Терминал доступа с функцией распознавания лиц F-KD-3313PMFCBWE1

Руководство пользователя

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 B, применительно к части 15 Правил FCC. Данный регламент разработан для того, чтобы обеспечить достаточную защиту от вредных помех, возникающих при использовании оборудования в коммерческой среде. Это оборудование генерирует, использует и может излучать радиоволны на разных частотах и, если устройство установлено и используется не в соответствии с инструкцией, оно может создавать помехи для радиосигналов. Тем не менее, нет никакой гарантии, что помехи не возникнут в каких-либо конкретных случаях установки. Если оборудование создает вредные помехи для приема радио- или телевизионных сигналов, что может быть определено путем включения и выключения оборудования, пользователю рекомендуется попытаться устранить помехи одним или несколькими способами, а именно:
— изменить ориентацию или местоположение приемной антенны;
— увеличить расстояние между оборудованием и приемником;
— подключить оборудование к розетке в цепи, отличной от той, к которой подключен приемник;
— обратиться к дилеру или опытному радио / телемастеру.
Данное оборудование следует устанавливать и использовать на расстоянии не менее 20 см между источником излучения и пользователем.
Условия FCC
Это устройство соответствует регламенту для цифрового устройства применительно к части 15 Правил FCC. Эксплуатация допускается при соблюдении следующих двух условий.
1. Данное устройство не должно создавать вредных помех.
2. Данное устройство должно выдерживать возможные помехи, включая те, которые могут привести к выполнению нежелательных операций.

Соответствие стандартам ЕС

CE

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



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



2006/66/EC (директива о батареях). Данный продукт оснащен батареей, которую запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Подробная информация о батарее изложена в документации продукта. Батарея отмечена значком, который может включать наименования, обозначающие содержание кадмия (Cd), свинца (Pb) или ртути (Hg). Для надлежащей утилизации возвратите батарею своему поставщику или утилизируйте ее в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: www.recyclethis.info

Инструкция по технике безопасности

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

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

⚠Предупреждения:

- Эксплуатация электронных устройств должна строго соответствовать правилам электробезопасности, противопожарной защиты и другим соответствующим нормам в регионе эксплуатации.
- 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

- 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.
- Биометрические системы аутентификации не могут гарантировать абсолютную защиту от подделки биометрических данных. Если требуется более высокий уровень безопасности, используйте несколько режимов аутентификации.

Доступные модели

Наименование продукта
Терминал доступа с функцией распознавания лиц

Содержание

Раздел 1 Внешний вид **1**

Раздел 2 Установка **3**

2.1 Среда установки 3

2.2 Накладная установка 3

Раздел 3 Подключение **7**

3.1 Описание разъемов 7

Раздел 4 Активация **8**

4.1 Активация через мобильный веб-интерфейс 8

4.2 Активация через веб-интерфейс 9

4.3 Активация через ПО SADP 9

4.4 Активация устройства через клиентское программное обеспечение Guarding Vision 10

Раздел 5 Настройка устройства через мобильный веб-интерфейс **12**

5.1 Вход в систему 12

5.2 Обзор 12

5.3 Забыть пароль 13

5.4 Настройка 13

5.4.1 Просмотр информации об устройстве 13

5.4.2 Настройка времени 13

5.4.3 Настройка параметров перехода на летнее время 14

5.4.4 Управление пользователями 15

5.4.5 Настройка сетевых параметров 15

5.4.6 Управление пользователями 19

5.4.7 Поиск событий 21

5.4.8 Настройки параметров контроля доступа 21

5.4.9 Настройка видеодомофонии 24

5.4.10 Настройки параметров аудио 27

5.4.11 Настройки параметров лица 27

5.4.12 Обновление и техническое обслуживание 29

5.4.13 Просмотр документации онлайн 29
5.4.14 Просмотр лицензии на ПО с открытым исходным кодом 30
Раздел 6 Работа через веб-интерфейс **31**
6.1 Вход с систему 31
6.2 Забыть пароль 31
6.3 Загрузка веб-плагина 32
6.4 Помощь 32
6.4.1 Лицензии на ПО с открытым исходным кодом 32
6.4.2 Просмотр онлайн справки 32
6.5 Выход из системы 32
6.6 Быстрые операции через веб-интерфейс 32
6.6.1 Изменение пароля 32
6.6.2 Выбор языка 33
6.6.3 Настройки времени 33
6.6.4 Настройки конфиденциальности 34
6.6.5 Настройки учетной записи администратора 35
6.6.6 Настройка номеров и сетевые настройки 35
6.7 Управление пользователями 37
6.8 Управление устройством 39
6.9 Управление контролем доступа 39
6.9.1 Обзор 39
6.9.2 Поиск событий 41
6.9.3 Конфигурация параметров двери 41
6.9.4 Настройки параметров аутентификации 44
6.9.5 Настройка параметров распознавания лиц 48
6.9.6 Настройки параметров карты 51
6.9.7 Настройки привязки 53
6.9.8 Настройка рабочего режима через веб-интерфейс ПК 54
6.9.9 Настройка удаленной проверки 54
6.9.10 Настройки конфиденциальности 55
6.9.11 Настройки вызова 57

6.10 Конфигурация системы 60
6.10.1 Просмотр информации об устройстве через веб-интерфейс ПК 60
6.10.2 Настройка времени 61
6.10.3 Изменение пароля администратора 62
6.10.4 Настройки безопасности учетной записи через веб-интерфейс ПК 62
6.10.5 Просмотр информации о постановке / снятии устройства с охраны через веб-интерфейс ПК 63
6.10.6 Параметры сети 63
7.10.7 Настройка параметров видео и аудио через веб-интерфейс ПК 68
6.10.8 Настройка параметров изображения 68
6.10.9 Конфигурация доступа 70
6.10.10 Настройки учета рабочего времени (УРВ) 71
6.11 Пользовательские настройки 73
6.11.1 Настройка спящего режима через веб-интерфейс ПК 73
6.11.2 Настройка панели аутентификации через веб-интерфейс ПК 74
6.11.3 Настройка отображения уведомлений через веб-интерфейс ПК 74
6.11.4 Настройка голосовых подсказок через веб-интерфейс ПК 75
6.11.5 Настройка текста результата аутентификации через веб-интерфейс ПК 75
6.12 Система и обслуживание 76
6.12.1 Перезагрузка 76
6.12.2 Обновление 76
6.12.3 Восстановление настроек 76
6.12.4 Экспорт параметров устройства через веб-интерфейс ПК 77
6.12.5 Импорт параметров устройства через веб-интерфейс ПК 77
6.12.6 Отладка устройства 78
6.12.7 Просмотр журнала через веб-интерфейс ПК 80
6.12.8 Расширенные настройки через веб-интерфейс ПК 81
6.12.9 Управление безопасностью 81
6.12.10 Управление сертификатами 82

A. Условные обозначения 86

B. Советы по сканированию отпечатков пальцев 87

C. Советы по сбору / сравнению изображений лиц 89

D. Рекомендации по среде установки 91

E. Размеры 92

Раздел 1 Внешний вид

Подробная информация о терминале доступа с функцией распознавания лиц представлена далее.

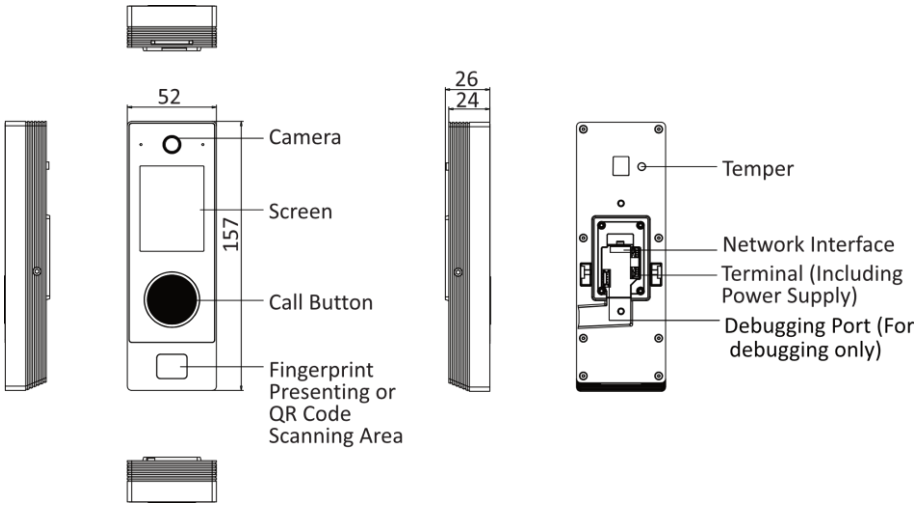


Рисунок 1-1. Внешний вид 1

Английский язык	**Русский язык**
Camera	Камера
Screen	Экран
Call button	Кнопка вызова
Fingerprint Presenting or QR Code Scanning Area	Область считывания отпечатка пальца или сканирования QR-кода
Tamper	Тампер
Network Interface	Сетевой интерфейс
Debugging Port (for debugging only)	Порт отладки (только для отладки)
Terminal (Including Power Supply)	Разъем подключения (включая питание)

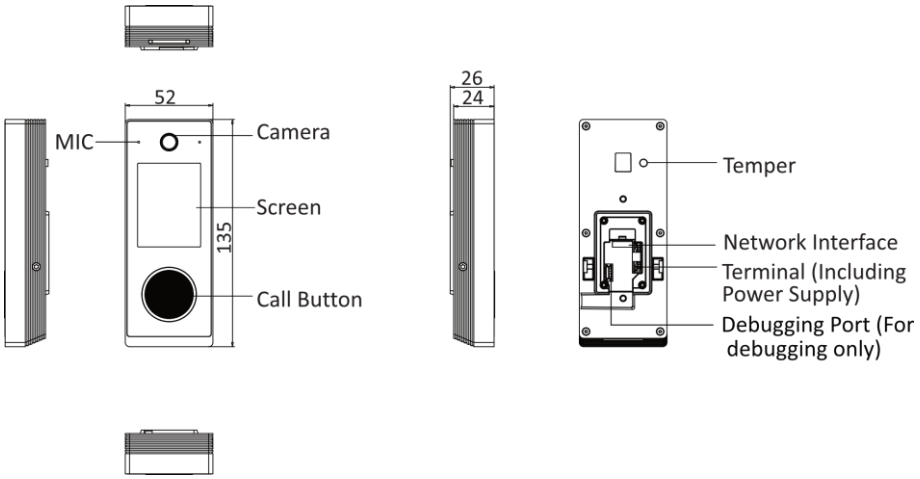


Рисунок 1-2. Внешний вид 2

Английский язык	**Русский язык**
Camera	Камера
Screen	Экран
MIC	Микрофон
Call button	Кнопка вызова
Tamper	Тампер
Network Interface	Сетевой интерфейс
Debugging Port (for debugging only)	Порт отладки (только для отладки)
Terminal (Including Power Supply)	Разъем подключения (включая питание)

Раздел 2 Установка

2.1 Среда установки

- Стена или другое место монтажа должно выдерживать массу втрое больше массы устройства.
- Подготовьте следующие инструменты и принадлежности: отвертку (приобретается самостоятельно), винты, кабели и адаптеры (приобретается самостоятельно).

2.2 Накладная установка

Шаги

1. Проложите кабели через отверстие.

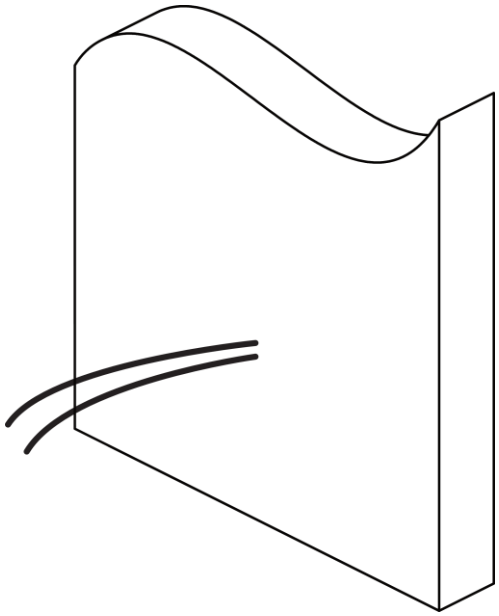


Рисунок 2-1. Прокладка кабелей

2. Закрепите монтажную плату на монтажной коробке с помощью двух винтов (SC-KA4×25), входящих в комплект поставки.

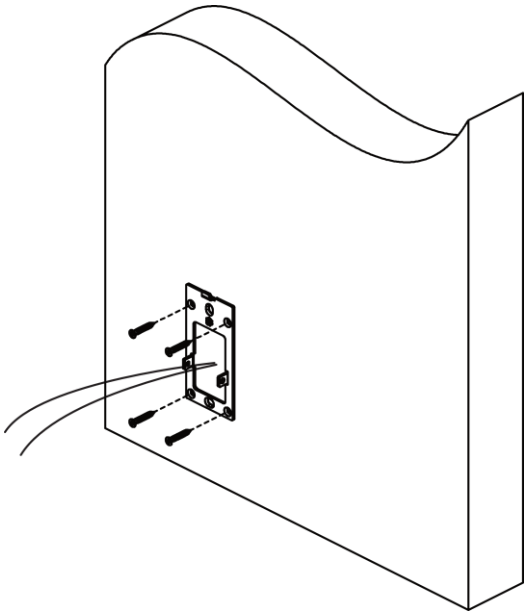


Рисунок 2-2. Фиксация монтажной платы

3. С помощью отвертки ослабьте винты на задней крышке устройства и снимите заднюю крышку.

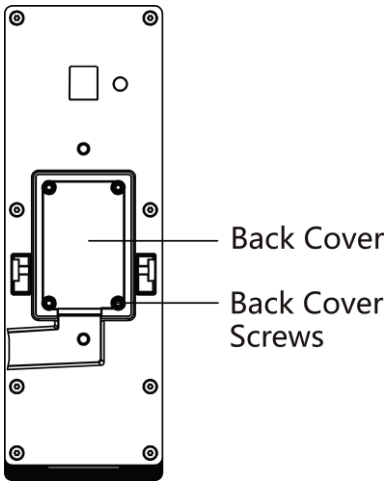


Рисунок 2-3. Снятие задней крышки

Английский язык	**Русский язык**
Back Cover	Задняя крышка
Back Cover Screws	Винты задней крышки

4. Завершите монтаж проводки. Подробная информация представлена в схеме (1.4). Зафиксируйте заднюю крышку.

