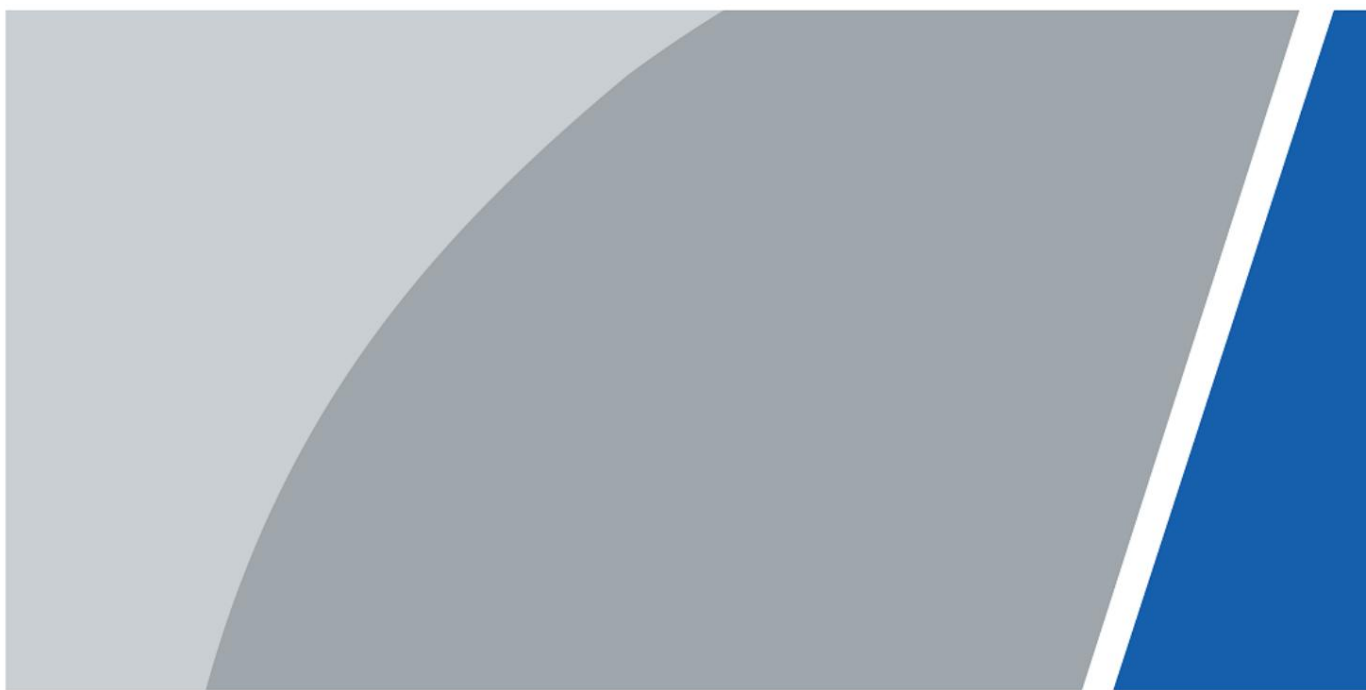


Контроллер доступа с распознаванием лиц Web 5.0

Руководство пользователя



V1.5.0

Предисловие

Общий

В данном руководстве описаны функции и работа контроллера доступа с распознаванием лиц (далее именуемого «Устройство»). Внимательно прочтите руководство перед использованием устройства и сохраните его для дальнейшего использования.

Символы

В руководстве могут встречаться следующие символы.

Символ	Описание
 DANGER	Указывает на высокую потенциальную опасность, которая, если ее не избежать, приведет к смерти или серьезным травмам.
 WARNING	Указывает на среднюю или низкую потенциальную опасность, которая, если ее не избежать, может привести к легким или умеренным травмам.
 CAUTION	Указывает на потенциальный риск, который, если его не предотвратить, может привести к повреждению имущества, потере данных, снижению производительности или непредсказуемым результатам.
 TIPS	Предлагает методы, которые помогут вам решить проблему или сэкономить время.
 NOTE	Предоставляет дополнительную информацию в качестве дополнения к тексту.

История изменений

Версия	Содержание для пересмотра	Время выпуска
V1.5.0	• Добавлен модуль расширения. • Обновлены параметры лица. • Обновлены функции домофона. • Добавлена функция локального кода. • Обновлены настройки конфиденциальности.	Июль 2026 г.
V1.4.1	• Обновлена инициализация процесс. • Добавлена аутентификация по PIN-коду при локальной работе. • Обновлено описание функции постоянной активности. • Обновлены настройки конфиденциальности.	Октябрь 2025 г.

Версия	Содержание для пересмотра	Время выпуска
V1.4.0	• Обновленная информация о посещаемости функция. • Обновлена проверка методы. • Обновленная система контроля доступа настройки и многое другое.	Июль 2025 г.
V1.3.1	Обновлены настройки карты.	Февраль 2025 г.
V1.3.0	Обновлены функции телефонной связи и другие функции.	Декабрь 2024 г.
V1.2.3	Обновлены важные меры безопасности. и предупреждения.	Август 2024 г.
V1.2.2	Обновлена информация о посещаемости. настройки прав доступа.	Июнь 2024 г.
V1.2.1	Обновил настройки домофона. настройки контроля доступа и более.	Май 2024 г.
V1.2.0	Обновленная информация настройки, настройки контроля доступа и многое другое.	Ноябрь 2023 г.
V1.1.0	Обновлено руководство.	Октябрь 2023 г.
V1.0.0	Первый релиз.	Июнь 2023 г.

Уведомление о защите конфиденциальности

Как пользователь устройства, вы можете собирать персональные данные отдельных лиц, такие как их имена и адреса электронной почты. адреса, изображения лиц, аудиозаписи и отпечатки пальцев. Вы несете полную ответственность за любые действия. в связи с обработкой персональных данных. Вы обязуетесь соблюдать местные правила защиты конфиденциальности. законы и нормативные акты для защиты законных прав и интересов отдельных лиц, и должны внедрять меры, требуемые действующим законодательством, включая, помимо прочего, предоставление Предоставление лицам четкой и исчерпывающей информации перед обработкой их персональных данных. получение согласия от отдельных лиц, когда это необходимо, информирование отдельных лиц о существовании зона наблюдения и предоставление необходимой контактной информации.

Заявление об использовании интеллектуального продукта

Интеллектуальные продукты используют технологии искусственного интеллекта для эффективного повышения безопасности. Интеллектуальное распознавание. а на работу тревожных функций изделия могут влиять такие факторы, как окружающее освещение. Углы обзора камеры, препятствия и задержки в сети могут привести к ложным срабатываниям или их пропуску. оповещения или задержки реакции. Этот интеллектуальный продукт предназначен исключительно для использования в целях безопасности. Вспомогательный инструмент. Результаты идентификации приведены только для озна ознакомления и не являются исчерпывающими. представляют собой абсолютную гарантию личной безопасности или безопасности имущества. Пользователям необходимо сочетать эти два подхода. продукция, оснащенная необходимыми мерами физической защиты для повышения общей безопасности. За исключением случаев, когда иным образом, предусмотренным законом, или в случае умышленной или грубой халатности со стороны Компания не несет ответственности за любые убытки, вызванные вышеупомянутыми факторами. относится к компании.

Объявление интерфейса

Данное руководство в основном описывает основные функции устройства. Интерфейсы, используемые при его производстве, процедуры возврата устройства на завод для проверки и выявления неисправностей в данном руководстве не описаны. Для получения информации об этих интерфейсах обратитесь в службу технической поддержки.

О руководстве пользователя

- Данное руководство предназначено только для общего ознакомления. Возможны расхождения между версиями. продукт и данное руководство, включая, помимо прочего, печатные, электронные и любые другие издания. • Руководство будет обновляться в соответствии с последними законами и правилами соответствующих юрисдикций. Технические характеристики и документация могут быть изменены без предварительного уведомления. Для получения актуальной информации, а также юридических уведомлений, обратитесь к печатному руководству, странице продукта на нашем официальном сайте или отсканируйте QR-код для доступа к электронной версии.
- Руководство будет обновляться по мере необходимости с учетом изменений в продукте и применимого законодательства. требования. Эти обновления не уменьшат ваши законные права и не удалят и не ослабят информацию о безопасности или основные инструкции, предоставленные во время покупки. • Хотя мы прилагаем все усилия для обеспечения точности, ошибки или отклонения в описаниях могут быть незначительными. Возможны несоответствия в функциях, операциях или технических данных. В случае возникновения каких-либо неясностей или разногласий мы оставляем за собой право окончательного разъяснения. • Все товарные знаки, зарегистрированные товарные знаки и названия компаний, упомянутые в данном руководстве, являются собственностью [название компании]. собственность их соответствующих владельцев.

Оглавление

Предисловие.....	Я
1 Обзор.....	1
2 Локальные операции.....	2
настройки.....	2
2.2 Инициализация.....	2
2.3 Экран ожидания.....	9
2.4 Общие значки.....	12
2.5 Вход в систему.....	12
2.6 Сброс пароля.....	13
2.7 Методы разблокировки.....	14
2.7.1 Разблокировка с помощью карт.....	14
2.7.2 Разблокировка по лицу.....	14
2.7.3 Разблокировка по отпечатку пальца.....	14
2.7.4 Разблокировка по паролю пользователя.....	15
2.7.5 Разблокировка по открытому паролю.....	15
2.7.6 Разблокировка по Bluetooth.....	15
2.7.7 Разблокировка с помощью временного пароля.....	16
2.7.8 Разблокировка с помощью QR-кода.....	16
2.8 Управление персоналом.....	16
2.8.1 Настройка отделов.....	16
2.8.2 Добавление пользователей.....	17
2.8.3 Просмотр информации о пользователе.....	21
2.9 Управление записями.....	22
2.9.1 Хранение записей о разблокировке.....	22
2.9.2 Поиск записей о разблокировке.....	22
2.9.3 Экспорт записей о разблокировке.....	23
2.9.4 Экспорт данных о посещаемости.....	24
2.10 Управление контролем доступа.....	24
2.10.1 Настройка метода разблокировки.....	24
2.10.2 Настройка открытого пароля.....	27
2.10.3 Настройка интервала проверки.....	27
2.10.4 Настройка состояния блокировки.....	28
2.10.5 Настройка сигнализации.....	28
2.10.6 Настройки карты.....	30
2.10.7 Настройка аутентификации по PIN-коду.....	31
2.10.8 Настройка блокировки2.....	31
2.11 Управление посещаемостью.....	32

