Комплекс тепловизионного контроля измерительный стационарный серии DS-K

Руководство по эксплуатации

Правовая информация

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.
 **Примечания**	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. Устройство должно выдерживать возможные излучения, включая и те, которые могут привести к выполнению нежелательных операций.

Соответствие стандартам ЕС

Данный продукт и (если применимо) поставляемые принадлежности отмечены знаком «CE» и, следовательно, согласованы с европейскими стандартами, перечисленными под директивой 2014/30/EC EMC, директивой 2014/53/EC RE, директивой 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. Для получения конкретной информации о батарее см. документацию по продукту. Батарея помечена символом, который может включать буквенное обозначение, сообщающее о наличии кадмия (Cd), свинца (Pb) или ртути (Hg).
Для надлежащей утилизации возвратите батарею своему поставщику или утилизируйте ее 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 любого из предостережений может привести к травмам или порче оборудования.

⚠	⚠
Предупреждения: следуйте данным правилам для предотвращения	**Предостережения:** следуйте мерам предосторожности, чтобы предотвратить

⚠Предупреждения:

- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в регионе эксплуатации.
- Используйте адаптер питания, входящий в комплект поставки. Это оборудование предназначено для питания от источника питания с защитой от перенапряжения класса 2, рассчитанного на DC 12 В, 2 А.
- 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.
- Избегайте проглатывания батареи, существует опасность химического ожога.
  Данное устройство оснащено батареей таблеточного типа. Проглатывание батареи таблеточного типа может вызвать серьезные внутренние ожоги всего за 2 часа и привести к смерти.
  Храните новые и использованные батареи в недоступном для детей месте. Если батарейный отсек не закрывается надежно, прекратите использование устройства и держите его подальше от детей. При подозрении, что кто-то мог проглотить батареи или поместить их внутрь какой-либо части тела, немедленно обратитесь к врачу.
- 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. Замена допускается исключительно на аналогичную батарею или батарею эквивалентного типа. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем батарей.
- Продукты с биометрическим распознаванием не на 100% применимы для защиты от подделки биометрических данных. Если требуется более высокий уровень безопасности, используйте несколько режимов аутентификации.
- Рабочая температура: от +10 до +35 °C; рабочая влажность: не более 90 % (без конденсата)
- Использование в помещениях. При установке устройства в помещении устройство необходимо разместить на расстоянии не менее 2 метров от источника света и не менее 3 метров от окна.

Доступные модели

Наименование	Модель
Терминал доступа с функцией распознавания лиц	DS-K5604A-3XF/V

Используйте только те источники питания, которые указаны ниже:

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

Содержание

Раздел 1 Обзор

Комплекс тепловизионного контроля измерительный стационарный серии DS-K (далее по тексту – комплекс) предназначен для непрерывных бесконтактных (дистанционных) измерений температуры тела человека в процессе эпидемиологического контроля (мониторинга) мест большого скопления или большой проходимости людского потока, при этом, измерения происходят в пределах зоны, определяемой полем зрения оптической системы тепловизионной камеры (терминала), и визуализации информации на мониторе терминала и (или) персонального компьютера.

В состав комплекса входят:

– терминал доступа, обеспечивающий измерение температуры тела человека;

– излучатель в виде модели «абсолютно чёрного тела» (далее по тексту - АЧТ), излучающий в инфракрасном спектре эквивалент постоянной температуры (установленная температура плюс 40 °С), основываясь на котором, измерительный алгоритм тепловизионной камеры автоматически производит постоянную «самокалибровку» в процессе измерений. АЧТ поставляется по дополнительному заказу;

– программное обеспечение (далее по тексту - ПО), которое устанавливается на компьютер контролирующего сотрудника, позволяет дистанционно получать результаты измерений температуры людей, выдает звуковой сигнал сирены при обнаружении и управлять основными функциями терминала.

В данном руководстве описан терминал доступа, входящий в состав комплекса DS-K5604A-3XF/V (серия DS-K)

1.1 Обзор

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

- Plug & play

  Быстрое развертывание Беспроводная установка/конфигурация
- Для измерения температуры тела используется неохлаждаемый микроболометрический детектор (оксид ванадия)
- Пределы допускаемой абсолютной погрешности измерений температуры:
  - в диапазоне температур от +30 до +32 °С, не включ.: ±1.0 °С
  - в диапазоне температур от +32 до +44 °С: ±0.5 (*); ±1.0(**)°С
- Дальность распознавания: от 0.3 до 2 м
- Простое измерение температуры: Детекция лица и одновременное распознавание поверхностной температуры тела человека, без аутентификации
- Разные режимы аутентификации совместно с функцией измерения температуры тела
- Тревога наличия/отсутствия маски

- При отсутствии респираторной маски устройство выдает голосовое предупреждение. Совместно с тревогой наличия/отсутствия маски устройство проводит аутентификацию, если аутентификация пройдена, проход разрешается. Принудительная тревога при отсутствии маски
  При отсутствии респираторной маски устройство выдает голосовое предупреждение. При использовании принудительной тревоги устройство запрещает проход при отсутствии маски, даже если аутентификация пройдена.
- Отображение измеренной температуры на экране аутентификации
- При превышении установленного порога температуры тела звучит голосовое предупреждение
- Конфигурация состояния двери (открыто/закрыто) с привязкой к порогу температуры
- Передача данных в клиентское программное обеспечение по протоколу TCP/IP и сохранение данных
- Конструкция учитывает возможность интеграции со стойкой
- Связь со сторонними турникетами при помощи IO выхода или Wiegand
- Регулируемая яркость подсветки
- Высокопроизводительный процессор с алгоритмом глубокого обучения. Кол-во изображений лиц: 50,000;
  кол-во событий: 100,000
- Время распознавания лиц ≤ 0.2 с/чел.; точность распознавания лиц ≥ 99%
- Передает и сохраняет результаты сравнения и захваченные изображения в Клиентское ПО или другое ПО
- NTP, синхронизация времени вручную и автоматическая синхронизация
- Поддержка ISAPI
- Функция сторожевого таймера для защиты и обеспечения правильной работы устройства
- Звуковое предупреждение при аутентификации

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

Примечания:
(*) - данное значение погрешности достигается при совместном использовании тепловизионной камеры со специальным ПО и высокостабильным излучателем в виде модели АЧТ (поставляется по дополнительному заказу) и находящимся в его поле зрения (при проведении измерений), и подтверждается при помощи метода передачи единицы температуры контактным способом с использованием вспомогательной вставки-излучателя с эталонным термометром, находящимся внутри корпуса вставки, помещенной в жидкостной термостат переливного типа;
(**) – без использования комплектного излучателя.

Раздел 2 Внешний вид устройства

Для получения подробной информации о терминале распознавания лиц см.:

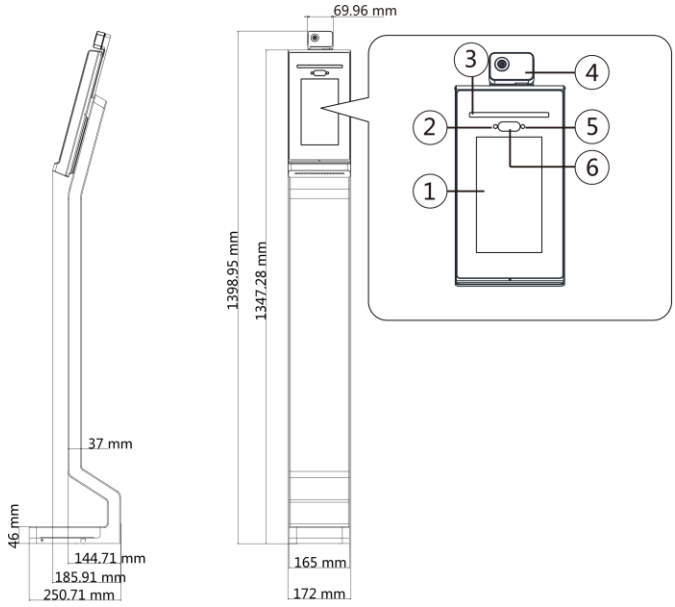


Рисунок 2-1 Схема терминала распознавания лиц

Таблица 2-1 Описание терминала распознавания лиц

№	Название
1.	Сенсорный экран
2	ИК-подсветка
3	Подсветка белым светом
4	Модуль тепловизора
5.	ИК-подсветка
6.	Камера

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.
- Используйте устройство только внутри помещений, не допускается сильная циркуляция воздуха.

Примечание

Для более подробной информации см. *Рекомендации по среде установки.*

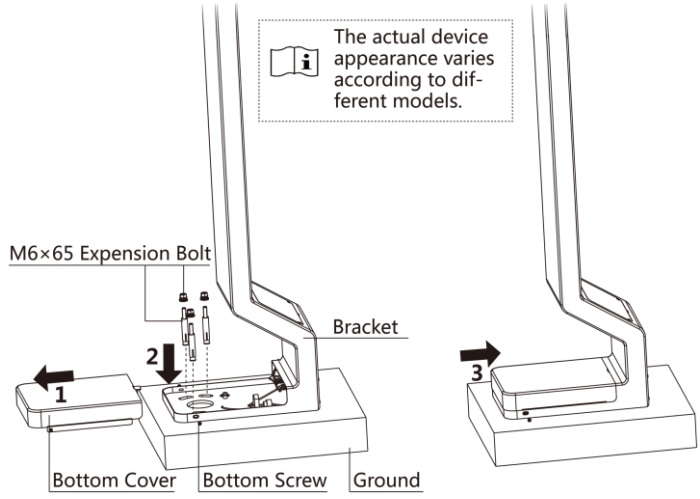
3.2 Установка устройства

Перед началом

Убедитесь, что на поверхности просверлены отверстия для установки устройства.

Шаги

1. Удалите два нижних винта (2-SC-KM3 × 5B-JMF) с обеих сторон нижней крышки.
2. Снимите нижнюю крышку.
3. Расположите устройство в соответствии с просверленными отверстиями и вставьте 3 прилагаемых дюбеля (M6 × 65). Убедитесь, что дюбели находятся выше уровня земли.
4. Закрепите дюбели с помощью гаек.
5. Расположите устройство в соответствии с монтажной платой и повесьте устройство на монтажной плате.
6. Установите нижнюю крышку на устройство с помощью 2 нижних винтов.



Английский язык	**Русский язык**
The actual device appearance varies according to different models.	Внешний вид устройства может отличаться в зависимости от модели.
M6 x 65 expansion bolt	Анкерный болт M6 x 65
Bracket	Кронштейн
Bottom cover	Нижняя крышка
Bottom screw	Нижний винт
Ground	Заземление

Рисунок 3- 1. Установка устройства

Примечание

- Устройство необходимо устанавливать на бетонную поверхность или на другие поверхности, не подвергаемые воспламенению.
- Устройство поддерживает технологию Plug & Play. Расположите устройство на поверхности, чтобы приступить к эксплуатации.

Раздел 4 Подключение

Устройство можно подключать к клемме RS-485, к дверному замку, к кнопке выхода, к устройствам вывода / ввода сигналов тревоги, к считывателю карт Wiegand, к терминалу контроль доступа и к источнику питания.

Подключите периферийные устройства в соответствии с описанием ниже.

Если соединить терминал WIEGAND с контроллером управления доступом, терминал распознавания лиц может передавать информацию аутентификации, на основании которой контроллер отпирает дверь или отказывает в доступе.

Примечание

- Если размер кабеля 18 AWG, используйте источник питания мощностью 12 В. Расстояние между источником питания и устройством не должно превышать 20 м.
- Если размер кабеля 15 AWG, используйте источник питания мощностью 12 В. Расстояние между источником питания и устройством не должно превышать 30 м.
- Если размер кабеля 12 AWG, используйте источник питания мощностью 12 В. Расстояние между источником питания и устройством не должно превышать 40 м.

4.1 Описание разъемов

Терминал оснащен входом питания, тревожным входом/выходом, RS-485, входом Wiegand и дверным замком.

Ниже представлена схема подключения терминала:

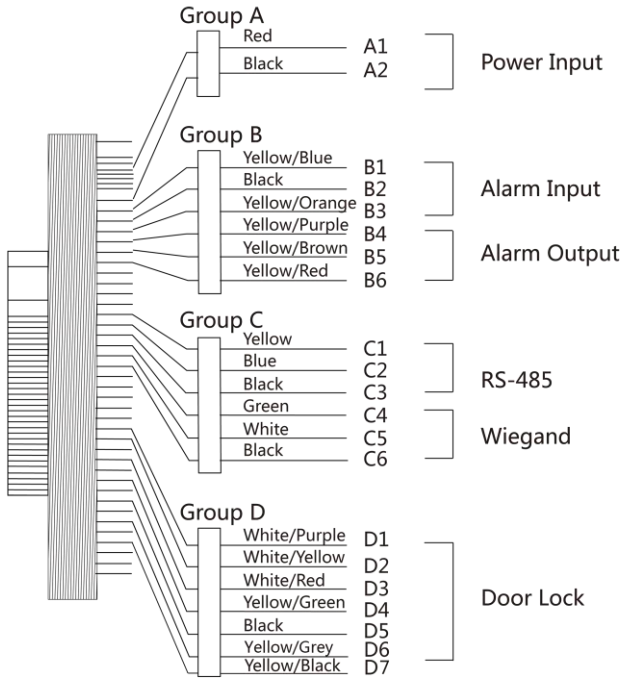


Рисунок 4-1 Схема подключения терминала

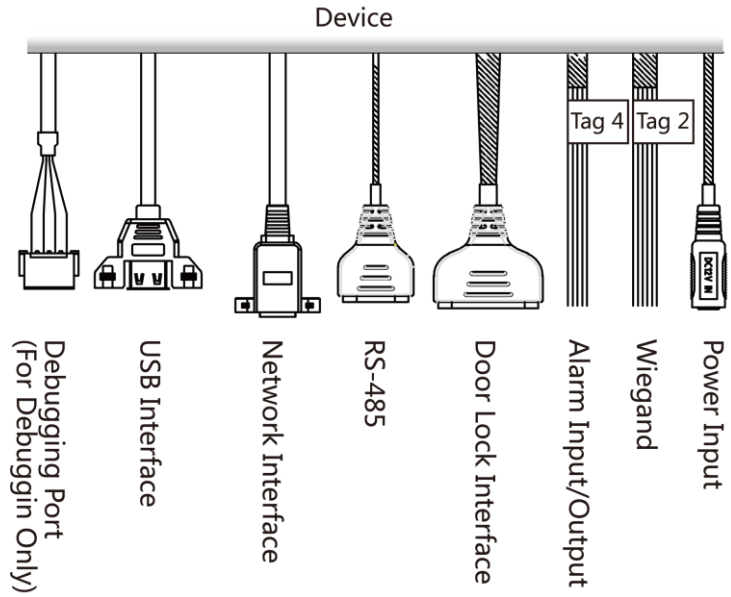
Терминал оснащен следующими разъемами:

Таблица 4-1 Описание разъемов

Группа	№	Функция	Цвет	Наименование	Описание
Группа A	A1	Вход питания	Красный	+12 В	Источник питания DC 12 В
	A2		Черный	GND	Заземление
Группа B	B1	Тревожный вход	Желто-голубой	IN1	Тревожный вход 1
	B2		Черный	GND	Заземление
	B3		Желто-оранжевый	IN2	Тревожный вход 2
	B4	Тревожный выход	Желто-фиолетовый	NC (нормально замкнутый)	Подключение тревожного выхода
	B5		Желто-коричневый	COM	
	B6		Желто-красный	NO (нормально разомкнутый)	
Группа C	C1	RS-485	Желтый	485+	Подключение по RS-485
	C2		Синий	485-	
	C3		Черный	GND	Заземление
	C4	Wiegand	Зеленый	W0	Подключение к Wiegand 0
	C5		Белый	W1	Подключение к Wiegand 1
	C6		Черный	GND	Заземление
Группа D	D1	Дверной замок	Бело-фиолетовый	NC (нормально замкнутый)	Подключение замка (NC)
	D2		Бело-желтый	COM	Обычный
	D3		Бело-красный	NO (нормально разомкнутый)	Подключение замка (NO)
	D4		Желто-зеленый	Матрица	Door Contact («Дверной контакт»)

	D5		Черный	GND	Заземление
	D6		Желто-серый	BTN	Подключение выходной двери
	D7		Желто-черный	GND	Заземление

4.2 Описание интерфейсов и меток



Английский язык	**Русский язык**
Power input	Вход питания
Wiegand	Интерфейс Wiegand
Alarm input/output	Тревожный вход/выход
Door lock interface	Интерфейс дверного замка
RS-485	Интерфейс RS-485
Network interface	Сетевой интерфейс
USB interface	USB-интерфейс
Debugging port (for debugging only)	Служебный порт (только для отладки)

Рисунок 4-2 Интерфейс подключения

Примечание

Описание меток 2 и 4 представлено в разделе ***Подключение устройства***.

4.3 Подключение устройства

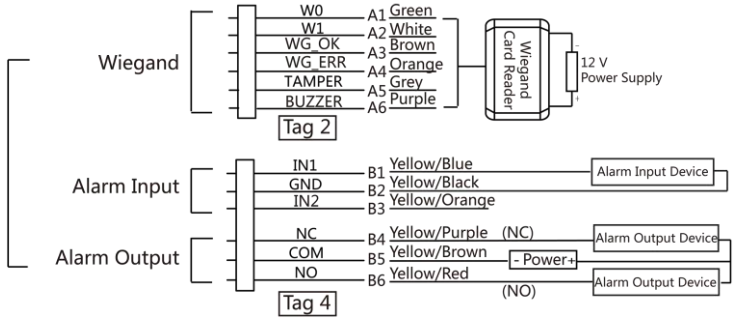


Рисунок 4- 3 Подключение устройства

Таблица 4-2 Описание разъемов

Группа	№	Функция	Цвет	Наименование	Описание
Метка 2	A1	Wiegand	Зеленый	W0	Подключение к Wiegand 0
	A2		Белый	W1	Подключение к Wiegand 1
	A3		Коричневый	WG_OK	Карта Wiegand аутентифицирована
	A4		Оранжевый	WG_ERR	Ошибка аутентификации карты Wiegand
	A5		Серый	Тампер	Подключение тампера
	A6		Фиолетовый	Бипер	Подключение бипера
Метка 4	B1	Тревожный вход	Желто-голубой	IN1	Тревожный вход 1
	B2		Желто-черный	GND	Заземление
	B3		Желто-оранжевый	IN2	Тревожный вход 2
	B4	Тревожный выход	Желто-фиолетовый	NC (нормально замкнутый)	Подключение тревожного выхода
	B5		Желто-коричневый	COM	
	B6		Желто-красный	NO (нормально разомкнутый)	

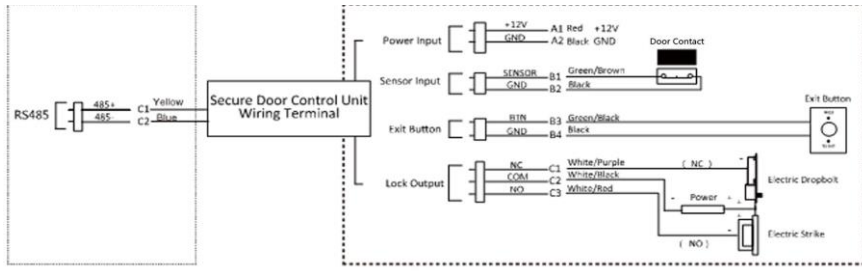
Примечание

- При этом для терминала доступа с функцией распознавания лиц необходимо задать направление Wiegand на значение **Input** («Вход») для подключения к считывателю карт Wiegand. Если необходимо подключиться к контроллеру доступа, задайте направление Wiegand на значение **Output** («Выход») для передачи информации аутентификации в терминал контроля доступа.
- Более подробная информация представлена в разделе ***Настройка параметров интерфейса Wiegand***.
- Рекомендуемые параметры блока питания: 12 В/ 2 А.

