

Руководство пользователя SenseFace 4 Series

Дата: Март 2024

Версия документа: 1.0

Русский

Спасибо, что выбрали наш продукт! Перед использованием продукта внимательно ознакомьтесь с инструкциями и неукоснительно следуйте им для обеспечения корректной работы продукта. Изображения, представленные в этом руководстве, предназначены только для иллюстративных целей.



Более подробную информацию Вы можете найти на нашем сайте www.zkteco.com.

СОДЕРЖАНИЕ

КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	8
МЕРЫ БЕЗОПАСНОСТИ.....	8
1. ИНСТРУКЦИИ ПО ПОЛЬЗОВАНИЮ.....	10
1.1 РАСПОЛОЖЕНИЕ ПАЛЬЦА НА СКАНЕРЕ.....	10
1.2 ПОЛОЖЕНИЕ СТОЯ, СТОЙКА И ВЫРАЖЕНИЕ ЛИЦА.....	10
1.3 РЕГИСТРАЦИЯ ШАБЛОНА ЛИЦА.....	11
1.4 ИНТЕРФЕЙС РЕЖИМА ОЖИДАНИЯ.....	12
1.5 ВИРТУАЛЬНАЯ КЛАВИАТУРА.....	14
1.6 РЕЖИМ ВЕРИФИКАЦИИ.....	15
1.6.1 ВЕРИФИКАЦИЯ ПО ОТПЕЧАТКУ ПАЛЬЦА ★	15
1.6.2 ВЕРИФИКАЦИЯ ПО QR-КОДУ ★	17
1.6.3 ВЕРИФИКАЦИЯ ПО КАРТЕ.....	18
1.6.4 ВЕРИФИКАЦИЯ ПО ЛИЦУ.....	20
1.6.5 ВЕРИФИКАЦИЯ ПО ПАРОЛЮ.....	22
1.6.6 КОМБИНИРОВАННАЯ ВЕРИФИКАЦИЯ.....	24
2. ГЛАВНОЕ МЕНЮ.....	25
3. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ.....	27
3.1 РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ.....	27
3.1.1 ID И ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ.....	27
3.1.2 РОЛЬ ПОЛЬЗОВАТЕЛЯ.....	28
3.1.3 ОТПЕЧАТОК ПАЛЬЦА ★	28
3.1.4 ШАБЛОН ЛИЦА.....	29
3.1.5 КАРТА.....	30
3.1.6 ПАРОЛЬ.....	31
3.1.7 ФОТО ПРОФИЛЯ.....	32
3.1.8 ПРАВА УПРАВЛЕНИЯ ДОСТУПОМ.....	32
3.2 ПОИСК ПОЛЬЗОВАТЕЛЕЙ.....	33
3.3 РЕДАКТИРОВАНИЕ ДАННЫХ ПОЛЬЗОВАТЕЛЯ	34
3.4 УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЕЙ	34
3.5 СТИЛЬ ОТОБРАЖЕНИЯ.....	35
4. РОЛЬ ПОЛЬЗОВАТЕЛЯ.....	37
5. НАСТРОЙКИ СВЯЗИ.....	39
5.1 СЕТЕВЫЕ НАСТРОЙКИ.....	39
5.2 ПОСЛЕДОВАТЕЛЬНАЯ СВЯЗЬ.....	40
5.3 ПОДКЛЮЧЕНИЕ К ПК.....	41
5.4 БЕСПРОВОДНАЯ СЕТЬ ★	42
5.5 НАСТРОЙКИ ОБЛАЧНОГО СЕРВЕРА.....	45
5.6 НАСТРОЙКИ WIEGAND.....	45
5.6.1 ВХОД WIEGAND.....	46
5.6.2 ВЫХОД WIEGAND.....	48

5.7	ДИАГНОСТИКА СЕТИ.....	49
6.	СИСТЕМНЫЕ НАСТРОЙКИ.....	50
6.1	ДАТА И ВРЕМЯ.....	50
6.2	НАСТРОЙКИ ЖУРНАЛОВ ДОСТУПА.....	52
6.3	ПАРАМЕТРЫ ШАБЛОНА ЛИЦА.....	53
6.4	ПАРАМЕТРЫ ОТПЕЧАТКА ПАЛЬЦА ★	55
6.5	НАСТРОЙКИ ТИПА УСТРОЙСТВА.....	56
6.6	НАСТРОЙКИ БЕЗОПАСНОСТИ.....	57
6.7	ОБНОВЛЕНИЕ ЧЕРЕЗ USB.....	58
6.8	ОБНОВЛЕНИЕ ПРОШИВКИ ОНЛАЙН.....	58
6.9	СБРОС ДО ЗАВОДСКИХ НАСТРОЕК.....	59
7.	НАСТРОЙКИ ПЕРСОНАЛИЗАЦИИ.....	60
7.1	НАСТРОЙКИ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА.....	60
7.2	ГОЛОСОВЫЕ НАСТРОЙКИ	61
7.3	РАСПИСАНИЯ ЗВОНКОВ.....	62
7.4	НАСТРОЙКИ СОБЫТИЙ РАБОЧЕГО ВРЕМЕНИ	63
7.5	МЕНЮ КНОПОК БЫСТРОГО ДОСТУПА.....	64
8.	УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ	67
8.1	УДАЛЕНИЕ ДАННЫХ.....	67
9.	ИНТЕРКОМ.....	69
9.1	НАСТРОЙКИ SIP.....	69
9.1.1	ПОДКЛЮЧЕНИЕ К SIP-СЕРВЕРУ.....	71
9.1.2	ИСПОЛЬЗОВАНИЕ ЛОКАЛЬНОЙ СЕТИ.....	73
9.1.3	НАСТРОЙКА ГОРЯЧИХ КЛАВИШ ВЫЗОВА.....	75
9.1.4	РЕЖИМ ПРЯМОГО ДОЗВОНА.....	76
9.2	НАСТРОЙКИ ДВЕРНОГО ЗВОНКА	77
9.2.1	ПОДКЛЮЧЕНИЕ ДВЕРНОГО ЗВОНКА ★	78
9.3	НАСТРОЙКИ ONVIF	79
10.	УПРАВЛЕНИЕ ДОСТУПОМ.....	82
10.1	НАСТРОЙКИ КОНТРОЛЯ ДОСТУПА.....	83
10.2	НАСТРОЙКИ ПРАВИЛА ВРЕМЕНИ	84
10.3	ВЫХОДНЫЕ (ПРАЗДНИЧНЫЕ)ДНИ.....	86
10.4	ГРУППЫ ДОСТУПА ★	87
10.5	КОМБИНИРОВАННАЯ ВЕРИФИКАЦИЯ	88
10.6	НАСТРОЙКА ЗАПРЕТА ДВОЙНОГО ПРОХОДА.....	89
10.7	ТРЕВОГА ПОД ПРИНУЖДЕНИЕМ.....	90
11.	USB-МЕНЕДЖЕР.....	92
11.1	ВЫГРУЗКА ДАННЫХ НА USB	92
11.2	ЗАГРУЗКА ДАННЫХ НА USB	93
12.	ПОИСК СОБЫТИЙ РАБОЧЕГО ВРЕМЕНИ.....	94
13.	АВТОДИАГНОСТИКА	96

14. ИНФОРМАЦИЯ О СИСТЕМЕ.....	97
15. ПОДКЛЮЧЕНИЕ К ПО ЗКВЮ CVACCESS	98
15.1 УСТАНОВКА АДРЕСА СВЯЗИ.....	98
15.2 ДОБАВЛЕНИЕ УСТРОЙСТВА НА ПО	99
15.3 ДОБАВЛЕНИЕ СОТРУДНИКОВ НА ПО	100
15.4 МОБИЛЬНЫЕ УЧЕТНЫЕ ДАННЫЕ ★	101
16. ПОДКЛЮЧЕНИЕ К ПО ЗКВЮ TIME	104
16.1 УСТАНОВКА АДРЕСА СВЯЗИ	104
16.2 ДОБАВЛЕНИЕ УСТРОЙСТВА НА ПО	104
16.3 ДОБАВЛЕНИЕ СОТРУДНИКОВ НА ПО.....	105

Конфиденциальность персональных данных

Для улучшения качества предоставляемых вам товаров и услуг компания ZKTeco как поставщик интеллектуальных продуктов может осуществлять сбор определенных персональных данных; при этом ZKTeco обязуется заботиться о сохранении конфиденциальности собираемых данных путем разработки Политики конфиденциальности..

Перед использованием продуктов ZKTeco прочтите Политику конфиденциальности, уясните ее содержание, а также обращайте внимание на важные уведомления, появляющиеся на экране устройства.

Как пользователь продукта, вы должны соблюдать нормативные акты, касающиеся защиты персональных данных, при их сборе, хранении и использовании, в том числе принимать меры по защите персональных данных, таких как разумное предоставление пользователям прав управления на устройствах, усиление физической безопасности сценариев применения устройств и т. д.

Меры безопасности

Приведенные ниже меры безопасности направлены на обеспечение безопасности пользователя и предотвращения причинения ему вреда. Внимательно ознакомьтесь с ними перед установкой продукта.

1. **Прочтите, следуйте и сохраните инструкции:** перед вводом устройства в эксплуатацию прочтите все инструкции по безопасности и эксплуатации и неукоснительно следуйте им.
2. **Не игнорируйте предупреждения:** внимательно относитесь ко всем предупреждениям, выдаваемым устройством, и содержащимся в настоящем руководстве.
3. **Вспомогательное оборудование:** применяйте только те приспособления и аксессуары, которые рекомендованы производителем или идут в комплекте с продуктом.
4. **Меры безопасности при установке:** не ставьте это устройство на неустойчивую поверхность: оно может упасть и причинить увечье или выйти из строя.
5. **Обслуживание:** не обслуживайте это устройство самостоятельно. Самостоятельное снятие крышек сопряжено с различными рисками, в том числе поражением электрическим током.
6. **Повреждения, требующие обслуживания (ремонта):** в случаях, описанных ниже, необходимо отключить устройство от источника питания переменного или постоянного тока и вызвать квалифицированного специалиста:

- повреждение шнура или соединения;
- попадание жидкости или инородных тел в систему;
- воздействие на устройство воды или непогоды (дождя, снега и пр.);
- устройство не работает нормально при соблюдении инструкций по эксплуатации.

Выполните настройки органов управления, как указано в эксплуатационных инструкциях. Неправильная настройка органов управления может привести к отказам и необходимости вызова квалифицированного мастера для восстановления работы устройства.

7. **Запасные части:** при необходимости замены деталей сервисные специалисты должны использовать только запасные части от поставщика. Применение иных запасных частей может привести к перегоранию, удару током или повлечь иные неблагоприятные последствия.
8. **Проверка безопасности:** после окончания обслуживания или ремонта устройства попросите специалиста выполнить проверку безопасности, чтобы убедиться в нормальной работе устройства.

9. **Источники питания:** подключайте систему только к источникам питания, указанным на маркировке. Если не ясно, какой источник питания следует использовать, свяжитесь с вашим продавцом.
10. **Молния:** можно установить внешние грозовые разрядники для защиты от электрических штормов. Это позволит защитить систему от перенапряжений, вызванных ударами молний.

Рекомендуется устанавливать устройства в местах с ограниченным доступом.

1. Указания по использованию

Перед рассмотрением характеристик и функций устройства рекомендуется ознакомиться с его основным функционалом, приведенным ниже.

1.1 Расположение пальца на сканере

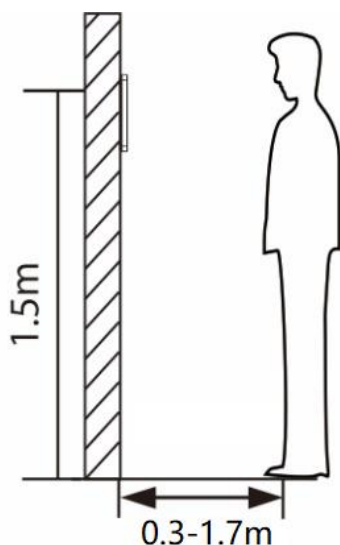
Рекомендуется использовать для сканирования указательный, средний или безымянный палец и избегать использования большого пальца или мизинца, так как последние трудно точно приложить к считывателю.



Примечание: Правильно прикладывайте палец к сканеру во время процедур регистрации отпечатка пальца и верификации. Наша компания не будет нести ответственность за какие-либо проблемы распознавания по причине неправильного использования продукта. Мы оставляем за собой право на окончательное толкование и изменение этого пункта.

1.2 Стойка, осанка и выражение лица

● Рекомендуемое расстояние



Рекомендуемое расстояние между устройством и пользователем, рост которого от 1,55 до 1,85 м, составляет от 0,3 до 1,7 м. Допускается небольшой наклон тела вперед или назад, чтобы улучшить снимок лица.

● Рекомендуемые положение тела и выражение лица:



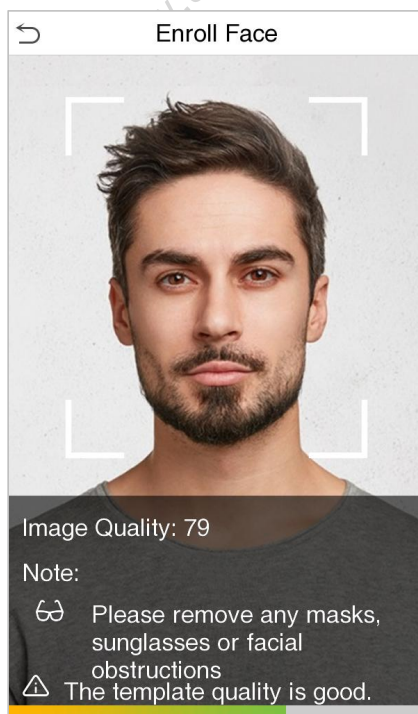
Стойка

Выражение лица

Примечание: Постарайтесь сохранять естественность выражения лица и положения тела во время прохождения процедур регистрации и верификации.

1.3 Регистрация шаблона лица

Убедитесь, что изображение вашего лица находится в центре экрана во время регистрации шаблона лица. Смотрите на камеру и старайтесь не шевелиться во время регистрации. Изображение на экране должен выглядеть следующим образом:



Правильный способ регистрации и верификации шаблона лица

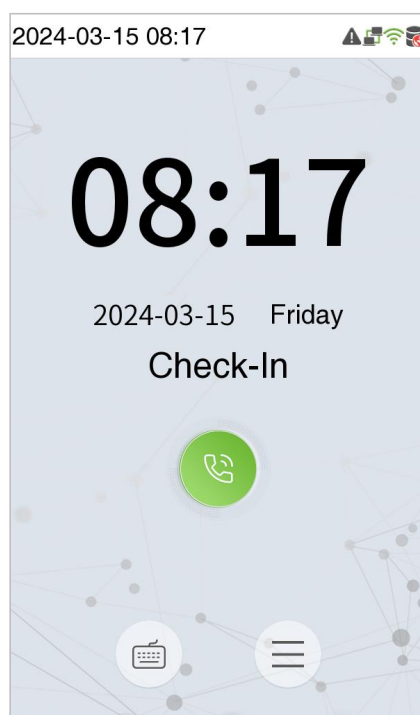
● Рекомендации по регистрации шаблона лица

- При регистрации шаблона лица поддерживайте расстояние между устройством и вашим лицом от 50 до 80 см.

- Следите за тем, чтобы выражение лица было естественным и не менялось (улыбка, гримаса, подмигивание и пр.)
 - Невыполнение указаний на экране может привести к увеличению времени регистрации шаблона лица или отказу в ней.
 - Не прикрывайте глаза или брови.
 - Снимите шапку, маску или очки.
 - Следите за тем, чтобы на экране не отображалось два лица. Регистрируйтесь по очереди.
 - Если вы пользуетесь очками, рекомендуется зарегистрировать шаблон лица в очках и без них.
- **Рекомендации по верификации по шаблону лица**
 - Убедитесь, что изображение лица не выходит за границы рамки на экране устройства.
 - Иногда случается сбой в аутентификации лица по причине того, что пользователь надел не те очки, в которых он был во время регистрации. В этом случае Вам может потребоваться использовать очки, в которых Вы были ранее, для аутентификации. Если Вы регистрировались без очков, то в дальнейшем при аутентификации лица Вы должны быть без очков.
 - Если часть лица закрыта головным убором, маской, повязкой на глазу или солнечными очками, может произойти сбой верификации. Не закрывайте лицо, устройство должно "видеть" и брови, и глаза.

1.4 Интерфейс режима ожидания

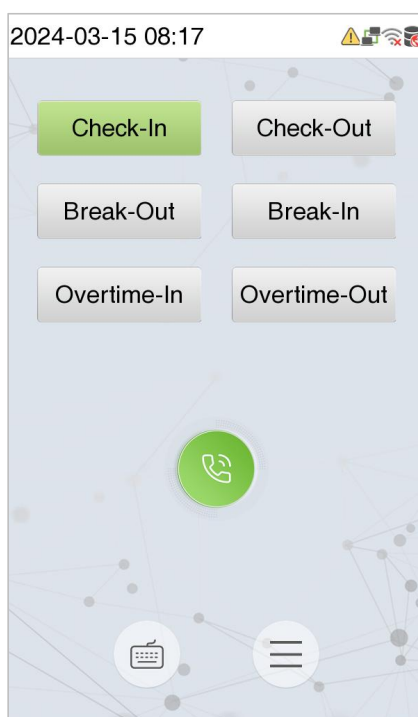
После включения устройство перейдет в режим ожидания, как показано на рисунке ниже:



- Нажмите  для входа в меню ввода ID пользователя.
- Если на устройстве отсутствует учетная запись супер администратора, нажмите  для входа в меню.
- После добавления учетной записи супер администратора для доступа к функциям меню потребуется верификация супер администратора.

Примечание: в целях безопасности рекомендуется зарегистрировать учетную запись супер администратора при первом использовании устройства.

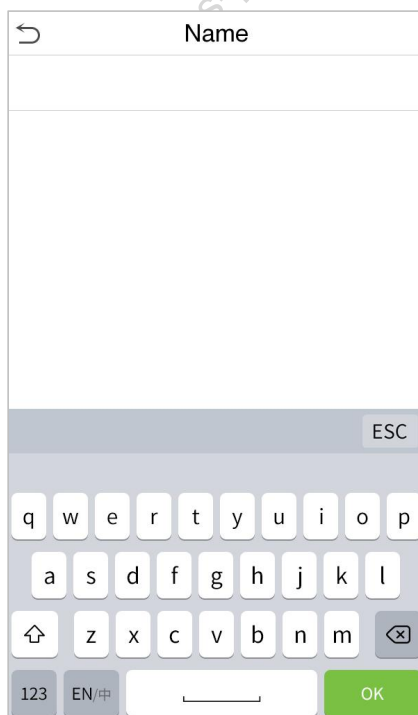
- В интерфейсе ожидания можно также вывести на экран меню функциональных клавиш событий учета рабочего времени (далее – функциональные клавиши). Для этого кликните на любое свободное место на экране, после чего на нем отобразятся шесть клавиш быстрого доступа, как показано на рисунке ниже:



- Нажмите функциональную клавишу для выбора соответствующего ей события (будет подсвечено зеленым).

Примечание: меню функциональных клавиш отключено по умолчанию. Для их отображения на экране в интерфейсе ожидания смотрите [раздел 7.5 "Настройка меню клавиш быстрого доступа"](#).

1.5 Виртуальная клавиатура



Примечание:

Устройство поддерживает ввод текста на китайском и английском языках, а также цифр и символов.

- Нажмите **EN** для переключения на английскую языковую раскладку.
- Нажмите **123** для переключения на раскладку с цифрами и символами.
- Нажмите **ABC** для возврата в буквенную раскладку.
- Нажмите на поле ввода для отображения на экране виртуальной клавиатуры.
- Нажмите **ESC** для выхода из режима виртуальной клавиатуры.

1.6 Способ верификации

1.6.1 Верификация по отпечатку пальца★

Примечание: эта функция реализована только в устройствах SenseFace 7A.

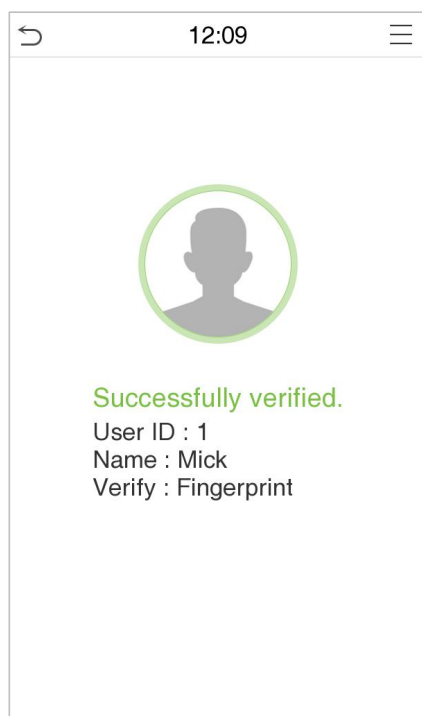
- **Верификация по отпечатку пальца в режиме 1:N**

Устройство сравнивает отсканированный отпечаток пальца с отпечатками пальцев, имеющимися в базе данных устройства.

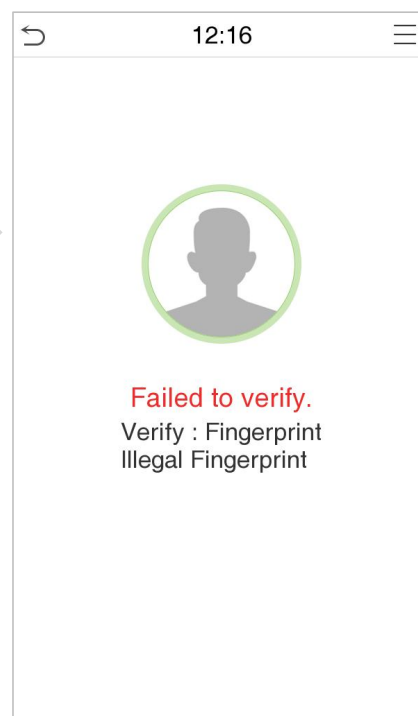
Режим верификации по отпечатку пальца активируется, когда пользователь прикладывает свой палец к сканеру.

Следуйте рекомендациям по размещению пальца на сканере (см. раздел "[Расположение пальца на сканере](#)").

Верификация успешна:



В верификации отказано:



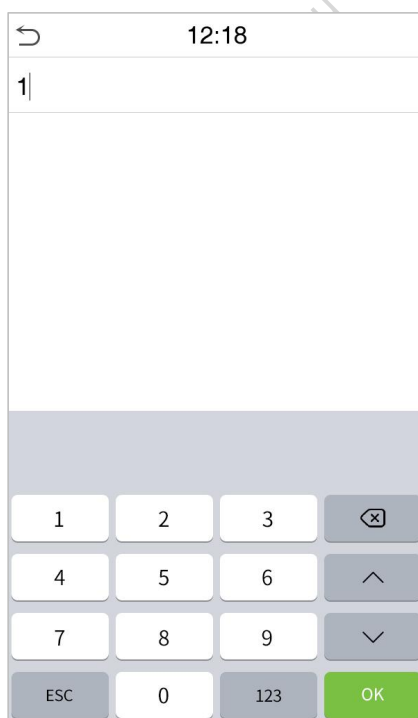
- **Верификация по отпечатку пальца в режиме 1:1**

Устройство сравнивает отсканированный отпечаток пальца с отпечатками пальцев, «привязанными» к введенному идентификатору пользователя.

Если не получается получить доступ к системе по отпечатку пальца в режиме 1:1, можно попробовать пройти верификацию в режиме 1:N.

Нажмите  в главном меню для перехода к верификации по отпечатку пальца в режиме 1:1.

Введите идентификатор пользователя и нажмите **ОК**.

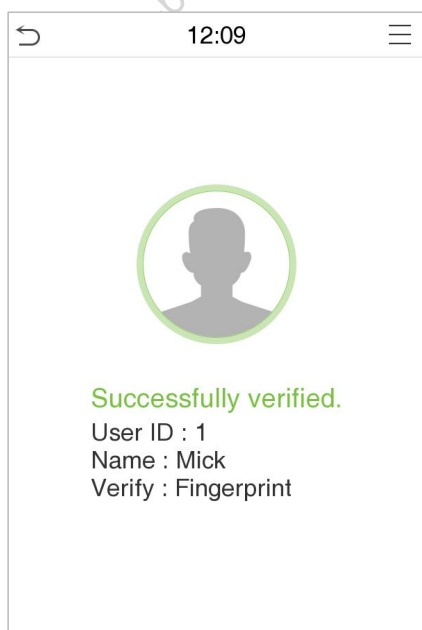


Если в качестве способа верификации пользователь зарегистрировал, помимо отпечатка пальца, шаблон лица и пароль, появится следующее окно. Нажмите  для перехода в режим верификации по отпечатку пальца.

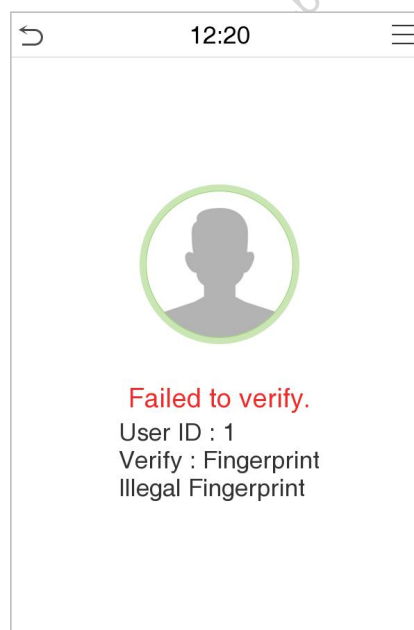


Приложите палец к сканеру для верификации.

Верификация успешна:



В верификации отказано:



1.6.2 Верификация по QR-коду ★

Примечание: эта функция реализована только в устройствах модели SenseFace 7C.

В этом режиме устройство сравнивает считанный ридером QR-код со всеми имеющимися в памяти устройства QR-кодами.

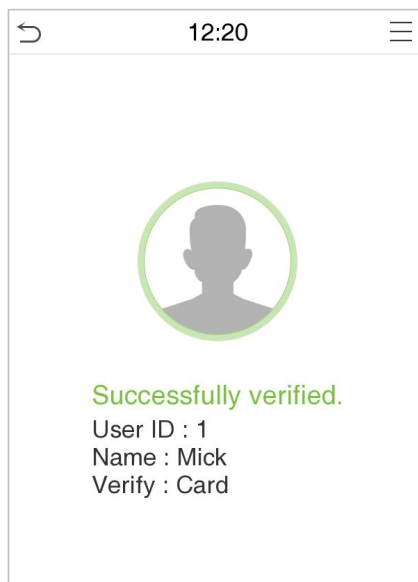
Нажмите **Mobile Credential (Мобильные учетные данные)** на странице ZKBioAccess для отображения QR-кода с «защитами» в нем идентификатором сотрудника и номером карты (статический QR-код содержит только номер карты). QR-код может заменить физическую карту для бесконтактной аутентификации. См. раздел [15.4 "Мобильные учетные данные"](#).



1.6.3 Верификация по карте

- **Верификация по карте в режиме 1:N**

В данном режиме устройство сравнивает считанный номер карты с номерами всех карт в памяти устройства. Ниже изображен интерфейс верификации по карте:

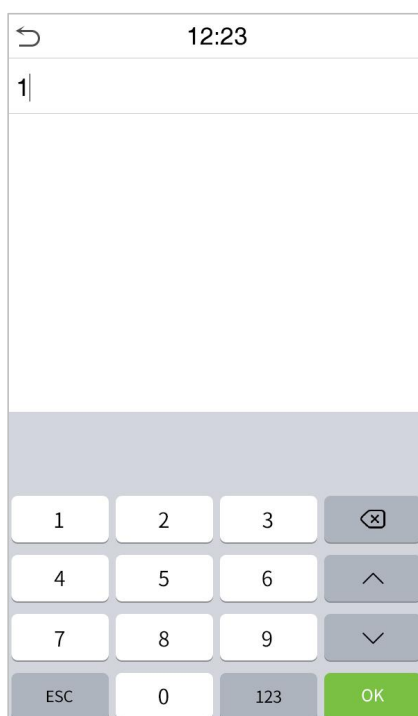


- **Верификация по карте в режиме 1:1**

В данном режиме устройство сравнивает считанный номер карты с номером карты, «привязанным» к идентификатору зарегистрированного на устройстве пользователя.

Нажмите  в главном меню для переключения в режим верификации по карте 1:1.

Введите ID пользователя и нажмите **OK**.

