

Руководство пользователя SpeedFace M4

Дата: август 2021

Версия документа: 1.0

Спасибо, что выбрали наше устройство. Пожалуйста, внимательно прочтите инструкции перед работой. Следуйте этим инструкциям, чтобы убедиться, что устройство работает правильно. Изображения, представленные в этом руководстве, предназначены только для иллюстративных целей.



Для получения дополнительной информации посетите веб-сайт нашей компании www.zkteco.com.

Copyright© 2020 ZKTECO CO., LTD. All rights reserved.

Без предварительного письменного согласия ZKTeco никакая часть данного руководства не может быть скопирована или переслана каким-либо образом или в любой форме. Все части данного руководства принадлежат ZKTeco и его дочерним компаниям (далее «Компания» или «ZKTeco»).

Товарный знак

ZKTeco является зарегистрированным товарным знаком ZKTeco. Остальные товарные знаки, упомянутые в данном руководстве, являются собственностью соответствующих владельцев.

Отказ от прав

Данное руководство содержит информацию по эксплуатации и техническому обслуживанию оборудования ZKTeco. Авторские права на все документы, чертежи и т. д., относящиеся к поставляемому ZKTeco оборудованию, принадлежат и являются собственностью ZKTeco. Содержимое этого документа не должно использоваться или передаваться получателем с любой третьей стороной без письменного разрешения ZKTeco.

Содержимое этого руководства должно быть прочитано целиком, прежде чем начинать эксплуатацию и техническое обслуживание поставляемого оборудования. Если какое-либо из содержимого руководства кажется неясным или неполным, свяжитесь с ZKTeco перед началом эксплуатации и технического обслуживания указанного устройства.

Для обеспечения удовлетворительной работы и технического обслуживания крайне важно, чтобы персонал по эксплуатации и техническому обслуживанию был полностью знаком с конструкцией и чтобы указанный персонал прошел тщательную подготовку по эксплуатации и техническому обслуживанию устройства / агрегата / оборудования. Кроме того для безопасной эксплуатации устройства / агрегата / оборудования важно, чтобы персонал прочитал, понял и выполнил инструкции по технике безопасности, содержащиеся в руководстве.

В случае любого противоречия между условиями данного руководства и спецификациями контракта, чертежи, инструкции или любые другие документы, связанные с контрактом, условия / документы контракта имеют преимущественную силу. Конкретные условия / документы контракта применяются в приоритетном порядке.

ZKTeco не предоставляет никаких гарантий или заверений в отношении полноты любой информации, содержащейся в данном руководстве, или любых внесенных законных изменений. ZKTeco не продлевает какие-либо гарантии, включая, помимо прочего, любые гарантии дизайна, пригодности для продажи или пригодности для конкретной цели.

ZKTeco не несет ответственности за любые ошибки или упущения в информации или документах, на которые ссылается данное руководство или которые связаны с ними. Весь риск, связанный с результатами и результатами, полученными при использовании информации, принимает на себя пользователь.

ZKTeco ни в коем случае не несет ответственности перед пользователем или любой третьей стороной за любые случайные, косвенные, косвенные, специальные или примерные убытки, включая, помимо прочего, потерю бизнеса, упущенную выгоду, прерывание деятельности, потерю деловой информации или любую другую информацию. материальный ущерб, возникший в результате, в связи с использованием информации, содержащейся в настоящем руководстве или на которую имеется ссылка, даже если ZKTeco был уведомлен о возможности такого ущерба.

Это руководство и содержащаяся в нем информация могут содержать технические, другие неточности или опечатки. ZKTeco периодически меняет информацию, которая будет включена в новые добавления / поправки к руководству. ZKTeco оставляет за собой право добавлять, удалять, изменять или изменять информацию. время от времени содержится в руководстве в форме циркуляров, писем, заметок и т. д. для улучшения работы и безопасности устройства / агрегата / оборудования. Указанные дополнения или поправки предназначены для улучшения / улучшения работы устройства / агрегата / оборудования и такие поправки не дают права требовать какую-либо компенсацию или ущерб при любых обстоятельствах.

ZKTeco никоим образом не несет ответственности (i) в случае неисправности устройства / агрегата / оборудования из-за какого-либо несоблюдения инструкций, содержащихся в данном руководстве (ii) в случае эксплуатации устройства / агрегата / оборудования сверх пределов нормы (iii) в случае эксплуатации машины и оборудования в условиях, отличных от предписанных условий руководства.

Время от времени продукт будет обновляться без предварительного уведомления. Последние процедуры и соответствующие документы доступны на <http://www.zkteco.com>

Если есть какие-либо проблемы, связанные с продуктом, свяжитесь с нами.

Главный офис ZKTeco

Адрес ZKTeco Industrial Park, No. 26, 188 Industrial Road, Tangxia Town, Dongguan, China.

Телефон +86 769 - 82109991

Факс +86 755 - 89602394

По вопросам, связанным с бизнесом, пожалуйста, пишите нам по адресу: sales@zkteco.com.

Чтобы узнать больше о наших филиалах по всему миру, посетите www.zkteco.com.

О компании

ZKTeco является одним из крупнейших в мире производителей RFID и биометрических считывателей

(по отпечаткам пальцев, лицу, ладоням) Предлагаемые устройства включают в себя считыватели и панели контроля доступа, камеры распознавания лиц ближнего и дальнего радиуса действия, контроллеры доступа к лифту / полу, турникеты, контроллеров шлагбаумов с распознаванием государственных номерных знаков (LPR) и потребительские товары, в том числе дверные замки с отпечатками пальцев и распознаванием лица на батарейках. Наши решения в области безопасности многоязычны и локализованы на более чем 18 языках. На современной площади 700 000 кв. футов сертифицированный по ISO9001 производственный объект компании ZKTeco мы управляем производством, дизайном устройств, осуществляем сборку компонентов и логистику / доставку, и все под одной крышей.

Основатели ZKTeco были настроены на независимое исследование и разработку процедур биометрической верификации и производство SDK для биометрической верификации, который первоначально широко применялся в областях безопасности ПК и аутентификации личности. С постоянным совершенствованием разработки и большим количеством рыночных приложений, Команда постепенно создала экосистему аутентификации личности и интеллектуальную систему безопасности, которые основаны на методах биометрической верификации. Имея многолетний опыт в области индустриализации биометрических верификаций, ZKTeco была официально основана в 2007 году и в настоящее время является одним из ведущих предприятий в отрасли биометрической верификации 6 лет подряд владеет различными патентами и выбирается в качестве национального высокотехнологичного предприятия, продукты которого защищены правами интеллектуальной собственности.

О руководстве

Руководство знакомит с работой устройства **SpeedFace M4**.

Все приведенные цифры приведены только в качестве иллюстрации. Фотографии в данном руководстве могут не полностью соответствовать фактическим устройствам.

Условные обозначения документа

Условные обозначения, используемые в данном руководстве, перечислены

ниже: Условные обозначения в графическом интерфейсе

Для программного обеспечения	
Условное обозначение	Описание
Жирный шрифт	Используется для идентификации имен программного интерфейса, например ОК, подтвердить, отменить
>	Многоуровневые меню разделены этими скобками. Например, Файл> Создать> Папка.
Для устройства	
Условное обозначение	Описание
<>	Названия кнопок или клавиш для устройств. Например, нажмите <ОК>
[]	Имена окон, пунктов меню, таблицы данных и имен полей заключены в квадратные скобки. Например, всплывающее окно [Новый пользователь]
/	Многоуровневые меню разделены косой чертой. Например, [Файл / Создать / Папка].

Символы

Условное обозначение	Описание
	Этот символ подразумевает информацию об уведомлении или обращает на себя внимание в руководстве.
	Общая информация, которая помогает быстрее выполнять операции.
	Информация, которая является важной
	Меры предпринятые, чтобы избежать опасности или ошибок
	Утверждение или событие, предупреждающее о чем-либо или служащее предостерегающим примером.

Содержание

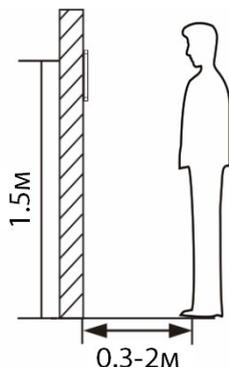
1 ИНСТРУКЦИЯ ПО ПРИМЕНЕНИЮ	7
1.1 ПОЛОЖЕНИЕ СТОЯ, ВЫРАЖЕНИЕ ЛИЦА И НЕПОДВИЖНАЯ ПОЗА	7
1.2 РЕГИСТРАЦИЯ ЛАДОНИ	8
1.3 РЕГИСТРАЦИЯ ЛИЦА	9
1.4 ИНТЕРФЕЙС ОЖИДАНИЯ	10
1.5 ВИРТУАЛЬНАЯ КЛАВИАТУРА	11
1.6 РЕЖИМ ВЕРИФИКАЦИИ	12
1.6.1 ВЕРИФИКАЦИЯ ЛАДОНИ	12
1.6.2 ВЕРИФИКАЦИЯ ЛИЦА	14
1.6.3 ВЕРИФИКАЦИЯ ПРОПУСКА	17
1.6.4 ВЕРИФИКАЦИЯ ПАРОЛЯ	20
1.6.5 КОМБИНИРОВАННАЯ ВЕРИФИКАЦИЯ	24
2 ГЛАВНОЕ МЕНЮ	25
3 УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ	26
3.1 ДОБАВИТЬ ПОЛЬЗОВАТЕЛЕЙ	26
3.2 ПОИСК ПОЛЬЗОВАТЕЛЕЙ	30
3.3 РЕДАКТИРОВАТЬ ПОЛЬЗОВАТЕЛЕЙ	31
3.4 УДАЛИТЬ ПОЛЬЗОВАТЕЛЕЙ	31
3.5 СТИЛЬ ОТОБРАЖЕНИЯ	31
4 РОЛЬ ПОЛЬЗОВАТЕЛЯ	33
5 НАСТРОЙКИ СВЯЗИ	35
5.1 СЕТЕВЫЕ НАСТРОЙКИ	35
5.2 ПОСЛЕДОВАТЕЛЬНАЯ СВЯЗЬ	36
5.3 ПОДКЛЮЧЕНИЕ ПК.....	37
5.4 БЕСПРОВОДНАЯ СЕТЬ	37
5.5 НАСТРОЙКА ОБЛАЧНОГО СЕРВЕРА.....	40
5.6 УСТАНОВКА WIEGAND	41
5.7 СЕТЕВАЯ ДИАГНОСТИКА	44
6 НАСТРОЙКИ СИСТЕМЫ	45
6.1 ДАТА И ВРЕМЯ	45
6.2 ПАРАМЕТРЫ УЧЕТА РАБОЧЕГО ВРЕМЕНИ	46
6.3 ПАРАМЕТРЫ ЛИЦА	48
6.4 ПАРАМЕТРЫ ЛАДОНИ	50
6.5 СБРОС ДО ЗАВОДСКИХ НАСТРОЕК	51
6.6 НАСТРОЙКА ТИПА УСТРОЙСТВА	52
6.7 УПРАВЛЕНИЕ ОБНАРУЖЕНИЕМ	53
7 НАСТРОЙКИ ПЕРСОНАЛИЗАЦИИ	54
7.1 НАСТРОЙКИ ИНТЕРФЕЙСА	54

7.2	ГОЛОСОВЫЕ НАСТРОЙКИ	55
7.3	ГРАФИКИ ЗВОНКОВ	56
8	УПРАВЛЕНИЕ ДАННЫМИ	57
8.1	УДАЛИТЬ ДАННЫЕ	57
9	КОНТРОЛЬ ДОСТУПА	59
9.1	ПАРАМЕТРЫ КОНТРОЛЯ ДОСТУПА	60
9.2	ВРЕМЕННОЙ ГРАФИК	61
9.3	НАСТРОЙКИ ПРАЗДНИЧНЫХ ДНЕЙ	63
9.4	НАСТРОЙКИ КОМБИНИРОВАННОЙ ВЕРИФИКАЦИИ	64
9.5	УСТАНОВКА КОНТРОЛЯ ПОВТОРНОГО ПРОХОДА	66
9.6	НАСТРОЙКИ ПАРАМЕТРОВ ПРИНУЖДЕНИЯ	67
10	ПОИСК СОБЫТИЙ УЧЕТА РАБОЧЕГО ВРЕМЕНИ	68
11	АВТОМАТИЧЕСКОЕ ТЕСТИРОВАНИЕ	70
12	ИНФОРМАЦИЯ О СИСТЕМЕ	71
13	ПОДКЛЮЧИТЬ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ ZKBIOACCESS MTD	72
13.1	УСТАНОВИТЬ АДРЕС СВЯЗИ	72
13.2	ДОБАВИТЬ УСТРОЙСТВО В ПО	73
13.3	ДОБАВИТЬ СОТРУДНИКОВ В ПО	73
ПРИЛОЖЕНИЕ 1	75
	ТРЕБОВАНИЯ К СБОРУ И РЕГИСТРАЦИИ ИЗОБРАЖЕНИЯ ЛИЦА В ВИДИМОМ СВЕТЕ	75
	ТРЕБОВАНИЯ К ДАННЫМ ЦИФРОВОГО ИЗОБРАЖЕНИЯ ЛИЦА В ВИДИМОМ СВЕТЕ	76
ПРИЛОЖЕНИЕ 2	77
	ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ	77
	ЭКОЛОГИЧЕСКИ БЕЗОПАСНАЯ РАБОТА	80

1 Инструкция по применению

1.1 Положение стоя, выражение лица и неподвижная поза

Рекомендуемое расстояние



Расстояние между устройством и пользователем, рост которого находится в пределах 1,55–1,85 м, рекомендуется от 0,3 до 2 м. Пользователи могут немного двигаться вперед и назад, чтобы улучшить качество захваченного изображения лица.

Выражение лица и положение стоя





Примечание: во время регистрации и верификации сохраняйте естественное выражение лица и прямую позу стоя.

1.2 Регистрация ладони

Поместите ладонь в мультимедийную зону сканирования ладони так, чтобы ладонь располагалась параллельно устройству. Убедитесь, что между пальцами есть зазор.



Примечание:

- 1) Расположите ладонь на расстоянии 30-50 см от устройства.
- 2) Поместите ладонь в зону сканирования ладони так, чтобы ладонь располагалась параллельно устройству.
- 3) Убедитесь, что между пальцами есть зазор.
- 4) Избегайте попадания прямых солнечных лучей при использовании функции ладони на открытом воздухе. Согласно лабораторным испытаниям, лучший эффект распознавания ладони достигается при освещенности не более 10000 люкс.

1.3 Регистрация лица

Во время регистрации старайтесь держать лицо в центре экрана. Пожалуйста, смотрите в камеру и оставайтесь неподвижными во время регистрации лица. Страница выглядит так, как показано ниже:



Регистрация лица и методы аутентификации

Инструкция по регистрации лица

- При регистрации лица соблюдайте расстояние от 40 до 80 см между устройством и лицом.
- Будьте осторожны, не меняйте выражение лица (улыбающееся лицо, искаженное лицо, подмигивание и т. д.)
- Если вы не будете следовать инструкциям на экране, регистрация лица может занять больше времени или может не пройти.
- Будьте осторожны, не прикрывайте глаза или брови.
- Не носите головные уборы, маски, солнечные очки или очки.
- Будьте осторожны, не показывайте на экране два лица. Регистрируйте по одному человеку за раз.
- Пользователям в очках рекомендуется регистрировать лица как в очках, так и без них.

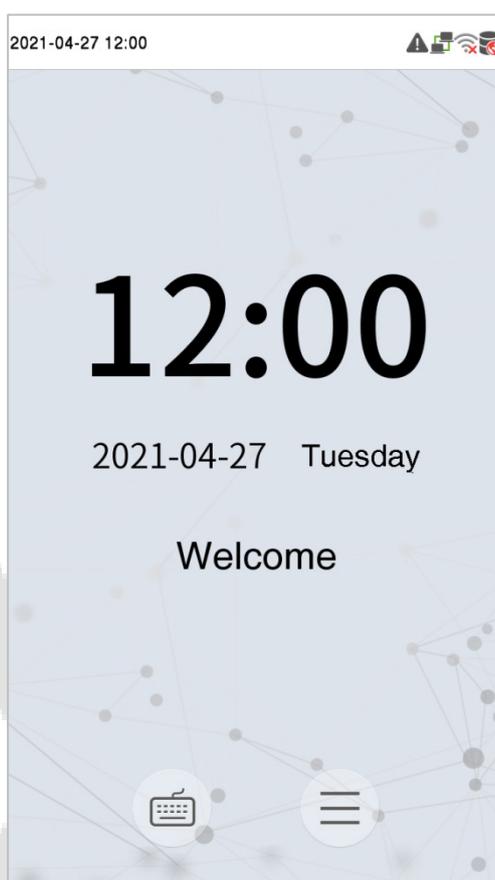
Инструкция по аутентификации лица

- Убедитесь, что лицо появляется внутри области обнаружения, отображаемой на экране устройства.

- Если очки были заменены, аутентификация может не пройти. Если было зарегистрировано лицо без очков, проведите аутентификацию без очков. Если было зарегистрировано только лицо в очках, еще раз проведите аутентификацию лица в ранее надетых очках.
- Если часть лица прикрыта шляпой, маской, повязкой на глаз или солнцезащитными очками, аутентификация может не пройти. Не закрывайте лицо, позвольте устройству распознавать и брови, и лицо.

1.4 Интерфейс ожидания

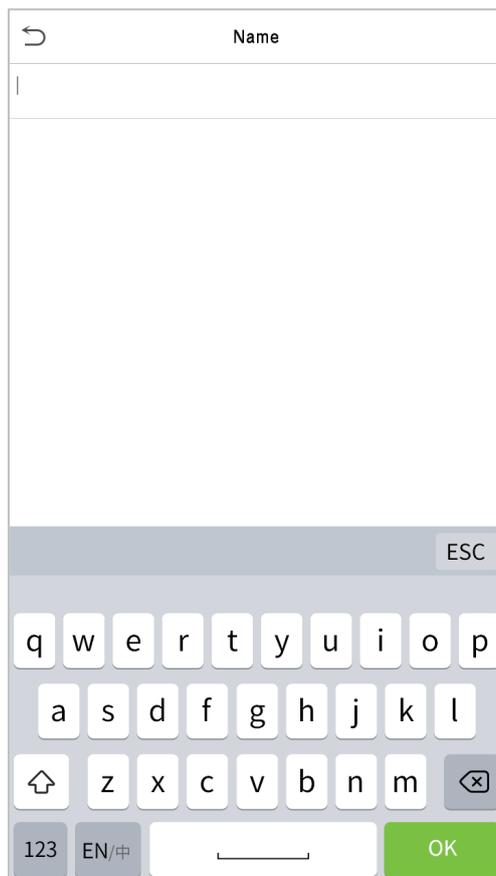
После подключения источника питания интерфейс выглядит, как показано ниже:



Примечание:

- 1) Нажмите , чтобы открыть интерфейс для ввода идентификатора пользователя.
- 2) Если в устройстве не установлен суперадминистратор, нажмите  для входа в меню. После установки суперадминистратора перед входом в меню требуется его верификация. Для обеспечения безопасности устройства рекомендуется зарегистрировать суперадминистратора при первом использовании устройства.

1.5 Виртуальная клавиатура



Примечание: устройство поддерживает ввод китайских и английских символов, цифр и символов. Нажмите [**En**], чтобы переключиться на английскую клавиатуру. Нажмите [**123**], чтобы переключиться на клавиатуру цифровых и специальных символов, и нажмите [**ABC**], чтобы вернуться к алфавитной клавиатуре. Нажмите поле ввода, и появится виртуальная клавиатура. Нажмите [**ESC**], чтобы закрыть экран клавиатуры.

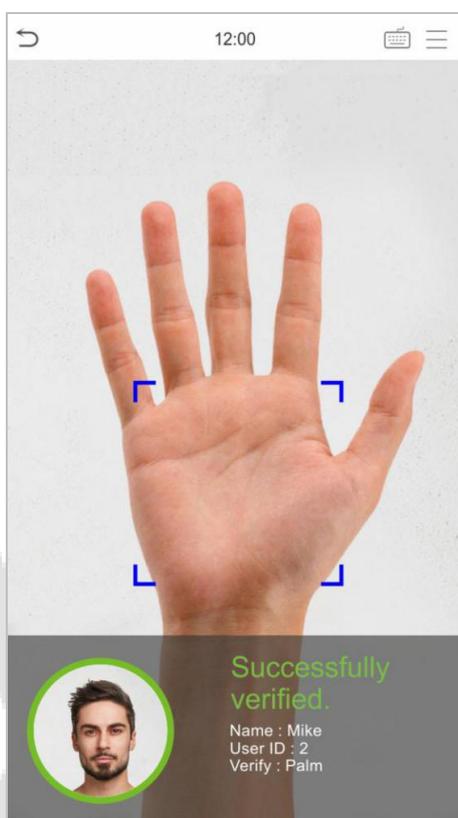
1.6 Режим верификации

1.6.1 Верификация ладони

Режим верификации ладони 1:N

Такой режим верификации сравнивает шаблон ладони, полученный модулем ладони, со всеми шаблонами данных ладони в устройстве.

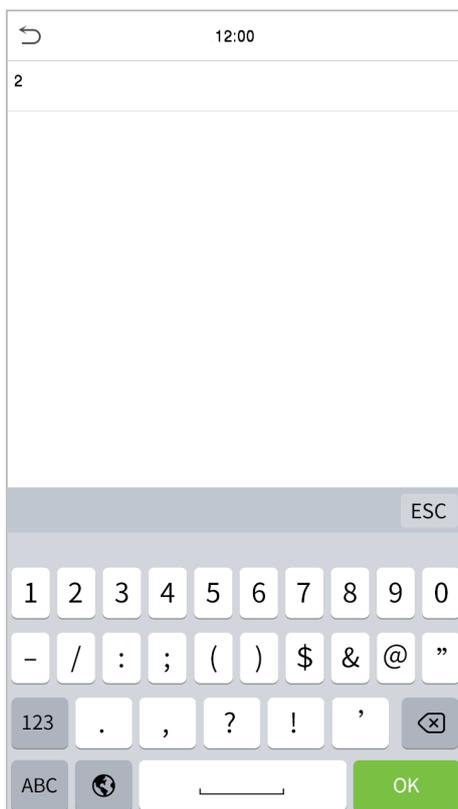
Устройство автоматически распознает режим верификации ладони и лица. Поместите ладонь в зону сканирования ладони так, чтобы устройство автоматически переключилось в режим верификации ладони.



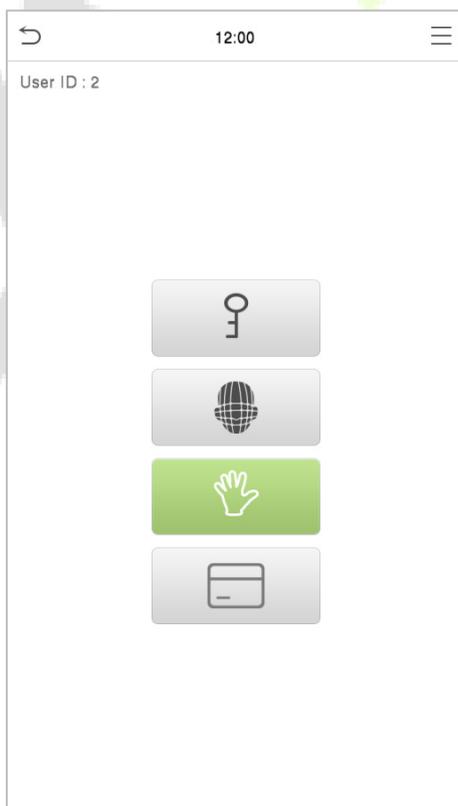
Режим верификации ладони 1:1

Нажмите на кнопку  на главном экране, чтобы открыть режим верификации ладони 1:1.

