Контроллер доступа с функцией распознавания лиц

Руководство пользователя

V1.0.1

Введение

Общие сведения

В данном руководстве описаны процедуры установки и основные операции с контроллером доступа с функцией распознавания лиц (далее – «контроллер доступа»).

Инструкции по технике безопасности

В руководстве могут встречаться следующие разделенные на категории условные обозначения с определенным значением.

Условное обозначение	Значение
ПРИМЕЧАНИЕ	Дополнительная информация, служащая для акцентирования внимания на тексте.

История редакций

Версия	Содержание редакции	Дата выпуска
V1.0.0	Первый выпуск	Август 2019 года

О руководстве

- Данное руководство используется только для ознакомления. В случае несоответствия между руководством и фактическим продуктом, последний имеет решающее значение.
- Мы не несем ответственности за какие-либо убытки, вызванные действиями, несоответствующими руководству.
- Руководство обновляется в соответствии с актуальным законодательством в соответствующих регионах. Более подробную информацию см. в бумажном руководстве пользователя, на компакт-диске, на нашем официальном вебсайте или с помощью QR-кода. При наличии несоответствий между руководством пользователя в бумажном формате и электронной версией, электронная версия имеет решающее значение.
- Любой дизайн и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта могут вызвать некоторые различия между фактическим продуктом и руководством. Чтобы получить последнее программное обеспечение или дополнительную документацию, свяжитесь со службой поддержки.
- Возможны отклонения в отношении технических данных, функций и описании операций, а также опечатки. При наличии каких-либо сомнений или разногласий, обратитесь к нам за окончательным разъяснением.
- Обновите программное обеспечение для чтения или используйте другое общедоступное программное обеспечение, если руководство (в формате PDF) невозможно открыть.
- Все торговые знаки и зарегистрированные торговые марки, упоминаемые в данном документе, являются собственностью соответствующих правообладателей.
- При возникновении каких-либо проблем в процессе эксплуатации устройства, посетите наш вебсайт, свяжитесь с поставщиком или службой поддержки.
- При наличии каких-либо сомнений или разногласий, обратитесь к нам за окончательным разъяснением.

Важные меры предосторожности и предупреждения

Данная глава охватывает правильное обращение с контроллером доступа, информация о предотвращении опасности и порчи имущества. Перед тем, как приступить к эксплуатации контроллера доступа, внимательно изучите данные указания, следуйте им при работе и сохраните их, чтобы можно было обратиться к ним в будущем.

Требования к эксплуатации

- Не размещайте и не устанавливайте контроллер доступа в местах, подверженных воздействию прямых солнечных лучей или вблизи отопительных приборов.
- Не устанавливайте контроллер доступа на влажном, пыльном, или покрытом копотью месте.
- Удерживайте контроллер доступа в горизонтальном положении на устойчивой поверхности, чтобы избежать его падения.
- Не подвергайте контроллер доступа воздействию каким-либо жидкостей; не ставьте на него какие-либо предметы, наполненные жидкостью, чтобы предотвратить попадание жидкости внутрь контроллера доступа.
- Устанавливайте контроллер доступа в местах с хорошей вентиляцией; не перекрывайте вентиляционные отверстия.
- Используйте контроллер доступа только в пределах номинального диапазона входа и выхода питания.
- Не разбирайте контроллер доступа.
- Транспортировка, эксплуатация и хранение контроллера доступа должны осуществляться при допустимой влажности и температуре.

Требования к электропитанию

- Неправильное обращение с аккумулятором может привести к возгоранию или взрыву.
- При замене используйте аккумуляторы одного типа.
- Используйте рекомендуемые для вашего региона кабели питания, соответствующие номинальным спецификациям.
- Используйте адаптер питания, идущий в комплекте с контроллером доступа; в противном случае возможно травмирование и повреждение устройства.
- Источник питания должен соответствовать требованиям стандарта безопасного сверхнизкого напряжения (SELV) и должен иметь номинальное напряжение, соответствующее требованиям к ограниченным источникам питания по IEC60950-1. Обратите внимание на то, что требования к электропитанию указываются в маркировке устройства.
- Подключайте устройство (с категорией конструкции I) к сетевым розеткам с защитным заземлением.
- Приборный соединитель является разъединяющим устройством. При обычной эксплуатации используйте угол, облегчающий работу.

Содержание

1 Обзор

1.1 Введение

Контроллер доступа представляет собой панель управления доступом, которая поддерживает разблокировку с помощью изображений лиц, паролей, отпечатков пальцев, карт, а также их комбинаций.

1.2 Особенности

- Поддержка разблокировки с помощью изображений лиц, IC-картам и паролям; разблокировка по периоду.
- Устройство распознавания лиц; первым происходит распознавание самого большого лица среди тех, которые одновременно появляются на экране; максимальный размер лица можно настроить в веб-интерфейсе.
- Объектив с разрешением 2 Мп, широким углом обзора и WDR; с автоматическим/ручным заполнением цветом
- Расстояние от лица до камеры: 0,3–2,0 м; рост человека: 0,9–2,4 м.
- С помощью алгоритма распознавания лиц терминал может распознавать более 360 положений на лице человека.
- Точность верификации лиц >99,5%; низкий уровень ложных распознаваний.
- Поддержка распознавания профиля; угол профиля: 0°–90°
- Поддержка детекции витальности.
- Поддержка тревоги принуждения и тампера.
- Поддержка общих пользователей, принуждения, патрулей, черного списка, VIP-пользователей, гостей и лиц с ограниченными возможностями.
- 4 режима отображения статуса разблокировки и различные режимы голосовых указаний.

1.3 Размеры и компоненты

Существует два типа контроллеров доступа: 7-дюймовые и 10-дюймовые. См. рисунки от 1-1 до 1-4.

Рисунок 1-1 Размеры и компоненты (1) (мм [дюймы])

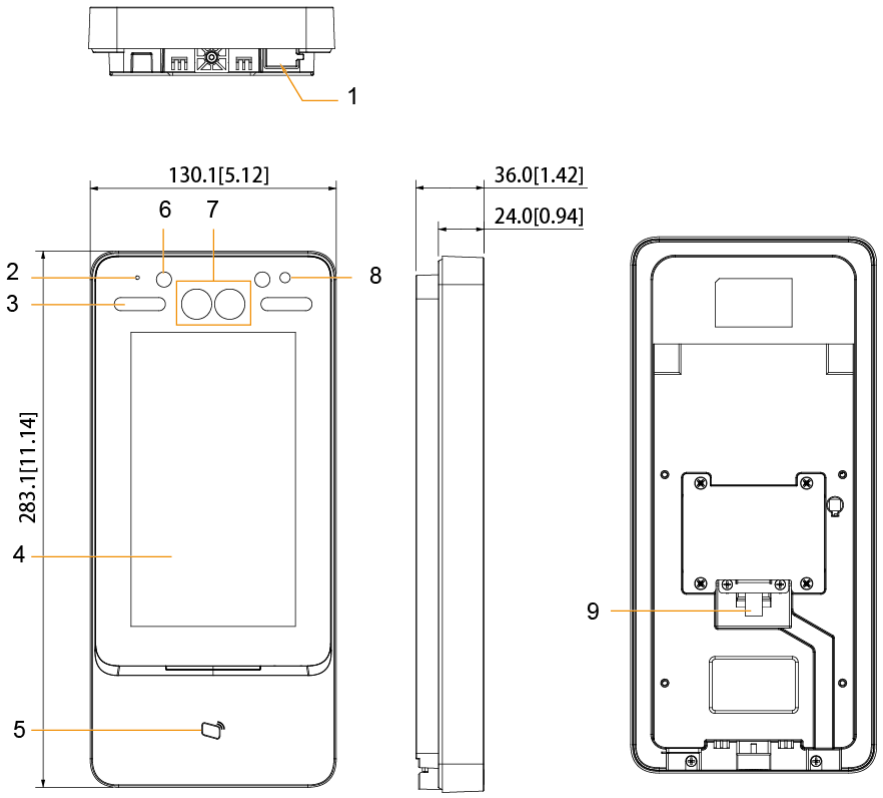


Таблица 1-1 Описание компонентов (1)

№	Название	№	Название
1	USB-порт	6	ИК-светодиод
2	Микрофон	7	Двойная камера
3	Источник белого света	8	Фототранзистор
4	Дисплей	9	Вход кабеля
5	Место сканирования карт	10	–

Рисунок 1-2 Размеры и компоненты (2) (мм [дюймы])

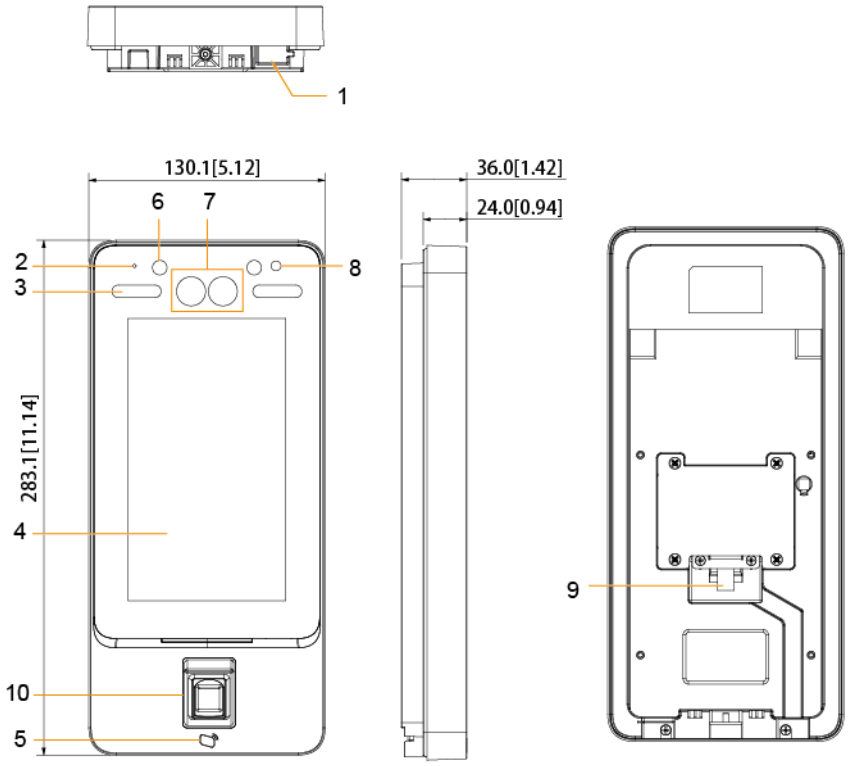


Таблица 1-2 Описание компонентов (2)

№	Название	№	Название
1	USB-порт	6	ИК-светодиод
2	Микрофон	7	Двойная камера
3	Источник белого света	8	Фототранзистор
4	Дисплей	9	Вход кабеля
5	Место сканирования карт	10	Сенсор отпечатков пальцев

Рисунок 1-3 Размеры и компоненты (3) (мм [дюймы])

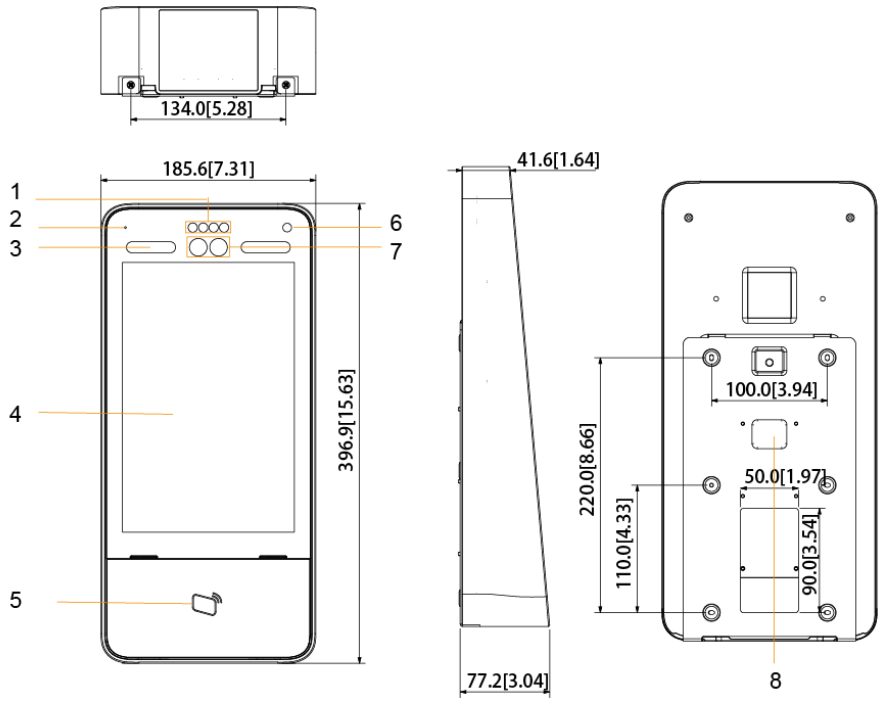


Таблица 1-3 Описание компонентов (3)

№	Название	№	Название
1	ИК-светодиод	6	Фототранзистор
2	Микрофон	7	Двойная камера
3	Источник белого света	8	Вход кабеля
4	Дисплей	9	–
5	Место сканирования карт	10	–

Рисунок 1-4 Размеры и компоненты (4) (мм [дюймы])

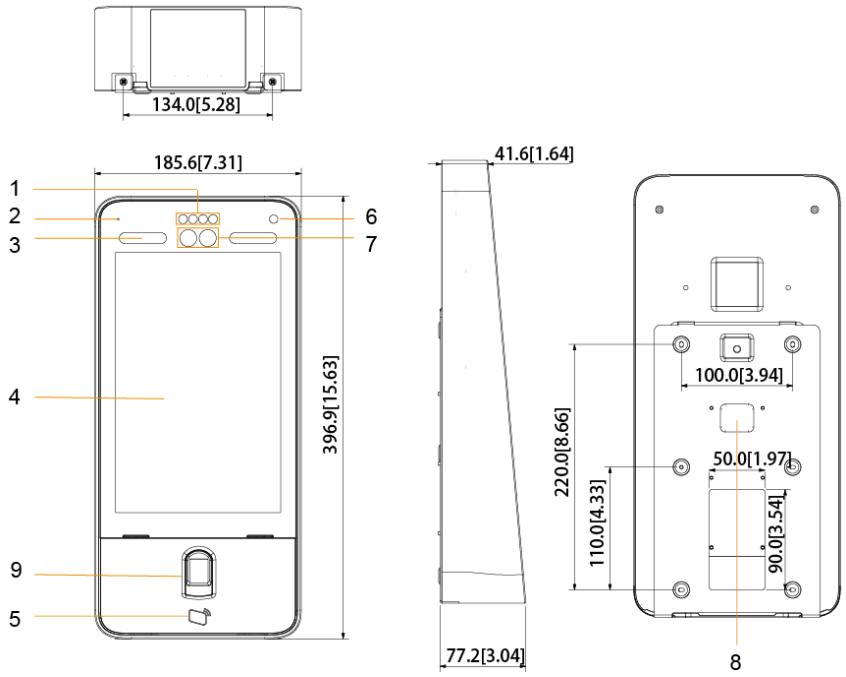


Таблица 1-4 Описание компонентов (4)

№	Название	№	Название
1	ИК-светодиод	6	Фототранзистор
2	Микрофон	7	Двойная камера
3	Источник белого света	8	Вход кабеля
4	Дисплей	9	Сенсор отпечатков пальцев
5	Место сканирования карт	10	–

2 Установка

2.1 Подключение кабелей

К контроллеру доступа необходимо подключать различные устройства, например, сирены, считыватели или дверные контакты. Информацию о подключении кабелей см. в таблице 2-1.

Таблица 2-1 Описание портов

Порт	Цвет кабеля	Название кабеля	Описание
CON1	Черный	RD–	Отрицательный электрод источника питания внешнего считывателя карт
	Красный	RD+	Положительный электрод источника питания внешнего считывателя карт
	Синий	CASE	Вход тревоги принуждения внешнего считывателя карт
	Белый	D1	Вход Wiegand D1 (подключение к внешнему считывателю карт)/выход (подключение к контроллеру)
	Зеленый	D0	Вход Wiegand D0 (подключение к внешнему считывателю карт)/выход (подключение к контроллеру)
	Коричневый	LED	Подключение к входу внешнего считывателя карт
	Желтый	B	Вход отрицательного электрода RS-485 (подключение к внешнему считывателю карт)/выход (подключение к контроллеру или модулю контроля безопасности двери) ● Если модуль безопасности активирован, вам необходимо отдельно приобрести модуль безопасности контроля доступа. Для модуля безопасности требуется отдельный источник питания. ● Если модуль безопасности активирован, кнопка выхода, управление блокировкой и функция отпечатков пальцев будут недоступны.
	Фиолетовый	A	Вход положительного электрода RS-485 (подключение к внешнему считывателю карт)/выход (подключение к контроллеру или модулю контроля безопасности двери). ● Если модуль безопасности активирован, вам необходимо отдельно приобрести модуль безопасности контроля доступа. Для модуля безопасности требуется отдельный источник питания. ● Once Если модуль безопасности активирован, кнопка выхода, управление блокировкой и функция отпечатков пальцев будут недоступны.

Порт	Цвет кабеля	Название кабеля	Описание
CON2	Белый и красный	ALARM1_NO	Нормально разомкнутый выходной порт Alarm 1
	Белый и оранжевый	ALARM1_COM	Общий выходной порт Alarm 1
	Белый и синий	ALARM2_NO	Нормально разомкнутый выходной порт Alarm 2
	Белый и серый	ALARM2_COM	Общий выходной порт Alarm 2
	Белый и зеленый	GND	Подключается к общему порту GND
	Белый и коричневый	ALARM1	Входной порт Alarm 1
	Белый и желтый	GND	Подключается к общему порту GND
	Белый и фиолетовый	ALARM2	Входной порт Alarm 2
CON3	Черный и красный	RX	Порт получения RS-232
	Черный и оранжевый	TX	Порт отправки RS-232
	Черный и синий	GND	Подключается к общему порту GND
	Черный и серый	SR1	Используется для детекции контакта с дверью
	Черный и зеленый	PUSH1	Кнопка открывания двери на двери № 1
	Черный и коричневый	DOOR1_COM	Общий порт управления блокировкой
	Черный и желтый	DOOR1_NO	Нормально разомкнутый порт управления блокировкой
	Черный и фиолетовый	DOOR1_NC	Нормально замкнутый порт управления блокировкой

2.2 Установка

Способы установки моделей A и B одинаковы. Убедитесь в том, что расстояние между объективом и землей составляет 1,4 метра. См. рисунок 2-1.

Рисунок 2-1 Высота установки

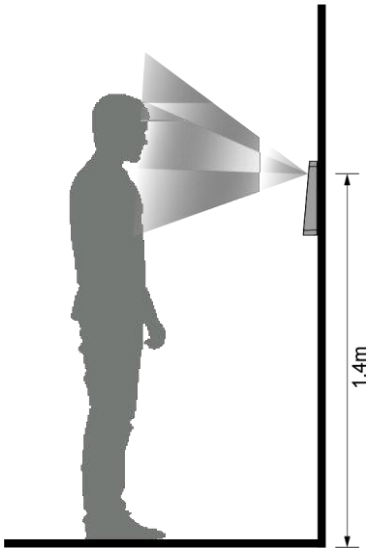
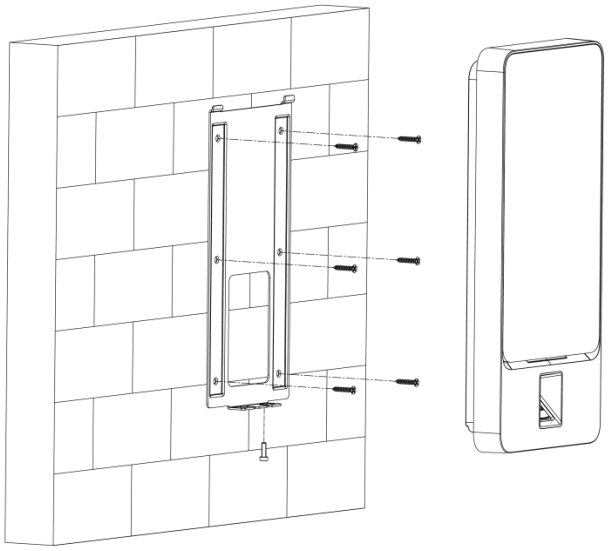


Рисунок 2-2 Схема установки



Процедуры установки

Шаг 1 Просверлите семь отверстий (шесть для установки кронштейна и один для входа кабеля) в соответствии с отверстиями на кронштейне.

Шаг 2 Зафиксируйте кронштейн на стене, вставив дюбели в шесть установочных отверстий кронштейна.

Шаг 3 Подсоедините кабели контроллера доступа.
См. Раздел 2.2 «Подключение кабелей».

Шаг 4 Повесьте контроллер доступа на крючок кронштейна.

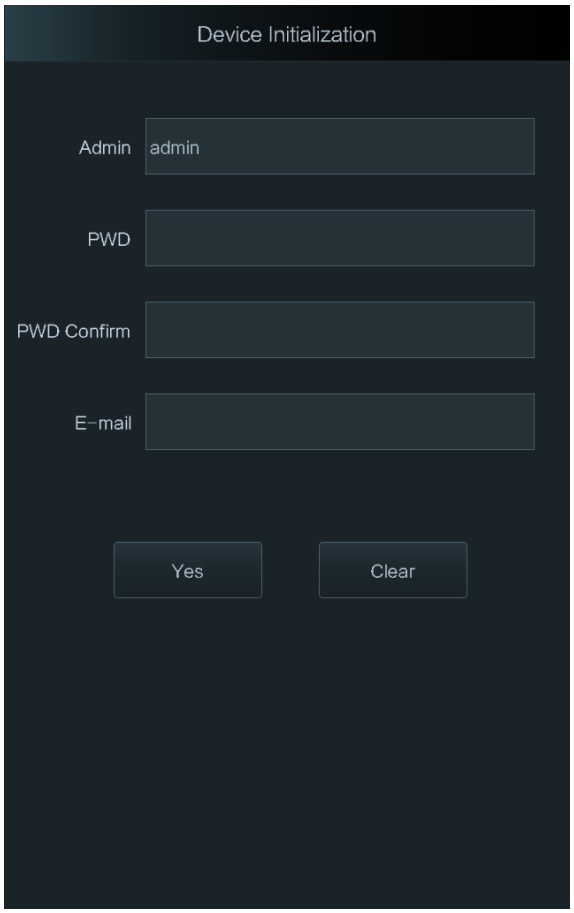
Шаг 5 Закрутите шурупы в нижней части контроллера доступа. Теперь установка выполнена.

3 Работа в системе

3.1 Инициализация

При первом включении контроллера доступа необходимо настроить пароль администратора и email; в противном случае контроллер доступа не будет работать.

Рисунок 3-1 Инициализация



- Администратор и пароль, настраиваемые в этом окне, используются для авторизации в веб-интерфейсе платформы управления.
- Если вы забыли пароль администратора, его можно переустановить с помощью указанного адреса электронной почты.
- Пароль должен состоять из от 8 до 32 символов без пробелов и как минимум два разных видов символов, включая верхний регистр, нижний регистр, цифры и специальные знаки (кроме ' " ; : &).

3.2 Окно режима ожидания

Разблокировать дверь можно с помощью изображений лиц, паролей, карт или отпечатков пальцев. См. таблицу 3-1.

Если в течение 30 секунд не выполняются какие-либо операции, контроллер доступа переходит в режим ожидания.

Рисунок 3-2 Начальная страница

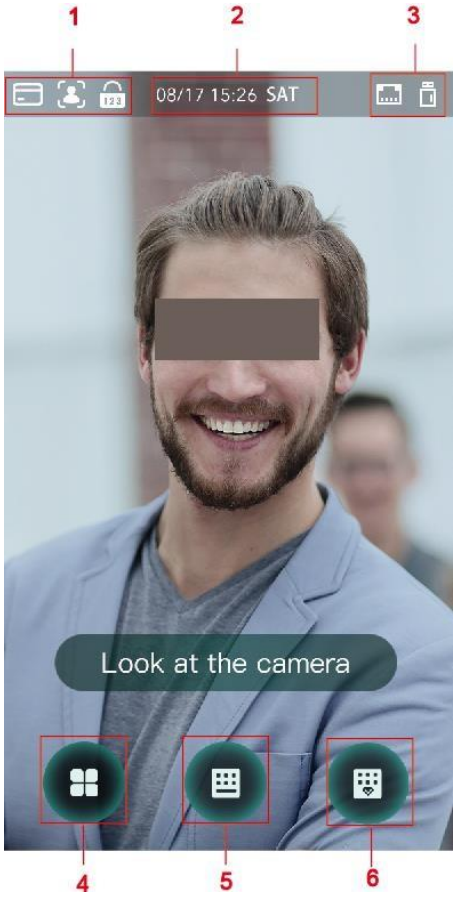


Таблица 3-1 Описание начальной страницы

№	Описание
1	Способы разблокировки: карта, лицо, отпечаток пальца и пароль. Если карты, изображения лиц, отпечатки пальцев и пароли все настроены для разблокировки, значок пароля не будет отображаться в верхнем левом углу экрана контроля доступа.
2	Дата и время: здесь отображаются текущая дата и время.
3	Здесь отображаются статус сети и статус USB.
4	Значок главного меню. Войти в главное меню может только администратор.
5	Значок разблокировки паролем.
6	Значок разблокировки паролем администратора.

