

Руководство пользователя

SpeedFace-V3LM1 Series

Дата: Декабрь 2023

Версия документа: 1.0

Благодарим за выбор нашей продукции. Перед эксплуатацией внимательно ознакомьтесь с инструкцией. Следуйте указанным рекомендациям для обеспечения надлежащей работы изделия. Изображения в данном руководстве приведены исключительно в иллюстративных целях.

СОДЕРЖАНИЕ

1 ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ.....	4
1.1 РАСПОЛОЖЕНИЕ ПАЛЬЦА НА СКАНЕРЕ★.....	4
1.2 ПОЛОЖЕНИЕ ТЕЛА, ПОЗА И ВЫРАЖЕНИЕ ЛИЦА.....	5
1.3 РЕГИСТРАЦИЯ ЛИЦА.....	6
1.4 ИНТЕРФЕЙС ОЖИДАНИЯ.....	7
1.5 ВИРТУАЛЬНАЯ КЛАВИАТУРА.....	10
1.6 РЕЖИМ ВЕРИФИКАЦИИ	11
1.6.1 ВЕРИФИКАЦИЯ ПО ОТПЕЧАТКУ ПАЛЬЦА★	11
1.6.2 ВЕРИФИКАЦИЯ ПО ЛИЦУ.....	14
1.6.3 ВЕРИФИКАЦИЯ ПО КАРТЕ★	16
1.6.4 ВЕРИФИКАЦИЯ ПО QR-КОДУ★	19
1.6.5 ВЕРИФИКАЦИЯ ПО ПАРОЛЮ.....	19
1.6.6 КОМБИНИРОВАННАЯ ВЕРИФИКАЦИЯ.....	22
2 ОБЗОР.....	24
2.1 ВНЕШНИЙ ВИД	24
2.2 ОПИСАНИЕ КАБЕЛЕЙ ПОДКЛЮЧЕНИЯ И ПРОВОДКИ	25
2.2.1 КАБЕЛИ ПОДКЛЮЧЕНИЯ.....	25
2.2.2 ОПИСАНИЕ ПРОВОДКИ.....	27
3 УСТАНОВКА.....	31
3.1 УСЛОВИЯ УСТАНОВКИ.....	31
3.2 УСТАНОВКА УСТРОЙСТВА.....	31
4 ГЛАВНОЕ МЕНЮ.....	32
5 УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ	34
5.1 РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ.....	34
5.1.1 РЕГИСТРАЦИЯ ID И ИМЕНИ ПОЛЬЗОВАТЕЛЯ.....	34
5.1.2 РОЛЬ ПОЛЬЗОВАТЕЛЯ.....	35
5.1.3 РЕГИСТРАЦИЯ ОТПЕЧАТКА ПАЛЬЦА★.....	36
5.1.4 ЛИЦО	36

5.1.5 КАРТА★	37
5.1.6 ПАРОЛЬ.....	38
5.1.7 РОЛЬ КОНТРОЛЯ ДОСТУПА.....	39
5.2 ПОИСК ПОЛЬЗОВАТЕЛЯ.....	40
5.3 РЕДАКТИРОВАНИЕ ПОЛЬЗОВАТЕЛЯ.....	41
5.4 УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЯ.....	42
5.5 СТИЛЬ ОТОБРАЖЕНИЯ.....	43
6 РОЛЬ ПОЛЬЗОВАТЕЛЯ.....	45
7 НАСТРОЙКИ СВЯЗИ.....	48
7.1 НАСТРОЙКИ СЕТИ.....	48
7.2 ПОСЛЕДОВАТЕЛЬНЫЙ ПОРТ.....	50
7.3 ПОДКЛЮЧЕНИЕ К ПК.....	51
7.4 НАСТРОЙКИ WI-FI.....	52
7.5 НАСТРОЙКА ОБЛАЧНОГО СЕРВЕРА.....	56
7.6 НАСТРОЙКА WIEGAND.....	57
7.6.1 ВХОД WIEGAND.....	57
7.6.2 ВЫХОД WIEGAND.....	61
7.7 ДИАГНОСТИКА СЕТИ.....	62
8 НАСТРОЙКИ СИСТЕМЫ.....	63
8.1 ДАТА И ВРЕМЯ.....	64
8.2 НАСТРОЙКА ЖУРНАЛОВ ДОСТУПА	66
8.3 ПАРАМЕТРЫ ЛИЦА.....	68
8.4 ОТПЕЧАТОК ПАЛЬЦА★	72
8.5 СБРОС К ЗАВОДСКИМ НАСТРОЙКАМ.....	74
8.6 НАСТРОЙКИ БЕЗОПАСНОСТИ.....	75
9 НАСТРОЙКИ ПЕРСОНАЛИЗАЦИИ.....	77
9.1 НАСТРОЙКИ ИНТЕРФЕЙСА.....	77
9.2 НАСТРОЙКИ ГОЛОСА.....	79
9.3 РАСПИСАНИЕ ЗВОНКОВ.....	80
9.4 ПАРАМЕТРЫ ОТМЕТКИ.....	82
9.5 НАЗНАЧЕНИЕ ГОРЯЧИХ КЛАВИШ.....	84
10 УПРАВЛЕНИЕ ДАННЫМИ.....	88
10.1 УДАЛЕНИЕ ДАННЫХ.....	88

11 КОНТРОЛЬ ДОСТУПА.....	90
11.1 ОПЦИИ КОНТРОЛЯ ДОСТУПА.....	91
11.2 РАСПИСАНИЕ ВРЕМЕНИ.....	94
11.3 ПРАЗДНИЧНЫЕ ДНИ.....	96
11.4 КОМБИНИРОВАННАЯ ВЕРИФИКАЦИЯ.....	97
11.5 НАСТРОЙКА ЗАПРЕТА ПОВТОРНОГО ПРОХОДА.....	99
11.6 НАСТРОЙКИ ПАРАМЕТРОВ СИГНАЛА ТРЕВОГИ.....	101
12 МЕНЕДЖЕР USB.....	103
12.1 ЗАГРУЗКА.....	103
12.2 ЗАГРУЗКА НА УСТРОЙСТВО.....	104
13 ПОИСК ОТМЕТОК.....	105
14 АВТОТЕСТ.....	107
15 СИСТЕМНАЯ ИНФОРМАЦИЯ.....	109
16 ПОДКЛЮЧЕНИЕ К ПО ZKBIO CVACCESS.....	110
16.1 НАСТРОЙКА АДРЕСА СВЯЗИ.....	110
16.2 ДОБАВЛЕНИЕ УСТРОЙСТВА В ПРОГРАММЕ.....	111
16.3 ДОБАВЛЕНИЕ ПЕРСОНАЛА В ПРОГРАММЕ.....	112
16.4 МОБИЛЬНЫЙ ИДЕНТИФИКАТОР★	113
ПРИЛОЖЕНИЕ 1.....	118
ТРЕБОВАНИЯ К ЖИВОЙ РЕГИСТРАЦИИ И СБОРУ ШАБЛОНОВ ЛИЦА В ВИДИМОМ СВЕТЕ	118
ТРЕБОВАНИЯ К ЦИФРОВЫМ ШАБЛОНАМ ЛИЦА В ВИДИМОМ СВЕТЕ.....	119

1 Инструкция по эксплуатации

Прежде чем приступить к изучению функций устройства, рекомендуется ознакомиться со следующими основными принципами.

1.1 Расположение пальца на сканере ★

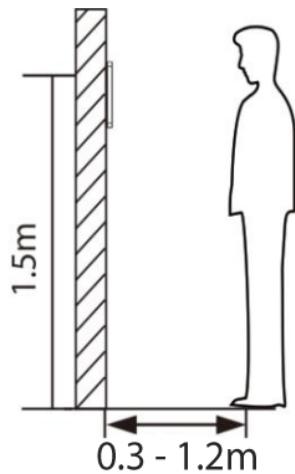
Для сканирования рекомендуется использовать указательный, средний или безымянный палец. Следует избегать использования большого пальца или мизинца, так как их сложно правильно расположить на сканере отпечатков.



Примечание: При регистрации и идентификации отпечатков пальцев необходимо правильно прикладывать палец к сканеру. Наша компания не несет ответственности за проблемы с распознаванием, вызванные нарушением правил эксплуатации. За компанией сохраняется право окончательного толкования и внесения изменений в данное положение.

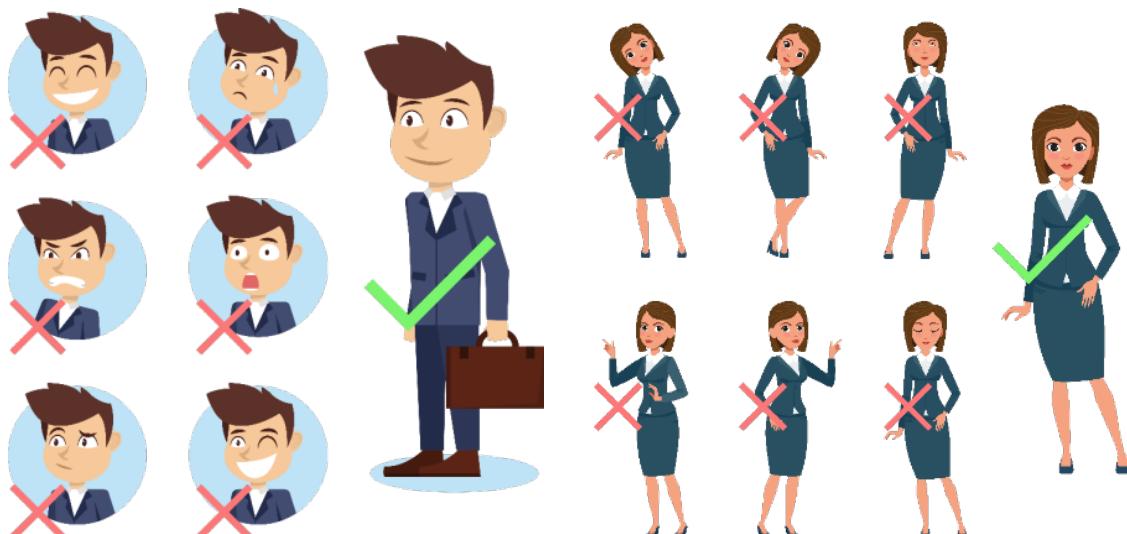
1.2 Положение тела, поза и выражение лица

➤ Рекомендуемое расстояние



Расстояние между устройством и пользователем ростом от 1,55 м до 1,85 м должно составлять от 0,3 м до 1,2 м. Пользователи могут немного приближаться или отдаляться для улучшения характеристик захватываемых изображений лица.

➤ Рекомендуемое выражение лица и поза



Выражение лица

Поза стоя

Примечание: Сохраняйте естественное выражение лица и позу во время регистрации или верификации.

1.3 Регистрация лица

Держите лицо в центре экрана во время регистрации. Смотрите прямо в камеру и оставайтесь неподвижны во время регистрации шаблона лица. Экран должен выглядеть следующим образом:



Правильная процедура регистрации и аутентификации шаблона лица

➤ Рекомендации по регистрации лица

- При регистрации лица соблюдайте расстояние от 50 см до 80 см между устройством и лицом.
- Сохраняйте естественное выражение лица без изменений (улыбка, гримасы, подмигивания и т.д.).
- При несоблюдении инструкций на экране регистрация лица может занять больше времени или завершиться неудачей.
- Следите, чтобы волосы или другие объекты не закрывали глаза и брови.

Не надевайте головные уборы, маски, солнцезащитные очки или обычные очки.

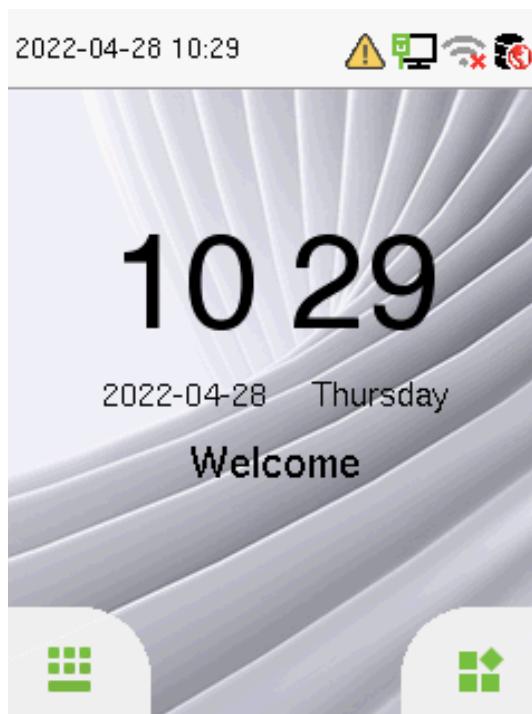
- Следите, чтобы в кадре не отображалось два лица. Регистрируйте по одному человеку.
- Пользователям в очках рекомендуется зарегистрировать лицо как в очках, так и без очков.

➤ **Рекомендации по аутентификации лица**

- Убедитесь, что лицо находится внутри направляющей линии, отображаемой на экране устройства.
- В некоторых случаях аутентификация может быть неудачной из-за смены очков по сравнению с теми, что были надеты при регистрации. В таком случае может потребоваться пройти аутентификацию в ранее использовавшихся очках. Если регистрация проводилась без очков, то и аутентификацию следует проходить без очков.
- Если часть лица закрыта головным убором, маской, повязкой на глаз или солнцезащитными очками, аутентификация может быть неудачной. Не закрывайте лицо, позвольте устройству распознать как брови, так и все лицо.

1.4 Интерфейс ожидания

После подключения питания отображается следующий интерфейс ожидания:



- Нажмите  , чтобы перейти к интерфейсу ввода ID пользователя
- Когда в устройстве не задан Супер-администратор, нажмите на  , чтобы перейти в меню.
- После добавления Супер-администратора на устройстве требуется верификация Супер-администратора для доступа к функциям меню.



Примечание: В целях безопасности устройства рекомендуется зарегистрировать супер-администратора при первом использовании устройства.

- Параметры состояния отметки также могут отображаться и использоваться непосредственно в интерфейсе ожидания. Нажмите в любом месте экрана, кроме значков, чтобы на экране появились шесть клавиш быстрого доступа, как показано на рисунке ниже:



• Нажмите соответствующую клавишу состояния отметки, чтобы выбрать ваше текущее состояние. Выбранное состояние будет отображаться зеленым цветом. Конкретный метод работы см. в разделе «Назначение клавиш быстрого доступа» ("Shortcut Key Mappings").

Примечание: Опции состояния отметки отключены по умолчанию. Для их отображения на экране ожидания необходимо выбрать другой режим в разделе «Опция состояния отметки» ("Punch State Option").

1.5 Виртуальная клавиатура



Примечание: Устройство поддерживает ввод на английском языке, цифр и символов.

- Нажмите **[EN]**, чтобы переключиться на цифровую клавиатуру.
- Нажмите **[123]**, чтобы переключиться на символьную клавиатуру.
- Нажмите **[@#&]**, чтобы вернуться к английской клавиатуре.
- Нажмите на , чтобы выйти из виртуальной клавиатуры.

1.6 Режим верификации

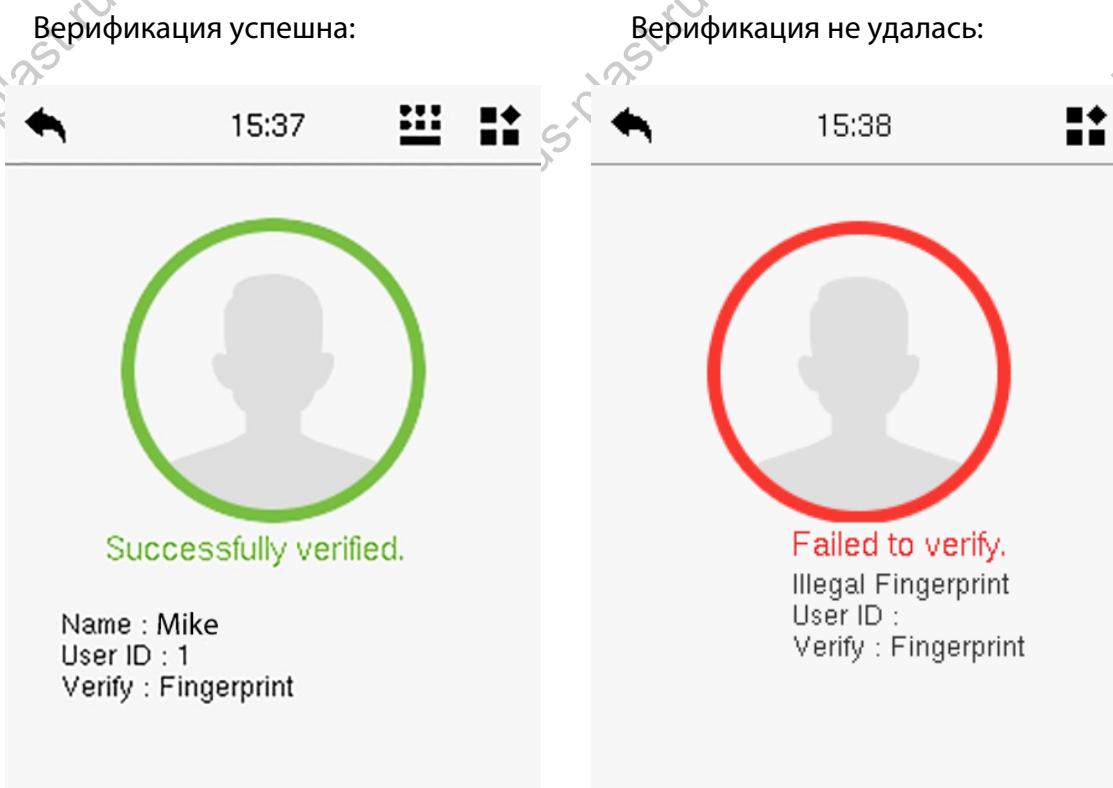
1.6.1 Верификация по отпечатку пальца★

- **Режим верификации по отпечатку 1:N**

Устройство сравнивает представленный отпечаток пальца с отпечатками, хранящимися в его базе данных.

Режим аутентификации по отпечатку пальца активируется, когда пользователь прикладывает палец к сканеру.

Следуйте рекомендуемому способу прикладывания пальца к датчику. Подробности смотрите в разделе **Позиционирование пальца**.



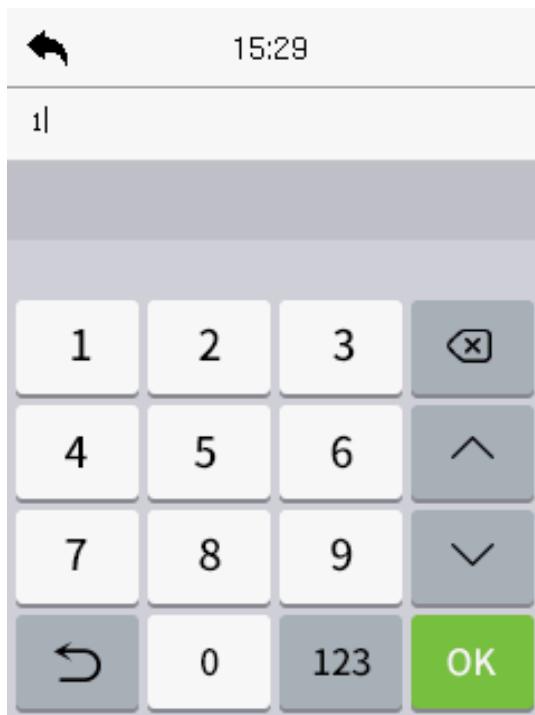
- **Режим верификации по отпечатку 1:1**

Устройство сравнивает текущий отпечаток пальца с отпечатками, привязанными к введенному ID пользователя, с помощью виртуальной клавиатуры.

Если пользователи не могут получить доступ с помощью метода аутентификации 1:N, они могут попытаться подтвердить свою личность с помощью режима верификации 1:1.

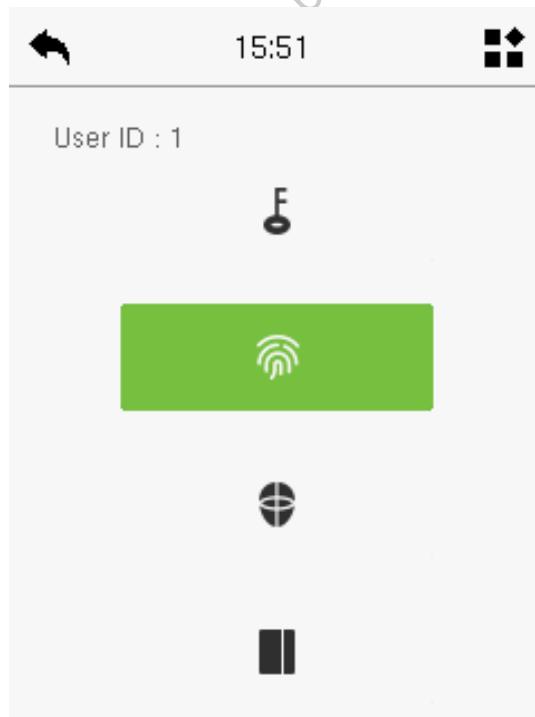
Нажмите  на главном экране, чтобы войти в режим верификации по отпечатку 1:1.

Введите идентификатор пользователя и нажмите **OK**.



Если пользователь зарегистрировал шаблон лица и пароль в дополнение к своим отпечаткам пальцев, и метод верификации установлен как «Пароль/Отпечаток/Шаблон лица», появится следующий экран.

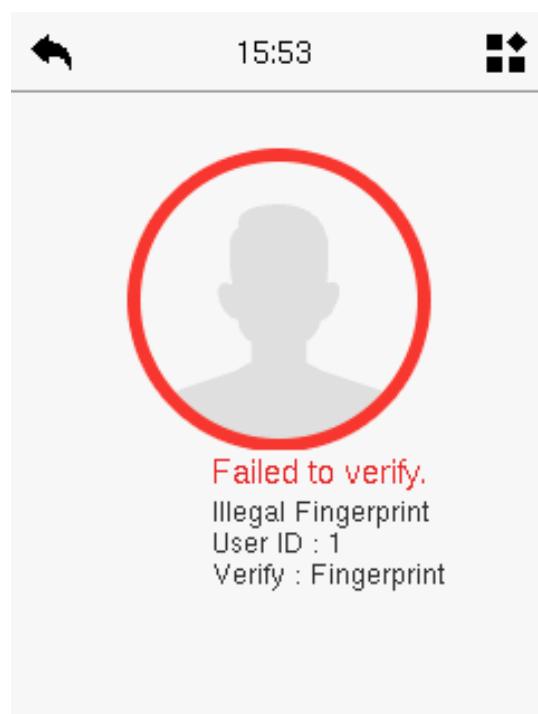
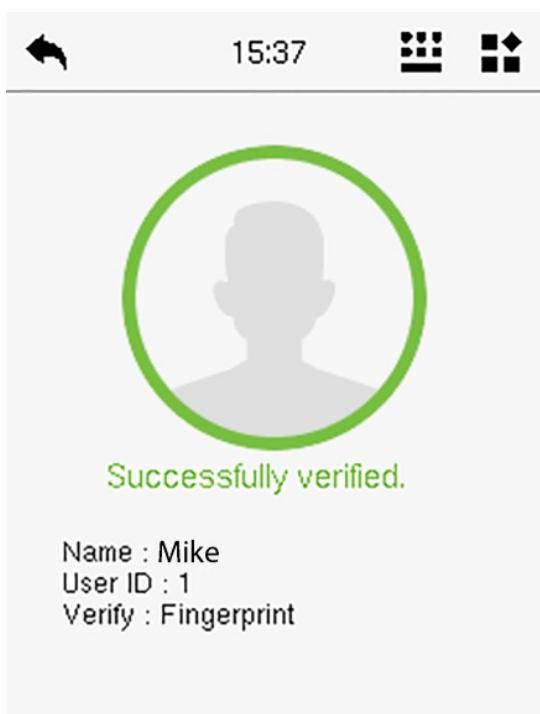
Выберите  значок отпечатка пальца для перехода в режим верификации по отпечатку.



Приложите палец для верификации.

Верификация успешна:

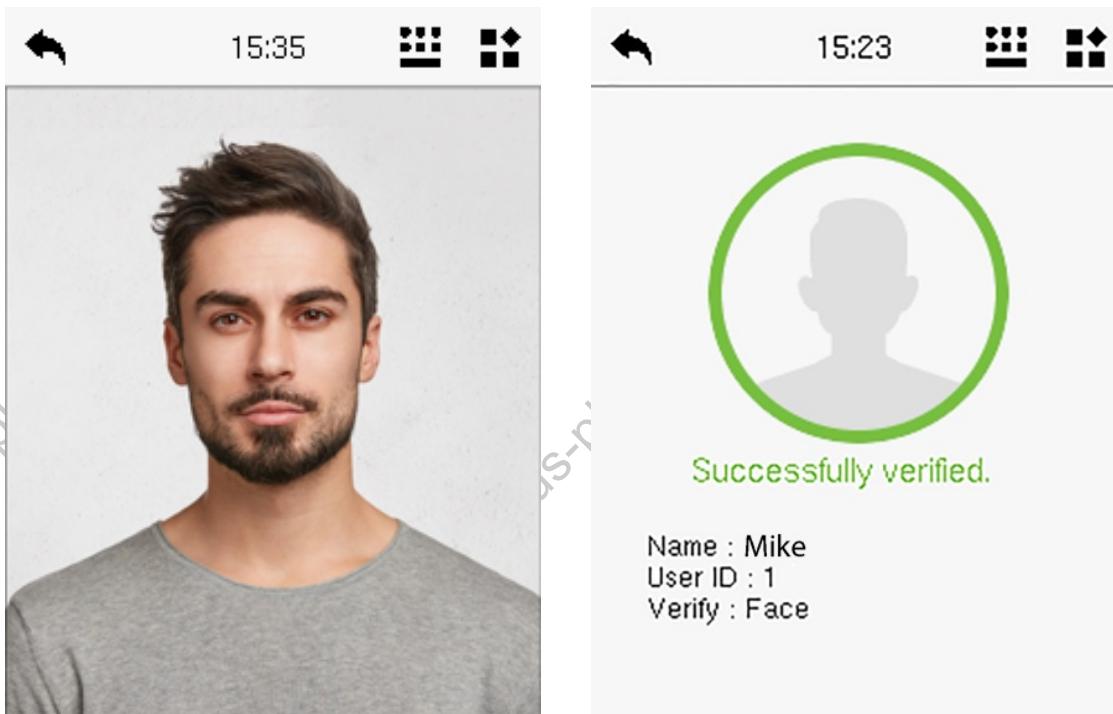
Верификация не удалась:



1.6.2 Верификация по лицу

➤ Режим верификации по лицу 1:N

В этом режиме выполняется сравнение полученного шаблона лица со всеми зарегистрированными в устройстве шаблонами. Ниже приведено всплывающее окно с результатами сравнения.



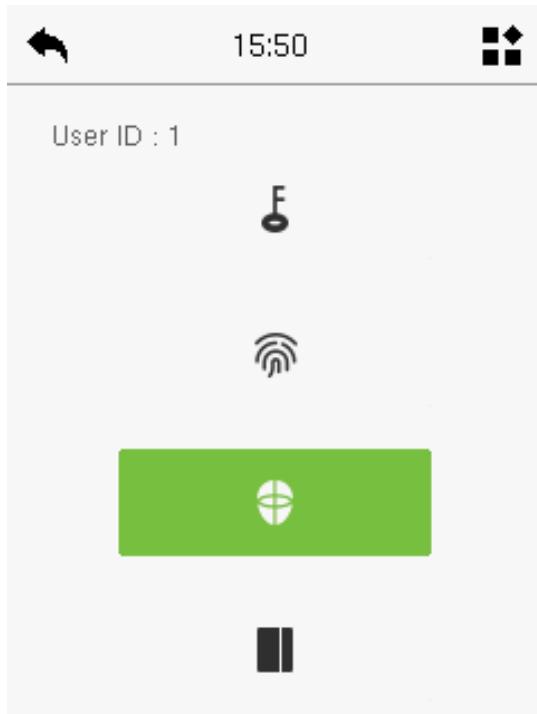
➤ Режим верификации по лицу 1:1

Сравнивает лицо, захваченное камерой, с шаблоном лица, связанным с введенным ID пользователя.

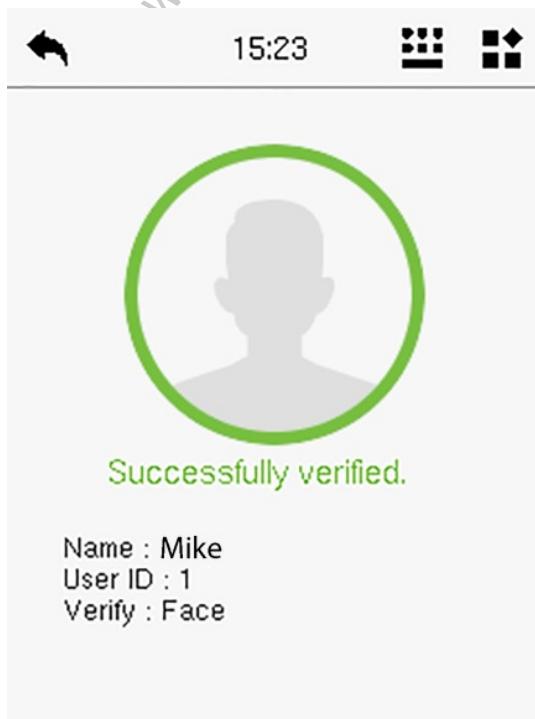
Нажмите на главном экране, чтобы войти в режим верификации по лицу 1:1. Введите ID пользователя и нажмите [OK].



Если сотрудник зарегистрировал отпечаток пальца, пароль и карту в дополнение к шаблону лица, появится следующий экран. Выберите  , чтобы войти в режим верификации по лицу.