4.4 Подключение к модулю безопасности двери

Также можно подключить терминал к модулю безопасности

двери. Ниже представлена схема подключения.



Английский язык	**Русский язык**
Power input	Вход питания
Sensor input	Вход датчика
Exit button	Кнопка выхода
Lock output	Выход замка
Secure door control unit wiring terminal	Разъем модуля безопасности двери
Electric strike	Электрическая защелка
Door contact	Дверной контакт

Рисунок 4- 4 Схема подключения к модулю безопасности двери

Примечание

Модуль безопасности необходимо подключать к внешнему источнику питания отдельно. Рекомендуемые параметры внешнего источника питания составляют 12 В, 0.5 А.

Раздел 5 Активация устройства

Перед первым входом в систему 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.

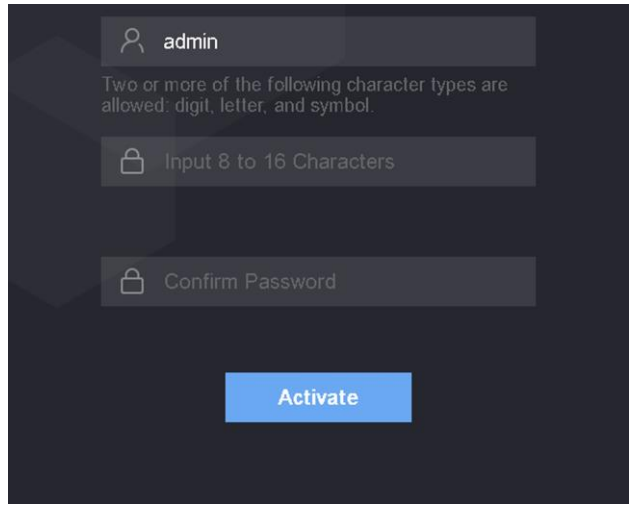


Рисунок 5-1 Страница активации

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется установить пароль самостоятельно (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные

символы) для обеспечения безопасности продукта. Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит повысить безопасность при использовании продукта.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

- После активации, выберите режим работы. Для получения подробной информации обратитесь к разделу ***Настройки режима работы***
- После активации, если требуется добавить устройство в клиентское программное обеспечение или в другие платформы, следует отредактировать IP-адрес устройства. Для получения подробной информации обратитесь к разделу ***Настройки связи***.

5.2 Активация через SADP

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

Перед началом

- ПО SADP загружено на диск, поставляемый в комплекте, также его можно скачать с официального сайта ***http:// www.hikvision.com/en/*** . Установите ПО SADP в соответствии с инструкцией.
- 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***.

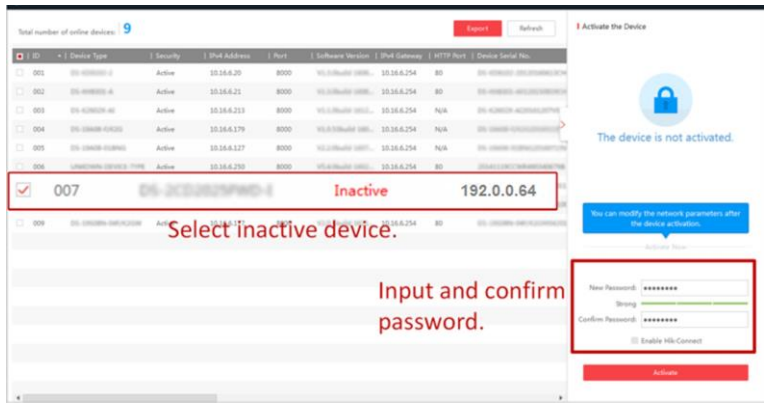
Шаги

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.

   Предостережение

   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 повысить безопасность при использовании продукта.

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 компьютер вручную или поставив галочку **Enable DHCP** («Включить DHCP»).
   3) Введите пароль администратора и нажмите **Modify** («Изменить») для изменения IP-адреса.

5.3 Активация устройства при помощи клиентского ПО

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

Шаги

Примечание

Эта функция должна поддерживаться устройством.

1. Откройте 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 (показано в столбце **Security Level** («Уровень безопасности»)) и выберите неактивное устройство.
5. Нажмите **Activate** («Активировать»), чтобы открыть окно активации.
6. Создайте и введите новый пароль в поле **Password** («Пароль») и подтвердите его **Confirm Password** («Подтвердите пароль»).

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, из них не менее трех элементов из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит повысить безопасность при использовании продукта.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

7. Для активации устройства нажмите **OK**.

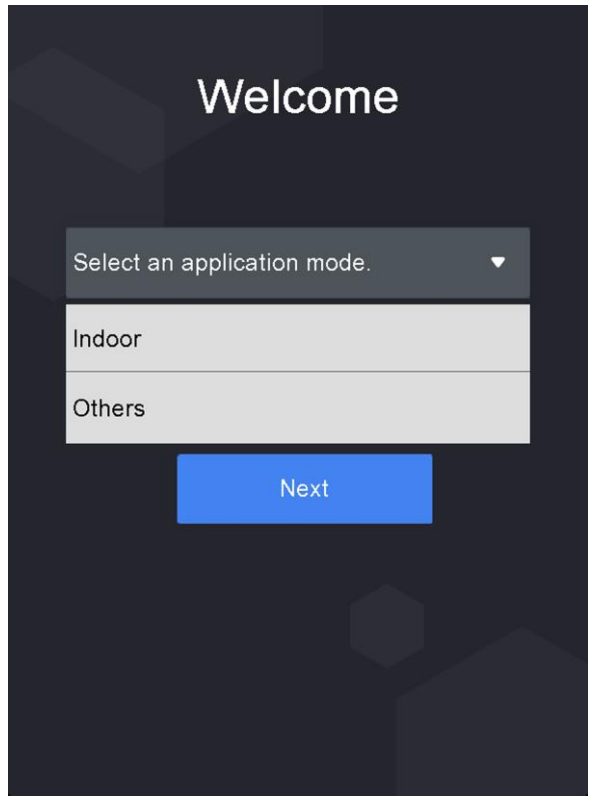
Раздел 6 Основные операции

6.1 Настройки режима работы

После активации устройства выберите необходимый режим работы.

Шаги

1. Из выпадающего списка на стартовой странице выберите режим **Indoor** («Использование внутри помещений») или **Others** («Другое»).



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

Рисунок 6-1 Стартовая страница

Примечание

- Настройки также можно изменить в меню *System Settings* («Настройки системы»).
- В меню 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** по умолчанию.
- При активации устройства с помощью других инструментов удаленно система выберет **Indoor** в качестве режима работы по умолчанию.

6.2 Вход в систему

Выполните вход в систему, чтобы настроить основные параметры устройства. Перед первым входом в систему необходимо ввести пароль для активации устройства. Также можно войти в систему с использованием ранее добавленных учетных данных администратора.

6.2.1 Первый вход в систему

Прежде чем начать работать с устройством, необходимо выполнить вход в систему.

Шаги

1. На начальной странице нажмите на экран и удерживайте в течение 3 секунд, чтобы перейти на страницу ввода пароля.
2. Нажмите на строку ввода пароля и введите пароль для активации устройства.
3. Нажмите **OK** для перехода на главную страницу.

Примечание

- Устройство будет заблокировано на 30 минут после 5 неудачных попыток ввода пароля.
- Для получения подробной информации о настройке работы в режиме администратора см. в меню *Adding User* («Добавление пользователей»).

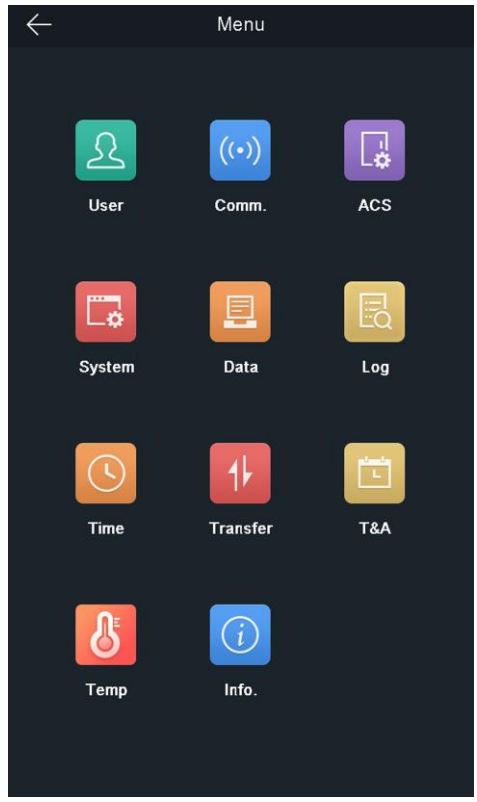


Рисунок 6-2 Главная страница

6.2.2 Вход в систему в качестве администратора

После добавления администратора для устройства только администратор может управлять устройством.

Шаги

1. На начальной странице нажмите на экран и удерживайте в течение 3 секунд, чтобы перейти на страницу входа в систему в качестве администратора.

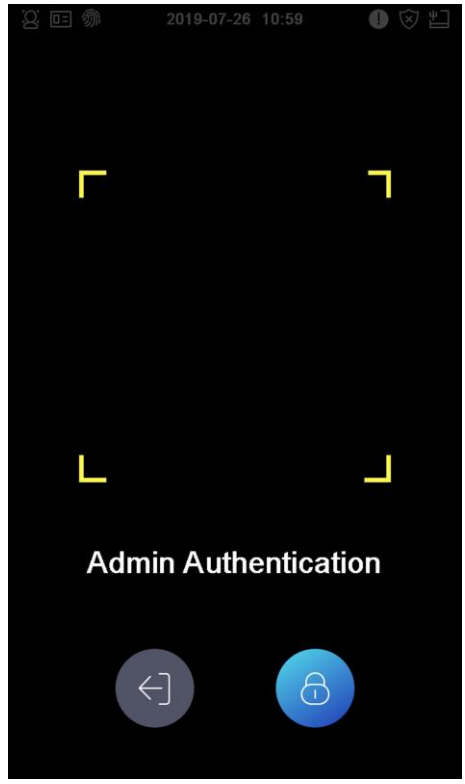


Рисунок 6-3 Вход в систему в качестве администратора

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

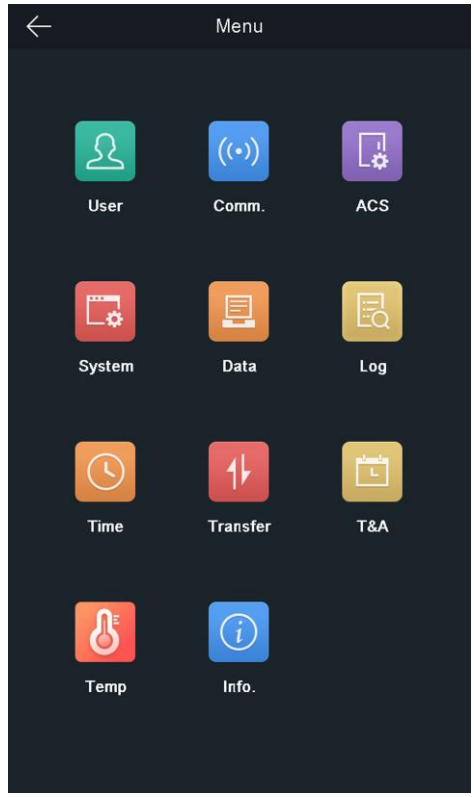


Рисунок 6-4 Главная страница

Примечание

Устройство будет заблокировано на 30 минут после 5 неудачных попыток аутентификации карты или считывания лица.

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

6.3 Настройки связи

Параметры сети, RS-485 и интерфейса Wiegand можно задать на странице настроек связи.

6.3.1 Настройка параметров сети

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

Шаги

1. Нажмите на кнопку **Comm**. («Настройки связи») на главной странице, чтобы перейти на страницу настроек связи.
2. На странице Communication Settings («Настройки связи») нажмите кнопку **Network** («Сеть»), чтобы перейти на соответствующую вкладку.

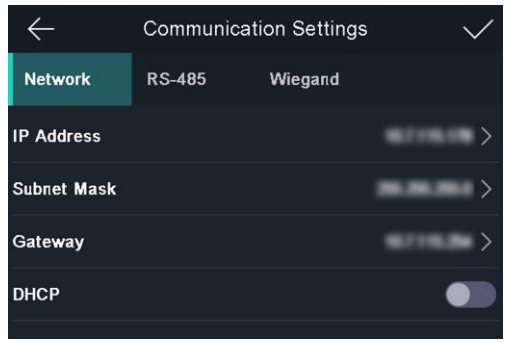


Рисунок 6-5 Сетевые параметры

3. В меню выберите IP-адрес, маску подсети и шлюз, затем введите параметры.
4. Нажмите **OK** для сохранения настроек.

Примечание

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

5. Нажмите для сохранения параметров сети.

6.3.2 Настройка параметров RS-485

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

Шаги

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

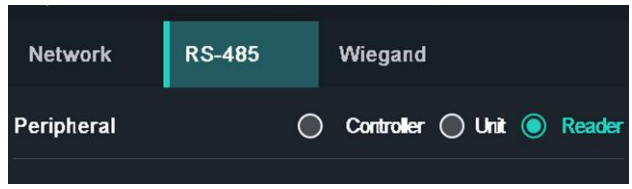


Рисунок 6-6 Настройка параметров RS-485

3. Выберите необходимое внешнее устройство.

Примечание

- Controller («Контроллер») — это контроллер доступа, Unit («Блок») — блок управления модуля безопасности двери, Reader («Считыватель») — считыватель карт.
- При выборе пункта **Controller** («Контроллер»): Если устройство подключено к терминалу через интерфейс RS-485, установите значение 2 для адреса RS-485. Если устройство подключено к контроллеру, установите адрес RS-485 в соответствии с номером двери.

4. Нажмите для сохранения параметров сети.

Примечание

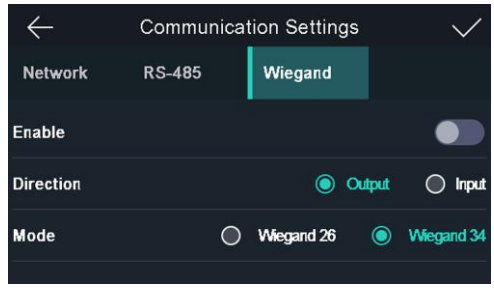
При изменении и сохранении параметров внешнего устройства произойдет его автоматическая перезагрузка.

6.3.3 Настройка параметров интерфейса Wiegand

Настройка направления передачи данных интерфейса Wiegand.

Шаги

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



3. Включить интерфейс Wiegand.
4. Выберите направление передачи данных.

Рисунок 6-7 Настройки интерфейса Wiegand

- Выход: Терминал распознавания лиц можно подключать к контроллеру внешнего доступа. Эти два устройства будут передавать номер карты через Wiegand 26 или Wiegand 34.
- Вход: Терминал распознавания лиц можно подключать к считывателю карт Wiegand.

5. Нажмите для сохранения параметров сети.

Примечание

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

6.4 Управление пользователями

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

6.4.1 Добавление администратора

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

Шаги

1. Нажмите на начальную страницу и удерживайте в течение нескольких секунд, затем войдите в аппаратную часть устройства.
2. Нажмите на кнопку **User → +** для перехода на страницу добавления 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, номер карты и пароль.

Примечание

- Для более подробной информации о добавлении изображения лица см. раздел ***Добавление изображения лица***.
- Для более подробной информации о добавлении карты см. раздел ***Добавление карты***.

- Для более подробной информации о добавлении пароля см. раздел ***Добавление пароля***.

6. **Опционально:** Можно выбрать тип аутентификации администратора.

Примечание

Для подробной информации о выборе типа аутентификации см. раздел ***Установка режима аутентификации***.

7. Настройте права администратора.

Включение прав администратора

Войдите в систему в качестве администратора. Кроме обычных функций контроля доступа, в этом случае пользователь может также перейти на стартовую страницу для управления устройством после аутентификации прав администратора.

8. Нажмите для сохранения настроек.

6.4.2 Добавление изображения лица

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

Шаги

1. Нажмите на начальную страницу и удерживайте в течение нескольких секунд, затем войдите в аппаратную часть устройства.
2. Нажмите на кнопку **User → +** для перехода на страницу добавления 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. Нажмите на пол Face Picture («Изображение лица»), чтобы открыть страницу добавления изображения лица.

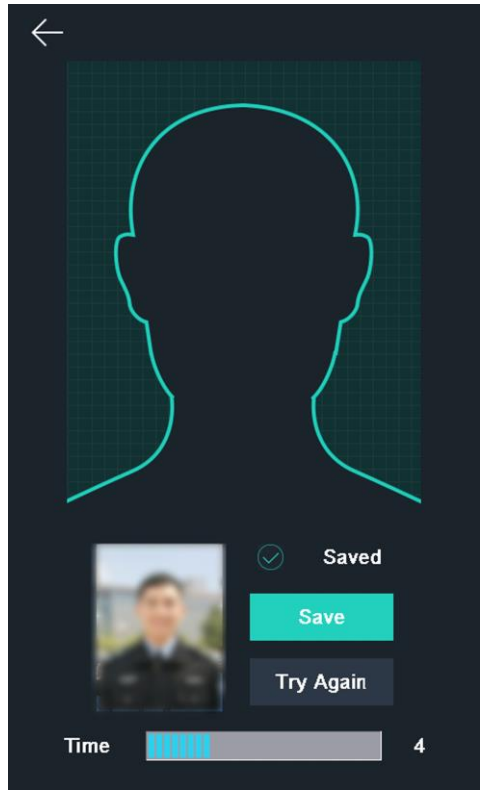


Рисунок 6-8 Добавление изображения лица

6. Расположите лицо прямо перед камерой.

Примечание

- Перед добавлением изображения лица убедитесь, что оно находится в соответствующем контуре.
- Убедитесь, что качество и размер изображения лица соответствуют требованиям.
- Подробные инструкции по добавлению изображений лиц смотрите в разделе *Советы по сбору/сравнению изображений лиц*.

После завершения процесса добавления изображения лица в правом верхнем углу страницы появится захваченная картинка.

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

Примечание

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

9. Включите/выключите права администратора.

Включение прав администратора

Войдите в систему в качестве администратора. Кроме обычных функций контроля доступа, в этом случае пользователь может также перейти на стартовую страницу для управления устройством после аутентификации прав администратора.

Выключение прав администратора

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

10. Нажмите для сохранения настроек.

6.4.3 Добавление карты

После добавления карты пользователь сможет проходить аутентификацию с помощью карты.

Шаги

1. Нажмите на начальную страницу и удерживайте в течение нескольких секунд, затем войдите в аппаратную часть устройства.
2. Нажмите на кнопку **User → +** для перехода на страницу добавления пользователя.
3. Нажмите на поле Employee ID («Идентификатор сотрудника») и внесите необходимые изменения.

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. Введите номер карты в соответствующем поле.
6. Изменение номера карты
- Введите номер карты вручную.
- Чтобы узнать номер карты, сканируйте карту в области считывания карты.

Примечание

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

7. **Опционально:** Включите функцию Duress Card (Карта принудительного открытия). Добавленная карта

   Если пользователь проходит процесс аутентификации путем проведения карты принудительного открытия, устройство загружает соответствующее событие в клиентское программное обеспечение.

8. Включите/выключите права администратора.

   Включение прав администратора

   Войдите в систему в качестве администратора. Кроме обычных функций контроля доступа, в этом случае пользователь может также перейти на стартовую страницу для управления устройством после аутентификации прав администратора.

   Выключение прав администратора

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

9. Нажмите для сохранения настроек.

