Контроллер доступа с распознаванием лиц

Краткое руководство пользователя

B1.0.2

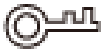
Предисловие

Общий

В этом руководстве описывается установка и эксплуатация контроллера доступа с распознаванием лиц (далее именуемого «контроллер доступа»). Внимательно прочтите перед использованием устройства и сохраните руководство для дальнейшего использования.

Инструкции по технике безопасности

В руководстве могут встречаться следующие сигнальные слова.

Сигнальные слова	Значение
 DANGER	Указывает на высокую потенциальную опасность, которая, если ее не предотвратить, приведет к смерти или серьезным травмам.
 WARNING	Указывает на среднюю или низкую потенциальную опасность, которая, если ее не избежать, может привести к легкой или средней травме.
 CAUTION	Указывает на потенциальный риск, который, если его не предотвратить, может привести к повреждению имущества, потере данных, снижению производительности или непредсказуемым результатам.
 TIPS	Предоставляет методы, которые помогут вам решить проблему или сэкономить время.
 NOTE	Предоставляет дополнительную информацию в качестве дополнения к тексту.

История изменений

Версия	Содержание пересмотра	Время выпуска
B1.0.2	Обновлен внешний вид изображение устройства.	Апрель 2023 г.
Версия 1.0.1	Обновлено приложение.	Февраль 2023 г.
Версия 1.0.0	Первый выпуск.	Октябрь 2022 г.

Уведомление о защите конфиденциальности

Как пользователь устройства или контроллер данных, вы можете собирать персональные данные других лиц, такие как их лицо, отпечатки пальцев и номерной знак. Вам необходимо соблюдать местные законы и правила о защите конфиденциальности, чтобы защищать законные права и интересы других лиц, реализуя меры, которые включают, но не ограничиваются: предоставление четкой и видимой идентификации для информирования людей о существовании зоны наблюдения и предоставление необходимой контактной информации.

О руководстве

- Руководство носит исключительно справочный характер. Между руководством и продуктом могут быть обнаружены незначительные различия.
- Мы не несем ответственности за убытки, возникшие в результате эксплуатации изделия способами, не соответствующими руководству.
- Руководство будет обновляться в соответствии с последними законами и правилами соответствующих юрисдикций. Для получения подробной информации см. бумажное руководство пользователя, используйте наш CD-ROM, отсканируйте QR-код или посетите наш официальный веб-сайт. Руководство предназначено только для справки. Между электронной и бумажной версиями могут быть обнаружены незначительные различия.

- Все конструкции и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта могут привести к появлению некоторых различий между фактическим продуктом и руководством. Пожалуйста, свяжитесь со службой поддержки клиентов для получения последней версии программы и дополнительной документации.
- Могут быть ошибки в печати или отклонения в описании функций, операций и технических данных. В случае возникновения сомнений или споров мы оставляем за собой право окончательного объяснения.
- Обновите программное обеспечение считывателя или попробуйте другое популярное программное обеспечение считывателя, если руководство (в формате PDF) не открывается.
- Все товарные знаки, зарегистрированные товарные знаки и названия компаний в руководстве являются собственностью их владельцев.
- Пожалуйста, посетите наш веб-сайт, обратитесь к поставщику или в службу поддержки клиентов, если при использовании устройства возникли какие-либо проблемы.
- В случае возникновения каких-либо неопределенностей или разногласий мы оставляем за собой право окончательного разъяснения.

Важные меры предосторожности и предупреждения

В этом разделе представлен контент, охватывающий правильное обращение с контроллером доступа, предотвращение опасностей и предотвращение повреждения имущества. Внимательно прочтите перед использованием контроллера доступа и следуйте инструкциям при его использовании.

Требования к транспортировке

Транспортируйте, используйте и храните контроллер доступа при допустимых условиях влажности и температуры.

Требования к хранению

Храните контроллер доступа при допустимых условиях влажности и температуры.

Требования к установке

- Не подключайте адаптер питания к контроллеру доступа, когда адаптер включен.
- Строго соблюдайте местные правила и стандарты электробезопасности. Убедитесь, что напряжение окружающей среды стабильно и соответствует требованиям к электропитанию контроллера доступа.
- Не подключайте контроллер доступа к двум или более типам источников питания, чтобы избежать повреждения контроллера доступа.
- Неправильное использование аккумулятора может привести к возгоранию или взрыву.

- Персонал, работающий на высоте, должен принимать все необходимые меры для обеспечения личной безопасности, включая ношение каски и ремней безопасности.
- Не размещайте контроллер доступа в местах, подверженных воздействию солнечного света или вблизи источников тепла.
- Берегите контроллер доступа от влаги, пыли и копоти.
- Установите контроллер доступа на устойчивую поверхность, чтобы предотвратить его падение.
- Устанавливайте контроллер доступа в хорошо проветриваемом месте и не блокируйте его вентиляцию.
- Используйте адаптер или блок питания для шкафа, предоставленный производителем.
- Используйте шнуры питания, рекомендованные для вашего региона и соответствующие номинальным характеристикам мощности.
- Источник питания должен соответствовать требованиям ES1 в стандарте IEC 62368-1 и быть не выше PS2. Обратите внимание, что требования к источнику питания зависят от этикетки контроллера доступа.
- Контроллер доступа — это электроприбор класса I. Убедитесь, что источник питания контроллера доступа подключен к розетке с защитным заземлением.

Требования к эксплуатации

- Перед использованием проверьте правильность электропитания.
- Не отсоединяйте шнур питания сбоку контроллера доступа, пока адаптер включен.
- Эксплуатируйте контроллер доступа в пределах номинального диапазона входной и выходной мощности.

- Используйте контроллер доступа при допустимых условиях влажности и температуры.
- Не допускайте попадания жидкости на контроллер доступа и не допускайте ее попадания на него. Убедитесь, что на контроллере доступа нет предметов, наполненных жидкостью, чтобы предотвратить попадание жидкости в контроллер.
- Не разбирайте контроллер доступа без профессиональных инструкций.

Оглавление

Предисловие.....я **Важные меры предосторожности и предупреждения**..... III **1 Внешний вид**.....1

