Терминал доступа с функцией распознавания лиц

Руководство пользователя

Правовая информация

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. Все права защищены.

О руководстве

Руководство содержит инструкции для использования и управления продуктом. Изображения, графики и вся другая информация предназначена только для ознакомления. Этот документ может быть изменен без уведомления, в связи с обновлением прошивки и по другим причинам. Последнюю версию настоящего документа можно найти на веб-сайте (***https://www.hikvision.com/***).
Используйте этот документ под руководством профессионалов, обученных работе с продуктом.

Торговые марки

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

Правовая информация

ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ДАННОЕ РУКОВОДСТВО, ПРОДУКТ, АППАРАТУРА, ПРОГРАММНОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», СО ВСЕМИ ОШИБКАМИ И НЕТОЧНОСТЯМИ. HIKVISION НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, КАСАТЕЛЬНО УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ. ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА НЕСЕТ ПОЛЬЗОВАТЕЛЬ.
HIKVISION НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД ПОТРЕБИТЕЛЕМ ЗА КАКОЙ-ЛИБО СЛУЧАЙНЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ, ВКЛЮЧАЯ УБЫТКИ ИЗ-ЗА ПОТЕРИ ПРИБЫЛИ, ПЕРЕРЫВА В ДЕЯТЕЛЬНОСТИ ИЛИ ПОТЕРИ ДАННЫХ ИЛИ ДОКУМЕНТАЦИИ, ПО ПРИЧИНЕ НАРУШЕНИЯ УСЛОВИЙ КОНТРАКТА, ТРЕБОВАНИЙ (ВКЛЮЧАЯ ХАЛАТНОСТЬ), УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ ИНОГО, В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ HIKVISION БЫЛО ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.
ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ; HIKVISION НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, HIKVISION ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.
ВЫ ОБЯЗУЕТЕСЬ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В СООТВЕТСТВИИ С ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, А ТАКЖЕ НЕСЕТЕ ПОЛНУЮ ОТВЕТСТВЕННОСТЬ ЗА ЕГО СОБЛЮДЕНИЕ. В ЧАСТНОСТИ, ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ДАННОГО ПРОДУКТА ТАКИМ ОБРАЗОМ, ЧТОБЫ НЕ НАРУШАТЬ ПРАВА ТРЕТЬИХ ЛИЦ, ВКЛЮЧАЯ ПРАВА НА ПУБЛИЧНОСТЬ, ПРАВА НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ, ЗАЩИТУ ДАННЫХ

И ДРУГИЕ ПРАВА КАСАТЕЛЬНО НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ. ВЫ ОБЯЗУЕТЕСЬ НЕ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В ЗАПРЕЩЕННЫХ ЦЕЛЯХ, ВКЛЮЧАЯ РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ, РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ХИМИЧЕСКОГО ИЛИ БИОЛОГИЧЕСКОГО ОРУЖИЯ, ЛЮБУЮ ДЕЯТЕЛЬНОСТЬ, СВЯЗАННУЮ С ЯДЕРНЫМИ ВЗРЫВЧАТЫМИ ВЕЩЕСТВАМИ, НЕБЕЗОПАСНЫМ ЯДЕРНЫМ ТОПЛИВНЫМ ЦИКЛОМ ИЛИ НАРУШАЮЩУЮ ПРАВА ЧЕЛОВЕКА.
В СЛУЧАЕ КАКИХ-ЛИБО КОНФЛИКТОВ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.

Защита данных

Во время использования устройства личные данные будут собираться, храниться и обрабатываться. При разработке устройств Hikvision соблюдаются принципы конфиденциальности в целях защиты данных. Например, устройства с функциями распознавания лиц разработаны таким образом, что сохраняемые биометрические данные защищены шифрованием; в устройствах с функцией идентификации по отпечатку пальца будут сохранены только шаблоны отпечатка пальца и, таким образом, изображение отпечатка пальца не подлежит реконструкции.
Поскольку данные находятся под вашим контролем, сбор, хранение, обработку и передачу данных необходимо выполнять в соответствии с применимыми законами и требованиями по защите данных. Также необходимо выполнять действия по безопасности для защиты личных данных, такие как разумный административный и физический контроль безопасности, периодические обзоры и оценки эффективности мер безопасности.

Условные обозначения

В настоящем документе используются следующие символы:

Символ	Описание
Предупреждения	Указывает на опасную ситуацию, которая, если не удастся ее избежать, может привести к летальному исходу или серьезным травмам.
Предостережения	Указывает на потенциально опасную ситуацию, которая, если не удастся ее избежать, может привести к повреждению оборудования, потере данных, ухудшению рабочих характеристик, либо к получению неожиданных результатов.
Примечание	Предоставляет дополнительную информацию, чтобы подчеркнуть или дополнить важные пункты основного текста.

Регулирующая информация

Информация о FCC

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 FCC: это оборудование прошло испытания и соответствует регламенту для цифрового устройства класса B, применительно к части 15 Правил FCC. Данный регламент разработан для того, чтобы обеспечить необходимую защиту от вредных помех, возникающих при использовании оборудования в коммерческой среде. Это оборудование генерирует, использует, и может излучать радиоволны на разных частотах и, если устройство установлено и используется не в соответствии с инструкцией, оно может создавать помехи для радиосигналов. Тем не менее, нет никакой гарантии, что помехи не возникнут в каких-либо конкретных случаях установки. 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:
—Изменить ориентацию или местоположение приемной антенны.
—Увеличить расстояние между оборудованием и приемником.
—Подключить оборудование к розетке в цепи, отличной от той, к которой подключен приемник.
—Обратиться к дилеру или опытному радио/телемастеру.
Данное оборудование следует устанавливать и эксплуатировать на расстоянии не менее 20 см между источником излучения и пользователем.
Условия FCC
Это устройство соответствует требованиям части 15 правил FCC. Эксплуатация допускается при соблюдении следующих двух условий:
1. Данное устройство не должно создавать вредных помех.
2. Данное устройство должно выдерживать возможные помехи, включая те, которые могут привести к выполнению нежелательных операций.

Соответствие стандартам ЕС

CE

Данный продукт и – если применимо – также и поставляемые принадлежности отмечены знаком «CE» и, следовательно, согласованы с европейскими стандартами, перечисленными под директивами 2014/30/EC EMC, 2014/53/EC и 2011/65/EC RoHS.

2012/19/EC (директива WEEE): продукты, отмеченные данным знаком, запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Для надлежащей переработки верните этот продукт своему местному поставщику при покупке эквивалентного нового оборудования или утилизируйте его в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info

2006/66/EC (директива о батареях): данный продукт оснащен батареей, которую запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Более подробная информация представлена в документации по продукту. Батарея отмечена значком, который может включать наименования, обозначающие содержание кадмия (Cd), свинца (Pb) или ртути (Hg). Для надлежащей утилизации возвратите батарею своему поставщику либо избавьтесь от нее в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info

Инструкция по технике безопасности

Эта инструкция предназначена для того, чтобы пользователь мог использовать продукт правильно и избежать опасности или причинения вреда имуществу.
Меры предосторожности разделены на «Предупреждения» и «Предостережения».
Предупреждения: игнорирование предупреждений может привести к тяжелым травмам или смерти.
Предостережения: игнорирование предостережений может привести к травмам или порче оборудования.

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

⚠ Предупреждения:

- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в регионе эксплуатации.
- Используйте адаптер питания соответствующей компании. Потребляемая мощность не может быть меньше требуемого значения.
- Не подключайте несколько устройств к одному блоку питания, перегрузка адаптера может привести к перегреву или возгоранию.
- Прежде чем подключать, устанавливать или разбирать устройство, убедитесь, что питание отключено.
- Если устройство устанавливается на потолок или стену, убедитесь, что оно надежно закреплено.
- Если из устройства идет дым или доносится шум – отключите питание, извлеките кабель и свяжитесь с сервисным центром.
- При замене батареи батареей несоответствующего типа существует риск взрыва.
- Замена батареи на батарею несоответствующего типа может привести к нарушению мер предосторожности (например, в случае некоторых типов литиевых батарей).
- Данное оборудование не подходит для использования в местах, где могут присутствовать дети.
- Запрещено помещать батарею в огонь или работающий духовой шкаф, разбивать и или резать батарею, так как это может привести к взрыву.
- Запрещено оставлять батарею в окружающей среде при очень высоких температурах, так как это может привести к взрыву или утечке горючей жидкости или газа.
- Запрещено подвергать батарею воздействию крайне низкого давления воздуха, так как это может привести к взрыву или утечке горючей жидкости или газа.
- Использованные батареи необходимо утилизировать в соответствии с инструкциями

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

⚠ Предостережения:

- Запрещено ронять устройство и подвергать воздействию сильных электромагнитных помех. Избегайте установки устройства на вибрирующую поверхность или в местах, подверженных ударам (пренебрежение этим предостережением может привести к повреждению устройства).
- Запрещено размещать устройство в местах с чрезвычайно высокой или низкой температурой окружающей среды (подробная информация о рабочей температуре представлена в спецификации устройства), в пыльной или влажной среде, запрещено подвергать устройство воздействию сильных электромагнитных помех.
- Не подвергайте крышку устройства, предназначенного для использования внутри помещения, воздействию дождя или влаги.
- Не подвергайте устройство воздействию прямых солнечных лучей, не устанавливайте в местах с плохой вентиляцией или рядом с источником тепла таким, как обогреватель или радиатор (пренебрежение этим предостережением может привести к пожару).
- Запрещено направлять устройство на солнце или очень яркие источники света. Яркий свет может вызвать размытие или потерю четкости изображения (что не является признаком неисправности), а также повлиять на срок службы матрицы.
- Используйте прилагаемую перчатку во время демонтажа крышки устройства, избегайте прямого контакта с крышкой устройства, так как пот и жир с пальцев могут стать причиной разрушения защитного покрытия на поверхности устройства.
- Для очистки внутренних и внешних поверхностей крышки устройства используйте мягкую и сухую ткань, не используйте щелочные моющие средства.
- Сохраните упаковку после распаковки для использования в будущем. В случае сбоя работы устройство необходимо вернуть на завод (с оригинальной упаковкой). Транспортировка без оригинальной упаковки может привести к повреждению устройства и к дополнительным расходам.
- Неправильное использование или замена батареи может привести к опасности взрыва. Проводите замену на такие же батареи или аналогичные. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем батарей.
- Продукты с биометрическим распознаванием не на 100 % применимы для защиты от подделки биометрических данных. Используйте несколько режимов аутентификации, если требуется более высокий уровень безопасности.
- Входное напряжение AC от 100 до 240 В или DC 12 В должно соответствовать стандарту безопасного сверхнизкого напряжения (SELV) и ограниченному источнику питания стандарта IEC60950-1. Подробная информация представлена в технических спецификациях.

Доступные модели

Наименование	Модель
Терминал доступа с функцией распознавания лиц	ACT-T1331
	ACT-T1331W

Используйте только те источники питания, которые указаны ниже:

Модель	Производитель	Стандарт
ADS-26FSG-12 12018EPG	Shenzhen Honor Electronic Co., Ltd.	PG
ADS-26FSG-12 12018EPI-01	Shenzhen Honor Electronic Co., Ltd.	PI
ADS-26FSG-12 12018EPCU	Shenzhen Honor Electronic Co., Ltd.	PCU
ADS-26FSG-12 12018EPB	Shenzhen Honor Electronic Co., Ltd.	PB
MSA-C1500IC12.0-18P-BR	MOSO Technology Co., Ltd.	PBR

Содержание

Раздел 1 Представление продукта

1.1 Представление продукта

Терминал распознавания лиц является терминалом доступа с функцией распознавания лиц. В основном применяется в системах контроля доступа на территории логистических центров, аэропортов, образовательных учреждений, жилых помещений, на станциях сигнализации и т. д.

1.2 Особенности

- 3.97” сенсорный LCD-экран
- 2 Мп, 2 широкоугольных объектива
- Детекция подлинности биометрических данных лица (антиспуфинг)
- Расстояние распознавания лиц: от 0.3 до 1.5 м
- Рекомендуемая высота установки для распознавания лиц: от 1.4 до 1.9 м
- Алгоритм глубокого обучения
- Количество лиц — 1000, количество карт (при подключении внешнего считывателя карт) — 1500, количество событий — 150 000, хранение до 20 000 захваченных изображений
- Скорость распознавания лиц < 0.2 с/чел.; точность распознавания лиц ≥ 99 %
- Привязка захвата и хранение захваченных изображений
- Передает данные карты и пользователя из или в клиентское программное обеспечение по протоколу TCP/IP и сохраняет данные в клиентском программном обеспечении
- Импорт изображений с USB-накопителя на устройство или экспорт изображений, событий с устройства на USB-накопитель
- Автономная работа
- Управление, поиск и установка данных устройства после локального входа в устройство
- Возможность подключения к одному внешнему считывателю карт через протокол RS-485
- Возможность подключения к модулю безопасности двери через протокол RS-485, чтобы избежать открытия двери при разрушении устройства
- Голосовое предупреждение
- Функция сторожевого таймера и детектор саботажа
- Поддержка английского, испанского (Южная Америка), арабского, тайского, индонезийского, русского, вьетнамского, португальского (Бразилия) языков

Раздел 2 Внешний вид устройства

Более подробная информация о терминале доступа с функцией распознавания лиц представлена далее.

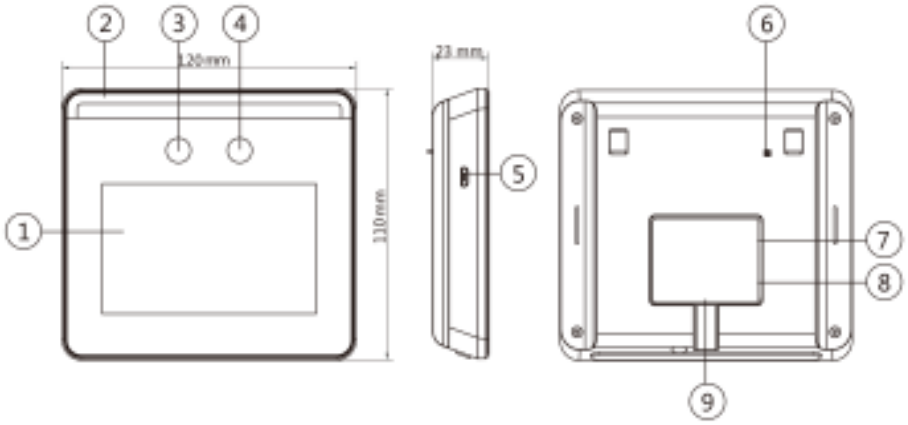


Рисунок 2-1. Схема терминала доступа с функцией распознавания лиц

Таблица 2-1. Описание терминала доступа с функцией распознавания лиц

№	Наименование	Описание
1	Экран	3.97” сенсорный LCD-экран
2	Подсветка	Подсветка камеры
3	Камера 1	Запись или захват видео или изображений
4	Камера 2	Запись или захват видео или изображений
5	Micro USB	Подключение к USB-накопителю через кабель microUSB-USB.
6	Детектор саботажа	После установки, если устройство будет разобрано, сработает тревога тампера
7	Сетевой интерфейс	Подключение к Ethernet.
8	Разъемы	Подключение к другим внешним устройствам, включая считыватель карт RS-485, дверной замок и т. д.
9	Служебный порт	Служебный порт, используется только для отладки

Раздел 3 Установка

3.1 Среда установки

- Избегайте попадания на устройство контрового света, а также прямых и непрямых солнечных лучей.
- Для обеспечения лучшего распознавания источник света должен быть расположен в среде установки или недалеко от места установки.

Примечание

Более подробная информация представлена в «*Рекомендациях по среде установки».*

3.2 Установка на основание

Установите устройство на стол или другую поверхность с помощью монтажного кронштейна.

Шаги

1. Проложите кабели через отверстие для кабеля на кронштейне и подключите кабели внешних устройств в разъемы.
2. Совместите два отверстия устройства с двумя креплениями кронштейна.
3. Повесьте устройство на кронштейн и убедитесь, что крепление, расположенное в середине кронштейна, вставлено в паз на задней панели устройства.

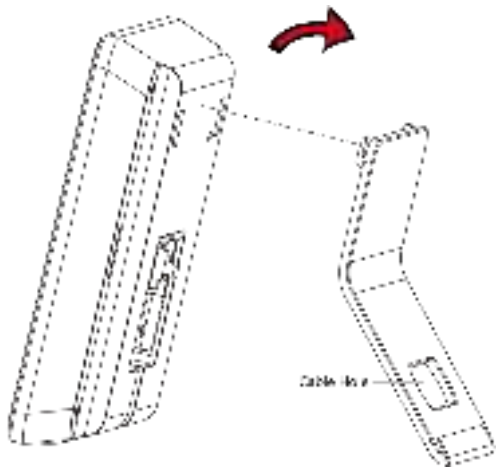


Рисунок 3-1. Установка на основание

Английский язык	Русский язык
Cable Hole	Отверстие для кабеля

4. Расположите собранное устройство и кронштейн на столе или другой плоской поверхности.

3.3 Установка с использованием монтажной коробки

Шаги

1. В соответствии с линией отсчета на монтажном шаблоне расположите монтажный шаблон на стене или другой поверхности на 1.45 метра выше уровня земли.

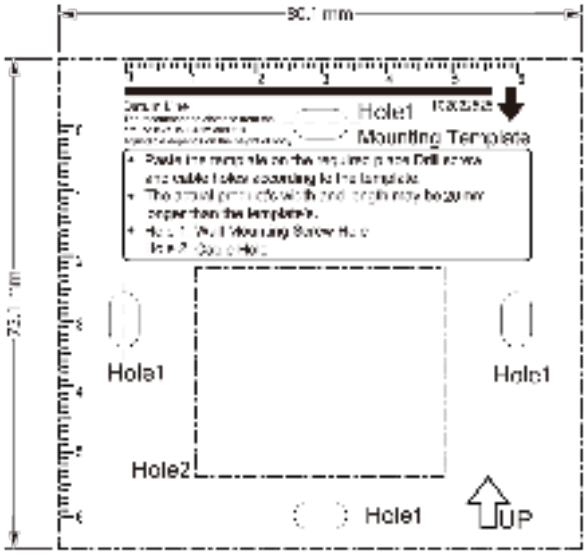


Рисунок 3-2. Монтажный шаблон

Английский язык	Русский язык
Hole	Отверстие
Mounting Template	Монтажный шаблон
Paste the template on the required place. Drill screw and cable holes according to the template.	Разместите шаблон в необходимом месте. Просверлите отверстия для винтов и кабелей по шаблону.
The actual product's width and length maybe be 20 mm longer than the template's.	Фактическая ширина и длина продукта могут быть на 20 мм больше, чем у шаблонов.
Hole 1: Wall Mounting Screw Hole Hole 2: Cable Hole	Отверстие 1: отверстие для винта для установки на стену Отверстие 2: отверстие для кабеля
UP	Верх

2. В соответствии с монтажным шаблоном просверлите отверстия в стене или другой поверхности и установите монтажную коробку.

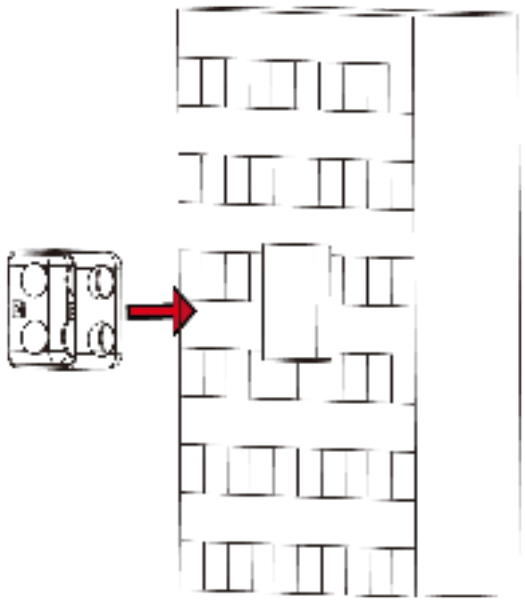


Рисунок 3-3. Установка монтажной коробки

3. Закрепите монтажную плату на монтажной коробке с помощью двух винтов, поставляемых в комплекте (SC-KM4x25-SUS или KA4 × 22-SUS).

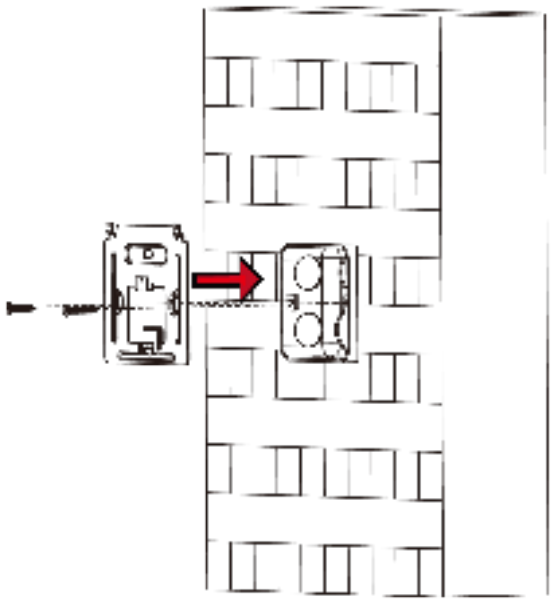


Рисунок 3-4. Установка монтажной платы

4. Проложите кабели через отверстие для кабеля на монтажной плате и подключите кабели внешних устройств к разъемам.
5. Расположите устройство в соответствии с монтажной платой и повесьте устройство на монтажной плате.

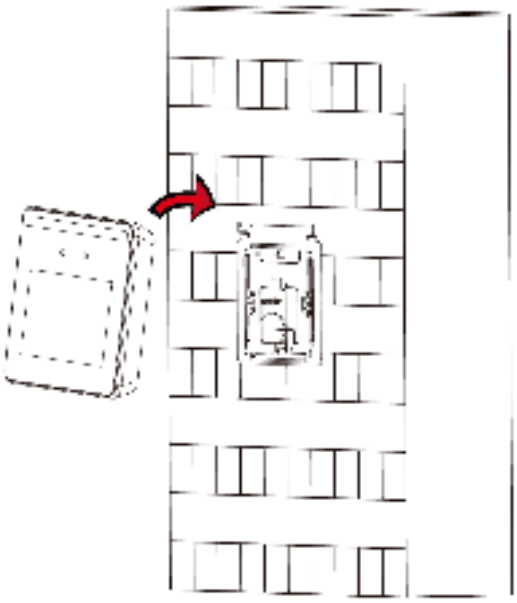


Рисунок 3-5. Установка устройства

6. Закрепите устройство и монтажную плату с помощью винта, поставляемого в комплекте.

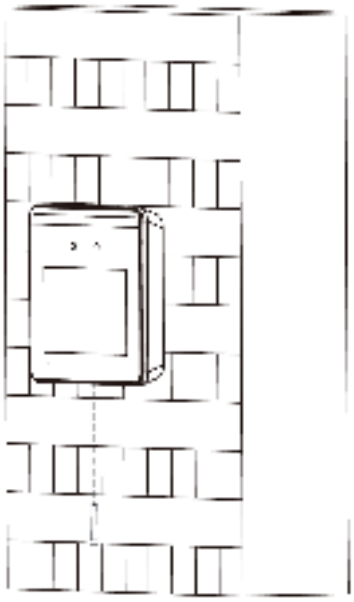


Рисунок 3-6. Фиксация устройства

Примечание

- Указанная высота установки является рекомендуемой. Высоту можно изменить на необходимый уровень.
- Просверлите отверстия на монтажной поверхности в соответствии с поставляемым монтажным шаблоном.

Раздел 4 Подключение

- Устройство может быть подключено к периферийным устройствам, поддерживается подключение считывателя карт RS-485, дверного замка, кнопки выхода, контроллера доступа и источника питания.

Примечание

Если размер кабеля 18 AWG, используйте источник питания мощностью 12 В. Расстояние между источником питания и устройством не должно превышать 80 м.

- Если нет необходимости подключать устройство к периферийным устройствам, устройство можно подключить к источнику питания напрямую, используя прилагаемый кабель питания.

4.1 Описание разъемов

К устройству можно подключить источник питания, RS-485 и дверной замок.
Ниже представлена схема подключения терминала:

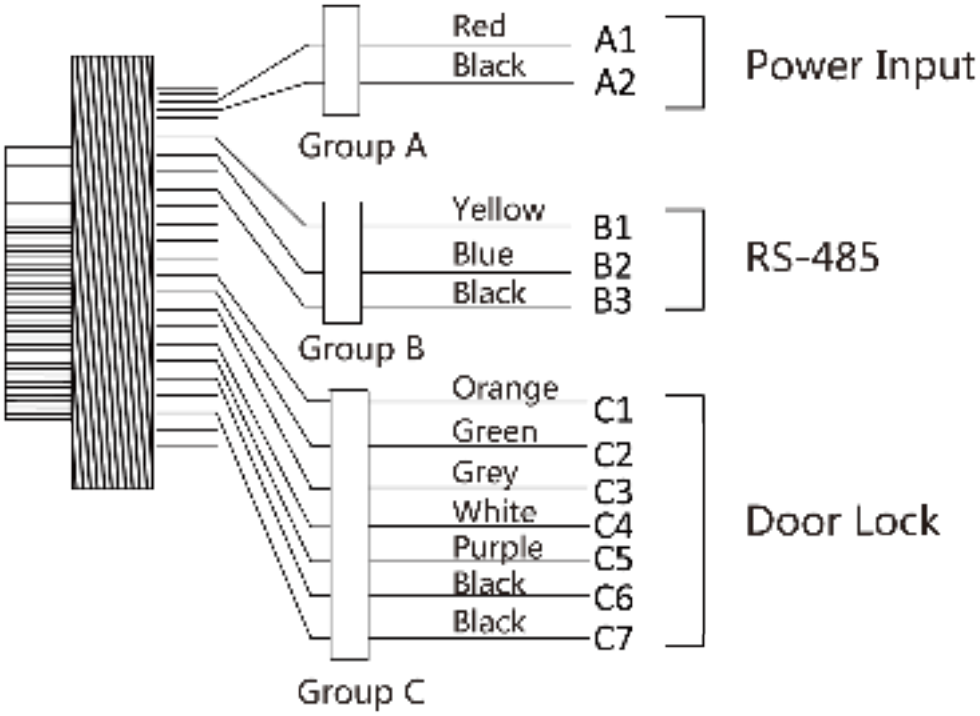


Рисунок 4-1. Схема подключения терминала

Английский язык	Русский язык
Group	Группа
Yellow	Желтый
Blue	Синий
Black	Черный
Orange	Оранжевый
Green	Зеленый
Grey	Серый
White	Белый
Purple	Фиолетовый
Power Input	Вход питания
RS-485	RS-485
Door Lock	Дверной замок

Терминал оснащен следующими разъемами:

Таблица 4-1. Описание разъемов

Группа	№	Функция	Цвет	Наименование	Описание
Группа A	A1	Вход питания	Красный	+12 V	Питание DC 12 В
	A2		Черный	GND	Заземление
Группа B	B1	RS-485	Желтый	485+	Подключение по RS-485
	B2		Синий	485-	
	B3		Черный	GND	Заземление
Группа C	C1	Дверной замок	Оранжевый	NC	Подключение замка (нормально замкнутый)
	C2		Зеленый	COM	Обычный
	C3		Серый	NO	Подключение замка (нормально разомкнутый)
	C4		Белый	SENSOR	Дверной контакт (датчик)
	C5		Фиолетовый	BTN	Подключение выходной двери
	C6		Черный	GND	Заземление
	C7		Черный	GND	Заземление

4.2 Подключение устройства (стандартный режим)

Терминал можно подключить к стандартному внешнему оборудованию.

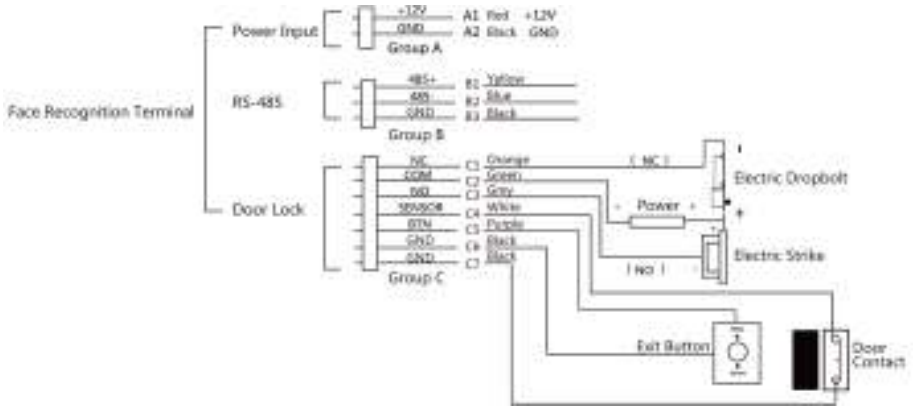


Рисунок 4-2. Подключение устройства

Английский язык	**Русский язык**
Face Recognition Terminal	Терминал доступа с функцией распознавания лиц
Power Input	Источник питания
RS-485	RS-485
Door Lock	Дверной замок
GND	Заземление
Sensor	Датчик
Red	Красный
Black	Черный
Yellow	Желтый
Blue	Синий
Orange	Оранжевый
Green	Зеленый
Grey	Серый
White	Белый
Purple	Фиолетовый
Power	Питание
NC	Нормально закрытый
NO	Нормально открытый
Exit Button	Кнопка выхода
Electric Dropbolt	Электромагнитная защелка
Electric Strike	Электромеханическая защелка
Door Contact	Дверной контакт

Примечание

- Применимы следующие параметры входного питания: DC 12 В, 1,5 А, 18 Вт.
- Запрещено подключать устройство напрямую к электрической сети.

4.3 Подключение с использованием кабеля питания

Если нет необходимости подключать устройство к периферийным устройствам, подключите устройство к источнику питания напрямую, используя прилагаемый кабель питания.
Схема подключения представлена далее.

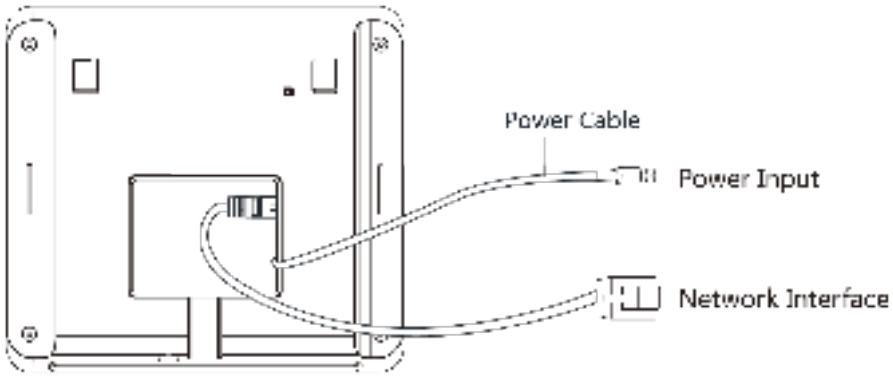


Рисунок 4-3. Подключение с использованием кабеля питания

Английский язык	**Русский язык**
Power Cable	Кабель питания
Power Input	Вход питания
Network Interface	Сетевой интерфейс

Раздел 5 Активация устройства

Перед первым входом в систему вам необходимо активировать устройство. После включения устройства система переключится на страницу активации устройства.
Поддерживается активация через само устройство, активация при помощи ПО SADP и при помощи клиентского ПО.
Значения по умолчанию для устройства следующие:

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

5.1 Активация через устройство

Если устройство еще не активировано, оно отобразит страницу активации после включения питания.
На странице активации устройства создайте пароль и подтвердите его. Нажмите **Activate** («Активировать»), чтобы активировать устройство.

Рисунок 5-1. Страница активации

Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

- После активации необходимо выбрать соответствующий язык.
- После активации устройства, выберите режим работы. Для получения подробной информации обратитесь к разделу ***«Настройка режима работы»***
- После активации, если требуется добавить устройство в клиентское ПО или в другие платформы, следует изменить IP-адрес устройства. Для получения подробной информации обратитесь к соответствующему разделу.
- После активации: если устройством необходимо управлять удаленно через приложение, необходимо сканировать QR-код для скачивания приложения. Для получения подробной информации обратитесь к соответствующему разделу.
- После активации: для управления параметрами устройства необходимо задать роль администратора. Для получения подробной информации обратитесь к разделу «***Добавление администратора»***.

5.2 Активация через веб-интерфейс

Можно активировать устройство через веб-интерфейс.

Шаги

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

Примечание

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

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

Предостережения

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

3. Нажмите **Activate** («Активировать»).
4. Изменение IP-адреса устройства. IP-адрес можно редактировать с помощью инструмента SADP, устройства и клиентского программного обеспечения.

5.3 Активация через ПО SADP

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

Перед началом

- ПО SADP доступно на диске, входящем в комплект или на официальном сайте ***http://www.hikvision.com/en/***, установите ПО SADP согласно инструкции.
- Устройство и ПК, на котором запущено ПО SADP, должны находиться в одной подсети.

Следующие шаги показывают, как активировать устройство и изменить его IP-адрес. Для получения подробной информации о пакетной активации и изменении IP-адресов смотрите ***Руководство пользователя ПО SADP***.

Шаги

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

Предостережения

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

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

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

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

5.4 Активация через клиентское ПО

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

Шаги

> **Примечание**
>
> Устройство должно поддерживать данную функцию.

1. Перейдите на страницу **Device Management** («Управление устройством»).
2. Нажмите в правой части экрана на странице **Device Management** («Управление устройством») и выберите **Device** («Устройство»).
3. Нажмите **Online Device** («Онлайн устройства»), чтобы отобразить область онлайн устройств.
   Искомые онлайн устройства отобразятся в списке.
4. Проверьте состояние устройства (отображено в столбце **Security Level** («Уровень безопасности»)) и выберите неактивное устройство.
5. Нажмите **Activate** («Активировать»), чтобы открыть окно активации.
6. Введите новый пароль в поле **Password** («Пароль») и подтвердите его в поле **Confirm Password** («Подтвердить пароль»).

Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

7. Нажмите **OK** для активации устройства.

Раздел 6 Быстрые операции

6.1 Выбор языка

Можно выбрать язык системы устройства.
После активации устройства можно выбрать язык системы устройства.

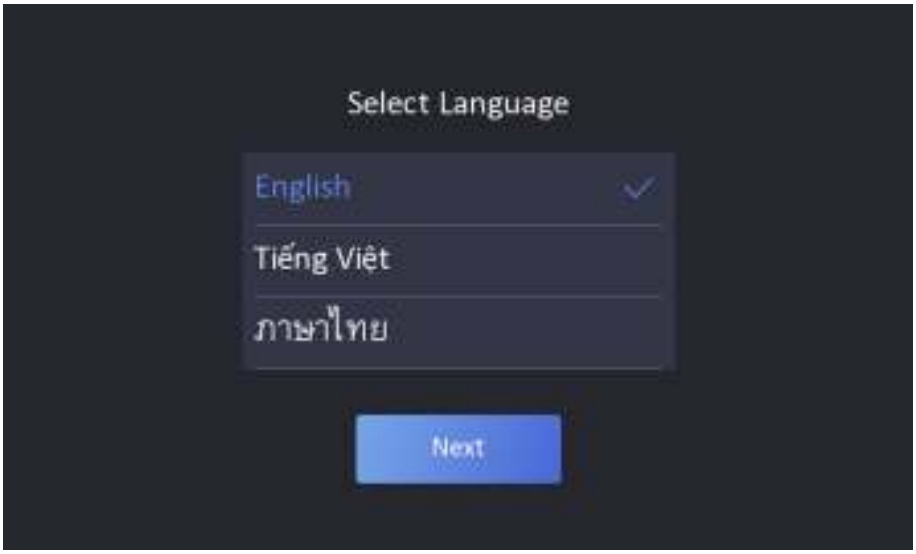


Рисунок 6-1. Выбор языка системы

По умолчанию языком системы выбран английский.

Примечание

После изменения языка системы устройство автоматически перезагрузится.

6.2 Настройка режима работы

После активации устройства выберите необходимый режим работы.

Шаги

1. Из выпадающего списка на стартовой странице выберите режим **Indoor** («Внутри помещения») или **Others** («Другое»).

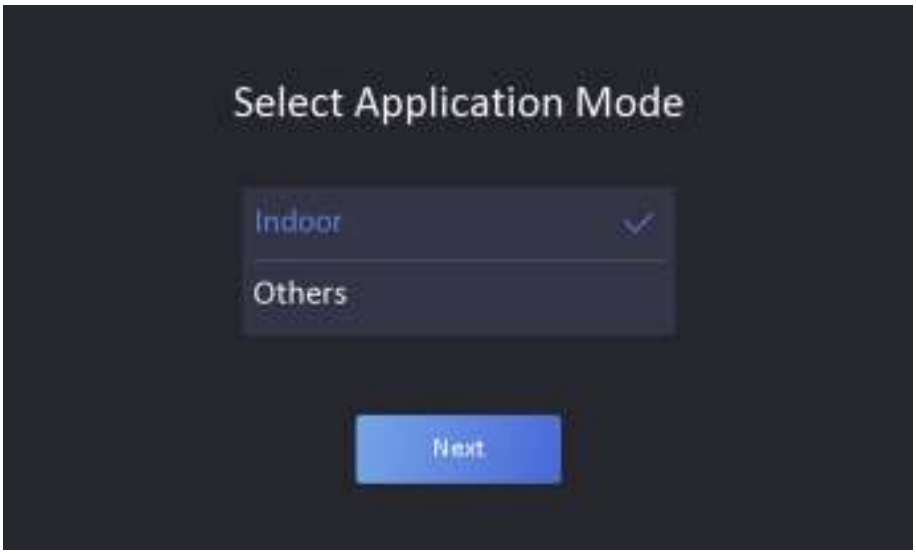


Рисунок 6-2. Стартовая страница

2. Нажмите **OK**, чтобы сохранить настройки.

Примечание

- Настройки также можно изменить в меню ***System Settings*** («Настройки системы»).
- Выберите **Others** («Другое») при установке устройства внутри помещения рядом с окном или если функция распознавания лиц работает неправильно.
- Если не выбрать режим работы и нажать **Next** («Далее»), система выберет режим **Indoor** («Внутри помещения») по умолчанию.
- При активации устройства с помощью других инструментов удаленно система выберет режим **Indoor** («Внутри помещения») по умолчанию.

6.3 Задание роли администратора

После активации устройства можно добавить роль администратора для управления параметрами устройства.

Перед началом

Активируйте устройство и выберите тип применения.

Шаги

1. Опционально. Чтобы пропустить добавление роли администратора, нажмите **Skip** («Пропустить»).
2. Введите имя администратора (необязательно) и нажмите **Next** («Далее»).