2.11.1 Настройка смен.....	32	2.11.2 Настройка планов на праздничные дни.....	35
2.11.3 Настройка графиков работы.....	36	2.11.4 Настройка режимов учета рабочего времени.....	39
2.12 Видеодомофон.....	43		
2.12.1 Настройка видеодомофона.....	43	2.12.2 Настройка SIP- сервера.....	44
2.12.3 Настройка локального кода.....	44	2.13 Настройки связи.....	45
2.13.1 Настройка сети.....	45		
2.13.2 Настройка RS-485	50	2.13.3 Настройка Bluetooth.....	52
2.13.4 Настройка Wiegand.....	53	2.13.5 Настройки безопасности.....	54
2.14 Биометрия.....	54		
2.14.1 Настройка параметров распознавания лица.....	54	2.14.2 Настройка параметров распознавания отпечатков пальцев.....	56
2.15 Системные настройки.....	57		
2.15.1 Настройка режима «Не беспокоить».....	57		
2.15.2 Настройка времени.....	58		
2.15.3 Настройка громкости.....	59	2.15.4 Настройка параметров экрана.....	60
2.15.5 Настройка параметров конфиденциальности.....	66	2.15.6 Управление хранилищем.....	67
2.15.7 Настройка сброса пароля.....	67		
2.15.8 Настройка модуля расширения.....	68	2.15.9 Настройка языка.....	68
2.15.10 Настройка сброса защиты от несанкционированного доступа.....	68	2.15.11 Обновление системы.....	69
2.15.12 Настройка пароля устройства.....	69		
2.15.13 Восстановление заводских настроек.....	69	2.15.14 Перезагрузка устройства.....	70
2.16 Информация об устройстве.....	70		
2.16.1 Объем данных для просмотра.....	70		
2.16.2 Версия устройства просмотра.....	70		
3 Веб-операции.....	72		
3.1 Инициализация.....	72		
3.2 Вход в систему.....	72		
3.3 Сброс пароля.....	73		
3.4 Мониторинг доступа.....	73		

3.5 Главная страница.....	75
3.6 Управление персоналом.....	76
3.7 Настройка контроля доступа.....	82
3.7.1 Параметры контроля доступа.....	82
3.7.2 Сигнализация.....	86
3.7.3 Настройка параметров лица.....	91
3.7.4 Настройки карты.....	95
3.7.5 Настройка QR-кода.....	101
3.7.6 Настройка периодов.....	102
3.7.7 Настройка модулей расширения.....	105
3.7.8 Настройки конфиденциальности.....	105
3.7.9 Настройка функций порта.....	106
3.7.10 Настройка параметров управления лифтом.....	107
3.7.11 Настройка сравнения на стороне сервера.....	108
3.7.12 Настройка разблокировки режима от первого лица.....	109
3.7.13 Настройка защиты от обратного прохода.....	110
Настройка внутренней связи.....	112
3.8.1 Использование устройства в качестве SIP-сервера.....	112
3.8.2 Использование VTO в качестве SIP-сервера.....	126
3.8.3 Использование платформы в качестве SIP-сервера.....	128
3.8.4 Настройка параметров вызова.....	131
3.9 Настройка учета рабочего времени.....	133
3.9.1 Настройка отделов.....	133
3.9.2 Настройка смен.....	134
3.9.3 Настройка праздников.....	137
3.9.4 Настройка графиков работы.....	138
3.9.5 Экспорт записей о посещаемости.....	141
3.9.6 Настройка режимов посещаемости.....	142
3.10 Настройка аудио и видео.....	143
3.10.1 Настройка видео.....	143
3.10.2 Настройка звуковых подсказок.....	148
3.10.3 Настройка обнаружения движения.....	150
3.10.4 Настройка локального кода.....	151
3.11 Настройки связи.....	152
3.11.1 Сетевые настройки.....	152
3.11.2 Настройки Bluetooth.....	165
3.11.3 Настройка RS-485.....	166
3.11.4 Настройка Wiegand.....	168
3.12 Настройка системы.....	169
3.12.1 Управление пользователями.....	169

3.12.2 Настройка времени.....	172
3.13 Персонализация.....	174
3.13.1 Реклама.....	174
3.13.2 Настройки экрана.....	178
3.14 Центр управления.....	182
3.14.1 Диагностика одним щелчком мыши.....	182
3.14.2 Информация о системе.....	183
3.14.3 Объем данных.....	183
3.14.4 Журналы просмотра.....	184
3.14.5 Центр технического обслуживания.....	185
3.14.6 Обновление системы.....	187
3.14.7 Расширенное техническое обслуживание.....	188
3.15 Настройки безопасности (необязательно)	189
3.15.1 Состояние безопасности.....	189
3.15.2 Настройка HTTPS.....	190
3.15.3 Атака Защита.....	191
3.15.4 Установка сертификата устройства.....	194
3.15.5 Установка сертификата доверенного центра сертификации.....	197
3.15.6 Шифрование данных.....	198
3.15.7 Предупреждение о безопасности.....	199
3.15.8 Аутентификация безопасности.....	199
4. Работа с телефоном.....	201
4.1 Инициализация.....	201
4.2 Вход на веб-страницу.....	201
4.3 Главная страница.....	203
4.4 Управление персоналом.....	205
4.5 Настройка системы.....	209
4.5.1 Просмотр информации о версии.....	209
4.5.2 Управление конфигурацией.....	209
4.5.3 Техническое обслуживание.....	209
4.5.4 Настройка времени.....	210
4.5.5 Объем данных.....	212
4.5.6 Язык.....	212
4.6 Настройка учета посещаемости.....	212
4.6.1 Настройка отделов.....	212
4.6.2 Настройка смен.....	214
4.6.3 Настройка праздничных дней.....	217
4.6.4 Настройка графиков работы.....	218
4.6.5 Настройка режимов учета рабочего времени.....	220
4.7 Настройка контроля доступа.....	221

4.7.1 Настройка методов разблокировки.....	221
4.7.2 Настройка параметров распознавания лиц.....	222
4.7.3 Настройка параметров контроля доступа.....	224
4.7.4 Настройка сигнализации.....	228
4.7.5 Настройка связи между сигналами тревоги (необязательно).....	231
4.7.6 Настройка связи событий тревоги.....	232
4.7.7 Настройка параметров карты.....	233
4.7.8 Настройки конфиденциальности.....	236
4.7.9 Настройка функций порта.....	236
4.7.10 Настройка параметров экрана.....	237
4.8 Настройки связи.....	238
4.8.1 Настройка TCP/IP.....	239
4.8.2 Настройка Wi-Fi.....	240
4.8.3 Настройка точки доступа Wi-Fi.....	241
4.8.4 Настройка облачного сервиса.....	241
4.8.5 Настройка автоматической регистрации.....	242
4.8.6 Настройка Wiegand.....	242
4.8.7 Настройка RS-485.....	244
4.8.8 Настройка Bluetooth.....	247
4.9 Настройка звуковых подсказок.....	247
4.10 Просмотр журналов.....	249
4.10.1 Системные журналы.....	249
4.10.2 Разблокировка записей.....	249
4.10.3 История звонков.....	250
4.10.4 Журналы аварийных сигналов.....	250
5 Настройка Smart PSS Lite.....	251
5.1 Установка и вход в систему.....	251
5.2 Добавление устройств.....	251
5.2.1 Добавление устройств по одному.....	251
5.2.2 Добавление устройств партиями.....	252
5.3 Управление пользователями.....	254
5.3.1 Настройка типа карты.....	254
5.3.2 Добавление персонала.....	254
5.3.3 Назначение прав доступа.....	257
5.3.4 Назначение разрешений на посещение.....	259
5.4 Управление доступом.....	261
5.4.1 Дистанционное открытие и закрытие двери.....	261
5.4.2 Настройка «Всегда открыта» и «Всегда закрыта».....	262
5.4.3 Мониторинг состояния двери.....	262
Приложение 1. Важные моменты регистрации лица.....	264

Приложение 2. Важные моменты работы домофона.....267 Приложение 3.
Важные моменты инструкции по регистрации отпечатков пальцев.....268 Приложение 4.
Важные моменты сканирования QR-кода..... 270 Приложение 5.
Рекомендации по безопасности..... 271

1. Обзор

Устройство представляет собой контроллер доступа, поддерживающий разблокировку с помощью лиц, паролей, отпечатков пальцев, карт, QR-кодов и их комбинаций. Благодаря алгоритму глубокого обучения, оно отличается более быстрым распознаванием и высокой точностью. Устройство может работать с платформой управления, что удовлетворяет различным потребностям клиентов.

Он широко используется в парках, жилых комплексах, деловых центрах и на заводах, а также идеально подходит для таких мест, как офисные здания, правительственные здания, школы и стадионы.

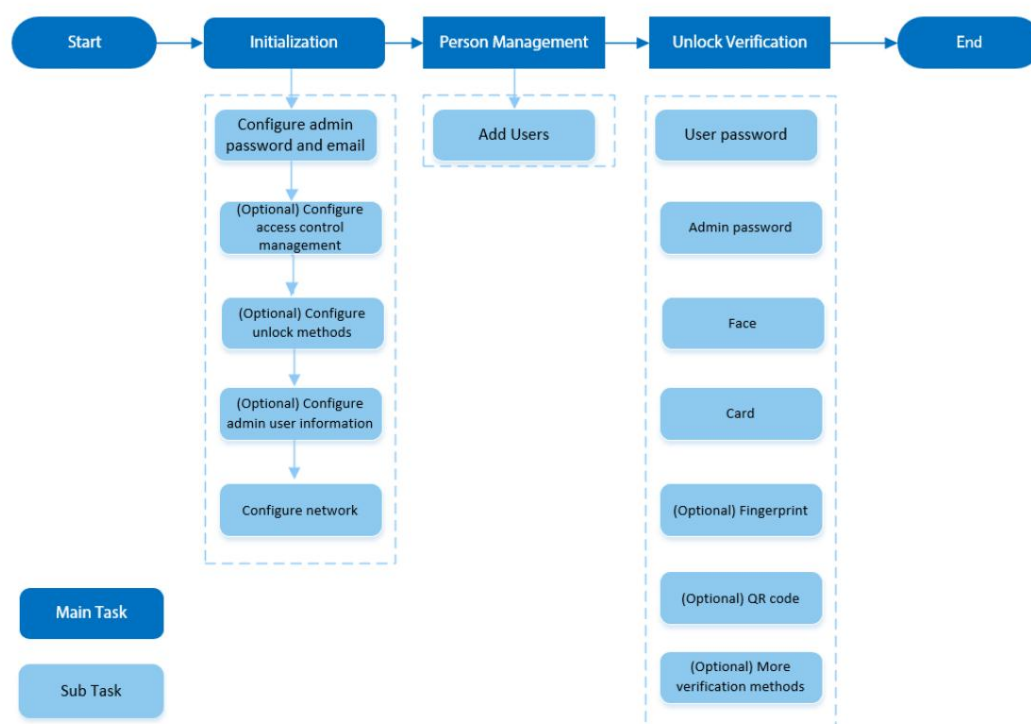
- Конфигурация может отличаться в зависимости от модели продукта, пожалуйста, ориентируйтесь на фактическую конфигурацию продукта.
- Для выполнения настроек устройства без сенсорного экрана должны быть подключены к мыши. Данное руководство В качестве примера используется устройство с сенсорным экраном.
- Некоторые модели поддерживают подключение дополнительных модулей, таких как модуль QR-кода, модуль отпечатка пальца и другие. Типы дополнительных модулей, поддерживаемых устройством, могут отличаться, пожалуйста, обратитесь к характеристикам конкретного продукта.