2. Электропроводка и монтаж.....2

2.1 Электропроводка.....2

2.2 Требования к установке..... 3

2.3 Процесс установки..... 4

2.3.1 Настенное крепление..... 4

2.3.2 86 Крепление коробки..... 5

3 локальные конфигурации..... 7

3.1 Инициализация.....7

3.2 Добавление новых пользователей.....7

4 веб-конфигурации.....10

4.1 Инициализация.....10

4.2 Вход в систему.....11

Приложение 1. Важные моменты эксплуатации домофона.....12

Приложение 2. Важные моменты сканирования QR-кода.....13

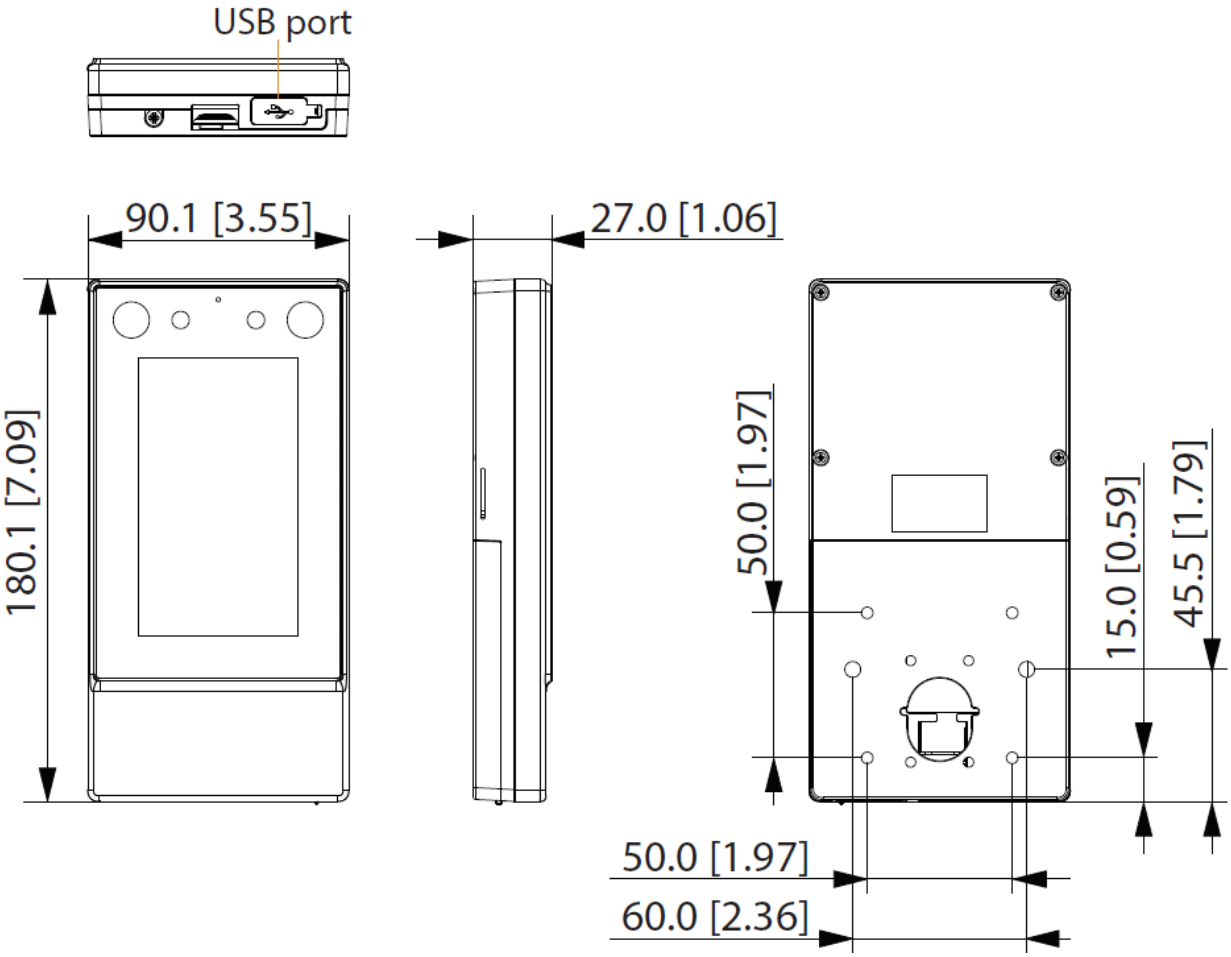
Приложение 3. Важные моменты регистрации лица.....14

Приложение 4 Рекомендации по кибербезопасности.....17

1 Внешний вид

Внешний вид передней панели может отличаться в зависимости от модели контроллера доступа.

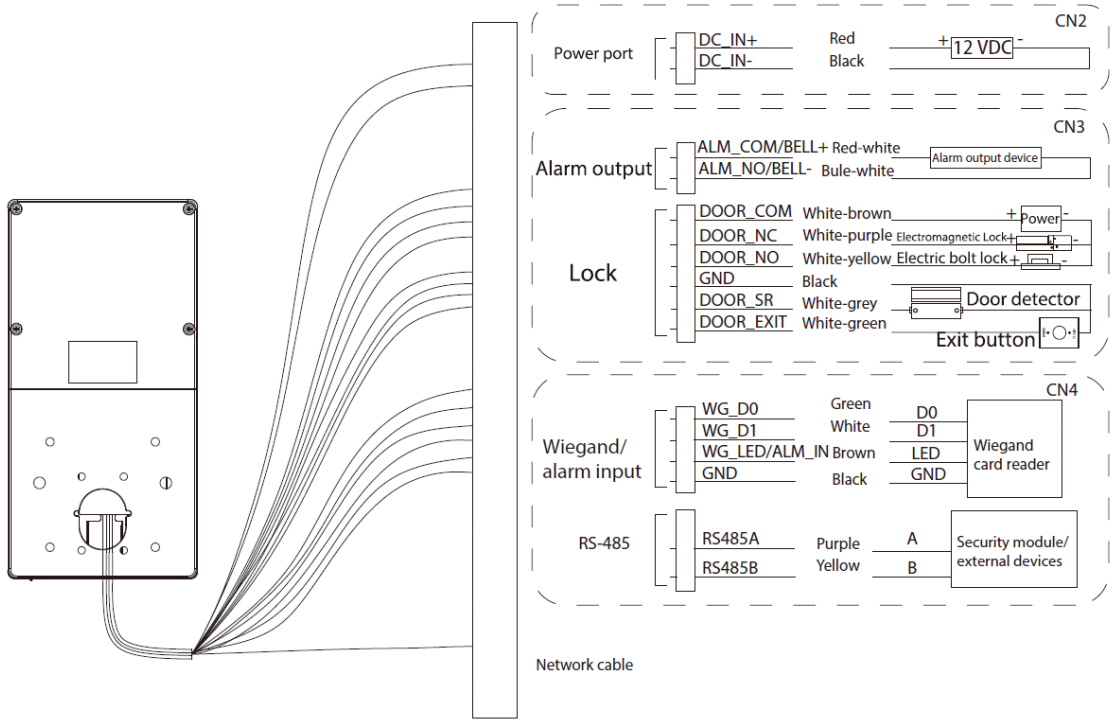
Рисунок 1-1 Внешний вид контроллера доступа (единица измерения: мм [дюйм])



2. Электропроводка и монтаж

2.1 Электропроводка

Рисунок 2-1. Схема подключения контроллера доступа.