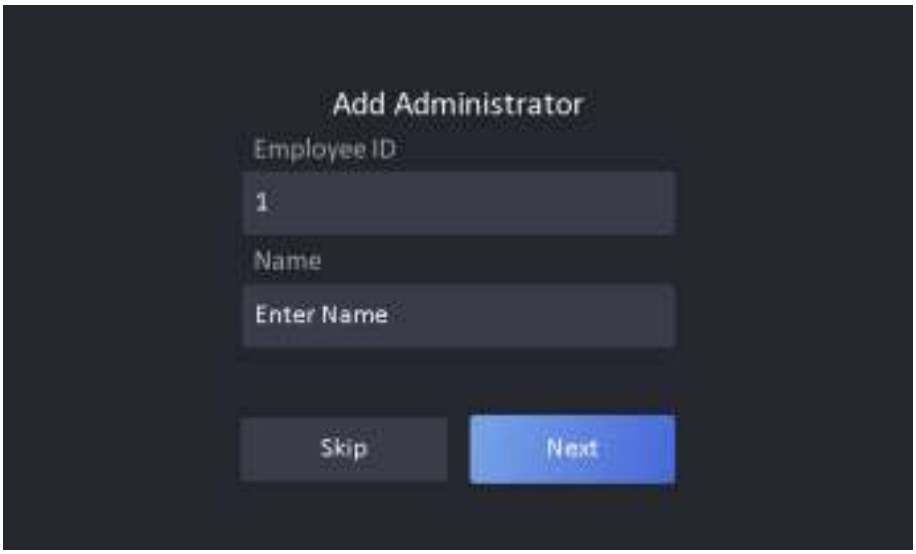


Рисунок 6-3. Страница добавления роли администратора

3. Выберите учетные данные для добавления.

Примечание

Необходимо добавить как минимум одну учетную запись.

– : Посмотрите прямо в камеру. Убедитесь, что лицо находится в рамке распознавания лица. Нажмите для захвата и нажмите для подтверждения.
– : Введите номер карты или предъявите карту в области считывания карты. Нажмите **OK**.

4. Нажмите **OK**.

Вы попадете на страницу аутентификации.

Описание значков состояния

/

Устройство поставлено на охрану/не поставлено на охрану.

/

Hik-Connect включен/отключен.

/ /

Устройство подключено к проводной сети/не подключено/сбой подключения.

/ /

Wi-Fi устройства включен и подключен/не подключен/включен, но не подключен.

Описание горячих клавиш

Примечание

Вы можете настроить сочетания клавиш, отображаемых на экране. Для получения подробной информации обратитесь к разделу ***«Основные настройки»***.

Сканируйте QR-код для аутентификации.

Примечание

QR-код можно получить на терминале для посетителей.

- Введите номер помещения и нажмите **ОК**, чтобы позвонить.
- Нажмите , чтобы позвонить в центр управления.

Примечание

Чтобы выполнить вызов, устройство необходимо добавить в центр управления.

Введите пароль для аутентификации.

Раздел 7 Основные операции

7.1 Вход в систему

Выполните вход в систему, чтобы настроить основные параметры устройства.

7.1.1 Вход в систему в качестве администратора

Если добавлена роль администратора, то только администратор может войти в систему для работы с устройством.

Шаги

1. Нажмите на экран начальной страницы, удерживайте кнопку мыши в течение 3 секунд, затем переместите курсор влево/вправо (в соответствии с инструкциями) и войдите в систему в качестве администратора.

Рисунок 7-1. Вход в систему в качестве администратора

2. Аутентифицируйте лицо администратора, чтобы войти на главную страницу.

Рисунок 7-2. Главная страница

Примечание

Устройство будет заблокировано на 30 минут после 5 неудачных попыток входа.

3. Опционально. Нажмите и введите пароль для активации устройства, чтобы войти в систему.
4. Опционально. Нажмите , чтобы выйти из страницы входа в систему в качестве администратора.

7.1.2 Вход в систему с использованием пароля активации

Прежде чем начать работать с устройством, необходимо выполнить вход в систему. Если вы не настраиваете роль администратора, для входа необходимо выполнить следующие действия.

Шаги

1. Нажмите на экран начальной страницы, удерживайте кнопку мыши в течение 3 секунд, затем переместите курсор влево/вправо (в соответствии с инструкциями) и войдите в систему с использованием пароля активации.
2. Введите пароль для активации устройства в поле **Password** («Пароль»).
3. Нажмите **OK** для перехода на главную страницу.

Примечание

Устройство будет заблокировано на 30 минут после 5 неудачных попыток ввода пароля.

Рисунок 7-3. Главная страница

7.2 Настройки связи

Можно настроить параметры сети, WI-Fi, интерфейса RS-485 на странице настроек связи.

7.2.1 Настройка параметров проводной сети

Можно настроить параметры проводной сети устройства, включая IP-адрес, маску подсети, шлюз и параметры DNS.

Шаги

1. Нажмите на кнопку **Comm**. («Настройки связи») на главной странице, чтобы перейти на страницу **Communication Settings** («Настройки связи»).
2. На странице **Communication Settings** («Настройки связи») нажмите **Wired Network** («Проводная сеть»).

Рисунок 7-4. Настройки проводной сети

3. Установите IP-адрес устройства, маску подсети и шлюз.
   – Включите **DHCP**, и система автоматически назначит IP-адрес, маску подсети и шлюз.
   – При отключении **DHCP** IP-адрес, маску подсети и шлюз необходимо устанавливать вручную.

Примечание

IP-адреса устройства и компьютера должны находиться в одной локальной сети.

4. Настройте параметры DNS. Вы можете включить **Auto Obtain DNS**(«Автоматическое получение DNS»), задать **Preferred DNS Server** («Предпочтительный DNS-сервер») и **Alternate DNS server** («Альтернативный DNS-сервер»).

7.2.2 Настройка параметров Wi-Fi

Можно включить функцию Wi-Fi и настроить соответствующие параметры.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите на кнопку **Comm**. («Настройки связи») на главной странице, чтобы перейти на страницу **Communication Settings** («Настройки связи»).
2. На странице **Communication Settings** («Настройки связи») нажмите **Wi-Fi** («Беспроводная сеть»).

Рисунок 7-5. Настройки Wi-Fi

3. Включите функцию Wi-Fi.
4. Настройте параметры Wi-Fi.
   – Выберите Wi-Fi сеть и введите пароль Wi-Fi для подключения. Нажмите **OK**.

– Если нужный Wi-Fi отсутствует в списке, нажмите **Add Wi-Fi** («Добавить Wi-Fi»). Введите имя и пароль Wi-Fi. Нажмите **OK**.

Примечание

В пароле можно использовать только цифры, буквы и специальные символы.

5. Задайте параметры Wi-Fi.
   – По умолчанию **DHCP** включен. Система автоматически задаст IP-адрес, маску подсети и шлюз.
   – При отключении **DHCP** IP-адрес, маску подсети и шлюз необходимо устанавливать вручную.
6. Нажмите **OK** для сохранения настроек и возврата ко вкладке Wi-Fi.
7. Нажмите для сохранения параметров сети.

7.2.3 Настройка параметров RS-485

Терминал распознавания лиц можно подключить к внешнему контроллеру доступа, модулю безопасности двери или считывателю карт, используя для этого клемму RS-485.

Шаги

1. Нажмите на кнопку **Comm**. («Настройки связи») на главной странице, чтобы перейти на страницу **Communication Settings** («Настройки связи»).
2. На странице **Communication Settings** («Настройки связи») нажмите кнопку **RS-485**, чтобы перейти на вкладку **RS-485.**

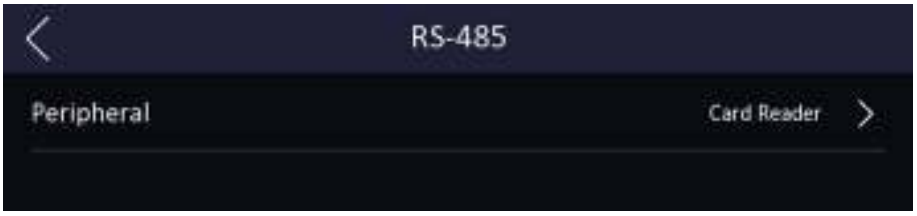


Рисунок 7-6. Настройка параметров RS-485

3. Выберите внешнее устройство согласно фактическим требованиям.

Примечание

При выборе **Access Controller** («Контроллер доступа»): если устройство подключено к терминалу через интерфейс RS-485, настройте адрес RS-485 на значение 2. Если устройство подключено к контроллеру, настройте адрес RS-485 в соответствии с номером двери.

4. Нажмите значок назад в верхнем левом углу. При изменении параметров следует перезагрузить устройство.

7.3 Управление пользователями

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

7.3.1 Добавление администратора

Администратор может войти в аппаратную часть устройства и настроить параметры устройства.

Шаги

1. Нажмите на экран начальной страницы, удерживайте кнопку мыши в течение 3 секунд, затем переместите курсор влево/вправо (в соответствии с инструкциями) и войдите в аппаратную часть устройства.
2. Нажмите User → + («Пользователь → +») для перехода на страницу Add User («Добавить пользователя»).
3. Внесите необходимые изменения в поле **Employee ID** («Идентификатор сотрудника»).

Примечание

- Идентификатор сотрудника может содержать до 32 символов. Он может состоять из букв верхнего/нижнего регистра и цифр.
- Не допускается дублирование идентификаторов сотрудников.

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

Примечание

- В имени пользователя могут быть цифры, буквы верхнего и нижнего регистра и специальные символы.
- Имя пользователя может содержать до 32 символов.

5. Опционально. Для администратора можно добавить изображение лица или карту.

Примечание

- Более подробная информация о добавлении изображения лица представлена в разделе ***«Добавление изображения лица»***.
- Более подробная информация о добавлении карты представлена в разделе ***«Добавление карты»***.

6. Опционально. Можно выбрать тип аутентификации администратора.

Примечание

Более подробная информация о выборе типа аутентификации представлена в разделе ***«Настройка режима аутентификации»***.

7. Включите права администратора.

Включить права администратора

Войдите в систему в качестве администратора. Кроме обычной функции УРВ, пользователь может также перейти на главную страницу для управления устройством после аутентификации прав администратора.

8. Нажмите , чтобы сохранить настройки.

7.3.2 Добавление изображения лица

Добавьте изображение лица пользователя. Изображение лица можно использовать для аутентификации личности.

Шаги

Примечание

Можно добавить до 1000 изображений лиц.

1. Нажмите на экран начальной страницы, удерживайте кнопку мыши в течение 3 секунд, затем переместите курсор влево/вправо (в соответствии с инструкциями) и войдите в аппаратную часть устройства.
2. Нажмите **User → +** («Пользователь → +») для перехода на страницу Add User («Добавить пользователя»).
3. Внесите необходимые изменения в поле **Employee ID** («Идентификатор сотрудника»).

Примечание

- Идентификатор сотрудника может содержать до 32 символов. Он может состоять из букв верхнего/нижнего регистра и цифр.
- Не допускается дублирование идентификаторов сотрудников.

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

Примечание

- В имени пользователя могут быть цифры, буквы верхнего и нижнего регистра и специальные символы.
- Предлагаемое имя пользователя должно содержать не более 32 символов.

5. Нажмите на поле **Face Picture** («Изображение лица»), чтобы перейти на страницу добавления изображения лица.

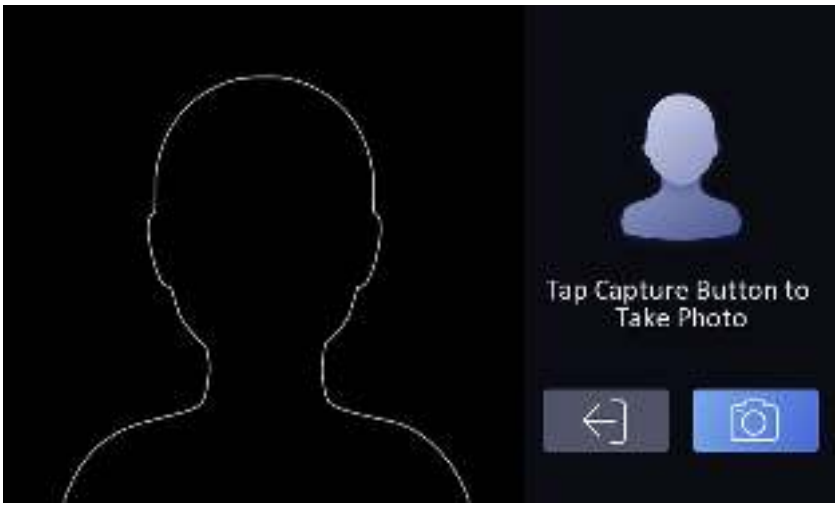


Рисунок 7-7. Добавление изображения лица

6. Посмотрите в камеру.

Примечание

- Перед добавлением изображения лица убедитесь, что положение лица находится в пределах отображенного контура.
- Убедитесь, что качество и размер изображения лица соответствуют требованиям.
- Более подробная информация по добавлению изображений лиц представлена в разделе ***«Рекомендации по сбору/сравнению изображений лиц»***.

После завершения процесса добавления изображения лица в правом верхнем углу страницы появится захваченное изображение.

7. Нажмите **Save** («Сохранить»), чтобы сохранить изображение.
8. Опционально. Нажмите кнопку **Try Again** («Попробовать снова») и измените положение лица, чтобы повторить процедуру добавления.
9. Задайте роль пользователя.

Администратор

Войдите в систему в качестве администратора. Кроме обычной функции УРВ, пользователь может также перейти на главную страницу для управления устройством после аутентификации прав администратора.

Обычный пользователь

Войдите в систему в качестве обычного пользователя. В этом случае пользователь может только пройти аутентификацию и отмечаться о прибытии на начальной странице.

10. Нажмите , чтобы сохранить настройки.

7.3.3 Добавление карты

После добавления карты пользователь сможет проходить аутентификацию с помощью

карты.

Шаги

Примечание

Можно добавить до 1500 карт.

1. Нажмите на экран начальной страницы, удерживайте кнопку мыши в течение 3 секунд, затем переместите курсор влево/вправо (в соответствии с инструкциями) и войдите в аппаратную часть устройства.
2. Нажмите **User** → + («Пользователь → +») для перехода на страницу **Add User** («Добавить пользователя»).
3. Подключите внешний считыватель карт согласно схеме подключения.
4. Внесите необходимые изменения в поле **Employee ID** («Идентификатор сотрудника»).

Примечание

- Идентификатор сотрудника может содержать до 32 символов. Он может состоять из букв верхнего/нижнего регистра и цифр.
- Не допускается дублирование идентификаторов сотрудников.

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

Примечание

- В имени пользователя могут быть цифры, буквы верхнего и нижнего регистра и специальные символы.
- Предлагаемое имя пользователя должно содержать не более 32 символов.

6. Нажмите поле **Card** («Карта») и нажмите **+**.
7. Настройте номер карты:

Вручную введите номер карты. Чтобы узнать номер карты, сканируйте карту в области считывания.

Примечание

- Поле **Card No** («Номер карты») нельзя оставлять незаполненным.
- Номер карты может содержать до 20 символов.
- Запрещается дублирование номера карты.

8. Настройте тип карты.
9. Задайте роль пользователя.

Администратор

Войдите в систему в качестве администратора. Кроме обычной функции УРВ, пользователь может также перейти на главную страницу для управления устройством после аутентификации прав администратора.

Обычный пользователь

Войдите в систему в качестве обычного пользователя. В этом случае пользователь может только пройти аутентификацию и отмечаться о прибытии на начальной странице.

10. Нажмите , чтобы сохранить настройки.

7.3.4 Добавление пароля

После добавления пароля пользователь сможет проходить аутентификацию с помощью пароля.

Шаги

1. Нажмите на экран начальной страницы, удерживайте кнопку мыши в течение 3 секунд, затем переместите курсор влево/вправо (в соответствии с инструкциями) и войдите в аппаратную часть устройства.
2. Нажмите **User** → + («Пользователь → +») для перехода на страницу **Add User** («Добавить пользователя»).
3. Внесите необходимые изменения в поле **Employee ID** («Идентификатор сотрудника»).

Примечание

- Идентификатор сотрудника может содержать до 32 символов. Он может состоять из букв верхнего/нижнего регистра и цифр.
- Не допускается дублирование идентификаторов сотрудников.

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

Примечание

- В имени пользователя могут быть цифры, буквы верхнего и нижнего регистра и специальные символы.
- Предлагаемое имя пользователя должно содержать не более 32 символов.

5. Создайте и подтвердите пароль в поле **Password** («Пароль»).

Примечание

- В пароле можно использовать только цифры.
- В пароле можно использовать от 4 до 8 цифр.

6. Задайте роль пользователя.

Администратор

Войдите в систему в качестве администратора. Кроме обычной функции УРВ, пользователь может также перейти на главную страницу для управления устройством после аутентификации прав администратора.

Обычный пользователь

Войдите в систему в качестве обычного пользователя. В этом случае пользователь может только пройти аутентификацию и отмечаться о прибытии на начальной странице.

7. Нажмите , чтобы сохранить настройки.

7.3.5 Настройка режима аутентификации

После добавления изображения лица пользователя, пароля или других учетных данных, выберите режим аутентификации. Пользователь сможет пройти аутентификацию через выбранный режим аутентификации.

Шаги

1. Нажмите на экран начальной страницы и удерживайте кнопку мыши в течение 3 секунд, затем войдите в аппаратную часть устройства.
2. Нажмите **User → Add User/Edit User → Authentication Mode** («Пользователь → Добавить пользователя/Изменить пользователя → Режим аутентификации»)**.**
3. В качестве режима аутентификации выберите **Device** («Режим устройства») или **Custom** («Пользовательский»).

Режим устройства

Перед установкой режима устройства перейдите на страницу **Access Control Settings** («Настройки контроля доступа»). Для получения подробной информации обратитесь к разделу *«Настройка параметров контроля доступа»*.

Пользовательский

При необходимости допускается сочетание различных режимов аутентификации.

4. Нажмите , чтобы сохранить настройки.

7.3.6 Поиск и изменение параметров пользователя

После добавления пользователя по его учетным данным можно осуществлять поиск и редактировать имеющуюся информацию.

Поиск пользователя

Зайдите на страницу **User Management** (**«**Управление пользователями»), нажмите на экран поиска, чтобы перейти на страницу **Search User** («Поиск пользователя»). Нажмите **Card** («Карта») в левой части страницы и выберите тип поиска из выпадающего списка. Для поиска введите ID сотрудника, номер карты или имя пользователя. Нажмите , чтобы начать поиск.

Изменение параметров пользователя

На странице **User Management** («Управление пользователями») выберите пользователя из списка, чтобы перейти на страницу **Edit User** («Изменить параметры пользователя»). Чтобы отредактировать параметры пользователя, следуйте инструкциям, указанным в разделе ***«Управление пользователями»***. Нажмите , чтобы сохранить настройки.

Примечание

Не допускается редактирование идентификатора сотрудника.

7.4 Управление данными

Данные можно удалять, импортировать и экспортировать.

7.4.1 Удаление данных

Удаление данных пользователя.
На домашней странице нажмите **Data** → **Delete Data** → **User Data** («Данные → Удалить данные → Данные пользователя»). Все данные пользователей, добавленные на устройство, будут удалены.

7.4.2 Импорт данных

Шаги

1. Вставьте USB-накопитель в устройство.
2. На домашней странице нажмите **Data** → **Import Data** («Данные → Импортировать данные»).
3. Нажмите **User Data** («Данные пользователя») или **Face Data** («Данные изображения лица»).
4. Введите созданный пароль для экспорта данных. Если вы не создали пароль при экспорте данных, оставьте пустым поле ввода и сразу нажмите ОК.

Примечание

- При передаче всех данных пользователя с одного устройства (устройство A) на другое (устройство B) необходимо экспортировать данные с устройства A на USB-накопитель, а затем импортировать данные с USB-накопителя на устройство B. В этом случае необходимо импортировать данные пользователя перед импортом фотографии профиля.
- Поддерживаемый формат USB-накопителя – FAT32.
- Импортированные изображения должны быть сохранены в папке корневой директории (enroll_pic), а имя изображения должно соответствовать следующим правилам: № карты_Имя_Отдел_Идентификатор сотрудника_Пол.jpg

- Если в папке enroll_pic нельзя сохранить все импортированные изображения, в корневой директории можно создать другие папки с названиями enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4.
- Идентификатор сотрудника может содержать до 32 символов. Он может состоять из букв верхнего/нижнего регистра и цифр. Он не может быть продублирован или начинаться с цифры 0.
- Ниже приведены следующие требования к изображению лица: лицо видно полностью, взгляд направлен прямо в камеру. При фотографировании запрещено надевать головной убор. Формат фотографии: JPEG или JPG. Разрешение: не менее 640 × 480 пикселей. Размер изображения не должен превышать 2 МБ.

7.4.3 Экспорт данных

Шаги

1. Вставьте USB-накопитель в устройство.
2. На домашней странице нажмите **Data** → **Export Data** («Данные → Экспортировать данные»).
3. Выберите **Event Data** («Данные события»), **User Data** («Данные пользователя») или **Face Data** («Данные изображения лица»).
4. Опционально: создайте пароль для экспорта. При импорте данных на другое устройство, необходимо ввести пароль.

Примечание

- Поддерживаемый формат USB-накопителя – DB.
- Система позволяет использовать USB-накопитель с памятью от 1 до 32 ГБ. Убедитесь в том, что объем свободного места на USB-накопителе составляет более 512 МБ.
- Данные пользователя экспортируются в файл в формате DB, который не подлежит редактированию.

7.5 Идентификация личности

После настройки сети, параметров системы и добавления пользователей вернитесь на начальную страницу для прохождения аутентификации личности. Система выполнит аутентификацию сотрудника/посетителя в соответствии с настроенным режимом работы. Установите личность с помощью сопоставления 1:N.

Сопоставление 1:N

Сопоставьте полученное изображение лица или все изображения лиц, хранящиеся на устройстве.

7.5.1 Аутентификация по лицу

Если выбран режим аутентификации по лицу, сотруднику/посетителю необходимо смотреть в камеру.
Если аутентификация прошла успешно, на экране появится сообщение **Authenticated** («Личность установлена»).

7.5.2 Аутентификация с помощью нескольких типов учетных данных

Перед началом

Перед аутентификацией установите тип аутентификации пользователя. Для получения подробной информации обратитесь к разделу ***Настройка режима аутентификации***.

Шаги

1. Если выбран режим аутентификации **Password and Face** («Пароль и лицо»), выполните аутентификацию по лицу согласно инструкциям в интерфейсе просмотра в режиме реального времени.
2. После завершения проверки учетных данных введите пароль.

Примечание

Более подробная информация об аутентификации лица представлена в разделе «*Рекомендации по сбору/сравнению изображений лиц*».

Если аутентификация прошла успешно, на экране появится сообщение **Authenticated** («Личность установлена»).

7.6 Основные настройки

Можно установить сочетание клавиш, настроить голосовые предупреждения, время, язык и подсветку.
Нажмите на экран начальной страницы, удерживайте кнопку мыши в течение 3 секунд, затем переместите курсор влево/вправо (в соответствии с инструкциями) и войдите в систему в качестве администратора. Нажмите **Basic** («Основные»).

Рисунок 7-8. Страница основных настроек

Настройка горячих клавиш, голосовых предупреждений, времени, номера микрорайона, номера здания и номера помещения.

Горячие клавиши

Выберите сочетание клавиш, отображаемое на странице аутентификации, включая функцию отображения QR-кода, функцию вызова и функцию ввода пароля.

Примечание

Если поддерживается комбинированная аутентификация по лицу и QR-коду, а горячая клавиша отображения QR-кода отключена (на странице аутентификации нет значка QR-кода), для аутентификации можно сканировать QR-код, расположенный в центре страницы.

Настройка голосовых предупреждений

Можно включить/отключить функцию голосовых предупреждений и настроить громкость.

Примечание

Можно установить громкость в диапазоне от 0 до 10.

Настройки времени

Установите часовой пояс, время устройства и летнее время.

Выбор языка

Выберите язык системы. После изменения языка система перезагрузится, чтобы изменения вступили в силу.

Настройки подсветки

Нажмите **White Light** («Подсветка белым светом»), чтобы задать режим подсветки. Можно включить/выключить подсветку, настроить яркость, время начала работы и время окончания работы подсветки.

7.7 Настройка биометрических параметров

Вы можете настроить параметры лица, чтобы улучшить производительность распознавания лиц. Можно настроить режим применения, уровень безопасности антиспуфинга, дальность распознавания лиц, интервал распознавания лиц, уровень WDR, уровень безопасности 1:N, ЭКО-режим и параметры детекции наличия/отсутствия маски.
На начальной странице нажмите на экран в течение 3 секунд и перейдите на главную страницу. Нажмите **Biometric** («Биометрические данные»).

Таблица 7-1. Параметры изображений лиц

Параметр	Описание
Режим применения	Режим **Indoor** («Внутри помещения») или **Others** («Другое») в соответствии со средой установки.
Уровень безопасности антиспуфинга	После включения функции антиспуфинга можно установить надлежащий уровень безопасности при выполнении аутентификации лица в режиме реального времени.
Дальность распознавания	Задание допустимого расстояния между пользователем и камерой при аутентификации.
Интервал распознавания лиц	Временной интервал между двумя циклами распознавания лиц при непрерывной работе. **Примечание** Можно ввести число от 1 до 10.
Широкий динамический диапазон (WDR)	Рекомендуется включить функцию WDR при установке устройства снаружи помещений. Когда на изображении одновременно присутствуют очень светлые и очень темные области, можно включить функцию WDR для уравновешивания уровня яркости всего изображения и обеспечения четкого детализированного изображения.
Уровень безопасности 1:N	Настройте пороговое значение совпадения при аутентификации в режиме сопоставления 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений.
ЭКО-режим	После включения ЭКО-режима устройство будет использовать ИК-подсветку для аутентификации лиц в условиях низкой освещенности или в темноте. Настройте пороговое значение для ЭКО-режима, ЭКО-режим (1:N) и ЭКО-режим (1:1). **Пороговое значение ЭКО-режима**

Параметр	Описание
	Настройте пороговое значение для ЭКО-режима при его включении. Чем больше значение, тем быстрее устройство переключается в ЭКО-режим. **ЭКО-режим (1:1)** Настройте пороговое значение совпадения при аутентификации в ЭКО-режиме 1:1. Чем больше данное значение, тем меньше вероятность ложных совпадений, и тем больше вероятность отклонений ложных совпадений. **ЭКО-режим (1:N)** Настройте пороговое значение совпадения при аутентификации в ЭКО-режиме 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений.
Детекция наличия/отсутствия маски	После включения детекции наличия/отсутствия маски система распознает лицо и наличие/отсутствие маски. Также для детекции лица и наличия/отсутствия маски можно установить уровень безопасности 1: N и настроить соответствующую стратегию. **Напоминание о необходимости ношения маски** Если у сотрудника/посетителя отсутствует маска при аутентификации, устройство выдаст предупреждение, затем дверь откроется. **Предупреждение об обязательном ношении маски** Если у сотрудника/посетителя отсутствует маска при аутентификации, устройство выдаст предупреждение, дверь будет оставаться закрытой.

7.8 Настройка параметров контроля доступа

Можно установить разрешения для управления доступом, например, для настройки режима аутентификации, включения распознавания NFC-карты, настройки дверного контакта и времени открытия двери.
Находясь на главной странице, нажмите кнопку **ACS** («Настройки контроля доступа»), чтобы перейти на соответствующую страницу. Отредактируйте параметры контроля доступа на этой странице.

Рисунок 7-10. Параметры контроля доступа

Ниже представлено следующее описание параметров:

Таблица 7-2. Описание параметров контроля доступа

Параметр	Описание
Режим аутентификации терминала	Выбор режима аутентификации лиц. Режим аутентификации может быть изменен. **Примечание** ● Продукты с биометрическим распознаванием не на 100 % применимы для защиты от подделки биометрических данных. Используйте несколько режимов аутентификации, если требуется более высокий уровень безопасности. ● При использовании нескольких режимов аутентификации перед началом аутентификации лица завершите предыдущие проверки.
Режим аутентификации при помощи считывателя карт	Выберите режим аутентификации при помощи считывателя карт.
Включение распознавания NFC-карты	Включите функцию для аутентификации с использованием NFC-карты.
Дверной контакт	Выберите необходимый режим: **Open (Remain Open)** («Открыть и оставить дверь открытой») или **Close (Remain Closed)** («Закрыть и оставить дверь закрытой»). По умолчанию, установлен режим **Close**

Параметр	Описание
	(Remain Closed) («Закрыть и оставить дверь закрытой»).
Длительность открытого состояния	Установите **Door Unlocking Duration** («Длительность разблокированного состояния двери»). Дверь будет заблокирована, если движение отсутствует в течение установленного времени. Доступный диапазон времени блокировки двери: от 1 до 255 с.
Интервал аутентификации	Установите интервал аутентификации устройства. Доступный диапазон интервала аутентификации: от 0 до 65535.

7.9 Настройки учета рабочего времени (УРВ)

Установите параметры учета рабочего времени. В зависимости от фактической ситуации установите один из следующих режимов учета рабочего времени: регистрация входа на работу, выхода с работы, ухода на перерыв, возвращения с перерыва, сверхурочной работы, раннего ухода с работы

Примечание

Данная функция должна быть использована совместно с функцией учета рабочего времени в клиентском ПО.

7.9.1 Отключение функции учета рабочего времени через устройство

После отключения функции учета рабочего времени устройство не будет отображать статусы посещений на начальной странице.
Нажмите **T&A Status** («Учет рабочего времени») для перехода на соответствующую страницу.

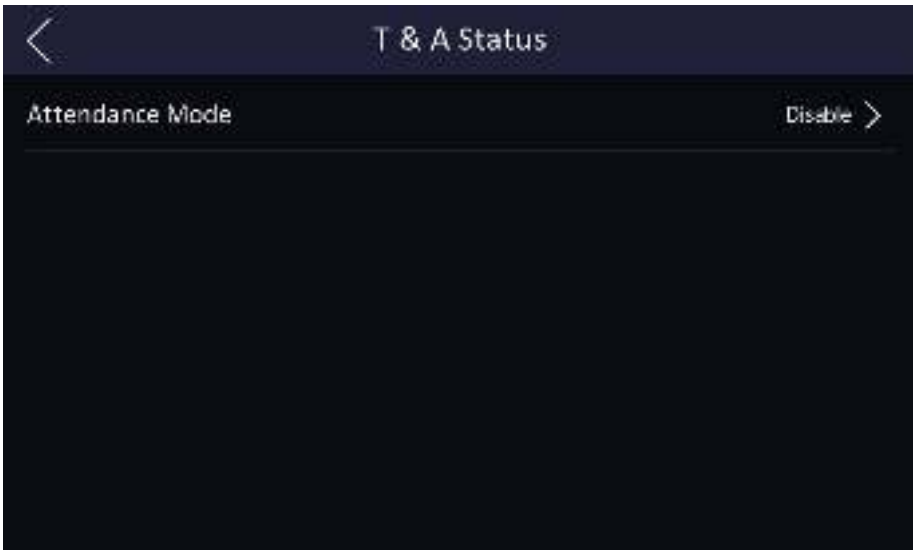


Рисунок 7-11. Отключение режим учета рабочего времени

Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Disable** («Отключить»).
На начальной странице не будут отображаться статусы посещений и интерфейс настроек учета рабочего времени. И система будет следовать правилам посещаемости, настроенным на платформе.

7.9.2 Настройка подсчета результатов посещаемости вручную через устройство

Установите режим подсчета рабочего времени вручную. При сборе статистики посещаемости можно вручную назначить режим подсчета.

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Для получения подробной информации обратитесь к разделу *«Управление пользователями».*

Шаги

1. Нажмите **T&A Status** («Учет рабочего времени») для перехода на соответствующую страницу.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual** («Подсчет вручную»).

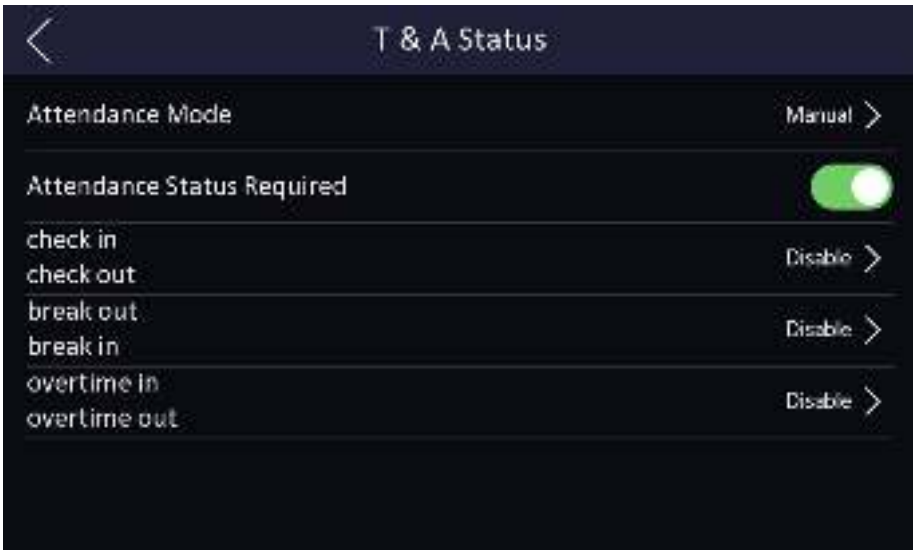


Рисунок 7-12. Режим подсчета рабочего времени вручную

3. Включите функцию **Attendance Status** («Учет рабочего времени»).

Результат

При аутентификации необходимо вручную выбрать статус посещения.

Примечание

Если не выбрать статус, аутентификация будет неудачной.

7.9.3 Настройка параметров автоматического учета рабочего времени через устройство

Установите режим автоматического учета рабочего времени, чтобы настроить статусы посещений и доступное расписание. Система автоматически изменит статус посещений в соответствии с настроенными параметрами.

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Для получения подробной информации обратитесь к разделу «*Управление пользователями».*

Шаги

1. Нажмите **T&A Status** («Учет рабочего времени») для перехода на соответствующую страницу.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Auto** («Автоматич.»).

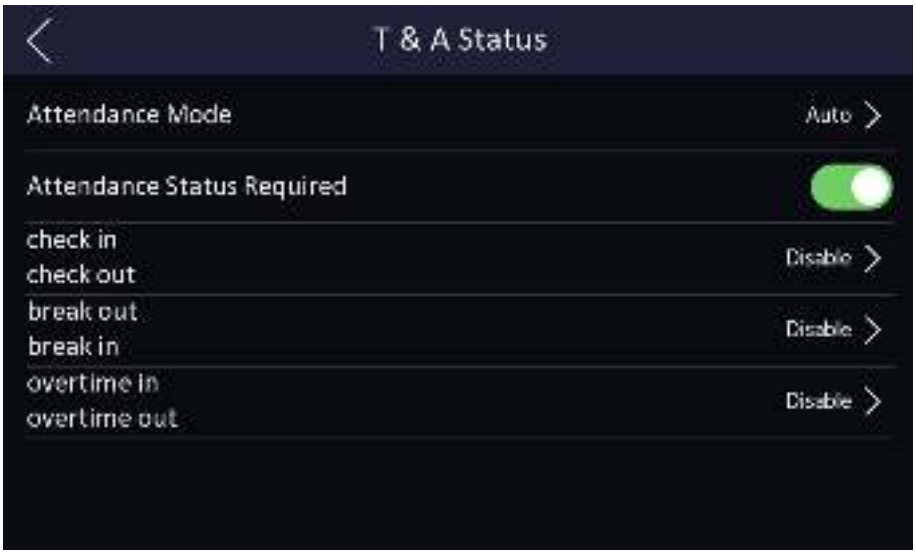


Рисунок 7-13. Режим автоматического учета рабочего времени

3. Выберите статус и расписание посещений.
   1) Выберите регистрацию **Check In** («Вход на работу»), **Check Out** («Выход с работы»), **Break Out** («Уход на перерыв»), **Break In** («Возвращение с перерыва»), **Overtime In** («Сверхурочная работы»), **Overtime Out** («Ранний уход с работы»).
   2) Нажмите на **Schedule** («Расписание»).
   3) Выберите **Monday** («Понедельник»), **Tuesday** («Вторник»), **Wednesday** («Среда»), **Thursday** («Четверг»), **Friday** («Пятница»), **Saturday** («Суббота») или **Sunday** («Воскресенье»).
   4) Нажмите на выбранную дату и установите время начала выбранного статуса посещений.
   5) Нажмите **Confirm** («Подтвердить»).
   6) При необходимости повторно выполните инструкции, изложенные выше.

Примечание

Статус посещений будет действителен в течение настроенного расписания.

Результат

При прохождении аутентификации на начальной странице будет отображаться статус посещений в соответствии с настроенным расписанием.

Пример

Если установить **Break Out Schedule** («Время ухода на перерыв») в 11:00 в понедельник и **Break In Schedule** («Время возвращения с перерыва») в 12:00 в понедельник, при аутентификации пользователя в понедельник с 11:00 до 12:00 будет отмечен «уход на перерыв».

6.11.4 Настройка параметров автоматического УРВ и УРВ вручную через устройство

В меню **Attendance Mode** («Учет рабочего времени») выберите **Manual and Auto** («Подсчет автоматически и вручную»). Система автоматически изменит статус посещений в соответствии с настроенными параметрами. При этом можно вручную изменить статус посещения при аутентификации.

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Для получения подробной информации обратитесь к разделу *Управление пользователями.*

Шаги

1. Нажмите **T&A Status** («Учет рабочего времени») для перехода на соответствующую страницу.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual and Auto** («Подсчет автоматически и вручную»).

Рисунок 7-14. Подсчет результатов посещаемости автоматически и вручную

3. Выберите статус и расписание посещений.
   1) Выберите регистрацию **Check In** («Вход на работу»), **Check Out** («Выход с работы»), **Break Out** («Уход на перерыв»), **Break In** («Возвращение с перерыва»), **Overtime In** («Сверхурочная работа»), **Overtime Out** («Ранний уход с работы»).
   2) Нажмите на **Schedule** («Расписание»).
   3) Выберите **Monday** («Понедельник»), **Tuesday** («Вторник»), **Wednesday** («Среда»), **Thursday** («Четверг»), **Friday** («Пятница»), **Saturday** («Суббота») или **Sunday** («Воскресенье»).
   4) Нажмите на выбранную дату и установите время начала выбранного статуса посещений.
   5) Нажмите **Confirm** («Подтвердить»).
   6) При необходимости повторно выполните инструкции, изложенные выше.