6.4.4 Добавление пароля

После добавления пароля пользователь сможет проходить аутентификацию с помощью пароля.

Шаги

1. Нажмите на начальную страницу и удерживайте в течение нескольких секунд, затем войдите в аппаратную часть устройства.
2. Нажмите на кнопку **User → +** для перехода на страницу добавления пользователя.
3. Нажмите на поле Employee ID («Идентификатор сотрудника») и внесите необходимые изменения.

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

Примечание

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

6. Включите/выключите права администратора.

Включение прав администратора

Войдите в систему в качестве администратора. Кроме обычных функций контроля доступа, в этом случае пользователь может также перейти на стартовую страницу для управления устройством после аутентификации прав администратора.

Выключение прав администратора

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

7. Нажмите ✓ для сохранения настроек.

6.4.5 Настройка режима аутентификации

После добавления изображения лица пользователя, пароля или других учетных данных, настройте режим аутентификации. Пользователь сможет аутентифицировать свою личность через настроенный режим аутентификации.

Шаги

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

Устройства

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

Custom («Пользовательский»)

При необходимости допускается сочетать различные режимы аутентификации.

4. Нажмите ✓ для сохранения настроек.

6.4.6 Поиск и редактирование 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, чтобы перейти на страницу поиска пользователя. Нажмите кнопку 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.

Редактирование пользователя

На странице User Management («Управление пользователями») выберите пользователя из списка, чтобы перейти на страницу Edit User («Редактировать параметры пользователя»). Чтобы редактировать параметры следуйте инструкциям, указанным разделе ***Управление доступом*** Нажмите для сохранения настроек.

Примечание

Не допускается редактирование идентификатора сотрудника.

6.5 Настройки измерения температуры

Здесь можно настроить параметры измерения температуры, в том числе определение температуры, пороговое значение температуры тревоги, параметры компенсации температуры, параметры состояния двери (открыто/закрыто) с привязкой к порогу температуры, режим измерения температуры, единицы измерения температуры, калибровку области измерения, область измерения, калибратор (АЧТ) и т. д.

На главной странице нажмите **Temp** («Температура») для перехода на страницу Temperature Settings («Настройки температуры»). Настройте параметры измерения температуры и нажмите , чтобы сохранить настройки.

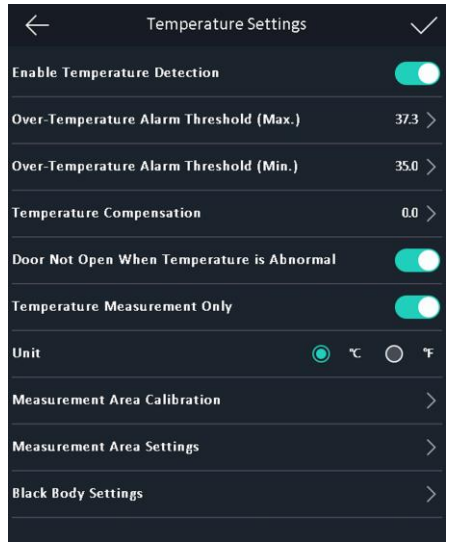


Рисунок 6-9 Параметры измерения температуры

Описание параметров:

Таблица 6-1 Описание параметров измерения температуры

Параметр	Описание
Включить функцию обнаружения температуры.	При включении этой функции устройство аутентифицирует разрешения и одновременно измеряет температуру. При отключении функции, устройство будет только аутентифицировать разрешения.
Пороговое значение температуры тревоги(Макс. / Мин.)	Настройте пороговое значение в соответствии с фактической ситуацией. При обнаружении температуры выше или ниже настроенных параметров, срабатывает
Компенсация температуры	Настройте параметры компенсации температуры, если измеренная температура оказывается выше / ниже фактической температуры объекта. Доступный
Не открывать дверь, если измеренная температура	При включении этой функции дверь остается закрытой, когда обнаруженная температура оказывается выше или ниже настроенного порогового значения температуры.
Только измерение температуры	При включении функции устройство будет только измерять температуру без аутентификации разрешений. При выключении этой функции устройство аутентифицирует разрешения и одновременно измеряет температуру.
Единицы измерения	Выберите необходимые единицы измерения температуры.
Калибровка области измерения / настройки области измерения	Настройте область измерения температуры и параметры коррекции.
Настройки калибратора (АЧТ)	Включите эту функцию и настройте параметры калибратора, в том числе расстояние, температуру и излучательную способность. **Примечание** При измерении АЧТ убедитесь, что камера устройства направлена на АЧТ, и между АЧТ и камерой отсутствуют посторонние предметы. Во избежание ошибок при измерении температуры, после калибровки образца АЧТ убедитесь, что область измерения АЧТ совпадает с калиброванной областью.

6.6 Импорт и экспорт данных

На странице Transfer («Передача данных») можно экспортировать данные о событии, данные пользователя, изображение пользователя и захваченное изображение на USB-накопитель. Также можно импортировать данные и изображение пользователя с USB-накопителя.

6.6.1 Экспорт данных

Шаги

1. Нажмите кнопку Transfer («Передача данных») на главной странице, чтобы перейти на соответствующую страницу.
2. На странице Transfer («Передача данных») нажмите кнопку Export Event («Экспорт данных о событии»), Export User Data («Экспорт данных пользователя»), Export Profile Photo («Экспорт фотографии пользователя») или Export Captured Picture («Экспорт захваченного изображения»).
3. Во всплывающем окне нажмите кнопку **Yes** («Да»), и данные будут экспортированы с устройства на USB-накопитель.

Примечание

- Поддерживается формат USB-накопителя DB.
- Система позволяет использовать USB-накопитель с памятью в диапазоне 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.

6.6.2 Импорт данных

Шаги

1. Вставьте USB-накопитель в устройство.
2. На странице Transfer («Передача данных») нажмите кнопку Import User Data («Импорт данных пользователя») и Import Profile Photo («Импорт фотографии профиля пользователя»).
3. Во всплывающем окне нажмите кнопку **Yes** («Да»), чтобы импортировать данные на устройство с USB-накопителя.

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.
- Поддерживается формат USB-накопителя FAT32.

- Импортированное изображение должно быть сохранено в корневом каталоге (enroll_pic), а название файла изображения должно формироваться в соответствии со следующим правилом:
  Номер карты_Имя_Отдел_Идентификатор сотрудника_Пол.jpg
- Идентификатор сотрудника может содержать до 32 символов. Он может состоять из букв верхнего/нижнего регистра и цифр. Он не может дублироваться или начинаться с 0.
- Требования к фотографии. Лицо видно полностью, взгляд направлен прямо в камеру. При фотографировании запрещено надевать шляпу или другой головной убор. Формат фотографии должен быть JPEG или JPG. Разрешение должно быть не менее 640 × 480 пикселей. Размер изображения должен быть в диапазоне от 60 до 200 КБ.

6.7 Аутентификация личности

После настройки сети, параметров системы и добавления пользователей вернитесь на начальную страницу для прохождения процедуры аутентификации личности. Система выполнит аутентификацию сотрудника/посетителя в соответствии с настроенным режимом работы.

Установите личность с помощью сопоставления 1:1 или сопоставления 1:N.

Сопоставление 1:N

Сопоставьте полученное изображение лица со всеми изображениями лиц, хранящимися на устройстве.

1: Сопоставление 1:1

Сопоставьте полученное изображение лица со всеми изображениями лиц, хранящимися на устройстве.

6.7.1 Аутентификация с помощью различных учетных данных

Перед началом

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

Шаги

1. Если для аутентификации используются карта и лицо, пароль и лицо, карта и пароль, используйте выбранный тип аутентификации согласно инструкциям на странице просмотра в режиме реального времени.

   Примечание

   - Карта может быть обычной интеллектуальной картой или зашифрованной картой.
   - Если функция сканирования QR-кода включена, поместите QR-код перед камерой устройства для прохождения аутентификации.

2. После завершения проверки приступите к следующему этапу аутентификации.

   Примечание

Подробную информацию об аутентификации лица см. в разделе «*Советы по сбору/сравнению изображений лиц*».

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

6.7.2 Аутентификация с помощью одного типа учетных данных

Перед аутентификацией установите тип аутентификации пользователя. Для получения подробной информации обратитесь к разделу ***Настройки режима работы.*** Пройдите аутентификацию лица, карты или QR -кода.

Изображения лиц

Расположите лицо прямо перед камерой и начните аутентификацию.

Карта

Приложите карту к области считывания карт для проверки личности.

Примечание

Карта может быть обычной интеллектуальной картой или зашифрованной картой.

QR-код

Поместите QR-код перед камерой устройства для прохождения аутентификации.

Примечание

Устройство должно поддерживать функцию аутентификации с помощью QR-кода.

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

6.8 Настройка системы

На странице System Settings («Настройки системы») можно установить основные параметры системы, параметры лиц, а также обновить прошивку.

6.8.1 Настройка основных параметров

Укажите номер микрорайона, номер здания, номер отдела. Настройте голосовые предупреждения, громкость звука, режим применения и яркость подсветки белым светом.

На главной странице нажмите **System** («Настройки системы») для перехода на соответствующую страницу.

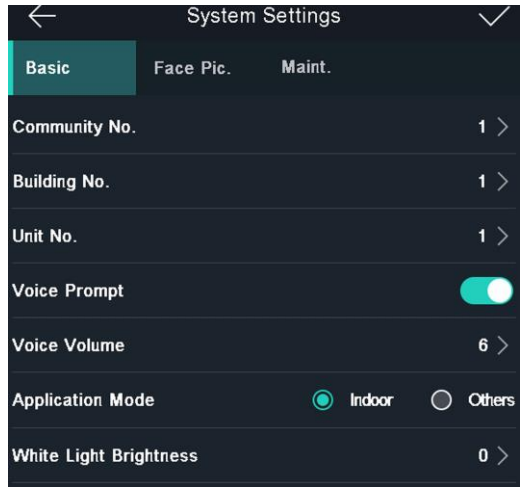


Рисунок 6-10 Основные параметры

Таблица 6-2 Основные параметры

Параметр	Описание
Community No. («Номер микрорайона»)	Укажите номер микрорайона, в котором установлено устройство.
Building No. («Номер здания»)	Укажите номер здания, в котором установлено устройство.
Unit No. («Номер отдела»)	Укажите номер отдела, в котором установлено устройство.
Voice prompt («Голосовое предупреждение»)	Нажмите кнопку или для включения/выключения голосовых предупреждений.
Voice volume («Громкость звука»)	Регулировка громкости голоса. Чем больше значение, тем выше громкость.
Application mode («Режим применения»)	Выберите режим Indoor («Использование внутри помещения») или Others («Другое») в соответствии с фактической ситуацией.
White light brightness («Яркость подсветки белым светом»)	Установите яркость вспомогательной подсветки белым светом. Диапазон яркости от 0 до 100. «0» - подсветка выключена. «1» - наименьшая яркость, а «100» - наибольшая яркость.

6.8.2 Настройка параметров изображений лиц

Здесь можно установить уровень безопасности 1:N, уровень безопасности 1:1, интервал распознавания, параметры обнаружения витальности, уровень WDR, межзрачковое расстояние, параметры детекции наличия/отсутствия маски и ЭКО-режим.

На главной странице нажмите **System** («Настройки системы») для перехода на соответствующую страницу.

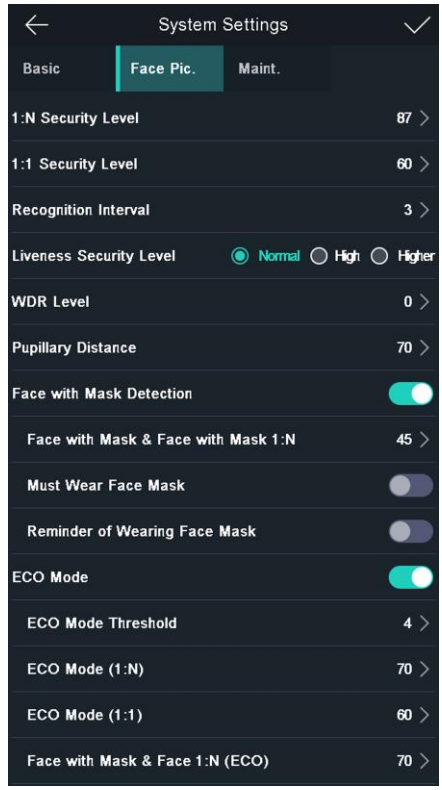


Рисунок 6-11 Параметры изображений лиц

Таблица 6-3 Параметры изображений лиц

Параметр	Описание
1:N Security level («Уровень безопасности 1:N»)	Установка порога опознавания при аутентификации в режиме 1:N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение составляет 84.
1:1 Security level («Уровень безопасности 1:1»)	Установка порога опознавания при аутентификации в режиме 1:1. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение составляет 75.
Recognition interval («Интервал распознавания»)	Установка временного интервала между двумя непрерывными распознаваниями лиц при аутентификации разрешения одного сотрудника/посетителя.
	Примечание Введите число от 1 до 10.
Liveness level («Уровень витальности)	После включения функции Live Face Detection («Обнаружение живых лиц») установите соответствующий уровень безопасности при выполнении аутентификации лица в режиме реального времени.
WDR level («Уровень WDR»)	Устройство может автоматически активировать функцию WDR. Чем выше уровень WDR, тем легче устройство переключается в режим WDR. «0» - функция WDR отключена.
Pupillary distance («Межзрачковое расстояние»)	Минимальное разрешение между двумя зрачками при запуске распознавания лица. Фактическое разрешение должно быть выше, чем заданное значение. По умолчанию значение составляет 40.
Face with mask detection («Детекция наличия/отсут ствия маски»)	После включения этой функции,при аутентификации разрешения на странице аутентификации, устройство может распознать наличие/отсутствие маски и предлагает надеть маску в соответствии с настройками.
Face with mask & Face with mask (1:N) («Детекция наличия/отсутствия маски 1:N»)	Установка порога распознавания наличия/отсутствия маски 1: N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. Максимальное значение составляет 100.

Must wear face mask («Обязательное наличие маски»)	После включения этой функции устройство запрещает проход при отсутствии маски.
Reminder of wearing face mask («Напоминание о ношении маски»)	После включения этой функции устройство предложит надеть маску, если не обнаружит ее в процессе аутентификации.
ECO mode («ЭКО-режим»)	После включения ЭКО-режима устройство будет использовать ИК-подсветку для аутентификации лиц в условиях низкой освещенности или в темноте. Установите пороговое значение для ECO-режима, режима ECO (1: N) и режима ECO (1: 1).
ECO mode threshold («Пороговое значение ЭКО-режима»)	Установите пороговое значение для ECO-режима при включении функции. Чем больше значение, тем легче устройство переходит в ЭКО-режим. Доступный диапазон: от 0 до 8.
ECO mode (1:N) («Режим ЭКО (1:N)»)	Установка порога опознавания при аутентификации в режиме ЭКО 1:N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение составляет 84.

Параметр	Описание
ECO mode (1:1) («Режим ЭКО (1:1)»)	Установка порога опознавания при аутентификации в режиме ЭКО 1:1. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. По умолчанию значение составляет 75.
Face with mask & Face with mask (1:N) (ECO) («Детекция наличия/отсутствия маски 1:N (ЭКО))	Установка порога распознавания наличия/отсутствия маски 1: N в ЭКО-режиме. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания. Максимальное значение составляет 100.

6.8.3 Настройка времени

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

Нажмите на кнопку **Время** («Настройки времени») на главной странице, чтобы перейти на соответствующую страницу. Настройте параметры времени и нажмите ✓, чтобы сохранить настройки.

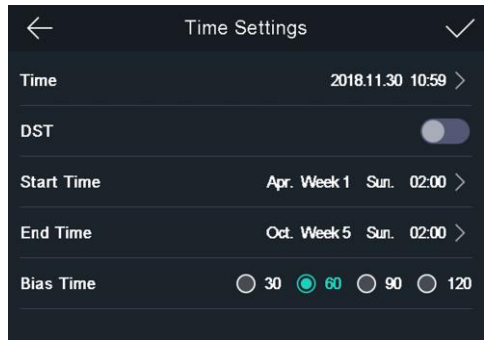


Рисунок 6-12 Параметры времени

6.9 Настройка параметров управления доступом

Установите разрешения на управление доступом, включая функции режима аутентификации, режима считывания карт, функции сканирования QR-кода, удаленной аутентификации, детекции дверного контакта и времени до закрытия двери.

Находясь на главной странице, нажмите кнопку **ACS** («Настройки контроля доступа»), чтобы перейти на соответствующую страницу. Установите параметры контроля доступа и нажмите ✓, чтобы сохранить настройки.

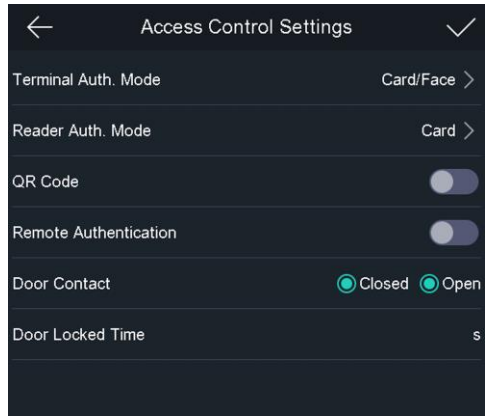


Рисунок 6-13 Параметры контроля доступа

Описание параметров:

Таблица 6-4 Описание параметров контроля доступа

Параметр	Описание
Terminal auth. mode («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. Если требуется более высокий уровень безопасности, используйте несколько режимов аутентификации. • При использовании нескольких режимов аутентификации перед началом аутентификации лица завершите предыдущие проверки.
Reader auth. mode («Режим аутентификации при помощи считывателя карт»)	Выберите режим аутентификации при помощи считывателя карт.
QR code («QR-код»)	Можно использовать функцию сканирования QR-кода в интерфейсе аутентификации. Устройство загрузит информацию, считанную с QR-кода, на платформу.
Remote authentication («Удаленная аутентификация»)	При аутентификации разрешения платформа предоставит доступ/откажет в предоставлении доступа удаленно.

Door contact («Дверной контакт»)	Выберите необходимый режим: **Open («Открыто»)** или **Closed («Закрыто»).** По умолчанию дверь **закрыта**.
Door locked time («Время до закрытия двери»)	Установите Door Unlocking Duration (**«Длительность открытого состояния двери»**). Дверь будет заблокирована, если движение отсутствует в течение установленного времени. Доступный диапазон времени блокировки двери: от 1 до 255 с.

6.10 Техническое обслуживание

6.10.1 Обновление прошивки устройства

Вставьте USB-накопитель в устройство. Нажмите Maint. («Обслуживание») на странице настроек системы, затем нажмите Upgrade («Обновить»). Устройство автоматически считает файл обновления с USB-накопителя и обновит прошивку.

Примечание

- Не выключайте устройство во время обновления.
- Файл обновления должен находиться в корневом каталоге.
- Он должен называться digicap.dav.

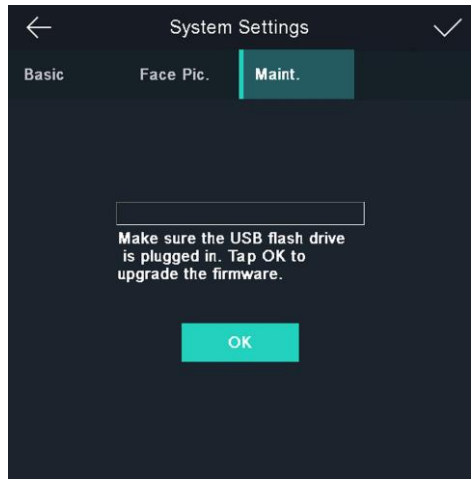


Рисунок 6-14 Обновление

6.10.2 Управление данными

На странице Data Management («Управление данными») можно удалить данные пользователя, восстановить заводские настройки или вернуться к настройкам по умолчанию.