3.3 Способы разблокировки

Дверь можно разблокировать с помощью изображений лиц, паролей, отпечатков пальцев и карт.

3.3.1 Карты

Приложите карту к месту сканирования, чтобы разблокировать дверь.

3.3.2 Изображения лиц

Убедитесь в том, что ваше лицо находится в центре рамки изображения, тогда вы сможете разблокировать дверь.

3.3.3 Отпечатки пальцев

Поместите палец на сенсор отпечатков пальцев, чтобы разблокировать дверь.

3.3.4 Пароли пользователей

Введите пароль пользователя, чтобы разблокировать дверь.

Шаг 1 Нажмите  на начальной странице.

Шаг 2 Введите ID пользователя и нажмите  .

Шаг 3 Введите пароль пользователя и нажмите  .

Дверь будет разблокирована.

3.3.5 Пароль администратора

Введите пароль администратора, чтобы разблокировать дверь. Для одного контроллера доступа возможен только один пароль администратора. С помощью пароля администратора можно разблокировать двери, вне зависимости от категорий пользователей, режимов разблокировки, периодов, планов праздничных дней и запретов на проход в обратном направлении.

Пароль администратора невозможно использовать, если период NC установлен как «3.6.1.5 NC Period».

Шаг 1 Нажмите  на начальной странице.

Шаг 2 Нажмите **Please Enter Administrator PWD (Введите пароль администратора)**.

Шаг 3 Введите пароль администратора и нажмите  .

Дверь будет разблокирована.

3.4 Главное меню

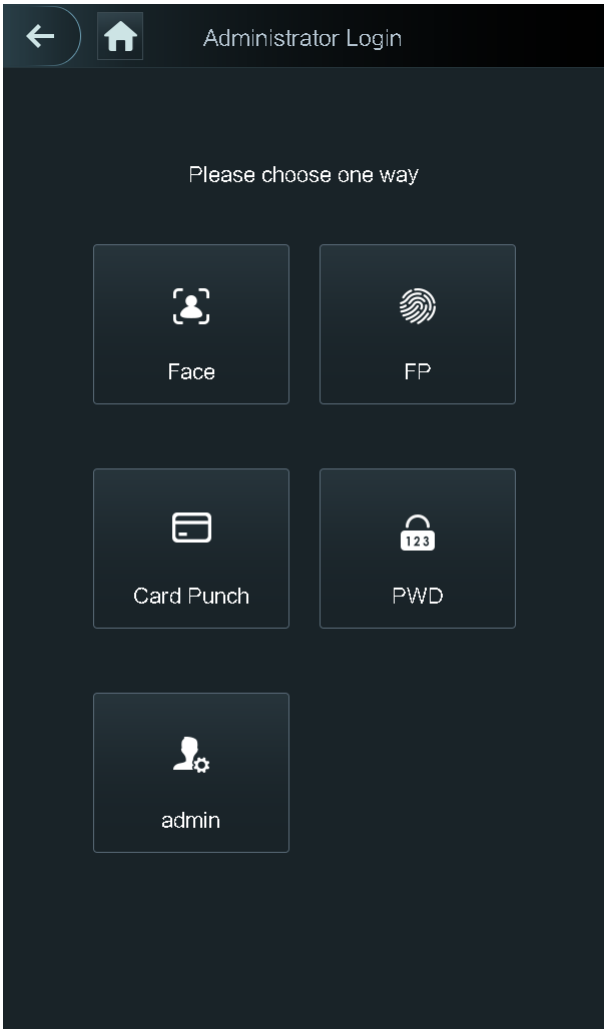
В главном меню администраторы могут добавлять пользователей разных категорий, настраивать параметры, связанные с доступом, выполнять настройки сети, просматривать записи о доступе и системную информацию и т.д.

Шаг 1 Нажмите  в режиме ожидания.

Откроется окно **Administrator Login (Вход администратора)**.

Разные режимы поддерживают разные способы разблокировки, и преимущественное значение имеет фактический интерфейс.

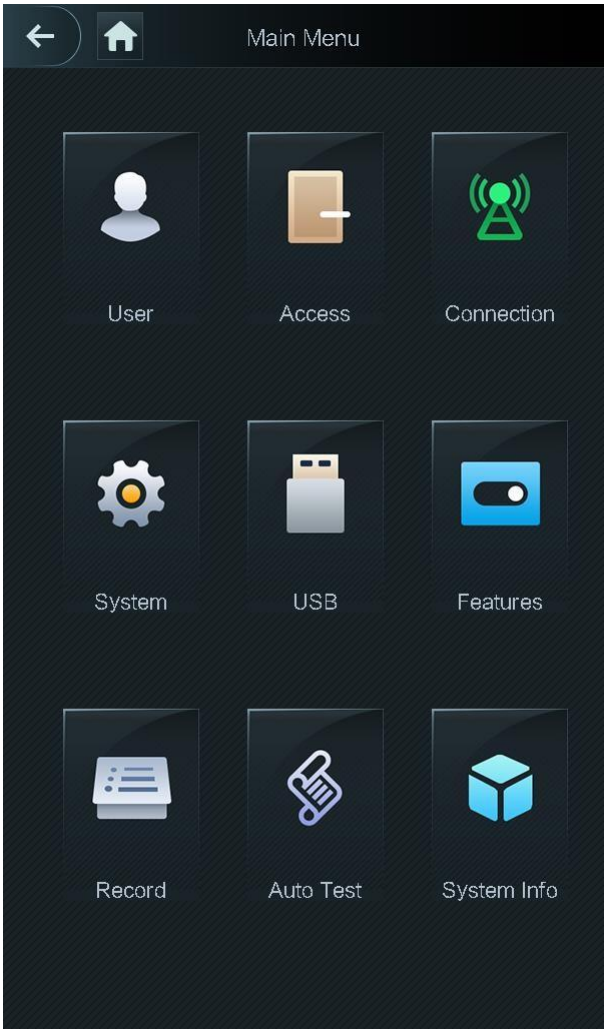
Рисунок 3-3 Вход администратора



Шаг 2 Выберите способ входа в главное меню.

Откроется интерфейс главного меню.

Рисунок 3-4 Главное меню



3.5 Управление пользователями

В окне **User (Пользователь)** можно добавлять новых пользователей, просматривать списки пользователей, списки администраторов и изменять пароль администратора.

3.5.1 Добавление новых пользователей

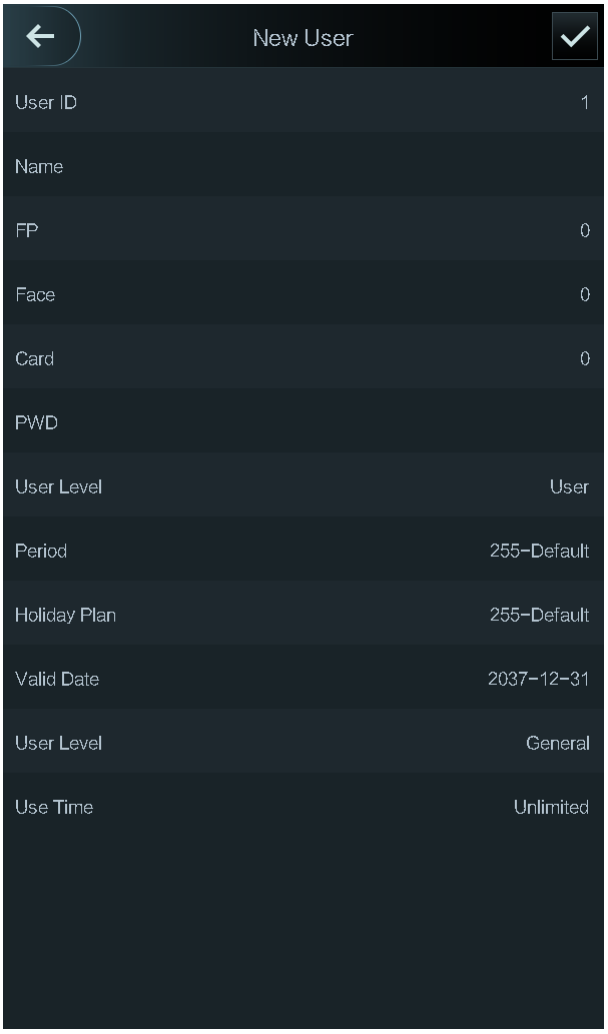
При добавлении новых пользователей вы можете вводить их ID, имена, импортировать их отпечатки пальцев, изображения лиц, карты, пароли, выбирать их категорию и т.д.

Следующие изображения представлены только для ознакомления, и преимущественное значение имеет реальный интерфейс.

Шаг 1 Выберите **User > New User (Пользователь > Новый пользователь)**.

Появится окно **New User** (**Новый пользователь)**. См. рисунок 3-5.

Рисунок 3-5 Информация о новом пользователе



Шаг 2 Выполните настройку параметров в этом окне. См. таблицу 3-2.

Таблица 3-2 Описание параметров нового пользователя

Параметр	Описание
User ID	Вы можете вводить ID пользователей. Для ID можно использовать цифры, буквы и их комбинации. Максимальная длина ID составляет 32 символа.
Name (имя)	Вы можете вводить имена пользователей, состоящие максимум из 32 символов (включая цифры, знаки и буквы).
FP	Можно записать максимум три отпечатка одного пользователя, и каждый отпечаток подтверждается трижды. Вы можете активировать функцию Duress FP для каждого отпечатка, и только один отпечаток будет использоваться для тревоги принуждения. Если такой отпечаток используется для открытия двери, срабатывает тревога. Не рекомендуется выбирать первый отпечаток пальца в качестве отпечатка для тревоги принуждения.
Face (лицо)	Убедитесь в том, что ваше лицо находится в центре изображения, контроллер доступа автоматически сделает снимок лица нового пользователя. Подробную информацию см. в *Кратком руководстве пользователя*.

Параметр	Описание
Card (карта)	Для каждого пользователя можно зарегистрировать до пяти карт. Введите номер вашей карты в окне регистрации карты или отсканируйте карту, после чего контроллер доступа будет осуществлять считывание карты. В окне регистрации карты можно активировать функцию **Duress Card**. При попытке разблокировать дверь с помощью карты с настройкой тревоги принуждения, сработает сигнализация. Только некоторые модели поддерживают разблокировку картой.
PWD	Пароль для разблокировки двери. Максимальная длина – 8 знаков.
User Level (категория пользователя)	Вы можете выбрать уровень для нового пользователя. Возможны два варианта. ● User (пользователь): Пользователь имеет полномочия только на открытие двери. ● Admin (администратор): Администраторы могут не только разблокировать двери, но и настраивать параметры системы. Аутентификация администратора требуется независимо от того, имеется ли администратор контроллера доступа.
Period (период)	Можно настраивать период, в течение которого пользователь может разблокировать дверь.
Holiday Plan (план праздничных дней)	Можно настраивать план праздничных дней, в течение которых пользователь может разблокировать дверь.
Valid Date (дата действия)	Можно настраивать период, в течение которого информация о разблокировании пользователем будет действительной.
User Level (категория пользователя)	Существует шесть категорий: ● General (общий): Общие пользователи могут открывать дверь в обычном режиме. ● Blacklist (черный список): Если дверь открывает пользователь из черного списка, обслуживающий персонал получает уведомление. ● Guest (гость): Гости могут открывать двери несколько раз в определенные периоды. После превышения максимального числа раз и истечения периода они не смогут открывать двери. ● Patrol (патруль): Отслеживается посещаемость патрулирующих пользователей, и они не имеют полномочий на открывание дверей. ● VIP: При открытии двери VIP-пользователем обслуживающий персонал получает уведомление. ● Disable (лица с ограниченными возможностями): Если дверь открывается лицом с ограниченными возможностями, произойдет задержка в 5 секунд до закрытия двери.
Use Time (время использования)	Для пользователей категории Guest можно настроить максимальное число раз открытия двери.

Шаг 3 После того, как вы установите параметры, нажмите чтобы сохранить настройки.

3.5.2 Просмотр информации о пользователях

В окне User можно просматривать списки пользователей, списки администраторов и активировать пароль администратора.

3.6 Управление доступом

You Вы можете осуществлять управление доступом по периодам, режиму разблокировки, сигнализации, статусу двери и времени задержки блокировки.

Нажмите **Access (доступ),** чтобы открыть окно управления доступом.

3.6.1 Управление периодами

Вы можете устанавливать периоды, периоды праздничных дней, периоды планов праздничных дней, периоды для открытой двери, периоды для закрытой двери и периоды удаленной верификации.

3.6.1.1 Настройка периодов

Вы можете настроить 128 периодов (недель) в диапазоне 0–127. Вы можете устанавливать по четыре периода для каждого дня периода (недели). Пользователи могут разблокировать дверь только в соответствии с установленными вами периодами.

3.6.1.2 Группы праздничных дней

Вы можете настроить группы праздничных дней, а затем планы для групп праздничных дней. Вы можете настроить 128 групп в диапазоне 0–127. В группу можно добавлять до 16 праздничных дней. Установите настройки времени начала и окончания для группы праздничных дней, и пользователи смогут разблокировать двери только в указанные вами периоды.

Можно вводить названия до 32 символов (включая цифры, знаки и буквы). Нажмите , чтобы сохранить название группы праздничных дней.

3.6.1.3 План праздничных дней

Группы праздничных дней можно добавлять в планы праздничных дней. Вы можете использовать планы праздничных дней, чтобы управлять полномочиями доступа пользователей в разных группах праздничных дней. Пользователи смогут разблокировать двери только в установленные вами периоды.

3.6.1.4 Период NO (открыто в штатном режиме)

Если период добавлен к периоду NO, в течение такого периода дверь будет открываться в обычном режиме.

Разрешения для периода NO/NC имеют преимущество над разрешениями в других периодах.

3.6.1.5 Период NC (закрыто в штатном режиме)

Если период добавлен к периоду NC, в течение такого периода дверь будет закрыта в штатном режиме. В этот период пользователи не смогут разблокировать двери.

3.6.1.6 Период удаленной верификации

Если настроить период удаленной верификации, при разблокировании двери в указанный период потребуется удаленная верификация. Чтобы разблокировать дверь в таком периоде, нужны инструкции по разблокировке двери, отправляемые с платформы управления.

You Необходимо активировать период удаленной верификации.

-  означает, что период активирован.
-  означает, что период не активирован.

3.6.2 Разблокирование

Существует три режима разблокирования: режим разблокирования, разблокирование по периоду и комбинация групп. Режимы разблокирования варьируются в зависимости от моделей контроллеров доступа, и фактический контроллер доступа будет иметь преимущественное значение.

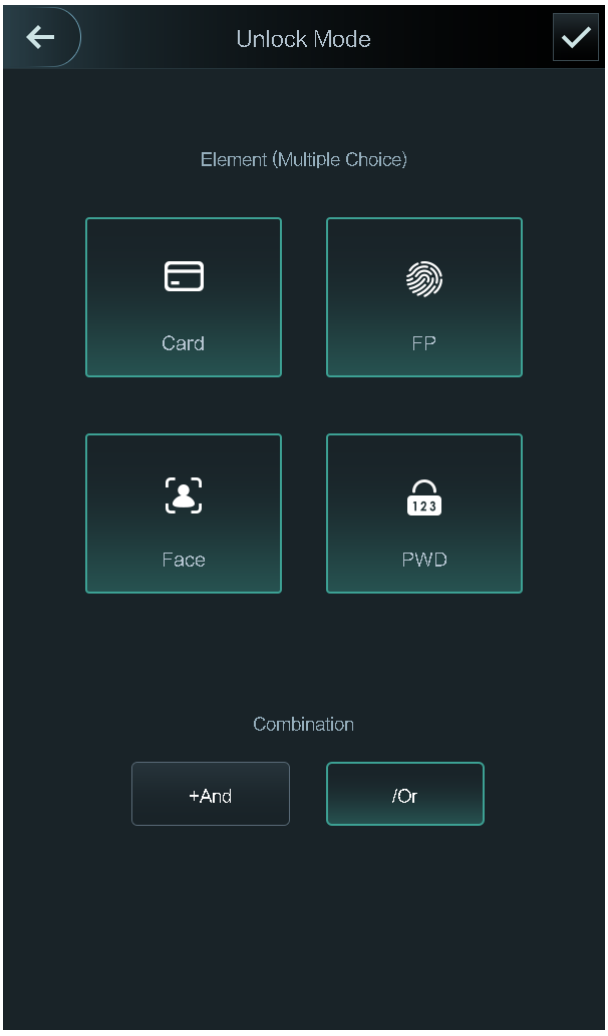
3.6.2.1 Режим разблокирования

Если **Unlock Mode (режим разблокирования)** активирован, пользователи могут разблокировать двери с помощью карт, отпечатков пальцев, изображений лиц, паролей или любым способом разблокирования.

Шаг 1 Перейдите по меню **Assess > Unlock Mode > Unlock Mode (Доступ > Режим разблокирования > Режим разблокирования)**.

Откроется окно **Element (Multiple Choice)**. См. рисунок 3-6.

Рисунок 3-6 Элемент (разные варианты)



Шаг 1 Выберите режим (ы) разблокирования.

Снова нажмите на режим разблокирования, чтобы удалить его.

Шаг 2 Выберите режим комбинации.

- **+ And** означает «и». Например, если выбрать «card + FP», это означает, чтобы разблокировать дверь, нужно сначала отсканировать карту, а затем отпечаток пальца.
- **/ Or** означает «или». Например, если выбрать «card/ FP», это означает, чтобы разблокировать дверь, нужно отсканировать либо карту, либо отпечаток пальца.

Шаг 4 Нажмите  , чтобы сохранить настройки.

Откроется окно **Unlock Mode (режим разблокирования)**.

Шаг 5 Активация режима разблокирования.

-  означает, что режим активирован.
-  означает, что режим не активирован.

3.6.2.2 Разблокирование по периодам

Двери можно разблокировать, используя разные режимы разблокирования в разные периоды. Например, в течение периода 1 дверь можно разблокировать только с помощью карты, а в течение периода 2 – только с помощью отпечатка пальца.

Шаг 1 Перейдите по меню Assess > Unlock Mode > Unlock by Period (Доступ > Режим разблокирования > Разблокирование по периоду).

Откроется окно **Unlock Config by Period (Настройка разблокирования по периоду)**. См. рисунок 3-7.

Рисунок 3-7 Разблокирование по периоду

Шаг 2 Установите время начала и окончания периода и выберите режим разблокирования.

Шаг 3 Нажмите  , чтобы сохранить настройки.

Откроется окно **Unlock Mode (Режим разблокирования)**.

Шаг 4 Активируйте функцию разблокирования по периоду.

-  означает, что функция активирована.
-  означает, что функция не активирована.

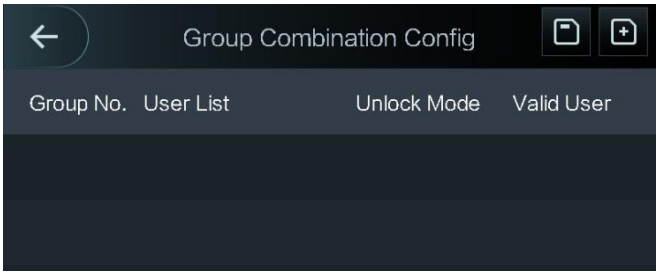
3.6.2.3 Комбинация групп

Двери можно открывать, используя группу или группы, состоящие из более двух пользователей, если активирована комбинация групп.

Шаг 1 Выберите **Assess > Unlock Mode > Group Combination (Доступ > Режим разблокирования > Комбинация групп)**.

Откроется окно **Group Combination Config (Настройка комбинации групп)**. См. рисунок 3-8.

Рисунок 3-8 Комбинация групп



Шаг 2 Нажмите  , чтобы создать группу.

Откроется окно **Add Group (Добавить группу)**. См. рисунок 3-9

Рисунок 3-9 Добавление группы

Таблица 3-3 Параметры группы

Параметр	Описание
User List (Список пользователей)	Добавление пользователей в новую создаваемую группу. 1. Нажмите **User List (Список пользователей)**. Откроется окно **User List**. 2. Нажмите  и введите ID пользователя. 3. Нажмите  , чтобы сохранить настройки.
Unlock Mode (Режим разблокирования)	Существует 4 варианта: **Card (карта), FP (отпечаток пальца), PWD (пароль)** и **Face (лицо)**.
Valid User (зарегистрированный пользователь)	Зарегистрированные пользователи – это пользователи, которые имеют разрешение на разблокирование двери. Двери могут быть разблокированы, только если количество пользователей, разблокирующих дверь, совпадает количеству зарегистрированных пользователей. ● Количество зарегистрированных пользователей не может превышать общее количество пользователей в группе. ● Если количество зарегистрированных пользователей равно общему количеству пользователей в группе, двери могут быть разблокированы всеми пользователями группы. ● Если количество зарегистрированных пользователей меньше общего количества пользователей в группе, двери могут быть разблокированы пользователями, количество которых соответствует количеству зарегистрированных пользователей.

Шаг 3 Нажмите  , чтобы вернуться в предыдущее окно.

Шаг 4 Нажмите  , чтобы сохранить настройки.

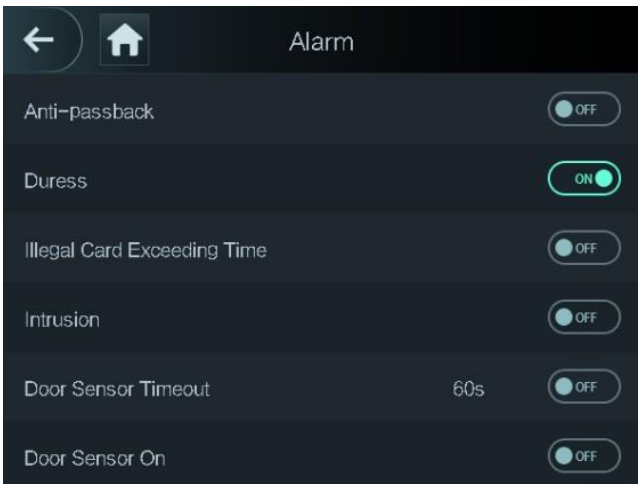
Шаг 5 Активируйте **Group Combination**.

-  означает, что комбинация групп активирована.
-  означает, что комбинация групп не активирована.

3.6.3 Настройка сигнализации

Администраторы могут управлять полномочиями пользователей по разблокированию с помощью настроек сигнализации. Перейдите по меню **Access > Alarm (Доступ > Сигнализация)**. Откроется окно Alarm. См. рисунок 3-10.

Рисунок 3-10 Сигнализация



-  означает, что сигнализация активирована.
-  означает, что сигнализация не активирована.

Таблица 3-4 Параметры окна «Сигнализация»

Параметр	Описание
Anti-passback (запрет прохода в обратном направлении)	• Если личность человека проверяется, когда он разблокирует дверь, но не проверяется, когда он выходит, сработает сигнал тревоги, и этот человек не сможет снова разблокировать дверь. • Если человек, входя в здание или помещение, не сканирует карту, но сканирует ее при выходе, он больше не сможет разблокировать двери.
Duress (принуждение)	Если для разблокирования двери используется карта, пароль или отпечаток пальца, для которых установлена тревога принуждения, сработает сигнал тревоги.
Illegal Card Exceeding Time (превышение времени для недействительной карты)	Если недействительная карта будет использоваться для разблокирования двери больше 5 раз за 50 секунд, сработает сигнал тревоги.
Intrusion (вторжение)	Сработает сигнал о вторжении, если при разблокировании двери дверной контакт не будет разомкнут.
Door Sensor Timeout (время ожидания для датчика двери)	Сработает сигнал о превышении времени, если время, используемое для разблокирования, превышает время ожидания для датчика двери. Время ожидания для датчика двери устанавливается в диапазоне 1–9999 секунд.
Door Sensor On (Датчик двери активен)	Сигналы о вторжении и времени ожидания для датчика двери будут срабатывать только если активирована функция **Door Sensor On**.

3.6.4 Статус двери

Существует три варианта: **NO (открыто в штатном режиме)**, **NC (закрыто в штатном режиме)** и **Normal (обычный режим)**.

- NO: Если выбрать **NO**, статус двери будет «открыта в штатном режиме», то есть дверь не будет закрываться.
- NC: Если выбрать **NC**, статус двери будет «закрыта в штатном режиме», то есть дверь не будет открываться.
- Normal: Если выбрать **Normal,** дверь будет открываться и закрываться в зависимости от установленных настроек.

3.6.5 Продолжительность разблокирования

Lock Holding Time (Продолжительность разблокирования) – это время разблокирования двери. Если разблокирование проходит дольше этого времени, произойдет автоматическая блокировка.

3.7 Сетевая связь

Чтобы обеспечить нормальную работу контроллера доступа, необходимо настроить параметры сети, серийных портов и портов Wiegand.

3.7.1 IP-адрес

3.7.1.1 Настройка IP-адреса

Выполните настройку IP-адреса для контроллера доступа, чтобы подключить его к сети. См. рисунок 3-11 и таблицу 3-5.

