



Терминал доступа F-KD-2502

Руководство пользователя

Условные обозначения

В настоящем документе используются следующие символы.

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

Регулирующая информация

Информация о FCC

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

Соответствие FCC: это оборудование прошло испытания и соответствует регламенту для цифрового устройства класса В, 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 регламенту для цифрового устройства применительно к 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 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/ЕС (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».

Предупреждение: игнорирование предупреждений может привести к тяжелым травмам или смерти.

Предостережение: игнорирование любого из предостережений может привести к травмам или порче оборудования.

	
Предупреждение: следуйте данным правилам для предотвращения серьезных травм и смертельных случаев.	Предостережение: следуйте мерам предосторожности, чтобы предотвратить возможные повреждения или материальный ущерб.

Предупреждение

- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в регионе эксплуатации.
- Используйте адаптер питания соответствующей компании. Потребляемая мощность не может быть меньше требуемого значения.
- Не подключайте несколько устройств к одному блоку питания, перегрузка адаптера может привести к перегреву или возгоранию.
- Прежде чем подключать, устанавливать или разбирать устройство, убедитесь, что питание отключено.
- Если устройство устанавливается на потолок или стену, убедитесь, что оно надежно закреплено.
- Если из устройства идет дым или доносится шум — отключите питание, извлеките кабель и свяжитесь с сервисным центром.
- 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. (Компания не несет ответственность за проблемы, вызванные несанкционированным ремонтом или техническим обслуживанием.)

Предостережение

- Данное оборудование не подходит для использования в местах, где могут присутствовать дети.
- Запрещено ронять устройство и подвергать воздействию сильных электромагнитных помех. Избегайте установки устройства на вибрирующую поверхность или в местах, подверженных ударам (пренебрежение этим предостережением может привести к повреждению устройства).
- Запрещено размещать устройство в местах с чрезвычайно высокой или низкой температурой окружающей среды (подробная информация о рабочей температуре представлена в спецификации устройства), в пыльной или влажной среде, запрещено подвергать устройство воздействию сильных электромагнитных помех.
- Не подвергайте крышку устройства, предназначенного для использования внутри помещения, воздействию дождя или влаги.
- Не подвергайте устройство воздействию прямых солнечных лучей, не устанавливайте в местах с плохой вентиляцией или рядом с источником тепла таким, как обогреватель или радиатор (пренебрежение этим предостережением может привести к пожару).
- Запрещено направлять устройство на солнце или очень яркие источники света. Яркий свет может вызвать размытие или потерю четкости изображения (что не является признаком неисправности), а также повлиять на срок службы матрицы.
- Используйте прилагаемую перчатку во время демонтажа крышки устройства, избегайте прямого контакта с крышкой устройства, так как пот и жир с пальцев могут стать причиной разрушения защитного покрытия на поверхности устройства.
- Для очистки внутренних и внешних поверхностей крышки устройства используйте мягкую и сухую ткань, не используйте щелочные моющие средства.
- Сохраните упаковку после распаковки для использования в будущем. В случае сбоя работы устройство необходимо вернуть на завод (с оригинальной упаковкой). Транспортировка без оригинальной упаковки может привести к повреждению устройства и к дополнительным расходам.
- Неправильное использование или замена батареи может привести к опасности взрыва. Проводите замену на такие же батареи или аналогичные. Утилизируйте использованные батареи в соответствии с инструкциями, предоставленными производителем батарей.

Доступные модели

Доступны следующие модели терминала доступа с функцией считывания отпечатков:

Наименование	Продукт	Беспроводное соединение
Терминал доступа	С функцией распознавания отпечатков пальцев	Частота считывания карт 13.56 МГц, Wi-Fi, 2.4G, Bluetooth
	Без функции распознавания отпечатков пальцев	Частота считывания карт 13.56 МГц, Wi-Fi, 2.4G, Bluetooth

Таблица 1-1 Доступные веб-интерфейсы мобильного телефона

Операционная	Браузер	Версия	Доступность
Android	Xiaomi 12, браузер по умолчанию	16.6.6	Да
	Huawei P30, браузер по умолчанию	12.1.1.321	Да
	Xiaomi 5s plus, браузер по умолчанию	14.2.22	Да
	Huawei P30 Pro, браузер по умолчанию	12.1.2.301	Да
	Redmi k40, браузер по умолчанию	16.5.12	Да
iOS	Safari	15.4	Да

Содержание

Раздел 1 Представление продукта	1
Раздел 2 Функции	2
Раздел 3 Описание внешнего вида	3
Раздел 4 Установка	4
4.1 Среда установки.....	4
4.2 Установка без монтажной коробки.....	4
Раздел 5 Подключение устройства	6
5.1 Описание разъемов.....	6
5.2 Подключение внешних устройств	8
5.3 Подключение к модулю безопасности двери	8
Раздел 6. Активация	10
6.1 Активация через веб-интерфейс	10
6.2 Активация устройства при помощи клиентского ПО iVMS-4200	10
Раздел 7 Работа через веб-интерфейс.....	12
7.1 Вход в систему	12
7.2 Забыли пароль	12
7.3 Просмотр в режиме реального времени.....	12
7.4 Управление сотрудниками / посетителями	14
7.5 Поиск событий	15
7.6 Управление устройством	16
7.7 Настройка	16
7.7.1 Настройка локальных параметров.....	16
7.7.2 Просмотр информации об устройстве	17
7.7.3 Настройка времени	17
7.7.4 Настройка перехода на летнее время (DST)	18
7.7.5 Просмотр лицензии на ПО с открытым исходным кодом	18

7.7.6	Обновление и техническое обслуживание.....	18
7.7.7	Управление записями в журналах	19
7.7.8	Настройки режима безопасности	20
7.7.9	Управление сертификатами	20
7.7.10	Изменение пароля администратора.....	21
7.7.11	Просмотр информации о постановке / снятии с охраны	22
7.7.12	Онлайн пользователи.....	22
7.7.13	Настройка параметров сети	22
7.7.14	Настройка параметров видео и аудио.....	26
7.7.15	Настройка параметров изображения	27
7.7.16	Привязка события	28
7.7.17	Настройка основных параметров.....	29
7.7.18	Настройки контроля доступа Настройка параметров двери	32
7.7.19	Настройка видеодомофонии	36
7.7.20	Настройка основных параметров.....	38
Раздел 8 Настройка устройства через мобильный интерфейс		39
8.1	Вход в систему	39
8.2	Поиск событий	39
8.3	Управление пользователями	39
8.4	Настройка	41
8.4.1	Просмотр информации об устройстве	41
8.4.2	Настройка времени	41
8.4.3	Настройка перехода на летнее время (DST)	42
8.4.4	Просмотр лицензии на ПО с открытым исходным кодом	43
8.4.5	Управление пользователями	43
8.4.6	Обновление и техническое обслуживание.....	43
8.4.7	Настройки безопасности	44
8.4.8	Настройка параметров сети	44

8.4.9	Настройка основных параметров.....	47
8.4.10	Настройки параметров лица	51
8.4.11	Настройки видеодомофонии	52
8.4.12	Настройки параметров контроля доступа	53
8.5	Операции для двери	56
Раздел 9	Настройка клиентского ПО.....	57
9.1	Схема настройки клиентского ПО.....	57
9.2	Управление устройством	59
9.2.1	Добавление устройства	59
9.2.2	Сброс пароля устройства	62
9.2.3	Управление добавленными устройствами	63
9.3	Управление группами	63
9.3.1	Добавление группы	64
9.3.2	Добавление ресурсов в группу.....	64
9.4	Управление сотрудниками / посетителями	65
9.4.1	Добавление организации.....	65
9.4.2	Настройка основной информации	65
9.4.3	Выпуск карт в локальном режиме	67
9.4.4	Сбор отпечатков пальцев с помощью клиента	68
9.4.5	Сбор отпечатков пальцев с помощью устройства контроля доступа	69
9.4.6	Настройка информации по контролю доступа	70
9.4.7	Редактирование информации о сотруднике / посетителе	72
9.4.8	Настройка дополнительной информации	72
9.4.9	Импорт и экспорт информации о сотруднике / посетителе	73
9.4.10	Импорт информации о сотруднике / посетителе.....	73
9.4.11	Экспорт информации о сотруднике / посетителе	74
9.4.12	Получение информации о пользователе с устройства контроля доступа	74
9.4.13	Перемещение пользователя в другую организацию	75

9.4.14	Выдача карт сотрудникам в пакетном режиме	75
9.4.15	Рапорт о потере карты	76
9.4.16	Настройка параметров выпуска карт	76
9.5	Настройка графиков и шаблонов	77
9.5.1	Добавление выходного дня	77
9.5.2	Добавление шаблона	78
9.6	Настройка группы контроля доступа для назначения разрешений на доступ	79
9.7	Настройка расширенных функций	81
9.7.1	Настройка параметров устройства	81
9.7.2	Настройка состояния двери «оставить заблокированной» / «разблокированной»	86
9.7.3	Настройка правила Wiegand.....	101
9.7.4	Настройка аутентификации при помощи считывателя карт	102
9.7.5	Настройка параметров устройства	104
9.8	Настройка привязанных действий	107
9.8.1	Настройка действий на клиентском ПО при событии доступа	108
9.8.2	Настройка действий устройства при событии доступа	108
9.8.3	Настройка действий устройства при считывании карт.....	109
9.8.4	Настройка действий устройства для идентификатора пользователя	110
9.9	Управление состоянием двери.....	111
9.9.1	Управление состоянием двери	111
9.9.2	Запись информации о считывании карт в режиме реального времени	112
Приложение А. Советы по сканированию отпечатков пальцев		113
Приложение В. Размеры		114

Раздел 1 Представление продукта

Терминал доступа является терминалом доступа с функцией распознавания лиц для аутентификации. Устройство поддерживает двустороннюю аудиосвязь, удаленный просмотр в режиме реального времени, захват изображений лиц, запись видео через NVR и т. д.

Раздел 2 Функции

- Управление системой контроля доступа, видеодомофонии и видеонаблюдения с помощью одного устройства
- Степень защиты IP65 и IK09; надежная конструкция из алюминиевого сплава
- Поддержка нескольких режимов аутентификации: аутентификация по отпечаткам пальцев, карте и т. д.



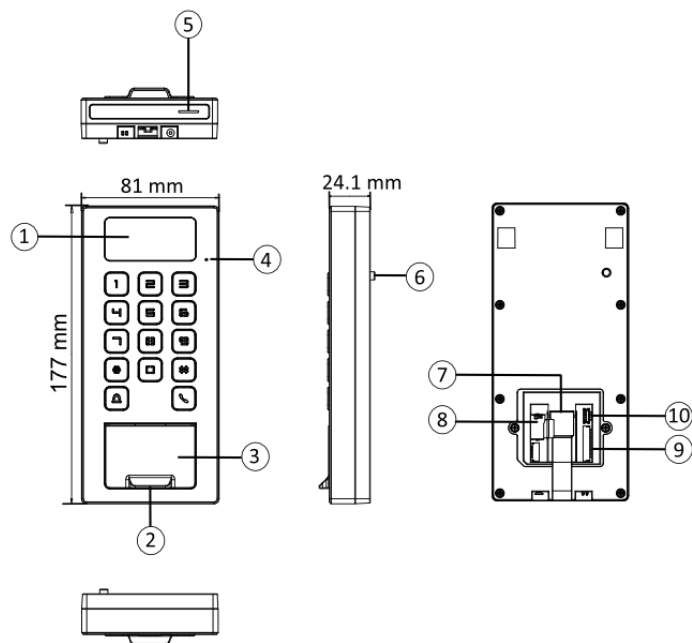
Примечание

Некоторые модели устройства поддерживают функцию считывания отпечатков пальцев.

- Дистанционное управление через мобильное приложение Guarding Vision
- Подключение к внешнему контроллеру доступа по протоколу Wiegand
- Двусторонняя аудиосвязь по протоколу SIP 2.0
- Интерфейс связи RS-485 для подключения внешнего считывателя карт

Раздел 3 Описание внешнего вида

Ниже представлено описание внешнего вида устройства.



Примечание

Указанные изображения представлены исключительно в справочных целях.

Таблица 3-1 Описание внешнего вида

№	Описание
1	Камера (поддерживают некоторые модели устройств)
2	Модуль считывания отпечатков пальцев (поддерживают некоторые модели устройств)
3	Область считывания карт
4	Микрофон
5	Динамик
6	Детектор саботажа
7	Сетевой интерфейс
8	Слот для SD-карты
9	Разъем
10	Служебный порт (только для отладки)

Раздел 4 Установка

4.1 Среда установки

- При установке устройство необходимо разместить на расстоянии не менее 2 метров от источника света и не менее 3 метров от окна или двери.
- Убедитесь, что уровень освещения окружающей среды составляет более 100 лк.



Примечание

Подробная информация представлена в разделе ***Рекомендации по среде установки.***

4.2 Установка без монтажной коробки

Шаги



Примечание

Дополнительная сила должна быть в три раза больше веса оборудования. Устройство и его соответствующая монтажная плата должны быть закреплены во время установки. После установки оборудование, включая любую соответствующую монтажную плату, не должно быть повреждено.

1. Закрепите монтажную плату на стене с помощью 4 прилагаемых винтов.

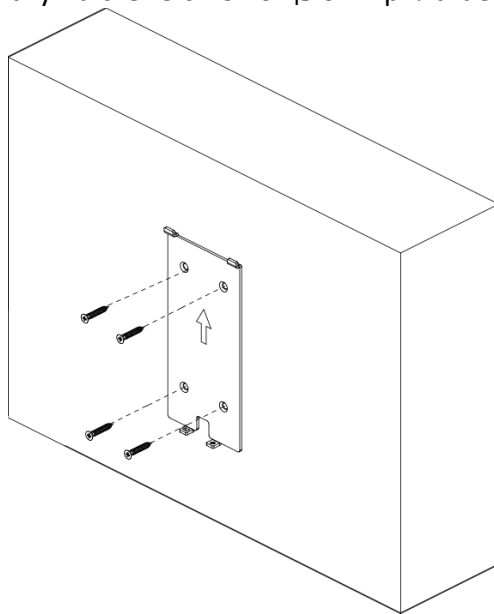
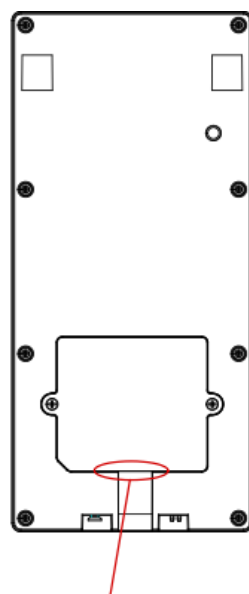


Рисунок 4-1 Закрепление монтажной платы

2. Проложите кабели через отверстие для кабеля на монтажной плате и подключите кабели внешних устройств к разъемам.
3. Нанесите силиконовый герметик на стыки между задней панелью устройства и стеной (кроме нижней стороны), чтобы предотвратить попадание воды в отверстия.



Apply
Silicone
Sealant

Рисунок 4-2 Нанесение силиконового герметика

4. Совместите устройство с монтажной платой и закрепите на монтажной плате с помощью 1 прилагаемого винта.

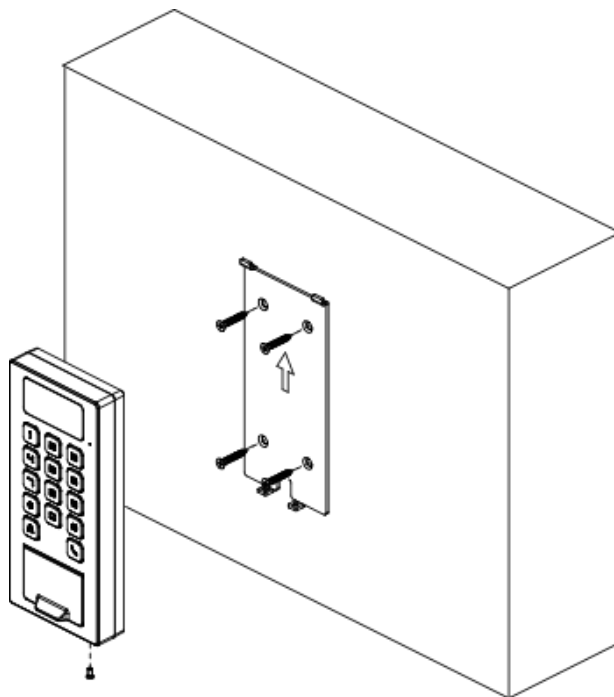


Рисунок 4-3 Закрепление устройства

Раздел 5 Подключение устройства

5.1 Описание разъемов

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

Ниже представлена схема подключения терминала:

