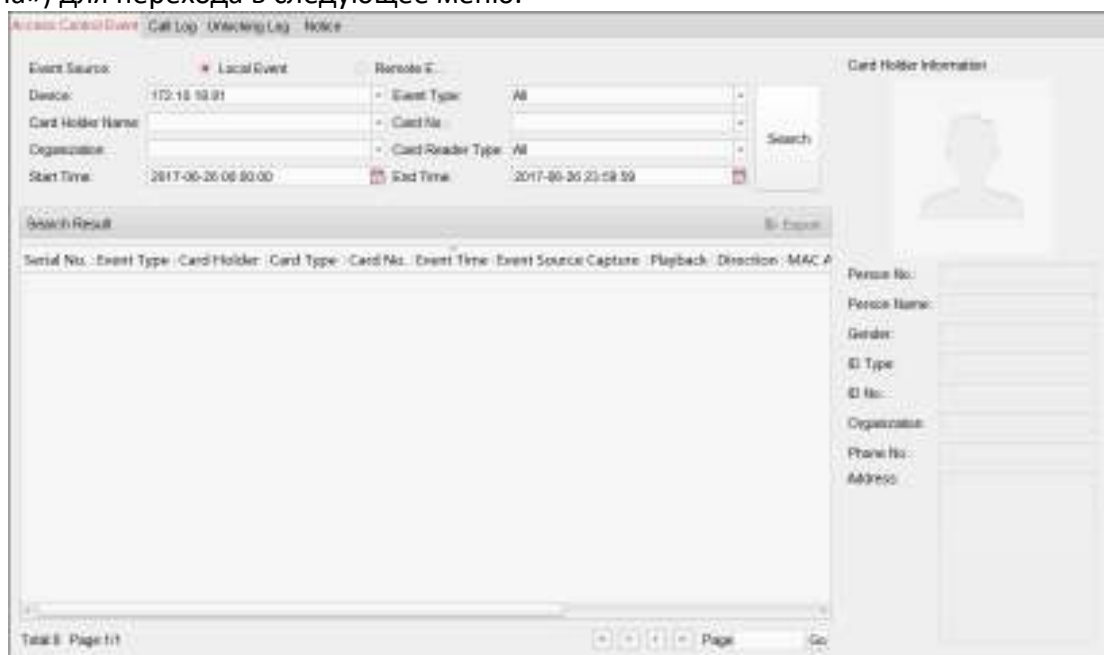
Цель:

Вы можете выполнять поиск по истории как удаленных, так и локальных событий при помощи клиента.

Local Event («Локальное событие»): Поиск событий контроля доступа в базе данных клиента управления.

Remote Event («Удаленное событие»): Поиск событий контроля доступа на устройстве.

Нажмите иконку  и нажмите на вкладку **Access Control Event** («Событие контроля доступа») для перехода в следующее меню.



6.9.1 Поиск локальных событий контроля доступа

Шаги:

1. Выберите в поле **Event Source** («Источник события») значение **Local Event** («Локальное событие»).
2. Введите условие поиска в соответствии с фактическими потребностями.
3. Нажмите **Search** («Поиск»). Результаты будут перечислены ниже.
4. Для событий контроля доступа, которые запущены владельцем карты, вы можете нажать на событие для просмотра подробной информации о владельце карты, включая № человека, имя человека, организацию, номер телефона, контактный адрес и фото.
5. (Опционально) Если событие содержит связанные изображения, вы можете нажать на колонку **Capture** («Захват») для просмотра захваченных изображений во время тревоги с камеры.
6. (Опционально) Если событие содержит связанные видео, вы можете нажать на колонку **Playback** («Воспроизведение») для просмотра записанных видео файлов во время тревоги с камеры.

Примечание: Для настройки срабатывающей камеры обратитесь к Разделу **Ошибка! Источник ссылки не найден. Ошибка! Источник ссылки не найден..**

7. Вы можете нажать **Export** («Экспорт») для экспорта результатов поиска на локальный ПК в *.csv файле.

6.9.2 Поиск удаленных событий контроля доступа

Шаги:

1. Выберите в поле **Event Source** («Источник события») значение **Remote Event** («Удаленное событие»).
2. Введите условие поиска в соответствии с фактическими потребностями.
3. (Опционально) Вы можете поставить галочку **With Alarm Picture** («С изображением тревоги») для поиска событий с тревожными изображениями.
4. Нажмите **Search** («Поиск»). Результаты будут перечислены ниже.
5. Вы можете нажать **Export** («Экспорт») для экспорта результатов поиска на локальный ПК в *.csv файле.

6.10 Конфигурация событий контроля доступа

Цель:

Для добавленного устройства контроля доступа вы можете настроить его привязку к управлению доступом, включая привязку событий контроля доступа, привязку тревожного входа контроля доступа, привязку карты/событий и межустройственную привязку.



Нажмите иконку  на панели управления, или нажмите **Tool -> Event Management** («Инструменты -> Управление событиями») для открытия страницы управления событиями.

6.10.1 Привязка событий контроля доступа

Цель:

Вы можете назначить связанные действия для событий контроля доступа при помощи настройки правил. Например, при детекции события контроля доступа может быть запущено аудио предупреждение или другое связанное действие.

Примечание: Здесь привязка относится к привязке собственных действий клиентского ПО.

Шаги:

1. Нажмите вкладку **Access Control Event** («Событие контроля доступа»).
2. Добавленные устройства контроля доступа будут отображены на панели **Access Control Device** («Устройство контроля доступа») слева.
Выберите устройство контроля доступа, или тревожный вход, или точку контроля доступа (дверь), или считыватель карт для конфигурации привязки событий.
3. Выберите **Event Type** («тип события») для установки привязки.
4. Выберите срабатывающую камеру. Изображение или видео с запущенной камеры появится во всплывающем окне, когда произойдет выбранное событие.
Для захвата изображения со сработавшей камеры при возникновении события вы можете установить расписание захвата и настроить хранение в расписании хранения.
5. Поставьте галочки для активации связанных действий. Для получения подробной информации смотрите *Таблицу Связанные действия для событий контроля доступа*.
6. Нажмите **Save** («Сохранить») для сохранения настроек.
7. Вы можете нажать кнопку **Copy to** («Копировать в») для копирования события контроля доступа в другое устройство контроля доступа, тревожный вход, контрольную точку доступа или считыватель карт.
Выберите параметры для копирования, выберите куда вы хотите скопировать параметры и нажмите кнопку **OK** для подтверждения.



Связанные действия для событий контроля доступа

Связанные действия	Описание
Звуковое предупреждение	Клиентское программное обеспечение издает звуковое предупреждение при срабатывании тревоги. Вы можете выбрать звуковой сигнал для аудио предупреждения.
Привязка Email	Отправка email уведомления с информацией о тревоге одному или нескольким получателям.
Запущенное по тревоге всплывающее изображение	Изображение с тревожной информацией будет всплывать на экране при запуске тревоги.

6.10.2 Связанные действия тревожного входа контроля доступа

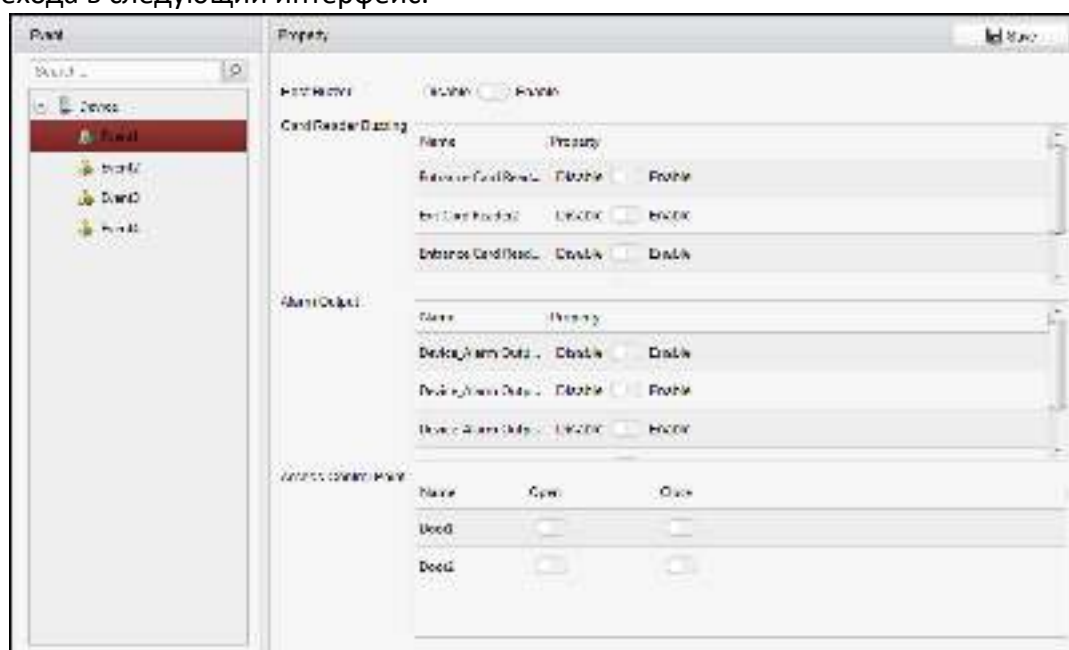
Цель:

Тревожные входы контроля доступа могут быть связаны с некоторыми действиями (например, тревожный выход, зуммер хоста), которые будут выполняться при запуске тревожных входов.