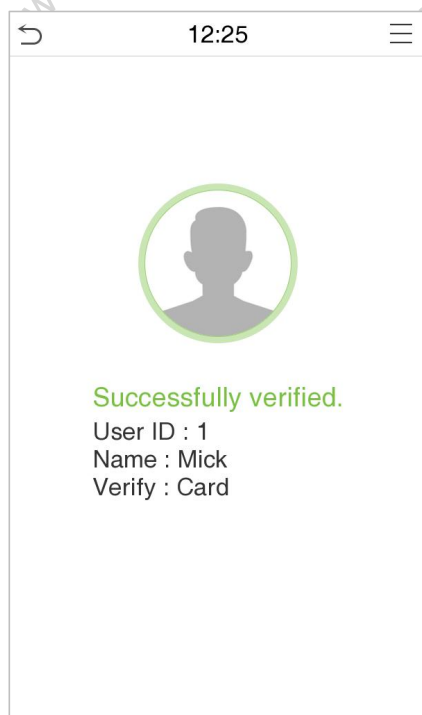


Если в качестве способа верификации пользователь зарегистрировал, помимо карты, шаблон лица и пароль, появится следующее окно. Выберите  для перехода в режим верификации по карте.

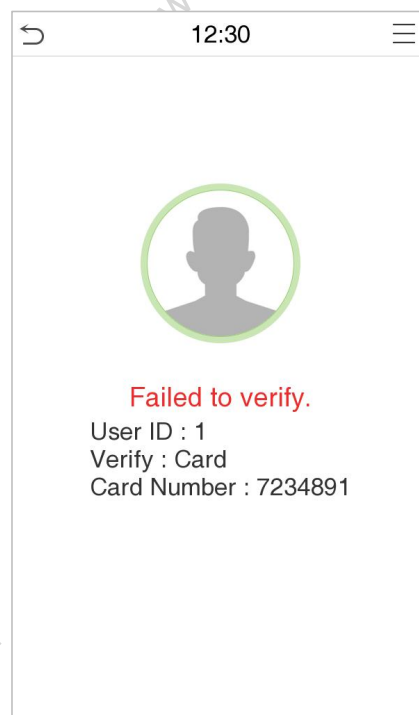


Приложите карту к зоне считывания для верификации .

Верификация успешна:



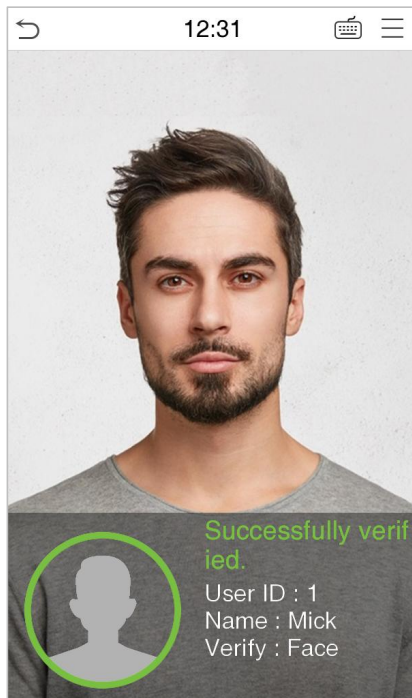
В верификации отказано:



1.6.4 Верификация по лицу

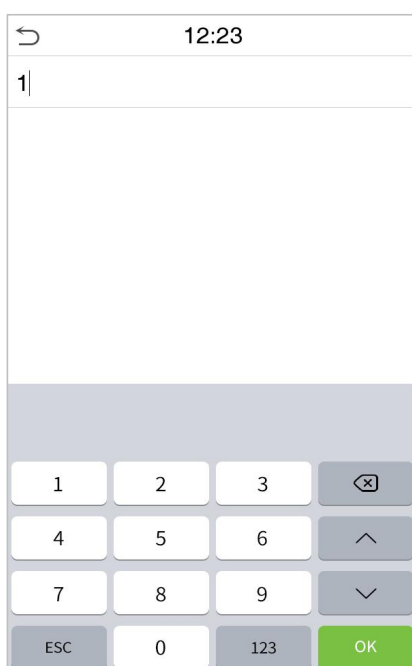
● Верификация по лицу в режиме 1:N

В данном режиме устройство сравнивает только что полученный снимок лица со всеми шаблонами лиц из базы данных устройства. Ниже всплывающее окно результата сравнения.



● Верификация по лицу в режиме 1:1

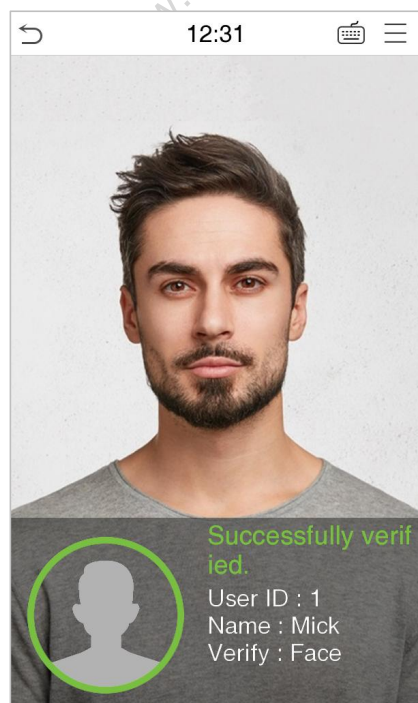
В этом режиме устройство сравнивает только что сделанный снимок лица с шаблоном лица, «привязанным» к ID пользователя. В главном меню нажмите  для перехода в режим распознавания по лицу 1:1, введите ID пользователя и нажмите [OK].



Если в качестве способа верификации пользователь зарегистрировал, помимо шаблона лица, карту, отпечаток пальца и пароль, появится следующее окно. Выберите  для перехода в режим верификации по лицу.



В случае успешной верификации на экране появится уведомление **"Successfully Verified" (Успешная верификация)**, как показано на рисунке ниже:

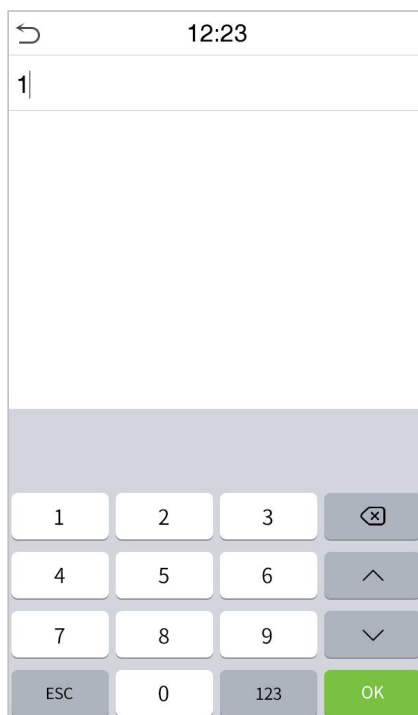


Если лицо не распознано, появится сообщение **"Please adjust your position!" (Измените свое положение)**.

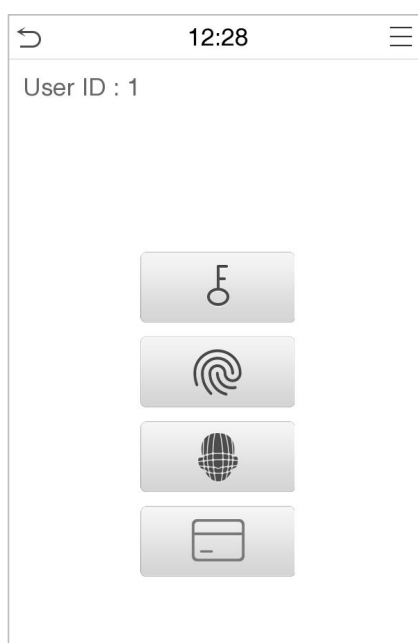
1.6.5 Верификация по паролю

Устройство сравнивает введенный пароль с паролем, который был зарегистрирован как идентификатор пользователя.

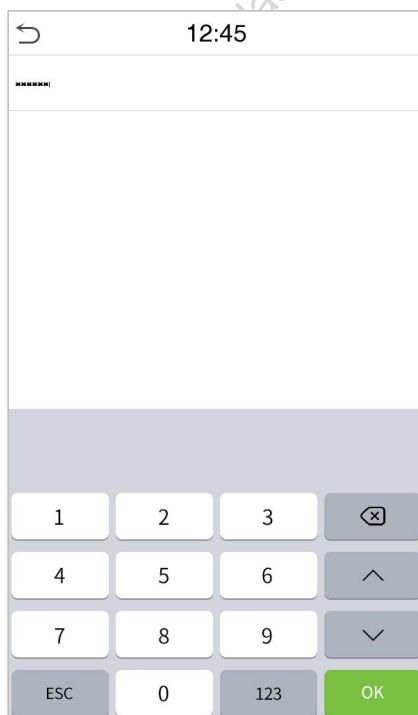
Нажмите  в главном меню для перехода в режим верификации по паролю 1:1. Затем введите ID пользователя и нажмите **ОК**.



Если в качестве способа верификации пользователь зарегистрировал, помимо пароля, шаблон лица и карту, появится следующее окно. Выберите  для перехода в режим верификации по паролю.

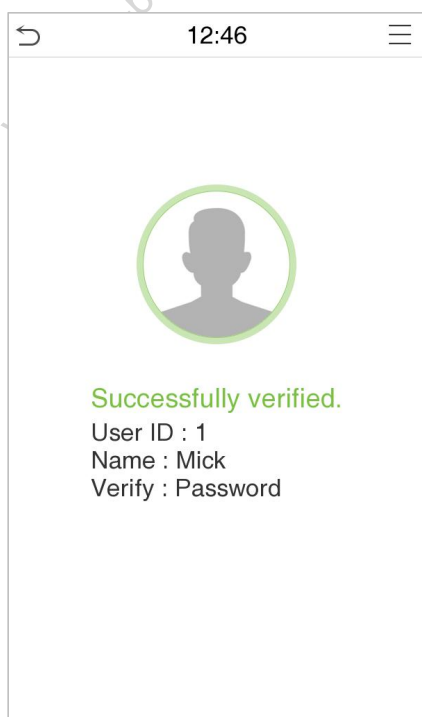


Введите пароль и нажмите **OK**.

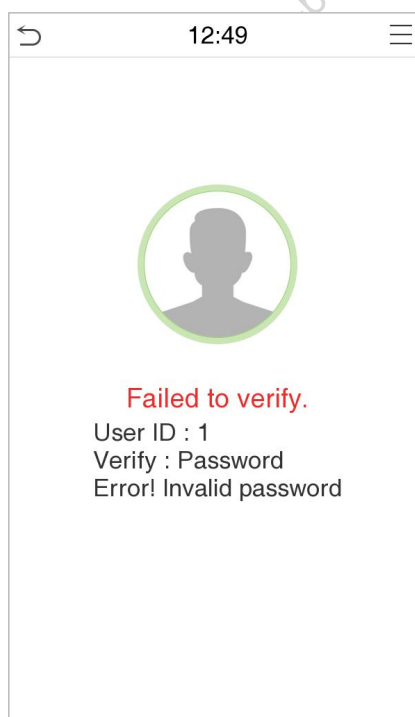


При вводе действительного и недействительного паролей откроются окна, как показано на рисунке ниже.

Верификация успешна:



В верификации отказано:



1.6.6 Комбинированная верификация

В целях повышения безопасности в данном устройстве реализована возможность применения различных комбинаций способов верификации (всего 21 комбинаций), как показано ниже:

Символы, применяемые при комбинированной верификации:

Символ	Значение	Описание
/	или	Сравнение предоставленных пользователем верификационных данных с ранее зарегистрированным на устройстве соответствующим шаблоном верификации данного пользователя.
+	и	Сравниваются представленные пользователем верификационные данные со всеми шаблонами верификации, которые ранее были привязаны к ID этого пользователя на устройстве.

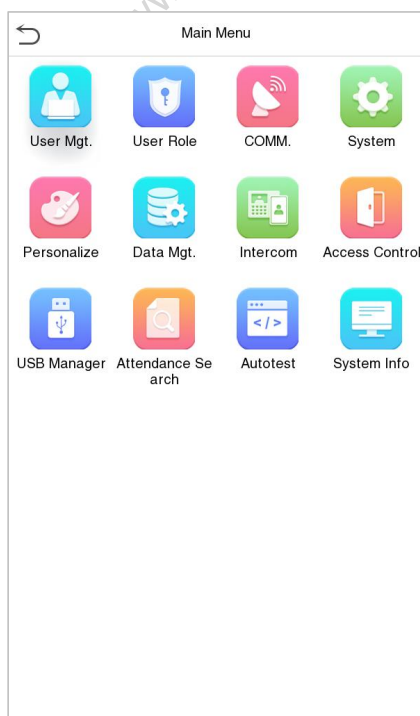
Verification Mode	Verification Mode	Verification Mode
☒ Password/Fingerprint/Card/Face	☐ Fingerprint+Password+Card	☐ Password+Card
☐ Fingerprint Only	☐ Password+Card	☐ Password/Card
☐ User ID Only	☐ Password/Card	☐ User ID+Fingerprint+Password
☐ Password	☐ User ID+Fingerprint+Password	☐ Fingerprint+(Card/User ID)
☐ Card Only	☐ Fingerprint+(Card/User ID)	☐ Face Only
☐ Fingerprint/Password	☐ Face Only	☐ Face+Fingerprint
☐ Fingerprint/Card	☐ Face+Fingerprint	☐ Face+Password
☐ User ID+Fingerprint	☐ Face+Password	☐ Face+Card
☐ Fingerprint+Password	☐ Face+Card	☐ Face+Fingerprint+Card
☐ Fingerprint+Card	☐ Face+Fingerprint+Card	☐ Face+Fingerprint+Password

Процедура установки режима комбинированной верификации:

- Установленный на устройстве режим комбинированной верификации предполагает регистрацию всех входящих в него способов верификации для получения пользователем доступа.
- Например, если пользователь в качестве способа верификации зарегистрировал только шаблон лица, а на устройстве установлен комбинированный режим верификации “Лицо + Пароль”, пользователь не сможет пройти процедуру верификации полностью.
- Верификация не будет завершена, так как устройство будет сравнивать снимок лица пользователя с зарегистрированным шаблоном верификации (состоящим из шаблона лица и пароля), привязанным к ID пользователя на устройстве.
- Но поскольку пользователь зарегистрировал только шаблон лица, без пароля, верификация не будет завершена и на экране появится сообщение “Verification Failed” (Верификация не выполнена).

2. Главное меню

Нажмите  на странице ожидания для входа в главное меню, экран приобретет вид ниже.

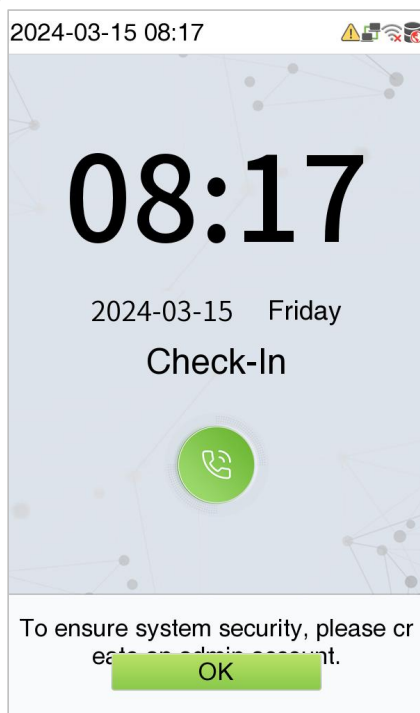


Описание функций

Меню	Описание
Управление пользователями	Добавление, редактирование, просмотр и удаление основной информации пользователя.
Роль пользователя	Установка роли пользователя, т.е. объема его прав пользования системой.
Связь	Установка параметров сети, последовательного интерфейса, связи с ПК, беспроводной сети, облачного сервера, Wiegand и диагностики сети.
Система	Настройка сетевых параметров, в том числе даты и времени, журнала доступа, шаблона лица и отпечатка пальца★, типа устройства, безопасности, обновления прошивки и USB, а также сброса к заводским параметрам.
Персонализация	Персонализированные настройки голосовой связи, расписания звонков, функциональных клавиш и клавиш быстрого доступа.
Управление данными	Удаление всех выбранных данных на устройстве.
Внутренняя связь	Установка параметров SIP и NVR.
Контроль доступа	Установка параметров замка и контроллера доступа, в т.ч. правила времени, выходных и праздничных дней, комбинированной верификации и тайного сигнала тревоги.
Менеджер USB портов	Выгрузка/загрузка данных на/с USB-устройства.

Поиск событий учета рабочего времени	Запрос записей журналов событий, проверка фото посещений и фото из списка блокировок.
Автоматическое тестирование	Автодиагностика работы модулей, в том числе ЖК-экрана, аудиоканала, микрофона, камеры, датчика отпечатков пальцев★ и часов реального времени.
Информация о системе	Просмотр объема памяти, информации об устройстве и его прошивке, а также политики конфиденциальности.

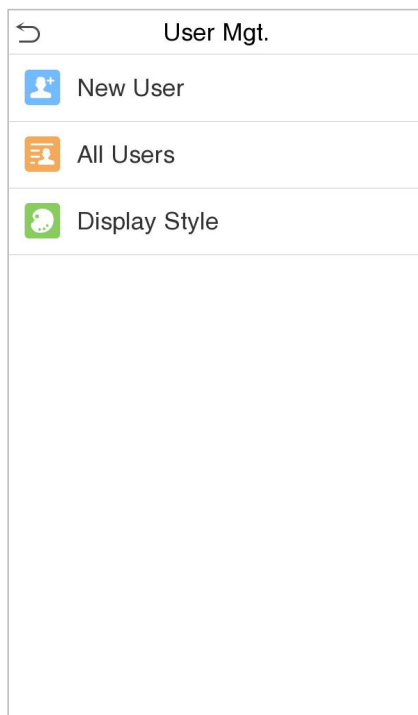
Примечание: При первом использовании продукта следует установить учетную запись администратора перед использованием устройства. Нажмите User Mgt. (Управление пользователями) для добавления учетной записи администратора или редактирования прав пользователей. Если на устройстве отсутствует учетная запись администратора, то каждый раз при входе в меню будет всплывать сообщение безопасности о необходимости создания учетной записи администратора.



3. Управление пользователями

3.1 Регистрация пользователя

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



3.1.1 Идентификатор и имя пользователя

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

New User	
User ID	1
Name	Mick
User Role	Normal User
Fingerprint	0
Face	0
Card	0
Password	
Profile Photo	0
Access Control Role	

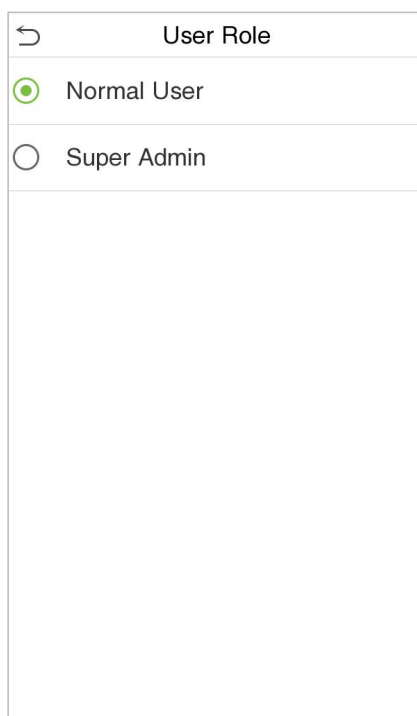
Примечание:

- Имя пользователя может включать до 34 символов.
- ID пользователя может содержать от 1 до 14 символов по умолчанию.
- Вы можете изменить свой ID только во время первоначальной регистрации (после этого его нельзя будет изменить).
- При появлении сообщения **"Duplicated!"** необходимо выбрать другой пароль, так как введенный уже существует.

3.1.2 Роль пользователя

На странице **New User** нажмите **User Role (Роль пользователя)** для установки его роли как **Normal User (обычный пользователь)** или **Super Admin (супер администратор)**.

- **Super Admin:** супер администратор обладает самыми полными правами управления на устройстве.
- **Normal User:** если на устройстве уже есть учетная запись супер администратора, обычные пользователи не будут иметь доступ только к процедурам верификации.
- **User Defined Roles:** определенным пользователям без полномочий администратора могут назначаться персонализированные роли .

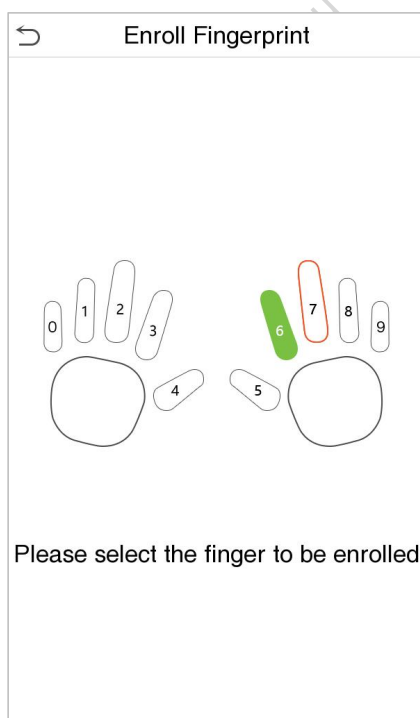


User Role	
☒	Normal User
☐	Super Admin

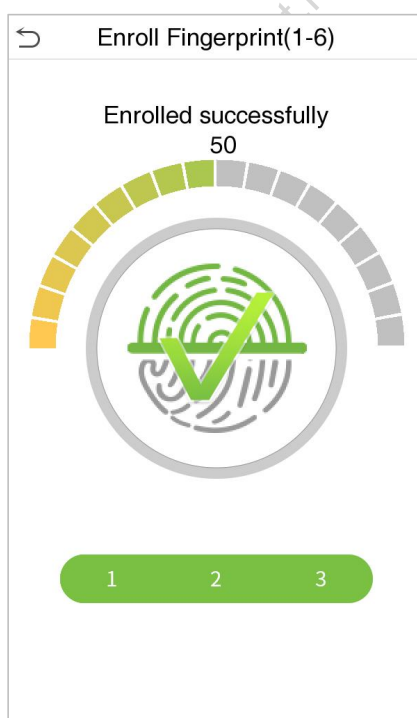
Примечание: Если за пользователем закреплена роль супер администратора, то для доступа к главному меню он должен пройти верификационную процедуру в зависимости от способа(ов) верификации, зарегистрированном(ых) супер администратором. См. раздел [1.6. "Способ верификации"](#).

3.1.3 Регистрация отпечатка пальца ★

Нажмите **Fingerprint (Отпечаток пальца)** для входа в меню регистрации отпечатка пальца. Выберите палец, по которому будет осуществляться верификация.



Приложите выбранный палец к сканеру три раза. Зеленая индикация означает, что отпечаток пальца был успешно зарегистрирован.

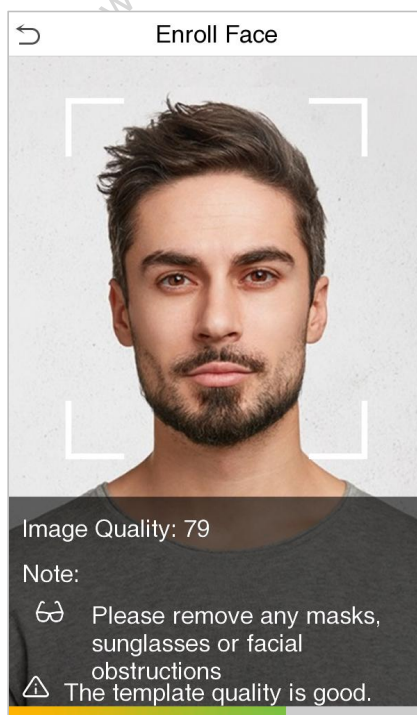


3.1.4 Регистрация шаблона лица

Нажмите **Face (Лицо)** в меню New User для перехода на страницу регистрации шаблона лица.

- Встаньте лицом к камере и убедитесь, что его изображение не выходит за пределы белой ограничительной рамки в течение всего процесса регистрации шаблона лица.

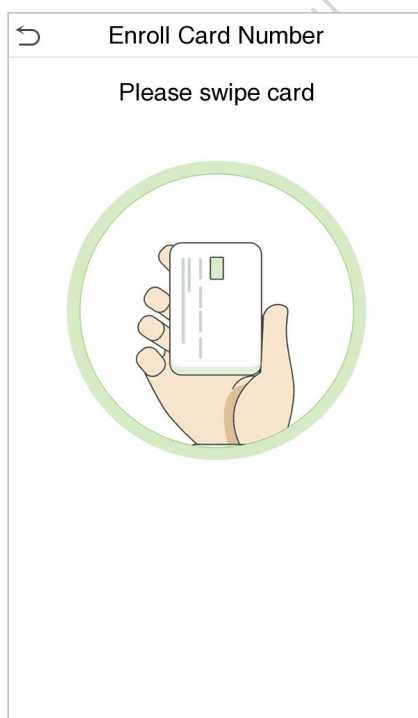
- Во время регистрации лица появится полоса загрузки, а затем сообщение **"Enrolled Successfully"** (Регистрация успешна) после окончания загрузки.
- Если такой шаблон лица уже был ранее зарегистрирован, на экране появится сообщение **"Duplicated Face"**. Вид страницы регистрации шаблона лица показан ниже:



3.1.5 Карта

Нажмите **Card (Карта)** в меню **New User** для перехода на страницу регистрации карты.

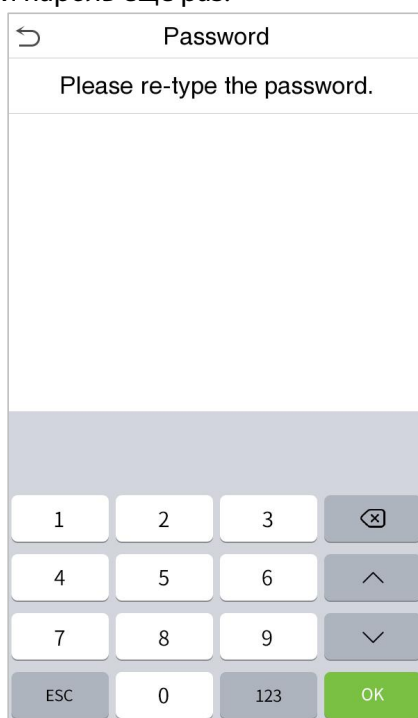
- В открывшемся окне проведите картой под область считывания. Регистрация карты успешна.
- Если такая карта ранее уже регистрировалась, появится сообщение **"Duplicate Card"**. Страница регистрации карты представлена ниже:



3.1.6 Пароль

Нажмите **Password (Пароль)** в меню **New User** для перехода на страницу регистрации пароля.

- На открывшейся странице введите пароль, затем введите его еще раз для подтверждения и нажмите **ОК**.
- Если повторно набранный пароль не совпадает с первоначально введенным, устройство выдаст сообщение "**Password does not match!**" (**Пароль не соответствует!**); пользователь должен подтвердить свой пароль еще раз.

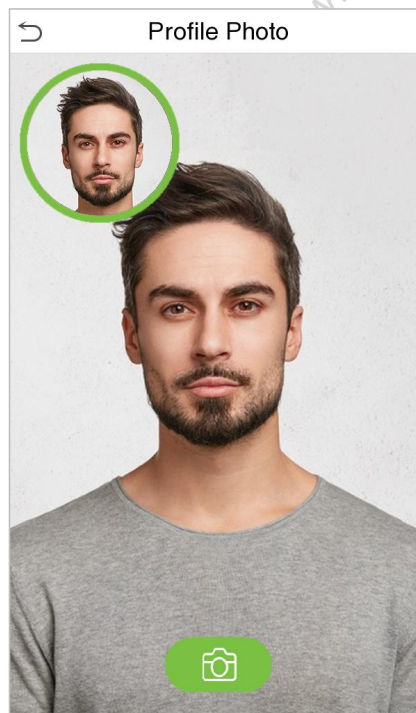


Примечание: Пароль может содержать от 6 до 8 знаков по умолчанию.

3.1.7 Фото профиля

Нажмите **Profile Photo (Фото профиля)** на странице **New User** для перехода в меню регистрации фото профиля.

New User	
User ID	1
Name	Mick
User Role	Normal User
Fingerprint	0
Face	0
Card	0
Password	
Profile Photo	0
Access Control Role	



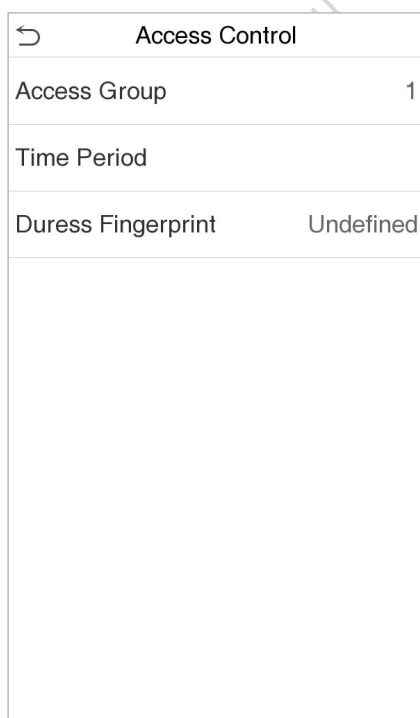
- Если пользователь зарегистрировал фото профиля, оно будет отображаться каждый раз при прохождении процедуры верификации в дальнейшем.
- Нажмите **Profile Photo (Фото профиля)**, откроется камера устройства, затем коснитесь значка камеры, чтобы сделать снимок. Снимок отобразится в левом верхнем углу экрана, а камера откроется снова, чтобы сделать новый снимок.