После успешной верификации во всплывающем окне отобразится сообщение «**Верификация успешна**» ("Successfully Verified."), как показано ниже:

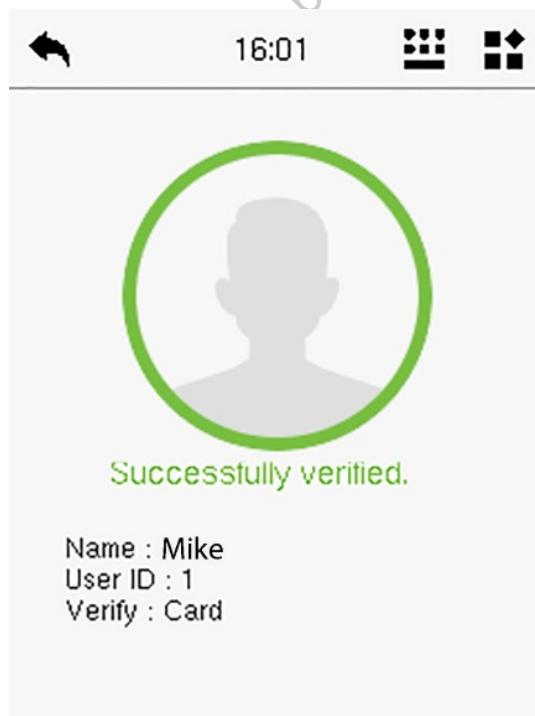


Если верификация не удалась, появляется сообщение: «Пожалуйста, скорректируйте ваше положение!» ("Please adjust your position!").

1.6.3 Вериfикация по карте★

➤ Режим верификации по карте 1:N

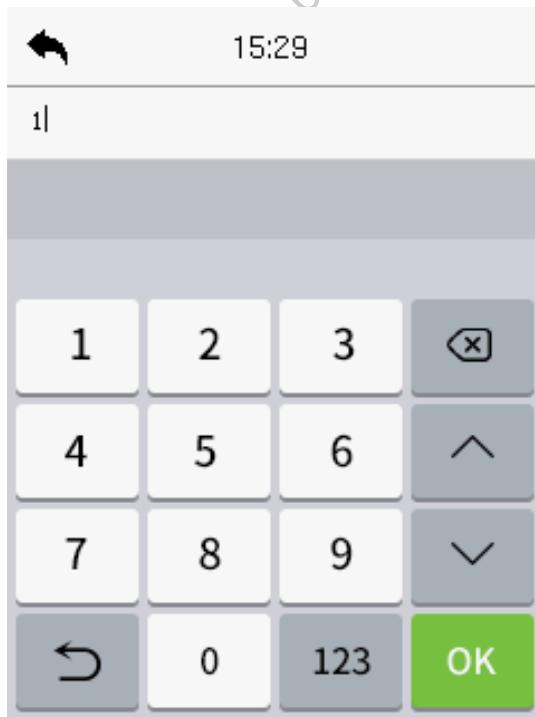
Режим верификации по карте 1:N сравнивает номер карты в зоне считывания со всеми номерами карт, зарегистрированными в устройстве. Ниже приведен экран верификации по карте.



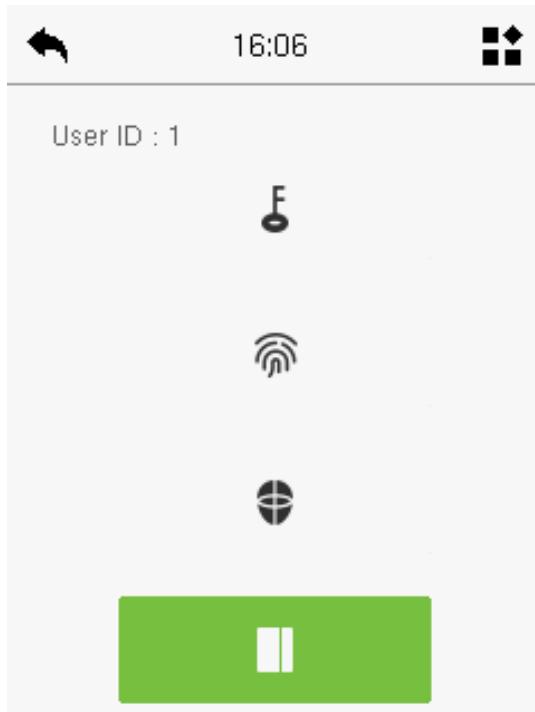
Режим верификации по карте 1:1

Режим верификации по карте 1:1 сравнивает номер карты в зоне считывания с номером, привязанным к зарегистрированному в устройстве ID пользователя сотрудника.

Нажмите  на главном экране, чтобы войти в режим верификации по карте 1:1. Введите ID пользователя и нажмите **[OK]**.



Если сотрудник зарегистрировал отпечаток пальца, шаблон лица и пароль в дополнение к карте, появится следующий экран. Выберите  , чтобы войти в режим верификации по карте.



1.6.4 Верификация по QR-коду★

В этом режиме верификации устройство сравнивает изображение QR-кода, полученное сканером, со всеми данными QR-кодов, хранящимися в устройстве.

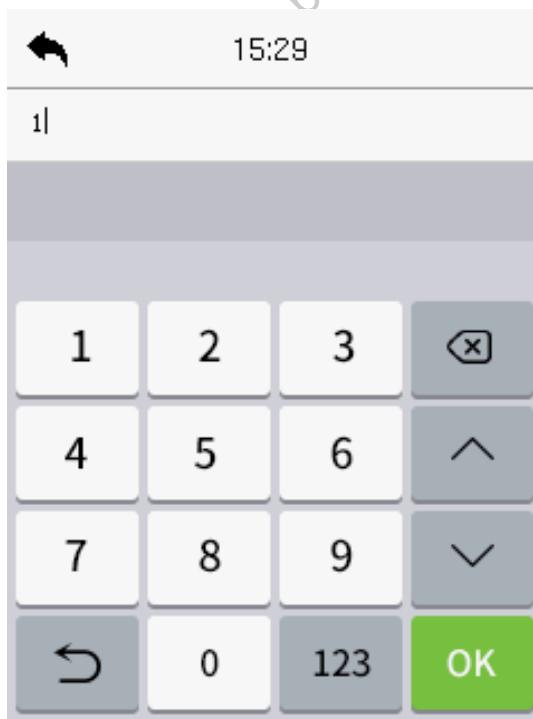
Нажмите **Mobile Credential (Мобильный пропуск)** на странице ZKBioAccess Mobile — появится QR-код, содержащий информацию об ID сотрудника и номере карты (статический QR-код содержит только номер карты). Этот QR-код может заменить физическую карту на определенном устройстве для осуществления бесконтактной аутентификации.



1.6.5 Верификация по паролю

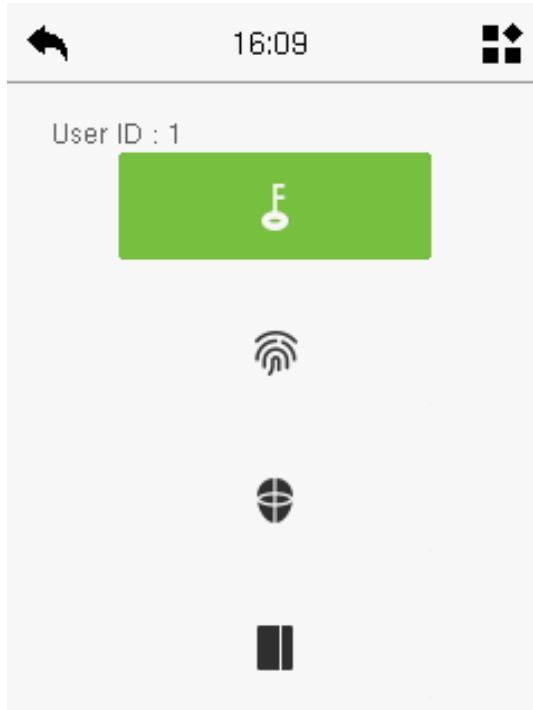
Устройство сравнивает введенный пароль с зарегистрированным паролем для указанного ID пользователя.

Нажмите на главном экране, чтобы войти в режим верификации по паролю 1:1. Затем введите ID пользователя и нажмите **[OK]**.



Если сотрудник зарегистрировал отпечаток пальца, шаблон лица и карту в дополнение к паролю, появится следующий экран.

Выберите , чтобы войти в режим верификации по паролю.

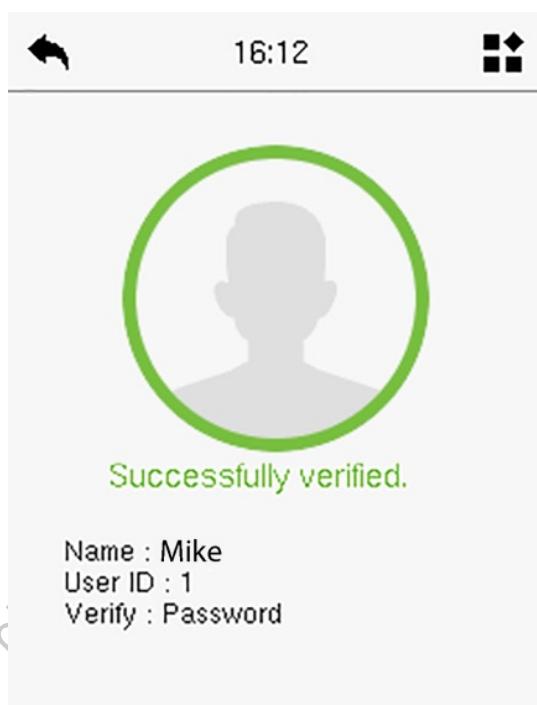


Введите пароль и нажмите **[OK]**.

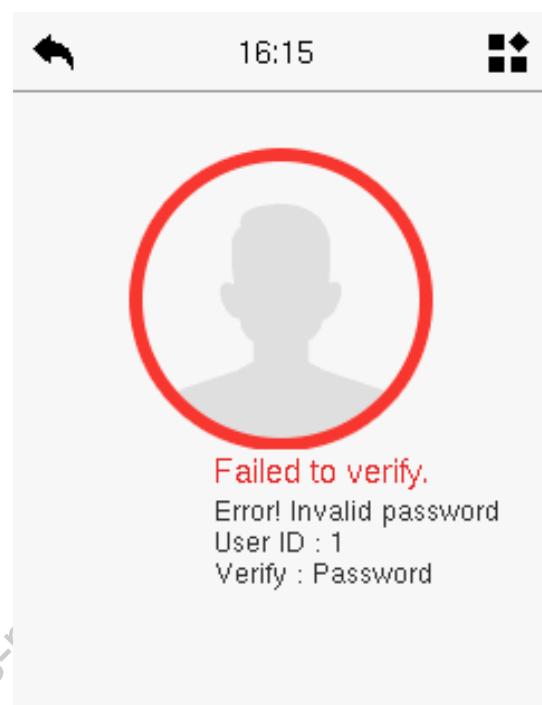


Ниже приведены экраны, отображаемые после ввода правильного и неправильного пароля соответственно.

Верификация успешна:



Верификация не удалась:

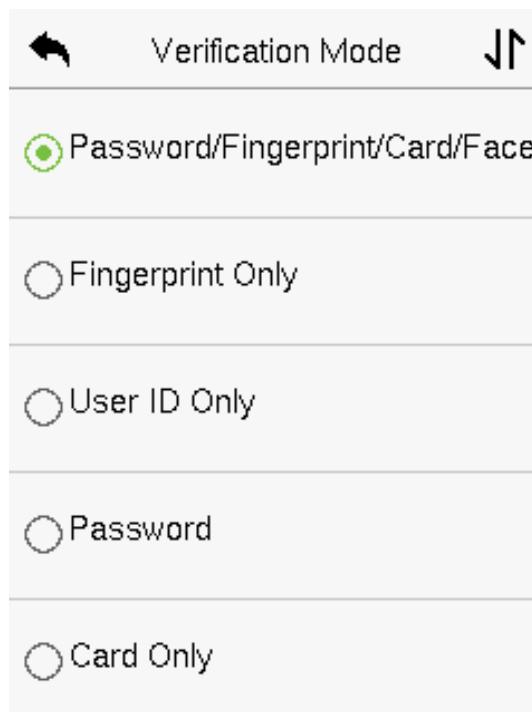


1.6.6 Комбинированная верификация

Данное устройство позволяет использовать различные методы верификации для повышения уровня безопасности. Всего доступно 21 различная комбинация верификации, как указано ниже:

Определение символов для комбинированной верификации

Символ	Определение	Пояснение
/	or	Этот метод сравнивает введенные данные верификации человека с соответствующим шаблоном верификации, ранее сохраненным для данного ID сотрудника в устройстве.
+	and	Этот метод сравнивает введенные данные верификации человека со всеми шаблонами верификации, ранее сохраненными для данного ID сотрудника в устройстве.



Процедура настройки комбинированного режима верификации

- Комбинированная верификация требует, чтобы сотрудник был зарегистрирован по всем указанным в настройках методам. В противном случае сотрудник не сможет успешно пройти процесс комбинированной верификации.
- Например, если сотрудник зарегистрировал только данные шаблона лица, а режим верификации устройства установлен как «Лицо + Пароль», сотрудник не сможет успешно завершить процесс верификации.
- Это происходит потому, что устройство сравнивает шаблон лица человека с зарегистрированным шаблоном верификации (как шаблон лица, так и пароль), ранее сохраненным для данного ID сотрудника.
- Но так как сотрудник зарегистрировал только шаблон лица, но не пароль, верификация не будет завершена, и устройство отобразит сообщение **"Verification Failed" (Верификация не удалась)**.

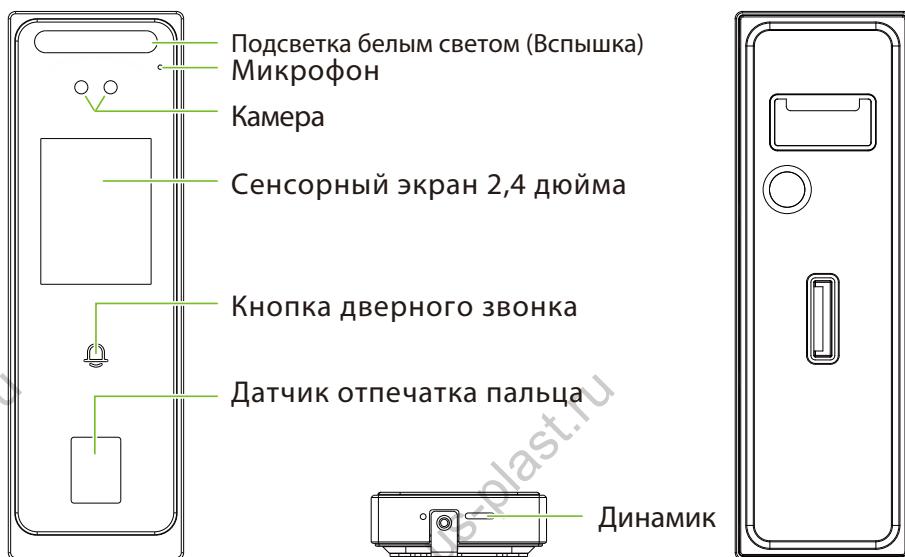
2 Обзор

2.1 Внешний вид

SpeedFace V3L:

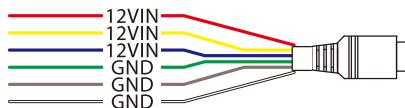


SpeedFace V3LM1:



2.2 Описание кабелей подключения и проводки

2.2.1 Кабели подключения



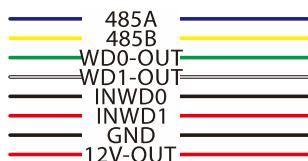
Контакт	Описание
6	Power In (Вход питания)



Контакт	Описание
4	Network (Сеть)



Контакт	Описание
4	USB



Контакт	Описание
8	485A 485B

WD0-OUT	Выход Wiegand, Вход Wiegand
WD1-OUT	
INWD0	
INWD1	
GND	
12V-OUT	



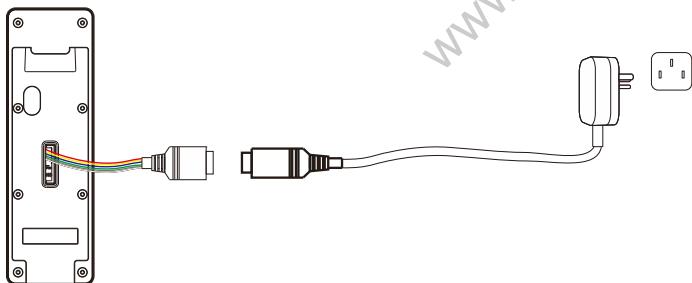
Контакт	Описание	
12	NC	Замок
	COM	
	NO	
	SEN	
	GND	
	BUT	
	AUX	
	GND	
Датчик двери, Кнопка выхода и Дополнительный вход		

BELL+	Звонок
BELL-	
ALARM+	
ALARM-	Тревога

2.2.2 Описание проводки

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

Подключение питания

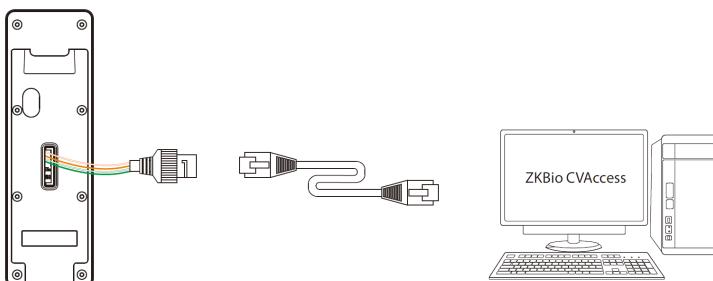


Рекомендуемый сетевой адаптер

1. $12V \pm 10\%$, не менее 1500 мА.
2. Для совместного использования питания с другими устройствами применяйте сетевой адаптер с более высоким номинальным током.

➤ Подключение по Ethernet

Подключите устройство и программное обеспечение на компьютере с помощью кабеля Ethernet. Как показано в примере ниже:



Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0

IP address: 192.168.1.130
Subnet mask: 255.255.255.0

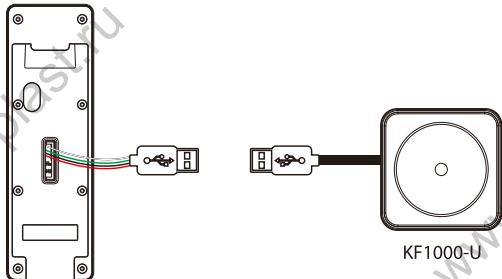
Нажмите [COMM.] > [Ethernet] > [IP Address], введите IP-адрес и нажмите [OK].

Примечание: При подключении к программному обеспечению ZKBio CVAccess в локальной сети IP-адреса сервера (ПК) и устройства должны находиться в одной подсети.

➤ **Подключение по USB**

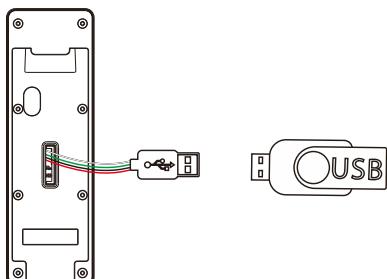
Устройство поддерживает подключение считывателя KF1000-U★ и USB-накопителя.

Считыватель KF1000-U★:



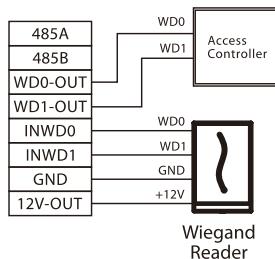
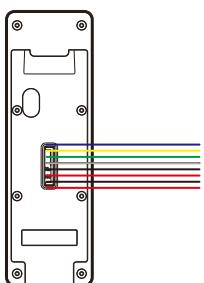
За подробностями обращайтесь к руководству пользователя KF1000-U.

USB-накопитель:



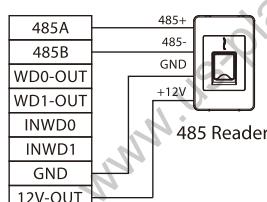
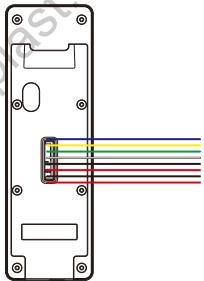
➤ Подключение RS485 и Wiegand

RS485:



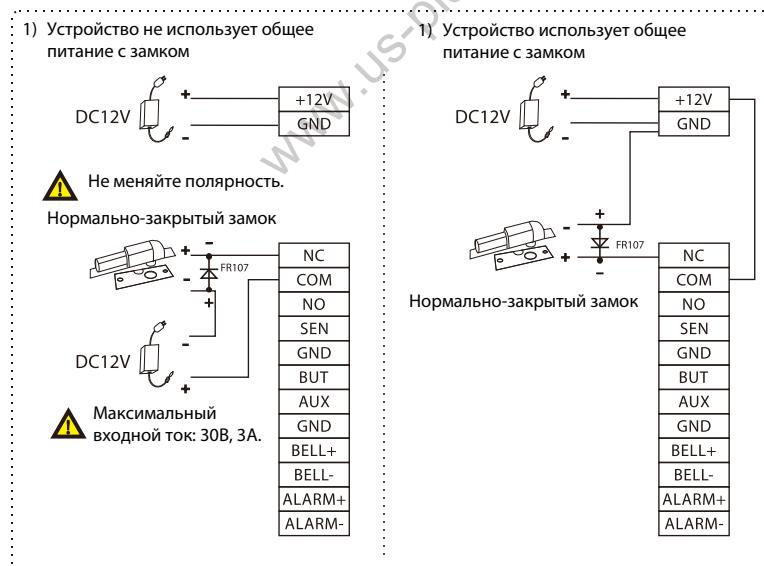
Примечание: Контакты 485A и 485B могут быть подключены либо к шлагбауму, либо к считывателю 485 по отдельности, но не могут быть подключены к шлагбауму и считывателю одновременно.

Wiegand:

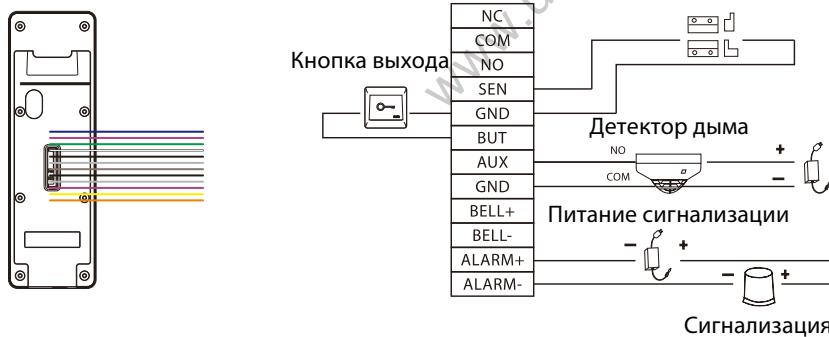


➤ Подключение реле замка

Система поддерживает нормально-разомкнутые (НО) и нормально-замкнутые (НЗ) замки. Нормально-открытый замок (разблокирован при подаче питания) подключается к клеммам 'NO' и 'COM', а нормально-закрытый замок (заблокирован при подаче питания) — к клеммам 'NC' и 'COM'. В качестве примера ниже приведено подключение НЗ замка:



➤ **Подключение датчика двери, кнопки выхода, сигнализации и вспомогательных устройств**



3 Монтаж

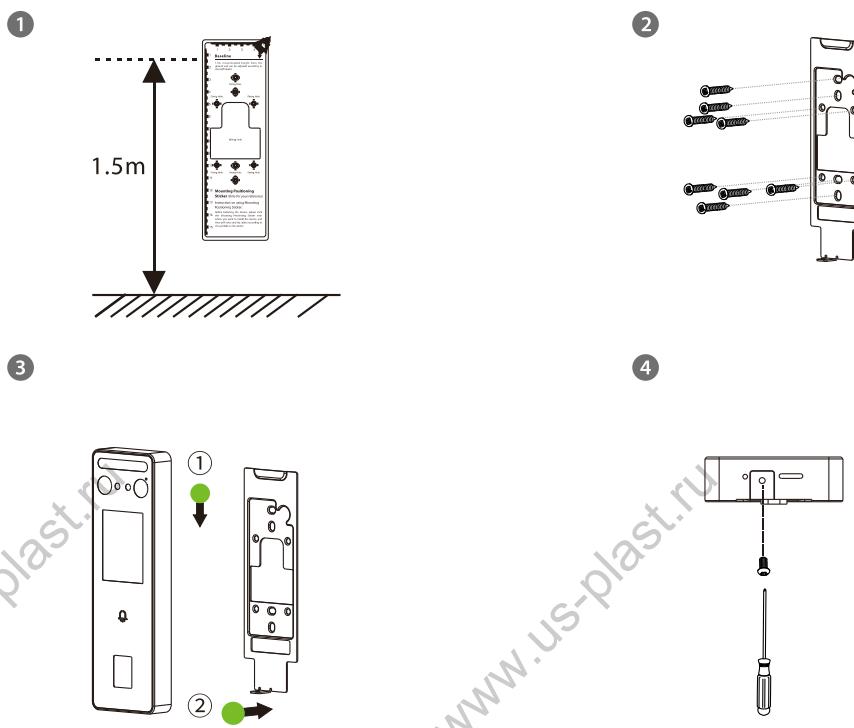
3.1 Условия установки

Рекомендации по установке приведены ниже.



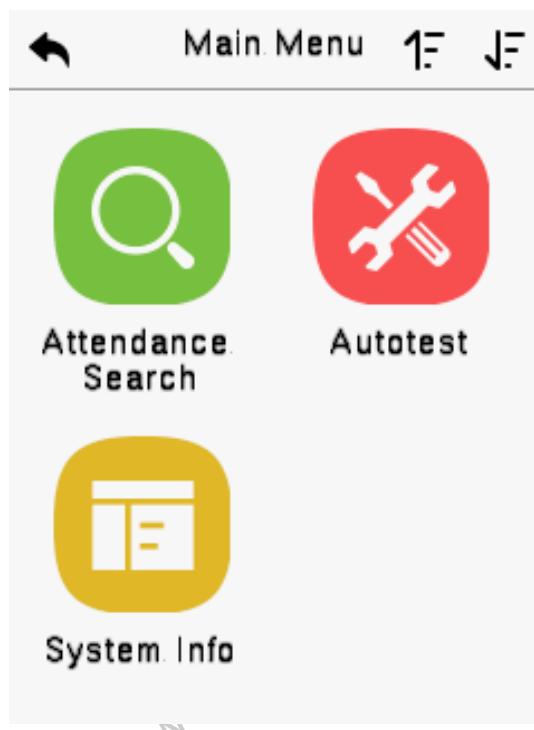
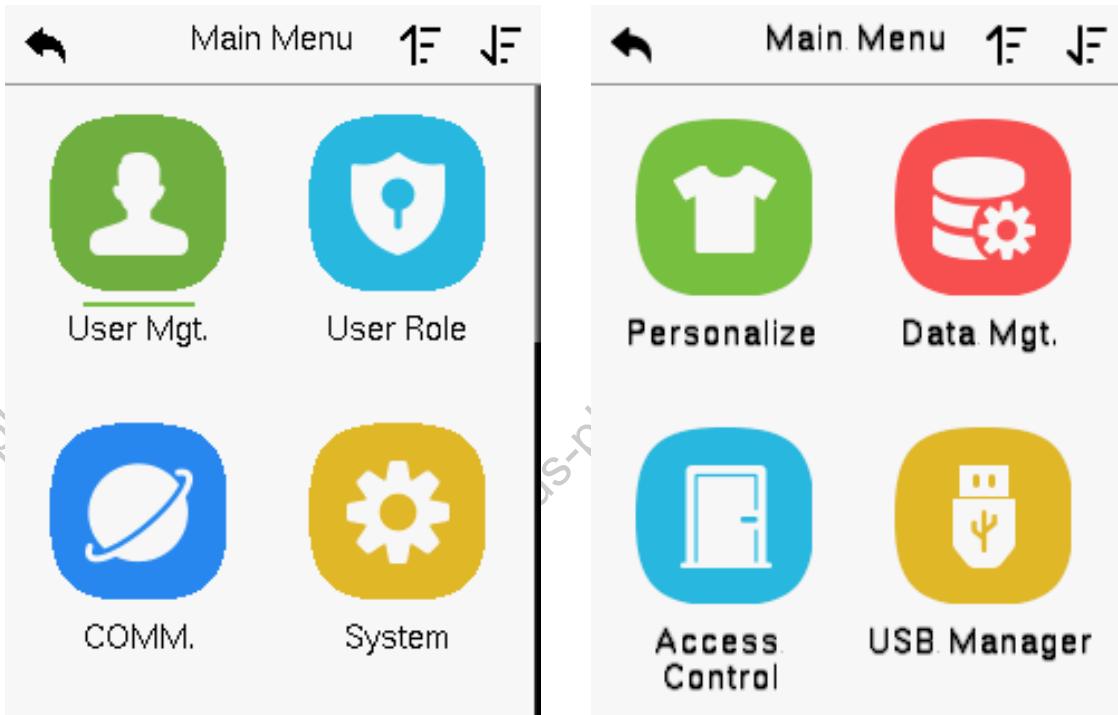
3.2 Установка устройства

1. Прикрепите монтажный шаблон (стикер) к стене и просверлите отверстия в соответствии с ним.
2. Закрепите монтажную пластину на стене с помощью винтов.
3. Установите устройство на монтажную пластину.
4. Зафиксируйте устройство на пластине защитным винтом.



4 Главное меню

Нажмите  на начальном экране, чтобы войти в главное меню (**main menu**), как показано ниже:



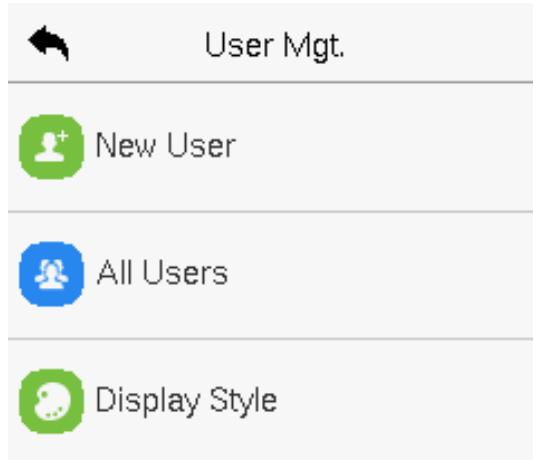
Function Description

Меню	Описание
User Mgt. Управление пользователями	Добавление, редактирование, просмотр и удаление информации о пользователе.
User Role Роль пользователя	Настройка области прав для пользовательской роли и регистратора: определение прав на операции в системе.
COMM. Связь	Настройка параметров сети, последовательной связи, подключения к ПК, Wi-Fi, облачного сервера, Wiegand и диагностики сети.
System Система	Настройка системных параметров: дата и время, журналы доступа, параметры лица и отпечатков, параметры видеодомофона, безопасность, сброс к заводским настройкам.
Personalize Персонализация	Настройка интерфейса пользователя, звука, расписания звонков, опций состояния отметки и назначения горячих клавиш.
Data Mgt. Управление данными	Удаление всех соответствующих данных на устройстве.
Access Control Контроль доступа	Настройка параметров замка и связанных устройств контроля доступа: расписания, праздничные дни, комбинированная верификация, предотвращение проноса (Anti-Passback), настройки экстренной сигнализации.
USB Manager Менеджер USB	Загрузка или выгрузка данных с USB-накопителя.
Attendance Search Поиск по отметкам	Запрос определенных журналов событий.
Autotest Автотест	Автоматическая проверка работы модулей: экран, звук, микрофон, датчик отпечатка, камера, часы реального времени.
System Info Информация о системе	Просмотр политики конфиденциальности, объема данных, сведений об устройстве и прошивке.

