

Доступ автономный

Руководство пользователя



Предисловие

Общая информация

Данное руководство знакомит с функциями и операциями автономного устройства Access (далее именуемого "Устройство"). Внимательно прочитайте перед использованием устройства и сохраните руководство для использования в будущем .

Модель

Модели J, модели H, модели F

Инструкции по технике безопасности

В руководстве могут присутствовать следующие сигнальные слова.

Сигнальные слова	Значение
ОПАСНОСТЬ	Указывает на высокую потенциальную опасность, которая, если ее не избежать, может привести к смерти или серьезным травмам.
ПРЕДУПРЕЖДЕНИЕ	Указывает на среднюю или низкую потенциальную опасность, которая, если ее не избежать, может привести к травмам легкой или средней степени тяжести.
ОСТОРОЖНО.	Указывает на потенциальный риск, который, если его не предотвратить, может привести к ущербу, потере данных, снижению производительности или непредвиденным последствиям.
ESD	Устройства, чувствительные к электростатическому разряду. Указывает на устройство, чувствительное к электростатическому разряду.
ПОРАЖЕНИЕ электрическим ТОКОМ	Указывает на опасное высокое напряжение. Будьте осторожны, избегайте контакта с электричеством.
ЛАЗЕРНОЕ ИЗЛУЧЕНИЕ	Указывает на опасность лазерного излучения. Следите за тем, чтобы избежать воздействия лазерного луча.
Советы	Предоставляет методы, которые помогут вам решить проблему или избежать ее.
ПРИМЕЧАНИЕ	Предоставляет дополнительную информацию в качестве дополнения к основной информации.

История изменений

Версия	Содержание изменений	
Версия 1.0.0	Первый выпуск.	

Как пользователь устройства или контролер данных, вы можете собирать персональные данные других лиц, такие как их лицо, звук, отпечатки пальцев и номерной знак. Вы должны соблюдать местные законы и нормативные акты о защите частной жизни для защиты законных прав и интересов других людей путем реализации мер, которые включают, но не ограничиваются ими: Обеспечение четкой и видимой идентификации для информирования людей о существовании зоны наблюдения и предоставления необходимой контактной информации.

О руководстве

- Руководство

Руководство предназначено только для справки. Между руководством и продуктом могут быть обнаружены незначительные различия.
- Мы

не несут ответственности за убытки, понесенные в результате эксплуатации изделия способами, не соответствующими указанному в руководстве.
- Это

руководство будет обновляться в соответствии с последними законами и нормативными актами соответствующих юрисдикций. Для получения подробной информации ознакомьтесь с бумажным руководством пользователя, воспользуйтесь нашим компакт-диском, отсканируйте QR-код или посетите наш официальный веб-сайт. Руководство предназначено только для справки. Между электронной и бумажной версиями могут быть обнаружены незначительные различия.

Дизайн и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта это может привести к появлению некоторых различий между реальным продуктом и руководством пользователя. Пожалуйста, обратитесь в службу поддержки клиентов за последней версией программы и дополнительной документацией.

При печати могут быть ошибки или отклонения в описании функций, операций и технических данных. В случае возникновения каких-либо сомнений или споров мы оставляем за собой право на окончательное объяснение.

Обновите программное обеспечение Reader или попробуйте другое стандартное программное обеспечение для чтения, если руководство (в формате PDF) не удастся открыть.

Все торговые марки, зарегистрированные товарные знаки и названия компаний, приведенные в руководстве, являются собственностью их соответствующих владельцев.

Пожалуйста, посетите наш веб-сайт, обратитесь к поставщику или в службу поддержки клиентов, если во время использования устройства возникнут какие-либо проблемы .

Если есть какая-либо неопределенность или разногласия, мы оставляем за собой право на окончательное объяснение.

Содержание

Предисловие...	
1 Обзор...	
2 Локальные операции (модели клавиатур)...	
2.1 Подготовка...	
2.1.1 Функция клавиатуры...	
2.1.2 Способ ввода...	
2.2 Инициализация...	
2.3 Главный экран...	
2.4 Вход в Главное меню...	
2.5 Способы разблокировки...	
2.5.1 Карта...	
2.5.2 Отпечаток пальца...	
2.5.3 Пароль пользователя...	
2.5.4 Общедоступный пароль ...	
2.5.5 Временный пароль...	... 9
2.6 Управление персоналом...	... 10
2.6.1 Добавление Нового пользователя.....	10
2.6.2 Список пользователей / Администраторов.....	12
2.6.3 Настройка общедоступного пароля.....	14
2.6.4 Удаление всех пользователей...	... 14
2.7 Управление контролем доступа...	... 14
2.7.1 Разблокировка комбинации.....	14
2.7.2 Настройка сигналов тревоги.....	15
2.7.3 Настройка состояния блокировки.....	16
2.7.4 Настройка Интервалов проверки.....	17
2.7.5 Управление основными картами...	... 17
2.7.6 Настройка аутентификации по PIN-коду...	... 18
2.8 Управление посещаемостью.....	18
2.9 Настройки связи.....	18
2.9.1 Настройка IP-адреса.....	18
2.9.2 Настройка Wi-Fi.....	19
2.9.3 Настройка точки доступа Wi-Fi...	... 20
2.9.4 Настройки режима...	...21
2.10 Системные настройки...	... 25
2.10.1 Настройка времени...	...25
2.10.2 Настройка громкости.....	26
2.10.3 Настройка языка...	... 27

2.10.4 Настройка параметров экрана.....	27
2.10.5 Настройка параметров карты...	... 28
2.10.6 Управление паролем устройства.....	29
2.10.7 Восстановление заводских настроек по умолчанию.....	30
2.10.8 Устройство для сброса настроек.....	31
2.11 Управление по USB...	... 31
2.11.1 Экспорт данных...	... 31
2.11.2 Импорт данных ...	... 32
2.11.3 Обновление устройства...	... 33
2.12 Управление документацией.....	33
2.13 Просмотр информации.....	33
2.13.1 Объем данных для просмотра.....	33
2.13.2 Версия устройства просмотра.....	34
3 Локальные операции (модели с сенсорным экраном)...	...35
3.1 Инициализация...	... 35
3.2 Внешний вид.....	35
3.3 Главный экран...	... 35
3.4 Вход в Главное меню.....	37
3.5 Сброс пароля.....	38
3.6 Способы разблокировки...	... 39
3.6.1 Карта...	... 39
3.6.2 Отпечаток пальца.....	39
3.6.3 Bluetooth.....	39
3.6.4 Пароль пользователя.....	40
3.6.5 Общедоступный пароль ...	...41
3.6.6 Временный пароль...	... 42
3.7 Управление персоналом...	... 43
3.7.1 Добавление Пользователей.....	43
3.7.2 Просмотр информации о пользователе и администраторе.....	45
3.7.3 Настройка общедоступного пароля...	... 47
3.8 Управление контролем доступа...	... 47
3.8.1 Настройка метода разблокировки...	... 47
3.8.2 Настройка аварийных сигналов...	... 49
3.8.3 Настройка Интервала проверки.....	51
3.8.4 Настройка состояния блокировки...	... 51
3.8.5 Управление Основными картами.....	52
3.8.6 Настройка аутентификации по PIN-коду.....	53
3.9 Управление посещаемостью...	... 53
3.10 Настройки связи...	... 54
3.10.1 Настройка IP...	...54

3.10.2 Настройка Wi-Fi... 3.10.3	... 55
Настройка точки доступа Wi-Fi...	...55
3.10.4 Настройка Bluetooth.....	56
3.10.5 Настройки режима.....	57
3.11 Системные настройки.....	61
3.11.1 Настройка времени.....	61
3.11.2 Настройка языка...	... 62
3.11.3 Настройка громкости...	...62
3.11.4 Настройка параметров экрана...	... 63
3.11.5 Настройка параметров карты.....	65
3.11.6 Настройка пароля устройства.....	67
3.11.7 Восстановление заводских настроек по умолчанию.....	67
3.11.8 Настройка сброса пароля.....	68
3.11.9 Перезапуск устройства...	...68
3.12 Управление с помощью USB...	... 68
3.12.1 Экспорт данных.....	69
3.12.2 Импорт данных.....	69
3.12.3 Устройство обновления.....	70
3.13 Управление документацией.....	70
3.14 Просмотр информации...	... 71
3.14.1 Объем данных для просмотра...	... 71
3.14.2 Версия устройства просмотра.....	71
4 Веб-операции.....	72
4.1 Инициализация.....	72
4.2 Вход в систему...	...72
4.3 Сброс пароля...	... 73
4.4 Мониторинг доступа...	... 73
4.5 Домашняя страница.....	75
4.6 Управление персоналом.....	75
4.7 Управление контролем доступа...	... 81
4.7.1 Параметры контроля доступа.....	81
4.7.2 Сигнал тревоги...	... 85
4.7.3 Настройки карты...	... 90
4.7.4 Настройка периодов.....	95
4.7.5 Настройка модулей расширения...	...98
4.7.6 Настройка внутреннего сравнения.....	98
4.7.7 Настройка разблокировки от первого лица...	...99
4.7.8 Настройка защиты от обратного доступа...	... 100
4.8 Настройка посещаемости...	... 102
4.8.1 Настройка Отделов.....	102

4.8.2 Настройка смен...	... 103
4.8.3 Настройка выходных...	... 105
4.8.4 Настройка графиков работы.....	106
4.8.5 Экспорт записи о посещаемости...	... 109
4.8.6 Настройка режимов посещаемости.....	110
4.9 Аудио...	... 111
4.9.1 Настройка параметров звука...	... 111
4.9.2 Управление аудиофайлами ...	... 113
4.10 Настройки связи...	... 113
4.10.1 Сетевые настройки...	...113
4.10.2 Настройки Bluetooth.....	125
4.10.3 Настройки режима.....	125
4.11 Управление системой.....	129
4.11.1 Управление пользователями...	... 129
4.11.2 Просмотр Онлайн-пользователей...	... 132
4.11.3 Настройка времени.....	132
4.11.4 Настройка "Всегда включено".....	134
4.12 Центр технического обслуживания.....	134
4.12.1 Диагностика одним щелчком мыши.....	134
4.12.2 Системная информация...	... 135
4.12.3 Емкость данных...	... 135
4.12.4 Просмотр журналов.....	136
4.12.5 Управление техническим обслуживанием.....	137
4.12.6 Обновление системы.....	139
4.12.7 Расширенное техническое обслуживание.....	140
4.13 Настройки безопасности (необязательно)...	... 141
4.13.1 Состояние безопасности...	... 141
4.13.2 Настройка HTTPS.....	142
4.13.3 Атака Защита.....	143
4.13.4 Установка сертификата устройства...	... 146
4.13.5 Установка сертификата доверенного центра сертификации...	... 149
4.13.6 Предупреждение системы безопасности ...	... 150
4.13.7 Аутентификация безопасности...	...151
5 Телефонные операции.....	152
5.1 Инициализация.....	152
5.2 Вход на Веб-страницу.....	152
5.3 Домашняя страница.....	154
5.4 Управление персоналом...	... 156
5.5 Настройка системы...	... 160
5.5.1 Просмотр информации о версии.....	160

5.5.2 Управление конфигурацией...	... 160
5.5.3 Техническое обслуживание...	... 160
5.5.4 Настройка времени.....	161
5.5.5 Емкость данных...	...162
5.5.6 Язык.....	162
5.6 Настройка посещаемости...	... 162
5.6.1 Настройка отделов...	... 162
5.6.2 Настройка смен ...	... 164
5.6.3 Настройка выходных...	... 167
5.6.4 Настройка графиков работы...	... 168
5.6.5 Настройка режимов посещаемости.....	170
5.7 Настройка контроля доступа.....	171
5.7.1 Настройка методов разблокировки...	... 171
5.7.2 Настройка параметров контроля доступа...	... 172
5.7.3 Настройка аварийных сигналов...	... 176
5.7.4 Настройка аварийных подключений (необязательно).....	179
5.7.5 Настройка привязки аварийных событий...	... 180
5.7.6 Настройка параметров карты.....	181
5.7.7 Настройка параметров экрана.....	183
5.8 Настройки связи...	... 184
5.8.1 Настройка TCP / IP...	... 184
5.8.2 Настройка Wi-Fi.....	186
5.8.3 Настройка точки доступа Wi-Fi.....	186
5.8.4 Настройка Облачного сервиса.....	187
5.8.5 Настройка автоматической регистрации.....	187
5.8.6 Режим настройки...	... 188
5.8.7 Настройка Bluetooth...	... 192
5.9 Настройка звуковых подсказок.....	193
5.10 Просмотр журналов.....	194
5.10.1 Системные журналы ...	... 194
5.10.2 Записи разблокировки ...	... 194
5.10.3 История вызовов...	...195
5.10.4 Журналы аварийных сигналов...	... 195
6 Конфигураций Smart PSS Lite...	... 196
6.1 Установка.....	196
6.2 Инициализация и вход в Систему...	... 196
6.3 Добавление устройств.....	197
6.3.1 Добавление устройства путем поиска...	... 197
6.3.2 Добавление устройств Одно за другим...	...198
Приложение 1 Важные моменты Инструкций по регистрации отпечатков пальцев.....	199

1 Общий обзор

Access standalone оснащен встроенным высокопроизводительным процессором и недавно обновленным дизайном экстерьера. Они поддерживают несколько методов ввода, включая отпечаток пальца (доступен на некоторых модели), карта, пароль, Bluetooth (доступно на некоторых моделях) и проверка комбинации. В паре с платформой управления эти устройства обеспечивают выполнение множества функций разнообразные потребности пользователей.

2 локальных операции (модели клавиатур)

2.1 Подготовка

2.1.1 Функция клавиатуры

Устройство не оснащено сенсорным экраном, поэтому для работы с ним требуются физические клавиши. Когда устройство в режиме ожидания вы можете нажать любую клавишу, чтобы активировать экран.



Только для определенных моделей нажатие кнопки вызова может активировать экран.

Рисунок 2-1 Модель H



Рисунок 2-2 Модель J



Таблица 2-1 Описание клавиатуры

Элемент	Описание
Число или буква	Используется для ввода информации или пароля.
	— Клавиши со стрелками для навигации по странице.
Esc	Отмените операцию или вернитесь на предыдущую страницу.
OK	Перейдите на выбранную страницу или подтвердите внесение изменений.
-	Нажмите клавишу "Назад".
	Нажмите кнопку звонка (только на экране ожидания), перейдите по экрану или измените метод ввода.

2.1.2 Метод ввода

Изменение метода ввода

Модель H: нажмите , чтобы изменить метод ввода.

 Модель J: нажмите , чтобы изменить метод ввода.

Обзор методов ввода

Вы можете вводить содержимое после переключения на соответствующий метод ввода.

 режим верхнего регистра.

 режим нижнего регистра.

 Цифровой режим 123.

 Aa : Комбинация прописных и строчных букв.

 : Символьный режим.

Ввод прописных или строчных букв.

При использовании режима ввода в верхнем или нижнем регистре несколько раз нажмите цифровую клавишу для циклического ввода по назначенным буквам. Например, в режиме ввода в нижнем регистре:

Нажмите клавишу 2 один раз, чтобы ввести a.

Дважды нажмите клавишу 2, чтобы ввести b.

- Трижды нажмите клавишу 2, чтобы ввести c.

В режиме ввода заглавных букв:

- Нажмите клавишу 2 один раз, чтобы ввести A.

Дважды нажмите клавишу 2, чтобы ввести B.

Нажмите клавишу 2 три раза, чтобы ввести C.

Таблица 2-2 Буквенно-ключевое сопоставление

Клавиша	Нажмите один раз	Нажмите два раза	Нажмите три раза
2	a / A	b / B	c / C
3	d / D	e / E	f / F
4	g / G	h / H	i / I
Аналогичная логика применима к клавишам 5-9.			

Ввод прописных и строчных букв.

В комбинированном режиме при первом нажатии цифровой клавиши выводится заглавная буква; при последующих нажатиях выводятся только строчные буквы. Например:

Первое нажатие: A (верхний регистр)

Второе нажатие: a (нижний регистр)

Ввод чисел

В цифровом режиме нажмите нужную цифровую клавишу.

Ввод символов

В символьном режиме, нажмите соответствующие цифровые клавиши для выбора нужного символа, а затем нажмите a/√, чтобы перейти к следующей/предыдущей странице.

Рисунок 2-3 введите символы



2.2 инициализация

Для первого использования или после восстановления заводских настроек по умолчанию вам необходимо установить пароль и связать свой адрес электронной почты для учетной записи администратора. Вам также необходимо установить часовой пояс устройства. Вы можете использовать учетную запись администратора для входа в главное меню устройства, настройки устройства и входа в систему веб-браузер и SmartPSS Lite.

Рисунок 2-4 Инициализация



Если вы забыли пароль администратора, отправьте запрос на сброс на связанный с ним адрес электронной почты. в пароль должен состоять из 8-32 непустых символов и содержать по крайней мере два типа следующие символы: верхний и нижний регистры, цифры и специальные символы (за исключением ";" &). Установите пароль высокого уровня безопасности, следуя подсказке о надежности пароля.

2.3 Главный экран

Вы можете открыть дверь на главном экране с вашей карты, пароля или отпечатков пальцев.



В Устройство переходит обратно на страницу ожидания, если нет операции в течение 30 секунд.

Экран в руководстве пользователя приведен только для справки.

Рисунок 2-5 Главный экран

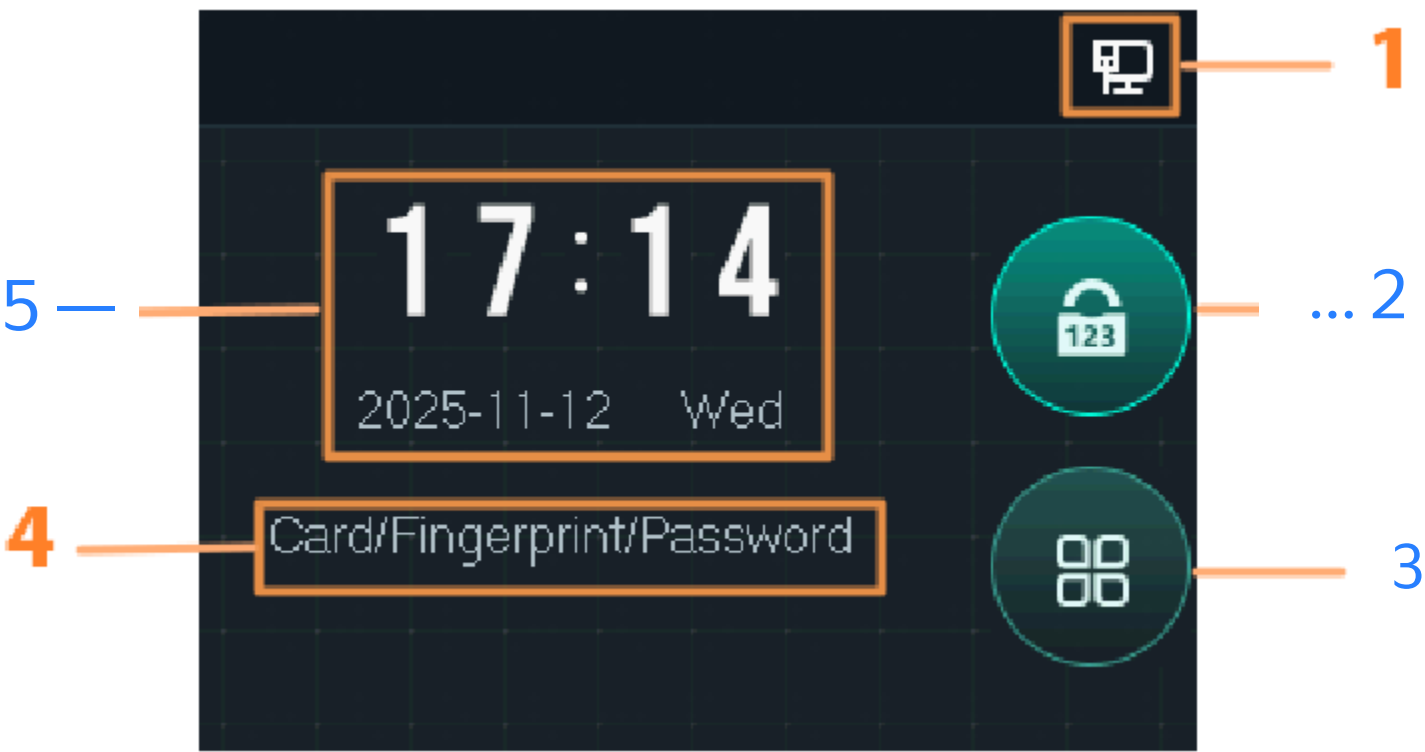


Таблица 2-3 Описание главного экрана

Нет.	Предмет	Описание
	Статус	Отображает состояние Wi-Fi, проводной сети (при наличии), и USB-накопителя.
	Откройте дверь с помощью пароля	Введите идентификатор пользователя и пароль или пароль администратора, чтобы разблокировать дверь.
	Главное меню	Нажмите, чтобы войти в главное меню. Только администратор и пользователи с правами администратора могут входить в главное меню.
4	Методы разблокировки	Отображает настроенные вами методы разблокировки.
5	Дата и время	Время и дата.

2.4 Вход в главное меню

Войдите в главное меню, чтобы настроить параметры устройства. Например, вы можете добавлять пользователей различные разрешения и изменение режима разблокировки.

Справочная информация

Только администратор и пользователи с правами администратора могут входить в главное меню.

Процедура

- Шаг 1

На экране ожидания коснитесь A / V, чтобы перейти к 



Методы проверки зависят от типа устройства.
- Шаг 2

Войдите в главное меню.

Войдите в систему как пользователь с правами администратора, используя карту, отпечаток пальца или Пароль.

Войдите в систему как администратор: нажмите admin, а затем введите пароль, который вы установили во время инициализации.

Шаг 3 В главном меню нажмите A /√ для перехода по странице, а затем нажмите OK для настройки параметры устройства.



Используйте сочетания клавиш для настройки параметров, просто нажав 1-6.

Чтобы настроить управление пользователями, нажмите 1.

Чтобы настроить контроль доступа, нажмите 2.

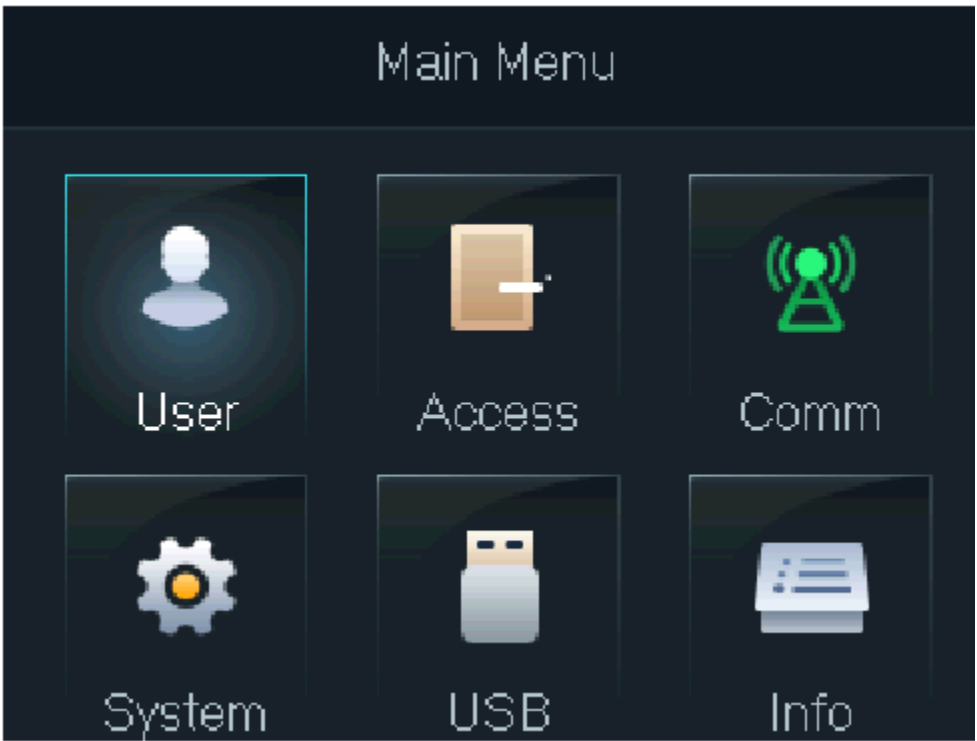
Чтобы настроить связь, нажмите 3.

Чтобы настроить систему, нажмите 4.

Чтобы настроить USB, нажмите 5.

Чтобы просмотреть системную информацию, нажмите 6.

Рисунок 2-6 Главное меню



2.5 Способы разблокировки

2.5.1 Карта

Проведите картой, чтобы разблокировать дверь.



Для устройство Access Standalone с функцией идентификации, если оно подключено к внешнему устройству считывания идентификационных карт, то расстояние между устройством Access Standalone и устройством считывания карт должно быть больше 10 см. В противном случае, устройство считывания карт может работать неправильно, поскольку оно расположено слишком близко к кнопке автономного доступа.

2.5.2 Отпечаток пальца

Нажмите зарегистрированный отпечаток пальца на сканере отпечатков пальцев, чтобы разблокировать дверь.

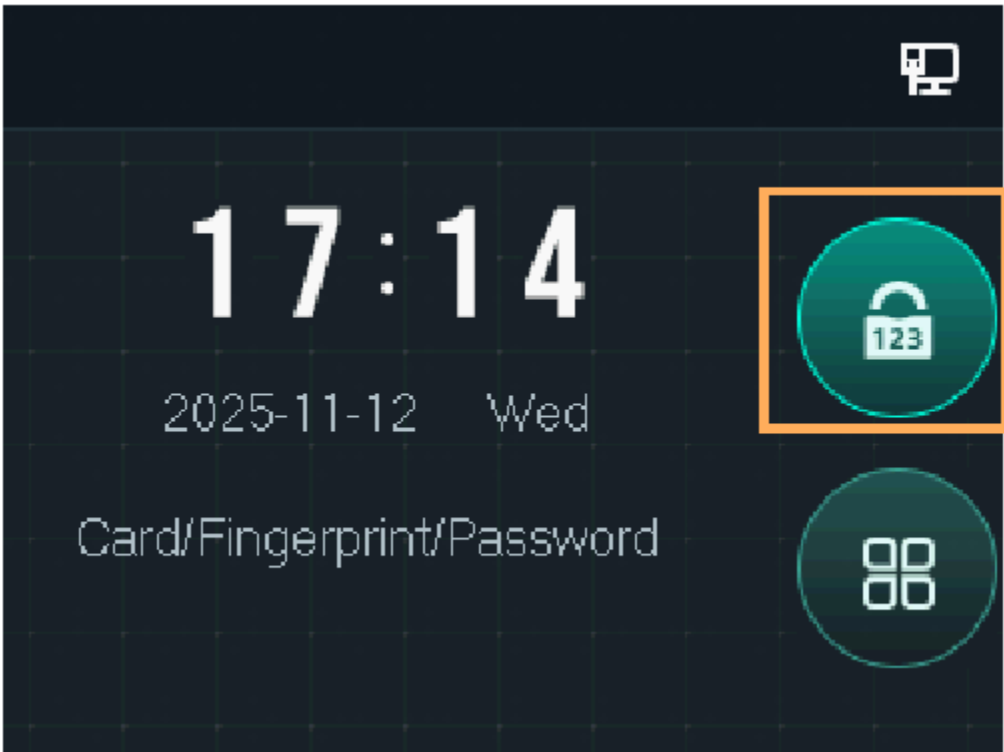
2.5.3 Пароль пользователя.

Введите идентификатор пользователя и пароль, чтобы разблокировать дверь.

Процедура

Шаг 1 Нажмите A и V на главном экране, выберите, а затем нажмите OK.

Рисунок 2-7 Главный экран



Шаг 2 Выберите Разблокировать по паролю, а затем нажмите OK.

Шаг 3 Введите идентификатор пользователя и пароль.



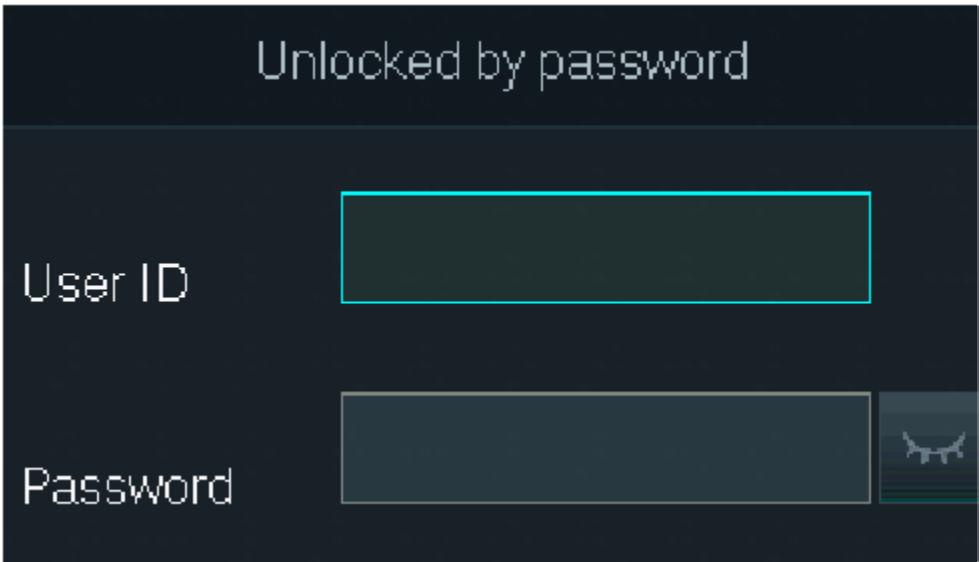
Чтобы ввести идентификатор пользователя, вам нужно выбрать поле ввода идентификатора пользователя и затем нажать OK. Вы можете ввести пароль непосредственно с клавиатуры.



Г, чтобы изменить метод ввода.

Шаг 4 Выберите OK, а затем нажмите OK.

Рисунок 2-8 Разблокировка по паролю пользователя



2.5.4 Общедоступный пароль

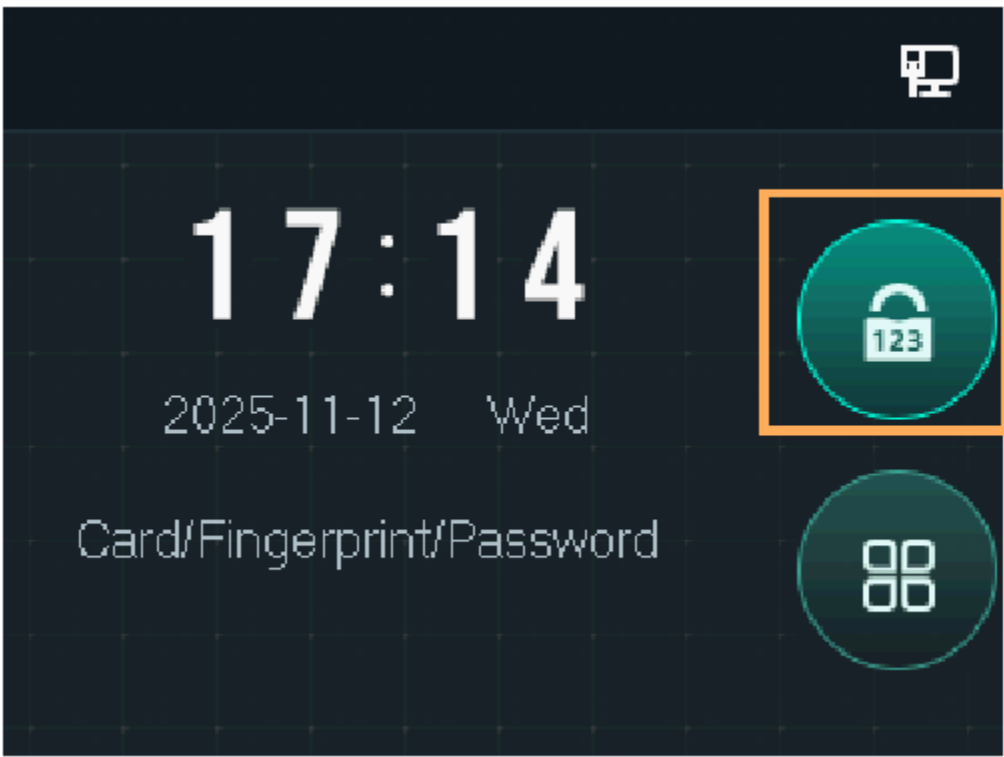
После установки общедоступного пароля и его активации вы можете разблокировать дверь, просто введя общедоступный пароль. Использование общедоступного пароля для разблокировки двери без зависимости от уровня пользователя, разблокируйте режимы, периоды, планы на отпуск и защиту от обратного доступа, за исключением нормально закрытой двери. Устройство допускает только один общедоступный пароль.

Справочная информация

Чтобы использовать общедоступный пароль для доступа к двери, вам необходимо включить эту функцию. Процедура

- Шаг 1
- Нажмите A и V на главном экране, выберите, а затем нажмите OK.

Рисунок 2-9 Главный экран



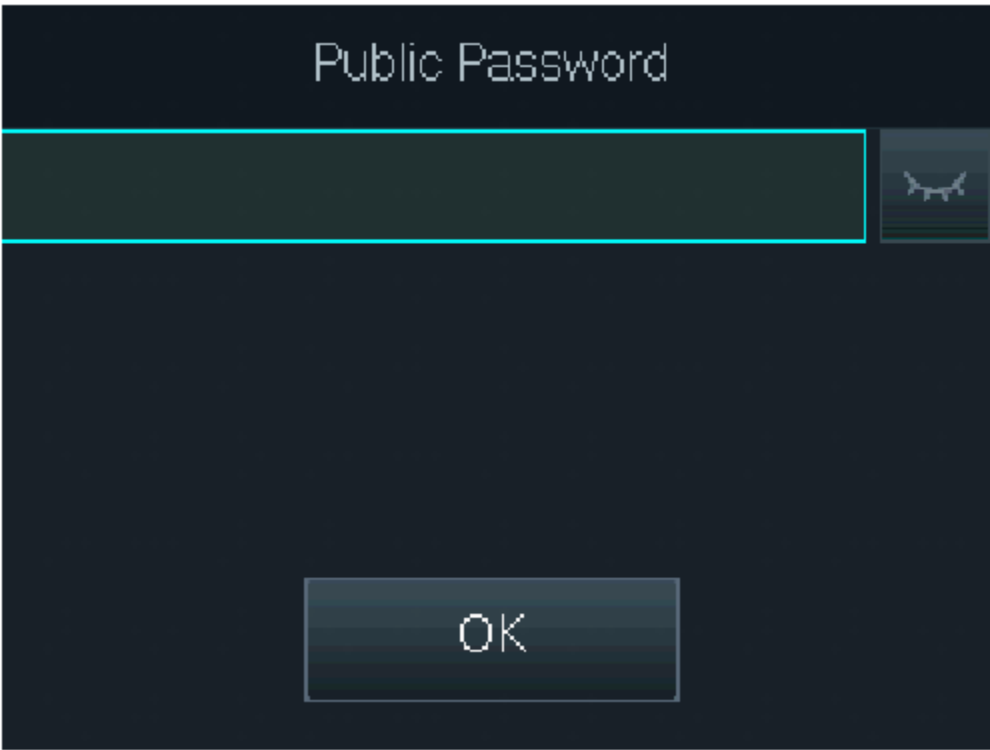
- Шаг 2
- Выберите Разблокировать с помощью общедоступного пароля, а затем нажмите OK.

- Шаг 3
- Введите общедоступный пароль, выберите OK, а затем нажмите OK.



На главном экране нажмите и удерживайте клавишу 0 в течение 3 секунд, чтобы перейти непосредственно к общедоступному Экран ввода пароля для разблокировки.

Рисунок 2-10 Разблокировка с помощью общедоступного пароля



2.5.5 Временный пароль

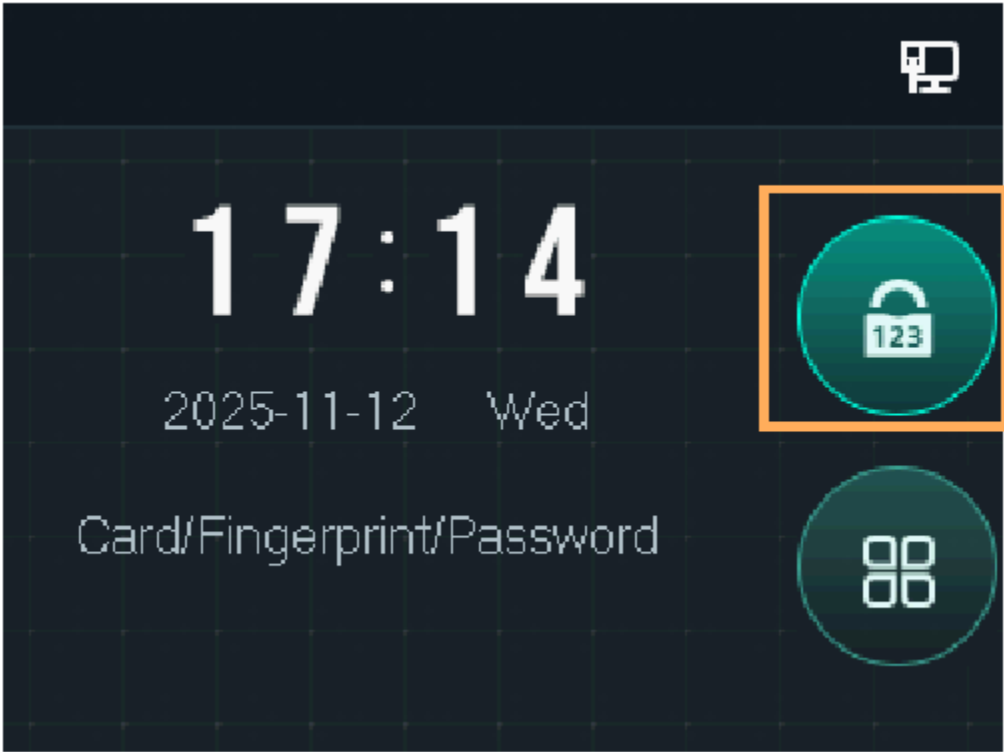
Необходимые требования

Вы получили временный пароль, выданный из приложения DMSS.

Процедура

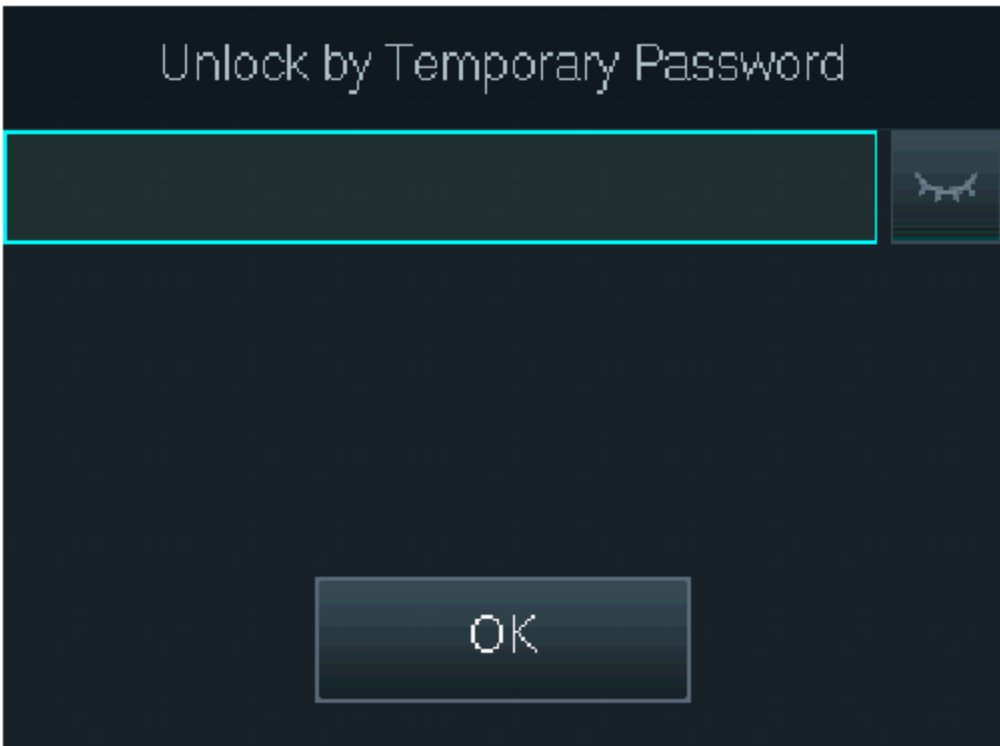
Шаг 1 Нажмите A и V на главном экране, выберите,  а затем нажмите OK.

Рисунок 2-11 Главный экран



Шаг 2 Выберите Разблокировать с помощью временного пароля, а затем нажмите OK. Шаг 3 Введите временный пароль, выберите OK, а затем нажмите OK.

Рисунок 2-12 Разблокировка с помощью временного пароля



2.6 Управление пользователями

Вы можете добавлять новых пользователей, просматривать список пользователей или список администраторов на экране Использовать г.

2.6.1 Добавление нового пользователя

Процедура

Шаг 1 На экране ожидания нажмите  для перехода к Шаг 2 Войдите в систему с учетной записью администратора, а затем выберите Пользователи> Создать пользователя.



Экраны в этом руководстве приведены только для справки и могут отличаться от реальных продукт.

Рисунок 2-13 Создание пользователей

Create User(1/4)

ID

2

Name

Verification Mode

Same as Device

Unlock Method

Card/Fingerprint/Password

Create User(2/4)

Fingerprint

0

Card

0

Password

User Permission

User >

Create User(3/4)

General Plan

255-Default

Holiday Plan

255-Default

Validity Period

Forever

User Type

General User >

Create User(4/4)

Department

1-Default

Schedule Mode

Dept Schedule

Permission Type

Unlock and Attendance

Шаг 3 Настройка параметров.

Таблица 2-4 Описание пользовательских параметров

Параметр	Описание
ID	Каждый идентификатор пользователя уникален. Он может состоять из 18 символов цифр и их комбинации.
Имя	Введите имя (максимум 32 символа, включая цифры, символы и буквы).
Отпечаток пальца	Каждый пользователь может добавить до 3 отпечатков пальцев. Следуйте инструкциям на экране и голосовым подсказкам, чтобы добавить отпечатки пальцев. Вы можете включить функцию принудительного снятия отпечатков пальцев под каждым отпечатком пальца. После включения функции принудительной сигнализации сработает сигнализация, если дверь будет отперта по отпечатку пальца принудительной функцией. Мы не рекомендуем устанавливать первый отпечаток пальца в качестве принудительного отпечаток пальца. Функцию "отпечаток пальца" поддерживают только определенные модели.

Параметр	Описание
Информация с карты	Вы можете зарегистрировать пять карт для каждого пользователя. На странице регистрации проведите своей картой по считывателю карт, после чего устройство считает информацию с карты. Информация с карты будет считана устройством. Вы можете включить функцию принудительной карты на странице регистрации карт. После включения функции принудительной сигнализации будет срабатывать сигнализация, если дверь отпирается принудительной картой.
Пароль	Введите пароль пользователя. Максимальная длина пароля составляет 8 цифр. Пароль для принудительного использования добавляется к 1 на основе последнего пароля для разблокировки. Например, если пароль пользователя равен 12345, то принудительный пароль будет равен 12346; если пароль пользователя равен 789, а за последний раз использовался принудительный пароль равен 780. При использовании пароля для разблокировки двери сработает аварийный сигнал.
Тип разрешения.	Вы можете выбрать разрешение пользователя для нового пользователя. У обычных пользователей есть только разрешение на разблокировку дверей. Администраторы могут настроить устройство и разблокировать дверь.
Общий план	Пользователь может иметь доступ к двери только в течение определенного периода. Значение по умолчанию равно 255, что означает, что период не настроен.
План отпуска	Пользователь может иметь доступ к двери только в течение запланированных праздничных дней. Значение по умолчанию равно 255, что означает, что план на отпуск не настроен.
Период действия	Укажите период, в течение которого пользователь имеет контроль доступа к двери.
Тип пользователя	Общие: Обычные пользователи могут разблокировать дверь в обычном режиме. Список блокировок: Когда пользователи из списка блокировок открывают дверь, обслуживающий персонал получает уведомление. Гость: Гости могут отпирать дверь в течение определенного периода или на определенное количество раз. По истечении установленного периода или времени отпирания они не смогут отпереть дверь. Патрулирование: Условно-досрочно освобожденные пользователи могут отслеживать статус двери, у них нет прав на разблокировку. VIP: Когда VIP-пользователи открывают дверь, они не ограничены режимами разблокировки, такими как мультикарта и раздел времени. Другие: Когда они откроют дверь, она останется незапертой еще 5 секунд. Пользовательский пользователь 1/2: То же, что и обычный.

Шаг 4 Нажмите Esc, а затем ОК, чтобы сохранить настройки.

2.6.2 Список пользователей / администраторов

Вы можете просматривать и выполнять поиск по всем обычным пользователям и администраторам, а также редактировать информацию о пользователе.

В главном меню выберите Пользователи > Список пользователей или Пользователи > Список администраторов.

Рисунок 2-14 Список пользователей

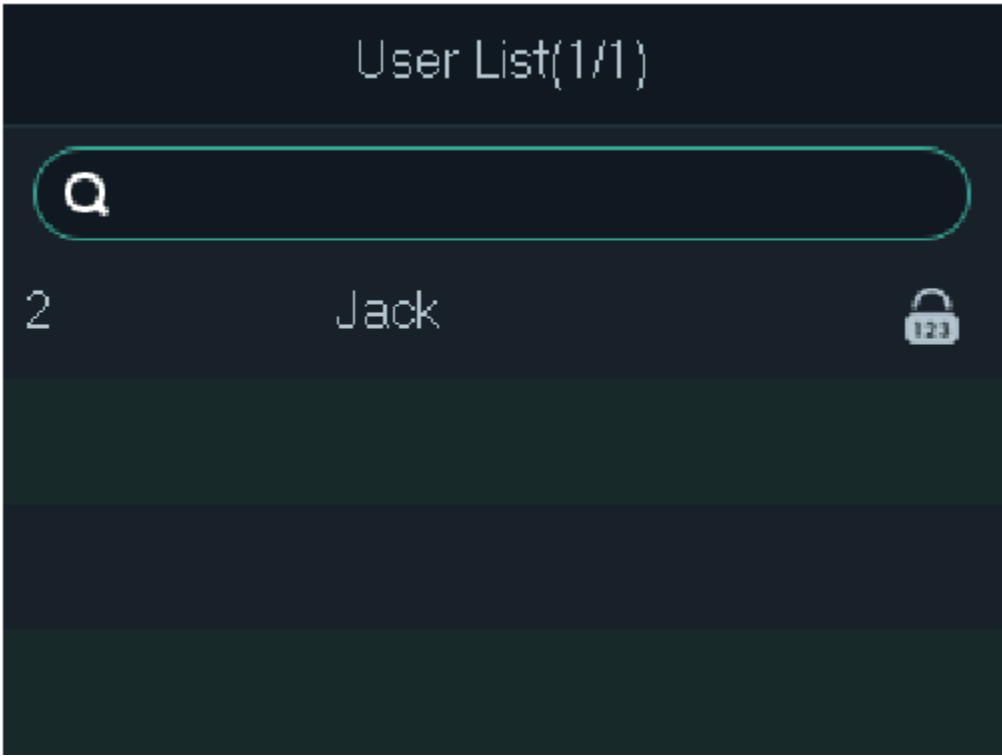


Рисунок 2-15 Список администраторов



Способ разблокировки



Отпечаток пальца.



Карта.



: Пароль.

Редактирование информации о пользователе

1. Выберите пользователя и нажмите OK.
2. Отредактируйте информацию о пользователе, а затем нажмите Esc.
3. Нажмите Esc для сохранения настроек.

Поиск пользователей

1. Выберите  и нажмите ОК.
2. Введите идентификатор пользователя, проведите карточкой или нажмите отпечаток пальца для поиска пользователя.

Удаление пользователей

Выберите пользователя, нажмите ОК, а затем выберите  чтобы удалить пользователя.

2.6.3 Настройка общедоступного пароля

Добавьте и включите общедоступный пароль. Общедоступный пароль можно использовать для разблокировки двери в любых режимах разблокировки .

Войдите в главное меню и выберите Пользователи > Общедоступный пароль.

Добавить общедоступный пароль

1. Выберите Настроить общедоступный пароль, введите новый пароль и нажмите ОК.
2. Введите пароль еще раз для подтверждения, а затем нажмите ОК.
3. Нажмите ОК, чтобы сохранить настройки.

Включить общедоступный пароль

Выберите Включить общедоступный пароль, а затем нажмите ОК.

2.6.4 Удаление всех пользователей

В главном меню выберите Пользователи > Удалить всех пользователей.

2.7 Управление контролем доступа

2.7.1 Комбинированная разблокировка

Процедура

Шаг 1 В главном меню выберите Доступ> Комбинированная разблокировка, а затем нажмите ОК.

Шаг 2 Настройте комбинации разблокировки.

Комбинированный метод: Выберите Или или И.

- ◇ И: Вы должны проверить все выбранные методы разблокировки, чтобы открыть дверь.
- ◇ Или: Вы можете подтвердить один из выбранных методов разблокировки, чтобы открыть дверь.

Карта: разблокировка с помощью карты. Выберите "Да" или "Нет".

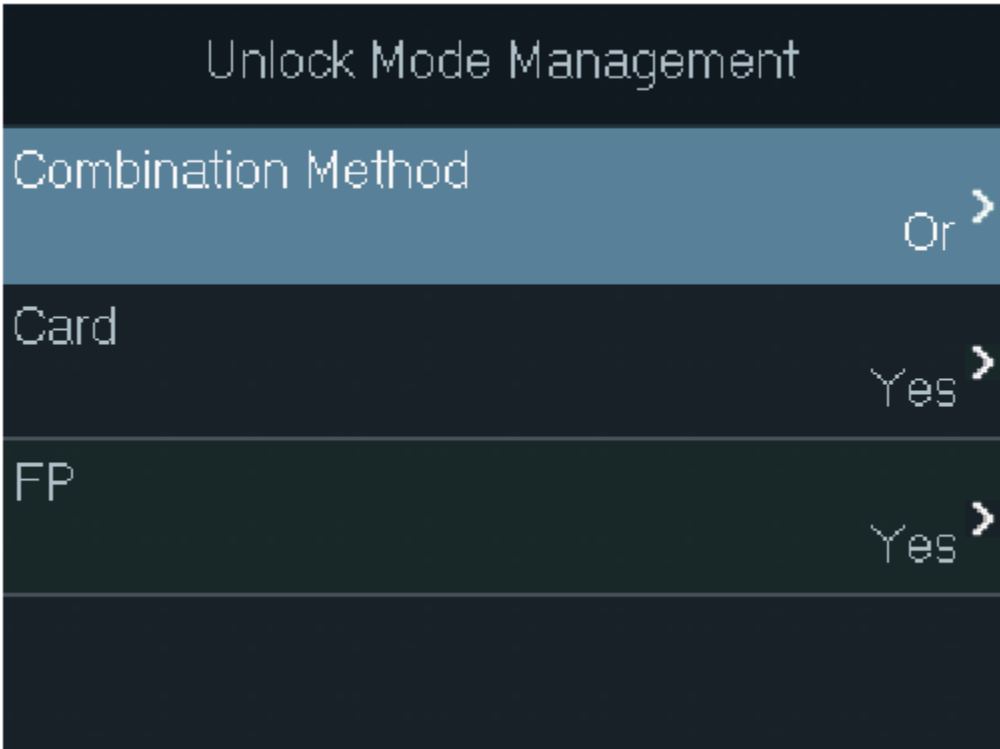


Поддерживается только на некоторых моделях. FP: разблокировка по отпечатку пальца. Выберите "Да" или "Нет".



Поддерживается только на некоторых моделях.

Рисунок 2-16 Комбинация разблокировки.



2.7.2 Настройка аварийных сигналов.

Настройте аварийные сигналы контроля доступа, и аварийные события могут своевременно отправляться администраторам.

Процедура

- Шаг 1 В главном меню выберите Доступ> Аварийный сигнал, а затем нажмите ОК.
- Шаг 2 Включите аварийные сигналы в соответствии с вашими потребностями.

Рисунок 2-17 Типы сигналов тревоги

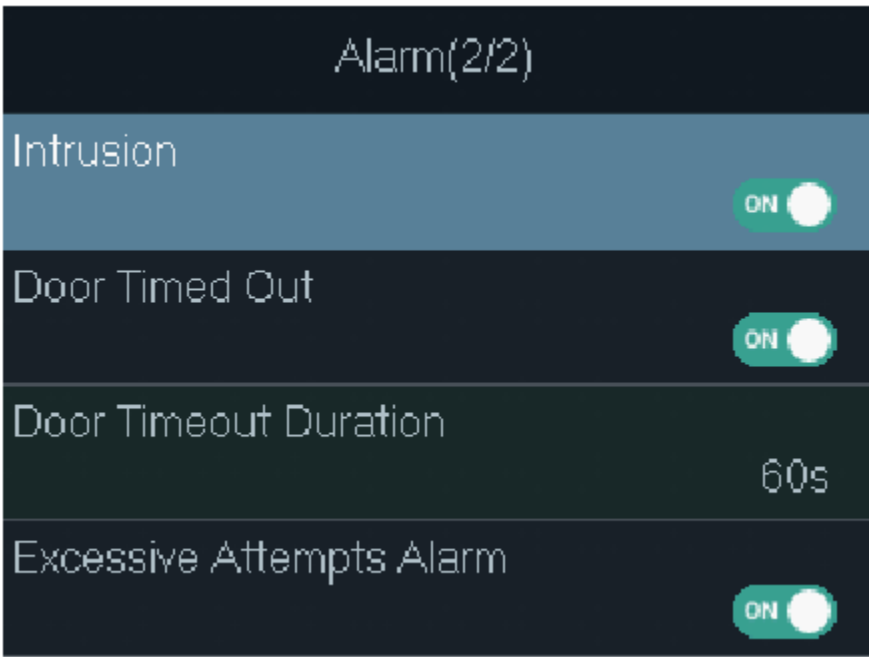


Таблица 2-5 Описание типов сигналов тревоги

Параметр	Описание
Защита от обратной передачи	Сигнал тревоги сработает, если кто-то снова войдет в систему без авторизации.

Параметр	Описание
Принуждение	Сигнал тревоги срабатывает, когда для отпирания двери используется принудительный отпечаток пальца.
Дверной извещатель	Когда дверной извещатель включен, отображаются как время ожидания, так и вторжение.
Тип дверного извещателя	Выберите тип дверного извещателя в зависимости от подключения. НЕТ: дверь считается открытой, когда сигнальная линия дверного извещателя обрвана (разомкнутая цепь). НС: Дверь считается открытой, когда дверной контакт сигнальная линия замкнута (замкнутая цепь).
Вторжение.	Когда и дверной детектор, и система вторжения включены, при аварийном отпирании двери срабатывает сигнализация о вторжении.
Время ожидания двери истекло	Когда время ожидания как дверного детектора, так и двери истекло, при включении срабатывает сигнализация тайм-аута, если дверь открыта дольше заданного тайм-аута. Продолжительность тайм-аута двери может быть настроена в диапазоне от 1 до 9999 секунд.
Время ожидания двери истекло.	
Сигнал тревоги о чрезмерных попытках	Если пароль будет введен неправильно 5 раз подряд в течение 60 секунд или 5 раз подряд будет проведен пальцем по неавторизованной карте, сработает сигнал тревоги.

2.7.3 Настройка состояния блокировки

Процедура

Шаг 1 В главном меню выберите Доступ > Настройка состояния блокировки и нажмите ОК. Шаг 2 Настройка параметров.

Рисунок 2-18 Состояние блокировки

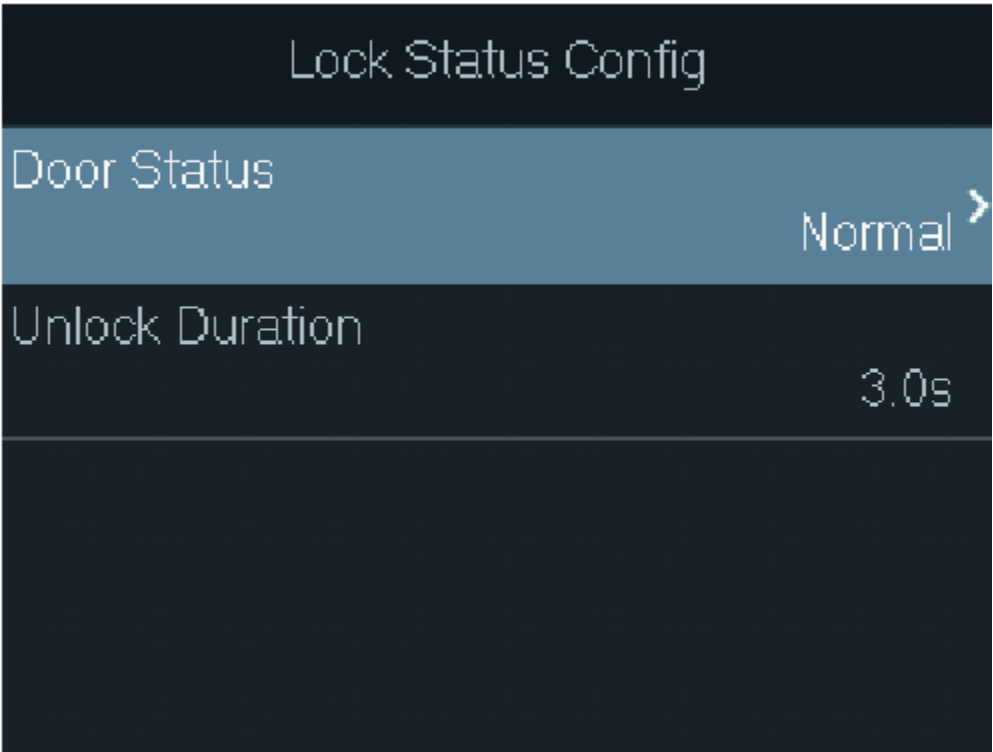


Таблица 2-6 Описание состояния двери

Параметр	Описание
Состояние двери	Нормальное: дверь будет открыта или закрыта в соответствии с настройками. НЕТ: дверь всегда открыта. НС: дверь всегда закрыта.
Продолжительность разблокировки	Продолжительность, в течение которой дверной замок остается открытым по истечении заданного времени.

2.7.4 Настройка интервалов проверки

Процедура

- Шаг 1 В главном меню выберите Доступ > Интервал проверки (сек) и
- Шаг 2 нажмите ОК. 2 Введите интервал и нажмите ОК.

После первоначальной успешной аутентификации для человека будет разрешена его разблокировка или посещаемость и будут созданы соответствующие записи. Если тот же человек попытается повторить аутентификацию в течение установленного времени, дверь не откроется и посещаемость не будет зафиксирована, и никакие записи не будут сгенерированы. Вторичная аутентификация должна быть выполнена после интервал времени истек.

2.7.5 Управление основными картами

Добавление основной карты

В главном меню выберите Доступ> Управление основной картой> Добавить основную карту, нажмите ОК и затем проведите пальцем по карте.

Удаление основной карты.

В главном меню выберите Доступ> Управление основной картой> Удалить основную карту, а затем нажмите ОК, чтобы удалить карту.

Связанные операции

На главном экране, проведя пальцем по основной карте, подождите 3 секунды без каких-либо действий, чтобы перейти в соответствующий режим. Если в течение этих 3 секунд провести пальцем по обычной карте, устройство не ответит.

Устройство определяет функцию на основе общего количества нажатий на основную карту. Как только соответствующий режим будет активирован, проведя пальцем по основной карте один раз, вы выйдете из текущего режима и вернетесь к главному экрану.



Если карта является одновременно основной и пользовательской, система проверяет, является ли она основной картой.

Проведите пальцем по основной карте, чтобы добавить карту пользователя. Проведите пальцем по карточке пользователя, чтобы добавить ее на устройство. Допускается непрерывное добавление.

Дважды проведите пальцем по основной карте, чтобы удалить карту пользователя. Проведите пальцем по карте пользователя, чтобы удалить ее из устройства. Допускается непрерывное удаление.

Проведите пальцем по основной карте 5 раз, чтобы удалить всех пользователей.

2.7.6 Настройка аутентификации по PIN-коду

Процедура

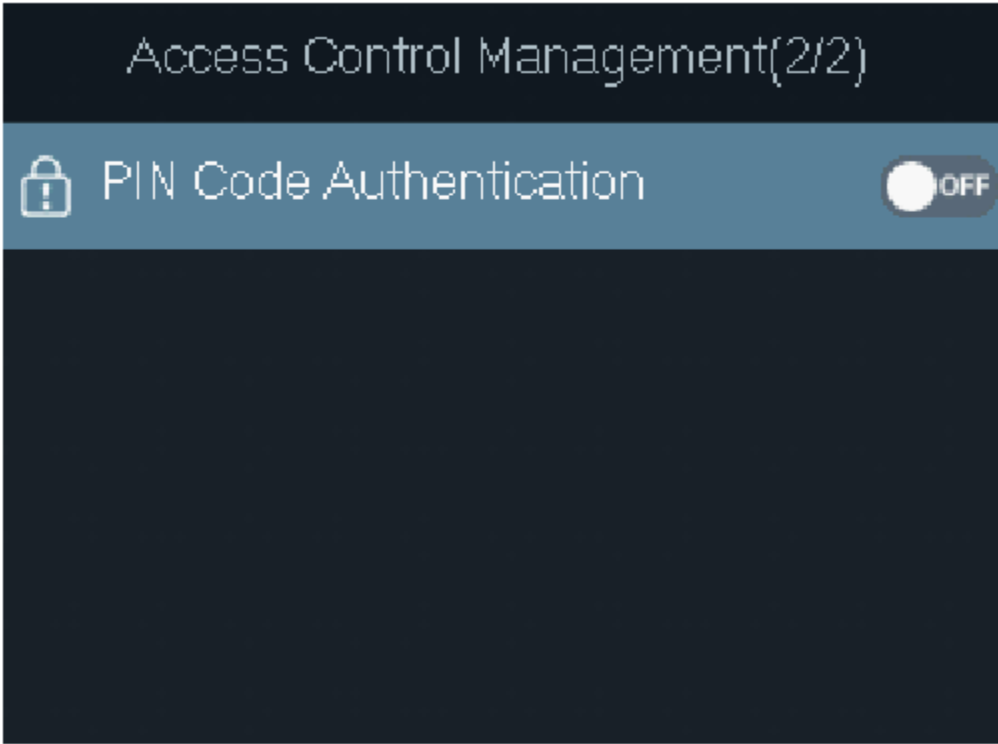
- Шаг 1 В главном меню выберите **Доступ > Аутентификация по PIN-коду**.
- Шаг 2 **Включить или отключить аутентификацию по PIN-коду**.

Аутентификация по PIN-коду по умолчанию отключена. Когда она включена, вы можете только открыть дверь с помощью пароля.



После включения аутентификации по PIN-коду вы можете напрямую ввести их пароль для подтверждения без ввода идентификатора пользователя.

Рисунок 2-19 PIN-код



2.8 Управление посещаемостью

В главном меню выберите пункт **Посещаемость**. Включите сетевую посещаемость или выключите ее.



После ее включения статус посещаемости не может быть настроен и передан платформе.

2.9 Настройки связи

2.9.1 Настройка IP

Настройте параметры IP для устройства.

Процедура

- Шаг 1 В главном меню выберите **Связь> Настройки IP**, а затем нажмите **ОК**.
- Шаг 2 Настройте параметры.

Рисунок 2-20 IP

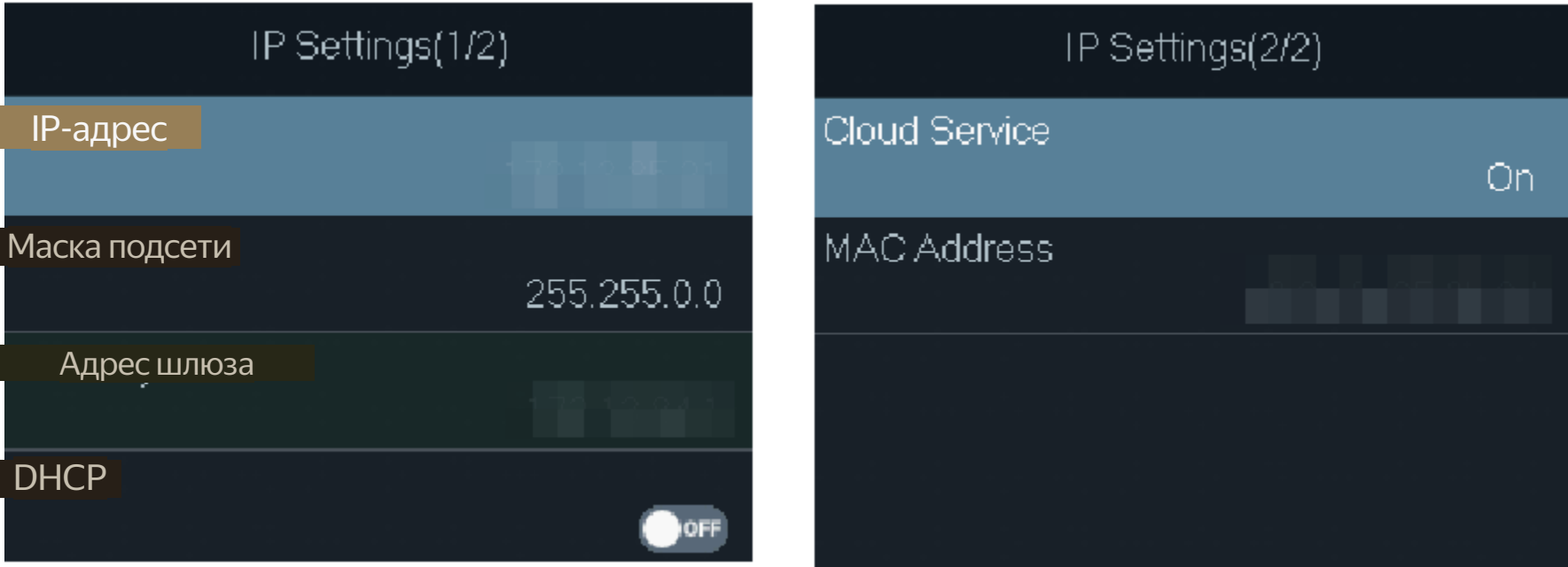


Таблица 2-7 Описание настроек IP

Параметр	Описание
IP - адрес Маска подсети Адрес шлюза MAC-адрес	Введите IP-адрес устройства, маску подсети, адрес шлюза и MAC адрес.
DHCP	Включите функцию DHCP (протокол динамической настройки хоста) для автоматического получения IP-адреса. В этом случае IP-адрес, маску подсети и адрес шлюза установить невозможно.
Облачный сервис	Включите эту функцию, и устройство сможет подключаться к облаку и работать через мобильное приложение.

Шаг 3 Нажмите Esc, а затем OK, чтобы сохранить настройки.

2.9.2 Настройка Wi-Fi

Подключите устройство к сети через беспроводную сеть



Устройства с модулем Wi-Fi имеют эту функцию.

Точка доступа Wi-Fi и функции Wi-Fi являются взаимоисключающими.

Процедура

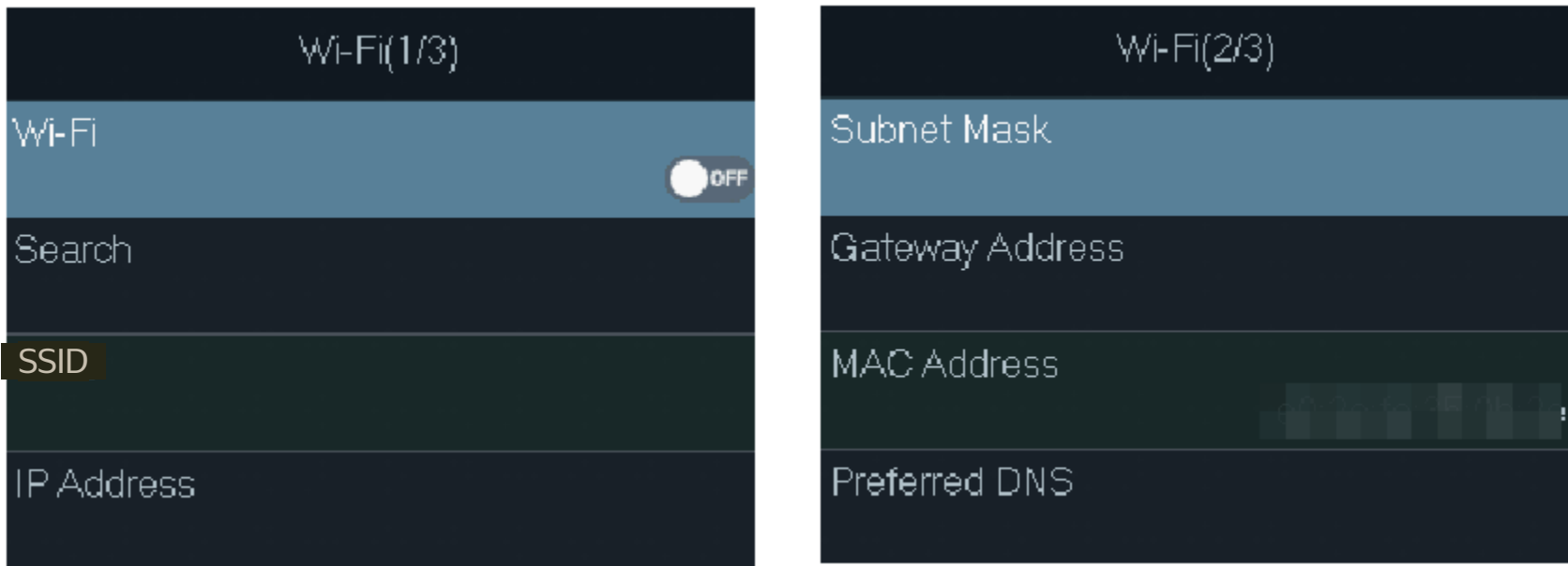
Шаг 1 В главном меню выберите Связь> Wi-Fi, а затем нажмите OK.

Отобразите экран результатов поиска.



Функция готова к обычному использованию через 1 минуту.

Рисунок 2-21 Wi-Fi



Шаг 2 Выберите искомый Wi-Fi и затем нажмите OK.

