



Терминал доступа F-KD-2405

Руководство пользователя

Правовая информация

Информация о документе

- Руководство содержит инструкции для использования и управления продуктом. Изображения, графики и вся другая информация предназначена только для ознакомления.
- Этот документ может быть изменен без уведомления, в связи с обновлением прошивки и по другим причинам. При использовании данного документа обращайтесь за помощью к профессионалам, обученным работе с продуктом.

О продукте

- Послепродажное обслуживание данного продукта возможно только в той стране или регионе, где была совершена покупка.
- Если выбранный вами продукт является видеопродуктом, сканируйте QR-код, чтобы ознакомиться с программой по использованию продукции видеомониторинга.

Признание прав интеллектуальной собственности

- iFLOW владеет авторскими правами и/или патентами, связанными с технологиями, реализуемыми в продукции и описанными в данном документе, которые могут включать лицензии, полученные от третьих лиц.
- Любая часть документа, включая текст, изображения, графику и т. д., принадлежит iFLOW. Никакая часть этого документа не может быть извлечена, скопирована, переведена или изменена полностью или частично любыми способами без письменного разрешения.
- Другие торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

Условные обозначения

В настоящем документе используются следующие символы.

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

Регулирующая информация

Информация о FCC

Обратите внимание, что изменения или модификации, не одобренные явно стороной, ответственной за соответствие, 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. Устройство должно выдерживать возможные излучения, включая и те, которые могут привести к выполнению нежелательных операций.

Соответствие стандартам ЕС



Данный продукт и (если применимо) поставляемые принадлежности отмечены знаком «СЕ» и, следовательно, согласованы с европейскими стандартами, перечисленными под директивой 2014/30/ЕС ЕМС, директивой 2011/65/ЕС



2012/19/ЕС (директива WEEE): продукты, отмеченные данным знаком, запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Для надлежащей утилизации верните продукт поставщику при покупке эквивалентного нового оборудования, либо избавьтесь от него в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info



2006/66/ЕС (директива о батареях): данный продукт содержит батарею, 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 предупреждений может привести к тяжелым травмам или смерти.

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

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

Предупреждения

- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в регионе эксплуатации.
- Используйте адаптер питания соответствующей компании. Потребляемая мощность не может быть меньше требуемого значения.
- Не подключайте несколько устройств к одному блоку питания, перегрузка адаптера может привести к перегреву или возгоранию.
- Прежде чем подключать, устанавливать или разбирать устройство, убедитесь, что питание отключено.
- Если устройство устанавливается на потолок или стену, убедитесь, что оно надежно закреплено.
- Если из устройства идет дым или доносится шум — отключите питание, извлеките кабель и свяжитесь с сервисным центром.
- Избегайте проглатывания батареи, существует опасность химического ожога. Данное устройство оснащено батареей таблеточного типа. Проглатывание батареи таблеточного типа может вызвать серьезные внутренние ожоги всего за 2 часа и привести к смерти.
Храните новые и использованные батареи в недоступном для детей месте. Если 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.
- Если продукт не работает должным образом, необходимо обратиться к дилеру или в ближайший сервисный центр. Не пытайтесь самостоятельно разобрать устройство. (Компания не несет ответственность за проблемы, вызванные несанкционированным ремонтом или техническим обслуживанием.)

Предостережения

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

Доступные модели

Доступны следующие модели терминала доступа с функцией считывания отпечатков:

Наименование	Модель	Беспроводное соединение
Терминал доступа	F-KD-2405SMK	Частота считывания карт 13.56 МГц
	F-KD-2405SMKBW	Частота считывания карт 13.56 МГц, Wi-Fi, Bluetooth
	F-KD-2405SMFKBW	Частота считывания карт 13.56 МГц, Wi-Fi, Bluetooth

Содержание

Раздел 1 Функции	1
Раздел 2 Внешний вид устройства.....	2
Раздел 3 Установка.....	5
3.1 Среда установки	5
3.2 Накладная установка	5
3.3 Врезная установка с монтажной коробкой	8
Раздел 4 Подключение устройства	14
4.1 Подключение внешних устройств	14
4.2 Подключение модуля безопасности двери	15
Раздел 5 Активация устройства	17
5.1 Активация через мобильный веб-интерфейс.....	17
5.2 Активация через веб-интерфейс	18
5.3 Активация через SADP	18
5.4 Активация устройства при помощи клиентского ПО iVMS-4200	20
Раздел 6 Аутентификация личности	21
6.1 Аутентификация с помощью одного типа учетных данных	21
6.2 Аутентификация с помощью нескольких типов учетных данных	21
Раздел 7 Быстрые операции через веб-интерфейс	22
7.1 Задание контрольного вопроса	22
7.2 Выбор языка	22
7.3 Настройки времени	22
7.4 Настройки учетной записи администратора	23
Глава 8 Работа через веб-интерфейс	24
8.1 Вход в систему.....	24
8.2 Забыть пароль	24

8.3 Обзор.....	24
8.4 Управление пользователями	26
8.5 Поиск событий.....	27
8.6 Настройка.....	27
8.6.1 Просмотр информации об устройстве	27
8.6.2 Настройка времени.....	28
8.6.3 Настройка перехода на летнее время (DST).....	28
8.6.4 Изменение пароля администратора.....	28
8.6.5 Настройки безопасности учетной записи	29
8.6.6 Онлайн пользователи.....	29
8.6.7 Просмотр информации о постановке / снятии с охраны	29
8.6.8 Настройка параметров сети.....	29
8.6.9 Привязка события	33
8.6.10 Настройки параметров контроля доступа.....	34
8.6.11 Настройки параметров карты.....	39
8.6.12 Настройка параметров конфиденциальности	40
8.6.14 Обновление и техническое обслуживание	40
8.6.15 Отладка устройства	41
8.6.16 Управление записями в журналах	42
8.6.17 Настройка режима безопасности	42
8.6.18 Управление сертификатами	42
Раздел 9 Настройка устройства через мобильный интерфейс.....	44
9.1 Вход в систему.....	44
9.2 Обзор.....	44
9.3 Забыть пароль	45
9.4 Настройка.....	45
9.4.1 Просмотр информации об устройстве	45
9.4.2 Настройки времени	45

9.4.3 Настройка перехода на летнее время (DST)	46
9.4.4 Управление пользователями	47
9.4.5 Настройка параметров сети	47
9.4.6 Управление пользователями	51
9.4.7 Поиск событий	53
9.4.8 Настройки параметров контроля доступа	53
9.4.9 Настройки параметров отпечатков пальцев	59
9.4.10 Обновление и техническое обслуживание	60
9.4.11 Просмотр документации онлайн	60
9.4.12 Просмотр лицензии на ПО с открытым исходным кодом	60
Раздел 10 Другие платформы	61
Приложение А. Рекомендации по сканированию отпечатков пальцев	62
Приложение В. Размеры	64

Раздел 1 Функции

- Высокий уровень защиты: IP65, IK08
- Тонкая гибкая металлическая конструкция
- Встроенный считыватель M1/EM-карт



Примечание

Поддержка M1-карт или EM-карт в зависимости от модели устройства.

- Управление с помощью мобильного приложения (Guarding Vision)
- Настройка точки доступа, настройка через веб-интерфейс ПК и мобильный веб-интерфейс



Примечание

Только устройство с функцией Wi-Fi поддерживает режим точки доступа.

- Несколько режимов аутентификации: карта, отпечаток пальца, PIN-код и Bluetooth



Примечание

Устройство должно поддерживать считывание отпечатков пальцев и Bluetooth.

Раздел 2 Внешний вид устройства

Подробная информация о терминале доступа представлена далее.

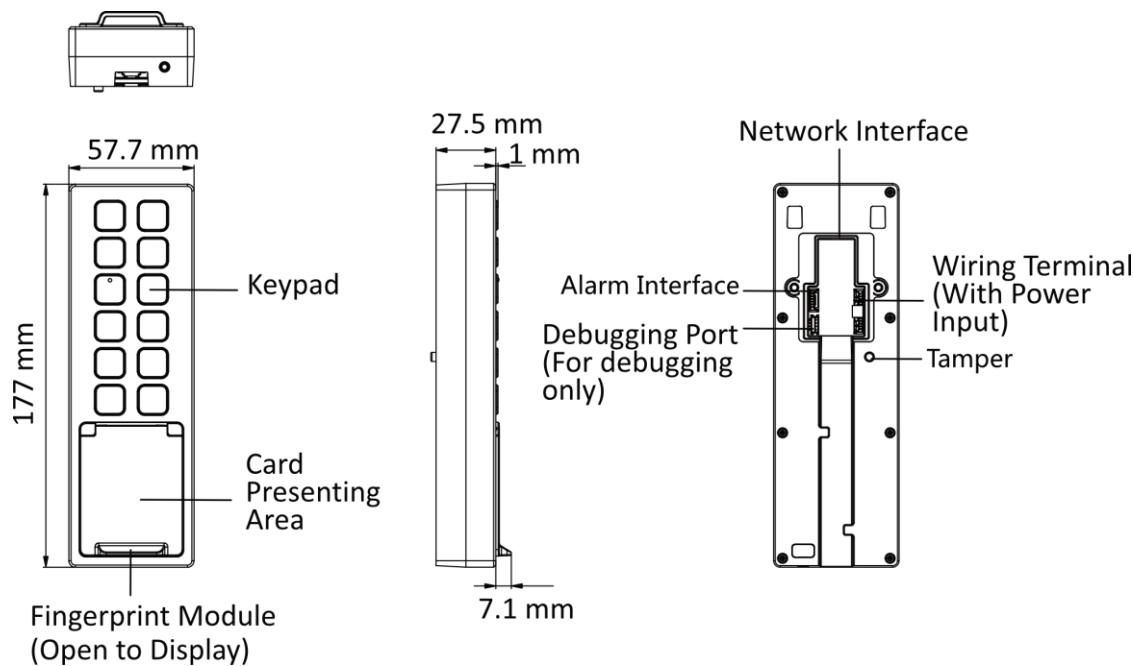


Рисунок 2-1. Терминал контроля доступа (отпечатки пальцев + карта)

Английский язык	Русский язык
Keypad	Клавиатура
Card Presenting Area	Область считывания карт
Fingerprint Module (open to display)	Модуль считывания отпечатков пальцев
Alarm Interface	Тревожный интерфейс
Debugging Port (for debugging only)	Порт отладки (только для отладки)
Network Interface	Сетевой интерфейс
Wiring Terminal (with Power Input)	Разъемы подключения (включая питание)
Tamper	Тампер

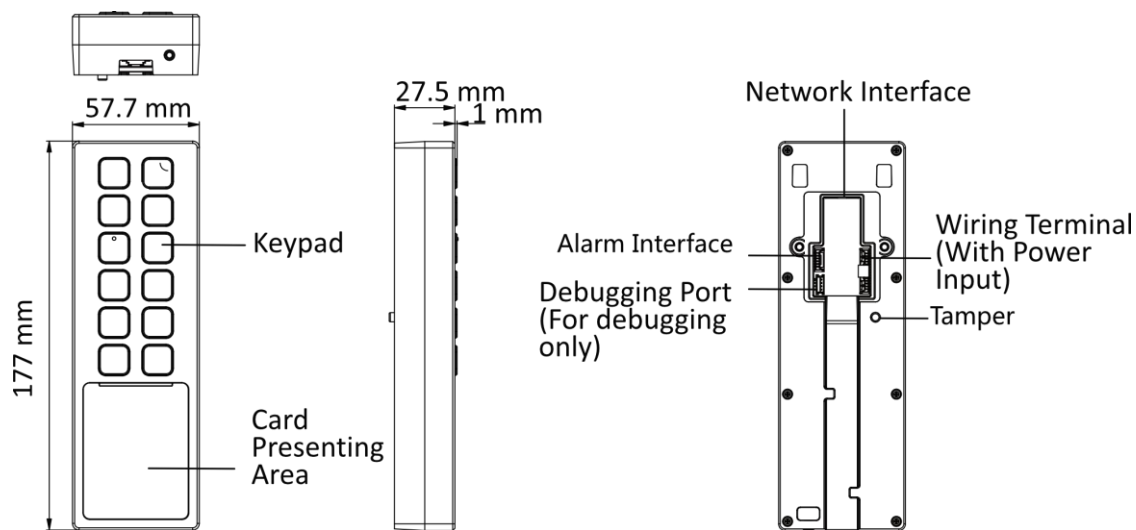


Рисунок 2-2. Терминал контроля доступа (карта)

Английский язык	Русский язык
Keypad	Клавиатура
Card Presenting Area	Область считывания карт
Alarm Interface	Тревожный интерфейс
Debugging Port (for debugging only)	Порт отладки (только для отладки)
Network Interface	Сетевой интерфейс
Wiring Terminal (with Power Input)	Разъемы подключения (включая питание)
Tamper	Тампер

 Примечание

Указанные изображения представлены исключительно в справочных целях.