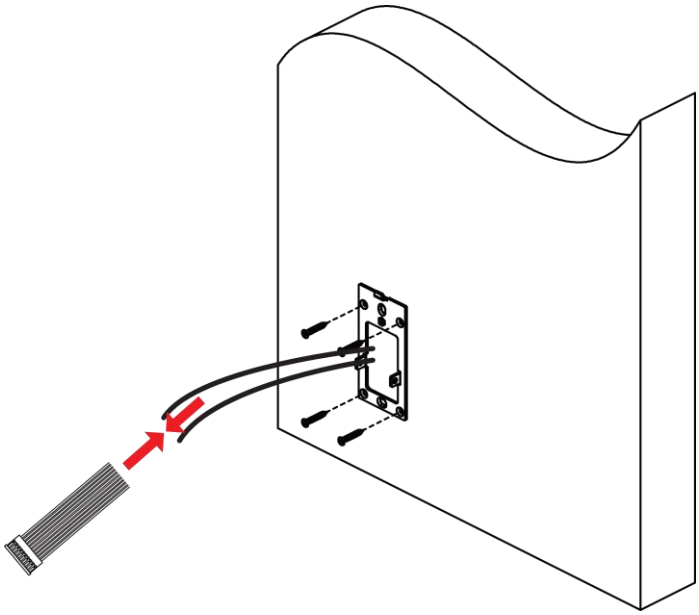


Рисунок 2-4. Проводка

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

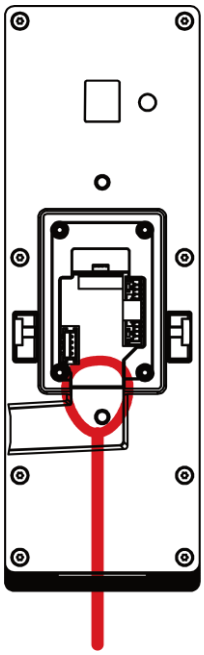


Рисунок 2-5. Фиксация силиконовым герметиком

Английский язык	**Русский язык**
Apply silicone sealant	Используйте герметик

6. Разместите устройство на плате сверху вниз. Закрепите устройство на монтажной плате с помощью 2 установочных винтов (SC-KM3X8-T10-SUS-NL).

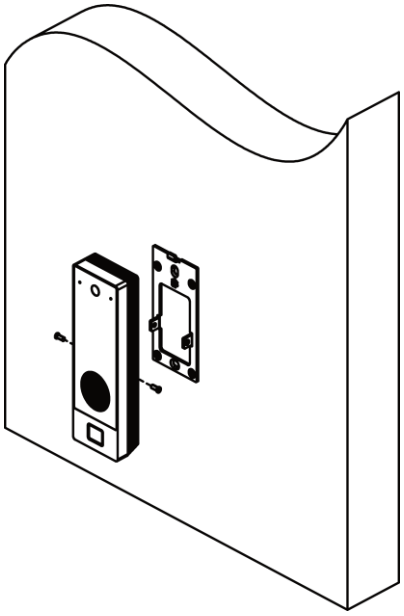


Рисунок 2-6. Фиксация устройства

7. Завершите установку.

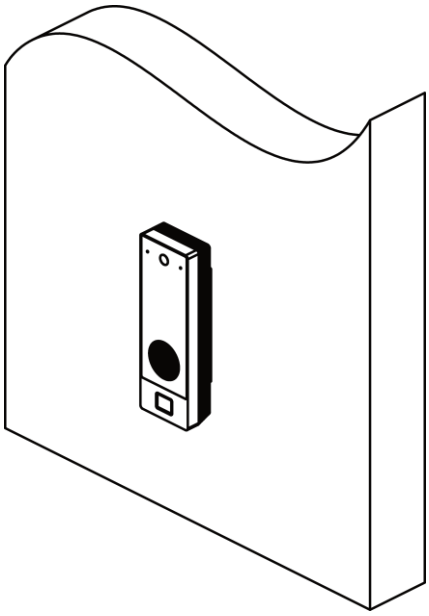


Рисунок 2-7. Завершение установки

Раздел 3 Подключение

Устройство можно подключать к клемме RS-485, к дверному замку, к кнопке выхода, к тревожному выходу / входу устройства, к считывателю карт Wiegand, к контроллеру доступа и к источнику питания. Подключите периферийные устройства в соответствии с описанием ниже.
Если соединить терминал WIEGAND с контроллером доступа, терминал распознавания лиц может передавать информацию аутентификации, на основании которой контроллер отпирает дверь или отказывает в доступе.

Примечание

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

3.1 Описание разъемов

Ниже представлена схема подключения терминала:

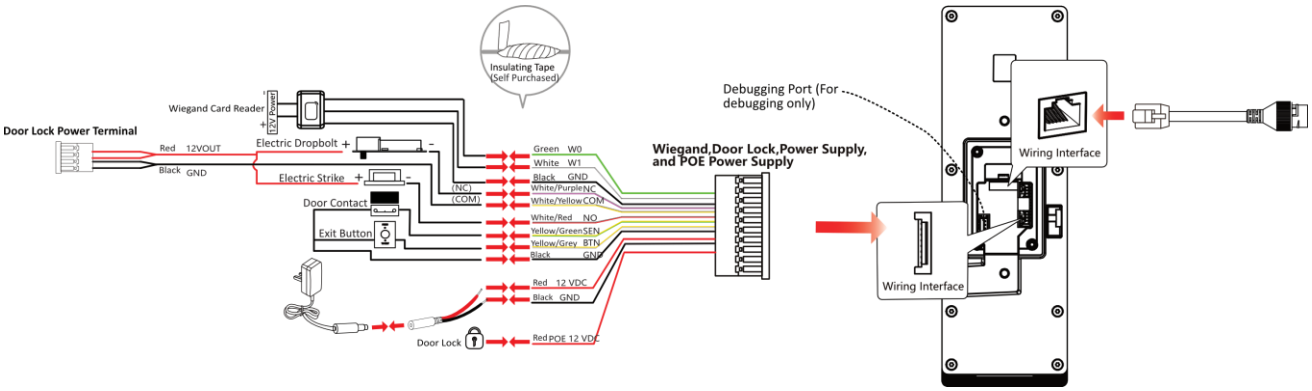


Рисунок 3-1. Схема разъемов

Раздел 4 Активация

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

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

4.1 Активация через мобильный веб-интерфейс

Можно активировать устройство через мобильный веб-интерфейс.

Шаги

1. После включения устройства точка доступа включена по умолчанию. Найдите точку доступа устройства на телефоне и подключитесь к ней.

Примечание

- Имя точки доступа устройства — AP_ Серийный номер, исходный пароль точки доступа устройства — Серийный номер. После перезагрузки или переключения из режима без точки доступа в режим точки доступа, пароль точки доступа будет изменен на пароль активации.
- Вход в мобильный веб-клиент возможен только тогда, когда устройство находится в режиме точки доступа.

2. Откройте адресную строку браузера мобильного телефона и введите 192.168.8.1, чтобы войти в интерфейс активации.
3. Установите пароль активации и подтвердите его.

Примечание

- Длина пароля должна составлять от 8 до 16 символов.
- Пароль должен состоять из двух или более комбинаций цифр, строчных букв, заглавных букв и специальных символов.
- Пароль не может содержать имя пользователя, 123, admin, 4 или более последовательных цифр в порядке возрастания или убывания, а также один и тот же символ.

4. Нажмите **Activate Device** («Активировать устройство»).

4.2 Активация через веб-интерфейс

Можно активировать устройство через веб-интерфейс.

Шаги

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

Примечание

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

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

Предостережение

- Надежность пароля устройства может быть автоматически проверена. Настоятельно рекомендуется использовать надежный пароль (используя не менее 8 символов, включая буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы). Также рекомендуется регулярно обновлять пароль. Ежемесячная или еженедельная смена пароля позволит сделать использование продукта безопаснее.
- Правильная настройка паролей и других параметров безопасности является обязанностью поставщика услуг и / или конечного пользователя.
- В пароле не должны содержаться следующие символы: имя пользователя, 123, admin (без учета регистра), 4 или более непрерывно увеличивающихся или уменьшающихся цифр или 4 или более последовательно повторяющихся символов.

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

4.3 Активация через ПО SADP

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

Перед началом

- ПО SADP доступно на диске, входящем в комплект или на официальном сайте; установите ПО SADP согласно инструкции.
- Устройство и ПК, на котором запущено ПО SADP, должны находиться в одной подсети.

Следующие шаги показывают, как активировать устройство и изменить его IP-адрес. Подробная информация о пакетной активации и изменении IP-адресов представлена в ***Руководстве пользователя ПО SADP***.

Шаги

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

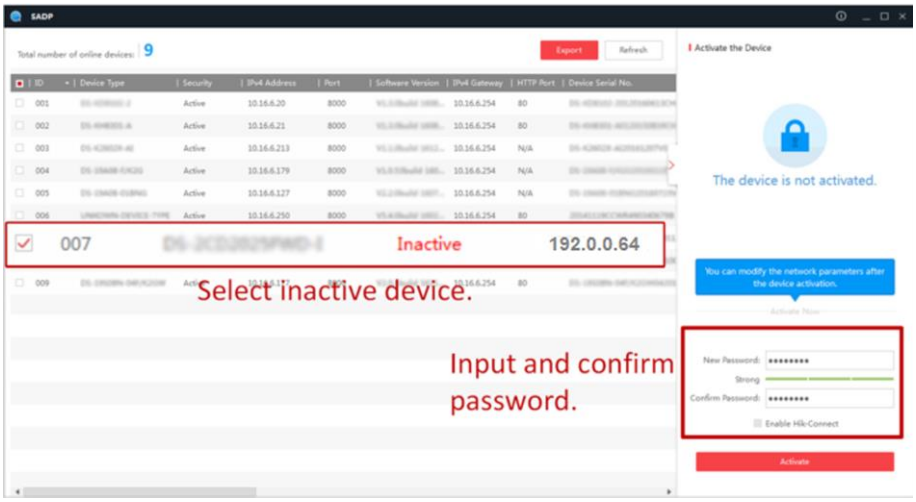
Предостережение

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

Примечание

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

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



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

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

4.4 Активация устройства через клиентское программное обеспечение Guarding Vision

Для исправной работы некоторых устройств необходимо создать пароль активации, прежде

чем добавлять их в ПО Guarding Vision.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

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

Предостережение

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

Примечание

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

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

Раздел 5 Настройка устройства через мобильный веб-интерфейс

5.1 Вход в систему

В систему можно войти через мобильный интерфейс.

Примечание

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

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

5.2 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, Bluetooth, ISUP и Guarding Vision.

Основная информация

Можно просмотреть модель, серийный номер и версию прошивки.

5.3 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 на адрес сервера электронной почты во вложении.
2. Проверочный код будет отправлен на зарезервированный адрес электронной почты в течение 5 минут.
3. Введите проверочный код в поле проверочного кода для подтверждения идентификации.

Создайте новый пароль и подтвердите его.

5.4 Настройка

5.4.1 Просмотр информации об устройстве

Просмотр названия устройства, языка, модели, серийного номера, версии, количества каналов, количества интерфейсов входа, количества интерфейсов выхода, числа тревожных входов, числа тревожных выходов, MAC-адреса, информации производителя, емкости устройства и т. д.
Нажмите → **System Settings → Basic Information** («Настройки системы → Основная информация») для перехода на соответствующую страницу.
Можно просмотреть данные названия устройства, языка, модели, серийного номера, версии, количества каналов, количества интерфейсов входа, количества интерфейсов выхода, числа тревожных входов, числа тревожных выходов, MAC-адреса, информации производителя, емкости устройства и т. д.

5.4.2 Настройка времени

Установите часовой пояс, режим синхронизации времени и отображаемое время.
Нажмите → **System Settings → Time Settings** («Настройки системы → Настройки времени») для перехода на соответствующую страницу.

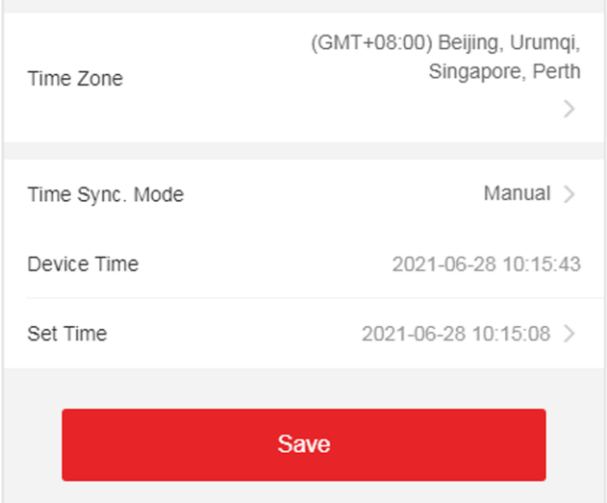


Рисунок 5-1. Настройки времени

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

Часовой пояс

Выберите часовой пояс, в котором находится устройство.

Синхронизация времени Режим

Вручную

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

NTP

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

5.4.3 Настройка параметров перехода на летнее время

Шаги

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

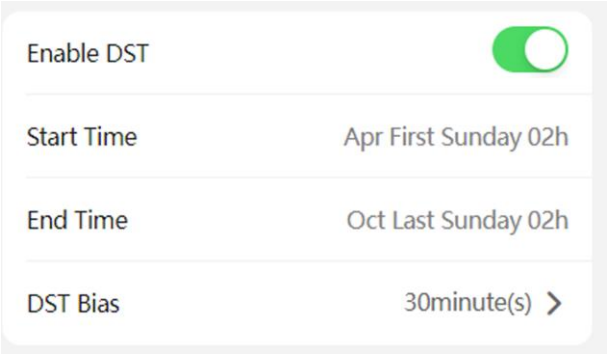


Рисунок 5-2. Летнее время

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

5.4.4 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.

5.4.5 Настройка сетевых параметров

Проводная сеть

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

DHCP

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

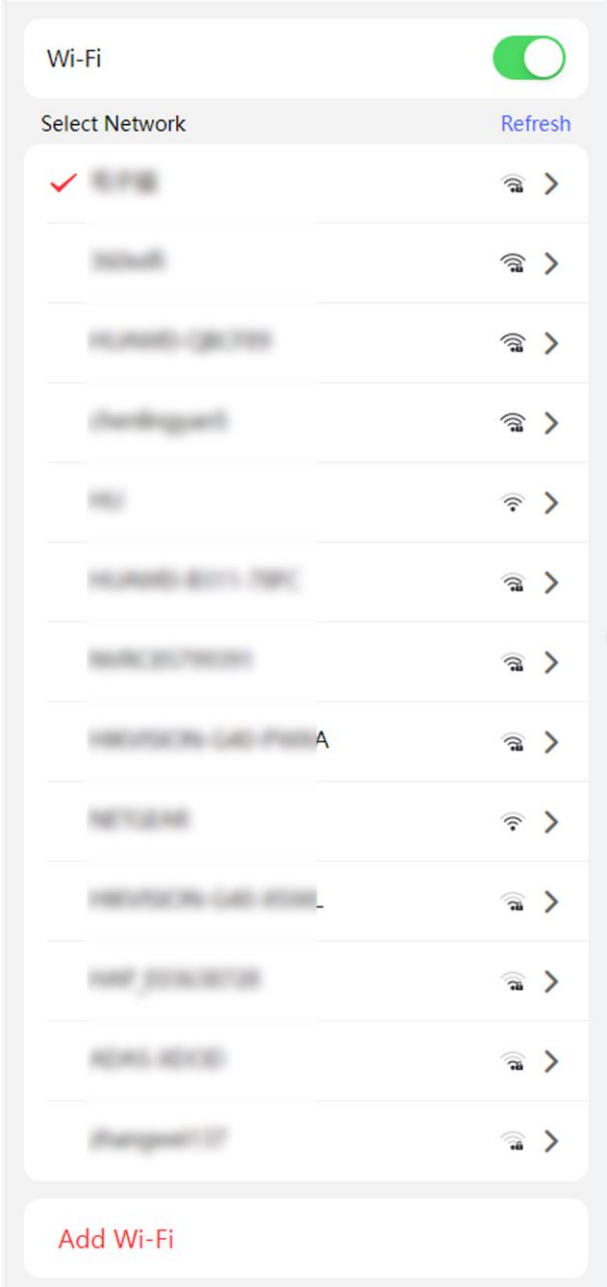


Рисунок 5-3. Wi-Fi

3. Добавьте Wi-Fi.
   1) Нажмите **Add Wi-Fi** («Добавить Wi-Fi»).
   2) Введите **Wi-Fi Name** («Имя Wi-Fi») и **Wi-Fi Password** («Пароль Wi-Fi») и выберите **Encryption Type** («Тип шифрования»).
   3) Нажмите **Save** («Сохранить»).
4. Выберите имя Wi-Fi и нажмите **Connect** («Подключиться»).
5. Введите пароль и нажмите **Save** («Сохранить»).

