



Терминал распознавания лиц

Руководство пользователя

Руководство пользователя

©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

Это руководство предназначено для терминала распознавания лиц.

Серия	Модели
Терминал распознавания лиц	DS-K1T604M
	DS-K1T604MF

Примечание. В названии данной модели буква F обозначает наличие модуля отпечатков пальцев. Буква M обозначает наличие у изделия поддержки карт Mifare.

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

О руководстве

Настоящее руководство защищено авторскими правами на внутреннем и международном уровнях. Все права на данное руководство принадлежат компании Hangzhou Hikvision Digital Technology Co., Ltd. (Hikvision). Руководство не может быть воспроизведено, изменено, переведено или распространено, частично или полностью, любыми способами без предварительного письменного разрешения Hikvision.

Торговые марки

HIKVISION и другие знаки Hikvision являются собственностью Hikvision и зарегистрированными товарными знаками или предметом заявок на собственность компании Hikvision и/или ее аффилированных лиц. Другие торговые марки, упомянутые в руководстве, являются собственностью соответствующих владельцев. Право на получение лицензии по использованию таких торговых марок предоставляется только по специальному разрешению.

Ограничение ответственности

НАСКОЛЬКО ЭТО РАЗРЕШЕНО ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, КОМПАНИЯ HIKVISION НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ В ОТНОШЕНИИ ДАННОГО РУКОВОДСТВА, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, В ТОМ ЧИСЛЕ (НО НЕ ОГРАНИЧИВАЯСЬ) КАСАТЕЛЬНО ПАРАМЕТРОВ КАЧЕСТВА И СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ. КОМПАНИЯ HIKVISION НЕ ГАРАНТИРУЕТ И НЕ ПРЕДОСТАВЛЯЕТ ЗАВЕРЕНИЙ В ОТНОШЕНИИ ИСПОЛЬЗОВАНИЯ ДАННОГО РУКОВОДСТВА, А ТАКЖЕ В ОТНОШЕНИИ ВЕРНОСТИ, ТОЧНОСТИ ИЛИ АКТУАЛЬНОСТИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В НЕМ. ОТВЕТСТВЕННОСТЬ ЗА РАБОТУ С ДАННЫМ РУКОВОДСТВОМ И ИСПОЛЬЗОВАНИЕ ЕГО СОДЕРЖИМОГО ВОЗЛАГАЕТСЯ НА ПОЛЬЗОВАТЕЛЯ.

ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ПОЛУЧЕНИЕМ ДОСТУПА В СЕТЬ ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ. HIKVISION НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА АНОМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕРНЕТИЧЕСКИМИ АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ РИСКАМИ, СВЯЗАННЫМИ С РАБОТОЙ В СЕТИ ИНТЕРНЕТ; ОДНАКО, HIKVISION ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.

ЗАКОНЫ, РЕГУЛИРУЮЩИЕ СФЕРУ ВИДЕОНАБЛЮДЕНИЯ, МОГУТ РАЗЛИЧАТЬСЯ ДЛЯ КАЖДОЙ КОНКРЕТНОЙ СТРАНЫ. УБЕДИТЕСЬ, ЧТО МОЖЕТЕ ИСПОЛЬЗОВАТЬ ПРОДУКТ В СООТВЕТСТВИИ С ЗАКОНАМИ ВАШЕЙ СТРАНЫ. НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ В СЛУЧАЕ, ЕСЛИ ЭТОТ ПРОДУКТ ИСПОЛЬЗУЕТСЯ В НЕЗАКОННЫХ ЦЕЛЯХ.

В СЛУЧАЕ ВОЗНИКНОВЕНИЯ ЛЮБЫХ ПРОТИВОРЕЧИЙ МЕЖДУ СОДЕРЖАНИЕМ ДАННОГО РУКОВОДСТВА И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПРЕИМУЩЕСТВОМ ОБЛАДАЮТ ТРЕБОВАНИЯ НОРМАТИВНЫХ АКТОВ.

Обслуживание

При возникновении каких-либо вопросов следует обращаться к местному поставщику.

Правовая информация

Информация касательно Федеральной комиссии по связи

Обратите внимание, что изменения или модификации, не одобренные явно стороной, ответственной за соответствие, может привести к аннулированию полномочий пользователя по работе с данным оборудованием.

Соответствие стандартам Федеральной комиссии по связи: Это оборудование было протестировано и признано соответствующим ограничениям для цифровых устройств класса В в соответствии с частью 15 правил FCC. Эти ограничения разработаны для обеспечения необходимой защиты от вредных помех в жилых помещениях. Данное оборудование генерирует, использует и может излучать радиочастотную энергию и, если не установлено и не используется в соответствии с инструкциями, может вызвать вредные помехи для радиосвязи. Тем не менее, нет гарантий того, что помехи не возникнут в конкретной установке. Если оборудование создает вредные помехи для приема радио- или телевизионных сигналов, что может быть определено путем включения и выключения оборудования, пользователю рекомендуется попытаться устранить помехи одним или несколькими способами, а именно:

- Измените ориентацию или местоположение приемной антенны.
- Увеличьте расстояние между оборудованием и приемником.
- Подключите оборудование к розетке в цепи, отличной от той, к которой подключен приемник.
- Обратитесь к дилеру или опытному радио- или телевизионному технику.

Оборудование следует устанавливать и эксплуатировать с минимальным расстоянием в 20 см между излучателем и телом пользователя.

Условия Федеральной комиссии по связи

Это устройство соответствует части 15 Правил Федеральной комиссии по связи. Эксплуатация допускается при соблюдении следующих двух условий:

1. Это устройство не может создавать вредные помехи.
2. Это устройство должно принимать любые полученные помехи, включая помехи, которые могут вызвать сбои в работе.

Заявление о соответствии нормам ЕС



Этот продукт и, если применимо, поставляемые аксессуары обозначены знаком «CE» и соответствуют применимым европейским стандартам, перечисленным в Директиве о радиооборудовании 2014/53/ЕС, Директиве по электромагнитной совместимости 2014/30/ЕС и Директиве об ограничении содержания вредных веществ 2011/65/ЕС.



Директива 2012/19/ЕС (Директива ЕС об отходах электрического и электронного оборудования): В пределах Европейского Союза продукты, обозначенные этим знаком, нельзя утилизировать вместе с бытовыми отходами. Для надлежащей утилизации верните этот продукт местному поставщику при покупке

эквивалентного нового оборудования или утилизируйте его в специальных пунктах приема.

Подробнее: www.recyclethis.info



Директива 2006/66/ЕС (Директива о батареях и аккумуляторах и отходах батареек и аккумуляторов): Этот продукт содержит аккумулятор, который в пределах Европейского Союза нельзя утилизировать вместе с бытовыми отходами. Подробнее об аккумуляторе см. документацию. Аккумулятор обозначают таким знаком, который может содержать надписи, указывающие

на наличие кадмия (Cd), свинца (Pb) или ртути (Hg). Для надлежащей утилизации верните аккумулятор местному поставщику или утилизируйте его в специальных пунктах приема.

Подробнее: www.recyclethis.info

Используйте только источники питания, перечисленные в руководстве пользователя:

Модель	Производитель
KPL-040F-VI	Channel Well Technology Co Ltd.

Инструкции по технике безопасности

Эти инструкции предназначены для обеспечения правильного использования продукта и предотвращения угроз или порчи имущества.

Меры предосторожности подразделяются на **Предупреждения** и **Предостережения**.

Предупреждения: игнорирование предупреждения может привести к тяжелым травмам или смерти.

Предостережения: игнорирование предостережения может привести к травмам или порче оборудования.

	
Предупреждения. Следуйте этим мерам безопасности, чтобы предотвратить серьезную травму или смерть.	Предостережения. Следуйте этим мерам безопасности, чтобы предотвратить возможную травму или материальный ущерб.



Предупреждения

- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в вашем регионе.
- Используйте адаптер питания, который предоставляется обычной компанией. Потребляемая мощность не может быть меньше требуемого значения.
- Не подключайте несколько устройств к одному блоку питания, так как его перегрузка может привести к перегреву или возгоранию.
- Отключите питание устройства перед его подключением, установкой или демонтажем.
- Если продукт установлен на стене или потолке, необходимо прочно закрепить устройство.

- Если вы заметите дым, запах или шум, исходящий от устройства, немедленно отключите питание и отсоедините шнур питания, а затем обратитесь в сервисный центр.
- Если изделие не функционирует должным образом, следует обратиться к поставщику или в ближайший сервисный центр. Никогда не пытайтесь разобрать устройство самостоятельно. (Мы не берем на себя ответственность за проблемы, вызванные несанкционированным ремонтом или обслуживанием).



Предостережения

- Не роняйте устройство и не подвергайте его физическим ударам или воздействию сильного электромагнитного излучения. Избегайте установки оборудования на вибрирующих поверхностях или в местах, подверженных ударам (это может привести к повреждению оборудования).
- Не размещайте устройство в очень жарком, холодном (диапазон рабочих температур указан в технических характеристиках устройства), запыленном или влажном месте и не подвергайте его воздействию сильного электромагнитного излучения.
- Не допускайте попадания дождевых капель и влаги на крышку устройства для использования в помещении.
- Не подвергайте оборудование воздействию прямого солнечного света, низко расположенного источника вентиляции или тепла, такого как нагреватель или радиатор (это может привести к возгоранию).
- Не направляйте устройство на солнце или очень яркие объекты. В противном случае может произойти размытие или смазывание изображения (что не является неисправностью), что одновременно влияет на срок эксплуатации датчика.
- При открытии крышки устройства используйте прилагаемую перчатку, избегайте прямого контакта с крышкой устройства, поскольку кислоты, содержащиеся в поту пальцев, могут разрушить поверхность покрытия крышки устройства.
- При чистке внутренних и наружных поверхностей крышки устройства используйте мягкую сухую ткань и не используйте щелочные моющие средства.
- Сохраните упаковочный материал после распаковки устройства для дальнейшего использования. В случае возникновения сбоя необходимо будет вернуть устройство на завод в оригинальной упаковке. Транспортировка без оригинальной упаковки может привести к повреждению устройства и дополнительным расходам.
- Неправильное использование или замена аккумулятора может привести к взрыву. Батареи нужно менять на элементы такого же либо эквивалентного типа. Утилизацию использованных батарей следует выполнять согласно инструкции производителя.

Содержание

Раздел 1	Обзор	1
1.1	Введение	1
1.2	Особенности продукта	1
Раздел 2	Внешний вид.....	3
Раздел 3	Монтаж	5
3.1	Монтаж с использованием установочной коробки	5
3.2	Монтаж без установочной коробки	6
Раздел 4	Подключение терминала.....	9
Раздел 5	Основные операции	11
5.1	Активация устройства	11
5.1.1	Активация при помощи устройства	11
5.1.2	Активация при помощи программного обеспечения SADP	11
5.1.3	Активация при помощи программного обеспечения клиента	13
5.2	Вход в систему	16
5.3	Настройка общих параметров.....	16
5.3.1	Настройки связи	16
5.3.2	Настройки системы	20
5.3.3	Настройка времени	26
5.4	Управление пользователями.....	27
5.4.1	Добавление пользователей.....	27
5.4.2	Управление пользователями.....	31
5.5	Настройка параметров управления доступом.....	32
5.6	Прочие функции управления	33
5.6.1	Управление данными.....	33
5.6.2	Управление записями в журналах	35
5.6.3	Импорт/экспорт данных	35
5.6.4	Просмотр системной информации	37
5.7	Аутентификация личности	39
5.7.1	Аутентификация с помощью сопоставления 1:1	39
5.7.2	Аутентификация с помощью сопоставления 1:N.....	40
5.7.3	Аутентификация с помощью сопоставления 1:1 и 1:N.....	40
Раздел 6	Работа клиента.....	42
6.1	Регистрация пользователя и вход в систему.....	42
6.2	Настройки системы	43
6.3	Управление доступом	43
6.3.1	Добавление устройства управления доступом	44

6.3.2	Просмотр состояния устройства	60
6.3.3	Редактирование основной информации	61
6.3.4	Настройки сети	61
6.3.5	Настройка терминала распознавания лиц	63
6.3.6	Настройки процесса захвата изображений	65
6.3.7	Настройки RS-485.....	66
6.3.8	Настройки интерфейса Wiegand	67
6.3.9	Установка нескольких сетевых адаптеров.....	68
6.3.10	Настройка терминала распознавания лиц.....	68
6.3.11	Удаленная настройка	69
6.4	Управление организациями	80
6.4.1	Добавление организации	80
6.4.2	Изменение параметров и удаление организаций	80
6.5	Управление пользователями:	81
6.5.1	Добавление пользователя	81
6.5.2	Управление пользователями.....	94
6.5.3	Выпуск карт в пакетном режиме.....	95
6.6	Графики и шаблоны.....	97
6.6.1	Недельный график работы	98
6.6.2	Группа нерабочих дней	99
6.6.3	Шаблоны	101
6.7	Настройка разрешений.....	103
6.7.1	Добавление разрешений.....	103
6.7.2	Назначение разрешения.....	104
6.8	Расширенные функции	105
6.8.1	Параметры контроля доступа.....	106
6.8.2	Аутентификация при помощи устройства для считывания карт.....	110
6.8.3	Множественная аутентификация.....	111
6.8.4	Открытие двери первой картой	114
6.8.5	Защита от обхода системы безопасности	115
6.9	Поиск события управления доступом	116
6.9.1	Поиск локального события управления доступом	117
6.9.2	Поиск удаленного события управления доступом.....	118
6.10	Конфигурация событий управления доступом.....	118
6.10.1	Привязка событий управления доступом	118
6.10.2	Привязка к событиям карты	120
6.10.3	Перекрестная привязка устройств	122

6.11	Управление состоянием двери	124
6.11.1	Контроль группы управления доступом	124
6.11.2	Блокировка точки управления доступом (двери)	125
6.11.3	Настройка длительности состояния	127
6.11.4	Запись информации о считывании карт в режиме реального времени	128
6.11.5	Сигнализация управления доступом в режиме реального времени	129
6.12	Просмотр в режиме реального времени	131
6.12.1	Начало и остановка просмотра в режиме реального времени	131
6.12.2	Ручная запись и захват изображений	131
6.12.3	Другие функции, используемые при просмотре в режиме реального времени ..	134
6.12.4	Управление дверью во время просмотра в режиме реального времени	135
6.13	Управление постановкой на сигнализацию	136
6.14	Учет рабочего времени	136
6.14.1	Управление графиком смен	137
6.14.2	Обработка данных о посещаемости	144
6.14.3	Расширенные настройки	148
6.14.4	Статистика посещаемости	153
Приложение А Советы по сканированию отпечатков пальцев		158
Приложение В Советы по сбору и сравнению изображений лица		159
Приложение С Советы в отношении рабочей среды на месте установки оборудования ...		161
Приложение D Размеры		162

Раздел 1 Обзор

1.1 Введение

Терминал распознавания лиц серии DS-K1T604 является вариантом устройства контроля доступа для распознавания лиц, которое главным образом применяется в системах обеспечения безопасности, таких как логистические центры, аэропорты, университетские городки, диспетчерские центры пожарной безопасности, жилые дома и т. д.

1.2 Особенности продукта

- 7-дюймовый сенсорный ЖК-экран с соотношением сторон 16:9 и разрешением 1024 × 600 пикселей для отображения интерфейса, обнаружения лиц в режиме реального времени, просмотра видео в режиме реального времени и т. д.
- Широкоугольный объектив с разрешением 2 000 000 пикселей
- Ручная или автоматическая регулировка яркости подсветки
- Аутентификация по QR-коду
- Расстояние распознавания лиц: 0,3... 1 м
- Предполагаемая высота распознавания лиц: 1,4... 1,9 м
- Обнаружение живых лиц: Обнаружение и распознавание происходит только для живых лиц
- Алгоритм глубинного обучения
- Хранение не более 10 000 изображений лиц
- Несколько режимов аутентификации:

Карта, карта и пароль, карта или пароль, отпечаток пальца, отпечаток пальца и пароль, отпечаток пальца или карта, отпечаток пальца и карта, отпечаток пальца и карта с паролем, карта или отпечаток пальца либо лицо или пароль, лицо и отпечаток пальца, лицо и пароль, лицо, идентификатор сотрудника и пароль, отпечаток пальца или пароль, идентификатор сотрудника и отпечаток пальца, идентификатор сотрудника и отпечаток пальца с паролем, карта и отпечаток пальца вместе с лицом, лицо и отпечаток пальца с паролем, идентификатор сотрудника и лицо, лицо и отпечаток пальца м паролем, идентификатор сотрудника и лицо , лицо или отпечаток пальца, карта или лицо или пароль

Примечание. Только продукты с модулем отпечатка пальца поддерживают функцию сканирования отпечатков пальцев.

- Продолжительность распознавания лиц составляет $\leq 0,5$ с/пользователь; точность распознавания лиц — $\geq 99\%$
- Управление параметрами устройства, поиск и настройки

- Импортирует пользовательские данные и данные карты на устройство через протокол TCP/IP или USB-накопитель
- Автономная работа
- Передача данных (результатов проверки подлинности и захваченных изображений) в клиентское программное обеспечение через TCP/IP и сохранение данных в клиентском программном обеспечении
- Привязка и сохранение захваченных изображений
- Импорт данных (изображений лиц и шаблонов лиц) на устройство с помощью USB-накопителя или из клиентского программного обеспечения
- Экспорт данных (изображений лиц, событий и снимков) с устройства при помощи USB-накопителя
- Управление, поиск и установка данных устройства после регистрации на сервере системы
- Подключение к одному внешнему устройству для считывания карт или контроллеру доступа по протоколу RS-485
- Подключение к контроллеру внешнего доступа или интерфейсу Wiegand через протокол Wiegand
- Подключение к блоку управления дверью по протоколу RS-485 во избежание открытия двери в случае уничтожения терминала
- Двусторонняя аудиосвязь

Раздел 2 Внешний вид

Подробную информацию о терминале распознавания лиц см. ниже.

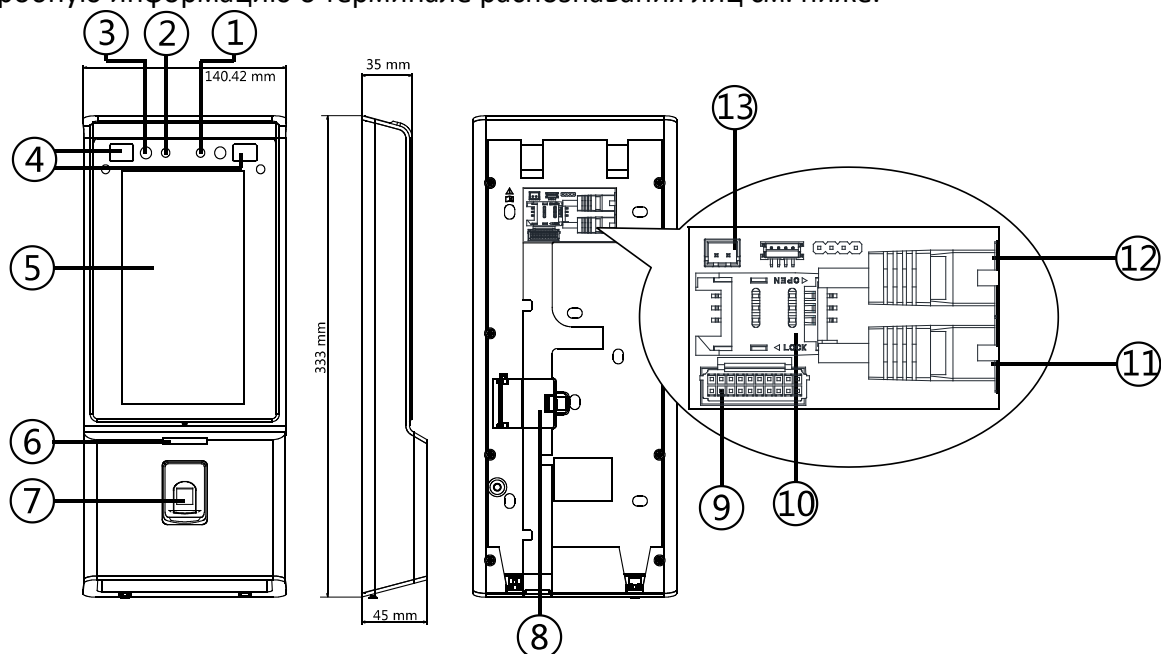


Таблица 1.1 Описание терминала распознавания лиц

№	Название	Описание
1	Камера (Белый свет)	Камера белого света для записи или съемки видео или изображений при белом свете.
2	Камера (ИК-свет)	Камера ИК-света для записи или съемки видео или изображений в ИК-свете.
3	Дополнительная подсветка (ИК-свет)	Дополнительная подсветка для ИК-камеры.
4	Дополнительная подсветка (Белый свет)	Дополнительная подсветка для камеры белого света.
5	Экран	7-дюймовый сенсорный ЖК-экран с разрешением 1024 × 600.
6	Индикатор	Непрерывное свечение красным цветом: Режим ожидания.
		Мигание красным цветом: Ошибка при аутентификации.
		Непрерывное свечение зеленым цветом: Аутентификация пройдена успешно.

Терминал распознавания лиц

Руководство пользователя

		Мигание зеленым цветом: Аутентификация (комбинированная).
7	Модуль отпечатков пальцев + зона считывания карты	Сканирование отпечатков пальцев или считывание карт. Примечание. Этот элемент есть только на устройствах с функцией сканирования отпечатков пальцев.
	Зона считывания карты	Зона для проведения карты. Примечание. Этот элемент есть только на устройствах без функции сканирования отпечатков пальцев.
8	Разъем для PSAM-карты	Вставка PSAM-карты. PSAM-карта представляет собой карту с модулем безопасного доступа, который поддерживает несколько методов безопасного предоставления доступа и разрешений. Она также обеспечивает установление безопасной связи.
9	Клеммы	Подключение к другим внешним устройствам, включая считыватель карт RS-485, считыватель карт Wiegand, дверной замок, вход/выход сигнала тревоги и т. д.
10	Слот (гнездо) для Micro SIM-карты	Обеспечивает возможность использования SIM-карты.
11	Сетевой интерфейс	Подключение к сети Ethernet.
12	Сетевой интерфейс	Подключение к сети Ethernet.
13	Интерфейс подачи питания	Подключение к источнику питания.

Раздел 3 Монтаж

Параметры места установки:

- При установке в помещении устройство должно находиться на расстоянии не менее 2 м от источника света и не менее 3 м от окна или двери.
- Убедитесь, что уровень освещенности в помещении превышает 100 лк.

Примечание. Подробную информацию о месте установки устройства см. в *0. Советы в отношении рабочей среды на месте установки оборудования*.

Типы монтажа: Монтаж на стене с использованием установочной коробки и без нее.

3.1 Монтаж с использованием установочной коробки

Инструкция:

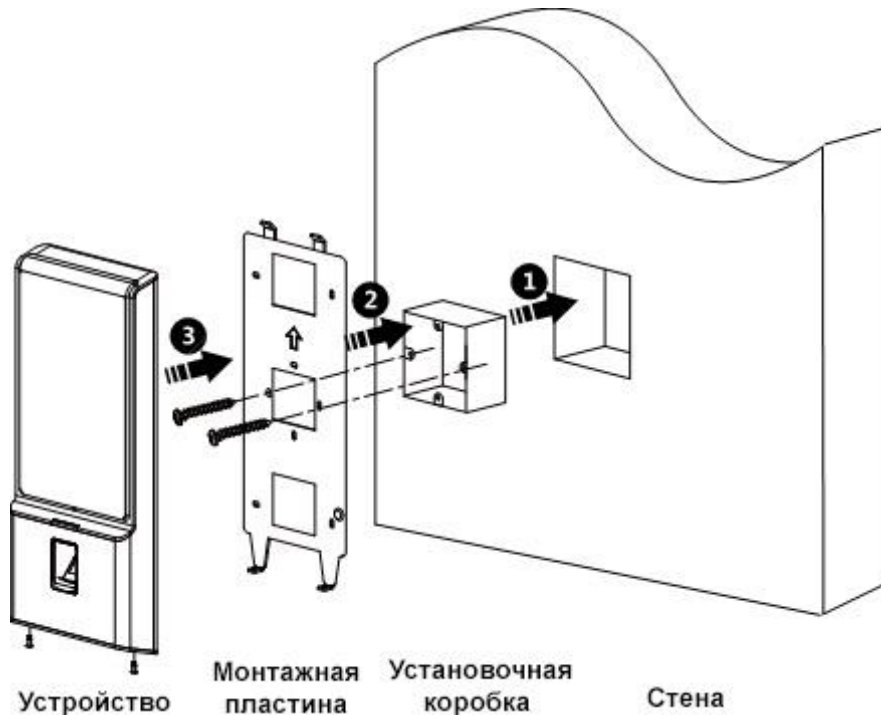
1. Используя базовую линию на монтажном шаблоне, закрепите его на стене или другой поверхности, расположив на высоте 1,3 м от уровня земли.



2. Просверлите отверстия в стене или другой поверхности, используя монтажный шаблон, и установите коробку (размером 80 мм × 80 мм).
3. Прикрепите монтажную пластину к коробке с помощью двух винтов, которые входят в комплект поставки.
4. Используя четыре других винта, поставляемых вместе с устройством, закрепите монтажную пластину на стене.
5. Выкрутите винт в нижней части устройства.
6. Совместите терминал с монтажной панелью и соедините их вместе.
7. Затяните винт в нижней части устройства с помощью шестигранного ключа.

Примечания.

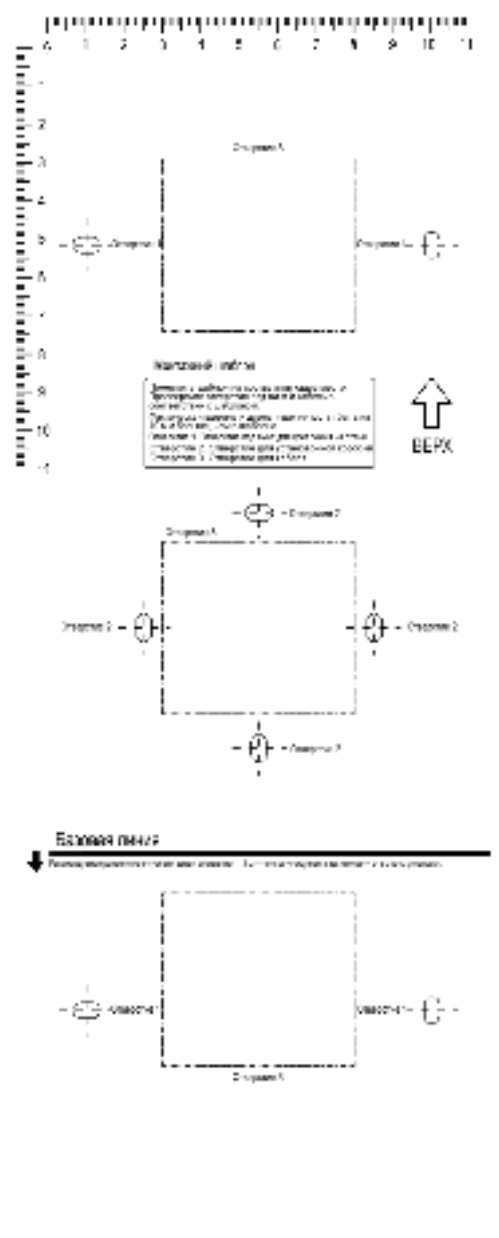
- Высота установки является рекомендуемой величиной. Ее можно изменить в соответствии с фактическими потребностями.
- Чтобы упростить процесс установки, просверлите в монтажной поверхности отверстия, используя прилагаемый шаблон.



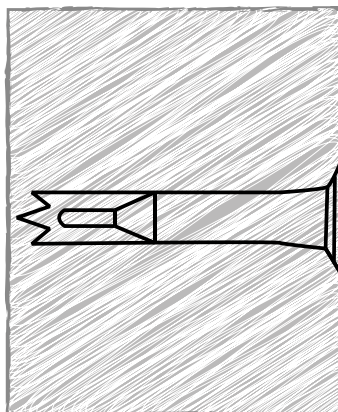
3.2 Монтаж без установочной коробки

Инструкция:

1. Используя базовую линию на монтажном шаблоне, закрепите его на стене или другой поверхности, расположив на высоте 1,3 м от уровня земли.



2. Просверлите 4 отверстия в стене или другой поверхности, сверяясь с положением Отверстия 1 на монтажном шаблоне.
3. Вставьте в просверленные отверстия дюбели для установочных винтов.

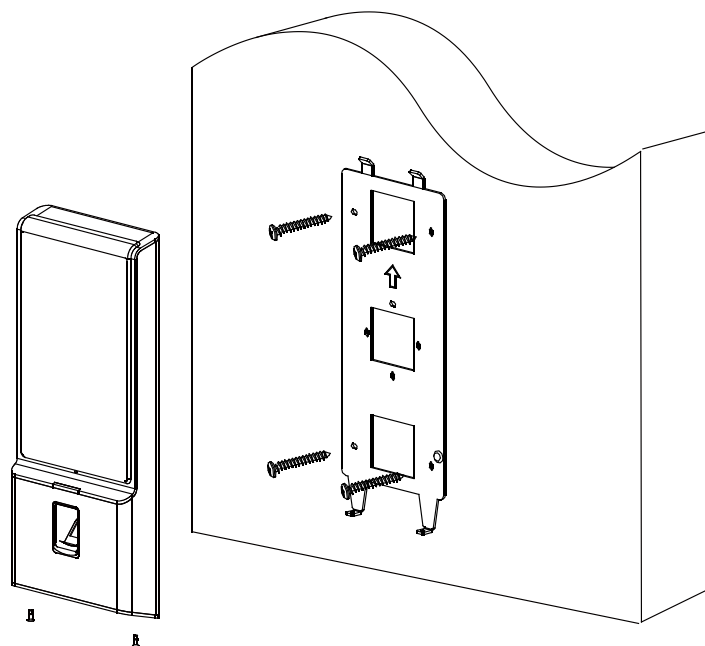


4. Совместите 4 отверстия монтажной пластины с просверленными отверстиями.

Терминал распознавания лиц

Руководство пользователя

5. Вкрутите винты в дюбели на стене или другой поверхности.
6. Выкрутите два винта из нижней части устройства.
7. Совместите терминал с монтажной панелью и соедините их вместе.
8. Затяните винт в нижней части устройства с помощью шестигранного ключа.



Раздел 4 Подключение терминала

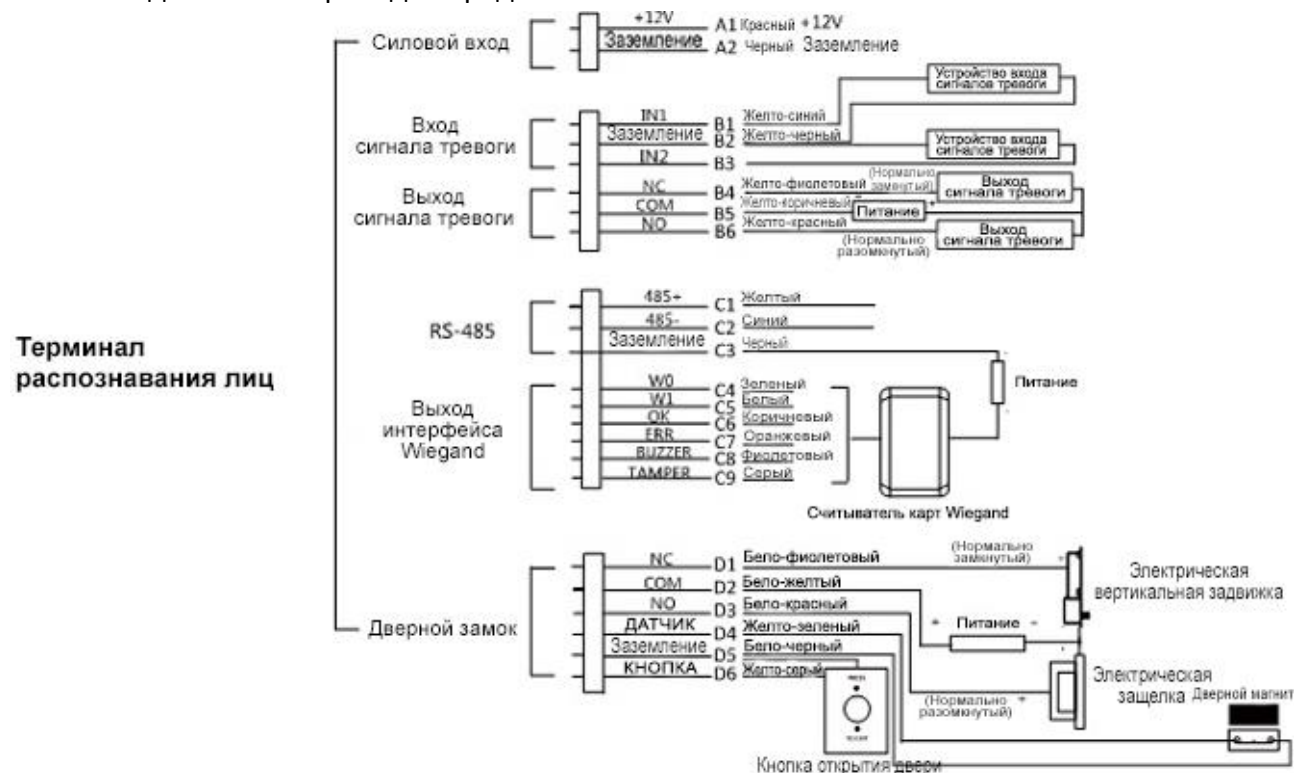
Вы можете подключить клемму RS-485 к считывателю карт RS-485, клеммы NC и COM — к замку двери, клемму **SENSOR (ДАТЧИК)** — к магнитному датчику двери, клемму **BUTTON/GND (КНОПКА/ЗАЗЕМЛЕНИЕ)** — к кнопке открытия двери, клеммы входа/выхода сигнала тревоги — к устройствам входа/выхода сигнализации, клемму Wiegand — к считывателю карт Wiegand или контроллеру доступа.

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

Примечания.

- При использовании кабелей сечением 1,0 мм² необходимо применять источник питания 12 В, который обеспечивает возможность переключения режимов. Расстояние между источником питания и устройством должно составлять не более 20 м.
- При использовании кабелей сечением 1,5 мм² необходимо применять источник питания 12 В, который обеспечивает возможность переключения режимов. Расстояние между источником питания и устройством должно составлять не более 30 м.

Способ подключения проводки представлен ниже:



Также можно подключить терминал к блоку управления дверью. Способ подключения проводки представлен ниже:

Терминал распознавания лиц

Руководство пользователя

Терминал распознавания лиц



Примечание. Блок управления дверью необходимо отдельно подключить к внешнему источнику питания.

Раздел 5 Основные операции

5.1 Активация устройства

Назначение:

Перед использованием терминал нужно активировать.

Активацию можно выполнить через устройство, с помощью ПО SADP, а также с помощью клиентского программного обеспечения.

Стандартные значения для терминала управления указаны ниже.

- Стандартный IP-адрес: 192.0.0.64.
- Стандартный номер порта: 8000.
- Стандартным именем пользователя является *admin*.

5.1.1 Активация при помощи устройства

Если устройство еще не было активировано, это можно сделать после включения.

Инструкция:

1. Перейдите в поле **Password (Пароль)** и создайте пароль.
2. Перейдите в поле **Confirm (Подтвердить)** и снова введите пароль.
3. Нажмите кнопку **Activate (Активировать)**, и устройство включится.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.

5.1.2 Активация при помощи программного обеспечения SADP

Назначение:

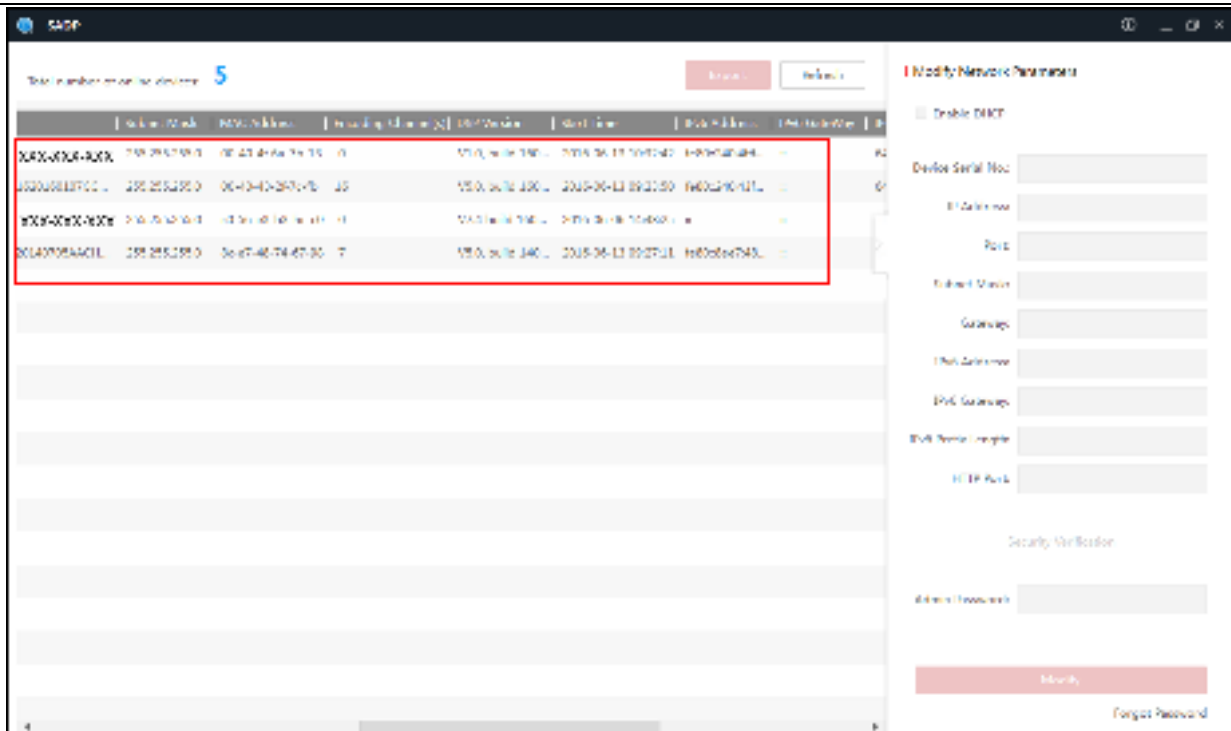
ПО SADP используется для обнаружения устройств в сети, их активации и сброса пароля.

Установите программу SADP с диска, который входит в комплект поставки, или загрузите ее с официального веб-сайта и выполните установку, следуя указаниям, которые появляются на экране. Чтобы активировать устройство, выполните соответствующие инструкции.

Инструкция:

1. Запустите программу SADP, чтобы выполнить поиск устройств в сети.
2. Выберите неактивное устройство в соответствующем списке.

Руководство пользователя



3. Введите пароль в соответствующем поле и подтвердите его.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.

4. Нажмите кнопку **Activate (Активировать)**, чтобы активировать устройство.
5. Проверьте работу активированного устройства. Вы можете изменить IP-адрес устройства на тот же сегмент подсети, в котором находится ваш компьютер. Для этого введите IP-адрес вручную или поставьте галочку в пункте Enable DHCP (Включить DHCP).

- Введите пароль и нажмите кнопку **Modify (Изменить)**, чтобы сохранить новый IP-адрес.

5.1.3 Активация при помощи программного обеспечения клиента

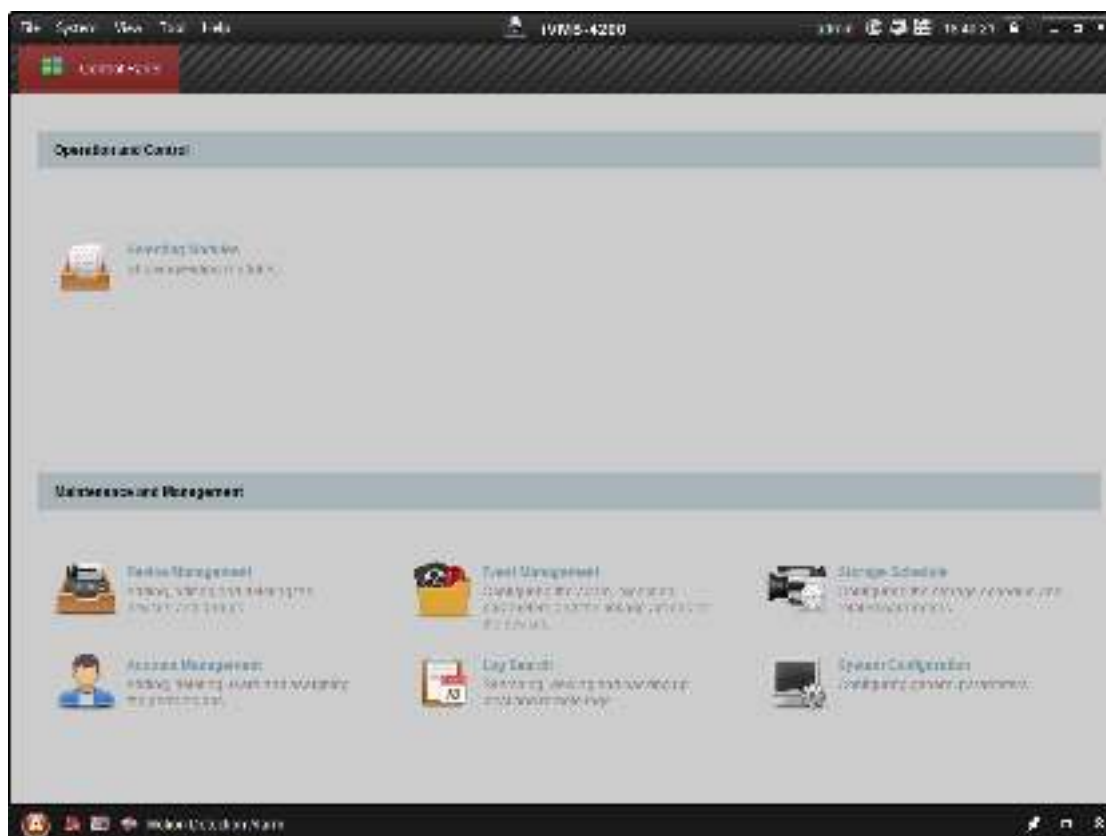
Назначение:

ПО клиента — это многоцелевое программное обеспечение управления видеоданными для множества видов устройств.

Установите ПО клиента с диска из комплекта поставки или загрузите его с официального веб-сайта и установите ПО, следуя подсказкам на экране. Следуйте инструкциям, чтобы активировать панель управления.

Инструкция:

- Запустите ПО клиента. На экране появится панель управления программы, как это показано на приведенном ниже рисунке.



2. Нажмите кнопку **Device Management (Управление устройством)**, чтобы перейти в окно управления устройством.
3. Выберите неактивное устройство в соответствующем списке.

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

4. Выберите неактивное устройство в соответствующем списке.
5. Нажмите кнопку **Activate (Активировать)**, чтобы на экране появилось всплывающее окно активации.
6. Во всплывающем окне создайте пароль, введите его в соответствующее поле и выполните подтверждение.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.



7. Нажмите кнопку **OK**, чтобы начать процесс активации.
8. Нажмите кнопку **Modify Netinfor (Изменить сведения о сети)**, чтобы перейти в окно изменения параметров сети.
9. Измените IP-адрес устройства на тот же сегмент подсети, в котором находится ваш компьютер, введя его вручную.
10. Введите пароль и нажмите кнопку **OK**, чтобы сохранить настройки.

После активации произойдет автоматический переход на начальную страницу.



5.2 Вход в систему

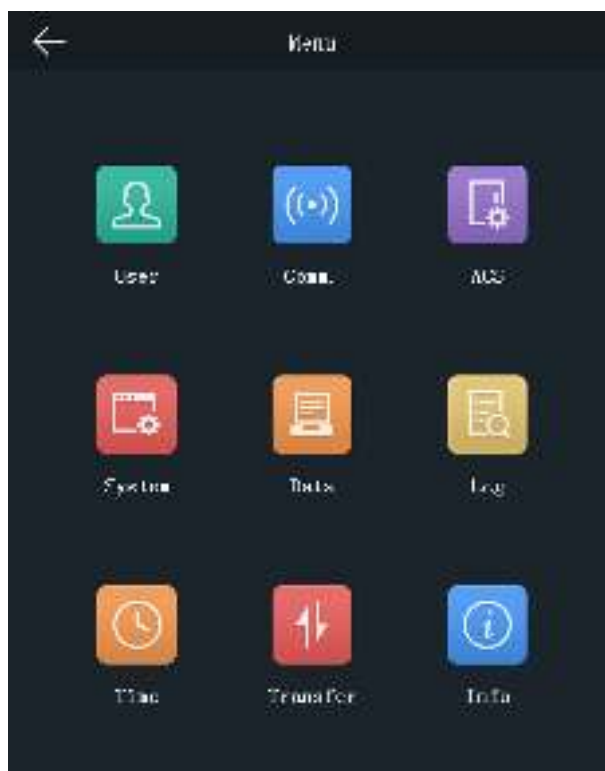
Прежде чем устанавливать параметры устройства, необходимо войти на сервер системы.

