Терминал распознавания лиц 607 серии

Руководство пользователя

Руководство пользователя

Настоящее Руководство предназначено для Терминала распознавания лиц.

Название	Модель
Терминал распознавания лиц	DS-K1T607M
	DS-K1T607MF
	DS-K1T607E
	DS-K1T607EF
	DS-K1T607MW
	DS-K1T607MFW
	DS-K1T607PE
	DS-K1T607PEF
	DS-K1T607PMW
	DS-K1T607PMFW
	DS-K1T607TM
	DS-K1T607TMF
	DS-K1T607TE
	DS-K1T607TEF
	DS-K1T607TMW
	DS-K1T607TMFW

Примечание: «W» используется для устройств, поддерживающих Wi-Fi связь, «E» используется для устройств, поддерживающих чтение 125K EM-карт, «M» используется для устройств, поддерживающих чтение 13.56 M M1-карт.

Руководство содержит инструкции по использованию продукта. Программное обеспечение, используемое в продукте, регулируется лицензионным соглашением пользователя, охватывающим этот продукт.

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 марки Hikvision являются собственностью Hikvision и являются зарегистрированными товарными знаками или предметом заявок на них со стороны компании Hikvision и/или ее аффилированных лиц. 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.

Защита данных

Во время использования устройства личные данные будут собираться, храниться и обрабатываться. Для защиты данных разработчики устройств Hikvision включают конфиденциальность в свои основные принципы проектирования. Например, для устройства с функциями распознавания лиц биометрические данные хранятся на вашем устройстве в зашифрованном виде; для устройств, работающих с отпечатками пальцев, сохраняется только шаблон отпечатка пальца, по которому невозможно восстановить изображение отпечатка пальца.

В качестве оператора данных, вам рекомендуется собирать, хранить, обрабатывать и передавать данные в соответствии с применимыми законами и правилами о защите данных, включая, помимо прочего, проведение мер безопасности для защиты личных данных, таких как внедрение разумных административных и физических мер безопасности, проводить периодические обзоры и оценки эффективности ваших мер безопасности.

Регулирующая информация

Информация о FCC

Пожалуйста, обратите внимание, что изменения или модификации, явно не одобренные стороной, ответственной за соответствие, могут лишить пользователя права использовать оборудование.

Соответствие FCC: Это оборудование было проверено и найдено соответствующим регламенту для цифрового устройства Класса B, 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 должно быть установлено и эксплуатироваться как минимум на расстоянии 20 см между излучателем и вашим телом.

Условия FCC

Это устройство соответствует регламенту для цифрового устройства применительно к части 15 Правил FCC. По которому при работе устройства 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

CE

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/EC (директива о батареях): Данный продукт содержит батарею, которую запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Подробная информация о батарее изложена в документации продукта. Батарея отмечена 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 нее в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info

Используйте только источники питания, указанные в руководствах пользователя:

Модель	**Производитель**	**Стандарт**
C2000IC12.0-24P-DE	MOSO Power Supply Technology Co.,Ltd.	CEE
C2000IC12.0-24P-GB	MOSO Power Supply Technology Co.,Ltd.	BS
KPL-040F-VI	Channel Well Technology Co Ltd.	CEE

Инструкции 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: Пренебрежение любым из предупреждений может привести к серьезным травмам или смерти.

Предостережения: Пренебрежение любым из предостережений может привести к травме или повреждению оборудования.

	
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

- 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 высокого 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.
- Биометрические продукты распознавания не на 100% применимы к анти-спуфинг средам. Если вам требуется более высокий уровень безопасности, используйте несколько режимов аутентификации.
- Рабочая температура: от минус 30 до плюс 60 °C.
- Возможна установка в помещении или снаружи помещения. При установке устройства в помещении оно должно находиться на расстоянии не менее 2 метров от источника света и не менее 3 метров от окна или двери. При установке устройства на открытом воздухе, вы должны нанести силиконовый герметик в зону кабельной проводки, чтобы предотвратить попадание капель дождя.
- Уровень защиты: IP65.

Содержание

Глава 1 Обзор

1.1 Представление

Терминал распознавания лиц серии DS-K1T607 является своего рода устройством контроля доступа для распознавания лиц, которое в основном применяется в системах контроля доступа, таких как логистические центры, аэропорты, университетские городки, тревожный центры, жилые помещения и так далее.

1.2 Основные особенности

1.2.1 Особенности DS-K1T607 серии

- 7-дюймовый ЖК-сенсорный экран
- 2МП широкоугольный двойной объектив
- Поддержка регулировки яркости подсветки вручную
- Дистанция распознавания лиц: от 0.3 до 1.5 м
- Рекомендуемая высота для распознавания лиц: от 1.4 до 1.9 м
- Алгоритм глубокого обучения
- Вместимость: 6000 лиц, 5000 отпечатков пальцев и 10000 событий
- Несколько режимов аутентификации
- Продолжительность распознавания лица ≤ 0,5 с/польз.; точность распознавания лиц ≥ 99%
- Управление параметрами устройства, поиск и настройка
- Возможность импорта данных карт и пользователей в устройство через TCP/IP или USB-накопитель
- Автономная работа
- Передает данные Клиентскому ПО по протоколу TCP / IP и сохраняет данные в Клиентском ПО
- Привязка захвата и сохранение захваченных изображений
- Импорт данных в устройство из Клиентского ПО
- Управление, поиск и установка данных устройства после локального входа в устройство
- Подключается к одному внешнему считывателю карт или контроллеру доступа по протоколу RS-485
- Подключается к внешнему контроллеру доступа или Wiegand считывателю карт по протоколу Wiegand
- Подключается к модулю безопасности по протоколу RS-485, чтобы избежать открытия двери при разрушении терминала

- Двустороннее аудио с Клиентским ПО, видеодомофоном и монитором консьержа
- Автоматическая детекция сетевого статуса (ANR)
- Удаленный просмотр в реальном времени при помощи RTSP протокола; режим кодирования: H.264
- NTP, ручная синхронизация времени и автоматическая синхронизация
- Аудио подсказки
- Конструкция включает в себя сторожевой таймер (Watchdog) и контакт несанкционированного вскрытия (тампер)

1.2.2 Особенности DS-K1T607P серии

- 7-дюймовый ЖК-сенсорный экран
- 2МП широкоугольный двойной объектив
- Поддержка регулировки яркости подсветки вручную
- Распознавание лиц в темной среде
- Дистанция распознавания лиц: от 0.3 до 1.5 м
- Рекомендуемая высота для распознавания лиц: от 1.4 до 1.9 м
- Алгоритм глубокого обучения
- Вместимость: 10000 лиц, 5000 отпечатков пальцев и 50000 событий
- Несколько режимов аутентификации
- Продолжительность распознавания лица ≤ 0,5 с/польз.; точность распознавания лиц ≥ 99%
- Управление параметрами устройства, поиск и настройка
- Автономная работа
- Передает данные Клиентскому ПО по протоколу TCP / IP и сохраняет данные в Клиентском ПО
- Привязка захвата и сохранение захваченных изображений
- Импорт данных в устройство из Клиентского ПО
- Управление, поиск и установка данных устройства после локального входа в устройство
- Подключается к одному внешнему считывателю карт или контроллеру доступа по протоколу RS-485
- Подключается к внешнему контроллеру доступа или Wiegand считывателю карт по протоколу Wiegand
- Подключается к модулю безопасности по протоколу RS-485, чтобы избежать открытия двери при разрушении терминала
- Двустороннее аудио с Клиентским ПО, видеодомофоном и монитором консьержа
- Автоматическая детекция сетевого статуса (ANR)
- Удаленный просмотр в реальном времени при помощи RTSP протокола; режим кодирования: H.264

- NTP, ручная синхронизация времени и автоматическая синхронизация
- Аудио подсказки
- Конструкция включает в себя сторожевой таймер (Watchdog) и контакт несанкционированного вскрытия (тампер)

1.2.3 Особенности DS- K1T607T серии

- 7-дюймовый ЖК-сенсорный экран
- 2МП широкоугольный двойной объектив
- Поддержка регулировки яркости подсветки вручную
- Распознавание лиц в темной среде
- Дистанция распознавания лиц: от 0.3 до 1.5 м
- Рекомендуемая высота для распознавания лиц: от 1.4 до 1.9 м
- Алгоритм глубокого обучения
- Вместимость: 20000 лиц, 5000 отпечатков пальцев и 50000 событий
- Несколько режимов аутентификации
- Продолжительность распознавания лица ≤ 0,5 с/польз.; точность распознавания лиц ≥ 99%
- Управление параметрами устройства, поиск и настройка
- Возможность импорта данных карт и пользователей в устройство через TCP/IP или USB-накопитель
- Автономная работа
- Передает данные Клиентскому ПО по протоколу TCP / IP и сохраняет данные в Клиентском ПО
- Привязка захвата и сохранение захваченных изображений
- Импорт данных в устройство из Клиентского ПО
- Управление, поиск и установка данных устройства после локального входа в устройство
- Подключается к одному внешнему считывателю карт или контроллеру доступа по протоколу RS-485
- Подключается к внешнему контроллеру доступа или Wiegand считывателю карт по протоколу Wiegand
- Подключается к модулю безопасности по протоколу RS-485, чтобы избежать открытия двери при разрушении терминала
- Двустороннее аудио с Клиентским ПО, видеодомофоном и монитором консьержа
- Автоматическая детекция сетевого статуса (ANR)
- Удаленный просмотр в реальном времени при помощи RTSP протокола; режим кодирования: H.264
- NTP, ручная синхронизация времени и автоматическая синхронизация
- Аудио подсказки

- Конструкция включает в себя сторожевой таймер (Watchdog) и контакт несанкционированного вскрытия (тампер)

Глава 2 Внешний вид

Для получения подробной информации о терминале распознавания лиц серии DS-K1T607 смотрите следующий рисунок:

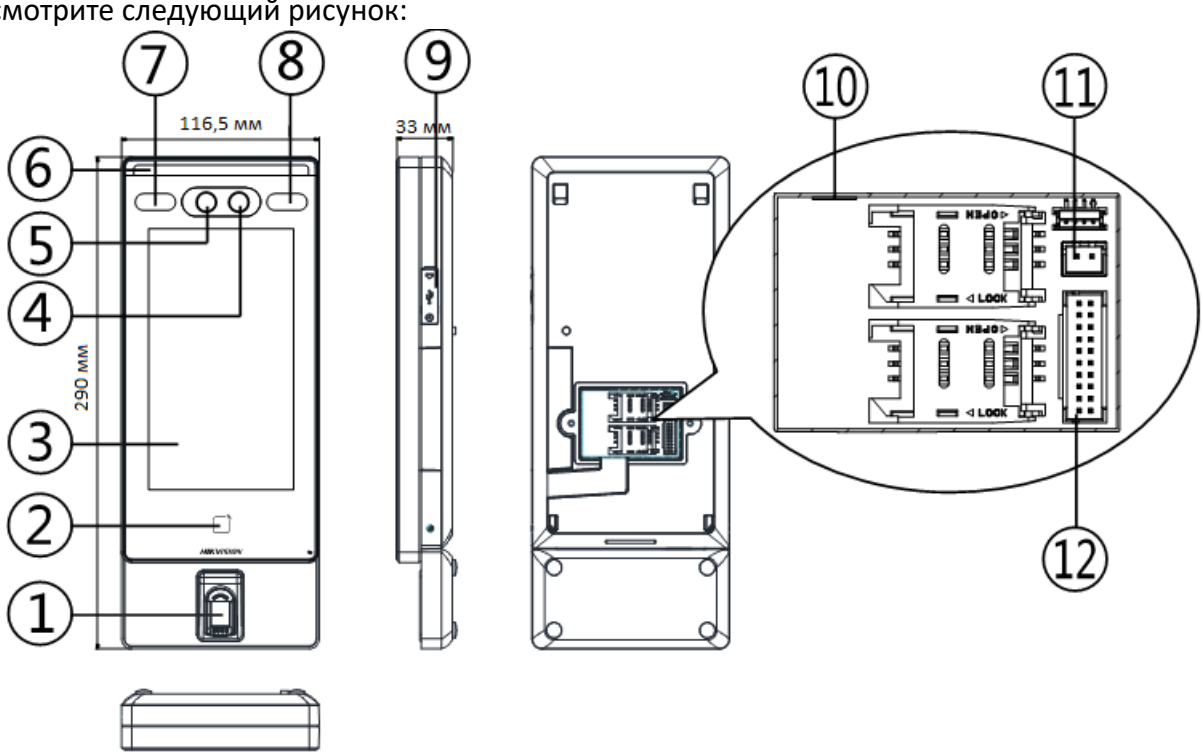


Таблица 2-1 Описание терминала распознавания лиц DS-K1T607 серии

№	Название	Описание
1	Модуль отпечатков пальцев	Сканирование отпечатков пальцев. ***Примечание:*** Некоторые модели не поддерживают функцию распознавания отпечатков пальцев.
2	Область проводки карт	Проведите карту в этой области.
3	Экран	7-дюймовый сенсорный ЖК-экран.
4	Камера (ИК-свет)	ИК-камера для записи или захвата видео или изображений с ИК-подсветкой.
5	Камера (Белый свет)	Камера с белой подсветкой для записи видео или изображений.

6	Вспомогательная подсветка (Белый свет)	Вспомогательная подсветка для камеры с белой подсветкой.
7	Вспомогательная подсветка (ИК-свет)	Вспомогательная подсветка для ИК-камеры.
8	Вспомогательная подсветка (ИК-свет)	Вспомогательная подсветка для ИК-камеры.
9	USB-интерфейс	Подключение USB флеш-накопителя.
10	Сетевой интерфейс	Подключение к Ethernet.
11	Интерфейс питания	Подключение к источнику питания.
12	Клеммы	Подключение к другим внешним устройствам, включая считыватель карт RS-485, считыватель карт Wiegand, дверной замок, тревожный вход, тревожный выход и т. д.

Глава 3 Установка

3.1 Среда установки

- При установке в помещении устройство должно находиться на расстоянии не менее 2 м от источника света и не менее 3 м от окна или двери.
- При установке устройства на открытом воздухе, вы должны нанести силиконовый герметик в зону кабельной проводки, чтобы предотвратить попадание капель дождя.
- Убедитесь, что уровень освещенности в помещении превышает 100 лк.

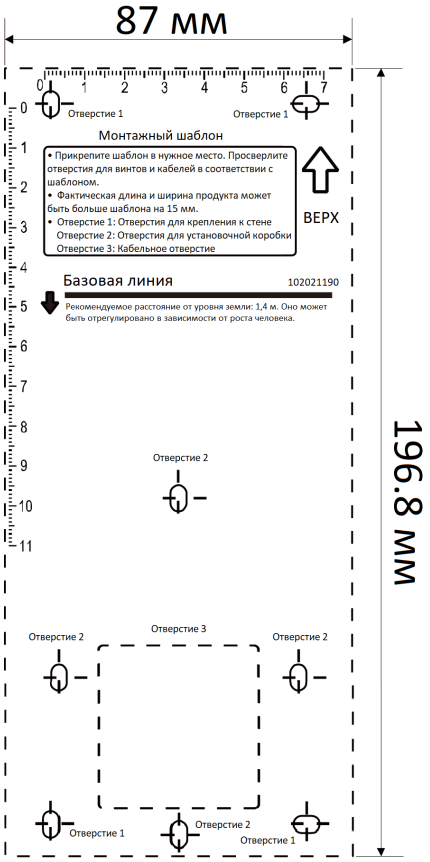
Примечания:

- Для получения подробной информации о среде установки смотрите *Приложение С Советы по среде установки*.
- Убедитесь, что выход внешнего источника питания соответствует LPS.

3.2 Установка с использованием установочной коробки

Шаги:

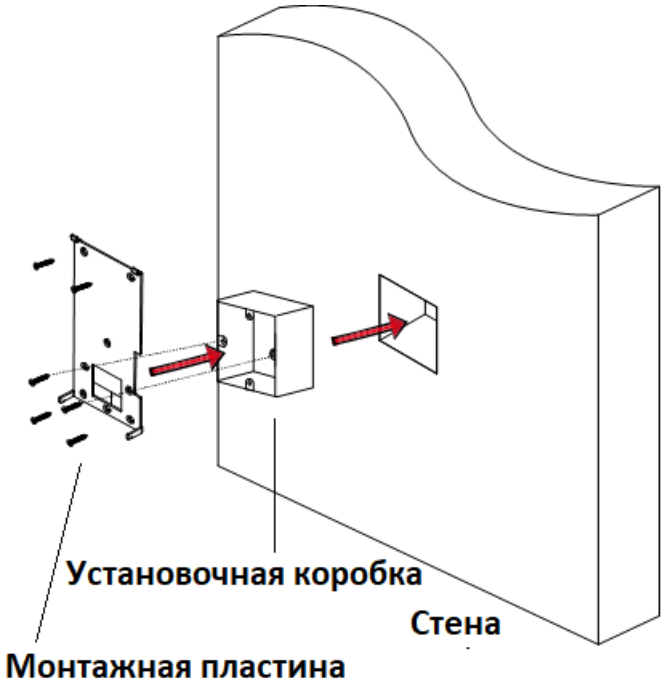
1. В соответствии с базовой линией на монтажном шаблоне наклейте монтажный шаблон на стену или другую поверхность на 1,4 метра выше уровня земли.



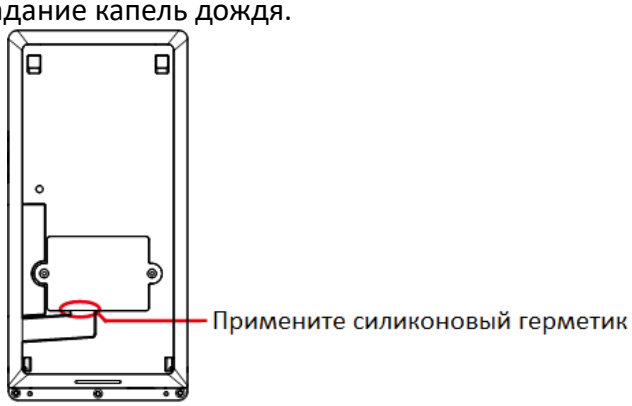
2. Просверлите отверстия в стене или другой поверхности в соответствии с монтажным

шаблоном и установите установочную коробку.

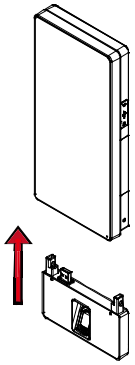
3. Используйте два входящих в комплект винта (4_KA4 × 22-SUS) для закрепления монтажной пластины на установочной коробке.
4. Используйте еще четыре прилагаемых винта, чтобы закрепить монтажную пластину на стене.



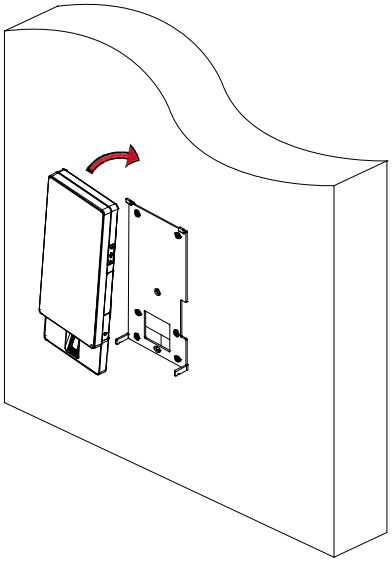
5. Проложите кабель через кабельное отверстие на монтажной пластине и подключите к кабелям соответствующих внешних устройств.
   Примечание: Нанесите силиконовый герметик в зоне кабельной проводки, чтобы предотвратить попадание капель дождя.



6. (Опционально) Вставьте модуль отпечатков пальцев в отверстия в нижней части основного блока.

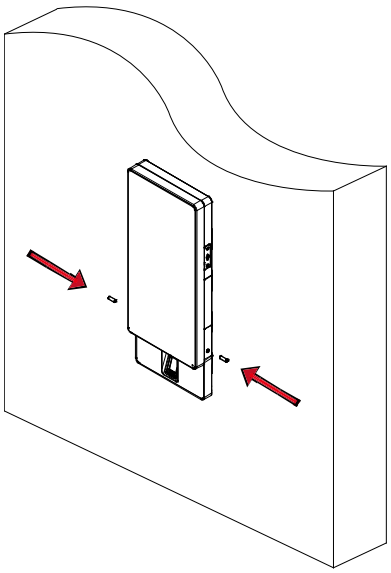


7. Совместите устройство с монтажной пластиной и подвесьте устройство на ней.



Убедитесь, что два штырька на каждой стороне монтажной пластины находятся в отверстиях на задней панели устройства.

8. Используйте два прилагаемых винта (SC-M4 × 12TP10-SUS), чтобы закрепить устройство на монтажной пластине.



Примечания:

- Высота установки является рекомендуемой величиной. Ее можно изменить в

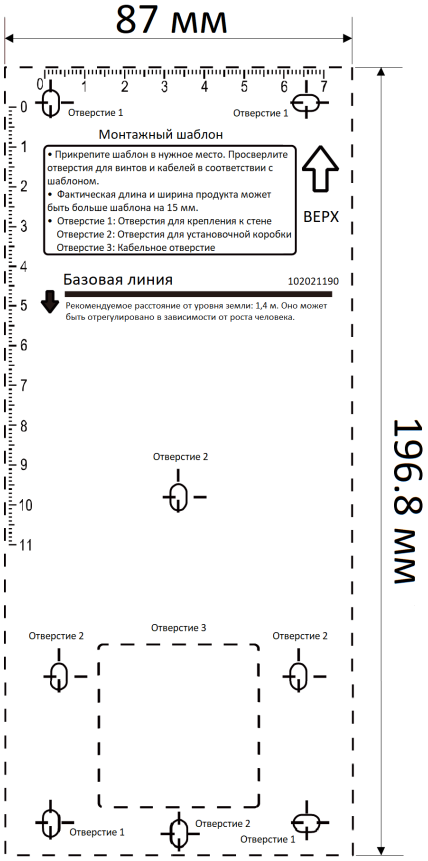
соответствии с фактическими потребностями.

- Чтобы упростить процесс установки, просверлите в монтажной поверхности отверстия, используя прилагаемый шаблон.

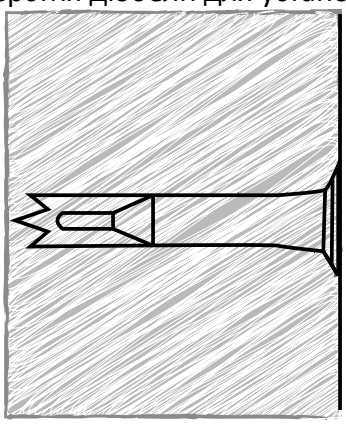
3.3 Установка без установочной коробки

Шаги:

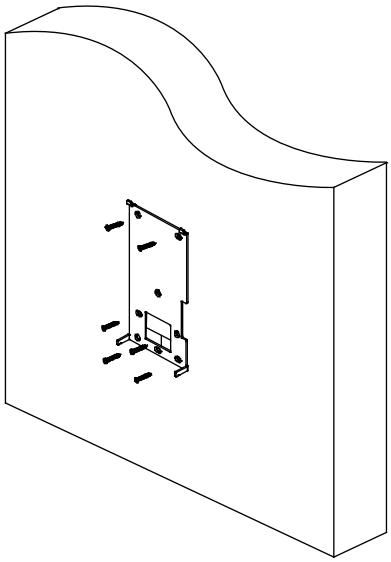
1. В соответствии с базовой линией на монтажном шаблоне наклейте монтажный шаблон на стену или другую поверхность на 1,4 метра выше уровня земли.



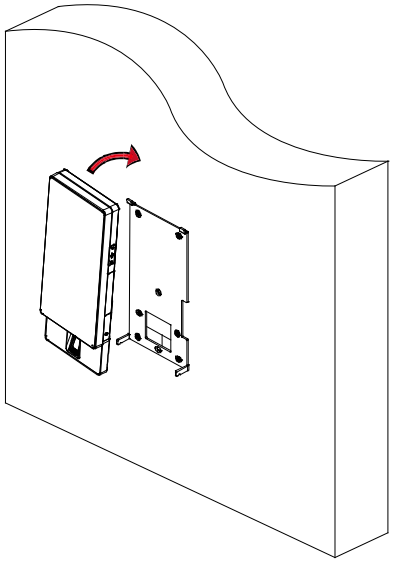
2. Просверлите 6 отверстий в стене или другой поверхности в соответствии с Отверстием 1 и Отверстием 2 на монтажном шаблоне.
3. Вставьте в просверленные отверстия дюбели для установочных винтов.



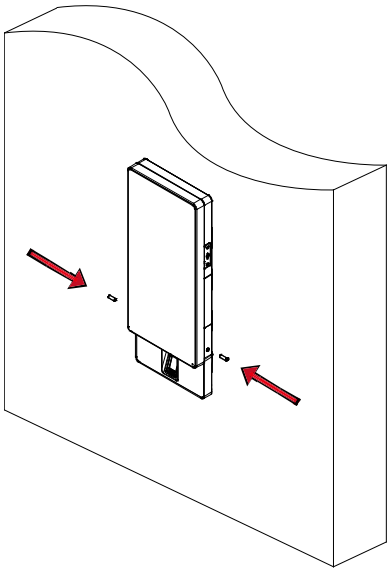
4. Совместите 6 отверстий с отверстиями в монтажной пластине, а затем закрепите ее при помощи 6 винтов.



5. Проложите кабель через кабельное отверстие на монтажной пластине и подключите к кабелям соответствующих внешних устройств.
   Примечание: Нанесите силиконовый герметик в зоне кабельной проводки, чтобы предотвратить попадание капель дождя.
6. Совместите устройство с монтажной пластиной и подвесьте устройство на ней.



   Убедитесь, что два штырька на каждой стороне монтажной пластины находятся в отверстиях на задней панели устройства.
7. Используйте два прилагаемых винта (SC-M4 × 12TP10-SUS), чтобы закрепить устройство на монтажной пластине.



Примечания:

- Высота установки является рекомендуемой величиной. Ее можно изменить в соответствии с фактическими потребностями.
- Чтобы упростить процесс установки, просверлите в монтажной поверхности отверстия, используя прилагаемый шаблон.

Глава 4 Подключение клемм

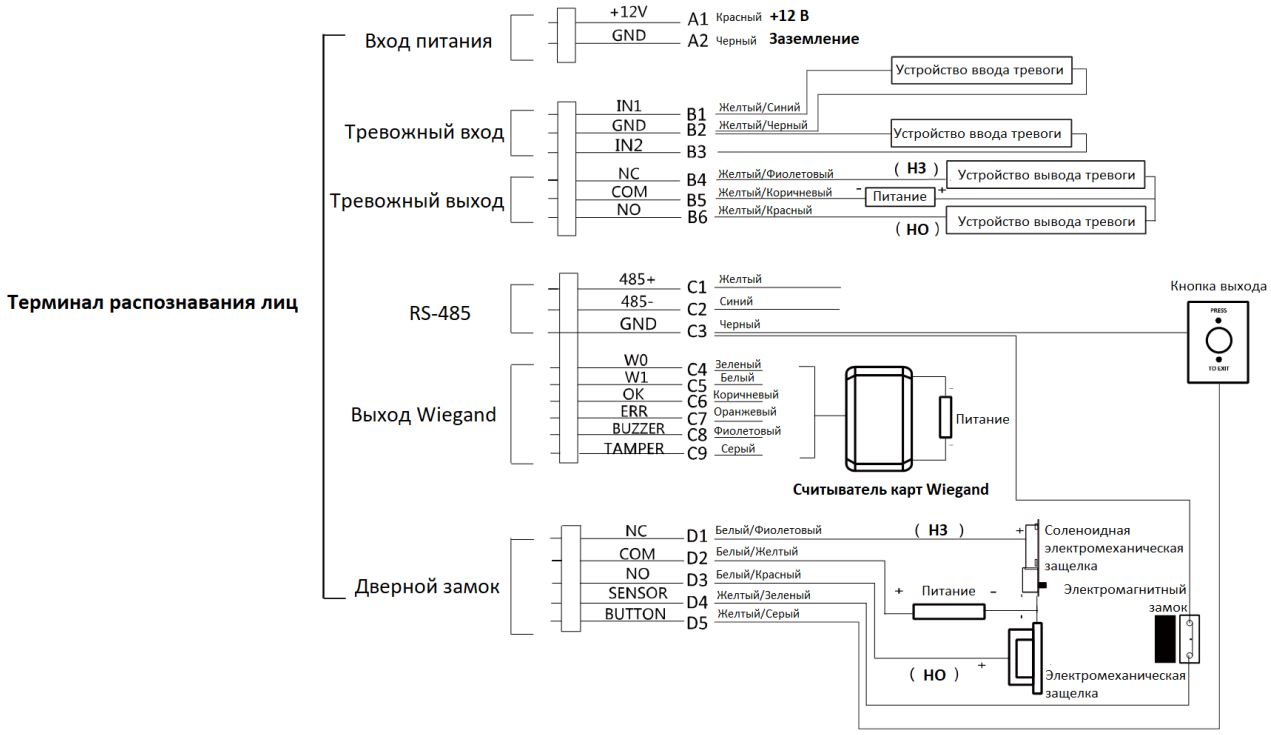
Вы можете подключить клемму RS-485 к считывателю карт RS-485, клеммы NC и COM — к замку двери, клемму SENSOR (ДАТЧИК) – к электромагнитному датчику двери, клемму BUTTON/GND (КНОПКА/ЗАЗЕМЛЕНИЕ) – к кнопке выхода, подключите клеммы тревожного входа и выхода к устройствам ввода/вывода тревоги, клемму Wiegand — к считывателю карт Wiegand или контроллеру доступа.

Если подключить клемму Wiegand к контроллеру доступа, терминал распознавания лиц сможет передавать на него информацию об аутентификации, чтобы контроллер доступа определял возможность открытия двери.

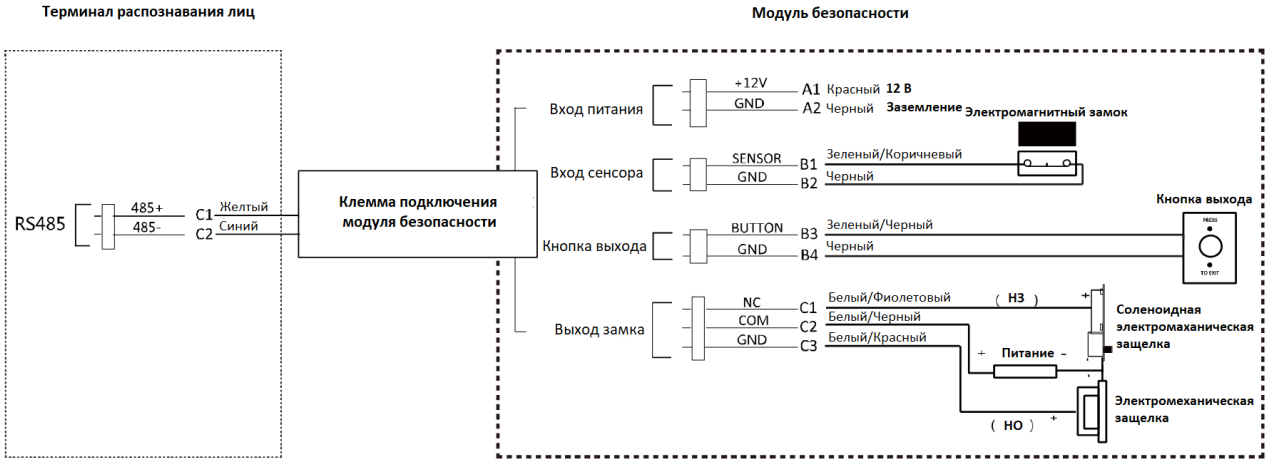
Примечания:

- Если вы используете кабели сечением 1,0 мм, вы должны использовать импульсный источник питания 12 В. А расстояние между источником питания и устройством должно быть не более 20 м.
- Если вы используете кабели сечением 1.5 мм, вы должны использовать импульсный источник питания 12 В. А расстояние между источником питания и устройством должно быть не более 30 м.
- Если вы используете кабели сечением 2.0 мм, вы должны использовать импульсный источник питания 12 В. А расстояние между источником питания и устройством должно быть не более 40 м.

Схема подключения представлена ниже:



Также можно подключить терминал к модулю безопасности. Схема подключения представлена ниже:



Примечание: Модуль безопасности необходимо отдельно подключить к внешнему источнику питания.

Глава 5 Активация устройства

Цель:

Вам необходимо активировать терминал перед его использованием.

Поддерживается активация через само устройство, 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 устройство

Если устройство еще не активировано, оно отобразит страницу активации после включения питания.

Шаги:

1. Нажмите на поле **Password** («Пароль») и создайте пароль.
2. Нажмите на поле **Confirm** («Подтверждение») и введите пароль снова.
3. Нажмите **Next** («Далее») и устройство будет активировано.

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.*

5.2 Активация через ПО SADP

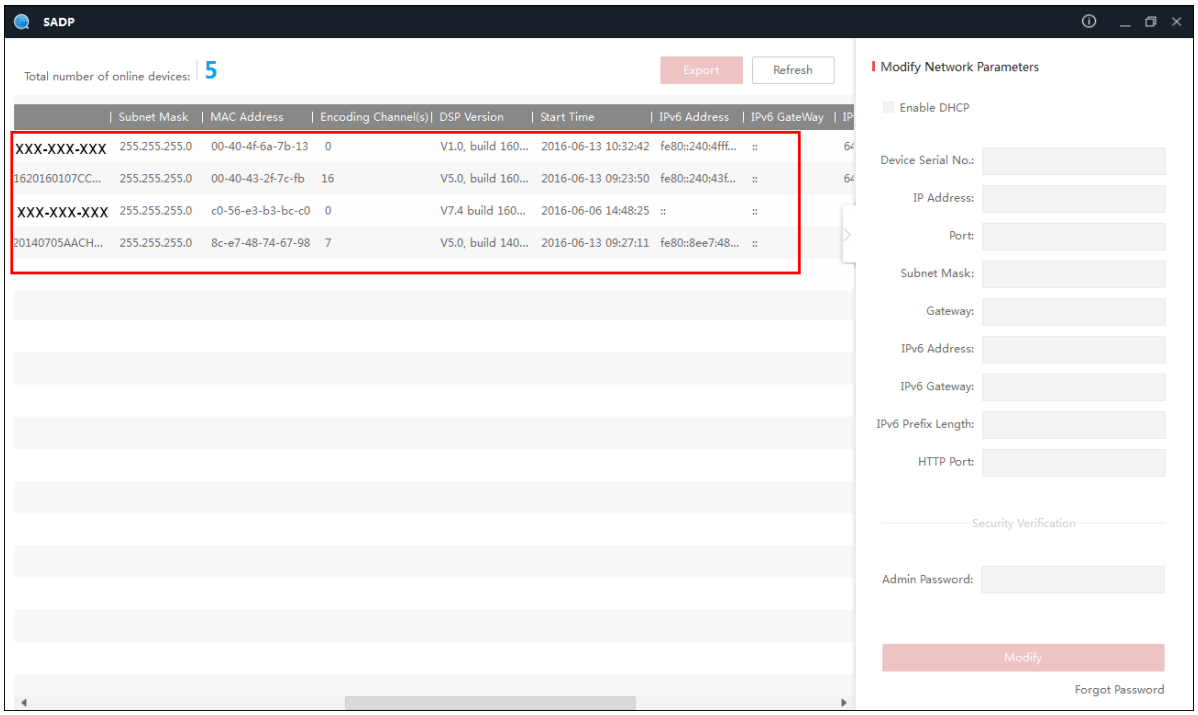
Цель:

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:

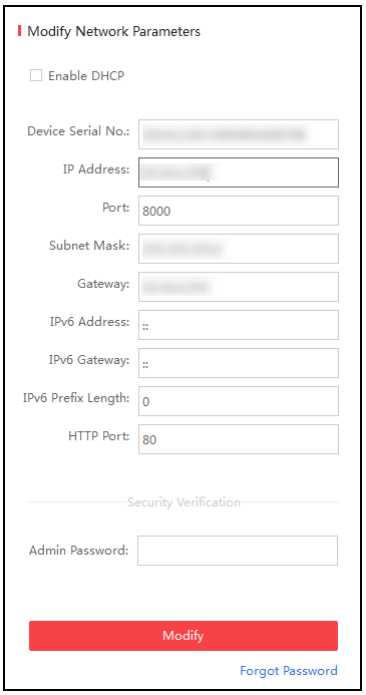
1. Запустите ПО SADP для поиска онлайн-устройств.
2. Проверьте статус устройства в списке устройств и выберите неактивное устройство.



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.

5.3 Активация при помощи Клиентского ПО

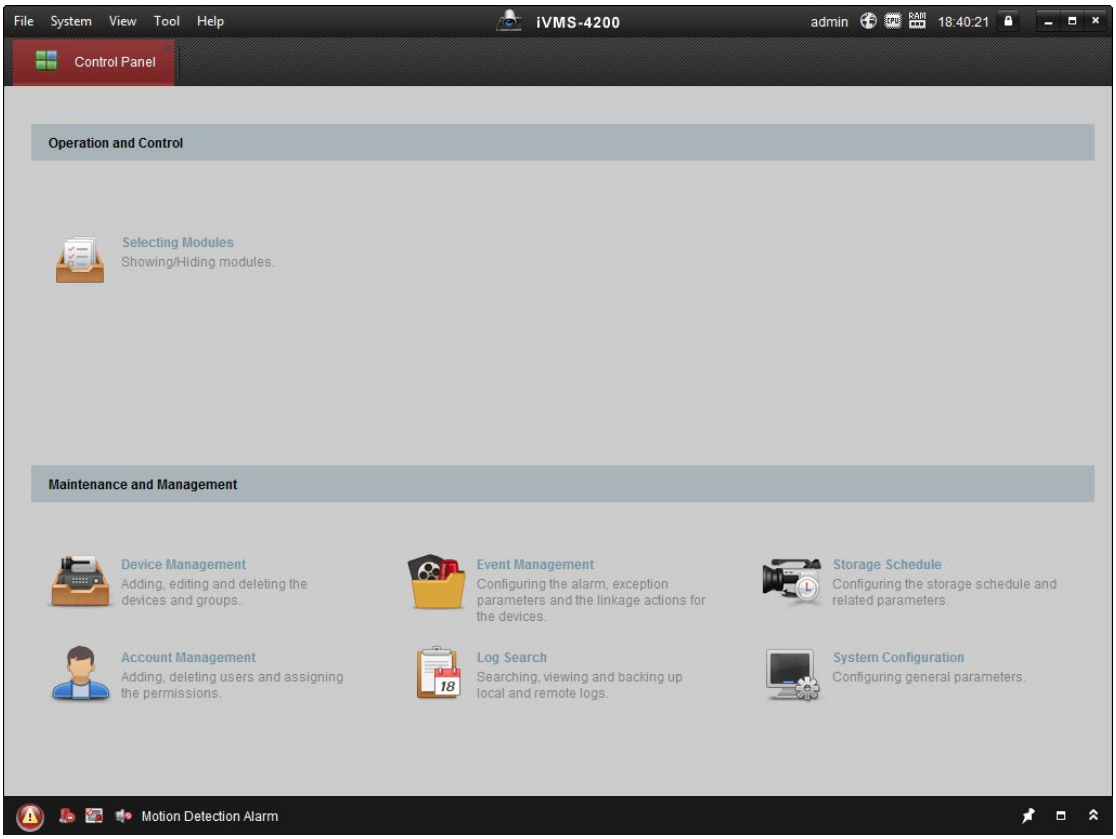
Цель:

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

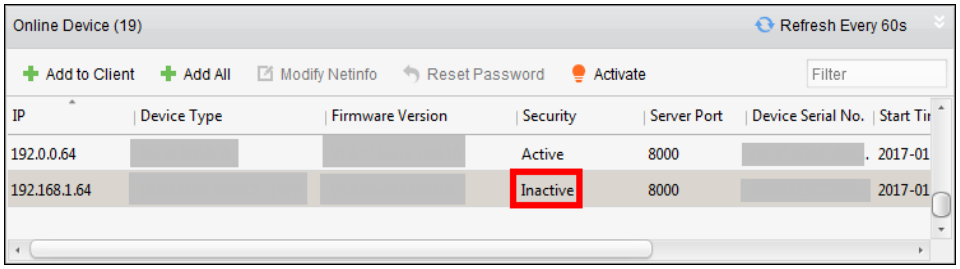
Получите Клиентское программное обеспечение с прилагаемого диска или на официальном сайте и установите программное обеспечение в соответствии с подсказками. Выполните следующие действия для активации устройства.

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.



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»).

<u>РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ</u> – *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.

После активации вы попадете на начальную страницу.

Глава 6 Основные операции

Цель:

После входа в устройство вы сможете управлять пользователями, устанавливать параметры связи, устанавливать параметры контроля доступа, устанавливать параметры системы, управлять данными, управлять запросом журнала, устанавливать время, импортировать и выводить данные, поддерживать хранение данных и просматривать информацию об устройстве.

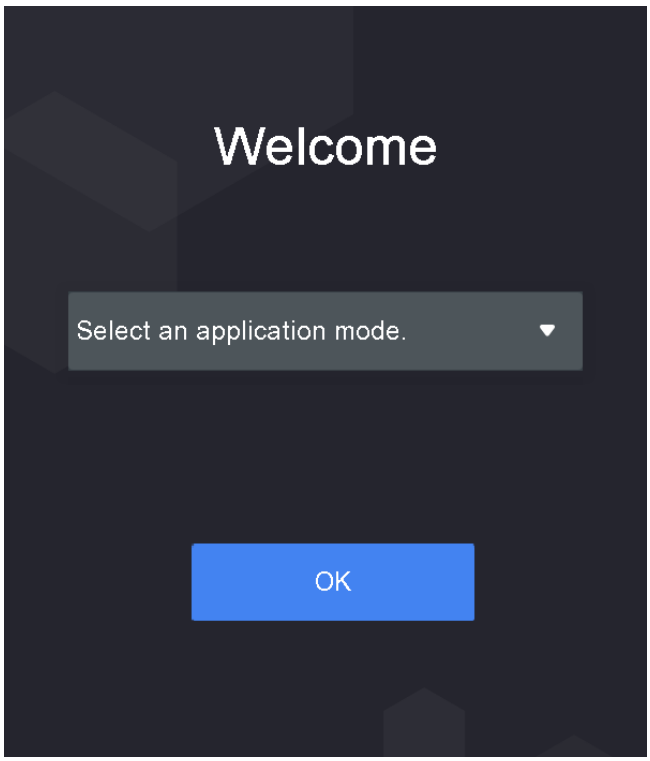
6.1 Настройки режима применения

Цель:

После активации устройства, вы должны выбрать режим применения для лучшего использования устройства.

Шаги:

1. На начальной странице выберите режим **Indoor** («В помещении») или **Others** («Другие») из выпадающего списка.



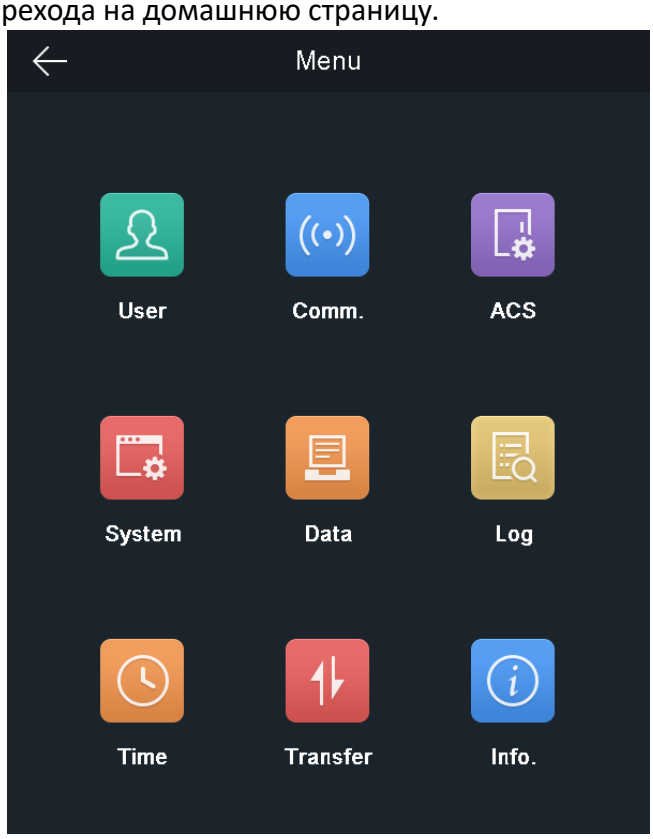
2. Нажмите **OK** для сохранения настроек.

   Примечание: Вы также можете изменить настройки в *Разделе 6.3.2 Настройки системы*.

6.2 Вход в систему

Шаги:

1. На начальной странице нажмите экран на 3 секунды, чтобы перейти на страницу **Enter Administrative Backend** («Вход в административную часть»).
2. Нажмите на поле **Password** («Пароль») и введите пароль активации устройства.
   Примечание: Пароль здесь – это пароль активации.
3. Нажмите **OK** для перехода на домашнюю страницу.



Примечания:

- Устройство будет заблокировано на 30 минут после 5 неудачных попыток ввода пароля.
- Для получения подробной информации о настройке режима аутентификации администратора смотрите *Раздел 6.4.1 Добавление пользователя*.

6.3 Настройки общих параметров

6.3.1 Настройки связи

Цель:

Вы можете установить сетевые параметры, параметры RS-485, параметры Wi-Fi и Wiegand параметры на странице настройки связи.

Нажмите **Comm.** («Настройки связи») на домашней странице для перехода в соответствующее меню.

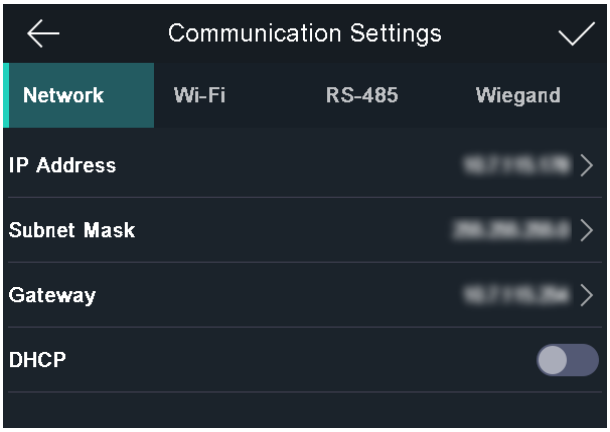
Настройка сетевых параметров

Цель:

Вы можете установить сетевые параметры устройства, включая IP-адрес, шлюз и маску подсети.

