Терминал доступа с функцией распознавания лиц

Руководство пользователя

Руководство пользователя

Настоящее Руководство предназначено для Терминала распознавания лиц.

Название	Модель
Терминал распознавания лиц	DS-K5603-Z
Терминал распознавания лиц	DS-K5603T-Z

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 торговые марки Hikvision и логотипы являются интеллектуальной собственностью Hikvision в различных юрисдикциях. Другие торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

Правовая информация

ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПРОДУКТ, АППАРАТУРА, ПРОГРАММНОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», СО ВСЕМИ ОШИБКАМИ И НЕТОЧНОСТЯМИ, HIKVISION НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, КАСАТЕЛЬНО УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА, СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ И ОТСУТСТВИЯ НАРУШЕНИЙ СО СТОРОНЫ ТРЕТЬИХ ЛИЦ. НИ HIKVISION, НИ ЕГО ДИРЕКТОРА, НИ СОТРУДНИКИ ИЛИ ПРЕДСТАВИТЕЛИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ПЕРЕД ПОТРЕБИТЕЛЕМ ЗА КАКОЙ-ЛИБО СЛУЧАЙНЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ, ВКЛЮЧАЯ УБЫТКИ ИЗ-ЗА ПОТЕРИ ПРИБЫЛИ, ПЕРЕРЫВА В ДЕЯТЕЛЬНОСТИ ИЛИ ПОТЕРИ ДАННЫХ ИЛИ ДОКУМЕНТАЦИИ, В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ HIKVISION БЫЛО ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

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

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

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

Поддержка

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

дилеру.

Регулирующая информация

Информация о FCC

Пожалуйста, обратите внимание, что изменения или модификации, явно не 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 радиатором 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

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

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: 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**

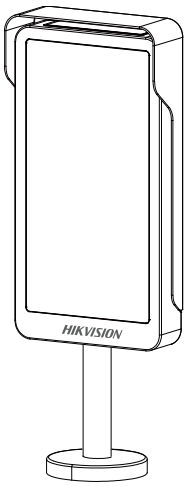
- Не бросайте устройство и не подвергайте его ударам, воздействию сильных электромагнитных излучений. Избегайте установки на поверхности, подверженные вибрациям и встряскам (игнорирование этого условия может привести к поломке оборудования).
- Не устанавливайте устройство в условиях экстремально высоких/низких 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 устройства без упаковки может привести к его поломке и снижению стоимости.
- Неправильное использование или замена батареи может привести к опасности взрыва. Проводите замену на такие же батареи или аналогичные. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем батарей.

Содержание

Глава 1 Обзор

1.1 Представление

Терминал распознавания лиц DS-K5603-Z разработанный с системой TX1, может применяться в сценариях экзаменационного зала, железнодорожного вокзала, банка, здания, гостиницы и т. д., в которых требуется аутентификация посетителей.



1.2 Основные особенности

- 10.1-дюймовый сенсорный экран с разрешением 1280 × 800
- Широкоугольный двойной объектив с разрешением 2 000 000 пикселей
- Детекция настоящего лица

  Функция может определить, является ли обнаруженное лицо реальным человеком или нет.
- Макс. 10,000 изображений лиц; Макс. 10,000 изображений лиц в «черном списке»; Макс. 50,000 событий для сравнения
- Несколько режимов проверки подлинности: аутентификация по карте Mifare + изображение лица, в автоматическом режиме (карта + изображение лица или изображение лица)
- Идентификация по QR-коду вместо карты Mifare

  Примечание: Устройство должно быть подключено к внешнему устройству для считывания карт или функция считывания карт не сможет быть использована.
- Два сетевых интерфейса

  Каждый сетевой интерфейс может автоматически посещать сервер EHome отдельно.
- Позволяет применить к устройству «черный список» лиц из клиента управления iVMS-4200

- Загружает аутентификацию «черного списка» и событие «черного списка», а также отображает их на главном экране
- Позволяет применить к устройству изображения лиц из клиента управления iVMS-4200
- Импорт изображений лиц на устройство через USB-интерфейс
- Экспорт изображений лиц и событий на устройство через USB-интерфейс
- Связь с контроллером доступа через режим связи RS-232 и связь со сторонними устройствами через режим связи RS-485
- Загрузка оффлайн событий
- Аудио подсказки

Глава 2 Внешний вид

Внешний вид устройства, размеры и описание представлены ниже.

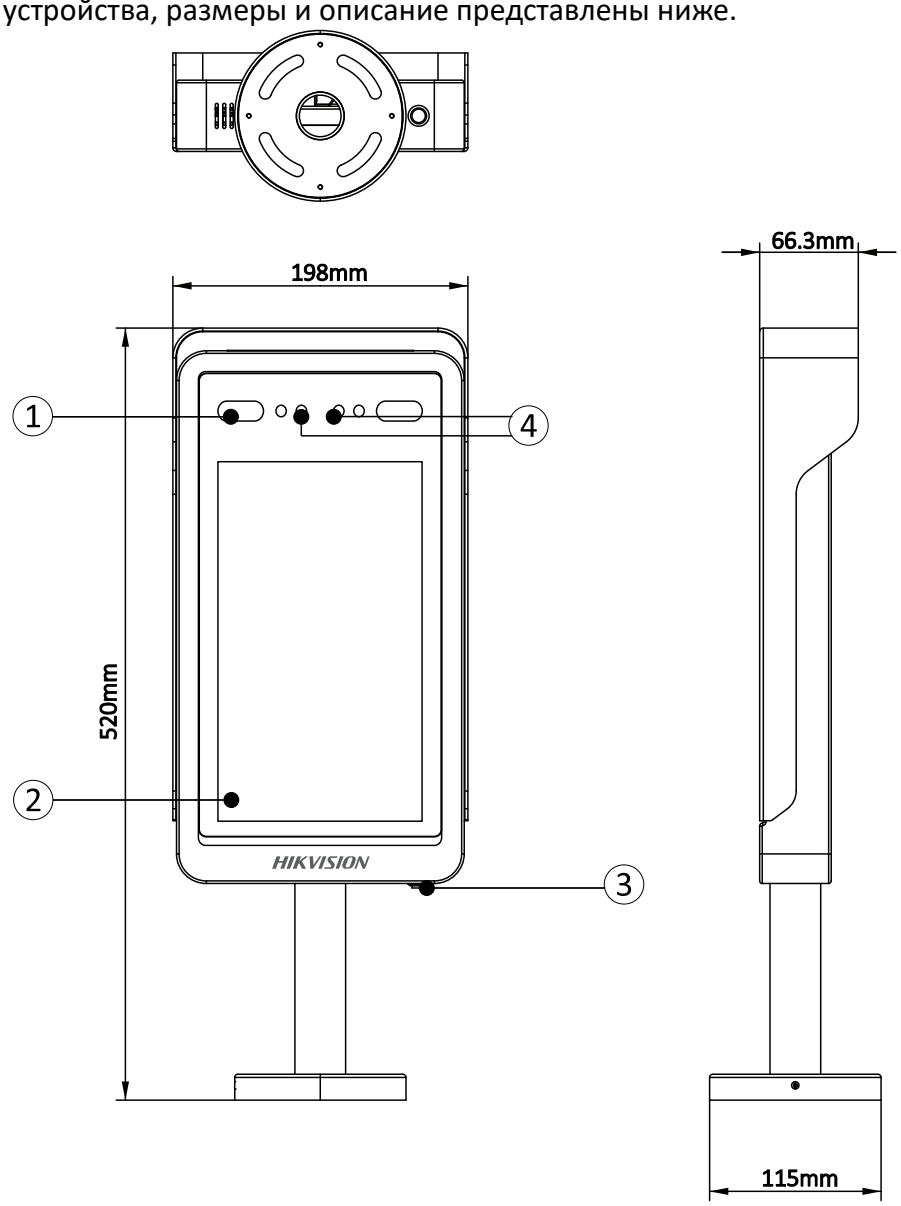


Таблица 2-1 Описание терминала распознавания лиц

№	Описание
1	Вспомогательная подсветка
2	Экран
3	Кнопка питания
4	Камеры

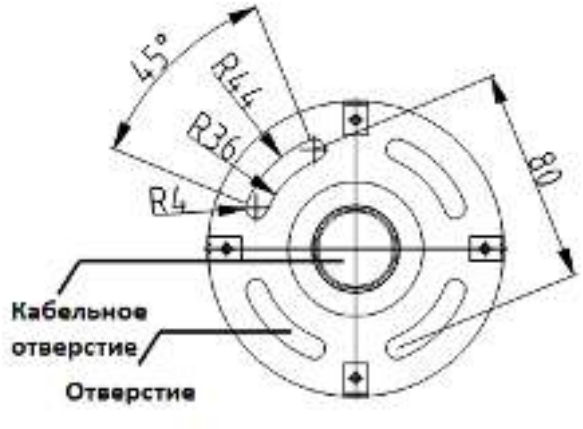
Глава 3 Установка

Условия установки:

- Избегайте задней засветки и прямых солнечных лучей.
- При установке на открытом воздухе установите солнцезащитный экран над устройством.
- Устройство должно быть установлено на пьедестале перед заграждением (дверью).

Перед началом:

- Просверлите отверстия в верхней панели пьедестала в соответствии со схемой, представленной на рисунке ниже.
- Убедитесь в наличии закрепленной водонепроницаемой гайки под верхней панелью.

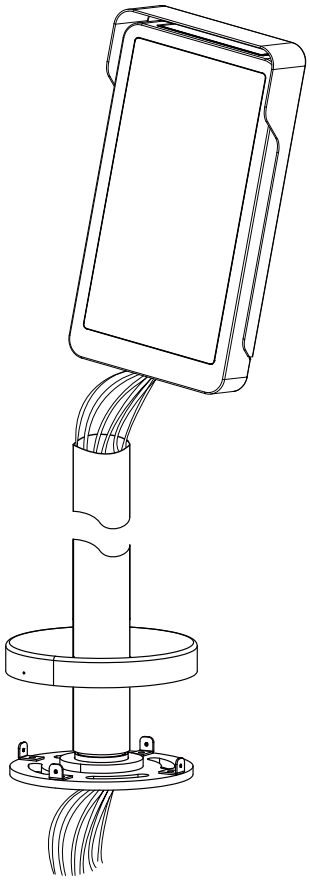


Примечания:

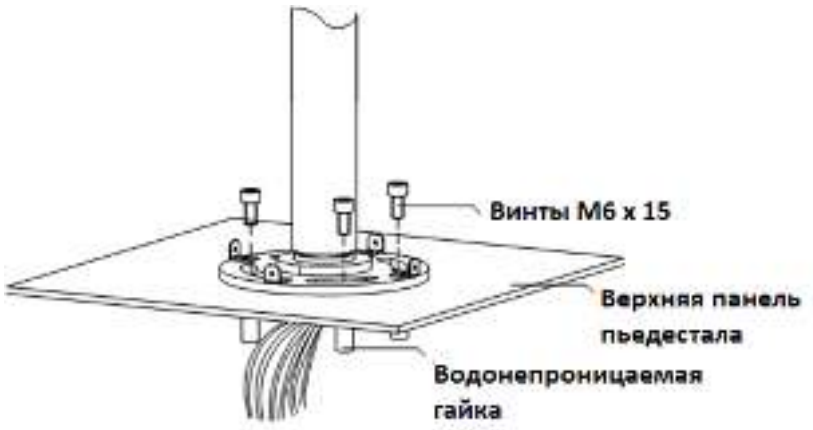
- ПОДХОДИТ ДЛЯ МОНТАЖА НА БЕТОННОЙ ПОВЕРХНОСТИ ИЛИ НА ДРУГОЙ НЕВОСПЛАМЕНЯЮЩЕЙСЯ ПОВЕРХНОСТИ.
- Модель водонепроницаемой гайки - BS-M6-1.

Шаги:

1. Проложите кабели через трубу сверху вниз, а затем проложите их через отверстия для кабелей в верхней панели пьедестала перед заграждением.

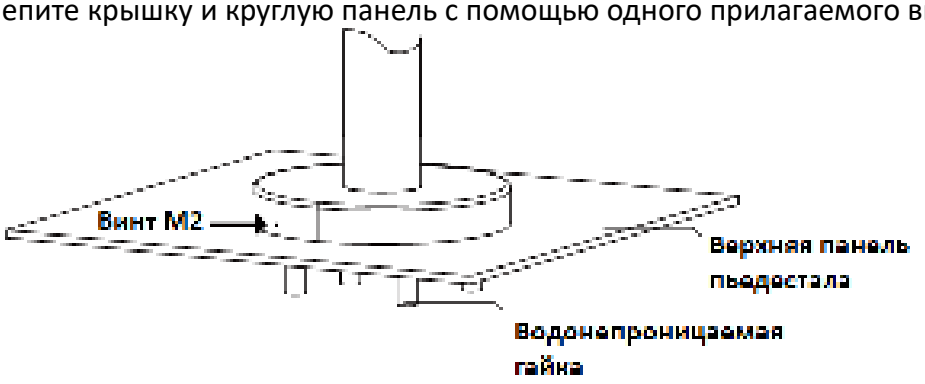


2. Проложите кабель с клеммами в пьедестале перед заграждением.
3. Приподнимите трубу и убедитесь, что труба и верхняя панель пьедестала расположены вертикально.
4. Закрепите шестигранные винты.
   1) Поверните трубу и выровняйте четыре отверстия на круглой панели с отверстиями на верхней панели пьедестала.
   2) Ввинтите прилагаемые четыре винта M6 × 15 в четыре отверстия. (Не затягивайте.)
   3) Немного поверните трубу и убедитесь, что экран устройства повернут в правильном направлении.
   4) Затяните четыре винта, чтобы зафиксировать устройство на пьедестале перед заграждением.



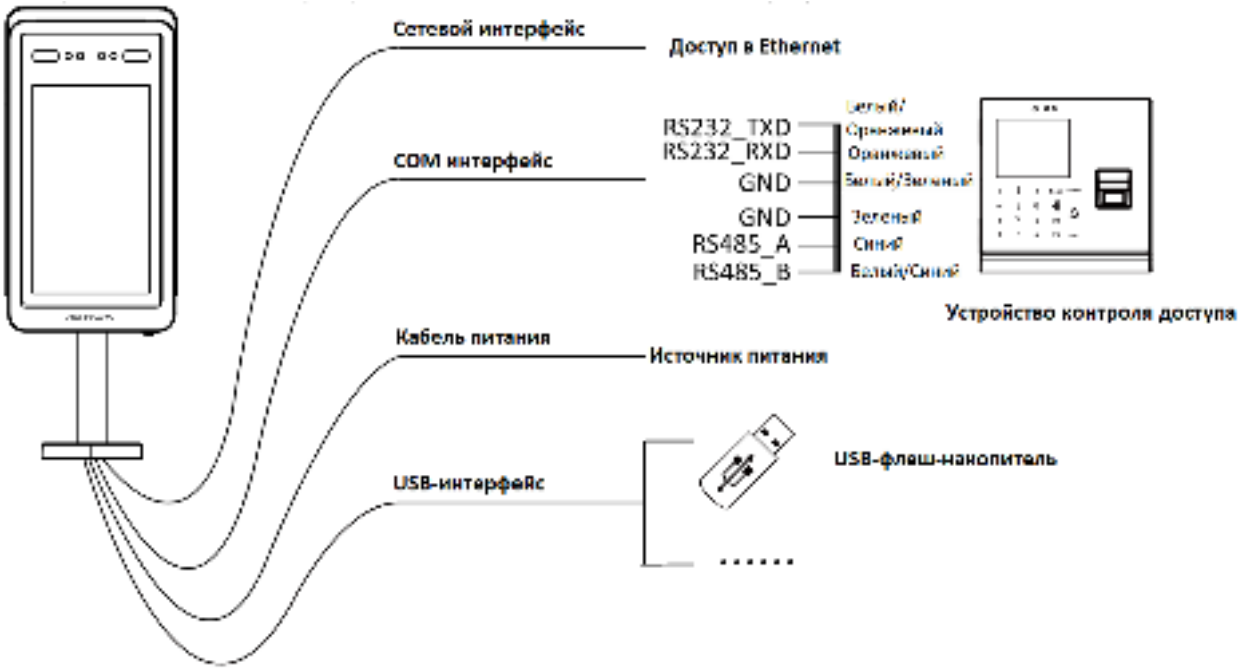
5. Установите крышку на круглую панель.

1) Переместите крышку на круглую панель, закрепленную на пьедестале.
2) Поверните крышку и скройте отверстие на крышке, выровняйте отверстие с помощью одной из четырех небольших меток на круглой панели.
3) Закрепите крышку и круглую панель с помощью одного прилагаемого винта M2.



Глава 4 Подключение

На приведенном ниже рисунке описывается подключение устройства.



Глава 5 Активация устройства

Цель:

Вам необходимо активировать устройство перед его использованием.

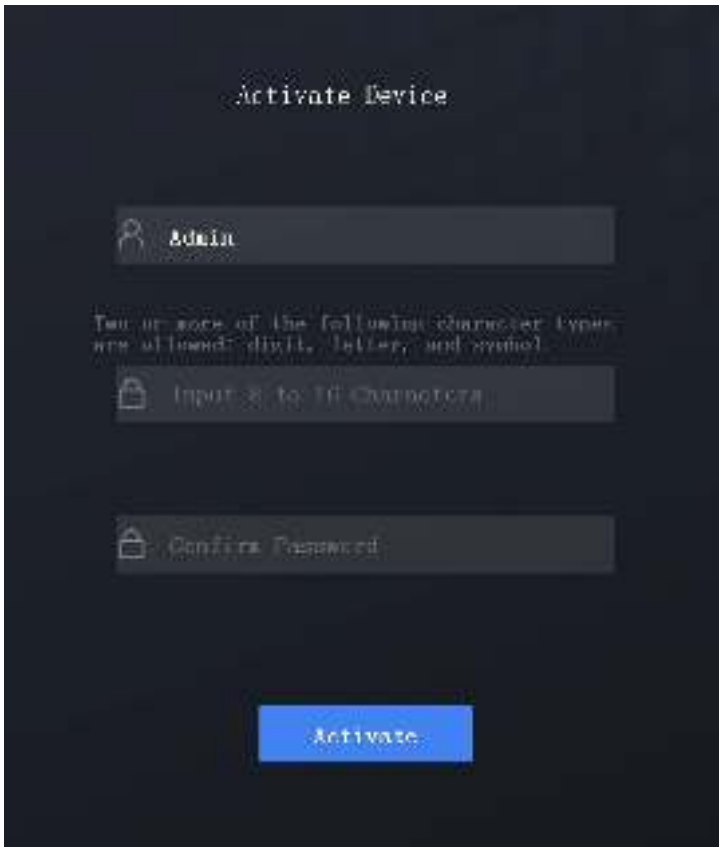
Поддерживается активация через само устройство, активация при помощи ПО SADP и при помощи клиентского ПО.

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. Создайте пароль для учетной записи *Admin*.
2. Подтвердите пароль.
3. Нажмите **Activate** («Активировать»).

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

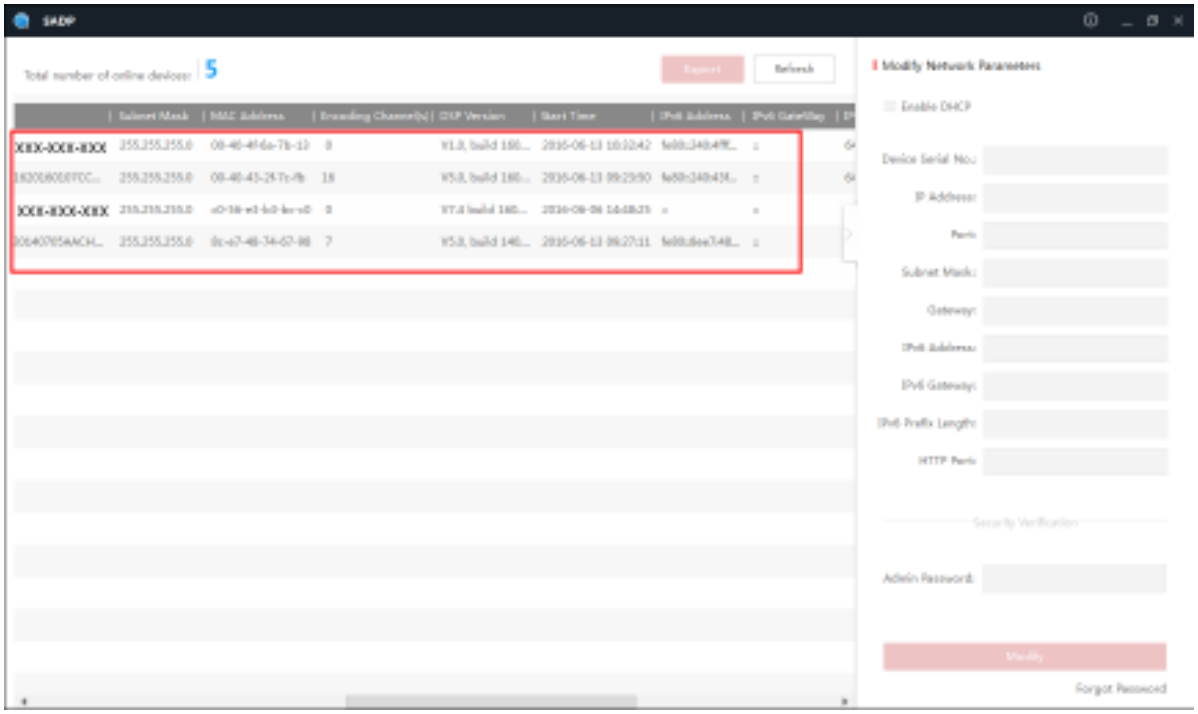
Цель:

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

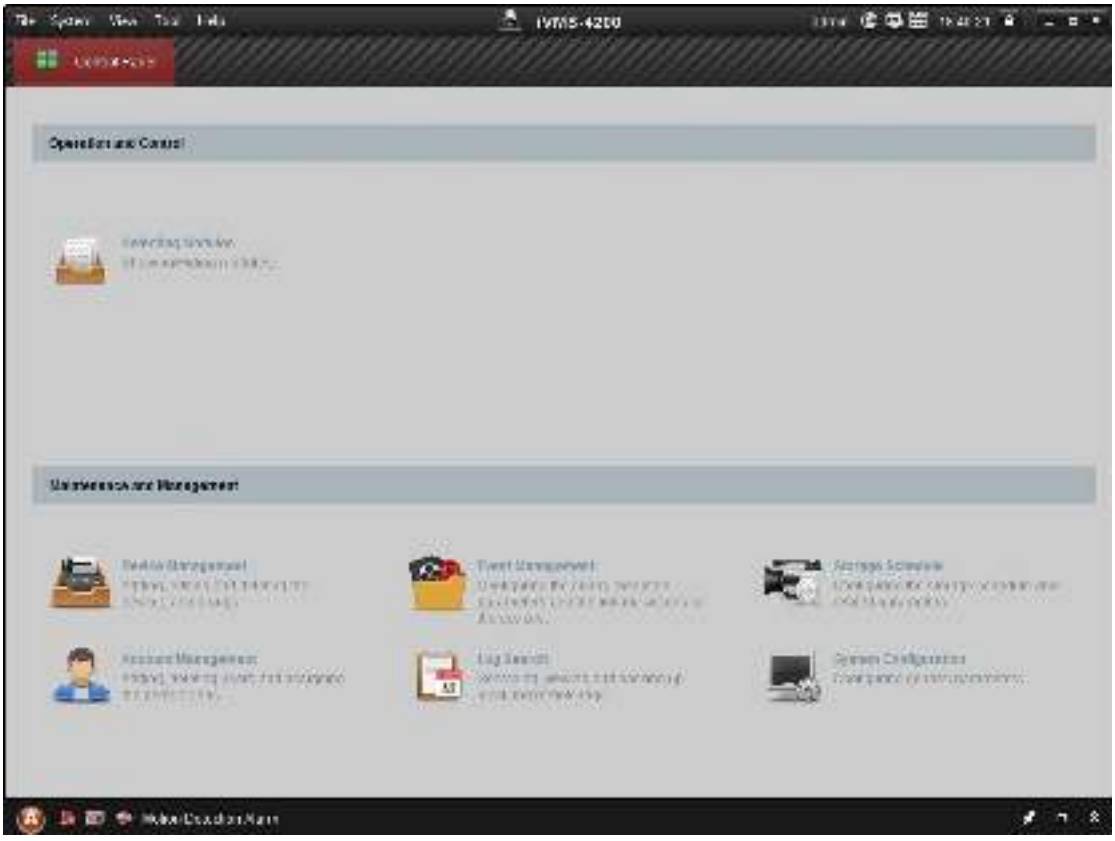
Цель:

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

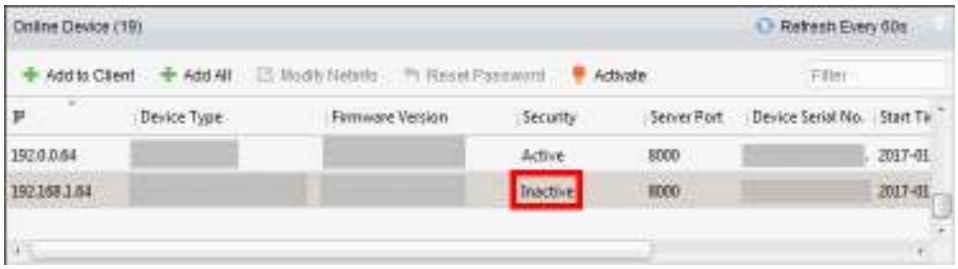
Получите клиентское программное обеспечение с прилагаемого диска или на официальном сайте и установите программное обеспечение в соответствии с подсказками. Выполните следующие действия для активации устройства.

