



Терминал доступа с функцией
распознавания лиц
F-KD-3322

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	Дополнительная информация для дополнения важных моментов основного текста.

Регулирующая информация

Информация о FCC

Обратите внимание, что изменения или модификации, не одобренные явно стороной, ответственной за соответствие, могут 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 достаточную 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 использовать 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. Данное устройство должно выдерживать возможные помехи, включая те, которые могут привести к выполнению нежелательных операций.

Соответствие стандартам ЕС



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



2012/19/ЕС (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. Подробная информация о батарее изложена в документации продукта. Батарея отмечена значком, который может включать наименования, обозначающие содержание 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 любого из предупреждений может привести к серьезным 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.

Предупреждения:

- Использование продукта должно строго соответствовать нормам электробезопасности страны и региона.
- Не подключайте несколько устройств к одному блоку питания, перегрузка адаптера может привести к перегреву или возгоранию.
- Если из устройства идет дым или доносится шум — отключите питание, извлеките кабель и свяжитесь с сервисным центром.
- Розетка должна быть установлена рядом с оборудованием и быть легко доступной.
- Не проглатывайте батарейку. 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 отсек для батареи закрывается ненадежно, прекратите использование продукта и храните его в недоступном для детей месте.
- В случае проглатывания батареи или ее перемещения в какую-либо часть тела, немедленно обратитесь за медицинской помощью.
- ПРЕДОСТЕРЕЖЕНИЕ. При замене батареи батареей несоответствующего типа, существует риск взрыва.
- Замена батареи на батарею несоответствующего типа может привести к нарушению мер предосторожности (например, в случае некоторых типов литиевых батарей).
- Запрещено помещать батарею в огонь или работающий духовой шкаф, разбивать и или резать батарею, так как это может привести к взрыву.

- Запрещено оставлять батарею в окружающей среде при очень высоких температурах, так как это может привести к взрыву или утечке горючей жидкости или газа.
- Запрещено подвергать батарею воздействию крайне низкого давления воздуха, так как это может привести к взрыву или утечке горючей жидкости или газа.
- Использованные батареи необходимо утилизировать в соответствии с инструкциями.

Предостережения

- Запрещено ронять устройство и подвергать воздействию сильных электромагнитных помех. Избегайте установки устройства на вибрирующую поверхность или в местах, подверженных ударам (пренебрежение этим предостережением может привести к повреждению устройства).
- Запрещено размещать устройство в местах с чрезвычайно высокой или низкой температурой окружающей среды (подробная информация о рабочей температуре представлена в спецификации устройства), в пыльной или влажной среде, запрещено подвергать устройство воздействию сильных электромагнитных помех.
- Не подвергайте 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).
- 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).

- Для очистки внутренних и внешних поверхностей крышки устройства используйте мягкую и сухую ткань, не используйте щелочные моющие средства.
- Биометрические системы аутентификации не могут гарантировать абсолютную защиту от подделки биометрических данных. Если требуется более высокий уровень безопасности, используйте несколько режимов аутентификации.
- Серийный интерфейс используется только для отладки.
- Установите оборудование в соответствии с инструкциями в этом руководстве. Во избежание травм оборудование должно быть надежно установлено на пол / стену в соответствии с инструкциями.
- 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.
- Этот кронштейн предназначен для использования только с оборудованными устройствами. Использование с другим оборудованием может привести к нестабильности и травмам.
- Данное оборудование предназначено для использования с оснаренным кронштейном. Использование с другими устройствами (тележками, подставками или держателями) может привести к нестабильности и травмам.

Доступные модели

Используйте только те источники питания, которые указаны ниже:

Модель	Производитель	Стандарт
F-KD-3322	Shenzhen Honor Electronic Co., Ltd	PG

Содержание

Раздел 1 Представление продукта 1

1.1 Представление продукта 1

1.2 Особенности 1

Раздел 2 Внешний вид устройства 3

Раздел 3 Установка 6

3.1 Среда установки 6

3.2 Установка с использованием монтажной коробки 6

3.3 Накладная установка 9

3.4 Установка на кронштейн 13

3.4.1 Подготовка перед установкой на кронштейн 14

3.4.2 Кронштейн 15

3.5 Установка на цилиндрический кронштейн 16

3.5.1 Подготовка перед установкой на кронштейн 16

3.5.2 Крепление цилиндрического кронштейна 18

Раздел 4 Подключение 20

4.1 Описание разъемов 20

4.2 Подключение устройства (стандартный режим) 21

4.3 Подключение к модулю безопасности двери 22

4.4 Подключение модуля пожарной тревоги 23

4.4.1 Схема подключения типа безопасности «Дверь остается открытой при отключении питания» 23

4.4.2 Схема подключения типа безопасности «Дверь закрывается при отключении питания» 25

Раздел 5 Активация устройства	27
5.1 Активация через устройство	27
5.2 Активация через веб-интерфейс	30
5.3 Активация через ПО SADP	31
5.4 Активация устройства при помощи клиентского ПО iVMS-4200	34
Раздел 6 Быстрые операции	36
6.1 Выбор языка	36
6.2 Настройка типа изменения пароля	37
6.3 Настройка параметров сети	37
6.4 Доступ к платформе	39
6.5 Настройки конфиденциальности	40
6.6 Настройка роли администратора	41
Раздел 7 Основные операции	45
7.1 Вход в систему	45
7.1.1 Вход в систему в качестве администратора	45
7.1.2 Вход в систему с использованием пароля активации	46
7.1.3 Забыть пароль	48
7.2 Настройка связи	49
7.2.1 Настройка параметров проводной сети	50
7.2.2 Настройка параметров Wi-Fi	52
7.2.3 Настройка параметров RS-485	54
7.2.4 Настройка параметров интерфейса Wiegand	56
7.2.5 Настройка параметров ISUP	57
7.2.6 Доступ к платформе	59

7.2.7 Настройки SNMP	60
7.3 Управление пользователями	60
7.3.1 Добавление администратора	60
7.3.2 Добавление изображения лица	63
7.3.3 Добавление отпечатков пальцев	66
7.3.4 Добавление карты	68
7.3.5 Добавление PIN-кода	70
7.3.6 Настройка режима аутентификации	73
7.3.7 Поиск и изменение параметров пользователя	74
7.4 Настройка учета рабочего времени (УРВ)	74
7.4.1 Отключение функции учета рабочего времени через устройство	75
7.4.2 Настройка подсчета результатов УРВ вручную через устройство	76
7.4.3 Настройка параметров автоматического учета рабочего времени через устройство	78
7.4.4 Настройка параметров автоматического УРВ и УРВ вручную через устройство	80
7.5 Управление данными	83
7.5.1 Удаление данных	83
7.5.2 Импорт данных	83
7.5.3 Экспорт данных	84
7.6 Идентификация личности	86
7.6.1 Аутентификация с помощью одного типа учетных данных	86
7.6.2 Аутентификация с помощью нескольких типов учетных данных	87
7.7 Основные настройки	88

7.8 Настройка биометрических параметров	91
7.9 Пользовательские настройки	96
7.10 Изменение пароля устройства	99
7.11 Настройки параметров аутентификации	100
7.12 Обслуживание системы	104
Раздел 8 Настройка устройства через мобильный интерфейс	109
8.1 Вход в систему	109
8.2 Обзор	109
8.3 Забыть пароль	110
8.4 Настройка	110
8.4.1 Отображение информации об устройстве	110
8.4.2 Настройка времени	111
8.4.3 Настройка параметров DST	112
8.4.4 Управление пользователями	112
8.4.5 Настройка сетевых параметров	113
8.4.6 Управление пользователями	118
8.4.7 Поиск событий	121
8.4.8 Настройки параметров контроля доступа	121
8.4.9 Настройка видеодомофонии	127
8.4.10 Настройки параметров аудио	131
8.4.11 Настройки параметров лица	132
8.4.12 Настройка параметров конфиденциальности	135
8.4.13 Режим пароля	137
8.4.14 Обновление и техническое обслуживание	137

8.4.15	Просмотр документации онлайн	138
8.4.16	Просмотр лицензии на ПО с открытым исходным кодом	138
Раздел 9 Быстрые операции через веб-интерфейс		139
9.1	Изменение пароля	139
9.2	Выбор языка	139
9.3	Настройка времени	139
9.4	Настройки параметров конфиденциальности	140
9.5	Настройки администратора	141
9.6	Настройка номеров и сетевые настройки	142
Глава 10 Работа через веб-интерфейс		145
10.1	Вход в систему	145
10.2	Забыть пароль	145
10.3	Справка	146
10.3.1	Лицензия на ПО с открытым исходным кодом	146
10.3.2	Просмотр онлайн справки	146
10.4	Выход из системы	146
10.5	Быстрые операции через веб-интерфейс	146
10.5.1	Изменение пароля	146
10.5.2	Выбор языка	147
10.5.3	Настройки времени	147
10.5.4	Настройки конфиденциальности	148
10.5.5	Настройки учетной записи администратора	149
10.5.6	Настройка номеров и сетевые настройки	150
10.6	Управление сотрудниками / посетителями	152

10.7 Обзор	156
10.8 Приложения контроля доступа	158
10.8.1 Настройки запрета двойного прохода.	158
10.8.2 Настройка блокировки нескольких дверей	159
10.9 Управление контролем доступа	160
10.9.1 Поиск событий	160
10.9.2 Конфигурация параметров двери	160
10.9.3 Настройка параметров аутентификации	166
10.9.4 Настройка привязки аутентификации	174
10.9.5 Настройка плана аутентификации	175
10.9.6 Настройка параметров распознавания лиц	175
10.9.7 Настройки параметров карты	184
10.9.8 Настройка удаленной проверки	187
10.9.9 Настройки конфиденциальности	188
10.9.10 Настройки вызова	192
10.10 Управление устройством	198
10.11 Конфигурация системы	199
10.11.1 Просмотр информации об устройстве через веб-интерфейс ПК	199
10.11.2 Настройка времени	200
10.11.3 Изменение пароля администратора	202
10.11.4 Настройки безопасности учетной записи через веб-интерфейс ПК	202
10.11.5 Просмотр информации о постановке / снятии устройства с охраны через веб-интерфейс ПК	203

10.11.6 Настройка рабочего режима через веб-интерфейс ПК	203
10.11.7 Настройка сетевых параметров	204
10.11.8 Настройка параметров видео и аудио через веб-интерфейс ПК	212
10.11.9 Конфигурация доступа	213
10.11.10 Настройка параметров изображения	215
10.11.11 Настройки привязки	218
10.11.12 Настройка учета рабочего времени (УРВ)	219
10.12 Пользовательские настройки	223
10.12.1 Настройка изображения в режиме ожидания через веб-интерфейс ПК	223
10.12.2 Настройка спящего режима через веб-интерфейс ПК	224
10.12.3 Настройка панели аутентификации через веб-интерфейс ПК	224
10.12.4 Настройка отображения уведомлений через веб-интерфейс ПК	226
10.12.5 Настройка расписания подсказок через веб-интерфейс ПК	228
10.12.6 Настройка голосовых подсказок через веб-интерфейс ПК	230
10.12.7 Настройка текста результата аутентификации через веб-интерфейс ПК	230
10.13 Система и обслуживание	231
10.13.1 Перезагрузка	231
10.13.2 Обновление	231
10.13.3 Восстановление настроек	232
10.13.4 Экспорт параметров устройства через веб-интерфейс ПК	234
10.13.5 Импорт параметров устройства через веб-интерфейс ПК	234

10.13.6 Отладка устройства	235
10.13.7 Просмотр журнала через веб-интерфейс ПК	238
10.13.8 Расширенные настройки через веб-интерфейс ПК	239
10.13.9 Управление безопасностью	240
10.13.10 Управление сертификатами	240
Раздел 11 Другие платформы	243
А. Рекомендации по сканированию отпечатков пальцев	244
Б. Советы по сбору/сравнению изображений лиц	246
В. Рекомендации по среде установки	248
Г. Размеры	249

Раздел 1 Представление продукта

1.1 Представление продукта

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

1.2 Особенности

- 4.3" сенсорный LCD-экран, разрешение экрана 272 × 480, обнаружение в режиме реального времени и отображение максимальной рамки лица.
- 2 Мп, 2 широкоугольных объектива
- Несколько режимов аутентификации: аутентификация по лицу / карте / отпечаткам пальцев / пин-коду и комбинации методов.
- Управление периодом контроля доступа (шаблон плана) и открытие дверей по требованию.
- Работа от сети и выдача полномочий для персонала через платформу.
- Функция загрузки данных по сети, которая позволяет загружать результаты сравнения данных и полученных изображений на платформу в режиме реального времени.
- Если устройство находится в режиме офлайн, события доступа будут загружены на платформу, когда устройство подключится к сети.
- NTP, калибровка времени вручную и автоматически.
- Видеодомофония между устройствами.
- Удаленный просмотр видео и вывод потоков видеокода по протоколу RTSP.
- Функция сторожевого таймера, конструкция тампера для обеспечения правильной работы устройства.
- Детекция наличия / отсутствия маски, включая напоминание о необходимости ношения маски и предупреждение об обязательном ношении.

- Степень защиты IP65.
- Питание осуществляется по стандартному PoE, а также одновременно обеспечивает питание дверного замка (DC 12 В / 1 А).

 Примечание

Эту функцию доступна только для устройств с поддержкой PoE.

Раздел 2 Внешний вид устройства

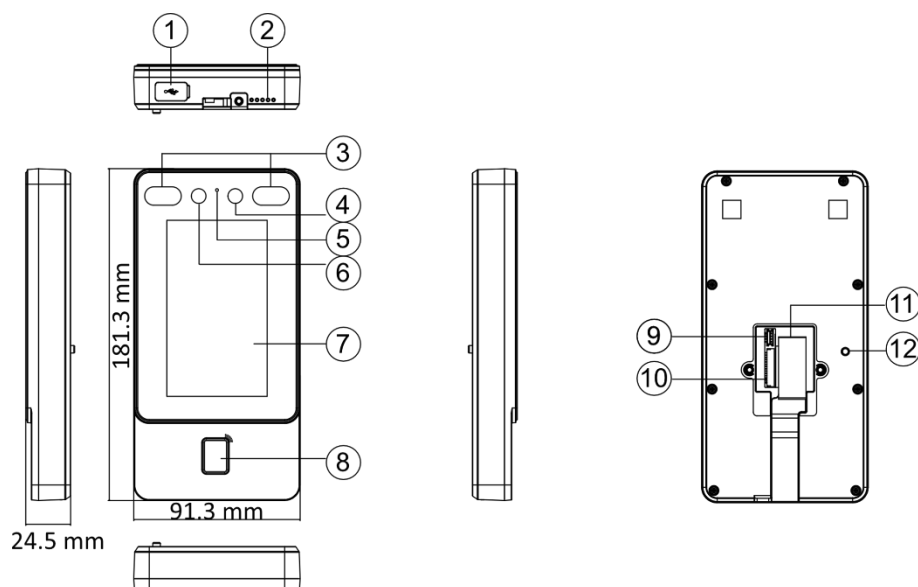


Рисунок 2-1. С модулем считывания отпечатков пальцев

Таблица 2-1 Описание внешнего вида

№	Наименование
1	USB-интерфейс
2	Динамик
3	ИК-подсветка
4	Камера
5	Микрофон
6	Камера
7	Сенсорный экран
8	Область считывания отпечатков пальцев / область считывания карт
9	Служебный порт (только для отладки)
10	Разъем

№	Наименование
11	Сетевой интерфейс
12	Тампер

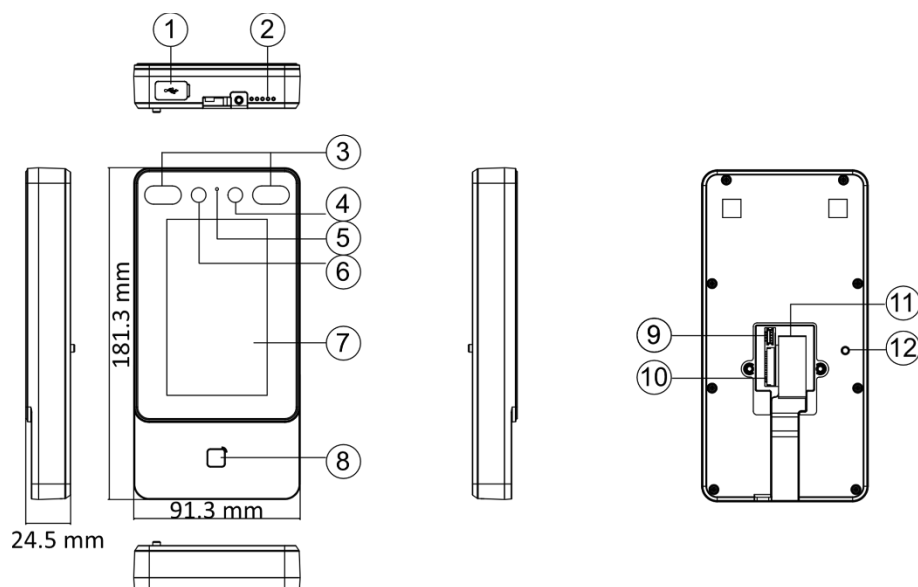


Рисунок 2-1. Без модуля считывания отпечатков пальцев

Таблица 2-2 Описание внешнего вида

№	Название
1	USB-интерфейс
2	Динамик
3	ИК-подсветка
4	Камера
5	Микрофон
6	Камера
7	Сенсорный экран

№	Название
8	Область считывания карт
9	Служебный порт (только для отладки)
10	Разъем
11	Сетевой интерфейс
12	Тампер

Раздел 3 Установка

3.1 Среда установки

- Избегайте попадания на устройство контрового света, а также прямых и непрямых солнечных лучей.
- Для обеспечения лучшего распознавания источник света должен быть расположен в среде установки или недалеко от места установки.
- Стена или другое место монтажа должно выдерживать массу втрое больше массы устройства.
- Не должно быть отражающих объектов (таких как стеклянные двери / стены, объекты из нержавеющей стали, акрила, глянцевого пластика, лака, керамической плитки и др.) в пределах 1 м от поля зрения прибора.
- Убедитесь, поблизости от устройства нет отражающих поверхностей.
- Дальность при распознавании лиц должна быть выше 30 см.
- Поддерживайте чистоту камеры.

Примечание

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

3.2 Установка с использованием монтажной коробки

Шаги

1. Убедитесь, что монтажная коробка установлена на стене.

Примечание

Монтажную коробку необходимо приобрести отдельно.

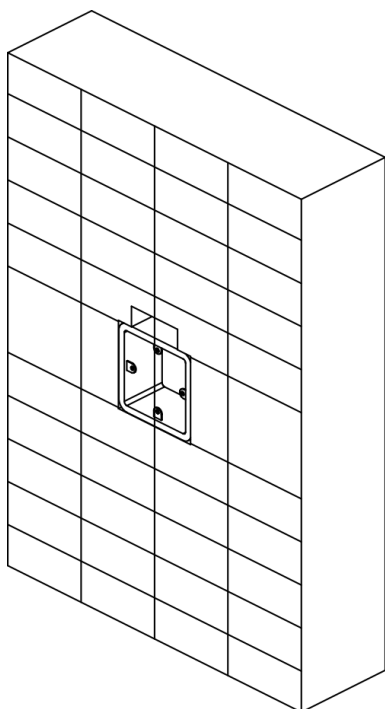


Рисунок 3-1. Установка монтажной коробки

2. Двумя винтами (SC-КА4Х22) в комплекте закрепите монтажную плату на монтажной коробке.

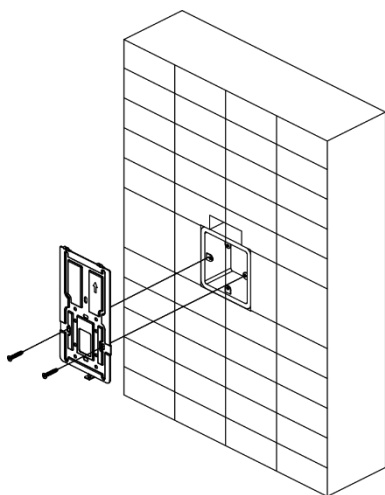


Рисунок 3-2. Установка монтажной платы

3. Протяните кабель через кабельное отверстие, подключите кабели и вставьте их в монтажную коробку.

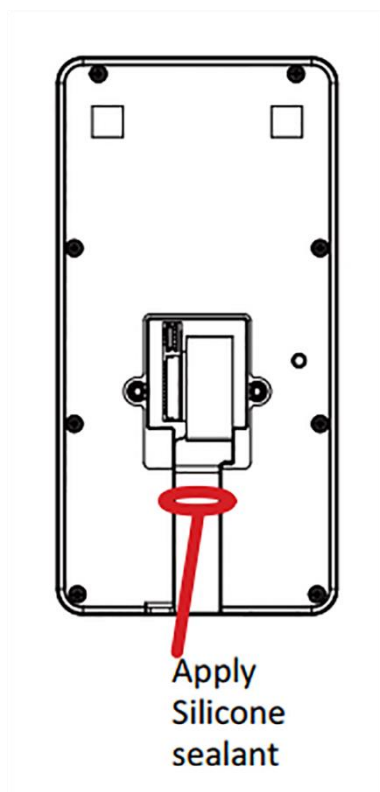


Рисунок 3-3. Фиксация силиконовым герметиком

4. Совместите устройство с монтажной платой и закрепите устройство на монтажной плате с помощью 1 винта (SC-KM3X6-T10-SUSS), поставляемого в комплекте.

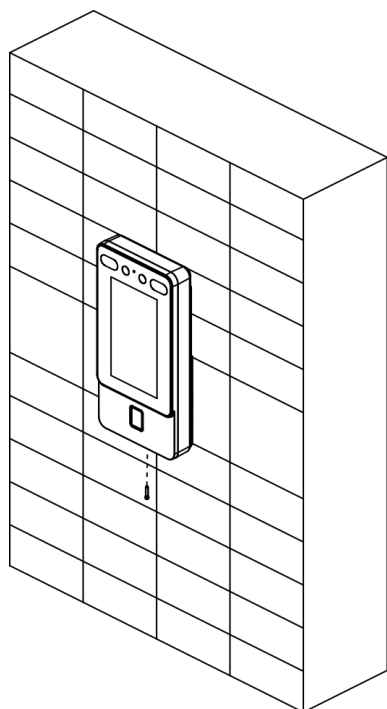


Рисунок 3-4. Фиксация устройства

3.3 Накладная установка

Шаги

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

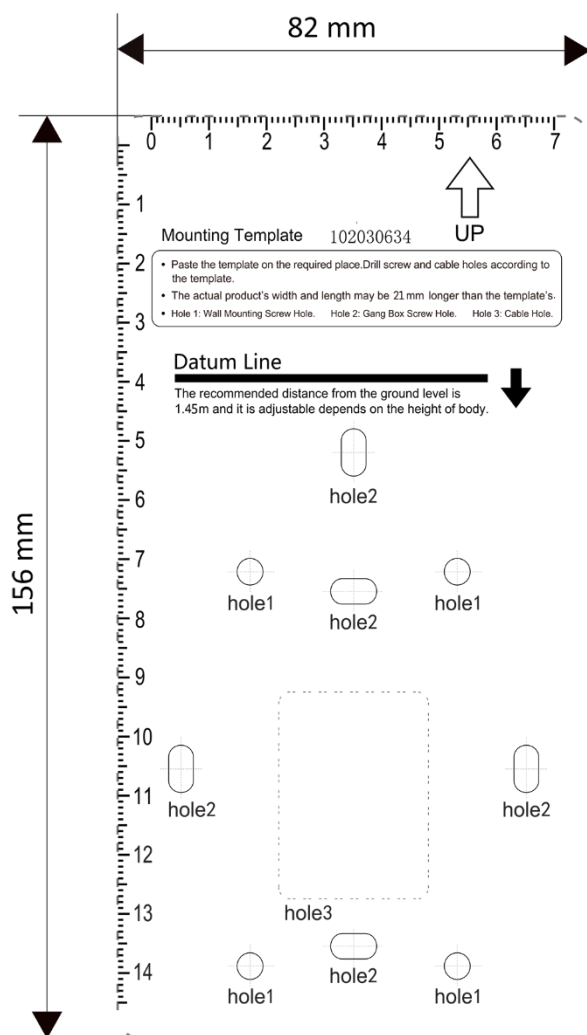


Рисунок 3-5. Монтажный шаблон

2. Просверлите отверстия в стене или другой поверхности в соответствии с отверстием 1 на монтажном шаблоне.
3. Вставьте дюбель в отверстия.
4. Совместите отверстия с монтажной платой и закрепите монтажную плату на стене двумя прилагаемыми винтами (KA4×22-SUS).

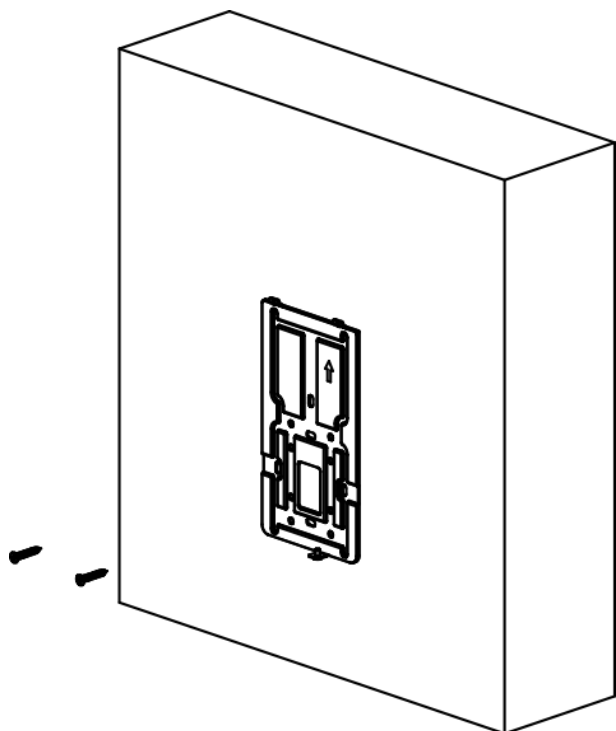


Рисунок 3-6 Установка монтажной платы

5. Протяните кабель через кабельное отверстие монтажной платы и подключите к соответствующим кабелям периферийных устройств.

 Примечание

Если устройство устанавливается снаружи помещения, необходимо нанести силиконовый герметик на место выхода проводки, чтобы исключить попадание воды.

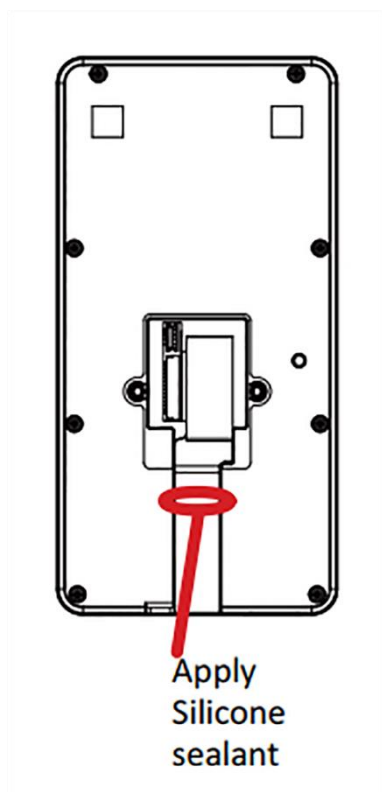


Рисунок 3-7. Фиксация силиконовым герметиком

6. Расположите устройство на монтажной плате в соответствии с инструкцией.

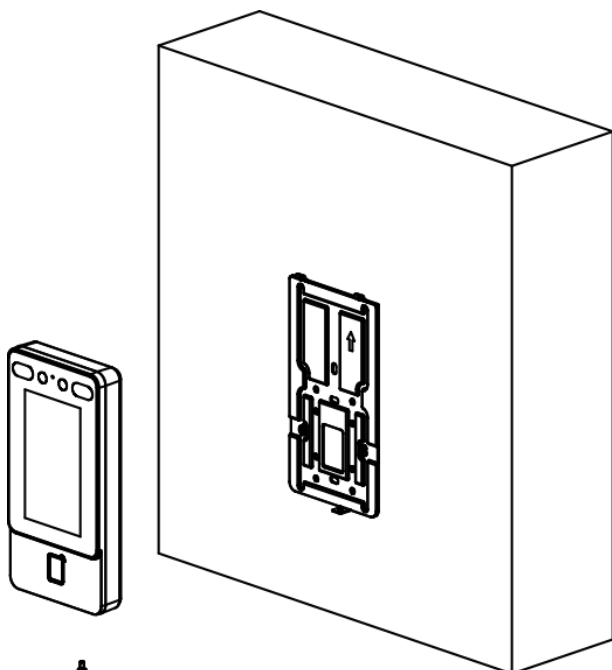


Рисунок 3-8 Установка устройства

7. Закрепите устройство и монтажную плату с помощью 1 винта (KM3×6-SUS), поставляемого в комплекте.

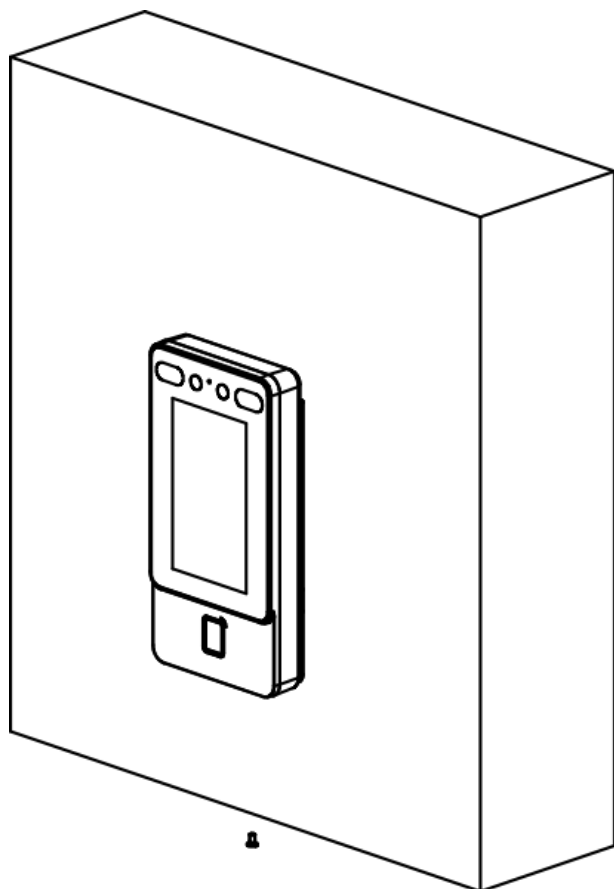


Рисунок 3-9 Фиксация устройства

Примечание

- Рекомендуемая высота установки составляет 1.45 метра, можно выбрать другую высоту установки в соответствии с требованиями проекта.
- Рекомендуется использовать монтажную плату, входящую в комплект поставки.

8. После установки для правильного использования устройства (снаружи помещений) наклейте на экран защитную пленку (детали моделей входят в комплект поставки).

3.4 Установка на кронштейн

3.4.1 Подготовка перед установкой на кронштейн

Шаги

1. Просверлите отверстия на поверхности турникета в соответствии с представленным ниже рисунком. Зафиксируйте водонепроницаемую гайку.

Примечание

Заклепки необходимо припаять, чтобы избежать попадания воды в конструкцию.

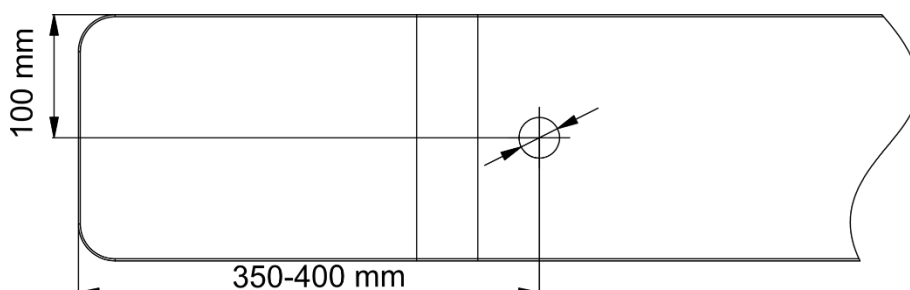


Рисунок 3-10. Сверление отверстий на турникете

2. Если угол установки детали должен составлять 180° перпендикулярно корпусу турникета, необходимо выполнить следующие операции.

1) Открутите 3 винта, как показано на рисунке.

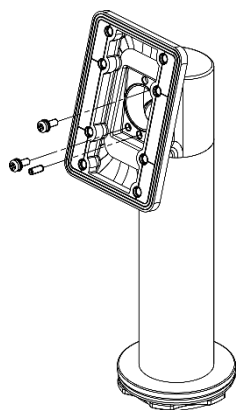


Рисунок 3-11 Откручивание винтов

2) Поверните фиксируемую деталь на 180° и вкрутите 3 винта обратно.

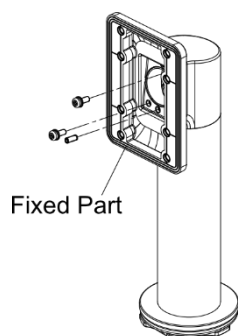


Рисунок 3-12 Вращение фиксируемой детали

3.4.2 Кронштейн

Шаги

1. Установите основание на турникет.

1) Сопоставьте отверстия на турникете и основании и установите основание на турникет.

2) Поверните основание в нужное положение, и убедитесь, что устройство повернуто в правильном направлении.

3) Зафиксируйте основание.

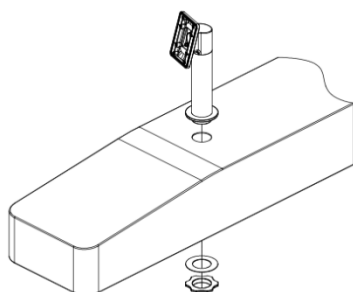


Рисунок 3-13. Установка основания

Примечание

Установите силиконовую накладку на переднюю и заднюю часть турникета.

2. Установите монтажный шаблон на кронштейн с помощью 4 винтов (SC-K1M4×6-SUS).