5 Управление пользователями

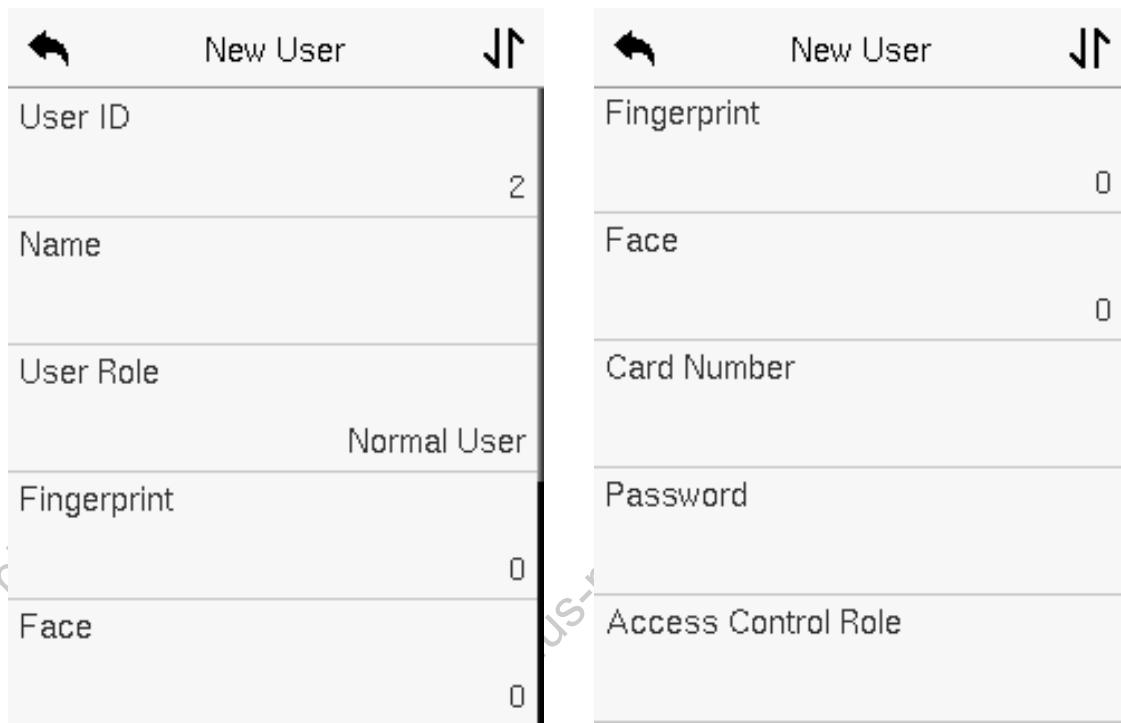
5.1 Регистрация пользователя

Нажмите **User Mgt.** (Управление пользователями) в главном меню.



5.1.1 Регистрация ID и имени пользователя

Нажмите **New User** (Новый пользователь) и введите **User ID** (ID пользователя) и **Name** (Имя).



The image contains two side-by-side registration forms for a new user.

Left Form (User ID screen):

User ID	2
Name	
User Role	Normal User
Fingerprint	0
Face	0

Right Form (Remaining fields):

Fingerprint	0
Face	0
Card Number	
Password	
Access Control Role	

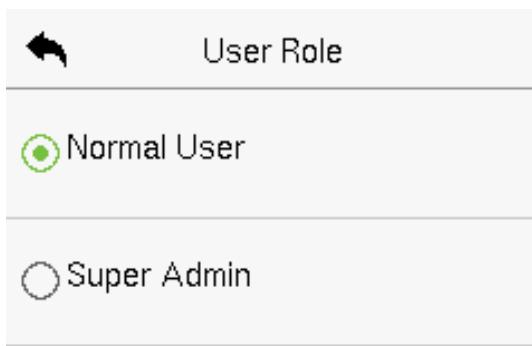
Примечание:

- 1) Имя может содержать до 36 символов.
- 2) ID пользователя по умолчанию может содержать от 1 до 14 символов (цифры и буквы).
- 3) ID можно изменить только во время первоначальной регистрации, но не после ее завершения.
- 4) Если появляется сообщение "**Duplicated!** (Дубликат)", необходимо выбрать другой ID, так как введенный уже существует.

5.1.2 Роль пользователя

В интерфейсе **New User** (Новый пользователь) нажмите **User Role** (Роль пользователя), чтобы назначить пользователю роль: **Normal User** (Обычный пользователь) или **Super Admin** (Супер-администратор).

- **Супер-администратор** (Super Admin): Обладает всеми правами управления на устройстве.
- **Обычный пользователь** (Normal User): Если на устройстве уже зарегистрирован Супер-администратор, обычные пользователи не имеют прав на управление системой и могут выполнять только операции верификации.
- **Пользовательские роли** (User Defined Roles): Обычному пользователю также могут быть назначены пользовательские роли. В этом случае пользователю можно разрешить доступ к определенным пунктам меню по необходимости.

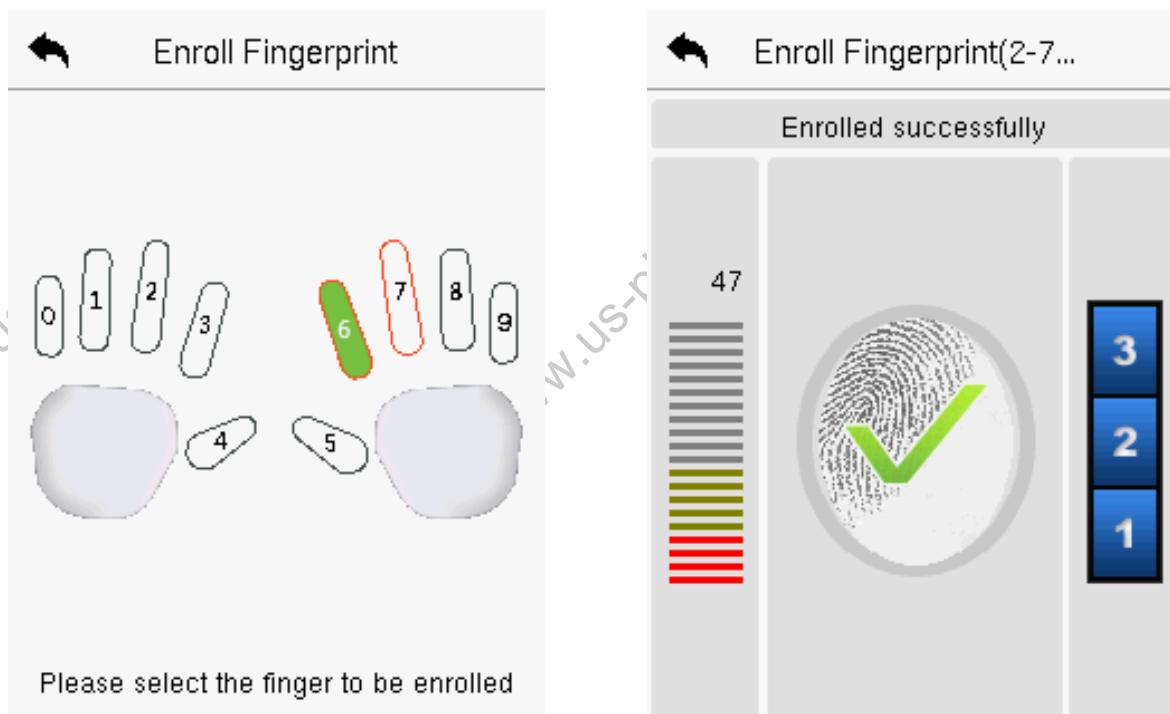


Примечание: Если выбранная роль — **Супер-администратор** (Super Admin), то для доступа к главному меню пользователь должен пройти аутентификацию. Аутентификация основана на методах верификации, которые зарегистрировал супер-администратор.

5.1.3 Регистрация отпечатка пальца★

Нажмите **Fingerprint** (Отпечаток пальца) в интерфейсе **New User** (Новый пользователь), чтобы перейти на страницу регистрации отпечатка.

- Выберите палец для регистрации.
- Приложите один и тот же палец к считывателю отпечатков три раза.
- Зеленый индикатор означает, что отпечаток успешно зарегистрирован.



5.1.4 Лицо

Нажмите **Face** (Лицо) в интерфейсе **New User** (Новый пользователь), чтобы перейти на страницу регистрации лица.

- Смотрите прямо в камеру и расположитесь так, чтобы изображение вашего лица находилось внутри белой направляющей рамки и оставалось неподвижным во время регистрации.
- Во время регистрации появится индикатор выполнения, и по его завершении отобразится сообщение "**Успешно зарегистрировано**" ("**Enrolled Successfully**").

- Если лицо уже зарегистрировано, появится сообщение "**Дубликат лица**" ("**Duplicated Face**"). Интерфейс регистрации выглядит следующим образом:

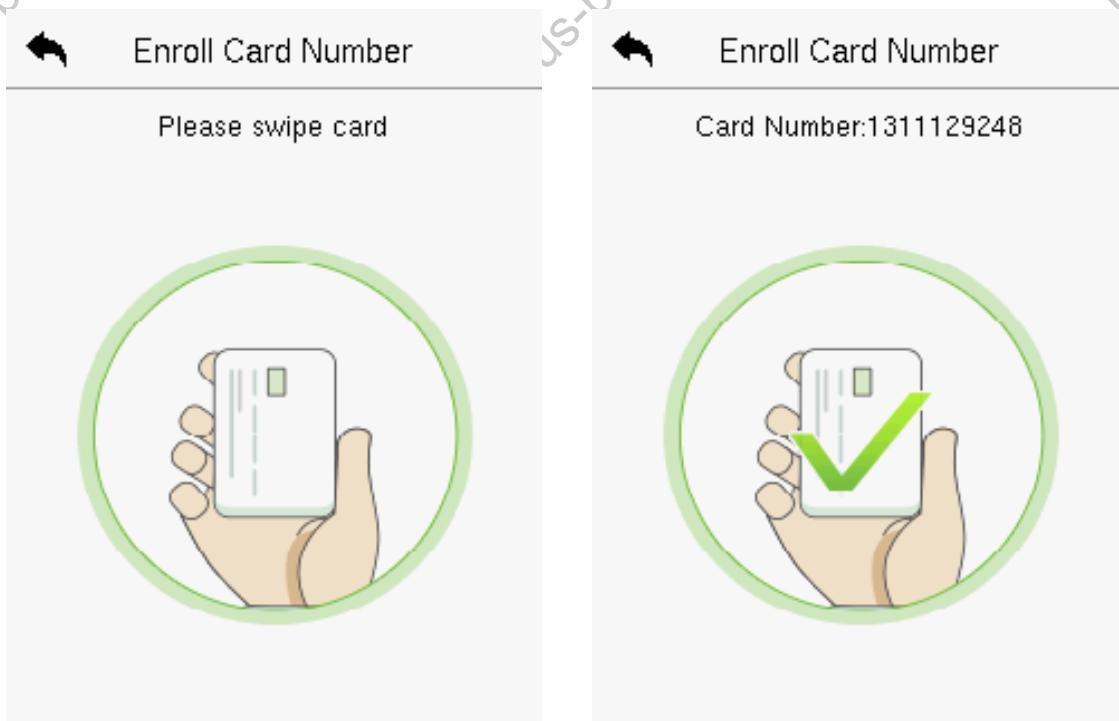


5.1.5 Карта★

Нажмите **Card** (Карта) в интерфейсе **New User** (Новый пользователь), чтобы перейти на страницу регистрации карты.

- Приложите карту к области считывания на интерфейсе регистрации карты. Регистрация будет успешной.
- Если карта уже зарегистрирована, появится сообщение "**Ошибка! Карта уже зарегистрирована**" ("**Error! Card already enrolled**").

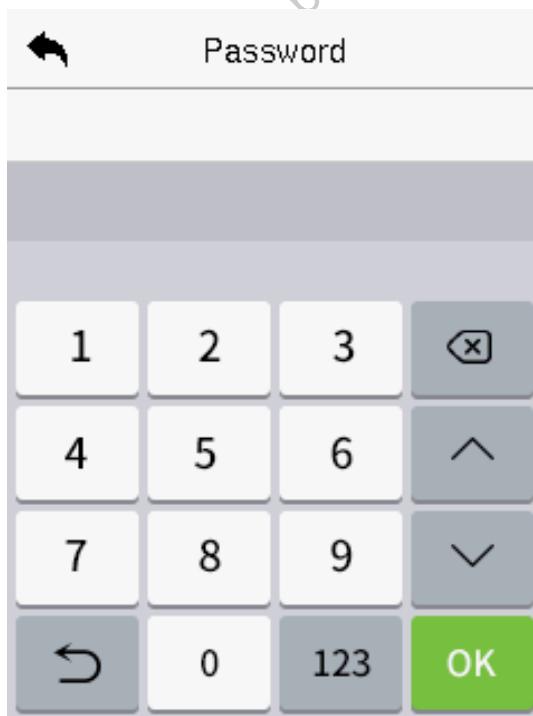
Интерфейс регистрации выглядит следующим образом:



5.1.6 Пароль

Нажмите **Password** (Пароль) в интерфейсе **New User** (Новый пользователь), чтобы перейти на страницу регистрации пароля.

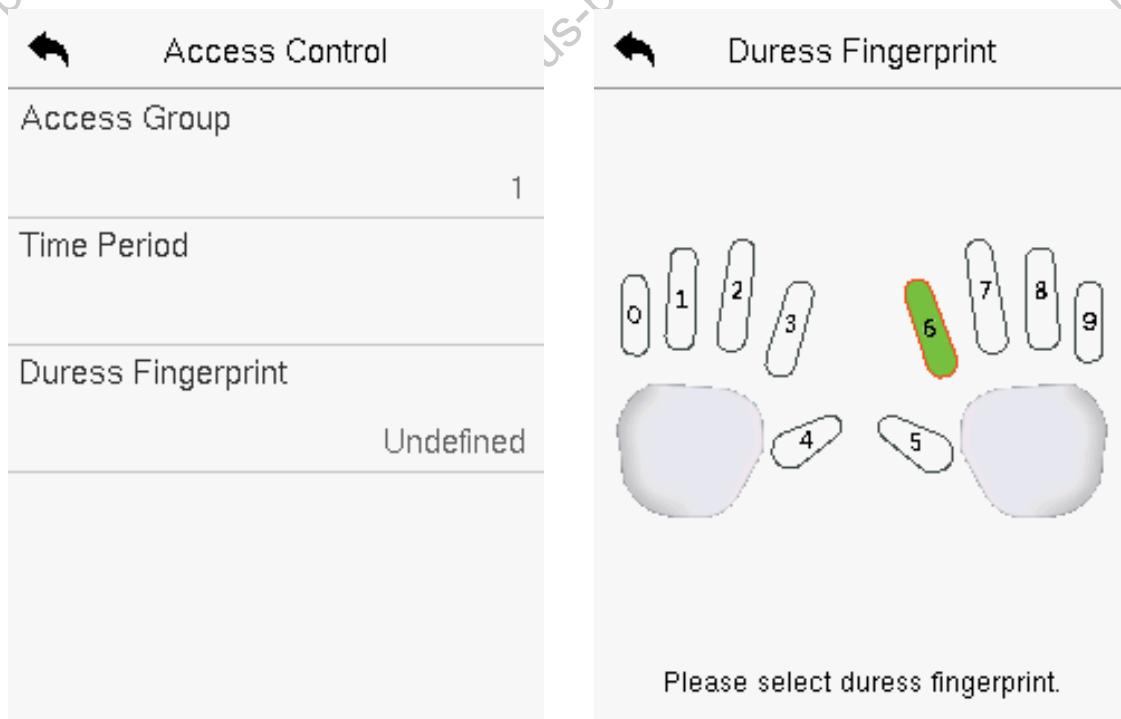
- На интерфейсе регистрации пароля введите требуемый пароль, введите его повторно для подтверждения и нажмите **OK**.
- Если повторно введенный пароль не совпадает с первоначальным, устройство выведет сообщение **"Пароль не совпадает!"** ("Password **does not match!**"), и пользователю потребуется подтвердить пароль заново.
- Пароль по умолчанию может содержать от 6 до 8 цифр.



5.1.7 Роль контроля доступа

Роль контроля доступа определяет права доступа пользователя к дверям. Она включает группу доступа, режим верификации и позволяет задать временной период доступа для группы.

- Нажмите **Access Control Role** (Роль контроля доступа) > **Access Group** (Группа доступа), чтобы распределить зарегистрированных пользователей по разным группам для удобства управления. Новые пользователи по умолчанию относятся к Группе 1, но могут быть переназначены. Устройство поддерживает до 99 групп контроля доступа.
- Нажмите **Time Period** (Временной период), чтобы выбрать разрешенное время доступа.
- Пользователь может назначить один или несколько зарегистрированных отпечатков пальцев как **тревожные** (duress fingerprint(s)). Если приложить к датчику палец, соответствующий тревожному отпечатку, и верификация пройдет успешно, система немедленно сгенерирует **тревожный сигнал** (duress alarm).



5.2 Поиск пользователя

В Главном меню нажмите **User Mgt.** (Управление пользователями), затем **All Users** (Все пользователи), чтобы выполнить поиск.

- В интерфейсе **All-Users** (Все пользователи) нажмите на строку поиска над списком пользователей, введите ключевое слово (это может быть ID, фамилия или полное имя), и система найдет соответствующую информацию о пользователе.

User Mgt.

New User

All Users

Display Style

All Users

1 Lucy

2 Mike

3 James

4 Shawn

Search

5.3 Редактирование пользователя

В интерфейсе **All-Users** (Все пользователи) выберите нужного пользователя из списка и нажмите **Edit** (Редактировать), чтобы изменить его информацию.

User : 1 Lucy

Edit

Delete

Edit : 1 Lucy

User ID
1

Name
Lucy

User Role
Normal User

Fingerprint
1

Face
1

Примечание: Процесс редактирования информации о пользователе аналогичен добавлению нового пользователя, за исключением того, что **ID пользователя (User ID)** нельзя изменить.

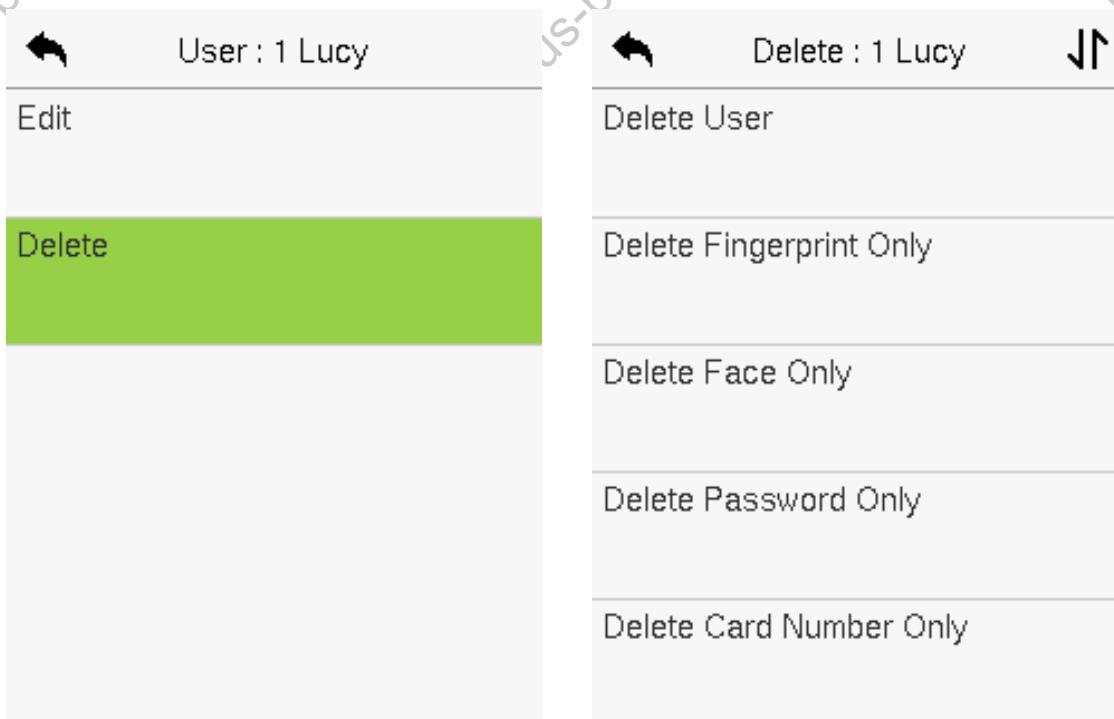
5.4 Удаление пользователя

В интерфейсе **All-Users** (Все пользователи) выберите нужного пользователя из списка и нажмите **Delete** (Удалить), чтобы удалить пользователя или определенную информацию о нем из устройства.

В интерфейсе **Delete** (Удаление) выберите требуемую операцию и нажмите **OK** для подтверждения.

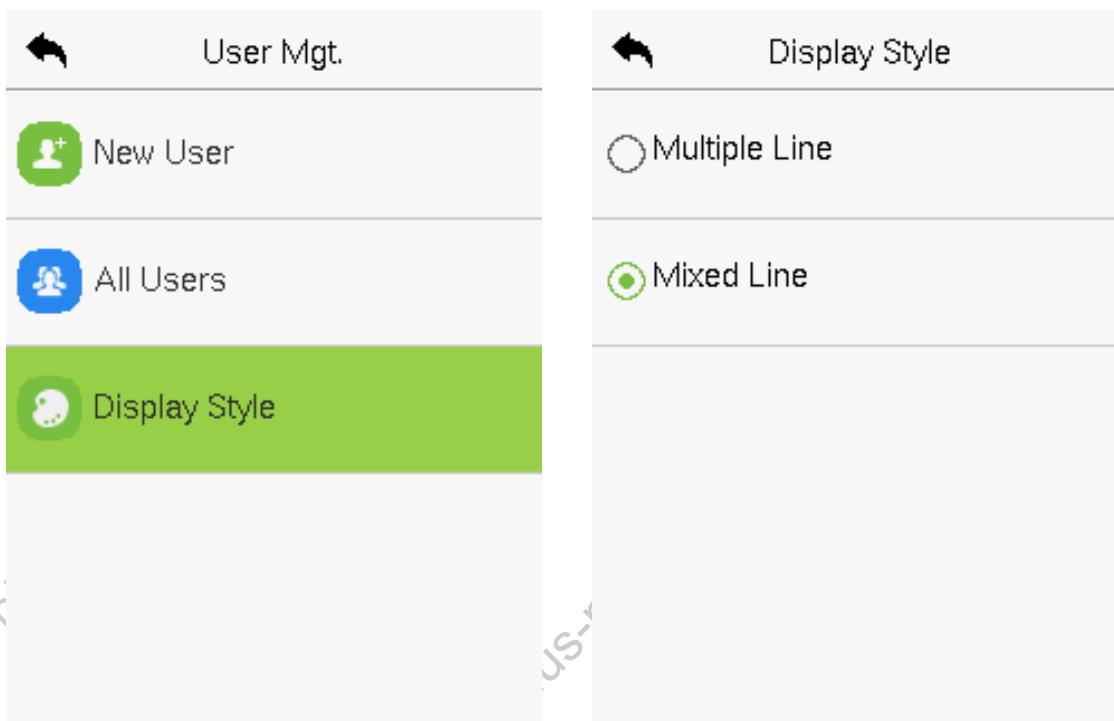
Операции удаления:

- **Delete User** (Удалить пользователя): Удаляет всю информацию о пользователе (полностью удаляет выбранного пользователя) с устройства.
- **Delete Fingerprint Only** (Удалить только отпечаток): Удаляет информацию об отпечатках пальцев выбранного пользователя.
- **Delete Fingerprint Only** (Удалить только отпечаток): Удаляет информацию об отпечатках пальцев выбранного пользователя.
- **Delete Password Only** (Удалить только пароль): Удаляет информацию о пароле выбранного пользователя.
- **Delete Card Number Only** (Удалить только карту): Удаляет информацию о карте выбранного пользователя.



5.5 Стиль отображения

В Главном меню нажмите **User Mgt.** (Управление пользователями), затем **Display Style** (Стиль отображения), чтобы перейти к настройкам стиля отображения.



Все стили отображения приведены ниже:

Многострочный

All Users	
1	Lucy
	⌚️ ███ 🔍 🌐
2	Mike
	⌚️ 🔍
3	James
	⌚️
4	Shawn
	⌚️
Q	

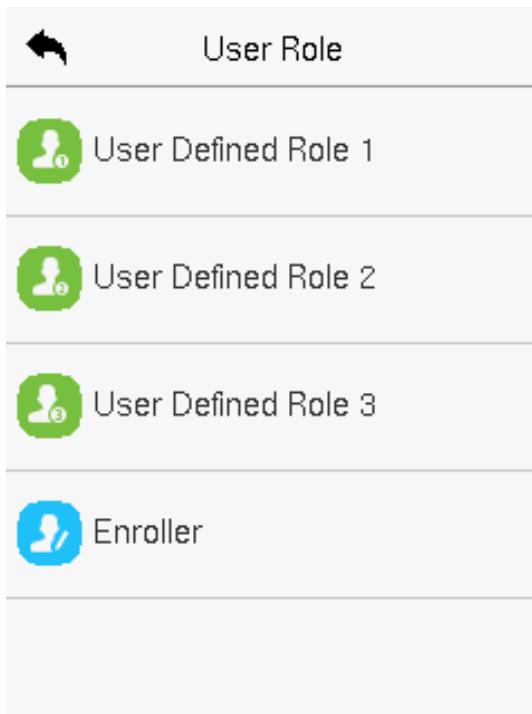
Смешанный:

All Users	
1	⌚️ ███ 🔍 🌐
	Lucy
2	⌚️ 🔍
	Mike
3	⌚️
	James
4	⌚️
	Shawn
Q	

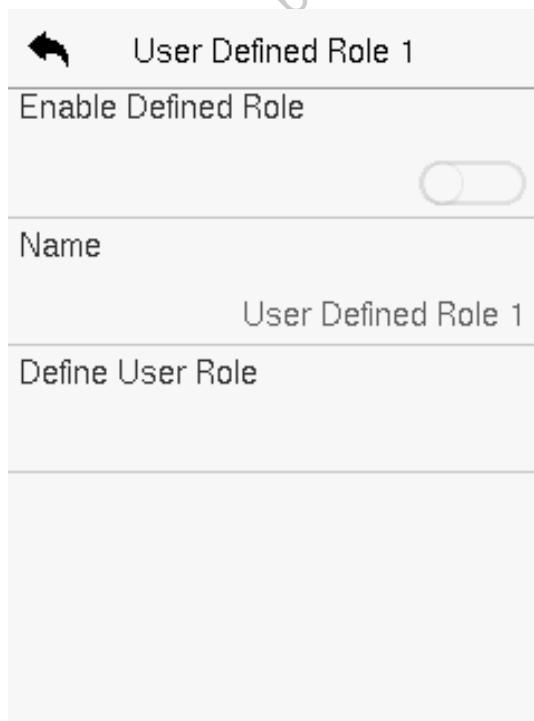
6 Роль пользователя

Роль пользователя позволяет назначать определенным пользователям специальные права в соответствии с требованиями.

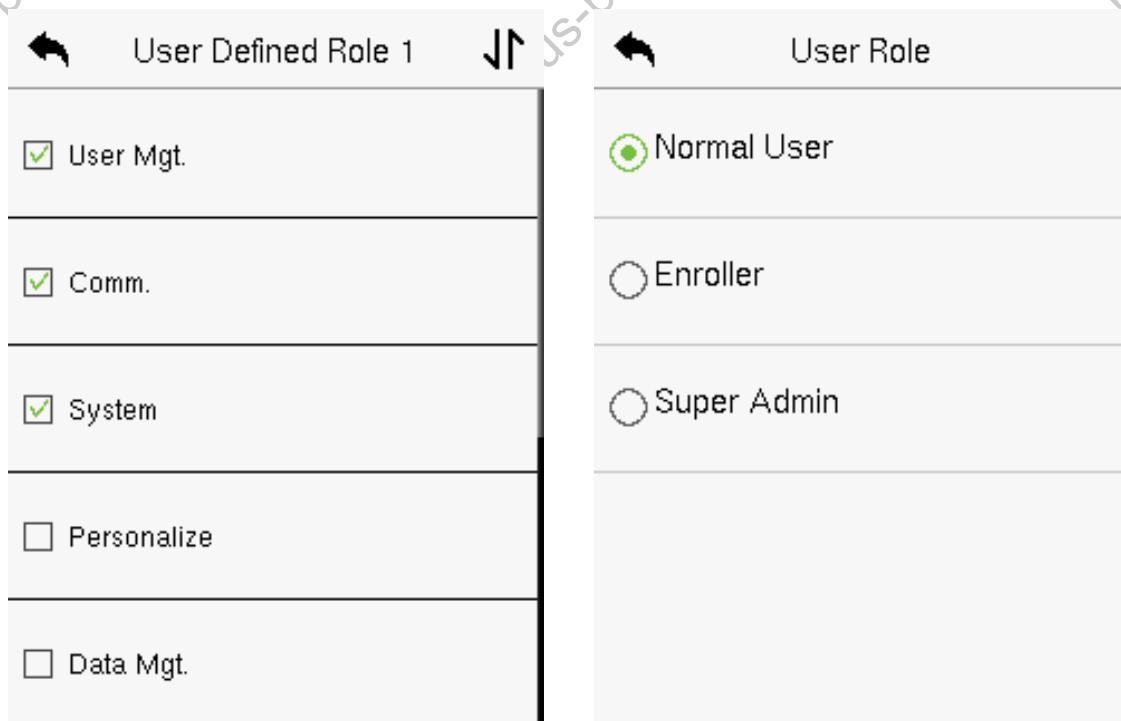
- В Главном меню нажмите **User Role** (Роль пользователя), затем **User Defined Role** (Пользовательская роль), чтобы настроить пользовательские права.
- Область прав для пользовательской роли может быть настроена на 3 уровня, определяющих доступ к функциям меню для данного пользователя.