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 административную аппаратную часть вы сможете управлять пользователями, устанавливать параметры связи, изменять пароль устройства, управлять и поддерживать данные и просматривать информацию об устройстве.

6.1 Вход в административную аппаратную часть

Цель:

Вы должны пойти в административную аппаратную часть перед настройкой других параметров.

Шаги:

1. На начальной странице нажмите экран на 3 секунды, чтобы перейти на страницу ввода пароля.
2. Введите пароль в текстовое поле. Пароль здесь относится к паролю активации.
3. Нажмите **OK** для входа в аппаратную часть.
4. (Опционально) Нажмите **Exit** («Выход») в нижнем левом углу для выхода из аппаратной части.

6.2 Настройки связи

Цель:

Вы можете установить сетевые параметры устройства и параметры COM.

6.2.1 Настройка сетевых параметров

Цель:

Устройство имеет два сетевых интерфейса. Вы можете выбрать включить ли один из них или включить оба, и установить сетевые параметры, включая IP-адрес, шлюз и маску подсети. Устройство может использовать сетевой интерфейс для связи с клиентом управления iVMS-4200.

Шаги:

1. В аппаратной части нажмите  для перехода на страницу настроек связи.
2. Нажмите **Network** («Сеть») для перехода на соответствующую вкладку.

3. Задайте параметры сетевого интерфейса, включая **IP address** («IP-адрес»), **subnet mask** («маску подсети») и **gateway** («шлюз»).

   Примечания:

   - IP-адрес устройства и IP-адрес ПК должны находиться в одной и той же LAN.
   - При одновременном использовании обоих сетевых интерфейсов IP-адреса сетевого интерфейса 1 и сетевого интерфейса 2 должны отличаться, чтобы избежать конфликта IP-адресов.
4. Нажмите **Logout** («Выход из системы») для выхода со страницы и сохранения параметров.

6.2.2 Настройка COM параметров

Цель:

Устройство может быть подключено к другому устройству контроля доступа через COM интерфейс. После выбора скорости передачи данных вы можете подключить устройство к другим устройствам контроля доступа по протоколу RS-232 или по протоколу RS-485. Подробнее о привязке устройства смотрите в *Разделе 6.11 Привязка устройства контроля доступа*.

Шаги:

1. Нажмите **COM** на странице **Communication Settings** («Настройки связи») для перехода на соответствующую вкладку.
2. Выберите скорость передачи в бодах для RS-232 протокола и для RS-485 протокола. Параметры вступят в силу сразу после их выбора.

6.3 Настройки системы

Цель:

На странице настроек системы вы можете настроить параметры ID устройства, уровень безопасности отпечатков пальцев, громкость голоса, разрешение экрана, режим аутентификации устройства, сканирование QR-кода, режим аутентификации с проверкой по «черному списку», детекцию реальности лица, режим энергосбережения, устройство считывания ID карт и автоматическую регулировку яркости подсветки.

Шаги:

1. В аппаратной части нажмите  для перехода на страницу системных настроек.

2. Задайте параметры.

   Описание параметров представлено ниже:

Название параметра	**Описание**
Device ID («ID устройства»)	Установите ID устройства для управления устройством. Когда устройство подключено к периферийному устройству (контроллеру доступа) по протоколу RS-485, ID устройства - это адрес DIP-переключателя протокола RS-485. ***Примечание:*** ID устройства должен быть числом от 1 до 255.
Voice Volume («Громкость голоса»)	Регулировка громкости аудио подсказок.

Blacklist Matching Threshold («Порог соответствия «черному списку»»)	Установите порог соответствия «черному списку» при сравнении пользователя с пользователями в «черном списке». Чем выше значение, тем ниже вероятность ложного распознавания. Чем выше значение, тем выше частота ложных отказов.
Device Authentication Mode («Режим аутентификации устройства»)	Вы можете выбрать режим аутентификации. **Auto** («Авто»): Аутентификация с помощью изображения лица, или изображения лица и карты. При аутентификации, если карта не была проведена, устройство запускает только 1: N аутентификацию. Если вы произвели проводку картой, устройство начнет 1:1 аутентификацию в соответствии с изображением лица на карте. **Face Picture** («Изображение лица»): Аутентификация только с помощью изображения лица. **Card + Face Picture** («Карта + Изображение лица»): Аутентификация с помощью изображения лица и карты ***Примечание:*** Если вам нужен более высокий уровень безопасности, не используйте один режим аутентификации.
QR Code Scanning («Сканирование QR-кода»)	Включение или выключение функции сканирования QR-кода. Если функция включена, камера устройства может отсканировать QR-код для аутентификации вместо считывания проводки карты. ***Примечания:*** ● По умолчанию функция отключена. ● Вы можете получить QR-код от клиента управления iVMS-4200. Для получения подробной информации об операции, смотрите руководство пользователя клиента управления iVMS-4200.
Blacklist Authentication Mode («Режим проверки по «черному списку»»)	Включение или отключение функции. Если функция включена, вы должны применить «черный список» при помощи Клиента управления iVMS-4200 перед работой. После аутентификации система будет определять, находится ли пользователь в «черном списке» или нет. ***Примечания:*** ● По умолчанию функция отключена. ● Для получения подробной информации об операции, смотрите руководство пользователя клиента управления iVMS-4200.

Live Face Detection («Детекция реальности лица»)	Включение или отключение функции. Если функция включена, устройство может понять, является ли пользователь реальным или нет.
Power Saving Mode («Режим энергосбережения»)	Включение или отключение функции. Если включено, питание устройства будет переведено в энергосберегающий режим.
ID Card Reader («Считыватель ID карт»)	Если устройство подключено к внешнему считывателю ID карт, вам следует выбрать модель считывателя ID карт. Если нет, выберите значение **None** («Нет»). ***Примечания:*** ● Вы должны подключить считыватель ID карт к USB-интерфейсу устройства, если вы хотите подключить внешний считыватель ID карт. ● Доступные модели считывателей ID карт: DS-K1F1110-A и DS-K1F1110-AB.
Supplement IR Light Brightness («Яркость вспомогательной ИК-подсветки»)	Установите яркость ИК-подсветки. «0» обозначает, что ИК-подсветка отключена.
Supplement White Light Brightness («Яркость белой вспомогательной подсветки»)	Установите яркость белой подсветки. «0» означает, что белая вспомогательная подсветка выключена.

3. Нажмите **Logout** («Выйти из системы») для сохранения настроек.

6.4 Управление пользователями

Цель:

Добавление информации пользователей вручную для аутентификации. Вы можете добавить имя пользователя, № карты и изображение лица. Вы также можете просматривать, искать и изменять добавленных пользователей.

6.4.1 Добавление пользователей

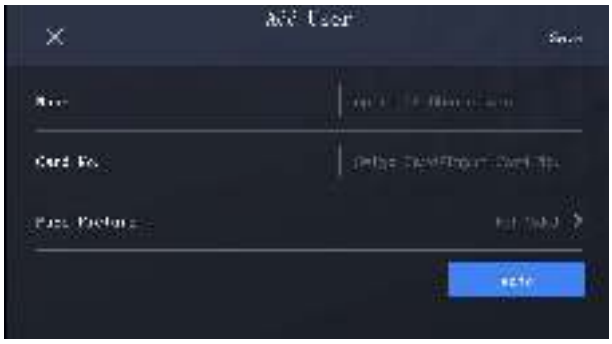
Цель:

Вы можете провести ID картой для добавления пользователя автоматически или вручную ввести информацию пользователя для его добавления в систему.

Добавление вручную

Шаги:

1. В аппаратной части нажмите  для перехода на страницу **User Management** («Управление пользователями»).
2. Нажмите **Add User** («Добавить пользователя») для перехода на страницу добавления пользователей.



3. Нажмите на текстовое поле **Name** («Имя») и введите имя пользователя.
   Введите имя пользователя с помощью всплывающей экранной клавиатуры.
4. Нажмите на текстовое поле **Card No.** («№ карты») и введите номер карты.
   Или вы можете провести картой через считыватель карт для получения номера карты.
   Примечание: В номере карточки допускается до 20 цифр или букв.
5. Добавьте изображение лица.
   1) Нажмите **Not Added** («Не добавлено») в правой части строки **Face Picture** («Изображение лица») для перехода на страницу добавления изображения лица.
   2) Поместите лицо перед камерой устройства.
      Убедитесь, что лицо находится в синей рамке на этой странице и дождитесь распознавания устройством.
      После успешного добавления изображения лица будет показано уведомление **“Saved”** («Сохранено»).
   3) Нажмите **Save** («Сохранить») для сохранения параметров и возврата на страницу добавления пользователей.
      Или подождите 3 секунды, и система автоматически вернется к странице добавления пользователей.
   4) (Опционально) Нажмите **Try Again** («Попробовать снова») для удаления сохраненного изображения лица и добавления нового изображения лица.
      Примечание: Для получения подробной информации о добавлении изображения лица, смотрите *Приложение B Советы по сбору/сравнению изображений лиц* .
6. Нажмите **Save** («Сохранить») для сохранения параметров.
   Добавленный пользователь отобразится в списке пользователей.

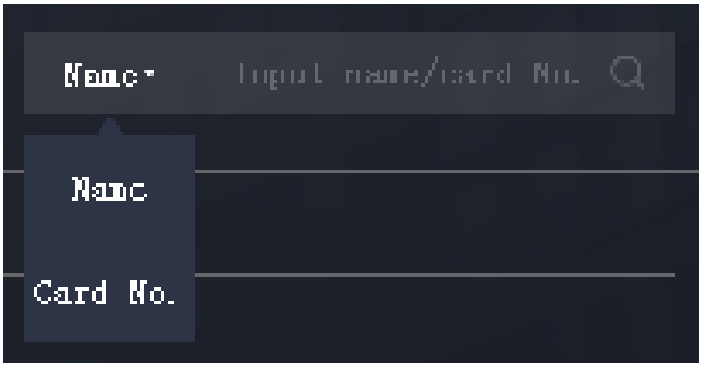
6.4.2 Поиск пользователей

Цель:

Когда в список пользователей добавлено слишком много пользователей, вы можете выполнить поиск по имени пользователя или номеру его карты.

Шаги:

1. На странице управления пользователями нажмите **Name** («Имя») или **Card No.** («№ карты») в правом верхнем углу страницы для выбора типа поиска.



2. Введите **user name** («имя пользователя») или **card No.** («№ карты») для поиска.
3. Нажмите для начала поиска.
   Результат будет отображен в списке пользователей.

6.4.3 Редактирование пользователей

Цель:

Вы можете изменить информацию добавленных пользователей при помощи следующих шагов.

Шаги:

1. На странице управления пользователями нажмите на пользователя, информацию которого вы хотите изменить, чтобы перейти на страницу редактирования пользователя.
2. Смотрите *Раздел 6.4.1 Добавление пользователей* для редактирования информации пользователя.
3. Нажмите **Save** («Сохранить») для сохранения параметров и возврата на страницу управления пользователями.

6.5 Настройка параметров изображения лица

Цель:

Вы можете установить параметры изображения лица для распознавания лица. Параметры включают в себя: **1:N Matching Threshold** («Порог соответствия 1:N»), **1:1 Matching Threshold** («Порог соответствия 1:1»), **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 **Score** («Оценка»).

Шаги:

1. В аппаратной части нажмите для перехода на страницу настройки изображения лица.

2. Задайте параметры изображения лица.

   Описание параметров представлено ниже:

Параметр	**Описание**
1:N Matching Threshold («Порог соответствия 1:N»)	Установите порог соответствия изображения лица при аутентификации в режиме **1:N Matching** («Соответствие 1:N»)
1:1 Matching Threshold («Порог соответствия 1:1»)	Установите порог соответствия изображения лица при аутентификации в режиме **1:1 matching** («Соответствие 1:1»).
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

Параметр	Описание
	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
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.

Параметр	Описание
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.
Score («Оценка»)	Установка оценки для изображения лица при распознавании. Устройство будет оценивать захваченное изображение в соответствии с углом наклона, углом поворота и межзрачковым расстоянием. Если оценка больше заданного значения, распознавание лица не удалось.

3. Нажмите **Logout** («Выйти из системы») для сохранения настроек и выхода из меню.

6.6 Изменение пароля

Цель:

Вы можете изменить пароль устройства (пароль активации).

Шаги:

1. В аппаратной части нажмите  для перехода на страницу **Change Password** («Изменение пароля»).

2. Введите **old password** («старый пароль»), **new password** («новый пароль») и **confirm** («подтверждение»).
3. Нажмите **Save** («Сохранить») для сохранения настроек.

<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.*

6.7 Управление данными

Цель:

Вы можете экспортировать добавленные изображения лиц и события аутентификации из системы. Вы также можете импортировать информацию о лицах в пакетном режиме в систему.

Шаги:

1. Подключите USB-накопитель к устройству.
2. В аппаратной части нажмите для перехода на страницу **Data Management** («Управление данными»).

3. Нажмите **Export Face Pic.** («Экспорт изобр. лица»), **Export Event** («Экспорт события») или **Import Face Pic.** («Импорт изобр. лица») для экспорта изображений лиц и событий на USB-накопитель, импорта изображений лиц с USB-накопителя соответственно.

   Примечания:

   - Формат имени импортированного изображения лица:
     Card No._Name_Department_Employee ID_Gender
     («Номер карты_Имя_Отдел_ID сотрудника_Пол»)
   - Импортированное изображение лица должно содержать фронтальное изображение лица пользователя в формате JPEG или JPG. Разрешение изображения лица должно быть 640 × 480 или более. Размер изображения должен быть от 60 до 200 КБ.
   - Импортируемый и экспортируемый файл должен быть Excel-файлом.

6.8 Обслуживание системы

Цель:

Вы можете сбросить систему до настроек по умолчанию или заводских настроек. Вы также можете обновить систему.

6.8.1 Восстановление параметров устройства

Цель:

Вы можете восстановить параметры устройства до значений по умолчанию или до заводских значений.

Шаги:

1. В аппаратной части нажмите  для перехода на страницу **System Maintenance** («Обслуживание системы»).

2. Нажмите **Restore to Default** («Восстановить настройки по умолчанию») или **Restore to Factory** («Восстановить заводские настройки»).

   Restore to Default («Восстановить настройки по умолчанию»): Все параметры будут восстановлены до параметров по умолчанию, кроме IP-адреса устройства.

   Restore to Factory («Восстановить заводские настройки»): Все параметры будут удалены. При следующем запуске устройства необходимо будет активировать его.

6.8.2 Обновление прошивки

Цель:

Если доступна новая версия или текущая версия не является последней, вы можете обновить прошивку устройства через USB-интерфейс.

Шаги:

1. Подключите USB-накопитель к USB-интерфейсу к устройству.

Примечание: Убедитесь, что на USB-накопителе находится файл обновления. Имя файла обновления должно быть *digicap.dav.*

2. В аппаратной части нажмите  для перехода на страницу **System Maintenance** («Обслуживание системы»).
3. Нажмите **Upgrade Firmware** («Обновить прошивку»).
   Устройство автоматически прочитает файл обновления на USB-накопителе и начнет обновление.
   Примечание: файл обновления должен находиться в корневом каталоге.

6.9 Просмотр информации устройства

В аппаратной части нажмите  , и вы сможете увидеть имя устройства, версию ПО и версию прошивки.

6.10 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: Если вам нужен более высокий уровень безопасности, не используйте один режим 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 или ID картой выполняется сравнение захваченного изображения лица или считанного отпечатка пальца с информацией, хранящейся на карте (или ID карте).

Перед началом:

Вы должны настроить режим аутентификации терминала. Для получения подробной информации смотрите *Раздел 6.3 Настройки системы*

6.10.1 Аутентификация при помощи Соответствия 1:1

Шаги:

1. Если в качестве режима аутентификации выбрано **Card + Face Picture** («Карта +

Изображение лица») или **Auto** («Авто»), то проведите картой в области считывания карт.

Примечание: Карта может быть обычной IC картой, зашифрованной картой или ID картой. Если функция сканирования QR-кода включена, вы можете поместить QR-код перед камерой устройства для аутентификации с помощью QR-кода.

2. (Опционально) Если включена функция **Blacklist Authentication Mode** («Режим проверки по «черному списку»»), устройство будет сравнивать информацию аутентификации с «черным списком».

   Если пользователь находится в «черном списке», на вспомогательном экране появится подсказка об исключении личности, и устройство отправит сигнал «черного списка» в центр управления.

   Примечания:

   - Для получения информации о включении функции **Blacklist Authentication Mode** («Режим проверки по «черному списку»») смотрите *Раздел 6.3 Настройки системы.*
   - Вы можете подключить внешний HDMI экран в качестве вспомогательного экрана.
3. Если в качестве режима аутентификации выбрано **Card + Face Picture** («Карта + Изображение лица») или **Auto** («Авто»), поместите лицо прямо перед камерой для начала аутентификации.

   Если аутентификация прошла успешно, появится уведомление “Authenticated” *(«Аутентифицировано»)*.

   Примечания:

   - Для лучшей аутентификации изображения лица высота пользователя должна составлять от 140 до 190 см, а расстояние между пользователем и устройством должно составлять от 30 см до 100 см.
   - Для получения подробной информации об аутентификации изображения лица смотрите *Приложение B Советы по сбору/сравнению изображений лиц.*

6.10.2 Аутентификация при помощи Соответствия 1:N

Если в качестве режима аутентификации выбрано **Card + Face Picture** («Карта + Изображение лица») или **Auto** («Авто»), поместите лицо прямо перед камерой для начала аутентификации. Если аутентификация прошла успешно, появится уведомление “Authenticated” *(«Аутентифицировано»)*.

6.11 Привязка устройства контроля доступа

Цель:

Терминал распознавания лиц может подключаться к устройству контроля доступа через протокол RS-232 и передавать информацию аутентификации на устройство контроля доступа одновременно.

Устройство контроля доступа может управлять состоянием двери в соответствии с результатом аутентификации и режимом аутентификации устройства контроля доступа и передавать события двери клиенту управления или другим системам.

Перед началом:

- Убедитесь, что устройство контроля доступа подключено к терминалу распознавания лиц по протоколу RS-232.
- Убедитесь, что терминал распознавания лиц и устройство контроля доступа включены.

Шаги:

1. Установите скорость передачи данных для протокола RS-232 на вкладке COM.
   Примечание: Скорость передачи данных в бодах терминала распознавания лиц по протоколу RS-232 должна быть такой же, как и у устройства контроля доступа. Для получения подробной информации о настройке скорости передачи данных в бодах протокола RS-232 смотрите *Раздел 6.2.2 Настройка COM параметров.*
2. Аутентифицируйтесь при помощи терминала распознавания лиц.
   Терминал распознавания лиц отправит результат аутентификации и номер карты на устройство контроля доступа. Устройство контроля доступа будет контролировать состояние двери в соответствии с результатом. И он также отправит связанные события в клиент или в другие системы.
   Примечание: Подробнее о режиме аутентификации устройства контроля доступа смотрите в руководстве пользователя соответствующего устройства контроля доступа.

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

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

Шаги:

1. Введите **user name** («имя пользователя») и **password** («пароль»), которые вы зарегистрировали.
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

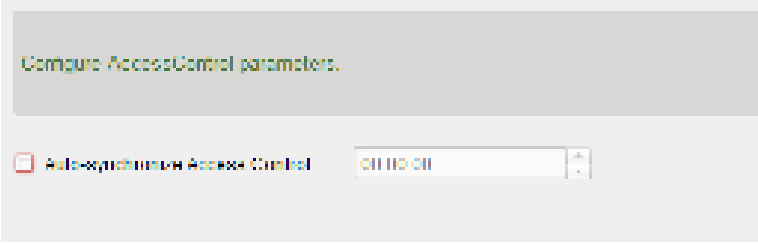
Цель:

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,

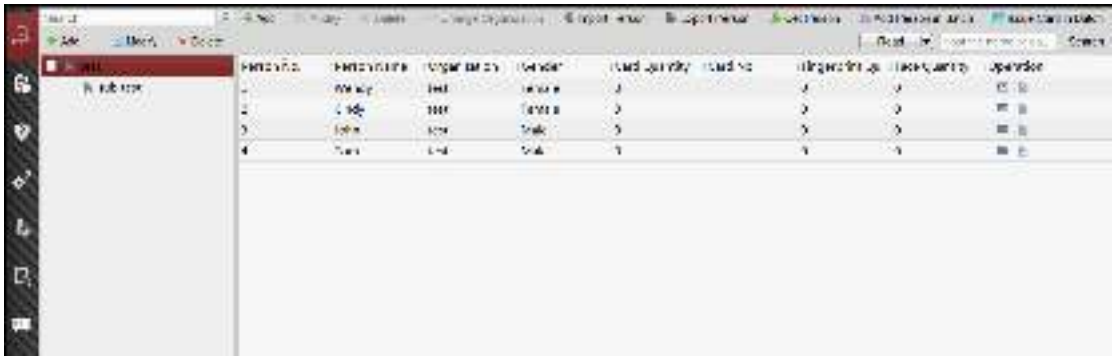
конфигурацию разрешений, управление статусом контроля доступа, видеодомофонию и другие расширенные функции.