1. Введите идентификатор пользователя и нажмите [OK].



Если пользователь зарегистрировал карту, лицо и пароль в дополнение к ладони, а метод верификации установлен на верификацию пароля / лица / ладони / карты, появится экран ниже. Выберите значок ладони , чтобы войти в режим верификации ладони.

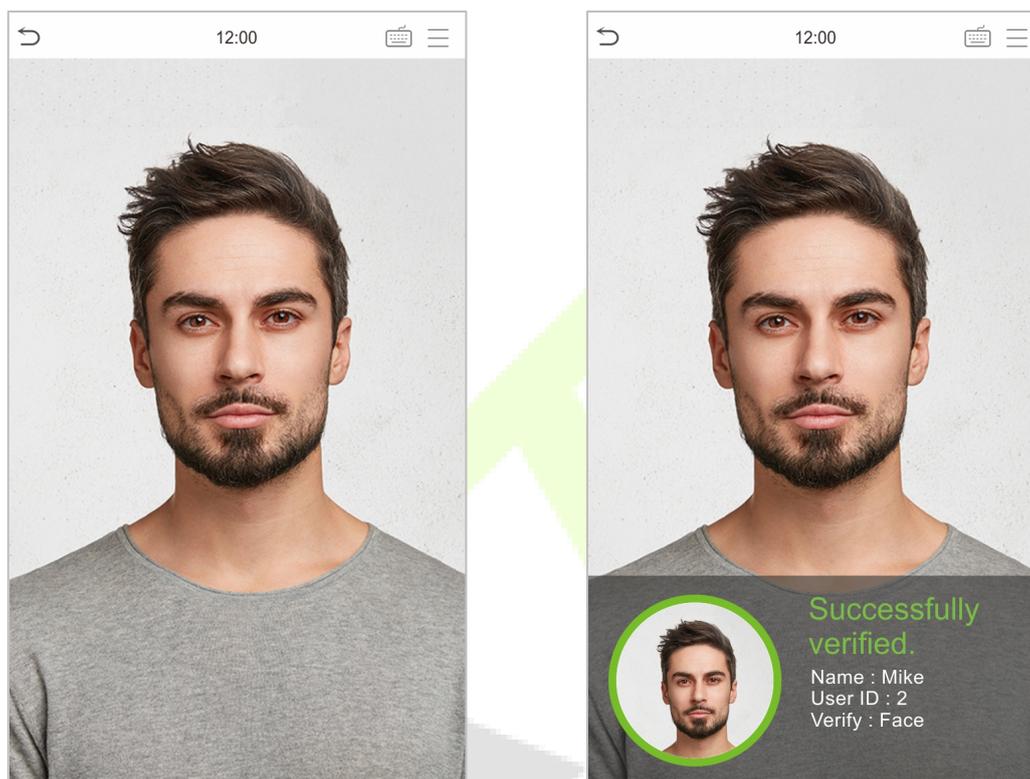


1.6.2 Верификация лица

Верификация лица 1:N (один ко многим)

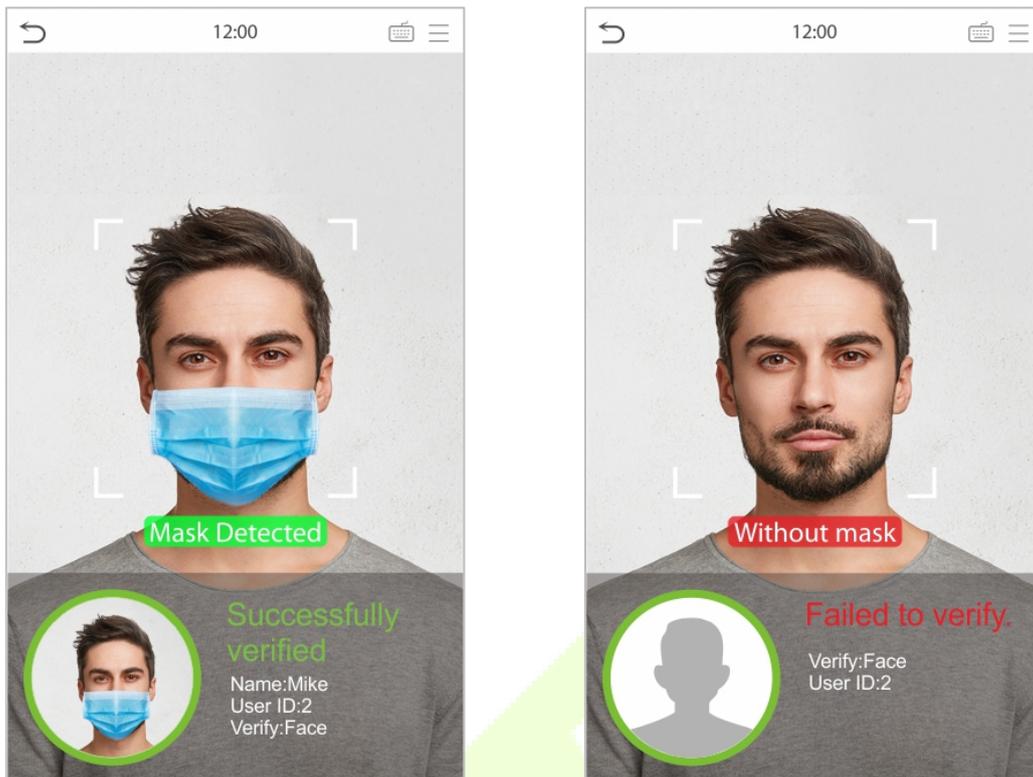
1. Обычная верификация

Такой режим верификация сравнивает полученные изображения лиц со всеми данными лиц, зарегистрированных в устройстве. Ниже показано всплывающее окно с подсказкой результата сравнения.



2. Включить обнаружение маски

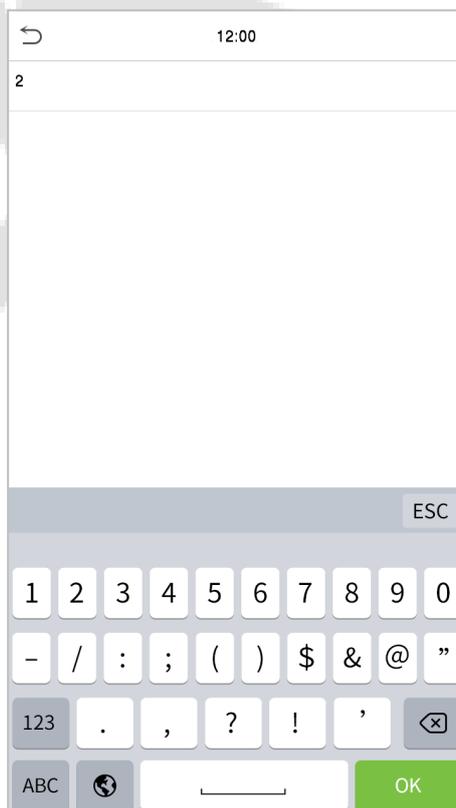
Когда пользователь включил функцию «**Включить обнаружение маски**», устройство будет определять, носит ли пользователь маску или нет. Ниже приведено всплывающее окно интерфейса подсказки результатов сравнения.



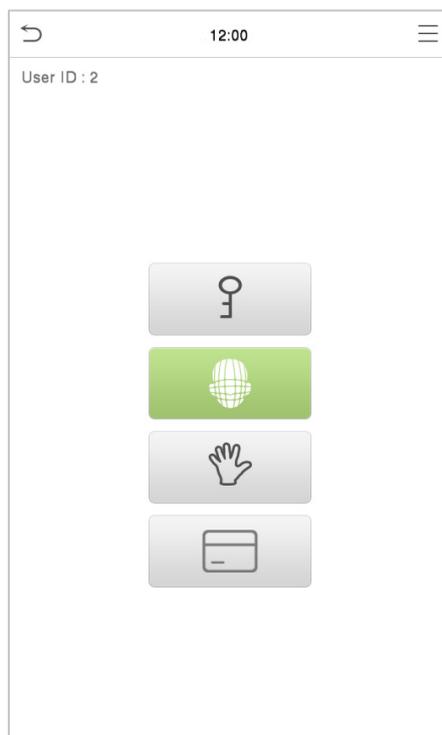
Верификация лица 1:1 (один к одному)

Такой метод верификации сравнивает лицо, захваченное камерой, с шаблоном лица, связанным с введенным идентификатором пользователя. Нажмите  на главном интерфейсе, чтобы открыть режим верификации лица 1:1 (один к одному).

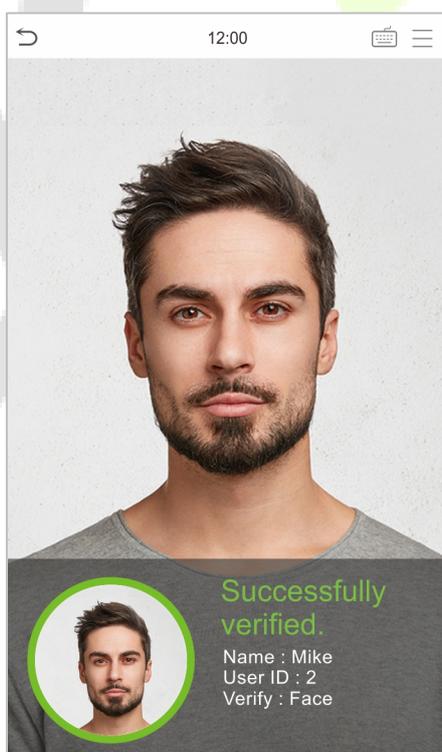
Введите идентификатор пользователя и нажмите [OK].



Если сотрудник регистрирует ладонь, карту и пароль в дополнение к лицу, а метод верификации установлен на пароль / карта / лицо / ладонь, появится экран ниже. Выберите значок , чтобы войти в режим верификации лица.



После успешной верификации появится сообщение **«Верификация прошла успешно»**, как показано ниже.

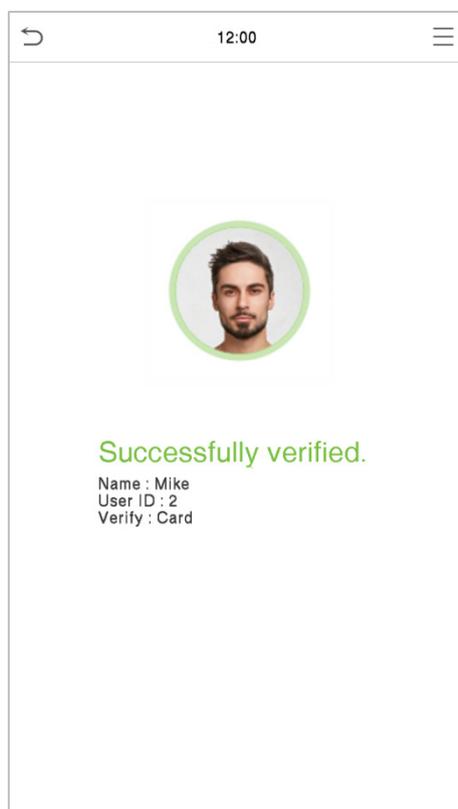


Если верификация не удалась, появится подсказка **«Пожалуйста, измените свое положение!»**.

1.6.3 Верификация карты

Верификация пропуска 1:N

В таком режиме верификации номер карты в области ввода карты сравнивается со всеми данными номеров карт, зарегистрированных в устройстве; Ниже показан экран верификации карты.



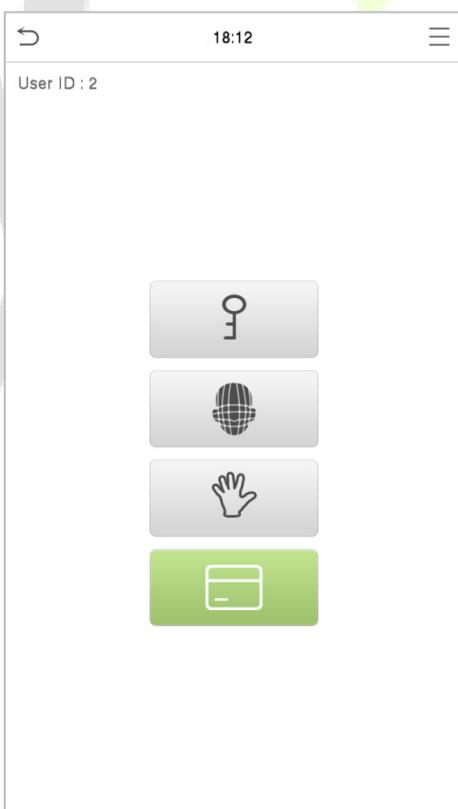
Верификация карты 1:1

Нажмите кнопку  на главном интерфейсе, чтобы открыть режим верификации карты 1:1.

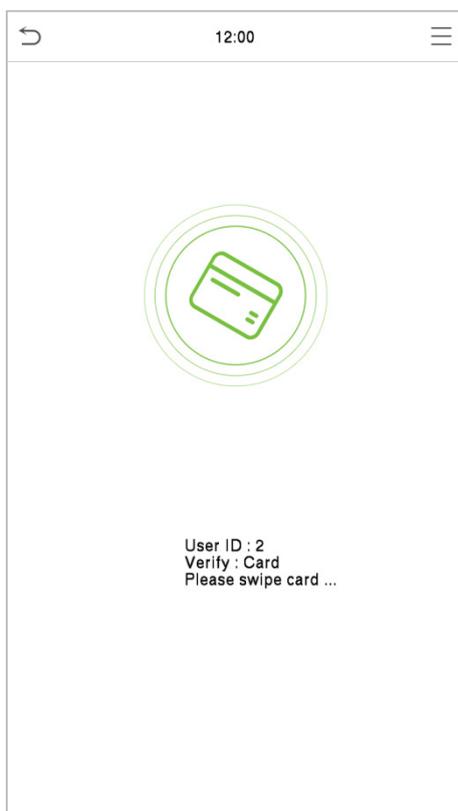
1. Введите идентификатор пользователя и нажмите [OK].



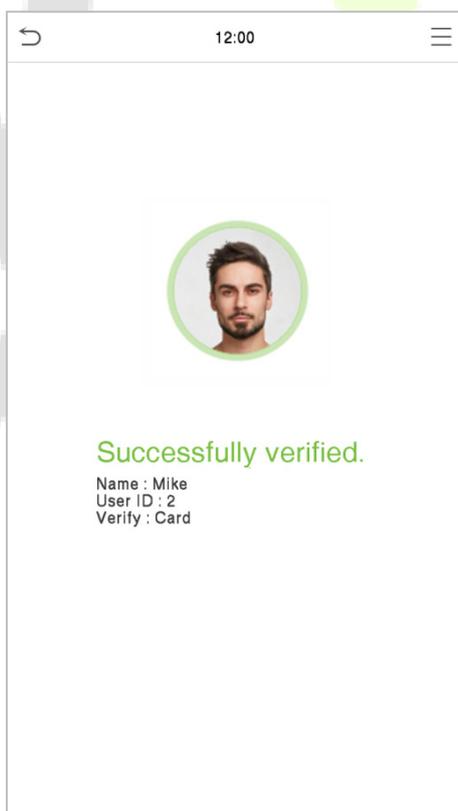
Если сотрудник регистрирует ладонь, лицо и пароль в дополнение к карте, а метод верификации установлен на Пароль / Пропуск / Лицо / Ладонь, появится экран ниже. Нажмите значок  , чтобы войти в режим верификации карты.



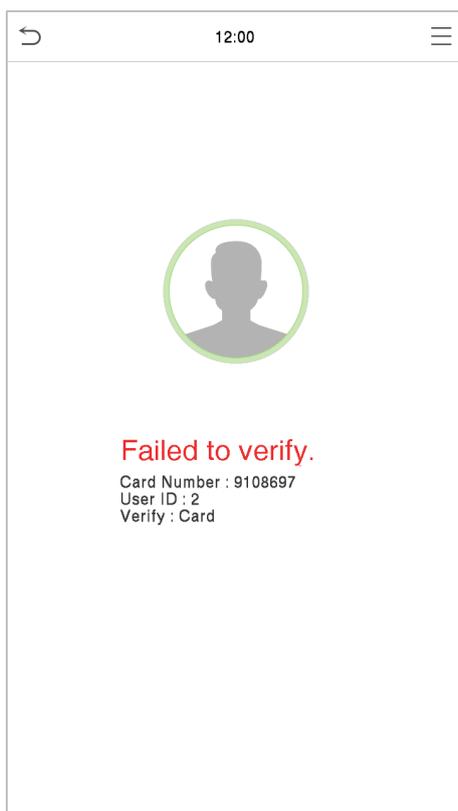
2. Просканируйте карту в зоне сканирования карты (сначала карта должна быть зарегистрирована).



Успешная верификация:



Неудавшаяся верификация:

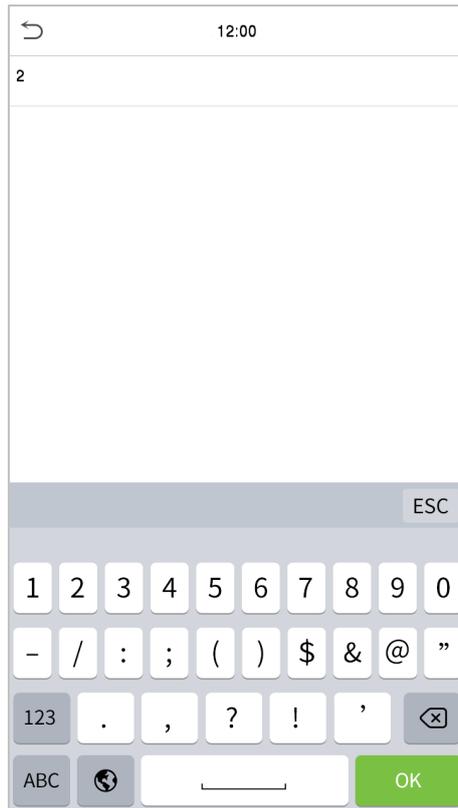


1.6.4 Верификация пароля

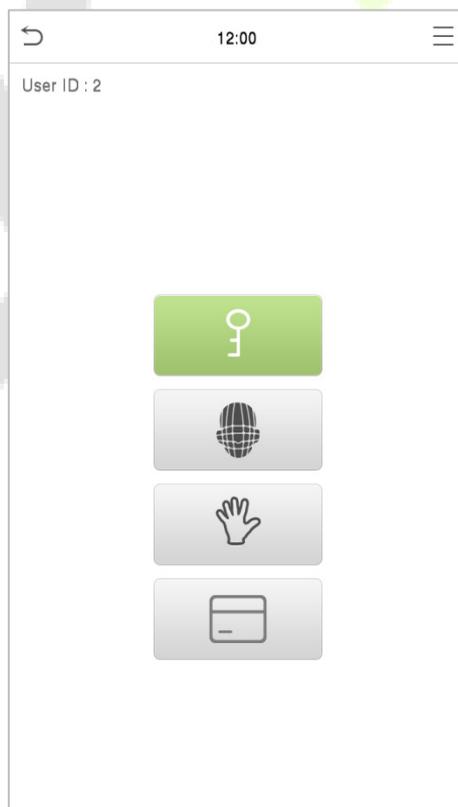
Режим верификации пароля сравнивает введенный пароль с идентификатором и паролем зарегистрированного пользователя.

Нажмите на кнопку  на главном экране, чтобы открыть режим верификации пароля 1:1.

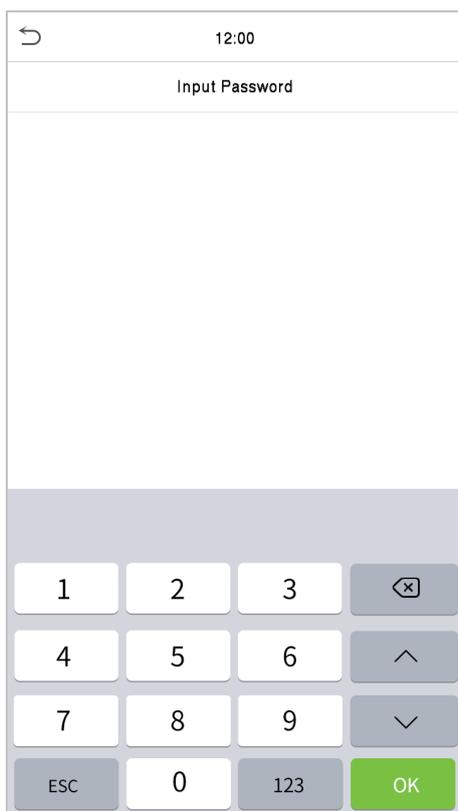
1. Введите идентификатор пользователя и нажмите [OK].



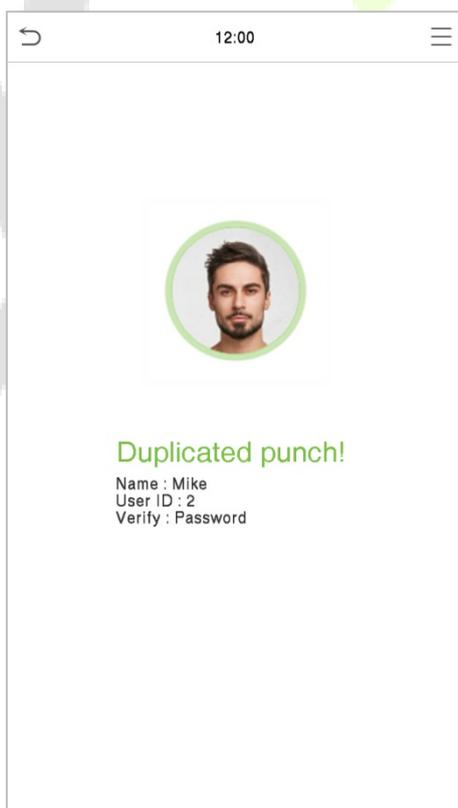
Если сотрудник регистрирует ладонь, карту и лицо в дополнение к паролю, а метод верификации установлен на Пароль / Карта / Лицо / Ладонь, появится экран ниже. Выберите значок  , чтобы войти в режим верификации пароля.



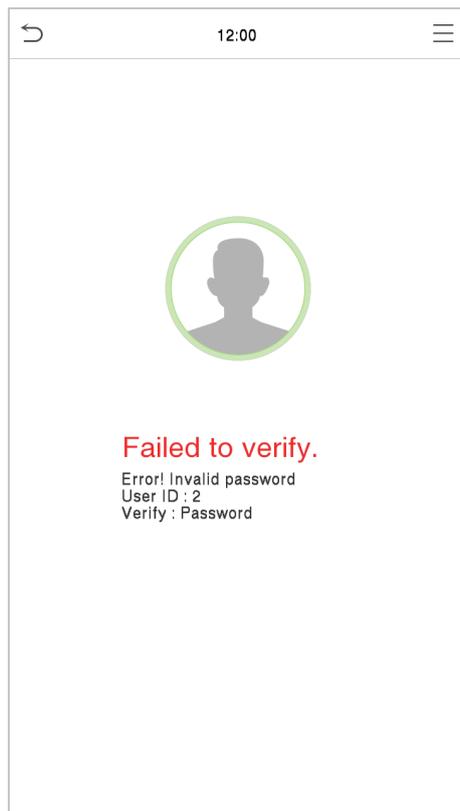
2. Введите пароль и нажмите [OK].