Рисунок 3-11 Настройка IP-адреса

Таблица 3-5 Параметры настройки IP-адреса

Parameter	Description
IP Address/Subnet Mask/Gateway IP Address (IP-адрес/маска подсети/ IP-адрес шлюза)	IP-адрес, маска подсети и IP-адрес шлюза должны быть в одном сетевой сегменте. После того, как вы установите настройки, нажмите , чтобы сохранить их.
DHCP	DHCP (протокол динамической настройки хостов). Если DHCP активирован, IP-адрес можно получить автоматически, а IP-адрес, маску подсети и IP-адрес шлюза нельзя настроить вручную.
P2P	P2P – это технология обхода частных сетей, которая позволяет управлять устройствами без DDNS, распределения портов или транзитного сервера.

3.7.1.2 Активный реестр

Используя активный реестр, можно подключить контроллер доступа к платформе управления и управлять контроллером доступа с ее помощью.

Установленные вами настройки можно удалить в платформе управления, и можно выполнить инициализацию контроллера доступа. Вам необходимо обеспечить защиту для полномочий по управлению платформой, чтобы предотвратить потерю данных, связанную с неправильной эксплуатацией.

Параметры активного реестра см. в таблице 3-6.

Таблица 3-6 Активный реестр

Название	Параметр
IP-адрес сервера	IP-адрес платформы управления.
Порт	Номер порта платформы управления.
ID устройства	Количество подчиненных устройств для платформы управления.

3.7.1.3 Wi-Fi

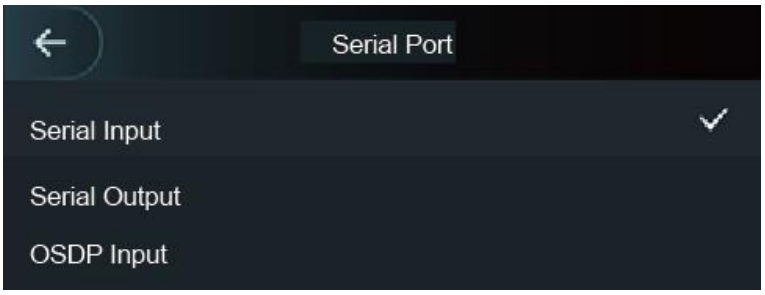
Контроллер доступа можно подключить к сети через Wi-Fi, если в нем предусмотрена функция Wi-Fi.

3.7.2 Настройки серийных портов

Выберите серийный входной или выходной порт в зависимости от направления входа и выхода.

Перейдите по меню **Connection > Serial Port (Подключение > Серийный порт)**, и откроется окно **Serial Port**. См. рисунок 3-12.

Рисунок 3-12 Серийный порт



- Выберите **Serial Input (Серийный вход),** если к контроллеру доступа подключены внешние устройства, выполняющие функции считывания карт и записи. **Serial Input** выбирается для того, чтобы отправлять информацию с карты доступа на контроллер доступа и платформу управления.
- Что касается контроллеров доступа с функциями распознавания лиц, отпечатков пальцев, считывания карт и записи, если выбрать **Serial Output (Серийный выход)**, контроллер доступа будет отправлять информацию о блокировке/разблокировке. К информации о блокировке/разблокировке относятся два вида данных:
  - ◇ ID пользователя
  - ◇ Номер карты
- Выберите **OSDP Input (Вход OSDP),** если к контроллеру доступа подключен считыватель карт с протоколом OSDP. Контроллер доступа будет отправлять информацию с карты на платформу управления.

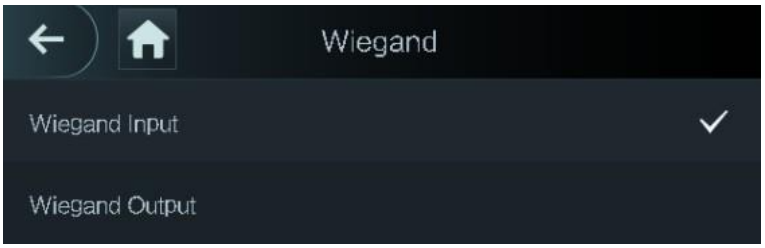
Этот контроллер доступа нельзя подключить к другим устройствам, таким как считыватели карт.

3.7.3 Настройка Wiegand

Выберите **Weigand Input (Вход Weigand)** или **Weigand Output (Выход Weigand)** в зависимости от направления входа и выхода.

Перейдите по меню **Connection > Weigand (Подключение > Weigand)**, и откроется окно **Weigand**. См. рисунок 3-13.

Рисунок 3-13 Weigand



- Выберите **Weigand Input (Вход Weigand),** если к контроллеру доступа подключен внешний механизм считывания карт.
- Выберите **Weigand Output (Выход Weigand),** если контроллер доступа работает как считыватель, который можно подключить к контроллеру. См. таблицу 3-7.

Таблица 3-7 Выход Weigand

Параметр	Описание
Weigand output type (Тип выхода Weigand)	Тип выхода Weigand определяет номер карты или знак номера, который может распознаваться контроллером доступа. ● Weigand26, три байта, шесть знаков. ● Weigand34, четыре байта, восемь знаков. ● Weigand66, восемь байтов, шестнадцать знаков.
Pulse Width (Ширина импульса)	Можно настроить ширину и интервал импульса.
Pulse Interval (Интервал импульса)	
Output Data Type (Тип выходных данных	Можно выбрать тип выходных данных. ● User ID: Если выбрать ID пользователя, будут передаваться ID пользователей. ● Card No.: Если выбрать номер карты, будут передаваться номера карт.

Этот контроллер доступа нельзя подключить к другим устройствам, таким как считыватели карт.

3.8 Система

3.8.1 Время

Вы можете настраивать формат даты, дату, время, DST, проверку NTP и часовой пояс.

- Если вы выбираете Network Time Protocol (NTP, сетевой протокол синхронизации времени), сначала нужно активировать функцию проверки NTP (NTP Check). IP-адрес сервера: введите IP-адрес сервера времени, и время контроллера доступа будет синхронизироваться со временем сервера времени.
- Port (Порт): Введите номер порта сервера времени.
- Interval (min) (Интервал (мин)): Интервал проверки NPT. Нажмите на значок сохранения, чтобы сохранить настройки.

3.8.2 Параметры распознавания лиц

Таблица 3-14 Параметры распознавания лиц

Нажмите на параметр, установите настройки, а затем нажмите .

Таблица 3-8 Параметры распознавания лиц

Название	**Описание**
Face Recognition Threshold (Предел распознавания лиц)	Можно настроить точность распознавания лиц. Чем больше значение, тем выше будет точность.
Max. Angle of Face Recognition (Макс. угол распознавания лиц)	Можно настроить снимки угла профиля с панели управления. Чем больше значение, тем шире будет диапазон профиля при распознавании.
Pupillary Distance (Межцентровое расстояние)	Межцентровое расстояние – это значение расстояния между центрами зрачков обоих глаз на изображении в пикселях. Вам нужно установить соответствующее значение, чтобы контроллер доступа мог распознавать лица должным образом. Значение изменяется в соответствии с размерами лиц и расстоянием между лицом и объективом. Чем ближе лицо к объективу, тем выше будет значение. Если взрослый находится на расстоянии 1,5 метра от объектива, значение межцентрового расстояния будет от 50 до 70.
Recognition Timeout (Максимальное время ожидания при распознавании)	Если человек, не имеющий права доступа, стоит перед контроллером доступа, и происходит распознавание его лица, контроллер сообщит, что распознавание не было успешно выполнено. Интервал сообщения называется максимальным временем ожидания при распознавании.
Recognition Interval (Интервал распознавания)	Если человек, имеющий права доступа, стоит перед контроллером доступа, и происходит распознавание его лица, контроллер сообщит, что распознавание было успешно выполнено. Интервал сообщения – это интервал распознавания.
Anti-fake Threshold (максимальное время ожидания при защите от подделок)	Эта функция предотвращает использование изображений и моделей лиц. Чем выше значение, тем труднее процесс разблокирования с помощью изображений лиц. Рекомендуемое значение: выше 80.

3.8.3 Настройка режима заполнения светом

Вы можете выбрать режим заполнения света, в соответствии с вашими требованиями. Существуют три режима:

- Auto: Если фотодатчик определяет, что сцена не является темной, заполняющий свет выключен в обычном режиме; в противном случае, он будет включаться.
- NO: Заполнение светом активно в штатном режиме.
- NC: Заполнение светом не активно в штатном режиме.

3.8.4 Настройка яркости при заполнении светом

Вы можете настроить яркость заполнения светом в соответствии с вашими требованиями.

3.8.5 Регулировка звука

Нажмите  или  , чтобы отрегулировать громкость звука.

3.8.6 Настройка яркости ИК-подсветки

Чем выше значение, тем более четкими будут изображения и наоборот.

3.8.7 Параметры отпечатков пальцев

Настройка уровня точности отпечатков пальцев. Чем выше значение, тем меньше будет число ложных распознаваний.

3.8.8 Сброс до заводских настроек

- Если выполнить сброс до заводских настроек, данные будут утеряны.
- После выполнения сброса контроллера доступа до заводских настроек IP-адрес не изменится.

Вы можете выбрать, нужно ли сохранять информацию о пользователях и журналы.

- Вы можете выбрать удаление всей информации о пользователях и устройстве при сбросе до заводских настроек.
- Вы можете выбрать сохранение всей информации о пользователях и устройстве при сбросе до заводских настроек.

3.8.9 Перезагрузка

Перейдите по меню **Setting > Reboot (Настройки > Перезагрузка)**, нажмите **Reboot**, и контроллер доступа будет перезагружен.

3.9 USB

- Перед выполнением экспорта пользовательской информации и обновлением убедитесь в том, что USB-устройство подключено. В ходе экспорта или обновление не извлекайте USB-устройство и не выполняйте другие операции; в противном случае, экспорт или обновление не будут выполнены.
- Чтобы импортировать информацию с одного контроллера доступа на другой, сперва нужно импортировать ее на USB-устройство.
- USB-устройство также можно использовать для обновления программы.

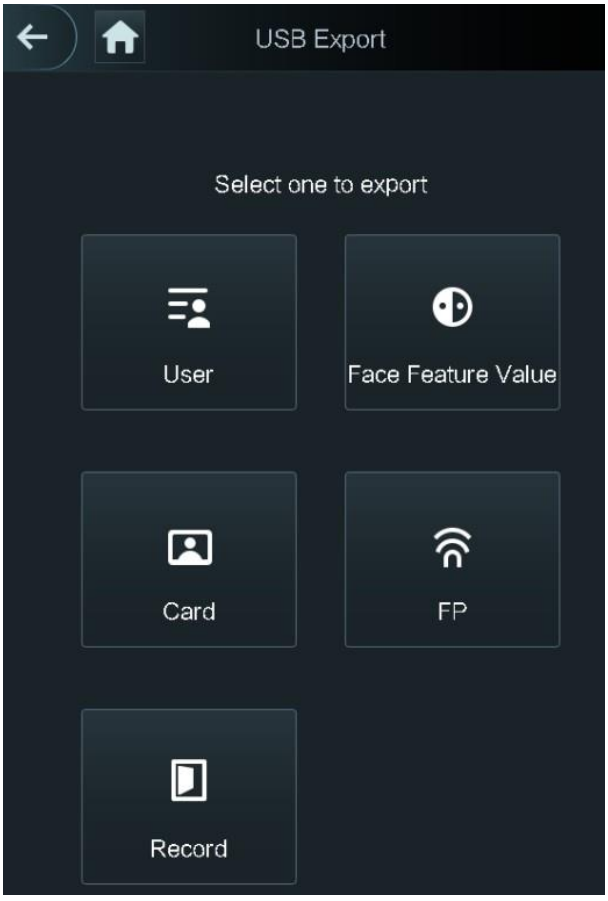
3.9.1 Экспортирование на USB-устройство

После того, как вы подключите USB-устройство, вы сможете экспортировать на него данные с контроллера доступа. Экспортируемые данные подвергаются шифрованию, и их невозможно редактировать.

Шаг 1 Перейдите по меню **USB > USB Export (USB > Экспорт на USB)**.

Откроется окно **USB Export**. См. рисунок 3-15.

Рисунок 3-15 Экспорт на USB-устройство



Шаг 2 Выберите тип данных, которые вы хотите экспортировать.

Появится сообщение о подтверждении (Confirm to export).

Шаг 3 Нажмите **OK**.

Экспортируемые данные будут сохранены на USB-устройстве.

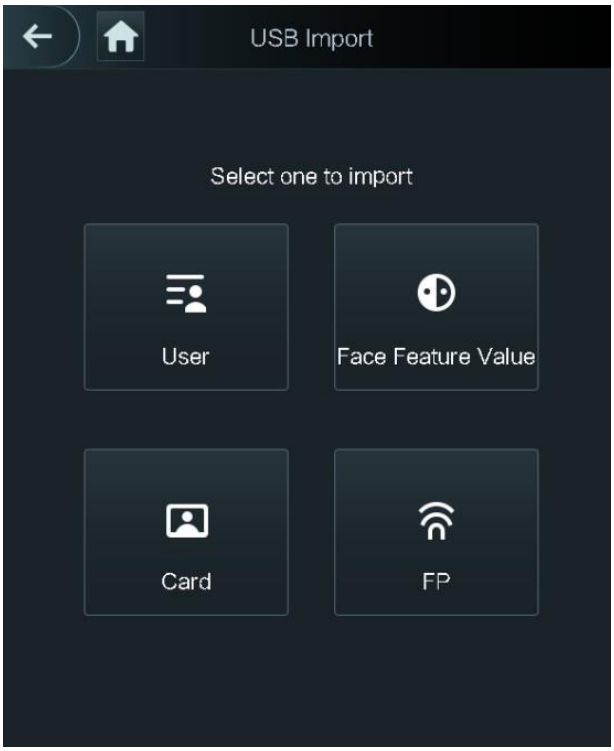
3.9.2 Импортирование с USB-устройства

Импортировать с одного контроллера доступа на другой можно только данные, сохраненные на USB-устройстве.

Шаг 1 Перейдите по меню **USB > USB Import (USB > Импорт с USB).**

Откроется окно **USB Import**. См. рисунок 3-16.

Рисунок 3-16 Импорт с USB-устройства



Шаг 2 Выберите тип данных, которые вы хотите экспортировать.

Появится сообщение о подтверждении (**Confirm to import**).

Шаг 3 Нажмите **OK**.

Данные с USB-устройства будут импортированы в контроллер доступа.

3.9.3 Обновление с помощью USB-устройства

USB-устройство можно использовать для обновления системы.

Шаг 1 Измените имя файла обновления на «update.bin» и сохраните «update.bin» в корневой директории USB-устройства.

Шаг 2 Перейдите по меню **USB > USB Update (USB > Обновление с USB)**.

Появится сообщение о подтверждении (**Confirm to Update**).

Шаг 3 Нажмите **OK**.

Запустится процесс обновления, и после завершения контроллер доступа будет перезагружен.

3.9.4 Функции

Вы можете устанавливать настройки приватности, инверсии номеров карт, модуля безопасности, типа датчика двери и данных о результатах. Подробную информацию об этих функциях см. на рисунке 3-17 и в таблице 3-9.

Рисунок 3-17 Функции

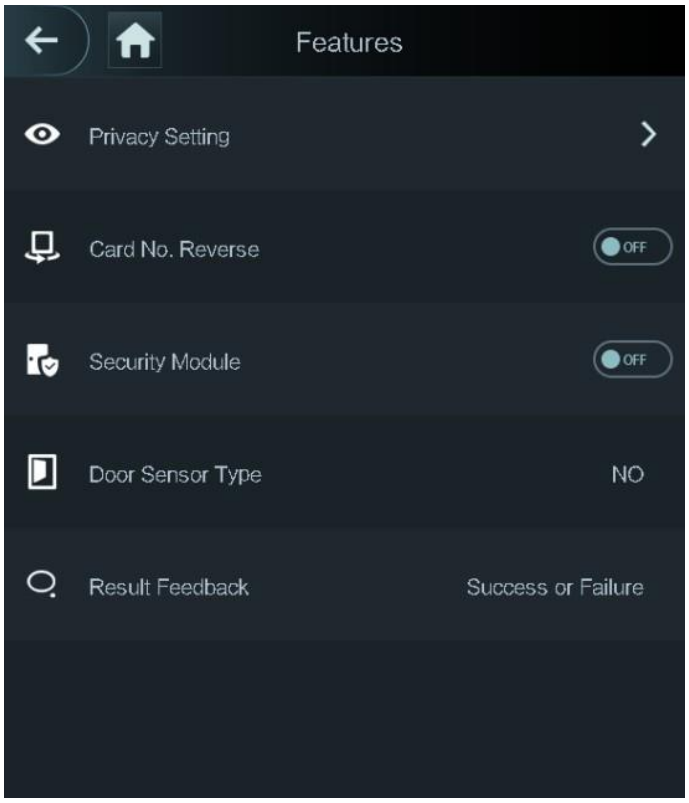


Таблица 3-9 Описание функций

Параметр	Описание
Privacy Setting (Настройки приватности)	Подробную информацию см. в разделе 3.9.5 «Настройки приватности).
Card No. Reverse (Инверсия номеров карт)	Если к контроллеру доступа необходимо подключить считыватель карт другого производителя через выходной порт Wiegand, нужно активировать функцию инверсии номеров карт, или связь между контроллером доступа и считывателем карт может быть не установлена из-за несоответствия протоколов.
Security Module (Модуль безопасности)	● Если модуль безопасности активирован, модуль безопасности для контроля доступа необходимо приобрести отдельно. Для модуля безопасности требуется отдельный источник питания. ● Если модуль безопасности активирован, кнопка выхода, управление блокировкой и пожарная сигнализация не будут активны.
Door Sensor Type (Тип датчика двери)	Существует два варианта: **NO (открыто в штатном режиме)** и **NC (закрыто в штатном режиме)**.
Result Feedback (Данные о результатах)	Показывает, успешно ли было выполнено разблокирование.

3.9.5 Настройки приватности

Рисунок 3-18 Настройки приватности

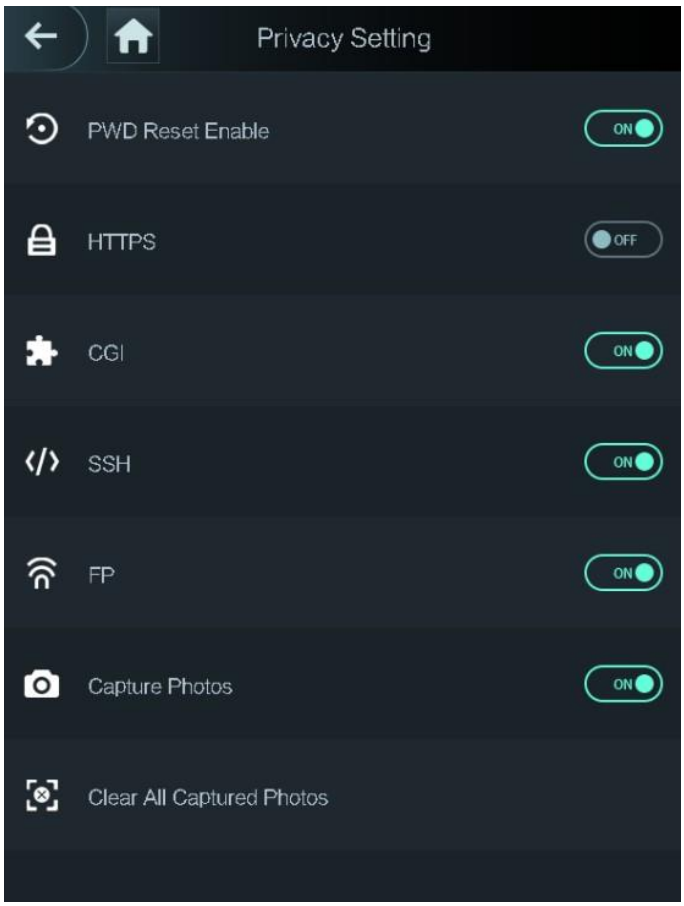


Таблица 3-10 Функции

Параметр	Описание
PWD Reset Enable (Активация сброса пароля)	Если функция **PWD Reset Enable** активирована, вы можете сбросить пароль. Функция сброса пароля активна по умолчанию.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS, протокол защищенной передачи гипертекста) – это протокол, обеспечивающий безопасную связь по компьютерной сети. Если HTTPS активирован, он будет использоваться для доступа к командам CGI; в противном случае, используется HTTP. Если активировать HTTPS, контроллер доступа автоматически перезапустится.
CGI	Common Gateway Interface (CGI, общий шлюзовый интерфейс) представляет собой стандартный протокол для веб-серверов для исполнения программ, например, консольных приложений, работающих на сервере, который создает веб-страницы динамически. Если CGI активирован, можно использовать команды CGI. CGI активен по умолчанию.
SSH	Secure Shell (SSH, протокол безопасной оболочки) – это протокол сети засекреченной связи с криптографической защитой для безопасной работы с сетевыми сервисами через незащищенную сеть. Если SSH активирован, он обеспечивает криптографические сервисы для передачи данных.

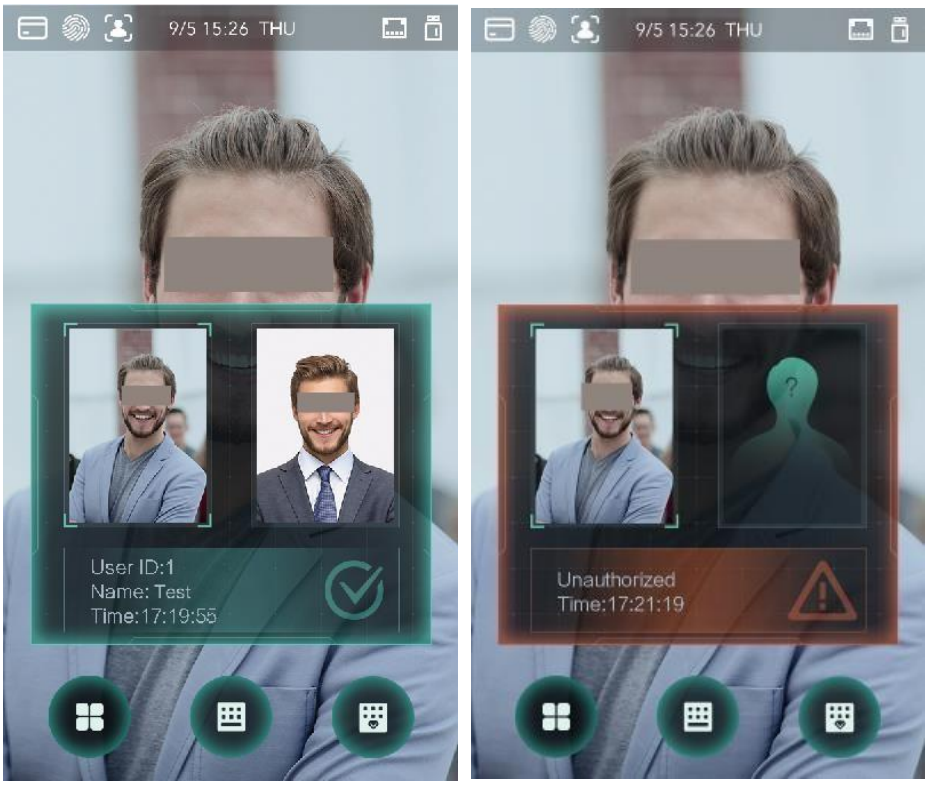
Параметр	Описание
FP	Если выбрать OFF для отпечатков пальцев (FP), информация об отпечатках пальцев пользователей не будет отображаться при записи отпечатков или их использовании для разблокирования дверей.
Capture photo (Снимок)	Если выбрать ON, когда пользователь разблокирует дверь, автоматически осуществляется снимок его фото. По умолчанию эта функция включена.
Clear all captured photos (Удалить все снимки)	Нажмите на значок, чтобы удалить все сделанные снимки.

3.9.6 Данные о результатах

Вы можете выбрать нужный режим для данных о результатах.