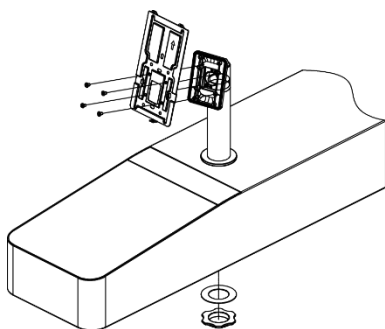


Рисунок 3-14. Фиксация монтажного шаблона

3. Проложите кабели через отверстие для кабелей на турникете и закрепите устройство на монтажной пластине с помощью 1 винта SC-KM3×6-T10-SUS.

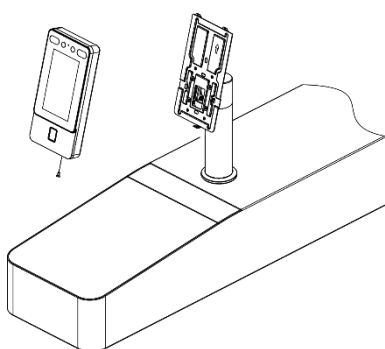


Рисунок 3-15. Фиксация устройства

4. После установки для правильного использования устройства (снаружи помещений) наклейте на экран защитную пленку (детали моделей входят в комплект поставки).

3.5 Установка на цилиндрический кронштейн

3.5.1 Подготовка перед установкой на кронштейн

Убедитесь, что на турникете просверлены отверстия. Если отверстий нет, выполните следующие шаги для сверления отверстий.

Шаги

1. Для установки усиливающей платы на внутренней поверхности турникета используйте 4 винта (M3 или M4), закрепленные фланцевыми гайками.

Примечание

Расстояние между турникетом и краем не должно превышать 10 мм.

2. Просверлите отверстия на внутренней поверхности турникета в соответствии с представленным ниже рисунком. Зафиксируйте водонепроницаемую гайку.

Примечание

Заклепки необходимо припаять, чтобы избежать попадания воды в конструкцию.

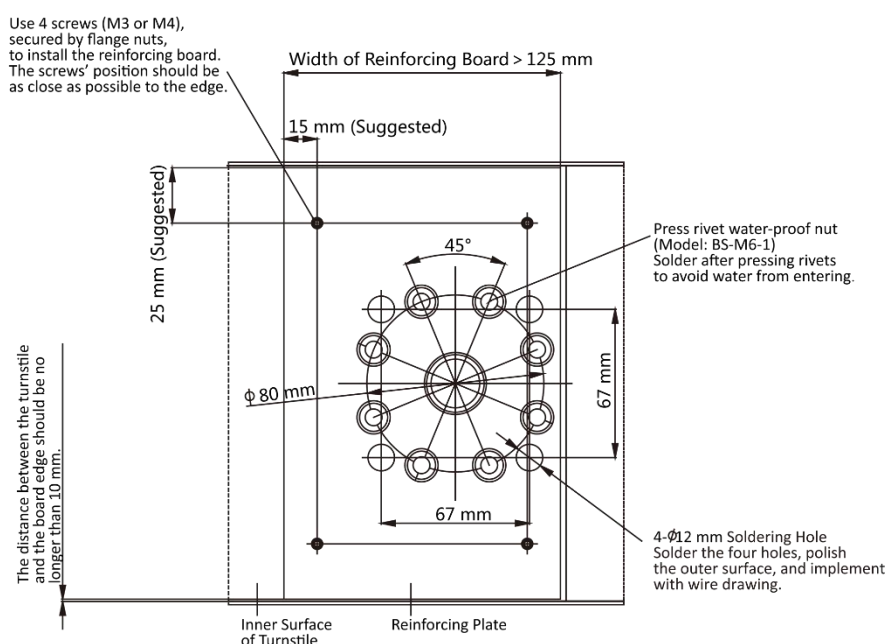


Рисунок 3-16 Сверление отверстий на турникете

3. Далее необходимо припаять 4 других отверстия, отполировать поверхность и провести проводку.

4. Необходимо припаять трубы круглого сечения на внутреннюю поверхность турникета, чтобы избежать попадания воды в конструкцию.

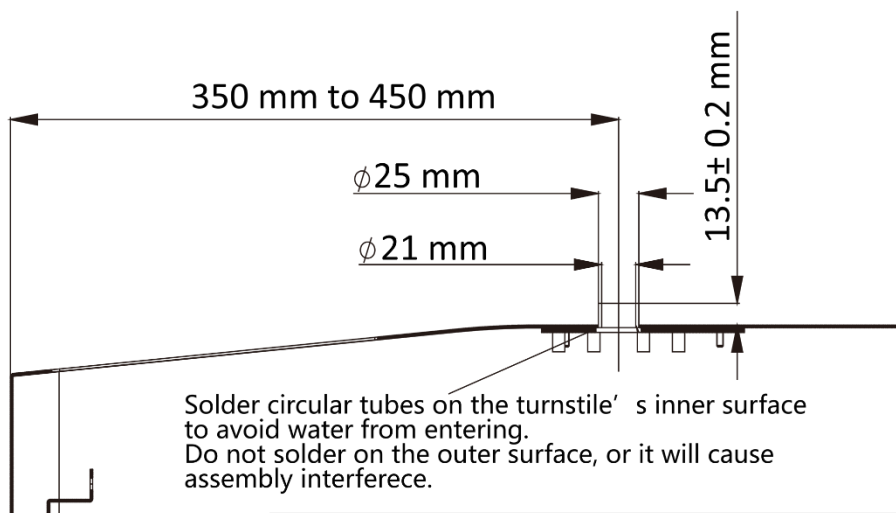


Рисунок 3-17. Припаивание труб

3.5.2 Крепление цилиндрического кронштейна

Шаги

1. Установите основание на турникет.
- 1) Сопоставьте отверстия на турникете и основании и установите основание на турникет.
- 2) Поверните основание в нужное положение, и убедитесь, что устройство повернуто в правильном направлении.
- 3) Закрепите основание четырьмя винтами SC-OM6×12-H-SUS.

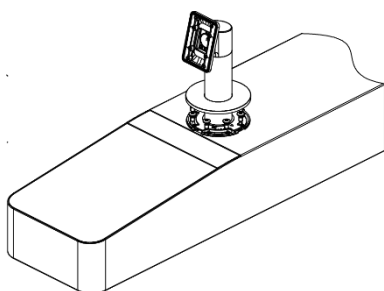


Рисунок 3-18 Установка основания

2. Закрепите монтажную плату на кронштейне 4 винтами SC-K1M4×6-SUS.

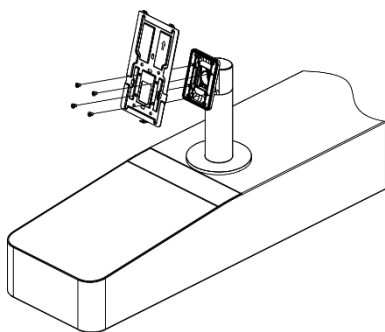


Рисунок 3-19. Фиксация монтажной платы

3. Проложите кабели через отверстие для кабелей на турникете.
4. Закрепите терминал распознавания лиц на монтажной пластине одним винтом SC-KM3×6-H2-SUS.

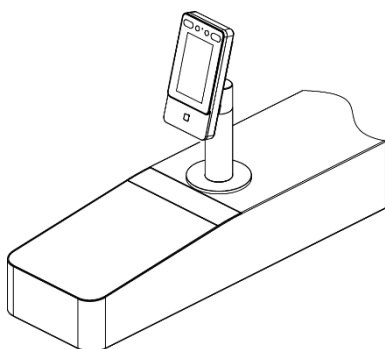


Рисунок 3-20 Фиксация монтажной платы

5. После установки для правильного использования устройства (снаружи помещений) наклейте на экран защитную пленку (детали моделей входят в комплект поставки).

Раздел 4 Подключение

Разъем RS-485 предназначен для подключения считывателя карт с RS-485, разъем NC/ NC и COM — для подключения дверного замка, разъем SEN и GND — для подключения дверного контакта, разъем BTN/GND — для подключения кнопки выхода, разъем Wiegand — для подключения контроллера доступа.

Если соединить терминал Wiegand с контроллером доступа, терминал доступа с функцией распознавания лиц может передавать информацию об аутентификации, на основании которой контроллер доступа отпирает дверь или отказывает в доступе.

Примечание

- Если размер кабеля 18 AWG, используйте источник питания мощностью 12 В. Расстояние между источником питания и устройством не должно превышать 20 м.
- Если размер кабеля 15 AWG, используйте источник питания мощностью 12 В. Расстояние между источником питания и устройством не должно превышать 30 м.
- Если размер кабеля 12 AWG, используйте источник питания мощностью 12 В. Расстояние между источником питания и устройством не должно превышать 40 м.
- Для внешнего считывателя карт, дверного замка, кнопки выхода и магнитоконтактного датчика требуется отдельное питание.

4.1 Описание разъемов

К устройству можно подключить источник питания, RS-485, выход Wiegand и дверной замок.

Терминал оснащен следующими разъемами:

Таблица 4-1. 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	RS-485	Желтый	485+	Подключение по RS-485
	B2		Синий	485-	
	B3		Черный	GND	Заземление
Группа С	C1	Wiegand	Зеленый	W0	Подключение к Wiegand 0
	C2		Белый	W1	Подключение к Wiegand 1
	C3		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	BUTTON	Подключение выходной двери

4.2 Подключение устройства (стандартный режим)

Терминал можно подключить к стандартному внешнему оборудованию.

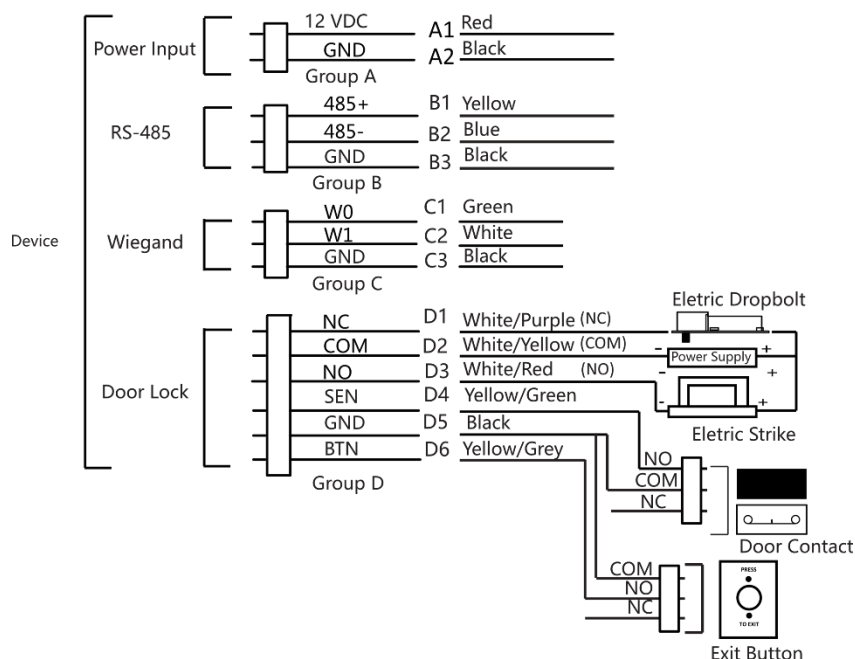


Рисунок 4-1. Подключение устройства

Примечание

- При этом для терминала доступа с функцией распознавания лиц необходимо задать направление Wiegand на значение **Input** («Вход») для подключения к считывателю карт Wiegand. Если необходимо подключиться к контроллеру доступа, задайте направление Wiegand на значение **Output** («Выход») для передачи информации аутентификации контроллеру доступа.
- Подробная информация представлена в разделе [Настройка параметров интерфейса Wiegand](#).
- Запрещено подключать устройство напрямую к электрической сети.

4.3 Подключение к модулю безопасности двери

Также терминал можно подключить к модулю безопасности двери.

Ниже представлена схема подключения.

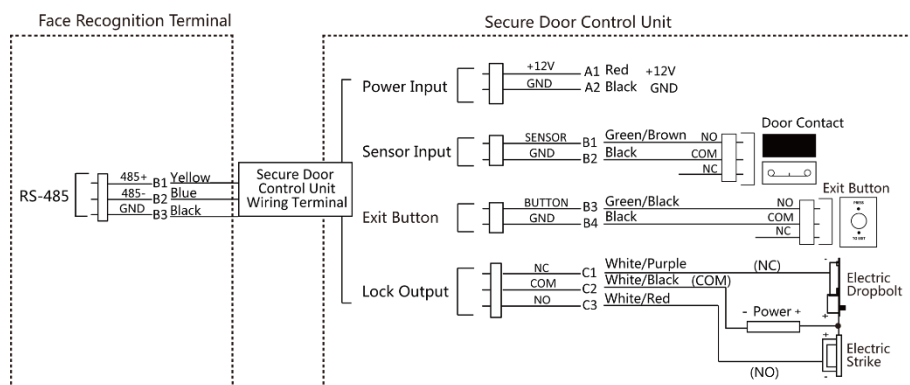


Рисунок 4-2. Подключение к модулю безопасности двери

Примечание

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

4.4 Подключение модуля пожарной тревоги

4.4.1 Схема подключения типа безопасности «Дверь остается открытой при отключении питания»

Тип замка: замок из анодированного алюминия, электромагнитный замок и электромеханическая защелка (NO)

Тип безопасности: «Дверь остается открытой при отключении питания».

Сценарий: установлен в систему обнаружения возгораний.

Тип 1

Примечание

Система обнаружения возгораний контролирует питание системы контроля доступа.

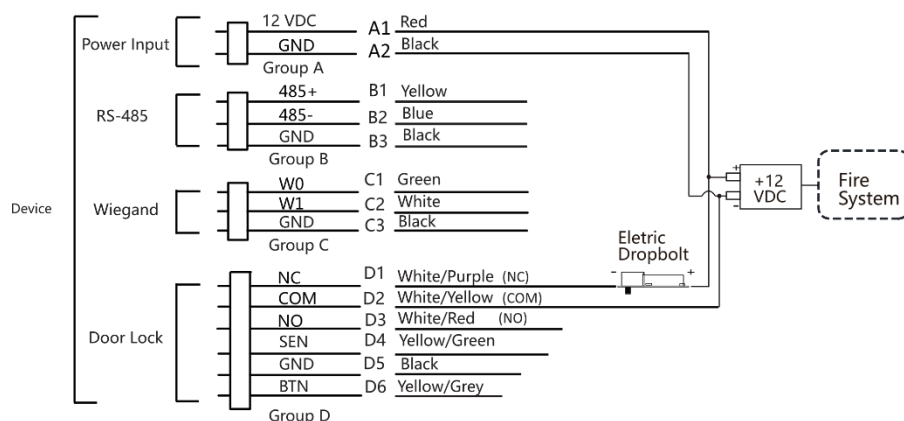


Рисунок 4-3. Подключение устройства

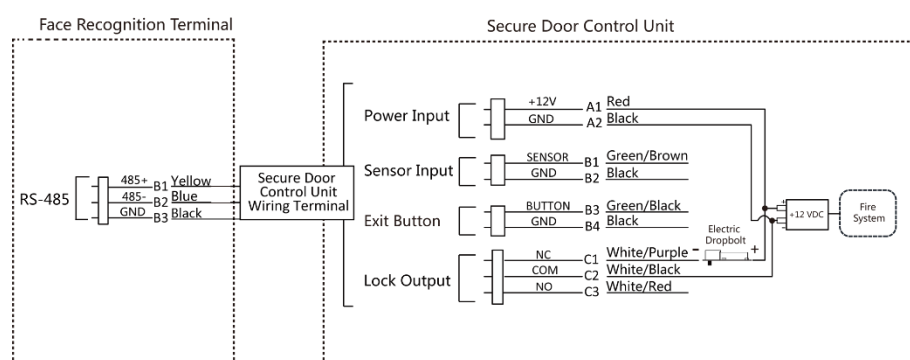


Рисунок 4-4. Подключение к модулю безопасности двери

Тип 2

Примечание

Система обнаружения возгораний (NO и COM, нормально разомкнутая при отключении питания) последовательно подключена к замку и блоку питания. Когда срабатывает пожарная сигнализация, дверь остается открытой. В обычных условиях NO и COM остаются закрытыми.

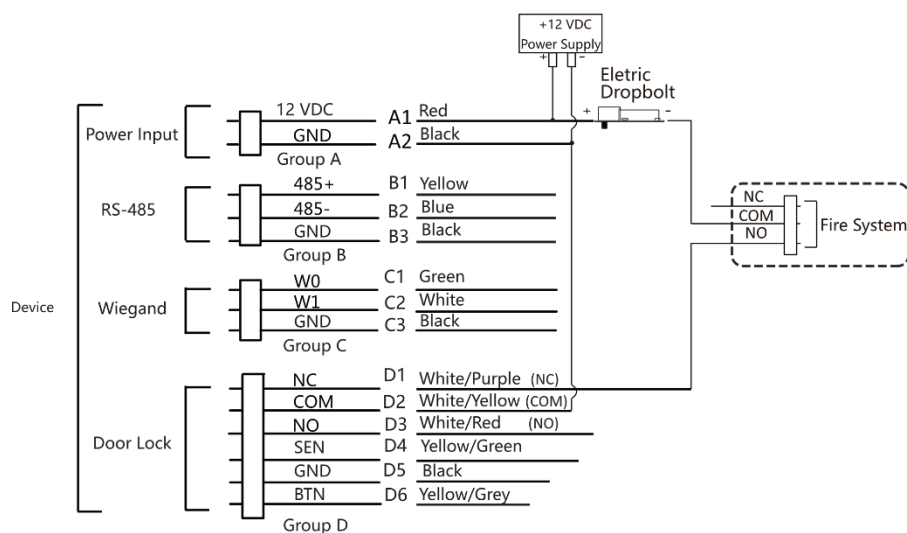


Рисунок 4-5. Подключение устройства

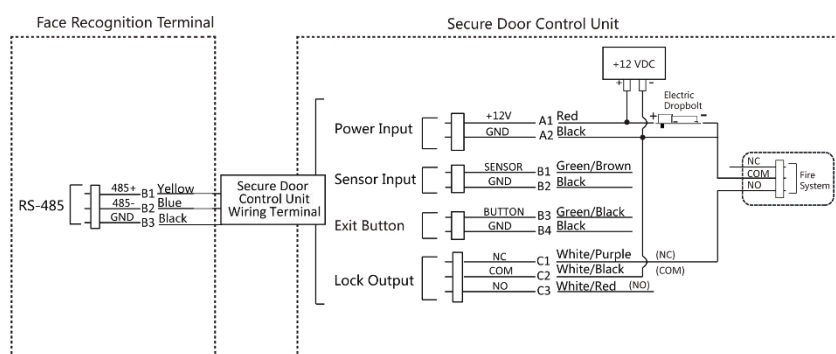


Рисунок 4-6. Подключение к модулю безопасности двери

4.4.2 Схема подключения типа безопасности «Дверь закрывается при отключении питания»

Тип замка: катодный замок, электромагнитный замок и электромеханическая защелка (NC)

Тип безопасности: «Дверь закрывается при отключении питания»

Сценарий: установлен в области входа / выхода с привязкой пожарной сигнализации

Примечание

- Требуется источник бесперебойного питания (ИБП).

- Система обнаружения возгораний (NC и COM, нормально замкнутая при отключении питания) последовательно подключена к замку и блоку питания. Когда срабатывает пожарная сигнализация, дверь остается открытой. В обычных условиях NC и COM остаются открытыми.

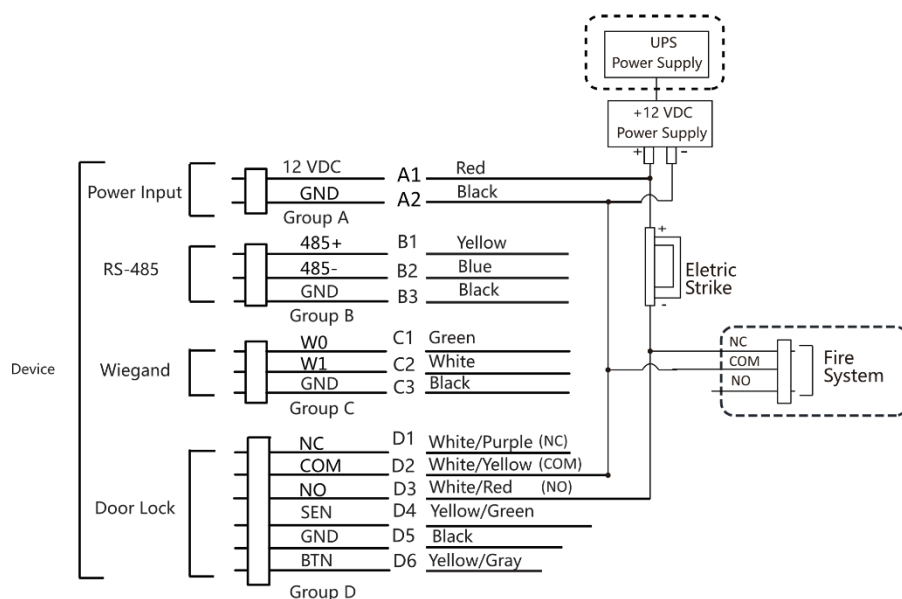


Рисунок 4-7 Подключение устройства

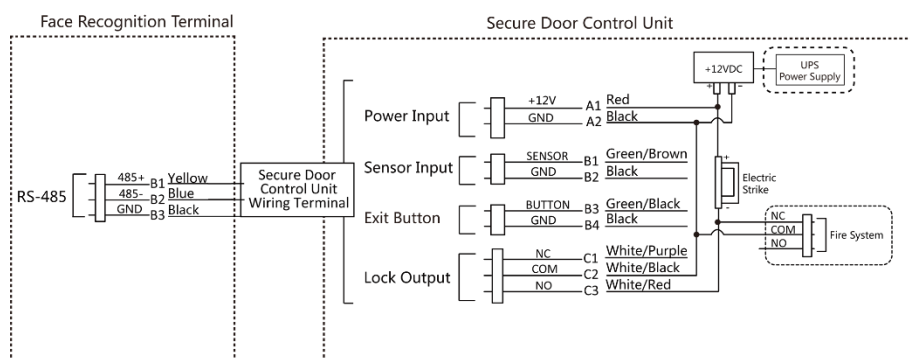


Рисунок 4-8. Схема подключения

Раздел 5 Активация устройства

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

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

Значения по умолчанию для устройства следующие:

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

5.1 Активация через устройство

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

Activate Device

Enter 8 to 16 characters.

Enter Password

Confirm Password

Confirm Password

Enter 8 to 16 characters (Two or more of the following character types are allowed: digit, letter, and symbol.)

Activate

Рисунок 5-1. Страница активации

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее.

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

Предостережение

- Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее.
- Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг и / или конечного пользователя.
- В пароле не должны содержаться следующие символы: имя пользователя, 123, admin (без учета регистра), 4 или более непрерывно увеличивающихся или уменьшающихся цифр или 4 или более последовательно повторяющихся символов.
- Пароль не может содержать такие слова, как hik, hkws и hikvision (регистр не учитывается).

- После активации необходимо выбрать соответствующий язык.
- После активации устройства, выберите режим работы. Подробная информация представлена в соответствующем разделе.
- После активации необходимо настроить сеть. Дополнительная информация представлена в разделе [Настройка параметров сети](#).
- После активации можно добавить устройство на платформу. Подробная информация представлена в разделе [Доступ к платформе](#).
- После активации, если необходимо настроить конфиденциальность, нужно проверить параметр. Подробная информация представлена в разделе [Настройки конфиденциальности](#).
- После активации: для управления параметрами устройства необходимо задать роль администратора. Подробная информация представлена в разделе [Добавление администратора](#).

5.2 Активация через веб-интерфейс

Можно активировать устройство через веб-интерфейс.

Шаги

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

Примечание

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

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

Предостережение

- Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее.

- Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг и / или конечного пользователя.
- В пароле не должны содержаться следующие символы: имя пользователя, 123, admin (без учета регистра), 4 или более непрерывно увеличивающихся или уменьшающихся цифр или 4 или более последовательно повторяющихся символов.
- Пароль не может содержать такие слова, как hik, hkws и iFlow (регистр не учитывается).

3. Нажмите **Activate** («Активировать»).

4. Изменение IP-адреса устройства. IP-адрес можно редактировать с помощью инструмента SADP, устройства и клиентского программного обеспечения.

5.3 Активация через ПО SADP

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

Перед началом

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

Следующие шаги показывают, как активировать устройство и изменить его IP-адрес.

Подробная информация о пакетной активации и изменении IP-адресов представлена в *Руководстве пользователя ПО SADP*.

Шаги

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

Предостережение

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

Примечание

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

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

The screenshot shows the SADP software interface. On the left, there is a table of devices. The table has columns: ID, Device Type, Security, IP Address, Port, Software Version, IPv4 Gateway, HTTP Port, and Device Serial No. The table lists several devices, with device 007 highlighted in red. A red box around device 007 contains the text "Select inactive device." Below the table, there is a red box with the text "Input and confirm password." On the right side of the interface, there is a section titled "Activate the Device" with a blue padlock icon and the text "The device is not activated." Below this, there is a blue box with the text "You can modify the network parameters after the device activation." At the bottom right, there is a red box containing the "New Password" and "Confirm Password" fields, both with asterisks for the password, and an "Enable Hi-Connect" checkbox. A red "Activate" button is at the bottom right.

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

5. Измените IP-адрес устройства.

1) Выберите устройство.

2) Измените IP-адрес устройства на адрес в той же подсети, к которой подключен компьютер вручную или поставив галочку **Enable DHCP** («Включить DHCP»).

3) Введите пароль администратора и нажмите **Modify** («Изменить») для изменения вашего IP-адреса.

5.4 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

Устройство должно поддерживать данную функцию.

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

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее.

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. Нажмите **ОК** для активации устройства.

Раздел 6 Быстрые операции

6.1 Выбор языка

Можно выбрать язык системы устройства.

После активации устройства можно выбрать язык системы устройства.

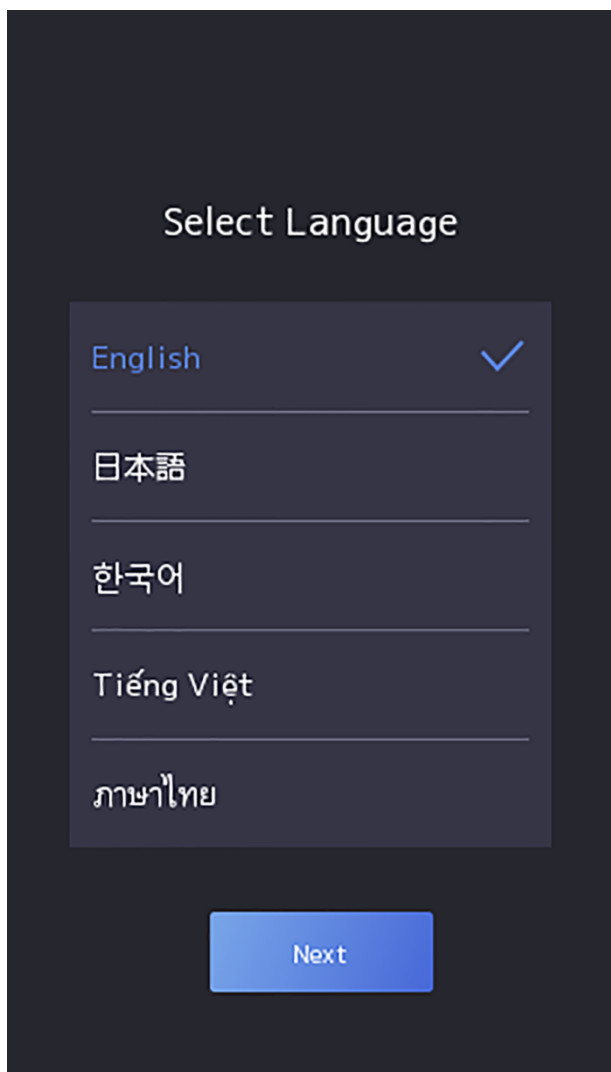


Рисунок 6-1 Выбор языка системы

По умолчанию языком системы выбран английский.

Примечание

После изменения языка системы устройство автоматически перезагрузится.

6.2 Настройка типа изменения пароля

После активации устройства, пароль администратора можно поменять с помощью резервного адреса электронной почты или контрольных вопросов. Если вы забыли пароль для доступа к устройству, пароль можно изменить с помощью выбранного типа изменения.

Изменение пароля с помощью электронной почты

Если необходимо изменить пароль через резервный адрес электронной почты, введите адрес электронной почты и нажмите **Next** («Далее»).

Изменение пароля с помощью контрольных вопросов

Если нужно изменить пароль с помощью контрольных вопросов, нажмите **Change to Security Questions** («Изменить с помощью контрольных вопросов») в правом углу. Выберите контрольные вопросы и ответы. Нажмите **Next** («Далее»).

Примечание

Вы можете выбрать только один тип изменения пароля. При необходимости, вы можете перейти в веб-страницу и настроить оба типа изменения.

6.3 Настройка параметров сети

После активации и выбора режима применения можно настроить сеть для устройства.

Шаги

Примечание

Некоторые модели поддерживают настройку Wi-Fi. Проверьте функционал фактического устройства.

1. Когда войдете на страницу выбора сети, нажмите **Wired Network** («Проводная сеть») или Wi-Fi в соответствии с текущими требованиями.

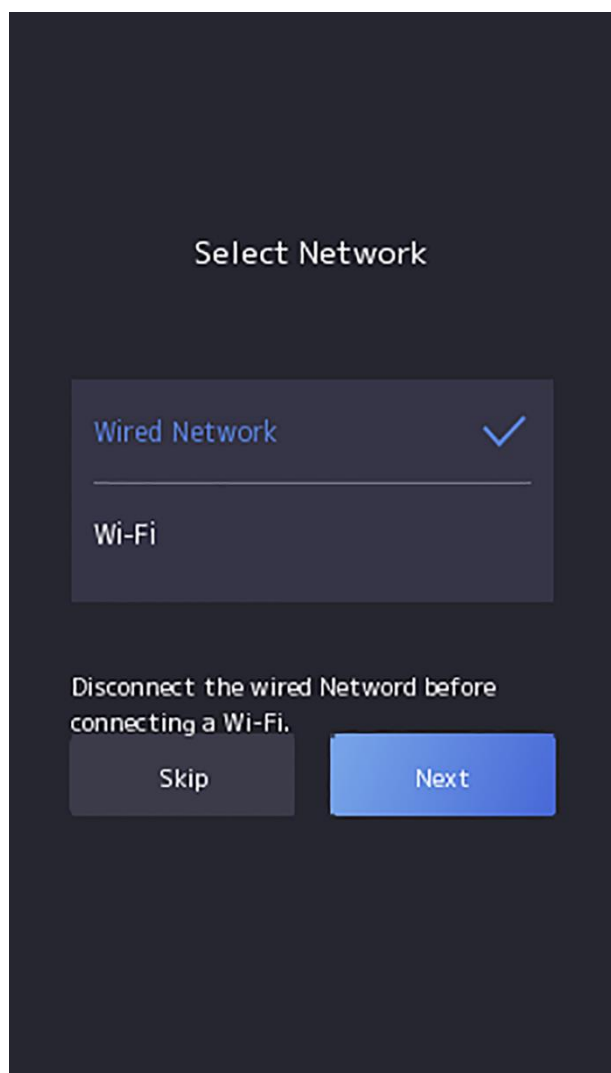


Рисунок 6-2. Выбор сети

 Примечание

Перед подключением Wi-Fi отключите проводную сеть.

2. Нажмите **Next** («Далее»).

Проводная сеть

 Примечание

Убедитесь, что устройство подключено к сети.

Если включить **DHCP**, система автоматически назначит IP-адрес и другие параметры.

Если **DHCP** отключен, необходимо установить IP-адрес, маску подсети и шлюз.

Wi-Fi

Выберите Wi-Fi сеть и введите пароль Wi-Fi для подключения.

Или нажмите **Add Wi-Fi** («Добавить Wi-Fi») и введите название Wi-Fi и пароль для подключения.

3. Опционально. Нажмите **Skip** («Пропустить»), чтобы пропустить настройки сети.

6.4 Доступ к платформе

Включите функцию и устройство сможет работать с помощью Hik-Connect.

Устройство может быть подключено к мобильному клиенту Hik-Connect и т.д.

Шаги

1. Включите **Access to Hik-Connect** («Доступ к Hik-Connect») и установите IP-адрес сервера и код подтверждения устройства.

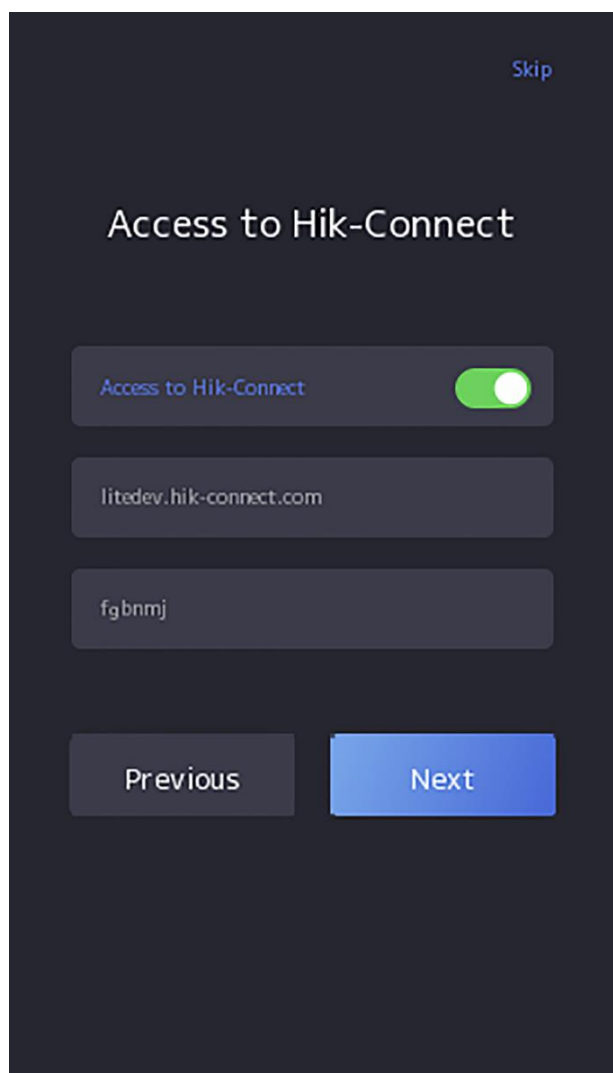


Рисунок 6-3. Доступ к Hik-Connect

2. Нажмите **Next** («Далее»).