Примечание

Статус посещений будет действителен в течение настроенного расписания.

Результат

Аутентификация на начальной странице. Если не выбрать статус вручную, при аутентификации будет отображаться статус посещений в соответствии с настроенным расписанием. Нажмите **Select Status** («Выбрать статус») и выберите необходимый статус посещений. В этом случае при аутентификации будет отображаться выбранный статус посещений.

Пример

Если установить **Break Out Schedule** («Время ухода на перерыв») в 11:00 в понедельник и **Break In Schedule** («Время возвращения с перерыва») в 12:00 в понедельник, при аутентификации пользователя в понедельник с 11:00 до 12:00 будет отмечен «уход на перерыв».

7.10 Обслуживание системы

Можно просмотреть системную информацию и емкость. Кроме того, можно обновить устройство, восстановить заводские настройки, восстановить настройки по умолчанию и перезагрузить устройство.
Нажмите на экран начальной страницы, удерживайте кнопку мыши в течение 3 секунд, затем переместите курсор влево/вправо (в соответствии с инструкциями) и войдите в систему. Нажмите **Maint.** («Обслуживание»).
Чтобы посмотреть версию устройства, нажмите **?** в правом верхнем углу страницы и введите пароль.

Рисунок 7-15. Страница обслуживания

Системная информация

Можно просмотреть модель устройства, серийный номер, версии, адрес, производственные данные, QR-код и лицензию с открытым исходным кодом.

Примечание

Страница может отличаться в зависимости от модели устройства. Подробная информация представлена на фактической странице интерфейса.

Емкость

Можно просмотреть количество пользователей, изображений лиц, карт и событий.

Обновление устройства

Вставьте USB-накопитель в USB-интерфейс устройства. Нажмите **Upgrade** («Обновить»), и устройство прочитает файл *digicap.dav* с USB-накопителя, чтобы начать обновление.

Отмена привязки к учетной записи приложения

После отмены привязки к учетной записи приложения управление устройством через приложение невозможно.

Восстановление настроек по умолчанию

Все параметры, за исключением настроек связи и информации о пользователе, импортированной удаленно, будут восстановлены до настроек по умолчанию. Система перезагрузится, чтобы изменения вступили в силу.

Восстановление настроек изготовителя

Все параметры будут сброшены до заводских настроек. Система перезагрузится, чтобы изменения вступили в силу.

Перезагрузка

Перезагрузите устройство.

Глава 8 Работа через веб-интерфейс

8.1 Вход в систему

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

Примечание

Устройство должно быть активировано. Более подробная информация представлена в разделе ***«Активация»***.

Вход в систему через веб-интерфейс

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

Примечание

Убедитесь, что IP-адрес начинается с https:.

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

Вход в систему через удаленную конфигурацию клиентского программного обеспечения

Загрузите и откройте клиентское программное обеспечение. После добавления устройства нажмите , чтобы перейти на страницу конфигурации.

8.2 Просмотр в режиме реального времени

Можно просматривать видео в режиме реального времени.
После входа в систему вы попадете на страницу просмотра в режиме реального времени. Можно выполнять просмотр в режиме реального времени, захват, запись видео и другие операции.

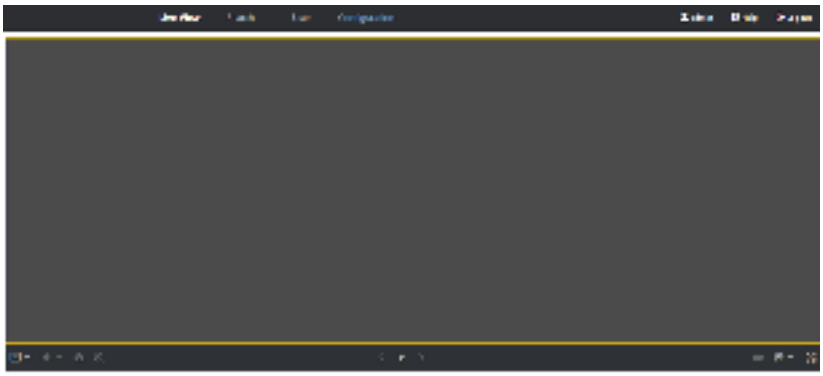


Рисунок 8-1. Страница просмотра в режиме реального времени

Описание функций

При запуске просмотра в режиме реального времени необходимо выбрать размер изображения.

При запуске просмотра в режиме реального времени необходимо настроить громкость.

Примечание

При настройке громкости во время двусторонней аудиосвязи можно услышать эхо.

При запуске просмотра в режиме реального времени можно выполнить захват изображения.

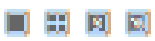
Зарезервированная функция. Данная функция позволяет увеличить любую область при просмотре в режиме реального времени.

Разблокировка подключенной двери.

Начало или остановка просмотра в режиме реального времени.

Начало или остановка записи видео.

При запуске просмотра в режиме реального времени можно выбрать тип потока. Можно выбрать основной поток и дополнительный поток.



При запуске просмотра в режиме реального времени можно выбрать тип разделения окна.

Полноэкранный просмотр.

8.3 Управление сотрудниками/посетителями

Можно добавить информацию о сотруднике/посетителе, в том числе основную информацию, карту, режим аутентификации и изображение.
Нажмите **OK** для сохранения сотрудника/посетителя.

Добавление основной информации

Нажмите **User** → **Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника/посетителя.
Добавьте основную информацию о сотруднике/посетителе, включая идентификатор, Ф. И. О., пол, уровень пользователя, номер этажа и номер помещения.
Нажмите **OK** для сохранения настроек.

Добавление карты

Нажмите **User** → **Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника/посетителя.
Нажмите **Add Card** («Добавить карту») и введите номер карты.
Нажмите **OK** для сохранения настроек.

Добавление изображения лица

Нажмите **User** → **Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника/посетителя.
Нажмите кнопку **+**, расположенную справа, чтобы загрузить изображение лица с локального ПК.

Примечание

Изображение формате должно быть JPG, JPEG или PNG. Размер не должен превышать 2 КБ.

Нажмите **OK** для сохранения настроек.

Установить время разрешения

Нажмите **User** → **Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника/посетителя.
Установите **Start Time** («Время начала») и **End Time** («Время окончания»).
Нажмите **OK** для сохранения настроек.

Настройка контроля доступа

Нажмите **User** → **Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника/посетителя.
В поле **Access Control** («Контроль доступа») выберите **Adminstrator** («Администратор») и добавленный сотрудник/посетитель может войти в систему посредством аутентификации по

лицу.
Нажмите **OK** для сохранения настроек.

Добавить режим аутентификации

Нажмите **User** → **Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника/посетителя.
Выберите тип аутентификации.
Нажмите **OK** для сохранения настроек.

8.4 Поиск события

Нажмите **Search** («Поиск») для перехода на соответствующую страницу.

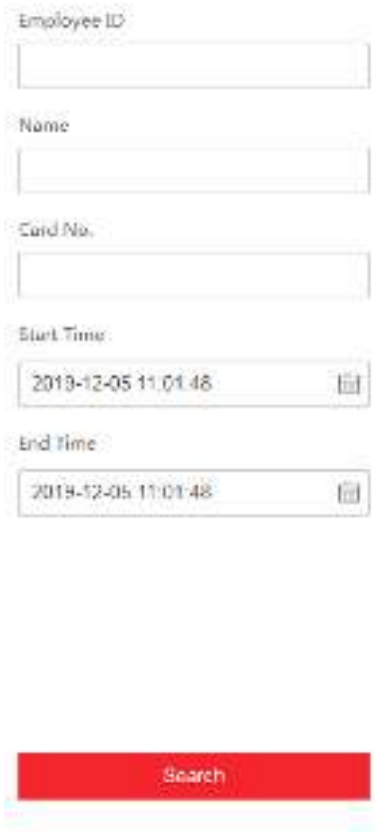


Рисунок 8-2. Страница поиска

Введите условия поиска, включая идентификатор сотрудника/посетителя, Ф. И. О., номер карты, время начала и время окончания доступа и нажмите **Search** («Поиск»).
После этого на панели справа появятся результаты поиска.

8.5 Настройка

8.5.1 Настройка локальных параметров

Установите параметры просмотра в режиме реального времени, путь сохранения файла записи и путь сохранения захваченных изображений.

Настройка параметров просмотра в режиме реального времени

Нажмите **Configuration** → **Local** («Настройки → Локальные») для перехода на соответствующую страницу. Настройте тип потока, параметры воспроизведения, автоматический запуск просмотра в режиме реального времени, формат изображения и нажмите **Save** («Сохранить»).

Настройка пути сохранения файлов записи

Нажмите **Configuration** → **Local** («Настройки → Локальные») для перехода на соответствующую страницу. Выберите размер файла записи, путь для сохранения на локальном компьютере и нажмите **Save** («Сохранить»).
Также можно нажать **Open** («Открыть»), чтобы открыть папку с файлами и просмотреть подробную информацию.

Настройка пути сохранения захваченных изображений

Нажмите **Configuration** → **Local** («Настройки → Локальные») для перехода на соответствующую страницу. Выберите путь для сохранения на локальном компьютере и нажмите **Save** («Сохранить»).
Также можно нажать **Open** («Открыть»), чтобы открыть папку с файлами и просмотреть подробную информацию.

8.5.2 Просмотр информации об устройстве

Просмотр названия устройства, языка, модели, серийного номера, QR-кода, версии, емкости устройства и т. д.
Нажмите **Configuration** → **System** → **System Settings** → **Basic Information** («Настройки → Система → Настройка системы → Основная информация»), чтобы перейти на соответствующую страницу.
Здесь можно посмотреть название устройства, язык, модель, серийный номер, QR-код, версию, емкость устройства и т. д.

8.5.3 Настройка времени

Установите часовой пояс, режим синхронизации и время устройства.
Нажмите **Configuration → System → System Settings → Time Settings** («Настройки → Система → Настройки системы → Настройки времени»).

Рисунок 8-3. Настройка времени

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

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

NTP

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

Вручную

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

8.5.4 Настройка перехода на летнее время (DST)

Шаги

1. Нажмите **Configuration** → **System** → **System Settings** → **DST** («Настройки → Система → Настройки системы → DST»).

Рисунок 8-4. Страница DST

2. Нажмите **Enable DST** («Включить DST»).
3. Установите время начала и окончания DST, а также смещение DST.
4. Нажмите **Save** («Сохранить») для сохранения настроек.

8.5.5 Просмотр лицензии на ПО с открытым исходным кодом

Перейдите в меню **Configuration** → **System** → **System Settings** → **About Device** («Настройки → Система → Настройки системы → Об устройстве») и нажмите **View Licenses** («Просмотр лицензии»), чтобы просмотреть лицензию устройства.

8.5.6 Обновление и техническое обслуживание

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

Перезагрузка устройства

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

Рисунок 8-5. Страница обновления и обслуживания

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

Восстановление параметров

Нажмите **Configuration** → **System** > **Maintenance** → **Upgrade & Maintenance** («Настройки → Система → Обслуживание→ Обновление и обслуживание»).

Сбросить все

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

Восстановление настроек по умолчанию

Настройки устройства будут восстановлены до настроек по умолчанию, за исключением IP-адреса устройства и информации о пользователе.

Отмена привязки к учетной записи приложения

Отключите учетную запись Hik-Connect от платформы.

Параметры импорта и экспорта

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

Экспорт

Нажмите **Export** («Экспорт»), чтобы экспортировать журналы или параметры устройства.

Примечание

Можно импортировать экспортированные параметры устройства на другое устройство.

Импорт

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

Обновление

Нажмите **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** («Настройки → Система → Обслуживание→ Обновление и обслуживание»).
Выберите тип обновления из выпадающего списка. Нажмите и выберите файл обновления с локального ПК. Нажмите **Upgrade** («Обновить») для начала обновления.

Примечание

Не выключайте устройство во время обновления.

8.5.7 Запрос журнала

Можно искать и просматривать журналы устройства.
Перейдите в меню **Configuration** → **System** → **Maintenance** → **Log Query** («Настройки → Система → Обслуживание → Запрос журнала»).
Установите основной и второстепенный тип журнала. Установите время начала и время окончания поиска и нажмите **Search** («Поиск»).
Результаты будут отображаться ниже, включая номер, время, основной тип, второстепенный тип, номер канала, информацию о локальном/удаленном пользователе, IP-адрес удаленного хоста и т. д.

8.5.8 Настройка режима безопасности

Настройте режим безопасности для входа в клиентское ПО.
На странице управления устройствами нажмите **Configuration → System → Security → Security Service** («Настройки → Система → Безопасность → Служба безопасности»).
Из всплывающего списка выберите режим безопасности и нажмите **Save** («Сохранить»).

Режим безопасности

Высокий уровень безопасности при проверке информации пользователя при входе в клиентское программное обеспечение.

Режим совместимости

Режим проверки информации пользователя при входе в систему совместим со старой версией клиентского программного обеспечения.

Включить SSH

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

Включить HTTP

Чтобы повысить уровень сетевой безопасности при посещении веб-сайтов, можно включить HTTP. Это обеспечит более безопасную зашифрованную среду сетевой связи. После включения HTTP связь должна быть аутентифицирована с помощью идентификатора и пароля шифрования, который сохраняется.

8.5.9 Управление сертификатами

Помогает управлять сертификатами сервера/клиента и сертификатом CA.

Примечание

Данная функция поддерживается только у определенных моделей устройств.

Создать и установить самозаверенный сертификат

Шаги

1. Перейдите в меню **Configuration → System → Security → Certificate Management** («Настройки → Система → Безопасность → Управление сертификатами»).
2. В области **Certificate Files** («Файлы сертификатов») выберите тип сертификата из выпадающего списка.
3. Нажмите **Create** («Создать»).
4. Введите информацию о сертификате.
5. Нажмите **OK**, чтобы сохранить и установить сертификат.
   Созданный сертификат отображается в области **Certificate Details** («Сведения о сертификате»).
   Сертификат будет сохранен автоматически.
6. Загрузите сертификат и сохраните его в запрашиваемом файле на локальном компьютере.
7. Отправьте запрашиваемый файл в центр сертификации на подпись.
8. Импортируйте подписанный сертификат.
   1) Выберите тип сертификата в области **Import Passwords** («Импорт паролей»), выберите сертификат на локальном компьютере и нажмите **Install** («Установить»).
   2) Выберите тип сертификата в области **Import Communication Certificate** («Импорт сертификата связи»), затем выберите сертификат на локальном компьютере и нажмите **Install** («Установить»).

Установка другого авторизованного сертификата

Если есть авторизованный сертификат (не созданный устройством), можно импортировать

его напрямую на устройство.

Шаги

1. Перейдите в меню **Configuration → System → Security → Certificate Management** («Настройки → Система → Безопасность → Управление сертификатами»).
2. В областях **Import Passwords** («Импорт паролей») и **Import Communication Certificate** («Импорт сертификата связи») выберите тип сертификата и загрузите сертификат.
3. Нажмите **Install** («Установить»).

Установка сертификата CA

Перед началом

Заранее подготовьте сертификат CA.

Шаги

1. Перейдите в меню **Configuration → System → Security → Certificate Management** («Настройки → Система → Безопасность → Управление сертификатами»).
2. Создайте идентификатор в области **Import CA Certificate** («Импорт сертификата CA»).

> **Примечание**
>
> Идентификатор сертификата не может совпадать с идентификатором уже существующих сертификатов.

3. Загрузите файл сертификата с локального ПК.
4. Нажмите **Install** («Установить»).

8.5.10 Изменение пароля администратора

Шаги

1. Нажмите **Configuration** → **User Management** («Настройки → Управление пользователями»).
2. Нажмите .
3. Введите старый пароль и создайте новый пароль.
4. Подтвердите новый пароль.
5. Нажмите **OK**.

Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

8.5.11 Просмотр информации о постановке/снятии с охраны

Просмотр информации о постановке устройства на охрану и IP-адреса постановки на охрану.
Нажмите **Configuration** → **Arming/Disarming Information** («Настройки → Информация о постановке на охрану/снятии с охраны»).
Можно просмотреть информацию о постановке на охрану/снятии с охраны. Для обновления нажмите кнопку **Refresh** («Обновить»).

8.5.12 Настройка сетевых параметров

Установите параметры TCP/IP и порта.

Настройка основных сетевых параметров

Нажмите **Configuration** → **Network** → **Basic Settings** → **TCP/IP** («Настройки → Сеть → Основные настройки → TCP/IP»).

Рисунок 8-6. Страница настройки TCP/IP

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

DHCP

При отключении этой функции необходимо настроить IPv4-адрес, IPv4-маску подсети, IPv4-шлюз по умолчанию, MTU и порт устройства.
При включении этой функции система автоматически задаст IPv4-адрес, IPv4-маску подсети и IPv4-шлюз.

Тип NIC

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

DNS-сервер

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

Настройка параметров порта

Установите параметры HTTP, RTSP, HTTPS, сервера и порта WebSocket.
Нажмите **Configuration** → **Network** → **Basic Settings** → **Port** («Настройки → Сеть → Основные настройки → Порт»).

HTTP

Через этот порт веб-интерфейс получает доступ к устройству. Например, если **HTTP Port** («Порт HTTP») изменен на 81, необходимо ввести ***http://192.168.1.64:81*** для входа в веб-интерфейс.

RTSP

Обозначает порт потокового протокола реального времени.

HTTPS

Задайте HTTPS для доступа к браузеру. Для доступа необходим сертификат.

Сервер

Через этот порт клиент добавляет устройство.

Настройка параметров Wi-Fi

Задайте параметры Wi-Fi для беспроводного подключения устройства.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **Configuration** → **Network** → **Basic Settings** → **Wi-Fi** («Настройки → Сеть → Основные настройки → Wi-Fi»).

Рисунок 8-7. Страница настроек Wi-Fi

2. Нажмите **Wi-Fi** («Wi-Fi»).
3. Выберите Wi-Fi.
   – Нажмите и введите пароль Wi-Fi для подключения.
   – Нажмите **Add** («Добавить») и введите имя, пароль и тип шифрования Wi-Fi. Нажмите **Connect** («Подключить»). Когда Wi-Fi подключен, нажмите **OK**.
4. Опционально. Настройте параметры WLAN.
   1) Нажмите **TCP/IP Settings** («Настройка параметров TCP/IP»).
   2) Установите IP-адрес, маску подсети и шлюз по умолчанию. Также можно нажать **Enable DHCP** («Включить DHCP»), и система автоматически задаст IPv4-адрес, IPv4-маску подсети и IPv4-шлюз.
5. Нажмите **Save** («Сохранить»).

Настройка способа уведомления

Настройте центральную группу для загрузки журнала по протоколу ISUP.
Нажмите **Configuration** → **Network** → **Basic Settings** → **Report Strategy** («Настройки → Сеть → Основные настройки → Способ уведомления»).
Настройте центральную группу для передачи журналов по протоколу ISUP. Нажмите **Save** («Сохранить») для сохранения настроек.

Центральная группа

Выберите центральную группу из выпадающего списка.

Основной канал

Устройство будет связываться с центром через основной канал.

Примечание

N1 относится к проводной сети.

Настройка параметров ISUP

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **Configuration** → **Network** → **Advanced Settings** → **Platform** («Настройки → Сеть → Расширенные настройки → Платформа»).
2. Из всплывающего списка выберите **ISUP** в меню **Platform Access Mode** («Режим платформы доступа»).
3. Нажмите **Enable** («Включить»).
4. Установите версию ISUP, адрес сервера, идентификатор устройства и статус ISUP.

Примечание

Если выбрана версия 5.0, необходимо также установить ключ ISUP.

5. Нажмите **Save** («Сохранить»).

Платформа доступа

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите **Configuration** → **Network** → **Advanced** → **Platform Access** («Настройки → Сеть → Расширенные настройки → Платформа доступа») для перехода на страницу настроек.
2. Нажмите **Enable** («Включить») для включения функции.
3. Выберите **Platform Access Mode** («Режим платформы доступа»).

Примечание

Hik-Connect является приложением для мобильных устройств. С помощью приложения Вы можете просматривать видео в реальном времени с устройства, получать тревожные уведомления и т. д.

4. Создайте **Stream Encryption/Encryption** Key («Шифрование потока/ключ шифрования») для устройства.

Примечание

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

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

Настройка прослушивания HTTP

Устройство может отправлять информацию о тревоге по IP-адресу назначения или имени хоста по протоколу HTTP.

Перед началом

Для получения информации о тревоге IP-адрес назначения или имя хоста должны поддерживать протокол HTTP.

Примечание

Устройство должно поддерживать данную функцию.

Шаги

1. Нажмите **Configuration** → **Network** → **Advanced** → **HTTP Listening** («Настройки → Сеть → Расширенные настройки → Прослушивание HTTP»).
2. Настраивайте IP-адрес назначения или имя хоста, URL-адрес и порт.
3. Опционально. Можно нажать **Test** («Тестировать»), чтобы проверить правильность введенного IP-адреса или имени хоста.
4. Опционально. Нажмите **Default** («По умолчанию»), чтобы сбросить IP-адрес назначения или имя хоста.
5. Нажмите **Save** («Сохранить»).

8.5.13 Настройка параметров видео и аудио

Настройте качество изображения, разрешение и громкость устройства.

Настройка параметров видео

Нажмите **Configuration** → **Video/Audio** → **Video** («Настройки → Видео/Аудио → Видео»).

Рисунок 8-8. Страница настройки параметров видео

Настройте тип потока, тип видео, тип битрейта, частоту кадров, макс. битрейт, параметры кодирования видео.

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

Настройка параметров аудио

Нажмите **Configuration** → **Video/Audio** → **Audio** («Настройки → Видео/Аудио → Аудио»).
Передвигайте бегунок для настройки выходной громкости устройства.
Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

8.5.14 Настройка голосовых предупреждений

Настройте голосовые предупреждения для случаев успешной аутентификации и сбоев аутентификации.

Шаги

1. Нажмите **Configuration** → **Video/Audio** → **Audio Prompt** («Настройки → Видео/Аудио → Голосовые предупреждения»).

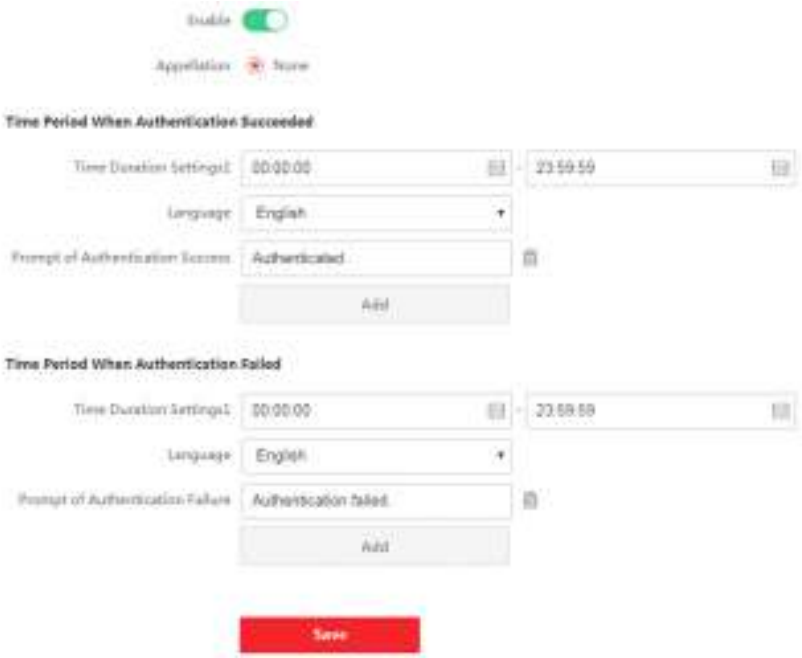


Рисунок 8-9. Настраиваемые голосовые предупреждения

2. Установите наименование.
3. Включите функцию.
4. Установите продолжительность предупреждения при успешной аутентификации.
   1) Нажмите **Add** («Добавить»).
   2) Установите продолжительность и язык.

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

   3) Введите аудиосообщение.

4) Опционально. Повторите шаги от 1 до 3.
5) Опционально. Нажмите , чтобы сбросить настроенную продолжительность предупреждения.

5. Установите продолжительность предупреждения при сбое аутентификации.
   1) Нажмите **Add** («Добавить»).
   2) Установите продолжительность и язык.

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

   3) Введите аудиосообщение.
   4) Опционально. Повторите шаги от 1 до 3.
   5) Опционально. Нажмите , чтобы сбросить настроенную продолжительность предупреждения.
6. Нажмите **Save** («Сохранить») для сохранения настроек.

8.5.15 Настройка параметров изображения

Установите стандарт видео, WDR, яркость, контраст, насыщенность и резкость.

Шаги

1. Нажмите **Configuration** → **Image Adjustment** («Настройки → Настройка изображения»).

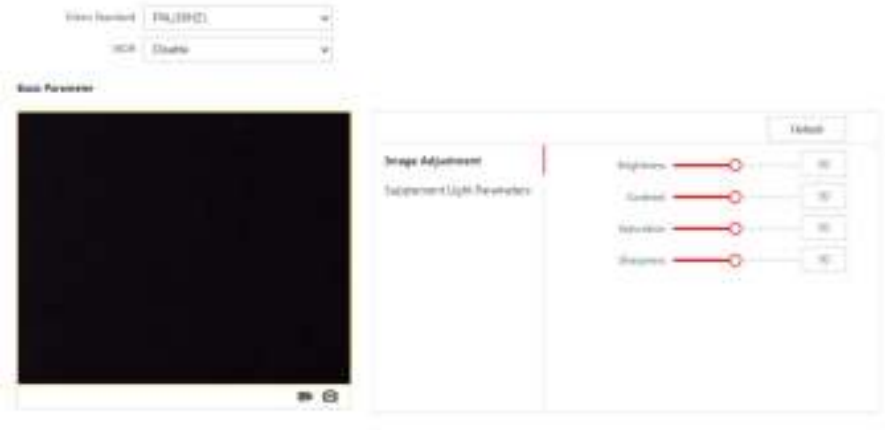


Рисунок 8-10. Страница настройки изображения

2. Настройте параметры изображения.

Стандарт видео

Установите частоту кадров видео при удаленном просмотре в режиме реального времени. После изменения стандарта необходимо перезагрузить устройство, чтобы изменения вступили в силу.

PAL

25 кадров в секунду. Подходит для материкового Китая, Гонконга (Китая), стран Ближнего Востока, стран Европы и др.

NTSC

30 кадров в секунду. Подходит для США, Канады, Японии, Тайваня (Китай), Кореи, Филиппин и др.

WDR

Включите/выключите WDR.
Когда на изображении одновременно присутствуют очень светлые и очень темные области, можно включить функцию WDR для уравновешивания уровня яркости всего изображения и обеспечения четкого детализированного изображения.

Яркость/Контрастность/Насыщенность/Резкость

Перемещайте бегунок или введите значение, чтобы настроить яркость, контрастность, насыщенность и резкость видео при просмотре в режиме реального времени.

Начало/остановка записи видео.

Захват изображения.

3. Нажмите **Default** («По умолчанию») для сброса всех параметров до значений по умолчанию.

8.5.16 Настройка яркости подсветки

Настройте яркость подсветки.

Шаги

1. Нажмите **Configuration** → **Image** → **Supplement Light Parameters** («Настройки → Изображение → Параметры подсветки»).

Рисунок 8-11. Страница настроек параметров подсветки

2. Выберите тип и режим подсветки из выпадающего списка параметров. При выборе параметра **ON** («Вкл.»), можно задать значения яркости.

8.5.17 Настройка учета времени (УРВ)

Если необходимо отслеживать и контролировать начало и окончание работы сотрудников, а также их рабочего времени и опозданий, ранних уходов с работы, времени перерывов и прогулов, можно добавить сотрудника в группу УРВ и назначить расписание смены (правило для посещения, определяющее повтор расписания, тип смены, настройки перерывов и правило шифрования карты) для группы УРВ, чтобы определить параметры УРВ для сотрудников группы.

Отключение функции учета рабочего времени через веб-интерфейс

После отключения функции учета рабочего времени устройство не будет отображать статусы посещений на начальной странице.

Шаги

1. Нажмите **Configuration** → **Attendance** («Настройки → УРВ») для перехода на страницу настроек.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Disable** («Отключить»).

Результат

На начальной странице не будут отображаться статусы посещений и интерфейс настроек учета рабочего времени. И система будет следовать правилам посещаемости, настроенным на платформе.

Настройки времени

Шаги

1. Нажмите **Configuration → Time Settings** («Настройки → Настройки времени») для перехода на соответствующую страницу.
2. Выберите **Status Type** («Тип состояния»).
3. Опционально. Нажмите **Schedule Name** («Название расписания») для изменения названия.
4. Перетащите курсор мыши, чтобы установить расписание.

Примечание

Установите расписание с понедельника по воскресенье в соответствии с необходимостью.

5. Опционально. Выберите шкалу и нажмите **Delete** («Удалить»). Также можно нажать **Delete All** («Удалить все»), чтобы удалить все настройки.
6. Нажмите **Save** («Сохранить»).

Настройка параметров учета рабочего времени вручную через веб-интерфейс

Установите режим УРВ вручную. При сборе статистики посещаемости можно вручную назначить режим подсчета.

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Для получения подробной информации обратитесь к разделу *«Управление пользователями».*

Шаги

1. Нажмите **Configuration** → **Attendance** («Настройки → УРВ») для перехода на страницу настроек.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual** («Подсчет вручную»).
3. Нажмите **Attendance Status Required** («Обязательный статус УРВ») и установите продолжительность статуса УРВ.
4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

5. Опционально. Выберите статус и при необходимости измените его название.

Результат

При аутентификации можно вручную выбрать статус УРВ.

Примечание

Если не выбрать статус, аутентификация будет неудачной.

Настройка параметров автоматического учета рабочего времени через веб-интерфейс

Установите режим автоматического учета рабочего времени, чтобы настроить статусы посещений и доступное расписание. Система автоматически изменит статус УРВ в соответствии с настроенным расписанием.

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Для получения подробной информации обратитесь к разделу *«Управление пользователями».*

Шаги

1. Нажмите **Configuration** → **Attendance** («Настройки → УРВ») для перехода на страницу настроек.

2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Auto** («Автоматич.»).
3. Включите функцию **Attendance Status** («Учет рабочего времени»).
4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

5. Опционально. Выберите статус и при необходимости измените его название.
6. Установите расписание статуса. Более подробная информация представлена в разделе ***«Настройки времени»***.

Настройка параметров автоматического УРВ и УРВ вручную через веб-интерфейс

В меню **Attendance Mode** («Учет рабочего времени») выберите **Manual and Auto** («Подсчет автоматически и вручную»). Система автоматически изменит статус посещений в соответствии с настроенным расписанием. При этом можно вручную изменить статус посещения при аутентификации.

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Для получения подробной информации обратитесь к разделу *«Управление пользователями».*

Шаги

1. Нажмите **Configuration** → **Attendance** («Настройки → УРВ») для перехода на страницу настроек.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual and Auto** («Подсчет автоматически и вручную»).
3. Включите функцию **Attendance Status** («Учет рабочего времени»).
4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

5. Опционально. Выберите статус и при необходимости измените его название.
6. Установите расписание статуса. Более подробная информация представлена в разделе ***«Настройки времени»***.

Результат

Аутентификация на начальной странице. При аутентификации будет отображаться статус УРВ в соответствии с настроенным расписанием. Если нажать значок редактирования на вкладке результатов, можно выбрать статус УРВ вручную. При аутентификации будет отображаться измененный статус УРВ.

Пример

Если установить **Break Out** («Время ухода на перерыв») в 11:00 в понедельник и **Break In** («Время возвращения с перерыва») в 12:00 в понедельник, при аутентификации пользователя в понедельник с 11:00 до 12:00 будет отмечен «уход на перерыв».

8.5.18 Настройка параметров контроля доступа

Задание параметров контроля доступа

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

Примечание

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

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

Тип устройства

В выпадающем списке выберите **Main Card Reader** («Основной считыватель карт») или **Sub Card Reader** («Дополнительный считыватель карт»).

Основной считыватель карт

Можно настроить параметры считывателя карт.

Дополнительный считыватель карт

Можно настроить параметры подключенных дополнительных считывателей карт.

При выборе **Main Card Reader** («Основной считыватель карт»):

Тип считывателя карт/описание считывателя карт

Просмотр типа и описания считывателя карт. Доступны только для чтения.

Включить считыватель карт

Включите считыватель карт.

Аутентификация

В выпадающем списке выберите режим аутентификации в соответствии с потребностями.

Отображение результата аутентификации

Выберите **Face Picture** («Изображение лица»), **Name** («Ф. И. О.») или **Employee ID** («Идентификатор сотрудника»). После выполнения аутентификации система отобразит выбранное содержимое.

Интервал распознавания

Можно установить временной интервал между двумя циклами распознавания лица сотрудника во время аутентификации. В заданный интервал сотрудник А может быть распознан только один раз. Если другой сотрудник (сотрудник В) был распознан в течение

заданного интервала, сотрудник A может быть распознан снова.

Интервал аутентификации

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

Запуск тревоги при достижении максимального количества неудачных попыток считывания карты

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

Включение тревоги тампера

Включите детектор саботажа на считывателе карт.

Включить считывание номера карты в обратной последовательности

После включения функции номер карты будет считываться в обратной последовательности.

При выборе **Sub Card Reader** («Дополнительный считыватель карт»):

Тип считывателя карт/описание считывателя карт

Просмотр типа и описания считывателя карт. Доступны только для чтения.

Enable Card Reader («Включить считыватель карт»)

Включите считыватель карт.

Аутентификация

В выпадающем списке выберите режим аутентификации в соответствии с потребностями.

Интервал распознавания

Если интервал считывания одной карты меньше заданного значения, считывание карты будет недействительным.

Интервал аутентификации

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

Запуск тревоги при достижении максимального количества неудачных попыток считывания карты

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

Связь с панелью управления

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

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 пользователь нажал до этого, будут автоматически удалены.

Правильная полярность светодиода / Ошибочная полярность светодиода

Настройте **OK LED Polarity** («Правильная полярность светодиода») / **Error LED Polarity** («Ошибочная полярность светодиода») устройства контроля доступа в соответствии с параметрами считывателя карт. Как правило, устройство получает настройки по умолчанию.

Включение тревоги тампера

Включите детектор саботажа на считывателе карт.

Настройка параметров двери

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

Рисунок 8-12. Страница настроек параметров двери

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

Номер двери

Выберите устройство, соответствующее номеру двери.

Наименование

Можно задать имя двери.

Длительность открытого состояния

Установите **Door Unlocking Duration** («Длительность разблокированного состояния двери»). Дверь будет заблокирована, если движение отсутствует в течение установленного времени.

Тревога тайм-аута открытой двери

Тревога сработает, если дверь не будет закрыта в течение заданного периода времени.

Дверной контакт

Можно установить параметры дверного контакта как **Remain Open** («Оставить открытым»)

или **Remain Closed** («Оставить закрытым») в соответствии с необходимостью. По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).

Тип кнопки выхода

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

Закрытие двери при отключении питания

Можно установить состояние дверного замка при отключении питания. По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).

Увеличение длительности открытого состояния

Дверной контакт может быть активирован с установленной задержкой после считывания карты пользователя с расширенным доступом.

Дверь остается открытой после авторизации первого сотрудника

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

Код принуждения

Дверь может быть открыта при помощи кода принуждения. В тоже время клиент создает уведомление о событии принуждения.

Суперпароль

Пользователь может открыть дверь с помощью суперпароля.

Примечание

Суперпароль должен отличаться от кода принуждения.

Настройка параметров безопасности карты

Нажмите **Configuration → Access Control Event → Card Security** («Настройки → Контроль доступа → Безопасность карты») для перехода на страницу настроек.
Настройте параметры и нажмите **Save** («Сохранить»).

Включение распознавания NFC-карты

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

Активация распознавания M1-карты

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

Шифрование M1-карты

Сектор

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

Активация распознавания EM-карты

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

Примечание

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

Настройка параметров RS-485

Можно установить параметры RS-485, параметры периферийных устройств, адрес, скорость передачи и т. д.
Нажмите **Configuration** → **Access Control** → **RS-485 Settings** («Настройки → Контроль доступа → Параметры RS-485»).
Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

№

Настройте номер RS-485.

Тип периферийного устройства

Выберите необходимое периферийное устройство из выпадающего списка. Можно выбрать **Card Reader** («Считыватель карт»), **Extension Module** («Модуль расширения»), **Access Controller** («Контроллер доступа») или **Disable** («Отключить»).

Примечание

После настройки и сохранения периферийного устройства устройство автоматически перезагрузится.

Адрес RS-485

Задайте необходимый адрес RS-485.

Примечание

При выборе **Access Controller** («Контроллер доступа»). Если устройство подключено к терминалу через интерфейс RS-485, настройте адрес RS-485 на значение 2. Если устройство подключено к контроллеру, настройте адрес RS-485 в соответствии с номером двери.

Скорость передачи данных

Скорость передачи при обмене данными по протоколу RS-485.

Настройка параметров конфиденциальности

Задайте тип хранения событий, параметры загрузки и хранения изображений, а также параметры очистки изображений.
Нажмите **Configuration** → **Access Control** → **Privacy** («Настройки → Контроль доступа → Конфиденциальность»).

Настройки хранения событий

Выберите способ удаления события. Можно выбрать **Delete Old Events Periodically** («Периодическое удаление старых событий»), **Delete Old Events by Specified Time** («Удаление старых событий в заданное время») или **Overwriting** («Перезапись»).

Периодическое удаление старых событий

Переместите курсор мыши или введите число, чтобы установить период для удаления событий. Все события будут удалены в соответствии с настроенным периодом времени.

Удаление старых событий в заданное время

Установите время, и все события будут удалены в указанное время.

Перезапись

Самые ранние 5 % событий будут удалены, когда система обнаружит, что сохраненные события занимают более 95 % заполненного пространства.

Загрузка и хранение изображений

Загрузка захваченного изображения при аутентификации

Загрузите полученные при аутентификации изображения на платформу автоматически.

Загрузка сохраненного изображения при аутентификации

Если эта функция активирована, можно сохранять изображения, захваченные при аутентификации.

Сохранение зарегистрированного изображения

При активации данной функции зарегистрированное изображение лица будет сохранено в системе.

Загрузка изображения после захвата

Если эта функция активирована, изображения, захваченные соответствующей камерой, будут автоматически загружаться на платформу.

Сохранение изображения после захвата

Если эта функция активирована, можно сохранять изображения, захваченные камерой, связанной с устройством.

Удаление всех изображений на устройстве

Примечание

После удаления изображения невозможно восстановить.

Удаление зарегистрированных изображений лиц

Все зарегистрированные изображения лиц будут удалены.