2 Локальные операции

- Настройки могут отличаться в зависимости от конкретного продукта. • Для моделей без сенсорного экрана требуется подключение проводной USB-мыши. В этом разделе в качестве примера используются модели с сенсорным экраном. • Внешние модули расширения доступны только для некоторых моделей. • Некоторые тексты интерфейса могут не отображаться из-за ограниченного пространства. Нажмите и удерживайте Подождите с текстом 3 секунды, и он отобразится.

2.1 Процедура базовой настройки

Рисунок 2-1. Базовая процедура настройки.



2.2 Инициализация

При первом использовании или после сброса до заводских настроек необходимо выбрать язык на устройстве, а затем установить пароль и адрес электронной почты для учетной записи администратора. С помощью учетной записи администратора можно получить доступ к главному меню устройства и его веб-странице.

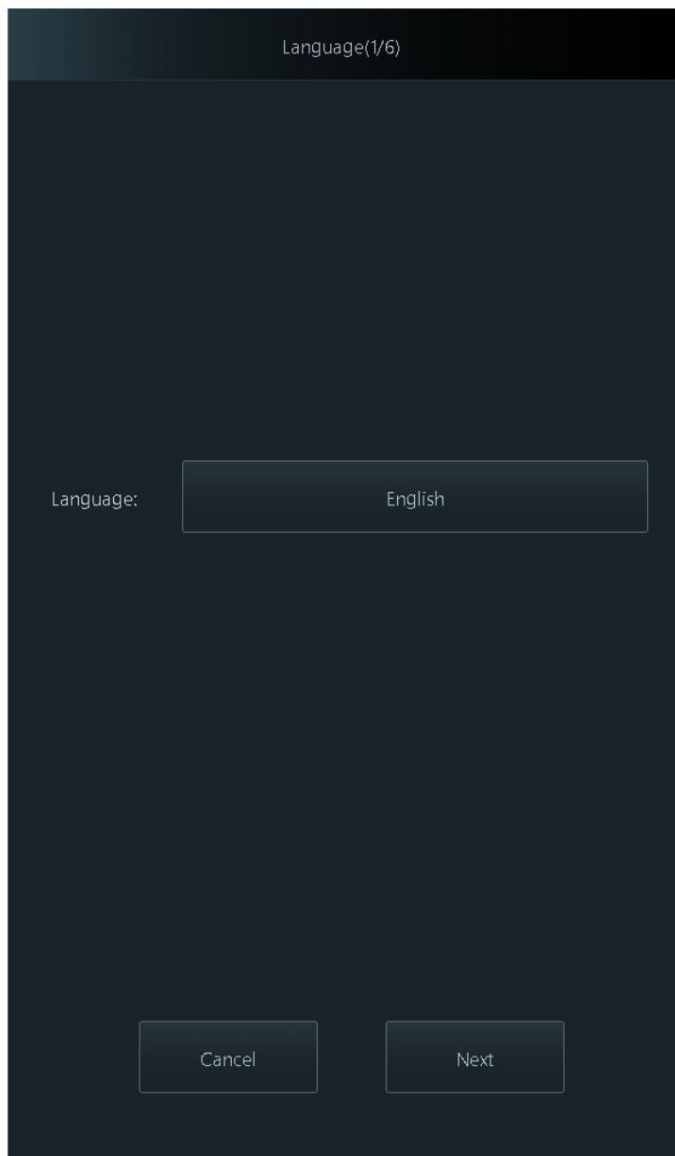
Процедура

Шаг 1 Для первого использования включите устройство, чтобы перейти к экрану инициализации.

Если устройство было восстановлено до заводских настроек, перезагрузите устройство, чтобы перейти к инициализации. экран.

Шаг 2. Выберите язык, а затем нажмите «Далее».

Рисунок 2-2. Выберите язык.



Language(1/6)

Language: English

Cancel Next

Шаг 3. Введите пароль, подтвердите пароль, введите адрес электронной почты, а затем нажмите «Далее».



- Если вы забыли пароль администратора, отправьте запрос на восстановление на указанный вами адрес электронной почты. адрес.
- Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' '). ; : &). Пожалуйста, настройте пароль повышенной безопасности в соответствии с подсказкой.

Рисунок 2-3. Настройка пароля.

Device Initialization(2/6)

Admin admin

Enter Password Please enter

Confirm Password Please enter

Email

Remove Next

Шаг 4. Настройте параметры контроля доступа, а затем нажмите «Далее».

Рисунок 2-4. Настройка параметров распознавания.

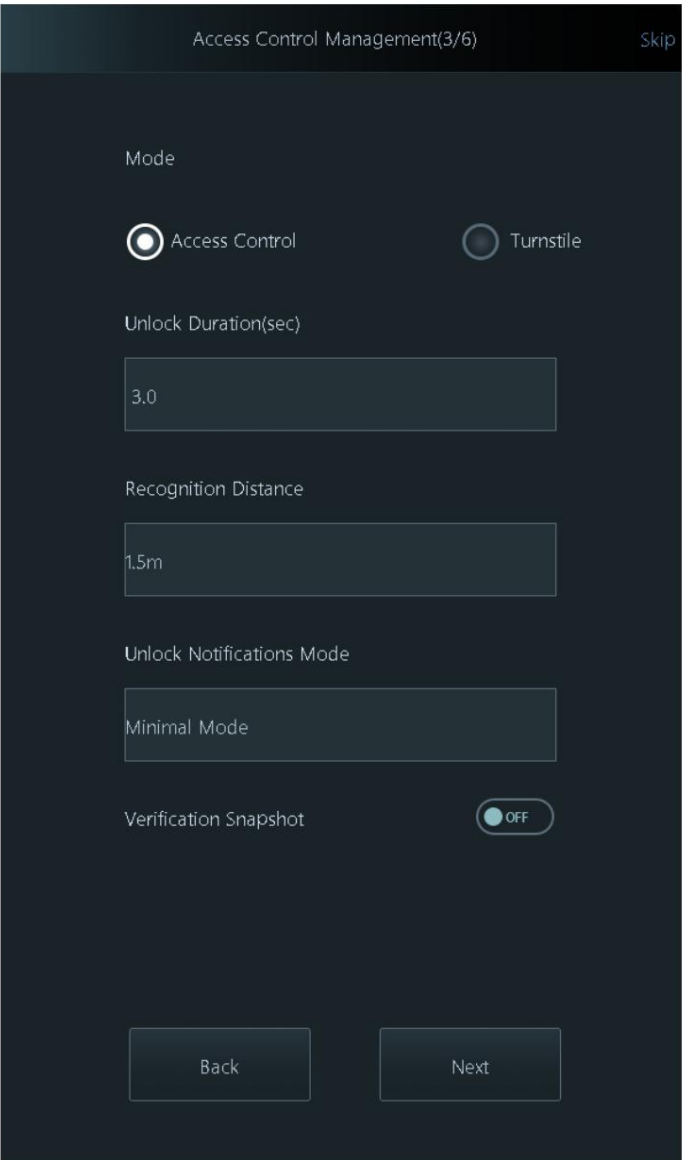


Таблица 2-1. Описание параметров контроля доступа.

Параметр	Описание
Режим	Выберите «Турникет», если система контроля доступа установлена на турникетах, и «Контроль доступа» для всех остальных случаев.
Длительность разблокировки (сек)	После того, как человеку будет предоставлен доступ, дверь останется открытой в течение определенного времени, чтобы он мог пройти.
Расстояние распознавания: расстояние между лицом и объективом.	По умолчанию составляет 1,5 м.
Уведомление о разблокировке Режим	Режим отображения для проверки личности. По умолчанию — минимальный режим .
Функция создания снимков состояния	во время проверки: включите эту функцию, и снимки состояния будут создаваться в процессе проверки.

Параметр	Описание
Магазин Разблокировать Записи	При включении этой функции записи о разблокировке сохраняются на локальном устройстве. Функция включена по умолчанию.  Эта функция доступна только на некоторых моделях.

Шаг 5. Настройте способ разблокировки с помощью комбинации клавиш, а затем нажмите «Далее».

Выберите способ разблокировки и комбинацию клавиш.

- +И : Для открытия двери необходимо проверить все выбранные способы разблокировки.

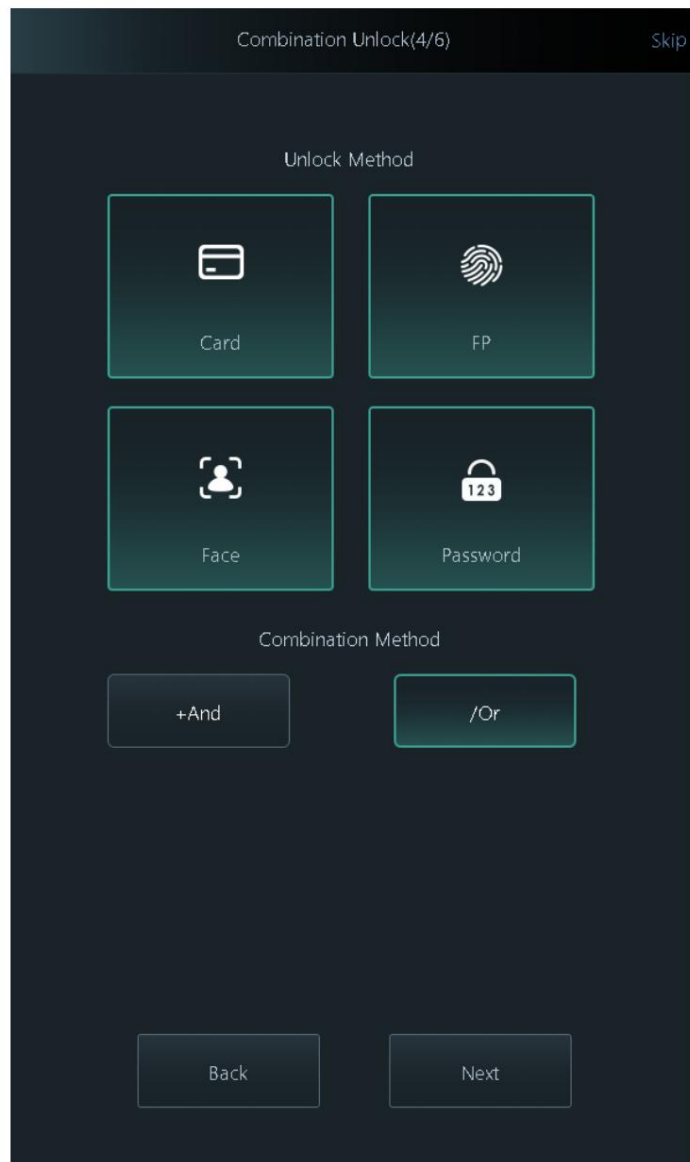
Например, если вы выберете распознавание лица и ввод пароля, вам потребуется подтвердить распознавание лица и пароль, чтобы разблокировать дверь. Вы можете разблокировать дверь в соответствии с подсказками на экране.