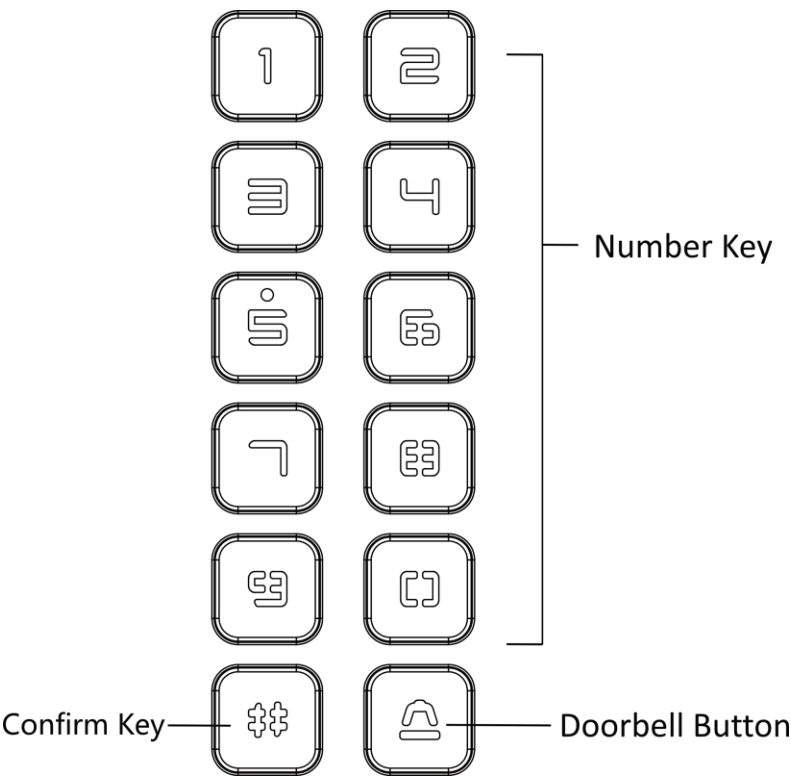


Рисунок 2-3. Клавиатура

Английский язык	Русский язык
Number Key	Кнопки цифр
Conform Key	Кнопка подтверждения
Doorbell Button	Кнопка дверного звонка

 Примечание

- Кнопка 5: удерживайте, чтобы включить режим точки доступа.
- #: Нажмите #, чтобы подтвердить ввод PIN-кода.

Раздел 3 Установка

3.1 Среда установки

Стена или другое место монтажа должно выдерживать массу втрое больше массы устройства.

3.2 Накладная установка

Шаги



Примечание

Дополнительная сила должна быть в три раза больше веса оборудования. При установке необходимо убедиться в надежной фиксации устройства и монтажной платы. После установки оборудование, включая любую соответствующую монтажную плату, не должно быть повреждено.

1. Закрепите монтажную плату на стене с помощью 4 прилагаемых винтов (SC-KA4X22).
Убедитесь, что кабели проходят через отверстие для кабеля.

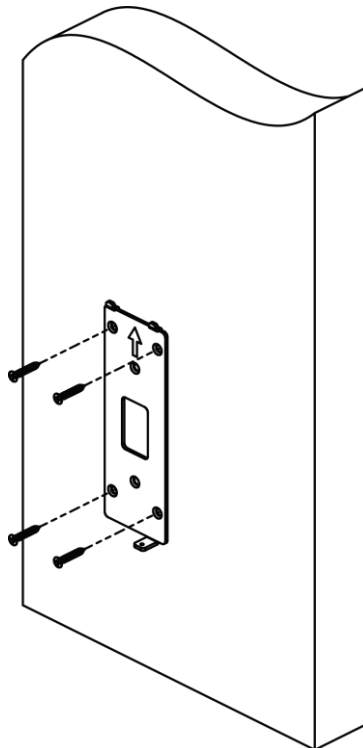


Рисунок 3-1. Установка монтажной платы

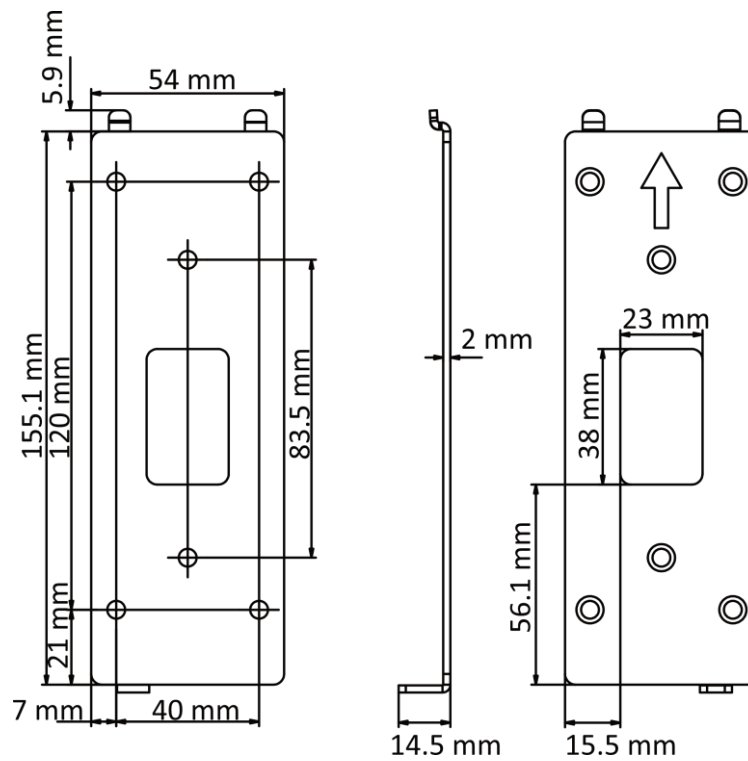


Рисунок 3-2. Размеры монтажной платы

2. Снимите заднюю панель, чтобы открыть зону проводки. Подключите кабели и установите заднюю панель обратно.

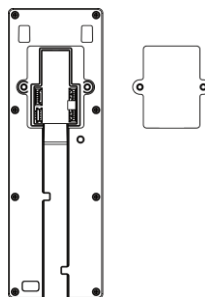


Рисунок 3-3. Снятие задней панели

Примечание

В зоне проводки кабеля необходимо нанести силиконовый герметик, чтобы предотвратить попадание воды в отверстия.

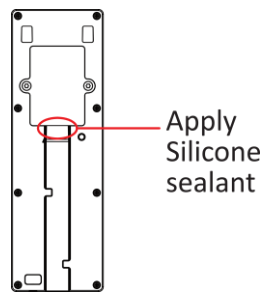


Рисунок 3-4. Фиксация силиконовым герметиком

-
- 3.** Выровняйте устройство и разместите его на монтажной плате.

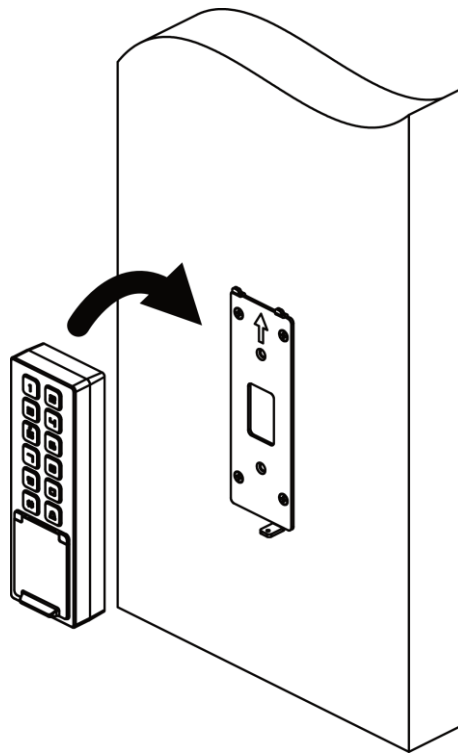


Рисунок 3-5. Выравнивание устройства

- 4.** Закрепите устройство и монтажную плату с помощью 1 винта (SC-KM3×8-T10-SUS-NL), поставляемого в комплекте.

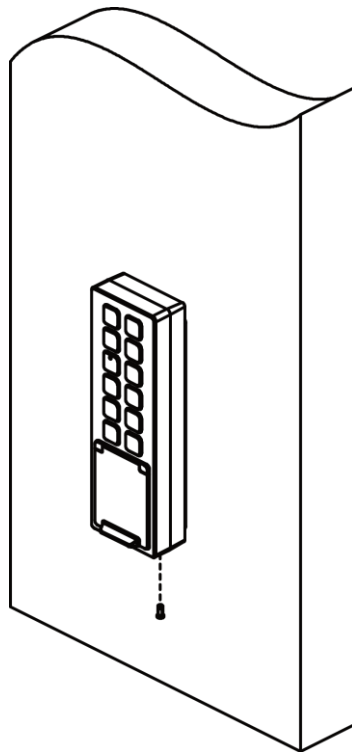


Рисунок 3-6. Фиксация устройства

3.3 Врезная установка с монтажной коробкой

Шаги



Примечание

Монтажная коробка не является обязательной. Приобретается отдельно.

1. Убедитесь, что монтажная коробка установлена на стене.

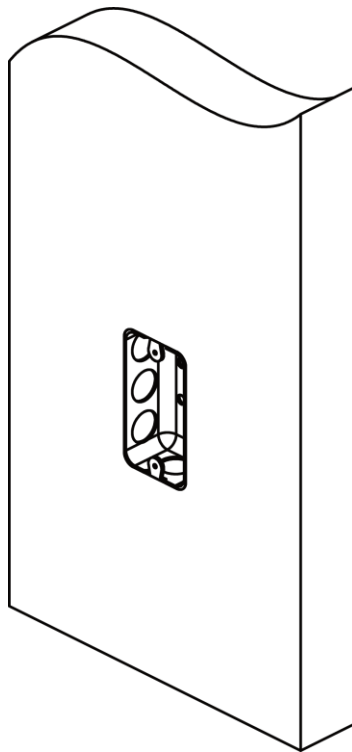


Рисунок 3-7. Размещение монтажной коробки на стене



Примечание

Монтажная коробка не входит в комплект поставки.

2. Закрепите монтажную плату на стене с помощью 4 прилагаемых винтов (SC-KA4X22).
Убедитесь, что кабели проходят через отверстие для кабеля.