Инструкция:

1. Нажмите и удерживайте кнопку начальной страницы в течение 3 с, чтобы открыть на экране окно ввода пароля.
2. Перейдите в поле **Password (Пароль)** и введите пароль активации устройства.

Примечание. Здесь вводится пароль активации.

3. Нажмите кнопку **OK**, чтобы перейти на главную страницу.



Примечания.

- После 5 неудачных попыток ввода пароля устройство будет заблокировано на 30 минут.
- Подробную информацию о настройке режима аутентификации администратора см. в 5.4.1 Добавить пользователя.

5.3 Настройка общих параметров

5.3.1 Настройки связи

Назначение:

Вы можете задать параметры сети, Wi-Fi, RS-485 и интерфейса Wiegand на странице настроек связи.

Нажмите кнопку **Comm. (Communication Settings) (Связь (Настройки связи))** на главной

странице, чтобы перейти на страницу настроек связи.

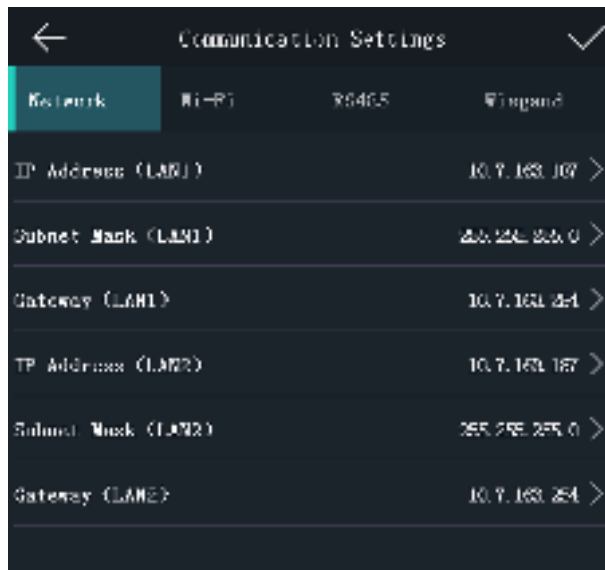
Настройка параметров сети

Назначение:

Здесь можно настроить параметры сети устройства, в том числе IP-адрес, маску подсети, адрес шлюза.

Инструкция:

1. На странице **Communication Settings (Настройки связи)** нажмите кнопку **Network (Сеть)**, чтобы перейти на соответствующую вкладку.



2. Настройте параметры сети, включая IP-адрес, маску подсети и шлюз.

Примечания.

- IP-адреса устройства и компьютера должны находиться в одной локальной сети.
- Чтобы избежать конфликта IP-адресов, IP-адрес сетевого интерфейса 1 должен отличаться от IP-адреса сетевого интерфейса 2, если необходимо применить их оба.

3. Нажмите кнопку **✓**, чтобы сохранить параметры сети.

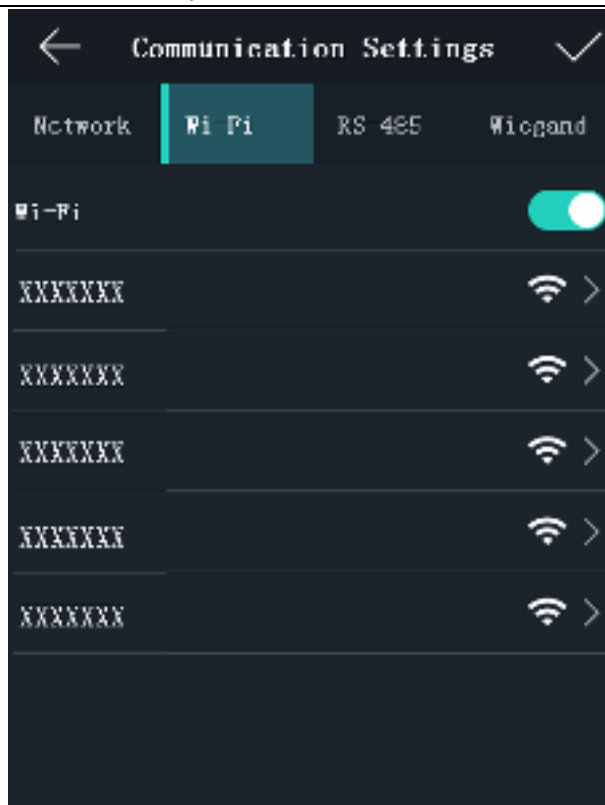
Настройка параметров сети Wi-Fi

Назначение:

Здесь можно активировать сеть Wi-Fi и настроить ее параметры. После завершения процесса настройки параметров Wi-Fi, для подключения и управления устройством можно использовать мобильный APP на мобильном телефоне. Подробную информацию см. в соответствующем руководстве пользователя мобильного клиента.

Инструкция:

1. На странице **Communication Settings (Настройки связи)** нажмите кнопку **Wi-Fi**, чтобы перейти на соответствующую вкладку.
2. Нажмите на ползунок, чтобы включить функцию Wi-Fi.
На экране появится список всех подключенных сетей Wi-Fi.

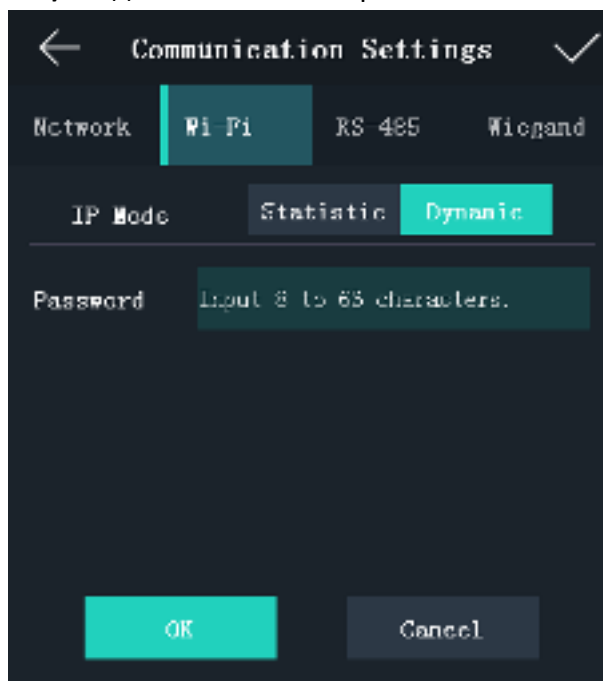


3. Выберите сеть Wi-Fi из списка — после этого на экране откроется окно настроек параметров Wi-Fi.

4. Выберите режим IP.

При выборе значения **Static (Статический)** вы должны ввести пароль Wi-Fi, IP-адрес, маску подсети и шлюз.

При выборе значения **Dynamic (Динамический)** вы должны ввести пароль Wi-Fi.



Примечание. В пароле Wi-Fi можно использовать цифры, заглавные/строчные буквы и специальные символы.

5. Нажмите кнопку **OK**, чтобы сохранить настройки и вернуться на вкладку Wi-Fi.

Если подключение к Wi-Fi было успешно выполнено, справа от названия сети Wi-Fi появится символ ✓.

6. Нажмите кнопку ✓ в верхнем правом углу страницы, чтобы сохранить параметры Wi-Fi.

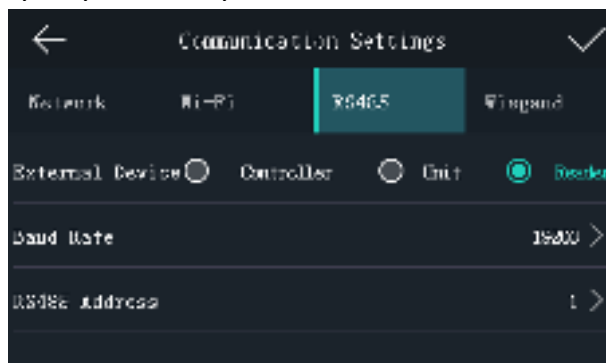
Настройка параметров RS-485

Назначение:

Терминал распознавания лиц можно подключить к внешнему контроллеру доступа, блоку управления дверью или устройству для считывания карт, используя для этого клемму RS-485.

Инструкция:

1. На странице **Communication Settings (Настройки связи)** нажмите кнопку **RS-485**, чтобы перейти на соответствующую вкладку.



2. Выберите требуемое внешнее устройство.

Примечание. **Controller (Контроллер)** — это контроллер доступа, **Unit (Блок)** — блок управления защищенной дверью, а **Reader (Считыватель)** — устройство для считывания карт.

3. Нажмите кнопку **Baud Rate (Скорость передачи данных)**, чтобы перейти на соответствующую страницу.
4. Выберите скорость передачи данных для подключения внешнего устройства по протоколу RS-485.
5. На странице **Commucation Settings (Настройки связи)** выберите адрес RS-485.
6. Нажмите кнопку ✓, чтобы сохранить параметры RS-485 и вернуться на главную страницу.

Примечание. При изменении и сохранении параметров внешнего устройства произойдет его автоматическая перезагрузка.

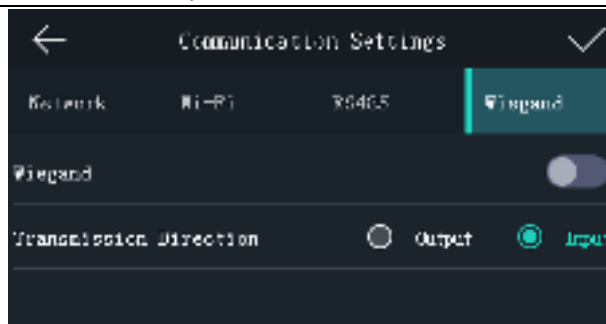
Настройка параметров интерфейса Wiegand

Назначение:

Настройка направления передачи данных и режима работы интерфейса Wiegand.

Инструкция:

1. На странице **Commucation Settings (Настройки связи)** нажмите кнопку **Wiegand**, чтобы перейти на соответствующую вкладку.



2. Нажмите на ползунок, чтобы включить интерфейс Wiegand.

3. Выберите направление передачи данных и режим работы.

Transmission Direction (Направление передачи данных):

- **Output (Вывод):** Терминал распознавания лиц можно подключать к контроллеру внешнего доступа. Эти два устройства будут передавать номер карты через Wiegand 26 или Wiegand 34.
- **Input (Ввод):** Терминал распознавания лиц можно подключать к считывателю карт Wiegand. При этом не нужно выбирать режим работы интерфейса Wiegand.

Mode (Режим):

Здесь можно выбрать Wiegand 26 или Wiegand 34. По умолчанию для терминала выбран режим Wiegand 34.

4. Нажмите кнопку **✓**, чтобы сохранить параметры интерфейса Wiegand и вернуться на главную страницу.

Примечание. При изменении режима работы интерфейса Wiegand и сохранении параметров устройства произойдет автоматическая перезагрузка.

5.3.2 Настройки системы

Назначение:

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

На главной странице нажмите кнопку **System (Системные System Settings) (Система (Настройки системы))**, чтобы перейти на соответствующую страницу.

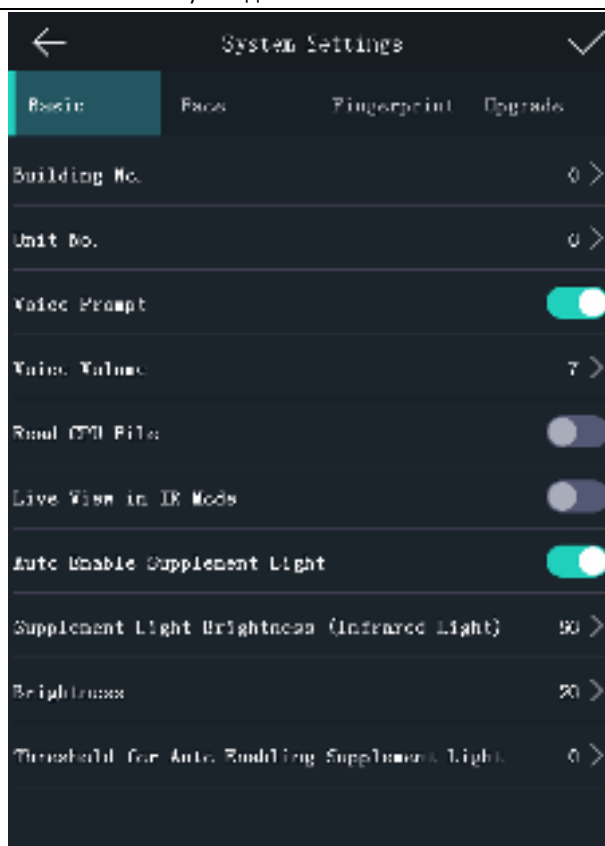
Настройка основных параметров

Назначение:

Вы можете указать этаж и номер здания, настроить голосовую подсказку, громкость голоса, процедуры считывания файла ЦП, просмотра в режиме реального времени с использованием ИК-подсветки, включить подсветку, увеличить ее яркость (инфракрасный свет), а также отрегулировать яркость и порог автоматического включения дополнительной подсветки.

Терминал распознавания лиц

Руководство пользователя



Параметр	Описание
Floor No. (Номер этажа)	Номер этажа, на котором установлено устройство.
Building No. (Номер здания)	Номер здания, на котором установлено устройство.
Voice Prompt (Голосовые подсказки)	Нажмите кнопку  или  , чтобы включить или выключить голосовые подсказки.
Voice Volume (Громкость звука)	Регулировка громкости голоса. Чем больше значение, тем громче голос.
Read CPU File (Считывание файла ЦП)	Если характеристики модели позволяют, при включении этой функции устройство сможет считывать информацию с процессорной карты.
Live View in IR Mode (Просмотр в режиме реального времени с использованием ИК-подсветки)	Изображение в режиме реального времени на экране устройства перейдет в режим использования ИК-подсветки.
Auto Enable Supplement Light (Автоматическое включение)	Если включить эту функцию, дополнительная подсветка автоматически включается, когда становится слишком темно. Если отключить эту функцию, дополнительная подсветка будет включена постоянно.

Терминал распознавания лиц

Руководство пользователя

дополнительной подсветки)	
Supplement Light Brightness (Infrared Light) (Яркость дополнительной подсветки (ИК свет))	Яркость ИК-подсветки, когда она включена.
Brightness (Яркость)	Яркость дополнительной подсветки. Значение яркости выбирается в диапазоне 0... 100. При выборе значения 0 лампочка выключается. 1 — самая низкая яркость, 100 — самая высокая.
Threshold for Auto Enable Supplement Light Brightness (Пороговое значение автоматического включения подсветки)	Дополнительная подсветка будет включаться автоматически, когда фактическое значение освещенности опуститься ниже заданного порога.

Настройка параметров лица

Назначение:

Вы можете установить порог опознавания лица 1:N, порог опознавания лица 1:1, обнаружение лиц в режиме реального времени, минимальную область обнаружения (ширина), минимальную область обнаружения (высота), минимальную ширину обнаружения (приближение), границу (слева) границу (сверху), границу (справа), границу (снизу), угол наклона, угол рыскания, межцентровое расстояние между зрачками и степень соответствия.



Параметр	Описание
1:N Security Level (Уровень безопасности 1:N)	Установка порога опознавания при распознавании в режиме 1:N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение составляет 84.
1:1 Security Level (Уровень безопасности 1:1)	Установка порога опознавания при распознавании в режиме 1:1. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение составляет 75.
Live Face Detection (Обнаружение живых лиц)	Включение и выключение функции обнаружения живых лиц. Если активировать эту функцию, устройство будет определять, живое лицо на изображении или нет.
Min. Detection Area (Width) (Минимальная область обнаружения (ширина))	Если расстояние между камерой и пользователем слишком велико, параметр представляет собой минимальный процент ширины лица от общей ширины области распознавания. Чтобы произвести опознавание лица, фактический процент должен быть больше, чем заданное значение.

Терминал распознавания лиц

Руководство пользователя

Параметр	Описание
	Другие процентные значения, расстояния и углы в этой таблице также должны соответствовать заданным условиям. Рекомендуемое значение: 14
Min. Detection Area (Height) (Минимальная область обнаружения (высота))	Если расстояние между камерой и пользователем слишком велико, параметр представляет собой минимальный процент высоты лица от общей высоты области распознавания. Чтобы произвести опознавание лица, фактический процент должен быть больше, чем заданное значение. Другие процентные значения, расстояния и углы в этой таблице также должны соответствовать заданным условиям. Рекомендуемое значение: 12
Min. Detection Width (Close to) (Минимальная ширина обнаружения (приближение))	Если расстояние между камерой и пользователем слишком мало, параметр представляет собой минимальный процент ширины лица от общей ширины области распознавания. Чтобы произвести опознавание лица, фактический процент должен быть больше, чем заданное значение. При таком условии устройство не будет выявлять другие параметры.
Margin (Left) (Граница (слева))	Расстояние от левого края лица до левого края области распознавания. Чтобы произвести опознавание лица, фактическое расстояние должно быть больше, чем заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.
Margin (Top) (Граница (сверху))	Расстояние от верхнего края лица до верхнего края области распознавания. Чтобы произвести опознавание лица, фактическое расстояние должно быть больше, чем заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.
Margin (Right) (Граница (справа))	Расстояние от правого края лица до правого края области распознавания. Чтобы произвести опознавание лица, фактическое расстояние должно быть больше, чем заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.
Margin (Bottom) (Граница (снизу))	Расстояние от нижнего края лица до нижнего края области распознавания. Чтобы произвести опознавание лица, фактическое

Терминал распознавания лиц

Руководство пользователя

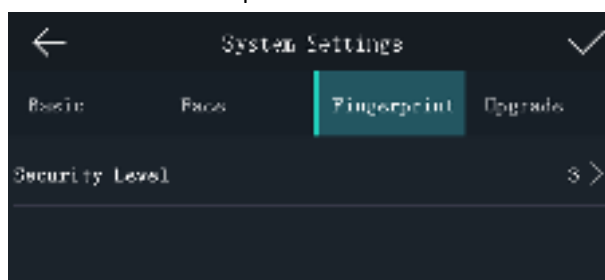
Параметр	Описание
	расстояние должно быть больше, чем заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.
Pitch Angle (Угол наклона)	Максимальный угол наклона в начале процедуры распознавания лиц. По умолчанию этот угол равен 30°.
Yaw Angle (Угол рыскания)	Максимальный угол рыскания в начале процедуры распознавания лиц. По умолчанию этот угол равен 45°.
Pupillary Distance (Межцентровое расстояние)	Минимальное расстояние между центрами двух зрачков при распознавании лица. Фактическое расстояние должно быть больше, чем заданное значение. По умолчанию это значение равняется 40.
Score (Степень соответствия)	Установка степени соответствия лица при распознавании. Устройство оценивает снятое изображение в соответствии с углом рыскания, углом наклона и межцентровым расстоянием. Если оценка будет меньше заданного значения, распознавание лица считается неудачным.

Установка параметров отпечатков пальцев

Назначение:

В этом разделе можно установить уровень безопасности при распознавании отпечатков пальцев.

Примечание. Распознавание отпечатков пальцев выполняется только на устройствах с функцией сканирования отпечатков пальцев.



Параметр	Описание
Security Level (Уровень безопасности):	Вы можете выбрать уровень безопасности процедуры распознавания отпечатков пальцев. Чем выше уровень безопасности, тем ниже коэффициент ложной идентификации (КЛИ). Чем выше уровень безопасности, тем выше коэффициент ошибочного отклонения (КОО).

Обновление прошивки

На странице **Upgrade (Обновление)** подключите USB-накопитель и нажмите кнопку **Start (Пуск)**. Устройство автоматически считывает файл обновления с USB-накопителя и обновит прошивку.

Примечание.

- Файл обновления должен находиться в корневом каталоге.
- Он должен называться digicap.dav.



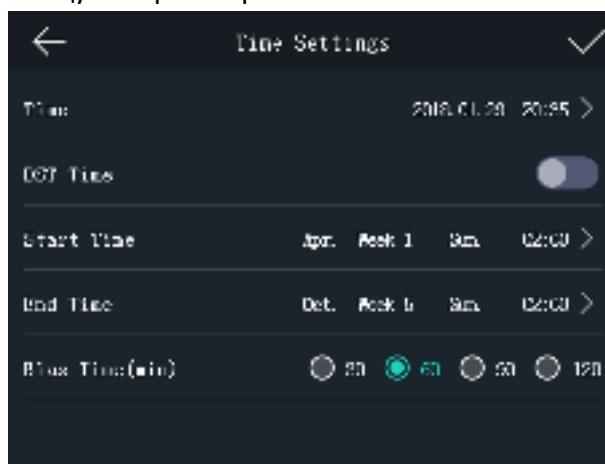
5.3.3 Настройка времени

Назначение:

В этом разделе вы можете задать время устройства и выбрать настройки перехода на летнее время.

Инструкция:

1. Нажмите кнопку **Time (Time Settings) (Время (Настройки времени))** на главной странице, чтобы перейти на страницу настроек времени.



2. Измените параметры времени.

Параметр	Описание
----------	----------

Time (Время)	Настройка времени, которое будет отображаться на экране устройства.
DST (Переход на летнее время)	Включение и выключение функции перехода на летнее время. Если активировать функцию перехода на летнее время, можно установить время начала периода летнего времени, время его окончания и величину смещения. Start Time (Время начала): Установка начала периода летнего времени. End Time (Время окончания): Установка окончания периода летнего времени. Bias Time (Смещение): Выбор величины смещения при переходе на летнее время.

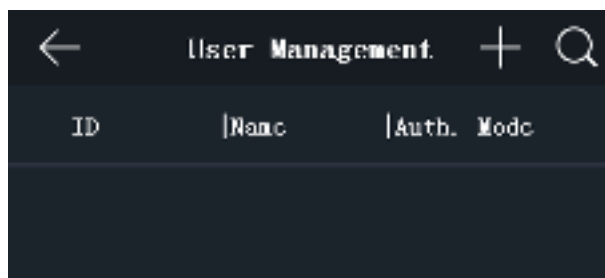
3. Нажмите кнопку , чтобы сохранить параметры и вернуться на главную страницу.

5.4 Управление пользователями

Назначение:

В интерфейсе управления пользователями можно добавлять, редактировать, удалять пользователей и выполнять поиск.

Нажмите кнопку **User (Пользователь)** на главной странице, чтобы перейти на страницу управления пользователями.



5.4.1 Добавление пользователей

Назначение:

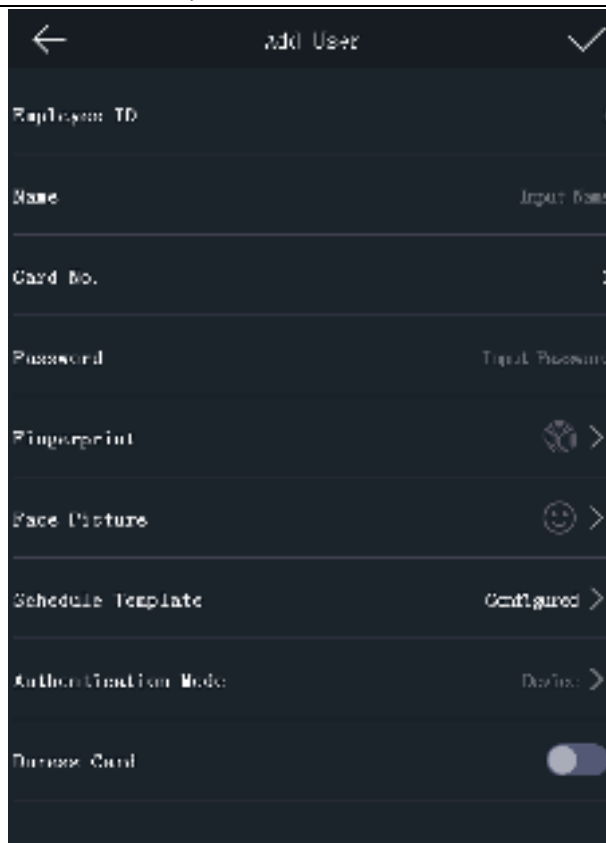
На странице **Add User (Добавить пользователя)** можно добавлять пользователей, включая номер сотрудника, имя, номер карты. Можно также связать отпечаток пальца, изображение лица с пользователем или установить пароль, режим проверки подлинности, шаблон расписания, разрешение администратора для пользователя.

Примечания.

- Можно добавить до 50000 пользователей.
- Устройство с моделью DS-K1T604M не поддерживает функцию распознавания отпечатка пальца.

Инструкция:

1. На странице **User Management (Управление пользователями)** нажмите кнопку +, чтобы перейти на страницу добавления пользователя.



2. Перейдите в поле **Employee ID (Идентификатор сотрудника)** и отредактируйте идентификатор сотрудника.

Примечания.

Идентификатор сотрудника должен находиться в диапазоне 1... 999999999. Идентификатор сотрудника не может начинаться на 0, а также не может повторяться.

3. Перейдите в поле **Name (Имя)** и введите на экранной клавиатуре имя пользователя.

Примечания.

- В имени пользователя могут быть цифры, заглавные/строчные буквы и специальные символы.
- Имя пользователя может содержать до 32 символов.

4. Перейдите в поле **Card (Карта)** и введите номер карты.

Способ 1. Введите номер карты вручную.

Способ 2: Проведите картой в области считывания, чтобы считать ее номер.

Примечания.

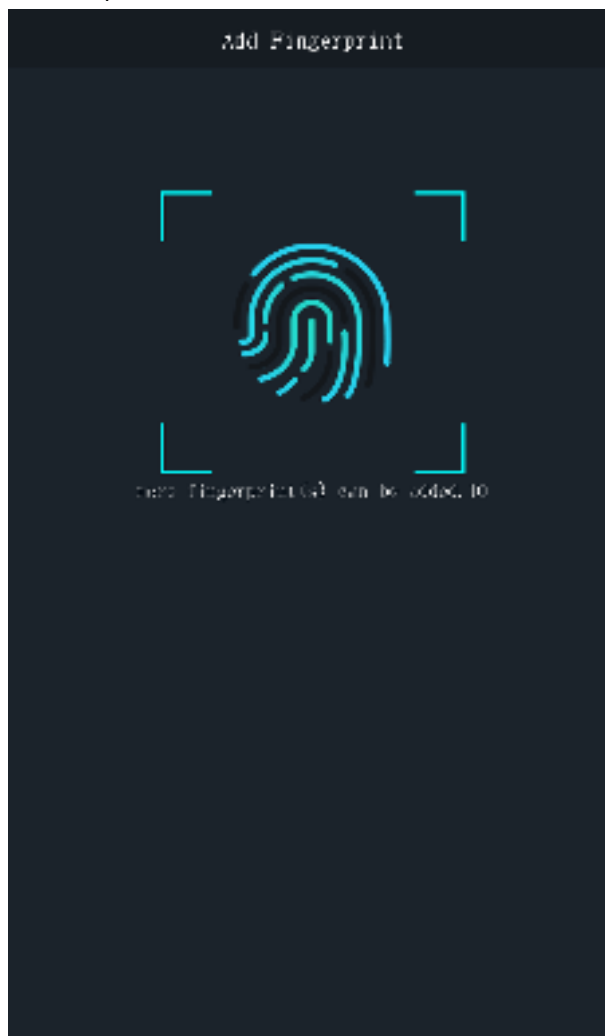
- Поле с номером карты должно быть заполнено.
- Номер карты может содержать до 20 символов.
- По умолчанию номер карты состоит из 10 символов. Система автоматически дополнит нулями 10-символьные номера. Например, 5 и 0000000005 — это два разных номера карты.
- Номер карты не должен повторяться.

5. Перейдите в поле **Password (Пароль)** и создайте пароль, а затем подтвердите его.

Примечание.

- В пароле можно использовать только числа.
- Длина пароля не должна превышать 8 символов.

6. Перейдите в поле **Fingerprint (Отпечаток пальца)**, чтобы на экране появилась страница добавления отпечатка пальца.



Чтобы добавить отпечаток пальца, следуйте инструкциям, приведенным ниже.

- 1) Поместите палец на модуль распознавания отпечатков.
- 2) Следуйте инструкциям на экране, чтобы выполнить запись отпечатка пальца.
- 3) После завершения процесса добавления отпечатка пальца во всплывающем диалоговом окне нажмите кнопку **Yes (Да)**, чтобы сохранить данный отпечаток и перейти к добавлению следующего.

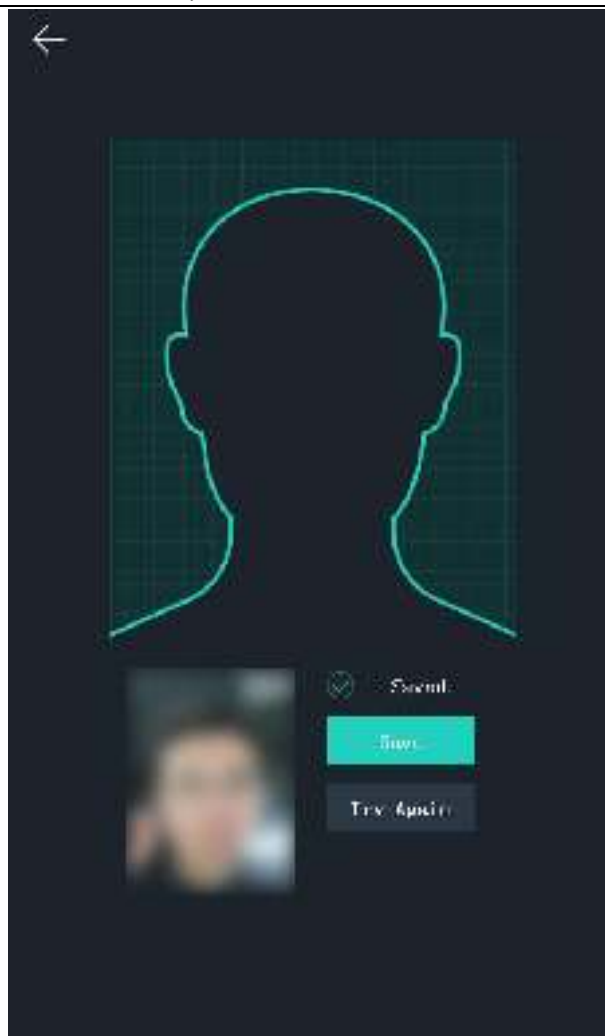
Или нажмите кнопку **No (Нет)**, чтобы сохранить отпечаток пальца и вернуться на страницу добавления пользователя.

Примечания.

- Нельзя зарегистрировать один и тот же отпечаток пальца несколько раз.
- Для одной камеры можно добавить не более 10 отпечатков пальцев.
- Чтобы выполнить запись отпечатков пальцев, можно также использовать клиентское программное обеспечение или специальное устройство.
- Подробные инструкции по сканированию отпечатков пальцев см. в 0.Приложение

А Советы по сканированию **ОТПЕЧАТКОВ ПАЛЬЦЕВ**.

7. Перейдите в поле **Face Picture (Изображение лица)**, чтобы открыть страницу добавления изображений лица.



Чтобы добавить изображение лица пользователя, выполните следующие действия.

- 1) Расположите лицо прямо перед камерой.

Примечание. Перед добавлением изображения лица убедитесь, что оно находится в соответствующем контуре.

После завершения процесса добавления изображений лица на странице появится захваченная картинка.

Примечания.

- Убедитесь в том, что захваченное изображение лица является точным и имеет хорошее качество.
- Подробные инструкции по добавлению изображений лица см. в *0. Советы по сбору и сравнению изображений лица*.

- 2) Чтобы сохранить изображения лица, нажмите кнопку **Save (Сохранить)**.

Или нажмите кнопку **Try Again (Попробовать снова)** и измените положение лица, чтобы повторить процедуру добавления.

Примечание. Максимальная длительность процесса добавления изображений лица составляет 15 с. Время, оставшееся для добавления изображений лица, будет отображаться в левой части страницы.

8. Перейдите в поле **Schedule Template (Шаблон графика)**, чтобы открыть на экране соответствующую страницу. Выберите шаблон графика и нажмите кнопку **✓**, чтобы сохранить настройки.

Примечание. Подробную информацию о настройке шаблона графика см. в *разделе 6.6 Графики и шаблоны*. После включения функции использования на устройстве шаблона графика из клиентского программного обеспечения можно будет выбрать соответствующий шаблон.

9. Включение и выключение функции **Duress Card (Карта принудительного открытия)**. Пока эта функция активирована, к пользователю будут привязаны карты принудительного открытия. Если пользователь проходит процесс аутентификации путем проведения этой карты принудительного открытия, устройство загружает соответствующее событие в клиентское программное обеспечение.
10. Нажмите кнопку **V**, чтобы сохранить параметры пользователя и вернуться на главную страницу.

5.4.2 Управление пользователями

Поиск пользователей

Назначение:

Вы можете искать пользователя в списке в соответствии с идентификатором сотрудника, номером карты или именем.

Инструкция:

1. На странице **User Management (Управление пользователями)** нажмите кнопку , чтобы перейти на страницу поиска пользователя.



2. Нажмите кнопку **Card (Карта)** в левой части страницы и выберите тип поиска из раскрывающегося списка.
3. Перейдите в поле ввода данных и укажите идентификатор сотрудника, номер карты или имя пользователя для осуществления поиска.
4. Нажмите кнопку , чтобы начать поиск.
Результаты поиска будут отображаться в списке, расположенном в нижней части экрана.

Редактирование параметров пользователей

Назначение:

Вы можете отредактировать информацию о добавленном пользователе, выполнив действия, описанные в этом разделе.

Инструкция:

1. На странице **User Management (Управление пользователями)** выберите пользователя, параметры которого необходимо отредактировать, чтобы перейти на страницу **Edit User**

(Редактировать параметры пользователя).

- Описание процедуры редактирования параметров пользователя см. в *разделе 5.4.1 Добавление пользователей*.
- Нажмите кнопку **V**, чтобы сохранить параметры и вернуться на страницу управления пользователями.

Примечание. Идентификатор сотрудника изменить нельзя.

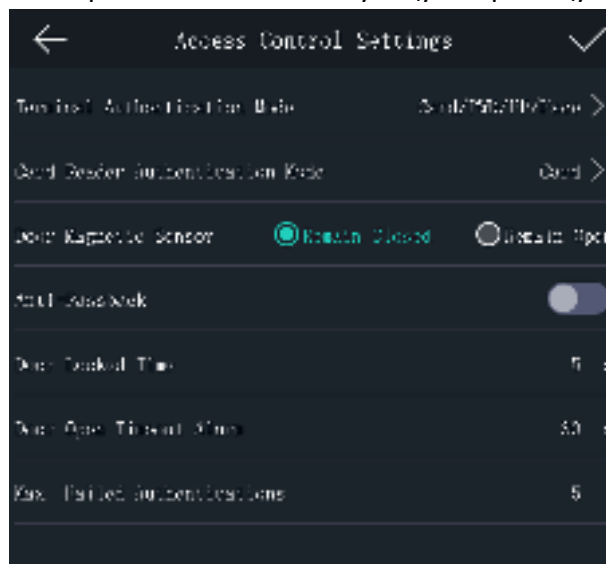
5.5 Настройка параметров управления доступом

Назначение:

Вы можете установить разрешения на управление доступом, включая функции режима аутентификации, магнитного датчика двери, запрета двойного прохода, блокировки времени закрытия, аварийного сигнала превышения времени открытия двери, а также максимальное количество неудачных попыток аутентификации.

Инструкция:

- Находясь на главной странице, нажмите кнопку **ACS (Access Control Settings) (Настройки контроля доступа)**, чтобы перейти на соответствующую страницу.



- Отредактируйте параметры контроля доступа.

Ниже приведено описание доступных для редактирования параметров:

Параметр	Описание
Terminal Authentication Mode (Режим проверки подлинности терминала)	Выбор режима проверки подлинности терминала распознавания лиц. Вы также можете настроить режим проверки подлинности. Примечания. - Распознавание отпечатков пальцев выполняется только на устройствах с функцией сканирования отпечатков пальцев. - Если вам нужно повысить уровень безопасности, не используйте только один режим проверки подлинности.
Card Reader Authentication Mode	Выбор режима аутентификации при помощи устройства для считывания карт.

Параметр	Описание
(Режим аутентификации при помощи устройства для считывания)	
Door Magnetic Sensor (Магнитный датчик двери)	Вы можете выбрать значения Remain Open (Не закрывать) или Remain Closed (Не открывать) , в соответствии с текущими потребностями. По умолчанию выбрано состояние Remain Closed (Не открывать) .
Anti-Passback (Запрет двойного прохода)	При активации функции запрета двойного прохода необходимо задать в клиентском программном обеспечении iVMS-4200 путь к ложному паролю. Человек должен проходить процедуру аутентификации согласно заданному алгоритму. В противном случае аутентификация не будет пройдена.
Door Locked Time (Время блокировки двери)	Установка длительности периода разблокировки двери. Если дверь не открывается в течение заданного времени, она будет заблокирована. Доступный диапазон времени блокировки двери: 1... 255 с.
Door Open Timeout Alarm (Сигнал тревоги о превышении заданного времени открытия двери).	Если дверь не будет закрыта, сработает сигнал тревоги. Допустимый диапазон: 0... 255 с.
Max. Failed Authentications (Максимальное количество неудачных попыток прохождения аутентификации)	Установка максимального количества попыток прохождения аутентификации. Если не удалось выполнить аутентификацию с использованием установленного количества попыток, будет сгенерирован сигнал тревоги.

3. Нажмите кнопку , чтобы сохранить настройки.

5.6 Прочие функции управления

5.6.1 Управление данными

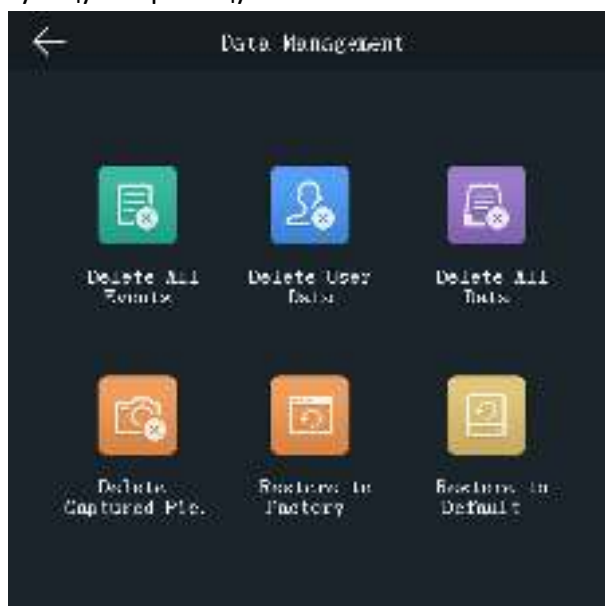
Назначение:

На странице **Data Management (Управление данными)** вы можете удалить все события, данные пользователя, все данные, отменить разрешения, удалить захваченные изображения, восстановить заводские настройки или вернуться к настройкам по умолчанию.

Инструкция:

1. Нажмите кнопку **Data (Data Management) (Данные (Управление данными))**, чтобы

перейти на соответствующую страницу.



2. Управление данными осуществляется при помощи кнопок, расположенных на странице. Ниже приведено описание доступных кнопок:

Параметр	Описание
Delete All Events (Удаление всех событий)	Удаление всех записанных событий с устройства.
Delete User Data (Удаление данных пользователя)	Удаление всех записанных данных пользователя с устройства.
Delete All Data (Удаление всех данных):	Удаление всех записанных событий и данных пользователя с устройства.
Delete Captured Pic. (Удаление захваченных изображений)	Удаление захваченных изображений с устройства.
Restore to Factory (Восстановление заводских настроек)	Восстановление системы до заводских настроек. После этого устройство будет перезагружено.
Restore to Default (Восстановление настроек по умолчанию)	Восстановление системы до настроек по умолчанию. Система сохранит коммуникационные настройки, а также настройки удаленного пользователя. Для других параметров будут восстановлены значения по умолчанию.

3. Во всплывающем окне нажмите кнопку **Yes (Да)**, чтобы завершить процесс настройки.

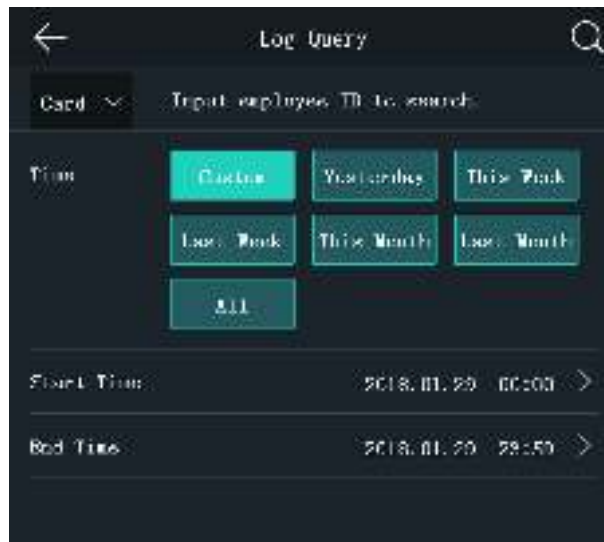
5.6.2 Управление записями в журналах

Назначение:

Вы можете выполнить поиск по журналам проверки подлинности в течение определенного периода времени, указав идентификатор сотрудника, номер карты или имя пользователя.

Инструкция:

1. На главной странице нажмите кнопку **Log (Log Query) (Журнал (Записи журнала))**, чтобы перейти на соответствующую страницу.



2. Нажмите кнопку **Card (Карта)** в левой части страницы и выберите тип поиска из раскрывающегося списка.
3. Перейдите в поле ввода данных и укажите идентификатор сотрудника, номер карты или имя пользователя для осуществления поиска.
4. Выберите время.
Доступны такие варианты: **Custom (Пользовательское)**, **Yesterday (Вчера)**, **This Week (Эта неделя)**, **Last Week (Последняя неделя)**, **This Month (Этот месяц)**, **Last Month (Последний месяц)**, или **All (Все)**.
Если было выбрано значение **Custom (Пользовательское)**, можно установить конкретное начальное и конечное время поиска.
5. Нажмите кнопку , чтобы начать поиск.
После этого на странице появятся результаты поиска.

5.6.3 Импорт/экспорт данных

Назначение:

На странице **Transfer (Передача данных)** можно экспортировать данные о посещаемости, пользовательские данные, изображение пользователя, параметры контроля доступа и захваченное изображение на USB-накопитель. Вы также можете импортировать пользовательские данные, изображение пользователя и параметры управления доступом с USB-накопителя.

Нажмите кнопку **Transfer (Передача данных)** на главной странице, чтобы перейти на

соответствующую страницу.



Экспорт данных

Инструкция:

1. Вставьте USB-накопитель в устройство.
2. На странице **Transfer (Передача данных)** нажмите кнопку **Export Att. Data (Экспорт данных о посещении)**, **Export User Data (Экспорт данных пользователя)**, **Export User Profile Photo (Экспорт фотографии профиля пользователя)**, **Export ACS Parameters (Экспорт параметров контроля доступа)** или **Export Picture (Экспорт изображения)**.
3. Во всплывающем окне нажмите кнопку **Yes (Да)**, и данные будут экспортированы с устройства на USB-накопитель.

Примечания.

- Поддерживается формат USB-накопителя FAT 32.
- Система позволяет использовать USB-накопитель с памятью в диапазоне 1... 32 Гб. Убедитесь в том, что объем свободного места на USB-накопителе составляет более 512 МБ.

Импорт данных

Инструкция:

1. Вставьте USB-накопитель в устройство.
2. На странице **Transfer (Передача данных)** нажмите кнопку **Import User Data (Импорт данных пользователя)**, **Import User Profile Photo (Импорт фотографии профиля пользователя)** или **Import ACS Parameters (Импорт параметров контроля доступа)**.
3. Во всплывающем окне нажмите кнопку **Yes (Да)**, и данные будут импортированы на

устройство с USB-накопителя.

Примечания.

- Перед импортом фотографии профиля вы должны импортировать данные пользователя.
- Поддерживается формат USB-накопителя FAT 32.
- Импортированное изображение должно быть сохранено в корневом каталоге (enroll_pic), а название файла изображения должно формироваться в соответствии со следующим правилом:
Номер карты_Имя_Отдел_Идентификатор_Пол.jpg
- Идентификатор сотрудника должен быть числом в диапазоне 1... 99999999, он не может дублироваться и или начинаться с 0.
- Требования к фотографии. Лицо видно полностью, взгляд направлен прямо в камеру. При фотографировании запрещено надевать шляпу или другой головной убор. Формат фотографии должен быть JPEG или JPG. Разрешение должно быть не менее 640 × 480 пикселей. Размер изображения должен быть в диапазоне 60... 200 КБ.