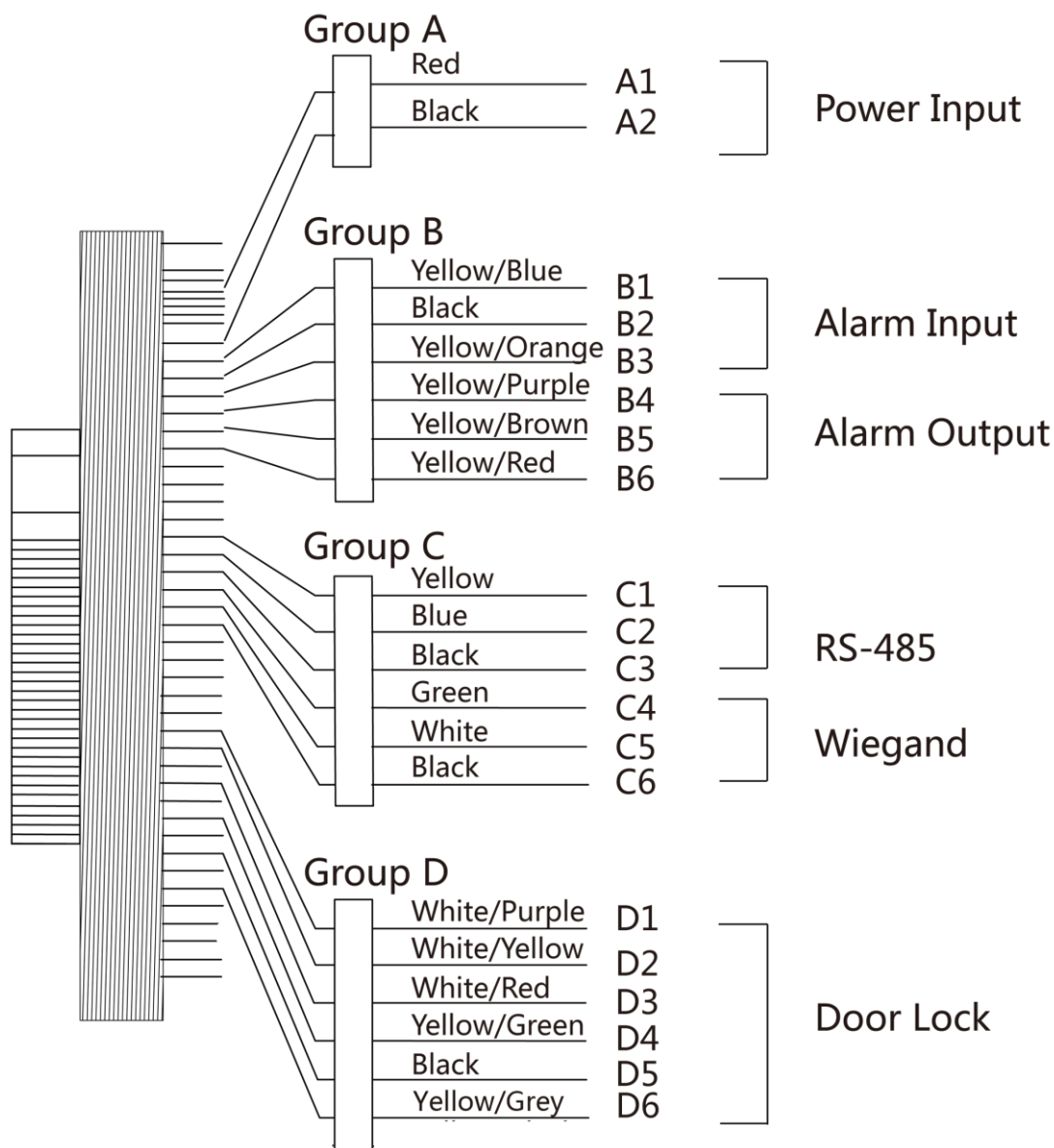


Рисунок 5-1 Схема разъемов

Терминал оснащен следующими разъемами:

Таблица 5-1 Описание разъемов

Группа	№	Функция	Цвет	Название	Описание
Группа А	A1	Вход питания	Красный	+12 В	Питание DC 12 В
	A2		Черный	GND	Заземление
Группа В	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	Подключение тревожного выхода
	B5		Желто-коричневый	COM	
	B6		Желто-красный	NO	
Группа С	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	Белый / фиолетовый	NC	Подключение замка (нормально замкнутый)
	D2		Белый / желтый	COM	Обычный
	D3		Белый / красный	NO	Подключение замка (нормально разомкнутый)
	D4		Желтый / зеленый	Датчик	Дверной контакт
	D5		Черный	GND	Заземление
	D6		Желтый / серый	BTN	Подключение выходной двери

5.2 Подключение внешних устройств

Подключение внешнего устройства.

Ниже представлена схема подключения.

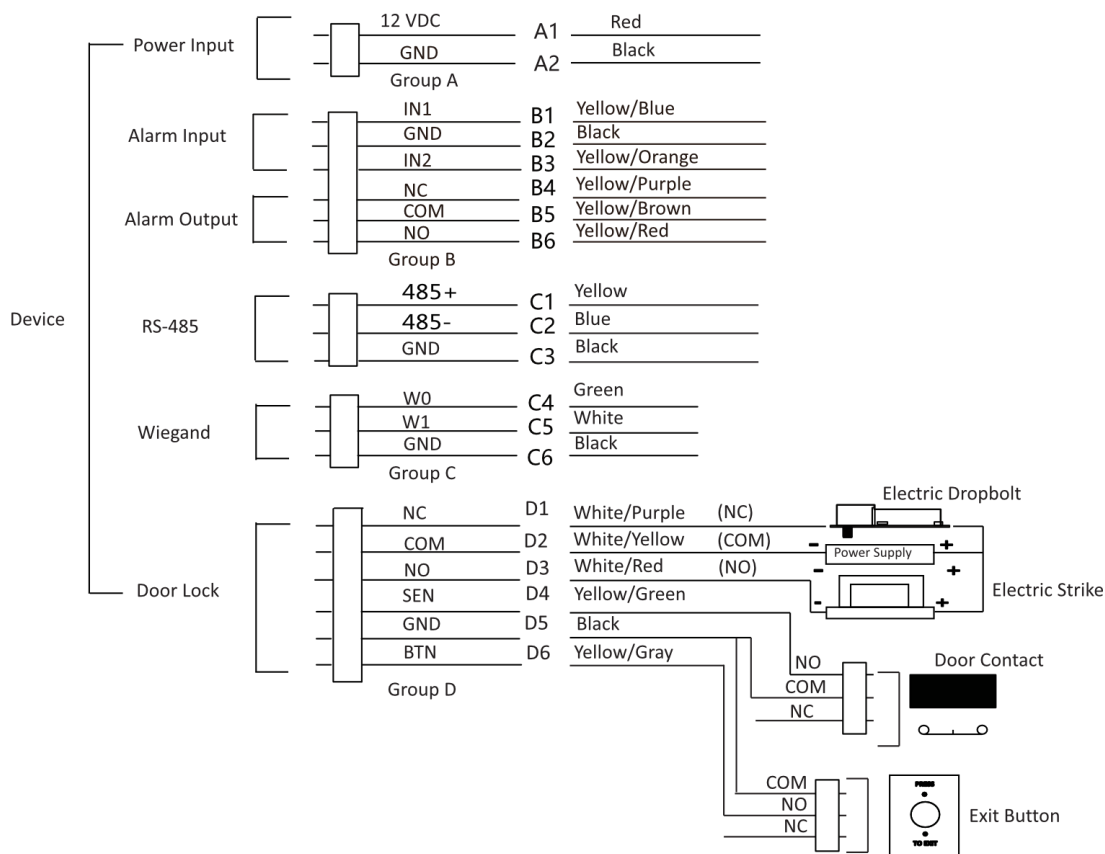


Рисунок 5-2 Подключение внешних устройств

5.3 Подключение к модулю безопасности двери

Также терминал можно подключить к модулю безопасности двери. Ниже представлена схема подключения.

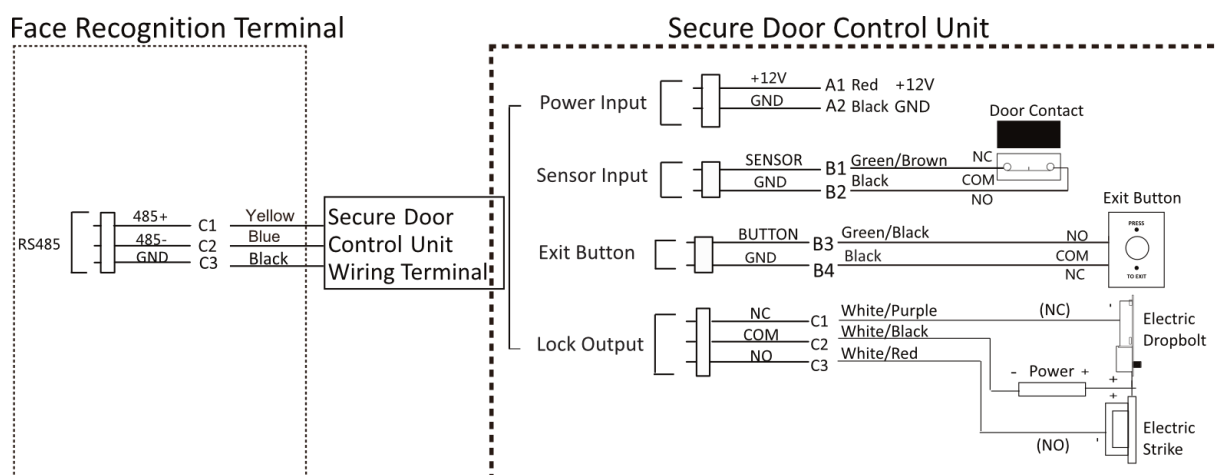


Рисунок 5-3 Подключение к модулю безопасности двери



Примечание

- Модуль безопасности двери необходимо отдельно подключать к внешнему источнику питания. Рекомендуемые параметры внешнего источника питания составляют 12 В, 0.5 А.
 - Для сценариев с высокими требованиями к безопасности в первую очередь необходимо подключиться к модулю безопасности двери.
 - Свяжитесь с отделом технической поддержки для приобретения модуля безопасности двери отдельно.
 - На рисунке представлены детали подключения. Подробная информация представлена в руководстве пользователя модуля безопасности двери.
-

Раздел 6. Активация

Перед первым входом в систему необходимо активировать устройство. После включения устройства система переключится на страницу активации устройства.

Поддерживается активация через устройство, через ПО SADP и клиентское ПО. Значения по умолчанию для устройства следующие:

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

6.1 Активация через веб-интерфейс

Можно активировать устройство через веб-интерфейс.

Шаги

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

Enter.



Примечание

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

2. Создайте 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 сделать использование продукта безопасным.



Примечание

Символы содержащие admin и nimda не могут быть использованы для активации пароля.

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

6.2 Активация устройства при помощи клиентского ПО iVMS-4200

Для исправной работы некоторых устройств необходимо создать пароль активации, прежде чем добавлять их в систему iVMS-4200.

Шаги

Примечание

Эта функция должна поддерживаться устройством.

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



Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

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



Примечание

Символы содержащие admin и nimda не могут быть использованы для активации пароля.

7. Для активации устройства нажмите **ОК**.

Раздел 7 Работа через веб-интерфейс

7.1 Вход в систему

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



Примечание

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

Вход в систему через веб-интерфейс

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

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

Вход в систему через удаленную настройку клиентского ПО

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

7.2 Забыли пароль

Если вы забыли пароль при входе в систему, пароль можно поменять с помощью адреса электронной почты или контрольных вопросов.

На странице входа в систему нажмите **Forget Password** («Забыли пароль»).

Выберите **Verification Mode** («Режим проверки»).

Security Question Verification («Проверка по контрольным вопросам»)

Ответьте на контрольные вопросы.

E-E-mail Verification («Подтверждение по электронной почте»)

1. Экспортируйте QR-код и отправьте его на адрес сервера электронной почты во вложении.
 2. Проверочный код будет отправлен на зарезервированный адрес электронной почты в течение 5 минут.
 3. Введите проверочный код в поле проверочного кода для подтверждения идентификации.
- Создайте новый пароль и подтвердите его.

7.3 Просмотр в режиме реального времени

Можно просматривать видео в режиме реального времени.

После входа в систему вы попадете на страницу просмотра в режиме реального времени.

Можно выполнять просмотр в режиме реального времени, захват, запись видео и другие операции.

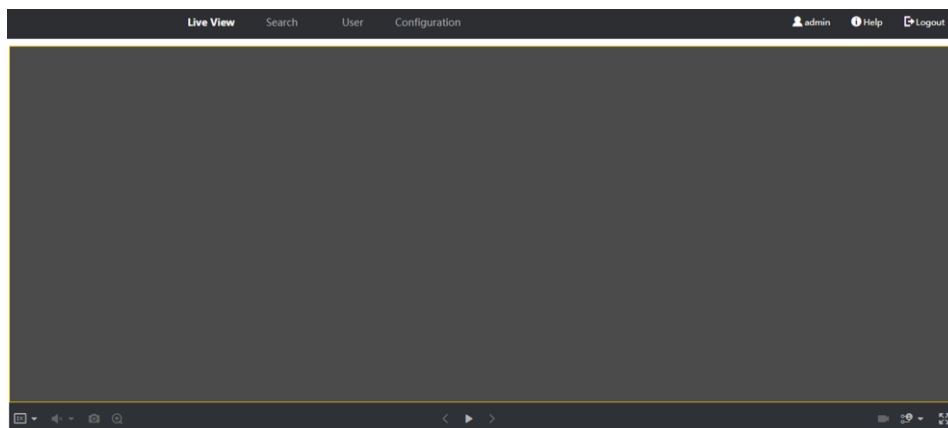


Рисунок 7-1. Страница просмотра в режиме реального времени

Описание функций:



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



При запуске просмотра в режиме реального времени необходимо настроить громкость



Примечание

При настройке громкости во время двусторонней аудиосвязи можно услышать эхо.



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



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



Поговорите с устройством.



Разблокировка подключенной двери.



Начало или остановка просмотра в режиме реального времени.



Начало или остановка записи видео.



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



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



Полноэкранный просмотр.

7.4 Управление сотрудниками / посетителями

Можно добавить информацию о сотруднике / посетителе, в том числе основную информацию, карту, режим аутентификации и отпечатки пальцев. Также можно редактировать информацию о пользователе и искать информацию о пользователе в списке пользователей.

Добавление основной информации

Нажмите **User → Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Добавьте основную информацию о сотруднике / посетителе, включая идентификатор, Ф. И. О., пол и роль пользователя.

При выборе роли пользователя **Visitor** («Посетитель») можно установить время посещений.

Нажмите **OK** для сохранения настроек.

Установка времени разрешения

Нажмите **User → Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Установите **Start Time** («Время начала») и **End Time** («Время окончания») и сотрудник / посетитель будет иметь доступ в течение заданного периода времени.

Нажмите **OK** для сохранения настроек.

Настройка контроля доступа

Нажмите **User → Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

В поле **Access Control** («Контроль доступа») выберите **Administrator** («Администратор»), и добавленный сотрудник / посетитель может войти в систему посредством аутентификации.

Нажмите **OK** для сохранения настроек.

Настройка номера помещения

Нажмите **User → Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя. Нажмите **Add** («Добавить»), чтобы добавить **Floor No.** («Номер этажа») и **Room No.** («Номер комнаты»). Нажмите  для удаления.

Нажмите **OK** для сохранения настроек.

Добавление режима аутентификации

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

Нажмите **OK** для сохранения настроек.

Добавление карты

Нажмите **User → Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Нажмите **Add Card** («Добавление карты»), введите **Card No.** («Номер карты») и выберите **Property** («свойство»), нажмите **OK**, чтобы добавить карту. Нажмите **OK** для сохранения настроек.

Добавление отпечатка пальца

Примечание

Только устройства с поддержкой функции считывания отпечатков пальцев могут добавлять считывание отпечатков пальцев.

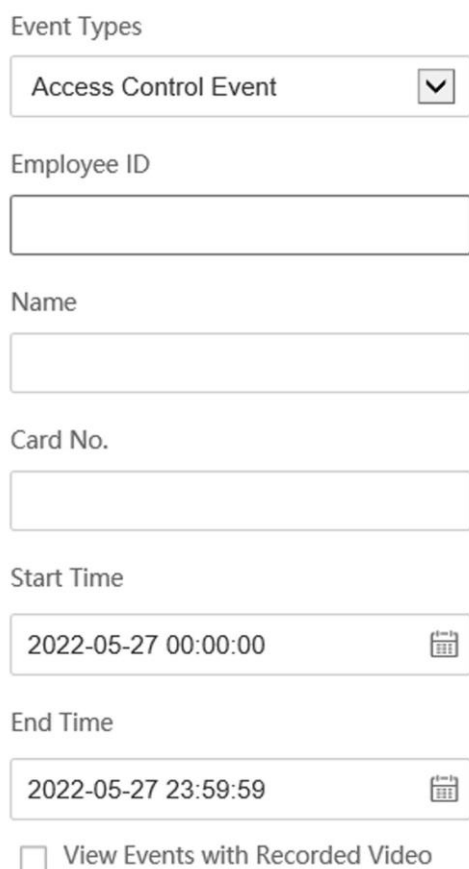
Нажмите **User → Add** («Пользователь → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Нажмите **Add Fingerprint** («Добавить отпечатки пальцев») и нажмите пальцем на модуль отпечатков пальцев устройства, чтобы добавить свой отпечаток пальца.

Нажмите **Complete** («Завершить») для сохранения настроек.

7.5 Поиск событий

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



The screenshot shows a search form with the following fields and controls:

- Event Types:** A dropdown menu currently showing "Access Control Event" with a downward arrow icon.
- Employee ID:** An empty text input field.
- Name:** An empty text input field.
- Card No.:** An empty text input field.
- Start Time:** A date and time picker showing "2022-05-27 00:00:00" with a calendar icon.
- End Time:** A date and time picker showing "2022-05-27 23:59:59" with a calendar icon.
- View Events with Recorded Video:** A checkbox that is currently unchecked.

Рисунок 7-2 Поиск событий

Введите условия поиска, включая идентификатор сотрудника / посетителя, имя, номер карты, время начала и время окончания доступа и нажмите **Search** («Поиск»).

Для просмотра событий с помощью записанных видео, нажмите **View Events with Recorded Video** («Просмотреть события с помощью записанного видео»).

• REC

Видео записывается.

•

Воспроизведение записанного видео.

•

Просмотр захваченного изображения.

После этого на панели справа появятся результаты поиска.

7.6 Управление устройством

Возможность управления подключенными устройствами с определенной страницы.

Шаги

1. Нажмите **Device Management** («Управление устройством») для перехода на страницу настроек.



Рисунок 7-3 Управление устройством

2. Нажмите **Add** («Добавить»), чтобы добавить видеодомофон или дополнительную вызывную панель. Введите параметры и нажмите ОК, чтобы добавить.
3. Нажмите **Import** («Импорт»). Введите информацию об устройстве в шаблон для импорта устройств в пакетном режиме.
4. Нажмите **Export** («Экспорт»), чтобы экспортировать данные на компьютер.
5. Выберите устройство и нажмите **Delete** («Удалить») для удаления выбранного устройства из списка.
6. Нажмите **Refresh** («Обновить») для получения информации об устройстве.
7. **Опционально:** настройка информации об устройстве.