Шаг 3 Введите пароль Wi-Fi, выберите Подключиться и нажмите OK.

DHCP включен по умолчанию для автоматического получения IP-адреса. Когда DHCP отключен, поддерживается ввод IP-адреса вручную.

Шаг 4 (необязательно) Если Wi-Fi не найден, выберите SSID и нажмите OK, чтобы вручную ввести Wi-Fi Имя.

Результаты

Если и ваш мобильный телефон, и само устройство подключены к одной сети Wi-Fi. Введите IP адрес, отображаемый на экране Wi-Fi, в браузере вашего телефона, чтобы получить доступ к устройству.

2.9.3 Настройка точки доступа Wi-Fi

Поддержка точки доступа Wi-Fi. После включения мобильные устройства могут получить доступ к устройству через точку доступа.



Эта функция доступна на устройствах с модулем Wi-Fi.
Точка доступа Wi-Fi и функции Wi-Fi являются взаимоисключающими.

Неинициализированные устройства автоматически активируют точку доступа Wi-Fi при первой загрузке. Точка доступа автоматически отключите, если ни один клиент не подключится в течение 30 минут.

Процедура

Шаг 1 В главном меню выберите Связь> Точка доступа Wi-Fi, а затем нажмите OK.

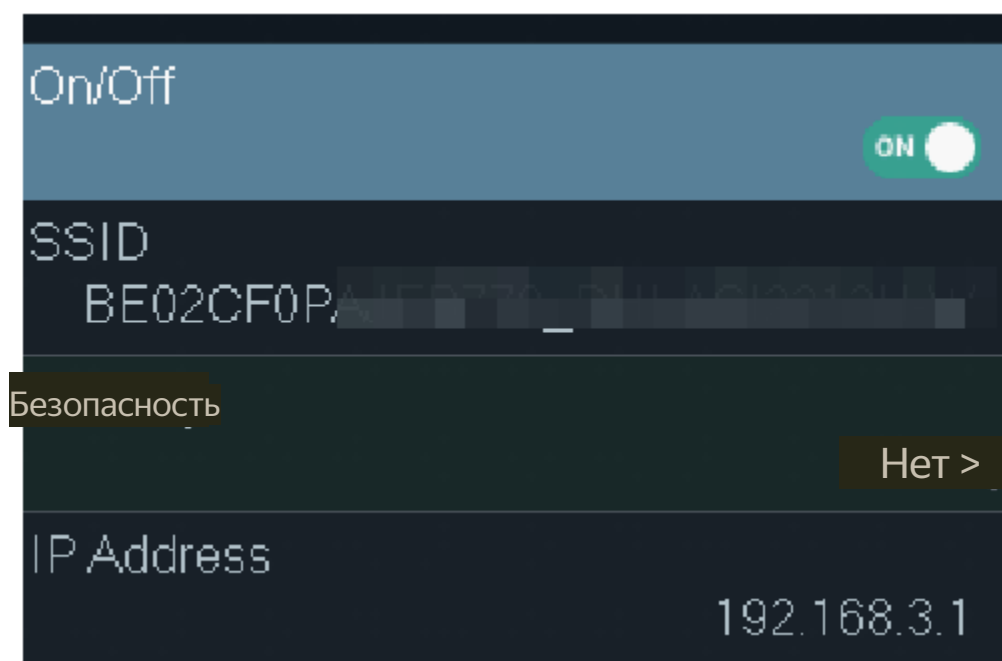
Шаг 2 Выберите Вкл / Выкл, а затем нажмите OK, чтобы включить функцию.

Вы можете изменить SSID и пароль приложения Wi-Fi.



Функция будет готова к обычному использованию через 1 минуту.

Рисунок 2-22 Точка ДОСТУПА Wi-Fi



Шаг 3 (Необязательно) Выберите Безопасность, чтобы настроить пароль точки доступа Wi-Fi.

Значение безопасности по умолчанию - Нет. Введите пароль для подключения к точке доступа.

Результаты

Когда ваш телефон подключится к точке доступа устройства, он автоматически перенаправится на страницу входа в систему. Кроме того, вы можете вручную ввести IP-адрес, отображаемый на экране точки доступа Wi-Fi (IP по умолчанию: 192.168.3.1) в вашем браузере, чтобы получить доступ к устройству.

2.9.4 Настройки режима.

2.9.4.1 Режим контроллера

Устройство функционирует как контроллер доступа и подключается к внешнему считывателю карт access контроллер или модуль безопасности управления дверью.

Процедура

- Шаг 1 В главном меню выберите Связь> Настройки режима и затем нажмите ОК.
- Шаг 2 Установите настройки режима в качестве контроллера доступа.
- Шаг 3 Настройте параметры RS-485 и Wiegand.

Выберите настройки RS-485.

Если вы подключаетесь к другим устройствам через порт RS-485, настройте параметры.

Рисунок 2-23 Контроллер доступа

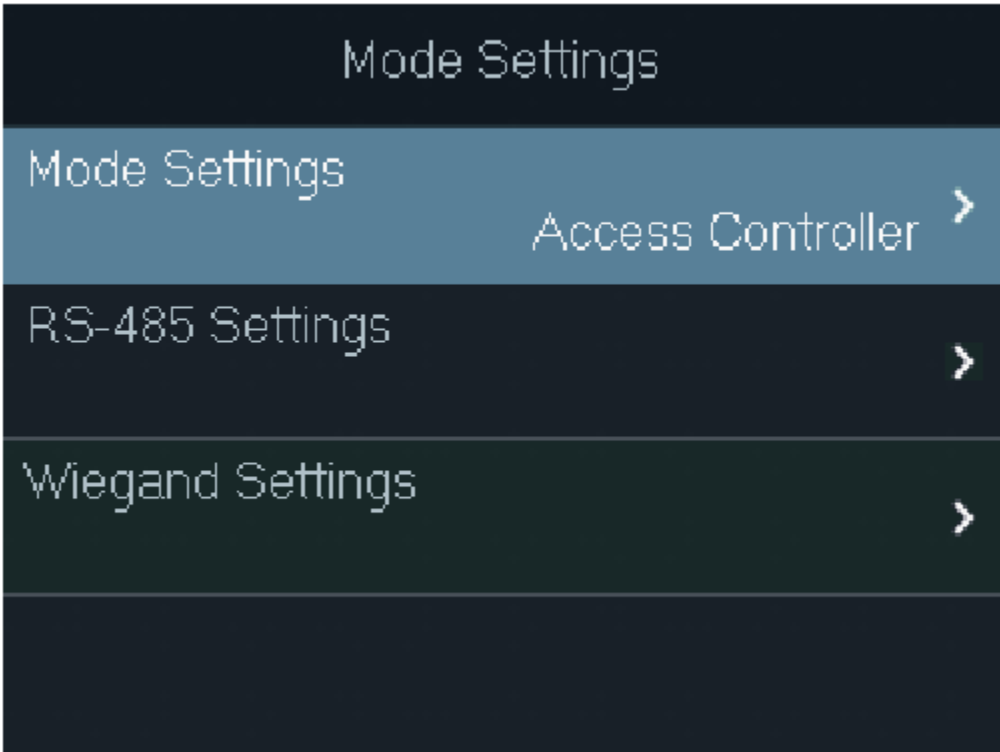


Таблица 2-8 Описание параметров RS-485

Параметр	Описание	Примечание
Контроллер доступа	Подключается к другим контроллерам доступа, когда устройство функционирует как устройство чтения карт, и отправляет данные на другие внешние контроллеры доступа для управления доступом. ID: выводит данные на основе идентификатора пользователя. Номер карты: выводит данные на основе номера карты, когда пользователь проводит пальцем по карте, чтобы разблокировать дверь; выводит данные на основе первого номера карты пользователя, когда он использует другие методы разблокировки.	Если устройство подключено к контроллеру, который проверяет ID, разные разрешения будут выдаваться разным людям контроллером. Если у пользователя есть разрешение к Устройству, он может использовать внешнее устройство для управления доступом. Если у пользователя есть разрешение к Устройству, он может использовать внешнее устройство для управления доступом. Если у пользователя есть разрешение к контроллеру, он может использовать устройство для управления доступом.
Устройство чтения карт памяти	Устройство функционирует как контроллер доступа и подключается к внешнему устройству чтения карт памяти.	

Параметр	Описание
Модуль защиты двери	Кнопка выхода из двери, замок и противопожарный рычаг не действуют после включения модуля безопасности. Поддерживает аутентификацию с помощью лица, карты, отпечатка пальца или пароля на этом устройстве для управления разблокировкой модуля безопасности двери. Поддерживает аутентификацию через внешний считыватель карт RS-485, подключенный к модулю безопасности системы управления дверью (провода по карте) или через внешнюю кнопку для управления разблокировкой модуля безопасности двери.
Модуль расширения замка	Выбран модуль расширения, устройство подключено к модулю расширения дверного замка. При блокировке аутентификация устройства разблокирует только локальную блокировку, в то время как аутентификация внешнего устройства чит карт разблокирует блокировку расширения. После выбора на странице настройки параметров контроля доступа и сигнализации, дверной канал поддерживает выбор двери 2, и соответствующие параметры для двери 2 могут быть настроены.
Устройство чтения (OSDP)	Устройство подключается к устройству чтения карт по протоколу OSDP, которое отправляет информацию о карте доступа к контроллеру доступа или платформе управления.

Выберите настройки Wiegand.

- Вход Wiegand: при подключении внешнего устройства чтения карт выберите Wiegand **Вход**.

Номер карты. Инверсия: если последовательность номеров карт, полученная с помощью ввода Wiegand не совпадает с фактической последовательностью номеров карт при взаимодействии со сторонним на сторонних устройствах включите эту функцию.

- Вывод Wiegand: когда устройство работает как устройство чтения карт, и вам необходимо подключить его к другому контроллеру доступа и выберите Конфигурацию вывода Wiegand.

Таблица 2-9 Описание Wiegand

Параметр	Описание
Wiegand Тип вывода	Разрядность номеров карт или ID, которые устройство может распознать и вывести. Wiegand 26: считывает 3 байта или 6 цифр. Wiegand 34: считывает 4 байта или 8 цифр. Wiegand 66: считывает 8 байт или 16 цифр.
Длительность импульса	Настройте ширину импульса и интервал для вывода wiegand.

Параметр	Описание
Интервал импульсов	
Тип выходных данных	Выберите формат Wiegand для считывания номеров карт или удостоверений личности. Идентификатор пользователя: выводит данные на основе идентификатора пользователя. Карта: выводит данные на основе первого номера карты пользователя.
Формат Wiegand	Если тип выходных данных задан как ID, вы можете выбрать десятичный или шестнадцатеричный форматы вывода.

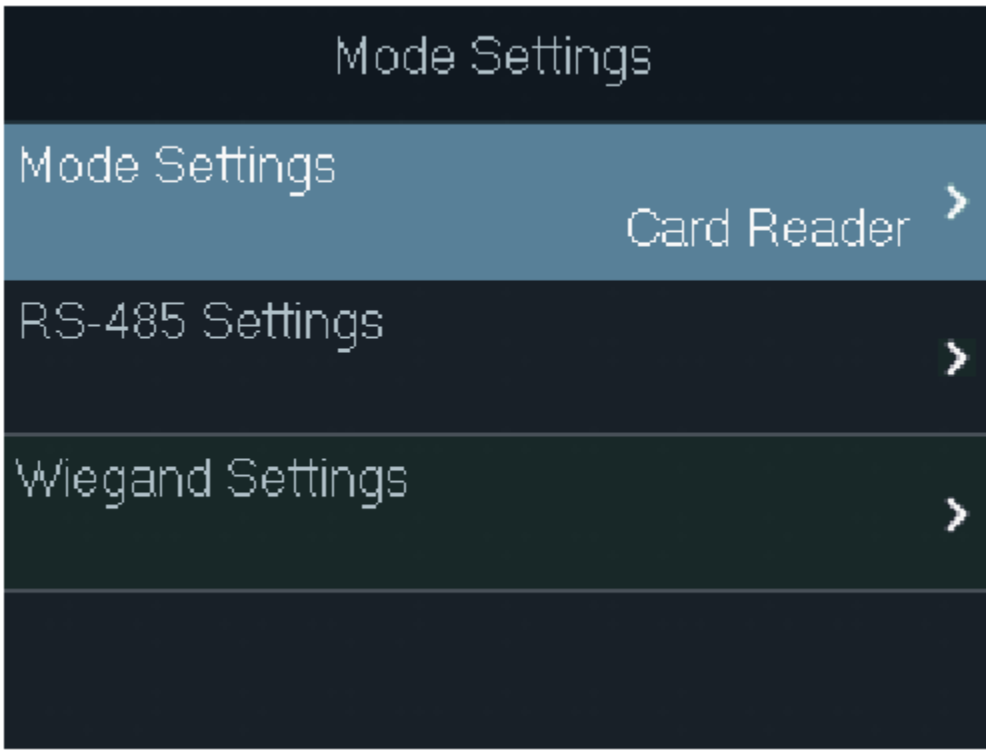
2.9.4.2 Режим чтения карт памяти.

Когда устройство функционирует как устройство чтения карт, подключенное к внешнему контроллеру доступа, оно не выполняет аутентификацию локально. Вместо этого оно напрямую передает данные контроля доступа в систему доступа контроллер, который затем обрабатывает аутентификацию и запускает разблокировку двери.

Процедура

- Шаг 1
- В главном меню выберите Связь> Настройки режима и затем нажмите ОК.
- Шаг 2
- Установите настройки режима в качестве устройства чтения карт памяти.**

Рисунок 2-24 Режим устройства чтения карт памяти

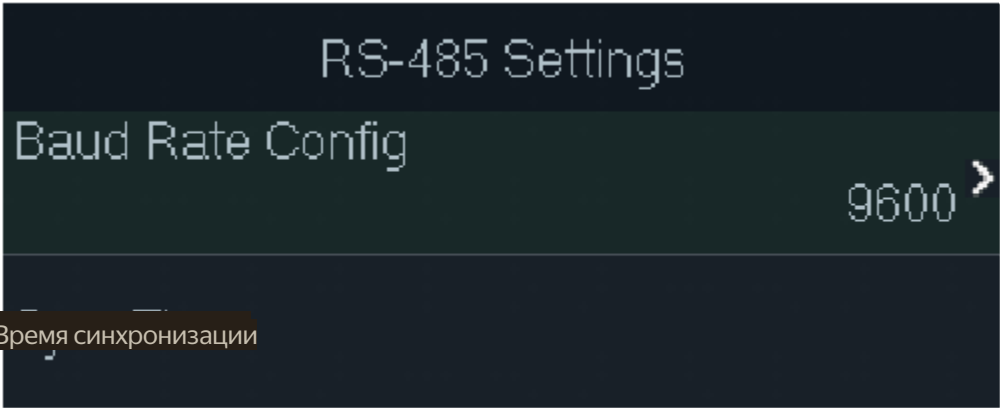


Шаг 3 Настройте параметры RS-485 и Wiegand.

Выберите настройки RS-485.

- Конфигурация скорости передачи данных в бодах: 9600 по умолчанию, которую можно изменить.
- Время синхронизации: отрегулируйте время работы устройства в зависимости от объема внешнего контроллера.После подключения внешнего контроллера доступа (модели H или J), синхронизируйте время этого устройства на основе времени внешнего контроллера.

Рисунок 2-25 RS-485

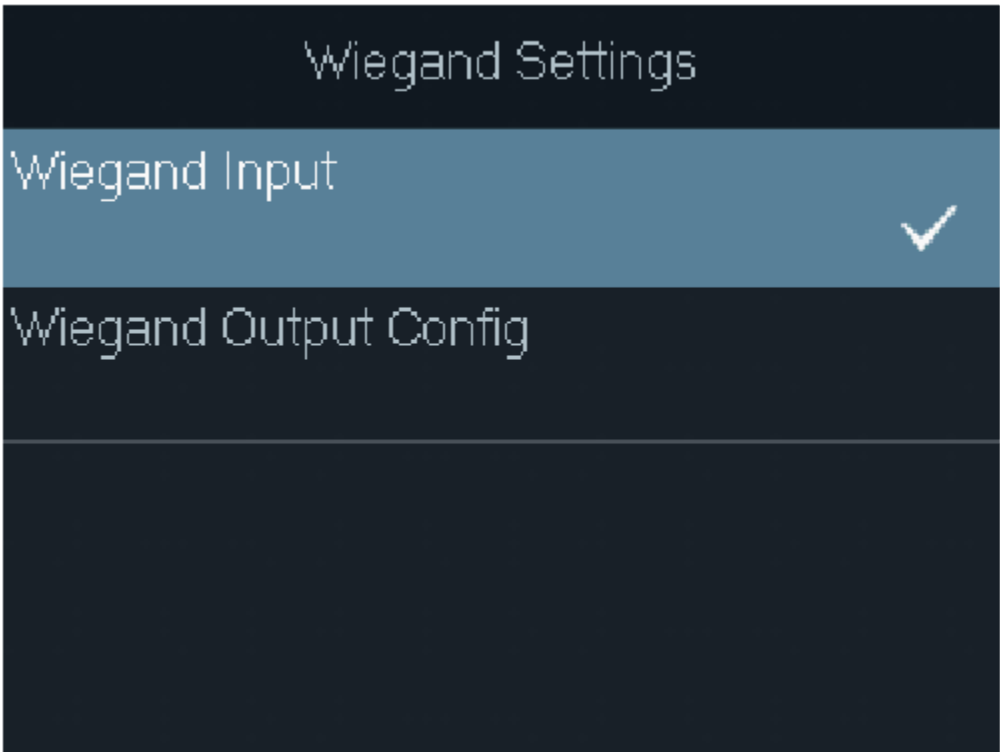


Выберите настройки Wiegand.

Разрядность номеров карт, которые устройство может распознавать и выводить.

- ◇ о Wiegand 26: считывает 3 байта или 6 цифр.
- Wiegand 34: считывает 4 байта или 8 цифр.
- ◇ Wiegand 66: считывает 8 байт или 16 цифр.

Рисунок 2-26 Wiegand



2.10 Системные настройки

2.10.1 Настройка времени

Настройте отображение системного времени и синхронизацию в соответствии с предпочтениями пользователя.

Процедура

- Шаг 1 В главном меню выберите Система> Время, а затем нажмите ОК.
- Шаг 2 Настройте параметры.

Рисунок 2-27 время

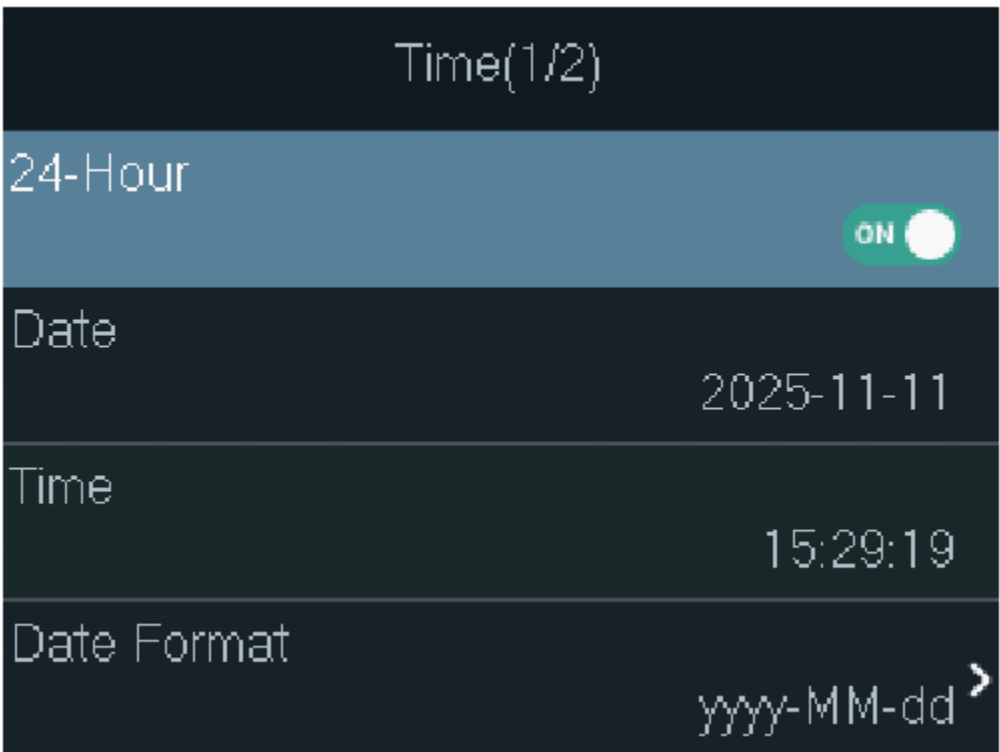


Таблица 2-10 Описание параметра time

Параметр	Описание
24-часовой режим	Нажмите < /> или ОК, чтобы включить или выключить 24-часовой формат. При включении время будет отображаться в 24-часовом формате; при выключении время будет отображаться в 12-часовом формате.
Дата	1.Нажмите A /\, чтобы выбрать дату, а затем нажмите ОК. 2.Введите дату и затем нажмите ОК.
Время	1.Нажмите A /\, чтобы выбрать время, а затем нажмите ОК. 2.Введите время и затем нажмите ОК.
Формат даты.	1.Нажмите A /\, чтобы выбрать формат даты. 2.Нажмите < /> или ОК, чтобы выбрать формат.
Часовой пояс	1.Нажмите A /\, чтобы выбрать часовой пояс. 2.Нажмите < /> или ОК, чтобы выбрать часовой пояс.

2.10.2 Настройка громкости

Процедура

- Шаг 1

В главном меню выберите Система > Громкость, а
- Шаг 2

затем нажмите ОК. Настройте параметры.



Параметры могут отличаться в зависимости от модели устройства.

Рисунок 2-28 Громкость

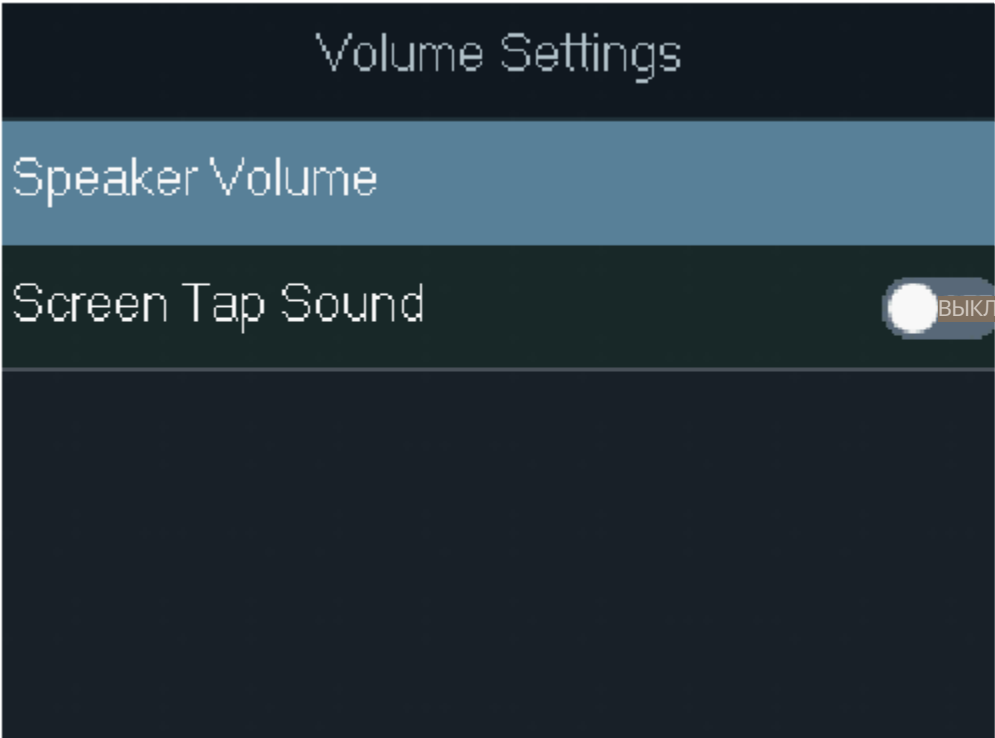


Таблица 2-11 Описание громкости

Параметр	Описание
Громкость динамика	Выберите громкость динамика, нажмите ОК и нажмите A, V, > или <, чтобы отрегулировать громкость. Доступно только на некоторых моделях.
Коснитесь экрана ЗвукВключите его, и при нажатии клавиш появится запрос времени.	

2.10.3 Настройка языка

Процедура

- Шаг1 В главном меню выберите Система> Язык, а затем нажмите ОК.
- Шаг 2Выберите нужный вам язык и нажмите ОК.
- По умолчанию это английский.

2.10.4 Настройка параметров экрана

Процедура

- Шаг 1 В главном меню выберите Система> Настройки экрана, а затем нажмите ОК.
- Шаг 2 Настройка параметров.

Рисунок 2-29 Настройки экрана

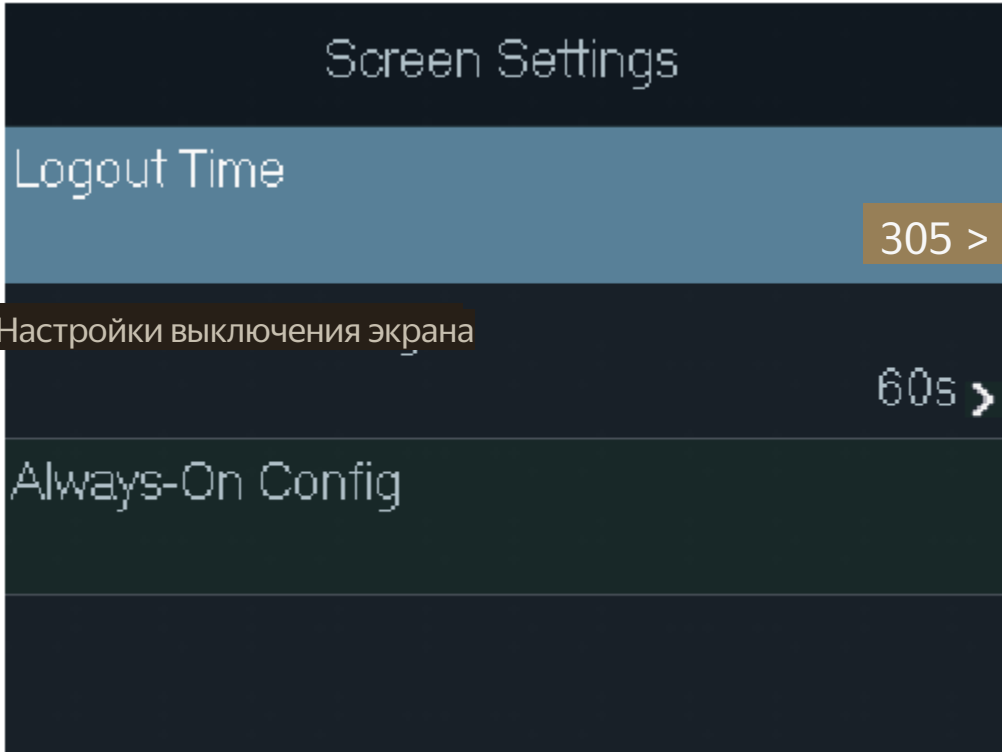


Рисунок 2-30 Всегда включен

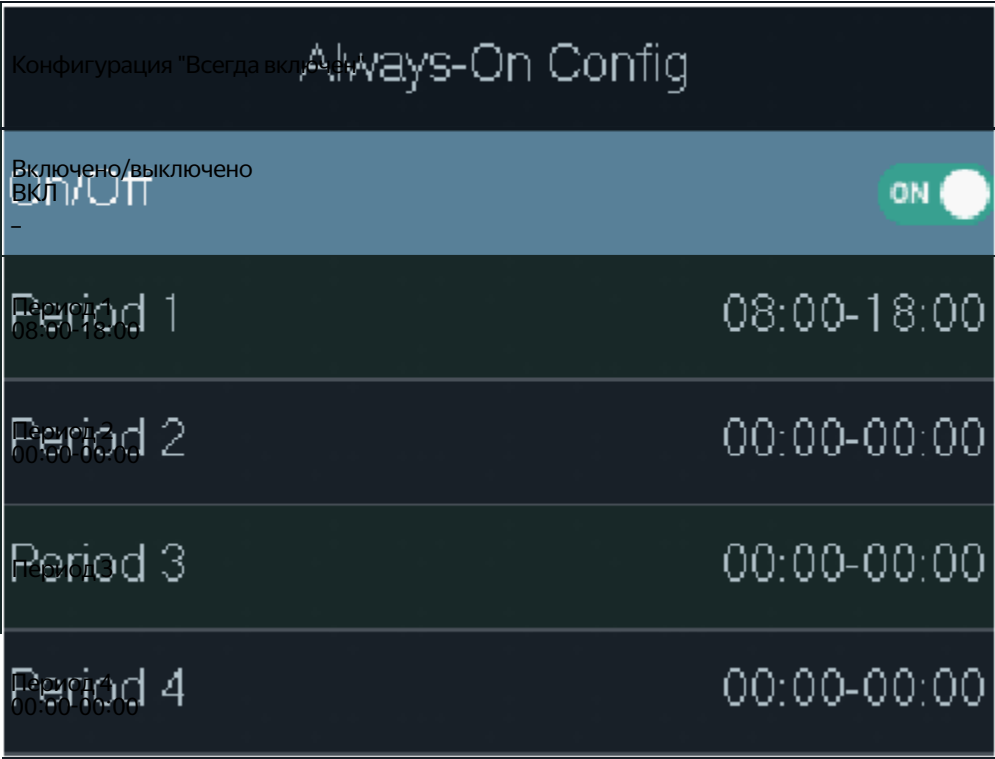


Таблица 2-12 Описание параметров экрана

Параметр	Описание
Время выхода из системы	Если ни с одним из интерфейсов не выполняется никаких операций более установленного времени, система возвращается к интерфейсу заставки.
Настройки выключения экрана	Если ни с одним из интерфейсов не выполняется никаких операций, система сначала возвращается к интерфейсу заставки. Если общее время бездействия достигает установленной продолжительности и оно выходит за пределы периода постоянного включения экрана, система переходит в режим отключения экрана. Если в течение периода постоянного включения экран тускнеет, продолжая отображать изображение заставки.
Постоянно включенная настройка	Включите его и настройте период "всегда включен". В течение этого периода времени экран всегда включен. Сохранение экрана включенным в течение длительного времени. периоды могут повлиять на срок ее службы. Рекомендуется ограничить общее ежедневное время постоянного просмотра экрана не более чем 8 часами.

2.10.5 Настройка параметров карты памяти

Справочная информация



Только устройства с IC поддерживают эту функцию.

Процедура

- Шаг 1

В главном меню выберите Система > Настройки
- Шаг 2

карты и нажмите OK. Настройте параметры.

Рисунок 2-31 Настройки карты

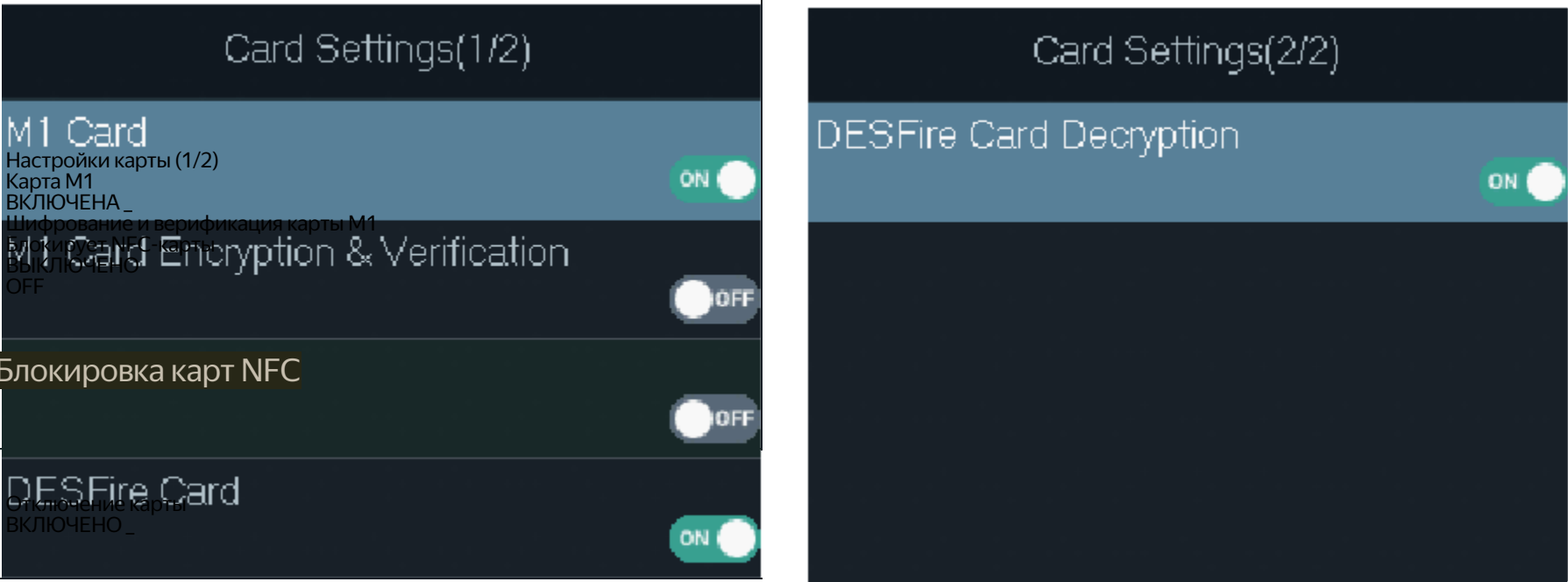


Таблица 2-13 Описание параметров карты

Параметр	Описание
Карта M1	
Шифрование карты M1 & Проверка	Только устройства с IC поддерживают эту функцию. Включите ее, и устройство сможет считывать серийный номер карты M1 и ID. Она включена по умолчанию. Включите шифрование и проверку карты M1 после того, как вы включите карту M1. Поддерживается только считывание карты M1.
Блокируйте NFC-карты.	Только устройства с IC поддерживают эту функцию. Только определенные телефоны поддерживают эту функцию. После включения IC-карты включите блокировку NFC-карт, чтобы предотвратить несанкционированный доступ, заблокировав открытие дверей картами, скопированными с NFC.
Отключите NFC-карту.	
Шифрование карты DESFire	Только устройства с IC поддерживают эту функцию., и принимаются только ше номера карт. Включите эту функцию, и устройство сможет считывать физический серийный номер (UID) карты DESFire card. После включения карты DESFire включите шифрование карты DESFire устройство может считывать содержимое карт DESFire.

2.10.6 Управление паролем устройства

2.10.6.1 Изменение пароля администратора

Процедура

- Шаг 1 В главном меню выберите Система> Пароль устройства> Изменить пароль, а затем нажмите ОК.
- Шаг 2 Введите старый пароль, новый пароль и затем подтвердите П.
- Шаг 3 Нажмите ОК, чтобы сохранить настройки.
- Новый пароль становится действительным сразу после изменения.

2.10.6.2 Изменение зарезервированного адреса электронной почты

Процедура

- Шаг 1 В главном меню выберите Система> Пароль устройства> Изменить зарезервированную информацию и затем нажмите ОК.
- Шаг 2 Введите зарезервированный адрес электронной почты и нажмите ОК.

2.10.7 Восстановление заводских настроек по умолчанию.



Восстановление заводских настроек по умолчанию приведет к потере данных. Пожалуйста, действуйте с осторожностью.

Восстановление настроек программного обеспечения

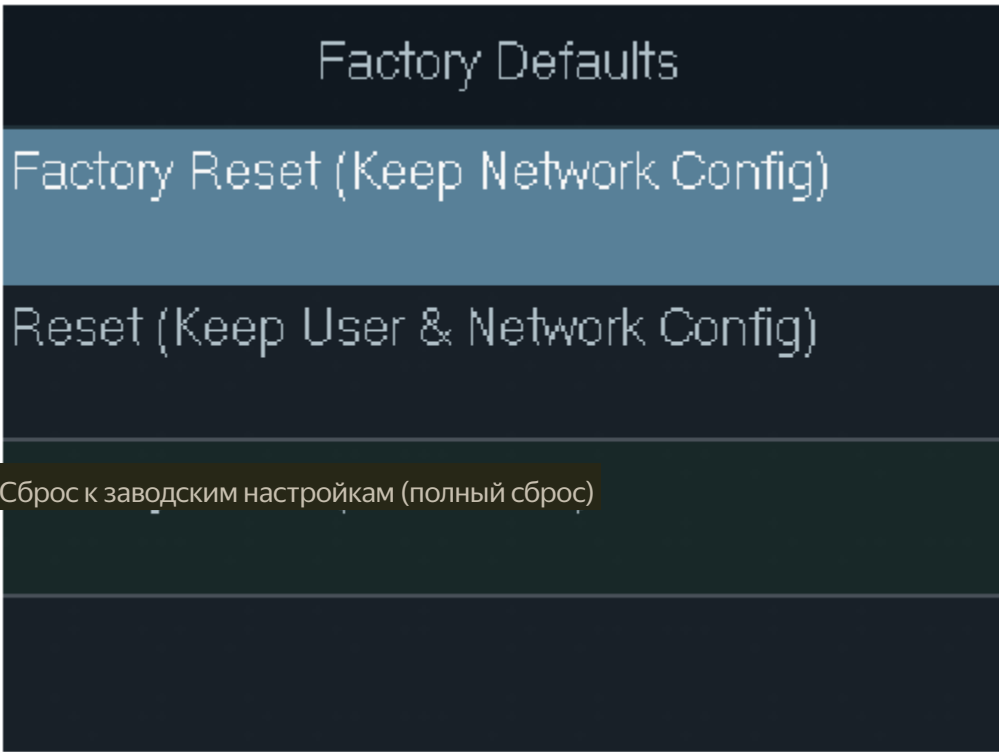
В главном меню выберите Система> Заводские настройки по умолчанию, а затем нажмите ОК.

Сброс к заводским настройкам (сохранить конфигурацию сети): восстанавливает все настройки до заводских значений по умолчанию, кроме сети конфигурация.

Сброс (сохранить конфигурацию пользователя и сети): восстанавливает все настройки до заводских значений по умолчанию, кроме пользовательских данных и конфигурация сети.

Сброс к заводским настройкам (полный сброс): все конфигурации и данные будут возвращены к заводским настройкам по умолчанию.

Рисунок 2-32 Заводские настройки по умолчанию



Аппаратный Сброс

Устройство поддерживает сброс к заводским настройкам с помощью кнопки защиты от несанкционированного доступа или точечного отверстия для сброса (если доступно).

Кнопка защиты от несанкционированного доступа: в течение 5 минут после запуска устройства нажмите кнопку защиты от несанкционированного доступа нажмите 5 раз подряд в течение 8 секунд. В интерфейсе ожидания отобразится сброс к заводским настройкам запрос; нажмите ОК или нажмите и удерживайте кнопку защиты от несанкционированного доступа в течение нескольких секунд. После того, как устройство перезагрузится, сброс будет успешным. Все конфигурации и информация будут восстановлены до заводских настроек.

Отверстие для сброса: в течение 5 минут после запуска устройства замкните отверстие для сброса.

- ♦ Короткое замыкание в течение 500 миллисекунд устройство подает звуковой сигнал, затем отключает устройство короткого замыкания. После перезагрузки устройства сброс будет успешным. За исключением информации о пользователе, журналов и IP настройки, все остальные конфигурации будут восстановлены до заводских настроек.
- ♦ Короткое замыкание в течение 5 секунд устройство подает звуковой сигнал, затем отключает устройство короткого замыкания. После устройство перезапустится, сброс будет успешным. Все конфигурации и информация будут восстановлены заводские настройки.

Только на некоторых устройствах есть точечное отверстие для сброса.

2.10.8 Устройство для сброса настроек.

В главном меню выберите Система> Сброс, а затем нажмите ОК.

2.11 Управление USB

2.11.1 Экспорт данных

После установки USB-накопителя экспортируйте данные с устройства на USB-накопитель. Некоторые экспортированные данные зашифрованы и не могут быть отредактированы.

Предварительные требования

USB-накопитель вставлен в устройство и распознан должным образом.

Поддерживаемые форматы USB-накопителя - FAT32 емкостью от 4 до 128 ГБ.

Процедура

- Шаг 1

Шаг 2
- В главном меню выберите USB> USB Export и нажмите ОК. Выберите тип данных, которые необходимо экспортировать, и нажмите ОК.

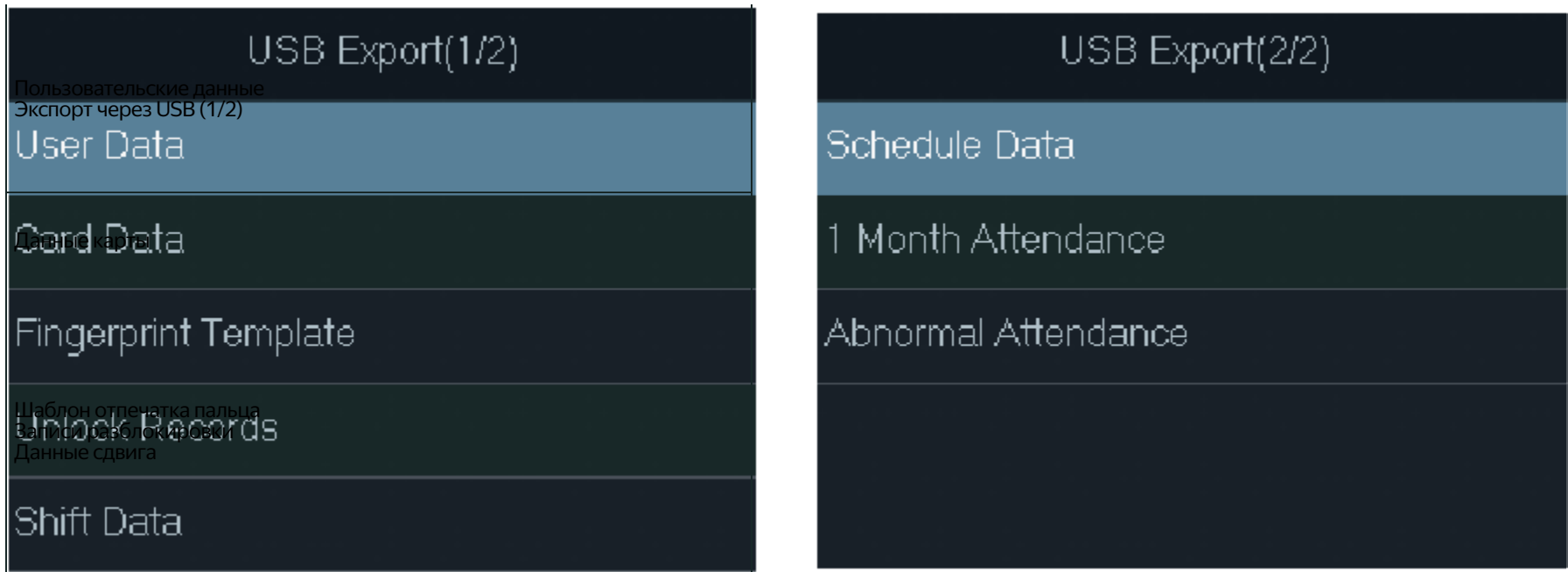
Экспортированная информация будет сохранена на USB-накопителе.

Если

экспортированные данные представлены в формате Excel, их можно редактировать

Данные пользователя, данные карты и данные отпечатка пальца экспортируются в зашифрованном виде.

Рисунок 2-33 Экспорт по USB



2.11.2 Импорт данных

Только данные, экспортированные с одного устройства, могут быть импортированы на другое устройство.

Предварительные требования

USB-накопитель вставлен и правильно распознан устройством.

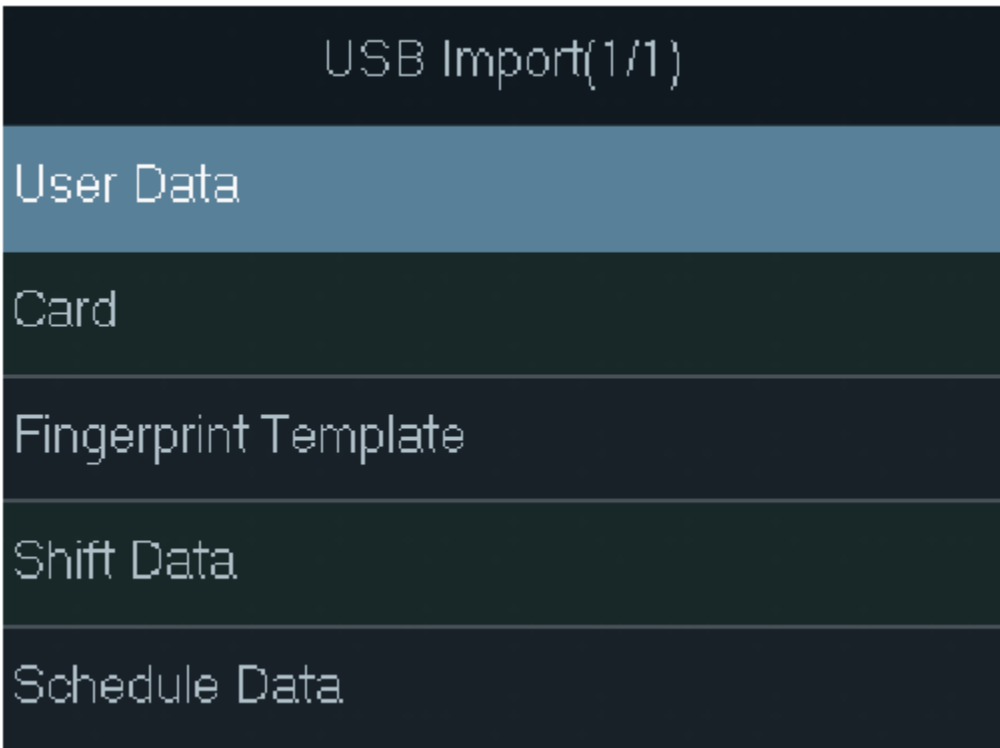
Процедура

- Шаг 1 В главном меню выберите USB> USB Импорт, а затем нажмите OK.
- Шаг 2 Выберите тип данных, который необходимо импортировать, и нажмите OK



Рекомендуется импортировать данные между устройствами одной модели и версии. Импорт данных между разными моделями или версиями может привести к потере данных.

Рисунок 2-34 Импорт через USB



2.11.3 Устройство обновления

Выполняйте обновление системы с помощью USB-накопителя.



Для новых устройств или после сброса настроек резервные копии системных файлов создаются в течение первых 10 минут после запуска. Обновление в течение этого времени не рекомендуется.

Процедура

Шаг 1 Переименуйте файл обновления в update.bin и сохраните его в корневом каталоге USB-накопителя.
Вставьте USB-накопитель в устройство.

Шаг 2 Войдите в главное меню устройства.

Шаг 3 Выберите USB> Обновление по USB, а затем нажмите ОК.

На экране отобразится запрос на подтверждение.

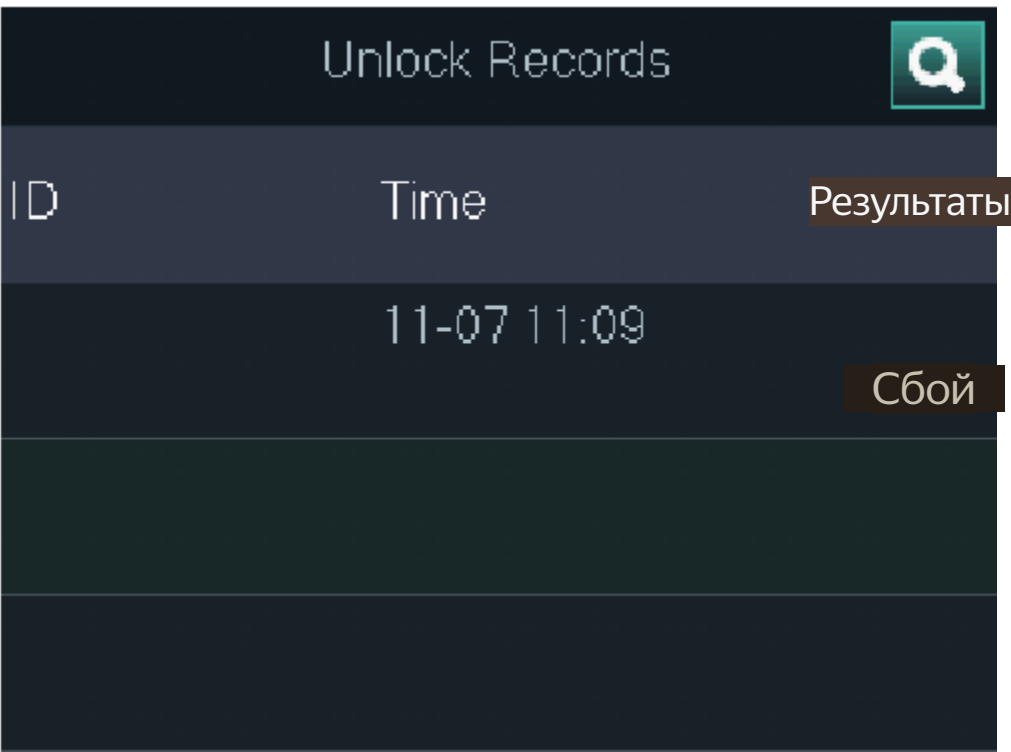
Шаг 4 Пресса ОК для обновления.

Обновление системы началось. Устройство автоматически перезагрузится после завершения обновления по завершении.

2.12 Управление записями

В главном меню выберите пункт Записи, а затем нажмите ОК, чтобы просмотреть записи разблокировки.

Рисунок 2-35 Записи разблокировки



2.13 Просмотр информации

2.13.1 Просмотр объема данных

В главном меню выберите Информация > Объем данных, а затем нажмите ОК, чтобы просмотреть объем данных, например, пользователь, карта, емкость отпечатка пальца устройства.

2.13.2 Версия устройства просмотра

В главном меню выберите Информация > Емкость данных, а затем нажмите ОК, чтобы просмотреть SN устройства, MAC адрес, версию программного обеспечения и другую информацию.

Выберите SN, нажмите ОК. Отобразится QR-код, отсканируйте его с помощью мобильного приложения, чтобы добавить устройство.

Выберите Documentation QR, нажмите ОК. Отобразится QR-код, отсканируйте его, чтобы просмотреть руководство пользователя руководство пользователя.



Поддерживается только на некоторых моделях.

3 Локальные операции (модели с сенсорным экраном)

- Конфигурации могут отличаться в зависимости от конкретного продукта.
Внешние модули расширения доступны только на некоторых моделях.
- Вы можете увидеть некоторые тексты пользовательского интерфейса не отображаются из-за ограниченного пространства. Нажмите и удерживайте текст для 3 секунд, и он покажет.

3.1 инициализация

Для первого использования или после восстановления заводских настроек по умолчанию вам необходимо установить пароль и связать свой адрес электронной почты для учетной записи администратора. Вам также необходимо установить часовой пояс устройства. Вы можете использовать учетную запись администратора для входа в главное меню устройства, настройки устройства и входа в систему веб-браузер и SmartPSS Lite.



- Если вы забыли пароль администратора, отправьте запрос на сброс на свой зарезервированный адрес электронной почты. В пароль должен состоять из 8-32 непустых символов и содержать по крайней мере два типа следующие символы: верхний и нижний регистры, цифры и специальные символы (за исключением "" и &). Установите пароль высокого уровня безопасности, следуя подсказке о надежности пароля.

3.2 Внешний вид.

Устройство представляет собой модель с сенсорным экраном, которая требует работы на экране.

Рисунок 3-1 Внешний вид



3.3 Главный экран

Вы можете разблокировать дверь с помощью карт, паролей, отпечатков пальцев, Bluetooth (некоторые способы разблокировки методы доступны только на избранных моделях). Методы разблокировки могут отличаться в зависимости от моделей продукта.

Вы можете изменить тему главного экрана только через веб-страницу устройства. В этом разделе в качестве примера используется общий режим.



Данное руководство предназначено только для справки. Могут быть обнаружены небольшие различия между основным экраном в этом руководстве и самим устройством.

Рисунок 3-2 Главный экран



Таблица 3-1 Описание главного экрана

No.	Description
1	Displays the connection status of Wi-Fi, Wi-Fi AP, wired network, USB drive, and Bluetooth.  Only certain models support Wi-Fi and Wi-Fi AP.
1	Display the current date, time, day of the week, and unlocking method.
3	Unlock by password. Supports user password, temporary password, or public password.
4	Main menu. Select the verification method to go to the main menu.

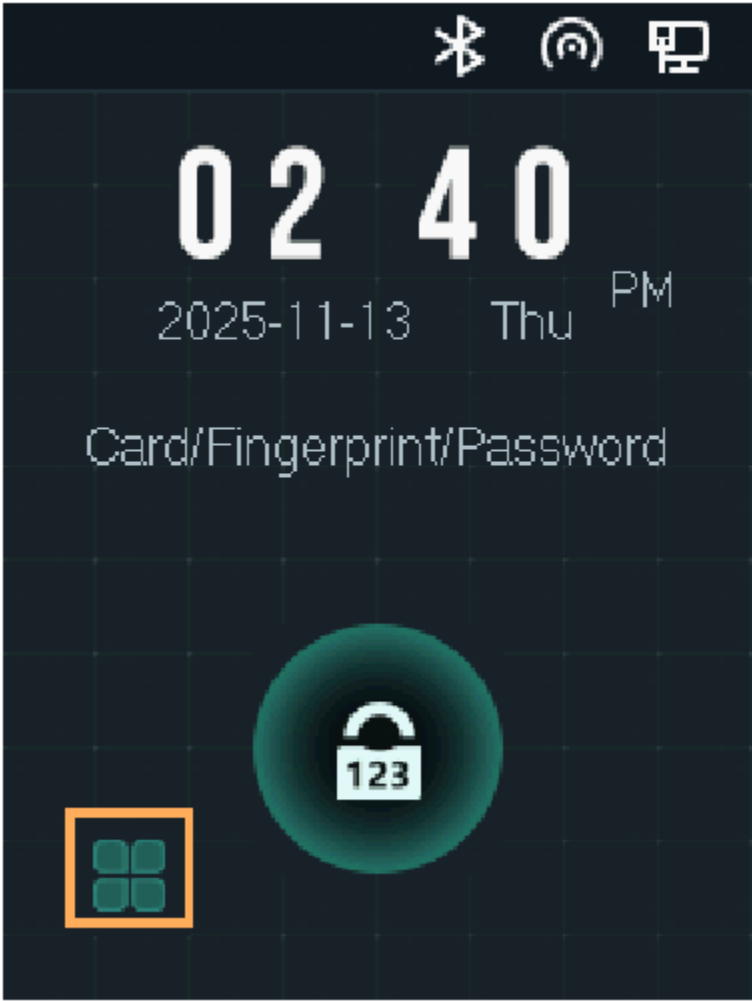
3.4 Вход в главное меню

Войдите в главное меню, чтобы настроить устройство. Войти в главное меню устройства могут только учетная запись администратора . При первом использовании используйте учетную запись администратора для входа в экран главного меню, а затем вы можете создать другие учетные записи администратора.

Процедура

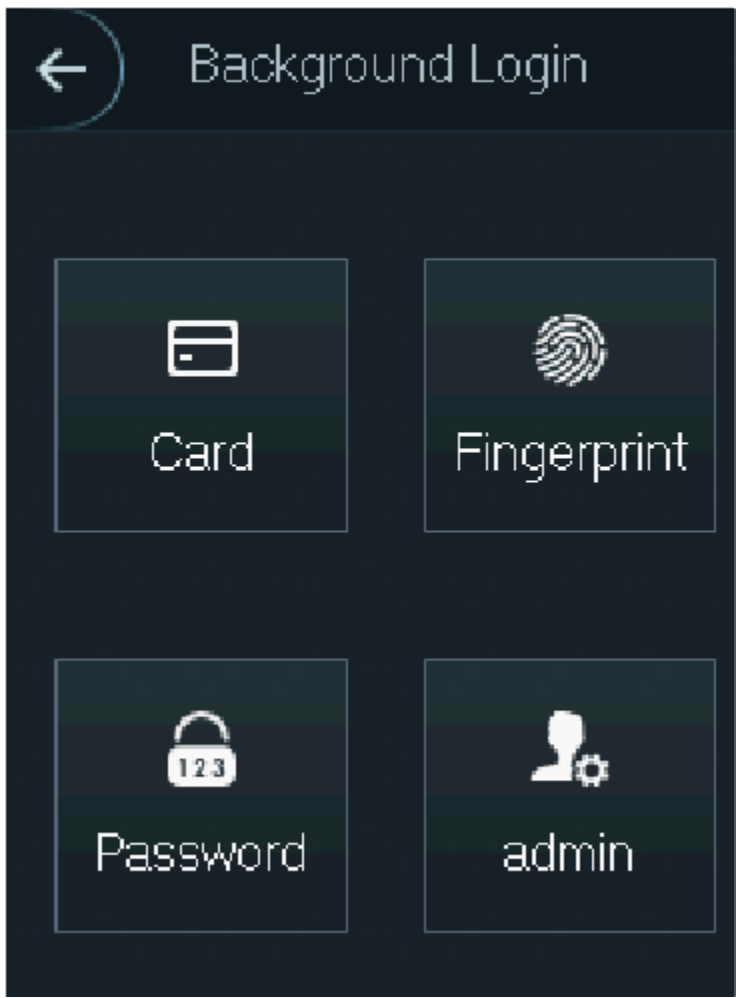
- Шаг 1
- На экране ожидания коснитесь 

Рисунок 3-3 Экран ожидания



- Шаг 2
- Выберите методы проверки.

Рисунок 3-4 Методы проверки



Отпечаток пальца: После успешного распознавания отпечатка пальца администратора вы можете перейти в главное меню.



Поддерживается только на некоторых моделях.

Пролистывание карточки: После успешного распознавания карточки администратора вы можете перейти к главное меню.

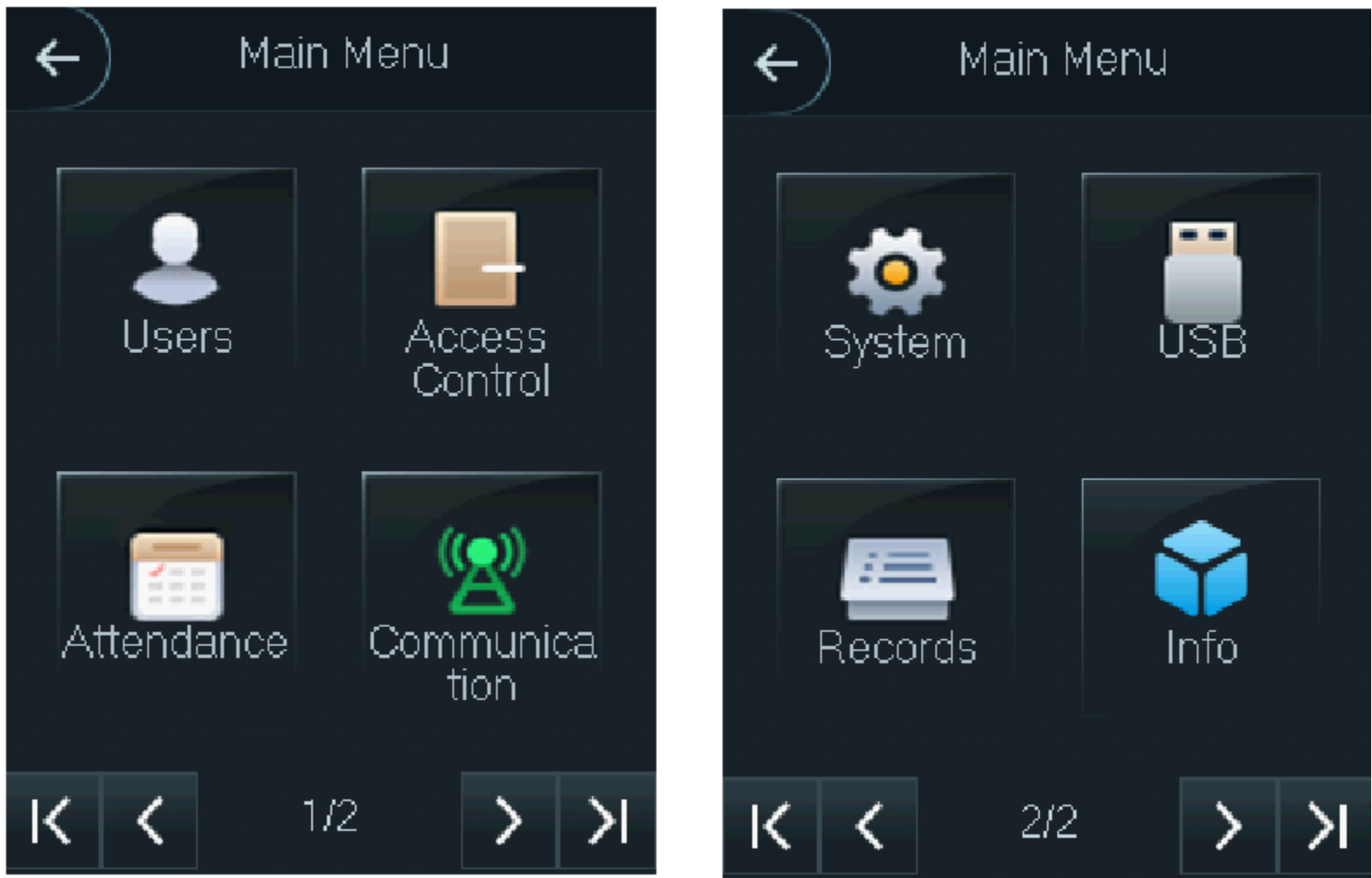
Пароль: Введите идентификатор администратора и пароль для перехода в главное меню.

Администратор: Введите пароль администратора, чтобы перейти в главное меню.

Результаты

После успешной аутентификации вы можете перейти в главное меню устройства.

Рисунок 3-5 Главное меню



3.5 Сброс пароля

Если пароль для входа в систему для пользователя admin забыт, пароль можно сбросить с помощью следующие два способа.

Вы настроили зарезервированный адрес электронной почты

- 1. Нажмите и удерживайте экран ожидания в течение 1,5 секунд.
- 2. Нажмите "Администратор", а затем коснитесь один раз пустой области экрана.
- 3. **Нажмите Забыли пароль.**
- 4. Прочитайте приглашение на экране, а затем нажмите Ввод.
- 5. Коснитесь QR-кода, а затем отсканируйте QR-код.
- 6. Отправьте результаты сканирования на указанный адрес электронной почты.
- 7. Введите защитный код.



Если неверный код безопасности будет введен 5 раз подряд, учетная запись администратора будет заблокирована на 5 минут.

8. Нажмите кнопку Далее.

9. Сбросьте и подтвердите пароль.



Пароль должен состоять из 8-32 непустых символов и содержать по крайней мере два из символы следующих типов: верхний регистр, нижний регистр, цифра и специальный символ (за исключением ' " ; : &). 10. Нажмите ОК.

Вы не настроили зарезервированный адрес электронной почты

1. Нажмите и удерживайте экран ожидания в течение 1,5 секунд.

2. Нажмите администратор, а затем коснитесь один раз пустой области экрана.

3. Нажмите Забыли пароль.

4. Следуйте подсказке на экране, чтобы связаться с местным руководителем, службой технической поддержки или справкой.

3.6 Способы разблокировки.

3.6.1 Карта

Поместите карту в область прокрутки, чтобы разблокировать дверь.



Эта функция доступна только на некоторых моделях.

3.6.2 Отпечаток пальца

Приложите палец к сканеру отпечатков пальцев.



Эта функция доступна только на избранных моделях.

3.6.3 Bluetooth

Вы можете разблокировать дверь по Bluetooth через приложение DMSS.



Эта функция доступна только на избранных моделях.

Подготовьте следующие действия.

Bluetooth включен. Дополнительные сведения см. в разделе "3.10.4 Настройка Bluetooth".

В Устройство добавлено в приложение DMSS. Дополнительные сведения см. в соответствующем руководстве пользователя.

Разблокируйте дверь через приложение DMSS.

Успешно разблокированная голосовая подсказка означает, что дверь открывается и вы можете войти.

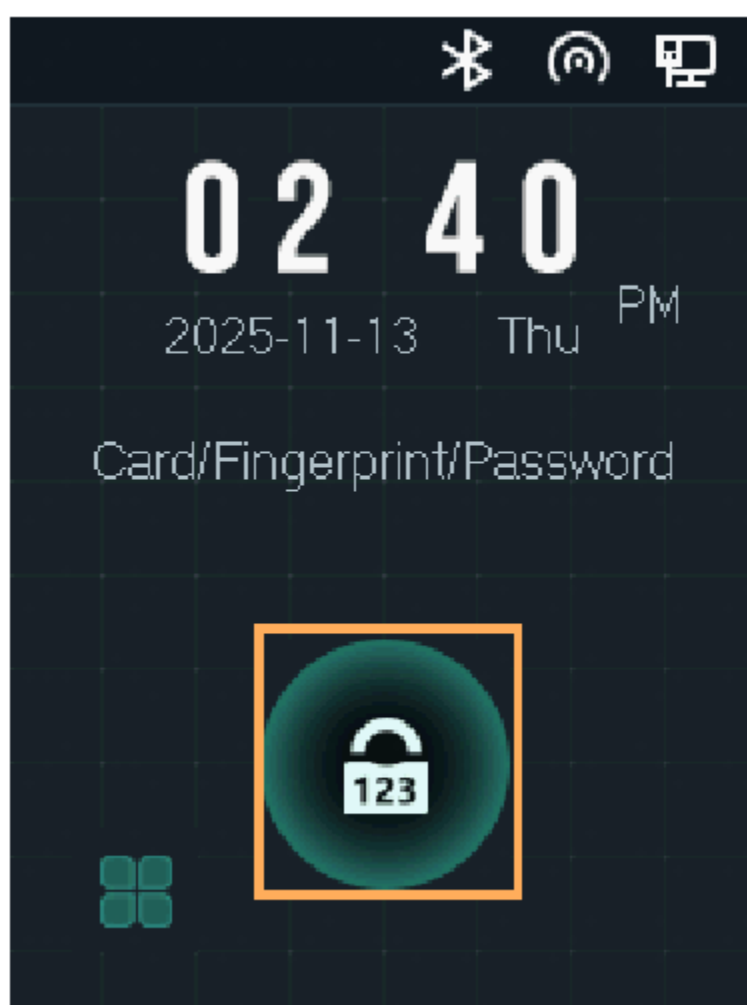
3.6.4 Пароль пользователя

Введите идентификатор пользователя и пароль, чтобы разблокировать дверь.

Процедура

Шаг 1 Коснитесь  на главном экране.

Рисунок 3-6 Главный экран



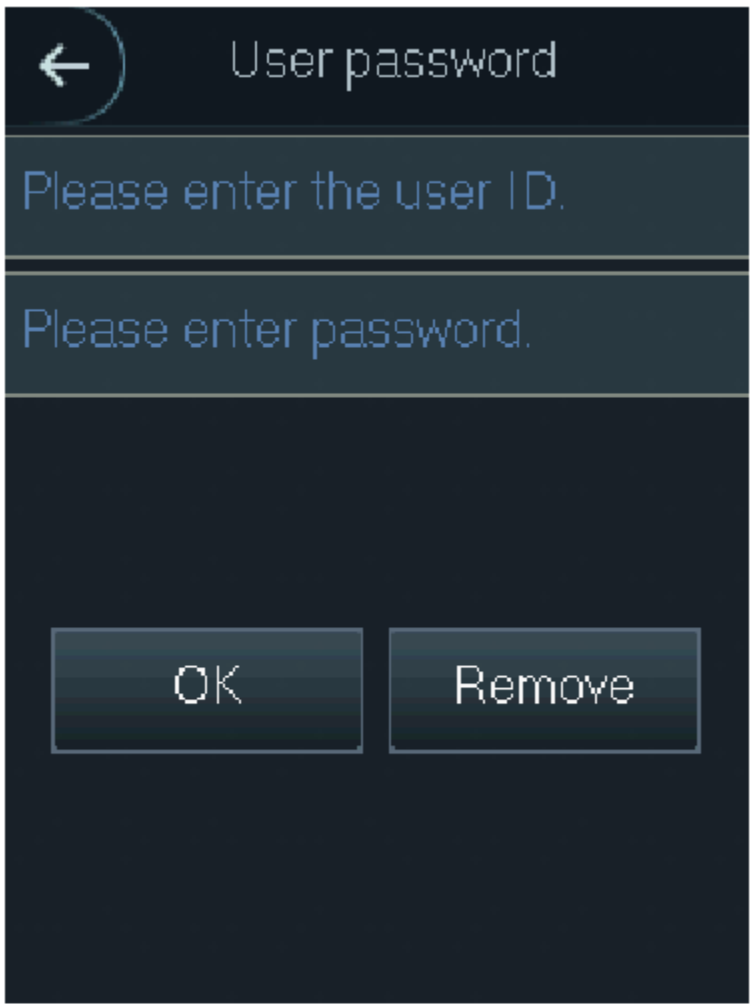
Шаг 2 Коснитесь Пароль пользователя.

Шаг 3 Введите зарегистрированный или выданный идентификатор пользователя и пароль, а затем нажмите OK.

После успешной проверки дверь можно открывать.

Если включена аутентификация по PIN-коду, вы можете ввести пароль пользователя для разблокировки двери.

Рисунок 3-7 Пароль пользователя



3.6.5 Общедоступный пароль

Для разблокировки двери введите только общедоступный пароль. Дверь можно разблокировать с помощью общедоступного пароль, за исключением всегда закрытой двери. Одно устройство допускает только один общедоступный пароль.