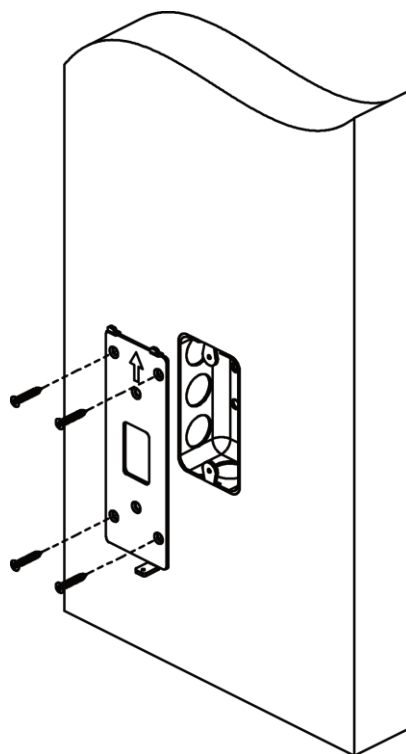


Рисунок 3-8. Установка монтажной платы

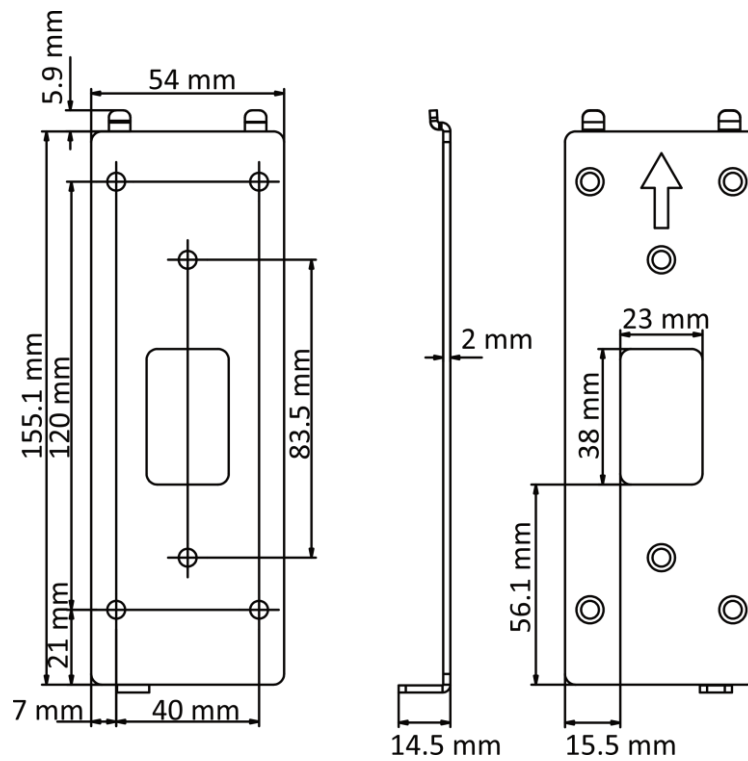


Рисунок 3-9. Размеры монтажной платы

3. Снимите заднюю панель, чтобы открыть зону проводки. Подключите кабели и установите заднюю панель обратно.

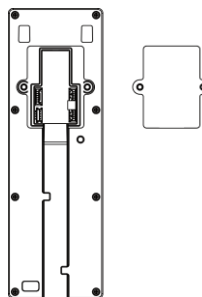


Рисунок 3-10. Снятие задней панели

Примечание

В зоне проводки кабеля необходимо нанести силиконовый герметик, чтобы предотвратить попадание воды в отверстия.

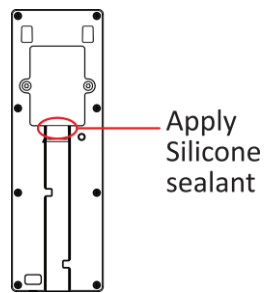


Рисунок 3-11. Фиксация силиконовым герметиком

-
- 4.** Выровняйте устройство и разместите его на монтажной плате.

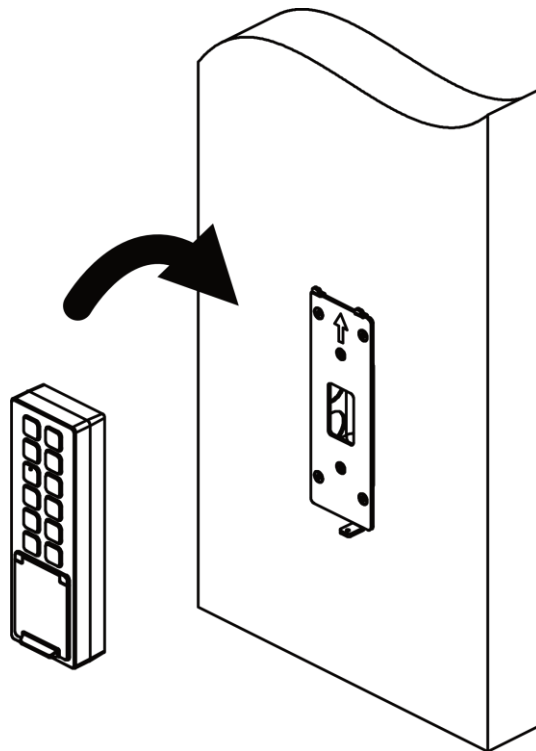


Рисунок 3-12. Выравнивание устройства

- 5.** Закрепите устройство на монтажной плате с помощью 4 установочных винтов (SC-KM3X8-T10-SUS-NL).

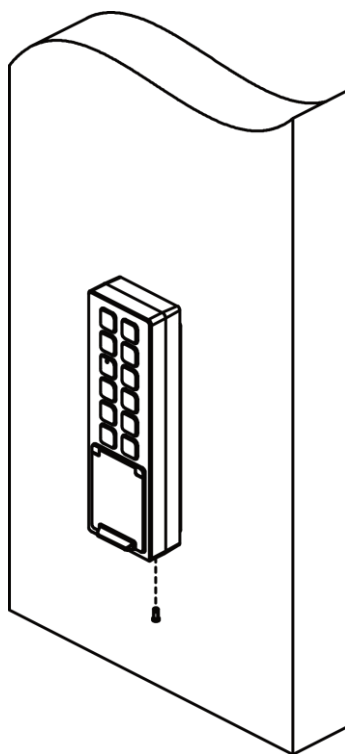


Рисунок 3-13. Фиксация устройства

Раздел 4 Подключение устройства

4.1 Подключение внешних устройств

Подключение внешнего устройства.
Ниже представлена схема подключения.

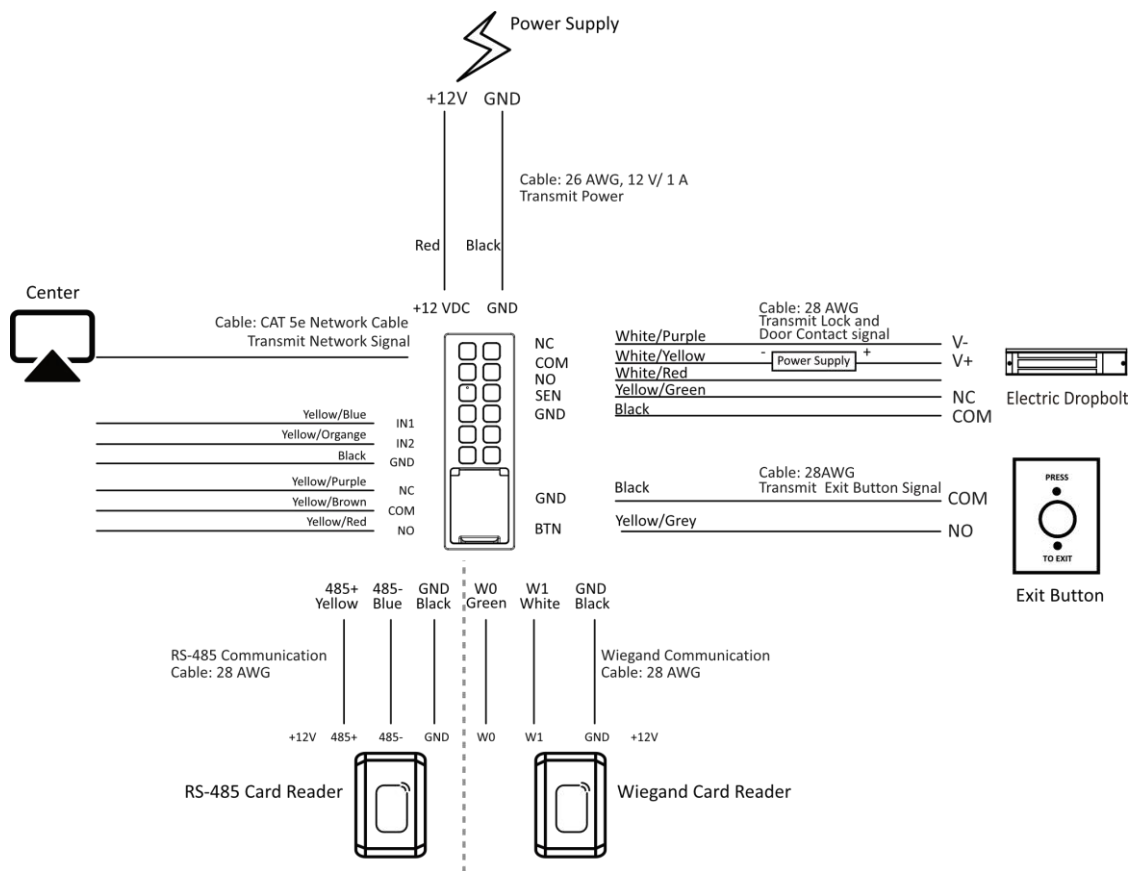


Рисунок 4-1. Подключение внешних устройств

Английский язык	Русский язык
Power Supply	Питание
Cable: 26 AWG, 12V/1A, Transmit Power	Кабель: 26 AWG, 12 В / 1 А, передача питания
Cable 5: CAT 5e Network Cable, Transmit Network Signal	Кабель 5: CAT 5e, передача сетевого сигнала
Cable: 28 AWG, Transmit Lock and Door Contact Signal	Кабель: 28 AWG, передача сигнала замка и дверного контакта
Cable: 28 AWG, Transmit Exit Button Signal	Кабель: 28 AWG, передача сигнала кнопки выхода
RS-485 Communication, Cable 28 AWG	Связь RS-485, кабель 28 AWG
Wiegand Communication, Cable 28 AWG	Связь Wiegand, кабель 28 AWG
Center	Центр

Electric Dropbolt	Электрическая защелка
Английский язык	Русский язык
Exit Button	Кнопка выхода
RS-485 Card Reader	Считыватель карт RS-485
Wiegand Card Reader	Считыватель карт Wiegand

**Примечание**

- При подключении дверного контакта и кнопки выхода устройство и считыватель карт RS-485 должны быть подключены к общему контуру заземления.
- При этом для терминала доступа с функцией распознавания лиц необходимо задать направление Wiegand на значение **Input** («Вход») для подключения к считывателю карт Wiegand. Если необходимо подключиться к контроллеру доступа, задайте направление Wiegand на значение **Output** («Выход») для передачи информации аутентификации в контроллере доступа.
- Подробная информация представлена в разделе **Настройка параметров интерфейса Wiegand**.
- Для устройства и дверного замка необходимы отдельные источники питания.
- Рекомендуемые параметры внешнего источника питания для дверного замка составляют 12 В, 1 А.
- Рекомендуемые параметры внешнего источника питания для считывателя карт Wiegand составляют 12 В, 1 А.
- Запрещено подключать устройство напрямую к электрической сети.