Примечание

Если вы нажмете **Previous** («Назад») для возврата на страницу настроек Wi-Fi, для перехода на страницу платформы нужно выбрать подключенный Wi-Fi или подключиться к другому.

6.5 Настройки конфиденциальности

После активации, выбора режима применения и выбора сети, необходимо настроить параметры конфиденциальности, включая параметры загрузки и хранения изображений.

Выберите параметры согласно фактическим требованиям.

Загрузка захваченного изображения при аутентификации

Загрузите полученные при аутентификации изображения на платформу автоматически.

Загрузка захваченного изображения при аутентификации

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

Сохранение зарегистрированного изображения

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

Загрузка изображения после привязанного захвата

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

Сохранение изображения после связанного захвата

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

Загрузка захваченных изображений во время звонка

Автоматическая загрузка полученных во время звонка изображений на платформу.

Нажмите **Next** («Далее»).

6.6 Настройка роли администратора

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

Перед началом

Активируйте устройство и выберите тип применения.

Шаги

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

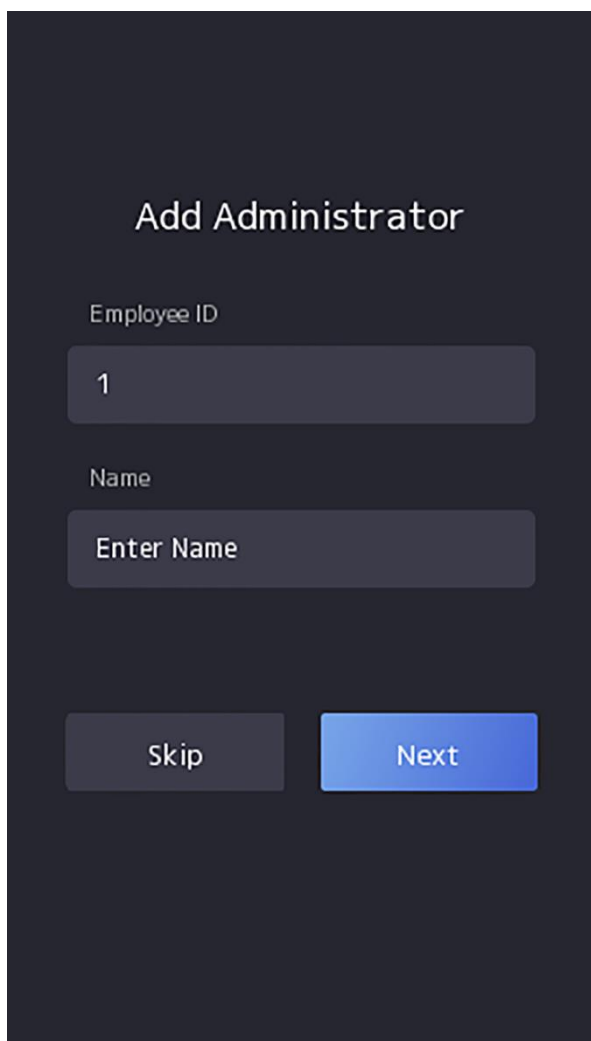


Рисунок 6-4 Страница добавления роли администратора

3. Выберите учетные данные для добавления.

Примечание

Необходимо добавить как минимум одну учетную запись.

- : Посмотрите прямо в камеру. Убедитесь, что лицо находится в рамке распознавания лица. Нажмите  для захвата и нажмите  для подтверждения.
- : Прислоните палец в соответствии с инструкциями на экране устройства. Нажмите  для подтверждения.
- : Введите номер карты или предъявите карту в области считывания карты. Нажмите **ОК**.

4. Нажмите **ОК**.

Вы попадете на страницу аутентификации.

Описание значков состояния



Устройство поставлено на охрану/не поставлено на охрану.



Nik-Connect включен/отключен.



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



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

Описание горячих клавиш

Примечание

Вы можете настроить сочетания клавиш, отображаемых на экране. Подробная информация представлена в разделе [Основные настройки](#).



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



Примечание

Чтобы выполнить вызов, устройство необходимо добавить в центр управления.



Введите PIN-код для аутентификации.

Раздел 7 Основные операции

7.1 Вход в систему

Выполните вход в систему, чтобы настроить основные параметры устройства.

7.1.1 Вход в систему в качестве администратора

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

Шаги

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



Рисунок 7-1. Вход в систему в качестве администратора

2. Чтобы войти на главную страницу, необходимо пройти аутентификацию по лицу, отпечаткам пальцев или карте администратора.

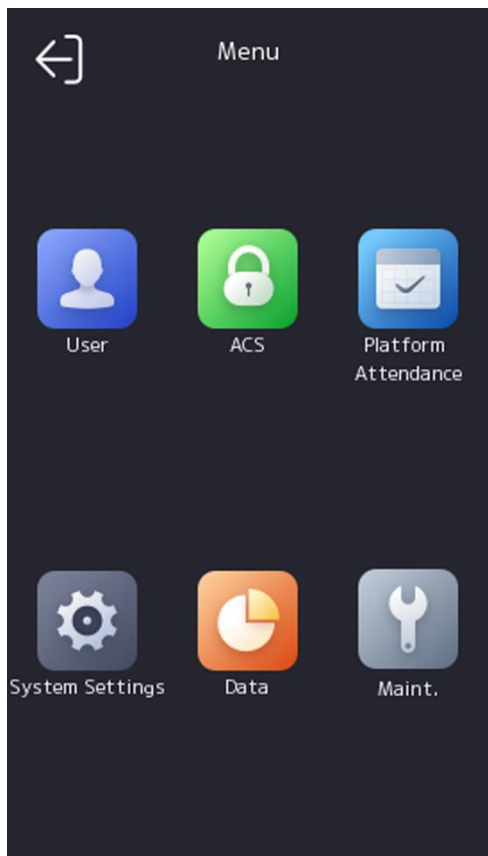


Рисунок 7-2 Главная страница

Примечание

Устройство будет заблокировано на 30 минут после 5 неудачных попыток аутентификации по отпечаткам пальцев или считыванию карты.

3. Опционально. Нажмите и введите пароль для активации устройства, чтобы войти в систему.

4. Опционально. Нажмите , чтобы выйти из страницы входа в систему в качестве администратора.

7.1.2 Вход в систему с использованием пароля активации

Прежде чем начать работать с устройством, необходимо выполнить вход в систему. Если настройка роли администратора не предполагается, для входа необходимо выполнить следующие действия.

Шаги

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

2. Введите пароль.

- При добавлении учетной записи администратора для устройства нажмите  и введите пароль.
- Если учетная запись администратора для устройства не добавлена, введите пароль

3. Нажмите **ОК** для перехода на главную страницу.

Примечание

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

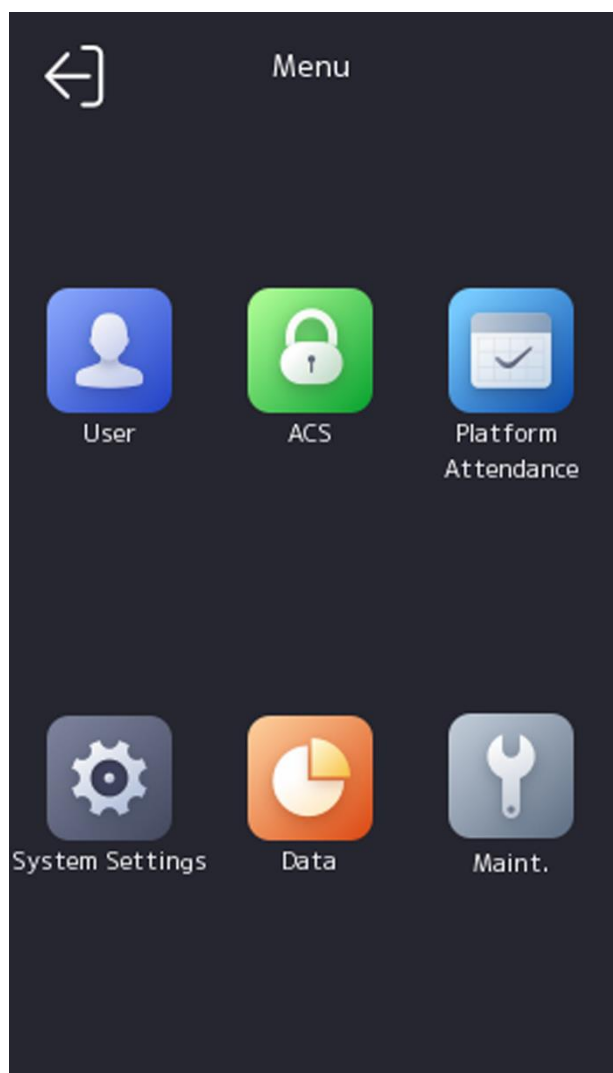


Рисунок 7-3. Главная страница

7.1.3 Забыть пароль

Если вы забыли пароль во время аутентификации, можно его изменить.

Шаги

1. Удерживайте кнопку мыши в течение 3 секунд на экране начальной страницы, затем переместите курсор влево/вправо и войдите на страницу.
2. Опционально. Если роль администратора настроена, нажмите  на всплывающей странице аутентификации в роли администратора.
3. Нажмите **Forgot Password** («Забыли пароль»).

4. Выберите тип изменения пароля из списка.

Примечание

Если настроен только один тип изменения пароля, откроется страница смены пароля для дальнейших настроек.

5. Ответьте на контрольные вопросы или измените пароль при помощи адреса электронной почты.

- Контрольные вопросы: Ответьте на вопросы безопасности, настроенные во время активации.
- Адрес электронной почты

Примечание

Убедитесь, что устройство добавлено в учетную запись Hik-Connect.

1. Загрузите приложение Hik-Connect.
2. Перейдите **More** → **Reset Device Password** («Дополнительно → Сброс пароля устройства»).
3. Сканируйте QR-код на устройстве, и появится код подтверждения.

Примечание

Нажмите QR-код, чтобы увеличить изображение.

4. Введите проверочный код на странице устройства.

6. Создайте новый пароль и подтвердите его.

7. Нажмите **ОК**.

7.2 Настройка связи

На странице настроек связи можно настроить проводную сеть, WI-Fi, параметры RS-485, Wiegand, ISUP и параметры доступа к Hik-Connect.

7.2.1 Настройка параметров проводной сети

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

Шаги

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

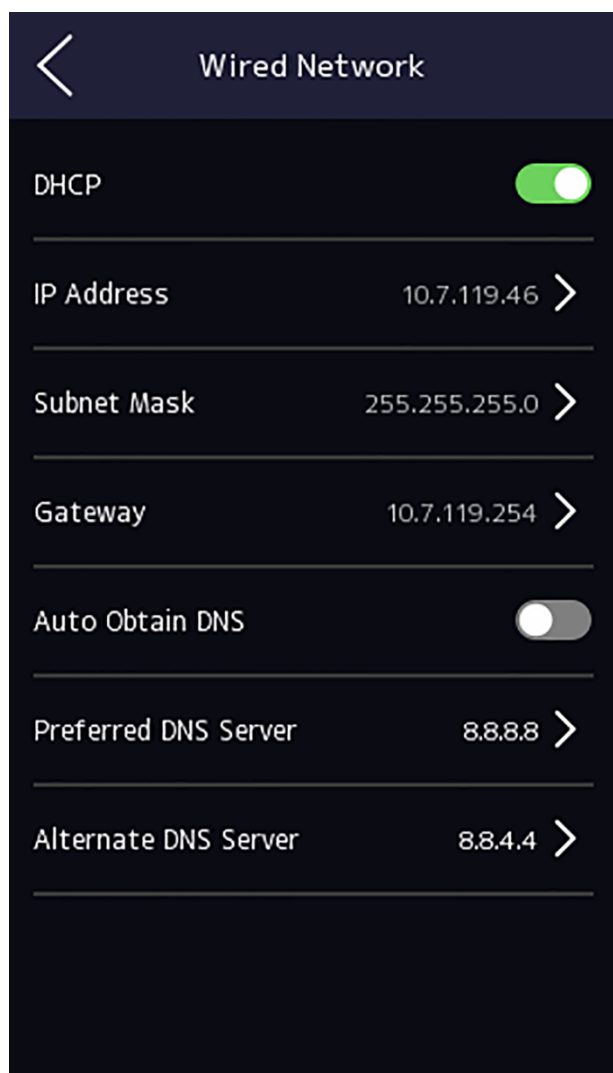


Рисунок 7-4. Настройки проводной сети

3. Установите IP-адрес устройства, маску подсети и шлюз.

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

Примечание

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

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

7.2.2 Настройка параметров Wi-Fi

Можно включить функцию Wi-Fi и настроить соответствующие параметры.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **System Settings** → **Comm.** («Настройки системы → Настройки связи») на главной странице, чтобы перейти на страницу **Communication Settings** («Настройки связи»).

2. Нажмите на странице **Communication Settings** («Настройки связи»).

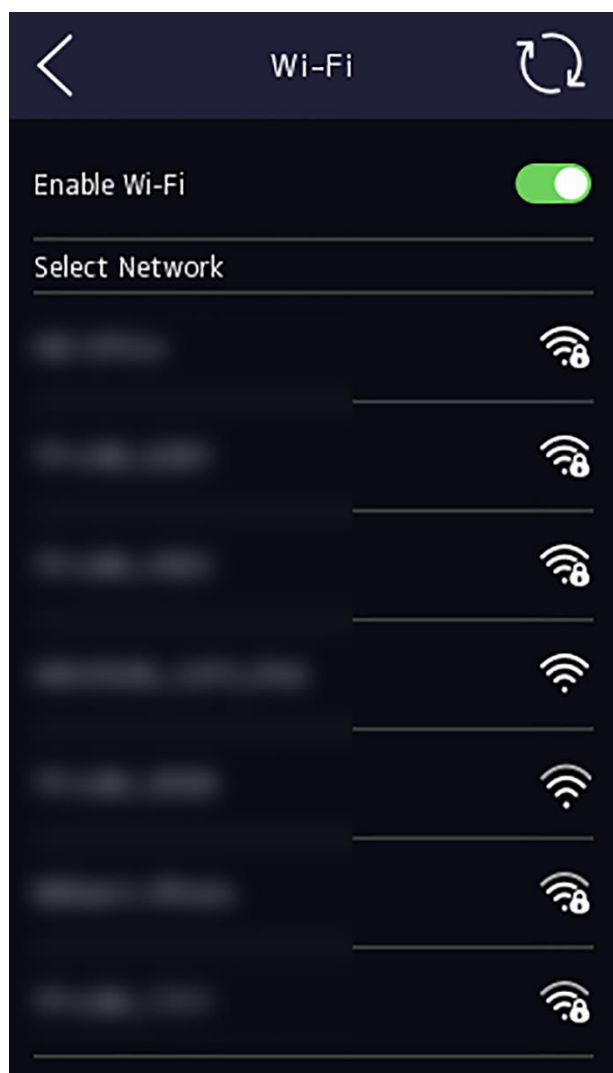


Рисунок 7-5. Настройка Wi-Fi

3. Включите функцию Wi-Fi.

4. Настройте параметры Wi-Fi.

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

Примечание

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

5. Задайте параметры Wi-Fi.

- По умолчанию DHCP включен. Система автоматически задаст IP-адрес, маску подсети и шлюз.
- При отключении **DHCP** IP-адрес, маску подсети и шлюз необходимо устанавливать вручную.

6. Нажмите **ОК** для сохранения настроек и возврата ко вкладке Wi-Fi.

7. Нажмите для сохранения параметров сети.

7.2.3 Настройка параметров RS-485

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

Шаги

1. Нажмите **System Settings** → **Comm.** («Настройки системы → Настройки связи») на главной странице, чтобы перейти на страницу **Communication Settings** («Настройки связи»).

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

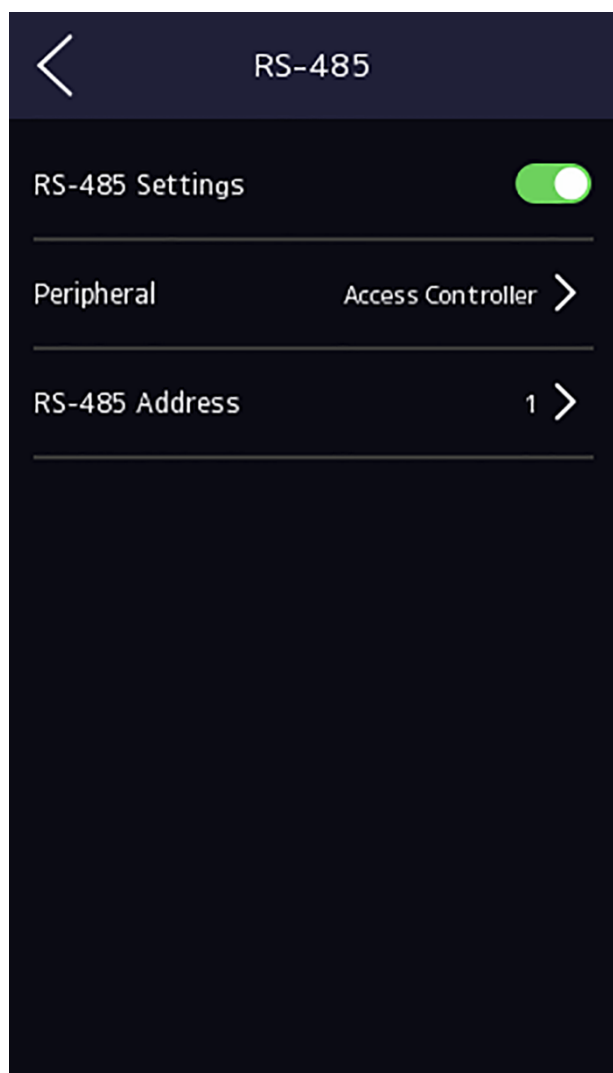


Рисунок 7-6. Настройка параметров RS-485

3. Выберите внешнее устройство согласно фактическим требованиям.

Примечание

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

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

7.2.4 Настройка параметров интерфейса Wiegand

Можно настроить направление передачи данных интерфейса Wiegand.

Шаги

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

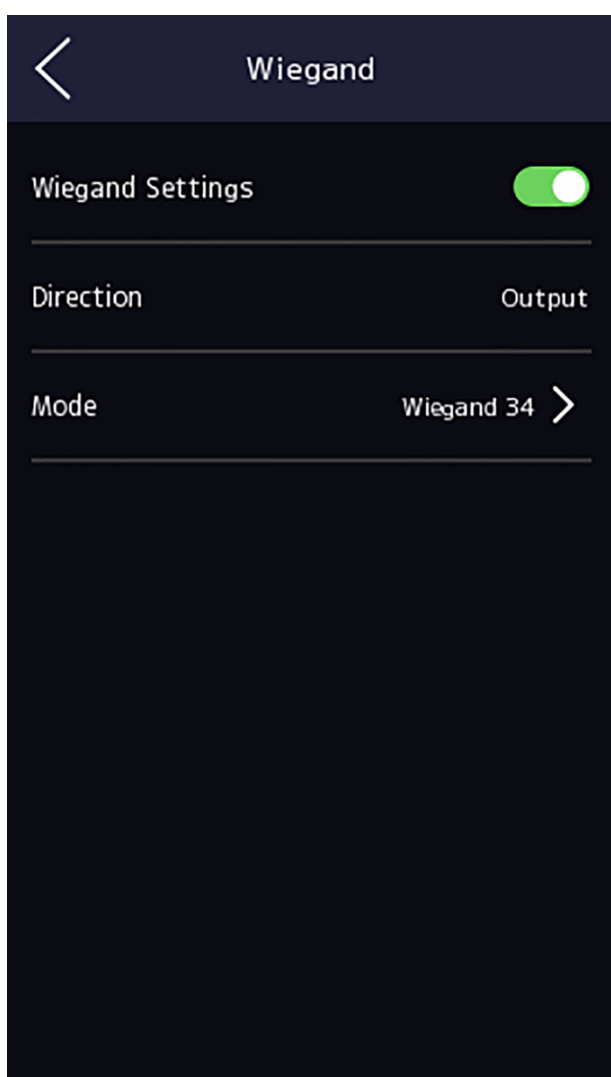


Рисунок 7-7. Настройка Wiegand

3. Включите функцию Wiegand.

4. Выберите режим Wiegand.

- Выход: терминал доступа с функцией распознавания лиц можно подключать к внешнему контроллеру доступа. Эти два устройства будут передавать номер карты через Wiegand 26 или Wiegand 34.

5. Нажмите ☒ для сохранения параметров сети.

Примечание

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

7.2.5 Настройка параметров ISUP

Настройте параметры ISUP, чтобы устройство смогло загрузить данные через протокол ISUP.

Перед началом

Убедитесь, что устройство подключилось к сети.

Шаги

1. Нажмите **System Settings** → **Comm.** → **ISUP** («Настройки системы → Настройки связи → ISUP») на главной странице, чтобы перейти на страницу настроек.

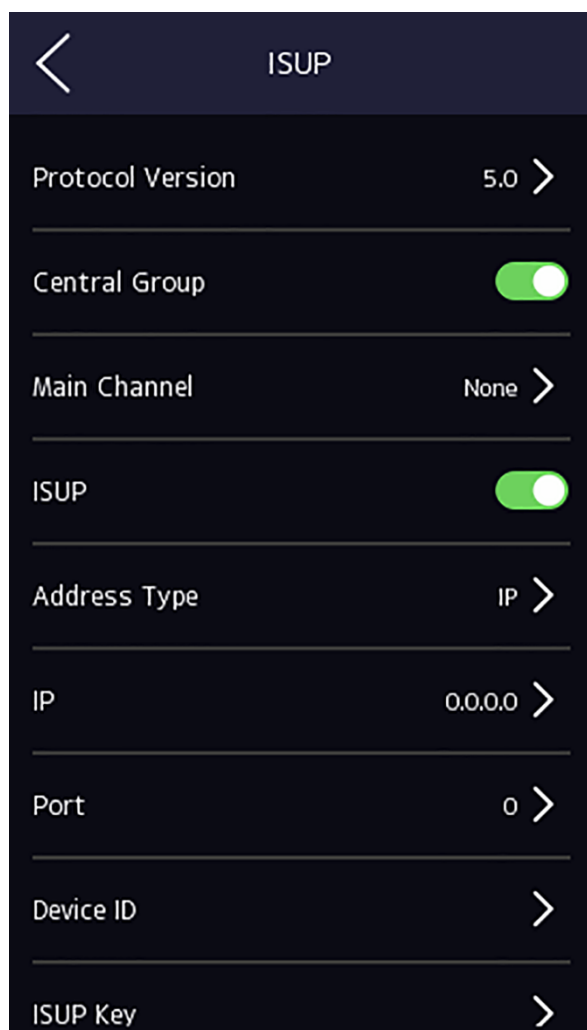


Рисунок 7-8. Настройка ISUP

2. Включите функцию ISUP и настройте параметры сервера ISUP.

Версия ISUP

Задайте необходимую версию ISUP.

Центральная группа

Включите центральную группу для загрузки данных.

Основной канал

Доступны N1 или None («Отсутствует»).

ISUP

Включите функцию ISUP для загрузки данных через протокол EHome.

Тип адреса

Выберите тип адреса согласно фактическим требованиям.

IP-адрес

Настройте IP-адрес сервера ISUP.

№ порта

Настройте № порта сервера ISUP.

Примечание

Диапазон № порта: от 0 до 65535.

ID устройства

Укажите серийный № устройства.

Пароль

При выборе V5.0 необходимо создать учетную запись и ключ ISUP. При выборе другой версии необходимо создать только учетную запись ISUP.

Примечание

- Запомните учетную запись ISUP и ключ ISUP. Необходимо ввести имя учетной записи или ключ, когда устройство связывается с другими платформами по протоколу ISUP.
- Диапазон ключа ISUP: от 8 до 32 символов.

7.2.6 Доступ к платформе

Можно изменить проверочный код устройства и задать адрес сервера перед тем, как добавить устройство в мобильный клиент Hik-Connect.

Перед началом

Убедитесь, что устройство подключилось к сети.

Шаги

1. Нажмите **System Settings** → **Comm.** («Настройки системы → Настройки связи») на главной странице, чтобы перейти на страницу **Communication Settings** («Настройки связи»).
2. На странице настроек связи нажмите **Access to Hik-Connect** («Доступ к Hik-Connect»).
3. Включите доступ к Hik-Connect
4. Введите **Server IP** («IP-адрес сервера»).
5. Создайте **Verification Code** («Проверочный код»), затем введите проверочный код при управлении устройствами через **Hik-Connect**.

7.2.7 Настройки SNMP

Можно настроить параметры SNMP.

Шаги

1. Нажмите **System Settings** → **Comm.** («Настройки системы → Настройки связи») на главной странице, чтобы перейти на страницу **Communication Settings** («Настройки связи»).
2. На странице **Communication Settings** («Настройки связи») нажмите **SNMP**.
3. Включите **SNMP**.
4. Установите **Trap Community String** («Строка аутентификации»).
5. Установите **NMS IP Address** («IP-адрес NMS») и **NMS Port** («Порт NMS»).

7.3 Управление пользователями

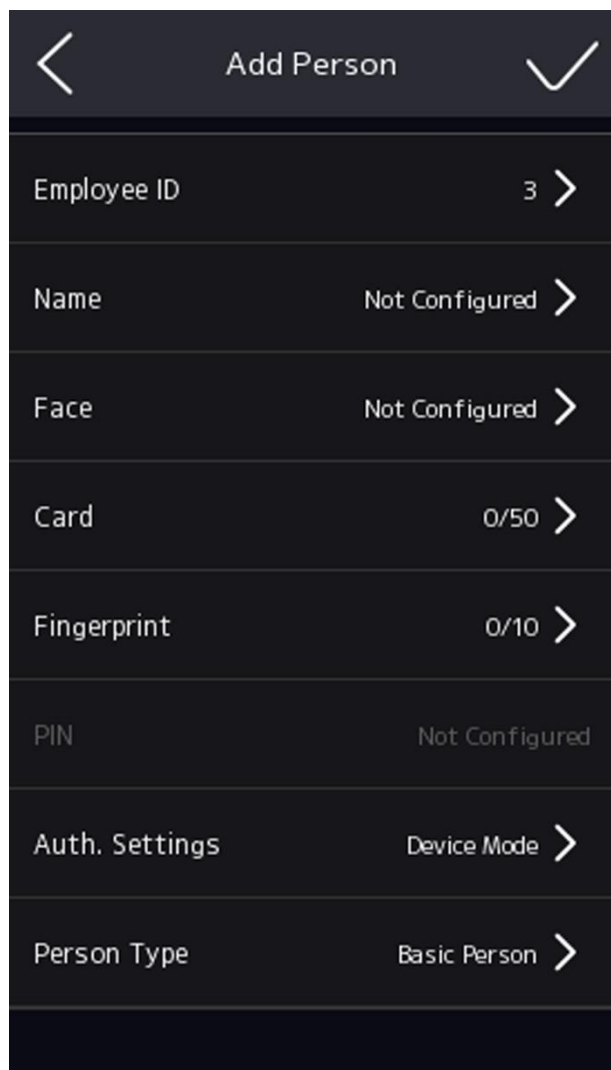
В интерфейсе управления пользователями можно добавлять, редактировать, удалять пользователей и выполнять поиск.

7.3.1 Добавление администратора

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

Шаги

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



Add Person	
Employee ID	3 >
Name	Not Configured >
Face	Not Configured >
Card	0/50 >
Fingerprint	0/10 >
PIN	Not Configured
Auth. Settings	Device Mode >
Person Type	Basic Person >

3. Внесите необходимые изменения в поле **Employee ID** («Идентификатор сотрудника»).

Примечание

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

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

Примечание

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

5. Опционально. Добавьте изображение лица, отпечатки пальцев, карты или пин-код для учетной записи администратора.

Примечание

- Подробная информация о добавлении изображения лица представлена в разделе [Добавление изображения лица](#).

Примечание

Подробная информация о добавлении отпечатков пальцев представлена в разделе [Добавление отпечатков пальцев](#).

- Подробная информация о добавлении карты представлена в разделе [Добавление карты](#).
- Подробная информация о добавлении пароля представлена в разделе [Добавление пароля](#).

6. Опционально. Можно выбрать тип аутентификации администратора.

Примечание

Подробная информация о выборе типа аутентификации представлена в разделе [Настройка режима аутентификации](#).

7. Установите **Person Type** («Тип сотрудника / посетителя») и **Person Role** («Роль сотрудника / посетителя»).

8. Включите права администратора.

Активация прав администратора

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

9. Можно включить **Attendance Check Only** («Только проверка УРВ»). После включения данного параметра для этого пользователя не будут предоставлены права доступа.

10. Нажмите , чтобы сохранить настройки.

7.3.2 Добавление изображения лица

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

Шаги

Примечание

Для добавления доступно до 1500 изображений лиц.

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

2. Нажмите **User** → + («Пользователь → +») для перехода на страницу **Add User** («Добавить пользователя»).

3. Внесите необходимые изменения в поле **Employee ID** («Идентификатор сотрудника»).

Примечание

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

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

Примечание

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

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

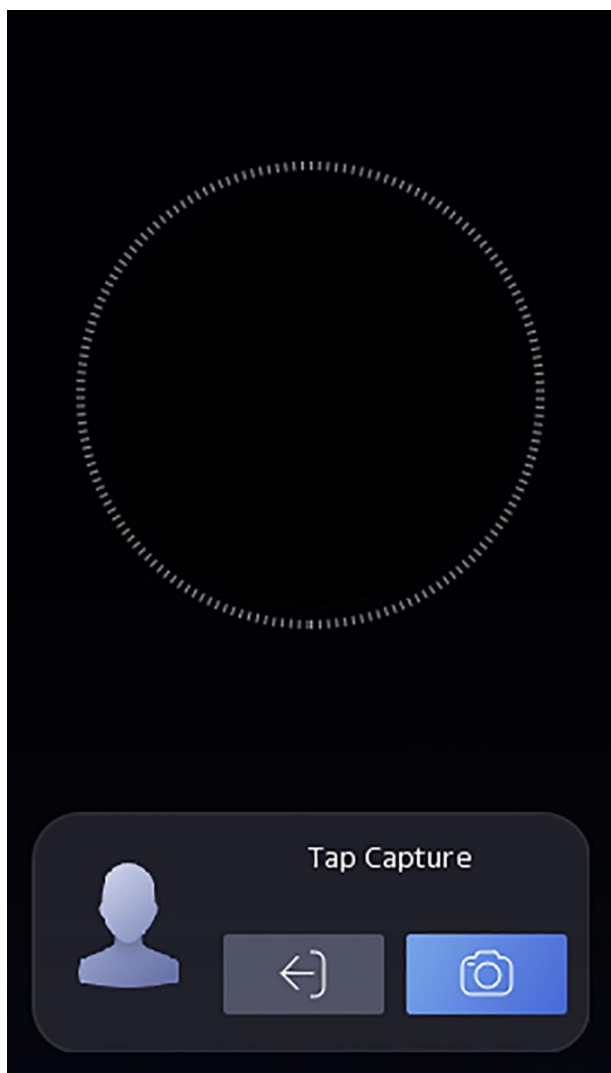


Рисунок 7-9. Добавление изображения лица

6. Посмотрите в камеру.

 Примечание

- Перед добавлением изображения лица убедитесь, что лицо находится в пределах отображенного контура.
- Убедитесь, что качество и размер изображения лица соответствуют требованиям.
- Подробная информация по добавлению изображений лиц представлена в разделе [Рекомендации по сбору / сравнению изображений лиц](#).

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

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

8. Опционально. Нажмите кнопку **Try Again** («Попробовать снова») и измените положение лица, чтобы повторить процедуру добавления.

9. Задайте роль пользователя.

Администратор

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

Обычный пользователь

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

10. Нажмите , чтобы сохранить настройки.

7.3.3 Добавление отпечатков пальцев

После добавления отпечатков пальцев пользователь сможет проходить аутентификацию с помощью отпечатков пальцев.

Шаги

Примечание

- Устройство должно поддерживать данную функцию.
- Для добавления доступно до 3000 отпечатков пальцев.

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

2. Нажмите **User** → + («Пользователь → +») для перехода на страницу **Add User** («Добавить пользователя»).

3. Внесите необходимые изменения в поле **Employee ID** («Идентификатор сотрудника»).

Примечание

- Идентификатор сотрудника может содержать до 32 символов. Он может состоять из букв верхнего / нижнего регистра и цифр.
- Идентификатор сотрудника не должен начинаться с цифры 0 и не должен дублироваться.

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

Примечание

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

5. Нажмите поле **Fingerprint** («Отпечаток пальца»), чтобы перейти на страницу добавления отпечатка пальцев.

6. Следуйте инструкциям, чтобы добавить отпечатки пальцев.

Примечание

- Один и тот же отпечаток пальца нельзя добавить повторно.
- Для одного пользователя можно добавить до 10 отпечатков пальцев.
- Для добавления отпечатков пальцев также можно использовать клиентское программное обеспечение или настольный считыватель отпечатков пальцев.

Подробная информация о сканировании отпечатков пальцев представлена в разделе [Рекомендации по сканированию отпечатков пальцев](#).

7. Задайте роль пользователя.

Администратор

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

Обычный пользователь

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

8. Нажмите , чтобы сохранить настройки.

7.3.4 Добавление карты

После добавления карты пользователь сможет проходить аутентификацию с помощью карты.

Шаги

Примечание

Для добавления доступно до 3000 карт.

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

Примечание

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

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

Примечание

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

6. Нажмите поле **Card** («Карта») и нажмите +.