Успешная верификация:



Неудавшаяся верификация:



1.6.5 Комбинированная верификация

Для повышения безопасности это устройство предлагает возможность использования нескольких форм методов верификации. Всего можно использовать 12 различных комбинаций верификации, как показано ниже:

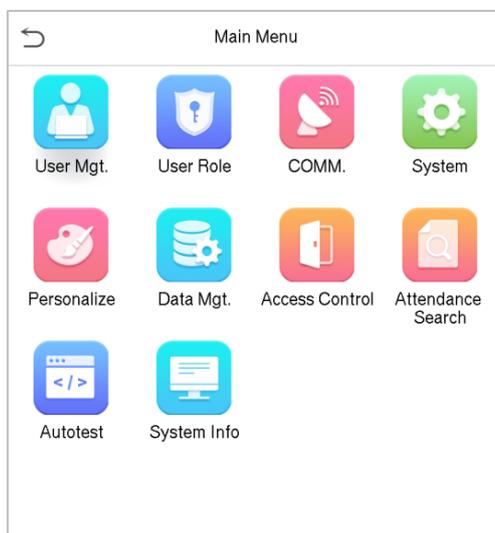
Verification Mode	
<input checked="" type="radio"/>	Password/Card/Face/Palm
<input type="radio"/>	User ID only
<input type="radio"/>	Password
<input type="radio"/>	Card only
<input type="radio"/>	Password+Card
<input type="radio"/>	Password/Card
<input type="radio"/>	Face only
<input type="radio"/>	Face+Password
<input type="radio"/>	Face+Card
<input type="radio"/>	Palm
<input type="radio"/>	Palm+Card
<input type="radio"/>	Palm+Face

Примечание:

- 1) «/» означает «или», а «+» означает «и».
- 2) Вы должны зарегистрировать необходимую информацию для верификации перед использованием режима комбинированной верификации, иначе верификация может не пройти. Например, если пользователь использует Регистрацию лица, но режим верификации - Лицо + Пароль, этот пользователь никогда не пройдет верификацию.

2 Главное меню

Нажмите  в начальном интерфейсе, чтобы войти в главное меню, как показано ниже:

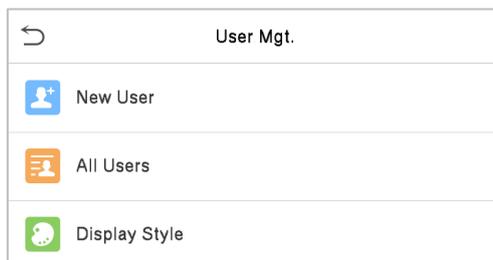


Меню	Описание
Управление пользователями	Для добавления, редактирования, просмотра и удаления основной информации о пользователе.
Роль пользователя	Для установки области разрешений роли пользователя, то есть для установки прав для работы с системой.
Связь	Для настройки соответствующих параметров сети, последовательной связи, подключения ПК, беспроводной сети, облачного сервера, Wiegand и сетевой диагностики.
Система	Для установки параметров, связанных с системой, включая дату и время, учет рабочего времени, шаблоны лиц, шаблоны ладоней, возврат к заводским настройкам, настройку типа устройства и управление обнаружением.
Персонализация	Включает в себя настройки пользовательского интерфейса, голоса и звонка.
Управление данными	Для удаления всех соответствующих данных в устройстве.
Контроль доступа	Для установки параметров замка и соответствующего устройства контроля доступа, включая такие параметры, как настройка правил времени, настройки праздничного дня, комбинированная верификация, настройка контроля повторного прохода и настройки параметров принуждения.
Поиск событий учета рабочего времени	Для запроса соответствующих журналов событий, проверки фотографий событий учета рабочего времени и фотографий черного списка.
Автоматическое тестирование	Для автоматического тестирования правильности работы каждого модуля, включая экран, звук, камеру и часы реального времени.
Информация о системе	Для просмотра информации об емкости данных, устройстве и прошивке данного устройства.

3 Управление пользователями

3.1 Добавить пользователей

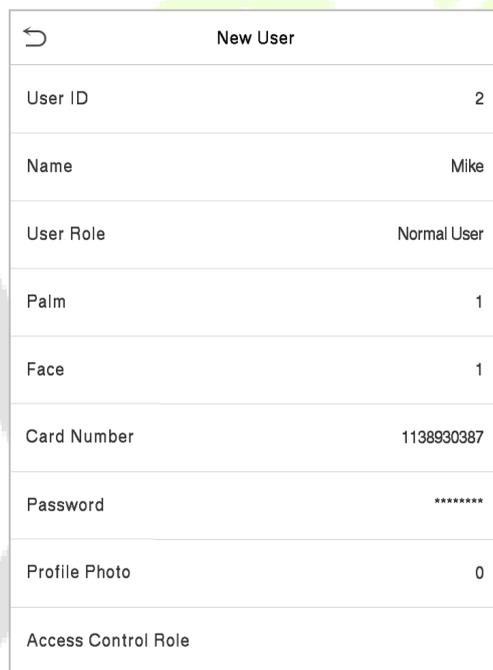
Нажмите «**Управление пользователями**» в главном меню.



Нажмите «**Новый пользователь**».

Зарегистрировать идентификатор и имя пользователя

Введите идентификатор и имя пользователя.



Примечания:

- 1) Имя пользователя может содержать 17 символов.
- 2) По умолчанию идентификатор пользователя может содержать от 1 до 9 цифр.
- 3) Во время начальной регистрации можно изменить свой идентификатор, который не может быть изменен после регистрации.
- 4) Если появляется сообщение «Повторяющийся идентификатор», необходимо выбрать другой идентификатор.

Установка роли пользователя

Существует два типа учетных записей пользователей: **Обычный пользователь** и **Суперадминистратор**. Если уже есть зарегистрированный администратор, обычные пользователи не имеют прав на управление системой и могут получить доступ только к верификациям аутентификации. Администратору принадлежат все права на управление. Если установлена настраиваемая роль, вы также можете выбрать для пользователя разрешения **определяемой пользователем роли**.

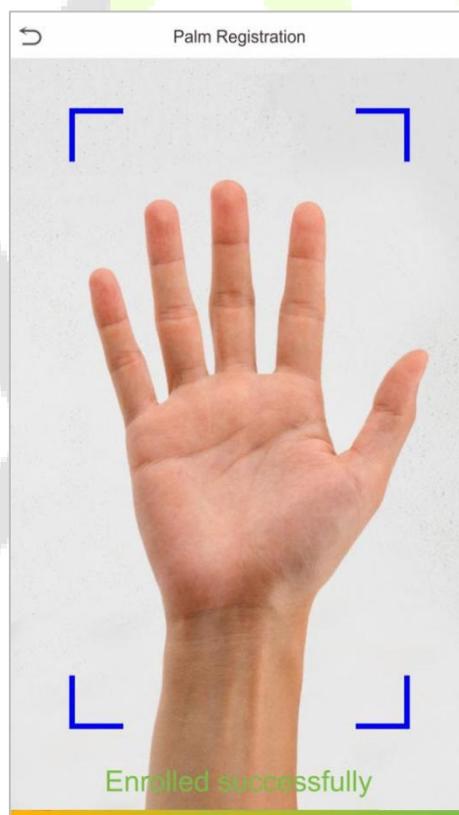
Нажмите **«Роль пользователя»**, чтобы выбрать обычного пользователя или суперадминистратора.



Примечание: если выбранная роль пользователя - суперадминистратор, пользователь должен пройти аутентификацию идентификационных данных, чтобы получить доступ к главному меню.

Зарегистрировать ладонь

Нажмите **«Ладонь»**, чтобы открыть страницу регистрации ладони. Выберите ладонь для регистрации.



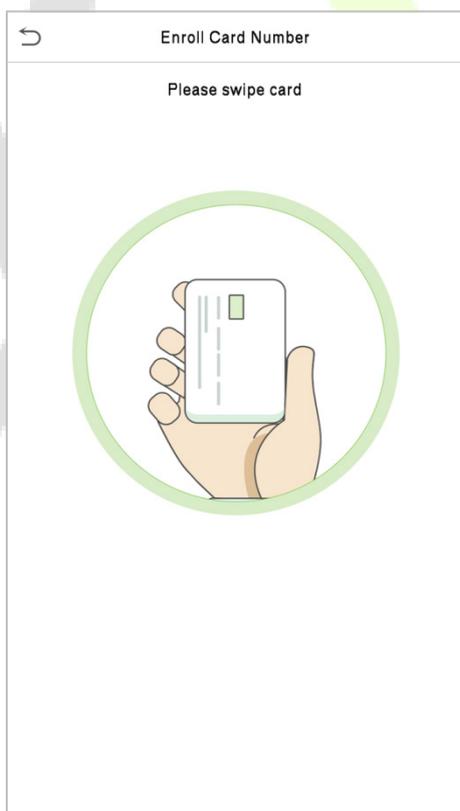
Зарегистрировать лицо

Нажмите **«Лицо»**, чтобы перейти на страницу регистрации лица. Пожалуйста, смотрите в камеру и оставайтесь неподвижными во время регистрации лица. Интерфейс регистрации выглядит следующим образом:



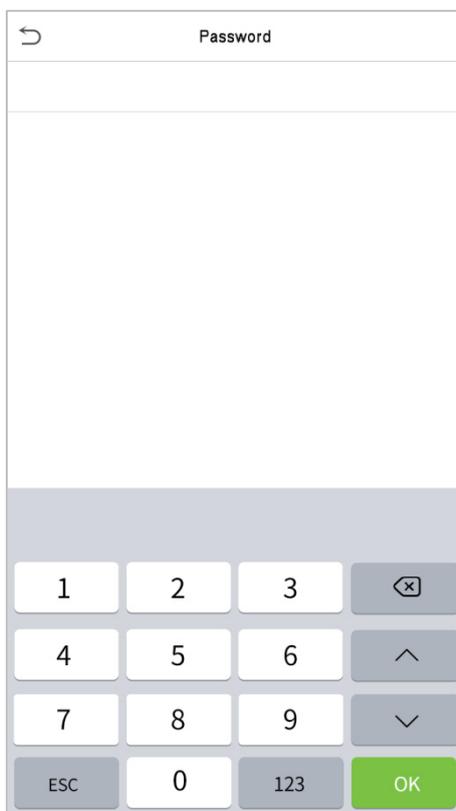
Зарегистрировать карту

Приложите свою **карту** в зоне сканирования карты. Регистрация номера карты будет успешной.



Зарегистрировать пароль

Нажмите **«Пароль»**, чтобы открыть страницу регистрации пароля. Введите пароль и введите его еще раз. Нажмите ОК. Если два введенных пароля различаются, появится подсказка «Пароль не совпадает».



Примечание: по умолчанию пароль может содержать от одной до восьми цифр.

Зарегистрировать фотографию пользователя

После успешной верификации зарегистрированного с фотографией пользователя, отображается зарегистрированная фотография.

Нажмите **«Фотография пользователя»**; нажмите значок камеры, чтобы сделать фотографию. После фотографирования система вернется к интерфейсу нового пользователя.

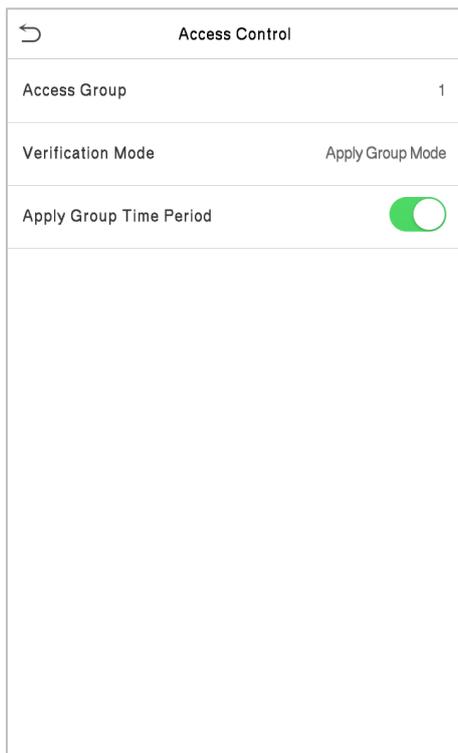
Примечание: при регистрации лица система автоматически назначит сделанную фотографию фотографией пользователя. Если вы не хотите регистрировать фотографию пользователя, система автоматически установит сделанную фотографию как фотографию по умолчанию.

Роль контроля доступа

Контроль доступа пользователей устанавливает права разблокировки дверей для каждого человека, включая группу и период времени, к которым относится пользователь.

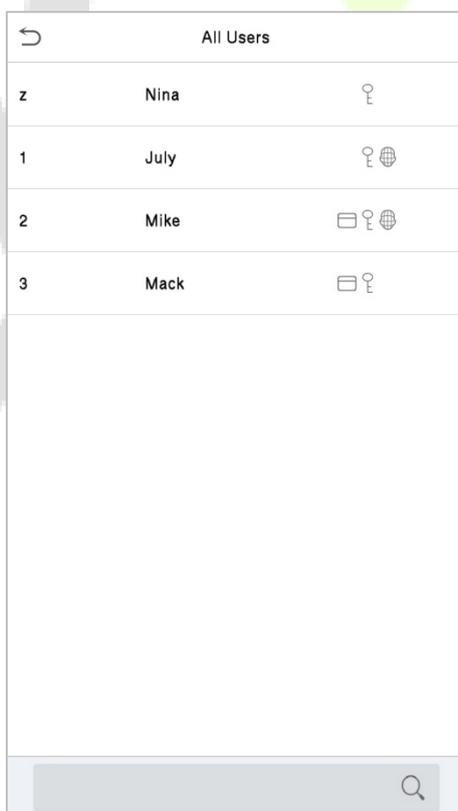
Нажмите **Роль контроля доступа > Группа доступа**, назначьте зарегистрированных пользователей в разные группы для лучшего управления. Новые пользователи по умолчанию принадлежат к Группе 1 и могут быть переназначены в другие группы. Устройство поддерживает до 99 групп контроля доступа.

Нажмите **«Режим верификации»**, выберите режим верификации, который нужно использовать.



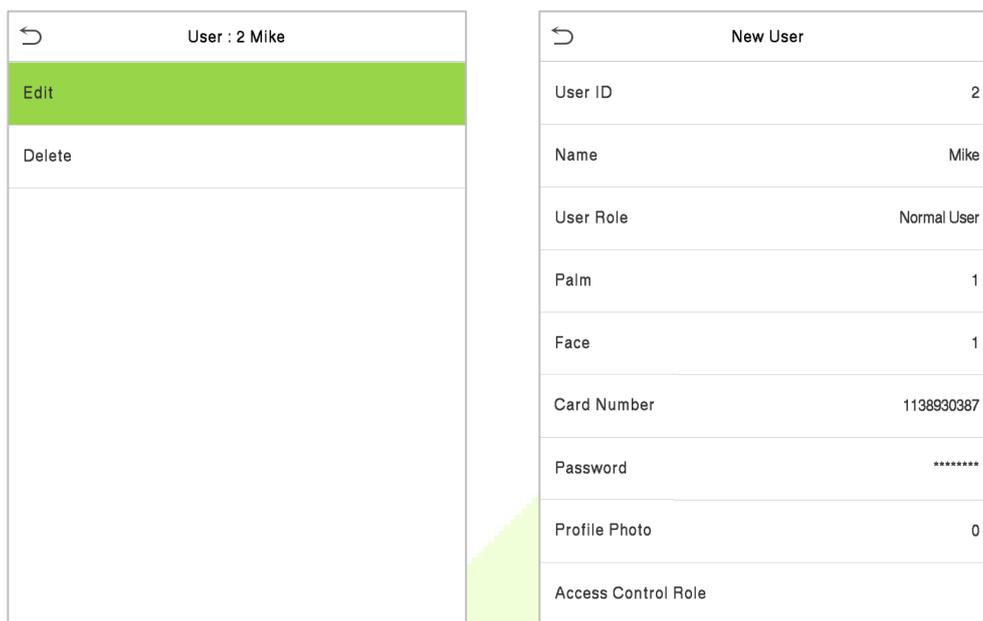
3.2 Поиск пользователей

Нажмите строку поиска в списке пользователей и введите ключевое слово для поиска (ключевое слово может быть идентификатором, фамилией или полным именем). Система будет искать пользователей, имеющих отношение к информации.



3.3 Редактировать пользователей

Выберите пользователя из списка и нажмите «**Редактировать**», чтобы открыть интерфейс редактирования пользователя.

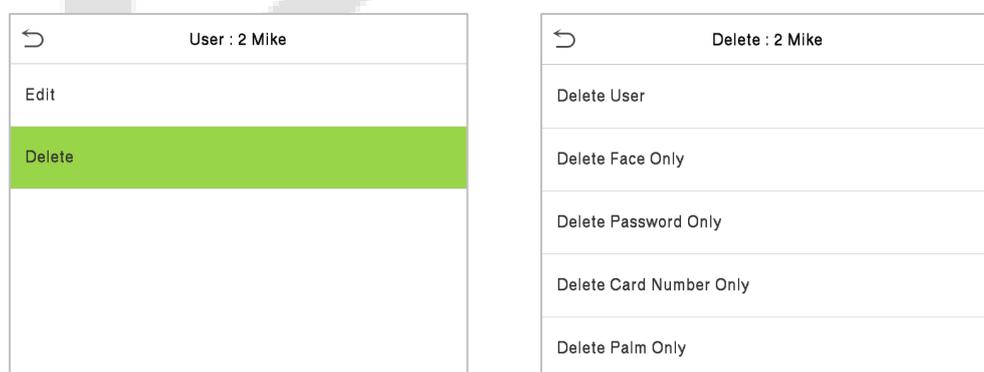


Примечание: операция редактирования пользователя такая же, как и операция добавления пользователя, за исключением того, что идентификатор пользователя не может быть изменен при редактировании пользователя. Для подробной информации см. «[3.1 Добавить пользователей](#)».

3.4 Удалить пользователей

Выберите пользователя из списка и нажмите «**Удалить**», чтобы войти в пользовательский интерфейс удаления. Выберите информацию о пользователе, которую нужно удалить, и нажмите **ОК**.

Примечание: если вы выберете «**Удалить пользователя**», вся информация о пользователе будет удалена.



3.5 Стиль отображения

В главном меню нажмите «**Управление пользователями**», а затем нажмите «**Стиль отображения**», чтобы войти в интерфейс настройки стиля отображения.

Display Style	
<input checked="" type="radio"/>	Single Line
<input type="radio"/>	Multiple Line
<input type="radio"/>	Mixed Line

Все стили отображения показаны ниже:

All Users		
z	Nina	👤
1	July	👤🌐
2	Mike	📄👤🌐
3	Mack	📄👤

Однострочный

All Users		
z		Nina
	👤	
1		July
	👤🌐	
2		Mike
	📄🌐	
3		Mack
	📄👤	

Многострочный

All Users		
z		👤
	Nina	
1		👤🌐
	July	
2		📄👤🌐
	Mike	
3		📄👤
	Mack	

Смешанная линия

4 Роль пользователя

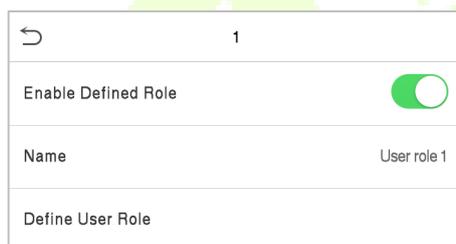
Если необходимо назначить определенные разрешения для определенных пользователей, можно отредактировать «Определенную пользователем роль» в меню **«Роль пользователя»**.

Можно установить область разрешений для настраиваемой роли (до 3 ролей), то есть область разрешений в меню операций.

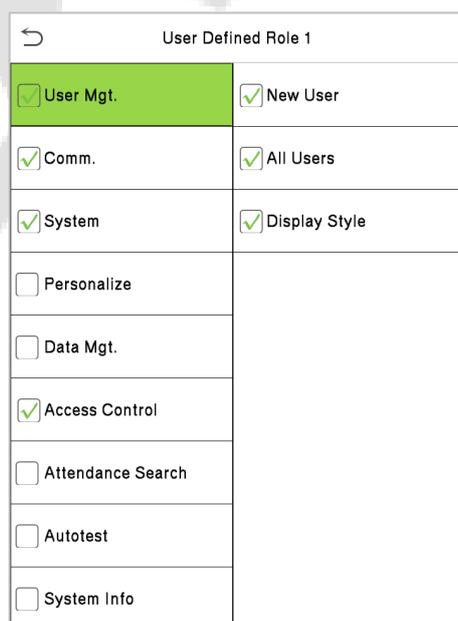
Нажмите **«Роль пользователя»** в интерфейсе главного меню.



1. Нажмите любую роль, чтобы установить определенную роль. Нажмите кнопку **«Включить определенную роль»**, чтобы включить эту определенную роль. Нажмите **«Имя»** и введите имя роли.



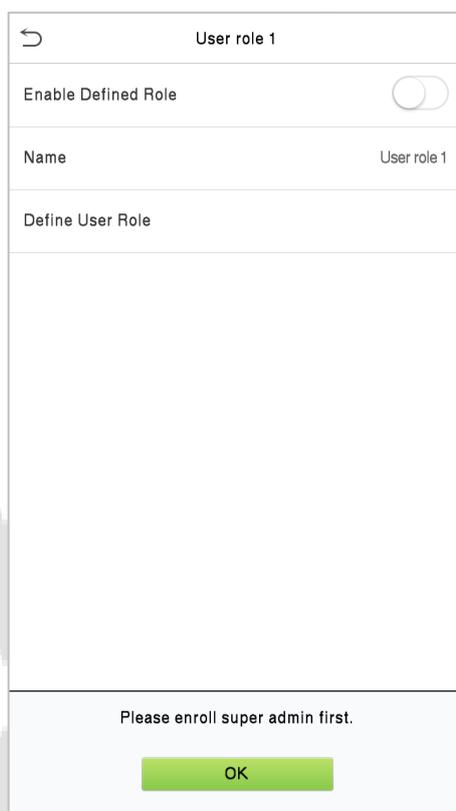
2. Нажмите **«Определить роль пользователя»**, чтобы назначить права роли. После назначения прав нажмите **«Возврат»**.



Примечание: во время назначения прав главное меню находится слева, а его подменю - справа. Нужно только выбрать функции в подменю. Если в устройстве включена роль, можно назначить роли, которые установлены пользователям, нажав **Управление пользователями > Новый пользователь > Роль пользователя.**



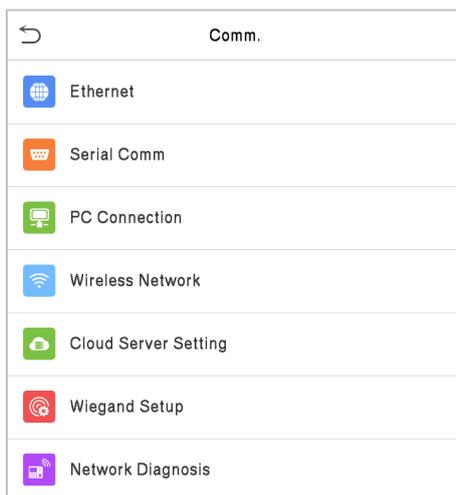
Если суперадминистратор не зарегистрирован, устройство предложит: «Сначала зарегистрируйте суперадминистратора!» после нажатия панели включения, как показано ниже.



5 Настройки связи

Параметры связи используются для настройки параметров сети, последовательной связи, подключения ПК, беспроводной сети, облачного сервера, Wiegand и сетевой диагностики.

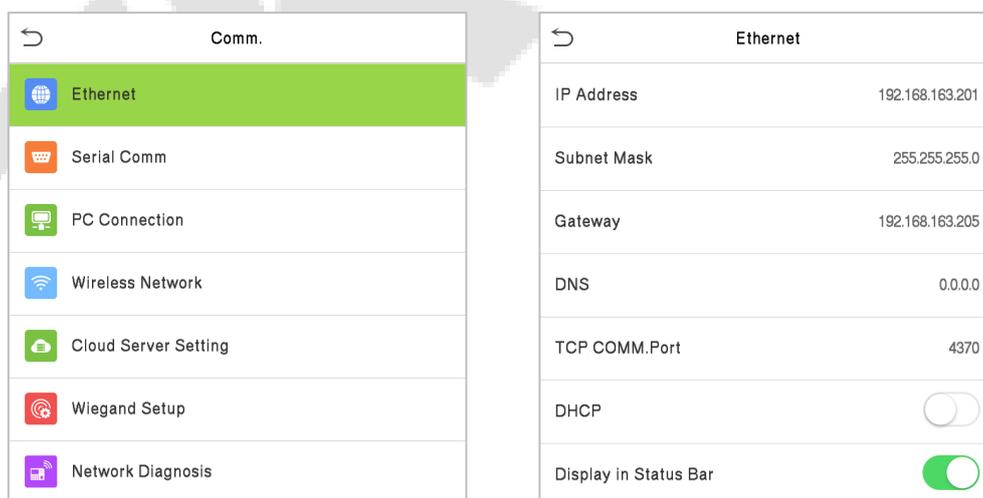
Нажмите «**Связь**» в главном меню.