Примечание: При регистрации шаблона лица система автоматически будет использовать его в качестве фото профиля пользователя. Если вы не зарегистрируете фото профиля, им по умолчанию станет фото, сделанное при регистрации шаблона лица.

3.1.8 Права управления доступом

В меню прав управления доступом можно управлять правами доступа для каждого пользователя или группы пользователей, настраивать отпечаток пальца принуждения, а также устанавливать временные ограничения доступа для группы пользователей.

- Нажмите **Access Control Role (Права управления доступом)>Access Group (Групповой доступ)** для "приписки" зарегистрированных пользователей к различным группам доступа для более эффективного управления. Новые пользователи зачисляются в Группу 1 по умолчанию, но могут быть переведены в другие группы. Максимальное количество групп пользователей на устройстве 99.
- Нажмите **Time Period** для выбора периода времени.

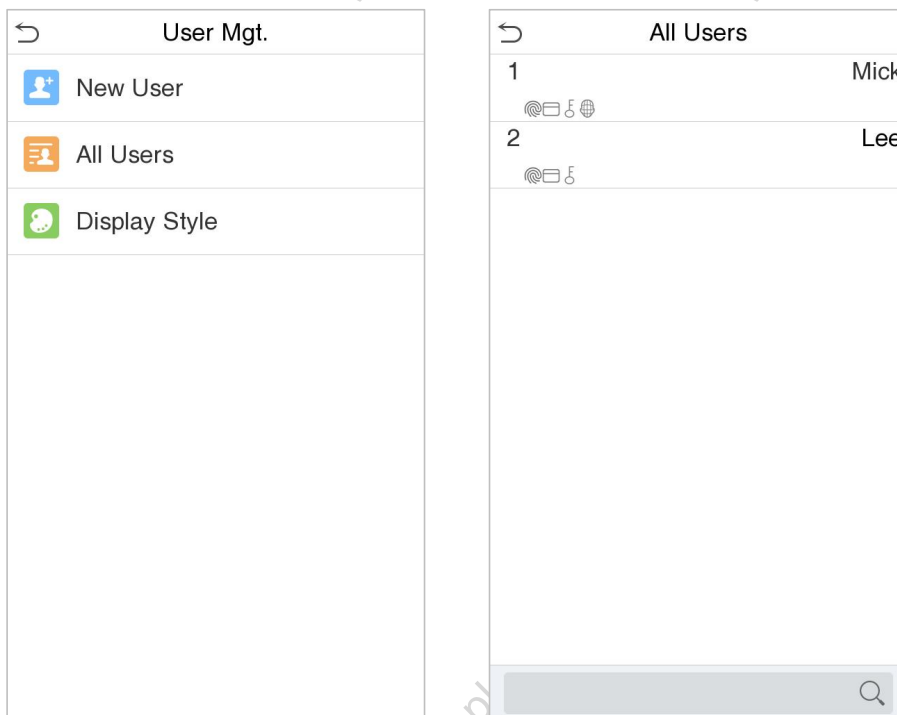


Access Control	
Access Group	1
Time Period	
Duress Fingerprint	Undefined

3.2 Поиск пользователей

В главном меню нажмите **User Mgt. (Управление пользователями)** и затем **All Users (Все пользователи)** для поиска пользователя.

- В меню **All Users** коснитесь строки поиска на перечне пользователей для ввода ключевого поискового слова (например, ID, фамилии или полного имени пользователя), и система начнет поиск пользователя с такими данными.



3.3 Редактирование данных пользователя

На странице **All Users (Все пользователи)** выберите нужного пользователя из списка и нажмите **Edit (Редактировать)** для редактирования его данных.

User : 1	
Edit	
Delete	

Edit : 1	
User ID	1
Name	Mick
User Role	Normal User
Fingerprint	1
Face	1
Card	1
Password	*****
Profile Photo	1
Access Control Role	

Примечание: Процесс редактирования информации о пользователе аналогичен добавлению нового пользователя с той лишь разницей, что при редактировании нельзя изменить ID пользователя. Более подробно в разделе [3 "Управление пользователями"](#).

3.4 Удаление пользователей

В меню **All Users (Все пользователи)** выберите нужного пользователя из списка и нажмите **Delete (Удаление)** для его удаления или каких-либо данных о нем с устройства. На странице Delete выберите действие, которое Вы хотите выполнить, и нажмите ОК для подтверждения удаления.

● **Варианты удаления:**

Delete User: удаление всей информации о пользователе (в том числе и самого пользователя) с устройства.

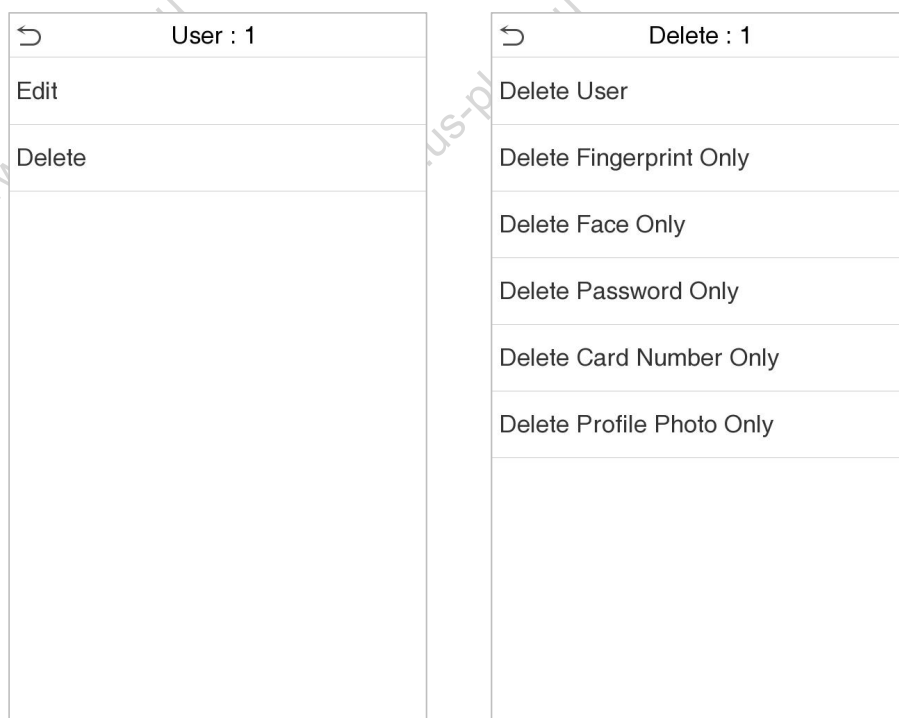
Delete Fingerprint Only: удаление зарегистрированного отпечатка пальца пользователя.

Delete Face Only: удаление шаблона лица пользователя.

Delete Password Only: удаление пароля пользователя.

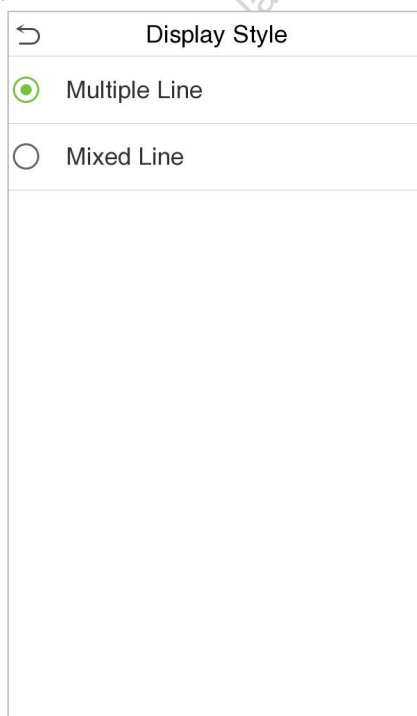
Delete Card Number Only: удаление карты пользователя.

Delete Profile Photo Only: удаление фото профиля пользователя.



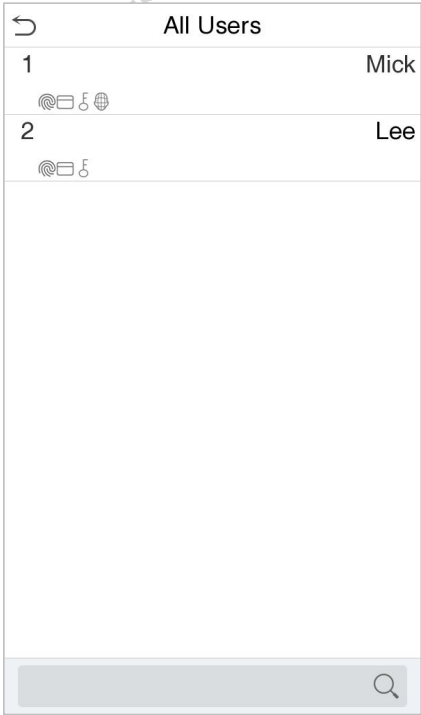
3.5 Стил ь отображения

Нажмите **User Mgt. > Display Style (Стил ь отображения)** для перехода в меню выбора стили я отображения страницы All Users.



Доступные стили отображения приведены ниже:

Многострочный:



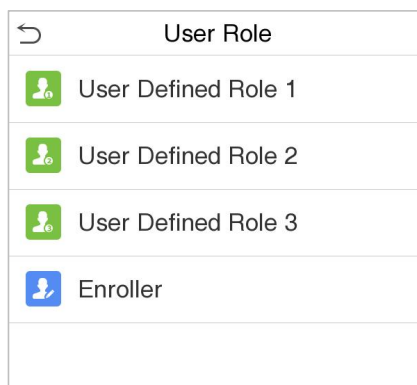
Смешанный:



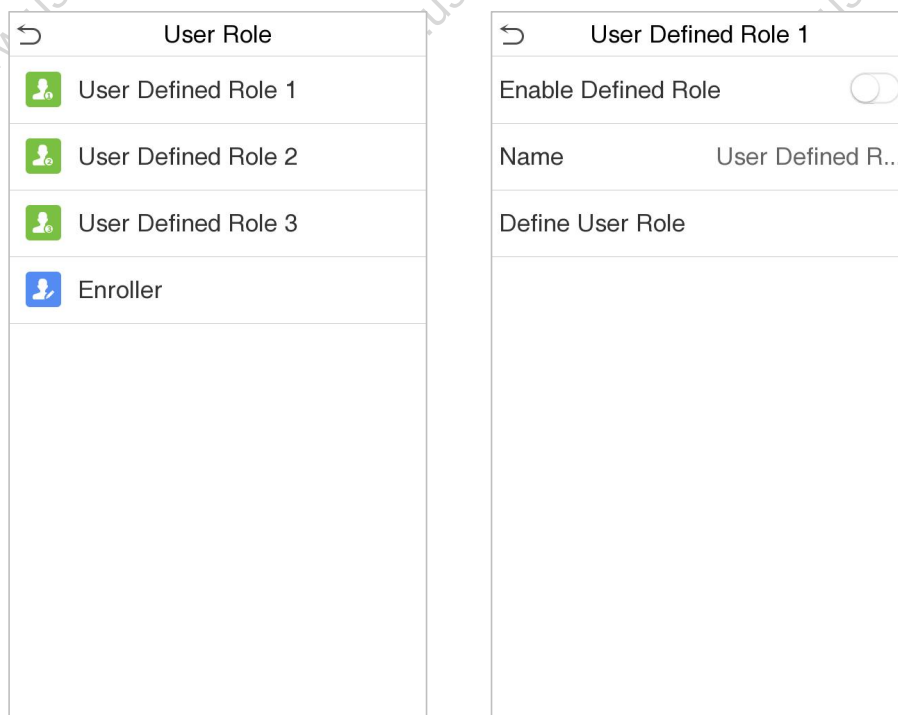
4. Роль пользователя

Данная функция упрощает предоставление специальных разрешений определенным пользователям по мере необходимости.

- В главном меню нажмите **User Role (Роль пользователя)** и затем **User Defined Role (Персонализированная роль)** для предоставления специальных разрешений пользователям.
- В рамках одной персонализированной роли возможно одновременно предоставить одному пользователю до трех разрешений, определяющих его права доступа к различным функциям устройства.



- На странице User Defined Role с помощью одноименного тумблера можно назначить пользователю персонализированную роль или отменить ее.
- Нажмите **Name (Имя)** и введите название персонализированной роли.



- Затем нажмите **Define User Role** и отметьте нужные права для создаваемой роли, после чего нажмите **Return (Назад)**.
- В процессе назначения прав для новой роли в левой части экрана будут отображаться функции главного меню, а справа – его подменю.

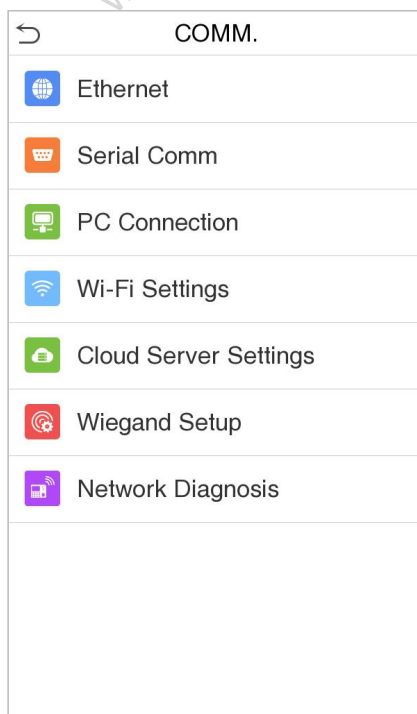
- Сначала поставьте галочки напротив нужных функций главного меню слева, а затем отметьте подменю справа.

← User Defined R... 1↓	← User Mgt.
☒ User Mgt.	☒ New User
☒ COMM.	☒ All Users
☒ System	☒ Display Style
☐ Personalize	
☐ Data Mgt.	
☒ Intercom	
☒ Access Contro l	
☐ USB Manager	
☐ Attendance Se arch	
☐ Autotest	

Примечание: Если на устройстве включена функция Роли пользователя, нажмите **User Mgt.>New User>User Role** для назначения созданных ролей определенным пользователям. Если на устройстве не зарегистрирована учетная запись супер администратора, при попытке включения функции Роли пользователя на экране появится сообщение **"Please enroll super admin first!"** ("Сначала зарегистрируйте супер администратора!").

5. Настройки связи

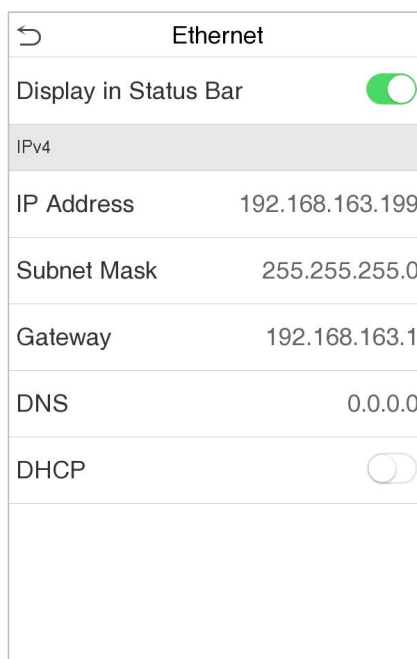
Нажмите **COMM (Связь)** в главном меню для установки нужных параметров сети, последовательного интерфейса, связи с ПК, беспроводной сети, облачного сервера, Wiegand и диагностики сети.



5.1 Настройки сети

Для связи устройства с ПК через Ethernet необходимо настроить конфигурацию сети и убедиться, что устройство и ПК подключены к одному и тому же сегменту сети.

Нажмите **Ethernet** на странице настройки Comm. для конфигурации настроек.



Описание функций

имя функции	Описание
Отображение в строке состояния	Включение/отключение отображение значка сети в строке состояния.
IP Адрес	IP-адрес по умолчанию 192.168.1.201. Его можно изменить согласно возможностям сети.
Маска подсети	Маска подсети по умолчанию 255.255.255.0. Его можно изменить согласно возможностям сети.
Шлюз	Адрес шлюза по умолчанию 0.0.0.0. Его можно изменить согласно возможностям сети.
DNS	DNS-адрес по умолчанию 0.0.0.0. Его можно изменить согласно возможностям сети.
DHCP	Протокол динамической конфигурации хоста (DHCP) автоматически назначает IP-адреса клиентам через сервер.

5.2 Последовательный интерфейс

Функция последовательного интерфейса облегчает установку связи с устройством через последовательный порт (RS485/ Главное устройство).

Нажмите **Serial Comm. (Последовательный интерфейс)** в меню настроек связи.

Serial Comm

Serial Port

No Using

Baudrate

115200

Serial Port

☐ No Using
☒ RS485(PC)
☐ Master Unit

Описание функций

Имя функции	Описание
Последовательный порт	no using: связь с устройством через последовательный порт отсутствует. RS485(PC): связь с устройством через последовательный порт RS485. Master Unit: при использовании RS485 в функции Главного блока, устройство будет работать как Главный блок и может быть подключено к считывателю карт RS485.

Скорость передачи в бодах	Есть 4 скорости в бодах для обмена данными с ПК (115200 (по умолчанию), 57600, 38400 и 19200). Чем выше скорость передачи данных, тем выше скорость связи, но вместе с тем и менее надежна. Следовательно, более высокая скорость в бодах может использоваться, когда расстояние передачи данных небольшая; в других случаях надежней выбирать менее высокую скорость в бодах.
----------------------------------	---

5.3 Подключение ПК

В целях повышения информационной безопасности установите ключ для защищенной связи (Comm Key) между устройством и ПК. Если такой ключ установлен, необходимо ввести пароль перед подключением устройства к ПК.

Нажмите **PC Connection (Подключение ПК)** в меню настроек связи для конфигурации настроек связи с ПК.

PC Connection

Comm Key *****

Device ID 1

TCP COMM.Port 4370

HTTPS ☒

Описание функций

Имя функции	Описание
Ключ связи	Пароль по умолчанию - 0, и он может быть изменен. Ключ должен содержать 6 цифр.
Идентификатор устройства	Идентификационный номер устройства - в диапазоне от 1 до 254. Если связь осуществляется через RS232/RS485, необходимо ввести идентификационный номер устройства в меню настройки связи.
Порт TCP COMM	Порт TCP COMM по умолчанию 4370. Он может быть изменен согласно возможностям сети.

Протокол HTTPS

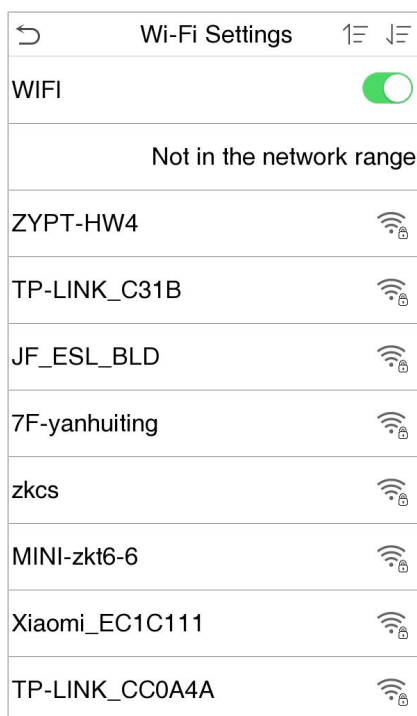
В целях повышения безопасности доступа к ПО пользователи могут активировать протокол HTTPS для создания безопасной и зашифрованной передачи данных по сети, а также использовать верификационные процедуры и ключи для защищенной связи. Эта функция включена по умолчанию. Эту функцию можно включить/выключить через интерфейс меню, а при изменении статуса HTTPS устройство выведет на экран запрос безопасности и выполнит перезапуск после подтверждения.

5.4 Беспроводная сеть★

В устройстве предусмотрен модуль Wi-Fi, который может быть встроен в устройство или подключаться отдельно.

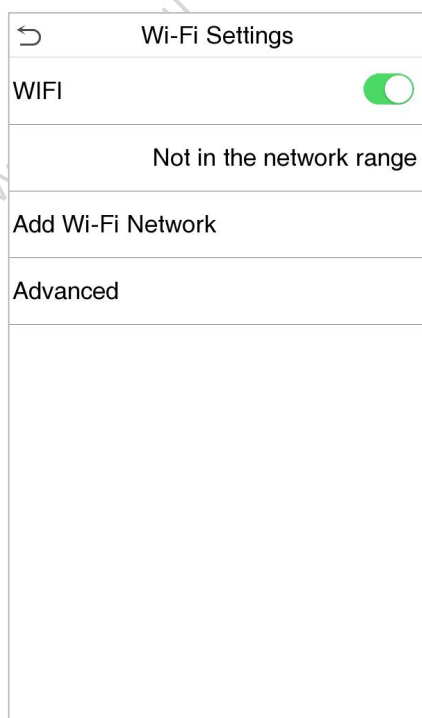
Модуль Wi-Fi позволяет передавать данные через Wi-Fi и создает сеть беспроводного доступа. Функция Wi-Fi активирована в этом устройстве по умолчанию. При неиспользовании сети Wi-Fi вы можете отключить ее путем нажатия на одноименную кнопку.

Нажмите **Wireless Network (Беспроводная сеть)** в меню настроек связи для конфигурации настроек Wi-Fi.

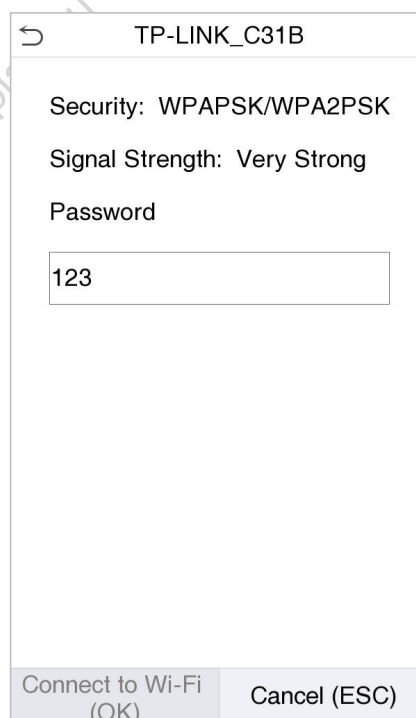


● Поиск сети Wi-Fi

- Сеть Wi-Fi активирована на устройстве по умолчанию. Используйте тумблер  для включения/отключения Wi-Fi
- После включения функции Wi-Fi устройство начнет поиск доступных сетей Wi-Fi в зоне действия сети.
- Выберите нужную сеть Wi-Fi из списка доступных сетей и введите пароль; затем нажмите **Connect to Wi-Fi (OK) (Подключиться к Wi-Fi))**.



Wi-Fi включена: Выберите нужную сеть из списка найденных сетей.

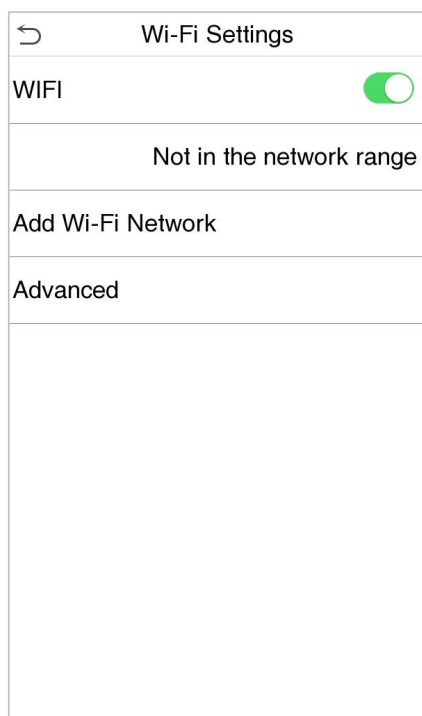


Введите пароль в строке ввода и нажмите Connect to Wi-Fi (OK).

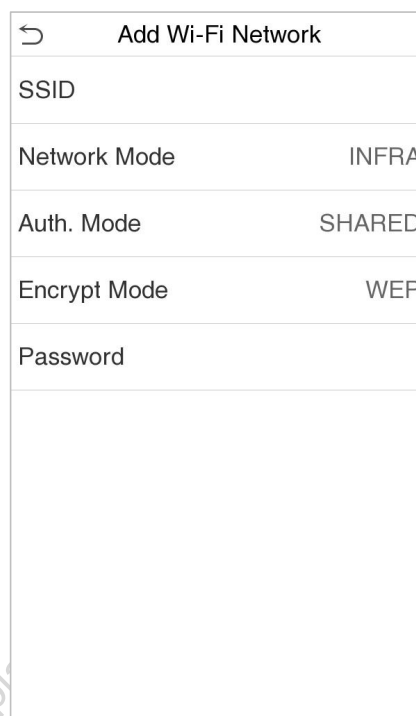
- Если вы успешно подключились к сети Wi-Fi, на странице отобразится символ Wi-Fi .

- Добавление сети Wi-Fi вручную**

Сеть Wi-Fi можно добавить вручную, если она отсутствует в списке найденных сетей.



Нажмите **Add Wi-Fi Network (Добавить сеть Wi-Fi)** для добавления сети вручную.



На открывшейся странице введите параметры сети Wi-Fi (добавляемая сеть должна физически существовать).

Примечание: После добавления сети Wi-Fi вручную выполните те же шаги для поиска добавленной сети Wi-Fi. Нажмите здесь для просмотра процесса поиска сети Wi-Fi.

● **Расширенные настройки**

В меню сети Wi-Fi нажмите **Advanced (Расширенные)** для установки необходимых дополнительных параметров сети.

↶Wi-Fi Settings WIFI Not in the network range Add Wi-Fi Network Advanced	↶Ethernet DHCP IP Address192.168.0.15 Subnet Mask255.255.255.0 Gateway192.168.0.1 DNS192.168.0.1
--	---

Описание функций

Имя функции	Описание
Протокол DHCP	DHCP динамически назначает IP-адреса клиентам сети. Если DHCP включен, IP-адрес не может быть установлен вручную.
IP-адрес	IP-адрес для сети Wi-Fi по умолчанию – 0.0.0.0. Его можно изменить согласно возможностям сети.
Маска подсети	Маска подсети сети Wi-Fi по умолчанию – 255.255.255.0. Ее можно изменить согласно возможностям сети.
Сетевой шлюз	Адрес шлюза по умолчанию – 0.0.0.0. Его можно изменить согласно возможностям сети.
DNS	Адрес DNS по умолчанию – 0.0.0.0. Его можно изменить согласно возможностям сети.

5.5 Настройки облачного сервера

Нажмите **Cloud Server Setting (Настройки облачного сервера)** в меню настроек связи для соединения с сервером ADMS.

↶

Cloud Server Settings

Server Mode	ADMS
Enable Domain Name	☐
Server Address	192.168.163.61
Server Port	8081
Enable Proxy Server	☐

Описание функций

Имя функции		Описание
Включить доменное имя	Адрес сервера	После включения этой функции будет использоваться имя домена "http://... ", такое как http://www.XYZ.com, где "XYZ" обозначает имя домена (когда этот режим включен).
	Порт сервера	Порт, используемый сервером ADMS.
Включить прокси-сервер		В случае активации прокси-сервера необходимо установить IP-адрес и номер порта прокси-сервера.

5.6 Настройки Wiegand

Для установки входных и выходных параметров Wiegand выполните следующие действия. Нажмите **Wiegand Setup (Настройки Wiegand)** в меню настроек связи для настройки входных и выходных параметров Wiegand .