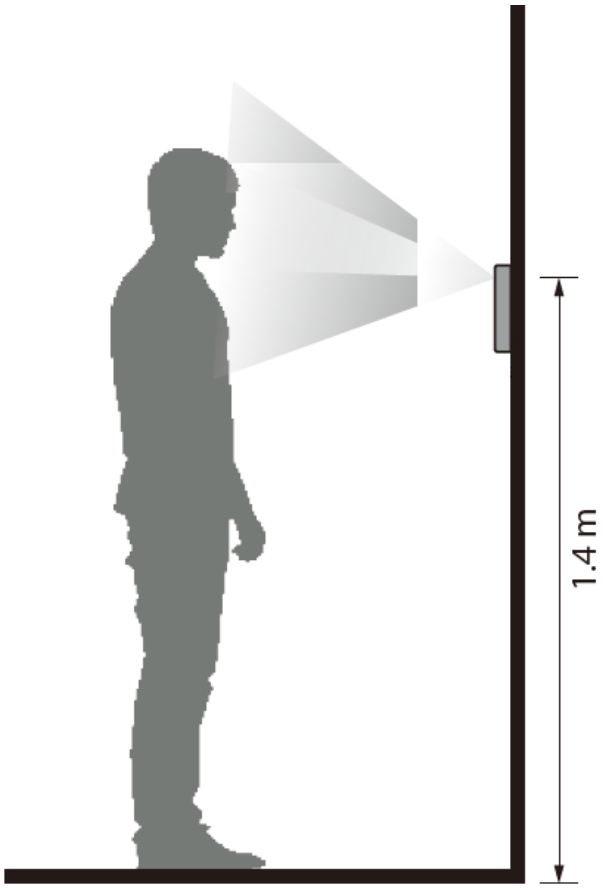
- Провод светодиода и входной провод сигнализации одинаковы, а провод звонка и выходной провод сигнализации одинаковы. одинаковый.
- Если вы хотите подключить внешний модуль безопасности, выберите**Связь**>**Последовательный порт**>**RS-485** **Настройки**>**Модуль безопасности**. Модуль безопасности необходимо приобретать отдельно. клиенты.
- При включении модуля безопасности кнопка выхода, управление замком и вход сигнализации будут активны. не будет эффективным.

2.2 Требования к установке

- Освещенность на расстоянии 0,5 метра от контроллера доступа должна быть не менее 100 люкс.
- Мы рекомендуем устанавливать контроллер доступа в помещении, на расстоянии не менее 3 метров от окон. и дверей, а также на расстоянии 2 метров от источника света.
- Избегайте контрового света, прямых солнечных лучей, близкого и косого света.

Высота установки

Рисунок 2-2 Требования к высоте установки

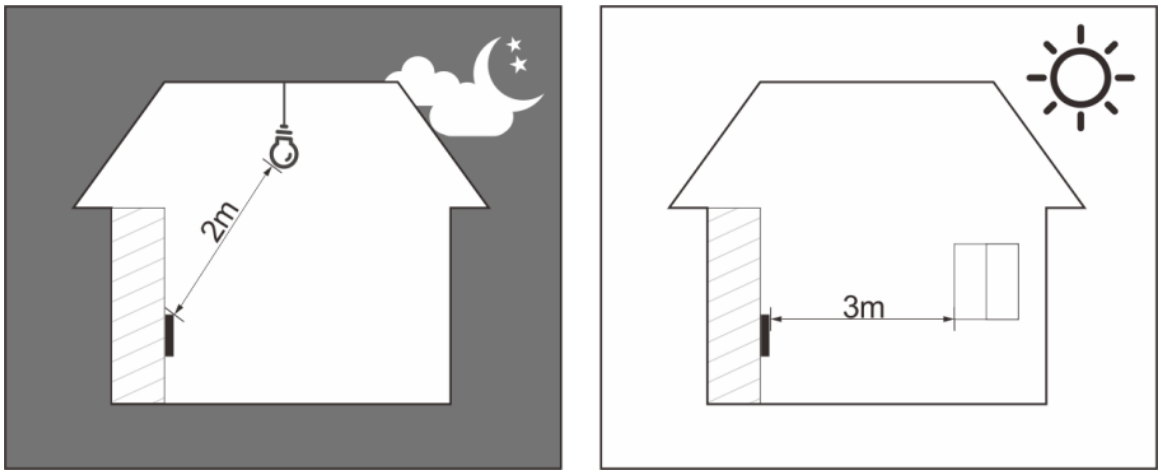


Требования к окружающему освещению

Рисунок 2-3 Требования к окружающему освещению

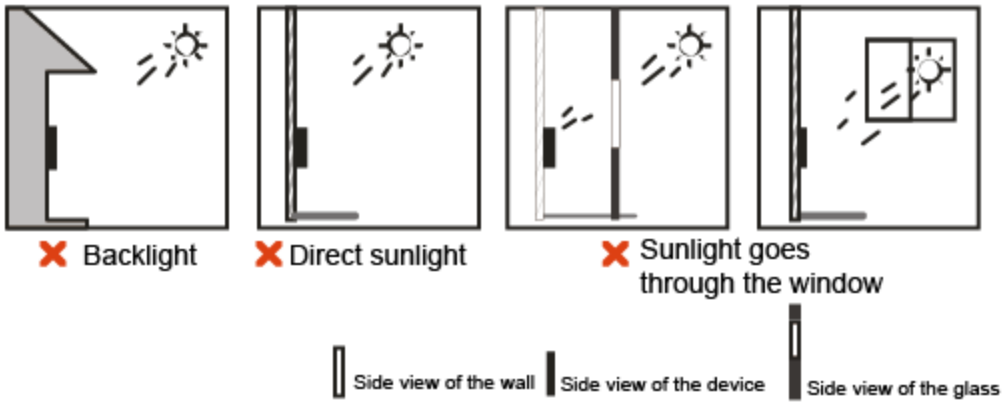
Рекомендуемые места установки

Рисунок 2-4 Рекомендуемые места установки



Нерекомендуемые места установки

Рисунок 2-5 Нерекомендуемые места установки



2.3 Процесс установки

Контроллер доступа имеет 4 способа установки: настенное крепление, напольное крепление, крепление на турникете и крепление на коробке 86. В этом разделе описывается только настенное крепление и крепление на коробке 86. Подробную информацию о напольном креплении и креплении на турникете см. в руководстве пользователя соответствующих устройств.

2.3.1 Настенное крепление

Процедура

Шаг 1 В соответствии с положением отверстий кронштейна просверлите в стене 4 отверстия и 1 кабельный вывод. Вставьте в отверстия дюбели.

Для поверхностной проводки вывод кабеля не требуется.

Шаг 2 Используйте 4 винта для крепления кронштейна к стене. Подключите проводку к

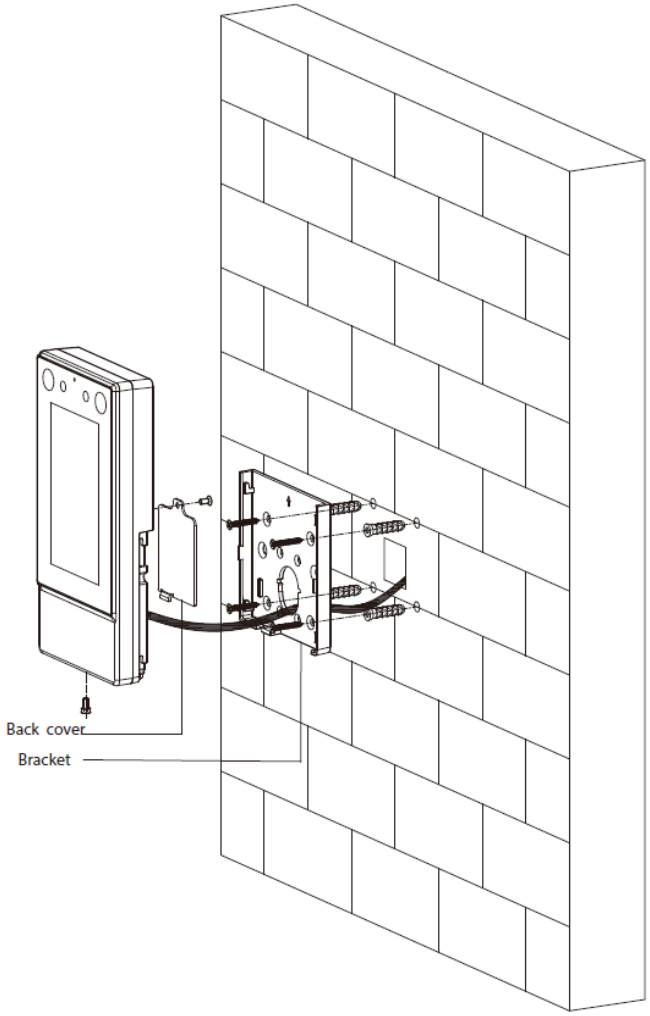
Шаг 3 контроллеру доступа. Подробности см. в разделе «2.1 Проводка». Используйте 1

Шаг 4 винт для крепления задней крышки к контроллеру доступа.