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.

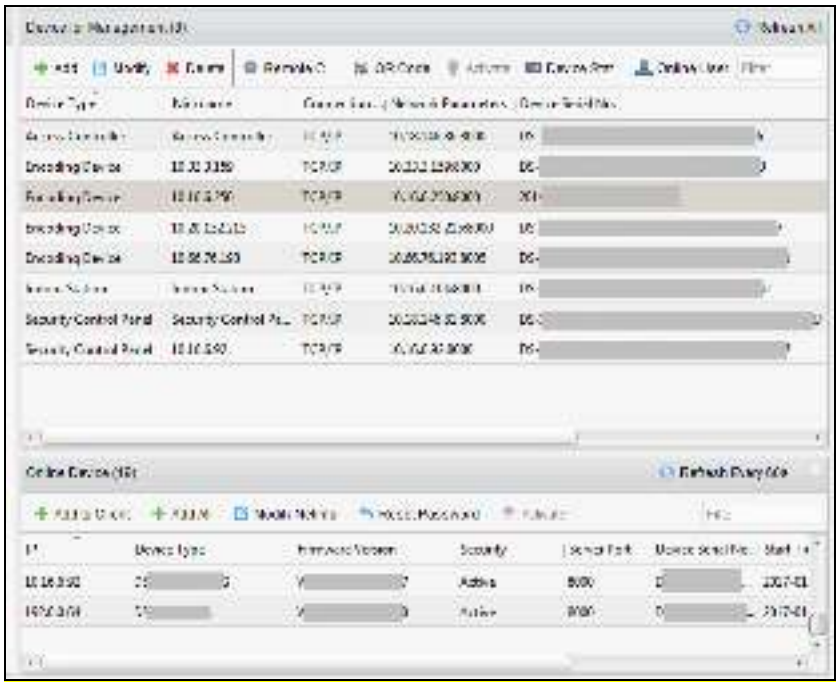
Non-residence («Нерезидент»): Вы можете установить правило посещаемости при добавлении человека, задав параметры контроля доступа.

Residence («Резидент»): 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 7.12 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 сплывающего окна.

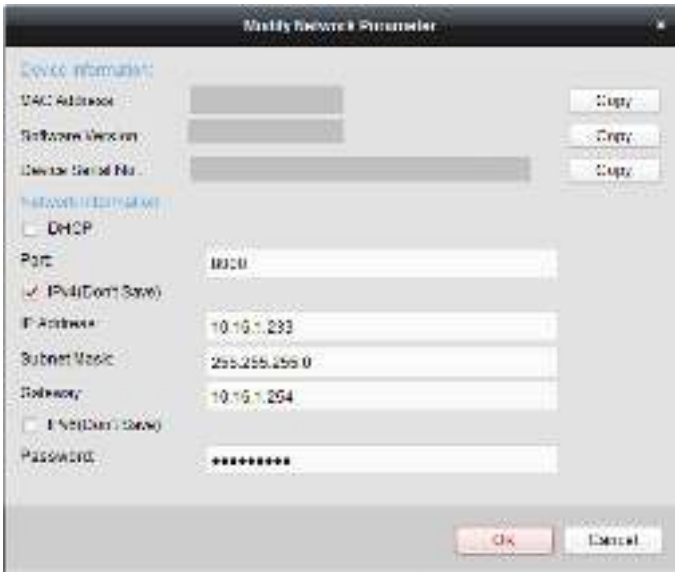
   2) Создайте **verification code** («проверочный код»).
   3) Подтвердите проверочный код в поле **Confirm verification code** («Подтверждение проверочного кода»).
   4) Нажмите **Terms of Service** («Условия предоставления услуг») и **Privacy Policy** («Политика конфиденциальности») для ознакомления 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 5.*
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.

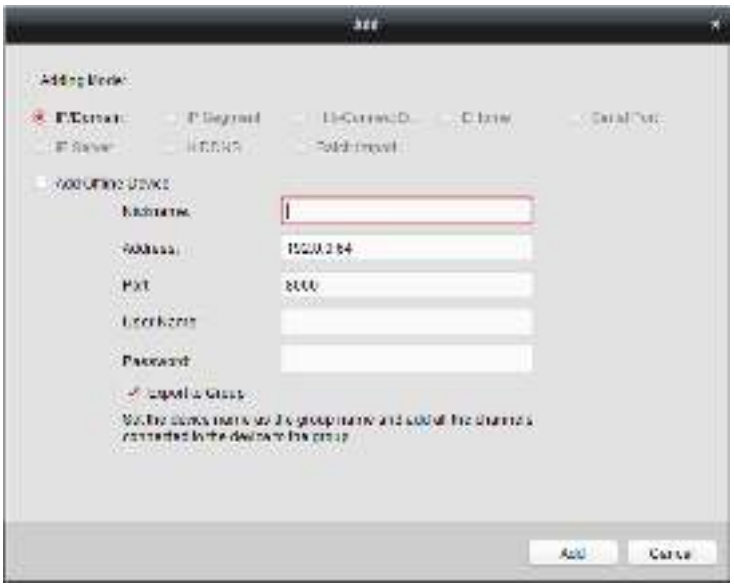
   Все каналы устройства будут импортированы в соответствующую группу по умолчанию.

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

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

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

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



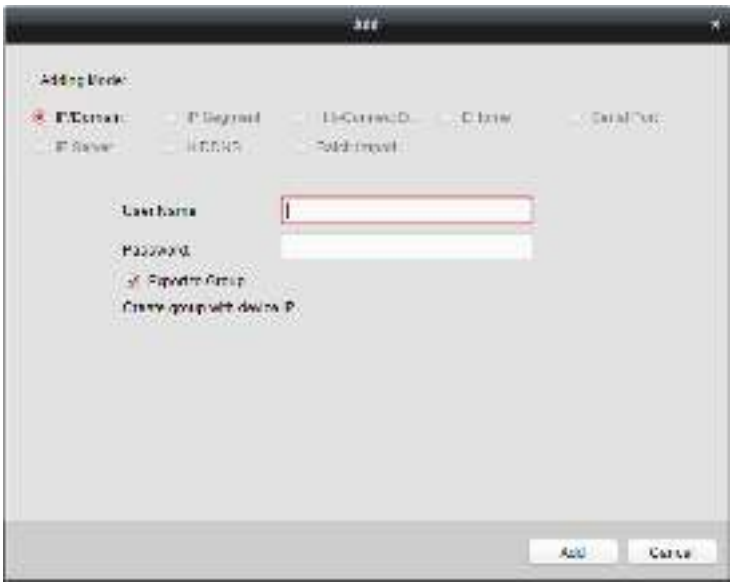
➢ Добавление нескольких онлайн устройств

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. 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 устройств.

<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.

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 оффлайн устройств.

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

   Когда устройство из оффлайн 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.

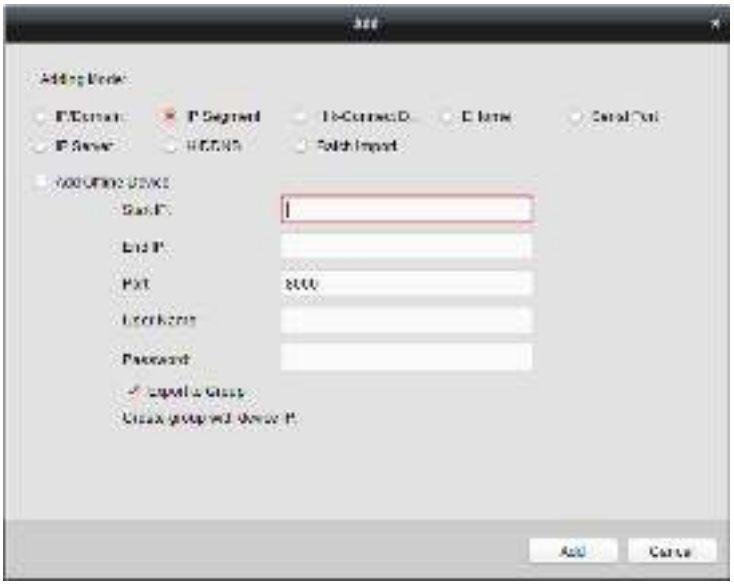
   Примечание: iVMS-4200 так же предоставляет метод добавления оффлайн устройств.

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

   Когда устройство из оффлайн 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 утройств 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 **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.

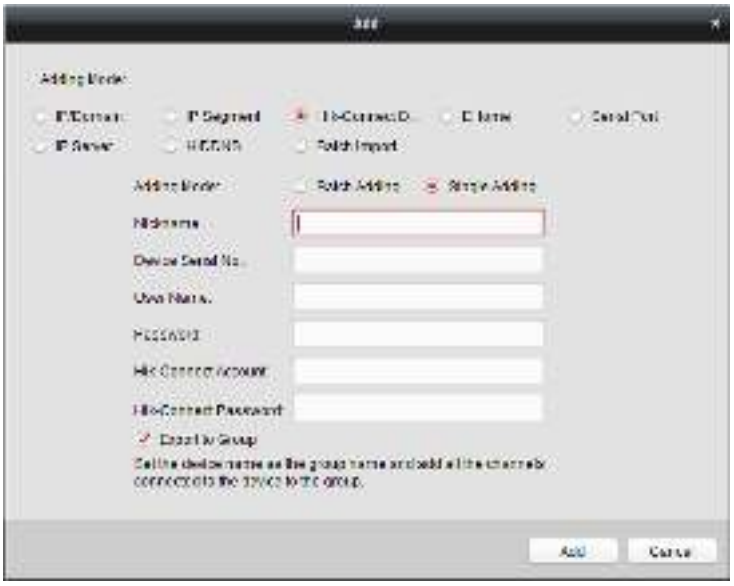
   

   РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ – *Настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля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

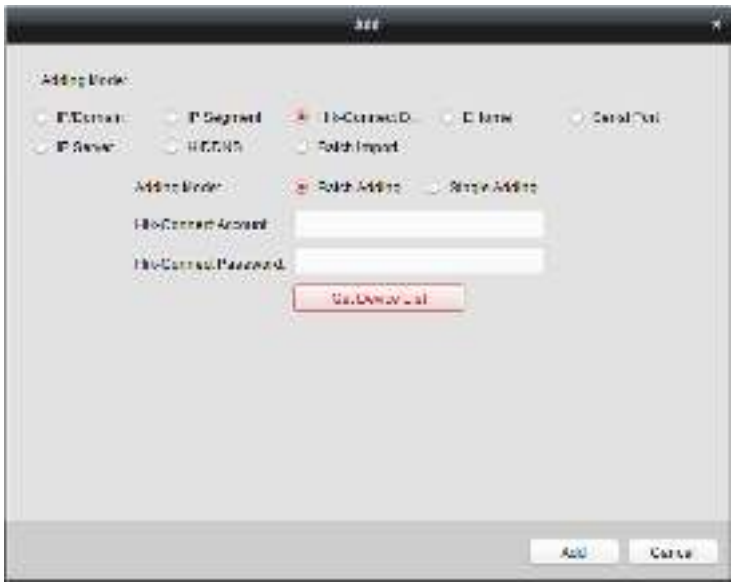
   Все каналы устройства будут импортированы в соответствующую группу по умолчанию.
6. Нажмите **Add** («Добавить»).



Пакетное добавление устройств

Шаги:

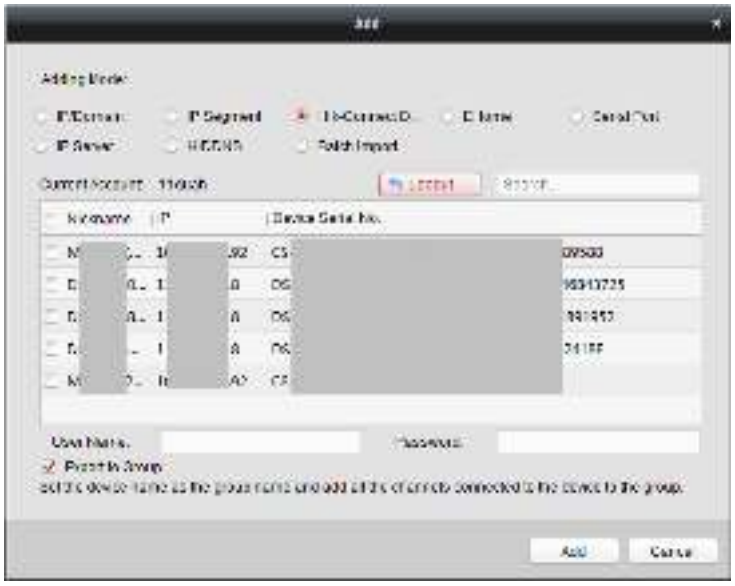
1. Нажмите **Add** («Добавить») для открытия диалогового окна добавления устройств.



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 оффлайн устройств.

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

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

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

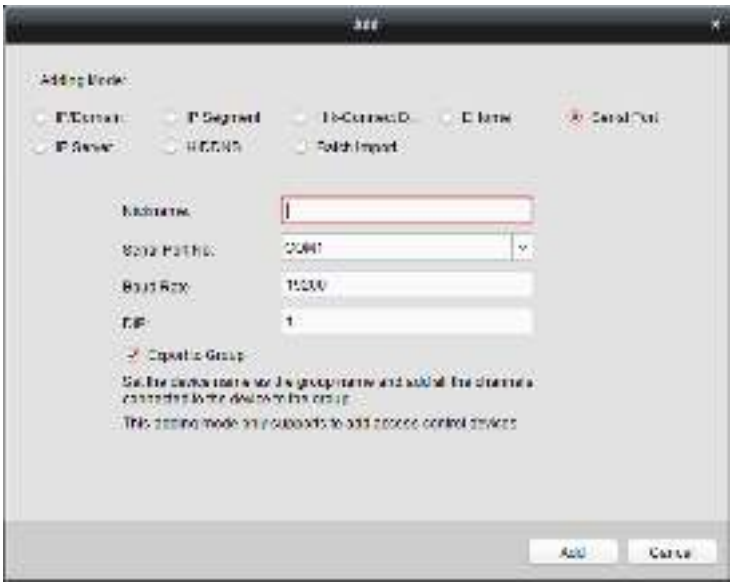
Добавление устройств при помощи последовательного порта

Цель:

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

Шаги:

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



3. Введите необходимую информацию.

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

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

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

   DIP: Введите DIP адрес устройства.

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

   Все каналы устройства будут импортированы в соответствующую группу по умолчанию.

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

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

   Когда устройство из оффлайн 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 оффлайн устройств.

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

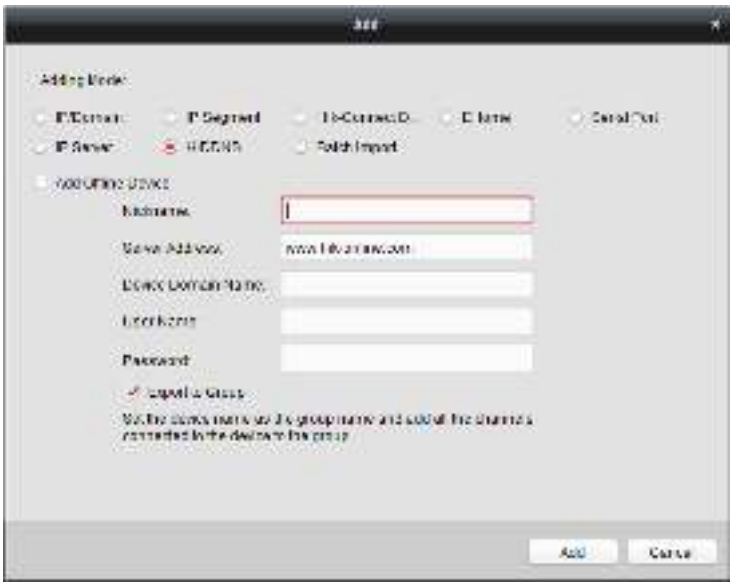
   Когда устройство из оффлайн режима перейдет в онлайн режим, программа подключится к нему автоматически.

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 оффлайн устройств.

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

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

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

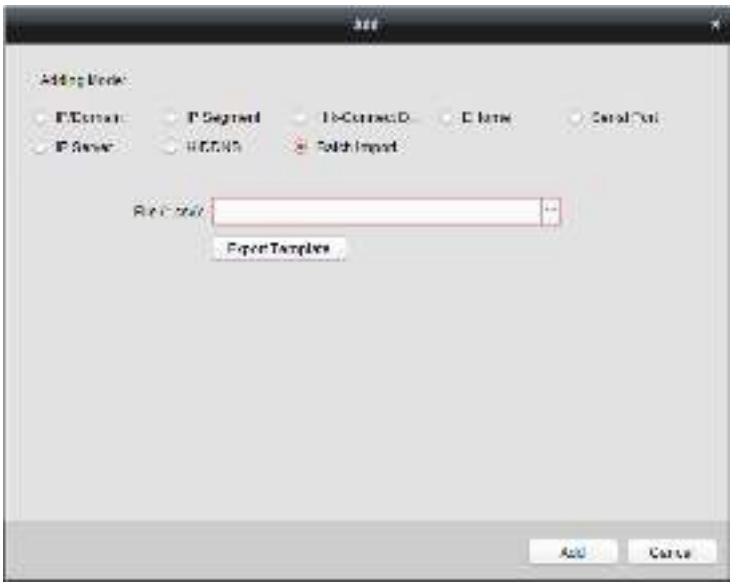
Импорт устройств в пакетном режиме

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 с 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 оффлайн устройство»): Вы можете поставить 1 для включения добавления оффлайн устройств, и затем программа будет автоматически подключаться к устройствам, 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 оффлайн устройство»), введите количество каналов устройства. Если вы установили 0 в поле **Add Offline Device** («Добавить оффлайн устройство»), заполнять это поле не нужно.
- **Alarm Input Number** («Количество тревожных входов»): Если вы установили 1 в поле **Add Offline Device** («Добавить оффлайн устройство»), введите количество тревожных входов устройства. Если вы установили 0 в поле **Add Offline Device** («Добавить оффлайн 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.

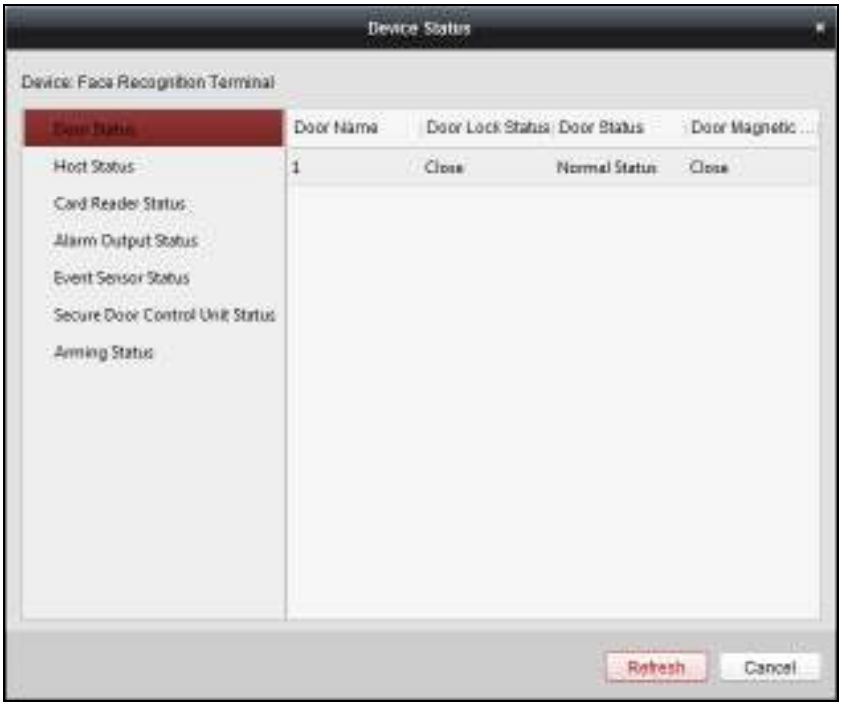
5. Нажмите … и выберите файл шаблона.
6. Нажмите **Add** («Добавить») для импорта устройств.

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 статуса устройства

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



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

- **Door Status** («Статус двери»): Статус подключенной двери.
- **Host Status** («Статус 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** («Статус считывателя карт»): Статус считывателя карт.

  Примечание: Если вы используете считыватель карт с соединением RS-485, вы можете просмотреть его статус - онлайн или оффлайн. Если вы используете считыватель карт с

соединением Wiegand, вы сможете увидеть оффлайн состояние.

- **Alarm Output Status** («Статус тревожного выхода»): Состояние тревожного выхода каждого порта.
- **Event Sensor Status** («Статус датчика событий»): Состояние датчика события каждого порта.
- **Secure Door Control Unit Status** («Статус Защитного блока управления дверью»): Онлайн статус и статус тамперинга Защитного блока управления дверью.
- **Arming Status** («Статус постановки на охрану»): Статус устройства.

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** 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 *Редактировании времени* в Разделе удаленной конфигурации. Для получения подробной информации смотрите пункт *Время* в *Разделе 7.3.8 Удаленная конфигурация*.

Настройки центра беспроводной связи

Шаги:

1. Нажмите вкладку **Wireless Communication Center** («Центр беспроводной связи»).

2. Выберите **APN name** («APN имя»): **CMNET** или **UNINET**.
3. Введите **SIM Card No** («№ сим-карты»).
4. Выберите группу центра из выпадающего списка.
5. Введите **IP address** («IP-адрес») и **port No** («№ порта»).
6. Выберите в поле **protocol type** («тип протокола») значение **EHome**. По умолчанию № порта для EHome - *7660*.
7. Задайте имя учетной записи для сетевого центра. Постоянная учетная запись должна использоваться на одной платформе.
8. 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:

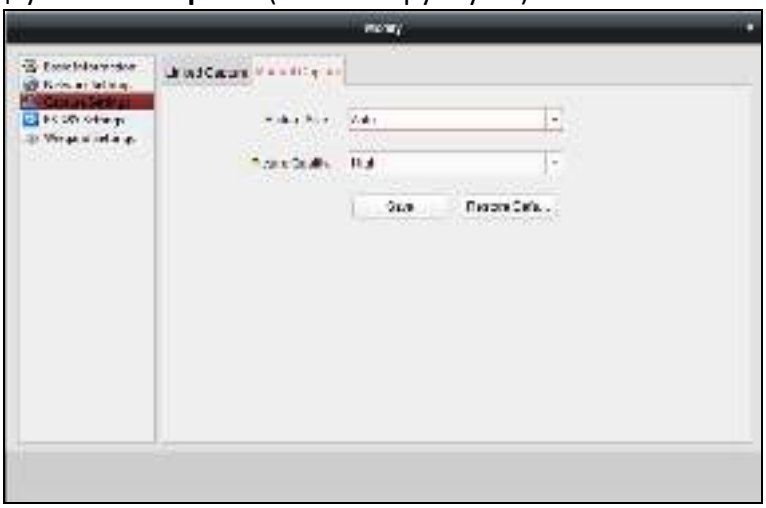
1. Выберите вкладку **Linked Capture** («Связанный захват»).