- /Или : Выберите один из способов разблокировки, чтобы открыть дверь.



Чтобы пропустить этот шаг, нажмите кнопку «Пропустить» в правом верхнем углу экрана.

Рисунок 2-5. Комбинированная разблокировка.



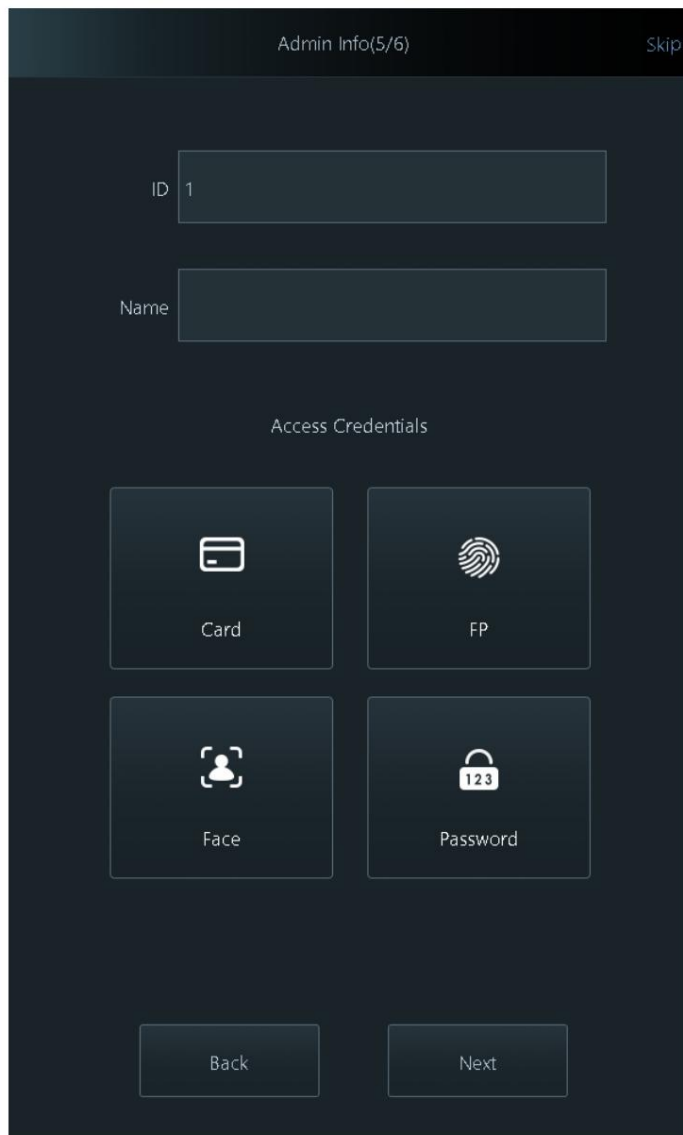
Шаг 6. Добавьте администратора, а затем нажмите «Далее».

Введите идентификатор и имя, выберите учетные данные доступа, а затем зарегистрируйте информацию в соответствии с подсказками.



Чтобы пропустить этот шаг, нажмите кнопку «Пропустить» в правом верхнем углу экрана.

Рисунок 2-6. Добавить администратора.



The screenshot shows a dark-themed interface for adding an administrator. At the top, it says 'Admin Info(5/6)' with a 'Skip' link on the right. Below this, there are two input fields: 'ID' with the value '1' and 'Name' which is empty. Underneath these fields is a section titled 'Access Credentials' containing four buttons: 'Card' (with a card icon), 'FP' (with a fingerprint icon), 'Face' (with a face icon), and 'Password' (with a lock icon). At the bottom of the screen are two buttons: 'Back' and 'Next'.

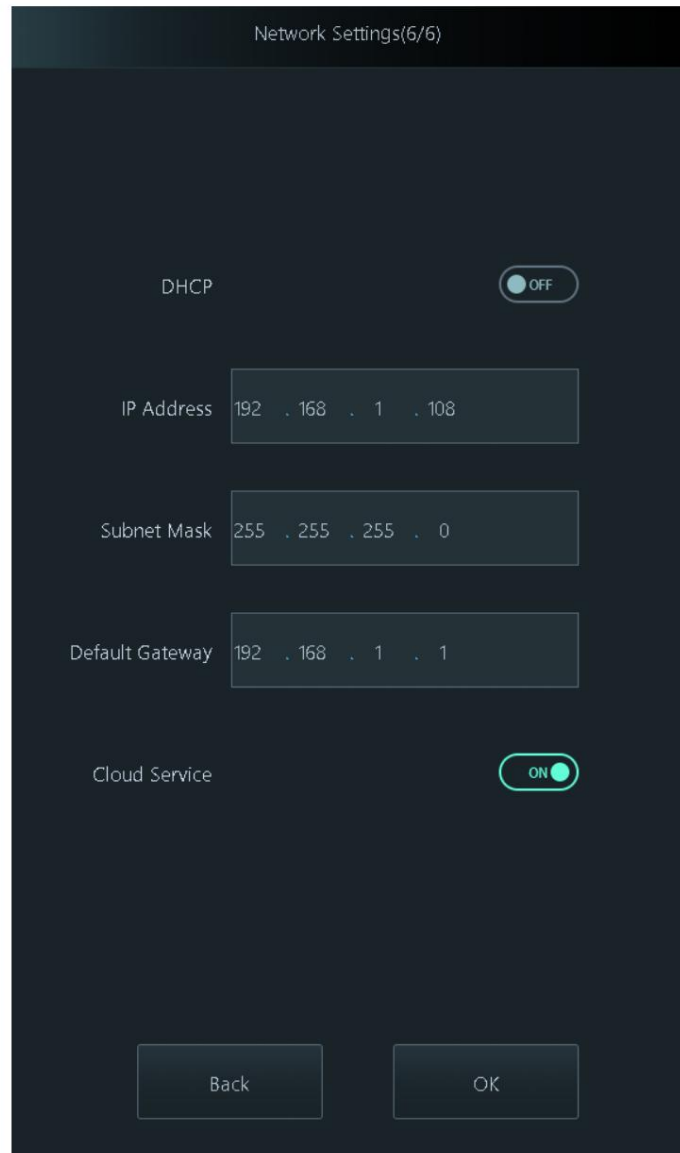
Шаг 7. Настройте параметры сети, а затем нажмите ОК.



Чтобы пропустить этот шаг, нажмите кнопку «Пропустить» в правом верхнем углу экрана.

- DHCP: Система автоматически назначает IP-адрес, маску подсети и шлюз по умолчанию для устройства.
- Облачный сервис: Включите эту функцию, и устройство сможет подключиться к облаку и... работает через мобильное приложение.

Рисунок 2-7. Настройка сети.



2.3 Экран ожидания

Дверь можно открыть с помощью распознавания лиц, карт, паролей и QR-кода. Также можно совершать звонки через функцию домофона. Способы разблокировки могут отличаться в зависимости от модели устройства.

Изменить тему главного экрана можно только через веб-страницу устройства. Подробнее см. раздел «3.13 Персонализация». В этом разделе в качестве примера используется общий режим.



Данное руководство носит исключительно справочный характер. Между экраном в режиме ожидания, описанным в данном руководстве, и фактическим устройством могут быть незначительные различия.

Рисунок 2-8. Экран ожидания

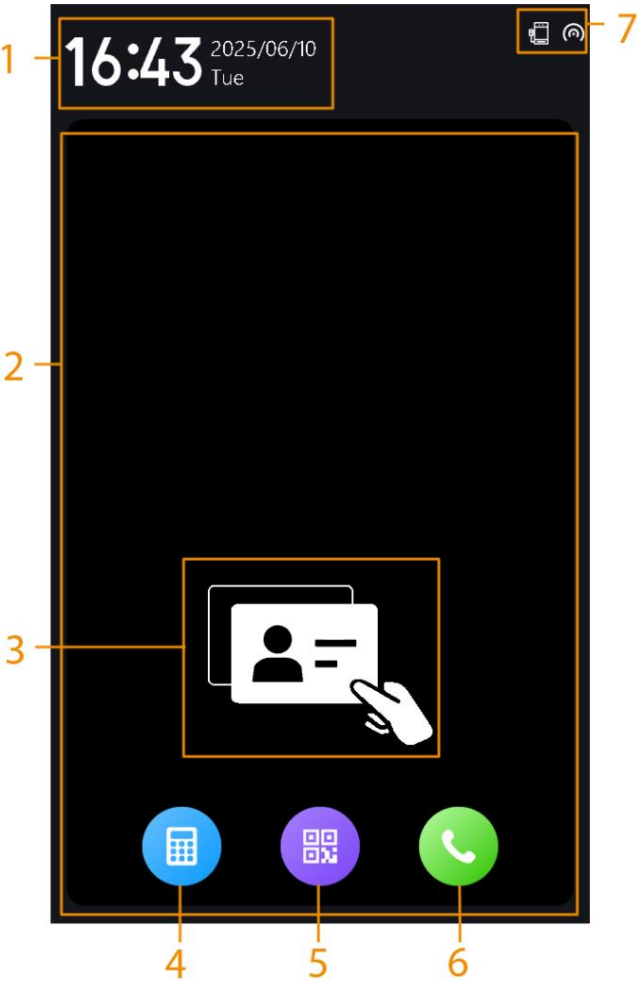
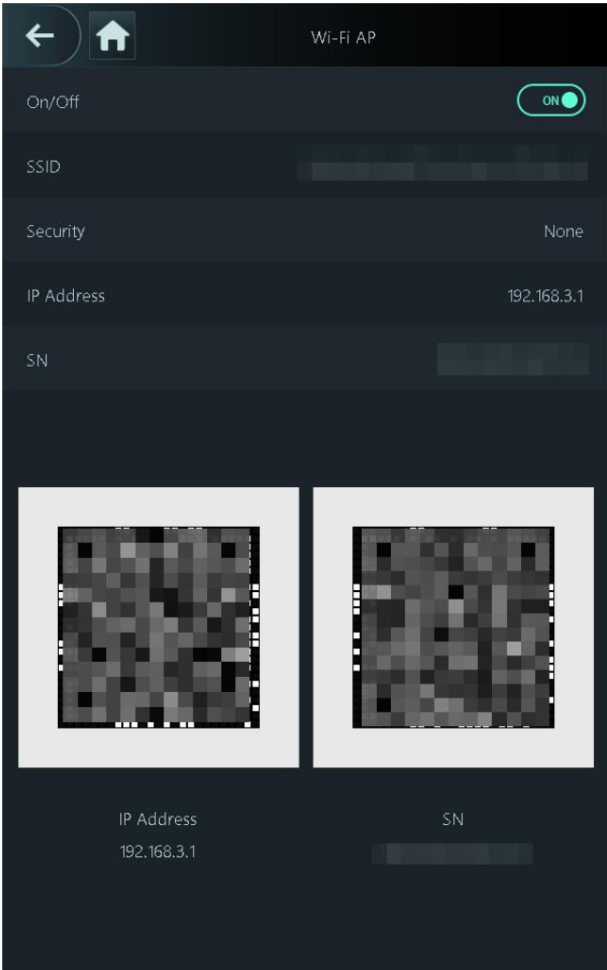