Примечание: Функция должна поддерживаться устройством.

Шаги:

1. Нажмите вкладку **Access Control Alarm Input** («Тревожный вход контроля доступа») для перехода в следующий интерфейс.



2. В списке событий слева выберите тревожный вход.
3. Включите переключатели свойств (иконка изменится с  на ) для их включения.
Host Buzzer («Зуммер хоста»): Звуковое предупреждение контроллера будет активировано.

Card Reader Buzzer («Зуммер считывателя карт»): Звуковое предупреждение считывателя карт будет активировано.

Alarm Output («Тревожный выход»): Тревожный выход будет активирован для уведомления.

Access Control Point (Open/Close) («Точка контроля доступа (Открыть/Заккрыть)»): Дверь будет открыта или закрыта.

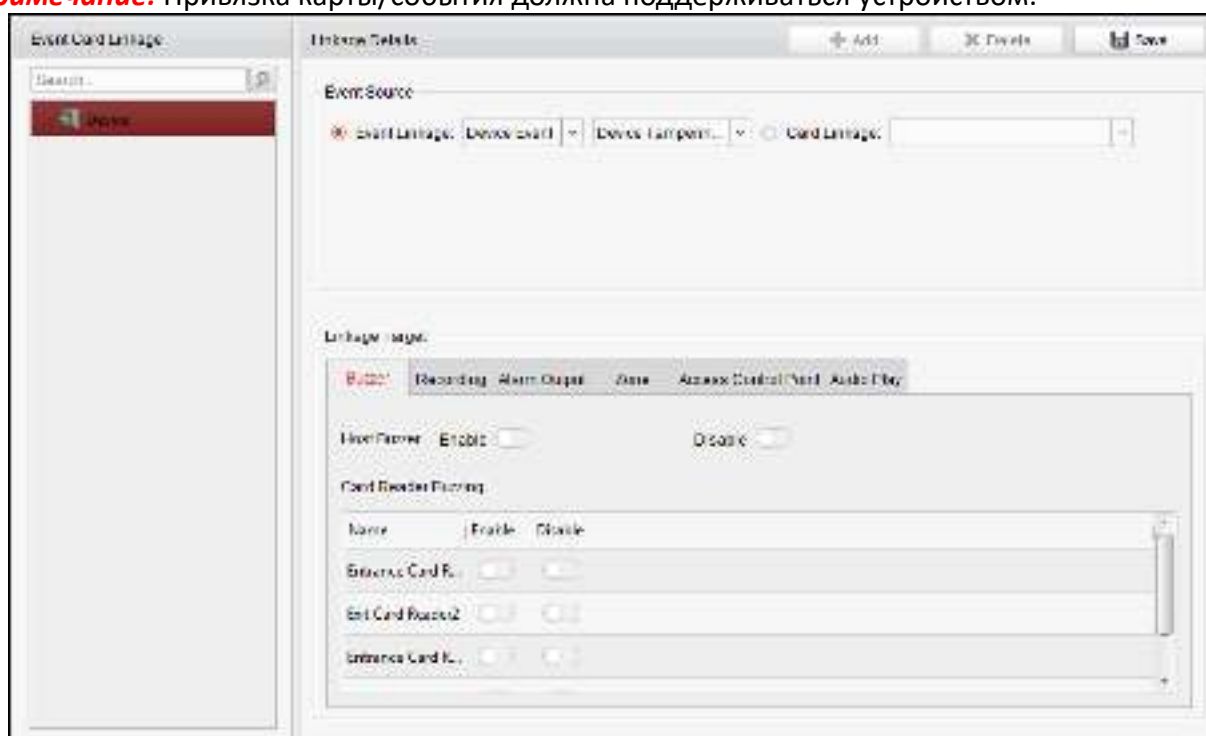
Примечание: Дверь нельзя настроить как открытую или закрытую одновременно.

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

6.10.3 Привязка карт/событий

Нажмите вкладку **Event Card Linkage** («Привязка карты/события») для перехода в соответствующий интерфейс.

Примечание: Привязка карты/события должна поддерживаться устройством.



Выберите устройство контроля доступа из списка слева.

Нажмите кнопку **Add** («Добавить») для добавления новой привязки. Вы можете выбрать в качестве **Event Source** («источник события»): **Event Linkage** («Привязка события») или **Card Linkage** («Привязка карты»).

Привязка события

Для привязки событий тревожные события могут быть разделены на 4 типа: **Device Event** («событие устройства»), **Alarm Input** («тревожный вход»), **Door Event** («событие двери») и **Card Reader Event** («событие считывателя карт»).

Шаги:

1. Выберите устройство слева и нажмите **Add** («Добавить»).

2. Щелкните для выбора в качестве типа привязки значения **Event Linkage** («Привязка события») и выберите тип события из выпадающего списка.
 - Для **Device Event** («Событие устройства») выберите тип события из выпадающего списка.
 - Для **Alarm Input** («Тревожный вход») выберите **Alarm** («тревога») или **Alarm Recovery** («восстановление тревоги»), и выберите имя тревожного входа.
 - Для **Door Event** («Событие двери») выберите тип события и выберите дверь источника.
 - Для **Card Reader Event** («Событие считывателя карт») выберите тип события и выберите считыватель карт.
3. Нажимайте на различные вкладки, чтобы установить разные параметры. Переключайте свойства с  на  для включения соответствующей функции.
Вы можете установить параметры зуммера, записи, зоны, тревожного выхода, точки контроля доступа и проигрывания аудио.

Тип привязки	Цель привязки	Описание
Buzzer («Зуммер»)	Host Buzzer («Зуммер хоста»)	Звуковое предупреждение контроллера будет запущено.
	Card Reader Buzzing («Срабатывание зуммера считывателя карт»)	Звуковое предупреждение считывателя карт будет запущено.
Recording («Запись»)	Capture Status («Статус захвата»)	Будет запущен захват в реальном времени.
Alarm Output («Тревожный выход»)	Alarm Output («Тревожный выход»)	Тревожный выход будет запущен для уведомления.
Zone («Зона»)	Zone («Зона»)	Зона будет установлена на охрану или снята с охраны в соответствии с вашими настройками.
Access Control Point («Точка контроля доступа»)	Access Control Point («Точка контроля доступа»)	Будут запущены различные состояния двери: Open («открыта»), Close («закрыта»), Remain Open («оставить открытой») и Remain Closed («оставить закрытой»). Примечания: ● Все состояния не могут быть запущены одновременно. ● Целевая дверь и дверь источника не могут быть одной и той же дверью.
Audio Play («Проигрывание аудио»)	Audio Play Status («Состояние проигрывания»)	Звуковая подсказка будет запущена. И аудио контент, связанный с выбранным аудио индексом, будет воспроизводиться в соответствии с

	аудио»)	настроенным режимом воспроизведения. Примечание: Для получения дополнительной информации о содержимом аудио индекса смотрите <i>Приложение С Таблица значений аудио индексо</i> .
--	---------	---

4. Нажмите **Save** («Сохранить») для сохранения и вступления в силу настроек.

Привязка карты

Шаги:

1. Щелкните для выбора в качестве типа привязки значения **Card Linkage** («Привязка карты»).
2. Введите номер карты или выберите карту из выпадающего списка.
3. Выберите устройство считывания карт.
5. Нажимайте на различные вкладки, чтобы установить разные параметры. Переключайте свойства с  на  для включения соответствующей функции.

Вы можете установить параметры зуммера, записи, зоны, тревожного выхода, точки контроля доступа и проигрывания аудио.

Тип привязки	Цель привязки	Описание
Buzzer («Зуммер»)	Host Buzzer («Зуммер хоста»)	Звуковое предупреждение контроллера будет запущено.
	Card Reader Buzzing («Срабатывание зуммера считывателя карт»)	Звуковое предупреждение считывателя карт будет запущено.
Recording («Запись»)	Capture Status («Статус захвата»)	Будет запущен захват в реальном времени.
Alarm Output («Тревожный выход»)	Alarm Output («Тревожный выход»)	Тревожный выход будет запущен для уведомления.
Zone («Зона»)	Zone («Зона»)	Зона будет установлена на охрану или снята с охраны в соответствии с вашими настройками.
Access Control Point («Точка контроля доступа»)	Access Control Point («Точка контроля доступа»)	Будут запущены различные состояния двери: Open («открыта»), Close («закрыта»), Remain Open («оставить открытой») и Remain Closed («оставить закрытой»). Примечания: ● Все состояния не могут быть запущены одновременно. ● Целевая дверь и дверь источника не могут быть одной и той же дверью.