5.6.4 Просмотр системной информации

Просмотр данных в хранилище

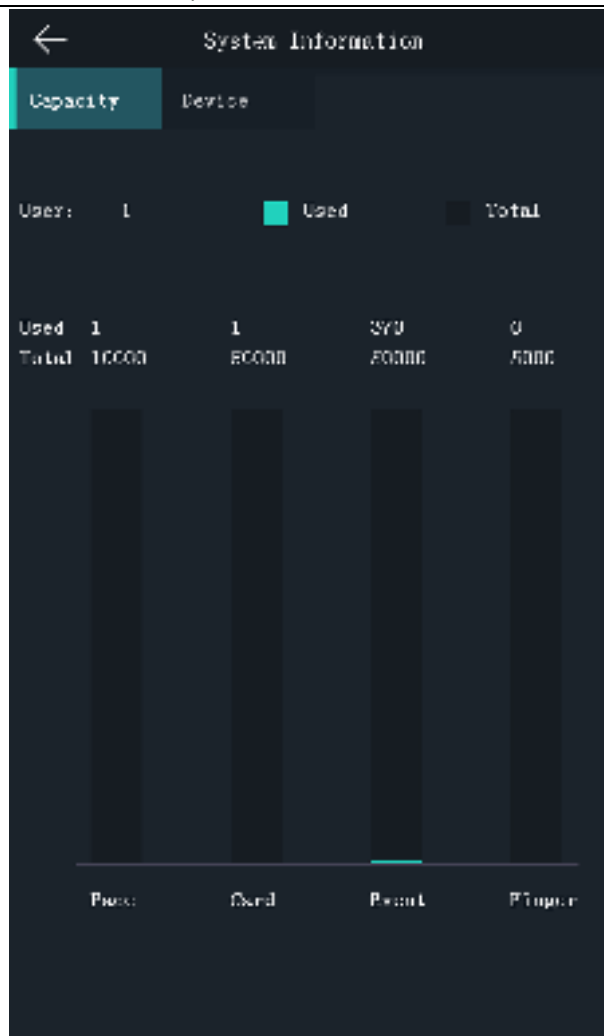
Назначение:

Вы можете просмотреть номер добавленного пользователя, номер лица, номер карты, номер пароля и номер отпечатка.

Примечание. Устройство с моделью DS-K1T604M не поддерживает функцию отображения данных в хранилище отпечатков пальцев.

Выберите пункт **Info. (System Information) (Информация (Системная информация))** ->

Capacity (Хранилище) на главной странице, чтобы перейти на соответствующую страницу.



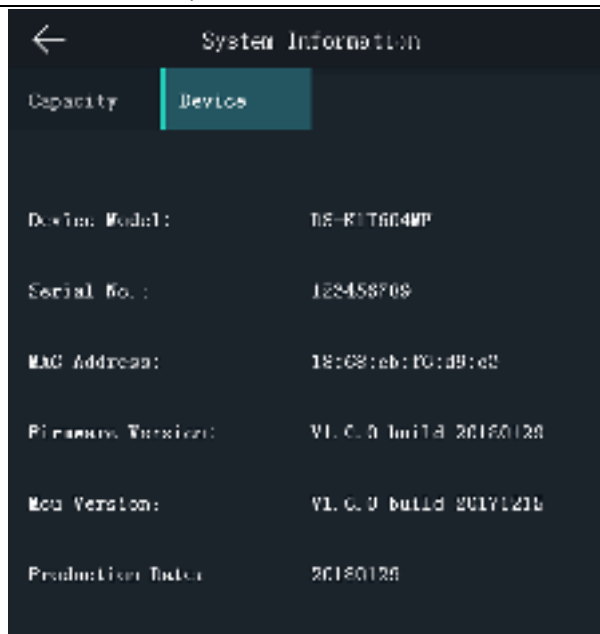
Просмотр информации об устройстве

Назначение:

Вы можете просмотреть модель устройства, серийный номер, MAC-адрес, версию прошивки, версию MCU и дату выпуска.

Нажмите кнопку **Device (Устройство)**, чтобы перейти на соответствующую страницу.

Примечание. Страница информации об устройстве может быть разной в различных моделях.



5.7 Аутентификация личности

Назначение:

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

Система выполнит аутентификацию человека в соответствии с настроенным режимом работы. Вы можете установить личность с помощью сопоставления 1:1 или сопоставления 1:N.

Примечание. Если вам нужно повысить уровень безопасности, не используйте только один режим проверки подлинности.

Сопоставление 1:N: Сравнение захваченного изображения лица или полученного отпечатка пальца со всеми изображениями лиц или всеми фотографиями отпечатков пальцев, хранящимися на устройстве.

Сопоставление 1:1: При использовании карты выполняется сравнение изображения захваченного изображения лица или полученного отпечатка пальца с информацией, хранящейся на устройстве.

5.7.1 Аутентификация с помощью сопоставления 1:1

Инструкция:

1. Если для аутентификации используются карта и лицо, карта и лицо и отпечаток пальца или этот процесс выполняется в автоматическом режиме, проведите карту через устройство для их считывания.

Примечание. Карта может быть обычной интеллектуальной картой или зашифрованной картой.

Если функция сканирования QR-кода включена, вы можете поместить перед камерой устройства QR-код для прохождения аутентификации.

2. Если для аутентификации используются карта и лицо или этот процесс выполняется в

автоматическом режиме, разместите лицо прямо перед камерой для проверки личности. Если для аутентификации используются карта и лицо и отпечаток пальца, после завершения проверки лица отсканируйте свой отпечаток пальца на соответствующем модуле устройства, дождавшись появления на экране сообщения **Continue to authenticate** (Продолжайте аутентификацию).

Если аутентификация прошла успешно, на экране появится сообщение **Authenticated** (Аутентифицировано).

Примечания.

- Чтобы получить оптимальные результаты аутентификации лиц человека, рост пользователя должен составлять 140... 190 см, а расстояние между пользователем и устройством — 30... 100 см.
- Подробную информацию о сканировании отпечатков пальцев см. в [Приложении А. Советы по сканированию отпечатков пальцев.](#)
- Подробную информацию об аутентификации с помощью сканирования лица см. в [Приложении В. Советы по сбору и сравнению изображений лица.](#)

5.7.2 Аутентификация с помощью сопоставления 1:N

Если для аутентификации используется лицо или этот процесс выполняется в автоматическом режиме, разместите лицо прямо перед камерой для проверки личности.

После завершения аутентификации на экране появится сообщение **Authenticated** («Аутентифицировано»).

5.7.3 Аутентификация с помощью сопоставления 1:1 и 1:N

Инструкция:

1. Если для аутентификации используются отпечаток пальца и лицо, после появления на экране устройства соответствующего оповещения сначала отсканируйте отпечаток своего пальца.
Устройство сравнит отпечаток пальца с информацией в базе данных устройства (сопоставление 1:N).
После завершения аутентификации на экране появится сообщение **Continue to authenticate** (Продолжайте аутентификацию).
2. Разместите лицо прямо перед камерой для проверки личности.
Устройство сравнит изображение лица с информацией о пользователе, полученной на последнем этапе (сопоставление 1:1).
После завершения аутентификации на экране появится сообщение **Authenticated** («Аутентифицировано»).

Примечания.

- Чтобы получить оптимальные результаты аутентификации лиц человека, рост пользователя должен составлять 140... 190 см, а расстояние между пользователем и устройством — 30... 100 см.
- Подробную информацию о сканировании отпечатков пальцев см. в [Приложении А. Советы по сканированию отпечатков пальцев.](#)

- Подробную информацию об аутентификации с помощью сканирования лица см. в *Приложении В. Советы по сбору и сравнению изображений лица.*

Раздел 6 Работа клиента

Вы можете установить и использовать устройства управления доступом при помощи программного обеспечения клиента. В этой главе представлены операции, связанные с устройством управления доступом, в программном обеспечении клиента. Информацию о встроенных операциях см. в *Руководстве пользователя программного обеспечения клиента iVMS-4200*.

6.1 Регистрация пользователя и вход в систему

Во время первого входа в программное обеспечение клиента iVMS-4200 сначала нужно зарегистрировать суперпользователя.

Инструкция:

1. Введите имя суперпользователя и пароль. Программное обеспечение автоматически оценит надежность пароля. Мы настоятельно рекомендуем использовать надежный пароль для обеспечения требуемой безопасности данных.
2. Подтвердите пароль.
3. Вы можете поставить галочку в пункте **Enable Auto-login (Входить в систему автоматически)**, чтобы автоматически входить в программу.
4. Нажмите кнопку **Register (Зарегистрировать)**. После этого можно будет войти в программное обеспечение в качестве суперпользователя.

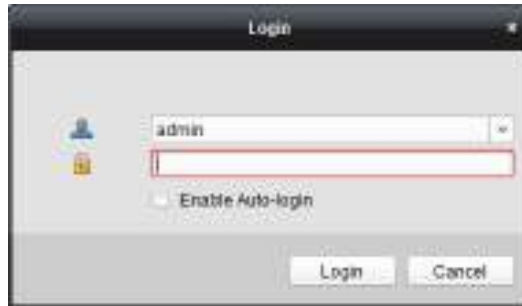


- ◆ Имя пользователя не должно содержать следующие символы: / \ : * ? " < > |. Длина пароля должна составлять не менее шести символов.
- ◆ Чтобы обеспечить надежную защиту данных, мы настоятельно рекомендуем вам изменить пароль по своему усмотрению (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта.
- ◆ Лицо, выполняющее установку и/или конечный пользователь несет ответственность за надлежащую настройку всех паролей и других параметров безопасности.

При открытии iVMS-4200 после регистрации можно войти в программное обеспечение клиента при помощи зарегистрированного имени пользователя и пароля.

Инструкция:

1. Введите имя и пароль зарегистрированного пользователя.
2. Вы можете поставить галочку в пункте **Enable Auto-login (Входить в систему автоматически)**, чтобы автоматически входить в программу.
3. Нажмите кнопку **Login (Войти в систему)**.



После запуска программного обеспечения клиента можно открыть мастер настройки (в том числе мастер настройки видеофайлов, мастер настройки видеостены, мастер настройки панели управления, мастер настройки управления доступом и видеодомофоном и мастер настройки функции контроля посещаемости), чтобы упростить процесс добавления устройства и выполнить другие настройки и операции. Подробную информацию о мастерах настройки см. в *Кратком руководстве пользователя iVMS-4200*.

6.2 Настройки системы

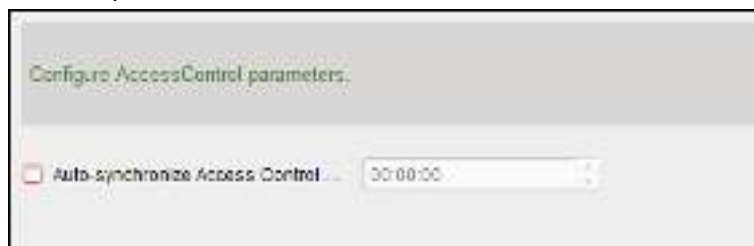
Назначение:

Вы можете синхронизировать пропущенные события управления доступом с клиентом.

Инструкция:

1. Перейдите в пункт **Tool (Инструменты) — System Configuration (Настройки системы)**.
2. В окне настроек системы поставьте галочку в пункте **Auto-synchronize Access Control Event (Автоматически синхронизировать события управления доступом)**.
3. Установите время синхронизации.

Клиент будет автоматически синхронизировать пропущенные события управления доступом в заданное время.



6.3 Управление доступом

Назначение:

Модуль управления доступом используется для устройств управления доступом и видеодомофонов. Он выполняет множество функций, в том числе управление пользователями и картами, настройка разрешений, управление состоянием системы предоставления доступа, контроль работы видеодомофона и другие расширенные возможности.

Вы также можете настроить конфигурацию событий для управления доступом и процесс

отображения точек и зон управления доступом на электронной карте.

Примечание. Пользователь, который обладает разрешениями на работу с модулем управления доступом, может войти в этот модуль и настроить его параметры.



Нажмите кнопку на панели управления и поставьте галочку в пункте **Access Control (Управление доступом)**, чтобы добавить модуль управления доступом на панель управления.



Нажмите кнопку , чтобы войти в модуль управления доступом.

Person No.	Person Name	Organization	Gender	Card Number	Card No.	Preparation Date	Card Number	Card No.
1	Li	Company	Female	1	12345	0	0	0
2	Wang	Company	Female	2	12345	0	0	0

Перед началом работы:

Во время первого открытия модуля управления доступом на экране появится следующее диалоговое окно. Выберите отображаемую зону в соответствии с фактическими потребностями.

Non-residence (Нежилое помещение). Для этого типа зоны можно установить правило посещаемости при добавлении пользователя, задав параметры управления доступом.

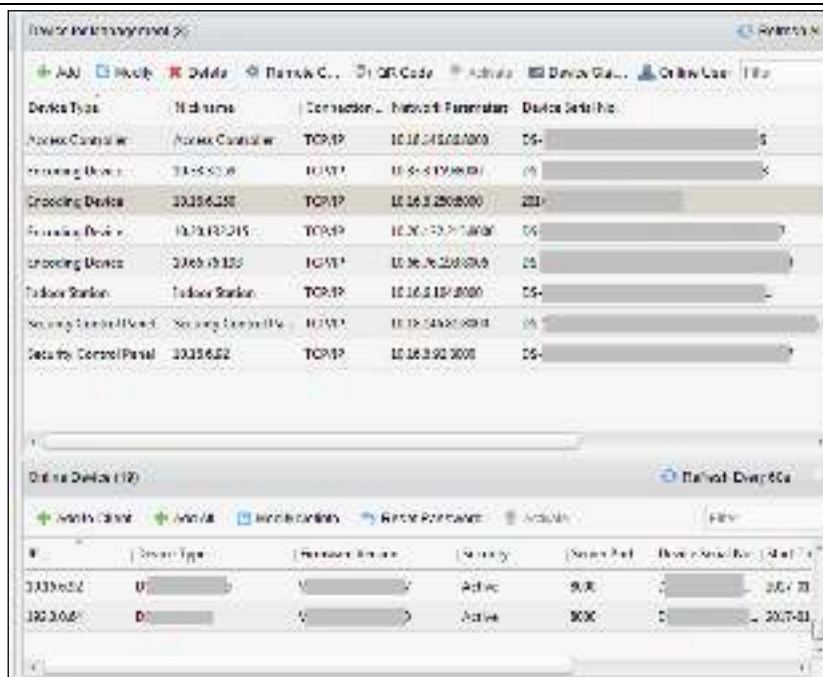
Residence (Жилое помещение). Для этого типа зоны нельзя установить правило посещаемости.



Примечание. После настройки параметров отображаемой зоны их нельзя будет изменить.

6.3.1 Добавление устройства управления доступом

Нажмите кнопку  в модуле управления доступом, чтобы перейти в следующее окно.



Примечание. После добавления устройства необходимо проверить состояние постановки устройства на сигнализацию в меню **Tool (Инструменты) — Device Arming Control (Управление постановкой устройства на сигнализацию)**. Чтобы получать информацию о событиях в режиме реального времени через программное обеспечение клиента, нужно поставить устройство на сигнализацию. Подробную информацию об управлении процессом постановки устройства на сигнализацию см. в *разделе 6.12 Управление постановкой на сигнализацию*.

Создание пароля

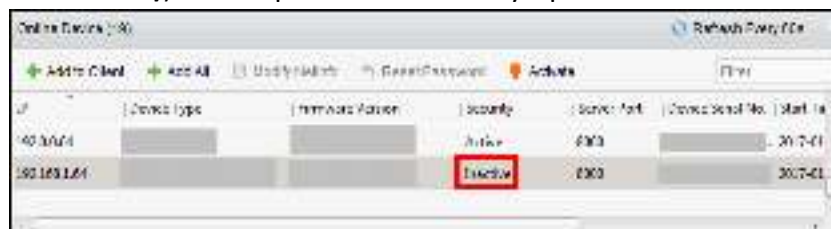
Назначение:

Для активации некоторых устройств необходимо создать пароль, который позволяет добавить их в программное обеспечение, а также контролировать правильность их работы.

Примечание. Эта функция должна быть предусмотрена в устройстве.

Инструкция:

1. Откройте страницу управления устройством.
2. В области **Device for Management (Управление устройством)** или **Online Device (Активное устройство)** проверьте состояние устройства (оно отображается в столбце **Security (Безопасность)**) и выберите неактивное устройство.



3. Нажмите кнопку **Activate (Активировать)**, чтобы перейти в окно активации.
4. Введите пароль в соответствующем поле и подтвердите его.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно

рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.



5. (Дополнительная опция) При активации устройства включите службу Hik-Connect, если она предусмотрена.

- 1) Поставьте галочку в пункте **Enable Hik-Connect (Включить Hik-Connect)**, чтобы отобразить на экране диалоговое окно с примечаниями.



- 2) Создайте код проверки.
- 3) Подтвердите код проверки.
- 4) Нажмите кнопку **Terms of Service (Условия обслуживания)** и **Privacy Policy (Политика обеспечения конфиденциальности)** и ознакомьтесь с требованиями.
- 5) Нажмите кнопку **OK**, чтобы включить службу Hik-Connect.
6. Нажмите кнопку **OK**, чтобы активировать устройство.
Если пароль был установлен успешно, на экране отобразится всплывающее окно с текстом **The device is activated (Устройство активировано)**.
7. Нажмите кнопку **Modify Netinfo (Изменить информацию о сети)**, чтобы перейти в окно редактирования параметров сети.

Примечание. Эта функция доступна только в области **Online Device (Активное устройство)**. Если нужно добавить устройство в программное обеспечение, вы можете назначить устройству IP-адрес той же подсети, в которой находится ваш компьютер.

8. Измените IP-адрес устройства на нужный сегмент сети на компьютере. Для этого введите IP-адрес вручную или поставьте галочку в пункте **DHCP**.
9. Введите пароль, созданный во время выполнения действий, описанных в пункте 4, и нажмите кнопку **OK**, чтобы завершить настройку параметров сети.

Добавление активного устройства

Назначение:

Активные сетевые устройства, которые находятся в одной локальной подсети с ПО клиента, отображаются в области **Online Device (Активные устройства)**. Нажмите кнопку **Refresh Every 60s (Обновлять каждые 60 с)**, чтобы обновлять информацию об активных устройствах.

Примечание. Нажмите кнопку , чтобы скрыть область **Online Device (Активные устройства)**.

IP	Device type	Network Action	Security	Service Port	Device Serial No.	Start Time
10.10.1.253	D		Active	8080	1007-01	2007-01
10.10.1.254	D		Active	8080	1007-01	2007-01
10.10.1.255	D		Active	8080	1007-01	2007-01

Инструкция:

1. Выберите в списке устройства, которые нужно добавить.

Примечание. Для добавления неактивного устройства следует сначала создать для него пароль. Подробную информацию см. в *Раздел 5*.

2. Нажмите кнопку **Add to Client (Добавить в клиент)**, чтобы открыть на экране диалоговое окно добавления устройства.
3. Введите требуемую информацию.

Nickname (Псевдоним). Введите требуемое название устройства.

Address (Адрес): Введите IP-адрес устройства. В этом режиме IP-адрес устройства присваивается автоматически.

Port (Порт): Введите номер порта устройства. По умолчанию используется номер 8000.

User Name (Имя пользователя). Введите имя пользователя устройства. По умолчанию это *admin*.

Password (Пароль). Введите пароль устройства.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми

символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.

4. Вы можете поставить галочку в пункте **Export to Group (Экспортировать в группу)**, чтобы создать группу по названию устройства.

Вы также можете импортировать все каналы устройства в соответствующую группу по умолчанию.

Примечание. iVMS-4200 также обеспечивает возможность добавления неактивных устройств.

- 1) Поставьте галочку в пункте **Add Offline Device (Добавить неактивное устройство)**.
- 2) Введите требуемую информацию, в том числе номер канала устройства и номер входа сигнала тревоги.
- 3) Нажмите кнопку **Add (Добавить)**.

Когда устройство появится в сети, программное обеспечение подключит его автоматически.

5. Нажмите кнопку **Add (Добавить)**, чтобы добавить устройство.



➤ Добавление нескольких активных устройств

Если вы хотите добавить несколько активных устройств в программное обеспечение клиента, нажмите и удерживайте клавишу *Ctrl*, чтобы выбрать несколько устройств, а затем нажмите кнопку **Add to Client (Добавить в клиент)**, чтобы открыть диалоговое окно добавления устройства. Введите имя пользователя и пароль устройств, которые нужно добавить, во всплывающем диалоговом окне.

➤ Добавление всех активных устройств

Если вы хотите добавить все активные устройства в программное обеспечение клиента, нажмите кнопку **Add All (Добавить все)**, а затем клавишу **OK** во всплывающем окне. Введите имя пользователя и пароль для устройств, которые нужно добавить.

3) Нажмите кнопку **Add (Добавить)**.

Когда устройство появится в сети, программное обеспечение подключит его автоматически.

5. Нажмите кнопку **Add (Добавить)**, чтобы добавить устройство.

Добавление устройств по сегменту IP-адреса.

Инструкция:

1. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране диалоговое окно добавления устройства.
2. Выберите режим добавления **IP Segment (Сегмент IP-адреса)**.
3. Введите требуемую информацию.

Start IP (Начальный IP-адрес). Введите начальный IP-адрес.

End IP (Конечный IP-адрес). Введите конечный IP-адрес в том же сегменте сети, что и начальный IP-адрес.

Port (Порт): Введите номер порта устройства. По умолчанию используется номер 8000.

User Name (Имя пользователя). Введите имя пользователя устройства. По умолчанию это *admin*.

Password (Пароль). Введите пароль устройства.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.

4. Вы можете поставить галочку в пункте **Export to Group (Экспортировать в группу)**, чтобы создать группу по названию устройства.

Вы также можете импортировать все каналы устройства в соответствующую группу по умолчанию.

Примечание. iVMS-4200 также обеспечивает возможность добавления неактивных устройств.

- 1) Поставьте галочку в пункте **Add Offline Device (Добавить неактивное устройство)**.
- 2) Введите требуемую информацию, в том числе номер канала устройства и номер входа сигнала тревоги.
- 3) Нажмите кнопку **Add (Добавить)**.

Когда устройство появится в сети, программное обеспечение подключит его автоматически.

5. Нажмите кнопку **Add (Добавить)**.

Вы можете добавить в список устройство, IP-адрес которого находится между начальным и конечным IP-адресом.



Добавление устройств по доменному имени Hik-Connect

Назначение:

Чтобы добавить устройства, подключенные с помощью Hik-Connect, нужно указать учетную запись и пароль Hik-Connect.

Перед началом работы: Сначала добавьте устройства в учетную запись Hik-Connect через iVMS-4200, мобильный клиент iVMS-4500 или Hik-Connect. Подробную информацию о добавлении устройств в учетную запись в Hik-Connect с помощью iVMS-4200 см. в *Руководстве пользователя программного обеспечения клиента iVMS-4200*.

➤ Добавление одного устройства

Инструкция:

1. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране диалоговое окно добавления устройства.
2. Выберите режим добавления **Hik-Connect Domain (Доменное имя Hik-Connect)**.
3. Выберите пункт **Single Adding (Добавить одно устройство)**.
4. Введите требуемую информацию.

Nickname (Псевдоним). Введите требуемое название устройства.

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

User Name (Имя пользователя). Введите имя пользователя устройства. По умолчанию это

admin.

Password (Пароль). Введите пароль устройства.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.

Hik-Connect Account (Учетная запись Hik-Connect). Введите данные учетной записи Hik-Connect.

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

5. Вы можете поставить галочку в пункте **Export to Group (Экспортировать в группу)**, чтобы создать группу по названию устройства.

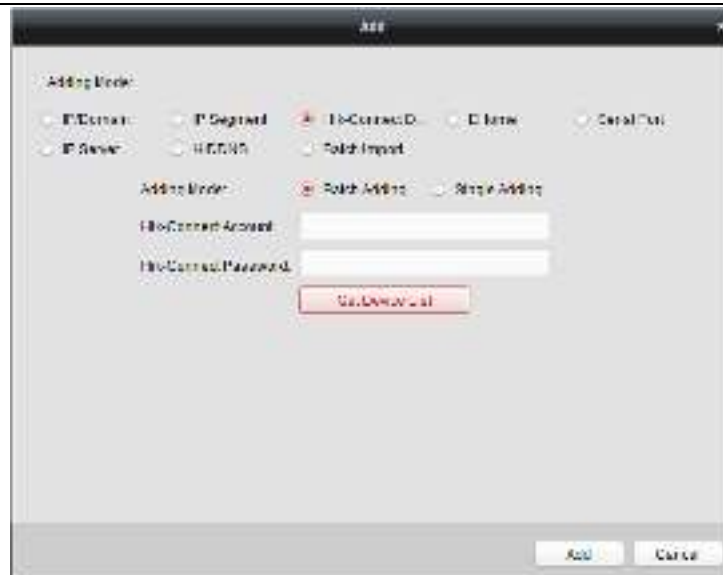
Вы также можете импортировать все каналы устройства в соответствующую группу по умолчанию.

6. Нажмите кнопку **Add (Добавить)**, чтобы добавить устройство.

Добавление устройств в пакетном режиме

Инструкция:

1. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране диалоговое окно добавления устройства.



2. Выберите режим добавления **Hik-Connect Domain (Доменное имя Hik-Connect)**.

3. Выберите пункт **Batch Adding (Добавление в пакетном режиме)**.

4. Введите требуемую информацию.

Hik-Connect Account (Учетная запись Hik-Connect). Введите данные учетной записи Hik-Connect.

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

5. Нажмите кнопку **Get Device List (Получить список устройств)**, чтобы отобразить на экране список устройств, добавленных в учетную запись Hik-Connect.



6. Отметьте галочками требуемые устройства.

7. Введите имя пользователя и пароль для устройств, которые нужно добавить.

8. Вы можете поставить галочку в пункте **Export to Group (Экспортировать в группу)**, чтобы создать группу по названию устройства.

Вы также можете импортировать все каналы устройства в соответствующую группу по умолчанию.

9. Нажмите кнопку **Add (Добавить)**, чтобы добавить устройства.

Добавление устройств с помощью учетной записи EHome

Назначение:

Чтобы добавить устройство управления доступом, подключенное с помощью протокола EHome, нужно ввести данные учетной записи EHome.

Перед началом работы: Сначала нужно настроить параметры сетевого центра. Подробную информацию см. в разделе 6.3.4 [Настройки сети](#).

Инструкция:

1. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране диалоговое окно добавления устройства.
2. Выберите режим добавления **EHome**.



3. Введите требуемую информацию.

Nickname (Псевдоним). Введите требуемое название устройства.

Account (Учетная запись). Введите имя учетной записи, зарегистрированной в протоколе EHome.

4. Вы можете поставить галочку в пункте **Export to Group (Экспортировать в группу)**, чтобы создать группу по названию устройства.

Вы также можете импортировать все каналы устройства в соответствующую группу по умолчанию.

Примечание. iVMS-4200 также обеспечивает возможность добавления неактивных устройств.

- 1) Поставьте галочку в пункте **Add Offline Device (Добавить неактивное устройство)**.

- 2) Введите требуемую информацию, в том числе номер канала устройства и номер входа сигнала тревоги.

- 3) Нажмите кнопку **Add (Добавить)**.

Когда устройство появится в сети, программное обеспечение подключит его автоматически.

5. Нажмите кнопку **Add (Добавить)**, чтобы добавить устройство.

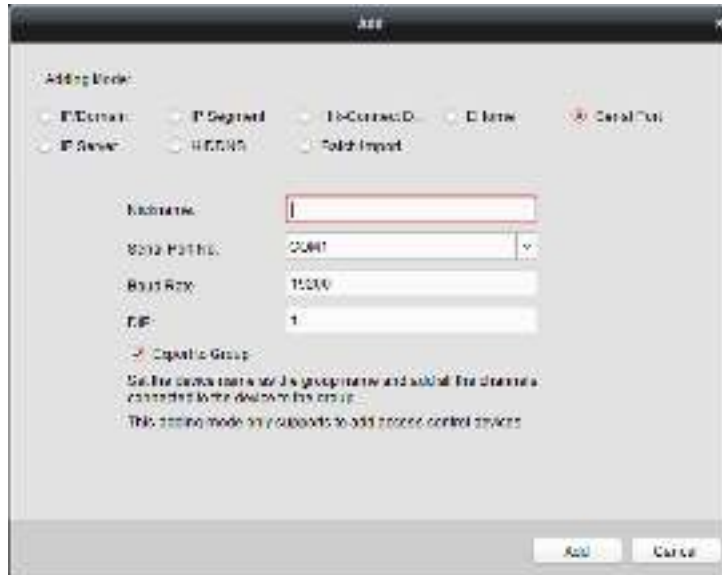
Добавление устройств с помощью последовательного порта

Назначение:

Вы можете добавить устройство управления доступом, подключенное через последовательный порт.

Инструкция:

1. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране диалоговое окно добавления устройства.
2. Выберите режим добавления **Serial Port (Последовательный порт)**.



3. Введите требуемую информацию.
Nickname (Псевдоним). Введите требуемое название устройства.
Serial Port No. (Номер последовательного порта). Выберите номер последовательного порта подключенного устройства.
Baud Rate (Скорость передачи данных). Введите значение скорости передачи данных устройства управления доступом.
DIP (Коммутируемое соединение). Введите адрес коммутируемого соединения устройства.

4. Вы можете поставить галочку в пункте **Export to Group (Экспортировать в группу)**, чтобы создать группу по названию устройства.
 Вы также можете импортировать все каналы устройства в соответствующую группу по умолчанию.

Примечание. iVMS-4200 также обеспечивает возможность добавления неактивных устройств.

- 1) Поставьте галочку в пункте **Add Offline Device (Добавить неактивное устройство)**.
- 2) Введите требуемую информацию, в том числе номер канала устройства и номер входа сигнала тревоги.
- 3) Нажмите кнопку **Add (Добавить)**.

Когда устройство появится в сети, программное обеспечение подключит его автоматически.

5. Нажмите кнопку **Add (Добавить)**, чтобы добавить устройство.

Добавление устройств с помощью IP-сервера

Инструкция:

1. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране диалоговое окно добавления устройства.
2. Выберите режим добавления **IP Server (IP-сервер)**.

3. Введите требуемую информацию.

Nickname (Псевдоним). Введите требуемое название устройства.

Server Address (Адрес сервера). Введите IP-адрес компьютера, на котором установлен IP-сервер.

Device ID (Идентификатор устройства). Введите идентификатор устройства, зарегистрированного на IP-сервере.

User Name (Имя пользователя). Введите имя пользователя устройства. По умолчанию это *admin*.

Password (Пароль). Введите пароль устройства.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.

4. Вы можете поставить галочку в пункте **Export to Group (Экспортировать в группу)**, чтобы создать группу по названию устройства.

Вы также можете импортировать все каналы устройства в соответствующую группу по умолчанию.

Примечание. iVMS-4200 также обеспечивает возможность добавления неактивных устройств.

- 1) Поставьте галочку в пункте **Add Offline Device (Добавить неактивное устройство)**.
- 2) Введите требуемую информацию, в том числе номер канала устройства и номер входа сигнала тревоги.
- 3) Нажмите кнопку **Add (Добавить)**.

Когда устройство появится в сети, программное обеспечение подключит его автоматически.

5. Нажмите кнопку **Add (Добавить)**, чтобы добавить устройство.

Добавление устройств с помощью HiDDNS

Инструкция:

1. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране диалоговое окно добавления устройства.
2. Выберите режим добавления **HiDDNS**.

3. Введите требуемую информацию.

Nickname (Псевдоним). Введите требуемое название устройства.

Server Address (Адрес сервера). www.hik-online.com.

Device Domain Name (Доменное имя устройства). Введите доменное имя устройства, зарегистрированного на сервере HiDDNS.

User Name (Имя пользователя). Введите имя пользователя устройства. По умолчанию это *admin*.

Password (Пароль). Введите пароль устройства.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.

4. Вы можете поставить галочку в пункте **Export to Group (Экспортировать в группу)**, чтобы создать группу по названию устройства.

Вы также можете импортировать все каналы устройства в соответствующую группу по умолчанию.

Примечание. iVMS-4200 также обеспечивает возможность добавления неактивных

устройств.

- 1) Поставьте галочку в пункте **Add Offline Device (Добавить неактивное устройство)**.
- 2) Введите требуемую информацию, в том числе номер канала устройства и номер входа сигнала тревоги.
- 3) Нажмите кнопку **Add (Добавить)**.

Когда устройство появится в сети, программное обеспечение подключит его автоматически.

5. Нажмите кнопку **Add (Добавить)**, чтобы добавить устройство.

Импорт устройств в пакетном режиме

Назначение:

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

Инструкция:

1. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране диалоговое окно добавления устройства.
2. Выберите режим добавления **Batch Import (Импорт в пакетном режиме)**.



3. Нажмите кнопку **Export Template (Экспортировать шаблон)** и сохраните предварительно выбранный шаблон (CSV-файл) на компьютере.
4. Откройте экспортированный файл шаблона и введите требуемую информацию об устройствах, которые нужно добавить, в соответствующий столбец.
 - **Nickname (Псевдоним)**. Введите требуемое название устройства.
 - **Adding Mode (Режим добавления)**. Вы можете ввести 0, 2, 3, 4, 5 или 6. Каждая цифра обозначает отдельный режим добавления устройств. 0 — устройство будет добавлено по IP-адресу или доменному имени; 2 — устройство будет добавлено по IP-серверу; 3 — устройство будет добавлено по HiDDNS; 4 — устройство будет добавлено по протоколу EName; 5 — устройство будет добавлено по последовательному порту; 6 — устройство будет добавлено по доменному имени Hik-Connect.
 - **Address (Адрес)**. Измените адрес устройства. Если установлен режим добавления 0, нужно ввести IP-адрес или доменное имя устройства; если установлен режим добавления 2, необходимо ввести IP-адрес компьютера, на котором установлен IP-

сервер; если установлен режим добавления 3, требуется ввести адрес *www.hik-online.com*.

- **Port (Порт).** Введите номер порта устройства. По умолчанию используется номер 8000.
- **Device Information (Сведения об устройстве).** Если установлен режим добавления 0, это поле заполнять не нужно; если установлен режим добавления 2, необходимо ввести идентификатор устройства, зарегистрированного на IP-сервере; если установлен режим добавления 3, требуется ввести доменное имя устройства, зарегистрированного на сервере HiDDNS; если установлен режим добавления 4, необходимо ввести данные учетной записи EHome; если установлен режим добавления 6, нужно ввести серийный номер устройства.
- **User Name (Имя пользователя).** Введите имя пользователя устройства. По умолчанию это *admin*.
- **Password (Пароль).** Введите пароль устройства.



РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ. Мы настоятельно рекомендуем создать надежный пароль по собственному выбору (с использованием не менее восьми символов, включая буквы верхнего и нижнего регистра, цифры и специальные символы), чтобы повысить безопасность вашего продукта. Также рекомендуется регулярно менять пароль, особенно в системах с высокой степенью безопасности. Еженедельная или ежемесячная смена пароля может улучшить безопасность вашего продукта.

- **Add Offline Device (Добавление неактивного устройства).** Введите 1, чтобы активировать функцию добавления неактивного устройства. После этого программное обеспечение автоматически подключит устройство в случае его появления в сети. Если значение равно 0, эта функция не работает.
- **Export to Group (Экспорт в группу).** Измените значение на 1, чтобы создать группу по названию устройства (псевдониму). Все каналы устройства будут импортированы в соответствующую группу по умолчанию. Если значение равно 0, эта функция не работает.
- **Channel Number (Номер канала).** Если для параметра **Add Offline Device (Добавление неактивного устройства)** установлено значение 1, нужно ввести номер канала устройства. Если для параметра **Add Offline Device (Добавление неактивного устройства)** установлено значение 0, это поле заполнять не нужно.
- **Alarm Input Number (Номер входа сигнала тревоги).** Если для параметра **Add Offline Device (Добавление неактивного устройства)** установлено значение 1, нужно ввести номер входа сигнала тревоги устройства. Если для параметра **Add Offline Device (Добавление неактивного устройства)** установлено значение 0, это поле заполнять не нужно.
- **Serial Port No. (Номер последовательного порта).** Если установлен режим добавления 5, нужно ввести номер последовательного порта устройства управления доступом.
- **Baud Rate (Скорость передачи данных).** Если установлен режим добавления 5, нужно ввести значение скорости передачи данных устройства управления доступом.

- **DIP (Коммутируемое соединение).** Если установлен режим добавления 5, нужно ввести адрес коммутируемого соединения устройства управления доступом.
- **Hik-Connect Account (Учетная запись Hik-Connect).** Если установлен режим добавления 6, нужно ввести данные учетной записи Hik-Connect.
- **Hik-Connect Password (Пароль Hik-Connect).** Если установлен режим добавления 6, нужно ввести пароль для учетной записи Hik-Connect.

5. Нажмите кнопку  и выберите файл шаблона.

6. Нажмите кнопку **Add (Добавить)**, чтобы добавить устройства.

После успешного добавления устройств они будут отображаться в списке компонентов, доступных для управления. Вы можете контролировать использование ресурсов, состояние жесткого диска, процедуру записи, а также получать другую информацию о добавленных устройствах в списке.

Нажмите кнопку **Refresh All (Обновить все)**, чтобы обновить информацию обо всех добавленных устройствах. Вы также можете ввести название устройства в поле фильтра для осуществления его поиска.

6.3.2 Просмотр состояния устройства

Выберите устройство из списка и нажмите кнопку **Device Status (Состояние устройства)**, чтобы вывести на экран его состояние.



Примечание. Внешний вид окна может отличаться от изображения, приведенного выше. При использовании данной функции нужно ориентироваться на параметры окна, которое отображается на вашем экране.

- **Door Status (Статус двери).** Состояние подключенной двери.
- **Host Status (Состояние хоста).** Здесь отображается состояние хоста, в том числе питающее напряжение аккумулятора, состояние источника питания устройства, состояние взаимной блокировки нескольких дверей, состояние защиты от обхода системы безопасности и

состояние защиты хоста от несанкционированного доступа.

- **Card Reader Status (Состояние устройства для считывания карт).** Здесь отображается состояние устройства для считывания карт.
Примечание. Если используется устройство для считывания карт с интерфейсом RS-485, можно также просматривать статус нахождения или отсутствия в сети. Если используется устройство для считывания карт с интерфейсом Wiegand, можно также просматривать статус отсутствия в сети.
- **Alarm Output Status (Состояние выхода сигнала тревоги).** Состояние выхода сигнала тревоги каждого порта.
- **Event Sensor Status (Состояние датчика событий).** Состояние датчика событий каждого порта.
- **Secure Door Control Unit Status (Состояние блока управления защищенной дверью).** Статус подключения к сети и состояние защиты от несанкционированного доступа блока управления защищенной дверью.
- **Arming Status (Статус постановки на сигнализацию).** Состояние устройства.

6.3.3 Редактирование основной информации

Назначение:

После добавления устройства управлением доступом можно изменить основную информацию о нем.

Инструкция:

1. Выберите устройство из списка.
2. Нажмите кнопку **Modify (Изменить)**, чтобы открыть окно изменения информации об устройстве.
3. Перейдите на вкладку **Basic Information (Основная информация)**.



4. Введите информацию об устройстве, в том числе режим добавления, название устройства, его IP-адрес, номер порта, имя пользователя и пароль.

6.3.4 Настройки сети

Назначение:

После добавления устройства управления доступом можно настроить режим загрузки, параметры сетевого центра и центра беспроводной связи.

Выберите устройство из списка и нажмите кнопку **Modify (Изменить)**, чтобы открыть окно редактирования информации об устройстве.

Перейдите на вкладку **Network Settings (Настройки сети)**.

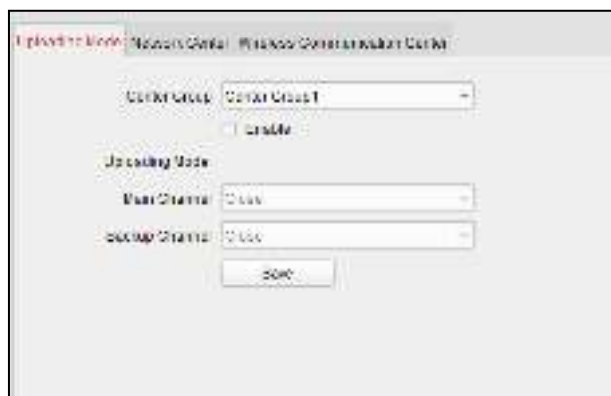
Настройки режима загрузки

Назначение:

Вы можете настроить центральную группу для загрузки журнала с помощью протокола EHome.

Инструкция:

1. Перейдите на вкладку **Uploading Mode (Режим загрузки)**.



2. Выберите центральную группу в выпадающем списке.
3. Поставьте галочку в пункте **Enable (Включить)**, чтобы активировать выбранную центральную группу.
4. Выберите режим загрузки в выпадающем списке. Вы можете установить значение **N1/G1** для основного и резервного канала или нажать кнопку **Close (Заккрыть)**, чтобы отключить основной или резервный канал.

Примечание. Невозможно одновременно выбрать N1 или G1 для основного и резервного канала.

5. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить параметры.

Настройки сетевого центра

Вы можете выбрать учетную запись протокола EHome на странице параметров сети. Это позволит добавить устройства с помощью протокола EHome.

Инструкция:

1. Перейдите на вкладку **Network Center (Сетевой центр)**.



2. Выберите центральную группу в выпадающем списке.
3. Укажите тип адреса **IP Address (IP-адрес)** или **Domain Name (Доменное имя)**.
4. Введите IP-адрес или доменное имя в соответствии с типом адреса.
5. Введите номер порта для протокола. По умолчанию используется значение 7660.
6. Выберите **EHome** в качестве типа протокола.
7. Укажите имя учетной записи сетевого центра.

Примечание. Длина имени учетной записи может составлять от 1 до 32 символов. Оно может содержать только буквы или цифры.

8. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить параметры.

Примечания.

- Номер порта беспроводной и проводной сети должен быть таким же, как и номер порта EHome.
- Доменное имя можно указать в пункте *Editing Time (Изменение времени)* области **Enable NTP (Активация NTP)** раздела **Remote Configuration (Удаленная настройка)**. Подробнее см. в разделе *Время* главы 6.3.9 *Установка нескольких сетевых адаптеров*

Назначение:

Можно установить такие параметры, как NIC type (Тип сетевого адаптера), IPv4 address (Адрес IPv4), Subnet mask (IPv4) (Маску подсети (IPv4)), Default gateway (Основной шлюз), MAC, MTU и Device port (Порт устройства).

Примечание. Устройство должно поддерживать эту функцию.

Перед началом работы:

Добавьте устройства с помощью учетной записи EHome.

Инструкция:

1. Нажмите кнопку **Multiple NICs Settings (Несколько сетевых адаптеров)**, чтобы перейти на соответствующую страницу.



2. Задайте требуемые параметры.
3. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

6.3.5 Настройка терминала распознавания лиц

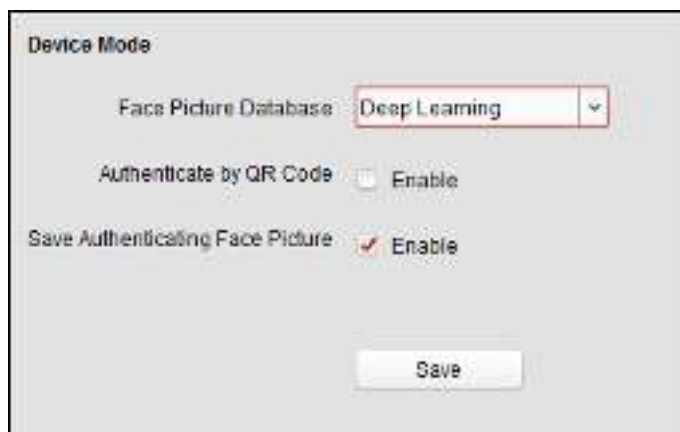
Назначение:

Вы можете установить режим работы терминала распознавания лиц, включая базу распознавания лиц, аутентификацию с помощью QR-кода и сохранение лица, прошедшего проверку.

Примечание. Устройство должно поддерживать эту функцию.

Инструкция:

1. Нажмите кнопку Face Recognition Terminal Settings (Параметры терминала распознавания лиц), чтобы перейти на соответствующую страницу.



2. Задайте параметры терминала распознавания лиц.

Описание параметров:

Параметр	Описание
Face Picture Database (База данных изображений лиц)	В качестве базы данных изображений лиц можно выбрать Deep Learning (Глубокое изучение).
Authenticate by QR Code (Аутентификация по QR-коду)	После активации данной функции камера устройства сможет сканировать QR-код для выполнения аутентификации. По умолчанию эта функция выключена.
Save Authenticating Face Picture (Сохранение изображения лица, прошедшего процедуру аутентификации)	После активации данной функции изображение лица, прошедшего процедуру аутентификации, будет сохранено на устройстве.

3. Нажмите кнопку Save (Сохранить), чтобы сохранить настройки.

Вы также можете редактировать параметры в окне Remote Configuration (Удаленная настройка). Подробную информацию см. в *разделе 6.3.11 Удаленная настройка*

Настройки центра беспроводной связи

Инструкция:

1. Перейдите на вкладку **Wireless Communication Center (Центр беспроводной связи)**.



2. Вы берите значение **CMNET** или **UNINET** в качестве имени APN.
3. Введите номер SIM-карты.
4. Выберите центральную группу в выпадающем списке.
5. Введите IP-адрес и номер порта.
6. Выберите **EHome** в качестве типа протокола. По умолчанию используется номер порта EHome 7660.
7. Укажите имя учетной записи сетевого центра. В рамках одной платформы следует использовать одну и ту же учетную запись.
8. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить параметры.