Шаг 5 Закрепите контроллер доступа на кронштейне.

Шаг 6 Надежно закрутите 1 винт в нижней части контроллера доступа.

Рисунок 2-6 Настенное крепление



2.3.2 86 Крепление коробки

Процедура

Шаг 1 Установите коробку 86 на стену на подходящей высоте. Прикрепите

Шаг 2 кронштейн к коробке 86 с помощью 2 винтов. Подключите контроллер

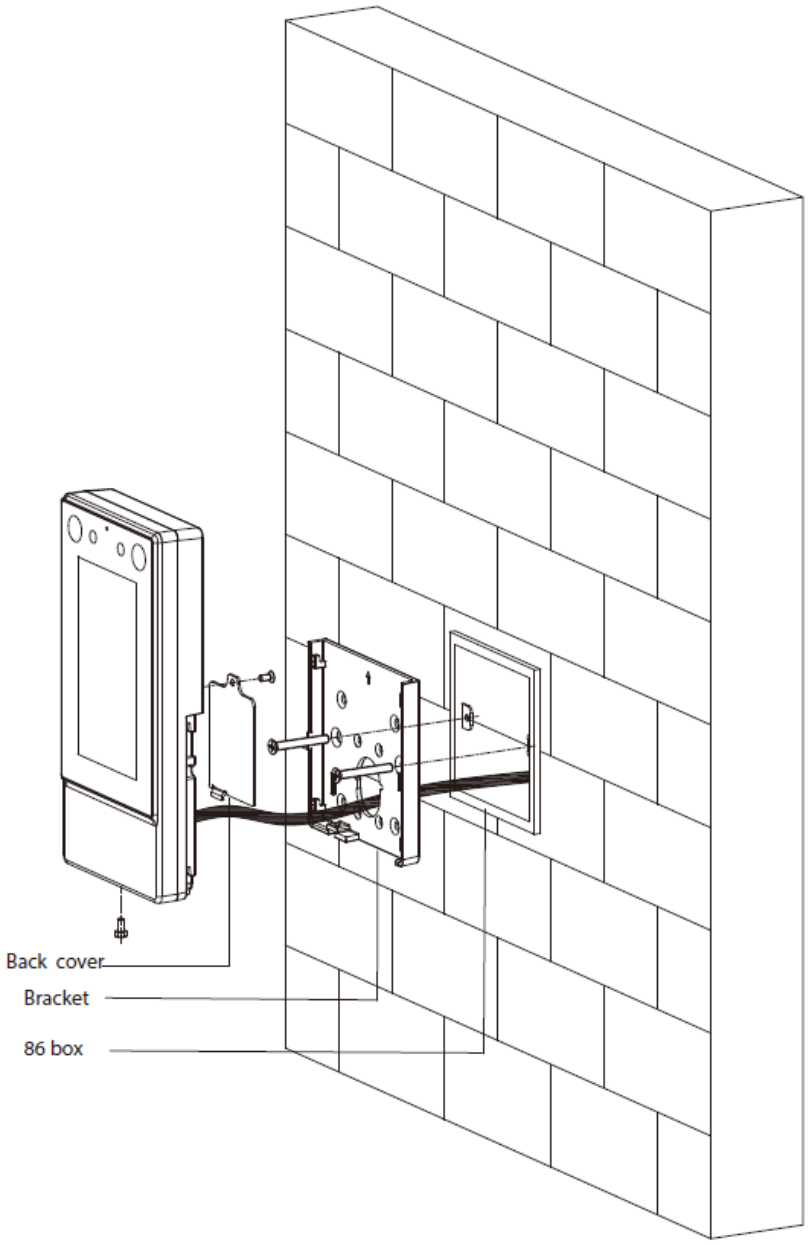
Шаг 3 доступа. Подробности см. в разделе «2.1 Подключение». Используйте 1 винт

Шаг 4 для фиксации задней крышки на контроллере доступа. Закрепите

Шаг 5 контроллер доступа на кронштейне.

Шаг 6 Надежно закрутите 1 винт в нижней части контроллера доступа.

Рисунок 2-7 Крепление коробки 86



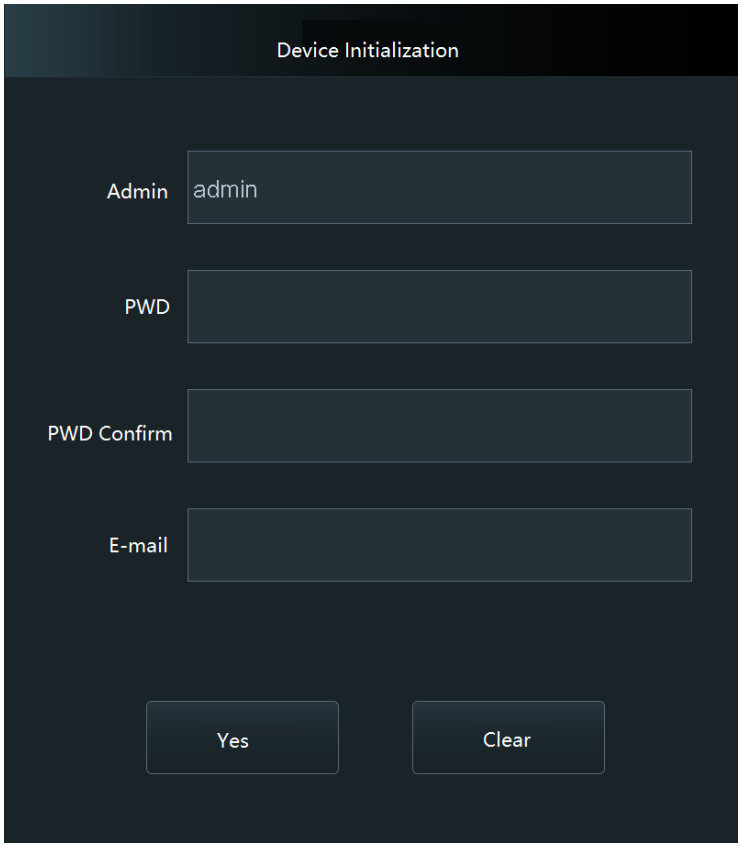
3 локальные конфигурации

Локальные операции могут отличаться в зависимости от разных моделей контроллера доступа.