7. Настройте номер карты.

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

Примечание

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

8. Настройте тип карты.

9. Задайте роль пользователя.

Администратор

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

Обычный пользователь

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

10. Нажмите , чтобы сохранить настройки.

7.3.5 Добавление PIN-кода

После добавления PIN-кода пользователь сможет проходить аутентификацию с помощью PIN-кода.

Перед началом

Примечание

Убедитесь, что выбран режим пароля: **Local Password** («Локальный пароль») или **Platform Password** («Пароль платформы»). Если выбран локальный пароль, можно добавить PIN-код через устройство или веб-интерфейс. Если выбран пароль платформы, нельзя добавить PIN-код через устройство или веб-интерфейс. Необходимо добавить PIN-код через платформу. Подробная информация о выборе типа пароля представлена в разделе [Настройка режима аутентификации](#).

Шаги

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

Примечание

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

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

Примечание

- В имени пользователя могут быть цифры, буквы верхнего и нижнего регистра и специальные символы.

- Предлагаемое имя пользователя должно содержать не более 32 символов.

5. Создайте PIN-код для пользователя.

Примечание

Убедитесь, что выбран режим пароля **Local Password** («Локальный пароль»), иначе область PIN-кода нельзя будет редактировать.

6. Задайте роль пользователя.

Администратор

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

Обычный пользователь

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

7. Нажмите , чтобы сохранить настройки.

7.3.6 Настройка режима аутентификации

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

Шаги

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

Device («Режим устройства»)

Перед установкой режима устройства перейдите на страницу **Access Control Settings** («Настройки контроля доступа»). Подробная информация представлена в разделе *Настройка параметров контроля доступа*.

Custom («Пользовательский режим»)

При необходимости допускается сочетание различных режимов аутентификации.

4. Нажмите , чтобы сохранить настройки.

7.3.7 Поиск и изменение параметров пользователя

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

Поиск пользователя

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

Редактирование параметров пользователя

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

Примечание

Не допускается редактирование идентификатора сотрудника.

7.4 Настройка учета рабочего времени (УРВ)

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

Примечание

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

7.4.1 Отключение функции учета рабочего времени через устройство

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

Нажмите **Platform Attendance** («УРВ через платформу») для перехода на соответствующую страницу.

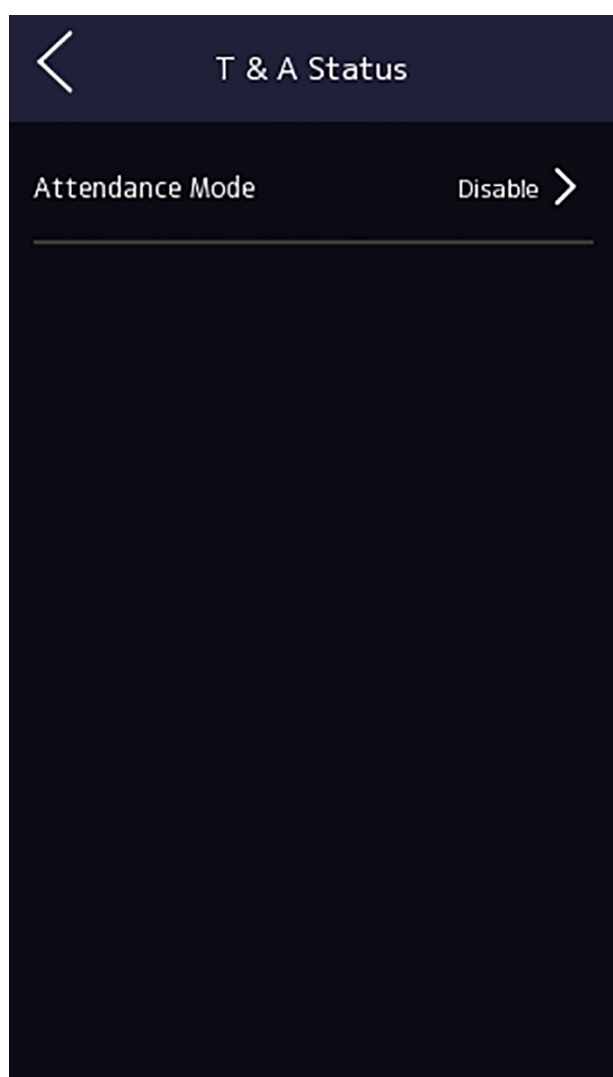


Рисунок 7-10. Отключение режима УРВ

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

На начальной странице не будут отображаться статусы УРВ и интерфейс настроек учета рабочего времени. Система будет следовать правилам УРВ, настроенным на платформе.

7.4.2 Настройка подсчета результатов УРВ вручную через устройство

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

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Подробная информация представлена в разделе **Управление пользователями**.

Шаги

1. Нажмите **Platform Attendance** («УРВ через платформу») для перехода на соответствующую страницу.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual** («Подсчет вручную»).

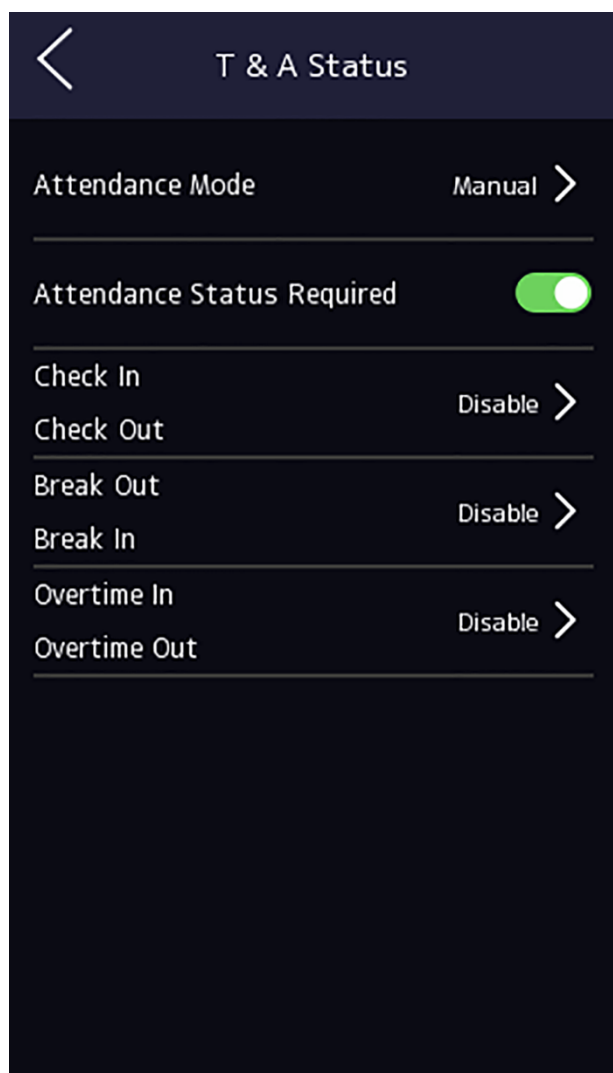


Рисунок 7-11. Режим УРВ вручную

3. Включите **Attendance Status Required** («Обязательный статус УРВ»).

4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

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

Имя будет отображаться на странице статуса УРВ и странице результатов аутентификации.

Результат

При аутентификации можно вручную выбрать статус УРВ.

Примечание

Если не выбрать статус, аутентификация будет неудачной.

7.4.3 Настройка параметров автоматического учета рабочего времени через устройство

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

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Подробная информация представлена в разделе [Управление пользователями](#).

Шаги

1. Нажмите **Platform Attendance** («УРВ через платформу») для перехода на соответствующую страницу.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Auto** («Автоматически»).

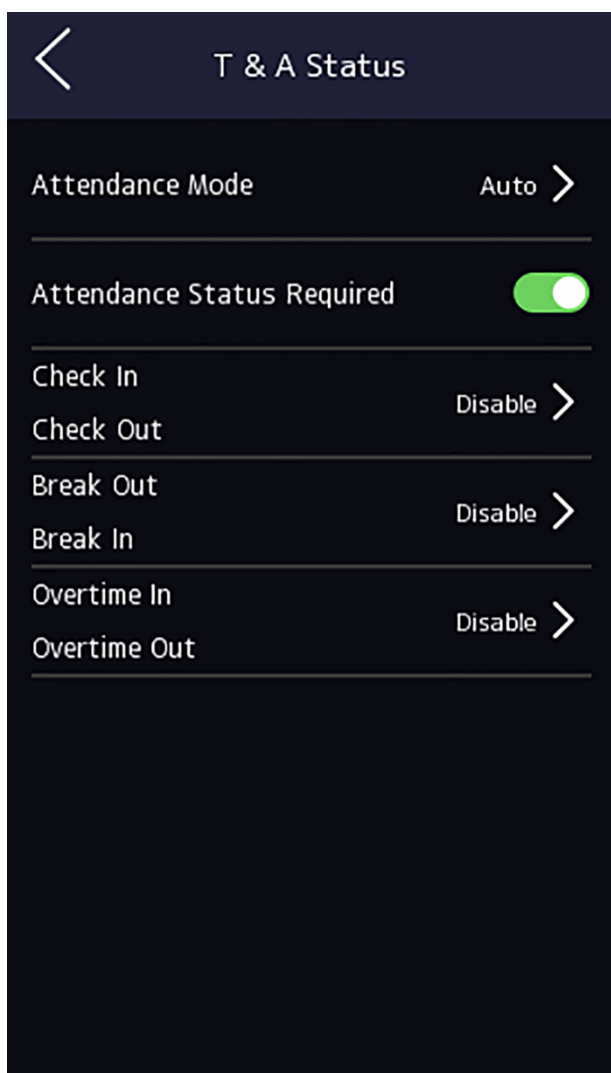


Рисунок 7-12. Режим автоматического учета рабочего времени

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

4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

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

Имя будет отображаться на странице статуса УРВ и странице результатов аутентификации.

6. Установите расписание статуса.

- 1) Нажмите **Attendance Schedule** («Расписание УРВ»).
- 2) Выберите **Monday** («Понедельник»), **Tuesday** («Вторник»), **Wednesday** («Среда»), **Thursday** («Четверг»), **Friday** («Пятница»), **Saturday** («Суббота») или **Sunday** («Воскресенье»).
- 3) Установите время начала дня для выбранного статуса УРВ.
- 4) Нажмите **Confirm** («Подтвердить»).
- 5) При необходимости повторно выполните инструкции, изложенные выше.

Примечание

Статус УРВ будет действителен в течение настроенного расписания.

Результат

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

Пример

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

7.4.4 Настройка параметров автоматического УРВ и УРВ вручную через устройство

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

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Подробная информация представлена в разделе **Управление пользователями.**

Шаги

1. Нажмите **Platform Attendance** («УРВ через платформу») для перехода на соответствующую страницу.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual and Auto** («Подсчет автоматически и вручную»).

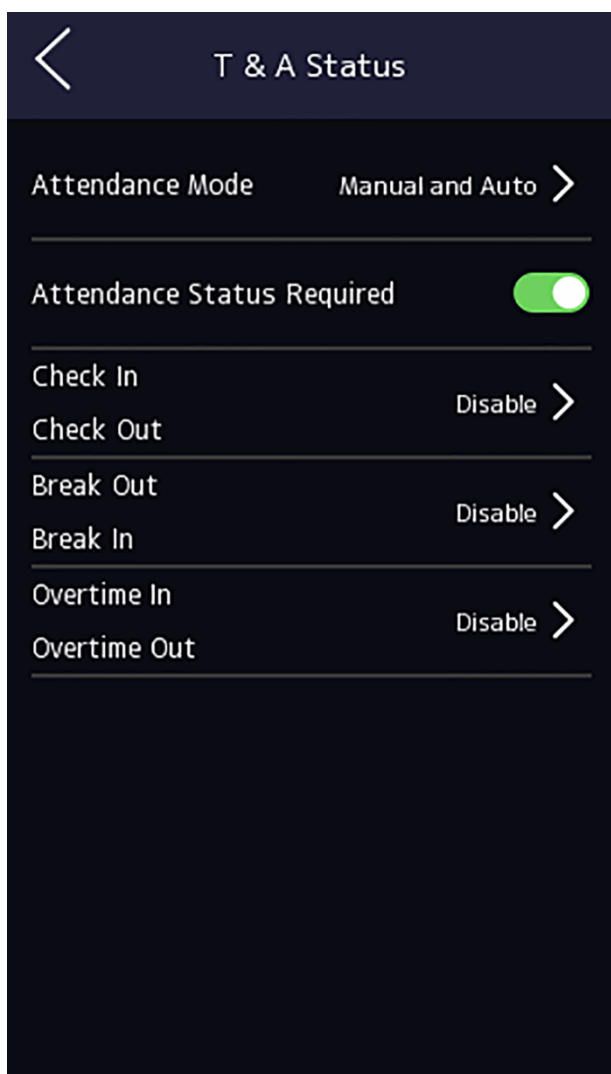


Рисунок 7-13. Подсчет результатов УРВ автоматически и вручную

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

4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

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

Имя будет отображаться на странице статуса УРВ и странице результатов аутентификации.

6. Установите расписание статуса.

1) Нажмите **Attendance Schedule** («Расписание УРВ»).

2) Выберите **Monday** («Понедельник»), **Tuesday** («Вторник»), **Wednesday** («Среда»), **Thursday** («Четверг»), **Friday** («Пятница»), **Saturday** («Суббота») или **Sunday** («Воскресенье»).

3) Установите время начала дня для выбранного статуса УРВ.

4) Нажмите **OK**.

5) При необходимости повторно выполните инструкции, изложенные выше.

Примечание

Статус УРВ будет действителен в течение настроенного расписания.

Результат

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

Пример

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

7.5 Управление данными

Данные можно удалять, импортировать и экспортировать.

7.5.1 Удаление данных

Удаление данных пользователя.

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

7.5.2 Импорт данных

Шаги

1. Вставьте USB-накопитель в устройство.
2. На домашней странице нажмите **Data** → **Import Data** («Данные → Импортировать данные»).
3. Нажмите **User Data** («Данные пользователя»), **Face Data** («Данные изображений лиц») или **Access Control Parameters** («Параметры контроля доступа»).

Примечание

Импортированные параметры контроля доступа являются файлами конфигурации устройства.

4. Введите созданный пароль для экспорта данных. Если при экспорте данных пароль не был создан, оставьте пустым поле ввода и сразу нажмите **ОК**.

Примечание

- При передаче всех данных пользователя с одного устройства (устройство А) на другое (устройство В) необходимо экспортировать данные с устройства А на USB-накопитель, а затем импортировать данные с USB-накопителя на устройство В. В этом случае необходимо импортировать данные пользователя перед импортом фотографии профиля.
- Поддерживаемый формат USB-накопителя – FAT32.
- Импортированные изображения должны быть сохранены в папке корневой директории (enroll_pic), а имя изображения должно соответствовать следующим правилам:

№ карты_Имя_Отдел_Идентификатор сотрудника_Пол.jpg

- Если в папке enroll_pic нельзя сохранить все импортированные изображения, в корневой директории можно создать другие папки с названиями enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4.
- Идентификатор сотрудника может содержать до 32 символов. Он может состоять из букв верхнего / нижнего регистра и цифр. Он не может быть продублирован или начинаться с цифры 0.
- Ниже приведены следующие требования к изображению лица: Лицо видно полностью, взгляд направлен прямо в камеру. При фотографировании запрещено надевать головной убор. Формат фотографии: JPEG или JPG. Разрешение: не менее 640 × 480 пикселей. Размер изображения: от 60 до 200 Кбайт.

7.5.3 Экспорт данных

Шаги

1. Вставьте USB-накопитель в устройство.
2. На домашней странице нажмите **Data** → **Export Data** («Данные → Экспортировать данные»).

3. Нажмите **Face Data** («Данные изображения лица»), **Event Data** («Данные события»), **User Data** («Данные пользователя») или **Access Control Parameters** («Параметры контроля доступа»).

Примечание

Импортированные параметры контроля доступа являются файлами конфигурации устройства.

4. Опционально. Создайте пароль для экспорта. При импорте данных на другое устройство, необходимо ввести пароль.

Примечание

- Поддерживаемый формат USB-накопителя – DB.

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

7.6 Идентификация личности

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

7.6.1 Аутентификация с помощью одного типа учетных данных

Перед аутентификацией установите тип аутентификации пользователя. Подробная информация представлена в разделе [Настройка режима аутентификации](#).

Пройдите аутентификацию по лицу, отпечаткам пальцев или карте.

Распознавание лиц

Расположите лицо прямо перед камерой и начните аутентификацию.

Считывание отпечатков пальцев

Поместите зарегистрированный отпечаток пальца на модуль считывания отпечатка пальца и запустите аутентификацию по отпечатку пальца.

Карта

Приложите карту к области считывания карт и начните аутентификацию.

Примечание

Можно использовать обычную IC-карту или зашифрованную карту.

PIN-код

Введите PIN-код для прохождения аутентификации.

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

7.6.2 Аутентификация с помощью нескольких типов учетных данных

Перед началом

Перед аутентификацией установите тип аутентификации пользователя.

Подробная информация представлена в разделе [Настройка режима аутентификации](#).

Шаги

1. Если для аутентификации доступны режимы **Card and Face** («Карта и лицо»), **Password and Face** («Пароль и лицо»), **Card and Password** («Карта и пароль»), **Card and Face and Fingerprint** («Карта, лицо и отпечатки пальцев»), используйте выбранный режим аутентификации учетных данных согласно инструкциям на интерфейсе просмотра в режиме реального времени.

Примечание

- Можно использовать обычную IC-карту или зашифрованную карту.

2. После завершения проверки учетных данных приступите к аутентификации других учетных данных.

Примечание

- Подробная информация о сканировании отпечатков пальцев представлена в разделе **Рекомендации по сканированию отпечатков пальцев**.
- Подробная информация об аутентификации лица представлена в разделе **Рекомендации по сбору / сравнению изображений лиц**.

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

7.7 Основные настройки

Можно настроить параметры голосовых предупреждений, времени, спящего режима, языка, номера микрорайона, номера здания, номера помещения, защиты данных и параметры отображения.

Нажмите на экран начальной страницы, удерживайте кнопку мыши в течение 3 секунд, затем переместите курсор влево/вправо (в соответствии с инструкциями) и войдите в систему в качестве администратора. Нажмите **System Settings** → **Basic** («Настройки системы → Основные настройки»)

Настройки звука

Можно включить/отключить функцию голосовых предупреждений и настроить громкость.

Примечание

Можно установить громкость в диапазоне от 0 до 10. 0 — отключение громкости.

Настройки времени

Установите часовой пояс, время устройства и летнее время.

Спящий режим

Настройте время перехода устройства в спящий режим (в минутах). На главной странице, если установлено время перехода в спящий режим на 30 минут, устройство перейдет в спящий режим через 30 минут без каких-либо операций.

Примечание

Если настроить время перехода в спящий режим на 0, устройство не перейдет в спящий режим.

Выбор языка

Выберите необходимый язык.

Номер микрорайона

Укажите номер микрорайона, в котором установлено устройство.

Номер здания

Укажите номер здания, в котором установлено устройство.

Номер помещения»

Укажите номер помещения, в котором установлено устройство.

Настройки вызова

Автоматический вызов после набора номера

Можно включить **Automatic Calling After Dialing** («Автоматический вызов после набора номера») и установить период ожидания.

Цель для кнопки вызова центра управления

Выберите цель вызова.

Сервер VoIP

Выберите сервер VoIP.

Конфиденциальность

Имя / Идентификатор сотрудника

Можно выбрать отображение / скрытие / частичное скрытие имени и идентификатора сотрудника при аутентификации.

Изображение лица

Можно выбрать отображение / скрытие изображения лица при аутентификации.

Сохранение зарегистрированного изображения

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

Сохранение изображения при аутентификации

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

Загрузка изображения при аутентификации

Загрузите полученные при аутентификации изображения на платформу автоматически.

Загрузка захваченных изображений во время звонка

Автоматическая загрузка полученных во время звонка изображений на платформу.

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 (50 Гц)

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

NTSC (60 Гц)

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

7.8 Настройка биометрических параметров

Вы можете настроить параметры лица, чтобы улучшить производительность распознавания лиц. Настраиваемые параметры включают уровень безопасности антиспуфинга, дальность распознавания лиц, интервал распознавания лиц, уровень безопасности 1:N, уровень безопасности 1:1, настройки режима ЕСО и детекцию наличия / отсутствия маски.

Длительное нажатие в течение 3 секунд на начальной странице позволяет перейти на страницу аутентификации администратора. Нажмите **System Settings** → **Biometrics** («Настройки системы → Биометрические данные»)

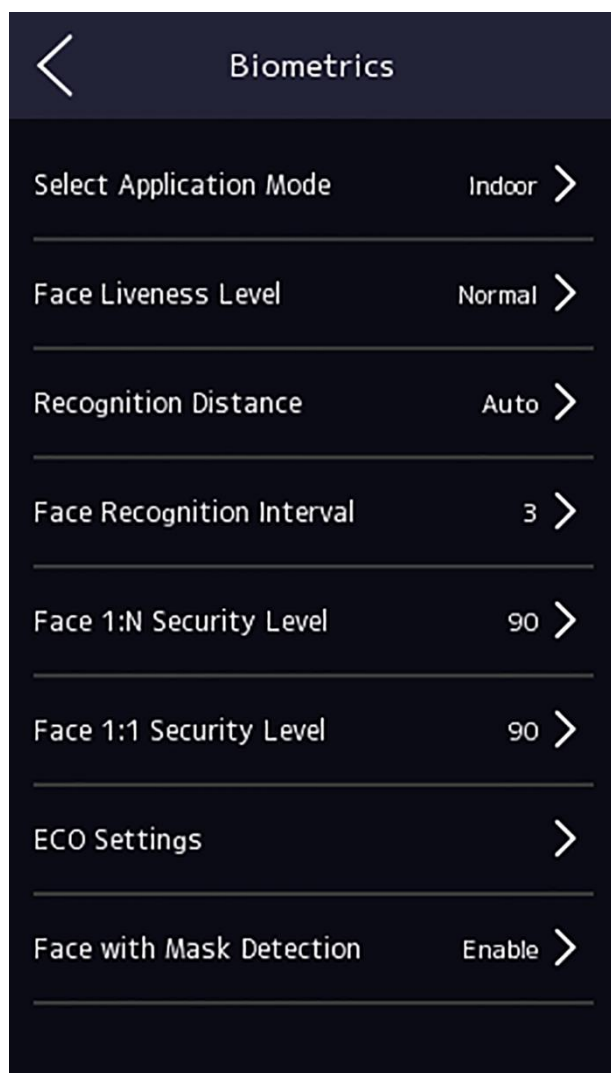


Рисунок 7-14 Страница настройки биометрических данных

Таблица 7-1 Параметры изображений лиц

Параметр	Описание
Уровень безопасности антиспуфинга	После включения функции антиспуфинга можно установить надлежащий уровень безопасности при выполнении аутентификации лица в режиме реального времени.
Дальность распознавания	Задание допустимого расстояния между пользователем и камерой при аутентификации.

Параметр	Описание
Интервал распознавания лиц	Временной интервал между двумя циклами распознавания лиц при непрерывной работе.  Примечание Можно ввести число от 1 до 10.
Уровень безопасности 1:N	Настройте пороговое значение совпадения при аутентификации в режиме сопоставления 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений.
Уровень безопасности 1:1	Настройте пороговое значение совпадения при аутентификации в режиме сопоставления 1:1. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений.
Настройки режима ЭКО	После включения ЭКО-режима устройство будет использовать ИК-подсветку для аутентификации лиц в условиях низкой освещенности или в темноте. Настройте пороговое значение для ЭКО-режима, ЭКО-режима (1:N) и ЭКО-режима (1:1). Пороговое значение ЭКО-режима Установите пороговое значение для ЭКО-режима при включении функции. Чем больше значение, тем быстрее устройство переключается в ЭКО-режим.

Параметр	Описание
	ЭКО-режим (1:1) Настройте пороговое значение совпадения при аутентификации в ЭКО-режиме 1:1. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. ЭКО-режим (1:N) Настройте пороговое значение совпадения при аутентификации в ЭКО-режиме 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений
Настройка детекции наличия / отсутствия маски	После включения детекции наличия / отсутствия маски система распознает наличие / отсутствие маски. Можно настроить Face with Mask & Face (1:1) («Лицо с маской (1:1)»), Face with Mask & Face (1:N) («Лицо с маской (1:N)»), ECO (1:1) Threshold («Пороговое значение ЭКО-режима (1:1)»), ECO Mode (1:N) Threshold («Пороговое значение ЭКО-режима (1:N)») и Prompt Method («Метод подсказки»). Сопоставление лица и лица с маской (1:1) Настройте значение сходства при детекции наличия / отсутствия маски в режиме сопоставления 1:1. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Сопоставление лица и лица с маской (1:N) Настройте значение сходства при детекции наличия / отсутствия маски в режиме сопоставления 1:N. Чем больше данное значение, тем меньше вероятность ложных

Параметр	Описание
	совпадений и тем больше вероятность отклонений ложных совпадений. Пороговое значение ЭКО-режима (1:1) Настройте значение сходства при детекции наличия / отсутствия маски в ЭКО-режиме сопоставления 1:1. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Пороговое значение ЭКО-режима (1:N) Настройте значение сходства при детекции наличия / отсутствия маски в ЭКО-режиме сопоставления 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Подсказка Настройте значения None («Нет»), Reminder of Wearing («Напоминание о необходимости ношения маски») и Must Wear («Предупреждение об обязательном ношении»). Напоминание о необходимости ношения маски Если у сотрудника / посетителя отсутствует маска при аутентификации, устройство выдаст предупреждение, затем дверь откроется. Предупреждение об обязательном ношении Если у сотрудника / посетителя отсутствует маска при аутентификации, устройство выдаст предупреждение, дверь будет оставаться закрытой. Нет

Параметр	Описание
	Если у сотрудника / посетителя отсутствует маска при аутентификации, устройство выдаст предупреждение.

7.9 Пользовательские настройки

Можно настроить пользовательские настройки.

Шаги

1. Нажмите **Basic Settings** → **Preference** («Основные настройки → Пользовательские настройки») для перехода на страницу пользовательских настроек.

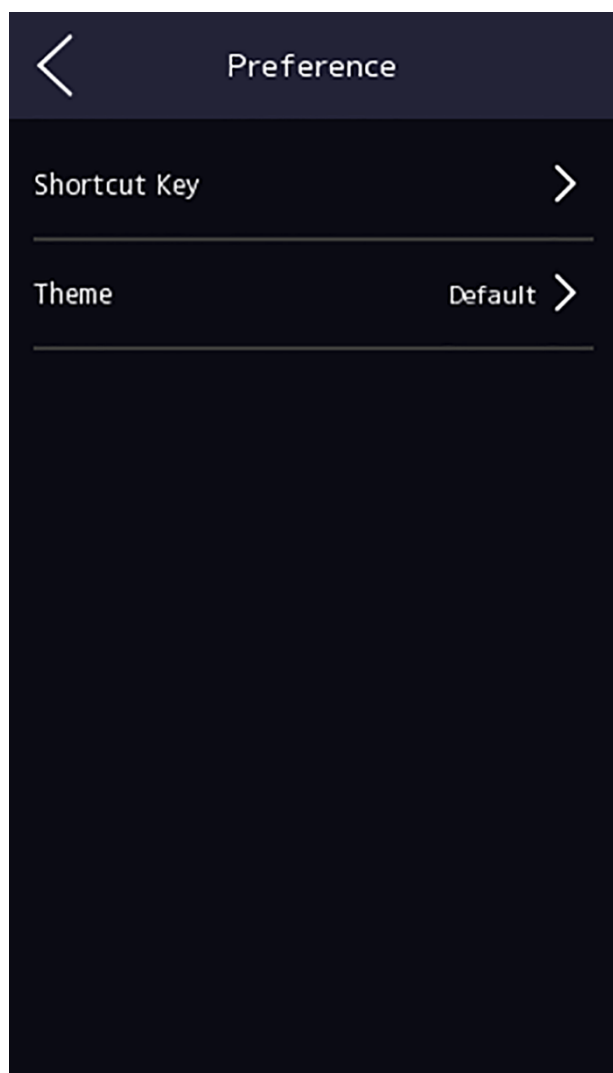


Рисунок 7-15 Настройка пользовательских предпочтений

Горячие клавиши

Выберите сочетание клавиш, отображаемое на странице аутентификации, для настройки функций, включая функцию ввода пароля, функцию QR-кода, функцию вызова и тип вызова.

Примечание

Доступны следующие типы вызова: **Call Room** («Вызов помещения»), **Call Center** («Вызов центра управления»), **Call Specified Room No.** («Вызов помещения по заданному номеру») и **Call APP** («Вызов приложения»).

Пароль

Включение этой функции позволит пройти аутентификацию через пароль.

QR-код

Можно использовать функцию сканирования QR-кода в интерфейсе аутентификации. Устройство загрузит информацию, считанную с QR-кода, на платформу.

Вызов кабинета

При нажатии кнопки вызова на странице аутентификации, необходимо набрать номер кабинета для звонка.

Вызов центра управления

При нажатии кнопки вызова на странице аутентификации можно связаться с центром управления напрямую.

Вызов кабинета по заданному номеру

Необходимо задать номер кабинета. При нажатии кнопки вызова на странице аутентификации можно связаться с настроенным кабинетом напрямую, без набора номера.

Вызов приложения

Когда нажимаете кнопку вызова на странице аутентификации, появляется мобильный клиент, в который добавлено устройство.

Вызов номера видеодомофона

После включения номер видеодомофона будет отображаться на странице аутентификации.

Вызов центра управления / вызов центра VoIP

После включения функции на странице аутентификации можно выполнить вызов в центр управления или центр VoIP.

Тема

Можно настроить тему окна подсказки на странице аутентификации. Можно нажать **Theme** («Тема») и выбрать **Authentication** («Аутентификация») или **Simple** («Упрощенный режим»).

Аутентификация

Страница аутентификации устройства будет отображаться на странице просмотра в режиме реального времени. Имя сотрудника, идентификатор сотрудника и изображения лица будут отображаться после аутентификации.

Простая

После выбора данного режима страница аутентификации не будет отображаться в окне просмотра в режиме реального времени, соответственно, имя сотрудника, идентификатор сотрудника и изображения лица будут скрыты.

Режим домофонии

После выбора этого режима ярлык будет отображаться внизу страницы аутентификации.

Отображение записи УРВ во время проверки

Можно включить **Show Attendance Record During Check** («Показывать запись УРВ во время проверки»), после включения запись УРВ будет отображаться во время проверки.

7.10 Изменение пароля устройства

Можно изменить пароль устройства, введя старый пароль.

Шаги

1. Длительное нажатие в течение 3 секунд на начальной странице позволяет перейти на страницу аутентификации администратора. Нажмите **System → Password** («Система → Пароль»).
2. Нажмите **Change Device Password** («Изменить пароль устройства»).
3. Введите старый пароль.

Примечание

Если вы забыли пароль, можно нажать **Forgot Password** («Забыли пароль») и изменить пароль. Подробная информация представлена в разделе [Забывать пароль](#).

4. Введите новый пароль и подтвердите его.

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее.

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

5. Нажмите **ОК**.

7.11 Настройки параметров аутентификации

Можно настроить разрешения управления доступом, включая режим аутентификации, включение карты NFC, включение карты M1, параметры дверного контакта, продолжительность открытия, интервал аутентификации, продолжительность отображения результата аутентификации и режим пароля.

На главной странице нажмите **Authentication Settings** («Настройки аутентификации»), чтобы перейти на страницу настроек.

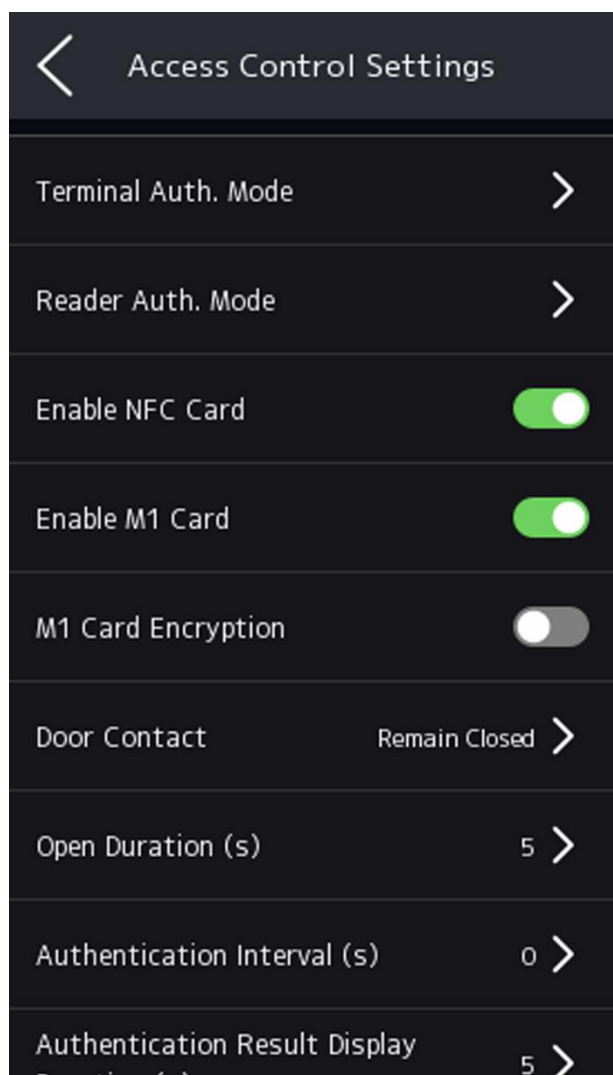


Рисунок 7-16 Настройки аутентификации

Ниже представлено следующее описание параметров:

Таблица 7-2. Описание параметров контроля доступа

Параметр	Описание
Режим аутентификации терминала	Выбор режима аутентификации лиц. Режим аутентификации может быть изменен.  Примечание - Только устройства с модулем считывания отпечатков пальцев поддерживают функции, связанные со считыванием отпечатков пальцев. - Биометрические системы аутентификации не могут гарантировать абсолютную защиту от подделки биометрических данных. Если требуется более высокий уровень безопасности, используйте несколько режимов аутентификации. - При использовании нескольких режимов аутентификации перед началом аутентификации лица завершите предыдущие проверки.
Режим аутентификации (Режим аутентификации при помощи считывателя карт)	Выберите режим аутентификации при помощи считывателя карт.
Включение распознавания NFC-карты	Включите функцию для аутентификации с использованием NFC-карты.
Включение распознавания M1-карты	Включите функцию для аутентификации с использованием M1-карты.