4.2 Подключение модуля безопасности двери

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

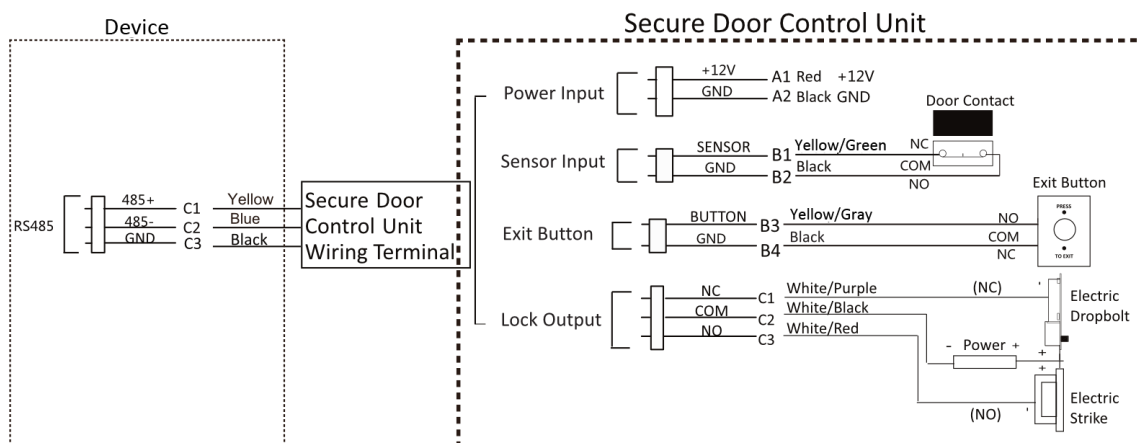


Рисунок 4-2. Подключение к модулю безопасности двери

Английский язык	Русский язык
Device	Устройство

Secure Door Control Unit Wiring Terminal	Подключение модуля безопасности двери
Английский язык	Русский язык
Secure Door Control Unit	Модуль безопасности двери
Power Input	Выход питания
Sensor Input	Выход датчика
Exit Button	Кнопка выхода
Lock Output	Выход замка
Door Contact	Дверной контакт
Exit Button	Кнопка выхода
Electric Dropbolt	Электрическая защелка
Electric Strike	Электромеханическая защелка



Примечание

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

Раздел 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: 80
- Имя пользователя по умолчанию: admin

5.1 Активация через мобильный веб-интерфейс

Можно активировать устройство через мобильный веб-интерфейс.

Шаги

Примечание

- После первого включения устройства функция точки доступа включается по умолчанию.
 - Только устройство с функцией Wi-Fi поддерживает активацию через режим точки доступа.
-

1. Подключитесь к точке доступа устройства с помощью мобильного телефона, введя пароль точки доступа. Откроется страница активации.
-

Примечание

- Если всплывающее окно не появилось автоматически. Введите IP-адрес устройства по умолчанию или введите www.acsvis.com в браузере, чтобы перейти на страницу активации.
 - Для неактивных устройств имя точки доступа устройства — AP_Serial Number, а пароль точки доступа — серийный номер устройства.
 - По умолчанию устройство находится в режиме точки доступа. Режим точки доступа будет отключен через 30 минут. Удерживайте кнопку 5 в течение 10 секунд, чтобы снова войти в режим точки доступа.
 - После активации устройства пароль точки доступа будет изменен на пароль активации устройства.
-

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

Примечание

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

Предостережения

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — для усиления защиты продукта 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 безопаснее.

3. Нажмите **Activate** («Активировать»).
4. Нажмите **Configuration → Communication Settings → Wi-Fi** («Настройки → Настройка связи → Wi-Fi») и подключитесь к сети Wi-Fi. Или измените IP-адрес через мобильный веб-интерфейс, веб-интерфейс ПК и клиентское программное обеспечение. Изменение IP-адреса устройства. IP-адрес можно редактировать с помощью инструмента SADP, ПК и клиентского программного обеспечения.

Дальнейшие шаги

Войдите в мобильную сеть, чтобы настроить параметры. Подробная информация представлена в разделе **Вход в систему**.

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** («Войти»).

Вход.



Примечание

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

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



Предостережение

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



Примечание

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

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

5.3 Активация через 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, установите ПО SADP согласно инструкции.
- Устройство и ПК, на котором запущено ПО SADP, должны находиться в одной подсети.

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

Шаги

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



Предостережения

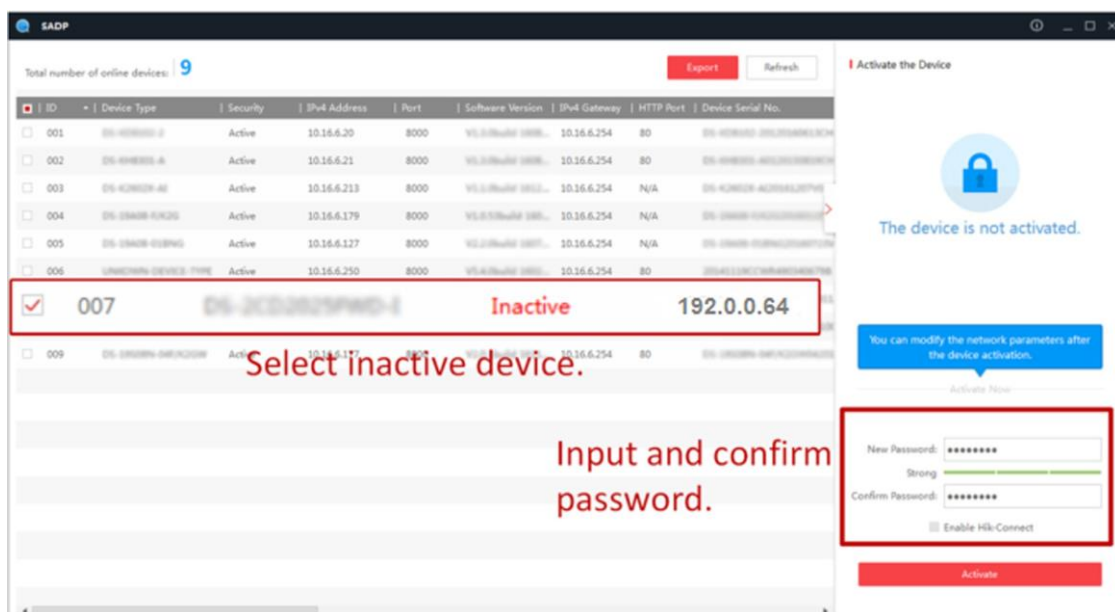
РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — настоятельно рекомендуется использовать надежный пароль (не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит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



Примечание

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

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



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

5. Измените IP-адрес устройства.
 - 1) Выберите устройство.

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

5.4 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 устройства»), чтобы отобразить область онлайн устройств. Искомые онлайн устройства отобразятся в списке.
4. Проверьте состояние устройства (отображено в столбце **Security Level** («Уровень безопасности»)) и выберите неактивное устройство.
5. Нажмите **Activate** («Активировать»), чтобы открыть окно активации.
6. Введите новый пароль в поле **Password** («Пароль») и подтвердите его в поле **Confirm Password** («Подтвердить пароль»).



Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая 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. Для активации устройства нажмите **ОК**.

Раздел 6 Аутентификация 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.

6.1 Аутентификация с помощью одного типа учетных данных

Перед аутентификацией установите тип аутентификации пользователя. Подробная информация представлена в разделе **Настройка режима аутентификации**.

Возможна аутентификация по отпечатку пальцев или карте.

Отпечаток пальца

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.

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

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. Выполните аутентификацию в соответствии с инструкциями на странице 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. Если аутентификация прошла успешно, на экране появится сообщение **Authenticated** («Личность установлена»).

Раздел 7 Быстрые операции через веб-интерфейс

7.1 Задание контрольного вопроса

Если вы забыли пароль активации устройства, можно изменить его с помощью контрольных вопросов и электронной почты. Настройте контрольные вопросы.

Нажмите  в верхнем правом углу веб-страницы для перехода на страницу **Change Password** («Изменить пароль»).

Проверка по контрольным вопросам

Ответьте на контрольные вопросы.

Подтверждение по электронной почте

1. Экспортируйте QR-код и отправьте его по адресу ***pw_recovery@hikvision.com*** 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. Затем нажмите **Next** («Далее»). Или нажмите **Skip** («Пропустить»), чтобы пропустить этот шаг.

7.2 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.

Нажмите **Next** («Далее»), чтобы завершить настройку.

7.3 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.

DST («Переход на летнее время»)

Включите DST. Установите время начала и окончания DST, а также смещение DST.

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

7.4 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 Card** («Добавить карту»), чтобы ввести номер карты и выбрать свойства карты.



Примечание

Поддерживается до 5 карт.

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



Примечание

Разрешено до 10 отпечатков пальцев.

4. Нажмите **Complete** («Завершить»).

Глава 8 Работа через веб-интерфейс

8.1 Вход в систему

В систему можно войти через веб-интерфейс.

Примечание

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

Вход в систему через веб-интерфейс

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

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

8.2 Забыть пароль

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

Примечание

Функция поддерживается, когда ПК / мобильный телефон находится в одном сегменте сети с устройством.

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 tech.support@iflow-tech.ru 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.

8.3 Обзор

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

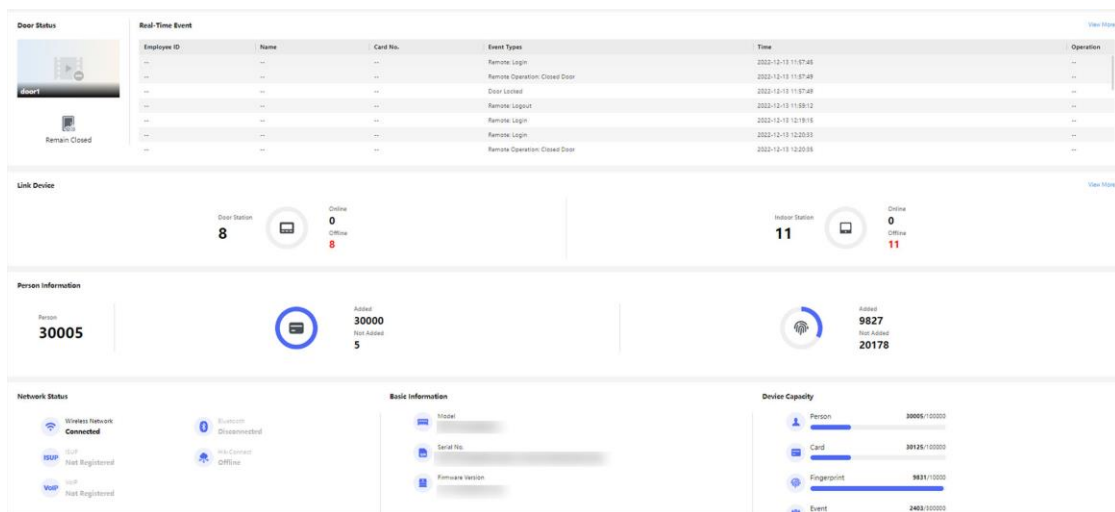


Рисунок 8-1. Страница обзора

Описание функций:

Операции для двери



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

Состояние двери

Настройка соответствующего состояния двери: открыта / закрыта / оставить открытой / оставить закрытой.

События в режиме реального времени

Можно просмотреть идентификатор сотрудника, имя, номер карты, тип события, время и операции. Можно нажать **View More** («Просмотреть больше») и ввести условия поиска, включая идентификатор сотрудника / посетителя, имя, номер карты, время начала и время окончания доступа, затем нажать **Search** («Поиск»). После этого на панели справа появятся результаты поиска.

Информация о пользователе

Можно просмотреть информацию о пользователе, карте и отпечатке пальца.

Состояние сети

Можно просмотреть состояние проводной сети, беспроводной сети, Bluetooth, ISUP и облачного сервиса.

Основная информация

Можно просмотреть модель, серийный номер и версию прошивки.

Емкость устройства

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



Примечание

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

Просмотреть больше

Можно нажать **View More** («Просмотреть больше»), чтобы узнать подробную информацию о событиях.