2. Установите **picture size** («размер изображения») и **quality** («качество»).
3. Установите **capture times** («число захватов») для одного срабатывания.
4. Установите **capture interval** («интервал захвата») в соответствии с числом захватов.
5. 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 Удаленная конфигурация

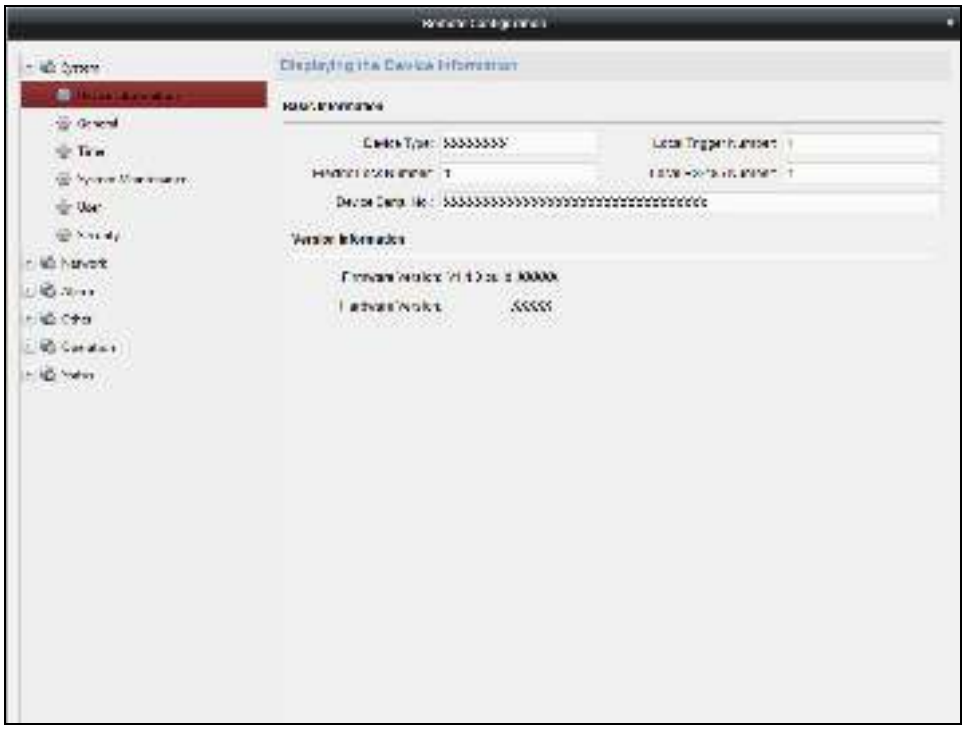
Цель:

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

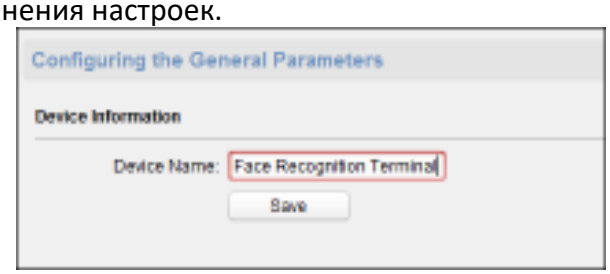
Шаги:

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

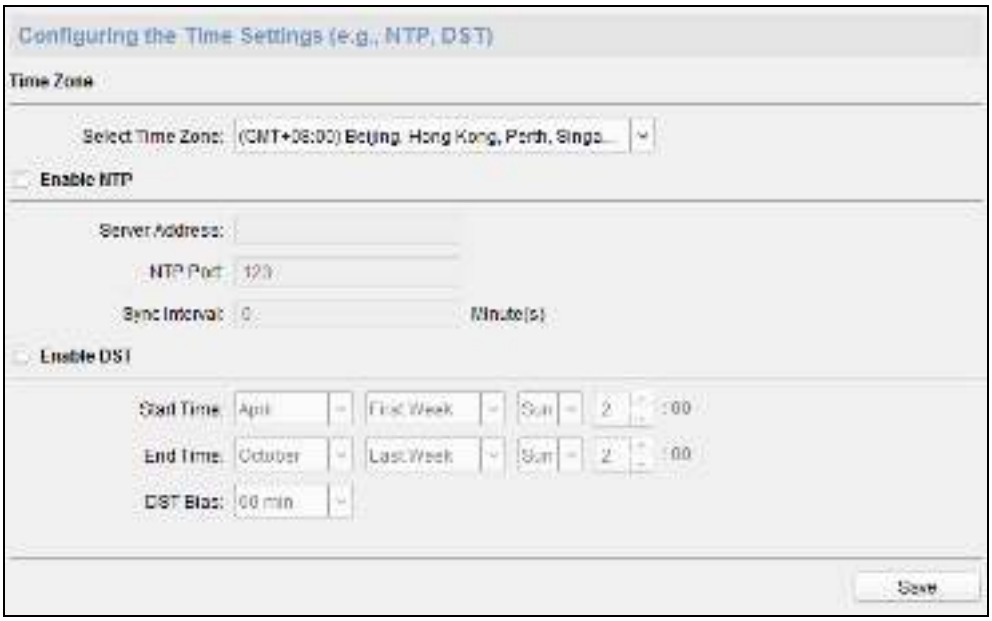
В меню удаленной конфигурации нажмите **System -> General** («Система -> Общие») для конфигурации имени устройства и перезаписи параметра файлов записи. Нажмите **Save** («Сохранить») для сохранения настроек.



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.



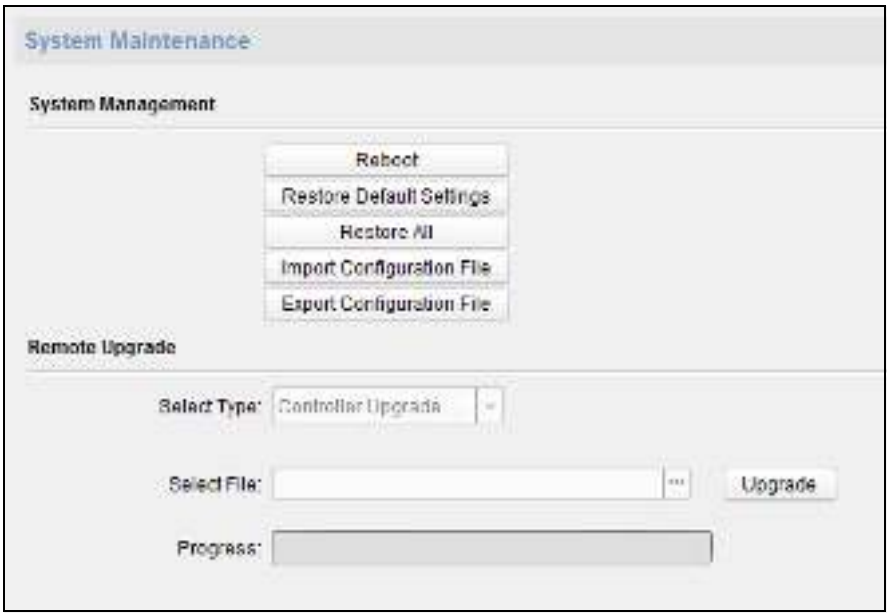
Настройка обслуживания системы

Цель:

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

Шаги:

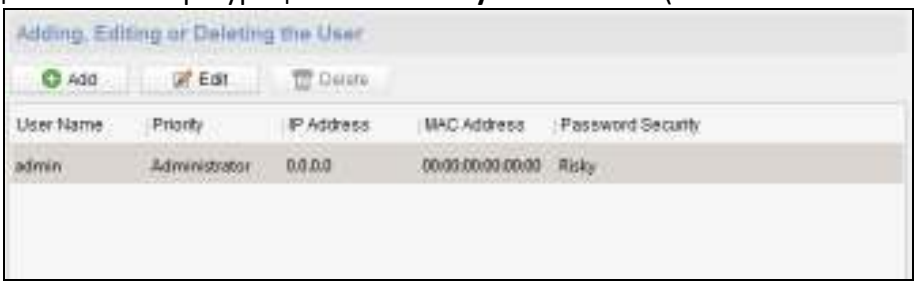
1. В меню удаленной конфигурации нажмите **System -> System Maintenance** («Система -> Обслуживание системы»).
2. Нажмите **Reboot** («Перезагрузить») для перезагрузки устройства.
   Или нажмите **Restore Default Settings** («Восстановить настройки по умолчанию») для восстановления настроек устройства 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.
   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») нажмите … для выбора файла обновления.
   2) Нажмите **Upgrade** («Обновить») для начала обновления.



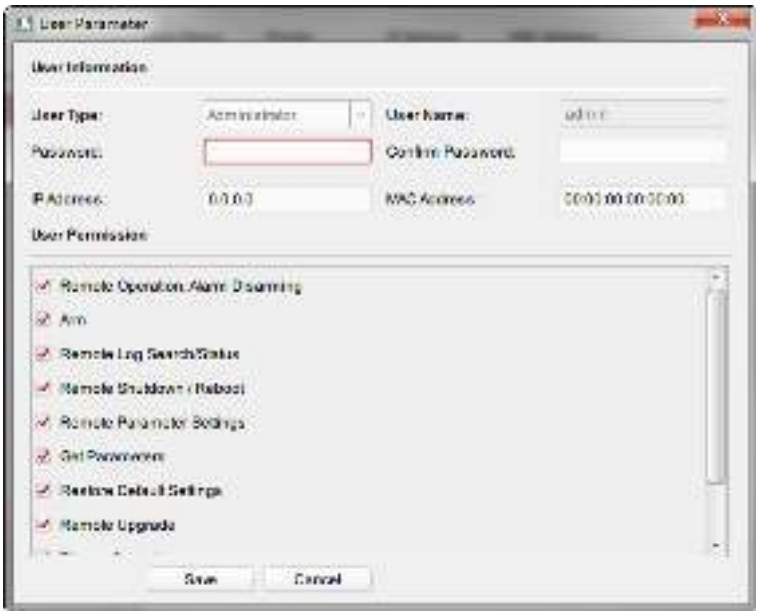
Управление пользователями

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

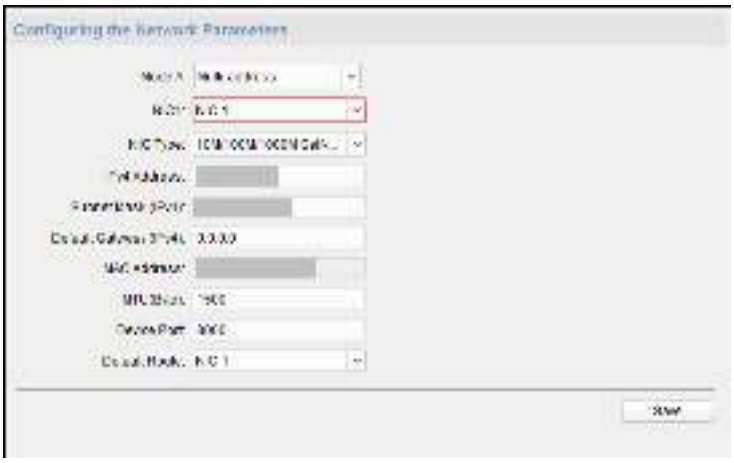
Шаги:

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

Конфигурация сетевых параметров

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



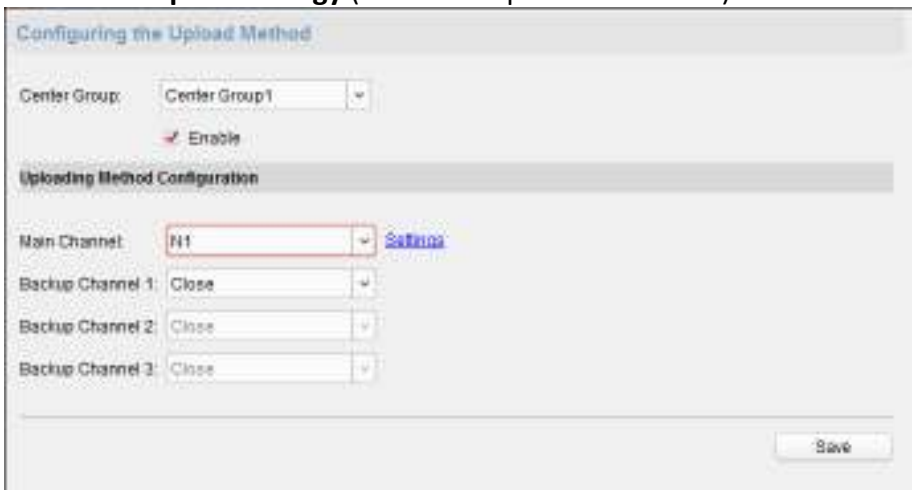
Настройка способа загрузки

Цель:

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

Шаги:

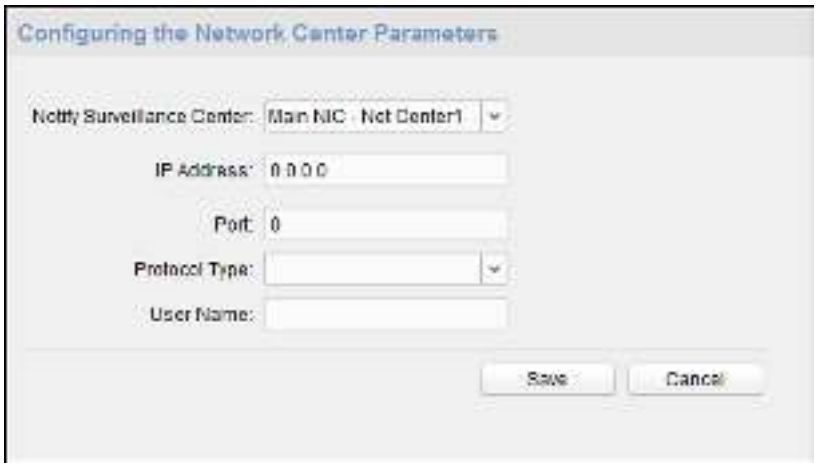
1. Нажмите **Network -> Report Strategy** («Сеть -> Стратегия отчета»).



2. Выберите группу центра из выпадающего списка.
3. Поставьте галочку **Enable** («Включить»).
4. Установите способ загрузки.
   Вы можете установить основной канал и резервный канал.
5. Нажмите **Settings** («Настройки») справа от поля выора канала для настройки подробной информации.
6. Нажмите **Save** («Сохранить») для сохранения настроек.

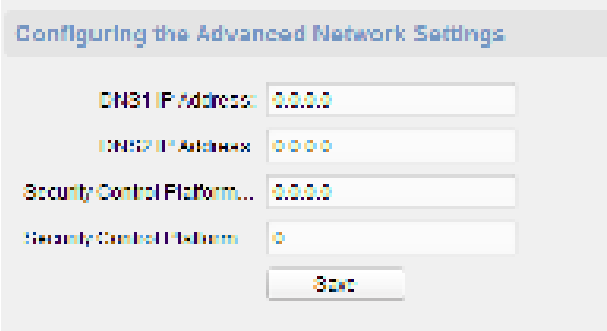
Конфигурация сетевого центра

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

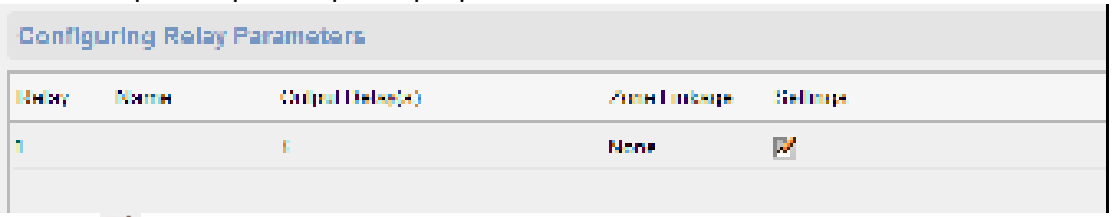
Нажмите **Network -> Advanced Settings** («Сеть -> Расширенные настройки»). Вы можете настроить **DNS IP address 1** («IP-адрес DNS 1»), **DNS IP address 2** («IP-адрес DNS 2»), **security control platform IP** («IP-адрес платформы управления безопасностью») и **security control platform port** («порт платформы управления безопасностью»). Нажмите **Save** («Сохранить») для сохранения настроек.



Конфигурация параметров реле

Шаги:

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

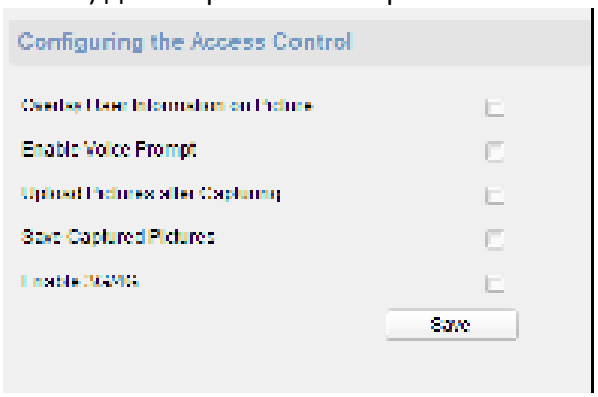


2. Нажмите  для появления всплывающего окна настройки параметров реле.
3. Настройте значения в полях **relay name** («имя реле») и **output delay** («задержка вывода»).
4. Нажмите **Save** («Сохранить») для сохранения параметров.
   Или нажмите **Copy to…** («Копировать в») для копирования информации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

Конфигурация параметров контроля доступа

Шаги:

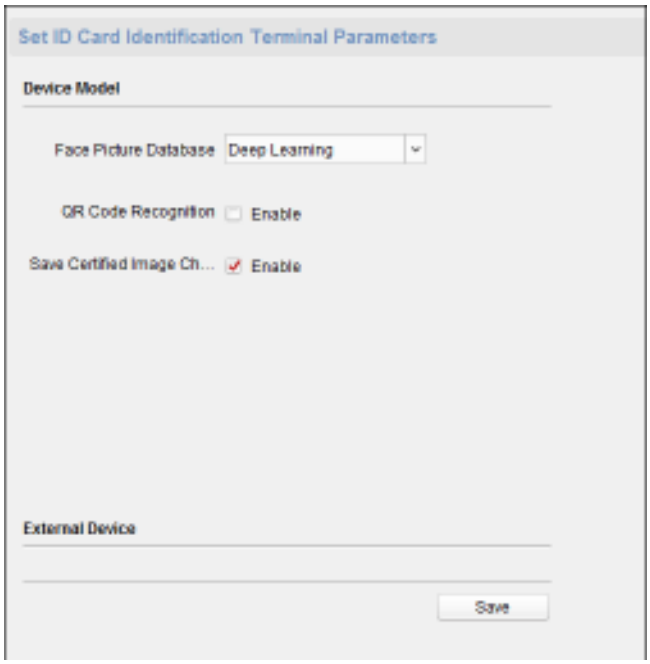
1. В меню удаленной конфигурации нажмите **Other -> Access Control Parameters** («Другие -> Параметры контроля доступа»).
2. Отметьте необходимые поля.
   - **Overlay User Information on Picture** («Наложение информации пользователя на изображение»): Отображение пользовательской информации на захваченных 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.
Authenticate by QR Code («Аутентификация по QR-коду»)	При включении функции камера устройства может сканировать QR-код для аутентификации. По умолчанию функция отключена.
Save Authenticating Face Picture («Сохранять изображение лица при аутентификации»)	При включении функции изображение захваченного лица при аутентификации будет сохранено на устройстве.

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

Параметр	Описание
	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. 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.

Параметр	Описание
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 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.
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. Если дополнительная подсветка находится в автоматическом режиме, 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 **supplement light mode** («режим вспомогательной подсветки») из выпадающего списка.
3. (Опционально) Если в поле **supplement light mode** («режим вспомогательной подсветки») установлено значение **Auto** («Авто»), вы можете установить яркость вспомогательной подсветки.
4. Нажмите **Save** («Сохранить») для сохранения настроек.

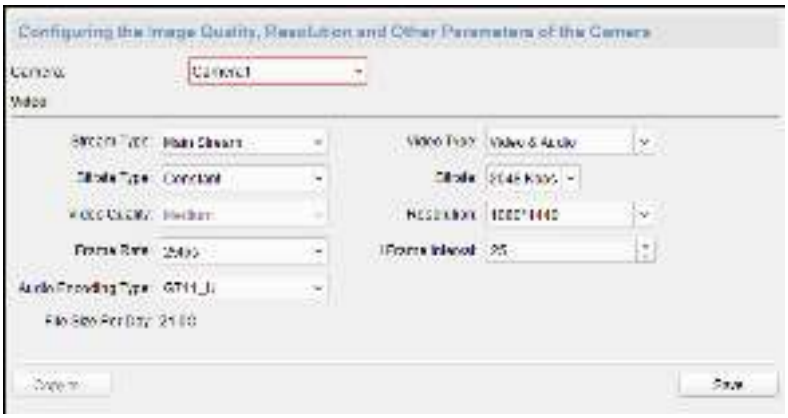
Конфигурация видео и аудио параметров

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.

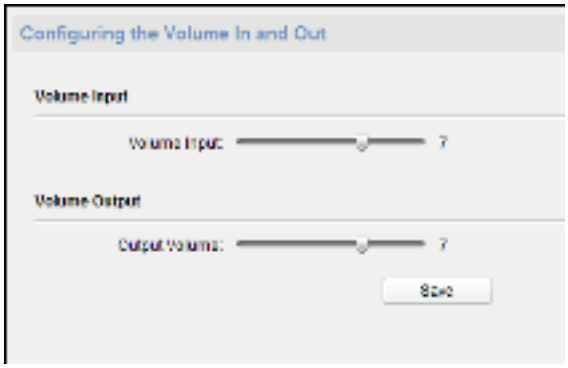


2. Задайте параметры камеры устройства, включая **stream type** («тип потока»), **bitrate type** («тип битрейта»), **video quality** («качество видео»), **frame rate** («частота кадров»), **audio encoding type** («тип кодирования аудио»), **video type** («видео тип»), **bitrate** («битрейт»), **resolution** («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 и выхода») для перехода на соответствующую страницу.



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

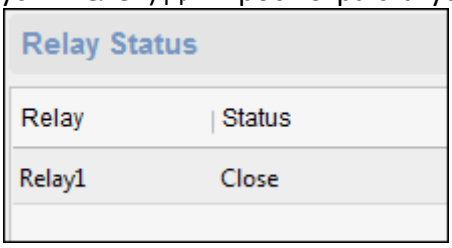
Управление реле

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 переходад в меню управления любьми 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 организаций.

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.