Параметр	Описание
Шифрование M1-карты	Включение шифрования M1-карты может повысить уровень безопасности при аутентификации. Копирование карты будет усложнено.
Дверной контакт	Выберите необходимый режим: Open (Remain Open) («Открыть и оставить дверь открытой») или Close (Remain Closed) («Закрыть и оставить дверь закрытой»). По умолчанию, установлен режим Close (Remain Closed) («Закрыть и оставить дверь закрытой»).
Длительность открытого состояния	Укажите длительность разблокированного состояния двери. Дверь будет заблокирована, если движение отсутствует в течение установленного времени. Доступный диапазон времени блокировки двери: от 1 до 255 с.
Интервал аутентификации	Установите интервал аутентификации устройства. Доступный диапазон интервала аутентификации: от 0 до 65535.
Отображение результата аутентификации	Настройте продолжительность отображения результата аутентификации.
Режим пароля	Персональный PIN-код, настраиваемый через платформу Управление PIN-кодом выполняется через платформу. Нельзя настроить PIN-код через веб-интерфейс. Персональный PIN-код, настраиваемый через устройство

Параметр	Описание
	PIN-код устанавливается через устройство или веб-интерфейс. Нельзя настроить PIN-код через другую платформу.

7.12 Обслуживание системы

Можно посмотреть системную информацию устройства и емкость. Также можно обновить устройство, изучить руководство пользователя, восстановить систему до заводских настроек, настроек по умолчанию и перезагрузить систему.

Длительное нажатие в течение 3 секунд на начальной странице позволяет перейти на страницу аутентификации администратора. Нажмите **Maint.** («Обслуживание»).

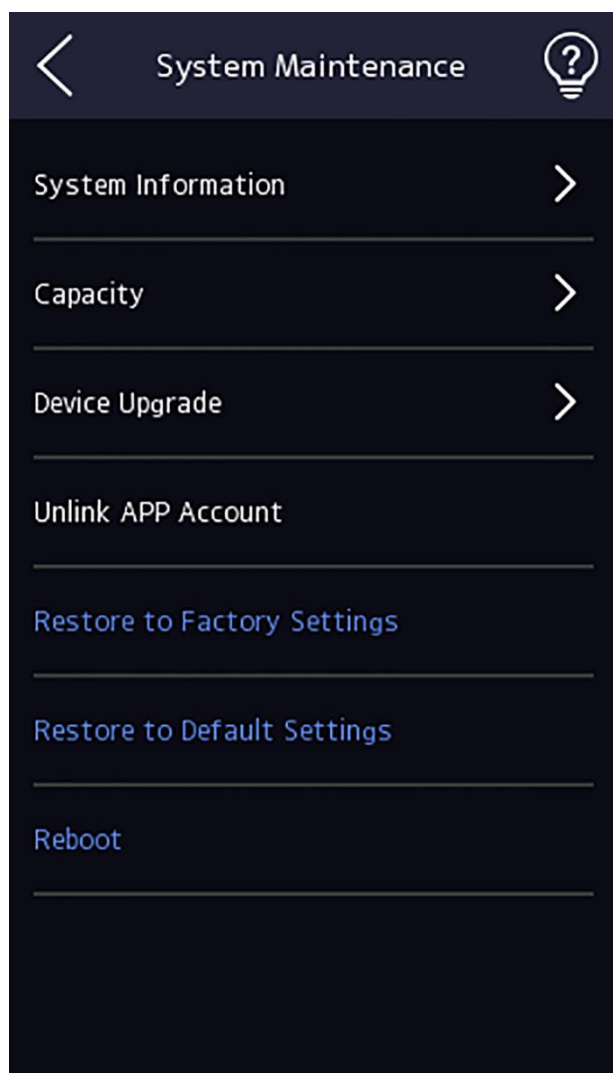


Рисунок 7-17 Страница обслуживания

Системная информация

Можно просмотреть информацию об устройстве, включая модель устройства, серийный номер, версию прошивки, MAC-адрес, данные о производстве и лицензию.

Примечание

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

Нажмите  и введите пароль администратора для просмотра информации о версии устройства.

Параметры изображения лица

Настройка детекции подлинности биометрических данных (антиспуфинг)

Уровень безопасности антиспуфинга

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

Пороговое значение детекции подлинности биометрических данных (антиспуфинг)

Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Чем меньше данное значение, тем больше вероятность ложных совпадений, и тем меньше вероятность отклонений ложных совпадений.

Блокировка при детекции подлинности биометрических данных (антиспуфинг)

При сбое детекции подлинности биометрических данных лица (антиспуфинг) устройство будет заблокировано.

Длительность блокировки

Длительность блокировки при сбое детекции подлинности биометрических данных лица (антиспуфинг)

Информация о версии устройства

Вы можете просмотреть информацию об устройстве.

Емкость

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

Примечание

Некоторые модели устройств поддерживают отображение количества отпечатков пальцев. Подробная информация представлена на фактической странице интерфейса.

Обновление устройства

Обновление онлайн

Когда устройство подключено к Hik-Connect и сети и доступен новый установочный пакет Hik-Connect, нажмите **Device Upgrade → Online Update** («Обновление устройства → Обновление онлайн») для обновления системы устройства онлайн.

Обновление через USB

Вставьте USB-накопитель в USB-интерфейс устройства. Нажмите **Device Upgrade → Update via USB** («Обновление устройства → Обновление через USB»). Устройство прочитает файл *digicap.dav* с USB-накопителя для запуска обновления.

Руководство пользователя

Для просмотра руководства пользователя необходимо сканировать QR-код.

Восстановление настроек изготовителя

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

Восстановление настроек по умолчанию

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

Перезагрузка

Устройство перезагрузится после подтверждения.

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.
- Убедитесь, что устройство и смартфон находятся в одной сети 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** («Войти»).

8.2 Обзор

Можно просмотреть состояние двери, состояние сети и основную информацию, а также настроить управление пользователями, задать интеллектуальные настройки, настройки аутентификации и параметры двери с помощью ярлыка быстрого доступа.

Описание функций:

Состояние двери



Состояние двери: открыта / закрыта / оставить открытой / оставить закрытой. Можно нажать, чтобы выбрать состояние двери «открыта / закрыта / оставить открытой / оставить закрытой».

Ярлык быстрого доступа

Можно настроить управление пользователями, задать интеллектуальные настройки, настройки аутентификации и параметры дверей с помощью ярлыка быстрого доступа.

Состояние сети

Можно посмотреть состояние подключения и регистрации в сети.

Основная информация

Можно посмотреть модель, серийный номер и версию прошивки.

8.3 Забыть пароль

Если вы забыли пароль для входа 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»).

Проверка по контрольным вопросам

Ответьте на контрольные вопросы.

Подтверждение по электронной почте

1. Экспортируйте QR-код и отправьте его по адресу в качестве вложения.
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.

8.4 Настройка

8.4.1 Отображение информации об устройстве

Просмотрите название устройства, язык, модель, серийный номер, версию, номер интерфейса входа / выхода, локальный номер RS-485, номер тревожного входа / выхода, номер регистрации, заводскую информацию, емкость устройства и т. д.

На главной странице нажмите  → **System Settings** → **Basic Information** («Настройки системы → Основная информация»).

Просмотрите название устройства, язык, модель, серийный номер, версию, номер интерфейса входа / выхода, локальный номер RS-485, номер тревожного входа / выхода, номер регистрации, заводскую информацию, емкость устройства и т. д.

Нажмите **Save** («Сохранить»).

8.4.2 Настройка времени

Установите часовой пояс, режим синхронизации времени и отображаемое время.

Нажмите  → **System Settings** → **Time Settings** («Настройки системы → Настройки времени») для перехода на соответствующую страницу.

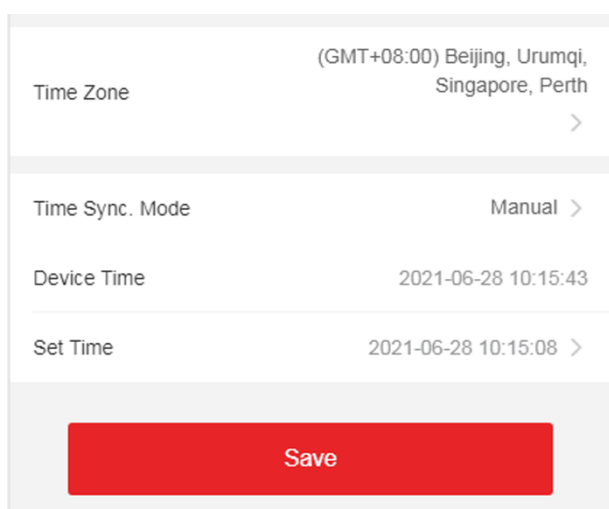


Рисунок 8-1. Настройка времени

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

Часовой пояс

Выберите часовой пояс, в котором находится устройство.

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 параметров DST

Шаги

1. Нажмите  → **System Settings** → **Time Settings** («Настройки системы → Настройки времени») для перехода на соответствующую страницу.

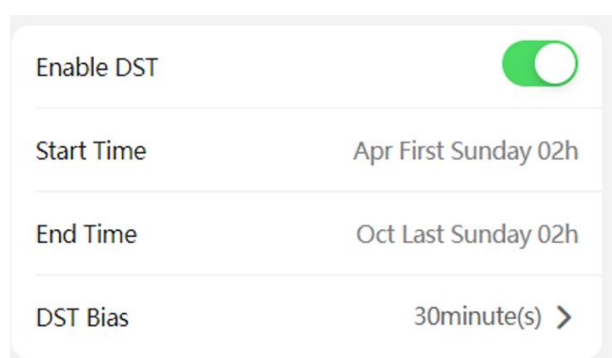


Рисунок 8-2. Летнее время

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

8.4.4 Управление пользователями

Шаги

1. Нажмите  → **User Management** → **User Management** → **admin** («Управление пользователями → Управление пользователями → Администратор»), чтобы перейти на соответствующую страницу.
2. Введите старый пароль и создайте новый пароль.
3. Подтвердите новый пароль.
4. Нажмите **Save** («Сохранить»).

Примечание

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя от 8 до 16 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 безопаснее.

8.4.5 Настройка сетевых параметров

Проводная сеть

Настройка проводной сети.

Нажмите  → **Communication Settings** → **Wired Network** («Настройки связи → Проводная сеть») для перехода на соответствующую страницу.

DHCP

Если отключить эту функцию, необходимо настроить адрес IPv4, маску подсети IPv4, шлюз по умолчанию IPv4, Мас-адрес и MTU, Мас-адрес, MTU.

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

DNS-сервер

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

Настройка параметров Wi-Fi

Задайте параметры Wi-Fi для беспроводного подключения устройства.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите  → **Communication Settings** → **Wi-Fi** («Настройки связи → Wi-Fi») для перехода на соответствующую страницу.

2. Включите **Wi-Fi**.

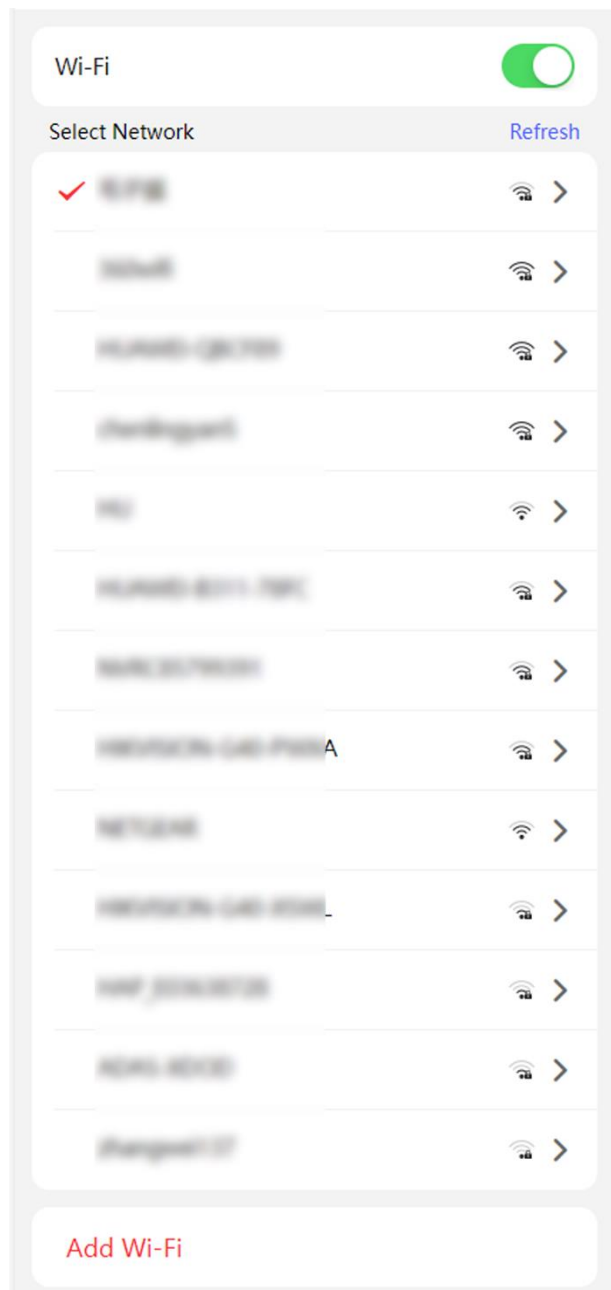


Рисунок 8-3. Wi-Fi

3. Добавьте Wi-Fi.

1) Нажмите **Add Wi-Fi** («Добавить Wi-Fi»).

2) Введите **Wi-Fi Name** («Имя Wi-Fi») и **Wi-Fi Password** («Пароль Wi-Fi») и выберите **Encryption Type** («Тип шифрования»).

3) Нажмите **Save** («Сохранить»).

4. Выберите имя Wi-Fi и нажмите **Connect** («Подключиться»).

5. Введите пароль и нажмите **Save** («Сохранить»).

Настройка параметров порта

Можно настроить HTTP и HTTPS при доступе к устройству через сеть.

Нажмите  → **Network Service** → **HTTP(S)** («Сетевая служба → HTTP(S), чтобы перейти на соответствующую страницу.

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.

HTTPS

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

Доступ к платформе

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите  → **Device Access** → **Nik-Connect** («Доступ устройств → Nik-Connect») для перехода на страницу настроек.

Примечание

Nik-Connect — это приложение 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. Можно включить **Custom** («Пользовательская настройка») для ввода адреса сервера.

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.
- Код подтверждения не может быть **123456** или **abcdef** (без учета регистра).

4. Можно посмотреть **Register Status** («Состояние регистрации») и **Binding Status** («Состояние привязки»).

5. Включите **Video Encryption** («Шифрование видео»), создайте пароль и подтвердите его.

Примечание

После добавления устройства в приложение необходимо ввести пароль шифрования видео, чтобы просмотреть устройство в режиме реального времени.

6. Можно нажать **Bind An Account** → **View QR Code** («Привязка учетной записи → Просмотр QR-кода») и сканировать QR-код, чтобы привязать учетную запись.

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

Настройка параметров ISUP

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите  → **Device Access** → **ISUP** («Доступ устройств → ISUP») для перехода на страницу настроек.
2. Включите **ISUP**.
3. Настройте версию ISUP, адрес сервера, порт, идентификатор устройства и код шифрования.

Примечание

Если выбрана версия 5.0, необходимо также установить ключ шифрования.

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

Настройка OTAP

Подключите устройство к платформе по протоколу OTAP, чтобы получить информацию об устройстве, загрузить информацию о состоянии работы и тревогах, перезагрузить и обновить устройство.

Шаги

1. Нажмите  → **Device Access** → **OTAP** («Доступ устройств → OTAP») для перехода на страницу настроек.
2. Нажмите **Enable** («Включить»), чтобы включить OTAP.
3. Настройте **Server Address** («Адрес сервера»), **Port** («Порт»), **Device ID** («ID-устройства») и **Encryption Key** («Ключ шифрования»).
4. Нажмите **Test** («Диагностика»), чтобы убедиться, что устройство может подключиться к серверу и успешно зарегистрироваться. Обновите страницу или перезагрузите устройство, чтобы увидеть **Register Status** («Состояние регистрации»).
5. Нажмите **Save** («Сохранить»).

Настройка службы проверки на проникновение в сеть

После развертывания устройства в локальной сети можно включить службу проверки на проникновение для удаленного управления устройством.

Шаги

1. Нажмите  → **Device Access** → **Network Penetration Service** («Доступ к устройству → Служба проверки на проникновение в сеть») для перехода на страницу настроек.
2. Нажмите **Enable Penetration Service** («Включить службу проверки на проникновение»).
3. Установите **Server IP Address** («IP-адрес сервера») и **Server Port** («Порт сервера»). Создайте **User Name** («Имя пользователя») и **Password** («Пароль»).
4. Опционально. Можно настроить **Heartbeat Timeout** («Период цикла Heartbeat»). Диапазон значений: от 1 до 6000.
5. Опционально. Можно посмотреть состояние службы проверки на проникновение. Нажмите **Refresh** («Обновить»), чтобы обновить состояние.
6. Нажмите **Save** («Сохранить»).

Примечание

Служба проверки на проникновение будет автоматически отключена через 48 часов.

8.4.6 Управление пользователями

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

Шаги

1. Нажмите  → **Person Management** («Управление пользователями») для перехода на страницу настроек.
2. Добавление пользователя.

1) Нажмите +.

2) Настройте следующие параметры.

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.

Имя

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

Пользователь с длительным разрешением

Настройте долгосрочное разрешение для пользователя.

Дата начала / Дата окончания

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

Роль пользователя

Выберите роль пользователя.

Роль сотрудника / посетителя

Выберите роль для сотрудника / посетителя.

Только проверка УРВ

После выбора параметра данный пользователь не получит права на управление доступом.

Изображение лица

Добавьте изображение лица. Нажмите **Face** («Лицо»), затем нажмите **Camera** («Камера»), чтобы добавить изображение лица, или нажмите **Choose from Album** («Выбрать из альбома»), чтобы импортировать изображение лица.

Считывание отпечатков пальцев

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

Карта

Добавление карты. Нажмите **Card** («Карта»), затем нажмите «+», введите номер карты и выберите тип карты.

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.

8.4.7 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.

8.4.8 Настройки параметров контроля доступа

Настройка параметров аутентификации

Настройка параметров аутентификации.

Шаги

1. Нажмите  → **Access Control** → **Authentication Settings** («Контроль доступа → Настройки аутентификации»).
2. Нажмите **Save** («Сохранить»).

Терминал

Выберите терминал для настройки.

Тип терминала / режим терминала

Получение описания терминалов. Доступно только для чтения.

Включить устройство с функцией аутентификации

Включить функцию аутентификации.

Аутентификация

В выпадающем списке выберите режим аутентификации в соответствии с потребностями.

Интервал непрерывного распознавания лица

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.

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.

Запуск тревоги при достижении максимального количества неудачных попыток считывания карты

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

Режим основного интерфейса

Можно настроить режим основного интерфейса, выбрав **Authentication Mode** («Режим аутентификации») или **Simple** («Простой режим»).

Включение тревоги тампера

Включите детектор саботажа на считывателе карт.

Включение считывания номера карты в обратной последовательности

После включения функции номер карты будет считываться в обратной последовательности.

Настройка параметров двери

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

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

Наименование двери

Можно задать имя двери.

Длительность открытого состояния

Укажите длительность разблокированного состояния двери. Дверь будет заблокирована, если движение отсутствует в течение установленного времени.

Тип кнопки выхода

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

Дверь остается открытой после авторизации первого сотрудника (мин)

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

Тревога тайм-аута открытой двери

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

Дверной контакт

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

Закрытие двери при отключении питания

При выключении дверного замка можно установить необходимые параметры: **Remain Open** («Оставить открытым») или **Remain Closed** («Оставить закрытым»). По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).

Увеличение длительности открытого состояния

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

Код принуждения

Дверь может быть открыта при помощи кода принуждения. При этом клиент может создать уведомление о событии принуждения.

Суперпароль

Пользователь может открыть дверь с помощью суперпароля.

Примечание

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

Параметры терминала

Можно настроить параметры терминала для получения доступа.

Нажмите  → **Access Control** → **Terminal Parameters** («Контроль доступа → Параметры терминала»).

Настройте **Working Mode** («Режим работы»), выбрав **Access Control Mode** («Режим контроля доступа»). Режим контроля доступа является нормальным режимом работы устройства. Для получения доступа необходимо пройти аутентификацию с использованием учетных данных.

Удаленная аутентификация

После включения **Remote Authentication** («Удаленная аутентификация») при аутентификации устройство загрузит информацию на платформу для подтверждения открытия двери.

Локальная проверка учетных данных

После включения этой функции устройство проверит разрешения, но не оценит шаблон плана.

Период ожидания

Можно установить период ожидания удаленной аутентификации.

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

Настройка параметров безопасности карты

Нажмите  → **Access Control** → **Card Security** («Контроль доступа → Безопасность карты») для перехода на страницу настроек.

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

Включение распознавания NFC-карты

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

Включение распознавания M1-карты

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

Шифрование M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

Сектор

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

Активация распознавания ЕМ-карты

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

Примечание

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

Активация распознавания DESfire-карты

Устройство может считывать данные с DESfire-карты.

Активация распознавания FeliCa-карты

Устройство может считывать данные с FeliCa-карты.

Настройка параметров RS-485

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

Нажмите  → **Access Control** → **RS-485** («Контроль доступа → RS-485»).

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

Тип периферийного устройства

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

Примечание

После настройки и сохранения периферийного устройства устройство автоматически перезагрузится.

Протокол RS-485

Частный

Устройство может подключаться к устройству стороннего производителя через RS-485.

OSDP

Стандартный протокол RS-485.

Адрес RS-485

Задайте необходимый адрес RS-485.

Примечание

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

Скорость передачи данных

Скорость передачи при обмене данными по протоколу RS-485.

Бит данных

Бит данных при обмене данными по протоколу RS-485.

Стоповый бит

Стоповый бит при обмене данными по протоколу RS-485.

Четность / Управление потоком / Беспроводная сеть

Функция включена по умолчанию.

8.4.9 Настройка видеодомофонии

Настройки ID устройства

Устройство может быть установлено снаружи и внутри помещений. Перед использованием необходимо задать номер устройства.

Шаги

1. Нажмите  → **Intercom** → **Device ID Settings** («Домофония → Настройки ID устройства»).
2. Настройте следующие параметры.

Тип устройства

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

Примечание

При изменении типа устройства необходимо перезагрузить устройство.

Номер периода

Укажите номер периода установленного устройства.

Номер здания

Укажите номер здания.

Номер помещения

Укажите номер помещения.

Примечание

При изменении номера необходимо перезагрузить устройство.

Номер этажа

Укажите номер этажа, на котором установлено устройство.

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.

Если в качестве типа устройства выбрано **Outer Door Station** («Уличная вызывная панель»), можно настроить номер вызывной панели и номер микрорайона.

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.

Номер периода

Укажите номер периода установленного устройства.

Настройки сеанса связи

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

Шаги

1. Нажмите  → **Intercom** → **Session Settings** («Домофония → Настройки сеанса»).
2. Укажите пароль регистрации, IP-адрес пульта консьержа / диспетчера, IP-адрес частного сервера и включите протокол 1.0.

Пароль регистрации

Пароль активации пульта консьержа / диспетчера.

IP-адрес пульта консьержа / диспетчера

Настройте IP-адрес пульта консьержа / диспетчера.

IP-адрес частного сервера

IP-адрес частного сервера.

Включение протокола 1.0

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

3. Нажмите **Save** («Сохранить»).

Настройка временных интервалов

Установите макс. продолжительность вызова.

Нажмите  → **Intercom** → **Call Settings** («Домофония → Настройки звонка»).

Установите максимальное время связи. Нажмите **Save** («Сохранить»).

Примечание

Макс. продолжительность вызова составляет от 90 до 120 с.

Нажатие кнопки для вызова

Шаги

1. Нажмите  → **Intercom** → **Press Button to Call** («Домофония → Нажатие кнопки для вызова»)

2. Нажмите **Call** («Вызов») или **Call Center** («Вызов центра»).

Настройка привязки номеров

Вызовите SIP-кабинет для вызова кабинета.

Шаги

1. Нажмите  → **Intercom** → **Number Settings** («Домофония → Настройки номера»).

2. Нажмите +, введите **Room No.** («Номер помещения») и **SIP Number** («Номер SIP»).

3. Нажмите **Save** («Сохранить»).

8.4.10 Настройки параметров аудио

Шаги

1. Нажмите  → **Audio** («Аудио»).
2. Опционально. Настройте громкость ввода и вывода.

8.4.11 Настройки параметров лица

Настройка параметров лица.

Настройки параметров лица

Нажмите  → **Smart** → **Face Recognition Parameters** («Интеллектуальные функции → Параметры распознавания лиц»).

Детекция подлинности биометрических данных лица (антиспуфинг)

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

Уровень безопасности «Детекция лиц в режиме реального времени»

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

Пороговое значение для сопоставления 1: 1

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

Пороговое значение для сопоставления 1:N

Настройте пороговое значение совпадения при аутентификации в режиме сопоставления 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Максимальное значение 100.

Лимит времени при распознавании лица

Настройте период таймаута для распознавания лиц. Если время распознавания лица превышает заданное значение, устройство выдаст уведомление о таймауте распознавания лица.

Параметры отпечатков пальцев

Нажмите  → **Smart** → **Fingerprint Parameters** («Интеллектуальные функции → Параметры отпечатков пальцев»).

Уровень безопасности отпечатков пальцев

Можно настроить уровень безопасности отпечатков пальцев. Чем выше настроенный уровень безопасности, тем ниже вероятность ошибочного предоставления доступа (FAR). Чем выше настроенный уровень безопасности, тем ниже вероятность ошибочного отказа в доступе (FRR).

Параметры детекции наличия / отсутствия маски

Детекция наличия / отсутствия маски

После включения детекции наличия / отсутствия маски система распознает лицо и наличие / отсутствие маски. Можно настроить лицо с пороговым значением для сопоставления 1:N, его ЭКО-режимом и сценарием.

Нет

Если у сотрудника / посетителя отсутствует маска при аутентификации, устройство выдаст предупреждение.

Напоминание о необходимости ношения

Если у сотрудника / посетителя отсутствует маска при аутентификации, устройство выдаст предупреждение, затем дверь откроется.

Предупреждение об обязательном ношении

Если у сотрудника / посетителя отсутствует маска при аутентификации, устройство выдаст предупреждение, дверь будет оставаться закрытой.

Лицо с маской (1:1)

Настройте значение сходства при детекции наличия / отсутствия маски в режиме сопоставления 1:1. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений.

Пороговое значение сходства при детекции наличия / отсутствия маски в режиме сопоставления 1:N

Настройте пороговое значение совпадения при детекции наличия / отсутствия маски в режиме сопоставления 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений.

Примечание

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

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

8.4.12 Настройка параметров конфиденциальности

Настройка параметров отображения, загрузки и хранения изображений.

Нажмите  → **Configuration** → **Security** → **Privacy Settings** («Настройка → Безопасность → Настройка параметров конфиденциальности»).

Настройки параметров аутентификации

Отображение изображения / отображение имени / идентификатора сотрудника

Можно настроить отображение изображения / отображение имени / идентификатора сотрудника. После выполнения аутентификации система отобразит выбранное содержимое.

Деидентификация имени / ID

Информация об имени / идентификаторе скрыта звездочками.

Обновление и хранение изображений

Можно загрузить и хранить изображения.

Сохранение зарегистрированного изображения

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

Сохранение изображения при аутентификации

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

Загрузка захваченного изображения при аутентификации

Загрузите полученные при аутентификации изображения на платформу автоматически.

Сохранение изображения после захвата

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

Загрузка изображения после захвата

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

8.4.13 Режим пароля

Перед настройкой паролей необходимо уточнить, через что настроен PIN-код: через устройство или через платформу. Если PIN-код настроен через устройство, его можно создать или изменить через устройство или веб-интерфейс, его нельзя настроить через другие платформы. Если PIN-код настроен через платформу, его можно создать или изменить через платформу, его нельзя настроить через устройство или веб-интерфейс.

Шаги

1. Нажмите  → **Security** → **PIN Mode** («Безопасность → Режим PIN-кода»)

Персональный PIN-код, настраиваемый через устройство

PIN-код можно создать или изменить через устройство или веб-интерфейс, его нельзя настроить через другие платформы.

Персональный PIN-код, настраиваемый через платформу

PIN-код можно создать или изменить через платформу, его нельзя настроить через устройство или веб-интерфейс.

2. Нажмите **Save** («Сохранить»).

8.4.14 Обновление и техническое обслуживание

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

Перезагрузка устройства

Нажмите  → **Restart Device** («Перезагрузить устройство»).

Нажмите **Restart** («Перезагрузить»), чтобы перезагрузить устройство.

Обновление

Нажмите  → **Upgrade** («Обновление»).

Нажмите **Upgrade** («Обновить»), чтобы обновить устройство.

Примечание

Не выключайте устройство во время обновления.

Восстановление параметров

Нажмите  → **Default** («По умолчанию»).

Восстановление настроек по умолчанию

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

Восстановление настроек изготовителя

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

8.4.15 Просмотр документации онлайн

Нажмите  → **View Online Document** («Просмотр документации онлайн»).

Нажмите **View Online Document** («Просмотр документации онлайн»), можно сканировать QR-код с помощью мобильного телефона для получения подробной информации.

8.4.16 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.

Раздел 9 Быстрые операции через веб-интерфейс

9.1 Изменение пароля

Можно изменить пароль устройства.

Нажмите  в верхнем правом углу веб-страницы для перехода на страницу **Change Password** («Изменить пароль»). Можно настроить контрольные вопросы из выпадающего списка и заполнить ответы.

Нажмите **Next** («Далее»), чтобы завершить настройку. Или нажмите **Skip** («Пропустить»), чтобы пропустить этот шаг.

9.2 Выбор языка

Можно выбрать язык системы устройства.

Нажмите  в верхнем правом углу веб-страницы для перехода на страницу **Device Language Settings** («Настройка языка устройства»). Можно выбрать язык для системы устройства из выпадающего списка.

По умолчанию языком системы выбран английский.

Примечание

После изменения языка системы устройство автоматически перезагрузится.

9.3 Настройка времени

Нажмите  в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек. После настройки языка устройства нажмите **Next** («Далее»), чтобы перейти на страницу настройки времени.

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

NTP

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

Вручную

По умолчанию время устройства должно быть синхронизировано вручную.

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

Адрес сервера / Порт NTP / Интервал

Можно настроить адрес сервера, порт NTP, интервал.

Переход на летнее время (DST)

Установите время начала и окончания перехода на летнее время (DST), а также смещение.

Нажмите **Next** («Далее»), чтобы сохранить настройки и перейти к следующему параметру. Или нажмите **Skip** («Пропустить»), чтобы пропустить настройки.

9.4 Настройки параметров конфиденциальности

Настройте параметры загрузки и хранения изображений.

Нажмите  в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек.

Загрузка и хранение изображений

Сохранение изображения при аутентификации

Автоматическое сохранение изображений при аутентификации.

Загрузка изображения при аутентификации

Загрузка изображений при автоматической аутентификации на платформу.

Сохранение зарегистрированного изображения

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

Загрузка изображения после захвата

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

Сохранение изображения после захвата

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

Нажмите **Next** («Далее»), чтобы сохранить настройки и перейти к следующему параметру. Или нажмите **Skip** («Пропустить»), чтобы пропустить настройки конфиденциальности.

9.5 Настройки администратора

Шаги

1. Нажмите  в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек.
2. Введите идентификатор сотрудника и имя администратора.
3. Выберите учетные данные для добавления.

Примечание

Необходимо выбрать хотя бы один сертификат.

- 1) Нажмите **Add Face** («Добавить лицо») для загрузки изображения лица из локального хранилища.

Примечание

Размер загружаемого изображения не должен превышать 200 КБ, поддерживаемые форматы: JPG, JPEG, PNG.

- 2) Нажмите **Add Card** («Добавить карту»), чтобы ввести номер карты и выбрать свойства карты.

Примечание

Поддерживается до 50 карт.

3) Нажмите **Add Fingerprint** («Добавить отпечаток пальца»), чтобы добавить отпечатки пальцев.

Примечание

Разрешено до 10 отпечатков пальцев.

9.6 Настройка номеров и сетевые настройки

Шаги

1. Нажмите  в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек. После предыдущих настроек можно нажать **Next** («Далее»), чтобы перейти на страницу настроек сети и сетевой системы.

2. Выберите тип устройства.

Примечание

- Если в качестве типа устройства выбрано **Door Station** («Вызывная панель»), можно настроить номер микрорайона, номер здания, номер корпуса, номер этажа и номер вызывной панели.
- Если в качестве типа устройства выбрано **Outer Door Station** («Уличная вызывная панель»), можно настроить номер вызывной панели и номер микрорайона.

Тип устройства

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

Номер микрорайона

Укажите номер микрорайона.

Номер здания

Укажите номер здания.

Номер помещения

Укажите номер помещения.

Номер этажа

Укажите номер этажа, на котором установлено устройство.

Номер вызывной панели

Укажите номер установленной вызывной панели.

Примечание

Номер вызывной панели: 0, номер дополнительной вызывной панели: от 1 до 16.

Номер вызывной панели, установленной снаружи помещения

Укажите номер установленной уличной вызывной панели.

Примечание

Номер в диапазоне от 1 до 99.

3. Настройте параметры сети видеодомофона.

Пароль регистрации

Установите регистрационный пароль пульта консьержа / диспетчера для связи.

Установите регистрационный пароль пульта консьержа / диспетчера для связи.