Нажмите кнопку Data (Data Management) («Данные») («Управление данными»), чтобы перейти на соответствующую страницу. Управление данными осуществляется при помощи кнопок, расположенных на странице. Во всплывающем окне нажмите Yes («Да»), чтобы установить настройки.

Ниже приведено описание доступных кнопок:

Таблица 6-5 Описание кнопок

Параметры	Описание
Delete user data («Удаление всех данных пользователя»)	Удаление всех записанных данных пользователя с устройства.
Restore to factory («Восстановление заводских настроек»)	Восстановление системы до заводских настроек. После этого устройство будет перезагружено.
Restore to default («Восстановление настроек по умолчанию»)	Восстановление системы до настроек по умолчанию. Система сохранит настройки связи, а также настройки удаленного пользователя. Для других параметров будут восстановлены значения по умолчанию. После этого устройство будет перезагружено.

6.10.3 Управление записями в журналах

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

Шаги

1. На главной странице нажмите кнопку **Log** («Журнал»), чтобы перейти на соответствующую страницу.

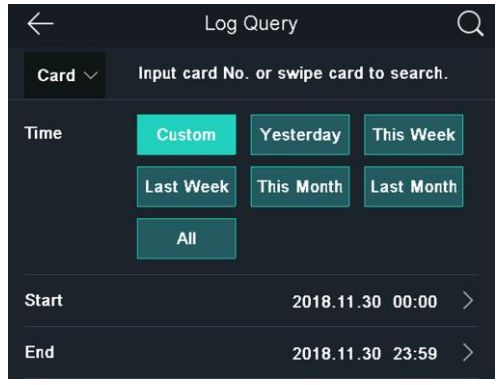


Рисунок 6-15 Записи журнала

2. Нажмите кнопку **Card** («Карта») в левой части страницы и выберите тип поиска из

выпадающего списка.

3. Перейдите в поле ввода данных и укажите идентификатор сотрудника, номер карты или имя пользователя для осуществления поиска.
4. Выберите время.

Примечание

Доступны следующие варианты: Custom («Настраиваемое»), Yesterday («Вчера»), This Week («Эта неделя»), Last Week («Последняя неделя»), This Month («Этот месяц»), Last Month («Последний месяц»), или All («Все»). Если было выбрано значение Custom («Настраиваемое»), можно установить время начала и окончания поиска.

5. Нажмите кнопку , чтобы начать поиск.

   После этого на странице появятся результаты поиска.

6.11 Настройка параметров учета рабочего времени

Установите параметры учета рабочего времени. В зависимости от фактической ситуации установите учет 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.

6.11.1 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.

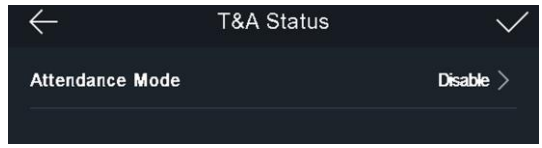


Рисунок 6-16 Отключение функции учета рабочего времени

Перейдите в меню **Attendance Mode («Учет рабочего времени»)** и выберите **Disable** («Отключить»). Далее нажмите .

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

6.11.2 Установка режима 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.»).

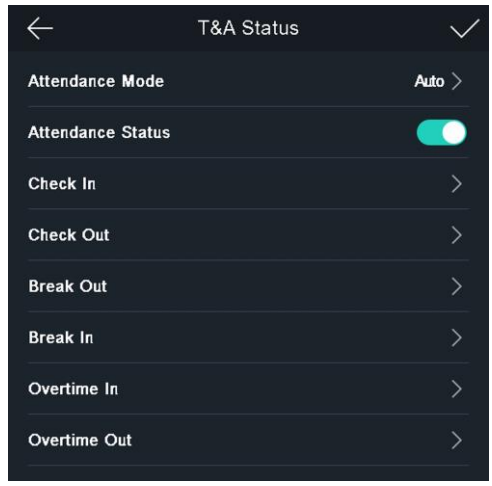


Рисунок 6-17 Установка режима автоматического учета рабочего времени

3. Выберите статус и расписание посещений.
   1) Выберите регистрацию **Check In** («Входа на работу»), **Check Out** («Выхода с работы»), **Break Out** («Ухода на перерыв»), **Break In** («Возвращения с перерыва»), **Overtime In** («Сверхурочной работы»), **Overtime Out**(«Раннего ухода 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.

4. Нажмите ✓.

Result («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».

6.11.3 Установка 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»).

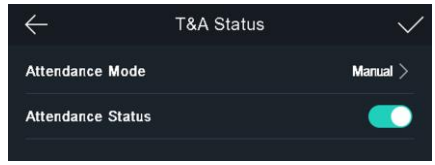


Рисунок 6-18 Режим подсчета результатов посещаемости вручную

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

Result («Результат»)

При аутентификации необходимо вручную выбрать статус посещения.

Примечание

Если не выбрать статус, аутентификация будет неудачной.

6.11.4 Установка подсчета результатов посещаемости автоматически и 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»).

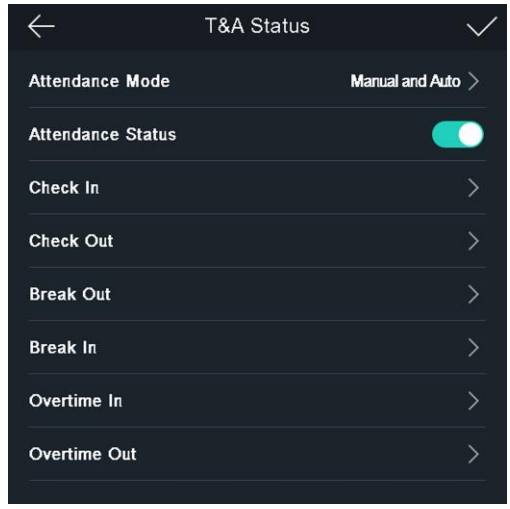


Рисунок 6-19 Подсчет результатов посещаемости автоматически и вручную

3. Выберите статус и расписание посещений.
   1) Выберите регистрацию **Check In** («Входа на работу»), **Check Out** («Выхода с работы»), **Break Out** («Ухода на перерыв»), **Break In** («Возвращения с перерыва»), **Overtime In** («Сверхурочной работы»), **Overtime Out** («Раннего ухода 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.

4. Нажмите .

Result («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».

6.12 Просмотр системной информации

Здесь можно просмотреть память устройства, информацию об устройстве и лицензии на ПО с открытым исходным кодом.

Просмотр памяти устройства

Здесь можно просмотреть номер добавленного пользователя, номер изображения лица, номер изображения лица с маской, номер карты и номер события.
Нажмите **Info. (System Information) → Capacity** («Системная информация → Память»), чтобы перейти на соответствующую страницу.

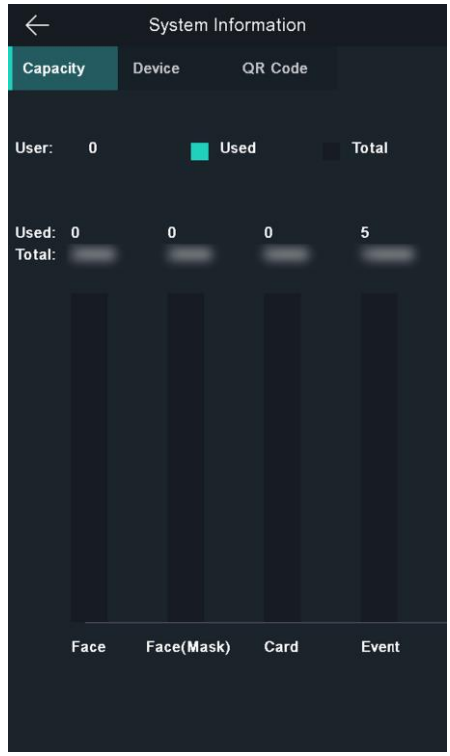


Рисунок 6-20 Память

Просмотр информации об устройстве

Здесь можно просмотреть информацию об устройстве.
Нажмите **Info. (System Information) → Device** («Системная информация → Устройство»), чтобы перейти на соответствующую страницу.

Лицензия с открытым исходным кодом

Просмотр информации о лицензии с открытым исходным кодом
Нажмите **Info. (System Information) → License** («Системная информация → Лицензия»), чтобы перейти на соответствующую страницу.

Просмотр QR-кода устройства

Сканируйте QR-код устройства, чтобы добавить его в мобильный клиент.
Нажмите **Info. (System Information) → QR Code** («Системная информация → QR-код»), чтобы просмотреть QR-код устройства.

6.13 Видеодомофония

После добавления устройства в клиентское ПО можно: вызвать устройство с клиентского ПО, вызвать консьержа/диспетчера с устройства, вызвать клиентское ПО с устройства, или вызвать видеодомофон с устройства.

6.13.1 Вызов клиентского ПО с устройства

Шаги

1. Клиентское ПО представлено на диске, входящем в комплект, и на официальном сайте. Установите ПО SADP согласно инструкции.
2. Запустите клиентское программное обеспечение. Во всплывающем окне появится панель управления программным обеспечением.
3. Нажмите **Device Management** (**«Управление устройством»**) для перехода в меню управления устройством.
4. Добавьте устройство в клиентское ПО.

   Примечание

   Для более подробной информации о добавлении устройства см. раздел *Добавление устройства.*

5. Вызовите клиентское ПО.
   1) На начальной странице нажмите **Call** («Вызвать»).
   2) Во всплывающем окне введите «***0».***
   3) Нажмите **Call** («Вызвать»), чтобы вызвать клиентское ПО.
6. Во всплывающем окне клиентского ПО нажмите **Answer** («Ответить»), чтобы включить двухстороннюю аудиосвязь между устройством и клиентским ПО.

   Примечание

   Если устройство добавлено в несколько клиентских ПО, при вызове клиентского ПО с устройства окно вызова отобразится только в первом добавленном клиентском ПО.

6.13.2 Вызов консьержа/диспетчера с устройства

Шаги

1. Клиентское ПО представлено на диске, входящем в комплект, и на официальном сайте. Установите ПО SADP согласно инструкции.
2. Запустите клиентское программное обеспечение. Во всплывающем окне появится панель управления программным обеспечением.
3. Нажмите **Device Management** (**«Управление устройством»**) для перехода в меню управления устройством.
4. Добавьте пульт консьержа/диспетчера и устройство в клиентское ПО.

   Примечание

   Для более подробной информации о добавлении устройства см. раздел *Добавление устройства.*

5. Установите IP-адрес и SIP-адрес пульта консьержа/диспетчера на странице удаленной конфигурации.

   Примечание

   Подробную информацию см. в руководстве пользователя пульта консьержа.

6. Примите вызов с пульта консьержа и начните двустороннюю аудиосвязь.

Примечание

При нажатии на значок устройство будет вызывать пульт консьержа/диспетчера в приоритетном порядке.

6.13.3 Вызов устройства с клиентского ПО

Шаги

1. Клиентское ПО представлено на диске, входящем в комплект, и на официальном сайте. Установите ПО SADP согласно инструкции.
2. Запустите клиентское программное обеспечение. Во всплывающем окне появится панель управления программным обеспечением.
3. Нажмите **Device Management** (**«Управление устройством»**) для перехода на страницу управления устройством.
4. Добавьте устройство в клиентское ПО.

   Примечание

   Для более подробной информации о добавлении устройства см. раздел *Добавление устройства.*

5. Перейдите на страницу **Live View** («Интерфейс просмотра в режиме реального времени») дважды щелкните иконку, чтобы запустить просмотр в режиме реального времени.

Примечание

Для получения подробной информации о **Live View («Интерфейс просмотра в режиме реального времени»)**, см. раздел *Просмотр в режиме реального* времени в руководстве пользователя клиентского ПО.

6. Нажмите правую кнопку мыши на окно просмотра в режиме реального времени, чтобы открыть контекстное меню.
7. Нажмите **Start Two-Way Audio** («Запуск двусторонней аудиосвязи»), чтобы начать двустороннюю аудиосвязь между устройством и клиентским ПО.

6.13.4 Вызов видеодомофона с устройства

Шаги

1. Клиентское ПО представлено на диске, входящем в комплект, и на официальном сайте. Установите ПО SADP согласно инструкции.
2. Запустите клиентское программное обеспечение. Во всплывающем окне появится панель управления программным обеспечением.
3. Нажмите **Device Management** (**«Управление устройством»**) для перехода в меню управления устройством.
4. Добавьте видеодомофон и устройство в клиентское ПО.

Примечание

Для более подробной информации о добавлении устройства см. раздел *Добавление устройства.*

5. Свяжите пользователя и видеодомофон, затем задайте номер кабинета для видеодомофона.
6. Нажмите на странице аутентификации устройства.
7. Введите номер кабинета на странице набора, затем нажмите для вызова видеодомофона.
8. Примите вызов с видеодомофона и начните двустороннюю аудиосвязь.

Раздел 7 Настройка клиентского ПО

7.1 Схема настройки клиентского ПО

Следуйте приведенной ниже схеме для настройки клиентского ПО.

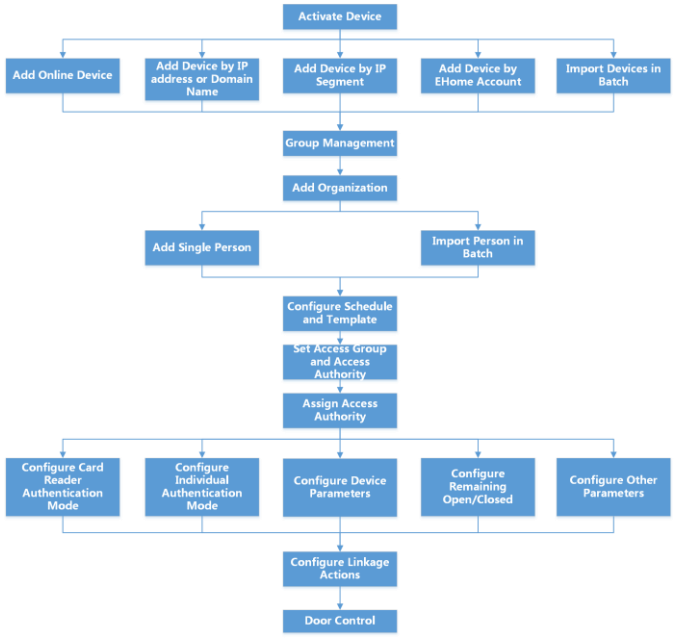


Рисунок 7-1 Схема настройки клиентского ПО

Английский язык	Русский язык
Group management	Управление группой
Add organization	Добавление организации
Add single person	Добавление сотрудника
Import person in batch	Импорт пользователей в пакетном режиме
Configure schedule and template	Настройка расписания и шаблона
Set access group and access authority	Назначение группы доступа и разрешений на доступ
Assign access authority	Назначение разрешений на доступ
Configure card reader autentification mode	Настройка параметров режима аутентификации считывателя карт
Configure individual autentification mode	Настройка параметров режима аутентификации отдельного устройства
Configure device parameters	Настройка параметров устройства
Configure remaining open/closed	Настройка режимов «оставить открытым»/ «оставить закрытым»
Configure other parameters	Настройка других параметров
Configure linkage actions	Настройка привязки
Door control	Управление дверью

7.2 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.

7.2.1 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.

Добавление обнаруженного онлайн-устройства

Выберите обнаруженное онлайн-устройство, отображаемое в списке онлайн-устройств, затем добавьте его в клиентское ПО.

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.

   Искомые онлайн-устройства отобразятся в

   списке.
4. Выберите онлайн-устройство в области **Online Device** («Онлайн-устройства») и нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.

   Примечание

   Для неактивного устройства необходимо создать пароль, прежде чем добавить устройство. Для более подробной информации см.
5. Введите необходимую информацию.

   Наименование

   Введите описательное имя для устройства.

   IP Address («IP-адрес»)

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

   Port («Порт»)

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

   User Name («Имя пользователя»)

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

Password («Пароль»)

Введите пароль устройства.

Предостережение

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

6. **Опционально:** Поставьте галочку в пункте **Transmission Encryption («Шифрование передачи») (TLS)** для включения шифрования передачи, защищенной протоколом TLS (безопасность на транспортном уровне).

Примечание

- Эта функция должна поддерживаться устройством.
- 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. См. подробную инструкцию по включению функции проверки сертификата.
- 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:** Поставьте галочку в пункте **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»).

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 необходимо создать пароль, прежде чем добавить устройство. Для более подробной информации см.
5. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
6. Введите необходимую информацию.

   User Name («Имя пользователя»)

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

   Password («Пароль»)

   Введите пароль устройства.

   Предостережение

   Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется установить пароль самостоятельно (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы) для обеспечения безопасности продукта. Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит повысить безопасность при использовании продукта.
   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:** Поставьте галочку в пункте **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 устройств.

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.

   Name («Наименование»)

   Создайте описательное имя для устройства. Например, можно использовать псевдоним, который указывает на местоположение или функцию устройства.

   Address («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.

   Предостережение

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

5. **Опционально:** Поставьте галочку в пункте **Transmission Encryption («Шифрование передачи») (TLS)** для включения шифрования передачи, защищенной протоколом TLS (безопасность на транспортном уровне).

   Примечание

   - Эта функция должна поддерживаться устройством.
   - 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. См. подробную инструкцию по включению функции проверки сертификата.
   - 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:** Поставьте галочку в пункте **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.

   Port («Порт»)

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

   User Name («Имя пользователя»)

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

   Password («Пароль»)

   Введите пароль устройства.

   Предостережение

   Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется установить пароль самостоятельно (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы) для обеспечения безопасности продукта. Также рекомендуется регулярно обновлять пароль.

Ежемесячная или еженедельная смена пароля позволит повысить безопасность при использовании продукта.

Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

6. **Опционально:** Поставьте галочку в пункте **Transmission Encryption («Шифрование передачи») (TLS)** для включения шифрования передачи, защищенной протоколом TLS (безопасность на транспортном уровне).

Примечание

- Эта функция должна поддерживаться устройством.
- 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. См. подробную инструкцию по включению функции проверки сертификата.
- 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:** поставьте галочку в пункте **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

Эта функция должна поддерживаться устройством.

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:** Поставьте галочку в пункте **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 DS-K1T331.

8. **Опционально:** Выполните следующие операции.

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

Редактирование информации устройства	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 экспортированный файл шаблона и введите необходимую информацию об устройствах, которые нужно добавить, в соответствующие столбцы.

Примечание

Подробное описание обязательных полей см. во введении.

Adding Mode («Режим добавления»)

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

Address («Адрес»)

Редактируйте адрес устройства.

Port («Порт»)

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

User Name («Имя пользователя»)

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

Password («Пароль»)

Введите пароль устройства.

Предостережение

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

Import to Group («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.

7.2.2 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.

     Предостережение

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

7.3 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.

7.3.1 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.

7.3.2 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. См. ***Add Group («Добавить группу»)*** .

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.

7.3.3 Редактирование 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** («Редактирование ресурса»).
5. Измените имя ресурса.
6. Нажмите **OK** для сохранения обновленных настроек.

7.3.4 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.

7.4 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.

7.4.1 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 удалить 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.

7.4.2 Настройка основной информации

Можно добавить пользователей в клиентское ПО поочередно и настроить основную информацию о пользователе, в том числе имя, пол, номер телефона и т. д.

Шаги

1. Войдите в модуль **Person** («Сотрудник/Посетитель»).
2. Выберите организацию из списка и добавьте сотрудника/посетителя.
3. Нажмите **Add** («Добавить»), чтобы открыть

   окно добавления сотрудника/посетителя.