3.1 Инициализация

При первом использовании или после восстановления заводских настроек вам необходимо выбрать язык, а затем задать пароль и адрес электронной почты для учетной записи администратора. После этого вы можете использовать учетную запись администратора для входа на экран главного меню контроллера доступа и его веб-страницу.

Рисунок 3-1 Инициализация



- Если вы забыли пароль администратора, отправьте запрос на сброс на привязанный адрес электронной почты.
- Пароль должен состоять из 8–32 непустых символов и содержать не менее двух типов символов. следующие символы: заглавные буквы, строчные буквы, цифры и специальные символы (кроме ' " ; : &). Установите пароль высокой надежности, следуя подсказкам по надежности пароля.

3.2 Добавление новых пользователей

Справочная информация

Добавьте новых пользователей, введя такую информацию, как имя, номер карты, лицо и отпечаток пальца, а затем установите разрешения для пользователей.

Процедура

Шаг 1 На**Главное меню**экран, выберите**Пользователь**, а затем нажмите .

Шаг 2 Настроить параметры пользователя.

Рисунок 3-2 Новый пользователь

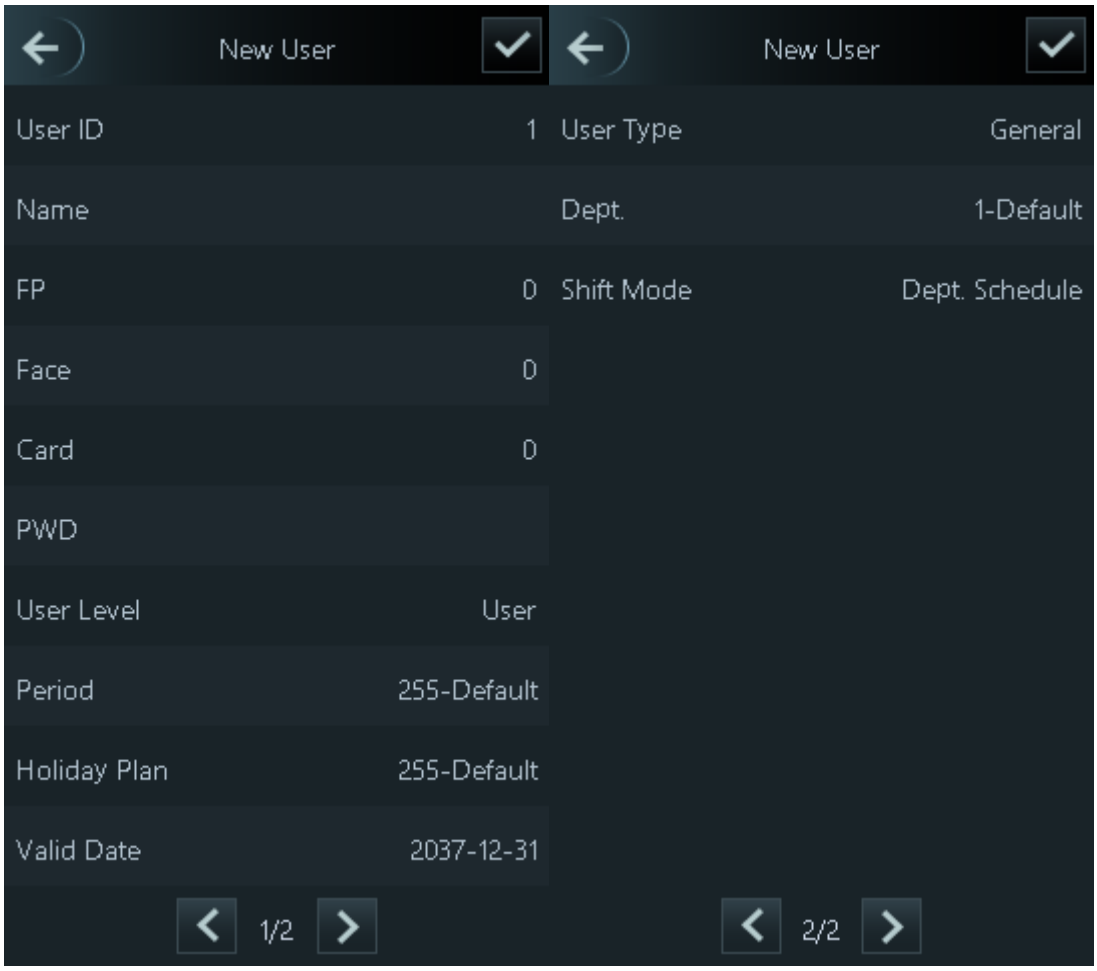


Таблица 3-1 Описание параметров добавления нового пользователя

Параметр	Описание
ID пользователя	Введите идентификатор пользователя. Идентификаторы могут быть цифрами, буквами и их комбинациями, максимальная длина идентификатора — 32 символа. Каждый идентификатор уникален.
Имя	Введите имя, содержащее не более 32 символов (включая цифры, символы и буквы).
ФП	Регистрация отпечатков пальцев. Пользователь может зарегистрировать до 3 отпечатков пальцев, и вы можете установить отпечаток пальца для отпечатка пальца принуждения. Сигнализация сработает, если отпечаток пальца принуждения будет использован для разблокировки двери. Только некоторые модели поддерживают разблокировку по отпечатку пальца.
Лицо	Убедитесь, что ваше лицо находится в центре кадра захвата изображения, и изображение лица будет захвачено и проанализировано автоматически.
Карточка	Пользователь может зарегистрировать максимум пять карт. Введите номер карты или проведите ею по считывателю, после чего данные карты будут считаны контроллером доступа. Вы можете включить**Карта принуждения**функция. Сигнализация сработает, если для разблокировки двери будет использована карта принуждения.

Параметр	Описание
ПВД	Введите пароль пользователя. Максимальная длина пароля — 8 цифр.
Уровень пользователя	Вы можете выбрать уровень пользователя для новых пользователей. ● **Пользователь**: Пользователи имеют разрешение только на доступ к двери. ● **Администратор**: Администраторы могут разблокировать дверь и настроить контроллер доступа.
Период	Пользователи могут разблокировать дверь только в течение определенного периода.
План отпуска	Пользователи могут разблокировать дверь только во время определенного праздничного дня.
Действительная дата	Установите дату, когда истекает срок действия прав доступа данного лица.
Тип пользователя	● **Общий**: Обычные пользователи могут разблокировать дверь. ● **Черный список**: Когда пользователи из черного списка открывают дверь, обслуживающий персонал получает уведомление. ● **Гость**: Гости могут разблокировать дверь в течение определенного периода или определенное количество раз. После истечения определенного периода или времени разблокировки они не смогут разблокировать дверь. ● **Патруль**: Посещаемость пользователей Patrol будет отслеживаться, но у них не будет разрешений на разблокировку. ● **ВИП**: Когда VIP-клиент откроет дверь, обслуживающий персонал получит уведомление. ● **Другие**: Когда они отпирают дверь, она останется открытой еще 5 секунд. ● Пользовательский пользователь 1/Пользовательский пользователь 2: То же, что и у обычных пользователей.
Отдел.	Установить отделы.
Режим смены	Выберите режимы смены.