Настройка параметров порта

Можно настроить HTTP и HTTPS при доступе к устройству через сеть.
Нажмите → **Network Service → HTTP(S)** («Сетевая служба → HTTP(S)»), чтобы перейти на соответствующую страницу.

HTTP

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

HTTPS

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

Точка доступа устройства

После включения точки доступа на устройстве можно использовать мобильный телефон для подключения к точке доступа и ее настройки.

Примечание

Настроить параметры можно только при подключении к устройству через точку доступа (hotspot). Если подключаться к устройству по IP-адресу, эта функция недоступна.

На главной странице нажмите → **Network Settings** → **Device Hotspot** («Настройки сети → Точка доступа устройства»).
Нажмите **Device Hotspot** («Точка доступа устройства») и нажмите **Save** («Сохранить»).

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

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

4. Можно просмотреть **Register Status** («Состояние регистрации») и **Binding Status** («Состояние привязки»).
5. Включите **Video Encryption** («Шифрование видео»), создайте пароль и подтвердите его.

Примечание

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

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

Настройка параметров ISUP

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

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

Примечание

Если выбрана версия 5.0, необходимо также установить ключ шифрования.

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

5.4.6 Управление пользователями

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

Шаги

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

2) Настройте следующие параметры.

ID сотрудника

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

Имя

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

Пользователь с длительным разрешением

Настройте долгосрочное разрешение для пользователя.

Дата начала / Дата окончания

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

Администратор

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

Только проверка УРВ

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

Роль пользователя

Выберите роль пользователя.

Распознавание лиц

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

Считывание отпечатков пальцев

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

Карта

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

3) Нажмите **Save** («Сохранить»).

3. Нажмите на пользователя в списке, чтобы изменить информацию о нем.
4. Нажмите на пользователя, которого нужно удалить из списка, затем нажмите , чтобы удалить его.
5. Можно осуществлять поиск пользователя по идентификатору сотрудника или имени в поле поиска.

5.4.7 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.

5.4.8 Настройки параметров контроля доступа

Настройка параметров аутентификации

Настройка параметров аутентификации.

Шаги

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

Терминал

Выберите терминал для настройки.

Тип терминала / режим терминала

Получение описания терминалов. Доступно только для чтения.

Включить устройство с функцией аутентификации

Включить функцию аутентификации.

Аутентификация

В выпадающем списке выберите режим аутентификации в соответствии с потребностями.

Интервал непрерывного распознавания лица

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

Интервал аутентификации

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

Запуск тревоги при достижении максимального количества неудачных попыток считывания карты

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

Режим основного интерфейса

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

Включение тревоги тампера

Включите детектор саботажа на считывателе карт.

Считывание номера карты в обратной последовательности

После включения функции номер карты будет считываться в обратной последовательности.

Настройка параметров двери

Нажмите → **Access Control** → **Door Parameters** («Контроль доступа → Параметры двери»).
Нажмите **Save** («Сохранить»), чтобы сохранить настройки.

Название

Можно задать имя двери.

Длительность открытого состояния

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

Тип кнопки выхода

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

Дверь остается открытой после авторизации первого сотрудника (мин)

Установите продолжительность открытия двери после авторизации первого сотрудника. После авторизации первого пользователя несколько других пользователей получат 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 создает 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»), выбрав **Access Control Mode** («Режим контроля доступа»). Режим контроля доступа является нормальным режимом работы устройства. Для получения доступа необходимо пройти аутентификацию с использованием учетных данных.

Remote Authentication («Удаленная аутентификация»)

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

Локальная проверка учетных данных

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

Период тайм-аута ответа

Можно установить период ожидания удаленной аутентификации.

Удаленная проверка разблокировки в режиме офлайн

После включения функции можно выполнять разблокировку удаленно, в режиме офлайн.

Режим возврата результата

Настройте режим возврата результата.

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

Настройка параметров безопасности карты

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

Включение распознавания NFC-карты

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

Включение распознавания M1-карты

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

Шифрование M1-карты

Шифрование M1-карты поможет повысить уровень безопасности при аутентификации.

Сектор

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

Активация распознавания 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.

Активация распознавания FeliCa-карты

Устройство может считывать данные с FeliCa-карты.

5.4.9 Настройка видеодомофонии

Настройки ID устройства

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

Шаги

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

Тип устройства

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

Примечание

При изменении типа устройства необходимо перезагрузить устройство.

Номер периода

Укажите номер периода установленного устройства.

Номер здания

Укажите номер здания.

Номер помещения

Укажите номер помещения.

Примечание

При изменении номера необходимо перезагрузить устройство.

Номер этажа

Укажите номер этажа, на котором установлено устройство.

Номер вызывной панели

Укажите номер этажа, на котором установлено устройство.

Примечание

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

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

Номер вызывной панели, установленной снаружи помещения

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

Примечание

При изменении номера необходимо перезагрузить устройство.

Номер периода

Укажите номер периода установленного устройства.

Настройки сеанса связи

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

Шаги

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

   Пароль регистрации

   Пароль активации пульта консьержа / диспетчера.

   IP-адрес пульта консьержа / диспетчера

   Настройте IP-адрес пульта консьержа / диспетчера.

   IP-адрес частного сервера

   IP-адрес частного сервера.

   Включение протокола 1.0

   После включения, устройство подключено к пульту консьержа / диспетчера по предыдущему протоколу. При выключении, устройство подключено к пульту консьержа / диспетчера по новому протоколу.
3. Нажмите **Save** («Сохранить»).

Настройка временных интервалов

Установите макс. продолжительность вызова.
Нажмите → **Intercom** → **Call Settings** («Домофония → Настройки звонка»).
Установите максимальное время связи. Нажмите **Save** («Сохранить»).

Примечание

Макс. продолжительность вызова составляет от 90 до 120 с.

Нажатие кнопки для вызова

Шаги

1. Нажмите → **Intercom** → **Press Button to Call** («Домофония → Нажатие кнопки для вызова»)
2. Выберите номер. Выберите **Call Indoor Station** («Вызов видеодомофона»), **Call Specified Indoor Station** («Вызов настроенного видеодомофона»), **Call Management Center** («Вызов центра управления») или **APP** («Приложение»).

Примечание

При выборе **Call Specified Indoor Station** («Вызов настроенного видеодомофона») необходимо ввести номер видеодомофона.

Настройка привязки номеров

Вызовите SIP-кабинет для вызова кабинета.

Шаги

1. Нажмите → **Intercom** → **Number Settings** («Домофония → Настройки номера»).
2. Нажмите **+**, введите **Room No.** («Номер помещения») и **SIP Number** («Номер SIP»).
3. Нажмите **Save** («Сохранить»).

5.4.10 Настройки параметров аудио

Шаги

1. Нажмите → **Audio** («Аудио»).
2. Опционально. Настройте громкость ввода и вывода.
3. Можно включить голосовые предупреждения в соответствии с потребностями.

5.4.11 Настройки параметров лица

Настройка параметров лица.

Настройки параметров лица

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

Детекция подлинности биометрических данных лица (антиспуфинг)

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

Уровень безопасности «Детекция лиц в режиме реального времени»

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

Пороговое значение для сопоставления 1: 1

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

Пороговое значение для сопоставления 1:N

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

Лимит времени при распознавании лица

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

Параметры отпечатков пальцев

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

Уровень безопасности отпечатков пальцев

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

Параметры детекции наличия / отсутствия маски

Детекция наличия / отсутствия маски

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

None («Нет»)

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

Напоминание о необходимости ношения

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

Предупреждение об обязательном ношении

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

Лицо с маской (1:1)

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

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

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

Примечание

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

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

5.4.12 Обновление и техническое обслуживание

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

Перезагрузка устройства

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

Обновление

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

Примечание

Не выключайте устройство во время обновления.

Восстановление параметров

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

Восстановление настроек по умолчанию

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

Восстановление настроек изготовителя

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

5.4.13 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.

5.4.14 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 6 Работа через веб-интерфейс

6.1 Вход с систему

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

Примечание

- Устройство должно быть активировано. Подробная информация представлена в разделе Активация.
- Рекомендуется входить в систему через браузер Chrome.

Вход в систему через веб-интерфейс

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

Вход в систему через удаленную настройку клиентского программного обеспечения

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

6.2 Забыть пароль

Если вы забыли пароль для входа в систему, пароль можно поменять с помощью адреса электронной почты или контрольных вопросов.
На странице входа в систему нажмите **Forget Password** («Забыть пароль»).
Выберите **Verification Mode** («Режим проверки»).

Проверка по контрольным вопросам

Ответьте на контрольные вопросы.

Подтверждение по электронной почте

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

Создайте новый пароль и подтвердите его.

6.3 Загрузка веб-плагина

Доступны как просмотр в режиме реального времени без плагина, так и просмотр в режиме реального времени после загрузки плагина. Для более качественного просмотра в режиме реального времени рекомендуется загрузить плагин.
Нажмите → **Download Web Plug-In** («Скачать веб-плагин»), чтобы загрузить плагин на локальный компьютер.

6.4 Помощь

6.4.1 Лицензии на ПО с открытым исходным кодом

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

6.4.2 Просмотр онлайн справки

Можно просмотреть справку по настройке через веб-интерфейс.
Нажмите → **Online Document** («Онлайн документ») в правом верхнем углу веб-страницы.

6.5 Выход из системы

Выйдите из учетной записи.
Нажмите **admin** → **Logout** → **OK** («Администратор → Выход из системы → ОК»).

6.6 Быстрые операции через веб-интерфейс

6.6.1 Изменение пароля

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

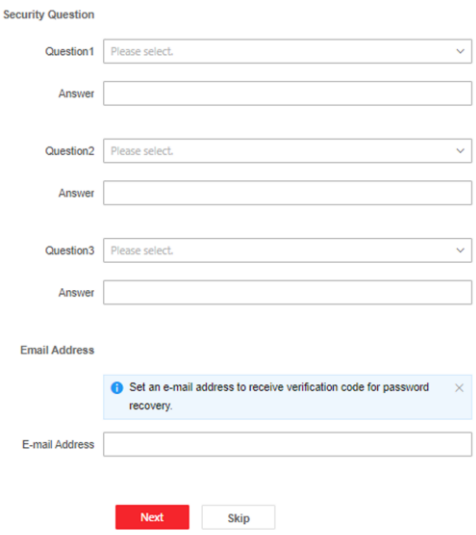


Рисунок 6-1. Изменение пароля

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

6.6.2 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.

6.6.3 Настройки времени

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

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

NTP

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

Вручную

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

Адрес сервера / Порт NTP / Интервал

Можно настроить адрес сервера, порт NTP, интервал.

Переход на летнее время (DST)

Установите время начала и окончания перехода на летнее время (DST), а также смещение.
Нажмите **Next** («Далее»), чтобы сохранить настройки и перейти к следующему параметру.
Или нажмите **Skip** («Пропустить»), чтобы пропустить настройки.

6.6.4 Настройки конфиденциальности

Настройте параметры загрузки и хранения изображений.
Нажмите в правом верхнем углу веб-страницы, чтобы открыть страницу мастера настроек.

Загрузка и хранение изображений

Сохранение изображения при аутентификации

Автоматическое сохранение изображений при аутентификации.

Загрузка изображения при аутентификации

Загрузка изображений при автоматической аутентификации на платформу.

Сохранение зарегистрированного изображения

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

Загрузка изображения после захвата

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

Сохранение изображения после захвата

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

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

6.6.5 Настройки учетной записи администратора

Шаги

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

Примечание

Необходимо выбрать хотя бы один сертификат.

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

Примечание

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

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

Примечание

Поддерживается до 5 карт.

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

Примечание

Разрешено до 10 отпечатков пальцев.

6.6.6 Настройка номеров и сетевые настройки

Шаги

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

Примечание

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

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

Тип устройства

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

Номер микрорайона

Укажите номер микрорайона.

Номер здания

Укажите номер здания.

Номер помещения

Укажите номер помещения.

Номер этажа

Укажите номер этажа, на котором установлено устройство.

Номер вызывной панели

Укажите номер установленной вызывной панели.

Примечание

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

Номер вызывной панели, установленной снаружи помещения

Укажите номер установленной уличной вызывной панели.

Примечание

Номер в диапазоне от 1 до 99.

3. Настройте параметры сети видеодомофона.

Пароль регистрации

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

IP-адрес пульта консьержа / диспетчера

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

IP-адрес частного сервера

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

Включение протокола 1.0

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

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

6.7 Управление пользователями

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

Добавление основной информации

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.
Добавьте основную информацию о сотруднике / посетителе, включая идентификатор, Ф. И. О., пол и роль пользователя.
При выборе роли пользователя **Visitor** («Посетитель») можно установить количество посещений.
Если выбран параметр **Custom Type** («Настраиваемый тип»), можно изменить имя. Измененное имя будет применено к устройству.
Нажмите **Save** («Сохранить») для сохранения настроек.

Настройка длительности разрешения

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.
Включите или настройте **Long-Term Effective User** («Пользователь с длительным разрешением»), и пользователь сможет получить разрешение только в течение настроенного периода времени.
Настройка разрешения для доступа к двери.
Нажмите **Save** («Сохранить») для сохранения настроек.

Настройки параметров аутентификации

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.
Выберите тип аутентификации.
Нажмите **Save** («Сохранить») для сохранения настроек.

Добавление карты

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

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

Добавление изображения лица

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.
Нажмите **+ Upload** («Загрузить»), чтобы загрузить изображение лица с локального ПК.

Примечание

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

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

Добавление отпечатка пальца

Примечание

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

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.
Нажмите **Add Fingerprint** («Добавить отпечатки пальцев») и приложите палец к модулю отпечатков пальцев, чтобы добавить отпечаток пальца.
Нажмите **Save** («Сохранить») для сохранения настроек.

Настройки номера устройства

Нажмите **Person Management → Add** («Управление пользователями → Добавить»), чтобы перейти на страницу добавления сотрудника / посетителя.
Добавьте основную информацию о пользователе. Перейдите в модуль номера устройства.
Нажмите **Add** («Добавить») и введите номер помещения и этаж. Нажмите **Add** («Добавить») или **Save and Continue** («Сохранить и продолжить»).

Удаление пользователя

На странице управления пользователями отметьте пользователя, которого нужно удалить, и нажмите **Delete** («Удалить»).
Нажмите **Clear All** («Очистить все»), чтобы удалить всех пользователей.

Редактирование пользователя

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

Фильтр

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

6.8 Управление устройством

Возможность управления подключенными устройствами с определенной страницы.