Примечаня:

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

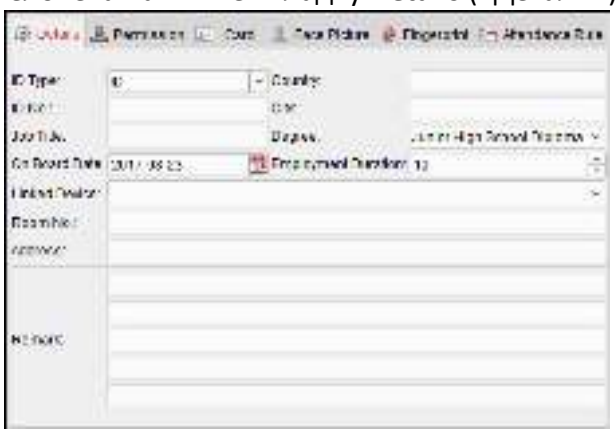
1. Выберите организацию в списке организаций и нажмите кнопку **Add** («Добавить») на панели **Person** («Человек») для появления всплывающего окна добавления людей.

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** («данные дня рождения») и **email**.
4. Нажмите **Upload Picture** («Зарузить 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 **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.

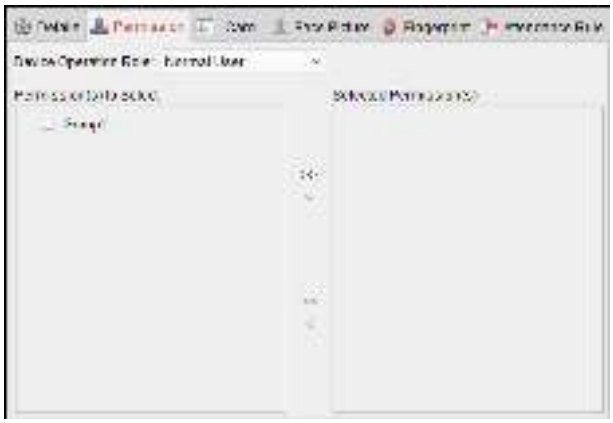
Добавление человека (Разрешения)

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

Примечание: Для получения подробной иноформации о разрешения конфитроля доступа смотрите *Раздел 6.7 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)

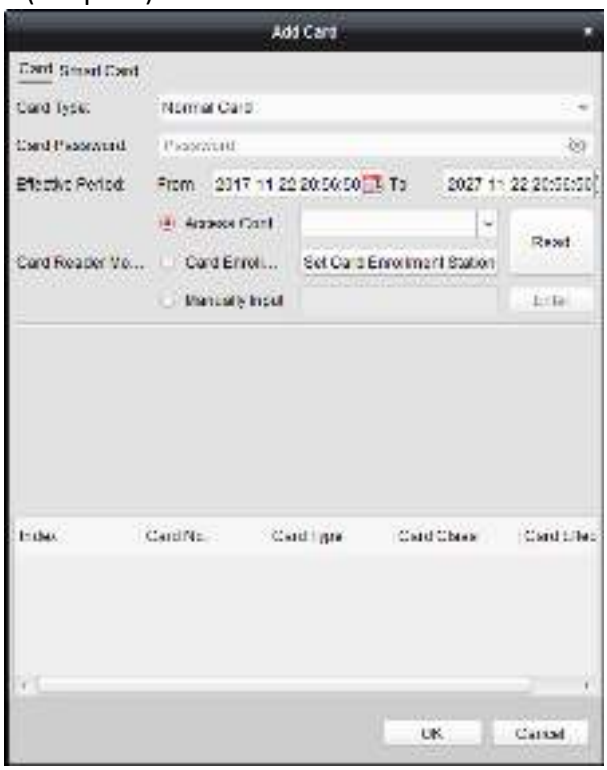
Вы можете добавлять карты и выдавать их людям.

➢ **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 людей с инвалидностью»): 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 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 аутентифкации считывателя карт как **Card and Password** («Карта и Пароль»), **Password and Fingerprint** («Пароль и Отпечаток пальца»), **Card** («Карта»), **Password** («Пароль») и **Fingerprint** («Отпечаток пальца»). Для получения подробной информации смотрите *Раздел 7.8.2 Аутентификация считывателя карт.*
6. Нажмите  для установки времени действия и истечения действия карты.
7. Выберите **Card Reader Mode** («Режим считывателя карт») для считывания номера карты.
   - **Access Controller Reader** («Считыватель карт контроллера доступа»): Поместите карту на считыватель контроллера доступа и нажмите **Read** («Считать») для получения номера карты.
   - **Card Enrollment Station** («Настольный считыватель карт»): Поместите карту на настольный считыватель карт и нажмите **Read** («Считать») для получения номера карты.

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

1) Выберите тип настольного считывателя карт.

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

2) Установите **serial port No.** («№ последовательного порта»), **baud rate** («скорость передачи в бодах»), **timeout value** («значение тайм-аута»), **buzzing** («звонок») и **card No. Type** («Тип номера карты»).

   Если карта является M1 картой и вам необходимо включить функцию шифрования M1 карт, вы должны поставить галочку **Enable** («Включить») напротив **M1 Card Encryption** («Шифрование карт») 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 внешего 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 людей с инвалидностью»): 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 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.

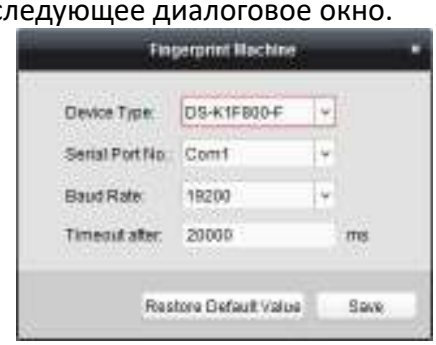
Добавление человека (Отпечатки пальцев)

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** («Нерезидент») в сцене приложения при первом запуске программного обеспечения.

Шаги:

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

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

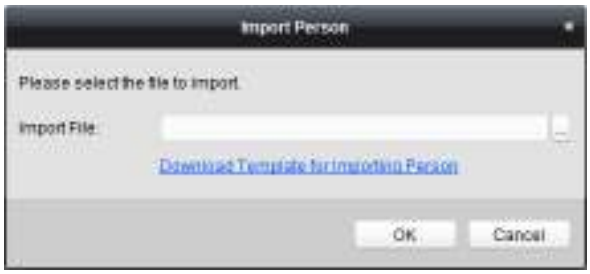
Импорт и экспорт информации человека

Информация человека может быть импортирована и экспортирована в пакетном режиме.

Шаги:

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

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



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

Получение информации о человеке с устройства контроля доступа

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

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

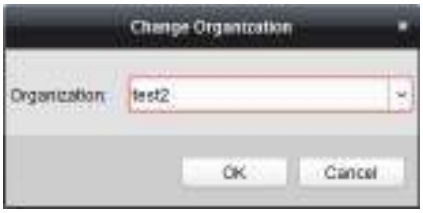
Изменение и удаление людей

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

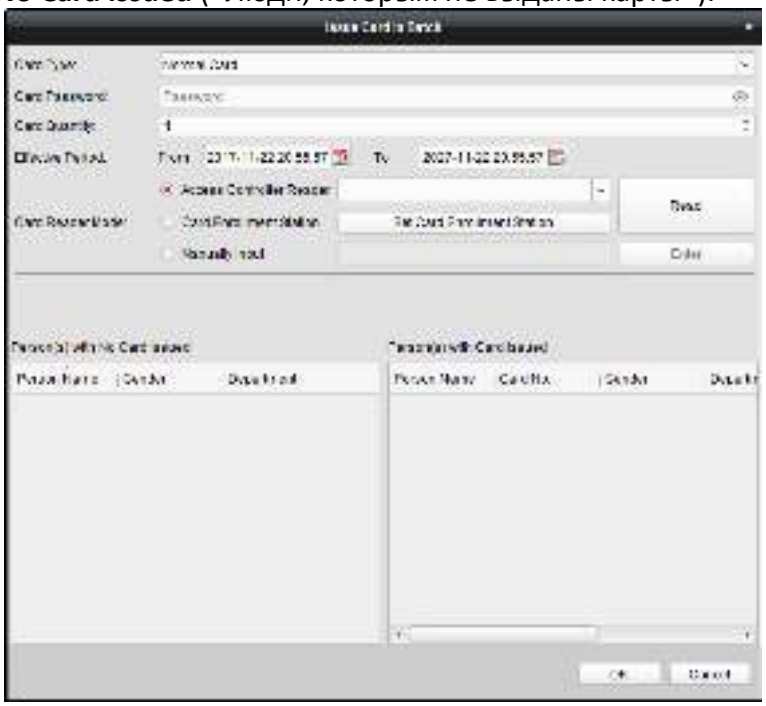
Вы можете ввести ключевое слово номера карты или имени человека в поле поиска, а затем нажать кнопку **Search** («Поиск») для поиска человека.
Вы можете ввести № карты, нажав кнопку **Read** («Считать») для получения номера карты при помощи подключенного настольного считывателя карт.
Вы можете нажать **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»). Для получения подробной информации смотрите *Раздел 7.8.2 Аутентификация считывателя карт.*
4. Введите количество карт, выданных для каждого человека.
   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») 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.

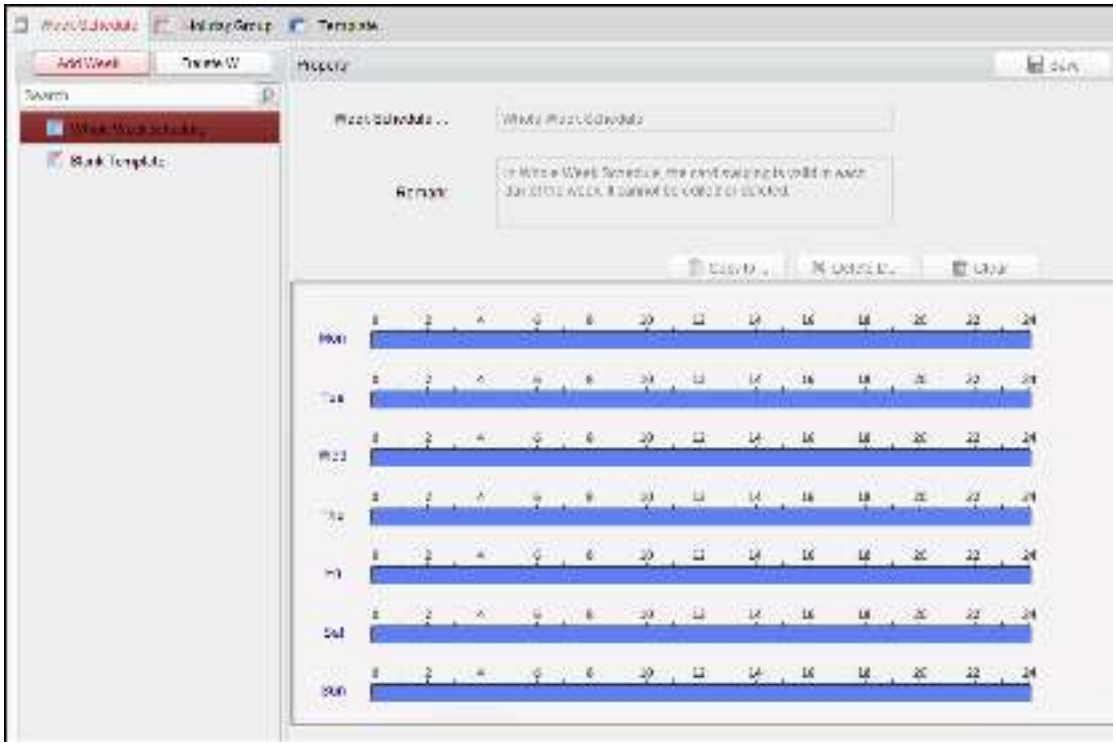
8. После выдачи карты человеку информация о нем и о карте будет отображаться в списке **Person(s) with Card Issued** («Люди, которым выданы карты»).
9. Нажмите **OK** для сохранения настроек.

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 Недельное расписание, Расписание выходных и Шаблоны. 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.

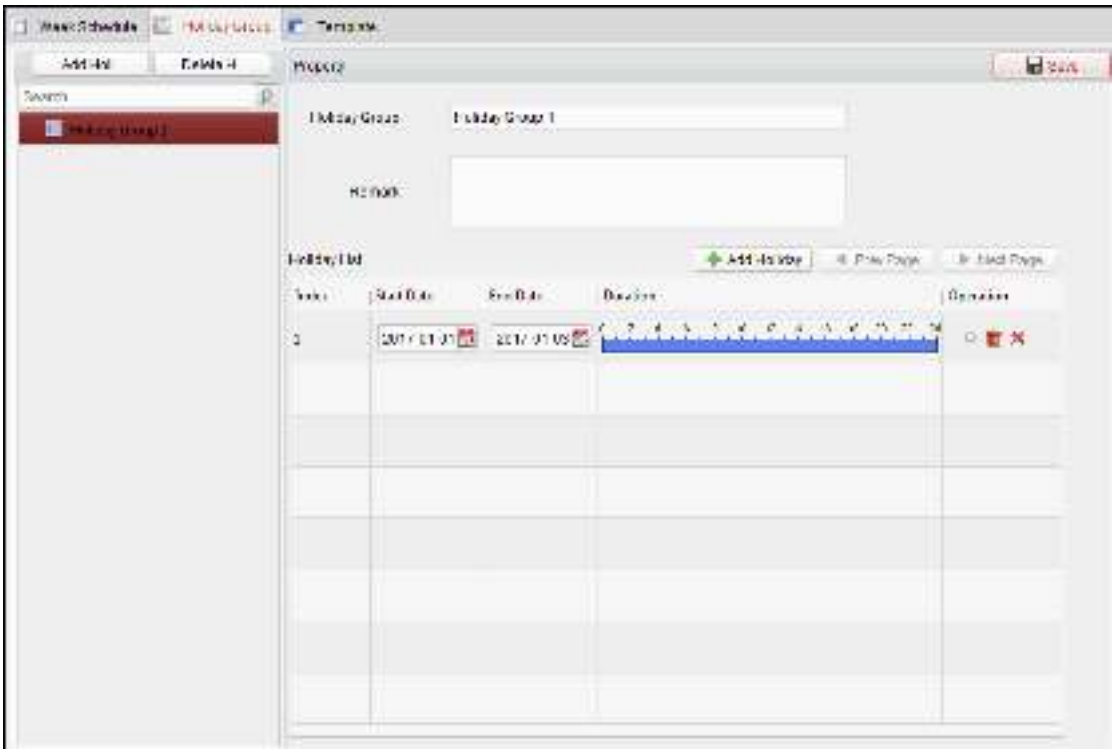
Шаги:

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 выхдных») для перехода в меню управления группами выходных.

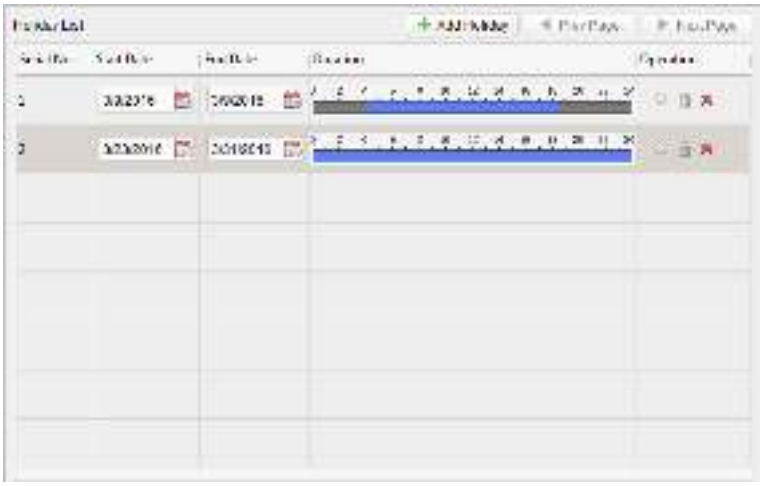


Шаги:

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

2. Введите **name of holiday group** («имя 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.

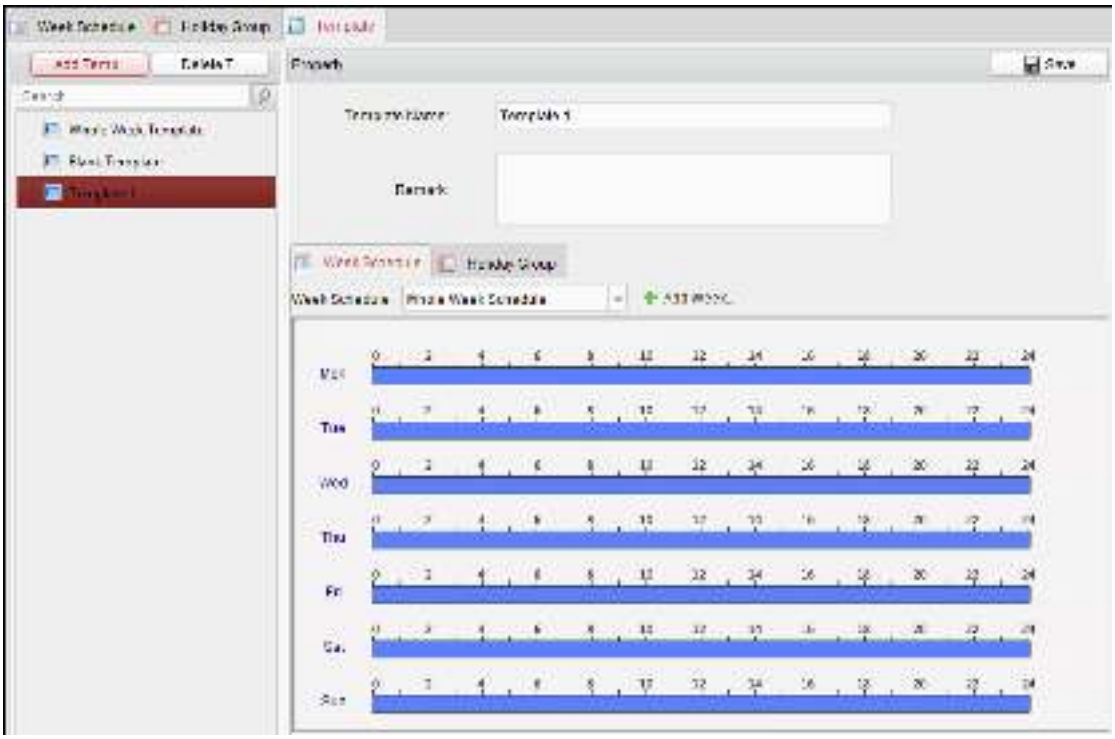
Примечание: Выходные не могут пересекаться друг с другом.

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.



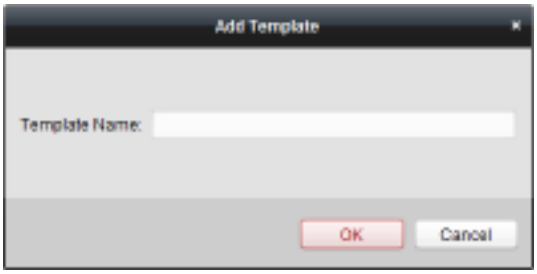
Есть два предопределенных шаблона по умолчанию: **Whole Week Template** («Шаблон для всей недели») и **Blank Template** («Пустой шаблон»), которые не могут быть удалены или изменены.

- **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.

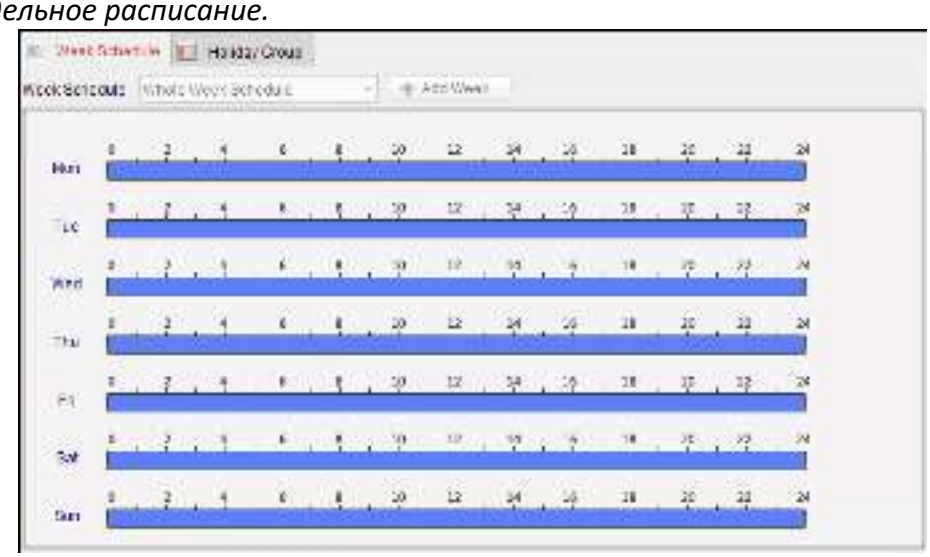
Шаги:

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



2. Введите **template name** («имя шаблона») в текстовое 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 6.6.1 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 6.6.2 Группа выходных.*

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

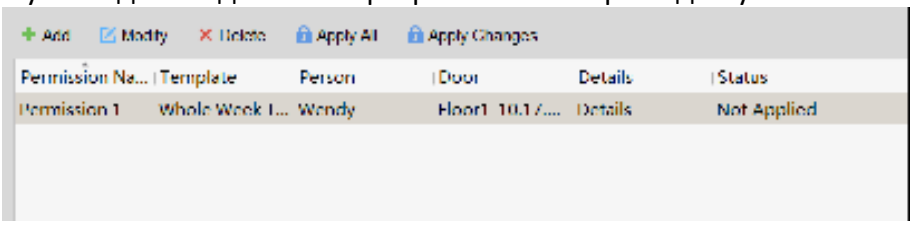
   Нажмите **Clear** («Очистить») для удаления всех добавленных групп выходных.

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:

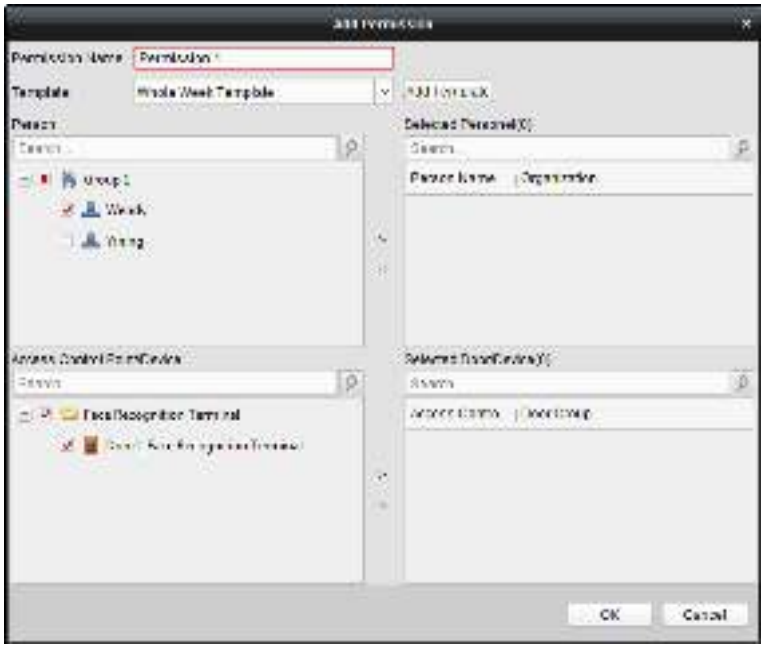
Вы можете назначать разрешения для людей на вход/выход через контрольные точки (двери) в этой секции.