Edit Device Information

(«Редактирование информации об устройстве»)

Нажмите  для редактирования информации об устройстве.

Delete Device Information

(«Удаление информации об устройстве»)

Нажмите  для удаления информации об устройстве из списка.

Search Devices («Поиск устройств»)

Выберите **Status** («Состояние») и **Device Type** («Тип устройства») для поиска устройств.

7.7 Настройка

7.7.1 Настройка локальных параметров

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

Настройка параметров просмотра в режиме реального времени

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

Настройка пути сохранения файлов записи

Нажмите **Configuration** → **Local** («Настройки → Локальные») для перехода на соответствующую страницу. Выберите размер файла записи, путь для сохранения на локальном компьютере и нажмите **Save** («Сохранить»).

Также можно нажать **Open** («Открыть»), чтобы открыть папку с файлами и просмотреть подробную информацию.

Настройка пути сохранения захваченных изображений

Нажмите **Configuration** → **Local** («Настройки → Локальные») для перехода на соответствующую страницу. Выберите путь для сохранения на локальном компьютере и нажмите **Save** («Сохранить»).

Также можно нажать **Open** («Открыть»), чтобы открыть папку с файлами и просмотреть подробную информацию.

7.7.2 Просмотр информации об устройстве

Просмотр названия устройства, имени Bluetooth, языка, модели, серийного номера, QR-кода, версии, числа каналов, номера интерфейса входа, номера интерфейса выхода, локального RS-485, номера регистрации, числа тревожных выходов, емкости устройства и т. д.

Нажмите **Configuration** → **System** → **System Settings** → **Basic Information** («Настройки → Система → Настройка системы → Основная информация»), чтобы перейти на соответствующую страницу.

Можно посмотреть название устройства, имя Bluetooth, язык, модель, серийный номер, QR-код, версию, число каналов, номер интерфейса входа, номер интерфейса выхода, локальный RS-485, номер регистрации, число тревожных выходов, емкость устройства и т. д.

7.7.3 Настройка времени

Установите часовой пояс, режим синхронизации, тип центра тревог, адрес сервера, порт NTP и интервал.

Нажмите **Configuration** → **System** → **System Settings** → **Time Settings** («Настройки → Система → Настройки системы → Настройки времени»).

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Timing mode ☒ NTP ☐ Manual

Alarm Receiver Type IPv4

Server Address 10.41.0.42

NTP Port 123

Interval 60 minute(s)

Save

Рисунок 7-4 Настройка времени

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

Time Zone («Часовой пояс»)

Выберите часовой пояс устройства из выпадающего списка.

Time Sync. («Синхронизация времени»)

NTP

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

Manual («Вручную»)

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

Server Address Type/Server Address/NTP Port/Interval («Тип адреса сервера / Адрес сервера / Порт NTP / Интервал»)

Здесь можно настроить тип адреса сервера, адрес сервера, порт NTP, интервал.

7.7.4 Настройка перехода на летнее время (DST)

Шаги

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

Enable DST ☒

Start Time: Apr, First, Sun, 02

End Time: Oct, Last, Sun, 02

DST Bias: 30minute(s)

Save

Рисунок 7-5 Страница DST

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

7.7.5 Просмотр лицензии на ПО с открытым исходным кодом

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

7.7.6 Обновление и техническое обслуживание

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

Перезагрузка устройства

Нажмите **Configuration → System → Maintenance → Upgrade & Maintenance** («Настройки → Система → Обслуживание → Обновление и обслуживание»). Нажмите **Reboot** («Перезагрузка») для перезагрузки устройства.

Восстановление параметров

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

Restore All («Сбросить все»)

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

Default («По умолчанию»)

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

Unlink APP Account («Отмена привязки к учетной записи приложения»)

Отключите учетную запись Guarding Vision от платформы.

Параметры импорта и экспорта

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

Export («Экспорт»)

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



Примечание

Можно импортировать экспортированные параметры устройства на другое устройство.

Import («Импорт»)

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

Обновление

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

Выберите тип обновления из выпадающего списка. Нажмите  и выберите файл обновления с локального ПК. Нажмите **Upgrade** («Обновить») для начала обновления.

Если устройство было подключено к Guarding Vision и сети, когда доступен новый установочный пакет Guarding Vision, нажмите **Upgrade** («Обновить») для обновления системы устройства.



Примечание

Не выключайте устройство во время обновления.

7.7.7 Управление записями в журналах

Можно искать и просматривать журналы устройства.

Перейдите в меню **Configuration → System → Maintenance → Log** («Настройки → Система → Обслуживание → Журнал»).

Установите основной и второстепенный тип журнала. Установите время начала и время окончания поиска и нажмите **Search** («Поиск»).

Результаты будут отображаться ниже, включая номер, время, основной тип, второстепенный тип, номер канала, информацию о локальном/удаленном пользователе, IP-адрес удаленного хоста и т. д.

7.7.8 Настройки режима безопасности

Настройте режим безопасности для входа в клиентское ПО.

На странице управления устройствами нажмите **Configuration → System → Security → Security Service** («Настройки → Система → Безопасность → Служба безопасности»).

Из всплывающего списка выберите режим безопасности и нажмите **Save** («Сохранить»).

Security Mode («Режим безопасности»)

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

Compatible Mode («Режим совместимости»)

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

Enable SSH («Включить ANR»)

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

Enable HTTP («Включить ANR»)

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

7.7.9 Управление сертификатами

Помогает управлять сертификатами сервера/клиента и сертификатом CA.



Примечание

Данная функция поддерживается только у определенных моделей устройств.

Создание и установка самозаверенного сертификата

Шаги

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

Установка другого авторизованного сертификата

Если есть авторизованный сертификат (не созданный устройством), можно импортировать его напрямую на устройство.

Шаги

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

Установка сертификата CA

Перед началом

Заранее подготовьте сертификат CA.

Шаги

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



Примечание

Идентификатор сертификата не может совпадать с идентификатором уже существующих сертификатов.

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

7.7.10 Изменение пароля администратора

Шаги

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



Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

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

7.7.11 Просмотр информации о постановке / снятии с охраны

Просмотр информации о постановке устройства на охрану и IP-адреса постановки на охрану. Нажмите **Configuration → Arming/Disarming Information** («Настройки → Информация о постановке на охрану / снятии с охраны»).

Можно просмотреть информацию о постановке на охрану / снятии с охраны. Для обновления нажмите кнопку **Refresh** («Обновить»).

7.7.12 Онлайн пользователи

Отображается информация о пользователях, выполняющих вход в устройство.

Перейдите в меню **Configuration → System → User Management → Online Users** («Настройки → Система → Управление пользователями → Онлайн пользователи») для просмотра списка онлайн пользователей.

7.7.13 Настройка параметров сети

Задайте параметры TCP / IP, порта, создания отчетов и доступа к платформе.

Настройка основных сетевых параметров

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

DHCP ☐

Network Card

Network Card1

IPv4 Address

10.7.116.210

IPv4 Subnet Mask

255.255.255.0

IPv4 Default Gateway

10.7.116.254

IPv6 Mode

Route Advertisement

View Route Advertisement

IPv6 Address

2001:dddd::aeb9:2ff:fedf:8488

IPv6 Subnet Prefix Length

64

IPv6 Default Gateway

::

Mac Address

ac:b9:2f:df:84:88

MTU

1500

NIC Type

Auto

DNS Server

DHCP ☐

Preferred DNS Server

8.8.8.8

Alternate DNS Server

8.8.4.4

Рисунок 7-6 Страница настроек TCP / IP

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

DHCP

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

При включении этой функции система автоматически задаст IPv4-адрес, IPv4-маску подсети и IPv4-шлюз.

NIC Type («Тип NIC»)

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

DNS Server («DNS-сервер»)

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

Настройка параметров порта

Установите параметры HTTP, RTSP, HTTPS.

Нажмите **Configuration → Network → Basic Settings → Port** («Настройки → Сеть → Основные настройки → Порт»).

HTTP

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

RTSP

Обозначает порт потокового протокола реального времени.

HTTPS

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

Настройка параметров Wi-Fi

Задайте параметры Wi-Fi для беспроводного подключения устройства.

Шаги



Примечание

Функция должна поддерживаться на устройстве.

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



Рисунок 7-7 Страница настроек Wi-Fi

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

Настройка параметров SIP

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



Примечание

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

Нажмите **Configuration** → **Network** → **Basic Settings** → **SIP** («Настройки → Сеть → Основные настройки → SIP»). Поставьте галочку **Enable VOIP Gateway** («Включить VOIP шлюз»).

Укажите зарегистрированное имя пользователя, пароль регистрации, адрес сервера, срок действия, номер и отображаемое имя пользователя.

Нажмите **Save** («Сохранить»).

Настройки способа уведомления

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

Настройте центральную группу для передачи журналов по протоколу ISUP. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Center Group («Центральная группа»)

Выберите центральную группу из выпадающего списка.

Main Channel («Основной канал»)

Устройство будет связываться с центром через основной канал.



Примечание

N1 относится к проводной сети.

Настройка параметров ISUP

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги



Примечание

Функция должна поддерживаться на устройстве.

1. Перейдите в меню **Configuration → Network → Advanced Settings → Platform** («Настройки → Сеть → Расширенные настройки → Платформа»).
2. Из всплывающего списка выберите **ISUP** в меню **Platform Access Mode** («Режим платформы доступа»).
3. Нажмите **Enable** («Включить»).
4. Задайте версию ISUP, и просмотрите тип центра тревог, адрес сервера, порт, ID устройства, статус регистрации.



Примечание

Если выбрана версия 5.0, необходимо также установить ключ ISUP.

5. Настройте параметры прослушивания ISUP, в том числе IP-адрес устройства / доменное имя центра тревог ISUP, URL-адрес центра тревог ISUP и порт центра тревог ISUP.
6. Нажмите **Save** («Сохранить»).

Доступ к платформе

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите **Configuration → Network → Advanced → Platform Access** («Настройки → Сеть → Расширенные настройки → Платформа доступа») для перехода на страницу настроек.

2. Выберите **Platform Access Mode** («Режим платформы доступа»).



Примечание

Guarding Vision является приложением для мобильных устройств. С помощью приложения можно просматривать видео в реальном времени с устройства, получать тревожные уведомления и т. д.

3. Поставьте галочку **Enable** («Включить») для включения функции.
4. **Опционально:** поставьте галочку возле **Custom** («Пользовательский») для настройки адреса сервера самостоятельно.
5. Создайте **Stream Encryption/Encryption Key** («Шифрование потока / Ключ шифрования») для устройства.



Примечание

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

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

Настройка прослушивания HTTP

Устройство может отправлять информацию о тревоге по IP-адресу или доменному имени по протоколу HTTP или HTTPS.

Перед началом

Для получения информации о тревоге IP-адрес или доменное имя должны поддерживать протокол HTTP или HTTPS.



Примечание

Функция должна поддерживаться на устройстве.

Шаги

1. Нажмите **Configuration → Network → Advanced → HTTP Listening** («Настройки → Сеть → Расширенные настройки → Прослушивание HTTP»).
2. Настраивайте IP-адрес или доменное имя, URL-адрес, порт, и протокол информации о тревоге.
3. **Опционально:** нажмите **Default** («По умолчанию») для сброса IP-адреса или доменного имени информации о тревоге.
4. Нажмите **Save** («Сохранить»).

7.7.14 Настройка параметров видео и аудио

Настройте качество изображения, разрешение и громкость устройства.

Настройка параметров видео

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

Настройте видеоканал, имя камеры, тип потока, тип видео, тип битрейта, частоту кадров, макс. битрейт, кодирование видео и интервал I-кадра.

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

Настройка параметров аудио

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

Выберите аудиоканал.

Выберите тип потока и кодирование аудио.

Также для настройки громкости ввода и вывода устройства можно перемещать соответствующий блок. Нажмите, чтобы включить **Voice Prompt** («Голосовое предупреждение»).

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



Примечание

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

7.7.15 Настройка параметров изображения

Установите стандарт видео, WDR, настройку изображения и дополнительную подсветку.

Шаги

1. Нажмите **Configuration** → **Image** («Настройки → Изображение»).

2. Настройте параметры изображения.

Video Standard («Стандарт видео»)

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

PAL

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

NTSC

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

WDR

Включите / выключите функцию WDR.

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

Brightness/Contrast/Saturation/Sharpness («Яркость / Контрастность / Насыщенность / Резкость»)

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

Supplement Light Parameters («Параметры подсветки»)

Выберите тип дополнительной подсветки из выпадающего списка и выберите включить или выключить. При выборе **On** («Вкл.») можно настроить яркость подсветки.

При выборе **Schedule** («Расписание») можно настроить яркость подсветки и расписание ее работы.



Начало / остановка записи видео.



Захват изображения.

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

7.7.16 Привязка события

Настройте действия привязки для событий.

Шаги

1. Нажмите **Configuration → Event → Basic Event → Event Linkage** («Настройки → События → Основные события → Привязка события»), чтобы перейти на соответствующую страницу.
2. Настройте источник события.
 - При выборе **Event Linkage** («Привязка события»), как **Linkage Type** («Тип привязки»), из выпадающего списка выберите тип события.
 - При выборе **Card Linkage** («Привязка карты»), как **Linkage Type** («Тип привязки»), введите № карты и выберите считыватель карт.
 - При выборе **Employee ID Linkage** («Привязка ID сотрудника»), как **Linkage Type** («Тип привязки»), введите ID сотрудника и выберите считыватель карт.
3. Настройте действие привязки.
 - Linked Door** («Привязанная дверь»)
Включите **Linked Door** («Привязанная дверь»), выберите **Door 1** или **Door 2** и настройте состояние двери для события.
 - Linked Alarm Output** («Привязанный тревожный выход»)
Включите **Linked Alarm Output** («Привязанный тревожный выход»), выберите **Alarm Output 1** или **Alarm Output 2** и настройте состояние тревожного выхода для события.
 - Capture Linkage** («Привязка захвата»)
Включите **Capture Linkage** («Привязка захвата») и выберите считыватель карт для захвата события.
 - Trigger Recording** («Запись по тревоге»)
Включите **Trigger Recording** («Запись по тревоге»). Нажмите **Configuration → Event → Basic Event → Recording** («Настройки → События → Основные события → Запись»), здесь можно включить **Record Audio When Recording** («Запись аудио во время записи») и установить время предварительной записи и постзаписи.



Примечание

Подключите к устройству SD-карту и используйте функцию записи видео. Чтобы просмотреть записанное видео, обратитесь к [Поиск события](#).

7.7.17 Настройка основных параметров

Задание параметров контроля доступа

Нажмите **Configuration → General → Authentication Settings** («Настройки → Настройка основных параметров → Настройка параметров аутентификации»).

Примечание

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

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

Card Reader («Считыватель карт»)

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

Main Card Reader («Основной считыватель карт»)

Можно настроить параметры считывателя карт.

Sub Card Reader («Дополнительный считыватель карт»)

Можно настроить параметры подключенных дополнительных считывателей карт.

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

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

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

Enable Card Reader («Включить считыватель карт»)

Включите считыватель карт.

Authentication («Аутентификация»)

В выпадающем списке выберите режим аутентификации в соответствии с потребностями.

Multiple People Authentication («Аутентификация нескольких людей»)

Несколько людей могут пройти аутентификацию одновременно.

Recognition Interval («Интервал распознавания»)

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

Authentication Interval («Интервал аутентификации»)

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

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.

Max. Authentication Failed Attempts («Достижение максимального количества неудачных попыток аутентификации»)

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

Enable Tampering Detection («Включение тревоги тампера»)

Включите детектор саботажа на считывателе карт.

Enable Card No. Reversing («Включение считывания номера карты в обратной последовательности»)

После включения функции номер карты будет считываться в обратной последовательности.

Open Door via Bluetooth («Открытие двери с помощью Bluetooth»)

После включения функции можно разблокировать дверь через Bluetooth.

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

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

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

Enable Card Reader («Включить считыватель карт»)

Включите считыватель карт.

Authentication («Аутентификация»)

В выпадающем списке выберите режим аутентификации в соответствии с потребностями.

Multiple People Authentication («Аутентификация нескольких людей»)

Несколько людей могут пройти аутентификацию одновременно.

Recognition Interval («Интервал распознавания»)

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

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.

Max. Authentication Failed Attempts («Достижение максимального количества неудачных попыток аутентификации»)

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

Communication 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.

Max. Interval When Entering Password («Максимальный интервал времени при вводе пароля»)

Если при вводе пароля в устройство для считывания карт интервал между нажатием двух цифр больше установленного значения, цифры, которые пользователь нажал до этого, будут автоматически удалены.

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

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

Enable Tampering Detection («Включение тревоги тампера»)

Включите детектор саботажа на считывателе карт.

Open Door via Bluetooth («Открытие двери с помощью Bluetooth»)

После включения функции можно разблокировать дверь через Bluetooth в Guarding Vision.

Настройка параметров конфиденциальности

Задайте тип хранения событий, параметры загрузки и хранения изображений, а также параметры очистки изображений.

Нажмите **Configuration → General → Privacy** («Настройки → Общее → Конфиденциальность»)

Настройки хранения событий

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

Delete Old Events Periodically («Периодическое удаление старых событий»)

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

Delete Old Events by Specified Time («Удаление старых событий в указанное время»)

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

Overwriting («Перезапись»)

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

Загрузка и хранение изображений

Upload Picture After Linked Capture («Загрузка изображения после захвата»)

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

Save Pictures After Linked Capture («Сохранение изображения после захвата»)

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

Удаление всех изображений на устройстве

Примечание

После удаления изображения невозможно восстановить.

Clear Captured Pictures («Удаление захваченных изображений»)

Все захваченные изображения лиц будут удалены.

Настройка параметров распознавания лиц

Установите параметры распознавания лиц для доступа.

Нажмите **Configuration → General → Face Recognition Parameters** («Настройки → Общее → Параметры распознавания лиц»).