   Идентификатор личности будет

   сгенерирован автоматически.
4. Введите основную информацию, в том числе имя, пол, номер телефона, адрес электронной почты и т. д.
5. **Опционально:** Установите срок действия разрешения сотрудника. После истечения срока действия учетные данные и настройки контроля доступа будут недействительными, и у пользователя не будет разрешения на доступ к дверям/этажам.

   Пример

   Например, если человек является посетителем, срок действия его/ее разрешения на доступ может быть непродолжительным или доступ может быть временным.
6. Подтвердите, чтобы добавить пользователя.
   - Нажмите **Add** («Добавить») для добавления пользователя и закройте окно добавления пользователя.
   - Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

7.4.3 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/посетителя.

   Примечание

   В первую очередь необходимо добавить основную информацию о пользователе. Для подробной информации о настройке основной информации о пользователе см. раздел ***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).

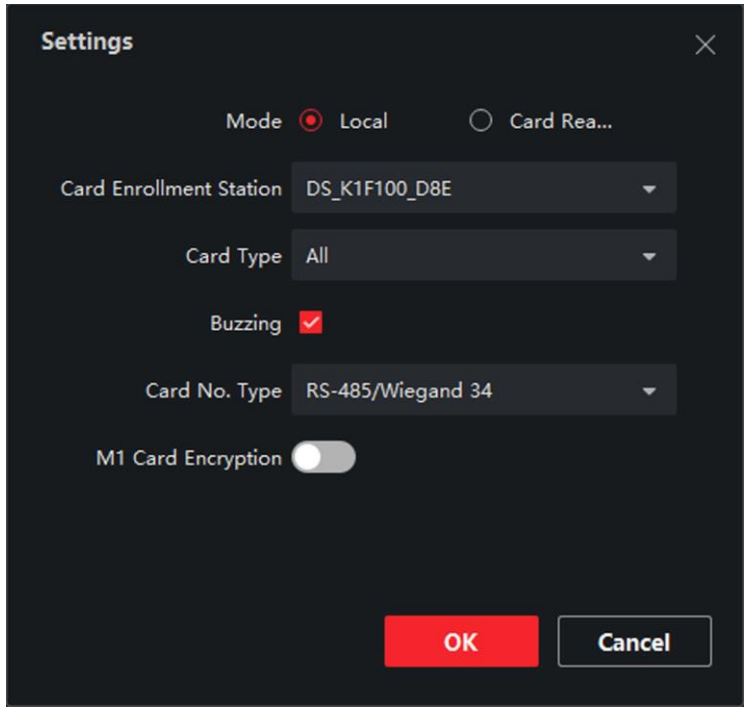


Рисунок 7-2 Выпуск карт в локальном режиме

6. Установите другие сопутствующие параметры.

Card Enrollment Station («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.

Card type («Тип карты»)

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

Buzzing («Зуммер»)

После успешного считывания номера карты включите или выключите зуммер.

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 карта M1 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.

7.4.4 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 пользователе. Для подробной информации о настройке основной информации о пользователе см. раздел ***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.
7. Подтвердите, чтобы добавить пользователя.
   - Нажмите **Add** («Добавить») для добавления пользователя и закройте окно добавления пользователя.
   - Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

7.4.5 Снимок лица с помощью клиентского ПО

При добавлении сотрудника/посетителя можно сфотографировать его/его через клиентское ПО и установить эту 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/посетителя.

   Примечание

   В первую очередь необходимо добавить основную информацию о сотрудника/посетителя. 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.
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 обновленных настроек.

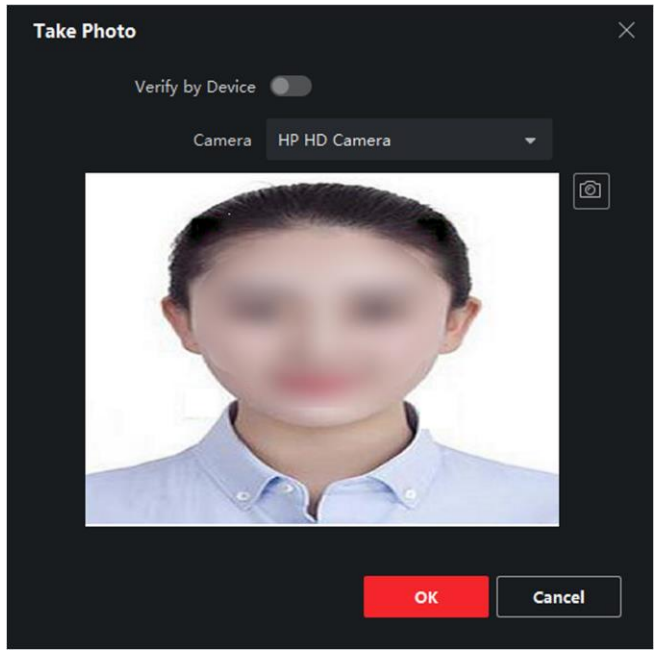


Рисунок 7-3 Снимок лица с помощью клиентского ПО

7. Подтвердите, чтобы добавить пользователя.

- Нажмите **Add** («Добавить») для добавления пользователя и закройте окно добавления пользователя.
- Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

7.4.6 Снимок 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 пользователе. Для подробной информации о настройке основной информации о пользователе см. раздел ***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 (антиспуфинг)»)** и выбрать уровень витальности: низкий, средний или высокий.

   Face Anti-Spoofing («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 лицо находится в середине окна сбора данных.
   2) Нажмите , чтобы сделать снимок лица.
   3) Нажмите **OK** для сохранения обновленных настроек.
7. Подтвердите, чтобы добавить пользователя.
   - Нажмите **Add** («Добавить») для добавления пользователя и закройте окно добавления пользователя.
   - Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

7.4.7 Настройка информации по контролю доступа

При добавлении сотрудника/посетителя можно установить информацию по контролю доступа, в том числе связать группы контроля доступа с сотрудником/посетителем, 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»), нажмите , чтобы выбрать группу контроля доступа для сотрудника/посетителя.

Примечание

Для более подробной информации см. раздел ***Настройка группы контроля доступа для назначения разрешений на доступ***.

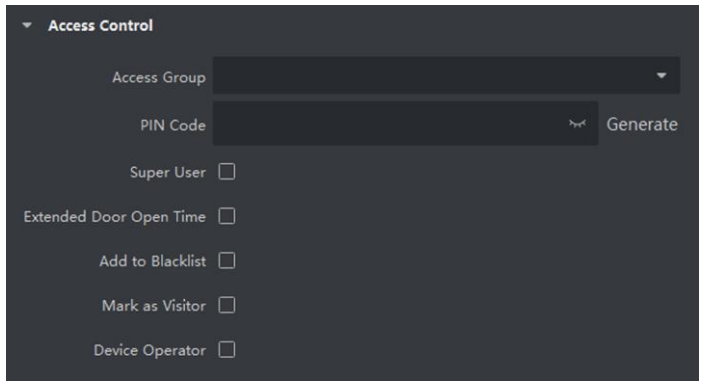


Рисунок 7-4 Настройка информации по контролю доступа

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** («Генерировать»), 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.

   Super User («Суперпользователь»)

   Если человек 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.

Extended Door Open Time («Увеличенная продолжительность открытия двери»)

Используйте эту функцию для обслуживания людей с ограниченной подвижностью. Таким людям будет предоставлено больше времени, чтобы пройти через двери.

Для подробной информации о настройке состояния дверей см. раздел ***Настройка параметров двери***.

Add to Blacklist («Добавление в черный список»)

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

Mark as Visitor («Назначение в качестве посетителя»)

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

При

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.

Device Operator («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 человек 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 пользователя и закройте окно добавления пользователя.
   - Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

7.4.8 Редактирование информации о сотруднике/посетителе

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 и нажмите **Add** («Добавить»).

      Примечание

      В первую очередь необходимо добавить основную информацию о пользователе. Для подробной информации о настройке основной информации о пользователе см. раздел ***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.

7.4.9 Настройка информации о жильце

Для связи с жильцом с помощью видеодомофона, необходимо установить номер комнаты и привязать ее к видеодомофону. Установив связь, 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 пользователе. Для подробной информации о настройке основной информации о пользователе см. раздел ***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 пользователя и закройте окно добавления пользователя.
   - Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

7.4.10 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 пользователе. Для подробной информации о настройке основной информации о пользователе см. раздел ***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 пользователя и закройте окно добавления пользователя.
- Нажмите **Add and New** («Добавить и продолжить») для добавления пользователя и продолжения добавления других пользователей.

7.4.11 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.

7.4.12 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 импортирования»).
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.

7.4.13 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.

7.4.14 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 о 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.

7.4.15 Экспорт изображений сотрудников/посетителей

Экспортируйте файл с изображением лиц добавленных сотрудников и сохраните 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_Имя_0» («0» - для лица, видимого во всех деталях).

7.4.16 Получение информации о пользователе с устройства управления доступом

Если в добавленном устройстве управления доступом была сконфигурирована информация о пользователе (включая подробную информацию о пользователе и информацию о выданной карте), эту 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 в это поле будет заполнено номером выданной карты после импорта в клиентское ПО.
- По умолчанию пол пользователя установлен как **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 клиент.

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.

7.4.17 Перемещение пользователя 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**.

7.4.18 Выдача карт сотрудникам 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. Для более подробной информации см.
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 клавишу ввода **Enter**. Карты будут выпущены для пользователей, отображаемых в списке.

7.4.19 Рапорт 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** («Редактировать»), чтобы открыть соответствующее окно.
3. На панели **Credential → Card** («Учетные данные → Карта»), нажмите на добавленную карту, 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 человек, он не сможет получить доступ к дверям, считав эту утерянную карту.
4. **Опционально:** Нажмите , чтобы отменить рапорт о потере карты, если карта найдена.

   После отмены рапорта об утере карты, авторизация доступа по этой карте будет действительной и активной.
5. Если утерянная карта добавленав группу доступа, которая применена к устройству, после сообщения об утере карты или отмене рапорта об утере карты появится окно с уведомлением о необходимости применить изменения к устройству. После применения к устройству эти изменения будут задействованы на устройстве.

7.4.20 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 работаем 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 карточки нажмите **Settings** («Настройки»), чтобы открыть соответствующее окно.

Локальный режим: Выпуск карт с помощью настольного считывателя карт

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

Card Enrollment Station («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.

Card type («Тип карты»)

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

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

Serial Port («Серийный интерфейс»)

Это поле доступно только для модели считывателя карт DS-K1F100-M. Выберите COM-интерфейс, к которому будет подключен настольный считыватель карт.

Buzzer («Зуммер»)

После успешного считывания номера карты включите или выключите зуммер.

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 и 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.

7.5 Настройка графиков и шаблонов

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

Примечание

Для подробной информации о настройке группы контроля доступа см. раздел ***Настройка группы контроля доступа для назначения разрешений на доступ***.

7.5.1 Добавление выходного дня

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

Шаги

Примечание

Вы можете 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 курсов 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 щелкните столбец Operation («Операции»), чтобы удалить его.
   5) Опционально: **н**ажмите кнопку , чтобы удалить все отрезки времени нерабочих дней.
   6) **Опционально:** или нажмите кнопку , чтобы удалить конкретный нерабочий день.
6. Нажмите **Save** («Сохранить»).

7.5.2 Добавить шаблон

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.

All-Day Authorized («Авторизован в течение всего дня»)

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

All-Day Denied («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 имя для шаблона.
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 курсов 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 выходных.

      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.

7.6 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 номер карты, изображение лица, привязку к номеру карты и связь между номером карты и паролем карты, сроком действия карты и т. д.).

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. Для подробной информации см. раздел ***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.

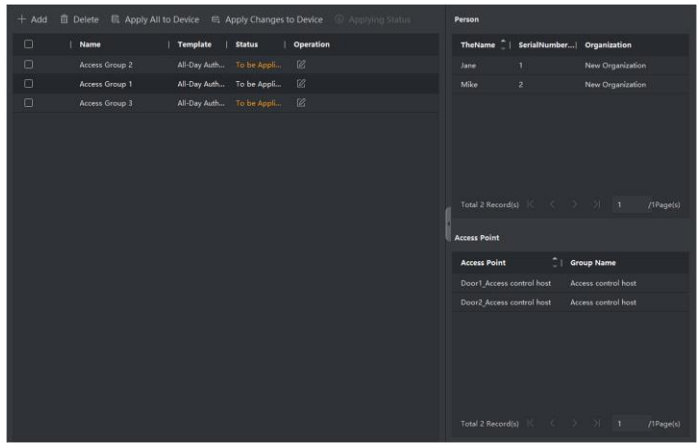


Рисунок 7-5 Отображение выбранных пользователей и точек доступа

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»). Apply to Devices («Применить к устройствам»)**

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

      Apply Changes to Devices («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 доступ.

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»).

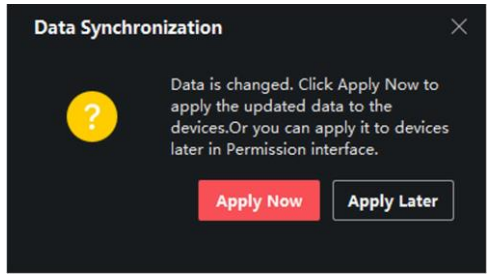


Рисунок 7-7 Синхронизация данных

7.7 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.

7.7.1 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 («Параметр устройства») в списке расширенных функций, наведите курсор, а затем нажмите , чтобы отобразить параметр 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.

   Voice Prompt («Голосовые предупреждения»)

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

   Upload pic. after linked capture («Загрузка изображения после связанного захвата»)

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

   Save pic. after linked capture («Сохранение изображения после связанного захвата»)

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

Face Recognition Mode («Режим распознавания лиц») Normal Mode («Обычный режим»)

Распознавание лиц с помощью камеры в обычном режиме.

Deep Mode («Углубленный режим»)

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

Enable NFC Card («Активация распознавания NFC-карты»)

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

Enable M1 Card («Активация распознавания M1-карты»)

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

Enable EM Card («Активация распознавания EM-карты»)

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

Enable CPU Card («Активация распознавания CPU-карты»)

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

Enable ID Card («Активация распознавания ID-карты»)

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

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

Настройка параметров двери

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 **More** («Дополнительная информация»), чтобы изменить параметры.

Name («Наименование»)

Выберите наименование считывателя карт по своему выбору.

Door Contact («Дверной контакт»)

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

Exit Button Type («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»).

Door Locked Time («Время до закрытия двери»)

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

Extended Open Duration («Расширенная длительность открытого состояния»)

Дверной контакт может быть активирован с установленной задержкой после того, как пользователь с расширенным доступом считает свою карту.

Door Left Open Timeout Alarm («Тревога тайм-аута открытой двери»)

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

Duress Code («Код принуждения»)

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

Super Password («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 на») и выберите устройство контроля доступа, чтобы копировать параметры, указанные на странице, на выбранное устройство.

Примечание

Настройки состояния двери и этажа 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, и выберите название устройства для считывания карт.
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 параметры»), для редактирования параметров.

Basic Information («Основная информация») Name («Наименование»)

Выберите наименование считывателя карт по своему выбору.

Minimum Card Swiping Interval («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.

Alarm of Max. Failed Attempts («Запуск тревоги при достижении максимального количества неудачных попыток считывания карты»)

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

Card Reader Type («Тип считывателя карт»)/ Card Reader Description («Описание считывателя карт»)

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

Расширенные функции

Enable Card Reader («Включить считыватель карт»)

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

OK LED Polarity («Правильная полярность светодиода»)/Error LED Polarity

(«Ошибочная полярность светодиода») /Buzzer Polarity («Полярность зуммера»)

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

Max. Interval When Entering PWD («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.

Tampering Detection («Тревога тампера»)

Включите детектор саботажа на считывателе карт.

Communicate with Controller Every («Связь с панелью управления»)

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

Face 1:N Matching Threshold («Пороговое значение для распознавания 1:N»)

Установка порога опознавания при аутентификации в режиме 1:N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания при аутентификации.

Face Recognition Interval («Интервал распознавания лиц»)

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

Face Anti-spoofing («Детекция подлинности биометрических данных лица (антиспуфинг)»)

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

Face 1:N Matching Threshold («Пороговое значение для распознавания 1:1»)

Установка порога опознавания при аутентификации в режиме 1:1. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания при аутентификации.

Тип применения

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

Lock Authentication Failed Face («Блокировка лица, не прошедшего аутентификацию»)

После включения функции Live Face Detection («Обнаружение живых лиц») система заблокирует лицо пользователя на 5 минут, если количество попыток обнаружения лица живого человека превышает установленное значение. После неудачных попыток аутентификация пользователя будет заблокирована на 5 минут. Для разблокировки пользователь должен успешно пройти аутентификацию два раза в течение 5 минут.

Liveness Detection Security Level («Обнаружение витальности»)

После включения функции Live Face Detection («Обнаружение живых лиц») установите соответствующий уровень безопасности при выполнении аутентификации лица в режиме реального времени.

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

Настройка параметров тревожного выхода

Настройте параметры тревожного выхода после добавления устройства контроля доступа.

Шаги

1. Нажмите **Access Control → Advanced Function → Device Parameter** («Контроль доступа → Расширенные функции → Параметры устройства»), чтобы перейти на соответствующую страницу.
2. Нажмите кнопку ▸ в списке устройств, расположенном слева, чтобы развернуть на экране информацию о двери, выберите тревожный вход и настройте его параметры на панели справа.
3. Настройте параметры тревожного выхода.

   Name («Наименование»)

   Выберите наименование считывателя карт по своему выбору.

   Время работы тревожного выхода

   Время работы тревожного выхода после активации.
4. Нажмите **OK**.
5. **Опционально:** Установите переключатель в верхнем правом углу в положение ON («Вкл.»), чтобы активировать тревожный выход.

7.7.2 Настройка параметров Remaining open («Оставить открытым»)/Remaining closed («Оставить закрытым»)

Настройте состояние двери: open («открыта») или closed («закрыта»). Например, можно перевести дверь в состояние «закрыта» в праздничные дни, или в состояние «открыта» в указанный 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 курсов 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

Copy to Whole Week («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.
Delete Selected («Удалить выбранные интервалы»)	Выберите временной интервал на шкале времени и нажмите **Delete Selected** («Удалить выбранные интервалы»), чтобы удалить временной интервал.
Clear («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 курсов 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 щелкните столбец Operation («Операции»), чтобы удалить его.
7) Опционально: Нажмите кнопку  , чтобы удалить все отрезки времени нерабочих дней.
8) **Опционально:** Или нажмите кнопку  , чтобы удалить конкретный нерабочий день.
9) Нажмите **Save** («Сохранить»).

5. **Опционально:** Нажмите **Copy to** («Скопировать на»), чтобы применить состояние двери к этой двери и к другим дверям.

7.7.3 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. Для более подробной информации см. раздел ***Настройка группы контроля доступа для назначения разрешений на доступ***.

Выполните следующие действия, чтобы настроить аутентификацию сразу нескольких карт для одной точки управления доступом (дверей).

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 своему усмотрению.
   3) Укажите время начала и время окончания периода действия разрешения 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 группы 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»).

Local Authentication («Локальная аутентификация»)

Аутентификация с помощью устройства контроля доступа.

Local Authentication and Remotely Open Door («Локальная аутентификация и удаленное открытие двери»)

Аутентификация с помощью устройства управления доступом и посредством клиентского ПО. После считывания карты появится окно. Дверь может быть разблокирована через клиентское ПО.

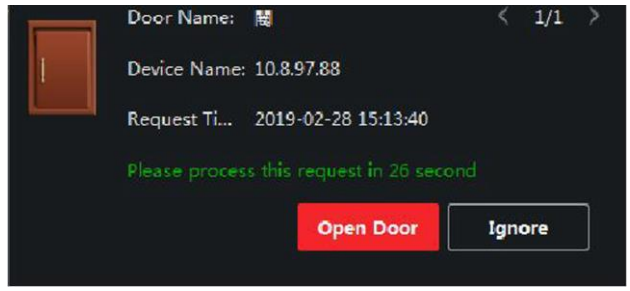


Рисунок 7-8 Удаленное открытие двери

Примечание

В меню нажмите **Offline Authentication** («Автономная аутентификация»), чтобы активировать функцию аутентификации по паролю суперпользователя, если устройство управления доступом было отключено от клиентского ПО.