Шаг 3 Кран**Сохранять**.

4 веб-конфигурации

На веб-странице вы также можете настроить и обновить контроллер доступа.

Веб-конфигурации различаются в зависимости от модели контроллера доступа.

4.1 Инициализация

Инициализируйте контроллер доступа при первом входе на веб-страницу или после восстановления заводских настроек контроллера доступа.

Предпосылки

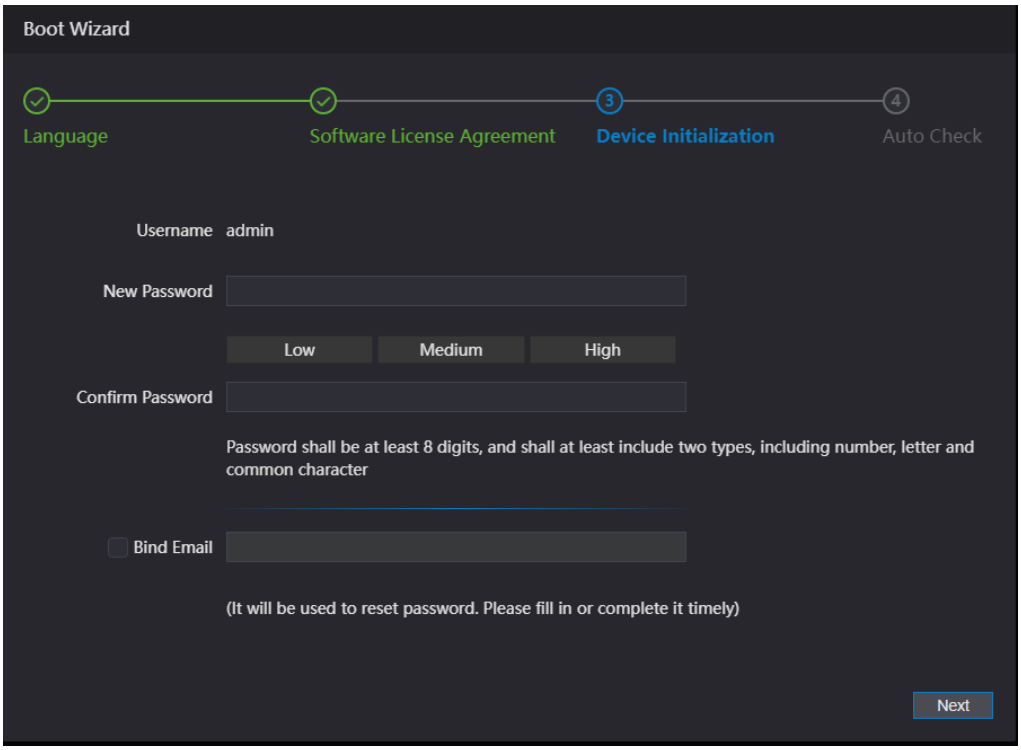
Убедитесь, что компьютер, используемый для входа на веб-страницу, находится в той же локальной сети, что и контроллер доступа.

Процедура

Шаг 1 Откройте веб-браузер и перейдите по IP-адресу (адрес по умолчанию — 192.168.1.108) контроллера доступа.

Вы можете войти в Интернет с помощью Chrome или Firefox.

Рисунок 4-1 Я



Шаг 2 Введите и подтвердите пароль, введите адрес электронной почты, а затем нажмите**Завершенный**.

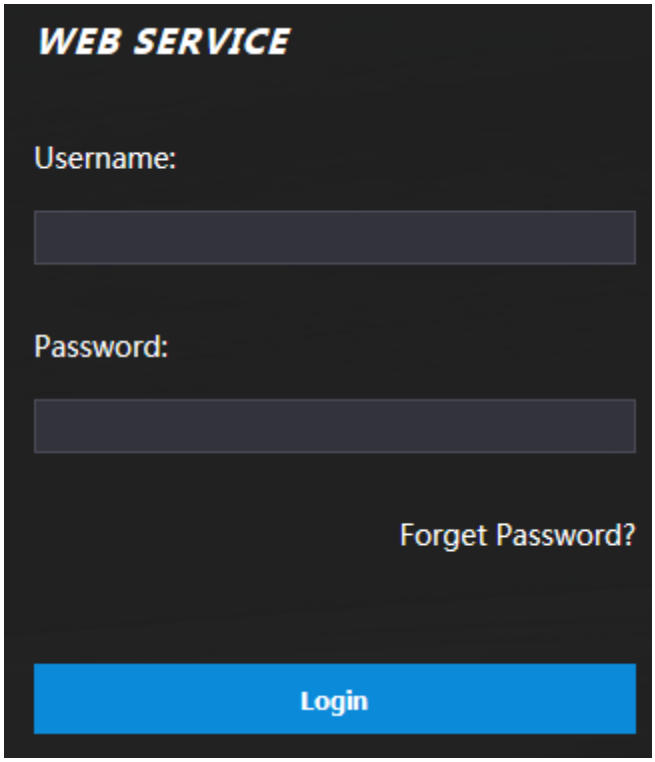
- Пароль должен состоять из 8–32 непустых символов и содержать не менее двух типы следующих символов: заглавные, строчные, цифры и специальные символы (исключая ' " ; : &). Установите пароль высокой степени безопасности, следуя паролю подсказка по силе.
- Сохраняйте пароль в безопасности после инициализации и регулярно меняйте его, чтобы повысить безопасность.
- Если вы хотите сбросить пароль администратора, отсканировав QR-код, вам понадобится привязанный адрес электронной почты для получения кода безопасности.

4.2 Вход в систему

Процедура

Шаг 1 Откройте веб-браузер, перейдите по IP-адресу контроллера доступа.

Рисунок 4-2 Вход



Шаг 2 Введите имя пользователя и пароль.

- Убедитесь, что компьютер находится в той же локальной сети, что и контроллер доступа.
- Имя пользователя администратора по умолчанию — admin, а пароль — тот, который вы установили. во время инициализации. Мы рекомендуем вам регулярно менять пароль администратора для повышения безопасности аккаунта.
- Если вы забыли пароль администратора, вы можете нажать**Забыли пароль?**для сброса пароля.

Шаг 3 Нажмите**Авторизоваться**.

Приложение 1. Важные моменты внутренней связи

Операция

Контроллер доступа может функционировать как VTO для реализации функции домофона.

Предпосылки

Функция внутренней связи настраивается на контроллере доступа и VTO.

Процедура

Шаг 1 На экране ожидания нажмите «Введите».

Шаг 2 номер комнаты», а затем нажмите .