5.1 Сетевые настройки

Когда устройству необходимо обмениваться данными с ПК через Ethernet, необходимо настроить параметры сети и убедиться, что устройство и ПК подключаются к одному и тому же сегменту сети.

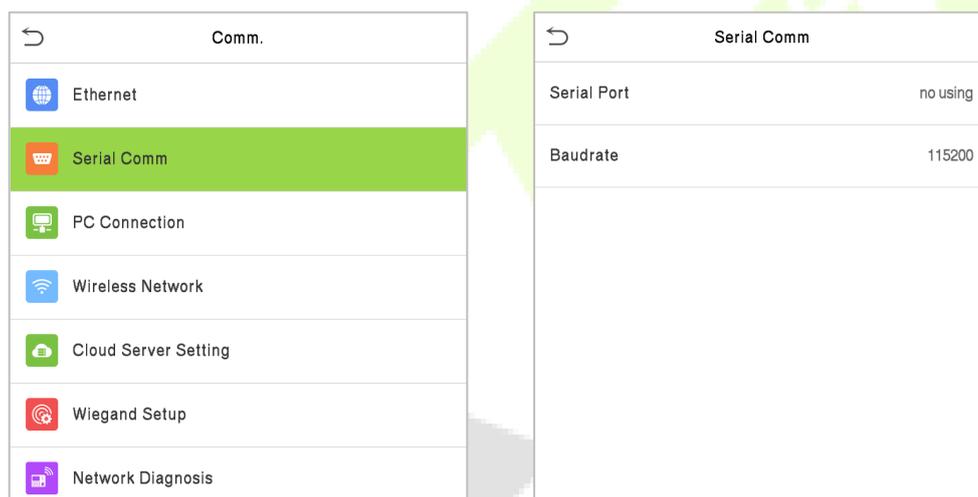
Нажмите «**Ethernet**» в интерфейсе настроек связи.



Меню	Описание
IP-адрес	Заводское значение по умолчанию - 192.168.1.201. Установите IP-адрес в соответствии с требованиями.
Маска подсети	Заводское значение по умолчанию - 255.255.255.0. Установите значение в соответствии с требованиями.

Шлюз	Заводской адрес по умолчанию - 0.0.0.0. Установите значение в соответствии с требованиями.
DNS	Заводской адрес по умолчанию - 0.0.0.0. Установите значение в соответствии с требованиями.
Порт TCP-связи	Заводское значение по умолчанию - 4370. Установите значение в соответствии с требованиями.
DHCP	Протокол динамической конфигурации хоста, который предназначен для динамического распределения IP-адресов для клиентов через сервер.
Отображение в строке состояния	Для отображения значка сети в строке состояния.

5.2 Последовательная связь



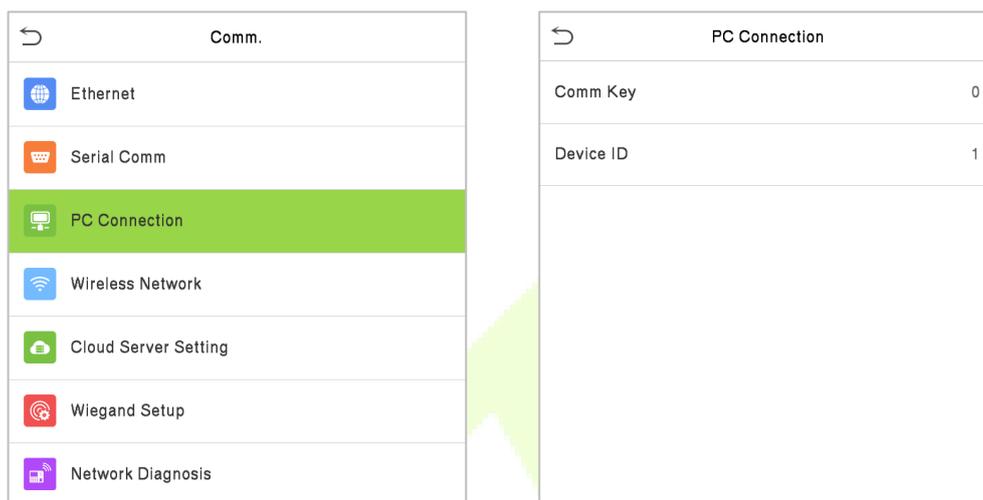
Меню	Описание
Последовательный порт	Включая отсутствие использования, RS232 (ПК) и RS485 (ПК), выберите RS232 (ПК) для связи с устройством через последовательный порт RS232. Выберите RS485 (ПК) для связи с устройством через последовательный порт RS485.
Скорость передачи данных	Скорость связи с ПК; существует 5 вариантов скорости передачи данных: 115200 (по умолчанию), 57600, 38400, 19200 и 9600. Чем выше скорость передачи, тем выше скорость передачи данных, но также менее надежна. Как правило, на коротком расстоянии связи может использоваться более высокая скорость передачи данных; на большом расстоянии связи выбор более низкой скорости передачи будет более надежным.

5.3 Подключение ПК

Для повышения безопасности данных установите **Ключ связи** для связи между устройством и ПК.

Если установлен ключ связи, этот пароль для подключения необходимо ввести до подключения устройства к программному обеспечению ПК.

Выберите «**Подключение ПК**» в интерфейсе настроек связи.

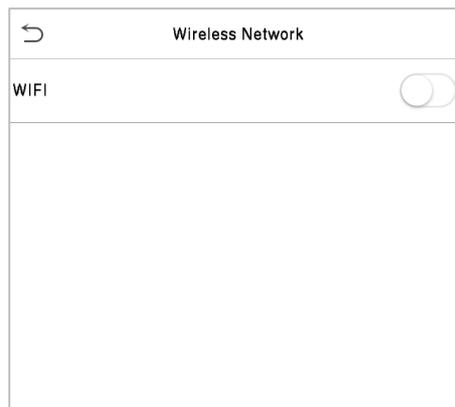
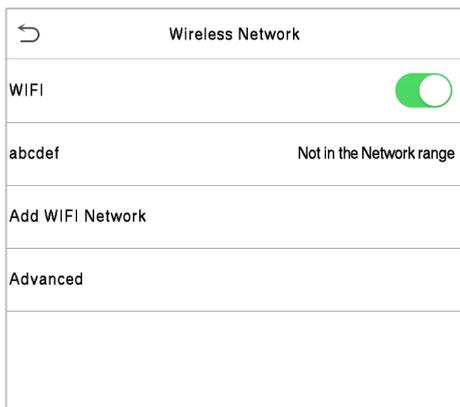


Меню	Описание
Ключ связи	Ключ связи: пароль по умолчанию - 0, который можно изменить. Ключ связи может содержать от 1 до 6 цифр.
Идентификатор устройства	Идентификационный номер устройства в диапазоне от 1 до 254. Если используется метод связи RS232/RS485, необходимо ввести этот идентификатор устройства в интерфейс связи программного обеспечения.

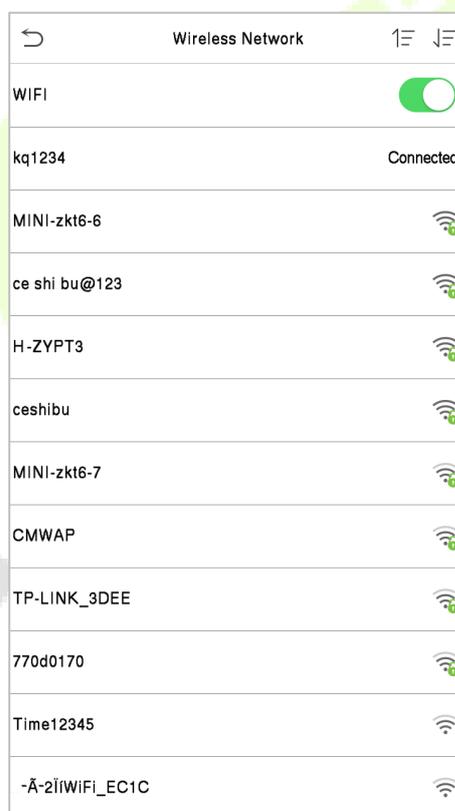
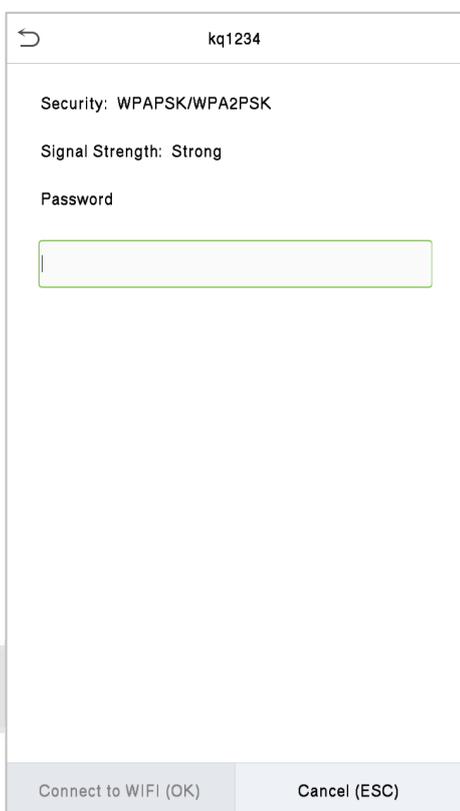
5.3 Беспроводная сеть

Wi-Fi - это сокращение от Wireless Fidelity. Устройство имеет модуль Wi-Fi, который может быть встроен в форму устройства или подключен к внешнему устройству, чтобы обеспечить передачу данных через Wi-Fi и установить беспроводную сетевую среду.

По умолчанию в системе включен Wi-Fi. Если сеть Wi-Fi использовать не требуется, можно нажать кнопку , чтобы отключить Wi-Fi.



Когда Wi-Fi включен, нажмите поисковую сеть. Нажмите текстовое поле для ввода пароля, чтобы ввести пароль, и нажмите **Подключиться к Wi-Fi (ОК)**.

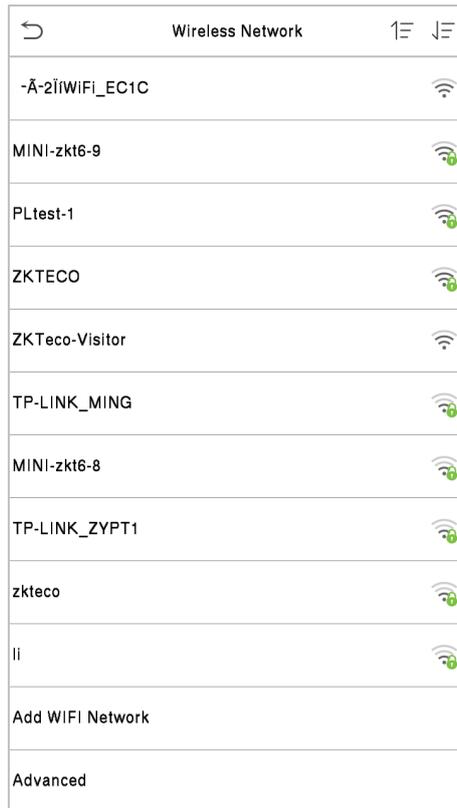


Соединение установлено успешно, состояние отображается на панели значков.

Добавить сеть Wi-Fi

Если нужной сети Wi-Fi нет в списке, можно добавить сеть Wi-Fi вручную.

Нажмите «**Страница вниз**» и «**Добавить сеть Wi-Fi**».



Введите параметры сети Wi-Fi. (Добавленная сеть должна существовать.)

Add WIFI Network	
SSID	
Network Mode	INFRA
Auth. Mode	OPEN

После добавления найдите добавленную сеть Wi-Fi в списке и подключитесь к сети указанным выше способом.

Расширенные параметры

Используется для настройки параметров сети Wi-Fi.

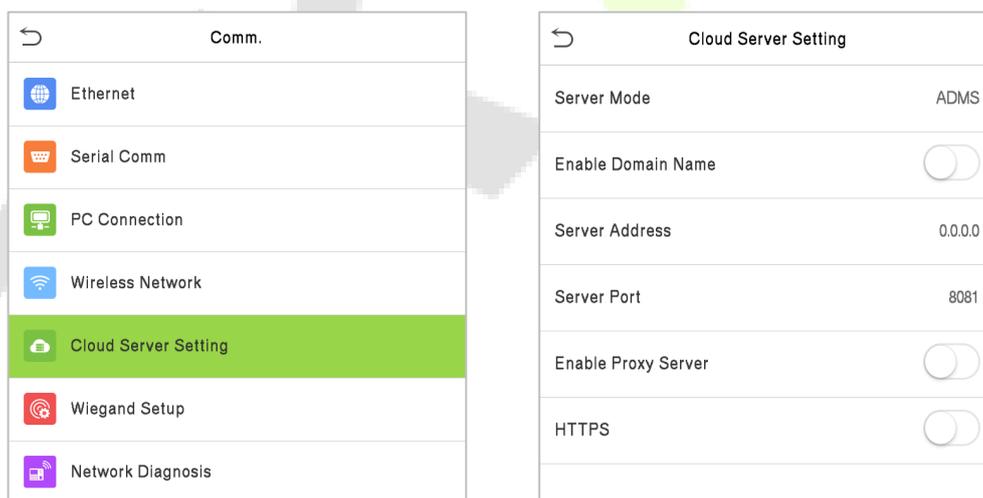
Ethernet	
DHCP	<input checked="" type="checkbox"/>
IP Address	192.168.11.113
Subnet Mask	255.255.255.0
Gateway	192.168.11.1

Меню	Описание
DHCP	Сокращение от протокола динамической конфигурации хоста, который включает в себя распределение динамических IP-адресов для сетевых клиентов.
IP-адрес	IP-адрес сети Wi-Fi.
Маска подсети	Маска подсети сети Wi-Fi.
Шлюз	Адрес шлюза сети Wi-Fi.

5.4 Настройка облачного сервера

Это настройки, используемые для подключения к серверу ADMS.

Нажмите **«Настройка облачного сервиса»** в интерфейсе настроек связи.



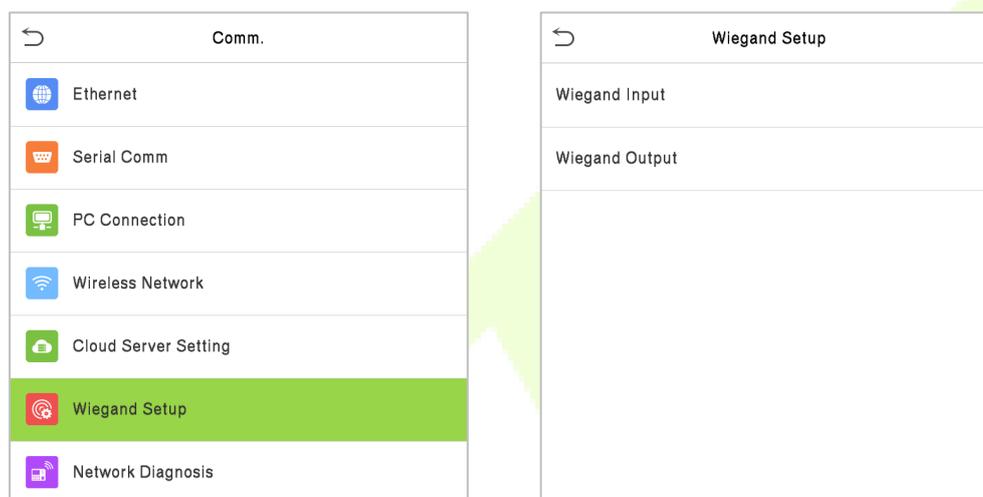
Menu	Description	
Включить доменное имя	Адрес сервера	Когда эта функция включена, будет использоваться режим имени домена «http://...», например http://www.XYZ.com, а «XYZ» обозначает имя домена, когда этот режим включен.
Отключить доменное имя	Адрес сервера	IP-адрес сервера ADMS.
	Порт сервера	Порт, используемый сервером ADMS.

Включить прокси-сервер	Когда вы решите включить прокси, необходимо установить IP-адрес и номер порта прокси-сервера.
HTTPS	Шифрование передачи и идентификация личности на основе HTTP обеспечивают безопасность процесса передачи.

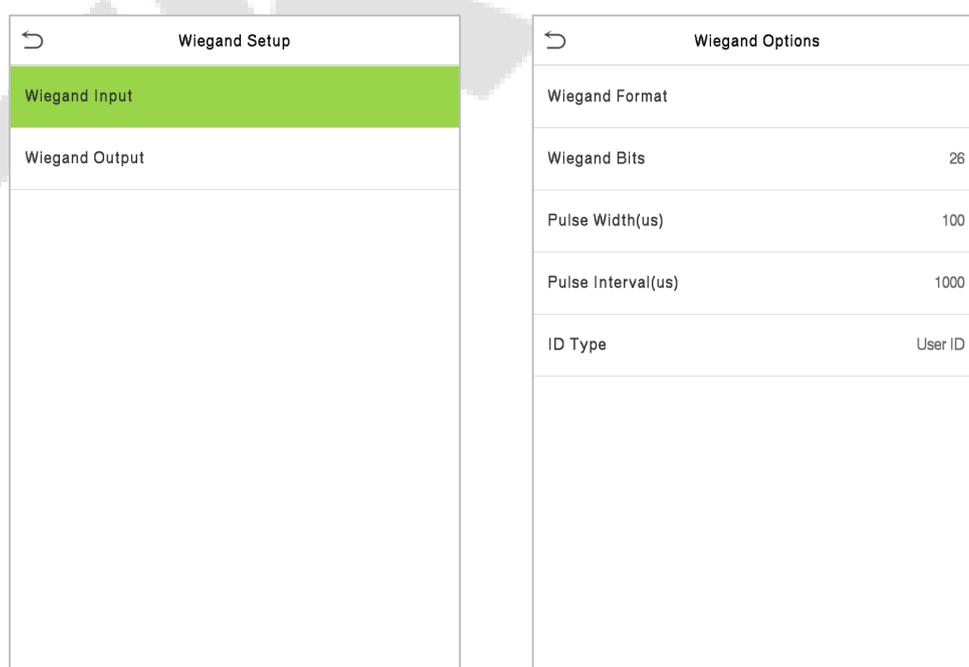
5.6 Установка Wiegand

Меню используется для установки входных и выходных параметров Wiegand.

Нажмите «**Установка Wiegand**» в интерфейсе настроек связи.



Входной параметр Wiegand



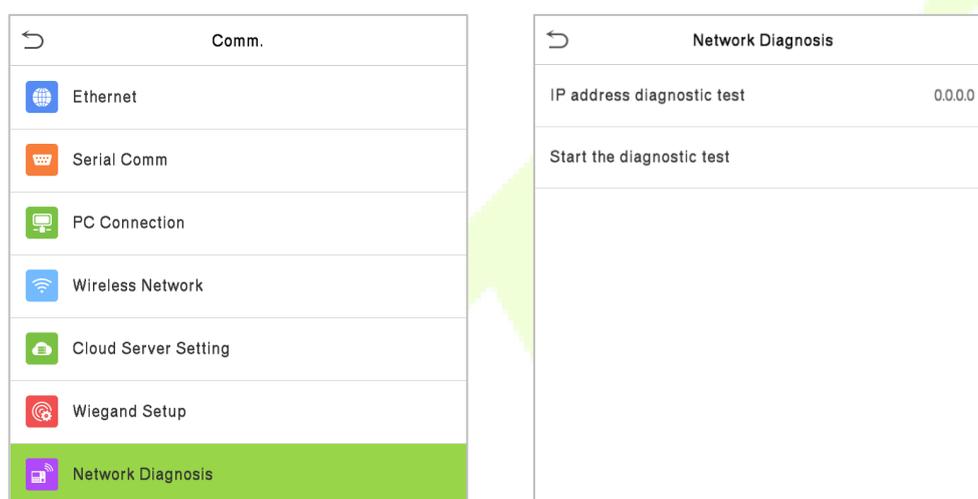
Меню	Описание
Формат Wiegand	Диапазон значений: 26, 34, 36, 37 и 50 бит.
Wiegand в битах	Число бит данных Wiegand.
Ширина импульса (мкс)	Значение ширины импульса, отправляемое Wiegand по умолчанию, составляет 100 микросекунд, и его можно регулировать в диапазоне от 20 до 100 микросекунд.
Интервал импульса (мкс)	Значение по умолчанию составляет 1000 микросекунд, которое можно регулировать в диапазоне от 200 до 20000 микросекунд.
Тип идентификатора	Выберите между идентификатором пользователя и номером карты.

Описание различных общих форматов Wiegand:

Формат Wiegand	Описание
Wiegand26	<p>ЕСССССССССССССССССССССССССССССССССС</p> <p>Состоит из 26 бит двоичного кода, причем 1-й бит является битом четности для 2-13-го битов, 26-й бит является битом нечетности для 14-25-го битов, а 2-25-й биты являются номерами карт.</p>
Wiegand26a	<p>ЕСССССССССССССССССССССССССССССССС</p> <p>Состоит из 26 бит двоичного кода. 1-й бит - это бит четности со 2-го по 13-й бит, а 26-й бит - это бит нечетности с 14-го по 25-й бит. Биты со 2-го по 9-й - это коды сайта, а биты с 10-го по 25-й - это номера карт.</p>
Wiegand34	<p>ЕСССССССССССССССССССССССССССССССССС</p> <p>Состоит из 34 бит двоичного кода. 1-й бит - это бит четности со 2-го по 17-й бит, а 34-й бит - это бит нечетности с 18-го по 33-й бит. Со 2-го по 25-й биты - это номера карт.</p>
Wiegand34a	<p>ЕСССССССССССССССССССССССССССССССССС</p> <p>Состоит из 34 бит двоичного кода, причем 1-й бит является битом четности для 2-17-го битов, 34-й бит является битом нечетности для 18-33-го битов, 2-9-ый биты являются кодами сайтов, а 10-25-й биты являются номерами карт.</p>
Wiegand36	<p>ОFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF</p> <p>Состоит из 36 бит двоичного кода. 1-й бит является битом нечетности от 2-го до 18-го битов, а 36-й бит является битом четности от 19-го до 35-го битов. 2-17-й бит - это коды устройств, 18-33-й - номера карт, а 34-35-й - коды производителей.</p>
Wiegand36a	<p>ЕFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF</p> <p>Состоит из 36 бит двоичного кода. 1-й бит является битом четности от 2-го до 18-го битов, а 36-й бит является битом нечетности от 19-го до 35-го битов. 2-19-й бит - это коды устройств, а 20-35-й - номера карт.</p>

Код сайта	Похоже на идентификатор устройства. Разница в том, что код сайта может быть установлен вручную, и это повторяется в другом устройстве. Допустимое значение от 0 до 256 по умолчанию.
Ширина импульса (мкс)	Ширина времени представляет изменения количества электрического заряда с изменением высокочастотной емкости регулярно в течение указанного времени.
Интервал импульса (мкс)	Интервал времени между импульсами.
Тип идентификатора	Выберите между идентификатором пользователя и номером карты.