8.4 Управление пользователями

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

Установка длительности разрешения

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

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

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»), выберите **Property** («Свойство») и нажмите **Save** («Сохранить»), чтобы добавить карту. 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.

8.5 Поиск событий

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

Event Types						
Access Control Event						
Employee ID						
Name						
Card No.						
Start Time						
End Time						
2022-07-06 00:00:00						
2022-07-06 23:59:59						

No.	Employee ID	Name	Card No.	Event Types	Time	Operation
1	—	—	—	Device Powering On	2022-07-06 09:32:04.00.00	-
2	—	—	—	Door Locked	2022-07-06 09:32:04.00.00	-
3	—	—	—	Device Tampered	2022-07-06 09:32:07.00.00	-
4	—	—	—	Authentication via Fingerprint Failed	2022-07-06 09:32:21.00.00	-
5	—	—	—	The password mismatches.	2022-07-06 09:54:24.00.00	-
6	—	—	—	The password mismatches.	2022-07-06 10:04:54.00.00	-
7	—	—	—	Network Disconnected	2022-07-06 10:05:05.00.00	-
8	—	—	—	Network Recovered	2022-07-06 10:05:08.00.00	-
9	—	—	—	Local Login	2022-07-06 10:06:06.00.00	-
10	—	—	—	Remote Login	2022-07-06 10:07:21.00.00	-
11	—	—	—	Remote Login	2022-07-06 10:12:59.00.00	-
12	—	—	—	Remote Login	2022-07-06 10:14:59.00.00	-
13	—	—	—	Remote Login	2022-07-06 10:20:46.00.00	-
14	—	—	—	Remote Login	2022-07-06 10:25:39.00.00	-
15	—	—	—	Remote Login	2022-07-06 10:37:30.00.00	-
16	—	—	—	Local Login	2022-07-06 10:40:55.00.00	-
17	—	—	—	Remote Login	2022-07-06 10:47:01.00.00	-
18	—	—	—	Remote Login	2022-07-06 11:05:29.00.00	-

Рисунок 8-2. Поиск событий

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.

8.6 Настройка

8.6.1 Просмотр информации об устройстве

Просмотр названия устройства, языка, модели, серийного номера, версии, количества интерфейсов входа, количества интерфейсов выхода, RS-485, числа тревожных входов, числа тревожных выходов, емкости устройства и т. д.

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

Просмотр названия устройства, языка, модели, серийного номера, версии, количества интерфейсов входа, количества интерфейсов выхода, RS-485, числа тревожных входов, числа тревожных выходов, емкости устройства и т. д.

8.6.2 Настройка времени

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

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

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

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

NTP

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

Вручную

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

8.6.3 Настройка перехода на летнее время (DST)

Шаги

1. Нажмите **Configuration → System → System Settings → Time Settings** («Настройки → Система → Настройки системы → Настройки времени»).
2. Включите DST.
3. Установите время начала и окончания DST, а также смещение DST.
4. Нажмите **Save** («Сохранить») для сохранения настроек.

8.6.4 Изменение пароля администратора

Шаги

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



Предостережения

Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая 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.

8.6.5 Настройки безопасности учетной записи

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 **Configuration → System → User Management → Account Security Settings** («Настройки → Система → Управление пользователями → Настройки безопасности учетной записи»).
2. Установите контрольные вопросы и адрес электронной почты.
3. Введите пароль устройства и нажмите **ОК** для подтверждения изменений.

8.6.6 Онлайн пользователи

Отображается информация о пользователях, выполняющих вход в устройство.

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

8.6.7 Просмотр информации о постановке / снятии с охраны

Просмотр информации о постановке устройства на охрану и IP-адреса постановки на охрану.

Перейдите **Configuration → User Management → Arming/Disarming Information** («Настройки → Управление пользователями → Информация о постановке / снятии с охраны»).

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

8.6.8 Настройка параметров сети

Задайте параметры TCP/IP, порта, Wi-Fi, точки доступа, Bluetooth, ISUP и доступа к платформе.



Примечание

Некоторые модели устройств не поддерживают настройку Wi-Fi и мобильных данных. Настройка параметров зависит от фактического функционала устройства.

Настройка основных сетевых параметров

Нажмите **Configuration → Network → Network Settings → TCP/IP** («Настройки → Сеть → Настройки сети → 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 **Configuration**→ **Network** → **Network Settings** → **Wi-Fi** («Настройки → Сеть → Настройки сети → Wi-Fi»).



Рисунок 8-3 Страница настроек Wi-Fi

2. Нажмите **Wi-Fi** («Wi-Fi»).
3. Добавьте Wi-Fi.
- Нажмите **Manual Add** («Добавить вручную») и настройте SSID и режим безопасности.
4. Выберите Wi-Fi

- Нажмите **Connect** («Подключить») и введите пароль от Wi-Fi.
- Нажмите **Manual Add** («Добавить вручную») и настройте SSID и режим безопасности. Нажмите **OK**.

5. Опционально. Настройте параметры WLAN.

- 1) Установите IP-адрес, маску подсети и шлюз по умолчанию. Или включите DHCP, и система автоматически задаст IP-адрес, маску подсети и по умолчанию шлюз.

6. Нажмите **Save** («Сохранить»).

Точка доступа устройства

Настройте точку доступа устройства.

Нажмите **Configuration → Network → Network Settings → Device Hotspot** («Настройки → Сеть → Настройки сети → Точка доступа устройства»).

Нажмите **Enable Device Hotspot** («Включить точку доступа устройства»), чтобы включить функцию и просмотреть имя точки доступа устройства.

Примечание

По умолчанию именем точки доступа является серийный номер устройства.

Нажмите **Save** («Сохранить»).

Настройки Bluetooth

Можно включить функцию Bluetooth.

Нажмите **Configuration → Network → Network Settings → Bluetooth** («Настройки → Сеть → Настройки сети → Bluetooth»).

Доступность

Нажмите **Open** («Открыть»), чтобы включить функцию.

Имя устройства

Можно редактировать имя устройства, подключенного к Bluetooth.

Статус подключения

Можно просмотреть состояние подключения.

Открытие двери с помощью Bluetooth

После включения этой функции можно открывать двери через систему контроля доступа iFlow Central

Настройка параметров порта

Настройте параметры HTTP, HTTPS, прослушивания HTTP.

Нажмите **Configuration → Network → Network Service → HTTP(S)** («Настройка → Сеть → Настройка сети → HTTP(S)»).

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.

Прослушивание HTTP

Устройство может отправлять информацию о тревоге по IP-адресу или доменному имени по протоколу HTTP или HTTPS. Настраивайте IP-адрес или доменное имя, URL-адрес, порт, и протокол информации о тревоге.



Примечание

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

Доступ к платформе

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите **Configuration → Network → Device Access → Guarding Vision** («Настройки → Сеть → Доступ устройств → Guarding Vision») для перехода на страницу настроек.



Примечание

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

2. Поставьте **Enable** («Включить») для включения соответствующей функции.
3. **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 активации настроек.
-

Настройка параметров ISUP

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги



Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **Configuration → Network → Device Access → ISUP** («Настройка → 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»).

8.6.9 Привязка события

Настройте действия привязки для событий.

Шаги

1. Нажмите **Configuration → Event → Event Detection → Linkage Settings** («Настройки → События → Детекция события → Настройка события»), чтобы перейти на соответствующую страницу.
2. Настройте источник события.
 - При выборе **Event Linkage** («Привязка события»), как **Linkage Type** («Тип привязки»), из выпадающего списка выберите тип события.
 - При выборе **Card Linkage** («Привязка карты») в поле **Linkage Type** («Тип привязки») введите № карты и выберите считыватель карт.
 - При выборе **Employee ID Linkage** («Привязка ID сотрудника») в поле **Linkage Type** («Тип привязки») введите ID сотрудника и выберите считыватель карт.
3. Настройте действие привязки.

Привязка бипера

Включите **Buzzer Linkage** («Привязка бипера») и нажмите **Start Buzzing** («Запустить бипер») или **Stop Buzzing** («Остановить бипер»).

Привязка двери

Включите **Linked Door** («Привязанная дверь»), выберите **Door 1** или **Door 2** и настройте состояние двери для события.

Привязка тревожного выхода

Включите **Linked Alarm Output** («Привязанный тревожный выход»), выберите **Alarm Output 1** или **Alarm Output 2** и настройте состояние тревожного выхода для события.

**Примечание**

Для записи видео подключите к устройству SD-карту. Чтобы просмотреть записанное видео, обратитесь к разделу [Поиск события](#).

8.6.10 Настройки параметров контроля доступа

Настройка параметров аутентификации

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

**Примечание**

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

Terminal 1

Terminal Type Fingerprint/Face

Terminal Model

Enable Authentication Device ☒

Authentication Card or Face or Fingerprint

① Continuous Face Recognition ... 3

① Authentication Interval 0

① Alarm of Max. Failed Attempts ☐

Tampering Detection ☒

① Card No. Reversing ☐

Save

Рисунок 8-4. Настройка параметров аутентификации

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

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 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.

Связь с панелью управления

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

Максимальный интервал времени при вводе пароля

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

Правильная полярность светодиода / Ошибочная полярность светодиода

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

Включение тревоги тампера

Включите детектор саботажа на считывателе карт.

Включение считывания номера карты в обратной последовательности

После включения функции номер карты будет считываться в обратной последовательности.

Настройка параметров двери

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

Door No.

Door Name

Open Duration s

Door Open Timeout Alarm s

Door Magnetic Sensor Type ☒ Remain Closed ☐ Remain Open

Exit Button Type ☐ Remain Closed ☒ Remain Open

Door Lock Powering Off Status ☒ Remain Closed ☐ Remain Open

Extended Open Duration s

Door Remain Open Duration with ... min

Duress Code

Super Password

Save

Рисунок 8-5. Страница настроек параметров двери

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

Номер двери

Выберите устройство, соответствующее номеру двери.

Название

Можно задать имя двери.

Длительность открытого состояния

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

Тревога тайм-аута открытой двери

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

Дверной контакт

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

Тип кнопки выхода

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

Закрывание двери при отключении питания

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

Увеличение длительности открытого состояния

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

Дверь остается открытой после авторизации первого сотрудника

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

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.

Настройка параметров RS-485

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

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

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

№

Настройте номер RS-485.

Тип периферийного устройства

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



Примечание

После настройки и сохранения периферийного устройства устройство автоматически перезагрузится.

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 интерфейса Wiegand

Можно настроить направление передачи данных интерфейса Wiegand.

Шаги

Примечание

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

1. Нажмите **Configuration → Access Control → Wiegand Settings** («Настройки → Контроль доступа → Настройки Wiegand»).
2. Нажмите **Wiegand** («Wiegand»), чтобы включить функцию Wiegand.
3. Установите направление передачи данных.

Вход

Устройство можно подключать к считывателю карт Wiegand.

Выход

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

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

Примечание

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

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

Примечание

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

Настройка параметров терминала

Можно настроить параметры терминала для получения доступа.

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

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

8.6.11 Настройки параметров карты

Настройка параметров безопасности карты

Нажмите **Configuration → Card Settings → Card Type** («Настройка → Настройка параметров карты → Тип 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.

Сектор шифрования M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

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

Активация распознавания EM-карты

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



Примечание

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

Активация распознавания DESfire-карты

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

Настройка параметров аутентификации № карты

Настройте параметры карты при аутентификации через карту на устройстве.

Перейдите в **Configuration → Card Settings → Card No. Authentication Settings** («Настройки → Настройки карты → № карты → Настройка параметров аутентификации»). Выберите режим аутентификации по карте и нажмите **Save** («Сохранить»).

Полный номер карты

Будет прочитан полный номер карты.