Примечание. Номер порта беспроводной и проводной сети должен быть таким же, как и номер порта EHome.

6.3.6 Настройки процесса захвата изображений

Вы можете настроить параметры привязки захвата изображений и процесс захвата изображений ручном режиме.

Выберите устройство из списка и нажмите кнопку **Modify (Изменить)**, чтобы открыть окно редактирования информации об устройстве.

Перейдите на вкладку **Capture Settings (Настройки захвата изображений)**, чтобы перейти в соответствующее окно.

Примечания.

- Устройство должно поддерживать функцию **Capture Settings (Настройки захвата изображений)**.
- Перед настройкой параметров захвата изображений нужно задать параметры сервера хранения изображений.

Привязка захваченного изображения

Инструкция:

1. Перейдите на вкладку **Linked Capture (Привязка захваченного изображения)**.



2. Укажите требуемый размер и параметры качества изображений.
3. Установите время привязки захваченного изображения после возникновения определенного события.
4. Задайте интервал захвата изображения в соответствии с указанной длительностью всего процесса.
5. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Захват изображений в ручном режиме

Инструкция:

1. Перейдите на вкладку **Manual Capture (Захват изображений в ручном режиме)**.



2. Выберите разрешение снимков в выпадающем списке.
3. Выберите уровень качества изображения — **High (Высокое)**, **Medium (Среднее)** или **Low (Низкое)**.
4. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.
5. Нажмите кнопку **Restore Default Value (Восстановить значения по умолчанию)**, чтобы сбросить настройки до значений по умолчанию.

6.3.7 Настройки RS-485

Назначение:

Вы можете настроить параметры RS-485, в том числе последовательный порт, скорость передачи информации, бит данных, стоповый бит, тип четности, коммуникационный режим, режим работы и режим установления соединения.

Примечание. Устройство должно поддерживать возможность настройки параметров RS-485.

Инструкция:

1. Выберите устройство из списка и нажмите кнопку **Modify (Изменить)**, чтобы открыть окно редактирования информации об устройстве.
2. Выберите вкладку **RS-485 Settings (Настройки RS-485)**, чтобы перейти в соответствующее окно.

2. Выберите серийный номер порта из выпадающего списка, чтобы настроить параметры RS-485.
3. Укажите скорость передачи данных, бит данных, стоповый бит, тип четности, контроль потока, коммуникационный режим, режим работы и режим установления соединения из выпадающего списка.
4. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки. Заданные параметры будут применены к устройству автоматически.

Примечание. После изменения режима работы произойдет автоматическая перезагрузка устройства. После изменения режима работы на экране появится соответствующее уведомление.

6.3.8 Настройки интерфейса Wiegand

Назначение:

Вы можете настроить канал и режим связи для интерфейса Wiegand.

Примечание. Устройство должно поддерживать возможность настройки интерфейса Wiegand.

Инструкция:

1. Выберите устройство из списка и нажмите кнопку **Modify (Изменить)**, чтобы открыть окно редактирования информации об устройстве.
2. Выберите вкладку **Wiegand Settings (Настройки интерфейса Wiegand)**, чтобы перейти в соответствующее окно.

3. Выберите номер канала и режим связи интерфейса Wiegand в выпадающем списке. Если для параметра **Communication Direction (Направление связи)** выбрано значение **Send (Отправка)**, нужно установить для режима интерфейса Wiegand значение Wiegand 26 или Wiegand 34.
4. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки. Заданные параметры будут применены к устройству автоматически.

Примечание. После изменения направления связи произойдет автоматическая перезагрузка устройства. После изменения направления связи на экране появится соответствующее уведомление.

уведомление.

6.3.9 Установка нескольких сетевых адаптеров

Назначение:

Можно установить такие параметры, как **NIC type (Тип сетевого адаптера)**, **IPv4 address (Адрес IPv4)**, **Subnet mask (IPv4) (Маску подсети (IPv4))**, **Default gateway (Основной шлюз)**, **MAC**, **MTU** и **Device port (Порт устройства)**.

Примечание. Устройство должно поддерживать эту функцию.

Перед началом работы:

Добавьте устройства с помощью учетной записи EHome.

Инструкция:

1. Нажмите кнопку **Multiple NICs Settings (Несколько сетевых адаптеров)**, чтобы перейти на соответствующую страницу.



2. Задайте требуемые параметры.
3. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

6.3.10 Настройка терминала распознавания лиц

Назначение:

Вы можете установить режим работы терминала распознавания лиц, включая базу распознавания лиц, аутентификацию с помощью QR-кода и сохранение лица, прошедшего проверку.

Примечание. Устройство должно поддерживать эту функцию.

Инструкция:

1. Нажмите кнопку **Face Recognition Terminal Settings (Параметры терминала распознавания лиц)**, чтобы перейти на соответствующую страницу.



2. Задайте параметры терминала распознавания лиц.

Описание параметров:

Параметр	Описание
Face Picture Database (База данных изображений лиц)	В качестве базы данных изображений лиц можно выбрать Deep Learning (Глубокое изучение) .
Authenticate by QR Code (Аутентификация по QR-коду)	После активации данной функции камера устройства сможет сканировать QR-код для выполнения аутентификации. По умолчанию эта функция выключена.
Save Authenticating Face Picture (Сохранение изображения лица, прошедшего процедуру аутентификации)	После активации данной функции изображение лица, прошедшего процедуру аутентификации, будет сохранено на устройстве.

3. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Вы также можете редактировать параметры в окне **Remote Configuration (Удаленная настройка)**. Подробную информацию см. в разделе 6.3.11 **Удаленная настройка**.

6.3.11 Удаленная настройка

Назначение:

Выберите устройство из списка и нажмите кнопку **Remote Configuration (Удаленная настройка)**, чтобы перейти в окно удаленной настройки. Вы можете настроить расширенные параметры выбранного устройства.

Проверка информации об устройстве

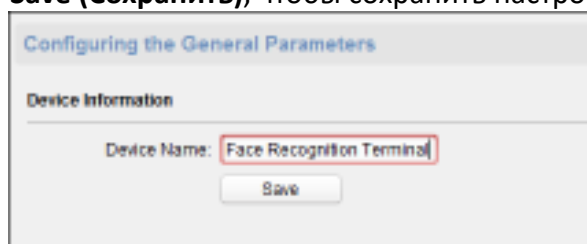
Инструкция:

1. Нажмите кнопку **Remote Configuration (Удаленная настройка)** в списке устройств, чтобы перейти в окно удаленной настройки.
2. Выберите пункт **System (Система) -> Device Information (Информация об устройстве)**, чтобы просмотреть основную информацию об устройстве, а также данные о его версии.



Изменение названия устройства

На странице удаленной настройки выберите пункт **System (Система)** -> **General (Общие параметры)**, чтобы отредактировать название устройства и перезаписать параметры записи файлов. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.



Изменение времени

Инструкция:

1. На странице удаленной настройки выберите пункт **System (Система)** -> **Time (Время)**, чтобы настроить часовой пояс.
2. (Дополнительная опция) Поставьте галочку в пункте **Enable NTP (Активировать NTP)** и укажите адрес, номер порта и интервал синхронизации NTP-сервера.
3. (Дополнительная опция) Поставьте галочку в пункте **Enable DST (Включить функцию перехода на летнее время)** и укажите время начала, время окончания и величину смещения.
4. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Configuring the Time Settings (e.g., NTP, DST)

Time Zone

Select Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singa...

☐ Enable NTP

Server Address:

NTP Port: 123

Sync Interval: 0 Minute(s)

☐ Enable DST

Start Time: April First Week Sun 2 :00

End Time: October Last Week Sun 2 :00

DST Bias: 00 min

Save

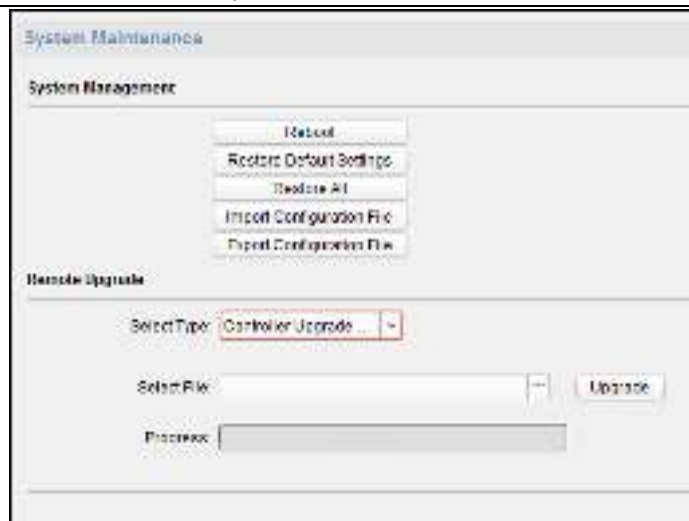
Настройка параметров обслуживания системы

Назначение:

Вы можете перезагружать устройство удаленно, восстанавливать настройки по умолчанию, импортировать файл конфигурации, обновлять устройство и т. д.

Инструкция:

1. На странице удаленной настройки выберите пункт **System (Система) -> System Maintenance (Обслуживание системы)**.
2. Нажмите кнопку **Reboot (Перезагрузить)**, чтобы перезагрузить устройство.
Или нажмите кнопку **Restore Default Settings (Восстановить настройки по умолчанию)**, чтобы сбросить настройки до значений по умолчанию (кроме IP-адреса).
Или нажмите кнопку **Restore All (Восстановить все)**, чтобы сбросить настройки до значений по умолчанию. После сброса настроек нужно будет снова активировать устройство.
Примечание. В файле конфигурации содержатся параметры устройства.
Или нажмите кнопку **Import Configuration File (Импортировать файл конфигурации)**, чтобы импортировать файл конфигурации с локального компьютера на устройство.
Или нажмите кнопку **Export Configuration File (Экспортировать файл конфигурации)**, чтобы экспортировать файл конфигурации с устройства на локальный компьютер.
Примечание. В файле конфигурации содержатся параметры устройства.
3. Вы также можете удаленно обновлять устройство.
 - 1) На странице удаленного обновления нажмите кнопку , чтобы выбрать файл обновления.
 - 2) Нажмите кнопку **Upgrade (Обновить)**, чтобы начать процесс обновления.



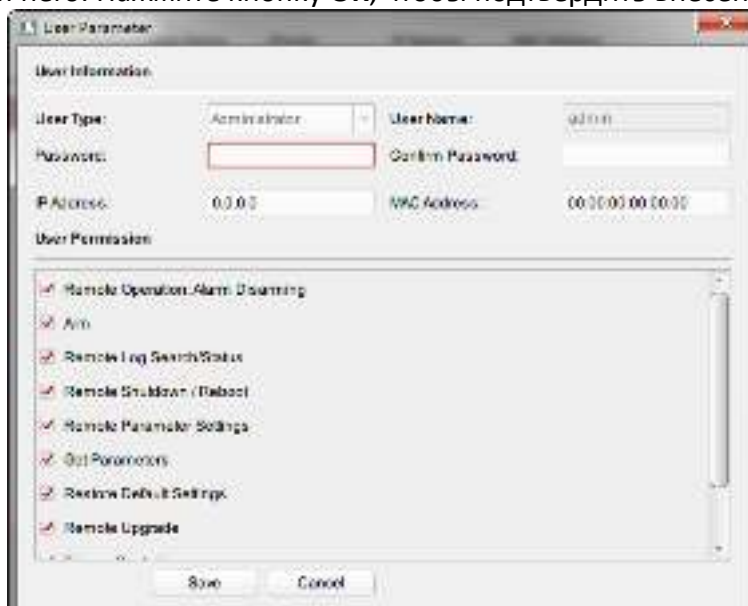
Управление пользователями

Инструкция:

1. На странице удаленной настройки выберите пункт **System (Система)** -> **User (Пользователи)**.



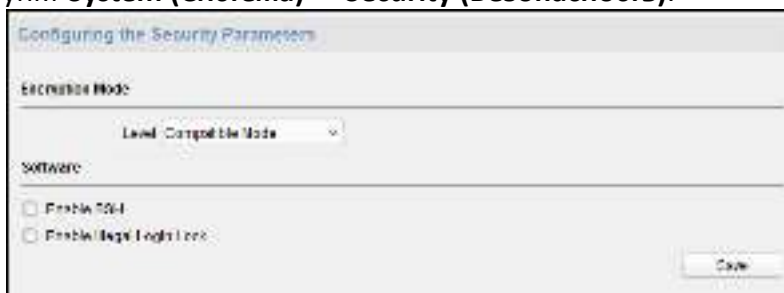
2. Нажмите кнопку **Add (Добавить)**, чтобы добавить пользователя (эта функция не поддерживается контроллером лифта).
Или выберите пользователя из списка и нажмите кнопку **Edit (Изменить)**, чтобы изменить его параметры. Вы можете изменить пароль пользователя, его IP-адрес, MAC-адрес и разрешения для него. Нажмите кнопку **OK**, чтобы подтвердить внесенные изменения.



Настройка параметров безопасности

Инструкция:

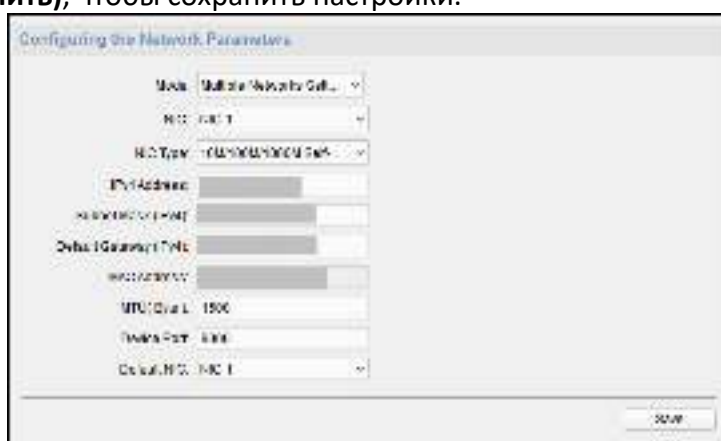
1. Перейдите в пункт **System (Система) -> Security (Безопасность)**.



2. Выберите режим шифрования в выпадающем списке.
Вы можете выбрать **Compatible Mode (Режим совместимости)** или **Encryption Mode (Режим шифрования)**.
3. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Настройка параметров сети

Выберите пункт **Network (Сеть) -> General (Общие параметры)**. Вы можете установить такие параметры, как **NIC type (Тип сетевого адаптера)**, **IPv4 address (Адрес IPv4)**, **Subnet mask (IPv4) (Маску подсети (IPv4))**, **Default gateway (IPv4) (Основной шлюз (IPv4))**, **MAC address (Адрес MAC)**, **MTU, Device port (Порт устройства)** и **Default NIC (Основной сетевой адаптер)**. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.



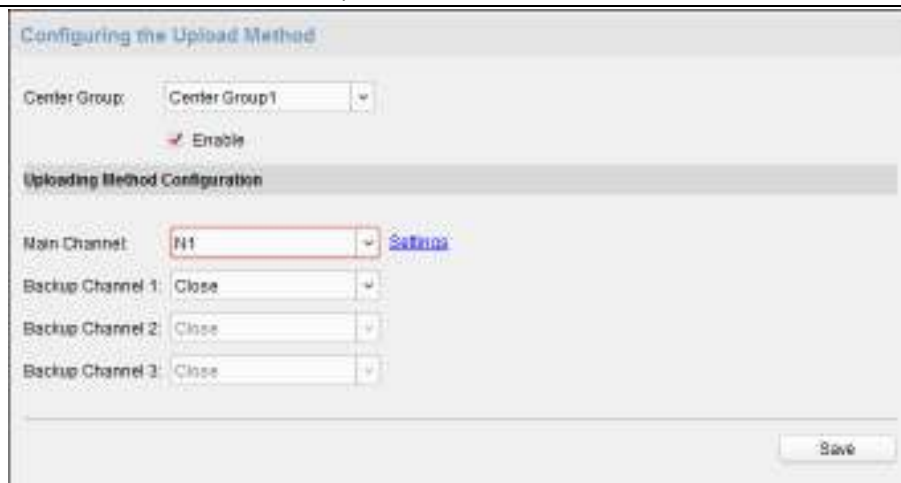
Настройка процесса загрузки

Назначение:

Вы можете настроить центральную группу для загрузки журнала с помощью протокола EHome.

Инструкция:

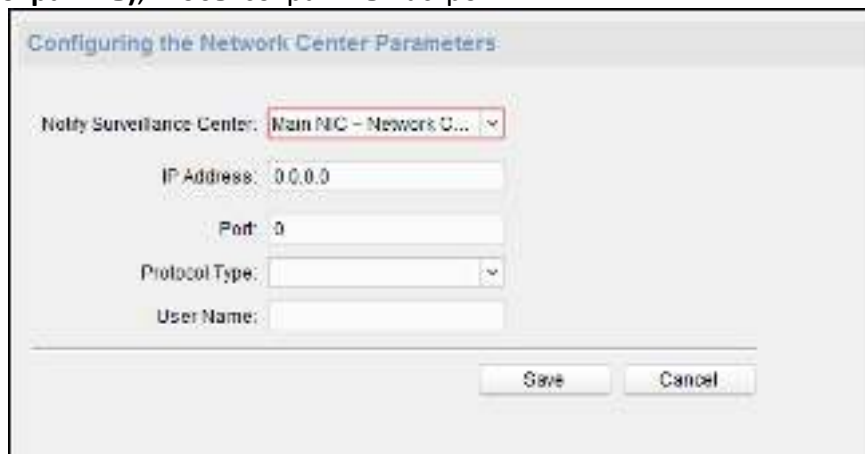
1. Выберите пункт **Network (Сеть) -> Report Strategy (Стратегия ведения отчетности)**.



2. Выберите центральную группу из выпадающего списка.
3. Поставьте галочку в пункте **Enable (Включить)**.
4. Настройте процесс загрузки.
Вы можете задать параметры основного и резервного каналов.
5. Нажмите кнопку **Settings (Настройки)** в правой части поля канала, чтобы внести подробную информацию о нем.
6. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Настройка сетевого центра

Вы можете настроить параметры центра видеонаблюдения, а также указать IP-адрес центра, номер порта, протокол (EHome) и имя пользователя учетной записи EHome для передачи данных по протоколу EHome. Подробную информацию о передаче данных по протоколу EHome см. в пункте *Настройки сетевого центра* в разделе 6.3.4 **Настройки сети**. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.



Расширенные настройки сети

Перейдите в пункт **Network (Сеть)** -> **Advanced Settings (Расширенные настройки)**. Вы можете указать **DNS IP address 1 (IP-адрес 1 DNS-сервера)** и **DNS IP address 2 (IP-адрес 2 DNS-сервера)**. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.



Настройка параметров управления доступом

Инструкция:

1. На странице удаленной настройки выберите пункт **Other (Прочие настройки)** -> **Access Control Parameters (Параметры управления доступом)**.

2. Отметьте галочками нужные пункты.

Overlay User Information on Picture (Наложение информации о пользователе на изображение). Позволяет отображать информацию о пользователе на захваченном изображении.

Enable Voice Prompt (Включение голосовых подсказок). Если эта функция активирована, устройство будет воспроизводить голосовые подсказки во время своей работы.

Upload Pictures after Capturing (Загрузка изображения после захвата). Если эта функция активирована, снимки, захваченные соответствующей камерой, будут автоматически загружаться в систему.

Save Captured Pictures (Сохранение захваченных изображений). Если эта функция активирована, вы можете сохранять изображения, захваченные камерой, связанной с устройством.

Enable 3G/4G (Включение 3G/4G). Если вы поставите галочку в соответствующем пункте, устройство активирует функцию связи 3G/4G.

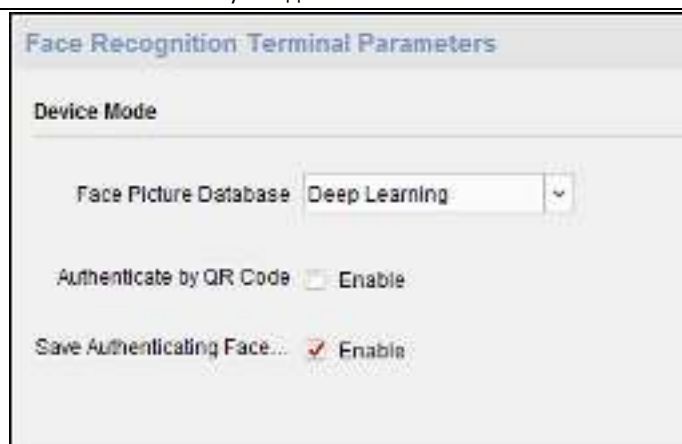
3. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.



Настройка параметров терминала распознавания лиц

Инструкция:

1. Выберите пункт **Other (Другие настройки)** – **Face Recognition Terminal Parameters (Параметры терминала распознавания лиц)**, чтобы перейти на страницу настройки параметров терминала распознавания лиц.



2. Настройте параметры.

Описание параметров:

Параметр	Описание
Face Picture Database (База данных изображений лиц)	В качестве базы данных изображений лиц можно выбрать Deep Learning (Глубокое изучение) .
Authenticate by QR Code (Аутентификация по QR-коду)	После активации данной функции камера устройства сможет сканировать QR-код для выполнения аутентификации. По умолчанию эта функция выключена.
Save Authenticating Face Picture (Сохранение изображения лица, прошедшего процедуру аутентификации)	После активации данной функции изображение лица, прошедшего процедуру аутентификации, будет сохранено на устройстве.

Настройка параметров изображения лиц

Вы берите пункт **Other (Другие настройки)** – **Face Picture Parameters (Параметры изображения лиц)**, чтобы перейти на страницу настроек параметров изображения лиц. Вы можете установить параметры изображения лиц, которые используются при аутентификации. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Описание параметров:

Параметр	Описание
Min. Detection Width (Close to) (Минимальная ширина обнаружения (приближение))	Если расстояние между камерой и пользователем слишком мало, параметр представляет собой минимальный процент ширины лица от общей ширины области распознавания. Для успешного распознавания лица фактический процент должен быть выше заданного значения. При таком условии устройство не будет выявлять другие параметры.
Pitch Angle (Угол)	Максимальный угол наклона при распознавании

Терминал распознавания лиц

Руководство пользователя

Параметр	Описание
наклона)	лиц. По умолчанию этот угол равен 30°.
Yaw Angle (Угол рыскания)	Максимальный угол рыскания при распознавании лиц. По умолчанию этот угол равен 45°.
Min. Detection Area (Width) (Минимальная область обнаружения (ширина))	Если расстояние между камерой и пользователем слишком велико, параметр представляет собой минимальный процент ширины лица от общей ширины области распознавания. Для успешного распознавания лица фактический процент должен быть выше заданного значения. Другие процентные значения, расстояния и углы в этой таблице также должны соответствовать заданным условиям. Рекомендуемое значение: 14
Min. Detection Area (Height) (Минимальная область обнаружения (высота))	Если расстояние между камерой и пользователем слишком велико, параметр представляет собой минимальный процент высоты лица от общей высоты области распознавания. Для успешного распознавания лица фактический процент должен быть выше заданного значения. Другие процентные значения, расстояния и углы в этой таблице также должны соответствовать заданным условиям. Рекомендуемое значение: 12
Margin (Left) (Граница (слева))	Расстояние от левого края лица до левого края области распознавания. Для успешного распознавания лица фактическое расстояние должно превышать заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.
Margin (Right) (Граница (справа))	Расстояние от правого края лица до правого края области распознавания. Для успешного распознавания лица фактическое расстояние должно превышать заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.
Margin (Top) (Граница (сверху))	Расстояние от верхнего края лица до верхнего края области распознавания. Для успешного распознавания лица фактическое расстояние должно превышать заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.
Margin (Bottom) (Граница (снизу))	Расстояние от нижнего края лица до нижнего края области распознавания. Для успешного распознавания лица фактическое

Параметр	Описание
	расстояние должно превышать заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.
Pupillary Distance (Межцентровое расстояние)	Минимальное расстояние между центрами двух зрачков при распознавании лица. Фактическое расстояние должно быть больше, чем заданное значение. По умолчанию это значение равняется 40.

Настройка параметров дополнительной подсветки

Назначение:

Вы можете включать или выключать дополнительную подсветку. Если дополнительная подсветка работает в автоматическом режиме, вы также можете отрегулировать ее яркость.

Инструкция:

1. Выберите пункт **Other (Другие настройки) – Supplement Light Parameters (Параметры дополнительной подсветки)**, чтобы перейти на страницу настроек параметров дополнительной подсветки.



2. В раскрывающемся списке выберите режим работы дополнительной подсветки.
3. (Дополнительная опция) Если дополнительная подсветка работает в режиме **Auto (Автоматический)**, вы также сможете отрегулировать ее яркость.
4. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

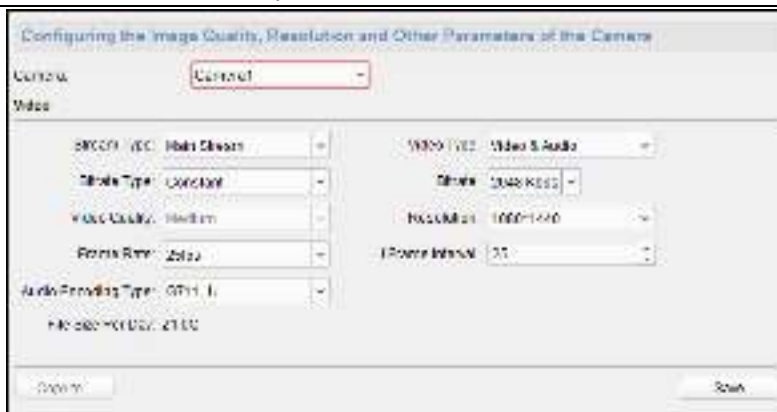
Настройка параметров видео и звука

Назначение:

Вы можете установить качество, разрешение и другие параметры камеры.

Инструкция:

1. Чтобы перейти к настройкам, выберите пункт **Image (Изображение) – Video & Audio (Видео и аудио)**.

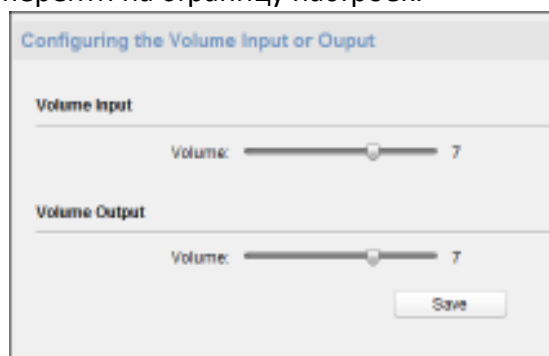


2. Задайте параметры камеры устройства, включая тип потока, тип передачи данных, качество видео, частоту кадров, тип кодирования звука, тип видео, скорость передачи данных, разрешение и интервал для информационных кадров.
3. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Настройка громкости на входе/выходе

Инструкция:

1. Выберите пункт **Image (Изображение) — Volume Input/Output (Громкость на входе/выходе)**, чтобы перейти на страницу настроек.



2. Задайте громкость устройства на входе/выходе.
3. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить введенные параметры.

Работа реле

1. Выберите пункт **Operation (Эксплуатация) -> Relay (Реле)**.
Вы можете просмотреть состояние реле.
2. Поставьте галочку возле соответствующего реле.
3. Нажмите кнопку **Open (Разомкнуть)** или **Close (Замкнуть)**, чтобы перевести реле в разомкнутое или замкнутое состояние.
4. (Дополнительная опция) Нажмите кнопку **Refresh (Обновить)**, чтобы получить обновленную информацию о состоянии реле.



Просмотр состояния реле

Выберите пункт **Status (Состояние)** -> **Relay (Реле)**, чтобы вывести на экран состояние реле.

Relay Status	
Relay	Status
Relay1	Close

6.4 Управление организациями

Вы можете добавлять, изменять или удалять организации.

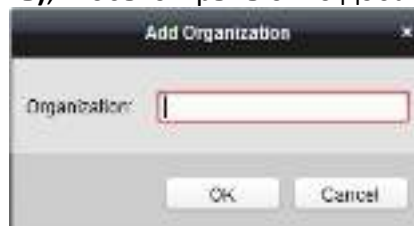
Нажмите на вкладку , чтобы перейти в окно управления пользователями и картами.

6.4.1 Добавление организации

Инструкция:

1. В списке организаций, расположенном слева, добавьте верхнюю организацию в качестве родительской.

Нажмите кнопку **Add (Добавить)**, чтобы открыть окно добавления организаций.



2. Введите желаемое название организации.
3. Нажмите кнопку **OK**, чтобы его сохранить.
4. Вы можете добавить несколько уровней организаций в соответствии со своими потребностями.

Чтобы добавить подуровни организации, выберите родительскую организацию и нажмите кнопку **Add (Добавить)**.

Повторите *шаги* 2 и 3, чтобы добавить подуровень организации.

После этого добавленная организация будет расцениваться системой как подуровень организации более высокого уровня.

Примечание. Вы можете создать до десяти уровней организаций.

6.4.2 Изменение параметров и удаление организаций

Выберите добавленную организацию и нажмите кнопку **Modify (Изменить)**, чтобы отредактировать ее название.

Выберите организацию и нажмите кнопку **Delete (Удалить)**, чтобы ее удалить.

Примечания.

- При удалении определенной организации также будут удалены все ее дочерние

элементы.

- Убедитесь в том, что в организации нет ни одного пользователя. Иначе вы не сможете ее удалить.

6.5 Управление пользователями:

После добавления организации можно будет добавить в нее пользователя и управлять его настройками, такими как выпуск карт в пакетном режиме, импорт и экспорт информации о пользователях в пакетном режиме и т. д.

Примечание. Вы можете добавить до 10 000 пользователей или карт.

6.5.1 Добавление пользователя

Добавление пользователя (основная информация)

Инструкция:

1. Выберите организацию из списка и нажмите кнопку **Add (Добавить)** на панели пользователей, чтобы открыть на экране диалоговое окно добавления пользователя.



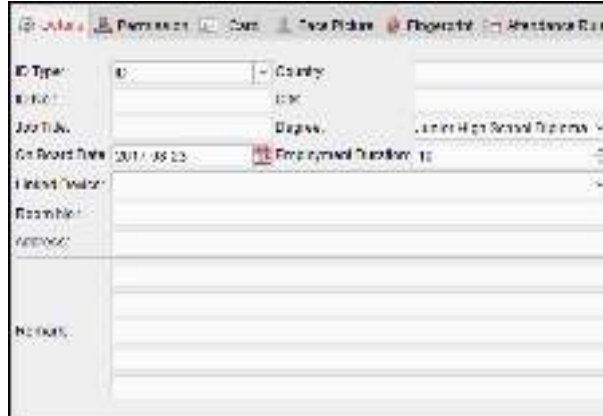
2. Номер пользователя создается автоматически и не может быть в дальнейшем изменен.
3. Введите основную информацию о пользователе, в том числе его имя, пол, номер телефона, дату рождения и адрес электронной почты.
4. Нажмите кнопку **Upload Picture (Загрузить изображение)**, чтобы выбрать изображение пользователя на локальном компьютере и загрузить его в клиент.
Примечание. Изображение должно быть в формате *.jpg.
5. (Дополнительная опция) Вы можете нажать кнопку **Take Photo (Сделать фотографию)**, чтобы получить изображение пользователя с помощью камеры компьютера.

6. Нажмите кнопку **ОК**, чтобы завершить процесс добавления сотрудника.

Добавление пользователя (подробная информация)

Инструкция:

1. Перейдите на вкладку **Details (Подробная информация)** на странице добавления пользователя.



2. Введите подробную информацию о пользователе, в том числе тип его идентификатора, номер идентификатора, страну проживания и другие данные по своему усмотрению.

➤ **Linked Device (Связанное устройство).** Вы можете привязать домофон к определенному пользователю.

Примечание. Если для связанного устройства был выбран параметр **Analog Indoor Station (Аналоговый домофон)**, на экране отобразится поле **Door Station (Вызывная панель)**, где нужно будет выбрать вызывную панель для привязки к аналоговому домофону.

➤ **Room No. (Номер комнаты).** Вы можете ввести номер комнаты пользователя.

3. Нажмите кнопку **ОК**, чтобы сохранить настройки.

Добавление пользователей (разрешения)

При добавлении пользователя вы можете назначить ему разрешения (в том числе разрешения на работу с устройством управления доступом и разрешения на управление доступом).

Примечание. Подробную информацию о настройке разрешений в сфере управления доступом см. в разделе 6.7 **Настройка разрешений**.

Инструкция:

1. Перейдите на вкладку **Permission (Разрешения)** на странице добавления пользователя.



2. В поле **Device Operation Role (Роль пользователя при работе с устройством)** выберите тип

соответствующего пользователя.

Normal User (Обычный пользователь). Этот пользователь может отмечаться о прибытии и уходе на устройстве, проходить через пункт управления доступом и т. д.

Administrator (Администратор). Этот пользователь обладает всеми разрешениями обычного пользователя, а также разрешениями на конфигурацию устройства, в том числе добавление обычных пользователей и т. д.

3. В списке выбора разрешений для пользователей отображаются все настроенные разрешения.

Поставьте галочки возле соответствующих разрешений и нажмите кнопку >, чтобы добавить их в список выбранных разрешений.

(Дополнительная опция) Нажмите кнопку >>, чтобы добавить все отображаемые разрешения в список выбранных разрешений.

(Дополнительная опция) Выберите разрешение в соответствующем списке и нажмите кнопку <, чтобы удалить его из списка. Нажмите кнопку <<, чтобы удалить все разрешения из списка.

4. Нажмите кнопку **ОК**, чтобы сохранить настройки.

Добавление пользователя (карта)

Вы можете добавлять и выпускать карту для конкретного пользователя.

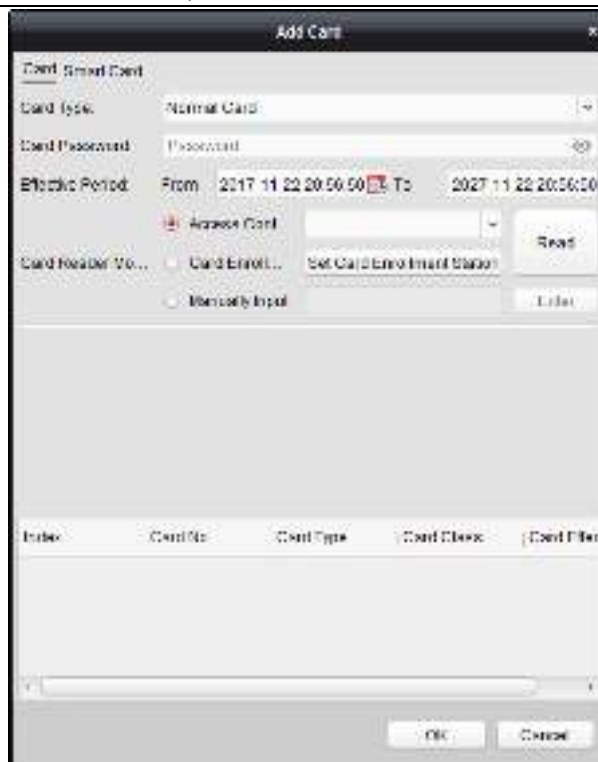
➤ Добавление обычной карты

Инструкция:

1. Перейдите на вкладку **Card (Карта)** на странице добавления пользователя.



2. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране окно добавления карты.
3. Нажмите кнопку **Card (Карта)**, чтобы открыть соответствующую вкладку.



4. Выберите требуемый тип карты.

- **Обычная карта**
- **Card for Disabled Person (Карта для людей с ограниченными возможностями).** Дверь будет открыта в течение заданного периода времени, который был выбран для владельца карты.
- **Card in Blacklist (Карта в черном списке).** Будут загружены параметры действия, связанного с проведением карты через считыватель, но дверь при этом не откроется.
- **Patrol Card (Проверочная карта).** Карта может использоваться для проверки рабочего состояния контролеров. Для контролеров также можно настроить разрешение на предоставление доступа.
- **Duress Card (Карта принудительного открытия).** Вы можете использовать эту карту, чтобы открыть дверь под принуждением. В то же время клиент получит информацию об открытии двери под принуждением.
- **Super Card (Карта суперпользователя).** Этой картой можно открыть любую дверь, связанную с контроллером, во время действия заданного графика работы.
- **Visitor Card (Карта посетителя).** Эта карта выдается посетителям. Для нее можно установить значение **Max. Swipe Times (Максимальное количество проведений в устройстве для считывания).**

Примечание. Параметр максимального количества проведений карты в устройстве для считывания можно выбирать в диапазоне 0... 255. Если данное значение равно 0, количество циклов считываний карты является неограниченным.

5. Введите пароль карты в поле **Card Password (Пароль карты).** Пароль карты может содержать от четырех до восьми символов.

Примечание. Если установлен режим аутентификации при помощи устройства для считывания карт **Card and Password (Карта и пароль), Password and Fingerprint (Пароль и отпечаток пальца), Card, Password, and Fingerprint (Карта, пароль и отпечаток пальца),**

при использовании карты нужно будет также ввести пароль, чтобы войти в дверь или выйти из нее. Подробную информацию см. в *разделе Уровень безопасности процедуры распознавания отпечатков пальцев*. Выберите уровень распознавания отпечатков пальцев в выпадающем списке.

- **Score (Степень соответствия):** Устройство оценивает снятое изображение в соответствии с углом рыскания, углом наклона и межцентровым расстоянием. Если оценка будет меньше заданного значения, распознавание лица считается неудачным.
- **Face Recognition Timeout Value (Длительность задержки при распознавании лиц):** Если длительность процесса распознавания превысит заданное значение, устройство выдаст соответствующее напоминание.
- **Face Recognition Interval (Интервал распознавания лиц):** Временной интервал между двумя циклами распознавания лиц при непрерывной работе. По умолчанию значение равно 0.
- **1:1 Match Threshold (Пороговое значение для сопоставления 1:1):** Установка порога опознавания при распознавании в режиме 1:1. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение равно 60.
- **1:N Match Threshold (Пороговое значение для сопоставления 1:N.):** Установка безопасного порога опознавания при распознавании в режиме 1:N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение равно 60.
- **Live Face Detection (Обнаружение живых лиц):** Включение и выключение функции обнаружения живых лиц. Если активировать эту функцию, устройство будет определять, живое лицо на изображении или нет.
- **Live Face Detection Security Level (Уровень обнаружения живых лиц):** После активации функции Live Face Detection (Обнаружение живых лица) можно установить соответствующий уровень живого лиц при их распознавании.
- **Application Mode (Режим работы):** Вы можете выбрать режим работы в помещении или любой другой режим, исходя из условий окружающей среды.
- Режим аутентификации при помощи устройства для считывания .Нажмите кнопку , чтобы задать период действия карты и дату его окончания.

6. Выберите режим работы устройства, в котором происходит считывание номера карты.

- **Access Controller Reader (Устройство для считывания карт контроллера доступа).** Разместите карту на считывателе карт контроллера доступа и нажмите кнопку **Read (Считать)**, чтобы получить номер карты.
- **Card Enrollment Station (Станция для регистрации карт).** Разместите карту на станции для регистрации карт и нажмите кнопку **Read (Считать)**, чтобы получить номер карты.
Примечание. Станция для регистрации карт должна быть подключена к клиенту, запущенному на компьютере. Нажмите кнопку **Set Card Enrollment Station (Настройка станции для регистрации карт)**, чтобы открыть на экране следующее диалоговое окно.



- 1) Выберите тип станции для регистрации карт.

Примечание. В настоящее время обеспечивается возможность использования устройств для считывания карт DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

- 2) Укажите номер последовательного порта, скорость передачи данных, значение таймера, параметры зуммера или тип номера карты.

Если используется карта M1 и нужно активировать функцию ее шифрования, поставьте галочку в пункте **Enable (Включить)** рядом с надписью **M1 Card Encryption (Шифрование карт M1)** и нажмите кнопку **Modify (Изменить)**, чтобы выбрать соответствующий сектор.

- 3) Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Нажмите кнопку **Restore Default Value (Восстановить значения по умолчанию)**, чтобы сбросить настройки до значений по умолчанию.

- **Manually Input (Ввод в ручном режиме).** Введите номер карты и нажмите кнопку **Enter (Ввод)**, чтобы сохранить его.

7. Нажмите кнопку **OK** — после этого произойдет выпуск карты для пользователя.

8. (Дополнительная опция) Выберите добавленную карту и нажмите кнопку **Modify (Изменить)**, или **Delete (Удалить)**, чтобы отредактировать или удалить ее.

9. (Дополнительная опция) Вы можете сгенерировать и сохранить QR-код карты для прохождения аутентификации по QR-коду.

- 1) Выберите добавленную карту и нажмите кнопку **QR Code (QR-код)**, чтобы сгенерировать QR-код карты.

- 2) Во всплывающем окне с QR-кодом нажмите кнопку **Download (Скачать)**, чтобы сохранить QR-код на локальном компьютере.

QR-код можно распечатать, чтобы в дальнейшем проходить процесс аутентификации на указанном устройстве.

Примечание. Устройство должно поддерживать функцию аутентификации по QR-коду. Подробную информацию о настройке функции аутентификации по QR-коду см. в руководстве по работе с указанным устройством.

10. (Дополнительная опция) Вы можете нажать кнопку **Link Fingerprint (Привязать отпечаток пальца)**, чтобы связать карту с отпечатком пальца пользователя. В этом случае для прохождения через дверь человек может поместить палец на сканер, а не прикладывать карту.

11. (Дополнительная опция) Нажмите кнопку **Link Face Picture (Привязать изображение лица)**,

чтобы связать карту с изображением лица. В этом случае для открытия двери пользователь сможет просканировать свое лицо, а не прикладывать карту.

12. Нажмите кнопку **ОК**, чтобы сохранить настройки.

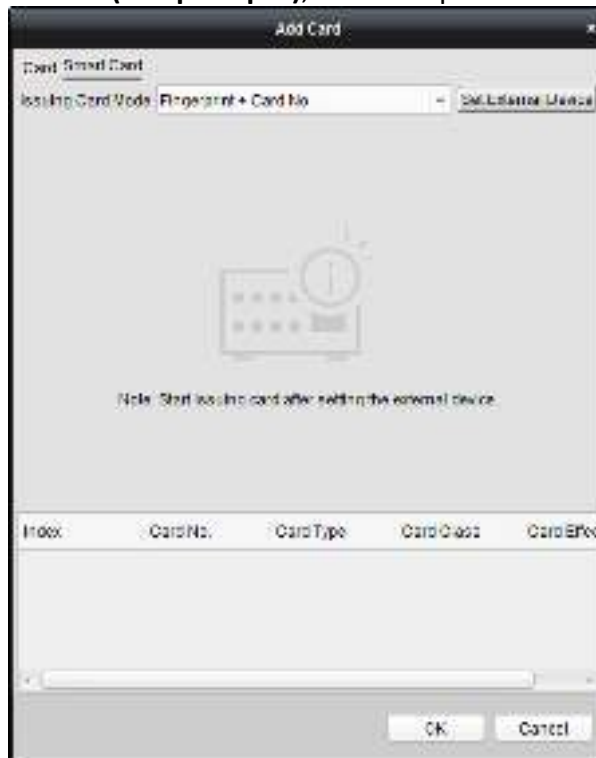
➤ Добавление смарт-карты

Назначение:

Вы можете хранить отпечатки пальцев и информацию ID-карты на смарт-карте. При прохождении аутентификации после считывания смарт-карты на устройстве можно отсканировать свой отпечаток пальца или провести через устройство свою идентификационную карту. Устройство сравнит информацию об отпечатке пальца или идентификационной карте на смарт-карте с имеющимися данными. Если вы используете смарт-карту для аутентификации, вам не нужно заранее сохранять отпечатки пальцев или информацию ID-карты в устройстве.

Инструкция:

1. На странице **Add Person (Добавление пользователя)** укажите основную информацию о пользователе.
2. Нажмите кнопку **Card (Карта)**, чтобы перейти на соответствующую вкладку.
3. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране окно добавления карты.
4. Нажмите кнопку **Smart Card (Смарт-карта)**, чтобы перейти на соответствующую вкладку.



5. В раскрывающемся списке выберите режим выдачи карт.
6. Настройте параметры внешнего устройства.
 - 1) Нажмите кнопку **Set External Device (Настройка параметров внешнего устройства)**, чтобы перейти на соответствующую страницу.
 - 2) (Дополнительная опция) Снова выберите режим выдачи карт.
 - 3) Настройте параметры станции для регистрации карт.
 - 4) Если в качестве режима выдачи выбрано значение **Fingerprint + Card No. (Отпечаток пальца + номер карты)**, укажите модель устройства для ввода отпечатков пальцев. Если в качестве режима выдачи значение **ID Card No.+ Card No. (Номер идентификационной карты + номер карты)**, укажите модель устройства для

считывания идентификационных карт.

Если в качестве режима выдачи значение **Fingerprint + ID Card No. + Card No. (Отпечаток пальца + номер идентификационной карты + номер карты)**, укажите модель устройства для ввода отпечатков пальцев и устройства для считывания идентификационных карт.