Шаги:

1. На странице **Communication Settings** («Настройки связи») нажмите **Network** («Сеть») для перехода на соответствующую вкладку.



2. Задайте параметры сетевого интерфейса, включая **IP address** («IP-адрес»), **Subnet mask** («Маска подсети») и **Gateway** («Шлюз»).
3. Нажмите для выхода со страницы и сохранения параметров.

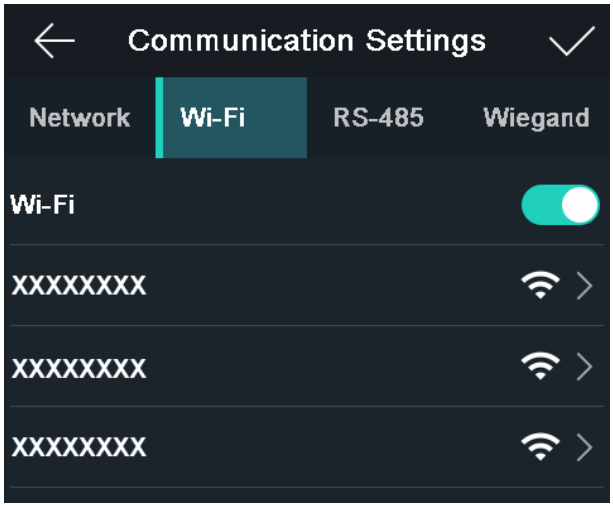
Настройка параметров Wi-Fi

Цель:

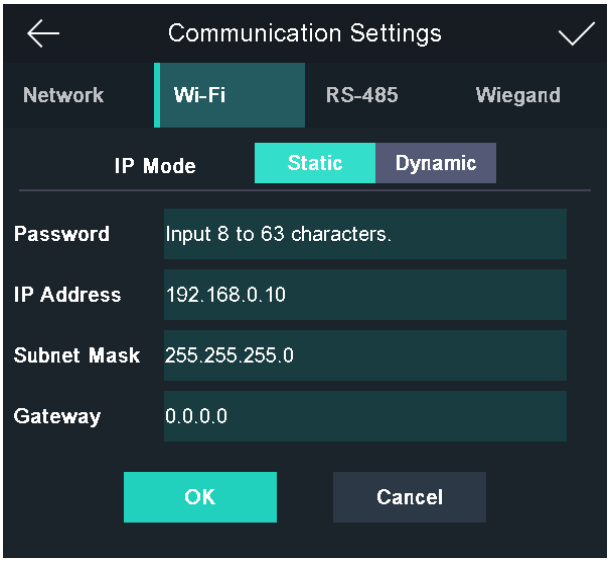
Вы можете включить функцию Wi-Fi и задать связанные параметры.

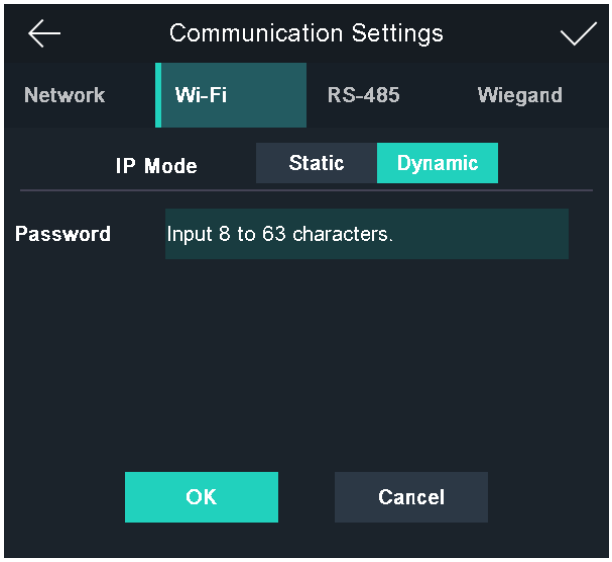
Шаги:

1. На странице **Communication Settings** («Настройки связи») нажмите **Wi-Fi** для перехода на соответствующую вкладку.
2. Нажмите для включения функции Wi-Fi.
   Иконка превратится в , и все найденные Wi-Fi сети будут отображены в списке.



3. Выберите Wi-Fi сеть из списка, чтобы перейти на страницу настроек параметров Wi-Fi.
4. Выберите **IP mode** («IP режим»).
   Если вы выберете **Static** («Статический»), вам необходимо будет ввести Wi-Fi пароль, IP-адрес, маску подсети и шлюз.
   Если вы выберете **Dynamic** («Динамический»), вам необходимо будет ввести Wi-Fi пароль.





Примечание: В Wi-Fi пароле допускаются цифры, заглавные буквы, строчные буквы и специальные символы.

5. Нажмите **OK**, чтобы сохранить настройки и вернуться на вкладку Wi-Fi.
6. Нажмите ✓ для сохранения параметров Wi-Fi и возврата на домашнюю страницу.

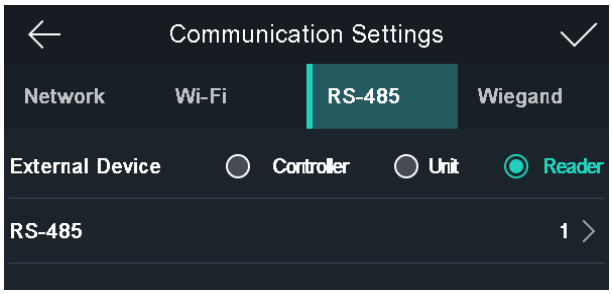
Настройка параметров RS-485

Цель:

Терминал распознавания лиц может подключаться к внешнему контроллеру доступа, модулю безопасности или считывателю карт через RS-485.

Шаги:

1. На странице **Communication Settings** («Настройки связи») нажмите **RS-485** для перехода на соответствующую вкладку.



2. Выберите внешнее устройство в соответствии с вашими потребностями.
   Примечание: В опции **«Controller»** («Контроллер») подразумевается контролер доступа, в опции **«Unit»** («Модуль») – модуль безопасности, в опции **«Reader»** («Считыватель») -

считыватель карт.

3. На странице **Communication Settings** («Настройки связи») выберите RS-485 адрес.
4. Нажмите для сохранения параметров RS-485 и возврата на домашнюю страницу.

Примечание: Если вы измените внешнее устройство и сохраните параметры устройства, оно автоматически перезагрузится.

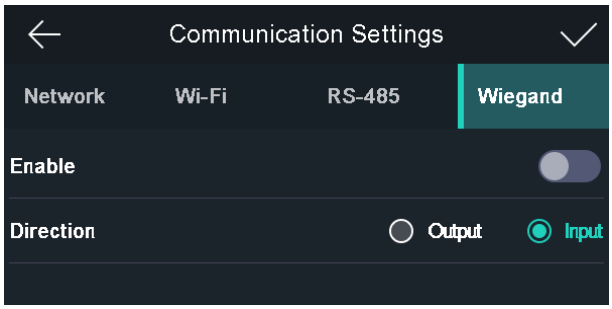
Настройка параметров Wiegand

Цель:

Вы можете установить направление Wiegand передачи.

Шаги:

1. На странице **Communication Settings** («Настройки связи») нажмите **Wiegand** для перехода на соответствующую вкладку.



2. Нажмите на ползунок, чтобы включить функцию Wiegand.
3. Выберите направление передачи.

   Направление передачи:

   - **Output** («Выход»): Терминал распознавания лиц может подключиться к внешнему контроллеру доступа. И два устройства будут передавать номера карт через Wiegand 34.
   - **Input** («Вход»): Терминал распознавания лиц может подключиться к Wiegand считывателю карт.
4. Нажмите для сохранения параметров Wiegand и возврата на домашнюю страницу.

6.3.2 Настройки системы

Цель:

На странице **System Settings** («Настройки системы») вы можете установить основные параметры системы, параметры лиц, параметры отпечатков пальцев и обновить прошивку.

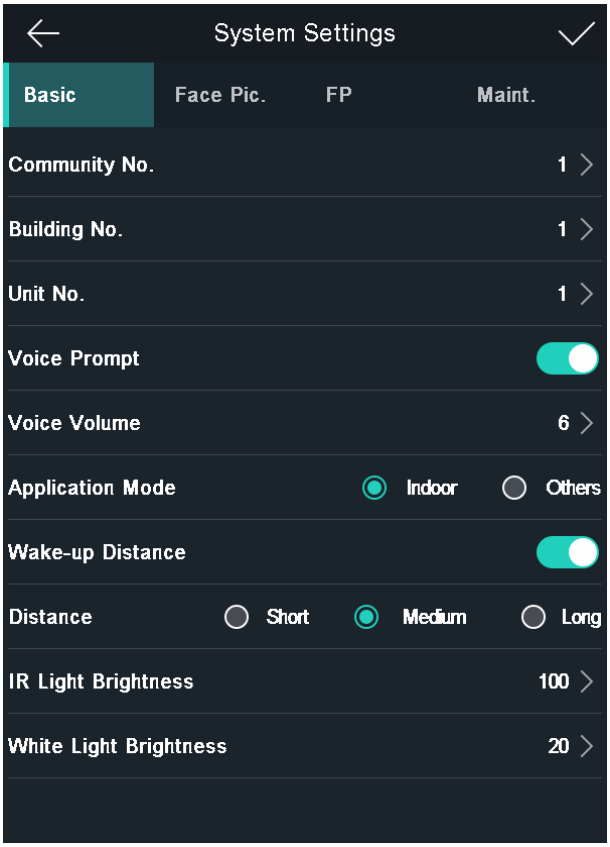
На домашней странице нажмите кнопку **System** («Система») для перехода на страницу **System Settings** («Настройки системы»).

Настройка основных параметров

Цель:

Вы можете установить номер микрорайона, номер здания, номер блока, голосовые

подсказки, громкость голосовых подсказок, режим применения, расстояние пробуждения, яркость ИК-подсветки и яркость белой подсветки.



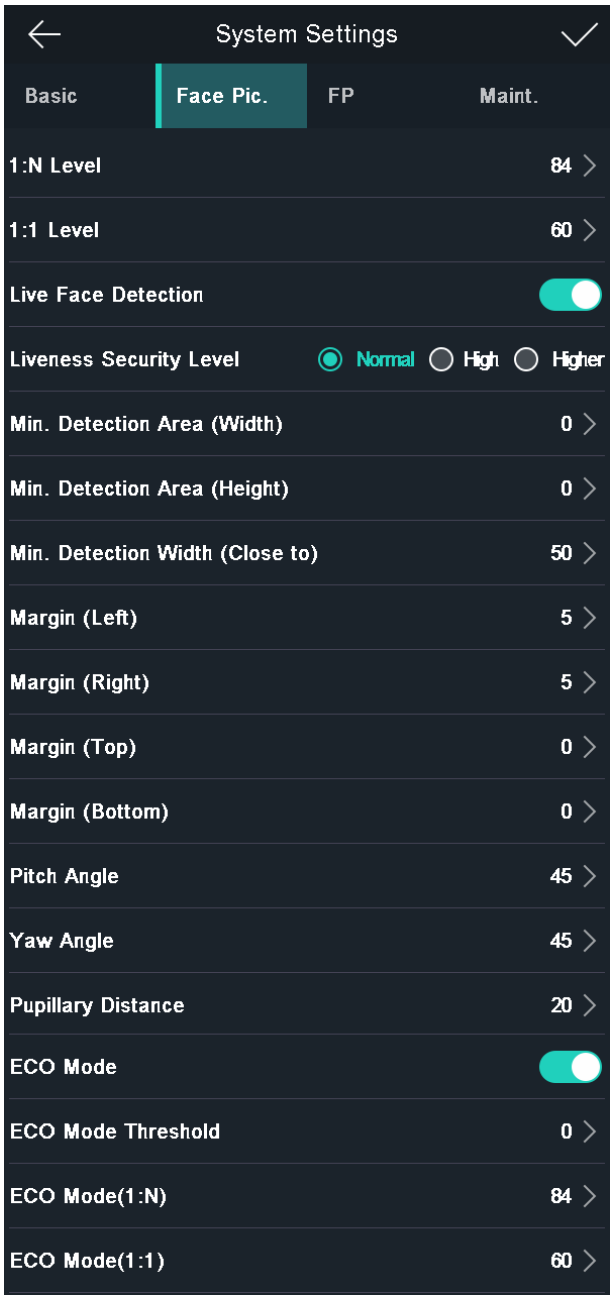
Название параметра	Описание
Community No. («№ микрорайона»)	Задайте № микрорайона, в котором установлено устройство
Building No. («№ здания»)	Задайте № здания, в котором установлено устройство.
Unit No. («№ блока»)	Задайте № блока, в котором установлено устройство.
Voice Prompt («Голосовые подсказки»)	Нажмите  или  для отключения или включения голосовых подсказок.
Voice Volume («Громкость голоса»)	Регулировка громкости аудио подсказок. Чем больше значение, тем выше громкость.
Application Mode («Режим применения»)	Вы можете выбрать либо **Others** («Другие»), либо **Indoor** («Внутри помещения») в зависимости от реальной обстановки.
Wake-up Distance («Расстояние пробуждения»)	Пробуждение означает смену состояния устройства со спящего режима на режим аутентификации при приближении к нему человека или объекта. Расстояние пробуждения означает максимальное расстояние для пробуждения устройства.

	Примечание: Обратитесь к *Приложению D Связь между расстоянием пробуждения и окружающей средой,* чтобы увидеть связь между расстоянием пробуждения и окружающей средой.
IR Light Brightness («Яркость ИК-подсветки»)	Установите яркость ИК-подсветки, когда она включена.
White Light Brightness («Яркость белой подсветки»)	Установите яркость белой вспомогательной подсветки. Яркость настраивается в диапазоне от 0 до 100. «0» означает, что белая вспомогательная подсветка выключена. «1» - самая темная, «100» - наиболее яркая.

Настройка параметров лиц

Цель:

Вы можете установить **1:N (Security) Level** («Уровень 1:N (Безопасность)»), **1:1 (Security) Level** («Уровень 1:1 (Безопасность)»), **Live Face Detection** («Детекция живого лица»), **Liveness Security Level** («Уровень безопасности живого лица»), **Min. Detection Area (Width)** («Мин. область детекции (ширина)»), **Min. Detection Area (Height)** («Мин. область детекции (высота)»), **Min. Detection Width (Close to)** («Мин. ширина детекции (Близость к)»), **Margin (Left)** («Отступ (Левый)»), **Margin (Top)** («Отступ (Верхний)»), **Margin (Right)** («Отступ (Правый)»), **Margin (Bottom)** («Отступ (Нижний)»), **Pitch Angle** («Угол наклона»), **Yaw Angle** («Угол поворота»), **Pupillary Distance** («Межзрачковое расстояние») и **ECO mode** («ЭКО режим»).


System Settings
Basic
Face Pic.
FP
Maint.
1:N Level 84
1:1 Level 60
Live Face Detection
Liveness Security Level Normal High Higher
Min. Detection Area (Width) 0
Min. Detection Area (Height) 0
Min. Detection Width (Close to) 50
Margin (Left) 5
Margin (Right) 5
Margin (Top) 0
Margin (Bottom) 0
Pitch Angle 45
Yaw Angle 45
Pupillary Distance 20
ECO Mode
ECO Mode Threshold 0
ECO Mode(1:N) 84
ECO Mode(1:1) 60

Параметр	Описание
1:N (Security) Level («Уровень 1:N (Безопасность)»)	Установите порог соответствия изображения лица при аутентификации в режиме **1:N matching** («Соответствие 1:N»). Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 84.
1:1 (Security) Level («Уровень 1:1 (Безопасность)»)	Установите порог соответствия изображения лица при аутентификации в режиме **1:1 matching** («Соответствие 1:1»). Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 75.
Live Face Detection («Детекция живого лица»)	Включите или отключите функцию детекции живого лица. При включении функции устройство может распознать, является ли человек живым или нет. ***Примечание:*** Биометрические продукты распознавания не на 100% применимы к анти-спуфинг средам. Если вам

Параметр	Описание
	требуется более высокий уровень безопасности, используйте несколько режимов аутентификации.
Liveness Security Level («Уровень безопасности живого лица»)	После включения функции **Live Face Detection** («Детекция живого лица»), вы можете установить уровень безопасности при выполнении аутентификации лица в реальном времени.
Min. Detection Area (Width) («Мин. область детекции (ширина)»)	Когда расстояние между камерой и пользователем большое, параметр представляет минимальный процент ширины лица в общей ширине области распознавания. При аутентификации фактический процент ширины лица должен быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям. Рекомендуемое значение: 14
Min. Detection Area (Height) («Мин. область детекции (высота)»)	Когда расстояние между камерой и пользователем большое, параметр представляет минимальный процент высоты лица в общей высоте области распознавания. При аутентификации фактический процент высоты лица должен быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям. Рекомендуемое значение: 12
Min. Detection Width (Close to) («Мин. ширина детекции (Близость к)»)	Когда расстояние между камерой и пользователем маленькое, параметр представляет минимальный процент ширины лица в общей ширине области распознавания. При аутентификации фактический процент ширины лица должен быть больше заданного значения. В этом состоянии устройство не обнаружит других параметров.
Margin (Left) («Отступ (Левый)»)	Расстояние от левого края лица до левого края области распознавания. При аутентификации фактическое расстояние должно быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям.
Margin (Top) («Отступ (Верхний)»)	Расстояние от верхнего края лица до верхнего края области распознавания. При аутентификации фактическое расстояние должно быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям

Параметр	Описание
Margin (Right) («Отступ (Правый)»)	Расстояние от правого края лица до правого края области распознавания. При аутентификации фактическое расстояние должно быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям.
Margin (Bottom) («Отступ (Нижний)»)	Расстояние от нижнего края лица до нижнего края области распознавания. При аутентификации фактическое расстояние должно быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям.
Pitch Angle («Угол наклона»)	Максимальный угол наклона при аутентификации лиц. По умолчанию угол составляет 30°.
Yaw Angle («Угол поворота»)	Максимальный угол поворота при аутентификации лиц. По умолчанию угол составляет 20°.
Pupillary Distance («Межзрачковое расстояние»)	Минимальное расстояние между двумя зрачками при распознавании лица. Фактическое значение должно быть больше заданного значения. По умолчанию, расстояние - 40.
ECO Mode («ЭКО режим»)	После включения ЭКО режима устройство будет использовать ИК-камеру для аутентификации лиц в условиях низкой освещенности или в темноте. И вы можете установить порог ЭКО режима, ЭКО режим (1:N) и ЭКО режим (1:1).
ECO Mode Threshold («Порог ЭКО режима»)	При включении ЭКО режима вы можете установить порог ЭКО режима. Чем больше значение, тем легче устройство переходит в ЭКО режим. Доступный диапазон: от 0 до 8.
ECO Mode (1:N) («ECO режим (1:N)»)	Установите порог совпадения при аутентификации в ЭКО режиме 1:N. Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 84.
ECO Mode (1:1) («ECO режим (1:1)»)	Установите порог совпадения при аутентификации в ЭКО режиме 1:1. Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 75.

Примечания:

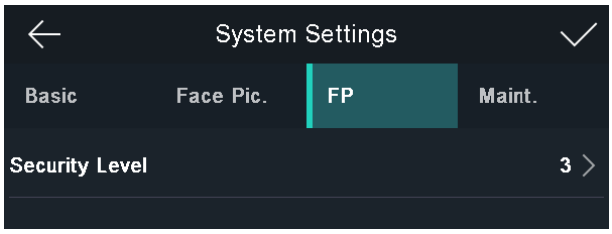
- Значение левого отступа и правого отступа должно быть меньше 100.
- Значение верхнего отступа и нижнего отступа должно быть меньше 100.

Настройка параметров отпечатков пальцев

Цель:

Вы можете установить уровень безопасности отпечатков пальцев в этом разделе.

Примечание: Только устройство с функцией сканирования отпечатков пальцев поддерживает функции, связанные с отпечатками пальцев.



Security Level («Уровень безопасности»): Вы можете выбрать уровень безопасности отпечатков пальцев.

Чем выше уровень безопасности, тем ниже уровень ложных допусков (FAR).

Чем выше уровень безопасности, тем выше уровень ложных недопусков (FRR).

Соотношение уровня ложных допусков (FAR) и уровня безопасности представлено ниже:

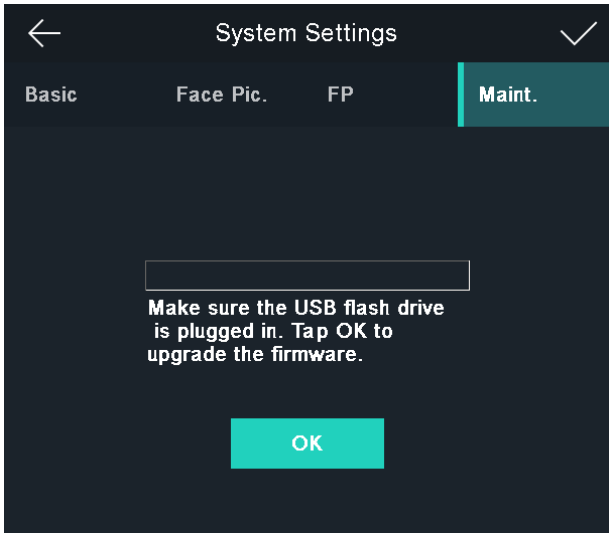
Уровень безопасности отпечатков пальцев	FAR
1	0.1%
2	0.003%
3	0.001%
4	0.0003%
5	0.0001%

Обновление прошивки

На странице обновления подключите USB-накопитель и нажмите **Start** («Старт»). Устройство автоматически считает файл обновления на USB-накопителе и обновит прошивку.

Примечания:

- Файл обновления должен находиться в корневом каталоге.
- Имя файла обновления должно быть: «digicap.dav».



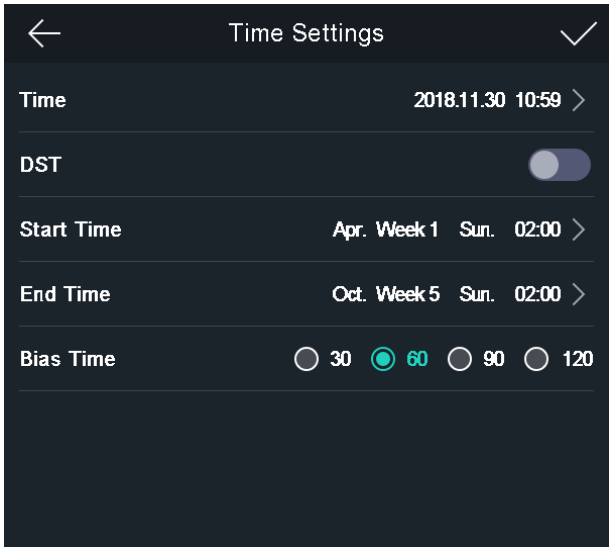
6.3.3 Настройки времени

Цель:

Вы можете установить время устройства и DST в этом разделе.

Шаги:

1. Нажмите **Time** («Время») на домашней странице для перехода на страницу настройки времени.



2. Измените параметры.

Параметр	Описание
Time («Время»)	Установите время, которое будет отображаться на экране устройства.
DST («Переход на летнее время»)	Включите или отключите функцию DST. Если функция включена, вы можете настроить дату перехода на летнее и зимнее время, а также смещение времени. **Start Time** («Время начала»): Установите время перехода на летнее время. **End Time** («Время окончания»): Установите время перехода на зимнее время. **Bias Time** («Смещение времени»): Установите смещения время при переходе на летнее время.

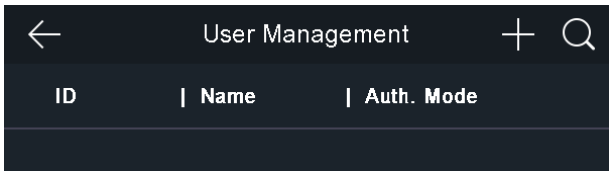
3. Нажмите для сохранения параметров и возврата на домашнюю страницу.

6.4 Управление пользователями

Цель:

В интерфейсе управления пользователями вы можете добавлять, редактировать, удалять и искать пользователей.

Нажмите **User** («Пользователь») на домашней странице для перехода на страницу **User Management** («Управление пользователями»).



6.4.1 Добавление пользователя

Цель:

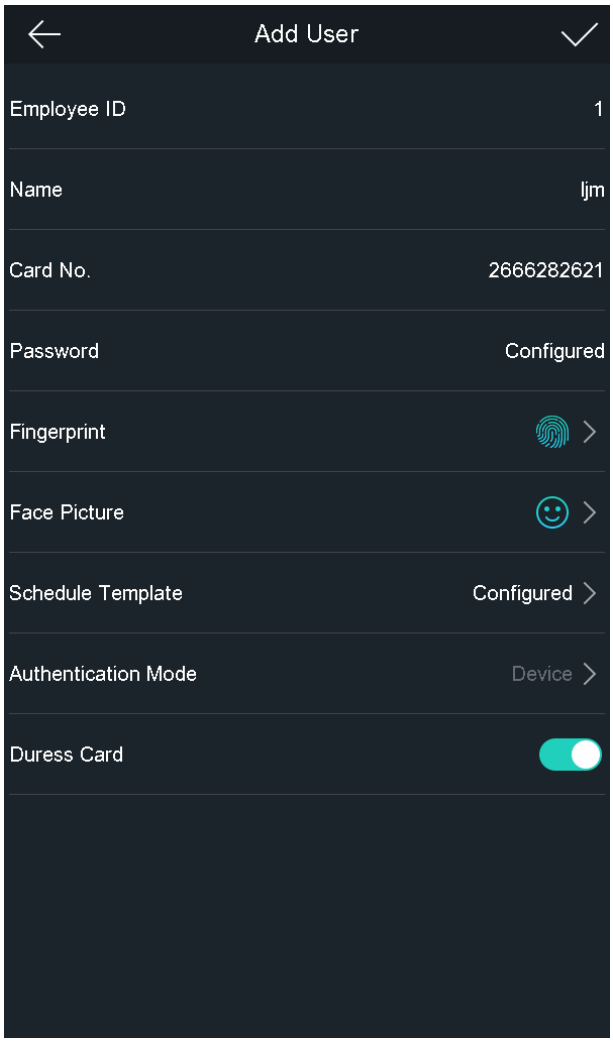
На странице **Add User** («Добавление пользователя») вы можете добавить пользователя, указав его № сотрудника, имя, № карты. Вы также можете привязать отпечаток пальца, изображение лица к пользователю или установить пароль, режим аутентификации, шаблон расписания, разрешение администратора для пользователя.

Примечания:

- Можно добавить до 50000 пользователей.
- Некоторые модели не поддерживают функции, связанные с отпечатками пальцев.

Шаги:

1. На странице **User Management** («Управление пользователями») нажмите **+** to для открытия страницы **Add User** («Добавление пользователя»).



2. Нажмите на поле **Employee ID.** («№ сотрудника») и измените ID сотрудника.

   Примечание:

   ID сотрудника должен быть в диапазоне от 1 до 99999999. ID сотрудника не должен начинаться с 0 и не должен повторяться.

3. Нажмите на поле **Name** («Имя») и введите имя пользователя на программной клавиатуре.

   Примечания:

   - В имени пользователя допускаются цифры, заглавные буквы, строчные буквы и специальные символы.
   - Имя пользователя может содержать максимум 32 символа.

4. Нажмите на поле **Card** («Карта») и введите номер карты.

   Вариант 1: Введите № карты вручную.

   Вариант 2: Проведите карту в области считывания карт, чтобы получить номер карты.

   Примечания:

   - Поле № карты не может быть пустым.
   - № карты может содержать максимум 20 символов.
   - № карты не может повторяться.

5. Нажмите на поле **Password** («Пароль») и создайте пароль, а затем подтвердите его.

   Примечания:

   - В пароле допускаются только цифры.
   - Пароль может содержать максимум 8 символов.

6. Нажмите на поле **Fingerprint** («Отпечаток пальцев») для перехода на страницу добавления отпечатков пальцев.

   Выполните следующие шаги для добавления отпечатков пальцев:

   1) Положите палец на модуль считывания отпечатков пальцев.
   2) Следуйте инструкциям на экране для записи отпечатка пальца.
   3) После полного добавления отпечатка пальца нажмите **Yes** («Да») во всплывающем окне для сохранения отпечатка пальца и продолжения добавления еще одного отпечатка пальца.

      Или нажмите **No** («Нет») для сохранения отпечатка пальца и возврата на страницу **Add User** («Добавление пользователя»).

      Примечания:

      - Один и тот же отпечаток не может быть добавлен повторно.
      - Для одного пользователя можно добавить до 10 отпечатков пальцев.
      - Вы также можете использовать Клиентское ПО или регистратор отпечатков пальцев для записи отпечатков пальцев.
      - Для получения подробной информации о сканировании отпечатков пальцев смотрите *Приложение А Рекомендации по сканированию отпечатков пальцев*.

7. Нажмите на поле **Face Picture** («Изображение лица») для перехода на страницу добавления изображения лица.

   Выполните следующие шаги для добавления изображения лица пользователя.

   1) Поместите ваше лицо прямо перед камерой.

      Примечание: Убедитесь, что ваше изображение лица находится ровно в контуре изображения лица на экране.

      После полного добавления изображения лица на странице отобразится захваченное изображение лица.

      Примечания:

      - Убедитесь, что захваченное изображение лица хорошего качества и достаточно точное.
      - Для получения подробной информации о правилах сбора изображений лиц смотрите *Приложение В Советы по сбору/сравнению изображений лиц.*

   2) Нажмите **Save** («Сохранить») для сохранения изображения лица.

      Или нажмите **Try Again** («Попробовать снова») и отрегулируйте положение вашего лица, чтобы снова добавить изображение лица.

      Примечание: Максимальная продолжительность добавления изображения лица составляет 15 сек. Вы можете проверить оставшееся время для добавления изображения лица в левой части страницы.

8. Нажмите на поле **Schedule Template** («Шаблон расписания») для перехода на соответствующую страницу. Выберите шаблон расписания и нажмите √ для сохранения настроек.

   Примечание: Для получения подробной информации о настройке шаблона расписания смотрите *Раздел 7.6 Расписание и шаблон*. После применения шаблона расписания из Клиентского ПО к устройству, вы можете выбрать соответствующий шаблон расписания.
9. Нажмите на поле **Authentication Mode** («Режим аутентификации») для перехода на соответствующую страницу. Выберите в качестве режима аутентификации: **Device** («Устройство») или **Custom** («Пользовательский»).

   Device («Устройство»): Если вы хотите выбрать режим устройства, вы должны сначала установить режим аутентификации терминала на странице **Access Control Settings** («Настройки контроля доступа»). Для получения подробной информации смотрите *Раздел 6.5 Установка параметров контроля доступа*. Пользователь будет аутентифицировать свою личность в соответствии с настроенным режимом аутентификации. По умолчанию в поле **Authentication Mode** («Режим аутентификации») выбрано значение **Device** («Устройство»). Этот режим применим для редактирования режимов аутентификации пользователей в пакетном режиме.

   Custom («Пользовательский»): Если пользователю необходимо использовать специальный режим аутентификации, который отличается от настроенного в *Разделе 6.5 Установка параметров контроля доступа* режима аутентификации, он может использовать другие режимы аутентификации. Пользователь будет сначала аутентифицировать свою личность в соответствии с пользовательским режимом аутентификации. Этот режим применим для редактирования режима аутентификации для одного пользователя, который имеет специальные разрешения.
10. Включите или отключите функцию **Duress Card** («Принудительная карта»).

    Когда функция включена, карта пользователя будет принудительной картой. Когда пользователь аутентифицируется при помощи проводки такой карты, устройство загружает событие принудительной карты в Клиентское ПО.
11. Нажмите  для сохранения параметров и возврата на домашнюю страницу.

6.4.2 Добавление пользователя

Поиск пользователя

Цель:

Вы можете искать пользователя в списке по ID сотрудника, номеру карты или имени пользователя.

Шаги:

1. На странице **User Management** («Управление пользователями») нажмите  для перехода на страницу **Search User** («Поиск пользователя»).
2. Нажмите **Card** («Карта») в левой части страницы и выберите тип поиска из выпадающего списка.
3. Нажмите на поле ввода и введите ID сотрудника, номер карты или имя пользователя для

поиска.

4. Нажмите для начала поиска.
   Результат поиска будет отображен в виде списка ниже.

Редактирование пользователя

Цель:

Вы можете редактировать добавленную информацию о пользователях, следуя шагам в этом разделе.

Шаги:

1. На странице **User Management** («Управление пользователями») нажмите на имя пользователя, которого вы хотите отредактировать для перехода на страницу **Edit User** («Редактирование пользователя»).
2. Обратитесь к описанию параметров пользователя в *Разделе 6.4.1 Добавление пользователя* для редактирования пользовательской информации.
3. Нажмите для сохранения параметров и возврата на страницу управления пользователями.
   Примечание: ID сотрудника не может быть изменен.

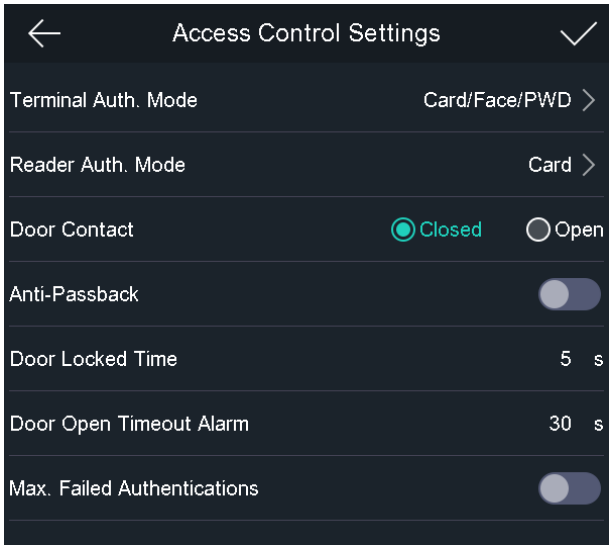
6.5 Установка параметров контроля доступа

Цель:

Вы можете установить разрешения контроля доступа, включая режим аутентификации, дверной контакт, запрет обратного прохода, время до закрытия двери, тревогу тайм-аута открытого состояния двери, макс. число неудачных аутентификаций.

Шаги:

1. На домашней странице нажмите **ACS** («Доступ») для перехода на страницу **Access Control Settings** («Настройки контроля доступа»).



2. Измените параметры контроля доступа.
   Описание доступных параметров представлено ниже:

Параметр	Описание
Terminal Auth. Mode («Режим аутентификации терминала»)	Выберите режим аутентификации терминала распознавания лиц. Вы также можете настроить режим аутентификации по вашему усмотрению. ***Примечания:*** ● Только устройство с функцией сканирования отпечатков пальцев поддерживает функции, связанные с отпечатками пальцев. ● Биометрические продукты распознавания не на 100% применимы к анти-спуфинг средам. Если вам требуется более высокий уровень безопасности, используйте несколько режимов аутентификации
Reader Auth. Mode («Режим аутентификации считывателя карт»)	Выберите режим аутентификации устройства считывания карт.
Door Contact («Дверной контакт»)	Вы можете выбрать значение **Open** («Открыт») (Оставить открытым) или **Closed** («Закрыт») (Оставить закрытым) в соответствии с вашими фактическими потребностями. По умолчанию выбрано значение **Remain Closed** («Оставить закрытым»).
Anti-Passback («Запрет обратного прохода»)	При включении функции запрета обратного прохода вы должны установить путь прохода в Клиентском ПО iVMS-4200. Человек должен пройти аутентификацию в соответствии с настроенным путем. Иначе аутентификация будет неудачной.
Door Locked Time («Время до закрытия двери»)	Установите длительность отпирания двери. Если дверь не открывается в течение установленного времени, она будет закрыта. Доступный диапазон времени до закрытия двери: от 1 до 255 с.
Door Open Timeout Alarm («Тревога тайм-аута открытого состояния двери»)	Тревога может быть запущена, если дверь не была закрыта. Доступный диапазон: от 0 до 255 с.
Max. Failed Authentications («Макс. число неудачных аутентификаций»)	Установите максимальное число попыток аутентификации. Если вам не удалось пройти аутентификацию за установленное число попыток, будет запущена тревога.

3. Нажмите  для сохранения настроек.

6.6 Управление другими параметрами

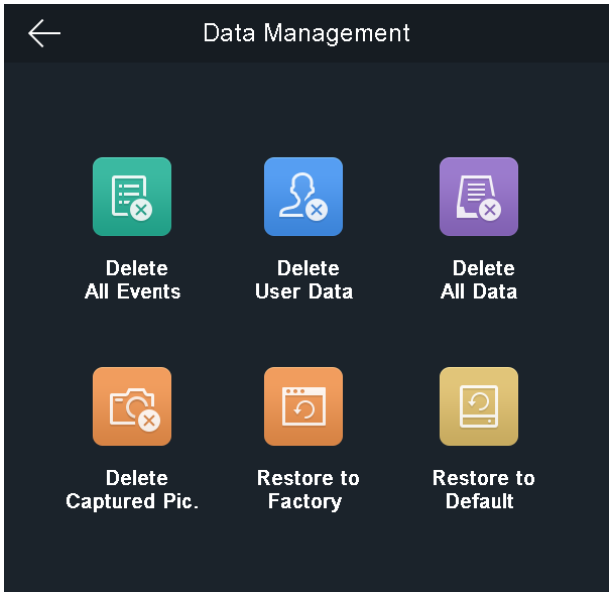
6.6.1 Управление данными

Цель:

На странице **Data Management** («Управление данными») вы можете удалять все события, удалять пользовательские данные, удалять все данные, удалять захваченные изображения, выполнять сброс до заводских настроек или восстанавливать настройки по умолчанию.

Шаги:

1. Нажмите **Data** («Данные») для перехода в меню **Data Management** («Управление данными»).



2. Нажмите на кнопку на странице, чтобы управлять данными.

   Описание доступных кнопок:

Параметр	**Описание**
Delete All Events («Удалить все события»)	Удаление всех событий, хранящихся в устройстве.
Delete User Data («Удалить пользовательские данные»)	Удаление всех пользовательских данных на устройстве.
Delete All Data («Удалить все данные»)	Удаление всех пользовательских данных и событий, хранящихся на устройстве.
Delete Captured Pic. («Удалить	Удаление всех захваченных изображений.

Параметр	Описание
захваченные изображения»)	
Restore to Factory («Сброс до заводских настроек»)	Сброс системы до заводских настроек. Устройство перезагрузится после настройки.
Restore to Default («Восстановление настроек по умолчанию»)	Восстановление настроек по умолчанию. Система сохранит настройки связи и настройки удаленного пользователя. Другие параметры будут восстановлены до значений по умолчанию.

3. Нажмите **Yes** («Да») во всплывающем окне для завершения настройки.

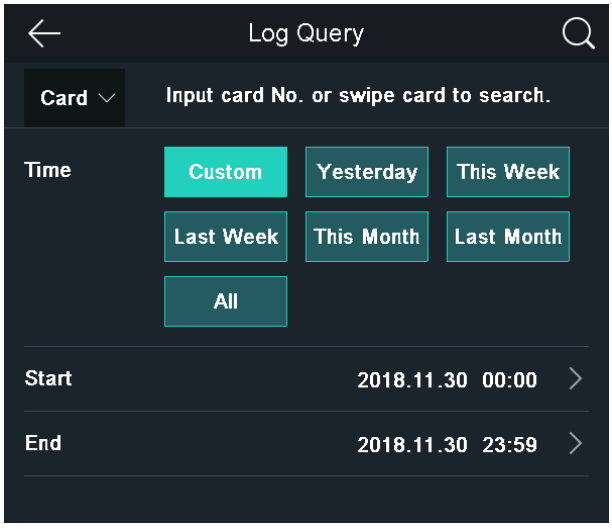
6.6.2 Управление запросом журнала

Цель:

Вы можете осуществлять поиск в журналах аутентификации за определенный период времени, введя ID сотрудника, номер карты или имя пользователя.

Шаги:

1. На домашней странице нажмите **Log** («Журнал») для перехода на страницу Log Query («Запрос журнала»).



2. Нажмите **Card** («Карта») в левой части страницы и выберите тип поиска из выпадающего списка.
3. Нажмите на поле ввода и введите ID сотрудника, № карты или имя пользователя для поиска.
4. Выберите время.

   Вы можете выбрать: **Custom** («Настраиваемый период»), **Yesterday** («Вчера»), **This Week** («На этой неделе»), **Last Week** («На прошлой неделе»), **This Month** («В этом месяце»), **Last Month** («В прошлом месяце») или **All** («За все время»).

Если вы выбрали значение **Custom** («Настраиваемый период») вы можете настроить время начала и время окончания поиска.

5. Нажмите для начала поиска.

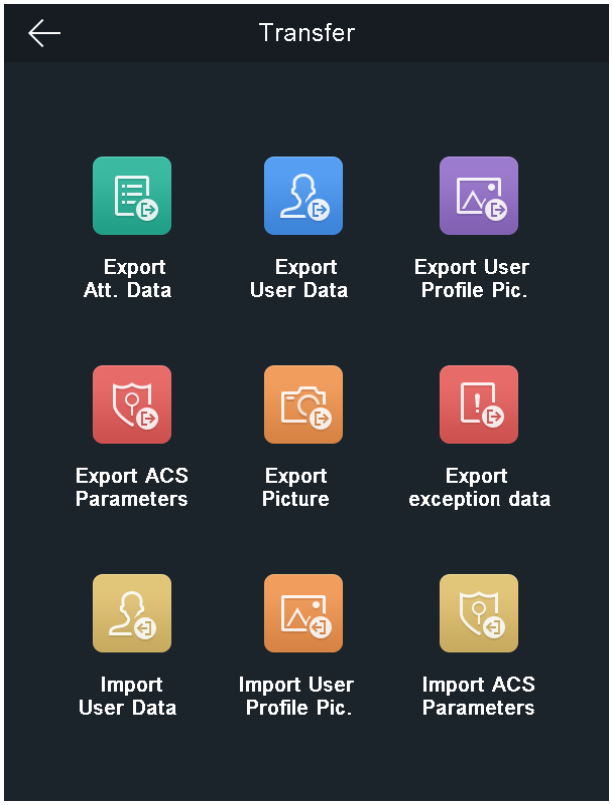
   Результат будет отображен на странице.

6.6.3 Импорт/Экспорт данных

Цель:

На странице **Transfer** («Передача») вы можете экспортировать данные посещаемости, данные пользователей, изображения лиц пользователей, параметры контроля доступа, захваченные изображения, и данные об исключениях на USB флеш-накопитель. Вы также можете импортировать данные пользователей, изображения лиц пользователей и параметры контроля доступа с USB флеш-накопителя.

Нажмите **Transfer** («Передача») на домашней странице для перехода в соответствующее меню.



Экспорт данных

Шаги:

1. Подключите USB флеш-накопитель к устройству.
2. На странице **Transfer** («Передача») нажмите **Export Att. Data** («Экспорт данных посещаемости»), **Export User Data** («Экспорт данных пользователей»), **Export Face Pic.** («Экспорт изображений лиц»), **Export Access Control Param.** («Экспорт параметров контроля доступа») или **Export Captured Pic** («Экспорт захваченных изображений»).

3. Нажмите **Yes** («Да») во всплывающем окне, и данные будут экспортированы с устройства на USB флеш-накопитель.

   Примечания:

   - Поддерживаемый USB флеш-накопителя: FAT 32.
   - Система поддерживает USB флеш-накопитель с объемом памяти от 1 до 32 ГБ. Убедитесь, что свободное место на USB флеш-накопителе превышает 512 МБ.
   - Экспортированные данные пользователя - это файл BIN, который нельзя отредактировать.

Импорт данных

Шаги:

1. Подключите USB флеш-накопитель к устройству.
2. На странице **Transfer** («Передача») нажмите **Import User Data** («Импорт данных пользователей»), **Import Face Pic.** («Импорт изображений лиц») или **Import Access Control Param** («Импорт параметров контроля доступа»).
3. Нажмите **Yes** («Да») во всплывающем окне, и данные будут импортированы с USB флеш-накопителя на устройство.

   Примечания:

   - Если вы хотите перенести информацию всех пользователей с одного устройства (Устройство A) на другое (Устройство B), вы должны экспортировать информацию с Устройства A на USB флеш-накопитель, а затем импортировать с USB флеш-накопителя на Устройство B. В этом случае, вы должны импортировать данные пользователей перед импортом фотографий профилей.
   - Поддерживаемый USB флеш-накопителя: FAT 32.
   - Импортированное изображение должно быть сохранено в корневом каталоге (enroll_pic) и имя файла должно соответствовать приведенному ниже правилу:

     № карты_Имя_Отдел_ ID сотрудника_Пол.jpg
   - ID сотрудника должен быть между 1 и 99999999, не должен дублироваться и не должен начинаться с 0.
   - Требования к изображению лица: человек при съемке должен быть повернут лицом к камере и должен смотреть прямо в камеру. При съемке лица не надевайте головные уборы или хиджаб. Формат изображения: JPEG или JPG. Разрешение: 640 × 480 пикселей или больше, чем 640 × 480 пикселей. Размер изображения должен быть от 60 до 200 КБ.

6.6.4 Просмотр системной информации

Просмотр объема данных

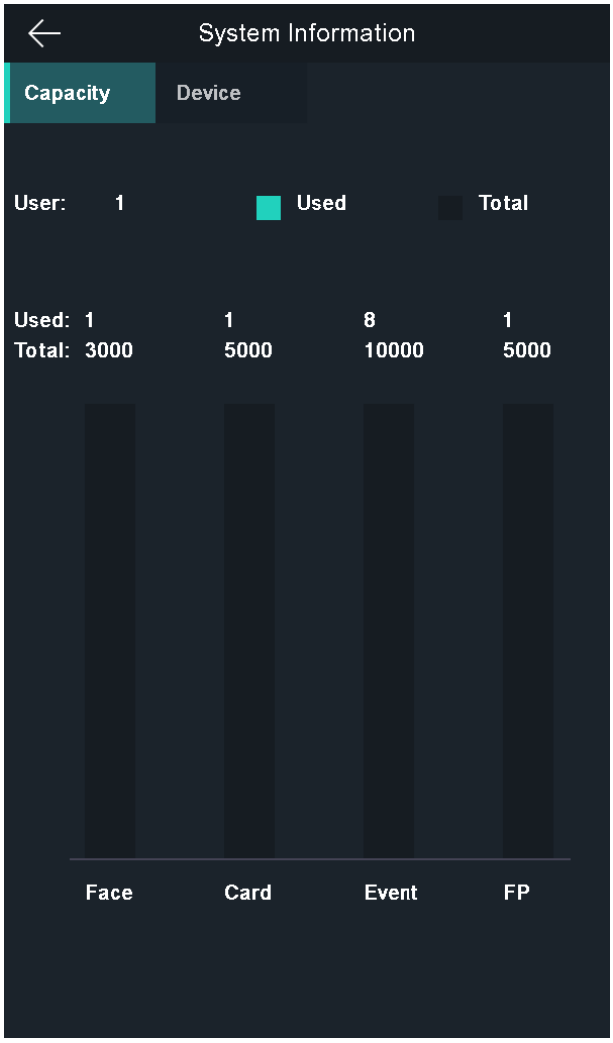
Цель:

Вы можете просмотреть число добавленных пользователей, число изображений лиц, число карт, число паролей и число отпечатков пальцев.