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:

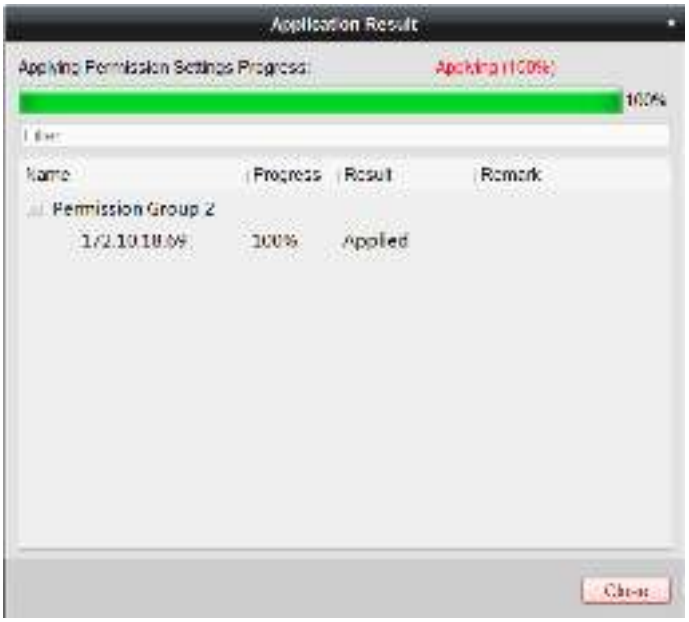
После конфигурации разрешений вы должны применить добавленные разрешения к устройствам контроля доступа.

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 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.).

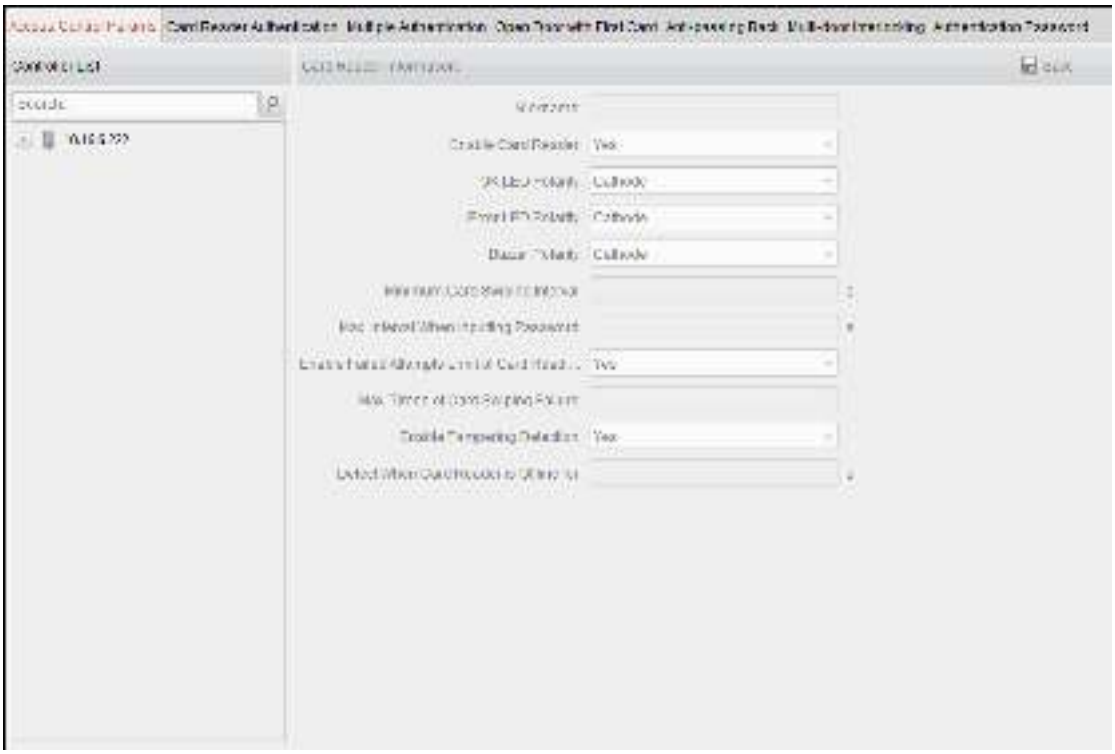
7.8 Расширенные функции

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 следующее 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 для людей с инвалидностью»): Магнитная дверь может быть настроена с необходимой задержкой, после того как человек с инвалидностью 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 ее 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:

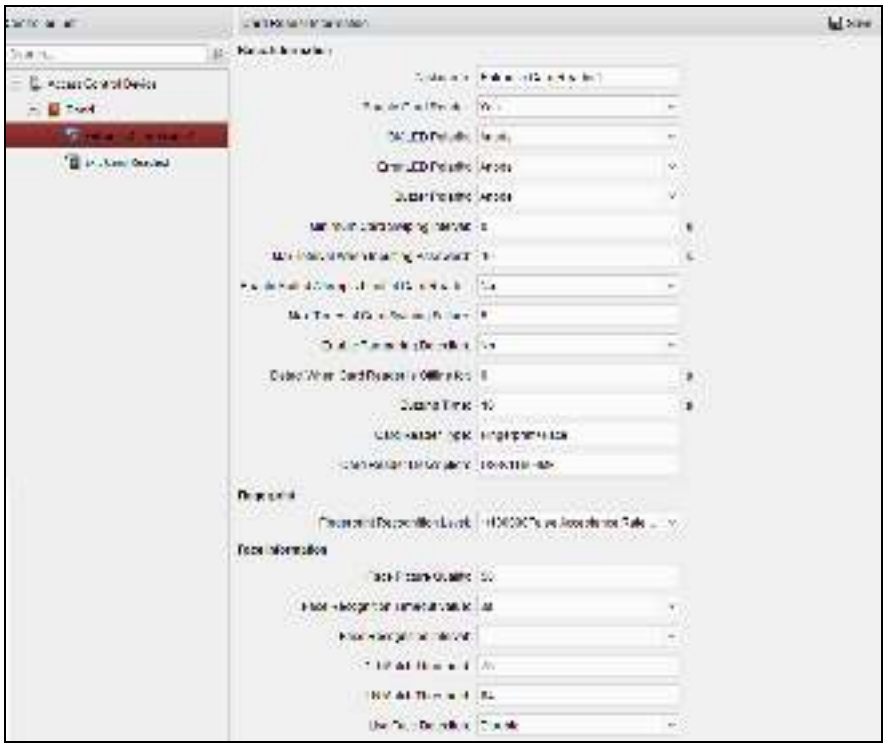
  - Принудительный код и супер пароль должны отличаться.
  - Принудительный код и супер пароль должны содержать 4 -8 цифр.

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:
   a) **Nickname** («Название»): Измените имя считыватея карт по вашему усмотрению.
   b) **Enable Card Reader** («Включить считыватель карт»): Выберите **Yes** («Да») для включения считывателя карт.
   c) **OK LED Polarity** («Полярность светодиода ОК»): Выберите полярность светодиода OK LED для системной платы считывателя карт.
   d) **Error LED Polarity** («Полярность светодиода ошибки»)**:** Выберите полярность светодиода ошибки для системной платы считывателя карт.
   e) **Buzzer Polarity** («Полярность звонка»): Выберите полярность звонка для системной платы считывателя карт.
   f) **Minimum Card Swiping Interval** («Минимальный интервал проводка карты»): Если интервал между проводками одной и той же карты меньше установленного значения, проводка карты недействительна. Вы можете установить значение от 0 до 255.
   g) **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 очищены.
   h) **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.
   i) **Max. Times of Card Swiping Failure** («Макс. число неуспешных считываний карты»): Установите максимальное количество неудачных попыток считывания карты.
   j) **Enable Tampering Detection** («Включить детекцию тамперинга»): Включить детекцию

тамперинга для считывателя карт.

k) **Detect When Card Reader is Offline for** («Детекция оффлайн состояния считывателя карт»): Когда устройство контроля доступа не может подключиться к считывателю карт дольше, чем установленное время, считыватель карт перейдет в оффлайн состояние автоматически.

l) **Buzzing Time** («Время звонка»): Установите время звонка считывателя карт. Доступное время составляет от 0 до 5999 секунд. 0 - непрерывный звон.

m) **Card Reader Type** («Тип считывателя карт»): Получить тип считывателя карт.

n) **Card Reader Description** («Описание считывателя карт»): Получить описание считывателя карт.

o) **Fingerprint Recognition Level** («Уровень распознавания отпечатков пальцев»): Выберите уровень распознавания отпечатков пальцев из выпадающего списка.

p) **Face Picture Quality** («Качество изображения лица»): Установите качество изображения лица при аутентификации.

q) **Face Recognition Interval** («Интервал распознавания лиц»): Интервал времени между двумя непрерывными распознаваниями лица при аутентификации.

r) **1:1 Match Threshold:** («Порог соответствия 1:1»): Установите порог соответствия при аутентификации в режиме **1:1 Matching** («Соответствие 1:1»).

s) **1:N Match Threshold** («Порог соответствия 1:N»): Установите порог соответствия при аутентификации в режиме **1:N Matching** («Соответствие 1:N»).

t) **Live Face Detection** («Детекция реальности лица»): Включение или отключение функции. Если функция включена, устройство может понять, является ли пользователь реальным или нет.

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 вышеуказанный 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

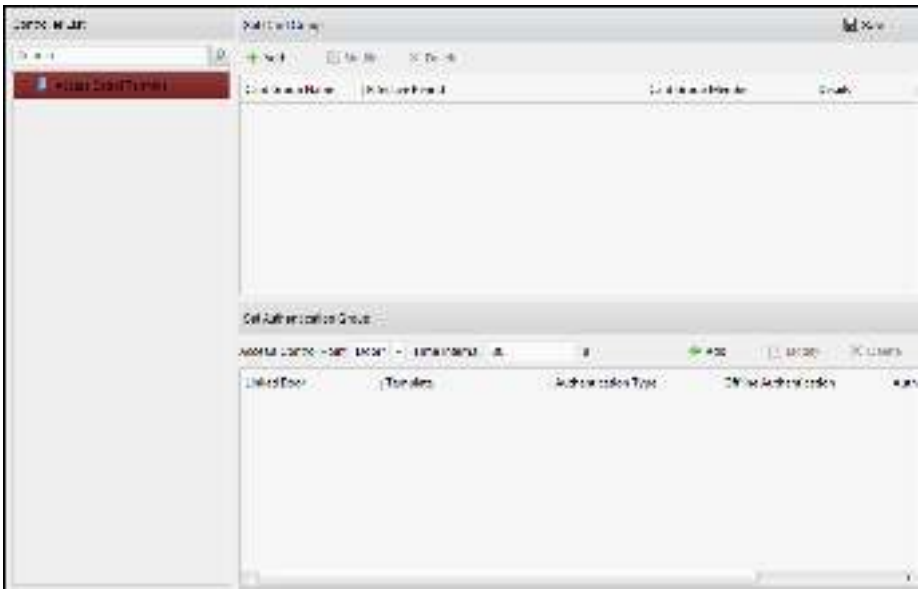
Цель:

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 6.7 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 сплывающего 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 6.6 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 аутентифкации 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»), **Disable Remain Open with First Card** («Отключить открытое состояние запущенное первой картой») и **First Card Authorization** («Авторизация первой карты»).

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

  Примечания:

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

Шаги:

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

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

   Примечания:

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

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

      Примечание: Установите разрешения карты и примените настройки разрешения к устройству контроля доступа. Для получения подробной информации смотрите *Раздел 7.7 Конфигурация разрешений.*
   2) Нажмите кнопку **OK** для подтверждения добавления карты.

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

7.8.5 Запрет обратного прохода

Цель:

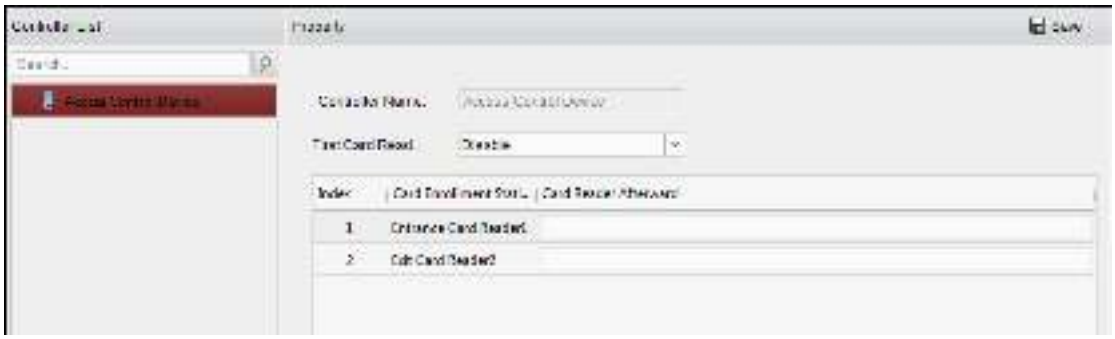
Вы можете установить только проход в одном направлении через контрольную точку в соответствии с заданным путем, и только один человек может пройти контрольную точку доступа после проводки карты.

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

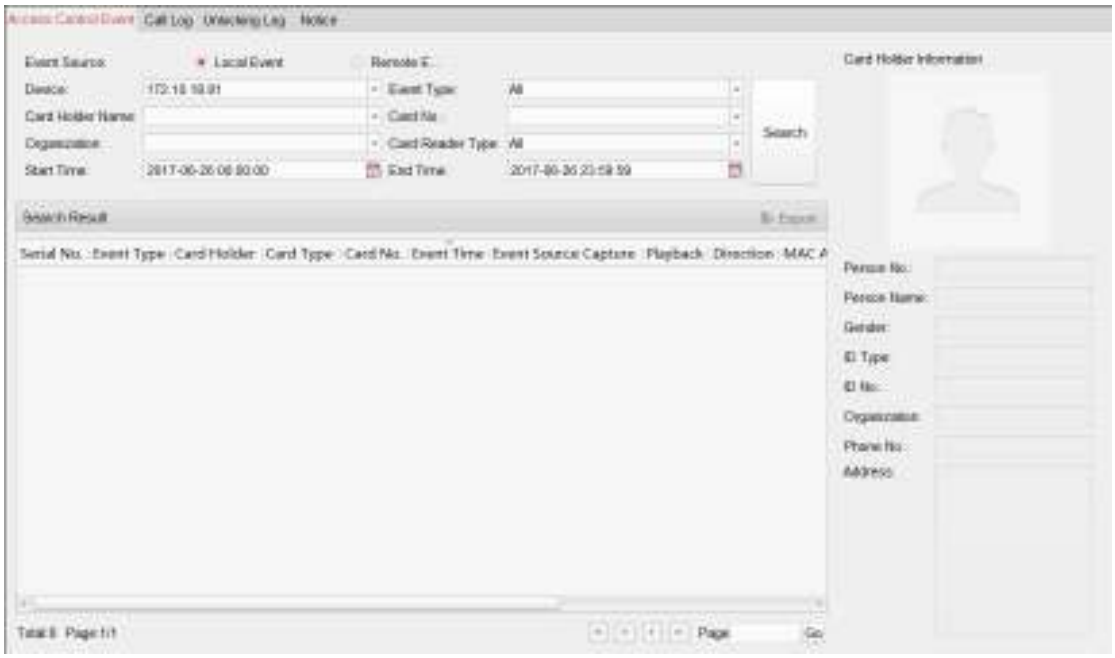
Цель:

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

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 видео файлов 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

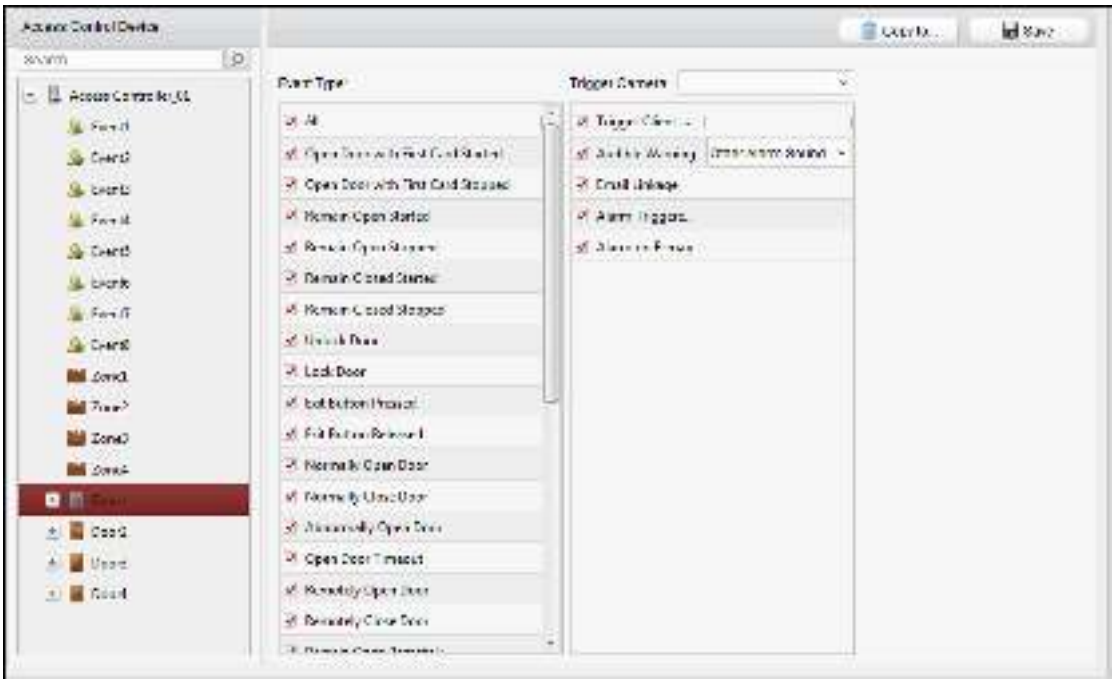
Цель:
Для добавленного устройства контроля доступа вы можете настроить его привязку к управлению доступом, включая привязку событий контроля доступа, привязку тревожного входа контроля доступа, привязку карты/событий и межустройственную привязку.

Нажмите иконку  на панели управления,
или нажмите **Tool -> Event Management** («Инструменты -> Управление событиями») для открытия страницу 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 14.1 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.

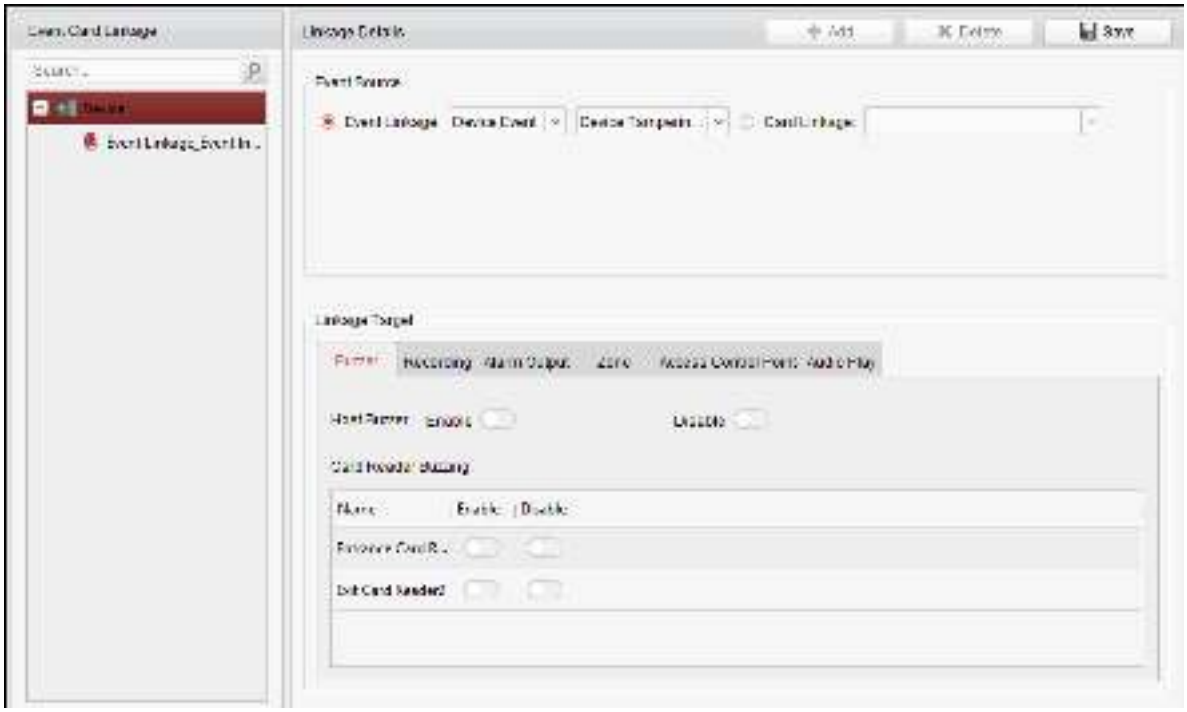


Связанные действия	Описание
Звуковое предупреждение	Клиентское программное обеспечение издает звуковое предупреждение при срабатывании тревоги. Вы можете выбрать звуковой сигнал для звукового предупреждения.
Привязка Email	Отправка email уведомления с информацией о тревоге одному или нескольким получателям.
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 подробный тип события из выпадающего списка.
   - Для **Alarm Input** («Тревожный вход») выберите **alarm** («тревога») или **alarm recovery** («восстановление»), и выберите имя тревожного входа.
   - Для **Door Event** («Событие двери») выберите подробный тип события и выберите дверь источника.
   - Для **Card Reader Event** («Событие считывателя карт») выберите подробный 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 звонка, записи, тревожного выхода и точки контроля доступа.

Тип привязки	Цель привязки	Описание
Buzzer («Звонок»)	**Host Buzzer** («Звонок хоста»)	Звуковое предупреждение контроллера будет запущено.
	Card Reader Buzzing («Звонок 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 звонка, записи, тревожного выхода и точки контроля доступа.

Тип привязки	Цель привязки	Описание
Buzzer («Звонок»)	**Host Buzzer** («Звонок хоста»)	Звуковое предупреждение контроллера будет запущено.
	Card Reader Buzzing («Звонок 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.