- В интерфейсе **User Defined Role** (Пользовательская роль) переключите **Enable Defined Role** (Включить пользовательскую роль), чтобы активировать или деактивировать ее.
- Нажмите **Name** (Имя) и введите собственное название для роли.



- Затем, нажав **Define User Role** (Определить роль пользователя), выберите необходимые привилегии для новой роли и нажмите кнопку **Return** (Назад).
- При назначении привилегий названия функций главного меню отображаются слева, а их подменю — справа.
- Сначала нажмите на нужную функцию из главного меню, затем выберите требуемые подменю из списка.

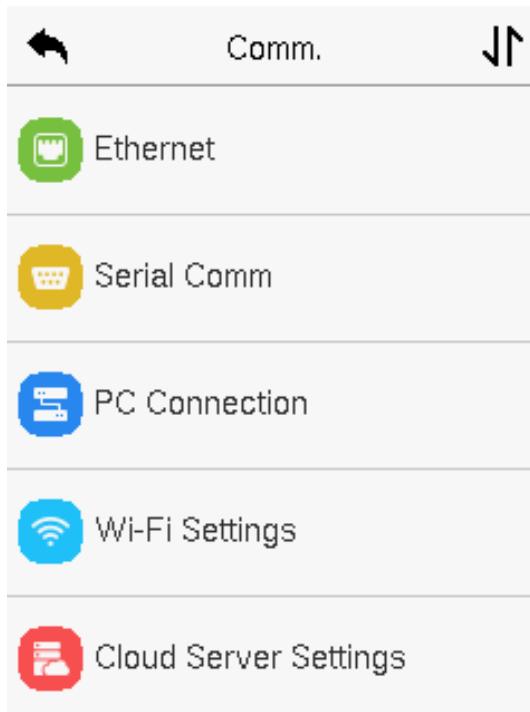


Примечание: Если на устройстве включена функция **User Role** (Роли пользователей), то при создании нового пользователя (**User Mgt. > New User > User Role**) можно назначить ему созданную роль. Однако если на устройстве еще не зарегистрирован супер-администратор, то при попытке включить эту функцию появится сообщение: **"Пожалуйста, сначала зарегистрируйте супер-администратора!"** ("Please enroll super admin first!").

Настройки связи

Настройки связи используются для конфигурации параметров сети, последовательного порта, подключения к ПК, Wi-Fi, облачного сервера, Wiegand и диагностики сети.

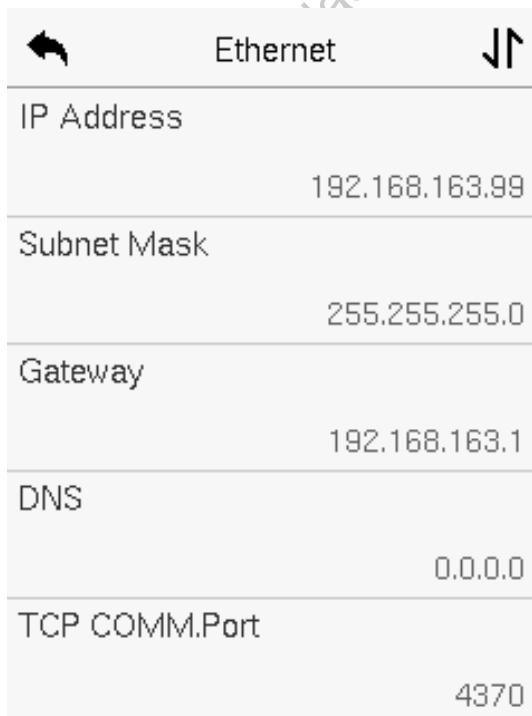
Нажмите **COMM.** (Связь) в главном меню.



7.1 Настройки сети

Если устройству требуется связь с ПК по Ethernet, необходимо настроить сетевые параметры и убедиться, что устройство и ПК находятся в одной подсети.

Нажмите **Ethernet** в интерфейсе настроек связи (**Comm. Settings**), чтобы выполнить конфигурацию.



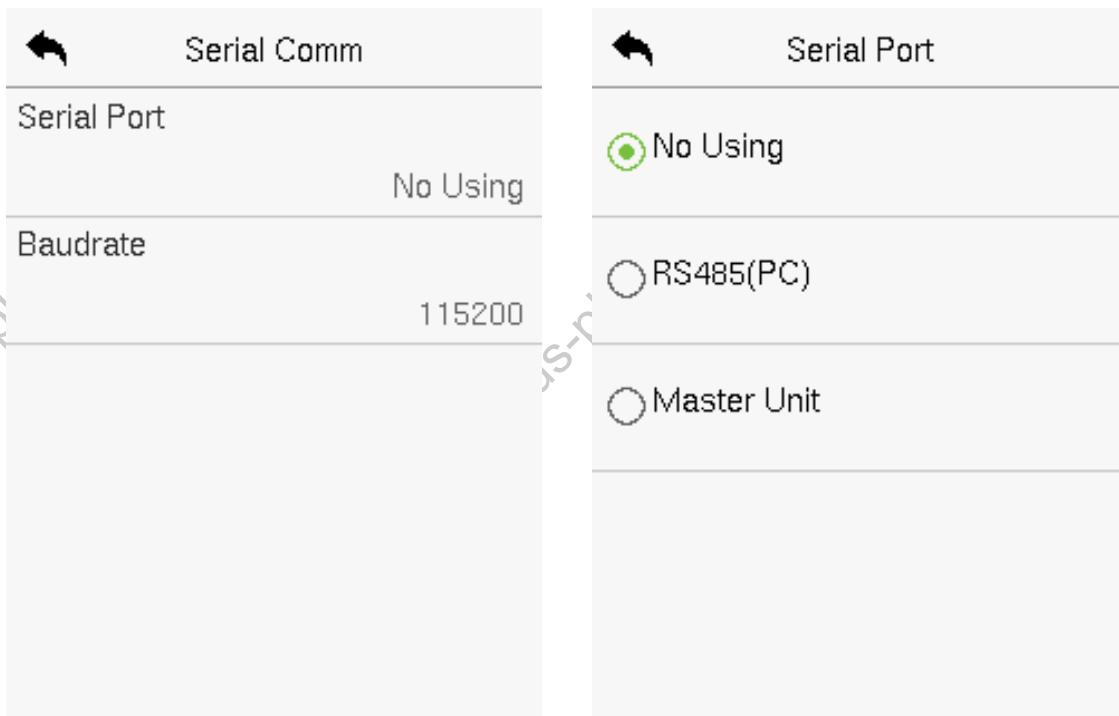
Описание функции

Название функции	Описание
IP Address IP-адрес	По умолчанию: 192.168.1.201. Можно изменить в соответствии с конфигурацией сети.
Subnet Mask Маска подсети	По умолчанию: 255.255.255.0. Можно изменить в соответствии с конфигурацией сети.
Gateway Шлюз	По умолчанию: 0.0.0.0. Можно изменить в соответствии с конфигурацией сети.
DNS DNS-сервер	По умолчанию: 0.0.0.0. Можно изменить в соответствии с конфигурацией сети.
TCP COMM. Port Порт TCP	По умолчанию: 4370. Можно изменить в соответствии с требованиями сети.
DHCP	Протокол динамической конфигурации узла, динамически назначает IP-адреса клиентам через сервер.
Display in Status Bar Отображение в строке состояния	Переключите, чтобы установить, будет ли отображаться значок сети в строке состояния.

7.2 Последовательный порт

Функция последовательного порта устанавливает связь с устройством через последовательный порт (RS485/Главный блок).

Нажмите **Serial Comm.** (Последовательный порт) в интерфейсе настроек связи (**Comm. Settings**).



Описание функции

Название функции	Описание
Serial Port Последовательный порт	<p>No Using (Не используется): Связь с устройством через последовательный порт не осуществляется.</p> <p>RS485(PC): Связь с устройством осуществляется через последовательный порт RS485.</p> <p>Master Unit (Главный блок): Когда RS485 используется в функции "Главный блок", к нему можно подключить считыватель карт.</p>

Baud Rate Скорость передачи	Доступно 4 варианта скорости передачи данных с ПК: 115200 (по умолчанию), 57600, 38400 и 19200.d 19200. Чем выше скорость передачи, тем быстрее происходит обмен данными, но тем менее он надежен. Таким образом, более высокая скорость может использоваться при коротком расстоянии связи; при большом расстоянии выбор более низкой скорости является более надежным.
---------------------------------------	--

7.3 Подключение к ПК

Ключ связи (Comm Key) служит для повышения безопасности данных путем настройки соединения между устройством и ПК. После установки ключа связи для подключения устройства к ПО на ПК потребуется пароль.

Нажмите **PC Connection** (Подключение к ПК) в интерфейсе настроек связи (**Comm. Settings**), чтобы настроить параметры связи.

Описание функции

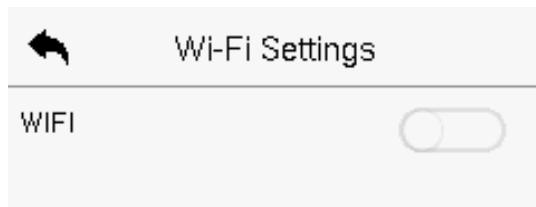
Название функции	Описание
Comm Key Ключ связи	Пароль по умолчанию — 0, можно изменить. Может содержать 1–6 цифр.
Baud Rate Идентификатор устройства	Это идентификационный номер устройства в диапазоне от 1 до 254. Если используется связь по RS485, этот ID необходимо указать в интерфейсе связи ПО.

7.4 Настройки Wi-Fi

Устройство оснащено модулем Wi-Fi, который может быть встроенным или подключаться внешне.

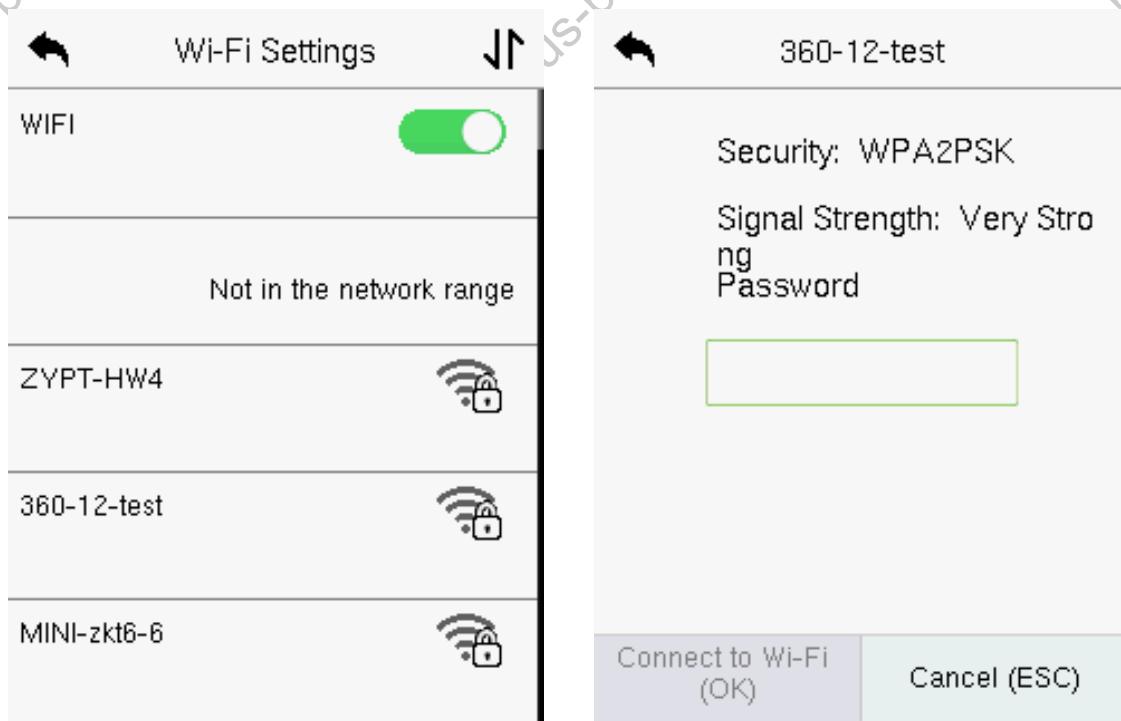
Модуль Wi-Fi позволяет передавать данные по беспроводной сети (Wireless Fidelity) и создает беспроводную сетевую среду. Wi-Fi включен на устройстве по умолчанию. Если использование сети Wi-Fi не требуется, можно переключить кнопку для его отключения.

Нажмите **Wi-Fi Settings** (Настройки Wi-Fi) в интерфейсе настроек связи (**Comm. Settings**), чтобы настроить параметры **Wi-Fi**.



➤ Поиск сети Wi-Fi

- Wi-Fi включен на устройстве по умолчанию. Переключите кнопку  для включения или отключения Wi-Fi.
- После включения Wi-Fi устройство начнет поиск доступных сетей в зоне действия.
- Выберите нужное имя сети (SSID) из списка доступных, введите правильный пароль в появившемся интерфейсе и нажмите **Connect to Wi-Fi** (Подключиться) и **OK**.

**Wi-Fi включен (WIFI Enabled):**

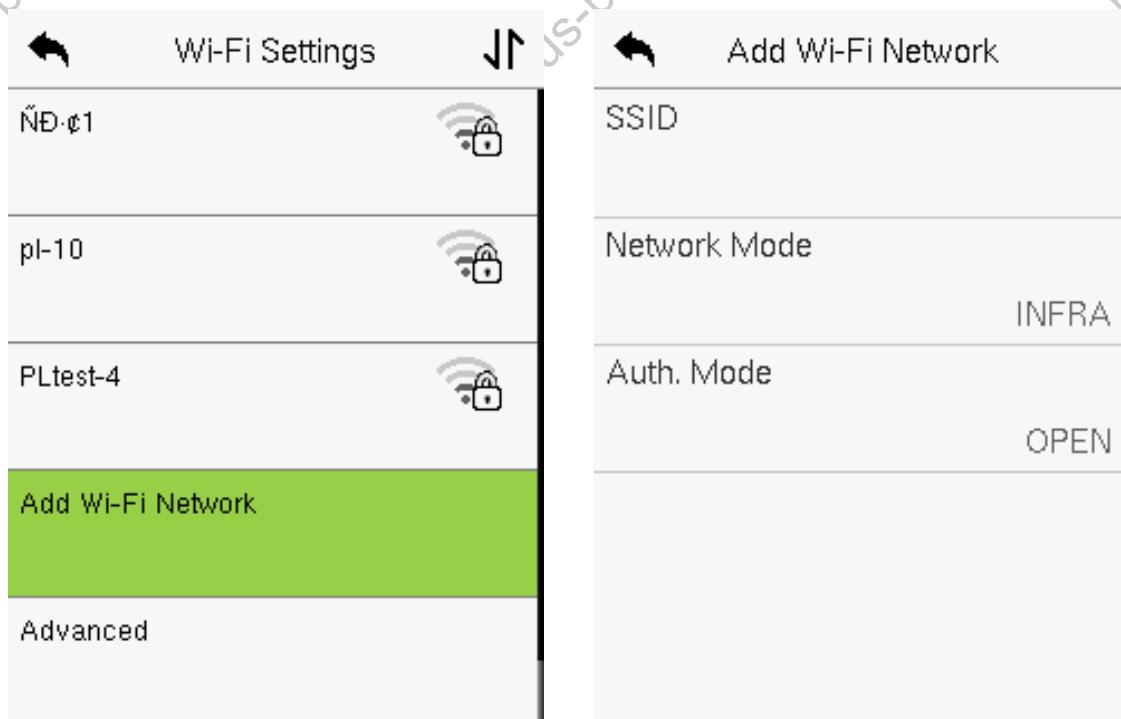
Выберите нужную сеть из списка найденных сетей.

Нажмите на поле для ввода пароля, введите пароль и нажмите **Connect to Wi-Fi (OK)**
(Подключиться к Wi-Fi (OK)).

- При успешном подключении к Wi-Fi на начальном экране появится значок Wi-Fi 

➤ Ручное добавление сети Wi-Fi

Если нужная сеть Wi-Fi не отображается в списке, ее можно добавить вручную.



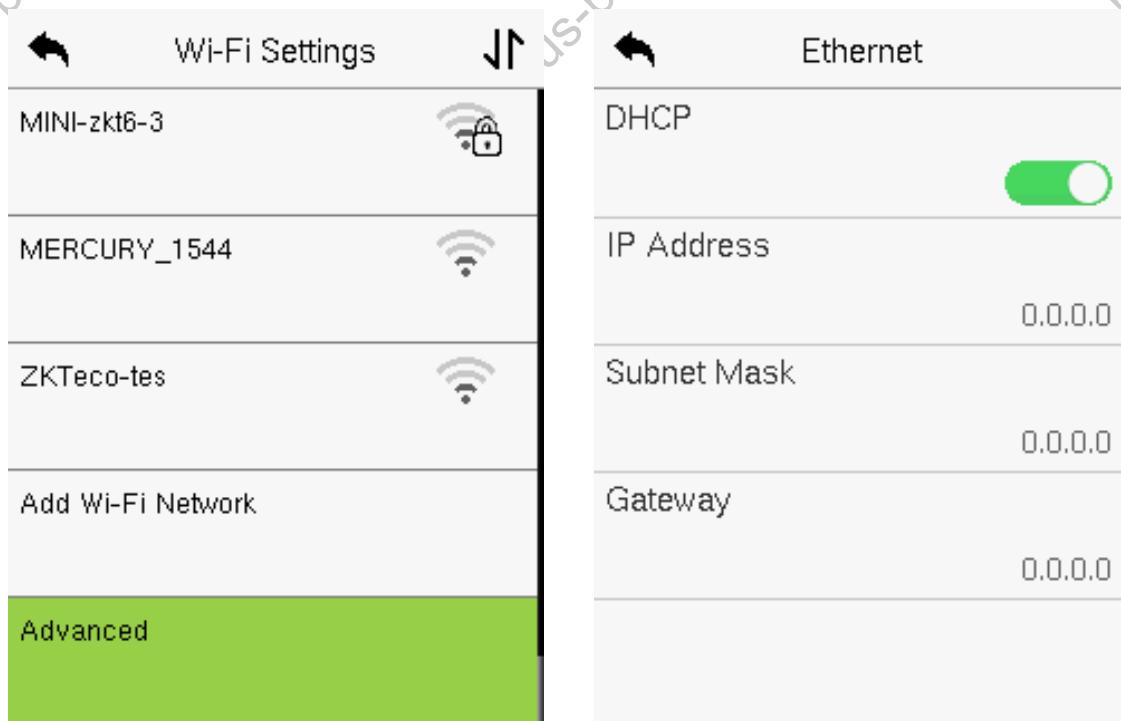
Нажмите **Add Wi-Fi Network**
(Добавить сеть Wi-Fi), чтобы
добавить сеть вручную.

В этом интерфейсе введите
параметры сети Wi-Fi.
(Добавляемая сеть должна
существовать.)

Примечание: После успешного ручного добавления Wi-Fi выполните тот же процесс поиска, чтобы найти добавленное имя сети.

➤ **Дополнительные настройки**

В интерфейсе **Wi-Fi Settings** (Настройки Wi-Fi) нажмите **Advanced** (Дополнительно), чтобы установить необходимые параметры.

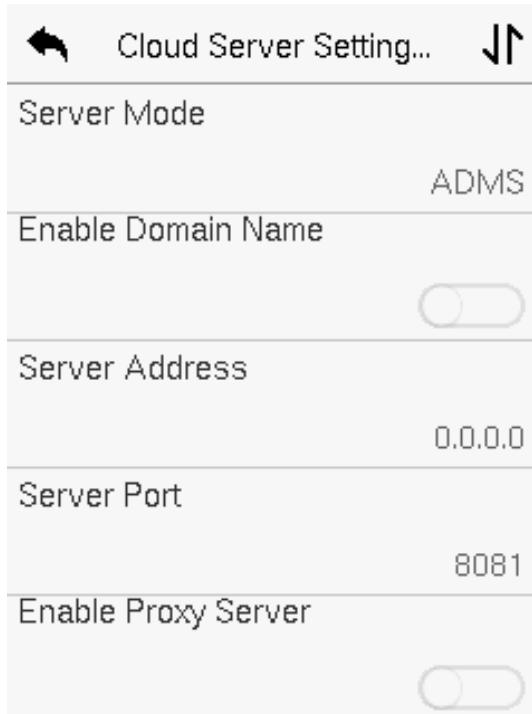


Описание функции

Название функции	Описание
DHCP	Протокол динамической конфигурации узла (DHCP) динамически назначает IP-адреса сетевым клиентам. Если DHCP включен, IP-адрес нельзя задать вручную.
IP Address IP-адрес	IP-адрес для сети Wi-Fi. По умолчанию: 0.0.0.0. Можно изменить в соответствии с конфигурацией сети.
Subnet Mask Маска подсети	Маска подсети для сети Wi-Fi. По умолчанию: 255.255.255.0. Можно изменить в соответствии с конфигурацией сети.
Gateway Шлюз	Адрес шлюза по умолчанию: 0.0.0.0. Можно изменить в соответствии с конфигурацией сети.

7.5 Настройка облачного сервера

Нажмите **Cloud Server Setting** (Настройка облачного сервера) в интерфейсе настроек связи (**Comm. Settings**), чтобы подключиться к серверу **ADMS**.



Описание функции

Название функции	Описание	
Enable Domain Name Включить доменное имя	Server Address Адрес сервера	Когда этот режим включен (ON), будет использоваться режим доменного имени в формате "http://...", например, http://www.XYZ.com, где "XYZ" обозначает доменное имя.
Disable Domain Name Отключить доменное имя	Server Address Адрес сервера	IP-адрес сервера ADMS.
	Server Port Порт сервера	Порт, используемый сервером ADMS.
Enable Proxy Server Включить прокси-сервер	При включении прокси-сервера его IP-адрес и номер порта задаются вручную.	

HTTPS

На основе HTTP шифрование передачи и аутентификация обеспечивают безопасность процесса передачи.

7.6 Настройка Wiegand

Она используется для настройки параметров входа и выхода Wiegand.

Нажмите **Wiegand Setup** (Настройка Wiegand) в интерфейсе настроек связи (**Comm. Settings**), чтобы настроить параметры входа и выхода **Wiegand**.



7.6.1 Вход Wiegand



Описание функции

Название функции	Описание
Wiegand Format Формат Wiegand	Может принимать значения: 26 бит, 34 бит, 36 бит, 37 бит и 50 бит.
Wiegand Bits Разрядность данных	Количество бит в данных Wiegand.
Pulse Width(us) Длительность импульса, мкс	Длительность импульса, отправляемого по Wiegand. По умолчанию: 100 мкс. Диапазон регулировки: от 20 до 400 мкс.
Pulse Interval(us) Интервал импульсов, мкс	По умолчанию: 1000 мкс. Диапазон регулировки: от 200 до 20000 мкс.
ID Type Тип ID	Выбор между User ID (ID пользователя) и Card Number (номер карты).

Описание распространенных форматов Wiegand

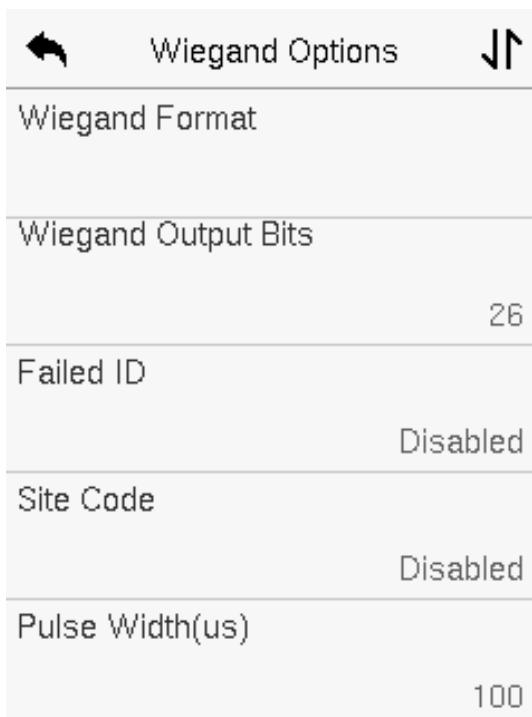
Формат Wiegand	Описание
Wiegand26	<p>ECCCCCCCCCCCCCCCCCCCCCCCCCO</p> <p>Он состоит из 26-битного двоичного кода. 1-й бит — это бит четности (even parity) для битов со 2-го по 13-й, а 26-й бит — бит нечетности (odd parity) для битов с 14-го по 25-й. Биты со 2-го по 25-й содержат номер карты.</p>

Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCCO Это 26-битный двоичный код. 1-й бит является битом четности (even parity) для битов со 2-го по 13-й, а 26-й бит — битом нечетности (odd parity) для битов с 14-го по 25-й. Биты со 2-го по 9-й представляют собой код объекта (site codes), а биты с 10-го по 25-й — номер карты (card numbers).
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Это 34-битный двоичный код. 1-й бит является битом четности (even parity) для битов со 2-го по 17-й, а 34-й бит — битом нечетности (odd parity) для битов с 18-го по 33-й. Биты со 2-го по 25-й содержат номер карты.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCO Это 34-битный двоичный код. 1-й бит является битом четности (even parity) для битов со 2-го по 17-й, а 34-й бит — битом нечетности (odd parity) для битов с 18-го по 33-й. Биты со 2-го по 9-й представляют собой код объекта (site codes), а биты с 10-го по 25-й — номер карты (card numbers).
Wiegand36	OFFFFFFFFFCCCCCCCCCCCCMME Это 36-битный двоичный код. 1-й бит является битом нечетности (odd parity) для битов со 2-го по 18-й, а 36-й бит — битом четности (even parity) для битов с 19-го по 35-й. Биты со 2-го по 17-й представляют собой код устройства (device codes). Биты с 18-го по 33-й — номер карты (card numbers), а биты с 34-го по 35-й — код производителя (manufacturer codes).

Wiegand36a	EFFFFFFFFFCCCCCCCCCCCC Это 36-битный двоичный код. 1-й бит является битом четности (even parity) для битов со 2-го по 18-й, а 36-й бит — битом нечетности (odd parity) для битов с 19-го по 35-й. Биты со 2-го по 19-й представляют собой код устройства (device codes), а биты с 20-го по 35-й — номер карты (card numbers).
Wiegand37	OMMMMSSSSSSSSSCCCCCCCC Это 37-битный двоичный код. 1-й бит является битом нечетности (odd parity) для битов со 2-го по 18-й, а 37-й бит — битом четности (even parity) для битов с 19-го по 36-й. Биты со 2-го по 4-й представляют собой код производителя (manufacturer codes). Биты с 5-го по 16-й — код объекта (site codes), а биты с 21-го по 36-й — номер карты (card numbers).
Wiegand37a	EMMMFFFFFFFFSSSSCCCC Это 37-битный двоичный код. 1-й бит является битом четности (even parity) для битов со 2-го по 18-й, а 37-й бит — битом нечетности (odd parity) для битов с 19-го по 36-й. Биты со 2-го по 4-й представляют собой код производителя (manufacturer codes). Биты с 5-го по 14-й — код устройства (device codes), биты с 15-го по 20-й — код объекта (site codes), а биты с 21-го по 36-й — номер карты (card numbers).
Wiegand50	ESSSSSSSSSSSSCCCCCCCCCCCCCCCC Это 50-битный двоичный код. 1-й бит является битом четности (even parity) для битов со 2-го по 25-й, а 50-й бит — битом нечетности (odd parity) для битов с 26-го по 49-й. Биты со 2-го по 17-й представляют собой код объекта (site codes), а биты с 18-го по 49-й — номер карты (card numbers).

C (Card): номер карты (card number); **E (Even):** бит четности (even parity bit)
O (Odd): бит нечетности (odd parity bit); **F (Facility):** код объекта/учреждения (facility code)
M (Manufacturer): код производителя (manufacturer code); **P (Parity):** бит четности (parity bit); **S (Site):** код площадки/сайта (site code)

7.6.2 Выход Wiegand



Описание функции

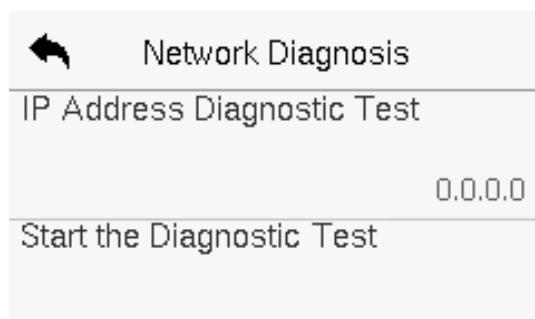
Название функции	Описание
Wiegand Format Формат Wiegand	Может принимать значения: 26 бит, 34 бит, 36 бит, 37 бит и 50 бит.
Wiegand Output Bits Выходные биты Wiegand	После выбора формата Wiegand укажите количество соответствующих выходных бит в этом формате.

Failed ID ID при ошибке	При неудачной верификации система отправит устройству этот ID, заменив им номер карты или ID пользователя.
Site Code Код объекта	Аналогичен идентификатору устройства, но его можно задать вручную, и он может повторяться на разных устройствах. Допустимый диапазон по умолчанию: от 0 до 256.
Pulse Width(us) Длительность импульса, мкс	Временная ширина импульса, представляющая изменение количества заряда при заданной емкости за определенное время.
Pulse Interval(us) Интервал импульсов, мкс	Временной интервал между импульсами
ID Type Тип ID	Выбор типа идентификатора: User ID (ID пользователя) или Card Number (номер карты).

7.7 Диагностика сети

Она помогает настроить параметры диагностики сети.