5) Нажмите кнопку **ОК**, чтобы сохранить настройки.

7. Выберите тип смарт-карты.

- **Обычная карта**
- **Card for Disabled Person (Карта для людей с ограниченными возможностями).** Дверь будет открыта в течение заданного периода времени, который был выбран для владельца карты.
- **Card in Blacklist (Карта в черном списке).** Будут загружены параметры действия, связанного с проведением карты через считыватель, но дверь при этом не откроется.
- **Patrol Card (Проверочная карта).** Карта может использоваться для проверки рабочего состояния контролеров. Для контролеров также можно настроить разрешение на предоставление доступа.
- **Duress Card (Карта принудительного открытия).** Вы можете использовать эту карту, чтобы открыть дверь под принуждением. В то же время клиент получит информацию об открытии двери под принуждением.
- **Super Card (Карта суперпользователя).** Этой картой можно открыть любую дверь, связанную с контроллером, во время действия заданного графика работы.
- **Visitor Card (Карта посетителя).** Эта карта выдается посетителям. Для нее можно установить значение **Max. Swipe Times (Максимальное количество проведений в устройстве для считывания)**.

Примечание. Параметр максимального количества проведений карты в устройстве для считывания можно выбирать в диапазоне 0... 255. Если данное значение равно 0, количество циклов считываний карты является неограниченным.

- **Dismiss Card (Карта для отключения).** Она используется для отключения сигнала тревоги.

8. Выберите другие параметры карты.

- 1) Установите пароль для карты.
- 2) Укажите дату окончания действия карты.
- 3) Отсканируйте свой отпечаток пальца и проведите идентификационную карту через устройство, воспользовавшись предоставленной подсказкой.
- 4) Проведите смарт-карту через устройство.

Информация о добавленной карте отобразится в списке, который расположен ниже.

9. Нажмите кнопку **ОК** — после этого произойдет выпуск карты для пользователя.

10. (Дополнительная опция) Выберите добавленную карту и нажмите кнопку **Modify (Изменить)**, или **Delete (Удалить)**, чтобы отредактировать или удалить ее.

11. (Дополнительная опция) Вы можете сгенерировать и сохранить QR-код карты для прохождения аутентификации по QR-коду.

- 1) Выберите добавленную карту и нажмите кнопку **QR Code (QR-код)**, чтобы сгенерировать QR-код карты.
- 2) Во всплывающем окне с QR-кодом нажмите кнопку **Download (Скачать)**, чтобы сохранить QR-код на локальном компьютере.

QR-код можно распечатать, чтобы в дальнейшем проходить процесс аутентификации на указанном устройстве.

Примечание. Устройство должно поддерживать функцию аутентификации по QR-коду. Подробную информацию о настройке функции аутентификации по QR-коду см. в руководстве по работе с указанным устройством.

12. (Дополнительная опция) Нажмите кнопку **Link Fingerprint (Привязать отпечаток пальца)**, чтобы связать карту с отпечатком пальца пользователя. В этом случае для прохождения через дверь пользователь сможет приложить палец к сканеру, а не прикладывать карту.
13. (Дополнительная опция) Нажмите кнопку **Link Face Picture (Привязать изображение лица)**, чтобы связать карту с изображением лица. В этом случае для открытия двери пользователь сможет просканировать свое лицо, а не прикладывать карту.
14. Нажмите кнопку **ОК**, чтобы сохранить настройки.

Добавление сотрудника (распознавание лиц)

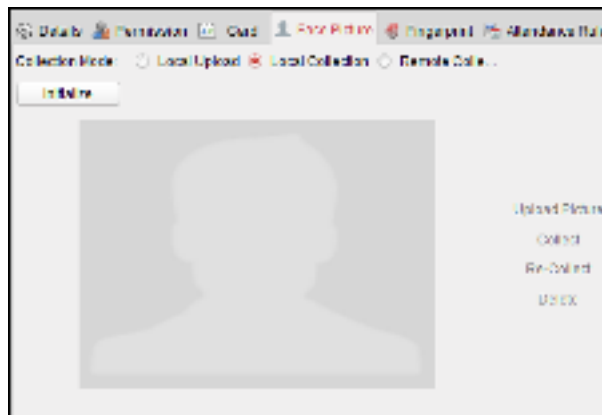
Вы можете получать изображения лица двумя способами: локальный и удаленный сбор.

- **Local Upload (Локальная загрузка).** Загрузка изображений лиц с локального компьютера.
- **Local Collection (Локальный сбор).** Считывание изображения лица с помощью специального сканера.
- **Remote Collection (Удаленный сбор).** Считывание изображения лица с помощью терминала управления доступом.

Примечание. Терминал управления доступом должен поддерживать функцию распознавания лиц.

Инструкция:

1. Перейдите на вкладку **Face Picture (Изображение лица)** на странице добавления пользователя.



2. Загрузка изображений лиц с локального компьютера:
 - 1) Выберите пункт **Local Upload (Локальная загрузка)**.
 - 2) Нажмите кнопку **Upload Picture (Загрузить изображение)** и выберите фотографию лица, которая хранится на локальном ПК.

Примечание. Загруженное изображение должно быть в формате JPG, а его размер не может превышать 200 Кбайт.

- 3) (Дополнительная опция) По умолчанию загруженное изображение лица должно быть проверено устройством.

Устройство для проверки загруженной фотографии можно выбрать из раскрывающегося списка. Процедура добавления изображения лица завершается

только после его проверки.

3. Считывание изображения лица с помощью специального сканера:

- 1) Выберите пункт **Local Collection (Локальный сбор)**.
- 2) Подключите сканер изображений лиц к ПК.
- 3) Выберите тип устройства.

Примечание. В настоящее время обеспечивается возможность использования сканера изображений лиц DS2CS5432B-S.

- 4) (Дополнительная опция) Вы можете нажать кнопку **Initialize (Инициализировать)**, чтобы активировать сканер изображений лиц.

4. Считывание изображения лица с помощью терминала управления доступом:

- 1) Выберите пункт **Remote Collection (Удаленный сбор)**.
- 2) Нажмите кнопку **Select Device (Выбрать устройство)**, чтобы выбрать терминал управления доступом, который поддерживает функцию распознавания лиц.

5. Нажмите кнопку **Collect (Съемка)**, чтобы выполнить захват изображения лица.

Чтобы выполнить захват еще раз, можно нажать кнопку **Re-Collect (Повторная съемка)**.

Чтобы удалить снимок, можно нажать кнопку **Delete (Удалить)**.

6. Нажмите кнопку **OK**, чтобы сохранить настройки.

Добавление пользователя (отпечаток пальца)

Инструкция:

1. Перейдите на вкладку **Fingerprint (Отпечаток пальца)** на странице добавления пользователя.



2. Выберите значение **Local Collection (Локальный сбор)**.

3. Перед регистрацией отпечатка пальца сначала нужно подключить сканер к компьютеру и настроить его параметры.

Нажмите кнопку **Set Fingerprint Machine (Настройка сканера отпечатков пальцев)**, чтобы открыть на экране следующее диалоговое окно.



- 1) Выберите тип устройства.

В настоящее время обеспечивается возможность использования сканеров отпечатков пальцев DS-K1F800-F, DS-K1F810-F, DS-K1F820-F и DS-K1F181-F.

- 2) Для сканера отпечатков пальцев DS-K1F800-F можно задать номер последовательного порта, скорость передачи данных и параметры сверхурочной работы.
- 3) Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.
Нажмите кнопку **Restore Default Value (Восстановить значения по умолчанию)**, чтобы сбросить настройки до значений по умолчанию.

Примечания.

- Номер последовательного порта должен соответствовать номеру последовательного порта на компьютере. Номер последовательного порта можно узнать в диспетчере устройств компьютера.
 - Значение скорости передачи данных нужно устанавливать в соответствии с параметрами внешнего устройства для считывания отпечатков пальцев и карт. По умолчанию используется значение 19 200.
 - Значение в поле **Timeout after (Промежуток времени)** указывает на фактическое время получения отпечатка пальца. Если пользователь не отсканирует отпечаток пальца вовремя или сделает это неправильно, устройство сообщит о том, что процедура получения отпечатка пальца завершена.
4. Нажмите кнопку **Start (Начать)** и выберите отпечаток пальца для начала процедуры его получения.
 5. Поднимите палец и дважды оставьте отпечаток на сканере, чтобы зарегистрировать его в клиенте.
 6. (Дополнительная опция) Нажмите кнопку **Remote Collection (Удаленное получение отпечатка)**, чтобы зарегистрировать отпечаток пальца с помощью устройства.
- Примечание.** Устройство должно поддерживать эту функцию.
7. (Дополнительная опция) Выберите зарегистрированный отпечаток пальца и нажмите кнопку **Delete (Удалить)**, чтобы его удалить.
Нажмите кнопку **Clear (Очистить)**, чтобы удалить все отпечатки пальцев.
 8. Нажмите кнопку **OK**, чтобы сохранить отпечатки пальцев.

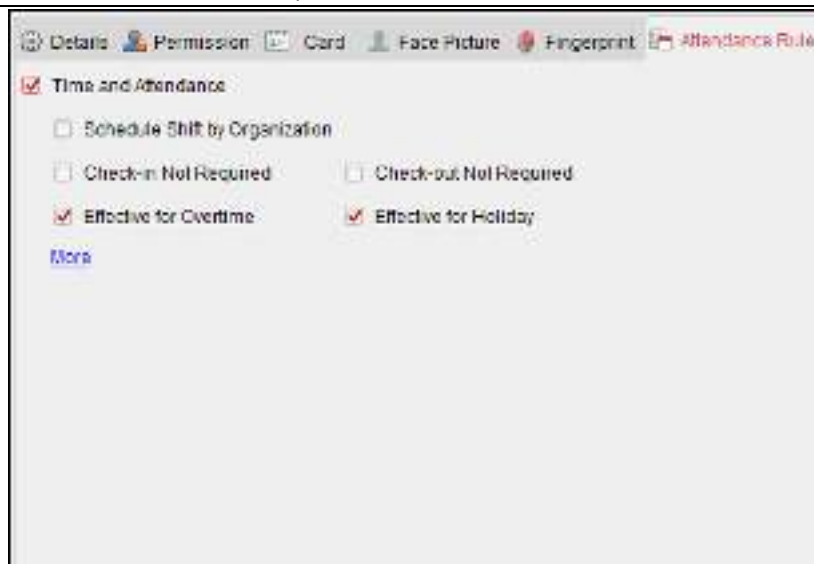
Добавление пользователя (правило посещаемости)

Вы можете задать правило посещаемости для конкретного пользователя.

Примечание. Если для соответствующей зоны был выбран режим **Non-Residence (Нежилое помещение)** при первом запуске программного обеспечения на экране появится эта вкладка.

Инструкция:

1. Перейдите на вкладку **Attendance Rule (Правило посещаемости)** на странице добавления пользователя.



2. Если пользователь имеет отношение к программе учета рабочего времени, поставьте галочку в пункте **Time and Attendance (Учет рабочего времени)**, чтобы активировать данную функцию для этого сотрудника. После этого информация о посещаемости будет записываться и анализироваться с целью учета рабочего времени.
Подробную информацию об учете рабочего времени можно узнать, нажав кнопку **More (Дополнительная информация)** и перейдя в модуль учета рабочего времени.
3. Нажмите кнопку **ОК**, чтобы сохранить настройки.

Импорт информации о сотрудниках

Назначение:

Вы можете импортировать информацию о нескольких лицах (включая идентификационную информацию, данные отпечатка пальца и номер карты, привязанной к отпечатку) в клиентское программное обеспечение с помощью импорта пакетного файла Excel с локального ПК.

Инструкция:

1. Нажмите кнопку **Import Person (Импорт сотрудника)** и выберите пункт **Person Information (Информация о сотруднике)** в качестве данных, которые нужно импортировать.
2. Во всплывающем окне нажмите кнопку **Download Template for Importing Person (Загрузить шаблон для импорта информации)**, чтобы загрузить соответствующий шаблон.
3. Введите информацию о людях в скачанный шаблон.
Примечание. Если у человека есть несколько карт, отделите номера карты точкой с запятой.
4. Выберите файл Excel, в котором указана информация о сотруднике.
5. Нажмите кнопку **ОК**, чтобы начать процедуру импорта.
Примечание. Если номер сотрудника уже существует в базе данных клиентского программного обеспечения, после импорта информация о человеке будет автоматически заменена.

Импорт фотографий сотрудников

Назначение:

После добавления людей вы сможете импортировать несколько изображений человека одним пакетом — для этого нужно импортировать ZIP-архив с изображениями в клиентское

программное обеспечение.

Инструкция:

1. Присвойте название фотографии человека в соответствии с его именем.

Примечание. Изображение должно быть в формате JPG, его размер не может превышать 200 КБ.

2. Сожмите файл, в котором содержатся личные фотографии, создав архив в формате ZIP.
3. В модуле **Person and Card (Пользователи и карты)** нажмите кнопку **Import Person (Импортировать пользователя)** и выберите пункт **Person Pictures (Фотографии пользователей)** в качестве данных, которые нужно импортировать.
4. В появившемся на экране окне выберите ZIP-архив.
5. Нажмите кнопку **ОК**, чтобы начать процедуру импорта.

Примечание. По умолчанию изображение импортированного лица привязывается к первой карте человека.

Экспорт информации о сотруднике

Вы можете экспортировать данные добавленного человека на локальный ПК в формате Excel.

Инструкция:

1. После добавления пользователя нажмите кнопку **Export Person (Экспорт сотрудника)**, чтобы открыть на экране соответствующее диалоговое окно.
2. Выберите путь сохранения экспортированного файла Excel.
3. Выберите пункты информации о сотруднике, которые нужно экспортировать.
4. Нажмите кнопку **ОК**, чтобы начать процедуру экспорта.

Получение информации о пользователе с устройства управления доступом

Если в добавленное устройство управления доступом записана информация о пользователе (в том числе личные сведения о человеке, отпечаток пальца, информация о выпущенной карте), вы можете получить информацию о пользователе с устройства и импортировать ее в клиент для дальнейшей работы.

Примечание. Эта функция поддерживается только устройствами, подключенными через TCP/IP.

Инструкция:

1. В списке организаций, расположенном слева, выберите организацию, в которую нужно импортировать информацию о пользователях.
2. Нажмите кнопку **Get Person (Получить информацию о пользователях)**, чтобы открыть на экране следующее диалоговое окно.



3. На дисплее появятся добавленные устройства управления доступом.
4. Выберите устройство и нажмите кнопку **ОК**, чтобы начать процедуру получения информации о пользователе с этого устройства.
Чтобы начать процедуру получения информации о пользователе, вы также можете дважды нажать на названии устройства.

Примечания.

- Информация о пользователе, в том числе подробная информация о человеке, информация об отпечатке пальца (если он зарегистрирован) и связанной карте (если она выпущена), будет импортирована в выбранную организацию.
- Если поле с именем человека, которое хранится на устройстве, не заполнено, после импорта в клиент в него будет внесен номер выпущенной карты.
- По умолчанию указан **Male (Мужской)** пол.
- Вы можете импортировать до 10 000 пользователей.

6.5.2 Управление пользователями

Редактирование параметров и удаление пользователя

Чтобы изменить информацию о пользователе и установленное для него правило посещаемости, нажмите кнопку  или  в столбце **Operation (Операция)** или выберите требуемого человека и нажмите кнопку **Modify (Изменить)**, чтобы открыть диалоговое окно для редактирования настроек пользователя.

Нажмите кнопку , чтобы просмотреть записи об использовании карты этого пользователя. Чтобы удалить пользователя, выберите его и нажмите кнопку **Delete (Удалить)**.

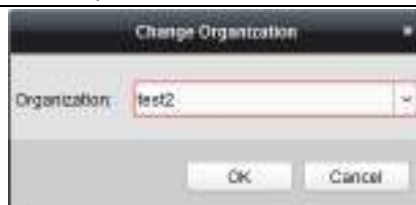
Примечание. Если карта была выпущена для текущего пользователя, после его удаления привязка карты будет аннулирована.

Перемещение пользователя в другую организацию

Если это необходимо, вы можете переместить пользователя в другую организацию.

Инструкция:

1. Выберите пользователя из списка и нажмите кнопку **Change Organization (Изменить организацию)**.



2. Выберите организацию, в которую нужно переместить пользователя.
3. Нажмите кнопку **OK**, чтобы сохранить настройки.

Поиск пользователей

Вы можете ввести ключевое слово номера карты или имя пользователя в поле поиска и нажать кнопку **Search (Поиск)**, чтобы найти этого человека.

Нажмите кнопку **Read (Считать)**, чтобы получить номер карты с подключенной станции для регистрации карт.

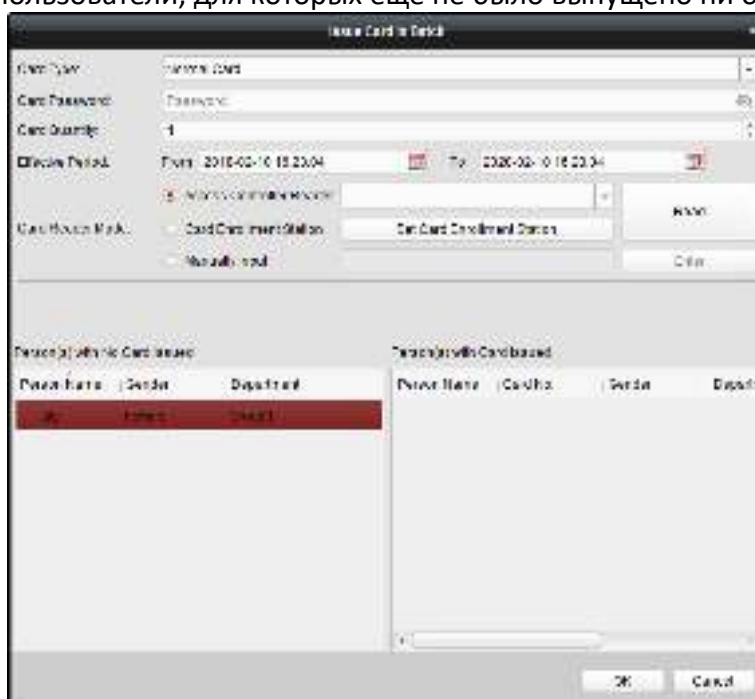
Выберите пункт **Set Card Enrollment Station (Настройка станции для регистрации карт)** из выпадающего списка, чтобы задать требуемые параметры устройства.

6.5.3 Выпуск карт в пакетном режиме

Пользователю, для которого еще не было выпущено ни одной карты, можно выпустить сразу несколько карт.

Инструкция:

1. Нажмите кнопку **Issue Card in Batch (Выпуск карт в пакетном режиме)**, чтобы открыть на экране следующее диалоговое окно.
В списке **Person(s) with No Card (Пользователи без карт)** будут отображены все добавленные пользователи, для которых еще не было выпущено ни одной карты.



2. Выберите требуемый тип карты.

Примечание. Подробную информацию о типах карт см. в разделе *Добавление пользователя*.

3. Введите пароль карты в поле **Card Password (Пароль карты)**. Пароль карты может содержать от четырех до восьми символов.

Примечание. Если установлен режим аутентификации при помощи устройства для считывания карт **Card and Password (Карта и пароль)**, **Password and Fingerprint (Пароль и отпечаток пальца)**, **Card, Password, and Fingerprint (Карта, пароль и отпечаток пальца)**, при использовании карты нужно будет также ввести пароль, чтобы войти в дверь или выйти из нее. Подробную информацию см. в *разделе Уровень безопасности процедуры распознавания отпечатков пальцев*. Выберите уровень распознавания отпечатков пальцев в выпадающем списке.

- **Score (Степень соответствия):** Устройство оценивает снятое изображение в соответствии с углом рыскания, углом наклона и межцентровым расстоянием. Если оценка будет меньше заданного значения, распознавание лица считается неудачным.
- **Face Recognition Timeout Value (Длительность задержки при распознавании лиц):** Если длительность процесса распознавания превысит заданное значение, устройство выдаст соответствующее напоминание.
- **Face Recognition Interval (Интервал распознавания лиц):** Временной интервал между двумя циклами распознавания лиц при непрерывной работе. По умолчанию значение равно 0.
- **1:1 Match Threshold (Пороговое значение для сопоставления 1:1):** Установка порога опознавания при распознавании в режиме 1:1. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение равно 60.
- **1:N Match Threshold (Пороговое значение для сопоставления 1:N):** Установка безопасного порога опознавания при распознавании в режиме 1:N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение равно 60.
- **Live Face Detection (Обнаружение живых лиц):** Включение и выключение функции обнаружения живых лиц. Если активировать эту функцию, устройство будет определять, живое лицо на изображении или нет.
- **Live Face Detection Security Level (Уровень обнаружения живых лиц):** После активации функции Live Face Detection (Обнаружение живых лиц) можно установить соответствующий уровень живого лица при их распознавании.
- **Application Mode (Режим работы):** Вы можете выбрать режим работы в помещении или любой другой режим, исходя из условий окружающей среды.

Режим аутентификации при помощи устройства для считывания

4. Введите количество карт, выпускаемых для каждого пользователя.
Например, если количество карт равно 3, вы можете считать или ввести номера трех карт для каждого пользователя.
5. Нажмите кнопку , чтобы задать период действия карты и дату его окончания.
6. В списке **Person(s) with No Card (Пользователи без карт)**, расположенном слева, выберите человека, для которого нужно выпустить карту.

Примечание. Нажмите на столбец **Person Name (Имя пользователя)**, **Gender (Пол)** и **Department (Отдел)**, чтобы отсортировать пользователей.

7. Выберите режим работы устройства, в котором происходит считывание номера карты.
- **Access Controller Reader (Устройство для считывания карт контроллера доступа).** Разместите карту на считывателе карт контроллера доступа и нажмите кнопку **Read (Считать)**, чтобы получить номер карты.
 - **Card Enrollment Station (Станция для регистрации карт).** Разместите карту на станции для регистрации карт и нажмите кнопку **Read (Считать)**, чтобы получить номер карты.
- Примечание.** Станция для регистрации карт должна быть подключена к клиенту, запущенному на компьютере. Нажмите кнопку **Set Card Enrollment Station (Настройка станции для регистрации карт)**, чтобы открыть на экране следующее диалоговое окно.



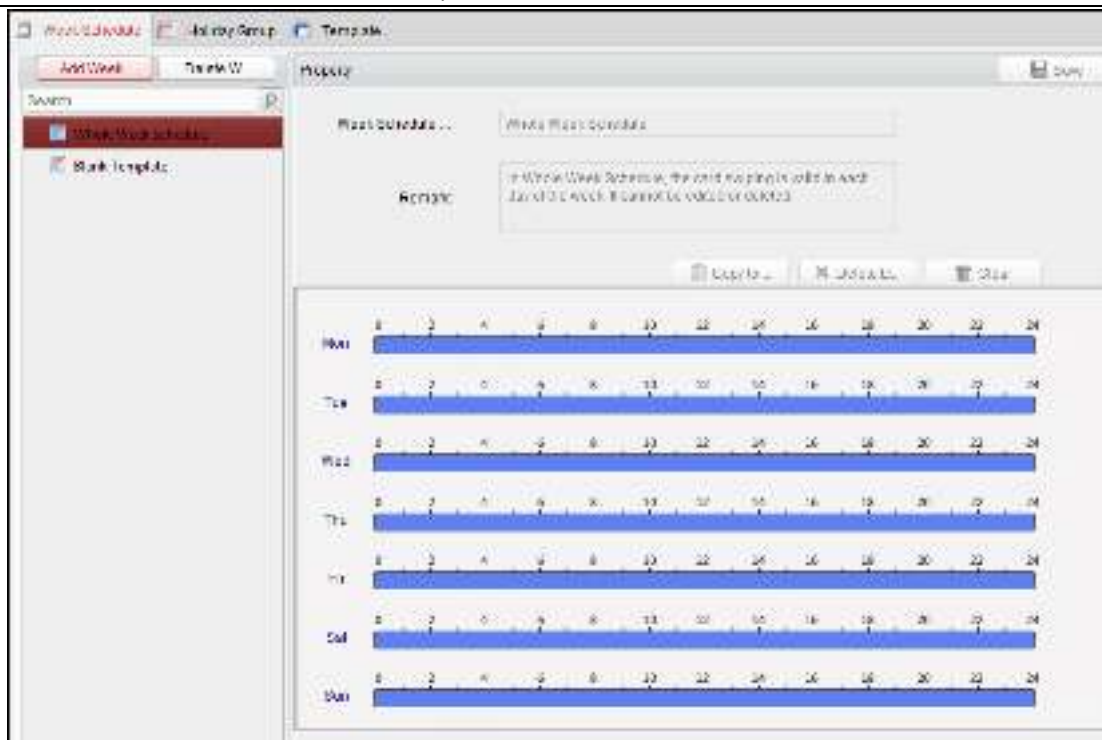
- 1) Выберите тип станции для регистрации карт.
Примечание. В настоящее время обеспечивается возможность использования устройств для считывания карт DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.
 - 2) Задайте параметры подключенной станции для регистрации карт.
Если используется карта M1 и нужно активировать функцию ее шифрования, поставьте галочку в пункте **Enable (Включить)** рядом с надписью **M1 Card Encryption (Шифрование карт M1)** и нажмите кнопку **Modify (Изменить)**, чтобы выбрать соответствующий сектор.
 - 3) Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.
Нажмите кнопку **Restore Default Value (Восстановить значения по умолчанию)**, чтобы сбросить настройки до значений по умолчанию.
- **Manually Input (Ввод в ручном режиме).** Введите номер карты и нажмите кнопку **Enter (Ввод)**, чтобы сохранить его.
8. После выпуска карты, информация о пользователе и карте будет отображаться в списке **Person(s) with Card Issued (Пользователи с выпущенными картами)**.
9. Нажмите кнопку **OK**, чтобы сохранить настройки.

6.6 Графики и шаблоны

Назначение:

Вы можете настроить шаблон, в том числе недельный график работы и график нерабочих дней. После создания настроенных шаблонов вы можете использовать их для предоставления разрешений на управление доступом, чтобы данные разрешения были действительными только на время действия шаблона.

Нажмите кнопку , чтобы перейти в окно графиков и шаблонов.



Вы можете управлять графиком предоставления разрешений на управления доступом, в том числе недельным графиком работы, графиком нерабочих дней и шаблонами. Подробную информацию о настройках разрешений см. в *разделе 6.7 Настройка разрешений*.

6.6.1 Недельный график работы

Нажмите на вкладку **Week Schedule (Недельный график работы)**, чтобы перейти в окно управления недельным графиком работы.

По умолчанию в клиенте используются два типа недельных графиков работы: **Whole Week Schedule (График работы на всю неделю)** и **Blank Schedule (Пустой график)**, которые нельзя удалить или изменить.

- **Whole Week Schedule (График работы на всю неделю)**. Использование карты будет регистрироваться в каждый день недели.
- **Blank Schedule (Пустой график)**. Использование карты не будет регистрироваться в каждый день недели.

Чтобы настроить пользовательские графики работы, вы можете выполнить описанные ниже действия.

Инструкция:

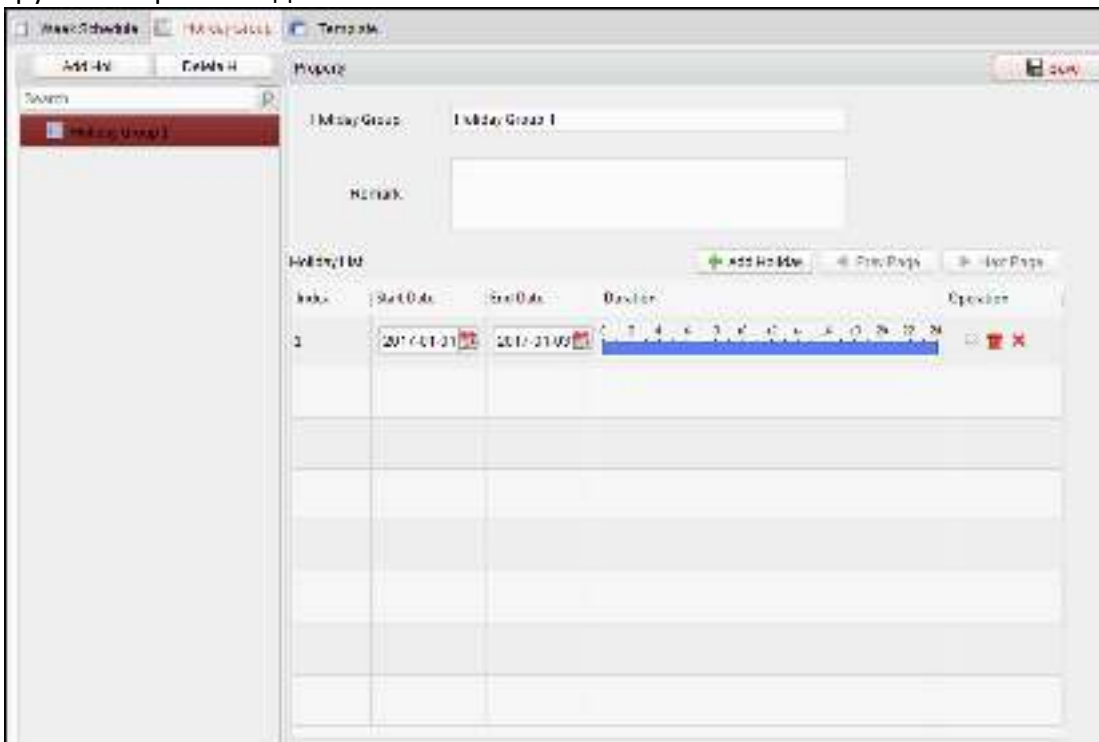
1. Нажмите кнопку **Add Week Schedule (Добавить недельный график работы)**, чтобы перейти в окно добавления графика.



2. Введите название недельного графика работы и нажмите кнопку **ОК**, чтобы его добавить.
3. Выберите добавленный недельный график работы в соответствующем списке, чтобы просмотреть его свойства, которые будут отображаться в правой части экрана.
Вы можете изменить название недельного графика работы, а также добавить комментарии.
4. Чтобы активировать настроенное разрешение, нажмите и перетащите его в соответствующий день, указанный в недельном графике работы.
Примечание. Вы можете установить до восьми периодов времени для каждого дня, указанного в графике.
5. Когда вид курсора изменится на , вы сможете переместить выбранный отрезок времени, который только что был изменен. Также можно изменить отображаемую точку времени, чтобы задать точный период.
Когда вид курсора изменится на , вы сможете изменить длительность выбранного отрезка времени.
6. Также можно выбрать отрезок времени на графике и нажать кнопку **Delete Duration (Удалить отрезок)**, чтобы его удалить.
Или нажмите кнопку **Clear (Очистить)**, чтобы удалить все отрезки времени.
Или нажмите кнопку **Copy to Week (Скопировать для всех дней недели)**, чтобы скопировать настройки отрезка времени для всех дней недели.
7. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

6.6.2 Группа нерабочих дней

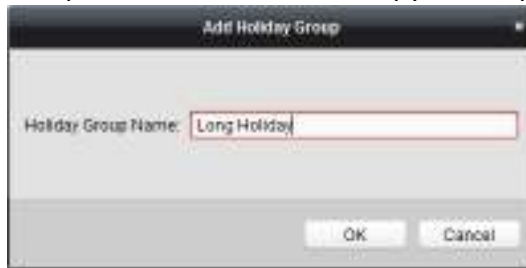
Выберите вкладку **Holiday Group (Группа нерабочих дней)**, чтобы перейти в окно управления группой нерабочих дней.



Инструкция:

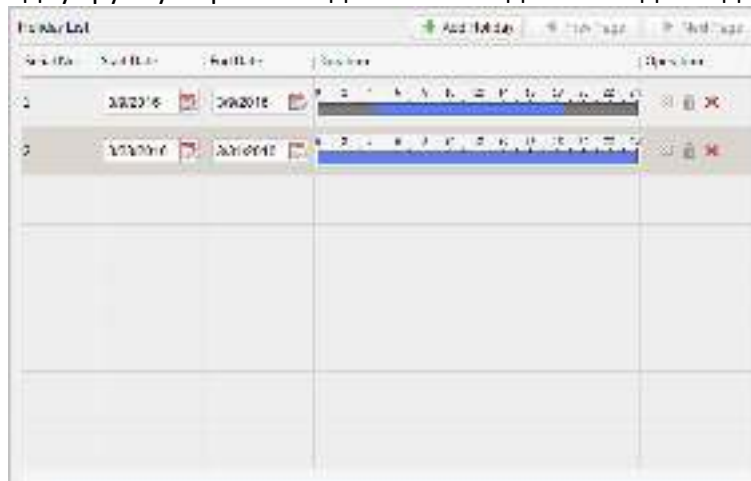
1. Нажмите кнопку **Add Holiday Group (Добавить группу нерабочих дней)**, расположенную в

левой части экрана, чтобы открыть окно добавления группы нерабочих дней.



2. Укажите название группы нерабочих дней в текстовом поле и нажмите кнопку **ОК**, чтобы добавить эту группу.
3. Выберите добавленную группу нерабочих дней, чтобы изменить ее название и добавить примечания.
4. Нажмите на значок **Add Holiday Group (Добавить нерабочий день)**, расположенный в правой части экрана, чтобы добавить период нерабочих дней в соответствующий список и выбрать его длительность.

Примечание. В одну группу нерабочих дней можно добавить до 16 дней.



- 1) Нажмите и перетащите курсор на графике для периода, чтобы определить его длительность. Для данного периода времени будет активировано настроенное разрешение.

Примечание. Вы можете установить до восьми периодов времени для каждого периода в графике.

- 2) Когда вид курсора изменится на , вы сможете переместить выбранный отрезок времени, который только что был изменен. Также можно изменить отображаемую точку времени, чтобы задать точный период.
- 3) Когда вид курсора изменится на , вы сможете изменить длительность выбранного отрезка времени.
- 4) Также можно выбрать отрезок времени на графике и нажать кнопку , чтобы его удалить.
Или нажмите кнопку , чтобы удалить все отрезки времени нерабочих дней.
Или нажмите кнопку , чтобы удалить конкретный нерабочий день.

5. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

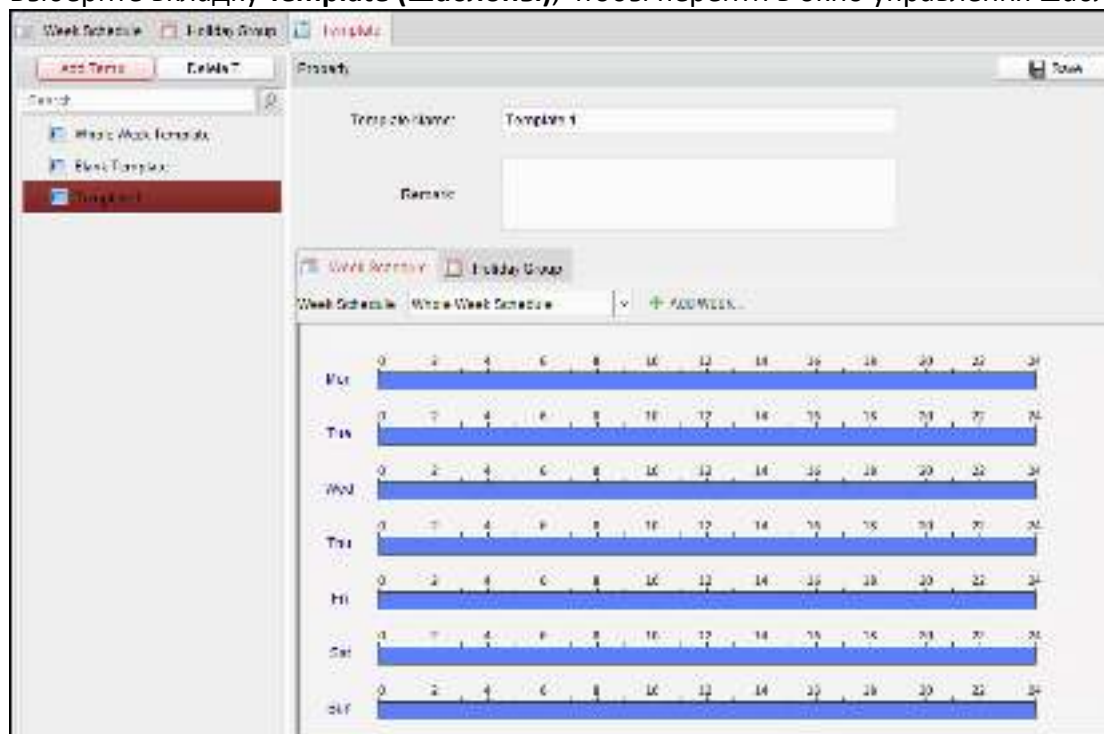
Примечание. Периоды нерабочих дней не могут накладываться друг на друга.

6.6.3 Шаблоны

После создания недельного графика работы и группы нерабочих дней можно настроить шаблон, который будет содержать недельный график и график группы нерабочих дней.

Примечание. Приоритет использования графика группы нерабочих дней является более высоким, чем у недельного графика работы.

Выберите вкладку **Template (Шаблоны)**, чтобы перейти в окно управления шаблонами.



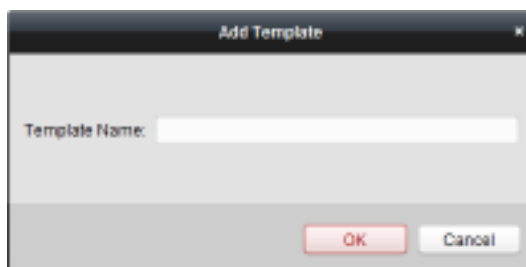
По умолчанию используются два предварительно настроенных шаблона: **Whole Week Template (Шаблон на всю неделю)** и **Blank Template (Пустой шаблон)**, которые нельзя удалить или изменить.

- **Whole Week Template (Шаблон на всю неделю).** Карту можно использовать в каждый день недели, а график группы нерабочих дней не предусмотрен.
- **Blank Template (Пустой шаблон).** Карту нельзя использовать в каждый день недели, а график группы нерабочих дней не предусмотрен.

Вы также можете настроить пользовательские шаблоны.

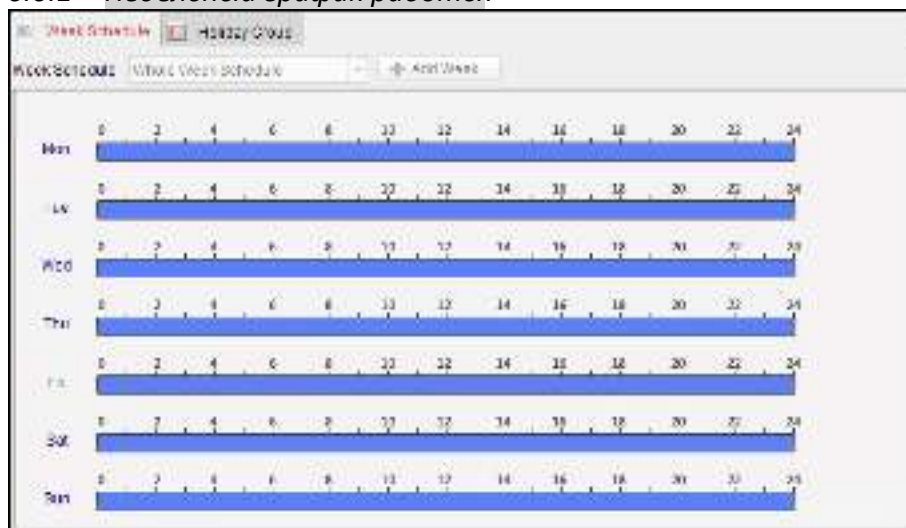
Инструкция:

1. Нажмите кнопку **Add Template (Добавить шаблон)**, чтобы перейти в окно добавления шаблонов.



2. Укажите название шаблона в текстовом поле и нажмите кнопку **OK**, чтобы добавить шаблон.

3. Выберите добавленный шаблон и измените его параметры, которые отображаются в правой части экрана. Вы можете изменить название шаблона и добавить комментарии.
4. Выберите недельный график работы, который нужно использовать в данном шаблоне. Перейдите на вкладку **Week Schedule (Недельный график работы)** и выберите график из выпадающего списка. Вы также можете нажать кнопку **Add Week Schedule (Добавить недельный график работы)**, чтобы добавить новый недельный график работы. Подробную информацию см. в разделе 6.6.1 *Недельный график работы*.



5. Выберите группы нерабочих дней, которые нужно использовать в данном шаблоне.
Примечание. Вы можете добавить до четырех групп нерабочих дней.

Index	Holiday Group Name	Remark
1	Holiday Group 1	

Выберите группу нерабочих дней в списке и нажмите кнопку **Add (Добавить)**, чтобы добавить ее в шаблон. Вы также можете нажать кнопку **Add Holiday Group (Добавить группу нерабочих дней)**, чтобы добавить новую группу. Подробную информацию см. в разделе 6.6.2 *Настройки группы нерабочих дней*.

Выберите добавленную группу нерабочих дней в списке, расположенном справа, и нажмите кнопку **Delete (Удалить)**, чтобы ее удалить.

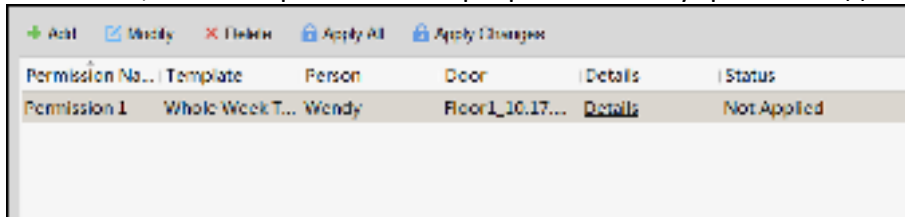
Нажмите кнопку **Clear (Очистить)**, чтобы удалить все добавленные группы нерабочих дней.

6. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

6.7 Настройка разрешений

В модуле настройки разрешений можно добавлять, изменять и удалять разрешения на управление доступом, а затем применять настройки разрешений для конкретного устройства.

Нажмите на значок , чтобы перейти в окно разрешений на управление доступом.



Permission Name	Template	Person	Door	Details	Status
Permission 1	Whole Week Template	Wendy	Floor_10.17...	Details	Not Applied

6.7.1 Добавление разрешений

Назначение:

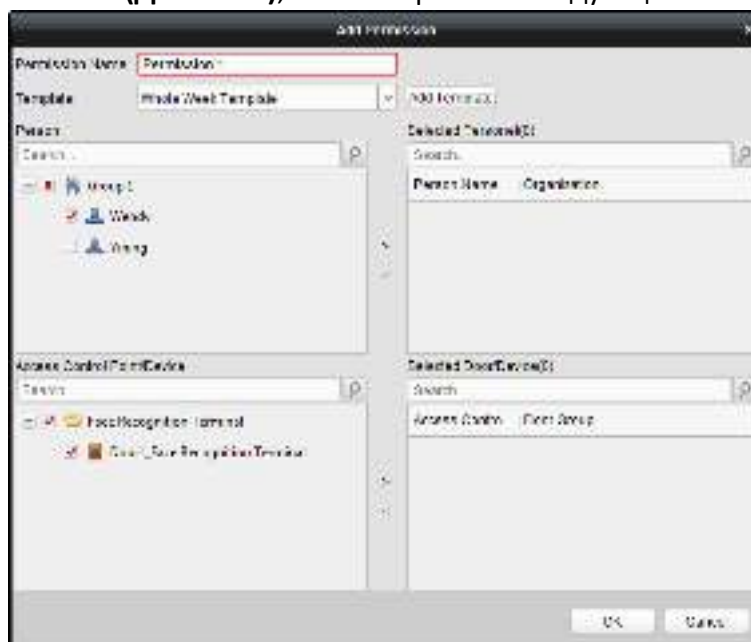
В этом разделе можно назначить разрешение для пользователей, которые позволят им входить или выходить через точки контроля доступа (двери).

Примечания.

- Вы можете добавить до четырех разрешений для одной точки управления доступом на одном устройстве.
- Всего можно добавить 128 разрешений.

Инструкция:

1. Нажмите на значок **Add (Добавить)**, чтобы перейти в следующее окно.



2. Введите желаемое название разрешения в поле **Permission Name (Название разрешения)**.
3. Выберите шаблон разрешения из выпадающего меню.

Примечание. Шаблон нужно будет создать перед настройками разрешений. Нажмите кнопку **Add Template (Добавить шаблон)**, чтобы добавить шаблон. Подробную информацию см. в разделе 6.6 *Графики и шаблоны*.