Таблица 2-2. Описание главного экрана.

Нет.	Описание	
1	Текущая дата и время.	
2	Область распознавания лица.	
3	Зона считывания карт.	
4	Введите пароль пользователя, публичный пароль или временный пароль, чтобы открыть дверь.	Вы можете повернуть включить или выключить функции через Система > Экран Настройки > Главный экран Конфигурация.
5	Нажмите на значок QR-кода и отсканируйте QR-код, чтобы открыть дверь.  Для моделей, имеющих автономный модуль QR-кода или функцию подключения. Если модуль расширения для QR-кодов не будет отображаться, значок отображаться не будет. Вы можете Просто поместите свой QR-код перед объективом устройства или Модуль расширения будет автоматически отсканирован.	

Нет.	Описание	
6	• Когда устройство функционирует как сервер, оно может вызывать VTO. и VTH. • Когда платформа управления функционирует как сервер, Устройство может вызывать VTO, VTS и платформу управления. • При работе с DMSS, он может вызывать DMSS.	
7	Отображает состояние Wi-Fi, сети, модуля расширения, USB и других устройств. Wi-Fi и модули расширения доступны только в некоторых моделях. Вы можете нажать , чтобы перейти к экрану точек доступа Wi-Fi. Подробности см. в разделе "2.13.1.4 Настройка Wi-Fi". • QR-код IP-адреса точки доступа Wi-Fi: После подключения телефона к точке доступа устройства откройте браузер на телефоне и отсканируйте QR-код, чтобы получить доступ к устройству и настроить параметры. • QR-код серийного номера: При подключении устройства к экстранету вы можете использовать соответствующее приложение для сканирования QR-кода и добавления этого устройства.	

Рисунок 2-9 Точка доступа Wi-Fi



2.4 Общие значки

Таблица 2-3. Описание значков.

Икона	Описание
	Значок главного меню.
	Значок подтверждения.
	Переверните страницу на первую страницу списка.
	Переверните страницу на последнюю страницу списка.
 или 	Перейдите на предыдущую страницу списка.
 или 	Переверните страницу списка.
	Вернуться в предыдущее меню.
	Включать.
	Выключать.
	Удалить.
	Поиск.

2.5 Вход в систему

Для настройки устройства войдите в главное меню. Доступ к главному меню устройства имеют только учетные записи администратора. При первом использовании для входа в главное меню используйте учетную запись администратора, после чего вы сможете создать другие учетные записи администратора.

Справочная информация

- Учетная запись администратора: может войти в главное меню устройства, но не имеет прав доступа к дверям.
- Учетная запись администратора: может войти в главное меню устройства и имеет права доступа к дверям.
- разрешения.

Процедура

Шаг 1 Нажмите и удерживайте кнопку на экране ожидания в течение 1,5 секунд.

Шаг 2 Выберите способ подтверждения для входа в главное меню.

- Лицо: Вход в главное меню с помощью распознавания лица.
- Отпечаток пальца: Вход в главное меню с помощью отпечатка пальца.

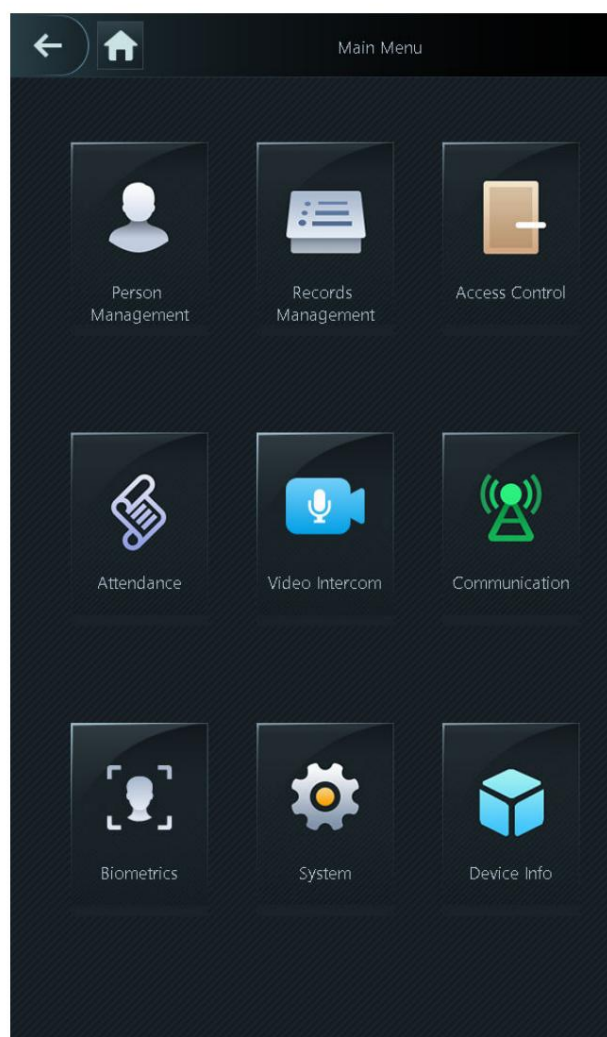


Функция сканирования отпечатков пальцев доступна только на некоторых моделях.

- Карта: Чтобы войти в главное меню, проведите картой.
- Пароль: Введите логин и пароль администратора.
- admin: Введите пароль администратора для входа в главное меню.

После успешной проверки отображается главное меню.

Рисунок 2-10. Главное меню



2.6 Сброс пароля

Если вы забыли пароль для входа в систему администратора, его можно восстановить двумя следующими способами.

Вы настроили зарезервированный адрес электронной почты.

1. Нажмите и удерживайте кнопку режима ожидания в течение 1,5 секунд.
2. Нажмите на «Администратор», а затем один раз нажмите на пустое место на экране.
3. Нажмите «Забыли пароль».
4. Прочитайте подсказку на экране, а затем нажмите Enter.
5. Нажмите на QR-код, а затем отсканируйте его.
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 «Далее».

9. Сбросьте и подтвердите пароль.



Пароль должен состоять из 8–32 непустых символов и содержать как минимум два из следующих типов символов: заглавные буквы, строчные буквы, цифра и специальный символ (за исключением ' '). ; : &).

10. Нажмите ОК.

Вы не указали зарезервированный адрес электронной почты.

1. Нажмите и удерживайте кнопку режима ожидания в течение 1,5 секунд.
2. Нажмите на «Администратор», а затем один раз нажмите на пустое место на экране.
3. Нажмите «Забыли пароль».
4. Следуйте инструкциям на экране, чтобы связаться с местным руководителем, службой технической поддержки или получить помощь.

2.7 Методы разблокировки

Дверь можно открыть с помощью распознавания лиц, паролей, отпечатков пальцев, карт и других способов.

- Для контроллера доступа с распознаванием лиц: методы разблокировки могут отличаться в зависимости от устройства. фактическое устройство.
- Для модульного контроллера доступа: для разблокировки двери используйте карту, распознавание лица или пароль. • Для модульного контроллера доступа с модулем расширения для распознавания отпечатков пальцев: если устройство восстановлено до заводских настроек, по умолчанию используются следующие методы разблокировки: карта, распознавание лица, пароль или отпечаток пальца.



Если модульный контроллер доступа подключен к модулю расширения, и устройство не восстанавливает заводские настройки, то по умолчанию разблокировка устройства осуществляется с помощью карты, распознавания лица или пароля.

2.7.1 Разблокировка с помощью карт

Вставьте карту в зону считывания, чтобы разблокировать дверь.



Эта функция доступна только на некоторых моделях.

2.7.2 Разблокировка по лицу

Подтвердите личность человека, обнаружив его лицо. Убедитесь, что лицо находится в центре кадра обнаружения лица.

2.7.3 Разблокировка по отпечатку пальца

Приложите палец к сканеру отпечатков пальцев.



Эта функция доступна только для некоторых моделей.

2.7.4 Разблокировка с помощью пароля пользователя

Введите логин и пароль, чтобы открыть дверь.

Процедура

 Шаг 1. Коснитесь экрана ожидания.

 Шаг 2. Нажмите «Пароль пользователя».

Если в настройках контроля доступа включена функция «Общий пароль», выполните этот шаг.

 Шаг 3. Введите зарегистрированный или отправленный идентификатор пользователя и пароль, а затем нажмите ОК.

После успешной проверки дверь открывается.

Если вы включите аутентификацию по PIN-коду через раздел «Контроль доступа» > «Параметры контроля доступа» на веб-странице устройства, вы сможете подтвердить свою личность с помощью пароля без ввода идентификатора пользователя.

2.7.5 Разблокировка с помощью открытого пароля

Для разблокировки двери введите только общедоступный пароль. Дверь можно разблокировать с помощью общедоступного пароля, за исключением постоянно закрытой двери. Одно устройство позволяет использовать только один общедоступный пароль.