5.7 Сетевая диагностика

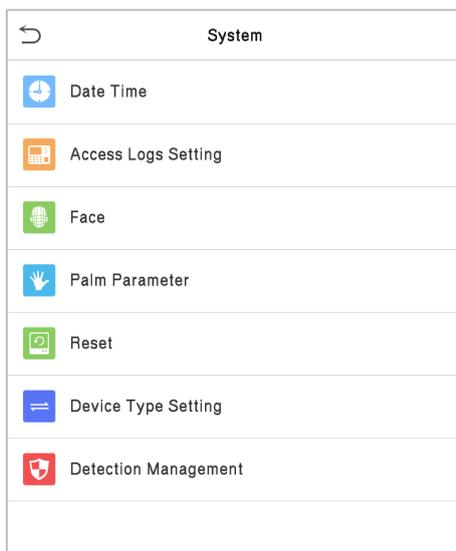


Меню	Описание
Диагностический тест IP-адреса	Заводской адрес по умолчанию - 0.0.0.0. Установите значение в соответствии с требованиями.
Начать диагностический тест	Нажмите «Старт» для автоматической диагностики сети.

6 Настройки системы

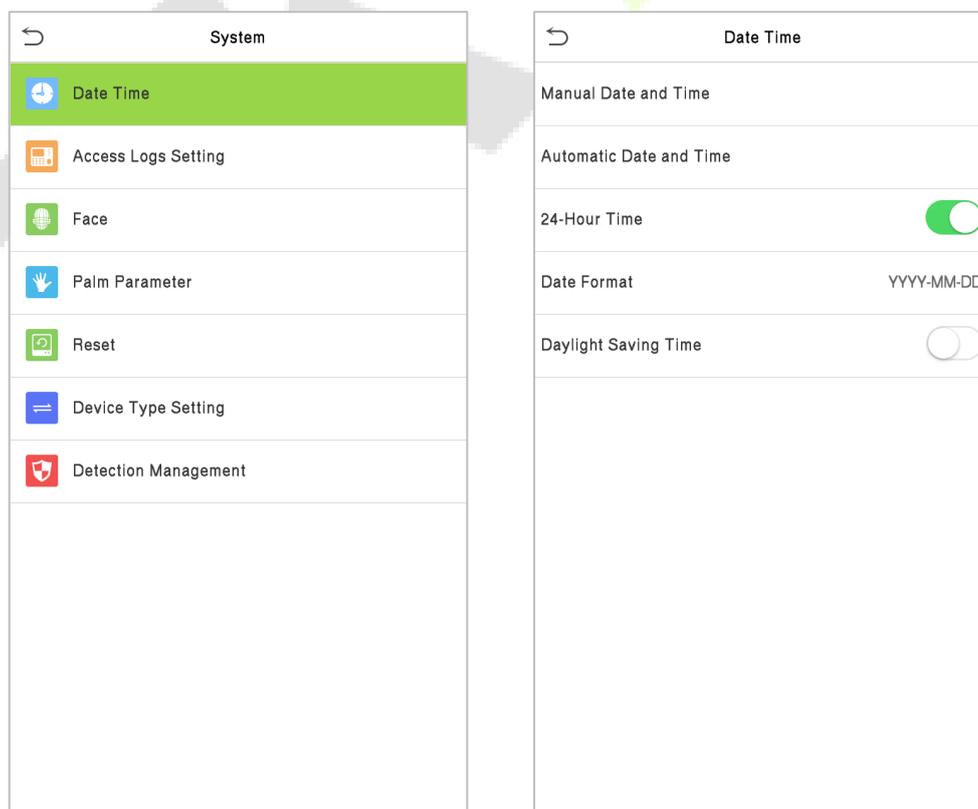
Настройки системы используются для установки соответствующих системных параметров в целях оптимизации рабочих характеристик устройства.

Нажмите **«Система»** в интерфейсе главного меню.



6.1 Дата и время

Нажмите **«Дата и время»** в интерфейсе системы.



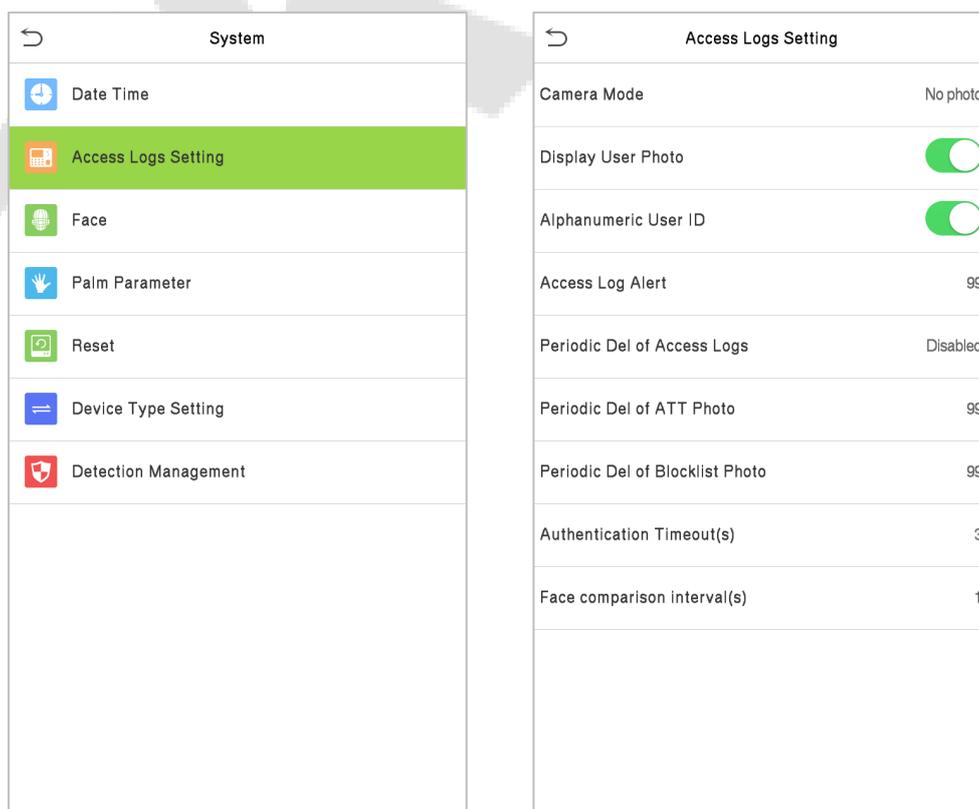
Меню	Описание
Дата и время вручную	Установите данные и время вручную, а затем нажмите «Подтвердить» для сохранения.
Автоматическая дата и время	Автоматически определять время и дату в главном интерфейсе. Необходимо установить адрес NTP-сервера, автоматически определить время и дату, а также выбрать период разрешенного доступа для вступления в силу.
24-часовое время	Включите или отключите этот формат. Если этот параметр включен, выберите формат даты, чтобы установить формат даты, т.е. способ отображения даты на устройстве.
Формат даты	Выберите формат отображения даты.
Летнее время	Нажмите «Летнее время», чтобы включить или отключить функцию. Если этот параметр включен, нажмите «Летнее время» , чтобы выбрать летнее время, а затем нажмите «Настройка летнего времени» , чтобы установить время перехода.

При восстановлении заводских настроек время (24 часа) и формат даты (ГГГГ-ММ-ДД) можно восстановить, но дату и время устройства восстановить нельзя.

Примечание: например, пользователь устанавливает время устройства (18:35, 15 марта 2020 г.) на 18:30, 1 января 2021 г. После восстановления заводских настроек время устройства изменится на 18:30, 1 января 2021 г.

6.2 Параметры учета рабочего времени

Нажмите **«Учет рабочего времени»** в интерфейсе системы..



Функция	Описание
Режим камеры	<p>Выберите, следует ли делать фотографию и сохранять текущую фотографию во время верификации. Присутствует 5 режимов:</p> <p>Фотография отсутствует: во время верификации пользователя фотография не делается.</p> <p>Сфотографировать без сохранения: во время верификации фотография сделана, но не сохраняется.</p> <p>Сфотографировать и сохранить: во время верификации фотография сделана и сохранена.</p> <p>Сохранить при успешной верификации: фотография делается и сохраняется для каждой успешной верификации.</p> <p>Сохранить при неудачной верификации: фотография делается и сохраняется при каждой неудачной верификации.</p>
Отображать фотографию пользователя	Выберите, следует ли отображать фотографию пользователя, когда пользователь проходит верификацию.
Буквенно-цифровой идентификатор пользователя	Поддерживать ли буквы в идентификаторе сотрудника.
Предупреждение журналов доступа	Когда емкость записи достигает установленного значения, устройство автоматически отображает предупреждение. Пользователи могут отключить функцию или установить допустимое значение от 1 до 9999.
Периодическое удаление записей доступа	Когда записи доступа достигнут полной емкости, устройство автоматически удалит установленное значение старых записей доступа. Пользователи могут отключить функцию или установить допустимое значение от 1 до 999.
Периодическое удаление фотографий УРВ	Когда фотографии учета рабочего времени (УРВ) достигнут полной емкости, устройство автоматически удалит установленное значение старых фотографий УРВ. Пользователи могут отключить функцию или установить допустимое значение от 1 до 99.
Периодическое удаление фотографий черного списка	Когда блокировка перечисленных фотографий достигает максимальной емкости, устройство автоматически удаляет набор старых заблокированных фотографий. Пользователи могут отключить функцию или установить допустимое значение от 1 до 99.
Время ожидания аутентификации (сек)	Время, необходимое для отображения сообщения об успешной верификации. Допустимое значение: от 1 до 9 секунд..
Интервал сравнения лиц (сек)	После нажатия (выбора) интервала идентификации, например, если интервал сравнения установлен на 5 секунд, то распознавание лица будет проверять лицо каждые 5 секунд. Допустимое значение: от 0 до 9 секунд. 0 означает непрерывную идентификацию, от 1 до 9 означает идентификацию через определенные промежутки времени.

6.3 Параметры лица

Нажмите «**Лицо**» в итерфейсе системы.

Параметр	Значение
1:N Threshold Value	70
1:N Match Threshold for Masked People	68
1:1 Threshold Value	70
Face Enrollment Threshold	70
Face Pitch Angle	35
Face Rotation Angle	25
Image Quality	40
Minimum Face Size	80
LED Light Trigger Value	80
Motion Detection Sensitivity	4
Live Detection	<input checked="" type="checkbox"/>
Live Detection Threshold	55
Anti-spoofing using NIR	<input checked="" type="checkbox"/>
Binocular Live Detection Threshold	50
WDR	<input type="checkbox"/>
Anti-flicker Mode	50HZ
Face Algorithm	

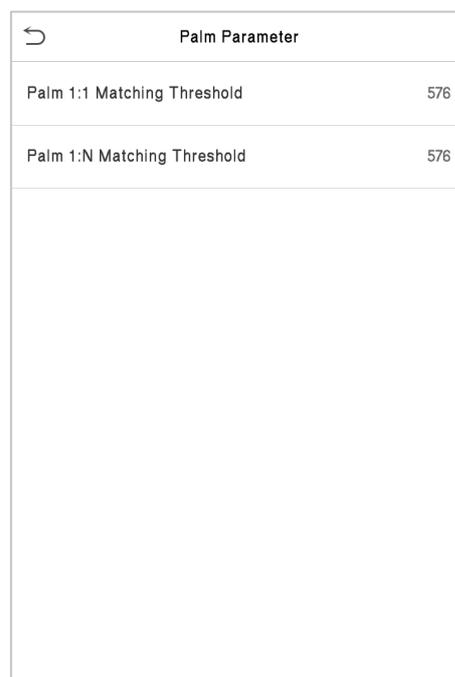
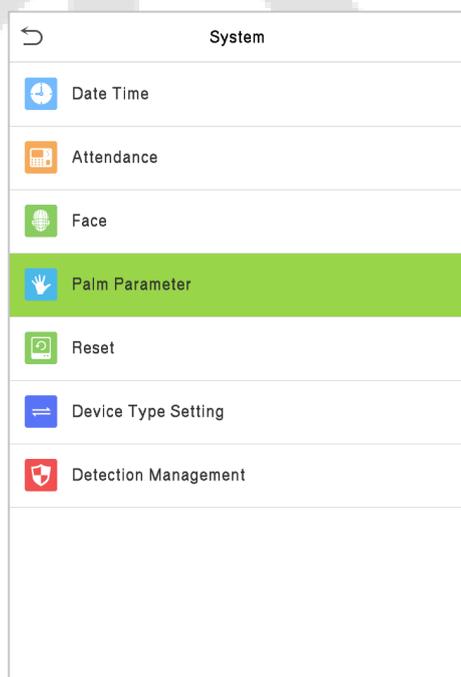
Меню	Описание
Значение порога сравнения 1:N	<p>В режиме верификации 1:N верификация будет успешной только в том случае, если сходство между полученным изображением лица и шаблонами всех зарегистрированных лиц больше установленного значения.</p> <p>Допустимое значение находится в диапазоне от 0 до 100. Чем выше пороговые значения, тем ниже вероятность процента ошибок и выше коэффициент отклонения, и наоборот. Рекомендуется установить значение по умолчанию 47.</p>
Значение порога сравнения 1:N для людей в маске	<p>В режиме верификации 1:N устройство выполнит сравнение сходства между лицом, в настоящее время носящим маску, и шаблоном зарегистрированного лица в устройстве. Когда сходство больше этого значения, это означает, что сравнение прошло успешно, иначе это означает, что сравнение не удалось.</p> <p>Допустимое значение находится в диапазоне от 0 до 100. Чем выше пороговые значения, тем ниже вероятность процента ошибок и выше коэффициент отклонения, и наоборот. Рекомендуется установить значение по умолчанию 68.</p>

<p>Порог сравнения 1:1</p>	<p>При режиме верификации 1:1 верификация будет успешной, только когда сходство полученного изображения лица и зарегистрированных в устройстве шаблонов лица больше установленного значения.</p> <p>Допустимое значение варьируется от 55 до 120. Чем выше пороговые значения, тем ниже вероятность процента ошибок, тем выше коэффициент отклонения и наоборот. Рекомендуется значение по умолчанию - 63.</p>
<p>Пороговое значение при регистрации лица</p>	<p>Во время регистрации лица сравнение 1: N используется для определения того, зарегистрировался ли пользователь ранее.</p> <p>Когда сходство между полученным изображением лица и всеми зарегистрированными шаблонами лица превышает это пороговое значение, это указывает на то, что лицо уже зарегистрировано.</p>
<p>Угол тангажа лица</p>	<p>Допуск угла тангажа лица для регистрации и сравнения лиц.</p> <p>Если угол тангажа лица превышает это установленное значение, он будет отфильтрован алгоритмом, т.е. проигнорирован терминалом, поэтому интерфейс регистрации и сравнения не будет запущен.</p>
<p>Угол поворота лица</p>	<p>Допуск угла поворота лица для регистрации и сравнения шаблонов лица.</p> <p>Если угол поворота лица превышает это установленное значение, он будет отфильтрован алгоритмом, т.е. проигнорирован терминалом, поэтому интерфейс регистрации и сравнения не будет запущен.</p>
<p>Качество изображения</p>	<p>Качество изображения для регистрации и сравнения лиц. Чем выше значение, тем четче изображение.</p>
<p>Минимальный размер лица</p>	<p>Требуется для регистрации лица и сравнения.</p> <p>Если размер объекта меньше этого установленного значения, объект будет отфильтрован и не распознается как лицо.</p> <p>Это значение можно принять за расстояние сравнения лиц. Чем дальше находится человек, тем меньше лицо и тем меньше пиксель лица будет получен алгоритмом. Следовательно, регулировка этого параметра может регулировать самое дальнее расстояние сравнения лиц. Когда значение равно 0, расстояние сравнения лиц не ограничено.</p>
<p>Порог срабатывания светодиодного света</p>	<p>Это значение управляет включением и выключением светодиода. Чем больше значение, тем чаще будет гореть светодиодный индикатор.</p>
<p>Чувствительность обнаружения движения</p>	<p>Измерение степени изменения поля зрения камеры, квалифицируемое как потенциальное обнаружение движения, которое выводит терминал из режима ожидания в интерфейс сравнения. Чем больше значение, тем более чувствительной будет система, т.е. если установлено большее значение, интерфейс сравнения будет срабатывать намного чаще и чаще.</p>

Обнаружение живого объекта	Обнаружение попытки подделки путем определения того, является ли источник биометрического образца живым человеком или поддельным изображением с использованием изображений в видимом свете.
Порог обнаружения живого объекта	Помогает определить, является ли полученное видимое изображение реальным человеком (живым человеком). Чем больше значение, тем лучше эффективность защиты от спуфинга при использовании видимого света.
Антиспуфинг помощью NIR	Использует изображение в ближнем инфракрасном диапазоне для выявления и предотвращения использования поддельных фотографий и видео для идентификации.
Порог бинокулярного обнаружения в реальном времени	Помогает определить, являются ли спектральные изображения в ближней инфракрасной области фальшивыми фото и видео. Чем больше значение, тем лучше эффективность антиспуфинга при построении спектральных изображений в ближней инфракрасной области.
WDR	Широкий динамический диапазон (WDR), который уравнивает свет и увеличивает видимость изображения для видео наблюдения в условиях высококонтрастного освещения и улучшает идентификацию объектов в яркой и темной среде.
Режим борьбы с мерцанием	Используется при отключенном WDR. Помогает уменьшить мерцание, когда экран устройства мигает с той же частотой, что и свет.
Алгоритм лица	Используется для обновления или просмотра основной и дополнительной версии алгоритма лица, а также для приостановки обновления шаблона лица.
Примечание	Неправильная настройка параметров экспозиции и качества может серьезно повлиять на работу устройства. Пожалуйста, регулируйте параметр экспозиции только под руководством персонала послепродажного обслуживания нашей компании.

6.4 Параметры ладони

Нажмите «Ладонь» в интерфейсе системы.

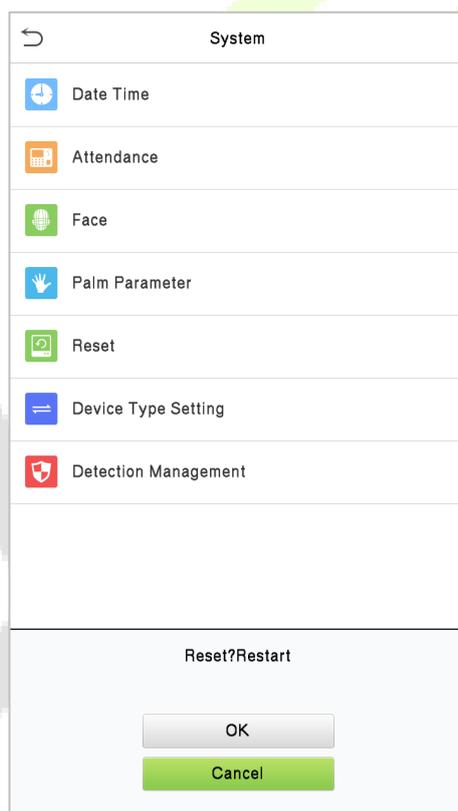


Меню	Описание
Порог сравнения ладони 1:1	В методе верификации 1:1 верификация может быть успешной только в том случае, если сходство между верифицируемой ладонью и зарегистрированной ладонью пользователя превышает это значение.
Порог сравнения ладони 1:N	В методе верификации 1:N верификация может быть успешной только в том случае, если сходство между верифицируемой ладонью и всеми зарегистрированными ладонями превышает это значение.

6.5 Сброс до заводских настроек

Этот параметр восстанавливает такие заводские настройки устройства, как настройки связи и настройки системы (не очищает зарегистрированные данные пользователя).

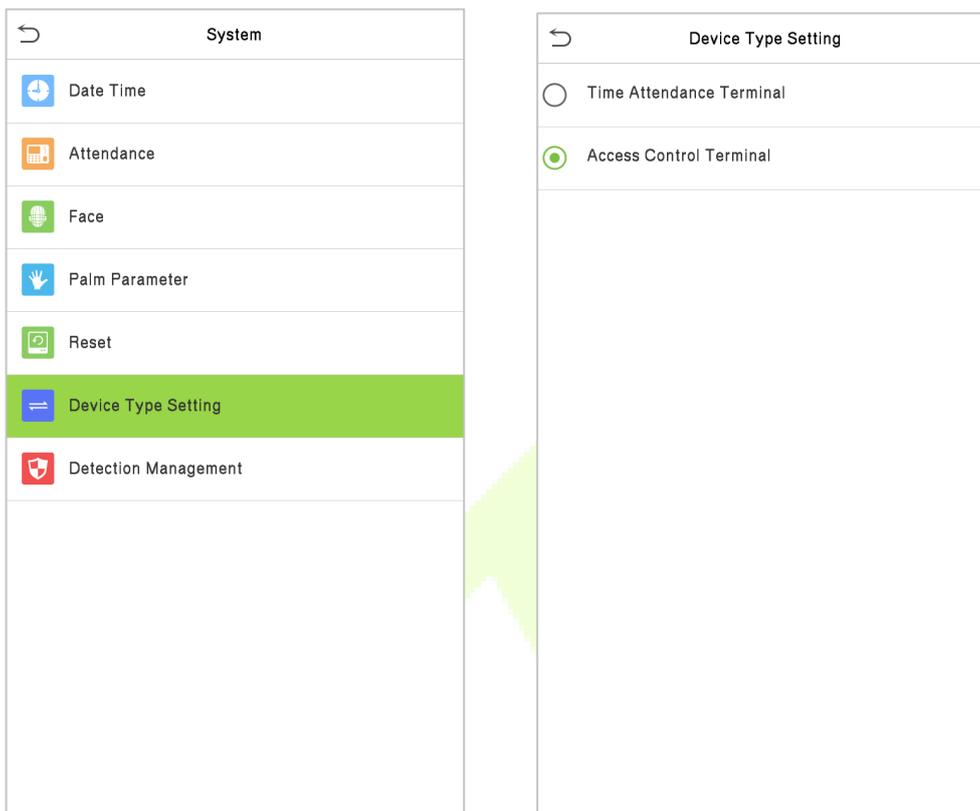
Нажмите **«Сброс»** в интерфейсе системы.



Нажмите **ОК**, чтобы сбросить.

6.6 Настройка типа устройства

Нажмите «**Настройка типа устройства**» в интерфейсе системы, чтобы настроить параметры настройки типа устройства.

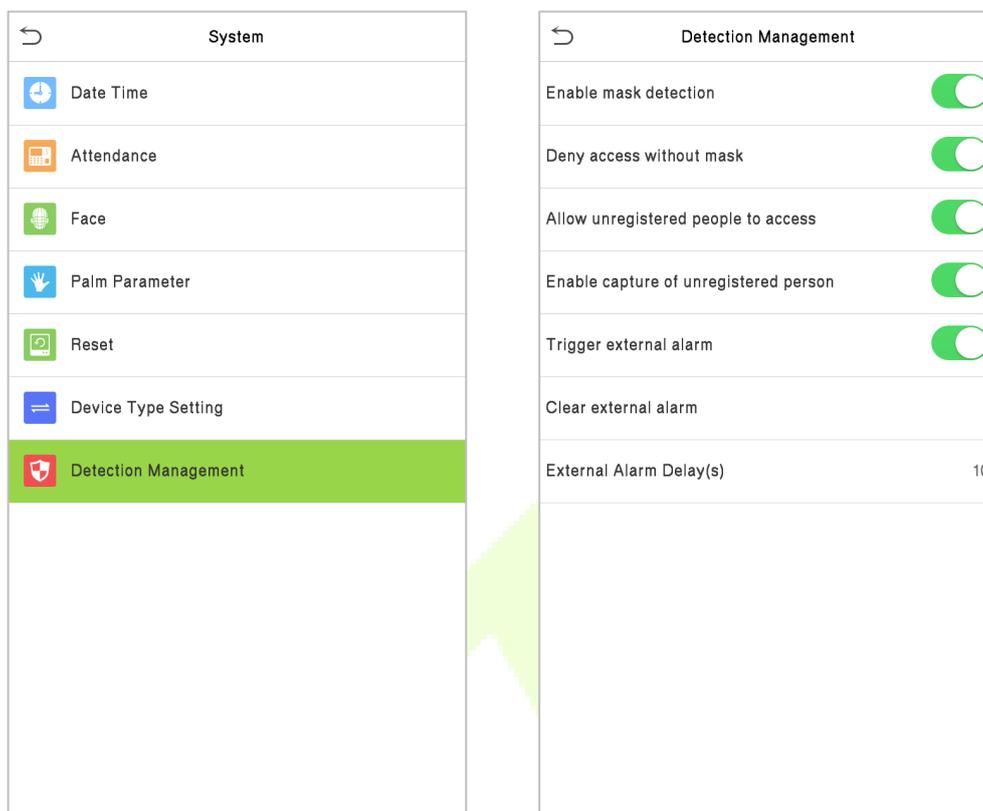


Функция	Описание
Терминал учета рабочего времени	Установите устройство в качестве терминала учета рабочего времени.
Терминал контроля доступа	Установите устройство в качестве терминала контроля доступа.