Примечание: Некоторые модели не поддерживают отображение количества отпечатков

пальцев.

Нажмите **Info.** («Информация») (Системная информация) **-> Capacity** («Емкость») на домашней странице для перехода на соответствующую страницу.



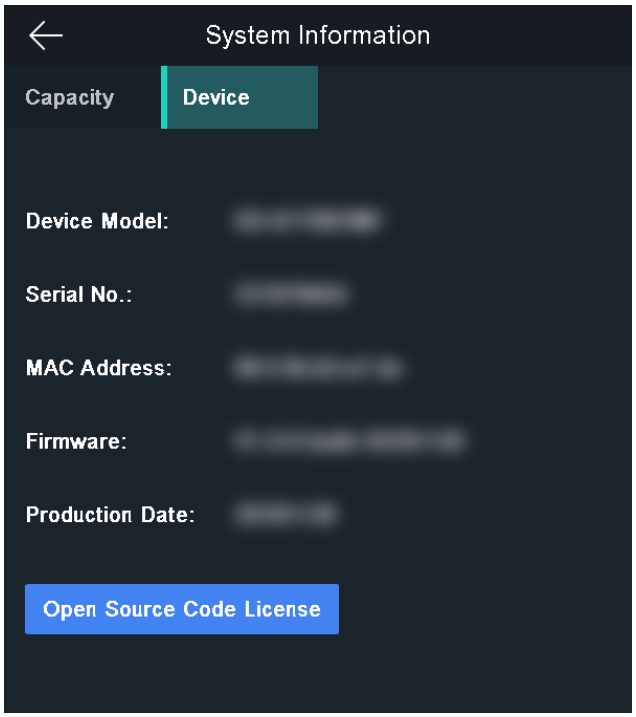
Просмотр информации устройства

Цель:

Вы можете просмотреть модель устройства, серийный номер, MAC-адрес, версию прошивки, дату производства и Лицензию открытого исходного кода.

Нажмите **Device** («Устройство») для перехода на соответствующую страницу.

Примечание: Страница информации об устройстве может отличаться в зависимости от модели устройства.



6.7 Аутентификация личности

Цель:

После настройки сети, параметров системы и добавления пользователя вы можете вернуться на начальную страницу для аутентификации личности.

Система будет аутентифицировать человека в соответствии с настроенным режимом аутентификации.

Вы можете выполнить аутентификацию личности при помощи **1:1 Matching** («Соответствие 1:1») или **1:N Matching** («Соответствие 1: N»).

Примечание: Биометрические продукты распознавания не на 100% применимы к анти-спуфинг средам. Если вам требуется более высокий уровень безопасности, используйте несколько режимов аутентификации.

1:N Matching («Соответствие 1: N»):	Сравнение захваченного изображения лица или считанного отпечатка пальца со всеми изображениями лиц или всеми отпечатками пальцев, хранящимися в терминале.
1:1 Matching («Соответствие 1:1»):	При проводке картой выполняется сравнение захваченного изображения лица или считанного отпечатка пальца с информацией, хранящейся на карте.

6.7.1 Аутентификация при помощи Соответствия 1:1

Шаги:

1. Если в качестве режима аутентификации выбрано значение **Card and Face** («Карта и Лицо») или **Card and Face and Fingerprint** («Карта, Лицо и Отпечаток пальца»), то проведите картой в области считывания карт.
   Если функция сканирования QR-кода включена, вы можете поместить QR-код перед камерой устройства для аутентификации с помощью QR-кода.
2. Если в качестве режима аутентификации выбрано значение **Card and Face** («Карта и Лицо»), поместите лицо прямо перед камерой для начала аутентификации.
   Если в качестве режима аутентификации выбрано значение **Card and Face and Fingerprint** («Карта, Лицо и Отпечаток пальца»), то после аутентификации по отпечатку пальца выполните аутентификация по лицу, когда появится сообщение **“Continue to authenticate”** *(«Продолжить аутентификацию»)*.
   Если аутентификация прошла успешно, появится уведомление **“Authenticated”** *(«Аутентифицировано»)*.
   Примечания:
   - Для лучшей аутентификации изображения лица рост пользователя должен быть от 140 до 190 см, а расстояние между пользователем и устройством должно составлять от 30 до 100 см.
   - Для получения подробной информации о сканировании отпечатков пальцев смотрите *Приложение А Рекомендации по сканированию отпечатков пальцев*.
   - Для получения подробной информации об аутентификации изображения лица смотрите *Приложение В Советы по сбору/сравнению изображений лиц.*

6.7.2 Аутентификация при помощи Соответствия 1:N

Если в качестве режима аутентификации выбрано **Face** («Лицо»), поместите лицо прямо перед камерой для начала аутентификации.
Если аутентификация прошла успешно, появится уведомление **“Authenticated”** *(«Аутентифицировано»)*.

6.7.3 Аутентификация при помощи Соответствия 1:1 и Соответствия 1:N

Шаги:

1. Если в качестве режима аутентификации выбрано **Fingerprint and Face** («Отпечаток пальца и Лицо»), сначала аутентифицируйте отпечаток пальца в соответствии с подсказками на экране устройства.
   Устройство сравнит отпечаток пальца с информацией об отпечатке пальца в базе данных устройства (Соответствие 1:N).
   Если аутентификация завершена, появится сообщение **“Continue to authenticate”** *(«Продолжить аутентификацию»)*.
2. Поместите лицо прямо перед камерой для начала аутентификации лица.

Устройство сравнит захваченное изображение лица с пользовательской информацией, полученной на последнем шаге (Соответствие 1:1).
Если аутентификация прошла успешно, появится уведомление **“Authenticated”** *(«Аутентифицировано»)*.

Примечания:

- Для лучшей аутентификации изображения лица рост пользователя должен быть от 140 до 190 см, а расстояние между пользователем и устройством должно составлять от 30 до 100 см.
- Для получения подробной информации о сканировании отпечатков пальцев смотрите *Приложение A Рекомендации по сканированию отпечатков пальцев*.
- Для получения подробной информации об аутентификации изображения лица смотрите *Приложение B Советы по сбору/сравнению изображений лиц.*

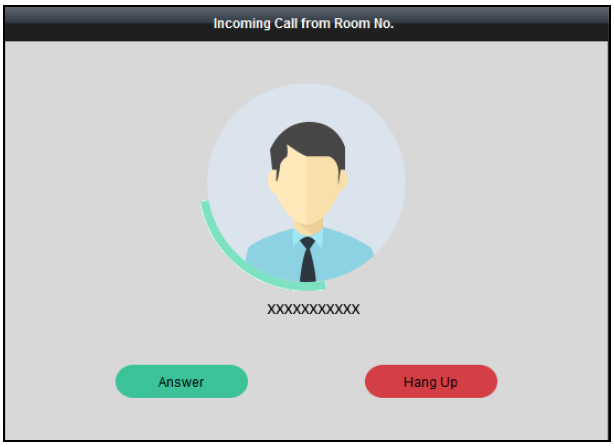
6.8 Двустороннее аудио

Цель:
После добавления устройства в Клиентское ПО iVMS-4200, вы сможете вызвать устройство из Клиентского ПО, вызвать монитор консьержа с устройства, вызвать Клиентское программное обеспечение с устройства или вызвать видеодомофон с устройства.

6.8.1 Вызов Клиентского ПО iVMS-4200 с устройства

Шаги:

1. Получите Клиентское программное обеспечение на прилагаемом диске или скачайте его с официального веб-сайта, затем установите программное обеспечение в соответствии с инструкциями.
2. Запустите клиентское программное обеспечение, и появится панель управления программным обеспечением.
3. Нажмите **Device Management** («Управление устройствами») для перехода на соответствующую страницу.
4. Добавьте устройство в Клиентское ПО.
   Примечание: Для получения подробной информации о добавлении устройств смотрите *Раздел 7.3.1 Добавление устройства контроля доступа*.
5. Выполните вызов Клиентского ПО.
   1) Нажмите **Call** («Вызов») на начальной странице устройства.
   2) Введите **0** во всплывающем окне.
   3) Нажмите **Call** («Вызов») для вызова Клиентского ПО.
6. Нажмите **Answer** («Ответить») во всплывающем окне Клиентского ПО, и вы сможете начать двустороннее аудио между устройством и Клиентским программным обеспечением.
   Примечание: Если устройство добавлено несколькими Клиентскими программами, то когда устройство вызывает Клиентское ПО, только первое добавленное Клиентское ПО откроет окно приема вызова.



6.8.2 Вызов монитора консьержа с устройства

Шаги:

1. Получите Клиентское программное обеспечение на прилагаемом диске или скачайте его с официального веб-сайта, затем установите программное обеспечение в соответствии с инструкциями.
2. Запустите Клиентское программное обеспечение, и появится панель управления программным обеспечением.
3. Нажмите **Device Management** («Управление устройствами») для перехода на соответствующую страницу.
4. Добавьте монитор консьержа и устройство в Клиентское ПО.
   Примечание: Для получения подробной информации о добавлении устройств смотрите *Раздел 7.3.1 Добавление устройства контроля доступа*.
5. Установите IP-адрес монитора консьержа и SIP-адрес на странице удаленной конфигурации.
   Примечание: Для получения дополнительной информации об этой операции смотрите Руководство пользователя монитора консьержа.
6. Нажмите  на странице аутентификации устройства и нажмите  (центр) во всплывающем окне.
7. После того, как монитор консьержа ответит на вызов, вы сможете запустить двустороннюю аудиосвязь ним.
   Примечание: Устройство будет вызывать монитор консьержа в приоритетном порядке при нажатии  .

6.8.3 Вызов устройства с Клиентского ПО iVMS-4200

Шаги:

1. Получите Клиентское программное обеспечение на прилагаемом диске или скачайте его с официального веб-сайта, затем установите программное обеспечение в соответствии с инструкциями.
2. Запустите Клиентское программное обеспечение, и появится панель управления программным обеспечением.
3. Нажмите **Device Management** («Управление устройствами») для перехода на

соответствующую страницу.

4. Добавьте устройство в Клиентское ПО.
   Примечание: Для получения подробной информации о добавлении устройств смотрите *Раздел 7.3.1 Добавление устройства контроля доступа*.
5. Перейдите на страницу просмотра в реальном времени и дважды щелкните добавленное устройство, чтобы начать просмотр в реальном времени.
   Примечание: Для получения подробной информации об операциях в режиме просмотра в реальном времени смотрите *Раздел 7.12 Просмотр в реальном времени*.
6. Нажмите правой кнопкой мыши на изображение в реальном времени, чтобы открыть контекстное меню.
7. Нажмите **Start Two-Way Audio** («Начать двустороннее аудио») для начала двустороннего аудио между устройством и Клиентским ПО.

6.8.4 Вызов видеодомофона с устройства

Шаги:

1. Получите Клиентское программное обеспечение на прилагаемом диске или скачайте его с официального веб-сайта, затем установите программное обеспечение в соответствии с инструкциями.
2. Запустите Клиентское программное обеспечение, и появится панель управления программным обеспечением.
3. Нажмите **Device Management** («Управление устройствами») для перехода на соответствующую страницу.
4. Добавьте видеодомофон и устройство в Клиентское ПО.
   Примечание: Для получения подробной информации о добавлении устройств смотрите *Раздел 7.3.1 Добавление устройства контроля доступа*.
5. Привяжите пользователя к видеодомофону и установите № комнаты для видеодомофона.
6. Нажмите  на странице аутентификации устройства.
7. Введите № комнаты на странице вызова и нажмите кнопку  для вызова видеодомофона.
8. После того, как видеодомофон ответит на вызов, вы сможете запустить двустороннюю аудиосвязь ним.

Глава 7 Операции в Клиентском ПО

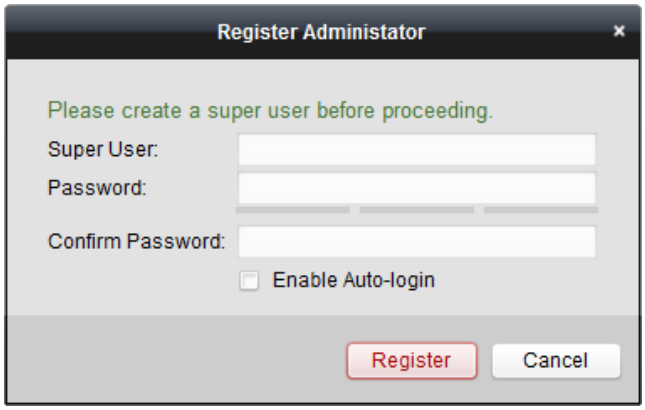
Вы можете настраивать и управлять устройствами контроля доступа через Клиентское программное обеспечение. В этой главе будут представлены операции связанные с управлением доступом в Клиентском программном обеспечении. Для получения подробной информации смотрите *Руководство пользователя Клиентского ПО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

7.1 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»). ПО 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.

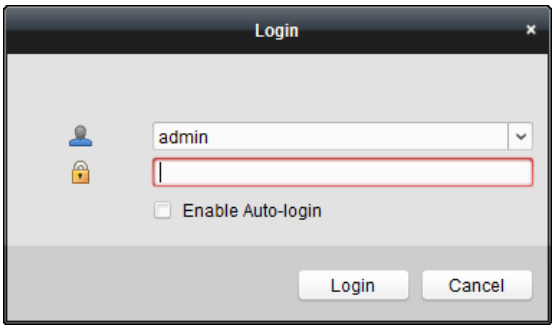


- *Имя пользователя не может содержать любой из следующих символов: / \ :* ?"<>|. Длина пароля не может быть меньше 6-ти символов.*
- *Для вашей безопасности, мы настоятельно рекомендуем изменить пароль на ваш собственный (используя как минимум 8 символов, включая символы верхнего или нижнего регистра, 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 открывается после регистрации, вы можете войти в него с зарегистрированным именем и паролем.

Шаги:

1. Введите **User name** («Имя пользователя») и **Password** («Пароль»), которые вы зарегистрировали.
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*.

7.2 Конфигурация системы

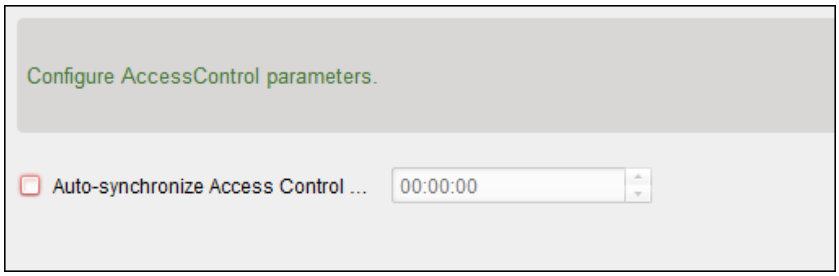
Цель:

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.



7.3 Управление контролем доступа

Цель:

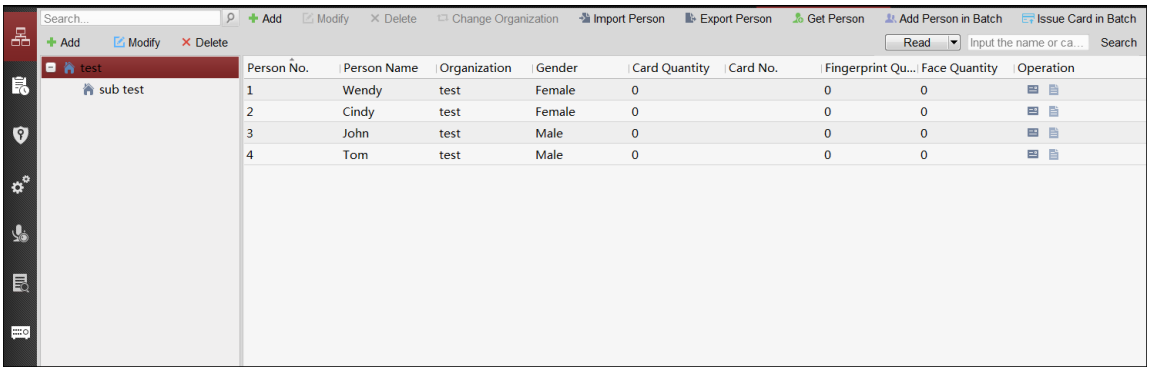
Модуль контроля доступа применим к устройствам контроля доступа и видеодомофонам. Он обеспечивает множество функций, включая управление людьми и карточками, конфигурацию разрешений, управление статусом контроля доступа, видеодомофонию и другие расширенные функции.

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

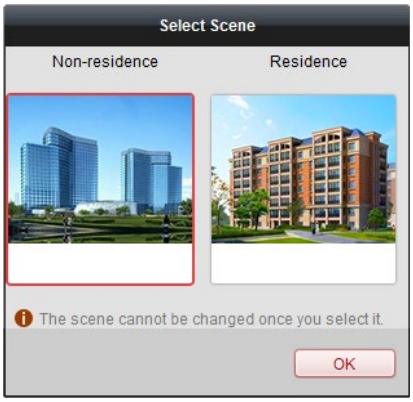


Перед началом:

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.

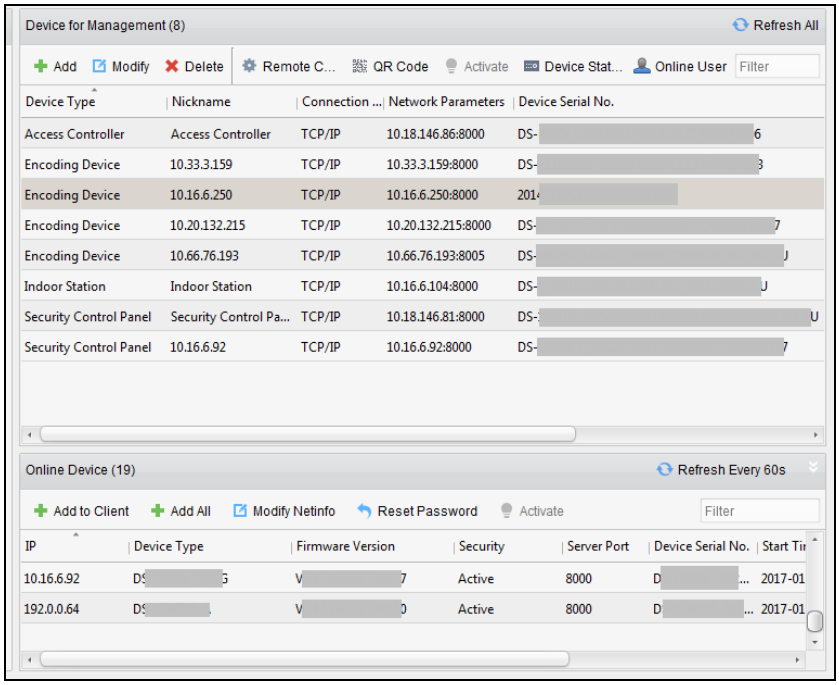
Residence («Жилой комплекс»): Вы не можете установить правило посещаемости при добавлении человека.



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

7.3.1 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 7.13 Управление охраной*.

Создание пароля

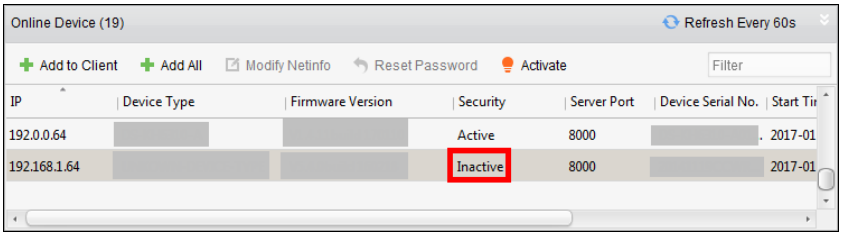
Цель:

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.

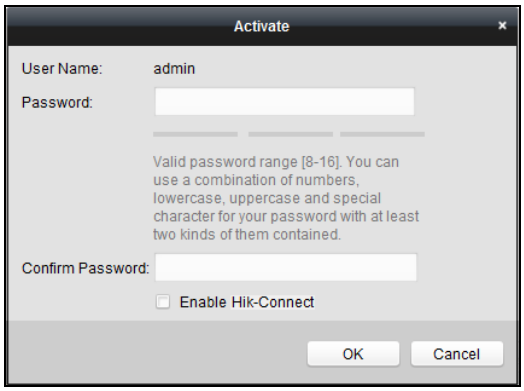


3. Нажмите кнопку **Activate** («Активировать») для появления всплывающего меню

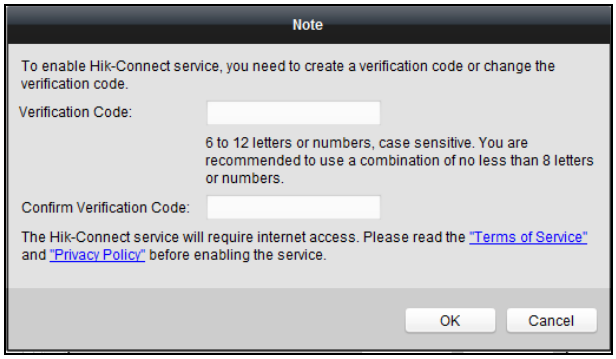
активации.

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.

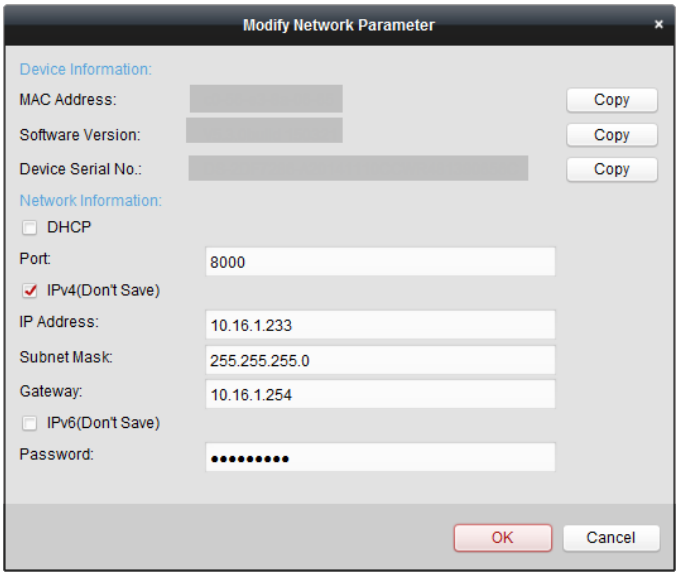


   2) Создайте **Verification code** («Проверочный код»).
   3) Подтвердите проверочный код в поле **Confirm verification code** («Подтверждение проверочного кода»).
   4) Нажмите **Terms of Service** («Условия предоставления услуг») и **Privacy Policy** («Политика конфиденциальности») для ознакомления 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»)*.

7. 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.
8. Измените IP-адрес устройства на адрес в той же подсети, что и ваш компьютер, вручную или поставив галочку напротив **DHCP**.
9. Введите пароль, установленный в шаге 4, и нажмите **OK** для завершения сетевых настроек.

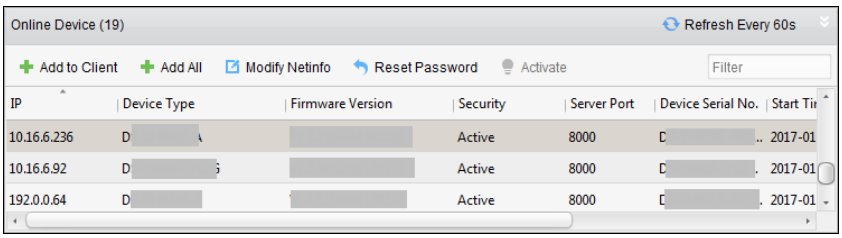


Добавление онлайн устройств

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:

1. 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. Для получения подробной информации смотрите *Раздел 7.3.1 Добавление устройств контроля доступа.*

2. Нажмите **Add to Client** («Добавить к клиенту») для открытия диалогового окна добавления устройств.
3. Введите необходимую информацию.

   Nickname («Имя устройства»): Измените имя 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.

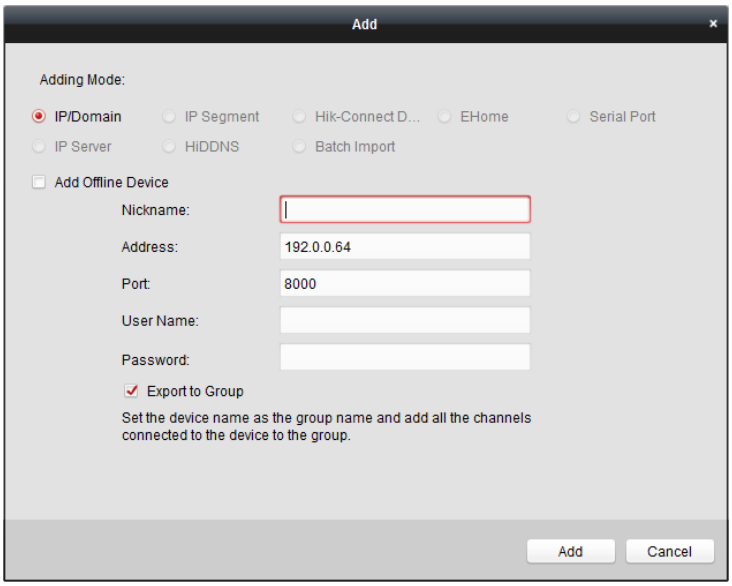
   РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ – *Настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля 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.

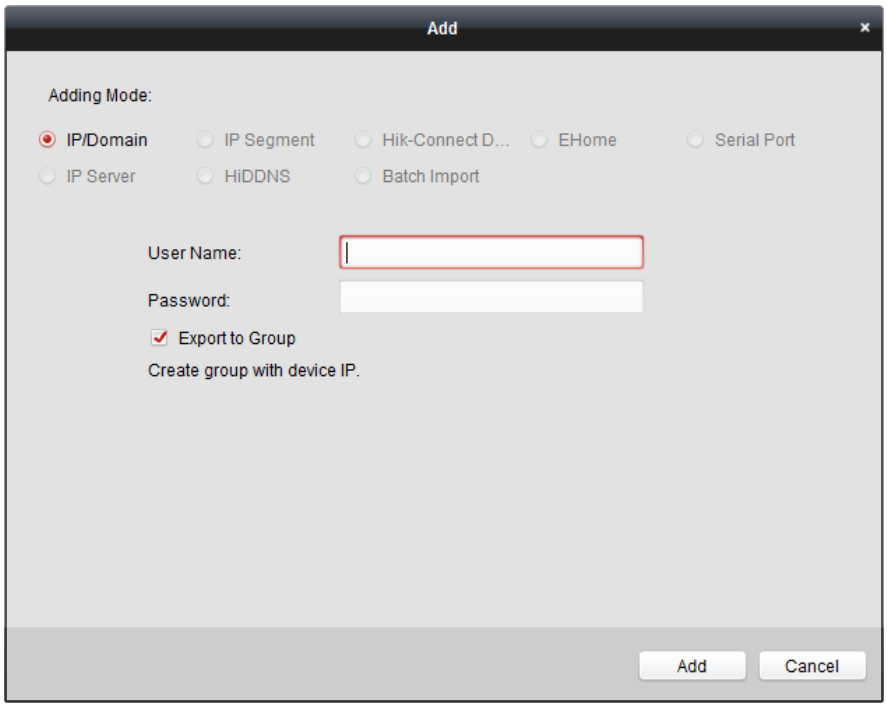


➢ Добавление нескольких онлайн устройств

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.

   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.*

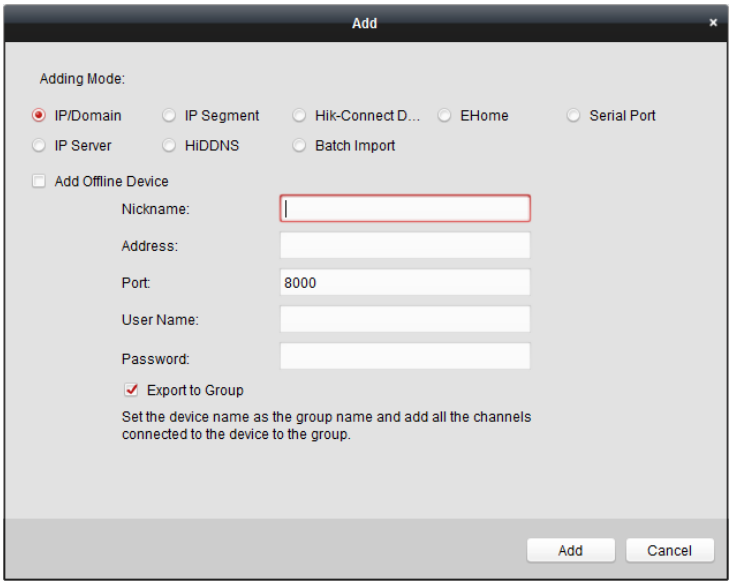
4. Опционально, вы можете поставить галочку **Export to Group** («Экспортировать в группу») для создания группы соответствующей имени устройства.

   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.*

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.

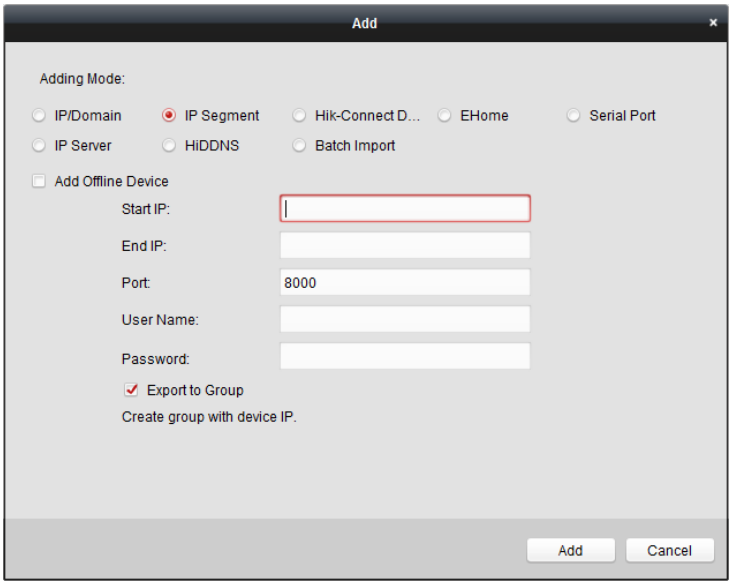
   Примечание: iVMS-4200 так же предоставляет метод добавления офлайн устройств.

   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»).

   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:

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

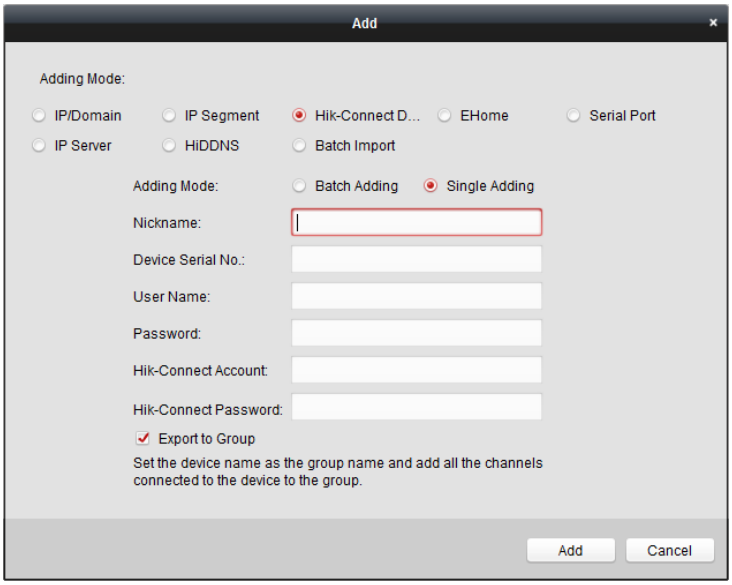
   

   РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ – *Настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля 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.

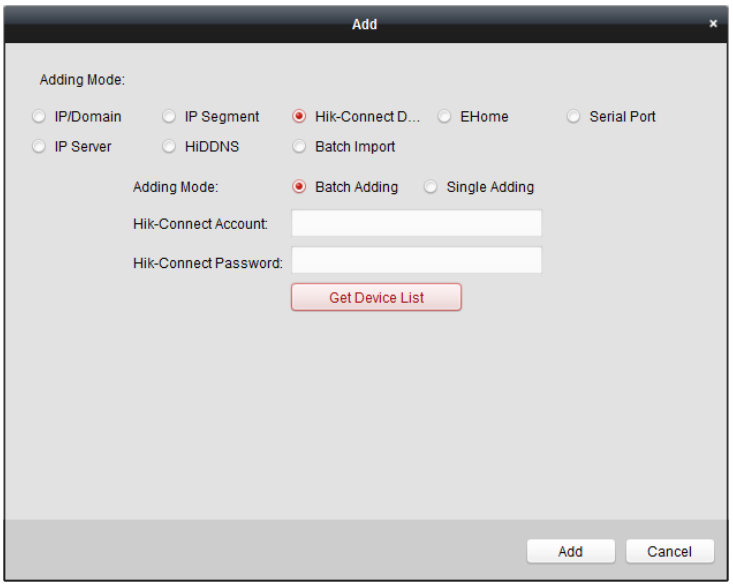
   Все каналы устройства будут импортированы в соответствующую группу по умолчанию.
6. Нажмите **Add** («Добавить») для добавления устройства.



Пакетное добавление устройств

Шаги:

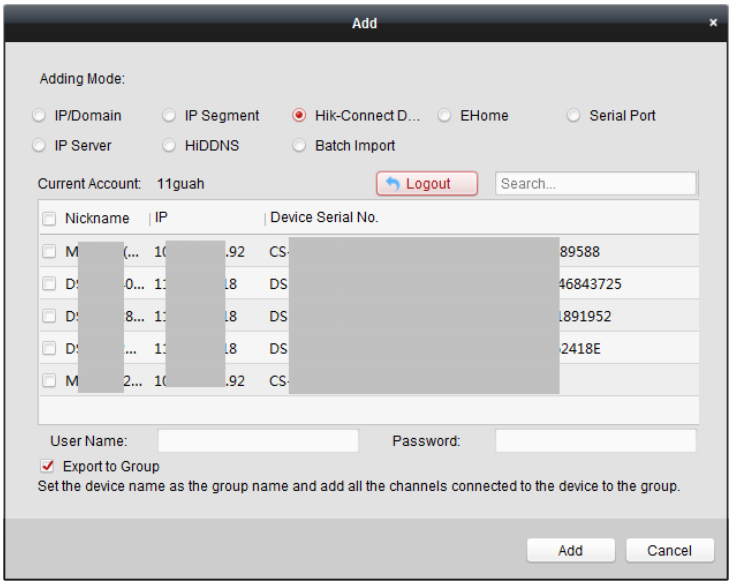
1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.



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 учетной записи EHome

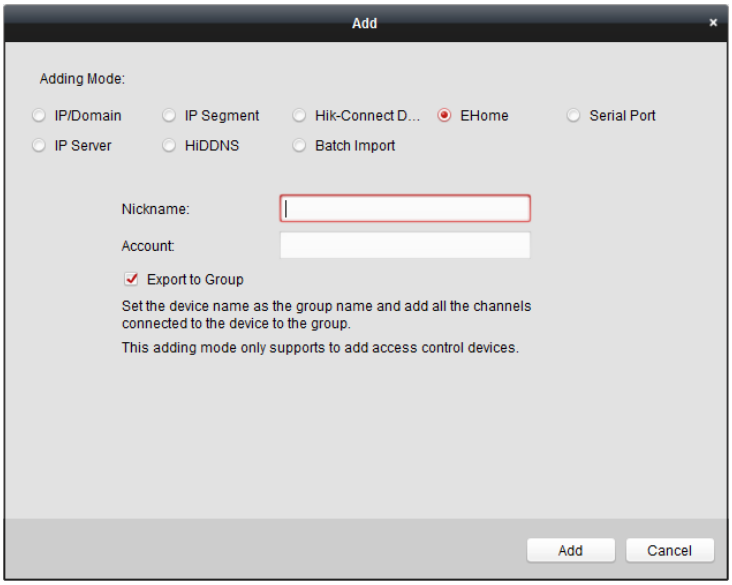
Цель:

Вы можете добавить устройство контроля доступа, подключенное по протоколу EHome, путем входа в учетную запись EHome.

Перед началом: Настройте параметры сетевого центра. Смотрите *Раздел 7.3.4 Сетевые настройки.*

Шаги:

1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.
2. Выберите значение **EHome** в поле **Adding mode** («Режим добавления»).



3. Введите необходимую информацию.

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

   Account («Учетная запись»): Введите имя учетной записи, зарегистрированное в протоколе EHome.

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»).

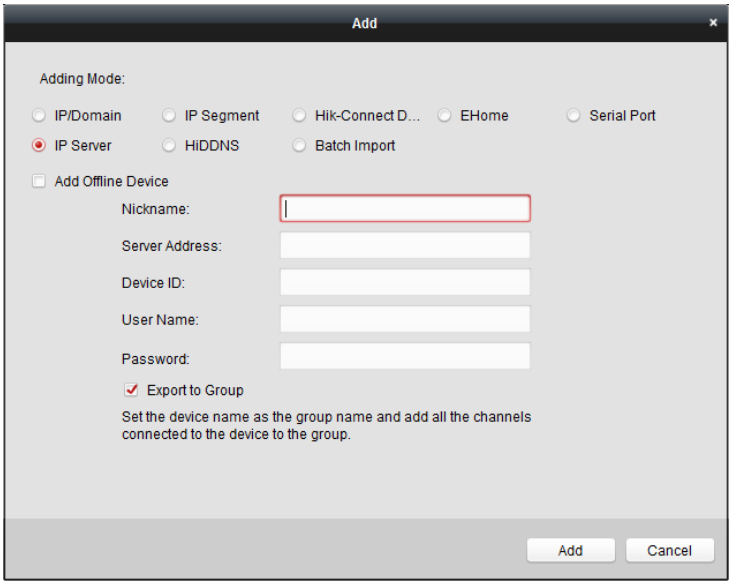
   Когда устройство из офлайн режима перейдет в онлайн режим, программа подключится к нему автоматически.

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»).

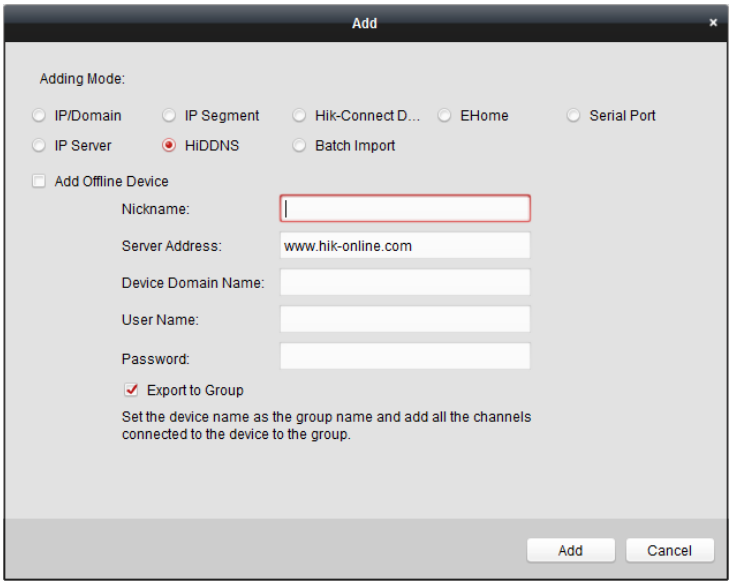
   Когда устройство из офлайн режима перейдет в онлайн режим, программа подключится к нему автоматически.

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

Добавление устройств при помощи HiDDNS

Шаги:

1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.
2. Выберите **HiDDNS** в поле **Adding mode** («Режим добавления»).



3. Введите необходимую информацию.

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

   Server Address («Адрес сервера»): *www.hik-online.com*.

   Device Domain Name («Доменное имя устройства»): Введите доменное имя устройства, зарегистрированное на HiDDNS 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.

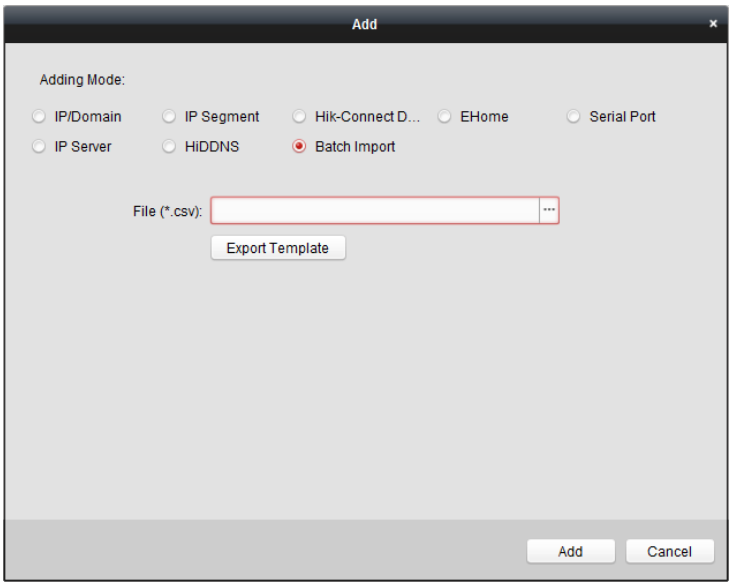
Импорт устройств в пакетном режиме

Цель:

Устройства могут быть добавлены в программу в пакетном режиме путем внесения информации об устройствах в заданный 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.
- **Baud Rate** («Скорость передачи данных (в бодах)»): Если вы установили «5» в качестве режима добавления, введите скорость передачи в бодах 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.

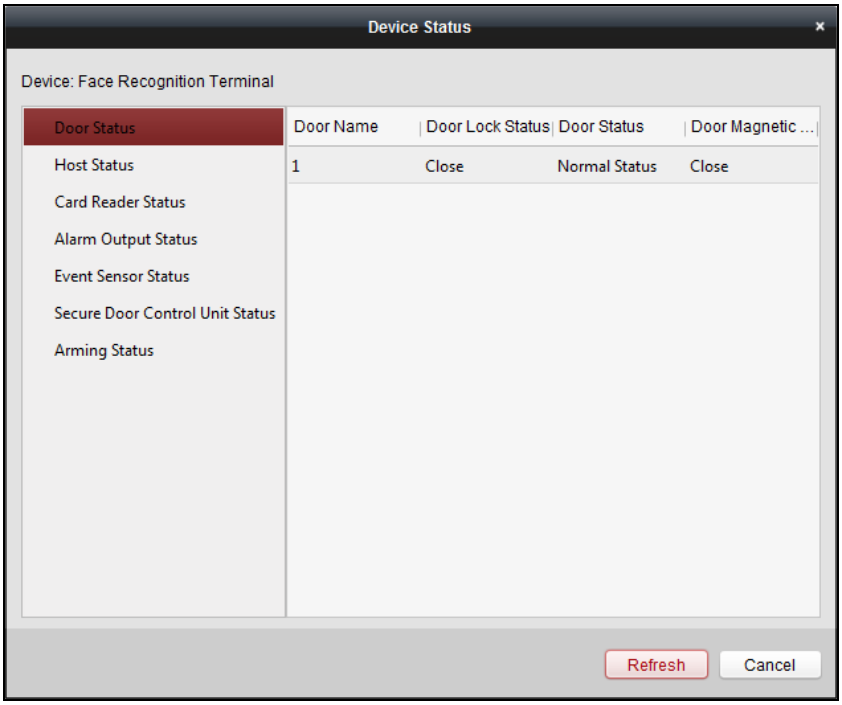
5. Нажмите [...] и выберите файл шаблона.
6. Нажмите **Add** («Добавить») для импорта устройств.

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.

7.3.2 Просмотр состояния устройства

В списке устройств вы можете выбрать устройство, а затем нажать кнопку **Device Status** («Состояние устройства») для просмотра его состояния.



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

- **Door Status** («Состояние двери»): Состояние подключенной двери.
- **Host Status** («Состояние хоста»): Состояние хоста, включая напряжение питания аккумуляторной батареи, состояние источника питания устройства, состояние блокировки нескольких дверей, состояние запрета обратного прохода и статус анти-тампериинга хоста.
- **Card Reader Status** («Состояние считывателя карт»): Состояние считывателя карт.

  Примечание: Если вы используете считыватель карт с соединением RS-485, вы можете просмотреть его состояние - онлайн или офлайн. Если вы используете считыватель карт с соединением Wiegand, вы сможете увидеть офлайн состояние.
- **Alarm Output Status** («Состояние тревожного выхода»): Состояние тревожного выхода каждого порта.
- **Event Sensor Status** («Состояние датчика событий»): Состояние датчика события каждого

порта.

- **Secure Door Control Unit Status** («Состояние модуля безопасности»): Онлайн состояние, состояние тампериинга модуля безопасности.
- **Arming Status** («Состояние постановки на охрану»): Состояние постановки устройства на охрану.