Приложение 2. Важные моменты QR-кода

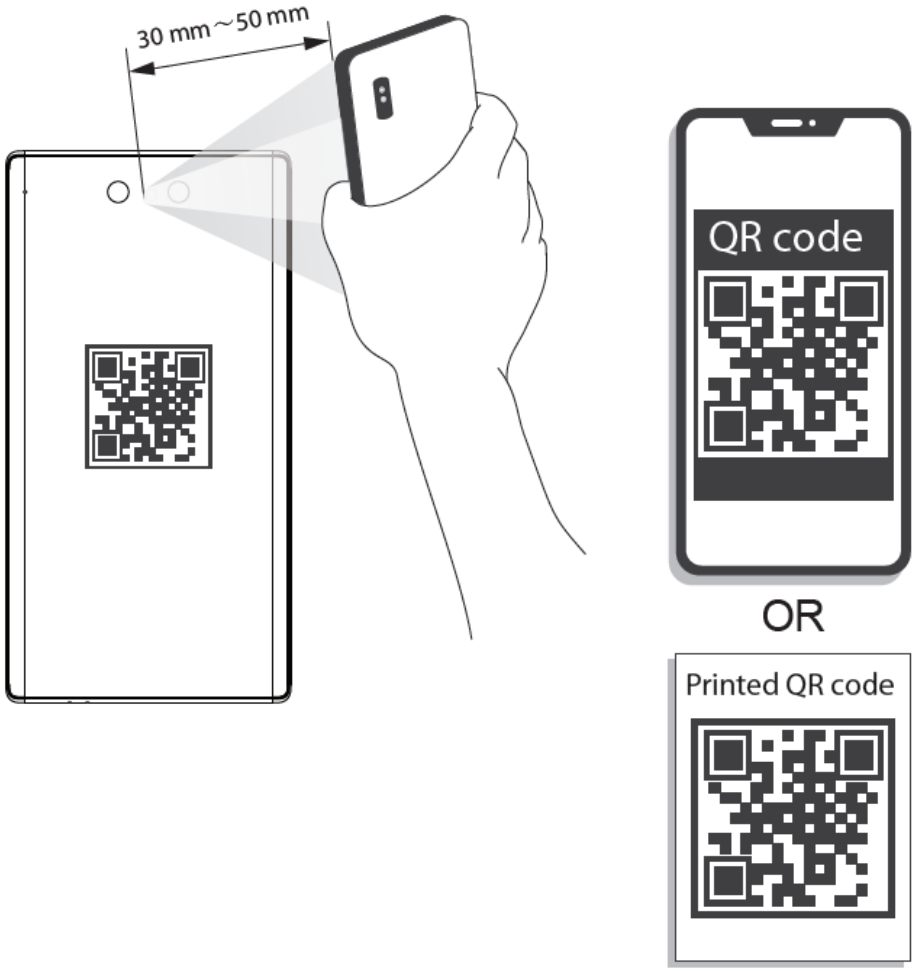
Сканирование

Поместите QR-код на свой телефон на расстоянии 3–5 см от линзы сканера QR-кода. Он поддерживает QR-код размером более 30 мм × 30 мм – 5 см × 5 см и размером менее 128 байт.

Расстояние обнаружения QR-кода различается в зависимости от байтов и размера QR-кода. Код OR

Информация ниже представлена только для справки. Пожалуйста, отсканируйте реальный QR-код.

Приложение Рисунок 2-1 Сканирование QR-кода



Приложение 3. Важные моменты лица

Регистрация

Перед регистрацией

- Очки, шляпы и бороды могут повлиять на эффективность распознавания лиц.
- Не закрывайте брови, надевая шляпу.
- Не меняйте сильно стиль бороды, если используете контроллер доступа, иначе распознавание лица может не сработать.
- Держите лицо в чистоте.
- Располагайте контроллер доступа на расстоянии не менее двух метров от источника света и не менее трех метров от окон или дверей; в противном случае подсветка и прямые солнечные лучи могут повлиять на эффективность распознавания лиц контроллером доступа.

Во время регистрации

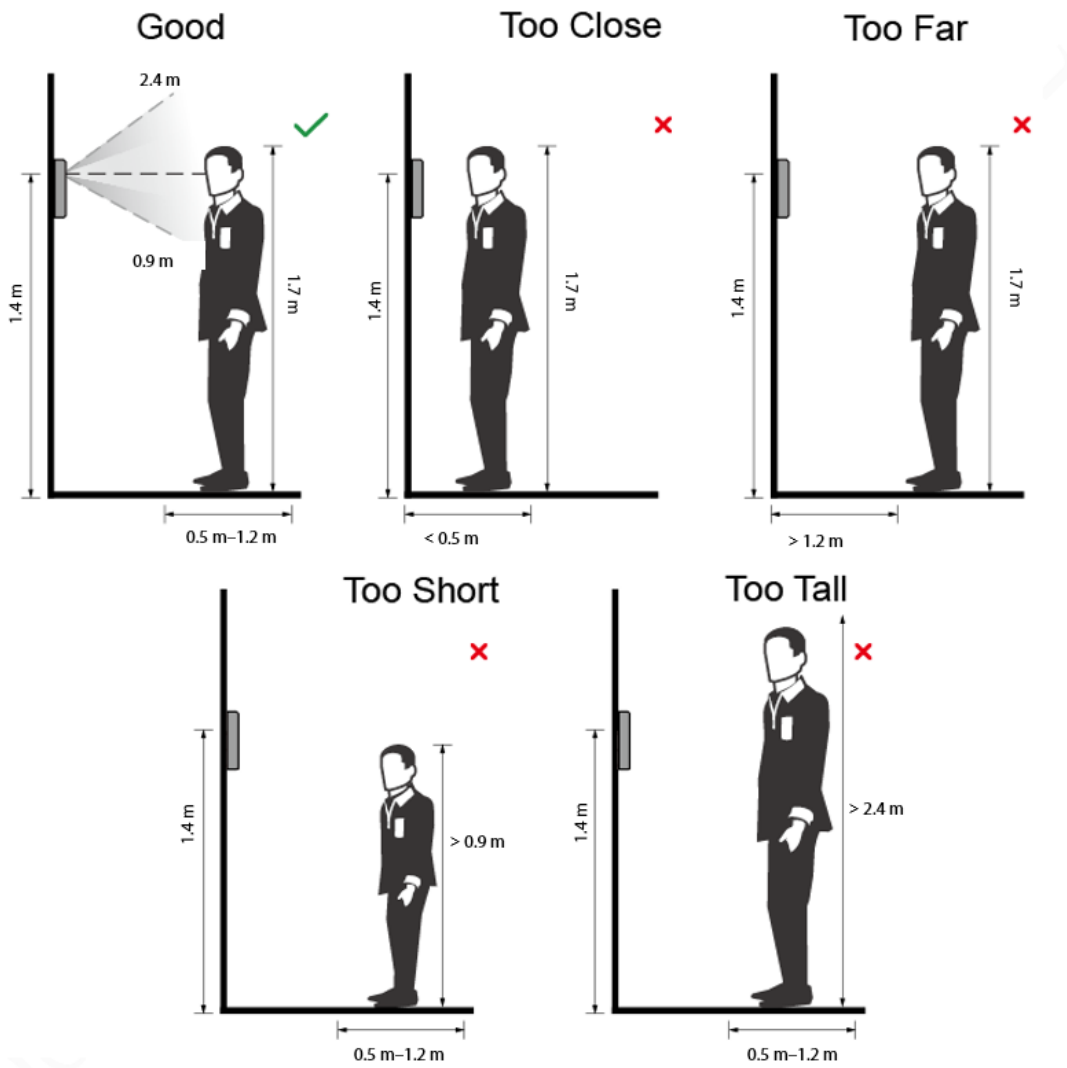
- Вы можете регистрировать лица через контроллер доступа или через платформу. Для регистрации через платформу см. руководство пользователя платформы.
- Поместите голову в центр рамки фотосъемки. Изображение лица будет захвачено автоматически.