Шаги

1. Нажмите **Device Management** («Управление устройством») для перехода на страницу настроек.
2. Нажмите **Add** («Добавить»), чтобы добавить видеодомофон или дополнительную вызывную панель. Введите параметры и нажмите **Save** («Сохранить»), чтобы добавить.
3. Нажмите **Import** («Импорт»), скачайте шаблон. Введите информацию об устройстве в шаблон и нажмите для импорта шаблона.
4. Нажмите **Export** («Экспорт»), чтобы экспортировать данные на компьютер.
5. Выберите устройство и нажмите **Delete** («Удалить») для удаления выбранного устройства из списка.
6. Нажмите **Refresh** («Обновить») для получения информации об устройстве.
7. Опционально. Настройка информации об устройстве.

Изменение информации устройства	Нажмите для редактирования информации об устройстве.
Удаление информации устройства	Нажмите для удаления информации об устройстве из списка.
Поиск устройств	Выберите **Status** («Состояние») и **Device Type** («Тип устройства») для поиска устройств.

6.9 Управление контролем доступа

6.9.1 Обзор

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

Состояние двери

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

При запуске просмотра в режиме реального времени необходимо настроить громкость.

Примечание

При настройке громкости во время двусторонней аудиосвязи можно услышать эхо.

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

/ / /

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

Можно начать запись при запуске просмотра в режиме реального времени.

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

Полноэкранный просмотр.

Контроль состояния

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

Событие в режиме реального времени

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

Привязка устройства

Можно просмотреть количество и статус привязанных устройств.

Примечание

Нажмите **View More** («Дополнительно»), чтобы перейти в раздел ***Управление устройствами***.

Информация о пользователе

Можно просмотреть добавленную и недобавленную информацию об учетных данных пользователя.

Состояние сети

Можно просмотреть состояние подключения и регистрации проводной сети, беспроводной сети, Guarding Vision, ISUP и VoIP.

Основная информация

Можно просмотреть модель, серийный номер и версию прошивки.

Емкость устройства

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

6.9.2 Поиск событий

Нажмите **Event Search** («Поиск события») для перехода на соответствующую страницу. Введите условия поиска, включая идентификатор сотрудника / посетителя, имя, номер карты, время начала и время окончания доступа и нажмите **Search** («Поиск»).
После этого на панели справа появятся результаты поиска.

6.9.3 Конфигурация параметров двери

Настройте параметры разблокировки дверей.

Просмотр состояния устройства в режиме онлайн

Просмотрите и обновите состояние устройства.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
Можно просмотреть состояние устройства в режиме онлайн. Нажмите **Refresh** («Обновить»), чтобы обновить состояние устройства.

Установка названия двери

Введите название двери.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
Установите **Door Name** («Название двери») и нажмите **Save** («Сохранить»).

Настройка длительности открытого состояния через веб-интерфейс ПК

Можно установить время открытия дверного замка после считывания карты.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
Установите продолжительность открытия, то есть время действия после разблокировки двери. Если дверь не будет открыта в течение установленного времени, она автоматически заблокируется. Настраиваемое время: от 1 до 255 секунд.
Нажмите **Save** («Сохранить»).

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

Если дверь не закрыта по истечении времени срабатывания блокировки, точка контроля доступа подаст звуковой сигнал тревоги.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
Настройте **Door Open Timeout Alarm** («Тревога тайм-аута открытой двери»). Если дверь не закрыта по истечении времени срабатывания блокировки, точка контроля доступа подаст звуковой сигнал тревоги. Если установлено значение 0, тревога не будет включена.
Нажмите **Save** («Сохранить»).

Настройка блокировки двери при закрытии

Можно установить блокировку двери при закрытии.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
Можно включить **Lock Door when Door Closed** («Блокировка двери при закрытии»).
Нажмите **Save** («Сохранить»).

Настройка состояния дверного замка через веб-интерфейс

Выберите состояние дверного замка в соответствии со способом подключения.
Нажмите **Access Control → Parameter Settings → Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»).
Выберите необходимый режим: **Remain Open** («Оставить дверь открытой») или **Remain Closed** («Оставить дверь закрытой»). По умолчанию задан параметр **Remain Closed** («Оставить закрытой»).
Нажмите **Save** («Сохранить»).

Настройка кнопки выхода через веб-интерфейс ПК

Можно установить необходимый параметр кнопки выхода: **Remain Open** («Оставить открытым») или **Remain Closed** («Оставить закрытым»).
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.

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

Настройка закрытия двери при отключении питания через веб-интерфейс ПК

Можно установить состояние дверного замка при отключении питания.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
Настройте **Door Lock Powering Off Status** («Состояние закрытия двери при отключении питания»). По умолчанию задан параметр **Remain Closed** («Оставить закрытым»).
Нажмите **Save** («Сохранить»).

Настройка увеличенной длительности открытого состояния через веб-интерфейс ПК

Дверной контакт может быть активирован с установленной задержкой после считывания карты пользователя с расширенным доступом.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
Настройте **Extended Open Duration** («Увеличенная длительность открытого состояния»).
Дверной контакт может быть активирован с установленной задержкой после считывания карты пользователя с расширенным доступом.
Нажмите **Save** («Сохранить»).

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

После авторизации первого пользователя несколько других пользователей получат доступ к дверям и разрешения на другие действия.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
Установите продолжительность открытия двери при входе первого сотрудника и нажмите **Save** («Сохранить»).

Настройка кода принуждения через веб-интерфейс ПК

После настройки кода принуждения, при возникновении угрозы, введите код для открытия двери. Одновременно система контроля доступа будет сообщать о событиях принуждения.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
Установите код принуждения и нажмите **Save** («Сохранить»).

Примечание

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

Установка суперпароля через веб-интерфейс ПК

Администратор или назначенный сотрудник может ввести суперпароль для открытия двери.
Нажмите **Access Control** → **Parameter Settings** → **Door Parameters** («Контроль доступа → Настройки параметров → Параметры двери»), чтобы перейти на страницу настроек.
После установки **Super Password** («Суперпароль») назначенный сотрудник сможет ввести суперпароль для открытия двери.
Нажмите **Save** («Сохранить»).

Примечание

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

6.9.4 Настройки параметров аутентификации

Выбор основного или дополнительного считывателя карт через веб-интерфейс ПК

Настройте терминал для аутентификации пользователя.
Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
Выберите терминал в качестве основного или дополнительного считывателя карт.
Установите другие параметры и нажмите **Save** («Сохранить»).

Просмотр типа и модели терминала через веб-интерфейс ПК

Можно просмотреть тип и модель терминала.
Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
Просмотрите **Terminal Type** («Тип терминала») и **Terminal Model** («Модель терминала»).

Включение устройства аутентификации через веб-интерфейс ПК

После включения терминал аутентификации можно использовать для считывания карт.

Шаги

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

Настройка аутентификации через веб-интерфейс ПК

Настройка сертификации.
Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
При установке основного считывателя карт в качестве терминала можно выбрать **Authentication** («Аутентификация») из выпадающего списка. При наличии нескольких типов аутентификаций следует установить параметры **Single Credential Authenticating Timeout** («Тайм-аут аутентификации с помощью одного типа учетных данных») и **Control Initial Authentication Type** («Управление типом первичной аутентификации»).

Тайм-аут аутентификации с помощью одного типа учетных данных

Настройка продолжительности каждой сертификации.

Примечание

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

Управление типом первичной аутентификации

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

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

Установка интервала распознавания через веб-интерфейс ПК

Установите временной интервал между двумя циклами распознавания лиц при непрерывной работе.
Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.

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

Примечание

Введите число от 1 до 10.

Установка интервала аутентификации через веб-интерфейс ПК

Можно установить интервал аутентификации одного и того же сотрудника во время аутентификации. Один сотрудник может пройти аутентификацию только один раз в заданный интервал. Вторая аутентификация будет невозможна. Если другой пользователь пройдет аутентификацию в течение заданного интервала, он сможет пройти аутентификацию повторно.

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

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

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

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

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

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

Нажмите **Save** («Сохранить»).

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

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

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

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

Нажмите **Save** («Сохранить»).

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

Можно включить или отключить функцию считывания номера карты в обратной последовательности.
Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
При включении функции **Card No. Reversing** («Считывание номера карты в обратной последовательности») считанный номер карты будет отображаться в обратном порядке.
Нажмите **Save** («Сохранить»).

Настройка положения дополнительного считывателя карт

Можно выбрать положение дополнительного считывателя карт.
Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
Если в качестве терминала выбран дополнительный считыватель карт, можно выбрать его положение как **Different Side from Main Card Reader** («С другой стороны от основного считывателя карт») или **Same Side as Main Card Reader** («На той же стороне, что и основной считыватель карт»). Нажмите **Save** («Сохранить»).

Настройка связи с панелью управления через веб-интерфейс ПК

Можно настроить связь с панелью управления для дополнительного считывателя карт. Если считыватель карт не может подключиться к контроллеру доступа в течение заданного времени, считыватель перейдет в режим офлайн.
Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
При выборе терминала в качестве дополнительного считывателя карт установите параметр **Communication with Controller Every** («Связь с панелью управления») и нажмите **Save** («Сохранить»).

Установка времени ожидания ввода пароля через веб-клиент

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

Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
При выборе дополнительного считывателя карт в качестве терминала установите **Max. Interval When Entering Password** («Максимальный интервал времени при вводе пароля») и нажмите **Save** («Сохранить»).

Настройка полярности светодиодов OK и Error через веб-интерфейс ПК

Выберите полярность светодиодов для интерфейсов OK и ERR в соответствии с подключением, по умолчанию – положительная полярность.
Нажмите **Access Control** → **Parameter Settings** → **Authentication Settings** («Контроль доступа → Настройки параметров → Настройки параметров аутентификации»), чтобы перейти на страницу настроек.
При выборе терминала в качестве дополнительного считывателя карт установите полярность светодиодов OK и Error и нажмите **Save** («Сохранить»).

6.9.5 Настройка параметров распознавания лиц

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

При включении этой функции устройство сможет отличать сотрудника / посетителя от изображения.
Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.
Включите **Face Anti-spoofing** («Детекция подлинности биометрических данных лица (антиспуфинг)») и нажмите **Save** («Сохранить»).
Здесь можно включить/выключить функцию детекции лиц в режиме реального времени. При включении этой функции устройство сможет отличать сотрудника / посетителя от изображения. Если лицо неактивно, аутентификация не удастся.

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

После включения функции антиспуфинга можно установить надлежащий уровень безопасности при выполнении аутентификации лица в режиме реального времени.
Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.
Выберите уровень детекции подлинности биометрических данных и нажмите **Save** («Сохранить»).
Можно выбрать общий, расширенный и профессиональный уровни. Чем выше уровень, тем ниже вероятность ложного распознавания и выше вероятность отказа.

Установка дальности распознавания через веб-интерфейс ПК

Можно установить расстояние между пользователем и камерой устройства при аутентификации.
Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.
Настройте дальность распознавания и нажмите **Save** («Сохранить»).

Настройка угла наклона через веб-интерфейс ПК

Можно настроить угол наклона объектива во время распознавания лица и аутентификации.
Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Примечание

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

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

Настройка угла поворота через веб-интерфейс ПК

Можно настроить угол поворота объектива во время распознавания лица и аутентификации.
Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Примечание

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

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

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

Уровень качества изображения лица должен быть выше порогового значения для успешной аутентификации.
Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.

Примечание

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

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

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

Установите пороговое значение качества изображения лица 1:1.
Перейдите **Access Control** → **Parameters Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»).
Установите **1:1 Face Picture Grade Threshold** («Пороговое значение качества изображения лица 1:1») и нажмите **Save** («Сохранить»).
Чем выше порог, тем выше требования к качеству изображений, полученных с фронтальной камеры, и тем чаще может возникать ошибка аутентификации.

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

Установите пороговое значение соответствия лица 1:1.
Нажмите **Access Control → Parameter Settings → Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.
Установите пороговое значение для соответствия лица 1:1 и нажмите **Save** («Сохранить»).
Чем больше значение порога, тем ниже будет процент ложных тревог и выше процент ложных отказов при аутентификации по лицу. Максимальное значение – 100.

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

Можно установить пороговое значение для сопоставления лиц 1:N.
Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.
Установите пороговое значение совпадения 1:N и нажмите **Save** («Сохранить»).
Чем больше данное значение, тем меньше вероятность ложных совпадений и тем больше вероятность отклонений ложных совпадений. Максимальное значение 100.

Настройка области распознавания лиц через веб-интерфейс

Можно настроить область распознавания при аутентификации лиц.
Нажмите **Access Control** → **Parameter Settings** → **Area Configuration** («Контроль доступа → Настройки параметров → Конфигурация области»), чтобы перейти на страницу настроек.
Переместите желтый прямоугольник на экране предварительного просмотра, чтобы настроить эффективную область распознавания лиц слева, справа, сверху и снизу.
Или перетащите область или введите число, чтобы задать параметры.

Нажмите **Save** («Сохранить»).
Нажмите ,  или  для захвата, записи или перехода в полноэкранный режим.

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

После включения детекции наличия / отсутствия маски система распознает наличие / отсутствие маски.
Нажмите **Access Control** → **Parameter Settings** → **Smart** («Контроль доступа → Настройки параметров → Интеллектуальные функции»), чтобы перейти на страницу настроек.
После включения детекции лица с маской можно установить **Face without Mask Strategy** («Стратегия распознавания лиц без масок»), **Face with Mask&Face (1:1)** («Распознавание лиц и лиц в масках (1:1)»), **Face with Mask 1:1 Match Threshold** («Пороговое значение сопоставления лица с маской (1:1)»).

Стратегия распознавания лиц без масок

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

Напоминание о необходимости ношения

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

Предупреждение об обязательном ношении

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

Распознавание лица и лица с маской (1:1)

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

Распознавание лица и лица с маской (1:N)

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

Нажмите **Save** («Сохранить»).

6.9.6 Настройки параметров карты

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

После включения устройство сможет считывать NFC-карты.

Нажмите **Access Control** → **Parameter Settings** → **Card Settings** («Контроль доступа → Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек. Выберите **Enable NFC Card** («Включение распознавания NFC-карты») и нажмите **Save** («Сохранить»). После включения устройство сможет считывать NFC-карты. Если данные устройств контроля доступа получены с помощью мобильных устройств, может возникнуть событие несанкционированного доступа. Чтобы предотвратить это, можно отключить функцию NFC.

Вкл. / выкл. карты M1 через веб-клиент

После включения функции устройство сможет считывать M1-карты.
Нажмите **Access Control** → **Parameter Settings** → **Card Settings** («Контроль доступа → Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.
Нажмите **Enable M1 Card** («Включить карту M1»).

Шифрование M1-карты

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

Сектор

После включения шифрования M1-карты необходимо установить зашифрованный сектор.

Примечание

Рекомендуется зашифровать сектор 13.

Нажмите **Save** («Сохранить»).

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

После включения функции устройство сможет считывать EM-карты.
Нажмите **Access Control** → **Parameter Settings** → **Card Settings** («Контроль доступа → Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.
Выберите **Enable EM Card** («Включение распознавания EM-карты») и нажмите **Save** («Сохранить»).

Примечание

- Если подключен периферийный считыватель карт с поддержкой EM-карт, после включения этой функции можно считывать EM-карты через этот считыватель.
- При подключении двухчастотного модуля считывания карт можно одновременно считывать EM-карты и DESfire-карты. Однако считывание карты непосредственно на устройстве не будет работать.