↶

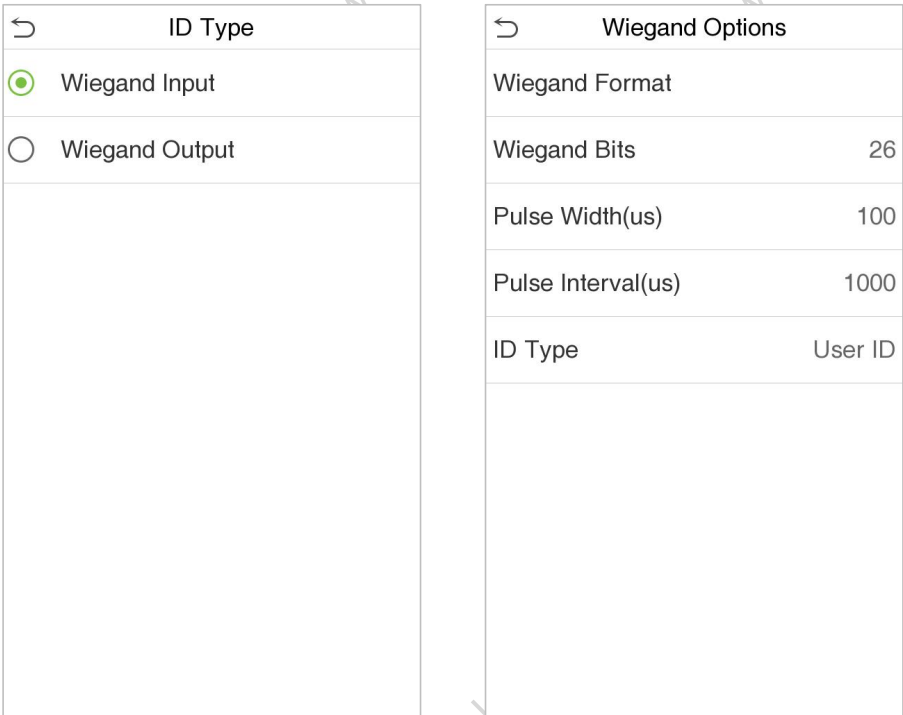
Wiegand Setup

ID Type	Wiegand Output
Wiegand Options	

Примечание: если несколько устройств используют интерфейс Wiegand, пользователь может выбрать вход или выход Wiegand для соединения с другими устройствами, поддерживающими тот же протокол связи.

5.6.1 Вход Wiegand

Нажмите **ID Type (Тип ID)** в меню **Wiegand Setup (Настройки Wiegand)**, выберите **Wiegand Input (Вход Wiegand)** и нажмите **Wiegand Options (Опции Wiegand)** в меню **Wiegand Setup**.



Описание функций

Имя функции	Описание
Формат Wiegand	Доступные значения: 26, 32, 34, 36, 37, 50 и 64 бит.
Wiegand в битах	Число битов данных Wiegand.
Ширина импульса (мкс)	По умолчанию ширина импульса, отправляемого по Wiegand, составляет 100 мкс; это значение можно корректировать в пределах от 20 до 400 мкс.
Интервал импульса (мкс)	Значение импульсного интервала по умолчанию 1000 мкс и может быть скорректировано в пределах от 200 до 20000 мкс.
Тип идентификатора	Выберите идентификатор типа: ID пользователя или номер карты.

Описание стандартных форматов Wiegand

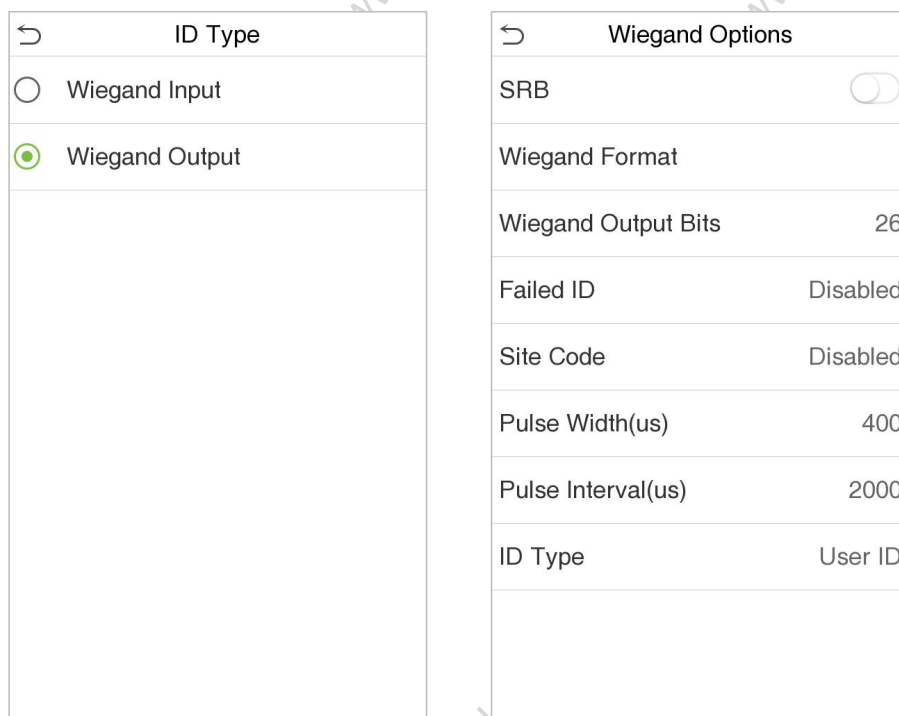
Формат Wiegand	Описание
Wiegand26	ЕСССССССССССССССССССССССССССССССССС Состоит из 26 бит двоичного кода. 1-й бит является битом проверки четности для 2-13 бита, а 26-й бит - битом проверки нечетности для 14-25 бита. Биты 2-25 являются номером карты.

Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Состоит из 26 бит двоичного кода. 1-й бит является битом проверки четности для 2-13 бита, а 26-й бит - битом проверки нечетности для 14-25 бита. Биты 2-9 являются кодом сайта, а 10-25 биты - номером карты.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCO Состоит из 34 бит двоичного кода. 1-й бит является битом проверки четности для 2-17 бита, а 34-й бит - битом проверки нечетности для 18-33 бита. 2-25 биты являются номером карты.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCO Состоит из 34 бит двоичного кода. 1-й бит является битом проверки четности для 2-17 бита, а 34-й бит - битом проверки нечетности для 18-33 бита. 2-9 биты являются кодом сайта, а 10-25 биты - номером карты.
Wiegand36	OFFFFFFFFFFFFFFFCCCCCCCCCCCMMME Состоит из 36 бит двоичного кода. 1-й бит является битом проверки нечетности для 2-18 бита, а 36-й бит - битом проверки четности для 19-35 бита. 2-17 биты - это коды устройства. 18-33 биты - номер карты, а 34-35 биты - код производителя.
Wiegand36a	EEEEEEEEEEEEEEEEFFFFCCCCCCCCCCCO Состоит из 36 бит двоичного кода. 1-й бит является битом проверки четности для 2-18 бит, а 36-й бит - битом проверки нечетности для 19-35 бита. 2-19 биты являются кодом устройства, а 20-35 биты - номер карты.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCE Состоит из 37 бит двоичного кода. 1-й бит является битом проверки нечетности для 2-18 бит, а 37-й бит - битом проверки четности для 19-36 бита. 2-4 биты - код производителя, 5-16 биты - код сайта, а 21-36 биты - номер карты.
Wiegand37a	EMMFFFFFFFFFSSSSSCCCCCCCCCCCCCO Состоит из 37 бит двоичного кода. 1-й бит является битом проверки четности для 2-18 бит, а 37-й бит - битом проверки нечетности для 19-36 бита. 2-4 биты - код производителя, 5-14 биты - код устройства, 15-20 биты - код сайта, а 21-36 биты - номер карты.
Wiegand50	ESSSSSSSSSSSSSSSAAAAAAAAAAAAA Состоит из 50 бит двоичного кода. 1-й бит является битом проверки четности для 2-25 бита, а 50-й бит - битом проверки нечетности для 26-49 бита. 2-17 биты - коды сайта, а 18-49 биты - номер карты.

"C" означает номер карты; "E" - бит проверки четности; "O" - бит проверки нечетности. "F" - код устройства; "M" - код производителя; "P" -бит проверки четности и "S" - код места.

5.6.2 Выход Wiegand

Нажмите **ID Type (Тип ID)** в меню **Wiegand Setup (Настройки Wiegand)**, выберите **Wiegand Output (Выход Wiegand)** и нажмите **Wiegand Options (Опции Wiegand)** в меню **Wiegand Setup**.



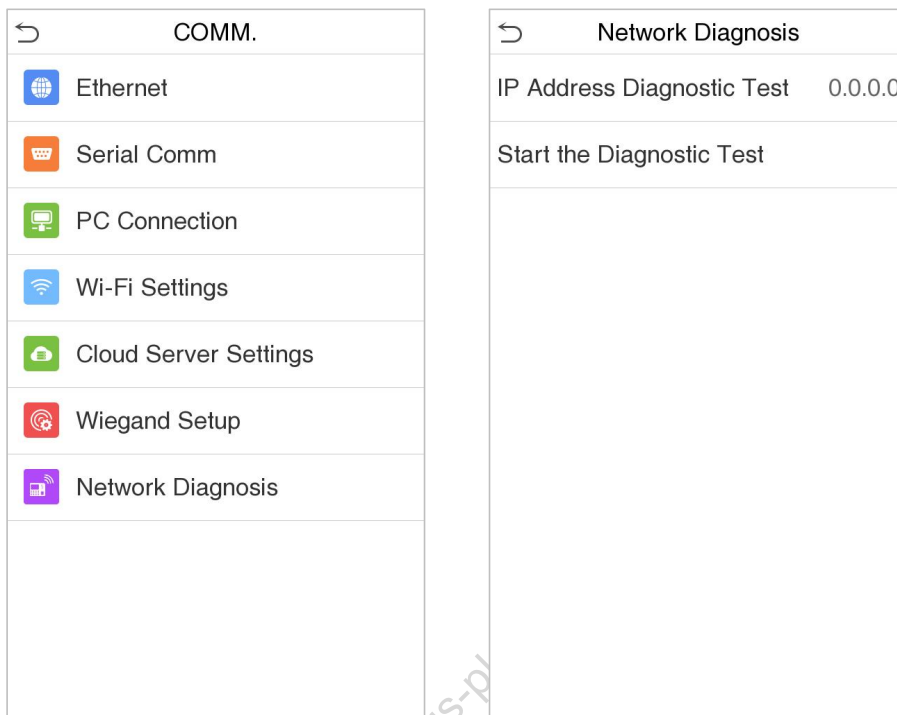
Описание функций

Имя функции	Описание
SRB(блок реле безопасности)	Когда SRB активирован, управление замком двери осуществляется через SRB для предотвращения его разблокировки по причине удаления устройства.
Формат Wiegand	Доступные значения: 26, 32, 34, 36, 37 и 50 бит.
Биты выходных параметров Wiegand	После выбора нужного формата Wiegand выберите соответствующие выходные биты Wiegand.
Неудавшийся идентификатор	Если верификация не удалась, система отправит недействительный идентификатор на устройство и заменит номер карты или ID сотрудника на новый.
Код сайта	Аналогичен идентификатору устройства с той лишь разницей, что код места может быть установлен вручную и повторен на другом устройстве. Диапазон - от 0 до 256 по умолчанию.
Ширина импульса (мкс)	Ширина импульса – это изменения в количестве электрического заряда с высокочастотной емкостью за определенный промежуток времени.
Интервал импульса (мкс)	Временной промежуток между импульсами.
Тип идентификатора	Выберите между идентификатором пользователя или номером карты.

5.7 Диагностика сети

Для установки параметров диагностики сети выполните следующие действия.

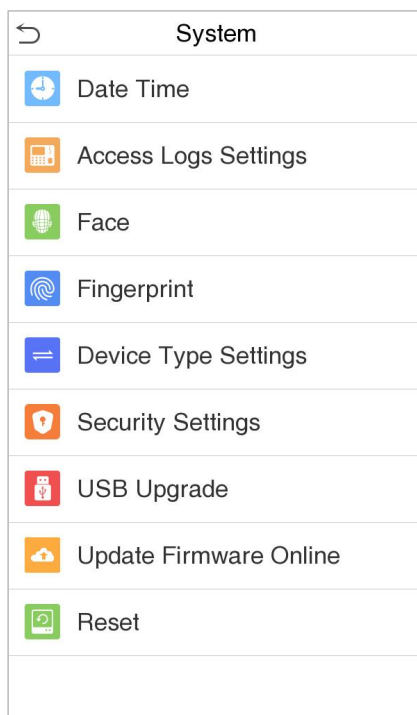
Нажмите **Network Diagnostics (Диагностика сети)** в меню настроек связи, чтобы ввести IP-адрес для диагностики и запустите диагностику.



6. Системные настройки

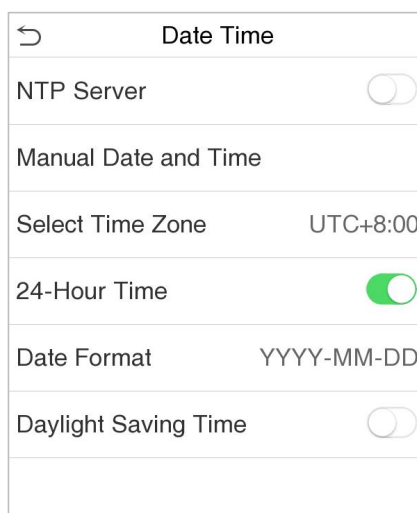
Установите системные параметры для оптимизации работы устройства.

Нажмите **System (Система)** в главном меню для установки системных настроек.



6.1 Дата и время

Нажмите **Date Time (Дата и время)** в меню **System (Система)** для установки даты и времени.



- По умолчанию устройство поддерживает синхронизацию времени по протоколу NTP. Для этого необходимо включить **сервер NTP** и установить связь с его адресом.
- Если вы хотите установить дату и время вручную, сначала отключитесь от **сервера NTP**, затем нажмите **Manual Data and Time (Установка даты и времени вручную)**, установите дату и время, и нажмите **Confirm (Подтвердить)** для сохранения выполненных настроек.

Date Time	
NTP Server	☐
Manual Date and Time	
Select Time Zone	UTC+8:00
24-Hour Time	☒
Date Format	YYYY-MM-DD
Daylight Saving Time	☒
Daylight Saving Mode	By Date/Time
Daylight Saving Setup	

- Нажмите **24-Hour Time**, чтобы включить/отключить данный формат времени. В случае использования этого формата нажмите **Date Format (Формат даты)** для установки формата даты.
- Нажмите **Daylight Saving Time (Летнее время)** для включения/выключения данной функции. При включении нажмите **Daylight Saving Mode (Режим летнего времени)** для выбора режима летнего времени и затем **Daylight Saving Setup (Настройка летнего времени)** для установки времени перехода на летнее время.

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

Week mode

Daylight Saving Setup	
Start Date	00-00
Start Time	00:00
End Date	00-00
End Time	00:00

Date mode

- При восстановлении заводских настроек можно восстановить формат времени (24-часовой) и даты (ГГГГ-ММ-ДД), но не установленные дату и время.

Примечание: Например, если пользователь устанавливает время устройства (18:35, 15 марта 2019) на 18:30, 1 января 2020 г., после восстановления заводских настроек время устройства останется таким же, т.е. 18:30, 1 января 2020 г.

6.2 Настройки журналов доступа

Нажмите **Access Logs Settings (Настройки журналов доступа)** в меню **System (Система)**.

Access Logs Settings	
Camera Mode	No photo
Display User Photo	☐
Alphanumeric User ID	☐
Access Log Alert	99
Periodic Del of Access Logs Disabled	
Periodic Del of T&A Photo	99
Periodic Del of Blocklist Photo	99
Authentication Timeout(s)	3
Recognition Interval(s)	1

Описание функций

Имя функции	Описание
Режим камеры	Эта функция отключена по умолчанию. При включении на экране появится запрос безопасности, и вы услышите звук затвора камеры. Имеются 5 режимов: No Photo: во время верификации фотографирование не выполняется. Take photo, no save: При верификации камера делает снимки, без сохранения. Take photo and save: При верификации камера делает снимки, с сохранением. Save on successful verification: Снимок сохраняется каждый раз при успешной верификации. Save on failed verification: Сохранение снимков происходит только в тех случаях, когда верификация не была выполнена успешно.
Отображать пользовательскую фотографию	Отображение фото пользователя отключено по умолчанию. При включении будет появляться запрос безопасности.
Буквенно-цифровой ID пользователя	Включение/выключение поддержки ввода букв в ID пользователя.
Предупреждение журналов доступа	В случае недостатка свободной памяти в журнале доступа (достижение нижнего порогового значения) отобразится соответствующее предупреждение. Пользователи могут отключить эту функцию или установить допустимое значение от 1 до 9999.

Циклическое удаление записей доступа	При заполнении памяти устройство автоматически удаляет старые записи журналов доступа. Пользователи могут отключить эту функцию или установить допустимое значение от 1 до 999.
Циклическое удаление фотографий УРВ	При заполнении памяти фото посещаемости устройство удаляет старые фото. Пользователи могут отключить эту функцию или установить допустимое значение от 1 до 99.
Циклическое удаление фотографий заблокированного списка	При заполнении хранилища фото из списка блокировок устройства автоматически удаляет старые фото. Пользователи могут отключить эту функцию или установить допустимое значение от 1 до 99.
Подтвердить время задержки экрана (сек)	Период времени отображения сообщения об успешной верификации. Допустимое значение: от 1 до 9 секунд.
Интервал сравнения лица (сек)	Установка временного интервала между сравнениями шаблонов лица. Допустимое значение: от 0 до 9 секунд.

6.3 Параметры шаблона лица

Нажмите **Face (Лицо)** в меню **System (Система)** для перехода в меню настроек параметров шаблона лица.

↶	Face	1↓
1:N Threshold		40
1:1 Threshold		30
Face Enrollment Threshold		70
Image Quality		40
Facial Recognition Distance		Far
Anti-spoofing Using NIR	☒	
Binocular Live Detection Thresh hold		30
Face AE	☐	
WDR	☐	
Anti-flicker Mode		Disable

↶	Face	1↓
1:1 Threshold		30
Face Enrollment Threshold		70
Image Quality		40
Facial Recognition Distance		Far
Anti-spoofing Using NIR	☒	
Binocular Live Detection Thresh hold		30
Face AE	☐	
WDR	☐	
Anti-flicker Mode		Disable
Face Algorithm		

FRR	FAR	Рекомендуемые пороговые значения сравнения	
		1:N	1:1
Высокое	Низкое	85	80
Среднее	Среднее	82	75
Низкое	Высокое	80	70

Описание функций

Имя функции	Описание
Порог сравнения 1:N (один ко многим)	В данном режиме верификация будет успешной, когда сходство между сделанным снимком лица и всеми зарегистрированными в устройстве шаблонами лиц превысит установленное пороговое значение. Допустимое значение: от 0 до 100. Чем выше заданный порог, тем ниже процент ошибок и выше процент отказов, и наоборот. Рекомендуется значение по умолчанию – 75.
Порог сравнения 1:1 (один к одному)	В данном режиме верификация будет успешной, только когда сходство между сделанным снимком лица и всеми шаблонами лица пользователя, зарегистрированными на устройстве, будет выше порогового значения. Допустимое значение: от 0 до 100. Чем выше заданный порог, тем ниже процент ошибок и выше процент отказов, и наоборот. Рекомендуется значение по умолчанию – 63.
Пороговое значение при регистрации лица	При регистрации шаблона лица используется метод сравнения 1:N для определения того, регистрировался ли пользователь ранее. Когда сходство между сделанным снимком лица и всеми зарегистрированными на устройстве шаблонами лиц выше заданного порога, это означает, что такой шаблон уже был зарегистрирован ранее.
Качество изображения	Качество изображения для регистрации и сравнения шаблонов лиц. Чем выше значение, тем более четкое изображение требуется.
Расстояние распознавания лиц	Система будет игнорировать распознавание лиц при превышении установленного значения расстояния распознавания лиц. Под расстоянием понимается размер шаблона лица, необходимый для регистрации и сравнения. Чем больше расстояние до человека, тем меньше будет плотность пикселей шаблона лица. Когда значение равно 0, то расстояние сравнения лиц не ограничено.
Борьба с подделкой с помощью NIR	Использование съемки в ближнем инфракрасном диапазоне для выявления и защиты от поддельных видео и фотографий.
Порог обнаружения живого объекта	Удобный инструмент для выявления фейковых фото- и видеоснимков, полученных в ближнем инфракрасном диапазоне. Чем больше значение, тем выше эффективность защиты от подделок при использовании спектральных изображений ближнего инфракрасного диапазона.
Режим Face AE	При включенном режиме Face AE устройство увеличивает яркость области лица перед камерой, в то же время затемняя иные области.
WDR	Технология WDR (широкого динамического диапазона) балансирует яркость изображения в камерах видеонаблюдения в сценах с сильным контрастом, а также позволяет идентифицировать объекты на фоне яркого света или в глубокой тени.
Режим борьбы с мерцанием	Используется при отключенном WDR. Помогает уменьшить мерцание, когда экран мерцает с той же частотой, что и свет.
Алгоритм распознавания лиц	Информация, относящаяся к алгоритму распознавания лица, и возможность приостановки обновлений шаблона лица.
Примечание	Некорректная настройка параметров экспозиции и качества может серьезно повлиять на работу устройства. Выполняйте данную операцию только под руководством наших специалистов.

6.4 Параметры отпечатков пальцев★

Нажмите **Fingerprint (Отпечаток пальца)** в меню **System (Система)**.

↩	Fingerprint
1:1 Threshold	15
1:N Threshold	35
FP Sensor Sensitivity	Low
1:1 Retry Attempts	3
Fingerprint Algorithm	ZKFinger VX13.0
Fingerprint Image	None

FRR	FAR	Рекомендуемые пороговые значения сравнения	
		1:N	1:1
Высокое	Низкое	45	25
Среднее	Среднее	35	15
Низкое	Высокое	25	10

Описание функций

Имя функции	Описание
Порог сравнения 1:1	В данном режиме верификация будет успешной, только когда сходство между снятым отпечатком пальца и зарегистрированным на устройстве шаблоном отпечатком пальца, «привязанным» к введенному пользователем идентификатору, выше установленного значения.
Порог сравнения 1:N	В данном режиме верификация будет успешной, только когда сходство между снятым отпечатком пальца и всеми зарегистрированными на устройстве шаблонами отпечатков пальцев выше установленного порогового значения.
Чувствительность датчика отпечатков пальцев	Настройка чувствительности снятия отпечатков пальцев. Рекомендуется установить уровень по умолчанию "Medium" (Средний). При повышенной сухости воздуха и, как следствие, более медленном распознавании отпечатков, вы можете установить уровень чувствительности "High" (Высокий); при повышенной влажности воздуха, затрудняющей идентификацию, вы можете установить низкий уровень "Low".
Число повторов 1:1	При верификации 1:1 пользователи могут забыть, какой палец был зарегистрирован, или приложить палец неправильно. Чтобы не вводить ID повторно, у пользователя есть вторая попытка.
Отображение отпечатка пальца	Переключение версии алгоритма отпечатков пальцев: Finger VX13.0 или Finger VX10.0.

Если данная функция отключена (по умолчанию), отпечаток сканируемого пальца не будет отображаться во время процедур регистрации и верификации. Можно включить эту функцию; при этом, будут всплывать запросы безопасности. Доступны четыре варианта:

Show for enroll: отображать отпечаток пальца на экране только при регистрации.

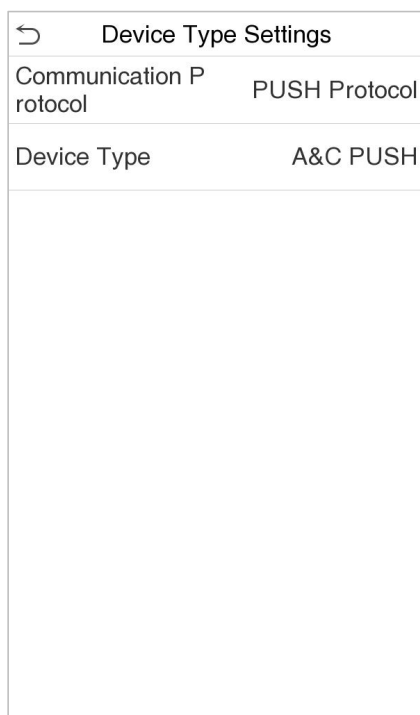
Show for match: отображать отпечаток пальца на экране только при верификации.

Always show: отображать отпечаток пальца во время регистрации и верификации.

None: не отображать отпечаток пальца.

6.5 Настройки типа устройства

Нажмите **Device Type Setting (Настройки типа устройства)** в меню System.

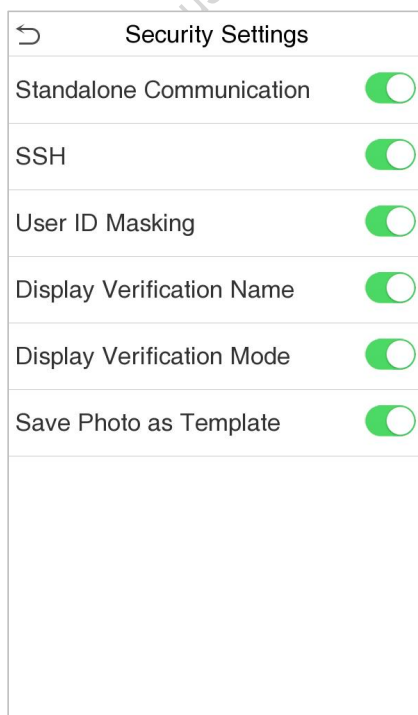


Описание функций

Имя функции	Описание
Протокол связи	Установите протокол связи для устройства (протокол BEST управляется через ZKBio Zlink; смотри раздел 15 "Подключение к ZKBio Zlink Web" и 16 "Подключение к ZKBio Zlink App").
Тип устройства	Настройте устройство как терминал учета рабочего времени (T&A PUSH) или контроллер доступа (A&C PUSH).

6.6 Настройки безопасности

Нажмите **Security Setting (Настройки безопасности)** в системном меню.



Описание функций

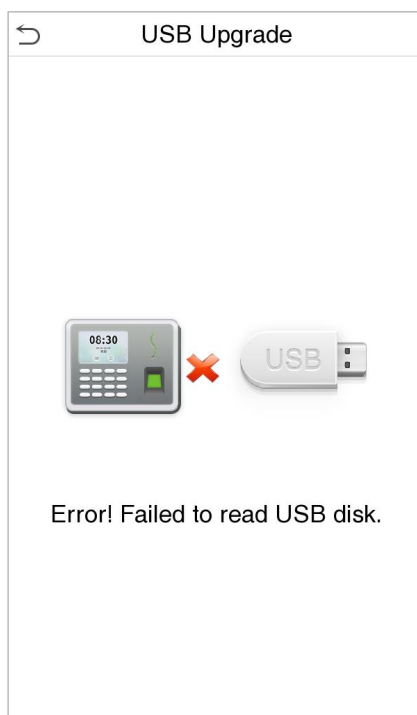
Имя функции	Описание
Автономная связь	Эта функция включается/отключается через интерфейс меню (по умолчанию отключена). В случае ее активации появится запрос безопасности, после подтверждения которого устройство перезагрузится.
SSH	Поскольку устройство не поддерживает протокол telnet, для удаленной отладки обычно используется SSH. Интерфейс меню позволяет включать/отключать SSH (по умолчанию функция включена). При активации появится запрос безопасности, но устройство не нужно будет перезагружать после подтверждения.
Маскировка идентификатора пользователя	При активации этой функции (включена по умолчанию) после верификации пользователя его идентификатор будет частично скрыт (только в том случае если он состоит из более чем двух знаков).
Отобразить имя для подтверждения	Имя пользователя будет отображаться/не будет отображаться после прохождения верификации при включении/отключении этой функции.
Режим проверки отображения	Способ верификации пользователя будет отображаться/не будет отображаться после прохождения верификации при включении/отключении этой функции.
Сохранение фотографии в качестве шаблона	В случае отключения этой функции будет необходима повторная регистрация шаблона лица после обновления алгоритма.

6.7 Обновление через USB

Нажмите **USB Upgrade (Обновление через USB)** в системном меню.

Прошивку устройства можно обновить с помощью файла обновления на USB-накопителе. Перед выполнением этой операции убедитесь, что USB-накопитель содержит нужный файл обновления и правильно вставлен в устройство.

Если USB-накопитель не вставлен, система выдаст соответствующее сообщение после нажатия **USB Upgrade** в системном меню.

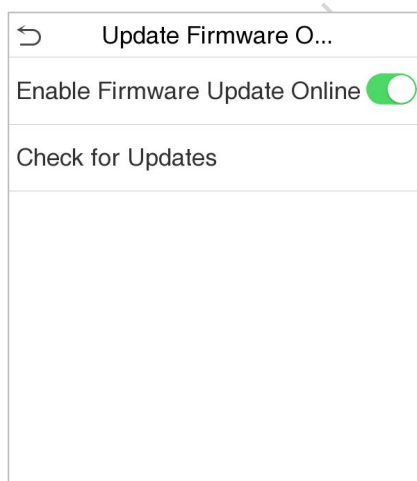


Примечание: Если требуется файл обновления, свяжитесь с нашей службой технической поддержки. Обновление прошивки не рекомендуется при нормальной работе устройства.

6.8 Обновление прошивки онлайн

Нажмите **Update Firmware Online (Обновление прошивки онлайн)** в системном меню.

Установите тумблер **Enable firmware update online (Активировать обновление прошивки онлайн)** в положение «включено». На экране появится сообщение о рисках при установке обновления, пользователь должен подтвердить согласие с обновлением, нажав на соответствующую кнопку (если функция предупреждения о рисках отключена, данное сообщение не будет отображаться при обновлении прошивки).