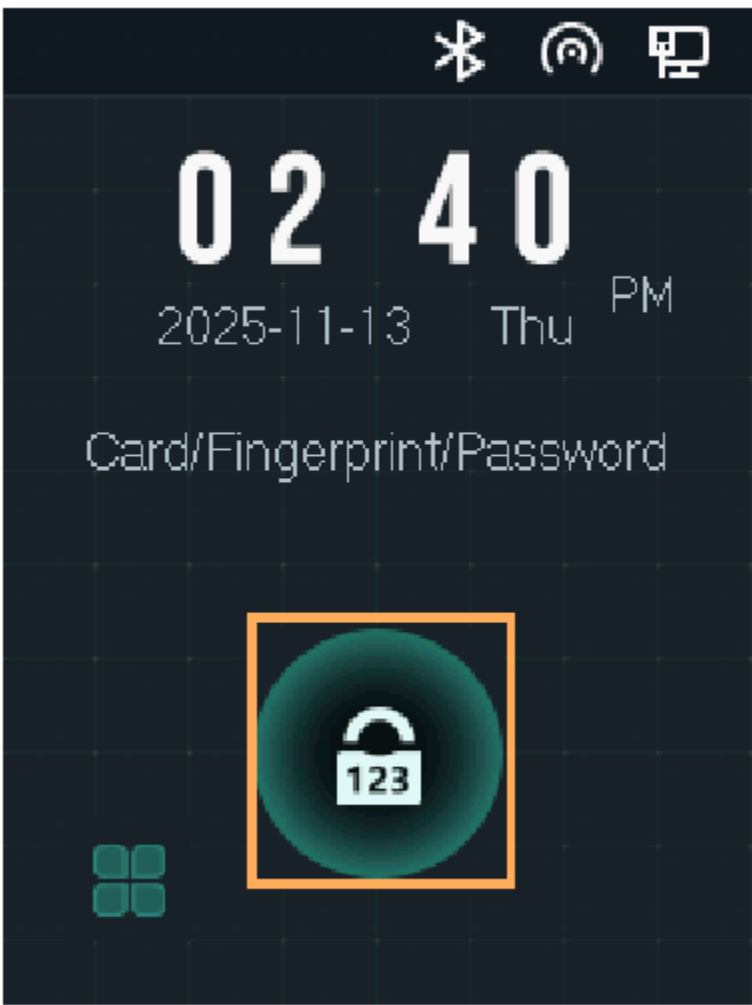
Предварительные требования.

Общий пароль был настроен. Подробности см. в разделе "3.7.3 Настройка общего пароля".

Процедура

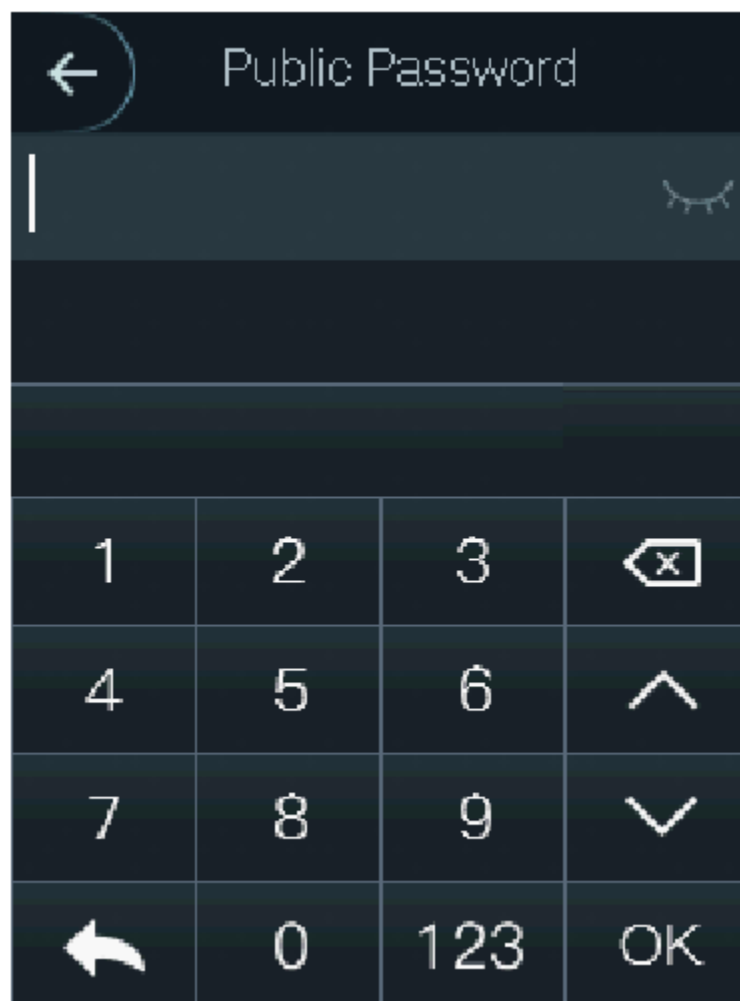
- Шаг 1 Коснитесь  главного экрана.

Рисунок 3-8 Главный экран



- Шаг 2 Коснитесь общего пароля.
- Шаг 3 Введите общедоступный пароль и затем нажмите ОК.
После успешной проверки дверь можно открывать.

Рисунок 3-9 Общедоступный пароль



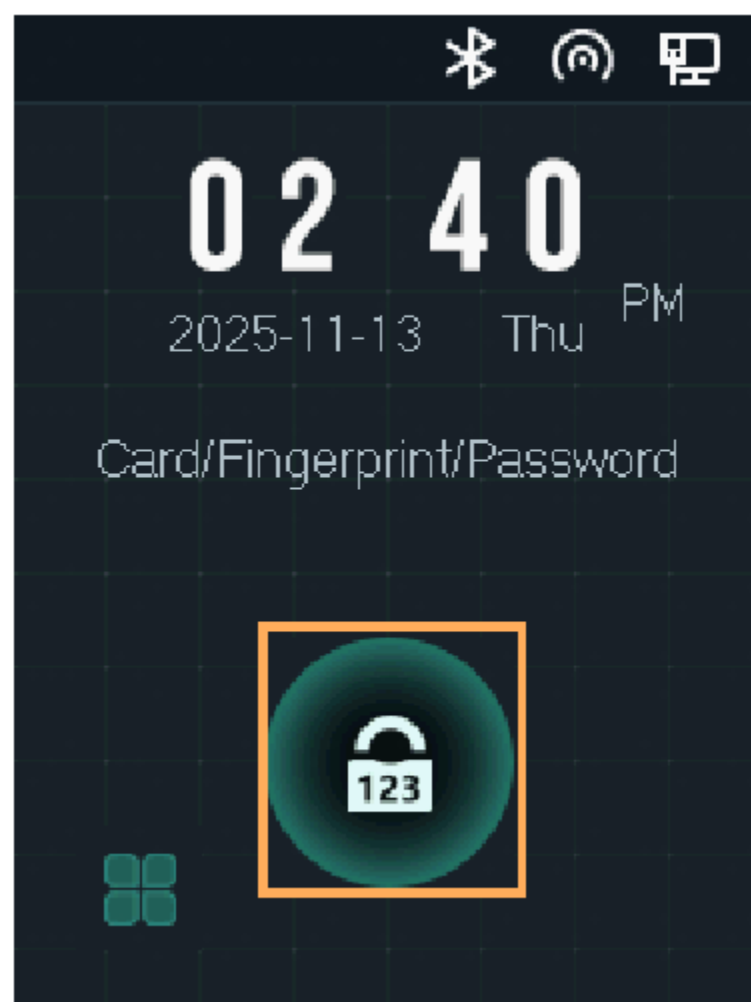
3.6.6 Временный пароль

Разблокируйте дверь с помощью временного пароля.

Процедура

- Шаг 1 Коснитесь  на главном экране.

Рисунок 3-10 Главный экран

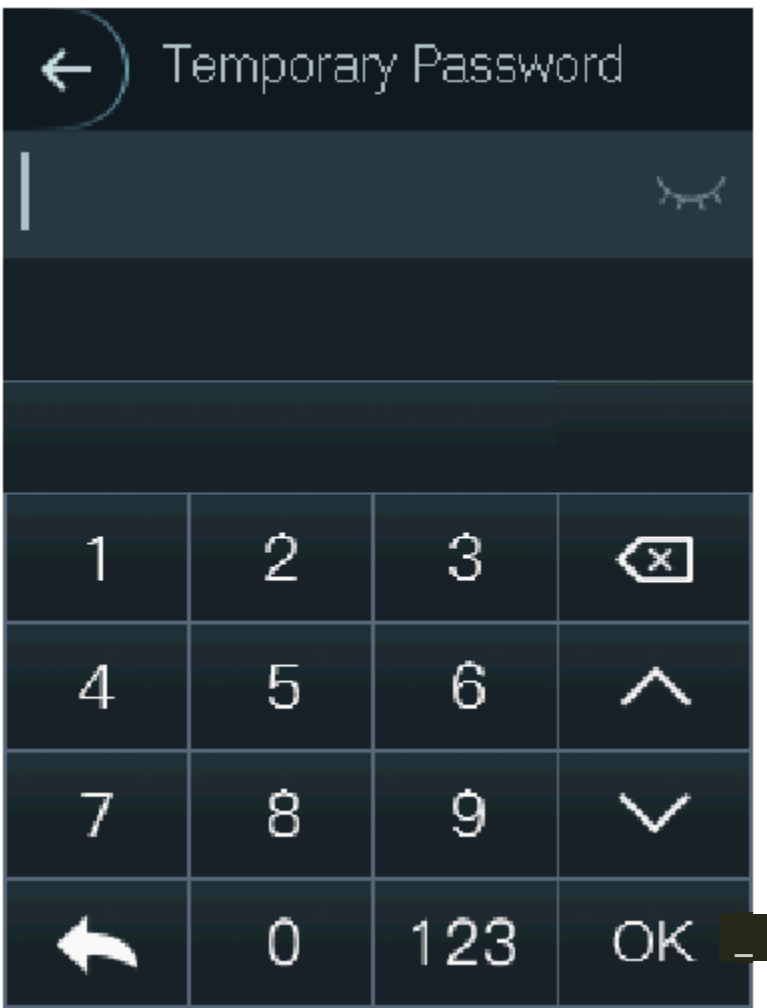


- Шаг 2

Коснитесь **Временный пароль.**
- Шаг 3

Введите временный пароль, а затем нажмите ОК.
- После успешной проверки дверь может быть открыта.

Рисунок 3-11 Временный пароль



3.7 Управление персоналом

Вы можете добавлять новых пользователей, просматривать список пользователей/администраторов и редактировать информацию о пользователе.



Изображения в этом руководстве приведены только для справки и могут отличаться от фактического продукта.

3.7.1 Добавление пользователей

Процедура

- Шаг 1

Войдите в систему с учетной записью администратора, а затем выберите Пользователи> Список пользователей.



Экраны в этом руководстве приведены только для справки и могут отличаться от фактического продукт.



- Шаг 2

Коснитесь  в правом верхнем углу, а затем настройте пользовательские параметры.

Рисунок 3-12 Добавление пользователей

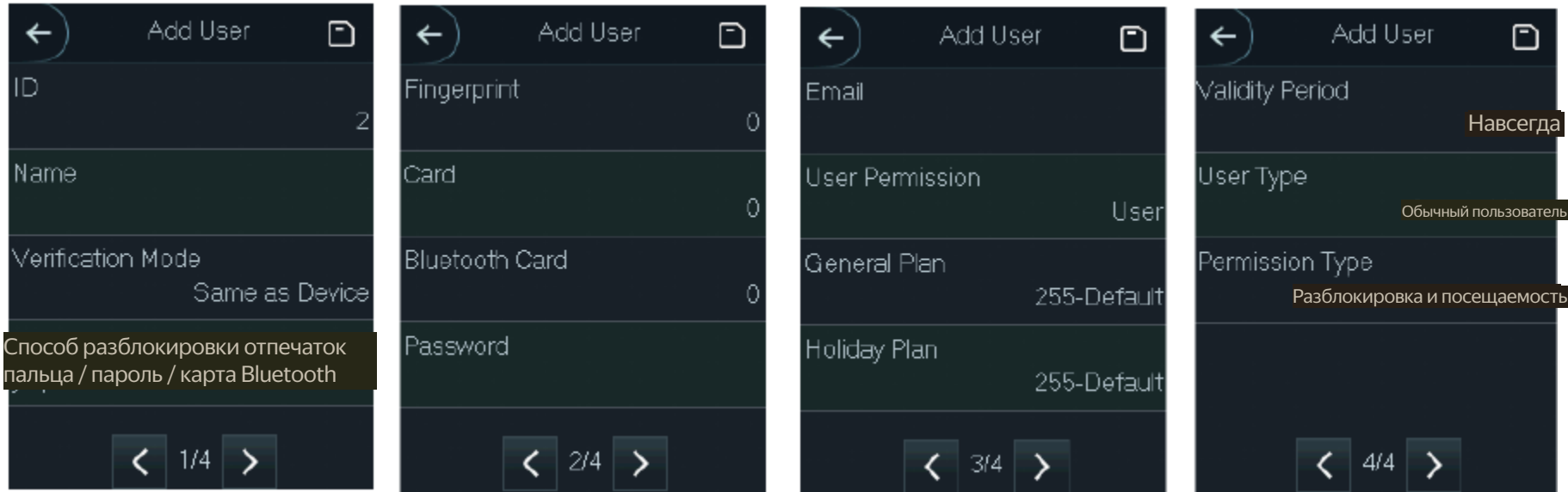


Таблица 3-2 Описание параметров пользователя

Параметр	Описание
ID _	Каждый идентификатор пользователя уникален. Это может быть 18 символов цифр, 0-9 и их комбинации.
Имя	Введите имя (не более 32 символов, включая цифры, символы и буквы).
Режим проверки.	Поддерживает настройку методов проверки для каждого сотрудника.
Метод разблокировки	Такой же, как у устройства: персонал будет использовать для аутентификации настроенный метод проверки. Пользовательский: аутентификация персонала будет проводиться с использованием методов. Выберите Пользовательский и выберите Метод разблокировки, нажмите OK. Выберите комбинационный элемент и комбинированный метод. Пользовательский метод разблокировки поддерживает только аутентификацию локального персонала и не работает с внешними кард-ридерами. Если пользовательский метод проверки противоречит методу устройства по умолчанию, приоритет отдается пользовательской конфигурации.
Отпечаток пальца	Каждый пользователь может добавить до 3 отпечатков пальцев. Следуйте инструкциям и голосовым подсказкам, чтобы добавить отпечатки пальцев. Вы можете включить функцию принудительного снятия отпечатков пальцев под каждым отпечатком пальца. После включения функции принудительной сигнализации сработает сигнализация, если дверь будет отперта по отпечатку пальца принудительно. Мы не рекомендуем устанавливать первый отпечаток пальца в качестве принудительного отпечатка пальца. Только определенные модели поддерживают функцию отпечатка пальца.
Карта	Вы можете зарегистрировать 5 карт для каждого пользователя. На странице регистрации проведите своей картой по кард-ридеру, после чего информация о карте будет считана устройством. Вы можете включить функцию принудительной карты на странице регистрации карт. После включения функции принудительной сигнализации будет срабатывать сигнализация, если дверь отпирается принудительной картой.

Параметр	Описание
Карта Bluetooth	Вы можете зарегистрировать 5 карт Bluetooth для каждого пользователя. На странице Регистрация карт Bluetooth выберите запрос по электронной почте или регистрационный код , чтобы зарегистрировать свою карту Bluetooth.
Пароль	Введите пароль пользователя. Максимальная длина пароля составляет 8 цифр. Принудительный пароль состоит в добавлении 1 на основе последней цифры пароля разблокировки. Например, если пароль пользователя равен 12345, то принудительный пароль будет равен 12346; если пароль пользователя равен 789, а затем принудительный пароль равен 780. Сигнализация о принудительном вводе будет срабатывать, если введен пароль для принудительного ввода.
Электронная почта	Введите адрес электронной почты, который используется для сброса пароля.
Тип разрешения	Вы можете выбрать разрешение пользователя для нового пользователя. У обычных пользователей есть только разрешение на разблокировку дверей. Администраторы могут настроить устройство и разблокировать дверь.
Общий план	Пользователь может иметь доступ к двери только в течение определенного периода. Значение по умолчанию равно 255, что означает, что период не настроен.
План отпуска	Пользователь может иметь доступ к двери только в течение запланированных праздников. Значение по умолчанию равно 255, что означает, что план на отпуск не настроен.
Период действия	Укажите период, в течение которого пользователь имеет контроль доступа к двери.
Тип пользователя	Общие: Обычные пользователи могут разблокировать дверь в обычном режиме. Список блокировок: Когда пользователи из списка блокировок открывают дверь, обслуживающий персонал получает уведомление. Гость: Гости могут отпирать дверь в течение определенного периода времени или на определенное количество раз. По истечении установленного периода или по истечении времени отпирания они не смогут отпереть дверь. Патрулирование: Условно-досрочно освобожденные пользователи могут отслеживать с помощью устройства, у них нет прав на разблокировку. VIP: Когда VIP-пользователи открывают дверь, они не ограничены режимами разблокировки, такими как мультикарта и раздел времени. Другие: Когда они откроют дверь, она останется незапертой еще 5 секунд. Пользовательский пользователь 1/2: То же, что и обычный.

Шаг 3 Нажмите Esc, а затем ОК, чтобы сохранить настройки.

3.7.2 Просмотр информации о пользователе и администраторе

Запросите пользователей или администраторов на устройстве и измените или удалите информацию о пользователе или информацию об администраторе.

Параметр	список пользователей используется для отображения всей информации о пользователе на текущем устройстве.
Параметр	список администраторов используется для отображения всей информации об администраторе на текущем устройстве.

Войдите в главное меню устройства, выберите Пользователи> Список пользователей или Пользователи> Список администраторов, чтобы просмотреть информацию о пользователе или администраторе.



Отпечаток пальца.

- : Card.
- : Palm vein.

Рисунок 3-13 Список пользователей

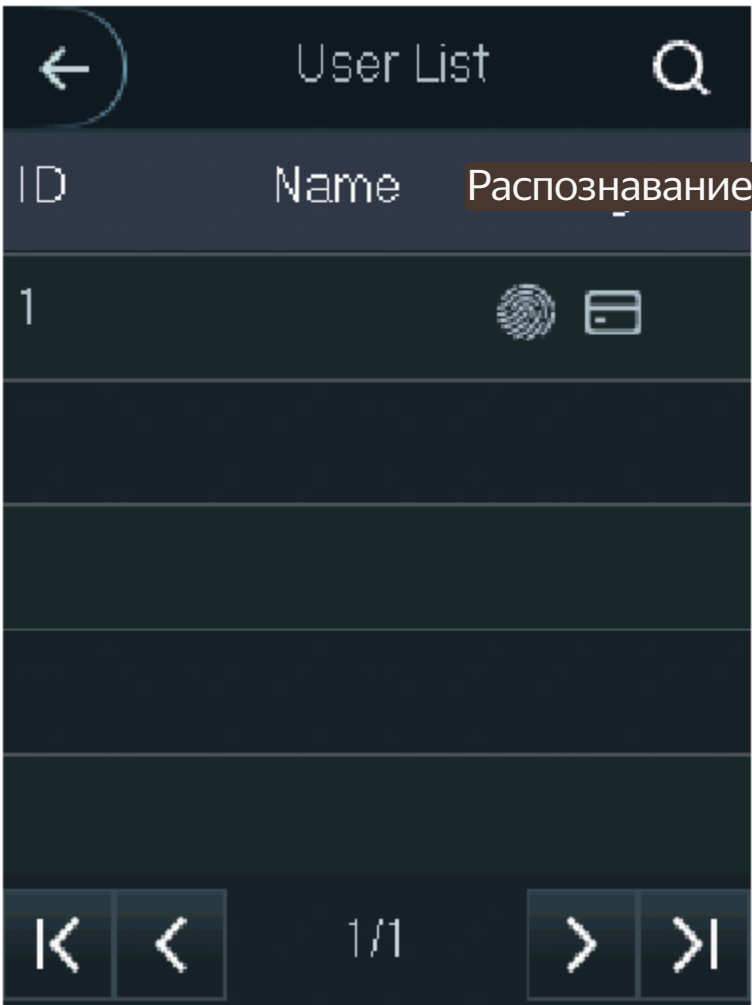
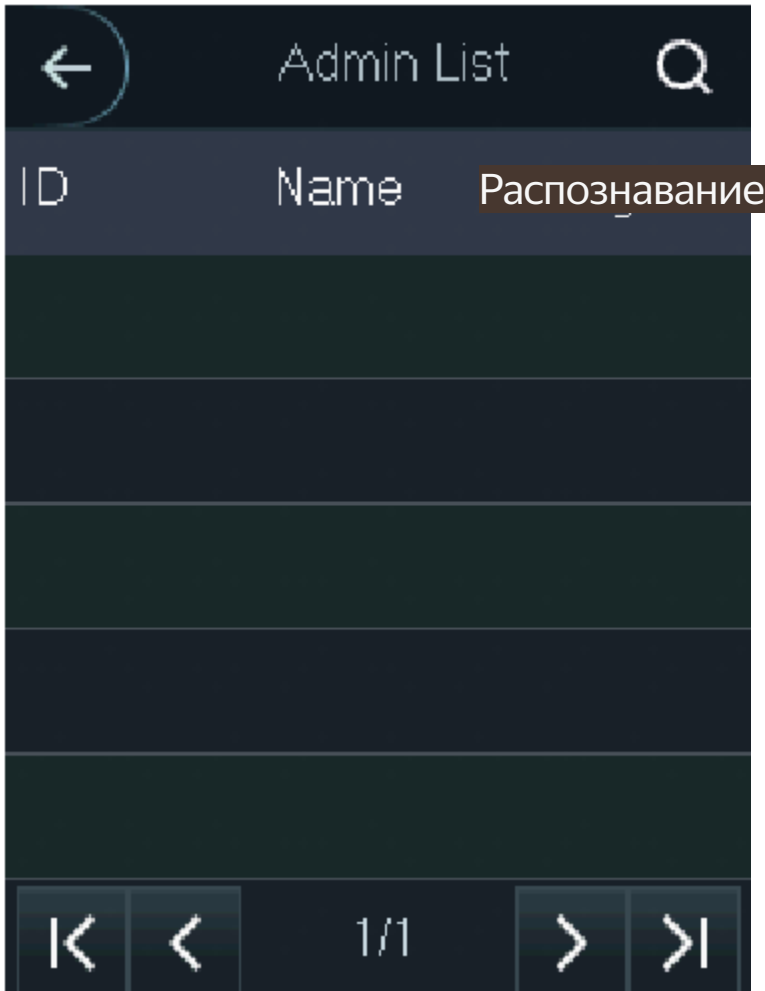


Рисунок 3-14 Список администраторов



Измените информацию о пользователе. Щелкните пользователя или администратора, которого вы хотите изменить, измените информацию, а затем коснитесь



Поиск пользователей. Коснитесь  и введите идентификатор пользователя для поиска пользователей.

Удалите пользователей.

- ◊ Удалять по очереди: В списке пользователей или администраторов коснитесь в правом верхнем углу, а затем коснитесь **ОК**.

- Удалить всех пользователей: На экране "Пользователи" коснитесь "Удалить всех пользователей", а затем нажмите "ОК".

3.7.3 Настройка общедоступного пароля.

При использовании общедоступного пароля нет необходимости вводить идентификатор пользователя, и он не ограничен пользователем Тип. Для каждого устройства может быть настроен только один общедоступный пароль.

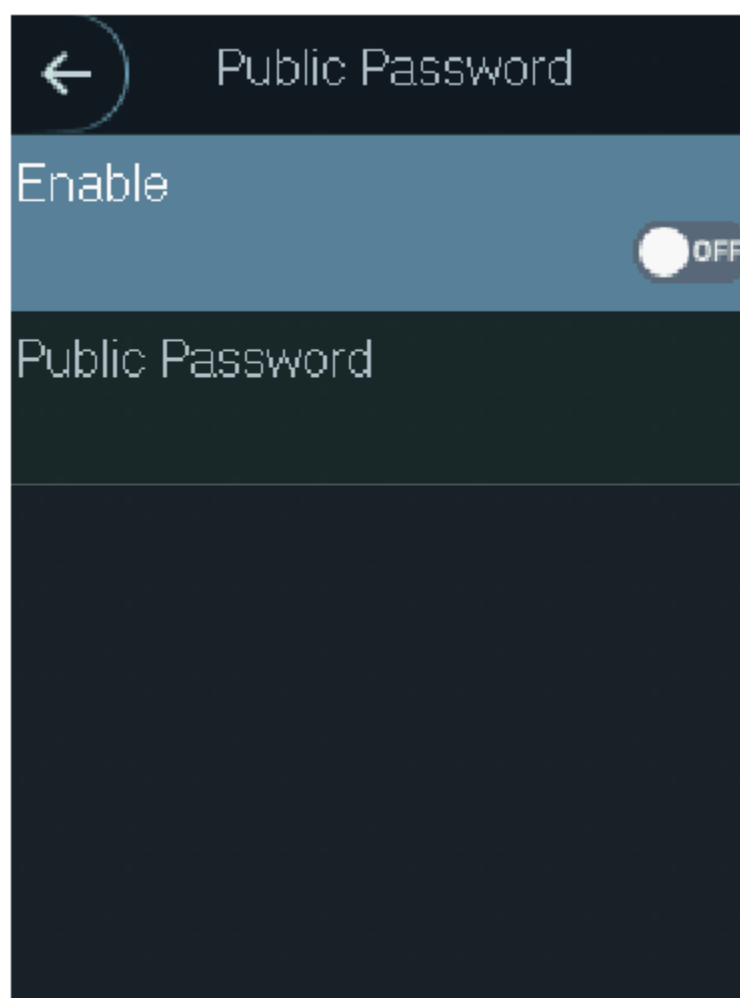
Процедура

Шаг 1 Войдите в главное меню.

Шаг 2 Выберите "Пользователи" > "Общедоступный пароль"

Шаг 3 Включите функцию, нажмите "Общедоступный пароль", чтобы ввести пароль, а затем нажмите "ОК".

Рисунок 3-15 "Общедоступный пароль"



3.8 Управление контролем доступа

Вы можете настроить параметры для дверей, такие как метод разблокировки, сигнализация, продолжительность разблокировки состояния двери и другие параметры. Доступные режимы разблокировки могут отличаться в зависимости от модели изделия.

В главном меню нажмите "Контроль доступа", чтобы перейти к экрану управления контролем доступа.

3.8.1 Настройка метода разблокировки

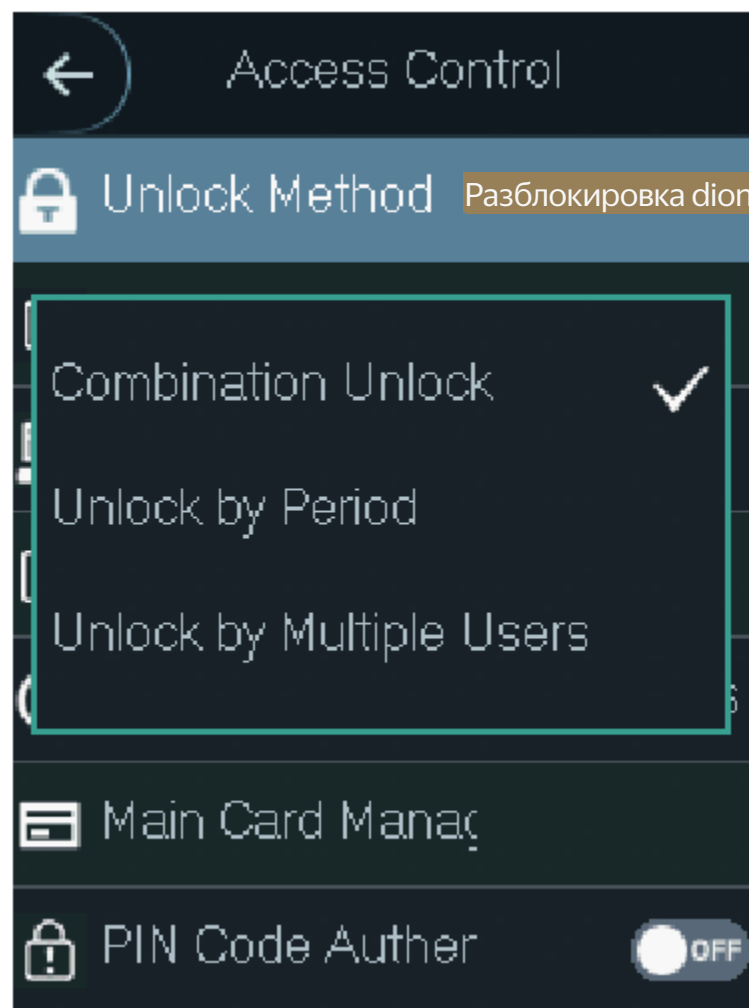
3.8.1.1 Настройка комбинаций разблокировки

Для разблокировки двери используйте карту, отпечаток пальца, лицо, пароль или их комбинации. Доступные режимы разблокировки могут отличаться в зависимости от модели устройства.

Процедура

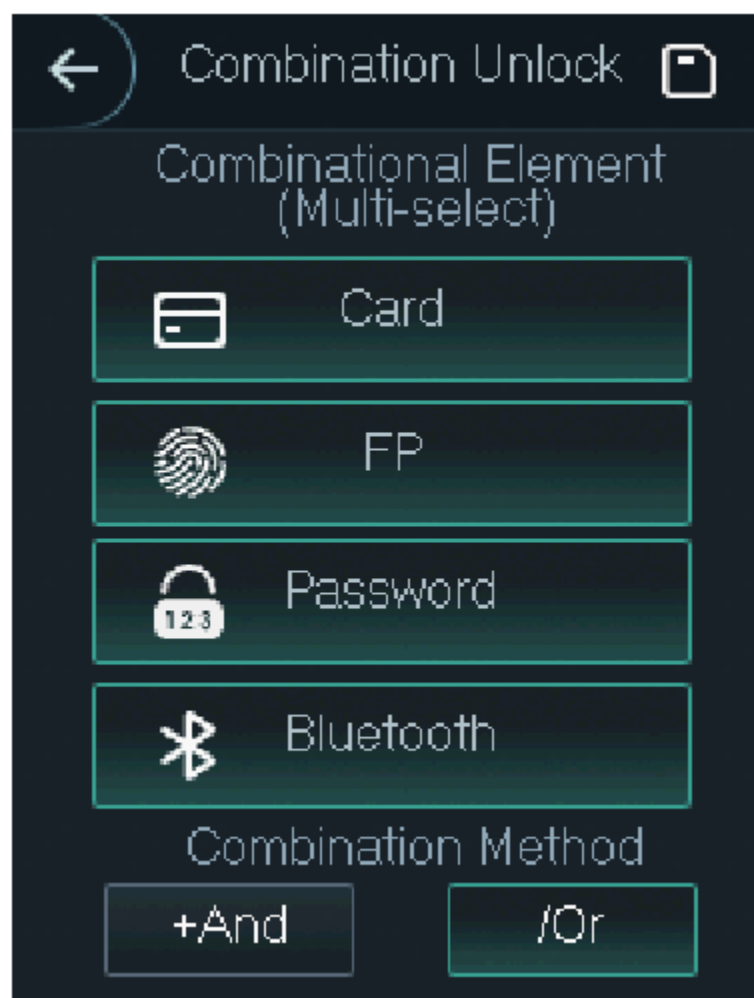
- Шаг 1 Войдите в главное меню.
- Шаг 2 Выберите Управление доступом> Метод разблокировки.

Рисунок 3-16 Комбинированная разблокировка



Шаг 3 Коснитесь Комбинированная разблокировка и выберите методы разблокировки.

Рисунок 3-17 Разблокировка комбинаций



Шаг 4 Нажмите + И или / Или, чтобы настроить комбинации.

Чтобы отменить выбор, коснитесь выбранного метода еще раз.

+ И:

Проверьте все выбранные методы разблокировки, чтобы открыть дверь.



Люди должны пройти верификацию в порядке использования карты, отпечатка пальца, лица и Пароль.

/ Или: Проверьте один из выбранных методов разблокировки, чтобы открыть дверь.

Шаг 5

Коснитесь



, чтобы сохранить изменения.

3.8.1.2 Настройка разблокировки по периодам

Процедура

Шаг 1 Выберите "Контроль доступа".

Шаг 2 Выберите "Контроль доступа"> "Метод разблокировки", а затем выберите "Разблокировать по периодам" из Список.

Подробные сведения о настройке разблокировки по периодам см. в разделе "4.7.1.2 Настройка разблокировки Методы".



Шаг 3 Нажмите, чтобы сохранить изменения.

3.8.1.3 Настройка разблокировки несколькими пользователями

Процедура

Шаг 1 Выберите "Контроль доступа".

Шаг 2 Выберите "Контроль доступа"> "Метод разблокировки", а затем выберите "Разблокировать несколькими пользователями" из списка.

Подробные сведения о том, как настроить разблокировку несколькими пользователями, см. в разделе "4.7.1.2 Настройка разблокировки Методы".



Шаг 3 Нажмите, чтобы сохранить изменения.

3.8.2 Настройка сигналов тревоги.

Настройте аварийные сигналы контроля доступа, и аварийные события могут своевременно отправляться администраторам. Процедура

Шаг 1 В главном меню выберите Контроль доступа> Аварийный сигнал.

Шаг 2 Включите аварийные сигналы в соответствии с вашими потребностями.

Рисунок 3-18 Типы аварийных сигналов

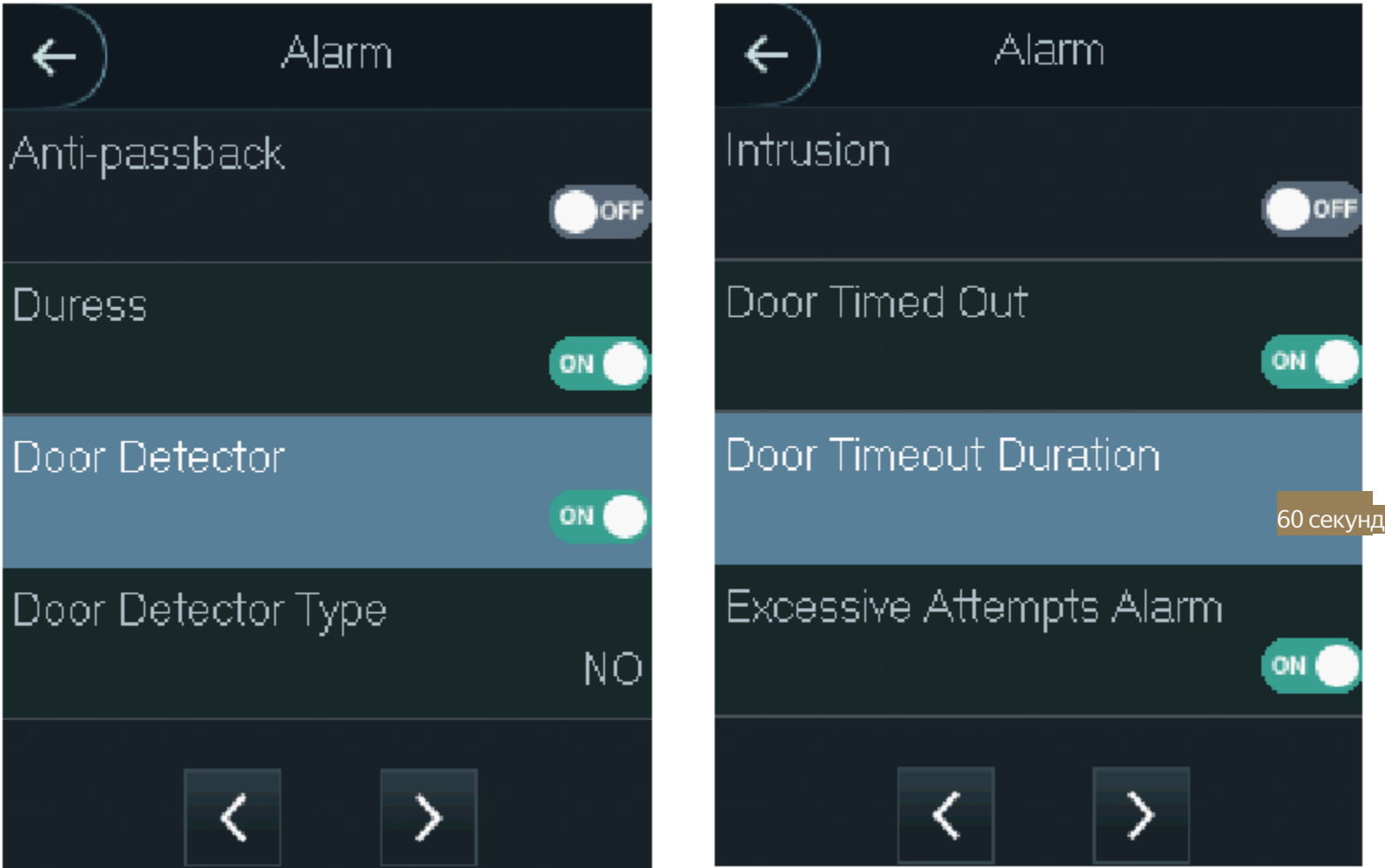


Таблица 3-3 Описание типов аварийных сигналов

Параметр	Описание
Защита от обратного доступа	Когда кто-либо снова войдет в систему без авторизации, сработает сигнализация.
Принуждение	Сигнал тревоги срабатывает, когда для отпирания двери используется принудительный отпечаток пальца.
Дверной детектор	Когда дверной детектор включен, отображаются как время ожидания вторжение.
Тип дверного детектора.	Выберите тип дверного извещателя в зависимости от подключения. • НЕТ: дверь считается открытой, когда сигнальная линия дверного датчика оборвана (разомкнутая цепь). • NC: дверь считается открытой, когда сигнальная линия дверного датчика короткозамкнута (замкнутая цепь).
Вторжение.	Когда и дверной детектор, и система вторжения включены, при аварийном отпирании двери срабатывает сигнализация о вторжении.
Время ожидания двери истекло	Когда время ожидания как дверного детектора, так и двери истекло, сработает сигнализация.
Время ожидания двери истекло.	при включении срабатывает сигнализация тайм-аута, если дверь открытой дольше заданного тайм-аута. Продолжительность тайм-аута двери может быть настроена в диапазоне от 1 до 9999 секунд.
Сигнал тревоги о чрезмерных попытках	Если пароль будет введен неправильно 5 раз подряд в течение 60 секунд или 5 раз подряд будет проведен пальцем по неавторизованной карте, сработает сигнализация.

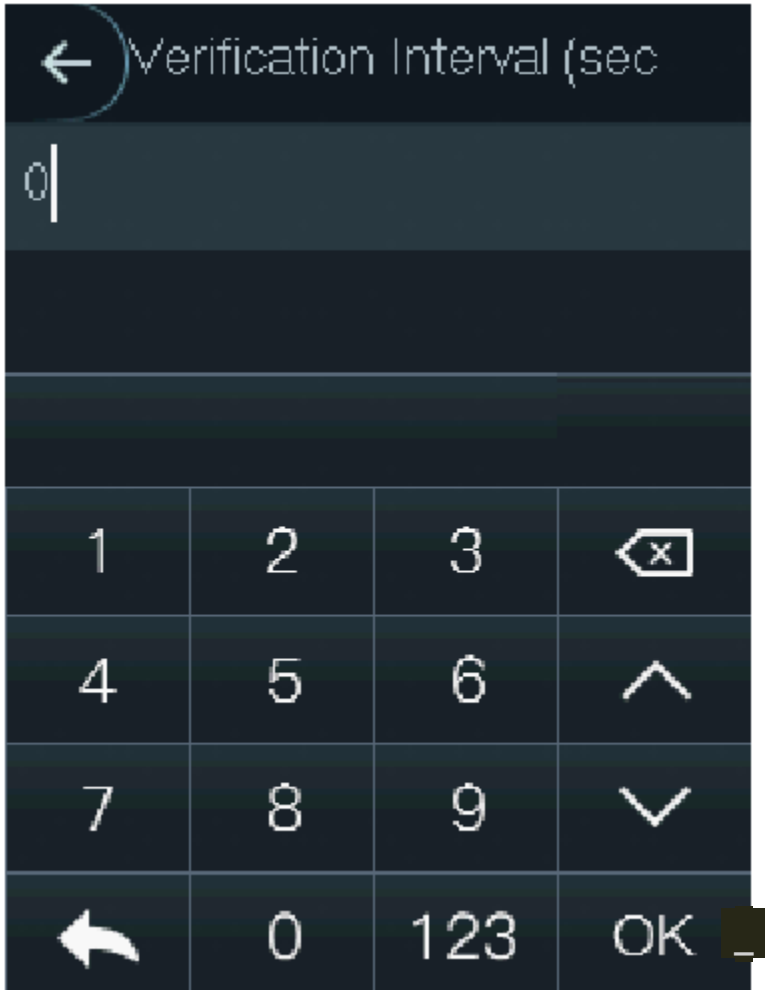
3.8.3 Настройка интервала проверки

Если вы подтвердите свою личность несколько раз в течение определенного периода, будет действовать только самая ранняя проверка. действительной считается самая ранняя проверка, и дверь не откроется после второй или более поздних проверок. Только по истечении установленного периода вы можете снова подтвердить личность.

Процедура

- Шаг 1 В главном меню выберите Контроль доступа> Сигнализация.
- Шаг 2 Коснитесь Интервал проверки (сек), введите временной интервал, а затем нажмите OK.

Рисунок 3-19 Интервал проверки

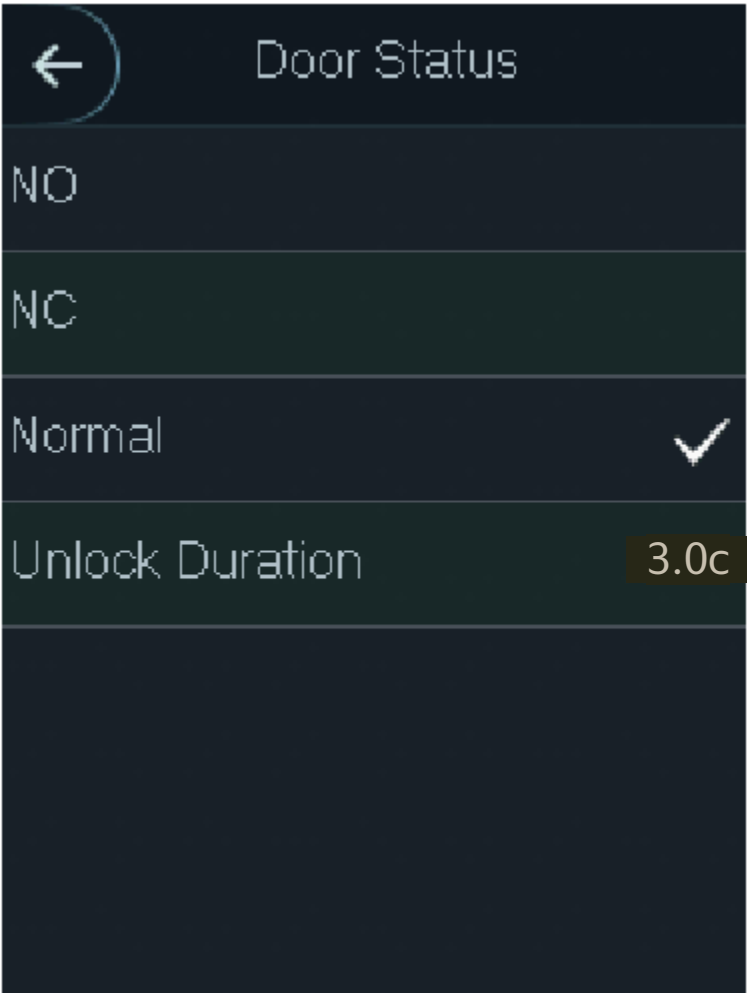


3.8.4 Настройка состояния блокировки

Процедура

- Шаг 1 В главном меню выберите пункт Контроль доступа > Дверь **Статус**.
- Шаг 2 Установите состояние двери.

Рисунок 3-20 Состояние блокировки



Описание параметров таблицы 3-4

Параметр	Описание
Состояние двери	• НЕТ: дверь остается незапертой все время. • NC: дверь остается заблокированной все время. • Normal : если выбрано значение Normal, дверь будет заблокирована и отперта в соответствии с вашими настройками.
Продолжительность разблокировки.	После того, как человеку будет предоставлен доступ, дверь останется в течение определенного времени, необходимого для его прохождения.

3.8.5 Управление основными картами

Добавление основных карт

Войдите в главное меню, выберите "Контроль доступа"> "Управление основными картами" > "Добавить основную карту", нажмите "Общие" "Карта" и затем проведите по карте пальцем.

Удаление основных карт

Войдите в главное меню, выберите "Контроль доступа" > "Управление основной картой" > "Удалить основную карту" и нажмите "ОК".

затем

Связанные операции

На главном экране, проведя пальцем по основной карте, подождите 3 секунды без каких-либо действий, чтобы перейти в соответствующий режим. Если в течение этих 3 секунд провести пальцем по обычной карте, устройство не ответит.

Устройство определяет функцию на основе общего количества нажатий на основную карту. После соответствующего если режим активирован, проведя пальцем по основной карте один раз, вы выйдете из текущего режима и вернетесь к главному экрану.



Если карта является одновременно основной и пользовательской, система проверяет, является ли она основной картой.

Проведите пальцем по основной карте, чтобы добавить карту пользователя. Проведите пальцем по карте пользователя, чтобы добавить ее на устройство. Непрерывно добавление разрешено.
Дважды проведите пальцем по основной карте, чтобы удалить карту пользователя. Проведите пальцем по карте пользователя, чтобы удалить ее с устройства. Допускается непрерывное удаление.

• Проведите пальцем по основной карте 5 раз, чтобы удалить всех пользователей.

3.8.6 Настройка аутентификации по PIN-коду.

Процедура

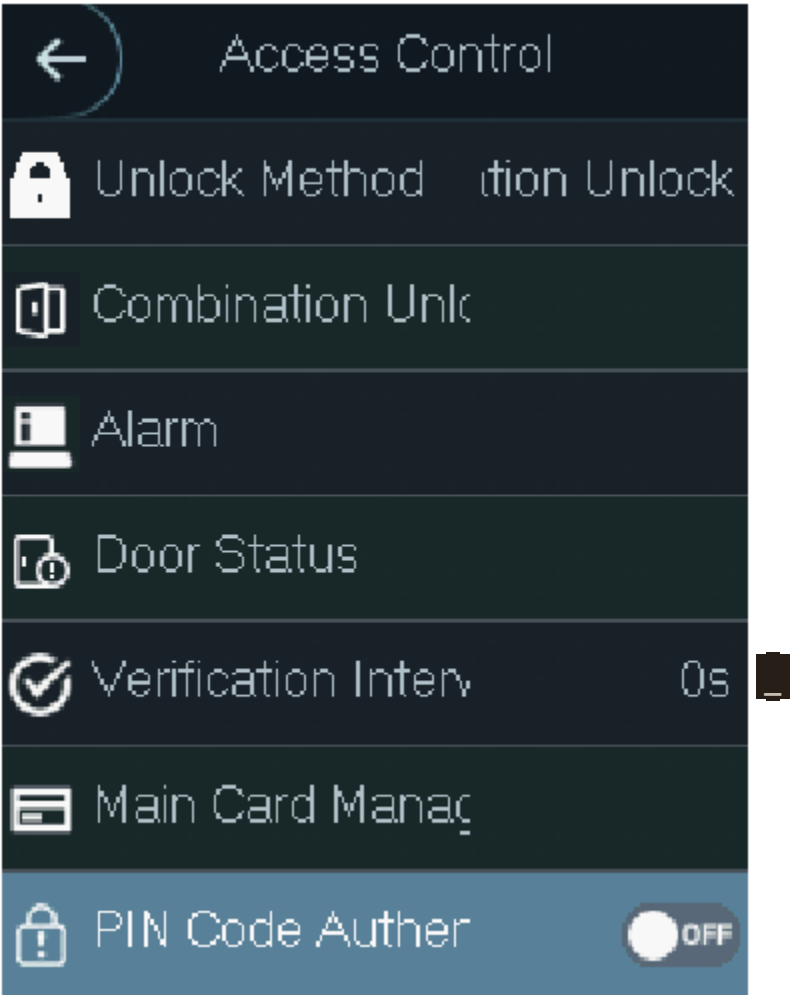
- Шаг 1
- Шаг 2
- В главном меню выберите "Контроль доступа"> "Аутентификация по PIN-коду". Включите или отключите аутентификацию по PIN-коду.

Аутентификация по pin-коду отключена по умолчанию. Когда он включен, вы можете только открыть дверь с помощью пароля.



После включения аутентификации по PIN-коду вы можете напрямую ввести их пароль для подтверждения без ввода идентификатора пользователя.

Рисунок 3-21 Аутентификация по PIN-коду



3.9 Управление посещаемостью

В главном меню выберите пункт Посещаемость. Включите сетевую посещаемость или выключите ее.



После ее включения статус посещаемости нельзя настроить и сообщить платформе.

3.10 Параметры связи

Настройте сеть, порт RS-485 и порт Wiegand.



Порт RS-485 и порт Wiegand могут отличаться в зависимости от модели устройства.

3.10.1 Настройка IP

Задайте IP-адрес для устройства, чтобы подключить его к сети. После этого вы можете войти на веб-страницу и платформу управления для управления устройством.

Процедура

Шаг 1 В главном меню выберите Связь> Настройки IP. Шаг 2 Установите IP-адрес.

Рисунок 3-22 IP-адрес

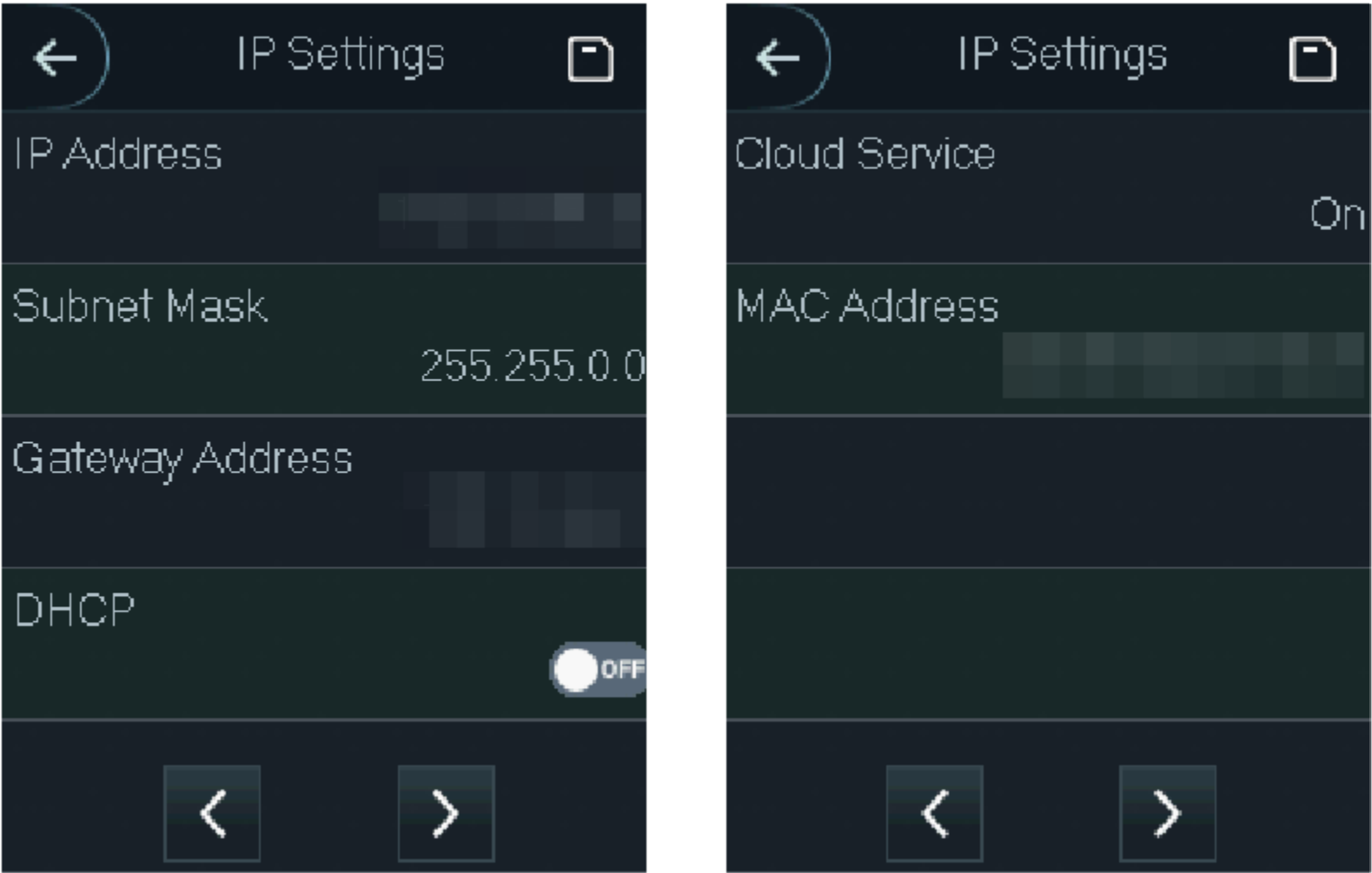


Таблица 3-5 Описание настроек IP

Параметр	
IP-адрес	Описание Введите IP-адрес устройства, маску подсети, адрес шлюза и MAC-адрес .
Маска подсети	
Адрес шлюза	
MAC-адрес	
DHCP	Включите функцию DHCP (протокол динамической настройки хоста) для автоматического получения IP-адреса. В этом случае IP-адрес, маску подсети и адрес шлюза установить невозможно.
Облачный сервис	Включите эту функцию, и устройство сможет подключаться к облаку и работать через мобильное приложение.

3.10.2 Настройка Wi-Fi



Подключите устройство к сети через беспроводную сеть.

Устройства с модулем Wi-Fi имеют эту функцию.
Функции точки доступа Wi-Fi и Wi-Fi являются взаимоисключающими.

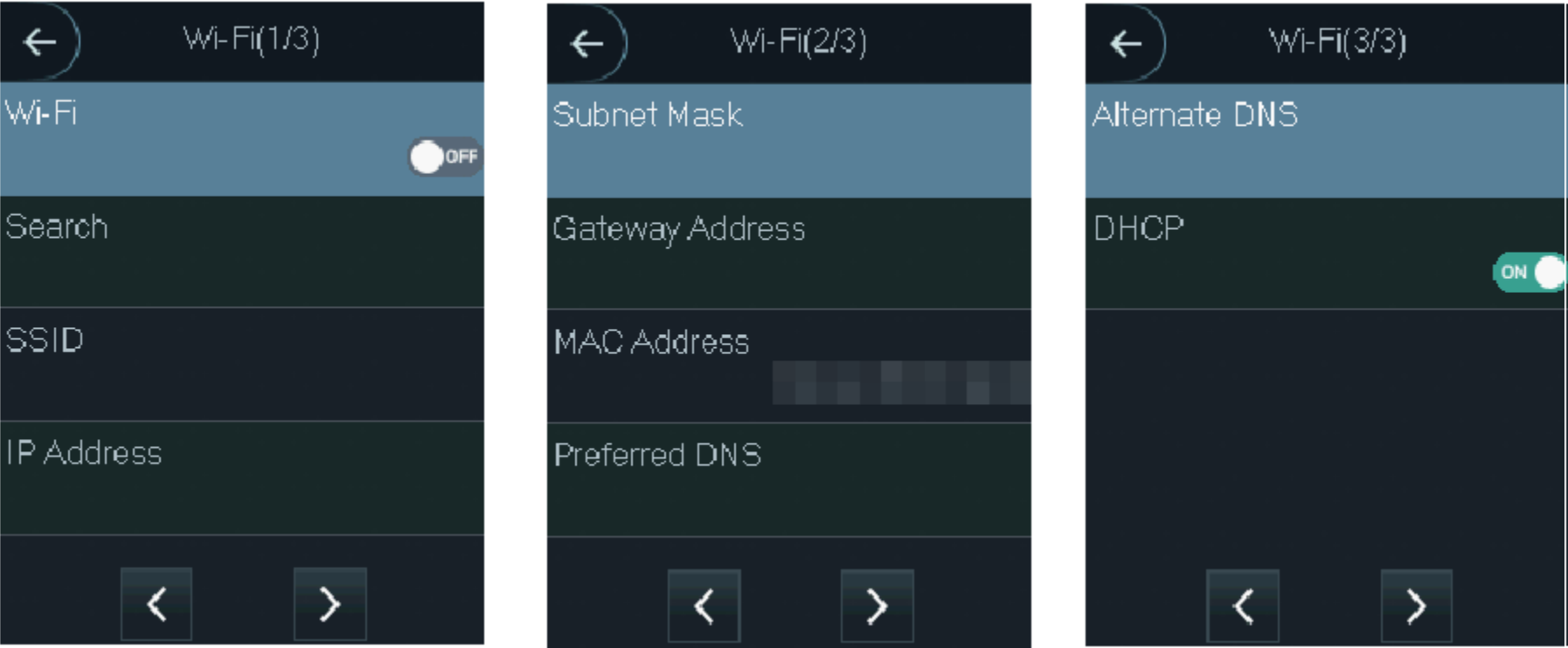
Процедура

- Шаг 1
- В главном меню выберите Связь> Wi-Fi.
- Отобразите экран результатов поиска.



Функция будет готова к обычному использованию через 1 минуту.

Рисунок 3-23 Wi-Fi



- Шаг 2
- Выберите искомый Wi-Fi и нажмите OK.
- Шаг 3
- Введите пароль Wi-Fi, выберите Подключиться, а затем нажмите OK.
- DHCP включен по умолчанию для автоматического получения IP-адреса. Когда DHCP отключен, поддерживается ручной ввод IP-адреса.
- Шаг 4 (необязательно) Если Wi-Fi не найден, выберите SSID и нажмите OK, чтобы вручную ввести название Wi-Fi.

Результаты

Если и ваш мобильный телефон, и само устройство подключены к одной сети Wi-Fi. Введите IP-адрес адрес, отображаемый на экране Wi-Fi, в браузере вашего телефона, чтобы получить доступ к устройству.

3.10.3 Настройка точки доступа Wi-Fi.

Используйте свой компьютер или телефон для подключения к точке доступа Wi-Fi устройства для доступа к его веб-странице. Эта функция доступна только на некоторых моделях.

Процедура

- Шаг 1
- В главном меню выберите Связь> Точка доступа Wi-Fi.
- Шаг 2
- Включите точку доступа Wi-Fi.
- Вы можете настроить безопасность точки доступа Wi-Fi.

Выберите Нет, чтобы напрямую подключиться к точке доступа Wi-Fi. Выберите WPA2-Персональный, чтобы настроить пароль и подключиться к точке доступа Wi-Fi с помощью пароля.



Точка доступа Wi-Fi и функция Wi-Fi не могут быть включены одновременно.
При каждом включении устройства функция точки доступа Wi-Fi будет включаться автоматически на 30 минут.

Рис. 3-24 Подключение к точке доступа Wi-Fi



Результаты

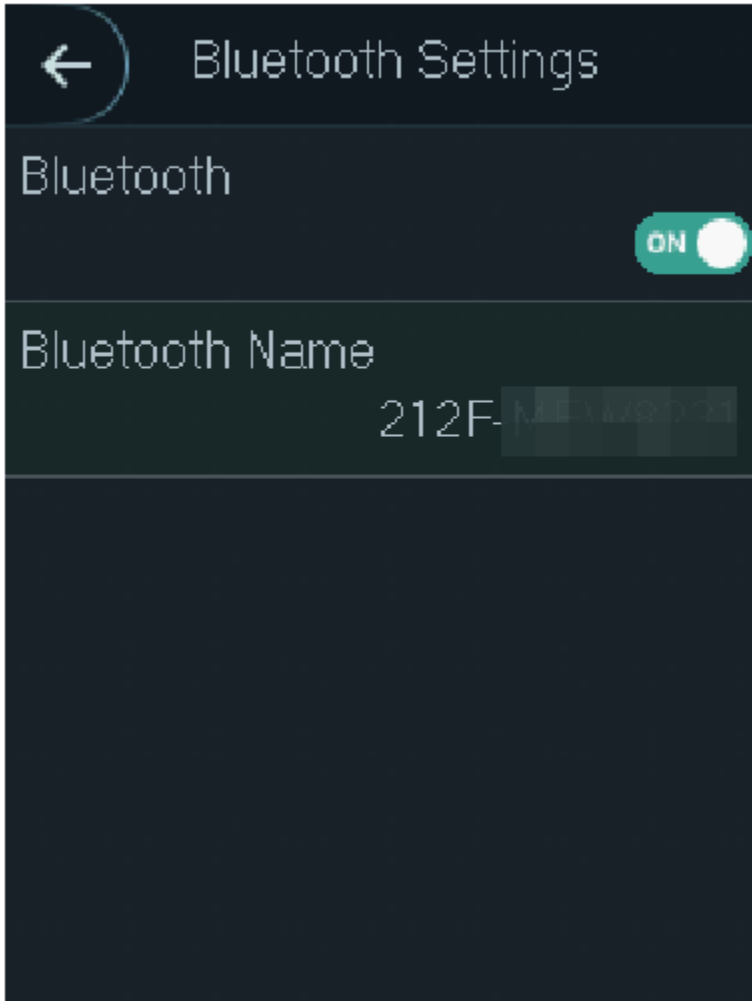
Когда ваш телефон подключится к точке доступа устройства, он автоматически перенаправится на страницу входа в систему. Кроме того, вы можете вручную ввести IP-адрес, отображаемый на экране точки доступа Wi-Fi (IP по умолчанию: 192.168.3.1) в вашем браузере, чтобы получить доступ к устройству.

3.10.4 Настройка Bluetooth

Процедура

Шаг 1 В главном меню выберите **Связь> Настройки Bluetooth**. **Шаг 2** Включите Bluetooth.

Рисунок 3-25 Bluetooth



Настройки режима 3.10.5

3.10.5.1 Режим контроллера

Устройство функционирует как контроллер доступа и подключается к внешнему считывателю карт access контроллер или модуль безопасности управления дверью.

Процедура

- Шаг 1 В главном меню выберите Связь > Настройки режима.
- Шаг 2 Установите настройки режима в качестве контроллера доступа.
- Шаг 3 Настройте настройки RS-485 и Wiegand.
Выберите настройки RS-485.
Если вы подключаетесь к другим устройствам с помощью порта RS-485, настройте параметры.

Рисунок 3-26 Контроллер доступа

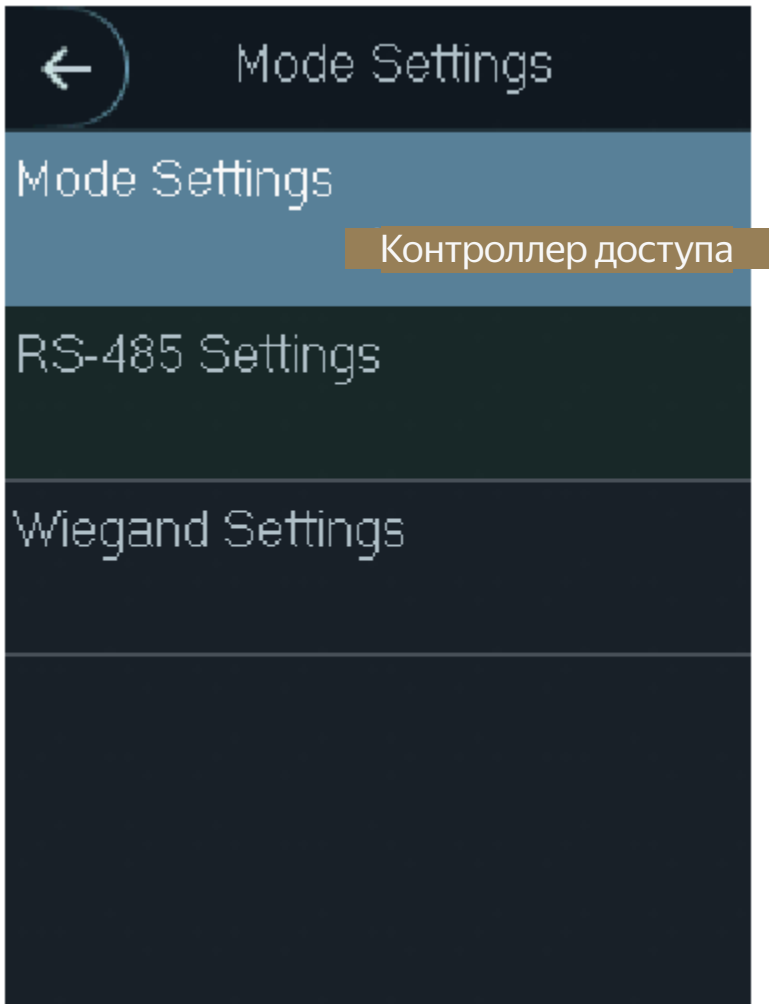


Таблица 3-6 Описание параметров RS-485

Параметр	Описание	Примечание
Контроллер доступа	Подключается к другим контроллерам доступа, когда устройство функционирует как устройство чтения карт , и отправляет данные на другие внешние контроллеры доступа для управления доступом. ID: выводит данные на основе идентификатора пользователя. Номер карты: выводит данные на основе номера карты, когда пользователь проводит пальцем по карте, чтобы разблокировать дверь; выводит данные на основе первого номера карты пользователя, когда он использует другие методы разблокировки .	Если устройство подключено к контроллеру, оба устройства проверяют ID карты и выдают разные разрешения людям контроллера. Если у пользователя есть разрешение к Устройству, но нет разрешения к внешнему контроллеру, то устройство не выдаст разрешение. Если у пользователя есть разрешение к Устройству, но нет разрешения к внешнему контроллеру, то устройство не выдаст разрешение. Если у пользователя есть разрешение к Устройству, но нет разрешения к внешнему контроллеру, то устройство не выдаст разрешение.
Устройство чтения карт памяти	Устройство функционирует как контроллер доступа и подключается к внешнему устройству чтения карт памяти.	

Параметр	Описание
Модуль защиты двери	Кнопка выхода из двери, замок и противопожарный рычаг не действуют после включения модуля безопасности. Поддерживает аутентификацию с помощью лица, карты, отпечатка пальца или пароля на этом устройстве для управления разблокировкой модуля безопасности двери. o Поддерживает аутентификацию через внешний считыватель карт RS-485, подключенный к модулю безопасности системы управления дверью (проводя по карте) или через внешнюю кнопку для управления разблокировкой модуля безопасности двери.
Модуль расширения замка	Выбран модуль расширения, устройство подключено к модулю расширения дверного замка. При блокировке проверка подлинности устройства разблокирует только локальную блокировку, в то время как проверка подлинности внешнего устройства карт разблокирует дополнительную блокировку. После выбора на странице настройки параметров контроля доступа и сигнализации, дверной канал поддерживает выбор двери 2, и соответствующие параметры для двери 2 могут быть настроены.
Устройство чтения (OSDP)	Устройство подключается к устройству чтения карт по протоколу OSDP, которое отправляет информацию о карте доступа к контроллеру доступа или платформе управления.

Выберите настройки Wiegand.

- o Вход Wiegand: при подключении внешнего устройства чтения карт выберите Wiegand **Вход**.

Номер карты. Инверсия: Если последовательность номеров карт, полученная с помощью ввода Wiegand , не совпадает с фактической последовательностью номеров карт при взаимодействии со сторонними устройствами сторонних производителей, включите эту функцию.

- ◇ Вывод Wigand: когда устройство работает как устройство чтения карт памяти, и вам необходимо подключить его к другому контроллеру доступа и выберите Конфигурацию вывода Wiegand.

Таблица 3-7 Описание Wiegand

Параметр	Описание
Wiegand Тип вывода	Разрядность номеров карт или ID, которые устройство может распознать и вывести Wiegand 26: считывает 3 байта или 6 цифр. o o Wiegand 34: считывает 4 байта или 8 цифр. Wiegand 66: считывает 8 байт или 16 цифр.
Длительность импульса	Настройте ширину импульса и интервал для вывода wiegand.

Параметр	Описание
Интервал импульсов	
Тип выходных данных	Выберите формат Wiegand для считывания номеров карт или удостоверений личности. Идентификатор пользователя: выводит данные на основе идентификатора пользователя. Карта: выводит данные на основе первого номера карты пользователя.
Формат Wiegand	Если тип выходных данных задан как ID, вы можете выбрать десятичный или шестнадцатеричный форматы вывода.

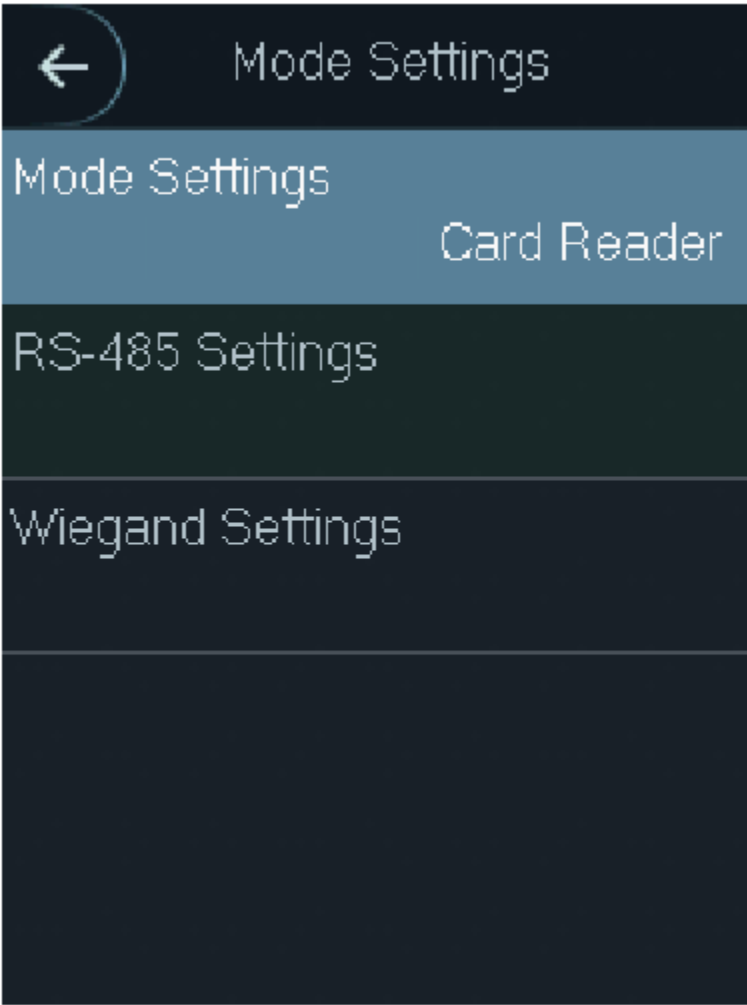
3.10.5.2 Режим чтения карт памяти.