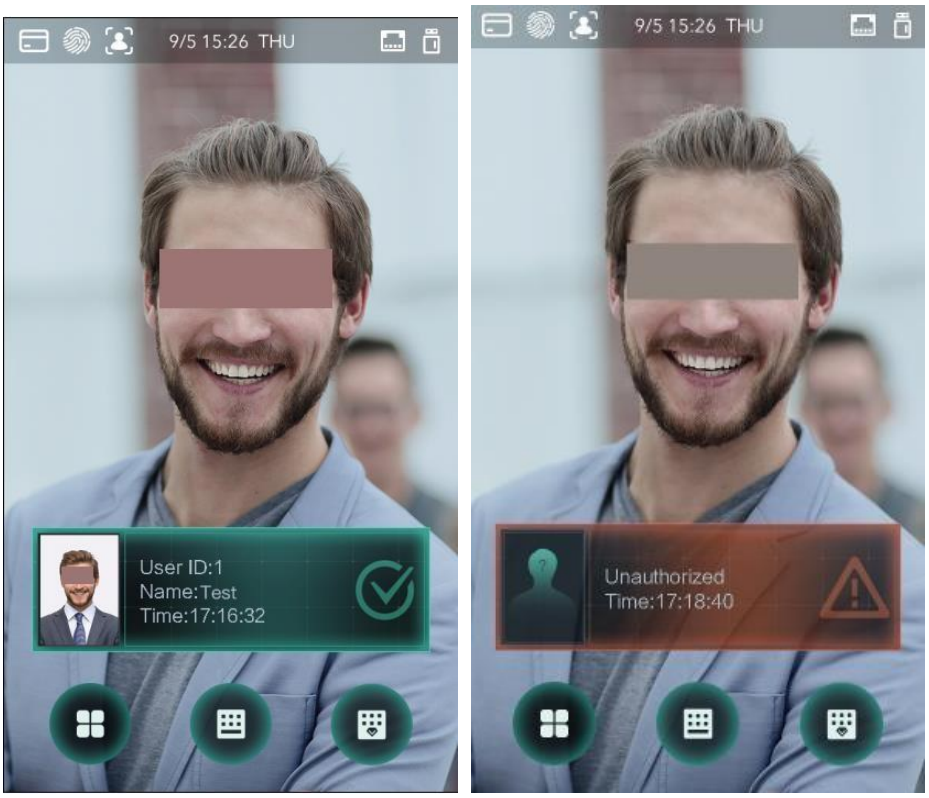
Режим 1

Рисунок 3-19 Режим 1



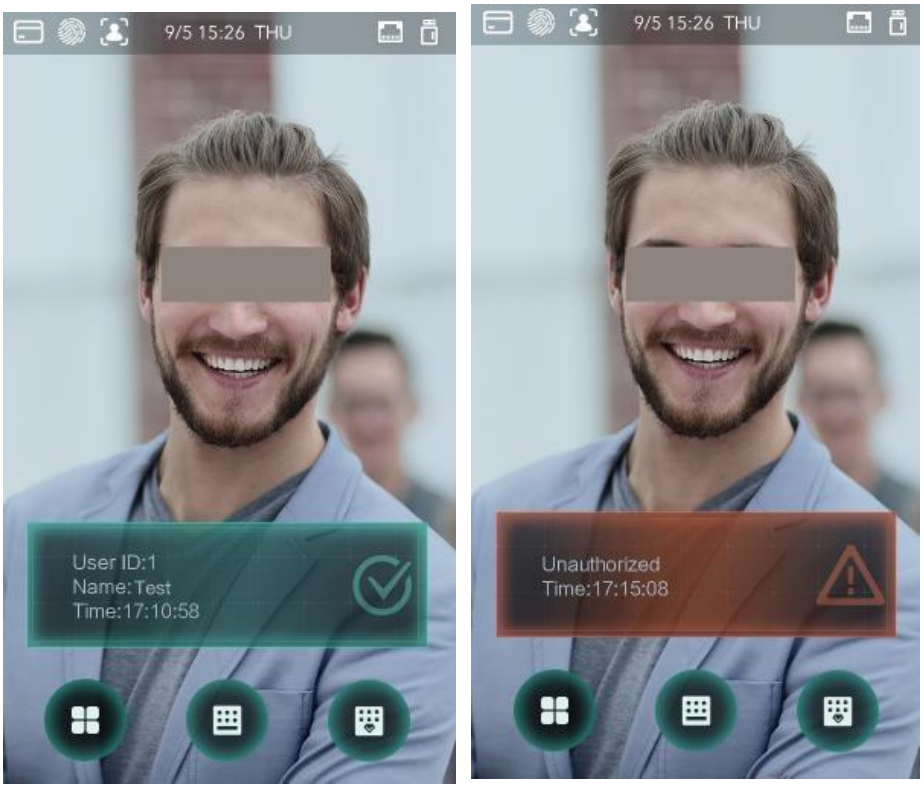
Режим 2

Рисунок 3-20 Режим 2



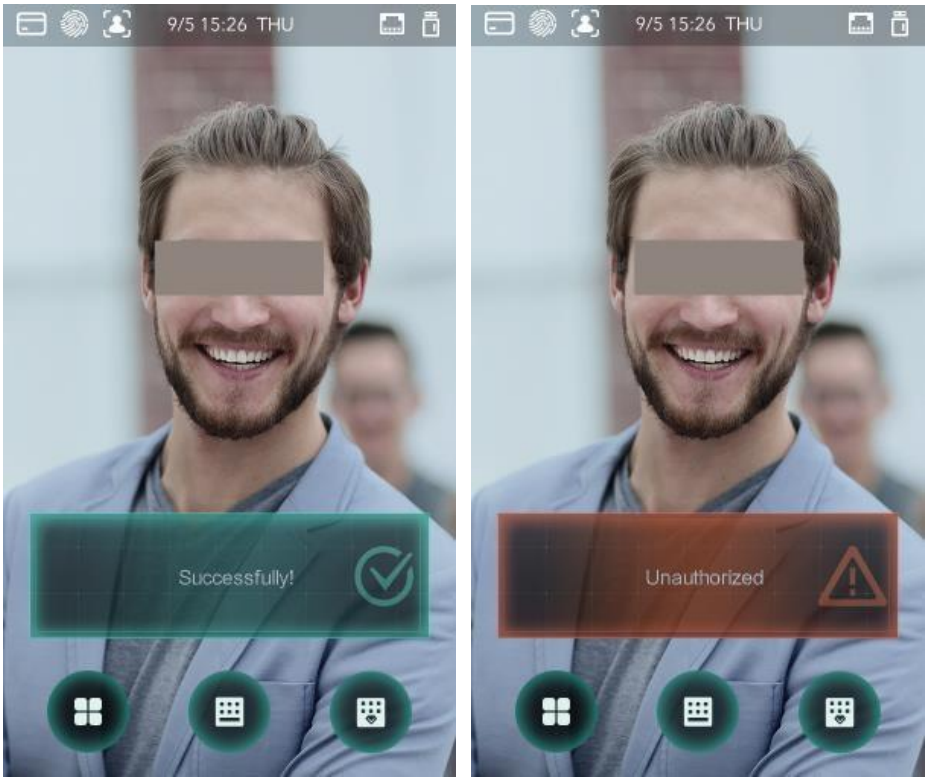
Режим 3

Рисунок 3-21 Режим 3



Режим 4

Рисунок 3-22 Режим 4



3.10 Запись

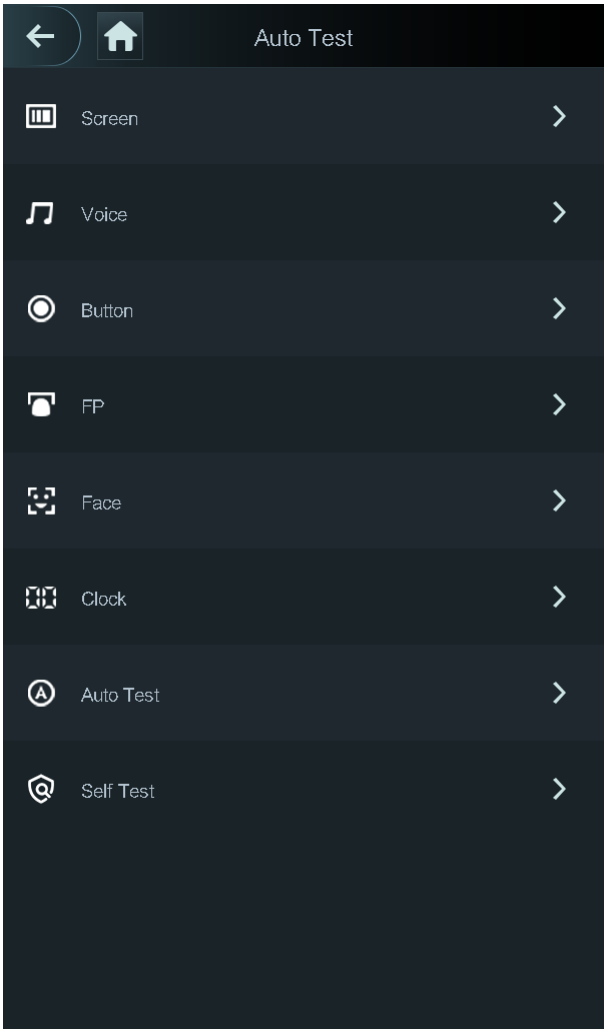
Вы можете запрашивать все записи о разблокировке.

Рисунок 3-23 Поиск записей

3.11 Автоматическое тестирование

Если вы используете контроллер доступа в первый раз или если контроллер доступа работает неправильно, вы можете использовать функцию автоматического тестирования, чтобы проверить, может ли контроллер нормально работать. Выполняйте действия в соответствии с указаниями.

Рисунок 3-24 Автоматическое тестирование



Если выбрать **Auto Test**, контроллер доступа будет отображать указания по выполнению автоматического тестирования.

3.12 Информация о системе

Узнать информацию об объеме данных, версии устройства и программном обеспечении контроллера доступа можно в окне **System Info**.

4 Работа с веб-интерфейсом

Контроллер доступа можно настраивать и работать с ним в веб-интерфейсе. С помощью веб-интерфейса можно настраивать такие параметры как параметры сети, параметры видео и параметры контроля доступа; здесь также можно осуществлять обновление системы.

4.1 Инициализация

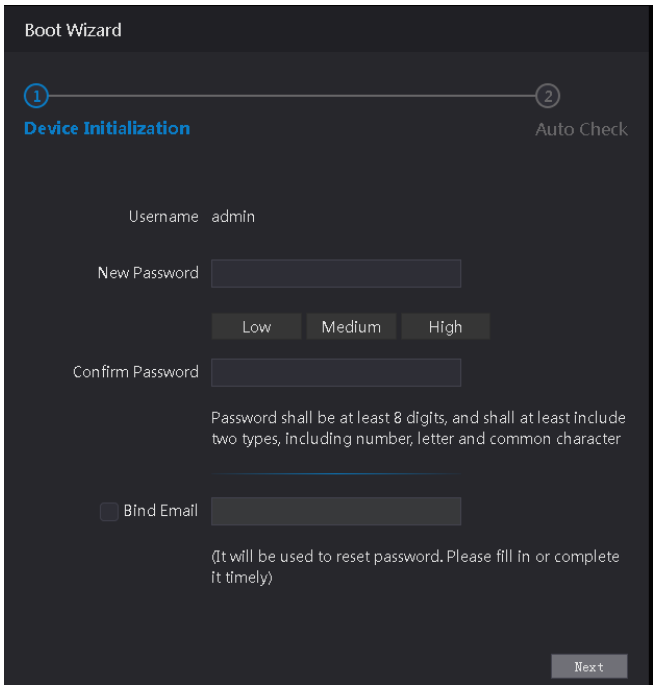
Перед первой авторизацией в веб-интерфейсе необходимо настроить пароль и указать адрес электронной почты.

Шаг 1 Откройте браузер IE, введите IP-адрес (192.168.1.108 по умолчанию) контроллера доступа в адресной строке и нажмите Enter.

Откроется окно **Initialization (Инициализация)**. См. рисунок 4-1

Используйте браузер версии позднее IE 8, или вы не сможете войти в систему.

Рисунок 4-1 Инициализация



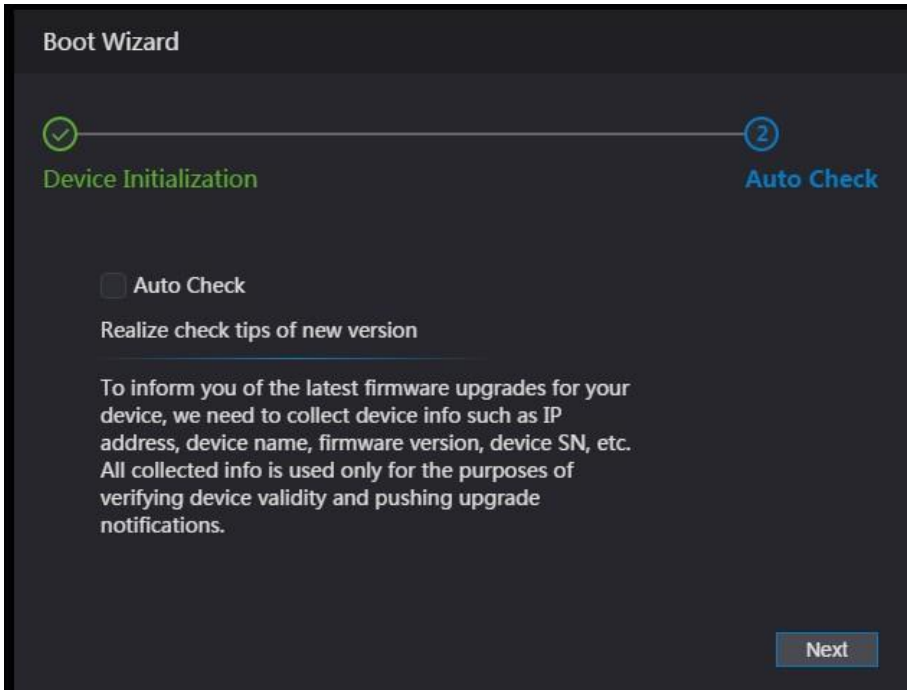
Шаг 2 Введите новый пароль, подтвердите пароль, введите адрес электронной почты и нажмите **Next (Далее)**.

- В целях обеспечения безопасности, после инициализации храните пароль надежным образом и регулярно меняйте пароли.
- Пароль должен содержать от 8 до 32 символов без пробелов и как минимум два типа символов, включая верхний и нижний регистр, цифры и специальные знаки (кроме ' " ; : &). Установите пароль с высоким уровнем безопасности в соответствии с подсказками по надежности паролей.
- Если вам нужно сбросить пароль администратора путем сканирования QR-кода, вам потребуется электронная почта, куда будет отправлен код безопасности.

Шаг 3 Нажмите **Next (Далее)**.

Откроется окно **Auto Check (Автоматическая проверка)**. См. рисунок 4-2.

Рисунок 4-2 Автоматическая проверка



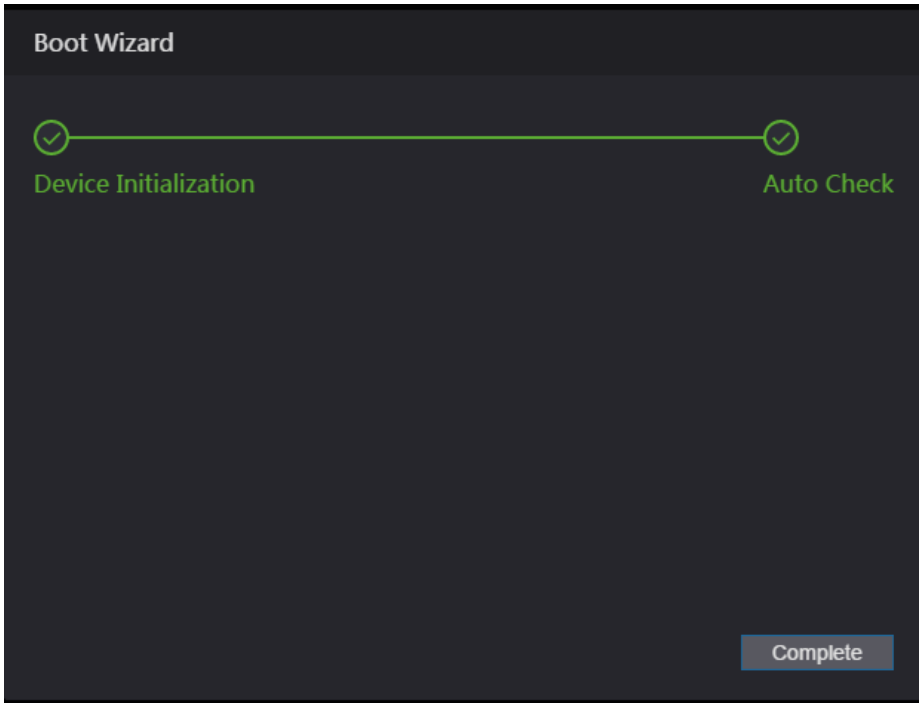
Шаг 4 Вы можете решить, нужно ли выбрать **Auto Check**.

Рекомендуется выбирать **Auto Check,** чтобы своевременно обновляться до последней версии программы.

Шаг 5 Нажмите Next (Далее).

Настройка окончена. См. рисунок 4-3.

Рисунок 4-3 Настройка завершена



Шаг 6 Нажмите **Complete (Завершить)**, и процесс инициализации будет завершен. Появится окно авторизации в веб-интерфейсе.

4.2 Авторизация

Шаг 1 Откройте браузер IE, введите IP-адрес контроллера доступа в адресной строке,

и нажмите **Enter**.

Рисунок 4-4 Авторизация

Шаг 2 Введите имя пользователя и пароль.

- Имя администратора по умолчанию – admin, а пароль – это пароль входа после инициализации контроллера доступа. Регулярно меняйте пароль администратора и обеспечивайте его надежное хранение.
- Если вы забыли пароль администратора, вы можете нажать **Forget Password? (Забыли пароль?),** чтобы переустановить пароль. См. раздел 4.3 «Смена пароля».

Шаг 3 Нажмите **Login (Войти)**.

Авторизация в веб-интерфейсе завершена.

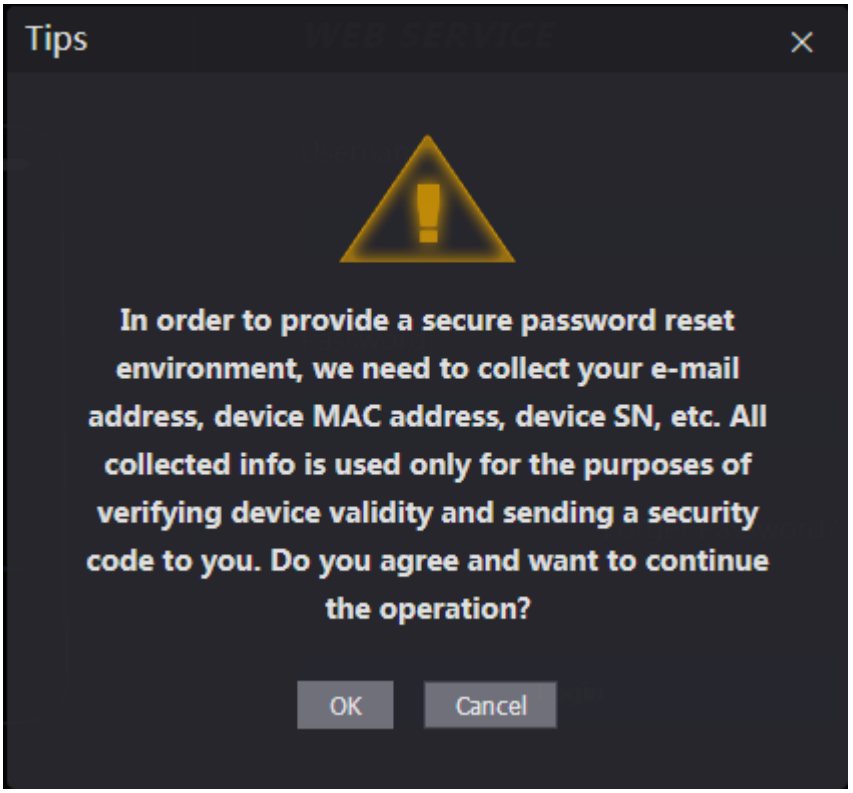
4.3 Смена пароля

При настройке пароля учетной записи администратора требуется ваш адрес электронной почты.

Шаг 1 Нажмите **Forgot password? (Забыли пароль?)** в окне авторизации.

Появится окно **Tips (Рекомендации)**.

Рисунок 4-5 Рекомендации

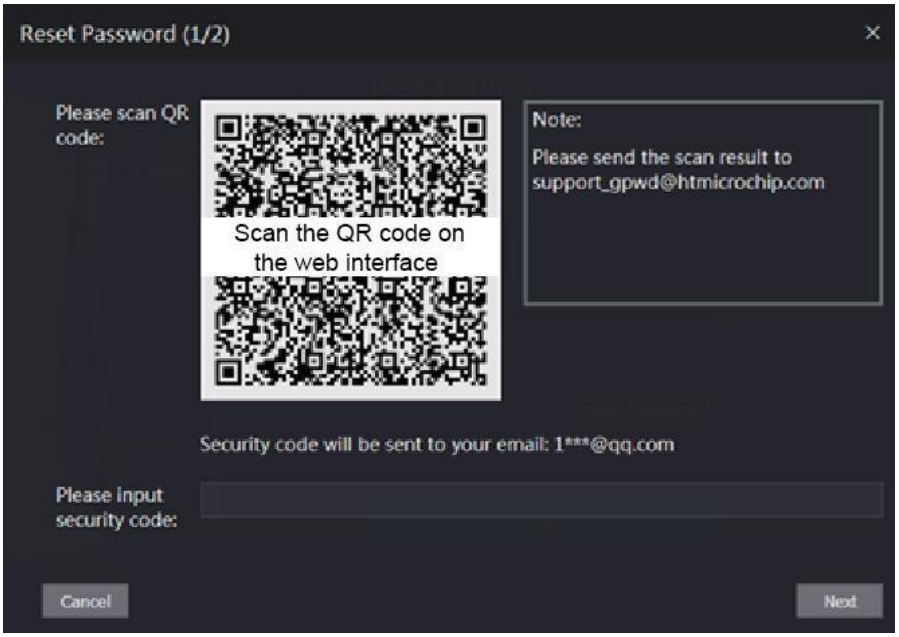


Шаг 2 Прочтите рекомендации.

Шаг 3 Нажмите OK.

Откроется окно **Reset Password (Сбросить пароль)**.

Рисунок 4-6 Сбросить пароль



Шаг 4 Отсканируйте QR-код в окне, и вы получите код безопасности.

- При сканировании одного QR-кода может быть генерировано не больше двух кодов безопасности. Если код безопасности стал недействительным, чтобы получить новые коды безопасности, обновите QR-код.
- После сканирования QR-кода полученное содержание необходимо отправить на указанный адрес электронной почты, тогда вы получите код безопасности.

- Используйте код безопасности в течение 24 часов после получения. В противном случае, он станет недействительным.
- Если пять раз подряд были введены неправильные коды безопасности, администратор будет заблокирован на пять минут.

Шаг 5 Введите полученный код безопасности.

Шаг 6 Нажмите **Next (Далее)**.

Откроется окно **Reset Password (Сбросить пароль).**

Шаг 7 Переустановите и подтвердите новый пароль.

Пароль должен содержать от 8 до 32 символов без пробелов и как минимум два тапа символов, включая верхний и нижний регистр, цифры и специальные знаки (кроме ' " ; : &).

Шаг 8 Нажмите **OK**, и смена пароля будет завершена.

4.4 Каналы сигнализации

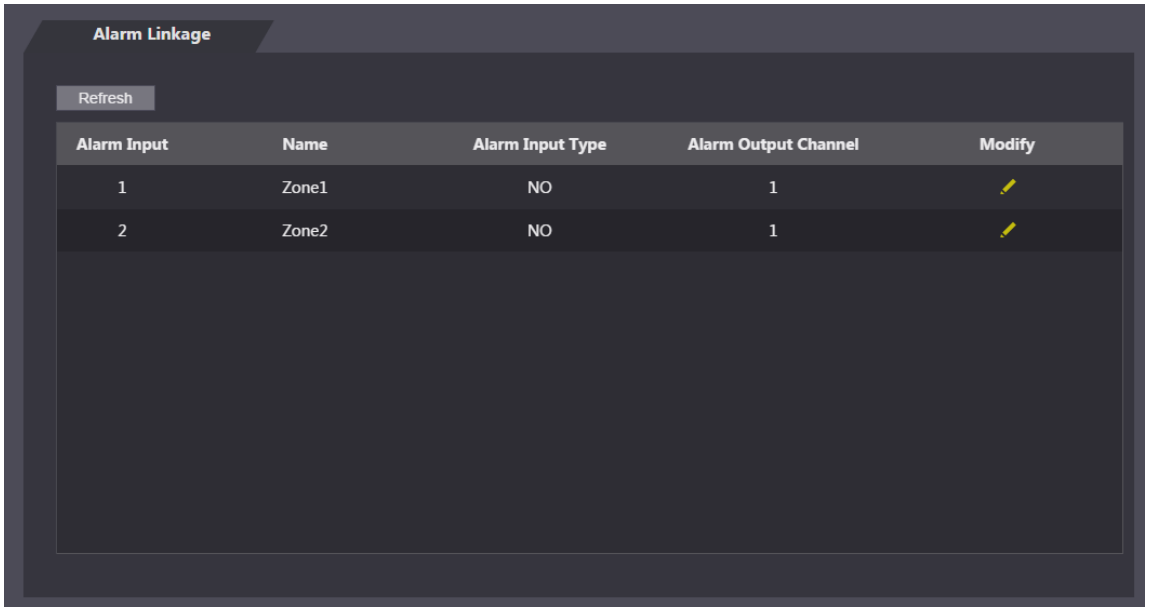
4.4.1 Настройка каналов сигнализации

К контроллеру доступа можно подключать входные устройства сигнализации. Вы можете изменять параметры соединений сигнализации в соответствии с вашими требованиями.

Шаг 1 Выберите **Alarm Linkage (каналы сигнализации)** на панели навигации.

Откроется окно **Alarm Linkage**. См. рисунок 4-7

Рисунок 4-7 Соединения сигнализации



Шаг 2 Нажмите  . Теперь вы можете изменить параметры каналов сигнализации. См. рисунок 4-8.