Audio Play («Проигрывание аудио»)	Audio Play Status («Состояние проигрывания аудио»)	Звуковая подсказка будет запущена. И аудио контент, связанный с выбранным аудио индексом, будет воспроизводиться в соответствии с настроенным режимом воспроизведения. Примечание: Для получения дополнительной информации о содержимом аудио индекса смотрите <i>Приложение С Таблица значений аудио индексо</i> .
---	--	---

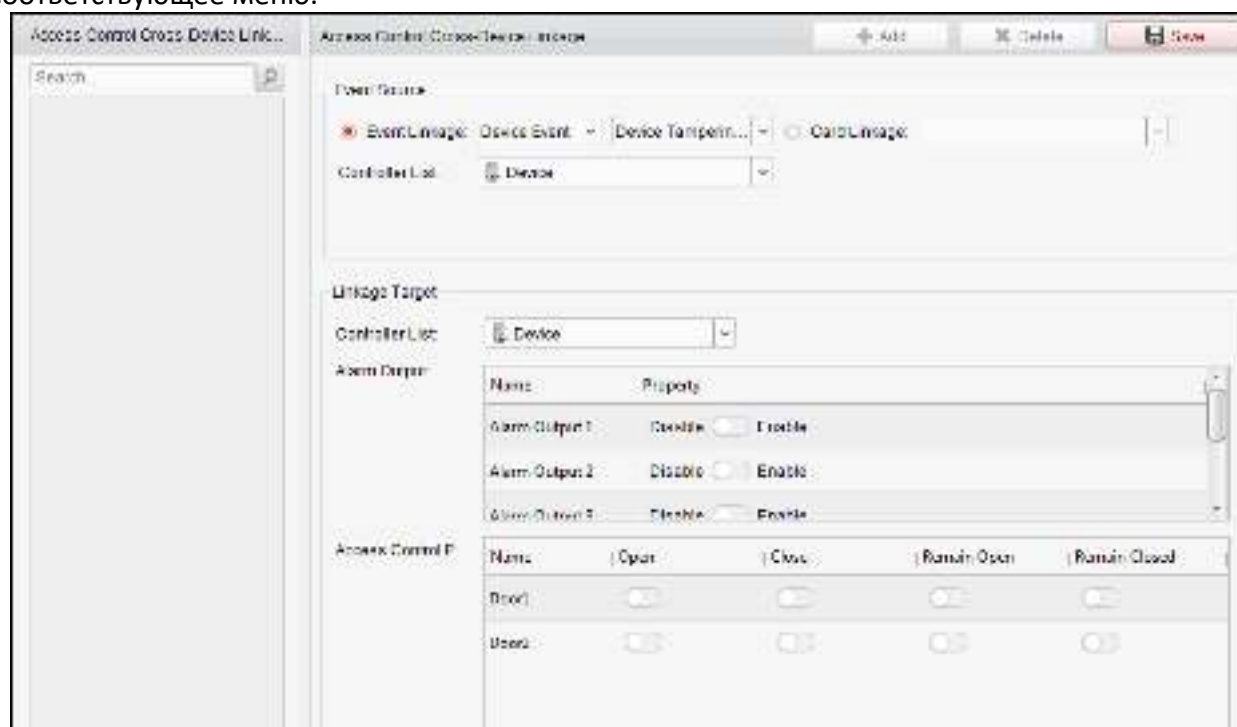
4. Нажмите **Save** («Сохранить») для сохранения и вступления в силу настроек.

6.10.4 Межустройственная привязка

Цель:

Вы можете назначить запуск другого устройства контроля доступа, настроив правило для срабатывания события контроля доступа.

Нажмите вкладку **Cross-Device Linkage** («Межустройственная привязка») для перехода в соответствующее меню.



Нажмите кнопку **Add** («Добавить») для добавления новой привязки. Вы можете выбрать в качестве **Event Source** («источник события»): **Event Linkage** («Привязка события») или **Card Linkage** («Привязка карты»).

Привязка события

Для привязки события тревожные события могут быть разделены на 4 типа: **Device Event** («событие устройства»), **Alarm Input** («тревожный вход»), **Door Event** («событие двери») и **Card Reader event** («событие считывателя карт»).

Шаги:

1. Щелкните для выбора в качестве типа привязки значения **Event Linkage** («Привязка события») и выберите тип события из выпадающего списка.
 - Для **Device Event** («Событие устройства») выберите тип события из выпадающего списка.
 - Для **Alarm Input** («Тревожный вход») выберите **Alarm** («тревога») или **Alarm Recovery** («восстановление тревоги»), и выберите имя тревожного входа.
 - Для **Door Event** («Событие двери») выберите тип события и выберите дверь источника.
 - Для **Card Reader Event** («Событие считывателя карт») выберите тип события и выберите считыватель карт.
2. Установите цель привязки, выберите устройство контроля доступа из выпадающего списка в качестве цели привязки, и переключайте свойства с  на  для их включения.
 - **Alarm Output** («Тревожный выход»): Тревожный выход будет инициирован для уведомления.
 - **Access Control Point** («Точка контроля доступа»): Будут запущены различные состояния двери: **Open** («открыта»), **Close** («закрыта»), **Remain Open** («оставить открытой») и **Remain Closed** («оставить закрытой»).

Примечание: Все состояния двери не могут быть запущены одновременно.
3. Нажмите **Save** («Сохранить») для сохранения параметров.

Привязка карты

Шаги:

1. Щелкните для выбора в качестве типа привязки значения **Card Linkage** («Привязка карты»).
2. Выберите карту из выпадающего списка и выберите **Access Control Device** («устройство контроля доступа») в поле **Event Source** («источник события»).
3. Выберите устройство считывания карт.
4. Установите цель привязки, выберите устройство контроля доступа из выпадающего списка в качестве цели привязки, и переключайте свойства с  на  для их включения.

Alarm Output («Тревожный выход»): Тревожный выход будет инициирован для уведомления.
5. Нажмите **Save** («Сохранить») для сохранения параметров.

6.11 Управление состоянием двери

Цель:

Состояние двери добавленного устройства контроля доступа будет отображаться в реальном времени. Вы можете проверить состояние двери и связанные события выбранной двери. Вы можете управлять состоянием двери и также устанавливать продолжительность состояний дверей.

6.11.1 Управление группой контроля доступа

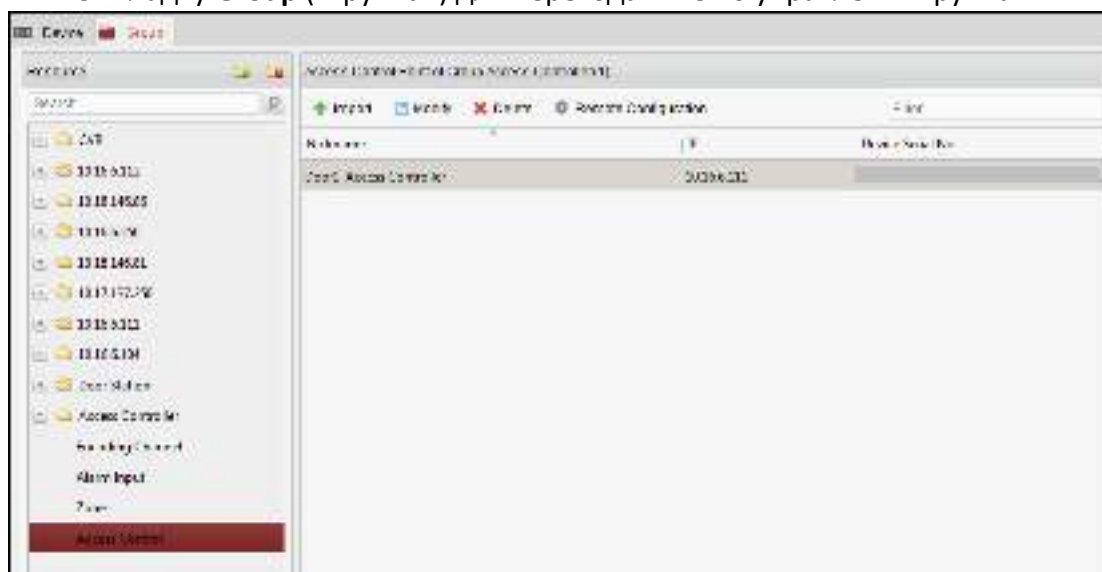
Цель:

Перед тем, как контролировать состояние двери и установить продолжительность состояния, вам необходимо организовать ее в группу для удобного управления.

Выполните следующие шаги, чтобы создать группу для устройства контроля доступа:

Шаги:

1. Нажмите  на панели управления для открытия страницы управления устройствами.
2. Нажмите вкладку **Group** («Группа») для перехода в меню управления группами.



3. Выполните следующие шаги для добавления группы.
 - 1) Нажмите , чтобы открыть диалоговое окно добавления группы.
 - 2) Введите **Group Name** («имя группы») по вашему желанию.
 - 3) Нажмите **OK** для добавления новой группы в список групп.

Вы также можете поставить галочку **Create Group by Device Name** («Создать группу по имени устройства») для создания новой группы с именем, совпадающим с именем выбранного устройства.