Когда устройство функционирует как устройство чтения карт, подключенное к внешнему контроллеру доступа, оно не выполняет аутентификацию локально. Вместо этого оно напрямую передает данные контроля доступа в систему доступа контроллер, который затем обрабатывает аутентификацию и запускает разблокировку двери.

Процедура

- Шаг 1
- В главном меню выберите Связь> Настройки режима и затем нажмите ОК.
- Шаг 2
- 2 Установите настройки режима в качестве устройства чтения карт памяти.**

Рисунок 3-27 Режим устройства чтения карт памяти



Шаг 3 Настройте параметры RS-485 и Wiegand.

Выберите настройки RS-485.

- Конфигурация скорости передачи данных в бодах: 9600 по умолчанию, которую можно изменить.
- ◇ ○ Время синхронизации: отрегулируйте время устройства в зависимости от объема внешнего контроллера.

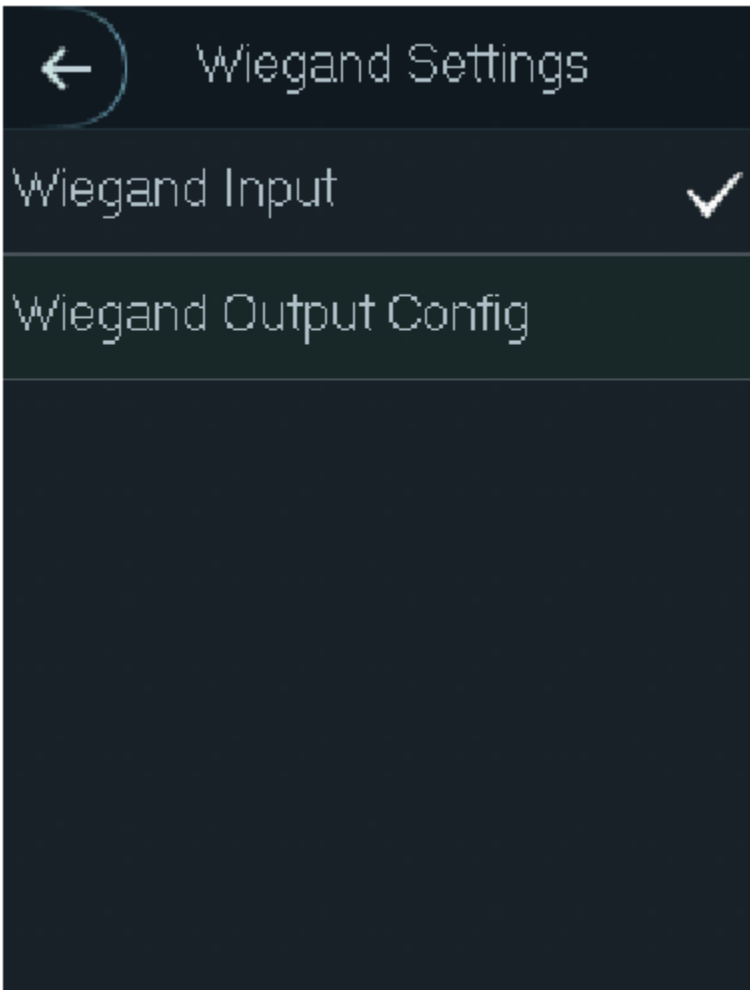
Выберите

Настройки Wiegand.

Разрядность номеров карт, которые устройство может распознавать и выводить.

- Wiegand 26: считывает 3 байта или 6 цифр.
- Wiegand 34: считывает 4 байта или 8 цифр.
- Wiegand 66: считывает 8 байт или 16 цифр.

Рисунок 3-28 Wiegand



3.11 Системные настройки

Параметры могут отличаться в зависимости от моделей устройств.

Коснит  или  для переключения страниц.

3.11.1 Настройка времени

Настройте отображение системного времени и синхронизацию в соответствии с предпочтениями пользователя.

Процедура

- Шаг 1 В главном меню выберите Система > Время.
- Шаг 2 Настройте параметры.

Рисунок 3-29 время

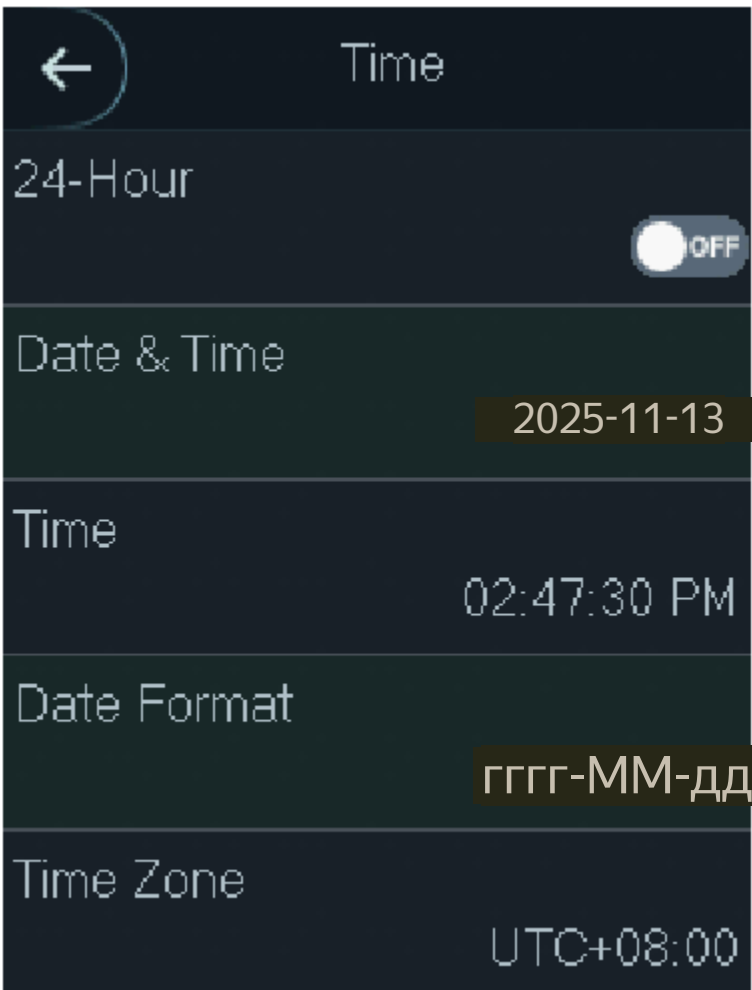


Таблица 3-8 Описание параметра time

Параметр	Описание
24-часовой режим	Включите или отключите 24-часовой формат. При включении время будет отображаться в 24-часовом формате; при выключении время будет отображаться в 12-часовом формате.
Дата и время	1.Коснитесь, чтобы выбрать дату и время. 2.Введите дату, а затем нажмите ОК.
Время	1.Нажмите, чтобы выбрать время. 2.Введите время, а затем нажмите ОК.
Формат даты.	1.Коснитесь, чтобы выбрать формат даты. 2.Выберите формат.
Часовой пояс	1.Коснитесь, чтобы выбрать часовой пояс. 2.Выберите часовой пояс.

3.11.2 Настройка языка

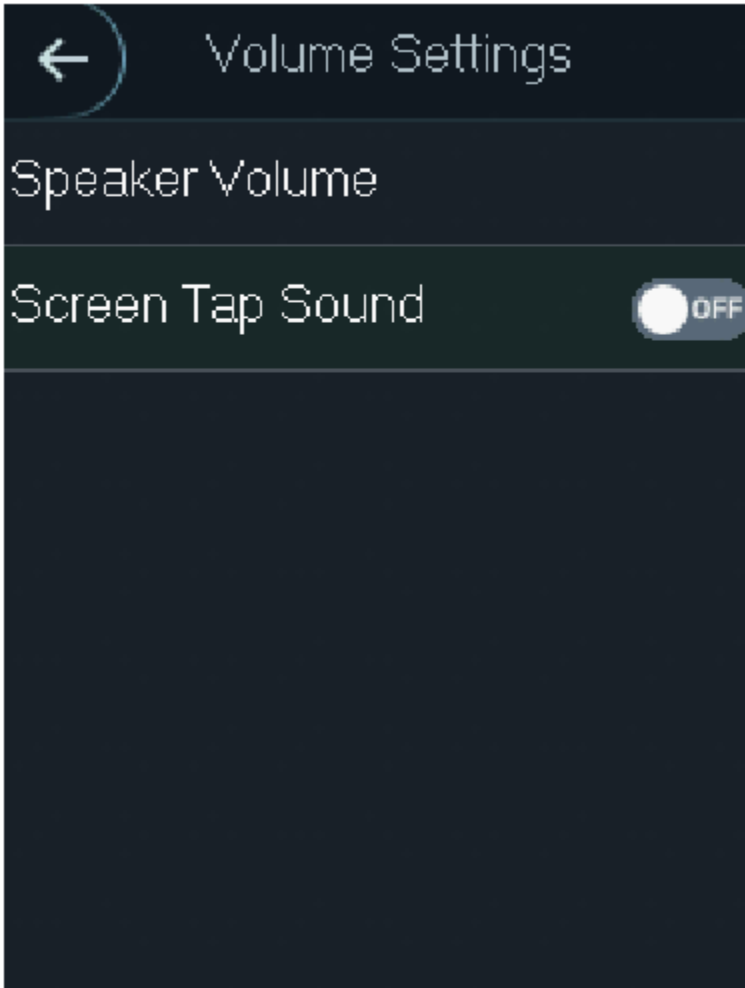
В главном меню выберите Система > Язык, выберите язык для устройства.

3.11.3 Настройка громкости

Процедура

Шаг 1 В главном меню выберите Система > Настройки громкости. Шаг 2 Настройте параметры.

Рисунок 3-30 Настройки громкости



Описание параметров таблицы 3-9

Параметры	Описание
Громкость динамика	Коснитесь громкости, а затем коснитесь или, чтобы отрегулировать громкость.
Звук при касании экрана	Когда эта функция включена, устройства с сенсорным экраном будут воспроизводить звук при касании экрана.

3.11.4 Настройка параметров экрана

Процедура

- Шаг 1 В главном меню выберите Система> Настройки экрана.
- Шаг 2 Настройте параметры.

Рисунок 3-31 Настройки экрана

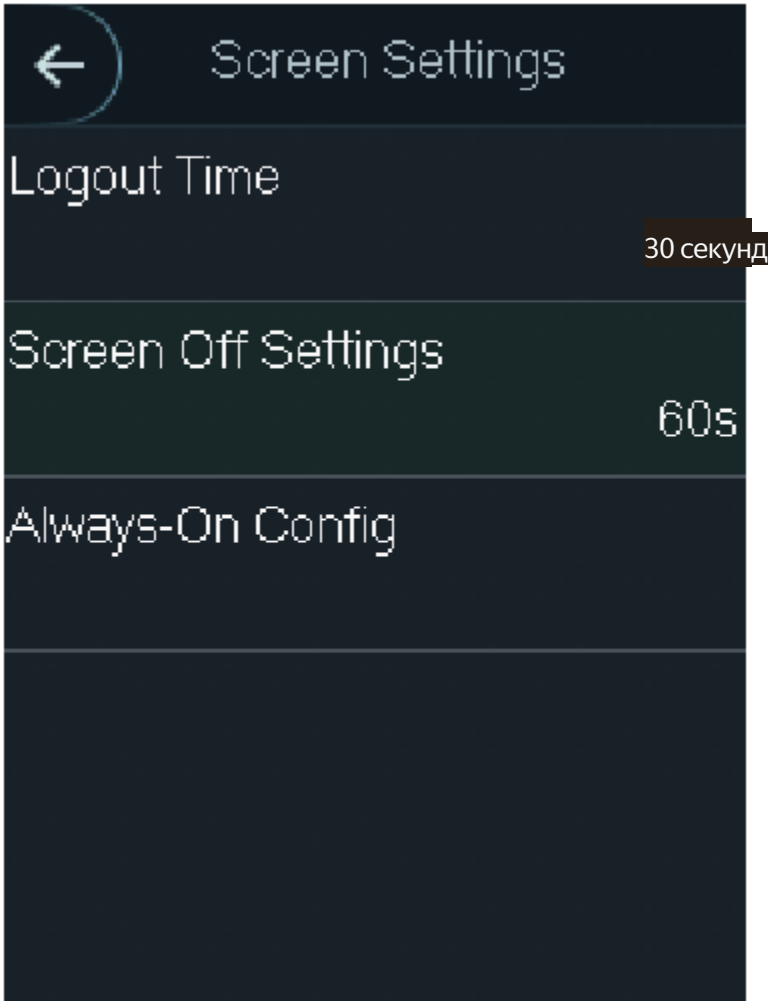


Рисунок 3-32 Постоянно включен

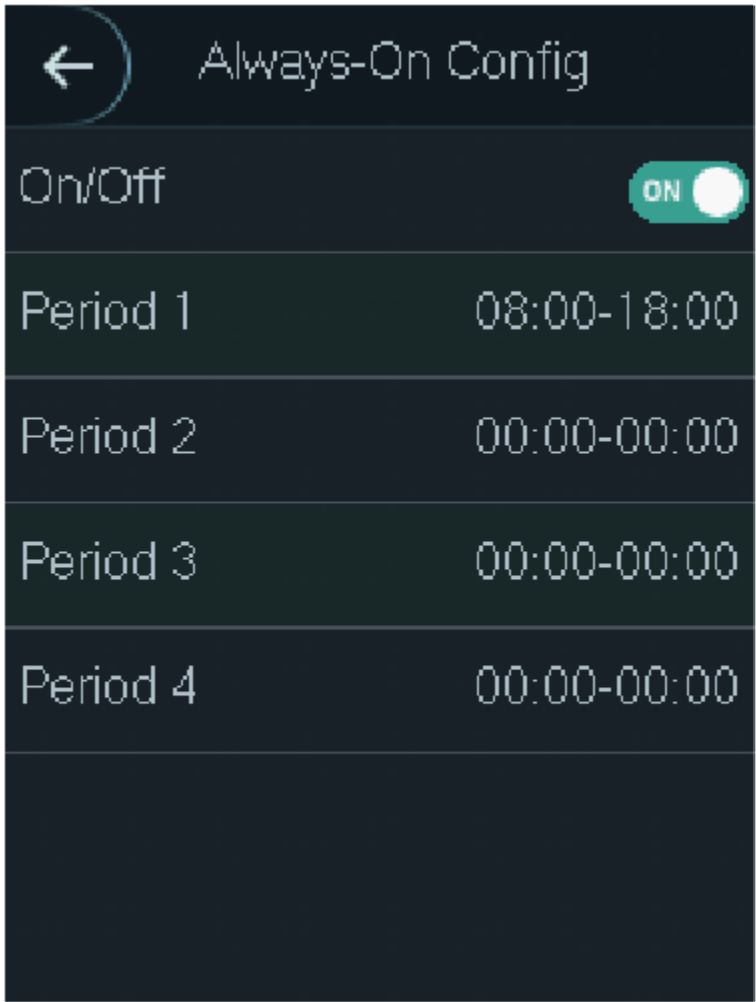


Таблица 3-10 Описание параметров экрана

Параметр	Описание
Время выхода из системы	Если ни с одним из интерфейсов не выполняется никаких операций более установленного времени, система возвращается к интерфейсу заставки.
Настройки выключения экрана	Если ни с одним из интерфейсов не выполняется никаких операций, система сначала возвращается к интерфейсу заставки. Если общее время бездействия достигает установленной продолжительности и оно выходит за пределы периода постоянного включения экрана, система переходит в режим отключения экрана. Если в течение периода постоянного включения экран тускнеет, продолжая отображать изображение заставки.
Постоянно включенная настройка	Включите его и настройте период "всегда включен". В течение этого периода времени экран всегда включен. Сохранение экрана включенным в течение длительного времени. периоды могут повлиять на срок ее службы. Рекомендуется ограничить общее ежедневное время постоянного просмотра экрана не более чем 8 часами.

3.11.5 Настройка параметров карты памяти

Справочная информация



Только устройства с IC поддерживают эту функцию.

Процедура

- Шаг 1 В главном меню выберите Система > Настройки карты.
- Шаг 2 Настройте параметры.

Рисунок 3-33 Настройки карты

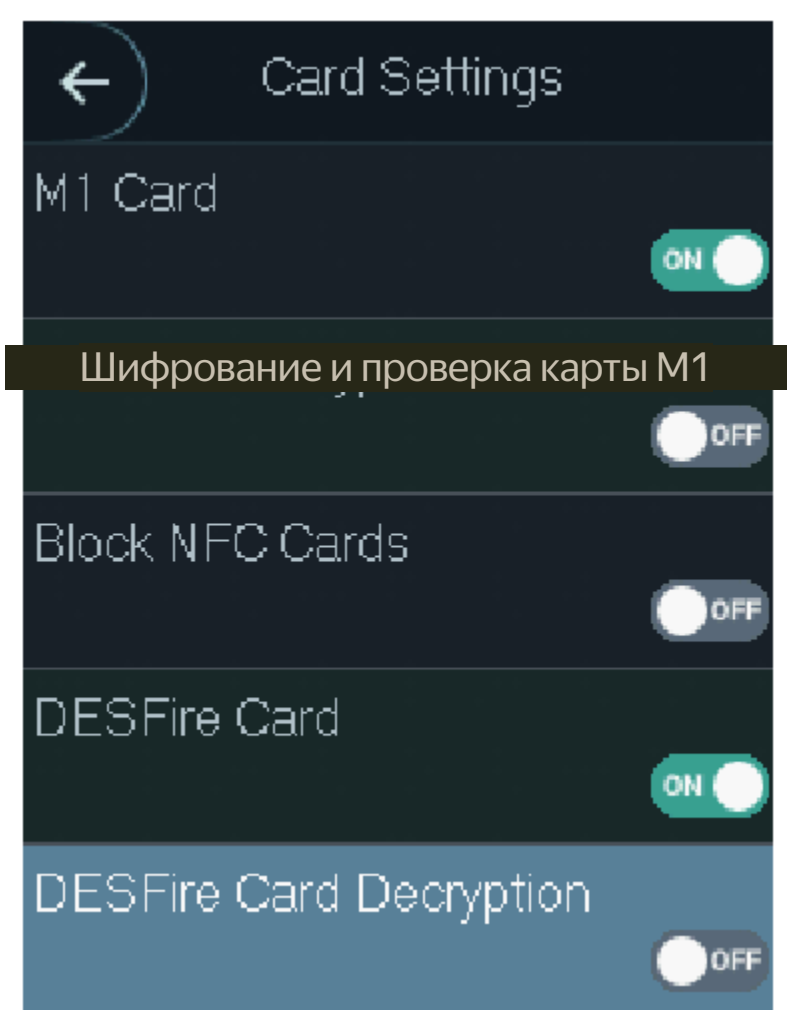


Таблица 3-11 Описание параметров карты.

Параметр	Описание
Карта M1	Только устройства с IC поддерживают эту функцию.
Шифрование карты M1 & Проверка.	Включите его, и устройство сможет считывать карту M1 и серийный номер ID. Это включено по умолчанию. Включите шифрование и проверку карты M1 после того, как вы включили карту M1. Поддерживает только считывание карты M1.
Блокировать карты NFC	Только устройства с IC поддерживают эту функцию. Только определенные телефоны поддерживают эту функцию. После включения IC-карты включите блокировку карт NFC, чтобы предотвратить несанкционированный доступ, заблокировав открытие дверей картами, скопир.
Отключите карту памяти.	Только устройства с IC поддерживают эту функцию., и принимаются только ше
Шифрование карты DESFire	Включите эту функцию, и устройство сможет считывать физический серийный номер (UID) карты DESFire card. После включения карты DESFire включите шифрование карты DESFire устройство может считывать содержимое карт DESFire.

3.11.6 Настройка пароля устройства

3.11.6.1 Смена пароля

Процедура

- Шаг 1

Выберите Система> Пароль устройства> Изменить пароль.
- Шаг 2

Введите старый пароль, новый пароль, подтвердите пароль, а затем нажмите ОК.

3.11.6.2 Изменение зарезервированной информации

Зарезервированный адрес электронной почты используется для получения кода безопасности для сброса пароля.

Процедура

- Шаг 1

Выберите "Система"> "Пароль устройства"> "Изменить зарезервированную информацию".
- Шаг 2

Введите адрес электронной почты и нажмите "ОК".

3.11.7 Восстановление заводских настроек по умолчанию.



Восстановление заводских настроек устройства может привести к потере данных. Обратите внимание.

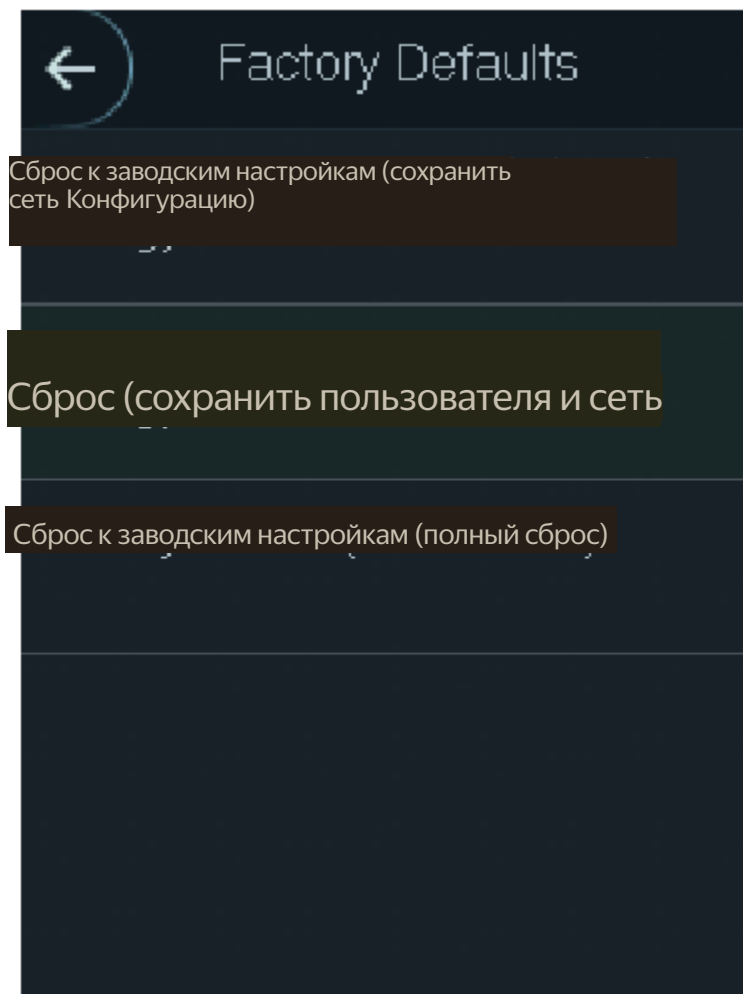
Восстановление с помощью программного обеспечения

1. В главном меню выберите Система> Заводские настройки по умолчанию.
2. При необходимости восстановите заводские настройки по умолчанию. При необходимости восстановите заводские настройки по умолчанию.

Восстановить заводские настройки (сохранить конфигурацию сети): сбрасывает все конфигурации, кроме конфигурации сети.

- Восстановить значения по умолчанию (сохранить журналы, информацию о пользователе и конфигурацию сети): сбрасывает все конфигурации и данные, за исключением информации о пользователе, журналов, конфигураций сети.
- Восстановление заводских настроек (полный сброс): сбрасывает все конфигурации.

Рисунок 3-34 Заводские настройки по умолчанию



Восстановление с помощью оборудования

Устройство поддерживает кнопку саботажа и кнопку сброса.

Кнопка вскрытия: в течение 5 минут после включения устройства, если нажать кнопку вскрытия 5 раз в течение 8 секунд, устройство отобразит запрос. Нажмите ОК или нажмите и удерживайте кнопку tamper в течение нескольких секунд, после чего устройство перезапустится. Все конфигурации и информация будут восстановлены к заводским настройкам.

Отверстие для сброса: Чтобы сбросить настройки устройства, необходимо замкнуть его, вставив PIN-код в точечное отверстие.

- ◊ Если вы хотите выполнить частичный сброс и сохранить информацию о пользователе, журналы и IP конфигурации, вывод должен быть вставлен на 500 мс.
- ° Если вы хотите выполнить полный сброс, штифт должен оставаться вставленным в течение 5 секунд.



Отверстие для сброса доступно на некоторых моделях.

3.11.8 Настройка сброса пароля

В главном меню выберите "Система", а затем включите "Сброс пароля". После включения функции если вы забудете пароль, вы можете использовать настроенный адрес электронной почты для получения кода безопасности и восстановить пароль. Он включен по умолчанию.

3.11.9 Перезапуск устройства

В главном меню выберите Система > Перезагрузка, и устройство будет перезапущено.

3.12 Управление через USB.

3.12.1 Экспорт данных

После установки USB-накопителя экспортируйте данные с устройства на USB-накопитель. Некоторые экспортированные данные зашифрованы и не могут быть отредактированы.

Предварительные требования.

USB-накопитель вставлен в устройство и распознан надлежащим образом.



Поддерживаемые форматы USB-накопителя - FAT32 емкостью от 4 до 128 ГБ.

Процедура

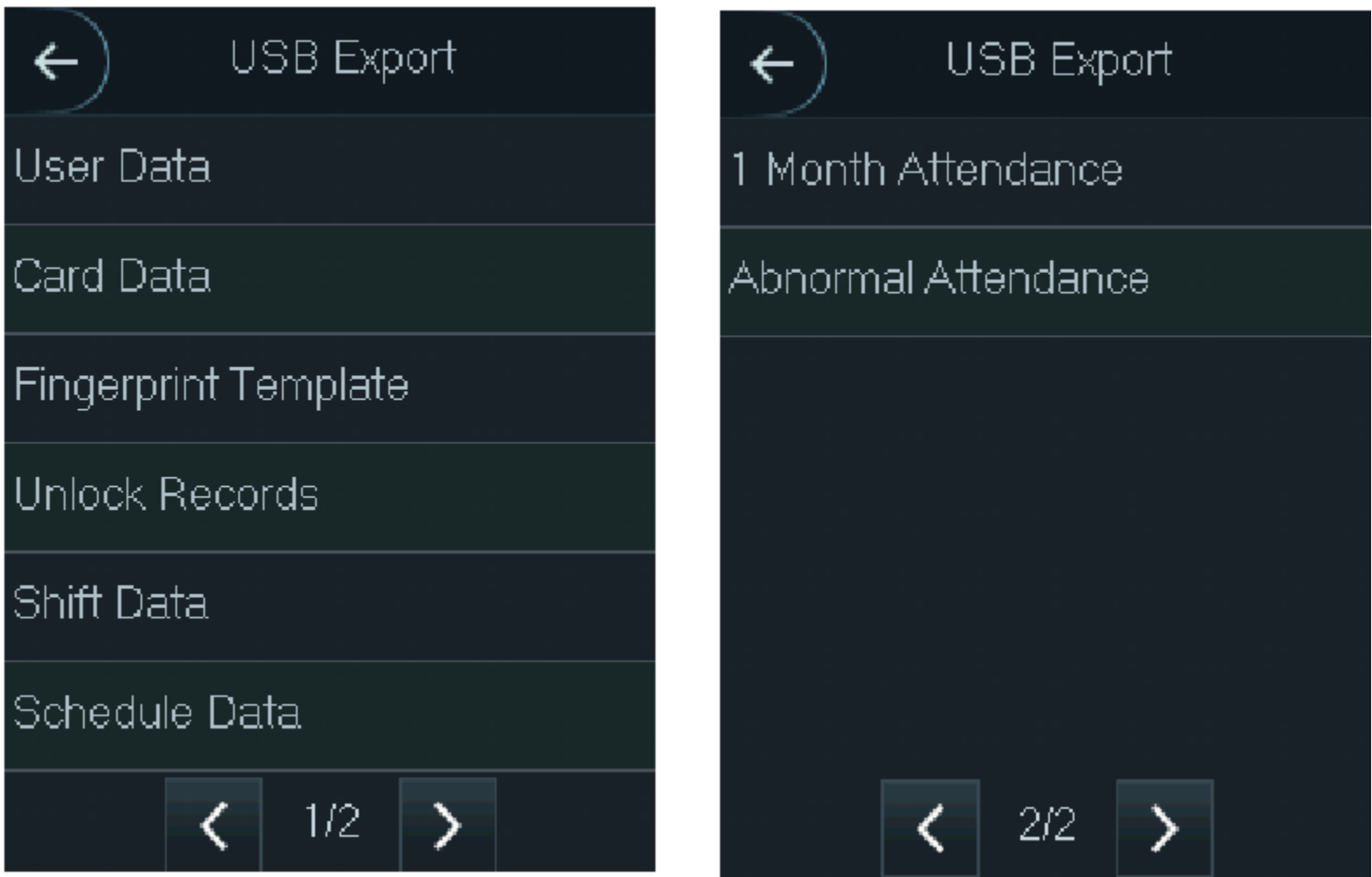
- Шаг 1 В главном меню выберите USB> USB Export.
- Шаг 2 Выберите тип данных, которые необходимо экспортировать, а затем нажмите OK.

Экспортированная информация будет сохранена на USB-накопителе.



Когда экспортируемые данные представлены в формате Excel, их можно редактировать
Данные пользователя, данные карты и данные отпечатка пальца экспортируются в зашифрованном виде.

Рисунок 3-35 USB-экспорт



3.12.2 Импорт данных

На другое устройство можно импортировать только данные, экспортированные с одного устройства.

Предварительные требования

USB-накопитель вставлен и правильно распознается устройством.

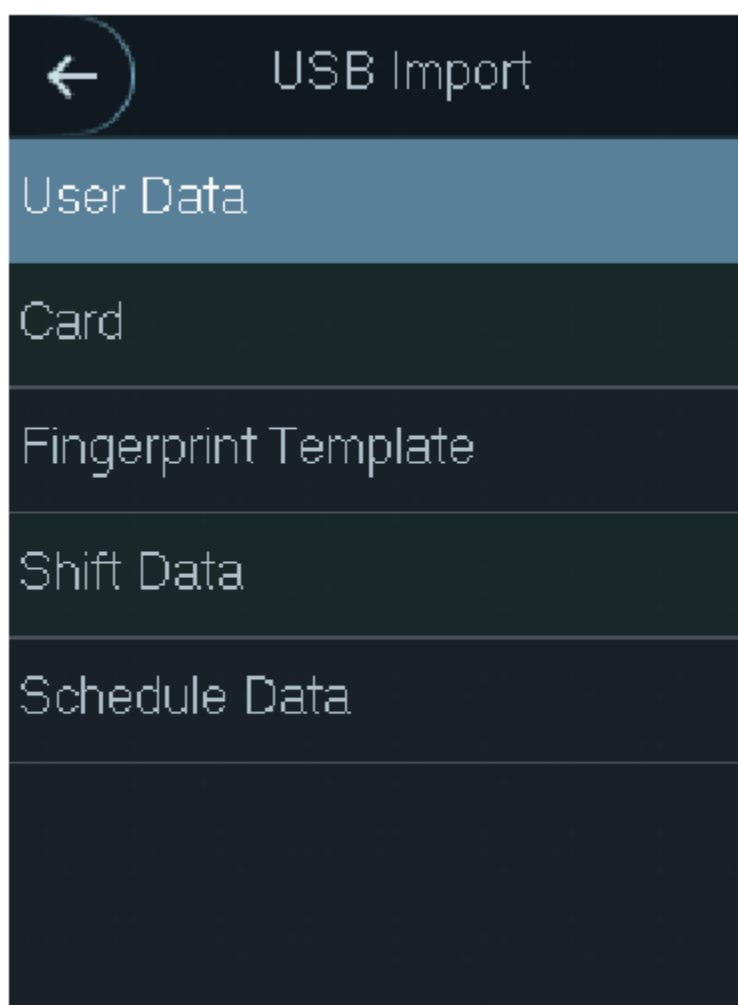
Процедура

- Шаг 1 В главном меню выберите USB> USB Импорт.
- Шаг 2 Выберите тип данных, который необходимо импортировать, а затем нажмите OK



Рекомендуется импортировать данные между устройствами одной модели и версии. Импорт данных между разными моделями или версиями может привести к потере данных.

Рисунок 3-36 Импорт через USB



3.12.3 Обновление устройства

Выполняйте обновление системы с помощью USB-накопителя.



Для новых устройств или после сброса настроек резервные копии системных файлов создаются в течение первых 10 минут после запуска. Обновление в течение этого времени не рекомендуется.

Процедура

Шаг 1 Переименуйте файл обновления в update.bin и сохраните его в корневом каталоге USB-накопителя.

Вставьте USB-накопитель в устройство.

Шаг 2 Войдите в главное меню устройства.

Шаг 3 Выберите USB> Обновление по USB.

На экране отобразится запрос на подтверждение.

Шаг 4 Нажмите ОК для обновления.

Обновление системы началось. Устройство автоматически перезагрузится после завершения обновления завершено.

3.13 Управление записями

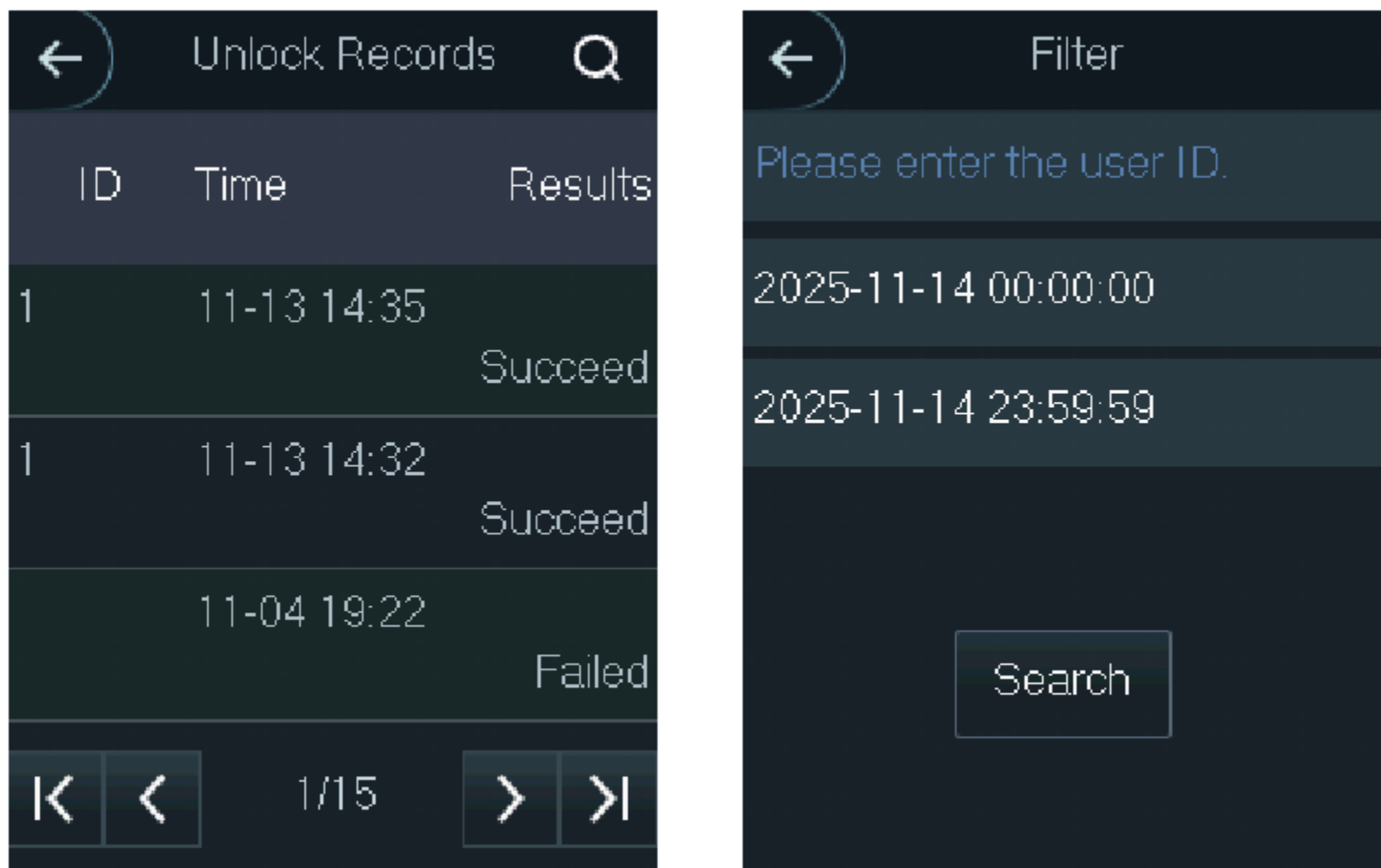
Процедура

Шаг 1 В главном меню выберите пункт Записи.

Отобразятся записи разблокировки.

Шаг 2 (Необязательно)  Нажмите в правом верхнем углу, введите идентификатор пользователя, выберите период времени и затем нажмите Поиск.

Рисунок 3-37 Разблокировка записей



3.14 Просмотр информации

Вы можете просмотреть объем данных и версию устройства.

3.14.1 Просмотр объема данных

В главном меню выберите Информация об устройстве> Объем данных. Вы можете просмотреть объем хранилища для каждого тип данных.

3.14.2 Просмотр версии устройства

В главном меню выберите Информация об устройстве> Версия устройства. Вы можете просмотреть версию устройства, например модель продукта, серийный номер, версию программного обеспечения и многое другое.

Коснитесь QR-код документации к продукту, отсканируйте QR-код с помощью телефона, чтобы просмотреть продукт документы.



Эта функция доступна только на некоторых моделях.

4 веб-операции

На веб-странице вы также можете настроить и обновить устройство.



Веб-конфигурации различаются в зависимости от модели устройства.

4.1 Инициализация

Инициализируйте устройство при первом входе на веб-страницу или после восстановления устройства к заводским настройкам по умолчанию.

Необходимые требования.

Убедитесь, что компьютер, используемый для входа на веб-страницу, находится в той же локальной сети, что и устройство. **Процедура**

Шаг 1 Откройте браузер, перейдите по IP-адресу (адрес по умолчанию 192.168.1.108) устройства.



Мы рекомендуем вам использовать последнюю версию Chrome или Firefox.

Шаг 2 Выберите язык на устройстве.

Шаг 3 Установите пароль и адрес электронной почты в соответствии с инструкциями на экране.



В Пароль должен состоять из 8-32 непустых символов и содержать не менее двух типы следующих символов: верхний регистр, нижний регистр, цифры и специальные символы (за исключением " ; : &). Установите пароль повышенной безопасности, следуя паролю запрос на проверку надежности.

Сохраняйте пароль в безопасности после инициализации и регулярно меняйте пароль, чтобы повысить безопасность.

4.2 Вход в систему

Процедура

Шаг 1 Откройте браузер, введите IP-адрес устройства в адресной строке и нажмите Клавишу Enter.

Шаг 2 Введите имя пользователя и пароль.



В Имя администратора по умолчанию - admin, а пароль - тот, который вы установили во время инициализации. Мы рекомендуем вам регулярно менять пароль администратора для повышения безопасности.

Если вы забыли пароль администратора для входа в систему, вы можете нажать "Забыть пароль"? Для сбросьте пароль.

Шаг 3 Нажмите Войти.

4.3 Сброс пароля

Сбросьте пароль по указанному электронному письму, если вы забыли пароль администратора. Если электронного письма нет адрес был введен для сброса пароля, вам необходимо связаться с местным дилером или службой технической поддержки.

Процедура

- Шаг 1 На странице входа нажмите Забыли пароль?.
- Шаг 2 Внимательно прочитайте приглашение на экране, а затем нажмите ОК.
- Шаг 3 Отсканируйте QR-код, и вы получите защитный код.

Рисунок 4-1 Сброс пароля



Please scan QR code.

Note (for admin only):

Please use an app that can scan and identify QR codes to scan the QR code on the left. Please send the results of the scan to support_rpwd@global.damtech.com.

Email Address: 1***@com

Security code:

Next



При сканировании одного и того же QR-кода будет сгенерировано до двух кодов безопасности. Если защитный код становится недействительным, обновите QR-код и отсканируйте еще раз.

После сканирования QR-кода вы получите защитный код по связанному с ним электронному письму адрес. Используйте защитный код в течение 24 часов после его получения. В противном случае он станет недействительным.

Если 5 раз подряд ввести неправильный защитный код, учетная запись администратора будет заморожен на 5 минут.

- Шаг 4 Введите код безопасности.
- Шаг 5 Нажмите Далее.
- Шаг 6 Сбросьте и подтвердите пароль.



Пароль должен состоять из 8-32 непустых символов и содержать не менее двух из следующие типы символов: верхний регистр, нижний регистр, число и специальный символ (исключая " ; : &).

- Шаг 7 Нажмите ОК.

4.4 Доступ к мониторингу

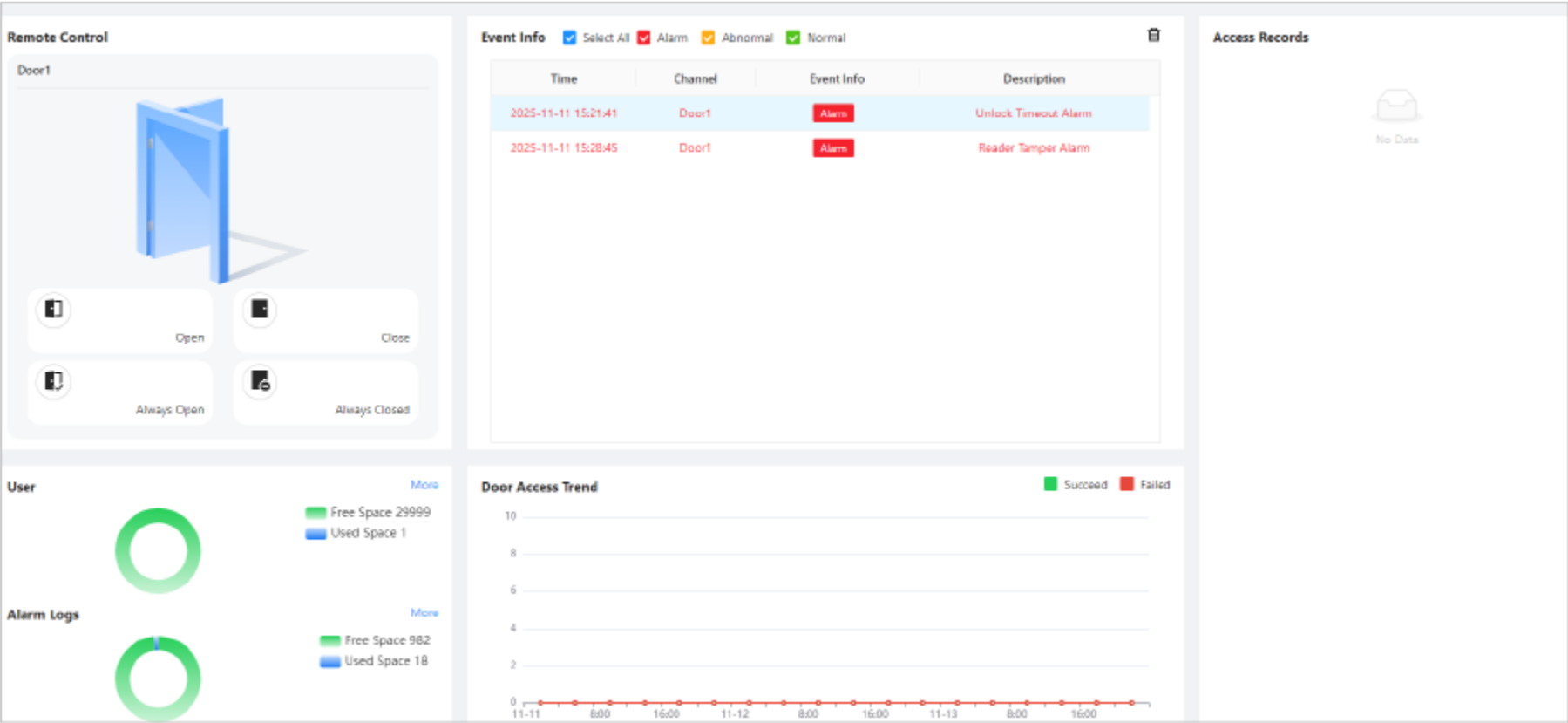
Войдите на веб-страницу, и система автоматически перейдет на страницу Мониторинга доступа.



Для Первого использования, пожалуйста, загрузите и установите плагин в соответствии с подсказкой.

Вы также можете щелкнуть значок веб-службы в левом верхнем углу, чтобы просмотреть мониторинг доступа Страница.

Рисунок 4-2 Контроль доступа



Дистанционное управление

Нажмите Открыть или закрыть рядом с дверью, чтобы дистанционно управлять дверью.

Нажмите Всегда открывать или всегда закрывать, чтобы дистанционно управлять дверью. Нажмите Восстановить, чтобы восстановить дверь в нормальное состояние.

Тенденция доступа к двери

Отображается динамика доступа за последние 3 дня. Зеленый означает успешный доступ, а красный - доступ не удался.

Доступ к записям

Отображаются записи о доступе в режиме реального времени, включая изображение, информацию о персонаже, верификацию метод и время верификации.

Информация о событии

В области Информации о событии выберите тип события, чтобы просмотреть события. Нажмите  чтобы очистите все события.

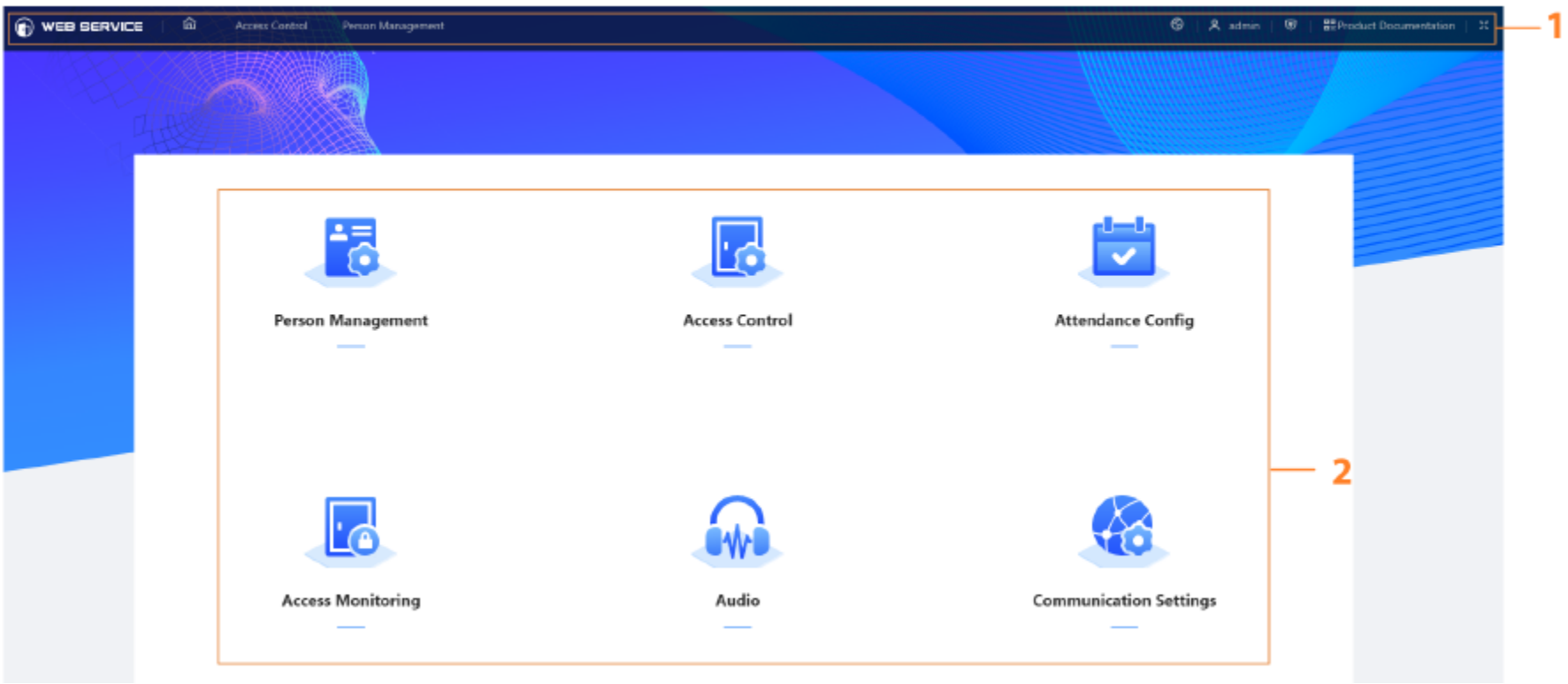
Журналы пользователей и тревог.

Просмотрите информацию о пространстве пользователей и журналы тревог. Нажмите Еще, чтобы просмотреть подробности.

4.5 Домашняя страница

Щелкните  в левом верхнем углу или на веб-странице, чтобы перейти на главную страницу.

Рисунок 4-3 Домашняя страница



Описание домашней страницы в таблице 4-1

No.	Description
1	• : Go to the home page. • : Select a language on the device. •  admin: Log out or restart the device. • : Enter the Security page. •  Product Documentation: Scan the QR code with your phone to view the product documents.  This function is only available on select models • : Display in full screen.
2	Main menu.

4.6 Управление персоналом

Процедура

- Шаг 1

На домашней странице выберите Управление персоналом, а затем нажмите Добавить.
- Шаг 2

Настройте информацию о пользователе.

Рисунок 4-4 Основная информация

Basic Info

* ID

* Department

1-

Validity Period

Forever

* User Type

General User

* General Plan

255-Default x

Permission Type

Unlock and Attendance

Name

* Schedule Mode

Department Schedule

* Permission

User

* Times Used

Unlimited

* Holiday Plan

255-Default x

Email

Verification Mode

Same as Device

Custom

Combination Meth...

And

Or

* Unlock Method

Card x

Fingerprint x

Password x

Bluetooth Card x

Таблица 4-2 Описание основной информации

Параметр	Описание
ID _	Идентификатор пользователя подобен идентификатору сотрудника, который может быть комбинациями, а максимальная длина номера составляет 30 символов.
Имя	Название может содержать до 32 символов (включая цифры, условные обозначения и буквы).
Отдел	Добавление пользователей в отдел. Если сотруднику назначено расписание отдела, он будет следовать установленному расписанию. Если не назначено, он создаст отдел, смотрите в разделе "4.8.1 Настройка отделов".
Режим расписания	Расписание отдела: назначьте пользователю расписание отдела. Для получения подробной информации смотрите "4.8.4 Настройка графиков работы". Личное расписание: назначьте пользователю личное расписание. Дополнительные сведения смотрите "4.8.4 Настройка графиков работы". ° Эта функция доступна только на некоторых моделях. Если вы установите здесь для режима расписания значение "Расписание отдела", то личное расписание, настроенное вами для пользователя в разделе "Посещаемость" > "Настройка расписания" > "Личное расписание", будет недействительным.
Срок действия	Установите дату, когда истечет срок действия разрешений на доступ к двери и посещение человека.
Разрешение	Пользователь: У пользователей есть только разрешения на доступ к двери или посещение. Администратор: Администраторы могут настраивать устройство помимо доступа к двери и посещения. Разрешений на посещение.

76

Параметр	Описание
Тип пользователя	Заблокировать Гостевой режим в определенное время Патрулирования, не VIP режимы, Другое подробнее Пользовательский пользователь 1 / Пользовательский пользователь 2: Такие же, как у обычных пользователей.
Использованное время	Установите разблокировку
Общий план	Люди, которых вы можете
План отдыха	Люди Вы можете
Тип разрешения	Разблокировать разблокировать • разблокировать один
Режим проверки.	Настройте тот же же пользовательский метод Или: o o

Обычный пользователь: Обычные пользователи могут разблокировать дверь.
Пользователь: Когда пользователи из списка заблокированных персоналов получат уведомление.
Пользователь: Гости могут отпирать дверь в течение определенного количества раз. По истечении установленного времени они не смогут отпереть дверь.
Пользователь : Патрульные пользователи могут следить за пользователями, у которых есть права доступа к двери.
Пользователь: Когда VIP-персоны открывают дверь, они не смогут использовать такую как мультикарта и раздел времени.
Пользователь: Когда он откроет дверь, она останется незапертой в течение 10 секунд.
Пользовательский пользователь 1 / Пользовательский пользователь 2: Такие же, как у обычных пользователей.

ограничение на разблокировку для приглашенных пользователей. Пользователь может открыть дверь.

вы можете отпереть дверь или записаться на прием в течение определенного времени. Выберите более одного плана.

вы можете отпереть дверь или записаться на прием в течение определенного времени.

выберите более одного праздника.

и посещаемость: У человека есть разрешение на посещение и разблокировку двери, используя настроенные методы проверки.
Посещаемость: У человека есть только разрешение на посещение и разблокировку двери. После того, как пользователь успешно подтвердит свое посещение, генерируется запись о сбросе разблокировки.

режим проверки для человека. Вы можете использовать режим проверки от имени устройства, или настроить режим проверки от имени устройства: режим такой же, как и у устройства.
: После выбора пользовательского режима отображаются комбинации методов. Выберите комбинированный метод и разблокируйте методы по мере необходимости.
Используйте один из выбранных методов разблокировки, чтобы проверить режим проверки.
И: Используйте все выбранные методы разблокировки, чтобы проверить режим проверки.

настраиваемый режим проверки действителен только для устройств, которые не являются внешними кард-ридерами.
Если настроенный режим проверки отличается от режима проверки устройства, приоритет отдается настроенному режиму.

Рисунок 4-5 Учетные данные для доступа

Access Credentials

▼ PasswordNot Added

Add

> CardNot Added

> FingerprintNot Added

> Bluetooth CardNo email was configured. You cannot request a Bluetooth card through email.Not Added

Таблица 4-3 Описание учетных данных для доступа

Параметр	Описание
Пароль	Введите пароль пользователя. Максимальная длина пароля - 8 цифр. Принудительный пароль - это пароль разблокировки + 1. Например, если у пользователя пароль равен 12345, то принудительный пароль будет равен 12346. Сигнал тревоги о принудите срабатывать, когда для отпираания двери используется пароль принудительного ввода.

Параметр	Описание
Карта	Функция карты доступна только на некоторых моделях. Пользователь может зарегистрировать не более 5 карт. Введите номер своей карты или проведите карту на устройстве или внешнем кард-ридере, и тогда информация с карты будет считана устройством. Только определенные модели поддерживают сбор данных через внешнее устройство чтения карт. Введите номер карты вручную. 1. Нажмите Добавить. 2. Введите номер карты, а затем нажмите Добавить. Считайте номер автоматически с помощью устройства для регистрации или устройства. 1. Нажмите "Добавить", а затем "Изменить", чтобы выбрать устройство для регистрации или устройство. 2. Прочтите карточку. o Для считывания регистрационных данных IC и ID-карты нажмите "Прочитать карточку", а затем проведите карточками по считывателю карт. Отображается 60-секундный обратный отсчет, напоминающий вам о том, что нужно провести карту, и система автоматически считывает номер карты. Если истечет 60-секундный обратный отсчет, нажмите "Прочитать карточку" еще раз, чтобы начать новый обратный отсчет. o Для считывателя регистрации карты Desfire поместите карточку на считыватель регистрации, а затем нажмите "Прочитать карточку". Если на карте Desfire указан номер карты, он будет считан и отображен здесь. Если карта пуста, то сначала нужно ввести номер карты. . Номер карты будет автоматически сгенерирован на компьютере и будет записан на карту. 3. Нажмите Добавить. Вы можете включить функцию принудительной карты. Если для отпирания двери будет использована принудительная карта, сработает сигнализация. à: Установите принудительную карту. : Измените номер карты. Один пользователь может установить только одну принудительную карту.

Параметр	Описание
Отпечаток пальца	Регистрируйте отпечатки пальцев. Пользователь может зарегистрировать до 3 отпечатков пальца в качестве отпечатка пальца принуждения. Сигнал тревоги сработает, принудительный отпечаток пальца. Регистрируйте отпечатки пальцев с помощью внешнего регистрационного считывателя. Только определенные модели поддерживают сбор отпечатков пальцев через внешний регистрационный считыватель. 1. Нажмите "Добавить", а затем "Изменить", чтобы выбрать регистрационный считыватель устройства. 2. Нажмите пальцем на сканер в соответствии с инструкциями на экране. 3. Нажмите Добавить. Функция отпечатка пальца доступна только на некоторых моделях. Мы не рекомендуем устанавливать первый отпечаток пальца в качестве принудительного отпечатка пальца. Один пользователь может установить только один принудительный отпечаток пальца. Функция снятия отпечатка пальца доступна, если устройство поддерживает подключение модуля снятия отпечатка пальца.
Карта Bluetooth	Bluetooth доступен только на некоторых моделях. Вы можете выбрать Запрос по электронной почте или запрос через регистрационный код. Запрос по электронной почте: подходит для первого запроса карты Bluetooth . Вы можете запросить до 5 карт Bluetooth и должны использовать адрес электронной почты, зарегистрированный в DMSS. Вы должны ввести свой зарезервированный адрес электронной почты, прежде чем использовать эту функцию. 1. Настройте адрес электронной почты, зарегистрированный в DMSS. 2. Нажмите "Запросить по электронной почте", после чего можно запросить карты Bluetooth. Запрос через регистрационный код: подходит, если у вас уже есть карта Bluetooth и вы хотите повторно использовать ее на другом контроллере доступа, поддерживающем функцию Bluetooth. 1. Скопируйте регистрационный код Bluetooth из DMSS. 2. Нажмите "Запросить через регистрационный код", а затем введите код. 3. Нажмите "ОК". Шаг 3. Нажмите "Добавить".

Вы можете нажать "Добавить еще", чтобы добавить других пользователей.

Связанные операции

- Очистить: очистить всех пользователей.
- Обновить: обновить список пользователей.
- Поиск: поиск по имени пользователя или идентификатору пользователя.

Щелкните Записи карт Bluetooth, а затем вы сможете просмотреть записи карт Bluetooth. Для пользователей которые выпустили карты неудачно, вы можете перевыпустить карты здесь.



Карты можно выпускать партиями на устройствах, поддерживающих функцию Bluetooth.

4.7 Управление контролем доступа

4.7.1 Параметры контроля доступа

4.7.1.1 Настройка основных параметров

Процедура

- Шаг 1
- Выберите Управление доступом > Параметры управления доступом.
- Шаг 2
- В разделе Основные настройки настройте основные параметры для управления доступом.

Рисунок 4-6 Основные параметры

Basic Settings

Name

Door1

Door Status

☒ Normal

☐ Always Closed

☐ Always Open

Normally Open Period

General Plan

Disabled

Holiday Plan

Disabled

Normally Closed Period

General Plan

Disabled

Holiday Plan

Disabled

Verification Interval

0

s (0-180)

Card Swiping Interval

0

s (0-86400)

Public Password

☐

Таблица 4-4 Описание основных параметров

Parameter	Description
Name	The name of the door.
Door Status	Set the door status. Normal: The door will be locked and unlocked according to your settings. Always open: The door remains unlocked all the time. Always closed: The door remains locked all the time.

Параметр	Описание
Обычно Открытый Период	Выбрав "Обычный", вы можете выбрать шаблон времени из раскрытого списка.
Период закрытия в обычном режиме	• Дверь остается открытой или закрытой в течение заданного времени. Дополнительные сведения о том, как настроить общие периоды, см. в разделе "4.7.4 Настройка периодов". • Когда нормально открытый период конфликтует с нормально закрытым периодом, нормально открытый период имеет приоритет над нормально закрытым периодом. Когда общий план противоречит плану отпусков, план отпусков имеет приоритет над общим планом.
Интервал проверки	Если вы подтвердите свою личность несколько раз в течение определенного периода времени, самая ранняя проверка будет считаться действительной, и дверь не откроется после второй или более поздних проверок. С момента, когда дверь не открывается, вы должны дождаться установленного времени, прежде чем пытаться подтвердить свою личность снова.
Интервал между перемещениями карты	Для первой проверки с помощью карты вы обычно можете отпереть дверь или выполнить явку, и записи будут сгенерированы. В течение заданного периода времени, если вы снова проведете картой для проверки, вы не сможете отпереть дверь или выполнить проверку посещаемости, и записи не будут сгенерированы. Пожалуйста, подтвердите идентификацию в конце периода. Интервал считывания карты имеет приоритет над интервалом проверки.
Общедоступный пароль Шаг 3 Нажмите Применить.	После включения общедоступного пароля настройте пароль. Вы можете использовать общедоступный пароль без ввода идентификационной карты. Для одного устройства поддерживается только один общедоступный пароль.

4.7.1.2 Настройка методов разблокировки

Для разблокировки двери можно использовать несколько методов разблокировки, таких как отпечаток пальца, карточка и пароль. Вы также можете объединить их, чтобы создать свой собственный метод разблокировки.

Процедура

Шаг 1 Выберите **Контроль доступа> Параметры контроля доступа.**

Шаг 2 В настройках разблокировки выберите метод разблокировки.

Комбинированная разблокировка

1. Выберите **Комбинированная разблокировка** в списке методов разблокировки.

2. Выберите **Или или И.**

 ◇ Или: Используйте один из выбранных методов разблокировки, чтобы открыть дверь.

 ○ И: Используйте все выбранные методы разблокировки, чтобы открыть дверь.

3. Выберите методы разблокировки, а затем настройте другие параметры.

Рисунок 4-7 Комбинированная разблокировка

Unlock Settings

Unlock Method

Combination Unlock

Combination Method

☒ Or

☐ And

Unlock Method (Multi-select)

☒ Card

☒ Fingerprint

☒ Password

☒ Bluetooth Card

Bluetooth Mode

☐ Short-range

☒ Long-range

PIN Code Authentication

☐

Door Unlocked Duration

3.0

s (0.2-600)

Remote Verification

☐

Apply

Refresh

Default

Разблокировка несколькими пользователями.

- ◇ Если добавлена только одна группа, дверь разблокируется только после того, как количество людей в группе, предоставляющей доступ, сравняется с определенным допустимым числом.
- ◇ Если добавлено более одной группы, дверь разблокируется только после того, как количество людей в каждой группе, которые предоставляют доступ, сравняется с определенным допустимым числом.

1. В списке режимов разблокировки выберите Разблокировать несколькими пользователями.
2. Нажмите Добавить, чтобы добавить группы.
3. Выберите способ разблокировки и пользователей, настройте действительный номер и затем нажмите "ОК".
 - ◇ Вы можете добавить до 4 групп.
 - ◇ Методы разблокировки поддерживают только связь Или.
 - Действительное число указывает количество людей в каждой группе, которым необходимо подтвердите их личность на устройстве, прежде чем дверь откроется. Например, если для действительного номера установлено значение 3 для группы, любые 3 человека в группе должны подтвердить их идентификационные данные для разблокировки двери.

Действительный номер не может превышать количество пользователей в списке пользователей.

Рисунок 4-8 Добавление группы

Add

No.1

Unlock Method ...Card x

Select PersonUser ID/Name

	No.	User ID	Name
☒	1	1000...	10000001
☒	2	1000...	10000002
☐	3	1000...	10000003
☐	4	1000...	10000004
☐	5	1000...	10000005

Valid No.1

Selected PeopleClear

No.	User ID	Name	Operation
1	100000...	100000...	
2	100000...	100000...	

OK

Cancel

Рисунок 4-9 Разблокировка несколькими пользователями

Unlock Settings

Unlock MethodUnlock by Multiple Users

You can add up to 4 multi-person unlock groups.

Add

No.	User List	Unlock Method	Valid No.	Operation

Verification of Multi-person Unlock Timeout Duration20s (10-60)

Bluetooth ModeShort-rangeMid-rangeLong-range

PIN Code Authentication

Door Unlocked Duration3.0s (0.2-600)

Remote Verification

Apply

Refresh

Default

Таблица 4-5 Описание настроек разблокировки

Параметр	Описание
Способ разблокировки (множественный выбор)	Способы разблокировки продукта.
Проверка длительности тайм-аута разблокировки для нескольких пользователей	Во время проверки интервал должен соответствовать этому параметру.

Параметр	Описание
Аутентификация по PIN-коду	Когда включена аутентификация по PIN-коду и вы выбираете пароль для разблокировки, вам нужно ввести только пароль пользователя без идентификатора пользователя.
	Когда включена аутентификация по PIN-коду, удаленная проверка не поддерживается при использовании пароля пользователя для
Режим Bluetooth	Выберите диапазон для Bluetooth. Вы можете выбрать режим дальнего и ближнего действия. Он доступен только для устройств с функцией Bluetooth.
Продолжительность разблокировки дверей	После того, как человеку будет предоставлен доступ, дверь остается открытой в течение определенного времени, необходимого для прохождения, 0,2 до 600 секунд.
Удаленная проверка.	Если эта функция включена, вы можете управлять дверью на соответствующей платформе.

- Разблокировка по периодам

1. В списке Методов разблокировки выберите Разблокировать по периодам.

2. Переместите ползунок, чтобы настроить период времени для каждого дня.



Вы также можете нажать Копировать, чтобы применить настроенный период времени к другим дням.

3. Выберите метод разблокировки для данного периода времени, а затем настройте другие параметры.

Рисунок 4-10 Разблокировка по периоду

Unlock Method

Unlock by Period

Sun	Card/Fingerprint/Password	Copy
Mon	Card/Fingerprint/Password	Copy
Tue	Card/Fingerprint/Password	Copy
Wed	Card/Fingerprint/Password	Copy
Thu	Card/Fingerprint/Password	Copy
Fri	Card/Fingerprint/Password	Copy
Sat	Card/Fingerprint/Password	Copy

Time

00:00:00 - 23:59:59

Combination ...
☒ Or ☐ And

Unlock Method...
☒ Card ☒ Fingerprint ☒ Password

OK Delete

Door Unlocked Duration

3.0 s (0.2-600)

Remote Verification

☐

Шаг 3 Нажмите кнопку Применить.

4.7.2 Аварийный сигнал

4.7.2.1 Настройка сигнализации

При возникновении события аварийного доступа будет срабатывать аварийный сигнал. Процедура

Шаг 1 Выберите Контроль доступа> Тревога> Тревога.

Шаг 2 (Необязательно) Выберите дверной канал.

Если вы выбрали модуль расширения блокировки в качестве внешнего устройства через Настройки связи> Настройки RS-485 на контроллере доступа, вы можете выбрать канал здесь.

Рисунок 4-11 Выбор канала

Door Channel

1

▼

Шаг 3 Настройка параметров сигнала тревоги.

Рисунок 4-12 Сигнал тревоги

Duress Alarm

Anti-passback

Door Detector

NCNO

Intrusion Alarm

Unlock Timeout Alarm

Unlock Timeout

60

s (1-9999)

Excessive Attempts Ala...

Apply

Refresh

Default

Таблица 4-6 Описание параметров сигнала тревоги

Параметр	Описание
Сигнализация о Принуждении	Сигнал тревоги срабатывает, когда для отпирания двери используется принудительный пароль или отпечаток пальца.

Параметр	Описание
Защита от обратной передачи	Пользователям необходимо подтвердить свою личность как при входе, так и при выходе. Если в противном случае будет подан сигнал тревоги. Это помогает предотвратить кражу карты. Владелец карты не сможет передать карту доступа обратно другому человеку для получения доступа. Когда защита от обратного доступа включена, пользователь должен покинуть охраняемую зону через считывающее устройство. Если система разрешит другой вход. Если человек входит после авторизации и выходит без повторной авторизации, при повторной попытке входа сработает аварийный сигнал, и в то же время доступ будет запрещен. Если человек входит без авторизации и выходит после повторной авторизации, при повторной попытке входа сработает аварийный сигнал, и в то же время доступ будет запрещен. Если устройство может подключить только один замок, проверка устройства означает направление входа, а проверка на внешнем считывателе карт по умолчанию означает направление выхода. Если устройство поддерживает несколько замков, настройку на платформе управления.
Дверной извещатель	С помощью дверного извещателя, подключенного к вашему устройству, можно настроить срабатывать сигнализация при неправильном открытии или закрытии двери. Дверной детектор бывает двух типов, включая детектор с ЧПУ и детектор без детектора. NC: датчик находится в замкнутом положении, когда дверь или окно закрыты. NO: Разомкнутая цепь возникает, когда окно или дверь фактически закрыты.
Сигнализация о вторжении	Если дверь открывается нештатно, сработает сигнализация о вторжении, которая будет действовать до тех пор, пока дверь не будет закрыта. Дверной детектор и система вторжения должны быть включены одновременно.
Сигнализация о тайм-ауте разблокировки Тайм-аут разблокировки	Когда дверь остается незапертой дольше, чем заданный тайм-аут, срабатывает сигнализация тайм-аута двери, которая действует в течение заданного времени. Дверной детектор и функция тайм-аута двери должны быть включены одновременно.
Сигнал тревоги о чрезмерных попытках	Если 5 раз подряд в течение 60 секунд будет использован неправильный пароль или карта, будет сработать сигнал тревоги о чрезмерном использовании незапертой двери.

Шаг 4 Нажмите кнопку Применить.

4.7.2.2 Настройка подключения сигнализации (необязательно)

Вы можете настроить подключение сигнализации.

Процедура

Шаг 1 Выберите Управление доступом> Сигнализация> Настройка подключения сигнализации.



Если устройство добавлено к платформе управления, настройки сигнализации будут синхронизированы с платформой.

Эта функция доступна только на моделях с портами ввода и вывода сигнала тревоги .

В количество портов ввода и вывода сигнала тревоги отличается в зависимости от модели продукт.



Шаг 2 Нажмите , чтобы настроить сигнал тревоги.

Рисунок 4-13 Привязка сигнала тревоги

Modify

Alarm-in Port

1

Name

Zone1

Alarm Input Type

NO

Link Fire Safety Control

Alarm-out Port

Duration

30

s (1-300)

Alarm Output Channel

☒ 1

Access Control Linkage

When the heat alarm signal disappears, the door will automatically return to the normal authentication mode.

Linkage Mode

Weak Execution

Channel Type

NO

OK

Cancel

Шаг 3 Создайте название для зоны тревоги.

Шаг 4 Включите Link Fire Safety Control и выберите тип устройства ввода сигнала тревоги.

NC: вход сигнала тревоги находится в нормально замкнутом состоянии (NC), когда сигнал тревоги не был сработал. Размыкание нормально замкнутой цепи приводит к срабатыванию сигнализации.

НЕТ: устройство ввода сигнала тревоги находится в состоянии нормально разомкнутой цепи, когда сработал сигнал тревоги не было срабатывания. Замыкание цепи приводит к срабатыванию сигнализации.

Шаг 5 Если вы хотите подключить контроль доступа при срабатывании пожарной сигнализации, включите контроль доступа



Эта функция вступает в силу только после включения управления пожарной безопасностью Link. Выберите режим подключения.