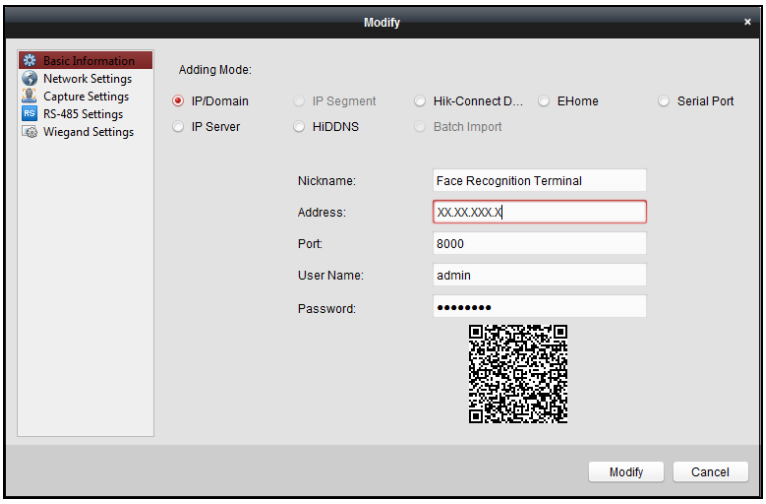
7.3.3 Редактирование основной информации

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.



4. 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»).

7.3.4 Сетевые настройки

Цель:

После добавления устройства контроля доступа вы можете настроить режим загрузки и настроить сетевой центр и центр беспроводной связи.

Выберите устройство из списка устройств и нажмите **Modify** («Изменить») для появления всплывающего окна изменения информации устройства.

Нажмите вкладку **Network Settings** («Настройки сети») для перехода в вменю сетевых настроек.

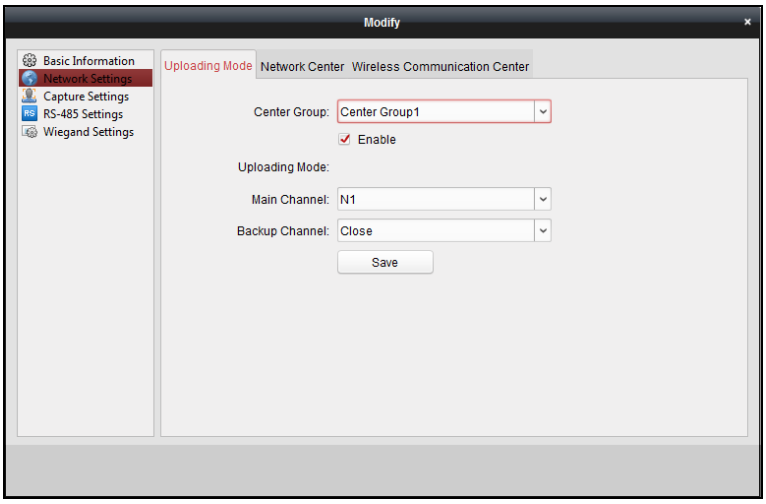
Настройки режима загрузки

Цель:

Вы можете установить группу центра для загрузки журнала через протокол EHome.

Шаги:

1. Нажмите вкладку **Uploading Mode** («Режим загрузки»).



2. Выберите группу центра из выпадающего списка.
3. Поставьте галочку **Enable** («Включить») для включения выбранной группы центра.
4. Выберите режим загрузки в раскрывающемся списке. Вы можете включить **N1/G1** для основного канала и резервного канала или выбрать **Close** («Закрыть») для отключения основного канала или резервного канала.

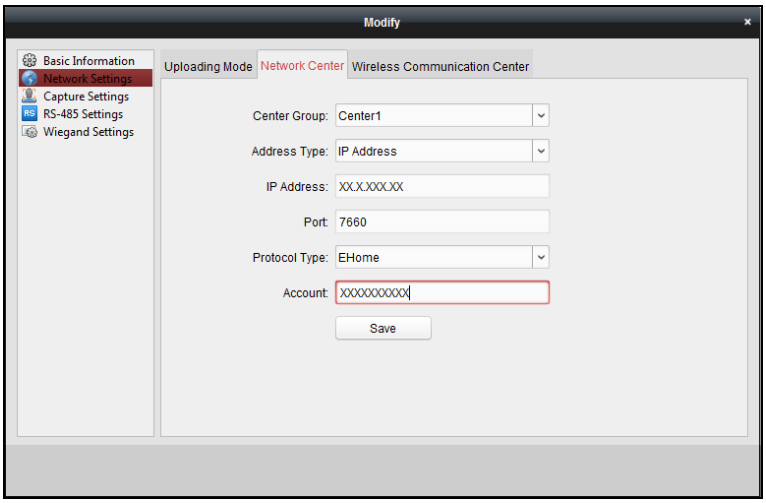
   Примечание: Основной канал и резервный канал не могут одновременно включать N1 или G1.
5. Нажмите **Save** («Сохранить») для сохранения параметров.

Настройки сетевого центра

Вы можете установить учетную запись для протокола EHome на странице сетевых настроек, затем вы сможете добавлять устройства через протокол EHome.

Шаги:

1. Нажмите вкладку **Network Center** («Сетевой центр»).



2. Выберите группу центра из выпадающего списка.
3. Выберите **Address Type** («Тип адреса»): **IP address** («IP-адрес») или **Domain Name** («Доменное имя»).
4. Введите **IP address** («IP-адрес») или **Domain name** («Доменное имя») в соответствии с типом адреса.
5. Введите **Port No.** («№ порта») для протокола. По умолчанию № порта - *7660*.
6. Выберите в поле **Protocol type** («Тип протокола») значение **EHome**.
7. Задайте имя учетной записи для сетевого центра.

   Примечание: Учетная запись должна содержать от 1 до 32 символов, и допускаются только буквы и цифры.
8. Нажмите **Save** («Сохранить») для сохранения параметров.

Примечания:

- Номер порта беспроводной сети и проводной сети должен согласовываться с номером порта EHome.
- Вы можете установить доменное имя в области **Enable NTP** («Включить NTP») в пункте *Редактирование времени* в Разделе удаленной конфигурации. Для получения подробной информации смотрите пункт *Время* в *Разделе 7.3.10 Удаленная конфигурация*.

Настройки центра беспроводной связи

Шаги:

1. Нажмите вкладку **Wireless Communication Center** («Центр беспроводной связи»).
2. Выберите группу центра из выпадающего списка.
3. Введите **IP address** («IP-адрес») и **Port No** («№ порта»).
4. Выберите в поле **Protocol type** («Тип протокола») значение **EHome**. По умолчанию № порта для EHome - *7660*.
5. Задайте имя учетной записи для сетевого центра. Постоянная учетная запись должна использоваться на одной платформе.
6. Нажмите **Save** («Сохранить») для сохранения параметров.

Примечание: Номер порта беспроводной сети и проводной сети должен согласовываться с номером порта EHome.

7.3.5 Настройки захвата

Вы можете установить параметры связанного захвата и захвата вручную.
Выберите устройство в списке устройств и нажмите **Modify** («Изменить») для появления всплывающего окна изменения информации устройства.
Нажмите вкладку **Capture Settings** («Настройки захвата») для перехода в меню настройки захвата изображений.

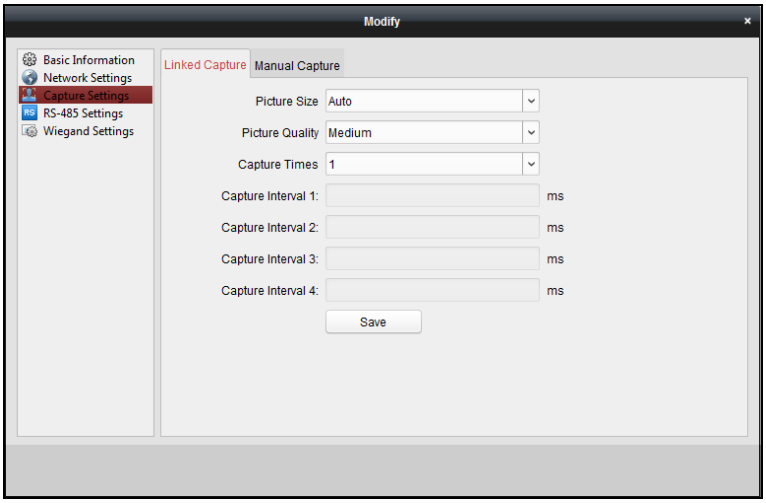
Примечания:

- Функция **Capture Settings** («Настройки захвата») должна поддерживаться устройством.
- Перед настройкой параметров захвата вы должны настроить сервер хранения для хранения изображений.

Связанный захват

Шаги:

1. Выберите вкладку **Linked Capture** («Связанный захват»).

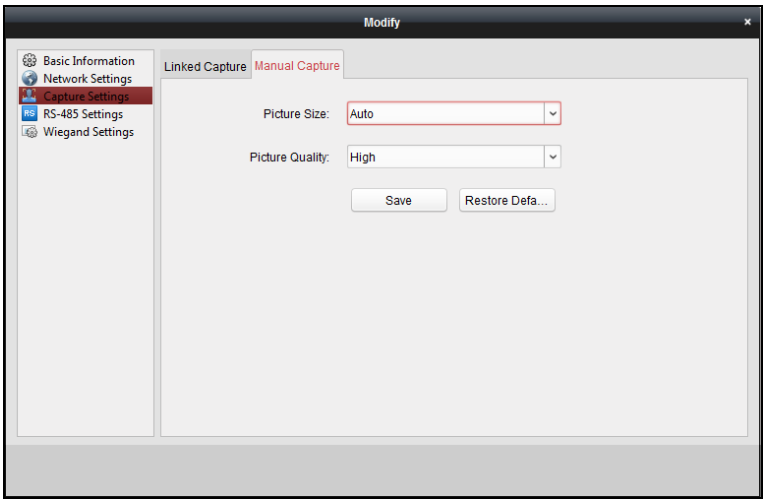


2. Установите **Picture size** («Размер изображения») и **Quality** («Качество»).
3. Установите **Capture times** («Число захватов») для одного срабатывания.
4. Нажмите **Save** («Сохранить») для сохранения параметров.

Захват вручную

Шаги:

1. Выберите вкладку **Manual Capture** («Захват вручную»).



2. Выберите **Resolution** («Разрешение») захваченного изображения из выпадающего списка.
3. Выберите в поле **Picture quality** («Качество изображения») значение **High** («Высокое»), **Medium** («Среднее») или **Low** («Низкое»).
4. Нажмите **Save** («Сохранить») для сохранения параметров.
5. Вы можете нажать **Restore Default Value** («Восстановить значения по умолчанию») для восстановления параметров по умолчанию.

7.3.6 Настройки RS-485

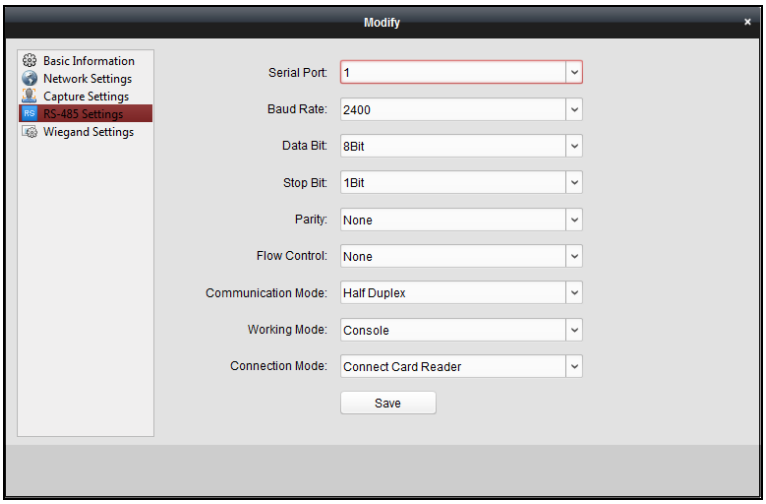
Цель:

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:

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



2. 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.

7.3.7 Настройки Wiegand

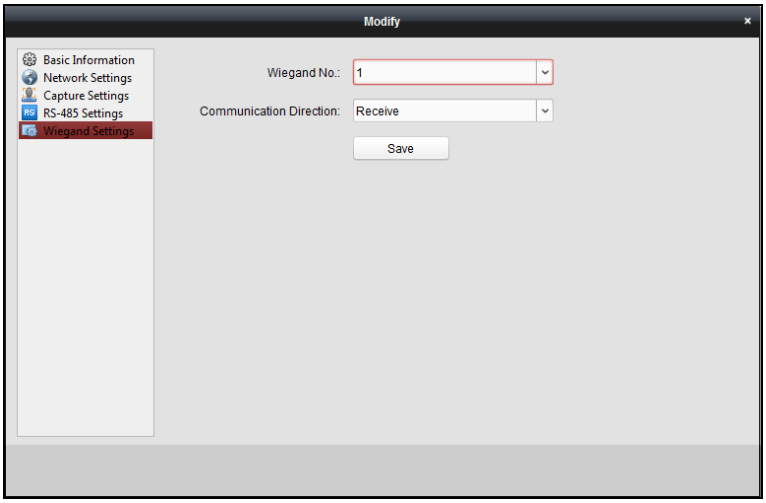
Цель:

Вы можете установить Wiegand канал и настроить режим связи.

Примечание: Настройки Wiegand должны поддерживаться устройством.

Шаги:

1. Выберите устройство в списке устройств и нажмите **Modify** («Изменить») для появления всплывающего окна изменения информации устройства.
2. Нажмите вкладку **Wiegand Settings** («Настройки Wiegand») для перехода в меню настроек Wiegand.



3. Выберите **Wiegand channel No.** («№ Wiegand канала») и **Communication Direction** («Направление связи») из выпадающего списка.

   Если вы установите в поле **Communication Direction** («Направление связи») значение **Send** («Отправка»), вам необходимо будет установить в поле **Wiegand Mode** («Режим Wiegand») значение **Wiegand 26** или **Wiegand 34**.
4. Нажмите **Save** («Сохранить») для сохранения настроек, и настроенные параметры будут применены к устройству автоматически.

Примечание: После изменения направления связи устройство будет перезагружено. После изменения направления связи появится соответствующая подсказка.

7.3.8 Настройка нескольких NIC

Цель:

Вы можете установить параметры NIC, NIC тип, IPv4-адрес, маске подсети, шлюз по умолчанию, MAC, MTU и порт устройства.

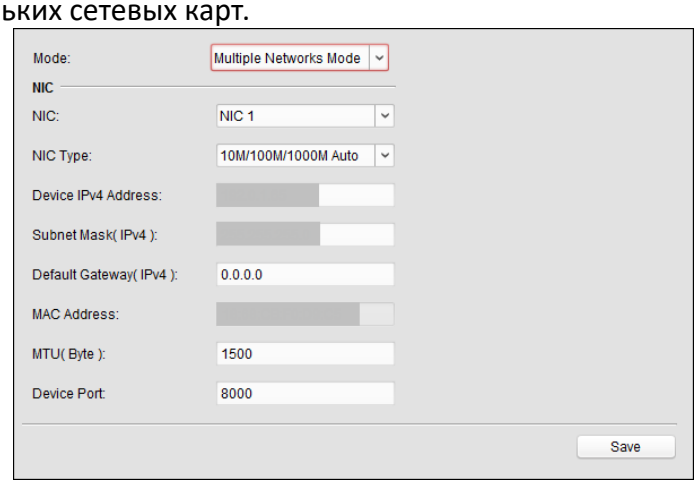
Примечание: Функция должна поддерживаться устройством.

Перед началом:

Добавление устройств при помощи учетной записи EHome.

Шаги:

1. Нажмите **Multiple NICs Settings** («Настройки нескольких NIC») для перехода на страницу настройки нескольких сетевых карт.



2. Установите параметры по вашему усмотрению.
3. Нажмите **Save** («Сохранить») для сохранения настроек.

7.3.9 Настройки терминала распознавания лиц

Цель:

Вы можете установить режим терминала распознавания лиц, включая базу данных изображений лиц, сохранение изображения лица при аутентификации, ECO режим и рабочий режим.

Примечание: Функция должна поддерживаться устройством.

Шаги:

1. Нажмите **Face Recognition Terminal Settings** («Настройки терминала распознавания лиц») для перехода в соответствующее меню.
2. Задайте параметры терминала распознавания лиц.
   Описание параметров представлено ниже:

Параметр	Описание
Face Picture Database («База данных изображений лиц»)	Вы можете выбрать значение **Deep Learning** («Глубокое обучение») в качестве базы данных изображений лиц.
Save Authenticating Face Picture	При включении функции захваченное изображение лица при аутентификации будет сохранено на устройстве.

Параметр	Описание
(«Сохранить изображение лица при аутентификации»)	
ECO Mode («ЭКО режим»)	После включения ЭКО режима устройство будет использовать ИК-камеру для аутентификации лиц в условиях низкой освещенности или в темноте. И вы можете установить порог ЭКО режима, ЭКО режим (1:N) и ЭКО режим (1:1).
ECO Mode (1:1) («ECO режим (1:1)»)	Установите порог совпадения при аутентификации в ЭКО режиме 1:1. Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 75.
ECO Mode (1:N) («ECO режим (1:N)»)	Установите порог совпадения при аутентификации в ЭКО режиме 1:N. Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 84.
ECO Mode Threshold («Порог ЭКО режима»)	При включении ЭКО режима вы можете установить порог ЭКО режима. Чем больше значение, тем легче устройство переходит в режим ЭКО. Доступный диапазон: от 0 до 8.
Work Mode («Рабочий режим»)	Установите в качестве режима работы устройства значение **Access Control Mode** («Режим контроля доступа»). Режим контроля доступа - это обычный режим устройства. Вы должны подтвердить свои учетные данные для доступа.

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

Вы также можете установить параметры в меню **Remote Configuration** («Удаленная конфигурация»). Для получения подробной информации смотрите *Раздел 7.3.10 Удаленная конфигурация*.

7.3.10 Удаленная конфигурация

Цель:

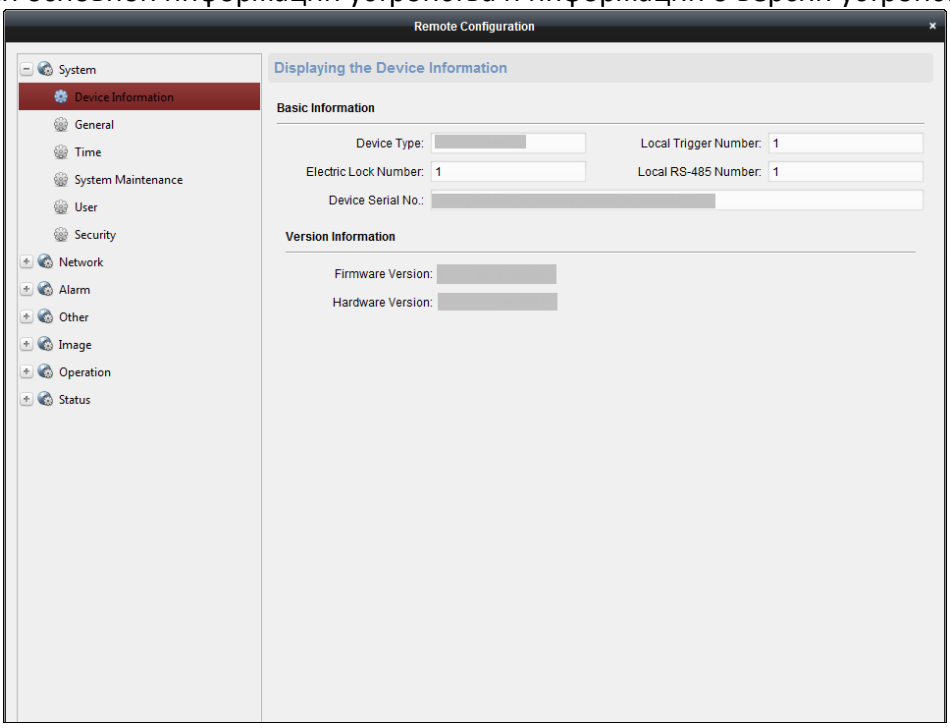
В списке устройств выберите устройство и нажмите кнопку **Remote Configuration** («Удаленная конфигурация») для перехода в меню удаленной конфигурации. Вы можете установить параметры выбранного устройства.

Проверка информации устройства

Шаги:

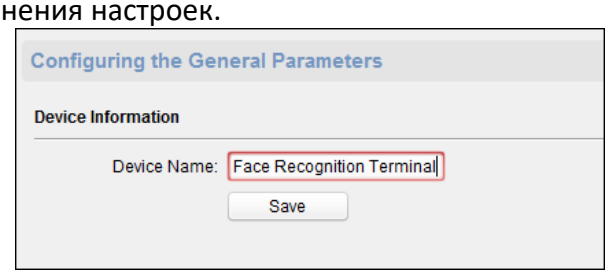
1. В списке устройств вы можете нажать **Remote Configuration** («Удаленная конфигурация») для перехода в меню удаленной конфигурации.
2. Нажмите **System -> Device Information** («Система -> Информация устройства») для

проверки основной информации устройства и информации о версии устройства.



Изменение имени устройства

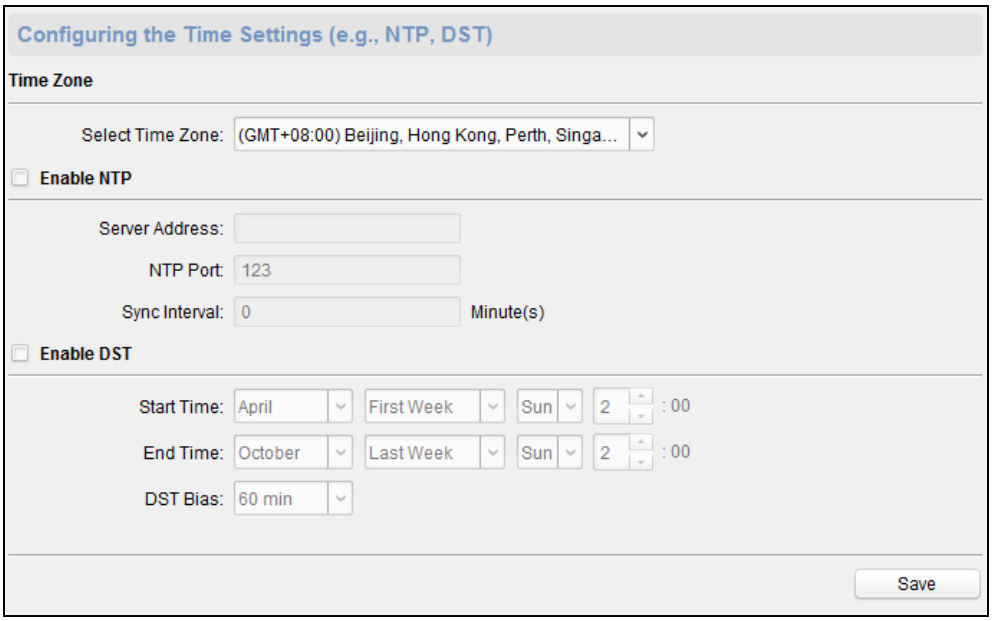
В меню удаленной конфигурации нажмите **System -> General** («Система -> Общие») для конфигурации имени устройства и перезаписи параметра файлов записи. Нажмите **Save** («Сохранить») для сохранения настроек.



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»), **End time** («Время окончания DST») и **Bias** («Смещение»).
4. Нажмите **Save** («Сохранить») для сохранения настроек.



Настройка обслуживания системы

Цель:

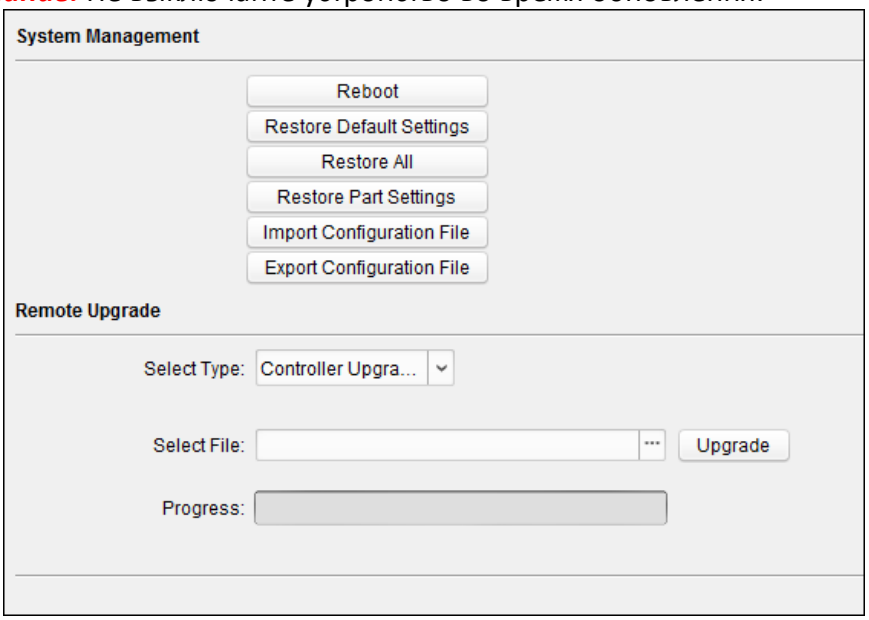
Вы можете перезагрузить устройство удаленно, восстановить настройки устройства по умолчанию, импортировать файл конфигурации, обновить устройство и т. д.

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.
   Или нажмите **Restore Part of Settings** («Восстановить часть настроек») для восстановления всех настроек, кроме настроек связи и настроек удаленного пользователя до значений по умолчанию.
   Или нажмите **Import Configuration File** («Импорт файла конфигурации») для импорта файла конфигурации с локального ПК на устройство.
   Или нажмите **Export Configuration File** («Экспорт файла конфигурации») для экспорта файла конфигурации с устройства на локальный ПК.
   Примечание: Файл конфигурации содержит параметры устройства.
3. Вы также можете удаленно обновить устройство.
   1) В разделе **Remote Upgrade** («Удаленное обновление») выберите тип обновления.
      Примечания:
      - Вам необходимо установить ID устройства перед обновлением, если в качестве типа удаленного обновления вы выбрали **Controller Upgrade File** («Файл обновления контроллера»).
      - Только считыватель карт, подключенный по протоколу RS-485, поддерживает обновление.

- Если вам необходимо обновить систему устройства, убедитесь, что версия контроллера и версия модуля расширения совпадают. Здесь контроллер относится к системе TX1 в то время как модуль расширения относится к системе MCU.

2) Нажмите ··· для выбора файла обновления.
3) Нажмите **Upgrade** («Обновить») для начала обновления.
   Примечание: Не выключайте устройство во время обновления.



Конфигурация параметров RS-485

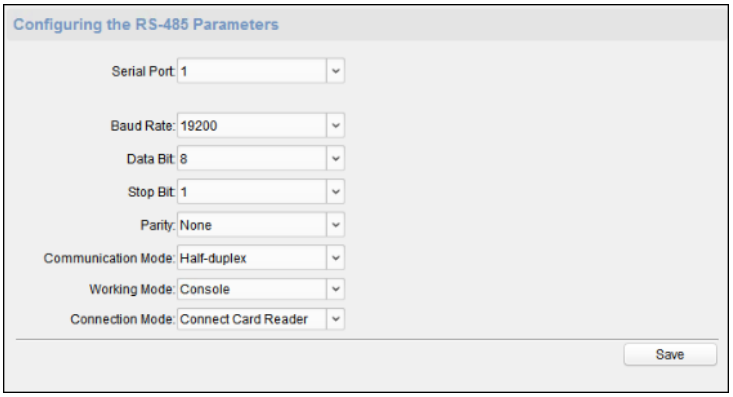
Цель:

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: Настройка параметров RS-485 должна поддерживаться устройством.

Шаги:

1. На странице удаленной конфигурации нажмите **System -> RS-485 Settings** («Система -> Настройки RS-485») для перехода на страницу конфигурации параметров RS-485.



2. Выберите **Port serial No.** («№ последовательного порта») из выпадающего списка для установки параметров RS-485.

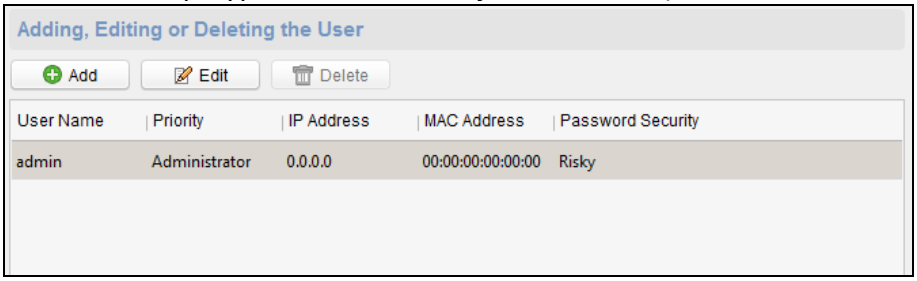
3. Установите **Baud rate** («Скорость передачи в бодах»), **Data bit** («Бит данных»), **Stop bit** («Стоповый бит»), **Parity** («Четность»), **Flow control** («Управление потоком»), **Communication mode** («Режим связи»), **Working mode**, («Рабочий режим») и **Connection mode** («Режим подключения»).
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.

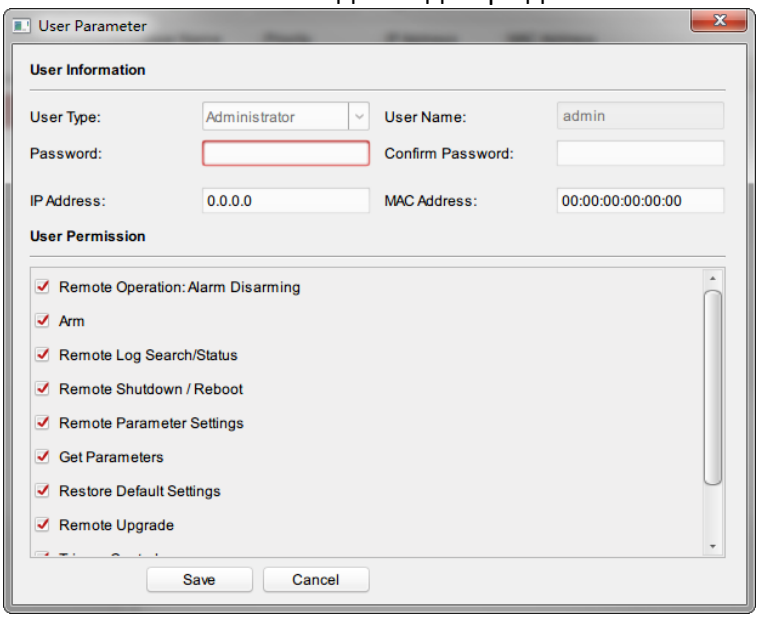
Управление пользователями

Шаги:

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



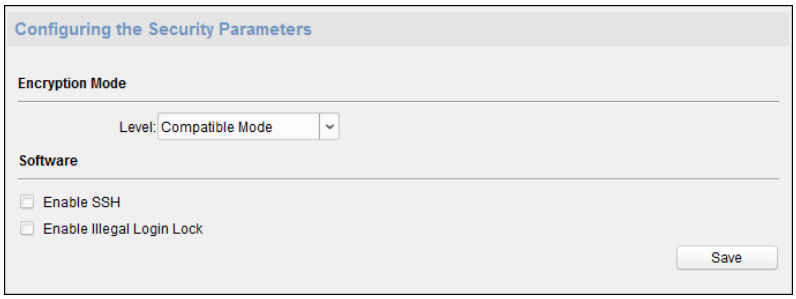
2. Нажмите **Add** («Добавить») для добавления пользователя (Не поддерживается контроллером лифта.).
   Или выберите пользователя из списка и нажмите **Edit** («Редактировать») для изменения пользователя. Вы можете изменить пароль пользователя, IP-адрес, MAC-адрес и разрешения пользователя. Нажмите **OK**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



Настройка безопасности

Шаги:

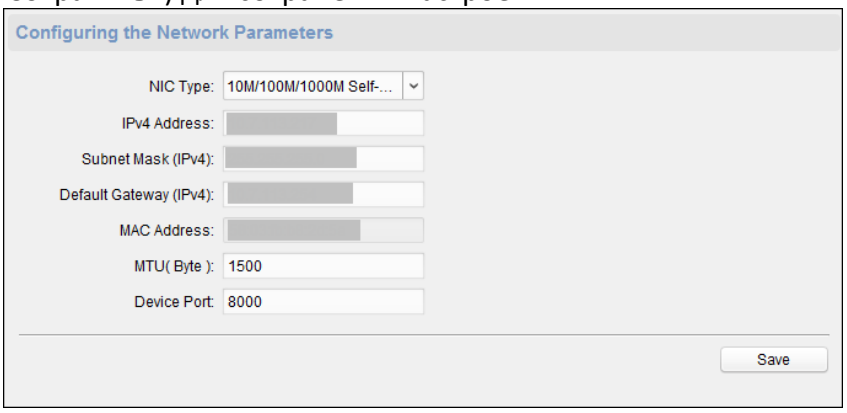
1. Нажмите **System -> Security** («Система -> Безопасность»).



2. Выберите **Encryption mode** («Режим шифрования») из выпадающего списка.
   Вы можете выбрать **Compatible Mode** («Совместимый режим») или **Encryption Mode** («Режим шифрования»).
   Compatible Mode («Совместимый режим»): Верификация пользовательской информации совместима со старой версией Клиентского программного обеспечения при входе в систему.
   Encryption Mode («Режим шифрования»): Высокий уровень безопасности при верификации пользовательской информации при входе в систему.
3. (Опционально) Поставьте галочку **Enable SSH** («Включить SSH»).
4. Нажмите **Save** («Сохранить») для сохранения настроек.

Конфигурация сетевых параметров

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



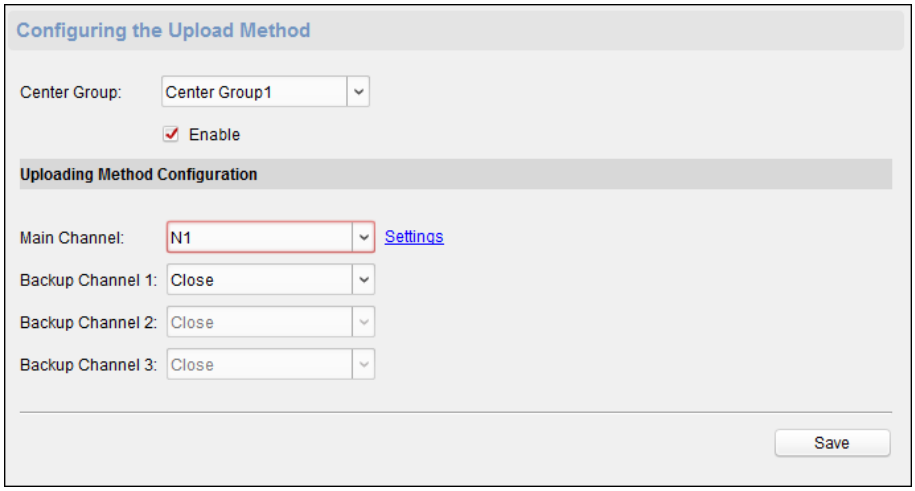
Настройка способа загрузки

Цель:

Вы можете установить группу центра для загрузки журнала через протокол EHome.

Шаги:

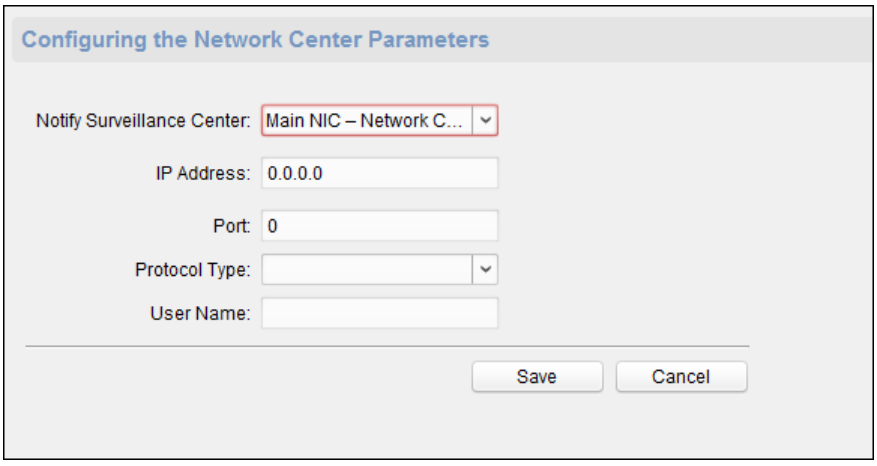
1. Нажмите **Network -> Report Strategy** («Сеть -> Стратегия отчета»).



2. Выберите группу центра из выпадающего списка.
3. Поставьте галочку **Enable** («Включить»).
4. Установите способ загрузки.
   Вы можете установить основной канал и резервный канал.
   Main Channel/Backup Channel («Основной канал/Резервный канал»): Устройство будет связываться с центром через основной канал. Когда происходит исключение в основном канале, устройство и центр будут связываться через резервный канал.
   Примечание: «N1» - относится к проводной сети, а «G1» - относится к GPRS.
5. Нажмите **Settings** («Настройки») справа от поля выбора канала для настройки подробной информации.
6. Нажмите **Save** («Сохранить») для сохранения настроек.

Конфигурация сетевого центра

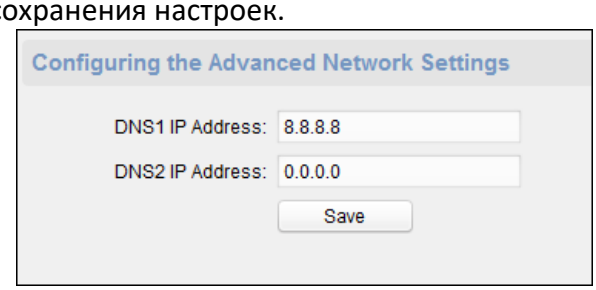
Вы можете установить уведомление центра наблюдения, настроив IP-адрес центра, номер порта, протокол (EHome) и имя пользователя учетной записи EHome для передачи данных по протоколу EHome. Для получения подробной информации смотрите *Настройки сетевого центра* в *Разделе 7.3.4 Сетевые настройки.* Нажмите **Save** («Сохранить») для сохранения настроек.



Настройка расширенных сетевых параметров

Нажмите **Network -> Advanced Settings** («Сеть -> Расширенные настройки»). Вы можете

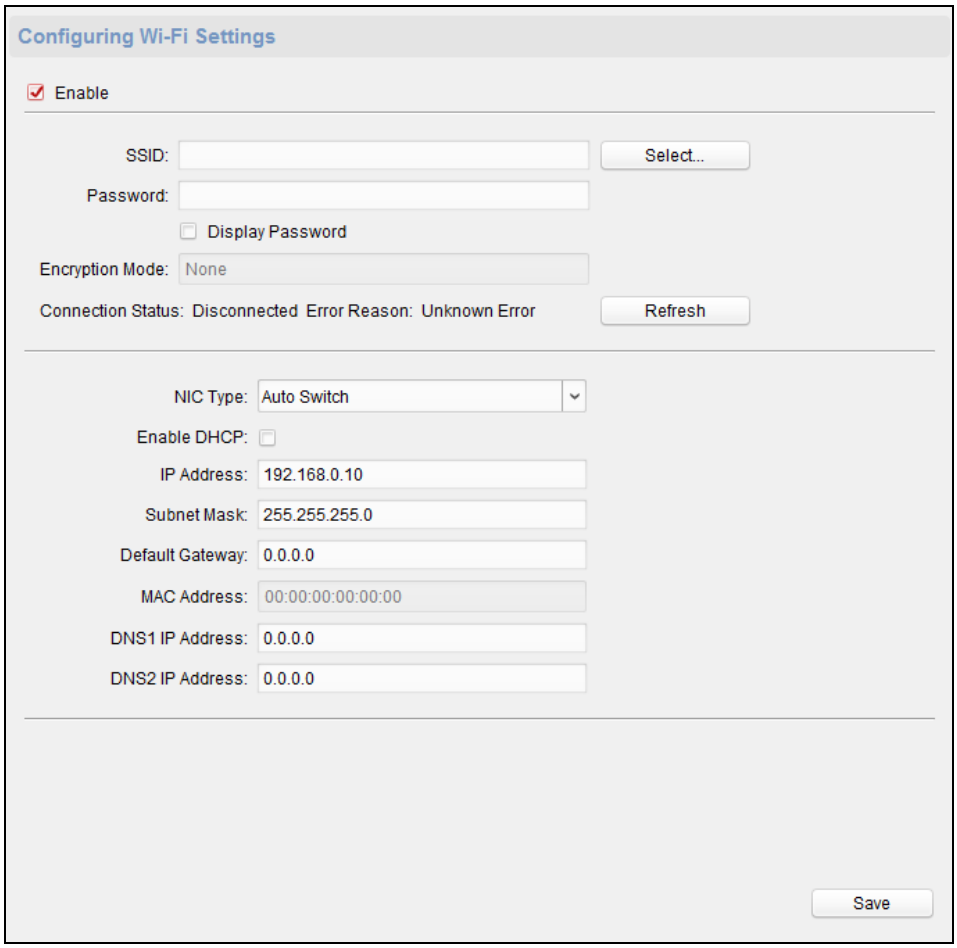
настроить **DNS IP address 1** («IP-адрес DNS 1»), **DNS IP address 2** («IP-адрес DNS 2»). Нажмите **Save** («Сохранить») для сохранения настроек.



Конфигурация Wi-Fi

Шаги:

1. Нажмите **Network –> Wi-Fi** («Сеть -> Wi-Fi»).



2. Поставьте галочку **Enable** («Включить») для включения функции Wi-Fi.
3. Введите название сети в поле **SSID**.
   Или вы можете нажать кнопку **Select…** («Выбрать…») для выбора Wi-Fi сети.
4. Введите пароль Wi-Fi в поде **Password** («Пароль»).
5. (Опционально) Нажмите **Refresh** («Обновить») для обновления сетевого статуса.
6. (Опционально) Выберите **NIC Type** («Тип NIC»).
7. (Опционально) Снимите галочку **Enable DHCP** («Включить DHCP») и установите значения в полях **IP address** («IP-адрес»), **Subnet mask** («Маска подсети»), **Default gateway** («Шлюз по

умолчанию»), **MAC address** («MAC-адрес»), **DNS1 IP Address** («IP-адрес DNS1») и **DNS2 IP address** («IP-адрес DNS2»).

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

Конфигурация параметров сети и SIP

Установите IP-адрес монитора консьержа и IP-адрес SIP-сервера. После настройки параметров вы сможете установить связь между устройством контроля доступа, вызывной панелью, видеодомофоном, монитором консьержа и платформой.

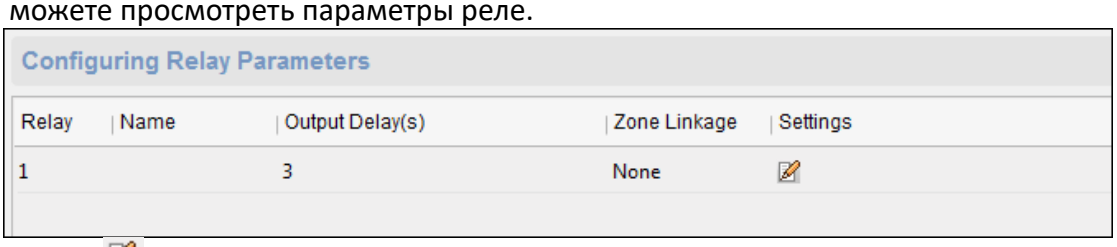
Примечание: Только среди устройств контроля доступа и других устройства или систем (такие как вызывная панель, видеодомофон, монитор консьержа, платформа), находящихся в одном и том же IP сегменте, может выполняться двусторонняя аудио связь.

Нажмите **Network – Linked Network Configuration** («Сеть - Конфигурация связанной сети») и установите IP-адрес монитора консьержа и IP-адрес SIP-сервера. Нажмите **Save** («Сохранить») для сохранения настроек.

Конфигурация параметров реле

Шаги:

1. Нажмите **Alarm -> Relay** («Тревога -> Реле»).
   Вы можете просмотреть параметры реле.



2. Нажмите  для появления всплывающего окна настройки параметров реле.
3. Настройте значения в полях **Relay name** («Имя реле») и **Output delay** («Задержка вывода»).
4. Нажмите **Save** («Сохранить») для сохранения параметров.
   Или нажмите **Copy to…** («Копировать в») для копирования информации реле в другие реле.

Конфигурация параметров контроля доступа

Шаги:

1. В меню удаленной конфигурации нажмите **Other -> Access Control Parameters** («Другие -> Параметры контроля доступа»).
2. Отметьте необходимые поля.
   - **Overlay User Information on Picture** («Наложение информации пользователя на изображение»): Отображение пользовательской информации на захваченных изображениях.
   - **Enable Voice Prompt** («Включить голосовые подсказки»): Если галочка установлена, включены голосовые подсказки в устройстве. Вы можете услышать голосовые подсказки при работе с устройством.
   - **Upload Pictures after Capturing** («Выгрузить изображение после захвата»): Если

галочка установлена, изображения, захваченные связанной камерой, будут автоматически загружаться в систему.

- **Save Captured Pictures** («Сохранять захваченные изображения»): Если галочка установлена, вы сможете сохранять захваченные связанной камерой изображения на устройство.
- **Enable 3G/4G** («Включить 3G/4G»): Если галочка установлена, устройство включит функцию 3G/4G связи.

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

Конфигурация параметров терминала распознавания лиц

Шаги:

1. Нажмите **Other – Face Recognition Terminal Parameters** («Другие – Параметры терминала распознавания лиц») для перехода на соответствующую страницу.
2. Задайте параметры.

   Описание параметров представлено ниже:

Параметр	Описание
Face Picture Database («База данных изображений лиц»)	Вы можете выбрать **Deep Learning** («Глубокое обучение») в качестве базы данных лиц.
Save Authenticating Face Picture («Сохранять изображение лица при аутентификации»)	При включении функции изображение захваченного лица при аутентификации будет сохранено на устройстве.
ECO Mode («ЭКО режим»)	После включения ЭКО режима устройство будет использовать ИК-камеру для аутентификации лиц в условиях низкой освещенности или в темноте. И вы можете установить порог ЭКО режима, ЭКО режим (1:N) и ЭКО режим (1:1).
ECO Mode (1:1) («ECO режим (1:1)»)	Установите порог совпадения при аутентификации в ЭКО режиме 1:1. Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 75.
ECO Mode (1:N) («ECO режим (1:N)»)	Установите порог совпадения при аутентификации в ЭКО режиме 1:N. Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 84.
ECO Mode Threshold («Порог ЭКО режима»)	При включении ЭКО режима вы можете установить порог ЭКО режима. Чем больше значение, тем легче устройство переходит в режим ЭКО. Доступный диапазон: от 0 до 8.

Work Mode («Рабочий режим»)	Установите в качестве режима работы устройства значение **Access Control Mode** («Режим контроля доступа»). Режим контроля доступа - это обычный режим устройства. Вы должны подтвердить свои учетные данные для доступа.