4. Выполните следующие шаги, чтобы импортировать точки контроля доступа в группу:

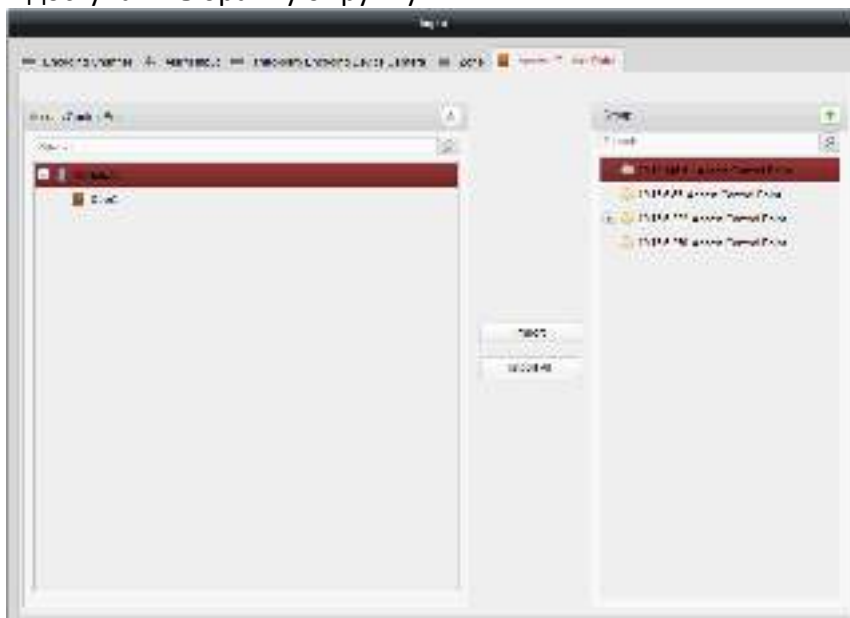
- 1) Нажмите **Import** («Импорт») в меню **Group Management** («Управление группой»), а затем нажмите вкладку **Access Control** («Контроль доступа») для перехода на страницу **Import Access Control** («Импорт контроля доступа»).

Примечания:

- Вы также можете выбрать вкладку **Alarm Input** («Тревожный вход») и импортировать тревожные входы в группу.
- Для видео терминала контроля доступа вы можете добавить камеры в качестве канала кодирования в группу.

- 2) Выберите имена точек контроля доступа в списке.
- 3) Выберите группу из списка групп.
- 4) Нажмите **Import** («Импорт») для импорта выбранных точек контроля доступа в группу.

Вы также можете нажать **Import All** («Импортировать все») для импорта всех точек контроля доступа в выбранную группу.



5. После импорта точек контроля доступа в группу вы можете нажать  или дважды щелкнуть по имени группы/точки контроля доступа для ее редактирования.

6.11.2 Анти-контроль точки контроля доступа (Дверь)

Цель:

Вы можете управлять состоянием для одной точки контроля доступа (двери), включая открытие двери, закрытие двери, удержание в открытом/закрытом состоянии.



Нажмите иконку на панели управления для перехода в меню мониторинга состояния.



Шаги:

1. Выберите группу управления доступом слева. Для управления группой контроля доступа смотрите **Раздел Ошибка! Источник ссылки не найден. Ошибка! Источник ссылки не найден..**
2. Точки контроля доступа выбранной группы контроля доступа будут отображаться справа.



Нажмите иконку на панели статуса для выбора двери.

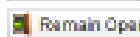
3. Нажмите на одну из кнопок, перечисленных на панели **Status Information** («Сведения о состоянии») для управления дверью.



(«Открыть дверь»): Нажмите на кнопку, чтобы открыть дверь один раз.



(«Закрыть дверь»): Нажмите на кнопку, чтобы закрыть дверь один раз.



(«Оставить открытой»): Нажмите на кнопку, чтобы оставить дверь открытой.



(«Оставить закрытой»): Нажмите на кнопку, чтобы оставить дверь закрытой.



(«Захват»): Нажмите для захвата изображения вручную.

4. Вы можете просмотреть результат операции анти-контроля на панели **Operation Log** («Журнал операций»).

Примечания:

- Если выбрано состояние **Remain Open** («Оставить открытой»)/**Remain Closed** («Оставить

закрытой»), дверь будет открыта/закрыта до тех пор, пока не будет выполнена новая команда анти-контроля.

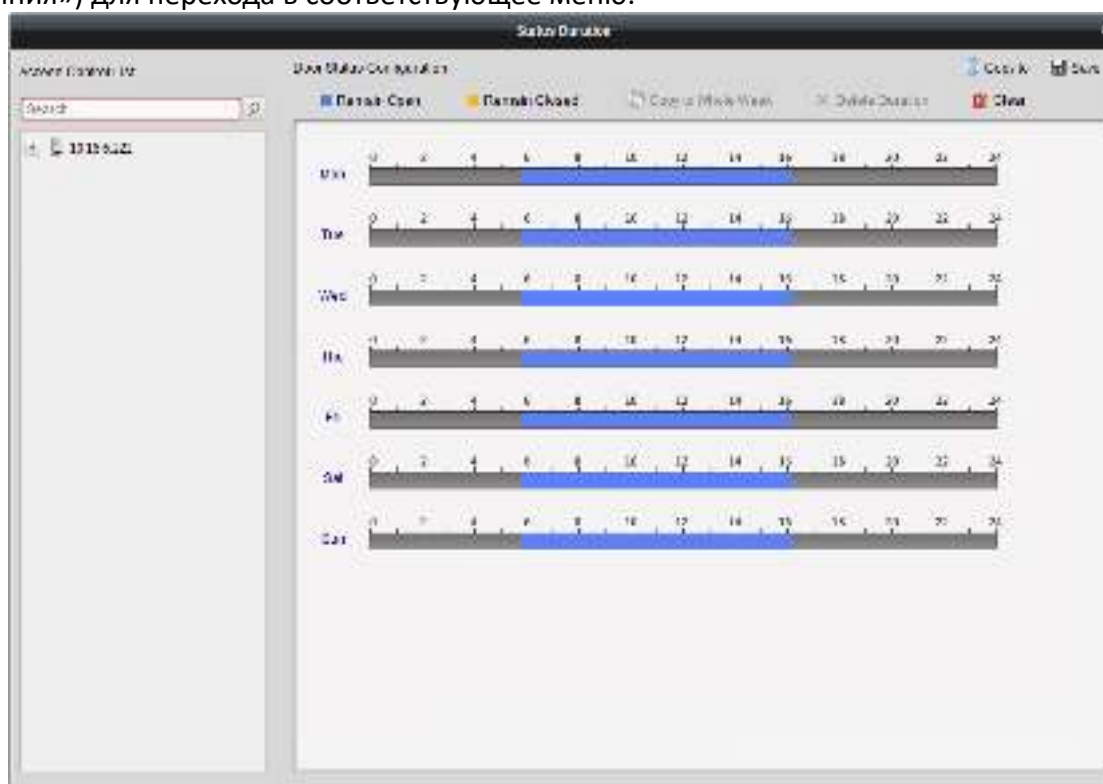
- Кнопка **Capture** («Захват») доступна, когда устройство поддерживает функцию захвата. Захват не может быть произведен, пока не настроен сервер хранения.
- Если дверь находится в состоянии **Remain Closed** («Оставить закрытой»), только супер пользователь может открыть дверь, или она может быть открыта через клиентское ПО.

6.11.3 Конфигурация длительности состояния

Цель:

Вы можете планировать еженедельные периоды времени для точки контроля доступа (двери), когда она будет оставаться открытой или оставаться закрытой.

В модуле **Door Status** («Состояние двери») нажмите кнопку **Status Duration** («Длительность состояния») для перехода в соответствующее меню.

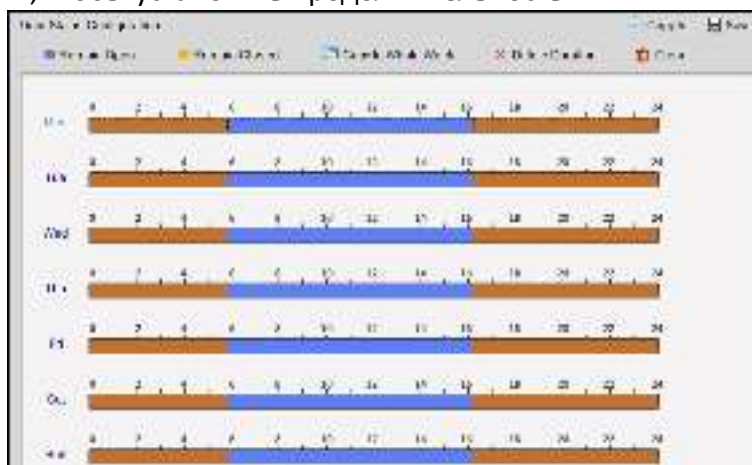


Шаги:

1. Нажмите, чтобы выбрать дверь из списка устройств управления доступом слева.
2. На панели **Door Status Configuration** («Конфигурация состояния двери») справа нарисуйте расписание для выбранной двери.
 - 1) Выберите кисть для маркировки состояния двери: ☐ **Remain Open** («Оставить открытой») или ☐ **Remain Closed** («Оставить закрытой»).
 - Remain Open** («Оставить открытой»): Дверь будет открыта в течение сконфигурированного периода времени. Кисть отмечена как ■.
 - Remain Closed** («Оставить закрытой»): Дверь будет закрыта в течение

сконфигурированного периода времени. Кисть отмечена как .

- 2) Нажмите и перетащите мышку по шкале времени, чтобы нарисовать цветную полосу в расписании, чтобы установить продолжительность.