Шаг 6

Надежное выполнение: когда сигнал пожарной сигнализации исчезает, дверь остается в текущем состоянии Статус. Пожалуйста, вручную измените настройки предыдущего состояния двери, если хотите.

Слабый режим работы

Выполнение: когда сигнал пожарной сигнализации исчезает, дверь автоматически возвращается к своему предыдущему состоянию двери.

Шаг 7

Выберите тип канала.

НЕТ: дверь автоматически открывается при срабатывании пожарной сигнализации.

Шаг 8

НС: дверь автоматически закрывается при срабатывании пожарной сигнализации. **Нажмите ОК.**

4.7.2.3 Настройка привязки событий тревоги

Процедура

Шаг 1 Выберите Управление доступом> Тревога> Привязка событий тревоги.

Шаг 2 Настройте привязки событий тревоги, а затем нажмите Применить.

Рисунок 4-14 Привязка событий тревоги

Intrusion Alarm Linkage

Please enable Intrusion Alarm.

Buzzer

Enable

Duration

15

s (1-1800)

Link Alarm Output

Enable

Duration

15

s (1-1800)

Unlock Timeout Alarm Linkage

Please enable Unlock Timeout Alarm.

Buzzer

Enable

Duration

Custom Time

15

s (1-1800)

Link Alarm Output

Enable

Duration

Custom Time

15

s (1-1800)

Max Use Alarm Link

Buzzer

Enable

Duration

15

s (1-1800)

Link Alarm Output

Enable

Duration

15

s (1-1800)

Tamper Alarm Linkage

Buzzer

Enable

Duration

3

s (1-1800)

Link Alarm Output

Enable

Duration

15

s (1-1800)

Apply

Refresh

Default

Таблица 4-7 Привязка событий будильника

Параметр	Описание
Система Сигнализации о вторжении	Если дверь открывается нештатно, сработает звуковой сигнал: звуковой сигнал звучит п... можете настроить продолжительность сип... Выходной сигнал связи: внешнее устройст... при срабатывании сигнализации о вторже... .
Сигнализация тайм-аута разблокировки Привязка	Когда дверь остается незапертой дольше, ... продолжительность, срабатывает сигнали... заданного времени. Звуковой сигнал: звуковой сигнал звучит п... срабатывании сигнала ожидания разблоки... закроется. o Пока дверь не закроется: звук будильник... закроется. o Пользовательское время: вы можете наст... Локальный вывод сигнала тревоги: внешне... при срабатывании сигнала ожидания разб... пользовательского времени и до тех пор, п... Пока дверь не закроется: сигнал тревоги пр... закрыта. o Пользовательское время: вы можете настр...
Максимальное использование ссылки на сигнал тревоги	При использовании неправильного пароля... секунд, сработает сигнализация о чрезмер... будет действовать в течение определенной... Звуковой сигнал: звуковой сигнал звучит п... . Вы можете настроить продолжительности... Выходной сигнал связи: внешнее устройст... при срабатывании сигнала ожидания разб... продолжительность сигнала тревоги.
Подключение сигнализации о несанкционированном вскрытии	Сигнализация о несанкционированном вскр... повредить устройство. Звуковой сигнал: звуковой сигнал звучит п... можете настроить продолжительность сип... Выходной сигнал связи: внешнее устройст... при срабатывании сигнализации о несанкн... .

4.7.3 Настройки карты памяти

4.7.3.1 Настройка параметров карты памяти



Эта функция доступна только на некоторых моделях.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите **Управление доступом**> **Настройки карты** > **Настройки карты**.
- Шаг 3 Настройте параметры карты.

Рисунок 4-15 Параметры карты

Card Settings

M1 Card

M1 Card Encryption & Verification

Block NFC Cards

DESFire Card

DESFire Card Decryption

Apply

Refresh

Default

Card No. System

After the number system is changed, the card numbers will become invalid.

Card No. System

Hexadecimal

Decimal

Apply

Refresh

Default

DESFire Card Write

Acquisition De...

Device

Please place the card on the swiping area and enable DESFire card and DESFire Card Decryption.

Card Number

Write

Таблица 4-8 Описание параметров карты

Элемент	Параметр	Описание
Настройки карты	Карта M1	Карту M1 можно считывать, когда эта функция включена. Эта функция доступна только на некоторых моделях.
	Шифрование карты M1 и верификация	Только зашифрованная IC-карта может быть прочитана, когда эта функция включена. Убедитесь, что карта M1 включена. Убедитесь, что карта M1 включена.

Пункт	Параметр	Описание
	Блокируйте NFC-карты.	Предотвратите разблокировку с помощью дублированной карты после включения этой функции. Эта функция доступна только на моделях, поддерживающих IC-карты. Убедитесь, что включена карта M1. Функция NFC доступна только на некоторых моделях телефонов.
	Desfire Card	Устройство может считывать номер карты Desfire Card, когда эта функция включена. Эта функция доступна только на моделях, поддерживающих IC-карты. Поддерживается только шестнадцатеричный формат.
	Расшифровка карты Desfire	Информация на карте Desfire может быть считана, когда одновременно включены Enable Desfire Card и расшифровка карты. Эта функция доступна только на моделях, поддерживающих IC-карты. Убедитесь, что включена функция Desfire card.
Номер карты. Система	Номер карты. Система	Выберите десятичный или шестнадцатеричный формат для номера карты при подключении устройства. Номер карты. Система одинакова как для ввода, так и для вывода на экран.
Отключите запись с карты.	Устройство сбора данных	Выберите устройство, поместите карту на считывающее устройство, введите номер карты, а затем нажмите "Написать", чтобы записать номер карты на карту.
	Номер карты	Функция Desfire card и функция дешифрования Desfire должна быть включена. Поддерживает только шестнадцатеричный формат. Поддерживает до 8 символов.

Шаг 4 Нажмите Применить.

4.7.3.2 Настройка Доступа К Параметрам Правило Карточка

Платформа поддерживает 5 видов форматы Wiegand по умолчанию. Вы также можете добавить пользовательские Виганд форматы.

Процедура

- Шаг 1 Войдите на веб-страницу.

- Шаг 2
- Выберите Контроль доступа> Настройки карты> Настройка правил карты доступа.
- Шаг 3
- Нажмите Добавить, а затем настройте новые форматы Wiegand.

Рисунок 4-16 Добавление новых форматов Wiegand

Add

Wiegand Format

Wiegand88

Total Bits

88

(1-128)

Facility Code

Add

No.	Start Bit	End Bit	Total Bits	Operation
FC	2	33	32	

Card Number

Add

No.	Start Bit	End Bit	Total Bits	Operation
ID0	34	87	54	

Parity Code

Add

Parity Code	Type	Start Bit	End Bit	Total Bits	Operation
1	Odd	2	33	32	
88	Even	34	87	54	

OK

Cancel

Таблица 4-9 Описание формата Wiegand

Параметр	Описание
Формат Wiegand	Название формата Wiegand.
Общее количество битов	Введите общее количество битов.
Код объекта.	Нажмите Добавить, а затем введите начальный и конечный разряды для кода учреждения.
Номер карты	Нажмите Добавить, а затем введите начальный и конечный разряды для номера карты.
Код четности	1. Нажмите Добавить. 2. Введите начальный бит четности и конечный бит четности. 3. Введите начальный бит четности и конечный бит нечетной четности.

Шаг 4 Нажмите ОК.

Связанные операции

Вы также можете нажать кнопку Добавить протокол, чтобы импортировать файл Wiegand на платформу.

Код учреждения: Если функция включена и вы установили номер карточки. Система принимает десятичный формат на странице Управления персоналом код учреждения и номер карточки преобразуются в десятичный формат по отдельности, а затем объединить вместе.

HID26: если функция включена:

- Поддерживается только Wiegand 26.
- Платформа поддерживает отображение карты только в десятичном формате.

В номер карты должен состоять из 5 символов, а код заведения - не более чем из 3 символов . При ручном вводе карты система автоматически добавит начальный ноль к фиксированная длина номера. Например, если введенный вами номер карты состоит менее чем из 5 символов, например, 56, добавляется начальный ноль, чтобы зафиксировать длину номера в 5 символов, например 00056, и еще один 0 добавляется для использования в качестве кода объекта. Следовательно, окончательный номер карты будет 000056.

4.7.3.3 Настройка пользовательского преобразования.

При считывании карт сторонних производителей с помощью встроенного считывателя устройства внешняя карта RS-485 считыватель или внешний кард-ридер Wiegand, если фактический номер карты не совпадает ни с одной картой номер в системе вы можете настроить пользовательское преобразование номера карты, чтобы гарантировать, что преобразованный номер карты соответствует номеру в системе.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Управление доступом> Настройки карты> Пользовательское преобразование.
- Шаг 3 Включите функцию преобразования, а затем выберите режим сопоставления.

Автоматическое сопоставление: используйте встроенное в устройство правило преобразования для преобразования номера карты.

1. Выберите тип ввода.
 - Ввод с устройства: Проведите пальцем по карте на устройстве, чтобы прочитать ее.
 - Вход RS-485: Проведите пальцем по карте на подключенном кард-ридере RS-485, чтобы прочитать ее карта.
 - Ввод Wiegand: Проведите пальцем по карте в подключенном кард-ридере Wiegand, чтобы прочитать карту.
2. Прочитайте номер карты через устройство или введите номер карты перед преобразование, а затем введите номер карты после преобразования.
3. Нажмите "Автоматическое сопоставление".
 - Если номера карт успешно совпадают, вы можете нажать "Экспорт", чтобы экспортировать правило и импорт на другое устройство для быстрого переключения правил сопоставления.
 - Если номера карточек не совпали, это указывает на то, что в системе нет правила сопоставления. Вам необходимо настроить сценарий правила сопоставления и выбрать Импорт Правило преобразования, чтобы импортировать правило на устройство.
 - Если вам нужно изменить правило сопоставления, нажмите Изменить правило сопоставления.

Рисунок 4-17 Автоматическое сопоставление (успешно сопоставлено)

Enable ☒

Matching Mode ☒ Auto Match ☐ Import Conversion Rule

Status

Applied

Default

* Input Type ☒ Device Input ☒ RS-485 Input ☒ Wiegand Input

No.	Card No. Before Conversion (Device Input)	Card No. Before Conversion (RS-485 Input)	Card No. Before Conversion (Wiegand Input)	Card No. After Conversion
1	1A2B3C4D	1A2B3C4D	1A2B3C4D	4D3C2B1A
2				
3				

Successfully Matched
This rule will automatically apply to this device.

Change Matching Rule

Export

Импортируйте правило преобразования: импортируйте другие правила для преобразования номера карты.

Нажмите "Загрузить файл", выберите файл правила и нажмите "Открыть".

Рисунок 4-18 "Импортировать правило преобразования".

Enable

Matching Mode

 Auto Match Import Conversion Rule

Version

2025-03-31

Upload File

Default

You can only upload files in zip format and the size must not exceed 1 MB.

4.7.4 Настройка периодов

Настройте временные интервалы и планы отпусков, а затем вы сможете определить, когда у пользователя есть разрешения на разблокировку дверей.

4.7.4.1 Настройка общего плана

Вы можете настроить до 128 периодов времени (с № 0 по №127). Для каждого периода вам необходимо настроить графики доступа к дверям на целую неделю. Люди могут открывать дверь только в назначенное время.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Управление доступом> Конфигурация периода> Общий план.
- Шаг 3 Нажмите Добавить.

1. Настройте номер плана и название плана.

2. Переместите ползунок времени, чтобы настроить время для каждого дня.

3. (Необязательно) Нажмите Копировать, чтобы скопировать конфигурацию на остальные дни.

Рисунок 4-19 Настройка общего плана

Add

No.

0

General Plan Name

Plan 1

Time Plan

Time

12:30:00

-

23:59:59

OK

Delete

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504
--	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

Шаг 4 Нажмите кнопку ОК.

4.7.4.2 Настройка плана праздников

Вы можете настроить до 128 групп праздников (с №0 по №127), и для каждого праздника сгруппируйте, вы можете добавить в нее до 16 праздников. После этого вы можете назначить настроенные группы праздников плану праздников. Пользователи могут открывать дверь только в течение определенного времени, указанного в плане отпуска.

Процедура

Шаг 1 Войдите на веб-страницу.

Шаг 2 Выберите Управление доступом> Настройка периода> План отпуска.

Шаг 3 Щелкните Управление праздниками, а затем нажмите Добавить.

1. Выберите номер для праздничной группы, а затем введите название группы.

Рисунок 4-20 Добавление праздничной группы

Add

No.

2

Holiday Group Name

Holiday Group for 2023

Holiday Group Config

Add

No.	Holiday Name	Start Time	End Time	Operation
1	National Day	2023-10-01	2023-10-07	 

OK

Cancel

2. Нажмите "Добавить", добавьте праздник в группу праздников, а затем нажмите "ОК".

Рисунок 4-21. Добавьте праздник в группу праздников

Edit

Holiday Name

National Day

* Period

2023-10-01

→

2023-10-07



OK

Cancel

Шаг 4 Нажмите "ОК".

Шаг 5 Выберите "Управление планами", а затем нажмите "Добавить".

1. Выберите номер для плана отдыха, а затем введите для него название.

2. Выберите группу отдыха, а затем перетащите ползунок, чтобы настроить время для каждого дня. Поддерживает добавление до 4 временных разделов в день.

Рисунок 4-22 Добавление плана отпуска

[illegible]

Шаг 6 Нажмите кнопку ОК.

4.7.5 Настройка модулей расширения

Для устройства, поддерживающего подключение модулей расширения, настройте тип модуля, который поддерживает Устройство.

Справочная информация



тип модуля расширения может отличаться в зависимости от модели устройства.

The настройки модуля расширения сохраняются после восстановления заводских настроек устройства по умолчанию.

Процедура

Шаг 1 На веб-странице выберите Управление доступом> Модуль расширения.

Шаг 2 Выберите тип модуля, который поддерживает

Шаг 3 устройство. **Нажмите кнопку Применить.**

Настройки вступают в силу после перезапуска устройства.

отображается в правом углу экрана в режиме ожидания, что означает, что он был успешно установлен.

Готобщается в правом углу экрана в режиме ожидания, что означает тип настроенный вами модуль расширения не соответствует фактическому модулю расширения, который подключен к устройству.

Если выбрано значение "Нет" и ни один модуль расширения не подключен к устройству, значок модуля расширения отображаться не будет.

4.7.6 Настройка внутреннего сравнения

Перед настройками, убедитесь, что устройство подключено к платформе стороннего производителя через SDK. Вы можете напрямую передавать данные, такие как QR-код или номер карты, на платформу стороннего производителя для проверки данных, а не проверку данных на устройстве.

Выберите Управление доступом> Серверное сравнение.

Рисунок 4-23 Внутреннее сравнение

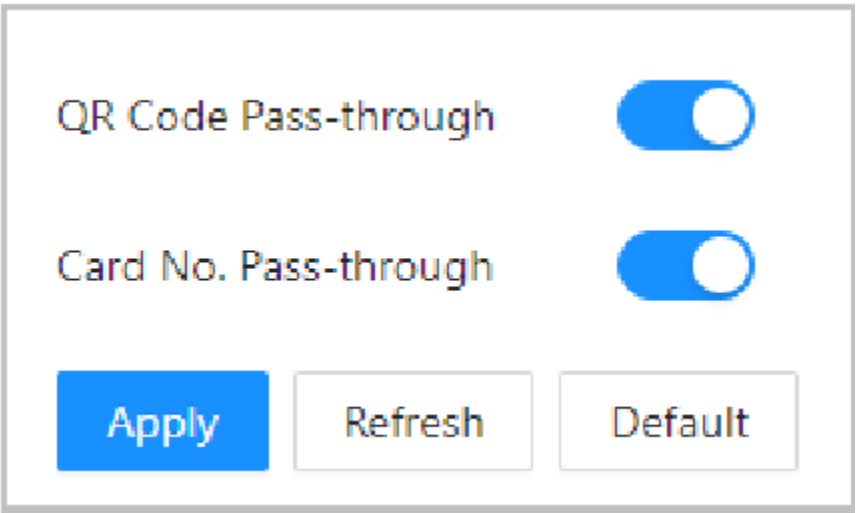


Таблица 4-10 Внутреннее сравнение

Параметры	Описание
Сквозной проход по QR-коду	После включения отсканированный QR-код передается на стороннюю платформу для проверки данных.
Номер карты. Сквозной	После включения номер карты передается сторонней платформе для проверки данных.

4.7.7 Настройка разблокировки от первого лица

Любой пользователь может получить доступ к дверям только после того, как указанные вами лица пройдут через них. Когда вы укажете несколько человек, другие лица могут получить доступ к дверям после того, как любой из указанных лиц пройдет через них.

Предварительные условия

Лица могут быть указаны в качестве первых лиц только в том случае, если у них есть разрешения на доступ к дверям.

Только обычные пользователи могут быть настроены от имени первого лица.

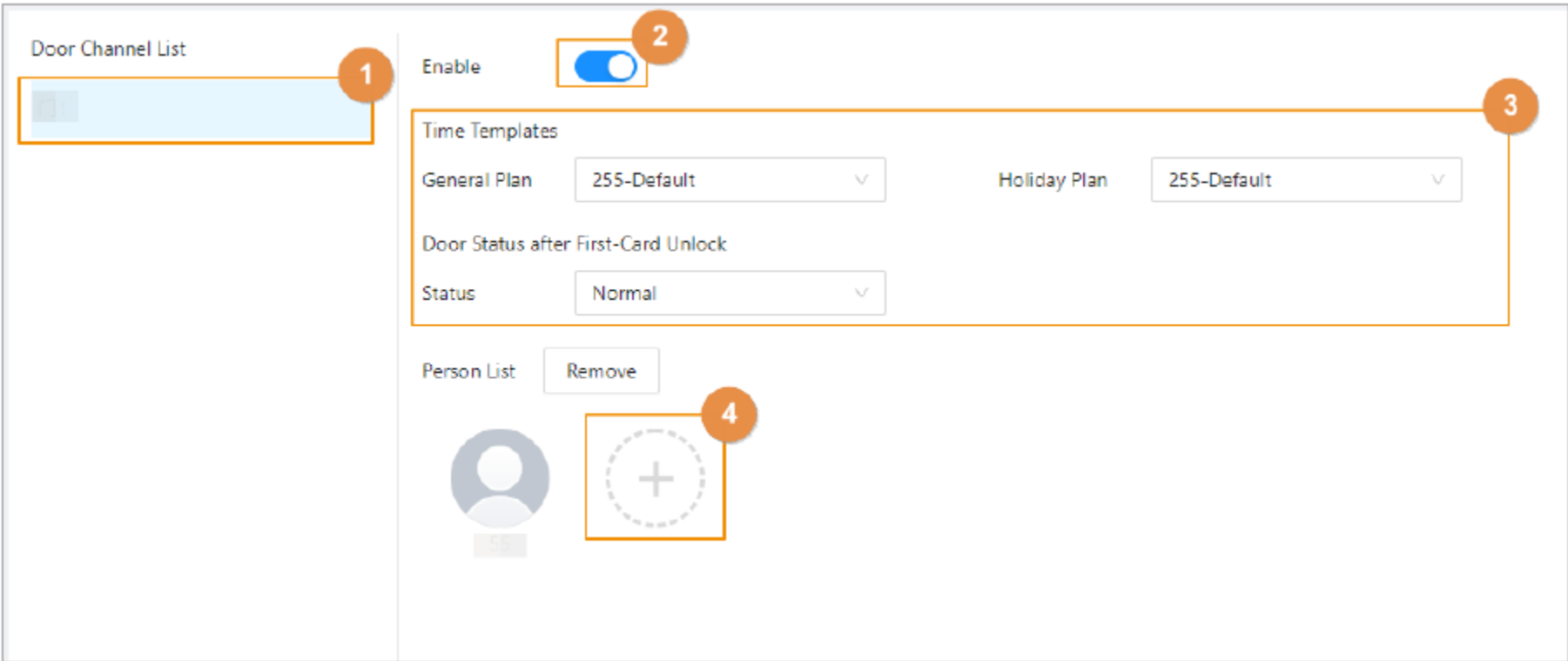
После того, как первое лицо подтвердит личность, если устройство перезагрузится, первому лицу необходимо подтвердить личность еще раз.

После включения функции пользователи патруля могут, как правило, входить и выходить.

Процедура

- Шаг 1 Выберите **Контроль доступа> Разблокировка от первого лица**.
- Шаг 2 Выберите дверной канал, а затем включите функцию.

Рисунок 4-24 Разблокировка от первого лица



Шаг 3 Настройте параметры.

Таблица 4-11 Описание параметров

Параметр	Описание
Временные шаблоны	Выберите, когда это правило вступит в силу.
Состояние двери после разблокировки первой картой	Обычный: Другие лица должны подтвердить свои у Всегда открыто: все люди могут проходить без подт удостоверений личности.
Список лиц	Нажмите +, чтобы выбрать одного или нескольких ч разрешения на доступ к дверям.

Шаг 4 Нажмите Применить.

4.7.8 Настройка защиты от обратного доступа.

Пользователям необходимо подтвердить свою личность как для входа, так и для выхода; в противном случае будет срабатывать сигнализация против обратного прохода . Это не позволяет владельцу карты передать карту доступа обратно другому лицу, чтобы оно получило доступ вход. Когда включена защита от обратного доступа, владелец карты должен покинуть защищенную зону, прежде чем система это сделает разрешите другой вход.

Если человек входит после авторизации и выходит без авторизации, будет подан сигнал тревоги при повторной попытке входа сработает сигнализация, и в то же время доступ будет запрещен.
Если человек не прошел авторизацию и выходит после авторизации, срабатывает сигнализация когда он попытается войти снова, в то же время доступ будет запрещен.

Процедура

Шаг 1 Выберите Контроль доступа> Защита от обратного доступа.

Шаг 2 Включите эту функцию, а затем настройте время сброса.

Укажите время, когда состояние защиты от обратного доступа всего персонала будет сброшено.

Шаг 3 Выберите общий план и план отдыха.

Защита от обратного доступа действует в течение определенного времени.

Шаг 4 В группе входа нажмите Добавить, а затем выберите устройство чтения карт.

Шаг 5 В группе выхода нажмите Добавить, а затем выберите устройство чтения карт.

Рисунок 4-25 Защита от обратного доступа

Enable ☒

Reset Time min (5-300)

Time Templates

General Plan

255-Default

Holiday Plan

255-Default

Anti-passback Group Config ?

Entry Group

+ Add

Clear

/Reader 1

Remove

Exit Group

+ Add

Clear

/Reader 2

Remove

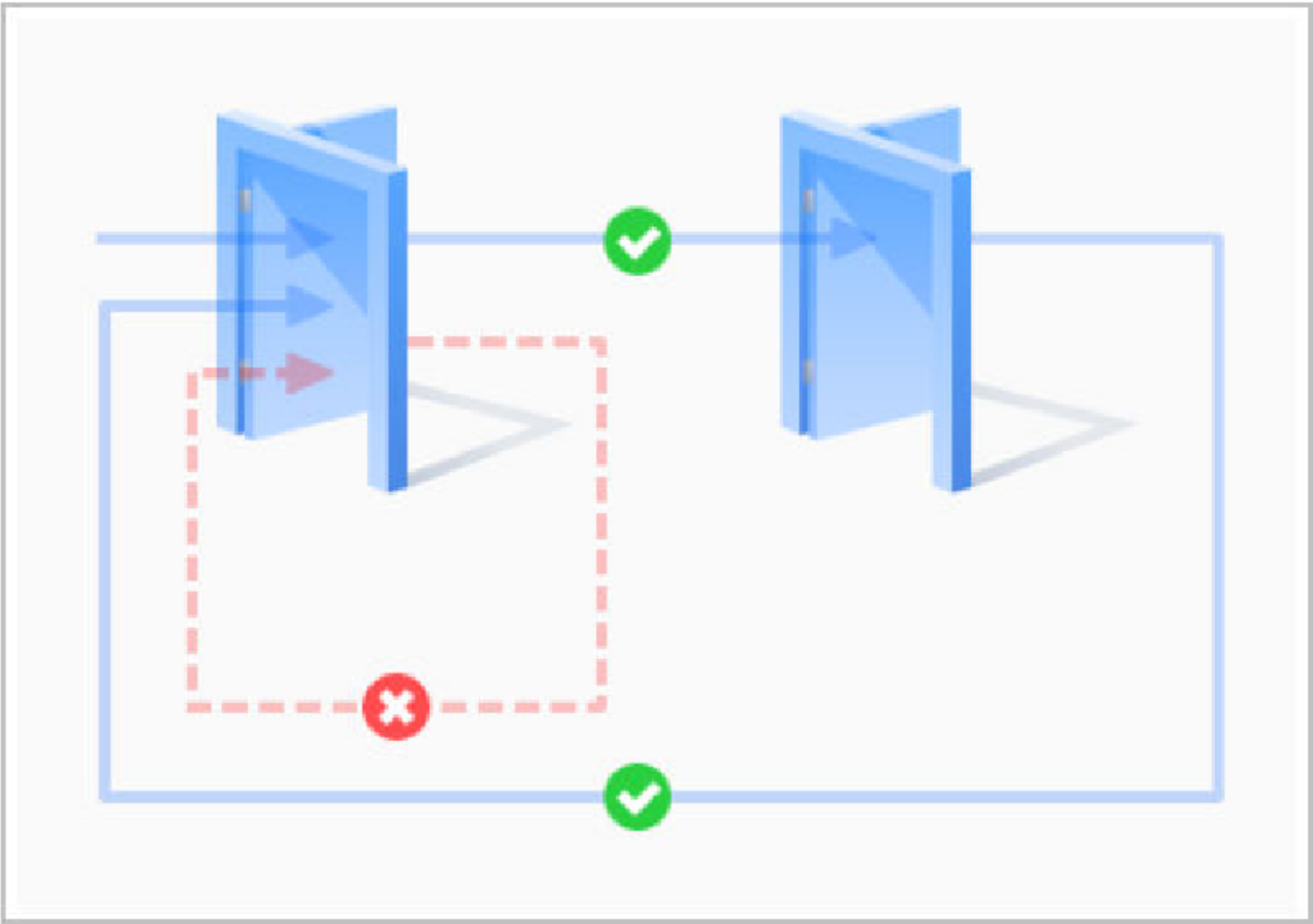
Шаг 6 Нажмите Применить.

Результаты

Номер группы указывает последовательность перемещения карточек. Карта должна использоваться в соответствии с определенной последовательностью групп. Например, вы должны провести карточкой по считывателю в группе входа, а затем по считывателю в группе выхода. Пока вы проводите карточкой в установленной последовательности, система работает нормально.

101

Рисунок 4-26 Функция защиты от обратного доступа



4.8 Настройка посещаемости

Эта функция доступна только на избранных моделях.

4.8.1 Настройка отделов

Процедура

Шаг 1 Выберите Конфигурация посещаемости > Настройки отдела.

Шаг 2 Нажмите , чтобы переименовать отдел.

По умолчанию существует 20 отделов. Мы рекомендуем вам переименовать их.

Рисунок 4-27 Создание отделов

Default			
ID	Department Name		Operation
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Связанные операции

Вы можете нажать "По умолчанию", чтобы восстановить для отделов настройки по умолчанию.

4.8.2 Настройка смен

Настройте смены, чтобы определить правила посещаемости по расписанию. Сотрудники должны работать в назначенное для время. они начинают свою смену и уходят в конце, за исключением случаев, когда они решают работать сверхурочно.

Процедура

Шаг 1 Выберите "Настройка посещаемости" > "Настройка смены".

Шаг 2 Щелкните , чтобы настроить смену.

Рисунок 4-28 Настройка сдвига

Edit Shift

*

 Shift No.

1

*

 Shift Name

Default

*

 Period 1

08:00 → 17:00 

*

 Period 2

00:00 → 00:00 

*

 Period 3

00:00 → 00:00 

*

 Overtime Period

00:00 → 00:00 

*

 Limit for Arriving Late

5

min (0-99)

*

 Limit for Leaving Early

5

min (0-99)

OK

Cancel

Таблица 4-12 Описание параметров сдвига

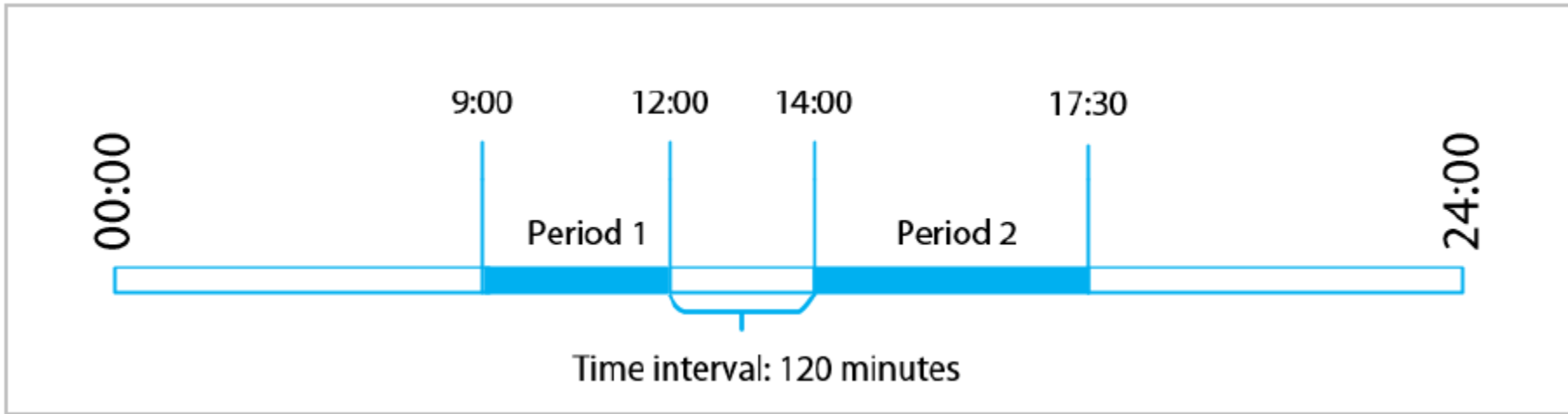
Parameter	Description
Shift Name	Enter the name of the shift.

Параметр	Описание
Период 1 Период 2	Укажите временной диапазон, в течение которого сотрудники могут рабочего дня. Необходимо настроить как минимум 1 период.
Период 3	Если вы установили только один период посещаемости, сотрудники приходят и уходят по назначенному времени, чтобы избежать по аномалий в их отчетах о посещаемости. Например, если вы установите с 08:00 на 17:00, сотрудники должны к 08:00 и заканчивать работу с 17:00 и далее. Если вы установите 2 периода посещаемости, эти два периода не м перекрываться. Сотрудники должны приходиться и уходить по распис периодов. Если вы установите 3 периода, эти 3 периода не могут перекрывать необходимо засекать время прихода и ухода за 2 смежными период
	Последний период может пересекать дни. Если период сверхурочн , вы можете настроить его на пересечение дней.
Период сверхурочной работы	Сотрудники, которые приходят или уходят в течение определенного считаются работающими сверх своего обычного рабочего времени.
Ограничение на опоздание (мин.)	Сотрудникам может быть предоставлено определенное количество они могли приходиться немного позже и уходить немного раньше. На
Ограничение на досрочный уход (мин.)	если обычное время приема - 08:00, допустимый период может быть установлен равным 5 минутам, чтобы сотрудники, прибывающ считались опоздавшими.

Если вы настраиваете более одного периода, обратитесь к следующим инструкциям для выполнения функция посещаемости.

Если временной интервал между двумя периодами равен четному числу, вы можете разделить время интервал на 2 и назначить первую половину интервала первому периоду, который будет время отсчета времени. Вторая половина интервала должна быть отнесена ко второму периоду в качестве отсчета времени.

Рисунок 4-29 Временной интервал (четное число)



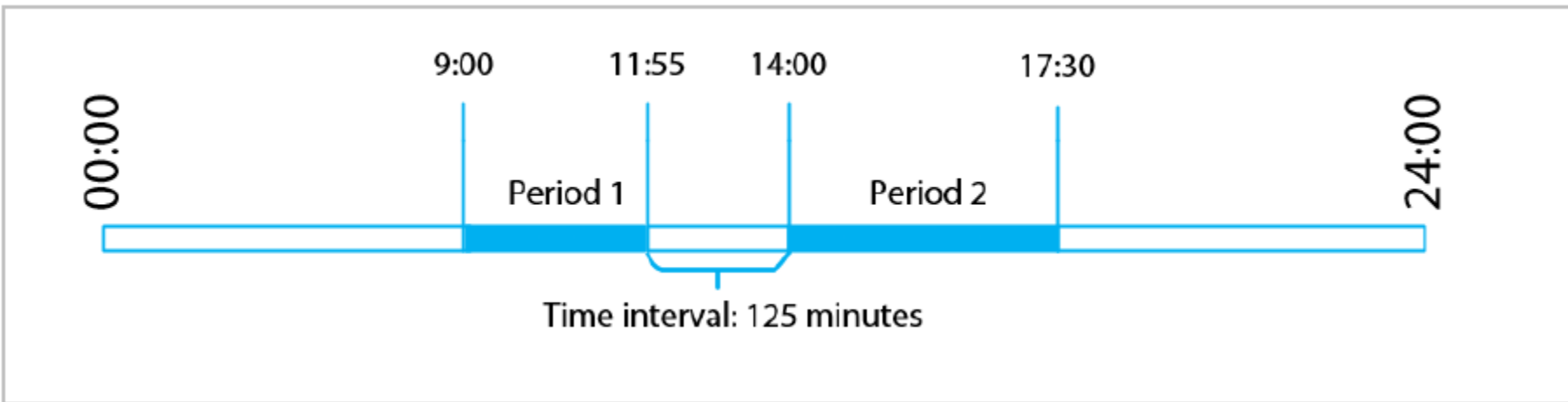
Например: если интервал равен 120 минутам, то время ожидания для периода 1 равно от с 12:00 до 12:59, а рабочее время для периода 2 - с 13:00 до 14:00.



Если пользователь отсчитывает время несколько раз в течение периода 1, действительным будет самое позднее время, и если он отсчитывает время несколько раз в течение периода 2, действительным будет самое раннее время.

Когда временной интервал между двумя периодами равен нечетному числу, наименьшей части интервал будет присвоен первому периоду, который будет временем отсчета времени. наибольшая часть интервала будет назначена второму периоду в качестве часов в время.

Рисунок 4-30 Интервал времени (нечетное число)



Например: если интервал равен 125 минутам, то время отсчета для периода 1 равно от с 11:55 до 12:57, а время начала периода 2 - с 12:58 до 14:00. Период 1 длится 62 минуты, а период 2 - 63 минуты.



Если пользователь отсчитывает время несколько раз в течение периода 1, действительным будет самое позднее время, и если он отсчитывает время несколько раз в течение периода 2, действительным будет самое раннее время.

Если есть только один период, и вы не приходите и не заканчиваете его к указанному времени, он считается отсутствующим в течение 1 дня.

Если имеется более одного периода, и вы не приходите и не выходите к назначенному времени время одного периода считается отсутствующим в течение 0,5 дня. Если вы не приходите или не уходите к назначенному времени в течение 2 или более чем 2 периодов, это считается отсутствием в течение 1 дня. Присутствие в периоды сверхурочной работы не изменяет статус отсутствия сотрудника.

Если вы настроите для последнего периода пересечение дней, обратитесь к следующим инструкциям, чтобы выполнить функцию присутствия.

Если второй день - обычная смена, посещаемость такая же, как обычно.

Если второй день - выходной, вы можете выйти в любое время из 24 часов в праздничный день.



Время всех посещений указано с точностью до секунды. Например, если обычный хронометраж время установлено на 8:05 утра, сотрудник, пришедший на работу в 8:05:59 утра, не будет считаться опоздавший. Но сотрудник, который прибудет в 8:06 утра, будет отмечен как опоздавший на 1 минуту.

Шаг 3. Нажмите "ОК".

Связанные операции

Вы можете нажать "По умолчанию", чтобы восстановить заводские настройки по умолчанию.

4.8.3 Настройка выходных дней.

Настройте планы отпусков, чтобы установить периоды, в течение которых посещаемость не отслеживалась. Процедура

- Шаг 1 Выберите посещаемость *Config > ShiftConfig > Holiday*
- Шаг 2 Нажмите Добавить, чтобы добавить планы отпусков.

Шаг 3 Настройте параметры.

Рисунок 4-31 Создание планов отпусков

Add Attendance Holiday

Attendance Holiday ...

1

Attendance Holiday

Attendance Holiday for October

Time

2023-10-01 → 2023-10-07

OK

Cancel

Описание параметров таблицы 4-13

Parameter	Description
Attendance Holiday No.	The number of the holiday.
Attendance Holiday	The name of the holiday.
Start Time	The start and end time of the holiday.
End Time	

Шаг 4 Нажмите кнопку OK.

4.8.4 Настройка графиков работы.

График работы обычно относится к дням в месяце и часам в день, которые сотрудник ожидается, что он будет находиться на своем рабочем месте. Вы можете создавать различные типы графиков работы на основе различных отдельные лица или отделы, а затем и сотрудники должны следовать установленному графику работы.

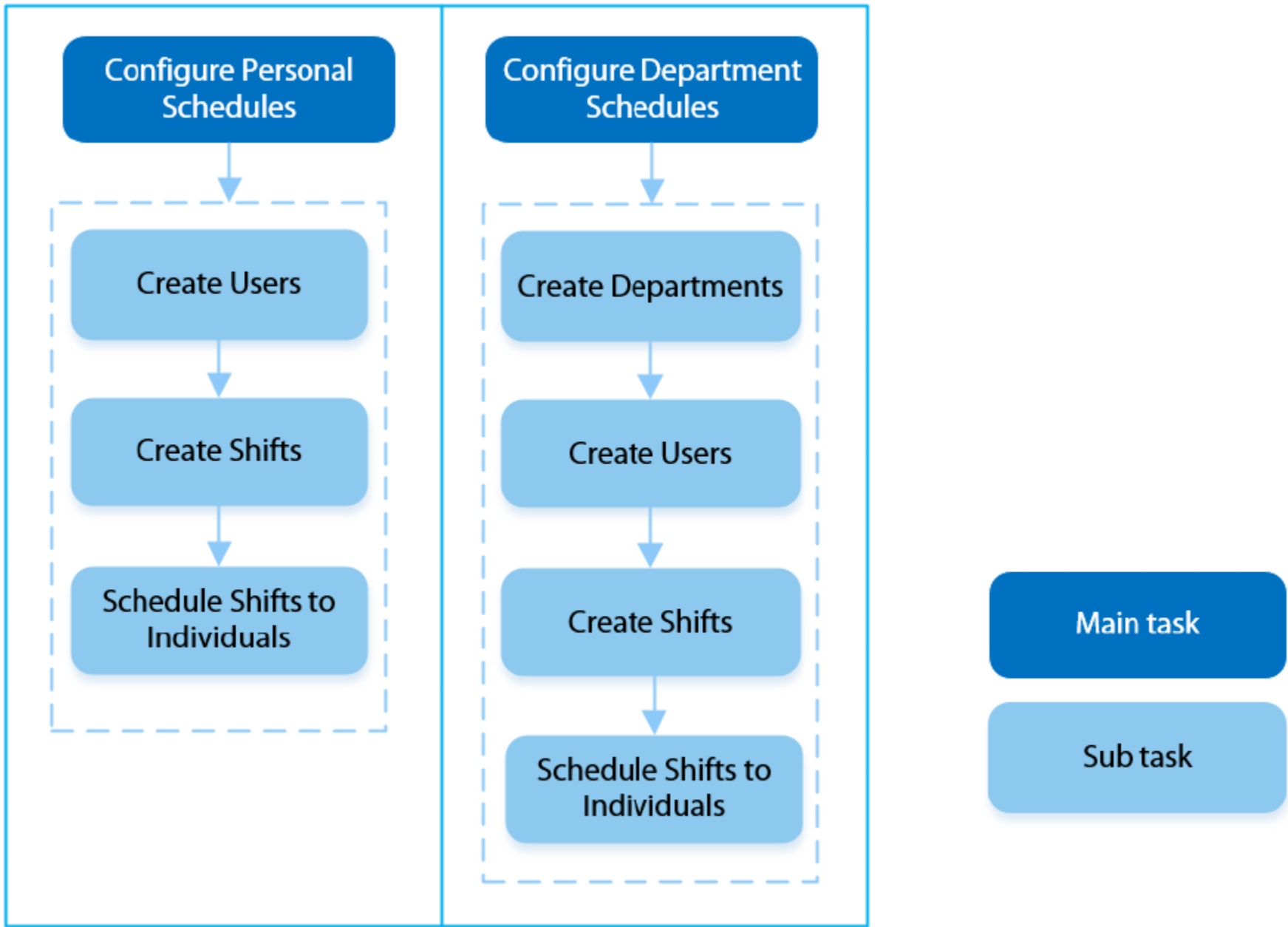
Справочная информация

Обратитесь к блок-схеме, чтобы настроить личные графики или графики отдела.



При настройке расписания не должно быть перекрывающихся периодов времени в один и тот же день и предыдущий или следующий день.

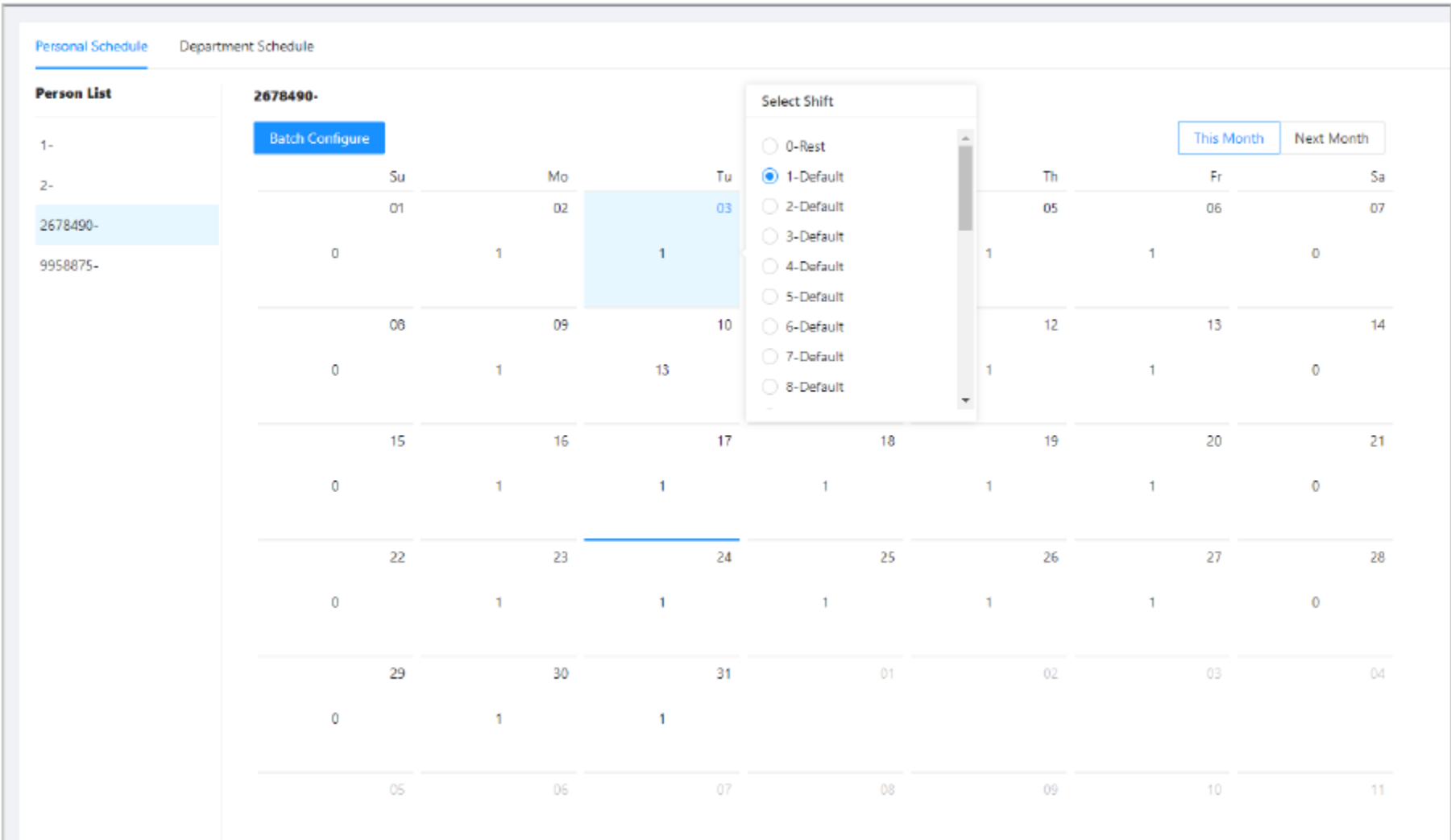
Рисунок 4-32 Настройка графиков работы



Процедура

- Шаг 1** Выберите "Настройка посещаемости" > "Настройка расписания".
- Шаг 2** Настройте графики работы для отдельных сотрудников.
- 1. Нажмите "Личное расписание".**
 - 2. Выберите сотрудника в списке сотрудников.
 - 3. В календаре выберите день, а затем смену.
- Вы также можете нажать кнопку Пакетная настройка, чтобы запланировать смены на несколько дней.

Рисунок 4-33 Личное расписание



Вы можете установить графики работы только на текущий и следующий месяц.

0 означает перерыв.

От 1 до 24 указывается количество заранее определенных смен. Чтобы узнать, как настроить смены, смотрите раздел "4.8.2 Настройка смен".

25 указывает на командировку.

26 указывает на отпуск.

Шаг 3

Установите графики работы для отделов.

1. Щелкните Расписание отдела.

2. Выберите отдел в списке отделов.

3. В календаре выберите день, а затем смену.

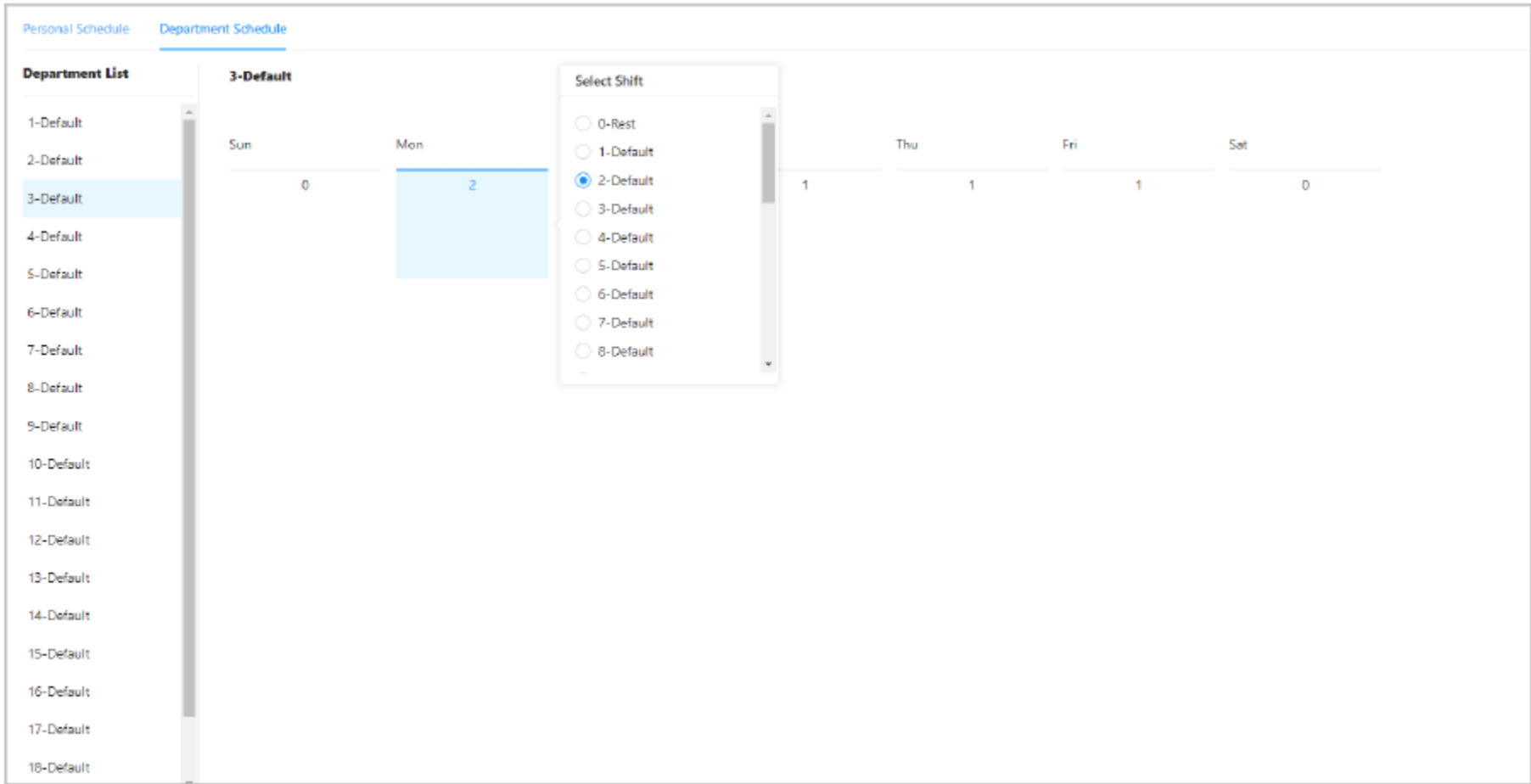
0 означает отдых.

от 1 до 24 указывается количество заранее определенных смен. Информацию о настройке смен см. "4.8.2 Настройка смен".

25 указывает на командировку.

26 указывает на отпуск.

Рисунок 4-34 Расписание смен для отдела



Определенный график работы рассчитан на неделю и будет применяться ко всем сотрудникам в отдел.

4.8.5 Экспорт записи о посещаемости.

Вы можете экспортировать запись разблокировки и записи посещаемости.

Процедура

- Шаг 1
- Выберите "Конфигурация посещаемости" > "Отчет о посещаемости".
- Шаг 2
- Выберите тип, выберите дату, а затем нажмите "Экспортировать".
- Для
- устройство контроля доступа, тип которого можно выбрать из записей разблокировки за 1 месяц **Посещаемость и ненормальная посещаемость.**
- Для
- устройства контроля посещаемости тип можно выбрать из записей посещаемости, **1**
Посещаемость за месяц и ненормальная посещаемость.

Если вы выберете посещаемость за 1 месяц, личный отчет о посещаемости, подробная посещаемость отчет и сводка посещаемости экспортируются одновременно.



Экспортируемые файлы представлены в формате XML.

Рисунок 4-35 Экспорт записи

Type

Unlock Records

Date

2025-06-10 → 2025-06-11

Export

4.8.6 Настройка режимов посещаемости

Процедура

- Шаг 1
- Выберите "Конфигурация посещаемости" > "Конфигурация посещаемости".
- Шаг 2
- Включите локальную посещаемость, а затем установите режим посещаемости.
- Шаг 3
- Настройте режимы посещаемости.

Рисунок 4-36 Режимы посещаемости

Local Attendance

Mode Settings

Auto/Manual Mode

Auto Mode

Manual Mode

Fixed Mode

Check In

06:00 AM

→

09:59 AM

Break Out

10:00 AM

→

12:59 PM

Break In

01:00 PM

→

03:59 PM

Check Out

04:00 PM

→

08:59 PM

Overtime Check In

12:00 AM

→

12:00 AM

Overtime Check Out

12:00 AM

→

12:00 AM

Apply

Refresh

Default

Таблица 4-14 Режим посещаемости

Параметр	Описание
Автоматический / ручной режим	Статус посещаемости отображается на экране автоматически после того, включаете или выключаете часы, но вы также можете вручную изменить с. Регистрация заезда: Приходите, когда начинается ваш обычный рабочий Перерыв: уходите, когда начинается ваш перерыв. Перерыв: приходите, когда заканчивается ваш перерыв. Расчетный час: заканчивается, когда заканчивается ваш обычный рабочий Зачет за сверхурочную работу: начинается период сверхурочной работы. Выписка сверхурочных: отсчет времени по окончании периода сверхуроч

Параметр	Описание
Автоматический режим	На экране автоматически отображается статус вашей посещаемости после того, как вы зарегистрируетесь. Регистрация: регистрируйтесь, когда начинается ваш обычный рабочий день. Перерыв: отбой, когда начнется перерыв. Перерыв: отбой, когда закончится перерыв. Выезд: отбой, когда закончится ваш обычный рабочий день. Регистрация на сверхурочную работу: засчитывается, когда начинается период сверхурочной работы. Регистрация на сверхурочную работу: засчитывается, когда заканчивается период сверхурочной работы.
Ручной режим	Вручную выберите статус своей посещаемости при входе или выходе по часам.
Фиксированный режим	При включении или выключении часов на экране постоянно будет отображаться заданный статус посещаемости.

Шаг 4 Нажмите Применить.

Связанные операции

Обновить: Если вы не хотите сохранять текущие изменения, нажмите Обновить, чтобы отменить изменения и восстановите предыдущие настройки.

По умолчанию: восстановите настройки посещаемости до заводских значений по умолчанию.

4.9 Аудио

4.9.1 Настройка параметров звука

Настройте распознавание голоса и голосовые объявления для успешной или неудачной проверки на локальный главный интерфейс.

Процедура

- Шаг 1 Выберите **Audio > Audio Config**
- Шаг 2 Настройте параметры звука, а затем нажмите Применить.

Рисунок 4-37 Аудио

Speaker Volume

80

(0-100) ⓘ

Key Sound

Voice Broadcast Settings

Successfully verified.

▼

Period1

00:00

⌚

23:59

⌚

☐ Enable

Audio File

▼

Period2

00:00

⌚

23:59

⌚

☐ Enable

Audio File

▼

Period3

00:00

⌚

23:59

⌚

☐ Enable

Audio File

▼

Period4

00:00

⌚

23:59

⌚

☐ Enable

Audio File

▼

Рисунок 4-38 DND

DND Mode

Time

Period 1

00:00

→

23:59

⌚

Period 2

00:00

→

00:00

⌚

Period 3

00:00

→

00:00

⌚

Period 4

00:00

→

00:00

⌚

Apply

Refresh

Default

Таблица 4-15 Описание звуковых параметров

Parameters	Description
Speaker Volume	Adjust the speaker volume.
	Only available on select models.

112

Параметры	Описание
Ключевой звук	Когда эта функция включена, устройства с сенсорным экраном будут издавать звуки для локальных сенсорных операций, в то время как устройства без сенсорного экрана будут издавать звуки подсказки для операций с клавишами.
Настройки голосовой трансляции	Установите голосовые подсказки для успешной и неудачной проверки. Поддерживаются 6 периодов времени. Доступны только на некоторых моделях. Щелкните соответствующий период времени, чтобы включить его. Настройка будет применена к следующему периоду времени. Выберите аудиофайл. Поддерживается выбор аудиофайлов, загруженных на устройство. Аудио > Аудиофайл. Подробнее см. "4.9.2 Управление аудиофайлами".
Режим DND	При включении не будет никаких звуковых подсказок для локальной проверки (таких как доступ к двери или посещаемость) в течение настроенных временных периодов. Поддерживает до 4 периодов времени.

4.9.2 Управление аудиофайлами

Справочная информация

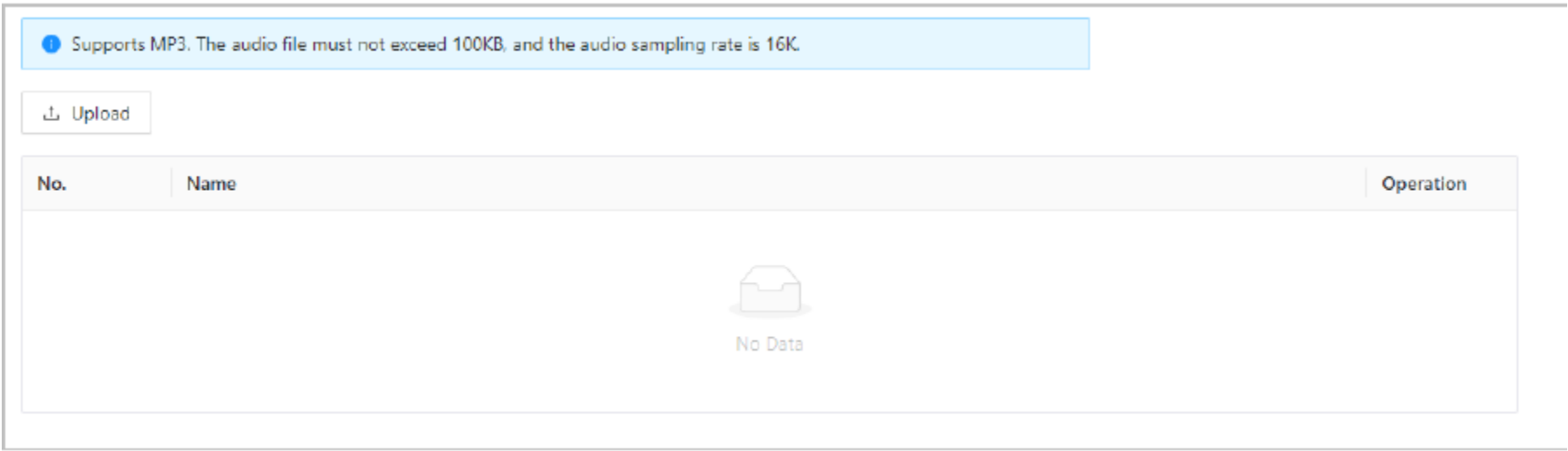
Загрузка аудиофайлов и управление ими.

Поддерживается только на некоторых моделях.

Процедура

- Шаг 1 Выберите Аудио > Аудиофайл.
- Шаг 2 Нажмите "Загрузить", выберите аудиофайлы, а затем нажмите "Открыть".
- Шаг 3 (необязательно) Нажмите , чтобы прослушать аудиофайл.

Рисунок 4-39 Управление аудиофайлом



4.10 Настройки связи

4.10.1 Сетевые настройки

4.10.1.1 Настройка TCP / IP

Вам необходимо настроить IP-адрес устройства, чтобы убедиться, что оно может взаимодействовать с другими устройствами.

Процедура

- Шаг 1
- Шаг 2
- Выберите Настройки связи> Настройки сети> TCP/IP.
- Настройте параметры.

Рисунок 4-40 TCP/IP

NIC

NIC 1

Mode

☐ DHCP

☒ Static

MAC Address

IP Version

IPv4

IP Address

172.16.5.21

Subnet Mask

255.255.0.0

Default Gateway

172.16.24.1

Preferred DNS

8.8.8.8

Alternate DNS

8.8.4.4

MTU

1500

Apply

Refresh

Default

Таблица 4-16 Описание TCP/IP

Параметр	Описание
Режим	Статический: вручную введите IP-адрес, маску подсети и шлюз. DHCP: Расшифровывается как Dynamic Host Configuration Protocol. Когда DHCP включен, устройству будет автоматически назначен IP-адрес, маска подсети и шлюз.

Параметр	Описание
MAC-адрес	MAC-адрес устройства.
Версия IP	IPv4 или IPv6.
IP-адрес Маску подсети	Если вы установили статический режим, настройте IP-адрес, подсеть маску и шлюз.
Шлюз по умолчанию	IPv6-адрес представлен в шестнадцатеричном формате. Версия IPv6 не требует установки масок подсети. IP-адрес и шлюз по умолчанию должны находиться в одном и том же сегменте сети.
Предпочитаемый DNS	Установите IP-адрес предпочтительного DNS-сервера.
Альтернативный DNS	Установите IP-адрес альтернативного DNS-сервера.
MTU	MTU (Максимальная единица передачи) относится к максимальному размеру данных, которые могут быть переданы в одном сетевом пакете в компьютерных сетях. По умолчанию он равен 1500.

Шаг 3 Нажмите OK.

4.10.1.2 Настройка Wi-Fi



Wi-Fi и точка доступа Wi-Fi не могут быть включены одновременно.
Функция Wi-Fi доступна только на некоторых моделях.

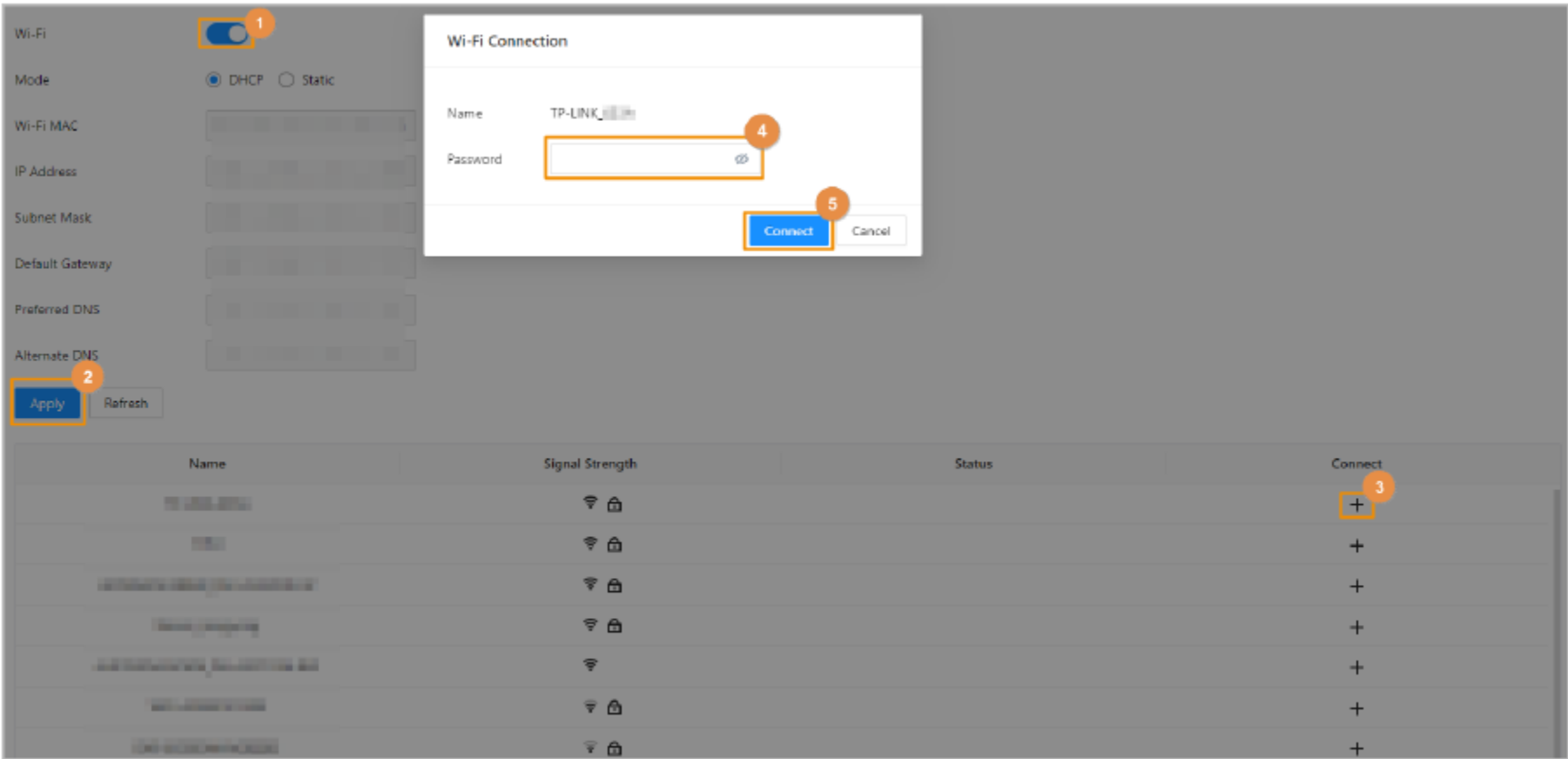
Процедура

- Шаг 1 **Выберите Настройки связи> Настройки сети> Wi-Fi.**
- Шаг 2 Включите Wi-Fi, а затем нажмите Применить.

Отобразятся все доступные Wi-Fi.
- Шаг 3 Нажмите +, а затем введите пароль Wi-Fi.

Wi-Fi подключен.

Рисунок 4-41 Wi-Fi



Связанные операции

- DHCP: Включите эту функцию и нажмите Применить, устройству автоматически будет назначен Wi-Fi адрес.
- Статический: Включите эту функцию, вручную введите адрес Wi-Fi, а затем нажмите Применить, устройство подключится к Wi-Fi.

4.10.1.3 Настройка точки доступа Wi-Fi



- The Функция Wi-Fi доступна на некоторых моделях.
- The Wi-Fi и точка доступа Wi-Fi не могут быть включены одновременно.

Процедура

- Шаг 1 Выберите Настройки связи> Настройки сети> Точка доступа Wi-Fi.
- Шаг 2 Включите эту функцию, а затем нажмите кнопку Применить.

Рисунок 4-42 Точка ДОСТУПА Wi-Fi

Enable

SSID

Security

WPA2 Personal

Password

12345678

IP Address

Apply

Refresh

Default

Результаты

После включения вы можете подключиться к устройству Wi-Fi через свой телефон и войти на веб-страницу устройства на вашем телефоне.

4.10.1.4 Настройка порта

Вы можете ограничить доступ к устройству одновременно через веб-страницу, настольный клиент и мобильный клиент.

Процедура

- Шаг 1 Выберите Настройки связи> Сетевые настройки> Порт.
- Шаг 2 Настройте порты.



За исключением максимального подключения и порта RTSP, вам необходимо перезапустить устройство, чтобы настройки вступили в силу после изменения других параметров.

Рисунок 4-43 Настройка портов

Max Connection

50

(1-50)

TCP Port

37777

(1025-65535)

HTTP Port

80

HTTPS Port

443

RTSP Port

554

Apply

Refresh

Default

Таблица 4-17 Описание портов

Параметр	Описание
Максимальное Подключение	Вы можете установить максимальное количество клиентов (таких как веб-страница, настольный клиент и мобильный клиент), которые могут одновременно подключаться к устройству.
TCP-порт	Значение по умолчанию - 37777.
Порт HTTP	Значение по умолчанию - 80. Если вы изменили номер порта, добавьте номер порта после IP-адреса при доступе к веб-странице.
Порт HTTPS	Значение по умолчанию - 443.
Порт RTSP	Значение по умолчанию 554.

Шаг 3 Нажмите кнопку Применить.

4.10.1.5 Настройка базовой службы

Если вы хотите подключить устройство к платформе сторонних производителей, включите CGI и ONVIF функции.

Процедура

Шаг 1 Выберите **Настройки связи> Сетевые настройки> Основные службы**. **Шаг 2** Настройте базовую службу.

Рисунок 4-44 Базовая услуга

SSH

Multicast/Broadcast Search

CGI

ONVIF

Emergency Maintenance

For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.

Private Protocol Authentication Mode

Security Mode (Recommended) ▾

Private Protocol

*Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.

TLSv1.1

LLDP

Apply

Refresh

Default

Таблица 4-18 Описание параметра базовой услуги

Параметр	Описание
SSH	SSH, или Secure Shell Protocol, - это протокол удаленного админист... который позволяет пользователям получать доступ к своим удаленным серверам, управлять ими и изменять их через Интернет
Mutlicast / Широковещательный поиск.	Поиск устройств с помощью многоадресной рассылки или широковещательного поиска
CGI	Общий интерфейс шлюза (CGI) представляет собой пересечение между веб-серверами, через которое возможен стандартизированный обмен данными между внешними приложениями и серверами.
ONVIF	ONVIF расшифровывается как Форум открытого сетевого видеон... - обеспечить стандарт интерфейса между различными устройствами. . Эти стандартизированные спецификации ONVIF подобны общему языку, который могут использовать все устройства для общения.
Экстренное обслуживание	Он включен по умолчанию.
Аутентификация по частному протоколу Режим	Установите режим аутентификации, включая безопасный режим и режим совместимости. Рекомендуется выбрать режим безопасности. Режим безопасности (рекомендуемый): не поддерживает доступ к устройству с помощью методов Digest, DES и plaintext аутентификации, что повышает безопасность устройства. Совместимый режим: Поддерживает доступ к устройству с помощью методов аутентификации Digest, DES и plaintext с пониженной безопасностью.
Частный протокол	Платформа добавляет устройства по частному протоколу.

Параметр	Описание
TLSv1.1	TLSv1.1 относится к версии безопасности транспортного уровня 1.1. TLS - это криптографический протокол, разработанный для обеспечения безопасной и аутентифицированной связи по компьютерной сети. При включении TLSv1.1 могут возникнуть угрозы безопасности. Пожалуйста, имейте в виду.
LLDP	LLDP - это сокращение от Link Layer Discovery Protocol, который представляет собой протокол канального уровня передачи данных. Это позволяет сетевым устройствам, таким как коммутаторы, маршрутизаторы или серверы, обмениваться информацией об их идентификаторах и возможностях друг с другом. Протокол LLDP помогает сетевым администраторам лучше понимать топологию сети и предоставляет стандартизированный способ автоматизации обнаружения и отображения соединений между сетевыми устройствами. Это упрощает настройку сети, устранение неполадок и оптимизацию производительности.

Шаг 3 Нажмите кнопку Применить.

4.10.1.6 Настройка облачной службы.

Облачный сервис предоставляет услугу проникновения NAT. Пользователи могут управлять несколькими устройствами через DMSS. Вам не нужно подавать заявку на динамическое доменное имя, настраивать сопоставление портов или развертывать сервер.

Процедура

Шаг 1 На домашней странице выберите Настройки связи> Настройки сети> Облако Обслуживание.

Шаг 2 Включите функцию облачного сервиса.

Облачный сервис подключается к Сети, если подключены P2P и PaaS.

Рисунок 4-45 Облачный сервис

Enable

After the function is enabled and the device connects to the network, we will collect device information such as the IP address, MAC address, device name and serial number. The collected information will only be used to remotely access the device. If you do not want to enable this function, please clear the selection from the check box.

P2P Status

Offline

PaaS Status

Offline

SN

8C 759

Apply

Refresh

Шаг 3 Нажмите Применить.

Шаг 4 Отсканируйте QR-код с помощью DMSS, чтобы добавить устройство.

4.10.1.7 Настройка автоматической регистрации SDK

Автоматическая регистрация позволяет добавлять устройства на платформу управления без ручного ввода информации об устройстве, такой как IP-адрес и порт.

Справочная информация.



Автоматическая регистрация поддерживает только SDK.