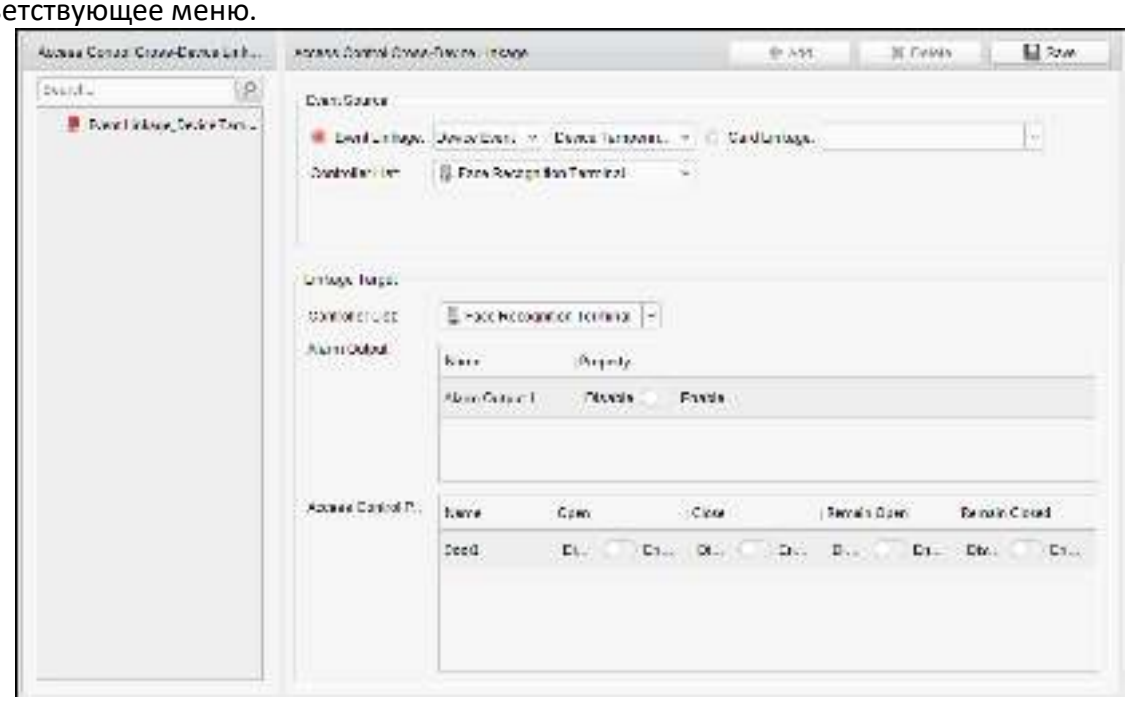
5. Нажмите **Save** («Сохранить») для сохранения и вступления в силу настроек.

7.10.3 Межустройственная привязка

Цель:

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

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



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

Привязка событий

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. 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 подробный тип события из выпадающего списка.
   - Для **Alarm Input** («Тревожный вход») выберите **alarm** («тревога») или **alarm recovery** («восстановление»), и выберите имя тревожного входа.
   - Для **Door Event** («Событие двери») выберите подробный тип события и выберите дверь источника.
   - Для **Card Reader Event** («Событие считывателя карт») выберите подробный тип события и выберите считыватель карт.
2. Установите цель привязки, выберите устройство контроля доступа из выпадающего списка в качестве цели привязки, и переключайте свойства с на  для их включения.
   - **Alarm Output** («Тревожный выход»): Тревожный выход будет инициирован для уведомления.
   - **Access Control Point** («Контрольная точка доступа»): Будут запущены различные состояния двери: **open** («открыта»), **close** («закрыта»), **remain open** («оставить открытой») и **remain closed** («оставить закрытой»).

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

Привязка карты

Шаги:

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

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

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.

7.11.1 Управление группой контроля доступа

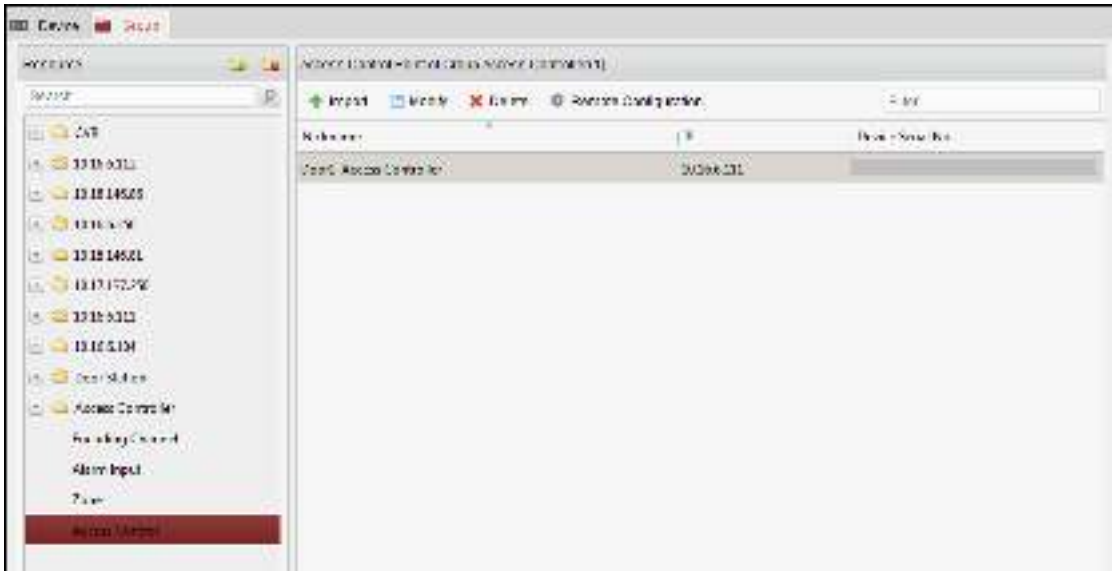
Цель:

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

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

Шаги:

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



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

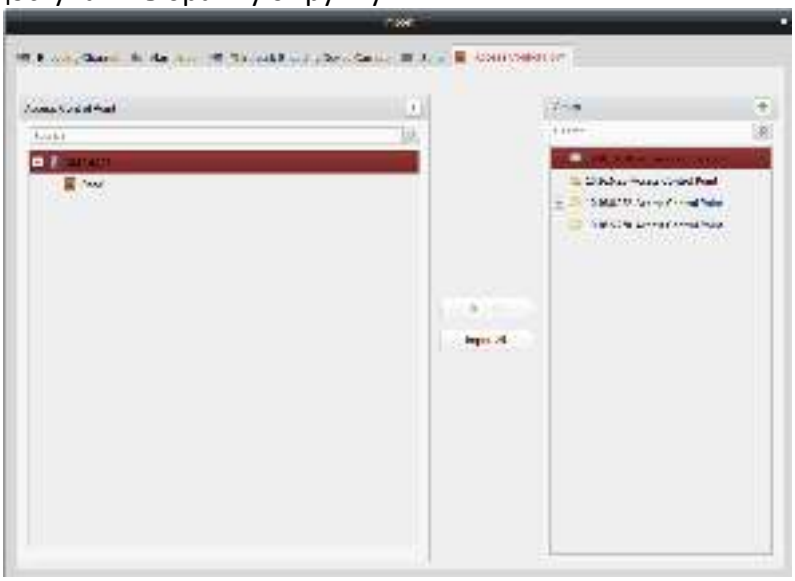
      Вы также можете поставить галочку **Create Group by Device Name** («Создать группу по имени устройства») для создания новой группы с именем, совпадающим с именем выбранного устройства.

4. Выполните следующие шаги, чтобы импортировать контрольные точки 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.



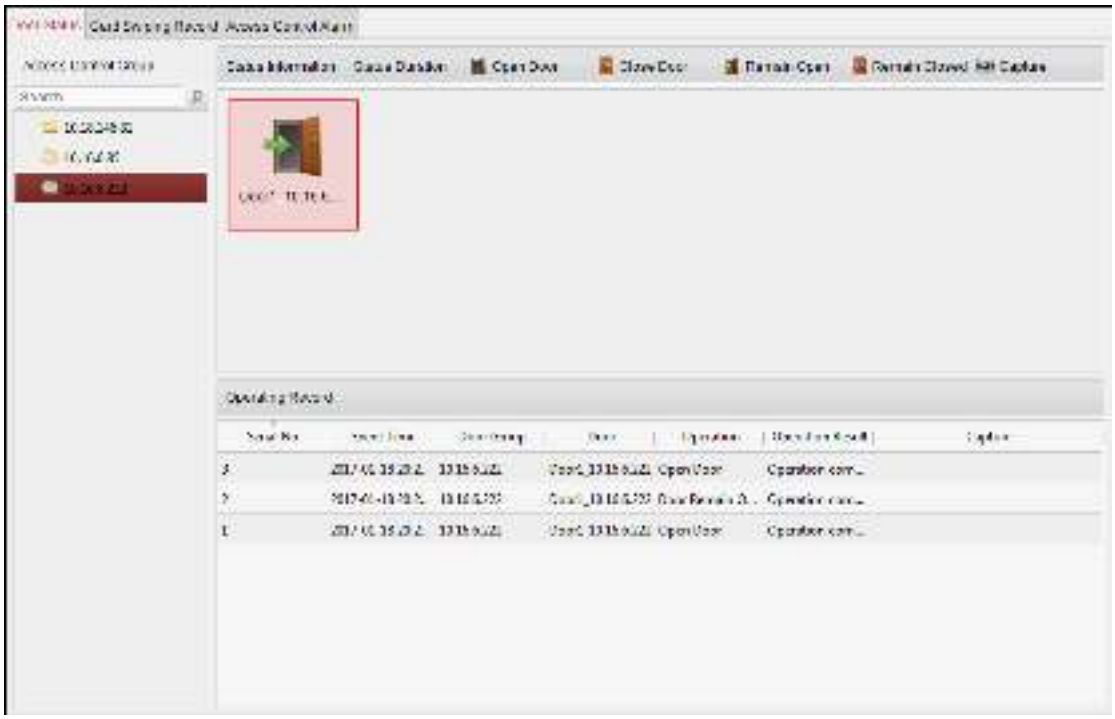
5. После импорта контрольных точек доступа в группу вы можете нажать  или дважды щелкнуть по имени группы/контрольной точки доступа для ее редактирования.

7.11.2 Анти-контроль контрольной точки 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.



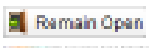
Шаги:

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

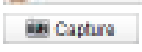
   Нажмите иконку  на панели статуса для выбора двери.
3. Нажмите на одну из кнопок, перечисленных на панели **Status Information** («Сведения о состоянии»), чтобы выбрать состояние для двери.

    («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 состояние выбрано как **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.

7.11.3 Конфигурация длительности состояния

Цель:

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

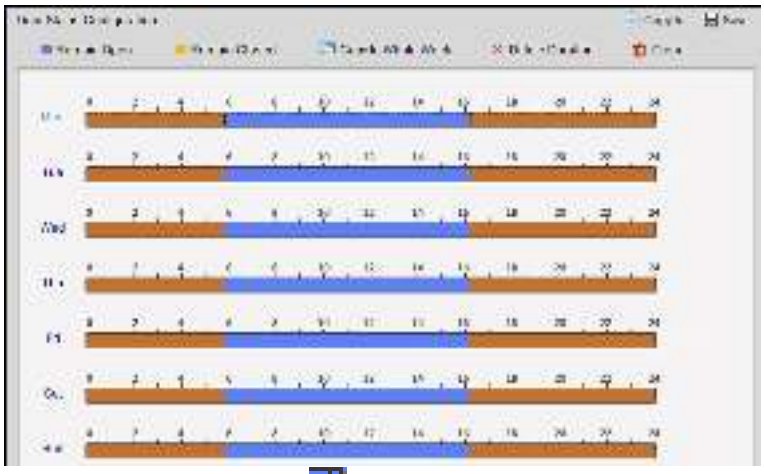
В модуле **Door Status** («Состояние двери») нажмите кнопку **Status Duration** («Длительность состояния») для перехода в соответствующее меню.

Шаги:

1. Нажмите, чтобы выбрать дверь из списка устройств управления доступом слева.
2. На панели **Door Status Configuration** («Конфигурация состояния двери») справа нарисуйте расписание для выбранной двери.
   1) Выберите кисть для маркировки состояния двери:  («Оставить открытой») или  («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.

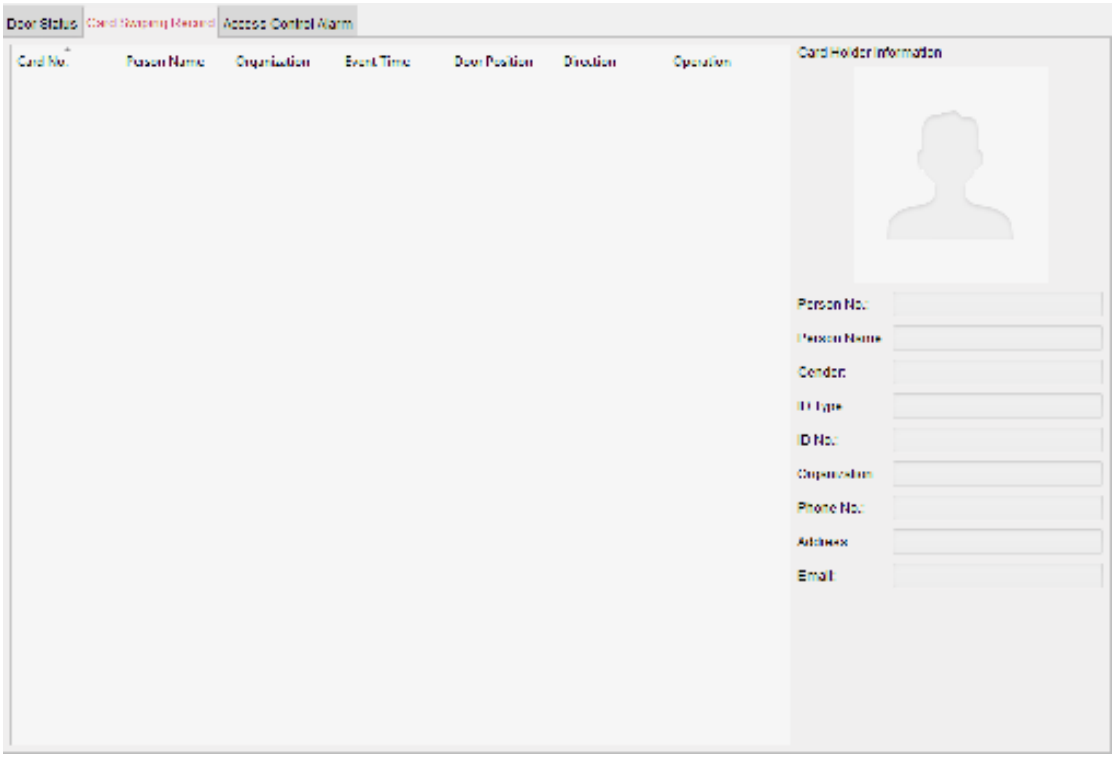


3) Когда курсор превращается в , вы можете переместить выбранную шкалу времени, которую вы только что отредактировали. Вы также можете отредактировать отображаемую временную точку, чтобы установить точный период времени.
   Когда курсор превращается в , вы можете удлинить или сократить выбранную временную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

7.11.4 Запись проводки карты в реальном времени

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



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

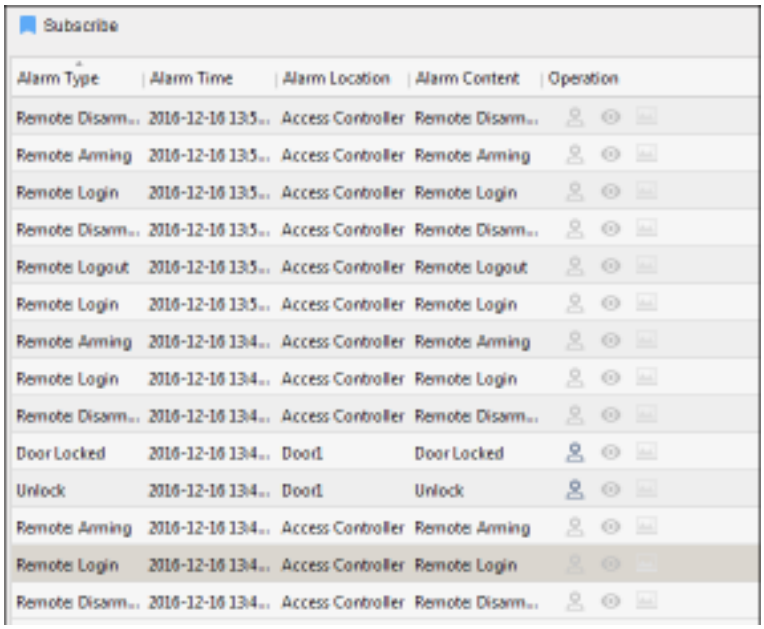
Вы можете нажать на событие для просмотра подробной информации о владельце карты, включая № человека, имя человека, организацию, телефон, контактный адрес и др.

7.11.5 Тревога контроля доступа в реальном времени

Цель:

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

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



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.

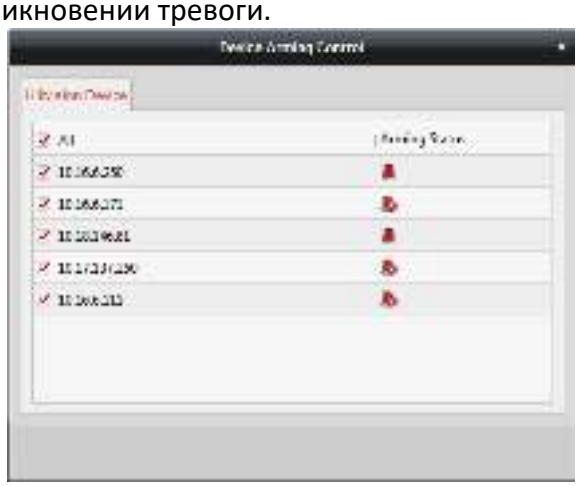
7.12 Управление охраной

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.



7.13 Время и посещаемость

Цель:

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

Перед началом:

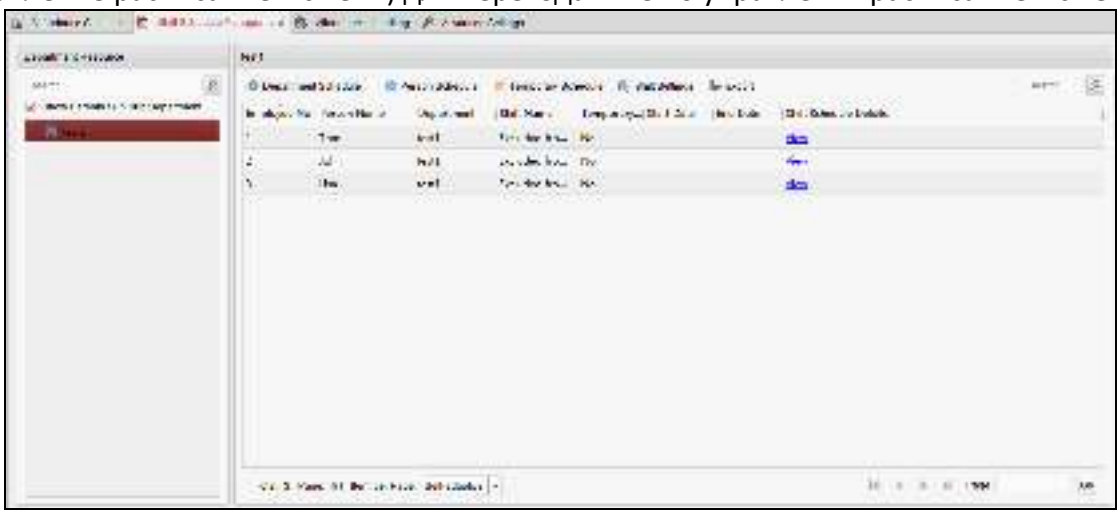
Вы должны добавить организацию и человека в модуле **Access Control** («Контроль доступа»). Для получения подробной информации смотрите *Раздел 7.4.1 Добавление организации* и *Раздел 7.5.1 Добавление людей.*

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:

7.13.1 Управление расписанием смены

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



Настройки смены

Цель:

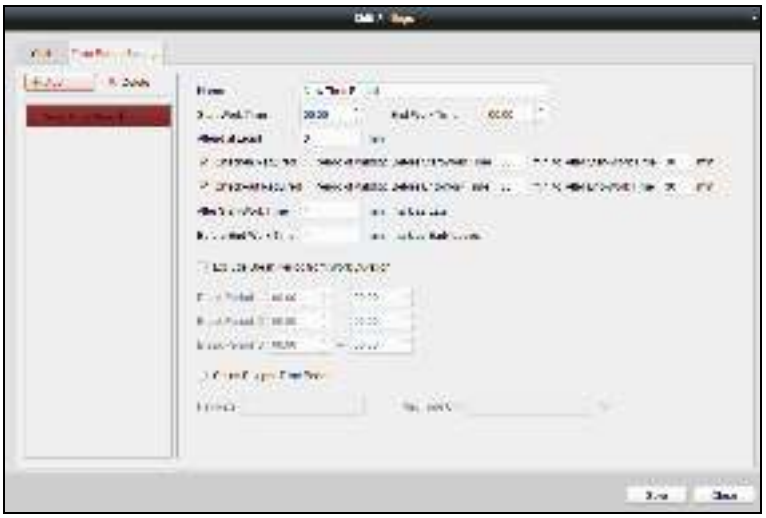
Вы можете добавлять периоды времени и смены для расписания смен.

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 периодов 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.

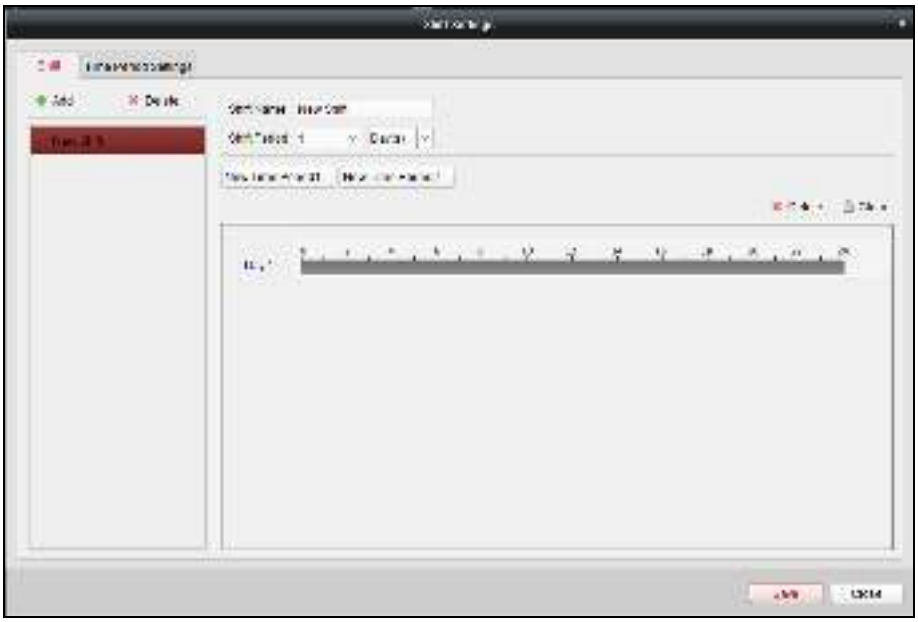
   Добавленный период времени отобразится на левой панели.