Конфигурация параметров изображения лица

Нажмите **Other – Face Picture Parameters** («Другие – Параметры изображения лица») для перехода на страницу конфигурации параметров изображения лица. Вы можете установить параметры изображения лица при аутентификации. Нажмите **Save** («Сохранить») для сохранения настроек.

Описание параметров представлено ниже:

Параметр	Описание
Min. Detection Width (Close to) («Мин. ширина детекции (Близость к)»)	Когда расстояние между камерой и пользователем маленькое, параметр представляет минимальный процент ширины лица в общей ширине области распознавания. При аутентификации фактический процент ширины лица должен быть больше заданного значения. В этом состоянии устройство не обнаружит других параметров.
Pitch Angle («Угол наклона»)	Максимальный угол наклона при аутентификации лиц. По умолчанию угол составляет 30°.
Yaw Angle («Угол поворота»)	Максимальный угол поворота при аутентификации лиц. По умолчанию угол составляет 20°.
Min. Detection Area (Width) («Мин. область детекции (ширина)»)	Когда расстояние между камерой и пользователем большое, параметр представляет минимальный процент ширины лица в общей ширине области распознавания. При аутентификации фактический процент ширины лица должен быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям. Рекомендуемое значение: 14
Min. Detection Area (Height) («Мин. область детекции (высота)»)	Когда расстояние между камерой и пользователем большое, параметр представляет минимальный процент высоты лица в общей высоте области распознавания. При аутентификации фактический процент высоты лица должен быть больше заданного значения.

Параметр	Описание
	Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям. Рекомендуемое значение: 12
Margin (Left) («Отступ (Левый)»)	Расстояние от левого края лица до левого края области распознавания. При аутентификации фактическое расстояние должно быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям.
Margin (Right) («Отступ (Правый)»)	Расстояние от правого края лица до правого края области распознавания. При аутентификации фактическое расстояние должно быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям.
Margin (Top) («Отступ (Верхний)»)	Расстояние от верхнего края лица до верхнего края области распознавания. При аутентификации фактическое расстояние должно быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям
Margin (Bottom) («Отступ (Нижний)»)	Расстояние от верхнего нижнего лица до нижнего края области распознавания. При аутентификации фактическое расстояние должно быть больше заданного значения. Другие процентные соотношения, расстояния и углы из этой таблицы также должны соответствовать необходимым условиям.
Pupillary Distance («Межзрачковое расстояние»)	Минимальное расстояние между двумя зрачками при распознавании лица. Фактическое расстояние должно быть больше заданного значения. По умолчанию расстояние равно 40.

Конфигурация параметров вспомогательной подсветки

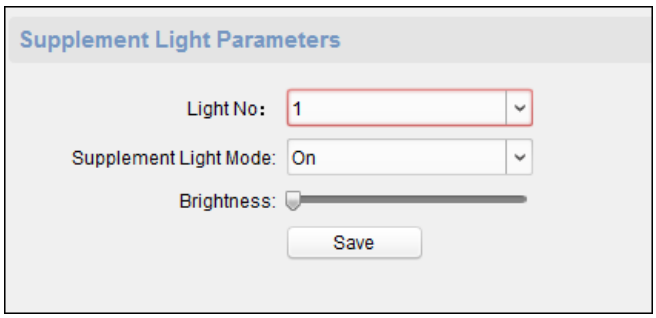
Цель:

Вы можете включить или выключить дополнительную подсветку. Вы также можете отрегулировать ее яркость.

Шаги:

1. Нажмите **Other – Supplement Light Parameters** («Другие – Параметры вспомогательной

подсветки») для перехода на страницу конфигурации параметров вспомогательной подсветки.



2. Выберите номер вспомогательной подсветки из выпадающего списка в поле **Light No.** («№ подсветки»).
   Примечание: **Light 1** («Подсветка 1») – это белая подсветка, **Light 2** («Подсветка 2») – это ИК-подсветка.
3. Выберите **Supplement light mode** («Режим вспомогательной подсветки») из выпадающего списка.
4. (Опционально) Если в поле **Supplement light mode** («Режим вспомогательной подсветки») установлено значение **Auto** («Авто»), вы можете установить яркость вспомогательной подсветки.
5. Нажмите **Save** («Сохранить») для сохранения настроек.

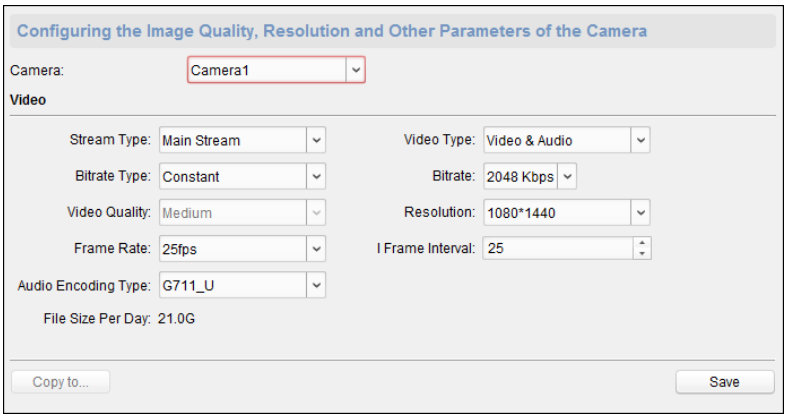
Конфигурация видео и аудио параметров

Цель:

Вы можете установить качество изображения камеры устройства, разрешение и другие параметры.

Шаги:

1. Нажмите **Image – Video & Audio** («Изображение – Видео и Аудио») для перехода на страницу настроек.

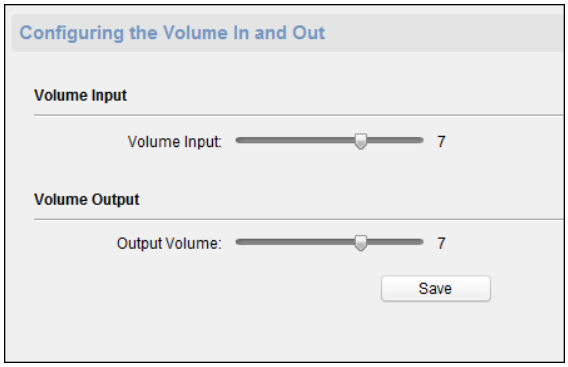


2. Задайте параметры камеры устройства, включая **Stream type** («Тип потока»), **Bitrate type** («Тип битрейта»), **Video quality** («Качество видео»), **Frame rate** («Частота кадров»), **Audio encoding type** («Тип кодирования аудио»), **Video type** («Видео тип»), **Bitrate** («Битрейт»), **Resolution** («Разрешение») и **I frame interval** («Интервал I кадра»).
3. Нажмите **Save** («Сохранить») для сохранения настроек.

Конфигурация громкости входа и выхода

Шаги:

1. Нажмите **Image – Volume Input/Output** («Изображение – Громкость входа/выхода») для перехода на соответствующую страницу.

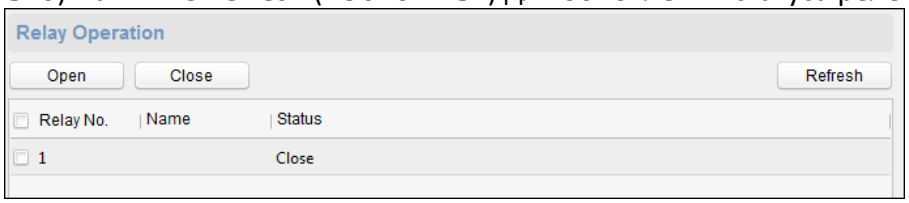


2. Установите уровень громкости входа и выхода устройства.
3. Нажмите **Save** («Сохранить») для сохранения параметров.

Управление реле

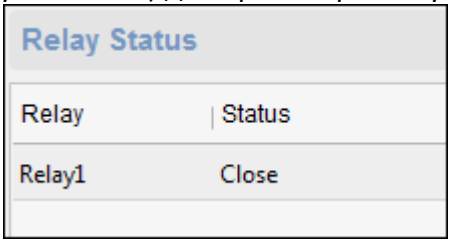
Шаги:

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



Просмотр статуса реле

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



7.4 Управление организацией

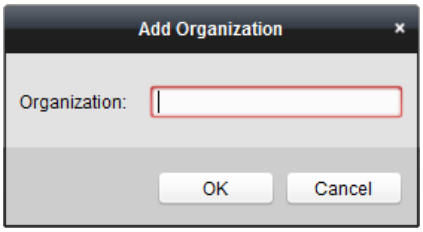
Вы можете добавлять, изменять или удалять организации по вашему желанию.

Нажмите иконку  для перехода в меню управления людьми и картами.

7.4.1 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 организации.

7.4.2 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.

7.5 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.

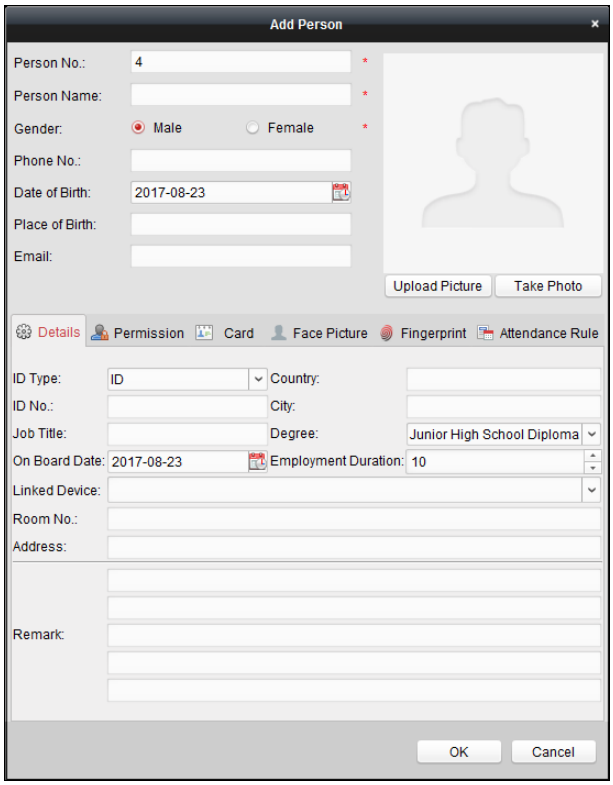
Примечание: Может быть добавлено до 10,000 человек или карт.

7.5.1 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.

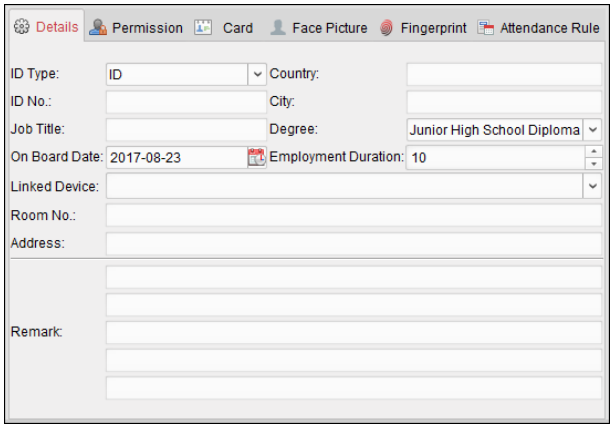


2. **Person No.** («№ человека») будет сгенерирован автоматически и не может быть изменен.
3. Введите основную информацию, включая **Person name** («Имя человека»), **Gender** («Пол»), **Phone No.** («№ телефона»), **Birthday details** («Детали рождения») и **Email**.
4. Нажмите **Upload Picture** («Загрузить 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.

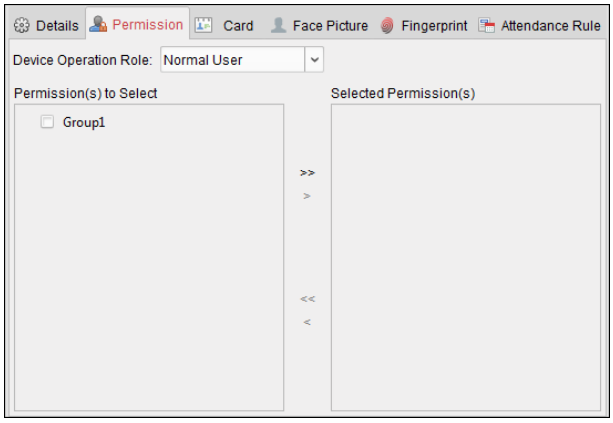
Добавление человека (Разрешения)

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 7.7 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 **OK** для сохранения настроек.

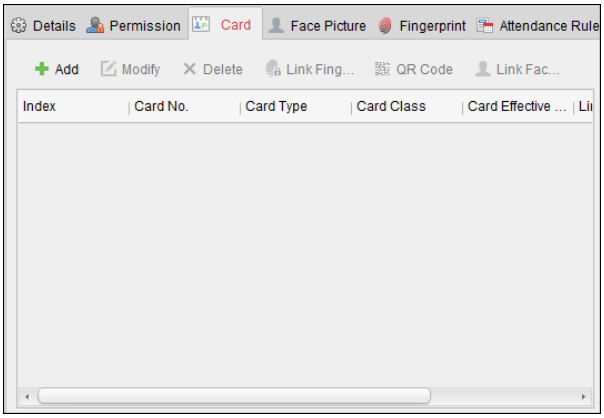
Добавление человека (Карта)

Вы можете добавлять карты и выдавать их людям.

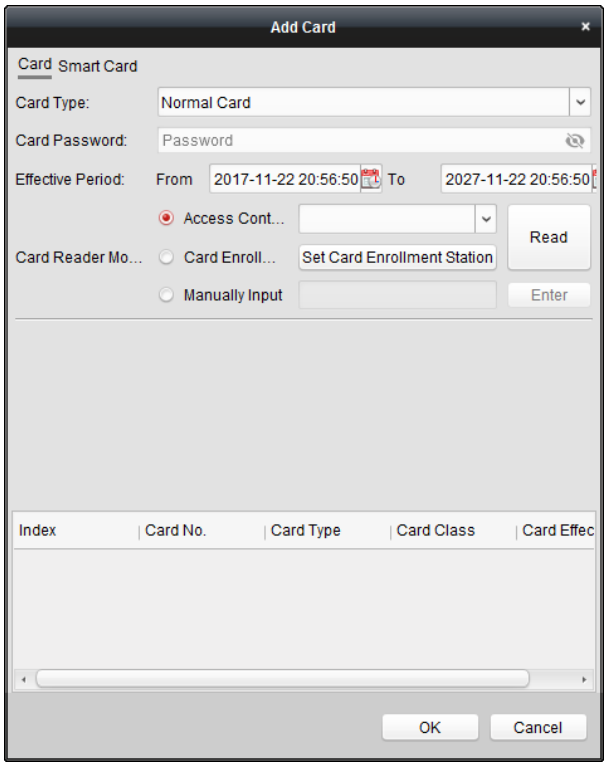
➢ Добавление обычной карты

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 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 может быть 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»).

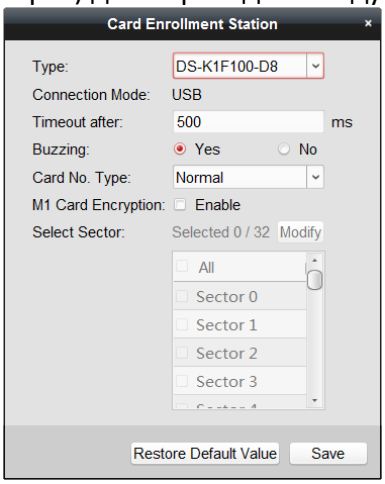
     Примечание: Параметр **Max. Swipe Times** («Макс. число проводок») должен быть в промежутке от 0 до 255. При установке значения «0» количество проводок карты не ограничено.
5. Введите пароль от самой карты в поле **Card Password** («Пароль карты»). Пароль карты должен содержать от 4 до 8 цифр.

   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»).

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** («Зуммер») 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») 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.

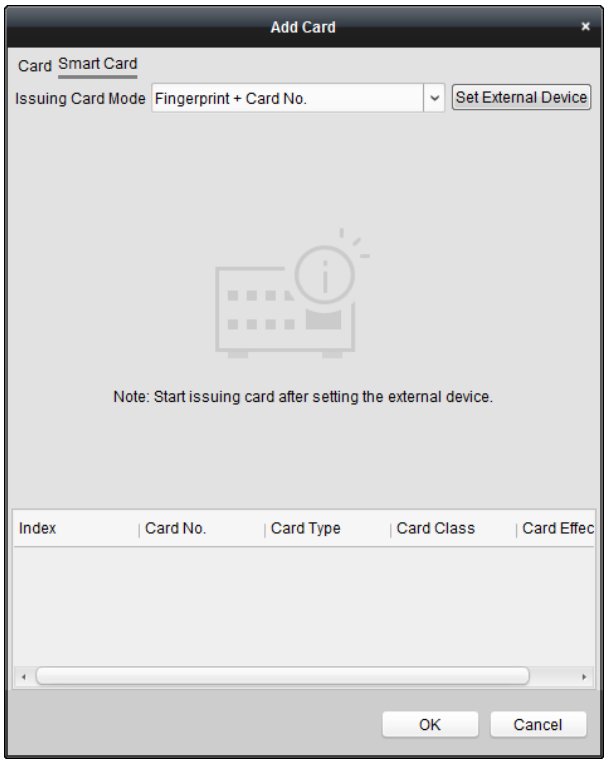
- **Добавление смарт карты**

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 может быть 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»).

  Примечание: Параметр **Max. Swipe Times** («Макс. число проводок») должен быть в промежутке от 0 до 255. При установке значения «0» количество проводок карты не ограничено.
- **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 лица)

Вы может получить изображение лица при помощи локальной загрузки, локального сбора и удаленного сбора.

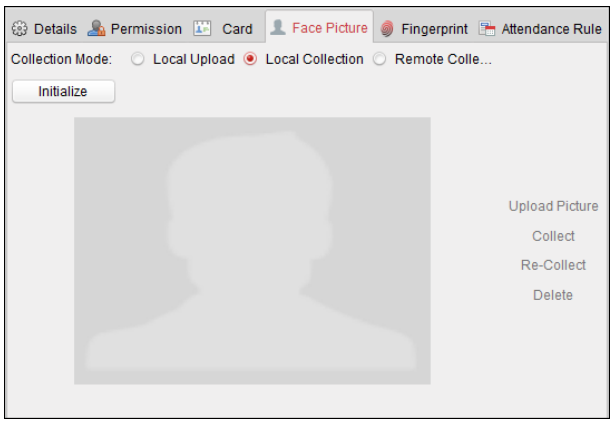
- **Local Upload** («Локальная загрузка»): Загрузка изображения лица с локального ПК.

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

  Примечание: Терминал контроля доступа должен поддерживать функцию распознавания лиц.

Шаги:

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



2. Для загрузки изображения лица с локального ПК:
   1) Выберите **Local Upload** («Локальная загрузка»).
   2) Нажмите **Upload Picture** («Загрузить изображение») и выберите изображение на локальном ПК.

      Примечание: Загруженное изображение должно быть в формате JPG, а размер должен быть менее 200 Кб.
   3) (Опционально) По умолчанию загруженное изображение лица должно быть верифицировано устройством.

      Вы можете выбрать устройство из выпадающего списка, чтобы верифицировать загруженное изображение лица. Только после того, как изображение лица верифицировано, оно будет окончательно добавлено.
3. Для получения изображения лица при помощи сканера изображений лиц:
   1) Выберите **Local Collection** («Локальный сбор»).
   2) Подключите сканер изображений лиц к ПК.
   3) Выберите тип устройства.

      Примечание: В настоящее время поддерживается сканер изображений лиц модели DS2CS5432B-S.
   4) (Опционально) Вы можете нажать **Initialize** («Инициализировать») для инициализации сканера изображений лиц.
4. Для получения изображения лица при помощи 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.

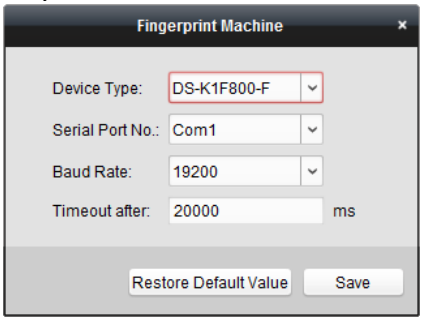
5. Нажмите **Collect** («Сбор») для захвата изображения лица.
   Вы можете нажать **Re-Collect** («Повторный сбор») для повторного выполнения захвата изображения лица.
   Вы можете нажать **Delete** («Удалить») для удаления захваченного изображения.
6. Нажмите **OK** для сохранения настроек.

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.

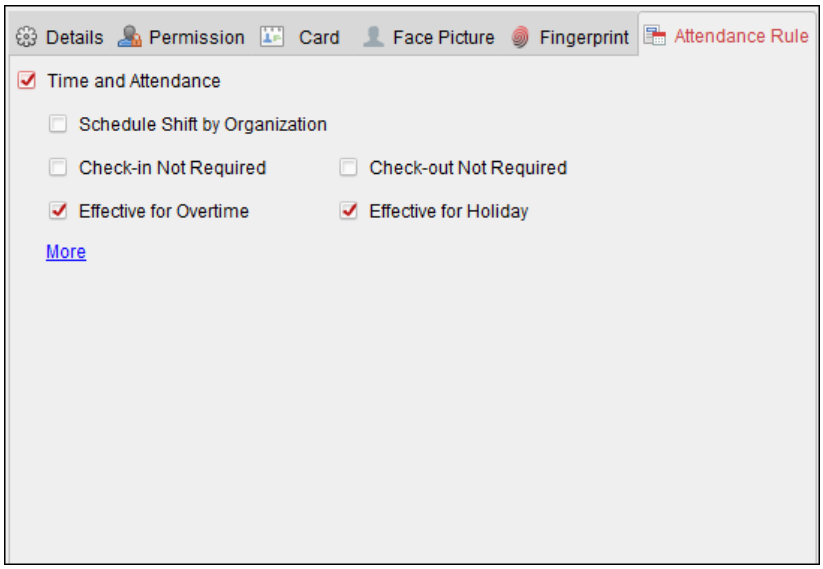
Добавление человека (Правило посещения)

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 информации людей

Вы можете импортировать информацию о нескольких людях (включая идентификационную информацию, данные отпечатков пальцев и номер карты, с которой связан отпечаток пальца) в Клиентское программное обеспечение в пакетном режиме, импортировав Excel файл с локального ПК.

Шаги:

1. Нажмите **Import Person** («Импорт человека») и нажмите **Person Information** («Информация человека») в качестве содержимого импорта.
2. Во всплывающем окне нажмите **Download Template for Importing Person** («Скачать шаблон для импорта людей») для скачивания шаблона.
3. Введите информацию о человеке в загруженный шаблон.
   Примечание: Если у человека есть несколько карточек, разделите номера карточек при помощи точкой с запятой.
4. Выберите Excel файл с информацией о человек.
5. Нажмите **OK** для начала импорта.
   Примечание: Если № человека уже существует в базе данных Клиентского ПО, оно автоматически заменит информацию о человеке после импорта.

Импорт изображений людей

Цель:

После добавления людей, вы можете импортировать изображения нескольких людей в пакетном режиме при помощи импорта ZIP файла с изображениями в Клиентское ПО.

Шаги:

1. Переименуйте изображения в соответствии с именами людей.
   Примечание: Изображение должно быть в формате JPG и меньше 200 Кб.
2. Создайте из необходимых изображений людей ZIP архив.
3. В модуле **Person and Card** («Люди и карты») нажмите **Import Person** («Импорт человека») и нажмите **Person Pictures** («Изображение человека») в качестве содержимого импорта.
4. Во всплывающем окне выберите ZIP файл.
5. Нажмите **OK** для начала импорта.
   Примечание: По умолчанию импортированное изображение человека связано с первой картой этого человека.

Экспорт информации человека

Вы можете экспортировать информацию о добавленных людях на локальный ПК в формате Excel.

Шаги:

1) После добавления человека вы можете нажать кнопку **Export Person** («Экспорт человека») для появления соответствующего всплывающего окна.
2) Выберите путь для сохранения экспортированного Excel файла.
3) Выберите элементы информации о человеке для экспорта.

4) Нажмите **OK** для начала экспорта.

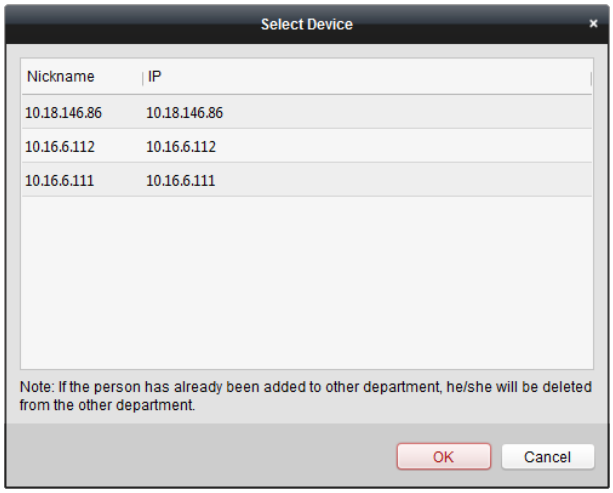
Получение информации о человеке с устройства контроля доступа

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 при добавлении устройства.

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.

7.5.2 Управление людьми

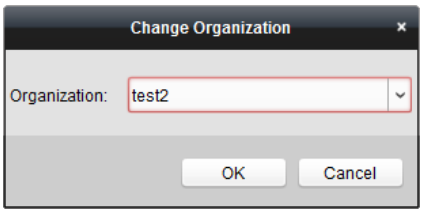
Изменение и удаление людей

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.

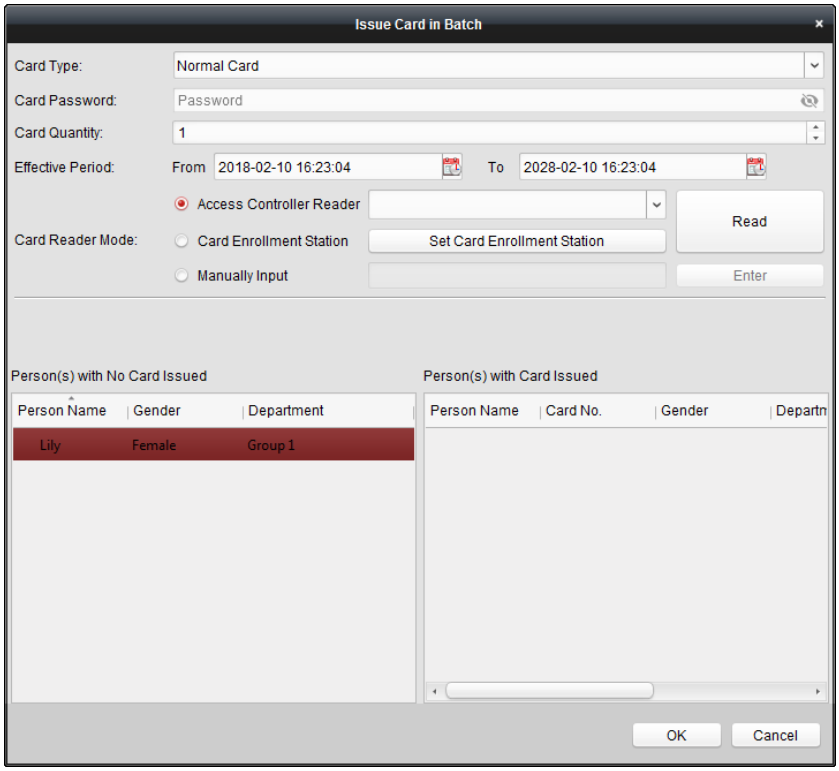
Поиск людей

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.

7.5.3 Выдача карт в пакетном режиме

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

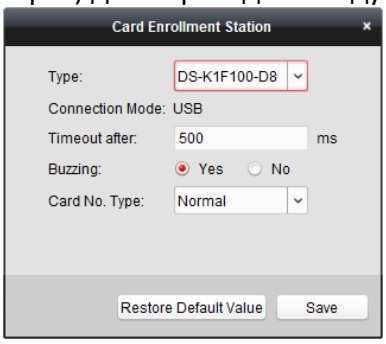
1. Нажмите кнопку **Issue Card in Batch** («Пакетная выдача карт») для перехода в следующее меню.
   Все добавленные люди, которым не были выданы карты, будут отображены в списке **Person(s) with No Card Issued** («Люди, которым не выданы карты»).



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»).
4. Введите количество карт, выданных для каждого человека, в поле **Card Quantity** («Количество карт»).
   Например, если **Card Quantity** («Количество карт») равно 3, вы можете считать или ввести вручную три номера карты 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.

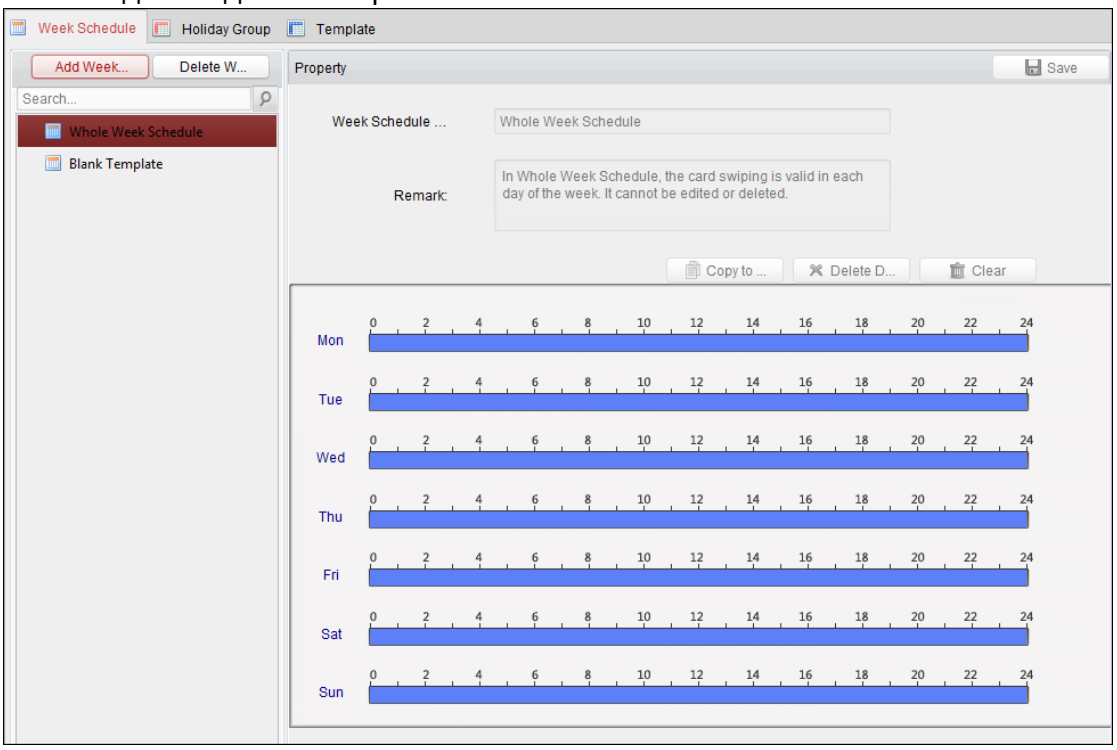
8. После выдачи карты человеку информация о нем и о карте будет отображаться в списке **Person(s) with Card Issued** («Люди, которым выданы карты»).
9. Нажмите **OK** для сохранения настроек.

7.6 Расписание и шаблоны

Цель:

Вы можете настроить шаблон, включая недельное расписание и расписание выходных. После настройки шаблонов вы можете применять их к разрешениям контроля доступа, чтобы разрешение на доступ вступало в силу во время действия шаблона.

Нажмите  для входа в меню расписаний и шаблонов.



Вы можете управлять расписанием разрешений контроля доступа, включая **Week Schedule** («Недельное расписание»), **Week Schedule** («Недельное расписание») и **Template** («Шаблон»). Для получения подробной информации смотрите *Раздел 7.7 Конфигурация разрешений.*

7.6.1 Недельное расписание

Нажмите вкладку **Week Schedule** («Недельное расписание») для перехода в меню управления недельным расписанием.

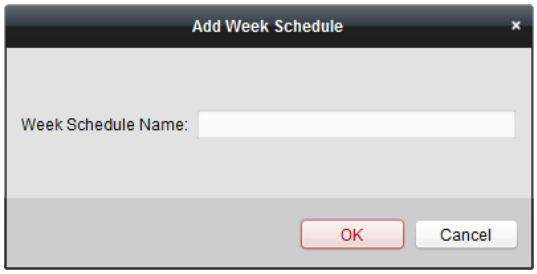
Клиент имеет два вида недельного плана по умолчанию: **Whole Week Schedule** («Расписание для всей недели») и **Blank Schedule** («Пустое расписание»), которые не могут быть удалены или изменены.

- **Whole Week Schedule** («Расписание для всей недели»): Проводка карты действительна в любой день недели.
- **Blank Schedule** («Пустое расписание»): Проводка карты недействительна в любой день недели.

Вы можете выполнить следующие шаги для определения пользовательских расписаний по вашему усмотрению.

Шаги:

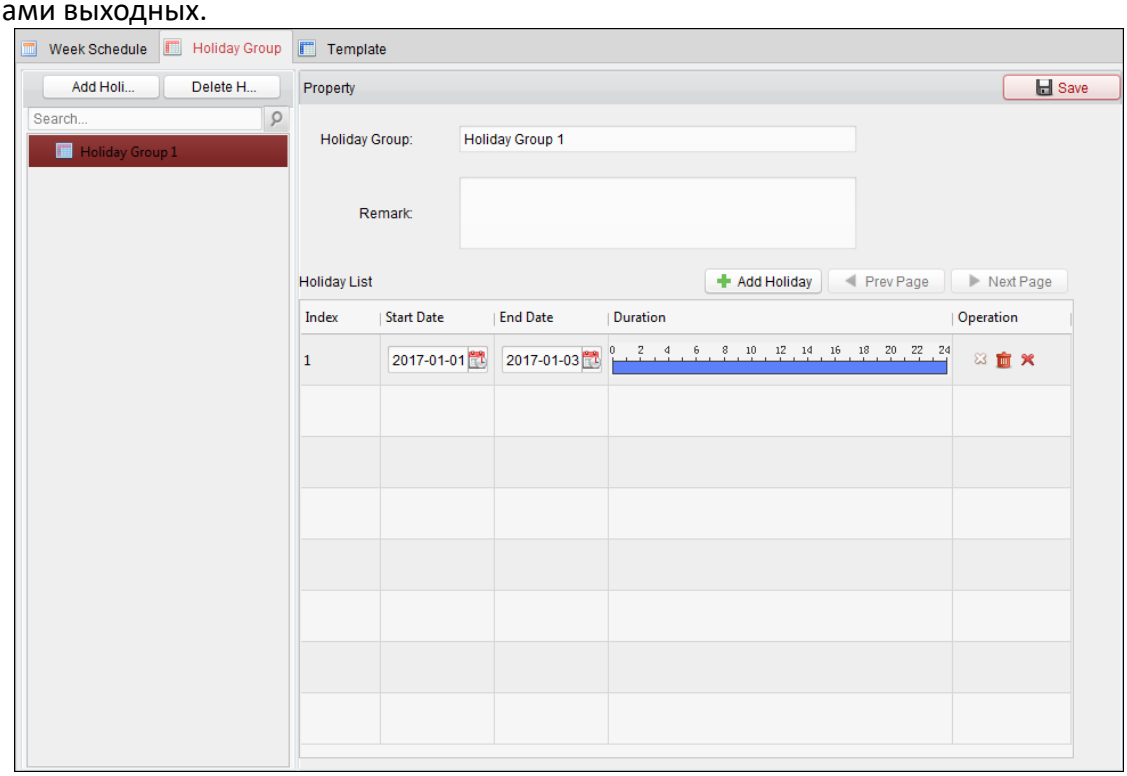
1. Нажмите кнопку **Add Week Schedule** («Добавить недельное расписание») для появления всплывающего окна добавления.



2. Введите **Name of week schedule** («Название недельного расписания») и нажмите **OK** для его добавления.
3. Выберите добавленное недельное расписание в списке расписаний, и вы сможете просмотреть его свойства справа.
   Вы можете изменить имя недельного расписания и внести информацию в качестве примечания.
4. Нажмите и перетащите указатель мыши на день, чтобы нарисовать синюю полосу в расписании, что означает, что в этот период времени активируется сконфигурированное разрешение.
   Примечание: Для каждого дня в расписании можно установить до 8 периодов времени.
5. 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.
6. Опционально, вы можете выбрать временную шкалу расписания,
   и затем нажать **Delete Duration** («Удалить длительность»), чтобы удалить выбранную шкалу времени,
   или нажать **Clear** («Очистить»), чтобы удалить все временные периоды,
   или нажать **Copy to Week** («Копировать на неделю») для копирования настроек на всю неделю.
7. Нажмите **Save** («Сохранить») для сохранения настроек.

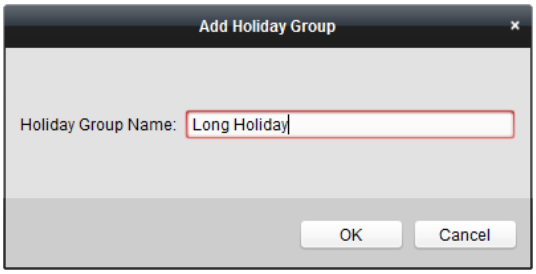
7.6.2 Группа выходных

Нажмите вкладку **Holiday Group** («Группа выходных») для перехода в меню управления группами выходных.



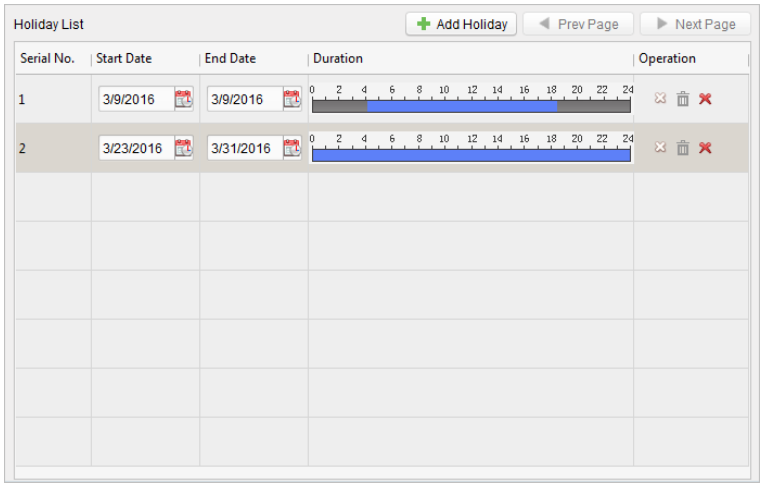
Шаги:

1. Нажмите кнопку **Add Holiday Group** («Добавить группу выходных») слева для появления всплывающего окна добавления группы выходных.



2. Введите **Name of holiday group** («Название группы выходных») в текстовое поле и нажмите кнопку **OK** для добавления группы выходных.
3. Выберите добавленную группу выходных, и вы сможете изменить ее имя и внести информацию в примечания.
4. Нажмите иконку **Add Holiday** («Добавить выходной») для добавления выходного в список выходных и конфигурации его длительности.

   Примечание: В одну группу выходных можно добавить до 16 выходных.



1) Нажмите и перетащите указатель мыши на день, чтобы нарисовать синюю полосу в расписании, что означает, что в этот период времени активируется сконфигурированное разрешение.
   Примечание: Для каждого дня в расписании можно установить до 8 периодов времени.
2) 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.
3) Когда курсор превращается в , вы можете удлинить или сократить выбранную временную шкалу.
4) Опционально, вы можете выбрать временную шкалу расписания,
   и затем нажать , чтобы удалить выбранную шкалу времени,
   или нажать , чтобы удалить все временные периоды выходного,
   или нажать , чтобы удалить выходной.

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

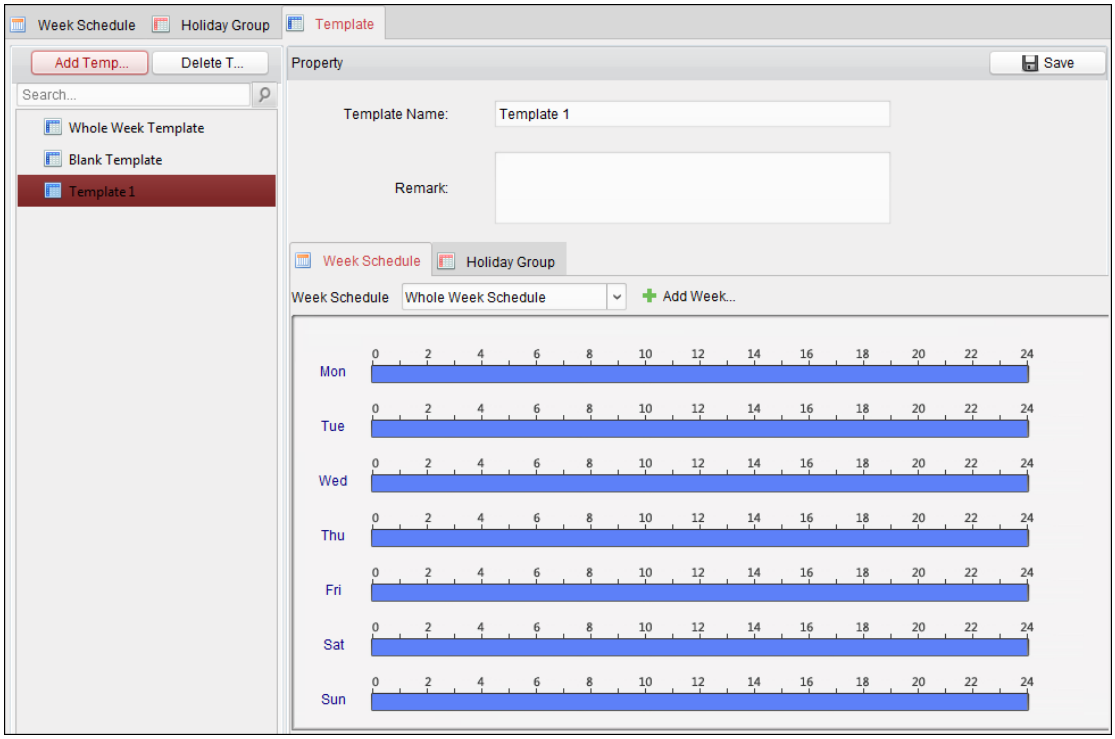
Примечание: Выходные не могут пересекаться друг с другом.

7.6.3 Шаблон

После настройки недельного расписания и группы выходных, вы можете сконфигурировать шаблон, который содержит недельное расписание и расписание группы выходных.

Примечание: Приоритет расписания групп выходных выше, чем приоритет недельного плана.

Нажмите вкладку **Template** («Шаблон») для перехода в меню управления шаблонами.



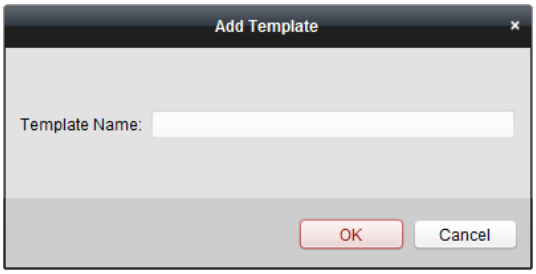
Есть два предопределенных шаблона по умолчанию: **Whole Week Template** («Шаблон для всей недели») и **Blank Template** («Пустой шаблон»), которые не могут быть удалены или изменены.

- **Whole Week Template** («Шаблон для всей недели»): Проводка карты действительна в каждый день недели, и в шаблоне нет расписания групп праздников.
- **Blank Template** («Пустой шаблон»): Проводка карты не действительна в каждый день недели, и в шаблоне нет расписания групп праздников.

Вы можете определить пользовательские шаблоны по вашему усмотрению.

Шаги:

1. Нажмите **Add Template** («Добавить шаблон») для появления всплывающего окна добавления шаблона.

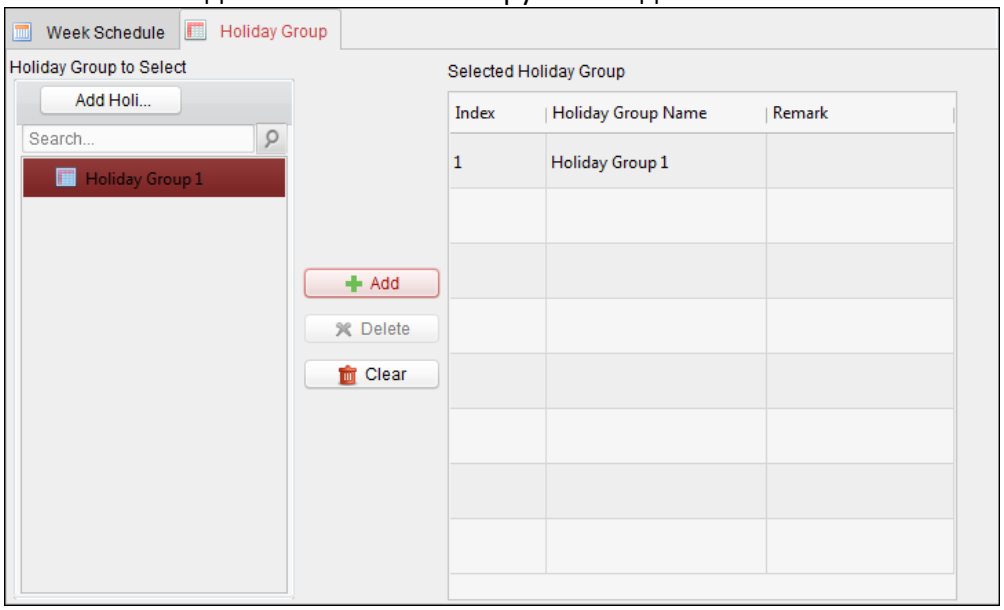


2. Введите **Template name** («Имя шаблона») в текстовое поле и нажмите кнопку **OK** для добавления шаблона.
3. Выберите добавленный шаблон, и вы сможете изменить его свойства в правой части окна. Вы можете изменить имя шаблона и внести информацию в примечания.
4. Выберите недельный план, который вы хотите применить к расписанию.
   Нажмите вкладку **Week Schedule** («Недельное расписание») и выберите расписание из выпадающего списка.
   Вы также можете нажать **Add Week Schedule** («Добавить недельное расписание») для

добавления нового недельного расписания. Для получения информации смотрите *Раздел 7.6.1 Недельное расписание.*

5. Выберите группы выходных, которые вы хотите применить к расписанию.