Wiegand 26 (3 байта)

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

Wiegand 34 (4 байта)

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

8.6.12 Настройка параметров конфиденциальности

Задайте тип хранения событий.

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

Настройки хранения событий

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

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.

8.6.13 Настройка интеллектуальных параметров

Настройка основных параметров

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

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

8.6.14 Обновление и техническое обслуживание

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

Перезагрузка устройства

Нажмите **Maintenance and Security → Maintenance → Restart** («Техническое обслуживание и безопасность → Техническое обслуживание → Перезагрузка»). Нажмите **Restart** («Перезагрузка») для перезагрузки устройства.

Обновление

Нажмите **Maintenance and Security → Maintenance → Upgrade** («Техническое обслуживание и безопасность → Техническое обслуживание → Обновление»).

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

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



Примечание

- Не выключайте устройство во время обновления.
 - Можно нажать **Check for Updates** («Проверить наличие обновлений»), чтобы проверить наличие новой версии.
-

Восстановление параметров

Нажмите **Maintenance and Security → Maintenance → Backup and Reset** («Техническое обслуживание и безопасность → Техническое обслуживание → Резервное копирование и сброс»).

Восстановить все

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

Восстановить

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

Параметры импорта и экспорта

Нажмите **Maintenance and Security → Maintenance → Backup and Reset** («Техническое обслуживание и безопасность → Техническое обслуживание → Резервное копирование и сброс»).

Экспорт

Нажмите **Export** («Экспорт») для экспорта параметров устройства.



Примечание

Можно импортировать экспортированные параметры устройства на другое устройство.

Импорт

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

8.6.15 Отладка устройства

Можно настроить параметры отладки устройства.

Шаги

1. Нажмите **Maintenance and Security → Maintenance → Device Debugging** («Техническое обслуживание и безопасность → Техническое обслуживание → Отладка устройства»).
2. Можно настроить следующие параметры.

Включить SSH

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

8.6.16 Управление записями в журналах

Можно искать и просматривать журналы устройства.

Перейдите в **Maintenance and Security → Maintenance → Log** («Техническое обслуживание и безопасность → Техническое 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.

8.6.17 Настройка режима безопасности

Настройте режим безопасности для входа в клиентское ПО.

На странице Device for Management («Устройство для управления») **Maintenance and Security → Security → Security Service** («Техническое обслуживание и безопасность → Безопасность → Служба безопасности»).

Выберите режим безопасности и нажмите **Save** («Сохранить»).

Режим безопасности

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

Режим совместимости

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

8.6.18 Управление сертификатами

Помогает управлять сертификатами сервера/клиента и сертификатом CA.



Примечание

Данная функция поддерживается только у определенных моделей устройств.

Создание и установка самозаверенного сертификата

Шаги

1. Перейдите в меню **Maintenance and Security → Security → Certificate Management** («Техническое обслуживание и безопасность → 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 Passwords** («Импорт паролей»), выберите сертификат на локальном компьютере и нажмите **Install** («Установить»).
 - 2) Выберите тип сертификата в области **Import Communication Certificate** («Импорт сертификата связи»), затем выберите сертификат на локальном компьютере и нажмите **Install** («Установить»).

Установка другого авторизованного сертификата

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

Шаги

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

Установка сертификата СА

Перед началом

Заранее подготовьте сертификат СА.

Шаги

1. Перейдите в меню **Maintenance and Security → Security → Certificate Management** («Техническое обслуживание и безопасность → 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 **Install** («Установить»).

Раздел 9 Настройка устройства через мобильный интерфейс

9.1 Вход в систему

Войдите в мобильную интерфейс, чтобы настроить параметры.



Примечание

- Некоторые модели поддерживают настройку Wi-Fi.
 - Устройство должно быть активировано.
 - Убедитесь, что устройство и смартфон находятся в одном сегменте сети.
-

Подключите мобильный телефон и устройство к 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»).

Или удерживайте кнопку 5 в течение 10 секунд, чтобы войти в режим точки доступа. Войдите на страницу Wi-Fi с мобильного телефона. Выберите точку доступа устройства и введите пароль точки доступа (пароль активации). На мобильном телефоне автоматически откроется страница входа в систему. Устройство должно поддерживать данную функцию.

9.2 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 просмотреть состояние проводной сети, беспроводной сети, ISUP и Hik-Connect.

Основная информация

Можно просмотреть модель, серийный номер и версию прошивки.

9.3 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 tech.support@iflow-tech.ru 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.

9.4 Настройка

9.4.1 Просмотр информации об устройстве

Просмотр названия устройства, языка, модели, серийного номера, версии, количества каналов, количества интерфейсов входа, количества интерфейсов выхода, RS-485, числа тревожных входов, числа тревожных выходов, MAC-адреса, емкости устройства и т. д.

Нажмите  → **System Settings** → **Basic Information** («Настройки системы → Основная информация») для перехода на соответствующую страницу.

Просмотр названия устройства, языка, модели, серийного номера, версии, количества каналов, количества интерфейсов входа, количества интерфейсов выхода, RS-485, числа тревожных входов, числа тревожных выходов, MAC-адреса, емкости устройства и т. д.

9.4.2 Настройки времени

Установите часовой пояс, режим синхронизации времени и отображаемое время.

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

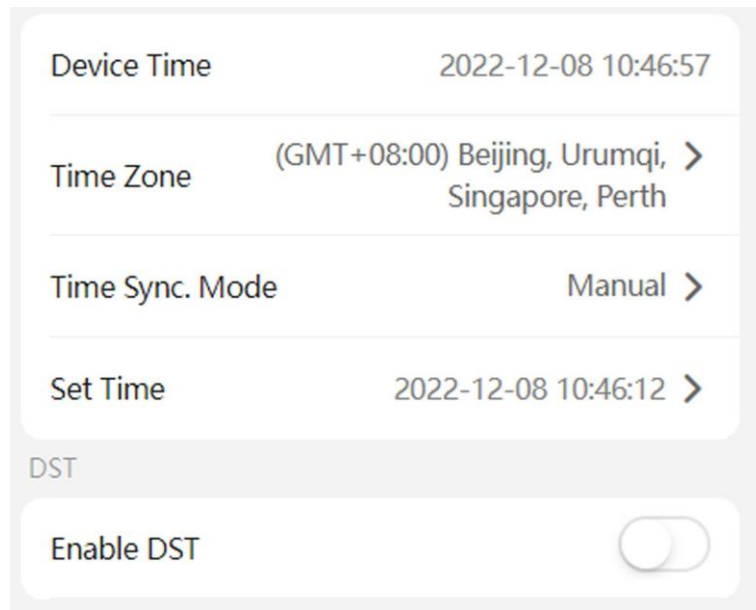


Рисунок 9-1 Настройка времени

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

Часовой пояс

Выберите часовой пояс, в котором находится устройство.

Синхронизация времени

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.

9.4.3 Настройка перехода на летнее время (DST)

Шаги

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

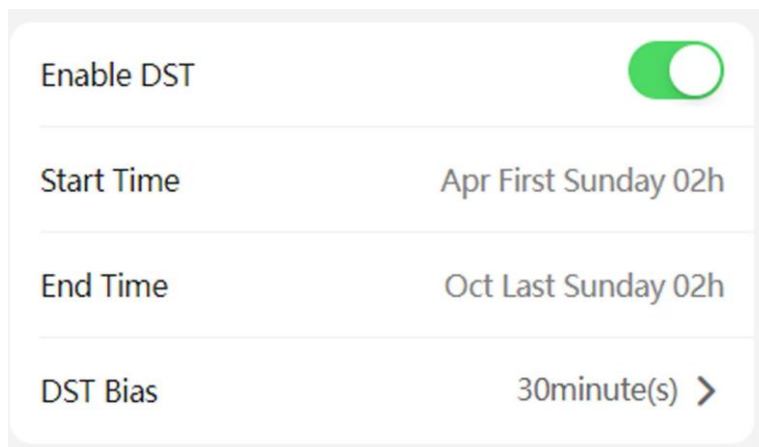


Рисунок 9-2. Летнее время

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

9.4.4 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.

9.4.5 Настройка параметров сети

Можно настроить проводную сеть, параметры Wi-Fi и порт устройства.

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**.

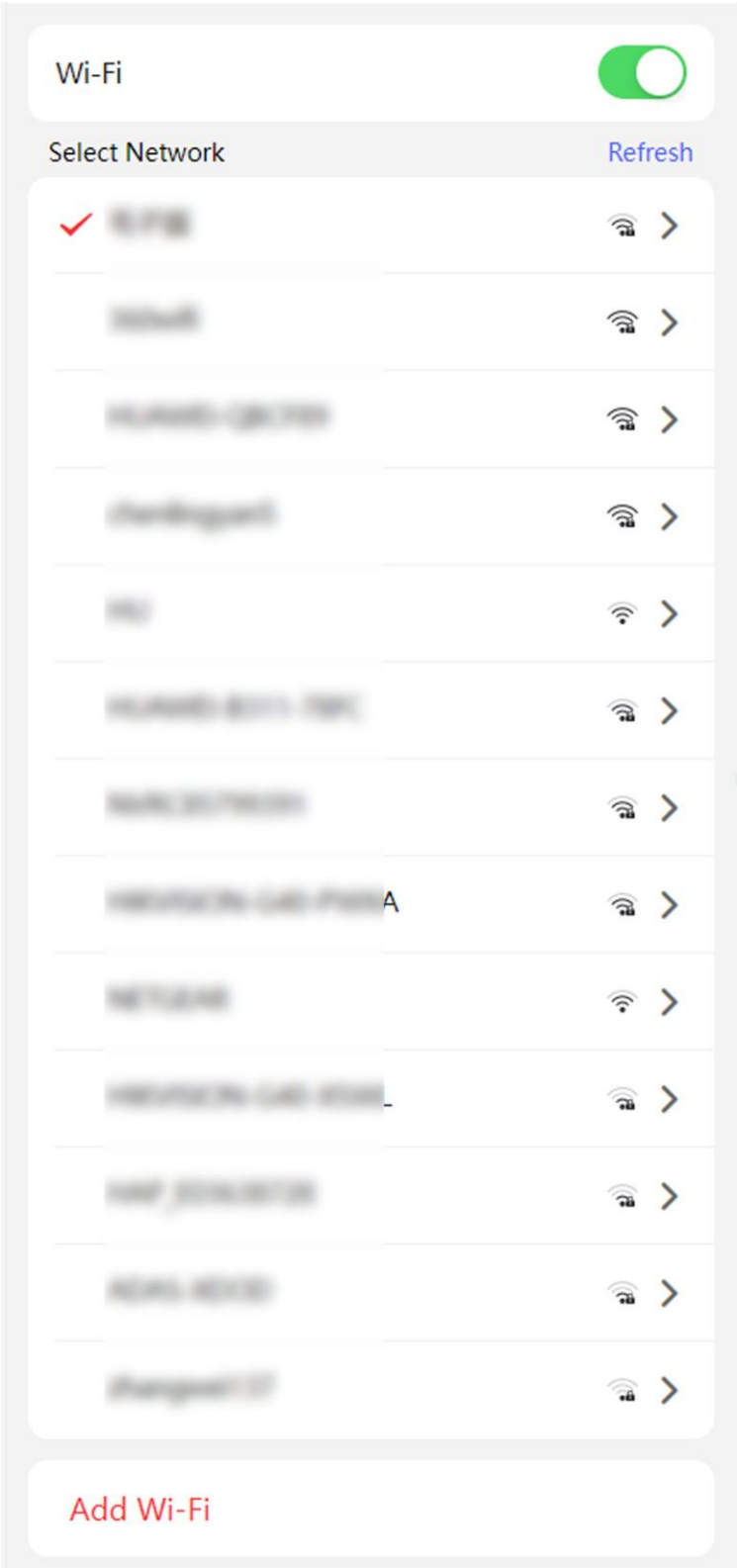


Рисунок 9-3. Wi-Fi

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 точки доступа устройства

Настройте точку доступа устройства, и мобильный телефон сможет подключиться к устройству для входа в мобильный браузер.