Локальная аутентификация и суперпароль

Аутентификация с помощью устройства управления доступом и пароля суперпользователя.

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 управления 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 L**ocal 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»).

7.7.4 Настройка аутентификации при помощи 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 на кнопку **Configuration** («Настройки»).

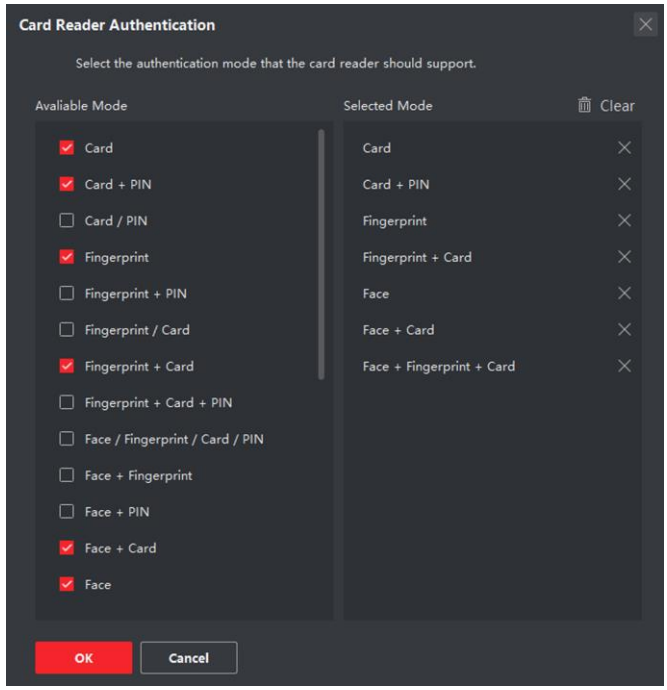


Рисунок 7-9 Выбор режима аутентификации для считывателя карт

Примечание

PIN означает PIN-код, установленный для разблокировки двери. См. раздел ***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 указателем мыши по определенному дню, чтобы нарисовать цветную полосу в графике. Это значит, что в данный отрезок времени будет использоваться аутентификация при помощи устройства для считывания карт.

5. Повторите этот шаг для установки других отрезков времени.

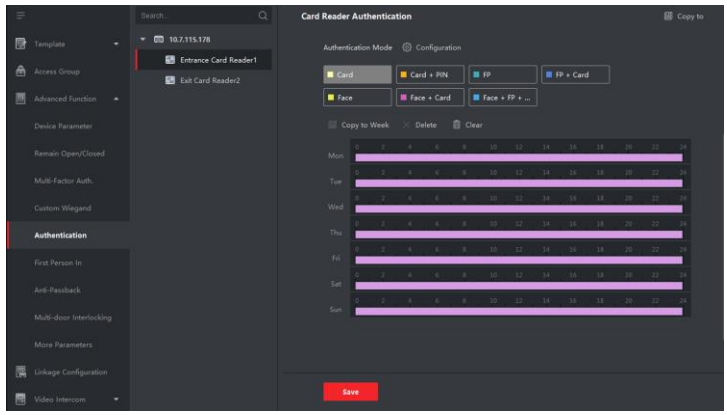


Рисунок 7-10 Установка режима аутентификации для считывателя карт

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»).

7.7.5 Настройки аутентификации в качестве 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. Для более подробной информации см.

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 в качестве 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 пользователя 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.

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

Деактивация функции аутентификации в качестве первого пользователя.

Примечание

Чтобы отключить режим авторизации в качестве первого пользователя, необходимо выполнить повторную авторизацию первого пользователя.

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»).

7.7.6 Настройка запрета двойного прохода

Установите контрольный пункт проверки доступа, через который возможен проход одного человека после считывания карты.

Перед началом

Включите функцию запрета двойного прохода по маршруту.

Для настройки функции запрета двойного прохода выполните следующие действия.

Шаги

Примечание

Для устройства контроля доступа можно одновременно настроить функцию запрета двойного прохода или блокировки нескольких дверей. Для настройки функции блокировки нескольких дверей см.

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 в устройстве.

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.

7.7.7 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.

Шаги

Примечание

Эта функция должна поддерживаться устройством.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации 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 Multiple NIC.
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»).

Установка 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 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 режим загрузки журнала.
6. Выберите режим загрузки из выпадающего списка.
   - Включите **N1** или **G1** для основного и резервного канала.
   - Выберите **Close** («Закрыть»), чтобы деактивировать основной или резервный канал.

Примечание

Не допускается активация N1 или G1 на основном и резервном канале одновременно.

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

Эта функция должна поддерживаться устройством.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации 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.
9. Укажите имя учетной записи сетевого центра.
10. Нажмите **Save** («Сохранить»).

Установка 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. Подробнее см. в разделе *Назначение хранилища изображений* руководства пользователя клиентского программного обеспечения.

Установка 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. Подробнее см. в разделе *Назначение хранилища изображений* руководства пользователя клиентского программного обеспечения.

Шаги

Примечание

Эта функция должна поддерживаться устройством.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации 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»).

Установка 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. Подробнее см. в разделе *Назначение хранилища изображений* руководства пользователя клиентского программного обеспечения.

Шаги

Примечание

Эта функция должна поддерживаться устройством.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации 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 и т. д.

Шаги

Примечание

Эта функция должна поддерживаться устройством.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации 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. Установите параметры.

Примечание

Отображаемые параметры могут отличаться в зависимости от модели.

Algorithm («Алгоритм»)

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

Save Authenticating Face Picture («Сохранение изображений лиц, захваченных при аутентификации»)

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

ECO Mode («ЭКО-режим»)

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

ECO Mode (1:1) («Режим ЭКО (1:1)»)

Установка порога опознавания при аутентификации в режиме ЭКО 1:1. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания.

ECO Mode (1:N) («Режим ЭКО (1:N)»)

Установка порога опознавания при аутентификации в режиме ЭКО 1:N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания.

ECO Mode Threshold («Пороговое значение ЭКО-режима»)

Установите пороговое значение для ECO-режима при включении функции. Чем больше значение, тем легче устройство переходит 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»).

Включить M1 Card Encryption («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 перейдите на **Advanced Function → More Parameters** («Расширенные функции → Прочие параметры»).
3. Выберите устройство контроля доступа в списке устройств и нажмите **M1 Card Encryption** («Шифрование карты M1»), чтобы открыть страницу «Шифрование карты M1».

4. Установите переключатель в положение On («Вкл.»), чтобы включить функцию шифрования карты M1.
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.

Установка 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 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. Установите скорость передачи данных, бит данных, стоповый бит, режим связи, режим работы и режим соединения из всплывающего списка.

Примечание

Если режим связи установлен как **Connect Access Control Device** («Подключение устройства контроля доступа»), выберите **Card No.** («Номер карты») или **Person ID («Идентификатор пользователя»)** в качестве типа выхода.

6. Нажмите **Save** («Сохранить»).
   - Настроенные параметры будут автоматически применены к устройству.
   - При изменении режима работы или режима подключения устройство автоматически перезагрузится.

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.

Шаги

Примечание

Эта функция должна поддерживаться устройством.

1. Нажмите на иконку для перехода в модуль контроля доступа.
2. На панели навигации 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 назначении **Communication Direction** («Направление коммуникации») в значение **Sending** («Отправить»), необходимо установить режим Wiegand в значение **Wiegand 26 или Wiegand 34.**

6. Поставьте галочку **Enable Wiegand** («Включить Wiegand»), чтобы включить функцию Wiegand.
7. Нажмите **Save** («Сохранить»).
   - Настроенные параметры будут автоматически применены к устройству.
   - После изменения направления коммуникации устройство автоматически перезагрузится.

7.8 Настройка привязанных действий

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:

- **Client Actions («Действия на клиентском ПО»):** При обнаружении события на клиентском ПО будут запущены привязанные действия, в том числе выдача звуковых предупреждений.
- **Device Actions («Действия на устройстве»):** При обнаружении события на устройстве будут запущены привязанные действия, а именно запускается зуммер и открываются/закрываются двери.

7.8.1 Настройка действий на клиентском ПО при событии доступа

Даже находясь далеко от точки доступа можно отслеживать событие на клиентском ПО, настроив привязанные действия при событии доступа. Уведомление о событии будет отправлено в клиентское ПО незамедлительно. Также можно настроить сразу несколько действий на точках доступа клиентского ПО в пакетном режиме.

Шаги

Примечание

Привязанные действия означают связанные операции клиентского ПО, в том числе звуковые предупреждения, отправка Email и т.д.

1. Нажмите **Event Management → Access Control Event («Управление событием → Событие доступа»).**

   Добавленные устройства контроля доступа отобразятся в списке.
2. Выберите ресурс (включая устройство, тревожный вход, дверь/лифт 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.

      Audible Warning («Звуковое предупреждение»)

      Клиентское программное обеспечение выдает звуковое предупреждение при срабатывании тревоги. Выберите сигнал для звукового предупреждения.

      Примечание

      Для настройки звукового сигнала тревоги обратитесь к разделу *Настройка звукового сигнала* руководства пользователя клиентского программного обеспечения.

      Send Email («Отправить Email»)

      Отправьте электронное уведомление о тревоге одному или нескольким получателям.

      Подробнее о настройке параметров электронной почты см. в разделе *Настройка параметров электронной почты* в руководстве пользователя клиентского программного обеспечения.
   2) Нажмите **OK**.
5. Обнаруженное событие будет отправлено в клиентское ПО, которое запустит привязанные действия.
6. **Опционально:** Нажмите кнопку **Copy to («**Копировать на»), чтобы скопировать настройки события на другое устройство контроля доступа, тревожный вход, дверь или считыватель карт.

7.8.2 Настройка действий устройства при событии доступа

Установите привязанные действия 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 («Целевая область привязки») установите цель свойства, чтобы включить соответствующее действие.

   Зуммер контроллера

   Устройство контроля доступа выдаст звуковое предупреждение.

   Захват

   Запуск захвата изображений в режиме реального времени.

   Access Point («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.

7.8.3 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

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 **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 («Целевая область привязки») установите цель свойства, чтобы включить соответствующее действие.

   Зуммер контроллера

   Устройство контроля доступа выдаст звуковое предупреждение.

   Захват

   Запуск захвата изображений в режиме реального времени.

   Access Point («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 настроенные параметры привязки из списка устройств. Измените параметры события, в том числе источник события и цель привязки.

7.8.4 Настройка действий устройства для идентификатора пользователя

Установите привязанные действия устройства контроля доступа для конкретного идентификатора пользователя. При обнаружении идентификатора пользователя устройством контроля доступа срабатывает зуммер и другие действия на считывателе карт.

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.

   Зуммер контроллера

   Устройство контроля доступа выдаст звуковое предупреждение.

   Зуммер считывателя карт

   Устройство контроля доступа выдаст звуковое предупреждение.

   Захват

   Изображение будет захвачено, когда произойдет выбранное событие.

   Запись

   Изображение будет захвачено, когда произойдет выбранное событие.

   Примечание

   Функция записи должна поддерживаться на устройстве.

   Access Point («Точка доступа»)

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

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.

7.9 Управление состоянием 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*** .

7.9.1 Управление состоянием двери

Можно контролировать состояние одной двери, включая открытие двери, закрытие двери, оставление двери открытой и оставление двери закрытой.

Шаги

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

   Примечание

   Для управления группой точек доступа см. раздел *Управление группами* в руководстве пользователя клиентского программного обеспечения.

   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.
4. Нажимайте следующие кнопки, чтобы управлять дверью.

   Разблокировка двери

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

   Блокировка двери

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

   Оставить дверь открытой

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

   Оставить дверь закрытой

   Дверь будет закрыта и заблокирована. 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.

Result («Результат»)

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

7.9.2 Запись информации о считывании карт 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.

7.10 Календарь 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 под охрану. Для получения дополнительной информации см. раздел ***Включение функции получения события от устройств*** .

7.10.1 Включение функции получения события от устройств

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

Шаги

1. Нажмите → **Tool** → **Device Arming Control** («Инструмент → Управление постановкой под охрану»), чтобы перейти на соответствующую страницу.

   Все добавленные устройства появляются на этой странице.
2. В столбце Auto-Arming («Автоматическая постановка под охрану») поверните переключатель, чтобы активировать функцию автоматической постановки под охрану.

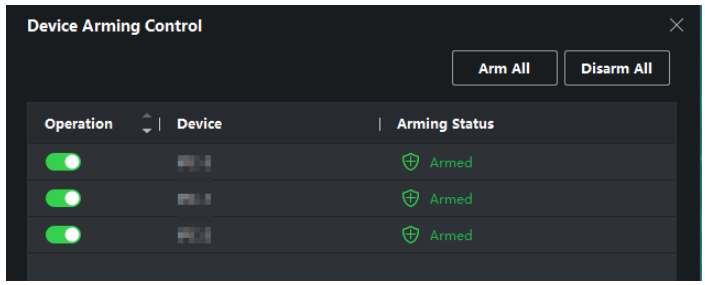


Рисунок 7-11 Постановка устройства по охрану

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

7.10.2 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 события от устройств, чтобы клиентское ПО могло получать события из устройства. Для подробной информации см. ***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. Просмотрите детали события.
   1) Выберите событие из списка событий.
   2) Нажмите **Expand** («Развернуть») в правом нижнем углу страницы.
   3) Посмотрите подробное описание и редактируйте записи о событии.
5. **Опционально:** При необходимости выполните следующие действия.

   Handle Single Event («Обработка параметров одного события») Нажмите **Handle** («Обработать»), чтобы перейти на страницу параметров обработки, затем нажмите **Commit** («Принять»).

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	Выберите события, которые подлежат обработке, затем нажмите **Handle in Batch**. («Обработать в пакетном режиме»). Введите параметр обработки, затем нажмите **Commit** («Принять»).
Включение/выключение звуковой сигнализации	Нажмите **Enable Audio**/**Disable Audio** («Включение/выключение звуковой сигнализации»), чтобы включить функцию включению/выключению звуковой сигнализации 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.

Clear Events («Очистить события») Нажмите кнопку **Clear («Очистить»)**, чтобы очистить все события из списка.

Send Email («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.

7.10.3 Поиск по журналу событий

В модуле поиска по журналу событий можно осуществлять поиск по времени, типу устройства и другим условиям в зависимости от типа устройства, затем можно обработать события.

Перед началом

Включите функцию получения события от устройств, чтобы клиентское ПО могло получать информацию с устройства. Для подробной информации см. ***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 при инициации события.

Поиск по

Устройства

Поиск событий с помощью устройства и каналов ресурсов устройств. При поиске по событию необходимо установить следующие настройки:

- **Include Sub-Node** («Включить подузел») Поиск событий с помощью устройства и всех его каналов.
- **Device Type** («Тип устройства») Выберите устройство, в котором необходимо выполнить поиск по событию.

Group («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 управления доступом нажмите **Show More** («Показать еще»), чтобы установить 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.

Состояние

Состояние обработки события.

3. Нажмите Search («Поиск») для поиска событий согласно указанным условиям.

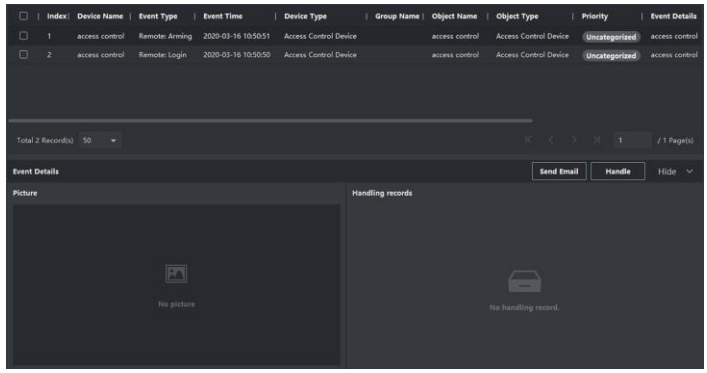


Рисунок 7-12 Поиск по журналу событий

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. **Опционально:** Выполните одну из следующих операций.

Обработка 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 одно событие, которое 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.

Send Email («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.

Экспорт информации о событии	Нажмите **Export** («Экспорт») для экспорта журнала и изображений события на компьютер в формате Excel/CSV. Задайте папку сохранения вручную.
Загрузка изображений события	Наведите курсор на соответствующее изображение, а затем щелкните значок загрузки в верхнем правом углу изображения, чтобы загрузить изображение на компьютер. Задайте папку сохранения вручную.

7.11 Рабочее время и посещаемость

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.

7.11.1 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 контрольного пункта проверки посещаемости можно указать считыватель карт точки управления доступом. В этом случае считывание карты будет регистрироваться для сбора статистики УРВ.

Перед началом
Добавьте устройство контроля доступа перед настройкой пункта проверки посещаемости. Для подробной информации см. радел ***Добавление устройства*** .

Шаги

Примечание

По умолчанию все считыватели карт устройства контроля доступа назначены в качестве контрольного пункта проверки посещаемости.

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. **Опционально:** Переведите переключатель **Set All Card Readers as Check Points** («Назначение всех считывателей карт в качестве контрольных пунктов проверки посещаемости») в положение Off («Выкл.»).

   В качестве контрольных пунктов проверки посещаемости будут назначены только считыватели карт, перечисленные в списке.
4. Назначьте некоторые из считывателей карт из списка в качестве контрольных пунктов проверки посещаемости по своему выбору.
5. Выберите статус функции контрольного пункта: **Start/End-Work** («Начало / Окончание работы»).
6. Нажмите **Set as Check Point** («Установите в качестве контрольного пункта проверки»).

   После настройки контрольные пункты проверки посещаемости будут отображаться в списке справа.

Настройки 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:

    Edit Holiday («Изменение выходного дня») Нажмите для редактирования информации о выходных днях.

    Delete Holiday («Удаление выходных дней») 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 выходной банка.

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:

    Edit Holiday («Изменение выходного дня») Нажмите для редактирования информации о выходных днях.

    Delete Holiday («Удаление выходных дней») Выберите один или несколько выходных дней, затем нажмите **Delete** («Удалить»), чтобы удалить выходной день из списка.

Настройки типа отпуска

Настройте тип отпуска (основной и дополнительный тип отпуска) в соответствии с фактическими 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.

   Edit («Изменить») Направьте курсов на основной тип отпуска и нажмите, для

изменения основного типа отпуска.

Delete («Удалить») Направьте курсов на основной тип отпуска и нажмите **Delete** («Удалить»), чтобы удалить основной тип отпуска.

5. Нажмите **Add** («Добавить») на панели слева, чтобы добавить основной тип отпуска.
6. **Опционально:** Для добавления дополнительных типов отпуска необходимо выполнить следующие действия.

Edit («Изменить») Направьте курсов на дополнительный тип отпуска и нажмите , для изменения дополнительного типа отпуска.

Delete («Удалить») 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 о посещаемости, записанные в клиентском программном обеспечении, могут быть использованы в другой системе для сбора статистики УРВ или других операций. Включите функцию синхронизации, чтобы автоматически применить запись аутентификации из клиентского программного обеспечения к сторонней базе данных.