Настройка карты DESFire

Можно включить карту DESFire и считывание информации с карты DESFire.
Нажмите **Parameter Settings** → **Card Settings** («Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.
Выберите **Enable DESFire Card** («Включить карту DESFire») и **DESFire Card Read Content** («Считывание информации с карты DESFire») и нажмите **Save** («Сохранить»).

Примечание

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

Настройка карты FeliCa

Можно включить карту FeliCa.
Нажмите **Parameter Settings** → **Card Settings** («Настройки параметров → Настройки карты»), чтобы перейти на страницу настроек.
Выберите **Enable FeliCa Card** («Включить карту FeliCa»).

Настройка параметров аутентификации по номеру карты через веб-интерфейс

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

Полный номер карты

Будет прочитан полный номер карты.

3 байта

Устройство будет считывать карту, используя 3 байта.

4 байта

Устройство будет считывать карту, используя 4 байта.

6.9.7 Настройки привязки

При срабатывании настроенного события загрузите информацию о событии на центральную платформу в соответствии с настроенным методом.

Шаги

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

2. Нажмите **+** .
3. Настройте источник события. Выберите тип привязки: **Event Linkage** («Привязка события»), **Card Linkage** («Привязка карты») или **Link Employee ID** («Привязка идентификатора сотрудника»).
   – При выборе **Event Linkage** («Привязка события») в качестве типа привязки укажите необходимые типы событий.
   – При выборе **Card Linkage** («Привязка карты») в качестве типа привязки введите номер карты и укажите считыватель карт.
   – При выборе **Link Employee ID** («Привязка идентификатора сотрудника») в качестве типа привязки введите идентификатор сотрудника и укажите считыватель карт.
4. Настройте действия привязки.
   1) Включите **Door Linkage** («Привязка двери»), установите флажок и выберите действие двери.
   2) Включите **Linked Capture** («Привязанный захват»).
5. Нажмите **Save** («Сохранить») для сохранения настроек.

6.9.8 Настройка рабочего режима через веб-интерфейс ПК

Можно настроить параметры терминала устройства.

Примечание

Эта функция поддерживается только некоторыми моделями, обратитесь к информации о конкретном устройстве.

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

Рабочий режим

Для рабочего режима можно выбрать режим контроля доступа или режим без разрешений.

Режим контроля доступа

Режим контроля доступа является нормальным режимом работы устройства. Для получения доступа необходимо пройти аутентификацию с использованием учетных данных.

6.9.9 Настройка удаленной проверки

Устройство загрузит на платформу информацию для аутентификации пользователя. Платформа определит, открывать дверь или нет.
Нажмите **Access Control → Parameter Settings → Terminal Parameters** («Контроль доступа → Настройки параметров → Параметры терминала»).
Нажмите **Save** («Сохранить») после настройки параметров.

Удаленная проверка

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

Локальная проверка учетных данных

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

6.9.10 Настройки конфиденциальности

Настройка типа хранения событий через веб-интерфейс ПК

Можно настроить тип хранения событий.
Нажмите **Access Control** → **Parameter Settings** → **Privacy Settings** («Контроль доступа → Настройки параметров → Настройка параметров конфиденциальности»), чтобы перейти на страницу настроек.
Для параметра **Event Storage Type** («Тип хранения события») можно выбрать: **Delete Old Events Periodically** («Периодическое удаление старых событий»), **Delete Old Events by Specified Time** («Удаление старых событий в заданное время») или **Overwriting** («Перезапись»).

Периодическое удаление старых событий

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

Удаление старых событий в заданное время

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

Перезапись

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

Нажмите **Save** («Сохранить»).

Настройка результатов аутентификации через веб-интерфейс ПК

Настройте информацию для результатов аутентификации, например, изображение, имя, идентификатор сотрудника и температуру.
Нажмите **Access Control** → **Access Control** → **Parameter Settings** → **Privacy Settings** («Контроль доступа → Контроль доступа → Настройки параметров → Настройка параметров конфиденциальности»), чтобы перейти на страницу настроек.
Проверьте отображаемую информацию в результатах аутентификации, например, изображение, имя, идентификатор сотрудника.

Выберите необходимый параметр: **Name De-identification** («Деидентификация имени») и **ID De-identification** («Деидентификация идентификатора»). После деидентификации имени и идентификатора будут отображаться части информации.
Установите **Authentication Result Display Duration** («Длительность отображения результата аутентификации»), и результаты аутентификации будут отображаться в течение заданного периода времени.
Нажмите **Save** («Сохранить»).

Настройка загрузки и хранения изображений через веб-интерфейс ПК

Можно установить параметры загрузки и хранения изображений.
Нажмите **Access Control** → **Parameter Settings** → **Privacy Settings** («Контроль доступа → Настройки параметров → Настройка параметров конфиденциальности»), чтобы перейти на страницу настроек.

Сохранение изображения при аутентификации

Автоматическое сохранение изображений при аутентификации.

Загрузка изображения при аутентификации

Загрузка изображений при автоматической аутентификации на платформу.

Режим изображения

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

Сохранение зарегистрированного изображения

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

Сохранение изображения после захвата

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

Загрузка изображения после захвата

Если эта функция активирована, изображения, захваченные соответствующей камерой, будут автоматически загружаться на платформу
Нажмите **Save** («Сохранить»).

Очистка изображений с устройства через веб-интерфейс ПК

Можно удалить все зарегистрированные или захваченные изображения лиц.
Нажмите **Visitor** → **Parameter Settings** → **Privacy Settings** («Посетитель → Настройки параметров → Настройка параметров конфиденциальности»), чтобы перейти на страницу настроек.

Нажмите **Clear** («Очистить»), чтобы очистить все зарегистрированные или захваченные изображения.

6.9.11 Настройки вызова

Настройки № устройства через веб-интерфейс

Устройство может быть установлено снаружи и внутри помещений. Перед использованием необходимо задать номер устройства.
Нажмите **Access Control → Call Settings → Device No.** («Контроль доступа → Настройки вызова → Номер устройства»).

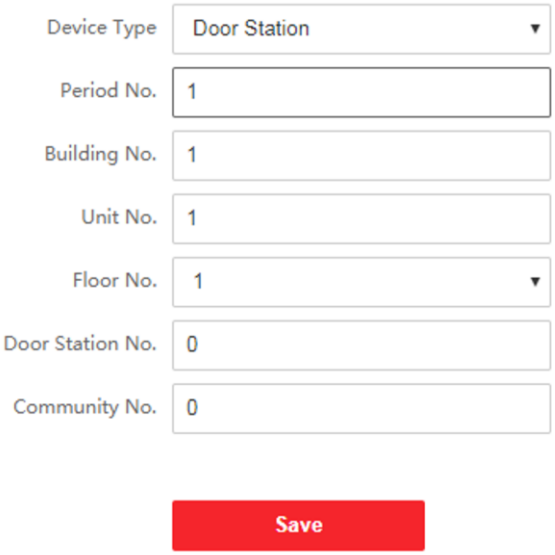


Рисунок 6-2. Настройки № устройства

Если для типа устройства выбран параметр **Door Station** («Вызывная панель»), можно настроить номер этажа, номер вызывной панели, номер микрорайона, номер здания и номер помещения.

Тип устройства

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

Примечание

При изменении типа устройства необходимо перезагрузить устройство.

Номер этажа

Укажите номер этажа, на котором установлено устройство.

Номер вызывной панели

Укажите номер этажа, на котором установлено устройство.

Примечание

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

Номер микрорайона

Укажите номер микрорайона.

Номер здания

Укажите номер здания.

Номер помещения

Укажите номер помещения.

Примечание

При изменении номера необходимо перезагрузить устройство.

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

Номер вызывной панели, установленной снаружи помещения

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

Примечание

При изменении номера необходимо перезагрузить устройство.

Номер микрорайона

Укажите номер микрорайона.

Настройка параметров сети видеодомофона через веб-интерфейс

Можно установить пароль регистрации, IP-адрес пульта консьержа / диспетчера и IP-адрес частного сервера, а также включить протокол 1.0.
Нажмите **Call Settings → Video Intercom Network** («Параметры вызова → Сеть видеодомофона») для перехода на страницу настроек.

Пароль регистрации

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

IP-адрес пульта консьержа / диспетчера

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

IP-адрес частного сервера

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

Включение протокола 1.0

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

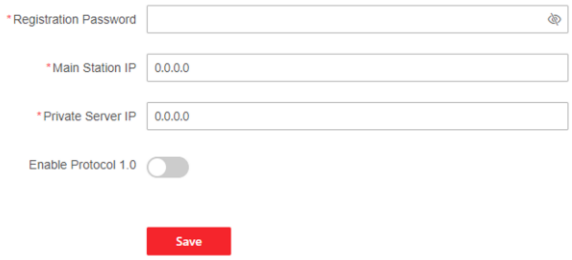


Рисунок 6-3. Сеть видеодомофонии

После настройки можно установить связь между устройствами контроля доступа и вызывной панелью, видеодомофоном, пультом консьержа / диспетчера, платформами и т. д.
Нажмите **Save** («Сохранить»).

Настройка времени связи через веб-интерфейс ПК

Установите макс. время связи.
Перейдите **Access Control** → **Call Settings** → **Call Settings** («Контроль доступа → Настройки вызова → Настройки вызова»).
Введите **Max. Communication Time** («Макс. время связи»). Нажмите **Save** («Сохранить»).

Примечание

Макс. продолжительность связи составляет от 90 до 120 с.

Нажатие кнопки для вызова

Шаги

1. Нажмите **Configuration** → **Intercom** → **Press Button to Call** («Конфигурация → Домофония → Нажатие кнопки для вызова») для перехода на страницу настроек.
2. Выберите **Call Indoor Station** («Вызов видеодомофона»), **Call Specified Indoor Station** («Вызов настроенного видеодомофона»), **Call Management Center** («Вызов центра управления») или **APP** («Приложение»).

Примечание

При выборе **Call Specified Indoor Station** («Вызов настроенного видеодомофона») необходимо ввести номер видеодомофона.

3. Нажмите **Save** («Сохранить»).

Настройка привязки номеров через веб-интерфейс ПК

Установите SIP-номер для помещения. Между устройствами в помещениях можно установить связь по SIP-номеру.

Шаги

1. Перейдите **Access Control** → **Call Settings** → **Number Settings** («Контроль доступа → Настройки вызова → Настройки номера»).



Рисунок 6-4. Настройки номера

2. Нажмите **Add** («Добавить») и введите **Room No.** («№ помещения») и номер телефона **SIP1**.
3. Опционально. Нажмите **Add** («Добавить»), чтобы добавить номер SIP, или нажмите , чтобы удалить номер.
4. Нажмите **Save** («Сохранить»).
5. Опционально. Нажмите **Delete** («Удалить»), чтобы удалить номер помещения и его номер SIP.

6.10 Конфигурация системы

6.10.1 Просмотр информации об устройстве через веб-интерфейс ПК

Можно просмотреть название устройства, номер устройства, язык, модель, серийный номер, версию, количество каналов, входы / выходы, замок, номер регистра, тревожный вход, тревожный выход, емкость устройства и т. д.
Нажмите **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Basic Information** («Система и обслуживание → Конфигурация системы → Система → Настройки системы → Основная информация»), чтобы перейти на соответствующую страницу.

Можно просмотреть название устройства, номер устройства, язык, модель, серийный номер, версию, количество каналов, интерфейсы выходов / входов, состояние замка, номер регистра, тревожный вход, тревожный выход, емкость устройства и т. д.
Нажмите **Upgrade** («Обновить») в разделе версии прошивки, чтобы перейти на страницу обновления и обновить устройство.

6.10.2 Настройка времени

Установите часовой пояс, режим синхронизации, адрес сервера, порт NTP и интервал.
Нажмите **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Time Settings** («Система и обслуживание → Конфигурация системы → Система → Настройки системы → Настройка времени»).

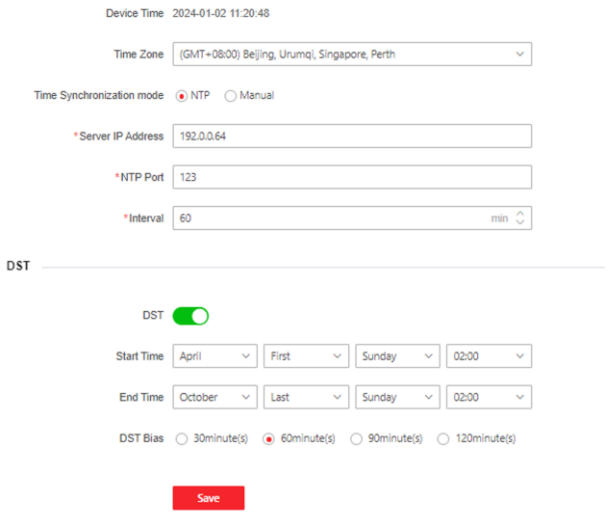


Рисунок 6-5. Настройка времени

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

Часовой пояс

Выберите часовой пояс устройства из выпадающего списка.

Синхронизация времени

NTP

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

Вручную

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

Тип адреса сервера / Адрес сервера / Порт NTP / Интервал

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

6.10.3 Изменение пароля администратора

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **User Management** («Система и обслуживание → Конфигурация системы → Система → Управление пользователем → Управление пользователем»).
2. Нажмите .
3. Введите старый пароль и создайте новый пароль.
4. Подтвердите новый пароль.
5. Нажмите **Save** («Сохранить»).

Предостережение

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

6.10.4 Настройки безопасности учетной записи через веб-интерфейс ПК

Можно изменить контрольные вопросы и ответы или адрес электронной почты для устройства. Если после изменения настроек вы забыли пароль устройства, необходимо ответить на новые вопросы или использовать новый адрес электронной почты для сброса пароля устройства.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **User Management** → **Account Security Settings** («Система и обслуживание → Конфигурация системы → Система → Управление пользователем → Управление пользователем → Настройки безопасности учетной записи»).
2. Установите контрольные вопросы и адрес электронной почты.
3. Введите пароль устройства и нажмите **OK** для подтверждения изменений.

6.10.5 Просмотр информации о постановке / снятии устройства с охраны через веб-интерфейс ПК

Просмотр информации о постановке устройства на охрану и IP-адреса постановки на охрану.
Перейдите **System and Maintenance** → **System Configuration** → **System** → **User Management** → **Arming/Disarming Information** («Система и обслуживание → Конфигурация системы → Система → Управление пользователями → Информация о постановке на охрану / снятии с охраны»).
Можно просмотреть информацию о постановке на охрану/снятии с охраны. Для обновления нажмите кнопку **Refresh** («Обновить»).

6.10.6 Параметры сети

Настройка базовых параметров сети через веб-интерфейс ПК

Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **TCP/IP** («Система и обслуживание → Конфигурация системы → Сеть → Настройки сети → TCP/IP»).
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, Mac-адрес и MTU.
При включении этой функции система автоматически задаст IPv4-адрес, IPv4-маску подсети и IPv4-шлюз.

DNS-сервер

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

Настройка параметров Wi-Fi

Задайте параметры Wi-Fi для беспроводного подключения устройства.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **Wi-Fi** («Система и обслуживание → Конфигурация системы → Сеть → Настройки сети → Wi-Fi»).