Шаги

1. Нажмите  → **Communication Settings** → **Device Hotspot** («Настройки связи → Точка доступа устройства»).
2. Можно включить точку доступа устройства и просмотреть имя точки доступа.



Примечание

По умолчанию именем точки доступа является серийный номер устройства.

3. 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** → **Guarding Vision** («Доступ устройств → Guarding Vision») для перехода на страницу настроек.



Примечание

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

2. Поставьте **Enable** («Включить») для включения соответствующей функции.
3. 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 просмотреть **Register Status** («Состояние регистрации») и **Binding Status** («Состояние привязки»).
5. Можно нажать **Bind An Account → View QR Code** («Привязка учетной записи → Просмотр QR-кода») и сканировать QR-код, чтобы привязать учетную запись.
6. Нажмите **Save** («Сохранить»), чтобы активировать 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, идентификатор устройства и код шифрования.



Примечание

Если выбрана версия 5.0, необходимо также установить ключ шифрования.

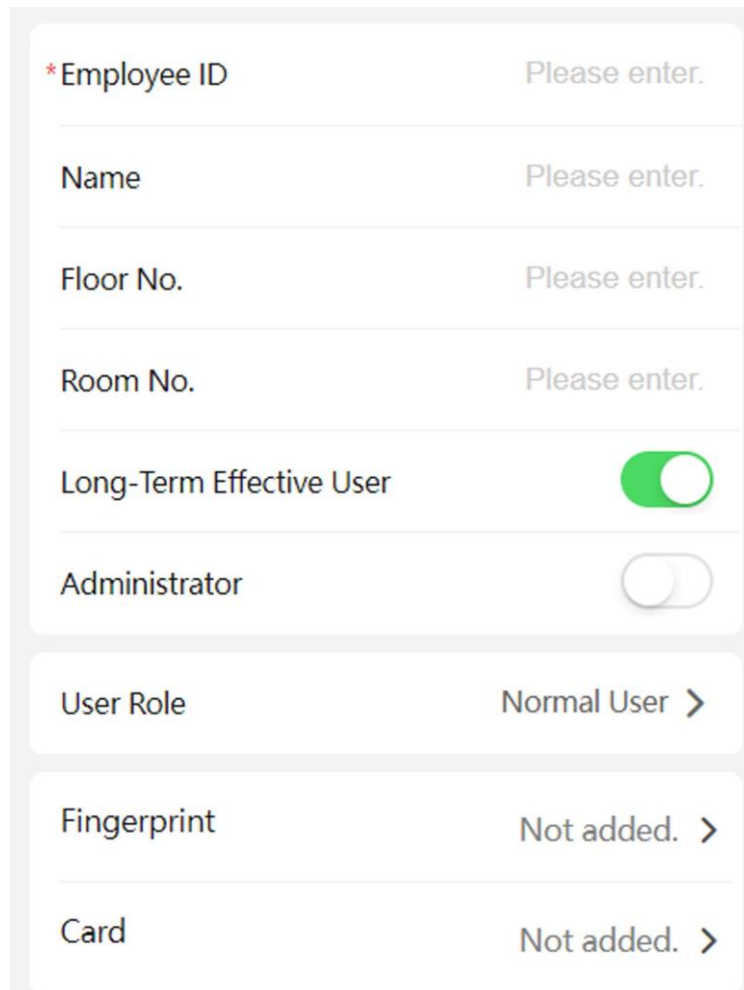
4. Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

9.4.6 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 +.



*Employee ID	Please enter.
Name	Please enter.
Floor No.	Please enter.
Room No.	Please enter.
Long-Term Effective User	☒
Administrator	☐
User Role	Normal User >
Fingerprint	Not added. >
Card	Not added. >

Рисунок 9-4. Добавление пользователя

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.

Администратор

Если пользователя нужно назначить в качестве администратора, включите **Administrator** («Администратор»).

Роль пользователя

Выберите роль пользователя.

Отпечаток пальца

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

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

9.4.7 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.

9.4.8 Настройки параметров контроля доступа

Настройка параметров аутентификации

Настройка параметров аутентификации.

Шаги

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

The screenshot displays a configuration menu for a terminal. The menu is organized into sections separated by light gray bars. The first section contains 'Terminal' (Main Card Reader >), 'Terminal Type' (FingerPrint/Card), 'Terminal Model' (BL-67700000000000000000), 'Enable Authentication Device' (toggle on), 'Authentication' (Fingerprint or Card >), 'Authentication Interval(s)' (0), 'Alarm of Max. Failed Attempts' (toggle off), 'Enable Tampering Detection' (toggle on), and 'Enable Card No. Reversing' (toggle off).

Terminal	Main Card Reader >
Terminal Type	FingerPrint/Card
Terminal Model	BL-67700000000000000000
Enable Authentication Device	☒
Authentication	Fingerprint or Card >
Authentication Interval(s)	0
Alarm of Max. Failed Attempts	☐
Enable Tampering Detection	☒
Enable Card No. Reversing	☐

Рисунок 9-5. Настройка аутентификации

2. Нажмите **Save** («Сохранить»).

Терминал

Выберите терминал для настройки.

Тип терминала / режим терминала

Получение описания терминалов. Доступны только для чтения.

Включить устройство с функцией аутентификации

Включить функцию аутентификации.

Authentication («Аутентификация»)

В выпадающем списке выберите режим аутентификации в соответствии с потребностями.

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 аутентификации / считывания карты

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

Включение тревоги тампера

Включите детектор саботажа на считывателе карт.

Включение считывания номера карты в обратной последовательности

После включения функции номер карты будет считываться в обратной последовательности.

Связь с контроллером

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

Максимальный интервал времени при вводе пароля

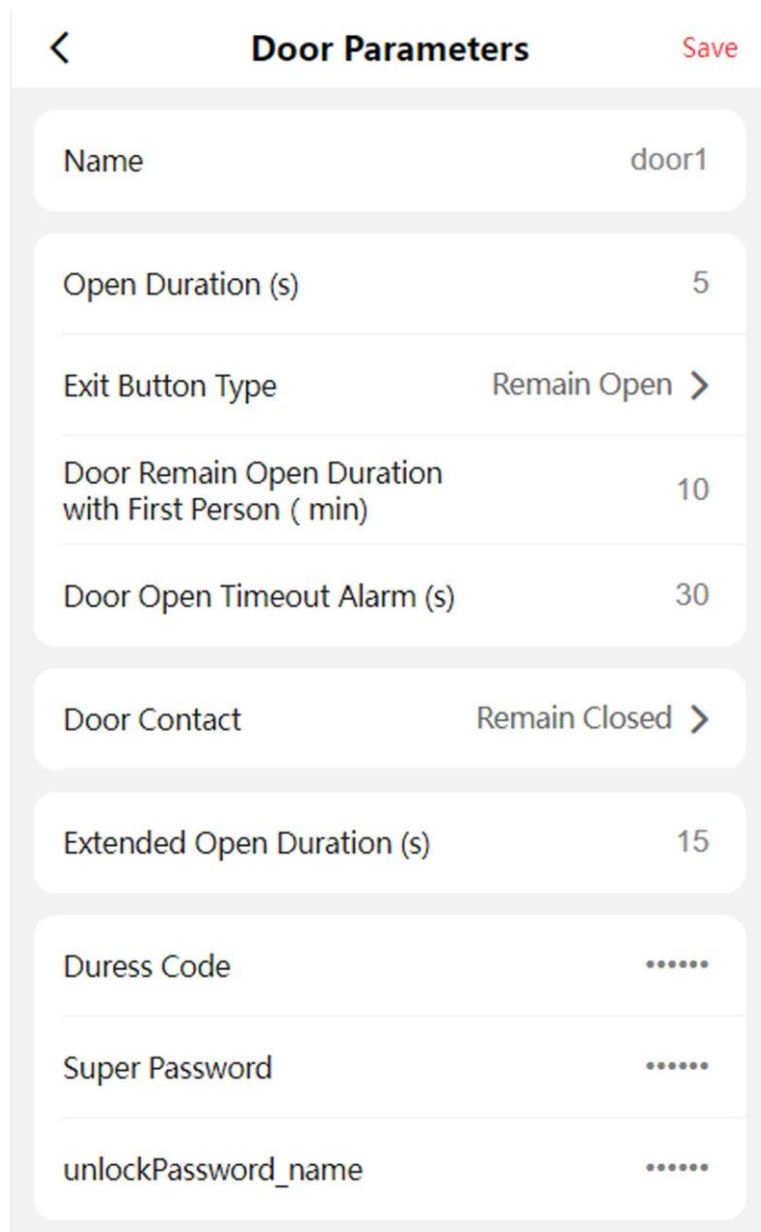
Если при вводе пароля в устройство для считывания карт интервал между нажатием двух цифр больше установленного значения, цифры, которые пользователь нажал до этого, будут автоматически удалены.

Правильная полярность светодиода / Ошибочная полярность светодиода

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

Настройка параметров двери

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



Door Parameters	
Name	door1
Open Duration (s)	5
Exit Button Type	Remain Open >
Door Remain Open Duration with First Person (min)	10
Door Open Timeout Alarm (s)	30
Door Contact	Remain Closed >
Extended Open Duration (s)	15
Duress Code	
Super Password	
unlockPassword_name	

Рисунок 9-6 Страница настроек параметров двери

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

Имя

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») в соответствии с необходимостью. 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»).

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.

Пароль разблокировки

Пользователь может открыть дверь с помощью пароля разблокировки.

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

Настройка параметров безопасности карты

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

Включение распознавания NFC-карты

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

Включение распознавания M1-карты

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

Сектор шифрования M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

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

Активация распознавания EM-карты

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



Примечание

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

Активация распознавания DESfire-карты

Устройство может считывать данные с DESfire-карты при включении функции CPU-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. Выберите из **Card Reader** («Считыватель карт»), **Extension Module** («Модуль расширения»), **Access Controller** («Контроллер доступа»).



Примечание

После настройки и сохранения периферийного устройства устройство автоматически перезагрузится.

Частный протокол

RS-485

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.

Тип выхода

Настройте тип выхода.

9.4.9 Настройки параметров отпечатков пальцев

Настройте уровень безопасности отпечатков пальцев. Нажмите → **Smart** («Интеллектуальные функции»).

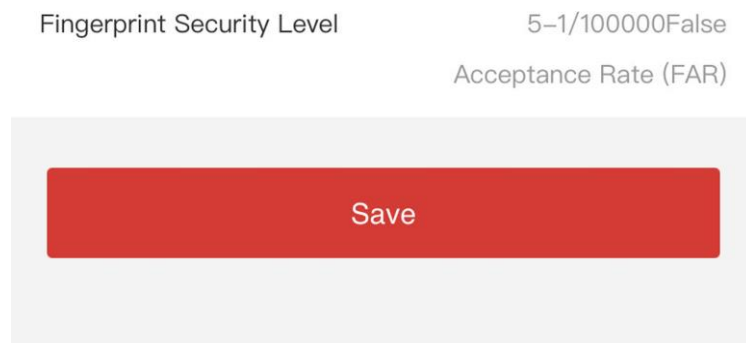


Рисунок 9-7. Уровень безопасности отпечатков пальцев



Примечание

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

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

9.4.10 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** («Обновить»).

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.

9.4.11 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.

9.4.12 Просмотр лицензии на ПО с открытым исходным кодом

Нажмите  → **Open Source Software License** («Лицензия на ПО с открытым исходным кодом»), чтобы просмотреть лицензию устройства.