IP-адрес пульта консьержа / диспетчера

Введите IP-адрес пульта консьержа / диспетчера, используемый для связи.

IP-адрес частного сервера

Относится к IP-адресу SIP-сервера. Введите IP-адрес пульта консьержа / диспетчера, используемый для связи. В настоящее время пульт консьержа / диспетчера используется в качестве SIP-сервера. Для осуществления связи по

этому адресу сервера должны быть зарегистрированы другие устройства домофонии.

Включение протокола 1.0

Если эта функция включена, вызывную панель можно зарегистрировать на пульте консьержа / диспетчера с использованием старой версии протокола. Если эта функция отключена, вызывная панель может быть зарегистрирована на пульте консьержа / диспетчера с помощью новой версии протокола.

4. Нажмите **Complete** («Завершить»), чтобы сохранить настройки после завершения конфигурации.

Глава 10 Работа через веб-интерфейс

10.1 Вход в систему

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

Примечание

Устройство должно быть активировано.

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 программного обеспечения

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

10.2 Забыть пароль

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

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

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

Проверка по контрольным вопросам

Ответьте на контрольные вопросы.

Подтверждение по электронной почте

1. Экспортируйте QR-код и отправьте его по адресу в качестве вложения.
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.

10.3 Справка

10.3.1 Лицензия на ПО с открытым исходным кодом

Просмотр лицензии на ПО с открытым исходным кодом.

Нажмите  → **Open Source Software Statement** («Лицензия на ПО с открытым исходным кодом») в правом верхнем углу, чтобы просмотреть лицензию.

10.3.2 Просмотр онлайн справки

Можно просмотреть справку по настройке через веб-интерфейс.

Нажмите  → **Online Document** («Онлайн документ») в правом верхнем углу веб-страницы.

10.4 Выход из системы

Выйдите из учетной записи.

Нажмите **admin** → **Logout** → **OK** («Администратор → Выход из системы → OK»).

10.5 Быстрые операции через веб-интерфейс

10.5.1 Изменение пароля

Можно изменить пароль устройства.

Нажмите  в верхнем правом углу веб-страницы для перехода на страницу **Change Password** («Изменить пароль»). Можно настроить контрольные вопросы из выпадающего списка и заполнить ответы.

Нажмите **Next** («Далее»), чтобы завершить настройку. Или нажмите **Skip** («Пропустить»), чтобы пропустить этот шаг.

10.5.2 Выбор языка

Можно выбрать язык системы устройства.

Нажмите  в верхнем правом углу веб-страницы для перехода на страницу **Device Language Settings** («Настройка языка устройства»). Можно выбрать язык для системы устройства из выпадающего списка.

По умолчанию языком системы выбран английский.

Примечание

После изменения языка системы устройство автоматически перезагрузится.

10.5.3 Настройки времени

Нажмите  в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек. После настройки языка устройства нажмите **Next** («Далее»), чтобы перейти на страницу настройки времени.

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

NTP

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

Вручную

По умолчанию время устройства должно быть синхронизировано вручную.

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

Адрес сервера / Порт NTP / Интервал

Можно настроить адрес сервера, порт NTP, интервал.

Переход на летнее время (DST)

Установите время начала и окончания перехода на летнее время (DST), а также смещение.

Нажмите **Next** («Далее»), чтобы сохранить настройки и перейти к следующему параметру. Или нажмите **Skip** («Пропустить»), чтобы пропустить настройки.

10.5.4 Настройки конфиденциальности

Настройте параметры загрузки и хранения изображений.

Нажмите  в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек.

Загрузка и хранение изображений

Сохранение изображения при аутентификации

Автоматическое сохранение изображений при аутентификации.

Загрузка изображения при аутентификации

Загрузка изображений при автоматической аутентификации на платформу.

Сохранение зарегистрированного изображения

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

Загрузка изображения после захвата

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

Сохранение изображения после захвата

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

Нажмите **Next** («Далее»), чтобы сохранить настройки и перейти к следующему параметру. Или нажмите **Skip** («Пропустить»), чтобы пропустить настройки конфиденциальности.

10.5.5 Настройки учетной записи администратора

Шаги

1. Нажмите  в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек.
2. Введите идентификатор сотрудника и имя администратора.
3. Выберите учетные данные для добавления.

Примечание

Необходимо выбрать хотя бы один сертификат.

- 1) Нажмите **Add Face** («Добавить лицо») для загрузки изображения лица из локального хранилища.

Примечание

Размер загружаемого изображения не должен превышать 200 КБ, поддерживаемые форматы: JPG, JPEG, PNG.

- 2) Нажмите **Add Card** («Добавить карту»), чтобы ввести номер карты и выбрать свойства карты.

Примечание

Поддерживается до 50 карт.

3) Нажмите **Add Fingerprint** («Добавить отпечаток пальца»), чтобы добавить отпечатки пальцев.

Примечание

Разрешено до 10 отпечатков пальцев.

10.5.6 Настройка номеров и сетевые настройки

Шаги

1. Нажмите  в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек. После предыдущих настроек можно нажать **Next** («Далее»), чтобы перейти на страницу настроек сети и сетевой системы.
2. Выберите тип устройства.

Примечание

- Если в качестве типа устройства выбрано **Door Station** («Вызывная панель»), можно настроить номер микрорайона, номер здания, номер корпуса, номер этажа и номер вызывной панели.
- Если в качестве типа устройства выбрано **Outer Door Station** («Уличная вызывная панель»), можно настроить номер вызывной панели и номер микрорайона.

Тип устройства

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

Номер микрорайона

Укажите номер микрорайона.

Номер здания

Укажите номер здания.

Номер помещения

Укажите номер помещения.

Номер этажа

Укажите номер этажа, на котором установлено устройство.

Номер вызывной панели

Укажите номер установленной вызывной панели.

 Примечание

Номер вызывной панели: 0, номер дополнительной вызывной панели: от 1 до 16.

Номер вызывной панели, установленной снаружи помещения

Укажите номер установленной уличной вызывной панели.

 Примечание

Номер в диапазоне от 1 до 99.

3. Настройте параметры сети видеодомофона.

Пароль регистрации

Установите регистрационный пароль пульта консьержа / диспетчера для связи.
Установите регистрационный пароль пульта консьержа / диспетчера для связи.

IP-адрес пульта консьержа / диспетчера

Введите IP-адрес пульта консьержа / диспетчера, используемый для связи.

IP-адрес частного сервера

Относится к IP-адресу SIP-сервера. Введите IP-адрес пульта консьержа / диспетчера, используемый для связи. В настоящее время пульт консьержа / диспетчера используется в качестве SIP-сервера. Для осуществления связи по этому адресу сервера должны быть зарегистрированы другие устройства домофонии.

Включение протокола 1.0

Если эта функция включена, вызывную панель можно зарегистрировать на пульте консьержа / диспетчера с использованием старой версии протокола. Если эта функция отключена, вызывная панель может быть зарегистрирована на пульте консьержа / диспетчера с помощью новой версии протокола.

4. Нажмите **Complete** («Завершить»), чтобы сохранить настройки после завершения конфигурации.

10.6 Управление сотрудниками / посетителями

Нажмите **Add** («Добавить»), чтобы добавить информацию о пользователе, включая основную информацию, сертификат и настройки аутентификации.

Добавление основной информации

Нажмите **Person Management** → **Add** («Управление пользователями → 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 количество посещений.

Если выбран параметр **Custom Type** («Настраиваемый тип»), можно изменить имя. Измененное имя будет применено к устройству.

Выберите **Person Role** («Роль для сотрудника / посетителя»).

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

Настройка длительности разрешения

Нажмите **Person Management** → **Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Включите или настройте **Long-Term Effective User** («Пользователь с длительным разрешением»), и пользователь сможет получить разрешение только в течение настроенного периода времени.

Можно включить **Attendance Check Only** («Только проверка УРВ»). После выбора параметра данный пользователь не получит права на управление доступом.

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

Назначение номера устройства

Нажмите **Person Management** → **Add Person** → **Add** («Управление сотрудниками / посетителями → Добавить сотрудника / посетителя → Добавить»), чтобы перейти на соответствующую страницу.

Нажмите на **Floor No.** («Номер этажа») и **Room No.** («Номер помещения») и введите число от 1 до 999, чтобы установить номер этажа и номер помещения.

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

Настройки параметров аутентификации

Нажмите **Person Management** → **Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Выберите тип аутентификации.

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

Добавление карты

Нажмите **Person Management** → **Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

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

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

Добавление изображения лица

Нажмите **Person Management** → **Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Нажмите + **Upload** («Загрузить»), чтобы загрузить изображение лица с локального ПК.

Примечание

Размер загружаемого изображения не должен превышать 200 КБ, поддерживаемые форматы: JPG, JPEG, PNG.

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

Добавление отпечатка пальца

Примечание

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

Нажмите **Person Management** → **Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Нажмите **Add Fingerprint** («Добавить отпечатки пальцев») и приложите палец к модулю отпечатков пальцев, чтобы добавить отпечаток пальца.

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

Добавление PIN-кода

Перед настройкой PIN-кода необходимо уточнить, через что настроен PIN-код: через устройство или через платформу. Если PIN-код настроен через устройство, его можно создать или изменить через устройство или веб-интерфейс, его нельзя настроить через другие платформы. Если PIN-код настроен через платформу, его можно создать или изменить через платформу, его нельзя настроить через устройство или веб-интерфейс.

Убедитесь, что для режима PIN-кода выбран параметр **Device-Set Personal PIN** («Персональный PIN-код, настраиваемый через устройство»). Нажмите **PIN Mode** («Режим PIN-кода») на странице, чтобы перейти к настройке.

Нажмите **Person Management** → **Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Установите PIN-код. Или нажмите **Auto Generate** («Автоматическая генерация»), чтобы автоматически сгенерировать PIN-код.

Нажмите **Add** («Добавить») для сохранения настроек.

Нажмите **Save and Continue** («Сохранить и продолжить»), чтобы сохранить настройки и продолжить добавление следующего пользователя.

Настройки номера устройства

Нажмите **Person Management** → **Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.

Добавьте основную информацию о пользователе. Перейдите в модуль номера устройства. Нажмите **Add** («Добавить») и введите номер помещения и этаж. Нажмите **Add** («Добавить») или **Save and Continue** («Сохранить и продолжить»).

Удаление сотрудника / посетителя

На странице управления пользователями отметьте пользователя, которого нужно удалить, и нажмите **Delete** («Удалить»).

Нажмите **Clear All** («Очистить все»), чтобы удалить всех пользователей.

Редактирование информации о сотруднике / посетителе

На странице управления пользователями отметьте пользователя, о котором нужно отредактировать информацию. Нажмите , чтобы отредактировать информацию о пользователе.

Фильтр

На странице управления пользователями введите **Employee ID** («Идентификатор сотрудника») / **Name** («Имя») / **Card No.** («Номер карты»). Выберите **Credential Status** («Состояние учетных данных») и нажмите **Filter** («Фильтровать»), чтобы найти нужного пользователя. Нажмите **Reset** («Сбросить»), чтобы очистить все условия поиска.

10.7 Обзор

Можно просматривать видео с устройства в режиме реального времени, видео с подключенного устройства, информацию о человеке, состояние сети, основную информацию и емкость устройства.

Нажмите .

Описание функций:

Состояние двери

Нажмите  на видео, чтобы просмотреть видео с устройства в режиме реального времени.



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.



Состояние двери: открыта / закрыта / оставить открытой / оставить закрытой.



Можно начать запись при запуске просмотра в режиме реального времени.



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



Полноэкранный просмотр.

Контроль состояния

Можно управлять состоянием двери: открыть, закрыть, оставить дверь открытой или оставить дверь закрытой.

События в режиме реального времени

Можно просмотреть идентификатор сотрудника, имя, номер карты, тип события, время и операции. Также можно нажать **View More** («Дополнительно»), чтобы перейти на страницу поиска событий. Выберите типы событий, введите идентификатор сотрудника, имя, номер карты, время начала и время окончания, а затем нажмите **Search** («Поиск»). После этого на панели справа появятся результаты поиска.

Привязка устройства

Можно просмотреть количество и статус привязанных устройств.

Примечание

Для перехода нажмите **View More** («Дополнительно»).

Информация о пользователе

Можно просмотреть добавленную и недобавленную информацию об учетных данных пользователя.

Состояние сети

Можно просмотреть состояние подключения и регистрации проводной сети, беспроводной сети, Hik-Connect, ISUP, OTAP и VoIP.

Основная информация

Можно просмотреть модель, серийный номер и версию прошивки.

Емкость устройства

Можно просмотреть емкость хранения записей пользователей, лиц, карт, отпечатков пальцев и событий.

Примечание

Только устройства с поддержкой модуля считывания отпечатков пальцев могут отображать записи отпечатков пальцев.

10.8 Приложения контроля доступа

10.8.1 Настройки запрета двойного прохода.

Функция запрета двойного прохода между устройствами требует от сотрудников последовательной аутентификации в соответствии с настроенным маршрутом. Эта функция поддерживается только дополнительным

устройством, и поддерживается только односторонний проход с аутентификацией.

Шаги

1. Нажмите **Access Control** → **Access Control Application** → **Cross-Device Anti-Passback** («Контроль доступа → Приложения контроля доступа → Запрет двойного прохода на разных устройствах»).
2. Включите функцию.
3. Установите параметры контроллера доступа, включая **Main Device IP Address** («IP-адрес основного устройства»), **Main Device Port No.** («Номер порта основного устройства») и **Main Device Password** («Пароль основного устройства»).
4. Установите регистрационный код устройства, чтобы просмотреть **Registration Status** («Статус регистрации»).
5. Выберите **Card Reader** («Считыватель карт»). Невыбранный считыватель карт не может быть подключен для запрета двойного прохода.

10.8.2 Настройка блокировки нескольких дверей

Можно установить блокировку нескольких дверей для нескольких дверей одного контроллера доступа. Чтобы открыть одну из дверей, другие двери должны оставаться закрытыми.

Шаги

1. Нажмите **Access Control** → **Access Control Application** → **Cross-Device Multi-Door Interlocking** («Контроль доступа → Приложения контроля доступа → Блокировка нескольких дверей на разных устройствах»).
2. Включите функцию.
3. Выберите **Device Type** («Тип устройства»).

Если устройство установлено как основное, необходимо указать **Port No.** («№ порта») и нажать **Add** («Добавить»), чтобы добавить точку доступа. Нажмите **Sub Device Management** («Управление дополнительным устройством»), чтобы просмотреть состояние устройства и удалить его. Если устройство установлено

как дополнительное, необходимо установить параметры контроллера доступа, включая **Main Device IP Address** («IP-адрес основного устройства»), **Main Device Port No.** («Номер порта основного устройства») и **Main Device Password** («Пароль основного устройства»). Установите регистрационный код устройства, чтобы просмотреть **Registration Status** («Статус регистрации»). Выберите **Card Reader** («Считыватель карт»). Невыбранный считыватель карт не может быть подключен для запрета двойного прохода.

4. Настройте **Anti-Passback Rule** («Правило запрета двойного прохода»).

По состоянию аутентификации

Процесс запрета двойного прохода определяется аутентификацией по карте.

По фактическому состоянию потока

Процесс запрета двойного прохода определяется фактическим открытием с помощью карты.

5. Нажмите **ОК**.

10.9 Управление контролем доступа

10.9.1 Поиск событий

Нажмите **Event Search** («Поиск события») 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»).

После этого на панели справа появятся результаты поиска.

10.9.2 Конфигурация параметров двери

Настройте параметры разблокировки дверей.

Выбор номера двери

Выберите дверь для настройки соответствующих параметров.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Выберите **Door No.** («Номер двери»). Обычно дверь 1 – это дверь, привязанная к устройству, а дверь 2 – это дверь, привязанная к модулю безопасности.

Установите другие параметры двери и нажмите **Save** («Сохранить»).

Просмотр состояния устройства в режиме онлайн

Просмотрите и обновите состояние устройства.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Можно просмотреть состояние устройства в режиме онлайн. Нажмите **Refresh** («Обновить»), чтобы обновить состояние устройства.

Установка названия двери

Введите название двери.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Установите **Door Name** («Название двери») и нажмите **Save** («Сохранить»).

Настройка длительности открытого состояния через веб-интерфейс ПК

Можно установить время открытия дверного замка после считывания карты.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Установите продолжительность открытия, то есть время действия после разблокировки двери. Если дверь не будет открыта в течение установленного времени, она автоматически заблокируется. Настройка времени: от 1 до 255 секунд.

Нажмите **Save** («Сохранить»).

Настройка тревоги тайм-аута открытой двери через веб-интерфейс ПК

Если дверь не закрыта по истечении времени срабатывания блокировки, точка контроля доступа подаст звуковой сигнал тревоги.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Настройте **Door Open Timeout Alarm** («Тревога тайм-аута открытой двери»). Если дверь не закрыта по истечении времени срабатывания блокировки, точка контроля доступа подаст звуковой сигнал тревоги. Если установлено значение 0, тревога не будет включена.

Нажмите **Save** («Сохранить»).

Настройка блокировки двери при закрытии

Можно установить блокировку двери при закрытии.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Можно включить **Lock Door when Door Closed** («Блокировка двери при закрытии»).

Нажмите **Save** («Сохранить»).

Настройка типа магнитоконтактного датчика двери через веб-интерфейс ПК

Можно выбрать тип дверного контакта в соответствии со способом подключения.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Выберите тип магнитоконтактного датчика: оставить закрытым или оставить открытым. По умолчанию – **Remain Closed** («Оставить закрытым») (за исключением особых случаев).

Нажмите **Save** («Сохранить»).

Настройка кнопки выхода через веб-интерфейс ПК

Можно установить необходимый параметр кнопки выхода: **Remain Open** («Оставить открытым») или **Remain Closed** («Оставить закрытым»).

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Настройте **Exit Button Type** («Тип кнопки выхода»). По умолчанию – **Remain Open** («Оставить открытой») (за исключением особых случаев).

Нажмите **Save** («Сохранить»).

Настройка закрытия двери при отключении питания через веб-интерфейс ПК

Можно установить состояние дверного замка при отключении питания.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Настройте **Door Lock Powering Off Status** («Состояние закрытия двери при отключении питания»). По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).

Нажмите **Save** («Сохранить»).

Настройка увеличенной длительности открытого состояния через веб-интерфейс ПК

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

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Настройте **Extended Open Duration** («Увеличенная длительность открытого состояния»). Дверной контакт может быть активирован с установленной задержкой после считывания карты пользователя с расширенным доступом.

Нажмите **Save** («Сохранить»).

Настройка открытого состояния двери после авторизации первого сотрудника через веб-интерфейс ПК

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

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Установите продолжительность открытия двери при входе первого сотрудника и нажмите **Save** («Сохранить»).

Настройка кода принуждения через веб-интерфейс ПК

После настройки кода принуждения, при возникновении угрозы, введите код для открытия двери. Одновременно система контроля доступа будет сообщать о событиях принуждения.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

Установите код принуждения и нажмите **Save** («Сохранить»).

 **Примечание**

Код принуждения и суперпароль не могут быть скопированы, обычно состоят из 4-8 цифр.

Установка суперпароля через веб-интерфейс ПК

Администратор или назначенный сотрудник может ввести суперпароль для открытия двери.

Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

После установки **Super Password** («Суперпароль») назначенный сотрудник сможет ввести суперпароль для открытия двери.

Нажмите **Save** («Сохранить»).

Примечание

Код принуждения и суперпароль не могут быть скопированы, обычно состоят из 4-8 цифр.

10.9.3 Настройка параметров аутентификации

Выбор основного или дополнительного считывателя карт через веб-интерфейс ПК

Настройте терминал для аутентификации пользователя.

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

Выберите терминал в качестве основного или дополнительного считывателя карт.

Установите другие параметры и нажмите **Save** («Сохранить»).

Просмотр типа и модели терминала через веб-интерфейс ПК

Можно просмотреть тип и модель терминала.

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

Просмотрите **Terminal Type** («Тип терминала») и **Terminal Model** («Модель терминала»).

Включение устройства аутентификации через веб-интерфейс ПК

После включения терминал аутентификации можно использовать для считывания карт.

Шаги

1. Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
2. Включите **Authentication Device** («Устройство аутентификации»). После включения терминал можно использовать для считывания карт в обычном режиме.
3. Нажмите **Save** («Сохранить»).

Настройка аутентификации через веб-интерфейс ПК

Конфигурация аутентификации.

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

При установке основного считывателя карт в качестве терминала можно выбрать **Authentication** («Аутентификация») из выпадающего списка. При наличии нескольких типов аутентификаций следует установить параметры **Single Credential Authenticating Timeout** («Тайм-аут аутентификации с помощью одного типа учетных данных») и **Control Initial Authentication Type** («Управление типом первичной аутентификации»).

Тайм-аут аутентификации с помощью одного типа учетных данных

Можно настроить продолжительность каждого типа аутентификации.

Примечание

Время ожидания аутентификации по паролю по умолчанию составляет 20 секунд, и оно не ограничено указанными выше настройками.

Управление типом первичной аутентификации

Если параметр включен, все выбранные типы могут использоваться для первичной аутентификации.

При установке дополнительного считывателя карт в качестве терминала можно выбрать **Authentication** («Аутентификация») из выпадающего списка.

Нажмите **Save** («Сохранить»).

Запуск аутентификации по лицу вручную через веб-интерфейс ПК

После включения функции **Manually Trigger Authentication via Face** («Запуск аутентификации по лицу вручную») необходимо вручную коснуться экрана устройства для распознавания лица.

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

Если в качестве терминала выбран основной считыватель карт, нажмите, чтобы включить функцию **Manually Trigger Authentication via Face** («Запуск аутентификации по лицу вручную»), и выберите режим аутентификации.

Распознавание одного человека

После завершения предыдущего распознавания лица, независимо от того, было ли оно успешным или нет, необходимо коснуться экрана, чтобы запустить следующее распознавание.

Непрерывное распознавание

После активации распознавание будет выполняться до тех пор, пока устройство не перейдет в спящий режим.

Нажмите **Save** («Сохранить»).

Установка интервала распознавания через веб-интерфейс ПК

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

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

При выборе терминала в качестве основного или дополнительного считывателя карт установите интервал распознавания и нажмите **Save** («Сохранить»).

Примечание

Введите число от 1 до 10.

Установка интервала аутентификации через веб-интерфейс ПК

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. Если другой пользователь пройдет аутентификацию в течение заданного интервала, он сможет пройти аутентификацию повторно.

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

При выборе терминала в качестве основного считывателя карт установите **Authentication Interval** («Интервал аутентификации») и нажмите **Save** («Сохранить»).

Включение тревоги макс. количества неудачных попыток через веб-интерфейс ПК

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

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

При выборе терминала в качестве основного или дополнительного считывателя карт, переместите ползунок, чтобы включить **Alarm of Max. Failed Attempts** («Тревога макс. количества неудачных попыток»), и установите **Max. Authentication Failed Attempts** («Макс. количество неудачных попыток аутентификации»).

Нажмите **Save** («Сохранить»).

Вкл. / выкл. тревоги тампера через веб-интерфейс ПК

Если включить тревогу тампера, устройство будет автоматически генерировать события тревоги тампера при извлечении считывателя карт.

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

Можно включить или отключить тревогу тампера по мере необходимости. После включения функции устройство будет автоматически генерировать события тревоги тампера при извлечении считывателя карт. Если функция отключена, события генерироваться не будут.

Нажмите **Save** («Сохранить»).

Вкл. / выкл. считывания номера карты в обратной последовательности через веб-интерфейс ПК

Можно включить или отключить функцию считывания номера карты в обратной последовательности.

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

При включении функции **Card No. Reversing** («Считывание номера карты в обратной последовательности») считанный номер карты будет отображаться в обратном порядке.

Нажмите **Save** («Сохранить»).

Настройка положения дополнительного считывателя карт

Можно выбрать положение дополнительного считывателя карт.

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

Если в качестве терминала выбран дополнительный считыватель карт, можно выбрать его положение как **Different Side from Main Card Reader** («С другой

стороны от основного считывателя карт») или **Same Side as Main Card Reader** («На той же стороне, что и основной считыватель карт»). Нажмите **Save** («Сохранить»).

Настройка связи с панелью управления через веб-интерфейс ПК

Можно настроить связь с панелью управления для дополнительного считывателя карт. Если считыватель карт не может подключиться к контроллеру доступа в течение заданного времени, считыватель перейдет в режим офлайн.

Нажмите **Access Control → Parameter Settings → Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

При выборе терминала в качестве дополнительного считывателя карт установите параметр **Communication with Controller Every** («Связь с панелью управления») и нажмите **Save** («Сохранить»).

Установка времени ожидания ввода пароля через веб-клиент

Установите максимальный интервал ввода двух символов пароля. Если после ввода одного символа следующий символ не будет введен в течение установленного интервала, все введенные символы будут автоматически удалены.

Нажмите **Access Control → Parameter Settings → Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

При выборе дополнительного считывателя карт в качестве терминала установите **Max. Interval When Entering Password** («Максимальный интервал времени при вводе пароля») и нажмите **Save** («Сохранить»).

Настройка полярности светодиодов ОК и Error через веб-интерфейс ПК

Выберите полярность светодиодов для интерфейсов ОК и ERR в соответствии с подключением, по умолчанию – положительная полярность.

Нажмите **Access Control → Parameter Settings → Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

При выборе терминала в качестве дополнительного считывателя карт установите полярность светодиодов ОК и Error и нажмите **Save** («Сохранить»).

10.9.4 Настройка привязки аутентификации

Можно настроить параметры привязки аутентификации.

Шаги

1. Нажмите **Access Control → Parameter Settings → Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
2. Настройте функции привязки.

Привязка вызова при аутентификации

В случае активации этой функции и успешной авторизации человека, система автоматически выполнит вызов целевого абонента из настроек кнопки для удаленного открытия двери.

Привязка вызова при ошибке аутентификации

Если количество неудачных попыток аутентификации достигнет установленного значения после включения функции, система автоматически выполнит вызов целевого абонента из настроек кнопки для удаленного открытия двери.

3. Нажмите **Save** («Сохранить»).

10.9.5 Настройка плана аутентификации

Можно настроить план аутентификации.

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

Выберите тип аутентификации и перетащите временной период на шкале времени.

Нажмите **Save** («Сохранить»).

10.9.6 Настройка параметров распознавания лиц

Вкл. / выкл. детекции подлинности биометрических данных лица (антиспуфинг) через веб-интерфейс

При включении этой функции устройство сможет отличать сотрудника / посетителя от изображения.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Включите **Face Anti-spoofing** («Детекция подлинности биометрических данных лица (антиспуфинг)») и нажмите **Save** («Сохранить»).

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

Вкл. / выкл. проверки повторяющихся изображений лиц

После включения проверки повторяющихся изображений лиц и при каждом добавлении лица человека система будет проверять наличие дубликатов. Если будет обнаружено повторяющееся изображение лица, появится соответствующее уведомление.

Примечание

Эта функция не поддерживается при удаленном добавлении изображений лиц или добавлении изображений лиц в пакетном режиме.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Включите **Face Duplicate Check** («Проверка повторяющихся изображений лиц»).

Нажмите **Save** («Сохранить»).

Настройка уровня детекции подлинности биометрических данных (антиспуфинг) через веб-интерфейс ПК

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

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Выберите уровень детекции подлинности биометрических данных и нажмите **Save** («Сохранить»).

Можно выбрать общий, расширенный и профессиональный уровни. Чем выше уровень, тем ниже вероятность ложного распознавания и выше вероятность отказа.

Установка дальности распознавания через веб-интерфейс ПК

Можно установить расстояние между пользователем и камерой устройства при аутентификации.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Настройте дальность распознавания и нажмите **Save** («Сохранить»).

Настройка угла наклона через веб-интерфейс ПК

Можно настроить угол наклона объектива во время распознавания лица и аутентификации.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Примечание

Разные модели могут поддерживать разные параметры. Подробная информация представлена на соответствующей странице.

Настройте **Pitch Angle** («Угол наклона») и нажмите **Save** («Сохранить»).

Настройка угла поворота через веб-интерфейс ПК

Можно настроить угол поворота объектива во время распознавания лица и аутентификации.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Примечание

Разные модели могут поддерживать разные параметры. Подробная информация представлена на соответствующей странице.

Настройте угол поворота и нажмите **Save** («Сохранить»).

Установка уровня качества изображения лица для аутентификации через веб-интерфейс ПК

Уровень качества изображения лица должен быть выше порогового значения для успешной аутентификации.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Примечание

Разные модели могут поддерживать разные параметры. Подробная информация представлена на соответствующей странице.

Установите **Face Picture Quality Grade for Applying** («Уровень качества изображения лица для аутентификации»). Значение для данного параметра должно быть выше порогового значения для успешной аутентификации.

Нажмите **Save** («Сохранить»).

Установка порогового значения качества изображения лица 1:1 через веб-интерфейс ПК

Установите пороговое значение качества изображения лица 1:1.

Перейдите **Access Control** → **Parameters Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»).

Установите **1:1 Face Picture Grade Threshold** («Пороговое значение качества изображения лица 1:1») и нажмите **Save** («Сохранить»).

Чем выше порог, тем выше требования к качеству изображений, полученных с фронтальной камеры, и тем чаще может возникать ошибка аутентификации.

Установка порогового значения соответствия лица 1:1 через веб-интерфейс ПК

Установите пороговое значение соответствия лица 1:1.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Установите пороговое значение для соответствия лица 1:1 и нажмите **Save** («Сохранить»).

Чем больше значение порога, тем ниже будет процент ложных тревог и выше процент ложных отказов при аутентификации по лицу. Максимальное значение – 100.

Настройка порогового значения соответствия лица 1:N через веб-интерфейс ПК

Можно установить пороговое значение для сопоставления лиц 1:N.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Установите пороговое значение для соответствия лица 1:N и нажмите **Save** («Сохранить»).

Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Максимальное значение 100.

Настройка области распознавания лиц через веб-интерфейс

Можно настроить область распознавания при аутентификации лиц.

Нажмите **Access Control** → **Parameter Settings** → **Area Configuration** («Контроль доступа → Настройки параметров → Конфигурация области»), чтобы перейти на страницу настроек.

Переместите желтый прямоугольник на экране предварительного просмотра, чтобы настроить эффективную область распознавания лиц слева, справа, сверху и снизу.

Или перетащите область или введите число, чтобы задать параметры.

Нажмите **Save** («Сохранить»).

Нажмите ,  или  для захвата, записи или перехода в полноэкранный режим.

Настройка параметров отпечатка пальца через веб-интерфейс ПК

Можно настроить параметры отпечатка пальца устройства.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Выберите **Fingerprint Security Level** («Уровень безопасности отпечатков пальцев»). Чем выше уровень, тем ниже вероятность ложного распознавания и выше вероятность отказа.

Нажмите **Save** («Сохранить»).

Вкл. / выкл. режима ЭКО через веб-интерфейс ПК

После включения ЭКО-режима устройство будет аутентифицировать лица в условиях низкой освещенности или в темноте с помощью ИК-подсветки камеры.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

После включения ЭКО-режима устройство будет аутентифицировать лица в условиях низкой освещенности или в темноте с помощью ИК-подсветки камеры. Можно установить ЭКО-режим (1:N) и ЭКО-режим (1:1).

Если функция детекции наличия / отсутствия маски включена, также можно установить параметры распознавания.

Пороговое значение ЭКО-режима (1:1)

Настройте пороговое значение совпадения при аутентификации в ЭКО-режиме 1:1. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Максимальное значение 100.

Пороговое значение ЭКО-режима (1:N)

Настройте пороговое значение совпадения при аутентификации в ЭКО-режиме 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Максимальное значение 100.

Пороговое значение сопоставления лица с маской в ЭКО-режиме 1:1

Настройте пороговое значение сходства при детекции наличия / отсутствия маски в ЭКО-режиме сопоставления 1:1. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Максимальное значение 100.

Пороговое значение сопоставления лица с маской в ЭКО-режиме 1:N

Настройте пороговое значение совпадения при детекции наличия / отсутствия маски 1:N (ЭКО-режим). Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Максимальное значение 100.

Нажмите **Save** («Сохранить»).

Вкл. / выкл. распознавания лица с маской через веб-интерфейс ПК

После включения детекции лица с маской система распознает наличие / отсутствие маски.

Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

После включения детекции лица с маской можно установить **Face without Mask Strategy** («Стратегия распознавания лиц без масок»), **Face with Mask&Face (1:1)** («Распознавание лиц и лиц в масках (1:1)»), **Face with Mask 1:N Match Threshold (ECO)** («Пороговое значение сопоставления лица с маской в ЭКО-режиме 1:N»), **Face with Mask 1:1 Match Threshold** («Пороговое значение сопоставления лица с маской 1:1») и **Face with Mask 1:N Match Threshold (ECO)** («Пороговое значение сопоставления лица с маской в ЭКО-режиме 1:N»).

Стратегия распознавания лиц без масок

Можно выбрать **None** («Нет»), **Reminder of Wearing Face Mask** («Напоминание о необходимости ношения маски») и **Must Wear Face Mask** («Предупреждение об обязательном ношении маски»).

Напоминание о необходимости ношения

Если сотрудник не носит маску на лице, при аутентификации на устройстве появится всплывающее окно с уведомлением, и дверь откроется.

Предупреждение об обязательном ношении

Если сотрудник не носит маску на лице, при аутентификации на устройстве появится всплывающее окно с уведомлением, и дверь останется закрытой.

Распознавание лица и лица с маской (1:1)

Настройте значение сходства при детекции наличия / отсутствия маски в режиме сопоставления 1:1. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Максимальное значение 100.

Распознавание лица и лица с маской (1:N)

Настройте пороговое значение совпадения при детекции наличия / отсутствия маски в режиме сопоставления 1:N. Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Максимальное значение 100.

Пороговое значение сопоставления лица с маской в ЭКО-режиме 1:1

Настройте значение сходства при детекции наличия / отсутствия маски в ЭКО-режиме сопоставления 1:1. Чем выше пороговое значение, тем ниже частота ошибок распознавания и тем выше процент отказов при аутентификации лиц. Максимальное значение 100.

Пороговое значение сопоставления лица с маской в ЭКО-режиме 1:N

Настройте значение сходства при детекции наличия / отсутствия маски в ЭКО-режиме сопоставления 1:N. Чем выше пороговое значение, тем ниже частота ошибок распознавания и тем выше процент отказов при аутентификации лиц. Максимальное значение 100.