Настройте **Working Mode** («Режим работы») как **Access Control Mode** («Режим контроля доступа»). Режим контроля доступа является нормальным режимом работы устройства. Для получения доступа необходимо пройти аутентификацию с использованием учетных данных. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Настройка параметров безопасности карты

Нажмите **Configuration → General → Card Security** («Настройки → Общее → Безопасность карты»), чтобы перейти на страницу настроек. Настройте параметры и нажмите **Save** («Сохранить»).

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

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

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

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

M1 Card Encryption («Сектор шифрования M1-карты»)

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

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

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



Примечание

EM-карта поддерживается, если к устройству подключен периферийный считыватель карт, поддерживающий распознавание EM-карты.

Enable DESFire Card («Активация распознавания DESfire-карты»)

Устройство может считывать данные с DESfire-карты при включении функции CPU-карты.

DESFire Card Read Content («Чтение DESFire-карт»)

После включения функции чтения DESFire-карт устройство может считывать содержимое DESFire-карты.

Настройка параметров аутентификации по карте

Настройте параметры карты при аутентификации через карту на устройстве. Нажмите **Configuration → General → Card Authentication Settings** («Настройки → Общее → Параметры аутентификации по карте»).

Выберите режим аутентификации по карте и нажмите **Save** («Сохранить»).

Full Card No. («Полный номер карты»)

Будет прочитан полный номер карты.

Wiegand 26 (3 байта)

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

Wiegand 34 (4 байта)

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

7.7.18 Настройки контроля доступа Настройка параметров двери

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

Door No. Door1

Name

Open Duration 5 s

Door Open Timeout Alarm 30 s

Door Contact ☒ Remain Closed ☐ Remain Open

Exit Button Type ☐ Remain Closed ☒ Remain Open

Door Lock Powering Off ☒ Remain Closed ☐ Remain Open

Extended Open Duration 15 s

Door Remain Open Duration with First Person 10 m

Duress Code *****
Enter 0 to 8 digits.

Super Password *****
Enter 0 to 8 digits.

Save

Рисунок 7-8 Страница настроек параметров двери

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

Door No. («Номер двери»)

Выберите устройство, соответствующее номеру двери.

Name («Название»)

Можно задать имя двери.

Open Duration («Длительность открытого состояния»)

Установите **Door Unlocking Duration** («Длительность разблокированного состояния двери»).

Дверь будет заблокирована, если движение отсутствует в течение установленного времени.

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

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

Door Contact («Дверной контакт»)

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

Exit Button Type («Тип кнопки выхода»)

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

Door Lock Powering Off Status («Закрытие двери при отключении питания»)

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

Extended Open Duration («Расширенная длительность открытого состояния»)

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

Door Remain Open Duration with First Person («Дверь остается открытой после авторизации первого сотрудника»)

Установите продолжительность открытия двери после авторизации первого сотрудника.

После авторизации первого пользователя несколько других пользователей получают доступ к дверям и разрешения на другие действия.

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.

Лифты

Шаги

1. Нажмите **Configuration → Access Control → Elevator Control Parameters** («Настройки → Контроль доступа → Параметры управления лифтом»).
2. Активируйте управление лифтом.
3. Установите параметры лифта.

Elevator No. («Номер лифта»)

Выберите номер лифта для настройки из выпадающего списка.

Elevator controller type («Тип контроллера лифта»)

Выберите контроллер лифта из выпадающего списка.

Interface Type («Тип интерфейса»)

Выберите тип связи для лифта из выпадающего списка.

Если вы выбрали **RS-485**, убедитесь, что вы подключили устройство к контроллеру лифта с помощью кабеля RS-485.

Если вы выбрали **Network Interface** («Сетевой интерфейс»), введите IP-адрес контроллера лифта, номер порта, имя пользователя и пароль.

Negative Floor Capacity («Количество минусовых этажей»)

Установите количество минусовых этажей.

Примечание

- К одному устройству может быть добавлено до 4 контроллеров лифтов.
 - Может быть добавлено до 10 минусовых этажей.
 - Убедитесь, что типы интерфейсов контроллеров лифта, которые подключены к одному и тому же устройству, совместимы.
-

Настройка параметров RS-485

Можно установить параметры RS-485, параметры периферийных устройств, адрес, скорость передачи и т. д.

Поставьте галочку **Enable RS-485** («Включить RS-485») и настройте параметры.

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

№

Настройте номер RS-485.

Peripheral Type («Тип периферийного устройства»)

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



Примечание

После настройки и сохранения периферийного устройства устройство автоматически перезагрузится.

RS-485 Address («Адрес RS-485»)

Задайте необходимый адрес RS-485.



Примечание

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

Baud Rate («Скорость передачи данных»)

Скорость передачи при обмене данными по протоколу RS-485.

Настройка параметров интерфейса Wiegand

Можно настроить направление передачи данных интерфейса Wiegand.

Шаги



Примечание

Некоторые модели устройств не поддерживают данную функцию. Настройка параметров зависит от фактического функционала устройства.

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

Wiegand ☐

Wiegand Direction ☒ Output

Wiegand Mode Wiegand 34

Time Interval 2 ms

Pulse Width 50 us

Рисунок 7-9 Страница настройки Wiegand

2. Нажмите **Wiegand** («Wiegand»), чтобы включить функцию Wiegand.

3. Установите направление передачи данных.

Input («Вход»)

Устройство можно подключать к считывателю карт Wiegand.

Output («Выход»)

Устройство можно подключать к внешнему устройству контроля доступа. Эти два устройства будут передавать номер карты через Wiegand 26 или 34.

4. Перемещайте бегунок для настройки временного интервала и ширины импульса.



Примечание

- Временной интервал в диапазоне от 1 до 20 мс.
- Ширина импульса в диапазоне от 1 до 100 мкс.

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



Примечание

При изменении и сохранении параметров периферийных устройств произойдет автоматическая перезагрузка устройства.

7.7.19 Настройка видеодомофонии

Настройка параметров видеодомофонии

Устройство можно использовать в качестве вызывной панели, установленной снаружи помещений вызывной панели или устройства контроля доступа. Перед использованием необходимо задать номер устройства.

Нажмите **Configuration** → **Intercom** → **Device No** («Настройки → Домофон → Номер устройства»).

Если тип устройства задан как **Door Station** («Вызывная панель») или **Access Control Device** («Устройство контроля доступа»), можно настроить номер этажа, номер вызывной панели. Выберите **Advanced Settings** («Расширенные настройки»), чтобы настроить **Community No.** («Номер микрорайона»), **Building No.** («Номер здания») и **Unit No.** («Номер помещения»).

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

Device Type («Тип устройства»)

Устройство может быть установлено снаружи и внутри помещений. Выберите тип устройства из выпадающего списка.



Примечание

При изменении типа устройства необходимо перезагрузить устройство.

Floor No. («Номер этажа»)

Укажите номер этажа, на котором установлено устройство.

Door Station No. («Номер вызывной панели»)

Укажите номер этажа, на котором установлено устройство.



Примечание

- При изменении номера необходимо перезагрузить устройство.
 - Номер вызывной панели: 0, номер дополнительной вызывной панели: от 1 до 16.
-

Community No. («Номер микрорайона»)

Укажите номер микрорайона.

Building No. («Номер здания»)

Укажите номер здания.

Unit No. («Номер помещения»)

Укажите номер помещения.



Примечание

При изменении номера необходимо перезагрузить устройство.

Если установить тип устройства как **Outer Door Station** («Вызывная панель, установленная снаружи помещения»), можно установить номер периода, номер вызывной панели и номер микрорайона.

Outer Door Station No. («Номер вызывной панели, установленной снаружи помещения»)

Если в качестве типа устройства выбрана вызывная панель, установленная снаружи помещения, необходимо ввести число в диапазоне от **1** до **99**.



Примечание

При изменении номера необходимо перезагрузить устройство.

Community No. («Номер микрорайона»)

Укажите номер микрорайона.

Session Settings («Настройки сеанса связи»)

Включите связь между вызывной панелью, пультом консьержа / диспетчера и сервером видеодомофонии.

Шаги

1. Нажмите **Configuration → Intercom → Session Settings** («Настройка → Домофон → Настройки сеанса связи»), чтобы перейти на страницу настроек.
2. Укажите пароль регистрации, IP-адрес пульта консьержа / диспетчера, IP-адрес частного сервера и включите протокол 1.0.

Registration Password («Пароль регистрации»)

Пароль активации пульта консьержа / диспетчера.

Main Station IP («IP-адрес пульта консьержа / диспетчера»)

IP-адрес пульта консьержа / диспетчера.

Private Server IP («IP-адрес частного сервера»)

IP-адрес частного сервера.

Enable Protocol 1.0 («Включение протокола 1.0»)

После включения, устройство подключено к пульту консьержа / диспетчера по предыдущему протоколу. При выключении, устройство подключено к пульту консьержа / диспетчера по новому протоколу.

3. Нажмите **Save** («Сохранить»).

Настройка временных интервалов

Установите макс. продолжительность вызова.

Перейдите в **Configuration → Intercom → Time Parameters** («Настройки → Домофония → Параметры времени»). Перемещайте бегунок для настройки макс. продолжительности вызова. Нажмите **Save** («Сохранить»).



Примечание

Макс. продолжительность вызова составляет от 90 до 120 с.

Настройка привязки номеров

Вызовите SIP-кабинет для вызова кабинета.

Шаги

1. Нажмите **Configuration → Intercom → Number Settings** («Настройка → Домофон → Настройка привязки номеров»), чтобы перейти на страницу настроек.
2. Нажмите **Add** («Добавить»), введите **Room No.** («Номер помещения») и **SIP**.
3. Нажмите **Save** («Сохранить»).

7.7.20 Настройка основных параметров

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

Выберите **Fingerprint Security Level** («Уровень безопасности отпечатков пальцев») согласно текущим требованиям.

Раздел 8 Настройка устройства через мобильный интерфейс

8.1 Вход в систему

В систему можно войти через мобильный интерфейс.



Примечание

- Некоторые модели поддерживают настройку Wi-Fi.
- Устройство должно быть активировано.

Получите IP-адрес от устройства после включения Wi-Fi. Убедитесь, что IP-сегмент устройства и компьютера совпадают. Подробная информация представлена в разделе **Настройка параметров Wi-Fi**.

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

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

8.2 Поиск событий

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

Введите условия поиска, включая идентификатор сотрудника / посетителя, имя, номер карты, время начала и время окончания доступа и нажмите **Search** («Поиск»).



Примечание

Поддерживает поиск по имени до 32 символов.

Результаты будут отображены в списке.

8.3 Управление пользователями

Можно добавлять, редактировать, удалять и искать пользователей через мобильный веб-интерфейс.

Шаги

1. Нажмите **User** («Пользователь»), чтобы перейти на страницу настроек.
2. Добавление пользователя.
 - 1) Нажмите **+**.

Basic Information	
*Employee ID	
Name	
Gender	unknown >
User Role	Normal User >
Floor No.	
Room No.	
Card No.	0 >
Fingerprint	0 >
Long-Term Effective ☐	
Start Date	2022-07-18 >
End Date	2032-07-17 >
Administrator	☐
Authentication Settings	

Рисунок 8-1 Добавление пользователя

2) Настройте следующие параметры.

Employee ID («ID сотрудника»)

Введите ID сотрудника. ID сотрудника не может быть 0 или превышать 32 символа. Он может состоять из букв верхнего / нижнего регистра и цифр.

Name («Имя»)

Введите ваше имя. Имя поддерживает числа, буквы верхнего / нижнего регистра и символы. Рекомендуется вводить имя в пределах 32 символов.

Gender («Пол»)

Выберите пол.

User Role («Роль пользователя»)

Выберите роль пользователя.

Floor No./Room No./Card No. («Номер этажа / Номер помещения / Номер карты»)

Введите номер этажа / номер помещения / номер карты.

Fingerprint («Отпечатки пальцев»)

Добавьте отпечатки пальцев. Нажмите **Fingerprint** («Отпечаток пальца»), затем нажмите +, чтобы добавить отпечатки пальцев с помощью модуля считывания отпечатков пальцев.

Long-Term Effective («Гарантия»)

Настройте разрешение пользователя как

Start Date/End Date («Дата начала / Дата окончания»)

Настройте **Start Date** («Дата начала») и **End Date** («Дата окончания») разрешения пользователя.

Administrator («Администратор»)

Если пользователя нужно назначить в качестве администратора, включите

Administrator («Администратор»).

Authentication Type («Тип аутентификации»)

Выберите тип аутентификации.

3) Нажмите **Save** («Сохранить»).

3. Нажмите на пользователя в списке, чтобы изменить информацию о нем.

4. Нажмите на пользователя, которого нужно удалить из списка, затем нажмите , чтобы удалить его.

5. Можно осуществлять поиск пользователя по идентификатору сотрудника или имени в поле поиска.

8.4 Настройка

8.4.1 Просмотр информации об устройстве

Просмотр названия устройства, языка, модели, серийного номера, QR-кода, версии и т. д.

Нажмите **Configuration → System → System Settings → Basic Information** («Настройки → Система → Настройка системы → Основная информация»), чтобы перейти на страницу настройки.

Можно посмотреть название устройства, язык, модель, серийный номер, QR-код, версию и т. д.

8.4.2 Настройка времени

Установите часовой пояс, режим синхронизации времени и отображаемое время.

Нажмите **Configuration → System → System Settings → Time Settings** («Конфигурация → Система → Настройки системы → Настройки времени»), чтобы перейти на страницу настроек.

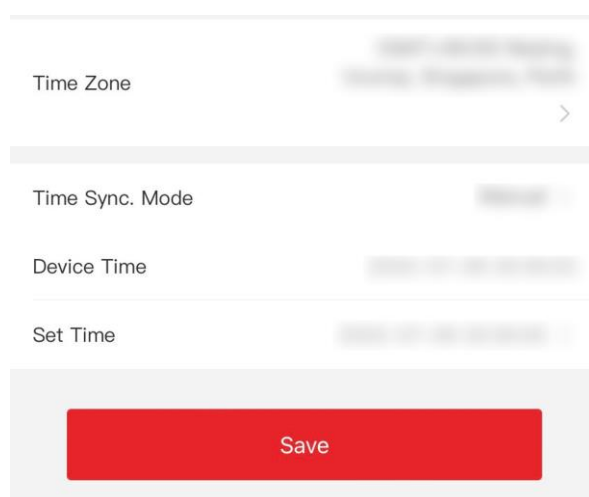


Рисунок 8-2. Настройка времени

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

Часовой пояс

Выберите часовой пояс, на котором находится устройство из выпадающего списка.

Синхронизация времени вручную

По умолчанию время устройства должно быть синхронизировано вручную. Можно установить время устройства вручную.

NTP

Задайте IP-адрес NTP-сервера, номер порта и интервал.

8.4.3 Настройка перехода на летнее время (DST)

Шаги

1. Нажмите **Configuration** → **System** → **System Settings** → **DST** («Конфигурация → Система → Настройки системы → Летнее время»), чтобы перейти на страницу настроек.

Enable DST ☐

Start Time Apr First Sunday 02h

Month Apr >

Week First >

Weekday Sunday >

Time 02 >

End Time Oct Last Sunday 02h

Month Oct >

Week Last >

Weekday Sunday >

DST Bias 30minute(s) >

Save

Рисунок 8-3 Летнее время

2. Нажмите **Enable DST** («Включить DST»).
3. Настройте время перехода на летнее время, время окончания и смещения.
4. Нажмите **Save** («Сохранить»).

8.4.4 Просмотр лицензии на ПО с открытым исходным кодом

Нажмите **Configuration** → **System** → **System Settings** → **About** («Настройки → Система → Настройки системы → Подробнее») и нажмите **View Licenses** («Просмотр лицензии»), чтобы просмотреть лицензию устройства.

8.4.5 Управление пользователями

Шаги

1. Нажмите **Configuration** → **System** → **User Management** → **admin** → **Modify Password** («Настройки → Система → Управление пользователями → Администратор → Изменить пароль»), чтобы перейти на страницу настроек.
2. Введите старый пароль и создайте новый пароль.
3. Подтвердите новый пароль.
4. Нажмите **OK**.



Примечание

Надежность пароля устройства может быть автоматически проверена. Для усиления защиты продукта настоятельно рекомендуется использовать надежный пароль (от 8 до 16 символов, включая как минимум два вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы).

Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

8.4.6 Обновление и техническое обслуживание

Можно выполнить перезагрузку устройства, обновление версии устройства и отключение приложения.

Перезагрузка устройства

Нажмите **Configuration** → **System** → **Maintenance** («Настройки → Система → Обслуживание»). Нажмите **Reboot** («Перезагрузка»), чтобы перезагрузить устройство.

Обновление

Нажмите **Configuration** → **System** → **Maintenance** («Настройки → Система → Обслуживание»).

Если устройство было подключено к Guarding Vision и сети, когда доступен новый установочный пакет Guarding Vision, Нажмите **Upgrade** («Обновить») для обновления системы устройства.



Примечание

Не выключайте устройство во время обновления.

Восстановление параметров

Нажмите **Configuration** → **System** → **Maintenance** («Настройки → Система → Обслуживание»).

Default («По умолчанию»)

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

Restore All («Сбросить все»)

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

Отмена привязки

Нажмите **Configuration → System → Maintenance** («Настройки → Система → Обслуживание»).

Нажмите **Unlink** («Отмена привязки»), чтобы отменить привязку приложения.

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

8.4.7 Настройки безопасности

Можно настроить SSH и HTTP согласно текущим требованиям.

Нажмите **Configuration → System → Security** («Конфигурация → Система → Безопасность»), чтобы перейти на страницу настроек. Нажмите **Enable** («Включить») для включения SSH.

Нажмите **Enable** («Включить») для включения HTTP.

8.4.8 Настройка параметров сети

Можно настроить параметры порта и Wi-Fi.

Настройка параметров Wi-Fi

Задайте параметры Wi-Fi для беспроводного подключения устройства.

Шаги

Примечание

Функция должна поддерживаться на устройстве.