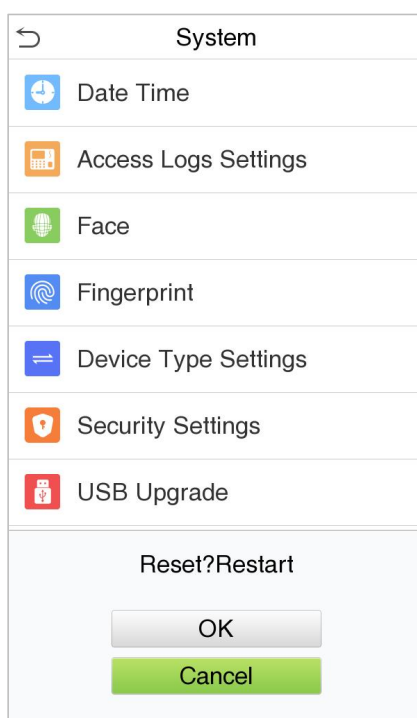
Нажмите **Check for Updates (Проверка доступных обновлений)**, результатом чего будет один из следующих трех сценариев:

- Если по запросу ничего не найдено, появится сообщение "Query failed" (Ошибка запроса).
- Если версия прошивки устройства актуальная, появится соответствующее сообщение о том, что вы пользуетесь последней версией.
- Если вы пользуетесь устаревшей версией прошивки, появятся номер и протокол изменений актуальной версии. Пользователи могут выбрать обновить прошивку до последней версии.

6.9 Сброс до заводских настроек

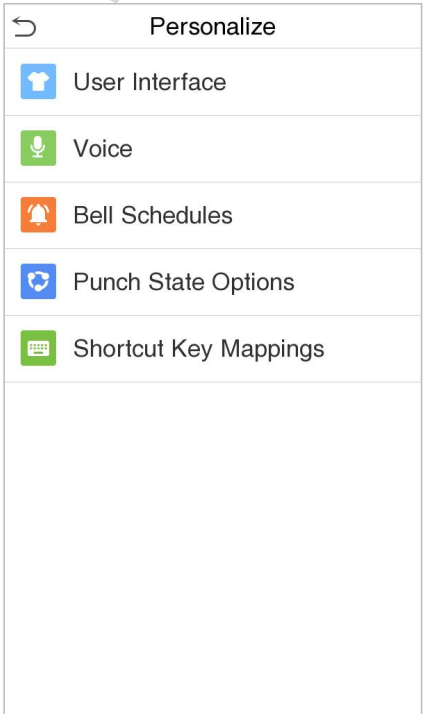
Функция сброса до заводских настроек сбрасывает такие настройки устройства, как настройки связи и системы, до заводских настроек по умолчанию, при этом зарегистрированные данные пользователя не удаляются.

Нажмите **Reset (Сброс)** в системном меню и затем нажмите **OK** для сброса до заводских настроек.



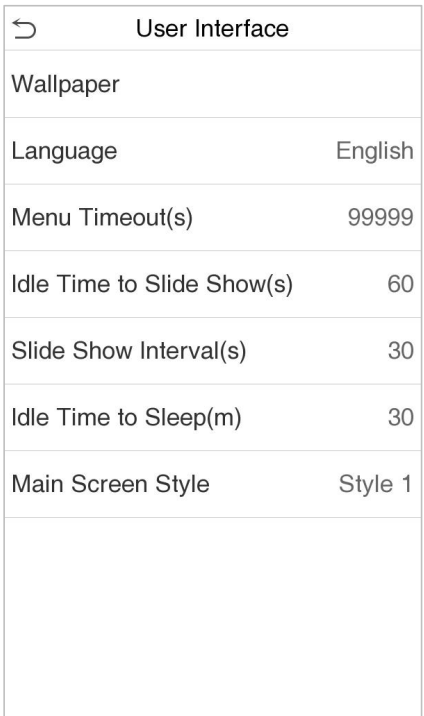
7. Персонализированные настройки

Нажмите **Personalize (Персонализация)** в главном меню для индивидуальной настройки интерфейса, голосовых сообщений, звонка, функциональных клавиш и "горячих" клавиш.



7.1 Настройка интерфейса пользователя

Нажмите **User Interface (Интерфейс пользователя)** в меню Personalize для настройки стиля отображения главного меню.

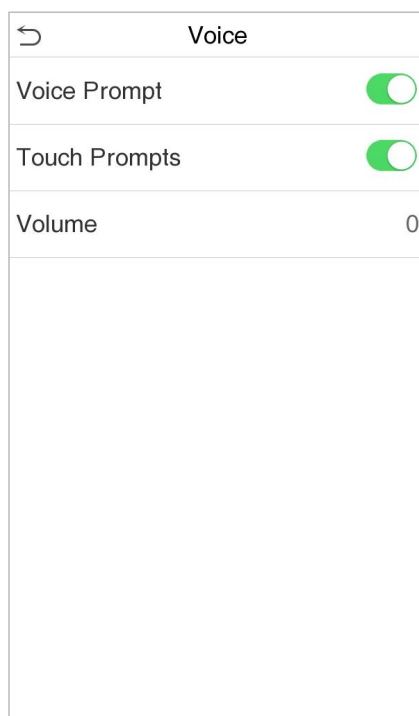


Описание функций

Имя функции	Описание
Обои	Выбор обоев главного экрана согласно предпочтениям пользователей.
Язык	Выбор языка интерфейса устройства.
Время ожидания экрана меню (сек.)	Когда время бездействия превысит установленное значение, устройство автоматически вернется к первоначальному интерфейсу. Вы можете отключить эту функцию или установить значение от 60 до 99999 секунд.
Время бездействия до перехода в слайд-шоу (сек.)	Когда время бездействия превысит установленное значение, устройство перейдет в режим проигрывания слайдов. Вы можете отключить эту функцию или установить значение от 3 до 999 секунд.
Интервал слайд-шоу (сек.)	Установка интервала времени между переключением слайдов. Функцию можно отключить или установить интервал от 3 до 999 секунд.
Время бездействия до перехода в спящий режим (мин.)	Если спящий режим активирован, после определенного времени бездействия устройство перейдет в режим ожидания. Коснитесь экрана для возврата устройства в обычный режим работы. Эту функцию можно отключить или установить значение от 1 до 999 минут.
Стиль главного экрана	Выбор стиля главного экрана согласно предпочтениям пользователей.

7.2 Голосовые настройки

Нажмите **Voice (Голос)** в меню Personalize для установки голосовых настроек.

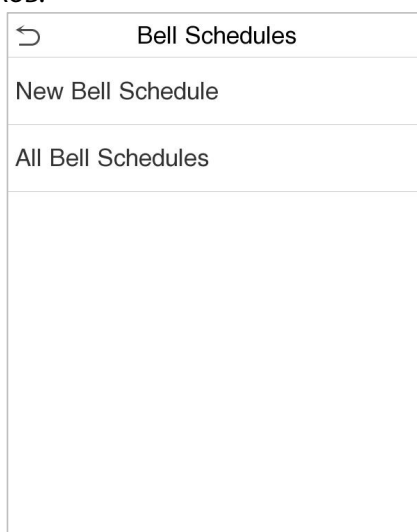


Описание функций

Имя функции	Описание
Голосовая подсказка	ТВключение/выключение голосовых подсказок во время работы устройства.
Сенсорная подсказка	Включение/выключение звукового сопровождения нажатия кнопок.
Громкость	Регулировка громкости устройства в пределах от 0 до 100.

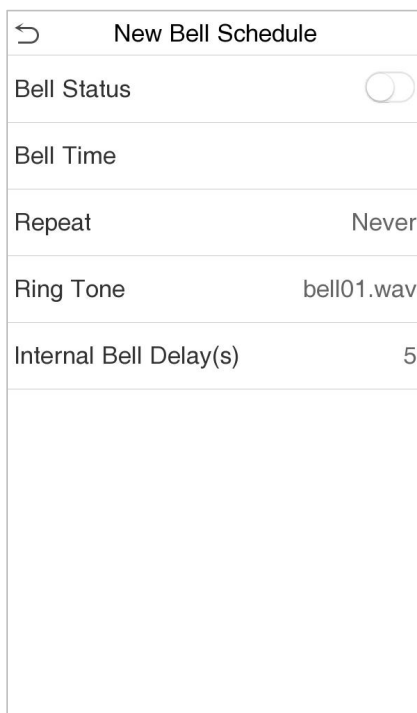
7.3 Расписание звонков

Нажмите **Bell Schedules (Расписание звонков)** на странице Personalize (Персонализация) для перехода в меню настроек звонков.



● Новое расписание звонков

Нажмите **New Bell Schedule (Новое расписание звонков)** на странице **Bell Schedule (Расписание звонков)** для добавления нового расписания.



Описание функций

Имя функции	Описание
Состояние звонка	Включение/выключение звонка.
Время звонка	Если время звонка установлено, устройство автоматически начнет звонить в установленное время.
Повтор	Установка необходимого количества повторений звонка.
Мелодия звонка	Выберите мелодию звонка.
Задержка внутреннего звонка (сек.)	Установка продолжительности проигрывания звонка в пределах от 1 до 999 секунд.

● Все расписания звонков:

Как только Вы установили новое расписание звонка, в меню **Bell Schedules (Расписания звонков)** нажмите **All Bell Schedules (Все расписания звонков)** для просмотра только что созданного расписания звонка.

● Редактирование расписаний звонков:

В меню **All Bell Schedules** выберите нужное расписание звонков и нажмите **Edit (Редактировать)** для его редактирования. Процесс редактирования аналогичен процессу добавления нового расписания.

● Удаление расписания звонков:

В меню **All Bell Schedules** выберите нужное расписание звонков и нажмите **Delete** и затем **Yes** для его удаления.

7.4 Настройки учета событий рабочего времени

Нажмите **Punch States Options (Настройки учета событий рабочего времени)** в меню **Personalize (Персонализация)**.

Punch State Options

Punch State Mode Manual Mode

Punch State Timeout(s) 10

Punch State Required ☐

Punch State Mode

☐ Off

☒ Manual Mode

☐ Auto Mode

☐ Manual and Auto Mode

☐ Manual Fixed Mode

☐ Fixed Mode

Описание функций

Имя функции	Описание
Режим состояния сканирования	Off: Отключение функции Punch State. Соответственно, кнопки учета событий рабочего времени в меню «горячих» клавиш станут неактивны. Manual Mode: Переключение кнопок учета событий рабочего времени вручную; кнопка исчезает при превышении времени ожидания. Auto Mode: Кнопка Punch State автоматически переключается в заданное состояние Punch в соответствии с определенным расписанием (может быть установлено в меню клавиш быстрого доступа). Manual and Auto Mode (): В главном меню отображается кнопка учета событий рабочего времени в автоматическом режиме, но при этом пользователи могут переключиться в ручной режим. При превышении времени ожидания кнопка учета событий рабочего времени, установленная в ручной режим, переходит в автоматический режим. Manual Fixed Mode: После установки кнопки Punch State вручную в определенное состояние оно остается неизменным до следующего ручного переключения. Fixed Mode: Будет отображаться только фиксированное вручную состояние кнопок Punch State, которое пользователи не смогут переключить нажатием каких-либо других кнопок.

7.5 Меню клавиш быстрого доступа

Пользователи могут назначить «горячие» клавиши для быстрого вызова соответствующих событий рабочего времени и функциональных клавиш из отображаемого в главном меню списка. Таким образом, при нажатии той или иной «горячей» клавиши на экран будет выводиться меню выбранного события рабочего времени или функции.

Нажмите **Shortcut Key Mappings (Меню «горячих» клавиш)** в меню персонализации.

Shortcut Key Mappi...	
F1	Check-In
F2	Check-Out
F3	Break-Out
F4	Break-In
F5	Overtime-In
F6	Overtime-Out

- В меню **Shortcut Key Mappings** выберите нужную «горячую» клавишу для ее настройки.
- В меню **Shortcut Key (F1)** выберите пункт **Function (Функция)**, чтобы определить «горячую» кнопку как кнопку события рабочего времени или как функциональную кнопку.
- Если кнопка быстрого доступа определена как функциональная клавиша (например, Новый пользователь, Все пользователи и пр.), отобразится меню, изображенное на рисунке ниже.

F1	
Punch State Value	0
Function	Punch State Options
Name	Check-In

F1	
Function	New User

- Если клавиша быстрого доступа определена как клавиша события рабочего времени (например, приход или уход с работы и пр.), необходимо установить значение от 0 до 250 и имя Punch State.

Примечание: Если Function (функция) установлена как Undefined (Не определено), устройство не активирует кнопку Punch State.

● Установка времени переключения

- Время переключения устанавливается в соответствии с выбранными настройками Punch State.
- Если установлен автоматический режим Punch State, необходимо задать время переключения в меню настроек Punch State.
- В меню выбранной кнопки быстрого доступа выберите пункт **Set Switch Time (Установить время переключения)**.
- В меню **Switch Cycle (Цикл переключения)** выберите нужный цикл (понедельник, вторник и пр.), как показано на рисунке ниже.
- После того как вы выбрали Switch cycle, установите время переключения на каждый день и нажмите ОК для подтверждения, как показано на рисунке ниже.

←

Punch State Mode

Off

Manual Mode

Auto Mode

Manual and Auto Mode

Manual Fixed Mode

Fixed Mode

←

F1

Punch State Value

0

Function

Punch State Options

Name

Set Switch Time

←

Switch Cycle

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

←

Set Switch Time

Switch Cycle

Daily

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

←

Monday

11:30

11

30

HH

MM

Confirm (OK)

Cancel (ESC)

←

Set Switch Time

Switch Cycle

Daily

Monday

11:30

Tuesday

Wednesday

Thursday

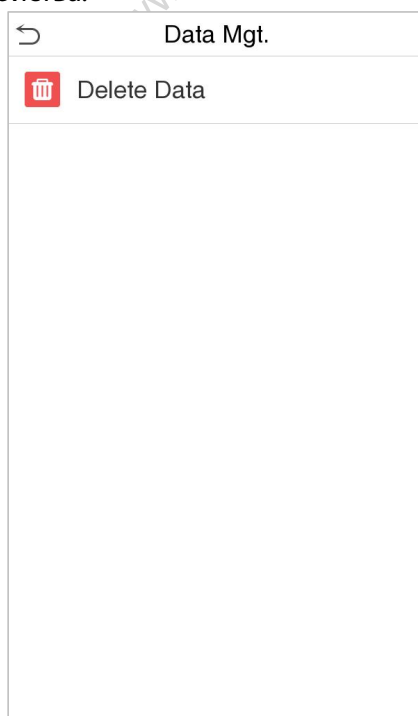
Friday

Saturday

Sunday

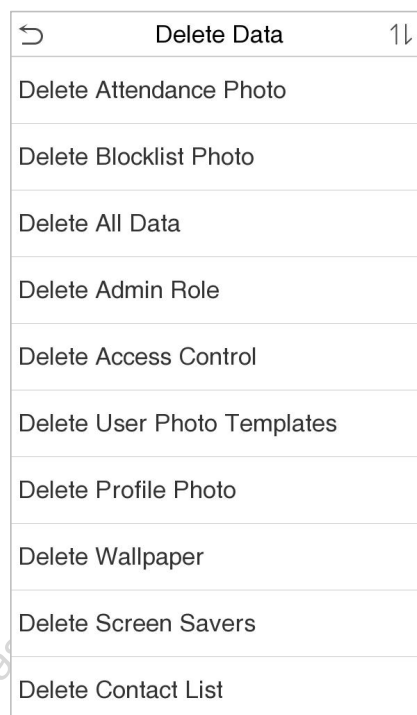
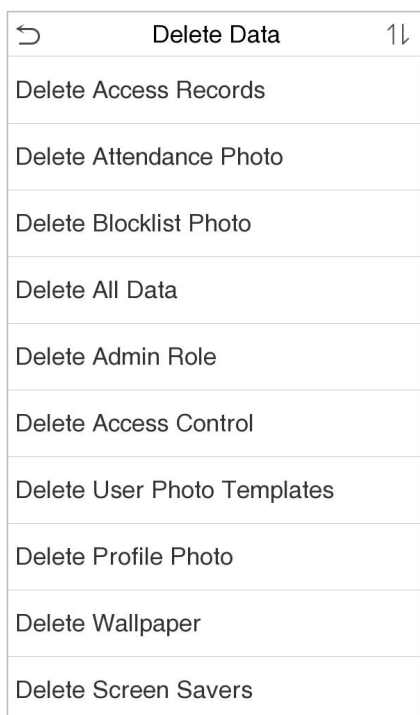
8. Управление данными

На странице главного меню нажмите **Data Mgt. (Управление данными)** для удаления соответствующих данных с устройства.



8.1 Удаление данных

Нажмите **Delete Data (Удалить данные)** в меню Data Mgt. для выбора категории данных, которые нужно удалить.



Описание функций

Имя функции	Описание
Удалить записи доступа	Удалить записи событий при определенных условиях.
Удалить фотографии учета рабочего времени	Удалить фото выбранных сотрудников.
Удалить фотографии черного списка	Удалить снимки, сделанные во время верификации, в которой было отказано.
Удалить все данные	Удалить данные и записи доступа/журналов событий учета рабочего времени всех зарегистрированных пользователей.
Удалить роль администратора	Удалить все права администратора.
Удалить контроль доступа	Удалить все данные управления доступа.
Удалить пользовательские шаблоны фотографий	Удалить шаблоны лиц с устройства. Во время удаления может появиться сообщение: "Face re-registration is required after an algorithm upgrade" (Требуется перерегистрация шаблона лица после обновления алгоритма).
Удалить фотографию пользователя	Удалить фото всех пользователей на устройстве.
Удалить обои	Удалить все обои на устройстве.
Удалить заставки экрана	Удалить заставки экрана на устройстве.
Удалить список контактов	Удалить весь контактный список видеодомофона с устройства.

В отношении удаления записей доступа, фото событий учета рабочего времени или фото из списка блокировок для пользователей доступны две опции: "Delete All" (Удалить все) или "Delete by Time Range" (Удалить за определенный период). При выборе второго варианта необходимо указать период времени, все записи в течение которого будут удалены.

↶Delete Access Rec...

Delete All

Delete by Time Range

↶Start Time

2024-03-19 00:00

▲

▲

▲

▲

▲

2024

03

19

00

00

▼

▼

▼

▼

▼

YYYY

MM

DD

HH

MM

Confirm (OK)

Cancel (ESC)

Выберите **Delete by Time Range**.

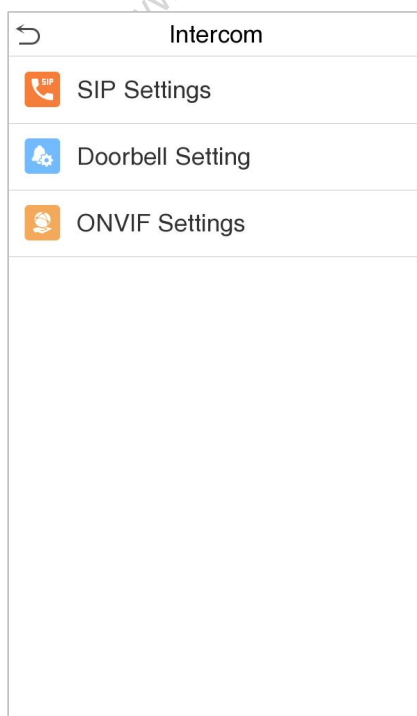
Задайте период времени и нажмите **OK**.

Page | 68

Copyright © 2024 ZKTECO CO., LTD. All rights reserved.

9. Видеодомофон

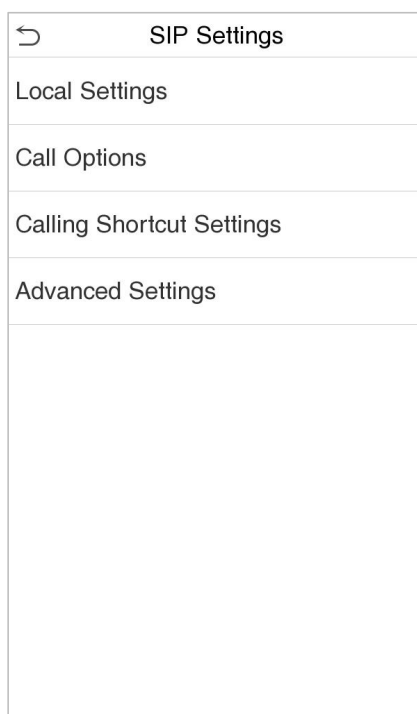
Нажмите **Video intercom Parameters (Параметры видеодомофона)** в меню System.



9.1 Настройки SIP

Примечание: Эта функция используется вместе с внутренним абонентским устройством.

Нажмите **SIP Settings (Настройки SIP)** в меню параметров видеодомофона для перехода к настройке параметров.



Описание функций

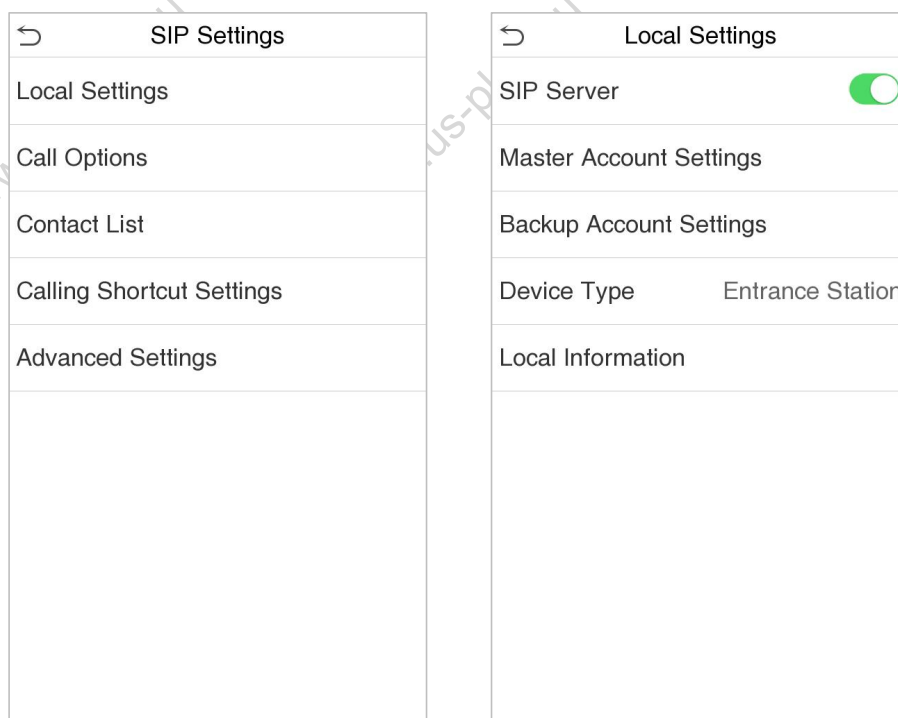
Имя функции		Описание
Локальные настройки	SIP-сервер	Включение адреса сервера. Если включен, вам необходимо установить адрес и порт сервера, отображение имени, имя и пароль пользователя.
	Настройки главной учетной записи	Выберите, включать или не включать адрес центрального сервера. Если включен, вам необходимо установить адрес и порт сервера, отображение имени, имя и пароль пользователя. <i>Примечание: функция SIP-сервера не будет работать при отключении указанной выше опции.</i> Enable Domain Mode: включение режима домена. Server Address: ввод адреса сервера. Server Port: ввод порта сервера. Display Name: отображение имени сервера. User Name: ввод имени пользователя сервера. Verify ID: ввод идентификатора верификации сервера. Password: ввод пароля сервера. Transport Protocol: установка транспортного протокола между устройством и внутренним абонентским устройством.
	Настройки учетной записи резервного копирования	Выберите, включать или не включать адрес резервного сервера. Если включен, вам необходимо установить адрес и порт сервера, отображение имени, имя и пароль пользователя. Enable Domain Mode: включение режима домена. Server Address: ввод адреса сервера. Server Port: ввод порта сервера. Display Name: отображение имени сервера. User Name: ввод имени пользователя сервера. Verify ID: ввод идентификатора верификации сервера. Password: ввод пароля сервера. Transport Protocol: установка транспортного протокола между устройством и внутренним абонентским устройством.
	Порт устройства	При использовании локальной сети для видеодомофона введите номер порта локальной сети.
	Тип устройства	Можно установить тип устройства как устройство входа, контроллер доступа или ограждающее устройство.
	Локальная информация	Информация о домовладельце, к которому относится устройство, включая здание, корпус, этаж и офис.
	Транспортный протокол	Установка транспортного протокола между устройством и внутренним абонентским устройством.

Варианты вызова	Задержки вызова	Установите время задержки вызова (от 30 до 60 секунд).
	Задержки разговора	Установите продолжительность разговора в диапазоне от 60 до 120 секунд.
	Настройки громкости вызова	Установите громкость звонка (от 0 до 100).
	Тип вызова	Установите тип звонка: звонок или звонок + видео.
	Стиль кнопки вызова	Изменение отображения кнопки вызова на экране видеодомофона в режиме ожидания (значки дверного звонка  и телефона  дополнительно)
	Настройки автоответчика	Когда внутреннее абонентское устройство успешно осуществляет дозвон до устройства, происходит автоматическое соединение в течение установленного времени ответа.
	Шифрование	Включение/выключение функции шифрования передачи данных по видеодомофону.
Список контактов	Когда SIP-сервер отключен, вы можете добавить номер устройства адрес вызова внутреннего абонентского устройства.	
Настройки быстрого вызова	Возможность установки до 5 "горячих" кнопок быстрого вызова на экране видеодомофона (кнопка вызова центра управления и еще 4 настраиваемые "горячие" кнопки. После включения функции настройте имя, введите номер устройства из списка контактов, выполните автоматическую проверку IP-адреса, и после завершения операции нажмите на созданный ярлык на экране видеодомофона для прямого дозвона. Поддержка стандартного режима и режима прямого вызова; в последнем режиме пользователи могут осуществлять вызов на несколько внутренних абонентских устройств одновременно. <i>Примечание: Когда SIP-сервер включен, в режиме прямого вызова можно совершать звонки только в Центр управления</i>	
Расширенные настройки	Установите тип передачи и значение DTMF устройства, при этом настройки DTMF на устройстве и внутреннем абонентском устройстве должны быть одинаковы.	

9.1.1 Подключение к SIP-серверу

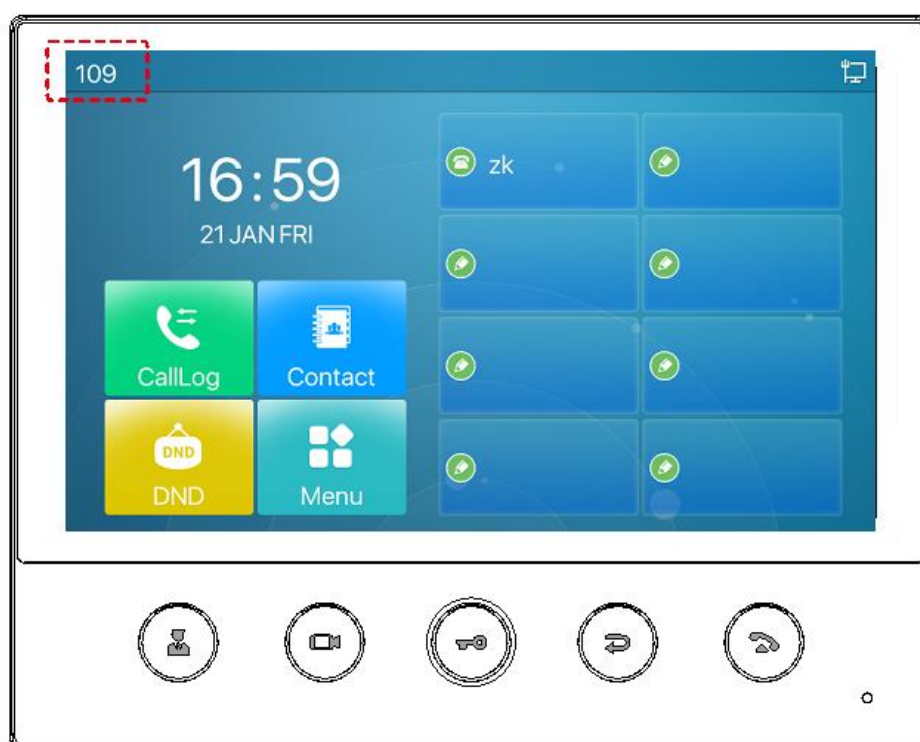
Примечание: Когда SIP-сервер включен, рекомендуется сначала выбрать режим TCP, а затем режим UDP, так как первый более надежен. Если эта функция включена, список контактов не отображается.