   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 временный 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 значение 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.

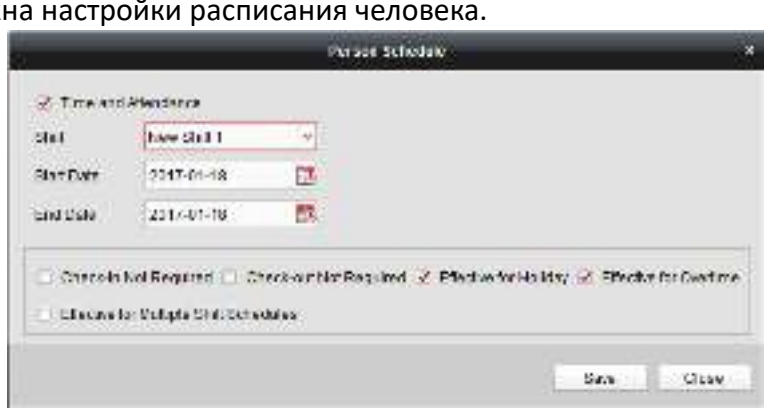
2) (Опционально) Для удаления выбранного периода времени, выберите его и нажмите «.

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.



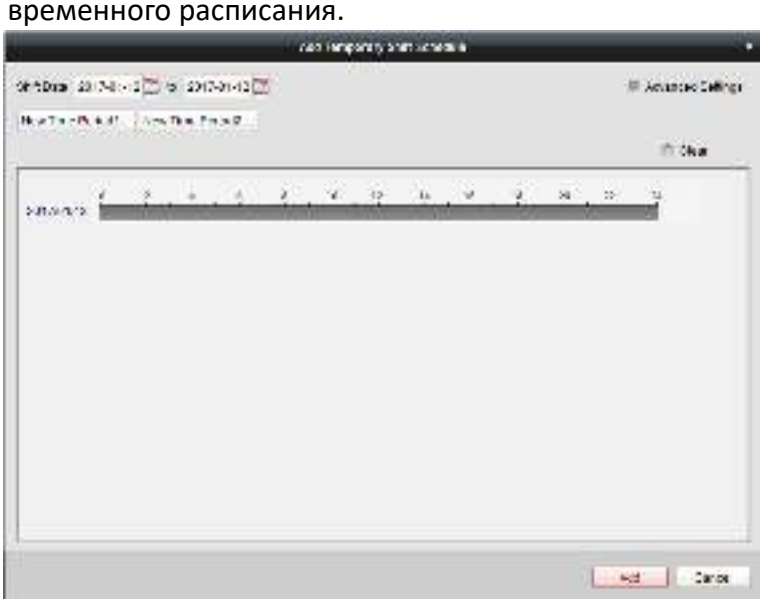
4. Поставьте галочку **Time and Attendance** («Время и посещаемость»).
   К выбранному человеку будет применено расписание посещаемости.
5. Выберите смену из выпадающего списка **shift** («смена»).
6. Установите значение для **start date** («дата начала») и **end date** («дата окончания»).
7. (Опционально) 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 людей на панели справа.
3. Нажмите **Temporary Schedule** («Временное расписание») всплывающего диалогового

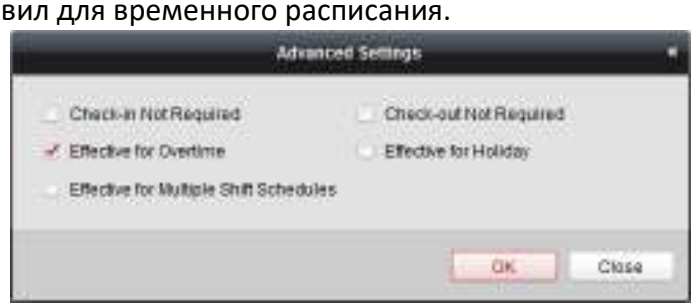
окна настройки временного расписания.



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.



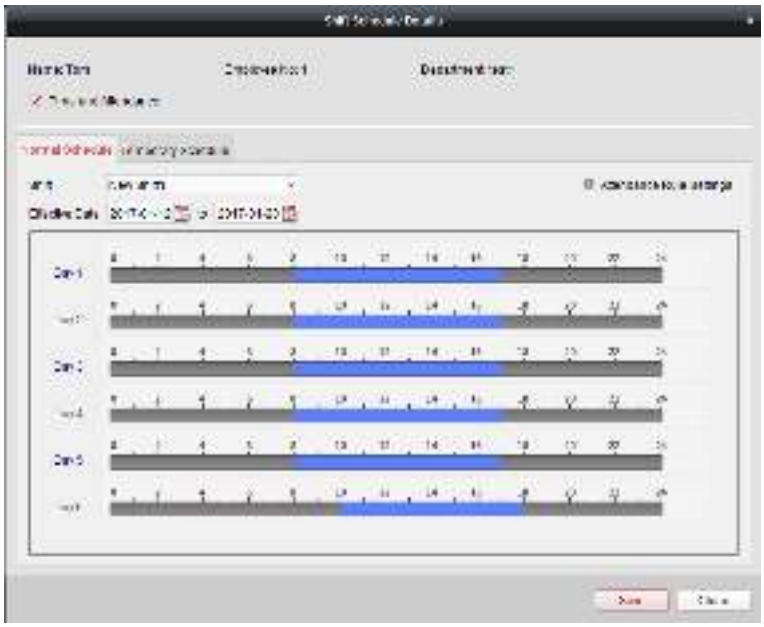
7. Нажмите **OK** для сохранения настроек.

➢ **Проверка деталей расписания смен**

Шаги:

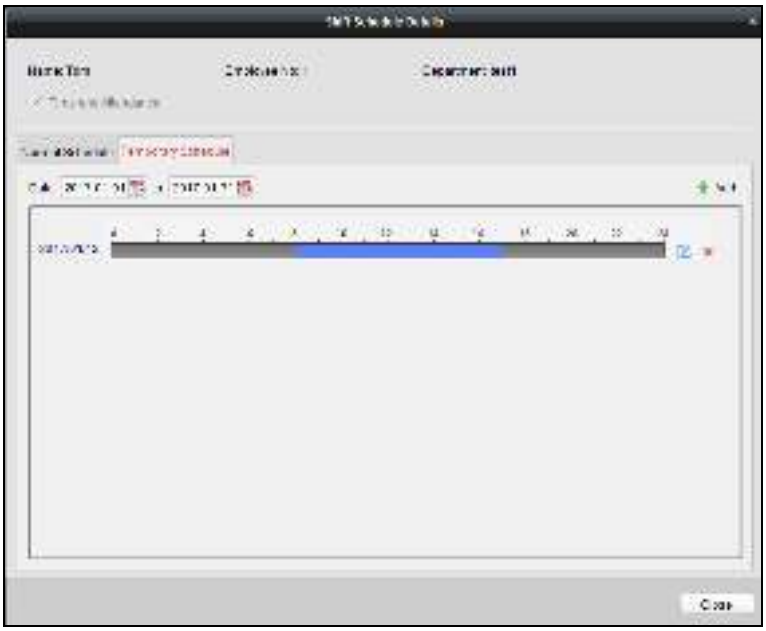
1. Откройте меню **Shift Schedule Management** («Управление расписанием смен») и выберите отдел на панели слева.
2. Выберите людей на панели справа.
3. Нажмите **View** («Просмотр») для появления всплывающего диалогового окна деталей расписания смен.

   Вы можете проверить и 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 отметить правила посещаемости по желанию 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.

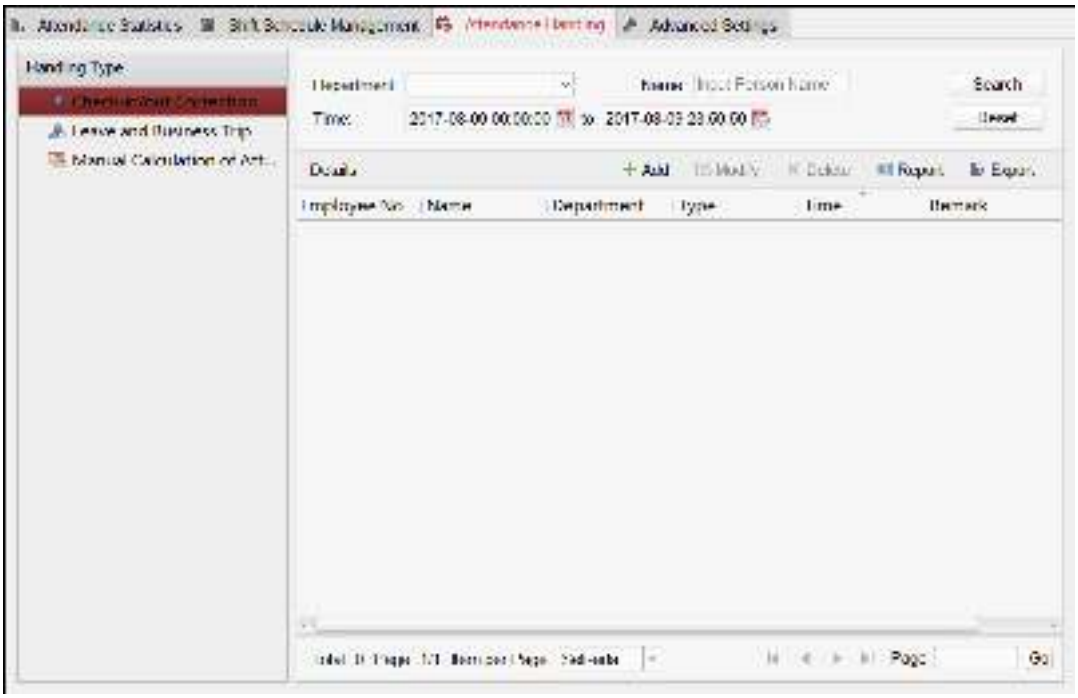
Примечание: Экспортированные данные сохраняются в формате *.csv.

7.13.2 Обработка посещаемости

Цель:

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

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



Корректировка отметки о приходе/уходе

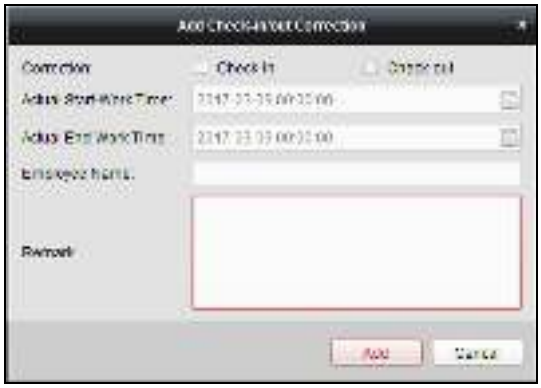
Цель:

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

- **Добавление корректировки отметки о приходе/уходе**

Шаги:

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



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

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

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

Шаги:

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

Отпуск и деловая поездка

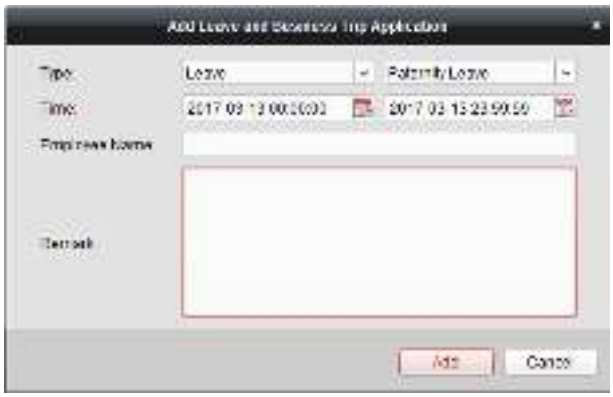
Цель:

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 *Раздел 7.13.3 Расширенные настройки* 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.

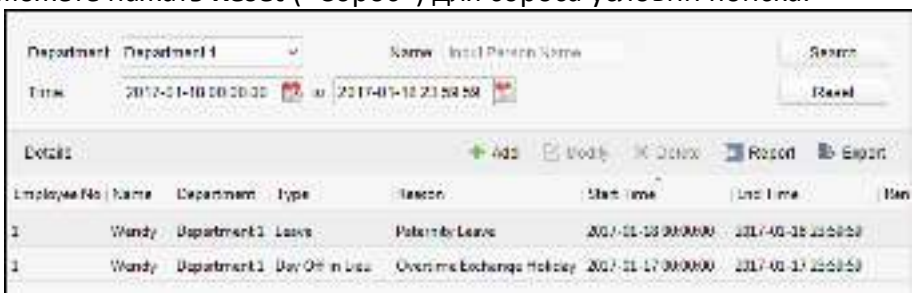
   Примечание: Экспортированные данные сохраняются в формате *.csv.

➢ **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: Он Могут быть рассчитаны данные о посещаемости в течение трех месяцев.

7.13.3 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.

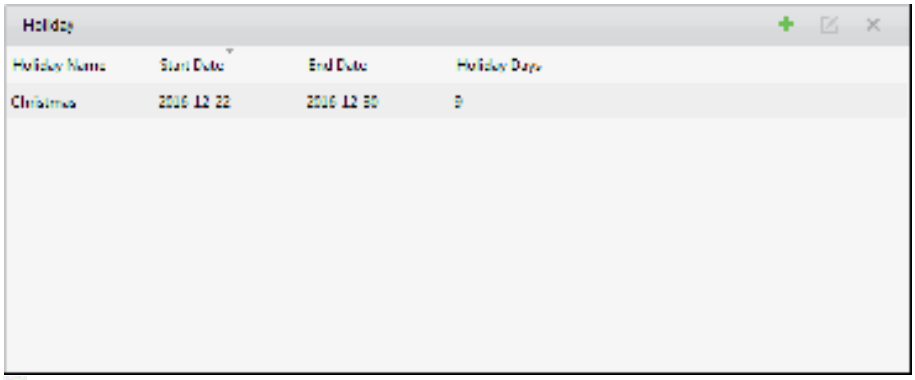
3. Задайте связанную информацию.
   Check Point Name («Имя контрольной точки»): Введите имя контрольной точки.
   Card Reader («Считыватель карт»): Выберите считыватель карт из выпадающего списка.
   Check Point Function («Функция контрольной точки»): Выберите функцию для контрольной точки.
   Door Location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

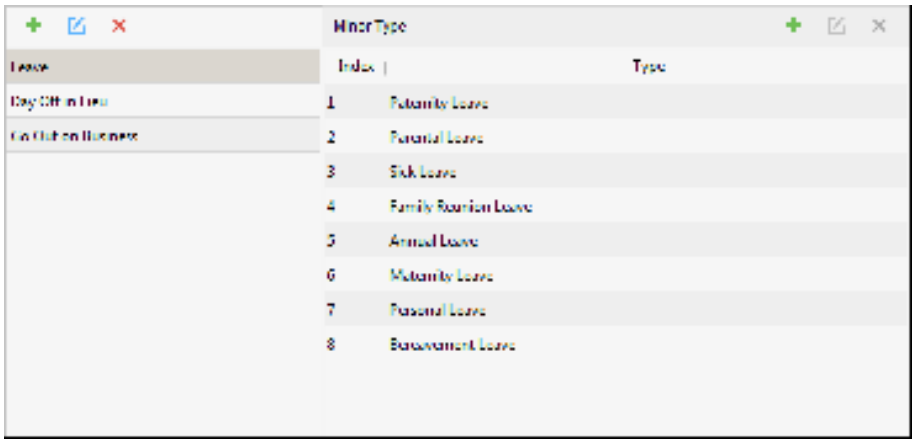
3. Установите связанные параметры.
   Holiday Name («Имя выходного»): Введите название для выходного.
   Start Date/End Date («Дата начала/окончания»): Нажмите для указания даты выходного.
4. Нажмите **Add** («Добавить») для добавления выходного.
   Добавленные выходные будут отображены в списке.

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

Настройка типа отпуска

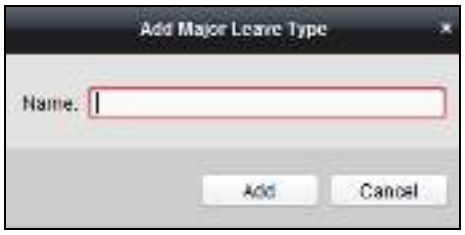
Шаги:

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.

7.13.4 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 7.13.2 Обработка посещаемости*.

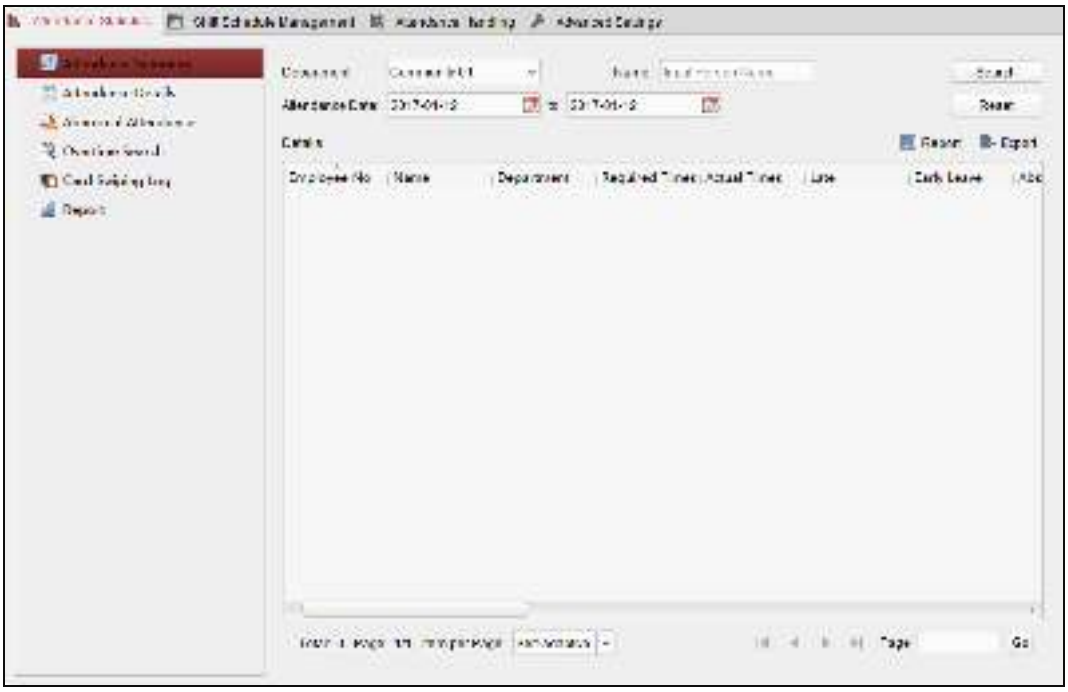
Сводка посещаемости

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.

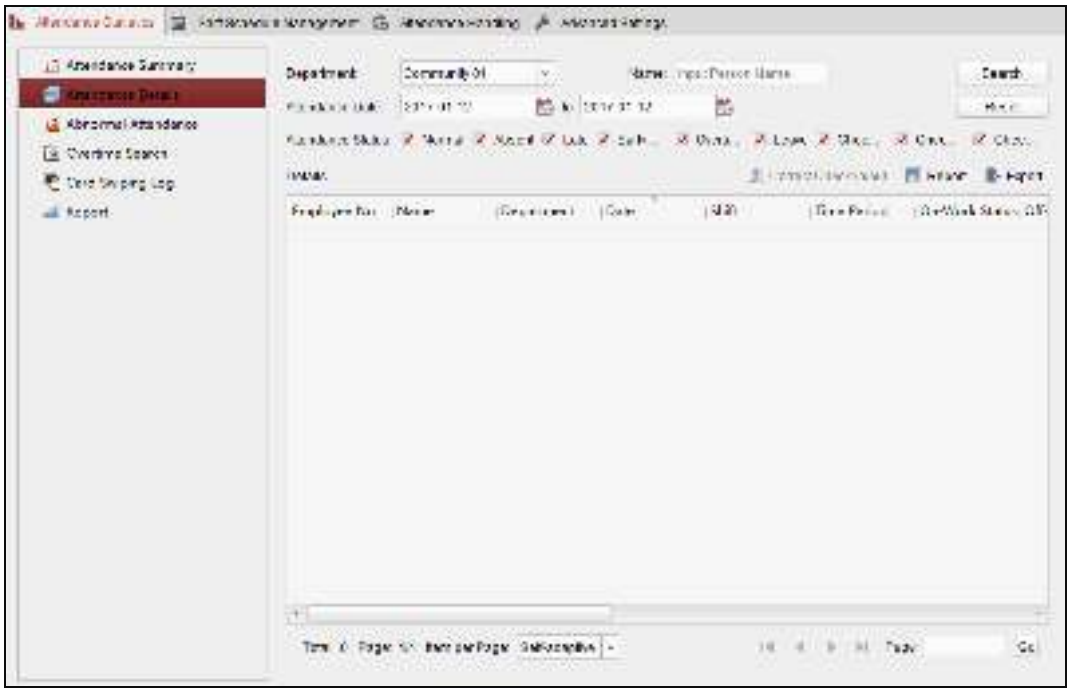


3. Задайте условия поиска, включая отдел, имя сотрудника и дату посещения.
   (Опционально) Вы можете нажать **Reset** («Сброс») для сброса всех настроенных условий поиска.
4. Нажмите **Search** («Поиск») для начала поиска, подходящие результаты будут отображены в виде списка на этой странице.
   (Опционально)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

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.

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.

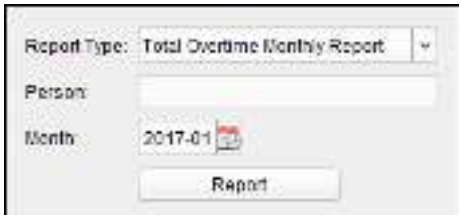
Отчет

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.*

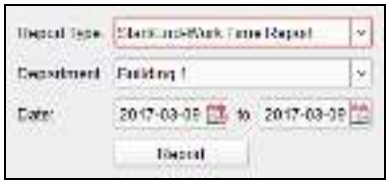
➢ **Генерация ежемесячного отчета о посещаемости**

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.

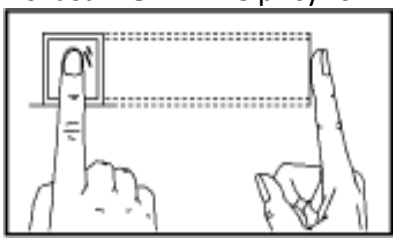
Приложение A Советы по сканированию отпечатков пальцев

Рекомендуемый палец

Указательный палец или средний палец.

Правильное сканирование

Показанный ниже рисунок - это правильный способ сканирования пальца:



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

Другое

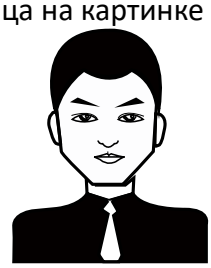
Если ваш отпечаток неглубокий или трудно отсканировать отпечаток пальца, мы рекомендуем использовать другие методы аутентификации.

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

Приложение B Советы по сбору/сравнению изображений лиц

B.1 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.2 Положение лица

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

B.3 Размер лица

Убедитесь, что ваше лицо находится в середине окна.


See Far, Go Further