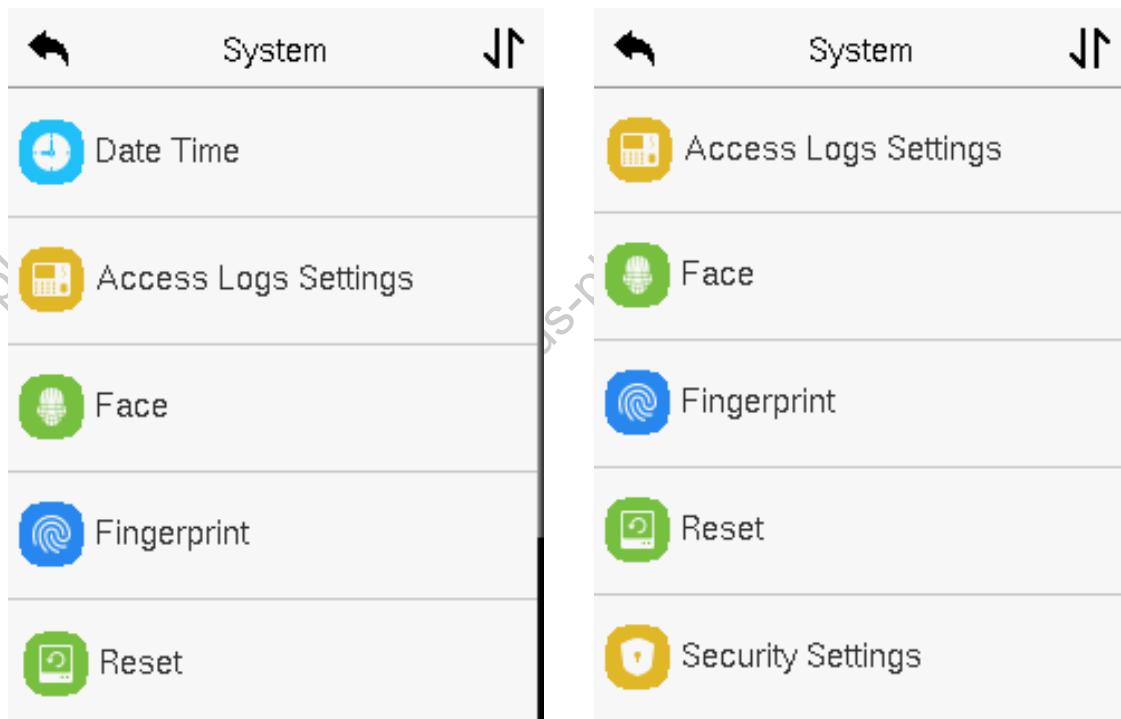
Нажмите **Network Diagnosis** (Диагностика сети) в интерфейсе настроек связи (**Comm. Settings**). Введите IP-адрес, который необходимо проверить, и нажмите **Start the Diagnostic Test** (Начать диагностику), чтобы проверить возможность подключения к устройству по сети.



8 Настройки системы

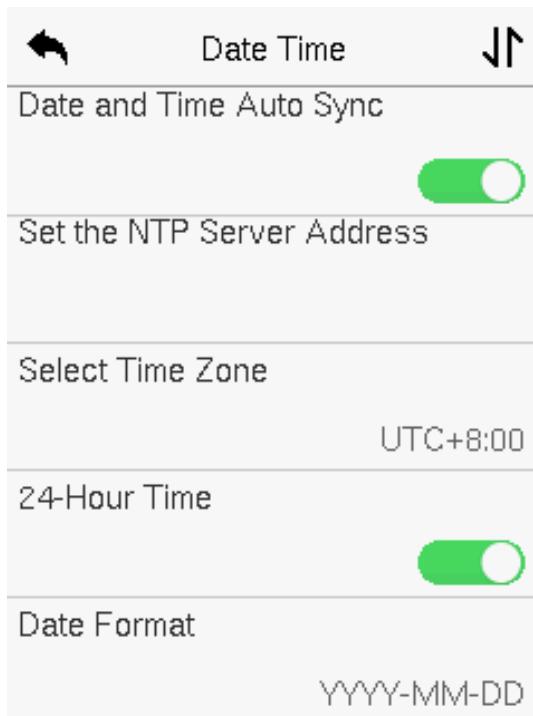
Настройка системы помогает настроить параметры системы для оптимизации доступности устройства.

Нажмите **System** (Система) в главном меню, чтобы перейти к ее опциям.



8.1 Дата и время

Нажмите **Date Time** (Дата и время) в интерфейсе **System** (Система), чтобы задать дату и время.



- Нажмите **Date and Time Auto Sync** (Автосинхронизация даты и времени), чтобы включить автоматическую синхронизацию на основе введенного адреса сервера.
- Нажмите **Manual Date and Time** (Ручная установка даты и времени), чтобы задать их вручную, затем нажмите **Confirm** (Подтвердить) для сохранения.
- Нажмите **Select Time Zone** (Выбор часового пояса), чтобы вручную выбрать часовой пояс, в котором находится устройство.
- Включите или отключите **24-Hour Time** (24-часовой формат). Если включен, выберите **Date Format** (Формат даты).
- Нажмите **Daylight Saving Time** (Летнее время), чтобы включить или отключить эту функцию. Если включена, нажмите **Daylight Saving Mode Setup** (Настройка летнего времени) для выбора режима, затем **Daylight Saving Setup** (Настройка летнего времени) для установки времени перехода.

Daylight Saving Setup	
Start Month	1
Start Week	1
Start Day	Sunday
Start Time	00:00
End Month	1
End Date	00-00
End Time	00:00

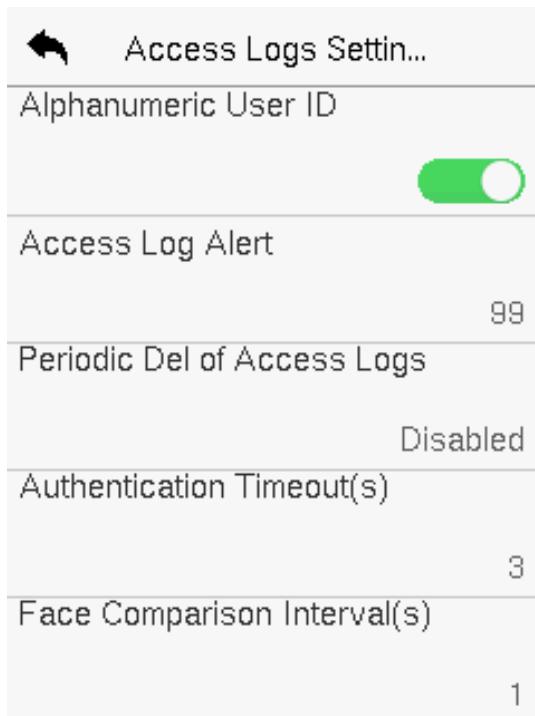
Режим недели**Режим даты**

- При восстановлении заводских настроек можно сбросить формат времени (24-часовой) и даты (ГГГГ-ММ-ДД), но дата и время, установленные на устройстве, не сбрасываются.

Примечание: Например, если пользователь изменил время на устройстве (с 15 марта 2020, 18:35) на 1 января 2021, 18:30, то после восстановления заводских настроек время на устройстве останется 1 января 2021, 18:30.

8.2

Нажмите **Access Logs Settings** (Настройка журналов доступа) в интерфейсе **System** (Система).



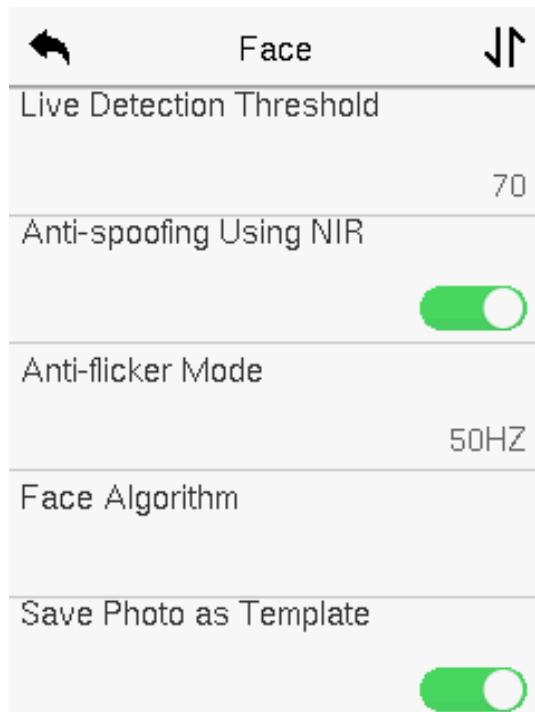
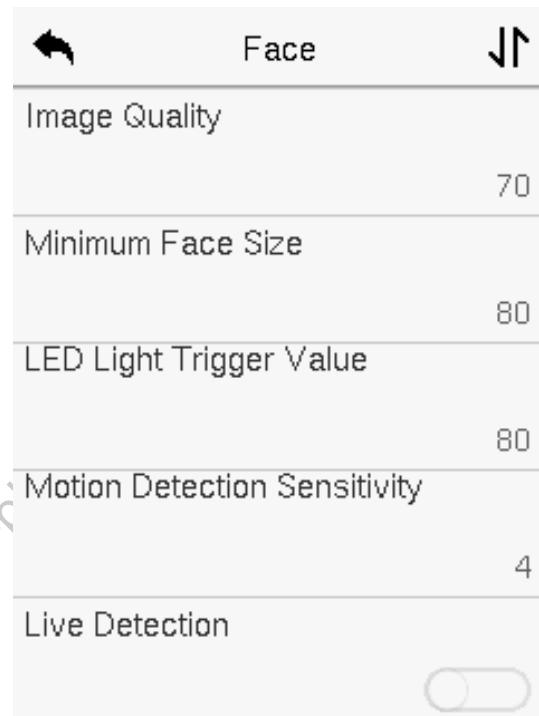
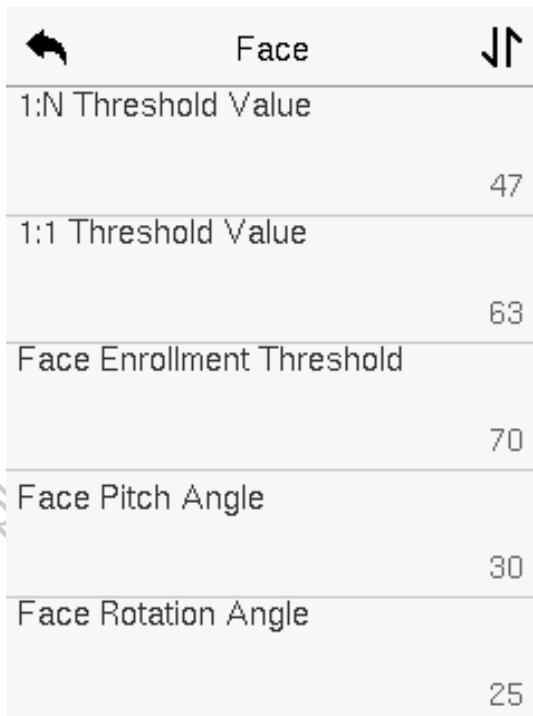
Описание функции

Название функции	Описание
Alphanumeric User ID Буквенно-цифровой ID пользователя	Включение/отключение использования буквенно-цифровых символов в качестве ID пользователя.
Access Log Alert Оповещение о журнале доступа	<p>Когда свободное пространство для записей о доступе и отметках достигает максимального порогового значения, устройство автоматически отображает предупреждение.</p> <p>Пользователь может отключить эту функцию или установить значение от 1 до 9999.</p>

Periodic Del of Access Logs Периодическое удаление журналов доступа	При заполнении журналов доступа устройство автоматически удаляет набор старых записей. Функцию можно отключить или задать значение от 1 до 999.
Authentication Timeout(s) Таймаут аутентификации, с	Время отображения сообщения об успешной верификации. Допустимое значение: от 1 до 9 секунд.
Face comparison Interval(s) Интервал сравнения лиц, с	После выбора интервального распознавания (например, при установке интервала 5 с) распознавание лица будет выполняться каждые 5 с. Допустимое значение: 0–9 с. 0 означает непрерывное распознавание, 1–9 — распознавание с интервалами.

8.3 Параметры лица

Нажмите **Face** (Лицо) в интерфейсе **System** (Система), чтобы перейти к настройкам параметров лица.



Описание функции

Название функции	Описание
1:N Threshold Value Пороговое значение для 1:N	<p>В режиме верификации 1:N верификация будет успешной только при условии, что степень сходства между полученным изображением лица и всеми зарегистрированными шаблонами превышает установленное значение.</p> <p>Допустимый диапазон: от 0 до 100. Чем выше порог, тем ниже вероятность ложного принятия и выше вероятность отказа, и наоборот. Рекомендуется устанавливать значение по умолчанию, равное 47.</p>
1:1 Threshold Value Пороговое значение для 1:1	<p>В режиме верификации 1:1 верификация будет успешной только при условии, что степень сходства между полученным изображением лица и зарегистрированным в устройстве шаблоном пользователя превышает установленное значение.</p> <p>Допустимый диапазон: от 0 до 100. Чем выше порог, тем ниже вероятность ложного принятия и выше вероятность отказа, и наоборот. Рекомендуется устанавливать значение по умолчанию, равное 63.</p>
Face Enrollment Threshold Порог при регистрации лица	<p>Во время регистрации лица используется сравнение 1:N для определения, регистрировался ли пользователь ранее.</p> <p>Если степень сходства между полученным изображением лица и всеми зарегистрированными шаблонами превышает установленный порог, это означает, что лицо уже зарегистрировано.</p>

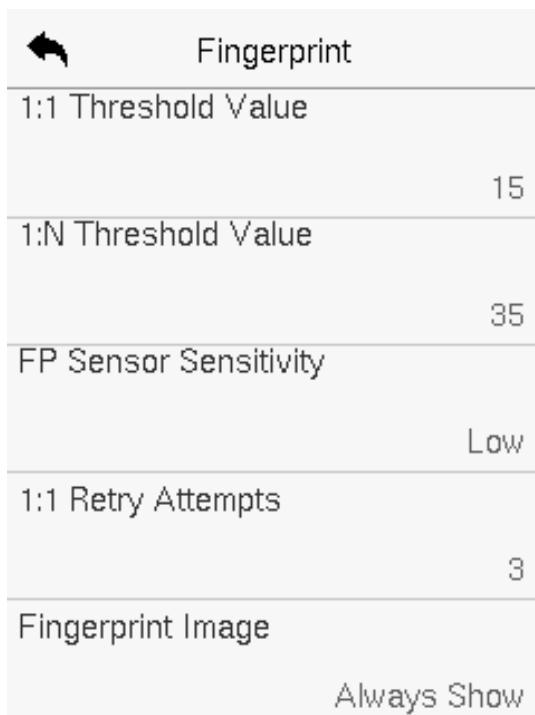
Face Pitch Angle Угол наклона лица	<p>Это допустимый угол наклона (вверх/вниз) лица при регистрации и сравнении шаблонов.</p> <p>Если угол наклона лица превышает установленное значение, алгоритм его отфильтрует (игнорирует), и интерфейс регистрации/сравнения не будет активирован.</p>
Face Rotation Angle Угол поворота лица	<p>Это допустимый угол поворота (влево/вправо) лица при регистрации и сравнении шаблонов.</p> <p>Если угол поворота лица превышает установленное значение, алгоритм его отфильтрует (игнорирует), и интерфейс регистрации/сравнения не будет активирован.</p>
Image Quality Качество изображения	<p>Это минимальное качество изображения для регистрации и сравнения лица. Чем выше значение, тем более четкое изображение требуется.</p>
Minimum Face Size Минимальный размер лица	<p>Устанавливает минимальный размер лица, необходимый для регистрации и сравнения.</p> <p>Если минимальный размер захваченного изображения меньше установленного значения, оно будет отфильтровано и не распознано как лицо.</p> <p>Это значение также можно интерпретировать как дистанцию для сравнения лиц. Чем дальше человек, тем меньше лицо и тем меньше пикселей получает алгоритм. Следовательно, регулировка этого параметра позволяет настроить максимальную дистанцию для сравнения лиц. При значении 0 дистанция сравнения не ограничена.</p>

LED Light Trigger Threshold Порог активации светодиодной подсветки	Это значение управляет включением и выключением светодиодной подсветки. Чем больше значение, тем чаще будет включаться/выключаться подсветка.
Motion Detection Sensitivity Чувствительность обнаружения движения	Устанавливает величину изменения в поле зрения камеры, при котором система обнаруживает потенциальное движение и переводит терминал из режима ожидания в интерфейс сравнения. Чем больше значение, тем чувствительнее система. То есть при более высоком значении интерфейс сравнения активируется легче, а обнаружение движения срабатывает чаще.
Live Detection Живое обнаружение	Обнаруживает попытку подделки с использованием изображений в видимом свете, чтобы определить, является ли предоставленный биометрический образец реальным человеком (живым) или подделкой.
Live Detection Threshold Порог живого обнаружения	Используется для оценки, является ли захваченное изображение в видимом свете реальным человеком (живым). Чем больше значение, тем лучше защита от подделки с использованием видимого света.
Anti-spoofing Using NIR Защита от подделки с использованием ближнего инфракрасного диапазона	Использование изображений в ближнем инфракрасном спектре для идентификации и предотвращения атак с помощью поддельных фотографий и видео.
Anti-flicker Mode Режим подавления мерцания	Используется при выключенном WDR. Помогает уменьшить мерцание, когда частота мерцания экрана устройства совпадает с частотой источника света.
Face algorithm Алгоритм лица	Содержит информацию, связанную с алгоритмом распознавания лиц, и позволяет приостановить обновление шаблонов лиц.

Save Photo as Template Сохранять фото как шаблон	После отключения этой функции потребуется повторная регистрация лиц при обновлении алгоритма.
--	---

8.4 Отпечаток пальца★

Нажмите **Fingerprint** (Отпечаток пальца) в интерфейсе **System** (Система), чтобы перейти к настройкам параметров отпечатков пальцев.



Описание функции

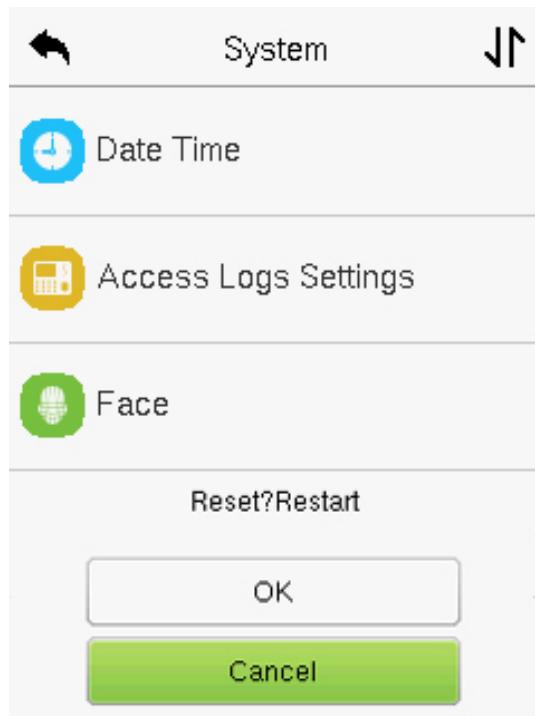
Название функции	Описание
1:1 Threshold Value Пороговое значение для 1:1	В режиме верификации 1:1 верификация будет успешной только при условии, что степень сходства между полученными данными отпечатка пальца и шаблоном, связанным с введенным ID пользователя, зарегистрированным в устройстве, превышает установленное значение.

1:N Threshold Value Пороговое значение для 1:N	В режиме верификации 1:N верификация будет успешной только при условии, что степень сходства между полученными данными отпечатка пальца и всеми шаблонами, зарегистрированными в устройстве, превышает установленное значение.
FP Sensor Sensitivity Чувствительность датчика отпечатка	Настройка чувствительности захвата отпечатка. Рекомендуется использовать уровень по умолчанию "Средний". В сухой среде, если обнаружение замедлено, можно установить уровень "Высокий". Во влажной среде, если идентификация затруднена, можно установить уровень "Низкий".
1:1 Retry Times Количество попыток для 1:1	При верификации 1:1 пользователь может забыть, какой палец зарегистрирован, или приложить палец неправильно. Чтобы избежать повторного ввода ID, разрешено несколько попыток.
Fingerprint Image Изображение отпечатка пальца	Настройка отображения изображения отпечатка на экране во время регистрации или верификации. Доступны четыре варианта: Показывать при регистрации (Show for Enroll): отображать только во время регистрации. Показывать при сравнении (Show for Match): отображать только во время верификации. Показывать всегда (Always Show): отображать и при регистрации, и при верификации. Не показывать (None): не отображать изображение.

8.5 Сброс к заводским настройкам

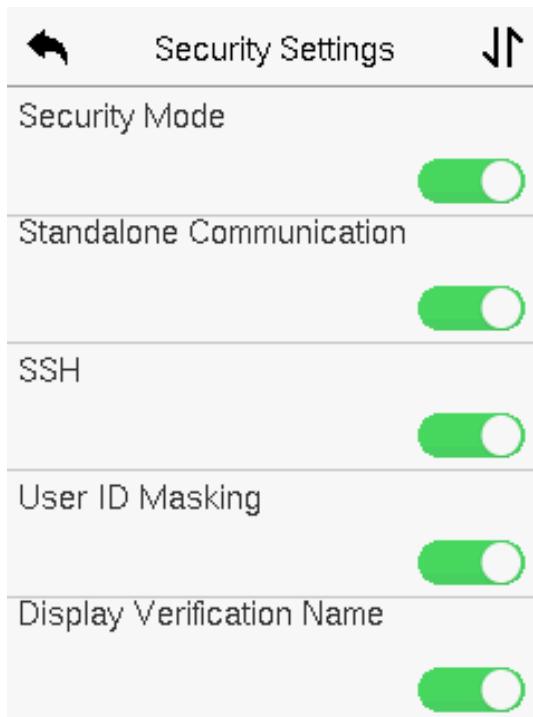
Функция **Сброса к заводским настройкам** (Factory Reset) восстанавливает параметры устройства (например, настройки связи и системы) до значений по умолчанию (при этом данные зарегистрированных пользователей не удаляются).

Нажмите **Reset** (Сброс) в интерфейсе **System** (Система), а затем **OK**, чтобы восстановить заводские настройки.



8.6 Настройки безопасности

Нажмите **Security Settings** (Настройки безопасности) в интерфейсе **System** (Система), чтобы перейти к настройкам безопасности.



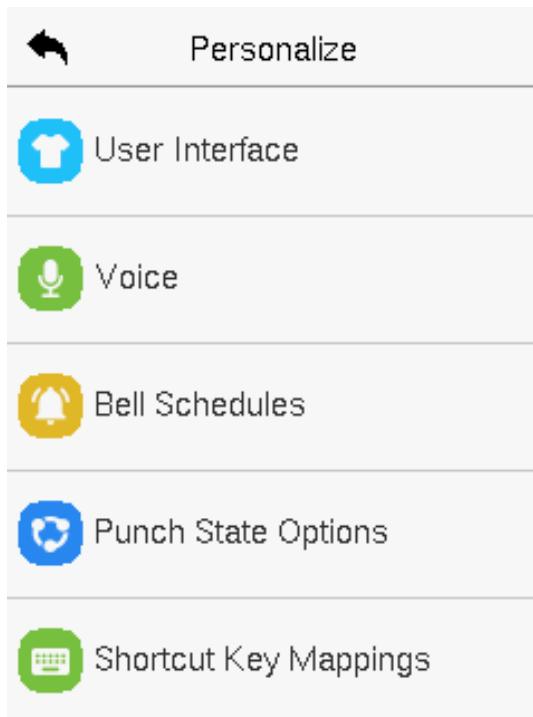
Описание функции

Название функции	Описание
Security Mode Режим безопасности	Выбор, включать ли режим безопасности для защиты устройства и личной информации пользователя. Можно настроить работу устройства в автономном режиме и скрыть личные данные пользователя во время верификации для предотвращения утечки.
Standalone Communication Автономная связь	Чтобы избежать невозможности использования при отключенном устройстве от сети, можно заранее установить на компьютер клиент-серверное ПО (например, ZKAccess 3.5) для автономной работы.

SSH	SSH используется для доступа к фоновым службам устройства в целях технического обслуживания.
User ID Masking Маскировка ID пользователя	При включении, после успешной верификации пользователя, ID пользователя в отображаемом результате будет заменен на * для обеспечения безопасной защиты конфиденциальных данных.
Display Verification Name Отображать имя при верификации	Настройка, отображать ли имя пользователя в интерфейсе с результатом верификации.
Display Verification Mode Отображать режим верификации	Настройка, отображать ли режим верификации в интерфейсе с результатом верификации.

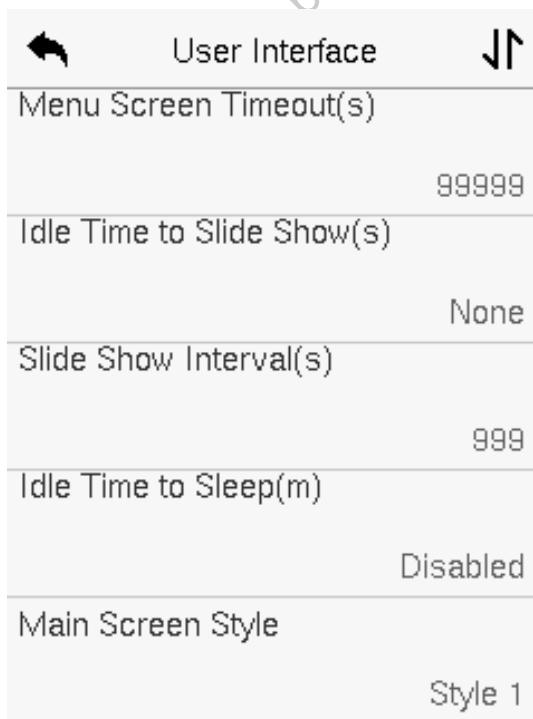
9 Настройки персонализации

Нажмите **Personalize** (Персонализация) в главном меню, чтобы настроить интерфейс, звук, звонок, параметры состояния отметки и назначение горячих клавиш.



9.1 Настройки интерфейса

Нажмите **User Interface** (Интерфейс пользователя) в интерфейсе **Personalize** (Персонализация), чтобы настроить стиль отображения главного экрана.



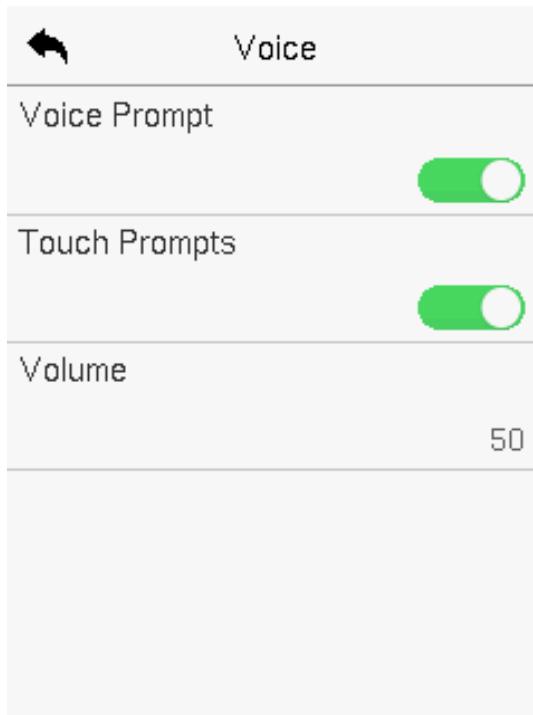
Описание функции

Название функции	Описание
Wallpaper Обои	Выбор фонового изображения (обоев) для главного экрана в соответствии с предпочтениями пользователя.
Language Язык	Выбор языка интерфейса устройства.
Menu Screen Timeout (s) Время ожидания экрана меню (с)	<p>Время бездействия, по истечении которого устройство автоматически возвращается на начальный экран.</p> <p>Значение может быть отключено или установлено в диапазоне от 60 до 99999 секунд.</p>
Idle Time to Slide Show (s) Время до перехода в слайд-шоу (с)	<p>Время бездействия, по истечении которого на экране автоматически запускается слайд-шоу.</p> <p>Значение может быть отключено или установлено в диапазоне от 3 до 999 секунд.</p>

Slide Show Interval (s) Интервал слайд-шоу (с)	Интервал времени между переключением изображений в режиме слайд-шоу. Функция может быть отключена или для нее может быть установлено значение в диапазоне от 3 до 999 секунд.
Idle Time to Sleep (m) Время бездействия до перехода в режим ожидания (мин)	Время бездействия, по истечении которого устройство переходит в режим ожидания (спящий режим). Функция может быть отключена или для нее может быть установлено значение в диапазоне от 1 до 999 минут.
Main Screen Style Стиль главного экрана	Выбор стиля отображения главного экрана в соответствии с предпочтениями пользователя.

9.2 Настройки голоса

Нажмите **Voice** (Голос) в интерфейсе **Personalize** (Персонализация), чтобы настроить параметры голосового/звукового оповещения.

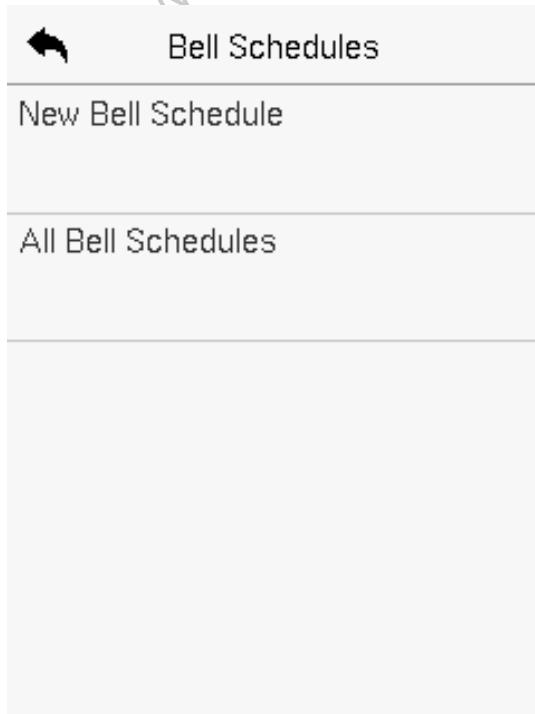


Описание функции

Название функции	Описание
Voice Prompt Голосовая подсказка	Включение или отключение голосовых подсказок при выполнении операций.
Touch Prompt Звук нажатия	Включение или отключение звукового сопровождения при нажатии клавиш.
Volume Громкость	Регулировка уровня громкости устройства в диапазоне от 0 до 100.