Раздел 10 Другие платформы

Также можно настроить устройство с помощью клиентского программного обеспечения Guarding Vision for PC или iFlow Central.

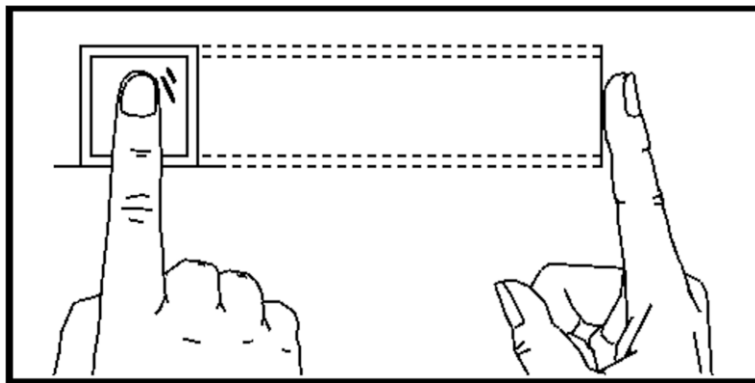
Приложение А. Рекомендации по сканированию отпечатков пальцев

Рекомендуемый палец

Рекомендуется использовать большой, указательный или средний палец.

Правильное сканирование

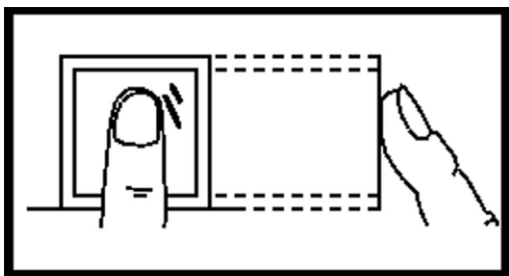
На рисунке ниже показан правильный способ сканирования пальца:



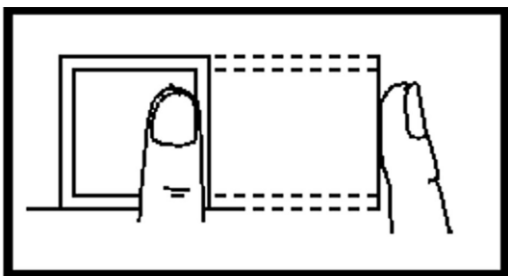
Вы должны прижать палец к сканеру горизонтально. Центр сканируемого пальца должен совпадать с центром сканера.

Неправильное сканирование

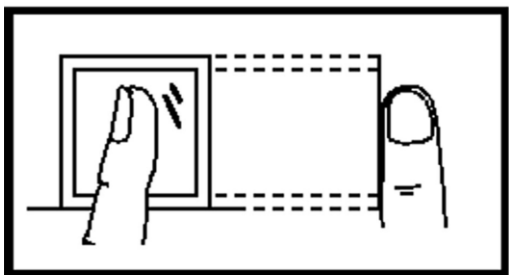
Приведенные ниже рисунки показывают неверные способы сканирования отпечатков пальцев:



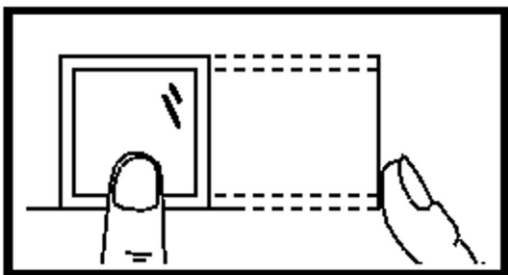
Vertical



Edge I



Side



Edge II

Английский язык	Русский язык
Vertical	Вертикально
Edge	Край
Side	Боковая поверхность

Окружающая среда

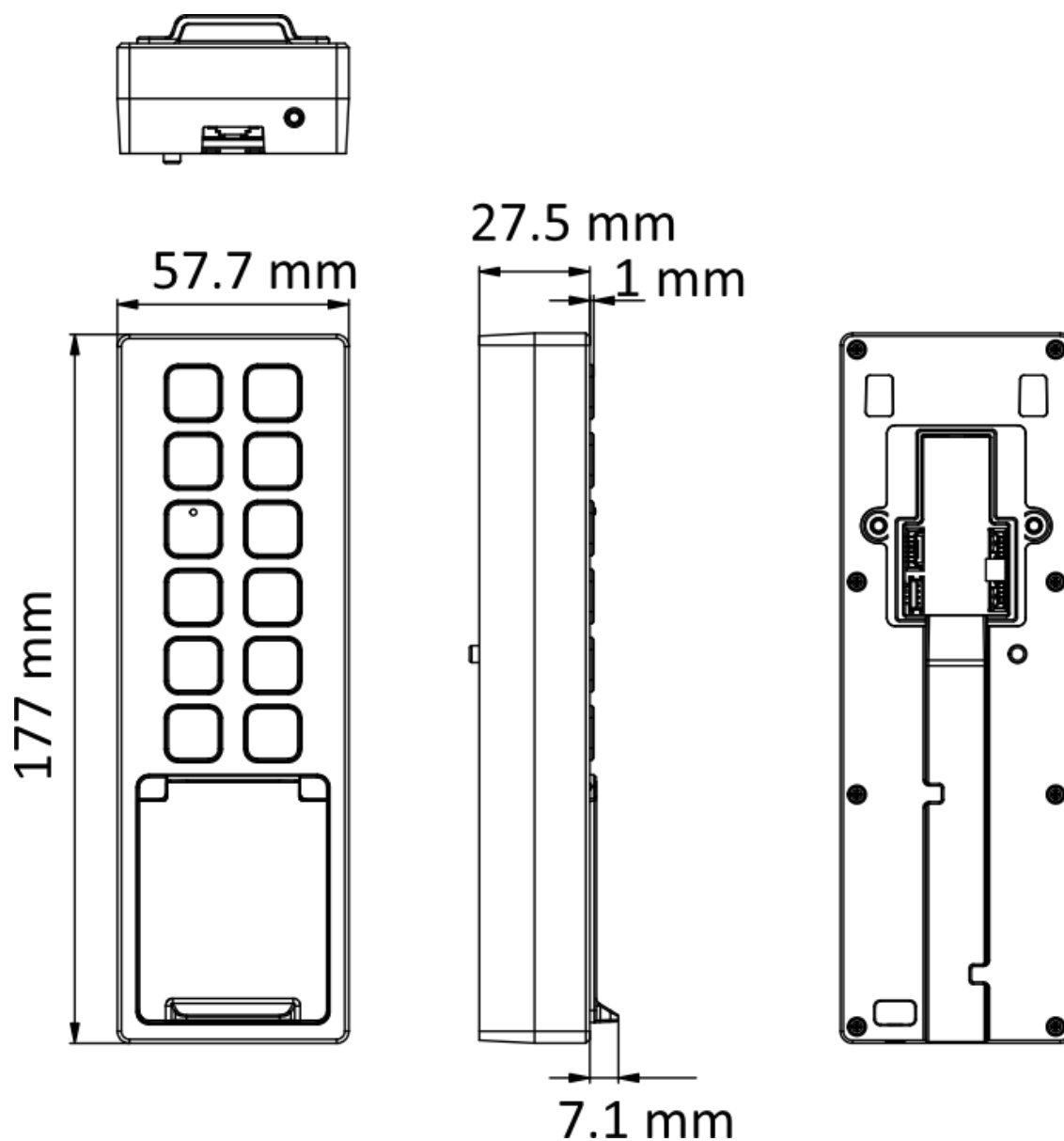
Не подвергайте сканер воздействию прямых солнечных лучей, высоких температур, влажных условий и дождя. Когда палец сухой, сканер может не распознать отпечаток пальца. Можно подуть на палец и снова приложить его к сканеру.

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.

Приложение В. Размеры

Размеры устройства (отпечаток пальца + карта)



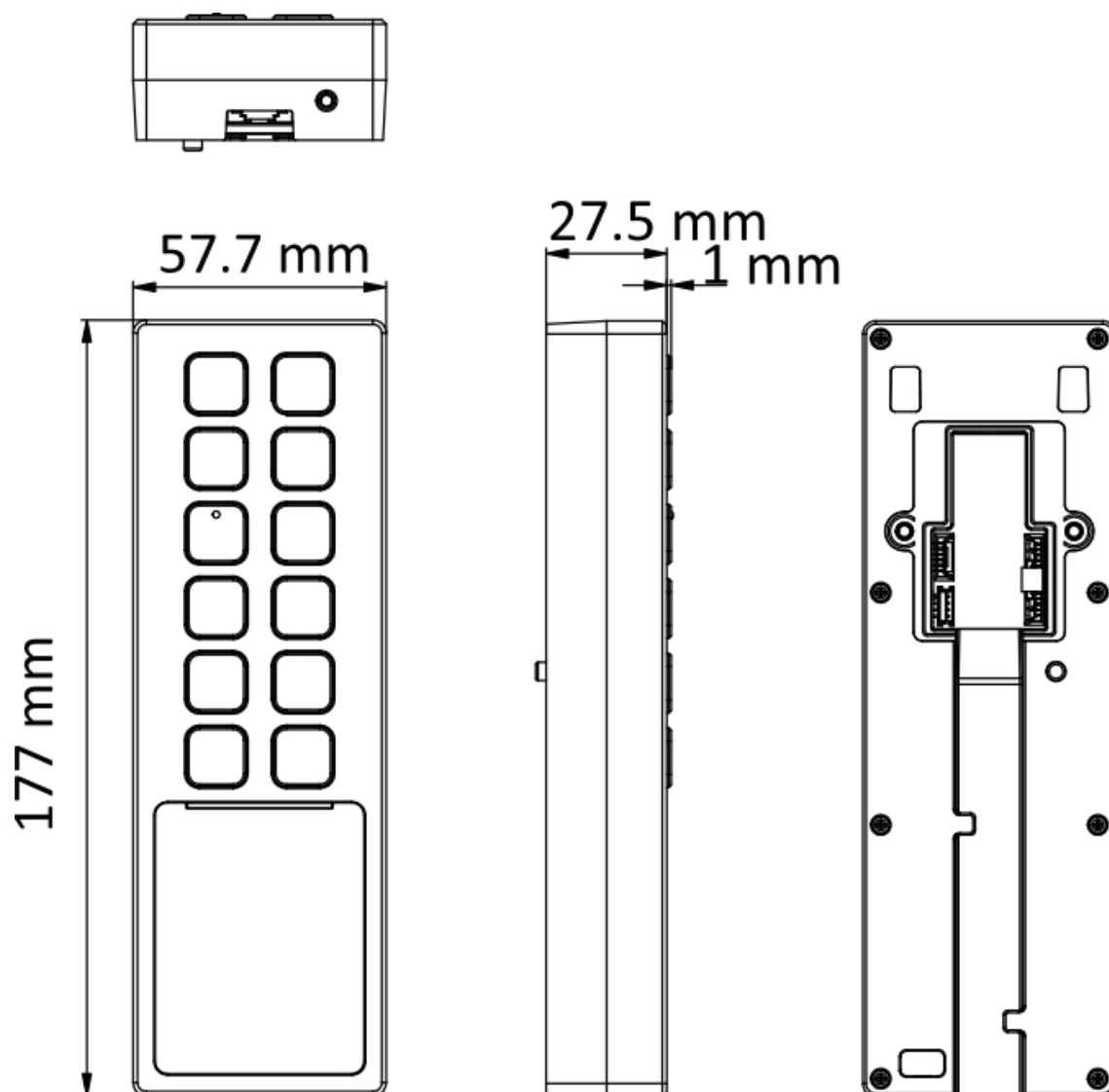


Рисунок В-1. Размеры устройства (карта)



Примечание

Указанные изображения представлены исключительно в справочных целях.

FLOW