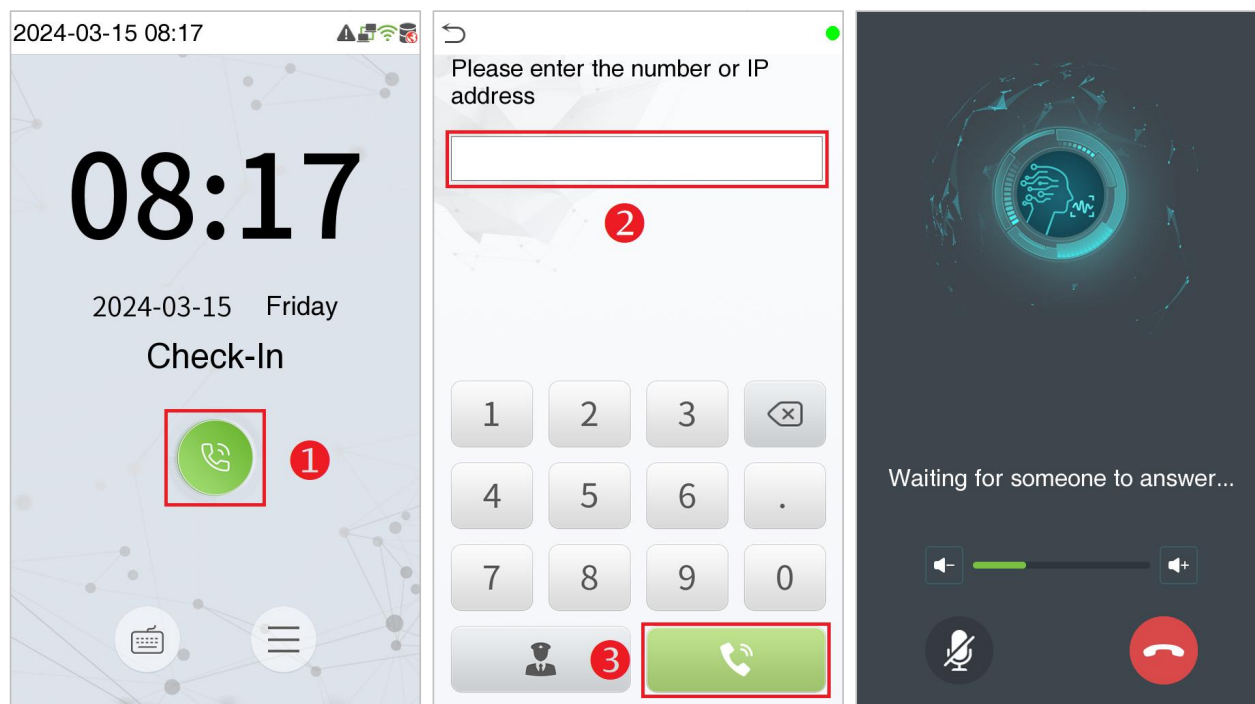
Нажмите **SIP Settings (Настройки SIP) > Local Settings (Местные настройки)** в меню параметров видеодомофона для перехода к настройке параметров.



1. При использовании устройства SenseFace7 нажмите **Local Settings** в меню SIP настроек и после перезагрузки устройства установите параметры сервера.
2. После правильной настройки SIP в правом верхнем углу страницы вызова появится зеленая точка, указывающая на то, что устройство SpeedFace7 подключено к серверу. Вы можете сделать вызов на внутреннее абонентское устройство.

Примечание: если пользователи хотят использовать SIP-сервер, они должны приобрести адрес и пароль сервера у дистрибьютора или создать сервер самостоятельно.



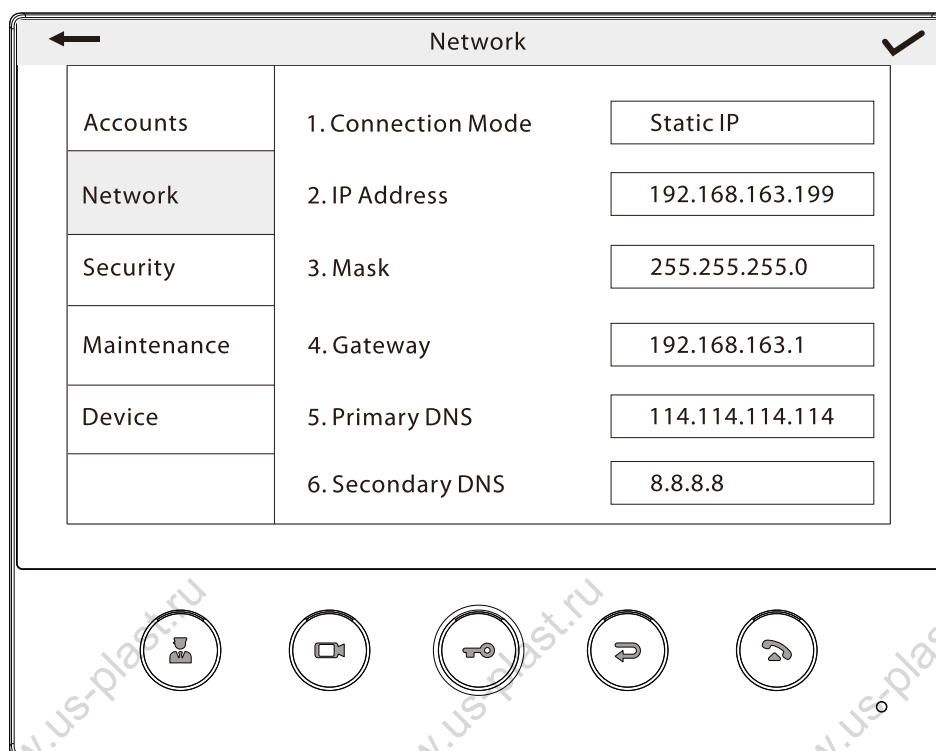


С подробной информацией о работе и использовании внутренней станции можно ознакомиться в руководстве пользователя на нее.

9.1.2 Использование локальной сети

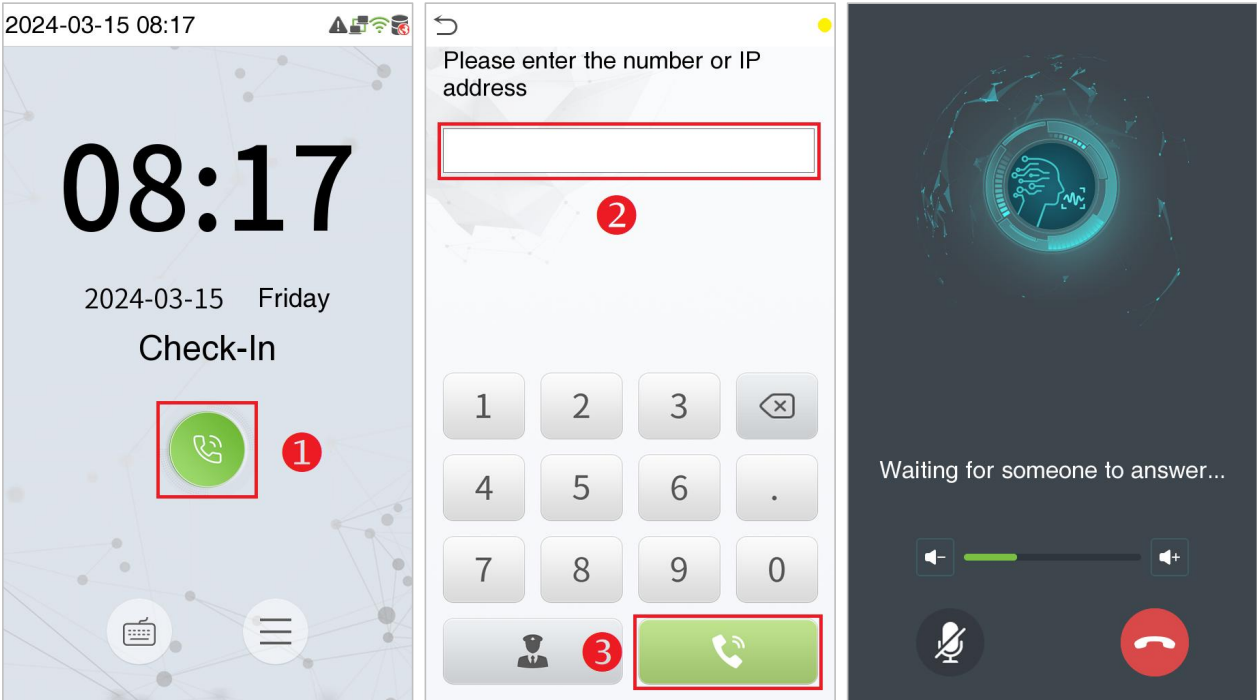
Примечание: для использования «горячих» клавиш и режима прямого вызова выключите SIP-сервер. Если SIP-сервер отключен и используется LAN, сначала выбирается режим UDP.

Установите IP-адрес внутреннего абонентского устройства и нажмите **Menu > Advanced > Network > 1. Network > 1. IPv4**.



● **Ввод IP-адреса внутренней станции напрямую**

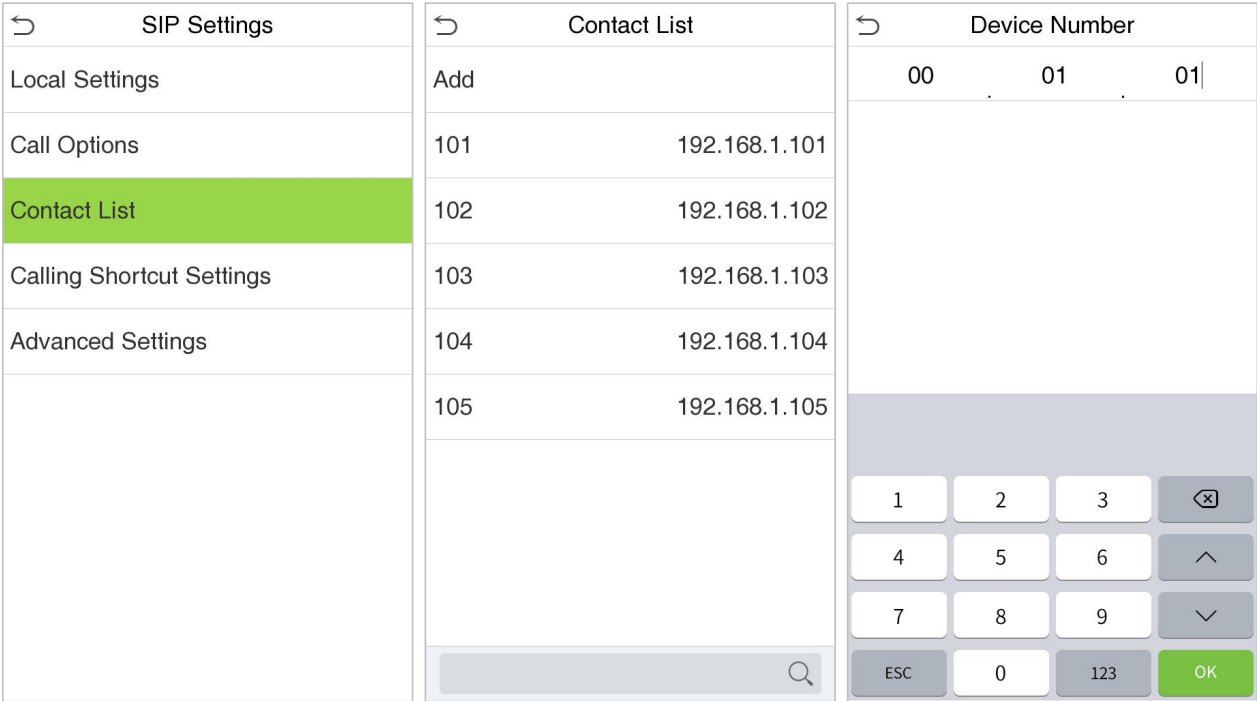
После того как настроены сетевые параметры внутренней станции, для использования видеодомофона нажмите на соответствующую иконку  на экране SpeedFace7 и введите IP-адрес внутреннего абонентского устройства в открывшемся окне.



● **Список контактов**

Примечание: когда SIP-сервер включен, список контактов не отображается.

1. Нажмите **SIP Settings (Настройки SIP) > Contact List (Список контактов)** в меню параметров видеодомофона.



2. Нажмите **Add (Добавить)**, введите номер устройства и адрес вызова для добавления нового контакта.

Примечание: Адрес вызова и устройство SpeedFace7 должны находиться в одном сегменте сети.

↩

Add

Device Number

Call Address

Описание функций

Имя функции	Описание
Номер устройства	Это номер набора из параметров конфигурации, который можно ввести на устройстве SpeedFace7 для быстрого вызова внутреннего абонентского устройства с видеодомофона (например, 101 соответствует 00.01.01 в настройках номера устройства).
Адрес для вызова	IP-адрес внутреннего абонентского устройства.

9.1.3 Настройки быстрого вызова

1. На устройстве SpeedFace7 нажмите **Calling Shortcut Settings (Настройки быстрого вызова)**, выберите любой пункт, кроме admin, и введите только что загруженные данные.

↩

Calling Shortcut Se...

Management Center101

Call ModeStandard Mode

ROOM1Enable

ROOM2Enable

ROOM3Enable

ROOM4Enable

↩

Device Number : 0

Enable

NameROOM1

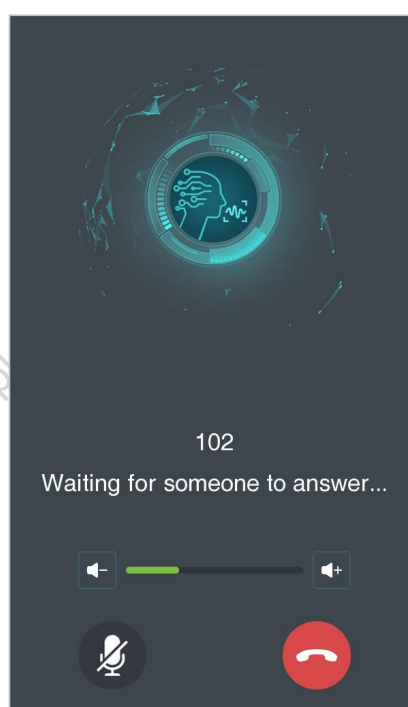
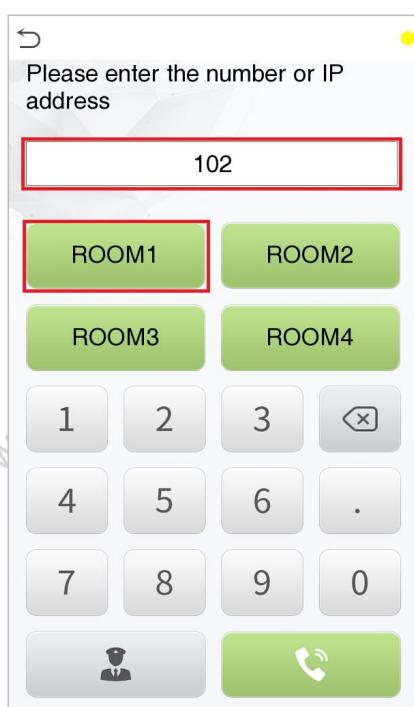
Device Number0

IP Address0.0.0.0

Описание функций

Им функции	Описание
Наименование	Вы можете настраивать любые отображаемые на странице вызова знаки (китайские или английские, цифры, символы и т. д.).
Номер устройства	Это номер набора из параметров конфигурации, который можно ввести на SpeedFace7 для быстрого вызова внутреннего абонентского устройства с видеодомофона.
IP-адрес	Введите номер устройства из Списка контактов и выполните автоматическую проверку IP-адреса.

2. Затем вы можете ввести номер устройства или нажать на соответствующую кнопку быстрого вызова для прямой связи с видеодомофоном.

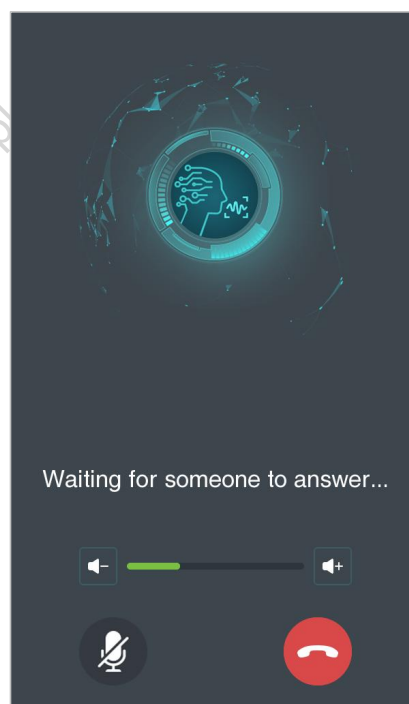
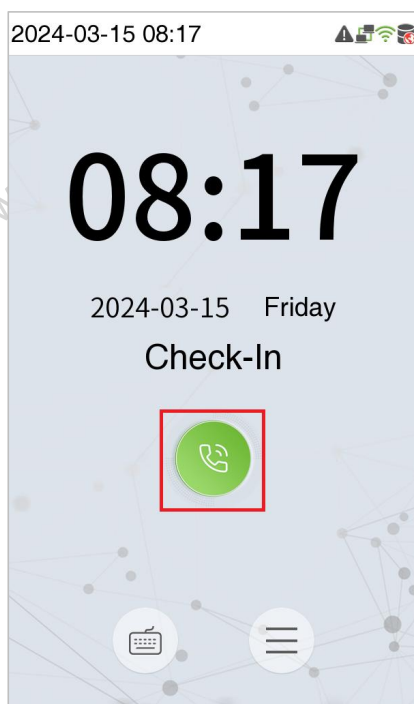


9.1.4 Режим прямого вызова

1. В меню настроек SIP нажмите **Calling Shortcut Settings > Call Mode > Direct Calling Mode > Add**. Выберите IP-адреса внутренних абонентских устройств, на которые вы хотите позвонить, и они отобразятся в списке.

← SIP Settings	← Calling Shortcut Se...	← Calling Shortcut Se...
Local Settings	Management Center 101	☒ Standard Mode
Call Options	Call Mode Standard Mode	☐ Direct Calling Mode
Contact List	ROOM1 Enable	
Calling Shortcut Settings	ROOM2 Enable	
Advanced Settings	ROOM3 Enable	
	ROOM4 Enable	

2. Затем нажмите  на устройстве для одновременного вызова внутренних абонентских устройств.



9.2 Настройки дверного звонка

Нажмите **Doorbell Setting (Настройки дверного звонка)** на странице параметров видеодомофона для перехода к настройкам дверного замка.

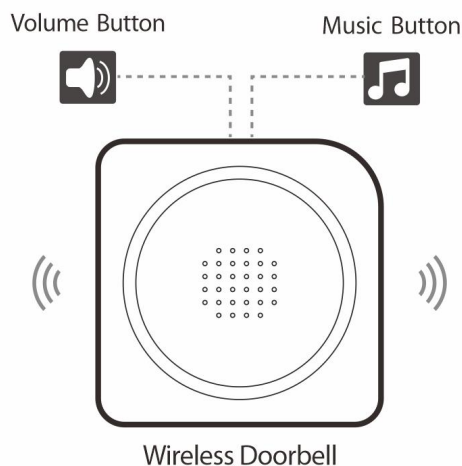
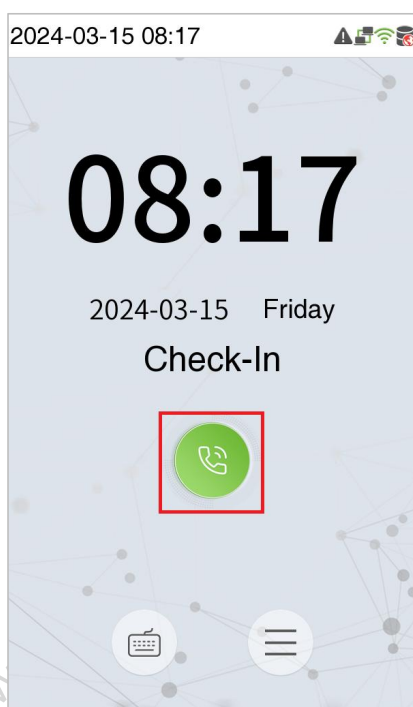
Описание функций

Имя функции	Описание
Только дверной звонок	Нажмите или в меню ожидания, зазвонит звонок.
Только видеодомофон	Нажмите или в меню ожидания для осуществления вызова абонентского устройства в режиме видеодомофона.
Дверной звонок + видеодомофон	Нажмите или в меню ожидания, зазвонит дверной звонок и пойдет вызов абонентского устройства в режиме видеодомофона.

9.2.1 Подключение беспроводного дверного звонка ★

Примечание: эта функция работает в паре с беспроводным дверным звонком.

1. Подайте питание на беспроводной дверной звонок, после чего нажмите и удерживайте кнопку музыки в течение 1,5 секунд, пока не начнет мигать индикатор, информируя пользователя о входе в режим сопряжения. Затем нажмите на устройстве SenseFace7; если дверной звонок звонит и индикатор мигает, соединение успешно установлено.



2. После сопряжения каждый раз при нажатии  устройстве SenseFace 4 будет звучать беспроводной дверной звонок.

Примечание: как правило, каждое устройство из серии SenseFace7 подключается к беспроводному дверному звонку.

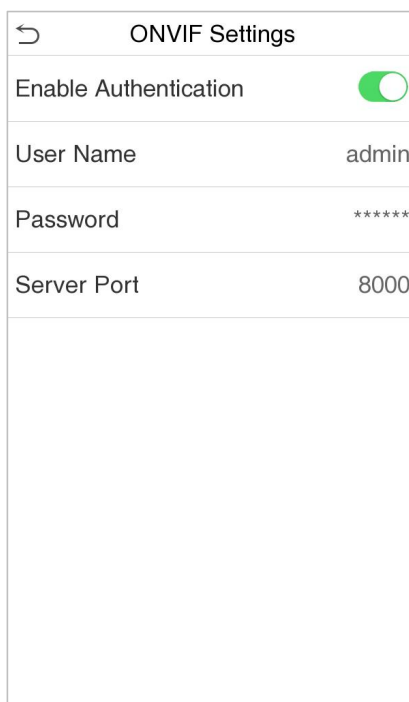
● Отмена сопряжения с беспроводным дверным звонком

Отключите питание дверного звонка, затем снимите и установите батареи, при этом удерживая кнопку музыки  нажатой до тех пор, пока не загорится индикатор, информируя пользователя о том, что сопряжение отменено.

9.3 Настройки ONVIF

Примечание: эта функция работает в паре с сетевым видеорегистратором (NVR).

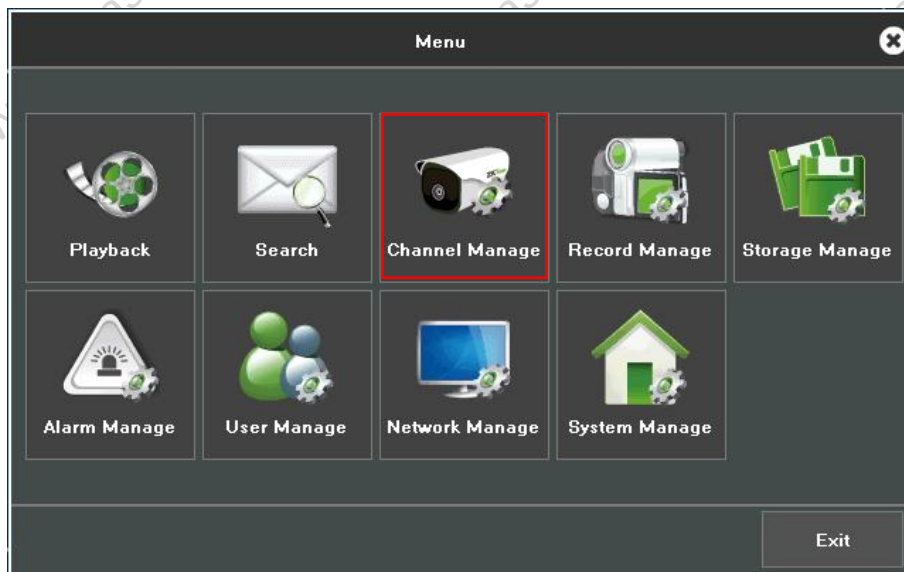
1. Установите устройство в том же сегменте сети, что и NVR.
2. Нажмите **ONVIF Settings (Настройки ONVIF)** на странице параметров видеодомофона.



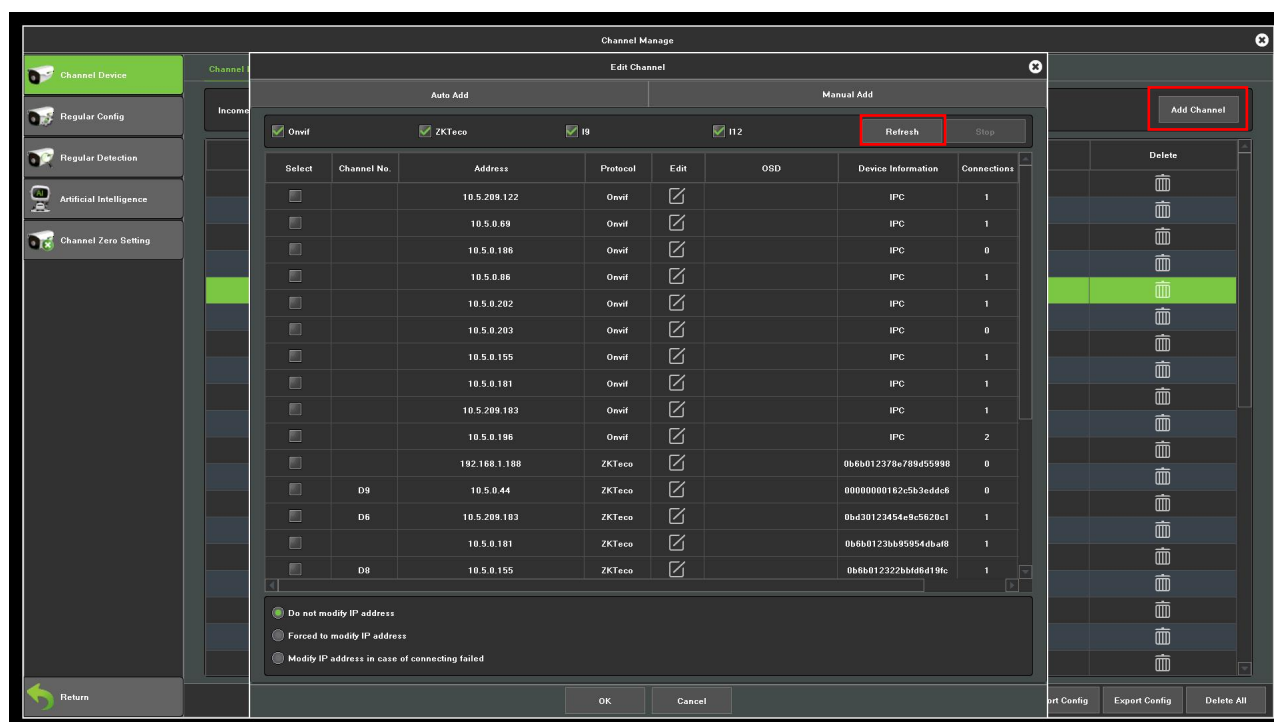
Описание функций

Имя	Description
Включить проверку аутентификации	Включение/выключение функции аутентификации. Если функция отключена, нет необходимости вводить имя и пароль пользователя при добавлении устройства в NVR.
Имя пользователя	Установка имени пользователя. По умолчанию - admin.
Пароль	Установка пароля пользователя. По умолчанию – admin.
Порт сервера	8000 по умолчанию и не может быть изменен.