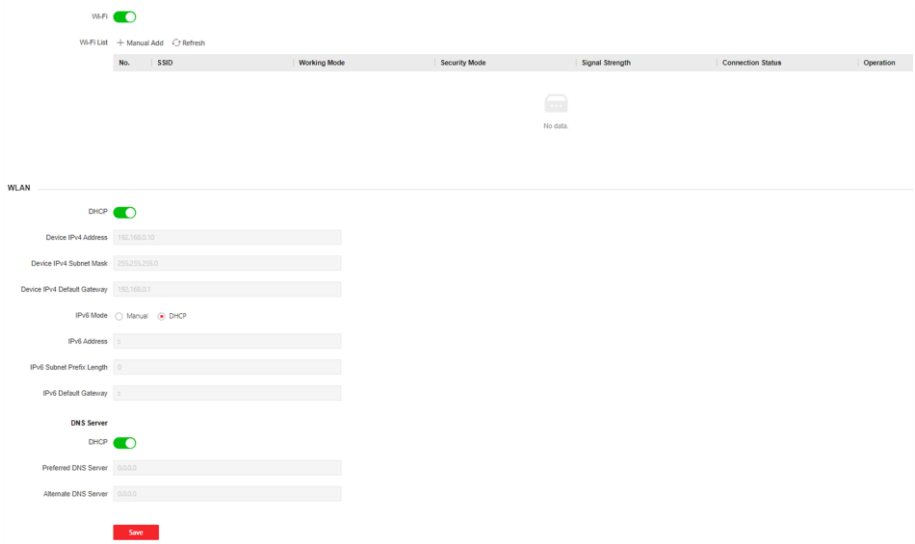


Рисунок 6-6. Страница настройки Wi-Fi

2. Нажмите **Wi-Fi** («Wi-Fi»).
3. Выберите Wi-Fi
   – Нажмите и введите пароль Wi-Fi для подключения.
   – Нажмите **Add** («Добавить») и введите имя, пароль и тип шифрования Wi-Fi. Нажмите **Connect** («Подключить»). Когда Wi-Fi подключен, нажмите **OK**.
4. Опционально. Настройте параметры WLAN.
   1) Настройте IP-адрес, маску подсети и шлюз по умолчанию. Или включите DHCP, и система автоматически задаст IP-адрес, маску подсети и по умолчанию шлюз.
5. Нажмите **Save** («Сохранить»).

Настройка порта через веб-интерфейс ПК

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба»).

Вкл. / выкл. HTTP

Включите функцию HTTP для повышения безопасности посещения браузера.

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **HTTP(S)** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба → HTTP(S)»).

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

Порт HTTP

При входе через браузер необходимо добавить измененный номер порта после адреса. Например, если номер HTTP-порта изменен на 81, необходимо ввести http://192.0.0.65:81 при входе в систему с помощью веб-интерфейса.

Порт HTTPS

Установите порт HTTPS для посещения веб-интерфейса. Но требуется сертификация.

Прослушивание HTTP

Устройство будет отправлять информацию о тревоге на целевой IP-адрес или доменное имя по протоколу HTTP. Целевой IP-адрес или доменное имя должны поддерживать протокол HTTP. Введите целевой IP-адрес или доменное имя, URL-адрес и порт. И выберите тип протокола.

Просмотр порта RTSP через веб-интерфейс ПК

Порт RTSP – это порт протокола потоковой передачи в режиме реального времени.

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **RTSP** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба → RTSP»).

Просмотрите порт.

Настройка WebSocket(s) через веб-интерфейс ПК

Просмотрите порт WebSocket и WebSockets.

Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **WebSocket(s)** («Система и обслуживание → Конфигурация системы → Сеть → Сетевая служба → WebSocket(s)»).

Просмотрите порт WebSocket и WebSockets.

Включение службы SDK

После включения службы SDK устройство может подключиться к серверу SDK.

Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **SDK Server** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → Сервер SDK») для перехода на страницу настроек.

Введите **Server Port** («Порт сервера»).

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

Настройка параметров ISUP через веб-интерфейс ПК

Установите параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги

Примечание

Устройство должно поддерживать данную функцию.

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **ISUP** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → ISUP»).
2. Нажмите **Enable** («Включить»).
3. Установите версию ISUP, адрес сервера, идентификатор устройства и статус ISUP.

Примечание

Если выбрана версия 5.0, необходимо также установить ключ шифрования.

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

Доступ к платформе через веб-интерфейс ПК

Устройствами можно управлять с помощью платформы доступа.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **Guarding Vision** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → 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 a до z, от A до Z) или цифр (от 0 до 9), с учетом регистра. Рекомендуется использовать комбинацию не менее 8 букв или цифр.

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

Настройки учетной записи VoIP

Можно совершать голосовые вызовы по сети.

Шаги

1. Перейдите **System and Maintenance** → **System Configuration** → **Network** → **Device Access** → **VoIP** («Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → VoIP»).
2. Включите **VoIP Gateway** («VoIP-шлюз»).
3. Настройте **Register User Name** («Зарегистрированное имя пользователя»), **Registration Password** («Пароль регистрации»), **Server IP Address** («IP-адрес сервера»), **Server Port** («Порт сервера»), **Expiry Time** («Время истечения срока действия»), **Register Status** («Состояние регистрации»), **Number** («Номер»), **Display User Name** («Отображение имени пользователя»).

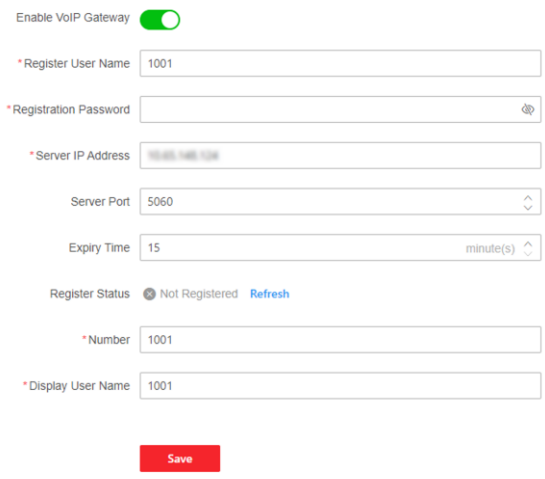


Рисунок 6-7. Настройки учетной записи VoIP

Пароль регистрации

Введите пароль регистрации для связи через SIP-сервер. Пароль регистрации для SIP-сервера обычно задается в настройках SIP пульта консьержа / диспетчера.

IP-адрес сервера

Введите IP-адрес пульта консьержа / диспетчера, используемый для связи VoIP. В настоящее время пульт консьержа / диспетчера используется в качестве SIP-сервера.

Для осуществления связи по этому адресу сервера должны быть зарегистрированы другие устройства домофонии.

Номер / Отображаемое имя пользователя

На экране устройства отображаются номер вызова и имя пользователя.

4. Нажмите **Save** («Сохранить»).

7.10.7 Настройка параметров видео и аудио через веб-интерфейс ПК

Настройка параметров видео через веб-интерфейс

Можно настроить качество, разрешение и другие параметры камеры устройства.

Нажмите **System and Maintenance** → **System Configuration** → **Video/Audio** → **Video** («Система и обслуживание → Конфигурация системы → Видео / аудио → Видео») для перехода на страницу настроек.

Установите название камеры, тип потока, тип видео, разрешение, тип битрейта, качество видео, частоту кадров, максимальный битрейт, кодирование видео и интервал I-кадров.

Нажмите **Save** («Сохранить»).

Настройка параметров звука через веб-интерфейс ПК

Можно настроить громкость устройства.

Перейдите в **System and Maintenance → System Configuration → Video/Audio → Audio** («Система и обслуживание → Конфигурация системы → Видео / аудио → Аудио»).

Переместите ползунок для установки громкости входа и выхода.

Включите **Voice Prompt** («Голосовое предупреждение»).

Нажмите **Save** («Сохранить»).

6.10.8 Настройка параметров изображения

Настройка яркости / контрастности / насыщенности / резкости через веб-интерфейс ПК

Можно настроить параметры изображения, включая яркость, контрастность, насыщенность и резкость на странице просмотра в режиме реального времени.

Нажмите **System and Maintenance** → **System Configuration** → **Image** → **Display Settings** («Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения») для перехода на страницу настроек.

Настройка изображения

Переместите курсор мыши или введите число, чтобы установить яркость, контрастность, насыщенность и резкость.

Нажмите **Restore Default Settings** («Восстановить настройки по умолчанию»), чтобы восстановить настройки по умолчанию.

Настройка LED-подсветки через веб-интерфейс ПК

Можно отрегулировать яркость дополнительной подсветки.

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Image** → **Display Settings** («Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения») для перехода на страницу настроек.
2. Установите тип, режим и яркость дополнительной подсветки.
3. Опционально. Нажмите **Restore Default Settings** («Восстановить настройки по умолчанию»), чтобы восстановить настройки по умолчанию.

Настройка WDR через веб-интерфейс ПК

Нажмите **System and Maintenance** → **System Configuration** → **Image** → **Display Settings** («Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения») для перехода на страницу настроек.

Включить или отключить широкий динамический диапазон. После включения этой функции светлые и темные участки сцены становятся видны более четко.

Нажмите **Restore Default Settings** («Восстановить настройки по умолчанию»), чтобы восстановить настройки по умолчанию.

Настройка видеостандарта через веб-интерфейс ПК

Можно установить видеостандарт на странице просмотра в режиме реального времени.

Нажмите **System and Maintenance** → **System Configuration** → **Image** → **Display Settings** («Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения») для перехода на страницу настроек.

Настройка видео

Установите частоту кадров видео во время удаленного предварительного просмотра. Для вступления новых настроек в силу необходимо перезагрузить устройство.

PAL

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

NTSC

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

Нажмите **Restore Default Settings** («Восстановить настройки по умолчанию»), чтобы восстановить настройки по умолчанию.

6.10.9 Конфигурация доступа

Настройка параметров Wiegand через веб-интерфейс ПК

Можно настроить направление передачи данных интерфейса Wiegand.

Шаги

Примечание

- Некоторые модели устройств не поддерживают данную функцию. Настройка параметров зависит от фактического функционала устройства.
- Параметры Wiegand можно задать только на устройстве, поддерживающем интерфейсную плату.

1. Нажмите **System and Maintenance** → **System Configuration** → **Access Configuration** → **Wiegand Settings** («Система и обслуживание → Конфигурация системы → Конфигурация доступа → Настройки Wiegand»).
2. Нажмите **Wiegand** («Wiegand»), чтобы включить функцию Wiegand.
3. Установите направление передачи данных.

   Вход

   Устройство можно подключать к считывателю карт Wiegand.
4. Нажмите **Save** («Сохранить») для сохранения настроек.

Примечание

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

6.10.10 Настройки учета рабочего времени (УРВ)

Если необходимо регистрировать рабочее время сотрудника, опоздания, ранние уходы, перерывы, прогулы и т. д., то можно добавить сотрудника в группу смен и назначить группе смен расписание смен (правило УРВ, определяющее, как расписание повторяется, тип смены, настройки перерывов и правило считывания карт), чтобы определить параметры УРВ для сотрудников в группе смен.

Отключение функции учета рабочего времени через веб-интерфейс

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

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Platform Attendance** («Система и обслуживание → Конфигурация системы → УРВ через платформу») для перехода на страницу настроек.
2. Отключите **Time and Attendance** («УРВ»).

Результат

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

Настройка параметров учета рабочего времени вручную через веб-интерфейс

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

Перед началом

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

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Platform Attendance** («Система и обслуживание → Конфигурация системы → УРВ через платформу») для перехода на страницу настроек.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual** («Подсчет вручную»).
3. Нажмите **Attendance Status Required** («Требуется УРВ») и укажите продолжительность состояния УРВ.
4. Включите статус УРВ для группы.

Примечание

Статистика УРВ не изменится.

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

Результат

При аутентификации можно вручную выбрать статус УРВ.

Примечание

Если не выбрать статус, аутентификация будет неудачной.

Настройка параметров автоматического учета рабочего времени через веб-интерфейс

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

Перед началом

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

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Platform Attendance** («Система и обслуживание → Конфигурация системы → УРВ через платформу») для перехода на страницу настроек.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Auto** («Автоматически»).
3. Включите **Attendance Status Required** («Требуется УРВ»).
4. Включите статус УРВ для группы.

   Примечание

   Статистика УРВ не изменится.

5. Опционально. Выберите статус и при необходимости измените его название.
6. Установите расписание статуса. Подробная информация представлена в соответствующем разделе.

Настройка параметров автоматического УРВ и УРВ вручную через веб-интерфейс

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

Перед началом

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

Шаги

1. Нажмите **System and Maintenance** → **System Configuration** → **Platform Attendance** («Система и обслуживание → Конфигурация системы → УРВ через платформу») для перехода на страницу настроек.
2. Перейдите в меню **Attendance Mode** («Учет рабочего времени») и выберите **Manual and Auto** («Подсчет автоматически и вручную»).
3. Включите **Attendance Status Required** («Требуется УРВ»).
4. Включите статус УРВ для группы.

> **Примечание**
>
> Статистика УРВ не изменится.

5. Опционально. Выберите статус и при необходимости измените его название.
6. Установите расписание статуса. Подробная информация представлена в соответствующем разделе.

Результат

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

Пример

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

6.11 Пользовательские настройки

6.11.1 Настройка спящего режима через веб-интерфейс ПК

Устройство перейдет в спящий режим по истечении заданного промежутка времени. Эта функция позволяет снизить энергопотребление.

Перейдите **System and Maintenance** → **Preference** → **Screen Display** («Система и обслуживание → Пользовательская настройка → Отображение»).



Рисунок 6-8. Настройки спящего режима

Переместите ползунок **Sleep** («Спящий режим») и установите время.

Нажмите **Save** («Сохранить»).

6.11.2 Настройка панели аутентификации через веб-интерфейс ПК

Настройте модули на странице / панели аутентификации.

Шаги

1. Перейдите **System and Maintenance** → **Preference** → **Screen Display** («Система и обслуживание → Пользовательская настройка → Отображение»).
2. Выберите **Application Mode** («Режим применения»).

   Режим аутентификации

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

   Обычный режим

   После выбора этого режима отображение страницы аутентификации в реальном времени будет отключено. Имя, идентификатор сотрудника, изображение лица будут скрыты после аутентификации.
3. Нажмите **Apply** («Применить»).

6.11.3 Настройка отображения уведомлений через веб-интерфейс ПК

Можно настроить отображение уведомления для устройства.

Перейдите **System and Maintenance** → **Preference** → **Notice Publication** («Система и обслуживание → Пользовательская настройка → Отображение уведомлений»).

Управление темой

Нажмите **Media Library Management** («Управление медиабиблиотекой») → **+** , чтобы загрузить изображение с локального ПК.

Примечание

Поддерживается только формат JPG и JPEG. Каждое изображение должно быть размером менее 1 МБ и с разрешением до 1920 × 1280.

Добавление программы

Можно задать название программы и выбрать тип программы.

Изображение

Чтобы добавить изображение, нажмите кнопку **+**.

6.11.4 Настройка голосовых подсказок через веб-интерфейс ПК

Также можно настроить голосовую подсказку для устройств.