Удаление захваченных изображений

Все захваченные изображения лиц будут удалены.

Настройка параметров аутентификации по карте

Настройте параметры карты при аутентификации через карту на устройстве.
Нажмите **Configuration** → **Access Control** → **Card Authentication Settings** («Настройки → Контроль доступа → Настройки аутентификации по карте»).
Выберите режим аутентификации по карте и нажмите **Save** («Сохранить»).

Полный номер карты

Будет прочитан полный номер карты.

Wiegand 26 (3 байта)

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

Wiegand 34 (4 байта)

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

8.5.19 Настройка биометрических параметров

Настройка основных параметров

Нажмите **Configuration** → **Smart** → **Smart** («Настройки → Интеллектуальные функции → Интеллектуальные функции»).

Рисунок 8-13. Страница настройки интеллектуальных функций

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

Детекция подлинности биометрических данных лица (антиспуфинг)

Здесь можно включить/выключить функцию детекции лиц в режиме реального времени. При включении этой функции устройство сможет отличать сотрудника/посетителя от изображения.

Примечание

Продукты с биометрическим распознаванием не на 100 % применимы для защиты от подделки биометрических данных. Используйте несколько режимов аутентификации, если требуется более высокий уровень безопасности.

Уровень безопасности «Детекция лиц в режиме реального времени»

После включения функции антиспуфинга можно установить надлежащий уровень безопасности при выполнении аутентификации лица в режиме реального времени.

Дальность распознавания

Настройте расстояние между пользователем и камерой устройства.

Режим применения

Режим **Indoor** («Внутри помещения») или **Others** («Другое») в соответствии со средой установки.

Режим распознавания лиц

Обычный режим

Распознавание лиц с помощью камеры в обычном режиме.

Режим распознавания на основе алгоритмов глубокого обучения

Устройство распознает более широкий диапазон лиц в сравнении с обычным режимом. Этот режим рекомендуется применять при сложных условиях эксплуатации.

Интервал распознавания лиц

Установите временной интервал между двумя циклами распознавания лиц при непрерывной работе.

Угол наклона

Максимальный угол наклона при запуске аутентификации лица.

Угол отклонения

Максимальный угол отклонения при запуске аутентификации лица.

Оценка лиц

Задайте необходимые параметры оценки лиц.

Пороговое значение для сопоставления 1:N

Настройте пороговое значение совпадения при аутентификации в режиме сопоставления 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений, и тем больше вероятность отклонений ложных совпадений.

Лимит времени при распознавании лиц

Установите лимит времени при распознавании лиц. Если распознавание лица выполняется дольше, чем установлено, система выдаст предупреждение.

ЭКО-режим

После включения ЭКО-режима устройство будет использовать ИК-подсветку для аутентификации лиц в условиях низкой освещенности или в темноте. Настройте пороговое значение для ЭКО-режима, ЭКО-режим (1:N) и ЭКО-режим (1:1).

ЭКО-режим (1:N)

Настройте пороговое значение совпадения при аутентификации в ЭКО-режиме 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений.

Настройка области распознавания

Нажмите **Configuration** → **Smart** → **Area Configuration** («Настройки → Интеллектуальные функции → Настройка области распознавания»).
Чтобы настроить область распознавания, при просмотре в режиме реального времени перетащите желтую рамку на видео. Система будет распознавать только лица в пределах заданной области.
Нажмите **Save** («Сохранить») для сохранения настроек.

Нажмите  или  для записи видео или захвата изображений.

8.5.20 Настройка отображения уведомлений

Можете установить заставку, а также настроить спящий режим устройства.
Нажмите **Configuration** → **Notice Publication** («Настройки → Отображение уведомлений»).

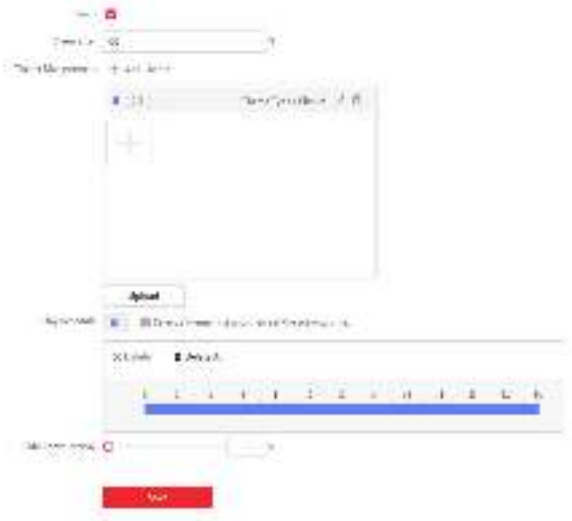


Рисунок 8-14. Страница настройки уведомлений

Спящий режим

Активируйте спящий режим, и устройство перейдет в спящий режим, если в течение настроенного времени не будет никаких операций.

Управление темой

Нажмите **+** в рамке и загрузите изображения заставки с локального ПК.

Примечание

В настоящее время можно добавить только одну тему.

Создание расписания

После создания темы можно выбрать тему и настроить расписание на временной шкале. Выберите настроенное расписание и задайте точное время начала и окончания, если необходимо.
Чтобы удалить расписание, выберите настроенное расписание и нажмите **Delete** («Удалить») или **Delete All** («Удалить все»).

Интервал показа слайдов

Переместите курсор мыши или введите число, чтобы установить интервала показа слайдов. Изображения будут меняться в соответствии с интервалом.

Раздел 9. Настройка клиентского ПО

9.1 Схема настройки клиентского ПО

Следуйте приведенной ниже схеме для настройки клиентского ПО.

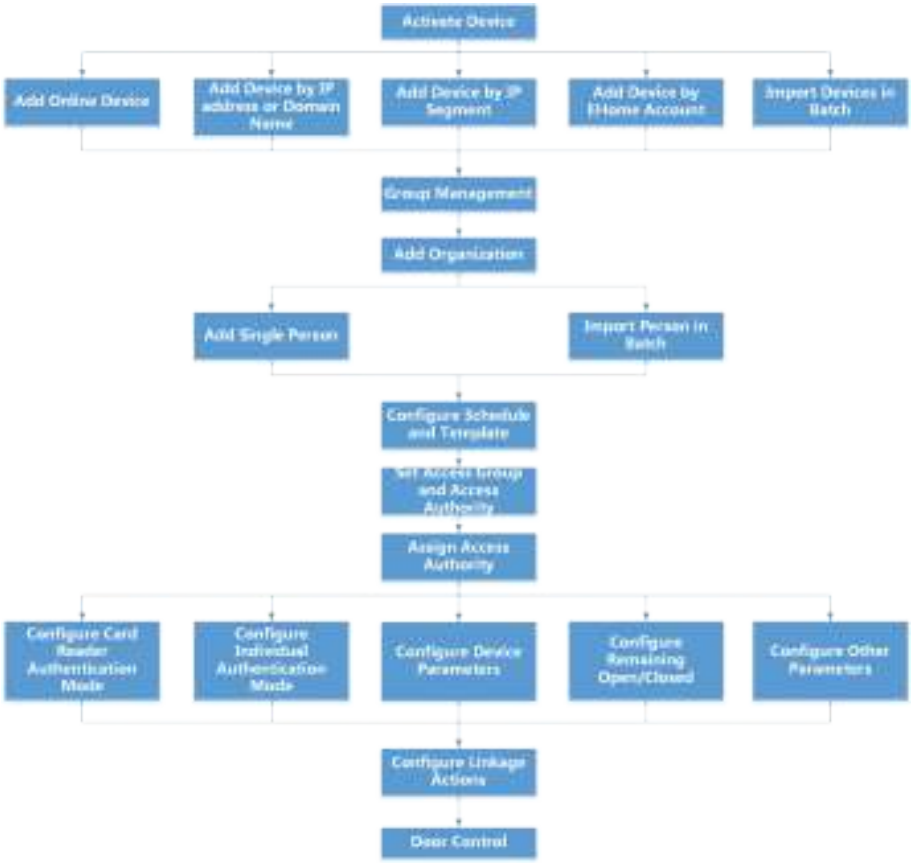


Рисунок 9-1. Схема настройки клиентского ПО

Английский язык	**Русский язык**
Activate Device	Активировать устройство
Add Online Device	Добавить онлайн устройство
Add Device by IP address or Domain Name	Добавить устройство по IP-адресу или доменному имени
Add Device by IP Segment	Добавить устройство по IP-сегменту
Add Device by EHome Account	Добавить устройство с помощью учетной записи EHome
Import Device in Batch	Импортировать устройство в пакетном режиме
Group Management	Управление группой

Английский язык	**Русский язык**
Add Organization	Добавить организацию
Add Single Person	Добавить одного сотрудника/посетителя
Import Person in Batch	Импортировать сотрудника/посетителя в пакетном режиме
Configure Schedule and Template	Настроить расписание и шаблон
Set Access Group and Access Authority	Установить группу доступа и доступ
Assign Access Authority	Назначить полномочия доступа
Configure Card Reader Authentication Mode	Настроить режим аутентификации считывателя карт
Configure Individual Authentication Mode	Настроить индивидуальный режим аутентификации
Configure Device Parameters	Настроить параметры устройства
Configure Remaining Open/Closed	Настроить параметры «Оставить открытым» / «Оставить закрытым»
Configure Other Parameters	Настроить другие параметры
Configure Linkage Actions	Настроить привязку
Door Control	Контроль двери

9.2 Управление устройством

Поддержка устройств контроля доступа и устройств видеодомофонии.

Пример

После добавления устройств контроля доступа в клиентское ПО доступно управление въездом и выездом, управление посещаемостью, видеодомофония с использованием вызывной панели, установленной внутри или снаружи помещений.

9.2.1 Добавление устройства

Предусмотрено три режима добавления устройств, в том числе через IP-адрес и доменное имя, IP-сегмент и протокол ISUP. Также поддерживается импорт нескольких устройств в пакетном режиме, когда требуется добавить большое количество устройств.

Добавление онлайн устройства

Активные онлайн устройства, которые находятся в одной локальной подсети с клиентским ПО, будут отображены в области **Online Device** («Онлайн устройства»). Нажмите кнопку **Refresh Every 60s** («Обновлять каждые 60 с»), чтобы обновлять информацию об активных

устройствах.

Добавить одно или несколько онлайн устройств

Клиент может обнаруживать онлайн устройства, которые находятся в той же сети, что и ПК, на котором запущен клиент. Выберите обнаруженное онлайн устройство, отображаемое в списке онлайн устройств, затем добавьте его в клиентское ПО. Если обнаруженные онлайн устройства имеют одинаковые имя пользователя и пароль, их можно одновременно добавить в клиентское ПО.

Перед началом

- Добавляемые устройства должны находиться в той же сети, что и ПК, на котором запущен клиент.
- Добавляемые устройства были активированы.

Шаги

1. Нажмите **Device Management** → **Device** («Управление устройством → Устройство»).
2. Нажмите **Online Device** («Онлайн устройства»), чтобы отобразить область онлайн устройств.
   Искомые онлайн устройства отобразятся в списке.

Рисунок 9-2. Онлайн устройство

3. В области **Online Device** («Онлайн устройство») отметьте одно или несколько устройств и нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.

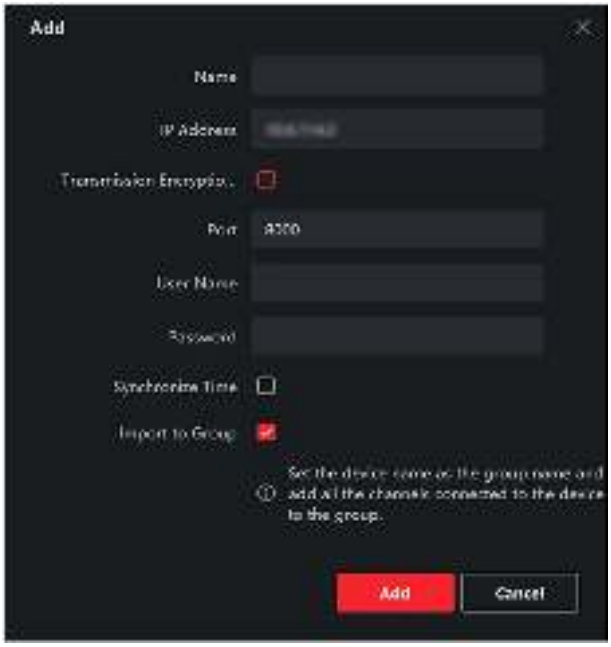


Рисунок 9-3. Добавить одно онлайн устройство

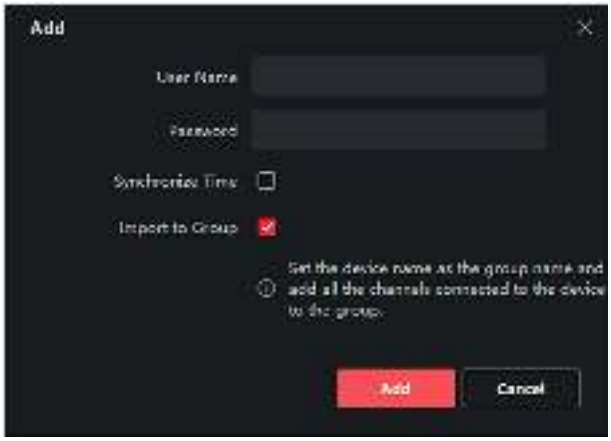


Рисунок 9-4 Добавление нескольких онлайн устройств

4. Введите необходимую информацию.

Имя

Введите описательное имя для устройства.

IP-адрес

Введите IP-адрес устройства. IP-адреса устройств получаются автоматически в данном режиме добавления.

Порты

Установите номер порта. Номер порта устройства назначается автоматически в данном режиме добавления.

Имя пользователя»)

По умолчанию имя пользователя - ***admin***.

Пароль

Введите пароль устройства.

Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

5. Опционально. Нажмите **Transmission Encryption** («Шифрование передачи») **(TLS)** для включения шифрования передачи, защищенной протоколом TLS (безопасность на транспортном уровне).

Примечание

- Устройство должно поддерживать данную функцию.
- Если функция **Certificate Verification** («Проверка сертификата») включена, нажмите **Open Certificate Directory** («Открыть каталог сертификатов»), чтобы открыть папку по умолчанию, затем скопируйте файл сертификата, экспортированный с устройства, в этот каталог по умолчанию для повышения уровня безопасности. Более подробная информация о проверке сертификата представлена в разделе ***«Проверка сертификата для шифрования передачи»***.
- Войдите в устройство, чтобы загрузить файл сертификата через веб-браузер.

6. Установите флажок **Synchronize Time** («Синхронизировать время»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО, после добавления устройства в клиентское ПО.
7. Опционально. Нажмите **Import to Group** («Импортировать в группу»), чтобы создать группу по названию устройства. Также можно импортировать все каналы устройства в соответствующую группу.

Пример

Точки доступа, тревожные входы/выходы и каналы кодирования (при наличии) устройства контроля доступа будут импортированы в эту группу.

8. Нажмите **Add** («Добавить»).

Добавление нескольких обнаруженных онлайн устройств

Если обнаруженные онлайн устройства имеют одинаковые имя пользователя и пароль, их

можно одновременно добавить в клиентское ПО.

Перед началом

Убедитесь, что все добавляемые устройства активны.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. В верхней части правой панели нажмите вкладку **Device** («Устройство»).
3. Нажмите **Online Device** («Онлайн устройства»), чтобы отобразить область онлайн устройств внизу страницы.
   Искомые онлайн устройства отобразятся в списке.
4. Выберите несколько устройств.

Примечание

Для неактивного устройства вам необходимо создать для него пароль, прежде чем вы сможете правильно добавить устройство. Более подробная информация представлена в соответствующем разделе.

5. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
6. Введите необходимую информацию.

Имя пользователя

По умолчанию имя пользователя - ***admin***.

Пароль

Введите пароль устройства.

Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

7. Опционально. Установите флажок **Synchronize Time** («Синхронизировать время»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО, после добавления устройства в клиентское ПО.
8. Опционально. Нажмите **Import to Group** («Импортировать в группу»), чтобы создать группу по названию устройства. Также можно импортировать все каналы устройства в соответствующую группу.

Пример

Точки доступа, тревожные входы/выходы и каналы кодирования (при наличии) устройства

контроля доступа будут импортированы в эту группу.

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

Добавление устройства по IP-адресу или доменному имени

Если IP-адрес или доменное имя устройства известны, можно добавить устройство в клиентское ПО, указав IP-адрес (или доменное имя), имя пользователя, пароль и т. д.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. В верхней части правой панели нажмите вкладку **Device** («Устройство»).
   Добавленные устройства отображаются на панели справа.
3. Нажмите кнопку **Add** («Добавить»), чтобы открыть окно добавления устройства. Выберите режим добавления **IP/Domain** («IP-адрес/доменное имя»).
4. Введите необходимую информацию.

   Название

   Создайте описательное название для устройства. Например, вы можете использовать название, которое отображает местоположение или функцию устройства.

   Адрес

   IP-адрес или доменное имя устройства.

   Port («Порт»)

   Добавляемые устройства имеют одинаковый номер порта. Значение по умолчанию - ***8000***.

   User Name («Имя пользователя»)

   Войдите имя пользователя устройства. По умолчанию имя пользователя - ***admin***.

   Password («Пароль»)

   Введите пароль устройства.

   Предостережения

   Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
   Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

5. Опционально. Нажмите **Transmission Encryption** («Шифрование передачи») **(TLS)** для включения шифрования передачи, защищенной протоколом TLS (безопасность на транспортном уровне).

Примечание

- Устройство должно поддерживать данную функцию.
- Если функция **Certificate Verification** («Проверка сертификата») включена, нажмите **Open Certificate Directory** («Открыть каталог сертификатов»), чтобы открыть папку по умолчанию, затем скопируйте файл сертификата, экспортированный с устройства, в этот каталог по умолчанию для повышения уровня безопасности. Более подробная информация о проверке сертификата представлена в разделе ***«Проверка сертификата для шифрования передачи»***.
- Войдите в устройство, чтобы загрузить файл сертификата через веб-браузер.

6. Установите флажок **Synchronize Time** («Синхронизировать время»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО, после добавления устройства в клиентское ПО.
7. Опционально. Нажмите **Import to Group** («Импортировать в группу»), чтобы создать группу по названию устройства. Также можно импортировать все каналы устройства в соответствующую группу.

   Пример

   Точки доступа, тревожные входы/выходы и каналы кодирования (при наличии) устройства контроля доступа будут импортированы в эту группу.
8. Завершите добавление устройства.
   - Нажмите **Add** («Добавить») для добавления устройств и возврата на страницу списка устройств.
   - Нажмите **Add and New** («Добавить и продолжить») для сохранения настроек и продолжения добавления других устройств.

Добавление устройств по сегменту IP-адресов

Если устройства имеют одинаковый номер порта, имя пользователя и пароль, диапазоны их IP-адресов находятся в одном сегменте, можно добавить их в клиентское ПО, указав начальный IP-адрес и конечный IP-адрес, номер порта, имя пользователя, пароль и т. д.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. В верхней части правой панели нажмите вкладку **Device** («Устройство»). Добавленные устройства отображаются на панели справа.
3. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
4. Выберите **IP Segment** («Сегмент IP-адресов») в поле **Adding Mode** («Режим добавления»).
5. Введите необходимую 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.

Порт

Войдите номер порта устройства. Значение по умолчанию - ***8000***.

Имя пользователя

По умолчанию имя пользователя - ***admin***.

Пароль

Введите пароль устройства.

Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

6. Опционально. Нажмите **Transmission Encryption** («Шифрование передачи») **(TLS)** для включения шифрования передачи, защищенной протоколом TLS (безопасность на транспортном уровне).

Примечание

- Устройство должно поддерживать данную функцию.
- Если функция **Certificate Verification** («Проверка сертификата») включена, нажмите **Open Certificate** («Открыть каталог сертификатов»), чтобы открыть папку по умолчанию, затем скопируйте файл сертификата, экспортированный с устройства, в этот каталог по умолчанию для повышения уровня безопасности. Более подробная информация о проверке сертификата представлена в разделе ***Проверка сертификата для шифрования передачи***.
- Войдите в устройство, чтобы загрузить файл сертификата через веб-браузер.

7. Установите флажок **Synchronize Time** («Синхронизировать время»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО, после добавления устройства в клиентское ПО.
8. Опционально. Нажмите **Import to Group** («Импортировать в группу»), чтобы создать группу по названию устройства. Также можно импортировать все каналы устройства в соответствующую группу.
9. Завершите добавление устройства.
   – Нажмите **Add** («Добавить») для добавления устройств и возврата на страницу списка устройств.
   – Нажмите **Add and New** («Добавить и продолжить») для сохранения настроек и продолжения добавления других устройств.

Добавление устройства по протоколу ISUP

Если устройства контроля доступа поддерживают протокол ISUP 5.0, устройства можно добавить в клиентское ПО по протоколу ISUP, указав идентификатор и ключ устройства, после настройки адресов серверов, номеров портов и идентификаторов устройств.

Перед началом

Устройства должны быть должным образом подключены к сети.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
   Добавленные устройства отображаются на панели справа.
2. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
3. Выберите значение **ISUP** в поле **Adding Mode** («Режим добавления»).
4. Введите необходимую информацию.

   Учетная запись устройства

   Введите учетное имя, зарегистрированное по протоколу ISUP.

   Ключ ISUP

   Если устройства поддерживают протокол ISUP 5.0, введите ключ ISUP, который был задан в сетевых настройках устройства.

   Примечание

   Устройство должно поддерживать данную функцию.

5. Опционально. Установите флажок **Synchronize Time** («Синхронизировать время»), чтобы синхронизировать время устройства со временем компьютера, на котором работает клиентское ПО, после добавления устройства в клиентское ПО.
6. Опционально. Нажмите **Import to Group** («Импортировать в группу»), чтобы создать группу по названию устройства. Также можно импортировать все каналы устройства в соответствующую группу.
7. Завершите добавление устройства.
   - Нажмите **Add** («Добавить») для добавления устройств и возврата к списку устройств.
   - Нажмите **Add and New** («Добавить и продолжить») для сохранения настроек и продолжения добавления других устройств.

   Примечание

   Изображения лиц нельзя загружать к устройствам, добавленным по протоколу ISUP, кроме устройств серии DS-K1T671 и ACT-T1331.

8. Опционально. Выполните следующие операции.

Состояние устройства	Нажмите в столбце **Operation** («Операции») для просмотра состояния устройства.

Изменение информации об устройстве	Нажмите в столбце **Operation** («Операции»), чтобы редактировать информацию устройства, в том числе имя устройства, учетную запись устройства, ключ ISUP.
Проверка онлайн пользователей	Нажмите в столбце **Operation** («Операции»), для проверки онлайн пользователей, которые имеют доступ к устройству. Здесь можно проверить имя пользователя, тип пользователя, IP-адрес пользователя и время входа в систему.
Обновление	Нажмите в столбце **Operation** («Операции»), чтобы получить актуальную информацию об устройстве.
Удаление устройства	Выберите одно или несколько устройств и нажмите **Delete** («Удалить»), чтобы удалить выбранные устройства.

Импорт устройств в пакетном режиме

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

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. В верхней части правой панели нажмите вкладку **Device** («Устройство»).
3. Нажмите кнопку **Add** («Добавить»), чтобы открыть окно добавления устройства. Выберите режим добавления **Batch Import** («Добавить в пакетном режиме»).
4. Нажмите **Export Template** («Скачать шаблон») и сохраните предварительно выбранный шаблон (файл CSV) на компьютере.
5. Откройте экспортируемый файл шаблона и введите необходимую информацию об устройствах, которые необходимо добавить, в соответствующий столбец.

Примечание

Более подробное описание обязательных полей представлено во введении.

Режим добавления

Введите ***0*** или ***1*** или ***2***.

Адрес

Редактируйте адрес устройства.

Порт

Введите номер порта устройства. Номер порта по умолчанию: ***8000***.

Имя пользователя

Войдите имя пользователя устройства. По умолчанию имя пользователя - ***admin***.

Пароль

Введите пароль устройства.

Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

Импортировать в группу

Введите ***1,*** чтобы создать группу по названию устройства. Все каналы устройства будут импортированы в соответствующую группу по умолчанию. Введите ***0***, чтобы отключить функцию.

6. Нажмите … и выберите файл шаблона.
7. Нажмите **Add** («Добавить»), чтобы импортировать устройства.

9.2.2 Сброс пароля устройства

Если пользователь забыл пароль обнаруженных онлайн устройств, пароль устройства можно сбросить через клиентское ПО.

Шаги

1. Откройте страницу **Device Management** («Управление устройством»).
2. Нажмите **Online Device** («Онлайн устройства»), чтобы отобразить область онлайн устройств.
   Все онлайн устройства, находящиеся в одной подсети, будут отображены в списке.
3. Выберите устройство из списка и нажмите в столбце **Operation** («Операции»).
4. Сбросьте пароль устройства.
   – Нажмите **Generate** («Создать»), чтобы открыть окно QR-кода, затем нажмите **Download** («Загрузить»), чтобы сохранить QR-код на компьютере. Также можно сфотографировать QR-код и сохранить его на телефон. Отправьте изображение в нашу службу технической поддержки.

Примечание

Для выполнения следующих операций по сбросу пароля обратитесь в службу технической поддержки.

Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

9.3 Управление группами

Клиентское ПО предоставляет области для управления добавленными ресурсами в разных группах. Ресурсы можно сгруппировать в разные группы в зависимости от расположения ресурсов.

Пример

Например, на первом этаже установлено 16 дверей, 64 тревожных входа и 16 тревожных выходов. Эти ресурсы можно организовать в одну группу (с именем «1-й этаж») для удобного управления. Можно контролировать состояние двери и выполнять другие операции с устройствами, объединив ресурсы по группам.

9.3.1 Добавление группы

Добавьте группы для удобного управления устройствами.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device Management → Group** («Управление устройством → Группа») для перехода на страницу управления группами.
3. Создайте группу.
   – Нажмите **Add Group** («Добавить группу») и введите желаемое название группы.
   – Нажмите **Create Group by Device Name** («Создать группу по названию устройства») и выберите добавленное устройство, чтобы создать новую группу по имени выбранного устройства.

   Примечание

   Ресурсы (такие как тревожные входы/выходы, точки доступа и т. д.) устройства будут импортированы в группу по умолчанию.

9.3.2 Добавление ресурсов в группу

Импортируйте ресурсы устройства (такие как тревожные входы/выходы, точки доступа и т. д.) в добавленную группу в пакетном режиме.

Перед началом

Добавьте группу для управления устройствами. Более подробная информация представлена в разделе ***«Добавление группы»***.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device Management → Group** («Управление устройством → Группа») для перехода на страницу управления группами.
3. Выберите группу и тип ресурса из списка: **Access Point** («Точка доступа»), **Alarm Input («Тревожный вход»)**, **Alarm Output** («Тревожный выход») и т. д.
4. Нажмите **Import** («Импорт»).
5. Выберите миниатюры / названия ресурсов для отображения в списке.

> **Примечание**
>
> Нажмите или , чтобы переключить режим отображения ресурса на режим просмотра миниатюр или списка.

6. Нажмите **Import** («Импорт») для импорта выбранных ресурсов в группу.

9.3.3 Изменение параметров ресурса

После импорта ресурсов в группу можно редактировать параметры ресурса. Измените имя точки доступа при необходимости. Здесь можно изменить имя тревожного входа. В качестве примера приведена точка доступа.

Перед началом

Добавление ресурсов в группу.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device Management → Group** («Управление устройством → Группа») для перехода на страницу управления группами.
   Все добавленные группы будут отображаться слева.
3. Выберите группу в списке групп и нажмите **Access Point** («Точка доступа»).
   Будут отображены точки доступа, импортированные в группу.
4. Нажмите в столбце **Operation** («Операции») для открытия окна **Edit Resource** («Изменение ресурса»).
5. Измените имя ресурса.
6. Нажмите **OK** для сохранения обновленных настроек.

9.3.4 Удаление ресурсов из группы

Удалите добавленные ресурсы из группы.

Шаги

1. Откройте модуль **Device Management** («Управление устройством»).
2. Нажмите **Device Management → Group** («Управление устройством → Группа») для перехода на страницу управления группами.
   Все добавленные группы будут отображаться слева.
3. Нажмите на иконку группы, чтобы отобразить ресурсы, добавленные в эту группу.
4. Выберите ресурс(-ы) и нажмите **Delete** («Удалить»), чтобы удалить ресурс(-ы) из группы.

9.4 Управление сотрудниками/посетителями

Добавьте информацию о сотруднике/пользователе в систему для дальнейших операций, таких как контроль доступа, видеодомофония, время и посещаемость и т. д. Здесь можно управлять добавленными пользователями, например, выпускать карточки в пакетном режиме, импортировать и экспортировать информацию пользователя в пакетном режиме и т. д.

9.4.1 Добавление организации

Добавьте организацию и импортируйте информацию о сотруднике/посетителе в организацию для эффективного управления персоналом. Также можно добавить подчиненную организацию для добавленной организации.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите головную организацию в левом столбце и нажмите **Add** («Добавить») в верхнем левом углу, чтобы добавить организацию.
3. Создайте имя для добавленной организации.

Примечание

Можно добавить до 10 уровней организаций.

4. Опционально. Выполните следующие операции.

Изменение организации	Наведите указатель мыши на добавленную организацию и нажмите , чтобы изменить ее название.
Удаление организации	Наведите указатель мыши на добавленную организацию и нажмите , чтобы удалить ее.

Примечание

- Организации нижнего уровня будут удалены, если вы удалите организацию верхнего уровня.
- Организация не может быть удалена, если ранее добавлены сотрудники.

Отображение персонала подчиненной организации

Нажмите **Show Persons in Sub Organization** («Отображение персонала подчиненной организации») и выберите организацию, чтобы показать персонал подчиненной организации.

9.4.2 Настройка основной информации

Можно добавить пользователей в клиент поочередно и настроить основную информацию о пользователе, в том числе Ф. И. О., пол, номер телефона и т. д.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).

Примечание

При первом входе в модуль **Person** («Сотрудник/Посетитель») появляется всплывающее окно, в котором можно установить правила создания идентификатора сотрудника/посетителя (буквы и цифры) при добавлении сотрудника/посетителя. Если при получении информации о сотруднике/посетителе с устройства идентификатор отсутствует, идентификаторы будут сгенерированы в соответствии с правилом.

2. Выберите организацию из списка и добавьте сотрудника/посетителя.
3. Нажмите **Add** («Добавить»), чтобы открыть окно добавления сотрудника/пользователя. Идентификатор личности будет сгенерирован автоматически.
4. Введите основную информацию, в том числе Ф. И. О., пол, номер телефона, адрес электронной почты, срок действия учетной записи и т. д.

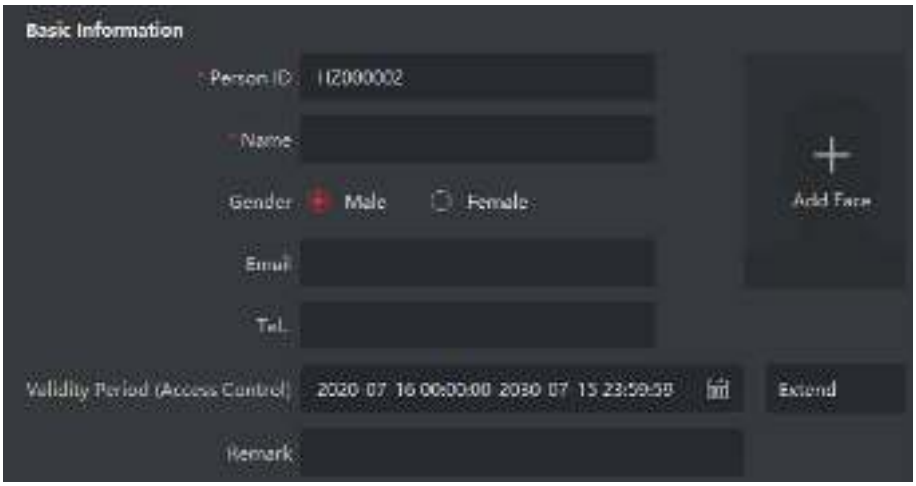


Рисунок 9-5. Настройка основной информации

Примечание

После истечения срока действия учетные данные и настройки контроля доступа станут недействительными, и у пользователя не будет разрешения на доступ к дверям/этажам. Можно нажать **Extend** («Продлить»), чтобы продлить срок действия учетной записи на 1 месяц, 3 месяца, 6 месяцев или 1 год.

5. Подтвердите, чтобы добавить пользователя.
   - Нажмите **Add** («Добавить») для добавления сотрудника/посетителя и закройте окно добавления.
   - Нажмите **Add and New** («Добавить и новый») для добавления сотрудника/посетителя и продолжения добавления других пользователей.

9.4.3 Выпуск карт в локальном режиме

При наличии настольного считывателя карт, можно выпустить карту в локальном режиме. Чтобы считать номер карты, необходимо подключить считыватель карт к компьютеру, на котором работает клиентское ПО, через USB или COM-интерфейс, затем поместить карту на настольный считыватель.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите организацию из списка, затем нажмите **Add** («Добавить»), чтобы открыть панель добавления сотрудника/пользователя.

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике/посетителе. Более подробная информация о настройке основной информации о пользователе представлена в разделе ***Настройка основной информации***.

3. Зайдите в меню **Credential → Card** («Учетные данные → Карта»), затем нажмите **+**.
4. Нажмите **Settings** («Настройки») для перехода на страницу настроек.
5. Выберите режим выпуска карт - **Local** («Локальный).

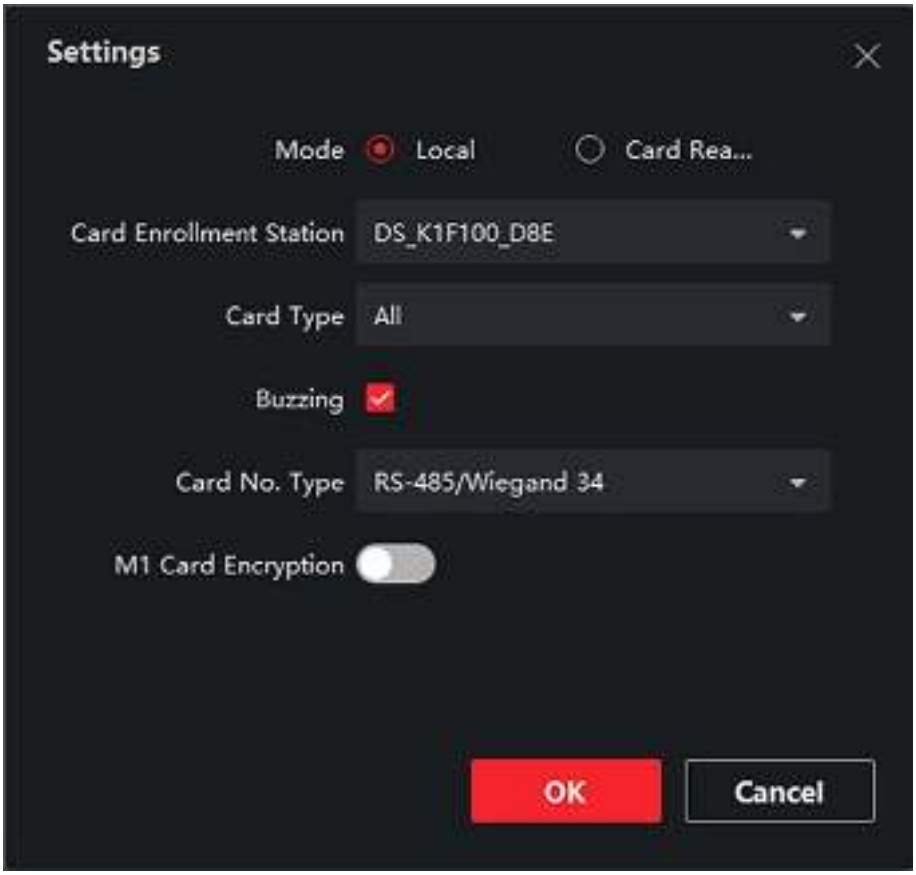


Рисунок 9-6. Выпуск карт в локальном режиме

6. Установите другие сопутствующие параметры.

Настольный считыватель карт

Выберите модель подключенного настольного считывателя карт.

Примечание

В настоящее время поддерживаются следующие модели считывателя карт: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

Тип карты

Это поле доступно только для моделей считывателя карт DS-K1F100-D8E или DS-K1F180-D8E. Выберите тип карты EM-карта или Mifare в соответствии с фактическим типом карты.

Тональный генератор (бипер)

После успешного считывания номера карты включите или выключите бипер.

Card No. Type («Тип номера карты»)

Выберите необходимый тип номера карты.

M1 Card Encryption («Шифрование M1-карты»)

Это поле доступно только для моделей считывателя карт DS-K1F100-D8, DS-K1F100-D8E или DS-K1F180- D8E. Если используется M1-карта и нужно активировать функцию ее шифрования, выберите соответствующий сектор.

7. Нажмите **OK** для подтверждения операции.
8. Поместите карту на настольный считыватель и нажмите **Read** («Считать») для получения номера карты.
   Номер карты автоматически отобразится в поле номера карты.
9. Нажмите **Add** («Добавить»).
   Карта будет выдана соответствующему лицу.

9.4.4 Загрузка изображения лица с локального ПК

При добавлении сотрудника/посетителя можно загрузить фотографию лица с локального ПК в профиль этого сотрудника/посетителя в клиентском ПО.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите организацию из списка и нажмите **Add** («Добавить»).

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике/посетителе. Более подробная информация о настройке основной информации о пользователе представлена в разделе ***«Настройка основной информации»***.

3. Нажмите **Add Face** («Добавить изображение лица») в панели основной информации.
4. Выберите **Upload** («Загрузить»).
5. Выберите изображение с компьютера, на котором работает клиентское ПО.

Примечание

Формат фотографии должен быть JPEG или JPG. Размер фотографии не должен превышать 200 КБ.

6. Опционально. Включите функцию **Verify by Device** («Проверка устройством»), чтобы проверить способность устройства распознавания лиц на клиентском ПО распознать лицо на фотографии.

Примечание

Эта функция скрыта или отображается в зависимости от емкости устройства.

7. Подтвердите, чтобы добавить пользователя.
   – Нажмите **Add** («Добавить») для добавления сотрудника/посетителя и закройте окно добавления.
   – Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

9.4.5 Получение снимка лица с помощью клиентского ПО

При добавлении сотрудника/посетителя можно сфотографировать его/его через клиентское ПО и установить полученную фотографию в профиле этого сотрудника/посетителя.

Перед началом

Убедитесь, что компьютер, на котором работает клиентское ПО, оснащен камерой или подключен к USB-камере.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите организацию из списка, затем нажмите **Add** («Добавить»), чтобы открыть панель добавления сотрудника/пользователя.