Шаги

1. Войдите в модуль Time & Attendance («Учет рабочего времени»).
2. Click **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, наименование базы данных, имя пользователя и пароль.
6. Установите табличные параметры базы данных в соответствии с фактической конфигурацией.
   1) Введите наименование таблицы сторонней базы данных.
   2) Задайте поля сопоставленной таблицы между клиентским программным обеспечением и сторонней базой данных.
7. Нажмите **Save** («Сохранить»), чтобы проверить возможность подключения к базе данных, и сохраните настройки для успешного подключения.
   - Данные о посещаемости 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** («Учет рабочего времени → Расписание»).

   Добавленные расписания отображаются в списке.
2. Выберите расписание и нажмите **Add** («Добавить»), чтобы перейти на страницу настроек расписания.
3. Нажмите на **Break Time** («Перерыв»), чтобы перейти на соответствующую страницу.
4. Нажмите **Break Time Settings** («Настройки времени перерыва»).
5. Добавьте перерыв.
   1) Нажмите **Add** («Добавить»).
   2) Введите наименование перерыва.
   3) Установите сопутствующие параметры.

      Start Time/End Time («Время начала/Время окончания»)

      Укажите время начала и время окончания перерыва.

      No Earlier Than / No Later Than («Не ранее/Не позднее»)

      Установите самое раннее возможное время начала перерыва и самое позднее время окончания перерыва.

      Break Duration («Продолжительность перерыва»)

      Продолжительность перерыва от времени начала до времени окончания перерыва.

      Calculation Auto Deduct («Автоматическое исключение из рабочего времени»)

      Фиксированная продолжительность перерыва будет исключена из рабочего времени.

      Must Check («Обязательная регистрация прихода/ухода»)

      Продолжительность перерыва будет рассчитана и исключена из рабочего времени в соответствии с фактическим временем регистрации прихода/ухода сотрудника.

      Примечание

      При выборе **Must Check** («Обязательная регистрация прихода/ухода») в качестве метода расчета, необходимо установить статус посещения для позднего или раннего возвращения с перерыва.
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.

   Company Name («Наименование компании»)

   Введите наименование компании для отображения в отчете.

   Attendance Status Mark («Отметка о статусе посещения»)

   Введите отметку и выберите цвет. Поля, связанные с полем статуса посещения, в отчете будут отображаться с указанной меткой и цветом.

   Weekend Mark («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»).

7.11.2 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.

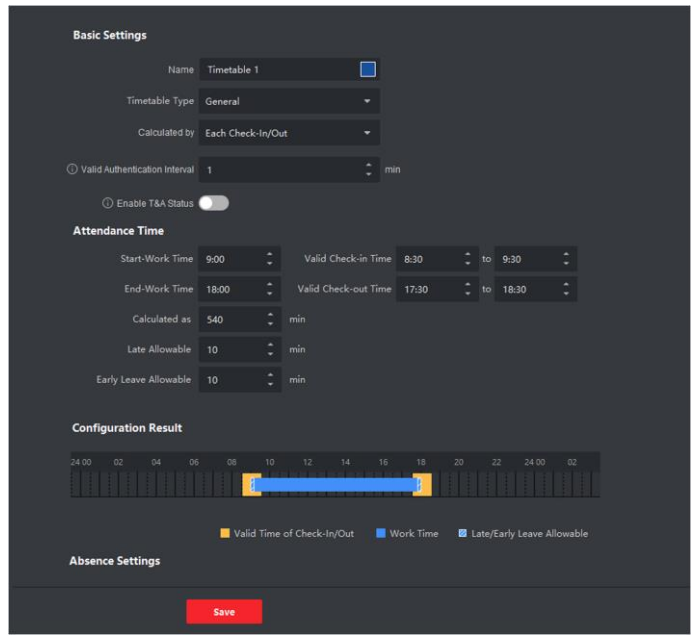


Рисунок 7 - 13 Добавление расписания

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.

   First In & Last Out («Регистрация первого прихода и последнего ухода»)

Время регистрации первого прихода учитывается как время начала работы, а время регистрации последнего ухода - как время окончания работы.

Each Check-In/Out («Регистрация каждого прихода/ухода»)

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 статусах посещений.

Примечание

Эта функция должна поддерживаться устройством.

7. Установите следующие сопутствующие параметры времени посещений:

Start/End-Work Time («Начало/Окончание рабочего времени»)

Установите время начала и время окончания работы.

Valid Check-in/out Time («Действительное время регистрации прихода/ухода»)

На временной шкале установите расписание, в течение которого регистрация прихода/ухода является действительной.

Calculated as («Рассчитывается как»)

Установите продолжительность, рассчитанную как фактическая продолжительность работы.

Late/Early Leave Allowable («Допустимый интервал опозданий/ранних уходов»)

Установите временные интервалы для ранних приходов и опозданий.

8. Установите другие сопутствующие параметры.

Check-In, Late for («Регистрация прихода с опозданием»)

Установите максимальный интервал опозданий для работников, прошедших регистрацию прихода на работу. При превышении установленного интервала опоздания сотрудник будет считаться отсутствующим.

Check-Out, Early Leave for («Регистрация раннего ухода»)

Установите максимальный интервал ранних уходов с работы. Сотрудник, прошедший регистрацию ухода ранее установленного времени, будет считаться отсутствующим.

No Check-in («Отсутствие регистрации прихода»)

Сотрудник, не прошедший регистрацию прихода, будет считаться отсутствующим или опоздавшим.

No Check-Out («отсутствие регистрации ухода»)

Сотрудник, не прошедший регистрацию ухода, будет считаться отсутствующим или опоздавшим.

9. Нажмите **Save** («Сохранить») для добавления расписания.

10. Опционально: После добавления расписания выполните следующие действия.

Edit Timetable («Изменение расписания») Выберите расписание из списка для редактирования соответствующей информации.

Delete Timetable («Удаление расписания») Выберите расписание из списка и нажмите**Delete** («Удалить»), чтобы удалить его.

7.11.3 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. Для подробной информации см.***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.

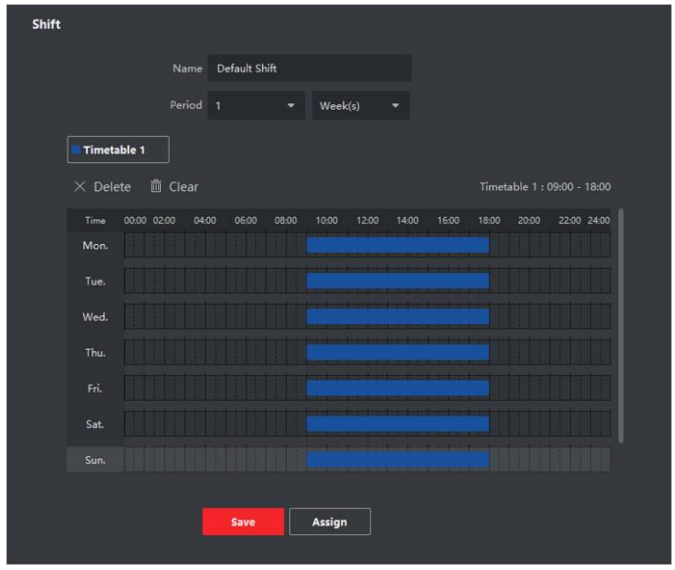


Рисунок 7 - 14 Добавление смены

Примечание

Можно выбрать несколько расписаний. Время начала и окончания работы, а также действительное время регистрации прихода/ухода не могут совпадать в разных расписаниях.

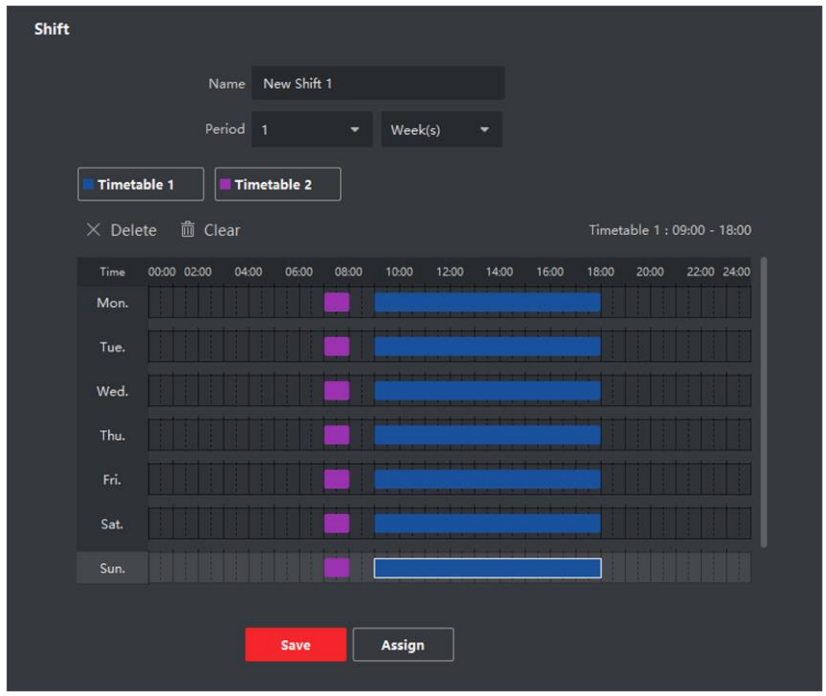


Рисунок 7 - 15 Добавление нескольких расписаний

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.

      Check-In Not Required («Регистрация прихода не требуется»)

      Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они приходят на работу.

      Check-Out Not Required («Регистрация ухода не требуется»)

      Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они уходят с работы.

      Scheduled on Holidays («График, предусмотренный для выходного дня»)

      Этот график действует в выходные дни, и сотрудники должны приходить на работу в соответствии с графиком.

Effective for Overtime («График, предусмотренный для сверхурочной работы»)

В этом графике будут указаны параметры сверхурочной работы сотрудников.

5) Нажмите **Save** («Сохранить»), чтобы сохранить график смены.

7.11.4 Управление графиком смены

Сменная работа - 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.

Установка 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. Настройка дату начала и дату окончания периода.
7. Установите другие параметры для графика.

   Check-In Not Required («Регистрация прихода не требуется»)

   Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они приходят на работу.

   Check-Out Not Required («Регистрация ухода не требуется»)

   Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они уходят с работы.

   Scheduled on Holidays («График, предусмотренный для выходного дня»)

   Этот график действует в выходные дни, и сотрудники должны приходить на работу в соответствии с графиком.

   Effective for Overtime («График, предусмотренный для сверхурочной работы»)

   В этом графике будут указаны параметры сверхурочной работы сотрудников.
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. Настройка дату начала и дату окончания периода.
7. Установите другие параметры для графика.

Check-In Not Required («Регистрация прихода не требуется»)

Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они приходят на работу.

Check-Out Not Required («Регистрация ухода не требуется»)

Сотрудникам, перечисленным в этом графике, не нужно регистрироваться, когда они уходят с работы.

Scheduled on Holidays («График, предусмотренный для выходного дня»)

Этот график действует в выходные дни, и сотрудники должны приходить на работу в соответствии с графиком.

Effective for Overtime («График, предусмотренный для сверхурочной работы»)

В этом графике будут указаны параметры сверхурочной работы сотрудников.

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.

   Calculated as («Рассчитывается как»)

   Выберите обычный или сверхурочный уровень работы, чтобы отметить статус посещения для временного графика.

   Timetable («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.

7.11.5 Коррекция записи регистрации прихода/ухода вручную

Если статус посещения неверен, можно вручную исправить запись о регистрации прихода/ухода. Также можно редактировать, удалить, выполнять поиск или 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 добавления изменений в записи регистрации прихода/ухода.
3. Выберите сотрудника из списка слева для внесения изменений.
4. Выберите дату внесения изменений.
5. Установите параметры коррекции записи о регистрации прихода/ухода.
   - Выберите **Check-in** («Регистрация прихода») и установите фактическое время начала работы.
   - Выберите **Check-out** («Регистрация ухода») и установите фактическое время окончания работы.

   Примечание

   Нажмите ⊕, чтобы добавить несколько пунктов для записей о регистрации прихода/ухода. Можно добавить до 8 пунктов.
6. **Опционально:** При необходимости создайте примечание.
7. Нажмите **Save** («Сохранить»).
8. **Опционально:** После добавления корректировки записи регистрации прихода/ухода выполните следующие действия:

   View («Просмотр») 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.

   Edit («Редактирование») •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.

Delete («Удаление») Удалите выбранные пункты.

Export («Экспорт») Экспортируйте информацию об обработке записей о посещениях на компьютер.

Примечание

Экспортируемые файлы сохраняются в формате CSV.

7.11.6 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** («Применить к отпуску/командировке»), 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 типы 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.

View («Просмотр») 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.

Edit («Редактирование») •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.

Delete («Удаление») Удалите выбранные пункты.

Export («Экспорт») Экспортируйте информацию об обработке записей о посещениях на компьютер.

Примечание

Экспортируемые файлы сохраняются в формате CSV.

7.11.7 Расчет данных о посещаемости

Необходимо рассчитать данные о посещаемости 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.

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

Рассчитайте данные о посещаемости вручную, предварительно установив диапазон данных.

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. Укажите другие данные, в том числе отдел, имя сотрудника, идентификатор пользователя и статус посещения.
5. Нажмите **Calculate** («Расчет»).

   Примечание

   Клиентское ПО может рассчитать данные о посещаемости только за три месяца.

6. Выполните одну из следующих операций.

   Correct Check-in/out («Корректировка записи прихода/ухода») Нажмите **Correct Check-in/out** («Корректировка записи прихода/ухода»), для добавления корректировки прихода/ухода.

   Выберите пункты, которые необходимо отобразить Нажмите , или щелкните правой кнопкой мыши заголовки различных пунктов, чтобы выбрать пункты для отображения в отчете.

Generate Report («Составление отчета») Нажмите **Report** («Отчет»), чтобы сгенерировать отчет по посещению.

Export Report («Экспорт отчета») Нажмите **Export** («Экспорт»), чтобы экспортировать данные о посещаемости на компьютер.

Примечание

Экспортируемые файлы сохраняются в формате CSV.

7.11.8 Статистика посещений

Проверьте исходную запись о посещении, сгенерируйте и экспортируйте отчет по посещению, созданный на основе рассчитанных данных.

Получение обзора данных о посещаемости сотрудников

Записи о посещениях сотрудника можно найти и просмотреть на клиентском ПО, в том числе время посещения, статус посещения, 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. Для подробной информации см. раздел ***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: **Original Records on Device** («Исходная запись на устройстве») или **Manual Handling Records** («Обработка записей вручную»).
6. **Опционально:** Нажмите **Get Events from Device** («Получение информации о событии с устройства»), чтобы получить информацию о посещении с устройства.
7. **Опционально:** Нажмите **Reset** («Сбросить»), чтобы сбросить все условия поиска, затем повторно отредактируйте условия поиска.
8. Нажмите **Search** («Поиск»).

После этого на странице появятся результаты поиска. Просмотрите статус посещений сотрудника и пункт проверки посещаемости.

9. **Опционально:** После поиска выполните следующие действия.

   Generate Report («Составление отчета») Нажмите **Report** («Отчет»), чтобы сгенерировать отчет по посещению. **Export Report («Экспорт отчета»)** Нажмите **Export** («Экспорт»), чтобы экспортировать данные о посещаемости на компьютер. **Custom Export («Настройки экспорта»)** Для подробной информации см.

Создание мгновенного отчета

Поддерживается функция создания серии отчетов о посещаемости вручную для просмотра посещаемости сотрудников.

Перед началом

Рассчитайте данные о посещаемости.

Примечание

Рассчитайте данные о посещаемости вручную или установите график таким образом, чтобы клиентское ПО производило расчет данных автоматически каждый день. Для подробной информации см. раздел ***Расчет данных о посещаемости*** .

Шаги

1. Войдите в модуль Time & Attendance («Учет рабочего времени»).
2. Нажмите **Attendance Statistics → Report Display** («Статистика посещений → Отображение отчета»).
3. Выберите тип отчета.
4. Выберите отдел или сотрудника, чтобы просмотреть отчет по посещению.
5. Установите время начала и время окончания расчетного периода для включения в отчет.
6. Нажмите **Report** («Отчет»), чтобы сгенерировать статистический отчет и открыть его.

Настройки отчета по посещению

Клиентское ПО поддерживает несколько типов отчетов. Можно предварительно определить содержимое отчета и автоматически отправлять отчет на указанный адрес электронной почты.

Шаги

Примечание

Установите параметры электронной почты, прежде чем включить функцию автоматической отправки электронной почты. Подробнее см. в разделе *Назначение параметров электронной почты* руководства пользователя клиентского программного обеспечения.

1. Войдите в модуль Time & Attendance («Учет рабочего времени»).
2. Нажмите **Attendance Statistics → Custom Report** («Статистика посещений → Настройки отчета»).
3. Нажмите **Add** («Добавить»), чтобы предварительно определить содержимое отчета.
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.
5. **Опционально:** Настройте график автоматического отправления отчета на электронный адрес.
   1) Выберите **Auto-Sending Email** («Отправление электронной почты в автоматическом режиме») и включите эту функцию.
   2) Установите период, в течение которого клиентское ПО будет отправлять отчеты.
   3) Выберите дату (даты) отправления отчета.
   4) Установите время отправления отчета.

      Пример

      Установите период с 10.03.2018 по 10.08.2018, 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 10.08.2018.

      Примечание

      Перед настройкой времени произведите расчет статистики посещений. Рассчитайте данные о посещаемости вручную или установите график таким образом, чтобы клиентское ПО производило расчет данных автоматически каждый день. Для подробной информации см. раздел ***Расчет данных о посещаемости***.
   5) Введите электронный адрес получателя.

      Примечание

      Нажмите **+** , чтобы добавить новый адрес электронной почты. Можно добавить до 5 адресов электронной почты.
   6) **Опционально:** Нажмите **Preview** («Предварительный просмотр») для просмотра параметров адреса электронной почты.
6. Нажмите **OK**.
7. **Опционально:** После добавления настроенного отчета выполните следующие действия: **Edit Report («Редактирование отчета»)** Выберите отчет и нажмите **Edit** («Редактировать»), чтобы изменить его параметры. **Delete Report («Удаление отчета»)** Выберите отчет и нажмите **Delete** («Удалить»),

чтобы удалить его.

Generate Report («Составление отчета») Нажмите **Report** («Отчет»), чтобы мгновенно сгенерировать отчет и просматривать его содержание.

7.12 Удаленная конфигурация (Web)

Настройте параметры устройства удаленно.

7.12.1 Просмотр информации об устройстве

Просмотр и назначение имени устройства, просмотр типа устройства, серийного номера, версии, номера реле и номера блокировки. Выберите устройство на вкладке управления устройствами и нажмите → **System** → **Device Information** («Система → Информация об устройстве»),
чтобы перейти на соответствующую страницу.

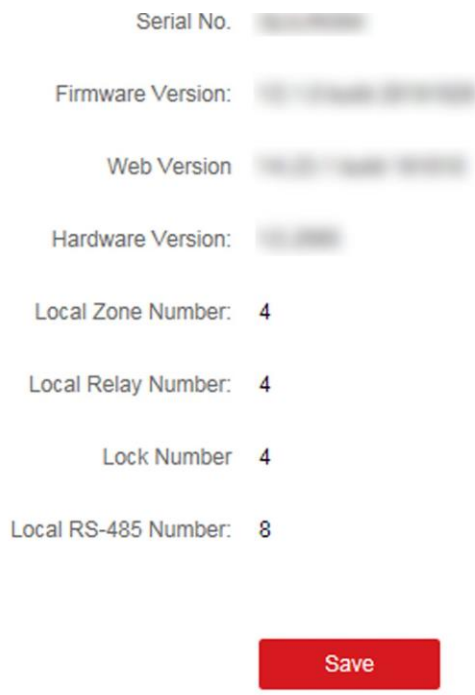


Рисунок 7 - 16 Просмотр информации об устройстве

Английский язык	Русский язык
Device name	Наименование устройства
Device type	Тип устройства
Serial No.	Серийный номер
Firmware version	Версия прошивки
WEB version	WEB-версия
Hardware version	Версия оборудования
Local zone number	Номер области
Local relay number	Номер реле
Lock number	Номер блокировки
Local RS-485 number	Номер интерфейса RS-485

Просмотр и назначение имени устройства, просмотр типа устройства, серийного номера, версии, номера реле и номера блокировки. Нажмите **Save** («Сохранить») для сохранения настроек.