- Не трясите головой и телом, иначе регистрация может быть не удалась.
- Избегайте одновременного появления в кадре двух лиц.

Положение лица

Если ваше лицо находится в неправильном положении, точность распознавания лица может быть снижена.

Приложение Рисунок 3-1 Соответствующее положение лица



Требования к лицам

- Убедитесь, что лицо чистое и лоб не закрыт волосами.
- Не надевайте очки, шляпы, густую бороду или другие украшения на лице, которые могут повлиять на запись изображения лица.
- С открытыми глазами, без выражения лица, поверните лицо к центру камеры.
- Во время записи вашего лица или во время распознавания лиц не держите лицо слишком близко или слишком далеко от камеры.

Приложение Рисунок 3-2 Положение головы

Приложение Рисунок 3-3 Расстояние до лица

- При импорте изображений лиц через платформу управления убедитесь, что изображение разрешение в диапазоне 150 × 300 пикселей–600 × 1200 пикселей; пиксели изображения более 500 × 500 пикселей; размер изображения менее 100 КБ, имя изображения и идентификатор человека совпадают.
- Убедитесь, что лицо занимает более 1/3, но не более 2/3 всей площади изображения, и соотношение сторон не превышает 1:2.

Приложение 4 Рекомендации по кибербезопасности

Обязательные действия, которые необходимо предпринять для обеспечения безопасности базовой сети устройства:

1.**Используйте надежные пароли**

Пожалуйста, воспользуйтесь следующими рекомендациями по установке паролей:

- Длина не должна быть менее 8 символов.
- Включите не менее двух типов символов; типы символов включают заглавные и строчные буквы, цифры и символы.
- Не используйте имя учетной записи или имя учетной записи в обратном порядке.
- Не используйте непрерывные символы, такие как 123, abc и т. д.
- Не используйте пересекающиеся символы, такие как 111, aaa и т. д.

2.**Своевременно обновляйте прошивку и клиентское программное обеспечение**

- Согласно стандартной процедуре в технологической отрасли, мы рекомендуем поддерживать прошивку вашего устройства (например, NVR, DVR, IP-камеры и т. д.) в актуальном состоянии, чтобы гарантировать, что система оснащена последними исправлениями и патчами безопасности. Когда устройство подключено к общедоступной сети, рекомендуется включить функцию «автоматической проверки обновлений», чтобы получать своевременную информацию об обновлениях прошивки, выпущенных производителем.
- Мы рекомендуем вам загрузить и использовать последнюю версию клиентского программного обеспечения.

Полезные рекомендации по улучшению сетевой безопасности вашего устройства:

1.**Физическая защита**

Мы предлагаем вам выполнить физическую защиту устройства, особенно устройств хранения данных. Например, поместите устройство в специальную компьютерную комнату и шкаф, а также внедрите хорошо организованный контроль доступа и управление ключами, чтобы предотвратить несанкционированный персонал от осуществления физических контактов, таких как повреждение оборудования, несанкционированное подключение съемного устройства (например, USB-флеш-диска, последовательного порта) и т. д.

2.**Регулярно меняйте пароли**

Мы рекомендуем вам регулярно менять пароли, чтобы снизить риск их угадывания или взлома.

3.**Установка и обновление паролей. Своевременный сброс информации.**

Устройство поддерживает функцию сброса пароля. Пожалуйста, настройте соответствующую информацию для сброса пароля вовремя, включая почтовый ящик конечного пользователя и вопросы защиты пароля. Если информация изменится, пожалуйста, измените ее вовремя. При установке вопросов защиты пароля рекомендуется не использовать те, которые можно легко угадать.

4.**Включить блокировку учетной записи**

Функция блокировки учетной записи включена по умолчанию, и мы рекомендуем вам оставить ее включенной, чтобы гарантировать безопасность учетной записи. Если злоумышленник попытается войти в систему с неправильным паролем несколько раз, соответствующая учетная запись и исходный IP-адрес будут заблокированы.

5.**Изменить HTTP-порты и другие сервисные порты по умолчанию**

Мы предлагаем вам изменить порты HTTP и других служб по умолчанию на любой набор чисел в диапазоне 1024–65535, чтобы снизить риск того, что посторонние смогут угадать, какие порты вы используете.

6.**Включить HTTPS**

Мы предлагаем вам включить HTTPS, чтобы вы могли посещать веб-сервис через защищенный канал связи.

7.**Привязка MAC-адреса**

Мы рекомендуем вам привязать IP и MAC-адрес шлюза к устройству, тем самым снизив риск подмены ARP.

8.**Разумно назначайте учетные записи и привилегии**

В соответствии с требованиями бизнеса и управления, разумно добавляйте пользователей и назначайте им

минимальный набор разрешений для них.

9.**Отключите ненужные службы и выберите безопасные режимы**

Если в них нет необходимости, рекомендуется отключить некоторые службы, такие как SNMP, SMTP, UPnP и т. д., чтобы снизить риски.

При необходимости настоятельно рекомендуется использовать безопасные режимы, включая, помимо прочего, следующие службы:

- SNMP: выберите SNMP v3 и установите надежные пароли шифрования и пароли аутентификации.
- SMTP: выберите TLS для доступа к серверу почтовых ящиков.
- FTP: выберите SFTP и установите надежные пароли.
- Точка доступа: выберите режим шифрования WPA2-PSK и установите надежные пароли.

10.**Зашифрованная передача аудио и видео**

Если ваши аудио- и видеоданные очень важны или конфиденциальны, мы рекомендуем вам использовать функцию зашифрованной передачи, чтобы снизить риск кражи аудио- и видеоданных во время передачи.

Напоминание: зашифрованная передача данных приведет к некоторой потере эффективности передачи.

11.**Безопасный аудит**

- Проверяйте пользователей в сети: мы рекомендуем вам регулярно проверять пользователей в сети, чтобы убедиться, что устройство не авторизовано.
- Проверьте журнал устройства: просматривая журналы, вы можете узнать IP-адреса, которые использовались для входа на ваши устройства, а также их основные операции.

12.**Сетевой журнал**

Из-за ограниченной емкости устройства, сохраненный журнал ограничен. Если вам необходимо сохранить журнал в течение длительного времени, рекомендуется включить функцию сетевого журнала, чтобы гарантировать синхронизацию критических журналов с сервером сетевого журнала для трассировки.

13.**Постройте безопасную сетевую среду**

Чтобы лучше обеспечить безопасность устройства и снизить потенциальные киберриски, мы рекомендуем:

- Отключите функцию сопоставления портов маршрутизатора, чтобы избежать прямого доступа к устройствам интрасети из внешней сети.
- Сеть должна быть разделена и изолирована в соответствии с реальными потребностями сети. Если между двумя подсетями нет требований к коммуникации, предлагается использовать VLAN, сетевой GAP и другие технологии для разделения сети, чтобы достичь эффекта изоляции сети.
- Внедрите систему аутентификации доступа 802.1x для снижения риска несанкционированного доступа к частным сетям.
- Включите функцию фильтрации IP/MAC-адресов, чтобы ограничить круг хостов, которым разрешен доступ к устройству.