Шаги

1. Перейдите **System and Maintenance** → **Preference** → **Custom Prompt** («Система и обслуживание → Пользовательская настройка → Пользовательская настройка подсказки»).

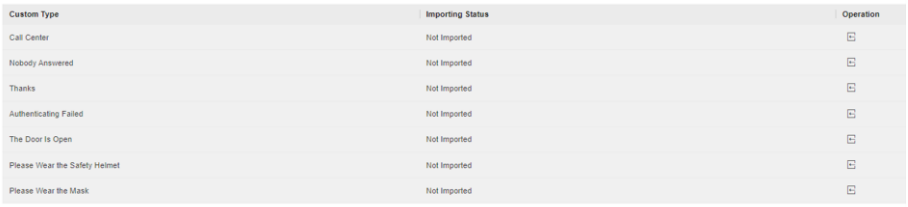


Рисунок 6-9. Пользовательская настройка подсказок

2. Нажмите → и импортируйте аудиофайл с локального компьютера.

Примечание

Загруженный аудиофайл должен иметь размер не более 512 КБ, в формате WAV.

6.11.5 Настройка текста результата аутентификации через веб-интерфейс ПК

Шаги

1. Перейдите **System and Maintenance** → **Preference** → **Authentication Result Text** («Система и обслуживание → Пользовательская настройка → Текст результата аутентификации»).

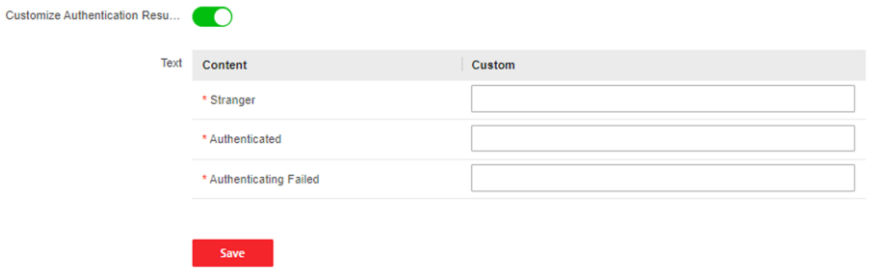


Рисунок 6-10. Текст результата аутентификации

2. Включить **Customize Authentication Result Text** («Настройка текста результата аутентификации»).
3. Введите текст.
4. Нажмите **Save** («Сохранить»).

6.12 Система и обслуживание

6.12.1 Перезагрузка

Перезагрузите устройство.

Нажмите **System and Maintenance** → **Maintenance** → **Restart** («Система и обслуживание → Обслуживание → Перезагрузка») для перехода на страницу настроек.

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

6.12.2 Обновление

Локальное обновление через веб-интерфейс ПК

Можно обновить устройство локально.

Нажмите **System and Maintenance** → **Maintenance** → **Upgrade** («Система и обслуживание → Обслуживание → Обновление») для перехода на страницу настроек.

Выберите тип обновления из выпадающего списка. Нажмите  и выберите файл обновления с локального ПК. Нажмите **Upgrade** («Обновить»), чтобы начать обновление.

Онлайн обновление через веб-интерфейс ПК

Можно обновить устройство онлайн.

Нажмите **System and Maintenance** → **Maintenance** → **Upgrade** («Система и обслуживание → Обслуживание → Обновление») для перехода на страницу настроек.

Нажмите **Check for Updates** («Проверить обновления»), чтобы проверить наличие обновленных версий.

Если устройство подключено к сети и добавлено в приложение Guarding Vision, можно нажать **Device Upgrade** → **Online Upgrade** («Обновление устройства → Онлайн обновление») на устройстве для обновления, когда в приложении Guarding Vision появится обновленная версия.

6.12.3 Восстановление настроек

Восстановление заводских настроек через веб-интерфейс

Можно восстановить устройство до заводских настроек.

Нажмите **System and Maintenance** → **Maintenance** → **Backup and Reset** («Система и обслуживание → Обслуживание → Резервное копирование и сброс») для перехода на страницу настроек.

Нажмите **Restore All** («Восстановить все»), и все параметры будут восстановлены до заводских настроек. Перед первым входом в систему необходимо активировать устройство.

Восстановление настроек по умолчанию через веб-интерфейс ПК

Можно восстановить устройство до настроек по умолчанию.

Нажмите **System and Maintenance** → **Maintenance** → **Backup and Reset** («Система и обслуживание → Обслуживание → Резервное копирование и сброс») для перехода на страницу настроек.

Нажмите **Restore** («Восстановить»), и устройство будет восстановлено до настроек по умолчанию, за исключением IP-адреса устройства и информации о пользователе.

6.12.4 Экспорт параметров устройства через веб-интерфейс ПК

Экспорт параметров устройства.

Перейдите **System and Maintenance** → **Maintenance** → **Backup and Reset** («Система и обслуживание → Обслуживание → Резервное копирование и сброс»).

Резервное копирование

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

Примечание

Экспортируйте параметры устройства и импортируйте эти параметры на другие устройства.

6.12.5 Импорт параметров устройства через веб-интерфейс ПК

Импорт параметров конфигурации.

Перейдите **System and Maintenance** → **Maintenance** → **Backup and Reset** («Система и обслуживание → Обслуживание → Резервное копирование и сброс»).

Импорт файлов настройки

Нажмите и выберите файл с локального компьютера. Нажмите **Import** («Импорт»).

6.12.6 Отладка устройства

Можно настроить параметры отладки устройства.

Вкл. / выкл. SSH через веб-интерфейс

Можно включить SSH для удаленной отладки.

Нажмите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Log for Debugging** («Система и обслуживание → Обслуживание → Отладка устройства → Журнал отладки»).

Включить SSH

SSH используется для удаленной отладки. Если служба не требуется, рекомендуется отключить SSH для повышения безопасности.

Печать журнала устройства через веб-интерфейс ПК

Можно распечатать журнал устройства.

Нажмите **System and Maintenance** → **Maintenance** → **Log** («Система и обслуживание → Обслуживание → Журнал») для перехода на страницу настроек.

Нажмите **Export** («Экспорт»), чтобы распечатать журнал устройства.

Захват сетевого пакета через веб-интерфейс ПК

Установите длительность и размер захватываемого пакета и выполните захват. Можно просмотреть журнал и выполнить отладку в соответствии с результатами захвата.

Перейдите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Log for Debugging** («Система и обслуживание → Обслуживание → Отладка устройства → Журнал отладки»).

Настройте **Capture Packet Duration** («Длительность захвата пакета») и **Capture Packet Size** («Размер захвата пакета»), затем нажмите **Start Capture** («Начать захват»).

Тестирование протокола через веб-интерфейс ПК

Выберите адрес протокола и введите протокол для тестирования. Можно выполнять отладку устройства в соответствии с заголовком ответа и полученным результатом.

Перейдите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Protocol Testing** («Система и обслуживание → Обслуживание → Отладка устройства → Тестирование протокола»).

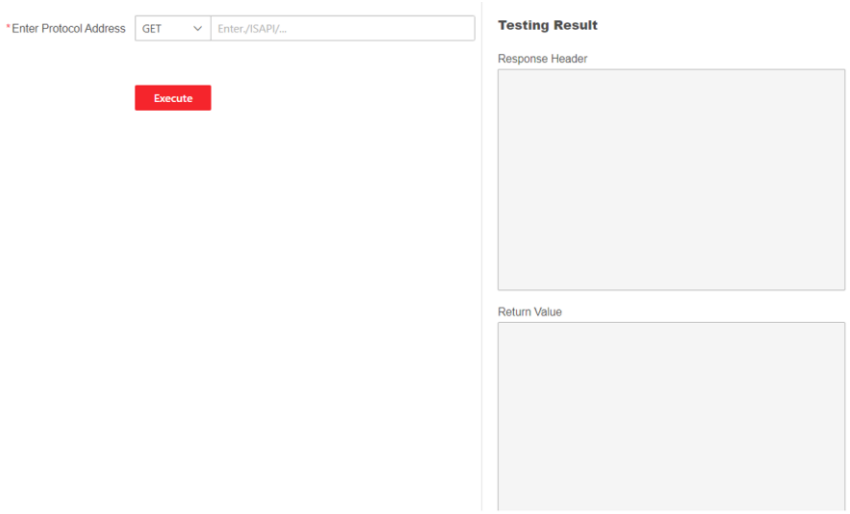


Рисунок 6-11. Тестирование протокола

Выберите адрес протокола и введите протокол. Нажмите **Execute** («Выполнить»).

Выполняйте отладку устройства в соответствии с заголовком ответа и полученным результатом.

Диагностика сети через веб-интерфейс ПК

Введите IP-адрес устройства или доменное имя, чтобы выполнить настройку PING. Выполните отладку сети в соответствии с результатом PING.

Перейдите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Network Diagnosis** («Система и обслуживание → Обслуживание → Отладка устройства → Диагностика сети»).

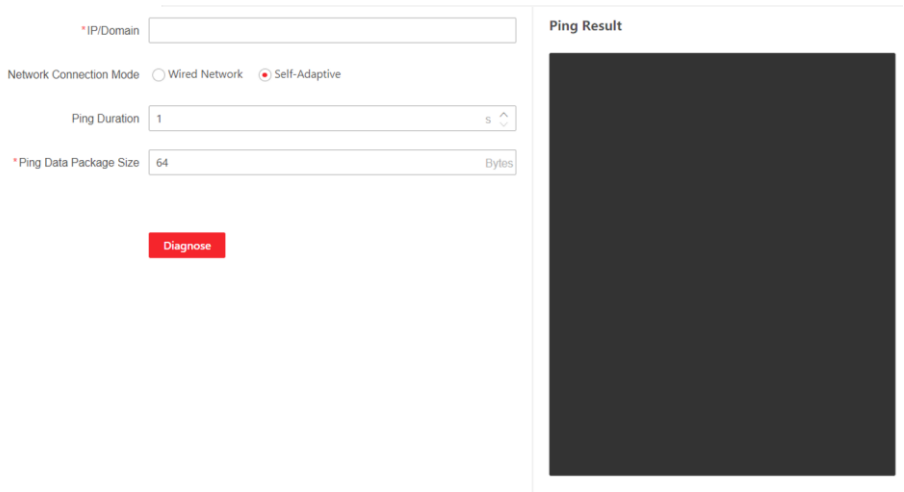


Рисунок 6-12. Диагностика сети

Введите IP-адрес устройства для выполнения операции PING, выберите режим сетевого подключения, продолжительность PING и размер пакета данных PING (рекомендуется использовать параметры по умолчанию). Нажмите **Diagnose** («Диагностика»). Результат будет отображен в разделе **PING Result** («Результаты PING»).

Настройка службы проверки на проникновение в сеть через веб-интерфейс ПК

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

Шаги

1. Перейдите **System and Maintenance** → **Maintenance** → **Device Debugging** → **Network Penetration Service** («Система и обслуживание → Обслуживание → Отладка устройства → Служба проверки на проникновение в сеть»).
2. Переведите ползунок **Enable Penetration Service** («Включить службу проверки на проникновение»).
3. Установите **Server IP Address** («IP-адрес сервера») и **Server Port** («Порт сервера»). Создайте **User Name** («Имя пользователя») и **Password** («Пароль»)
4. Опционально. Можно настроить **Heartbeat Timeout** («Период цикла Heartbeat»). Диапазон значений: от 1 до 6000.
5. Опционально. Можно посмотреть состояние службы проверки на проникновение. Нажмите **Refresh** («Обновить»), чтобы обновить состояние.
6. Нажмите **Save** («Сохранить»).

Примечание

Служба проверки на проникновение будет автоматически отключена через 48 часов.

6.12.7 Просмотр журнала через веб-интерфейс ПК

Можно искать и просматривать журналы устройства.

Перейдите **System and Maintenance** → **Maintenance** → **Log** («Система и обслуживание → Обслуживание → Журнал»).

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

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

6.12.8 Расширенные настройки через веб-интерфейс ПК

Можно настроить параметры лица, параметры ладони и просмотреть информацию о версии.

Перейдите **System and Maintenance** → **Maintenance** → **Advanced Settings** («Система и обслуживание → Обслуживание → Расширенные настройки»).

Введите пароль активации устройства и нажмите **Enter**.

Параметры изображения лица

Включите **Custom Anti-Spoofing Detection** («Настройка детекции подлинности биометрических данных (антиспуфинг)») и установите **Anti-Spoofing Detection Threshold 1:1** («Пороговое значение детекции подлинности биометрических данных (антиспуфинг) 1:1»), **Anti-Spoofing Detection Threshold 1:N** («Пороговое значение детекции подлинности биометрических данных (антиспуфинг) 1:N»).

Включите **Lock Face for Authentication** («Блокировка лица для аутентификации») и установите **Lock Duration** («Длительность блокировки»). После достижения лимита неудачных попыток детекции подлинности биометрических данных лица, распознавание лица будет заблокировано на заданный период блокировки.

Нажмите **Save** («Сохранить»).

Информация о версии устройства

Здесь можно просмотреть информацию о различных версиях.

6.12.9 Управление безопасностью

Установите уровень безопасности при входе в веб-интерфейс ПК.

Перейдите **System and Maintenance** → **Safe** → **Security Service** («Система и обслуживание → Безопасность → Служба безопасности»).

Режим безопасности

Высокий уровень безопасности при входе в систему и проверке информации о пользователе.

Режим совместимости

Совместимость со старым методом проверки пользователя.

Нажмите **Save** («Сохранить»).

6.12.10 Управление сертификатами

Помогает управлять сертификатами сервера/клиента и сертификатом CA.

Примечание

Данная функция поддерживается только у определенных моделей устройств.

Создание и импорт самозаверенного сертификата

Шаги

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

Импорт другого авторизованного сертификата

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

Шаги

1. Перейдите **System and Maintenance** → **Safe** → **Certificate Management** («Система и обслуживание → Безопасность → Управление сертификатами»).
2. В областях **Import Key** («Импорт ключа») и **Import Communication Certificate** («Импорт сертификата связи») выберите тип сертификата и загрузите сертификат.
3. Нажмите **Import** («Импорт»).

Импорт сертификата CA

Перед началом

Заранее подготовьте сертификат центра сертификации (CA).

Шаги

1. Перейдите **System and Maintenance** → **Safe** → **Certificate Management** («Система и обслуживание → Безопасность → Управление сертификатами»).
2. Создайте идентификатор в области **Import CA Certificate** («Импорт сертификата CA»).

Примечание

Идентификатор сертификата не может совпадать с идентификатором уже существующих сертификатов.

3. Загрузите файл сертификата с локального ПК.
4. Нажмите **Import** («Импорт»).

Правовая информация

Информация о документе

- Документ 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. Актуальная версия настоящего документа представлена на веб-сайте компании. Если не оговорено иное, компания не предоставляет никаких гарантий, явных или подразумеваемых.
- 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.