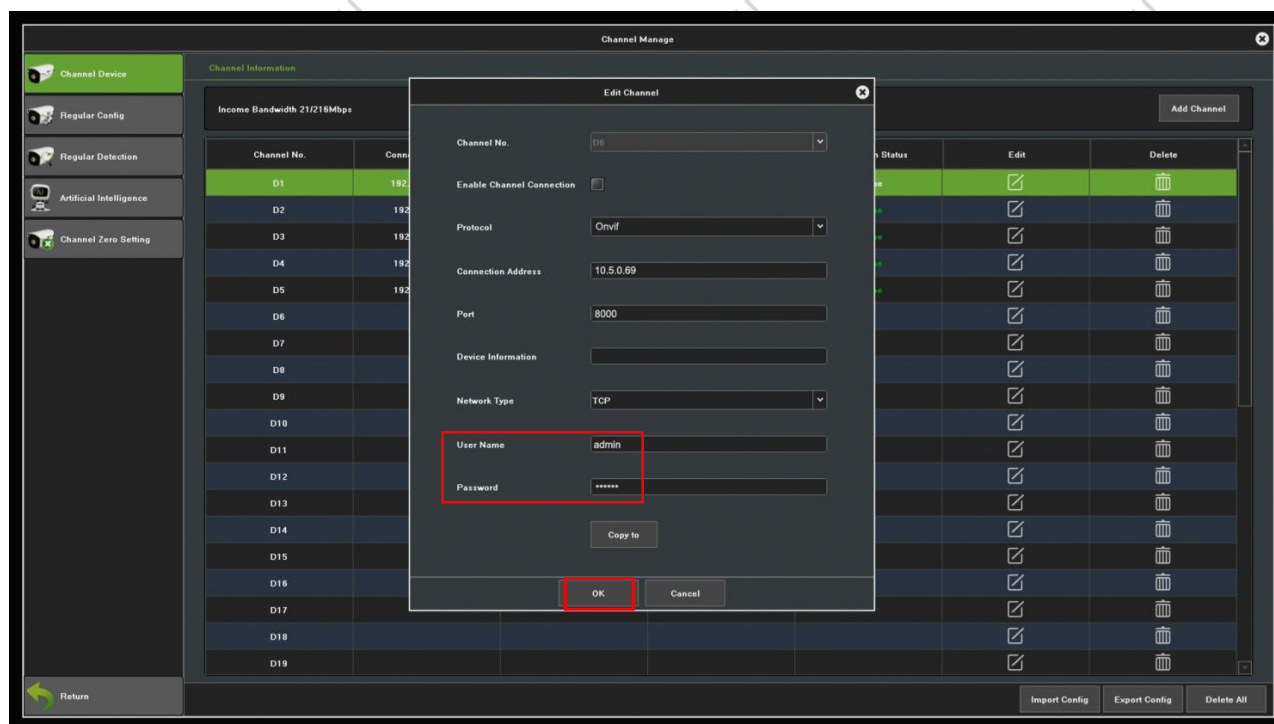
3. В меню NVR нажмите **[Start] > [Menu]**, после чего откроется главное меню.



4. Нажмите **[Channel Manage] > [Add Channel] > [Refresh]** для поиска устройства.

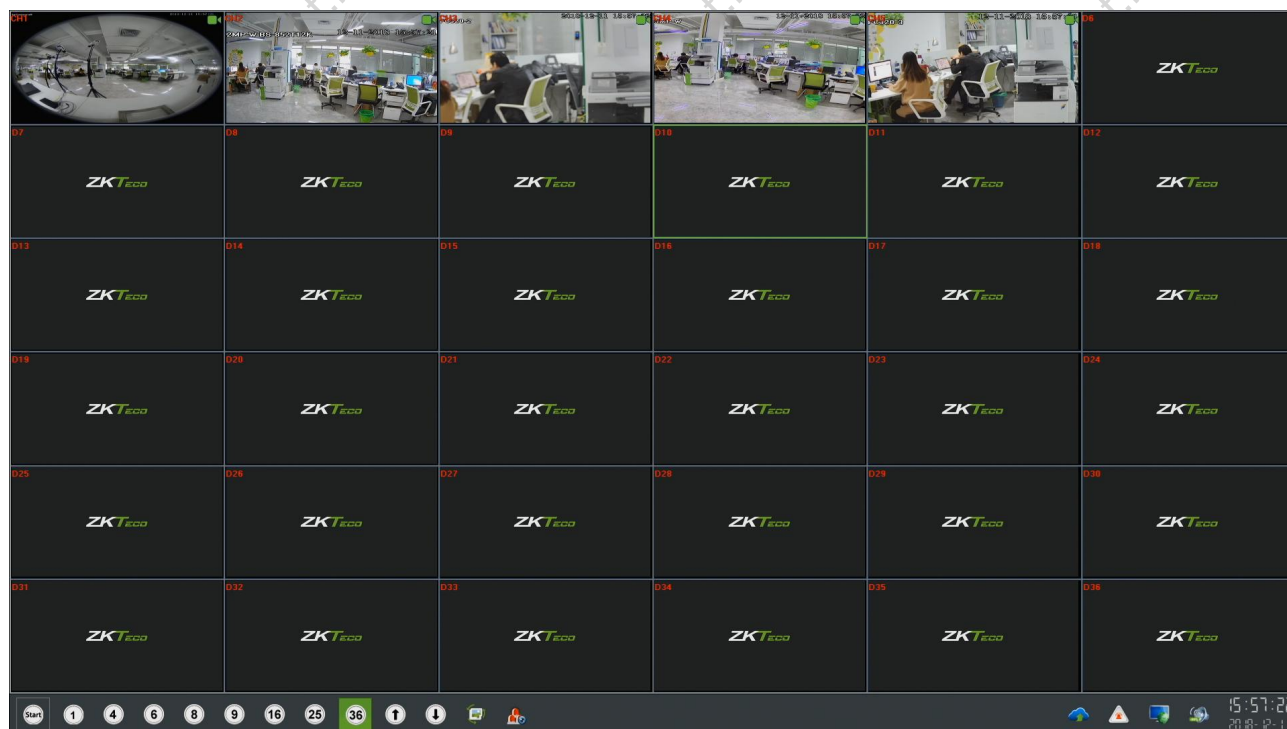


5. Отметьте поле напротив устройства, которое вы хотите добавить и отредактируйте параметры в соответствующем текстовом поле, затем нажмите **[OK]** для добавления устройства с список соединений.



Примечание: Имя и пароль пользователя устанавливаются в настройках ONVIF устройства.

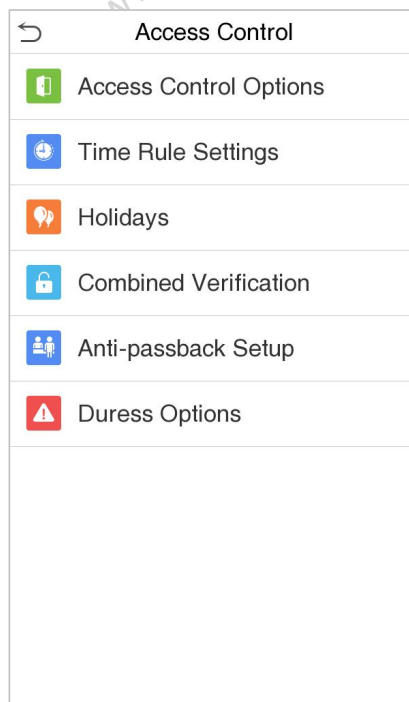
6. После добавления видеоизображение, получаемое с устройства, можно просматривать в режиме реального времени.



Более подробная информация в руководстве пользователя на NVR.

10. Управление доступом

В главном меню нажмите **Access Control (Управление доступом)** для установки расписания открытия двери, управления замками и настройки иных параметров контроля доступа.



- **Для получения доступа зарегистрированный пользователь должен соответствовать следующим требованиям:**
 - Текущее время открытия двери должно быть в пределах времени разрешенного доступа для пользователя.
 - Группа доступа, в которую входит пользователь, должна уже быть включена в комбинацию разблокировки двери (если есть другие группы, включенные в ту же комбинацию разблокировки, потребуется также верификация членов такой группы для разблокировки двери).
 - В настройках по умолчанию новые пользователи зачисляются в первую группу с периодом разрешенного доступа по умолчанию, где комбинация доступа - "1" и установлена в разблокированном состоянии по умолчанию.

10.1 Параметры контроля доступа

Нажмите **Access Control Options (Параметры контроля доступа)** в меню Access Control для установки параметров управления замком устройства и связанного с ним оборудования.

← Access Control Opti... 1↓	← Access Control Opti... 1↓
Gate Control Mode ☐	Door Sensor Type Normal Close(NC)
Door Lock Delay(s) 5	Verification Mode Password/Fingerprint/Card/Face
Door Sensor Delay(s) 10	Door Available Time Period 1
Door Sensor Type Normal Close(NC)	Normal Open Time Period None
Verification Mode Password/Fingerprint/Card/Face	Master Device In
Door Available Time Period 1	Slave Device Out
Normal Open Time Period None	Auxiliary Input Configuration
Master Device In	Verify Mode by RS485 Card Only
Slave Device Out	Speaker Alarm ☐
Auxiliary Input Configuration	Reset Access Settings

Описание функций

Имя функции	Описание
Режим управления дверью	Включение/выключение режима управления дверью. Если режим активирован, происходит удаление настроек реле дверного замка, реле датчика двери и типа датчика двери.
Задержка замка двери (сек.)	Продолжительность времени, в течение которого электрический замок будет находиться в открытом положении. Допустимый диапазон: 1~10 секунд, где 0 – отключение функции.
Задержка датчика двери (сек.)	Если дверь находится в открытом положении более установленного времени (задержка датчика двери), срабатывает тревожная сигнализация. Диапазон времени задержки срабатывания датчика двери: от 1 до 255 сек.
Тип датчика двери	3 варианта: Отсутствует, Нормально-открытый и Нормально-закрытый. None: датчик двери не используется. Normal Open: дверь всегда открыта при включении питания. Normal Closed: дверь всегда закрыта при включенном питании.
Режим верификации	Поддерживаемые способы верификации включают: Пароль/Отпечаток пальца/Карта/Лицо, только Отпечаток пальца, только ID пользователя, Пароль, только Карта, Отпечаток пальца/Пароль, Отпечаток пальца/Карта, ID пользователя + Отпечаток пальца, Отпечаток пальца + Пароль, Отпечаток пальца + Карта, Отпечаток пальца + Пароль + Карта, Пароль+Карта, Пароль/Карта, ID пользователя + Отпечаток пальца + Пароль, Отпечаток пальца + (Карта/ID пользователя), Только Лицо, Лицо + Отпечаток пальца, Лицо + Пароль, Лицо + Карта, Лицо + Отпечаток пальца + Карта и Лицо + Отпечаток пальца + Пароль.

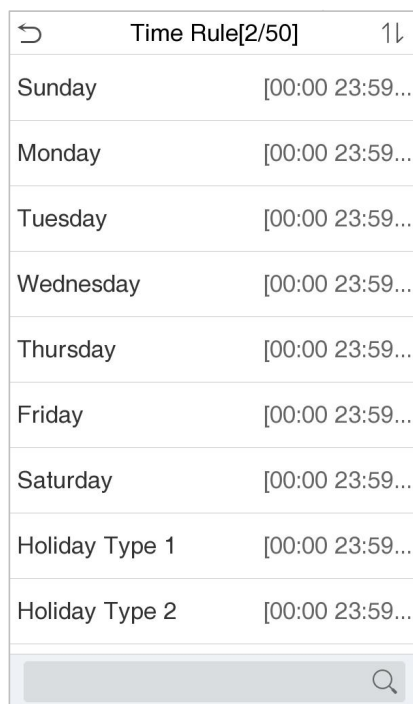
Период времени доступа к двери	Установка периода времени, в течение которого будет доступ к двери.
Период времени режима нормально-открытый	Установить период времени для работы двери в нормально открытом режиме, в течение которого дверь будет все время открыта.
Главное устройство	При настройке главного устройства оно может быть установлено на выход или вход. Out: записью, подтвержденной на главном устройстве, будет запись выхода. In: записью, подтвержденной на главном устройстве, будет запись входа.
Дополнительное устройство	При настройке подчиненного устройства оно может быть установлено на выход или вход. Out: записью, подтвержденной на подчиненном устройстве, будет запись выхода. In: записью, подтвержденной на подчиненном устройстве, будет запись входа.
Конфигурация дополнительного входа	Установка периода разблокировки двери и типа дополнительного выхода резервного терминала. Типы дополнительных выходов: "Отсутствует", "Открыть дверь", "Включить сигнализацию" и "Открыть дверь и включить сигнализацию".
Проверка режима по RS485	Данный способ верификации применяется в тех случаях, когда устройство используется как главное или подчиненное. Поддерживаемые способы верификации: только Карта и Карта + Пароль..
Сигнализация динамика	Включение/отключение звуковой сигнализации. При закрытии двери или успешной идентификации пользователя система отключит сигнализацию.
Сброс настроек контроля доступа	Возможен сброс следующих параметров контроля доступа: задержки срабатывания дверного замка и дверного датчика, типа датчика двери, способа верификации, времени доступа к двери, времени работы в нормально открытом режиме, главного устройства и сигнализации; удаленные данные контроля доступа в Data Mgt. не восстанавливаются.

10.2 Настройка правила времени

Нажмите **Time Rule Setting (Настройка правила времени)** в меню Access Control для настройки времени.

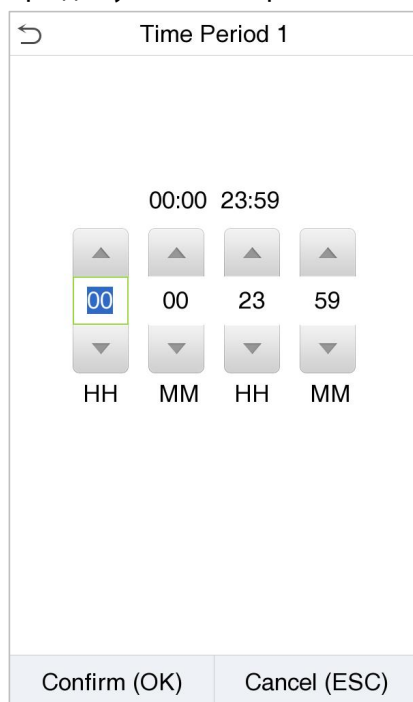
- Система может определять до 50 периодов времени.
- Каждый период времени представляет 10 зон с программируемым временем доступа, т.е. 1 рабочую неделю и 3 выходных дня; при этом каждая из таких зон представлена в стандартном формате 24-часового дня; пользователь может пройти верификацию лишь в пределах времени разрешенного доступа.
- Можно установить не более 3 временных промежутков для каждой зоны. Логические отношения между этими промежутками - "ИЛИ". Таким образом, верификация пользователей для получения доступа может быть успешной, только когда время верификации находится в пределах одного из таких периодов.
- Зона разрешенного доступа любого из периодов времени представлена в формате ЧЧ ММ-ЧЧ ММ, с точностью до минут в 24-часовом формате.

Коснитесь подсвеченного серым поля для поиска нужной программируемой зоны и введите номер нужной вам зоны (до 50 зон).



Time Rule[2/50]	
Sunday	[00:00 23:59...]
Monday	[00:00 23:59...]
Tuesday	[00:00 23:59...]
Wednesday	[00:00 23:59...]
Thursday	[00:00 23:59...]
Friday	[00:00 23:59...]
Saturday	[00:00 23:59...]
Holiday Type 1	[00:00 23:59...]
Holiday Type 2	[00:00 23:59...]

На странице выбранной зоны разрешенного времени доступа выберите соответствующий день недели (понедельник, вторник и пр.) для установки времени.



Time Period 1			
00:00 23:59			
▲	▲	▲	▲
00	00	23	59
▼	▼	▼	▼
HH	MM	HH	MM
Confirm (OK)		Cancel (ESC)	

Укажите время начала и окончания и нажмите **ОК**.

Примечание:

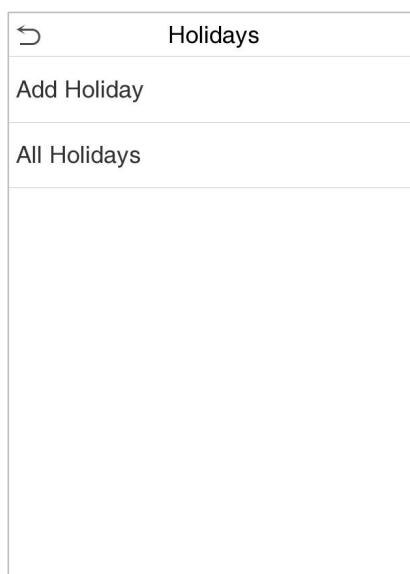
- Если время окончания предшествует времени начала (например, 23:57~23:56), доступ к двери будет запрещен в течение всего дня.
- Если время окончания следует за временем начала (например, 00:00~23:59), интервал времени указан правильно.

- Примерами корректного указания периода времени могут быть – 00:00~23:59 (доступ к двери имеется в течение всего дня) и 08:00~23:59 (т.е. когда время окончания следует за временем начала).
- Установленная по умолчанию зона разрешенного времени доступа №1 означает, что к двери имеется круглосуточный доступ.

10.3 Выходные и праздничные дни

Если необходимо разрешить доступ к двери в определенное время в выходные дни, предоставление такого разрешения каждому сотруднику может быть крайне затруднительным. В этой связи можно установить время разрешенного доступа в выходной день для всех сотрудников.

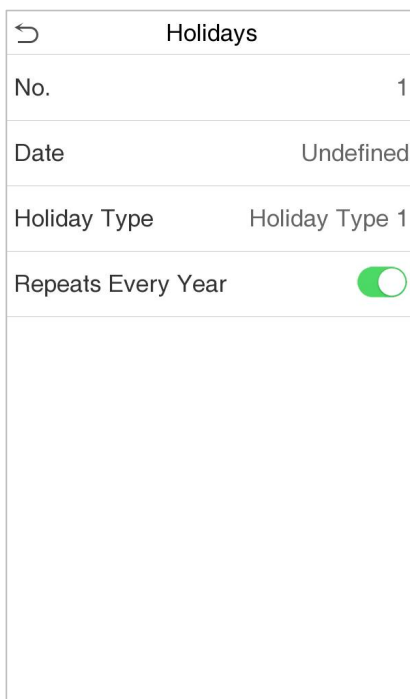
Нажмите **Holidays (Праздники)** в меню Access Control для установки доступа в выходной день.



Holidays	
Add Holiday	
All Holidays	

- **Добавить новый выходной (праздничный) день:**

Нажмите **Add Holiday (Добавить праздник)** на странице Holidays (Праздники) и установите желаемые параметры.



Holidays	
No.	1
Date	Undefined
Holiday Type	Holiday Type 1
Repeats Every Year	☒

- **Редактировать выходной (праздничный) день:**

В меню Holidays выберите пункт, который вы хотите изменить. Нажмите **Edit (Редактировать)**, чтобы выполнить редактирование.

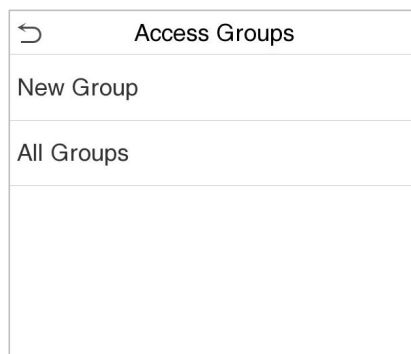
- **Удалить выходной (праздничный) день:**

В меню Holidays выберите пункт, который Вы хотите удалить, и нажмите **Delete (Удалить)**. Нажмите **OK** для подтверждения удаления. После удаления это нерабочее время не будет отображаться на странице All Holidays (Все праздники).

10.4 Группы доступа ★

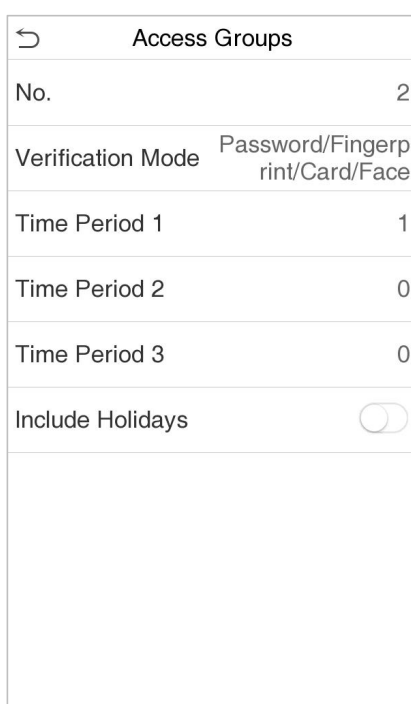
Данная функция обеспечивает удобное управление как группами доступа, так и отдельными пользователями, входящими в группы. Настройки группы доступа, например, зоны с программируемым временем доступа, по умолчанию применяются ко всем членам группы. Однако по мере необходимости пользователи могут устанавливать такие зоны вручную. В случае конфликта между верификацией пользователя и верификацией группы доступа приоритет будет иметь первая. Для одной группы доступа можно установить не более трех зон разрешенного времени доступа. По умолчанию новые зарегистрированные пользователи зачисляются в группу доступа 1; но могут быть переведены в другие группы доступа.

Нажмите **Access Groups (Группы доступа)** в меню Access Control.



- **Добавить новую группу**

Нажмите New Group (Новая группа) в меню Access Groups и установите параметры группы доступа.



Примечания:

- Эта функция используется только с протоколом T&A PUSH.
- По умолчанию назначается группа доступа 1; эта группа не удаляется, но может быть изменена.
- Номер группы не может быть изменен после того как был установлен.
- Если установлен режим выходного дня, то сотрудники из той или иной группы доступа могут открыть дверь только в том случае, если установленное для группы пользователей время разрешенного доступа к двери совпадает с выходным днем.

Если режим выходного дня не установлен, то это никак не влияет на права доступа к двери для членов группы доступа.

10.5 Комбинированная верификация

Группы доступа организованы в различных комбинациях разблокировки двери для целей повышения безопасности. В любой комбинации разблокировки дверей количество пользователей, входящих в группу доступа (N) -- $0 \leq N \leq 5$, и все они могут принадлежать к одной группе доступа или пяти разным группам доступа.

Нажмите **Combined Verification (Комбинированная верификация)** в меню Access Control.

↶	Combined Verification	1↴
1	01 00 00 00 00	
2	00 00 00 00 00	
3	00 00 00 00 00	
4	00 00 00 00 00	
5	00 00 00 00 00	
6	00 00 00 00 00	
7	00 00 00 00 00	
8	00 00 00 00 00	
9	00 00 00 00 00	
Q		

В меню комбинированной верификации выберите комбинацию разблокировки двери, которую вы хотите установить, и с помощью стрелок "up" и "down" установите нужные цифры в ней, после чего нажмите **ОК**.

Например:

- Если **комбинация разблокировки двери 1** установлена как **(01 03 05 06 08)**, это значит, что эта комбинация состоит из 5 человек, и все они из 5 разных групп доступа, а именно: **Группа КД 1, Группа КД 3, Группа КД 5, Группа КД 6 и Группа КД 8, соответственно.**

- Если **комбинация разблокировки двери 2** установлена как **(02 02 04 04 07)**, это значит, что эта комбинация состоит из 5 человек; первые двое из Группы КД 2, следующие двое из Групп КД 4, а последний Группы КД 7.
- Если **комбинация разблокировки двери 3** установлена как **(09 09 09 09 09)**, это значит, что эта комбинация состоит из 5 человек, все из которых из Группы КД 9.
- Если **комбинация разблокировки двери 4** установлена как **(03 05 08 00 00)**, это значит, что в этой комбинации только 3 человека. Первый - из Группы КД 3, второй - из Группы КД 5, а последний - из Группы КД 8.

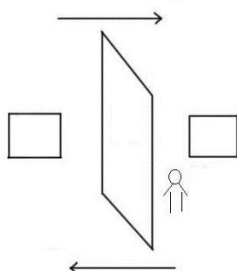
- **Удаление комбинации разблокировки двери:**

Введите «0» в каждой цифровой ячейку комбинации для ее удаления.

10.6 Настройка запрета двойного прохода

Чтобы исключить возможность прохода некоторых людей, следующих непосредственно за пользователями, без верификации, что приводит к проблемам с безопасностью, в устройстве реализована функция запрета двойного прохода. Если она активирована, проход будет разрешен только при совпадении записей входа и выхода.

Для работы запрета двойного прохода два устройства должны работать вместе: одно – установленное с внутренней стороны двери (главное устройство), и второе – снаружи двери (подчиненное устройство). Связь между ними осуществляется через сигнал Wiegand. Формат Wiegand и тип выхода (ID пользователя/номер карты), принятые главным и подчиненным устройствами, должны быть сонастроены.



Нажмите **Anti-passback Setup (Настройка запрета двойного прохода)** в меню Access Control.

Anti-passback Setup	
Anti-passback Direction	No Anti-passback

Описание функций

Имя функции	Описание
Контроль прохода в обоих направлениях	No Anti-passback: запрет двойного прохода отключен, т.е. для разблокировки двери достаточно пройти верификацию на главном или подчиненном устройстве. Записи учета рабочего времени при этом не сохраняются. Out Anti-passback: дверь разблокируется на выход только при условии, что последней записью пользователя была запись на вход, в противном случае сработает сигнализация. Ограничений на вход при этом нет. In Anti-passback: дверь разблокируется на вход только при условии, что последней записью пользователя была запись на выход, в противном случае включится сигнализация. При этом, ограничений на выход нет. In/Out Anti-passback: пользователь может войти, только если его последняя запись была регистрация на выход, или выйти, если последняя запись была регистрация на вход, в противном случае сработает сигнализация.

10.7 Настройки тревоги принуждения

Если активирована функция срабатывания тревоги под принуждением при верификации пользователя одним из доступных способов, устройство разблокирует дверь в случае успешной верификации пользователя соответствующим способом, но при этом подаст сигнал тревоги.

В меню **Access Control** нажмите **Duress Options (Настройки тревоги принуждения)**.

Duress Options	
Alarm on Password	☐
Alarm on 1:1 Match	☐
Alarm on 1:N Match	☐
Alarm Delay(s)	10
Duress Password	None

Описание функций

Имя функции	Описание
Тревога по паролю	При выборе верификации по паролю как верификации под принуждением тревога будет срабатывать при вводе пароля.

Сигнал тревоги в режиме 1:1	Тревожная сигнализация сработает после того, как пользователь приложит палец к сканеру при верификации по отпечатку пальца в режиме 1:1.
Сигнал тревоги в режиме 1:N	Если пользователь использует любой отпечаток пальца для верификации методом сравнения 1:N, генерируется сигнал тревоги, в противном случае сигнализация не сработает.
Задержка срабатывания сигнализации	Тревожная сигнализация сработает только после истечения определенного времени. Доступные значения от 1 до 999 секунд.
Пароль принуждения	Установите 6-значный пароль принуждения. При вводе этого пароля при верификации будет срабатывать тревожная сигнализация.

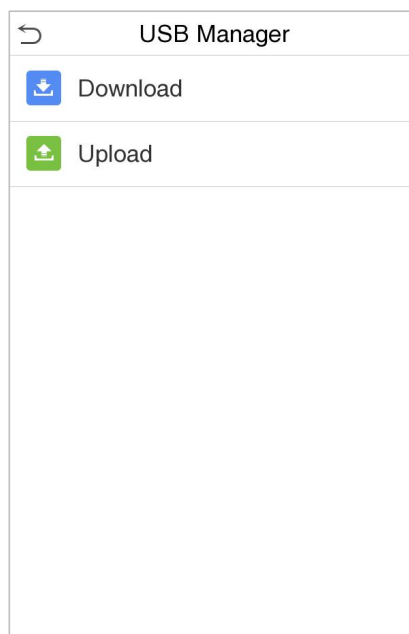
11. USB-менеджер

Вы можете импортировать данные пользователей и учета рабочего времени для их обработки или копирования на терминал или иные устройства с USB-носителя.

Перед загрузкой или скачиванием данных на/с USB-диска, вставьте его в соответствующий порт.

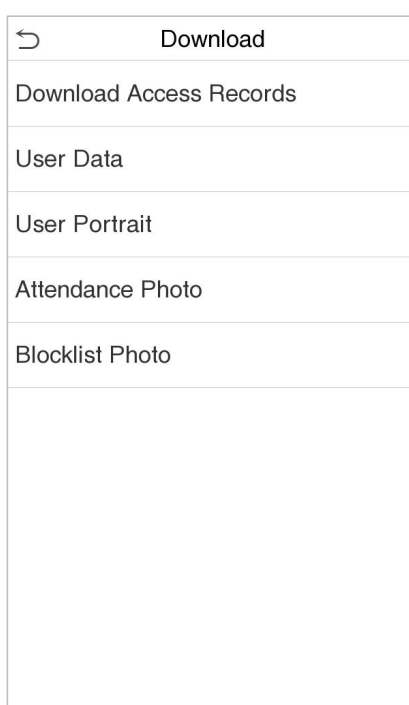
Примечание: загрузка данных с USB-диска возможна только в формате FAT32..

Нажмите **USB Manager** на странице главного меню.



11.1 Выгрузка данных на USB

Нажмите **Download (Загрузить)** в меню USB Manager.