Рисунок 4-8 Изменение параметров соединений сигнализации

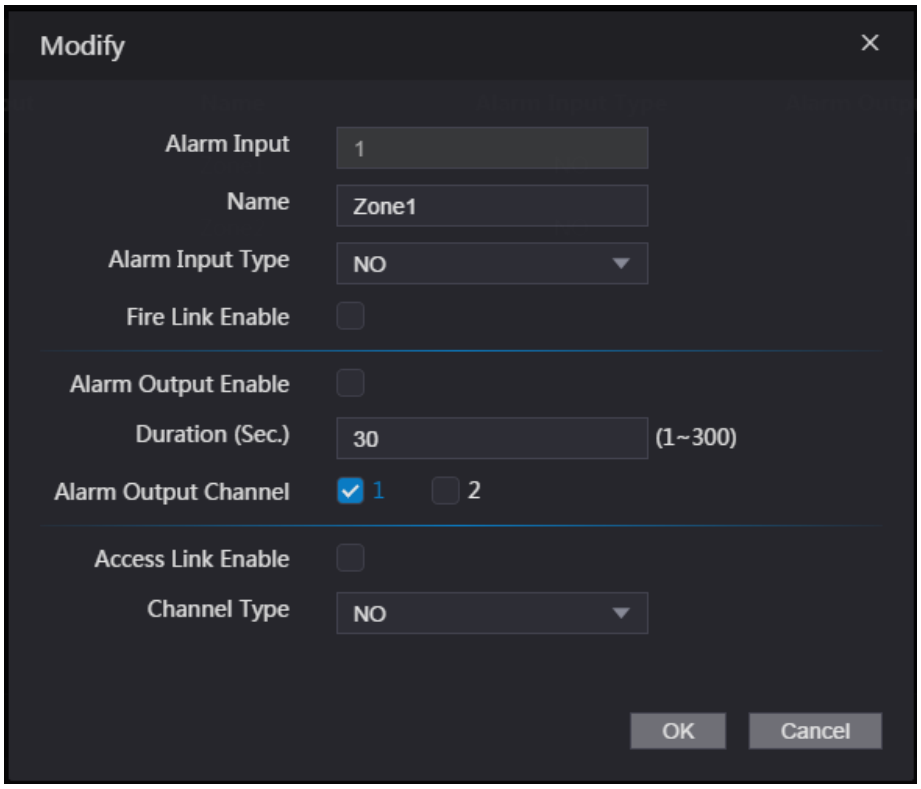


Таблица 4-1 Описание параметров соединений сигнализации

Параметр	**Описание**
Alarm Input (Тревожный вход)	Вы не можете изменить это значение. Оставляйте значение по умолчанию.
Name (Название)	Введите название зоны.
Alarm Input Type (Тип тревожного входа)	Существует два варианта: NO и NC. Если тип тревожного входа приобретенного вами устройства сигнализации NO, необходимо выбрать NO; в противном случае, выберите NC.
Fire Link Enable (Включить канал пожарной тревоги)	Если канал пожарной тревоги активирован, контроллер доступа будет передавать сигналы при срабатывании пожарной тревоги. Подробности о сигналах тревоги будут отображаться в журнале сигналов тревоги. Тревожный выход и канал доступа по умолчанию NO, если канал пожарной тревоги активирован.
Alarm Output Enable (Включить тревожный выход)	Реле может передавать информацию о выходных сигналах тревоги (отправляется на платформу управления), если активировать **Alarm Output**.
Duration (Sec.) (Продолжительность (сек.))	Продолжительность сигналов тревоги, диапазон: 1–300 секунд.
Alarm Output Channel (Канал тревожного выхода)	Вы можете выбрать канал тревожного выхода для установленного устройства сигнализации. Каждое устройство сигнализации может считаться одним каналом.
Access Link Enable (Включить канал доступа)	После активации канала доступа контроллер доступа будет включен или закрыт в штатном режиме при входных сигналах тревоги.
Channel Type (Тип канала)	Существуют два варианта: NO и NC.

Шаг 3 Нажмите **OK**. Теперь настройка завершена.

Настройка в веб-интерфейсе будет синхронизироваться с конфигурацией клиента, если добавить контроллер доступа к клиенту.

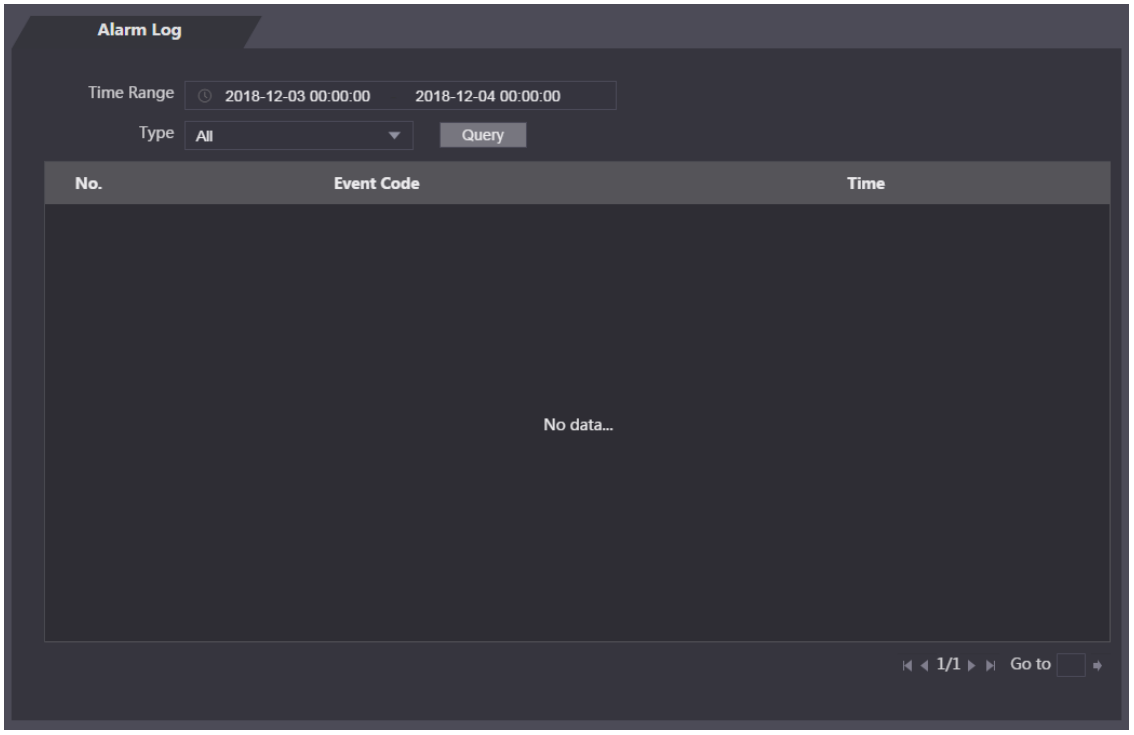
4.4.2 Журнал сигналов тревоги

Типы сигналов тревоги и временные диапазоны можно просматривать в окне **Alarm Log (Журнал сигналов тревоги)**.

Шаг 1 Перейдите по меню **Alarm Linkage > Alarm Log (Каналы сигнализации > Журнал сигналов тревоги)**.

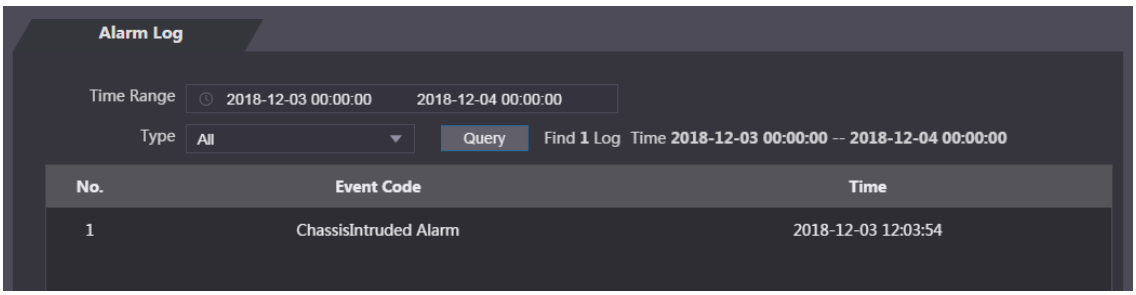
Откроется окно **Alarm Log**. См. рисунок 4-9

Рисунок 4-9 Журнал сигналов тревоги



Шаг 2 Выберите временной диапазон и тип сигнала тревоги, затем, нажмите **Query (Запрос)**. На экране будут показаны запроса. См. рисунок 4-10.

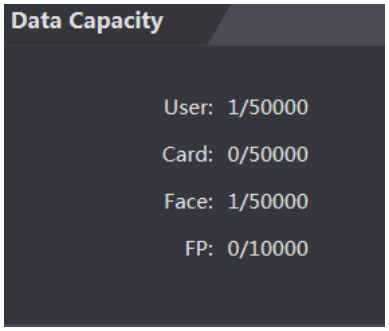
Рисунок 4-10 Результаты запроса



4.5 Объем данных

Количество пользователей, карт, изображений лиц и отпечатков пальцев, которое можно сохранить в контроллере доступа, вы можете узнать в окне **Data Capacity (Объем данных)**.

Рисунок 4-11 Объем данных



4.6 Настройки видео

You В окне **Video Setting (Настройки видео)** можно настраивать различные параметры, включая скорость передачи данных, параметры изображений (яркость, контраст, цветовой тон, насыщенность и т.д.) и экспозицию.

4.6.1 Скорость передачи данных

Рисунок 4-12 Скорость передачи данных

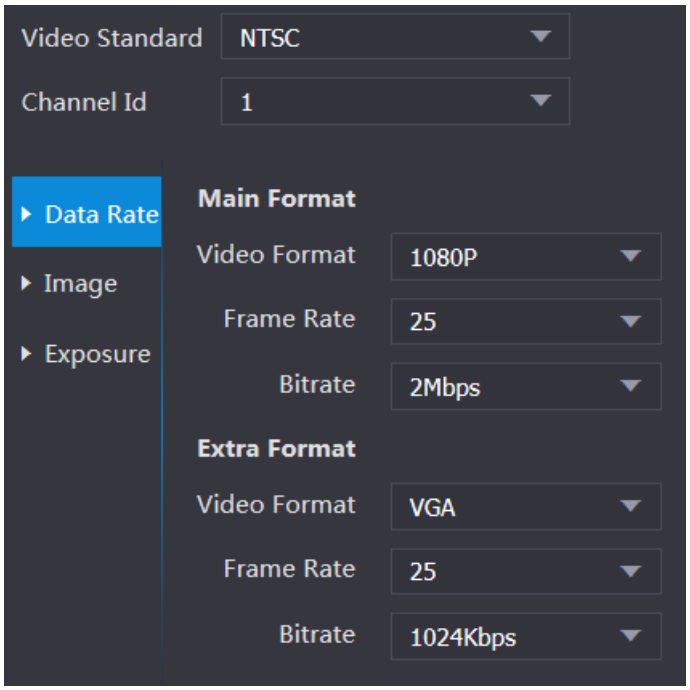


Таблица 4-2 Описание параметров скорости передачи данных

Параметр		Описание
Video Standard (Стандарт видео)		Имеются две опции: NTSC и PAL. Выберите стандарт видео, принятый в вашем регионе.
Channel (Канал)		Имеются две опции: 1 и 2. 1 – это камера с источником белого света 2 – это камера с ИК-подсветкой.
Main Format (Основной формат)	Video Format (Формат видео)	Имеются четыре опции: D1, VGA, 720p и 1080p. Выберите вариант в соответствии с нужным качеством видео.
	Frame Rate (Частота кадров)	Частота появления последовательных кадров на экране. Диапазон частоты кадров: 1–25 к/с.

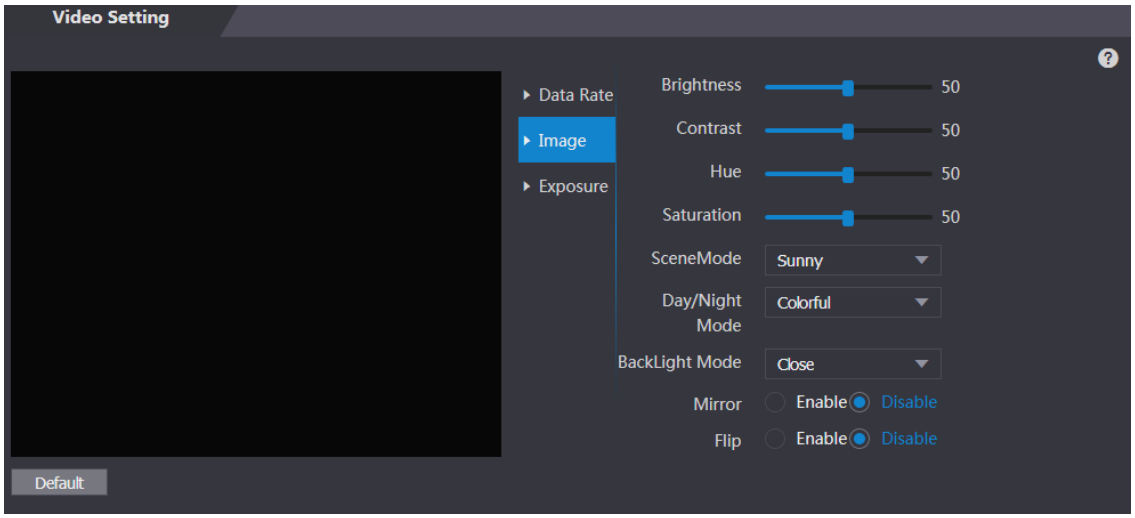
Параметр		Описание
	Bit Rate (Битрейт)	Количество битов, передаваемых или обрабатываемых за единицу времени. Имеются пять опций: 1,75 Мбит/с, 2 Мбит/с, 4 Мбит/с, 6 Мбит/с и 8Mbps.
Extra Format (Доп. Формат)	Video Format (Формат видео)	Имеются три опции: D1, VGA и QVGA.
	Frame Rate (Частота кадров)	Частота появления последовательных кадров на экране. Диапазон частоты кадров: 1–25 к/с.
	Bit Rate (Битрейт)	Количество битов, передаваемых или обрабатываемых за единицу времени. Опции: 256 Кбит/с, 320 Кбит/с, 384 Кбит/с, 448 Кбит/с, 512 Кбит/с, 640 Кбит/с, 768 Кбит/с, 896 Кбит/с, 1024 Кбит/с, 1,25 Мбит/с, 1,5 Мбит/с and 1,75 Мбит/с.

4.6.2 Изображения

Имеются два канала, и необходимо настроить параметры для каждого из них.

Шаг 1 Перейдите по меню **Video Setting > Video Setting > Image (Настройки видео > Настройки видео > Изображения)**.

Рисунок 4-13 Изображения



Шаг 2 Выберите Wide Dynamic (Широкий динамический диапазон) в Backlight Mode (Режим подсветки).

Таблица 4-3 Описание параметров изображений

Параметр	Описание
Brightness (Яркость)	Чем больше значение, тем ярче будет изображение.
Contrast (Контраст)	Контраст – это разница в освещенности или цвете, которая делает объект различимым. Чем выше значение контраста, тем выше будет яркость и цветовой контраст.
Hue (Цветовой тон)	Чем больше значение, тем больше будет глубина цвета.
Saturation (Насыщенность)	Чем больше значение, тем ярче будут цвета. Это значение не изменяет яркость изображения.

Параметр	Описание
Scene Mode (Режим сцены)	● Close (Отключен): Без режима. ● Auto (Авто): Система автоматически регулирует режимы сцены. ● Sunny (Солнечно): В этом режиме уменьшается цветовой тон. ● Night (Ночь): В этом режиме повышается уменьшается цветовой тон. Режим **Sunny** выбран по умолчанию.
Day/Night Mode (Режим день/ночь)	Режим день/ночь определяет рабочий статус заполнения цветом. ● Auto (Авто): Система автоматически регулирует режим день/ночь. ● Colorful (Цветной): В этом режиме изображения цветные. ● Black and white (Черно-белый): В этом режиме изображения черно-белые.
Back Light Mode (Режим задней подсветки)	● Close (Отключен): Без задней подсветки. ● BLC: Компенсация задней подсветки обеспечивает корректировку регионов с крайне высокими или низкими уровнями света, чтобы обеспечить нормальный и применимый уровень света для фокусируемого объекта. ● WDR: В широком динамическом диапазоне система затемняет яркие участки и компенсирует темные участки, чтобы обеспечить различимость объекта в ярких и темных участках. Когда задняя подсветка направлена на лица людей, необходимо активировать Wide Dynamic. ● HLC: Компенсация яркой засветки нужна для компенсации чрезмерного воздействия световых эффектов и источников освещения, таких как фары, прожекторы, фонари и т.д., чтобы создавать приемлемые изображения без слишком яркого освещения.
Mirror (Зеркалирование)	Если эта функция активирована, изображения будут горизонтально перевернутыми.
Flip (Поворот	Если эта функция активирована, видео можно переворачивать.

4.6.3 Экспозиция

Описание параметров экспозиции см. в таблице 4-4.

Таблица 4-4 Описание параметров экспозиции

Параметр	Описание
Anti-flicker (Устранение бликов)	● 50Hz (50 Гц): Если частота переменного тока в сети 50 Гц, экспозиция автоматически регулируется, чтобы обеспечить отсутствие полос на изображениях. ● 60Hz (60 Гц): Если частота переменного тока в сети 60 Гц, экспозиция автоматически регулируется, чтобы обеспечить отсутствие полос на изображениях. ● Outdoor (Улица): Если выбрать **Outdoor**, можно переключать режим экспозиции.

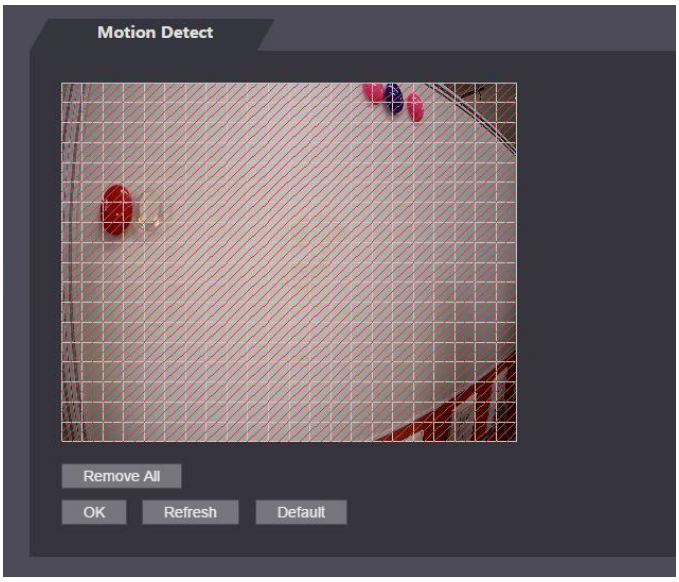
Параметр	Описание
Exposure Mode (Режим экспозиции)	🕮 ● Если выбрать **Outdoor** в раскрывающемся списке Anti-flicker, можно выбрать режим экспозиции **Shutter Priority (Приоритет выдержки)**. ● Режимы экспозиции разных устройств варьируются, и преобладающее значение имеет фактический продукт. Можно выбрать следующие варианты: ● Auto (Авто): Контроллер доступа будет автоматически регулировать яркость изображений. ● Shutter Priority (Приоритет выдержки): Контроллер доступа будет регулировать яркость изображений в соответствии со диапазоном значений приоритета выдержки. Если яркость изображения недостаточная и значение выдержки достигло верхнего или нижнего предела, контроллер доступа автоматически скорректирует значение усиления, чтобы обеспечить идеальную яркость. ● Manual (Вручную): Чтобы отрегулировать яркость изображений, можно вручную настраивать значения усиления и выдержки.
Shutter (Выдержка)	Чем больше значение выдержки и меньше время экспозиции, тем темнее будет изображение.
Shutter Value Range (Диапазон значений выдержки)	Если выбрать **Customized Range (Пользовательский диапазон)**, можно установить свой диапазон значений выдержки.
Gain Value Range (Диапазон значений усиления)	Если настроить диапазон значений усиления, качество видео будет повышаться.
Exposure Compensation (Компенсация экспозиции)	Регулировкой значения компенсации экспозиции можно повысить яркость видео.
3D NR	Если включить 3D-шумоподавление (RD), будет уменьшен шум на видео, и видео будет иметь высокое разрешение.
Grade (Степень)	Если включен 3D NR, можно регулировать значение 3D NR. Чем больше значение, тем меньше шум.

4.6.4 Обнаружение движения

Настройка диапазона определения движущегося объекта.

Шаг 1 Перейдите по меню **Video Setting > Video Setting > Motion Detection (Настройки видео > Настройки видео > Обнаружение движения)**. Откроется окно **Motion Detection (Обнаружение движения)**. См. рисунок 4-14.

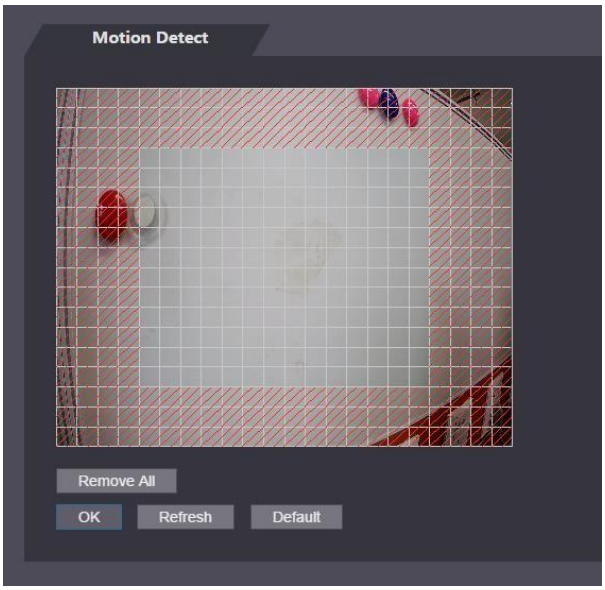
Рисунок 4-14 Обнаружение движения



Шаг 2 Нажмите и удерживайте левую кнопку мыши и перетащите мышь в красную область. Появится зона обнаружения движения (Motion Detection). См. рисунок 4-15.

- Красные прямоугольники – это область обнаружения движения. Диапазон обнаружения движения по умолчанию – все прямоугольники.
- Чтобы создать область обнаружения движения, сначала нужно нажать **Remove All (Удалить все)**.
- Создаваемая вами область не будет областью обнаружения движения, если вы используете область по умолчанию.

Рисунок 4-15 Область обнаружения движения

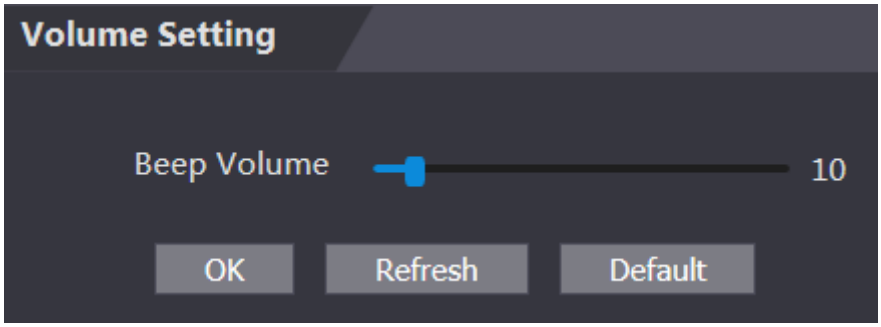


Шаг 3 Нажмите **OK,** чтобы завершить настройку.

4.6.5 Настройка громкости звука

Вы можете настраивать громкость звука динамика контроля доступа.

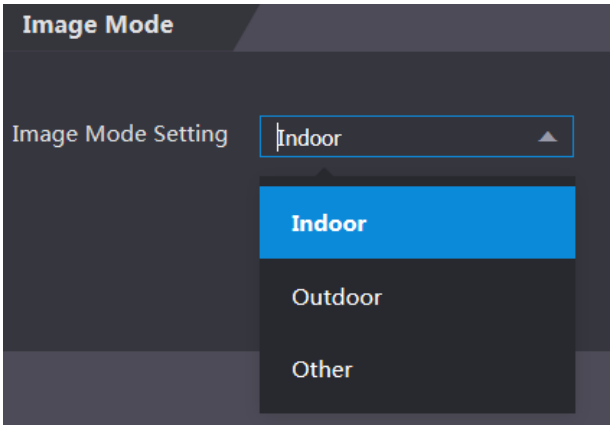
Рисунок 4-16 Настройка громкости звук



4.6.6 Режим изображений

Имеются три варианта: помещение, улица или другое. Выберите **Indoor (Помещение),** если контроллер доступа установлен в помещении; выберите **Outdoor (Улица),** если контроллер доступа установлен на улице; выберите **Other (Другое),** если контроллер доступа установлен в местах с задним освещением, таких как коридоры и проходы внутри зданий.