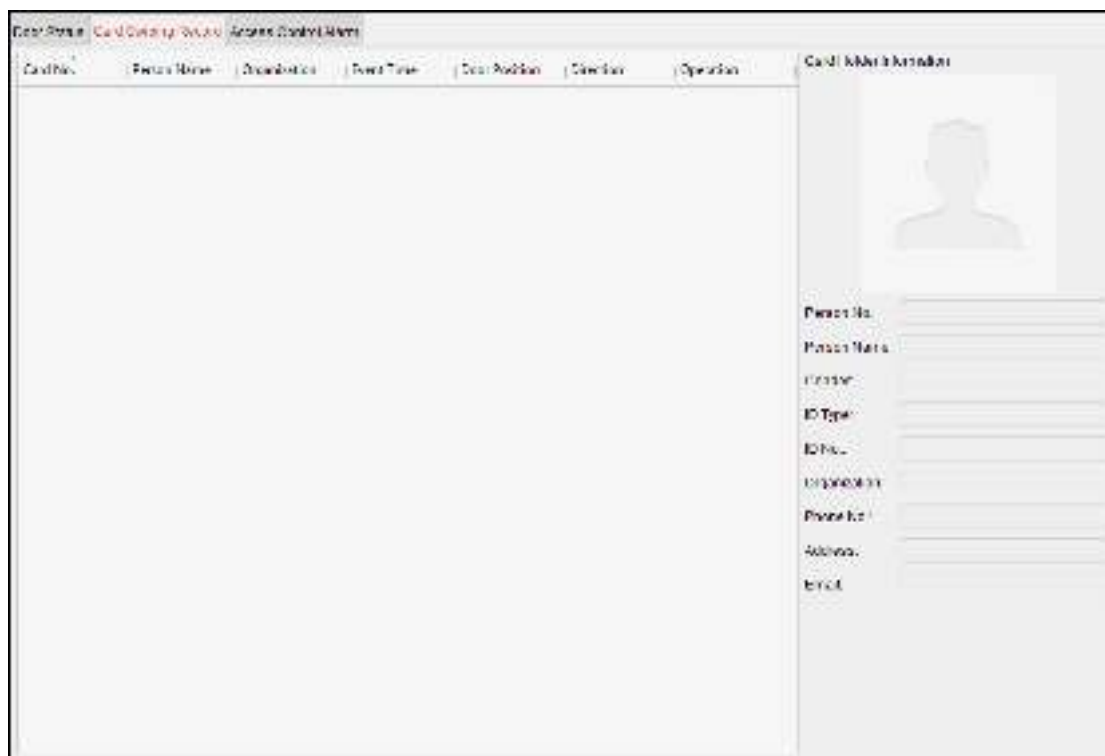


- 3) Когда курсор превращается в , вы можете переместить выбранную шкалу времени, которую вы только что отредактировали. Вы также можете отредактировать отображаемую временную точку, чтобы установить точный период времени. Когда курсор превращается в , вы можете удлинить или сократить выбранную временную шкалу.

3. Опционально, вы можете выбрать временную шкалу расписания и нажать **Copy to Whole Week** («Копировать на целую неделю») для копирования настроек временной шкалы на другие дни недели.
4. Вы можете выбрать временную шкалу и нажать **Delete Duration** («Удалить длительность») для удаления периода времени. Или вы можете нажать **Clear** («Очистить») для очистки всех настроенных длительностей в расписании.
5. Нажмите **Save** («Сохранить») для сохранения настроек.
6. Вы можете нажать кнопку **Copy to** («Копировать в») для копирования расписания на другие двери.

6.11.4 Запись проводки карты в реальном времени

Нажмите вкладку **Card Swiping Record** («Запись проводки карты») для перехода в соответствующее меню.



Записи журнала проводок карт для всех устройств контроля доступа будут отображаться в реальном времени. Вы можете просмотреть детали событий проводки карты, включая № карты, имя человека, организацию, время события и др.

Вы можете нажать на событие для просмотра подробной информации о владельце карты, включая № человека, имя человека, организацию, телефон, контактный адрес и др.

6.11.5 Тревога контроля доступа в реальном времени

Цель:

Записи журнала событий контроля доступа будут отображаться в реальном времени, включая исключения устройства, события дверей, события считывателя карт и тревожного входа.

Нажмите вкладку **Access Control Alarm** («Тревога контроля доступа») для перехода в следующее меню.

Subscribe				
Alarm Type	Alarm Time	Alarm Location	Alarm Content	Operation
Remote Disarm...	2016-12-16 13:5...	Access Controller	Remote Disarm...	  
Remote Arming	2016-12-16 13:5...	Access Controller	Remote Arming	  
Remote Login	2016-12-16 13:5...	Access Controller	Remote Login	  
Remote Disarm...	2016-12-16 13:5...	Access Controller	Remote Disarm...	  
Remote Logout	2016-12-16 13:5...	Access Controller	Remote Logout	  
Remote Login	2016-12-16 13:5...	Access Controller	Remote Login	  
Remote Arming	2016-12-16 13:4...	Access Controller	Remote Arming	  
Remote Login	2016-12-16 13:4...	Access Controller	Remote Login	  
Remote Disarm...	2016-12-16 13:4...	Access Controller	Remote Disarm...	  
Door Locked	2016-12-16 13:4...	Door1	Door Locked	  
Unlock	2016-12-16 13:4...	Door1	Unlock	  
Remote Arming	2016-12-16 13:4...	Access Controller	Remote Arming	  
Remote Login	2016-12-16 13:4...	Access Controller	Remote Login	  
Remote Disarm...	2016-12-16 13:4...	Access Controller	Remote Disarm...	  

Шаги:

1. Все тревоги контроля доступа будут отображаться в списке в реальном времени. Вы можете просмотреть тип тревоги, время тревоги, местоположение и др.
 2. Нажмите  для отображения всех тревог на электронной карте (E-map).
 3. Вы можете нажать  или  для просмотра вида в реальном времени или захваченного изображения с камеры при срабатывании тревоги.
- Примечание:** Для установки срабатывающей камеры обратитесь к Разделу **Ошибка! Источник ссылки не найден. Ошибка! Источник ссылки не найден.**
4. Нажмите **Subscribe** («Подписаться») для выбора тревоги, которую сможет получать клиент при ее запуске.



- 1) Поставьте галочки для выбора тревог, включая тревогу исключений устройства, тревогу событий дверей, тревогу считывателя карт и тревожного входа.
- 2) Нажмите **ОК** для сохранения настроек.

6.12 Управление охраной

Цель:

Вы можете устанавливать на охрану/снимать с охраны устройство. После постановки устройства на охрану клиент сможет получать информацию о тревогах от устройства.

Шаги:

1. Нажмите **Tool -> Device Arming Control** («Инструменты -> Управление охраной устройства») для появления всплывающего окна управления охраной устройства.
2. Поставьте устройство на охрану при помощи установки соответствующих галочек. Затем информация о тревоге будет автоматически загружена в клиентское программное обеспечение при возникновении тревоги.



6.13 Время и посещаемость

Цель:

Модуль **Time and Attendance** («Время и посещаемость») обеспечивает множество функциональных возможностей, включая управление расписанием смен, обработку посещаемости, статистику посещаемости и другие расширенные функции.

Перед началом:

Вы должны добавить организацию и человека в модуле **Access Control** («Контроль доступа»). Для получения подробной информации смотрите *Раздел **Ошибка! Источник ссылки не найден.** Добавление организации* и *Раздел **Ошибка! Источник ссылки не найден.** Добавление людей*.

Выполните следующие шаги для доступа к модулю **Time and Attendance** («Время и посещаемость»).

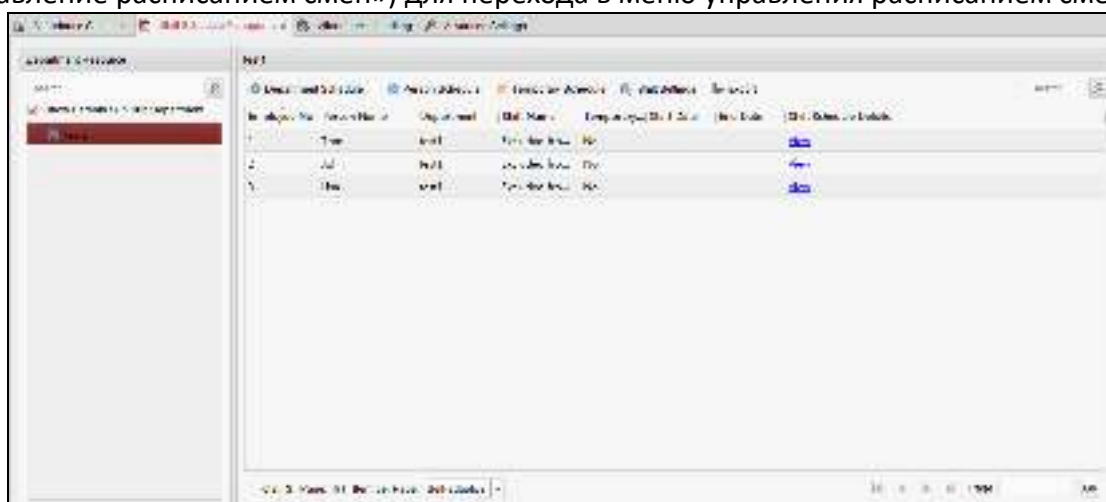


Нажмите  для входа в модуль Времени и посещаемости как показано на рисунке:



6.13.1 Управление расписанием смены

Откройте модуль Время и посещаемость и нажмите **Shift Schedule Management** («Управление расписанием смен») для перехода в меню управления расписанием смен.