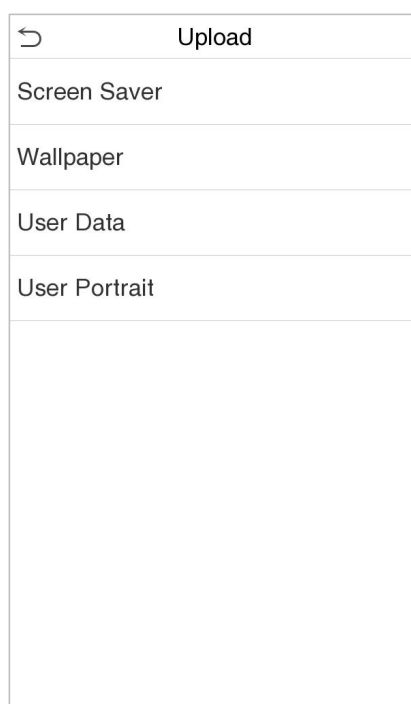


Описание функций

Имя функции	Описание
Загрузка записей доступа	Выгрузить все записи событий доступа за установленный период на USB-накопитель.
Данные пользователя	Выгрузить все данные пользователей из устройства на USB-накопитель.
Фотографии пользователя	Выгрузить все фото профиля пользователя из устройства на USB-носитель.
Фотографии участника	Выгрузить все фото пользователя с устройства на USB-носитель.
Фотографии из черного списка	Скачать все фото из списка блокировок (фото, сделанные при отказах в верификации) с устройства на USB-накопитель.

11.2 Загрузка данных с USB

Нажмите **Download (Загрузить)** в меню USB Manager.



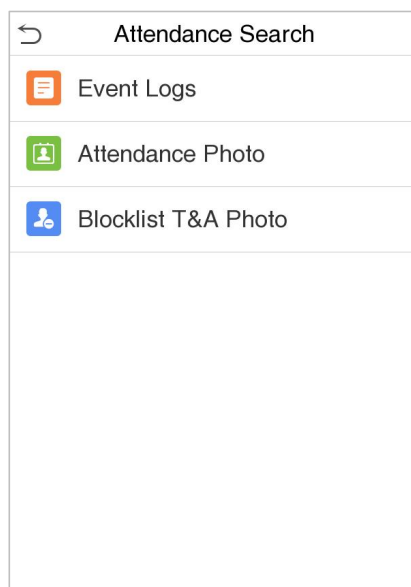
Описание функций

Имя функции	Описание
Экранная заставка	Скачать все заставки экрана с USB-накопителя в устройство. Перед загрузкой можно выбрать одну из двух опций: "Upload selected picture" (Загрузка выбранной заставки) или "Upload all pictures" (Загрузить все).
Обои	Загрузить обои с USB-накопителя в устройство. Перед загрузкой выберите "Upload selected wallpapers" (Загрузка выбранных обоев) или "Upload all wallpapers" (Загрузка всех обоев). Обои будут отображаться на экране после скачивания.
Данные пользователя	Загрузить все пользовательские данные с USB-накопителя в устройство.
Фотографии пользователя	Загрузить все пользовательские фото с USB-накопителя в устройство.

12. Поиск событий учета рабочего времени

После верификации личности пользователя запись события сохраняется в память устройства. Эта функция позволяет пользователям просматривать свои записи доступа.

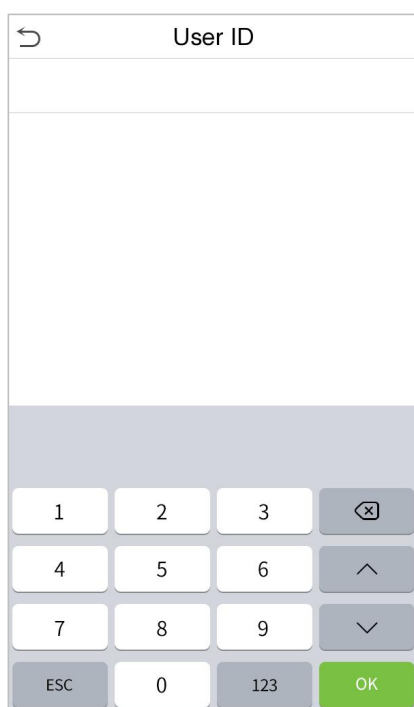
Выберите **Attendance Search (Поиск событий учета рабочего времени)** на странице главного меню для поиска нужных записей событий доступа/учета рабочего времени.



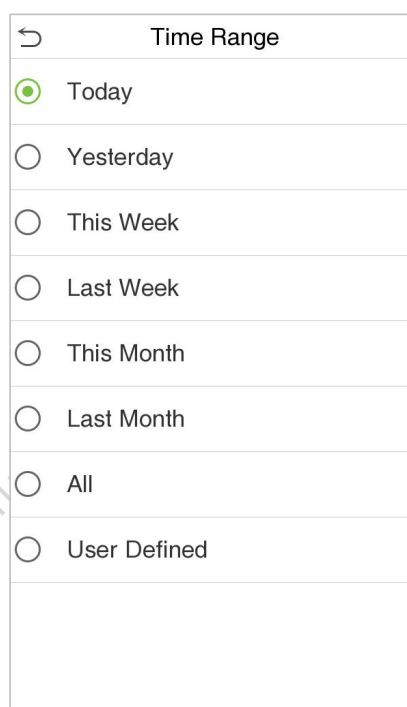
Поиск событий учета рабочего времени и фото из списка блокировок осуществляется аналогично поиску записей журналов событий. Ниже приведен пример поиска записей журналов событий.

В меню Attendance Search нажмите **Event Logs (Журналы событий)** для поиска нужной записи.

1. Введите ID нужного пользователя и нажмите OK. Если Вам нужны записи всех пользователей, нажмите OK без ввода какого-либо ID.



2. Выберите временной интервал, в пределах которого находятся нужные вам записи событий.



3. После того как нужная запись найдена, нажмите на логин, подсвеченный зеленым, для просмотра информации о ней.

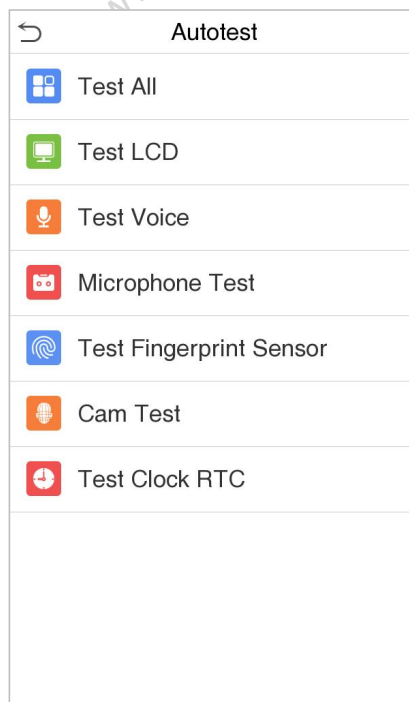
Personal Record S...		
Date	User ID	Time
03-19	Number of Records:7	
	0	09:47 09:47 09:32 09:32
		07:13 07:13 07:13

4. На рисунке показана информация о выбранной записи.

Personal Record S...	
User ID	Time
0	03-19 09:47
0	03-19 09:47
0	03-19 09:32
0	03-19 09:32
0	03-19 07:13
0	03-19 07:13
0	03-19 07:13
Name : Status : Other Verification Mode : Other	

13. Автодиагностика

На странице главного меню нажмите **Autotest (Автодиагностика)** для автоматической проверки исправности всех модулей устройства, в том числе ЖК-экрана, аудиоканала, камеры и часов реального времени (RTC).

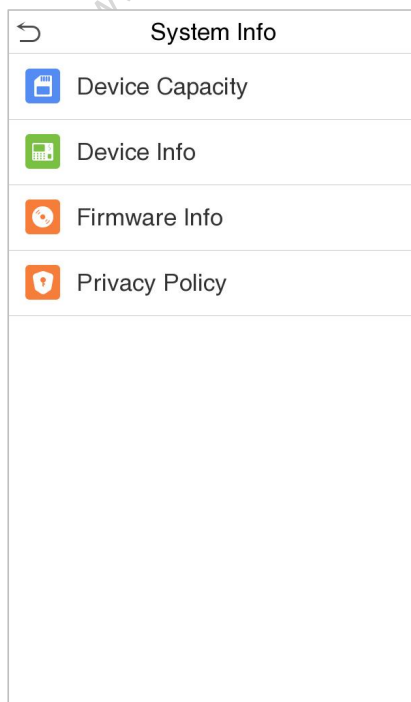


Описание функций

Имя функции	Описание
Тестировать все	Автоматическая диагностика работы ЖК-экрана, аудиоканала, камеры и часов реального времени (RTC).
Тестировать ЖК	Автоматическая проверка качества отображения цветов на ЖК-дисплее посредством вывода на экран тестовых изображений (полноцветного, чисто белого и чисто черного).
Тестировать голос	Автоматическое тестирование аудиофайлов на устройстве и качества записи голоса.
Тестировать микрофон	Автоматическое тестирование исправности микрофона (говорить в микрофон и прослушивать запись).
Тестировать датчик отпечатков пальцев	Проверка четкости получаемого изображения путем прикладывания пальца к зоне сканирования. При нажатии пальцем на сканер изображение отпечатка выводится на экран.
Тестировать камеру	Проверка исправности камеры путем проверки четкости получаемых снимков лиц
Тестировать часы реального времени	Тестирование работы часов реального времени с помощью секундомера. Коснитесь экрана для начала отсчета; повторное нажатие остановит счет.

14. Информация о системе

На странице главного меню нажмите **System Info (Информация о системе)** для просмотра состояния хранилища, версии устройства и информации о прошивке.



Описание функций

Имя функции	Описание
Емкость устройства	Отображает память, где хранятся данные о пользователях текущего устройства, паролях, шаблонах лиц, отпечатках пальцев, картах, записи доступа, фото учета рабочего времени и фото из списка отказов, а также фото профилей пользователей.
Информация об устройстве	Отображает имя устройства, заводской номер, MAC-адрес, алгоритмы отпечатков пальцев и шаблонов лиц, информацию о платформе устройства, версию микроконтроллера, а также дату изготовления.
Информация о прошивке	Отображает версию прошивки и другую информацию о версии устройства.
Политика конфиденциальности	При первом включении устройства на экране появится информация о политике конфиденциальности. Для дальнейшего использования устройства нажмите "I have read it" (Я прочитал). Нажмите System Info (Инфо о системе) > Privacy Policy (Политика конфиденциальности) для просмотра политики конфиденциальности (ее текст не может быть экспортирован на USB-диск). Примечание: текущая редакция политики конфиденциальности доступна только на упрощенном китайском/английском языках. Однако в настоящее время ведется работа по переводу содержимого на другие языки.

15. Подключение к ZKBio CVAccess

15.1 Установка адреса связи

● На устройстве

1. Нажмите **COMM. > Ethernet** в главном меню устройства для установки IP-адреса и шлюза устройства.

Примечание: убедитесь, что IP-адрес находится в том же сегменте сети, что и адрес сервера, и что установлено соединение с ZKBio CVAccessserver.

2. В главном меню нажмите **COMM. > Cloud Server Setting (Настройки облачного сервера)** для установки адреса и порта сервера.

Адрес сервера: установите IP-адрес такой же, как сервера ZKBio CVAccess.

Порт сервера: установите порт сервера такой же, как у ZKBio CVAcc.

Ethernet	
Display in Status Bar	☒
IPv4	
IP Address	192.168.163.199
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	0.0.0.0
DHCP	☐

Cloud Server Settings	
Server Mode	ADMS
Enable Domain Name	☐
Server Address	192.168.163.61
Server Port	8081
Enable Proxy Server	☐

● В программном обеспечении

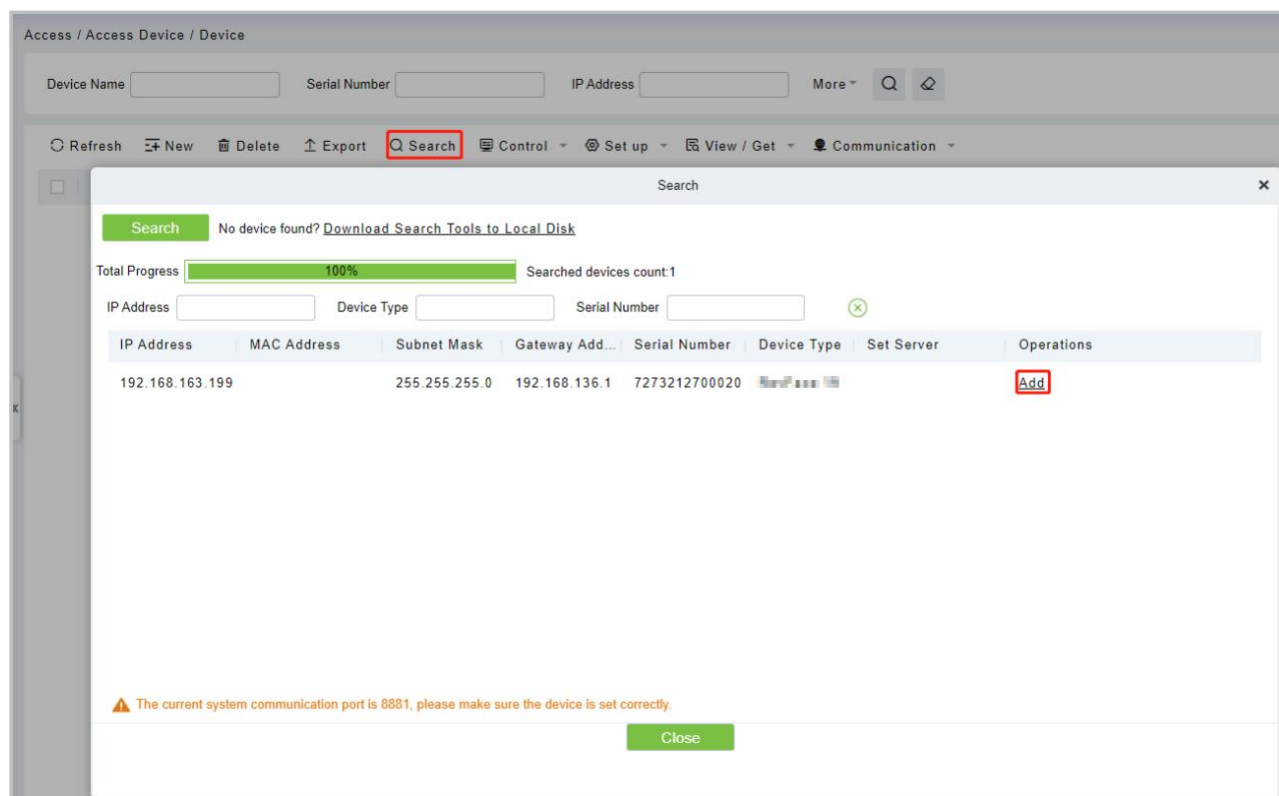
Войдите в приложение ZKBio CVAccess и нажмите **System > Communication > Communication Monitor** для настройки порта службы adms, как показано на рисунке ниже:

Adms Service Settings	
Adms Service Port	8881
⚠ The current port is for device communication service, if there is a network mapping for the service port, please refer to the actual mapped port.	
Project control file version	None
Turn on encrypted transmission	☒ Yes

15.2 Добавление устройства в ПО

Добавьте устройство через поиск. Процедура следующая:

1. Нажмите **Access > Device > Search Device**, чтобы открыть меню поиска.
2. Нажмите **Search (Поиск)** и начнется процесс поиска...
3. После окончания поиска отобразится список и общее количество контроллеров доступа.



4. Нажмите **Add (Добавить)** в столбце Operations, всплывет диалоговое окно Выберите **Icon type (Тип иконки)**, **Area (Область)** и **Add to Level (Добавить в уровень)** из каждого выпадающего списка и нажмите **OK** для добавления устройства.

15.3 Добавление сотрудников в ПО

1. Нажмите **Personnel (Персонал) > Person (Сотрудник) > New (Новый)**:

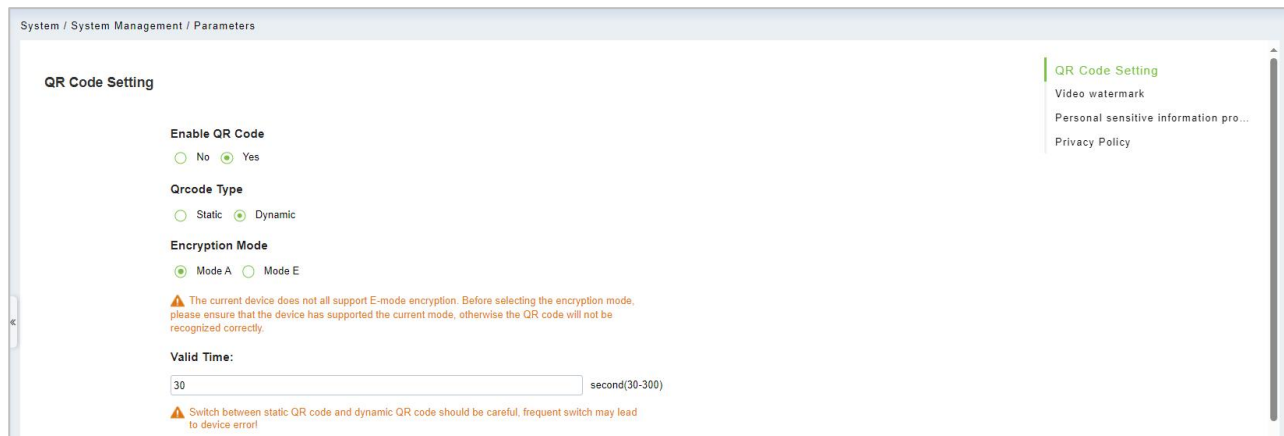
2. Заполните все необходимые поля и нажмите **OK** для регистрации нового пользователя.
3. Нажмите **Access (Доступ) > Device (Устройство) > Control (Управление) > Synchronize All Data to Devices (Синхронизировать все данные с устройствами)** для синхронизации всех данных, включая новых пользователей, на устройстве.

15.4 Мобильные учетные данные ★

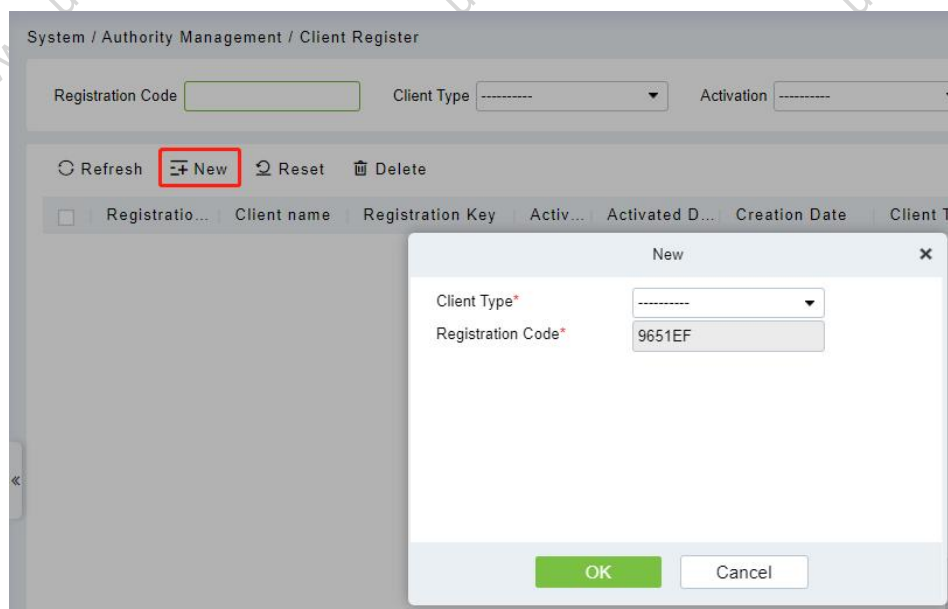
Примечание: данная функция реализована только для устройств модели SenseFace7C.

После загрузки и установки мобильного приложения ZKBioAccess пользователь должен выполнить настройки сервера перед входом в мобильное приложение, для чего нужно сделать следующее:

1. В меню **ZKBio CVAccess > System (Система) > System Management (Управление системой) > Parameters (Параметры)** выберите "Yes" для параметра Enable QR Code (Активировать QR-код) и выберите статус QR-кода в соответствии с текущей ситуацией. По умолчанию установлено значение Dynamic (Динамический), срок действия QR-кода может быть определен.



2. На сервере выберите **System > Authority Management (Управление правами) > Client Register (Регистрация клиента)** для добавления зарегистрированного в приложении клиента.

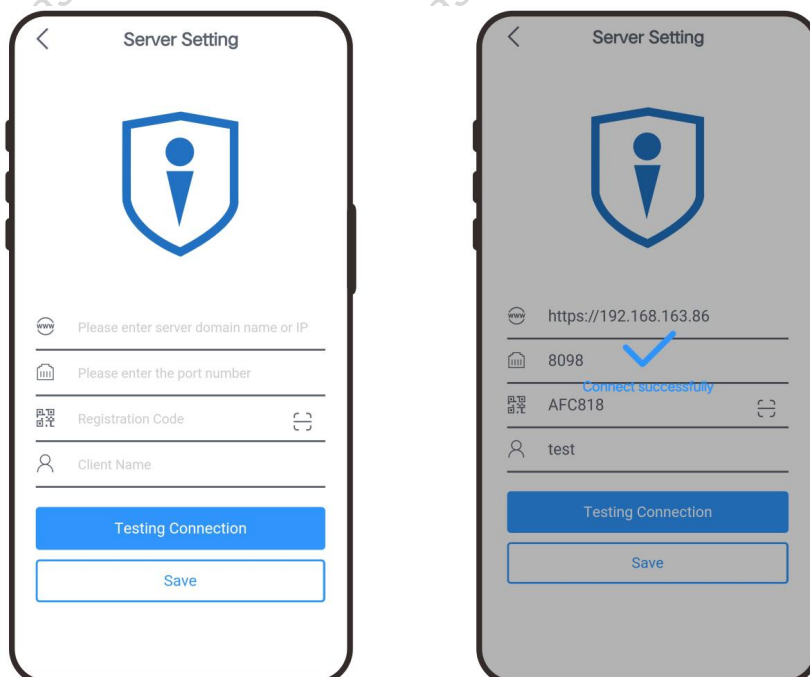


3. Откройте приложение на смартфоне. На экране входа в систему нажмите **Server Setting (Настройки сервера)** и введите IP-адрес или доменное имя сервера, а также номер его порта.

Примечание: смартфон и сервер должны находиться в одном и том же сегменте сети.

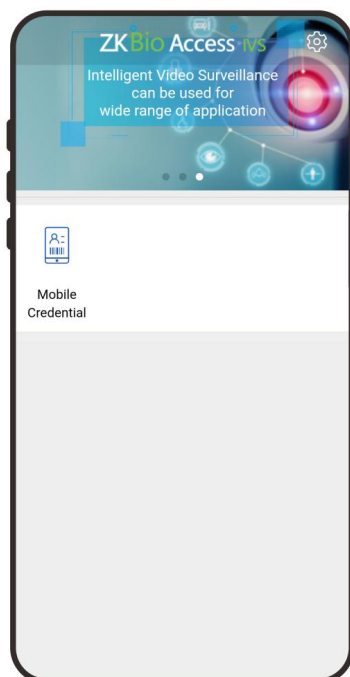
4. Нажмите значок **QR Code** для сканирования QR-кода нового пользователя приложения. После того как пользователь успешно идентифицирован, установите его имя и нажмите **Connection Test (Тест подключения)**.

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

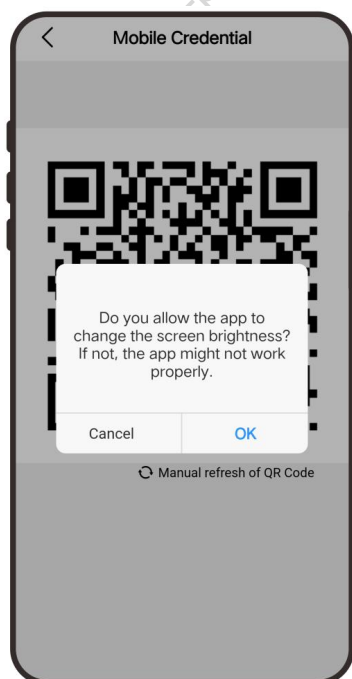


Функция мобильных учетных данных действует только при входе в систему в качестве сотрудника. Нажмите Employee (Сотрудник), чтобы перейти на экран входа сотрудников. Введите ID сотрудника и пароль (по умолчанию: 123456) для входа в систему.

6. Нажмите **Mobile Credential (Мобильные учетные данные)** в приложении, после чего появится QR-код, содержащий ID сотрудника и номер карты (статический QR-код содержит только номер карты).
7. QR-код заменяет физическую карту доступа на конкретном устройстве для бесконтактной верификации для целей разблокировки двери.



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



9. QR-код обновляется автоматически каждые 30 секунд и поддерживает функцию обновления в ручном режиме.



Примечание: более подробная информация приведена в **Руководстве пользователя на ZKBio CVAccess**.

16. Подключение к ПО ZKBioTime

16.1 Установка адреса связи

1. Нажмите **COMM. > Ethernet** в главном меню устройства для установки IP-адреса и шлюза устройства.

Примечание: убедитесь, что IP-адрес находится в том же сегменте сети, что и адрес сервера, и что установлено соединение с ZKBio CVAccessserver.

2. В главном меню нажмите **COMM. > Cloud Server Setting (Настройки облачного сервера)** для установки адреса и порта сервера.

Адрес сервера: установите IP-адрес такой же, как сервера BioTime.

Порт сервера: установите порт сервера такой же, как у BioTime (по умолчанию 8081).

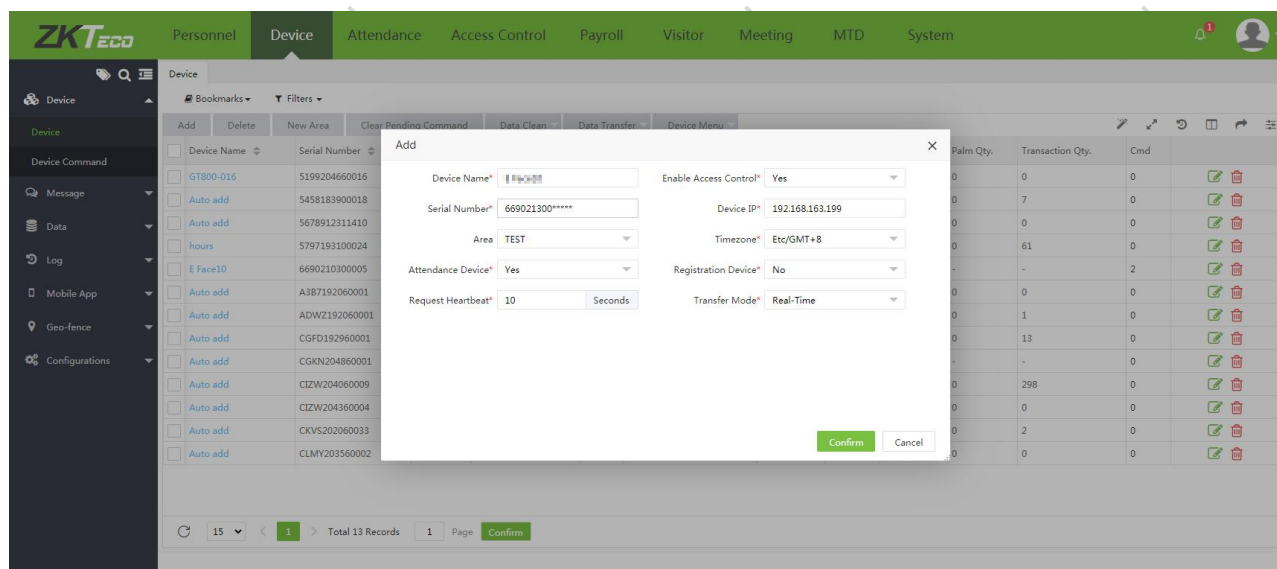
Ethernet	
Display in Status Bar	☒
IPv4	
IP Address	192.168.163.199
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	0.0.0.0
DHCP	☐

Cloud Server Settings	
Server Mode	ADMS
Enable Domain Name	☐
Server Address	192.168.163.61
Server Port	8081
Enable Proxy Server	☐

16.2 Добавление устройства в ПО

Добавьте устройство через поиск. Процедура следующая:

1. Нажмите **Device > Device > Add** для добавления устройства в ПО.
2. После нажатия **Add** откроется новое диалоговое окно. Введите в нем необходимую информацию об устройстве и нажмите **Confirm (Подтвердить)**, после этого добавленные устройства будут автоматически отображаться.



16.3 Добавление сотрудников в ПО

1. Нажмите **Personnel > Employee > Add**:

2. Заполните все необходимые поля и нажмите **Confirm** для регистрации нового пользователя.
3. Нажмите **Device > Device > Data Transfer (Передача данных) > Sync Data to Device (Синхронизировать данные на устройстве)** для синхронизации всех данных, включая новых пользователей, на устройстве.

www.us-plast.ru

www.us-plast.ru

www.us-plast.ru

www.us-plast.ru

www.us-plast.ru

www.us-plast.ru

ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.
Phone : +86 769 - 82109991
Fax : +86 755 - 89602394
www.zkteco.com