   Примечание: Можно добавить не более 4 групп выходных.



   Нажмите для выбора группы выходных в списке слева и нажмите **Add** («Добавить») для добавления ее в шаблон. Вы также можете нажать **Add Holiday Group** («Добавить группу выходных») для добавления новой группы. Для получения информации смотрите *Раздел 7.6.2 Группа выходных.*

   Нажмите для выбора группы выходных в списке справа и нажмите **Delete** («Удалить») для ее удаления.

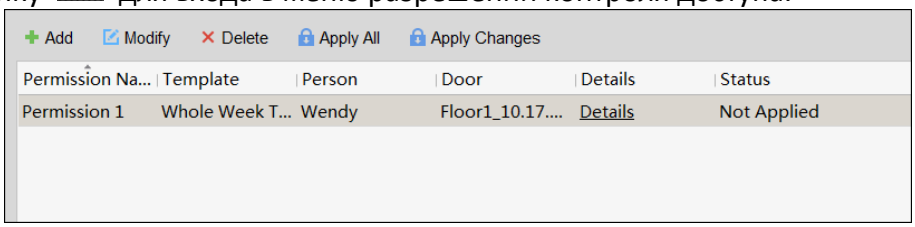
   Нажмите **Clear** («Очистить») для удаления всех добавленных групп выходных.

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

7.7 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.



7.7.1 Добавление разрешений

Цель:

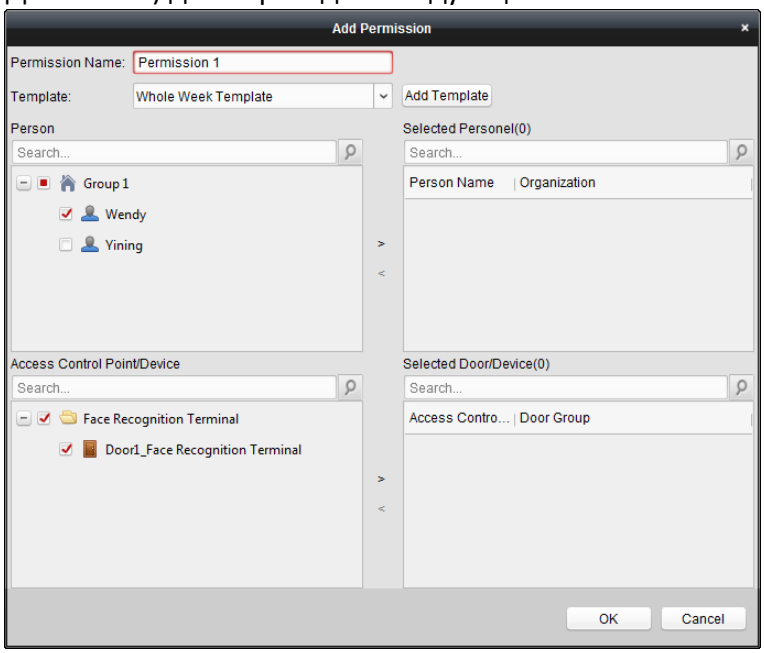
Вы можете назначать разрешения для людей на вход/выход через контрольные точки (двери) в этом разделе.

Примечания:

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

Шаги:

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



2. В поле **Permission Name** («Имя разрешения») введите имя для разрешения по вашему желанию.
3. 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. Для получения информации смотрите *Раздел 7.6 Расписание и Шаблоны*.

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.

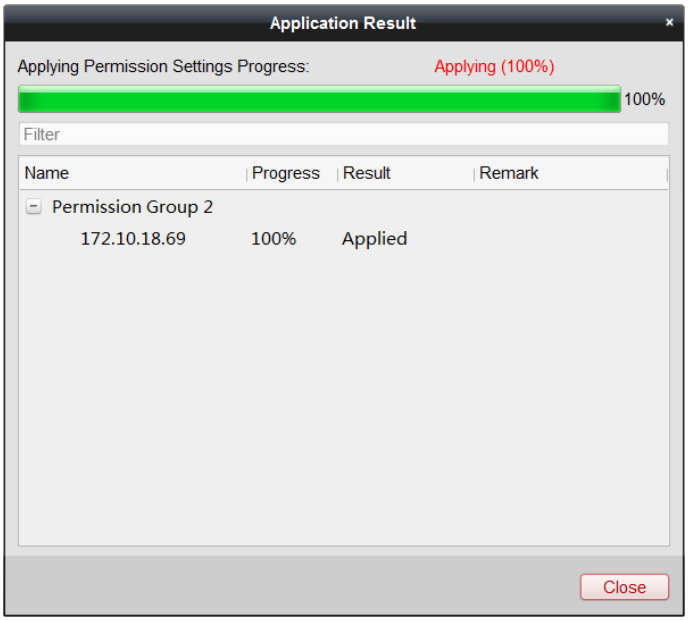
7.7.2 Применение разрешений

Цель:

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

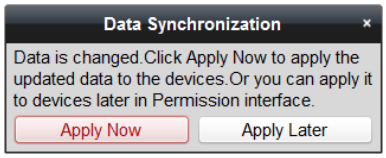
Шаги:

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.).

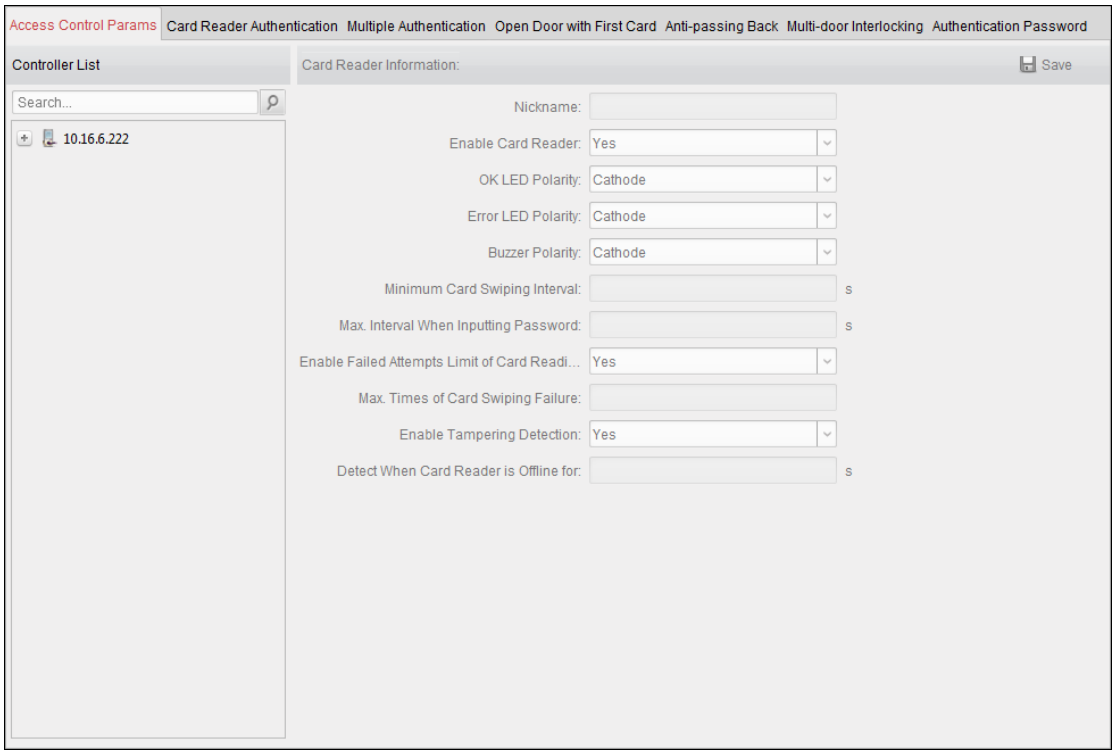
7.8 Расширенные функции

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.



7.8.1 Параметры контроля доступа

Цель:

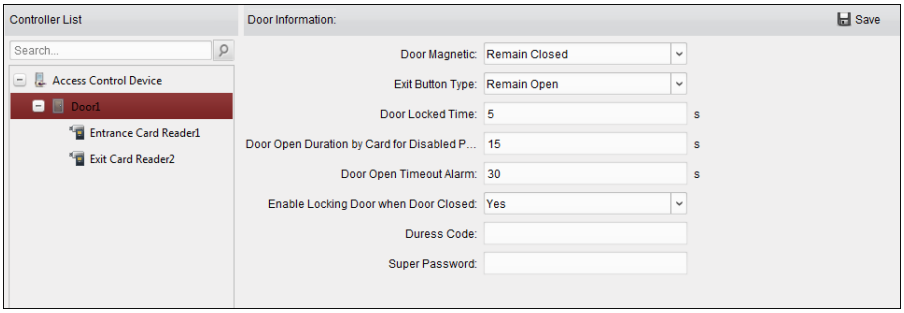
После добавления устройства контроля доступа вы можете настроить параметры его точки контроля доступа (двери) и параметры его считывателя карт.

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 Duration by Card for Disabled Person** («Длительность открытия двери для карты инвалида»): Магнитная дверь может быть настроена с необходимой задержкой, после того как инвалид проведет своей картой.
- **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.

  Примечания:

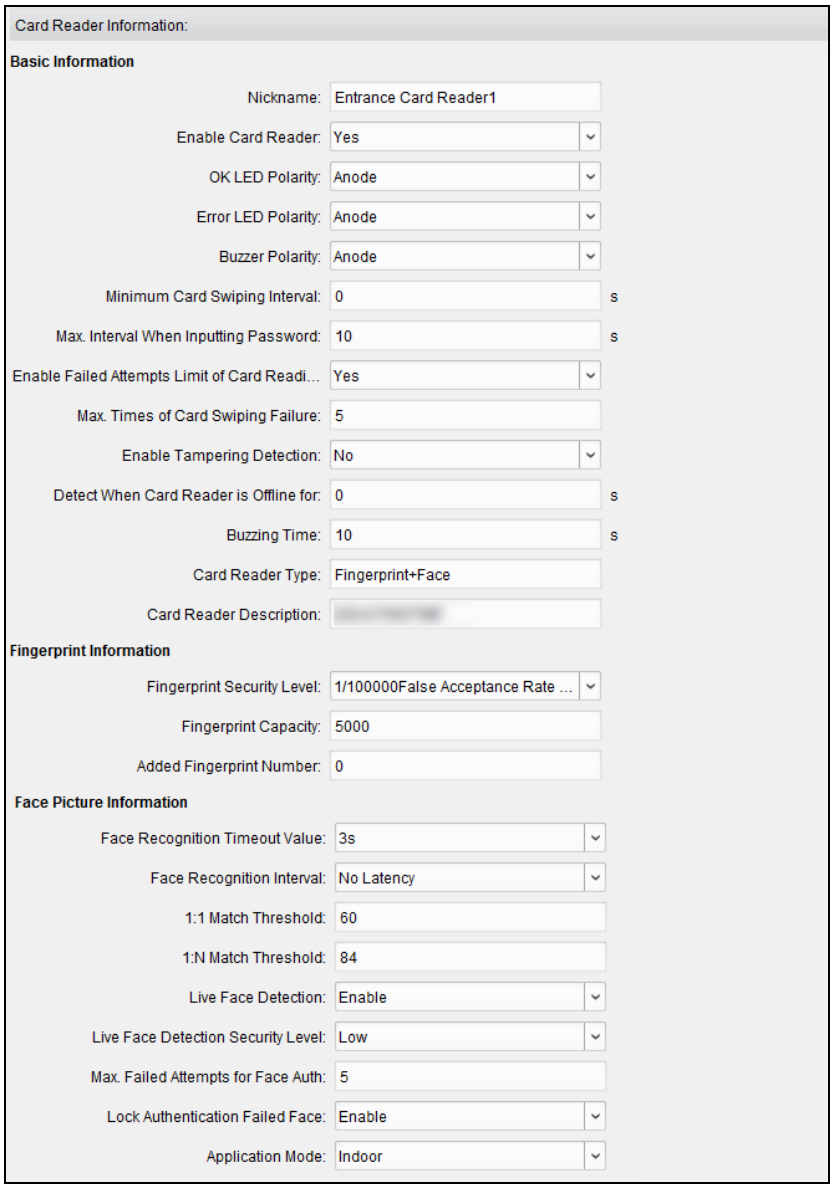
  - Принудительный код и супер пароль должны отличаться.
  - Принудительный код и супер пароль должны содержать 4 -8 цифр.

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

Параметры считывателя карт

Шаги:

1. В области **Controller list** («Список контроллеров») слева нажмите , чтобы развернуть дверь, выберите считыватель карт, и вы сможете изменить информацию выбранной двери справа.



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 неуспешных 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 Security Level** («Уровень безопасности отпечатков пальцев»): Выберите уровень распознавания отпечатков пальцев из выпадающего списка.
- **Fingerprint Capacity** («Количество отпечатков пальцев»): Просмотр общего количества отпечатков пальцев в устройстве.
- **Added Fingerprint Number** («Число добавленных отпечатков пальцев»): Просмотр добавленного количества отпечатков пальцев.
- **Face Recognition Timeout Value** («Значение тайм-аута распознавания лица»): Если время распознавания превышает настроенное время, устройство выдаст напоминание.
- **Face Recognition Interval** («Интервал распознавания лиц»): Интервал времени между двумя непрерывными распознаваниями лица при аутентификации. По умолчанию установлено значение «0».
- **1:1 Match Threshold:** («Порог соответствия 1:1»): Установите порог соответствия при аутентификации в режиме **1:1 Matching** («Соответствие 1:1»). Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 60.
- **1:N Match Threshold** («Порог соответствия 1:N»): Установите порог соответствия при аутентификации в режиме **1:N Matching** («Соответствие 1:N»). Чем больше значение, тем меньше вероятность ложного допуска и тем больше вероятность ложного недопуска. Значение по умолчанию - 60.

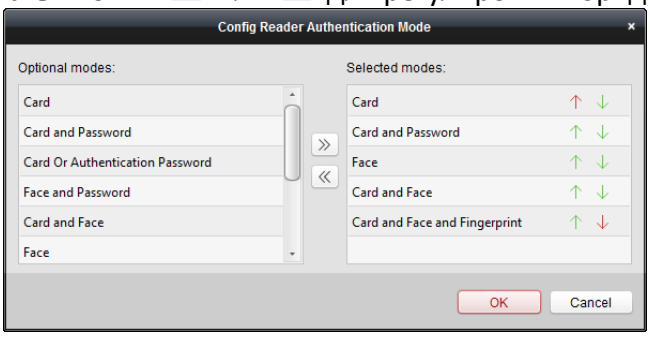
- **Live Face Detection** («Детекция реальности лица»): Включение или отключение функции детекции реальности лица. Если функция включена, устройство может понять, является ли лицо живым человеком или нет.
  Примечание: Биометрические продукты распознавания не на 100% применимы к анти-спуфинг средам. Если вам требуется более высокий уровень безопасности, используйте несколько режимов аутентификации.
- **Live Face Detection Security Level** («Уровень безопасности детекции реальности лица»): После включения функции **Live Face Detection** («Детекция реальности лица») вы можете установить соответствующий уровень безопасности при выполнении проверки подлинности лица.
- **Lock Authentication Failed Face** («Блокировка лица, провалившего аутентификацию»): После включения функции **Live Face Detection** («Детекция реальности лица»), система заблокирует лицо пользователя на 5 минут, если детекция реальности лица будет провалена большее число раз, чем заданное допустимое число попыток. Тот же пользователь не сможет аутентифицироваться при помощи поддельного лица в течение 5 минут. В течение 5 минут пользователь может дважды проходить аутентификацию с помощью реального лица, чтобы разблокировать устройство.
- **Max. Failed Attempts for Face Auth.** («Макс. число неудачных попыток для аутентификации лица»): Установите максимальное количество неудачных попыток детекции реальности лица. Система заблокирует лицо пользователя на 5 минут, если детекция реальности лица будет провалена большее число раз, чем заданное допустимое число попыток. Тот же пользователь не сможет аутентифицироваться при помощи поддельного лица в течение 5 минут. В течение 5 минут пользователь может дважды проходить аутентификацию с помощью реального лица, чтобы разблокировать устройство.
- **Application Mode** («Режим применения»): Вы можете выбрать либо **Others** («Другие»), либо **Indoor** («Внутри помещения») в зависимости от реальной обстановки.

7.8.2 Аутентификация считывателя карт

Цель:
Вы можете установить правила 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.

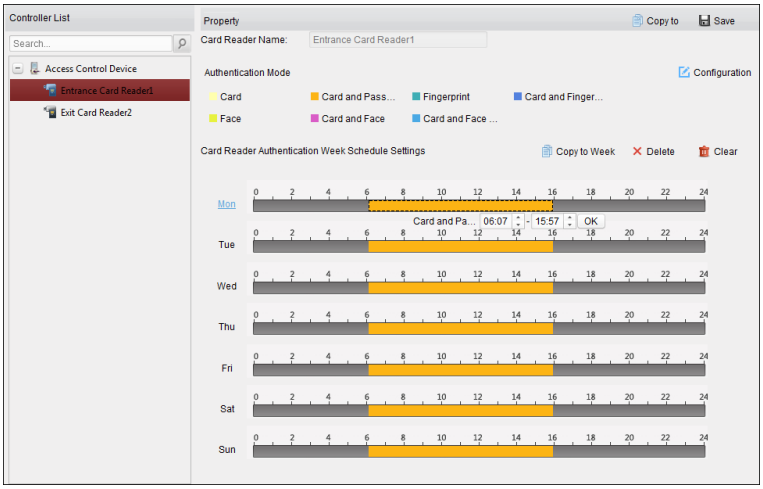
- Пароль относится к паролю карты, установленному при выдаче карты человеку, подробности смотрите в *Разделе 7.5 Управление людьми.*

1) Выбирайте режимы в поле слева и нажимайте » для добавления в список выбранных режимов.
   Вы можете нажимать иконки ↑ или ↓ для регулировки порядка отображения.

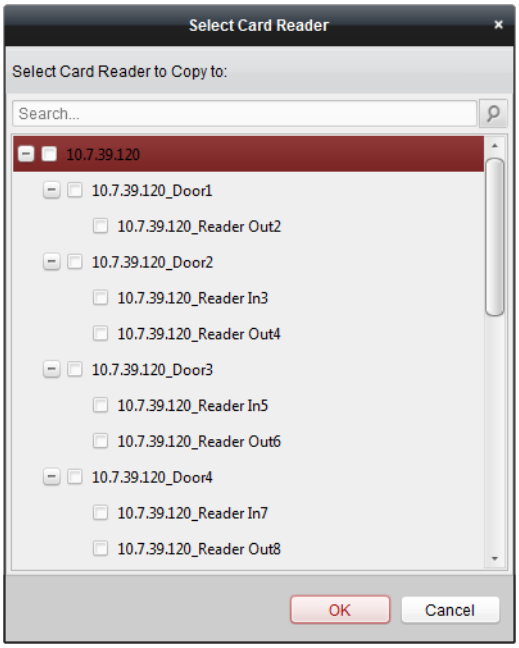


2) Нажмите **OK** для подтверждения выбора.

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.

7.8.3 Многократная аутентификация

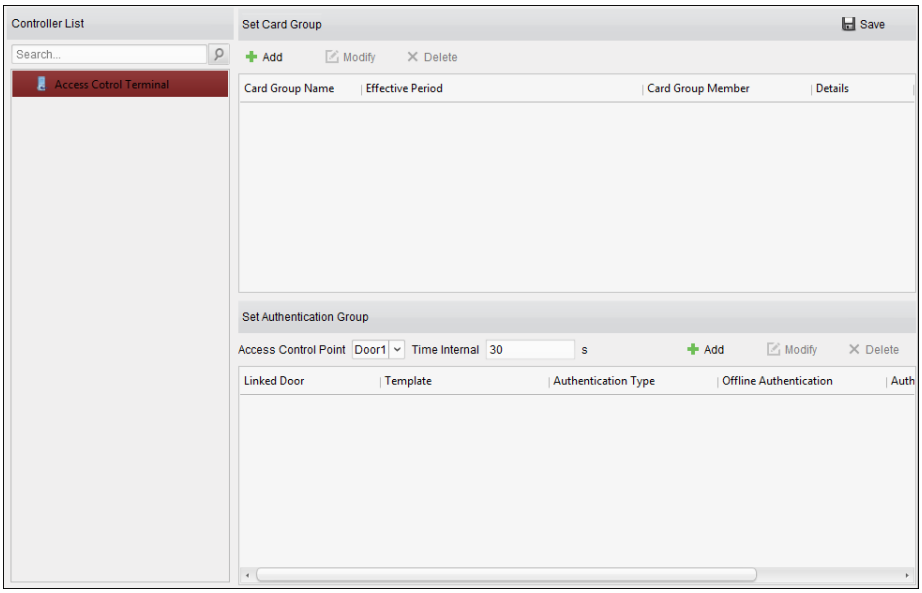
Цель:

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 7.7 Конфигурация разрешений.*

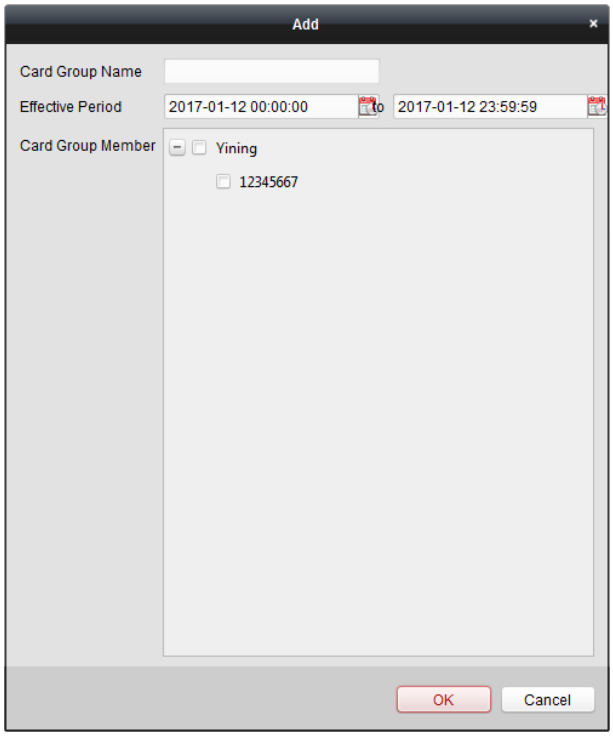
Шаги:

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

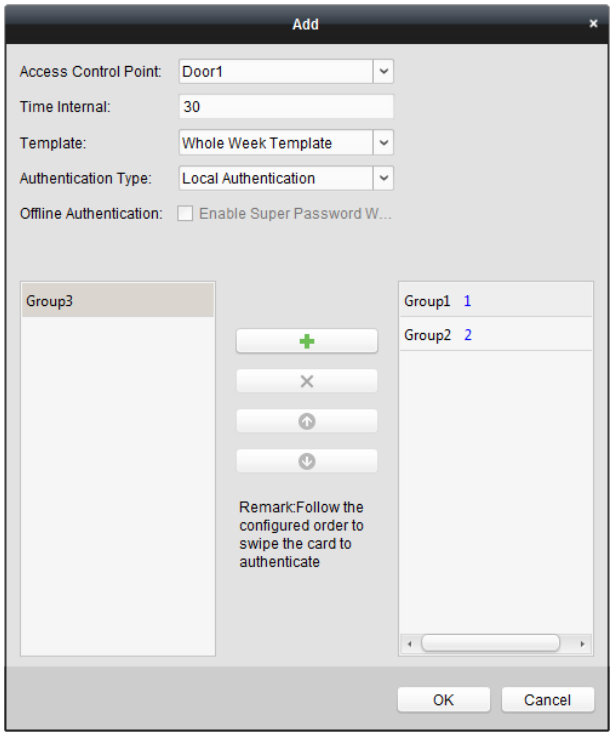


2. Выберите устройство контроля доступа из списка слева.

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. Для получения подробной информации о настройке шаблона смотрите *Раздел 7.6 Расписание и Шаблоны*.
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 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.

7.8.4 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») и **Disable Remain Open with First Card** («Отключить открытое состояние запущенное первой картой»).

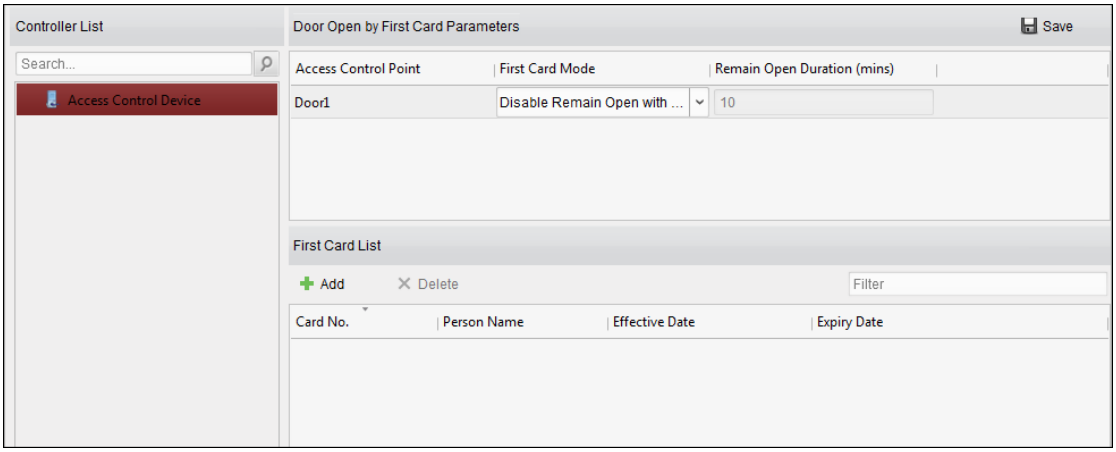
- **Remain Open with First Card** («Оставить открытой после проводки первой карты»): Дверь остается открытой в течение заданной продолжительности времени после проводки первой карты до тех пор, пока не закончится продолжительность открытого состояния.
- **Disable Remain Open with First Card** («Отключить открытое состояние запущенное первой картой»): Отключение функции.

  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:

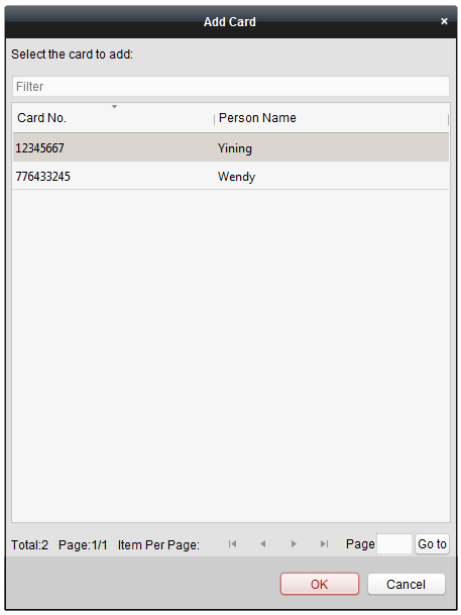
1. Нажмите вкладку **Open Door with First Card** («Открыть дверь при помощи первой карты») для перехода в соответствующее меню.



2. Выберите устройство контроля доступа из списка слева.
3. Выберите **First card mode** («Режим первой карты») из выпадающего списка для контрольной точки доступа.

   (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.
4. 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 7.7 Конфигурация разрешений.*
   2) Нажмите кнопку **OK** для подтверждения добавления карты.

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

7.8.5 Запрет обратного прохода

Цель:

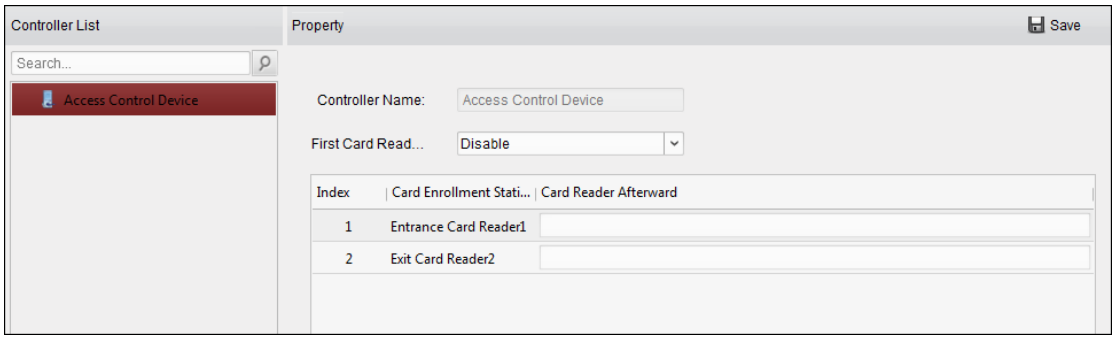
Вы можете установить только проход в одном направлении через контрольную точку в соответствии с заданным путем, и только один человек может пройти контрольную точку доступа после проводки карты.

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.

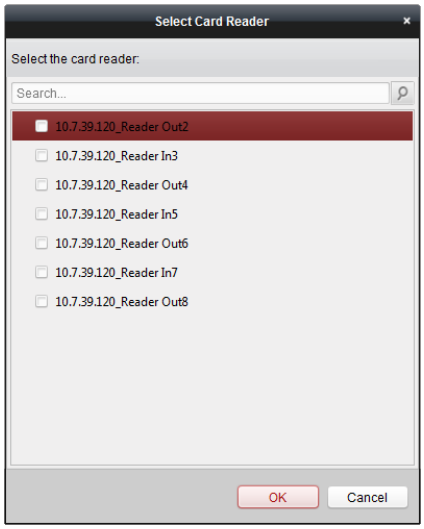
Шаги:

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 устройства считывания карт»), чтобы изменить его считыватели.
6. Нажмите **Save** («Сохранить») для сохранения и вступления в силу настроек.

7.9 Поиск событий контроля доступа

Цель:

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

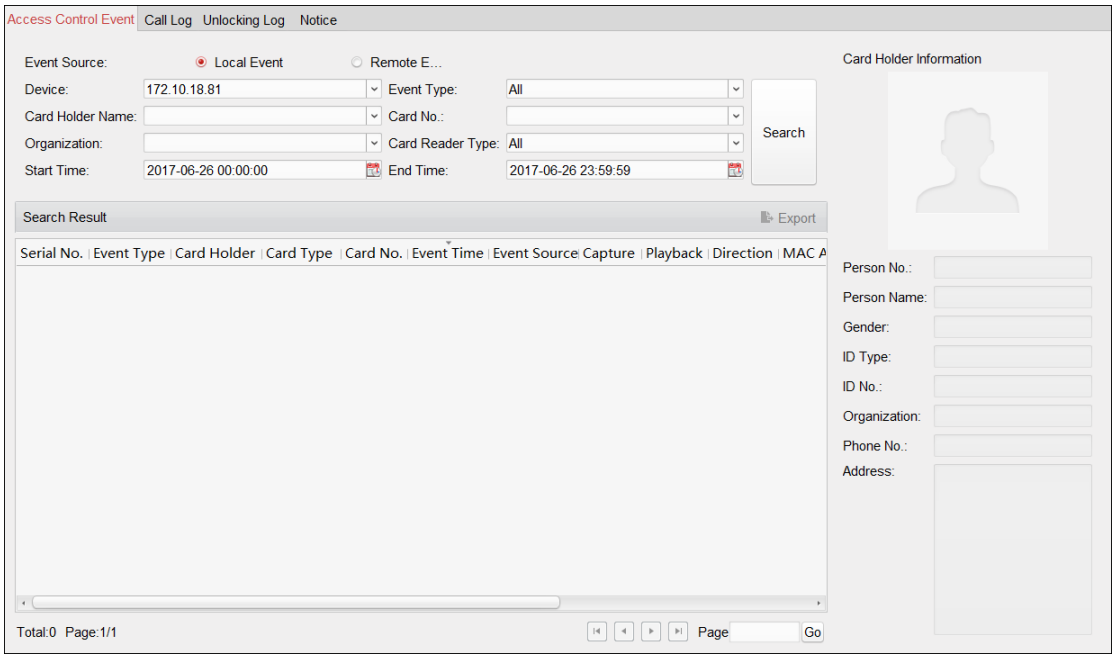
Перед началом:

Вы должны настроить удаленное хранилище для просмотра захваченного изображения лица перед поиском события контроля доступа. Для получения подробной информации о настройке удаленного хранилища смотрите *Раздел 5.1 Удаленное хранилище* в *Руководстве пользователя iVMS-4200*.

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.



7.9.1 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 видеофайлов во время тревоги с камеры.

Примечание: Для настройки срабатывающей камеры обратитесь к *Разделу 7.10.1 Привязка событий контроля доступа.*

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

7.9.2 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.

7.10 Конфигурация событий контроля доступа

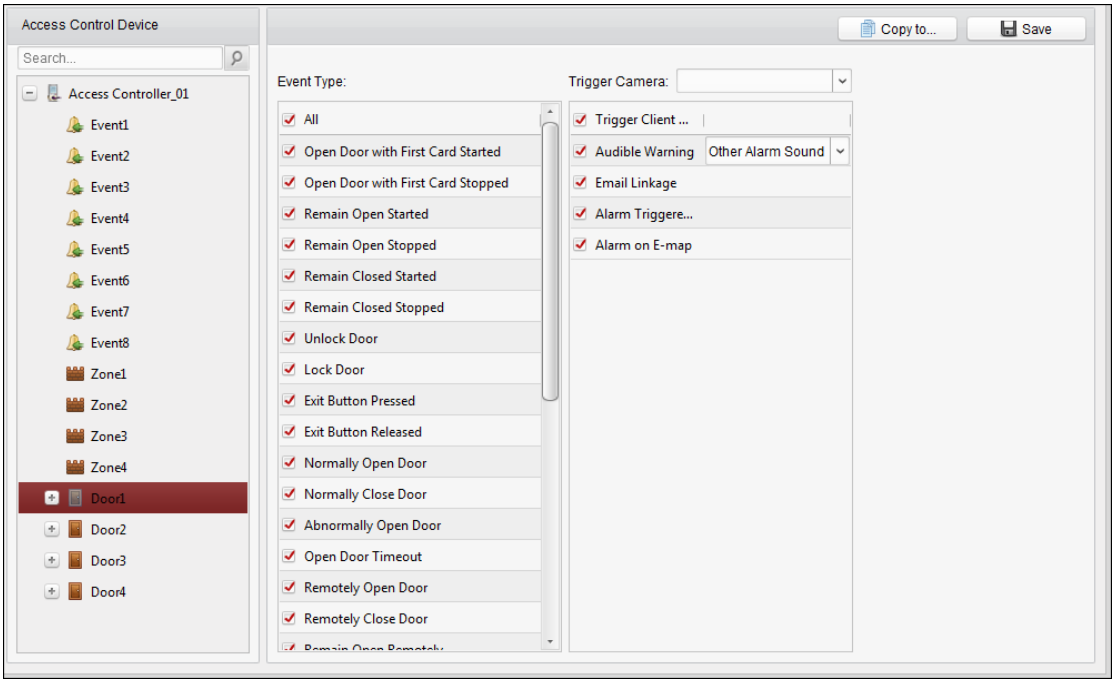
Цель:
Для добавленного устройства контроля доступа вы можете настроить его привязку к управлению доступом, включая привязку событий контроля доступа, привязку тревожного входа контроля доступа, привязку карты/событий и межустройственную привязку.

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

7.10.1 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.



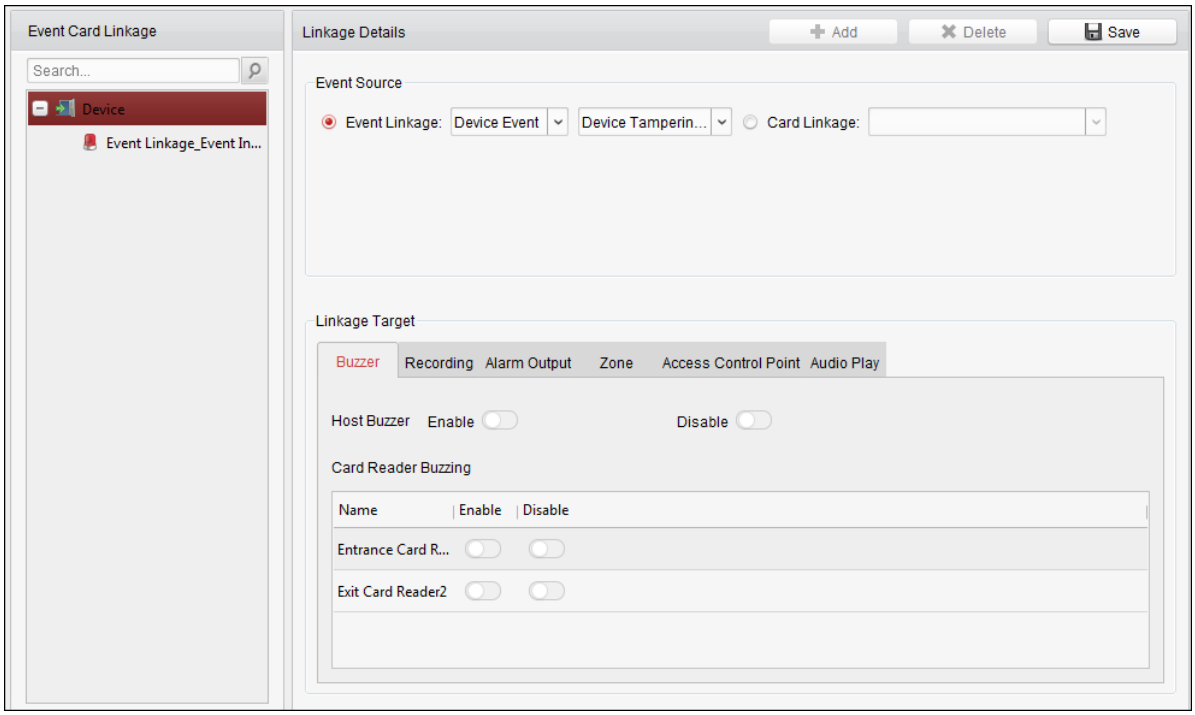
Связанные действия для событий контроля доступа

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.
Тревога на E-map	Отображение тревожной информации на электронной карте (E-map). ***Примечание:*** Данный вид привязки доступен только для точек контроля доступа и для тревожных входов.
Запущенное по тревоге всплывающее изображение	Изображение с тревожной информацией будет всплывать на экране при запуске тревоги.

7.10.2 Привязка карты/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, тревожного выхода и точки контроля доступа.

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.
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.

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.
4. Нажимайте на различные вкладки, чтобы установить разные параметры. Переключайте свойства с на  для включения соответствующей функции.
   Вы можете установить параметры зуммера, записи, тревожного выхода и точки контроля доступа.

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	**Alarm Output**	Тревожный выход будет запущен для

(«Тревожный выход»)	(«Тревожный выход»)	уведомления.
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.

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

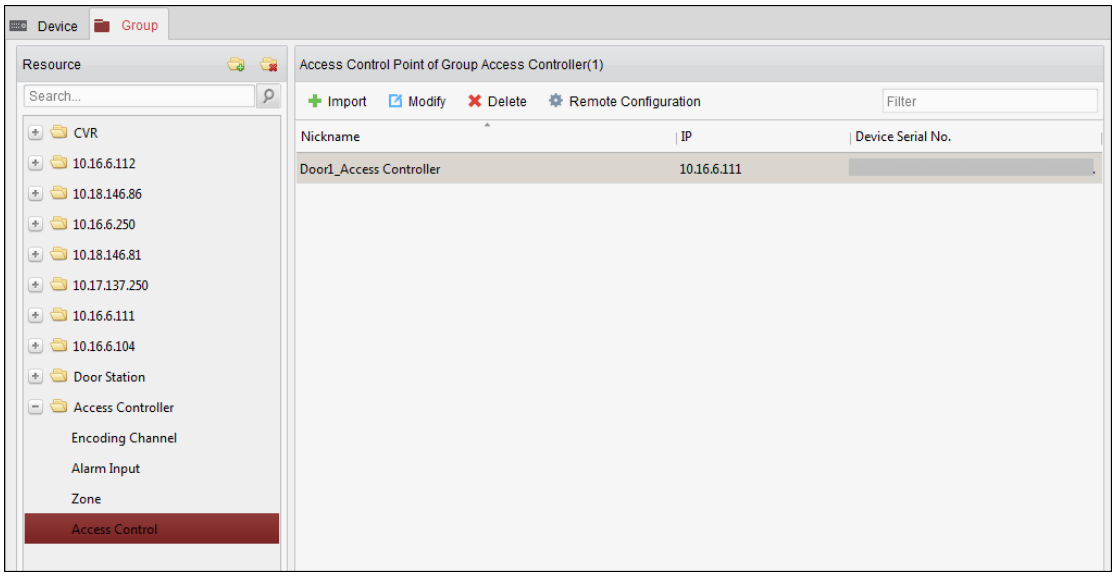
7.11 Управление состоянием двери

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.

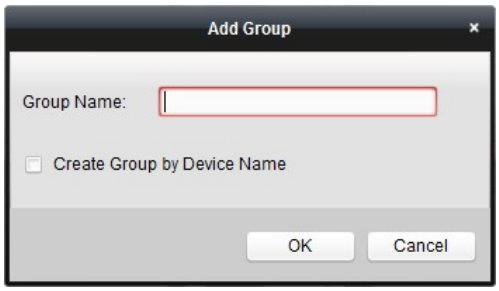
7.11.3 Управление группой контроля доступа

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:

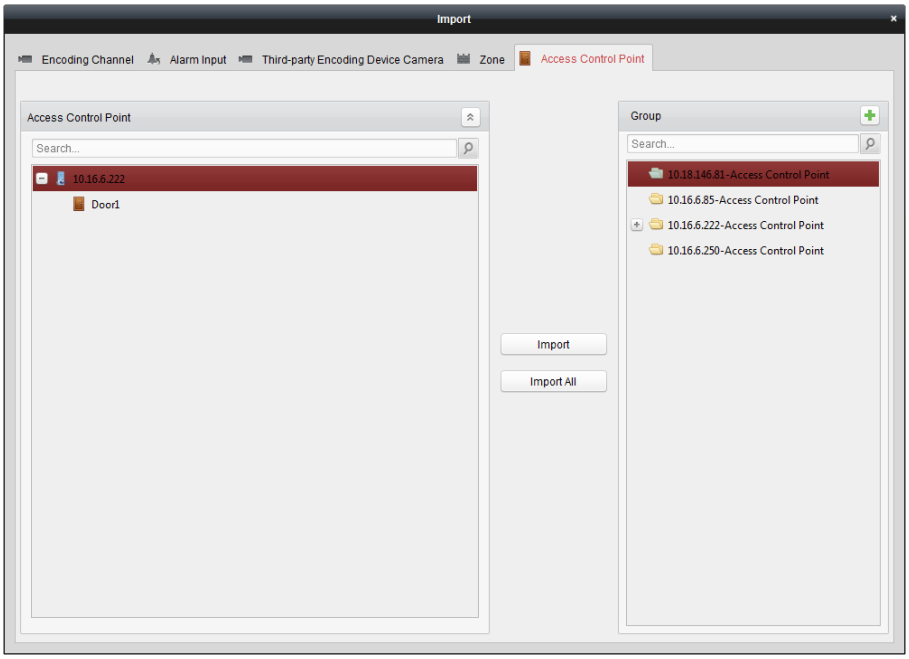
1. Нажмите  на панели управления для открытия страницы управления устройствами.
2. Нажмите вкладку **Group** («Группа») для перехода в меню управления группами.



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.



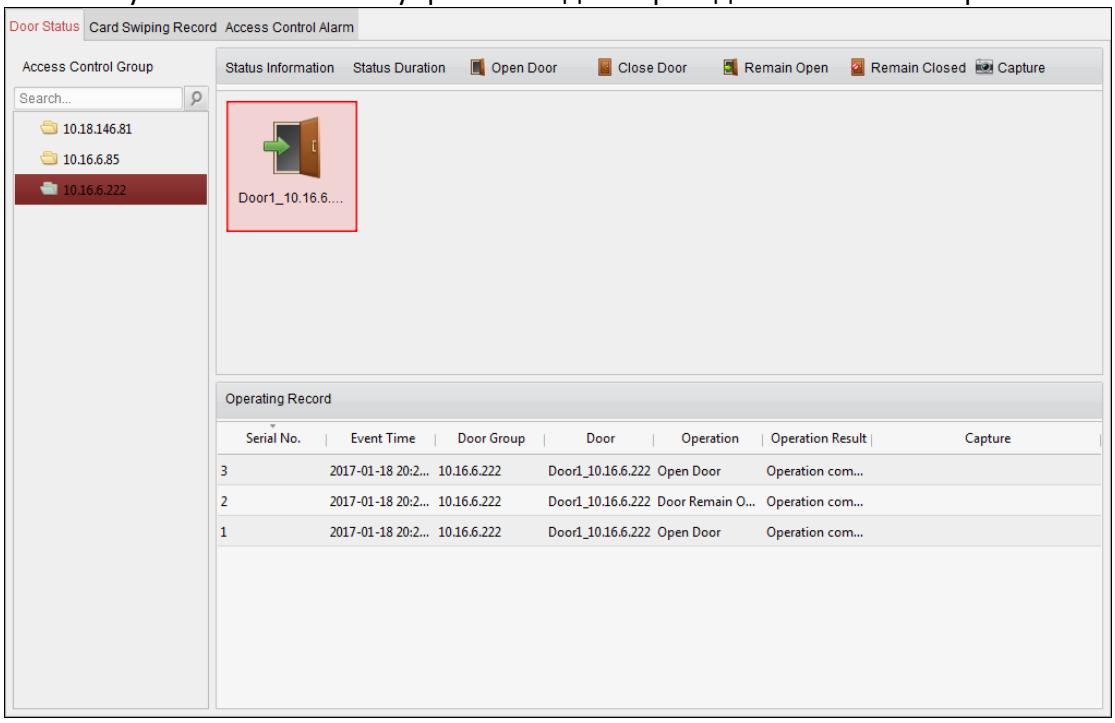
5. После импорта точек контроля доступа в группу вы можете нажать или дважды щелкнуть по имени группы/точки контроля доступа для ее редактирования.

7.11.4 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.

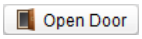
Нажмите иконку  на панели управления для перехода в меню мониторинга состояния.