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике/посетителе. Для получения подробной информации обратитесь к разделу ***«Настройка основной информации»***.

3. Нажмите **Add Face** («Добавить изображение лица») в панели основной информации.
4. Выберите **Take Photo** («Сделать снимок»), чтобы войти в соответствующее окно.
5. Опционально. Включите функцию **Verify by Device** («Проверка устройством»), чтобы проверить, соответствует ли захваченная фотография лица установленным требованиям.

Примечание

Эта функция скрыта или отображается в зависимости от емкости устройства.

6. Сделайте снимок.
   1) Расположите лицо перед камерой и убедитесь, что лицо находится в середине окна сбора данных.
   2) Нажмите , чтобы сделать снимок лица.
   3) Опционально. Нажмите для повторного захвата.
   4) Нажмите **OK** для сохранения захваченного изображения.

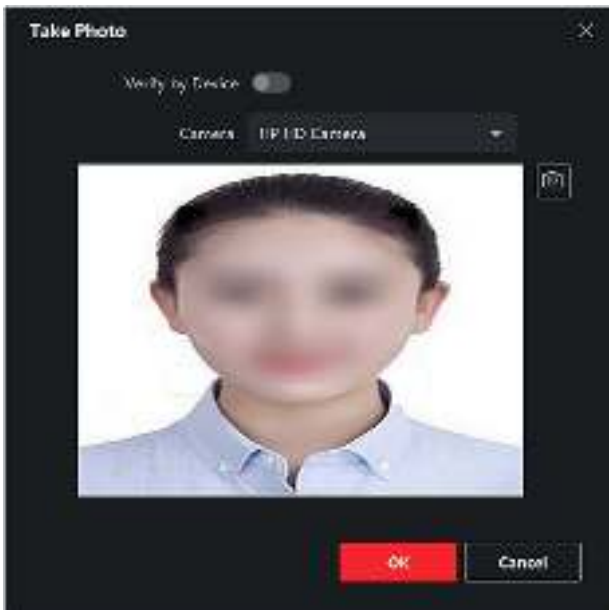


Рисунок 9-7. Снимок лица, сделанный с помощью клиентского ПО

7. Подтвердите, чтобы добавить пользователя.
   – Нажмите **Add** («Добавить») для добавления сотрудника/посетителя и закройте окно добавления.
   – Нажмите **Add and New** («Добавить и новый») для добавления сотрудника/посетителя и продолжения добавления других пользователей.

7.4.6 Получение снимка лица с помощью устройства контроля доступа

При добавлении сотрудника/посетителя можно сделать снимок лица сотрудника/посетителя с помощью устройства контроля доступа, добавленного в клиентское ПО, которое поддерживает функцию распознавания лиц.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите организацию из списка и нажмите **Add** («Добавить»).

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике/посетителе. Более подробная информация о настройке основной информации о пользователе представлена в разделе ***«Настройка основной информации»***.

3. Нажмите **Add Face** («Добавить изображение лица») в панели основной информации.
4. Нажмите **Remote Collection** («Удаленный сбор»).
5. Выберите добавленное устройство контроля доступа или настольный считыватель карт из выпадающего списка.

Примечание

При выборе настольного считывателя карт, нажмите **Login** («Войти»), чтобы установить соответствующие параметры устройства, в том числе IP-адрес, номер порта, имя пользователя и пароль. Кроме того, можно включить функцию **Face Anti-Spoofing** («Детекция подлинности биометрических данных лица») и выбрать уровень витальности: низкий, средний или высокий.

Детекция подлинности биометрических данных лица (антиспуфинг)

При включении этой функции устройство сможет определить, является ли пользователь, снимок лица которого будет захвачен, авторизованным.

6. Сбор изображения лица.
   1) Расположите лицо перед камерой и убедитесь, что оно находится в середине окна сбора данных.
   2) Нажмите , чтобы сделать снимок.
   3) Нажмите **OK** для сохранения захваченного изображения.
7. Подтвердите, чтобы добавить пользователя.
   – Нажмите **Add** («Добавить») для добавления сотрудника/посетителя и закройте окно добавления.
   – Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

9.4.7 Настройка информации контроля доступа

При добавлении сотрудника/пользователя можно установить информацию по контролю доступа, в том числе связать группы контроля доступа с сотрудником/пользователем, настроить PIN-код, назначить человека в качестве посетителя, добавить пользователя в черный список или назначить в качестве суперпользователя и т. д.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите организацию из списка и нажмите **Add** («Добавить»).
3. В меню **Access Control** («Контроль доступа») выберите группу контроля доступа для сотрудника/пользователя.

Примечание

Более подробная информация представлена в разделе ***«Настройка группы контроля доступа для назначения разрешений на доступ»***.

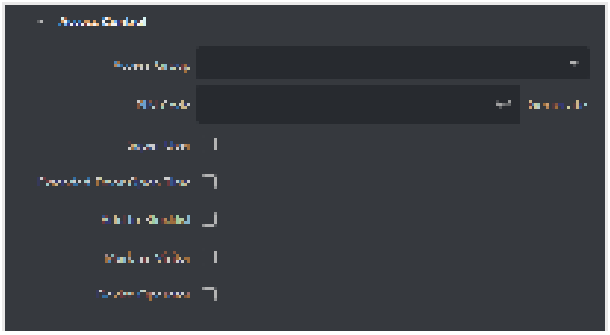


Рисунок 9-8. Настройка информации контроля доступа

4. Установите уникальный PIN-код, который может быть использован для аутентификации доступа конкретного лица.
   – Вручную введите PIN-код. PIN-код должен содержать от 4 до 8 цифр.

   Примечание

   Не допускается дублирование PIN-кодов.

   – Нажмите **Generate** («Создать»), чтобы случайным образом создать уникальный PIN-код из 6 цифр.

   Примечание

   При обнаружении повторяющегося PIN-кода появится предупреждение. Администратор может сформировать новый PIN-код для замены повторяющегося PIN-кода и уведомить связанных лиц.

5. Проверьте разрешения лица.

   Суперпользователь

   Если пользователь назначен в качестве суперпользователя, он/она будет иметь разрешение на доступ ко всем дверям/этажам и будет освобожден/освобождена от других закрытых ограничений, запрета двойного прохода и авторизации от первого лица.

   Увеличенная продолжительность открытия двери

   Используйте эту функцию для обслуживания людей с ограниченной подвижностью. Таким людям будет предоставлено больше времени, чтобы пройти через двери. Более подробная информация о настройке состояния дверей представлена в разделе ***«Настройка параметров двери/лифта»***.

   Добавление в черный список

   Добавьте пользователя в черный список. При попытке получения доступа к дверям/этажам, будет запущено событие и отправлено в клиентское ПО для уведомления сотрудников службы безопасности.

Назначение в качестве посетителя

Если пользователь является посетителем, необходимо установить количество проходов через систему контроля доступа.

Примечание

Максимальное количество проходов через систему контроля доступа должно находиться в диапазоне от 1 до 100. Также можно выбрать значение **No Limit** («Неограниченный доступ»), тогда посетитель не будет ограничен по времени для доступа к дверям/этажам.

Оператор устройства

Оператор устройства имеет право работать с устройствами контроля доступа.

Примечание

Функции **Super User** («Суперпользователь»), **Extended Door Open Time** («Увеличенная продолжительность открытия двери»), **Add to Blacklist** («Добавление в черный список») и **Mark as Visitor** («Назначение в качестве посетителя») не могут быть включены одновременно. Например, если пользователь назначен в качестве суперпользователя, функции увеличенной продолжительности открытия двери, добавления в черный список и назначения в качестве посетителя будут недоступны.

6. Подтвердите, чтобы добавить пользователя.
   - Нажмите **Add** («Добавить») для добавления сотрудника/посетителя и закройте окно добавления.
   - Нажмите **Add and New** («Добавить и новый») для добавления сотрудника/посетителя и продолжения добавления других пользователей.

9.4.8 Редактирование информации о сотруднике/пользователе

Доступна настройка свойств дополнительной информации о сотруднике, которая предварительна не задана в системе. Например, можно указать место рождения сотрудника. После настройки свойств заполните информацию о сотруднике/пользователе.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Настройте поле пользовательской информации.
   1) Нажмите **Custom Property** («Пользовательские свойства»).
   2) Нажмите **Add** («Добавить») для добавления нового свойства.
   3) Введите название свойства.
   4) Нажмите **OK**.
3. Настройте пользовательскую информацию при добавлении сотрудника/пользователя.
   1) Выберите организацию из списка, чтобы добавить сотрудника/посетителя, и нажмите **Add** («Добавить»).

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике/посетителе. Более подробная информация о настройке основной информации о пользователе представлена в разделе ***«Настройка основной информации»***.

2) На панели **Custom Information** («Пользовательская информация») введите информацию о сотруднике/посетителе.
3) Нажмите **Add** («Добавить»), чтобы добавить сотрудника/посетителя, и закройте окно **Add Person** («Добавить сотрудника/посетителя»), или нажмите **Add and New** («Добавить и продолжить»), чтобы добавить сотрудника/посетителя и продолжить добавление других пользователей.

9.4.9 Настройка информации о жильце

Для связи с жильцом с помощью видеодомофона, необходимо установить номер комнаты и привязать ее к видеодомофону. Установив соединение, можно связаться с человеком через видеодомофон.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите организацию из списка и нажмите **Add** («Добавить»).

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике/посетителе. Более подробная информация о настройке основной информации о пользователе представлена в разделе ***«Настройка основной информации»***.

3. На панели **Resident Information** («Информация о жильце») выберите видеодомофон и привяжите его к конкретному пользователю.

Примечание

При выборе значения **Analog Indoor Station** («Аналоговый видеодомофон») будет отображено поле **Door Station** («Вызывная панель»), после чего необходимо будет выбрать вызывную панель для связи с аналоговым видеодомофоном.

4. Введите номер этажа и номер помещения пользователя.
5. Подтвердите, чтобы добавить пользователя.
   – Нажмите **Add** («Добавить») для добавления сотрудника/посетителя и закройте окно добавления.
   – Нажмите **Add and New** («Добавить и новый») для добавления сотрудника/посетителя и продолжения добавления других пользователей.

9.4.10 Настройка дополнительной информации

При добавлении пользователя можно настроить дополнительную информацию, такую как тип пользователя, номер пользователя, страна и т. д., в соответствии с фактическими значениями.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите организацию из списка и нажмите **Add** («Добавить»).

Примечание

В первую очередь необходимо добавить основную информацию о сотруднике/посетителе. Более подробная информация о настройке основной информации о пользователе представлена в разделе ***«Настройка основной информации»***.

3. На панели **Additional Information** («Дополнительная информация»), введите дополнительную информацию о пользователе, в том числе **ID type** («Тип ID»), **ID No.** («Номер ID »), **Job title** («Должность») и т. д.
4. Подтвердите, чтобы добавить пользователя.
   – Нажмите **Add** («Добавить») для добавления сотрудника/посетителя и закройте окно добавления.
   – Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

9.4.11 Импорт и экспорт информации о сотруднике/посетителе

Можно импортировать информацию и изображения нескольких пользователей в клиентское ПО в пакетном режиме. Также можно экспортировать информацию и изображения пользователей и сохранить их на компьютере.

9.4.12 Импорт информации о сотруднике/посетителе

Введите информацию о нескольких пользователях в предварительно настроенный шаблон (файл CSV / Excel) и импортируйте информацию в клиентское ПО в пакетном режиме.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите добавленную организацию из списка и нажмите **Add** («Добавить») в верхнем левом углу, чтобы добавить организацию, затем выберите эту организацию.
3. Нажмите **Import** («Импорт»), чтобы открыть соответствующую панель.
4. Выберите значение **Person Information** («Информация о сотруднике/посетителе») в поле **Importing Mode** («Режим импорта»).
5. Нажмите **Download Template for Importing Person** («Скачать шаблон для импорта сотрудника/посетителя»), чтобы скачать шаблон.

6. Введите информацию о пользователе в загруженный шаблон.

Примечание

- Если у пользователя несколько карт, отделите каждый номер карты точкой с запятой.
- Поля, отмеченные звездочкой, являются обязательными.
- По умолчанию **Hire Date** («Дата найма») является текущей датой.

7. Нажмите , чтобы выбрать файл CSV/Excel с информацией о пользователе с локального ПК.
8. Нажмите **Import** («Импорт») для начала импорта.

Примечание

- Если номер пользователя уже существует в базе данных клиента, удалите существующую информацию перед импортом.
- Можно импортировать информацию не более, чем о 2000 пользователях.

9.4.13 Импорт изображений сотрудников/посетителей

После импорта изображений лиц в клиентское ПО, пользователи на изображениях могут быть идентифицированы с помощью терминала доступа с функцией распознавания лиц. Можно импортировать изображения пользователей по одному или импортировать несколько изображений одновременно.

Перед началом

Не забудьте заранее импортировать информацию о пользователе в клиентское ПО.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите добавленную организацию из списка и нажмите **Add** («Добавить») в верхнем левом углу, чтобы добавить организацию, затем выберите эту организацию.
3. Нажмите **Import** («Импорт»), чтобы открыть соответствующую панель, затем выберите **Face** («Лицо»).
4. Опционально. Включите функцию **Verify by Device** («Проверка устройством»), чтобы проверить способность устройства распознавания лиц на клиентском ПО распознать лицо на фотографии.
5. Нажмите , чтобы выбрать файл с изображением лица.

Примечание

- Папка с изображениями лиц должна быть в формате ZIP.
- Изображение должно быть в формате JPG. Размер изображения не должен превышать 200 КБ.
- Название файла изображения должно формироваться в соответствии со следующим правилом: «Идентификатор сотрудника_Имя». Идентификатор пользователя должен

совпадать с идентификатором импортированного пользователя.

6. Нажмите **Import** («Импорт») для начала импорта.
   Прогресс и результат импорта будут отображены на экране.

9.4.14 Экспорт информации о сотруднике/посетителе

Экспортируйте данные о добавленном пользователе на локальный ПК в формате CSV/Excel.

Перед началом

Убедитесь, что пользователь добавлен в организацию.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Опционально. Выберите организацию из списка.

Примечание

Если не выбрать конкретную организацию, будет экспортирована информация обо всех пользователях.

3. Нажмите **Export** («Экспорт»), чтобы открыть соответствующую панель.
4. Выберите **Person Information** («Информация о сотруднике/посетителе») для экспорта.
5. Выберите параметры, которые необходимо экспортировать.
6. Нажмите **Export** («Экспорт»), чтобы сохранить экспортированный файл в формате CSV/Excel на ПК.

9.4.15 Экспорт изображений сотрудников/посетителей

Экспортируйте файл с изображением лиц добавленных сотрудников и сохраните его на компьютере.

Перед началом

Убедитесь, что пользователи и изображения их лиц добавлены в организацию.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Опционально. Выберите организацию из списка.

Примечание

Если не выбрать конкретную организацию, будут экспортированы изображения лиц всех пользователей.

3. Нажмите **Export** («Экспорт»), чтобы открыть соответствующую панель, затем выберите **Face** («Лицо»).

4. Нажмите **Export** («Экспорт») для начала экспорта.

Примечание

- Файл будет экспортирован в формате ZIP.
- Название файла экспортированного изображения должно формироваться в соответствии со следующим правилом: «Идентификатор сотрудника_Ф. И. О._0» («0» - для лица, видимого во всех деталях).

9.4.16 Удаление зарегистрированных изображений

Можно автоматически удалить файл с изображением лиц добавленных сотрудников/посетителей.

Перед началом

Убедитесь, что необходимые данные сохранены.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Опционально. Выберите сотрудника/посетителя из списка.
3. Нажмите **Delete Registered Picture** («Удалить зарегистрированное изображение»), чтобы удалить зарегистрированное изображение.

9.4.17 Получение информации о пользователе с устройства контроля доступа

Если добавленное устройство контроля доступа было дополнено информацией о пользователе (включая подробную информацию о пользователе и выданной карте), данную информацию можно получить с устройства и импортировать ее в клиент для дальнейшей работы.

Шаги

Примечание

- Если в информации о пользователе, хранящейся на устройстве, в поле **Name** («Имя») не указаны данные, то это поле будет заполнено номером выданной карты после импорта в клиентское ПО.
- По умолчанию задан пол: **Male** («Мужской»).
- Если номер карты или идентификатор пользователя (идентификатор сотрудника), который хранится на устройстве, уже существует в клиентской базе данных, пользователь с таким номером карты или идентификатором не будет импортирован в клиентское ПО.

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).

2. Выберите организацию для импорта сотрудников.
3. Нажмите **Get from Device** («Получить из устройства»).
4. Выберите добавленное устройство контроля доступа или настольный считыватель карт из выпадающего списка.

Примечание

При выборе настольного считывателя карт, нажмите **Login** («Войти»), затем установите IP-адрес, номер порта, имя пользователя и пароль.

5. Нажмите **Import** («Импорт») для начала импорта информации о пользователе в Клиентское ПО.

Примечание

Можно импортировать до 2000 пользователей и до 5000 карт.

Информация о пользователе, включая подробную информацию о пользователе и связанных картах (если настроены), будет импортирована в выбранную организацию.

9.4.18 Перемещение сотрудника/посетителя в другую организацию

При необходимости можно переместить пользователя в другую организацию.

Перед началом

- Необходимо предварительно добавить не менее 2 организаций.
- Импортируйте информацию о пользователе.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите организацию из списка на панели слева.
   Пользователи, добавленные в организацию, будут отображаться на панели справа.
3. Выберите пользователя, которого необходимо переместить.
4. Нажмите **Change Organization** («Изменить организацию»).
5. Выберите организацию, в которую нужно переместить пользователя.
6. Нажмите **OK**.

9.4.19 Выдача карт сотрудникам/посетителям в пакетном режиме

В клиентском ПО предусмотрена возможность выпустить сразу несколько карт в пакетном режиме.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Нажмите **Batch Issue Cards** («Выпуск карт в пакетном режиме»).
   На панели справа будут отображены все добавленные пользователи, для которых еще не

было выпущено ни одной карты.

3. Опционально. Введите ключевое слово (имя или идентификатор пользователя) в поле ввода информации, чтобы выделить пользователей, для которых необходимо выпустить карты.
4. Опционально. Нажмите **Settings** («Настройки»), чтобы установить параметры выпуска карт. Более подробная информация представлена в разделе ***«Выпуск карт в локальном режиме»***.
5. Нажмите **Initialize** («Инициализировать»), чтобы инициализировать считыватель карт и подготовить его к выдаче карт.
6. Нажмите на колонку **Card No.** («Номер карты») и введите номер карты.
   – Поместите карту на настольный считыватель.
   – Считайте карту через считыватель карт.
   – Вручную введите номер карты и нажмите **Enter** («Ввод»).

   Карты будут выпущены для пользователей, отображаемых в списке.

9.4.20 Уведомление о потере карты

В случае утери карты необходимо сообщить о потере для деактивации доступа с помощью утерянной карты.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите сотрудника, о потере карты которого необходимо сообщить, и нажмите **Edit** («Изменить»), чтобы открыть соответствующее окно.
3. На панели **Credential → Card** («Учетные данные → Карта»), нажмите  на добавленной карте, чтобы изменить ее статус на **Lost card** («Утерянная карта»).
   После уведомления об утере карты авторизация доступа по этой карте будет недействительной и неактивной. Если картой решит воспользоваться другой пользователь, он не сможет получить доступ к дверям, используя утерянную карту.
4. Опционально. Нажмите  , чтобы отменить уведомление о потере карты, если карта найдена.
   После отмены уведомления об утере карты, авторизация доступа по этой карте будет действительной и активной.
5. Если утерянная карта добавлена в группу доступа, которая применена к устройству, после сообщения об утере карты или отмене уведомления об утере карты появится окно с уведомлением о необходимости применить изменения к устройству. После применения к устройству эти изменения будут задействованы на устройстве.

9.4.21 Настройка параметров выпуска карт

Предусмотрено два режима считывания номера карты: с помощью настольного считывателя карт или считывателя карт устройства контроля доступа. Подключите настольный считыватель карт к ПК, на котором работает клиент, через USB или COM-интерфейс, затем поместите карту на настольный считыватель карт. При отсутствии настольного считывателя

карт считайте карту через считыватель карт добавленного устройства контроля доступа, чтобы получить номер карты. Перед выпуском карты для пользователя необходимо установить параметры выпуска карты, в том числе режим выпуска карт и сопутствующие параметры.

При добавлении карты нажмите **Settings** («Настройки»), чтобы открыть соответствующее окно.

Локальный режим: выпуск карт с помощью настольного считывателя карт

Подключите настольный считыватель карт к ПК, на котором работает клиент. Поместите карту на настольный считыватель для получения номера карты.

Настольный считыватель карт

Выберите модель подключенного настольного считывателя карт

Примечание

В настоящее время поддерживаются следующие модели считывателя карт: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E и DS-K1F180-D8E.

Тип карты

Это поле доступно только для моделей считывателя карт DS-K1F100-D8E или DS-K1F180-D8E.

Выберите тип карты: EM-карта или IC-карта в соответствии с фактическим типом карты.

Серийный интерфейс

Доступно только для модели DS-K1F100-M.

Выберите COM-интерфейс, к которому будет подключен настольный считыватель карт.

Бипер

После успешного считывания номера карты включите или выключите бипер.

Тип номера карты

Выберите необходимый тип номера карты.

Шифрование M1-карты

Это поле доступно только для моделей считывателя карт DS-K1F100-D8, DS-K1F100-D8E или DS-K1F180- D8E.

Если используется карта M1 и нужно активировать функцию ее шифрования, выберите соответствующий сектор.

Удаленный режим: выпуск карт с помощью считывателя карт

Выберите устройство контроля доступа, добавленное в клиент, и считайте карту через

считыватель карт, чтобы получить ее номер.

9.5 Настройка графиков и шаблонов

Настройте шаблон, в том числе недельный график работы и график выходных дней. После настройки шаблона, его можно использовать для настройки групп доступа, чтобы настройки указанной группы доступа были действительны во время действия шаблона.

Примечание

Более подробная информация о настройке группы контроля доступа представлена в разделе ***«Настройка группы контроля доступа для назначения разрешений на доступ»***.

9.5.1 Добавление выходных дней

Здесь можно установить выходные дни и настроить параметры выходных дней, в том числе дату начала, дату окончания и продолжительность указанного периода.

Шаги

Примечание

Можно добавить до 64 групп выходных дней.

1. Нажмите **Access Control → Schedule → Holiday** («Контроль доступа → Графики → Выходные дни»), чтобы перейти на соответствующую страницу.
2. На панели слева нажмите **Add** («Добавить»).
3. Создайте название для выходного дня.
4. Опционально. Введите описание или уведомления об этом выходном дне в поле **Remark** («Замечания»).
5. Добавьте период и настройте продолжительность выходных дней.

Примечание

Для одной группы выходного дня можно добавить до 16 периодов.

1) Нажмите **Add** («Добавить») в поле списка выходных дней.
2) Двигайте курсор, чтобы указать временной интервал. Для данного периода времени будет активировано настроенное разрешение.

Примечание

Для одного периода выходных может быть установлено до 8 временных интервалов.

3) Опционально. Для изменения временных интервалов выполните следующие действия.
   - Когда вид курсора изменится на , можно изменить длительность выбранного

отрезка времени, переместив курсор в необходимое положение.
- Наведите курсор на временную шкалу и измените время начала/окончания периода в появившемся диалоговом окне.
- Когда вид курсора изменится на  , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.

4) Опционально. Выберите отрезок времени, который необходимо удалить, а затем нажмите  в столбце **Operation** («Операции»), чтобы удалить его.
5) Опционально. Нажмите кнопку  в столбце **Operation** («Операции»), чтобы удалить все отрезки времени во временной шкале.
6) Опционально. Нажмите  в столбце **Operation** («Операции»), чтобы удалить добавленный выходной день из списка.

6. Нажмите **Save** («Сохранить»).

9.5.2 Добавление шаблона

Шаблон может содержать недельный график работы и график выходных дней. Установите недельный график работы и назначьте время авторизации доступа для конкретного пользователя или группы. Также можно выбрать добавленные выходные дни и включить их в шаблон.

Шаги

Примечание

Можно добавить до 255 шаблонов.

1. Нажмите **Access Control → Schedule → Template** («Контроль доступа → Графики → Шаблон»), чтобы перейти на соответствующую страницу.

Примечание

По умолчанию предусмотрено два вида шаблонов: **All-Day Authorized** («Авторизован в течение всего дня») и **All-Day Denied** («Доступ запрещен в течение всего дня»). Указанные шаблоны не подлежат редактированию или удалению.

Авторизован в течение всего дня

Авторизация действует в каждый день недели и не предусматривает выходных дней.

Доступ запрещен в течение всего дня

Авторизация не действует в течение недели и не предусматривает выходных дней.

2. На панели слева нажмите **Add** («Добавить»), чтобы создать новый шаблон.
3. Создайте название для шаблон.
4. Введите описание или уведомления об этом шаблоне в поле **Remark** («Замечания»).
5. Внесите изменения в недельный график и примените их к шаблону.
   1) Перейдите на вкладку **Week Schedule** («Недельный график работы») на панели снизу.
   2) Выберите день недели и укажите продолжительность на шкале времени.

Примечание

Для каждого дня в недельном графике может быть установлено до 8 временных интервалов.

3) Опционально. Для изменения временных интервалов выполните следующие действия.
   - Когда вид курсора изменится на  , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.
   - Наведите курсор на временную шкалу и измените время начала/окончания периода в появившемся диалоговом окне.
   - Когда вид курсора изменится на  , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
4) Повторите два последних действия выше, чтобы задать несколько временных интервалов в другие дни недели.

6. Добавьте выходной день и примените его к шаблону.

Примечание

В один шаблон можно добавить до 4 выходных дней.

1) Нажмите на вкладку **Holiday** («Выходной день»).
2) Выберите выходной день из списка слева, чтобы добавить его в выбранный список на панели справа.
3) Опционально. Нажмите **Add** («Добавить») для добавления нового выходного.

Примечание

Для получения подробной информации о добавлении выходных обратитесь к разделу «***Добавление выходных»***.

4) Опционально. Выберите выходной день из списка справа и нажмите  , чтобы удалить его, или нажмите **Clear** («Очистить»), чтобы удалить все выбранные выходные дни из списка справа.

7. Нажмите **Save** («Сохранить») для сохранения настроек и завершите добавление шаблона.

9.6 Настройка группы контроля доступа для назначения разрешений на доступ

После добавления пользователя и настройки его учетных данных можно создать группы контроля доступа, чтобы предоставить доступ к дверям для определенных пользователей. После этого необходимо применить группу контроля доступа к устройству контроля доступа, чтобы измененные настройки были задействованы.

Шаги

После изменения настроек группы доступа необходимо снова применить эти группы доступа к устройствам, чтобы изменения вступили в силу. Изменения в группе доступа включают в себя изменения шаблона, настроек группы доступа, настроек группы доступа пользователя и сведений о связанных лицах (включая № карты, отпечатки пальцев, изображения лиц, привязку № карты и отпечатков пальцев, пароль карты, срок действия карты и др.).

1. Нажмите **Access Control → Authorization → Access Group** («Контроль доступа → Авторизация → Группа доступа»), чтобы перейти на соответствующую страницу.
2. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
3. В текстовом поле **Name** («Имя») введите имя для группы доступа по своему выбору.
4. Выберите шаблон для группы доступа.

Примечание

Необходимо настроить шаблон перед настройкой группы доступа. Более подробная информация представлена в разделе ***«Настройка графиков и шаблонов»***.

5. В списке слева поля **Select Person** («Выбрать пользователя») выберите пользователей, которым необходимо назначить разрешения на доступ.
6. В списке слева поля **Select Person** («Выбрать пользователя») выберите двери, вызывные панели и этажи, к которым будут иметь доступ выбранные пользователи.
7. Нажмите **Save** («Сохранить»).
   Выбранные пользователи и точки доступа отображаются в правой части экрана.

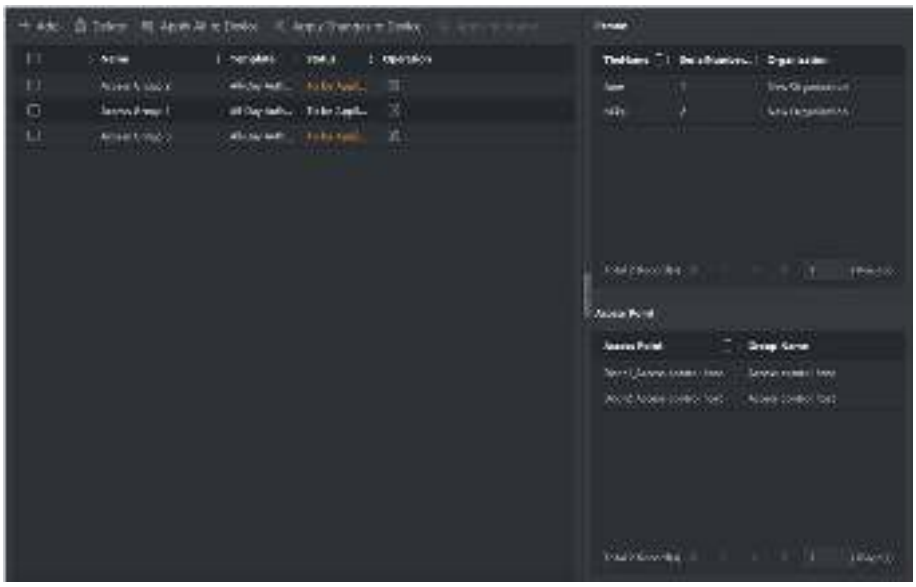


Рисунок 9-9. Отображение выбранных пользователей и точек доступа

8. После добавления группы доступа необходимо применить их к устройству контроля доступа, чтобы изменения были задействованы.
   1) Выберите группы доступа, которые необходимо применить к устройству контроля доступа.
   2) Нажмите **Apply to Devices** («Применить к устройствам») для начала применения выбранных групп доступа к устройству контроля доступа или вызывной панели.
   3) Нажмите **Apply to Devices** («Применить к устройствам») или **Apply Changes to Devices** («Применить изменения к устройствам»).

      Применить к устройствам

      Операция очистит все группы доступа, привязанные к выбранным устройствам, а затем задаст новую группу доступа.

      Применить изменения к устройствам

      Операция не очистит группы доступа, привязанные к выбранным устройствам и применит только измененную часть выбранных групп доступа к устройству.
   4) Присвоенный статус отображается в столбце **Status** («Статус»). Также можно нажать **Applying Status** («Присвоенный статус»), чтобы просмотреть все примененные группы доступа.

   Примечание

   Выберите **Display Failure Only** («Отображать только ошибки») для фильтрации примененных изменений.

   Выбранные пользователи будут иметь разрешения на вход/выход через выбранные двери/вызывные панели при помощи привязанных карт.
9. Опционально. При необходимости нажмите для редактирования групп доступа.

Примечание

При изменении информации о доступе пользователя или другой связанной информации появится предупреждение **Access Group to Be Applied** («Применить группу доступа») в правом углу.
Нажмите на подсказку для применения изменений к устройству. Выберите **Apply Now** («Применить сейчас») или **Apply Later** («Применить позже»).

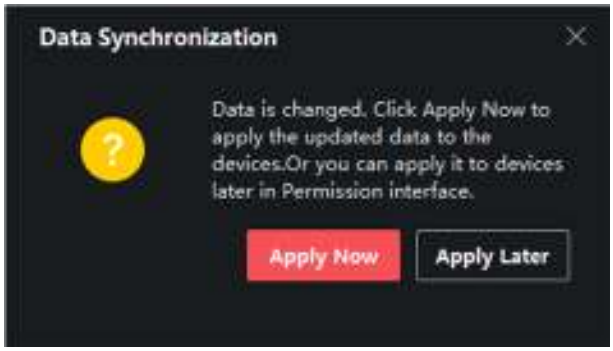


Рисунок 9-10. Синхронизация данных

9.7 Настройка расширенных функций

Настройте расширенные функции контроля доступа в соответствии со сценой наблюдения.

Примечание

- При использовании функций, связанных с картами (с картами контроля доступа), во время добавления карт будут перечислены только карты с примененной группой доступа.
- Устройство должно поддерживать возможность использования расширенных функций.
- Наведите курсор на **Advanced Function** («Расширенная функция»), затем нажмите для настройки расширенной функции.

9.7.1 Настройка параметров устройства

После добавления устройства контроля доступа можно настроить параметры устройства контроля доступа и точки управления доступом.

Настройка параметров устройства контроля доступа

После добавления устройства контроля доступа можно настроить его параметры, в том числе наложить пользовательскую информацию на изображение, загрузить изображения

после захвата, сохранить захваченные изображения и т. д.

Шаги

1. Нажмите **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»).

Примечание

Выберите **Device Parameter** («Параметры устройства») в списке расширенных функций, наведите курсор, а затем нажмите , чтобы отобразить параметры устройства.

2. Выберите устройство контроля доступа, чтобы отобразить его параметры на странице справа.
3. Нажмите **ON** («Вкл.»), чтобы включить соответствующую функцию.

Примечание

- Отображаемые параметры могут различаться в зависимости от устройства контроля доступа.
- Некоторые из следующих параметров не перечислены на странице **Basic Information** («Основная информация»), нажмите **More** («Дополнительная информация»), чтобы изменить параметры.

Голосовое предупреждение

Активируйте эту функцию для включения голосовых предупреждений. Устройство будет воспроизводить голосовые предупреждения во время своей работы.

Загрузка изображения после захвата

Если эта функция активирована, изображения, захваченные соответствующей камерой, будут автоматически загружаться в систему.

Сохранение изображения после связанного захвата

Если эта функция активирована, можно сохранять изображения, захваченные камерой, связанной с устройством.

Режим распознавания лиц

Обычный режим

Распознавание лиц с помощью камеры в обычном режиме.

Режим распознавания на основе алгоритмов глубокого обучения

Устройство распознает более широкий диапазон лиц в сравнении с обычным режимом. Этот режим рекомендуется применять при сложных условиях эксплуатации.

Активация распознавания NFC-карты

После активации этой функции устройство сможет распознавать NFC-карты. Поднесите NFC-карту к устройству.

Активация распознавания M1-карты

После активации этой функции устройство сможет распознавать M1-карты. Поднесите M1-карту к устройству.

Активация распознавания EM-карты

После активации этой функции устройство сможет распознавать EM-карты. Поднесите EM-карту к устройству.

Примечание

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

4. Нажмите **OK**.
5. Опционально. Нажмите **Copy to** («Копировать в...») и выберите устройство контроля доступа, чтобы копировать параметры, указанные на странице, на выбранное устройство.

Настройка параметров дверей/лифтов

После добавления устройства контроля доступа можно настроить параметры его точки доступа (двери).

Шаги

1. Нажмите **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»).
2. Выберите устройство контроля доступа на панели слева, а затем нажмите , чтобы показать двери или этажи выбранного устройства.
3. Выберите дверь или этаж, чтобы отобразить его параметры в правой части экрана.
4. Измените параметры двери или этажа.

Примечание

- Отображаемые параметры могут различаться в зависимости от устройства контроля доступа.
- Некоторые из следующих параметров не перечислены на странице **Basic Information** («Основная информация»), нажмите **Advanced** («Расширенные функции»), чтобы изменить параметры.

Наименование

Выберите наименование считывателя карт по своему выбору.

Дверной контакт

Установите датчик двери в режим **Remaining closed** («Оставить открытым») или **Remaining open** («Оставить закрытым»). По умолчанию активирован режим **Remaining closed** («Оставить открытым»).

Тип кнопки выхода

Установите кнопку выхода в режим **Remaining closed** («Оставить открытым») или **Remaining open** («Оставить закрытым»). По умолчанию активирован режим **Remaining open** («Оставить закрытым»).

Длительность открытого состояния

После считывания обычной карты и срабатывания реле запускается таймер для блокировки двери.

Увеличение длительности открытого состояния

Дверной контакт может быть активирован с установленной задержкой после считывания карты пользователя с расширенным доступом.

Тревога тайм-аута открытой двери

Тревога сработает, если дверь не будет закрыта в течение заданного периода времени. Тревога не сработает, если установлено значение «0».

Код принуждения

Дверь может быть открыта при помощи кода принуждения. В тоже время клиент создает уведомление о событии принуждения.

Суперпароль

Пользователь может открыть дверь с помощью суперпароля.

Примечание

- Суперпароль должен отличаться от кода принуждения.
- Суперпароль и код принуждения должны отличаться от пароля аутентификации.
- Длина суперпароля и кода принуждения установлена устройством. Обычно пароль должен содержать от 4 до 8 цифр.

5. Нажмите **OK**.
6. Опционально. Нажмите **Copy to** («Копировать в...») и выберите устройство контроля доступа, чтобы копировать параметры, указанные на странице, на выбранное устройство.

Примечание

Настройки состояния двери будут также применены к выбранной двери.

Настройка параметров считывателя карт

После добавления устройства контроля доступа можно настроить параметры его

считывателя карт.

Шаги

1. Нажмите **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»).
2. Нажмите кнопку ▪ в списке устройств, расположенном слева, чтобы развернуть на экране информацию о двери, выберите считыватель карт и измените его параметры справа.
3. Затем измените основные параметры данного устройства, приведенные на соответствующей странице.

Примечание

- Отображаемые параметры могут различаться в зависимости от устройства контроля доступа. Ниже приведены некоторые параметры. Для подробной информации обратитесь к руководству пользователя устройства.
- Некоторые из следующих параметров не перечислены на странице **Basic Information** («Основная информация»), нажмите **Advanced** («Расширенные функции»), чтобы изменить параметры.

Основная информация

Наименование

Выберите наименование считывателя карт по своему выбору.

Минимальный интервал считывания карты

Если интервал считывания одной и той же карты меньше установленного значения, считывание карты будет недействительным. Можно задать данное значение в диапазоне от 0 до 255.

Запуск тревоги при достижении максимального количества неудачных попыток считывания карты

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

Тип считывателя карт/Описание считывателя карт

Просмотр типа и описания считывателя карт. Доступны только для чтения.

Расширенные функции

Включить считыватель карт

Включите эту функцию, чтобы использовать устройство в качестве считывателя карт.

Правильная полярность светодиода/Ошибочная полярность светодиода/Полярность бипера

Настройте **OK LED Polarity** («Правильная полярность светодиода»)/**Error LED Polarity** («Ошибочная полярность светодиода»)/**Buzzer Polarity** («Полярность бипера») основной платы в соответствии с параметрами считывателя карт. Как правило, устройство получает настройки по умолчанию.

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 пользователь нажал до этого, будут автоматически удалены.