Предварительные требования

Пароль для общего доступа был настроен. Подробности см. в разделе "2.10.2 Настройка пароля для общего доступа".

Процедура

 Шаг 1. Нажмите на экране ожидания.

«Публичный пароль», затем введите публичный пароль.

 Шаг 3. Нажмите .

После успешной проверки дверь открывается.



Если для разблокировки двери установлено значение «всегда закрыта», то использовать общедоступный пароль нельзя.

2.7.6 Разблокировка по Bluetooth

Дверь можно разблокировать через Bluetooth с помощью приложения DMSS.



Эта функция доступна только на некоторых моделях.

Подготовьте следующие вещи.

- Bluetooth включен. Подробности см. в разделе "3.11.2 Настройки Bluetooth".
- Устройство добавлено в приложение DMSS. Подробности см. в соответствующем руководстве пользователя.

Откройте дверь через приложение DMSS. Голосовое сообщение «Успешно открыто» означает, что дверь открывается, и вы можете войти.

2.7.7 Разблокировка с помощью временного пароля

Откройте дверь с помощью временного пароля.

Процедура

Шаг 1. Добавьте устройство в DMSS.

DMSS сгенерирует временный пароль, который позволит вам разблокировать дверь до истечения срока его действия.

Шаг 2. На главном экране нажмите , а затем нажмите «Временный пароль».

Шаг 3. Введите временный пароль, а затем нажмите .

2.7.8 Разблокировка с помощью QR-кода

Воспользуйтесь QR-кодом, чтобы открыть дверь.



Метод использования QR-кода доступен при использовании устройства с модулем для посетителей системы поддержки принятия решений (DSS).

-  Затем поднесите QR-код к объективу, чтобы разблокировать дверь.
- Прикоснитесь • Поднесите QR-код непосредственно к линзе, чтобы разблокировать дверь.
- Если вы выберете «Турникет» в разделе «Настройки связи» > «Настройки RS-485», вы сможете проверить QR-код на внешнем модуле QR-кодов, подключенном к турникету, чтобы разблокировать дверь.

2.8 Управление персоналом

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



Изображения в данном руководстве приведены только для ознакомления и могут отличаться от реального изделия.

2.8.1 Настройка отделов

По умолчанию существует 20 отделов. Мы рекомендуем переименовать их для удобства различения отделов.



Добавить или удалить отдел невозможно.

Процедура

Шаг 1. Выберите «Управление персоналом» > «Настройки отдела».

Шаг 2. Выберите отдел, а затем переименуйте его.

Рисунок 2-11. Переименование отделов.



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

Шаг 3 Нажмите . 

2.8.2 Добавление пользователей

Процедура

Шаг 1. В главном меню выберите «Управление персоналом» > «Создать пользователя».

Шаг 2. Настройте параметры интерфейса.



Параметры могут различаться в зависимости от модели устройства.

Рисунок 2-12. Добавить пользователя.

←

Add User

✓

ID

1

Name

Verification Mode

Same as Device

Unlock Method

Card, Face or Password

Face

0

Card

0

Password

User Permission

User

General Plan

255-Default

Holiday Plan

255-Default

Validity Period

2037-12-31

User Type

General User

Permission Type

Unlock and Attendance

<

1/1

>

Таблица 2-4. Описание параметров.

Параметр	Описание
Идентификатор	Идентификатор пользователя подобен идентификатору сотрудника и может состоять из цифр, букв и их символов. комбинации, а максимальная длина номера составляет 30 символов.
Имя	Имя может содержать до 32 символов (включая цифры, символы и т. д.). буквы).

Параметр	Описание
Режим проверки	Настройте режим проверки для пользователя. Вы можете использовать режим, совпадающий с режимом устройства, или настроить свой собственный.
Способ разблокировки	- Аналогично устройству : режим работы совпадает с режимом работы устройства. Разблокировка Метод нельзя редактировать. - Пользовательский : После выбора «Пользовательский» вы можете настроить способ разблокировки. Выберите способ комбинации и разблокируйте необходимые способы. - Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы открыть дверь. - И ещё: используйте все выбранные способы разблокировки, чтобы открыть дверь.  - Настраиваемый режим проверки действителен только для локального устройства. Он не может использоваться во внешних считывателях карт. - Если пользовательский режим проверки отличается от режима устройства, приоритет отдается пользовательскому режиму.
Отпечаток пальца	Регистрация отпечатков пальцев. Пользователь может зарегистрировать до 3 отпечатков пальцев, и вы можете назначить один из них в качестве отпечатка для вызова помощи. Сигнализация сработает, когда отпечаток пальца будет использован для разблокировки двери.  - Функция распознавания отпечатков пальцев доступна только на некоторых моделях. - Функция распознавания отпечатков пальцев доступна, если модульное устройство подключено к модулю распознавания отпечатков пальцев. - Мы не рекомендуем устанавливать первый отпечаток пальца в качестве принудительного отпечатка пальца. Один пользователь может установить только один отпечаток пальца для принудительного снятия давления.
Лицо	Расположите лицо внутри рамки, и изображение лица будет автоматически запечатлено. Вы можете зарегистрироваться снова, если вас что-то не устроит. исход.
Карта	Пользователь может зарегистрировать максимум 5 карт. Введите номер карты или проведите картой по считывателю, после чего устройство считывает информацию о карте. Вы можете включить функцию «Карта принуждения». Сигнализация сработает, если для разблокировки двери будет использована карта принуждения.  - Эта функция доступна только на некоторых моделях. - Один пользователь может установить только одну карту принуждения.
Bluetooth-карта	Для каждого пользователя можно зарегистрировать 5 Bluetooth-карт. На странице регистрации карты выберите опцию «Запрос по электронной почте или с помощью регистрационного кода», чтобы зарегистрировать свою Bluetooth-карту.
Пароль	Введите пароль пользователя. Максимальная длина пароля — 8 цифр. Пароль принуждения — это прибавление 1 к последней цифре пароля разблокировки. Например, если пароль пользователя — 12345, то пароль для принудительного открытия двери будет 12346; если пароль пользователя — 789, то пароль для принудительного открытия двери будет 780. Сигнализация сработает, когда для разблокировки двери будет использован пароль для принудительного открытия.

Параметр	Описание
Разрешение пользователя	- Пользователь : Пользователи имеют только права доступа к дверям или учета рабочего времени. - Администратор : Администраторы могут настраивать устройство, помимо доступа к дверям и т. д. Разрешения на посещение.
Генеральный план	В течение установленного периода люди могут открывать дверь или отмечать присутствие. Подробную информацию о настройке периодов см. в разделе «3.7.6.1 Настройка общего плана».
План на отпуск	В дни установленных праздников посетители могут открывать двери или отмечать присутствие. Подробную информацию о настройке праздничных дней см. в разделе "3.7.6.2 Настройка плана праздничных дней".
Срок действия	Укажите дату, когда истекает срок действия разрешений на доступ к двери и учет рабочего времени данного лица.
Тип пользователя	- Обычный пользователь : Обычные пользователи могут открыть дверь. - Пользователь из черного списка : Когда пользователи из черного списка открывают дверь, происходит открытие двери. Будет активирована сигнализация. - Гостевой пользователь : Гости могут открыть дверь в течение определенного периода времени или на определенное количество раз. По истечении установленного периода или по истечении времени разблокировки, открыть дверь будет невозможно. - Патрульный пользователь : Патрульные пользователи могут отмечать посещаемость на устройстве, но они не имеют доступа к двери. - VIP-пользователь : Когда VIP-пользователь открывает дверь, на него не распространяются ограничения по времени и способу открытия. - Другой пользователь : Когда он откроет дверь, она останется открытой в течение 5 минут. ещё несколько секунд.  Эта функция не работает, если включена удаленная проверка. - Пользователь 1/Пользователь 2 : Аналогично обычным пользователям.
Тип разрешения	- Открытие и учет присутствия: У пользователя есть разрешение на учет присутствия, и он может открыть дверь, используя настроенные методы проверки. - Учет присутствия: У пользователя есть только разрешение на учет присутствия, и он не может открыть дверь. После успешной проверки личности пользователя создается одна запись о неудачной попытке открытия.
Отделение	Выберите отделы, что полезно при настройке расписаний работы отделов. Инструкции по созданию отделов см. в разделе "2.8.1 Настройка отделов".  Эта функция доступна только на некоторых моделях.

Параметр	Описание
Режим расписания	• Расписание отдела: Применяет расписание отдела к пользователю. • Личное расписание: Применяет личное расписание к пользователю. Инструкции по настройке личных или departmental графиков см. в разделе "2.11.3 Настройка графиков работы".  ◆ Эта функция доступна только на некоторых моделях. ◆ Если вы установите здесь режим расписания на «расписание отдела», то персональное расписание, настроенное для пользователя в разделе «Учет посещаемости > Настройка расписания > Персональное расписание», станет недействительным.

Шаг 3 Нажмите . 

2.8.3 Просмотр информации о пользователе

Процедура

Шаг 1. В главном меню выберите «Управление персоналом» > «Список пользователей» или выберите «Персонал». Управление > Список администраторов.

Шаг 2. Просмотрите все добавленные учетные записи пользователей и администраторов.

- : Разблокировка с помощью пароля.
-  Разблокировка осуществляется с помощью считывания карты.
- : Разблокировка с помощью распознавания лица. • :
- Разблокировка с помощью отпечатка пальца.