Нажмите **Save** («Сохранить»).

10.9.7 Настройки параметров карты

Вкл. / выкл. защиты NFC через веб-интерфейс ПК

После включения устройство сможет считывать NFC-карты.

Нажмите **Access Control** → **Parameter Settings** → **Card Settings** («Контроль доступа → Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.

Выберите **Enable NFC Card** («Включение распознавания NFC-карты») и нажмите **Save** («Сохранить»). После включения устройство сможет считывать NFC-карты. Если данные устройств контроля доступа получены с помощью мобильных устройств, может возникнуть событие несанкционированного доступа. Чтобы предотвратить это, можно отключить функцию NFC.

Вкл. / выкл. карты M1 через веб-клиент

После включения функции устройство сможет считывать M1-карты.

Нажмите **Access Control** → **Parameter Settings** → **Card Settings** («Контроль доступа → Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.

Нажмите **Enable M1 Card** («Включить карту M1»).

Шифрование M1-карты

Включение шифрования M1-карты может повысить уровень безопасности входной карты. Таким образом, входную карту будет сложнее скопировать.

Сектор

После включения шифрования M1-карты необходимо установить зашифрованный сектор.

Примечание

Рекомендуется зашифровать сектор 13.

Нажмите **Save** («Сохранить»).

Вкл. / выкл. ЕМ-карты через веб-клиент

После включения функции устройство сможет считывать ЕМ-карты.

Нажмите **Access Control** → **Parameter Settings** → **Card Settings** («Контроль доступа → Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.

Выберите **Enable EM Card** («Включение распознавания ЕМ-карты») и нажмите **Save** («Сохранить»).

Примечание

- Если подключен периферийный считыватель карт с поддержкой ЕМ-карт, после включения этой функции можно считывать ЕМ-карты через этот считыватель.

- При подключении двухчастотного модуля считывания карт можно одновременно считывать EM-карты и DESfire-карты. Однако считывание карты непосредственно на устройстве не будет работать.

Вкл. / выкл. карты CPU через веб-клиент

После включения функции устройство сможет считывать CPU-карты.

Нажмите **Access Control** → **Parameter Settings** → **Card Settings** («Контроль доступа → Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.

Нажмите **Enable CPU Card** («Включить карту CPU»).

Нажмите **Enable CPU Card Read Content** («Считывание информации с карты CPU»). После включения устройство сможет считывать информацию с карты CPU.

Нажмите **Save** («Сохранить»).

Настройка карты DESFire

Можно включить карту DESFire и считывание информации с карты DESFire.

Нажмите **Parameter Settings** → **Card Settings** («Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.

Выберите **Enable DESFire Card** («Включить карту DESFire») и **DESFire Card Read Content** («Считывание информации с карты DESFire») и нажмите **Save** («Сохранить»).

Примечание

При подключении двухчастотного модуля считывания карт можно одновременно считывать EM-карты и DESfire-карты. Однако считывание карты непосредственно на устройстве не будет работать.

Настройка карты FeliCa

Можно включить карту FeliCa.

Нажмите **Parameter Settings** → **Card Settings** («Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.

Выберите **Enable FeliCa Card** («Включить карту FeliCa»).

Настройка параметров аутентификации по номеру карты через веб-интерфейс

Настройте параметры карты при аутентификации через карту на устройстве.

Нажмите **Access Control** → **Parameter Settings** → **Card Settings** («Контроль доступа → Настройки параметров → Настройки карты»).

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

Полный номер карты

Будет прочитан полный номер карты.

3 байта

Устройство будет считывать карту, используя 3 байта.

4 байта

Устройство будет считывать карту, используя 4 байта.

10.9.8 Настройка удаленной проверки

Устройство загрузит на платформу информацию для аутентификации пользователя. Платформа определит, открывать дверь или нет.

Нажмите **Access Control** → **Parameter Settings** → **Terminal Parameters** («Контроль доступа → Настройки параметров → Параметры терминала»).

Нажмите **Save** («Сохранить») после настройки параметров.

Удаленная проверка

После включения **Remote Authentication** («Удаленная аутентификация») при аутентификации устройство загрузит информацию на платформу для подтверждения открытия двери.

Удаленная проверка типа пользователя

Выберите **Verifying Person Type Remotely** («Удаленная проверка типа пользователя»).

Локальная проверка учетных данных

После включения этой функции устройство проверит разрешения, но не оценит шаблон плана.

Время ожидания удаленной проверки

Установите время ожидания удаленной проверки.

Удаленная проверка разблокировки в режиме офлайн

Можно включить **Offline Remote Verifying Unlocking** («Удаленная проверка разблокировки в режиме офлайн»).

Режим возврата результата

Настройте **Result Return Mode** («Режим возврата результата»).

10.9.9 Настройки конфиденциальности

Настройка типа хранения событий через веб-интерфейс ПК

Можно настроить тип хранения событий.

Нажмите **Access Control** → **Parameter Settings** → **Privacy Settings** («Контроль доступа → Настройки параметров → Настройка параметров конфиденциальности»), чтобы перейти на страницу настроек.

Для параметра **Event Storage Type** («Тип хранения события») можно выбрать: **Delete Old Events Periodically** («Периодическое удаление старых событий»), **Delete Old Events by Specified Time** («Удаление старых событий в заданное время») или **Overwriting** («Перезапись»).

Периодическое удаление старых событий

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

Удаление старых событий в заданное время

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

Перезапись

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

Нажмите **Save** («Сохранить»).

Настройка результатов аутентификации через веб-интерфейс ПК

Настройте информацию для результатов аутентификации, например, изображение, имя, идентификатор сотрудника и температуру.

Нажмите **Access Control** → **Access Control** → **Parameter Settings** → **Privacy Settings** («Контроль доступа → Контроль доступа → Настройки параметров → Настройка параметров конфиденциальности»), чтобы перейти на страницу настроек.

Проверьте отображаемую информацию в результатах аутентификации, например, изображение, имя, идентификатор сотрудника.

Выберите необходимый параметр: **Name De-identification** («Деидентификация имени») и **ID De-identification** («Деидентификация идентификатора»). После деидентификации имени и идентификатора будут отображаться части информации.

Установите **Authentication Result Display Duration** («Длительность отображения результата аутентификации»), и результаты аутентификации будут отображаться в течение заданного периода времени.

Нажмите **Save** («Сохранить»).

Настройка загрузки и хранения изображений через веб-интерфейс ПК

Можно установить параметры загрузки и хранения изображений.

Нажмите **Access Control** → **Parameter Settings** → **Privacy Settings** («Контроль доступа → Настройки параметров → Настройка параметров конфиденциальности»), чтобы перейти на страницу настроек.

Сохранение изображения при аутентификации

Автоматическое сохранение изображений при аутентификации.

Загрузка изображения при аутентификации

Загрузка изображений при автоматической аутентификации на платформу.

Режим изображения

При выборе этого режима по умолчанию устройство будет выполнять захват панорамного вида. Можно установить максимальный размер изображения и разрешение изображения.

При выборе режима кадрирования изображения лица устройство будет захватывать только лица. Можно установить максимальный размер изображения.

Сохранение зарегистрированного изображения

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

Сохранение изображения после захвата

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

Загрузка изображения после захвата

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

Загрузка захваченных изображений во время звонка

Если функция активирована, во время звонков изображения будут автоматически захватываться и загружаться.

Нажмите **Save** («Сохранить»).

Очистка изображений с устройства через веб-интерфейс ПК

Можно удалить все зарегистрированные, авторизованные или захваченные изображения лиц.

Нажмите **Access Control** → **Parameter Settings** → **Privacy Settings** («Контроль доступа → Настройки параметров → Настройка параметров конфиденциальности»), чтобы перейти на страницу настроек.

Нажмите **Clear** («Очистить»), чтобы удалить все зарегистрированные, авторизованные, захваченные изображения лиц или отпечатков ладоней.

Установка PIN-кода через веб-интерфейс ПК

Перед настройкой убедитесь, что PIN-код является персональным PIN-кодом, установленным платформой, или персональным PIN-кодом, установленным устройством. Если PIN-код является персональным PIN-кодом, установленным устройством, можно изменить PIN-код на устройстве или в веб-интерфейсе ПК, но нельзя установить его на платформе. Если PIN-код является персональным PIN-кодом, установленным платформой, необходимо установить PIN-код на платформе, а не на устройстве или в веб-интерфейсе ПК.

Нажмите **Access Control** → **Parameter Settings** → **Privacy Settings** («Контроль доступа → Настройки параметров → Настройки конфиденциальности»).

В модуле режима PIN-кода можно установить следующие параметры. Нажмите **Save** («Сохранить») после завершения настройки.

Персональный PIN-код, настраиваемый через платформу

Можно создать PIN-код пользователя на платформе. PIN-код необходимо применить к устройству. Нельзя создать или изменить PIN-код на устройстве или в веб-интерфейсе ПК.

Персональный PIN-код, настраиваемый через устройство

Можно создать или изменить PIN-код на устройстве или в веб-интерфейсе ПК. Нельзя установить PIN-код на платформе.

Нажмите **Save** («Сохранить»).

10.9.10 Настройки вызова

Настройки № устройства через веб-интерфейс

Устройство может быть установлено снаружи и внутри помещений. Перед использованием необходимо задать номер устройства.

Нажмите **Video Intercom** → **Call Settings** → **Device No.** («Видеодомофон → Параметры вызова → Номер устройства»).

Device Type	Door Station ▼
Period No.	1
Building No.	1
Unit No.	1
Floor No.	1 ▼
Door Station No.	0
Community No.	0

Save

Рисунок 10-1 Настройки № устройства

Если для типа устройства выбран параметр **Door Station** («Вызывная панель»), можно настроить номер этажа, номер вызывной панели, номер микрорайона, номер здания и номер помещения.

Тип устройства

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

Примечание

При изменении типа устройства необходимо перезагрузить устройство.

Номер этажа

Укажите номер этажа, на котором установлено устройство.

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.

Номер микрорайона

Укажите номер микрорайона.

Номер здания

Укажите номер здания.

Номер помещения

Укажите номер помещения.

Примечание

При изменении номера необходимо перезагрузить устройство.

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

Если в качестве типа устройства выбрано **Outer Door Station** («Уличная вызывная панель»), можно настроить номер вызывной панели и номер микрорайона.

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.

Номер микрорайона

Укажите номер микрорайона.

Настройка параметров сети видеодомофона через веб-интерфейс

Можно установить пароль регистрации, IP-адрес пульта консьержа / диспетчера и IP-адрес частного сервера, а также включить протокол 1.0.

Нажмите **Video Intercom** → **Call Settings** → **Video Intercom Network** («Видеодомофон → Параметры вызова → Сеть видеодомофона») для перехода на страницу настроек.

Пароль регистрации

Установите регистрационный пароль пульта консьержа / диспетчера для связи. Установите регистрационный пароль пульта консьержа / диспетчера для связи.

IP-адрес пульта консьержа / диспетчера

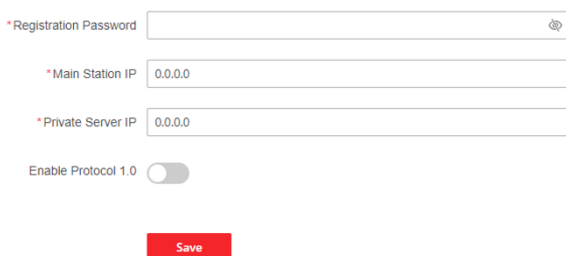
Введите IP-адрес пульта консьержа / диспетчера, используемый для связи.

IP-адрес частного сервера

Относится к IP-адресу SIP-сервера. Введите IP-адрес пульта консьержа / диспетчера, используемый для связи. В настоящее время пульт консьержа / диспетчера используется в качестве SIP-сервера. Для осуществления связи по этому адресу сервера должны быть зарегистрированы другие устройства домофонии.

Включение протокола 1.0

Если эта функция включена, вызывную панель можно зарегистрировать на пульте консьержа / диспетчера с использованием старой версии протокола. Если эта функция отключена, вызывная панель может быть зарегистрирована на пульте консьержа / диспетчера с помощью новой версии протокола.



*Registration Password

*Main Station IP

*Private Server IP

Enable Protocol 1.0 ☐

Save

Рисунок 10-2 Сеть видеодомофона

После настройки можно установить связь между устройствами контроля доступа и вызывной панелью, видеодомофоном, пультом консьержа / диспетчера, платформами и т. д.

Нажмите **Save** («Сохранить»).

Настройка времени связи через веб-интерфейс ПК

Установите макс. время связи.

Перейдите **Video Intercom** → **Call Settings** → **Call Settings** («Видеодомофон → Настройки вызова → Настройки вызова»).

Введите **Max. Communication Time** («Макс. время связи»). Можно включить **Auto Answer** («Автоматический ответ»).

Примечание

Макс. продолжительность связи составляет от 90 до 120 с.

Нажмите **Save** («Сохранить»).

Нажмите кнопку для вызова через веб-интерфейс ПК

Шаги

1. Нажмите **Access Control** → **Call Settings** → **Press Button to Call** («Контроль доступа → Настройки вызова → Нажатие кнопки для вызова»), чтобы перейти на страницу настроек.

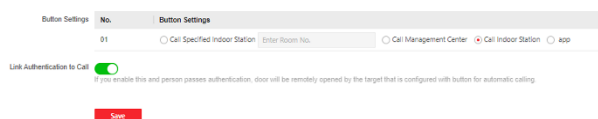


Рисунок 10-3 Нажмите кнопку вызова

2. Выберите **Call Specified Indoor Station** («Вызов настроенного видеодомофона»), **Call Management Center** («Вызов центра управления»), **Call Indoor Station** («Вызов видеодомофона») или **APP** («Приложение»).

Примечание

При выборе **Call Specified Indoor Station** («Вызов настроенного видеодомофона») необходимо ввести **Room No.** («№ помещения») для видеодомофона.

3. Если необходимо, включите **Link Authentication to Call** («Привязка вызова при аутентификации»). После включения, когда человек пройдет аутентификацию, дверь будет удаленно открыта устройством, настроенным с помощью кнопки для автоматического вызова.

4. Нажмите **Save** («Сохранить»).

Приоритет вызова

Можно установить приоритет вызова.

Шаги

1. Нажмите **Video Intercom** → **Call Settings** → **Call Priority** («Видеодомофон → Параметры вызова → Приоритет вызова») для перехода на страницу настроек.

2. Выберите **Call Type** («Тип вызова») и установите **Ring Duration** («Длительность звонка») для каждого из 3 приоритетов.

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

Примечание

Чем выше уровень, тем раньше будет вызвано устройство. После окончания времени вызова запускается следующий уровень вызова.

Настройки номера через веб-интерфейс ПК

Установите SIP-номер для помещения. Между устройствами в помещениях можно установить связь по SIP-номеру.

Шаги

1. Перейдите **Access Control** → **Call Settings** → **Number Settings** («Контроль доступа → Настройки вызова → Настройки номера»).

+ Add Delete

☐	No. ↓	Room No. ↓	SIP Number ↓	Operation
☐	1	4	SIP1 : 114	↙ 🗑
☐	2	5	SIP1 : 115	↙ 🗑
☐	3	2	SIP1 : 116 SIP2 : 114	↙ 🗑
☐	4	6	SIP1 : 116	↙ 🗑
☐	5	1	SIP1 : 2002	↙ 🗑

Рисунок 10-4 Настройки номера

2. Нажмите **Add** («Добавить») и введите **Room No.** («№ помещения») и номер телефона **SIP1**.

3. Опционально. Нажмите **Add** («Добавить»), чтобы добавить номер SIP, или нажмите 🗑, чтобы удалить номер.

4. Нажмите **Save** («Сохранить»).

5. Опционально. Нажмите **Delete** («Удалить»), чтобы удалить номер помещения и его номер SIP.

10.10 Управление устройством

Можно просмотреть номер устройства, тип, IP-адрес, серийный номер, модель, версию, номер этажа, номер комнаты, состояние постановки на охрану, имя пользователя, состояние сети и режим работы. Также можно добавить видеодомофони дополнительную вызывную панель на странице управления устройствами, а также можно управлять, обновлять или удалять устройства.

Шаги

1. Нажмите **Device Management** («Управление устройством»).

2. Нажмите **Add** («Добавить»).

3. Выберите **Device Type** («Тип устройства»), введите **Device Password** («Пароль устройства»), **Registration Password** («Пароль регистрации»), **Serial No.** («Серийный номер»), **IP Address** («IP-адрес»), **IPv4 Subnet Mask** («IPv4-маска подсети»), **IPv4 Default Gateway** («IPv4-шлюз по умолчанию») и **Port** («Порт») (номер этажа и номер видеодомофона вводить не нужно).

4. Нажмите **Save** («Сохранить»).

5. Опционально. Также можно выполнить следующие операции.

Удаление устройства	Отметьте устройства, которые необходимо удалить, и нажмите Delete («Удалить»).
Импорт с устройства	Подключите USB-накопитель (с информацией об устройстве) к устройству, нажмите Import («Импорт»), чтобы импортировать информацию об устройстве.
Экспорт устройства	Нажмите Export («Экспортировать»), чтобы экспортировать файлы с информацией об устройстве на USB-накопитель.

10.11 Конфигурация системы

10.11.1 Просмотр информации об устройстве через веб-интерфейс ПК

Можно просмотреть название устройства, номер устройства, язык, модель, серийный номер, версию, количество каналов, интерфейсы выходов / входов, состояние замка, локальный номер RS-485, номер регистра, тревожный вход, тревожный выход, емкость устройства и т. д.

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

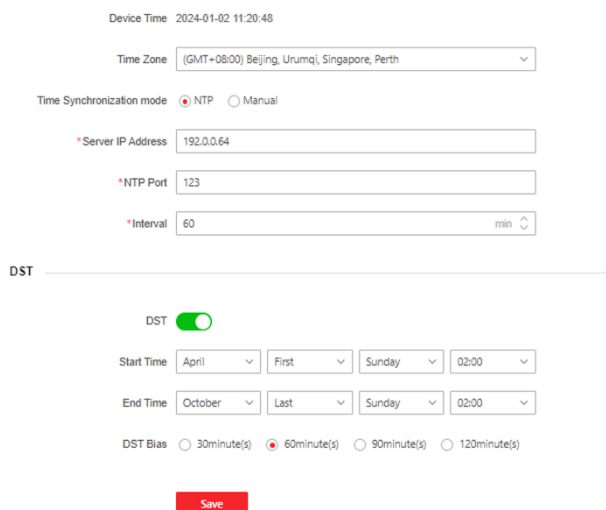
Можно просмотреть название устройства, номер устройства, язык, модель, серийный номер, версию, количество каналов, интерфейсы выходов / входов, состояние замка, локальный номер RS-485, номер регистра, тревожный вход, тревожный выход, емкость устройства и т. д.

Нажмите **Upgrade** («Обновить») в разделе версии прошивки, чтобы перейти на страницу обновления и обновить устройство.

10.11.2 Настройка времени

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

Нажмите **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Time Settings** («Система и обслуживание → Конфигурация системы → Система → Настройки системы → Настройка времени»).



Device Time 2024-01-02 11:20:48

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

Time Synchronization mode ☒ NTP ☐ Manual

*Server IP Address 192.0.0.64

*NTP Port 123

*Interval 60 min

DST

DST ☒

Start Time April First Sunday 02:00

End Time October Last Sunday 02:00

DST Bias ☐ 30minute(s) ☒ 60minute(s) ☐ 90minute(s) ☐ 120minute(s)

Save

Рисунок 10-5 Настройка времени

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

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

NTP

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

Вручную

По умолчанию время устройства должно быть синхронизировано вручную.

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

Тип адреса сервера / Адрес сервера / Порт NTP / Интервал

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

10.11.3 Изменение пароля администратора

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **User Management** («Система и обслуживание → Конфигурация системы → Система → Управление пользователем → Управление пользователем»).
2. Нажмите .
3. Введите старый пароль и создайте новый пароль.
4. Подтвердите новый пароль.
5. Нажмите **Save** («Сохранить»).

Предостережение

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя 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 безопаснее.

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

10.11.4 Настройки безопасности учетной записи через веб-интерфейс ПК

Можно изменить контрольные вопросы и ответы или адрес электронной почты для устройства. Если после изменения настроек вы забыли пароль устройства, необходимо ответить на новые вопросы или использовать новый адрес электронной почты для сброса пароля устройства.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **User Management** → **Account Security Settings** («Система и обслуживание → Конфигурация системы → Система → Управление пользователем → Управление пользователем → Настройки безопасности учетной записи»).
2. Установите контрольные вопросы и адрес электронной почты.
3. Введите пароль устройства и нажмите **ОК** для подтверждения изменений.

10.11.5 Просмотр информации о постановке / снятии устройства с охраны через веб-интерфейс ПК

Просмотр информации о постановке устройства на охрану и IP-адреса постановки на охрану.

Перейдите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **Arming/Disarming Information** («Система и обслуживание → Конфигурация системы → Система → Управление пользователями → Информация о постановке на охрану / снятии с охраны»).

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

10.11.6 Настройка рабочего режима через веб-интерфейс ПК

Можно настроить параметры терминала устройства.

Примечание

Эта функция поддерживается только некоторыми моделями, обратитесь к информации о конкретном устройстве.

Нажмите **Access Control** → **Parameter Settings** → **Terminal Parameters** («Контроль доступа → Настройки параметров → Параметры терминала»), чтобы перейти на страницу настроек.

Рабочий режим

Для рабочего режима можно выбрать режим контроля доступа или режим без разрешений.

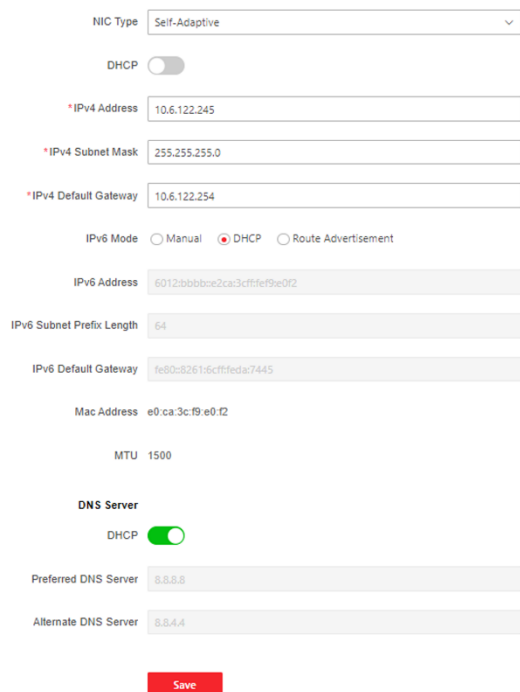
Режим контроля доступа

Режим контроля доступа является нормальным режимом работы устройства. Для получения доступа необходимо пройти аутентификацию с использованием учетных данных.

10.11.7 Настройка сетевых параметров

Настройка базовых параметров сети через веб-интерфейс ПК

Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **TCP/IP** («Система и обслуживание → Конфигурация системы → Сеть → Настройки сети → TCP/IP»).



NIC Type: Self-Adaptive

DHCP: ☐

*IPv4 Address: 10.6.122.245

*IPv4 Subnet Mask: 255.255.255.0

*IPv4 Default Gateway: 10.6.122.254

IPv6 Mode: ☐ Manual ☒ DHCP ☐ Route Advertisement

IPv6 Address: 6012:bbbbb:2ca:3c:ff:fe9e0f2

IPv6 Subnet Prefix Length: 64

IPv6 Default Gateway: fe80::8261:6c:ff:fe9e0f2

Mac Address: e0:ca:3c:f9:e0:f2

MTU: 1500

DNS Server: ☐

DHCP: ☒

Preferred DNS Server: 8.8.8.8

Alternate DNS Server: 8.8.4.4

Save

Рисунок 10-6 Страница настроек TCP/IP

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

Тип NIC

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

DHCP

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

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

DNS-сервер

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

Настройка параметров Wi-Fi

Задайте параметры Wi-Fi для беспроводного подключения устройства.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **Wi-Fi** («Система и обслуживание → Конфигурация системы → Сеть → Настройки сети → Wi-Fi»).

Рисунок 10-7 Страница настроек Wi-Fi

2. Нажмите **Wi-Fi** («Wi-Fi»).

3. Выберите Wi-Fi

- Нажмите и введите пароль Wi-Fi для подключения.
- Нажмите **Add** («Добавить») и введите имя, пароль и тип шифрования Wi-Fi. Нажмите **Connect** («Подключить»). Когда Wi-Fi подключен, нажмите **OK**.

4. Опционально. Настройте параметры WLAN.

1) Настройте IP-адрес, маску подсети и шлюз по умолчанию. Или включите DHCP, и система автоматически задаст IP-адрес, маску подсети и по умолчанию шлюз.

5. Нажмите **Save** («Сохранить»).

Настройка порта через веб-интерфейс ПК

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба»).

Вкл. / выкл. HTTP

Включите функцию HTTP для повышения безопасности посещения браузера.

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **HTTP(S)** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба → HTTP(S)»).

Нажмите **Save** («Сохранить») после настройки параметров.

Порт HTTP

При входе через браузер необходимо добавить измененный номер порта после адреса. Например, если номер HTTP-порта изменен на 81, необходимо ввести `http://192.0.0.65:81` при входе в систему с помощью веб-интерфейса.

Порт HTTPS

Установите порт HTTPS для посещения веб-интерфейса. Но требуется сертификация.

Прослушивание HTTP

Устройство будет отправлять информацию о тревоге на целевой IP-адрес или доменное имя по протоколу HTTP. Целевой IP-адрес или доменное имя должны поддерживать протокол HTTP. Введите целевой IP-адрес или доменное имя, URL-адрес и порт. И выберите тип протокола.

Просмотр порта RTSP через веб-интерфейс ПК

Порт RTSP – это порт протокола потоковой передачи в режиме реального времени.

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **RTSP** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба → RTSP»).

Просмотрите порт.

Настройка WebSocket(s) через веб-интерфейс ПК

Просмотрите порт WebSocket и WebSockets.

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **WebSocket(s)** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба → WebSocket(s)»).

Просмотрите порт WebSocket и WebSockets.

Включение службы SDK

После включения службы SDK устройство может подключиться к серверу SDK.

Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **SDK Server** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → Сервер SDK») для перехода на страницу настроек.

Введите **Server Port** («Порт сервера»).

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

Настройка параметров ISUP через веб-интерфейс ПК

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **ISUP** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → ISUP»).

2. Нажмите **Enable** («Включить»).

3. Установите версию ISUP, адрес сервера, идентификатор устройства и статус ISUP.

Примечание

Если выбрана версия 5.0, необходимо также установить ключ шифрования.

4. 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.

5. Нажмите **Save** («Сохранить»).

Настройка ОТАР через веб-интерфейс ПК

Подключите устройство к платформе по протоколу ОТАР, чтобы получить информацию об устройстве, загрузить информацию о состоянии работы и тревогах, перезагрузить и обновить устройство.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **ОТАР** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → ОТАР»).

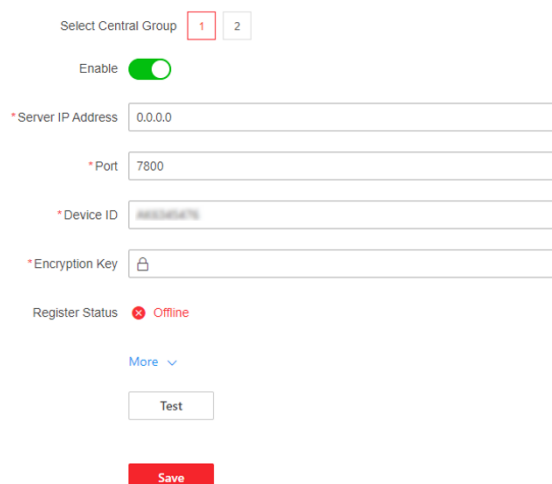


Рисунок 10-8 Настройка OTAP

2. Нажмите **Enable** («Включить»), чтобы включить OTAP.
3. Установите **Server IP Address** («IP-адрес сервера»), **Port** («Порт»), **Device ID** («ID-устройства») и **Encryption Key** («Ключ шифрования»).
4. Нажмите **Test** («Диагностика»), чтобы убедиться, что устройство может подключиться к серверу и успешно зарегистрироваться. Обновите страницу или перезагрузите устройство, чтобы увидеть **Register Status** («Состояние регистрации»).
5. Нажмите **More** («Дополнительно»), чтобы просмотреть тип сети и приоритет доступа. Перетащите значок операции вверх или вниз, чтобы отрегулировать приоритет сети.
6. Нажмите **Save** («Сохранить»).

Доступ к платформе через веб-интерфейс ПК

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **Hik-Connect** («Система и обслуживание» → Конфигурация системы → Сеть → Доступ к устройству → Hik-Connect») для перехода на страницу настроек.

Примечание

Nik-Connect — это приложение 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. Опционально. Поставьте галочку возле **Custom** («Пользовательская настройка»), чтобы настроить адрес сервера самостоятельно.
4. Введите проверочный код.
5. Нажмите **View** («Просмотр»), чтобы просмотреть QR-код устройства. Сканируйте QR-код, чтобы выполнить привязку учетной записи.

Примечание

От 8 до 32 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 сохранения настроек.

Настройки учетной записи VoIP

Можно совершать голосовые вызовы по сети.

Шаги

1. Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **VoIP** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → VoIP»).
2. Нажмите **Call Type** («Тип звонка») и выберите VoIP.
3. Включите **VoIP Gateway** («VoIP-шлюз»).
4. Настройте **Register User Name** («Зарегистрированное имя пользователя»), **Registration Password** («Пароль регистрации»), **Server IP Address** («IP-адрес сервера»), **Server Port** («Порт сервера»), **Expiry Time** («Время истечения срока

действия»), **Register Status** («Состояние регистрации»), **Number** («Номер»), **Display User Name** («Отображение имени пользователя») и **Center No.** («Номер центра»).

5. Нажмите **Save** («Сохранить»).

10.11.8 Настройка параметров видео и аудио через веб-интерфейс ПК

Настройка параметров видео через веб-интерфейс

Можно настроить качество, разрешение и другие параметры камеры устройства.

Нажмите **System and Maintenance** → **System Configuration** → **Video/Audio** → **Video** («Система и обслуживание → Конфигурация системы → Видео / аудио → Видео») для перехода на страницу настроек.

Установите название камеры, тип потока, тип видео, разрешение, тип битрейта, качество видео, частоту кадров, максимальный битрейт, кодирование видео и интервал I-кадров.

Нажмите **Save** («Сохранить»).

Настройка параметров аудио через веб-интерфейс

Можно настроить громкость устройства.

Нажмите **System and Maintenance** → **System Configuration** → **Video/Audio** → **Audio** («Система и обслуживание → Конфигурация системы → Видео / аудио → Аудио») для перехода на страницу настроек.

Настройте тип потока и кодирование звука. Переместите ползунок для установки громкости входа и выхода.

Переместите ползунок для включения функции голосовых подсказок.

Можно включить **Audio Mixing** («Микширование звука») и настроить **Output Sub-Volume** («Громкость выхода»).

Выберите **SIP Audio Encoding** («Кодирование аудио SIP»).

Нажмите **Save** («Сохранить»).

10.11.9 Конфигурация доступа

Настройка параметров RS-485 через веб-интерфейс ПК

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

Нажмите **System and Maintenance** → **System Configuration** → **Access Configuration** → **RS-485** («Система и обслуживание → Конфигурация системы → Конфигурация доступа → RS-485») для перехода на страницу настроек.

Выберите **RS-485 Protocol** («Протокол RS-485»).

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

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

№

Настройте номер RS-485.

Тип периферийного устройства

Выберите необходимое периферийное устройство из выпадающего списка.

Примечание

После настройки и сохранения периферийного устройства устройство автоматически перезагрузится.

Адрес RS-485

Задайте необходимый адрес RS-485.

Примечание

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

Скорость передачи данных

Скорость передачи при обмене данными по протоколу RS-485.

Настройка параметров Wiegand через веб-интерфейс ПК

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 **System and Maintenance** → **System Configuration** → **Access Configuration** → **Wiegand Settings** («Система и обслуживание → Конфигурация системы → Конфигурация доступа → Настройки Wiegand»).

Рисунок 10-9 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. Нажмите **Save** («Сохранить») для сохранения настроек.

Примечание

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

10.11.10 Настройка параметров изображения

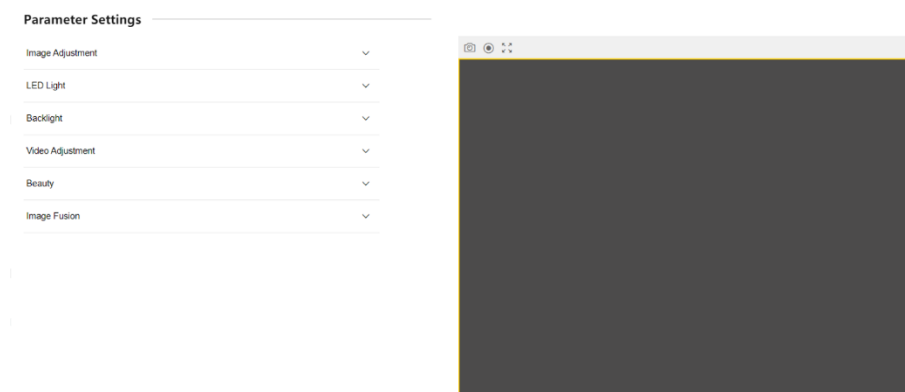


Рисунок 10-10 Настройки отображения

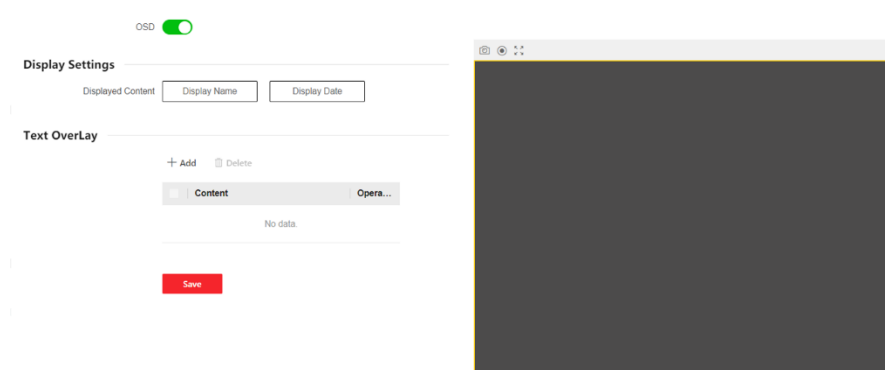


Рисунок 10-11 Настройки OSD режима

Настройка яркости / контрастности / насыщенности / резкости через веб-интерфейс ПК

Можно настроить параметры изображения, включая яркость, контрастность, насыщенность и резкость на странице просмотра в режиме реального времени.