4. В списке **Person (Пользователи)** отображаются все добавленные пользователи.
Отметьте галочками соответствующих людей и нажмите кнопку **>**, чтобы добавить их в список выбранных пользователей.
(Дополнительная опция) Выберите человека в списке выбранных пользователей и нажмите кнопку **<**, чтобы отменить свой выбор.
5. В списке точек и устройств управления доступом отображаются все точки управления доступом (двери) и вызывные панели.
Отметьте галочками соответствующие двери или вызывные панели и нажмите кнопку **>**, чтобы добавить их в список.
(Дополнительная опция) Выберите дверь или вызывную панель в списке выбранных элементов и нажмите кнопку **<**, чтобы отменить свой выбор.
6. Нажмите кнопку **OK**, чтобы завершить процесс добавления разрешений. Выбранный пользователь получит разрешение на вход или выход из выбранной двери/использование вызывной панели при помощи связанной карты или отпечатка пальца.
7. (Дополнительная опция) После добавления разрешений можно нажать кнопку **Details (Подробная информация)**, чтобы изменить соответствующие данные. Выберите разрешение и нажмите кнопку **Modify (Изменить)**, чтобы отредактировать его параметры. Выберите добавленное разрешение в соответствующем списке и нажмите кнопку **Delete (Удалить)**, чтобы его удалить.

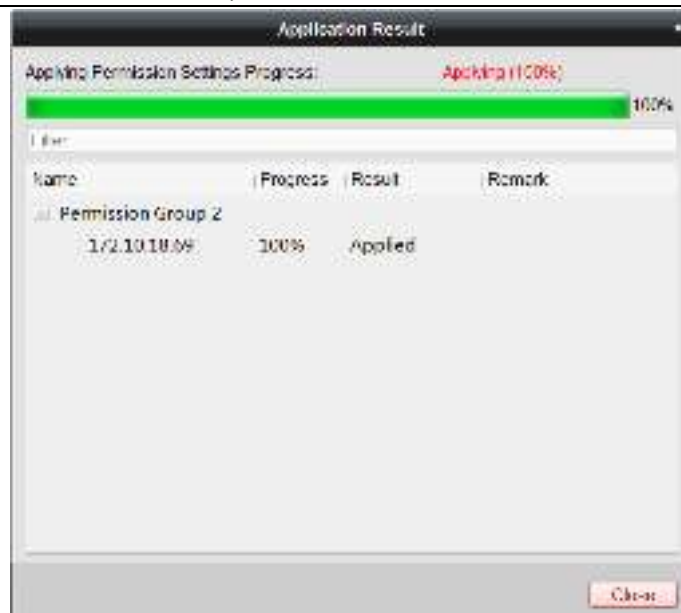
6.7.2 Назначение разрешения

Назначение:

Чтобы активировать разрешение, после выполнения настроек его нужно назначить конкретному устройству.

Инструкция:

1. Выберите разрешение, которое нужно применить к устройству управления доступом.
Чтобы выбрать сразу несколько разрешений, зажмите клавишу **Ctrl** или **Shift** и выберите требуемые пункты.
2. Нажмите кнопку **Apply All (Применить все)**, чтобы начать процесс назначения всех выбранных разрешений для устройства управления доступом или вызывной панели.
Нажмите кнопку **Apply Changes (Применить изменения)**, чтобы применить измененные параметры выбранных разрешений к устройствам.
3. На экране появится показанное ниже окно, в котором будет отображен результат назначения разрешений.

**Примечания.**

- При изменении настроек разрешений на экране появится следующая всплывающая подсказка.



Нажмите кнопку **Apply Now (Назначить сейчас)**, чтобы назначить измененные разрешения устройству.

Или нажмите кнопку **Apply Later (Назначить позже)**, чтобы применить изменения позже в соответствующем окне.

- Изменения разрешений включают в себя изменения графиков и шаблонов, настройки разрешений, настройки прав пользователя и связанных с пользователем параметров (в том числе номер карты, отпечаток пальца, изображение лица, связь между номером карты и отпечатком пальца, пароль для карты, период действия карты и т. д.).

6.8 Расширенные функции

Назначение:

После настройки параметров пользователя, шаблона и разрешения на управление доступом, можно настроить расширенные функции управления доступом (например, параметры контроля доступа, пароль для аутентификации и открытие двери первой картой, защиту от обхода системы безопасности и т. д.).

Примечание. Устройство должно поддерживать возможность использования расширенных функций.

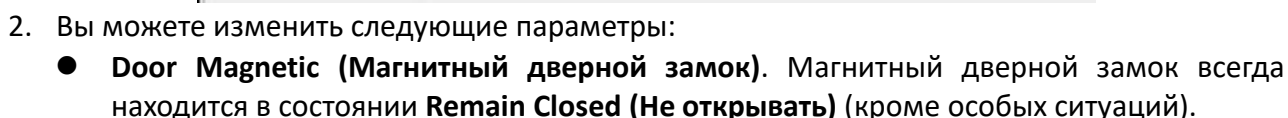
Нажмите на значок , чтобы перейти в следующее окно.



После добавления устройства управления доступом можно настроить параметры точки управления доступом (двери) и параметры, связанные с устройством для считывания карт данного элемента.

Параметры двери

1. Нажмите кнопку в списке контроллеров, расположенном слева, чтобы развернуть на экране информацию об устройстве управления доступом. Затем выберите дверь (точку управления доступом) и измените параметры выбранной двери, представленные в правой части экрана.



- **Exit Button Type (Тип кнопки открытия двери).** Для типа кнопки открытия двери всегда используется значение **Remain Open (Остаться в разомкнутом состоянии)** (кроме особых ситуаций).
- **Door Locked Time (Время блокировки двери).** После считывания обычной карты и срабатывания реле начинает работать таймер блокировки двери.
- **Door Open Duration by Card for Disabled Person (Продолжительность пребывания двери в открытом состоянии при использовании карты, принадлежащей человеку с ограниченными возможностями).** Магнитный дверной замок можно снова включить с соответствующей задержкой времени после того, как своей картой воспользуется человек с ограниченными возможностями.
- **Door Open Timeout Alarm (Сигнал тревоги о превышении заданного времени открытия двери).** Если дверь не будет закрыта, сработает сигнал тревоги.
- **Enable Locking Door when Door Closed (Активации блокировки двери при ее закрытии).** Дверь можно заблокировать в закрытом положении, даже если время для ее блокировки еще не наступило.
- **Duress Code (Код принудительного открытия).** Введите данный код, чтобы открыть дверь под принуждением (если это необходимо). В то же время клиент получит информацию об открытии двери под принуждением.
- **Super Password (Пароль суперпользователя).** Определенный пользователь сможет открывать дверь при помощи пароля суперпользователя.

Примечания.

- Код принудительного открытия и код суперпользователя должны отличаться.
- Код принудительного открытия и пароль суперпользователя должны содержать от четырех до восьми цифр.

3. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить параметры.

Параметры устройства для считывания карт

Инструкция:

1. Нажмите кнопку  в списке устройств, расположенном слева, чтобы развернуть на экране информацию о двери, и выберите название устройства для считывания карт. Затем измените параметры данного устройства, приведенные в правой части экрана.



2. Вы можете изменить следующие параметры:

- **Nickname (Псевдоним).** Измените название устройства для считывания карт.
- **Enable Card Reader (Включение устройства для считывания карт).** Выберите значение **Yes (Да)**, чтобы включить устройство для считывания карт.
- **OK LED Polarity (Правильная полярность светодиода).** Выберите правильную полярность светодиода материнской платы устройства для считывания карт.
- **Error LED Polarity (Ошибочная полярность светодиода).** Выберите ошибочную полярность светодиода материнской платы устройства для считывания карт.
- **Buzzer Polarity (Полярность зуммера).** Выберите полярность светодиода зуммера материнской платы устройства для считывания карт.
- **Minimum Card Swiping Interval (Минимальный интервал считывания карт).** Если интервал считывания одной и той же карты меньше установленного значения, считывание карты будет недействительным. Вы можете задать данное значение в диапазоне 0... 255.
- **Max. Interval When Inputting Password (Максимальный интервал времени при вводе пароля).** Если при вводе пароля в устройство для считывания карт интервал между нажатием двух цифр больше установленного значения, цифры, которые вы нажали до этого, будут автоматически удалены.
- **Enable Failed Attempts Limit of Card Reading (Включение функции ограничения количества неудачных попыток считывания карты).** Вы можете активировать функцию отправки сообщений о срабатывании сигналов тревоги, когда количество попыток считывания карты достигает установленного значения.
- **Max. Times of Card Swiping Failure (Максимальное количество неудачных попыток считывания карты).** Вы можете установить максимальное количество неудачных попыток считывания карты.
- **Enable Tampering Detection (Активация функции выявления несанкционированного доступа).** Вы можете включить функцию обнаружения умышленного нарушения

настроек устройства для считывания карт.

- **Detect When Card Reader is Offline for (Выявление автономной работы устройства для считывания карт).** Если устройство управления доступом не может подключиться к устройству для считывания карт дольше заданного периода времени, устройство для считывания карт автоматически переключится на работу в автономном режиме.
- **Buzzing Time (Время работы зуммера).** Вы можете установить время работы зуммера устройства для считывания карт. Допустимый диапазон составляет 0... 5 999 с. Значение 0 обуславливает постоянную работу зуммера.
- **Card Reader Type (Тип устройства для считывания карт).** Вы можете выбрать тип устройства для считывания карт.
- **Card Reader Description (Описание устройства для считывания карт).** Вы можете ввести описание устройства для считывания карт.
- **Fingerprint Security Level (Уровень безопасности процедуры распознавания отпечатков пальцев).** Выберите уровень распознавания отпечатков пальцев в выпадающем списке.
- **Score (Степень соответствия).** Устройство оценивает снятое изображение в соответствии с углом рыскания, углом наклона и межцентровым расстоянием. Если оценка будет меньше заданного значения, распознавание лица считается неудачным.
- **Face Recognition Timeout Value (Длительность задержки при распознавании лиц).** Если длительность процесса распознавания превысит заданное значение, устройство выдаст соответствующее напоминание.
- **Face Recognition Interval (Интервал распознавания лиц).** Временной интервал между двумя циклами распознавания лиц при непрерывной работе. По умолчанию значение составляет 0.
- **Пороговое значение для сопоставления 1:1.** Установка порога опознавания при распознавании в режиме 1:1. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение составляет 60.
- **Пороговое значение для сопоставления 1:N.** Установка безопасного порога опознавания при распознавании в режиме 1:N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение составляет 60.
- **Live Face Detection (Обнаружение живых лиц).** Включение и выключение функции обнаружения живых лиц. Если активировать эту функцию, устройство будет определять, живое лицо на изображении или нет.
- **Live Face Detection Security Level (Уровень обнаружения живых лиц).** После активации функции **Live Face Detection (Обнаружение живых лица)** можно установить соответствующий уровень живого лица при их распознавании.
- **Application Mode (Режим работы).** Вы можете выбрать режим работы в помещении или любой другой режим, исходя из условий окружающей среды.

6.8.2 Аутентификация при помощи устройства для считывания карт

Назначение:

Вы можете установить правила прохождения через контрольные пункты для устройства считывания карт устройства управления доступом.

Инструкция:

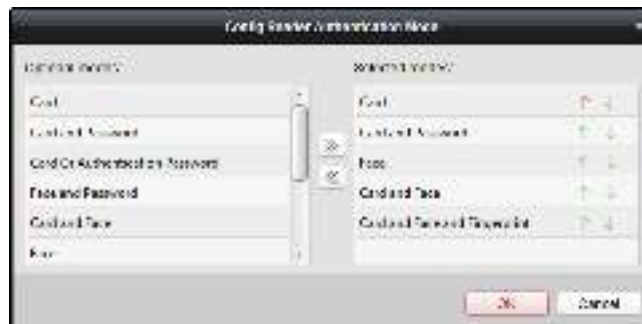
1. Перейдите на вкладку **Card Reader Authentication (Аутентификация при помощи устройства для считывания карт)** и выберите устройство для считывания карт в левой части экрана.
2. Нажмите кнопку **Configuration (Конфигурация)**, чтобы выбрать режимы аутентификации при помощи устройства для считывания карт с целью настройки параметров графика.

Примечания.

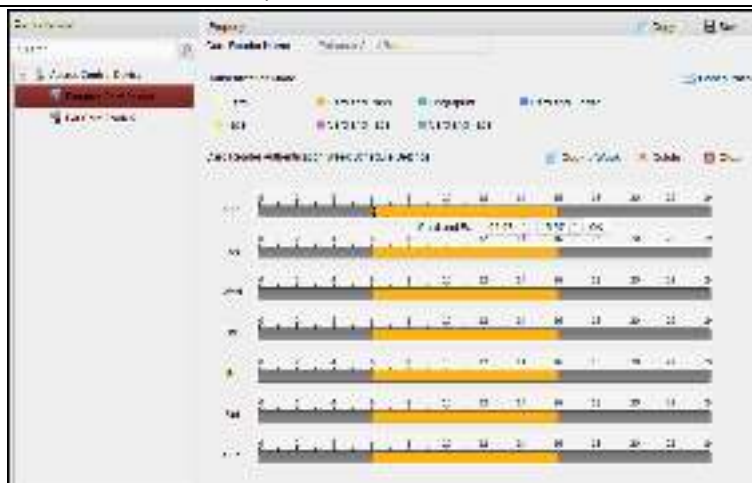
- Доступные режимы аутентификации зависят от типа устройства.
- Пароль — это пароль карты, установленный во время ее выпуска для пользователя. См. раздел 6.5 **Управление пользователями**.

- 1) Выберите режимы и нажмите кнопку , чтобы добавить их в список выбранных режимов.

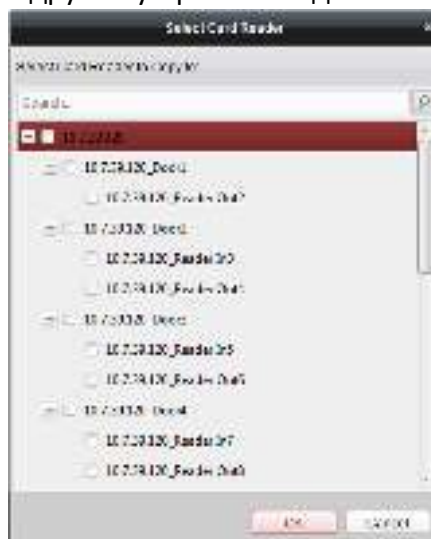
Нажмите кнопку  или , чтобы изменить порядок отображения информации на экране.



- 2) Нажмите кнопку **OK**, чтобы подтвердить свой выбор.
3. После завершения процедуры выбора режимов они будут отображаться на экране в виде значков.
Нажмите на значок, чтобы выбрать режим аутентификации устройства для считывания карт.
4. Нажмите и проведите указателем мыши по определенному дню, чтобы нарисовать цветную полосу в графике. Это значит, что в данный отрезок времени будет использоваться аутентификация при помощи устройства для считывания карт.



5. Повторите этот шаг для установки других отрезков времени.
Или выберите настроенный день и нажмите кнопку **Copy to Week (Копировать для всех дней недели)**, чтобы применить эти настройки ко всем дням недели.
(Дополнительная опция) Нажмите кнопку **Delete (Удалить)**, чтобы удалить выбранный отрезок времени, или кнопку **Clear (Очистить)**, чтобы удалить все созданные отрезки времени.
6. (Дополнительная опция) Нажмите кнопку **Copy to (Копировать в)**, чтобы копировать настройки и применить их к другим устройствам для считывания карт.



7. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить параметры.

6.8.3 Множественная аутентификация

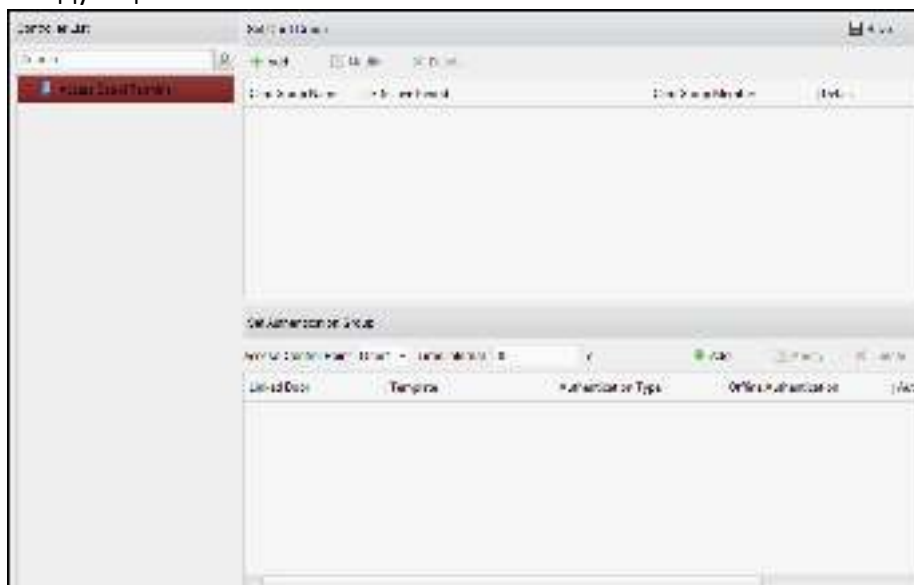
Назначение:

Вы можете управлять группами карт и настраивать аутентификацию сразу нескольких карт для одной точки управления доступом (дверей).

Примечание. Установите разрешение для карты и сначала примените настройки данного разрешения для устройства управления доступом. Подробную информацию см. в *разделе 6.7 Настройка разрешений*.

Инструкция:

1. Выберите вкладку **Multiple Authentication (Множественная аутентификация)**, чтобы перейти в следующее окно.



2. Выберите устройство управления доступом из списка, расположенного слева.
3. На панели **Set Card Group (Создание группы карт)**, расположенной справа, нажмите кнопку **Add (Добавить)**, чтобы открыть на экране следующее диалоговое окно:



- 1) Введите название разрешения в поле **Card Group Name (Название группы карт)**.
 - 2) Нажмите кнопку , чтобы задать период действия группы карт его окончания.
 - 3) Отметьте галочками карты, которые нужно добавить в группу.
 - 4) Нажмите кнопку **OK**, чтобы сохранить группу карт.
4. На панели **Set Card Group (Создание группы карт)** выберите точку управления доступа (дверь) устройства для множественной аутентификации.
 5. Введите временной интервал для считывания карт.
 6. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране следующее диалоговое окно.



- 1) Выберите шаблон группы аутентификации из выпадающего списка. Подробную информацию о создании шаблона см. в разделе 6.6 **Графики и шаблоны**.
- 2) Выберите тип аутентификации группы из выпадающего списка.
 - **Local Authentication (Локальная аутентификация)**. Аутентификация с помощью устройства управления доступом.
 - **Local Authentication and Remotely Open Door (Локальная аутентификация и удаленное открытие двери)**. Аутентификация с помощью устройства управления доступом и посредством клиента.
При выборе типа **Local Authentication and Remotely Open Door (Локальная аутентификация и удаленное открытие двери)** можно установить галочку в соответствующем поле, чтобы активировать функцию аутентификации по паролю суперпользователя, если устройство управления доступом было отключено от клиента.
 - **Local Authentication and Super Password (Локальная аутентификация и пароль суперпользователя)**. Аутентификация с помощью устройства управления доступом и пароля суперпользователя.
- 3) Добавленная группа карт будет отображаться в списке, расположенном слева. Выберите группу карт и нажмите кнопку **+**, чтобы добавить ее в группу аутентификации.
Выберите добавленную группу карт и нажмите кнопку **X**, чтобы убрать ее из группы аутентификации.
Нажимайте кнопку **↑** или **↓**, чтобы установить порядок считывания карт.
- 4) Введите значение параметра **Card Swiping Times (Количество попыток считывания карты)** для выбранной группы карт.

Примечания.

- Количество попыток считывания карты должно быть больше 0 и меньше, чем количество добавленных карт в соответствующей группе.

- Максимальное значение данного параметра равняется 16.

5) Нажмите кнопку **ОК**, чтобы сохранить настройки.

7. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить и применить новые настройки.

Примечания.

- Для каждой точки управления доступом (дверей) можно добавить до 20 групп аутентификации.
- В группу аутентификации с типом сертификата **Local Authentication (Локальная аутентификация)** можно добавить до восьми групп карт.
- В группу аутентификации с типом сертификата **Local Authentication and Super Password (Локальная аутентификация и пароль суперпользователя)** или **Local Authentication and Remotely Open Door (Локальная аутентификация и удаленное открытие двери)** можно добавить до 7 групп карт.

6.8.4 Открытие двери первой картой

Назначение:

Для одной точки управления доступом можно добавить несколько первых карт. Считывание первой карты позволяет нескольким пользователям получить доступ к дверям или выполнить другие действия, связанные с аутентификацией. Доступные режимы использования первой карты: **Remain Open with First Card (Не закрывать первой картой)** и **Disable Remain Open with First Card (Закрывать первой картой)**.

- **Remain Open with First Card (Не закрывать первой картой).** Дверь не будет закрываться в течение указанного периода времени после считывания первой карты.
- **Disable Remain Open with First Card (Закрывать первой картой).** Отключение описанной выше функции.

Примечания.

- Авторизация первой карты действует только в течение текущего дня. Срок действия авторизации истекает через 24 часа с момента считывания карты.
- Чтобы отключить режим использования первой карты, нужно считать ее еще раз.

Инструкция:

1. Перейдите на вкладку **Open Door with First Card (Открытие двери первой картой)**, чтобы открыть на экране следующее окно.



2. Выберите устройство управления доступом из списка, расположенного слева.

3. Выберите режим использования первой карты для устройства управления доступом в выпадающем списке, расположенном слева, и укажите длительность пребывания двери в открытом состоянии.

Примечания.

- Значение этого параметра должно быть в диапазоне 0... 1 440 минут. Значение по умолчанию составляет 10 минут.
 - Чтобы отключить режим использования первой карты, нужно считать ее еще раз.
4. Нажмите кнопку **Add (Добавить)** в списке первых карт, чтобы открыть на экране следующее диалоговое окно.



- 1) Выберите карты, которые нужно добавить в качестве первых карт для выбранной двери.

Примечание. Установите разрешение для карты и сначала примените настройки разрешения для устройства управления доступом. Подробную информацию см. в разделе 6.7 *Настройка разрешений*.

- 2) Нажмите кнопку **OK**, чтобы добавить карту.

5. Нажмите кнопку **Delete (Удалить)**, чтобы удалить карту из списка первых карт.
6. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить и применить новые настройки.

6.8.5 Защита от обхода системы безопасности

Назначение:

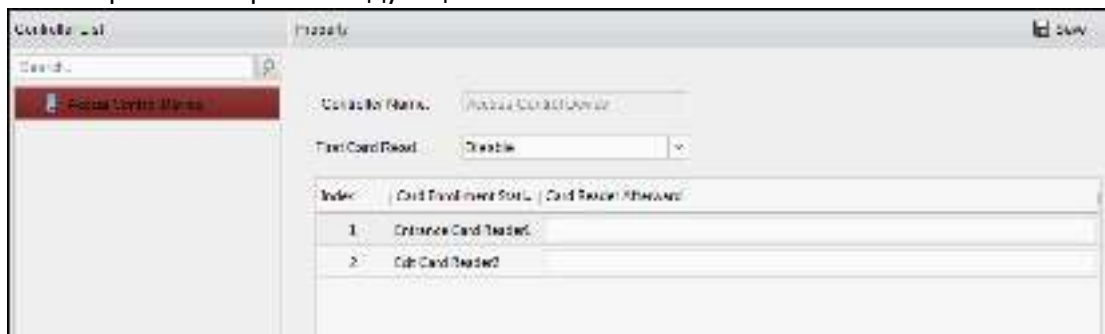
Вы можете настроить параметры прохождения точки управления доступом в соответствии с указанным маршрутом, после чего только один пользователь может пройти точку управления доступом при считывании карты.

Примечания.

- В устройстве управления доступом можно настроить только функцию защиты от обхода системы безопасности или только функцию взаимной блокировки нескольких дверей.
- Сначала нужно включить функцию защиты от обхода системы безопасности в устройстве управления доступом.

Инструкция:

1. Перейдите на вкладку **Anti-passing Back (Защита от обхода системы безопасности)**, чтобы открыть на экране следующее окно.



2. Выберите устройство управления доступом из списка, расположенного слева.
3. В поле **First Card Reader (Первое устройство для считывания карт)** укажите первое устройство для считывания карт на маршруте.
4. В представленном списке перейдите в поле **Card Reader Afterward (Следующее устройство для считывания карт)** и выберите связанные устройства для считывания карт.
Пример. Устройство Reader In_01 выбрано в качестве начального, а устройства Reader In_02 и Reader Out_04 выбраны в качестве связанных устройств для считывания карт. Вы сможете пройти через точку управления доступом, считав карту на устройствах в таком порядке: Reader In_01, Reader In_02 и Reader Out_04.



Примечание. Одному устройству для считывания карт можно назначить не более четырех связанных устройств.

5. (Дополнительная опция) Снова войдите в диалоговое окно **Select Card Reader (Выбор устройства для считывания карт)**, чтобы отредактировать последующие устройства для считывания карт.
6. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить и применить новые настройки.

6.9 Поиск события управления доступом

Назначение:

Вы можете искать события в архивных данных об управлении доступом, в том числе удаленное и локальное событие в клиенте.

Перед началом работы:

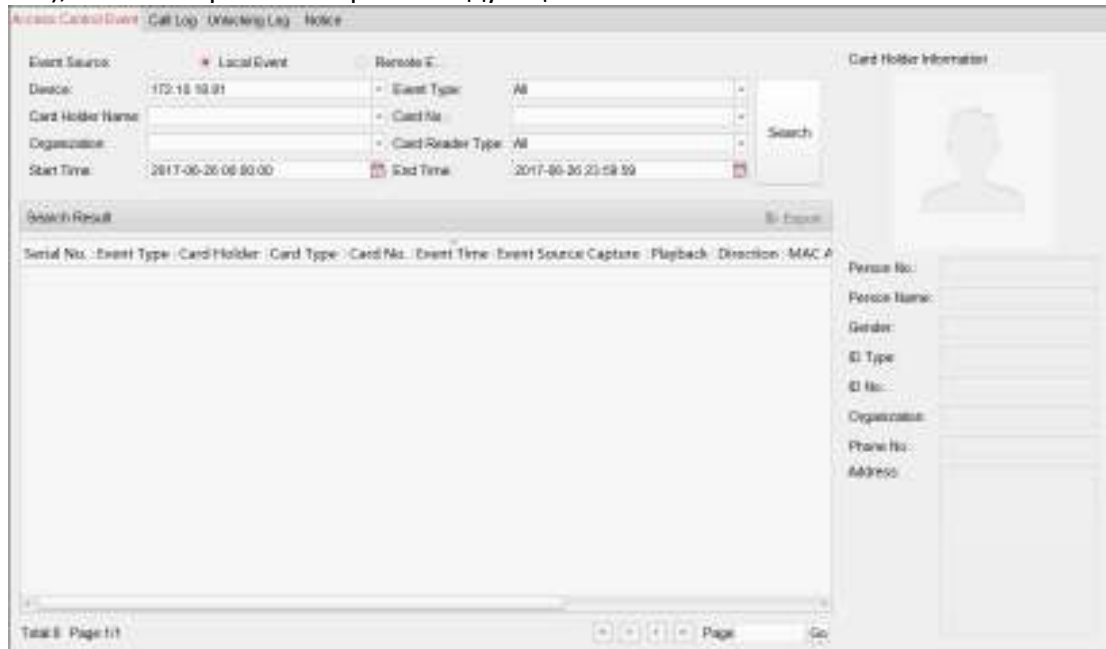
Перед поиском события контроля доступа необходимо указать удаленное хранилище, в котором находятся захваченные изображения лица. Подробную информацию о настройке параметров удаленного хранилища см. в *разделе 5.1 Удаленное хранилище в Руководстве пользователя iVMS-4200*.

Local Event (Локальное событие). Поиск события управления доступом в базе данных клиента управления.

Remote Event (Удаленное событие). Поиск события управления доступом на устройстве.



Нажмите на значок  и перейдите на вкладку Access Control Event (События управления доступом), чтобы открыть на экране следующее окно.



6.9.1 Поиск локального события управления доступом

Инструкция:

1. Выберите в качестве источника события **Local Event (Локальное событие)**.
2. Введите критерии поиска.
3. Нажмите кнопку **Search (Поиск)**. Результаты поиска будут представлены в виде списка, расположенного в нижней части экрана.
4. Нажмите на событие управления доступом, которое было активировано владельцем карты, чтобы просмотреть сведения об этом человеке, в том числе номер пользователя, его имя, организацию, номер телефона, контактный адрес и фотографию.
5. (Дополнительная опция) Если событие содержит связанные изображения, нажмите на столбец **Capture (Захват изображений)**, чтобы просмотреть изображение, захваченное камерой при срабатывании сигнала тревоги.

6. (Дополнительная опция) Если событие содержит связанное видео, нажмите на столбец **Playback (Воспроизведение видеофайла)**, чтобы просмотреть видеоролик, снятый камерой при срабатывании сигнала тревоги.

Примечание. Подробную информацию о настройке работы камеры при срабатывании сигнала тревоги см. в разделе 6.10.1 **Привязка событий управления доступом**.

7. Нажмите кнопку **Export (Экспорт)**, чтобы экспортировать результаты поиска на локальный компьютер в виде файла *.csv.

6.9.2 Поиск удаленного события управления доступом

Инструкция:

1. Выберите в качестве источника события **Remote Event (Удаленное событие)**.
2. Введите критерии поиска.
3. (Дополнительная опция) Поставьте галочку в пункте **With Alarm Picture (С изображением, захваченным при срабатывании сигнала тревоги)**, чтобы найти события с изображениями, захваченными при срабатывании сигнала тревоги.
4. Нажмите кнопку **Search (Поиск)**. Результаты поиска будут представлены в виде списка, расположенного в нижней части экрана.
5. Нажмите кнопку **Export (Экспорт)**, чтобы экспортировать результаты поиска на локальный компьютер в виде файла *.csv.

6.10 Конфигурация событий управления доступом

Назначение:

Вы можете настроить параметры привязки для добавленного устройства управления доступом, в том числе привязку событий управления доступом, входную связь с сигналами входа в систему управления доступом, связь с картами событий и связь между устройствами.



Нажмите на значок , расположенный на панели управления или выберите пункт **Tool (Инструменты) -> Event Management (Управление событиями)**, чтобы перейти на соответствующую страницу.

6.10.1 Привязка событий управления доступом

Назначение:

Вы можете настроить правило, чтобы назначить связанные действия для события управления доступом. Например, при обнаружении события управления доступом появляется звуковое предупреждение или происходят другие связанные действия.

Примечание. Здесь, прод привязкой подразумевается связывание действий программного обеспечения клиента с определенными событиями.

Инструкция:

1. Нажмите кнопку **Access Control Event (События управления доступом)**.

2. Добавленные устройства управления доступом отображаются на соответствующей панели, расположенной в левой части экрана.
Выберите устройство управления доступом, вход сигнала тревоги, точку управления доступом (дверь) или устройство для считывания карт, чтобы настроить привязку событий.
3. Выберите тип события, чтобы настроить привязку.
4. Выберите камеру, которая начинает процесс съемки при срабатывании сигнала тревоги.
Изображение или видео с активированной камеры появится на экране, когда произойдет выбранное событие.
Вы также можете настроить график работы и параметры хранения захваченных изображений или видеофайлов в специальном хранилище, чтобы захватить изображение с активированной камеры при выявлении выбранного события.
5. Поставьте галочки в соответствующих пунктах, чтобы активировать связанные действия.
Подробную информацию см. в *Таблице 14.1. Связанные действия для событий управления доступом*.
6. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.
7. Нажмите кнопку **Copy to (Копировать в)**, чтобы скопировать событие управления доступом для другого устройства управления доступом, входа сигнала тревоги, точки управления доступом или устройства для считывания карт.
Выберите параметры, которые нужно скопировать, целевой элемент и нажмите кнопку **OK** для подтверждения.

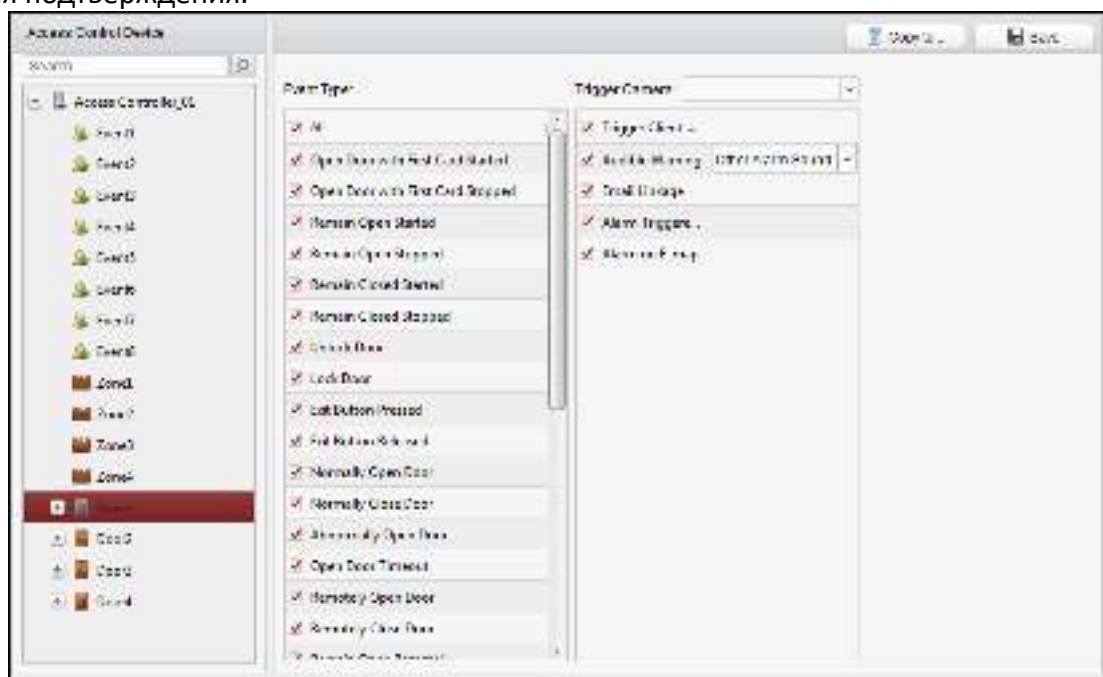


Table 1. 1 Связанные действия для событий управления доступом

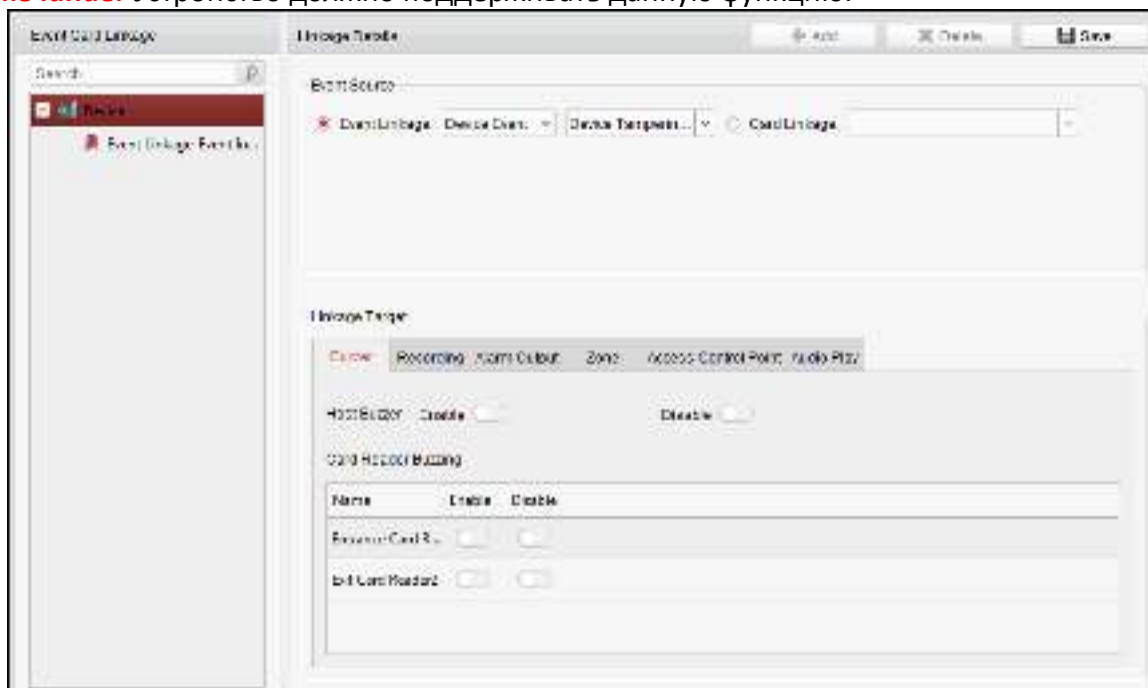
Связанное действие	Описание
Звуковое оповещение	Программное обеспечение клиента генерирует звуковое оповещение при срабатывании сигнала тревоги. Вы можете выбрать звук данного оповещения.
Привязка к электронной почте	Отправка уведомления по электронной почте о срабатывании сигнала тревоги одному или нескольким получателям.

Сигнал тревоги на электронной карте	Отображение информации о сигнале тревоги на электронной карте. Примечание. Эта привязка используется только для точки управления доступом и входа сигнала тревоги.
Всплывающее изображение при срабатывании сигнала тревоги	Изображение с информацией о сигнале тревоги появляется на экране при его срабатывании.

6.10.2 Привязка к событиям карты

Нажмите кнопку **Event Card Linkage (Привязка к событиям карты)**, чтобы перейти в следующее окно.

Примечание. Устройство должно поддерживать данную функцию.



Выберите устройство управления доступом из списка, расположенного слева.

Нажмите кнопку **Add (Добавить)**, чтобы добавить новую привязку. Источником события может служить **Event Linkage (Привязка события)** или **Card Linkage (Привязка карты)**.

Привязка события

События срабатывания сигнала тревоги, используемые для привязки событий, можно разделить на четыре типа: событие устройства, вход сигнала тревоги, событие двери и событие устройства для считывания карт.

Инструкция:

1. Выберите устройство из списка, расположенного слева, и нажмите кнопку **Add (Добавить)**.
2. Выберите тип привязки **Event Linkage (Привязка события)**, после чего укажите тип события из выпадающего списка.
 - Для событий устройства выберите тип события из выпадающего списка.

- Для входа сигнала тревоги выберите тип (сигнал тревоги или его сброс) и укажите название входа сигнала тревоги на соответствующей панели.
- Для событий двери выберите тип события и укажите дверь на соответствующей панели.
- Для событий устройства для считывания карт выберите тип события и укажите устройство на соответствующей панели.

3. Переходите на различные вкладки, чтобы задать требуемые параметры. Чтобы активировать данную функцию, переведите ползунок из положения  в положение .

Вы можете задать параметры зуммера, записи, выхода сигнала тревоги и точки управления доступом.

Тип привязки	Цель привязки	Описание
Зуммер	Зуммер хоста	Запуск звукового оповещения контроллера.
	Зуммер устройства для считывания карт	Запуск звукового оповещения устройства для считывания карт.
Видеозапись	Статус захвата изображений	Запуск захвата изображения в режиме реального времени.
Выход сигнала тревоги	Выход сигнала тревоги	Выход сигнала тревоги будет активирован для отправки уведомлений.
Точка управления доступом	Точка управления доступом	Выбор состояния двери: открыта, закрыта, не закрывать или не открывать. Примечания. ● Состояния двери «открыта», «закрыта», «не закрывать» и «не открывать» нельзя использовать одновременно. ● Целевая дверь и дверь, используемая в качестве источника, не могут являться одной дверью.

4. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить и применить параметры.

Привязка карты

Инструкция:

1. Выберите тип привязки **Card Linkage (Привязка карты)**.
2. Введите номер карты или выберите карту из выпадающего списка.
3. На соответствующей панели выберите устройство для считывания карт, которое нужно активировать.
5. Переходите на различные вкладки, чтобы задать требуемые параметры. Чтобы активировать данную функцию, переведите ползунок из положения  в положение .

Вы можете задать параметры зуммера, записи, выхода сигнала тревоги и точки управления доступом.

Тип привязки	Цель привязки	Описание
--------------	---------------	----------

Терминал распознавания лиц

Руководство пользователя

Зуммер	Зуммер хоста	Запуск звукового оповещения контроллера.
	Зуммер устройства для считывания карт	Запуск звукового оповещения устройства для считывания карт.
Видеозапись	Статус захвата изображений	Запуск захвата изображения в режиме реального времени.
Выход сигнала тревоги	Выход сигнала тревоги	Выход сигнала тревоги будет активирован для отправки уведомлений.
Точка управления доступом	Точка управления доступом	Выбор состояния двери: открыта, закрыта, не закрывать или не открывать. Примечания. ● Состояния двери «открыта», «закрыта», «не закрывать» и «не открывать» нельзя использовать одновременно. ● Целевая дверь и дверь, используемая в качестве источника, не могут являться одной дверью.

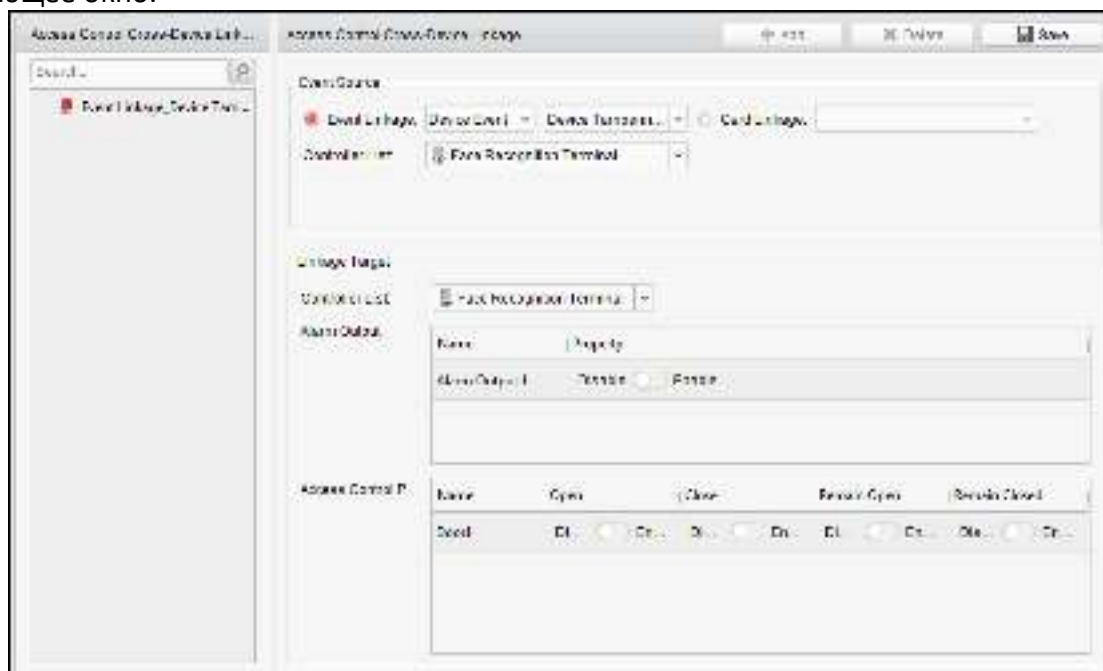
4. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить и применить параметры.

6.10.3 Перекрестная привязка устройств

Назначение:

Вы можете назначить запуск другого действия устройства управления доступом, настроив соответствующее правило при запуске события управления доступом.

Выберите вкладку **Cross-Device Linkage (Перекрестная привязка устройств)**, чтобы перейти в следующее окно.



Нажмите кнопку **Add (Добавить)**, чтобы добавить новую привязку клиента. Источником события может служить **Event Linkage (Привязка события)** или **Card Linkage (Привязка карты)**.

Привязка события

События срабатывания сигнала тревоги, используемые для привязки событий, можно разделить на четыре типа: событие устройства, вход сигнала тревоги, событие двери и событие устройства для считывания карт.

Инструкция:

1. Выберите тип привязки **Event Linkage (Привязка события)**, укажите устройство управления доступом, которое является источником события, а также тип события из выпадающего списка.
 - Для событий устройства выберите тип события из выпадающего списка.
 - Для входа сигнала тревоги выберите тип (срабатывание сигнала тревоги или его сброс) и укажите название входа сигнала тревоги в соответствующей таблице.
 - Для события двери выберите подробный тип события и укажите дверь в соответствующей таблице.
 - Для события устройства для считывания карты выберите тип события и укажите устройство в соответствующей таблице.
2. Выберите цель привязки, укажите устройство управления доступом из списка в нижней части экрана в качестве цели привязки, а также измените положение ползунка с  на , чтобы активировать данную функцию.
 - **Alarm Output (Выход сигнала тревоги)**. Выход сигнала тревоги будет активирован для отправки уведомлений.
 - **Access Control Point (Точка управления доступом)**. Выбор состояния двери: открыта, закрыта, не закрывать или не открывать.

Примечание. Состояния двери «открыта», «закрыта», «не закрывать» и «не открывать» нельзя использовать одновременно.
3. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить параметры.

Привязка карты

Инструкция:

1. Выберите тип привязки **Card Linkage (Привязка карты)**.
2. Выберите карту из выпадающего списка и укажите устройство управления доступом в качестве источника события.
3. Выберите устройство для считывания карт, которое нужно активировать, из соответствующей таблицы.
4. Выберите цель привязки, укажите устройство управления доступом из списка в нижней части экрана в качестве цели привязки, и измените положение ползунка с  на , чтобы активировать данную функцию.