Примечание: после изменения типа устройства устройство удалит все данные и перезапустится, а некоторые функции будут соответствующим образом скорректированы.

6.7 Управление обнаружением

Нажмите «**Управление обнаружением**» в интерфейсе системы.



Функция	Описание
Включить обнаружение маски	Включает или отключает функцию обнаружения маски. При включении устройство определяет, носит ли пользователь маску во время верификации.
Запретить доступ без маски	Включает или отключает доступ человека без маски. При включении устройство запрещает доступ человеку, если на нем не надета маска.
Разрешить доступ незарегистрированным людям	Включает или отключает доступ незарегистрированного человека. При включении устройство позволяет человеку входить без регистрации.
Включить захват изображения незарегистрированного человека	Для включения или отключения захвата изображения незарегистрированного человека. Если этот параметр включен, устройство автоматически сделает снимок незарегистрированного человека, для включения этой функции необходимо разрешить доступ незарегистрированным людям.
Активировать внешнюю тревогу	Если этот параметр включен, если пользователь не носит маску, система вызовет тревогу.
Очистить внешнюю тревогу	Очищает записи сработавших сигналов тревоги устройства.
Задержка внешнего сигнала тревоги (сек)	Это время задержки (сек) для срабатывания внешнего сигнала тревоги. Его можно установить за секунды. Пользователи могут отключить функцию или установить значение от 1 до 255.

7 Настройки персонализации

Можно настроить параметры интерфейса, звука и звонка.

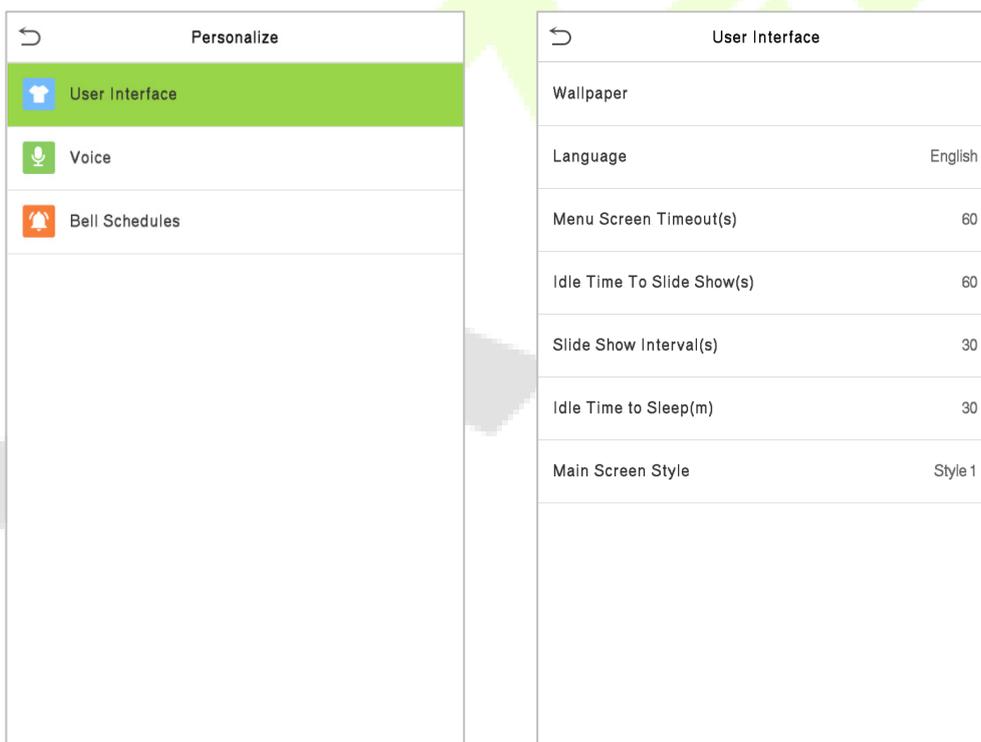
Нажмите «**Персонализация**» в интерфейсе главного меню.



7.1 Настройки интерфейса

Можно настроить стиль отображения главного интерфейса.

Нажмите «**Пользовательский интерфейс**» в интерфейсе персонализации.

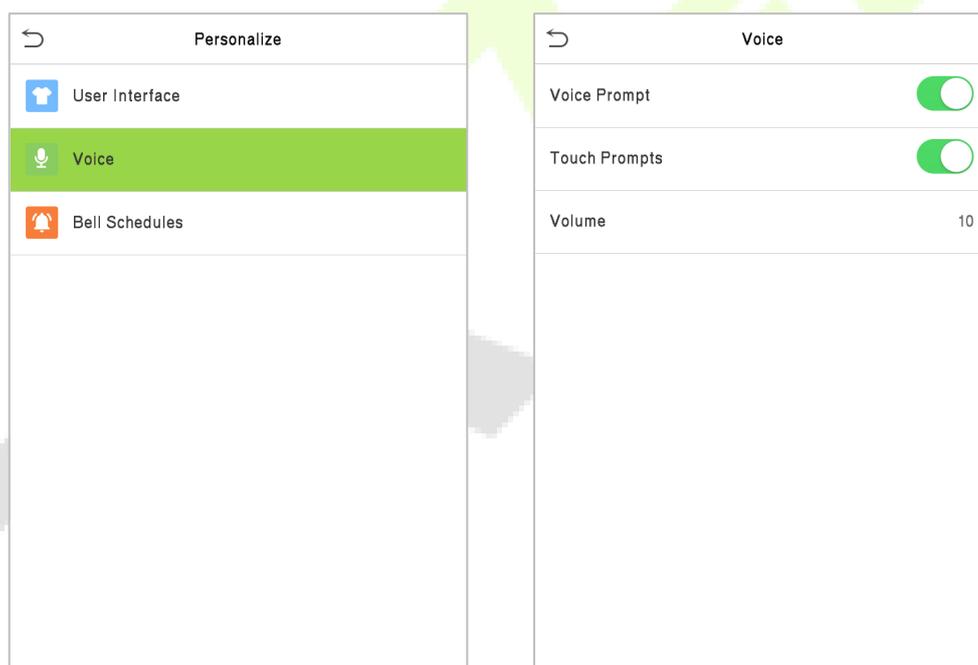


Меню	Описание
Обои	Для выбора обоев главного экрана в соответствии с вашими личными предпочтениями.
Язык	Выбрать язык устройства.
Время ожидания экрана меню (сек.)	Когда нет операций и время превышает установленное значение, устройство автоматически вернется к начальному интерфейсу. Можно отключить эту функцию или установить значение от 60 до 99999 секунд.

Время бездействия до перехода в слайд-шоу (сек.)	При отсутствии операций и превышением по времени установленного значения будет воспроизводиться слайд-шоу. Функцию можно отключить, или можно установить значение от 3 до 999 секунд.
Интервал слайд-шоу (сек.)	Относится к временному интервалу переключения различных изображений слайд-шоу. Функцию можно отключить или установить интервал от 3 до 999 секунд.
Время бездействия до перехода в спящий режим (мин.)	Если активирован спящий режим, когда нет никаких операций, устройство войдет в режим ожидания. Нажмите любую клавишу или палец, чтобы возобновить нормальный рабочий режим. Вы можете отключить эту функцию или установить значение в течение 1-999 минут.
Стиль главного экрана	Для выбора стиля главного экрана в соответствии с вашими личными предпочтениями.

7.2 Голосовые настройки

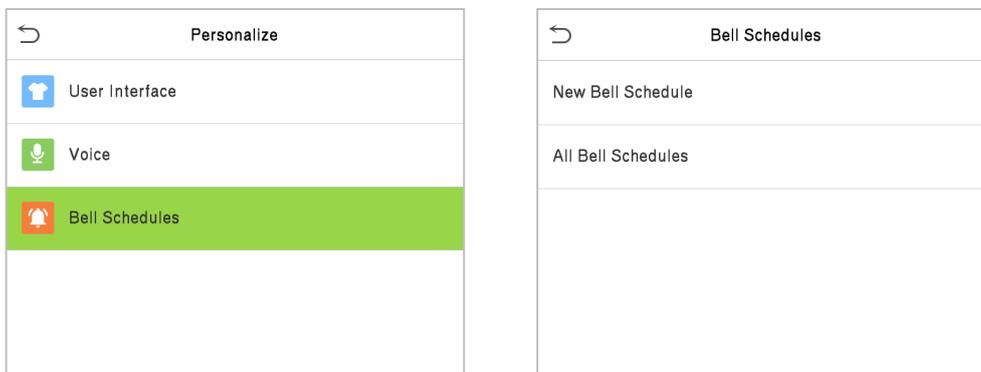
Нажмите «Голос» в интерфейсе персонализации.



Меню	Описание
Голосовая подсказка	Выберите, следует ли включать голосовые подсказки во время работы.
Сенсорная подсказка	Выберите, следует ли включить звуки работы клавиатуры.
Громкость	Отрегулируйте громкость устройства; действительное значение: 0-100.

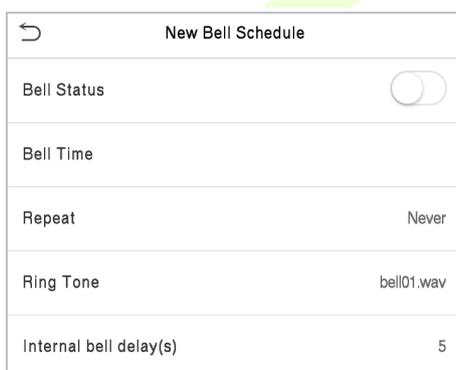
7.3 Графики звонков

Нажмите «**Графики звонков**» в интерфейсе персонализации.



Добавить звонок

1. Нажмите «**Новый график звонков**», чтобы войти в интерфейс добавления:



Меню	Описание
Состояние звонка	Установите, следует ли включать состояние звонка.
Время звонка	В это время суток устройство автоматически издает звонок.
Повтор	Установите цикл повтора звонка.
Мелодия звонка	Выберите мелодию звонка.
Задержка внутреннего звонка (сек)	Установите продолжительность внутреннего звонка. Допустимые значения: от 1 до 999 секунд.

2. Вернитесь в интерфейс графиков звонков, нажмите «**Все графики звонков**», чтобы просмотреть недавно добавленный звонок

Редактировать звонок

В интерфейсе всех графиков звонков нажмите редактируемый звонок.

Нажмите «**Редактировать**», метод редактирования такой же, как при операции добавления звонка

Удалить звонок

В интерфейсе всех графиков звонков нажмите удаляемый звонок.

Нажмите «**Удалить**» и выберите [**Да**], чтобы удалить звонок.

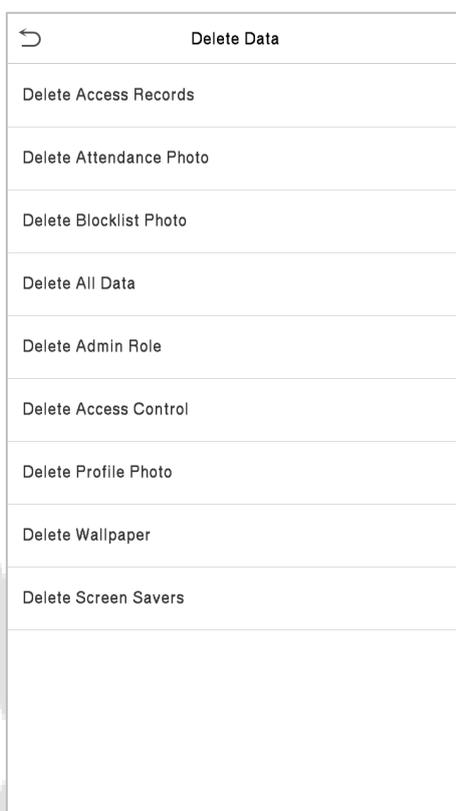
8 Управление данными

Интерфейс управления данными используется для удаления соответствующих данных в устройстве. Нажмите «**Управление данными**» в интерфейсе главного меню.



8.1 Удалить данные

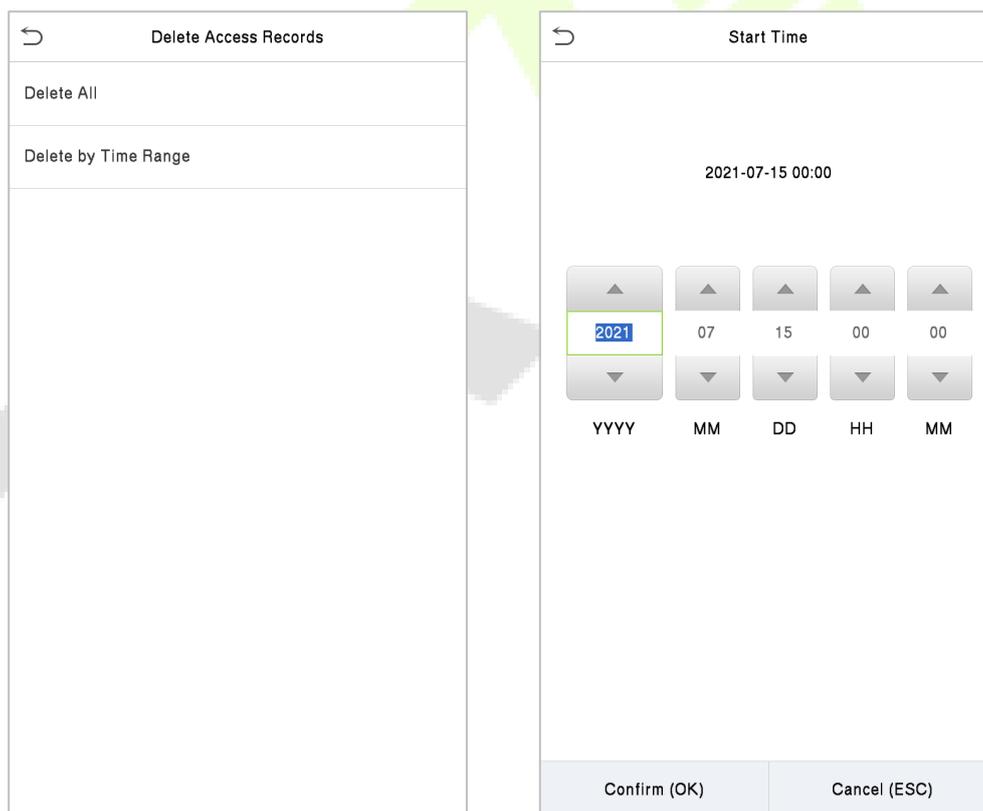
Нажмите «**Удалить данные**» в интерфейсе управления данными.



Меню	Описание
Удалить записи доступа	Для условного удаления данных учета рабочего времени / записей доступа.
Удалить фотографии учета рабочего времени	Для удаления фотографий учета рабочего времени соответствующих сотрудников.
Удалить фотографии черного списка	Для удаления фотографий, сделанные во время неудачных верификаций

Удалить все данные	Для удаления информации и журналов учета рабочего времени / записей доступа всех зарегистрированных пользователей.
Удалить роль администратора	Для удаления всех прав администратора.
Удалить контроль доступа	Для удаления всех данных доступа.
Удалить фотографию пользователя	Для удаления всех пользовательских фотографий в устройстве.
Удалить обои	Для удаления все обоев в устройстве.
Удалить экранные заставки	Для удаления экранных заставок в устройстве.

Пользователь может выбрать «Удалить все» или «Удалить по временному диапазону» при удалении записей доступа, фотографий учета рабочего времени или фотографий черного списка. Выбрав «Удалить по временному диапазону», необходимо установить определенный временной диапазон для удаления всех данных за определенный период.

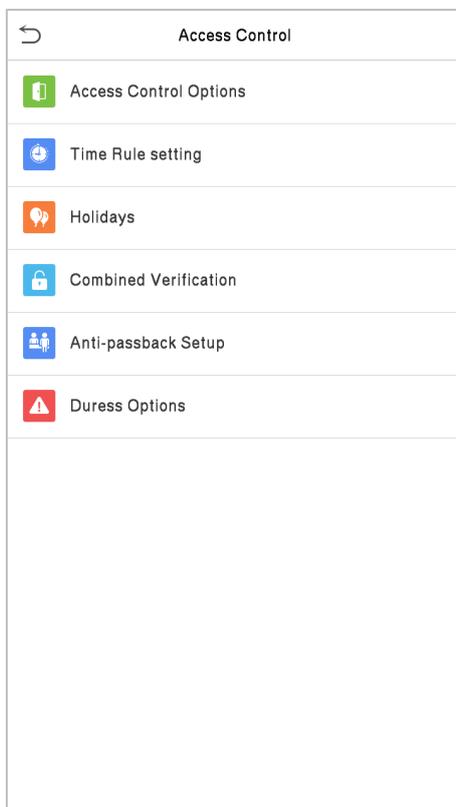


Выберите Удалить по временному диапазону Установите временной диапазон и нажмите ОК

9 Контроль доступа

Контроль доступа используется для установки графика открытия двери, управления замками и настроек других параметров, связанных с контролем доступа.

Нажмите «**Контроль доступа**» в интерфейсе главного меню.



Для получения доступа зарегистрированный пользователь должен соответствовать следующим условиям:

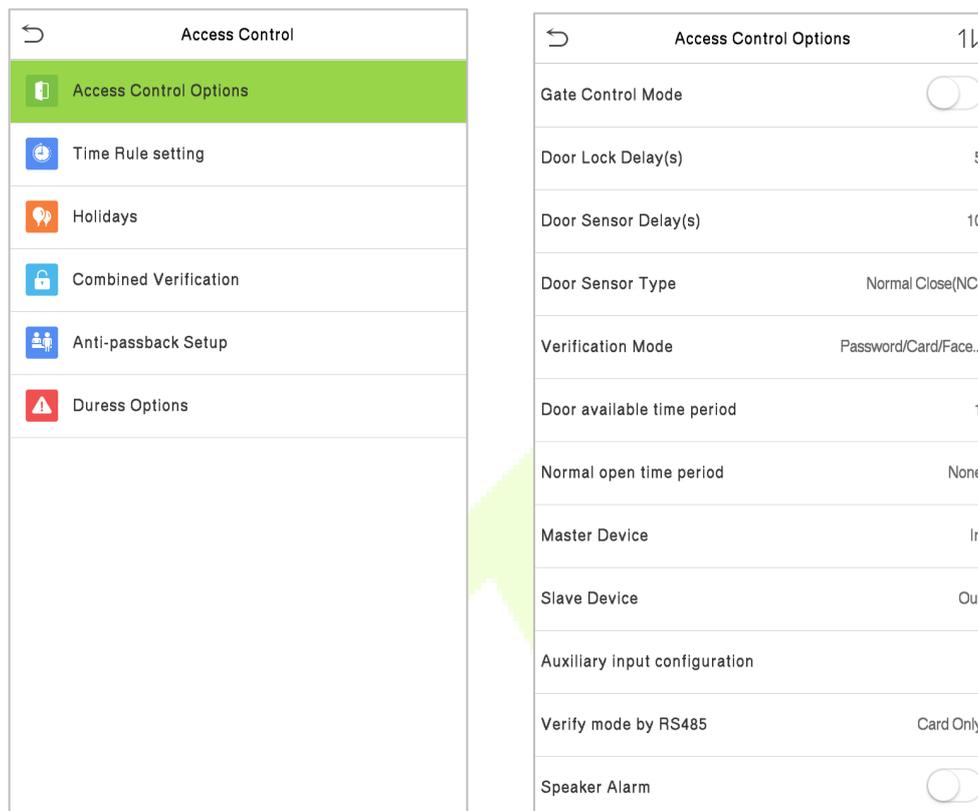
1. Время разблокировки текущей двери должно быть в пределах любого периода времени действия разрешенного доступа для пользователя.
2. Группа пользователя должна входить в комбинацию разблокировки двери (когда в той же комбинации доступа присутствуют другие группы, для разблокировки двери также требуется верификация членов этих групп).

В настройках по умолчанию новые пользователи распределяются в первую группу с периодом разрешенного доступа группы по умолчанию и комбинацией доступа «1» и устанавливаются в состояние разблокировки.

9.1 Параметры контроля доступа

Этот параметр используется для установки параметров управления замком устройства и связанных параметров.

Нажмите «**Параметры контроля доступа**» в интерфейсе контроля доступа.



Меню	Описание
Режим управления дверью	Переключается между положением ВКЛ или ВЫКЛ , чтобы войти в режим управления воротами или нет. Если установлено значение ВКЛ , интерфейс удаляет параметр «Реле дверного замка», «Реле дверного датчика» и «Тип дверного датчика».
Задержка замка двери (сек)	Время, в течение которого устройство управляет разблокировкой электромагнитного замка. Допустимый диапазон - от 1 до 10 секунд; 0 секунд означает отключение функции.
Задержка датчика двери (сек)	Если дверь не заблокирована и остается открытой после открытия в течение определенного времени (Задержка датчика двери), сработает тревожная сигнализация. Допустимое значение задержки датчика двери составляет от 1 до 255 секунд.
Тип датчика двери	Существует три типа режима: Отсутствует , Нормально-открытый и Нормально-закрытый . Отсутствует означает, что датчик двери не используется; Нормально-открытый означает, что дверь всегда открывается при включенном питании; Нормально-закрытый означает, что дверь всегда закрыта при включенном питании.
Режим верификации	Поддерживаемый режим верификации включает пароль/лицо, только идентификатор пользователя, пароль, только лицо, и лицо + пароль.

Период времени доступа к двери	Установить период времени для двери так, чтобы дверь была доступна только в этот период.
Период времени режима Нормально-открытый	Запланированный период времени для режима Нормально-открытый , чтобы дверь всегда была разблокирована в течение этого периода.
Главное устройство	При настройке главного и подчиненного устройств, состояние главного устройства может быть установлено на выход или на вход . Выход: запись верификации в главном устройстве является записью регистрации выхода. Вход: запись верификации в главном устройстве является записью регистрации входа.
Подчиненное устройство	При настройке главного и подчиненного устройств можно установить состояние подчиненного устройства как выход или вход . Выход: запись верификации на подчиненном устройстве - это запись регистрации выхода. Вход: запись верификации на подчиненном устройстве - это запись регистрации входа.
Конфигурация дополнительного входа	Установите время разблокировки двери и тип дополнительного выхода вспомогательного терминала устройства. Типы дополнительных выходов включают в себя «Отсутствует», «Запуск режима дверь открыта», «Запуск тревоги», «Запуск режима дверь открыта и Тревога».
Режим верификации с помощью RS485	Режим верификации используется, когда устройство используется в качестве главного или подчиненного устройства. Поддерживаемый режим верификации включает только карту и карту + пароль.
Сигнал тревоги динамика	Для передачи звуковой сигнализации или отключения сигнализации локальной сети. Когда дверь закрыта или верификация прошла успешно, система отменит сигнал тревоги от локальной сети.
Сброс настроек контроля доступа	Восстановленные параметры контроля доступа включают задержку дверного замка, задержку дверного датчика, тип дверного датчика, режим верификации, период времени доступности двери, период времени нормального открытия, главное устройство и сигнал тревоги. Однако стертые данные управления доступом в Управлении данными исключены.