Процедура

Шаг 1 На домашней странице выберите Настройки сети> Автоматическая регистрация SDK.

Шаг 2 Включите функцию автоматической регистрации и настройте параметры.

Рисунок 4-46 Автоматическая регистрация

Enable

Status

Offline

Server Address

172.5.2.27

Port

7000

(1-65535)

Registration ID

none

Apply

Refresh

Default

Описание автоматической регистрации в таблице 4-19

Параметр	Описание
Статус	Отображает состояние подключения при автоматической регистрации.
Адрес сервера	IP-адрес или доменное имя сервера.
Порт	Порт сервера, который используется для автоматической регистрации.
Регистрационный идентификатор.	Регистрационный идентификатор (определяемый пользователем) устройства. Управление путем ввода регистрационного идентификатора на платформе.

Шаг 3 Нажмите Применить.

4.10.1.8 Настройка автоматической регистрации CGI

Подключение к платформе сторонних производителей по протоколу CGI.

Справочная информация



Поддерживается только IPv4.

Процедура

Шаг 1 На домашней странице выберите Настройки связи> Сетевые настройки> CGI Auto Регистрация.

Шаг 2 Включите эту функцию, а затем настройте параметры.



Шаг 3 Click , а затем настройте параметры.

Рисунок 4-47 Автоматическая регистрация CGI

Edit

X

Enable

Device ID

none

Address Type

Host IP

▼

Host IP

10.0.0.10

Port

60005

HTTPS

Username

Password

OK

Cancel

Таблица 4-20 Описание автоматической регистрации.

Параметр	Описание
Идентификатор устройства	Поддерживает до 32 байт, включая китайский язык, цифры, буквы и специальные символы.
Тип адреса	Поддерживает 2 способа регистрации.
IP-адрес хоста	IP-адрес хоста: введите IP-адрес сторонней платформы.
Доменное имя	Доменное имя: Введите доменное имя сторонней платформы.
HTTPS	Получите доступ к сторонней платформе через HTTPS. Протокол HTTPS обеспечивает безопасную связь по компьютерной сети.
Имя пользователя/пароль	Введите имя пользователя и пароль устройства.

Шаг 4 Нажмите OK.

4.10.1.9 Настройка автоматической загрузки

Отправляйте информацию о пользователе и разблокируйте записи на платформу управления.

Процедура

Шаг 1 На домашней странице выберите Настройки связи> Сетевые настройки> Авто Загрузка.

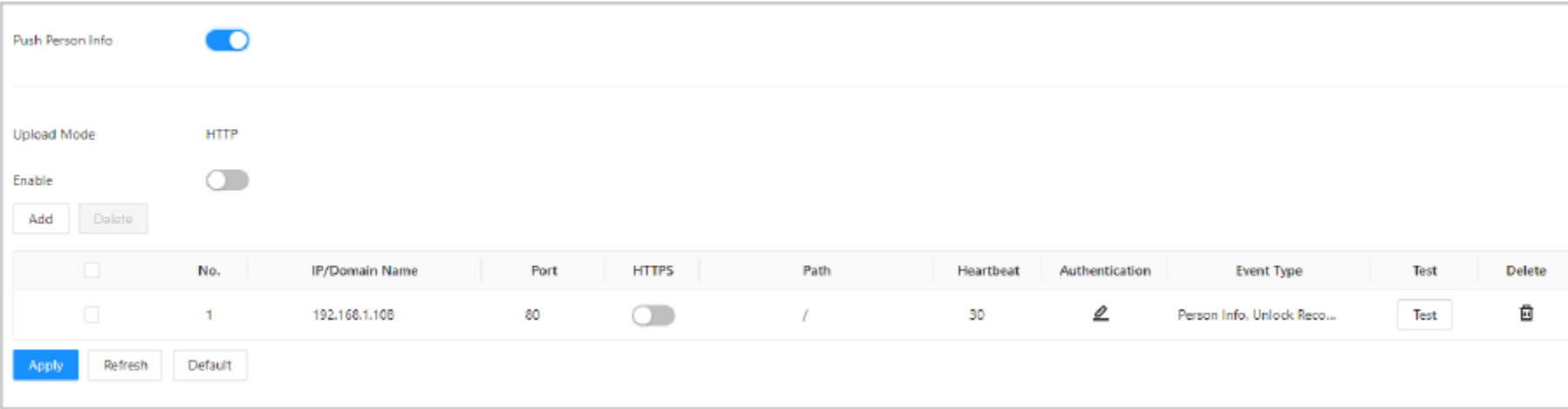
Шаг 2 (Необязательно) Включите отправку информации о пользователе.

Когда информация о пользователе обновляется или добавляются новые пользователи, устройство автоматически отправит информацию о пользователе на платформу управления.

Шаг 3 Включите режим HTTP-загрузки.

Шаг 4 Нажмите "Добавить", а затем настройте параметры.

Рисунок 4-48 Автоматическая загрузка



Описание параметров в таблице 4-21

Параметр	Описание
IP / доменное имя	IP или доменное имя платформы управления.
Порт	Порт платформы управления.
HTTPS	Доступ к платформе управления осуществляется по протоколу HTTPS. Протокол HTTPS обеспечивает связь по компьютерной сети.
Аутентификация	Включите аутентификацию учетной записи при доступе к платформе управления. Для входа требуются имя пользователя и пароль .
Тип события	Выберите тип события, которое будет отправлено на платформу управления. Прежде чем использовать эту функцию, включите отправку информации о персонале. Информацию о персонале можно отправлять только на одну платформу управления, а записи о разблокировке можно отправлять на несколько платформ управления.

Шаг 5 Нажмите Применить.

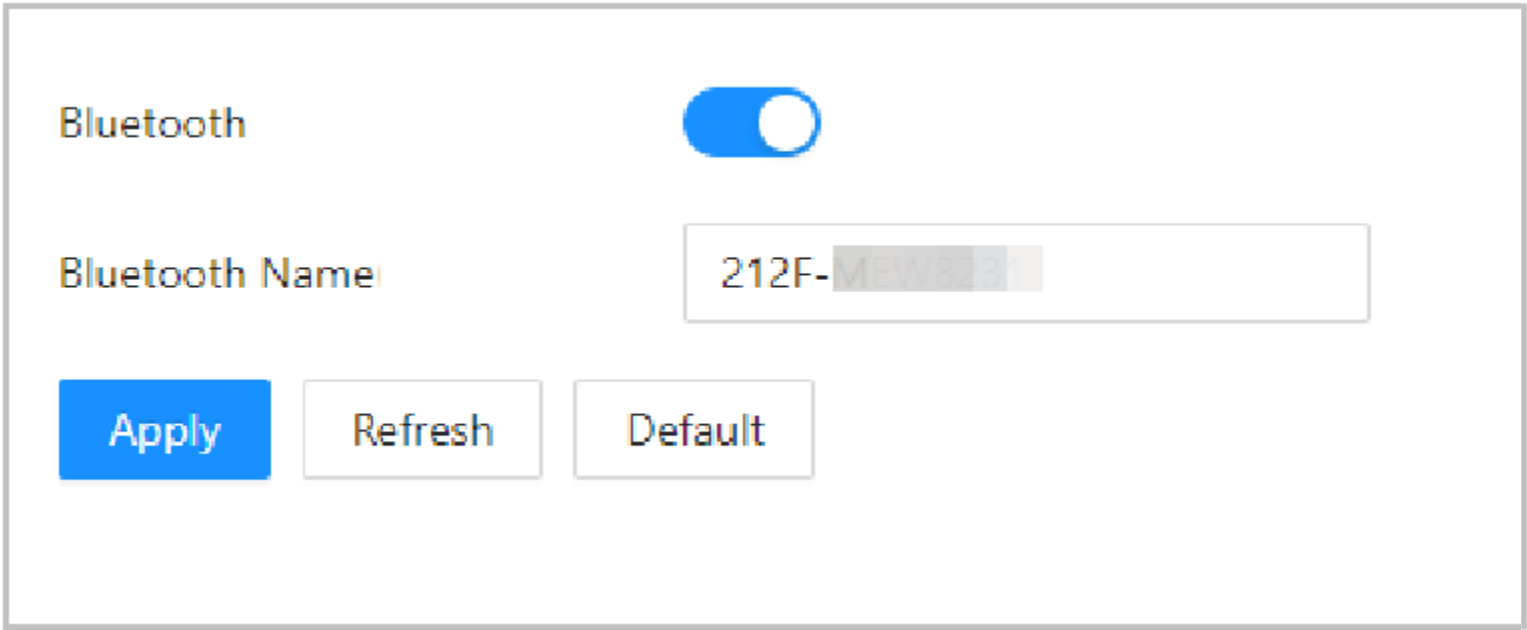
4.10.2 Настройки Bluetooth

Настройте функцию Bluetooth устройства. Эта функция доступна только на некоторых моделях.

Процедура

- Шаг 1
- Выберите Настройки связи> Настройка Bluetooth.
- Шаг 2
- Включите или выключите Bluetooth, настройте название Bluetooth.

Рисунок 4-49 Bluetooth



Шаг 3 Нажмите Применить.

Результаты

Вы можете разблокировать дверь по Bluetooth через приложение DMSS. Для получения подробной информации см. "3.6.3 Bluetooth".

4.10.3 Настройки режима.

Войдите на веб-страницу и выберите Настройки связи > Настройки режима.

Режим чтения карт памяти

Выберите режим в качестве устройства чтения карт памяти. Устройство выполняет функцию устройства чтения карт, подключенного извне к устройству доступа контроллер управления. Он не выполняет аутентификацию, но напрямую передает информацию о контроле доступа информацию (такую как карта, пароль, отпечаток пальца) контроллеру контроля доступа, который затем проверяет подлинность и разблокирует дверь.

Рисунок 4-50 Режим считывания карт памяти

Mode

☒ Card Reader

☐ Access Controller

RS-485 Settings

Baud Rate

9600

▼

Data Bit

8

▼

Stop Bit

1

▼

Parity Code

None

▼

Wiegand Settings

Wiegand Output Type

Wiegand 34

▼

Pulse Width (μs)

200

(20-200)

Pulse Interval (μs)

1000

(200-5000)

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Apply

Refresh

Default

Режим контроллера доступа

Установите режим в качестве контроллера доступа.

Рисунок 4-51 Режим контроллера доступа

Mode

☐ Card Reader ☒ Access Controller

RS-485 Settings

External Device

Card Reader

?

Baud Rate

9600

Data Bit

8

Stop Bit

1

Parity Code

None

Wiegand Settings

Wiegand Settings

☒ Wiegand Input ☐ Wiegand Output

Card No. Inversion

☒

Apply

Refresh

Default

Таблица 4-22 Описание RS-485

Внешнее устройство	Описание
Контроллер доступа	Выберите контроллер доступа, когда устройство функционирует как устройство считывания карт и отправляет данные на другие внешние контроллеры управления доступом. Тип выходных данных: Номер карты: выводит данные на основе номера карты, когда пользователь проводит пальцем по карте, чтобы разблокировать дверь; выводит данные номера карты пользователя, когда он использует другие методы разблокировки. ID: выводит данные на основе идентификатора пользователя. При успешной аутентификации соответствующая информация передается контроллеру доступа. В этом случае отображаемый результат аутентификации является результатом аутентификации контроллера доступа. Когда аутентификация завершается неудачно, соответствующая информация передается контроллеру доступа, и результат аутентификации отображается как сбой.
Устройство чтения карт	Устройство подключается к устройству считывания карт извне и передает информацию о карте контроля доступа контроллеру доступа или платформе управления.
Устройство считывания карт (OSDP)	Устройство подключается извне к считывателю карт OSDP и передает информацию о карте контроля доступа контроллеру доступа или платформе управления.
Дверной модуль безопасности.	Кнопка выхода из двери, замок и противопожарная система не действуют, если включен модуль безопасности. Поддерживает аутентификацию по лицу, карте, отпечатку пальца, паролю и другим методам для управления модулем разблокировки дверей. Поддерживает разблокировку с помощью подключенного извне кард-ридера или кнопки открытия, подключенной к модулю безопасности системы управления. Дистанционное разблокирование дверного замка, подключенного извне к модулю безопасности двери не поддерживается.
Модуль расширения замка.	Когда контроллер доступа подключен к модулю расширения external lock, если вы выберете Модуль расширения Lock, локальная блокировка будет разблокирована после подтверждения идентификации на локальном устройстве. Дополнительная блокировка будет разблокирована после подтверждения идентификации во внешнем считывателе карт. После выбора модуля расширения блокировки вы можете выбрать канал на странице Параметров контроля доступа и сигнализации на веб-странице контроллера доступа.

Таблица 4-23 Описание Wiegand

Параметр		Описание
Настройки Wiegand		- При подключении внешнего устройства чтения карт выберите Wiegand Входной сигнал. - Когда устройство функционирует как устройство чтения карт памяти, и вам нужно подключить его к другому контроллеру доступа и выбрать Wiegand Output Config.
Вход Wiegand	Номер карты инверсия	Если последовательность номеров карт, полученная с помощью ввода, не совпадает с фактической последовательностью номеров карт при использовании устройствами сторонних производителей, включите эту функцию.
Вывод Wiegand	Тип вывода Wiegand	Длина в битах номеров карт или ID, которые устройство может распознать и вывести. Wiegand 26: считывает 3 байта или 6 цифр. Wiegand 34: считывает 4 байта или 8 цифр. Wiegand 66: считывает 8 байт или 16 цифр.
	Ширина импульса — интервал импульсов	Настройте ширину импульса и интервал для вывода wiegand.
	Тип выходных данных	Выберите формат Wiegand для считывания номеров карт или удостоверений. Идентификатор пользователя: выводит данные на основе идентификационного номера. Карта: выводит данные на основе первого номера карты пользователя.
	Формат Wiegand	Если тип выходных данных задан как ID, вы можете выбрать десятичный или шестнадцатеричный форматы вывода.

4.11 Управление системой

4.11.1 Управление пользователями

Вы можете добавлять или удалять пользователей, изменять пароли пользователей и вводить адрес электронной почты для сброса пароль, если вы забудете свой пароль.

4.11.1.1 Добавление администраторов.

Вы можете добавить новые учетные записи администратора, и тогда они смогут входить на веб-страницу устройства.

Процедура

- Шаг 1 На домашней странице выберите Система> Учетная запись.
- Шаг 2 Нажмите Добавить и введите информацию о пользователе.



Имя пользователя не может совпадать с существующей учетной записью. Имя пользователя состоит из до 31 символа и допускает использование только цифр, букв, подчеркиваний, средних линий, точек или @.

Пароль должен состоять из 8-32 непустых символов и содержать не менее двух типов следующих символов: верхний регистр, нижний регистр, цифры и специальные символы (исключая " ; : &).

Установите пароль высокого уровня безопасности, следуя подсказке о надежности пароля.

Рисунок 4-52 "Добавить администраторов"

Add

X

* Username

* Password

* Confirm Password

Remarks

OK

Cancel

Шаг 3 Нажмите "ОК".



Изменить пароль может только учетная запись администратора, а удалить учетную запись администратора нельзя.

4.11.1.2 Добавление пользователей ONVIF

Справочная информация

Форум открытых сетевых видеоинтерфейсов (ONVIF), глобальный и открытый отраслевой форум, который создан для разработки глобального открытого стандарта интерфейса физической безопасности на основе IP продукты, обеспечивающие совместимость от разных производителей. Пользователи ONVIF имеют свои удостоверения личности проверены по протоколу ONVIF. Пользователь ONVIF по умолчанию - администратор.

Процедура

Шаг 1 На домашней странице выберите Система> Учетная запись> Пользователь ONVIF.

Шаг 2 Нажмите кнопку **Добавить**, а затем настройте параметры.

Рисунок 4-53 Добавление пользователя ONVIF

Add

*

Username

*

Password

*

Confirm Password

*

Group

OK

Cancel

Таблица 4-24 Описание пользователя ONVIF

Параметр	Описание
Имя пользователя	Имя пользователя не может совпадать с существующей учетной записью. Имя пользователя состоит до 31 символа и допускает использование только цифр, букв, подчеркивания, средних линий, точек или @.
Пароль	Пароль должен состоять из 8-32 непустых символов и содержать по крайней мере два типа следующих символов: верхний регистр, нижний регистр, цифры и специальные символы (исключая " " ; &).
Группа	Существует три группы разрешений, которые представляют разные уровни разрешения администратор: вы можете просматривать другие учетные записи пользователей и управлять диспетчер устройств. Оператор: Вы не можете просматривать другие учетные записи пользователей или управлять диспетчер устройств. Пользователь: Вы не можете просматривать другие учетные записи пользователей и управлять диспетчере устройств ONVIF.

Шаг 3 Нажмите ОК.

4.11.1.3 Сброс пароля

Сбросьте пароль по связанному электронному письму, если забудете свой пароль.

Процедура

- Шаг 1 Выберите Система> Учетная запись.
- Шаг 2 Введите адрес электронной почты и установите срок действия пароля время.
- Шаг 3 Включите функцию сброса пароля.

Рисунок 4-54 Сброс пароля

Password Reset

Enable

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Email Address

1***@.com

Password Expires in

Never

Days

Если вы забыли пароль, вы можете получить коды безопасности по связанному электронному письму адрес для сброса пароля.

Шаг 4 Нажмите Применить.

4.11.2 Просмотр онлайн-пользователей

Вы можете просмотреть онлайн-пользователей, которые в данный момент входят на веб-страницу. На домашней странице выберите Система > Онлайн-пользователь.

4.11.3 Настройка времени

Процедура

- Шаг 1 На домашней странице выберите Система > Время.
- Шаг 2 Настройте время платформы.

Рисунок 4-55 Настройки даты

Time and Time Zone



Date :

2024-11-04 Monday

Time :

5:44:03 PM

Time

☒ Manually Set

☐ NTP

System Time

2024-11-04 5:44:03 PM



Sync PC

Time Format

YYYY-MM-DD

▼

12-Hour

▼

Time Zone

▼

DST

Enable

☐

Type

☒ Date

☐ Week

Start Time

Jan

▼

1

▼

12:00 AM



End Time

Jan

▼

2

▼

12:00 AM



Apply

Refresh

Default

Таблица 4-25 Описание настроек времени

Параметр	Описание
Время	Ручная настройка: введите время вручную или вы можете нажать кнопку Синхронизировать, чтобы синхронизировать время с компьютером. NTP: устройство автоматически синхронизирует время с NTP сервером. Сервер : Введите домен NTP-сервера. Порт : введите порт NTP-сервера. Интервал : введите его время с интервалом синхронизации.
Формат времени	Выберите формат времени.
Часовой пояс	Введите часовой пояс.

Параметр	Описание
ЛЕТНЕЕ время	1. (Необязательно) Включите летнее время. 2. Выберите дату или неделю из списка типов. 3. Настройте время начала и окончания летнего времени.

Шаг 3 Нажмите Применить.

4.11.4 Настройка "Всегда включено"

Процедура

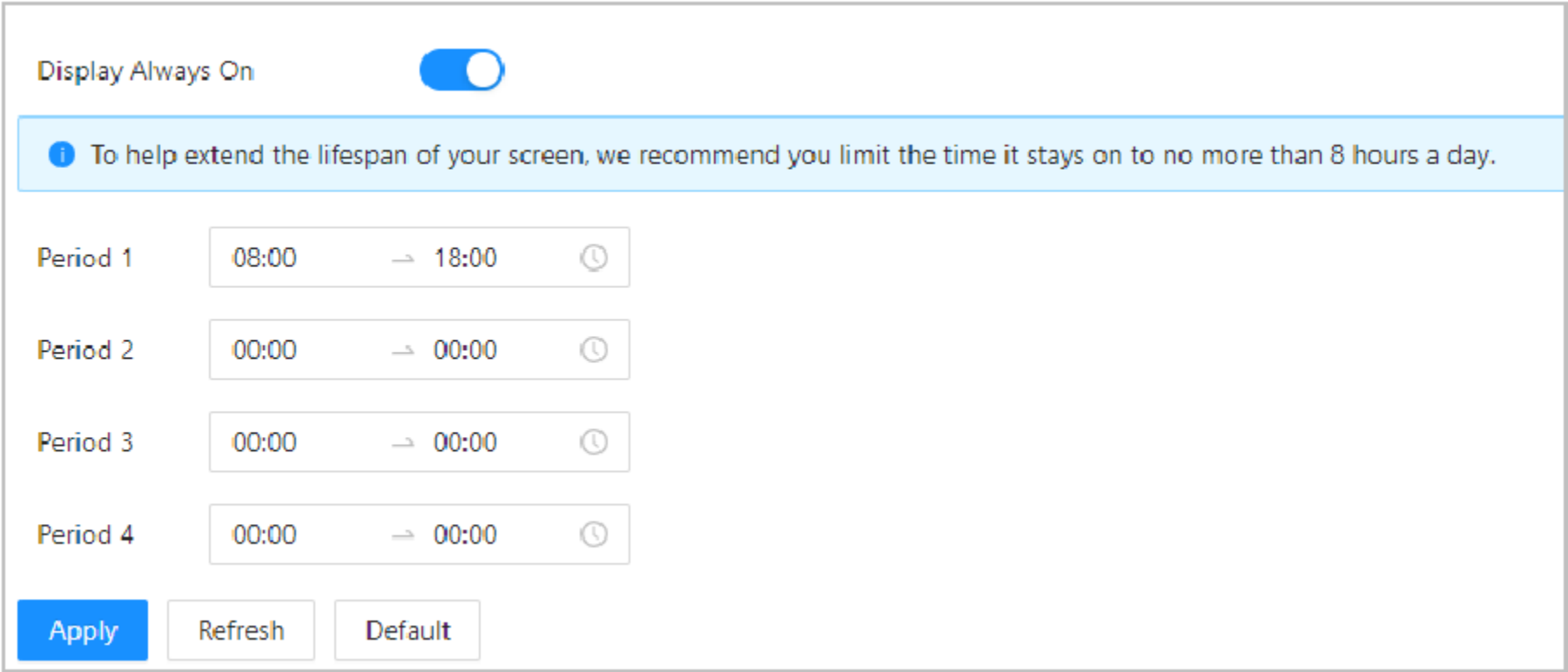
- Шаг 1 На домашней странице выберите "Система" > "Всегда включенная конфигурация".
- Шаг 2 Щелкните , а затем нажмите "Применить"
- Экран будет оставаться включенным в течение установленного периода времени после включения.



Длительное включение экрана может повлиять на срок его службы. Рекомендуется что вы используете более 8 часов непрерывного включения экрана в день.

- Шаг 3 Настройте период "Всегда включен", а затем нажмите "Применить".

Рисунок 4-56 "Всегда включен"



4.12 Центр технического обслуживания

4.12.1 Диагностика одним щелчком мыши

Система автоматически диагностирует конфигурации и состояние устройства для улучшения его работы Производительность.

Процедура

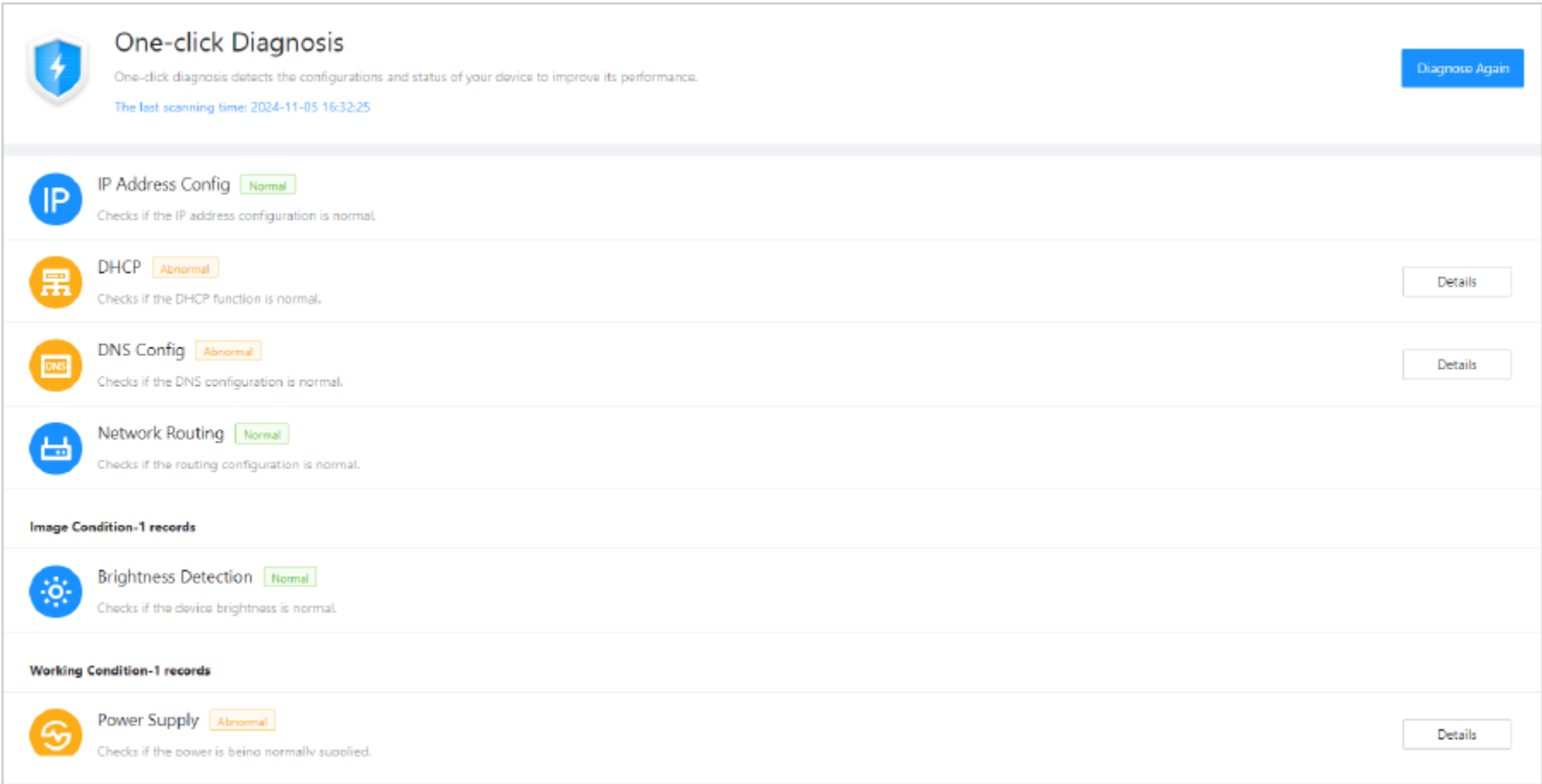
- Шаг 1 На домашней странице выберите Центр технического обслуживания > Диагностика одним щелчком мыши. Шаг 2 Нажмите кнопку Диагностика.

Система автоматически диагностирует конфигурации и состояние устройства и отображает результаты диагностики после ее завершения.

Шаг 3 (Необязательно) Щелкните Сведения, чтобы просмотреть сведения об аномальных элементах.

Вы можете проигнорировать аномалию или оптимизировать ее. Вы также можете снова нажать кнопку Диагностировать, чтобы снова выполнить автоматическую диагностику.

Рисунок 4-57 Диагностика одним щелчком мыши



4.12.2 Информация о системе

4.12.2.1 Просмотр информации о версии

На веб-странице выберите Центр технического обслуживания> Информация о системе> Версия, и вы сможете просмотреть версию информация об устройстве.

4.12.2.2 Просмотр юридической информации

На домашней странице выберите Центр обслуживания> Информация о системе> Юридическая информация, и вы сможете просмотреть лицензионное соглашение на программное обеспечение, политику конфиденциальности и уведомление о программном обеспечении с открытым исходным кодом.

4.12.3 Объем данных.

Вы можете видеть, сколько пользователей, карточек и изображений лиц может хранить Устройство. **Войдите на веб-страницу и выберите Центр обслуживания > Емкость данных.**

4.12.4 Просмотр журналов

Просмотр журналов, таких как системные журналы, журналы администратора и записи разблокировки.

4.12.4.1 Системные журналы.

Выполните поиск и просмотрите системные журналы.

Процедура

- Шаг 1
- Войдите на веб-страницу.
- Шаг 2
- Выберите Центр обслуживания > Log > Log**
- Шаг 3
- Выберите временной диапазон и тип журнала, а затем нажмите Поиск.

Связанные операции.

нажмите "Экспорт", чтобы экспортировать найденные журналы на ваш локальный компьютер.

Нажмите "Зашифровать резервную копию журнала", а затем введите пароль. Экспортированный файл можно открыть только после ввода пароля.

Нажмите , чтобы просмотреть подробную информацию о журнале.

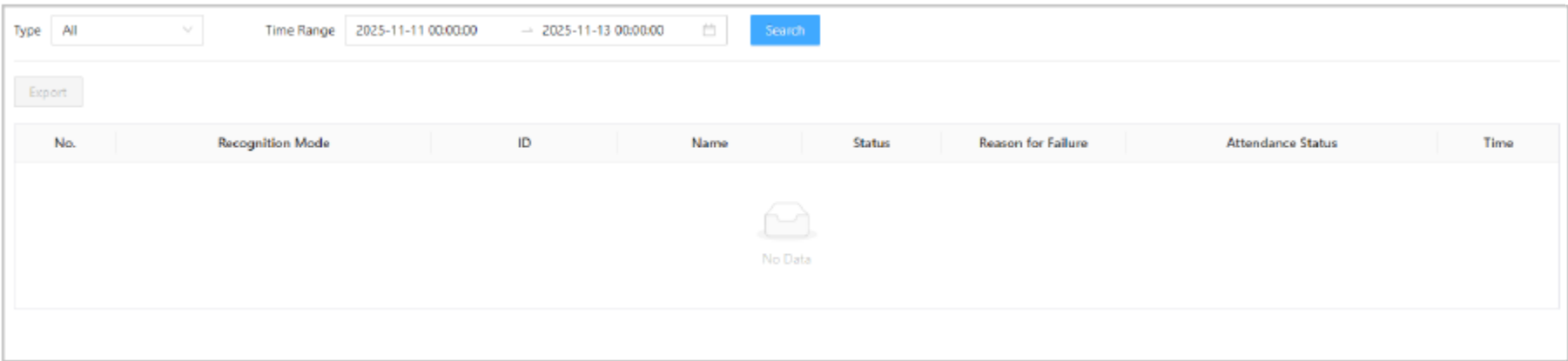
4.12.4.2 Записи разблокировки

Найдите записи разблокировки и экспортируйте их.

Процедура

- Шаг 1
- Войдите на веб-страницу.
- Шаг 2
- Выберите Центр обслуживания> Журнал> Записи разблокировки.**
- Шаг 3
- Выберите временной диапазон и тип, а затем нажмите кнопку Поиск.

Рисунок 4-58 Записи разблокировки



Связанные операции

Нажмите Экспорт, чтобы экспортировать записи разблокировки на свой компьютер.

4.12.4.3 Журнал вызовов

Просмотр журналов вызовов.

Процедура

- Шаг 1
- Войдите на веб-страницу.
- Шаг 2
- Выберите Центр обслуживания> Журнал> Журнал вызовов.**

4.12.4.4 Журналы аварийных сигналов

Просмотрите журналы аварийных сигналов.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Центр технического обслуживания > Log > AlarmLog
- Шаг 3 Выберите тип и временной диапазон.
- Шаг 4 Введите идентификатор администратора, а затем нажмите Поиск.

4.12.4.5 Журналы администратора

Выполните поиск журналов администратора с помощью идентификатора администратора.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Центр обслуживания > Log > AdminLog
- Шаг 3 Введите идентификатор администратора и нажмите кнопку Поиск.
- Нажмите Экспорт, чтобы экспортировать журналы администратора.

4.12.4.6 Управление USB.

Экспортируйте информацию о пользователе с / на USB.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Центр обслуживания. > Log > USB Руководство.



Убедитесь, что к устройству подключен USB-порт, прежде чем экспортировать данные или обновлять систему. Во избежание сбоев не вынимайте USB-порт и не выполняйте никаких операций с Устройство во время процесса.

Вы должны использовать USB для экспорта информации с устройства на другие устройства. Изображения лиц нельзя импортировать через USB.

- Шаг 3 Выберите тип данных, а затем нажмите "Импорт по USB" или "Экспорт по USB", чтобы импортировать данные.

4.12.5 Управление обслуживанием

4.12.5.1 Управление конфигурацией

Если нескольким устройствам требуются одинаковые конфигурации, вы можете настроить параметры для них импортируя или экспортируя файлы конфигурации.

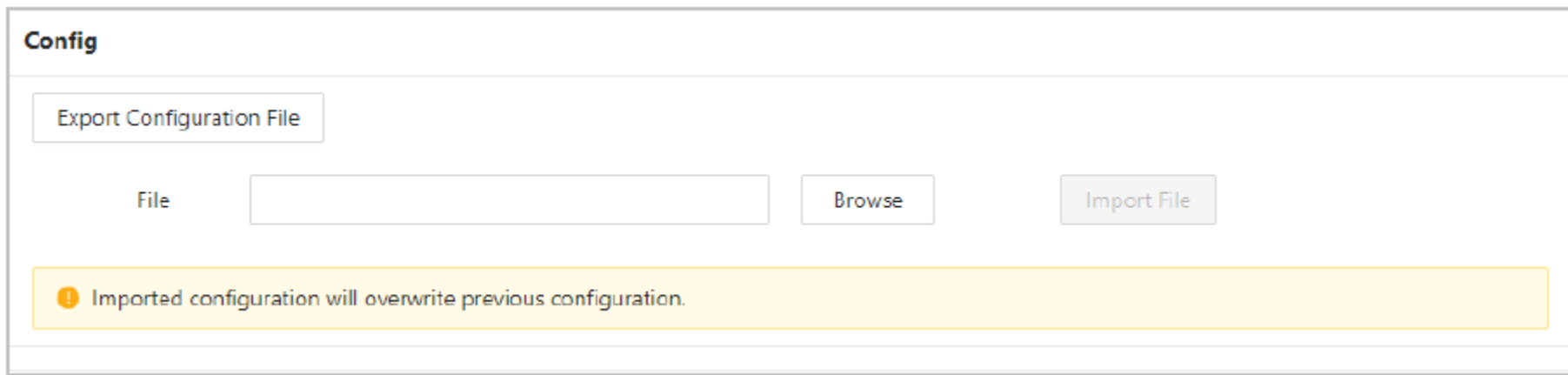
4.12.5.1.1 Экспорт и импорт файлов конфигурации

Вы можете импортировать и экспортировать файл конфигурации для данного устройства. Если вы хотите применить одинаковые конфигурации к нескольким устройствам, вы можете импортировать файл конфигурации на них.

Процедура

- Шаг 1
- Войдите на веб-страницу.
- Шаг 2
- Выберите "Управление обслуживанием" > "Конфигурация".

Рисунок 4-59 "Управление конфигурацией"



- Шаг 3
- Экспортируйте или импортируйте файлы конфигурации.

Экспортируйте файл конфигурации.

Нажмите кнопку Экспортировать файл конфигурации, чтобы загрузить файл на локальный компьютер.



IP-адрес экспортирован не будет.

Импортируйте файл конфигурации.

1. Нажмите кнопку Обзор, чтобы выбрать файл конфигурации.
2. Нажмите кнопку **Импортируйте конфигурацию.**



Файлы конфигурации могут быть импортированы только на устройства той же модели.

4.12.5.1.2 Настройка порога отпечатка пальца

Выберите Управление обслуживанием> Конфигурация. Настройте порог отпечатка пальца в соответствии с фактической ситуацией. Чем больше значение, тем выше точность сопоставления отпечатков пальцев, тем ниже частота ложного распознавания, в то время как скорость прохождения также снижается.



Для устройства с функцией отпечатков пальцев отображается эта конфигурация.

Введите пороговое значение сходства отпечатков пальцев, а затем нажмите Применить.

Рисунок 4-60 Пороговое значение отпечатка пальца

Fingerprint

Fingerprint Si...

3

(1-10)

Apply

Refresh

Default

4.12.5.1.3 Восстановление заводских настроек по умолчанию

Процедура

- Шаг 1

Выберите Управление обслуживанием> Настройка.

!

Восстановление настроек устройства по умолчанию приведет к потере данных. Пожалуйста, имейте в виду рекомендуется.
- Шаг 2

При необходимости восстановите заводские настройки по умолчанию.

Восстановить заводские настройки (сохраняет конфигурацию сети): сбрасывает все конфигурации устройства, за исключением конфигурации сети.

Восстановить значение по умолчанию (сохраняет журналы, информацию о пользователе и конфигурацию сети): сбрасывает конфигурации устройства и удаляет все данные, кроме информации о пользователе, журналов и сетевых конфигураций.
- 4.12.5.2 Техническое обслуживание
- Регулярно перезапускайте устройство во время простоя, чтобы улучшить его производительность.
- Процедура
- Шаг 1

Войдите на веб-страницу.

Шаг 2

Выберите Управление техническим обслуживанием> Техническое обслуживание.

Шаг 3

Установите время, а затем нажмите Применить.

Устройство перезагрузится в запланированное время, или вы можете нажать кнопку Перезапустить, чтобы перезапустить его немедленно.
- 4.12.6 Обновление системы
- !

Используйте правильный файл обновления. Убедитесь, что вы получили правильный файл обновления из технической Поддержка.

Не отключайте источник питания или сеть, а также не перезапускайте и не выключайте устройство во время обновления.
- 139

4.12.6.1 Обновление файла

Процедура

- Шаг 1

На домашней странице выберите Система> Обновить.
- Шаг 2

В разделе Обновление файла нажмите Обзор, а затем загрузите файл обновления.



Файл обновления должен быть файлом.bin.
- Шаг 3

Нажмите Обновить.

Устройство перезагрузится после завершения обновления.

4.12.6.2 Онлайн-обновление

Процедура

- Шаг 1

На домашней странице выберите Система> Обновить.
- Шаг 2

В области Онлайн-обновлений выберите метод обновления.

Выберите

Автоматическая проверка обновлений, и устройство автоматически проверит наличие последней обновление версии.

Выберите "Проверка вручную", и вы сможете сразу же проверить, установлена ли последняя версия Доступно.

Шаг 3

(Необязательно) Нажмите Обновить сейчас, чтобы немедленно обновить устройство.
- 4.12.7 Расширенное обслуживание.
- Получение информации об устройстве и захват пакета, чтобы упростить работу обслуживающего персонала устранение неполадок.
- 4.12.7.1 Экспорт
- Процедура
- Шаг 1** На домашней странице выберите Центр обслуживания> Расширенное обслуживание> Экспорт. **Шаг 2** Нажмите Экспорт, чтобы экспортировать серийный номер, версию встроенного ПО, журналы работы устройства и информация о конфигурации.
- 4.12.7.2 Перехват пакетов
- Перехват пакетов
1. На домашней странице выберите Центр обслуживания> Расширенное обслуживание> Перехват пакетов.
- Рисунок 4-61 Перехват пакетов
- | Packet Capture | | | | | | |
|----------------|----------------|--------------|------------|--------------|------------|-----------------------|
| NIC | Device Address | IP 1: Port 1 | | IP 2: Port 2 | | Packet Sniffer Size |
| | | | | | | Packet Sniffer Backup |
| eth0 | 1 166 | Optional | : Optional | Optional | : Optional | 0.00MB ▶ |
| eth2 | 1 101 | Optional | : Optional | Optional | : Optional | 0.00MB ▶ |
- 140

2. Введите IP-адрес, нажмите 

 изменить на .

3. После сбора достаточного количества данных нажмите .

Перехваченные пакеты автоматически загружаются на ваш локальный компьютер.

Проверка сети

1. На домашней странице выберите **Центр обслуживания>Расширенное обслуживание>Сбор пакетов.**

2. В области тестирования сети введите адрес назначения, а затем настройте размер пакета данных.

Рисунок 4-62 Сетевое тестирование

Network Test

Destination Address

Test

Data Packet Size

64

Byte (64-4096)

Test Result

Copy

3. Нажмите кнопку Проверить.

Результат отобразится в области результатов тестирования. Вы можете скопировать результат.

4.13 Настройки безопасности (необязательно)

4.13.1 Состояние безопасности

Просканируйте модули пользователей, обслуживания и безопасности, чтобы проверить состояние безопасности устройства.

Справочная информация

Обнаружение пользователей и служб: Проверьте, соответствует ли текущая конфигурация рекомендации.

Сканирование модулей безопасности: Проверяет состояние работы модулей безопасности, таких как аудио и передача видео, надежная защита, предупреждение о безопасности и защита от атак, но не определяет, включены ли они.

Процедура

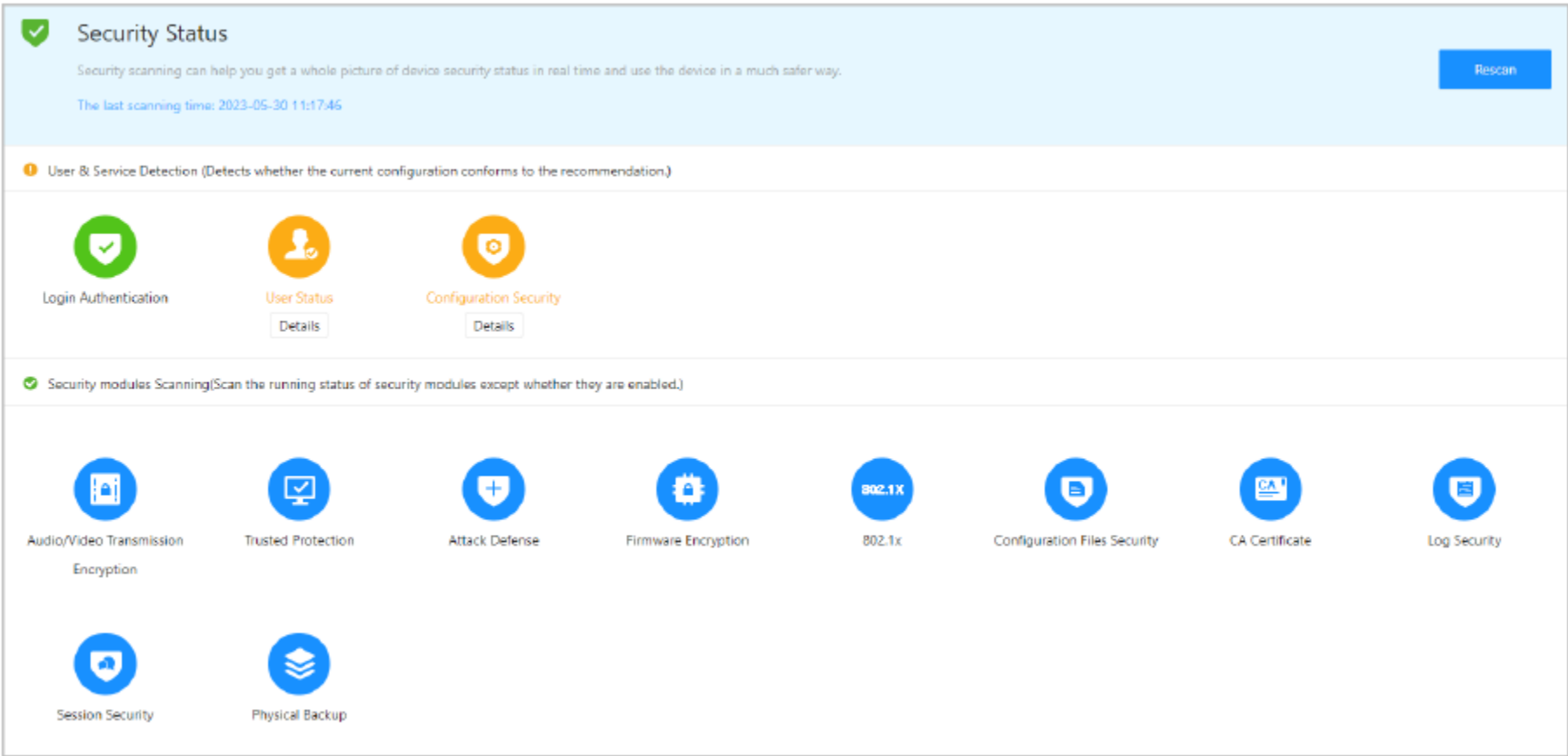
Шаг 1  **Выберите>Состояние безопасности.**

Шаг 2 Нажмите кнопку Повторное сканирование, чтобы выполнить проверку безопасности устройства.



Наведите указатель мыши на значки модулей безопасности, чтобы увидеть их состояние работы.

Рисунок 4-63 Состояние безопасности



Связанные операции

После выполнения сканирования результаты будут отображаться разными цветами. Желтый указывает на то, что модули безопасности неисправны, а зеленый указывает на то, что модули безопасности работают нормально.

Нажмите "Подробнее", чтобы просмотреть подробную информацию о результатах сканирования.

Нажмите "Игнорировать", чтобы проигнорировать отклонение, и оно не будет сканироваться. Отклонение, которое было проигнорировано, будет выделено серым цветом.

Нажмите кнопку Оптимизировать, чтобы устранить неисправность.

4.13.2 Настройка HTTPS

Создайте сертификат или загрузите сертификат, прошедший проверку подлинности, и затем вы сможете войти на веб-страницу через HTTPS на вашем компьютере. Протокол HTTPS обеспечивает связь по компьютерной сети.

Процедура

Шаг 1 Выберите  > **Системная служба> HTTPS.**

Шаг 2 Включите службу HTTPS.



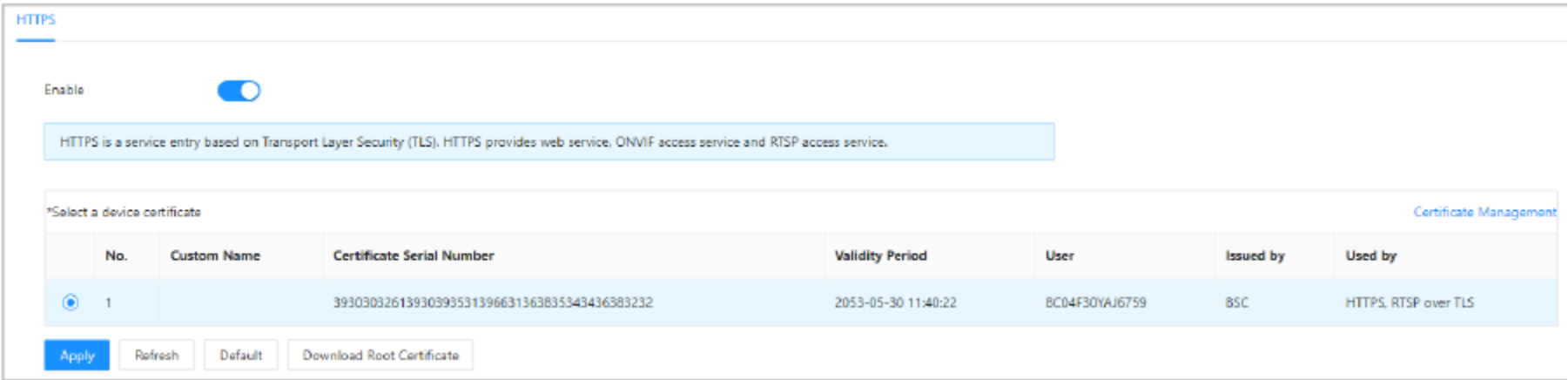
Если вы включите совместимый с TLS v1.1 и более ранние версии, могут возникнуть угрозы безопасности. Обратите внимание.

Шаг 3 Выберите сертификат.



Если в списке нет сертификатов, нажмите "Управление сертификатами", чтобы загрузить сертификат.

Рисунок 4-64 HTTPS



Шаг 4 Нажмите Применить.

Введите “https://IP адрес: порт https” в веб-браузере. Если сертификат установлен, вы можете успешно войти на веб-страницу. В противном случае на веб-странице сертификат будет отображаться как неправильный или ненадежный.

4.13.3 Защита от атак

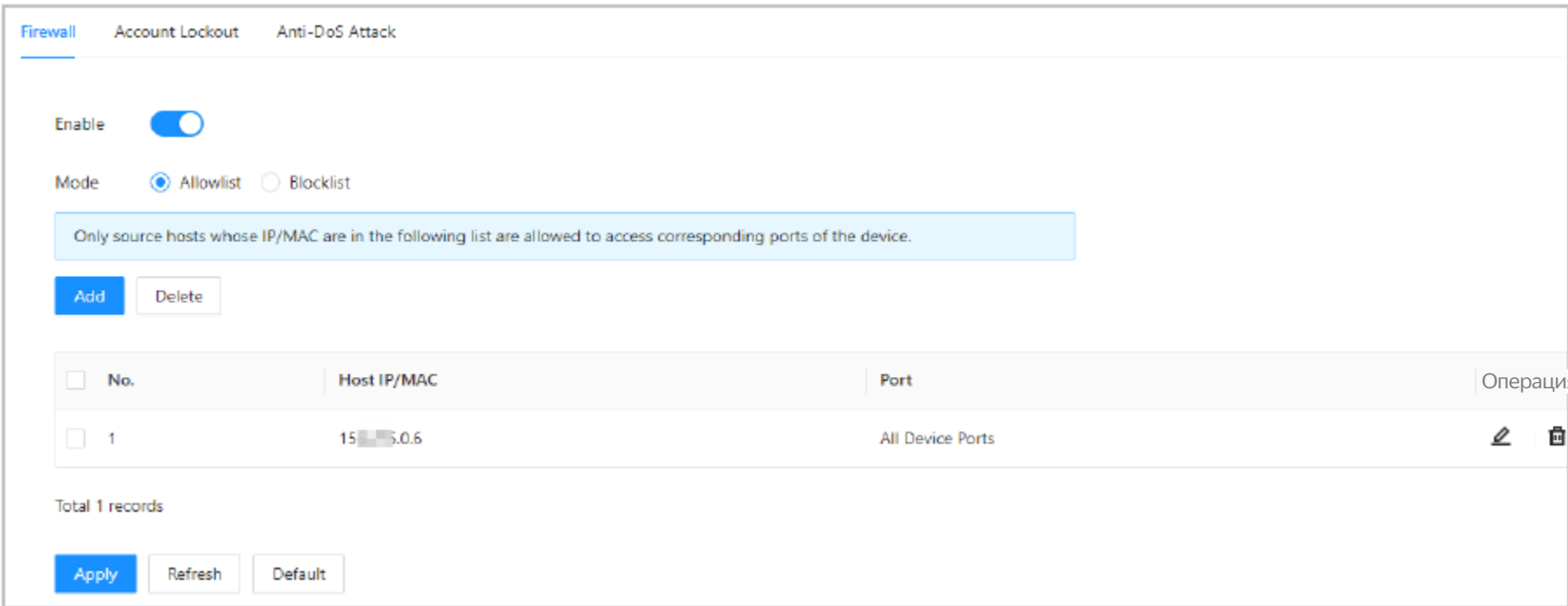
4.13.3.1 Настройка брандмауэра

Настройте брандмауэр для ограничения доступа к устройству.

Процедура

- Шаг 1 Выберите > **Защита от атак**> **Брандмауэр**.
- Шаг 2 Щелкните , чтобы включить функцию брандмауэра.

Рисунок 4-65 Брандмауэр



Шаг 3 Выберите режим: Список разрешений и список блокировок.

- Список разрешенных адресов: только IP / MAC-адреса из списка разрешенных адресов могут получить доступ к Устройству.
- Список блокировок: IP / MAC-адреса из списка блокировок не позволяют получить доступ к устройству.

Шаг 4 Нажмите "Добавить", чтобы ввести информацию об IP-адресе.

Рисунок 4-66 Добавление информации об IP-адресе

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there are four fields: "Add Mode" with a dropdown menu showing "IP", "IP Version" with a dropdown menu showing "IPv4", "IP Address" with a text input field containing three dots, and "All Device Ports" with a toggle switch that is currently turned on. At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Шаг 5 Нажмите "OK".

Связанные операции

Нажмите  чтобы отредактировать информацию об IP.

Нажмите  чтобы удалить IP-адрес.

4.13.3.2 Настройка блокировки учетной записи

Если неправильный пароль вводится определенное количество раз, учетная запись будет заблокирована.

Процедура

- Шаг 1 Выберите  > **Защита от атак** > **Блокировка учетной записи**.
- Шаг 2 Введите количество попыток входа в систему и время, на которое будут заблокированы учетная запись администратора и ONVIF пользователь будет заблокирован.

Рисунок 4-67 Блокировка учетной записи

Firewall

Account Lockout

Anti-DoS Attack

Device Account

Login Attempt

5time(s)

Lock Time

5

min

Apply

Refresh

Default

Попытка входа в систему: ограничение попыток входа в систему. Если неправильный пароль вводится в течение определенного количества раз, учетная запись будет заблокирована.

Время блокировки: продолжительность, в течение которой вы не можете войти в систему после блокировки учетной записи.

Шаг 3 Нажмите Применить.

4.13.3.3 Настройка защиты от DoS-атаки.

Вы можете включить SYN Flood Attack Defense и ICMP Flood Attack Defense для защиты устройства от Dos-атак.

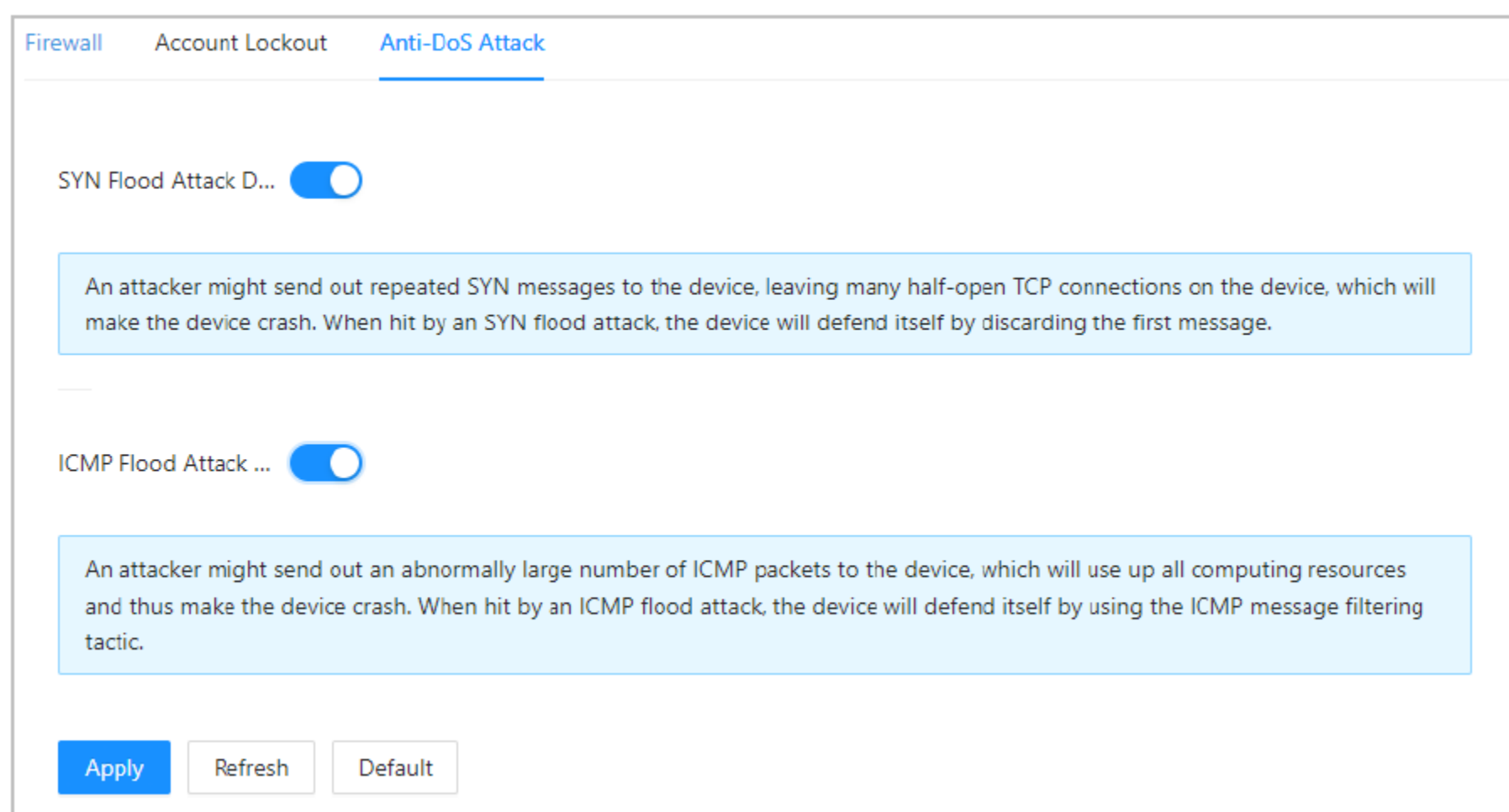
Процедура

- Шаг 1

Выберите  > Защита от атак > Защита от DoS-атаки.
- Шаг 2

Включите SYN Flood Attack Defense или ICMP Flood Attack Defense, чтобы защитить Устройство от Dos-атаки.

Рисунок 4-68 Анти-DoS-атака



Шаг 3 Нажмите Применить.

4.13.4 Установка сертификата устройства

Создайте сертификат или загрузите аутентифицированный сертификат, а затем вы сможете войти в систему через HTTPS на своем компьютере.

4.13.4.1 Создание сертификата

Создайте сертификат для устройства.

Процедура

Шаг 1 Выберите > Сертификат центра сертификации> Сертификат устройства.

Шаг 2 Выберите Установить сертификат устройства.

Шаг 3 Выберите Создать сертификат и нажмите **Далее**.

Шаг 4 Введите информацию о сертификате.

Рисунок 4-69 Информация о сертификате

Step 2: Fill in certificate information.

Custom Name

* IP/Domain Name

103

Organization Unit

Organization

* Validity Period

Days (1~5000)

* Region

Province

City Name

Back

Create and install certificate

Cancel



Название региона не должно превышать 2 символов. Мы рекомендуем ввести сокращение названия региона.

Шаг 5 Нажмите **Создайте и установите сертификат**.

Только что установленный сертификат отображается на странице Сертификата устройства после того, как сертификат успешно установлен.

Связанные операции

Нажмите "Войти в режим редактирования" на странице "Сертификат устройства", чтобы отредактировать название сертификата.

Нажмите , чтобы загрузить сертификат.

Нажмите , чтобы удалить сертификат.

4.13.4.2 Подача заявки на получение сертификата CA и импорт

Импортируйте сертификат CA сторонних производителей на устройство.

Процедура

Шаг 1 Выберите  Сертификат CA> Сертификат устройства.

Шаг 2 Нажмите Установить сертификат устройства.

Шаг 3 Выберите "Подать заявку на сертификат центра сертификации и импорт" (рекомендуется) и нажмите "Далее".

Шаг 4 Введите информацию о сертификате.

IP/ доменное имя: IP-адрес или доменное имя устройства.

Регион: Название региона не должно превышать 3 символов. Мы рекомендуем вам ввести сокращение названия региона.

Рисунок 4-70 Информация о сертификате (2)

Step 2: Fill in certificate information.

* IP/Domain Name

1703

Organization Unit

Organization

* Region

Province

City Name

Back

Create and Download

Cancel

Шаг 5 Нажмите Создать и загрузить.

Сохраните файл запроса на свой компьютер.

Шаг 6 Обратитесь к стороннему центру сертификации за сертификатом, используя файл запроса.

Шаг 7 Импортируйте подписанный сертификат центра сертификации.

1. Сохраните сертификат центра сертификации на своем компьютере.

2. **Нажмите кнопку Установка сертификата устройства.**

3. Нажмите кнопку Обзор, чтобы выбрать сертификат центра сертификации.

4. Нажмите кнопку **Импортировать и установить.**

Недавно установленный сертификат отображается на странице Сертификата устройства после того, как сертификат успешно установлен.

Нажмите Воссоздать, чтобы снова создать файл запроса.

Нажмите Импортировать позже, чтобы импортировать сертификат в другой раз.

Связанные операции

Нажмите Войти в режим редактирования на странице Сертификата устройства, чтобы отредактировать название сертификата.

Нажмите , чтобы загрузить сертификат.

Нажмите , чтобы удалить сертификат.

4.13.4.3 Установка существующего сертификата

Если у вас уже есть сертификат и файл закрытого ключа, импортируйте сертификат и файл закрытого ключа. Процедура

Шаг 1 Выберите Безопасность> Сертификат центра сертификации > Сертификат устройства.

- Шаг 2 Нажмите "Установить сертификат устройства".
- Шаг 3 Выберите "Установить существующий сертификат" и нажмите Далее.
- Шаг 4 Нажмите кнопку Обзор, чтобы выбрать файл сертификата и закрытого ключа и ввести закрытый ключ Пароль.

Рисунок 4-71 Сертификат и закрытый ключ

Step 2: Select certificate and private key.

Custom Name

Certificate Path

Browse

Private Key

Browse

Private Key Password

Back

Import and Install

Cancel

- Шаг 5 Нажмите кнопку **Импорт и установка**.

Недавно установленный сертификат отображается на странице Сертификата устройства после сертификат успешно установлен.

Связанные операции

- Нажмите Войти в режим редактирования на странице Сертификата устройства, чтобы отредактировать название сертификата.
- Нажмите , чтобы загрузить сертификат.
- Нажмите , чтобы удалить сертификат.

4.13.5 Установка сертификата доверенного центра сертификации

Сертификат доверенного центра сертификации - это цифровой сертификат, который используется для проверки подлинности веб-сайтов и серверы. Например, когда используется протокол 802.1x, сертификат СА для коммутаторов требуется для проверки подлинности его идентификатора.

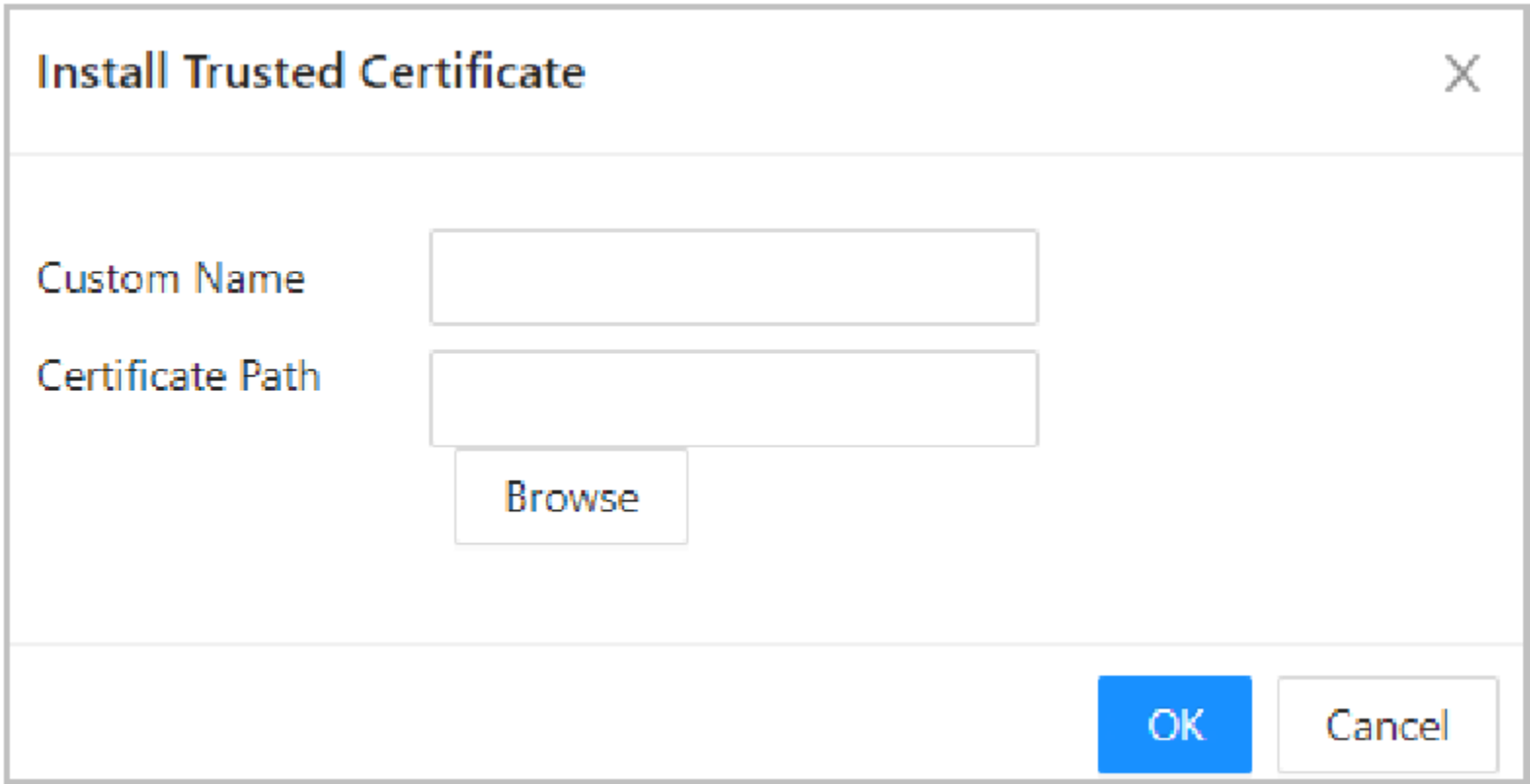
Справочная информация

802.1X - это протокол сетевой аутентификации, который открывает порты для доступа к сети, когда организация проверяет подлинность личности пользователя и разрешает ему доступ к сети.

Процедура

- Шаг 1 Выберите  > **Сертификат ЦС** > **Сертификаты доверенных ЦС**.
- Шаг 2 Выберите **Установить доверенный сертификат**.
- Шаг 3 Нажмите кнопку Обзор, чтобы выбрать доверенный сертификат.

Рисунок 4-72 Установите доверенный сертификат



Шаг 4 Нажмите OK.

Недавно установленный сертификат отображается на странице Сертификаты доверенного центра сертификации после того, как сертификат успешно установлен.

Связанные операции

Нажмите Войти в режим редактирования на странице Сертификат устройства, чтобы отредактировать название сертификата.

Нажмите , чтобы загрузить сертификат.

Нажмите , чтобы удалить сертификат.

4.13.6 Предупреждение системы безопасности

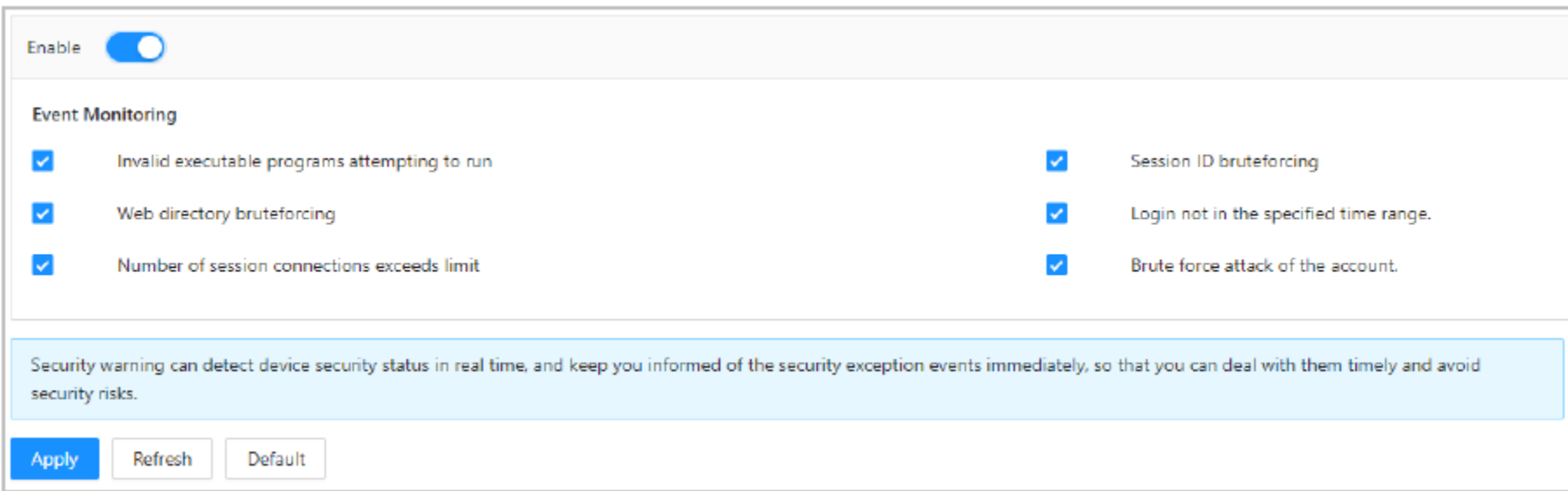
Процедура

Шаг 1 Выберите >  Предупреждение системы безопасности.

Шаг 2 Включите функцию предупреждения системы безопасности.

Шаг 3 Выберите элементы мониторинга.

Рисунок 4-73 Предупреждение системы безопасности



Шаг 4 Нажмите Применить.

4.13.7 Проверка подлинности безопасности

Процедура

Шаг 1 Выберите Безопасность> Проверка подлинности безопасности.

Шаг 2 Выберите алгоритм обработки сообщений.

Шаг 3 Нажмите Применить.

Рисунок 4-74 Проверка подлинности системы безопасности

Digest Algorithm for Authentication

Digest Algorithm for User Authentication

☒ MD5☐ SHA256

Digest Algorithm for ONVIF User Authentication

☒ MD5☐ SHA256

Apply

Refresh

Default

5 Операции с телефоном

5.1 Инициализация

Когда телефон подключен к той же локальной сети, что и контроллер доступа, вы можете инициализировать доступ Контроллер в первый раз или после восстановления заводских настроек устройства по умолчанию на веб-странице телефон. В этом разделе описывается инициализация телефона через точку доступа Wi-Fi.

Предварительные требования

Убедитесь, что контроллер доступа не подключен к сети Wi-Fi или 4G.



Wi-Fi и точка доступа Wi-Fi доступны на некоторых моделях.

Процедура

- Шаг 1 Включите устройство.
- Шаг 2 через 30 секунд после того, как устройство отобразится на экране инициализации, подключитесь к точке доступа Wi-Fi
на вашем телефоне. Название точки доступа - это серийный номер продукта + модель устройства.
- Если вы не подключались к точке доступа Wi-Fi в течение 30 минут, точка доступа отключена. Шаг 3 Откройте браузер на своем телефоне и перейдите по IP-адресу (адрес по умолчанию - 192.168.3.1) точки доступа.
- Шаг 4 Нажмите **Начать инициализацию**.
- Шаг 5 Выберите язык.
- Шаг 6 Введите и подтвердите пароль, введите адрес электронной почты, а затем нажмите Далее.