1. Нажмите **Network → Basic Settings → Wi-Fi** («Сеть → Основные настройки → Wi-Fi») для перехода на страницу настроек.
2. Поставьте галочку **Enable Wi-Fi** («Включить Wi-Fi»).

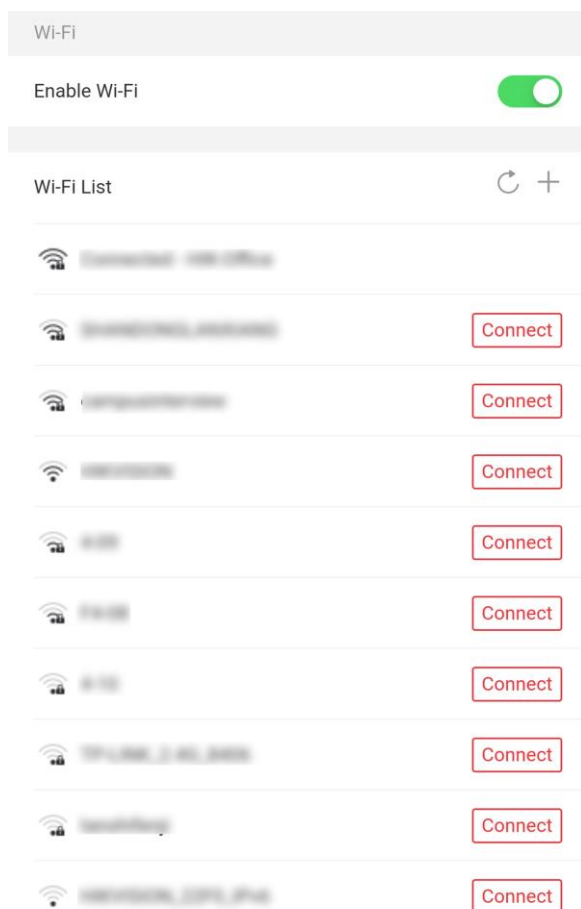


Рисунок 8-4 Wi-Fi

3. Добавьте Wi-Fi.

1) Нажмите +.

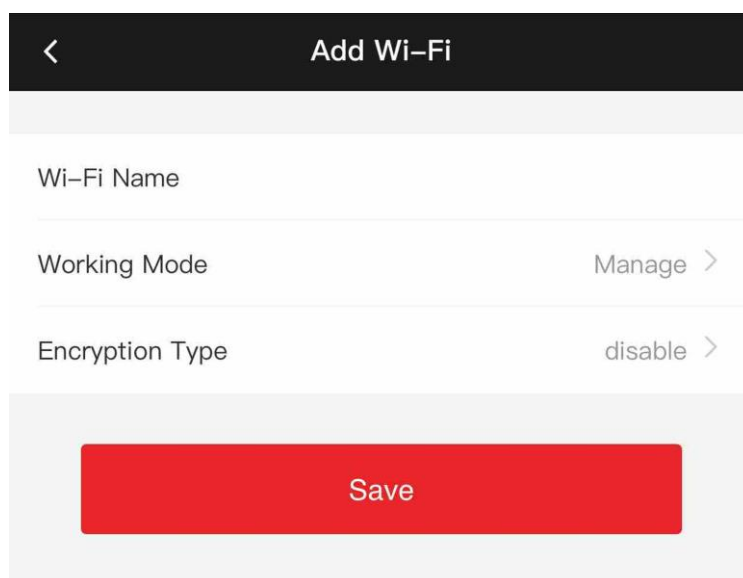


Рисунок 8-5 Добавление Wi-Fi

- 2) Введите **Wi-Fi Name** («Имя Wi-Fi») и **Wi-Fi Password** («Пароль Wi-Fi»), и выберите **Working Mode** («Рабочий режим») и **Encryption Type** («Тип шифрования»).
- 3) Нажмите **Save** («Сохранить»).
4. Выберите имя Wi-Fi и нажмите **Connect** («Подключиться»).
5. Введите пароль и нажмите **Save** («Сохранить»).
6. Настройте параметры WLAN.
 - 1) Установите IP-адрес устройства, маску подсети и шлюз. Включите DHCP, и система автоматически задаст IP-адрес, маску подсети и шлюз.
 - 2) Нажмите **Save** («Сохранить»).

Настройка параметров порта

Можно настроить HTTP, RTSP, HTTPS при доступе к устройству через сеть согласно текущим потребностям.

Нажмите **Configuration → Network → Basic Settings → Port** («Настройка → Сеть → Основные настройки → Порт»), чтобы перейти на страницу настроек.

HTTP

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

RTSP

Обозначает порт потокового протокола реального времени.

HTTPS

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

Доступ к платформе

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите **Configuration → Network → Advanced → Guarding Vision** («Настройка → Сеть → Расширенные настройки → Guarding Vision»), чтобы перейти на страницу настроек.



Примечание

Guarding Vision является приложением для мобильных устройств. С помощью приложения можно просматривать видео в реальном времени с устройства, получать тревожные уведомления и т. д.

-
2. Поставьте **Enable** («Включить») для включения соответствующей функции.
 3. Введите адрес сервера и шифрование потока.



Примечание

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

-
4. Можно просматривать **Register Status** («Статус регистрации») и **Device QR Code** («QR-код устройства.»).
 5. Нажмите **Save** («Сохранить»), чтобы активировать настройки.

Настройка параметров ISUP

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги

Примечание

Функция должна поддерживаться на устройстве.

1. Нажмите **Configuration → Network → Advanced** («Настройка → Сеть → Расширенные настройки»).
2. Нажмите **Enable** («Включить»).
3. Задайте версию ISUP, IP-адрес, порт и учетную запись.

Примечание

Если выбрана версия 5.0, необходимо также установить ключ шифрования.

4. Настройка центральной группы.

Center Group («Центральная группа»)

Выберите центральную группу из выпадающего списка.

Main Channel/Backup Channel («Основной канал / резервный канал»)

Устройство будет связываться с центром через основной канал. Когда в основном канале возникает исключение, устройство и центр будут связываться друг с другом через резервный канал.

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

Прослушивание HTTP

Можно настроить параметры прослушивания HTTP.

Шаги

1. Нажмите **Configuration → Network → Advanced → HTTP Listening** («Настройки → Сеть → Расширенные настройки → Прослушивание HTTP»).
2. Настраивайте IP-адрес назначения или доменное имя, URL-адрес и порт.
3. **Опционально:** нажмите **Default** («По умолчанию»), чтобы сбросить IP-адрес назначения или доменное имя.
4. Нажмите **Save** («Сохранить»).

8.4.9 Настройка основных параметров

Настройка параметров аутентификации

Настройка параметров контроля доступа.

Шаги

1. Нажмите **Configuration → General Settings → Authentication Settings** («Настройки → Настройка основных параметров → Настройка параметров аутентификации»).

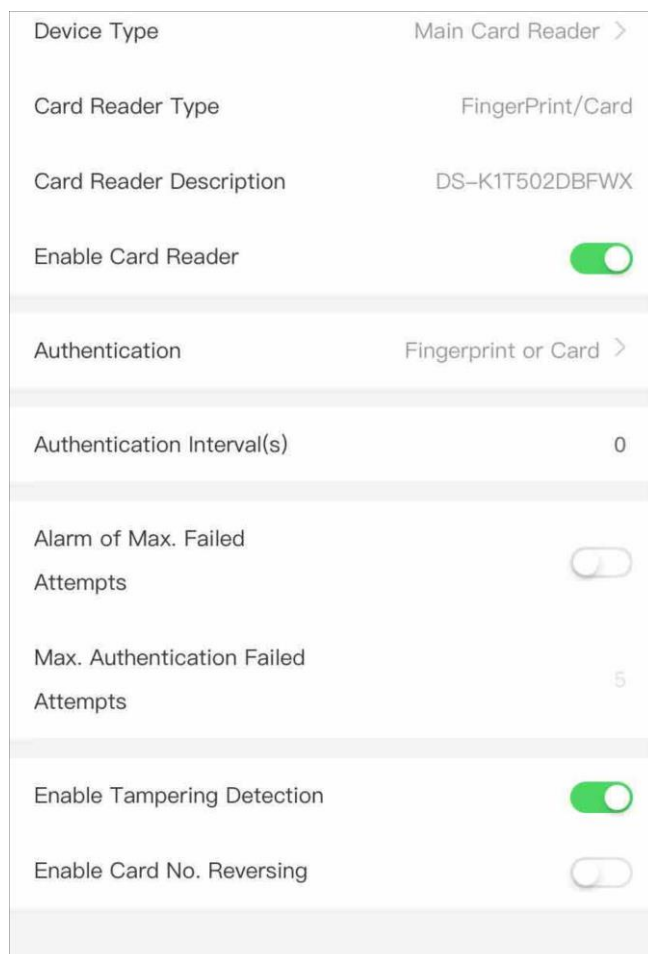


Рисунок 8-6 Настройка параметров аутентификации

2. Нажмите **Save** («Сохранить»).

Device Type («Тип устройства»)

Main Card Reader («Основной считыватель карт»)

Можно настроить параметры считывателя карт. Если вы выбрали основной считыватель карт, необходимо установить следующие параметры: **тип считывателя карт, описание считывателя карт, включение считывателя карт, аутентификация, интервал распознавания, минимальный интервал считывания карты, запуск тревоги при достижении максимального количества неудачных попыток аутентификации / считывания карты, включение тревоги тампера, включение считывания номера карты в обратной последовательности.**

Card Reader Type («Тип считывателя карт»)

Просмотр типа считывателя карт.

Card Reader Description («Описание считывателя карт»)

Просмотр описания считывателя карт. Доступно только для чтения.

Enable Card Reader («Включить считыватель карт»)

Включение считывателя карт.

Authentication («Аутентификация»)

В выпадающем списке выберите режим аутентификации в соответствии с потребностями.

Authentication Interval («Интервал аутентификации»)

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

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

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

Enable Tampering Detection («Включение тревоги тампера»)

Включите детектор саботажа на считывателе карт.

Enable Card No. Reversing («Включить считывание номера карты в обратной последовательности»)

После включения функции номер карты будет считываться в обратной последовательности.

Настройка параметров конфиденциальности

Задайте тип хранения событий.

Нажмите **Configuration → General Settings → Privacy («Настройки → Настройка основных параметров → Конфиденциальность»)**.

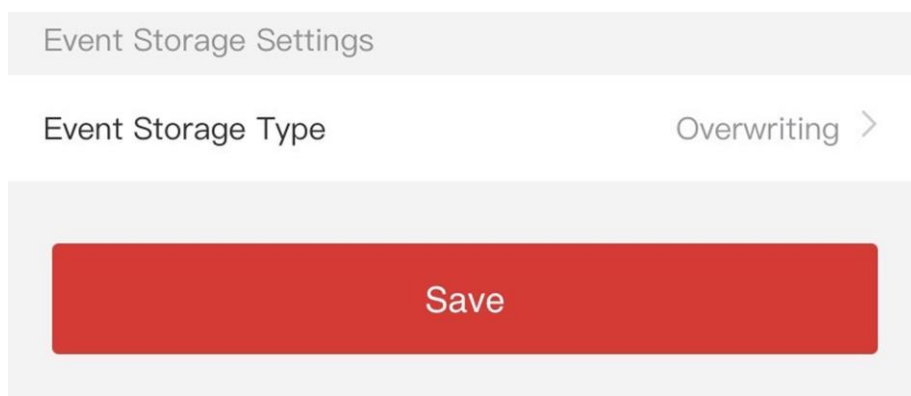


Рисунок 8-7 Настройки параметров конфиденциальности

Настройки хранения событий

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

Delete Old Events Periodically («Периодическое удаление старых событий»)

Введите число, чтобы установить период для удаления событий. Все события будут удалены в соответствии с настроенным периодом времени.

Delete Old Events by Specified Time («Удаление старых событий в указанное время»)

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

Overwriting («Перезапись»)

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

Настройка параметров безопасности карты

Нажмите **Configuration → General Settings → Card Security** («Настройки → Настройка основных параметров → Безопасность карты»), чтобы перейти на страницу настроек.

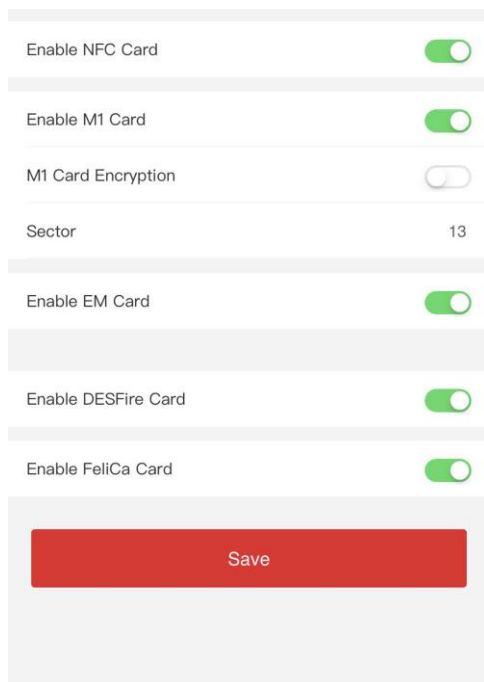


Рисунок 8-8 Безопасность карты

Настройте параметры и нажмите **Save** («Сохранить»).

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

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

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

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

M1 Card Encryption («Шифрование M1-карты»)

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

Sector («Сектор»)

Активируйте функцию и установите сектор шифрования. По умолчанию сектор 13 зашифрован. Рекомендуется зашифровать сектор 13.

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

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



Примечание

EM-карта поддерживается, если к устройству подключен периферийный считыватель карт, поддерживающий распознавание EM-карты.

Enable DESFire Card («Активация распознавания DESfire-карты»)

Устройство может считывать данные с DESfire-карты при включении функции CPU-карты.

Настройка параметров аутентификации по карте

Настройте параметры карты при аутентификации через карту на устройстве. Нажмите **Configuration → General Settings → Card Authentication Settings** («Настройки → Настройка основных параметров → Настройка аутентификации по карте»).

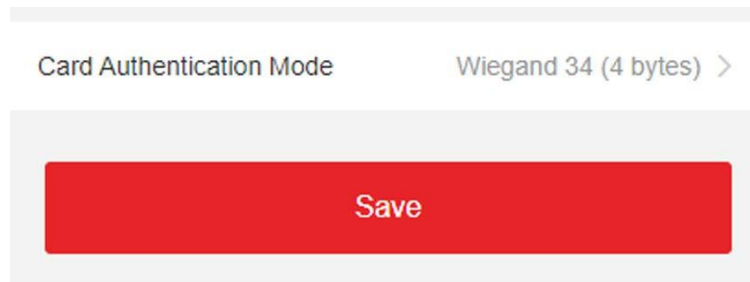


Рисунок 8-9 Страница аутентификации по карте

Выберите режим аутентификации по карте и нажмите **Save** («Сохранить»).

Full Card No. («Полный номер карты»)

Будет прочитан полный номер карты.

Wiegand 26 (3 байта)

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

Wiegand 34 (4 байта)

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

8.4.10 Настройки параметров лица

Настройте уровень безопасности отпечатков пальцев.

Нажмите **Configuration → Smart → Intelligent Parameter** («Настройки → Интеллектуальное → Интеллектуальные параметры»).

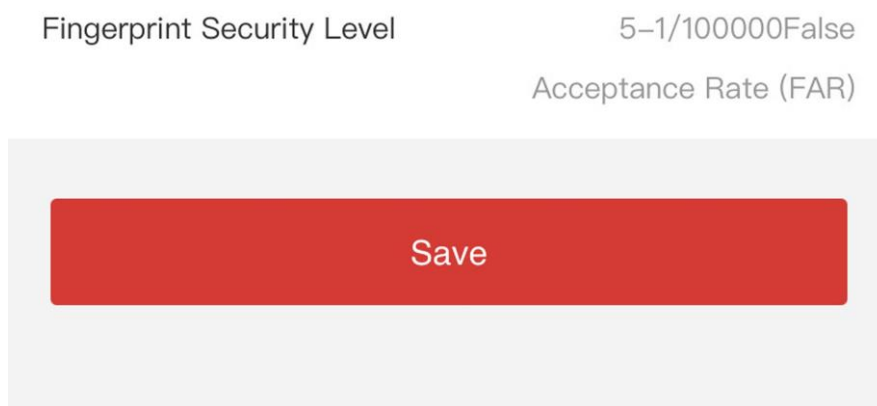


Рисунок 8-10 Уровень безопасности отпечатков пальцев

Примечание

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

Выберите уровень безопасности согласно текущим требованиям. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

8.4.11 Настройки видеодомофонии

Настройка ID устройства

Устройство можно использовать в качестве вызывной панели, установленной снаружи помещений вызывной панели или устройства контроля доступа. Перед использованием необходимо задать ID устройства.

Настройки ID устройства

Нажмите **Configuration** → **Intercom** → **Device ID Settings** («Настройки → Домофон → Настройки ID устройства»).

Если установить тип устройства как **Door Station** («Вызывная панель»), можно настроить номер этажа и номер вызывной панели. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Device Type	Door Station >
Floor No.	1 >
Door Station No.	0
Save	

Рисунок 8-11 Настройки ID устройства (Вызывная панель)

Device Type («Тип устройства»)

Устройство можно использовать в качестве вызывной панели или установленной снаружи помещений вызывной панели. Выберите тип устройства из выпадающего списка.



Примечание

При изменении типа устройства необходимо перезагрузить устройство.

Floor No. («Номер этажа»)

Укажите номер этажа, на котором установлено устройство.

Door Station No. («Номер вызывной панели»)

Укажите номер этажа, на котором установлено устройство.



Примечание

При изменении номера необходимо перезагрузить устройство.

Если установить тип устройства как **Outer Door Station** («Вызывная панель, установленная снаружи помещения»), можно установить номер вызывной панели.