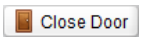


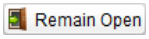
Шаги:

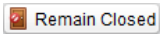
1. Выберите группу управления доступом слева. Для управления группой контроля доступа смотрите *Раздел 7.11.1 Управление группой контроля доступа.*
2. Точки контроля доступа выбранной группы контроля доступа будут отображаться справа.

   Нажмите на иконку  на панели статуса для выбора двери.
3. Нажмите на одну из кнопок, перечисленных на панели **Status Information** («Сведения о состоянии»), чтобы выбрать состояние для двери.

    («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:

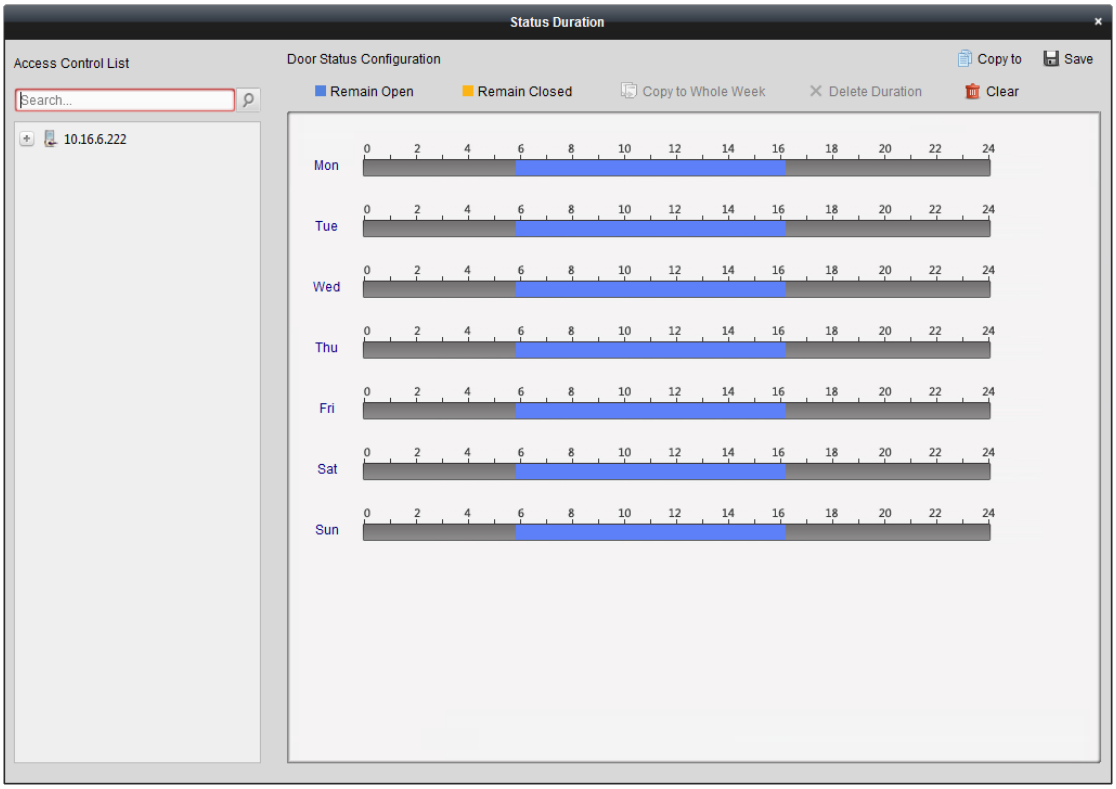
- Если выбрано состояние **Remain Open** («Оставить открытой»)/**Remain Closed** («Оставить закрытой»), дверь будет открыта/закрыта до тех пор, пока не будет выполнена новая команда управления.
- Кнопка **Capture** («Захват») доступна, когда устройство поддерживает функцию захвата. Захват не может быть 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.

7.11.5 Конфигурация длительности состояния

Цель:

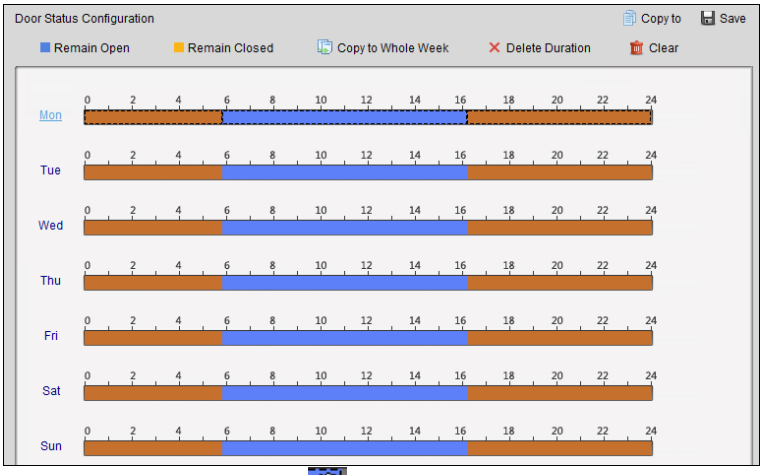
Вы можете планировать еженедельные периоды времени для точки контроля доступа (двери), когда она будет оставаться открытой или оставаться закрытой.

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



Шаги:

1. Нажмите на дверь, чтобы выбрать ее 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.



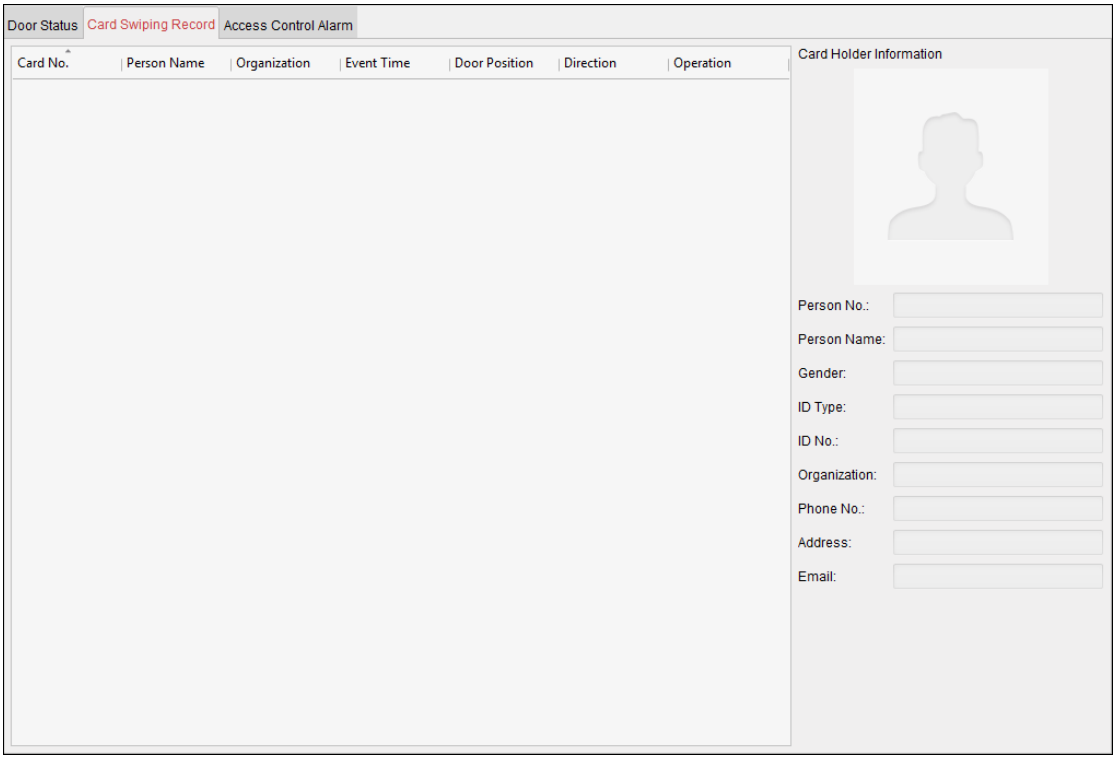
   3) Когда курсор превращается в , вы можете переместить выбранную шкалу

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.

7.11.6 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.

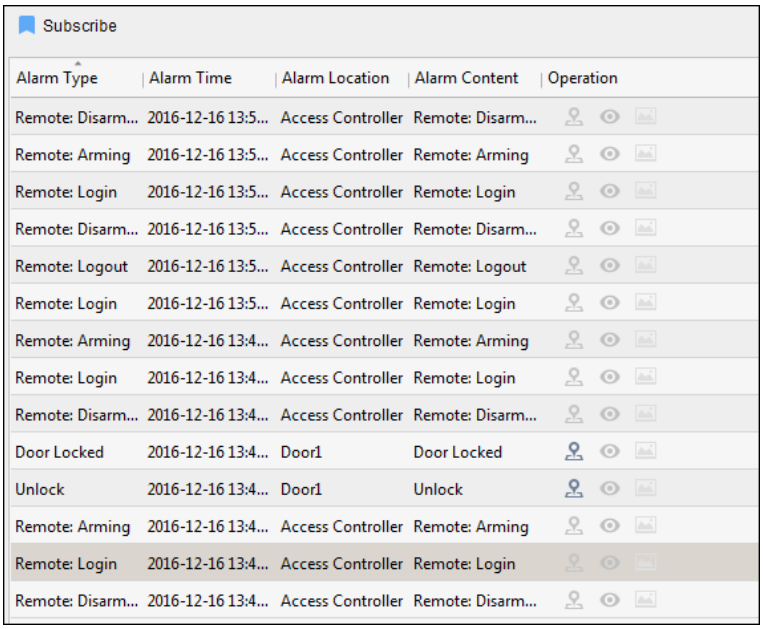
Вы можете нажать на событие для просмотра подробной информации о владельце карты, включая № человека, имя человека, организацию, телефон, контактный адрес и др.

7.11.7 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.

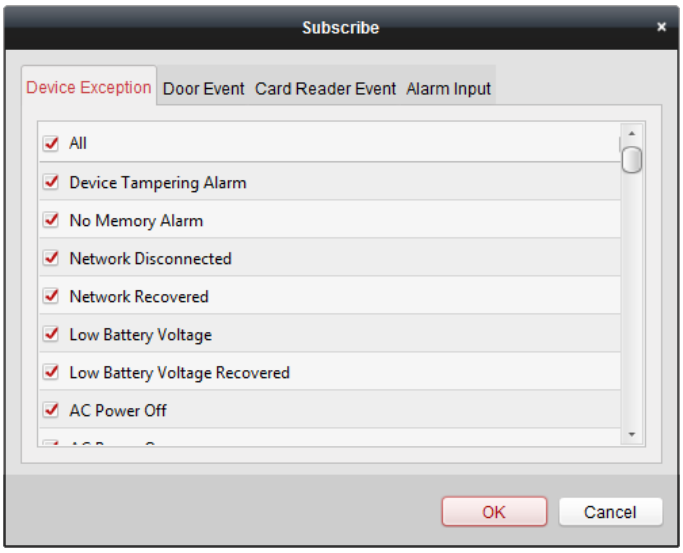
Нажмите вкладку **Access Control Alarm** («Тревога контроля доступа») для перехода в следующее меню.



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 7.10.1 Привязка событий контроля доступа.*
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 **OK** для сохранения настроек.

7.12 Просмотр в реальном времени

Вы можете выполнять просмотр видео в реальном времени с добавленных устройств. Также поддерживаются некоторые основные операции, в том числе захват изображения, запись вручную и т. д.

Перед началом:

Группа камер должна быть определена для просмотра в реальном времени.

Вы можете установить тип чередования, если необходимо, в меню **Group Management** («Управление группами»). Для получения подробной информации смотрите *Руководство пользователя Клиентского ПО iVMS-4200*.

7.12.1Запуск и остановка просмотра в реальном времени

Запуск просмотра в реальном времени

Шаги:

1. Нажмите иконку  на панели управления.
   Или нажмите **View -> Main View** («Вид -> Главный вид») для перехода на соответствующую страницу.
2. Перетащите камеру в окно отображения.
   Или дважды нажмите на имя камеры после выбора окна отображения, чтобы начать просмотр в реальном времени.
   Примечание: При необходимости вы можете перетащить видео с камеры в режиме реального времени в другое окно отображения.

Остановка просмотра в реальном времени

Шаги:

1. Выберите окно отображения.
2. Нажмите на иконку  , которая появляется в верхнем правом углу, когда указатель мыши находится на окне отображения,
   Или нажмите **Stop Live View** («Остановить отображение в реальном времени») в меню, всплывающем при нажатии правой кнопки мышки, для остановки просмотра в реальном времени в окне отображения.
   Вы также можете нажать кнопку  на панели инструментов просмотра в реальном времени, чтобы остановить просмотр в реальном времени во всех окнах.

7.12.2 Запись и захват вручную

Запись вручную в режиме просмотра в реальном времени

Цель:

Функция записи вручную позволяет вам записывать видео в реальном времени на странице **Main View** («Главный вид») вручную, а видеофайлы будут сохраняться на локальном ПК.

Шаги:

1. Переместите указатель мыши на окно отображения в режиме реального времени, чтобы отобразить панель инструментов.
2. Нажмите  на панели инструментов окна отображения или в меню **Live View Management** («Управление отображением в реальном времени»), всплывающем при нажатии правой кнопки мышки, для начала записи вручную. Иконка превратится из  в  .
3. Нажмите на иконку  для остановки записи вручную.
   При успешном выполнении всех операций появится окно с указанием пути сохранения только что записанных видеофайлов.

Примечания:

- Во время записи вручную в верхнем правом углу окна отображения появится индикатор  .
- Путь сохранения видеофайлов можно настроить в меню **System Configuration** («Конфигурация системы»). Для получения подробной информации смотрите *Руководство пользователя Клиентского ПО iVMS-4200.*

Просмотр локальных видеофайлов

Шаги:

1. Нажмите **File -> Open Image File** («Файл -> Открыть файл изображения») для открытия страницы **Video Files** («Видеофайлы»).
2. Выберите камеру для поиска из списка **Camera Group** («Группа камер»).
3. Нажмите на иконку  для указания времени начала и времени окончания для поиска.
4. Нажмите **Search** («Поиск»). Будут отображены видеофайлы, записанные между временем

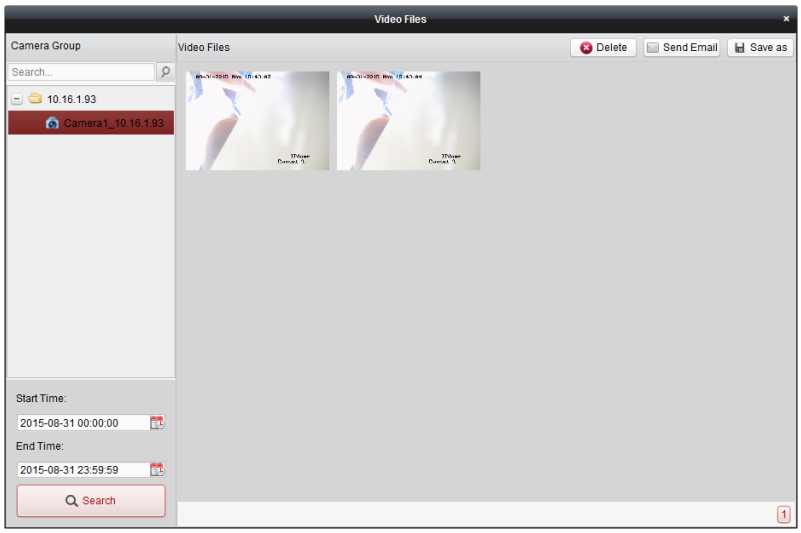
начала и временем окончания.

Выберите видеофайл и нажмите **Delete** («Удалить»). Вы можете удалить видеофайл.

Выберите видеофайл и нажмите **Send Email** («Отправить Email»). Вы можете отправить уведомление по электронной почте с вложенным выбранным видеофайлом.

Выберите видеофайл и нажмите **Save as** («Сохранить как»). Вы можете сохранить новую копию видеофайла.

Примечание: Чтобы отправить уведомление по Email, необходимо настроить параметры электронной почты.



Дважды нажмите на видеофайл для локального воспроизведения.

На локальной странице воспроизведения доступны следующие кнопки:

cif 4cif	**CIF/4CIF**	Отображение видео в разрешении CIF/4CIF.
	Полноэкранный режим	Отображение локальной страницы воспроизведения в полноэкранном режиме.
	Закрыть	Закрытие страницы воспроизведения видеофайлов.

	Пауза/Старт	Пауза/Начало воспроизведения видеофайлов.
	Стоп	Остановка воспроизведения видеофайлов.
1x	**Скорость**	Установка скорости воспроизведения.
	Покадровое воспроизведение	Воспроизведение видеофайла кадр за кадром.
	Цифровой зум	Включение функции цифрового зума. Нажмите снова для отключения функции.
	Включить/Выключить аудио	Нажмите для включения/выключения аудио при локальном воспроизведении.
	Захват	Захват изображения в процессе воспроизведения.

Захват изображений во время просмотра в реальном времени

Шаги:

1. Переместите указатель мыши на окно отображения в режиме реального времени, чтобы отобразить панель инструментов.
2. Нажмите на иконку на панели инструментов в окне отображения или в меню **Live View Management** («Управление отображением в реальном времени»).
   Небольшое окно с захваченным изображением будет отображено, чтобы уведомить, выполнена ли операция захвата или нет.

Примечание: Путь сохранения захваченных изображений можно настроить в меню **System Configuration** («Конфигурация системы»). Для получения подробной информации смотрите *Руководство пользователя Клиентского ПО iVMS-4200.*

Просмотр захваченных изображений

Изображения, захваченные в режиме реального времени, сохраняются на ПК, на котором запущено программное обеспечение. Вы можете просматривать захваченные фотографии, если это необходимо.

Шаги:

1. Нажмите **File -> Open Image File** («Файл -> Открыть файл изображения») для открытия страницы **Captured Images** («Захваченные изображения»).
2. Выберите камеру для поиска из списка **Camera Group** («Группа камер»).
3. Нажмите на иконку для указания времени начала и времени окончания для поиска.
4. Нажмите **Search** («Поиск»). Будут отображены изображения, захваченные между временем начала и временем окончания.
5. Дважды щелкните на захваченном изображении, чтобы увеличить его для лучшего обзора.
   Выберите захваченное изображение, нажмите **Print** («Печать»). Вы можете напечатать выбранное изображение.
   Выберите захваченное изображение, нажмите **Delete** («Удалить»). Вы можете удалить выбранное изображение.
   Выберите захваченное изображение, нажмите **Send Email** («Отправить Email»). Вы можете отправить уведомление по электронной почте с вложенным выбранным

изображением.

Выберите захваченное изображение, нажмите **Save as** («Сохранить как»). Вы можете сохранить новую копию выбранного изображения.

7.12.3 Другие функции в режиме просмотра в реальном времени

В режиме реального времени поддерживаются некоторые другие функции, в том числе двустороннее аудио, отображение состояния камеры, синхронизация и т.д.

Двустороннее аудио

Функция двустороннего аудио позволяет осуществлять голосовую связь с камерой. Вы можете получить с камеры не только видео в реальном времени, но и звук в реальном времени. Если устройство имеет каналов двустороннего аудио, вы можете выбрать канал для запуска двустороннего аудио.

Двустороннее аудио может использоваться только для одной камеры одновременно.

Примечание: Устройство Hik-Connect не поддерживает выбор канала во время двусторонней аудиосвязи.

Состояние камеры

Состояние камеры, такое как состояние записи, состояние сигнала, число соединений и т. д., может быть обнаружено и отображено для проверки. Информация о состоянии обновляется каждые 10 секунд.

Синхронизация

Функция синхронизации позволяет синхронизировать часы устройства с ПК, на котором запущено Клиентское программное обеспечение.

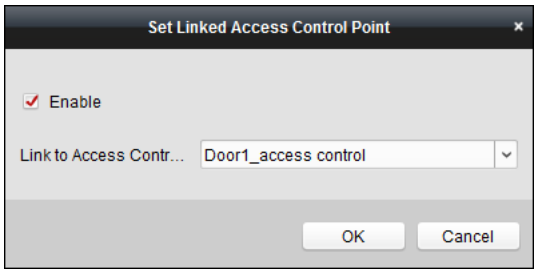
7.12.4 Управление дверями во время просмотра в реальном времени

Цель:

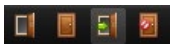
Вы можете управлять дверью во время просмотра видео в реальном времени.

Шаги:

1. Нажмите правой кнопкой мыши на окно просмотра в реальном времени, чтобы открыть контекстное меню.
2. Нажмите **Link to Access Control Point** («Привязать к точке контроля доступа») для появления диалогового окна **Set Linked Access Control Point** («Установка связанной точки контроля доступа »).
3. Поставьте галочку **Enable** («Включить») для включения функции привязки.
4. Выберите точку контроля доступа из выпадающего списка.



5. Нажмите **OK** для сохранения настроек.
   Вы также можете нажать **Cancel** («Отменить») для отмены операции.
6. Получите поток снова (дважды щелкните камеру), чтобы настройки вступили в силу.
   Четыре кнопки управления дверью появятся на панели инструментов во время просмотра в реальном времени.



   В следующей таблице приведены описания четырех кнопок.

Кнопка	Описание
	Открыть дверь.
	Закрыть дверь
	Оставить дверь открытой.
	Оставить дверь закрытой.

7. Нажмите  для открытия или закрытия двери.
   Или нажмите  для установки в качестве состояния двери значений **Remain open** («Оставить открытой») или **Remain closed** («Оставить закрытой»).

Примечание: Камера может быть привязана только к одной точке контроля доступа; Разные камеры могут быть привязаны к одной и той же точке контроля доступа.

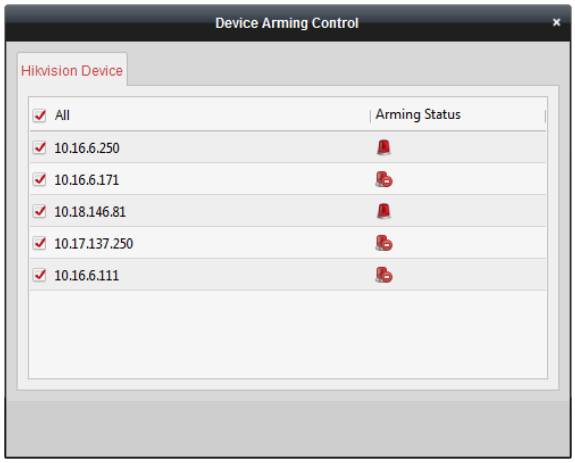
7.13 Управление охраной

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.



7.14 Время и посещаемость

Цель:

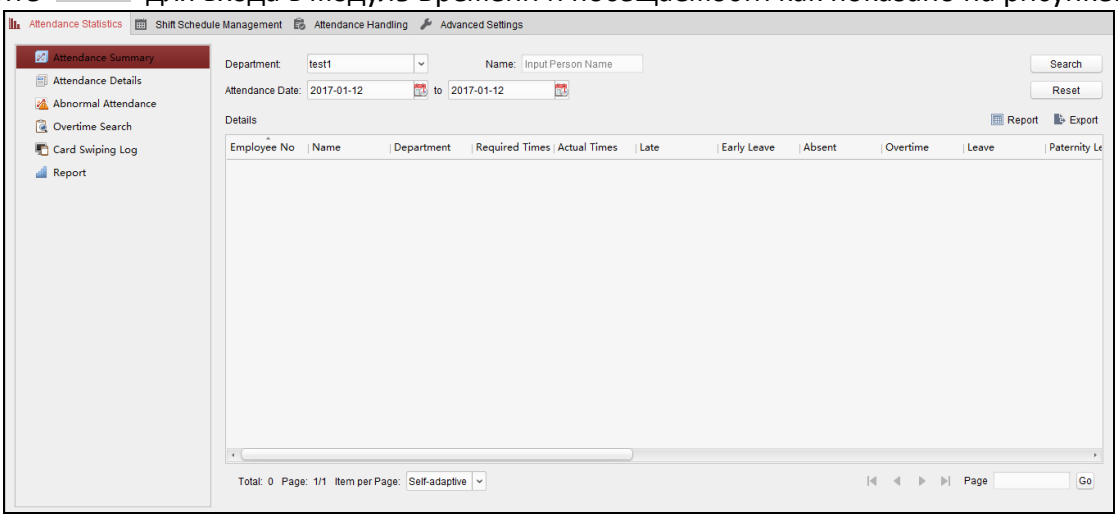
Модуль **Time and Attendance** («Время и посещаемость») обеспечивает множество функциональных возможностей, включая управление расписанием смен, обработку посещаемости, статистику посещаемости и другие расширенные функции.

Перед началом:

Вы должны добавить организацию и человека в модуле **Access Control** («Контроль доступа»). Для получения подробной информации смотрите *Раздел 7.4.1 Добавление организации* и *Раздел 7.5.1 Добавление людей.*

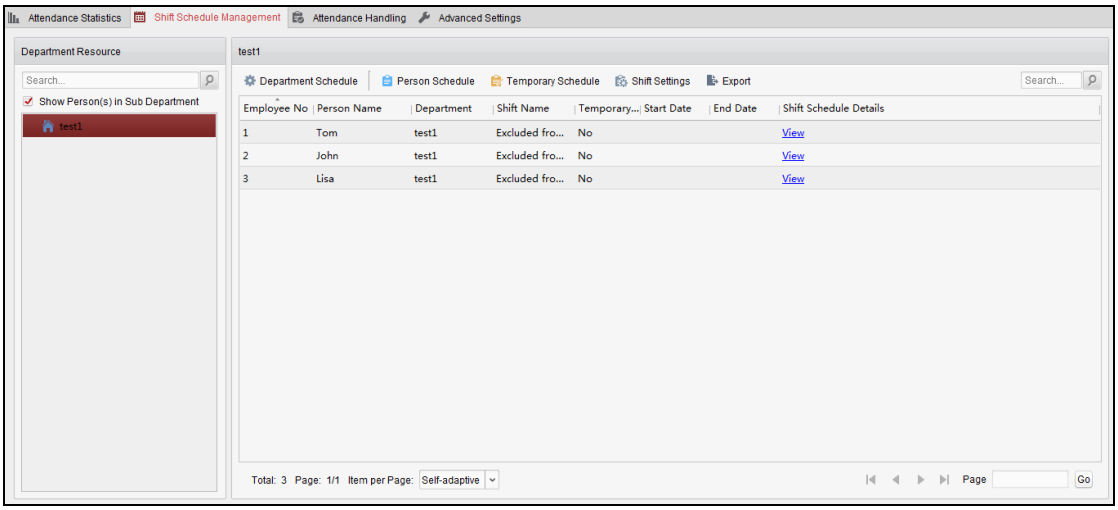
Выполните следующие шаги для доступа к модулю **Time and Attendance** («Время и посещаемость»).

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



7.14.1 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:

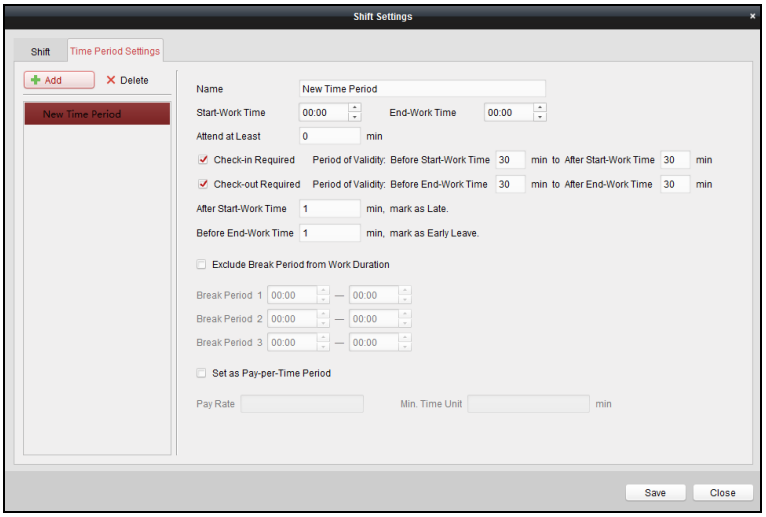
Вы можете добавлять периоды времени и смены для расписания смен.

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. Задайте параметры.

   Name («Имя»): Задайте имя для периода времени.

   Start-Work/End-Work Time («Время начала/окончания работы»): Установите время начала работы и время окончания работы.

   Attend at Least («Присутствовать как минимум»): Установите минимальное время посещения.

   Check-in/Check-out Required («Требуется отметка о приходе/об уходе»): Поставьте галочки и установите действительный период для отметки о приходе/отметки об уходе.

Mark as Late/Mark as Early Leave («Отметить как опоздание/Отметить как ранний уход»): Установите период времени для позднего прихода или раннего ухода.

Exclude Break Period from Work Duration («Исключить период перерыва из времени работы»): Поставьте галочку и установите исключенный период для перерыва.

Примечание: Может быть установлено до трех перерывов в день.

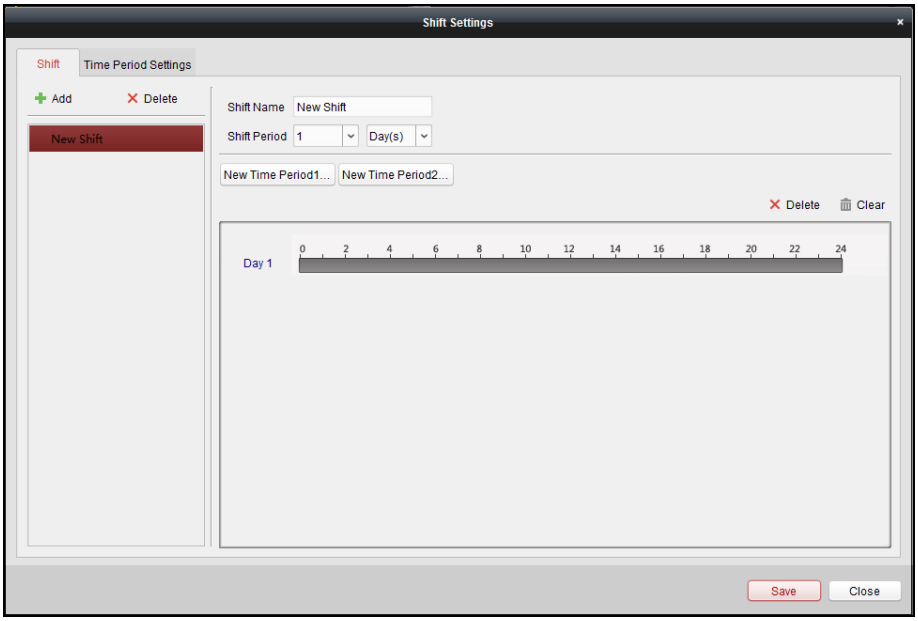
Set as Pay-per-Time Period («Установка периода повременной оплаты»): Поставьте галочку и установите ставку оплаты и минимальную единицу времени.

4. Нажмите **Save** («Сохранить») для сохранения настроек.
   Добавленный период времени отобразится на левой панели.
   Вы также можете нажать **Delete** («Удалить») для удаления периода времени.

➢ **Добавление смены**

Шаги:

1. Нажмите вкладку **Shift** («Смена»).
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.

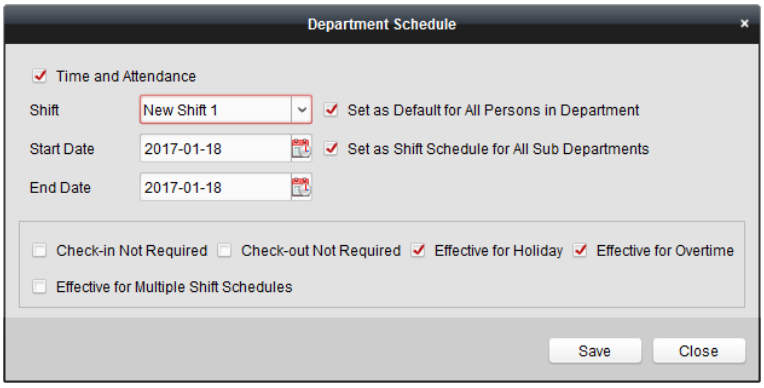
➢ **Расписание отдела**

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 7.4 Управление организацией.*

Шаги:

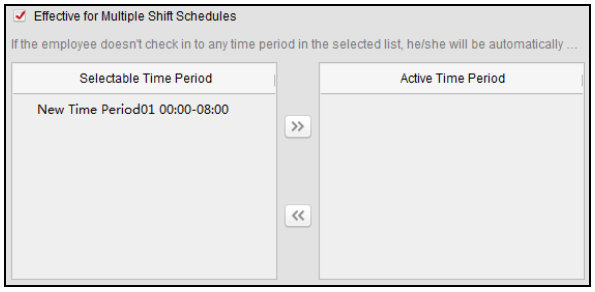
1. Откройте меню **Shift Schedule Management** («Управление расписанием смен») и выберите отдел на панели слева.
2. Нажмите **Department Schedule** («Расписание отдела») для появления диалогового окна настройки расписания отдела.



3. Поставьте галочку **Time and Attendance** («Время и посещаемость»).
   Всем людям в отделе, кроме тех, кто был исключен из правил посещаемости, будет присвоено расписание посещаемости.
4. Выберите смену из выпадающего списка **Shift** («Смена»).
5. Установите значения для **Start date** («Дата начала») и **End date** («Дата окончания»).
6. (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.



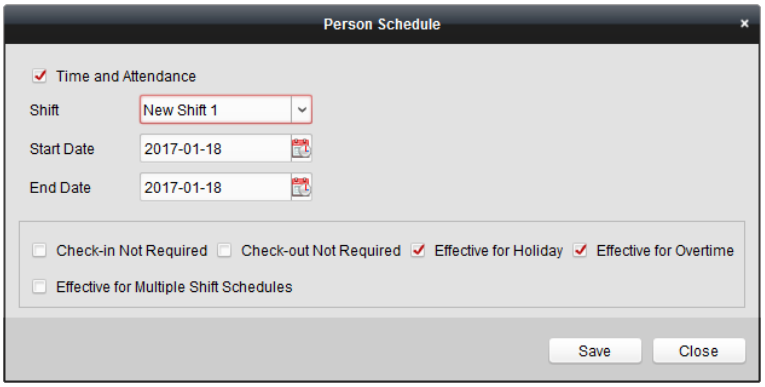
1) В списке **Selectable Time Period** («Доступные для выбора периоды времени») слева нажмите на добавленный период времени и нажмите » для добавления его в список справа.
2) (Опционально) Для удаления выбранного периода времени, выберите его и нажмите «.

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.



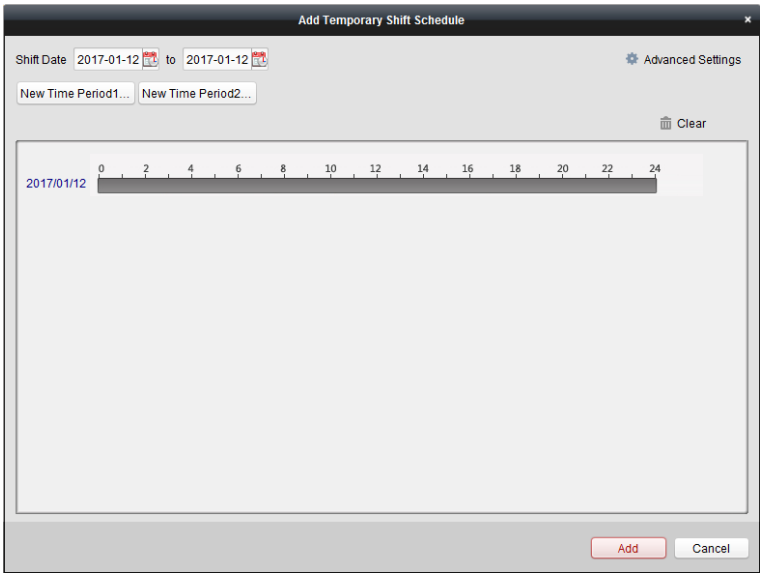
4. Поставьте галочку **Time and Attendance** («Время и посещаемость»).
   К выбранному человеку будет применено расписание посещаемости.

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.

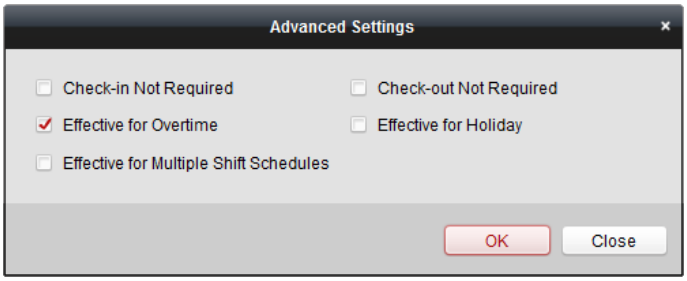
➢ **Временное расписание**

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.

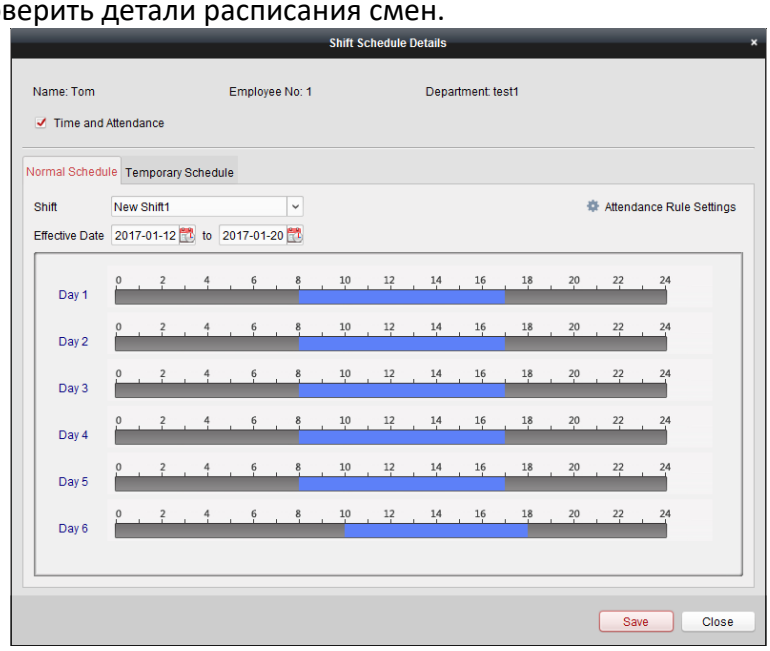


7. Нажмите **Add** («Добавить») для сохранения настроек.

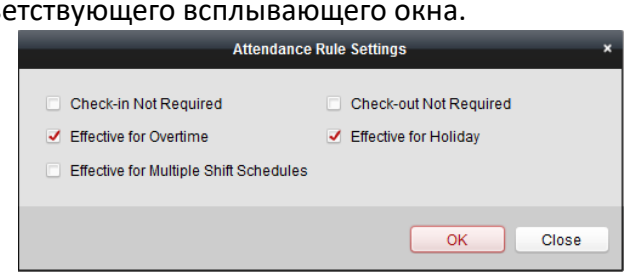
➢ **Проверка деталей расписания смен**

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.



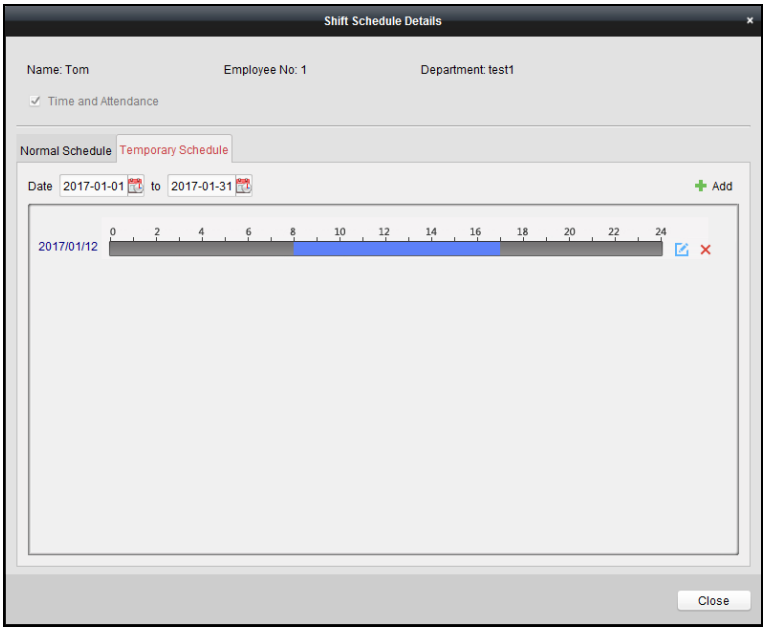
4. Нажмите вкладку **Normal Schedule** («Обычное расписание»).
   Вы можете проверить и отредактировать детали обычного расписания.
   1) Выберите смену из выпадающего списка.
   2) Нажмите **Attendance Rule Settings** («Настройки правила посещаемости») для появления соответствующего всплывающего окна.



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 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.

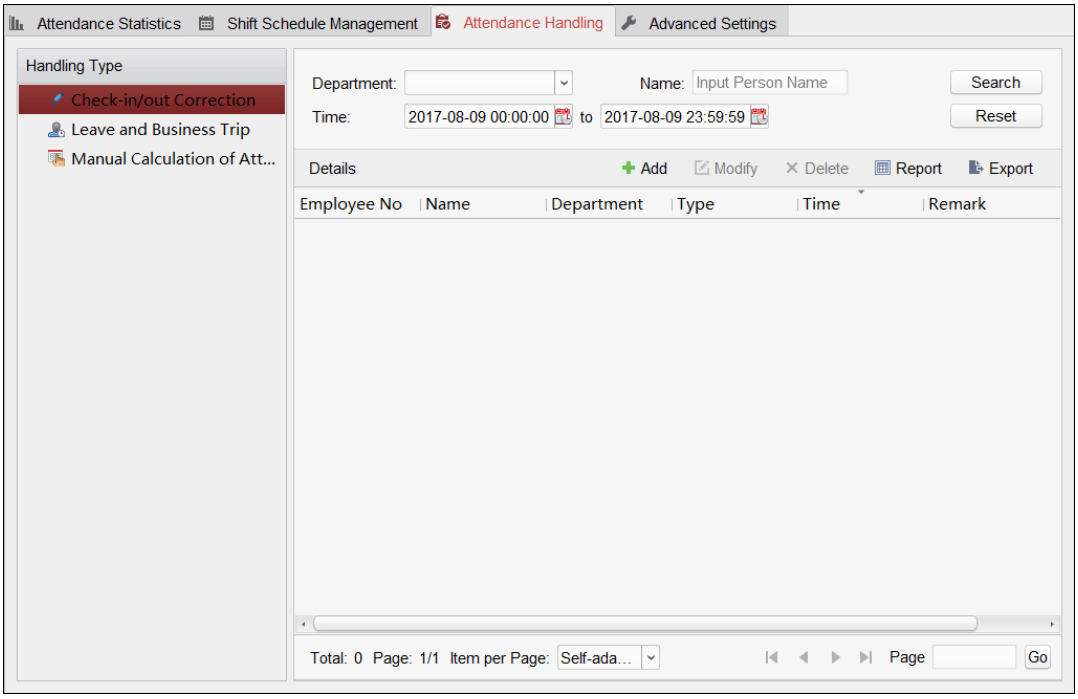
Примечание: Экспортированные данные сохраняются в формате *.csv.

7.14.2 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

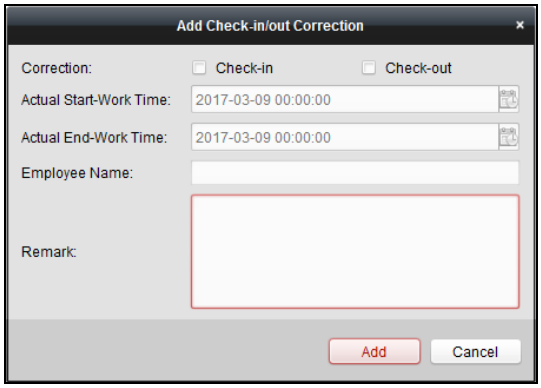
Цель:

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.



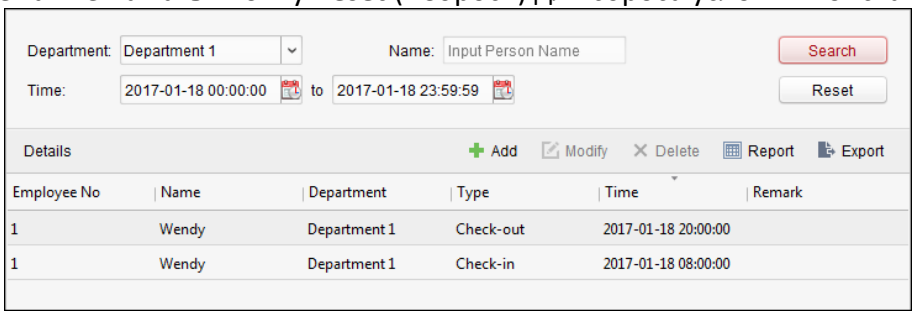
3. Установите параметры корректировки отметки о приходе/уходе.
   Для корректировки отметки о приходе: Поставьте галочку **Check-in** («Отметка о приходе») и установите фактическое время начала работы.
   Для корректировки отметки об уходе: Поставьте галочку **Check-out** («Отметка об уходе») и установите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



Отпуск и деловая поездка

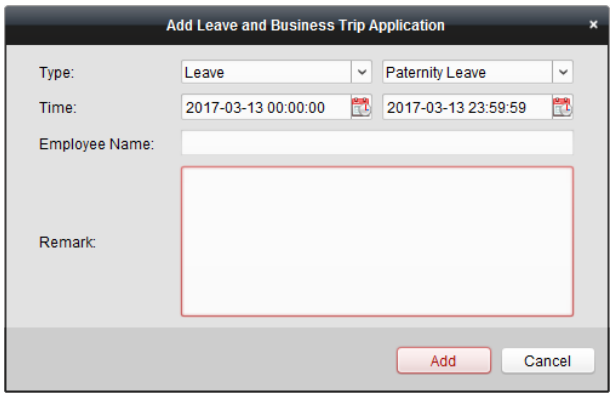
Цель:

Вы можете добавлять, редактировать, удалять, искать отпуска и командировки, а также генерировать соответствующий отчет. Вы можете экспортировать данные об отпусках и командировках на локальный ПК.

➢ **Добавление отпуска и деловой поездки**

Шаги:

1. Нажмите вкладку **Leave and Business Trip** («Отпуск и деловая поездка»).
2. Нажмите **Add** («Добавить») для появления всплывающего окна добавления отпуска и деловой поездки.