Настройки смены

Цель:

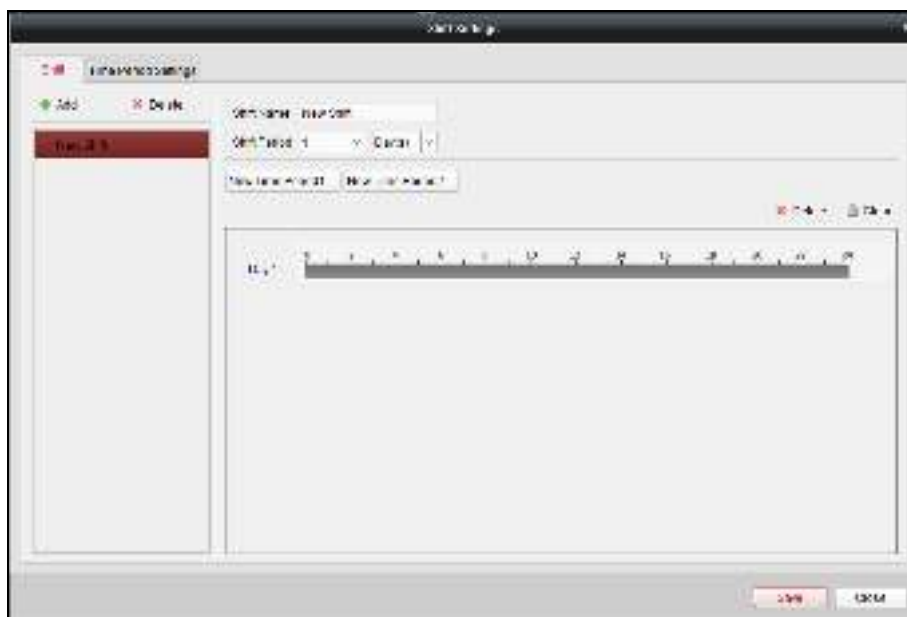
можете добавлять периоды времени и смены для расписания смен.

Нажмите **Shift Settings** («Настройки смены») для появления всплывающего окна настроек смен.

➤ Добавление периода времени

Шаги:

1. Нажмите вкладку **Time Period** («Период времени»).
2. Нажмите **Add** («Добавить»).



3. Установите **Shift Name** («имя смены»).
4. Выберите **Shift Period** («период смены») из выпадающего списка.
5. Настройте период смены с добавленным периодом времени.
 - 1) Выберите период времени.
 - 2) Нажмите на шкалу времени, чтобы применить период времени для выбранного дня. Вы можете нажать на период времени и нажать  или **Delete** («Удалить») для удаления периода.

Вы можете также нажать **Clear** («Очистить») для удаления всех периодов времени дня.
6. Нажмите **Save** («Сохранить») для сохранения настроек.

Добавленные смены будут отображены на панели слева.

Вы также можете нажать **Delete** («Удалить») на панели слева для удаления смены.

Настройки расписания смен

Цель:

После установки смены вы можете установить расписание отделов, расписание людей и временное расписание.

Примечание: Временное расписание имеет более высокий приоритет, чем расписание отделов и расписание персонала.

➤ Расписание отдела

Вы можете установить расписание смены для одного отдела, и всем людям из данного отдела будет назначено это расписание смены.

Примечание: В модуле **Time and Attendance** («Время и посещаемость») список отделов такой же, как и список организаций в модуле **Access Control** («Контроль доступа»). Для настройки организаций в модуле **Access Control** («Контроль доступа») обратитесь к Разделу **Ошибка!** *Источник ссылки не найден. Управление организацией.*

Шаги:

1. Откройте меню **Shift Schedule Management** («Управление расписанием смен») и выберите отдел на панели слева.

- Нажмите **Department Schedule** («Расписание отдела») для появления диалогового окна настройки расписания отдела.



- Поставьте галочку **Time and Attendance** («Время и посещаемость»).
Всем людям в отделе, кроме тех, кто был исключен из правил посещаемости, будет присвоено расписание посещаемости.
- Выберите смену из выпадающего списка **Shift** («смена»).
- Установите значения для **Start Date** («дата начала») и **End Date** («дата окончания»).
- (Опционально) Установите другие параметры для расписания.
Вы можете выбрать **Check-in Not Required** («Отметка о приходе не требуется»), **Check-out Not Required** («Отметка об уходе не требуется»), **Effective for Holiday** («Действует для выходных»), **Effective for Overtime** («Действует для переработки»), **Effective for Multiple Shift Schedules** («Действует для сложного расписания смен»).

Примечания:

- Multiple Shift Schedules** («Сложное расписание смен») содержит более одного периода времени. Человек может входить / выходить в любой из периодов времени, и посещения будут действительными.

Пример: Если сложное расписание смены содержит три периода времени: 00:00-07:00, 08:00-15:00 и 16:00-23:00. Посещаемость человека, работающего в соответствии с этими сменами, будет действительна в любой из этих трех периодов времени. Если человек отметился при входе в 07:50, то он будет отнесен к ближайшему периоду 08:00 - 15:00.

- После установки галочки **Effective for Multiple Shift Schedules** («Действует для сложного расписания смен») вы можете выбрать действующие периоды времени из добавленных периодов времени для людей в отделе.



- В списке **Selectable Time Period** («Доступные для выбора периоды времени») слева нажмите на добавленный период времени и нажмите  для добавления его в список справа.

- 2) (Опционально) Для удаления выбранного периода времени, выберите его и нажмите .
7. (Опционально) Поставьте галочку **Set as Default for All Persons in Department** («Установить в качестве значения по умолчанию для всех людей в отделе»).
Все люди в отделе будут использовать это расписание смен по умолчанию.
8. (Опционально) Если выбранный отдел содержит вспомогательные подразделения, поставьте галочку **Shift Schedule for All Sub Departments** («Расписание смен для всех подразделений»), чтобы применить расписание отдела к его подразделениям.
9. Нажмите **Save** («Сохранить») для сохранения настроек.

➤ Расписание человека

Шаги:

1. Откройте меню **Shift Schedule Management** («Управление расписанием смен») и выберите отдел на панели слева.
2. Выберите человека (людей) на панели справа.
3. Нажмите **Person Schedule** («Расписание человека») для появления всплывающего диалогового окна настройки расписания человека.



4. Поставьте галочку **Time and Attendance** («Время и посещаемость»).
К выбранному человеку будет применено расписание посещаемости.
5. Выберите смену из выпадающего списка **Shift** («смена»).
6. Установите значения для **Start Date** («дата начала») и **End Date** («дата окончания»).
7. (Опционально) Установите другие параметры для расписания.
Вы можете выбрать **Check-in Not Required** («Отметка о приходе не требуется»), **Check-out Not Required** («Отметка об уходе не требуется»), **Effective for Holiday** («Действует для выходных»), **Effective for Overtime** («Действует для переработки»), **Effective for Multiple Shift Schedules** («Действует для сложного расписания смен»).
8. Нажмите **Save** («Сохранить») для сохранения настроек.

➤ Временное расписание

Шаги:

1. Откройте меню **Shift Schedule Management** («Управление расписанием смен») и выберите отдел на панели слева.
2. Выберите человека (людей) на панели справа.
3. Нажмите **Temporary Schedule** («Временное расписание») для появления всплывающего

диалогового окна настройки временного расписания.



4. Нажмите  для установки даты смены.
5. Настройте дату смены с добавленным периодом времени.
 - 1) Выберите период времени.
 - 2) Нажмите на шкалу времени, чтобы применить период времени для выбранного дня. Вы можете нажать на период времени и нажать  для удаления периода. Вы можете также нажать **Clear** («Очистить») для удаления всех периодов времени дня.
6. Вы можете нажать **Advanced Settings** («Расширенные настройки») для конфигурации расширенных правил для временного расписания.

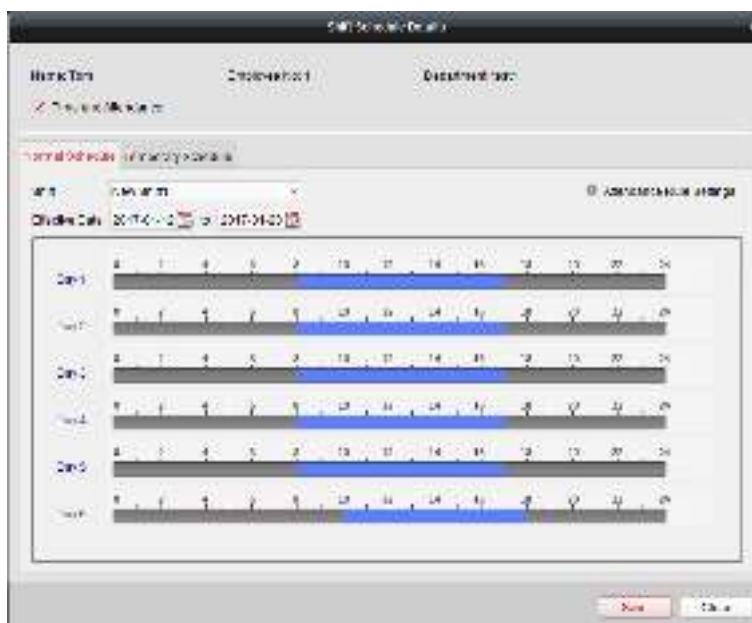


7. Нажмите **Add** («Добавить») для сохранения настроек.