Рисунок 4-17 Режим изображений



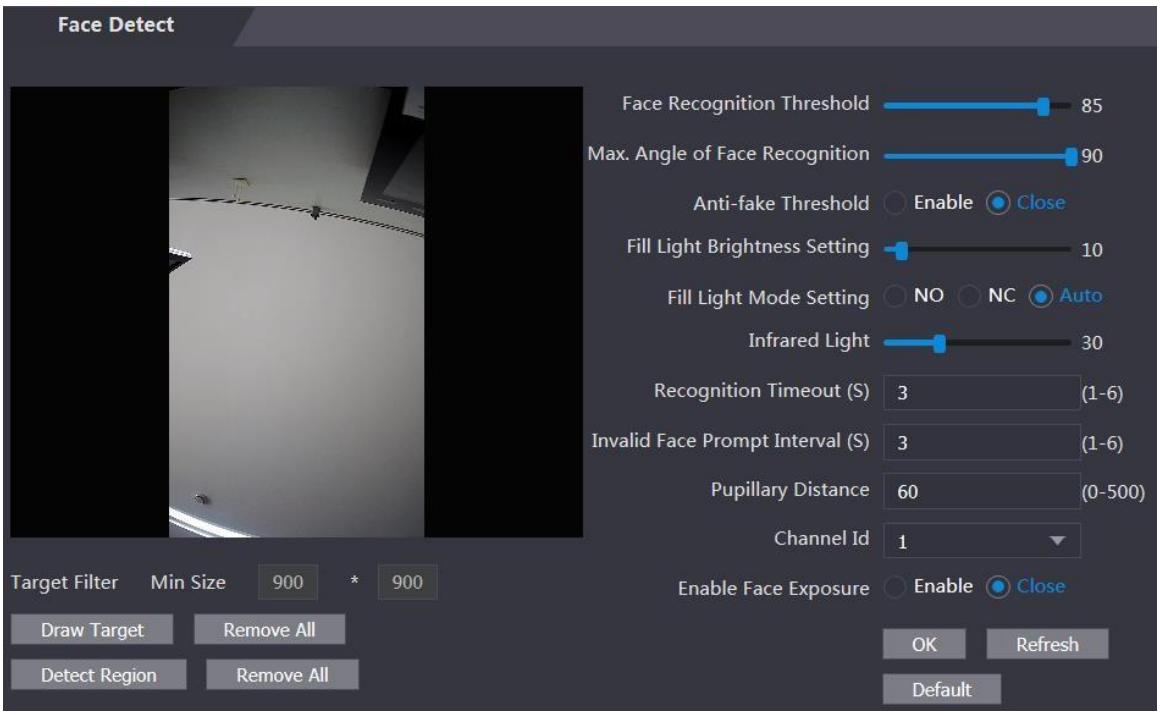
4.7 Детекция лиц

You В этом окне можно настраивать параметры, связанные с лицами, чтобы повысить точность распознавания лиц.

Шаг 1 Выберите **Face Detect (Детекция лиц)**.

Откроется окно **Face Detect**. См. рисунок 4-18.

Рисунок 4-18 Детекция лиц



Шаг 2 Настройка параметров. См. таблицу 4-5.

Таблица 4-5 Описание параметров детекции лиц

Параметр	**Описание**
Face Recognition Threshold (Предел распознавания лиц)	Чем выше значение, тем выше будет точность.
Max. Angle of Face Recognition (Макс. угол распознавания)	Чем выше угол, тем шире будет диапазон распознаваемого профиля.
Anti-fake Threshold (Предел защиты от подделок)	Два варианта: **Enable (Включить)** и **Close (Отключить)**.
Fill Light Brightness Setting (Настройки яркости заполняющего света)	Можно настраивать яркость заполняющего света.
Fill Light Mode Setting (Настройки режима заполняющего света)	Имеются три режима заполняющего цвета. ● NO: Заполняющий свет включен в штатном режиме. ● NC: Заполняющий свет выключен в штатном режиме. ● Auto (Авто): Заполняющий свет будет автоматически включаться при срабатывании обнаружения движения. Если выбрать **Auto**, заполняющий свет будет активирован, даже если значение ИК-подсветки выше 19.
Infrared Light (ИК-подсветка)	Регулировка яркости ИК-подсветки путем перемещения полосы прокрутки.
Recognition Timeout (Превышение времени ожидания при распознавании)	Если человек, не имеющий права доступа, стоит перед контроллером доступа, и происходит распознавание его лица, контроллер отправит сообщение о том, что распознавание не было успешно выполнено. Интервал сообщения называется превышением времени ожидания при распознавании.
Invalid Face Prompt Interval (Интервал сообщения о незарегистрированном лице)	Если человек, не имеющий права доступа, стоит перед контроллером доступа, будет передано сообщение о том, что лицо не зарегистрировано. Интервал сообщения – это интервал сообщения о незарегистрированном лице.
Pupillary Distance (Межцентровое расстояние)	Межцентровое расстояние – это значение расстояния между центрами зрачков обоих глаз на изображении в пикселях.

Параметр	Описание
	Вам нужно установить соответствующее значение, чтобы контроллер доступа мог распознавать лица должным образом. Значение изменяется в соответствии с размерами лиц и расстоянием между лицом и объективом. Чем ближе лицо к объективу, тем выше будет значение. Если взрослый находится на расстоянии 1,5 метра от объектива, значение межцентрового расстояния будет от 50 до 70.
Enable Face Exposure (Активировать экспозицию лица)	После активации экспозиции лица лицо будет видно более четко, если контроллер доступа установлен на улице.
Channel Id (ИДН канала)	Два варианта: 1 и 2. 1 для камеры с белым светом и 2 для камеры с ИК-подсветкой.
Draw Target (Создание цели)	Нажмите **Draw Target**, чтобы создать минимальный кадр детекции лиц. Нажмите **Remove All (Удалить все)**, чтобы удалить все созданные кадры.
Detect Region (Регион обнаружения)	Нажмите **Detect Region**, передвиньте мышь, после чего вы сможете настроить регион обнаружения лиц. Нажмите **Remove All (Удалить все)**, чтобы удалить все регионы обнаружения.

Шаг 3 Нажмите **OK,** чтобы завершить настройку.

4.8 Настройка сети

4.8.1 TCP/IP

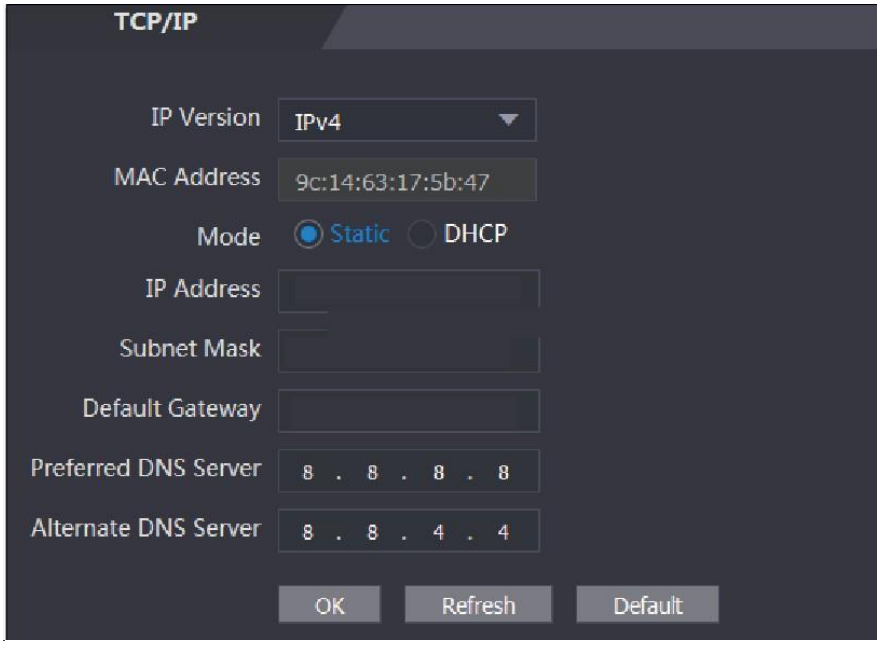
Чтобы обеспечить связь контроллера доступа с другими устройствами, необходимо настроить to configure IP-адрес и DNS-сервер.

Необходимые условия

Убедитесь в том, что контроллер доступа подключен к сети надлежащим образом.

Шаг 1 Перейдите по меню **Network Setting > TCP/IP (Настройка сети > TCP/IP)**.

Рисунок 4-19 TCP/IP



Шаг 2 Выполните настройку параметров.

Таблица 4-6 TCP/IP

Параметр	Описание
IP Version (Версия IP)	Только один вариант: IPv4.
MAC Address (MAC-адрес)	Отображение MAC-адреса контроллера доступа.
Mode (Режим)	● Static (Статический) Настройка IP-адреса, маски подсети и адреса шлюза вручную. ● DHCP ◇ После активации DHCP настройка IP-адреса, маски подсети и адреса шлюза невозможна. ◇ Если DHCP активирован, IP-адрес, маска подсети и адрес шлюза будут отображаться автоматически; если DHCP не активирован, IP-адрес, маска подсети и адрес шлюза будут нулевыми. ◇ Если вы хотите узнать IP-адрес по умолчанию, когда DHCP активирован, вам необходимо отключить DHCP.
Link-local address (Адрес локальной связи)	Адрес локальной связи доступен, только если выбрать IPv6 в версии IP. Сетевому интерфейсу контроллера будет назначен уникальный адрес локальной связи в каждой области сети, чтобы обеспечить связь. Адрес локальной связи нельзя изменить.
IP Address (IP-адрес)	Введите IP-адрес, и настройте маску подсети и адрес шлюза. IP-адрес и адрес шлюза должны быть в одном сетевом сегменте.
Subnet Mask (Маска посети)	
Default Gateway (Шлюз по умолчанию)	
Preferred DNS Server (Предпочитаемый DNS-сервер)	Настройка IP-адреса предпочитаемого DNS-сервера.
Alternate DNS Server (Альтернативный DNS-сервер)	Настройка IP-адреса альтернативного DNS-сервера.

Шаг 3 Нажмите **OK**, чтобы завершить настройку.

4.8.2 Порт

Установите максимальное количество клиентов связи, к которым может быть подключен контроллер доступа, а также номера портов.

Шаг 1 Перейдите по меню **Network Setting > Port (Настройка сети > Порт)**.

Откроется окно **Port**.

Шаг 2 Настройте номера портов. См. следующую таблицу.

Чтобы активировать конфигурацию после изменения значений, кроме максимального числа соединений, необходимо перезагрузить контроллер доступа.

Таблица 4-7 Описание портов

Параметр	Описание
Max connection (Макс. количество соединений)	Вы можете настроить максимальное количество клиентов связи, к которым может быть подключен контроллер. Клиенты платформ, такие как Smartpss, не учитываются.
Порт TCP	Значение по умолчанию: 37777.
Порт HTTP	Значение по умолчанию: 80. Если в качестве номера порта используется другое значение, при входе через браузер необходимо добавить это значение после адреса.
Порт HTTPS	Значение по умолчанию: 443.
Порт RTSP	Значение по умолчанию: 554.

Шаг 3 Нажмите **OK**, чтобы завершить настройку.

4.8.3 Регистрация

При подключении к внешней сети контроллер доступа отправит свой адрес на сервер, установленный пользователем, чтобы клиент мог получить доступ к контроллеру доступа.

Шаг 1 Перейдите по меню **Network Setting > Auto Register (Настройка сети > Автоматическая регистрация)**. Откроется окно **Auto Register**.

Шаг 2 Выберите **Enable (Включить)** и введите IP -адрес хоста, порт и ID подчиненного устройства.

Таблица 4-8 Описание автоматической регистрации

Параметр	Description
IP-адрес хоста	IP-адрес или имя домена сервера.
Порт	Порт сервера, используемый для автоматической регистрации.
ID подчиненного устройства	ID контроллера доступа, назначенный пользователем.

Шаг 3 Нажмите **OK**, чтобы завершить настройку.

4.8.4 P2P

Вычисления в одноранговых сетях – это распределенная архитектура приложений, которая разделяет задачи или рабочие нагрузки между одноранговыми сетями. Пользователи могут загрузить мобильное приложение, отсканировав QR-код, а затем зарегистрировать учетную запись, при этом, с помощью мобильного приложения можно управлять несколькими контроллерами доступа. Вам не нужно использовать динамическое имя домена, транзитный сервер или выполнять распределение портов.

Если вам необходимо использовать P2P, нужно подключить контроллер доступа к внешней сети; в противном случае, работа с контроллером будет невозможной.

Рисунок 4-20 P2P

Шаг 1 Перейдите по меню **Network Setting > P2P (Настройка сети > P2P)**. Откроется окно **P2P**.

Step 2 Выберите **Enable,** чтобы активировать функцию P2P.

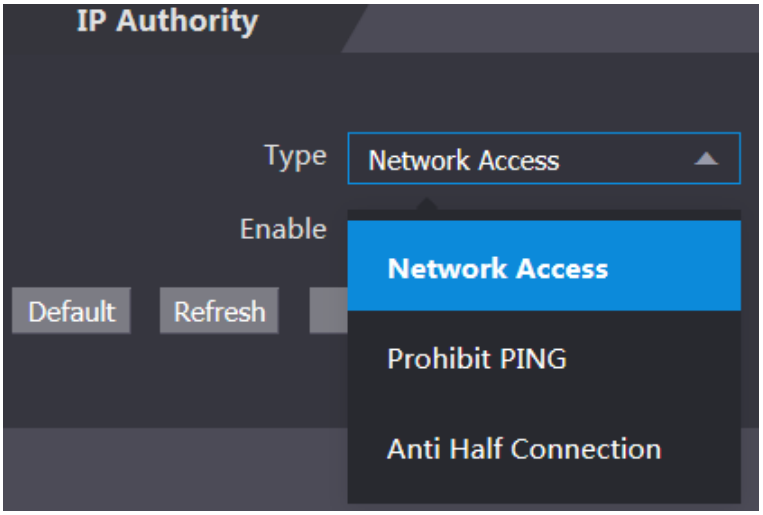
Step 3 Нажмите **OK**, чтобы завершить настройку.

Отсканируйте QR-код в веб-интерфейсе, чтобы получить серийный номер вашего контроллера доступа.

4.9 Управление безопасностью

4.9.1 Полномочия для IP

Рисунок 4-21 Полномочия для IP



Выберите нужный режим кибербезопасности.

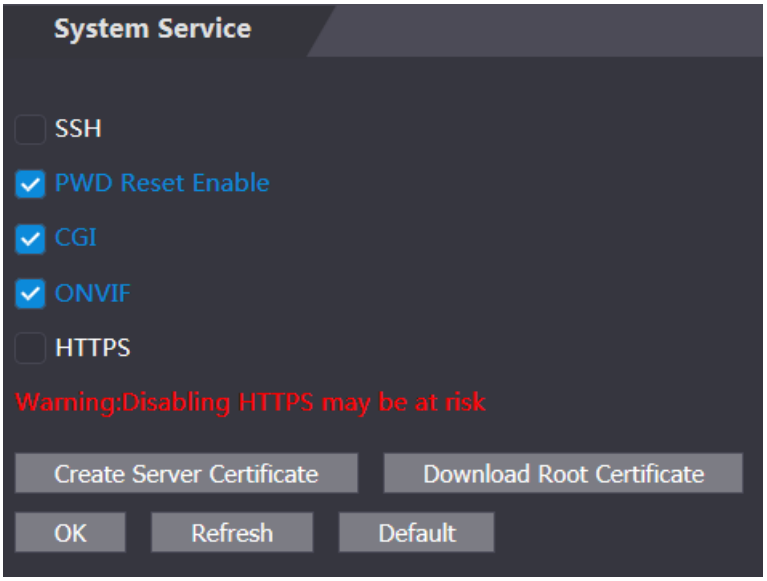
4.9.2 Системы

4.9.2.1 Системные сервисы

Четыре опции: SSH, активация сброса пароля, CGI и HTTPS. Чтобы выбрать одну из них или несколько, см. раздел 3.9.4 «Функции».

Конфигурация системных сервисов, выполненная на веб-странице, и конфигурация в окне on the **Features (Функции) контроллера доступа будут синхронизироваться**.

Рисунок 4-22 Системные сервисы



4.9.2.2 Создание сертификата сервера

Нажмите **Create Server Certificate (Создать сертификат сервера)**, введите нужную информацию, нажмите **Save (Сохранить)**, после чего контроллер доступа будет перезагружен.

4.9.2.3 Загрузка корневого сертификата

Шаг 1 Нажмите **Download Root Certificate (Загрузить корневой сертификат)**.

Выберите путь для сохранения сертификата в диалоговом окне **Save File (Сохранить файл)**.

Шаг 2 Дважды нажмите на **Root Certificate (Корневой сертификат),** который вы загрузили, чтобы установить сертификат. Установите сертификат, следуя инструкциям на экране.

4.9.3 Управление пользователями

Вы можете добавлять и удалять пользователей, изменять пароли пользователей и ввести адрес электронной почты, чтобы сменить забытый пароль.

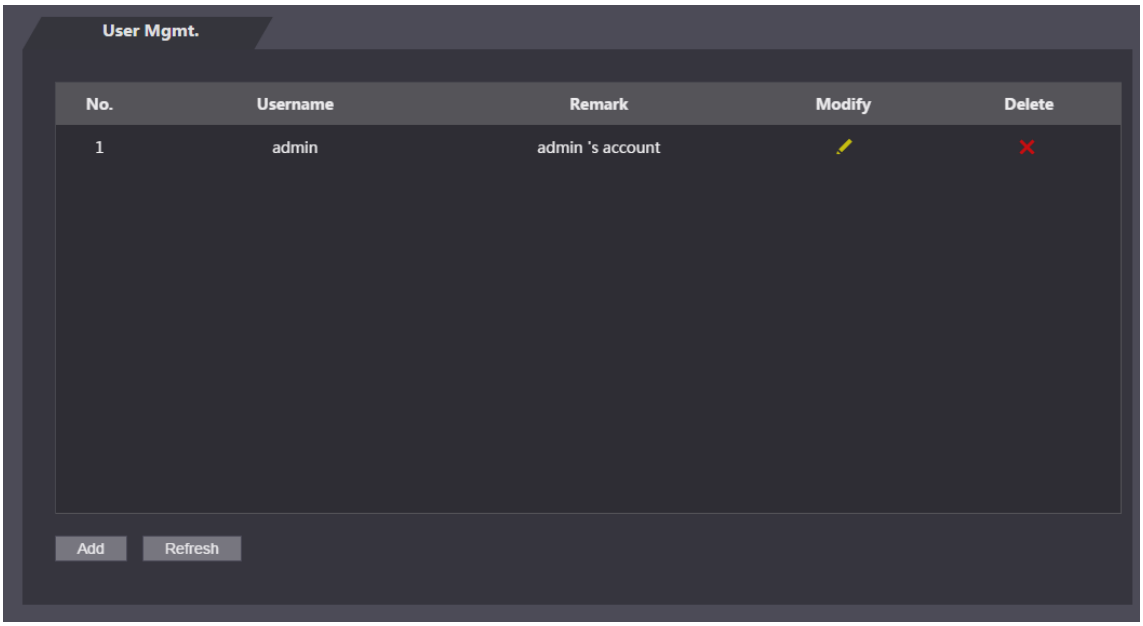
4.9.3.1 Добавление пользователей

Нажмите **Add (Добавить)** в окне **User Mgmt. (Управление пользователями),** чтобы добавить пользователя, затем, введите имя пользователя, пароль, подтвердите пароль и введите примечание. Нажмите **OK,** чтобы завершить процесс добавления пользователя.

4.9.3.2 Изменение информации о пользователях

Вы можете изменить информацию о пользователях, нажав в окне **User Mgmt. (Управление пользователями)**. См. рисунок 4-23

Рисунок 4-23 Управление пользователями

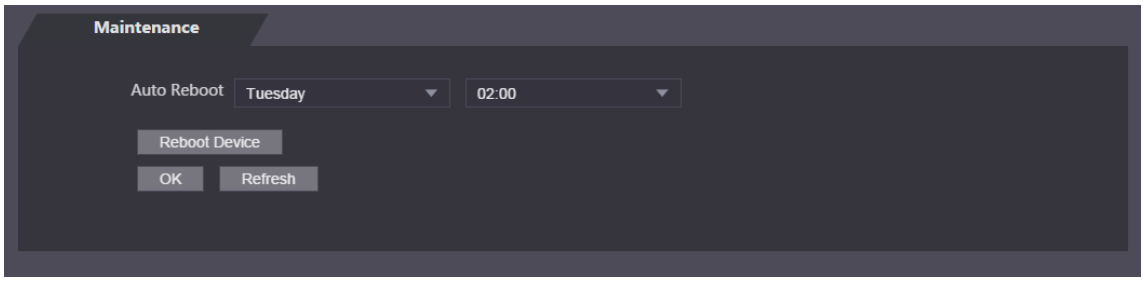


4.9.4 Обслуживание

Вы можете настроить контроллер доступа таким образом, что он будет перезагружаться в режиме ожидания с целью повышения скорости работы. Вам необходимо настроить дату и время автоматической перезагрузки.

Время перезагрузки по умолчанию – 2 часа утра в четверг. Нажмите **Reboot Device (Перезагрузить устройство)**, после чего контроллер доступа будет сразу же перезагружен. Нажмите **OK**, и контроллер доступа будет перезагружаться в 2 часа утра каждый четверг. См. рисунок 4-24.

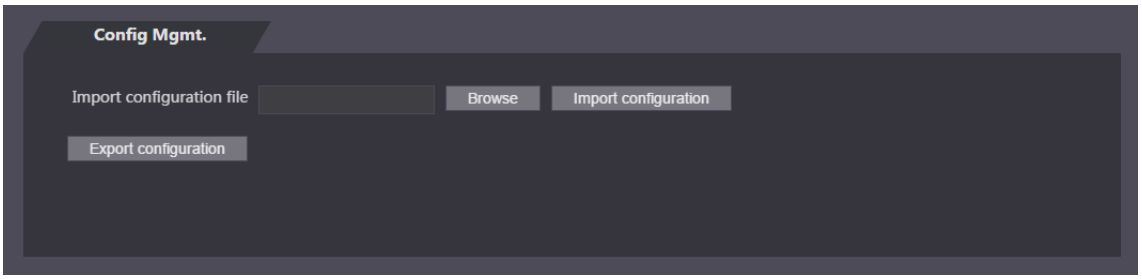
Рисунок 4-24 Обслуживание



4.9.5 Управление конфигурацией

Когда для нескольких контроллеров доступа нужна одинаковая конфигурация, вы можете настроить их параметры, импортируя или экспортируя файлы конфигурации. См. рисунок 4-25.

Рисунок 4-25 Управление конфигурацией



4.9.6 Обновление

Вы можете выбрать **Auto Check (Автоматическая проверка),** чтобы система обновлялась автоматически. Вы также можете выбрать **Manual Check (Проверка вручную),** чтобы обновить систему вручную.

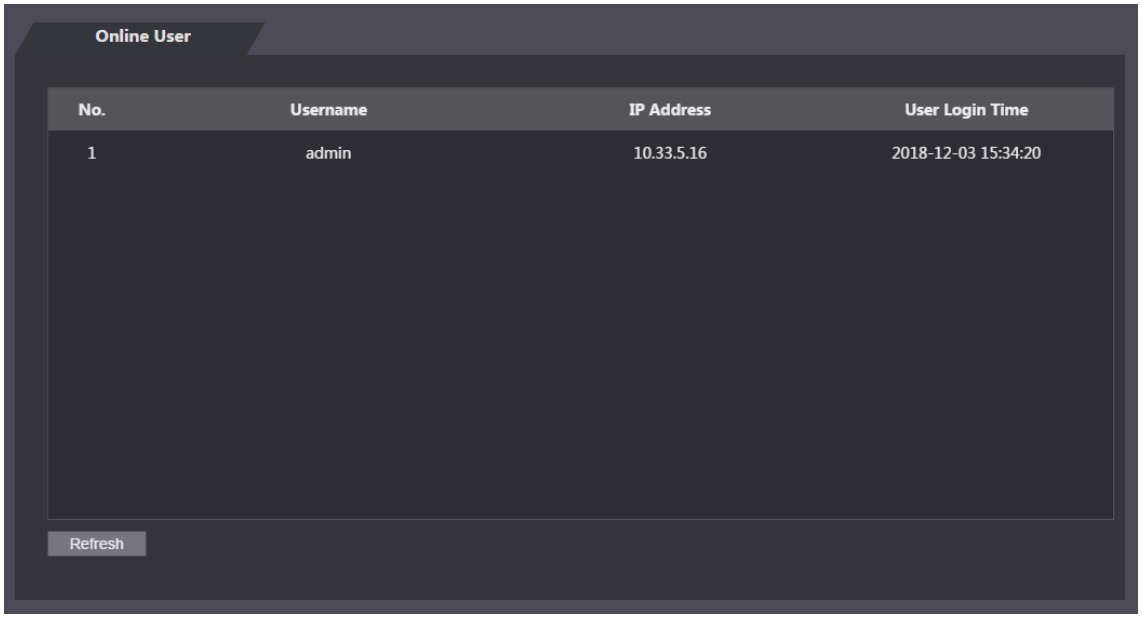
4.9.6 Информация о версии

Вы можете просматривать информацию, включая MAC-адрес, серийный номер, версию address, MCU, веб-версию, версию базового уровня безопасности и версию системы.

4.9.7 Онлайн-пользователи

В окне **Online User (Онлайн-пользователь)** можно увидеть имя пользователя, IP-адрес и время входа в систему. См. рисунок 4-26.