Рисунок 2-13 Список пользователей

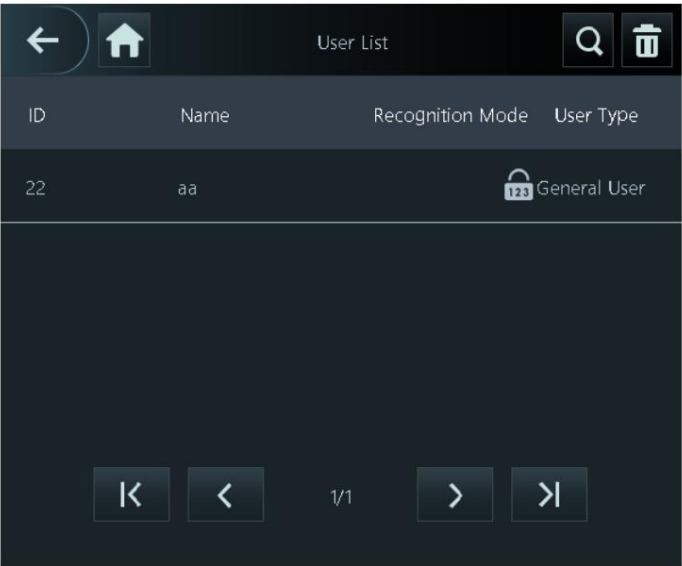
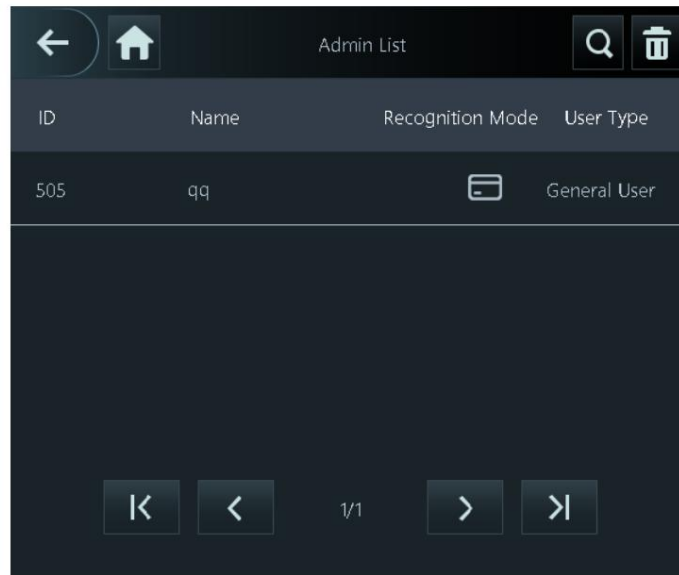


Рисунок 2-14 Список администраторов



Связанные операции

На экране «Пользователи» вы можете управлять добавленными пользователями.

- Поиск пользователей: Нажмите и введите имя пользователя или идентификатор пользователя. • Редактирование пользователей: Нажмите на пользователя, чтобы отредактировать его информацию.
- Удаление пользователей

- ◇ Удалять по одному: выберите пользователя, а затем нажмите
- ◇ Удаление партиями:

- На экране «Список пользователей» нажмите, чтобы удалить всех пользователей. •

На экране «Список администраторов» нажмите, чтобы удалить всех администраторов.

2.9 Управление документацией

Вы можете настроить сохранение записи о разблокировке, поиск записей о разблокировке, а также экспорт записей о разблокировке и посещаемости.

2.9.1 Хранение записей о разблокировке

Процедура

Шаг 1. В главном меню выберите пункт «Управление записями».

Шаг 2. Включите или выключите сохранение записей о разблокировке.

Записи, доступные для разблокировки, сохраняются по умолчанию. Если вы отключите эту функцию, записи не смогут быть сохранены на этом устройстве.

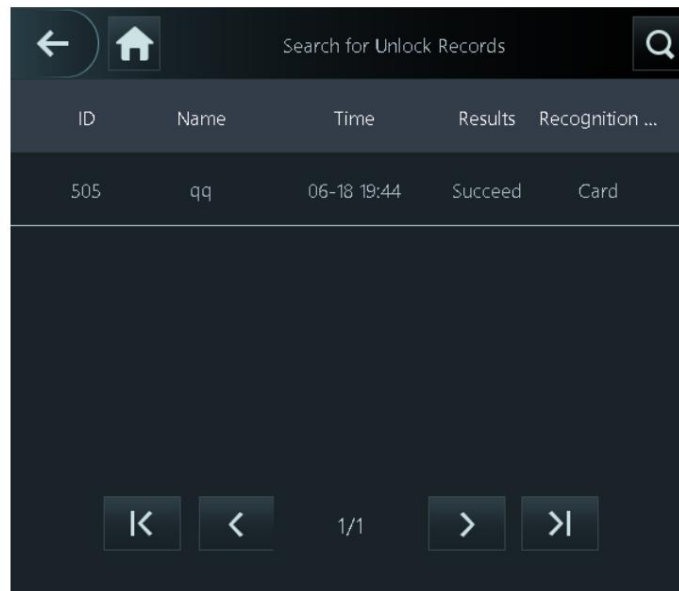
2.9.2 Поиск записей разблокировки

Процедура

Шаг 1. В главном меню выберите «Управление записями» > «Найти разблокировку записей».

Отображаются записи о разблокировке, включая идентификатор, имя, время разблокировки, результаты и метод распознавания.

Рисунок 2-15. Поиск записей о разблокировке.



Шаг 2 Нажмите



Для поиска записи введите имя пользователя и его идентификатор.

2.9.3 Экспорт записей разблокировки

Процедура

Шаг 1 Вставьте USB-накопитель в USB-порт устройства.

Шаг 2 В главном меню выберите «Управление записями» > «Экспорт разблокированных записей».

Шаг 3. Выберите время начала и время окончания, а затем нажмите.



Файл в формате .xml экспортируется.

Рисунок 2-16 Экспорт записей разблокировки



Связанные операции

Чтобы просмотреть экспортированные данные, необходимо открыть Excel, выбрать «Файл» > «Открыть», а затем выбрать экспортированный файл в формате .xml.

2.9.4 Экспорт данных о посещаемости

Вы можете экспортировать данные о сменах, расписаниях, посещаемости за месяц и аномальной посещаемости.

Процедура

Шаг 1 Вставьте USB-накопитель в USB-порт устройства.

Шаг 2 В главном меню выберите «Управление записями» > «Экспорт записей о посещаемости».

Шаг 3. Выберите данные для экспорта.

Файл в формате .xml экспортируется на USB-накопитель.

Связанные операции

Чтобы просмотреть экспортированные данные, необходимо открыть Excel, выбрать «Файл» > «Открыть», а затем выбрать экспортированный файл в формате .xml.

2.10 Управление контролем доступа

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

В главном меню нажмите «Контроль доступа», чтобы перейти к экрану «Управление контролем доступа».

2.10.1 Настройка метода разблокировки

2.10.1.1 Настройка комбинаций разблокировки

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

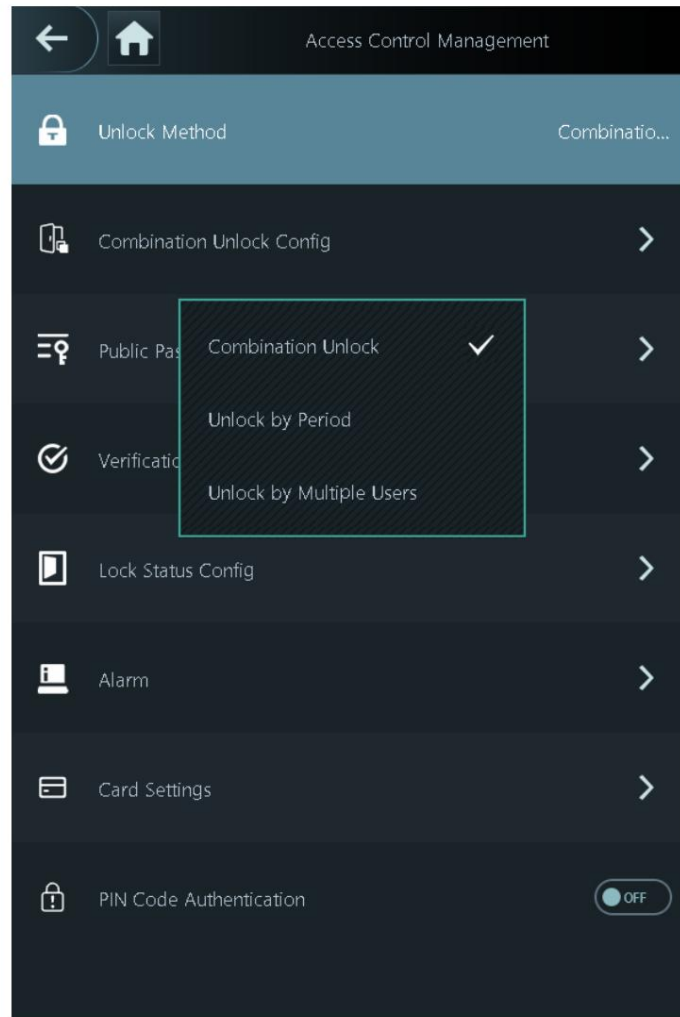
Процедура

Шаг 1. Выберите «Контроль доступа».

Шаг 2. Нажмите «Разблокировка комбинацией» рядом с пунктом «Способ разблокировки», а затем выберите «Комбинация».

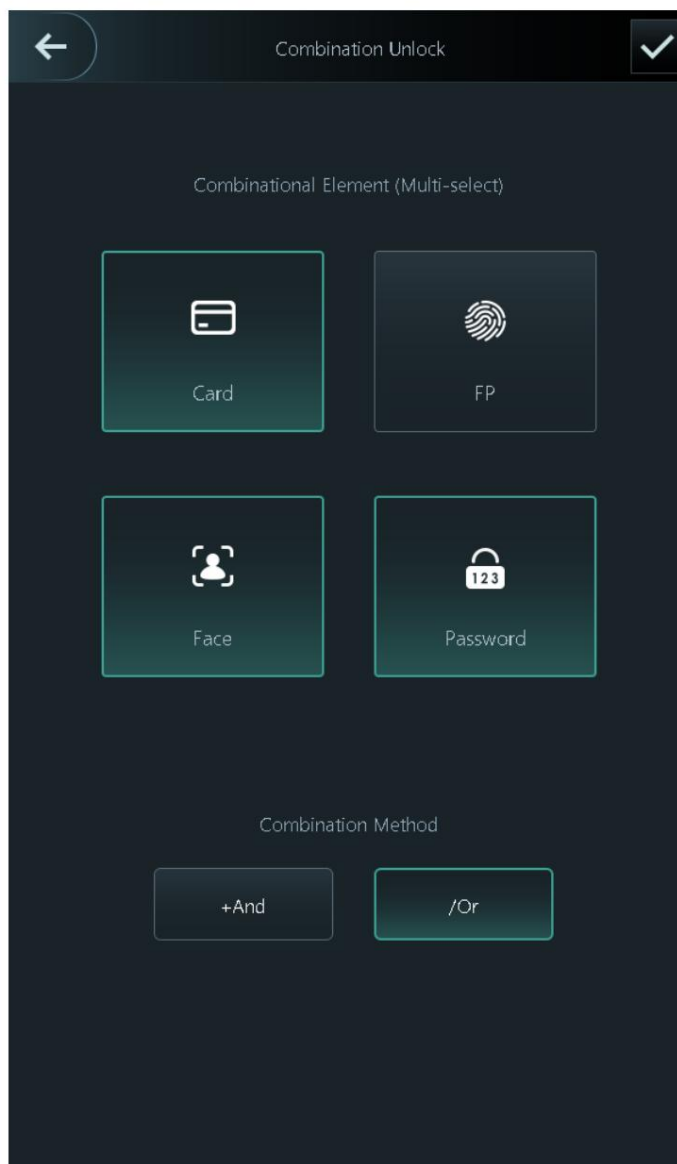
Разблокировать из списка.