➤ Проверка деталей расписания смен

Шаги:

1. Откройте меню **Shift Schedule Management** («Управление расписанием смен») и выберите отдел на панели слева.
2. Выберите человека (людей) на панели справа.
3. Нажмите **View** («Просмотр») для появления всплывающего диалогового окна деталей расписания смен. Вы можете проверить детали расписания смен.



4. Нажмите вкладку **Normal Schedule** («Обычное расписание»).

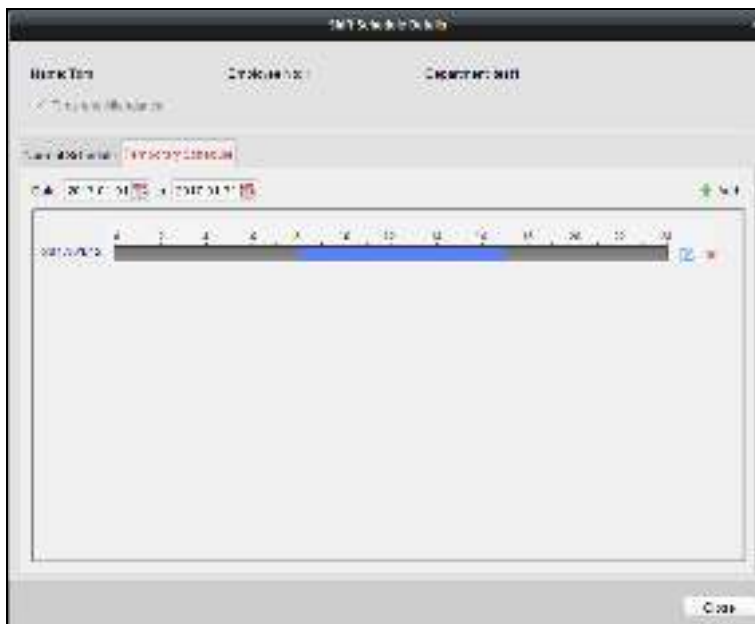
Вы можете проверить и отредактировать детали обычного расписания.

- 1) Выберите смену из выпадающего списка.
- 2) Нажмите **Attendance Rule Settings** («Настройки правила посещаемости») для появления соответствующего всплывающего окна.



Вы можете поставить галочки у необходимых правил посещаемости и нажать **OK** для сохранения настроек.

- 3) Нажмите  для установки даты.
- 4) Нажмите **Save** («Сохранить») для сохранения настроек.
5. (Опционально) Нажмите вкладку **Temporary Schedule** («Временное расписание»).



Вы можете проверить и отредактировать детали временного расписания.

(Опционально) Нажмите **Add** («Добавить») для добавления временного расписания для выбранного человека.

(Опционально) Нажмите  для редактирования периода времени.

(Опционально) Нажмите  для удаления временного расписания.

➤ Экспорт деталей расписания смен

В меню **Shift Schedule Management** («Управление расписанием смен») выберите отдел на панели слева и нажмите **Export** («Экспорт») для экспорта деталей всех расписаний смен людей на локальный ПК.

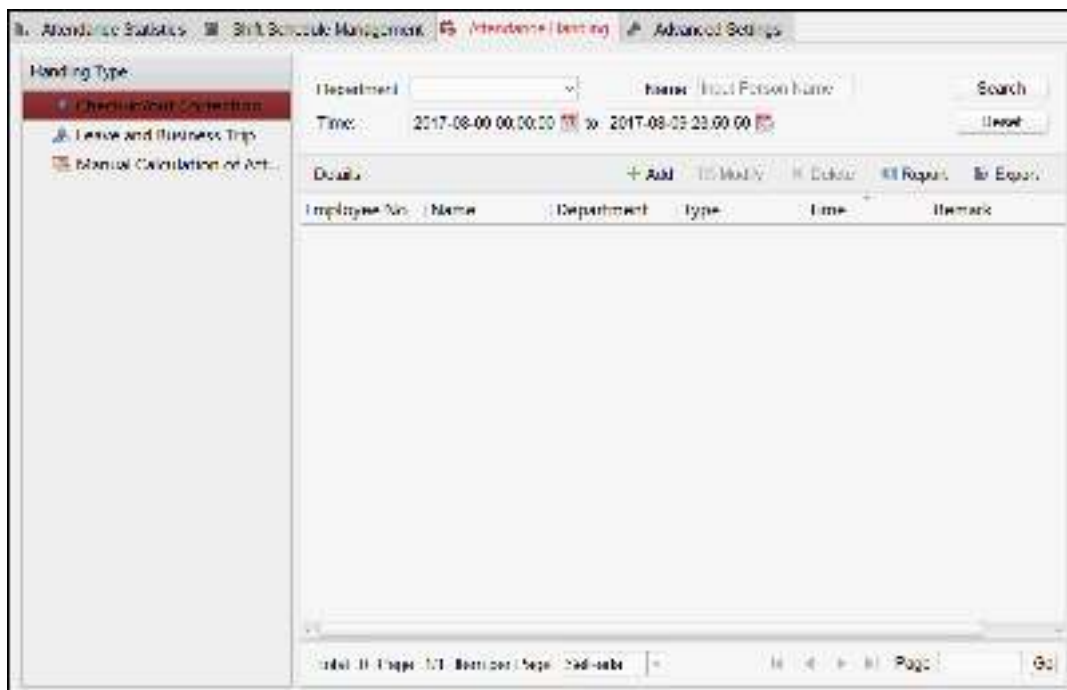
Примечание: Экспортированные данные сохраняются в формате *.csv.

6.13.2 Обработка посещаемости

Цель:

Вы можете обрабатывать посещаемость, включая коррекцию отметки о приходе, коррекцию отметки об уходе, отпуска и командировки, а также подсчет посещаемости вручную.

Откройте модуль **Time and Attendance** («Время и посещаемость») и нажмите **Attendance Handling** («Обработка посещаемости») для входа в соответствующее меню.



Корректировка отметки о приходе/уходе

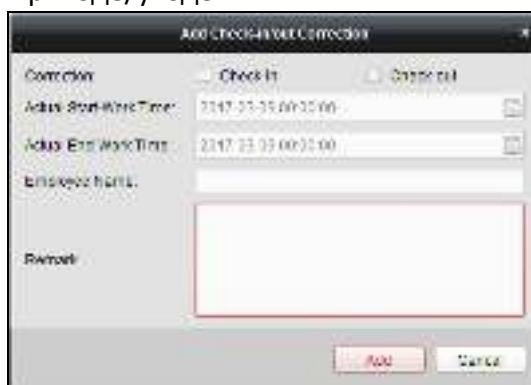
Цель:

Вы можете добавлять, редактировать, удалять, искать корректировку отметки о приходе/уходе и генерировать соответствующий отчет. Вы также можете экспортировать детали корректировки отметки о приходе/уходе на локальный ПК.

➤ Добавление корректировки отметки о приходе/уходе

Шаги:

1. Нажмите вкладку **Check-in/out Correction** («Корректировка отметки о приходе/уходе»).
2. Нажмите **Add** («Добавить») для появления всплывающего окна добавления корректировки отметки о приходе/уходе.



3. Установите параметры корректировки отметки о приходе/уходе.
 Для корректировки отметки о приходе: Поставьте галочку **Check-in** («Отметка о приходе») и установите фактическое время начала работы.
 Для корректировки отметки об уходе: Поставьте галочку **Check-out** («Отметка об уходе») и установите фактическое время окончания работы.

4. Нажмите на поле **Employee Name** («Имя сотрудника») и выберите человека.
Вы также можете ввести ключевое слово и нажать  для поиска необходимого человека.
5. (Опционально) Внесите какие-либо заметки в поле **Remark** («примечание»), если необходимо.
6. Нажмите **Add** («Добавить») для добавления корректировки отметки о приходе/уходе.
Добавленные корректировки отметки о приходе/уходе будут отображены в меню **Attendance Handling** («Обработка посещаемости»).
(Опционально) Выберите корректировку отметки о приходе/уходе и нажмите кнопку **Modify** («Изменить») для редактирования корректировки.
(Опционально) Выберите корректировку отметки о приходе/уходе и нажмите кнопку **Delete** («Удалить») для удаления корректировки.
(Опционально) Нажмите кнопку **Report** («Отчет») для генерирования отчета о корректировке отметки о приходе/уходе.
(Опционально) Нажмите кнопку **Export** («Экспорт») для экспорта деталей корректировки отметки о приходе/уходе на локальный ПК.