- В пароль должен состоять из 8-32 непустых символов и содержать не менее двух типы следующих символов: заглавные, строчные, цифры и специальные символы (исключая " " ; &). Установите пароль повышенной безопасности, следуя инструкциям по вводу пароля запрос на проверку надежности.
- Сохраняйте пароль в безопасности после инициализации и регулярно меняйте пароль на повышение безопасности.
- Если вы хотите сбросить пароль администратора путем сканирования QR-кода, вам понадобится связанный адрес электронной почты для получения кода безопасности.

- Шаг 7 При необходимости включите автоматическую проверку, а затем нажмите Завершено.

5.2 Вход на веб-страницу

Предварительные требования

Убедитесь, что телефон, используемый для входа на веб-страницу, подключен к той же локальной сети, что и устройство.

Процедура

- Шаг 1 Откройте браузер, а затем введите IP-адрес устройства.
- Вы можете войти на веб-страницу следующими тремя способами:
- В Телефон и устройство подключены к одной локальной сети. Откройте браузер на телефоне и затем введите IP-адрес.

В Телефон и устройство подключены к одной локальной сети. Отсканируйте QR-код с помощью **Настройки связи> Сетевые настройки> Wi-Fi на веб-странице вашего** телефона.

Подключите точку доступа устройства на вашем телефоне. На главном экране устройства, коснитесь верхнего правого угла, чтобы перейти к экрану точки доступа Wi-Fi. Отсканируйте QR-код IP-адреса через браузер на вашем телефоне или в браузере вашего телефона введите IP адрес, который отображается на экране точки доступа Wi-Fi.

Вы также можете выбрать Настройки связи> Настройки сети> Точку доступа Wi-Fi, чтобы перейти в главное меню.



Wi-Fi и точка доступа Wi-Fi доступны на некоторых моделях.

Шаг 2

Введите имя пользователя и пароль.

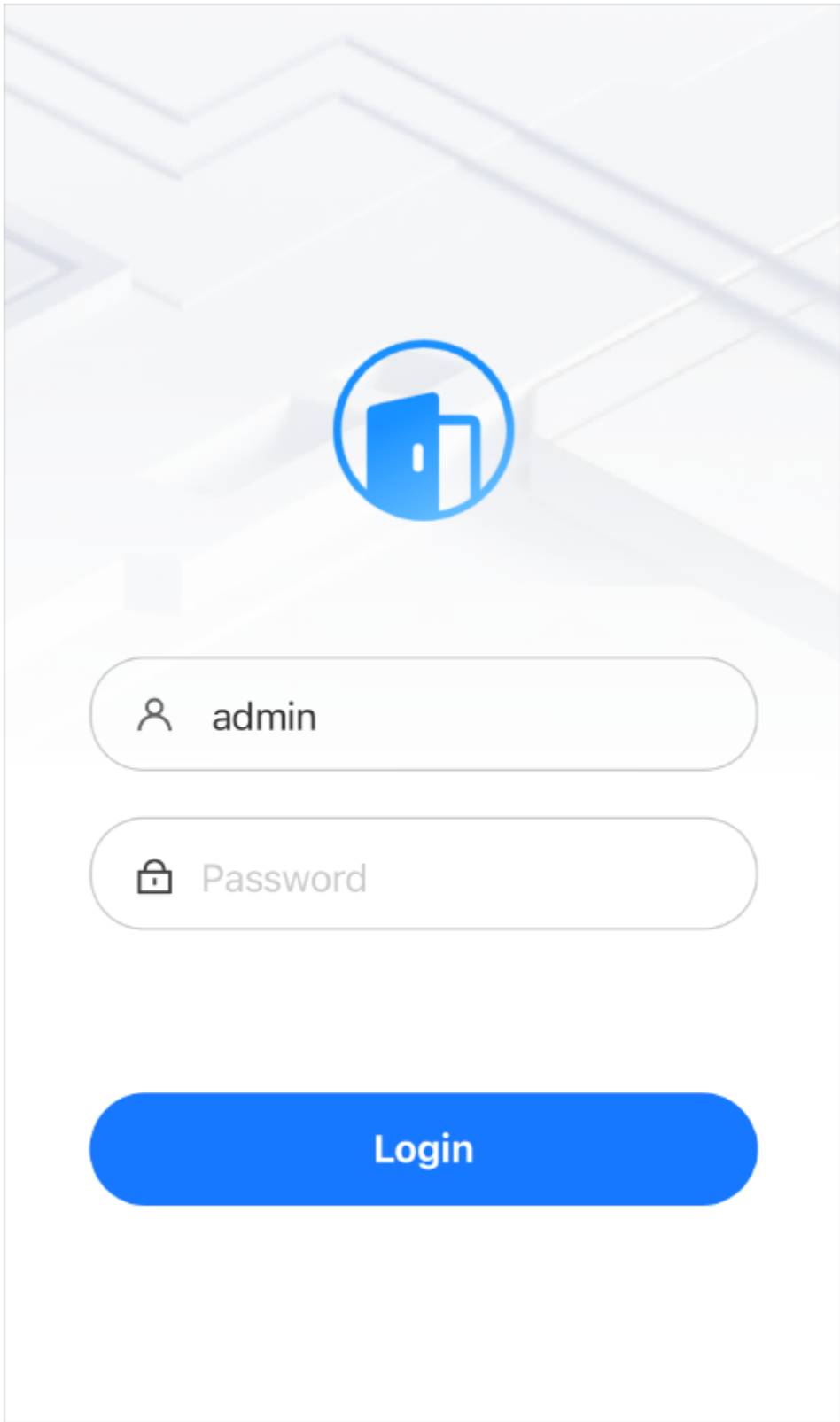
Нажмите рядом с паролем, чтобы просмотреть его.



В Имя администратора по умолчанию - admin, а пароль - тот, который вы установили во время инициализации. Мы рекомендуем вам регулярно менять пароль администратора для повышения безопасности.

Если вы забыли пароль администратора для входа, вы можете сбросить пароль через веб-страницу на компьютере. Дополнительные сведения см. в разделе "4.3 Сброс пароля".

Рис. 5-1 страницу входа



Шаг 3 Нажмите "Вход".

5.3 Домашняя Страница

На главной странице отображается после успешного входа в систему.

Нажмите в правом верхнем углу веб-страницы. а затем коснитесь QR-кода документации на продукт Код, чтобы отсканировать QR-код и получить информацию о продукте, или коснитесь Выход, чтобы выйти из учетной записи.

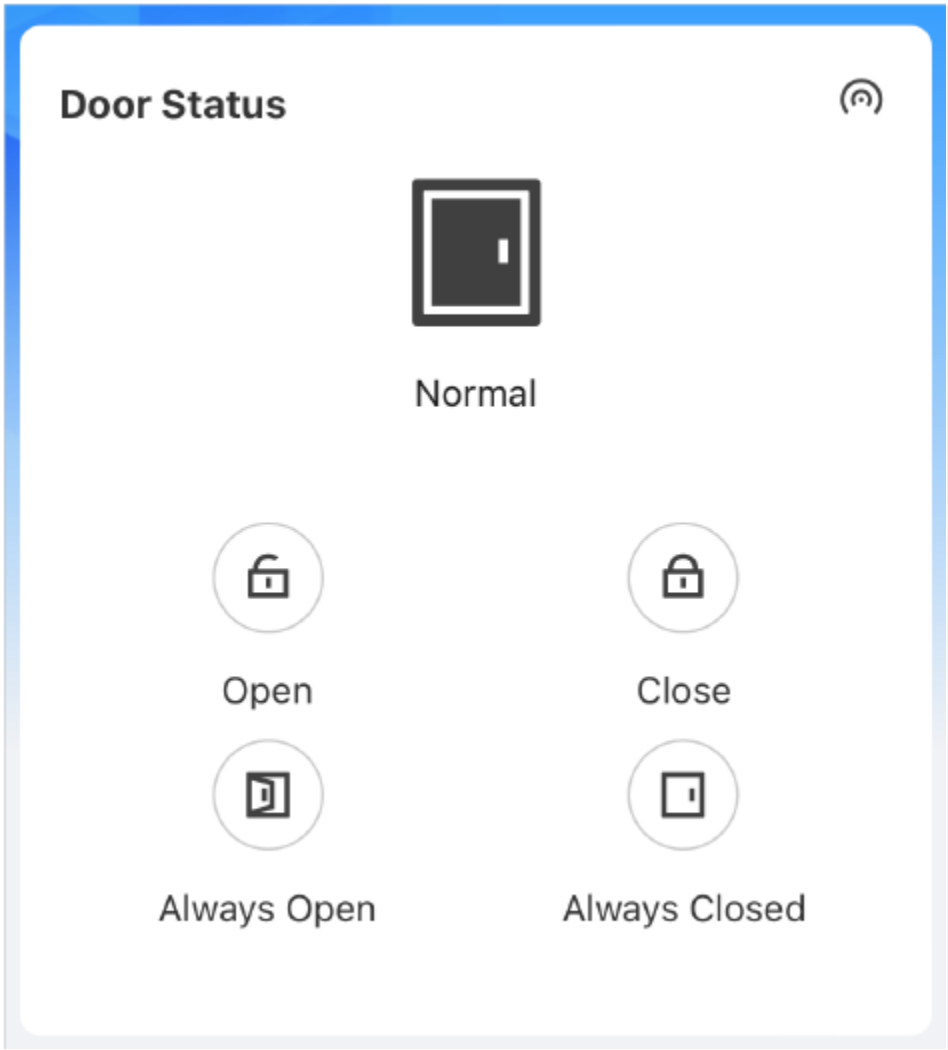


Документ на продукт доступен на некоторых моделях.

В В области состояния двери отображается состояние двери. Вы можете дистанционно открывать или закрывать дверь. Вы также можете настроить состояние двери как всегда открытой или всегда закрытой.

- ◇  указывает, что подключена проводная сеть.
- ◇  указывает, что точка доступа Wi-Fi включена.

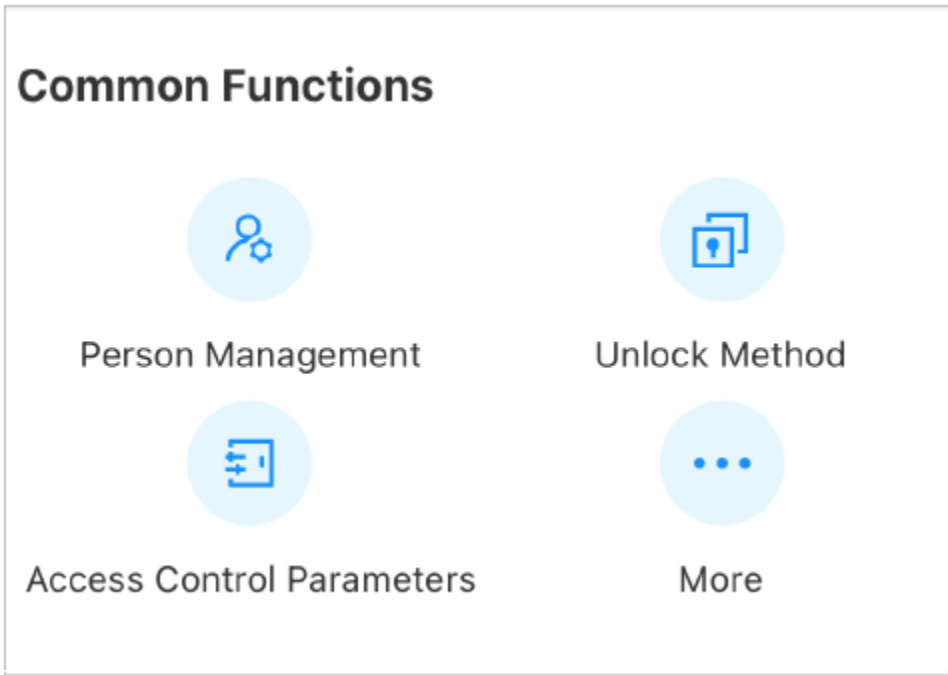
5-2 Состояние двери



На Рисунке

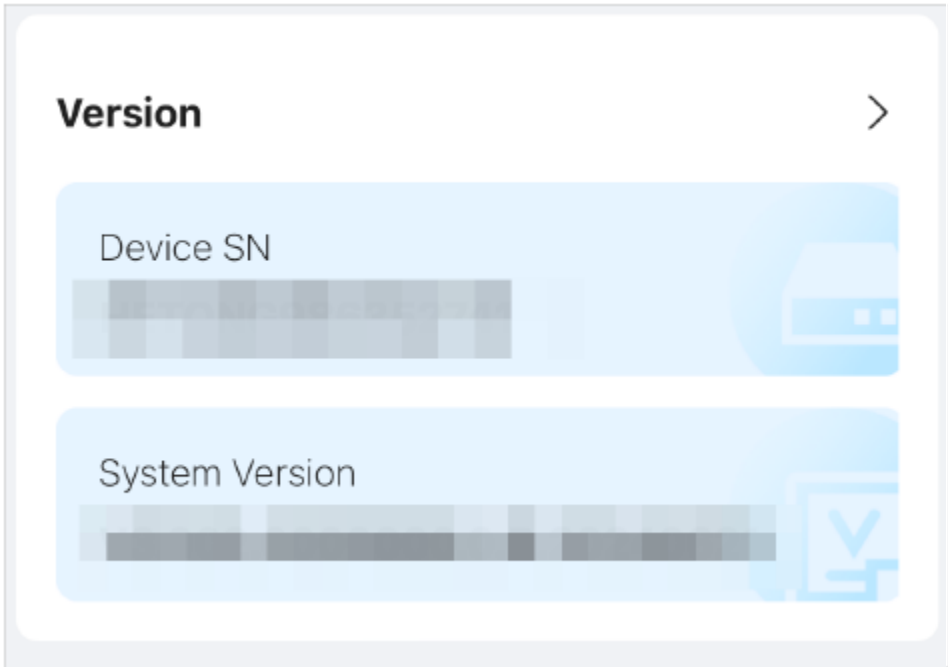
В области общих функций отображается меню конфигурации устройства. Нажмите Ещё, чтобы просмотреть все меню конфигурации.

Рисунок 5-3 Общие функции



Просмотрите серийный номер и информацию о версии в области Версии. Нажмите>, чтобы просмотреть сведения о версии.

Рисунок 5-4 Версия



5.4 Управление персоналом

Добавьте пользователя и настройте разрешения.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Коснитесь Управление пользователями, а затем нажмите +.
- Шаг 3 Настройте информацию о пользователе.

Рисунок 5-5 Добавление пользователя (1)

Basic Info

* ID

Name

Access Credentials

PasswordNot Added >

Card0 >

Fingerprint0 >

Bluetooth Card

No email was configured. You cannot request a Bluetooth card through email.

0 >

Verification ModeSame as Device >

PermissionUser >

Рисунок 5-6 Добавление пользователя (2)

Validity Period

Forever

Email

General Plan

255-Default

Holiday Plan

255-Default

User Type

General User

Times Used

Unlimited

Department

1-10-11

Schedule Mode

Department Schedule

Permission Type

Unlock and Attendance

Add

Таблица 5-1 Описание параметров

Параметр	Описание
ID	Идентификатор пользователя подобен идентификатору сотрудника, который может быть цифрами и буквенными комбинациями, а максимальная длина номера составляет 30 символов.
Имя	Имя может содержать до 32 символов (включая цифры, условные обозначения и буквы).
Пароль	Настройте пароль пользователя. Максимальная длина пароля составляет 8 цифр. Принудительный пароль - это пароль разблокировки + 1. Например, если пароль пользователя равен 12345, принудительный пароль будет 12346. Сигнализация о принудительном пароле сработает, когда для отпирания двери будет использован принудительный пароль.
Карта	Нажмите "Добавить", вручную введите номер карты или проведите пальцем по карте в области "Добавить карту" на устройстве. Пользователь может зарегистрировать не более 5 карт. После успешного добавления коснитесь добавленной карты, вы можете изменить номер карты, настроить карту в качестве принудительной или удалить карту. Если вы включите принудительную сигнализацию, сработает сигнал тревоги, если для отпирания двери будет использована принудительная карта. Один пользователь может установить только одну принудительную карту.

Параметр	Описание
Отпечаток пальца	Регистрируйте отпечатки пальцев. Пользователь может зарегистрировать до 3 отпечатков пальца в качестве отпечатка пальца принуждения. Сигнализация сработает, когда отпечаток пальца с целью принуждения. 1. Нажмите Добавить. 2. Прижмите палец к сканеру в соответствии с инструкциями на экране. 3. Нажмите ОК. Функция отпечатка пальца доступна только на некоторых моделях. Мы не рекомендуем устанавливать первый отпечаток пальца в качестве принудительного отпечатка пальца. Один пользователь может установить только один принудительный отпечаток пальца.
Карта Bluetooth	Bluetooth доступен только на некоторых моделях. Вы можете выбрать Запрос по электронной почте или запрос через регистрационный код. Запрос по электронной почте: подходит для первого запроса карты Bluetooth . Вы можете запросить до 5 карт Bluetooth и должны использовать адрес электронной почты, зарегистрированный в DMSS. Вы должны ввести свой зарезервированный адрес электронной почты, прежде чем использовать эту функцию. 1. Настройте адрес электронной почты, зарегистрированный в DMSS. 2. Нажмите "Запросить по электронной почте"., и тогда можно запросить карты Bluetooth. Запрос через регистрационный код: подходит, если у вас уже есть карта Bluetooth и вы хотите повторно использовать ее на другом контроллере доступа, поддерживающем функцию Bluetooth. 1. Скопируйте регистрационный код Bluetooth из DMSS. 2. Нажмите "Запросить через регистрационный код", а затем введите код. 3. Нажмите "ОК".
Режим проверки	Настройте режим проверки для пользователя. Вы можете использовать режим, который совпадает с режимом устройства, или настроить режим. То же, что и на устройстве: режим такой же, как и на устройстве. Пользовательский: после выбора пользовательского отображаются комбинированный метод и разблокируйте методы по мере необходимости. Или: Используйте один из выбранных методов разблокировки, чтобы открыть дверь. О И: Используйте все выбранные методы разблокировки, чтобы открыть дверь. о Режим индивидуальной проверки действителен только для локального устройства. Его нельзя использовать во внешних кард-ридерах. Если режим индивидуальной проверки отличается от режима на устройстве приоритет отдается настроенному режиму.

Параметр		Описание
Разрешение	Пользователь Администратор	: У пользователей есть только разрешения на доступ к двери и : Администраторы могут настраивать устройство помимо раз посещение.
Срок действия	Укажите лицо	дата истечения срока действия разрешений на доступ к двери .
Общий план	Люди	вы можете отпереть дверь или записаться на прием в течение
	Вы	можете выбрать более одного плана.
План на Отпуск	Люди	вы можете отпереть дверь или принять дежурство в течение с
	Вы	можете выбрать более одного праздничного дня.
Разрешение на блокировку	Выберите	локальный и внешний замок по мере необходимости.
Тип пользователя	Гость	Обычный пользователь: Обычные пользователи могут разбл Пользователь из списка блокировки: Когда пользователи из сп персонал получит уведомление. Пользователь: Гости могут отпирать дверь в течение определ определенное количество раз. По истечении установленного они не смогут отпереть дверь. Патрульный пользователь: Патрульные пользователи могут от нет прав доступа к двери. VIP-пользователь: Когда VIP-пользователь открывает дверь, он режимами разблокировки, такими как мультикарта и раздел в Другой пользователь: Когда он откроет дверь, она останется н секунд. Пользовательский пользователь 1 / Пользовательский пользо
Использованное время	Установите разблокировку	ограничение на разблокировку для приглашенных пользовате открыть дверь.
Отдел	Добавьте человека,	пользователей в отдел. Если для отдела назначено расписание, они будут следовать установле
Режим расписания		Расписание отдела: назначьте расписание отдела пользователю. Личное расписание: Назначьте пользователю личное расписа
	o	Эта функция доступна только на некоторых моделях. Если вы установите здесь для режима расписания значение "Р личное расписание, настроенное вами для пользователя в раз Настройка расписания" > "Личное расписание", будет недейст
Тип разрешения		Разблокировка и посещаемость: Пользователь имеет разреш разблокировать дверь, используя настроенные методы прове Посещаемость: У человека есть только разрешение на посеще отпереть дверь. После того, как человек успешно подтвердит создается одна запись о неудачной разблокировке.

Шаг 4 Нажмите Добавить.

5.5 Настройка системы

5.5.1 Просмотр информации о версии

На веб-странице выберите "Дополнительно"> "Система"> "Версия", и вы сможете просмотреть информацию о версии на Устройстве.

5.5.2 Управление конфигурацией

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Дополнительно> Система> Конфигурация.
- Шаг 3 При необходимости восстановите заводские настройки по умолчанию.

Восстановить заводские настройки (сохраняет конфигурацию сети): сбрасывает все конфигурации устройства, за исключением конфигурации сети.

Восстановить значение по умолчанию (сохраняет журналы, информацию о пользователе и конфигурацию сети): сбрасывает конфигурации устройства и удаляет все данные, кроме информации о пользователе, журналов и сетевых конфигураций.

5.5.3 Техническое обслуживание

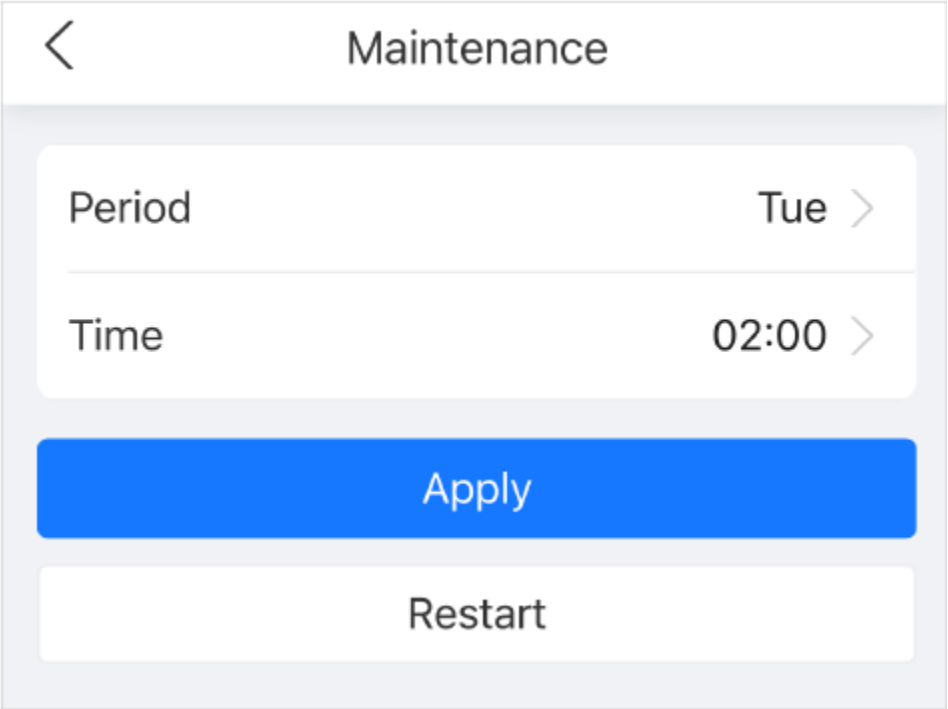
Регулярно перезапускайте устройство во время простоя, чтобы улучшить его производительность.

Процедура.

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите "Дополнительно"> "Система"> "Техническое обслуживание".
- Шаг 3 Установите время, а затем нажмите Применить.

Устройство перезагрузится в запланированное время, или вы можете нажать Перезагрузить, чтобы перезапустить его немедленно.

Рисунок 5-7 Обслуживание



5.5.4 Настройка времени

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите "Дополнительно"> "Система"> "Время".
- Шаг 3 Настройте время.

Рисунок 5-8 Настройка параметров времени

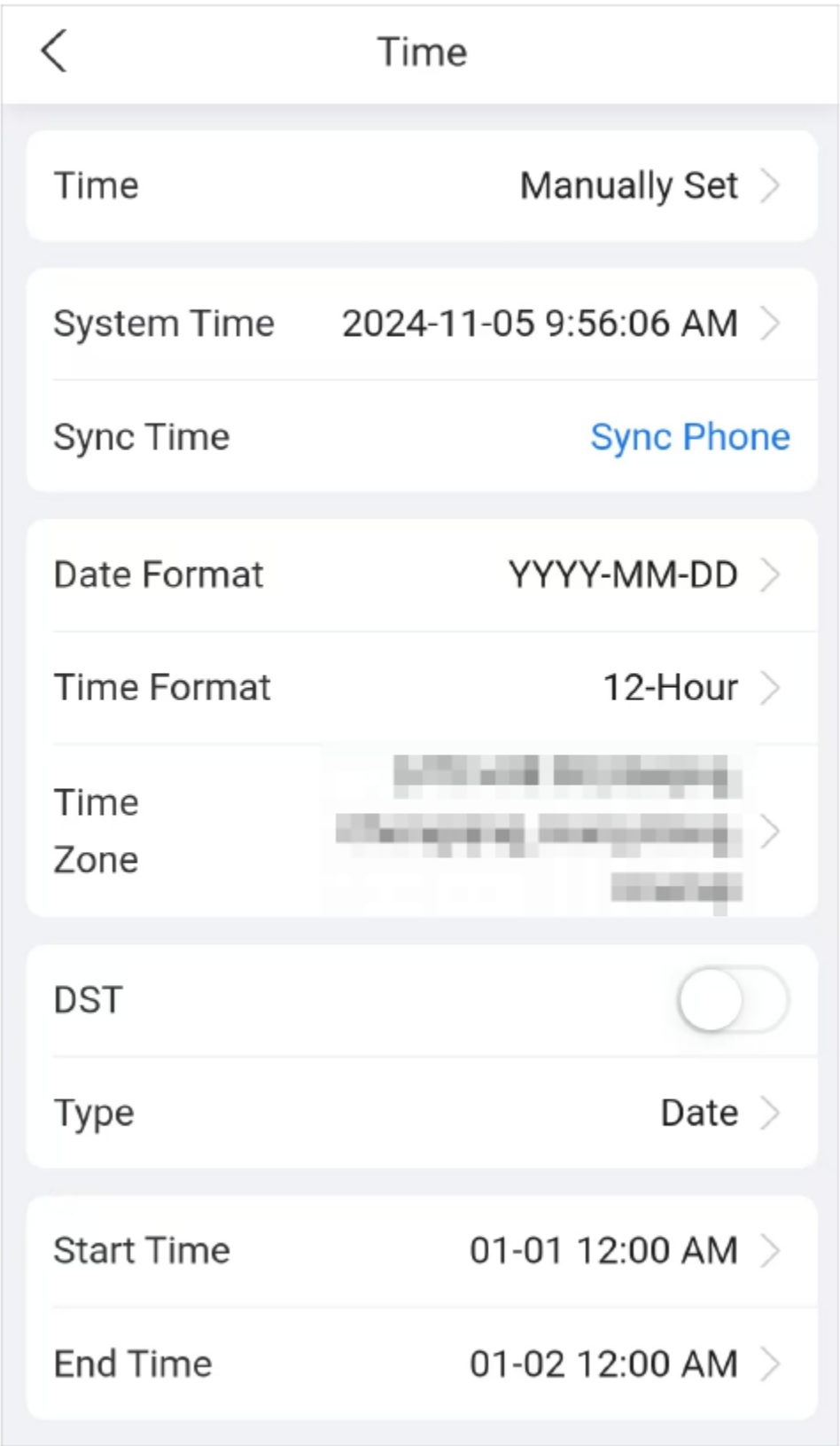


Таблица 5-2 Описание настроек времени

Параметр	Описание
Время	Ручная настройка: введите время вручную или вы можете нажать Синхронизировать телефон, чтобы синхронизировать время с телефоном. NTP: устройство автоматически синхронизирует время с NTP сервером. Сервер : Введите домен NTP-сервера. Порт : введите порт NTP-сервера. Интервал: введите его время с интервалом синхронизации.

Параметр	Описание
Формат даты Формат времени	Выберите формат даты и формат времени.
Часовой пояс.	Выберите часовой пояс.
Летнее время	1. (Необязательно) Включите летнее время. 2. Выберите дату или неделю в качестве типа. 3. Настройте время начала и окончания летнего времени.

Шаг 4 Нажмите Применить.

5.5.5 Объем данных

Вы можете видеть, сколько пользователей, карточек, изображений лиц, отпечатков пальцев, журналов, записей разблокировки и другой информации, которую может хранить устройство.

Войдите на веб-страницу и выберите Дополнительно> Система> Емкость данных.

5.5.6 Язык

Войдите на веб-страницу, выберите Дополнительно> Система> Язык. Измените язык, а затем нажмите **Применить**.

5.6 Настройка посещаемости

Эта функция доступна только на избранных моделях.

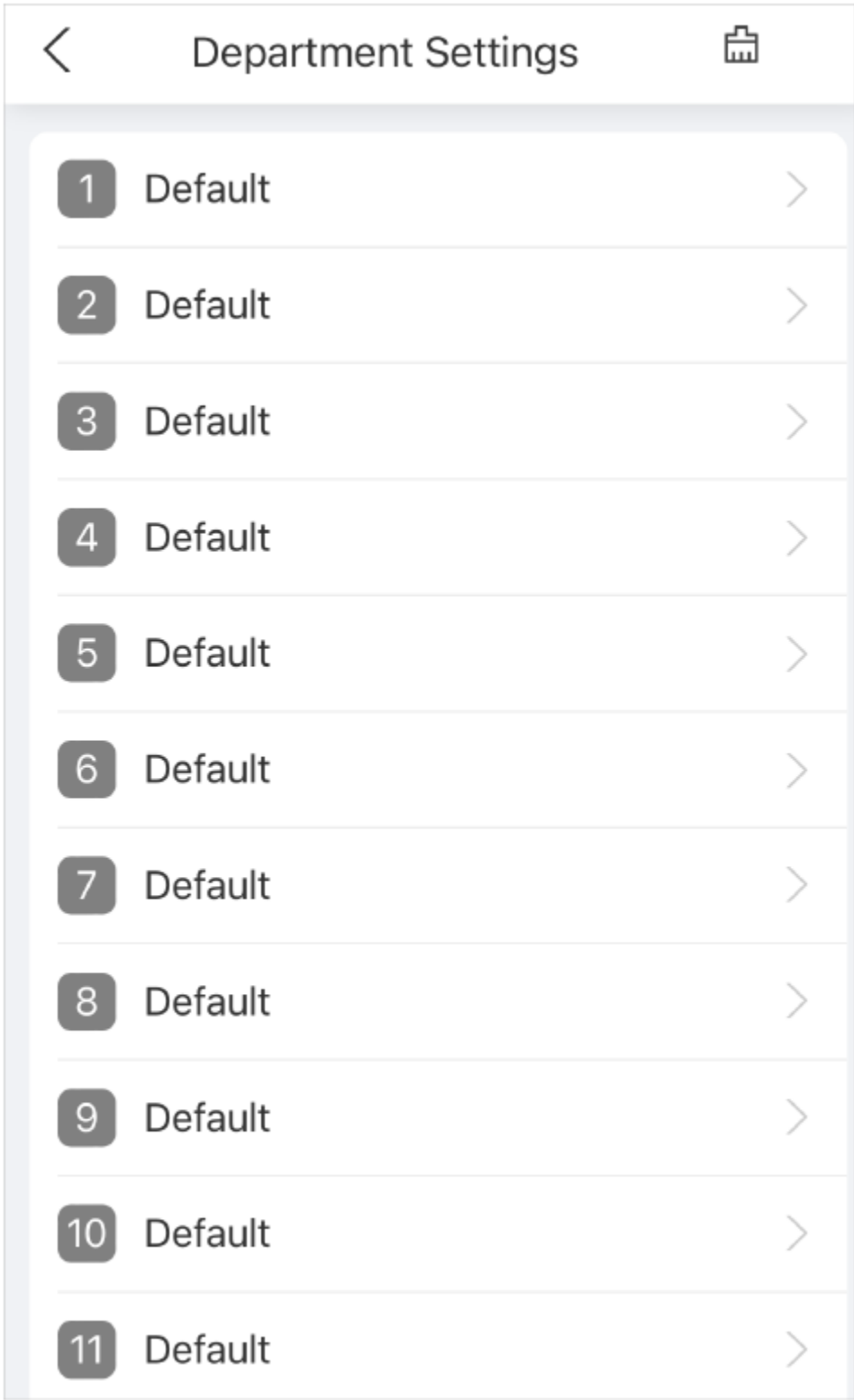
5.6.1 Настройка отделов

Процедура

Шаг 1 Войдите на веб-страницу.

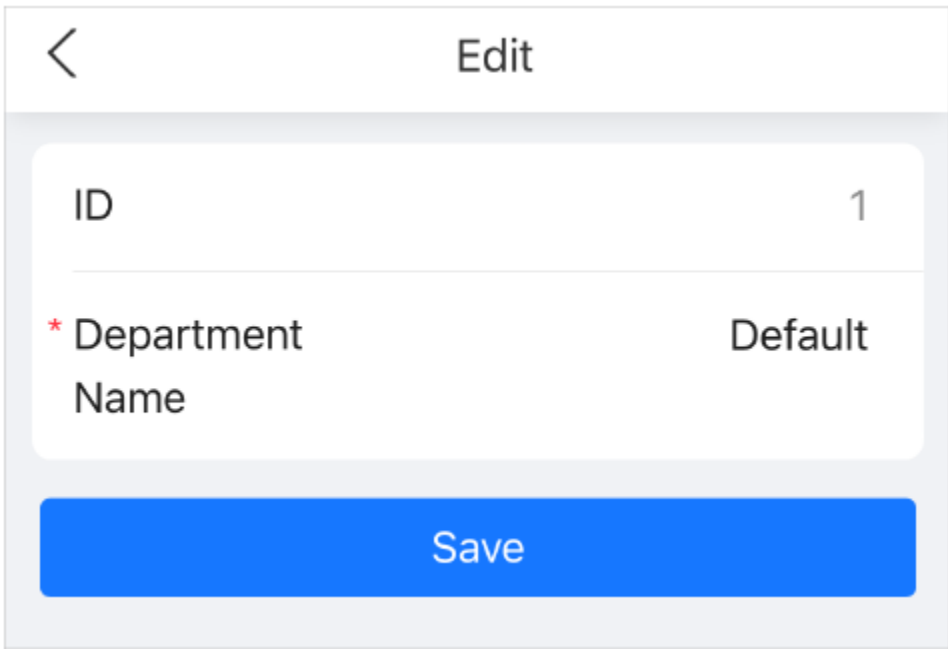
Шаг 2 Выберите Дополнительно> Настройка посещаемости> Настройки отдела.

Рисунок 5-9 Настройки отдела



Шаг 3 Коснитесь отдела, чтобы переименовать отдел, а затем нажмите Сохранить.
Существует 20 отделов по умолчанию. Мы рекомендуем вам переименовать их.

Рисунок 5-10 Переименовать отдел



Связанные операции

Вы можете нажать  чтобы восстановить настройки отделов по умолчанию.

5.6.2 Настройка смен

Настройте смены для определения правил посещаемости по времени. Сотрудники должны работать в назначенное время начинать свою смену и уходить в конце, за исключением случаев, когда они решают работать сверхурочно.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите "Дополнительно" > "Настройка посещаемости" > "Конфигурация смены"> "Смена".

Рисунок 5-11 Список смен

Shift Config			
Shift		Holiday	
1	Default 08:00-17:00	00:00-00:00	>
2	Default 08:00-17:00	00:00-00:00	>
3	3 08:00-17:00	00:00-00:00	>
4	4 08:00-17:00	00:00-00:00	>
5	5 08:00-17:00	00:00-00:00	>
6	6 08:00-17:00	00:00-00:00	>
7	7 08:00-17:00	00:00-00:00	>
8	8 08:00-17:00	00:00-00:00	>

- Шаг 3 Коснитесь "Смены", чтобы настроить параметры смены, а затем нажмите "Сохранить".

Рисунок 5-12 Настройка смены

<

Edit Shift

Shift No.

1

* Shift Name

Period 1

08:00~17:00

>

Period 2

00:00~00:00

>

Period 3

00:00~00:00

>

Overtime Period

00:00~00:00

>

* Limit for Arriving Late

5 min

* Limit for Leaving Early

5 min

Save

Таблица 5-3 Описание параметров смены

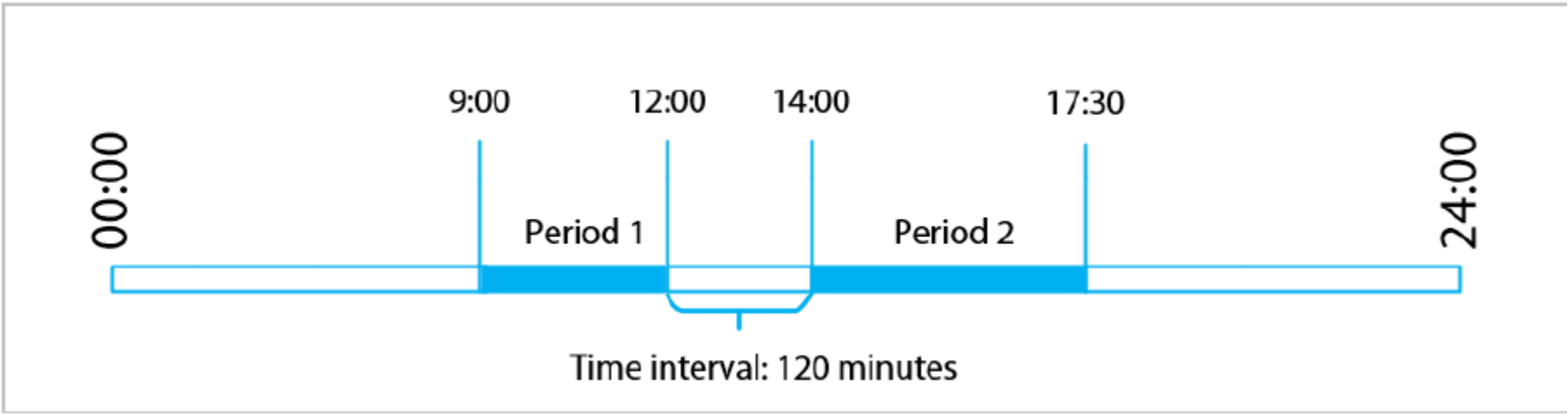
Параметр	Описание
Название смены	Введите название смены.
Период 1 Период 2	Укажите временной диапазон, в течение которого сотрудники могут приходить и уходить в течение рабочего дня. Необходимо настроить как минимум 1 период.
Период 3	Если вы установили только один период посещаемости, сотрудникам необходимо приходить и уходить по назначенному времени, чтобы избежать появления аномалий в их отчетах о посещаемости. Например, если вы установите с 08:00 на 17:00, сотрудники должны приходить к 08:00 и заканчивать работу с 17:00 и далее. Если вы установите 2 периода посещаемости, эти два периода не могут перекрываться. Сотрудники должны приходить и уходить по расписанию для обоих периодов. Если вы установите 3 периода, эти 3 периода не могут перекрываться. Сотрудникам необходимо засекать время прихода и ухода за 2 смежными периодами. Последний период может превышать дни. Если период сверхурочной работы является пос вы можете настроить его на пересечение дней.

Параметр	Описание
Период сверхурочной работы	Сотрудники, которые приходят или уходят в течение определенного периода, считаются работающими сверх обычного рабочего времени.
Ограничение на поздний приход (мин.) Ограничение на ранний уход (мин.)	Сотрудникам может быть предоставлено определенное количество времени, в течение которого они могли прийти немного позже и уйти немного раньше. Например, если обычное время приема - 08:00, допустимый период может быть установлен равным 5 минутам, чтобы сотрудники, прибывающие в течение этого периода, считались опоздавшими.

Если вы настраиваете более одного периода, обратитесь к следующим инструкциям для выполнения функции посещаемости.

Если интервал времени между двумя периодами равен четному числу, вы можете разделить время интервала на 2 и назначить первую половину интервала первому периоду, который будет временем отсчета времени. Вторую половину интервала следует назначить второму периоду как часы во времени.

Рисунок 5-13 Временной интервал (четное число)

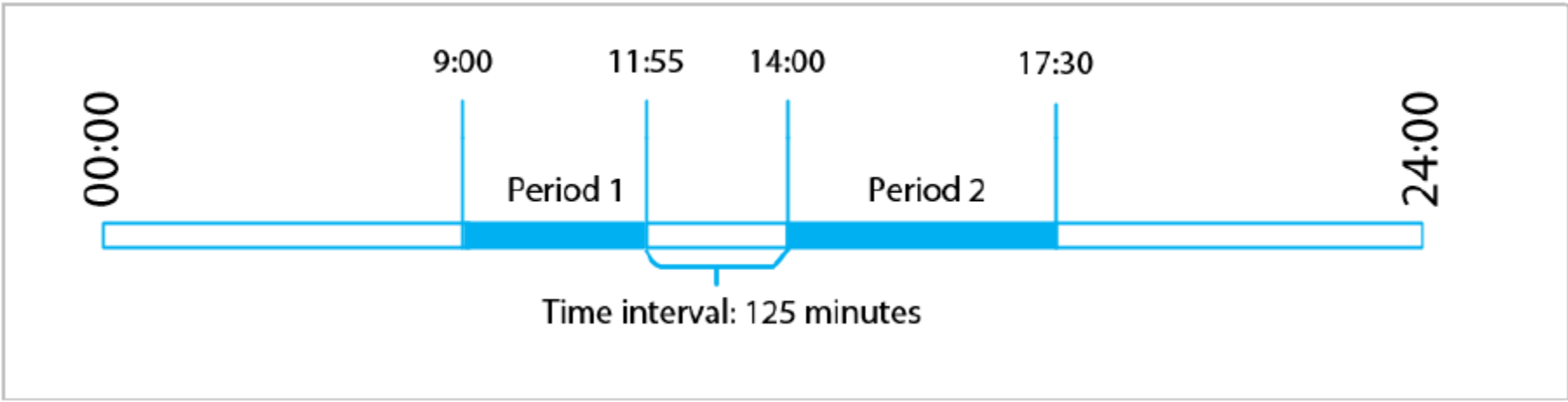


Например: если интервал равен 120 минутам, то время отсчета для периода 1 равно от с 12:00 до 12:59, а рабочее время для периода 2 - с 13:00 до 14:00.

Если пользователь отсчитывает время несколько раз в течение периода 1, действительным будет самое позднее время, и если он отсчитывает время несколько раз в течение периода 2, действительным будет самое раннее время.

Когда временной интервал между двумя периодами равен нечетному числу, наименьшей части интервала будет присвоен первому периоду, который будет временем отсчета времени. Наибольшая часть интервала будет отнесена ко второму периоду в качестве отсчета времени в time.

Рисунок 5-14 Временной интервал (нечетное число)



Например: если интервал равен 125 минутам, то время отсчета для периода 1 равно от с 11:55 до 12:57, а время начала периода 2 - с 12:58 до 14:00. Период 1 длится 62 минуты, а период 2 - 63 минуты.



Если пользователь отсчитывает время несколько раз в течение периода 1, действительным будет самое позднее время, а если он отсчитывает время несколько раз в течение периода 2, действительным будет самое раннее время.

Если есть только один период, и вы не приходите и не заканчиваете его к указанному времени, он считается отсутствующим в течение 1 дня.

Если имеется более одного периода, и вы не приходите и не выходите к назначенному времени время одного периода считается отсутствующим в течение 0,5 дня. Если вы не приходите или не уходите к назначенному времени в течение 2 или более чем 2 периодов, это считается отсутствием в течение 1 дня. Присутствие в периоды сверхурочной работы не меняет статус отсутствия сотрудника.

Если вы настроите для последнего периода пересечение дней, обратитесь к следующим инструкциям, чтобы выполнить функцию присутствия.

- Если второй день приходится на обычную смену, посещаемость остается такой же, как обычно.

Если второй день приходится на праздничный, вы можете выйти в любое время из 24 часов в праздничный день.



Время всех посещений указано с точностью до секунды. Например, если обычный хронометраж время установлено на 8:05 утра, сотрудник, пришедший на работу в 8:05:59 утра, не будет считаться опоздавший. Но сотрудник, который прибудет в 8:06 утра, будет отмечен как опоздавший на 1 минуту.

Связанные операции

Вы можете нажать  чтобы восстановить заводские настройки по умолчанию для смен.

5.6.3 Настройка выходных

Настройте планы отпусков, чтобы установить периоды, в течение которых посещаемость не отслеживалась. Процедура

Шаг 1 Войдите на веб-страницу.

Шаг 2 Выберите "Дополнительно"> "Настройка посещаемости"> "Конфигурация смены"> "Отпуск".

Шаг 3 Нажмите +, чтобы добавить планы на отпуск.

Шаг 4 Настройте параметры, а затем нажмите Сохранить.

Рисунок 5-15 Добавление отпуска

<

Add Attendance Holiday

* Attendance Holiday No.

>

* Attendance Holiday

Time

>

Save

Таблица 5-4 Описание параметров

Параметр	Описание
Посещаемость праздничного дня №	Номер праздничного дня.
Праздничный день посещаемости	Название праздничного дня.
Время	Время начала и окончания праздничного дня.

Шаг 5 Нажмите ОК.

5.6.4 Настройка графиков работы

График работы обычно относится к дням в месяце и часам в день, которые сотрудник ожидается, что он будет находиться на своем рабочем месте. Вы можете создавать различные типы графиков работы на основе различных отдельных лица или отделы, а затем и сотрудники должны следовать установленному графику работы.

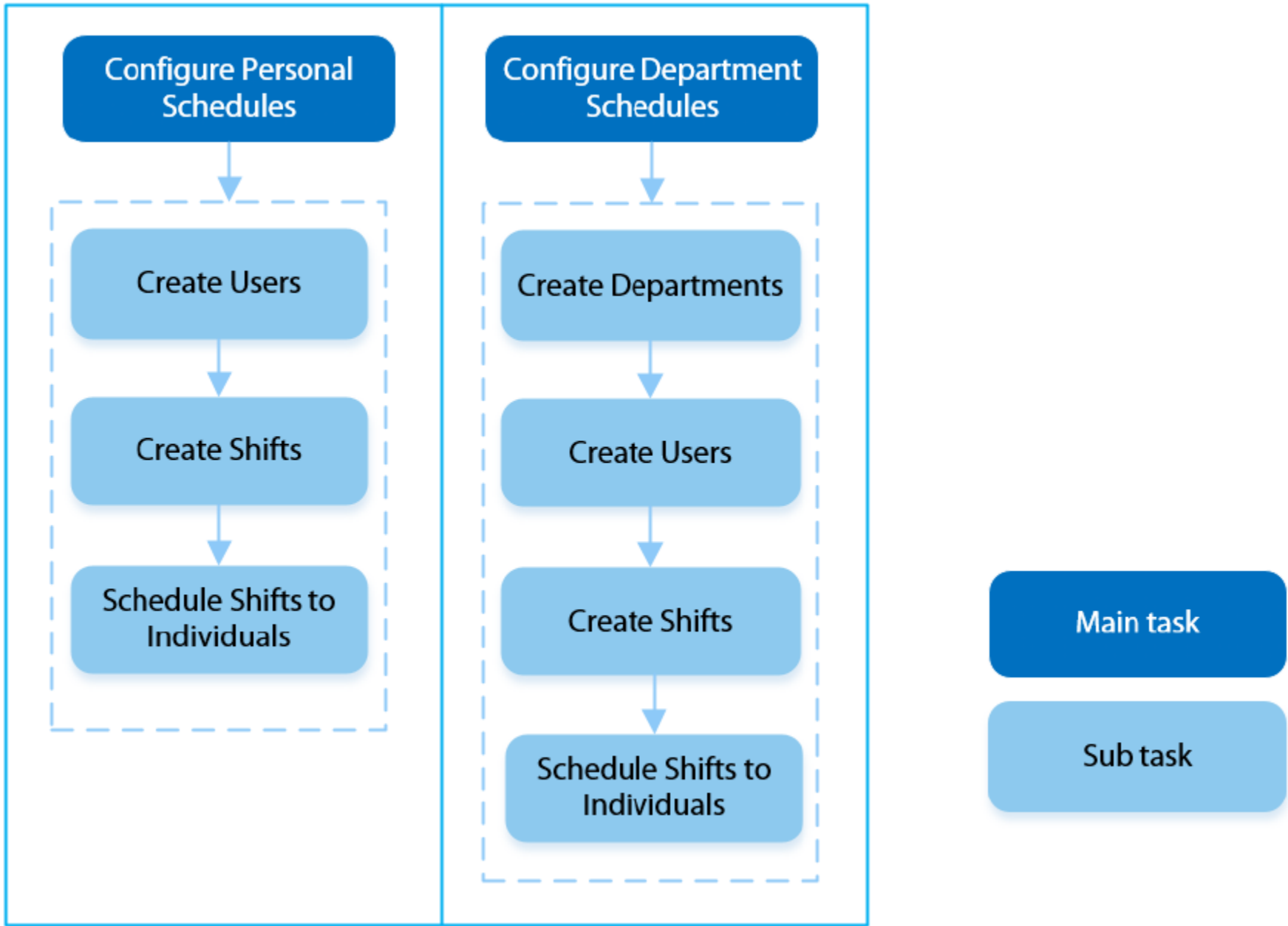
Справочная информация

Обратитесь к блок-схеме, чтобы настроить личные графики или графики отдела.



При настройке расписания не должно быть перекрывающихся периодов времени в один и тот же день и предыдущий или следующий день.

Рисунок 5-16 Настройка графиков работы



Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите "Дополнительно" > "Настройка посещаемости" > "Настройка расписания".

Шаг 3 Установите рабочие графики для отдельных сотрудников.

1. Коснитесь Личного расписания.

2. Выберите сотрудника в списке сотрудников.



После настройки режима расписания в качестве личного расписания при добавлении пользователя этот пользователь отображается в списке пользователей.

3. В календаре выберите день, а затем смену.



Вы можете установить графики работы только на текущий и следующий месяц.

0 означает перерыв.

от 1 до 24 указывается количество заранее определенных смен.

25 указывает на командировку.

26 указывает на отпуск.

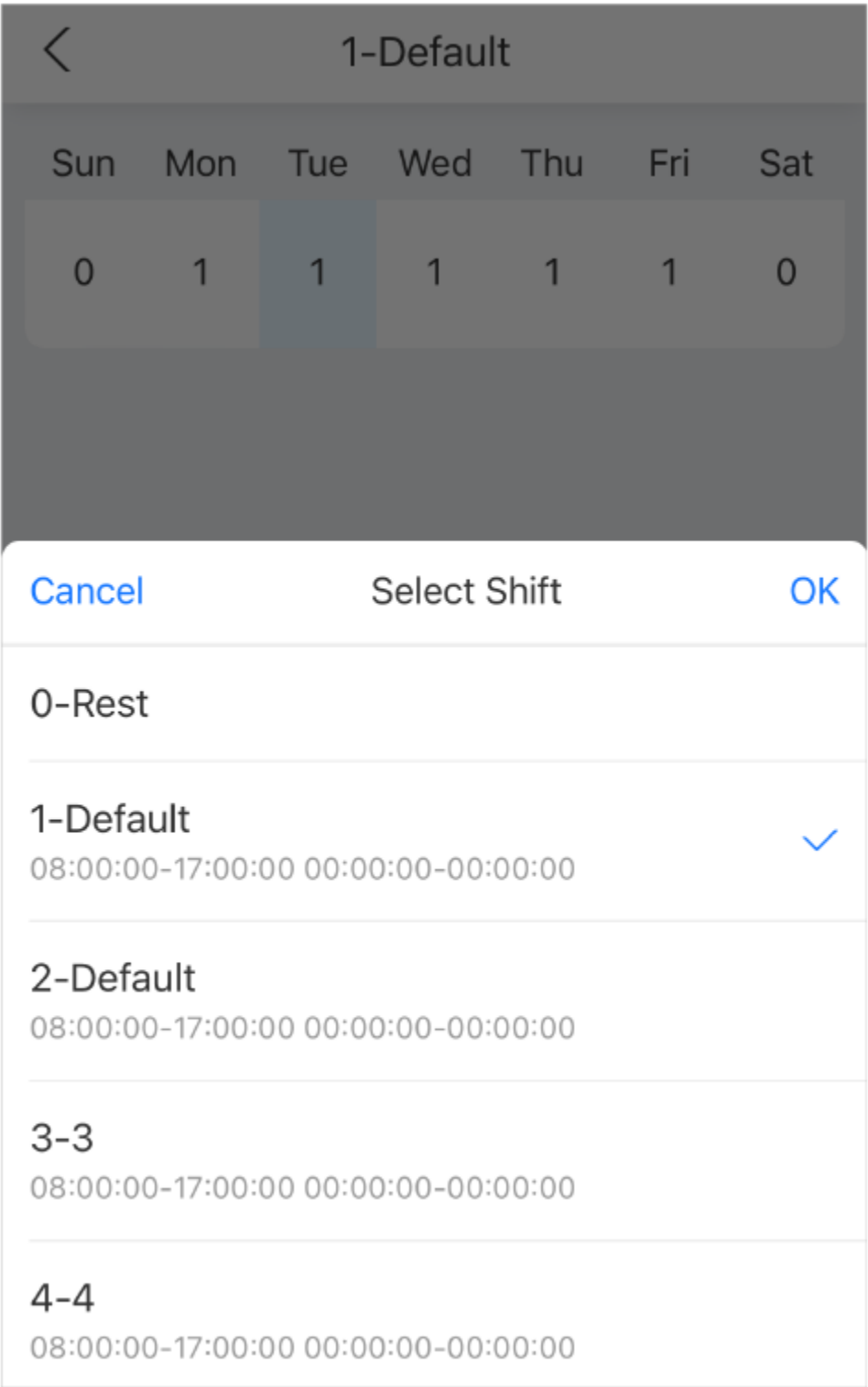
Шаг 4 Установите графики работ для отделов.

1. Коснитесь Расписание отдела.

2. Выберите отдел в списке отделов.

3. В календаре выберите день, а затем смену.

На рисунке 5-17 расписание отдела



0 указывает на отдых.

от 1 до 24 указывается количество заранее определенных смен.
25 указывает на командировку.
26 указывает на отпуск.



Установленный график работы рассчитан на неделю и будет применяться ко всем сотрудникам в отделе.

5.6.5 Настройка режимов посещаемости

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите "Дополнительно" > "Настройка посещаемости" > "Настройка посещаемости".
- Шаг 3 Включите локальную посещаемость, а затем настройте режим посещаемости.

Рисунок 5-18 "Конфигурация посещаемости".

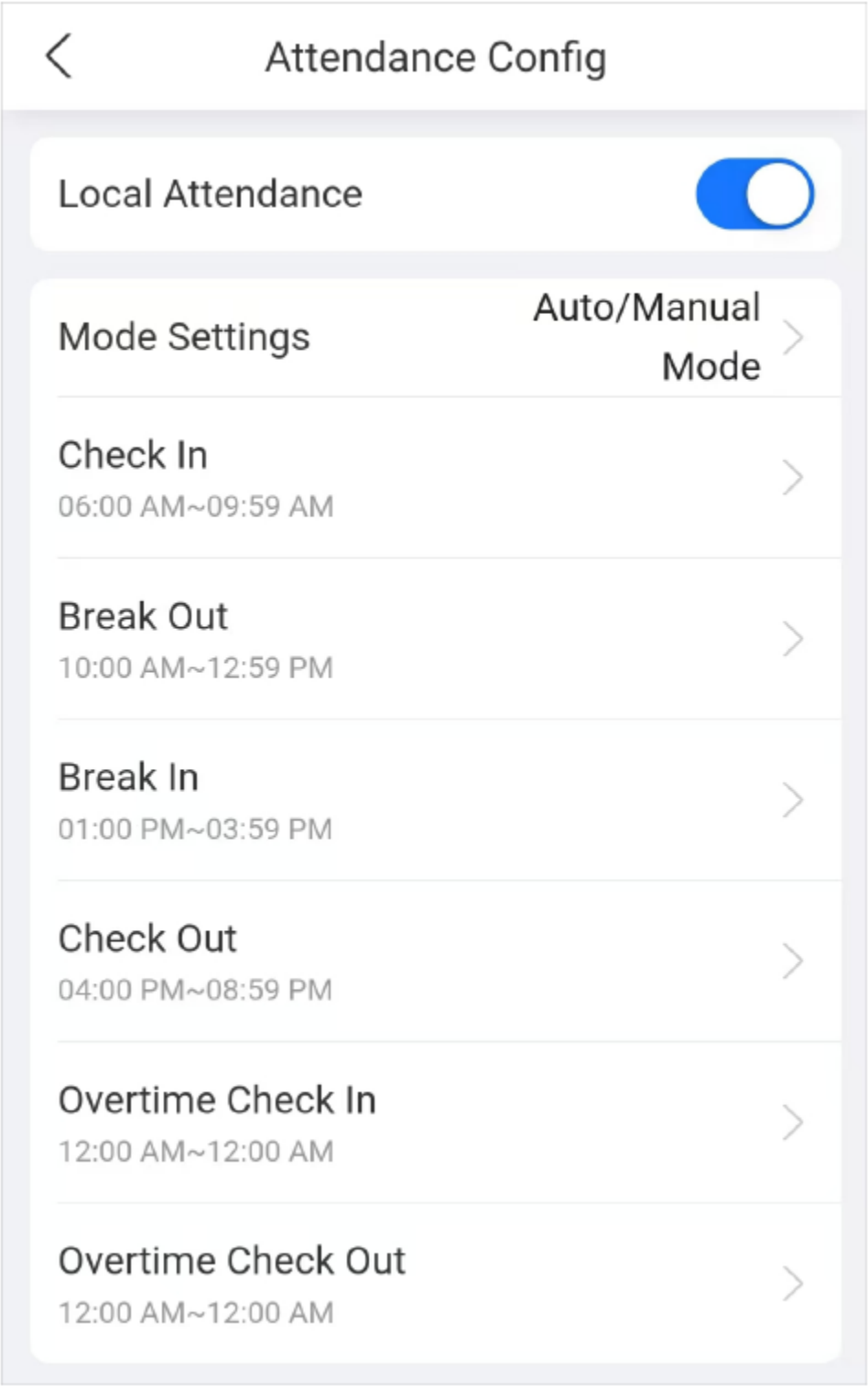


Таблица 5-5 Описание параметров посещаемости

Параметр Автоматический/Ручной режим	Описание Статус посещаемости отображается на экране автоматически после того, включаете или выключаете часы, но вы также можете вручную изменить св Регистрация заезда: Приходите, когда начинается ваш обычный рабочий д Перерыв: уходите, когда начинается ваш перерыв. Перерыв: приходите, когда заканчивается ваш перерыв. Расчетный час: заканчивается, когда заканчивается ваш обычный рабочий Зачет за сверхурочную работу: начинается период сверхурочной работы. Выезд на сверхурочную работу: выход по истечении периода сверхурочно
Автоматический режим	На экране автоматически отображается статус вашей посещаемости после пришли или вышли. Регистрация заезда: Приходите, когда начинается ваш обычный рабочий д Перерыв: уходите, когда начинается ваш перерыв. Перерыв: приходите, когда заканчивается ваш перерыв. Расчетный час: заканчивается, когда заканчивается ваш обычный рабочий Зачет за сверхурочную работу: начинается период сверхурочной работы. Выезд на сверхурочную работу: отбой по окончании периода сверхурочно
Ручной режим	Вручную выберите статус посещаемости при входе или выходе.
Фиксированный режим.	При включении или выключении часов на экране постоянно будет отображ статус посещаемости.

Шаг 4 Нажмите кнопку Применить.

5.7 Настройка контроля доступа

5.7.1 Настройка методов разблокировки

Для разблокировки двери можно использовать несколько методов разблокировки, таких как отпечаток пальца, карточка и пароль. Вы также можете объединить их, чтобы создать свой собственный метод разблокировки.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Нажмите Метод разблокировки в главном меню или выберите "Дополнительно"> "Контроль доступа"> "Разблокировать"
Метод.

Шаг 3 (Необязательно) Настройте комбинированный метод и метод разблокировки, а затем нажмите Применить.
- Комбинированный метод
 - Или: Используйте один из выбранных методов разблокировки, чтобы открыть дверь.
 - о И: Используйте все выбранные методы разблокировки, чтобы открыть дверь.Метод разблокировки
 - Выберите метод разблокировки в соответствии с поддерживаемыми возможностями устройства.
- 171

Рисунок 5-19 Способ разблокировки

Unlock Method

Combination Unlock

Combination Method

Or >

Unlock Method

Card, Fingerprint, Password, Bluetooth Card >

Apply

5.7.2 Настройка параметров контроля доступа

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Коснитесь параметров контроля доступа в главном меню или выберите "Дополнительно"> "Контроль доступа" > Параметры контроля доступа.
- Шаг 3 Настройте основные параметры для контроля доступа, а затем нажмите Применить.

Рисунок 5-20 Параметры контроля доступа (1)

Name	Door1
Door Status	Normal >
Verification Interval	0 s
Card Swiping Interval	0 s (0-86400)
Public Password	☐
Normally Open Period	
General Plan	Disabled >
Holiday Plan	Disabled >
Normally Closed Period	
General Plan	Disabled >
Holiday Plan	Disabled >

Рис. 5-21 Параметры контроля доступа (2)

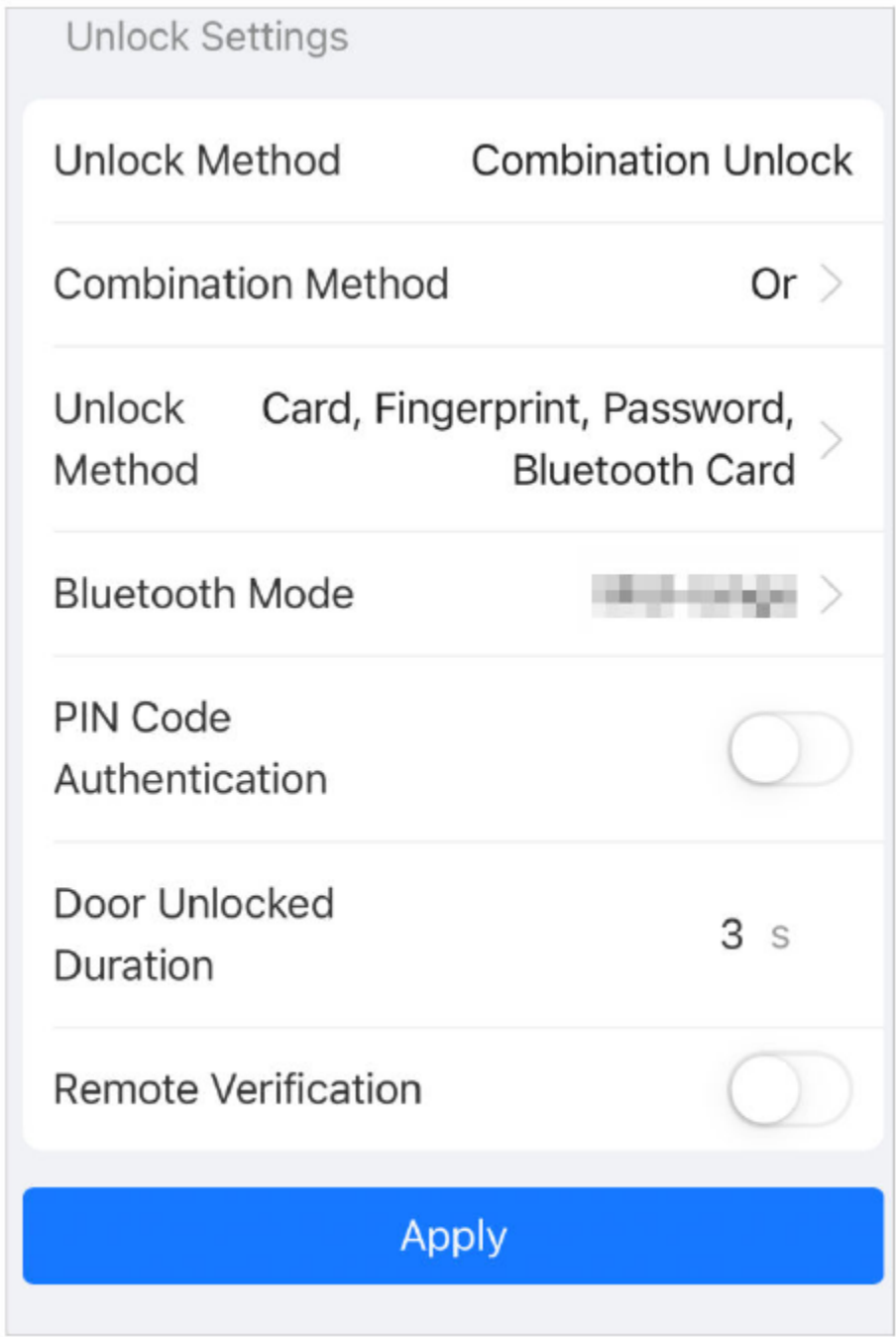


Таблица 5-6 Описание параметров контроля доступа

Параметр	Описание
Имя	Название двери.
Основные настройкиСостояние двери	Установите состояние двери. Обычный: дверь будет отперта и заблокирована в соответствии с вашими настройками. Всегда открыта: дверь остается незапертой все время. Всегда закрыто: дверь остается запертой все время .
Интервал проверки	Если вы подтвердите свою личность несколько раз в течение установленного периода, только самая ранняя проверка будет считаться действительной, и дверь не откроется после второй или более поздней проверки. С момента, когда дверь не открывается, вы должны дождаться установленного для проверки временного интервала, прежде чем пытаться подтвердить свою личность снова.

Параметр		Описание
	Интервал между перемещениями карты	Для первой проверки с помощью карты, вы можете использовать обычный образ отпереть дверь. Если вы не сможете отпереть дверь или карта не будет считываться, будут созданы записи. В течение периода времени, если вы снова попытаетесь отпереть дверь или карта не будет считываться, записи не будут сгенерированы. Идентификация по истечении периода времени. Интервал считывания карты или интервалом проверки.
	Общедоступный пароль	После включения общедоступного пароля. Вы можете использовать ввод идентификатора пользователя или общедоступный пароль.
Период работы в обычном режиме	Общий план / Праздничный план	Выбрав "Обычный", вы можете выбрать шаблон из выпадающего списка. Если дверь открыта или закрыта в течение периода времени, настройка общих планов и планов. "4.7.4 Настройка периодов". Когда нормально открытый период нормально закрытым периодом имеет приоритет над нормальным. Когда общий план конфликтует с планом, праздничный план имеет приоритет над общим планом.
	Обычно закрытый период	
Настройки разблокировки	Метод разблокировки	Комбинированная разблокировка. Дополнительные сведения о настройке методов разблокировки.
	Комбинированный метод	Или: Используйте один из выбранных методов, чтобы открыть дверь. Или: Используйте все выбранные методы, чтобы открыть дверь.
	Метод разблокировки	Методы разблокировки могут различаться в зависимости от модели продукта.
	Режим Bluebooth	Выберите режим Bluebooth в настройках. Эта функция отображается только в Метод разблокировки.

Параметр	Описание
Аутентификация по PIN-коду	Когда включена аутентификация по PIN-коду, вы можете открыть дверь, используя только пароль. Вам не нужно вводить идентификатор пользователя, если эта функция включена. Удаленная проверка не поддерживается.
Дверь разблокирована Продолжительность действия	После предоставления человеку доступа, дверь будет оставаться незапертой в течение определенного времени, необходимого для их прохода. Это время составляет от 0,2 до 600 секунд.
Удаленная проверка.	Откройте дверь удаленно.

Шаг 4 Нажмите Применить.

5.7.3 Настройка аварийных сигналов

Аварийный сигнал будет срабатывать при возникновении аварийного события доступа.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Дополнительно> Контроль доступа> Аварийный сигнал.
- Шаг 3 (Необязательно) Выберите дверной канал.

Если вы выбрали модуль расширения замка в качестве внешнего устройства через Настройки связи> Настройки RS-485 на контроллере доступа, вы можете выбрать канал здесь.

Шаг 4 Настройте параметры будильника, а затем нажмите Применить.

Рисунок 5-22 Настройки сигнализации

Duress Alarm

☒

Anti-passback

☐

Door Detector

☒

Door Detector Status

NO >

Intrusion Alarm

☐

Unlock Timeout Alarm

☐

Unlock Timeout

60 s

Excessive Attempts Alarm

☒

Apply

Таблица 5-7 Описание параметров сигнализации

Параметр	Описание
Сигнализация о Принуждении	Сигнал тревоги срабатывает, когда для отпирания двери используется карта или отпечаток пальца принудительного доступа.

Параметр	Описание
Защита от обратного доступа	Пользователям необходимо подтвердить свою личность как для входа, так и для выхода. В противном случае сработает сигнализация. Это помогает предотвратить кражу карты. Владелец карты не сможет передать карту доступа обратно другому пользователю для получения доступа. Когда защита от обратного доступа включена, пользователь должен покинуть охраняемую зону через считывающее устройство. Если система разрешит другой вход, защита от обратного доступа будет отключена. Если человек входит после авторизации и выходит без повторной авторизации, при повторной попытке входа сработает аварийный сигнал, и в то же время доступ будет запрещен. Если человек входит без авторизации и выходит после повторной авторизации, при повторной попытке входа сработает аварийный сигнал, и в то же время доступ будет запрещен. Если устройство может подключить только один замок, проверка на внутреннем считывателе означает направление входа, а проверка на внешнем считывателе карт по умолчанию означает направление выхода. Если устройство поддерживает настройку на платформе управления, настройка должна быть выполнена.
Дверной извещатель	С помощью дверного извещателя, подключенного к вашему устройству, можно срабатывать сигнализация при неправильном открытии или закрытии двери. Дверной детектор бывает двух типов, включая детектор с ЧПУ и детектор без детектора. NC: датчик находится в замкнутом положении, когда дверь или окно закрыты. NO: Разомкнутая цепь возникает, когда окно или дверь фактически закрыты.
Сигнализация о вторжении	Если дверь открывается нештатно, сработает сигнализация о вторжении, которая будет действовать до тех пор, пока дверь не будет закрыта. Дверной детектор и система вторжения должны быть включены одновременно.
Сигнализация о тайм-ауте разблокировки Тайм-аут разблокировки	Когда дверь остается незапертой дольше, чем заданный тайм-аут, срабатывает сигнализация тайм-аута двери, которая действует в течение заданного времени. Дверной детектор и функция тайм-аута двери должны быть включены одновременно.
Сигнал тревоги о чрезмерных попытках	Если 5 раз подряд в течение 60 секунд будет использован неправильный пароль или карта, будет срабатывать сигнал тревоги о чрезмерном использовании незапертой двери.