Device Type	Outer Door Station >
Outer Door Station No.	0
Save	

**Рисунок 8-12 Настройки ID устройства
(Вызывная панель, установленная снаружи помещения)**

Outer Door Station No. («Номер вызывной панели, установленной снаружи помещения»)

Если в качестве типа устройства выбрана вызывная панель, установленная снаружи помещения, необходимо ввести число в диапазоне от **1** до **99**.



Примечание

При изменении номера необходимо перезагрузить устройство.

8.4.12 Настройки параметров контроля доступа

Настройка параметров двери

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

Door No.	Door1 >
Name	door1
Open Duration(s)	5
Door Open Timeout Alarm(s)	30
Door Contact	Remain Closed >
Exit Button Type	Remain Open >
Extended Open Duration(s)	15
Door Remain Open Duration with First Person(min)	10
Duress Code	••••••
Super Password	••••••
Unlock Password	••••••

Рисунок 8-13. Страница настроек параметров двери

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

Door No. («Номер двери»)

Выберите устройство, соответствующее номеру двери.

Name («Название»)

Можно задать имя двери.

Open Duration («Длительность открытого состояния»)

Установите **Door Unlocking Duration** («Длительность разблокированного состояния двери»).

Дверь будет заблокирована, если движение отсутствует в течение установленного времени.

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

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

Door Contact («Дверной контакт»)

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

Exit Button Type («Тип кнопки выхода»)

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

Extended Open Duration («Расширенная длительность открытого состояния»)

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

Door Remain Open Duration with First Person («Дверь остается открытой после авторизации первого сотрудника»)

Установите продолжительность открытия двери после авторизации первого сотрудника.

После авторизации первого пользователя несколько других пользователей получают доступ к дверям и разрешения на другие действия.

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.

Unlock Password («Пароль разблокировки»)

Пользователь может открыть дверь с помощью пароля разблокировки.



Примечание

Суперпароль должен отличаться от кода принуждения. Содержит от 4 до 8 цифр.

Настройка параметров RS-485

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

RS-485 Settings	☒
RS-485 Protocol	Private >
No.	1 >
Peripheral Type	Card Reader >
RS-485 Address	1
Baud Rate	19200 >
Data Bit	8 >
Stop Bit	1 >
Parity	None >
Flow Ctrl	None >
Communication Mode	Half-Duplex >

Save

Рисунок 8-14 Страница RS-485

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

Peripheral Type («Тип периферийного устройства»)

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



Примечание

После настройки и сохранения периферийного устройства устройство автоматически перезагрузится.

RS-485 Address («Адрес RS-485»)

Задайте необходимый адрес RS-485.



Примечание

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

Baud Rate («Скорость передачи данных»)

Скорость передачи при обмене данными по протоколу RS-485.

Data Bit («Бит данных»)

Бит данных при обмене данными по протоколу RS-485.

Stop Bit («Стоповый бит»)

Стоповый бит при обмене данными по протоколу RS-485.

Parity/Flow Ctrl/Communication Mode («Четность / Управление потоком / Беспроводная сеть»)

Функция включена по умолчанию.

Настройка параметров интерфейса Wiegand

Можно настроить направление передачи данных интерфейса Wiegand.

Шаги

1. Нажмите **Configuration → Access Control → Wiegand Settings** («Настройки → Контроль доступа → Настройки Wiegand»).

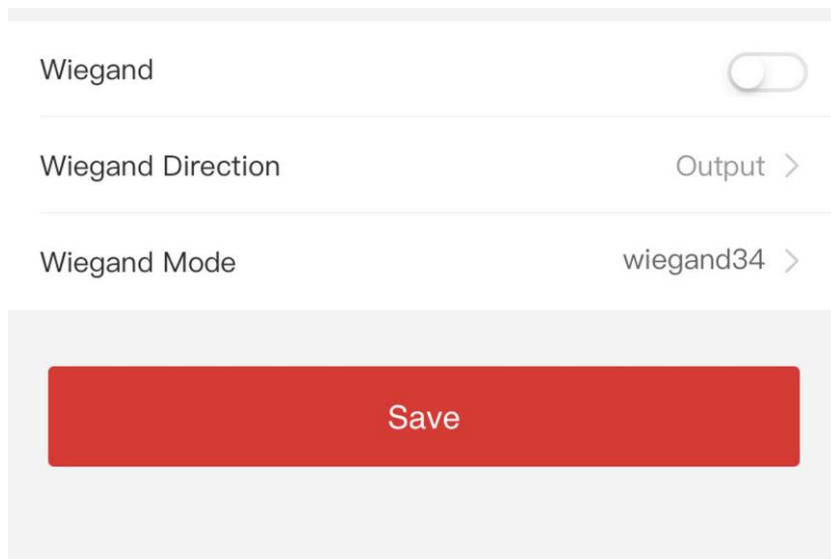


Рисунок 8-15 Страница настройки Wiegand

2. Нажмите **Wiegand**, чтобы включить функцию Wiegand.

3. Установите направление передачи данных.

Output («Выход»)

Устройство можно подключать к внешнему устройству контроля доступа. Эти два устройства будут передавать номер карты через Wiegand 26 или 34.

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



Примечание

При изменении и сохранении параметров периферийных устройств произойдет автоматическая перезагрузка устройства.

8.5 Операции для двери

Можно управлять дверью через мобильный веб-интерфейс. Нажмите **Door Operation** («Операции для двери») для перехода на страницу операций.

Нажмите , чтобы открыть дверь.

Нажмите , чтобы закрыть дверь.

Нажмите , чтобы дверь оставалась открытой.

Нажмите , чтобы дверь оставалась закрытой.

Раздел 9 Настройка клиентского ПО

Вы можете позвонить на горячую линию, чтобы получить установочный пакет ПО клиента Guarding Vision.

9.1 Схема настройки клиентского ПО

Следуйте приведенной ниже схеме для настройки клиентского ПО.

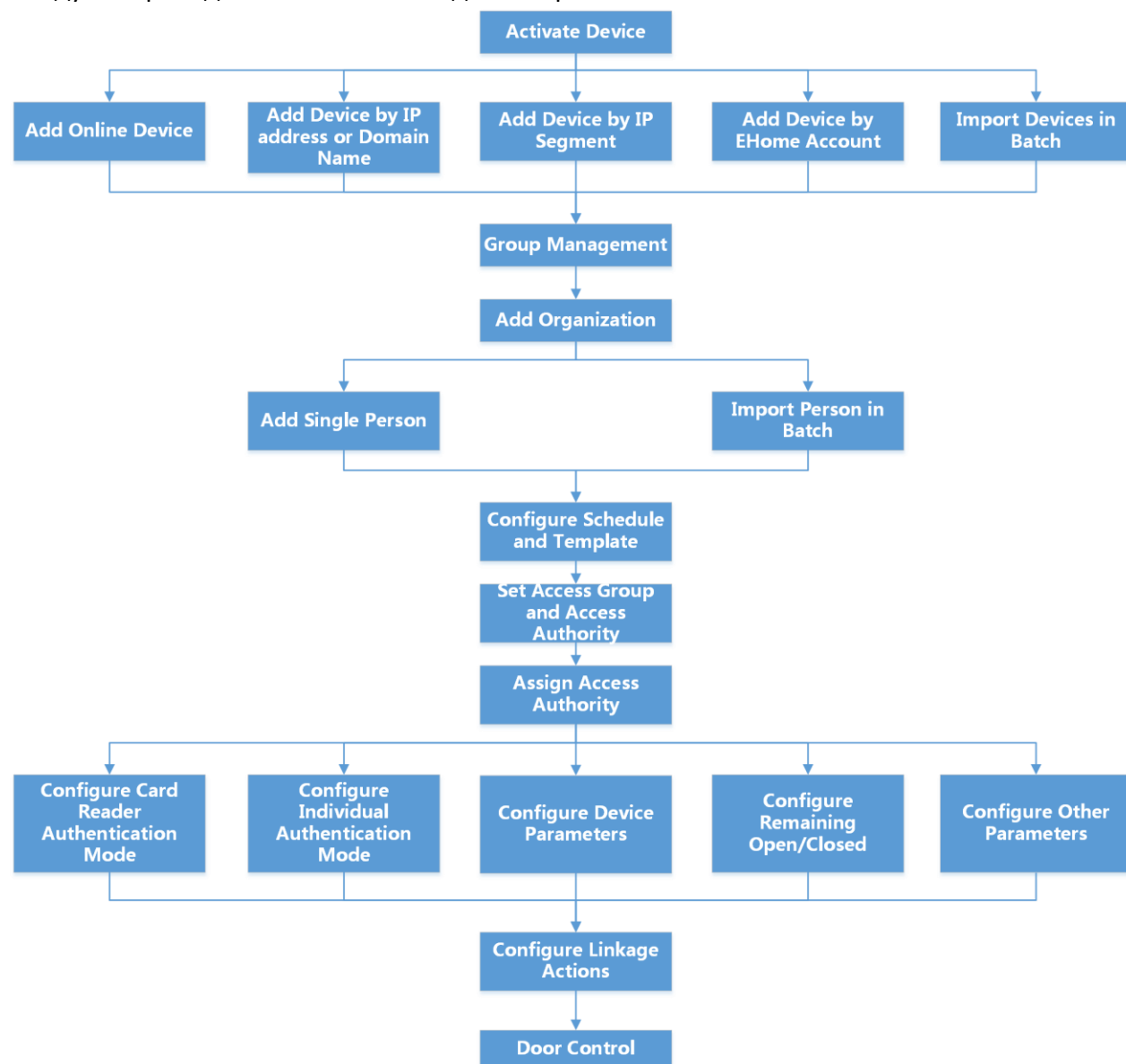


Рисунок 9-1. Схема настройки клиентского ПО

Английский язык	Русский язык
Activate Device	Активация устройства
Add Online Device	Добавление онлайн устройства
Add Device by IP Address or Domain name	Добавление устройства по IP-адресу или доменному имени
Add Device by IP Segment	Добавление устройств по сегменту IP-адресов
Add Device by EHome Account	Добавление устройств по учетной записи EHome
Import Device in Batch	Импорт устройств в пакетном режиме
Group Management	Управление группами
Add Organization	Добавление организации
Add Single Person	Добавление одного пользователя
Import Person in Batch	Импорт пользователя в пакетном режиме
Configure Schedule and Template	Настройка графиков и шаблонов
Set Access Group and Access Authority	Настройка группы контроля доступа и разрешения на доступ
Assign Access Authority	Назначение разрешения на доступ
Configure Card Reader Authentication Mode	Настройка аутентификации при помощи считывателя карт
Configure Device Parameters	Настройка параметров устройства
Configure Remaining Open / Closed	Настройка параметров оставить открытым / закрытым
Configure Other Parameters	Настройка других параметров
Configure Linkage Actions	Настройка привязанных действий
Door Control	Управление дверью

9.2 Управление устройством

Поддержка устройств контроля доступа и устройств видеодомофонии.

Пример

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

9.2.1 Добавление устройства

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

Добавление 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.

Рисунок 9-2 Добавление устройства по IP-адресу или доменному имени

3. Нажмите кнопку **Add** («Добавить»), чтобы открыть окно добавления устройства. Выберите режим добавления **IP/Domain** («IP-адрес / доменное имя»).

4. Введите необходимую информацию.

Name («Имя»)

Создайте описательное имя для устройства. Например, можно использовать название, которое отображает местоположение или функцию устройства.

Address («Адрес»)

IP-адрес или доменное имя устройства.

Port («Порт»)

Добавляемые устройства имеют одинаковый номер порта. Значение по умолчанию - **80**.

User Name («Имя пользователя»)

Введите имя пользователя устройства. По умолчанию имя пользователя — **Admin** («Администратор»).

Password («Пароль»)

Введите пароль устройства.



Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

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

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



Примечание

- Устройство должно поддерживать данную функцию.
- Если функция Certificate Verification («Проверка сертификата») включена, нажмите **Open Certificate Directory** («Открыть каталог сертификатов»), чтобы открыть папку по умолчанию, затем скопируйте файл сертификата, экспортированный с устройства, в этот каталог по умолчанию для повышения уровня безопасности. См. подробную инструкцию по включению функции проверки сертификата.
- Войдите в устройство, чтобы загрузить файл сертификата через веб-интерфейс.

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.

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»).

Рисунок 9-3 Добавление устройств 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, подлежащих добавлению, в соответствующие столбцы.



Примечание

Подробное описание обязательных полей см. во введении.

Adding Mode («Режим добавления»)

Введите **0** или **1** или **2**.

Address («Адрес»)

Измените адрес устройства.

Port («Порт»)

Введите номер порта устройства. По умолчанию номер порта: **80**.

User Name («Имя пользователя»)

Введите имя пользователя устройства. По умолчанию имя пользователя — **Admin** («Администратор»).

Password («Пароль»)

Введите пароль устройства.



Предостережение

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

Import to Group («Импорт в группу»)

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

6. Нажмите  и выберите файл шаблона.

7. Нажмите **Add** («Добавить»), чтобы импортировать устройства.

9.2.2 Сброс пароля устройства

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

Шаги

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



Примечание

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



Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая как минимум три вида из следующих категорий: буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопасным.

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

9.2.3 Управление добавленными устройствами

После добавления устройств вы можете управлять добавленными устройствами, в том числе: редактировать параметры устройства, выполнять удаленную настройку устройства, просмотреть состояние устройства и т. д.

Таблица 9-1 Управление добавленными устройствами

Редактирование устройства	Нажмите  , чтобы изменить информацию об устройстве, включая имя устройства, адрес, имя пользователя, пароль и т. д.
Удаление устройства	Выберите одно или более устройств, затем нажмите Delete («Удалить»), чтобы удалить выбранные устройства.
Удаленная настройка	Нажмите  , чтобы выполнить удаленную настройку соответствующего устройства. Подробная информация представлена в руководстве пользователя устройства.
Просмотр состояния устройства	Нажмите  , чтобы просмотреть состояние устройства, включая наименование двери, номер, статус и т. д.  Примечание Доступная информация о состоянии устройства зависит от модели фактического устройства.
Просмотр пользователей в сети	Нажмите  , чтобы просмотреть подробную информацию о пользователях в сети, которые имеют доступ к устройству, включая имя пользователя, тип пользователя, IP-адрес и время входа в систему.
Обновить информацию об устройстве	Нажмите  , чтобы обновить и получить последнюю информацию об устройстве.

9.3 Управление группами

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

Пример

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

9.3.1 Добавление группы

Добавьте группы для удобного управления устройствами.

Шаги

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



Примечание

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

9.3.2 Добавление ресурсов в группу

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

Перед началом

Добавьте группу для управления устройствами. Подробная информация представлена в разделе [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.

9.4 Управление сотрудниками / посетителями

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

9.4.1 Добавление организации

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

Шаги

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



Примечание

Можно добавить до 10 уровней организаций.

4. Опционально: выполните следующие операции.

Edit Organization

(«Изменение организации»)

Наведите указатель мыши на добавленную организацию и нажмите , чтобы изменить ее название.

Delete Organization

(«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.

Show Persons in

Sub Organization

(«Отображение персонала подчиненной организации»)

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

9.4.2 Настройка основной информации

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

Шаги

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



Примечание

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

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

Basic Information

* Person ID

* Name

Gender ☒ Male ☐ Female

Email

Tel.

Validity Period (Access Control)

Remark

Рисунок 9-4 Настройка основной информации



Примечание

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

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

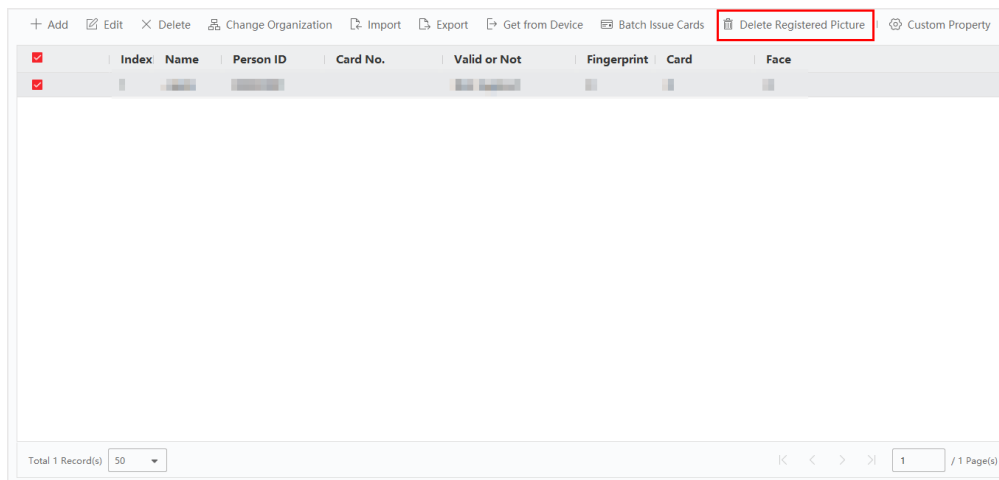


Рисунок 9-5 Удаление зарегистрированного изображения



Примечание

Если включен параметр **Save Pictures in Structure Data Format** («Сохранение изображений в формате структурированных данных»), на страницу пользователя будет добавлена кнопка **Delete Registered Picture** («Удалить зарегистрированное изображение»). Как правило, зарегистрированные изображения профиля сотрудника / посетителя будут автоматически удалены после того, как информация о сотруднике / посетителе будет применена к устройству. Дважды нажмите на профиль сотрудника, откроется окно **Edit Person** («Редактирование сотрудника»), в котором можно проверить, было ли удалено зарегистрированное изображение лица.

В противном случае можно выбрать сотрудника и нажать **Delete Registered Picture** («Удалить зарегистрированное изображение»), чтобы удалить изображение вручную.

9.4.3 Выпуск карт в локальном режиме

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

Шаги

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



Примечание

В первую очередь необходимо добавить основную информацию о пользователе. Подробная информация о настройке основной информации о пользователе представлена в разделе **Настройка основной информации**.



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

Card Enrollment Station («Настольный считыватель карт»)

Из раскрывающегося списка выберите модель настольного считывателя карт. Настольный считыватель карт можно подключить к ПК и передавать основную информацию о добавленном сотруднике между двумя устройствами через USB.