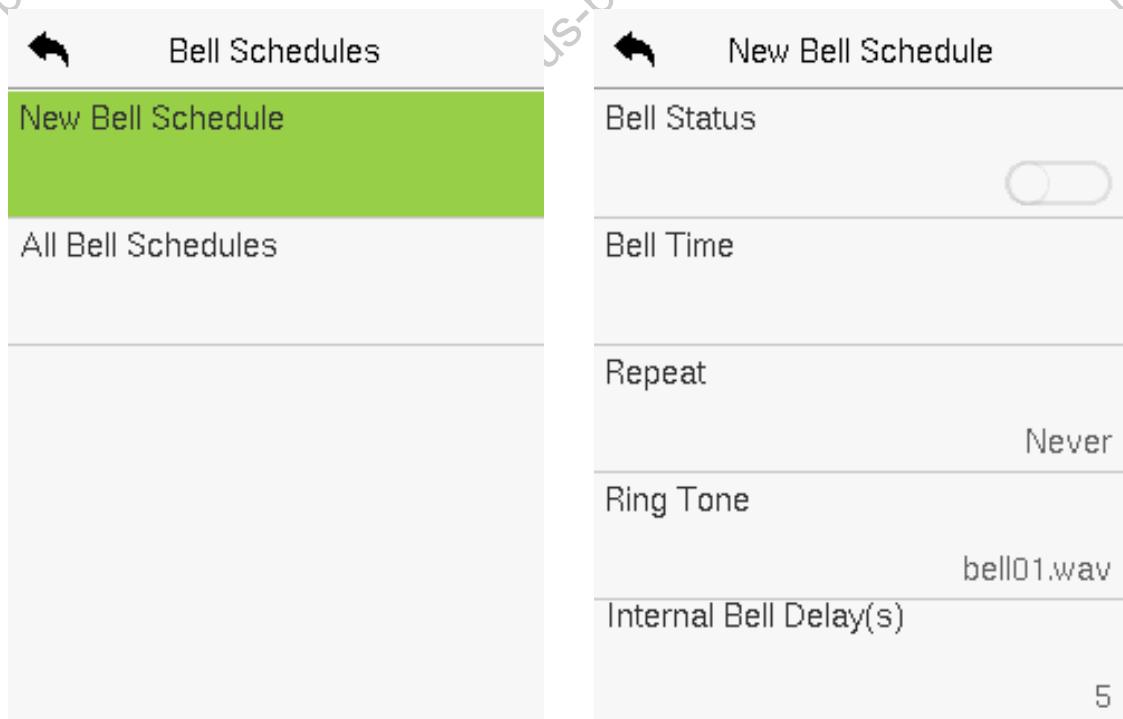
9.3 Расписание звонков

Нажмите **Bell Schedules** (Расписание звонков) в интерфейсе **Personalize** (Персонализация), чтобы настроить параметры звонка.



➤ Новое расписание звонков

Нажмите **New Bell Schedule** (Новое расписание звонков) в интерфейсе **Bell Schedule** (Расписание звонков), чтобы добавить новое расписание.



Описание функции

Название функции	Описание
Bell Status Время звонка	Включение или отключение функции звонка.
Bell Time Время звонка	После установки требуемого времени устройство автоматически активирует звонок в указанный период.
Repeat Повтор	Установите необходимое количество повторений для запланированного звонка.
Ring Tone Мелодия звонка	Выберите мелодию звонка.
Internal Bell Delay(s) Задержка внутреннего звонка (с)	Установите время повторения внутреннего звонка. Допустимые значения в диапазоне от 1 до 999 секунд.

➤ **Все расписания звонков**

После создания расписания, в интерфейсе **Bell Schedules** (Расписание звонков) нажмите **All Bell Schedules** (Все расписания звонков), чтобы просмотреть новое расписание.

➤ **Редактирование запланированного звонка**

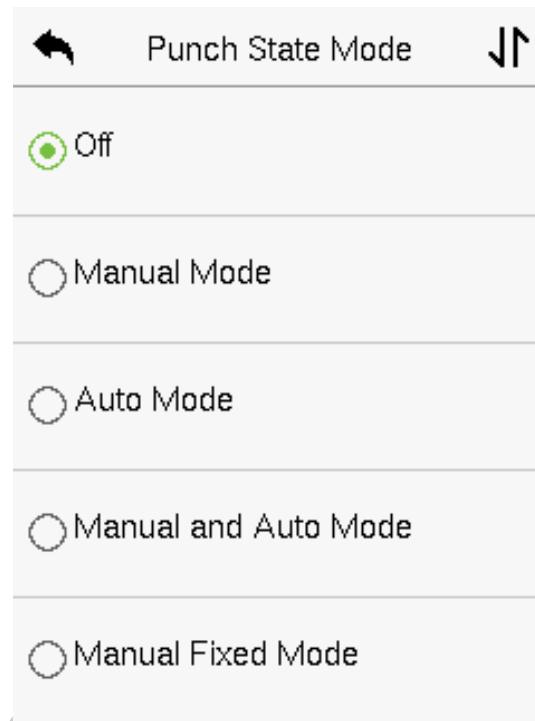
В интерфейсе **All Bell Schedules** (Все расписания звонков) выберите нужное расписание, нажмите **Edit** (Редактировать), чтобы изменить его. Процесс редактирования аналогичен созданию нового расписания.

➤ **Удаление звонка**

В интерфейсе **All Bell Schedules** (Все расписания звонков) выберите нужное расписание, нажмите **Delete** (Удалить), а затем подтвердите действие, нажав **Yes** (Да), чтобы удалить выбранный звонок.

9.4 Параметры отметки

Нажмите **Punch States Options** (Параметры отметки) в интерфейсе **Personalize** (Персонализация), чтобы настроить параметры состояния отметки.



Описание функции

Название функции	Описание
Punch State Mode Режим отметки	<p>Off (Выкл.): Функция отметки отключена. Клавиша отметки, настроенная в меню Shortcut Key Mappings (Назначение горячих клавиш), станет неактивной.</p> <p>Manual Mode (Ручной режим): Клавиша статуса отметки переключается вручную и исчезает с экрана по истечении времени Punch State Timeout (Тайм-аут отметки).</p> <p>Auto Mode (Автоматический режим): Клавиша отметки автоматически переключается на заданный статус в соответствии с предустановленным расписанием, которое можно настроить в меню Shortcut Key Mappings (Назначение горячих клавиш).</p> <p>Manual and Auto Mode (Ручной и автоматический режим): На главном экране отображается клавиша автоматической отметки. Пользователи также могут вручную выбрать альтернативный статус присутствия. По истечении тайм-аута клавиша ручного переключения вернется к статусу автоматической отметки.</p> <p>Manual Fixed Mode (Ручной фиксированный режим): После ручной установки клавиши отметки на определенный статус, функция останется неизменной до следующего ручного переключения.</p> <p>Fixed Mode (Фиксированный режим): Отображается только клавиша фиксированной ручной отметки. Пользователи не могут изменить статус нажатием других клавиш.</p>

9.5 Назначение горячих клавиш

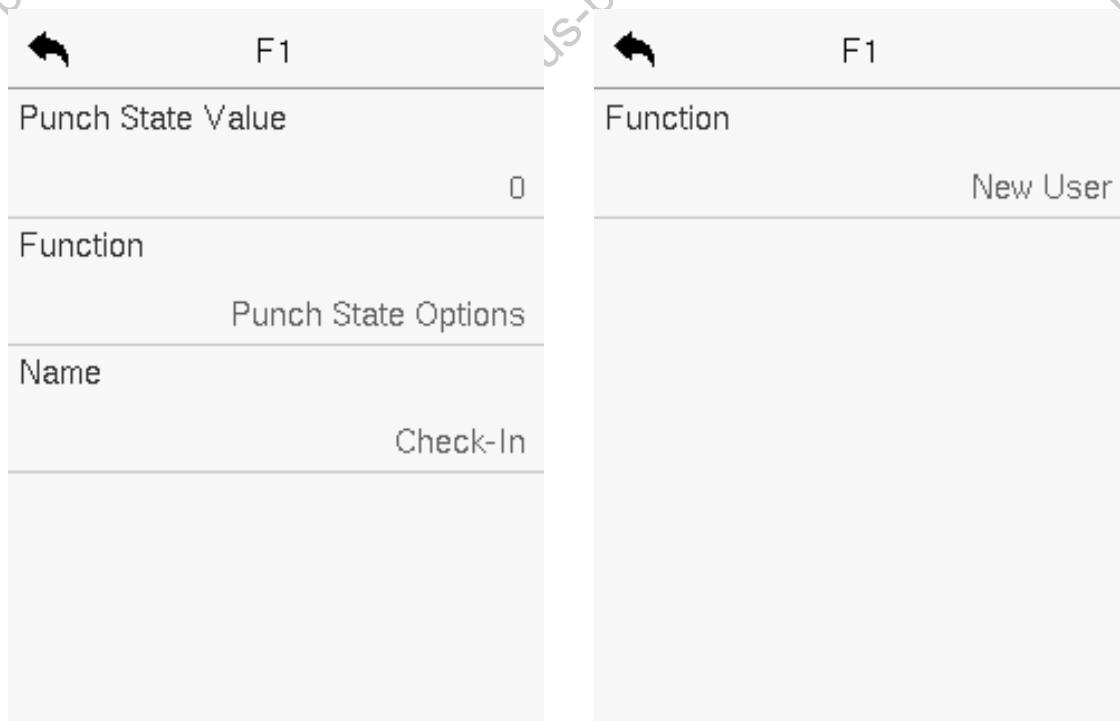
Пользователи могут назначить горячие клавиши для статусов присутствия и функциональных клавиш, которые будут отображаться на главном экране. При нажатии этих клавиш на главном экране непосредственно откроется соответствующий интерфейс статуса присутствия или функции.

Нажмите **Shortcut Key Mappings** (Назначение горячих клавиш) в интерфейсе **Personalize** (Персонализация), чтобы настроить необходимые сочетания клавиш.



- В интерфейсе **Shortcut Key Mappings** (Назначение горячих клавиш) выберите нужную клавишу для настройки её параметров.
- В интерфейсе настройки выбранной клавиши (например, "F1") нажмите **function** (функция), чтобы задать её назначение: либо как клавишу статуса отметки (**punch state key**), либо как функциональную клавишу (**function key**).

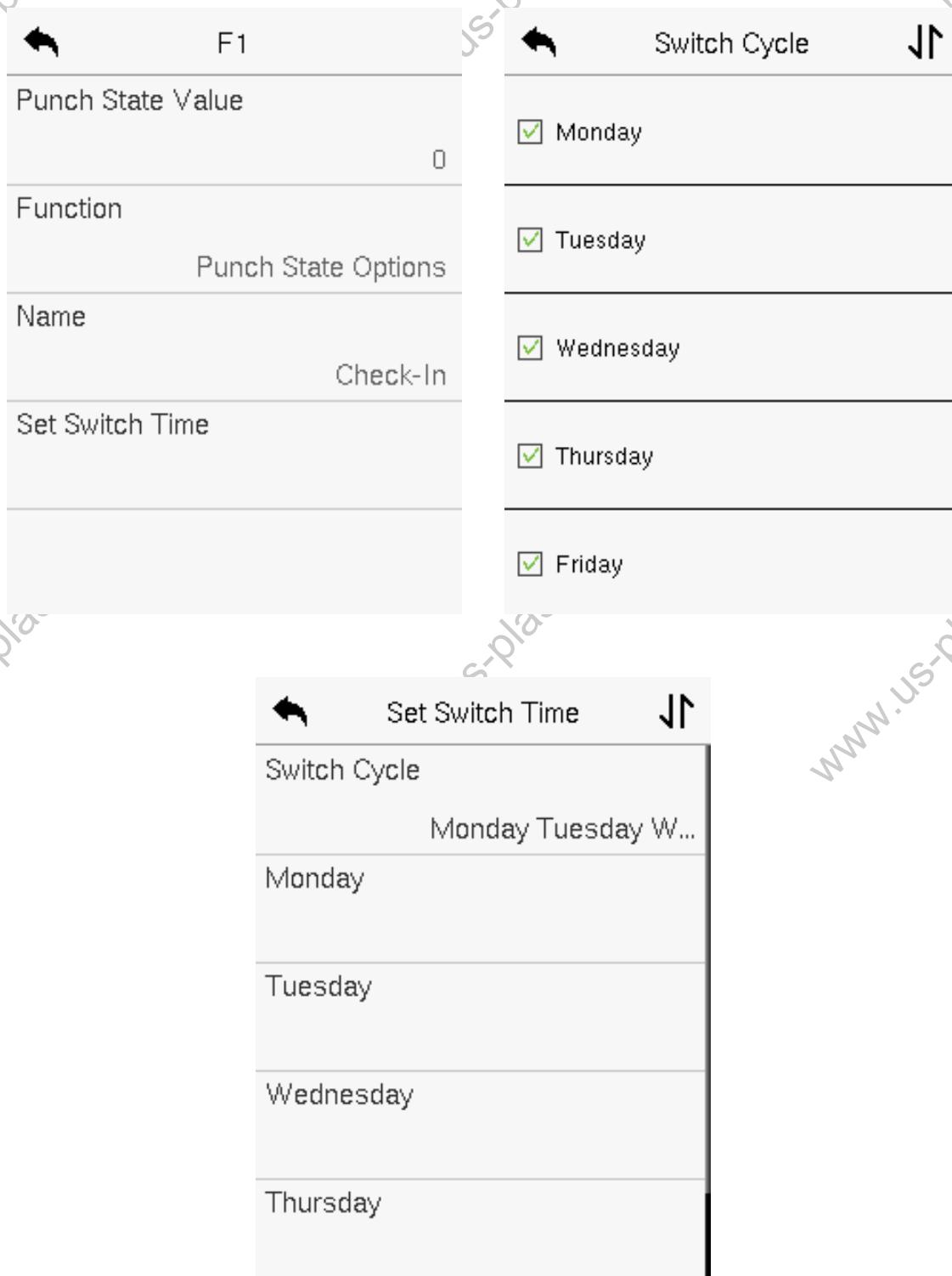
Если клавиша назначается как функциональная (например, для функций **New user** (Новый пользователь), **All users** (Все пользователи) и т.д.), конфигурация завершается, как показано на изображении ниже.



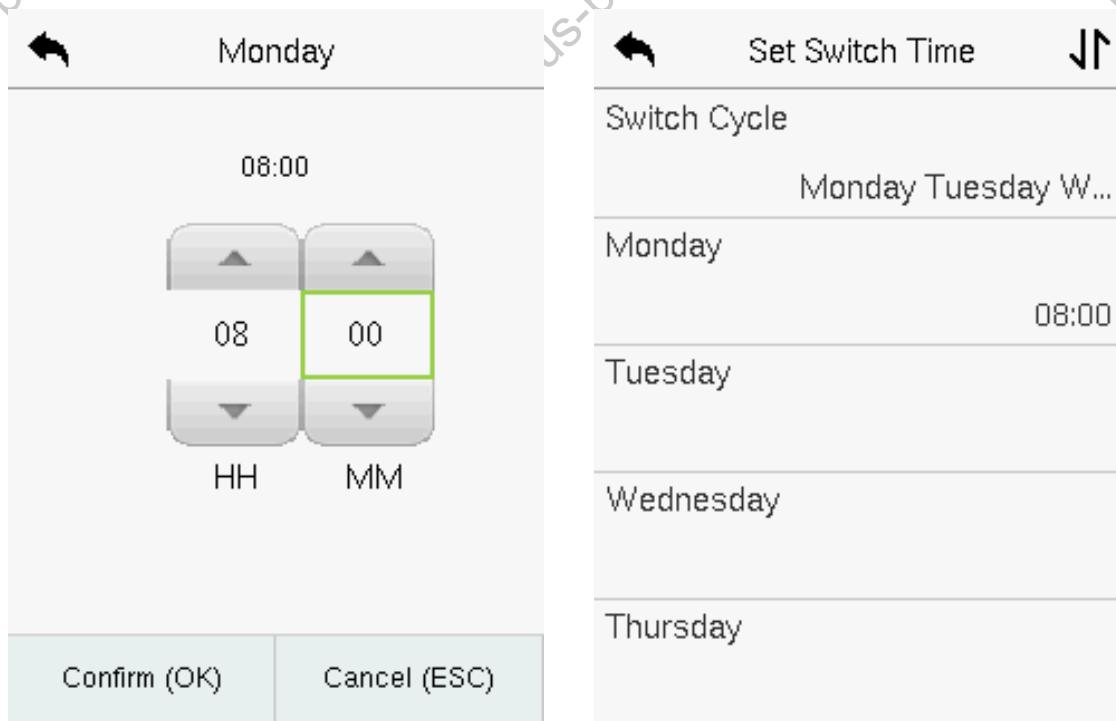
Если клавиша назначается как клавиша статуса отметки (например, **check in** (приход), **check out** (уход) и т.д.), необходимо задать значение статуса отметки (допустимый диапазон 0–250) и его название.

➤ **Настройка времени переключения**

- Время переключения настраивается в соответствии с параметрами отметки (Punch State Options).
- Время переключения необходимо задавать, когда **Режим отметки (Punch State Mode)** установлен в **Автоматический режим (Auto Mode)**.
- В интерфейсе настройки горячей клавиши (Shortcut Key) нажмите **Set Switch Time** (Установить время переключения), чтобы задать время.
- В интерфейсе **Switch Cycle** (Цикл переключения) выберите дни недели для переключения (понедельник, вторник и т.д.), как показано на изображении ниже.



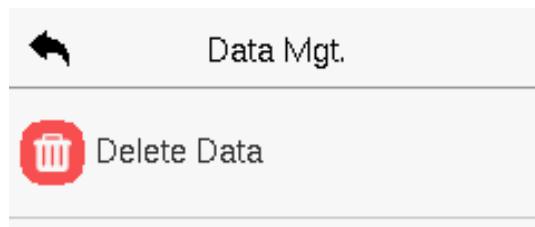
- После выбора дней цикла задайте время переключения для каждого дня и нажмите **OK** (OK), чтобы подтвердить, как показано на изображении ниже.



Примечание: Если для функции установлено значение **Undefined** (Не задано), устройство не активирует клавишу статуса отметки.

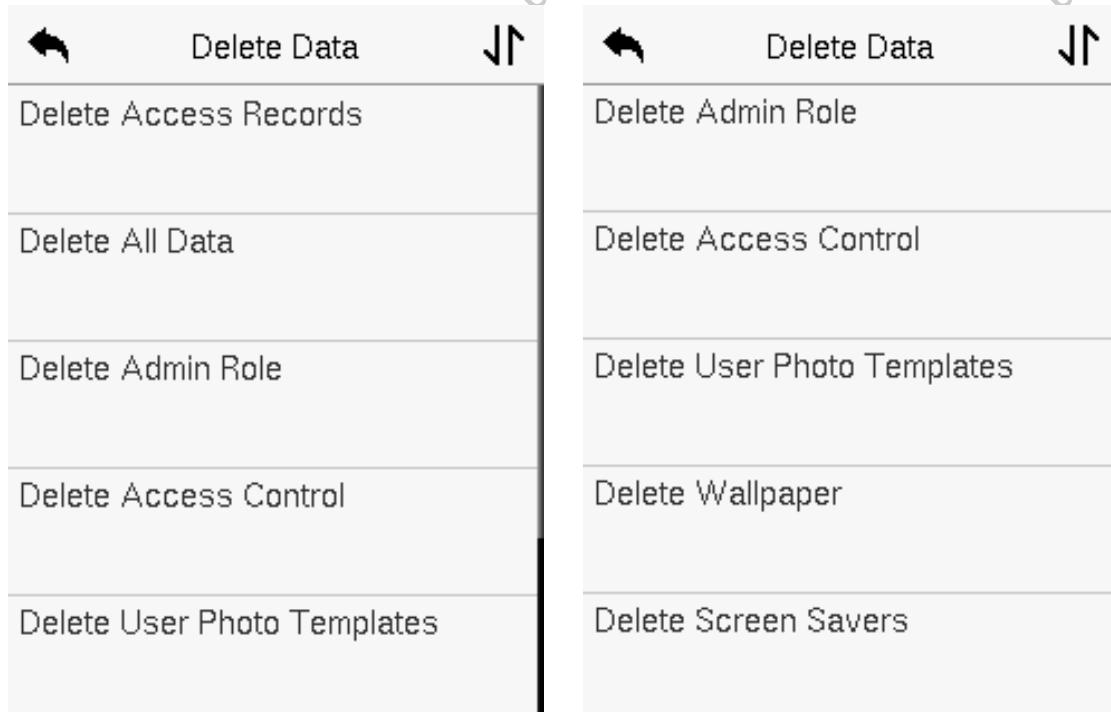
10 Управление данными

В Главном меню (Main Menu) нажмите **Data Mgt.** (Упр. данными / Управление данными), чтобы удалить соответствующие данные в устройстве.



10.1 Удаление данных

Нажмите **Delete Data** (Удалить данные) в интерфейсе **Data Mgt.** (Управление данными), чтобы удалить требуемые данные.

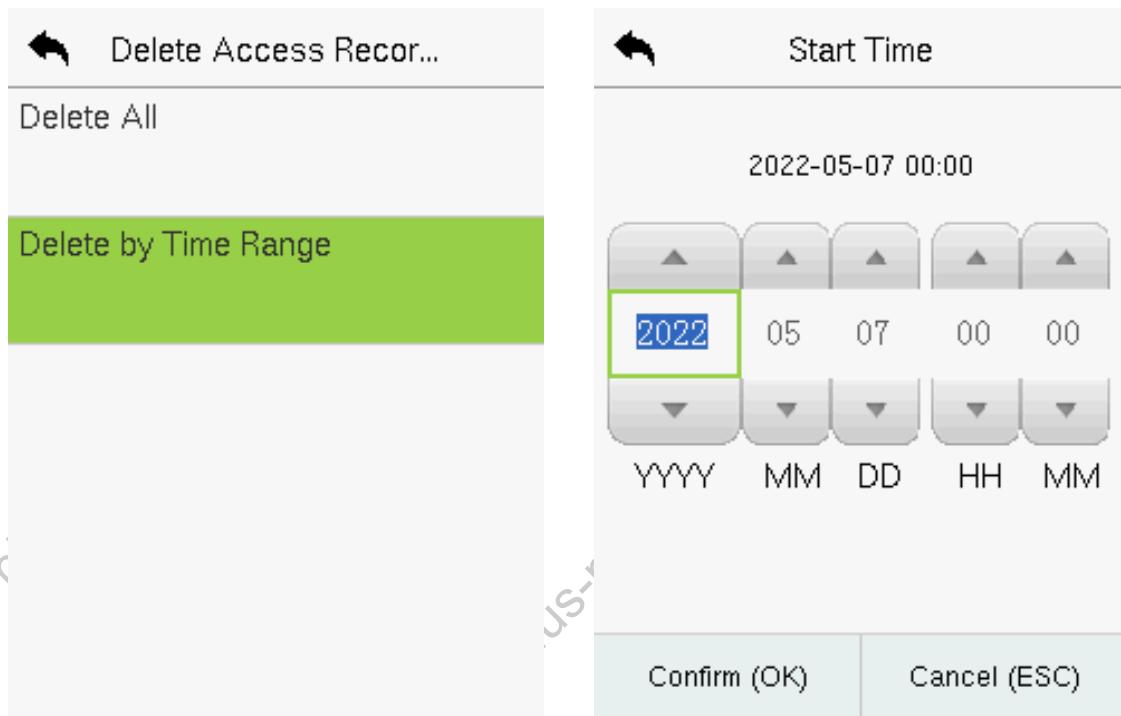


Описание функции

Название функции	Описание
Delete Access Records Удалить записи доступа	Удаление записей доступа по заданным условиям.

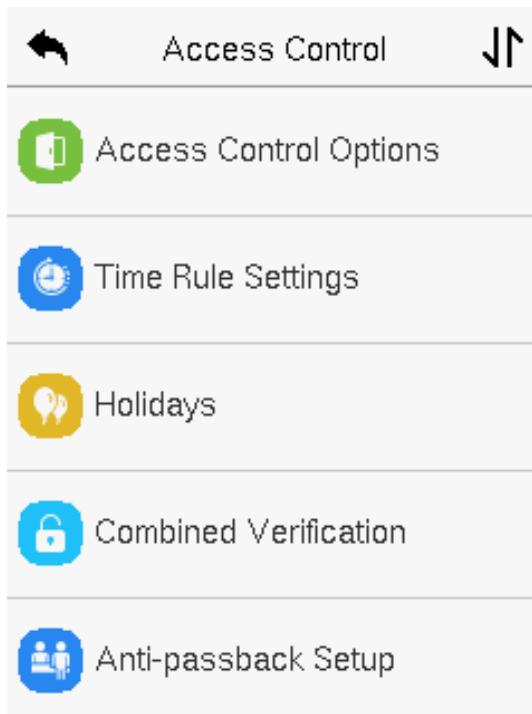
Delete All Data Удалить все данные	Удаление информации и записей доступа всех зарегистрированных пользователей.
Delete Admin Role Удалить роль администратора	Удаление всех привилегий администратора.
Delete Access Control Удалить контроль доступа	Удаление всех данных контроля доступа.
Delete User Photo Templates Удалить шаблоны фотографий пользователей	Удаление всех шаблонов фотографий пользователей с устройства.
Delete Wallpaper Удалить обои	Удаление всех обоев с устройства.
Delete Screen Savers Удалить заставки	Удаление всех заставок с устройства.

При удалении записей доступа, фотографий отметок или фотографий из стоп-листа пользователь может выбрать **Delete All** (Удалить все) или **Delete by Time Range** (Удалить по диапазону времени). При выборе удаления по диапазону времени необходимо задать конкретный временной интервал для удаления всех данных за указанный период.



1 Контроль доступа

В Главном меню (Main Menu) нажмите **Access Control** (Контроль доступа), чтобы настроить расписание открытия дверей, управление замками и другие параметры, связанные с контролем доступа.

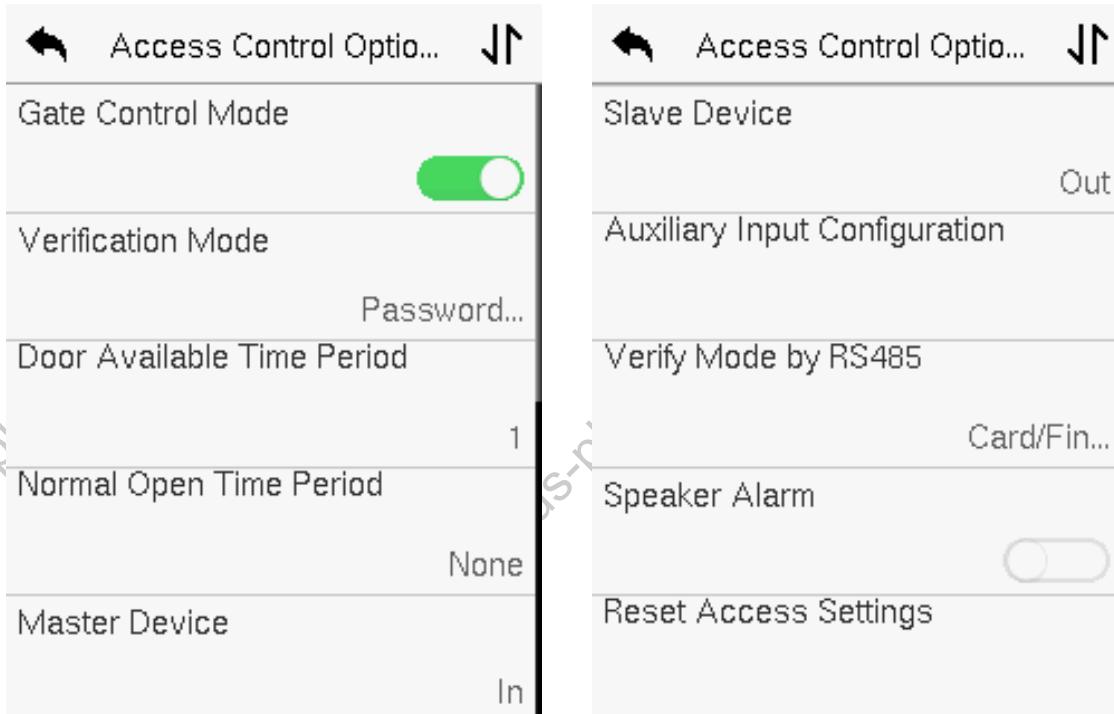


Для получения доступа зарегистрированный пользователь должен соответствовать следующим условиям:

1. Текущее время разблокировки соответствующей двери должно находиться в пределах любого действующего временного интервала пользователя.
2. Соответствующая группа пользователя должна быть уже установлена в комбинации разблокировки двери (если в той же комбинации доступа настроены и другие группы, то для открытия двери также требуется верификация их членов).
3. В настройках по умолчанию новые пользователи назначаются в первую группу с временным интервалом по умолчанию. Комбинация доступа для нее — «1», и по умолчанию она установлена в режиме разблокировки.

1.1 Опции контроля доступа

Нажмите **Access Control Options** (Опции контроля доступа) в интерфейсе **Access Control** (Контроль доступа), чтобы настроить параметры управляющего замка терминала и связанного оборудования.



Описание функции

Название функции	Описание
Gate Control Mode Режим управления воротами	Переключатель ВКЛ (ON) или ВыКЛ (OFF) для активации режима управления воротами. В режиме ВКЛ (ON) в интерфейсе становятся недоступны параметры Door Lock Delay (Задержка замка), Door Sensor Delay (Задержка датчика двери) и Door Sensor Type (Тип датчика двери).
Door Lock Delay (s) Задержка замка (с)	Время, в течение которого устройство удерживает электрозамок в разблокированном состоянии. Допустимое значение: 1–99 секунд.