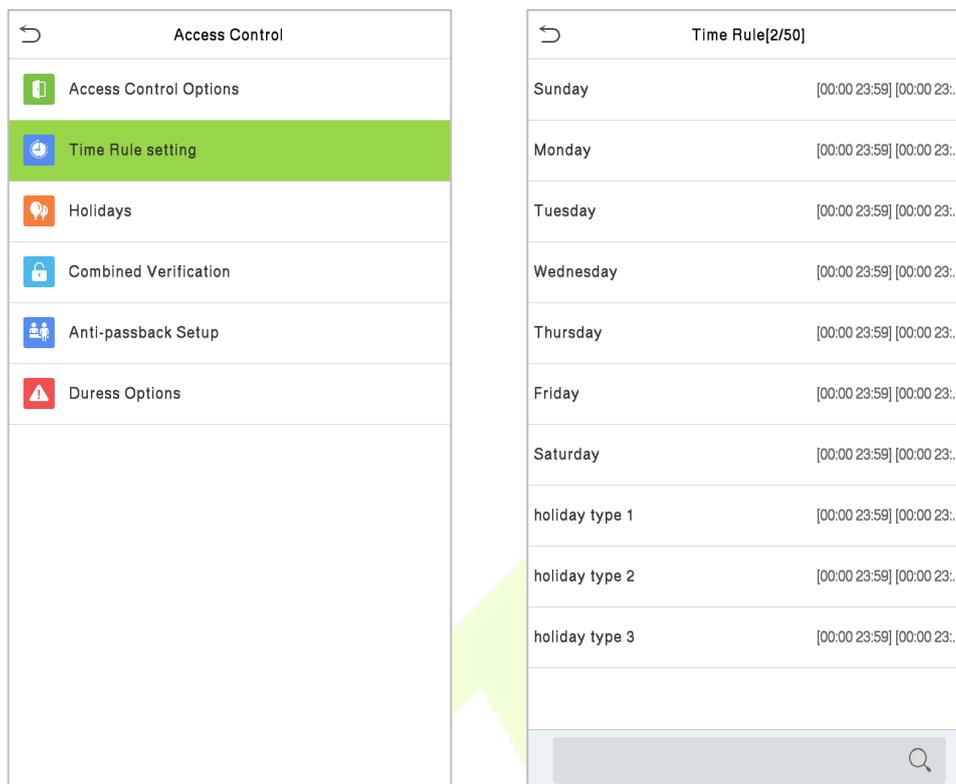
9.2 Настройка правила времени

Нажмите «**Настройка правила времени**» в интерфейсе контроля доступа, чтобы настроить параметры времени.

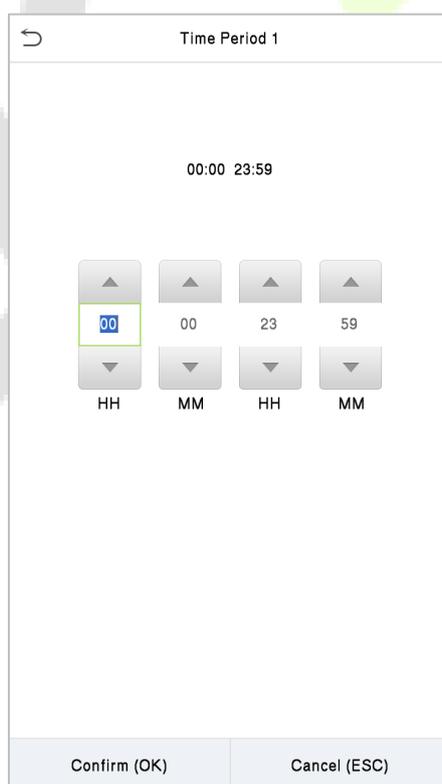
- Вся система может определять до 50 периодов времени.
- Каждый временной период представляет **10** периодов разрешенного доступа, то есть **1** неделя и **3** праздничных дня, а каждый период разрешенного доступа является стандартным 24-часовым периодом в день, и пользователь может проходить верификацию только в пределах допустимого периода времени.
- Можно установить максимум 3 временных периода для каждого периода разрешенного доступа. Связь между этими периодами времени - «ИЛИ». Таким образом, когда время верификации попадает в любой из этих периодов времени, верификация считается действительной.

- Формат периода разрешенного доступа для каждого периода времени - **ЧЧ ММ-ЧЧ ММ**, с точностью до минут в 24-часовом формате.

Нажмите серое поле, чтобы найти требуемый период разрешенного доступа и указать требуемое количество периодов разрешенного доступа (максимум до 50 зон).



В интерфейсе выбранного количества периодов разрешенного доступа нажмите нужный день (то есть понедельник, вторник и т. д.), чтобы установить время.



Укажите время начала и окончания, а затем нажмите **OK**.

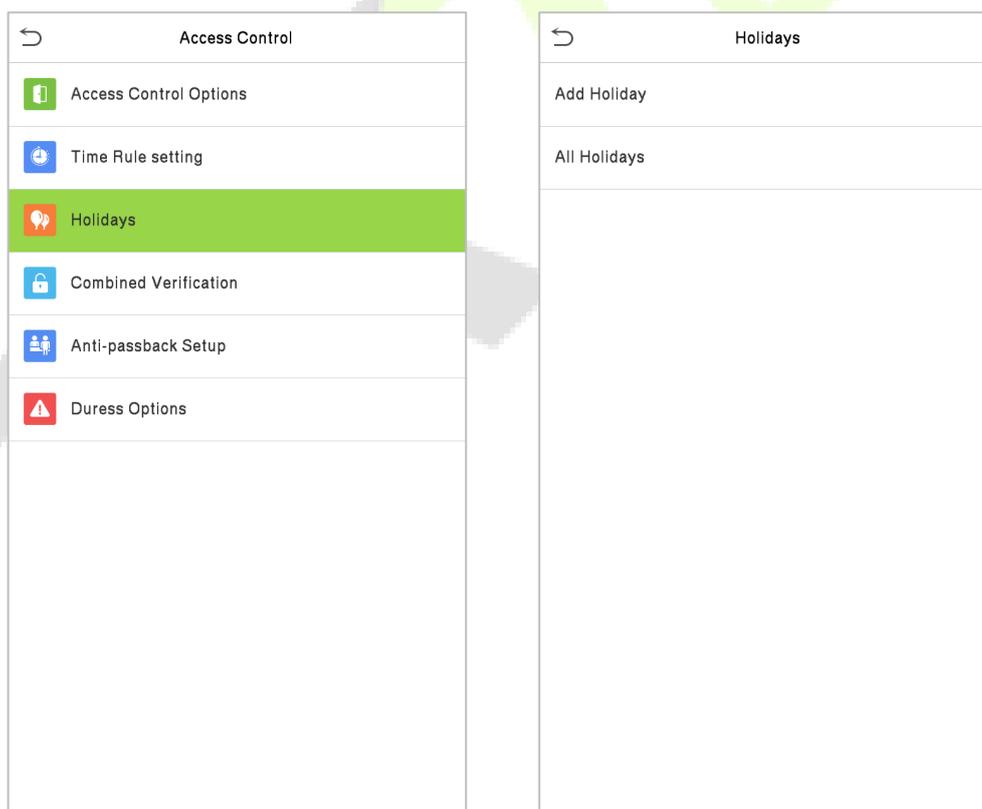
Примечание:

- 1) Дверь будет недоступна в течение всего дня, если время окончания наступает раньше времени начала (например, **23:57 ~ 23:56**).
- 2) Это временной интервал для действительного доступа, когда время окончания наступает после времени начала (например, **08:00 ~ 23:59**).
- 3) Дверь доступна в течение всего дня, если время окончания наступает позже времени начала (например, время начала - **00:00**, а время окончания - **23:59**).
- 4) Часовой пояс по умолчанию 1 указывает, что дверь открыта в течение всего дня.

9.3 Настройки праздничного дня

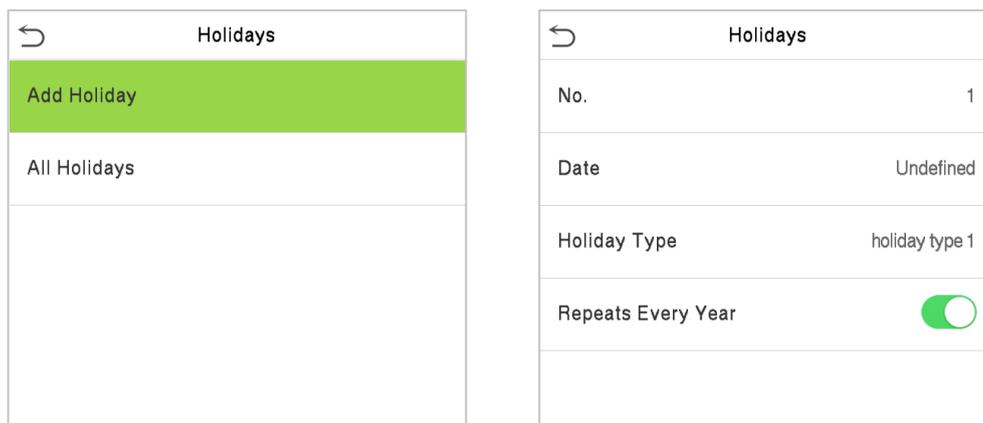
Всякий раз, когда есть праздничный день, может понадобиться специальное время доступа; но изменять время доступа каждого по одному чрезвычайно громоздко, поэтому можно установить время доступа в праздничные дни, которое будет применимо ко всем сотрудникам, и пользователь сможет открывать дверь в праздничные дни.

Нажмите «**Праздничный день**» в интерфейсе контроля доступа.



Добавить новый праздничный день

Нажмите «**Добавить праздничный день**» в интерфейсе праздничных дней и установите параметры праздничных дней.



Редактировать праздничный день

В интерфейсе праздничных дней выберите элемент праздничного дня, который нужно изменить. Нажмите «**Редактировать**», чтобы изменить параметры праздничного дня.

Удалить праздничный день

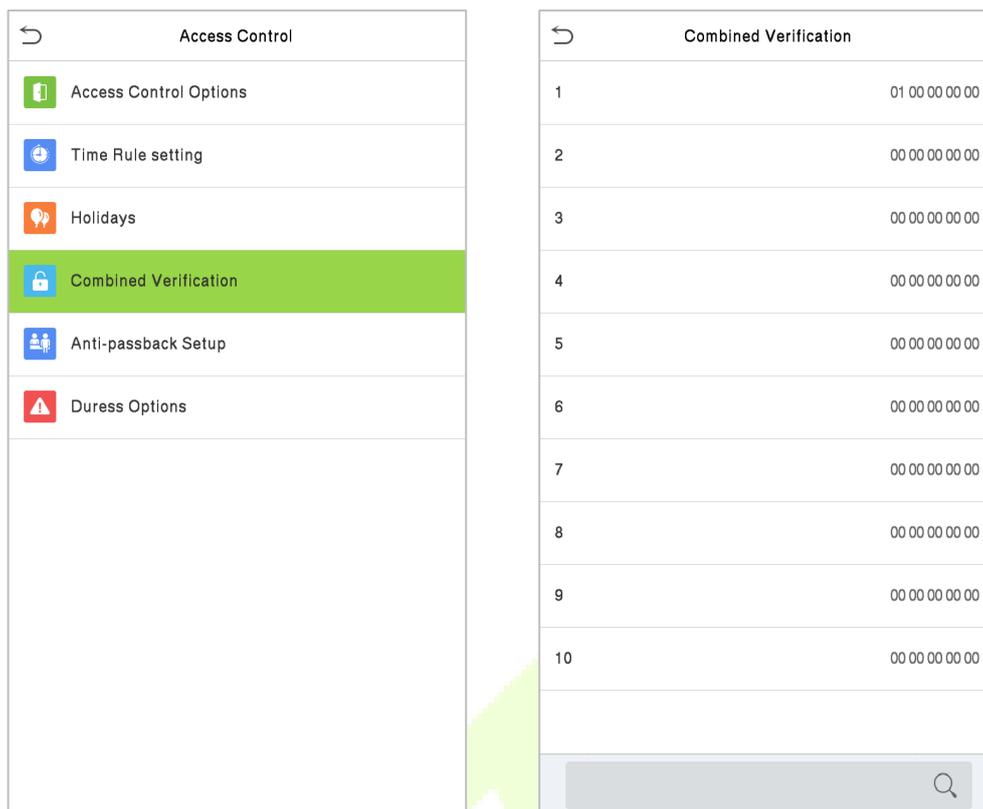
В интерфейсе праздничных дней выберите элемент праздничного дня, который нужно удалить, и нажмите «**Удалить**». Нажмите **ОК**, чтобы подтвердить удаление. После удаления этот праздничный день больше не отображается в интерфейсе всех праздничных дней.

9.4 Настройки комбинированной верификации

Группы контроля доступа организованы в различные комбинации разблокировки дверей для одновременной верификации нескольких человек и усиления безопасности.

В комбинации для разблокировки двери диапазон числа комбинаций N составляет: $0 \leq N \leq 5$, и число членов N могут все относиться к одной группе доступа или могут относиться к пяти различным группам доступа.

Нажмите «**Комбинированная верификация**» в интерфейсе контроля доступа.



Нажмите комбинацию разблокировки двери, которую нужно установить. Нажмите стрелки вверх и вниз, чтобы ввести номер комбинации, затем нажмите ОК.

Примеры:

Комбинация разблокировки двери 1 установлена как (01 03 05 06 08), что указывает на то, что комбинация разблокировки 1 состоит из 5 человек, а 5 человек относятся к 5 группам, а именно, к группе контроля доступа 1 (группа КД1), группе КД3, группе КД5, группе КД6 и группе КД8 соответственно.

Комбинация разблокировки двери 2 установлена как (02 02 04 04 07), что указывает на то, что комбинация разблокировки двери 2 состоит из 5 человек; первые два относятся к группе КД2, следующие два человека относятся к группе КД4, а последний человек относится к группе КД7.

Комбинация разблокировки двери 3 установлена как (09 09 09 09 09), что означает, что в этой комбинации 5 человек; все относятся к группе КД9.

Комбинация разблокировки двери 4 установлена как (03 05 08 00 00), что означает, что комбинация разблокировки 4 состоит из трех человек. Первый человек относится к группе КД3, второй человек относится к группе КД5, а третий человек относится к группе КД8.

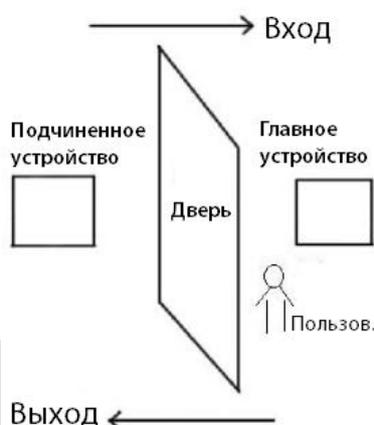
Удалить комбинацию разблокировки двери

Установите для всех групповых номеров значение 0, если вы хотите удалить комбинации для разблокировки дверей.

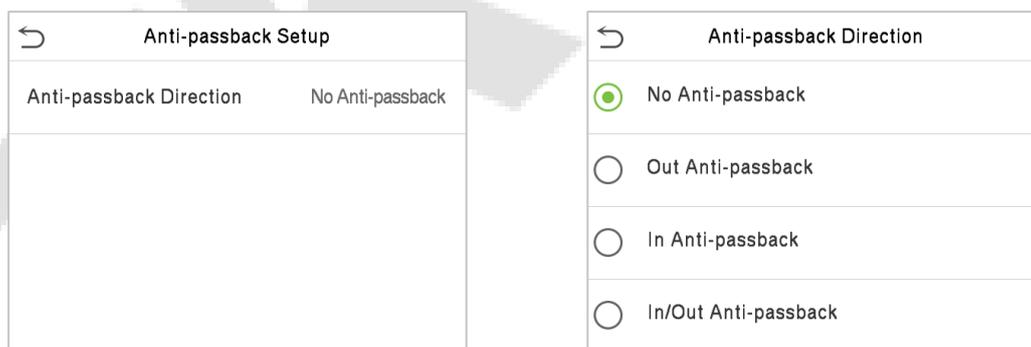
9.5 Установка контроля повторного прохода

Для того, чтобы некоторые люди не следовали за пользователями и не входили в дверь без верификации, что приводит к проблемам с безопасностью, пользователи могут включить функцию контроля повторного прохода. После ее включения для того, чтобы открыть дверь запись регистрации входа должна совпадать с записью регистрации выхода.

Эта функция требует двух устройств для совместной работы: одно устанавливается внутри помещения (главное устройство), другое - снаружи двери (подчиненное устройство). Эти два устройства связываются с помощью сигнала Wiegand. Формат Wiegand и тип вывода (идентификатор пользователя/номер карты), принятые главным устройством и подчиненным устройством, должны быть согласованы.



Нажмите «**Установка контроля повторного прохода**» в интерфейсе контроля доступа.

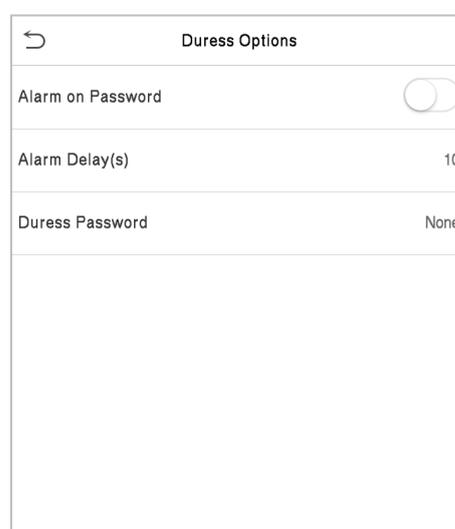
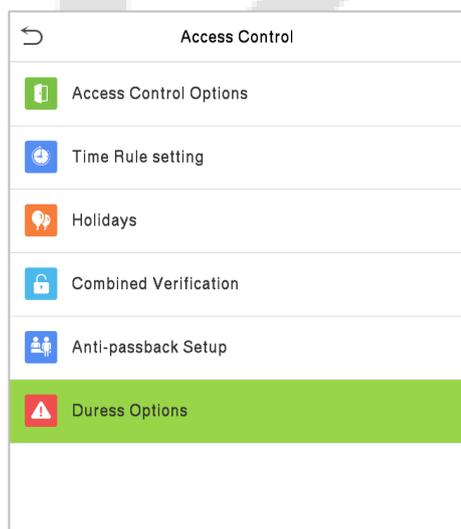


Параметр	Описание
<p>Контроль повторного прохода</p>	<p>Контроль повторного прохода отсутствует: функция Контроля повторного прохода отключена, что означает, что прохождение верификации как на главном, так и на подчиненном устройстве может разблокировать дверь. Состояние учета рабочего времени не сохраняется.</p> <p>Контроль повторного прохода на выход: пользователь может зарегистрировать выход, только если последняя запись является записью регистрации входа; в противном случае сработает сигнал тревоги. Тем не менее, пользователь может свободно зарегистрировать вход.</p> <p>Контроль повторного прохода на вход: пользователь может зарегистрировать вход, только если последняя запись является записью о регистрации выхода; в противном случае сработает сигнал тревоги. Тем не менее, пользователь может свободно зарегистрировать выход.</p> <p>Контроль повторного прохода на вход/выход: в этом случае пользователь может зарегистрировать вход, только если последняя запись является записью регистрации выхода; или может зарегистрировать выход снова, только если последняя запись является записью о регистрации входа; в противном случае сработает сигнал тревоги.</p>

9.6 Настройки параметров принуждения

Если пользователь активировал функцию верификации по принуждению с определенным методом (ами) аутентификации, когда он / она находится под принуждением во время аутентификации с помощью такого метода, устройство разблокирует дверь как обычно, но в то же время будет отправлен сигнал для запуска тревоги.

Нажмите «**Параметры принуждения**» в интерфейсе контроля доступа.

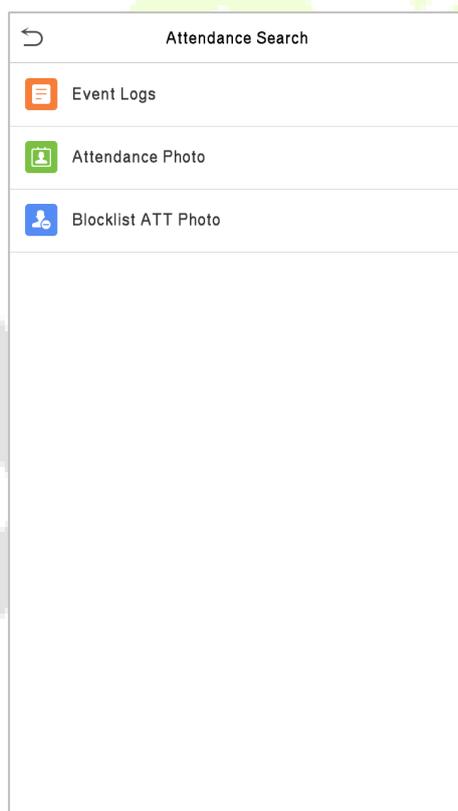


Меню	Описание
Тревога по паролю	Когда пользователь использует метод верификации пароля, сигнал тревоги генерируется только при успешной верификации пароля, в противном случае сигнал тревоги отсутствует.
Задержка тревожной сигнализации (сек)	Сигнал тревоги не будет передаваться, пока не истечет время задержки тревоги. Значение колеблется от 1 до 999 секунд.
Пароль принуждения	Установите 6-значный пароль принуждения. Когда пользователь вводит этот пароль принуждения для верификации, срабатывает сигнал тревоги.

10 Поиск событий учета рабочего времени

После того, как личность пользователя прошла верификацию, запись будет сохранена в устройстве. Эта функция позволяет пользователям проверять журналы событий.

Нажмите **«Поиск событий учета рабочего времени»** в главном меню для поиска требуемых журналов событий.



Процесс поиска фотографий учета рабочего времени и черного списка аналогичен процессу поиска журналов событий. Ниже приведен пример поиска журналов событий.

В интерфейсе поиска событий учета рабочего времени нажмите **«Журналы события»**.

1. Введите идентификатор искомого пользователя для поиска и нажмите ОК. Если вы хотите искать записи всех пользователей, нажмите ОК, не вводя идентификатора какого-либо пользователя.

2. Выберите временной диапазон, в котором находятся записи, которые вы желаете найти.

3. Поиск записи успешен. Нажмите на запись в зеленом, чтобы просмотреть информацию.

Date	User ID	Time
10-09		Number of Records:18
		14:18 14:13
	2	16:47 16:44 16:43 15:03 14:58
		14:56 14:55 14:55 14:53 14:43
		14:41 14:38
	1000702	14:55 14:54 14:27 14:18

4. На рисунке ниже показана информация по выбранной записи.