Торговая марка

Все торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

ПРАВОВАЯ ИНФОРМАЦИЯ

- В МАКСИМАЛЬНОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, НАСТОЯЩИЙ ДОКУМЕНТ И ОПИСАННЫЙ ПРОДУКТ С ЕГО АППАРАТНЫМ, ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ И ПРОШИВКОЙ ПРЕДОСТАВЛЯЮТСЯ «КАК ЕСТЬ» И «СО ВСЕМИ НЕИСПРАВНОСТЯМИ И ОШИБКАМИ». НАША КОМПАНИЯ НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, КАСАТЕЛЬНО УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ. ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА НЕСЕТ ПОЛЬЗОВАТЕЛЬ. НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД ПОТРЕБИТЕЛЕМ ЗА КАКОЙ-ЛИБО СЛУЧАЙНЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ, ВКЛЮЧАЯ УБЫТКИ ИЗ-ЗА ПОТЕРИ ПРИБЫЛИ, ПЕРЕРЫВА В ДЕЯТЕЛЬНОСТИ ИЛИ ПОТЕРИ ДАННЫХ ИЛИ ДОКУМЕНТАЦИИ, ПО ПРИЧИНЕ НАРУШЕНИЯ УСЛОВИЙ КОНТРАКТА, ТРЕБОВАНИЙ (ВКЛЮЧАЯ ХАЛАТНОСТЬ), УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ ИНОГО, В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ НАШЕЙ КОМПАНИИ БЫЛО ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.
- ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ; НАША КОМПАНИЯ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, НАША КОМПАНИЯ ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО.

- ВЫ СОГЛАШАЕТЕСЬ ИСПОЛЬЗОВАТЬ ДАННЫЙ ПРОДУКТ В СООТВЕТСТВИИ СО ВСЕМИ ПРИМЕНИМЫМИ ЗАКОНАМИ, И ВЫ НЕСЕТЕ ЕДИНОЛИЧНУЮ ОТВЕТСТВЕННОСТЬ ЗА ОБЕСПЕЧЕНИЕ ТОГО, ЧТОБЫ ВАШЕ ИСПОЛЬЗОВАНИЕ СООТВЕТСТВОВАЛО ПРИМЕНИМЫМ ЗАКОНАМ. В ЧАСТНОСТИ, ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ДАННОГО ПРОДУКТА ТАКИМ ОБРАЗОМ, КОТОРЫЙ НЕ НАРУШАЕТ ПРАВА ТРЕТЬИХ ЛИЦ, ВКЛЮЧАЯ, БЕЗ ОГРАНИЧЕНИЙ, ПРАВА НА ПУБЛИЧНОСТЬ, ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ ИЛИ ПРАВА НА ЗАЩИТУ ДАННЫХ И ДРУГИЕ ПРАВА НА КОНФИДЕНЦИАЛЬНОСТЬ. ВЫ ОБЯЗУЕТЕСЬ НЕ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В ЗАПРЕЩЕННЫХ ЦЕЛЯХ, ВКЛЮЧАЯ РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ, РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ХИМИЧЕСКОГО ИЛИ БИОЛОГИЧЕСКОГО ОРУЖИЯ, ЛЮБУЮ ДЕЯТЕЛЬНОСТЬ, СВЯЗАННУЮ С ЯДЕРНЫМИ ВЗРЫВЧАТЫМИ ВЕЩЕСТВАМИ, НЕБЕЗОПАСНЫМ ЯДЕРНЫМ ТОПЛИВНЫМ ЦИКЛОМ ИЛИ НАРУШАЮЩУЮ ПРАВА ЧЕЛОВЕКА.
- В СЛУЧАЕ ВОЗНИКНОВЕНИЯ ПРОТИВОРЕЧИЙ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.

Защита данных

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

A. Условные обозначения

В настоящем документе используются следующие символы.

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

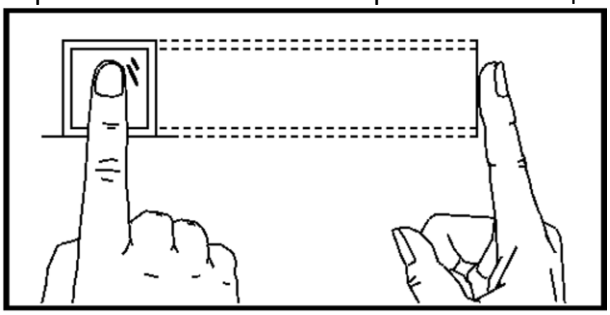
B. Советы по сканированию отпечатков пальцев

Рекомендуемый палец

Рекомендуется использовать большой, указательный или средний палец.

Правильное сканирование

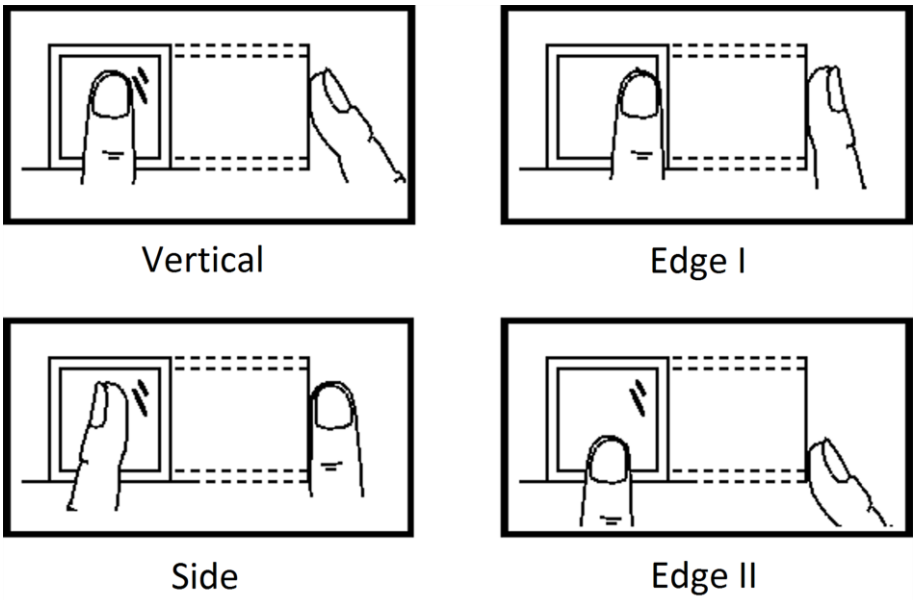
На рисунке ниже показан правильный способ сканирования пальца:



Палец необходимо прижать горизонтально к сканеру. Центр сканируемого пальца должен совпадать с центром сканера.

Неправильное сканирование

Приведенные ниже рисунки показывают неверные способы сканирования отпечатков пальцев:



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.

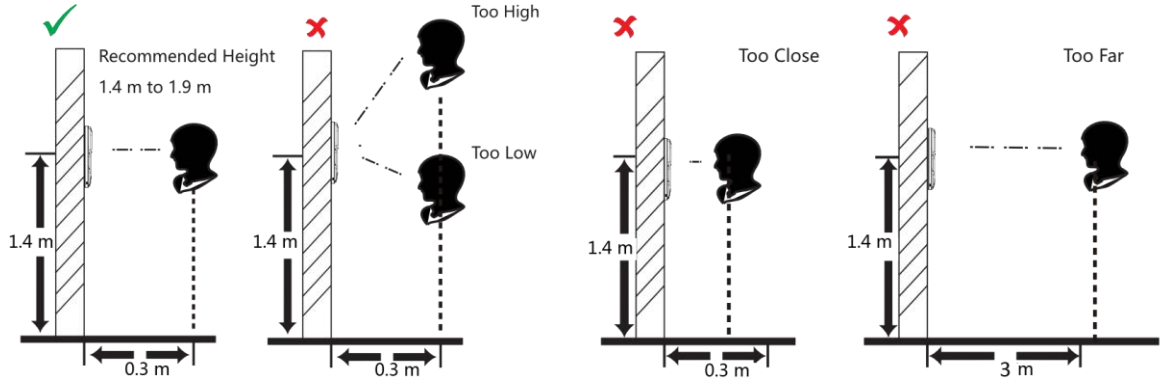
Другое

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.

C. Советы по сбору / сравнению изображений лиц

Положение при сборе или сравнении изображения лица:

Положения (рекомендуемое расстояние: 0.3 м)



Английский язык	Русский язык
Recommended Height: 1.4 m to 1.9 m	Рекомендуемая высота: от 1.4 до 1.9 м
Too High	Слишком высоко
Too Low	Слишком низко
Too Close	Слишком близко
Too Far	Слишком далеко

Выражение лица

- Сохраняйте свое естественное выражение лица при сборе или сравнении изображений лиц, как это показано на рисунке ниже.



- Не надевайте шляпу, солнцезащитные очки или другие аксессуары, которые могут повлиять на функцию распознавания лиц.
- Убедитесь, что волосы не закрывают глаза, уши и т. д., также запрещается яркий макияж.

Положение лица

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



Английский язык	**Русский язык**
Correct	Верно
Tilt	Наклоните набок
Side	Поверните боком
Raise	Поднимите
Bow	Опустите

Размер

Убедитесь, что ваше лицо находится в середине окна сбора данных.



Английский язык	**Русский язык**
Correct	Правильно
Too Close	Слишком близко
Too Far	Слишком далеко

D. Рекомендации по среде установки

1. Номинальное значение освещенности источника света



Свеча: 10 лк

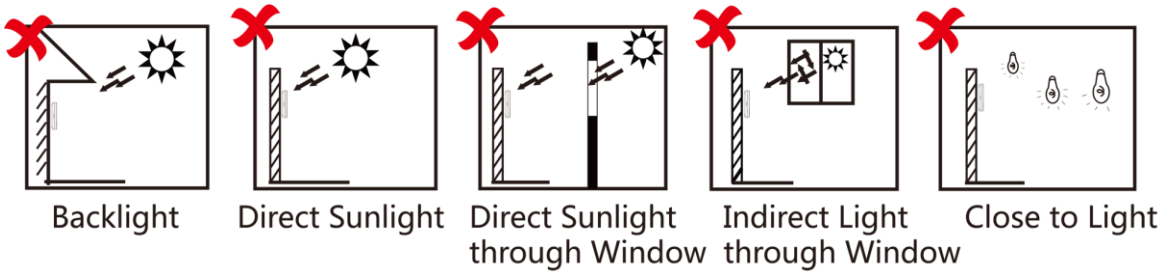


Лампа: 100 ~ 850 лк



Солнечный свет: свыше 1200 лк

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



Английский язык	**Русский язык**
Backlight	Сильная задняя засветка
Direct Sunlight	Прямые солнечные лучи
Direct Sunlight through Window	Прямые солнечные лучи, падающие через окно
Indirect Light through Window	Рассеянные солнечные лучи, падающие через окно
Close to Light	Близко расположенный источник света

E. Размеры

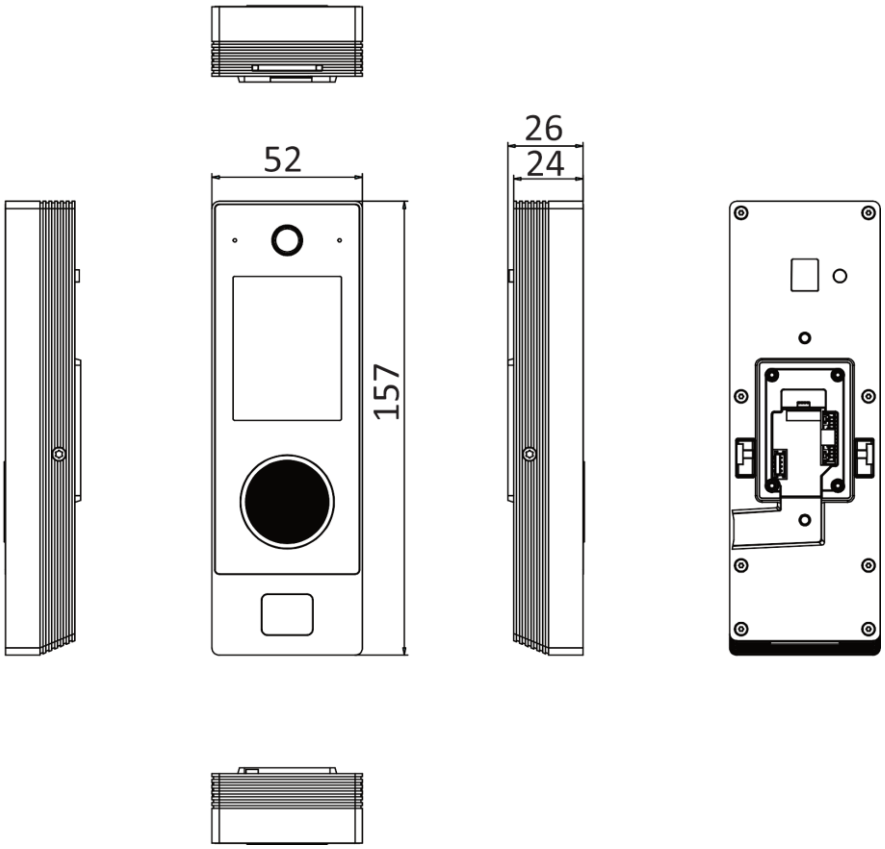


Рисунок E-1. Размеры 1

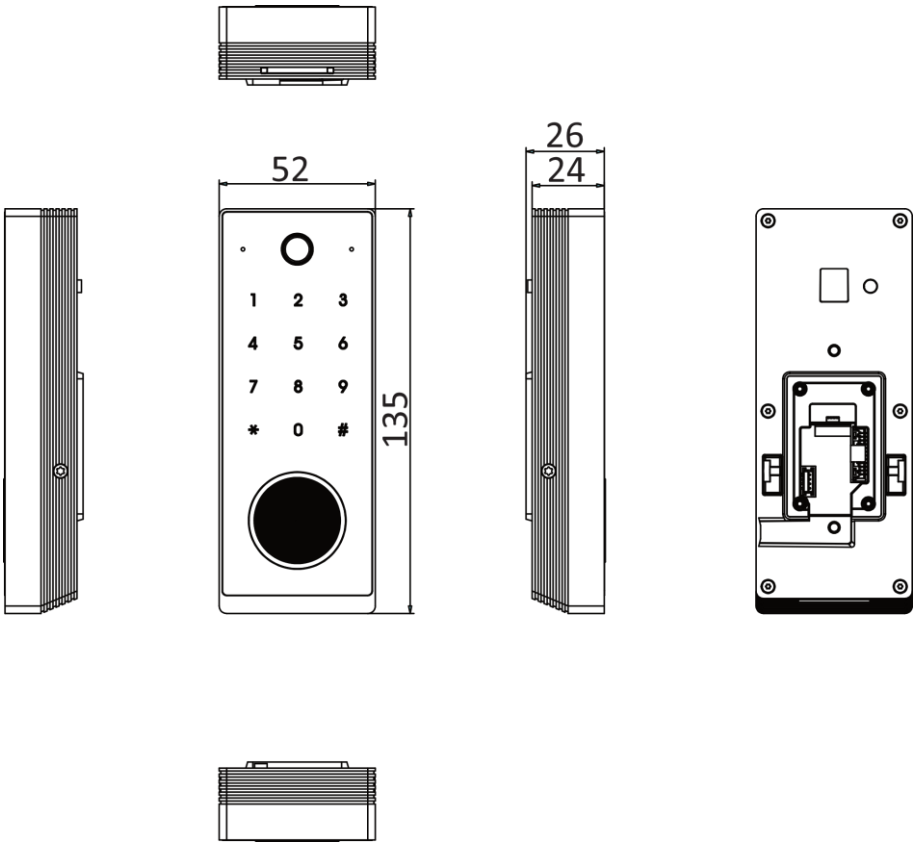


Рисунок Е-2. Размеры 2