Тревога тампера

Включите детектор саботажа на считывателе карт.

Связь с панелью управления

Установите максимальное количество неудачных попыток считывания карты.

Пороговое значение для распознавания 1:N

Настройте пороговое значение совпадения при аутентификации в режиме сопоставления 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений, и тем больше вероятность отклонений ложных совпадений при аутентификации.

Интервал распознавания лиц

Временной интервал между двумя циклами распознавания лиц при непрерывной работе. По умолчанию значение составляет 2 с.

Детекция подлинности биометрических данных лица (антиспуфинг)

Здесь можно включить/выключить функцию детекции лиц. При включении этой функции устройство сможет отличать сотрудника/посетителя от изображения.

Режим применения

Выберите режим **Indoor** («Использование внутри помещения») или **Others** («Другое») в соответствии с фактической ситуацией.

Блокировка лица, не прошедшего аутентификацию

После включения функции **Live Face Detection** («Детекция лиц в режиме реального времени») система заблокирует лицо пользователя на 5 минут, если количество попыток обнаружения лица превышает установленное значение. После неудачных попыток аутентификации пользователь будет заблокирован на 5 минут. Для разблокировки пользователь должен успешно пройти аутентификацию два раза в течение 5 минут.

Уровень безопасности антиспуфинга

После включения функции антиспуфинга можно установить надлежащий уровень безопасности при выполнении аутентификации лица в режиме реального времени.

4. Нажмите **OK**.
5. Опционально. Нажмите **Copy to** («Копировать в...») и выберите считыватель карт, чтобы копировать параметры, указанные на странице, на выбранное устройство.

9.7.2 Настройка параметров «Оставить открытой» / «Оставить закрытой»

Настройте состояние двери: **Open** («Открыта») или **Closed** («Закрыта»). Например, можно перевести дверь в состояние **Remaining closed** («Оставить закрытой») в праздничные дни или в состояние **Remaining open** («Оставить открытой») в указанный период рабочего дня.

Перед началом

Добавьте устройство контроля доступа в систему.

Шаги

1. Нажмите **Access Control → Advanced Function → Remain Open/Closed** («Контроль доступа → Расширенные функции → Оставить открытой/закрытой»), чтобы перейти на соответствующую страницу.
2. Выберите дверь, параметры которой необходимо настроить, на панели слева.
3. Для настройки состояния двери в течение рабочего дня нажмите **Week Schedule** («График рабочей недели») и выполните следующие действия.
   1) Нажмите **Remain Open** («Оставить открытой») или **Remain Closed** («Оставить закрытой»).
   2) Двигайте курсор, чтобы указать временной интервал. Для данного периода времени будет активировано настроенное разрешение.

   Примечание

   Для каждого дня в недельном графике может быть установлено до 8 временных интервалов.

   3) Опционально. Для изменения временных интервалов выполните следующие действия.
      - Когда вид курсора изменится на  , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.
      - Наведите курсор на временную шкалу и измените время начала/окончания периода в появившемся диалоговом окне.
      - Когда вид курсора изменится на  , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
   4) Нажмите **Save** («Сохранить»).

   Сопутствующие операции

Применить ко всей неделе	Выберите временной интервал на шкале времени и нажмите **Copy to Whole Week** («Применить ко всей неделе»), чтобы применить настройки ко всем дням недели.

Удалить выбранные интервалы	Выберите временной интервал на шкале времени и нажмите **Delete Selected** («Удалить выбранные интервалы»), чтобы удалить временной интервал.
Очистить	Нажмите **Clear** («Очистить»), чтобы очистить все настройки временных интервалов в недельном графике.

4. Для настройки состояния двери в течение выходного дня нажмите **Holiday** («Выходной день») и выполните следующие действия.
   1) Нажмите **Remain Open** («Оставить открытой») или **Remain Closed** («Оставить закрытой»).
   2) Нажмите **Add** («Добавить»).
   3) Введите дату начала и дату окончания периода.
   4) Двигайте курсор, чтобы указать временной интервал. Для данного периода времени будет активировано настроенное разрешение.

> **Примечание**
>
> Для одного периода выходных может быть установлено до 8 временных интервалов.

   5) Для изменения временных интервалов выполните следующие действия.
      - Когда вид курсора изменится на , можно изменить длительность выбранного отрезка времени, переместив курсор в необходимое положение.
      - Наведите курсор на временную шкалу и измените время начала/окончания периода в появившемся диалоговом окне.
      - Когда вид курсора изменится на , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
   6) Опционально. Выберите отрезок времени, который необходимо удалить, а затем нажмите в столбце **Operation** («Операции»), чтобы удалить его.
   7) Опционально. Нажмите кнопку в столбце **Operation** («Операции»), чтобы удалить все отрезки времени во временной шкале.
   8) Опционально. Нажмите в столбце **Operation** («Операции»), чтобы удалить добавленный выходной день из списка.
   9) Нажмите **Save** («Сохранить»).
5. Опционально. Нажмите **Copy to** («Скопировать в...»), чтобы применить настройки состояния двери к другим дверям.

9.7.3 Настройка многофакторной аутентификации

Настройте управление пользователями по группам и установите аутентификацию для нескольких пользователей в одной точке контроля доступа (двери).

Перед началом

Установите группу доступа и примените ее к устройству контроля доступа. Более подробная информация представлена в разделе ***«Настройка группы контроля доступа для назначения разрешений на доступ»***.

Выполните следующие действия, чтобы настроить аутентификацию сразу нескольких карт для одной точки контроля доступа (двери).

Шаги

1. Нажмите **Access Control → Advanced Function → Multi-Factor Auth** («Контроль доступа → Расширенные функции → Многофакторная аутентификация»).
2. Выберите устройство контроля доступа из списка слева.
3. Добавьте пользователя/группу карт для устройства контроля доступа.
   1) На панели справа нажмите **Add** («Добавить»).
   2) Создайте имя для группы по своему усмотрению.
   3) Укажите время начала и время окончания периода действия разрешения для пользователя/группы карт.
   4) Выберите доступных членов группы и карты из списка, чтобы добавить их в выбранный список.

      Примечание

      Карта должна быть предварительно выпущена для пользователя.
      Предварительно установите группу доступа и примените ее к устройству контроля доступа.

   5) Нажмите **Save** («Сохранить»).
   6) Опционально. Выберите пользователя/группу карт, затем нажмите **Delete** («Удалить»), чтобы удалить их.
   7) Опционально. Выберите пользователя/ группы карт и нажмите **Apply** («Применить»), чтобы повторно применить группу доступа, которую ранее не удалось применить к устройству контроля доступа.
4. Выберите точку контроля доступа (дверь) выбранного устройства на панели слева.
5. Введите максимальный интервал времени при вводе пароля.
6. Добавьте группу аутентификации для выбранной точки контроля доступа.
   1) На панели **Authentication Groups** («Группы аутентификации») нажмите **Add** («Добавить»).
   2) Из выпадающего списка выберите настроенный шаблон в качестве шаблона аутентификации.

      Примечание

      Для настройки шаблона обратитесь к разделу ***«Настройка графиков и шаблонов»***.

   3) Выберите тип аутентификации из выпадающего списка **Local Authentication** («Локальная аутентификация»), **Local Authentication and Remotely Open Door** («Локальная аутентификация и удаленное открытие двери») или **Local Authentication and Super Password** («Локальная аутентификация и пароль суперпользователя»).

      Локальная аутентификация

      Аутентификация с помощью устройства контроля доступа.

Локальная аутентификация и удаленное открытие двери

Аутентификация через устройство контроля доступа и клиентское ПО. После считывания карты появится окно. Дверь может быть разблокирована через клиентское ПО.

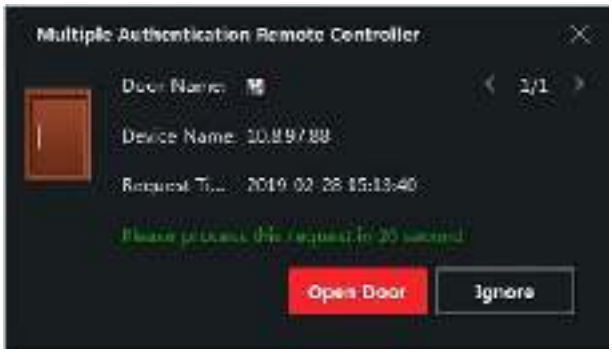


Рисунок 9-12. Удаленное открытие двери

Примечание

Выберите **Offline Authentication** («Автономная аутентификация»), чтобы активировать функцию аутентификации по суперпаролю, если устройство контроля доступа было отключено от клиентского ПО.

Локальная аутентификация и суперпароль

Аутентификация с помощью устройства контроля доступа и суперпароля.

4) Выберите добавленного пользователя/группу карт из списка слева внизу экрана, чтобы добавить его в список в качестве группы аутентификации.
5) Нажмите на добавленную группу аутентификации в списке справа, чтобы установить количество попыток аутентификации в столбце **Auth Times** («Количество попыток считывания карты»).

Примечание

- Количество попыток считывания карты должно быть больше 0 и не превышать количество добавленных пользователей в соответствующей группе.
- Максимальное значение данного параметра составляет 16.

6) Нажмите **Save** («Сохранить»).

Примечание

- Для каждой точки контроля доступом (дверей) можно добавить до 4 групп аутентификации.
- В группу аутентификации с типом **Local Authentication** («Локальная аутентификация») можно добавить до восьми пользователей/групп карт.
- В группу аутентификации с типом **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.

7. Нажмите **Save** («Сохранить»).

9.7.4 Настройка режима аутентификации и расписания считывателя карт

Установите правила прохождения через контрольные пункты для считывателя карт устройства контроля доступа.

Шаги

1. Нажмите **Access Control → Advanced Function → Authentication** («Контроль доступа → Расширенные функции → Аутентификация»), чтобы перейти на соответствующую страницу.
2. На панели слева выберите считыватель карт, который необходимо настроить.
3. Установите режим аутентификации для считывателя карт.
   1) Нажмите **Configuration** («Настройки»).

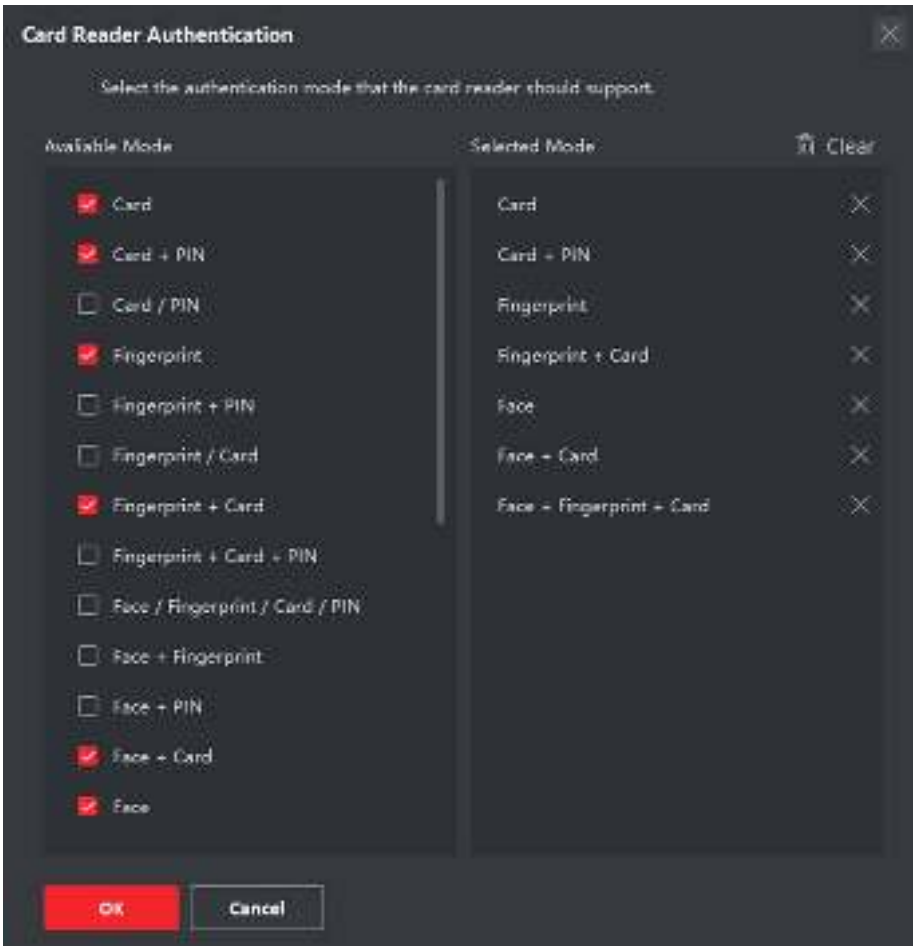


Рисунок 9-13. Выбор режима аутентификации для считывателя карт

Примечание

PIN означает PIN-код, установленный для разблокировки двери. Более подробная информация представлена в разделе ***«Настройка информации по контролю доступа»***.

2) Выберите режим из списка доступных режимов, чтобы добавить его в список выбранных режимов.
3) Нажмите **OK**.
   После завершения процедуры выбора режимов, они будут отображаться на экране в виде значков.

4. Нажмите на значок, чтобы выбрать режим аутентификации устройства для считывания карт. Проведите курсором 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.

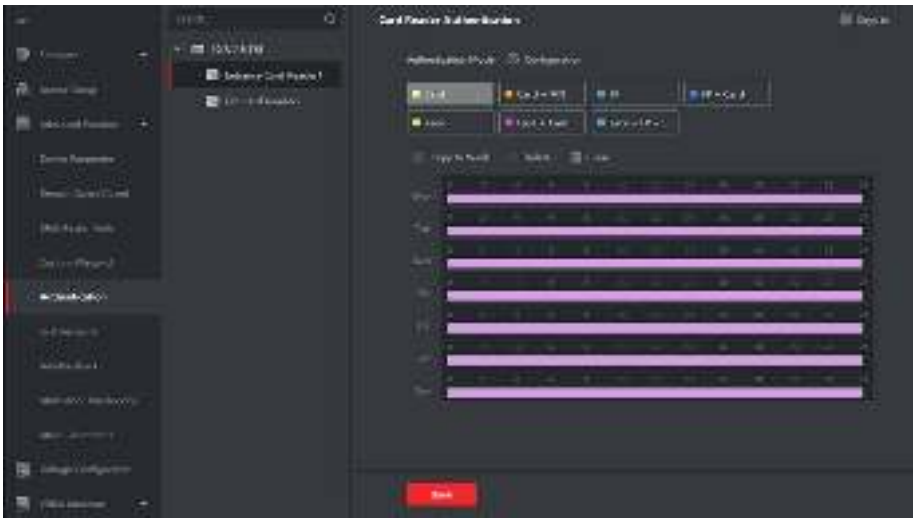


Рисунок 9-14. Настройка режима аутентификации для считывателей карт

6. Опционально. Выберите настроенный день и нажмите кнопку **Copy to Week** («Применить ко всем дням недели»), чтобы применить эти настройки ко всем дням недели.
7. Опционально. Нажмите **Copy to (**«Копировать в...»), для копирования настроек в другие считыватели карт.
8. Нажмите **Save** («Сохранить»).

9.7.5 Настройка аутентификации первого пользователя

Для одной точки контроля доступа можно назначить несколько первых пользователей. После авторизации первого пользователя несколько других пользователей получат доступ к дверям и разрешения на другие действия.

Перед началом

Установите группу доступа и примените ее к устройству контроля доступа. Более подробная информация представлена в разделе ***«Настройка группы контроля доступа для назначения разрешений на доступ»***.

Для настройки параметров разблокировки двери с помощью авторизации в качестве первого пользователя выполните следующие действия.

Шаги

1. Нажмите **Access Control → Advanced Function → First Person In** («Контроль доступа → Расширенные функции → Аутентификация первого пользователя»), чтобы перейти на соответствующую страницу.
2. Выберите устройство контроля доступа из списка слева.
3. Из выпадающего списка выберите режим для каждого устройства: **Enable Remaining Open after First Person** («Активировать функцию, при которой дверь остается открытой после аутентификации первого пользователя») или **Disable Remaining Open after First Person** («Деактивировать функцию, при которой дверь остается открытой после аутентификации первого пользователя»).

Активировать функцию, при которой дверь остается открытой после аутентификации первого пользователя

После авторизации первого сотрудника/посетителя дверь остается открытой в течение заданного промежутка времени и до истечения оставшегося времени открытия. При выборе этого режима необходимо установить длительность открытого состояния двери.

Примечание

Допустимый диапазон длительности открытого состояния двери: от 0 до 1440 минут. По умолчанию длительность открытого состояния составляет 10 минут.

Выключение функции, при которой дверь остается открытой после аутентификации первого пользователя

Выключение функции аутентификации первого пользователя.

Примечание

Чтобы отключить режим авторизации после первого лица, необходимо выполнить повторную авторизацию первого лица.

4. В списке **First Person** («Первый пользователь») нажмите **Add** («Добавить»).
5. Выберите пользователей из списка слева, чтобы добавить их к выбранным пользователям в качестве первого пользователя дверей.
   Добавленные первые пользователи будут перечислены в списке первых пользователей.
6. Опционально. Выберите пользователя из списка и нажмите **Delete** («Удалить»), чтобы удалить пользователя из списка первых пользователей.
7. Нажмите **Save** («Сохранить»).

9.7.6 Настройка запрета двойного прохода

Функция «Запрет двойного прохода» разработана для минимизации неправомерного или мошеннического использования учетных данных для доступа, таких как передача карты несанкционированному сотруднику/посетителю или проход нескольких сотрудников/посетителей по одним учетным данным друг за другом. Функция «Запрет двойного прохода» устанавливает особую последовательность использования учетных данных для доступа для предоставления доступа. С помощью клиента можно задать последовательность в соответствии с фактическим путем, и если сотрудник/посетитель использует учетные данные в неправильной последовательности, можно сбросить соответствующие записи.

Перед началом

Добавьте устройство контроля доступа в клиенту и включите функцию запрета двойного прохода по маршруту.

Шаги

Примечание

Для устройства контроля доступа можно одновременно настроить функцию запрета двойного прохода или блокировки нескольких дверей. Информация о настройке функции блокировки нескольких дверей представлена в соответствующем разделе.

1. Нажмите **Access Control → Advanced Function → Anti-Passback** («Контроль доступа → Расширенные функции → Запрет двойного прохода»), чтобы перейти на соответствующую страницу.
2. Выберите устройство контроля доступа на панели слева.
3. Выберите считыватель карт в качестве точки начала маршрута в поле **First Card Reader** («Первый считыватель карт»).
4. Нажмите на выбранный считыватель карт в колонке **Card Reader Afterward** («Следующий считыватель карт»), чтобы открыть выбранный считыватель карт.
5. Выберите считыватель карт, который следует за первым считывателем карт.

Примечание

Для одного считывателя карт можно добавить до 4 последующих считывателей карт.

6. В диалоговом окне нажмите **OK**, чтобы сохранить выбранные настройки.
7. На странице функции запрета двойного прохода нажмите **Save** («Сохранить») для сохранения настроек и их применения.

Пример

Установите маршрут считывания карты. Выберите Reader In_01 в качестве начала маршрута, а Reader In_02, Reader Out_04 в качестве связанных считывателей карт. После этого пользователь сможет пройти через точку контроля доступа, считав карту в следующей последовательности: Reader In_01, Reader In_02 и Reader Out_04.

8. Нажмите **Reset Anti-Passback** («Сброс запрета двойного прохода») и выберите сотрудника/посетителя, чтобы удалить соответствующие записи запрета двойного прохода на устройстве.

Примечание

Устройство должно поддерживать данную функцию.

9.7.7 Настройка параметров устройства

После добавления устройства контроля доступа можно настроить параметры его сети.

Настройка параметров нескольких сетевых плат

Если устройство поддерживает несколько сетевых интерфейсов, можно установить сетевые

параметры этих сетевых плат через клиент, а именно IP-адрес, MAC-адрес, номер порта и т. д.

Перед началом

Добавьте устройство контроля доступа в клиент и убедитесь, что устройство поддерживает несколько сетевых плат.

Шаги

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации слева перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа из списка устройств и нажмите NIC, чтобы открыть страницу настроек параметров нескольких сетевых плат.
4. Из выпадающего списка выберите NIC, который необходимо настроить.
5. Установите его сетевые параметры, такие как IP-адрес, шлюз по умолчанию, маска подсети и т. д.

   MAC-адрес

   MAC-адрес - это уникальный идентификатор, назначаемый сетевому интерфейсу для связи в физическом сегменте сети.

   MTU

   MTU - это максимальный объем данных, передаваемый по сети без дальнейшего фрагментирования.
6. Нажмите **Save** («Сохранить»).

Настройка параметров сети

После добавления устройства контроля доступа можно установить режим загрузки журнала устройства и создать учетную запись ISUP через проводную сеть.

Настройка режима загрузки журнала

Настройте режим загрузки журнала через протокол ISUP.

Шаги

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации слева перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа из списка устройств и перейдите **Network → Uploading Mode** («Сеть → Режим загрузки»).
4. Выберите центральную группу из выпадающего списка.
5. Нажмите **Enable** («Включить»), чтобы включить настройку режима загрузки.
6. Выберите режим загрузки из выпадающего списка.
   – Включите **N1** или **G1** для основного канала.

Выберите **Close** («Закрыть»), чтобы отключить основной канал.

7. Нажмите **Save** («Сохранить»).

Создание учетной записи ISUP через проводную сеть.

Создайте учетную запись для протокола ISUP через проводную сеть. После этого можно добавить устройства через протокол ISUP.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации слева перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа из списка устройств и перейдите во вкладку **Network → Network Center** («Сеть → Сетевой центр»).
4. Выберите центральную группу из выпадающего списка.
5. Укажите тип адреса **IP Address** («IP-адрес») или **Domain Name** («Доменное имя»).
6. Введите IP-адрес или доменное имя в соответствии с типом адреса.
7. Введите номер порта для протокола.

Примечание

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

8. Выберите **ISUP** в качестве типа протокола.

Примечание

При ISUP версии 5.0 необходимо создать ключ ISUP для учетной записи ISUP.

9. Укажите имя учетной записи сетевого центра.
10. Нажмите **Save** («Сохранить»).

Настройка параметров захвата изображений

Настройте параметры захвата изображений устройства контроля доступа, включая захват изображений вручную и захват по событию.

Примечание

- Устройство должно поддерживать функцию захвата изображений.
- Перед настройкой параметров захвата необходимо назначить хранилище изображений, в которое будут сохраняться изображения, захваченные по событию. Более подробная информация представлена в разделе «*Назначение хранилища изображений*» Руководства пользователя клиентского программного обеспечения.

Настройка параметров захвата изображений по событию

При возникновении события камера устройства контроля доступа сработает для захвата изображения (изображений), связанного с событием. Просмотрите захваченные изображения при проверке деталей события в центре событий. Перед этим необходимо установить параметры захвата изображения, в том числе количество снимков, сделанных за один раз.

Перед началом

Перед настройкой параметров захвата необходимо назначить хранилище изображений, в которое будут сохраняться изображения, захваченные по событию. Более подробная информация представлена в разделе «*Назначение хранилища изображений»* Руководства пользователя клиентского программного обеспечения.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации слева перейдите на **Advanced Function → More Parameters → Capture** («Расширенные функции → Прочие параметры → Захват изображения»).
3. Выберите устройство контроля доступа из списка устройств и выберите **Linked Capture** («Захваченные изображения, связанные с событиями»).
4. Установите размер и разрешение изображения.
5. Установите количество захваченных изображений за один раз после запуска.
6. Если количество захваченных изображений больше 1, установите временной интервал для каждого захвата.
7. Нажмите **Save** («Сохранить»).

Настройка параметров захвата изображений вручную

В модуле мониторинга состояния устройства можно сделать снимок вручную с помощью камеры устройства контроля доступа. Перед этим необходимо установить параметры для захвата изображений, в том числе разрешение изображения.

Перед началом

Перед настройкой параметров захвата необходимо назначить хранилище изображений, в которое будут сохраняться изображения, захваченные по событию. Более подробная информация представлена в разделе «*Назначение хранилища изображений»* Руководства пользователя клиентского программного обеспечения.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации слева перейдите на **Advanced Function → More Parameters → Capture** («Расширенные функции → Прочие параметры → Захват изображения»).
3. Выберите устройство контроля доступа из списка устройств и выберите **Manual Capture** («Захват изображений вручную»).
4. Выберите разрешение захваченных изображений из выпадающего списка.
5. Выберите качество изображения: **High** («Высокое»), **Medium** («Среднее») или **Low** («Низкое»). Чем выше качество изображения, тем больше его размер.
6. Нажмите **Save** («Сохранить»).

Настройка параметров терминала доступа с функцией распознавания лиц

Установите параметры настроек для терминала доступа с функцией распознавания лиц, в том числе базу данных изображений лиц, аутентификацию по QR-коду и т. д.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации слева перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа из списка и нажмите на иконку **Face Recognition Terminal** («Терминал доступа с функцией распознавания лиц»).
4. Настройте параметры.

Примечание

Отображаемые параметры могут отличаться в зависимости от модели.

Алгоритм

Выберите **Deep Learning** («Глубокое обучение») в качестве базы данных изображений лиц.

Сохранение изображений, захваченных при аутентификации

При включении этой функции изображения, захваченные при аутентификации, будут сохраняться на устройстве.

ЭКО-режим

После включения ЭКО-режима устройство будет аутентифицировать лица в условиях низкой освещенности или в темноте. Настройте пороговое значение для ЭКО-режима, ЭКО-режима (1:N) и ЭКО-режима (1:1).

ЭКО-режим (1:N)

Настройте пороговое значение совпадения при аутентификации в ЭКО-режиме 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений, и тем больше вероятность отклонений ложных совпадений.

Пороговое значение ЭКО-режима

Установите пороговое значение для ЭКО-режима при включении функции. Чем больше значение, тем быстрее устройство переключается в ЭКО-режим. Доступный диапазон: от 0 до 8.

Рабочий режим

Установите режим работы устройства: **Access Control Mode** («Режим контроля доступа»). Режим контроля доступа является нормальным режимом работы устройства. Для получения доступа необходимо пройти аутентификацию с использованием учетных данных.

5. Нажмите **Save** («Сохранить»).

Настройка параметров RS-485

Установите параметры RS-485 устройства контроля доступа, включая скорость передачи данных, бит данных, стоповый бит, тип контроля четности, тип управления потоком, режим связи, режим работы и режим соединения.

Шаги

Примечание

Настройки RS-485 должны поддерживаться устройством.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации слева перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа в списке устройств и нажмите **RS-485**, чтобы открыть страницу настроек RS-485.
4. Из выпадающего списка выберите номер серийного интерфейса, чтобы настроить параметры RS-485.
5. Задайте серийный номер, внешнее устройство, центр аутентификации, скорость передачи данных, бит данных, стоповый бит, тип четности, тип управления потоком, режим связи и рабочий режим.
6. Нажмите **Save** («Сохранить»).
   - Настроенные параметры будут автоматически применены к устройству.

- При изменении режима работы или режима подключения устройство автоматически перезагрузится.

Включить шифрование M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

Шаги

Примечание

Эта функция должна поддерживаться устройством контроля доступа и считывателем карт.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации слева перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа в списке устройств и нажмите **M1 Card Encryption Verification** («Верификация шифрования M1-карты»), чтобы открыть страницу верификации шифрования M1-карты.
4. Установите переключатель в положение **On** («Вкл.»), чтобы включить функцию шифрования M1-карты.
5. Установите идентификатор сектора.

Примечание

- Диапазон яркости от 1 до 100.
- По умолчанию сектор 13 зашифрован. Рекомендуется зашифровать сектор 13.

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

Настройка параметров интерфейса Wiegand

Установите канал Wiegand устройства контроля доступа и режим связи. После настройки параметров Wiegand устройство может подключиться к считывателю карт Wiegand по протоколу коммуникации Wiegand.

Перед началом

Добавьте устройство управления доступом к клиенту и убедитесь, что оно поддерживает Wiegand.

Шаги

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации слева перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа в списке устройств и нажмите **Wiegand**, чтобы открыть страницу настроек Wiegand.

4. Установите переключатель в положение **ON** («ВКЛ.») для включения функции Wiegand на устройстве.
5. Выберите номер канала Wiegand и необходимое значение из выпадающего списка.

Примечание

При настройке **Communication Direction** («Направление связи») в качестве **Sending** («Отправка») необходимо установить режим Wiegand в значение Wiegand 26 или Wiegand 34.

6. Нажмите **Save** («Сохранить»).
   - Настроенные параметры будут автоматически применены к устройству.
   - После изменения направления коммуникации устройство автоматически перезагрузится.

9.8 Настройка действий привязки для устройств контроля доступа

Настройте параметры для действий, связанных с обнаружением события с помощью устройства контроля доступа. Привязанные действия будут запущены после обнаружения события. Этот механизм используется для уведомления сотрудников службы безопасности о событии или запуска автоматического контроля доступа в режиме реального времени.

Поддерживаются два типа привязанных действий:

- **Действия на клиентском ПО.** При обнаружении тревожного события на клиентском ПО будут запущены привязанные действия, в том числе выдача звуковых предупреждений.
- **Действия на устройстве.** При обнаружении тревожного события на устройстве будут запущены привязанные действия, а именно запускается бипер и открываются/закрываются двери.

9.8.1 Настройка действий на клиентском ПО при событии доступа

Даже находясь далеко от точки доступа можно отслеживать события через клиент, настроив действия клиента для события доступа. Действия клиента представляют собой действия, автоматически выполняемые самим клиентом, например, создание звукового предупреждения и отправка электронного письма. При обнаружении тревожного события клиент уведомляет персонал службы безопасности, чтобы были приняты своевременные меры.

Перед началом

Добавьте устройство контроля доступа в клиент.

Шаги

1. Нажмите **Event Configuration→ Access Control Event** («Настройки события → Событие доступа»).
   Добавленные устройства контроля доступа отобразятся в списке.
2. Выберите ресурс (включая устройство, тревожный вход, дверь и считыватель карт) из списка устройств.
   На экране отобразятся типы событий, которые поддерживают выбранный ресурс.
3. Выберите событие (события) и нажмите **Edit Priority** («Изменить приоритет»), чтобы установить приоритет события (событий), который можно использовать для фильтрации событий в центре событий.
4. Установите действия, привязанные к событию.
   1) Выберите событие и нажмите **Edit Linkage** («Изменить привязку»), чтобы настроить действия клиентского ПО при возникновении события.

      Звуковое предупреждение

      Клиентское программное обеспечение выдает звуковое предупреждение при обнаружении тревожного события. Можно выбрать сигнал для звукового предупреждения.

      Примечание

      Более подробная информация о настройке звукового сигнала тревоги представлена в разделе «*Настройка звукового сигнала*» Руководства пользователя клиентского программного обеспечения.

      Отправка Email

      Отправьте уведомление о тревожном событии на электронную почту одному или нескольким получателям.
      Более подробная информация о настройке параметров электронной почты представлена в разделе *«Настройка параметров электронной почты*» Руководства пользователя клиентского программного обеспечения.

   2) Нажмите **OK**.
5. Обнаруженное тревожное событие будет отправлено в клиентское ПО, которое запустит настроенные действия.
6. Опционально. Нажмите **Copy to** («Копировать в...»), чтобы скопировать настройки события на другое устройство контроля доступа, тревожный вход, дверь или считыватель карт.

9.8.2 Настройка действий устройства при событии доступа

Настройте действия устройства контроля доступа при возникновении события доступа. При срабатывании событие может инициировать тревожный выход, бипер хоста и другие

действия на том же устройстве.

Шаги

Примечание

Функция должна поддерживаться устройством.

1. Нажмите **Access Control → Linkage Configuration** («Контроль доступа → Конфигурация привязки»).
2. Выберите устройство контроля доступа из списка слева.
3. Нажмите кнопку **Add** («Добавить») для добавления новой привязки.
4. Вы можете выбрать в качестве **Event source** («Источник события») значение **Event Linkage** («Привязка события»).
5. Выберите тип и описание события, чтобы установить привязку.
6. В области **Linkage Target** («Привязка цели») установите цель, чтобы включить соответствующее действие.

Бипер контроллера

Устройство контроля доступа выдаст звуковое предупреждение.

Захват

Запуск захвата изображений в режиме реального времени.

Точка доступа

Выберите одно из следующих состояний двери: открыта/закрыта, оставить открытой/оставить закрытой.

Примечание

Целевая дверь и дверь, используемая в качестве источника, не могут являться одной дверью.

7. Нажмите **Save** («Сохранить»).
8. Опционально. После привязки нескольких устройств можно выполнить одно или несколько из следующих действий:

Изменение настроек привязки	Выберите настроенные параметры привязки из списка устройств. Измените параметры события, в том числе источник события и цель привязки.
Удаление настроек привязки	Выберите настроенные параметры привязки из списка устройств и нажмите **Delete** («Удалить»), чтобы удалить их.

9.8.3 Настройка действий устройства при считывании карт

Установите привязанные действия устройства контроля доступа при возникновении события доступа. При считывании карт может быть инициирован бипер хоста и другие действия на том же устройстве.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **Access Control → Linkage Configuration** («Контроль доступа → Конфигурация привязки»).
2. Выберите устройство контроля доступа из списка слева.
3. Нажмите кнопку **Add** («Добавить») для добавления новой привязки.
4. Выберите **Card Linkage** («Привязка карты») в качестве источника события.
5. Введите номер карты и выберите карту из выпадающего списка.
6. Выберите считыватель карт, чтобы запустить привязанные события.
7. В области **Linkage Target** («Привязка цели») установите цель, чтобы включить соответствующее действие.

   Бипер контроллера

   Устройство контроля доступа выдаст звуковое предупреждение.

   Захват

   Запуск захвата изображений в режиме реального времени.

   Точка доступа

   Выберите одно из следующих состояний двери: открыта/закрыта, оставить открытой/оставить закрытой.
8. Нажмите **Save** («Сохранить»).
   При считывании карты (настроенной в соответствии с шагом 5) с помощью считывателя карт (настроенного в соответствии с шагом 6) запускаются привязанные действия (настроенные в соответствии с шагом 7).
9. Опционально. После привязки нескольких устройств можно выполнить одно или несколько из следующих действий:

Удаление настроек привязки	Выберите настроенные параметры привязки из списка устройств и нажмите **Delete** («Удалить»), чтобы удалить их.
Изменение настроек привязки	Выберите параметры привязки из списка устройств. Измените параметры, в том числе источник события и цель привязки.

9.8.4 Настройка действий устройства для идентификатора

пользователя

Можно настроить действия устройства контроля доступа для определенного идентификатора сотрудника/посетителя. При детекции определенного идентификатора сотрудника/посетителя устройством контроля доступа срабатывают тревожный выход, бипер считывателя карт и другие действия. Таким образом, можно следить за определенными сотрудниками/посетителями.

Шаги

Примечание

Функция должна поддерживаться устройством.

1. Нажмите **Access Control → Linkage Configuration** («Контроль доступа → Конфигурация привязки»).
2. Выберите устройство контроля доступа из списка слева.
3. Нажмите кнопку **Add** («Добавить») для добавления новой привязки.
4. Выберите **Person Linkage** («Привязка пользователя») в качестве источника события.
5. Введите номер сотрудника и выберите карту из выпадающего списка.
6. Выберите считыватель карт из списка.
7. В области **Linkage Target** («Целевая область привязки») установите цель свойства, чтобы включить соответствующее действие.

Бипер контроллера

Устройство контроля доступа выдаст звуковое предупреждение.

Бипер считывателя карт

Устройство контроля доступа выдаст звуковое предупреждение.

Захват

Изображение будет захвачено, когда произойдет выбранное событие.

Запись

Изображение будет записано, когда произойдет выбранное событие.

Примечание

Функция записи должна поддерживаться на устройстве.

Тревожный выход

Тревожный выход будет активирован для уведомления.

Тревожный вход

Постановка на охрану/снятие с охраны тревожного входа.

Примечание

Устройство должно поддерживать функцию зонирования.

Точка доступа

Выберите одно из следующих состояний двери: открыта/закрыта, оставить открытой/оставить закрытой.

Воспроизведение голосового предупреждения

Вызывает срабатывание голосового предупреждения. Настроенное голосовое предупреждение будет воспроизведено в соответствии с заданным режимом воспроизведения.

8. Нажмите **Save** («Сохранить»).
9. Опционально. После привязки можно выполнить одно или несколько из следующих действий:

Удаление настроек привязки	Выберите настроенные параметры привязки из списка устройств и нажмите **Delete** («Удалить»), чтобы удалить их.
Изменение настроек привязки	Выберите настроенные параметры привязки из списка устройств. Измените параметры события, в том числе источник события и цель привязки.

9.9 Контроллер двери

Состояние двери добавленного устройства контроля доступа будет отображаться в режиме реального времени в модуле **Monitoring** («Мониторинг») добавленного устройства контроля доступа. Также можно управлять дверьми, например, открывать/закрывать дверь или оставлять дверь открытой/закрытой удаленно через клиентское ПО. События доступа отображаются в этом модуле в режиме реального времени. Здесь можно просматривать информацию о допуске и данные пользователей.

Примечание

Пользователь с разрешением на управление дверью может войти в модуль мониторинга и осуществлять управление дверьми. Для других пользователей панель управления устройством отображаться не будет. Для настройки разрешения пользователя обратитесь к разделу ***«Управление пользователями»***.

9.9.1 Управление состоянием двери

Можно контролировать состояние двери (дверей): разблокировать/заблокировать, оставить

дверь разблокированной/заблокированной, оставить все двери разблокированными и т. д.

Перед началом

- Добавьте сотрудника/посетителя и назначьте уровень доступа, тогда у сотрудника/посетителя будет право доступа к точкам доступа (дверям). Более подробная информация представлена в разделах ***«Управление сотрудниками/посетителями»*** и ***«Настройка группы контроля доступа для назначения разрешений на доступ»***.
- Убедитесь, что у пользователя есть разрешение выполнять операции с точками доступа (двери). Более подробная информация представлена в соответствующем разделе.

Шаги

1. Нажмите **Monitoring** («Мониторинг») для перехода на соответствующую страницу.
2. В правом верхнем углу выберите группу точки доступа.

Примечание

Более подробная информация об управлении группой точек доступа представлена в разделе ***«Управление группами»***.

На экране будут отображены двери в выбранной группе контроля доступа.

3. Нажмите на значок двери, чтобы выбрать ее, или нажмите **Ctrl** и выберите несколько дверей.

Примечание

При активированных опциях **Remain All Unlocked** («Оставить все двери разблокированными») и **Remain All Locked** («Оставить все двери заблокированными») этот шаг пропускают.

4. Нажимайте следующие кнопки, чтобы управлять дверью.