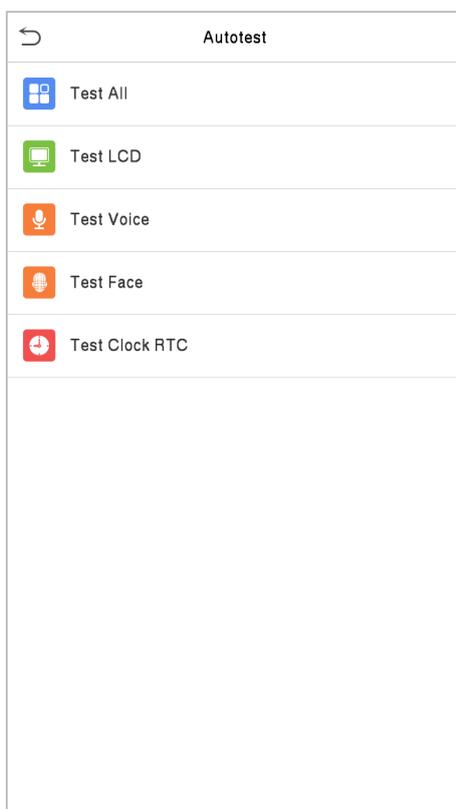
User ID	Name	Time	Mode	State
2	Mike	10-09 16:47	15	255
2	Mike	10-09 16:44	15	255
2	Mike	10-09 16:43	15	255
2	Mike	10-09 15:03	15	255
2	Mike	10-09 14:58	15	255
2	Mike	10-09 14:56	25	255
2	Mike	10-09 14:55	15	255
2	Mike	10-09 14:55	15	255
2	Mike	10-09 14:53	25	255
2	Mike	10-09 14:43	15	255
2	Mike	10-09 14:41	15	255
2	Mike	10-09 14:38	15	255

Verification Mode : Face Punch State : 255

11 Автоматическое тестирование

Эта функция автоматически тестирует правильность работы всех модулей в устройстве, включая ЖК-дисплей, аудиосистему, камеру и часы реального времени (RTC).

Нажмите «**Автоматическое тестирование**» в интерфейсе главного меню.

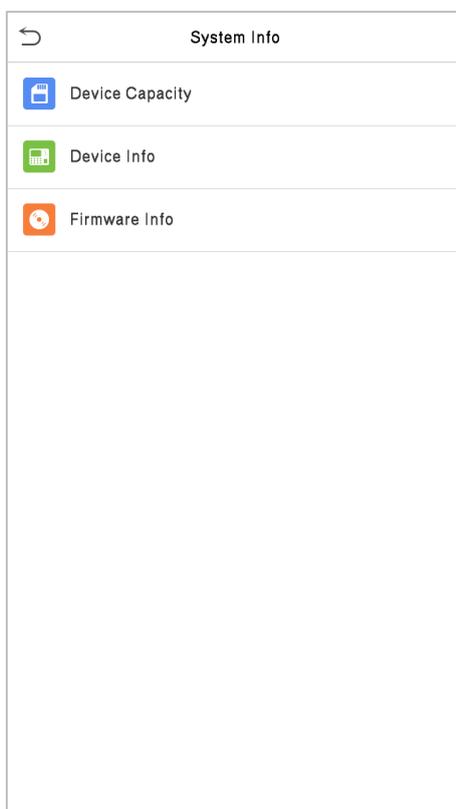


Меню	Описание
Тестировать все	Для автоматического тестирования нормальной работы ЖК-дисплея, звука, камеры и часов реального времени.
Тестировать ЖК	Для автоматического тестирования эффекта отображения на ЖК-экране, полноцветного отображения, отображения чисто белого, и чисто черного, для тестирования нормального отображения экрана.
Тестировать голос	Для автоматического тестирования заполнения аудиофайлов, хранящихся в устройстве, и качества голоса.
Тестировать лицо	Для тестирования правильности работы камеры, проверяя сделанные снимки, чтобы убедиться, что они достаточно четкие.
Тестировать часы реального времени	Для тестирования часов реального времени. Устройство проверяет, работают ли часы нормально и точно посредством секундомера. Нажмите на экран, чтобы начать подсчет, и нажмите его еще раз, чтобы остановить подсчет.

12 Информация о системе

С помощью параметра информации о системе можно просматривать состояние хранилища, информацию о версии устройства и т. д.

Нажмите «**Информация о системе**» в интерфейсе главного меню.



Меню	Описание
Емкость устройства	Отображает текущее состояние хранилища пользователя, хранилища ладоней, паролей и лиц, администраторов, записей доступа, фотографий учета рабочего времени и черного списка, и фотографий пользователей.
Информация об устройстве	Отображает имя устройства, серийный номер, MAC-адрес, информацию о версии алгоритма лица и ладони, информацию о платформе, версии MCU, производителе и дате производства.
Информация о прошивке	Отображает версию прошивки и другую информацию об устройстве.

13 Подключение к программному обеспечению ZKBioAccess IVS

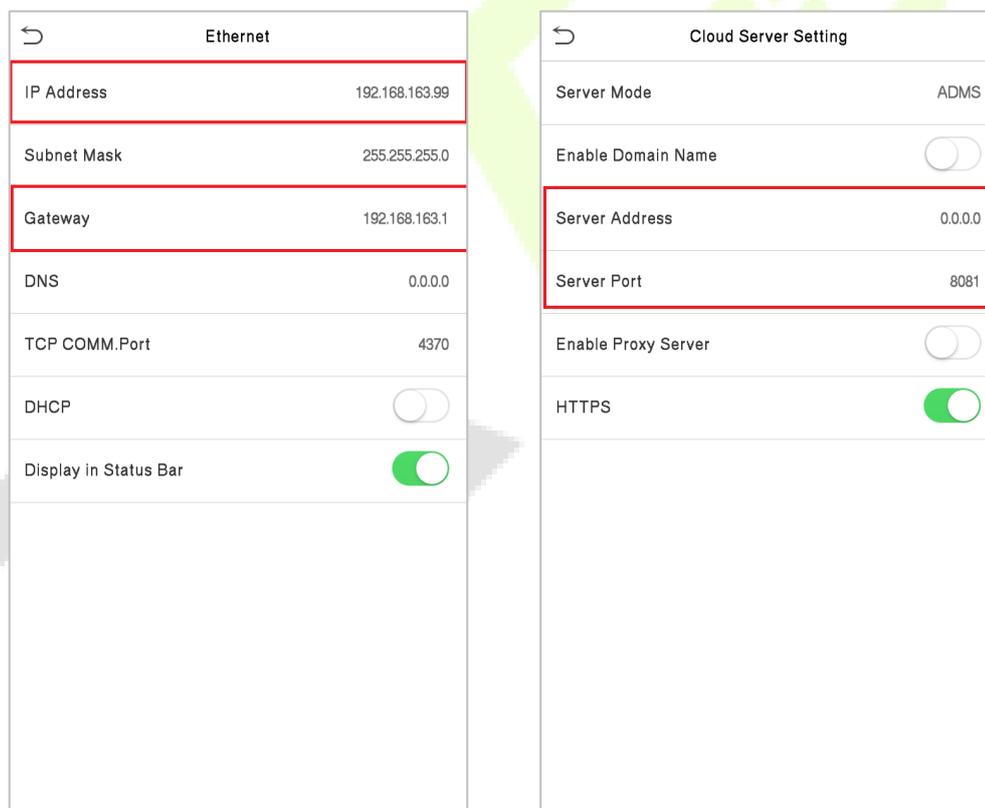
13.1 Установка адреса связи

Для устройства

1. Нажмите **Связь > Ethernet** в главном меню, чтобы установить IP-адрес и шлюз устройства. (**Примечание:** IP-адрес должен иметь возможность связываться с сервером ZKBioAccess IVS, предпочтительно в том же сегменте сети, что и адрес сервера).
2. В главном меню нажмите **Связь > Настройка облачного сервера**, чтобы установить адрес и порт сервера.

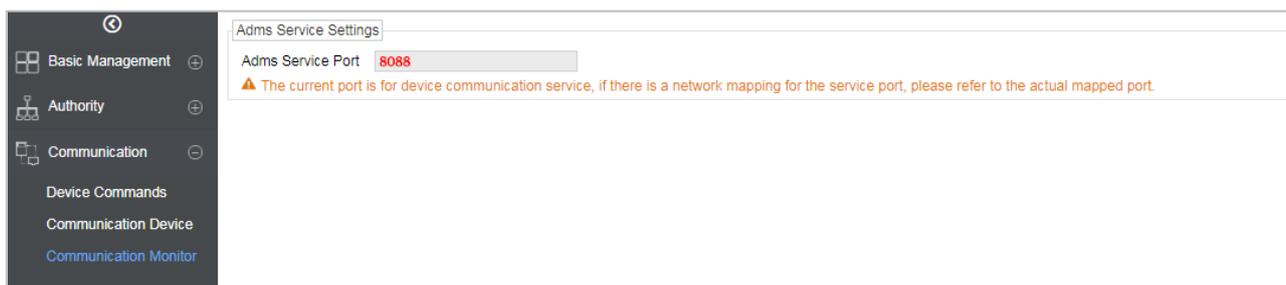
Адрес сервера: установите как IP-адрес сервера ZKBioAccess IVS.

Порт сервера: установите как порт службы ZKBioAccess IVS (по умолчанию 8088).



Для Программного обеспечения

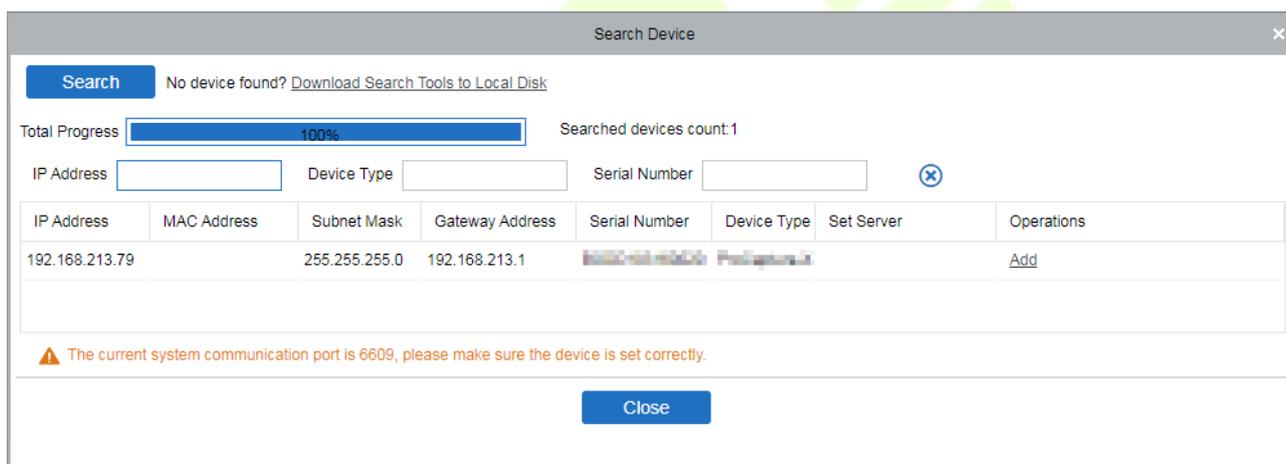
Войдите в программное обеспечение ZKBioAccess IVS, нажмите **Система > Связь > Монитор связи**, чтобы настроить порт службы ADMS, как показано на рисунке ниже:



13.2 Добавить устройство в программное обеспечение

Добавьте устройство с помощью поиска. Процесс выглядит следующим образом:

- 1) Нажмите **Контроль доступа > Устройство > Устройство поиска**, чтобы открыть интерфейс поиска в программном обеспечении.
- 2) Нажмите «**Поиск**», и появится запрос [**Поиск...**].
- 3) После поиска отобразится список и общее количество контроллеров доступа.



- 4) Нажмите «**Добавить**» столбце операций появится новое окно. В каждом раскрывающемся списке выберите Тип значка, Область и Добавить на уровень и нажмите [**ОК**], чтобы добавить устройство.

13.3 Добавить сотрудников в программное обеспечение

1. Нажмите **Сотрудники > Сотрудник > Создать**:

New ×

Personnel ID*	<input type="text" value="5"/>	Department*	<input type="text" value="Ban Giam Đốc"/>	 <input type="button" value="Browse"/> <input type="button" value="Capture"/>
First Name	<input type="text"/>	Last Name	<input type="text"/>	
Gender	<input type="text" value="-----"/>	Mobile Phone	<input type="text"/>	
Certificate Type	<input type="text" value="-----"/>	Certificate Number	<input type="text"/>	
Birthday	<input type="text"/>	Email	<input type="text"/>	
Device Verification Password	<input type="text" value="*****"/>	Card Number	<input type="text"/>	
Biometrics Type	<input type="text"/>			

Access Control

Time Attendance

Personnel Detail

Levels Settings <input checked="" type="checkbox"/> General <input checked="" type="checkbox"/> Test <input checked="" type="checkbox"/> 深圳 <input checked="" type="checkbox"/> office <input checked="" type="checkbox"/> a	<input type="button" value="Add"/> <input type="button" value="Select All"/> <input type="button" value="Unselect All"/>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td>Superuser</td> <td><input type="text" value="No"/></td> </tr> <tr> <td>Device Operation Role</td> <td><input type="text" value="Ordinary User"/></td> </tr> <tr> <td>Disabled</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Set Valid Time</td> <td><input type="checkbox"/></td> </tr> </table>	Superuser	<input type="text" value="No"/>	Device Operation Role	<input type="text" value="Ordinary User"/>	Disabled	<input type="checkbox"/>	Set Valid Time	<input type="checkbox"/>
Superuser	<input type="text" value="No"/>									
Device Operation Role	<input type="text" value="Ordinary User"/>									
Disabled	<input type="checkbox"/>									
Set Valid Time	<input type="checkbox"/>									

2. Заполните все обязательные поля и нажмите **[OK]**, чтобы зарегистрировать нового пользователя.
3. Нажмите **Доступ > Устройство > Контроль устройств > Синхронизировать все данные с устройствами**, чтобы синхронизировать все данные с устройством, включая новых пользователей.

Для получения более подробной информации, пожалуйста, см. *Руководство пользователя ZKBioAccess IVS*.

Приложение 1

Требования к динамическому сбору и регистрации изображений лица в видимом свете

- 1) Рекомендуется выполнять регистрацию в помещении с подходящим источником света без недоэкспонирования или переэкспонирования.
- 2) Не снимайте в сторону внешних источников света, таких как дверь или окно, или других сильных источников света.
- 3) Для регистрации рекомендуется одежда темного цвета, которая отличается от фоновго цвета.
- 4) Пожалуйста, держите открытым свое лицо и лоб и не прикрывайте лицо и брови волосами.
- 5) Рекомендуется показывать простое выражение лица. Улыбка приемлема, но не закрывайте глаза и не наклоняйте голову в какую-либо сторону. Для людей в очках требуются два изображения: одно изображение в очках, а другое - без очков.
- 6) Не носите аксессуары, такие как шарф или маску, которые могут закрывать рот или подбородок.
- 7) Поворачивайтесь вправо к устройству захвата и найдите свое лицо в области захвата изображения, как показано на Рис.1.
- 8) Не помещайте более одного лица в область захвата.
- 9) Рекомендуется 50–80 см для съемки на расстоянии, регулируемом в зависимости от роста.



Рис.1 Зона захвата лица

Требования к данным цифрового изображения лица в видимом свете

Цифровая фотография должна быть с прямыми краями, цветная, с изображением в полкорпуса только с одним человеком, и это лицо не должно быть схематичным и носить униформу. Люди, которые носят очки, должны оставаться в очках для фотосъемки.

- **Расстояние глаз**

Рекомендуется 200 пикселей или больше с расстоянием не менее 115 пикселей.

- **Выражение лица**

Рекомендуется нейтральное лицо или улыбка с естественно открытыми глазами.

- **Жесты и углы**

Угол поворота по горизонтали не должен превышать $\pm 10^\circ$, угол возвышения не должен превышать $\pm 10^\circ$, а угол тангажа не должен превышать $\pm 10^\circ$.

- **Аксессуары**

Использование масок и цветных очков запрещено. Оправа очков не должна закрывать глаза и отражать свет. Людям с толстой оправой очков рекомендуется сделать два изображения: одно в очках, а другое - без очков.

- **Лицо**

Полностью лицо с четким контуром, реальным масштабом, равномерно распределенным светом и отсутствием теней.

- **Формат изображения**

Должен быть в формате BMP, JPG или JPEG.

- **Требование к данным**

Необходимо соответствовать следующим требованиям:

- 1) Белый фон с темной одеждой.
- 2) 24-битный режим истинного цвета.
- 3) Сжатое изображение в формате JPG размером не более 20 КБ.
- 4) Разрешение должно быть от 358 x 441 до 1080 x 1920.
- 5) Вертикальный масштаб головы и тела должен быть 2:1.
- 6) Фотография должна включать плечи снимаемого человека на одном горизонтальном уровне.
- 7) Захваченный человек должен быть с открытыми глазами и с хорошо видимой радужной оболочкой.
- 8) Обычное лицо или улыбка предпочтительны, показ зубов нежелателен.
- 9) Снятый человек должен быть четко виден, иметь естественный цвет, без явных искажений изображения, без тени, светлого пятна или отражения на лице или фоне, а также с соответствующим уровнем контрастности и освещенности.

Политика конфиденциальности

Уведомление:

Для того, чтобы помочь вам лучше использовать продукты и услуги ZKTeco (далее «мы», «наш» или «нас»), поставщика интеллектуальных услуг, мы постоянно собираем вашу личную информацию. Поскольку мы понимаем важность вашей личной информации, мы искренне относимся к вашей конфиденциальности и сформулировали эту политику конфиденциальности для защиты вашей личной информации. Мы перечислили политику конфиденциальности ниже, чтобы точно понимать меры защиты данных и конфиденциальности, связанные с нашими интеллектуальными продуктами и услугами.

Перед использованием наших продуктов и услуг внимательно прочтите и примите все правила и положения настоящей Политики конфиденциальности. Если вы не согласны с соответствующим соглашением или любым из его условий, вы должны прекратить использование наших продуктов и услуг.

I. Собранная информация

Для того, чтобы обеспечить нормальную работу продукта и улучшить обслуживание, мы будем собирать информацию, добровольно предоставленную вами или предоставленную в соответствии с вашим разрешением во время регистрации и использования или созданную в результате использования вами услуг.

1. Регистрационная информация пользователя: при вашей первой регистрации шаблон функции (шаблон отпечатка пальца / шаблон лица / шаблон ладони) будет сохранен на устройстве в соответствии с типом устройства, которое вы выбрали, чтобы проверить уникальное сходство между вами и идентификатором пользователя, который вы зарегистрировались. При желании вы можете ввести свое имя и код. Вышеуказанная информация необходима для использования наших продуктов. Если вы не предоставите такую информацию, вы не сможете регулярно использовать некоторые функции продукта.
2. Информация о продукте: в соответствии с моделью продукта и предоставленным вами разрешением при установке и использовании наших услуг, соответствующая информация о продукте, на котором используются наши сервисы, будет собираться при подключении продукта к программному обеспечению, включая модель продукта. , Номер версии микропрограммы, серийный номер продукта и информацию о емкости продукта. Когда вы подключаете свой продукт к программному обеспечению, внимательно ознакомьтесь с политикой конфиденциальности для конкретного программного обеспечения.

II. Безопасность и управление продуктом

1. Когда вы впервые используете наши продукты, вы должны установить права администратора перед выполнением определенных операций. В противном случае вам часто будут напоминать о необходимости установить права администратора при входе в интерфейс главного меню. Если вы по-прежнему не установили права администратора после получения системного приглашения, вы должны знать о возможной угрозе безопасности (например, данные могут быть изменены вручную).

2. Все функции отображения биометрической информации в наших продуктах по умолчанию отключены. Вы можете выбрать «Меню» > «Системные настройки», чтобы указать, следует ли отображать биометрическую информацию. Если вы активируете эти функции, мы предполагаем, что вы знаете о рисках безопасности личной конфиденциальности, указанных в политике конфиденциальности.
3. По умолчанию отображается только ваш идентификатор пользователя. Вы можете указать, следует ли отображать другую информацию для проверки пользователя (например, имя, отдел, фото и т. д.) с правами администратора. Если вы решите отображать такую информацию, мы предполагаем, что вы знаете о потенциальных рисках безопасности (например, ваша фотография будет отображаться в интерфейсе устройства).
4. По умолчанию функция камеры отключена в наших продуктах. Если вы хотите включить эту функцию, чтобы делать снимки себя для записи посещаемости или снимать незнакомых людей для контроля доступа, продукт включит быстрый звуковой сигнал камеры. Как только вы включите эту функцию, мы предполагаем, что вы знаете о потенциальных рисках безопасности.
5. Все данные, собранные нашими продуктами, зашифрованы с использованием алгоритма AES 256. Все данные, загружаемые администратором в наши продукты, автоматически шифруются с использованием алгоритма AES 256 и надежно хранятся. Если администратор загружает данные из наших продуктов, мы предполагаем, что вам необходимо обработать данные и вы знаете о потенциальной угрозе безопасности. В таком случае вы берете на себя ответственность за хранение данных. Вы должны знать, что некоторые данные нельзя загрузить из соображений безопасности.
6. Вся личная информация в наших продуктах может быть запрошена, изменена или удалена. Если вы больше не пользуетесь нашими продуктами, пожалуйста, удалите свои личные данные.

III.

Наши устройства, веб-сайт и услуги в основном предназначены для взрослых. Несовершеннолетние не могут создавать собственные учетные записи без согласия родителей или опекунов. Если вы несовершеннолетний, рекомендуется попросить своих родителей или опекуна внимательно прочитать настоящую Политику и использовать наши услуги или информацию, предоставленную нами только с согласия ваших родителей или опекуна.

Мы будем использовать или раскрывать личную информацию несовершеннолетних, собранную с согласия их родителей или опекунов, только если такое использование или раскрытие разрешено законом или если мы получили явное согласие их родителей или опекунов, и такое использование или раскрытие информации осуществляется с целью защиты несовершеннолетних.

Узнав, что мы собрали личную информацию о несовершеннолетних без предварительного согласия проверяемых родителей, мы удалим такую информацию как можно скорее.

IV. Другое

Вы можете посетить https://www.zkteco.com/cn/index/Index/privacy_protection.html, чтобы узнать больше о том, как мы собираем, используем и безопасно храним вашу личную информацию. Чтобы идти в ногу с быстрым развитием технологий, корректировкой бизнес-операций и удовлетворять потребности клиентов, мы будем постоянно обдумывать и оптимизировать наши меры и политики защиты конфиденциальности. Приглашаем посетить наш официальный сайт в любое время, чтобы узнать о нашей последней политике конфиденциальности.



Экологически безопасная работа



Период экологичного использования (EFUP), обозначенный на этом устройстве, относится к периоду безопасности, в течение которого продукт используется в условиях, указанных в инструкциях по устройству, без утечки вредных и вредных веществ.

EFUP этого устройства не распространяется на расходные материалы, которые необходимо регулярно заменять, такие как батареи и т. д. EFUP батарей составляет 5 лет.

Названия и концентрация токсичных и опасных веществ или элементов

Название компонентов	Токсичные и опасные вещества или элементы					
	Свинец (Pb)	Ртуть (Hg)	Кадмий (Cd)	Шестивалентный хром (Cr6+)	Полибромир. дифенилы (PBB)	Полибромир. дифениловые эфиры (PBDE)
Чип резистор	×	○	○	○	○	○
Чип конденсатор	×	○	○	○	○	○
Чип индуктор	×	○	○	○	○	○
Чип диод	×	○	○	○	○	○
Компоненты ESD	×	○	○	○	○	○
Зуммер	×	○	○	○	○	○
Адаптер	×	○	○	○	○	○
Винты	○	○	○	×	○	○

○ : указывает, что это токсичное или опасное вещество, содержащееся во всех однородных материалах для этой части, ниже предельного требования в SJ / T11363-2006.

× : указывает, что это токсичное или опасное вещество, содержащееся по крайней мере в одном из однородных материалов для этой части, превышает предельное требование в SJ / T11363-2006.

Примечание: 80% деталей в этом продукте изготовлены из неопасных для окружающей среды материалов. Содержащиеся в них опасные вещества или элементы в настоящее время не могут быть заменены экологически чистыми материалами из-за технических или экономических ограничений.

Официальное представительство "ZKTECO CO.,LTD"

в России и СНГ: Тел. +7 (495) 132-31-33.

107078, г. Москва, ул. Новорязанская, д.18, стр. 5.

www.zkteco.ru

www.zkteco.com



Copyright © 2021 ZKTECO CO., LTD. All Rights Reserved.