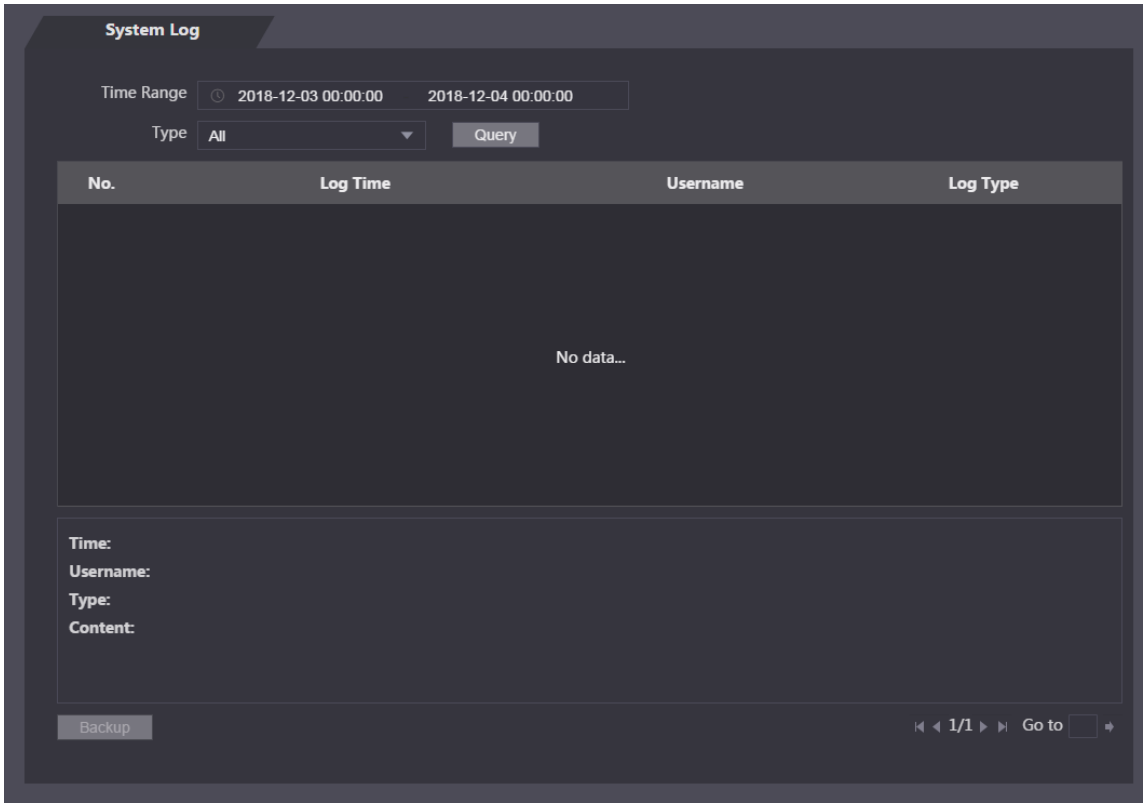
Рисунок 4-26 Онлайн-пользователь



4.10 Системный журнал

В окне **System Log (Системный журнал)** можно просматривать и создавать резервные копии системного журнала. См. рисунок 4-27.

Рисунок 4-27 Системный журнал



4.10.1 Журналы запросов

Выберите диапазон времени и тип, нажмите **Query (Запрос)**, и на экране будут отображены журналы, соответствующие этим условиям.

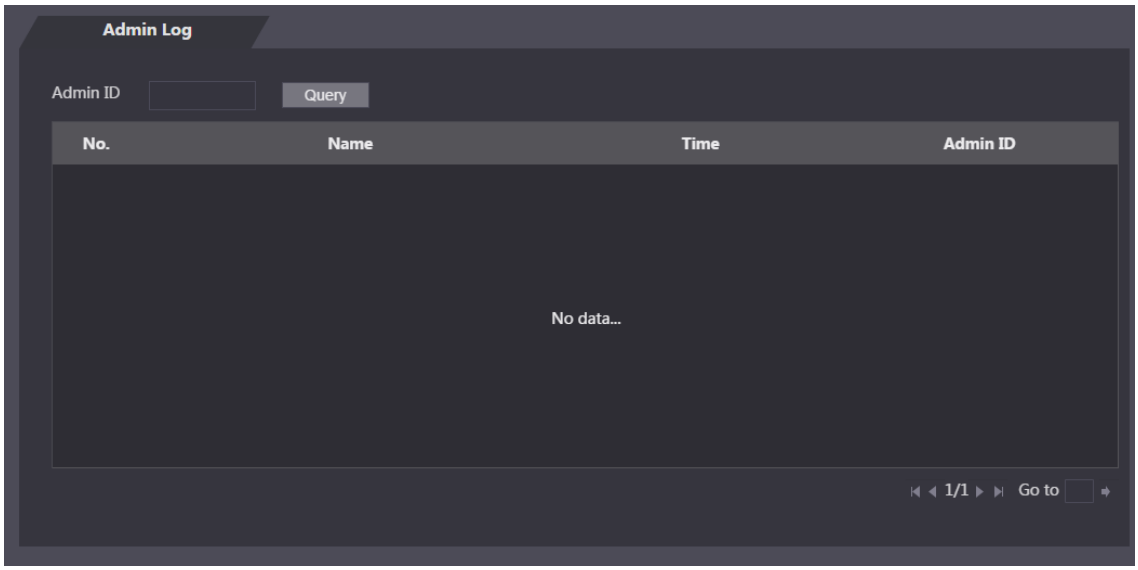
4.10.2 Резервное копирование журналов

Нажмите **Backup (Резервное копирование),** чтобы сделать резервные копии отображаемых журналов.

4.11 Журнал администратора

Введите идентификационный номер администратора (Admin ID) в окне **Admin Log (Журнал администратора)**, нажмите **Query (Запрос)**, и вы увидите записи об операциях, выполненных администратором. См. рисунок 4-28.

Рисунок 4-28 Журнал администратора



Наведите указатель мыши на , чтобы просмотреть подробную информацию о текущем пользователе.

4.12 Выход

Нажмите , нажмите **OK**, чтобы выйти из системы в веб-интерфейсе.

4 Настройка Smart PSS

С помощью клиента Smart PSS вы можете настроить разрешения на доступ для одной двери или группы дверей. Подробную информацию о настройке см. в руководстве пользователя Smart PSS.

Smart PSS может иметь разный интерфейс в зависимости от версии, и преимущественное значение имеет фактический интерфейс.

5.1 Авторизация

Установите Smart PSS (имя пользователя по умолчанию – admin, пароль по умолчанию – admin123) и дважды нажмите 

, чтобы запустить его. Следуйте инструкциям, чтобы завершить инициализацию и войти в систему.

5.2 Добавление устройств

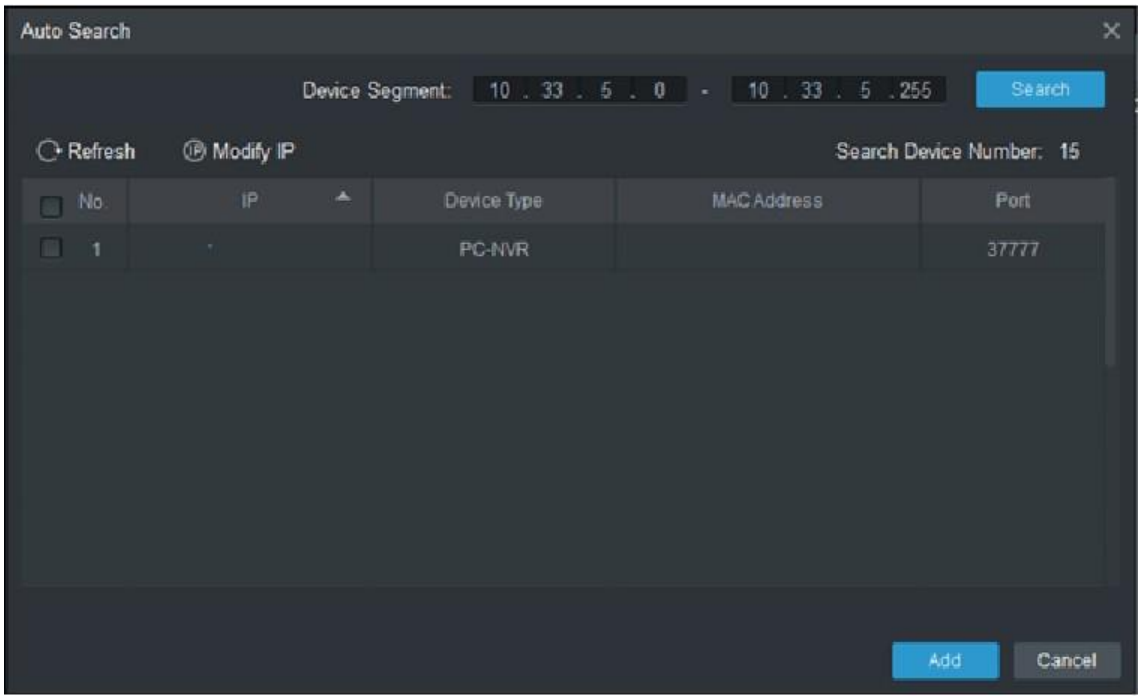
Вам необходимо добавить контроллер доступа в Smart PSS. Вы можете нажать **Auto Search (Автоматический поиск)** и нажать **Add (Добавить),** чтобы добавить устройства вручную.

5.2.1 Автоматический поиск

Вы можете осуществлять поиск и добавлять контроллеры доступа в одном сетевом сегменте в Smart PSS. См. рисунок 5-1 и рисунок 5-2.

Рисунок 5-1 Устройства

Рисунок 5-2 Автоматический поиск



Шаг 1 Нажмите **Auto Search (Автоматический поиск)**, введите сетевой сегмент и нажмите Search (Поиск). На экране будет отображен список.

Шаг 2 Выберите контроллеры доступа, которые вы хотите добавить в Smart PSS, и нажмите Add (Добавить). Откроется окно Login information (Информация о входе).

Шаг 3 Введите имя пользователя и пароль, чтобы осуществить вход.

Список добавленных контроллеров доступа можно просмотреть в окне **Devices (Устройства)**.

Выберите контроллер доступа и нажмите **Modify IP (Изменить IP)**, чтобы изменить IP-адрес контроллера доступа. Более подробную информацию об изменении IP-адреса см. в руководстве пользователя Smart PSS.

5.2.2 Добавление вручную

Вам нужно знать IP-адреса и имена доменов контроллеров доступа, которые вы хотите добавить. См. рисунок 5-3 и рисунок 5-4.

Рисунок 5-3 Устройства

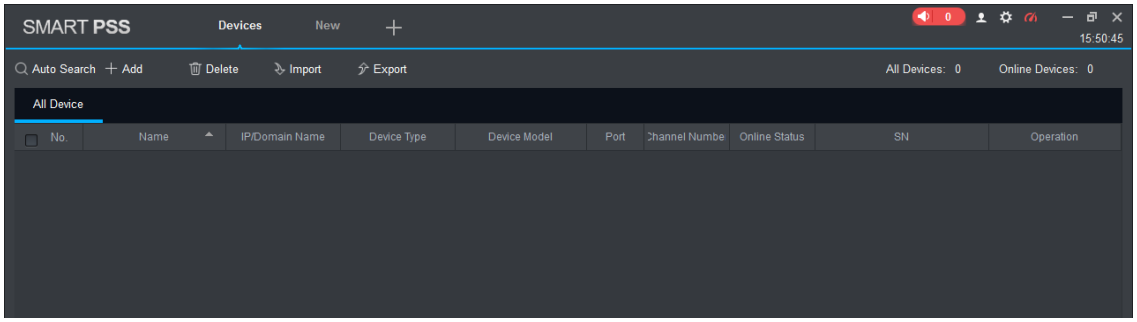
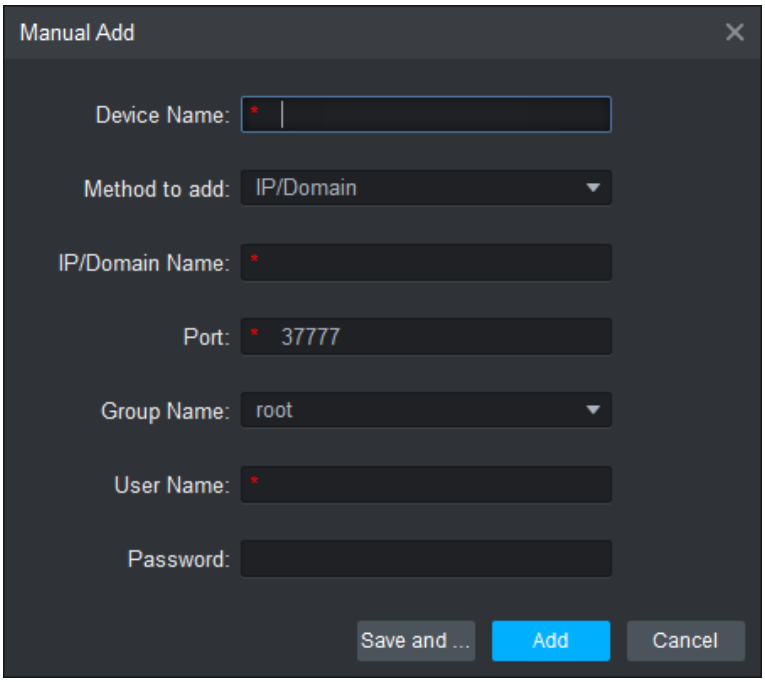


Рисунок 5-4 Добавление вручную



Шаг 1 Нажмите **Add (Добавить)** в окне Devices (Устройства). Откроется окно Manual Add (Добавить вручную).

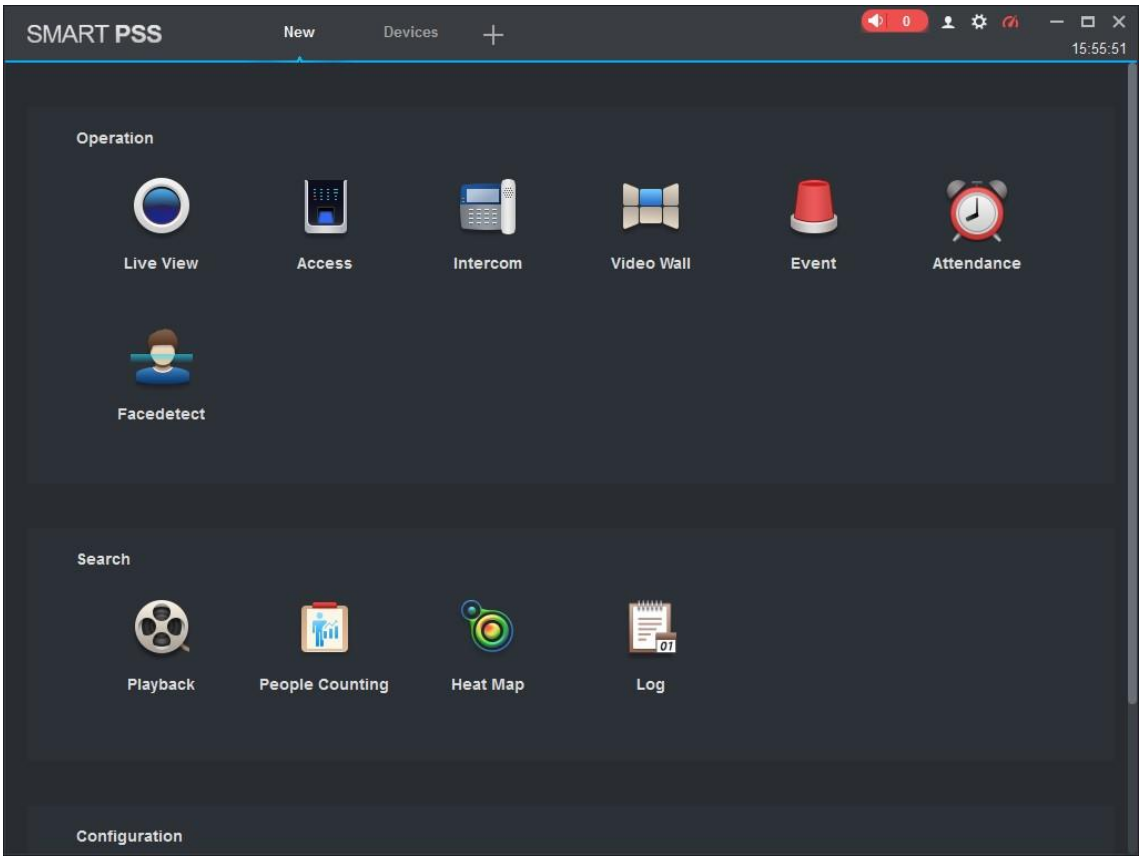
Шаг 2 Введите название устройства (Device Name), выберите способ добавления, введите IP/имя домена, номер порта (37777 по умолчанию), имя группы, имя пользователя и пароль.

Шаг 3 Нажмите **Add**, и контроллер доступа будет показан в окне Devices (Устройства).

5.3 Добавление пользователей

Пользователи связаны с картами. После того, как вы добавите пользователей в Smart PSS, вы сможете настроить разрешения на доступ в меню **New > Access (Новый > Доступ)**. См. рисунок 5-5.

Рисунок 5-5 Новый



5.3.1 Выбор типа карты

Тип карты должен совпадать с типом изготовителя карт; в противном случае, номера карт не будут считываться.

В окне **Access (Доступ)** нажмите  , затем, нажмите на значок IC или ID и выберите тип карты. Два варианта: ID-карта и IC-карта. См. рисунок 5-6 и рисунок 5-7.

Рисунок 5-6 Доступ

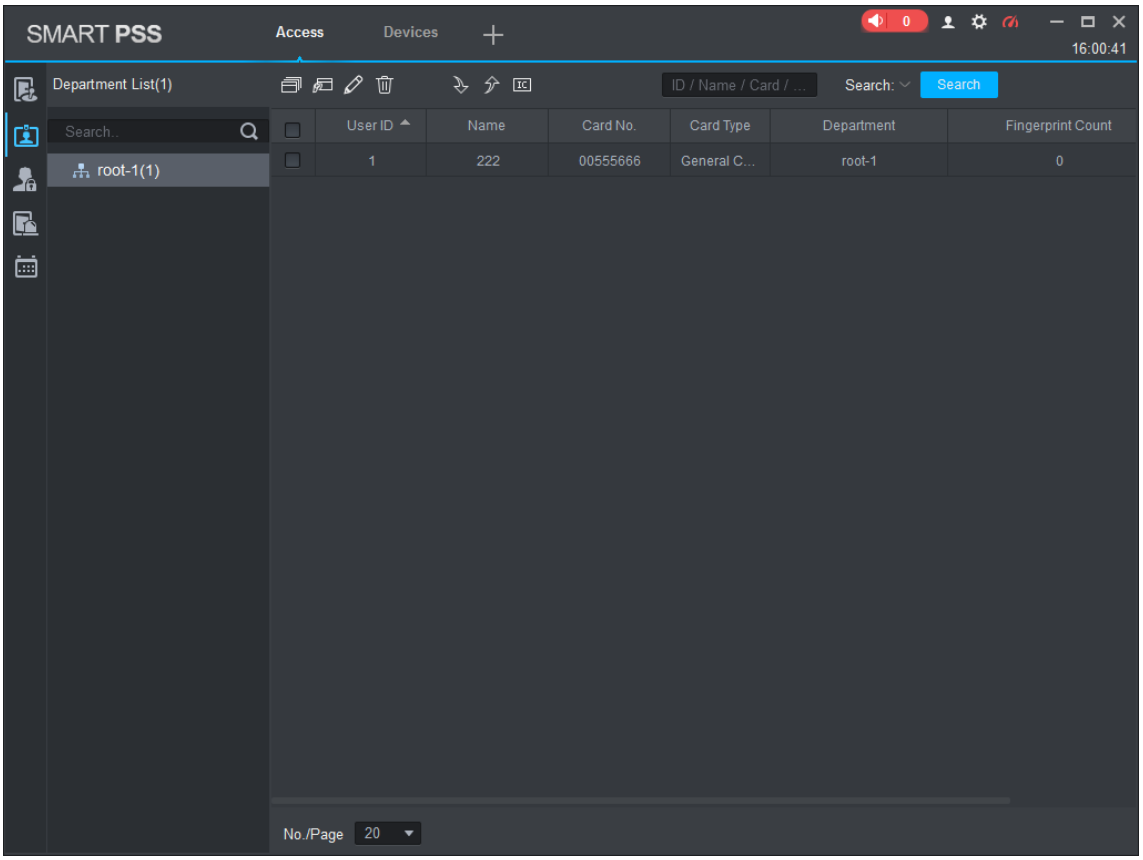
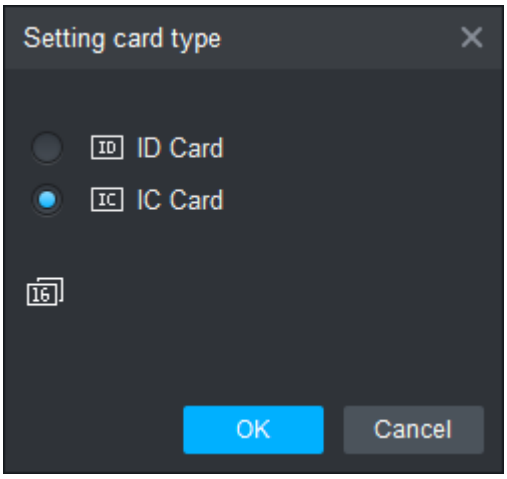


Рисунок 5-7 Настройка типа карты



5.3.2 Добавление одного пользователя

Вы можете добавлять пользователей по одному.

В окне **Access (Доступ)** нажмите  , затем, нажмите  и введите информацию о пользователе. Нажмите **Finish (Завершить),** чтобы завершить процесс добавления пользователя. См. рисунок 5-8 и рисунок 5-9.

Рисунок 5-8 Доступ

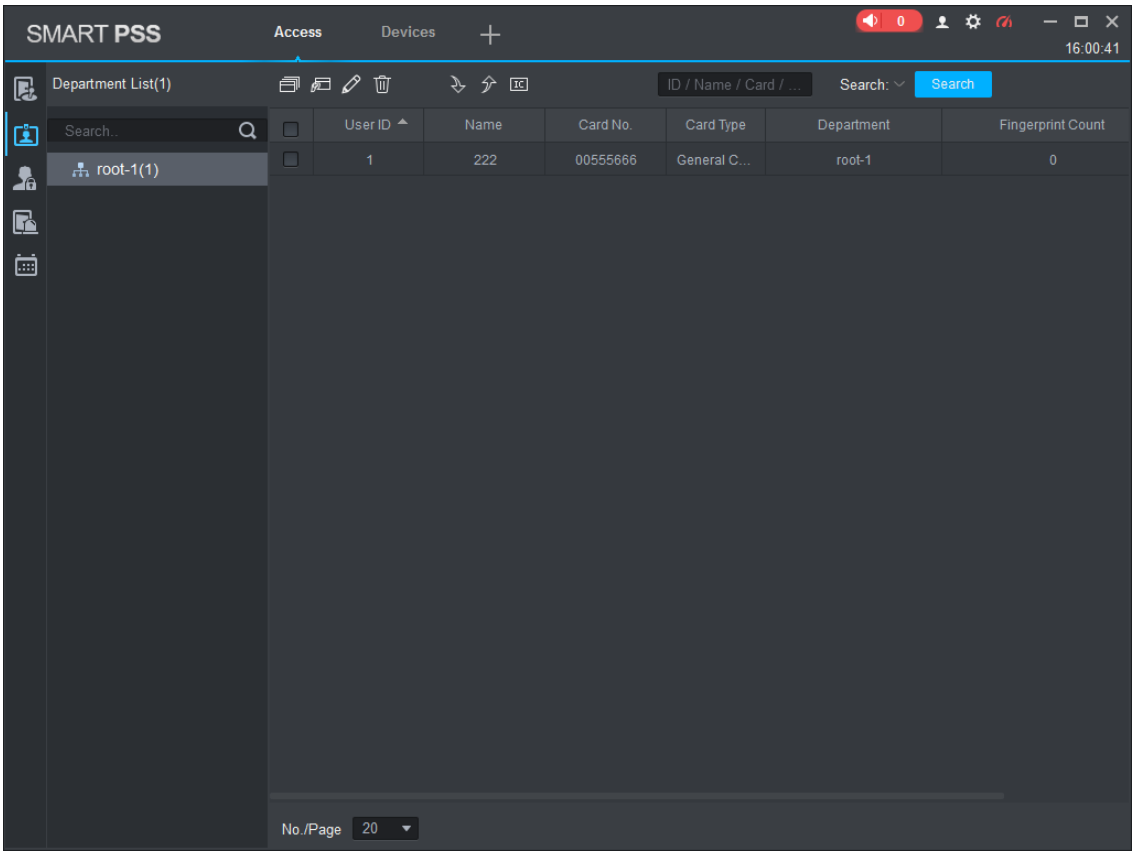
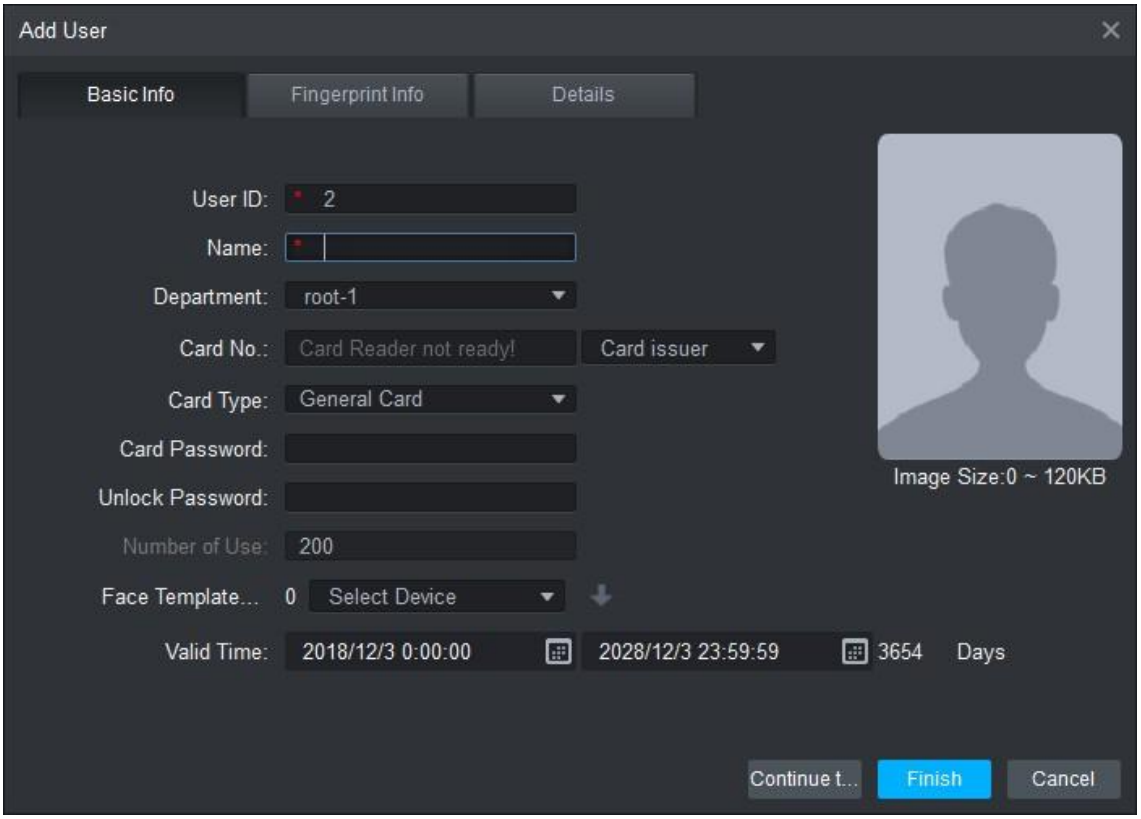


Рисунок 5-9 Добавление пользователя



5.4 Добавление группы дверей

Вы можете управлять дверьми, объединяя их в группы.