Примечание

Поддерживаемые в настоящее время модели считывателя карт: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, DS-K1F180-D8E, DS-K1F100A-D8E и настольный считыватель.

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 («Тональный генератор (бипер)»)

После успешного считывания номера карты включите или выключите бипер.

Card No. Type («Тип номера карты»)

Выберите необходимый тип номера карты.

M1 Card Encryption («Шифрование M1-карты»)

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

9.4.4 Сбор отпечатков пальцев с помощью клиента

Сбор отпечатков пальцев в локальном режиме значит, что можно выполнять сбор отпечатков пальцев с помощью настольного считывателя отпечатков пальцев, подключенного непосредственно к ПК, на котором запущен клиент. Зарегистрированные отпечатки пальцев могут быть использованы в качестве учетных данных для доступа к разрешенным дверям.

Перед началом

Подключите считыватель отпечатков пальцев к ПК, на котором работает клиент.

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. Подробная информация о настройке основной информации о пользователе представлена в разделе **Настройка основной информации**.

3. Внутри панели **Credential → Fingerprint** («Учетные данные → Отпечаток пальца») нажмите .
4. Во всплывающем окне выберите режим сбора **Local** («Локальный»).
5. Выберите модель подключенного считывателя отпечатков пальцев.



Примечание

При использовании настольного считывателя отпечатков пальцев DS-K1F800-F можно нажать **Settings** («Настройки»), чтобы выбрать COM-порт, к которому подключается настольный считыватель отпечатков пальцев.

6. Зарегистрируйте отпечаток пальца.

- 1) Нажмите **Start** («Начать»).
- 2) Поместите палец на считыватель отпечатков пальцев и сделайте отпечаток.
- 3) Нажмите **Add** («Добавить») для сохранения данных отпечатков пальцев.

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.
-



Примечание

После добавления отпечатка пальца его тип изменить нельзя.

9.4.5 Сбор отпечатков пальцев с помощью устройства контроля доступа

При добавлении сотрудника / посетителя можно добавить информацию об отпечатках пальцев через модуль считывания отпечатков пальцев устройства контроля доступа.

Зарегистрированные отпечатки пальцев могут быть использованы в качестве учетных данных для доступа к разрешенным дверям.

Перед началом

Убедитесь, что устройство контроля доступа поддерживает функцию сбора отпечатков пальцев.

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.

Подробная информация о настройке основной информации о пользователе представлена в разделе **Настройка основной информации**.



3. Внутри панели **Credential → Fingerprint** («Учетные данные → Отпечаток пальца») нажмите
 4. Во всплывающем окне выберите режим сбора **Remote** («Удаленный»).
 5. В раскрывающемся списке выберите устройство контроля доступа, которое поддерживает функцию считывания отпечатков пальцев.
 6. Зарегистрируйте отпечаток пальца.
 - 1) Нажмите **Start** («Начать»).
 - 2) Поместите палец на сканер отпечатков пальцев выбранного устройства контроля доступа, затем уберите палец.
 - 3) Нажмите **Add** («Добавить») для сохранения данных отпечатков пальцев.
-

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.



Примечание

После добавления отпечатка пальца его тип изменить нельзя.

9.4.6 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 Blocklist («Черный список») 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

Подробная информация представлена в разделе **Настройка группы контроля доступа для назначения разрешений на доступ..**

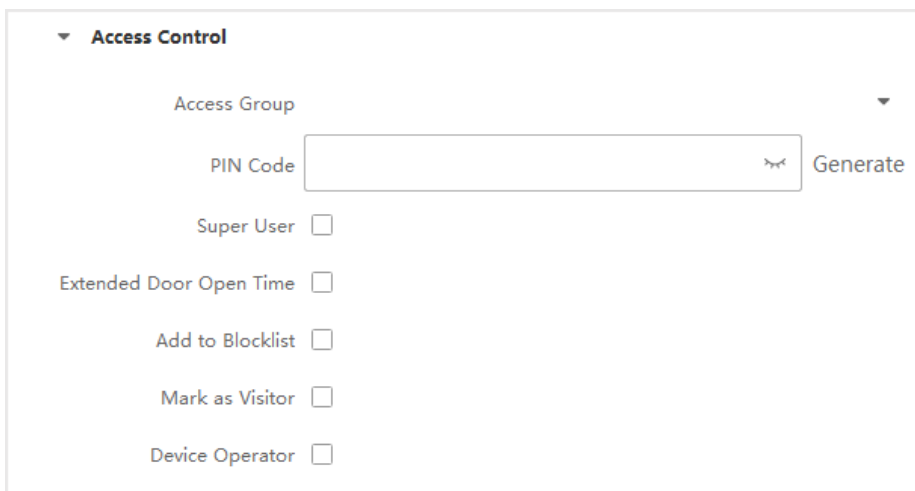


Рисунок 9-6 Настройка информации контроля доступа

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



Примечание

Не допускается дублирование PIN-кодов.

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



Примечание

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

5. Проверьте разрешения лица.

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. Подробная информация о настройке длительности открытой двери представлена в разделе **Настройка параметров двери**.

Add to Blacklist («Добавление в черный список»)

Добавьте человека в Blacklist («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.



Примечание

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

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 пользователь назначен в качестве суперпользователя, функции увеличенной продолжительности открытия двери, добавления в черный список и назначения в качестве посетителя будут недоступны.

6. Подтвердите, чтобы добавить пользователя.

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

9.4.7 Редактирование информации о сотруднике / посетителе

Доступна настройка свойств дополнительной информации о сотруднике, которая предварительно 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 / посетителя.
 - 1) Выберите организацию из списка и нажмите **Add** («Добавить»).



Примечание

В первую очередь необходимо добавить основную информацию о пользователе. Подробная информация о настройке основной информации о пользователе представлена в разделе **Настройка основной информации**.

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

9.4.8 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. Подробная информация о настройке основной информации о пользователе представлена в разделе **Настройка основной информации**.

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

9.4.9 Импорт и экспорт информации о сотруднике / посетителе

Можно импортировать информацию о нескольких пользователях в клиентское ПО в пакетном режиме. Также информацию о пользователях можно экспортировать и сохранить на компьютере.

9.4.10 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.
-

9.4.11 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.

9.4.12 Получение информации о пользователе с устройства контроля доступа

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

Шаги



Примечание

- Если в информации о пользователе, хранящейся на устройстве, в поле **Name** («Имя») не указаны данные, то это поле будет заполнено номером выданной карты после импорта в клиентское ПО.
- По умолчанию 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. Выберите **Getting Mode** («Режим получения»).



Примечание

Режим получения может различаться в зависимости от устройства. Устройство контроля доступа поддерживает получение личной информации о пользователе с помощью ID сотрудника. Могут быть указаны до 5 ID сотрудников.

-
6. 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, информацию об отпечатках пальцев (если настроены) и связанных картах (если настроены), будет импортирована в выбранную организацию.

9.4.13 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**.

9.4.14 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.
Подробная информация представлена в разделе *Выпуск карт в локальном режиме*.
5. Нажмите **Initialize** («Инициализировать»), чтобы инициализировать считыватель карт и подготовить его к выдаче карт.
6. Нажмите на колонку **Card No.** («Номер карты») и введите номер карты.
 - Поместите карту на настольный считыватель.
 - Считайте карту через считыватель карт.
 - Вручную введите номер карты и нажмите клавишу ввода **Enter**. Карты будут выпущены для пользователей, отображаемых в списке.

9.4.15 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 пользователь, он не сможет получить доступ к дверям, используя 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 добавлена в группу доступа, которая применена к устройству, после сообщения об утере карты или отмене уведомления об утере карты появится окно с уведомлением о необходимости применить изменения к устройству. После применения к устройству эти изменения будут задействованы на устройстве.

9.4.16 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 используется настольный считыватель DS-K1F180-D8E.

Card Type («Тип карты»)

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

Buzzing («Тональный генератор (бипер)»)

После успешного считывания номера карты включите или выключите бипер.

Card No. Type («Тип номера карты»)

Выберите необходимый тип номера карты.

M1 Card Encryption («Шифрование M1-карты»)

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

Удаленный режим: выпуск карт с помощью считывателя карт

Выберите устройство контроля доступа, добавленное в клиент, и считайте карту через считыватель карт, чтобы получить ее номер.

9.5 Настройка графиков и шаблонов

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

Примечание

Подробная информация о настройке группы контроля доступа представлена в разделе **Настройка группы контроля доступа для назначения разрешений на доступ**.

9.5.1 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 курсор в необходимое положение.
 - Наведите курсор на временную шкалу и измените время начала / окончания периода в появившемся диалоговом окне.
 - Когда вид курсора изменится на , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
- 4) **Опционально:** выберите отрезок времени, который необходимо удалить, а затем щелкните  столбец Operation («Операции»), чтобы удалить его.
 - 5) **Опционально:** нажмите кнопку , чтобы удалить все отрезки времени нерабочих дней.
 - 6) **Опционально:** или нажмите кнопку , чтобы удалить конкретный нерабочий день.
6. Нажмите **Save** («Сохранить»).

9.5.2 Добавление шаблона

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

Шаги

Примечание

Можно добавить до 255 шаблонов.

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

Примечание

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

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 курсор в необходимое положение.
 - Наведите курсор на временную шкалу и измените время начала / окончания периода в появившемся диалоговом окне.
 - Когда вид курсора изменится на , переместите курсор в начало или конец временной шкалы, чтобы увеличить или уменьшить продолжительность периода.
- 4) Повторите два последних действия выше, чтобы задать несколько временных интервалов в другие дни недели.
6. Добавьте выходной день и примените его к шаблону.



Примечание

В один шаблон можно добавить до 4 выходных дней.

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



Примечание

Подробная информация о добавлении выходных представлена в разделе **Добавление выходных**.

- 4) **Опционально:** выберите выходной день из списка справа и нажмите , чтобы удалить его, или нажмите **Clear** («Очистить»), чтобы удалить все выбранные выходные дни из списка справа.
7. Нажмите **Save** («Сохранить») для сохранения настроек и завершите добавление шаблона.

9.6 Настройка группы контроля доступа для назначения разрешений на доступ

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

Перед началом

- Добавьте сотрудника / посетителя в клиент.
- Добавьте устройство контроля доступа в клиент и групповые точки доступа. Подробная информация представлена в разделе **Управление группами**.
- Добавьте шаблон.

Шаги

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

1. Нажмите **Access Control** → **Authorization** → **Access Group** («Контроль доступа → Авторизация → Группа доступа»), чтобы перейти на соответствующую страницу.

2. Нажмите **Add** («Добавить»), чтобы открыть окно добавления устройства.
3. В текстовом поле **Name** («Имя») введите имя для группы доступа по своему выбору.
4. Выберите шаблон для группы доступа.



Примечание

Необходимо настроить шаблон перед настройкой группы доступа. Подробная информация представлена в разделе [Настройка графиков и шаблонов](#).

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

Выбранные пользователи и точки доступа отображаются в правой части экрана.

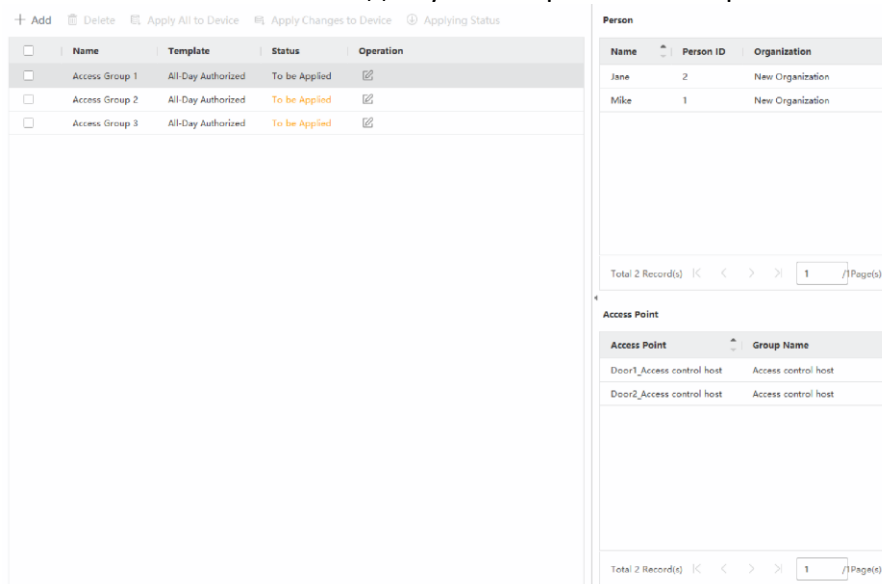


Рисунок 9-7. Отображение выбранных пользователей и точек доступа

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

Применить к устройствам

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

Применить изменения к устройствам\

Операция не очистит группы доступа, привязанные к выбранным устройствам, и применит только измененную часть выбранных групп доступа к устройству.

- 4) Присвоенный статус отображается в столбце Status («Статус»). Также можно нажать **Applying Status** («Присвоенный статус»), чтобы просмотреть все примененные группы доступа.



Примечание

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

Выбранные пользователи будут иметь разрешения на вход/выход через выбранные двери / вызывные панели при помощи привязанных карт или отпечатков пальцев.

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»).

9.7 Настройка расширенных функций

Настройте расширенные функции контроля доступа в соответствии со сценой наблюдения.



Примечание

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

9.7.1 Настройка параметров устройства

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

Настройка параметров устройства контроля доступа

После добавления устройства контроля доступа можно настроить его параметры, в том числе наложить пользовательскую информацию на изображение, загрузить изображения после захвата, сохранить захваченные изображения и т. д.

Перед началом

Добавьте устройство контроля доступа в клиент.

Шаги

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



Примечание

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

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



Примечание

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

RS-485 Comm. Redundancy («Резервирование связи RS-485»)

Можно включить функцию RS-485 Communication Redundancy («Резервирование связи RS-485») при подключении карты RS-485 к устройству контроля доступа с резервированием.

Display Detected Face («Отображение обнаруженного лица»)

Отображение изображений лиц при аутентификации.

Display Card Number («Отображение номера карты»)

Отображение информации о карте при аутентификации.

Display Person Information («Отображение информации о сотруднике»)

Отображение информации о сотруднике при аутентификации.

Overlay Person Info. on Picture («Наложение информации о сотруднике на изображении»)

Отображение информации о сотруднике на изображении.

Voice Prompt («Голосовое предупреждение»)

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

Download Pic. After Linked Capture («Сохранение 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.

Press Key to Enter Card Number («Нажмите кнопку, чтобы ввести номер карты»)

Если функция включена, можно ввести номер карты, нажав кнопку.

Wi-Fi Probe («Зонд Wi-Fi»)

Если функция включена, устройство может проверить MAC-адрес окружающих устройств связи и загрузить MAC-адрес в систему. Если MAC-адрес совпадает с указанным MAC-адресом, система может инициировать некоторые действия привязки.

3G / 4G

Если функция включена, устройство сможет работать в сети 3G / 4G.

NFC Anti-Cloning («Предотвращение копирования NFC-карт»)

Если функция включена, можно использовать копированную карту для аутентификации и дальнейшего повышения безопасности.

4. Нажмите **OK**.

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

Настройка параметров двери

После добавления устройства контроля доступа можно настроить параметры точки доступа.

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 выбранного устройства.
3. Выберите дверь, чтобы отобразить 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 («Название»)

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.

Door 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».

Super Password («Суперпароль»)

Пользователь может открыть дверь с помощью суперпароля.

Extended Open Duration («Расширенная длительность открытого состояния»)

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

Duress Code («Код принуждения»)

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

Dismiss Code («Код отклонения»)

Создайте код отклонения, который можно использовать для отключения зуммера считывателя карт (путем ввода кода отклонения на клавиатуре).



Примечание

- Код отклонения, суперпароль и код принуждения должны отличаться.
- Код отклонения, суперпароль и код принуждения должны отличаться от пароля аутентификации.
- Длина кода отклонения, суперпароля и кода принуждения должна быть установлена устройством. Обычно пароль должен содержать от 4 до 8 цифр.

5. Нажмите **ОК**.

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



Примечание

Настройки длительности состояния двери также будут скопированы в выбранную дверь.

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. Подробная информация представлена в руководстве пользователя устройства.
- Некоторые из следующих параметров не перечислены на странице Basic Information («Основная информация»), нажмите **More** («Дополнительная информация»), чтобы изменить параметры.

Name («Название»)

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.

Max. Times of Card Failure («Максимальное количество сбоев при считывании карты»)

Установите максимальное количество неудачных попыток считывания карты.

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

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

Default Authentication Mode («Режим аутентификации по умолчанию»)

Отображение режима аутентификации при помощи считывателя карт по умолчанию.

Fingerprint Capacity («Макс. количество сохраненных отпечатков пальцев»)

Просмотр максимального количества доступных отпечатков пальцев.

Existing Fingerprint Number («Количество зарегистрированных отпечатков пальцев»)

Просмотр количества зарегистрированных отпечатков пальцев на устройстве.

4. Нажмите **Advanced** («Расширенные настройки») и настройте другие параметры.

Enable Card Reader («Включить считыватель карт»)

Включите функцию для их использования на считывателе карт.

OK LED Polarity/Error LED Polarity/Buzzer Polarity («Правильная полярность светодиода / Ошибочная полярность светодиода / Полярность бипера»)

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

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.

Fingerprint Recognition Level («Уровень распознавания отпечатков пальцев»)

Выберите уровень распознавания отпечатков пальцев из выпадающего списка.

Fingerprint Recognition Interval («Интервал распознавания отпечатков пальцев»)

Выберите интервал распознавания отпечатков пальцев из выпадающего списка.

5. Нажмите **OK**.

6. **Опционально:** нажмите **Copy to** («Копировать в...») 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.

Перед началом

Добавьте устройство контроля доступа в клиент и убедитесь, что устройство поддерживает тревожный выход.

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 («Название»)

Выберите наименование считывателя карт по своему выбору.

Alarm Output Active Time («Время работы тревожного выхода»)

Время работы тревожного выхода после активации.