Door Sensor Delay (s) Задержка датчика двери (с)	<p>Если дверь не заблокирована и остается открытой в течение определенного времени (Задержка датчика двери), будет активирована тревога.</p> <p>Допустимое значение задержки: от 1 до 255 секунд.</p>
Door Sensor Type Тип датчика двери	<p>Существует три типа датчика: None (Нет), Normal Open (Нормально разомкнутый) и Normal Closed (Нормально замкнутый).</p> <p>None (Нет): Датчик двери не используется.</p> <p>Normal Open (НО, Нормально разомкнутый): Цепь датчика разомкнута при закрытой двери (состояние покоя). При открытии двери цепь замыкается.</p> <p>Normal Closed (НЗ, Нормально замкнутый): Цепь датчика замкнута при закрытой двери (состояние покоя). При открытии двери цепь размыкается.</p>
Verification Mode Режим верификации	<p>Поддерживаемые режимы верификации: Пароль/Отпечаток/Карта/Лицо, Только отпечаток, Только ID пользователя, Пароль, Только карта, Отпечаток/Пароль, Отпечаток/Карта, ID пользователя + Отпечаток, Отпечаток + Пароль, Отпечаток + Карта, Отпечаток + Пароль + Карта, Пароль + Карта, Пароль/Карта, ID пользователя + Отпечаток + Пароль, Отпечаток + (Карта/ID пользователя), Только лицо, Лицо + Отпечаток, Лицо + Пароль, Лицо + Карта, Лицо + Отпечаток + Карта, Лицо + Отпечаток + Пароль.</p>
Door Available Time Period Доступное время для двери	<p>Настройка временного интервала, в течение которого дверь доступна для открытия.</p>

Normal Open Time Period Период нормально открытого состояния	Это запланированный временной интервал для режима " Normal Open " (Нормально открыто), в течение которого дверь постоянно находится в открытом состоянии.
Master Device Ведущее устройство	При конфигурации ведущего (master) и ведомого (slave) устройств можно установить статус ведущего устройства как Out (Уход) или In (Приход). Out (Уход): Запись верификации на ведущем устройстве считается записью ухода. In (Приход): Запись верификации на ведущем устройстве считается записью прихода.
Slave Device Ведомое устройство	При конфигурации ведущего и ведомого устройств можно установить статус ведомого устройства как Out (Уход) или In (Приход). Out (Уход): Запись верификации на ведомом устройстве считается записью ухода. In (Приход): Запись верификации на ведомом устройстве считается записью прихода.
Auxiliary Input Configuration Конфигурация вспомогательного входа	Настройка временного интервала разблокировки двери и типа вспомогательного выхода для дополнительного терминального устройства. Типы вспомогательного выхода включают: None (Нет), Trigger door open (Открыть дверь), Trigger Alarm (Тревога), Trigger door open and Alarm (Открыть дверь и тревога).
Speaker Alarm Звуковая сигнализация	Передает звуковой сигнал тревоги или сигнал о вскрытии локально. Когда дверь закрывается или верификация проходит успешно, система отменяет локальную тревогу.

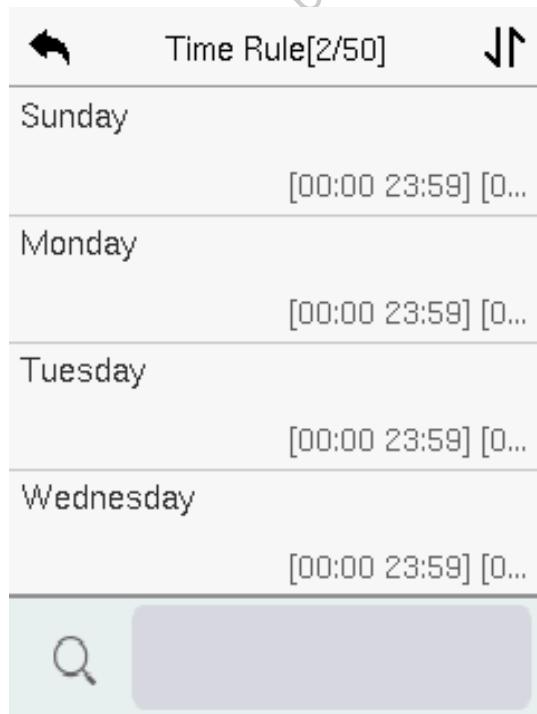
Reset Access Setting Сброс настроек доступа	Параметры сброса настроек контроля доступа включают: задержку замка, задержку датчика двери, тип датчика двери, режим верификации, доступное время для двери, период нормально открытого состояния, ведущее устройство и настройки тревоги. Однако удаленные данные контроля доступа в разделе Data Mgt. (Управление данными) не восстанавливаются.
---	---

11.2 Расписание времени

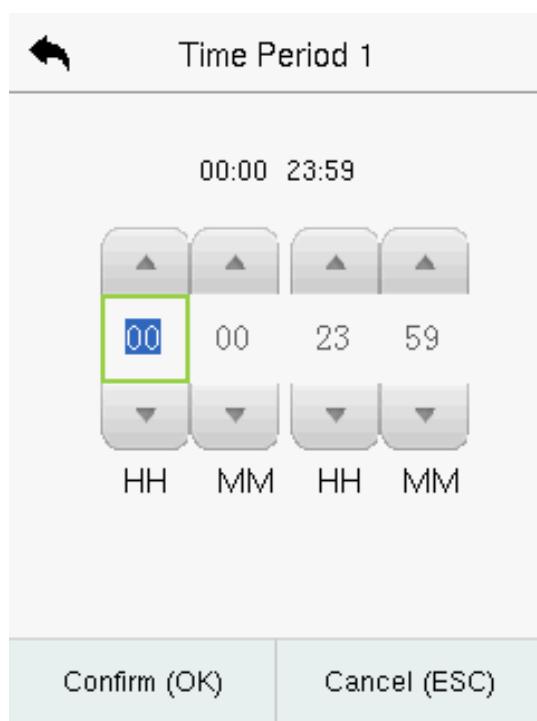
Нажмите **Time Rule Setting** (Настройка временных правил) в интерфейсе **Access Control** (Контроль доступа), чтобы настроить параметры времени.

- Вся система может содержать до 50 Временных периодов (Time Periods).
- Каждый временной период включает до 10 Временных зон (Time Zones) (например, 1 рабочая неделя и 3 праздничных дня). Каждая временная зона представляет собой стандартный 24-часовой период в сутки, и пользователь может проходить верификацию только в течение действующих временных периодов.
- Для каждой временной зоны можно задать максимум 3 временных периода. Связь между этими периодами — логическое «ИЛИ». Таким образом, если время верификации попадает в любой из этих периодов, верификация считается действительной.
- Формат временной зоны для каждого периода: **ЧЧ ММ-ЧЧ ММ**, что соответствует 24-часовому формату с точностью до минуты.

Нажмите на серое поле, чтобы найти нужную Временную зону (Time Zone) и указать её номер (максимум до 50 зон).



В интерфейсе настроек выбранного номера **Временной зоны** (Time Zone) нажмите на нужный день (например, Понедельник, Вторник и т.д.), чтобы установить время.



Задайте время начала и окончания, затем нажмите **OK**.

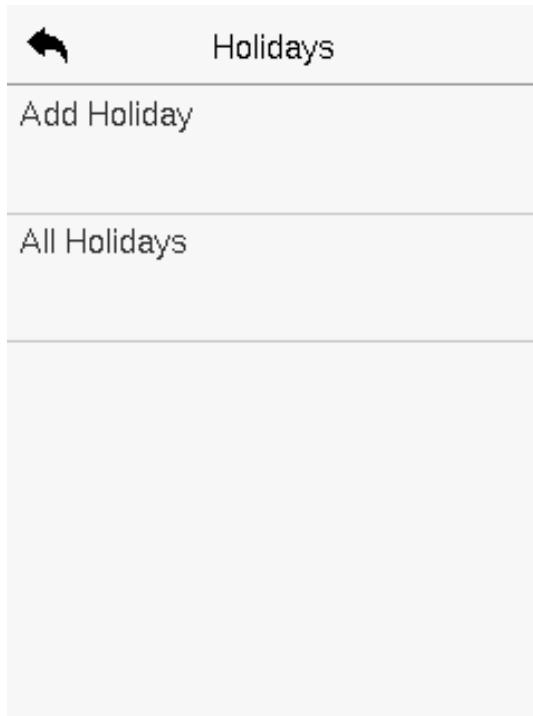
Примечание:

1. Дверь недоступна весь день, если время окончания (End Time) раньше времени начала (Start Time) (например, **23:57–23:56**)
2. Это временной интервал для допустимого доступа, если время окончания позже времени начала (например, **08:00–23:59**).
3. Дверь доступна весь день, если время окончания позже времени начала, при этом время начала — **00:00**, а время окончания — **23:59**.
4. Временная зона (Time Zone) 1 по умолчанию означает, что дверь открыта круглосуточно.

11.3 Праздничные дни

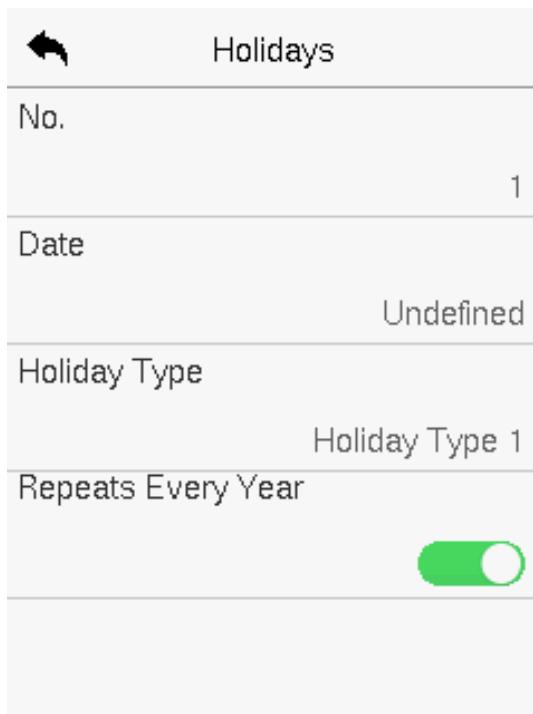
Когда наступает праздничный день, может потребоваться особое время доступа. Изменять время доступа для каждого пользователя в отдельности крайне неудобно, поэтому можно настроить время доступа на праздники, которое будет применяться ко всем сотрудникам, и пользователи смогут открывать дверь в эти дни.

Нажмите **Holidays** (Праздничные дни) в интерфейсе **Access Control** (Контроль доступа), чтобы настроить доступ на праздники.



➤ **Добавить новый праздник**

Нажмите Add Holiday (Добавить праздник) в интерфейсе Holidays (Праздничные дни) и задайте параметры праздника.



➤ **Редактировать праздник**

В интерфейсе **Holidays** (Праздничные дни) выберите запись праздника для изменения. Нажмите **Edit** (Редактировать), чтобы изменить его параметры.

➤ **Удалить праздник**

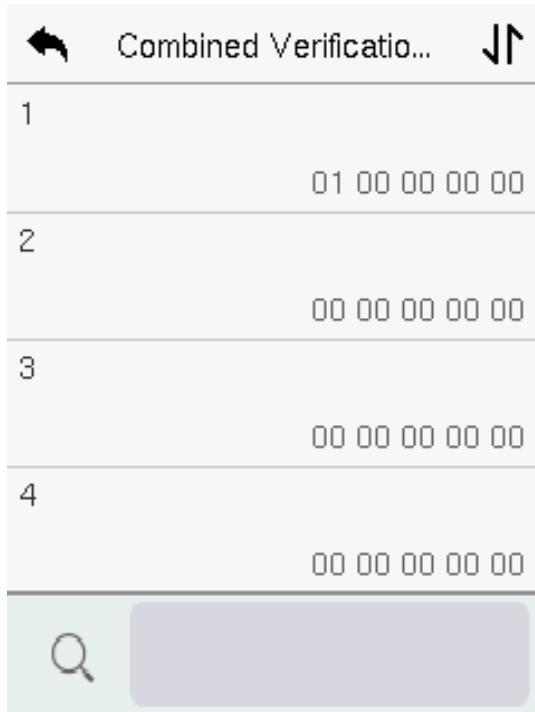
В интерфейсе **Holidays** (Праздничные дни) выберите запись праздника для удаления и нажмите **Delete** (Удалить). Нажмите **OK** (OK) для подтверждения удаления. После удаления этот праздник не будет отображаться в интерфейсе **All Holidays** (Все праздники).

11.4 Комбинированная верификация

Группы доступа объединяются в различные комбинации разблокировки двери для реализации многократной верификации и повышения уровня безопасности.

В комбинации разблокировки двери количество требуемых верификаций (N) может быть в диапазоне $0 \leq N \leq 5$, и эти N участников могут принадлежать как к одной группе доступа, так и к пяти разным группам доступа.

Нажмите **Combined Verification** (Комбинированная верификация) в интерфейсе **Access Control** (Контроль доступа), чтобы настроить параметры совместной проверки.



В интерфейсе комбинированной верификации выберите Комбинацию разблокировки двери (Door-unlock combination), которую требуется настроить. Используйте стрелки вверх и вниз для ввода номеров групп в комбинацию, затем нажмите OK.

Например:

- Если **Комбинация разблокировки 1** (Door-unlock combination 1) задана как **(01 03 05 06 08)**, это означает, что для открытия требуется 5 человек, каждый из которых принадлежит к разным группам доступа: Группа 1, Группа 3, Группа 5, Группа 6 и Группа 8 соответственно.
 - Если **Комбинация разблокировки 2** (Door-unlock combination 2) задана как **(02 02 04 04 07)**, это означает, что для открытия требуется 5 человек: первые двое — из Группы 2, следующие двое — из Группы 4, последний — из Группы 7.
- Если **Комбинация разблокировки 3** (Door-unlock combination 3) задана как **(09 09 09 09 09)**, это означает, что для открытия требуется 5 человек, и все они из Группы 9.

- Если **Комбинация разблокировки 4** (Door-unlock combination 4) задана как **(03 05 08 00 00)**, это означает, что для открытия требуется только 3 человека. Первый — из Группы 3, второй — из Группы 5, третий — из Группы 8. (Значение 00 означает, что позиция в комбинации не используется).

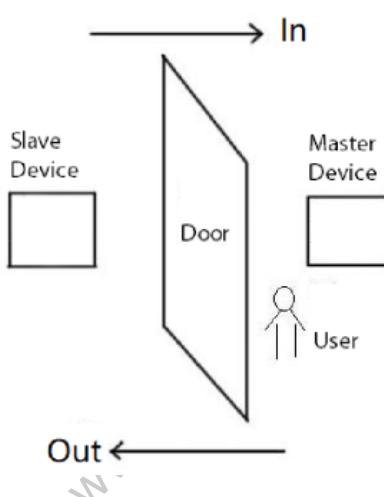
Примечание: Чтобы удалить комбинацию разблокировки, установите для всех позиций **Door-unlock combination** (Комбинация разблокировки) значение 0.

11.5 Настройка запрета повторного прохода

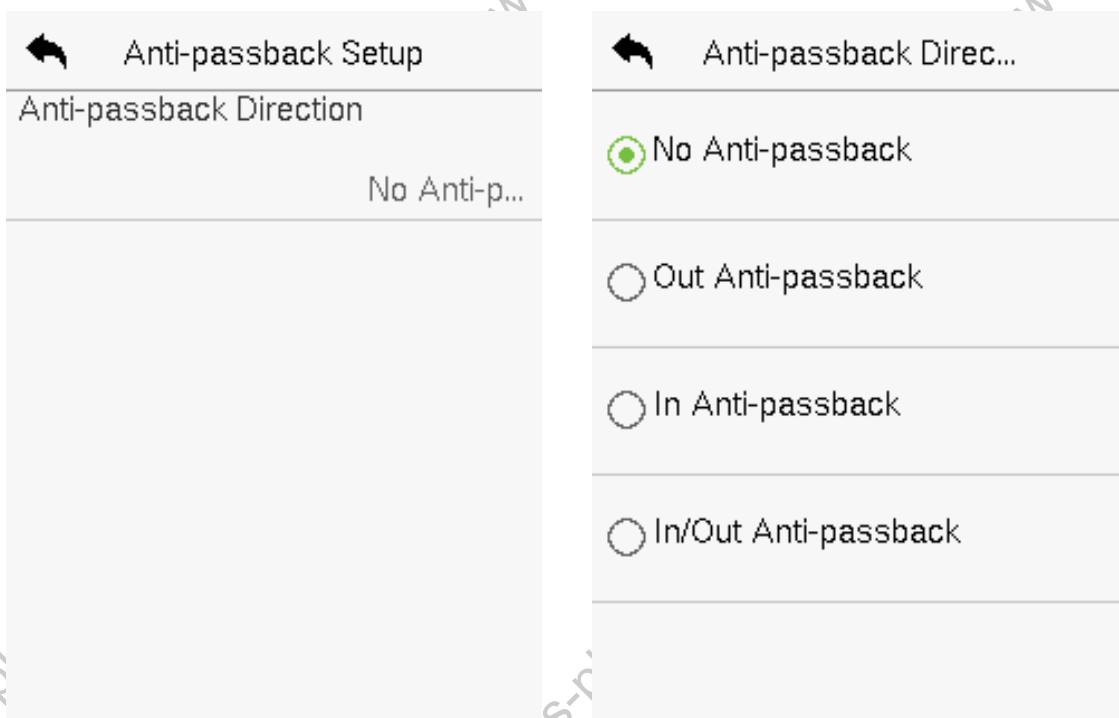
Пользователя может провести другой человек для входа без верификации, что создает угрозу безопасности. Для предотвращения таких ситуаций был разработан параметр **Anti-Passback** (Запрет повторного прохода). После его активации для открытия двери записи прихода и ухода должны чередоваться, формируя последовательный шаблон.

Эта функция требует совместной работы двух устройств:

Одно устройство устанавливается на внутренней стороне двери (ведущее устройство / master device), а другое — на внешней стороне (ведомое устройство / slave device). Устройства обмениваются данными по сигналу Wiegand. Формат Wiegand и Тип вывода (ID пользователя / Номер карты), используемые ведущим и ведомым устройствами, должны быть одинаковыми.



Нажмите **Anti-passback Setup** (Настройка контроля повторного входа) в интерфейсе **Access Control** (Контроль доступа).



Описание функции

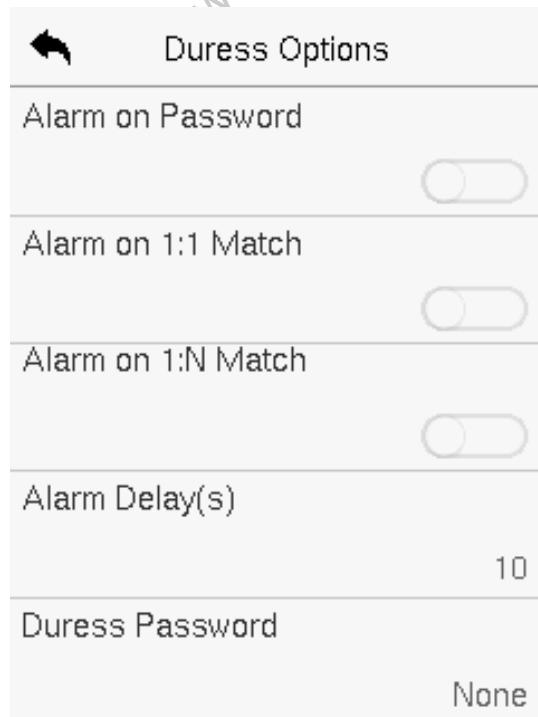
Название функции	Описание
Anti-passback Direction Направление контроля повторного входа	<p>No Anti-passback (Контроль отключен): Функция запрета повторного прохода отключена. Успешная верификация на ведущем или ведомом устройстве открывает дверь. Статус присутствия не сохраняется в этом режиме.</p> <p>Out Anti-passback (Контроль на выход): Пользователь может зарегистрировать уход (check-out) только в том случае, если предыдущей записью был приход (check-in), в противном случае активируется тревога. Однако пользователь может свободно регистрировать приход.</p> <p>In Anti-Passback (Контроль на вход): Пользователь может зарегистрировать приход (check-in) снова только в том случае, если предыдущей записью был уход (check-out), в противном случае активируется тревога. Однако пользователь может свободно регистрировать уход.</p>

In/Out Anti-passback (Контроль на вход/выход): В этом режиме пользователь может зарегистрировать приход (check-in) только если предыдущей записью был уход (check-out), и может зарегистрировать уход только если предыдущей записью был приход. В противном случае активируется тревога.

11.6 Настройки параметров сигнала тревоги

Если пользователь активирует функцию верификации под принуждением с помощью определенного метода(ов) аутентификации и, находясь под давлением, использует эту верификацию, устройство разблокирует дверь как обычно. Одновременно с этим отправляется сигнал для активации тревоги.

В интерфейсе **Access Control** (Контроль доступа) нажмите **Duress Options** (Параметры сигнала тревоги), чтобы настроить эти параметры.



Описание функции

Название функции	Описание
Alarm on Password Тревога при пароле	При использовании пользователем метода верификации по паролю будет сгенерирован сигнал тревоги, в противном случае сигнала не будет.
Alarm on 1:1 Match Тревога при верификации 1:1	При использовании пользователем метода верификации 1:1 будет сгенерирован сигнал тревоги, в противном случае сигнала не будет.
Alarm on 1:N Match Тревога при верификации 1:N	При использовании пользователем метода верификации 1:N будет сгенерирован сигнал тревоги, в противном случае сигнала не будет.
Alarm Delay (s) Задержка тревоги (с)	Сигнал тревоги не будет передан до истечения времени задержки. Значение может быть установлено в диапазоне от 1 до 999 секунд.
Duress Password Пароль для тревоги	Установите 6-значный пароль для активации тревоги. При вводе пользователем этого пароля во время верификации будет сгенерирован сигнал тревоги.

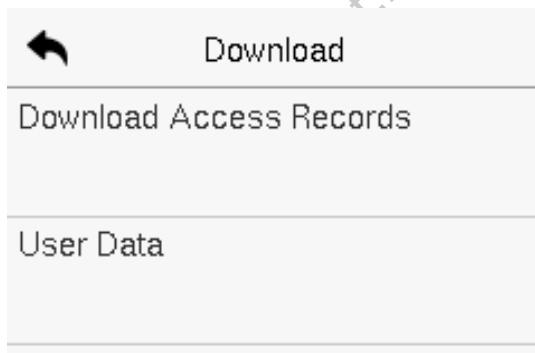
12 Менеджер USB

Позволяет импортировать информацию о пользователях, данные доступа и другие данные с USB-накопителя на компьютер или другие устройства.

Перед выгрузкой или загрузкой данных на USB-накопитель или с него сначала вставьте накопитель в USB-разъем.

В главном меню нажмите **USB Manager** (Менеджер USB).

12.1 Загрузка

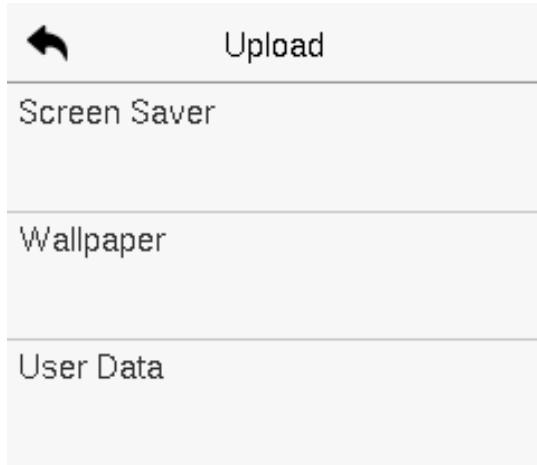


Описание функции

Название функции	Описание
Download Access Records Загрузить записи доступа	Загрузка данных о доступе за указанный период времени или всех данных на USB-накопитель.
User Data Данные пользователей	Загрузка всей информации о пользователях с устройства на USB-накопитель.

12.2 Загрузка на устройство

После успешной верификации личности пользователя запись о доступе сохраняется в устройстве. Эта функция позволяет пользователям просматривать журнал событий.



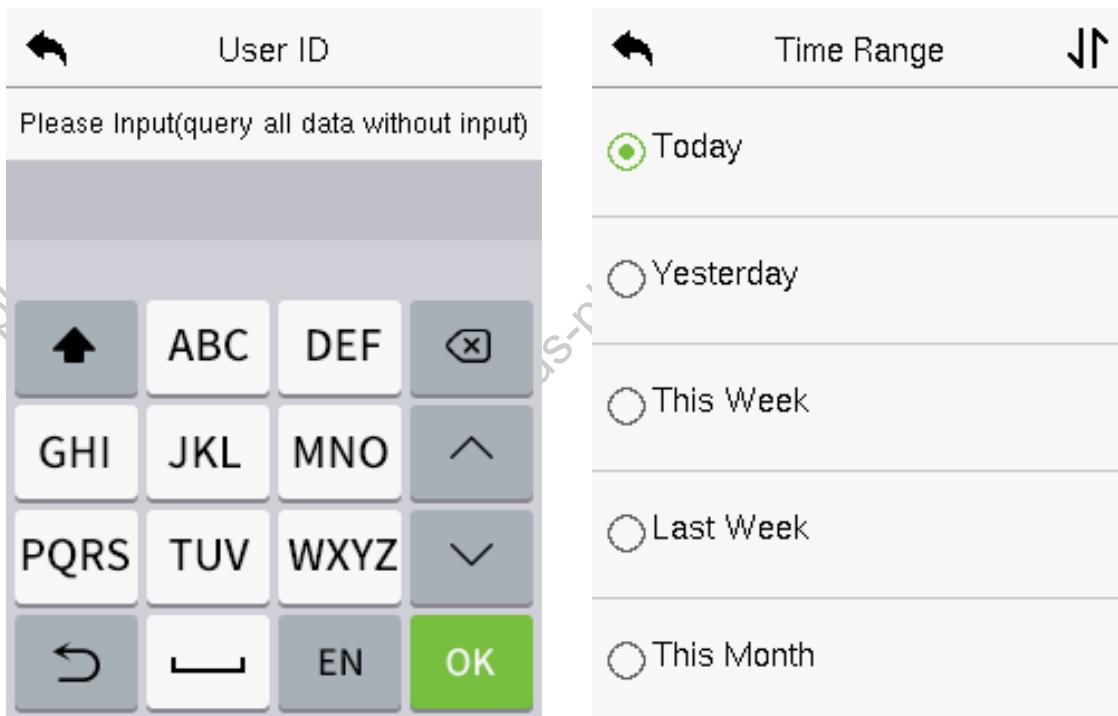
Описание функции

Название функции	Описание
Screen Saver Заставка	Выгрузка заставки с USB-накопителя на устройство. Перед выгрузкой можно выбрать Upload selected picture (Выгрузить выбранное изображение) или Upload all pictures (Выгрузить все изображения).
Wallpaper Обои	Выгрузка обоев с USB-накопителя на устройство. Перед выгрузкой можно выбрать Upload selected picture (Выгрузить выбранное изображение) или Upload all pictures (Выгрузить все изображения). Изображения появятся на экране после ручной настройки.
User Data Данные пользователей	Выгрузка всей информации о пользователях с USB-накопителя на устройство.

13 Поиск отметок

После успешной верификации личности пользователя запись о доступе сохраняется в устройстве. Эта функция позволяет пользователям просматривать журнал событий.

В Главном меню (Main Menu) выберите **Attendance Search** (Поиск отметок), чтобы найти нужные записи в журнале событий.



1. Введите ID пользователя (user ID) для поиска и нажмите OK (OK). Если необходимо найти записи всех пользователей, нажмите OK (OK), не вводя ID.

2. Выберите временной диапазон (time range), за который требуется найти записи.in

Date	User ID	Time
05-09	04	
	0	09:10 09:10 09:10
		09:10
05-07	08	
	0	11:58 11:58 11:52
		11:52 11:52 11:52
		11:52 11:52
05-06	04	
	0	09:03 09:03 09:03
		09:03
05-05	131	
	0	18:02 18:02 16:32
		16:32 16:30 16:30

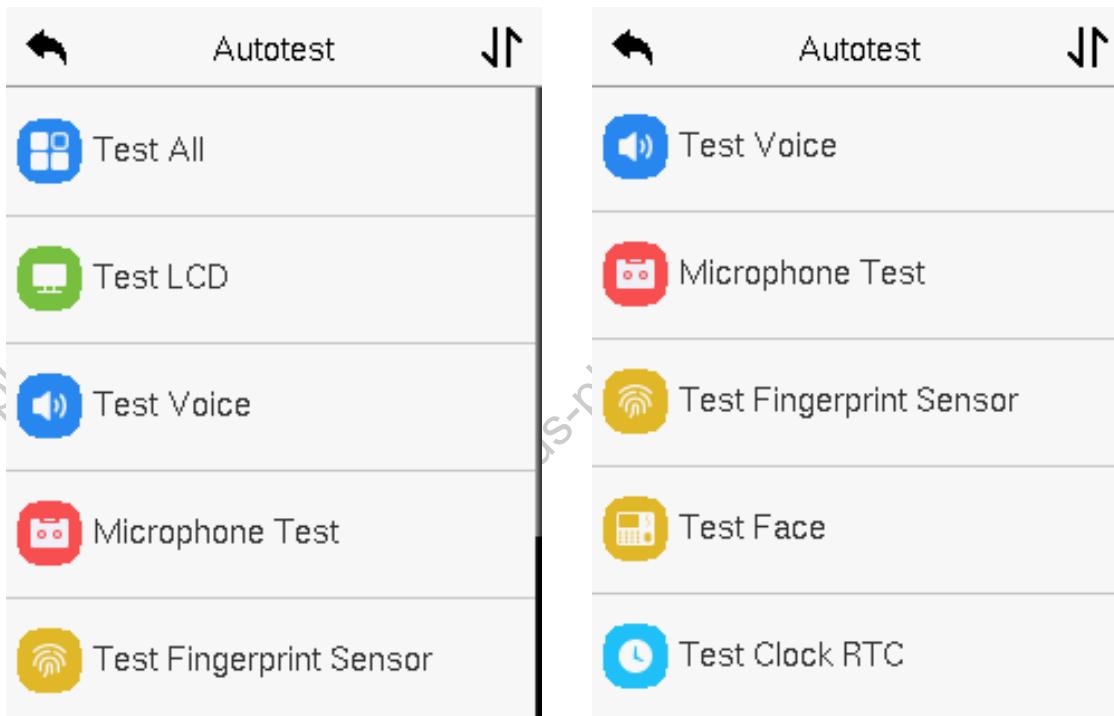
User ID	Name	Time
0		05-09 09:10
0		05-09 09:10
0		05-09 09:10
0		05-09 09:10

3. После завершения поиска нажмите на запись, выделенную зеленым цветом, чтобы просмотреть её детали.