7.12.2 Изменение пароля устройства

Здесь можно изменить пароль устройства.

Перед началом
Устройство должно быть активировано. Подробная информация представлена в разделе *Активация*.

Шаги
1. На странице управления устройствами нажмите → **System** → **User** («Система → Пользователь»), чтобы перейти на соответствующую страницу.
2. Выберите пользователя и нажмите **Edit** («Редактировать»), чтобы перейти на страницу редактирования.
3. Введите старый пароль, затем придумайте и подтвердите новый пароль.

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, из них не менее трех элементов из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит повысить безопасность при использовании продукта.
Правильная настройка паролей и других параметров безопасности является обязанностью лица, выполняющего установку, или конечного пользователя.

4. Нажмите **OK**. **Result («Результат»)**

Пароль устройства изменен. Для повторного подключения устройства необходимо ввести новый пароль на странице управления устройством.

7.12.3 Управление временем

Выберите часовой пояс устройства, затем синхронизируйте время и параметры DST.

Часовой пояс и синхронизация времени

На странице управления устройствами выберите устройство и нажмите → **System** → **Time** («Система→ Время»), чтобы перейти на соответствующую страницу.
Выберите часовой пояс, настройте NTP-параметры или синхронизируйте время вручную.

Часовой пояс

Выберите часовой пояс из выпадающего списка.

NTP

Устройство автоматически синхронизирует время с NTP. После добавления NTP необходимо задать адрес сервера NTP, NTP-порт и интервал синхронизации.

Синхронизация времени вручную

Включив функцию **Manual Time Synchronization** («Синхронизация времени в ручном режиме»).

При выборе функции **Synchronize with Computer Time («Синхронизировать с временем на ПК»)**, **Set Time** («Установленное время») примет текущее время на ПК. Деактивируйте функцию **Synchronize with Computer Time («Синхронизировать с временем на ПК»)** и нажмите , чтобы установить время на устройстве в ручном режиме.

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

DST («Летнее время»)

На странице управления устройствами нажмите **Remote Configuration → System → Time → DST** («Удаленная конфигурация → Система → Время → DST»), чтобы перейти на соответствующую вкладку.
Включите функцию DST, чтобы установить смещение DST, время начала и время окончания DST. Нажмите **Save** («Сохранить»).

7.12.4 Обслуживание системы

Перезагрузите устройство удаленно, восстановите настройки устройства по умолчанию, импортируйте файл конфигурации, обновите устройство и т. д.

Перезагрузка

На странице управления устройствами нажмите → **System** → **System Maintenance** («Система → Обслуживание системы»), чтобы перейти на соответствующую вкладку.
Нажмите **Reboot**, чтобы перезагрузить устройство.

Восстановление настроек

На странице управления устройствами нажмите **Remote Configuration → System → System Maintenance** («Удаленная конфигурация → Система → Обслуживание системы»), чтобы перейти на соответствующую вкладку.

Восстановление настроек по умолчанию

Параметры будут сброшены до заводских настроек, за исключением IP-адреса.

Восстановление части настроек

Восстановите заводские настройки, кроме настроек связи и настроек удаленного пользователя.

Восстановить все настройки

Параметры будут сброшены до заводских настроек. После сброса настроек необходимо активировать устройство.

Импорт и экспорт

На странице управления устройствами нажмите **Remote Configuration → System → System Maintenance** («Удаленная конфигурация → Система → Обслуживание системы»), чтобы перейти на соответствующую вкладку.
Импортируйте/экспортируйте файл конфигурации.

Импорт файла конфигурации

Импортируйте файл конфигурации с ПК на устройство.

Примечание

В файле конфигурации содержится информация о параметрах устройства.

Экспорт файла конфигурации

Экспортируйте файл конфигурации с ПК на устройство.

Примечание

В файле конфигурации содержится информация о параметрах устройства.

Обновление

На странице управления устройствами нажмите **Remote Configuration → System → System Maintenance**(«Удаленная конфигурация → Система → Обслуживание системы»), чтобы перейти на соответствующую вкладку.

Выберите тип устройства в раскрывающемся списке, затем нажмите **Browse** («Обзор»), выберите файл обновления на локальном компьютере и нажмите **Upgrade** («Обновить»).

Примечание

- При выборе считывателя карт в качестве типа устройства следует выбрать номер считывателя карт из раскрывающегося списка.
- Обновление длится около 2 минут. Не выключайте устройство во время обновления. После обновления устройство перезагрузится автоматически.

7.12.5 Настройка RS-485

Установите параметры RS-485, в том числе скорость передачи, бит данных, стоповый бит, тип четности, режим связи, режим работы и режим соединения.

Шаги

1. Нажмите **Maintenance and Management → Device** («Обслуживание и управление → Устройство»), чтобы открыть список.
2. Нажмите для перехода на страницу удаленной настройки.
3. Нажмите **System → RS-485 Settings** («Система → Настройки RS-485»), чтобы перейти на вкладку конфигурации RS-485.
4. Из выпадающего списка выберите номер серийного интерфейса, чтобы настроить параметры RS-485.
5. Установите скорость передачи данных, бит данных, стоповый бит, режим связи, режим работы и режим соединения из всплывающего списка.
6. Нажмите **Save** («Сохранить»), чтобы автоматически применить настроенные параметры к устройству.

При

После изменения режима работы устройство перезагрузится. После изменения режима работы появится подсказка.

7.12.6 Настройки режима безопасности

Установите режим безопасности для входа в клиентское ПО.

На странице управления устройствами нажмите **→ System → Security** («Система → Безопасность»), чтобы перейти на соответствующую страницу.

Из всплывающего списка выберите режим безопасности и

нажмите **Save** («Сохранить»). Также можно включить SSH для

повышения уровня безопасности сети.

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.

7.12.7 Настройки параметров сети

Настройте параметры сети устройства, в том числе тип NIC, DHCP и HTTP.

На странице управления устройствами нажмите **→ Network → Network Parameters** («Сеть→ Параметры сети»), чтобы перейти на соответствующую вкладку.

NIC Type («Тип NIC»)

Выберите тип NIC из выпадающего списка Выберите один их предложенных типов: адаптивный, 10M или 100M.

DHCP

При отключении этой функции необходимо вручную установить IPv4-адрес устройства, IPv4-маску подсети, IPv4-шлюз по умолчанию, MTU и порт.

При включении этой функции система автоматически назначит IPv4-адрес устройства,

IPv4-маску подсети, IPv4-шлюз по умолчанию устройства.

HTTP

Установите порт HTTP, адрес сервера DNS1 и адрес сервера DNS2.

7.12.8 Настройки способа уведомления

Установите центральную группу для загрузки журнала по протоколу EHome.

На странице управления устройствами нажмите → **Network** → **Report Strategy** («Сеть→ Способ уведомления»), чтобы перейти на соответствующую вкладку.

Настройте центральную группу для передачи журналов по протоколу EHome. 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.

7.12.9 Настройки параметров сетевого центра

Для передачи данных по протоколу EHome установите центр мониторинга, IP-адрес центра, номер порта, протокол EHome, имя пользователя учетной записи EHome и т. д.

На странице управления устройствами нажмите → **Network** → **Network Center Parameters** («Сеть → Параметры сетевого центра»), чтобы перейти на соответствующую вкладку.

Выберите центр из выпадающего списка.

После включения функции можно назначить тип адреса центра, IP-адрес/имя домена, номер порта, имя пользователя EHome и т. д.

Нажмите **Save** («Сохранить»).

7.12.10 Настройка параметров SIP.

Задайте IP-адрес главной станции и IP-адрес сервера SIP. После настройки параметров можно установить связь между устройством контроля доступа, вызывной панелью, видеодомофоном, пультом консьержа/диспетчера и платформой.

Примечание

Для двусторонней аудиосвязи необходимо, чтобы устройство контроля доступа и другие устройства или системы (такие как вызывная панель, видеодомофон, пульт консьержа/диспетчера, платформа) находились в одном сегменте IP.

Нажмите **Maintenance and Management → Device** («Обслуживание и

управление → Устройство»), чтобы открыть список. Нажмите для перехода на страницу удаленной настройки.

Нажмите **Network → Linked Network Configuration** («Сеть → Конфигурация сети связанных устройств»), чтобы назначить IP-адрес пульта консьержа/диспетчера и IP-адрес SIP-сервера.

Нажмите **Save** («Сохранить»).

7.12.11 Настройка параметров реле

Нажмите **Maintenance and Management → Device** («Обслуживание и управление → Устройство»), чтобы открыть список. Нажмите для перехода на страницу удаленной настройки.

Нажмите **Alarm → Relay** («Тревога → Реле»). Выберите реле и нажмите , чтобы установить наименование реле и время задержки срабатывания. Нажмите **OK** для сохранения настроек.

7.12.12 Настройка параметров управления доступом

Шаги

1. На странице управления устройствами нажмите → **Others → Access Control Parameters** («Другое→ Параметры контроля доступа»), чтобы перейти на соответствующую вкладку.
2. Поставьте галочку **Enable** («Включить») для включения соответствующей функции.

   Голосовое предупреждение

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

   Загрузка изображений после захвата

   Если функция активирована, захваченные изображения будут отправлены в клиентское ПО.

   Сохранение захваченных изображений

   Если функция активирована, захваченные изображения будут сохранены.

   Только измерение температуры

   При включении функции устройство будет только измерять температуру без аутентификации разрешений. При выключении этой функции устройство аутентифицирует разрешения и одновременно измеряет температуру.

   Захват изображений с подсветкой белым светом

   Если функция активирована, изображения, захваченные камерой с подсветкой белым светом, будут загружены на платформу. Если функция отключена, устройство будет загружать на платформу только изображения, захваченные тепловизионной камерой.

   Не открывать дверь, если измеренная температура оказывается выше/ниже порогового значения

   При включении этой функции дверь остается закрытой, когда обнаруженная температура оказывается выше или ниже настроенного порогового значения температуры. Функция измерения температуры активирована по умолчанию.

Обязательное наличие маски

После включения этой функции устройство запрещает проход при отсутствии маски.

Тревога превышения порогового значения температуры

Настройте пороговое значение в соответствии с фактической ситуацией. При обнаружении температуры выше или ниже настроенных параметров срабатывает сигнал тревоги. Значение должно находиться в диапазоне от 35.1 до 44.9 ℃.

3. Нажмите **Save** («Сохранить»).

7.12.13 Настройка параметров терминала доступа с функцией распознавания лиц

Нажмите **Maintenance and Management → Device** («Обслуживание и управление → Устройство»), чтобы открыть список. Нажмите **CTRL** и выберите для перехода на страницу удаленной настройки.

Нажмите **Other → Face Recognition Terminal Parameters** («Другое → Параметры терминала доступа с функцией распознавания лиц») для настройки параметров устройства.

База данных изображений лиц

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

Сохранение изображений лиц, захваченных при аутентификации

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

Считывание CPU-карты

Выберите функцию считывания номера карты или файла.

Рабочий режим

Установите режим работы устройства: **Normal Mode** («Обычный режим»). Для получения доступа необходимо пройти аутентификацию с использованием учетных данных.

ЭКО-режим

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

Режим ЭКО (1:1)

Установка порога опознавания при аутентификации в режиме ЭКО 1:1. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания.

Режим ЭКО (1:N)

Установка порога опознавания при аутентификации в режиме ЭКО 1:N. Чем больше данное значение, тем меньше будет ложных срабатываний, и тем больше будет вероятность отклонения ложного опознавания.

Пороговое значение ЭКО-режима

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

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

7.12.14 Настройка параметров изображений лиц

Шаги

1. Нажмите **Maintenance and Management → Device** («Обслуживание и управление → Устройство»), чтобы открыть список.
2. Нажмите для перехода на страницу удаленной настройки.
3. Нажмите **Other → Face Picture Parameters** («Другое → Параметры изображений лиц») для настройки параметров изображений лиц.

Pitch Angle («Угол наклона»)

Максимальный угол наклона при запуске аутентификации лица.

Yaw Angle («Угол отклонения»)

Максимальный угол отклонения при запуске аутентификации лица.

Margin (Left) («Граница (слева)»)

Расстояние от левого края лица до левого края области распознавания.

Чтобы произвести опознавание лица, фактическое расстояние должно быть больше, чем заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.

Margin (Right) («Граница (справа)»)

Расстояние от правого края лица до правого края области распознавания.

Чтобы произвести опознавание лица, фактическое расстояние должно быть больше, чем заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.

Margin (Top) («Граница (сверху)»)

Расстояние от верхнего края лица до верхнего края области распознавания.

Чтобы произвести опознавание лица, фактическое расстояние должно быть больше, чем заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.

Margin (Bottom) («Граница (снизу)»)

Расстояние от нижнего края лица до нижнего края области распознавания.

Чтобы произвести опознавание лица, фактическое расстояние должно быть больше, чем заданное значение. Другие процентные значения, расстояния и углы также должны соответствовать заданным условиям.

Pupillary distance («Межзрачковое расстояние»)

Минимальное разрешение между двумя зрачками при

распознавания лица. Фактическое разрешение должно быть выше,

чем заданное значение.

Score («Степень соответствия»)

Устройство оценивает захваченное изображение в соответствии с углом отклонения, углом наклона и межзрачковым расстоянием. Если оценка будет меньше заданного значения, распознавание лица считается неудачным.

Настройте параметры изображений лиц перед аутентификацией.

4. Нажмите **Save** («Сохранить»).

7.12.15 Конфигурация параметров дополнительной подсветки

Можно включить или выключить дополнительную подсветку. Также можно настроить яркость дополнительной подсветки.

Шаги

1. Нажмите **Maintenance and Management → Device** («Обслуживание и управление → Устройство»), чтобы открыть список.
2. Нажмите для перехода на страницу удаленной настройки.
3. Нажмите **Other →Supplement Light Parameters** («Другое → Параметры дополнительной подсветки») для настройки параметров дополнительной подсветки.
4. Выберите тип дополнительной подсветки из выпадающего списка.
5. Выберите режим дополнительной подсветки из выпадающего списка.
6. **Опционально:** Настройте яркость дополнительной подсветки.
7. Нажмите **Save** («Сохранить») для сохранения настроек.

7.12.16 Назначение номера устройства

Выберите тип устройства, номер микрорайона, номер здания, номер этажа, номер отдела и номер комнаты. Нажмите **Maintenance and Management → Device** («Обслуживание и управление → Устройство»), чтобы открыть список устройств.

Нажмите для перехода на страницу удаленной настройки.

Нажмите **Other → No. Settings** («Другое → Настройки номера») и выберите тип устройства, номер микрорайона, номер здания, номер этажа, номер отдела и номер комнаты.

7.12.17 Настройка параметров аудио/видео

Настройте качество изображения, разрешение изображения и другие параметры камеры устройства.

Шаги

1. Нажмите **Maintenance and Management → Device** («Обслуживание и управление → Устройство»), чтобы открыть список.
2. Нажмите для перехода на страницу удаленной настройки.
3. Нажмите **Image → Video & Audio** («Изображение → Видео и аудио») для перехода на страницу настроек.
4. Настройте параметры камеры устройства, в том числе тип потока, тип битрейта, качество видео, частоту кадров, тип кодирования звука, тип видео, битрейт, разрешение и интервал I-кадра.
5. Нажмите **Save** («Сохранить»).

7.12.18 Настройка входной и выходной громкости

Шаги

1. На странице управления устройствами нажмите → **Image → Audio Input or Output** («Изображение → Аудиовход и аудиовыход»), чтобы перейти на соответствующую страницу.

2. Передвигайте курсор для настройки входной и выходной громкости устройства.
3. Нажмите **Save** («Сохранить»).

7.12.19 Управление реле

Шаги

1. Нажмите **Maintenance and Management → Device** («Обслуживание и управление → Устройство»), чтобы открыть список.
2. Нажмите для перехода на страницу удаленной настройки.
3. Нажмите **Operation → Relay** («Управление → Реле»).
4. Включите/выключите реле.

7.12.20 Просмотр статуса реле

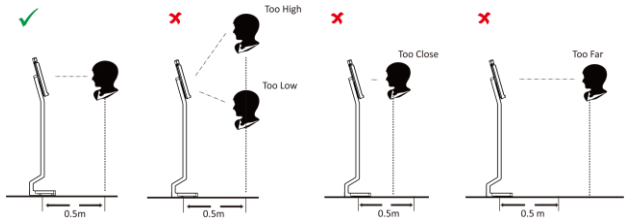
Нажмите **Maintenance and Management → Device** («Обслуживание и управление → Устройство»), чтобы открыть список. Нажмите **CTRL** и выберите для перехода на страницу удаленной настройки.

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

Приложение A. Советы по сбору/сравнению изображений лиц

Положение головы при сборе или сравнении изображения лица:

Положения (Рекомендуемое расстояние: 0.5 м)



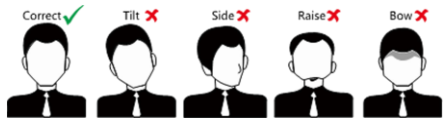
Выражение лица

- 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.

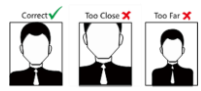
Положение лица

Для получения качественного и точного изображения лица, смотрите прямо в камеру при сборе или сравнении изображений лиц.



Размер

Убедитесь, что лицо находится в середине окна сбора данных.



Приложение B. Советы в отношении рабочей среды на месте установки оборудования

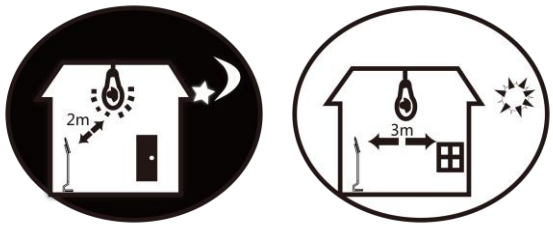
1. Номинальное значение освещенности источника света

Свеча: 10 лк

Лампа: 100 ~ 850 лк

Солнечный свет: свыше 1200 лк

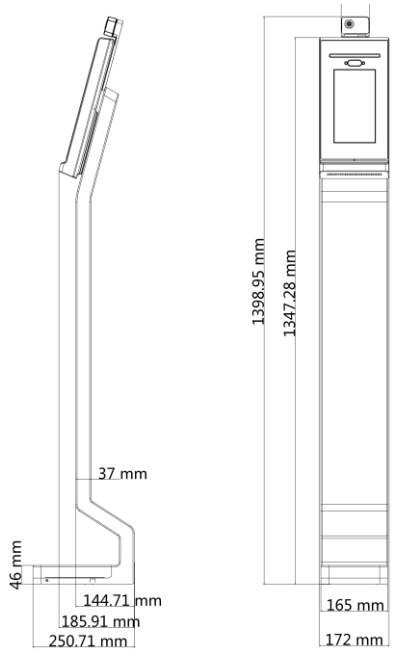
2. I При установке устройства в помещении устройство должно находиться на расстоянии не менее 2 метров от источника света и не менее 3 метров от окна или двери.



3.Избегайте засветки, а также воздействия прямых и отраженных солнечных лучей.

Английский язык	**Русский язык**
Backlight	Засветка
Direct sunlight	Прямые солнечные лучи
Indirect sunlight through window	Непрямые солнечные лучи, попадающие через окно
Direct sunlight through window	Прямые солнечные лучи, попадающие через окно
Close to light	Близко к свету

Приложение C. Размеры




See Far, Go Further