4. Нажмите **ОК**.

5. **Опционально:** установите переключатель в верхнем правом углу в положение ON («Вкл.»), чтобы активировать тревожный выход.

9.7.2 Настройка состояния двери «оставить заблокированной» / «разблокированной»

Настройте состояние двери как «разблокирована» или «заблокирована», а также настройте контроллер лифта как «свободный» и «контролируемый». Например, можно перевести дверь в состояние «заблокирована» в праздничные дни, или в состояние «разблокирована» в указанный рабочий день.

Перед началом

Добавьте устройство контроля доступа в систему.

Шаги

1. Нажмите **Access Control → Advanced Function → Remain Locked/Unlocked** («Контроль доступа → Расширенные функции → Оставить заблокированной / разблокированной»), чтобы перейти на соответствующую страницу.
2. На панели слева выберите дверь и контроллер лифта, которые необходимо настроить.
3. Для настройки контроллера лифта и двери в течение рабочего дня нажмите **Week Schedule** («График рабочей недели») и выполните следующие действия.
 - 1) Нажмите **Remain Unlocked** («Оставить разблокированным») или **Remain Locked** («Оставить заблокированным»).
 - 2) Для контроллера лифта выберите значение: **Free** («Свободный») или **Controlled** («Контролируемый»).
 - 3) 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.

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

5) 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 Unlocked** («Оставить разблокированным») или **Remain Locked** («Оставить заблокированным»).

2) Нажмите **Add** («Добавить»).

3) Введите дату начала и дату окончания периода.

4) Двигайте курсор, чтобы указать временной интервал. Для данного периода времени будет активировано настроенное разрешение.



Примечание

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

5) Для изменения временных интервалов выполните следующие действия.

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

6) **Опционально:** выберите отрезок времени, который необходимо удалить, а затем 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.

9.7.3 Настройка правила Wiegand

Основываясь на знании правил загрузки для стороннего Wiegand, можно установить несколько настраиваемых правил Wiegand для связи между устройством и сторонними считывателями карт.

Перед началом

Подключите сторонние считыватели карт к устройству.

Шаги

Примечание

- По умолчанию устройство отключает настраиваемую функцию Wiegand. Если устройство включает настраиваемую функцию Wiegand, все интерфейсы Wiegand в устройстве будут использовать настроенный протокол Wiegand.
- Можно установить до 5 Wiegand.
- Подробная информация о настраиваемом Wiegand представлена в разделе Описание настраиваемых правил Wiegand.

1. Нажмите **Access Control** → **Advanced Function** → **Custom Wiegand** («Контроль доступа → Расширенные функции → Настраиваемый Wiegand»), чтобы перейти на соответствующую страницу.
2. Выберите настраиваемый Wiegand слева.
3. Создайте имя для Wiegand.

Примечание

Имя настраиваемого Wiegand может содержать до 32 символов.

4. Нажмите **Select Device** («Выбрать устройство»), чтобы выбрать устройство контроля доступа для настройки пользовательского интерфейса Wiegand.
5. Установите режим четности в соответствии со свойством стороннего считывателя карт.

Примечание

- Общая длина допускается до 80 бит.
 - Старт-бит и длина нечетности, и старт-бит и длина четности находятся в диапазоне от 1 до 80 бит.
 - Старт-бит ID карты, кода производителя, кода сайта и производителя оборудования должны находиться в диапазоне от 1 до 80 бит.
6. Установите правило преобразования выходного сигнала.
 - 1) Нажмите **Set Rule** («Установить правило»), чтобы открыть окно установки правила преобразования выходного сигнала.
 - 2) Выберите правила в левом списке.
Выбранные правила будут добавлены в правый список.
 - 3) **Опционально:** перетащите правила, чтобы изменить их порядок.
 - 4) Нажмите **ОК**.
 - 5) На вкладке настраиваемого Wiegand установите старт-бит правила, длину и десятичную цифру.
 7. Нажмите **Save** («Сохранить»).

9.7.4 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»).

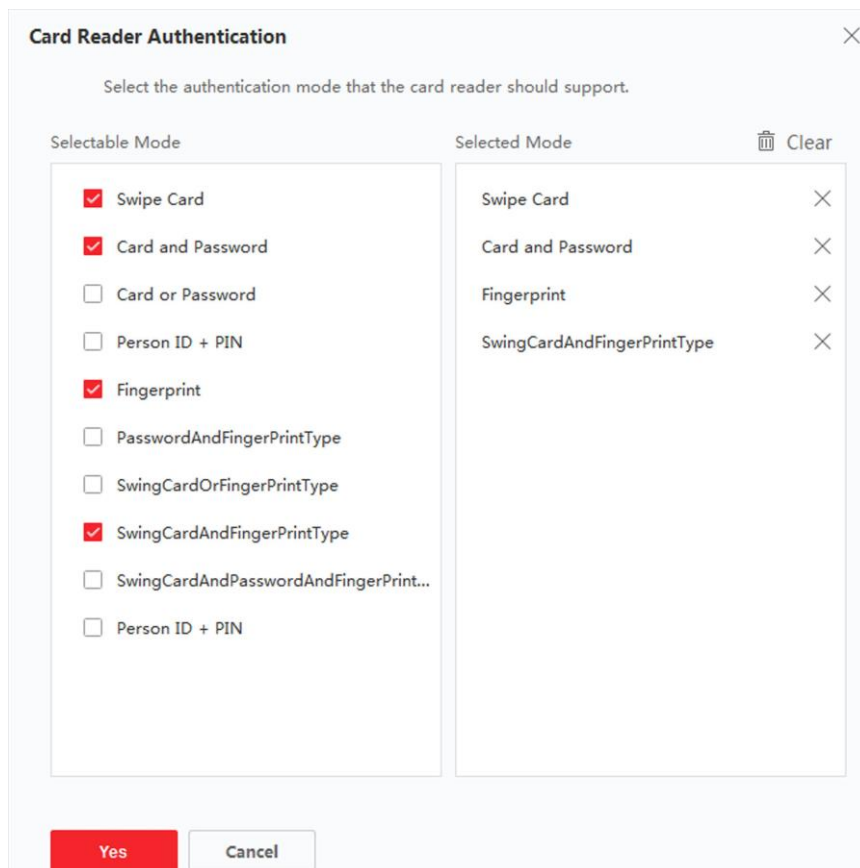


Рисунок 9-8 Выбор режима аутентификации для считывателя карт



Примечание

PIN означает PIN-код, установленный для разблокировки двери. Подробная информация представлена в разделе **Настройка информации о контроле доступа**.

- 2) Выберите режим из списка доступных режимов, чтобы добавить его в список выбранных режимов.
- 3) Нажмите **ОК**.
После завершения процедуры выбора режимов они будут отображаться на экране в виде значков.
4. Нажмите на значок, чтобы выбрать режим аутентификации устройства для считывания карт. Проведите курсором мыши по определенному дню, чтобы нарисовать цветную полосу в графике. Это значит, что в данный отрезок времени будет использоваться аутентификация при помощи устройства для считывания карт.

5. Повторите этот шаг для установки других отрезков времени.

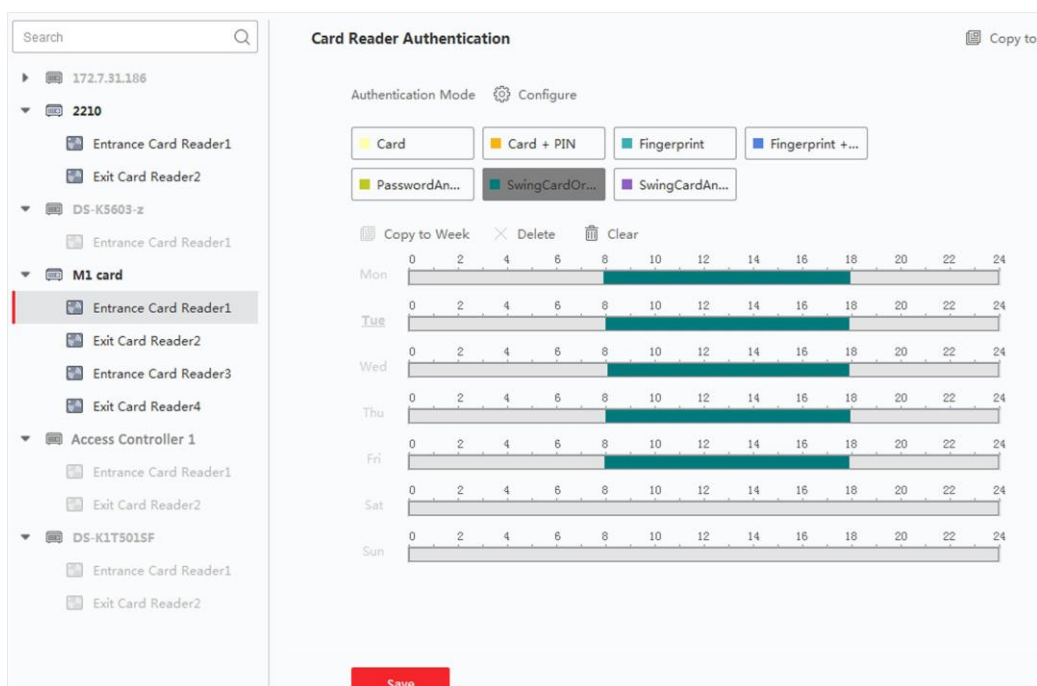


Рисунок 9-9 Настройка режима аутентификации для считывателей карт

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

9.7.5 Настройка параметров устройства

После добавления устройства контроля доступа можно настроить параметры его сети.

Настройка параметров сети

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

Настройка режима загрузки журнала

Настройте режим загрузки журнала через протокол ISUP.

Шаги

Примечание

Убедитесь, что устройство не добавлено по протоколу ISUP.

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.
 - N1 относится к проводной сети.
-

7. Нажмите **Save** («Сохранить»).

Создание учетной записи EHome через проводную сеть

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

Шаги



Примечание

- Устройство должно поддерживать данную функцию.
 - Убедитесь, что устройство не добавлено по протоколу EHome.
-

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 EHome.

8. Выберите EHome в поле Protocol Type («Тип протокола») и выберите версию EHome.



Примечание

При EHome версии **5.0** необходимо создать ключ EHome для учетной записи EHome.

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

Включить Шифрование M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

Шаги

Примечание

Эта функция должна поддерживаться устройством контроля доступа и считывателем карт.

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

Примечание

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

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

Настройка параметров 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.

Перед началом

Добавьте устройство контроля доступа в клиент и убедитесь, что устройство поддерживает RS-485.

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 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 настройке **Communication Direction** («Направление связи») в качестве **Sending** («Отправка»), необходимо установить режим Wiegand в значение **Wiegand 26, Wiegand 34, Wiegand 27, или Wiegand 35**.

6. Нажмите **Save** («Сохранить»).

- Настроенные параметры будут автоматически применены к устройству.
- После изменения направления коммуникации устройство автоматически перезагрузится.

9.8 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:

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

9.8.1 Настройка действий на клиентском ПО при событии доступа

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

Перед началом

Добавьте устройство контроля доступа в клиент.

Шаги

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

Audible Warning («Звуковое предупреждение»)

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



Примечание

Подробная информация о настройке звукового сигнала тревоги представлена в разделе **Настройка звукового сигнала** Руководства пользователя клиентского программного обеспечения.

Send Email («Отправка Email»)

Отправьте уведомление о тревожном событии на электронную почту одному или нескольким получателям.

Подробная информация о настройке параметров электронной почты представлена в разделе *Настройка параметров электронной почты* Руководства пользователя клиентского программного обеспечения.

2) Нажмите **ОК**.

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

9.8.2 Настройка действий устройства при событии доступа

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

Устройство должно поддерживать данную функцию.

1. Нажмите **Access Control** → **Linkage Configuration** («Контроль доступа → Конфигурация привязки»).
2. Выберите устройство контроля доступа из списка слева.
3. Нажмите кнопку **Add** («Добавить») для добавления новой привязки.
4. Вы можете выбрать в качестве **Event source** («Источник события») значение **Event Linkage** («Привязка события»).
5. выберите тип и описание события, чтобы установить привязку.
6. В области **Linkage Target** («Привязка цели») установите цель, чтобы включить соответствующее действие.
Buzzer on Controller («Бипер контроллера») — Устройство контроля доступа выдаст звуковое предупреждение.
7. Нажмите **Save** («Сохранить»).
8. **Опционально:** после привязки нескольких устройств можно выполнить одно или несколько из следующих действий:

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

9.8.3 Настройка действий устройства при считывании карт

Установите привязанные действия устройства контроля доступа при возникновении события доступа. Считывание определенной карты может инициировать срабатывание тревожного выхода, бипера хоста и другие действия устройства.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

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

Buzzer on Controller («Бипер контроллера»)

Устройство контроля доступа выдаст звуковое предупреждение.

Buzzer on Reader («Бипер считывателя карт»)

Считыватель карт выдаст звуковое предупреждение.

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:

Edit Linkage Settings

(«Изменение настроек привязки»)

Выберите настроенные параметры привязки из списка устройств. Измените параметры события, в том числе источник события и цель привязки.

Delete Linkage Settings

(«Удаление настроек привязки»)

Выберите настроенные параметры привязки из списка устройств и нажмите **Delete** («Удалить»), чтобы удалить их.

9.8.4 Настройка действий устройства для идентификатора пользователя

Установите привязанные действия устройства контроля доступа для конкретного идентификатора пользователя. Когда устройство контроля доступа обнаруживает указанный идентификатор сотрудника, оно может активировать тревожный выход, бипер хоста и другие действия на том же устройстве.

Шаги

 Примечание

Устройство должно поддерживать данную функцию.

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

Buzzer on Controller («Бипер контроллера»)

Устройство контроля доступа выдаст звуковое предупреждение.

Buzzer on Reader («Бипер считывателя карт»)

Считыватель карт выдаст звуковое предупреждение.

8. Нажмите **Save** («Сохранить»).

9. **Опционально:** после привязки нескольких устройств можно выполнить одно или несколько из следующих действий:

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

9.9 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 дверью, 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 дверью. Для других пользователей панель управления устройством отображаться не будет. Для настройки разрешения пользователя обратитесь к разделу **Управление сотрудниками / посетителями**.

9.9.1 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

Подробная информация об управлении группой точек доступа представлена в разделе **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.

Open Door («Открыть дверь»)

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

Close Door («Закрыть дверь»)

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

Remain Open («Оставить дверь открытой»)

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

Remain Closed («Оставить дверь закрытой»)

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

Capture («Захват»)

Захват изображения вручную.



Примечание

Кнопка **Capture** («Захват») доступна, когда устройство поддерживает функцию захвата изображений. Изображение сохраняется на компьютере, на котором работает клиентское ПО. Подробная информация о настройке параметров сохранения представлена в разделе *Настройка звукового сигнала* руководства пользователя клиентского программного обеспечения.

Результат

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

9.9.2 Запись информации о считывании карт в режиме реального времени

Записи доступа будут отображаться в режиме реального времени, включая записи считывания карт, записи сравнения отпечатков пальцев и т. д. Можно просмотреть информацию о сотруднике / посетителях и просмотреть изображение, сделанное во время получения 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.

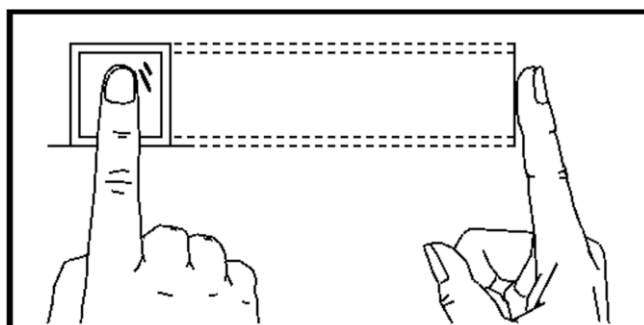
Приложение А. Советы по сканированию отпечатков пальцев

Рекомендуемый палец

Рекомендуется использовать большой, указательный или средний палец.

Правильное сканирование

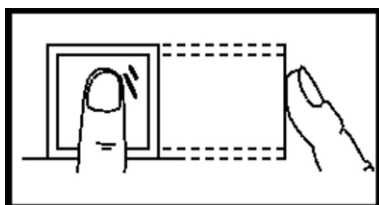
На рисунке ниже показан правильный способ сканирования пальца:



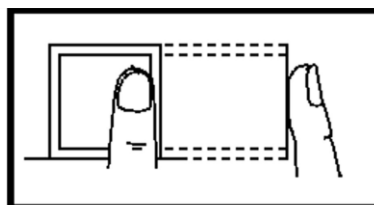
Необходимо прижать палец к сканеру горизонтально. Центр сканируемого пальца должен совпадать с центром сканера.

Неправильное сканирование

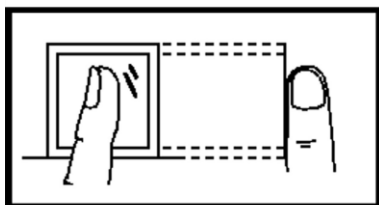
Приведенные ниже рисунки показывают неверные способы сканирования отпечатков пальцев:



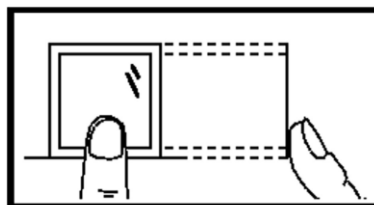
Vertical



Edge I



Side



Edge II

Окружающая среда

Сканер должен быть расположен в месте, защищенном от воздействия прямых солнечных лучей, высоких температур, влаги и дождя. Когда палец очень сухой, сканер может не распознать отпечаток пальца. Можно подуть на палец и снова приложить его к сканеру.

Прочее

При неглубоком отпечатке пальца или сложностях при сканировании, рекомендуется использовать другие методы аутентификации.

Сканер может не распознать отпечаток при наличии травм на сканируемом пальце. Можно использовать другой палец и повторить попытку снова.

Приложение В. Размеры

Размеры устройства