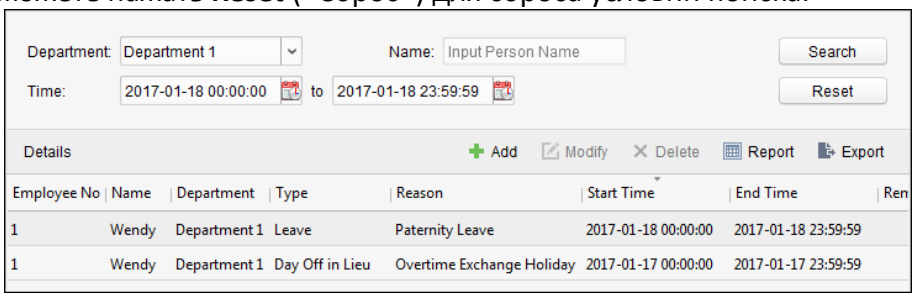
3. Выберите **Leave and business trip type** («Тип отпуска и деловой поездки») из выпадающего списка.
   Вы можете сконфигурировать тип отпуска в Расширенных настройках. Для получения подробной информации смотрите пункт *Настройки типа отпуска*.
4. Нажмите для установки определенного диапазона времени.
5. Нажмите на поле **Employee Name** («Имя сотрудника») и выберите необходимого человека.
   Вы также можете ввести ключевое слово и нажать для поиска необходимого человека.
6. (Опционально) Внесите какие-либо заметки в поле **Remark** («Примечание»), если необходимо.
7. Нажмите **Add** («Добавить») для добавления отпуска и деловой поездки.
   Добавленные отпуска и деловые поездки будут отображены в меню **Attendance Handling** («Обработка посещаемости»).
   (Опционально) Выберите отпуск и деловую поездку и нажмите кнопку **Modify** («Изменить») для редактирования отпуска или деловой поездки.
   (Опционально) Выберите отпуск и деловую поездку и нажмите кнопку **Delete** («Удалить») для удаления отпуска или деловой поездки.
   (Опционально) Нажмите кнопку **Report** («Отчет») для генерирования отчета об отпуске или деловой поездке.
   (Опционально) Нажмите кнопку **Export** («Экспорт») для экспорта деталей отпуска или деловой поездки на локальный ПК.
   Примечание: Экспортированные данные сохраняются в формате *.csv.

➢ **Поиск отпуска и деловой поездки**

Шаги:

1. Нажмите вкладку **Leave and Business Trip** («Отпуск и деловая поездка»).
2. Задайте условия поиска.
   Department («Отдел»): Выберите отдел из выпадающего списка.
   Name («Имя»): Введите имя человека.
   Time («Время»): Нажмите для установки диапазона времени.

3. Нажмите **Search** («Поиск») для поиска отпусков и деловых поездок.
   Сведения об отпусках и командировках будут отображены в списке.
   Вы также можете нажать **Reset** («Сброс») для сброса условий поиска.



Подсчет посещаемости вручную

Цель:

Вы можете вычислить результат посещаемости вручную, если необходимо, указав время начала и окончания.

Шаги:

1. Нажмите вкладку **Manual Calculation of Attendance** («Подсчет посещаемости вручную»).
2. Установите **Start time** («Время начала») и **End time** («Время окончания») для расчета.
3. Нажмите **Calculate** («Рассчитать») для начала.

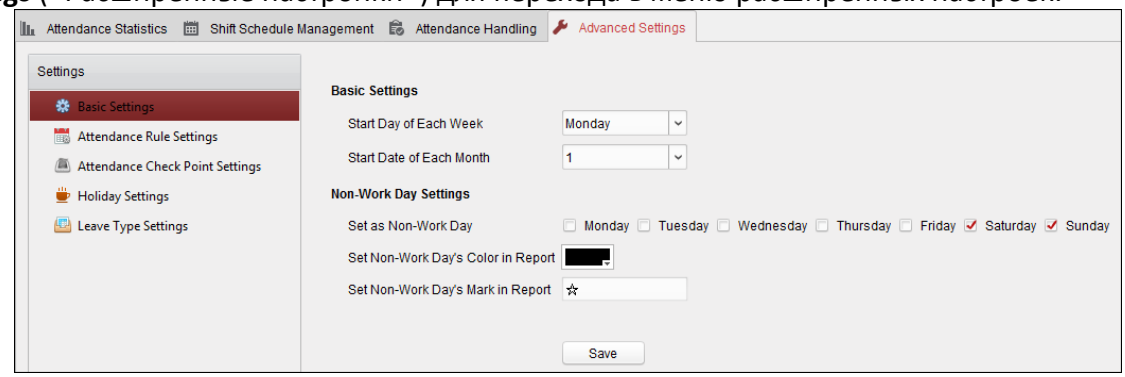
Примечание: Могут быть рассчитаны данные о посещаемости в течение трех месяцев.

7.14.3 Расширенные настройки

Цель:

Вы можете задать основные параметры, правила посещаемости, контрольные точки посещаемости, настройки выходных и тип отпуска.

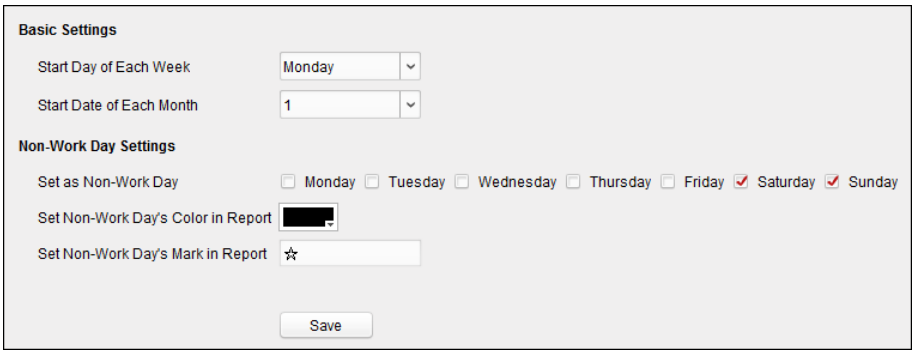
Откройте модуль **Time and Attendance** («Время и посещаемость») и нажмите **Advanced Settings** («Расширенные настройки») для перехода в меню расширенных настроек.



Основные настройки

Шаги:

1. Нажмите вкладку **Basic Settings** («Основные настройки») для входа в меню основных настроек.

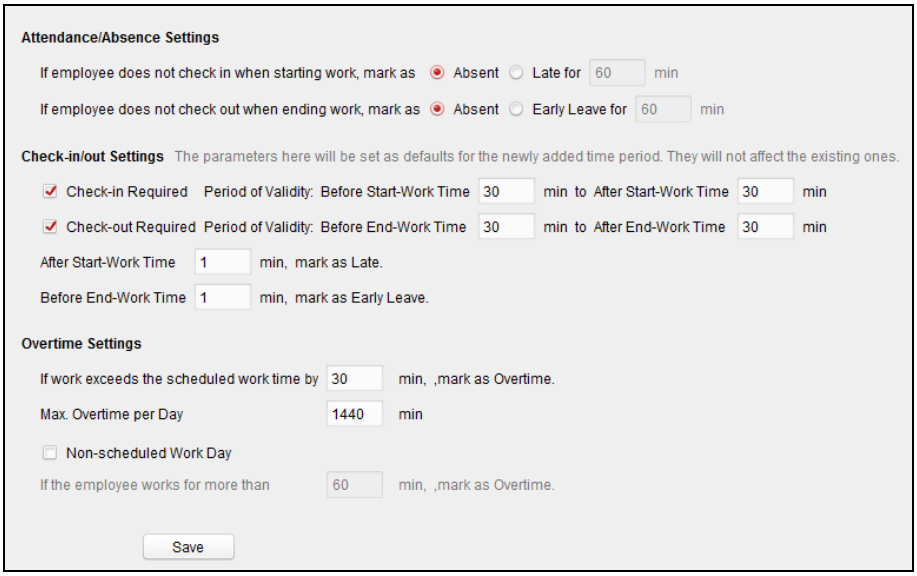


2. Задайте основные параметры.
   Start Day of Each Week («День начала недели»): Вы можете выбрать один день в качестве первого дня недели.
   Start Date of Each Month («Начальная дата каждого месяца»): Вы можете выбрать один день в качестве первого дня месяца.
3. Задайте настройки нерабочего дня.
   Set as Non-Work Day («Установить как нерабочий день»): Поставьте галочки, чтобы установить выбранные дни в качестве нерабочих дней.
   Set Non-Work Day's Color in Report («Установить цвет нерабочего дня в отчете»): Нажмите на цветное поле и выберите цвет, чтобы отметить нерабочий день в отчете.
   Set Non-Work Day's Mark in Report («Установить отметку для нерабочего дня в отчете»): Введите отметку для нерабочего дня в отчете.
4. Нажмите **Save** («Сохранить») для сохранения настроек.

Настройки правил посещаемости

Шаги:

1. Нажмите вкладку **Attendance Rule Settings** («Настройки правил посещаемости») для перехода в соответствующее меню.



2. Задайте настройки посещения или отсутствия.
   Если сотрудник не отметился при приходе на работу, вы можете отметить **Absent** («Отсутствует») или **Late** («Опаздывает») и установить время опоздания.

Если сотрудник не отметился при уходе с работы, вы можете отметить **Absent** («Отсутствует») или **Early Leave** («Ушел раньше») и установить время раннего ухода.

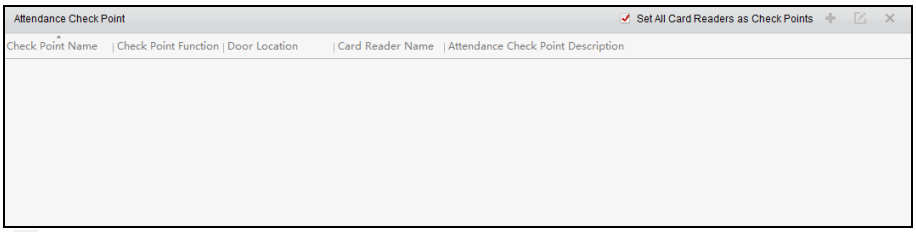
3. Установите параметры отметки о приходе/об уходе.
   Вы можете поставить галочку **Check-in Required** («Требуется отметка о приходе») или **Check-out Required** («Требуется отметка об уходе») и установить действительный период.
   Вы также можете установить правило для опоздания или раннего ухода.
   Примечание: Параметры здесь будут установлены по умолчанию для вновь добавленного периода времени. Это не повлияет на существующие периоды.
4. Установите параметры сверхурочной работы.
   Вы можете установить правило сверхурочной работы и установить максимальную переработку на каждый день.
   (Опционально) Вы можете поставить галочку **Non-scheduled Work Day** («Ненормированный рабочий день») и установить правило сверхурочной работы.
5. Нажмите **Save** («Сохранить») для сохранения настроек.

Настройки контрольной точки посещаемости

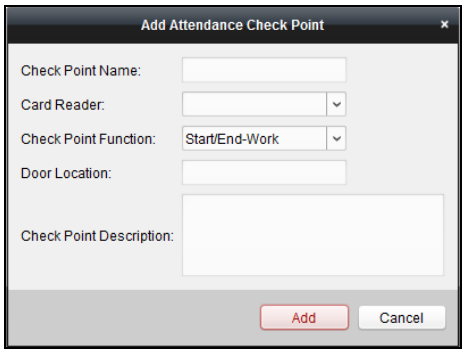
Вы можете установить считыватель карт контрольной точки доступа в качестве контрольной точки посещаемости, чтобы проводка карты через считыватель карты учитывалась в посещаемости.

Шаги:

1. Нажмите вкладку **Attendance Check Point Settings** («Настройки контрольной точки посещаемости») для перехода в соответствующее меню.



2. Нажмите  для появления всплывающего окна добавления контрольной точки посещаемости.



3. Задайте связанную информацию.
   Check Point Name («Имя контрольной точки»): Введите имя контрольной точки.
   Card Reader («Считыватель карт»): Выберите считыватель карт из выпадающего списка.
   Check Point Function («Функция контрольной точки»): Выберите функцию для контрольной точки.
   Door Location («Местоположение двери»): Введите местоположение двери.

Check Point Description («Описание контрольной точки»): Задайте описание для контрольной точки.

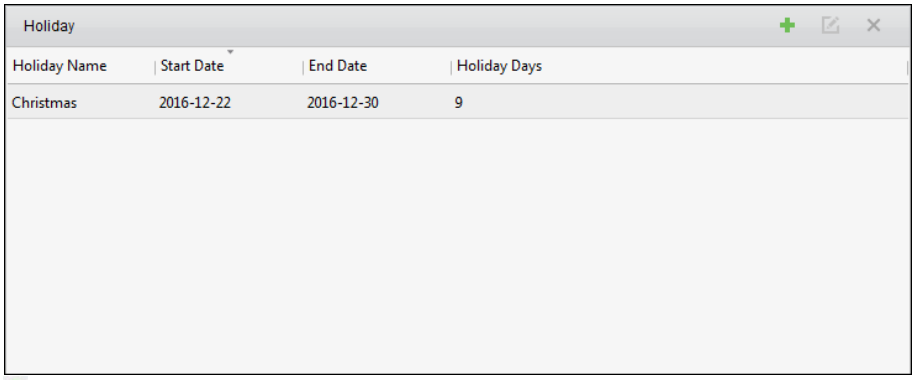
4. Нажмите **Add** («Добавить») доя добавления контрольной точки посещаемости.
   Добавленные контрольные точки посещаемости будут отображены в списке.
5. (Опционально) Поставьте галочку **Set All Card Readers as Check Points** («Установить все считыватели карт в качестве контрольной точки»).
   Вы можете использовать все считыватели карт в качестве контрольных точек.
   Примечание: Если галочка не установлена, тогда только считыватели карт в списке будут добавлены в качестве контрольных точек.

Вы также можете редактировать или удалять считывателя карт.
Нажмите для редактирования считывателя карт.
Нажмите для удаления считывателя карт.

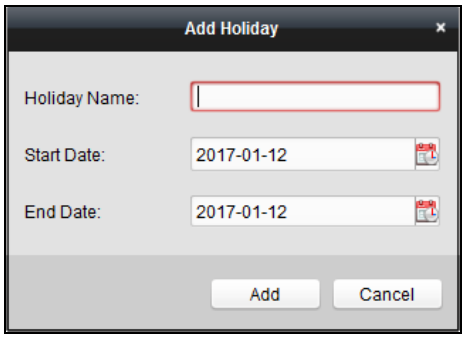
Настройки выходных

Шаги:

1. Нажмите вкладку **Holiday Settings** («Настройки выходных») для перехода в меню настройки выходных.



2. Нажмите для появления всплывающего окна добавления выходных.



3. Установите связанные параметры.
   Holiday Name («Имя выходного»): Введите название для выходного.
   Start Date/End Date («Дата начала/окончания»): Нажмите для указания даты выходного.
4. Нажмите **Add** («Добавить») для добавления выходного.
   Добавленные выходные будут отображены в списке.

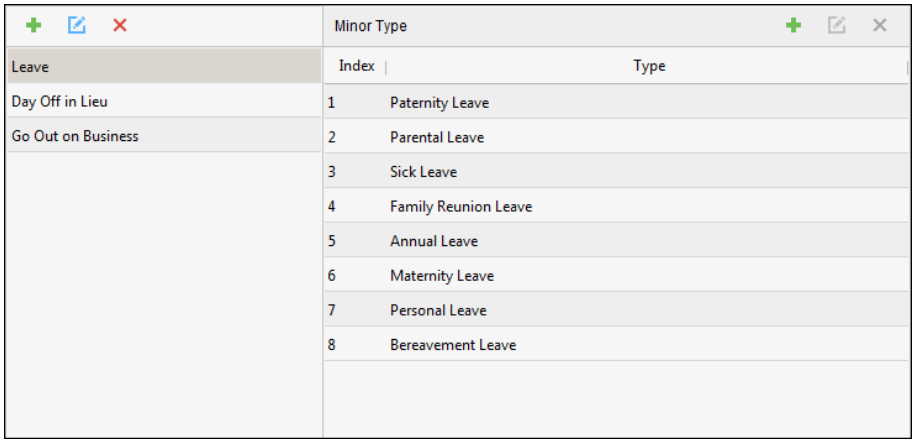
Вы также можете редактировать или удалять выходные.
Нажмите для редактирования выходного.

Нажмите ✕ для удаления выходного.

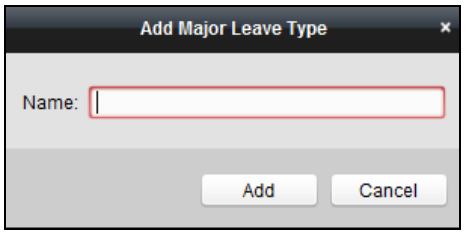
Настройка типа отпуска

Шаги:

1. Нажмите вкладку **Leave Type Settings** («Настройки типа отпуска») для перехода в соответствующее меню.

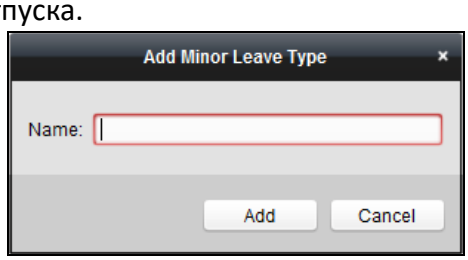


2. Добавьте основной тип отпуска.
   1) Нажмите ✚ на панели слева для появления всплывающего окна добавления основного типа отпуска.



   2) Введите имя для основного типа отпуска.
   3) Нажмите **Add** («Добавить») для добавления основного типа отпуска.

   Вы также можете редактировать или удалять основной тип отпуска.
   Нажмите ✎ для редактирования основного типа отпуска.
   Нажмите ✕ для удаления основного типа отпуска.
3. Добавьте второстепенный тип отпуска.
   1) Выберите основной тип отпуска.
      Второстепенный тип отпуска, относящийся к этому основному типу отпуска, будет отображаться на правой панели.
   2) Нажмите ✚ на панели справа для появления всплывающего окна добавления второстепенного типа отпуска.



   3) Введите имя для второстепенного типа отпуска.

4) Нажмите **Add** («Добавить») для добавления второстепенного типа отпуска.

Вы также можете редактировать или удалять второстепенный тип отпуска.

Нажмите для редактирования второстепенного типа отпуска.

Нажмите для удаления второстепенного типа отпуска.

7.14.4 Статистика посещаемости

Цель:

После расчета данных посещаемости вы можете проверить сводку посещаемости, данные о посещаемости, ненормальную посещаемость, сверхурочные часы сотрудников, журналы проводок карт и отчеты на основе рассчитанных данных посещаемости.

Примечания:

- Клиент автоматически вычисляет данные о посещаемости предыдущего дня в 1:00 утра на следующий день.
- Оставляйте клиент работать на ночь, чтобы в 1:00 он смог провести вычисление данных о посещаемости предыдущего дня автоматически, иначе эта процедура не сможет быть выполнена. Если подсчет не будет выполнен автоматически, вы сможете выполнить его вручную. Для получения подробной информации смотрите *Руководство расчета посещаемости* в *Разделе 7.14.2 Обработка посещаемости*.

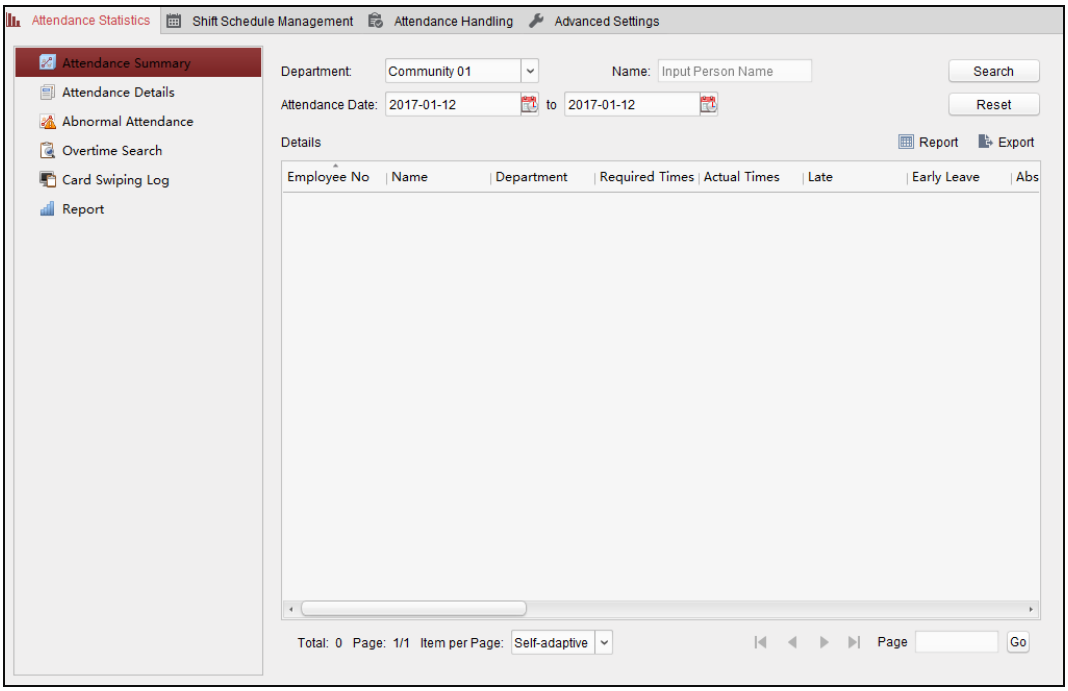
Сводка посещаемости

Цель:

Вы можете получить всю статистику посещаемости сотрудников за указанный период времени.

Шаги:

1. В модуле **Time and Attendance** («Время и посещаемость») нажмите вкладку **Attendance Statistics** («Статистика посещаемости») для перехода на страницу статистики посещаемости.
2. Нажмите элемент **Attendance Summary** («Сводка посещаемости») на панели слева для перехода в соответствующее меню.

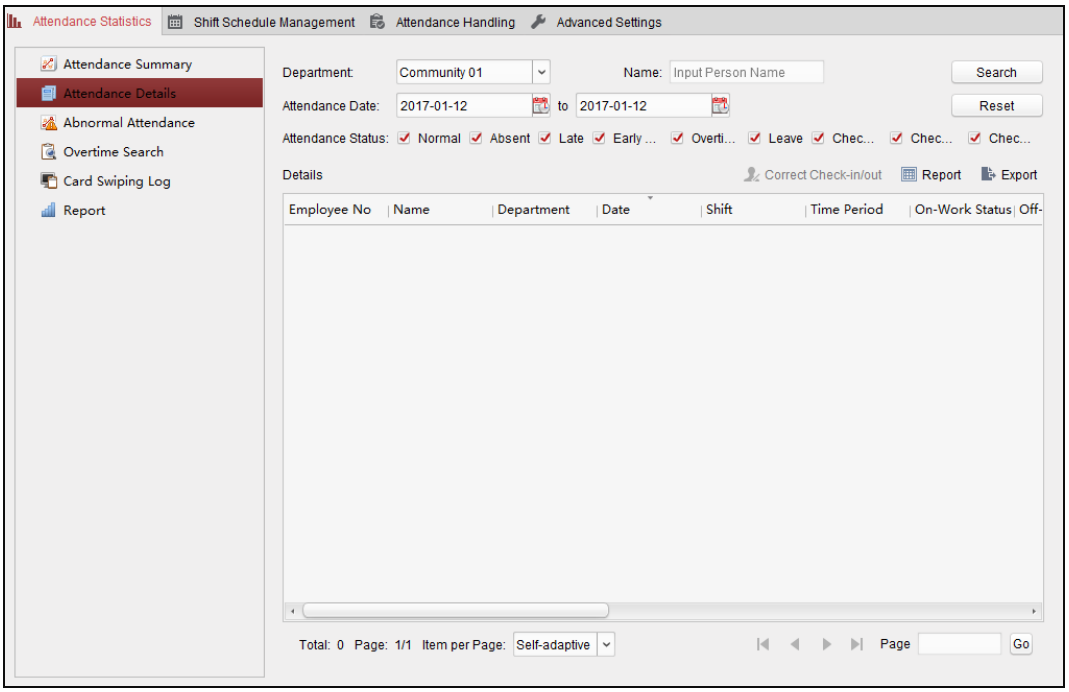


3. Задайте условия поиска, включая отдел, имя сотрудника и дату посещения.
   (Опционально) Вы можете нажать **Reset** («Сброс») для сброса всех настроенных условий поиска.
4. Нажмите **Search** («Поиск») для начала поиска, подходящие результаты будут отображены в виде списка на этой странице.
   (Опционально) Нажмите **Report** («Отчет») для генерации отчета посещаемости.
   (Опционально) Нажмите **Export** («Экспорт») для экспорта результатов на локальный ПК.

Детали посещаемости

Шаги:

1. На странице Статистики посещаемости нажмите **Attendance Details** («Детали посещаемости») на панели слева для перехода в меню деталей посещаемости.



2. Задайте условия поиска, включая отдел, имя сотрудника, дату посещения и статус.
   (Опционально) Вы можете нажать **Reset** («Сброс») для сброса всех настроенных условий поиска.
3. Нажмите **Search** («Поиск») для начала поиска, подходящие результаты будут отображены в виде списка на этой странице.
   (Опционально) Вы можете выбрать результат в списке и нажать **Correct Check-in/out** («Корректировать отметку о приходе/об уходе») для корректировки состояния прихода/ухода.
   (Опционально) Нажмите **Report** («Отчет») для генерации отчета посещаемости.
   (Опционально) Нажмите **Export** («Экспорт») для экспорта результатов на локальный ПК.

Ненормальная посещаемость

Вы можете выполнять поиск и получить статистику ненормальных данных посещаемости, включая номер, имя и отдел сотрудников, ненормальности события тип, время начала/окончания и дату посещения. Для получения подробной информации об операциях смотрите *Раздел 7.14.4 Статистика посещаемости*.

Поиск сверхурочной работы

Вы можете выполнять поиск и получать статистику о переработках выбранных сотрудников за определенный период времени. И вы можете проверить подробную информацию о сверхурочной работе, включая номер, имя и отдел сотрудника, дату посещения, продолжительность сверхурочной работы и тип сверхурочной работы. Для получения подробной информации об операциях смотрите *Раздел 7.14.4 Статистика посещаемости*.

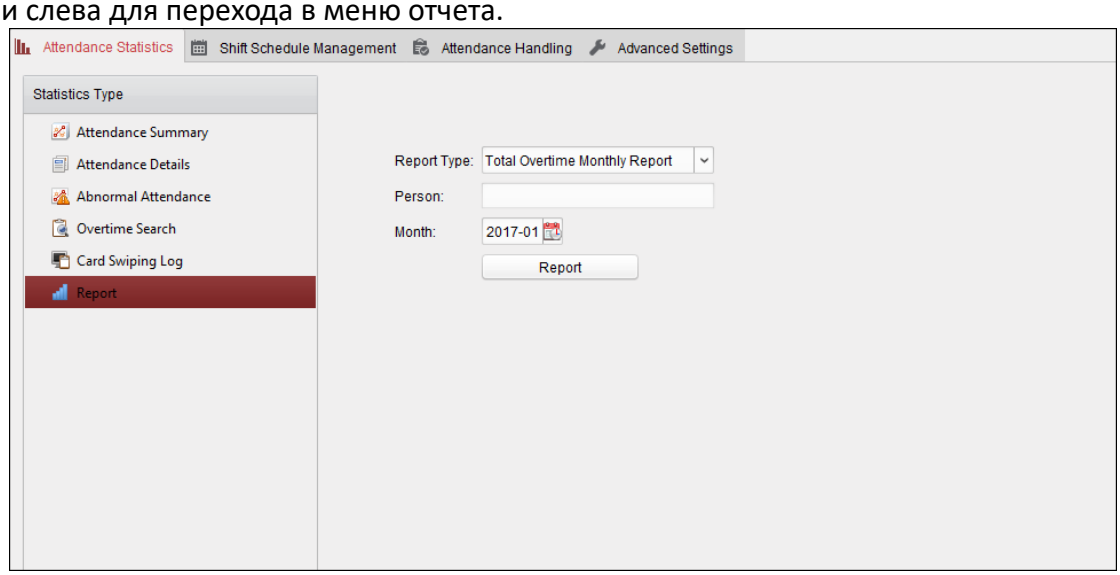
Журнал проводок карт

Вы можете выполнять поиск в журнале проводок карт, используемом для сбора статистики посещаемости. После поиска записей журнала вы можете проверить данные о проводке

картой, включая имя и отдел сотрудников, время проводки карты, режим аутентификации считывателя карт и № карты. Для получения подробной информации об операциях смотрите *Раздел 7.14.4 Статистика посещаемости*.

Отчет

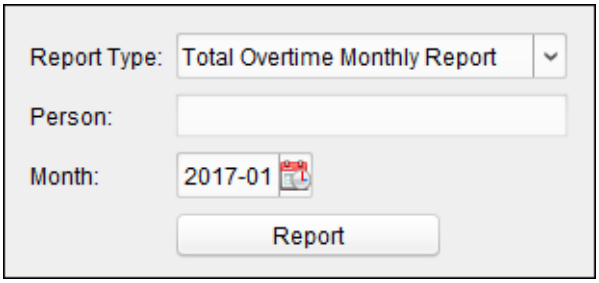
На страницу **Attendance Statistics** («Статистика посещаемости») нажмите **Report** («Отчет») на панели слева для перехода в меню отчета.



➢ **Генерация итогового отчета за месяц по переработкам**

Шаги:

1. Нажмите в поле **Report Type** («Тип отчета»), чтобы развернуть выпадающий список и выбрать **Total Overtime Monthly Report** («Итоговый отчет за месяц по переработкам»).



2. Нажмите поле **Person** («Человек») для выбора человека.
3. Нажмите для указания месяца.
4. Нажмите **Report** («Отчет») для начала генерации отчета.

➢ **Генерация месячного отчета о деталях переработки**

Выберите **Overtime Details Monthly Report** («Месячный отчет о деталях переработки») в поле **Report Type** («Тип отчета»). Вы можете сгенерировать месячный отчет о деталях переработки. Для получения подробной информации смотрите пункт *Генерация итогового отчета за месяц по переработкам.*

➢ **Генерация ежемесячного отчета о посещаемости**

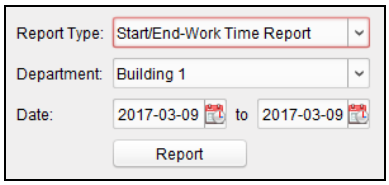
Выберите **Attendance Monthly Report** («Месячный отчет о посещаемости») в поле **Report**

Type («Тип отчета»). Вы можете сгенерировать месячный отчет о посещаемости. Для получения подробной информации смотрите пункт *Генерация итогового отчета за месяц по переработкам.*

➢ **Генерация отчета о времени начала/окончания работы**

Шаги:

1. Нажмите в поле **Report Type** («Тип отчета»), чтобы развернуть выпадающий список и выбрать **Start/End-Work Time Report** («Отчет о времени начала/окончания работы»).



2. Нажмите **Department** («Отдел») для выбора отдела.
3. Нажмите для указания времени начала и окончания периода.
4. Нажмите **Report** («Отчет») для начала генерации отчета.

➢ **Генерация отчета о посещаемости по отделу**

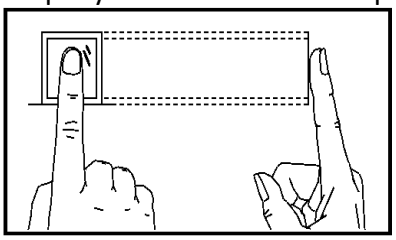
Выберите **Department Attendance Report** («Отчет о посещаемости по отделу») в поле **Report Type** («Тип отчета»). Для получения подробной информации смотрите пункт *Генерация отчета о времени начала/окончания работы* выше.

Приложение A Рекомендации по сканированию отпечатков пальцев

Для сканирования отпечатка используйте указательный, средний или безымянный палец.

Правильное сканирование

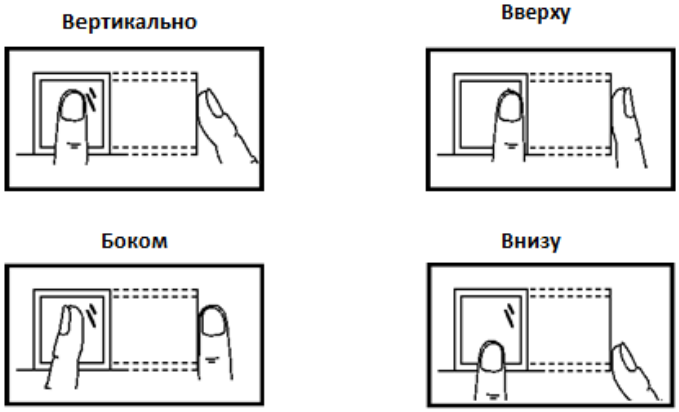
На рисунке ниже показан правильный способ сканирования:



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

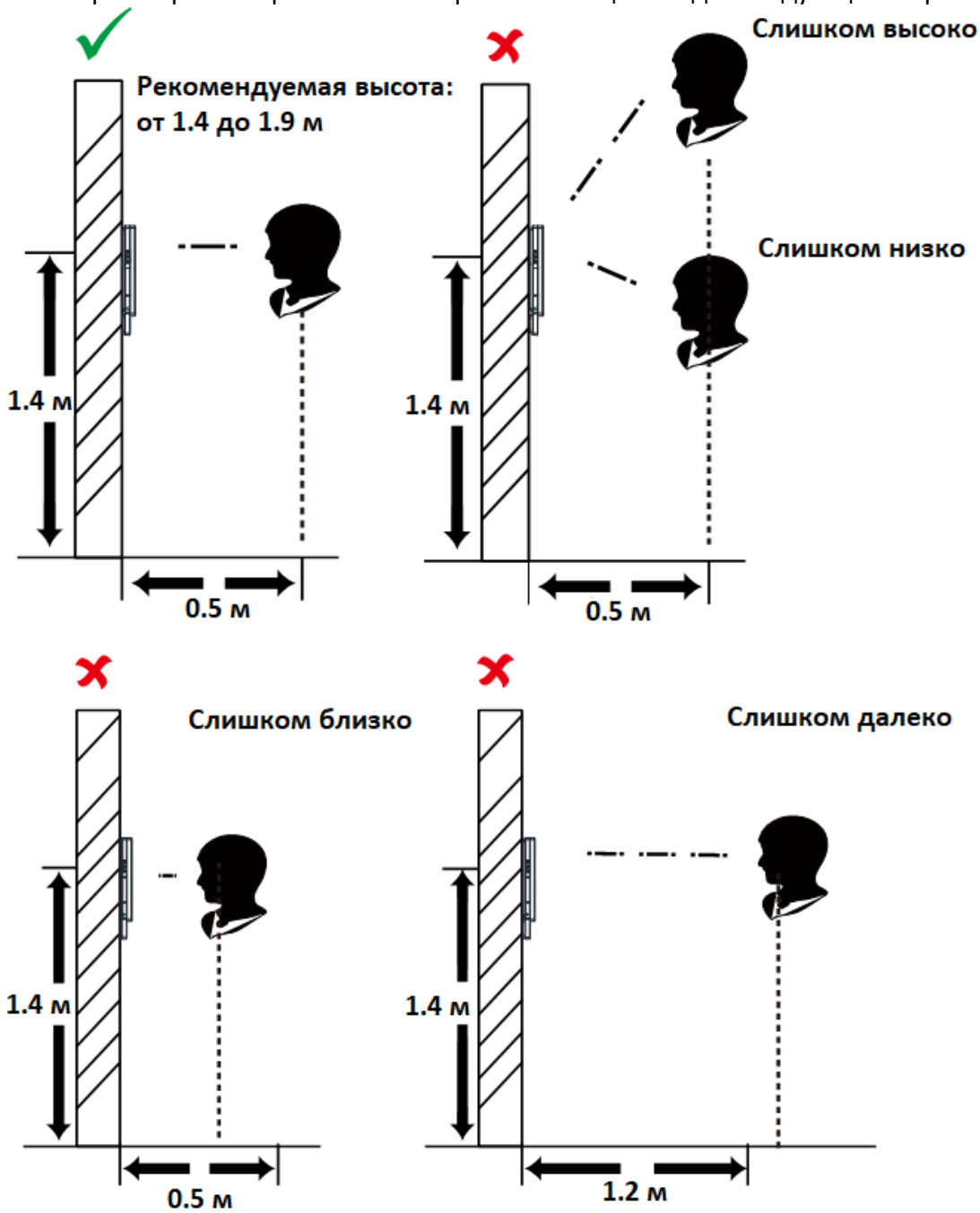
Если у вас неглубокий отпечаток пальца или его сложно отсканировать, мы рекомендуем вам использовать другие методы аутентификации.

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

Приложение B Советы по сбору/сравнению изображений лиц

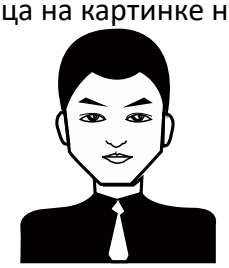
B.1 Положения (Рекомендуемое расстояние: 0,5 м)

Положение при сборе или сравнении изображений лиц выглядит следующим образом:



B.2 Выражение лица

- Сохраняйте свое выражение естественным при сборе или сравнении изображений лица, так же как выглядит выражение лица на картинке ниже.



- Не надевайте шляпу, солнцезащитные очки или другие аксессуары, которые могут повлиять на функцию распознавания лиц.
- Не позволяйте вашим волосам закрывать глаза, уши и т.п., также не разрешается сильный макияж.

B.3 Положение лица

Чтобы получить качественное и точное изображение лица смотрите в камеру прямо при сборе или сравнении изображений лиц.

B.4 Размер лица

Убедитесь, что ваше лицо находится в середине окна.

Приложение С Советы по среде установки

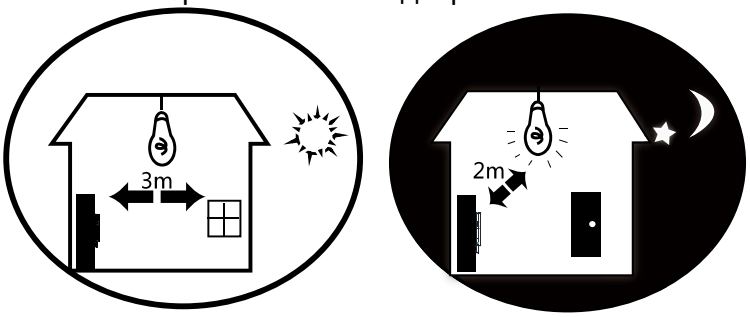
1. Эталонные значения освещенности для разных источников света

Свеча: 10 лк

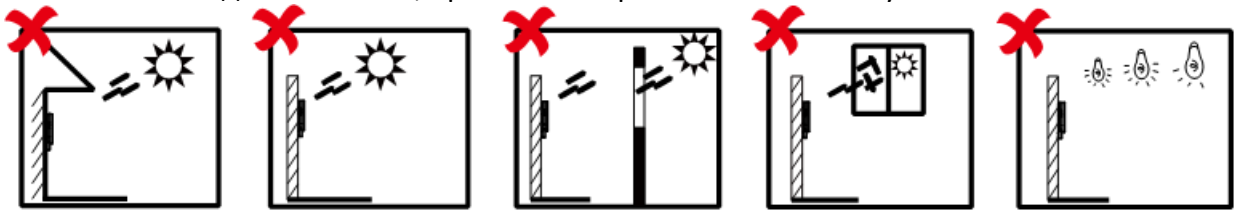
Лампа: от 100 до 850 лк

Солнечный свет: Более 1200 лк

2. Если источник света находится на расстоянии 0,5 м от устройства, освещенность должна быть не менее 100 лк.
3. Установите устройство в помещении, на расстоянии не менее 2 метров от источника света и не менее чем в 3 метрах от окна или двери.



4. Избегайте задней засветки, прямых и непрямых солнечных лучей.

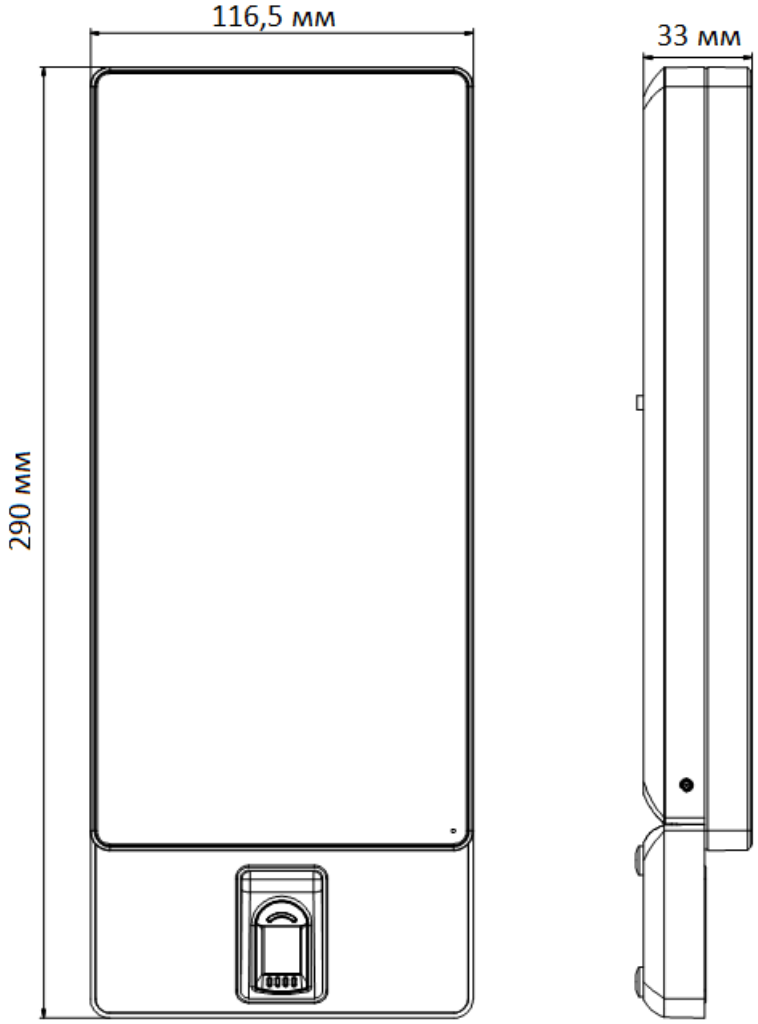


Приложение D Связь между расстоянием пробуждения и окружающей средой

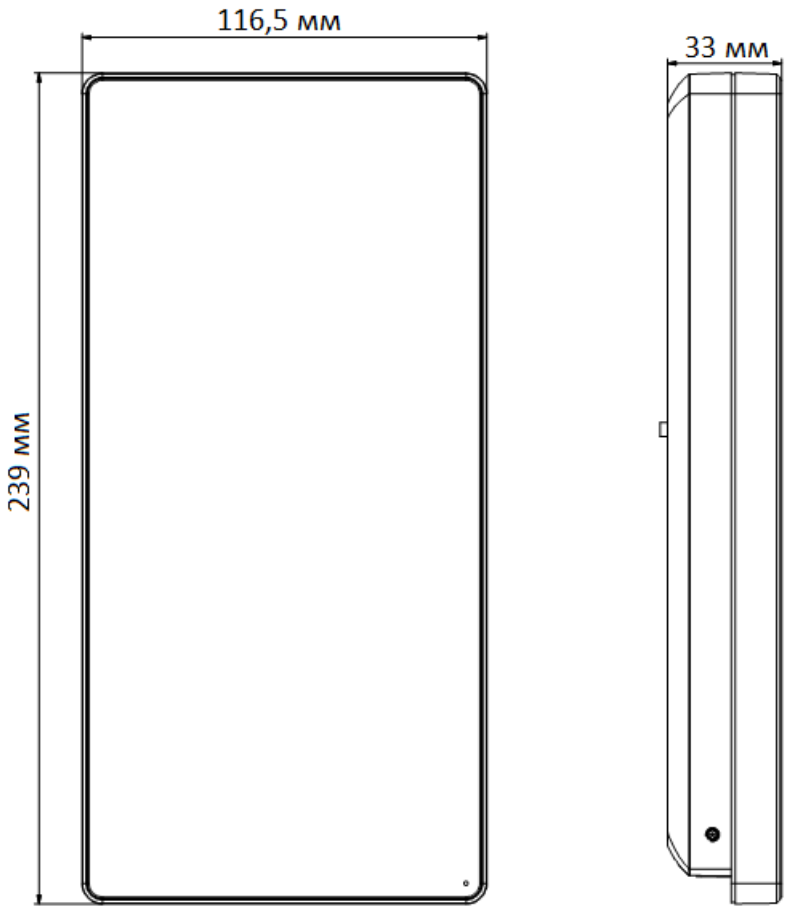
	Среда	**Короткая**	**Средняя**	**Длинная**
В сумерках (Низкая освещенность)	Обычная белая стена	1.06 м	1.67 м	3.62 м
	Акриловая стена в лаборатории	0.85/0.73 м	1.30/1.21 м	4.16 м
	Тело человека	0.74 м	0.94 м	1.50/1.45 м
	Оконное стекло	/	/	/
Ночью (Свет выключен)	Обычная белая стена	0.97 м	1.61 м	3.91 м
	Акриловая стена в лаборатории	0.79 м	1.32 м	3.67 м
	Тело человека	0.47 м	1.03 м	1.65 м
	Оконное стекло	1.18/1.65 м (Включенный свет в ночное время)	1.53/2.66 м (Включенный свет в ночное время)	3.35 м
День (Включена люминесцентная лампа)	Обычная белая стена	1.1 м	1.8 м	> 4 м
	Акриловая стена в лаборатории	0.8 м	1.5 м	3.1 м
	Тело человека	0.7/0.6 м	1.2/1.14 м	1.5/1.42 м
	Оконное стекло	1.1 м	1.8 м	> 4 м
День (Камера повернута к солнечному свету)	Тело человека	0.3/0.26 м	0.56/0.5 м	1.03/1.06 м
День (Камера отвернута от солнечного света)	Тело человека	0.36 м	0.6 м	1.25 м
Ночью (Свет включен)	Акриловая черная стена	0.56 м	0.83 м	1.25 м

Приложение E Размеры

Размеры DS-K1T607 (С модулем отпечатков пальцев)



Размеры DS-K1T607 (Без модуля отпечатков пальцев)




See Far, Go Further