5.7.4 Настройка привязки сигналов тревоги (необязательно)

Вы можете настроить привязку сигналов тревоги.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Дополнительно> Контроль доступа> Настройка привязки сигналов тревоги.
- Шаг 3 Выберите зону для настройки сигнализации.

Рисунок 5-23 Привязка сигнализации

Alarm-in Port1

NameZone1

Alarm Input TypeNO >

Link Fire Safety Control☐

Alarm-out Port☐

Duration30 s

Alarm Output Channel1 >

Access Control Linkage☐

Linkage ModeWeak Execution >

When the heat alarm signal disappears, the door will automatically return to the normal authentication mode.

Local LockNO >

External LockNO >

- Шаг 4 Создайте название для зоны сигнализации.
- Шаг 5 Включите Link Fire Safety Control и выберите тип устройства ввода сигнала тревоги.

NC: вход сигнала тревоги находится в нормально замкнутом состоянии (NC), когда сигнал тревоги не был сработал. Размыкание нормально замкнутой цепи приводит к срабатыванию сигнализации.

НЕТ: устройство ввода сигнала тревоги находится в состоянии нормально разомкнутой цепи, когда сработал сигнал тревоги не было срабатывания. Замыкание цепи приводит к срабатыванию сигнализации.
- Шаг 6 Если вы хотите подключить контроль доступа при срабатывании пожарной сигнализации, включите контроль доступа **Подключение**.



Шаг 7 Эта функция вступает в силу только после включения управления пожарной безопасностью Link. Выберите режим подключения.

Надежное выполнение: когда сигнал пожарной сигнализации исчезает, дверь остается в текущем состоянии Статус. Пожалуйста, вручную измените предыдущие настройки состояния двери, если хотите.

Слабый режим работы
Выполнение: когда сигнал пожарной сигнализации исчезает, дверь автоматически возвращается к своему предыдущему состоянию двери.

Шаг 8 Выберите тип локального замка и внешнего замка.

НЕТ: дверь автоматически открывается при срабатывании пожарной сигнализации.

НС: дверь автоматически закрывается при срабатывании пожарной сигнализации.

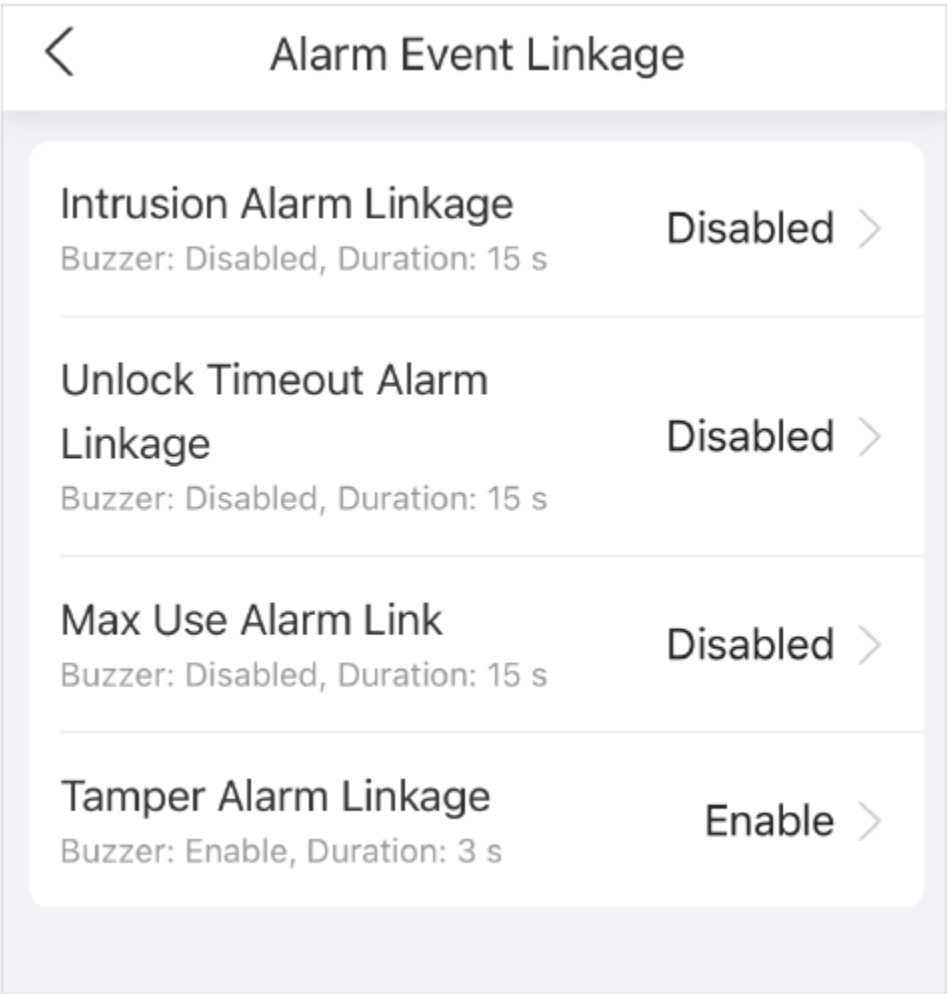
Шаг 9 Нажмите ОК.

5.7.5 Настройка привязки аварийных событий

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Дополнительно> Управление доступом> Привязка аварийных событий.

Рисунок 5-24 Привязка аварийных событий



- Шаг 3 Коснитесь привязки, чтобы настроить привязку сигнализации, а затем нажмите ОК.

Таблица 5-8 Привязка событий будильника

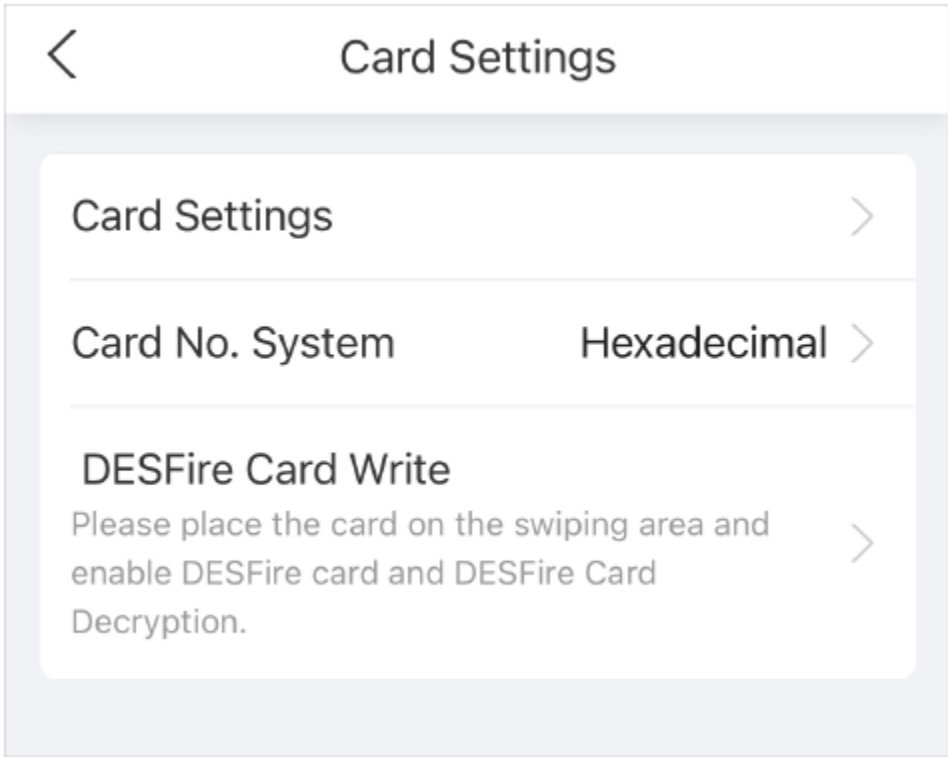
Параметр	Описание
Система Сигнализации о вторжении	Если дверь открывается нештатно, сработает звуковой сигнал: звуковой сигнал звучит п... можете настроить продолжительность сип... Выходной сигнал связи: внешнее устройст... при срабатывании сигнализации о вторже... .
Сигнализация тайм-аута разблокировки Привязка	Когда дверь остается незапертой дольше, ... продолжительность, срабатывает сигнали... заданного времени. Звуковой сигнал: звуковой сигнал звучит п... срабатывании сигнала ожидания разблоки... закроется. о Пока дверь не закроется: звук будильник... закрыта. Пользовательское время: вы можете настр... Локальный вывод сигнала тревоги: внешне... при срабатывании сигнала ожидания разб... пользовательского времени и до тех пор, п... Пока дверь не закроется: сигнал тревоги п... закрыта. о Пользовательское время: вы можете настр...
Максимальное использование ссылки на сигнал тревоги	Если 5 раз подряд в течение 60 секунд будет использован неправильный п... будет действовать в течение определенно... Звуковой сигнал: звуковой сигнал звучит п... . Вы можете настроить продолжительность... Выходной сигнал связи: внешнее устройст... при срабатывании сигнала ожидания разб... продолжительность сигнала тревоги.
Подключение сигнализации о несанкционированном вскрытии	Сигнализация о несанкционированном вскр... повредить устройство. Звуковой сигнал: звуковой сигнал звучит п... можете настроить продолжительность сип... Выходной сигнал связи: внешнее устройст... при срабатывании сигнализации о несанкп... .

5.7.6 Настройка параметров карты

Процедура

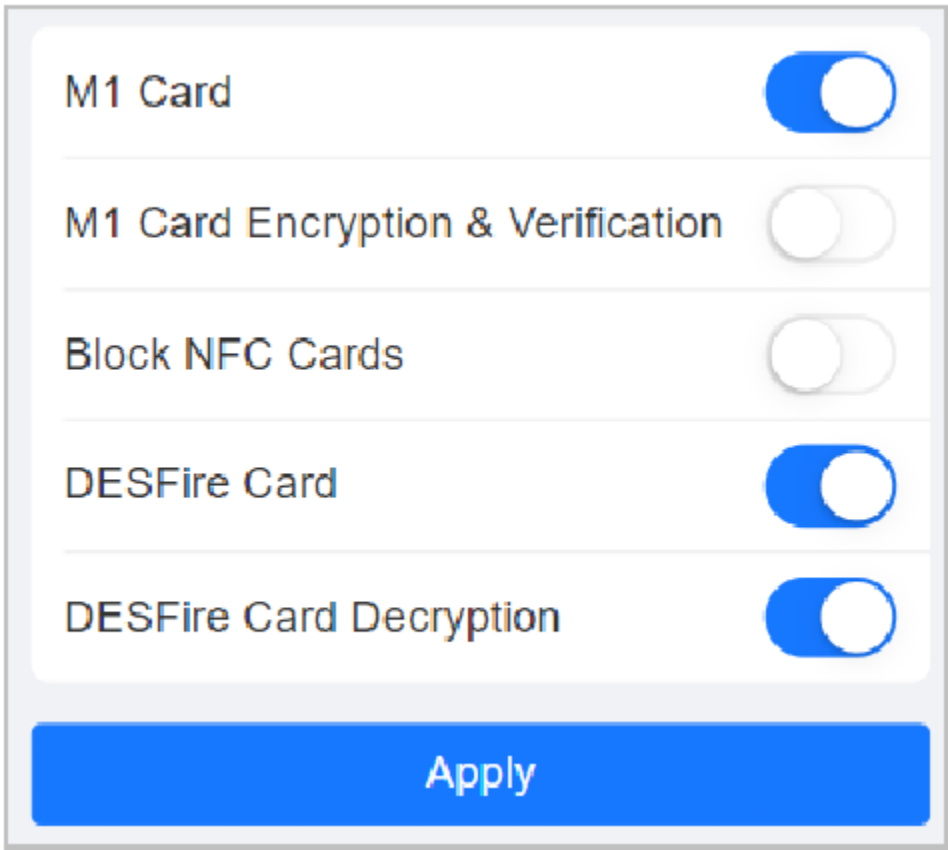
- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите "Дополнительно"> "Контроль доступа"> "Настройки карты".

Рисунок 5-25 Настройки карты



Шаг 3 Коснитесь Настроек карты, настройте параметры карты, а затем нажмите Применить.

Рисунок 5-26 Параметры карты



Описание параметров карты в таблице 5-9

Параметр	Описание
Карта M1	Карта M1 может быть считана, когда эта функция включена. Эта функция доступна только на некоторых моделях.
Шифрование и проверка карты M1	Когда эта функция включена, можно прочитать только зашифрованную карту IC. Убедитесь, что включена карта M1. Убедитесь, что включена карта M1.

Параметр	Описание
Блокируйте NFC-карты.	Предотвратите разблокировку с помощью дублированной NFC-карты после NFC-функции. Эта функция доступна только на моделях, поддерживающих карты IC . Убедитесь, что включена карта M1. Функция NFC доступна только на некоторых моделях телефонов.
Карта удаления огня	Устройство может считывать номер карты Desfire card, когда эта функция включена. При этом устройство может считывать номер карты Desfire card, когда эта функция включена. Функция доступна только на моделях, поддерживающих IC карты. Функция доступна только на моделях, поддерживающих IC карты. Поддерживает только шестнадцатеричный формат. Поддерживает только шестнадцатеричный формат.
Дешифрование карты Desfire	Информация на карте Desfire может быть прочитана при включении Карта Desfire и дешифрование карты Desfire включены при включении Это то же самое время. Функция доступна только на моделях, поддерживающих карты IC. Функция доступна только на моделях, поддерживающих IC карты. Убедитесь, что включена функция Desfire card. Убедитесь, что включена функция Desfire card.

Шаг 4 Нажмите "Номер карты". Система, выберите формат, а затем нажмите Применить.

Выберите десятичный или шестнадцатеричный формат для номера карты, если карта Wiegand устройство чтения подключено. Система ввода номера карты одинакова как для ввода номера карты, так и для вывода.

Шаг 5 Нажмите **Отменить запись с карты.**

Приложите карту к считывающему устройству, введите номер карты, а затем нажмите кнопку "Запись", чтобы записать карту номер карты.



Функция Desfire card и функция дешифрования Desfire card должны быть включены.

Поддерживает только шестнадцатеричный формат.

Поддерживает до 8 символов.

5.7.7 Настройка параметров экрана

Настройте период постоянного включения экрана и информацию об устройстве, которая отображается на экране когда тема настроена на общий режим.

Процедура

Шаг 1 Войдите на веб-страницу.

Шаг 2 Выберите "Дополнительно"> "Контроль доступа"> "Настройки экрана".

Шаг 3 Настройте постоянно включенный экран.

Постоянно включенная конфигурация: экран всегда включен в течение настроенного периода времени.

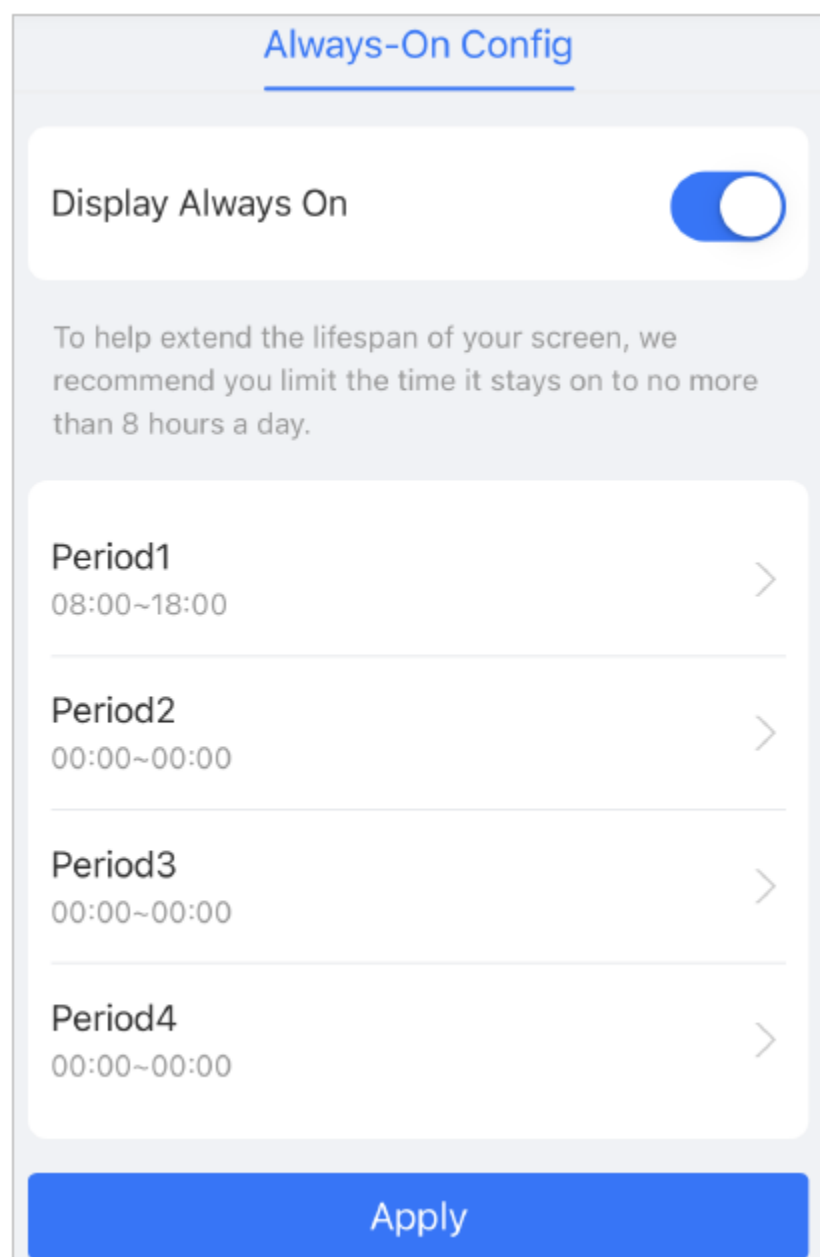
- Нажмите "Всегда включенная настройка".

2. Включите функцию и затем нажмите "ОК".
3. Коснитесь периода, настройте время начала и время окончания, а затем нажмите "ОК".
4. Нажмите "Применить".



Чтобы продлить срок службы вашего экрана, мы рекомендуем ограничить время его включения не более чем 8 часами в день.

Рисунок 5-27 Дисплей всегда включен



5.8 Настройки связи

5.8.1 Настройка TCP / IP

Вам необходимо настроить IP-адрес устройства, чтобы убедиться, что оно может взаимодействовать с другими устройствами.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите "Дополнительно" > "Настройки связи"> "Настройки сети"> "TCP / IP".
- Шаг 3 Настройте параметры, а затем нажмите "Применить".

Рисунок 5-28 TCP/IP

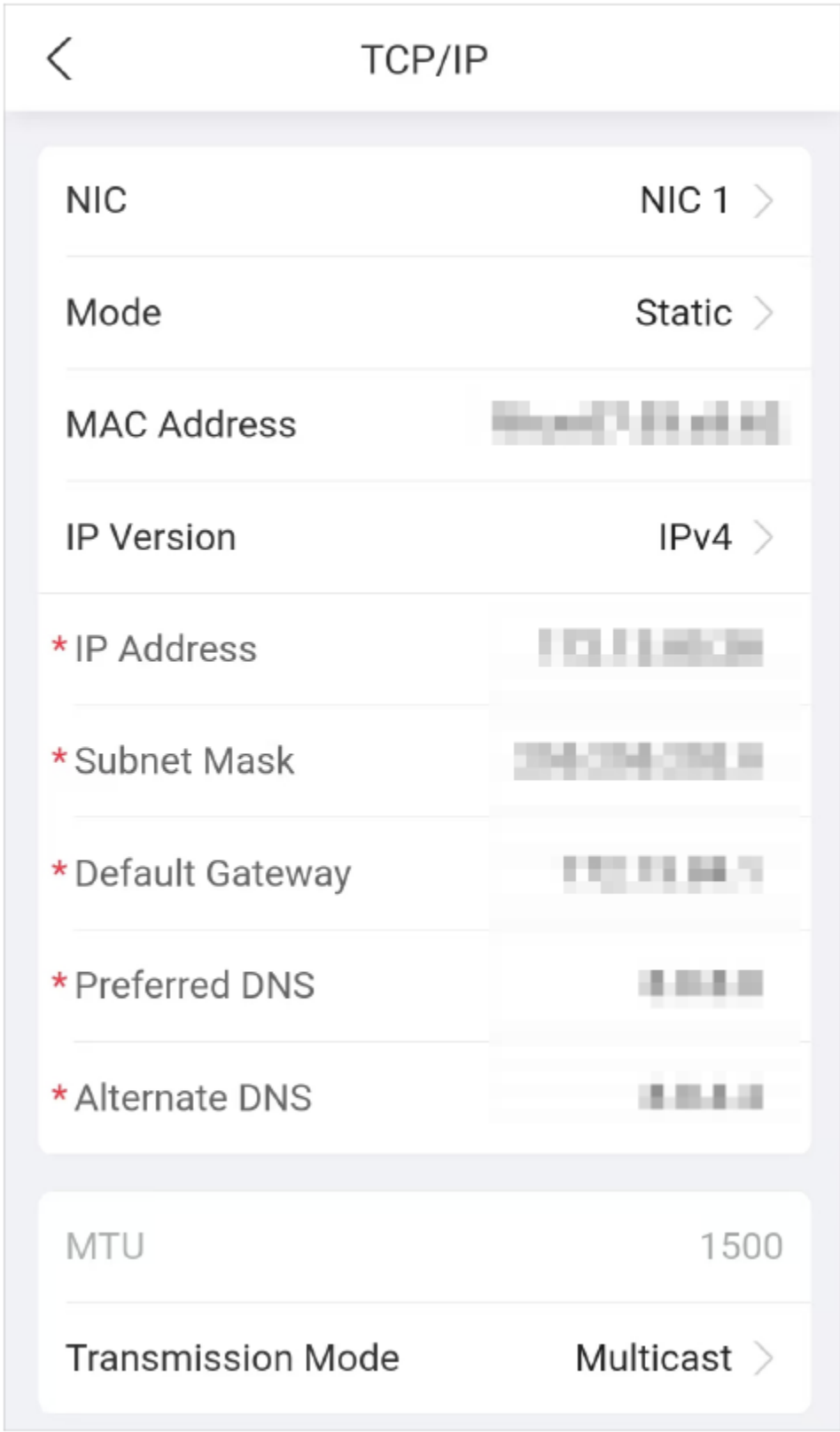


Таблица 5-10 Описание TCP/IP

Параметр	Описание
Режим	Статический: вручную введите IP-адрес, маску подсети и шлюз. DHCP: Расшифровывается как Dynamic Host Configuration Protocol. Когда DHCP включен, устройству будет автоматически назначен IP-адрес, маска подсети и шлюз.
MAC-адрес	MAC-адрес устройства.
Версия IP	IPv4 или IPv6.
IP-адрес, Маска подсети	Если вы установили статический режим, настройте IP-адрес, маску подсети и шлюз.
Шлюз по умолчанию	IPv6-адрес представлен в шестнадцатеричном формате. Версии IPv6 не требуют установки масок подсети. IP-адрес и шлюз по умолчанию должны находиться в одном и том же сегменте сети.

Параметр	Описание
Предпочтительный DNS	Установите IP-адрес предпочтительного DNS-сервера.
Альтернативный DNS	Установите IP-адрес альтернативного DNS-сервера.
MTU	MTU (Максимальная единица передачи) относится к максимальному размеру данных, которые могут быть переданы в одном сетевом пакете в компьютерных сетях. По умолчанию он равен 1500.

5.8.2 Настройка Wi-Fi

Процедура

- Шаг 1

Войдите на веб-страницу.
- Шаг 2

Выберите Дополнительно> Настройки связи> Wi-Fi.
- Шаг 3

Включите Wi-Fi.

Отображаются все доступные Wi-Fi.



Функция

Wi-Fi доступна на некоторых моделях.

Функция

Wi-Fi и точка доступа Wi-Fi не могут быть включены одновременно.

- Шаг 4

Коснитесь Wi-Fi, а затем введите пароль.
- Wi-Fi подключен.

Связанные операции

- DHCP: Выберите режим DHCP и нажмите Применить, устройству автоматически будет назначен Wi-Fi адрес.
- Статический: Выберите статический режим, вручную введите адрес Wi-Fi, а затем нажмите Применить, устройство подключится к Wi-Fi.

5.8.3 Настройка точки доступа Wi-Fi



The

Функция Wi-Fi доступна на некоторых моделях.

The

Wi-Fi и точка доступа Wi-Fi не могут быть включены одновременно.

Процедура

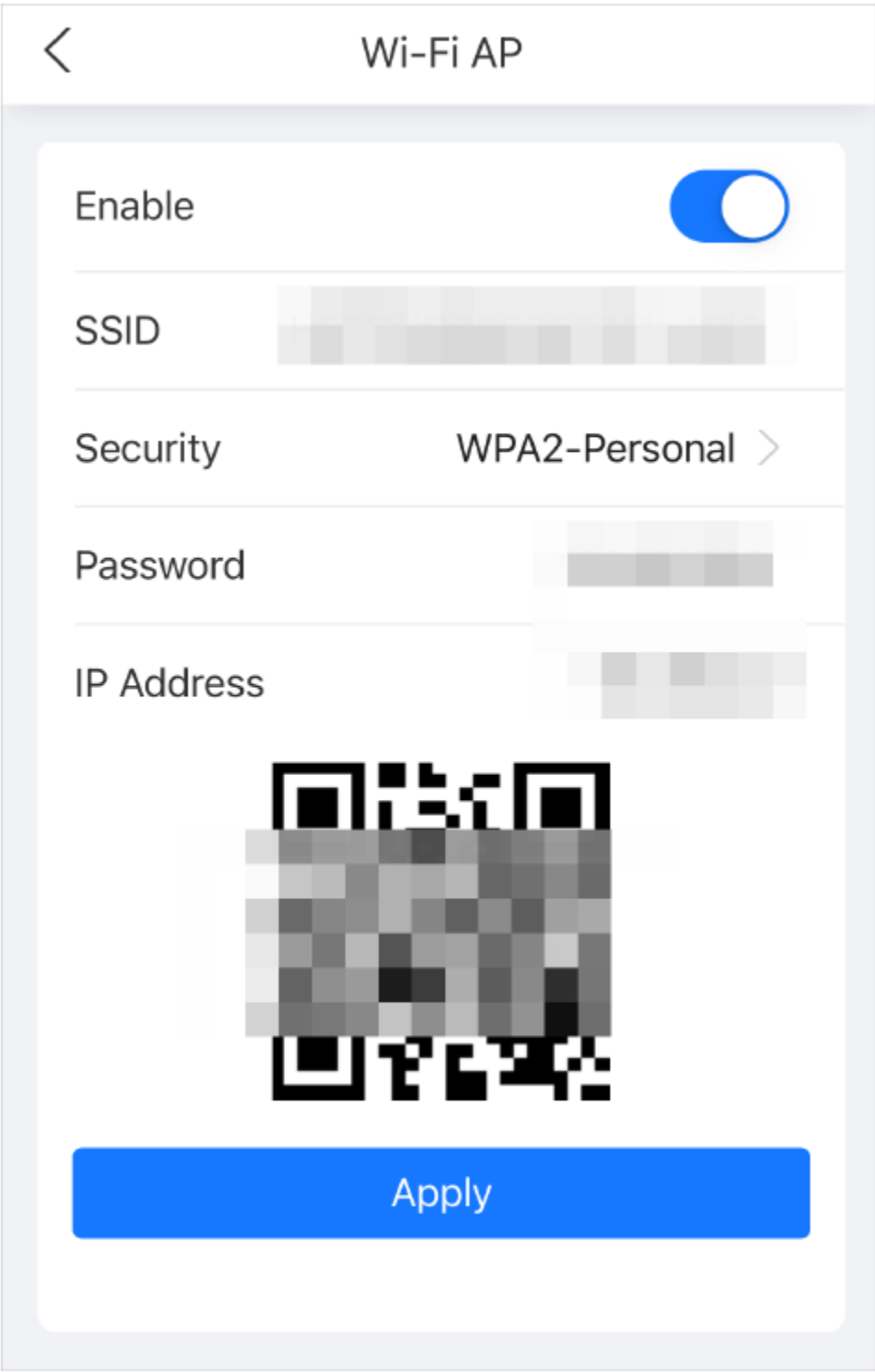
- Шаг 1

Войдите на веб-страницу.
- Шаг 2

Выберите "Дополнительно" > "Настройки связи"> "Точка доступа Wi-Fi".
- Шаг 3

Включите функцию, а затем нажмите "Применить".

Рисунок 5-29 Точка доступа Wi-Fi



5.8.4 Настройка облачного сервиса

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 **Выберите "Дополнительно" > "Настройки связи" > "Облачный сервис".**
- Шаг 3 Включите функцию облачного сервиса.
Облачный сервис переходит в оперативный режим, если подключены P2P и PaaS.
- Шаг 4 Нажмите Применить.

5.8.5 Настройка автоматической регистрации

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 **Выберите Дополнительно> Настройки сети> Автоматическая регистрация.**
- Шаг 3 Включите функцию автоматической регистрации, настройте параметры, а затем нажмите Применить.

Рисунок 5-30 Автоматическая регистрация

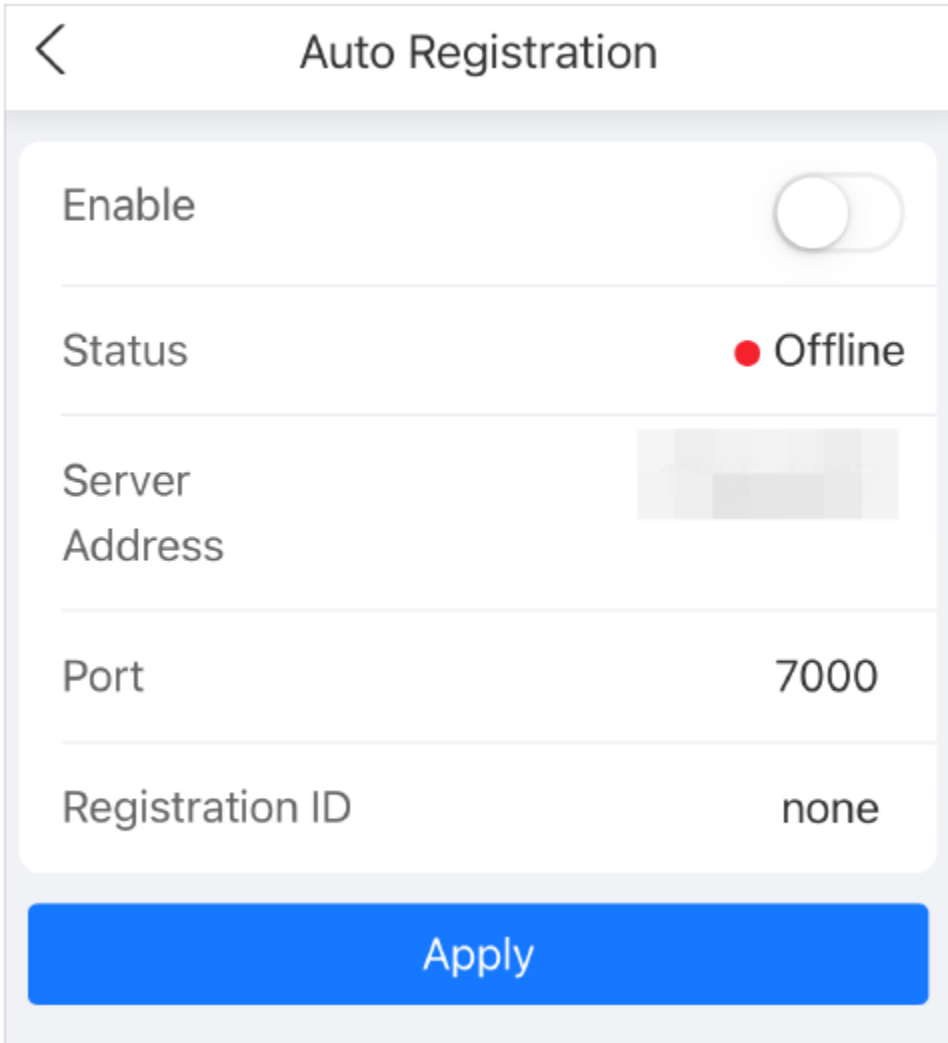


Таблица 5-11 Описание автоматической регистрации

Параметр	Описание
Статус	Отображает состояние подключения при автоматической регистрации.
Адрес сервера	IP-адрес или доменное имя сервера.
Порт	Порт сервера, который используется для автоматической регистрации.
Регистрационный идентификатор	Регистрационный идентификатор (определяемый пользователем) устройства. Управление путем ввода регистрационного идентификатора на платформе.

5.8.6 Настройка режима

Войдите на веб-страницу и выберите Настройки связи > Настройки режима.

Режим чтения карт

Выберите режим в качестве устройства чтения карт. Устройство выполняет функцию считывателя карт, подключенного извне к устройству доступа контроллер управления. Оно не выполняет аутентификацию, но напрямую передает управление доступом информация (например, карта, пароль, отпечаток пальца) передается контроллеру контроля доступа, который затем проверяет подлинность и отпирает дверь.

Рисунок 5-31 Режим считывания карт памяти

Mode

Card Reader >

RS-485 Settings

Baud Rate

9600 >

Data Bit

8 >

Stop Bit

1 >

Parity Code

None >

Wiegand Settings

Wiegand Output Type

Wiegand 34 >

Pulse Width (μs)

200

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Pulse Interval (μs)

1000

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Apply

Режим контроллера доступа

Установите режим в качестве контроллера доступа.

Рисунок 5-32 Режим контроллера доступа

External Device

Access Controller >

Access controller: This device acts as a card reader, and connects to an access controller, which manages the opening of doors.

Baud Rate

9600 >

Data Bit

8 >

Stop Bit

1 >

Parity Code

None >

Output Data Type

Card Number >

Wiegand Settings

Wiegand Settings

Wiegand Input >

Card No. Inversion

☒

Таблица 5-12 Описание RS-485

Внешнее устройство	Описание
Контроллер доступа	Выберите контроллер доступа, когда устройство функционирует как устройство считывания карт и отправляет данные на другие внешние контроллеры управления доступом. Тип выходных данных: Номер карты: выводит данные на основе номера карты, когда пользователь проводит пальцем по карте, чтобы разблокировать дверь; выводит данные номера карты пользователя, когда он использует другие методы разблокировки. ID: выводит данные на основе идентификатора пользователя. При успешной аутентификации соответствующая информация передается контроллеру доступа. В этом случае отображаемый результат аутентификации является результатом аутентификации контроллера доступа. Когда аутентификация завершается неудачно, соответствующая информация передается контроллеру доступа, и результат аутентификации отображается как сбой.
Устройство чтения карт	Устройство подключается к устройству считывания карт извне и передает информацию о карте контроля доступа контроллеру доступа или платформе управления.
Устройство считывания карт (OSDP)	Устройство подключается извне к считывателю карт OSDP и передает информацию о карте контроля доступа контроллеру доступа или платформе управления.
Дверной модуль безопасности.	Кнопка выхода из двери, замок и противопожарная система не действуют, если включен модуль безопасности. Поддерживает аутентификацию по лицу, карте, отпечатку пальца, паролю и другим методам для управления модулем разблокировки дверей. Поддерживает разблокировку с помощью подключенного извне кард-ридера или кнопки открытия, подключенной к модулю безопасности системы управления. Дистанционное разблокирование дверного замка, подключенного извне к модулю безопасности двери не поддерживается.
Модуль расширения замка.	Когда контроллер доступа подключен к модулю расширения external lock, если вы выберете Модуль расширения Lock, локальная блокировка будет разблокирована после подтверждения идентификации на локальном устройстве. Дополнительная блокировка будет разблокирована после подтверждения идентификации во внешнем считывателе карт. После того, как вы выберете Модуль расширения Блокировки, вы можете настроить параметры на странице Параметров контроля доступа и сигнализации на веб-странице контроллера доступа.

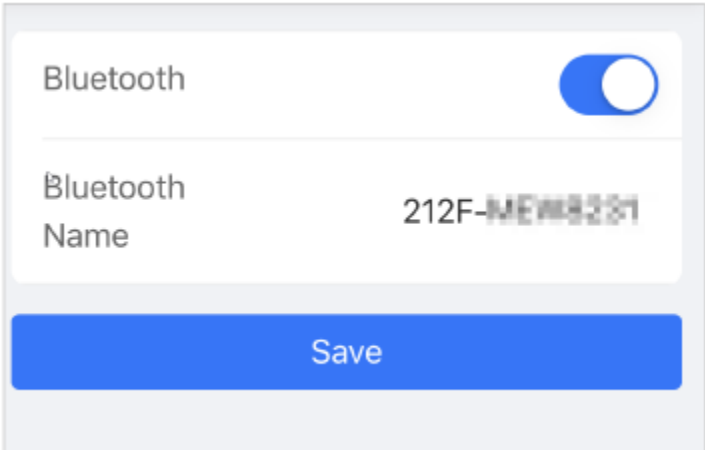
Параметр		Описание
Настройки Wiegand		- При подключении внешнего устройства чтения карт выберите Wiegand Входной сигнал. - Когда устройство функционирует как устройство чтения карт памяти, подключить его к другому контроллеру доступа и выбрать Wiegand Output Config.
Вход Wiegand	Номер карты инверсия	Если последовательность номеров карт, полученная с помощью не совпадает с фактической последовательностью номеров карт устройствами сторонних производителей, включите эту функцию.
Вывод Wiegand	Тип вывода Wiegand	Длина в битах номеров карт или ID, которые устройство может р и вывести. Виганд 26: считывает 3 байта или 6 цифр. Виганд 34: считывает 4 байта или 8 цифр. Wiegand 66: считывает 8 байт или 16 цифр.
	Ширина импульса Интервал импульсов	Настройте ширину импульса и интервал для вывода wiegand.
	Введите выходные данные	Выберите формат Wiegand для считывания номеров карт или идентификатор пользователя: выводит данные на основе идентифи Карта: выводит данные на основе первого номера карты пользов
	Формат Wiegand	Если тип выходных данных задан как ID, вы можете выбрать десяти шестнадцатеричный форматы вывода.

5.8.7 Настройка Bluetooth

Процедура

- Шаг 1
- Войдите на веб-страницу.
- Шаг 2
- Выберите Связь> Настройки Bluetooth.**
- Шаг 3
- Включите или выключите Bluetooth.

Рисунок 5-33 Bluetooth



- Шаг 4
- Нажмите Сохранить.

Результаты

Вы можете разблокировать дверь по Bluetooth через приложение DMSS. Подробнее см. в разделе "3.6.3 Bluetooth".

5.9 Настройка звуковых подсказок

Установите звуковые подсказки во время проверки личности.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите "Дополнительно" > "Настройка аудио и видео" > "Аудио".
- Шаг 3 Настройте параметры звука, а затем нажмите "Применить".

Рисунок 5-34 Настройка параметров звука

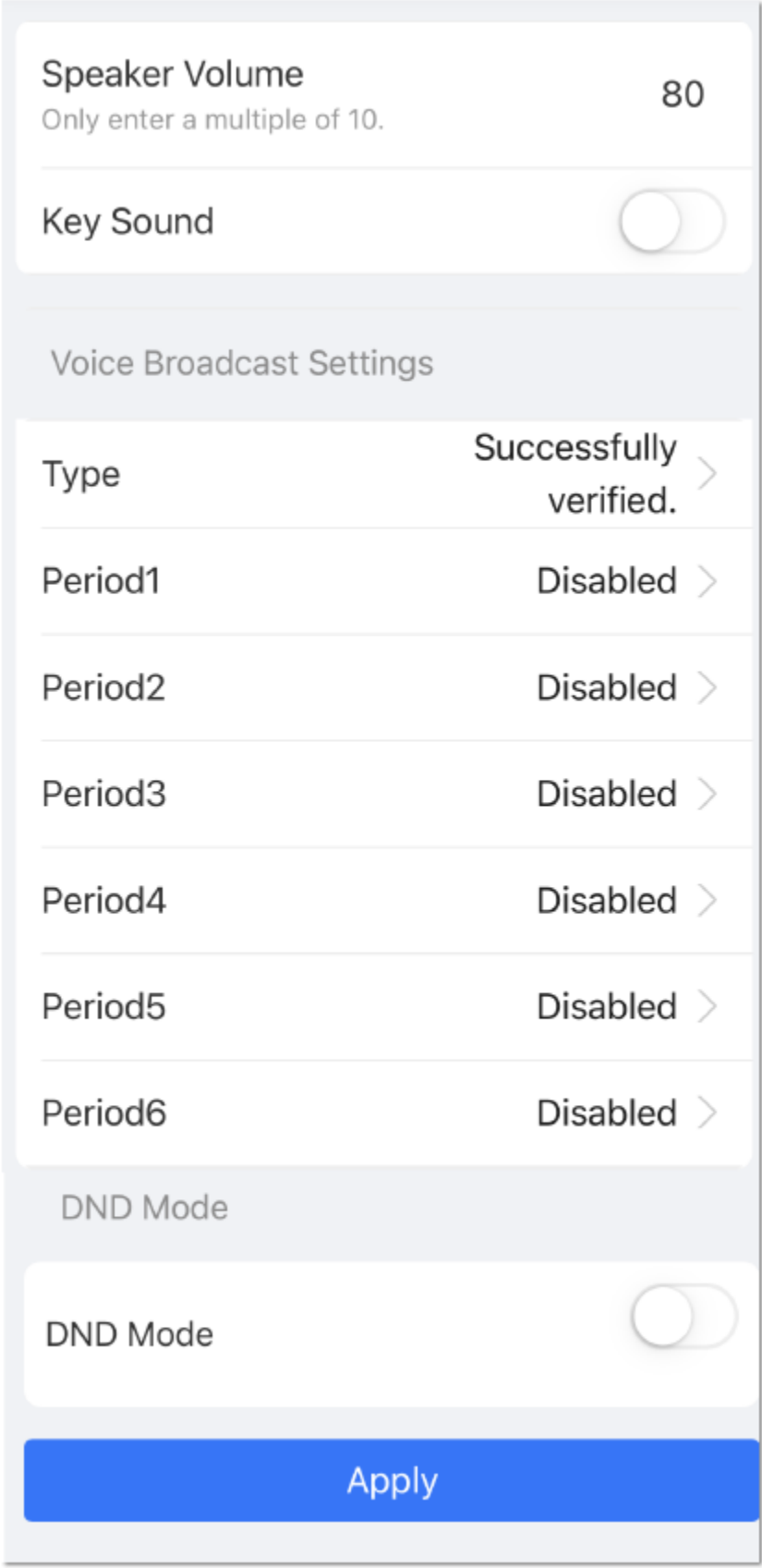


Таблица 5-14 Описание параметров

Параметры	Описание
Динамик	Установите громкость динамика.
Звук касания экрана	Когда эта функция включена, устройства с сенсорным экраном будут воспроизводить звук касания, а устройства без сенсорного экрана - звук нажатия мышью.
Коллекция аудио.	Если эта функция включена, звук с микрофона устройства будет записываться во время просмотра в режиме реального времени.

Параметры	Описание
Режим DND	Отсутствие голосовых подсказок в течение установленного времени при подтверждении своей личности на устройстве. Можно настроить до 4 периодов.

5.10 Просмотр журналов

Просматривайте журналы, такие как системные журналы, записи разблокировки и журналы аварийных сигналов.

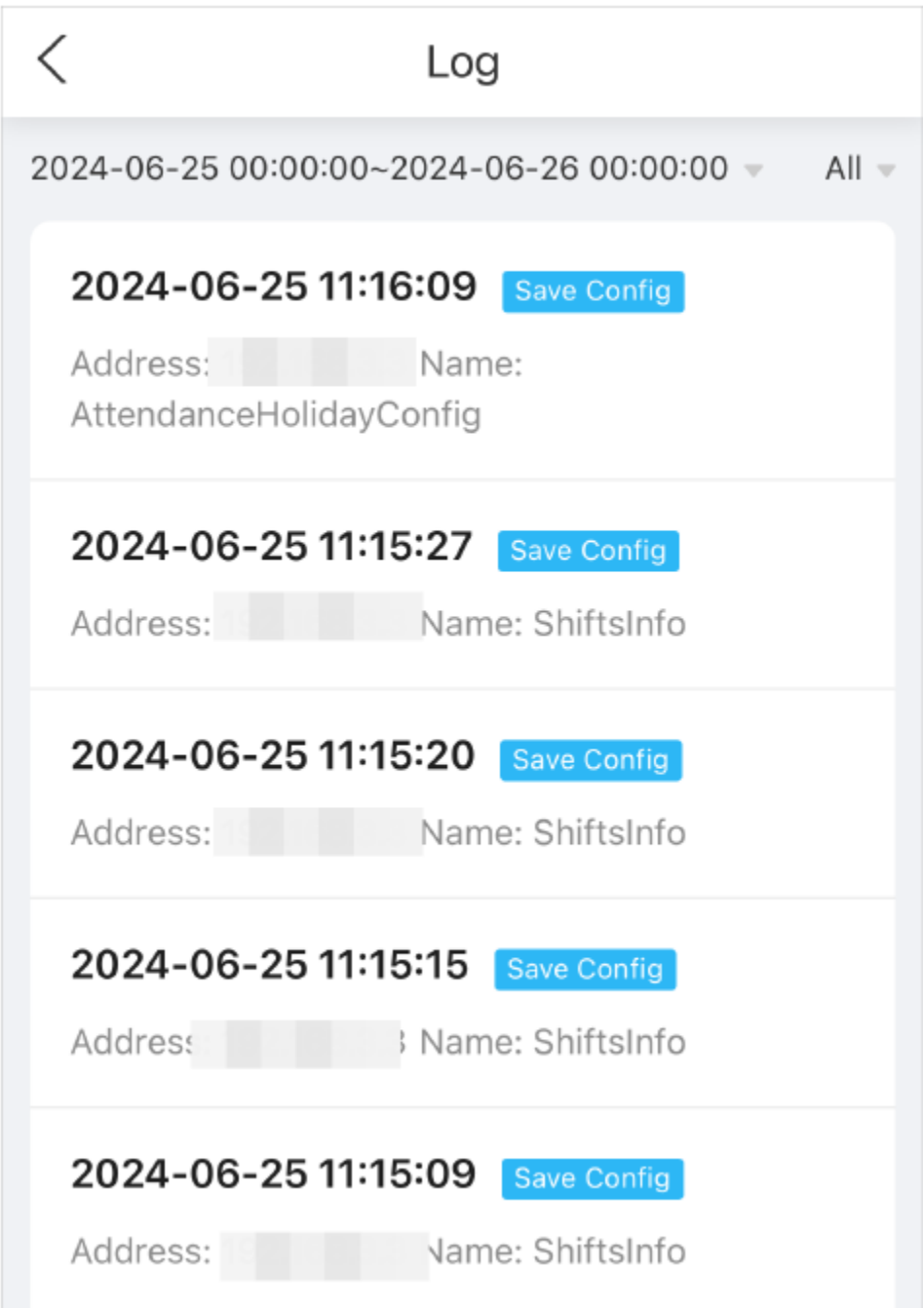
5.10.1 Системные журналы

Просматривайте системные журналы и выполняйте поиск.

Процедура

- Шаг 1 Войдите на веб-страницу.
- Шаг 2 Выберите Еще > Log > Log
- Шаг 3 Выберите время и тип записи.

Рисунок 5-35 Журналы.



5.10.2 Записи разблокировки.

Найдите записи разблокировки.

Процедура.

- Шаг 1. Войдите на веб-страницу.

Шаг 2 Выберите "Дополнительно"> "Журнал" > "Разблокировать записи".

Шаг 3 Выберите время и тип записи.

Шаг 4 Коснитесь записи, чтобы просмотреть подробную информацию.

5.10.3 История вызовов

Найдите историю вызовов.

Процедура

Шаг 1 Войдите на веб-страницу.

Шаг 2 Выберите Дополнительно> Журнал> Журнал вызовов.

5.10.4 Журналы тревог

Просмотрите журналы тревог.

Процедура

Шаг 1 Войдите на веб-страницу.

Шаг 2 Выберите "Подробнее"> "Журнал" > "Журнал тревоги".

Шаг 3 Выберите время и тип журнала.

6 Интеллектуальная конфигурация PSS Lite

В этом разделе рассказывается о том, как управлять устройством и настраивать его с помощью Smart PSS Lite. подробную информацию смотрите в руководстве пользователя Smart PSS Lite.

Установка 6.1

Обратитесь в службу технической поддержки или перейдите на официальный веб-сайт, чтобы получить SmartPSS Lite. Если вы получаете программный пакет SmartPSS Lite, установите и запустите программное обеспечение в соответствии с инструкциями на странице.

6.2 Инициализация и вход в систему

Инициализируйте SmartPSS Lite при первом входе в систему, включая установку пароля для входа в систему и контрольные вопросы для сброса пароля.

Процедура

- Шаг 1 Дважды щелкните SmartPSSLite.exe.
- Шаг 2 Выберите язык из выпадающего списка, выберите "Я прочитал и согласен с программным обеспечением"
соглашение, а затем нажмите "Далее".
- Шаг 3 Нажмите "Обзор", чтобы выбрать путь установки, а затем нажмите "Установить".
- Шаг 4 Нажмите "Готово", чтобы завершить установку.
- 

Выберите "Запустить SmartPSSLite", чтобы запустить SmartPSS Lite.
- Шаг 5 Выберите сцены приложения, которые вы хотите добавить, а затем нажмите "ОК".
- Шаг 6 Нажмите "Я прочитал и согласен с условиями лицензионного соглашения по программному обеспечению", чтобы согласиться
ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ПО ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ.
- Шаг 7 Нажмите Я прочитал и согласен с условиями политики конфиденциальности
программного обеспечения, чтобы согласиться с продуктом
Политика конфиденциальности.
- Шаг 8 Установите пароль на странице инициализации, а затем нажмите "Далее".

Таблица 6-1 Параметры настройки пароля

Параметр	Описание
Пароль	Пароль должен состоять из 8-32 непустых символов и содержать по крайней мере два типа символов: верхний регистр, нижний регистр, цифру и специальный символ (исключая пробел).
Надежность пароля	Отображает эффективность пароля против угадывания атак методом перебора. Зеленый цвет означает, что пароль надежный, а красный - менее надежный. Установите пароль высокой надежности в соответствии с запросом надежности пароля.
Подтвердите пароль.	Введите пароль еще раз, чтобы подтвердить пароль.
Автоматический вход в систему после регистрации.	Включите автоматический вход в систему после регистрации. Если вы не хотите, чтобы устройство автоматически входило в систему после инициализации, выберите "Нет".

Шаг 9 Задайте контрольные вопросы, а затем нажмите Завершить.

Шаг 10 Дважды щелкните SmartPSSLite.exe.

Шаг 11 Введите имя пользователя и пароль, а затем нажмите Войти.

Если на вашем компьютере доступно несколько сетей, вы можете выбрать одну из них.

6.3 Добавление устройств

Доступно 3 способа добавления устройств.

Автоматический поиск

- Добавление вручную
- Пакетный импорт

6.3.1 Добавление устройства с помощью поиска

Вы можете добавить несколько устройств, выполнив их поиск в текущем сегменте сети или в других сегментах сети.



Мы рекомендуем добавлять устройства с помощью поиска, если устройства находятся в одной сети сегмент, или когда вы хотите добавить устройства с известным сетевым сегментом, но не знаете точный IP-адрес устройств.

Процедура

Шаг 1 На домашней странице нажмите Устройства.

Шаг 2 Выберите метод поиска.

Нажмите Автоматический поиск, чтобы автоматически выполнить поиск устройств, подключенных к той же сети подключите сегмент к вашему компьютеру.

Введите начальный IP-адрес и конечный IP-адрес рядом с сегментом сети устройства, нажмите Поиск и затем система автоматически выполнит поиск устройств в этом диапазоне IP-адресов.

Шаг 3 Выберите устройства и нажмите "Добавить".

Шаг 4 Введите имя пользователя для входа и пароль, а затем нажмите "ОК".

Устройства будут добавлены на платформу.



: Измените информацию об устройстве.



: Переходит к модулю конфигурации устройства в платформе.



: Переходит на веб-страницу устройства.



: Выйдите из устройства, и состояние устройства станет автономным.



: Войдите в систему на устройстве, и состояние устройства станет оперативным.



: Удалите устройство.

Связанные операции

Меняйте IP-адреса один за другим: выберите устройство, а затем нажмите "Изменить IP", чтобы изменить IP-адрес устройства. Изменение IP-адресов пакетно: выберите несколько устройств, а затем нажмите "Изменить", чтобы изменить их IP-адреса адреса.



Введите начальный IP-адрес, и система автоматически назначит IP-адрес устройствам путем увеличения на 1 в IP-адресе, основанном на начальном IP-адресе. Например, если начальный IP-адрес равен 10.XX.XXX.52, а следующими IP-адресами устройств будут 10.XX.XXX.53, 10.XX.XXX.54 и более.

Инициализация устройств: Нажмите кнопку Инициализировать, чтобы инициализировать устройства.



Поддерживает активацию только тех устройств, которые находятся в том же сегменте сети, что и ваш компьютер.

6.3.2 Добавление устройств одно за другим.

Если вы уже знаете IP-адрес устройства, вы можете вручную добавить его на платформу. Процедура

Шаг 1 На домашней странице нажмите Устройства.

Шаг 2 Нажмите Добавить, а затем введите информацию об устройстве.

Шаг 3 Нажмите Добавить.

Вы также можете нажать Добавить и продолжить добавлять другие устройства.

Приложение 1 Важные моменты снятия отпечатков пальцев

Инструкции по регистрации

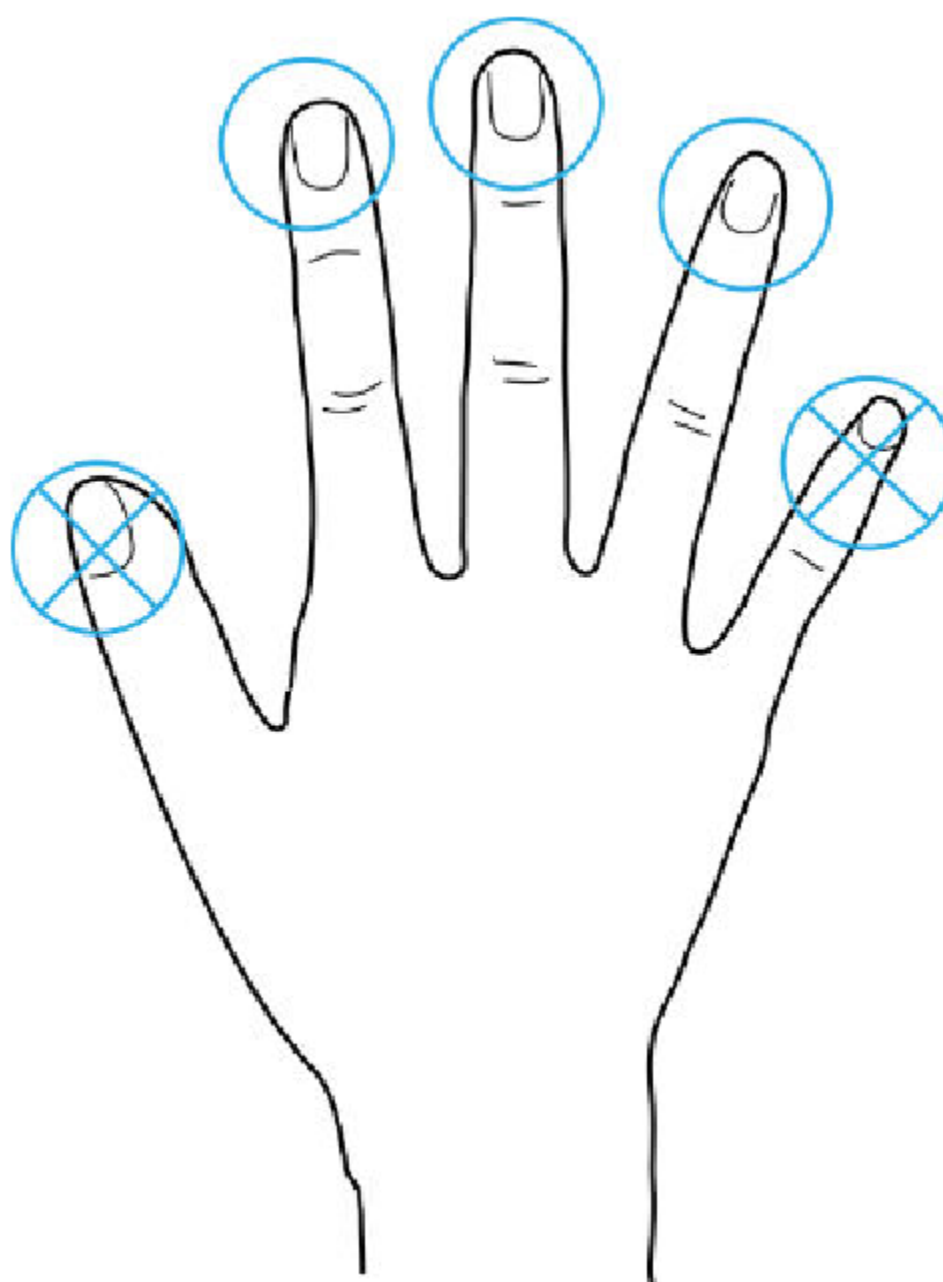
При регистрации отпечатка пальца обратите внимание на следующие моменты:

- Убедитесь, что ваши пальцы и поверхность сканера чистые и сухие.
Нажмите пальцем на центр сканера отпечатков пальцев.
- Не размещайте датчик отпечатков пальцев в местах с интенсивным освещением, высокой температурой и повышенной влажностью.
- Если отпечатки пальцев нечеткие, используйте другие методы разблокировки.

Рекомендуется использовать пальцы.

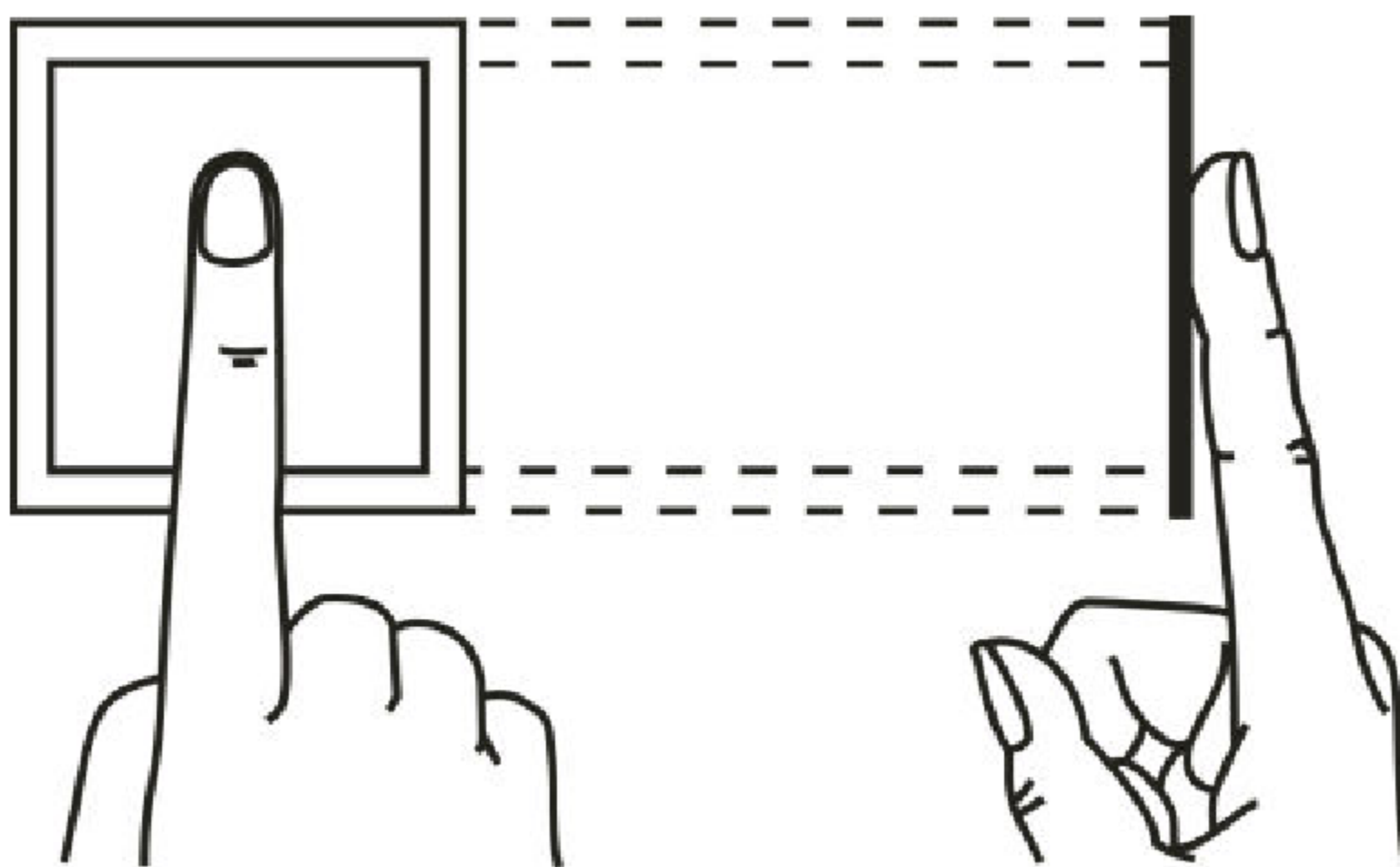
Рекомендуются указательные, средние и безымянные пальцы. Большие пальцы и мизинцы невозможно легко поместить в центр записи.

Приложение Рисунок 1-1 Рекомендуемые пальцы

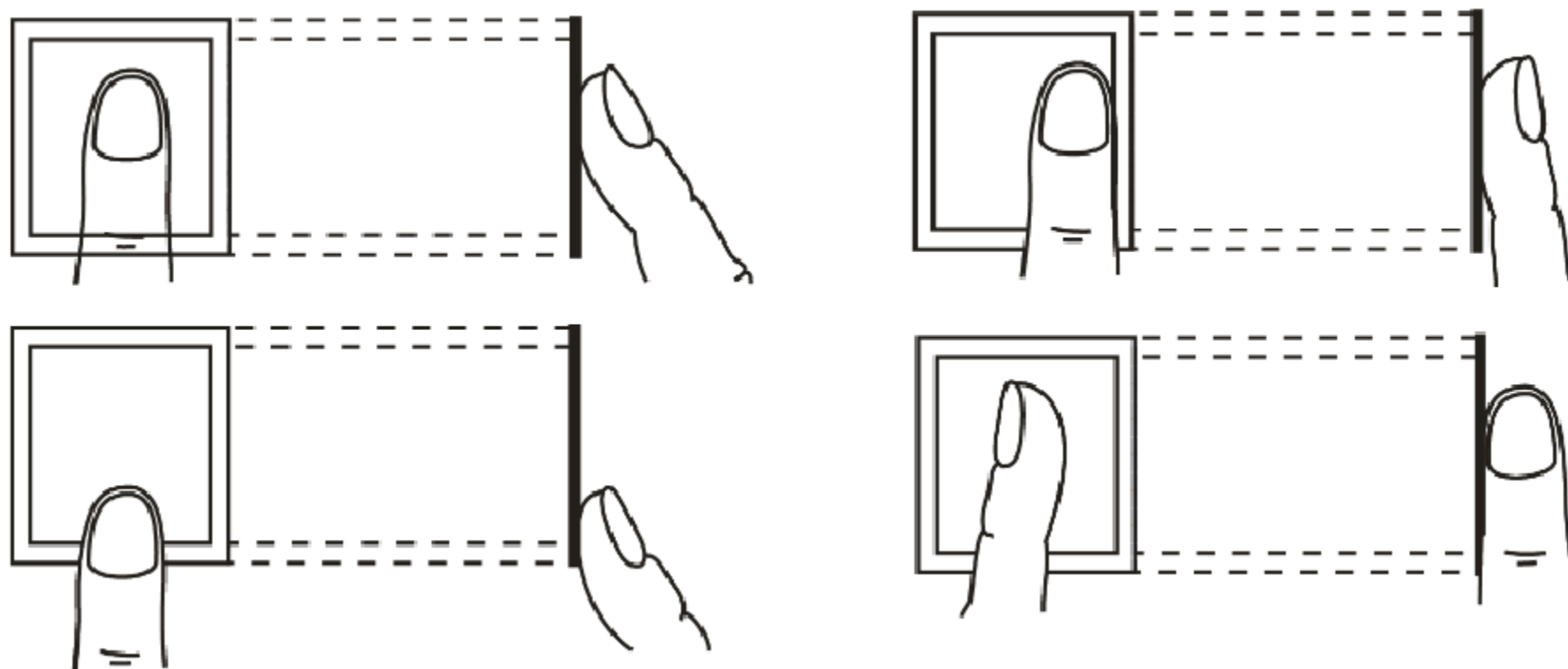


Как нажимать отпечаток пальца на сканер

Приложение Рис. 1-2 Правильное размещение



Приложение Рис. 1-3 Неправильное размещение



Приложение 2 Рекомендации по безопасности

Управление учетной записью

1. Используйте сложные пароли

Пожалуйста, ознакомьтесь со следующими рекомендациями по установке паролей:

- Длина должна быть не менее 8 символов;
- Содержать по крайней мере два типа символов: буквы верхнего и нижнего регистра, цифры и условные обозначения;
- Не содержать название учетной записи или название учетной записи в обратном порядке порядок;
- Не используйте непрерывные символы, такие как 123, abc и т.д.;
- Не используйте повторяющиеся символы, такие как 111, aaa и т.д.

2. Периодически меняйте пароли

Рекомендуется периодически менять пароль устройства, чтобы снизить риск того, что его угадают или взломают.

3. Соответствующим образом распределите учетные записи и разрешения

Соответствующим образом добавляйте пользователей на основе требований к сервису и управлению и назначайте минимальные наборы разрешений для пользователей.

4. Включите функцию блокировки учетной записи

Функция блокировки учетной записи включена по умолчанию. Рекомендуется поддерживать его включенным для защиты безопасности учетной записи. После нескольких неудачных попыток ввода пароля соответствующая учетная запись и исходный IP-адрес будут заблокированы.

5. Своевременно устанавливайте и обновляйте информацию о сбросе пароля

Устройство поддерживает функцию сброса пароля. Чтобы снизить риск использования этой функции участниками угрозы, если в информации происходят какие-либо изменения, пожалуйста, своевременно внесите в нее изменения. При настройке контрольные вопросы рекомендуется не использовать ответы, которые легко угадать.

Конфигурация службы

1. Включите HTTPS

Рекомендуется включить протокол HTTPS для доступа к веб-сервисам по защищенным каналам.

2. Передача аудио и видео в зашифрованном виде

Если содержимое ваших аудио- и видеоданных очень важно или конфиденциально, рекомендуется использовать функция зашифрованной передачи для снижения риска перехвата ваших аудио- и видеоданных во время передачи.

3. Отключите второстепенные службы и используйте безопасный режим.

Если в этом нет необходимости, рекомендуется отключить некоторые службы, такие как SSH, SNMP, SMTP, UPnP, AP точка доступа и т.д., чтобы уменьшить возможности атаки.

При необходимости настоятельно рекомендуется выбрать безопасные режимы, включая, но не ограничиваясь ими следующие службы:

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

4. Измените порты HTTP и других служб по умолчанию

Рекомендуется изменить порт HTTP и других служб по умолчанию на любой порт между 1024 и 65535, чтобы снизить риск быть угаданным субъектами угрозы.

Конфигурация сети

1. Включите список разрешений

Рекомендуется включить функцию списка разрешенных адресов и разрешать доступ к устройству только по IP-адресу из списка разрешенных. Поэтому, пожалуйста, не забудьте добавить IP-адрес вашего компьютера и вспомогательный адрес, указанный в списке разрешенных адресов. Поэтому, пожалуйста, не забудьте добавить IP-адрес вашего компьютера и поддержку IP-адрес устройства в списке разрешений.

2. Привязка MAC-адреса

Рекомендуется привязать IP-адрес шлюза к MAC-адресу на устройство для снижения риска ARP-спуфинг.

3. Построение безопасной сетевой среде

Для того, чтобы лучше обеспечить безопасность устройств и снижения возможных кибер-рисков, следующие рекомендуются:

Отключите функцию сопоставления портов маршрутизатора, чтобы избежать прямого доступа к устройствам внутренней сети из внешней сети;

В соответствии с фактическими потребностями сети разделите сеть: если связь отсутствует по требованию между двумя подсетями рекомендуется использовать VLAN, шлюз и другие методы разделения сети для достижения сетевой изоляции;

· Установить 802.система аутентификации 1x access для снижения риска незаконного терминального доступа к частной сети.

Аудит безопасности

1. Проверка онлайн-пользователей

Рекомендуется регулярно проверять онлайн-пользователей для выявления нелегальных пользователей.

2. Проверьте журнал устройства

Просматривая журналы, вы можете узнать об IP-адресах, по которым осуществляется вход в систему устройства, и ключевые операции зарегистрированных пользователей.

3. Настройте сетевой журнал.

Из-за ограниченного объема памяти устройств объем сохраняемого журнала ограничен. Если вам необходимо сохранить вести журнал в течение длительного времени, рекомендуется включить функцию сетевого журнала, чтобы гарантировать, что критические журналы синхронизируются с сервером сетевых журналов для отслеживания.

Безопасность программного обеспечения

1. Своевременно обновляйте встроенное ПО

В соответствии с отраслевыми стандартными рабочими спецификациями, микропрограммное обеспечение устройств должно быть своевременно обновлено до последней версии, чтобы гарантировать, что устройство имеет новейшие функции и безопасность. Если устройство подключено к общедоступной сети, рекомендуется включить функцию автоматического обнаружения онлайн-обновления, чтобы получить информацию об обновлении встроенного ПО своевременно выпускается производителем.

2. Своевременно обновляйте клиентское программное обеспечение.

Рекомендуется загружать и использовать новейшее клиентское программное обеспечение.

Физическая защита

Рекомендуется обеспечить физическую защиту устройств (особенно устройств хранения данных), например, поместить устройство в специальное машинное отделение или шкаф и установить контроль доступа

и управление ключами для предотвращения повреждения оборудования посторонним персоналом
другое периферийное оборудование (например, флэш-диск USB, последовательный порт).