4. На рисунке показаны детали выбранной записи.

14 Автотест

В Главном меню (Main Menu) нажмите **Autotest** (Автотест). Система автоматически проверит работоспособность различных модулей, включая **LCD** (дисплей), **Voice** (звук), **Microphone** (микрофон), **Fingerprint** (отпечаток пальца), **Camera** (камера) и **Real-Time Clock** (RTC, часы реального времени).



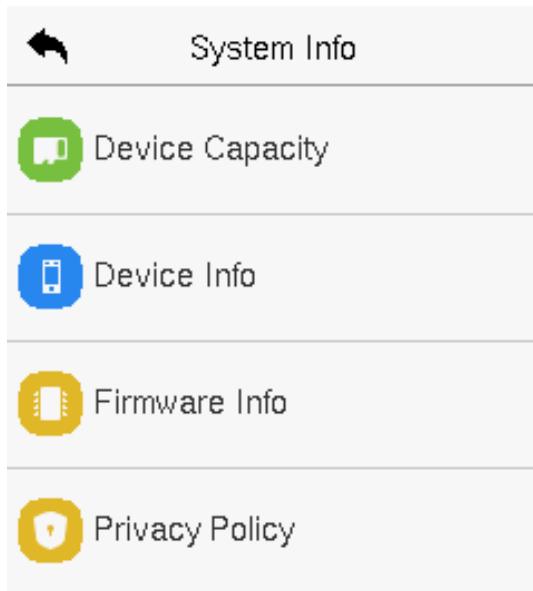
Описание функции

Название функции	Описание
Test All Тестиовать все	Автоматическая проверка работоспособности модулей LCD (дисплей), Voice (звук), Microphone (микрофон), Fingerprint (отпечаток пальца), Camera (камера) и Real-Time Clock (RTC, часы реального времени).
Test LCD Тестиовать LCD	Автоматическая проверка качества отображения экрана LCD путем демонстрации полноцветного, чистого белого и чистого черного изображений для контроля корректности отображения цветов.

Test Voice Тестировать голос	Автоматическая проверка целостности аудиофайлов, хранящихся в устройстве, и качества звука.
Micophone test Тест микрофона	Проверка работоспособности микрофона путем произнесения речи в него.
Test Fingerprint Sensor Тест датчика отпечатка пальца	Проверка датчика отпечатка пальца путем прикладывания пальца к сканеру для контроля четкости получаемого изображения. При прикладывании пальца изображение отпечатка будет отображаться на экране.
Test Face Тест лица	Проверка работоспособности камеры путем анализа сделанных снимков на предмет достаточной четкости.
Test Clock RTC Тест часов RTC	Проверка часов реального времени (RTC). Устройство тестирует нормальную и точную работу часов с помощью секундомера. Коснитесь экрана, чтобы начать отсчет, и коснитесь снова, чтобы остановить.

15 Системная информация

В Главном меню (Main Menu) нажмите **System Info** (Сист. информация / Системная информация), чтобы просмотреть состояние памяти, информацию о версии устройства, данные о прошивке и политику конфиденциальности.



Описание функции

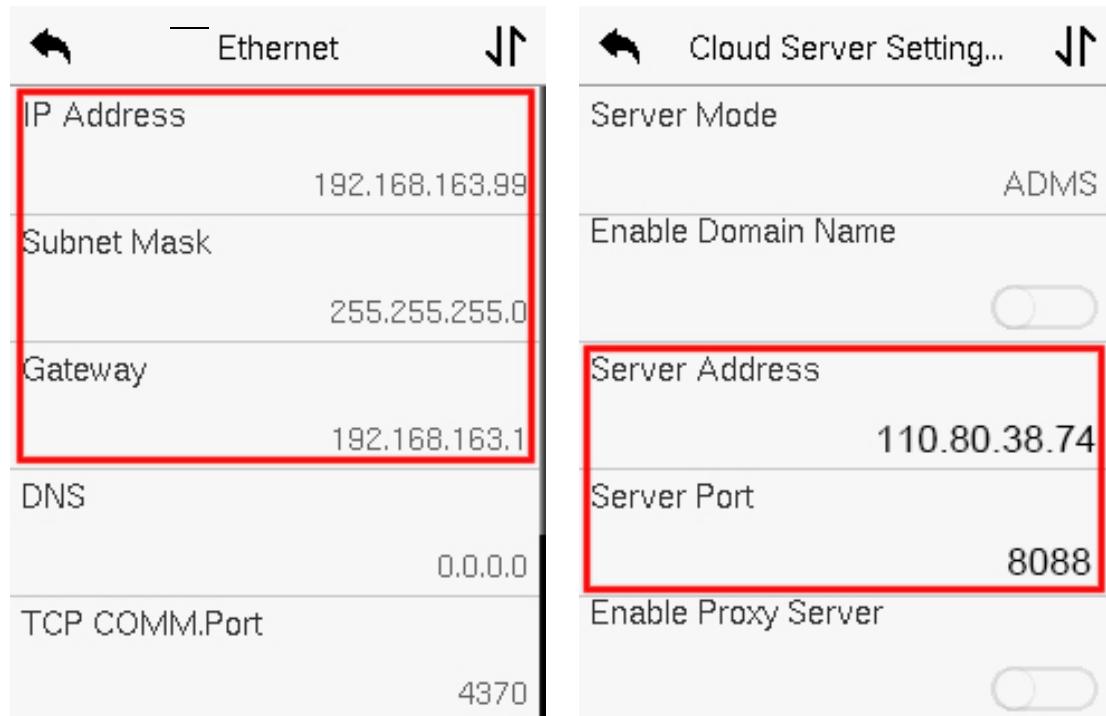
Название функции	Описание
Device Capacity Объем памяти устройства	Отображает текущее использование памяти устройства: пользователи, отпечатки пальцев, карты, пароли, лица, администраторы и записи.
Device Info Информация об устройстве	Отображает имя устройства, серийный номер, MAC-адрес, алгоритм отпечатка пальца, алгоритм распознавания лица, информацию о платформе, версию MCU, производителя и дату изготовления.
Firmware Info Информация о прошивке	Отображает версию прошивки и другую версионную информацию устройства.
Privacy Policy Политика конфиденциальности	Отображает политику конфиденциальности устройства.

16 Подключение к ПО ZKBio CVAccess

16.1 Настройка адреса связи

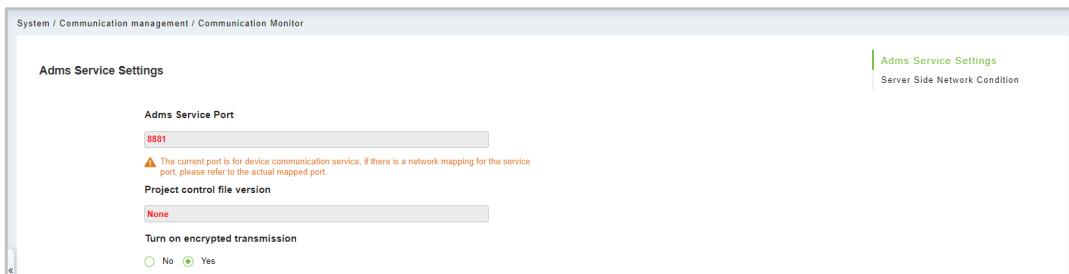
➤ Настройка на стороне устройства

1. В Главном меню (Main Menu) выберите COMM. > Ethernet (Связь > Ethernet), чтобы задать IP-адрес (IP address) и шлюз (gateway) устройства.
(Примечание: Убедитесь, что IP-адрес устройства находится в одной подсети с адресом сервера и может обмениваться данными с сервером ZKBio CVAccess.)
2. В Главном меню (Main Menu) нажмите COMM. > Cloud Server Setting (Связь > Настройки облачного сервера), чтобы задать адрес сервера (server address) и порт сервера (server port).
Адрес сервера (Server address): Укажите IP-адрес сервера ZKBio CVAccess.
Порт сервера (Server port): Укажите порт сервера ZKBio CVAccess.



➤ Настройка на стороне программного обеспечения

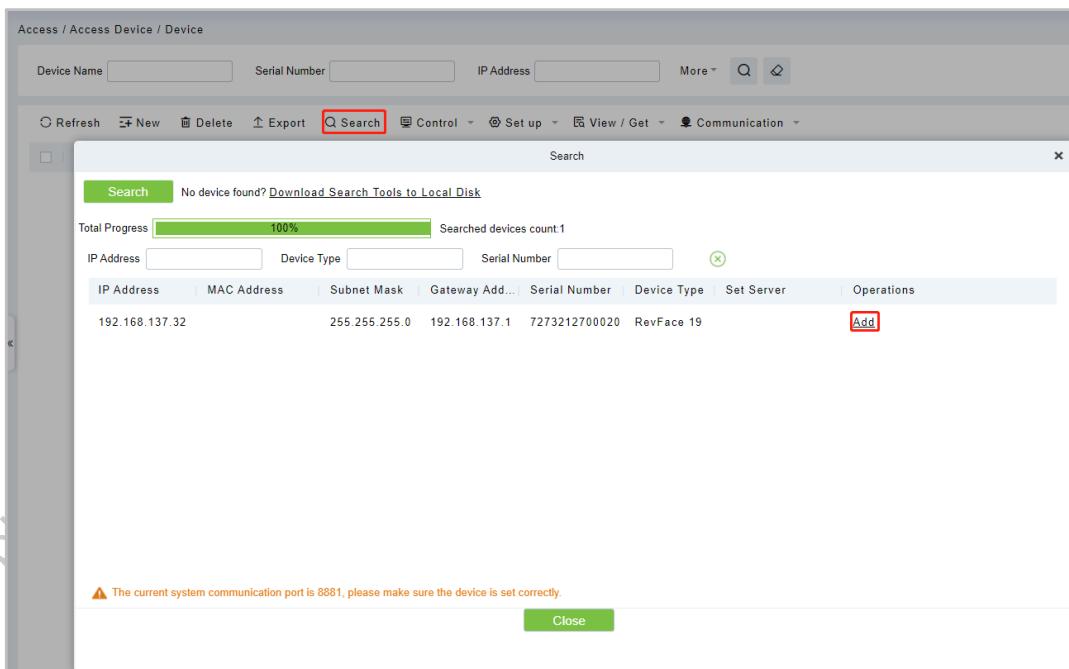
Войдите в программу ZKBio CVAccess, нажмите System > Communication > Communication Monitor (Система > Связь > Монитор связи), чтобы задать порт службы ADMS (ADMS service port), как показано на рисунке ниже:



16.2 Добавление устройства в программе

Добавление устройства путем поиска. Процесс следующий:

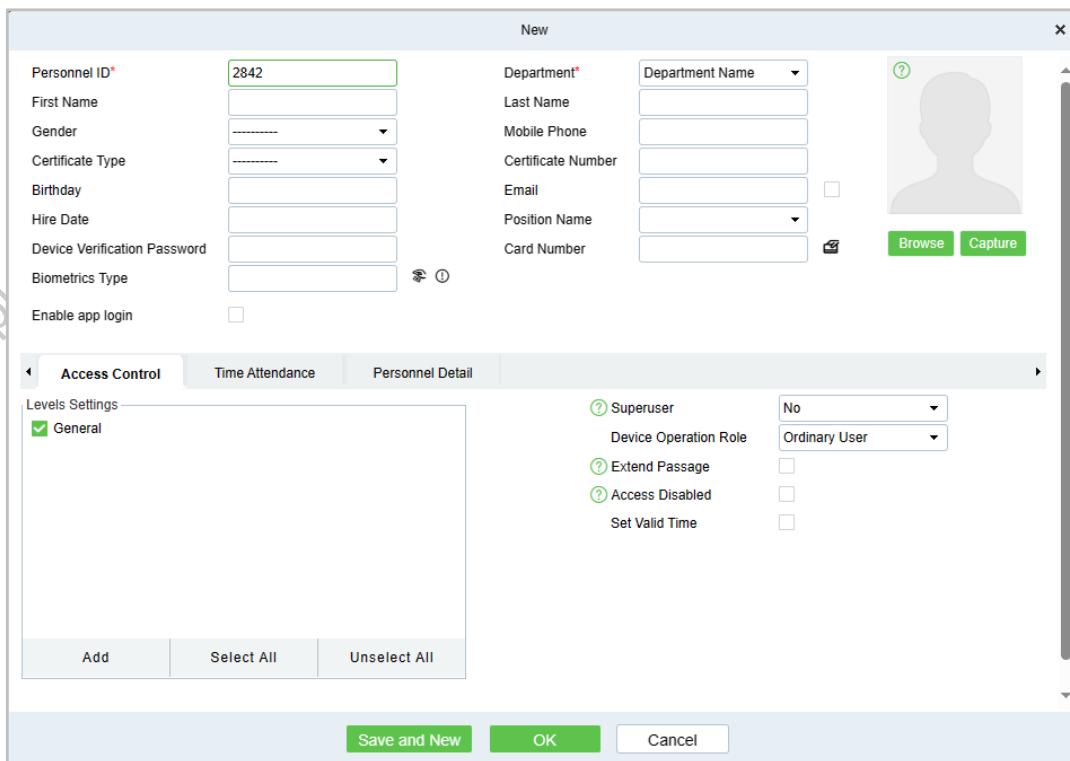
1. В программе нажмите Access > Device > Search Device (Доступ > Устройства > Поиск устройств), чтобы открыть интерфейс поиска.
2. Нажмите Search (Поиск), появится сообщение [Searching.....] (Идет поиск...).
3. После завершения поиска будет отображен список найденных контроллеров доступа и их общее количество.



4. В столбце Operation (Действия) нажмите [Add] (Добавить), откроется новое окно. В выпадающих списках выберите Icon type (Тип значка), Area (Зона) и Add to Level (Добавить на уровень), затем нажмите [OK] (OK), чтобы добавить устройство.

16.3 Добавление персонала в программе

1. В программе нажмите **Personnel > Person > New** (Персонал > Сотрудники > Новый):



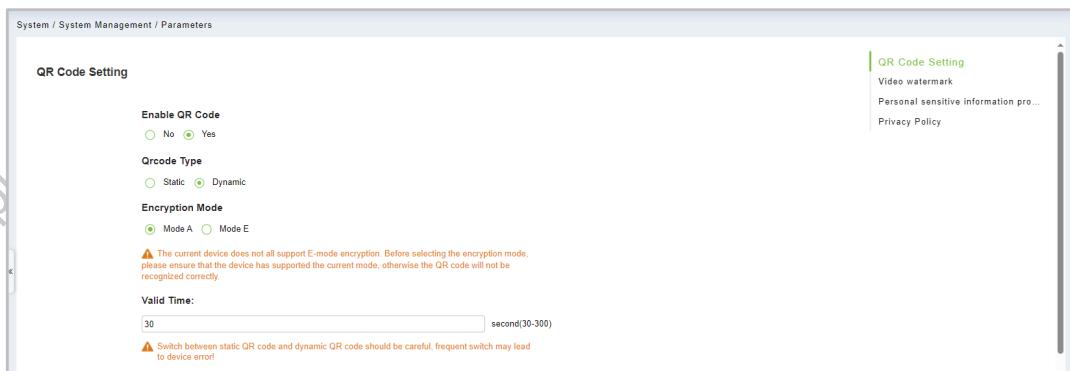
2. Заполните все обязательные поля и нажмите **[OK]** ([OK]), чтобы зарегистрировать нового пользователя.

3. Нажмите **Access > Device > Control > Synchronize All Data to Devices** (Доступ > Устройства > Управление > Синхронизировать все данные с устройствами), чтобы синхронизировать все данные с устройством, включая новых пользователей.

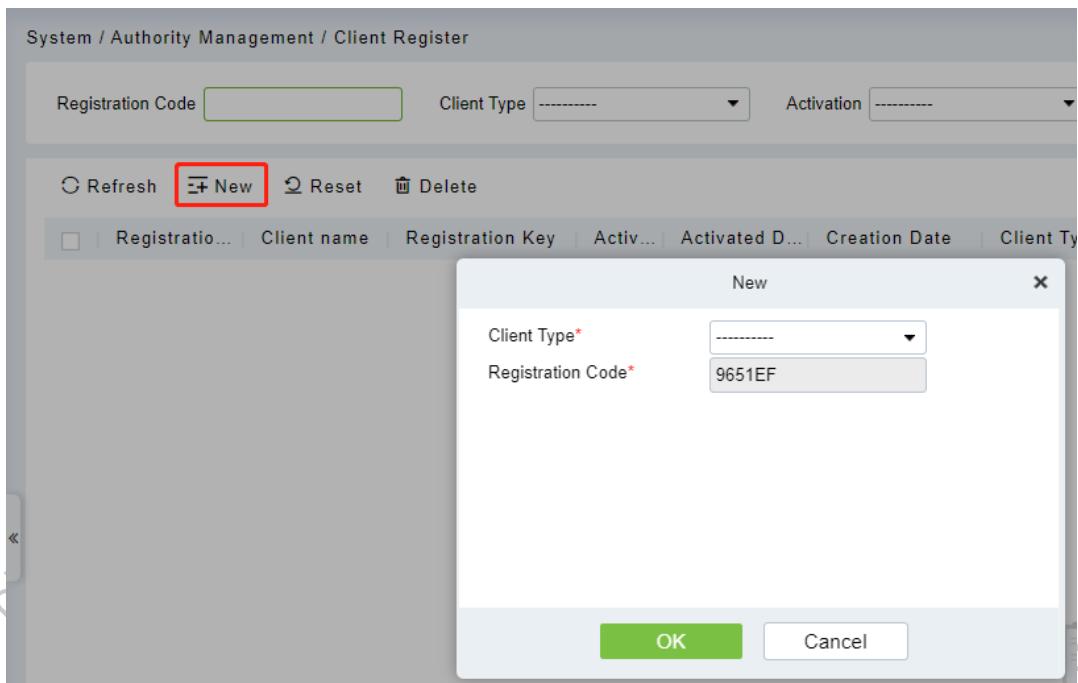
16.4 Мобильный идентификатор★

После загрузки и установки приложения пользователю необходимо настроить Сервер (Server) перед входом. Шаги следующие:

1. В программе **ZKBio CVAccess** перейдите в **System > System Management > Parameters** (Система > Управление системой > Параметры). Установите параметр **Enable QR Code** (Включить QR-код) в значение "**Yes**" ("Да") и выберите статус QR-кода в соответствии с фактической ситуацией. По умолчанию используется **Dynamic** (Динамический), также можно задать время действия QR-кода.



2. На Сервере (Server) выберите **System > Authority Management > Client Register** (Система > Управление правами > Регистрация клиента), чтобы добавить зарегистрированного клиента приложения (**App**).

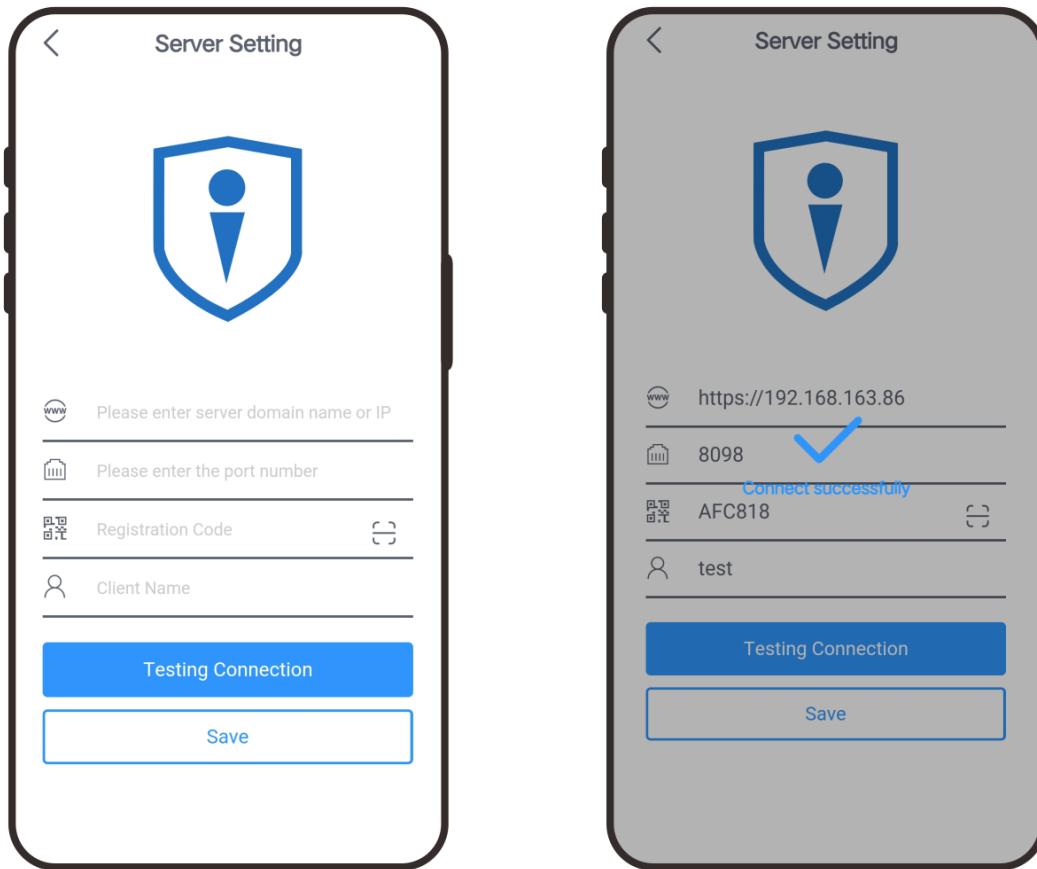


3. Откройте Приложение (App) на смартфоне. На экране входа нажмите **Server Setting** (Настройки сервера) и введите **IP-адрес** (IP Address) или доменное имя (domain name) сервера, а также его номер порта (port number).

Примечание: Смартфон и сервер должны находиться в одной подсети.

4. Нажмите значок **QR Code** (QR-код), чтобы отсканировать QR-код нового клиента приложения. После успешной идентификации клиента задайте его имя и нажмите **Connection Test** (Тест соединения).

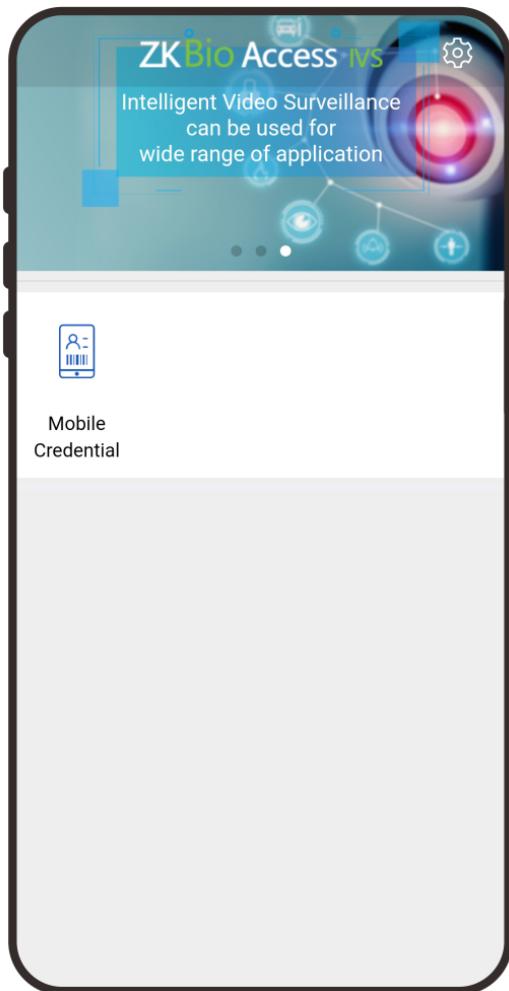
5. После успешного подключения к сети нажмите **Save** (Сохранить).



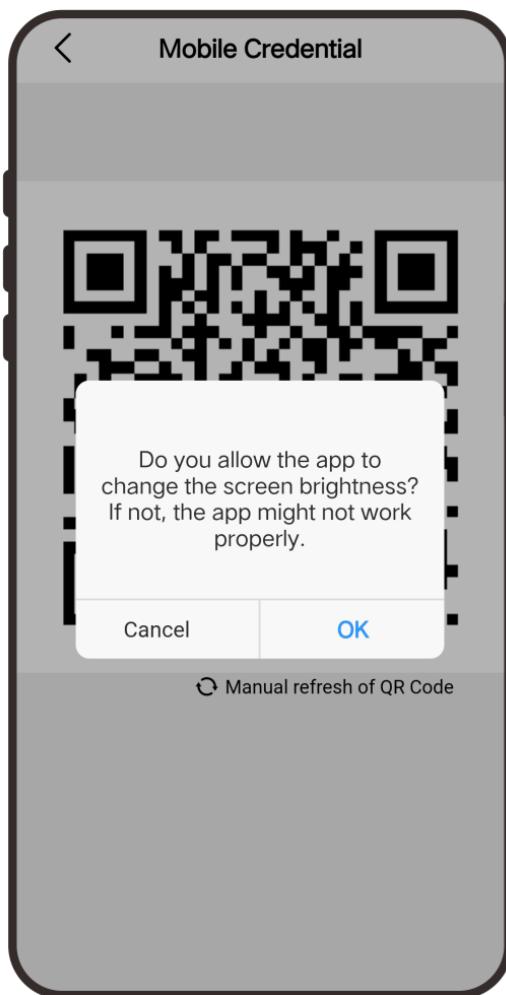
Функция **Mobile Credential** (Мобильный идентификатор) активна только при входе в качестве сотрудника (employee). Нажмите **Employee** (Сотрудник), чтобы перейти на экран входа для сотрудников. Введите ID сотрудника (employee ID) и пароль (password) (по умолчанию: 123456) для входа.

6. В приложении нажмите **Mobile Credential** (Мобильный идентификатор), и появится QR-код, который содержит информацию об **ID сотрудника** (employee ID) и **номере карты** (card number) (статический QR-код содержит только номер карты).

7. Этот QR-код может заменить физическую карту на определенном устройстве для осуществления бесконтактной аутентификации и открытия двери.



8. При первом использовании этой функции приложение запросит разрешение на изменение настроек яркости экрана, как показано на рисунке:



9. QR-код автоматически обновляется каждые 30 секунд и поддерживает ручное обновление.

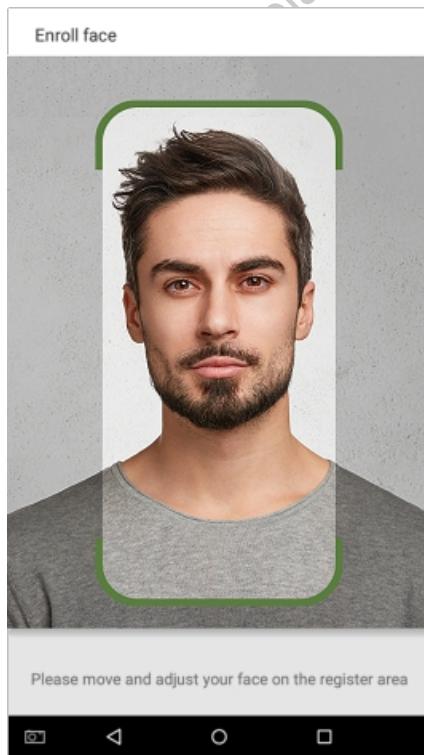


Примечание: За подробными инструкциями по другим операциям обратитесь к Руководству пользователя ZKBio CVAccess (ZKBio CVAccess User Manual).

Приложение 1

Требования к живой регистрации и сбору шаблонов лица в видимом свете

- 1) Рекомендуется проводить регистрацию в помещении с подходящим источником света, без недодержки или передержки на лице.
- 2) Не направляйте устройство на источники наружного света, такие как дверь или окно, или другие яркие источники света.
- 3) Для регистрации рекомендуется носить одежду темного цвета, отличного от цвета фона.
- 4) Правильно откройте лицо и лоб, не закрывайте лицо и брови волосами.
- 5) Рекомендуется сохранять обычное выражение лица. (Улыбка допустима, но не закрывайте глаза и не наклоняйте голову в какую-либо сторону).
- 6) Для лиц в очках требуется два изображения: одно в очках, другое без них.
- 7) Не носите аксессуары, такие как шарф или маска, которые могут закрывать рот или подбородок.
- 8) Смотрите прямо на регистрирующее устройство и расположите лицо в зоне захвата изображения, как показано на рисунке ниже.
- 9) Не допускайте присутствия более одного лица в зоне захвата.
- 10) Рекомендуемое расстояние для захвата изображения — от 50 до 80 см. (Расстояние можно регулировать в зависимости от роста).



Требования к цифровым шаблонам лица в видимом свете

Цифровое фото должно быть прямолинейным, цветным, полупортретным, с изображением только одного человека, не ретушированным, в повседневной одежде. Лицам в очках следует оставаться в очках при фотографировании.

- **Расстояние между глазами**

Рекомендуется расстояние 200 пикселей или более, но не менее 115 пикселей.

- **Выражение лица**

Рекомендуется нейтральное лицо или улыбка с естественно открытыми глазами.

- **Поза и угол**

Угол горизонтального поворота не должен превышать $\pm 10^\circ$, угол подъема — $\pm 10^\circ$, угол наклона вниз — $\pm 10^\circ$.

● Аксессуары

Маски или цветные очки не допускаются. Оправа очков не должна закрывать глаза и не должна отражать свет. Для лиц с толстой оправой очков рекомендуется сделать два снимка: один в очках, другой без них.

● Лицо

Полное лицо с четким контуром, реальным масштабом, равномерно распределенным светом и без теней.

● Формат изображения

Должен быть в формате BMP, JPG или JPEG.

● Требования к данным

Должны соответствовать следующим требованиям:

- 1) Белый фон, одежда темного цвета.
- 2) 24-битный режим True Color.
- 3) Сжатое изображение в формате JPG размером не более 20 КБ.
- 4) Разрешение должно быть в диапазоне от 358 x 441 до 1080 x 1920 пикселей.
- 5) Вертикальное соотношение головы и тела должно быть 2:1.
- 6) На фото должны быть видны плечи снятого человека на одном горизонтальном уровне.
- 7) Глаза снятого человека должны быть открыты, радужная оболочка четко видна.
- 8) Предпочтительно нейтральное выражение лица или улыбка, показ зубов нежелателен.
- 9) Снятый человек должен быть хорошо виден, цвета естественные, на лице или фоне не должно быть резких теней, бликов или отражений. Контрастность и уровень яркости должны быть подходящими.