Нажмите **System and Maintenance** → **System Configuration** → **Image** → **Display Settings** («Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения») для перехода на страницу настроек.

Настройка изображения

Переместите курсор мыши или введите число, чтобы установить яркость, контрастность, насыщенность и резкость.

Нажмите **Restore Default Settings** («Восстановить настройки по умолчанию»), чтобы восстановить настройки по умолчанию.

Настройка LED-подсветки через веб-интерфейс ПК

Можно отрегулировать яркость дополнительной подсветки.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Image** → **Display Settings** («Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения») для перехода на страницу настроек.
2. Установите тип, режим и яркость дополнительной подсветки.
3. Опционально. Нажмите **Restore Default Settings** («Восстановить настройки по умолчанию»), чтобы восстановить настройки по умолчанию.

Настройка видеостандарта через веб-интерфейс ПК

Можно установить видеостандарт на странице просмотра в режиме реального времени.

Нажмите **System and Maintenance** → **System Configuration** → **Image** → **Display Settings** («Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения») для перехода на страницу настроек.

Настройка видео

Установите частоту кадров видео во время удаленного предварительного просмотра. Для вступления новых настроек в силу необходимо перезагрузить устройство.

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.

Нажмите **Restore Default Settings** («Восстановить настройки по умолчанию»), чтобы восстановить настройки по умолчанию.

10.11.11 Настройки привязки

При срабатывании настроенного события загрузите информацию о событии на центральную платформу в соответствии с настроенным методом.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Event** → **Linkage Settings** («Система и обслуживание → Конфигурация системы → Событие → Настройки привязки») для перехода на страницу настроек.

2. Нажмите + .

3. Настройте источник события. Выберите тип привязки: **Event Linkage** («Привязка события»), **Card Linkage** («Привязка карты») или **Link Employee ID** («Привязка идентификатора сотрудника»).

- При выборе **Event Linkage** («Привязка события») в качестве типа привязки укажите необходимые типы событий.
- При выборе **Card Linkage** («Привязка карты») в качестве типа привязки введите номер карты и укажите считыватель карт.
- При выборе **Link Employee ID** («Привязка идентификатора сотрудника») введите идентификатор сотрудника и укажите считыватель карт.

4. Настройте действия привязки.

1) Включите **Door Linkage** («Привязка двери»), установите флажок и выберите действие двери.

2) Включите **Linked Capture** («Привязанный захват»).

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

10.11.12 Настройка учета рабочего времени (УРВ)

Если необходимо регистрировать рабочее время сотрудника, опоздания, ранние уходы, перерывы, прогулы и т. д., то можно добавить сотрудника в группу смен и назначить группе смен расписание смен (правило УРВ, определяющее, как расписание повторяется, тип смены, настройки перерывов и правило считывания карт), чтобы определить параметры УРВ для сотрудников в группе смен.

Отключение функции учета рабочего времени через веб-интерфейс

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

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Platform Attendance** («Система и обслуживание → Конфигурация системы → УРВ через платформу») для перехода на страницу настроек.
2. Отключите **Time and Attendance** («УРВ»).

Результат

На начальной странице не будут отображаться статусы УРВ и интерфейс настроек учета рабочего времени. Система будет следовать правилам УРВ, настроенным на платформе.

Настройка параметров учета рабочего времени вручную через веб-интерфейс

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

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Подробная информация представлена в разделе **Управление пользователями**.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Platform Attendance** («Система и обслуживание → Конфигурация системы → УРВ через платформу») для перехода на страницу настроек.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual** («Подсчет вручную»).
3. Нажмите **Attendance Status Required** («Требуется УРВ») и укажите продолжительность состояния УРВ.
4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

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

Результат

При аутентификации можно вручную выбрать статус УРВ.

Примечание

Если не выбрать статус, аутентификация будет неудачной.

Настройка параметров автоматического учета рабочего времени через веб-интерфейс

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

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Подробная информация представлена в разделе **Управление пользователями**.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Platform Attendance** («Система и обслуживание → Конфигурация системы → УРВ через платформу») для перехода на страницу настроек.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Auto** («Автоматически»).
3. Включите **Attendance Status Required** («Требуется УРВ»).
4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

5. Опционально. Выберите статус и при необходимости измените его название.
6. Установите расписание статуса.

Настройка параметров автоматического УРВ и УРВ вручную через веб-интерфейс

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

Перед началом

Добавьте хотя бы одного пользователя и установите режим аутентификации пользователя. Подробная информация представлена в разделе **Управление пользователями**.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Platform Attendance** («Система и обслуживание → Конфигурация системы → УРВ через платформу») для перехода на страницу настроек.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual and Auto** («Подсчет автоматически и вручную»).
3. Включите **Attendance Status Required** («Требуется УРВ»).
4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

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

6. Установите расписание статуса.

Результат

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

Пример

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

10.12 Пользовательские настройки

10.12.1 Настройка изображения в режиме ожидания через веб-интерфейс ПК

Установите параметры изображения в режиме ожидания, включая время перехода в режим ожидания, изображение заставки, эффект отображения и интервал показа слайдов.

Перейдите **System and Maintenance** → **Preference** → **Screen Display** («Система и обслуживание → Пользовательская настройка → Отображение»).

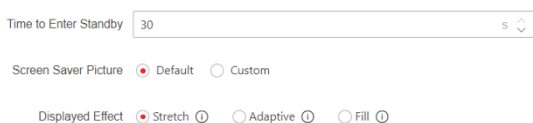


Рисунок 10-12 Настройки изображения в режиме ожидания

Установите параметры изображения в режиме ожидания и нажмите **Save** («Сохранить»).

Время перехода в режим ожидания

Устройство отобразит изображение в режиме ожидания по истечении заданного промежутка времени.

Изображение заставки

Установите изображения в режиме ожидания в качестве изображения по умолчанию или пользовательского изображения. Выберите **Custom** («Пользовательский») и нажмите +, чтобы загрузить изображение для режима ожидания из локального интерфейса.

Примечание

Допускается не более 3 изображений. Размер одного изображения: не более 1024 КБ; формат: jpg.

Эффект отображения

Установите эффект отображения изображения в режиме ожидания: **Stretch** («Растянуть»), **Adaptive** («Адаптировать») или **Fill** («Заполнить»).

Интервал показа слайдов

Если добавить несколько изображений, можно установить время переключения между ними.

10.12.2 Настройка спящего режима через веб-интерфейс ПК

Устройство перейдет в спящий режим по истечении заданного промежутка времени. Эта функция позволяет снизить энергопотребление.

Перейдите **System and Maintenance** → **Preference** → **Screen Display** («Система и обслуживание» → Пользовательская настройка → Отображение»).



Рисунок 10-13 Настройки спящего режима

Переместите ползунок **Sleep** («Спящий режим») и установите время.

Нажмите **Save** («Сохранить»).

10.12.3 Настройка панели аутентификации через веб-интерфейс ПК

Настройте модули на странице / панели аутентификации.

Шаги

1. Перейдите **System and Maintenance** → **Preference** → **Custom Home Page** («Система и обслуживание → Пользовательская настройка → Настройка главной страницы»).
2. Выберите **Application Mode** («Режим применения»).

Режим доступа

Страница аутентификации устройства будет отображаться на странице просмотра в режиме реального времени. Имя сотрудника, идентификатор сотрудника и изображения лица будут отображаться после аутентификации.

Режим домофонии

Интерфейс аутентификации отображает область быстрого доступа и область аутентификации. Область быстрого доступа поддерживает настраиваемые сочетания клавиш для функций.

Простая

После выбора этого режима отображение страницы аутентификации в реальном времени будет отключено. Имя, идентификатор сотрудника, изображение лица будут скрыты после аутентификации.

3. Нажмите **Apply** («Применить»).

10.12.4 Настройка отображения уведомлений через веб-интерфейс ПК

Можно настроить отображение уведомления для устройства.

Перейдите **System and Maintenance** → **Preference** → **Notice Publication** («Система и обслуживание → Пользовательская настройка → Отображение уведомлений»).

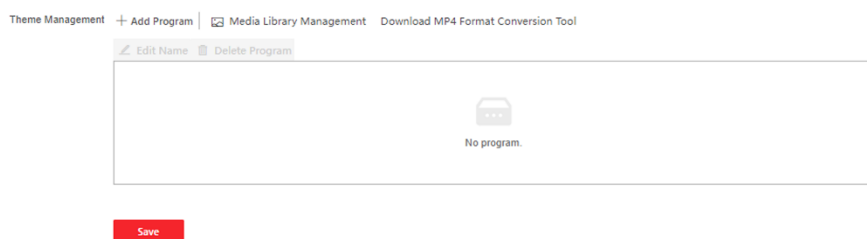


Рисунок 10-14 Отображение уведомления

Загрузка инструмента преобразования в формат MP4

Если необходимо изменить формат, нажмите **Download MP4 Format Conversion Tool** («Загрузить инструмент преобразования в формат MP4»).

Управление материалами

Можно нажать **+ Add Theme** («Добавить тему») и установить **Theme Name** («Название темы») и **Theme Type** («Тип темы»).

Нажмите **Upload** («Загрузить»), а затем **+**, чтобы загрузить изображение или видео с локального ПК.

Примечание

В настоящее время можно добавить только одну тему.

Добавление программы

Можно задать название программы и выбрать тип программы.

Изображение

Чтобы добавить изображение, нажмите кнопку **+**.

Приветственное сообщение

Можно установить шаблон, отображаемую информацию, размер шрифта и цвет основного текста и подзаголовка. Также можно настроить фоновое изображение.

Стандартный режим

При выборе стандартного режима можно установить цвет фона и изображение.

Создание расписания

После создания темы можно выбрать тему и настроить расписание на временной шкале.

Выберите настроенное расписание и задайте точное время начала и окончания, если необходимо.

Чтобы удалить расписание, выберите настроенное расписание и нажмите **Delete** («Удалить») или **Delete All** («Удалить все»).

Интервал показа слайдов

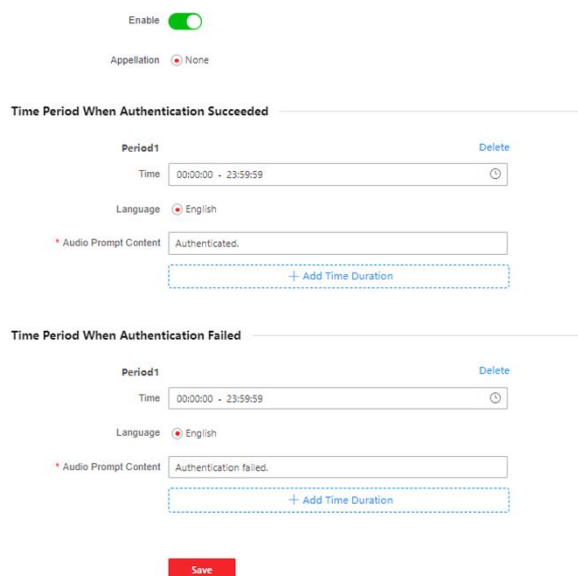
Переместите курсор мыши или введите число, чтобы установить интервала показа слайдов. Изображения и видео будут меняться в соответствии с интервалом.

10.12.5 Настройка расписания подсказок через веб-интерфейс ПК

Настройте голосовые предупреждения для случаев успешной аутентификации и сбоев аутентификации.

Шаги

1. Перейдите **System and Maintenance** → **Preference** → **Prompt Schedule** («Система и обслуживание → Пользовательская настройка → Расписание подсказок»).



Enable ☒

Appellation ☐ None

Time Period When Authentication Succeeded

Period1 Delete

Time 00:00:00 - 23:59:59

Language ☒ English

* Audio Prompt Content Authenticated.

+ Add Time Duration

Time Period When Authentication Failed

Period1 Delete

Time 00:00:00 - 23:59:59

Language ☒ English

* Audio Prompt Content Authentication failed.

+ Add Time Duration

Save

Рисунок 10-15 Настройка расписания подсказок

2. Включите функцию.

3. Укажите наименование.
4. Выберите расписание по времени.
5. Настройте период предупреждения при успешной аутентификации.
 - 1) Нажмите **Add Time Duration** («Добавить продолжительность»).
 - 2) Установите продолжительность времени.

Примечание

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

- 3) Установите содержимое голосовых подсказок.
- 4) Опционально. Повторите шаги от 1 до 3.
- 5) Опционально. Нажмите , чтобы сбросить настроенную продолжительность предупреждения.
6. Установите продолжительность предупреждения при сбое аутентификации.
 - 1) Нажмите **Add Time Duration** («Добавить продолжительность»).
 - 2) Установите продолжительность времени.

Примечание

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

- 3) Установите содержимое голосовых подсказок.
- 4) Опционально. Повторите шаги от 1 до 3.
- 5) Опционально. Нажмите , чтобы сбросить настроенную продолжительность предупреждения.
7. Нажмите **Save** («Сохранить») для сохранения настроек.

10.12.6 Настройка голосовых подсказок через веб-интерфейс ПК

Также можно настроить голосовую подсказку для устройств.

Шаги

1. Перейдите **System and Maintenance** → **Preference** → **Custom Prompt** («Система и обслуживание → Пользовательская настройка → Пользовательская настройка подсказки»).

Custom Type	Importing Status	Operation
Call Center	Not Imported	
Nobody Answered	Not Imported	
Thanks	Not Imported	
Authenticating Failed	Not Imported	
The Door Is Open	Not Imported	
Please Wear the Safety Helmet	Not Imported	
Please Wear the Mask	Not Imported	

Рисунок 10-16 Пользовательская настройка подсказок

2. Нажмите → и импортируйте аудиофайл с локального компьютера.

Примечание

Загруженный аудиофайл должен иметь размер не более 512 КБ, в формате WAV.

10.12.7 Настройка текста результата аутентификации через веб-интерфейс ПК

Шаги

1. Перейдите **System and Maintenance** → **Preference** → **Authentication Result Text** («Система и обслуживание → Пользовательская настройка → Текст результата аутентификации»).

Customize Authentication Resu... ☒

Text	Content	Custom
* Stranger		
* Authenticated		
* Authenticating Failed		

Рисунок 10-17 Текст результата аутентификации

2. Включить **Customize Authentication Result Text** («Настройка текста результата аутентификации»).

3. Введите текст.

4. Нажмите **Save** («Сохранить»).

10.13 Система и обслуживание

10.13.1 Перезагрузка

Перезагрузите устройство.

Нажмите **System and Maintenance** → **Maintenance** → **Restart** («Система и обслуживание → Обслуживание → Перезагрузка») для перехода на страницу настроек.

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

10.13.2 Обновление

Локальное обновление через веб-интерфейс ПК

Можно обновить устройство локально.

Нажмите **System and Maintenance** → **Maintenance** → **Upgrade** («Система и обслуживание → Обслуживание → Обновление») для перехода на страницу настроек.

Выберите тип обновления из выпадающего списка. Нажмите  и выберите файл обновления с локального ПК. Нажмите **Upgrade** («Обновить»), чтобы начать обновление.

Онлайн обновление через веб-интерфейс ПК

Можно обновить устройство онлайн.

Нажмите **System and Maintenance** → **Maintenance** → **Upgrade** («Система и обслуживание → Обслуживание → Обновление») для перехода на страницу настроек.

Нажмите **Check for Updates** («Проверить обновления»), чтобы проверить наличие обновленных версий.

Если устройство подключено к сети и добавлено в приложение Hik-Connect, можно нажать **Device Upgrade** → **Online Upgrade** («Обновление устройства → Онлайн обновление») на устройстве для обновления, когда в приложении Hik-Connect появится обновленная версия.

Обновление брелока

Примечание

- Убедитесь, что периферийный модуль подключен к сети.
- При обновлении брелока держите рядом только один терминал распознавания лиц и не перемещайте брелок.

Нажмите **System and Maintenance** → **Maintenance** → **Upgrade** («Система и обслуживание → Обслуживание → Обновление»). В раскрывающемся списке настроек обновления выберите **Keyfob** («Брелок»). Выберите файл обновления с локального ПК. Нажмите **Upgrade** → **OK** («Обновление → ОК»). Нажмите любую кнопку брелока для обновления.

10.13.3 Восстановление настроек

Восстановление заводских настроек через веб-интерфейс

Можно восстановить устройство до заводских настроек.

Нажмите **System and Maintenance** → **Maintenance** → **Backup and Reset** («Система и обслуживание → Обслуживание → Резервное копирование и сброс») для перехода на страницу настроек.

Нажмите **Restore All** («Восстановить все»), и все параметры будут восстановлены до заводских настроек. Перед первым входом в систему необходимо активировать устройство.

Восстановление настроек по умолчанию через веб-интерфейс ПК

Можно восстановить устройство до настроек по умолчанию.

Нажмите **System and Maintenance** → **Maintenance** → **Backup and Reset** («Система и обслуживание → Обслуживание → Резервное копирование и сброс») для перехода на страницу настроек.

Нажмите **Restore** («Восстановить»), и устройство будет восстановлено до настроек по умолчанию, за исключением IP-адреса устройства и информации о пользователе.

10.13.4 Экспорт параметров устройства через веб-интерфейс ПК

Экспорт параметров устройства.

Перейдите **System and Maintenance** → **Maintenance** → **Backup and Reset** («Система и обслуживание → Обслуживание → Резервное копирование и сброс»).

Резервное копирование

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

Примечание

Экспортируйте параметры устройства и импортируйте эти параметры на другие устройства.

10.13.5 Импорт параметров устройства через веб-интерфейс ПК

Импорт параметров конфигурации.

Перейдите **System and Maintenance** → **Maintenance** → **Backup and Reset** («Система и обслуживание → Обслуживание → Резервное копирование и сброс»).

Импорт файла конфигурации

Нажмите  и выберите файл с локального компьютера. Нажмите **Import** («Импорт»).

10.13.6 Отладка устройства

Можно настроить параметры отладки устройства.

Вкл. / выкл. SSH через веб-интерфейс

Можно включить SSH для удаленной отладки.

Нажмите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Log for Debugging** («Система и обслуживание → Обслуживание → Отладка устройства → Журнал отладки»).

Включение SSH

SSH используется для удаленной отладки. Если служба не требуется, рекомендуется отключить SSH для повышения безопасности.

Печать журнала устройства через веб-интерфейс ПК

Можно распечатать журнал устройства.

Нажмите **System and Maintenance** → **Maintenance** → **Log** («Система и обслуживание → Обслуживание → Журнал») для перехода на страницу настроек.

Нажмите **Export** («Экспорт»), чтобы распечатать журнал устройства.

Захват сетевого пакета через веб-интерфейс ПК

Установите длительность и размер захватываемого пакета и выполните захват. Можно просмотреть журнал и выполнить отладку в соответствии с результатами захвата.

Перейдите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Log for Debugging** («Система и обслуживание → Обслуживание → Отладка устройства → Журнал отладки»).

Настройте **Capture Packet Duration** («Длительность захвата пакета») и **Capture Packet Size** («Размер захвата пакета»), затем нажмите **Start Capture** («Начать захват»).

Тестирование протокола через веб-интерфейс ПК

Выберите адрес протокола и введите протокол для тестирования. Можно выполнять отладку устройства в соответствии с заголовком ответа и полученным результатом.

Перейдите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Protocol Testing** («Система и обслуживание → Обслуживание → Отладка устройства → Тестирование протокола»).

*Enter Protocol Address

GET

Enter /ISAPI/...

Execute

Testing Result

Response Header

Return Value

Рисунок 10-18 Тестирование протокола

Выберите адрес протокола и введите протокол. Нажмите **Execute** («Выполнить»).

Выполняйте отладку устройства в соответствии с заголовком ответа и полученным результатом.

Диагностика сети через веб-интерфейс ПК

Введите IP-адрес устройства или доменное имя, чтобы выполнить настройку PING. Выполните отладку сети в соответствии с результатом PING.

Перейдите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Network Diagnosis** («Система и обслуживание» → «Обслуживание» → «Отладка устройства» → «Диагностика сети»).

*IP/Domain

Network Connection Mode

☐ Wired Network
 ☒ Self-Adaptive

Ping Duration

1

s

*Ping Data Package Size

64

Bytes

Diagnose

Ping Result

Рисунок 10-19 Диагностика сети

Введите IP-адрес устройства для выполнения операции PING, выберите режим сетевого подключения, продолжительность PING и размер пакета данных PING (рекомендуется использовать параметры по умолчанию). Нажмите **Diagnose** («Диагностика»). Результат будет отображен в разделе **PING Result** («Результаты PING»).

Настройка службы проверки на проникновение в сеть через веб-интерфейс ПК

После развертывания устройства в локальной сети можно включить службу проверки на проникновение для удаленного управления устройством.

Шаги

1. Перейдите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Network Penetration Service** («Система и обслуживание → Обслуживание → Отладка устройства → Служба проверки на проникновение в сеть»).
2. Переведите ползунок **Enable Penetration Service** («Включить службу проверки на проникновение»).
3. Установите **Server IP Address** («IP-адрес сервера») и **Server Port** («Порт сервера»). Создайте **User Name** («Имя пользователя») и **Password** («Пароль»).
4. Опционально. Можно настроить **Heartbeat Timeout** («Период цикла Heartbeat»). Диапазон значений: от 1 до 6000.
5. Опционально. Можно посмотреть состояние службы проверки на проникновение. Нажмите **Refresh** («Обновить»), чтобы обновить состояние.
6. Нажмите **Save** («Сохранить»).

Примечание

Служба проверки на проникновение будет автоматически отключена через 48 часов.

10.13.7 Просмотр журнала через веб-интерфейс ПК

Можно искать и просматривать журналы устройства.

Перейдите **System and Maintenance** → **Maintenance** → **Log** («Система и обслуживание → 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.

10.13.8 Расширенные настройки через веб-интерфейс ПК

Можно настроить параметры лица, параметры ладони и просмотреть информацию о версии.

Перейдите **System and Maintenance** → **Maintenance** → **Advanced Settings** («Система и обслуживание → Обслуживание → Расширенные настройки»).

Введите пароль активации устройства и нажмите **Enter**.

Параметры изображения лица

Включите **Custom Anti-Spoofing Detection** («Настройка детекции подлинности биометрических данных (антиспуфинг)») и установите **Anti-Spoofing Detection Threshold 1:1** («Пороговое значение детекции подлинности биометрических данных (антиспуфинг) 1:1»), **Anti-Spoofing Detection Threshold 1:N** («Пороговое значение детекции подлинности биометрических данных (антиспуфинг) 1:N»).

Включите **Lock Face for Authentication** («Блокировка лица для аутентификации») и установите **Lock Duration** («Длительность блокировки»). После достижения лимита неудачных попыток детекции подлинности биометрических данных лица, распознавание лица будет заблокировано на заданный период блокировки.

Нажмите **Save** («Сохранить»).

Параметры отпечатка ладони

Включите **Custom Anti-Spoofing Detection** («Настройка детекции подлинности биометрических данных (антиспуфинг)») и установите **Anti-Spoofing Detection Threshold** («Пороговое значение детекции подлинности биометрических данных (антиспуфинг)»).

Нажмите **Save** («Сохранить»).

Информация о версии устройства

Здесь можно просмотреть информацию о различных версиях.

10.13.9 Управление безопасностью

Установите уровень безопасности при входе в веб-интерфейс ПК.

Перейдите **System and Maintenance** → **Safe** → **Security Service** («Система и обслуживание → Безопасность → Служба безопасности»).

Режим безопасности

Высокий уровень безопасности при входе в систему и проверке информации о пользователе.

Режим совместимости

Совместимость со старым методом проверки пользователя.

Нажмите **Save** («Сохранить»).

10.13.10 Управление сертификатами

Помогает управлять сертификатами сервера/клиента и сертификатом СА.

 **Примечание**

Данная функция поддерживается только у определенных моделей устройств.

Создание и импорт самозаверенного сертификата

Шаги

1. Перейдите **System and Maintenance** → **Safe** → **Certificate Management** («Система и обслуживание → 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 **ОК**, 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 Key** («Импорт ключа»). Выберите сертификат из локального хранения и нажмите **Import** («Импорт»).

2) Выберите тип сертификата в области **Import Communication Certificate** («Импорт сертификата связи»), затем выберите сертификат на локальном компьютере и нажмите **Import** («Импорт»).

Импорт другого авторизованного сертификата

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

Шаги

1. Перейдите **System and Maintenance** → **Safe** → **Certificate Management** («Система и обслуживание → Безопасность → Управление сертификатами»).
2. В областях **Import Key** («Импорт ключа») и **Import Communication Certificate** («Импорт сертификата связи») выберите тип сертификата и загрузите сертификат.
3. Нажмите **Import** («Импорт»).

Импорт сертификата СА

Перед началом

Заранее подготовьте сертификат СА.

Шаги

1. Перейдите **System and Maintenance** → **Safe** → **Certificate Management** («Система и обслуживание → Безопасность → Управление сертификатами»).
2. Создайте идентификатор в области **Import CA Certificate** («Импорт сертификата СА»).

Примечание

Идентификатор сертификата не может совпадать с идентификатором уже существующих сертификатов.

3. Загрузите файл сертификата с локального ПК.
4. Нажмите **Import** («Импорт»).

Раздел 11 Другие платформы

Также можно настроить устройство с помощью клиентского программного обеспечения iVMS-4200 или HikCentral Access Control. Подробная информация представлена в соответствующих руководствах.

Клиентское ПО iVMS-4200

Нажмите ссылку, чтобы просмотреть руководство пользователя клиентского программного обеспечения.

<http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247>

HikCentral Access Control (HCAC)

Нажмите ссылку, чтобы просмотреть руководство пользователя клиентского программного обеспечения.

<http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42>

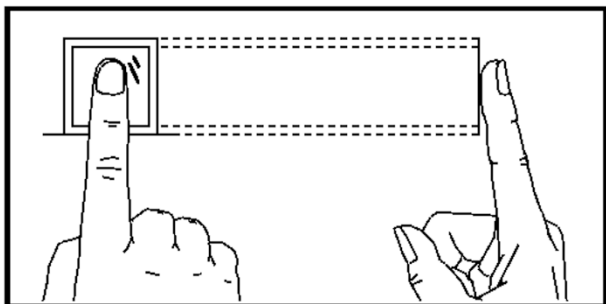
А. Рекомендации по сканированию отпечатков пальцев

Рекомендуемый палец

Рекомендуется использовать большой, указательный или средний палец.

Правильное сканирование

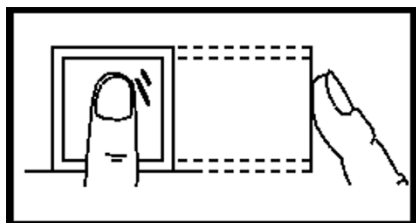
На рисунке ниже показан правильный способ сканирования пальца:



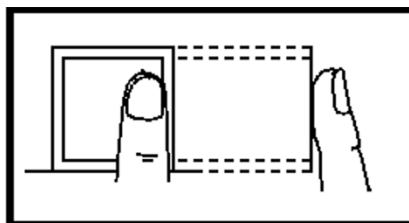
Палец необходимо прижать горизонтально к сканеру. Центр сканируемого пальца должен совпадать с центром сканера.

Неправильное сканирование

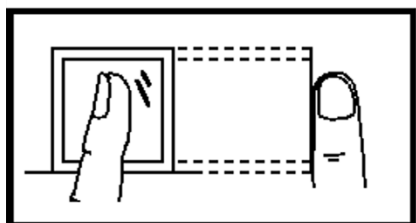
Приведенные ниже рисунки показывают неверные способы сканирования отпечатков пальцев:



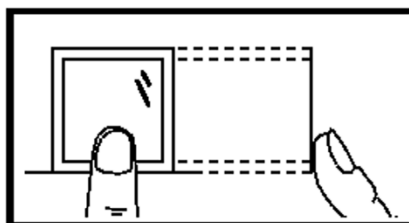
Vertical



Edge I



Side



Edge II

Окружающая среда

Не подвергайте сканер воздействию прямых солнечных лучей, высоких температур, влажных условий и дождя.

Когда палец сухой, сканер может не распознать отпечаток пальца. Можно подуть на палец и снова приложить его к сканеру.

Другое

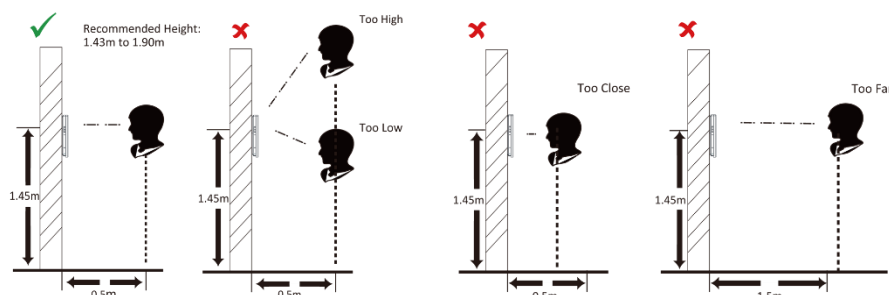
Если у вас неглубокий отпечаток пальца или его сложно сканировать, рекомендуется использовать другие методы аутентификации.

Если на сканируемом пальце есть травмы, сканер может его не распознать. Можно использовать другой палец и повторить попытку снова.

Б. Советы по сбору/сравнению изображений лиц

Положение при сборе или сравнении изображения лица:

Положения (рекомендуемое расстояние: 0.5 м)



Выражение лица

- Сохраняйте свое естественное выражение лица при сборе или сравнении изображений лиц, как это показано на рисунке ниже.



- Не надевайте шляпу, солнцезащитные очки или другие аксессуары, которые могут повлиять на функцию распознавания лиц.
- Убедитесь, что волосы не закрывают глаза, уши и т. д., также запрещается яркий макияж.

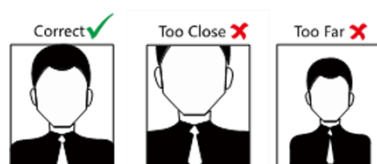
Положение лица

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



Размер

Убедитесь, что ваше лицо находится в середине окна сбора данных.



В. Рекомендации по среде установки

1. Номинальное значение освещенности источника света



Свеча: 10 лк

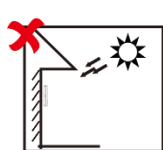


Лампа: 100 ~ 850 лк

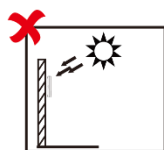


Солнечный свет: Свыше 1200 лк

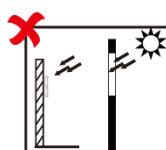
2. Избегайте засветки, а также воздействия прямых и отраженных солнечных лучей



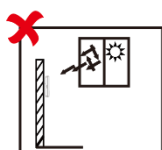
Backlight



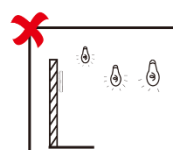
Direct Sunlight



Direct Sunlight
through Window



Indirect Light
through Window



Close to Light

Г. Размеры

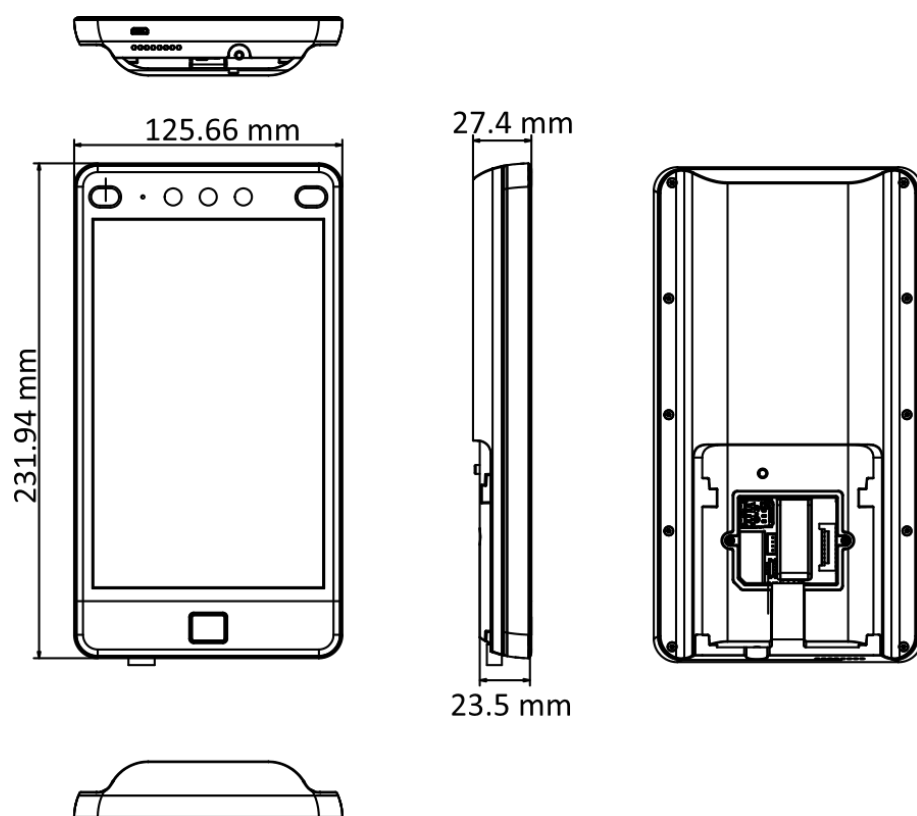


Рисунок Г-1. Размеры (ед. изм.: мм)