Разблокировка

Разблокируйте дверь, чтобы открыть ее на определенный промежуток времени. По истечении заданного времени дверь будет автоматически заблокирована.

Блокировка

Когда дверь открыта, заблокируйте ее. Пользователь с соответствующим разрешением может получить доступ к двери с помощью учетных данных.

Оставить разблокированной

Дверь будет разблокирована (из открытого или закрытого состояния). Для доступа к двери не требуется предъявление учетных данных.

Оставить заблокированной

Дверь будет закрыта и заблокирована. Дверь будет недоступна даже для пользователей с соответствующими разрешениями, за исключением суперпользователей.

Все двери остаются разблокированными

Все двери из группы будут разблокированы (из открытого или закрытого состояния). Для доступа к двери не требуется предъявление учетных данных.

Все двери остаются заблокированными

Все двери из группы будут закрыты и заблокированы (из открытого или закрытого состояния). Дверь будет недоступна даже для пользователей с соответствующими разрешениями, за исключением суперпользователей.

Захват

Захват изображения вручную.

Примечание

Кнопка **Capture** («Захват») доступна, когда устройство поддерживает функцию захвата изображений. Изображение сохраняется на компьютере, на котором работает клиентское ПО. Для настройки параметров сохранения обратитесь к разделу *«Настройка звукового сигнала»* Руководства пользователя клиентского программного обеспечения.

Результат

Иконки дверей изменятся в режиме реального времени, если операция завершена успешно.

9.9.2 Проверка информации о событиях доступа в режиме реального времени

Журналы с информацией о считывании карт, распознавании и сравнении лиц будут отображаться в режиме реального времени. Здесь можно просматривать личную информацию пользователя и изображение, захваченное во время доступа.

Шаги

1. Нажмите **Monitoring** («Мониторинг») и выберите группу из списка в правом верхнем углу. Записи событий доступа, сработавших на дверях в выбранной группе, будут отображаться в режиме реального времени. Здесь можно просмотреть подробную информацию о записях, включая номер карты, имя сотрудника, организацию, время события и т. д.
2. Опционально. Выберите тип и статус события, чтобы отобразить их в списке при обнаружении событий. События, тип и состояние которых не установлены, не будут отображаться в списке.
3. Опционально. Установите флажок **Show Latest Event** («Показать последнее событие»), и последняя запись доступа будет выбрана и отображена в верхней части списка записей.
4. Опционально. Нажмите на событие, чтобы просмотреть сведения о пользователе, в том числе изображения пользователя (захваченное изображение и изображение профиля), номер карты пользователя, имя пользователя, наименование организация, телефон, контактный адрес и т. д.

Примечание

Дважды нажмите на захваченное изображение, чтобы увеличить его и рассмотреть в деталях.

5. Опционально. Нажмите правой кнопкой мыши на название колонки события доступа в таблице, чтобы отобразить или скрыть колонку.

9.10 Центр событий

На экране отображается информация о событии (например, если устройство вышло из сети), отправленная на клиентское ПО. В календаре событий можно проверить подробную информацию о событиях в режиме реального времени и журнал событий, просмотреть видео, связанное с событиями, обработать события и совершать другие операции.

Прежде чем клиентское ПО сможет получить информацию о событиях с устройства, необходимо активировать события источника и поставить устройство на охрану. Более подробная информация представлена в разделе ***«Включение функции получения события от устройств»***.

9.10.1 Включение функции получения события от устройств

Прежде чем клиентское программное обеспечение сможет получать уведомления о событиях от устройства, необходимо поставить устройство на охрану.

Шаги

1. Нажмите → **Tool** → **Device Arming Control** («Инструмент → Управление постановкой на охрану»), чтобы перейти на соответствующую страницу.
   Все добавленные устройства появляются на этой странице.
2. Опционально. Если устройств много, введите ключевые слова в поле **Filter** («Фильтр»), чтобы отфильтровать нужные устройства.

Примечание

Для отфильтрованных устройств можно выбрать **Arm All** («Поставить все на охрану») или **Disarm All** («Снять все с охраны»), чтобы разрешить получение событий с этих устройств.

3. В столбце **Auto-Arming** («Автоматическая постановка на охрану») переместите переключатель, чтобы активировать функцию автоматической постановки на охрану.

Рисунок 9-15. Постановка устройства на охрану

После включения устройства будут поставлены на охрану. Уведомления о событиях, инициируемых устройством под охраной, будут автоматически отправляться в клиентское ПО в режиме реального времени.

9.10.2 Просмотр событий в режиме реального времени

На экране отображается информация о событиях в режиме реального времени, полученная клиентом подключенных ресурсов. Просмотрите информацию о событии в режиме реального времени, в том числе об источнике события, времени события, временном приоритете и т. д.

Перед началом

Включите функцию получения информации о событии от устройств, чтобы клиентское ПО получало информацию с устройства. Более подробная информация представлена в разделе ***«Включение функции получения информации о событии с устройства»***.

Шаги

1. Нажмите **Event Center → Real-time Event** («Календарь событий → Событие в режиме реального времени»), чтобы перейти на соответствующую страницу и просматривать события в режиме реального времени, полученные клиентским ПО.

   Время события

   Для устройства кодирования, время события совпадает со временем на клиентском ПО в момент получения события. Для других типов устройств, временем события является время запуска события.

   Приоритет

   Приоритет отражает степень чрезвычайности события.
2. Фильтрация событий.

Фильтрация по типу устройства и (или) по приоритету	Для фильтрации событий выберите тип устройства и временные приоритеты.
Фильтрация по ключевым словам	Введите ключевые слова для фильтрации событий.

3. Опционально. Щелкните правой кнопкой мыши на заголовок таблицы в списке событий, чтобы настроить элементы, связанные с событием, которые будут отображаться в списке событий.
4. Чтобы просмотреть более подробную информацию о событии, выберите событие из списка событий.
5. Опционально. При необходимости выполните следующие действия.

Обработка параметров одного события	Нажмите **Handle** («Обработать»), чтобы перейти на страницу обработки, затем нажмите **OK**. **Примечание** После обработки события кнопка **Handle** («Обработать») будет заменена на кнопку **Add Remark** («Добавить примечание»). Нажмите кнопку **Add Remark** («Добавить примечание»), чтобы добавить примечание к обработанному событию.
Обработка событий в пакетном режиме	Выберите события, которые подлежат обработке, затем нажмите **Handle in Batch** («Обработать в пакетном режиме»). Введите параметр обработки, затем нажмите **OK**.
Включение/ выключение звуковой сигнализации	Нажмите **Audio On/Mute** («Включение/выключение звуковой сигнализации»), чтобы включить/выключить звуковую сигнализацию по событию.
Автоматический выбор последнего события	Нажмите **Auto-Select Latest Event** («Автоматический выбор последнего события»), чтобы выбрать последнее событие автоматически и отобразить информацию о событии.
Очистить события	Нажмите кнопку **Clear** («Очистить»), чтобы очистить все события из списка.
Отправка Email	Выберите событие и нажмите **Send Email** («Отправить Email»), чтобы отправить информацию о событии по электронной почте.

Примечание

Перед этим необходимо настроить параметры электронной почты. Более подробная информация о настройке параметров электронной почты представлена разделе *«Настройка параметров электронной почты»* Руководства пользователя клиентского программного обеспечения.

Автоматическое воспроизведение видео	Нажмите **Auto-Play Video** («Автоматическое воспроизведение видео»), чтобы автоматически воспроизводить видео при отображении сведений о событии.
Увеличение видео или изображения	● Нажмите видеоизображение дважды, чтобы просмотреть видео в большом окне. ● Поместите курсор на изображение и нажмите , чтобы просмотреть изображение в большом окне.
Загрузка захваченного изображения	Чтобы загрузить изображение на компьютер, наведите курсор на соответствующее изображение, нажмите значок загрузки в верхнем правом углу изображения.
Скачивание связанного с событием видео	Наведите курсор на записанное видео, нажмите , чтобы загрузить связанное с событием видео (30 секунд до события).

9.10.3 Поиск по журналу событий

В клиенте можно искать и просматривать события, задав определенные условия поиска. Найденные события можно обработать и экспортировать.

Перед началом

Включите функцию получения информации о событии от устройств, чтобы клиентское ПО могло получать информацию с устройства. Более подробная информация представлена в разделе ***«Включение функции получения информации о событии с устройства»***.

Шаги

1. Нажмите **Event Center → Event Search** («Календарь событий → Поиск события»), чтобы перейти на страницу поиска.
2. Настройте параметры фильтрации для отображения только выбранных событий.

Время

Время начала события.

Поиск

Устройство

Поиск событий с помощью устройства и каналов ресурсов устройств. При поиске по устройству необходимо установить следующие настройки:

- **Включить подузел.** Поиск событий с помощью устройства и всех его каналов.
- **Тип устройства.** Выберите устройство, в котором необходимо выполнить поиск по событию.

Группа

Поиск событий с помощью каналов ресурсов устройства.

Примечание

- Для событий системы видеодомофонии необходимо выбрать область поиска: Все события и журнал блокировки.
- При работе с устройством контроля доступа нажмите **Show More** («Показать еще»), чтобы настроить статус события, тип события, тип считывателя карт, имя пользователя, номер карты, организацию.

Приоритет

Приоритет может быть установлен как низкий, средний, высокий и неопределенный, что указывает на степень срочности события.

Тип события

В выпадающем списке выберите один или несколько типов событий для поиска.

Примечание

Можно ввести ключевое слово (поддерживается приблизительное соответствие) в поле поиска для поиска надлежащего типа событий.

Состояние

Состояние обработки события.

Поиск по ключевым словам

Введите ключевое слово (поддерживается приблизительное соответствие) для быстрого поиска необходимого события. Например, можно ввести имя сотрудника/посетителя для поиска событий, связанных с этим сотрудником/посетителем.

3. Нажмите **Search** («Поиск») для поиска событий согласно указанным условиям.

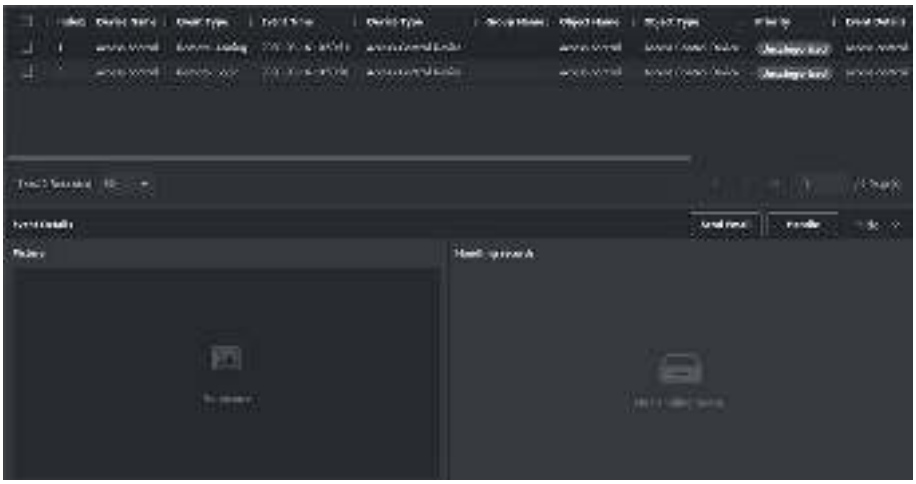


Рисунок 9-16. Поиск событий

Примечание

Если в рамках шага 2 в качестве типа устройства выбран **Access Control** («Терминал контроля доступа»), то в найденных событиях можно просматривать дополнительную информацию, например, номер карты, поверхностную температуру тела сотрудника/посетителя и повышенную температуру (если устройство поддерживает функцию измерения температуры).

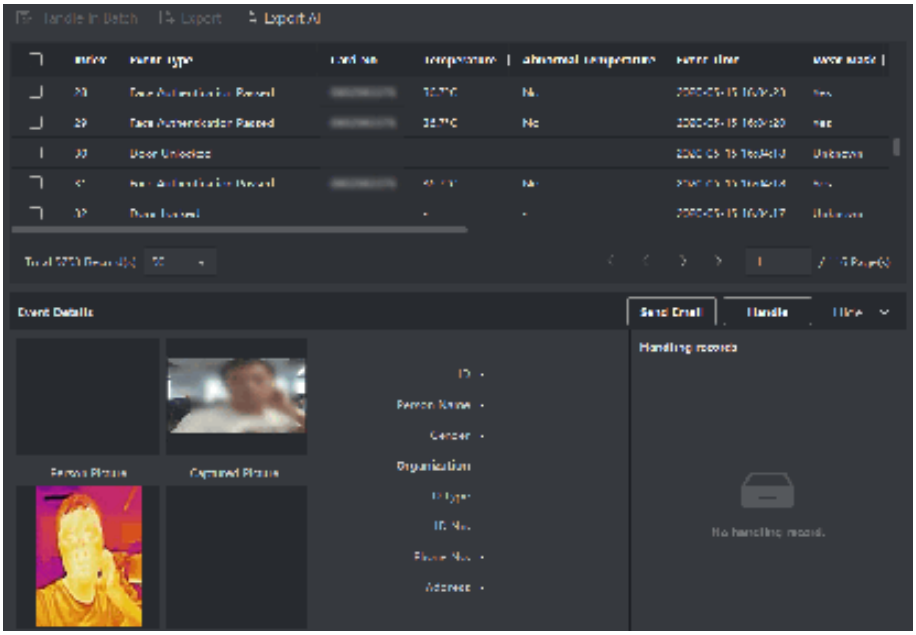


Рисунок 9-17. Поиск события

4. Опционально. Щелкните правой кнопкой мыши на заголовок таблицы в списке событий, чтобы настроить элементы, связанные с событием, которые будут отображаться в списке событий.

5. Чтобы просмотреть более подробную информацию о событии, выберите событие из списка событий.
6. Опционально. Выполните одну из следующих операций.

Обработка параметров одного события	Обработка одного события. Выберите одно событие, которое необходимо обработать, затем нажмите **Handle** («Обработать») на странице сведений о событии и выберите параметры обработки.
	Примечание После обработки события кнопка **Handle** («Обработать») будет заменена на кнопку **Add Remark** («Добавить примечание»). Нажмите на кнопку **Add Remark** («Добавить примечание»), чтобы добавить примечание к обработанному событию.
Обработка событий в пакетном режиме	Обработка событий в пакетном режиме. Выберите события, которые необходимо обработать, затем нажмите **Handle in Batch** («Обработать в пакетном режиме»), чтобы перейти на страницу параметров обработки.
	Примечание После обработки события кнопка **Handle** («Обработать») будет заменена на кнопку **Add Remark** («Добавить примечание»). Нажмите на кнопку **Add Remark** («Добавить примечание»), чтобы добавить примечание к обработанному событию.
Автоматическое воспроизведение видео	Нажмите **Auto-Play Video** («Автоматическое воспроизведение видео»), чтобы автоматически воспроизводить видео при отображении сведений о событии.
Увеличение видео или изображения	● Нажмите видеоизображение дважды, чтобы просмотреть видео в большом окне. ● Поместите курсор на изображение и нажмите , чтобы просмотреть изображение в большом окне.
Отправить Email	Выберите событие и нажмите **Send Email** («Отправить Email»), чтобы отправить информацию о событии по электронной почте.

Примечание

Перед этим необходимо настроить параметры электронной почты. Более подробная информация о настройке параметров электронной почты представлена разделе *«Настройка параметров электронной почты»* Руководства пользователя клиентского программного обеспечения.

Экспорт информации о событии	Нажмите **Export** («Экспорт») для экспорта журнала и изображений события на компьютер в формате Excel/CSV. Задайте папку сохранения вручную.
Загрузка захваченного изображения	Чтобы загрузить изображение на компьютер, наведите курсор на соответствующее изображение, нажмите значок загрузки в верхнем правом углу изображения.
Скачивание связанного с событием видео	Наведите курсор на записанное видео, нажмите , чтобы загрузить связанное с событием видео (30 секунд до события).

9.11 УРВ

Модуль «Учет рабочего времени (УРВ)» обеспечивает отслеживание и мониторинг начала и завершения работы сотрудников, отслеживание рабочего времени и опозданий, ранних уходов, времени перерывов и прогулов сотрудников.

Примечание

В данном разделе представлены настройки, которые необходимо установить для получения отчетов по посещению. Записи доступа, полученные после установки настроек, будут учтены в статистике.

9.11.1 Настройка параметров УРВ

Настройте параметры посещаемости, в том числе общее правило, параметры сверхурочной работы, пункта проверки посещаемости, выходные дни, типы отпусков и т. д.

Настройка выходных дней

Периоды нерабочих дней могут отличаться в зависимости от страны или региона. В клиентском ПО предусмотрена функция назначения выходных дней. Выберите один или

несколько дней в качестве выходных дней в соответствии с фактическими требованиями и установите разные правила посещения для выходных и рабочих дней.

Шаги

Примечание

Параметры, настроенные здесь, будут установлены по умолчанию для нового добавленного периода времени. Это не повлияет на ранее установленные периоды времени.

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Settings** → **General Rule** («Настройки посещаемости → Общее правило»).
3. Назначьте один или несколько дней в качестве выходных, например, субботу и воскресенье.
4. Нажмите **Save** («Сохранить»).

Настройка параметров сверхурочной работы

Настройте параметры сверхурочной работы для рабочих и выходных дней, в том числе уровень сверхурочной работы, стоимость часа сверхурочной работы, статус посещения для сверхурочной работы и т. д.

Шаги

1. Нажмите **Time & Attendance → Attendance Settings → Overtime** («Учет рабочего времени → Настройки посещаемости → Сверхурочная работа»).
2. Установите необходимую информацию.

Уровень сверхурочной работы для рабочего дня

Работая в течение определенного периода после окончания рабочего дня в рабочий день, сотрудник может достичь одного из уровней сверхурочной работы: уровня сверхурочной работы 1, уровня сверхурочной работы 2 и уровня сверхурочной работы 3. Установите соответствующую стоимость часа работы для трех уровней сверхурочной работы.

Размер оплаты

Размер оплаты рассчитывается как произведение стоимости часа сверхурочной работы на количество часов, отработанных сверхурочно. Работая в течение определенного периода после окончания рабочего дня в выходной день, сотрудник может достичь одного из уровней сверхурочной работы. Для трех уровней сверхурочной работы можно установить разную стоимость часа сверхурочной работы (1-10, может быть десятичным числом). Например, допустимое количество часов сверхурочных работ составляет один час (для уровня сверхурочных 1), а коэффициент рабочего времени для уровня сверхурочных 1 равен 2. В этом случае сверхурочная работа оплачивается в двойном размере.

Правило сверхурочной работы в выходные дни

Установите правило сверхурочной работы в выходные дни и порядок расчета оплаты сверхурочных часов.

3. Нажмите **Save** («Сохранить»).

Настройка контрольного пункта проверки посещаемости

В качестве устройства контроля УРВ можно указать считыватель карт точки контроля доступа. В этом случае считывание карты будет регистрироваться для сбора статистики УРВ.

Перед началом

- Добавьте устройство контроля доступа. Более подробная информация представлена в разделе ***«Добавление устройства»***.
- Включите модуль УРВ. Более подробная информация представлена в разделе ***«Добавление общего расписания»***.

По умолчанию все считыватели карт устройств контроля доступа назначены в качестве контрольного пункта проверки посещаемости (учет начала/окончания рабочего времени). Если необходимо изменить параметры контрольной точки считывателя карт, можно выполнить следующие операции.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Settings → Attendance Check Point** («Настройки посещаемости → Контрольный пункт проверки посещаемости»), чтобы перейти на соответствующую страницу.
3. Переведите переключатель **Set All Card Readers as Check Points** («Назначение всех считывателей карт в качестве контрольных пунктов проверки посещаемости») в положение **Off** («Выкл.»).
4. Установите желаемые считыватели карт в качестве контрольных пунктов проверки посещаемости в приведенном ниже списке.
5. Выберите состояние контрольного пункта: **Start/End-Work** («Начало работы» / «Окончание работы»).

Примечание

При выборе **Start-Work** («Начало работы») или **End-Work** («Окончание работы») будет загружаться статистика УРВ с заданного контрольного пункта.

Начало работы

Состояние УРВ, загруженное с устройства, будет считаться началом работы.

Окончание работы

Состояние УРВ, загруженное с устройства, будет считаться окончанием работы.

Начало работы / Окончание работы

Состояние УРВ будет считаться как «Начало работы» / «Окончание работы» в соответствии с фактической посещаемостью, зарегистрированной устройством.

6. Нажмите **Set as Check Point** («Установить в качестве контрольного пункта проверки»).
   После настройки контрольные пункты проверки посещаемости будут отображаться в списке справа.
7. Опционально. После установки контрольных пунктов проверки посещаемости выполните следующие действия.

Изменение информации контрольного пункта	Выберите один контрольный пункт проверки посещаемости, нажмите **Edit** («Изменить»), чтобы изменить информацию, включая имя, функцию контрольного пункта и т. д. Выберите два или более контрольных пункта проверки посещаемости, нажмите **Edit** («Изменить») для пакетного редактирования функции контрольного пункта, добавления примечания и т. д.
Удалить контрольный пункт проверки посещаемости	Выберите один или несколько контрольных пунктов и нажмите **Delete** («Удалить»), чтобы удалить пункт/пункты.

Настройка нерабочих дней

Добавьте выходной день, в течение которого регистрация прихода/ухода осуществляться не будет.

Добавление постоянного выходного дня

Настройте выходной день, который будет действовать на регулярной основе в течение установленного срока, в том числе Новый год, День независимости, Рождество и т. д.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Settings → Holiday** («Настройки посещаемости → Выходной день»), чтобы перейти на соответствующую страницу.
3. Выберите тип выходного дня **Regular Holiday** («Постоянный выходной день»).
4. Введите наименование выходного дня.
5. Установите дату начала выходного дня.
6. Введите количество выходных дней.
7. Назначьте соответствующий статус посещения при работе сотрудника в выходной день.
8. Опционально. Выберите пункт **Repeat Annually** («Повторять ежегодно»), чтобы задействовать указанные настройки на ежегодной основе.
9. Нажмите **OK**.
   Добавленный выходной день отобразится в списке выходных дней и в календаре.

Если выбранная дата выходного дня совпадает с датой другого выходного дня, будет зарегистрирована дата первого добавленного выходного дня.

10. Опционально. Выполните следующие действия, чтобы добавить выходной день:

Изменение выходного дня	Нажмите  для редактирования информации о выходных днях.
Удаление выходного дня	Выберите один или несколько выходных дней, затем нажмите **Delete** («Удалить»), чтобы удалить выходной день из списка.

Добавление выходного дня с плавающей датой

Настройте выходной день, который будет действовать в разные дни ежегодно в течение установленного срока, в том числе Банковские каникулы.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Settings → Holiday** («Настройки посещаемости → Выходной день»), чтобы перейти на соответствующую страницу.
3. Нажмите **Add** («Добавить»), чтобы открыть соответствующую страницу.
4. Выберите тип выходного дня **Irregular Holiday** («Выходной день с плавающей датой»).
5. Введите наименование выходного дня.
6. Установите дату начала выходного дня.

   Пример

   Чтобы установить четвертый четверг ноября 2019 года в качестве праздника Дня благодарения, необходимо выбрать 2019 год, 4 ноября и четверг из выпадающих списков.
7. Введите количество выходных дней.
8. Назначьте соответствующий статус посещения при работе сотрудника в выходной день.
9. Опционально. Выберите пункт **Repeat Annually** («Повторять ежегодно»), чтобы задействовать указанные настройки на ежегодной основе
10. Нажмите **OK**.

    Добавленный выходной день отобразится в списке выходных дней и в календаре.

    Если выбранная дата выходного дня совпадает с датой другого выходного дня, будет зарегистрирована дата первого добавленного выходного дня.
11. Опционально. Выполните следующие действия, чтобы добавить выходной день:

Изменение выходного дня	Нажмите  для редактирования информации о выходных днях.
Удаление выходного дня	Выберите один или несколько выходных дней, затем нажмите **Delete** («Удалить»), чтобы удалить выходной день из списка.

Настройка типа отпуска

Настройте тип отпуска (основной и дополнительный тип отпуска) в соответствии с

требованиями. Данный тип отпуска может быть удален или изменен.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Settings → Leave Type** («Настройки посещаемости → Тип отпуска»), чтобы перейти на соответствующую страницу.
3. Нажмите **Add** («Добавить») на панели слева, чтобы добавить основной тип отпуска.
4. Опционально. Для добавления основных типов отпуска необходимо выполнить следующие действия.

Изменение	Направьте курсор на основной тип отпуска и нажмите для изменения основного типа отпуска.
Удаление	Направьте курсор на основной тип отпуска и нажмите **Delete** («Удалить»), чтобы удалить основной тип отпуска.

5. Нажмите **Add** («Добавить») на панели справа, чтобы добавить дополнительный тип отпуска.
6. Опционально. Для добавления дополнительных типов отпуска необходимо выполнить следующие действия.

Изменение	Направьте курсор на основной тип отпуска и нажмите для изменения дополнительного типа отпуска.
Удаление	Выберите один или несколько основных типов отпусков, затем нажмите **Delete** («Удалить»), чтобы удалить отпуск из списка.

Синхронизация записи аутентификации с помощью сторонней базы данных

Данные УРВ, записанные в клиент, могут быть использованы в другой системе для сбора статистики УРВ или других операций. Включите функцию синхронизации, чтобы автоматически применить запись аутентификации из клиента к сторонней базе данных.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Settings → Third-Party Database** («Настройки посещаемости → Сторонняя база данных»).
3. Переведите переключатель в пункте **Apply to Database** («Применить к базе данных») в положение **ON** («Вкл.»), чтобы включить функцию синхронизации.
4. Выберите тип базы данных: **SQLServer** или **MySQL**.

Примечание

При выборе **MySQL**, импортируйте файл конфигурации (libmysql.dll) с локального компьютера.

5. Установите другие обязательные параметры сторонней базы данных, включая IP-адрес сервера, номер порта, наименование базы данных, имя пользователя и пароль.

Примечание

Номер порта по умолчанию для выбранного типа базы данных отображается автоматически. Можно ввести число от 1 до 65535, чтобы настроить номер порта.

6. Настройте параметры таблицы базы данных в соответствии с текущей конфигурацией.
   1) Введите название таблицы сторонней базы данных.
   2) Задайте поля сопоставленной таблицы между клиентским обеспечением и сторонней базой данных.
7. Нажмите **Save** («Сохранить»), чтобы проверить возможность подключения к базе данных, и сохраните настройки для успешного подключения.
   - Данные УРВ будут записаны в стороннюю базу данных.
   - Во время синхронизации, при отключении клиентского ПО от сторонней базы данных, попытка повторного подключения будет выполняться каждые 30 минут. После повторного подключения клиентское ПО синхронизирует данные, записанные за время сбоя подключения, со сторонней базой данных.

Настройка времени перерывов

Добавьте время перерыва и установите время начала, время окончания, продолжительность, порядок расчета и другие параметры для перерыва. Добавленное время перерыва также можно редактировать или удалять.

Шаги

1. Нажмите **Time & Attendance → Timetable** → **Break Time** («Учет рабочего времени → Расписание → Время перерыва»).
   Добавленное время перерыва отображается в списке.
2. Нажмите на **Break Time Settings** («Настройки времени перерыва»), чтобы перейти на соответствующую страницу.
3. Нажмите **Add** («Добавить»).
4. Введите наименование перерыва.
5. Установите сопутствующие параметры.

Время начала/Время окончания

Укажите время начала и время окончания перерыва.

Не ранее/Не позднее

Установите самое раннее возможное время начала перерыва и самое позднее время окончания перерыва.

Продолжительность перерыва

Продолжительность перерыва от времени начала до времени окончания перерыва.

Автоматическое исключение из рабочего времени

Продолжительность перерыва автоматически рассчитана и составляет 60 минут.

Обязательная регистрация прихода на работу/ухода с работы

Продолжительность перерыва будет рассчитана и исключена из рабочего времени в соответствии с фактическим временем регистрации прихода/ухода сотрудника.

Раннее возвращение с перерыва

Фактическое время прихода и ухода не превышает времени перерыва и может быть отмечено как обычная работа или сверхурочная работа.

Позднее возвращение с перерыва

Фактическое время прихода и ухода превышает время перерыва и может быть отмечено как опоздание, отсутствие или ранний уход с работы.

Расчет

Регистрация каждого прихода на работу/ухода с работы. Каждое время прихода/ухода регистрируется, и сумма всех периодов между каждым приходом/уходом будет учтена как время перерыва.
Регистрация первого прихода на работу и последнего ухода с работы. Время регистрации первого прихода на работу учитывается как время начала рабочего времени, а время регистрации последнего ухода с работы — как время окончания рабочего времени.

Включение УРВ

Переведите переключатель в пункте **Enable T&A Status** («Включить учет рабочего времени») в положение **ON** («Вкл.») для расчета времени перерыва в соответствии с записями о состояниях посещений.

Примечание

Устройство должно поддерживать данную функцию.

Действительный интервал аутентификации

В течение действующего интервала аутентификации несколько считываний карты одного сотрудника будут учитываться только как один раз.

6. Нажмите **Save** («Сохранить») для сохранения настроек.
7. Опционально. Нажмите **Add** («Добавить»), чтобы добавить еще один перерыв.

Настройка отображения отчета

Настройте параметры отображения отчета по посещению, например, название компании,

логотип, формат даты, формат времени и отметки.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Statistics** → **Report Display** («Статистика посещений → Отображение отчета»).
3. Настройте параметры отображения для отчетов по посещению сотрудников.

   Наименование компании

   Введите наименование компании для отображения в отчете.

   Отметка о статусе посещения

   Введите отметку и выберите цвет. Поля, связанные с полем статуса посещения, в отчете будут отображаться с указанной меткой и цветом.

   Отметка о выходном дне

   Введите отметку и выберите цвет. Поля, связанные с полем выходного дня, в отчете будут отображаться с указанной меткой и цветом.
4. Нажмите **Save** («Сохранить»).

9.11.2 Добавление общего расписания

На странице расписания можно добавить общее расписание для сотрудников, для которого требуется фиксированное время начала и окончания рабочего дня. Также можно установить необходимое время прихода/ухода, допустимые интервалы опозданий и ранних уходов.

Шаги

1. Нажмите **Time and Attendance → Timetable** («Учет рабочего времени → Расписание»), чтобы перейти на страницу настроек расписания.
2. Нажмите **Add** («Добавить»), чтобы добавить расписание.

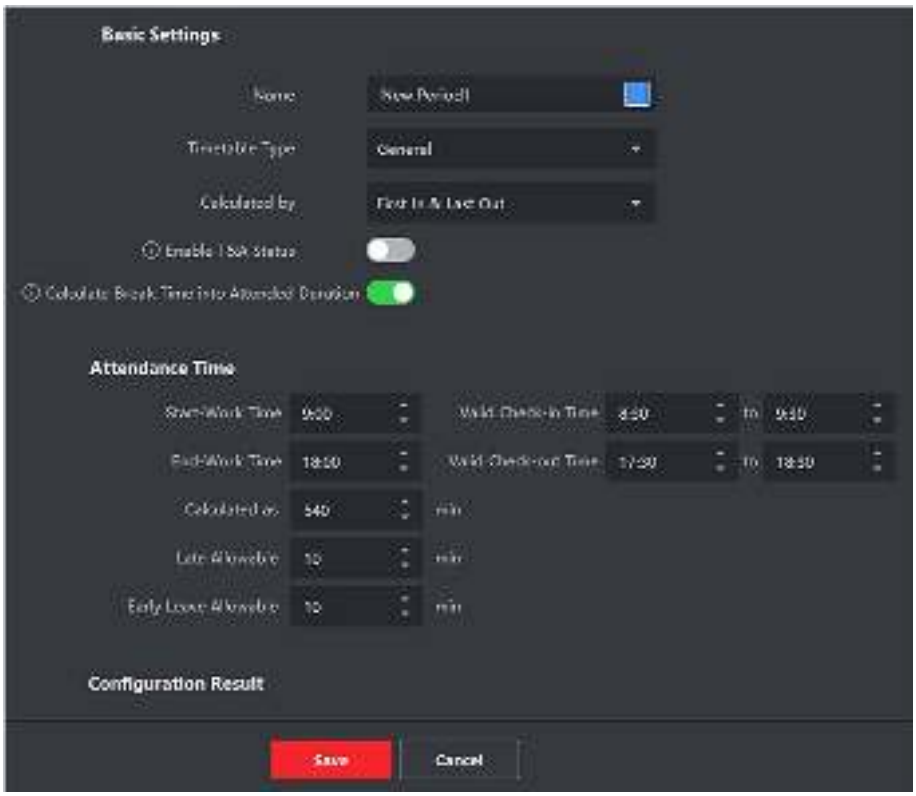


Рисунок 9-18. Добавление расписания

3. Создайте наименование для расписания.

Примечание

Нажмите на иконку цвета рядом с наименованием, чтобы настроить цвет для действующего расписания на временной шкале в области **Configuration Result** («Результат конфигурации»).

4. Выберите тип расписания: общий.
5. Выберите метод расчета.

Регистрация первого прихода и последнего ухода

Время регистрации первого прихода учитывается как время начала работы, а время регистрации последнего ухода — как время окончания работы.

Регистрация каждого прихода на работу/ухода с работы

Каждое время прихода/ухода регистрируется, и сумма всех периодов между каждым приходом/уходом будет учтена при расчете продолжительности рабочего времени. Для этого метода расчета необходимо установить **Valid Authentication Interval** («Действительный интервал аутентификации»). Например, если интервал считывания одной и той же карты меньше установленного значения, считывание карты будет недействительным.

6. Опционально. Переведите переключатель в пункте **Enable T&A Status** («Включить учет рабочего времени») в положение **ON** («Вкл.») для расчета рабочего времени в соответствии с записями о состояниях посещений.

Примечание

Устройство должно поддерживать данную функцию.

7. Опционально. Включите **Calculate Break Time into Attended Duration** («Регистрация времени перерыва в продолжительность рабочего времени»).

Примечание

Если этот параметр включен, время перерыва будет засчитано в общую продолжительность рабочего времени. То есть фактическая продолжительность рабочего времени равна общей продолжительности рабочего времени (включая время перерыва).

8. Установите следующие сопутствующие параметры времени посещений:

Начало работы / Окончание работы

Установите время начала и время окончания работы.

Действительное время регистрации прихода/ухода

На временной шкале установите расписание, в течение которого регистрация прихода/ухода является действительной.

Рассчитывается как

Установите продолжительность, рассчитанную как фактическая продолжительность работы.

Допустимый интервал опозданий/ранних уходов

Установите временные интервалы для ранних уходов и опозданий.

9. Установите другие сопутствующие параметры.

Регистрация прихода с опозданием

Установите максимальный интервал опозданий для работников, прошедших регистрацию прихода на работу. При превышении установленного интервала опоздания сотрудник будет считаться отсутствующим.

Регистрация раннего ухода

Установите максимальный интервал ранних уходов с работы. Сотрудник, прошедший регистрацию ухода ранее установленного времени, будет считаться отсутствующим.

Отсутствие регистрации прихода

Сотрудник, не прошедший регистрацию прихода, будет считаться отсутствующим или опоздавшим.

Отсутствие регистрации ухода

Сотрудник, не прошедший регистрацию ухода, будет считаться отсутствующим или опоздавшим.

10. Нажмите **Save** («Сохранить») для добавления расписания.
11. Опционально. После добавления расписания выполните следующие действия.

Изменение расписания	Выберите расписание из списка для редактирования соответствующей информации.
Удаление расписания	Выберите расписание из списка и нажмите **Delete** («Удалить»), чтобы удалить его.

9.11.3 Добавление смены

Добавьте смену для работы сотрудников. Настройте период смены (день, неделя, месяц) и время посещения. В соответствии с фактическими требованиями, можно добавить несколько расписаний в одну смену. В этом случае сотрудникам необходимо будет проходить регистрацию прихода/ухода для каждого расписания.

Перед началом

В первую очередь добавьте расписание. Более подробная информация представлена в разделе ***«Добавление общего расписания»***.

Шаги

1. Нажмите **Time and Attendance → Shift** («Учет рабочего времени → Смена»), чтобы перейти на страницу настроек смены.
2. Нажмите **Add** («Добавить»), чтобы добавить смену.
3. Введите наименование смены.
4. Выберите период смены из выпадающего списка.
5. Выберите расписание нажмите на временную шкалу, чтобы применить выбранное расписание.

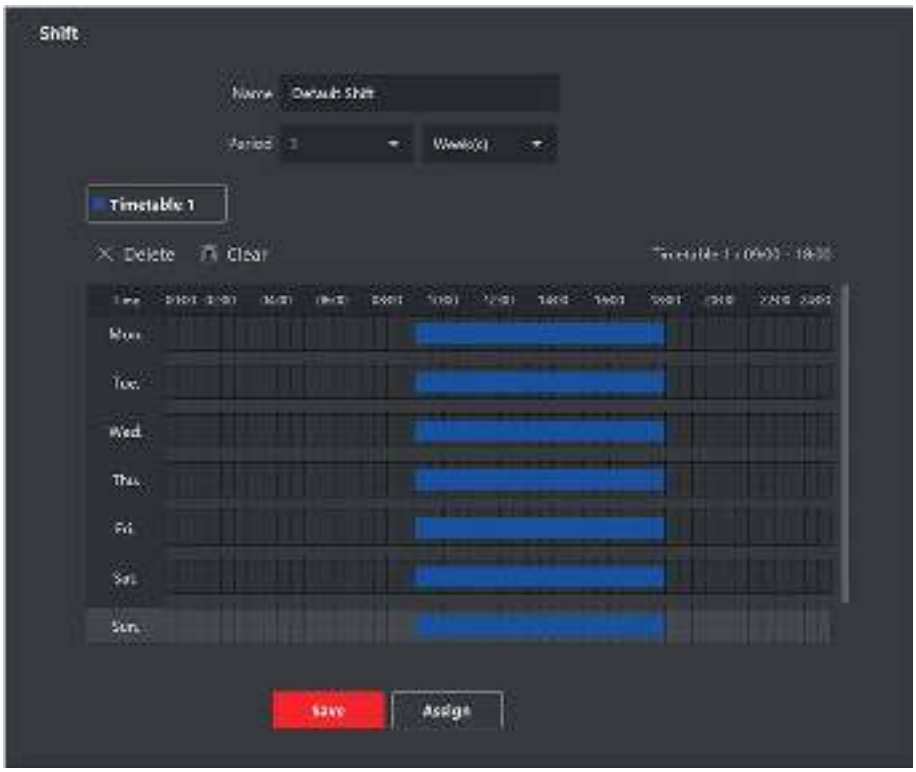


Рисунок 9-19. Добавление смены

Примечание

Можно выбрать несколько расписаний. Время начала и окончания работы, а также действительное время регистрации прихода/ухода не могут совпадать в разных расписаниях.