Alarm Output (Выход сигнала тревоги). Выход сигнала тревоги будет активирован для отправки уведомлений.
5. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить параметры.

6.11 Управление состоянием двери

Назначение:

Состояние двери добавленного устройства управления доступом будет отображаться в режиме реального времени. Вы можете проверить состояние и связанные события выбранной двери. Вы можете управлять состоянием двери и устанавливать его продолжительность.

6.11.1 Контроль группы управления доступом

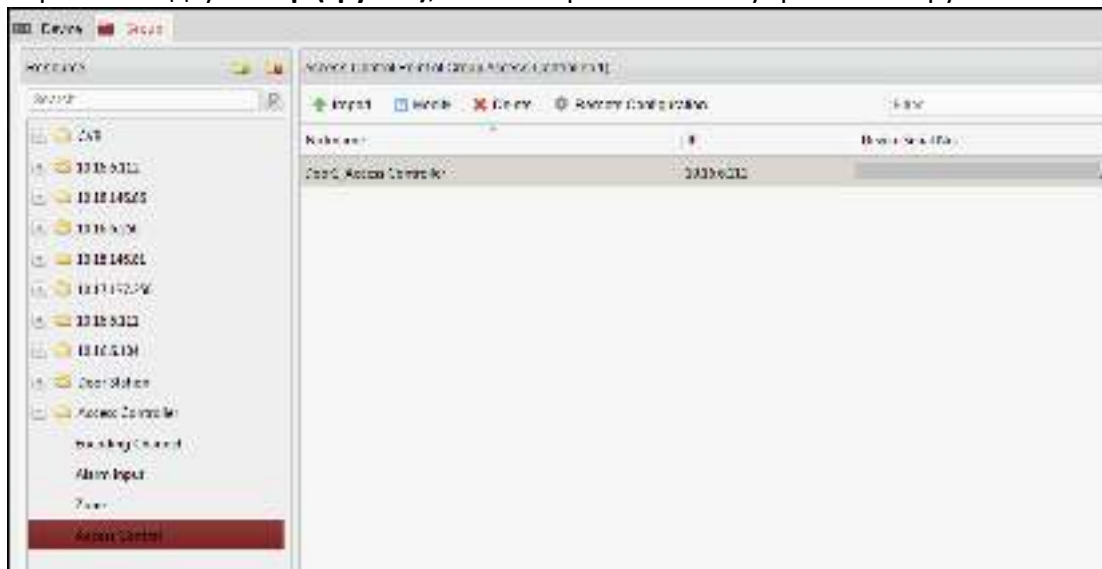
Назначение:

Перед настройкой управления статусом двери и указанием длительности ее состояния нужно создать группу для удобного управления данными параметрами.

Чтобы создать группу для устройства управления доступом, соблюдайте следующие инструкции.

Инструкция:

1. Нажмите кнопку  на панели управления, чтобы открыть страницу управления устройством.
2. Выберите вкладку **Group (Группа)**, чтобы перейти в окно управления группами.



3. Выполните описанные ниже действия, чтобы добавить группу.
 - 1) Нажмите кнопку , чтобы открыть на экране диалоговое окно добавления группы.
 - 2) Введите название группы.
 - 3) Нажмите кнопку **OK**, чтобы добавить новую группу в соответствующий список.Поставьте галочку возле надписи **Create Group by Device Name (Создать группу по названию устройства)**, чтобы создать новую группу, которая будет иметь то же название, что и выбранное устройство.

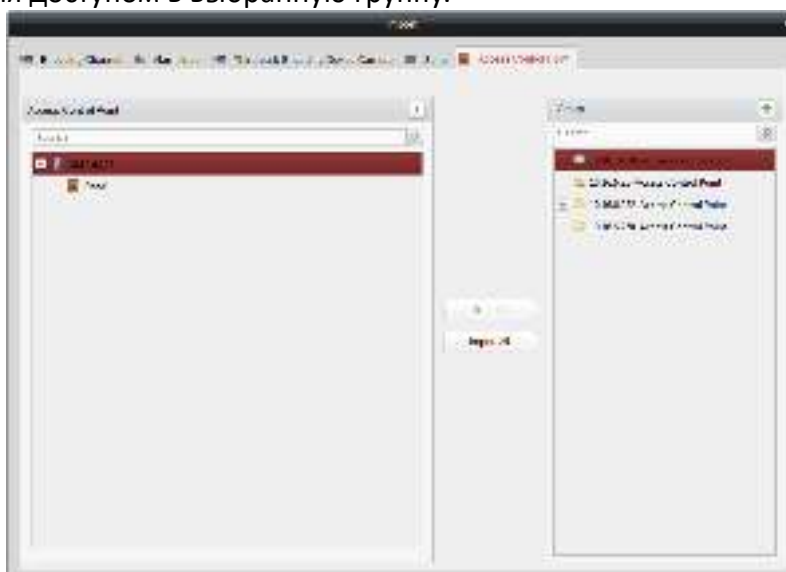


4. Чтобы импортировать точки управления доступом в группу, выполните приведенные ниже действия:

- 1) Нажмите кнопку **Import (Импортировать)** в окне управления группой, а затем перейдите на вкладку **Access Control (Управление доступом)**, чтобы открыть страницу импорта настроек управления доступом.

Примечания.

- Вы также можете импортировать входы сигналов тревоги в группу на вкладке **Alarm Input (Входы сигналов тревоги)**.
 - В группу можно добавить камеры в качестве канала кодирования для видеотерминала управления доступом.
- 2) Выберите названия точек управления доступом из списка.
 - 3) Выберите группу из списка.
 - 4) Нажмите кнопку **Import (Импортировать)**, чтобы импортировать выбранные точки управления доступом в группу.
Нажмите кнопку **Import All (Импортировать все)**, чтобы импортировать все точки управления доступом в выбранную группу.



5. После импорта точек управления доступом в группу нажмите кнопку  или дважды нажмите на названии группы или точки управления доступом, чтобы изменить его.

6.11.2 Блокировка точки управления доступом (двери)

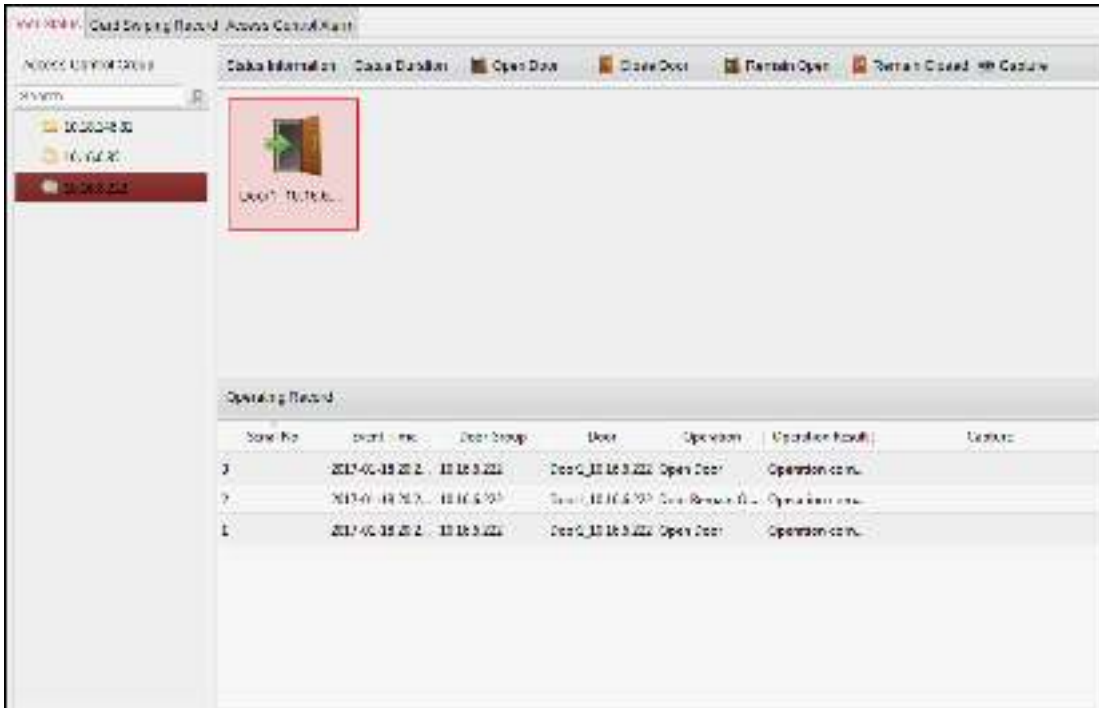
Назначение:

Вы можете управлять состоянием одной точки управления доступом (двери), в том числе

менять его на «открыта», «закрыта», «не закрывать» или «не открывать».



Нажмите на значок , расположенный на панели управления, чтобы перейти в окно отслеживания состояния.



Инструкция:

1. Выберите группу управления доступом в левой части экрана. Подробную информацию о контроле группы управления доступом см. в *разделе 6.11.1 Контроль группы управления доступом*.
2. Точки управления доступом выбранной группы будут отображаться в правой части экрана.



Нажмите на значок , расположенный на панели информации о состоянии, чтобы выбрать дверь.

3. Нажмите одну из кнопок, размещенных на панели **Status Information (Информация о состоянии)**, чтобы управлять статусом двери.

Open Door : нажмите данную кнопку, чтобы открыть дверь один раз.

Close Door : нажмите данную кнопку, чтобы закрыть дверь один раз.

Remain Open : нажмите данную кнопку, чтобы не закрывать дверь.

Remain Closed : нажмите данную кнопку, чтобы не открывать дверь.

Capture : нажмите данную кнопку, чтобы захватить изображение в ручном режиме.

4. Результат выполнения операции, связанной с блокировкой двери, можно просмотреть на панели **Operation Log (Журнал выполнения операций)**.

Примечания.

- Если было выбрано состояние **Remain Open/Remain Closed (Не закрывать/Не открывать)**, дверь будет открыта или закрыта до тех пор, пока не будет выполнена новая команда, связанная с ее блокировкой.
- Кнопка **Capture (Захват изображения)** будет доступна, только если устройство поддерживает данную функцию. Она не может использоваться до тех пор, пока не будет настроен сервер хранения.

- Если дверь находится в состоянии **Remain Closed (Не открывать)**, ее можно будет открыть только при помощи карты суперпользователя через программное обеспечение клиента.

6.11.3 Настройка длительности состояния

Назначение:

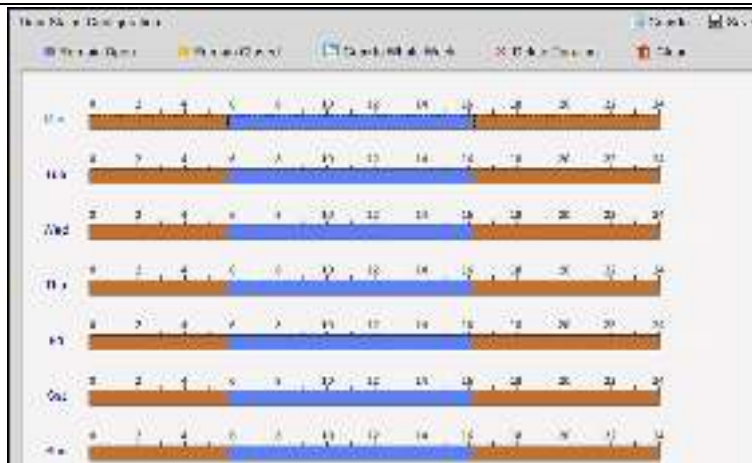
Вы можете планировать еженедельные периоды времени для точки управления доступом (двери), в течение которых она будет оставаться открытой или закрытой.

В модуле состояния двери нажмите кнопку **Status Duration (Длительность состояния)**, чтобы перейти в окно настройки длительности состояния.



Инструкция:

1. Выберите дверь из списка устройств управления доступом, расположенного в левой части экрана.
2. Нарисуйте график для выбранной двери на панели настройки ее состояния, расположенной в правой части экрана.
 - 1) Выберите цвет заливки для состояния двери: Remain Open или Remain Closed.
Remain Open (Не закрывать). Дверь не будет закрываться в течение указанного периода времени. Период помечается цветом .
Remain Closed (Не открывать). Дверь будет закрыта в течение указанного периода времени. Период помечается цветом .
 - 2) Проведите курсором по временной шкале, чтобы нарисовать цветную линию в графике и указать длительность определенного состояния.



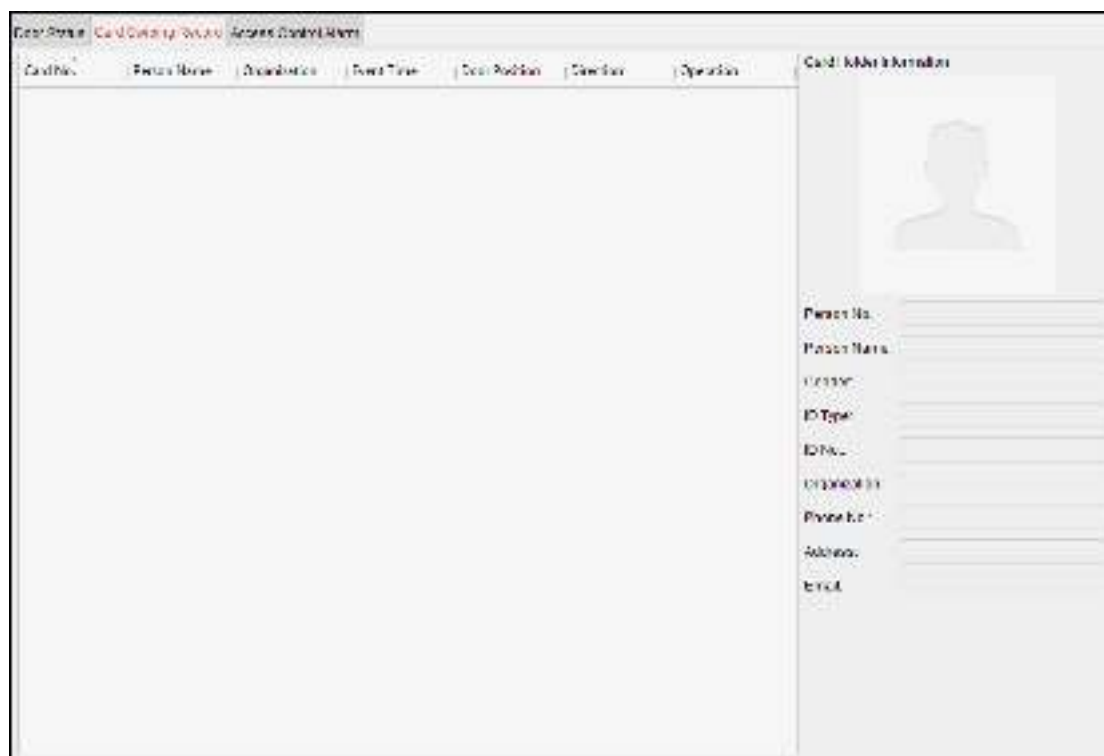
3) Когда вид курсора изменится на , вы сможете переместить выбранный отрезок времени, который только что был изменен. Также можно изменить отображаемую точку времени, чтобы задать точный период.

Когда вид курсора изменится на , вы сможете изменить длительность выбранного отрезка времени.

3. (Дополнительная опция) Выберите отрезок времени в графике и нажмите кнопку **Copy to Whole Week (Копировать для всех дней недели)**, чтобы копировать настройки этого отрезка для других дней недели.
4. Выберите отрезок времени и нажмите кнопку **Delete Duration (Удалить период)**, чтобы удалить выбранный интервал.
Или нажмите кнопку **Clear (Очистить)**, чтобы удалить все созданные периоды времени из графика.
5. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.
6. Нажмите кнопку **Copy to (Копировать в)**, чтобы скопировать график для других дверей.

6.11.4 Запись информации о считывании карт в режиме реального времени

Выберите вкладку **Card Swiping Record (Запись информации о считывании карт)**, чтобы перейти в следующее окно.



Журналы с информацией о считывании карт всех устройств управления доступом будут отображаться в режиме реального времени. Вы можете просматривать подробную информацию о событиях считывания карт, в том числе номер карты, имя пользователя, организацию, время выявления события и т. д.

Нажмите на событие, чтобы просмотреть подробную информацию о владельце карты, в том числе номер пользователя, его имя, организацию, номер телефона, контактный адрес и т. д.

6.11.5 Сигнализация управления доступом в режиме реального времени

Назначение:

Журналы событий управления доступом отображаются в режиме реального времени, в том числе в них приводится информация об исключении устройств, события дверей, устройств считывания карт и входов сигналов тревоги.

Выберите вкладку **Access Control Alarm (Сигнализация управления доступом)**, чтобы перейти в окно настройки параметров.

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

Инструкция:

1. Все сигналы тревоги, связанные с управлением доступом, будут отображаться в виде списка в режиме реального времени.

Вы можете просмотреть тип сигнала тревоги, время и место его появления и т. д.

2. Нажмите кнопку , чтобы отобразить информацию о сигнале тревоги на электронной карте.
3. Нажмите кнопку  или , чтобы просмотреть информацию о сигнале тревоги в режиме реального времени или просмотреть изображение, захваченное камерой при срабатывании сигнализации.

Примечание. Подробную информацию о настройке работы камеры при срабатывании сигнала тревоги см. в разделе 6.10.1 *Привязка событий управления доступом*.

4. Нажмите кнопку **Subscribe (Подписаться)**, чтобы выбрать тип сигнала тревоги, при появлении которого клиент будет получать соответствующие оповещения.



- 1) Поставьте галочки напротив соответствующих типов сигналов тревоги, в том числе напротив сигналов об исключении устройства, событиях двери, устройства считывания карт и входа сигнализации.
- 2) Нажмите кнопку **OK**, чтобы сохранить настройки.

6.12 Просмотр в режиме реального времени

Для выполнения определенных задач в системе видеонаблюдения можно просмотреть видео с добавленного устройства в режиме реального времени. Предусмотрена возможность выполнения некоторых основных операций, включая захват изображений, запись в ручном режиме и т. д.

Перед началом работы:

Необходимо настроить параметры группы камер для наблюдения в режиме реального времени.

Если необходимо, вы можете выбрать тип поворота в разделе **Group Management (Управление группами)**. Подробную информацию см. в *Руководстве пользователя программного обеспечения клиента iVMS-4200*.

6.12.1 Начало и остановка просмотра в режиме реального времени

Запуск просмотра в режиме реального времени

Инструкция:

1. Нажмите на значок  , расположенный на панели управления.
или выберите пункт **View (Просмотр) -> Main View (Основной экран)**, чтобы открыть на экране соответствующую страницу.
2. Перетащите камеру в окно дисплея.
Или дважды щелкните на названии камеры после выбора окна дисплея изображения, чтобы запустить просмотр в режиме реального времени.

Примечание. При необходимости во время просмотра в режиме реального времени можно перетащить видео с камеры в другое окно дисплея.

Остановка просмотра в режиме реального времени

Инструкция:

1. Выберите окно дисплея.
2. Нажмите на значок  , который появляется в правом верхнем углу экрана, когда указатель мыши находится над окном дисплея.
или нажмите кнопку **Stop Live View (Остановить просмотр в режиме реального времени)** в контекстном меню, чтобы остановить просмотр в режиме реального времени в окне дисплея.
Вы также можете нажать кнопку  , расположенную на панели инструментов окна просмотра в режиме реального времени, чтобы остановить все просмотры в режиме реального времени.

6.12.2 Ручная запись и захват изображений

Ручная запись при просмотре в режиме реального времени

Назначение:

Данная функция позволяет вручную записывать видео в режиме реального времени на странице **Main View (Основной экран)**, а также сохранять видеофайлы на локальном

компьютере.

Инструкция:

1. Переместите курсор в окно просмотра в режиме реального времени, чтобы отобразить на экране панель инструментов.
2. Чтобы начать ручную запись, нажмите кнопку , расположенную на панели инструментов окна просмотра или в контекстном меню **Live View Management (Управление просмотром в режиме реального времени)**. Значок  изменится на .
3. Нажмите на значок , чтобы остановить запись в ручном режиме. Если все операции будут выполнены успешно, на экране появится окно с указанием пути сохранения записанных вами видеофайлов.

Примечания.

- Во время записи в ручном режиме в верхнем правом углу окна дисплея будет отображаться индикатор .
- Путь сохранения видеофайлов можно указать в окне настроек параметров системы. Подробную информацию см. в *Руководстве пользователя программного обеспечения клиента iVMS-4200*.

Просмотр локальных видеофайлов**Инструкция:**

1. Выберите пункт **File (Файл) -> Open Video File (Открыть видеофайл)**, чтобы перейти на страницу с видеофайлами.
2. Выберите камеру, которую нужно найти, в списке **Camera Group (Группа камер)**.
3. Нажмите на значок , чтобы указать период поиска.
4. Нажмите кнопку **Search (Поиск)**. На экране отобразятся видеофайлы, записанные в указанном диапазоне времени. Выберите видеофайл и нажмите кнопку **Delete (Удалить)**. Вы можете удалить видеофайл. Выберите видеофайл и нажмите кнопку **Send Email (Отправить электронное письмо)**. Вы можете отправить вместе с выбранным видеофайлом электронное уведомление. Выберите видеофайл и нажмите кнопку **Save as (Сохранить как)**. Вы можете сохранить новую копию видеофайла.

Примечание. Чтобы отправить уведомление по электронной почте, сначала нужно настроить параметры электронной почты.



Дважды нажмите на видеофайле, чтобы его можно было воспроизвести в локальном режиме.



На странице локального воспроизведения расположены такие кнопки:

	CIF/4CIF	Просмотр видео с разрешением cif/4cif.
	Full Screen (Во весь экран)	Отображение страницы локального воспроизведения в полноэкранном режиме.
	Close (Заккрыть)	Закрытие страницы локального воспроизведения видеофайлов.
	Pause/Play (Пауза/возобновление)	Приостановка или возобновление процесса воспроизведения видеофайлов.
	Stop (Остановка)	Остановка воспроизведения видеофайлов.
	Speed (Скорость)	Выбор скорости воспроизведения.
	Single Frame (Покадровое воспроизведение)	Покадровое воспроизведение видеофайлов.
	Digital Zoom (Цифровое увеличение)	Активация функции цифрового масштабирования. Нажмите эту кнопку еще раз, чтобы отключить данную функцию.
	Enable/Disable Audio (Включить/выключить звук)	Нажмите данную кнопку, чтобы включить/выключить звук во время локального воспроизведения.
	Capture (Захват изображений)	Захват изображения в процессе воспроизведения.

Захват изображения в режиме реального времени

Инструкция:

1. Переместите курсор в окно просмотра в режиме реального времени, чтобы отобразить на экране панель инструментов.
2. Нажмите на значок на панели инструментов окна просмотра или в контекстном меню **Live View Management (Управление просмотром в режиме реального времени)**.

На экране появится небольшое окно со снятым изображением, где будет указана информация о процессе выполнения операции.

Примечание. Путь сохранения захваченного изображения можно задать в окне настроек параметров системы. Подробную информацию см. в *Руководстве пользователя программного обеспечения клиента iVMS-4200*.

Просмотр захваченных изображений

Изображения, снятые в режиме реального времени, хранятся на ПК, на котором была запущена программа. При необходимости вы можете просмотреть полученные снимки.

Инструкция:

1. Выберите пункт **File (Файл) -> Open Image File (Открыть файл изображения)**, чтобы перейти на страницу с захваченными изображениями.
2. Выберите камеру, которую нужно найти, в списке **Camera Group (Группа камер)**.
3. Нажмите на значок , чтобы указать период поиска.
4. Нажмите кнопку **Search (Поиск)**. На экране отобразятся снимки, сделанные в указанном диапазоне времени.
5. Дважды нажмите на захваченном изображении, чтобы увеличить его для более удобного просмотра.
Выберите захваченное изображение и нажмите кнопку **Print (Печать)**. Вы можете распечатать выбранный снимок.
Выберите захваченное изображение и нажмите кнопку **Delete (Удалить)**. Вы можете удалить выбранный снимок.
Выберите захваченное изображение и нажмите кнопку **Send Email (Отправить электронное письмо)**. Вы можете отправить вместе с выбранным изображением электронное уведомление.
Выберите захваченное изображение и нажмите кнопку **Save as (Сохранить как)**. Вы можете сохранить новую копию выбранного изображения.

6.12.3 Другие функции, используемые при просмотре в режиме реального времени

Во время просмотра в режиме реального времени предусмотрена возможность реализации некоторых других функций, включая использование двусторонней аудиосвязи, просмотр статуса камеры, синхронизацию и т. д.

Двусторонняя аудиосвязь

Функция двусторонней аудиосвязи обеспечивает возможность голосового общения через камеру. Вы можете получать с камеры не только видео-, но и аудиосигнал в режиме реального времени. Если устройство имеет несколько каналов двусторонней аудиосвязи, вы можете выбрать один из них.

Двусторонний обмен звуковыми сообщениями можно осуществлять только для одной камеры.

Примечание. Устройство Hik-Connect не обеспечивает возможность выбора канала во время использования двусторонней аудиосвязи.

Статус камеры

Статус камеры (состояние записи, состояние передачи сигнала, номер подключения и т. д.) можно определять и отображать на экране. Информация о состоянии устройства обновляется через каждые 10 с.

Синхронизация

Данная функция обеспечивает синхронизацию часов устройства с ПК, на котором работает клиентское программное обеспечение.

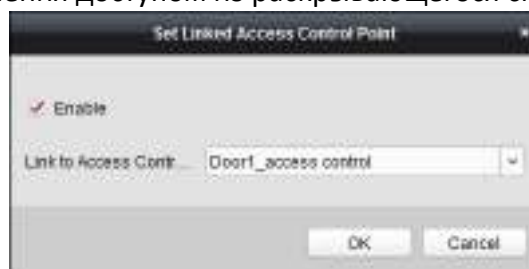
6.12.4 Управление дверью во время просмотра в режиме реального времени

Назначение:

Вы можете управлять дверью во время просмотра видео в режиме реального времени

Инструкция:

1. Нажмите правой кнопкой мыши на окне просмотра в режиме реального времени, чтобы открыть контекстное меню.
2. Нажмите кнопку **Link to Access Control Point (Привязать к точке управления доступом)**, чтобы открыть диалоговое окно установки связи с точкой управления доступом.
3. Поставьте галочку в пункте **Enable (Включить)**, чтобы включить функцию привязки.
4. Выберите точку управления доступом из раскрывающегося списка.



5. Нажмите кнопку **OK**, чтобы сохранить настройки.
6. Нажмите кнопку **Cancel (Отмена)**, чтобы отменить выполнение данной операции.
6. Снова получите поток данных (дважды щелкните по камере), чтобы применить выполненные настройки.

Во время просмотра в режиме реального времени на панели инструментов появятся четыре кнопки для управления дверью.



В следующей таблице приводится описание этих кнопок.

Кнопка	Описание
	Открыть дверь.
	Закрыть дверь.
	Не закрывать.
	Не открывать.

7. Нажмите кнопку / , чтобы открыть или закрыть дверь. Или нажмите кнопку / , чтобы установить статус двери как «не закрывать» или «не открывать».

Примечание. Одну камеру можно связать только с одной точкой управления доступом. С одной и той же точкой управления доступом можно связывать разные камеры.

6.13 Управление постановкой на сигнализацию

Назначение:

Сигнализацию устройства можно включать и выключать. После включения сигнализации на устройстве клиент будет получать информацию о срабатывании соответствующего сигнала тревоги.

Инструкция:

1. Перейдите в пункт **Tool (Инструменты) -> Device Arming Control (Управление постановкой устройства на сигнализацию)**, чтобы отобразить на экране соответствующее окно.
2. Чтобы поставить устройство на сигнализацию, пометьте галочкой соответствующий пункт. После этого информация о срабатывании сигнала тревоги будет автоматически загружаться в программное обеспечение клиента.



6.14 Учет рабочего времени

Назначение:

Модуль учета рабочего времени предоставляет множество возможностей, в том числе управление графиком смен, обработка данных о посещаемости, просмотр статистики посещаемости и другие расширенные функции.

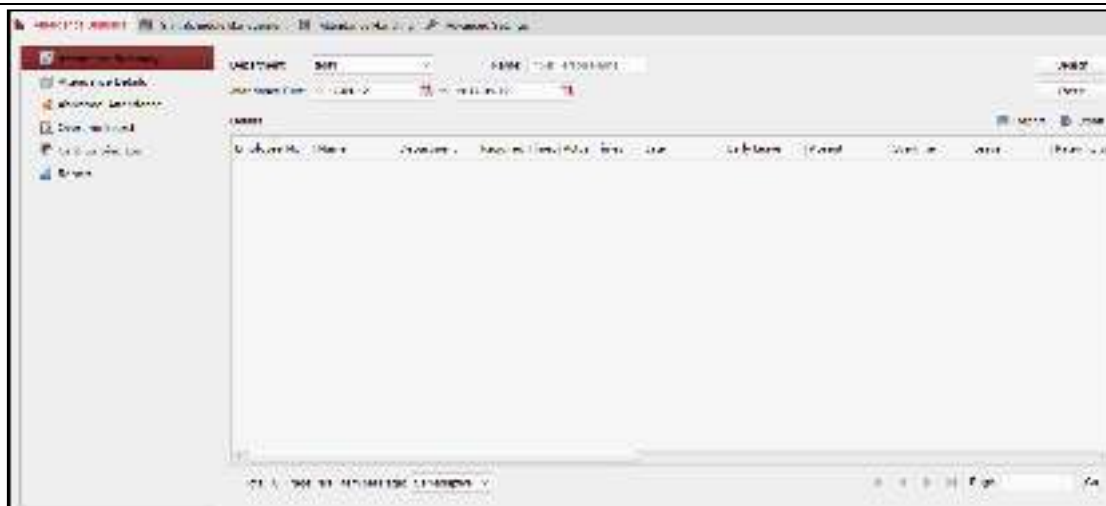
Перед началом работы:

Добавьте организацию и пользователей в модуль управления доступом. Подробную информацию см. в разделе 6.4.1 **Добавление организации** и разделе 6.5.1 **Добавление пользователя**.

Чтобы получить доступ к модулю учета рабочего времени, выполните описанные ниже действия.

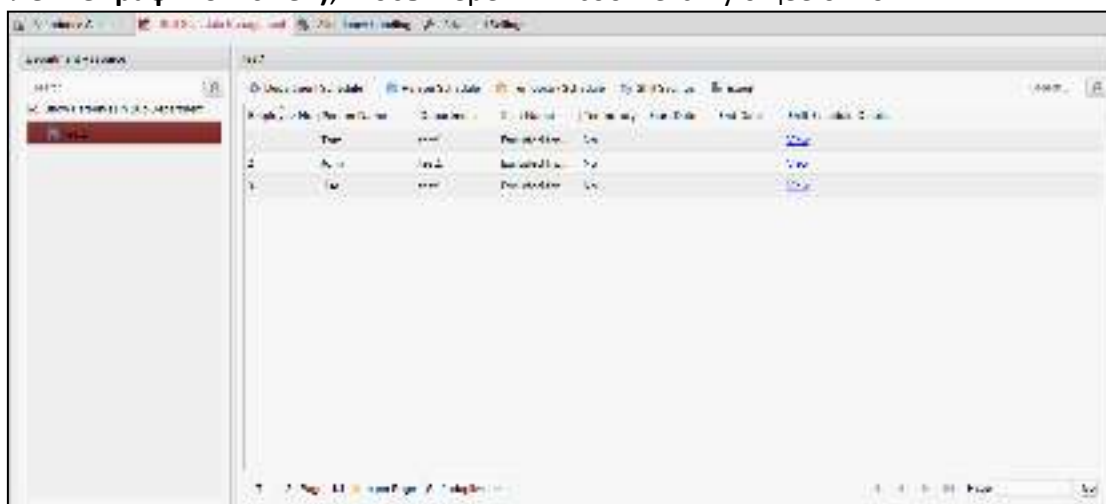


Нажмите кнопку , чтобы перейти в модуль учета рабочего времени:



6.14.1 Управление графиком смен

Откройте модуль учета рабочего времени и нажмите кнопку **Shift Schedule Management (Управление графиком смен)**, чтобы перейти в соответствующее окно.



Настройки смен

Назначение:

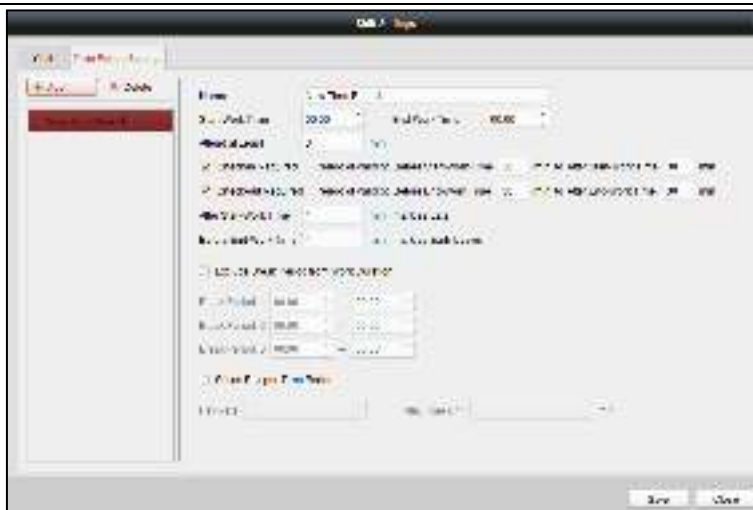
Вы можете добавить период времени и смены в соответствующий график.

Нажмите кнопку **Shift Settings (Настройки смен)**, чтобы открыть на экране диалоговое окно настроек смен.

➤ Добавление периода времени

Инструкция:

1. Перейдите на вкладку **Time Period (Период времени)**.
2. Нажмите кнопку **Add (Добавить)**.



3. Задайте требуемые параметры.

Name (Название). Название периода времени.

Start-Work / End-Work Time (Время начала и окончания работы). Время начала и время окончания рабочей смены.

Attend at Least (Минимальное время присутствия). Минимальное время присутствия на рабочем месте.

Check-in / Check-out Required (Требования к регистрации прибытия или ухода). Здесь можно поставить соответствующие галочки и задать допустимый период времени для регистрации прибытия или ухода.

Mark as Late/Mark as Early Leave (Отметки о позднем или раннем уходе с работы). Период времени для позднего или раннего ухода с работы.

Exclude Break Period from Work Duration (Исключение перерыва из учета рабочего времени). Здесь можно поставить соответствующую галочку и задать период времени, который не должен учитываться при расчете.

Примечание. Вы можете настроить до трех перерывов.

Set as Pay-per-Time Period (Выбор периода повременной оплаты). Здесь можно поставить соответствующую галочку и указать ставку и минимальную единицу времени.

4. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

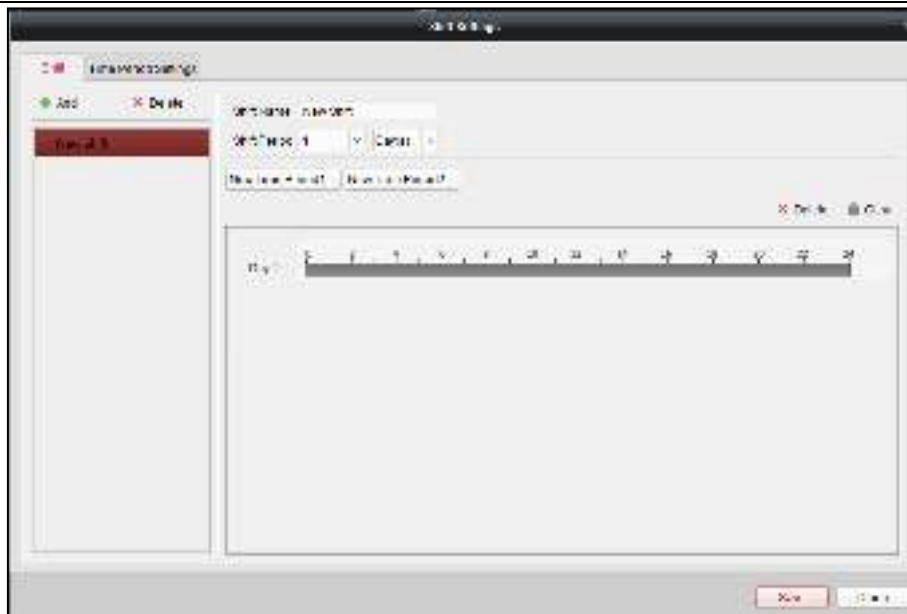
Добавленный период времени будет отображаться на левой панели диалогового окна.

Нажмите кнопку **Delete (Удалить)**, чтобы удалить период времени.

➤ **Добавление смены**

Инструкция:

1. Откройте вкладку **Shift (Смена)**.
2. Нажмите кнопку **Add (Добавить)**.



3. Введите название смены.
4. Выберите период времени для смены из выпадающего списка.
5. Укажите продолжительность смены, используя созданный период времени.
 - 1) Выберите период времени.
 - 2) Нажмите на шкалу времени, чтобы применить данный период к выбранному дню.Нажмите на период времени на шкале и нажмите кнопку  или **Delete (Удалить)**, чтобы его удалить.
Нажмите кнопку **Clear (Очистить)**, чтобы удалить все периоды времени для данного дня.
6. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.
Добавленная смена будет отображаться на левой панели диалогового окна.
Нажмите кнопку **Delete (Удалить)** на левой панели, чтобы удалить смену.

Настройки графика смен

Назначение:

После создания смены вы можете задать график работы отдела, график работы пользователя и временный график работы.

Примечание. Временный график работы имеет более высокий приоритет, чем график работы отдела и график работы пользователя.

➤ График работы отдела

Вы можете установить график смен для конкретного отдела. Он будет применен ко всем пользователям из этого отдела.

Примечание. Список отделов в модуле учета рабочего времени соответствует списку **organization (организаций)** в разделе управления доступом. Подробную информацию о настройке параметров организации на вкладке управления доступом см. в *разделе 6.4 Управление организациями*.

Инструкция:

1. Откройте окно управления графиком смен и выберите отдел на левой панели.
2. Нажмите кнопку **Department Schedule (График работы отдела)**, чтобы открыть на экране соответствующее диалоговое окно.



3. Поставьте галочку в пункте **Time and Attendance (Учет рабочего времени)**.

График работы будет применен ко всем пользователям в этом отделе, кроме тех людей, которые исключены из учета посещаемости.

4. Выберите смену из выпадающего списка.

5. Укажите дату ее начала и дату окончания.

6. (Дополнительная опция) Задайте другие параметры графика работы.

Доступные параметры: **Check-in Not Required (Регистрация прибытия не требуется)**, **Check-out Not Required (Регистрация ухода не требуется)**, **Effective for Holiday (Действует по нерабочим дням)**, **Effective for Overtime (Действует для сверхурочного времени)**, **Effective for Multiple Shift Schedules (Действует для графиков нескольких смен)**.

Примечания.

- Графики для нескольких смен содержат более одного периода времени.

Пользователь может регистрировать время прибытия и ухода в любой из периодов времени, и рабочее время при этом будет учитываться.

Пример. График для нескольких смен содержит три периода времени: с 00:00 до 07:00, с 08:00 до 15:00 и с 16:00 до 23:00. Рабочее время человека, который работает в любую из этих смен, будет учитываться при расчете. Если пользователь регистрирует прибытие в 07:50, оно будет отнесено к ближайшему периоду времени — с 08:00 до 15:00.

- Поставив галочку в пункте **Effective for Multiple Shift Schedules (Действует для графиков нескольких смен)**, можно выбрать из соответствующего списка используемый период времени для пользователей данного отдела.



- 1) В списке, расположенном слева, нажмите на добавленный период времени, а затем нажмите кнопку , чтобы добавить его в правый список.
- 2) (Дополнительная опция) Чтобы удалить выбранный период времени, нажмите кнопку .

7. (Дополнительная опция) Поставьте галочку в пункте **Set as Default for All Persons in Department (Установить в качестве графика работы по умолчанию для всех пользователей в отделе)**.

Все сотрудники отдела будут пользоваться графиком смен, установленным по умолчанию.

8. (Дополнительная опция) Если выбранный отдел содержит подотделы, в окне появится пункт **Shift Schedule for All Sub Departments (График смен для всех подотделов)**. Вы можете поставить галочку в этом пункте, чтобы применить график отдела ко всем его подотделам.
9. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

➤ График работы пользователя

Инструкция:

1. Откройте окно управления графиком смен и выберите отдел на левой панели.
2. Выберите пользователя на панели, расположенной справа.
3. Нажмите кнопку **Person Schedule (График работы пользователя)**, чтобы открыть на экране соответствующее диалоговое окно.

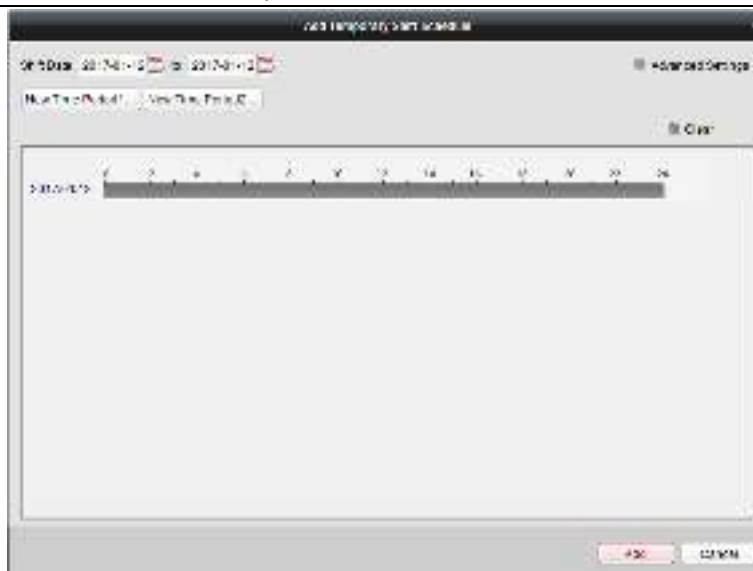


4. Поставьте галочку в пункте **Time and Attendance (Учет рабочего времени)**. График работы будет применен к данному пользователю.
5. Выберите смену из выпадающего списка.
6. Укажите дату ее начала и дату окончания.
7. (Дополнительная опция) Задайте другие параметры графика работы.
Доступные параметры: **Check-in Not Required (Регистрация прибытия не требуется)**, **Check-out Not Required (Регистрация ухода не требуется)**, **Effective for Holiday (Действует по нерабочим дням)**, **Effective for Overtime (Действует для сверхурочного времени)**, **Effective for Multiple Shift Schedules (Действует для графиков нескольких смен)**.
8. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

➤ Временный график работы

Инструкция:

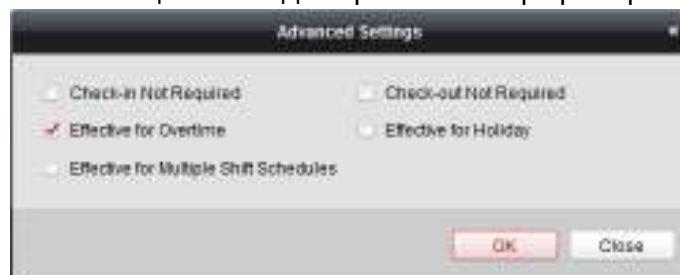
1. Откройте окно управления графиком смен и выберите отдел на левой панели.
2. Выберите пользователя на панели, расположенной справа.
3. Нажмите кнопку **Temporary Schedule (Временный график работы)**, чтобы открыть на экране соответствующее диалоговое окно.



4. Нажмите кнопку , чтобы выбрать дату для смены.
5. Укажите дату для смены, используя созданный ранее период времени.
 - 1) Выберите период времени.
 - 2) Нажмите на шкалу времени, чтобы применить период времени к выбранной дате.

Нажмите на период времени на шкале и нажмите кнопку , чтобы удалить его.

Нажмите кнопку **Clear (Очистить)**, чтобы удалить все периоды времени для данного дня.
6. Нажмите кнопку **Advanced Settings (Расширенные настройки)**, чтобы задать расширенные правила посещаемости для временного графика работы.



7. Нажмите кнопку **Add (Добавить)**, чтобы сохранить настройки.

➤ Проверка информации о графике смен

Инструкция:

1. Выберите отдел на левой панели окна управления графиком смен.
 2. Выберите пользователя на панели, расположенной справа.
 3. Нажмите кнопку **View (Показать)**, чтобы открыть на экране диалоговое окно с подробной информацией о графике смен.
- В нем вы можете просмотреть подробную информацию о графике смен.



4. Перейдите на вкладку **Normal Schedule (Обычная смена)**.

Здесь вы можете просмотреть и изменить подробную информацию об обычной смене.

- 1) Выберите смену из выпадающего списка.
- 2) Нажмите кнопку **Attendance Rule Settings (Настройки правил посещения)**, чтобы открыть на экране соответствующее диалоговое окно.



Вы можете просмотреть правила посещаемости и нажать кнопку **ОК**, чтобы сохранить настройки.

- 3) Нажмите кнопку , чтобы указать дату вступления правил в силу.
- 4) Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.
5. (Дополнительная опция) Перейдите на вкладку **Temporary Schedule (Временный график работы)**.