В окне **Access (Доступ)** нажмите  нажмите **Add (Добавить)**, введите название группы дверей и выберите часовой пояс. Нажмите **Finish (Завершить),** чтобы завершить процесс добавления пользователя. См. рисунок 5-10 и рисунок 5-11.

Рисунок 5-10 Доступ

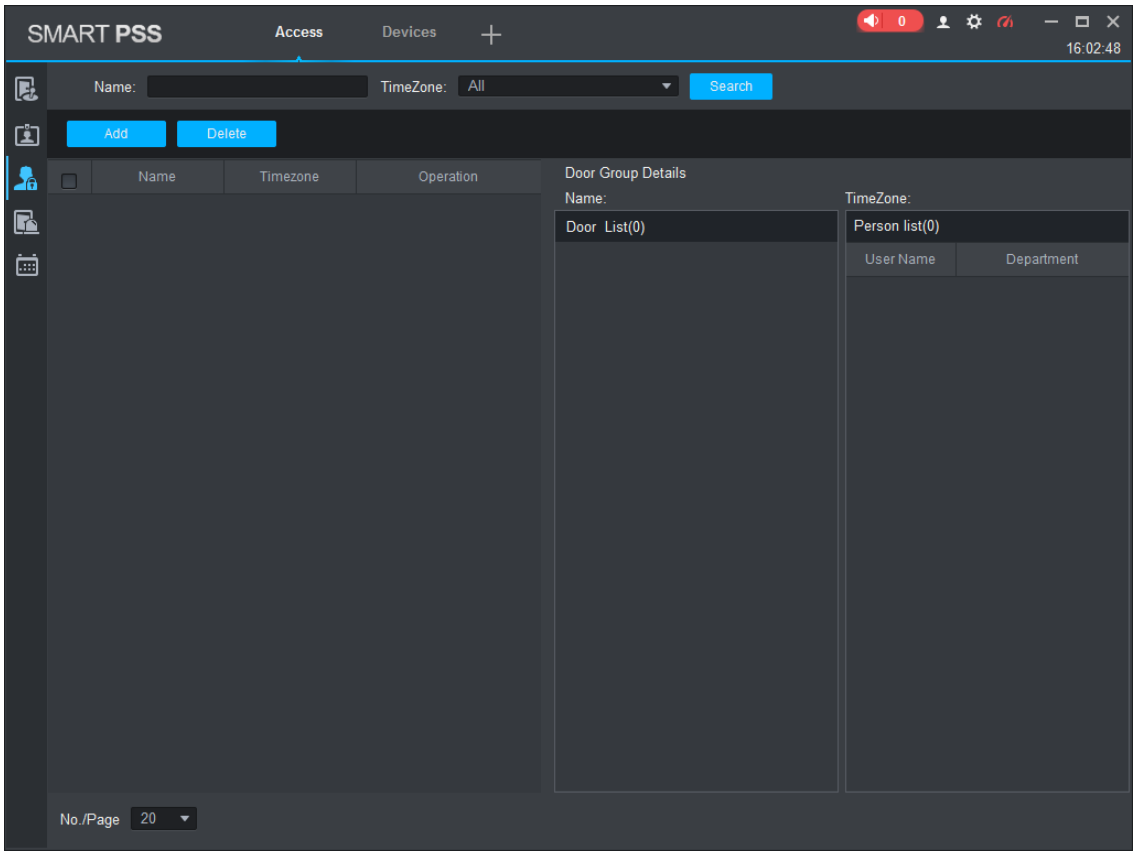
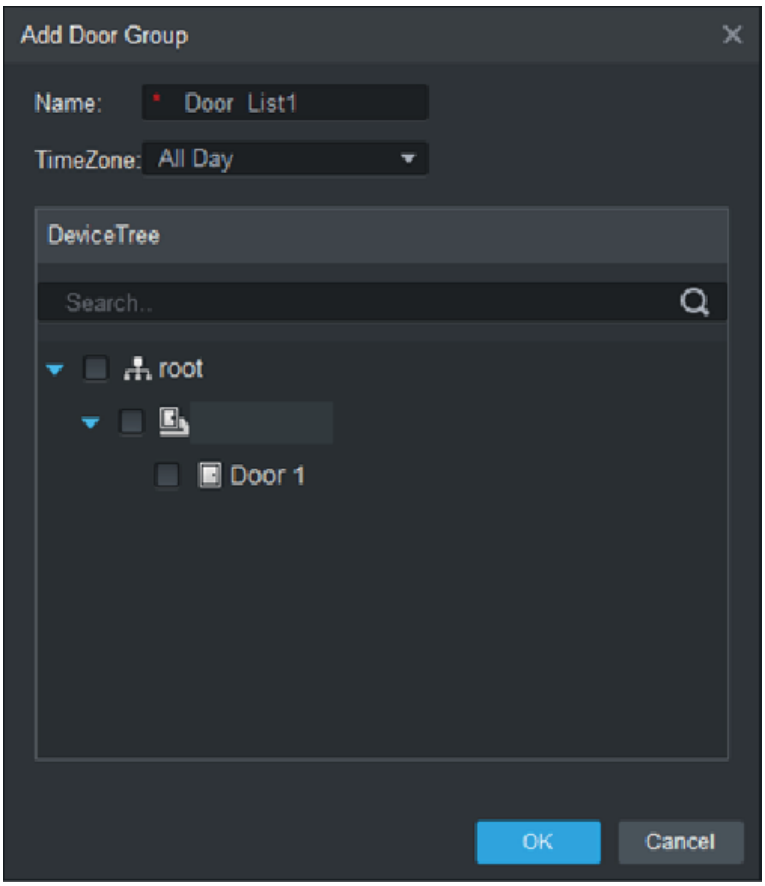


Рисунок 5-11 Добавление группы дверей



5.5 Настройка разрешений на доступ

Вы можете настраивать разрешения на доступ. Имеются два варианта: разрешения для групп дверей и разрешения для пользователей. Информация о пользователях, которым предоставлен доступ, в Smart PSS и контроллерах доступа будет синхронизироваться.

5.5.1 Разрешения по группам дверей

Выберите группу дверей, добавьте пользователей в список дверей, и пользователи в списке дверей получат разрешение для всех дверей в списке. См. рисунок 5-12 и 5-13.

Рисунок 5-12 Доступ

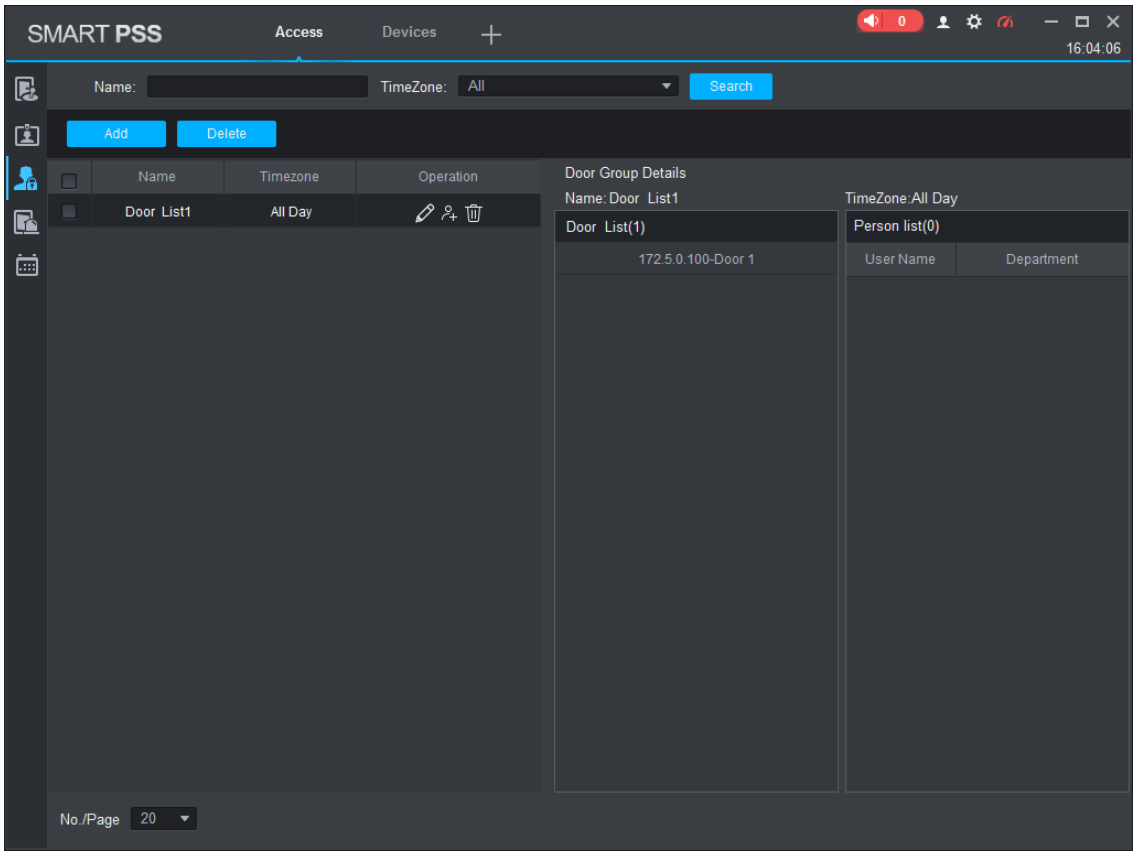
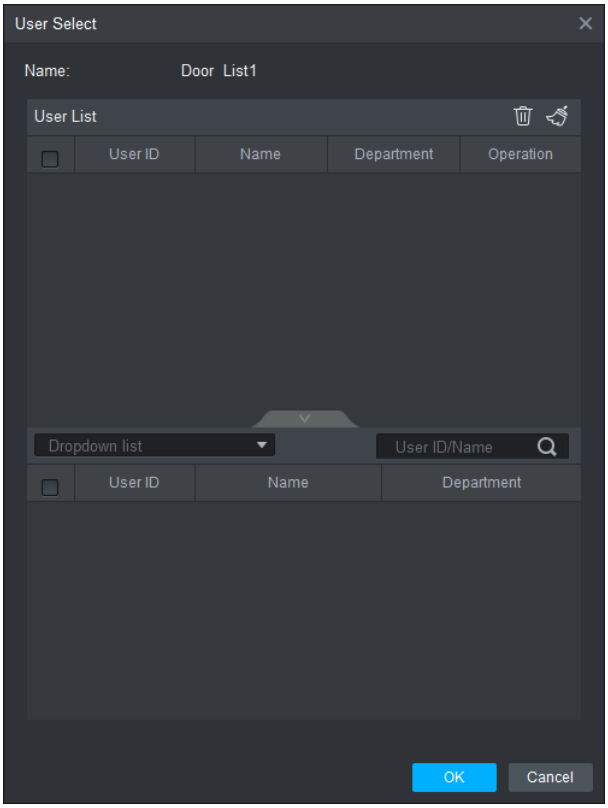


Рисунок 5-13 Список пользователей



Шаг 1 В окне **Access (Доступ)** нажмите,  нажмите **Add** и **Door Group Permission**.

Шаг 2 Нажмите  . Выберите отдел для пользователя (Department) в раскрывающемся списке или введите **ID/имя пользователя**, и выполните поиск пользователей

Выберите нужных пользователей.

Шаг 3 Нажмите **Finish (Завершить)**, чтобы завершить процесс настройки.

Пользователей без ID невозможно найти.

5.5.2 Разрешение по ID пользователей

Вы можете предоставить разрешение для пользователей, выбрав его, а затем, группу дверей для пользователя. См. рисунок 5-14 и рисунок 5-15.

Рисунок 5-14 Доступ

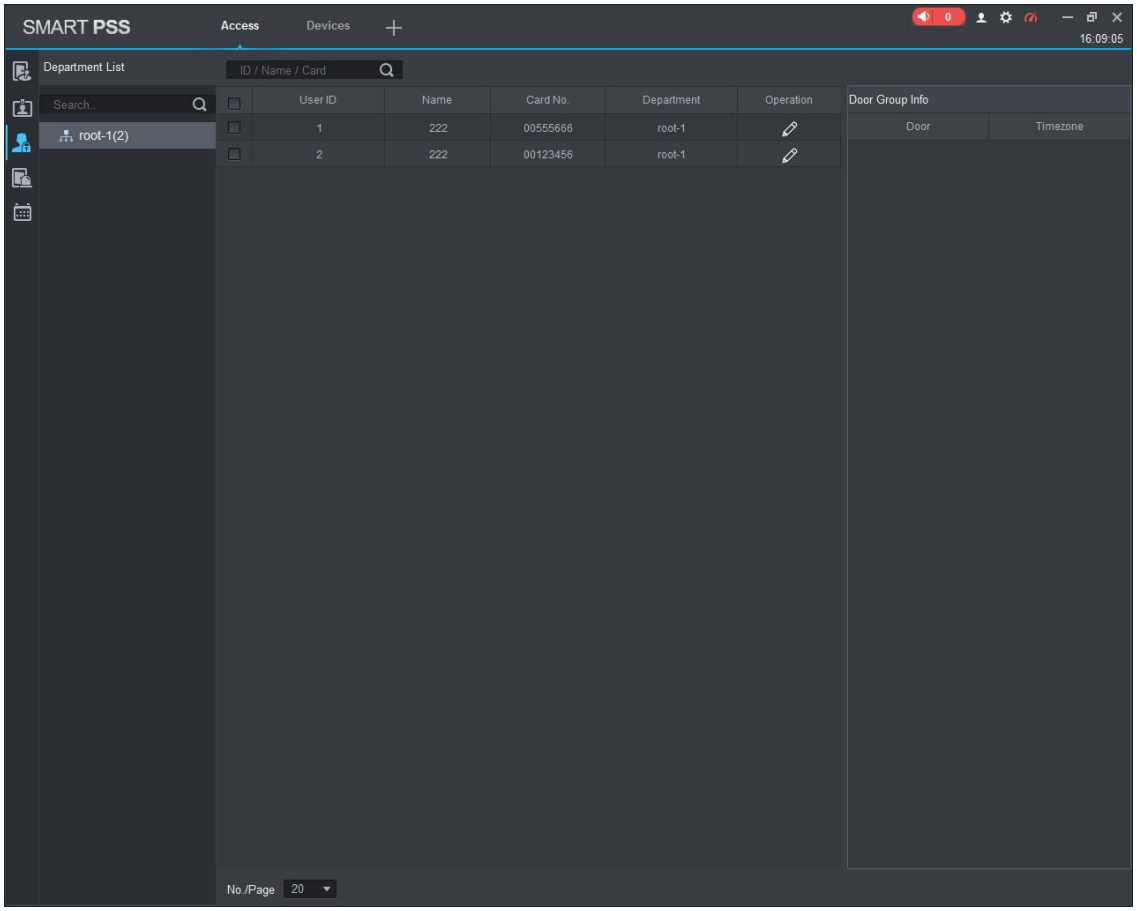
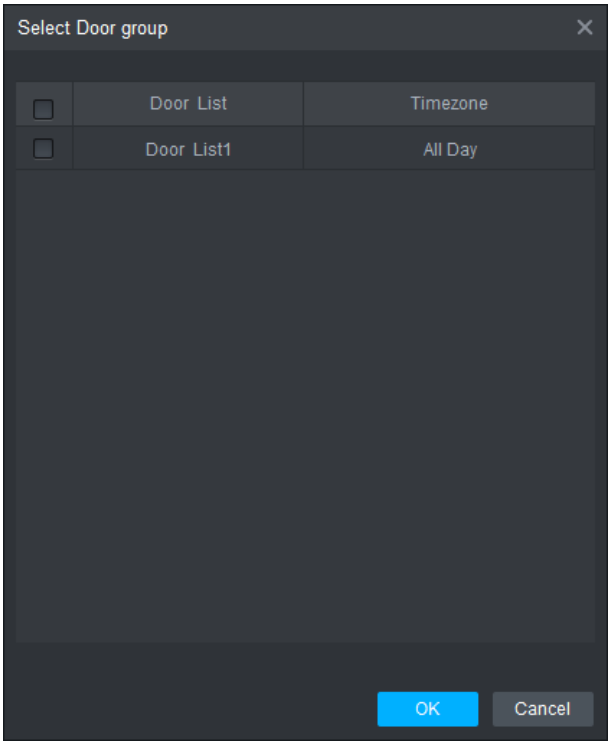


Рисунок 5-15 Выбор группы дверей



Шаг 1 В окне **Access (Доступ)** нажмите 

Шаг 2 Нажмите  . Откроется окно Select Door Group (Выбрать группу дверей).

Step 3 Выберите отдел для пользователя (Department) в раскрывающемся списке или введите ID/имя пользователя, затем, выберите список дверей.

Шаг 4 Нажмите Finish (Завершить), чтобы завершить процесс настройки.

Приложение 1 Рекомендации по кибербезопасности

Кибербезопасность – это не просто модное слово: она относится к любому устройству, которое подключается к Интернету. IP-видеонаблюдение не может быть неуязвимым перед рисками кибератак, но базовые процедуры по обеспечению защиты, усиление сетей и сетевых устройств позволяет снизить такую уязвимость. Ниже представлено несколько советов о том, как создать более защищенную систему безопасности.

Обязательные действия, обеспечивающие базовую сетевую безопасность оборудования:

1. **Использование надежных паролей**

   Соблюдайте следующие указания по установке паролей:

   - Длина должна быть не меньше 8 символов.
   - Используйте как минимум два вида символов; к видам символов относятся буквы в верхнем и нижнем регистре, цифры и знаки.
   - Не используйте название учетной записи или его же в обратном порядке.
   - Не используйте последовательные символы, такие как 123, abc и т.д.
   - Не используйте повторяющиеся символы, такие как 111, aaa и т.д.

2. **Своевременно обновляйте программное обеспечение**

   - Как принято в технической индустрии, мы рекомендуем постоянно обновлять программное обеспечения вашего оборудования (например, NVR, DVR, IP-камер и т.д.), чтобы обеспечить самые последние патчи для устранения уязвимостей системы. Если оборудование подключается к публичной сети, рекомендуется включать «автоматический поиск обновлений», чтобы получать актуальную информацию об обновлениях программного обеспечения, выпущенных производителем.
   - Мы рекомендуем скачивать и использовать последние версии клиентского программного обеспечения.

Необязательные рекомендации по повышению сетевой безопасности:

1. **Физическая защита**

   Мы рекомендуем обеспечивать физическую защиту оборудования, особенно устройств для хранения данных. Например, размещать оборудование в специальных помещениях для ЭВМ и шкафах, а также обеспечивать надлежащий контроль доступа и распределение ключей, чтобы избежать физического контакта неуполномоченного персонала с оборудованием, например, повреждение оборудования, несанкционированное подключение съемных устройств (таких как USB-накопители, серийные порты) и т.д.

2. **Регулярно меняйте пароли**

   Мы рекомендуем регулярно менять пароли, чтобы избежать доступа неуполномоченных пользователей или взлома.

3. **Своевременно настраивайте и обновляйте информацию о смене паролей**

   Оборудование поддерживает функцию смены паролей. Своевременно настраивайте информацию, необходимую для смены паролей, включая электронную почту конечного пользователя и контрольные вопросы. Если информация изменилась, своевременно заменяйте ее. При настройке контрольных вопросов не рекомендуется использовать простые вопросы.

4. **Активируйте блокировку учетной записи**

   Функция блокировки учетной записи установлена по умолчанию, и мы рекомендуем использовать ее, чтобы обеспечить безопасность учетной записи. Если злоумышленник попытается войти систему, используя неправильный пароль несколько раз, соответствующая учетная запись и IP-адрес источника будут заблокированы.

5. **Меняйте HTTP и другие сервисные порты по умолчанию**

   Мы рекомендуем менять HTTP и другие сервисные порты по умолчанию, используя любой набор цифр между 1024~65535. Это позволяет снизить риск того, что посторонние смогут догадаться, какие порты вы используете.

6. **Активируйте HTTPS**

   Мы рекомендуем активировать HTTPS, чтобы вы получали доступ к веб-сервису через защищенный канал связи.

7. **Активируйте «белый список»**

   Мы рекомендуем использовать функцию «белого списка», чтобы вход в систему был возможен только с указанных IP-адресов. При этом, убедитесь в том, что IP-адрес вашего ПК и IP-адреса прочего оборудования были добавлены в «белый список».

8. **Привязка по MAC-адресу**

   Мы рекомендуем связывать IP- и MAC-адрес шлюза оборудования, чтобы снизить риск сетевой атаки с помощью протокола ARP.

9. **Предоставляйте учетные записи и привилегии рациональным образом**

   Добавляйте пользователей и назначайте минимальный набор разрешений для них в соответствии с целями бизнеса и управления.

10. **Отключайте ненужные сервисы и выбирайте безопасные режимы**

    Чтобы снизить возможные риски, рекомендуется отключать сервисы SNMP, SMTP, UPnP и т.д., если они не нужны.

    Если такие сервисы нужны, настоятельно рекомендуется использовать безопасные режимы, включая следующие сервисы, но не ограничиваясь ими:

    - SNMP: Выберите SNMP v3 и установите надежные пароли шифрования и авторизации.
    - SMTP: выберите TLS для доступа к серверу электронной почты.
    - FTP: выберите SFTP и установите надежные пароли.
    - Точка доступа AP: Выберите режим шифрования WPA2-PSK и установите надежные пароли.

11. **Передача аудио и видеоданных с шифрованием**

    Если ваши аудио и видеоданные очень важны или являются конфиденциальными, мы рекомендуем использовать функцию передачи с шифрованием, чтобы снизить риск перехвата аудио и видео при передаче

    .

12. **Контроль безопасности**

    - Проверка онлайн-пользователей: мы рекомендуем регулярно проверять онлайн-пользователей, чтобы видеть, если в систему вошли несанкционированные пользователи.
    - Проверка журналов оборудования: Просматривая журналы, вы можете узнать IP-адреса, используемые для авторизации и выполненные ключевые операции.

13. **Сетевой журнал**

    Поскольку место для хранения данных в устройствах ограничено, также ограничены и сохраняемые журналы. Если вам необходимо хранить журнал в течение продолжительного времени, рекомендуется активировать функцию сетевого журнала, чтобы обеспечить синхронизацию критических журналов с сервером сетевого журнала для отслеживания.

14. **Создание безопасной сетевой среды**

    Чтобы обеспечить более надежную защиту оборудования и снизить возможные риски для кибербезопасности, мы рекомендуем:

    - Отключать функцию распределения портов для роутера, чтобы избежать прямого доступа к устройствам интрасети из внешней сети.

- Сеть должна быть разделена и изолирована в соответствии с реальными нуждами. Если какие-либо требования к связи между двумя подсетями отсутствуют, рекомендуется использовать VLAN, сетевой GAP и другие технология для разделения сети, чтобы обеспечить изолирование сети.
- Используйте систему доступа 802.1x, чтобы снизить риск доступа неуполномоченных пользователей к частным сетям.