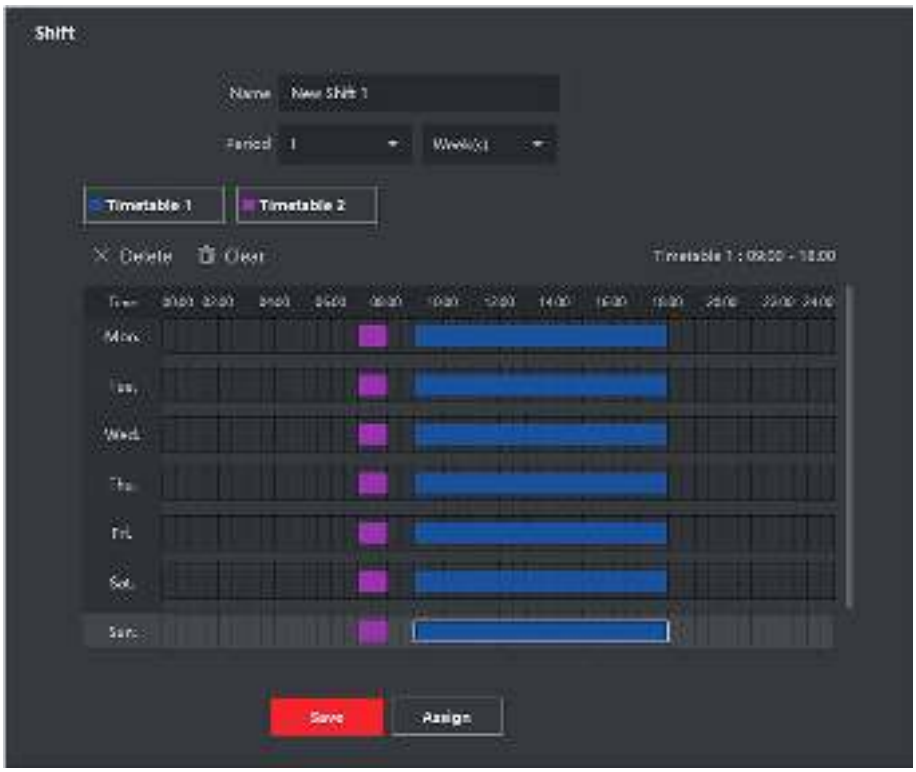


Рисунок 9-20. Добавление нескольких расписаний

6. Нажмите **Save** («Сохранить»).
   Добавленная смена будет отображаться в списке на панели слева. Можно добавить не более 64 смен.
7. Опционально. Для составления графика смен назначьте смену для организации или сотрудника.
   1) Нажмите **Assign** («Назначить»).
   2) Выберите вкладку **Organization** («Организация») или **Person** («Сотрудник») и установите флажок для нужной организации или сотрудника.
      Выбранные организации или сотрудники будут перечислены в правой части экрана.
   3) Установите **Expire Date** («Дата истечения») для графика смены.
   4) Установите другие параметры для графика.

      Регистрация прихода не требуется

      Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они приходят на работу.

      Регистрация ухода не требуется

      Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они уходят с работы.

      График, предусмотренный для выходного дня

      Этот график действует в выходные дни и сотрудники должны приходить на работу в соответствии с графиком.

График, предусмотренный для сверхурочной работы

В этом графике будут указаны параметры сверхурочной работы сотрудников.

5) Нажмите **Save** («Сохранить»), чтобы сохранить график смены.

9.11.4 Управление графиком смены

Рабочая смена — это практика трудоустройства, при которой работы ведутся в непрерывном цикле 24 часа в сутки каждый день недели. В данном режиме рабочий день подразделяется на смены, установленные периоды времени, в течение которых сотрудники посменно выполняют свои обязанности.

Установите график работы отдела, график работы сотрудников и временный график.

Настройка графика работы отдела

Установите график работы смены для отдела, чтобы назначить соответствующий график для каждого сотрудника в отделе.

Перед началом

В модуле УРВ отдел отображается в списке вместе с соответствующей организацией. Прежде чем установить график работы необходимо добавить организацию и сотрудников в модуле **Person** («Сотрудник»). Для подробной информации обратитесь к разделу ***«Управление сотрудниками»***.

Шаги

1. Нажмите **Time & Attendance** → **Shift Schedule** («Учет рабочего времени→ Расписание смены») для перехода на страницу управления расписанием смен.
2. Нажмите **Department Schedule** («График работы отдела»), чтобы перейти на соответствующую страницу.
3. Выберите отдел организации из списка на панели слева.

Примечание

Если активирована функция **Include Sub Organization** («Включить подведомственную организацию»), при выборе организации одновременно будут выбраны ее подведомственные организации.

4. Выберите смену из выпадающего списка.
5. Опционально. Включите функцию **Multiple Shift Schedules** («График работы для нескольких смен») и выберите необходимые периоды из выбранных расписаний работы сотрудников.

Примечание

Эта функция доступна только для смен с единственным расписанием.

График работы для нескольких смен

Данный график содержит более одного расписания. Сотрудник может пройти

регистрацию во время действия любого расписания, и статус его посещения будет эффективным.
Если график работы для нескольких смен содержит три расписания: с 00:00 до 07:00, с 08:00 до 15:00 и с 16:00 до 23:00. Статус посещения сотрудника с данным графиком работы будет эффективным в любом из трех расписаний. Если сотрудник приходит на работу в 07:50, будет применено ближайшее расписание с 08:00 до 15:00 для регистрации его прихода.

6. Настройте дату начала и дату окончания периода.
7. Установите другие параметры для графика.

Регистрация прихода не требуется

Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они приходят на работу.

Регистрация ухода не требуется

Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они уходят с работы.

График, предусмотренный для выходного дня

Этот график действует в выходные дни, и сотрудники должны приходить на работу в соответствии с графиком.

График, предусмотренный для сверхурочной работы

В этом графике будут указаны параметры сверхурочной работы сотрудников.

Гибкий график смен по выходным

Работа в выходные дни будет засчитана как сверхурочная работа.

8. Нажмите **Save** («Сохранить»).

Настройка графика работы сотрудника

Назначьте график сменной работы для одного или нескольких сотрудников. Также можно просматривать и редактировать детали графика работы сотрудника.

Перед началом

В модуле **Person** («Сотрудник») добавьте отдел и сотрудника. Для подробной информации обратитесь к разделу ***«Управление сотрудниками»***.

Шаги

Примечание

График работы сотрудника имеет более высокий приоритет, чем график работы отдела.

1. Нажмите **Time & Attendance** → **Shift Schedule** («Учет рабочего времени→ Расписание смены») для перехода на страницу управления расписанием смен.

2. Нажмите **Person Schedule** («График работы сотрудника»), чтобы перейти на соответствующую страницу.
3. Выберите организацию и сотрудников.
4. Выберите смену из выпадающего списка.
5. Опционально. Включите функцию **Multiple Shift Schedules** («График работы для нескольких смен») и выберите необходимые периоды из выбранных расписаний работы сотрудников.

Примечание

Эта функция доступна только для смен с единственным расписанием.

График работы для нескольких смен

Данный график содержит более одного расписания. Сотрудник может пройти регистрацию во время действия любого расписания, и статус его посещения будет эффективным.
Если график работы для нескольких смен содержит три расписания: с 00:00 до 07:00, с 08:00 до 15:00 и с 16:00 до 23:00. Статус посещения сотрудника с данным графиком работы будет эффективным в любом из трех расписаний. Если сотрудник приходит на работу в 07:50, будет применено ближайшее расписание с 08:00 до 15:00 для регистрации его прихода.

6. Настройте дату начала и дату окончания периода.
7. Установите другие параметры для графика.

Регистрация прихода не требуется

Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они приходят на работу.

Регистрация ухода не требуется

Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они уходят с работы.

График, предусмотренный для выходного дня

Этот график действует в выходные дни, и сотрудники должны приходить на работу в соответствии с графиком.

График, предусмотренный для сверхурочной работы

В этом графике будут указаны параметры сверхурочной работы сотрудников.

Гибкий график смен по выходным

Работа в выходные дни будет засчитана как сверхурочная работа.

8. Нажмите **Save** («Сохранить»).

Настройка временного графика работы

Добавьте временный график для сотрудника, и ему будет назначен временный график смены. Также можно просматривать и редактировать детали временного графика работы

сотрудника.

Перед началом

В модуле **Person** («Сотрудник») добавьте отдел и сотрудника. Для подробной информации обратитесь к разделу ***Управление сотрудниками***.

Шаги

Примечание

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

1. Нажмите **Time & Attendance** → **Shift Schedule** («Учет рабочего времени→ Расписание смены») для перехода на страницу управления расписанием смен.
2. Нажмите **Person Schedule** («График работы сотрудника»), чтобы перейти на соответствующую страницу.
3. Выберите организацию и сотрудников.
4. Нажмите одну дату или щелкните и перетащите иконку, чтобы выбрать несколько дат для временного графика.
5. Выберите **Workday** («Рабочий день») или **Non-Workday** («Нерабочий день») из выпадающего списка.

   При выборе нерабочего дня необходимо установить следующие параметры.

   Рассчитывается как

   Выберите обычный или сверхурочный уровень работы, чтобы отметить статус посещения для временного графика.

   Расписание

   Выберите **Timetable** («Расписание») из выпадающего списка.

   График работы для нескольких смен

   Данный график содержит более одного расписания. Сотрудник может пройти регистрацию во время действия любого расписания, и статус его посещения будет эффективным.
   Если график работы для нескольких смен содержит три расписания: с 00:00 до 07:00, с 08:00 до 15:00 и с 16:00 до 23:00. Статус посещения сотрудника с данным графиком работы будет эффективным в любом из трех расписаний. Если сотрудник приходит на работу в 07:50, будет применено ближайшее расписание с 08:00 до 15:00 для регистрации его прихода.

   Правило

   Установите дополнительное правило для графика, например **Check-in Not Required** («Регистрация прихода не требуется») и **Check-out Not Required** («Регистрация ухода не требуется»).
6. Нажмите **Save** («Сохранить»).

Проверка графика для работы смены

Проверить график смены можно в календаре или в списке. Также можно изменить или удалить график смены.

Шаги

1. Нажмите **Time & Attendance** → **Shift Schedule** («Учет рабочего времени→ Расписание смены») для перехода на страницу управления расписанием смен.
2. Выберите организацию и сотрудников.
3. Нажмите  или  для просмотра графика смены в календаре или в списке.

Календарь

В календаре можно просматривать графики смен на каждый день в течение месяца. Назначьте временный график на один день, чтобы изменить или удалить его.

Список

В списке можно просмотреть сведения о графике смены одного сотрудника или организации, а именно наименование, тип, смены, срок действия графика смены и т. д. Выберите график и нажмите **Delete** («Удалить») для удаления выбранных графиков.

9.11.5 Изменение записи регистрации прихода/ухода вручную

Если статус посещения неверен, можно вручную исправить запись о регистрации прихода/ухода. Также можно редактировать, удалять и экспортировать записи о регистрации.

Перед началом

- Добавьте организацию и сотрудников в модуле **Person** («Сотрудник»). Для подробной информации обратитесь к разделу ***«Управление сотрудниками»***.
- Статус посещения некорректен.

Шаги

1. Нажмите **Time and Attendance → Attendance Handling** («Учет рабочего времени → Обработка записей о посещениях»), чтобы перейти на страницу обработки записей о посещениях.
2. Нажмите **Correct Check-In/Out** («Изменить запись о регистрации прихода/ухода вручную»), чтобы перейти на страницу изменения записи регистрации прихода/ухода.
3. Выберите сотрудника (сотрудников) из списка слева для внесения изменений.
4. Выберите дату внесения изменений.
5. Выберите тип изменения: **Check-in** («Регистрация прихода»), **Check-out** («Регистрация ухода»), **Break-in** («Начало перерыва»), **Break-out** («Окончание перерыва») и другое и установите правильное время.

Примечание

Нажмите , чтобы добавить несколько пунктов для изменения записи. Можно добавить до 8 пунктов.

6. Опционально. При необходимости создайте примечание.
7. Нажмите **Save** («Сохранить»), чтобы сохранить вышеуказанные настройки.
8. Опционально. После добавления корректировки записи регистрации прихода/ухода выполните следующие действия:

Виды

Нажмите или для просмотра информации об обработке записей о посещениях в календаре или в списке.

Изменение

- В режиме календаря нажмите → **Edit** («Изменить»), чтобы изменить сведения.
- В режиме просмотра списка дважды нажмите соответствующее поле в столбце **Date** («Дата»), **Handling Type** («Тип обработки»), **Time** («Время») или **Remark** («Примечание»), чтобы изменить сведения.

Примечание

Изменения вступят в силу.

Удаление

- В режиме календаря выберите одно изменение записи регистрации прихода/ухода и нажмите **Delete** («Удалить»), чтобы удалить выбранный элемент.
- В режиме списка выберите одно или несколько изменений записей регистрации прихода/ухода и нажмите **Delete** («Удалить»), чтобы удалить выбранные элементы.

Примечание

Внесенные изменения будут удалены.

Экспорт

В режиме списка выберите одно или несколько изменений записи регистрации прихода/ухода, чтобы экспортировать данные УРВ (файл CSV) на локальный компьютер.

9.11.6 Добавление отпусков и командировок

Добавьте отпуск или командировку при необходимости.

Перед началом

Добавьте организацию и сотрудников в модуле **Person** («Сотрудник»). Для подробной информации обратитесь к разделу ***«Управление сотрудниками»***.

Шаги

1. Нажмите **Time and Attendance → Attendance Handling** («Учет рабочего времени → Обработка записей о посещениях»), чтобы перейти на страницу обработки записей о посещениях.
2. Нажмите **Apply for Leave/Business Trip** («Добавить отпуск/командировку»), чтобы перейти на страницу добавления отпусков/командировок.
3. Выберите сотрудника из списка слева для внесения изменений.
4. Выберите даты командировки или отпуска.
5. Выберите основной тип отпуска и дополнительный тип отпуска из выпадающего списка.

Примечание

Установите тип отпуска в настройках посещаемости. Для получения подробной информации обратитесь к разделу ***«Настройка типа отпуска»***.

6. Установите время отпуска.
7. Опционально. При необходимости создайте примечание.
8. Нажмите **Save** («Сохранить»).
9. Опционально. После добавления отпуска или командировки выполните следующие действия.

Виды	Нажмите  или  для просмотра информации об обработке записей о посещениях в календаре или в списке.
	Примечание В режиме просмотра календаря нажмите **Calculate** («Рассчитать»), чтобы получить информацию о статусе посещений сотрудника за один месяц.
Изменение	● В режиме просмотра календаря нажмите на иконку даты посещения для редактирования записи. ● В режиме просмотра списка дважды щелкните соответствующий файл в столбце **Date** («Дата»), **Handling Type** («Тип обработки»), **Time** («Время») или **Remark** («Примечание»), чтобы изменить информацию.

Удаление	Удалите выбранные пункты.
Экспорт	Экспортируйте информацию об обработке записей о посещениях на компьютер.

Примечание

Экспортируемые файлы сохраняются в формате CSV.

9.11.7 Расчет данных о посещаемости вручную

Перед поиском и просмотром обзора данных о посещаемости, подробных данных о посещаемости сотрудников, данных об отклонениях в посещаемости сотрудников, информации о сверхурочной работе сотрудников и журнала считывания карт необходимо рассчитать данные о посещаемости.

Автоматический расчет данных о посещаемости

Настройте график таким образом, чтобы клиентское ПО автоматически рассчитывало данные о посещаемости за предыдущий день в настроенное время.

Шаги

Примечание

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Settings** → **General Rule** («Настройки посещаемости → Общее правило»).
3. В области автоматического расчета посещаемости укажите время для расчета данных клиентским ПО.
4. Нажмите **Save** («Сохранить»).
   Клиентское ПО рассчитает данные о посещаемости за предыдущий день с указанного момента.

Расчет данных о посещаемости вручную

Можно вручную рассчитать данные о посещаемости, задав условия, включая продолжительность посещаемости, отдел, состояние УРВ и т. д.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Statistics** → **Calculation** («Статистика посещений → Расчет»).

3. Установите время начала и время окончания, чтобы определить диапазон данных о посещениях.
4. Выберите отдел в выпадающем списке.
5. Опционально. Укажите другие условия, включая имя и идентификатор сотрудника.
6. Выберите состояние УРВ (поддержка множественного выбора).
7. Нажмите **Calculate** («Расчет»).

Примечание

Можно рассчитать только данные УРВ за три месяца.

8. Опционально. Выполните одну из следующих операций.

Изменение записи регистрации прихода/ухода	Выберите сотрудника, нажмите **Correct Check-in/out (**«Изменение записи регистрации прихода/ухода») для добавления изменений в записи регистрации прихода/ухода.
Выбор пунктов, которые необходимо отобразить	Чтобы настроить элементы, которые будут отображаться в списке, Нажмите в правом верхнем углу или нажмите правой кнопкой мыши заголовок таблицы в списке данных УРВ.
Настройка последовательности элементов	Нажмите один элемент (кроме идентификатора сотрудника) и переместите курсор мыши, чтобы настроить последовательность различных элементов.
Создание отчета	Нажмите **Report** («Отчет»), чтобы создать отчет по посещению. **Примечание** Элементы отчета будут отображаться в установленной последовательности.
Экспорт отчета	Нажмите **Export** («Экспорт»), чтобы экспортировать данные УРВ (CSV-файл) на компьютер. **Примечание** Элементы отчета будут отображаться в установленной последовательности.

9.11.8 Статистика УРВ

Проверьте исходную запись о посещении, сгенерируйте и экспортируйте отчет по посещению, созданный на основе рассчитанных данных.

Получение обзора данных о посещаемости сотрудников

В клиентском ПО можно найти и посмотреть данные УРВ сотрудника, в том числе длительность посещения, состояние УРВ, контрольный пункт проверки и т. д.

Перед началом

- Добавьте организацию и сотрудников в модуле **Person** («Сотрудник»). Считайте карты сотрудников. Для подробной информации обратитесь к разделу ***«Управление сотрудниками»***.
- Рассчитайте данные о посещаемости

Примечание

- Клиентское ПО автоматически рассчитает данные о посещаемости за предыдущий день в 1:00 утра следующего дня.
- Клиентское ПО должно быть включенным в 1:00 утра, чтобы автоматически рассчитать данные о посещаемости за предыдущий день. Если расчет не был выполнен автоматически, можно выполнить расчет данных о посещаемости вручную. Более подробная информация представлена в разделе ***«Расчет данных о посещаемости вручную»***.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Statistics** → **Attendance Record** («Статистика посещений → Запись о посещении»).
3. Установите время начала и время окончания искомого посещения.
4. Укажите другие условия поиска, включая отдел, имя и идентификатор сотрудника.
5. Выберите источник данных: **All** («Все»), **Original Records on Device** («Исходная запись на устройстве») или **Manual Handled Records** («Обработка записей вручную»).
6. Опционально. Нажмите **Get Events from Device** («Получение информации о событии с устройства»), чтобы получить информацию о посещении с устройства.

Примечание

Два метода получения событий УРВ с устройства: **Online** («Онлайн») и **Import File** («Импорт файла»). Более подробная информация об операциях представлена в разделе *«Получение информации о событии с устройства»* Руководства пользователя клиентского программного обеспечения.

7. Опционально. Нажмите **Reset** («Сбросить»), чтобы сбросить все условия поиска, затем повторно отредактируйте условия поиска.

8. Нажмите **Search** («Поиск»).
9. Опционально. С отображаемыми результатами поиска можно выполнить одну из следующих операций.

Изменение состояния УРВ	Выберите одну ошибочную запись, дважды нажмите поле столбца **Attendance Status** («Состояние УРВ») и выберите из раскрывающегося списка элемент для изменения. Выберите две или более ошибочные записи, нажмите **Edit Attendance Status** («Изменить состояние УРВ») в верхнем левом углу и выберите из раскрывающегося списка элементы для изменения в пакетном режиме.
Создание отчета	Нажмите **Report** («Отчет»), чтобы создать отчет по посещению.
Экспорт отчета	Нажмите **Export** («Экспорт») и выберите путь для сохранения экспортированного отчета о УРВ (CSV-файл) на локальном компьютере.
Настройки экспорта	Нажмите **Custom Report** («Настройки отчета») и установите условия для экспорта записей УРВ в соответствии с потребностями. Более подробная информация представлена в разделе *«Настраиваемый экспорт записей УРВ»* Руководства пользователя клиентского программного обеспечения.

Создание мгновенного отчета

Поддерживается функция создания серии отчетов о посещаемости вручную для просмотра посещаемости сотрудников.

Перед началом

Рассчитайте данные о посещаемости

Примечание

Рассчитайте данные УРВ вручную или установите расписание таким образом, чтобы клиентское ПО производило расчет данных автоматически каждый день. Более подробная информация представлена в разделе ***«Расчет данных УРВ»***.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Statistics** → **Report** («Статистика посещений → Отчет»).
3. Выберите **Report Type** («Тип отчета»).
4. Выберите отдел или сотрудника, чтобы просмотреть отчет по посещению.
5. Укажите время начала и время окончания периода, в течение которого данные УРВ будут отображены в отчете.
6. Нажмите **Report** («Отчет»), чтобы создать статистический отчет и открыть его.

Регулярная отправка отчета

Клиентское ПО поддерживает несколько типов отчетов. Можно предварительно определить содержимое отчета и автоматически отправлять отчет на указанный адрес электронной почты.

Шаги

1. Войдите в модуль **Time & Attendance** («Учет рабочего времени»).
2. Нажмите **Attendance Statistics** → **Regularly Send Report** («Статистика посещений → Регулярная отправка отчета»).
3. Нажмите **Add** («Добавить») для перехода на страницу добавления настраиваемой отчетности.
4. Установите содержимое отчета.

   Наименование отчета

   Введите наименование отчета.

   Тип отчета

   Выберите тип отчета, чтобы сгенерировать этот отчет.

   Период отчета

   Период отчета может различаться в зависимости от типа отчета.

   Сотрудник

   Выберите сотрудников, данные о посещениях которых необходимо включить в отчет.

   Примечание

   Можно просмотреть выбранных сотрудников в правой части области сотрудников.

5. Настройте график автоматического отправления отчета на электронный адрес.

   Примечание

   Функция **Auto-Send Email** («Автоматическая отправка Email») включена по умолчанию.

   1) Задайте период, в течение которого клиентское ПО будет отправлять отчеты.
   2) Задайте дату (даты) отправки, когда клиентское ПО будет отправлять отчет.
   3) Задайте время отправки отчета.

   Пример

   Установите период с 10.03.2018 по 10.04.2018, выберите пятницу в качестве даты отправки и установите время отправки в 20:00:00, клиентское ПО будет отправлять отчеты в 20:00 по пятницам с 10.03.2018 по 10.04.2018.

Примечание

Перед настройкой времени произведите расчет статистики посещений. Рассчитайте данные УРВ вручную или установите расписание таким образом, чтобы клиентское ПО производило расчет данных автоматически каждый день. Более подробная информация представлена в разделе ***«Расчет данных УРВ»***.

4) Введите электронный адрес получателя.

Примечание

Можно добавить до 5 адресов. Нажмите **+**, чтобы добавить новый адрес электронной почты.

5) Опционально. Нажмите **Preview** («Предварительный просмотр») для просмотра параметров адреса электронной почты.

6. Нажмите **OK**.
7. Опционально. После добавления настроенного отчета выполните следующие действия:

Редактирование отчета	Выберите отчет и нажмите **Edit** («Редактировать»), чтобы изменить его параметры.
Удаление отчета	Выберите отчет и нажмите **Delete** («Удалить»), чтобы удалить его.
Создание отчета	Выберите один отчет и нажмите **Report** («Отчет»), чтобы мгновенно создать отчет и просматривать его содержание.

9.12 Настройки системы

9.12.1 Настройка основных параметров

Можно настроить часто используемые параметры, включая срок действия журнала, настройки сети и т. д.

Шаги

1. Войдите в модуль настройки системы.
2. Нажмите вкладку **General** («Основные параметры»), чтобы перейти на страницу настройки основных параметров.
3. Настройте основные параметры.

Формат даты/формат времени

Отображение даты и времени на страницах.

Срок действия журнала

Указана продолжительность хранения журналов. При истечении срока действия

журналы будут удалены.

Режим максимального отображения

В качестве максимального режима выберите **Maximize** («Развернуть») или **Full Screen** («Полный экран»). В режиме развертывания можно развернуть окно отображения и отобразить панель задач. В полноэкранном режиме информация отображается на всем экране.

Тип календаря

Выберите **Gregorian Calendar** («Григорианский календарь») или **Nepali Calendar** («Непальский календарь») в качестве типа календаря. При выборе непальского календаря календарь переключится на непальский язык, и время будет рассчитываться по непальскому календарю. После переключения календаря необходимо перезапустить клиент.

Сетевые характеристики

Выберите условия соединения как **Normal** («Нормальные»), **Better** («Хорошие») или **Best** («Отличные»).

Сохранение изображений в формате структурированных данных

Можно включить **Save Pictures in Structure Data Format** («Сохранение изображений в формате структурированных данных»), чтобы сохранить данные структуры и удалить зарегистрированное изображение.

Сохранение события

Задайте цикл удаления старых событий.

Поиск новой версии программного обеспечения

После включения клиент может автоматически определять новую версию программного обеспечения и напоминать пользователю об обновлении программного обеспечения.

Автоматическая синхронизация времени

Автоматическая синхронизация времени добавленных устройств со временем ПК, на котором запущен клиент, в указанный момент времени.

Автоматическое обновление устройства

Установите режим обновления после обнаружения новой версии устройства.

Отключить

После включения клиент не будет загружать пакет прошивки и обновлять его, даже если клиент обнаруживает новую версию клиента.

Уведомление о загрузке и обновлении

После того, как клиент обнаружит новую версию устройства, он предложит пользователю загрузить пакет прошивки и обновить его.

Загрузка пакета обновления и уведомление об обновлении

После того, как клиент обнаружит новую версию устройства, он автоматически загрузит пакет прошивки и предложит пользователю выполнить обновление.

Автоматическая загрузка и предупреждение

После того, как клиент обнаружит новую версию устройств, он загрузит пакет прошивки и автоматически обновит новую версию.
При этом необходимо задать расписание в поле **Upgrade Time** («Время обновления»), когда клиент автоматически обновляет новую версию.

4. Нажмите **Save** («Сохранить»).

9.12.2 Настройка хранения изображений

Изображения тревожных событий, полученные с камеры терминала контроля доступа, могут быть сохранены на ПК, на котором запущена платформа iVMS-4200. Здесь можно вручную задать путь хранения изображений.

Шаги

1. Войдите в модуль настройки системы.
2. Нажмите **Event Picture Storage** («Хранение изображений событий»).
3. Установите переключатель **Store Pictures in Server** («Хранить изображения на сервере») в положение «Вкл.».
   Будут показаны все диски компьютера, на котором запущена служба iVMS-4200.
4. Выберите диск для сохранения изображений.

Примечание

Путь сохранения по умолчанию: Disk/iVMS-4200alarmPicture

5. Нажмите **Save** («Сохранить»).

9.12.3 Настройка звукового сигнала тревоги

При тревожном событии клиент выдает звуковое предупреждение, чтобы уведомить персонал службы безопасности. В этом разделе можно настроить звук звукового предупреждения.

Шаги

1. Откройте страницу настройки системы.
2. Нажмите вкладку **Alarm Sound** («Звуковой сигнал тревоги»), чтобы перейти на страницу настройки параметров звукового сигнала тревоги.
3. Опционально. Нажмите и выберите аудиофайлы для различных событий из локального хранилища.
4. Опционально. Добавление настраиваемого звукового сигнала.
   1) Нажмите **Add** («Добавить») для добавления настраиваемого звукового сигнала.

2) Дважды нажмите поле **Type** («Тип»), чтобы настроить название звукового сигнала.
3) Нажмите и выберите аудиофайлы для различных событий из локального хранилища.

5. Опционально. Нажмите для проверки аудиофайла.
6. Опционально. Нажмите в столбце **Operation** («Операции») для удаления настраиваемого звукового сигнала.
7. Нажмите **Save** («Сохранить»).

Примечание

Поддерживается только WAV-формат аудиофайла.

9.12.4 Настройка параметров контроля доступа и видеодомофонии

В соответствии с требованиями можно настроить параметры контроля доступа и видеодомофонии.

Шаги

1. Откройте страницу настройки системы.
2. Нажмите вкладку **Access Control & Video Intercom** («Контроль доступа и видеодомофония»).
3. Введите необходимую информацию.

Мелодия звонка

Нажмите и выберите аудиофайл мелодии звонка видеодомофона из локального хранилища. Кроме того, можно нажать для проверки аудиофайла.

Максимальная продолжительность звонка

Задайте значение максимальной продолжительности звонка (в секундах). Максимальная продолжительность звонка может быть установлена в диапазоне от 15 до 60 секунд.

Максимальная продолжительность сеанса видеодомофонии

Задайте максимальную продолжительность сеанса видеодомофонии. Максимальная продолжительность сеанса видеодомофонии может быть установлена в диапазоне от 120 до 600 с.

Максимальная продолжительность сеанса домофонии

Задайте максимальную продолжительность сеанса домофонии. Максимальная продолжительность сеанса домофонии может быть установлена в диапазоне от 90 до 120 с.

Максимальная продолжительность сеанса связи с устройством контроля доступа

Задайте максимальную продолжительность сеанса связи с устройством контроля доступа. Максимальная продолжительность сеанса связи с устройством контроля доступа может быть установлена в диапазоне от 90 до 120 с.

4. Нажмите **Save** («Сохранить»).

9.12.5 Настройка пути сохранения файлов

Изображения, полученные в модуле мониторинга состояния, хранятся на локальном ПК. Можно настроить путь сохранения этих файлов.

Шаги

1. Откройте страницу настройки системы.
2. Нажмите вкладку **File** («Файл»), чтобы перейти на страницу **File Saving Path Settings** («Настройка пути сохранения файлов»).
3. Нажмите и выберите локальный путь для файлов.
4. Нажмите **Save** («Сохранить»).

9.12.6 Настройка параметров электронной почты

При включении функции **Send Email** («Отправить Email») клиент отправит получателям электронное письмо для уведомления о тревожном событии. В этом разделе необходимо настроить параметры электронной почты и указать получателей.

Шаги

1. Войдите в модуль настройки системы.
2. Нажмите вкладку **Email** («Электронная почта»), чтобы перейти на страницу настройки параметров электронной почты.
3. Введите необходимую информацию.

SMTP-сервер

IP-адрес STMP-сервера или имя хоста (например, smtp.263xmail.com).

Тип шифрования

Можете проверить связь и выбрать **Non-Encrypted** («Незашифрованный»), **SSL** («Протокол SSL») или **STARTTLS** («Протокол STARTTLS»).

Порт

Настройте порт связи, используемый для SMTP. Порт по умолчанию: 25.

Адрес отправителя

Адрес электронной почты отправителя.

Сертификат безопасности (необязательно)

Если для входа на почтовый сервер требуется аутентификация, выберите данную функцию, чтобы пройти аутентификацию для входа на сервер. Введите имя пользователя и пароль для входа в учетную запись электронной почты.

Имя пользователя

Если выбрано **Server Authentication** («Серверная аутентификация»), необходимо ввести имя учетной записи пользователя, которая принадлежит отправителю электронного письма.

Пароль

Если выбрано **Server Authentication** («Серверная аутентификация»), необходимо ввести пароль учетной записи пользователя, которая принадлежит отправителю электронного письма.

Количество получателей электронного письма

Введите адрес электронной почты получателя. Можно настроить до трех получателей.

4. Опционально. Нажмите **Send Test Email** («Отправить тестовое электронное письмо»), чтобы отправить получателю электронное письмо для проверки.
5. Нажмите **Save** («Сохранить»).

9.13 Эксплуатация и техническое обслуживание

Чтобы обеспечить бесперебойное и удобное использование клиента, можно выполнять операции технического обслуживания через меню.

В правом верхнем углу клиента нажмите → **File** → **System** → **Tool** («Файл → Система → Инструмент») и выполните следующие операции.

Открытие файла журнала

Можно открыть сохраненный на локальном ПК файл журнала или файлы журнала клиента.

Импорт/экспорт файла конфигурации

При необходимости можно импортировать файлы конфигурации с локального ПК на клиент (и наоборот).

Автоматическое резервное копирование

Выберите день и время для резервного копирования файлов конфигурации и данных, а также для восстановления данных из резервной копии.

Оформление клиента

Измените цвет оформления клиента.

Синхронизация времени в пакетном режиме

Синхронизируйте время выбранных устройств со временем ПК.

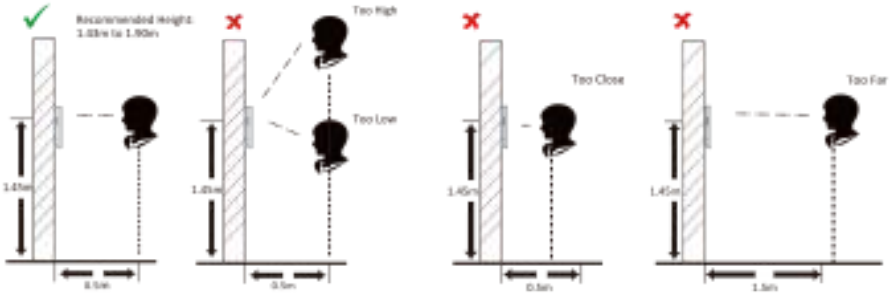
Очередность сообщений

После настройки электронной почты здесь будут отображаться сообщения о тревожных событиях. Выберите событие и отмените отправку электронного письма получателю.

A. Советы по сбору/сравнению изображений лиц

Положение при сборе или сравнении изображения лица:

Положения (рекомендуемое расстояние: 0.5 м)



Английский язык	Русский язык
Recommended Height: 1.43 m to 1.90 m	Рекомендуемая высота: от 1.43 до 1.90 м
Too High	Слишком высоко
Too Low	Слишком низко
Too Close	Слишком близко
Too Far	Слишком далеко

Выражение лица

- Сохраняйте свое естественное выражение лица при сборе или сравнении изображений лиц, как это показано на рисунке ниже.

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

Положение лица

Для получения качественного и точного изображения лица, смотрите прямо в камеру при

сборе или сравнении изображений лиц.

Английский язык	**Русский язык**
Correct	Правильно
Tilt	Наклон набок
Side	Поворот
Raise	Подъем
Bow	Наклон вниз

Размер

Убедитесь, что ваше лицо находится в середине окна сбора данных.

Английский язык	**Русский язык**
Correct	Правильно
Too Close	Слишком близко
Too Far	Слишком далеко

Б. Рекомендации по среде установки

1. Номинальное значение освещенности источника света

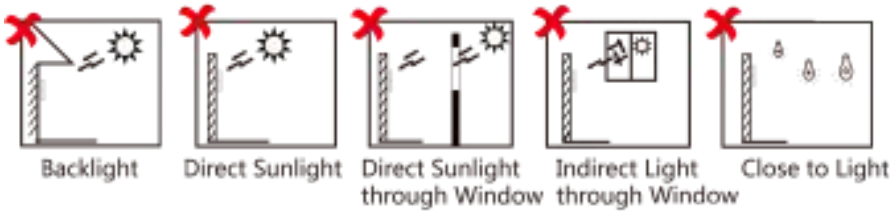
Свеча: 10 лк

Лампа: 100 ~ 850 лк

Солнечный свет: свыше 1200 лк

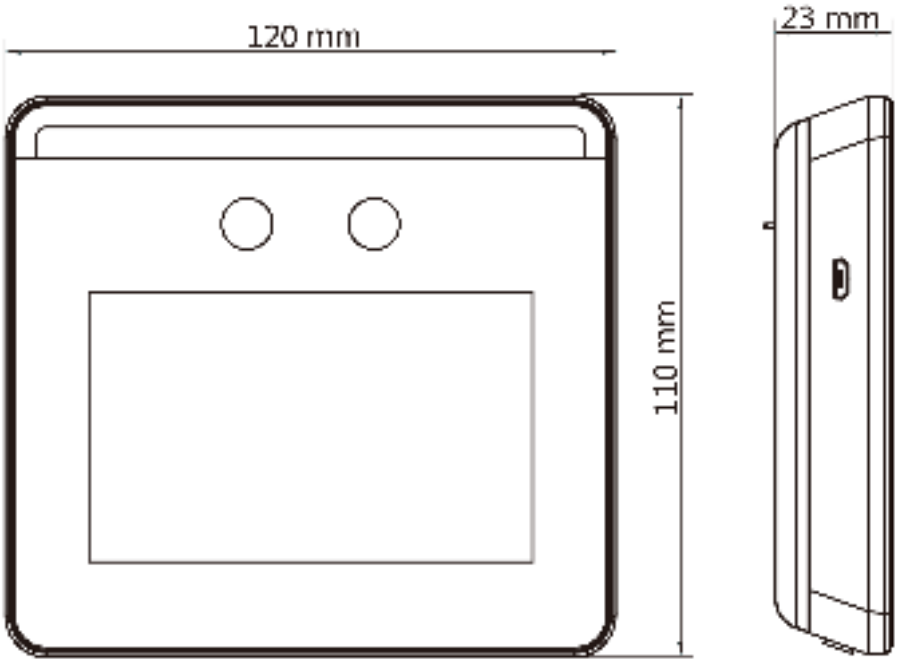
2. При установке устройства в помещении устройство должно находиться на расстоянии не менее 2 метров от источника света и не менее 3 метров от окна или двери.

Избегайте засветки, а также воздействия прямых и отраженных солнечных лучей.



Английский язык	**Русский язык**
Backlight	Сильная задняя засветка
Direct Sunlight	Прямые солнечные лучи
Direct Sunlight through Window	Прямые солнечные лучи, падающие через окно
Indirect Light through Window	Рассеянные солнечные лучи, падающие через окно
Close to Light	Близко расположенный источник света

C. Размеры



D. Коммуникационная матрица и команды устройства

Коммуникационная матрица

Сканируйте следующий QR-код, чтобы получить коммуникационную матрицу устройства. Обратите внимание, что в матрице представлены все порты связи устройств контроля доступа и видеодомофонии Hikvision.

Рисунок D-1. QR-код коммуникационной матрицы

Команды устройства

Сканируйте следующий QR-код, чтобы получить общие команды серийного интерфейса устройства.
Обратите внимание, что в списке команд представлены все часто используемые команды серийных интерфейсов для всех устройств контроля доступа и видеодомофонии Hikvision.

Рисунок D-2. Команды устройства

hi.watch