Примечание: Экспортированные данные сохраняются в формате *.csv.

➤ **Поиск корректировки отметки о приходе/уходе**

Шаги:

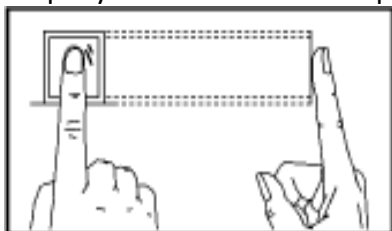
1. Нажмите вкладку **Check-in/out Correction** («Корректировка отметки о приходе/уходе»).
2. Задайте условия поиска.
Department («Отдел»): Выберите отдел из выпадающего списка.
Name («Имя»): Введите имя человека.
Time («Время»): Нажмите  для установки определенного диапазона времени.
3. Нажмите **Search** («Поиск») для поиска корректировок отметок о приходе/уходе.
Детали корректировок отметок о приходе/уходе будут отображены в списке.
Вы можете также нажать кнопку **Reset** («Сброс») для сброса условий поиска.

Приложение А Рекомендации по сканированию отпечатков пальцев

Для сканирования отпечатка используйте указательный, средний или безымянный палец.

Правильное сканирование

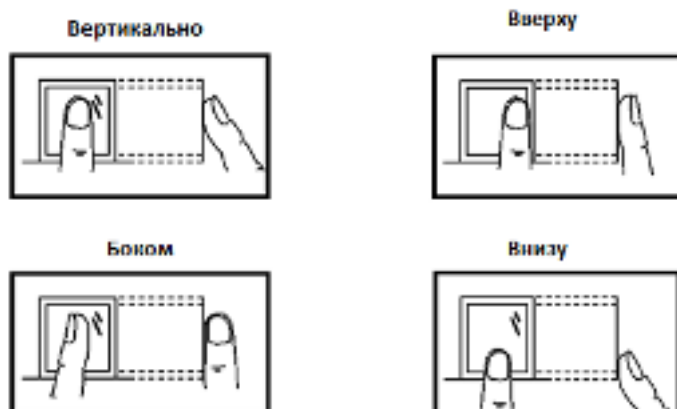
На рисунке ниже показан правильный способ сканирования:



Вы должны прижать палец к сканеру горизонтально. Центр сканируемого пальца должен совпадать с центром сканера.

Неправильное сканирование

Приведенные ниже рисунки показывают неверные способы сканирования отпечатков пальцев:



Окружающая среда

Сканер должен избегать прямых лучей света, высоких температур, влажных условий и дождя.

Когда палец сухой, сканер может не распознать ваш отпечаток пальца. Вы можете подуть на палец и снова приложить его к сканеру.

Другое

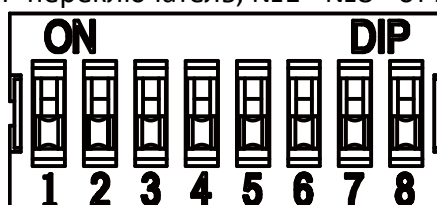
Если у вас неглубокий отпечаток пальца или его сложно отсканировать, мы рекомендуем вам использовать другие методы аутентификации.

Если у вас есть травмы на сканируемом пальце, сканер может его не распознать. Вы можете использовать другой палец и повторить попытку снова.

Приложение В Описание DIP-переключателей

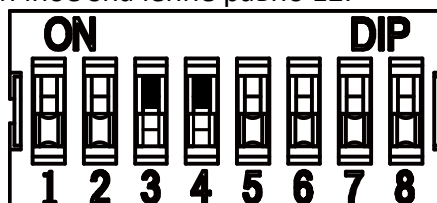
Представление DIP-переключателей

На ведущей плате управления проходом есть две группы DIP-переключателей. Возьмем в качестве примера 8-битный DIP-переключатель; №1 - №8 - от младшего бита к старшему.



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

Если вы установите DIP-переключатели, как показано на рисунке ниже, двоичное значение будет равно 00001100, а десятичное значение равно 12.



Соответствующие DIP-переключателям функции

Функции 8-битного DIP-переключателя на ведущей плате управления проходом:

Бит	Функция	Десятичное значение	Двоичное значение
1 - 2	Нормальный режим	0	00
	Режим обучения	1	01
	Тестовый режим	2	10
3	Включить режим памяти	0	0
	Выключить режим памяти	1	1
4	Разрешает открытие турникета при проводке карты в зоне тревоги	0	0
	Запрещает открытие турникета при проводке карты в зоне тревоги	1	1
5 - 8	Контролируемое двунаправленное движение	0	0000
	Контролируемый вход и запрещенный выход	1	0001
	Контролируемый вход и свободный выход	2	0010
	Свободное двунаправленное	3	0011

	движение		
	Свободный вход и контролируемый выход	4	0100
	Свободный вход и запрещенный выход	5	0101
	Запрещенное двунаправленное движение	6	0110
	Запрещенный вход и контролируемый выход	7	0111
	Запрещенный вход и свободный выход	8	1000

Функции 4-битного DIP-переключателя на ведущей плате управления проходом:

Бит	Функция	Десятичное значение	Двоичное значение
1	Нормальный режим	0	0
	Режим сопряжения с пультом дистанционного управления	1	1
2~4	Зарезервированы		

Приложение С Таблица значений аудио индексов

Индекс	Содержание
1	Аутентифицирован.
2	Карта № не существует.
3	Карта № и отпечаток пальца не совпадают.
4	Человек перелезает через турникет.
5	Обратный проход.
6	Тайм-аут прохода.
7	Вторжение.
8	Принудительный доступ.
9	Несоблюдение дистанции.
10	Нет разрешений.
11	Тайм-аут аутентификации.
13	Ошибка аутентификации.
14	Просроченная карта.

Приложение D Описание кодов ошибок

В случае возникновения ошибки распашной турникет отобразит код ошибки на семисегментном дисплее. Обратитесь к таблице ниже, чтобы найти описание каждого кода ошибки.

Причина ошибки	№	Причина ошибки	№
Нормальная работа	00	Верхняя ИК-плата 5 офлайн	29
Первый ИК-луч на верхней ИК-плате сработал	01	Верхняя ИК-плата 6 офлайн	30
Второй ИК-луч на верхней ИК-плате сработал	02	Верхняя ИК-плата 7 офлайн	31
Третий ИК-луч на верхней ИК-плате сработал	03	Верхняя ИК-плата 8 офлайн	32
Четвертый ИК-луч на верхней ИК-плате сработал	04	Верхняя ИК-плата 9 офлайн	33
Пятый ИК-луч на верхней ИК-плате сработал	05	Верхняя ИК-плата 10 офлайн	34
Шестой ИК-луч на верхней ИК-плате сработал	06	Верхняя ИК-плата 11 офлайн	35
Седьмой ИК-луч на верхней ИК-плате сработал	07	Верхняя ИК-плата 12 офлайн	36
Восьмой ИК-луч на верхней ИК-плате сработал	08	Нижняя ИК-плата 1 офлайн	37
Девятый ИК-луч на верхней ИК-плате сработал	09	Нижняя ИК-плата 2 офлайн	38
Десятый ИК-луч на верхней ИК-плате сработал	10	Нижняя ИК-плата 3 офлайн	39
Одиннадцатый ИК-луч на верхней ИК-плате сработал	11	Нижняя ИК-плата 4 офлайн	40
Двенадцатый ИК-луч на верхней ИК-плате сработал	12	Нижняя ИК-плата 5 офлайн	41
Первый ИК-луч на нижней ИК-плате сработал	13	Нижняя ИК-плата 6 офлайн	42
Второй ИК-луч на нижней ИК-плате сработал	14	Нижняя ИК-плата 7 офлайн	43
Третий ИК-луч на нижней ИК-плате сработал	15	Нижняя ИК-плата 8 офлайн	44
Четвертый ИК-луч на нижней ИК-плате сработал	16	Нижняя ИК-плата 9 офлайн	45

Причина ошибки	№	Причина ошибки	№
Пятый ИК-луч на нижней ИК-плате сработал	17	Нижняя ИК-плата 10 офлайн	46
Шестой ИК-луч на нижней ИК-плате сработал	18	Нижняя ИК-плата 11 офлайн	47
Седьмой ИК-луч на нижней ИК-плате сработал	19	Нижняя ИК-плата 12 офлайн	48
Восьмой ИК-луч на нижней ИК-плате сработал	20	Световая плата офлайн (Вход)	49
Девятый ИК-луч на нижней ИК-плате сработал	21	Световая плата офлайн (Выход)	50
Десятый ИК-луч на нижней ИК-плате сработал	22	ИК-адаптер офлайн (Верхний)	51
Одиннадцатый ИК-луч на нижней ИК-плате сработал	23	ИК-адаптер офлайн (Нижний)	52
Двенадцатый ИК-луч на нижней ИК-плате сработал	24	Исключение шины CAN	53
Верхняя ИК-плата 1 офлайн	25	Не обучается	54
Верхняя ИК-плата 2 офлайн	26	Затор	55
Верхняя ИК-плата 3 офлайн	27	Превышение учебного диапазона	56
Верхняя ИК-плата 4 офлайн	28	Исключение двигателя	57