Здесь вы можете просмотреть и изменить подробную информацию о временном графике работы.

(Дополнительная опция) Нажмите кнопку **Add (Добавить)**, чтобы добавить временный график работы для выбранного пользователя.

(Дополнительная опция) Нажмите кнопку , чтобы изменить период времени.

(Дополнительная опция) Нажмите кнопку , чтобы удалить временный график работы.

➤ Экспорт информации о графике смен

В окне управления графиком смен выберите отдел на панели, расположенной слева, и нажмите кнопку **Export (Экспортировать)**, чтобы экспортировать информацию о графике смен всех пользователей на локальный компьютер.

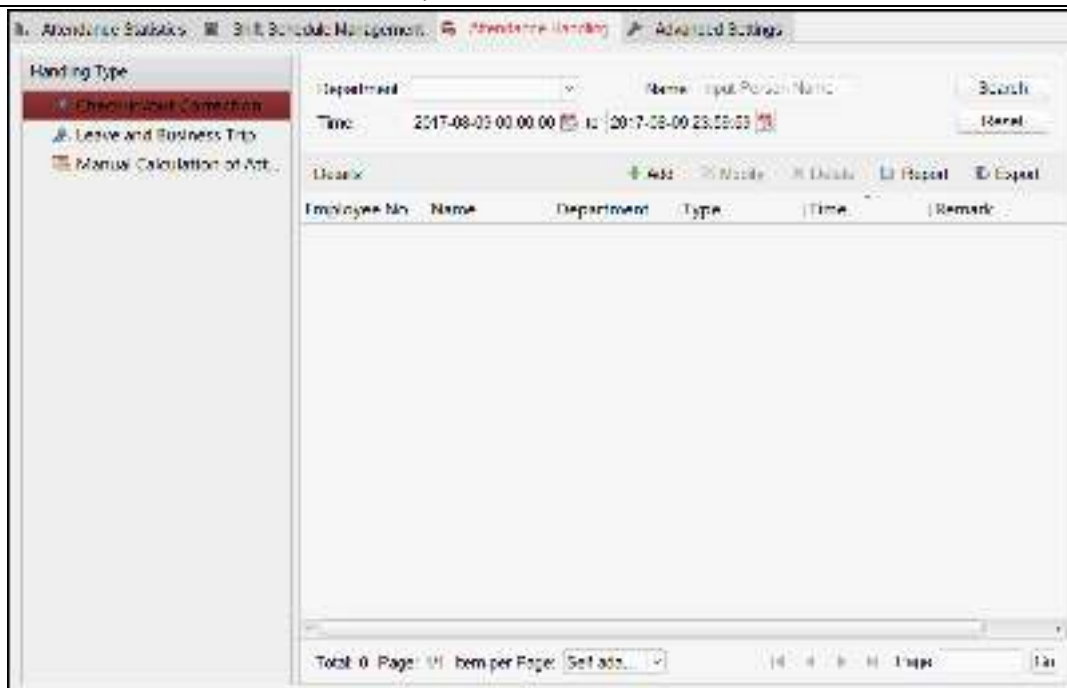
Примечание. Экспортированная информация сохраняется в формате *.csv.

6.14.2 Обработка данных о посещаемости

Назначение:

Можно обрабатывать данные о посещаемости, в том числе регистрацию времени прибытия на работу, времени ухода с работы, отпуск и командировки, а также данные ручного расчета посещаемости.

Откройте модуль учета рабочего времени и нажмите кнопку **Attendance Handling (Обработка данных о посещаемости)**, чтобы перейти в соответствующее окно.



Коррекция регистрации времени прибытия/ухода

Назначение:

Вы можете добавлять, изменять, удалять и искать варианты коррекции регистрации времени прибытия/ухода с работы и генерировать соответствующие отчеты. Информацию о коррекции можно также экспортировать на локальный компьютер.

➤ Добавление варианта коррекции регистрации времени прибытия/ухода

Инструкция:

1. Перейдите на вкладку **Check-in/out Correction (Коррекция регистрации времени прибытия/ухода)**.
2. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране соответствующее диалоговое окно.



3. Задайте параметры коррекции регистрации времени прибытия/ухода с работы.
For Check-in Correction (Для коррекции регистрации времени прибытия). Поставьте галочку в пункте **Check-in (Регистрация времени прибытия)** и укажите актуальное время начало работы.
For Check-out Correction (Для коррекции регистрации времени ухода). Поставьте галочку в пункте **Check-out (Регистрация времени ухода)** и укажите актуальное время окончания работы.

4. Перейдите в поле **Employee Name (Имя сотрудника)** и выберите пользователя.
Вы также можете ввести ключевое слово и нажать кнопку , чтобы найти нужного пользователя.
5. (Дополнительная опция) Введите примечание.
6. Нажмите кнопку **Add (Добавить)**, чтобы добавить вариант коррекции регистрации времени прибытия/ухода с работа.
Добавленный вариант коррекции регистрации времени прибытия/ухода с работы будет отображаться в окне обработки данных о посещаемости.
(Дополнительная опция) Выберите требуемый вариант коррекции регистрации времени прибытия/ухода с работы и нажмите кнопку **Modify (Изменить)**, чтобы его откорректировать.
(Дополнительная опция) Выберите требуемый вариант коррекции регистрации времени прибытия/ухода с работы и нажмите кнопку **Delete (Удалить)**, чтобы его удалить.
(Дополнительная опция) Нажмите кнопку **Report (Отчет)**, чтобы создать отчет о коррекции регистрации времени прибытия/ухода с работы.
(Дополнительная опция) Нажмите кнопку **Export (Экспортировать)**, чтобы экспортировать информацию о коррекции времени прибытия/ухода с работы на локальный компьютер.
Примечание. Экспортированная информация сохраняется в формате *.csv.

➤ **Поиск варианта коррекции регистрации времени прибытия/ухода**

Инструкция:

1. Перейдите на вкладку **Check-in/out Correction (Коррекция регистрации времени прибытия/ухода)**.
2. Задайте требуемые критерии поиска.
Department (Отдел). Выберите отдел из выпадающего списка.
Name (Название). Введите имя пользователя.
Time (Время). Нажмите кнопку , чтобы установить требуемый период времени в качестве диапазона.
3. Нажмите кнопку **Search (Поиск)**, чтобы найти требуемый вариант коррекции регистрации времени прибытия/ухода с работы.
Информация о коррекции регистрации времени прибытия/ухода будет отображаться в виде списка.
Нажмите кнопку **Reset (Сбросить)**, чтобы сбросить критерии поиска.



The screenshot shows a web application interface for managing check-in/out corrections. At the top, there are search filters: a dropdown for 'Department' (set to 'Department 1'), a text input for 'Name' (containing 'Wendy'), and a date range selector for 'Time' (from '2017-01-18 00:00:00' to '2017-01-18 23:59:59'). There are 'Search' and 'Reset' buttons. Below the filters is a toolbar with icons for 'Add', 'Modify', 'Delete', 'Report', and 'Export'. The main area contains a table with the following data:

Employee No	Name	Department	Type	Time	Remark
1	Wendy	Department 1	Check-out	2017-01-18 23:59:59	
1	Wendy	Department 1	Check-in	2017-01-18 00:00:00	

Отпуск и командировки

Назначение:

Вы можете добавлять, изменять, удалять и искать отпуска и командировки, а также генерировать соответствующие отчеты. Также можно экспортировать информацию об отпусках и командировках на локальный компьютер.

➤ Добавление отпуска и командировки

Инструкция:

1. Перейдите на вкладку **Leave and Business Trip (Отпуск и командировка)**.
2. Нажмите кнопку **Add (Добавить)**, чтобы открыть на экране соответствующее диалоговое окно.



3. Выберите тип отпуска и командировки из выпадающего списка.
Тип отпуска можно настроить в расширенных настройках. Подробную информацию см. в разделе 0 *Настройки типа отпуска*.
4. Нажмите кнопку , чтобы установить требуемый период времени в качестве диапазона.
5. Перейдите в поле **Employee Name (Имя сотрудника)** и выберите требуемого пользователя.
Вы также можете ввести ключевое слово и нажать кнопку , чтобы найти нужного пользователя.
6. (Дополнительная опция) Введите примечание.
7. Нажмите кнопку **Add (Добавить)**, чтобы добавить отпуск и командировку.
Добавленные отпуска и командировки будут отображаться в окне обработки данных о посещаемости.
(Дополнительная опция) Выберите отпуск и командировку и нажмите кнопку **Modify (Изменить)**, чтобы их откорректировать.
(Дополнительная опция) Выберите отпуск и командировку и нажмите кнопку **Delete (Удалить)**, чтобы их удалить.
(Дополнительная опция) Нажмите кнопку **Report (Отчет)**, чтобы создать отчет об отпуске или командировке.
(Дополнительная опция) Нажмите кнопку **Export (Экспортировать)**, чтобы экспортировать информацию об отпусках и командировках на локальный компьютер.

Примечание. Экспортированная информация сохраняется в формате *.csv.

➤ Поиск отпусков и командировок

Инструкция:

1. Перейдите на вкладку **Leave and Business Trip (Отпуск и командировка)**.
2. Задайте требуемые критерии поиска.
Department (Отдел). Выберите отдел из выпадающего списка.
Name (Название). Введите имя пользователя.
Time (Время). Нажмите кнопку , чтобы установить требуемый период времени в качестве диапазона.
3. Нажмите кнопку **Search (Поиск)**, чтобы найти отпуска и командировки.
Информация об отпусках и командировках будет отображаться на экране в виде списка.

Нажмите кнопку **Reset (Сбросить)**, чтобы сбросить критерии поиска.

The screenshot shows a web interface for searching attendance records. At the top, there are input fields for 'Department' (set to 'Department 1') and 'Name' (set to 'Intel Person Name'). Below these are date pickers for 'Time' (2017-01-10 00:00:00) and 'to' (2017-01-10 23:59:59). A 'Search' button is on the right. Below the search fields is a 'Details' section with a table of results. The table has columns: Employee No, Name, Department, Type, Reason, Start Time, End Time, and Item. Two rows are visible, both for 'Wendy' in 'Department 1'. The first row is for 'Leave' with reason 'Paternity Leave' and dates 2017-01-08 00:00:00 to 2017-01-10 23:59:59. The second row is for 'Day Off in Lieu' with reason 'Overtime Exchange Holiday' and the same dates. Above the table are buttons for 'Add', 'Modify', 'Delete', 'Report', and 'Export'.

Расчет рабочего времени в ручном режиме

Назначение:

Вы можете рассчитать рабочее время вручную, указав время начала и окончания работы.

Инструкция:

1. Перейдите на вкладку **Manual Calculation of Attendance (Расчет рабочего времени в ручном режиме)**.
2. Укажите время начала и время окончания, используемые для расчета.
3. Нажмите кнопку **Calculate (Рассчитать)**, чтобы начать данную процедуру.

Примечание. С помощью этой функции можно рассчитать рабочее время только в пределах трех месяцев.

6.14.3 Расширенные настройки

Назначение:

Вы можете настроить основные параметры, правило посещаемости, контрольную точку посещаемости, параметры нерабочих дней и тип отпуска.

Откройте модуль учета рабочего времени и нажмите кнопку **Advanced Settings (Расширенные настройки)**, чтобы перейти в соответствующее окно.

The screenshot shows the 'Advanced Settings' window. On the left is a sidebar with a tree view containing 'Attendance Management' and its sub-items: 'Attendance Rule Settings', 'Attendance Check Point Settings', 'Holiday Settings', and 'Leave Type Settings'. The main area is titled 'Basic Settings' and contains several configuration options: 'Start Day of Each Week' (set to 'Monday'), 'End Day of Each Week' (set to '1'), 'Non-Work Day Settings' (with radio buttons for 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', 'Saturday', and 'Sunday', where 'Saturday' and 'Sunday' are selected), 'Section-Work Day's Control Report' (set to 'None'), and 'Section-Work Day's Mark in Report' (set to '0'). A 'Save' button is at the bottom right.

Основные настройки

Инструкция:

1. Выберите вкладку **Basic Settings (Основные настройки)**, чтобы перейти в соответствующее окно.

2. Задайте основные настройки.

Start Day of Each Week (Начальный день недели). Здесь можно выбрать один день в качестве начального дня недели.

Start Date of Each Month (Начальный день месяца). Здесь можно выбрать один день в качестве начальной даты месяца.

3. Укажите нерабочие дни.

Set as Non-Work Day (Выбрать нерабочий день). Поставьте галочки напротив дней, которые нужно отменить как нерабочие.

Set Non-Work Day's Color in Report (Выбор цвета для нерабочих дней в отчете). Перейдите в поле цвета и выберите цвет, которым нужно отметить нерабочие дни в отчете.

Set Non-Work Day's Mark in Report (Выбор метки для нерабочих дней в отчете). Укажите метку, которой будут отмечаться нерабочие дни в отчете.

4. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Настройки правила посещаемости

Инструкция:

1. Выберите вкладку **Attendance Rule Settings (Настройки правила посещаемости)**, чтобы перейти в соответствующее окно.

2. Настройте параметры присутствия или отсутствия на работе.

Если сотрудник не отметит начало работы, можно использовать для него отметку **Absent (Отсутствует)** или **Late (Опоздал)** и указать время опоздания.

Если сотрудник не отметит конец работы, можно использовать для него отметку **Absent (Отсутствует)** или **Early Leave (Ушел слишком рано)** и указать время раннего ухода.

3. Укажите параметры регистрации времени прибытия и ухода с работы.

При помощи опций **Check-in Required (Требуется регистрация времени прибытия)** или **Check-out Required (Требуется регистрация времени ухода)** можно настроить промежуток времени, в течение которого пользователи могут отмечать свое прибытие или уход с работы.

Вы также можете создать правило обработки информации об опоздании или раннем уходе с работы.

Примечание. Эти параметры будут устанавливаться по умолчанию для всех добавляемых периодов времени. Они не будут применяться для уже существующих интервалов.

4. Выберите параметры сверхурочной работы.

Вы можете создать правило обработки информации о периоде сверхурочной работы и указать его максимальную длительность для каждого дня.

(Дополнительная опция) Поставьте галочку в пункте **Non-scheduled Work Day (Незапланированный рабочий день)** и задайте правило обработки информации о периоде сверхурочной работы для нерабочего дня.

5. Нажмите кнопку **Save (Сохранить)**, чтобы сохранить настройки.

Настройки контрольной точки посещаемости

В качестве контрольной точки посещаемости можно указать устройство (-а) для считывания карт точки управления доступом. В этом случае считывание карты будет регистрироваться.

Инструкция:

1. Выберите вкладку **Attendance Check Point Settings (Настройки контрольной точки посещаемости)**, чтобы перейти в соответствующее окно.



2. Нажмите кнопку **+**, чтобы открыть на экране диалоговое окно добавления контрольной точки посещаемости.



3. Введите требуемую информацию.

Check Point Name (Название контрольной точки) Введите название контрольной точки.

Card Reader (Устройство для считывания карт). Выберите устройство для считывания карт из выпадающего списка.

Check Point Function (Функция контрольной точки). Выберите функцию контрольной точки.

Door Location (Местоположение двери). Укажите местоположение двери.

Check Point Description (Описание контрольной точки). Введите описание контрольной точки.

- Нажмите кнопку **Add (Добавить)**, чтобы добавить контрольную точку посещаемости. Добавленная контрольная точка посещаемости будет отображаться в списке.
- (Дополнительная опция) Поставьте галочку в пункте **Set All Card Readers as Check Points (Назначить все устройства считывания карт в качестве контрольных точек посещаемости)**.

Вы можете использовать все устройства для считывания карт в качестве контрольных точек.

Примечание. Если эту галочку не поставить, в качестве контрольных точек посещаемости будут добавлены только устройства для считывания карт из списка.

Вы также можете изменять или удалять устройства для считывания карт.

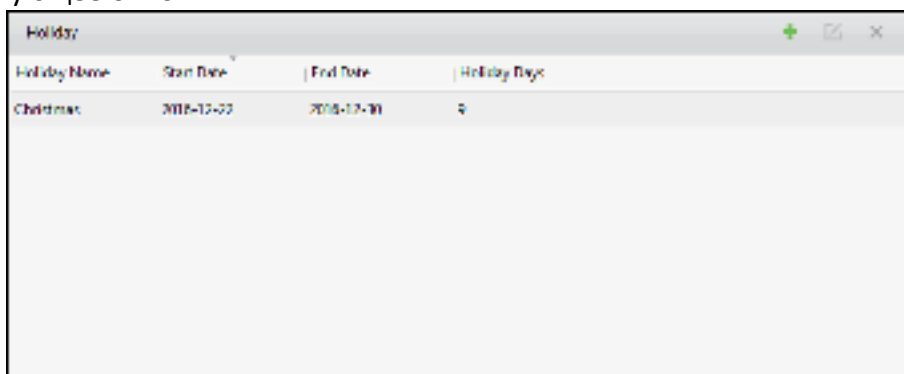
Нажмите кнопку , чтобы изменить параметры устройства для считывания карт.

Нажмите кнопку , чтобы удалить устройство для считывания карт.

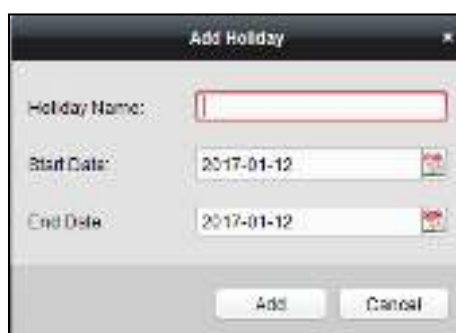
Настройки нерабочих дней

Инструкция:

- Выберите вкладку **Holiday Settings (Настройки нерабочих дней)**, чтобы перейти в соответствующее окно.



- Нажмите кнопку , чтобы открыть на экране диалоговое окно добавления нерабочего дня.



- Задайте требуемые параметры.
Holiday Name (Название нерабочего дня). Введите название нерабочего дня.
Start Date / End Date (Дата начала и дата окончания). Нажмите кнопку , чтобы указать дату нерабочего дня.
- Нажмите кнопку **Add (Добавить)**, чтобы добавить нерабочий день.
Новый нерабочий день появится в списке.
Вы также можете изменять или удалять нерабочие дни.

Нажмите кнопку , чтобы изменить параметры нерабочего дня.

Нажмите кнопку , чтобы удалить нерабочий день.

Настройки типа отпуска

Назначение:

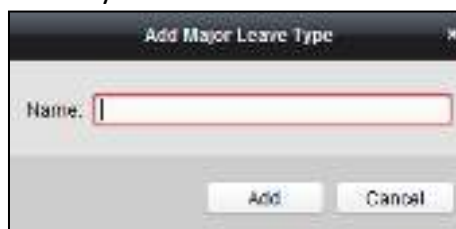
Инструкция:

1. Выберите вкладку **Leave Type Settings (Настройки типа отпуска)**, чтобы перейти в соответствующее окно.



2. Добавьте основной тип отпуска.

- 1) Нажмите кнопку  на панели, расположенной слева, чтобы открыть на экране окно добавления основного типа отпуска.



- 2) Введите название основного типа отпуска.

- 3) Нажмите кнопку **Add (Добавить)**, чтобы добавить основной тип отпуска.

Вы также можете изменить или удалить основной тип отпуска.

Нажмите кнопку , чтобы изменить параметры основного типа отпуска.

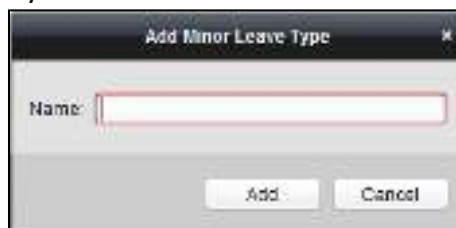
Нажмите кнопку , чтобы удалить основной тип отпуска.

3. Добавьте дополнительный тип отпуска.

- 1) Выберите основной тип отпуска.

Дополнительный тип отпуска будет отображаться на панели, расположенной справа.

- 2) Нажмите кнопку  на панели справа, чтобы открыть на экране окно добавления дополнительного типа отпуска.



- 3) Введите название дополнительного типа отпуска.

- 4) Нажмите кнопку **Add (Добавить)**, чтобы добавить дополнительный тип отпуска.

Вы также можете изменить или удалить дополнительный тип отпуска.

Нажмите кнопку , чтобы изменить параметры дополнительного типа отпуска.

Нажмите кнопку , чтобы удалить дополнительный тип отпуска.

6.14.4 Статистика посещаемости

Назначение:

После расчета данных посещаемости можно проверить сводную информацию о посещаемости, подробные данные о посещаемости, аномальные данные о посещаемости, информацию о сверхурочной работе, журналы считывания карт и отчеты, составленные на основе рассчитанных данных посещаемости.

Примечания.

- Клиент автоматически вычисляет данные о посещаемости предыдущего дня в 01:00 следующего дня.
- Не закрывайте клиент до 01:00 ночи, иначе он не сможет автоматически рассчитать данные о посещаемости предыдущего дня. Вы также можете рассчитать данные о посещаемости вручную. Подробную информацию см. в пункте *Расчет рабочего времени в ручном режиме* в разделе 6.14.2 *Обработка данных о посещаемости*.

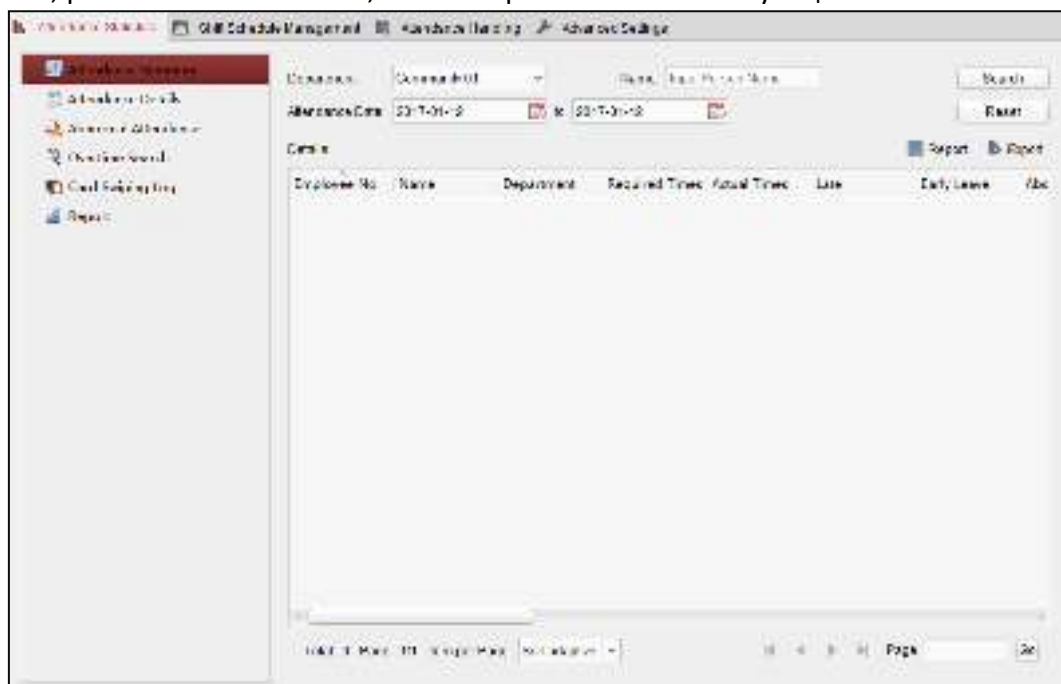
Сводная информация о посещаемости

Назначение:

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

Инструкция:

1. В модуле учета рабочего времени выберите вкладку **Attendance Statistics (Статистика посещаемости)**, чтобы перейти на соответствующую страницу.
2. Нажмите на элемент **Attendance Summary (Сводная информация о посещаемости)** на панели, расположенной слева, чтобы перейти в соответствующее окно.

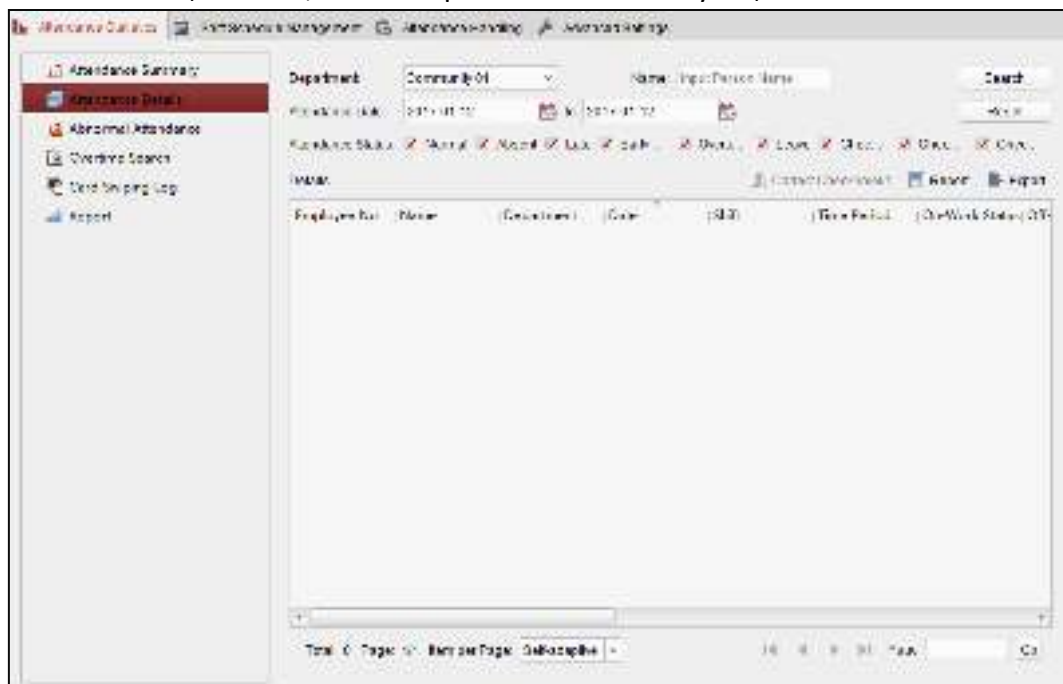


3. Укажите критерии поиска, в том числе отдел, имя сотрудника и дату посещения.
(Дополнительная опция) Нажмите кнопку **Reset (Сбросить)**, чтобы сбросить все заданные критерии поиска.
4. Нажмите кнопку **Search (Поиск)**, чтобы начать поиск. Все результаты будут отображены в виде списка на данной странице.
(Дополнительная опция) Нажмите кнопку **Report (Отчет)**, чтобы создать отчет о посещаемости.
(Дополнительная опция) Нажмите кнопку **Export (Экспортировать)**, чтобы экспортировать результаты на локальный компьютер.

Подробные данные о посещаемости

Инструкция:

1. Нажмите кнопку **Attendance Details (Подробные данные о посещаемости)** на странице статистики посещаемости, чтобы перейти в соответствующее окно.



2. Укажите критерии поиска, в том числе отдел, имя сотрудника, дату посещения и статус.
(Дополнительная опция) Нажмите кнопку **Reset (Сбросить)**, чтобы сбросить все заданные критерии поиска.
3. Нажмите кнопку **Search (Поиск)**, чтобы начать поиск. Все результаты будут отображены в виде списка на данной странице.
(Дополнительная опция) Выберите результат поиска в списке и нажмите кнопку **Correct Check-in/out (Коррекция регистрации времени прибытия/ухода)**, чтобы скорректировать статус регистрации времени прибытия или ухода с работы.
(Дополнительная опция) Нажмите кнопку **Report (Отчет)**, чтобы создать отчет о посещаемости.
(Дополнительная опция) Нажмите кнопку **Export (Экспортировать)**, чтобы экспортировать результаты на локальный компьютер.

Аномальные данные о посещаемости

Вы можете искать и получать статистику аномальных данных о посещаемости, в том числе

номер, имя и отдел сотрудников, тип аномальных данных, время начала и окончания, а также дата посещения. Подробную информацию см. в *разделе 0 Назначение*:

После расчета данных посещаемости можно проверить сводную информацию о посещаемости, подробные данные о посещаемости, аномальные данные о посещаемости, информацию о сверхурочной работе, журналы считывания карт и отчеты, составленные на основе рассчитанных данных посещаемости.

Примечания.

- Клиент автоматически вычисляет данные о посещаемости предыдущего дня в 01:00 следующего дня.
- Не закрывайте клиент до 01:00 ночи, иначе он не сможет автоматически рассчитать данные о посещаемости предыдущего дня. Вы также можете рассчитать данные о посещаемости вручную. Подробную информацию см. в Расчет рабочего времени в ручном режиме в *разделе 6.14.2 Обработка данных о посещаемости*.

Сводная информация о посещаемости.

Поиск информации о сверхурочной работе

Вы можете искать и получать статистику статуса работы в сверхурочное время для выбранного сотрудника за указанный период. Вы также можете просматривать подробную информацию о сверхурочной работе, в том числе номер, имя и отдел сотрудников, дату посещения, продолжительность и тип сверхурочной работы. Подробную информацию см. в *разделе 0 Назначение*:

После расчета данных посещаемости можно проверить сводную информацию о посещаемости, подробные данные о посещаемости, аномальные данные о посещаемости, информацию о сверхурочной работе, журналы считывания карт и отчеты, составленные на основе рассчитанных данных посещаемости.

Примечания.

- Клиент автоматически вычисляет данные о посещаемости предыдущего дня в 01:00 следующего дня.
- Не закрывайте клиент до 01:00 ночи, иначе он не сможет автоматически рассчитать данные о посещаемости предыдущего дня. Вы также можете рассчитать данные о посещаемости вручную. Подробную информацию см. в Расчет рабочего времени в ручном режиме в *разделе 6.14.2 Обработка данных о посещаемости*.

Сводная информация о посещаемости.

Журнал считывания карт

Вы можете выполнять поиск в журналах считывания карт, используемых для формирования статистики посещаемости. После поиска в журналах можно просмотреть данные о считывании карты, в том числе имя и отдел сотрудников, время считывания карты, режим проверки подлинности устройства для считывания карт и номер карты. Подробную информацию см. в *разделе 0 Назначение*:

После расчета данных посещаемости можно проверить сводную информацию о посещаемости, подробные данные о посещаемости, аномальные данные о посещаемости, информацию о сверхурочной работе, журналы считывания карт и отчеты, составленные на основе рассчитанных данных посещаемости.

Примечания.

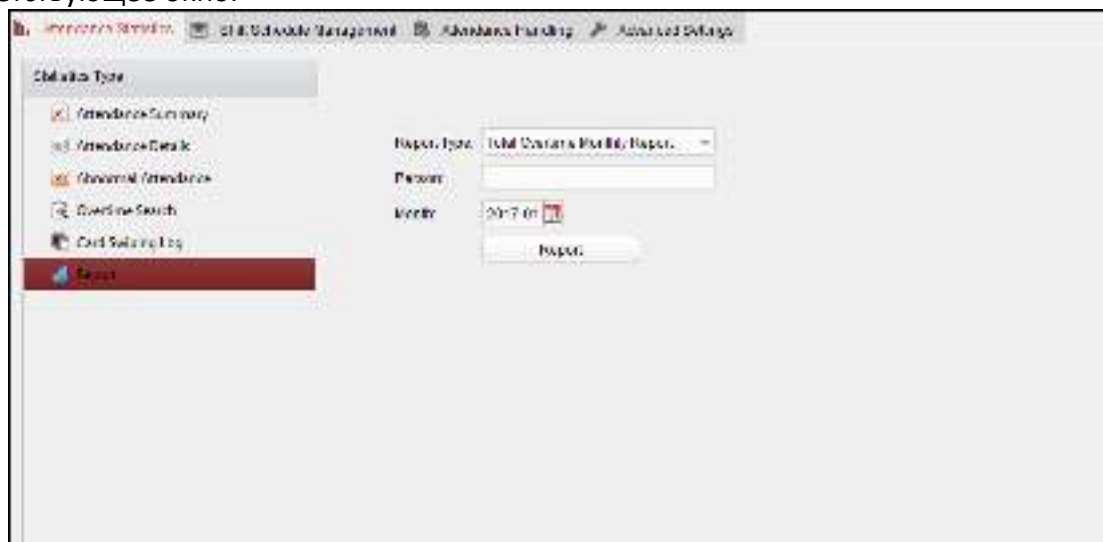
- Клиент автоматически вычисляет данные о посещаемости предыдущего дня в 01:00 следующего дня.

- Не закрывайте клиент до 01:00 ночи, иначе он не сможет автоматически рассчитать данные о посещаемости предыдущего дня. Вы также можете рассчитать данные о посещаемости вручную. Подробную информацию см. в Расчет рабочего времени в ручном режиме в *разделе 6.14.2 Обработка данных о посещаемости*.

Сводная информация о посещаемости.

Отчет

Нажмите кнопку **Report (Отчет)** на странице статистики посещаемости, чтобы перейти в соответствующее окно.

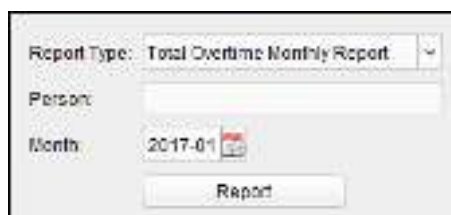


➤ Создание месячного отчета об общем количестве сверхурочных часов работы

Инструкция:

1. Нажмите кнопку  в поле **Report Type (Тип отчета)** и выберите пункт **Total Overtime**

Monthly Report (Месячный отчет об общем количестве сверхурочных часов работы) в выпадающем списке.



2. Перейдите в поле **Person (Пользователь)** и выберите требуемого сотрудника.
3. Нажмите кнопку  и выберите месяц.
4. Нажмите кнопку **Report (Отчет)**, чтобы создать месячный отчет об общем количестве сверхурочных часов работы.

➤ Создание месячного отчета о сверхурочной работе

Выберите в качестве типа отчета **Overtime Details Monthly Report (Месячный отчет о сверхурочной работе)**. Вы можете создать месячный отчет о сверхурочной работе. Подробную информацию см. в разделе *Создание месячного отчета об общем количестве сверхурочных часов работы*.

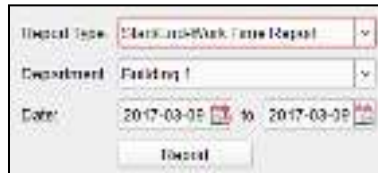
➤ Создание месячного отчета о посещаемости

Выберите в качестве типа отчета **Attendance Monthly Report (Месячный отчет о посещаемости)**. Вы можете создать месячный отчет о посещаемости. Подробную информацию см. в разделе *Создание месячного отчета об общем количестве сверхурочных часов работы*.

➤ **Создание отчета о времени начала и окончания работы**

Инструкция:

1. Нажмите кнопку  в поле **Report Type (Тип отчета)** и выберите пункт **Start/End-Work Time Report (Отчет о времени начала и окончания работы)** в выпадающем списке.



2. Перейдите в поле **Department (Отдел)** и выберите требуемый отдел.
3. Нажмите кнопку , чтобы указать дату начала и окончания заданного периода.
4. Нажмите кнопку **Report (Отчет)**, чтобы создать месячный отчет об общем количестве сверхурочных часов работы.

➤ **Создание отчета о посещаемости в отделе**

Выберите в качестве типа отчета **Department Attendance Report (Отчет о посещаемости в отделе)**, чтобы создать соответствующий отчет. Подробную информацию см. в разделе *Создание отчета о времени начала и окончания работы*, который приведен выше.

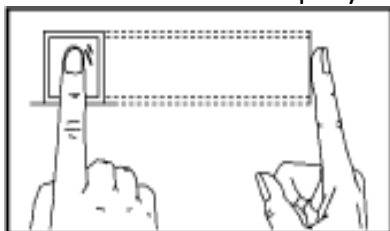
Приложение А Советы по сканированию отпечатков пальцев

Рекомендуемый палец

Указательный, средний или безымянный палец.

Правильное выполнение сканирования

На показанном ниже рисунке изображен правильный способ сканирования пальца:

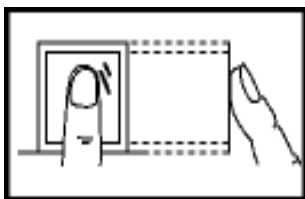


Палец нужно прикладывать к сканеру горизонтально. Центр сканируемого пальца должен располагаться в центре сканера.

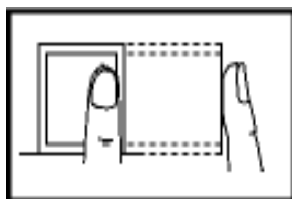
Неправильное сканирование

На приведенных далее рисунках показаны варианты неправильного сканирования отпечатка пальца:

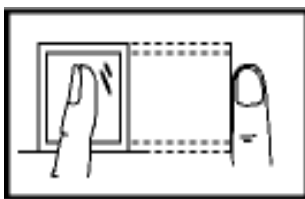
Приложение пальца по вертикали



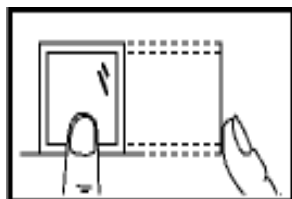
Край I



Боковая часть



Край II



Рабочая среда

Не подвергайте сканер воздействию яркого света, высокой температуры, чрезмерной влажности и капель дождя.

В условиях повышенной сухости сканер может не распознать ваш отпечаток пальца. Подуйте на палец, чтобы высушить кожу, и попробуйте выполнить операцию еще раз.

Прочая информация

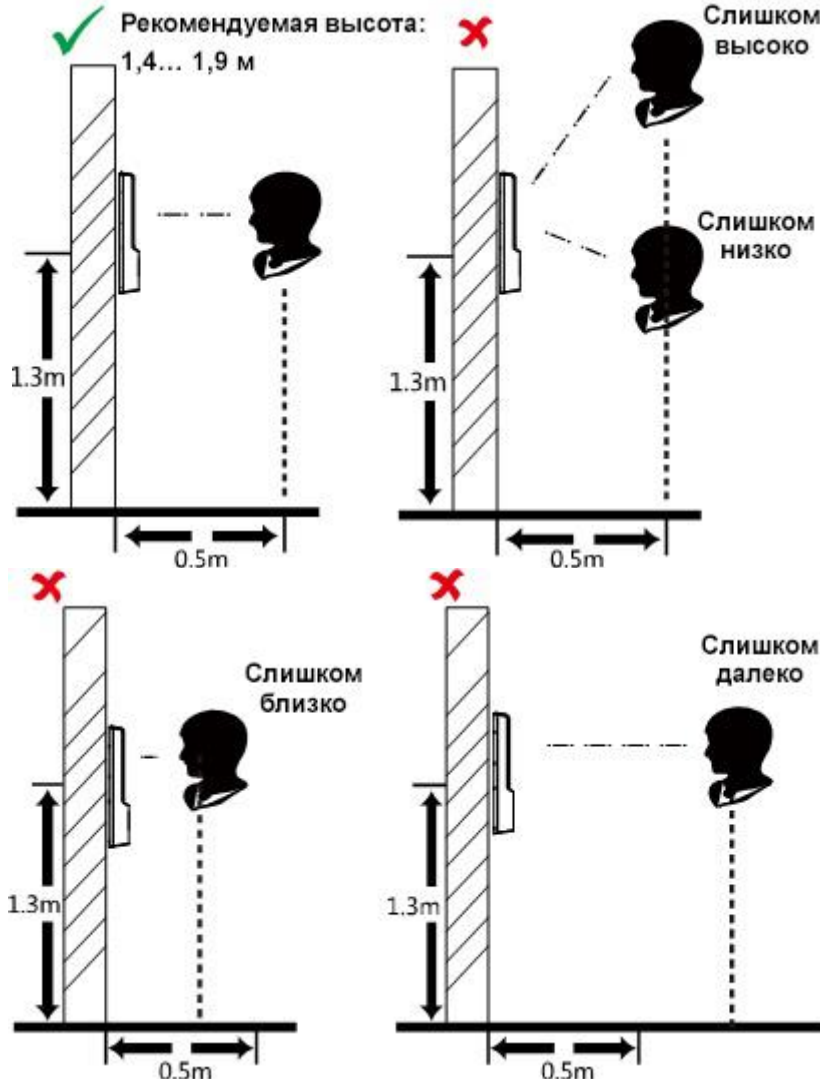
Если отпечаток пальца слишком нечеткий, или его тяжело отсканировать, используйте другие способы аутентификации.

Сканер может не распознать отпечаток пальца, если кожа пальца была повреждена. Попробуйте отсканировать отпечаток другого пальца.

Приложение В Советы по сбору и сравнению изображений лица

В 1 Положение (рекомендуемое расстояние — 0,5 м)

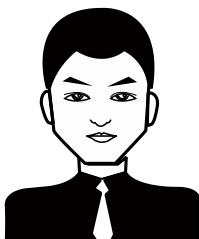
Варианты положения головы при сборе и сравнении изображения лица представлены ниже:



Примечание. Подробную информацию о соотношении между ростом человека, высотой расположения устройства и расстоянием между человеком и устройством см. в Приложении С.

В 2 Выражение лица

- При сборе или сравнении изображений сохраняйте свое естественное выражение лица, как это показано на следующем рисунке.



- Не надевайте шляпу, солнцезащитные очки или другие аксессуары, которые могут повлиять на функцию распознавания лиц.
- Не закрывайте волосами глаза, уши и т. д. Не наносите сильный макияж.

В 3 Поза

Чтобы получить качественное и точное изображение лица, при выполнении сбора или сравнения разместите лицо прямо перед камерой.



В 4 Размер

Убедитесь, что ваше лицо находится в середине окна для съемки изображения.



Приложение С Советы в отношении рабочей среды на месте установки оборудования

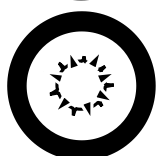
1. Номинальное значение освещенности источника света



Свеча: 10 лк



Лампа: 100... 850 лк.

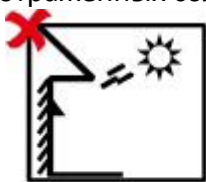


Солнечный свет: Свыше
1 200 лк

2. Если источник света находится на расстоянии 0,5 м от устройства, освещение должно быть не менее 100 лк.
3. При установке в помещении устройство должно находиться на расстоянии не менее 2 м от источника света и не менее 3 м от окна или двери.



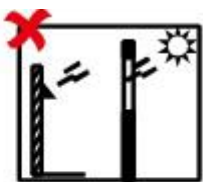
4. Избегайте наличия света, падающего на объект сзади, а также воздействия прямых и отраженных солнечных лучей.



Освещение,
направленное
на объект сзади



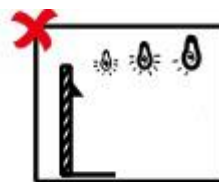
Прямой
солнечный свет



Прямой
солнечный свет
сквозь окно

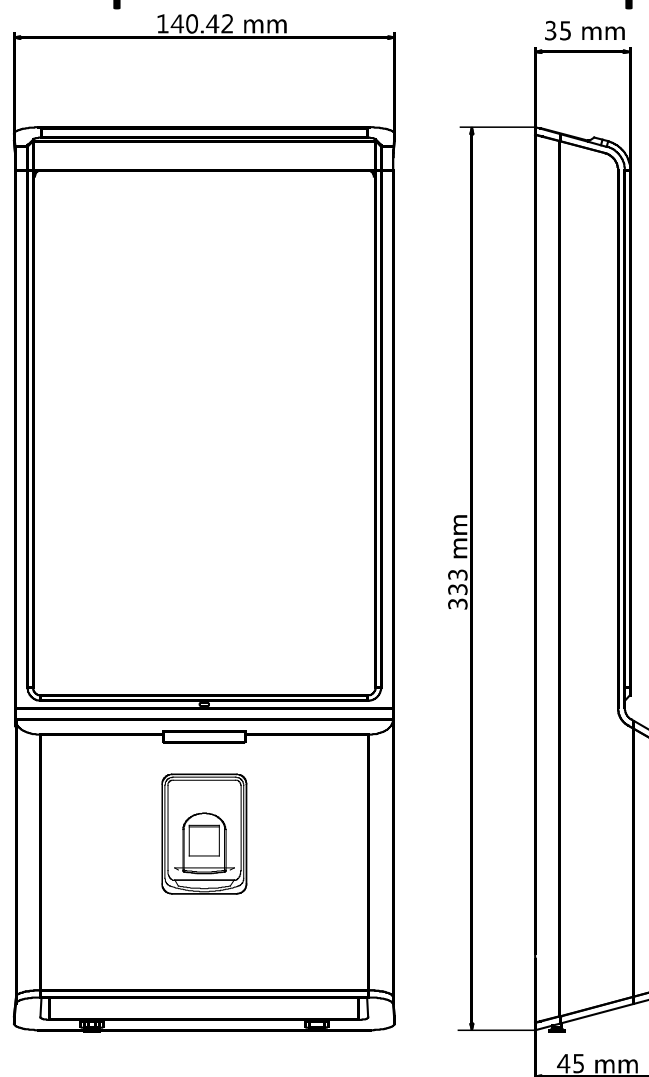


Отраженный
солнечный свет
сквозь окно



Близко к
источнику света

Приложение D Размеры



0100001080205



See Far, Go Further