Рисунок 2-17. Комбинированная разблокировка.



Шаг 3. Нажмите «Настройка разблокировки комбинацией» и выберите методы разблокировки.

Рисунок 2-18. Способ разблокировки.



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

Чтобы отменить выбор, снова коснитесь выбранного метода.

- +И :

Проверьте все выбранные способы разблокировки, чтобы открыть дверь.



Пользователи должны пройти верификацию в следующем порядке: карта, отпечаток пальца, распознавание лица и пароль.

- /Или : Выберите один из способов разблокировки, чтобы открыть дверь.

Шаг 5. Нажмите, чтобы  сохранить изменения.

2.10.1.2 Настройка разблокировки по периоду

Процедура

Шаг 1. Выберите «Контроль доступа».

Шаг 2. Нажмите «Разблокировка комбинацией» рядом с пунктом «Способ разблокировки», а затем выберите «Разблокировка по периоду» из списка.

Подробную информацию о настройке разблокировки по периодам см. в разделе "3.7.1.2 Настройка методов разблокировки".

Шаг 3. Нажмите, что  сохранить изменения.

2.10.1.3 Настройка разблокировки для нескольких пользователей

Процедура

Шаг 1. Выберите «Контроль доступа».

Шаг 2. Нажмите «Комбинированная разблокировка» рядом с пунктом «Способ разблокировки», а затем выберите из списка «Разблокировка несколькими пользователями» .

Подробную информацию о настройке разблокировки для нескольких пользователей см. в разделе "3.7.1.2 Настройка методов разблокировки".

Шаг 3. Нажмите, что  сохранить изменения.

2.10.2 Настройка публичного пароля

Вы можете открыть дверь, введя только общедоступный пароль. Этот пароль не ограничен типами пользователей. Для одного устройства разрешен только один общедоступный пароль разблокировки.

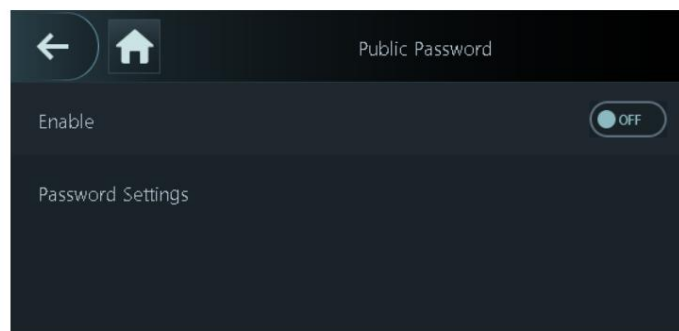
Процедура

Шаг 1. Выберите «Контроль доступа».

Шаг 2. Нажмите «Настройки пароля», введите пароль, а затем нажмите .



Рисунок 2-19. Открытый пароль



Шаг 3. Включите функцию публичного пароля.

2.10.3 Настройка интервала проверки

Если вы подтверждаете свою личность несколько раз в течение определенного периода, действительной будет считаться только самая ранняя проверка, и дверь не откроется после второй или последующих проверок. Повторная проверка личности возможна только по истечении заданного периода.

Процедура

Шаг 1. Выберите «Контроль доступа».

Шаг 2. Нажмите «Интервал проверки (сек)», введите временной интервал, а затем нажмите .



2.10.4 Настройка состояния блокировки

Процедура

Шаг 1. Выберите «Контроль доступа» > «Настройка состояния блокировки».

Шаг 2. Установите состояние двери.

Рисунок 2-20. Состояние блокировки.

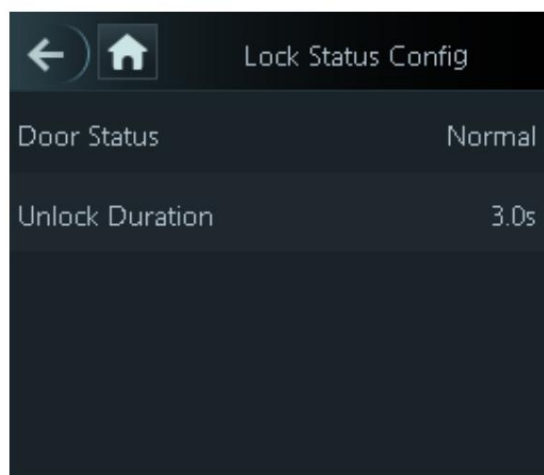


Таблица 2-5. Описание параметров.

Параметр	Описание
Состояние двери	• Нормально открыто : Дверь постоянно остается незапертой. • Нормально закрыто : Дверь постоянно остается запертой. • Обычный режим : Если выбран обычный режим , дверь будет запирается и отпираться в соответствии с вашими настройками.
Длительность разблокировки	После того, как человеку будет предоставлен доступ, дверь останется открытой в течение определенного времени, чтобы он мог пройти.

2.10.5 Настройка сигналов тревоги

Сигнализация сработает при несанкционированном доступе к входу или выходу.

Процедура

Шаг 1. Выберите «Контроль доступа» > «Сигнализация».

Шаг 2. Включите этот тип сигнализации.



Типы сигналов тревоги могут различаться в зависимости от модели изделия.

Рисунок 2-21 Сигнал тревоги

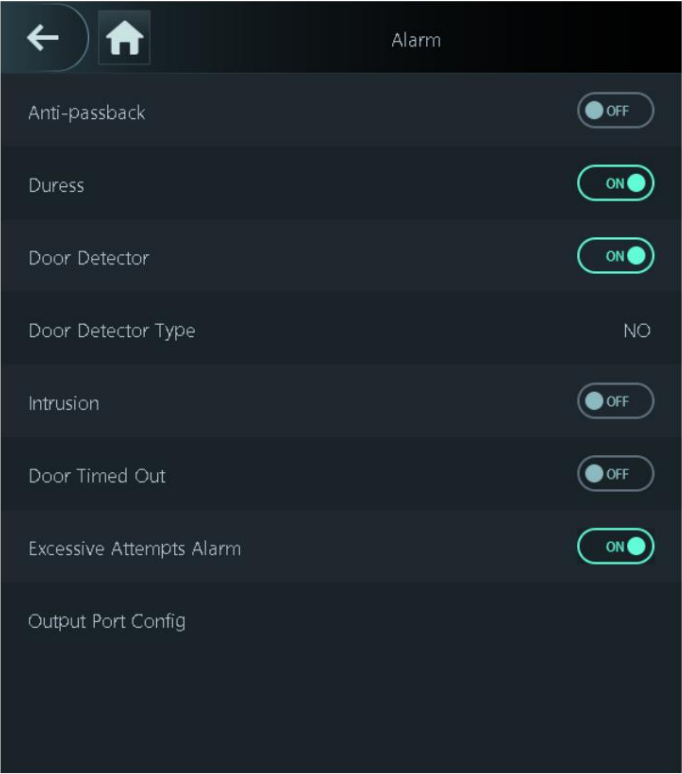


Таблица 2-6. Описание параметров тревоги.

Параметр	Описание
Защита от повторного прохода	Пользователи должны подтвердить свою личность как при входе, так и при выходе; в противном случае сработает сигнализация. Это помогает предотвратить передачу карты другими лицами для предоставления доступа. При включении функции защиты от повторного прохода владелец карты должен покинуть охраняемую зону через считыватель на выходе, прежде чем система снова предоставит ему доступ. Для входа в охраняемую зону необходимо провести картой через считыватель «на вход», а для выхода — через считыватель «на выход». • Если человек входит после проверки, но выходит, не пройдя проверку Если их действия будут подтверждены, сработает сигнализация, и им будет отказано в доступе. • Если человек входит без проверки, но выходит после проверки Если их действия будут подтверждены, сработает сигнализация, и им будет отказано в доступе.  Если устройство может подключиться только к одному замку, проверка через устройство означает, что человек вошел в направлении «вход», а проверка через внешний считыватель карт означает, что он вышел в направлении «выход». Это значение по умолчанию.
Принуждение	Сигнализация сработает при использовании карты принудительного вызова, пароля принудительного вызова или отпечатка пальца для разблокировки двери.

Параметр	Описание
Детектор двери	При подключении дверного датчика к вашему устройству, сигнализация может срабатывать при ненормальном открытии или закрытии дверей. Существует 2 типа дверных датчиков: нормально замкнутые (NC) и нормально разомкнутые (NO) датчики.
Тип дверного датчика	- Нормально замкнутый: В этом режиме короткое замыкание в датчике указывает на то, что дверь открыта. - Нормально разомкнутый: В этом режиме разомкнутая цепь указывает на то, что дверь открыта.
Вторжение	Если дверь открывается ненормально, сработает охранная сигнализация, которая будет гореть в течение определенного времени.
Дверь закрыта по истечении времени.	Если дверь остается незапертой дольше заданного времени, сработает сигнализация об истечении времени ожидания, которая будет действовать в течение заданного времени.
Продолжительность ожидания открытия двери	 Датчик открытия двери и функция автоматического закрытия двери должны быть включены одновременно.
Сигнализация о чрезмерном употреблении	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании нелегальной карты, которая будет гореть в течение определенного времени.
Конфигурация выходного порта	Выберите функцию, для которой может использоваться порт. Если выходной сигнал тревоги и функция дверного звонка используют один и тот же кабель, и устройство вывода сигнала тревоги подключено к устройству, выберите «Порт выхода сигнала тревоги» . Если дверной звонок подключен к устройству, выберите «Дверной звонок».  - Если кабель может использоваться для различных функций, используется параметр «Конфигурация порта» . - Функции могут отличаться в зависимости от конкретной модели устройства.

2.10.6 Настройки карты

Процедура

Шаг 1. Выберите «Контроль доступа» > «Настройки карты».

Шаг 2. Настройте параметры карты.

Таблица 2-7. Описание параметров карты.

Параметр	Описание
Карта M1	При включении этой функции карту M1 можно считать.  Эта функция доступна только на некоторых моделях.

Параметр	Описание
Шифрование и проверка карт M1	При включении этой функции можно считать только зашифрованную IC-карту.  Убедитесь, что карта M1 активирована.
FeliCa Card	При включении этой функции карту FeliCa можно считать.  Эта функция доступна только на некоторых моделях.
Удостоверение личности	При включении этой функции удостоверение личности можно считать.  Эта функция доступна только на некоторых моделях.
Карта DESFire	При включении этой функции устройство может считывать номер карты Desfire.  • Эта функция доступна только в моделях, поддерживающих IC-карты. • Поддерживается только шестнадцатеричный формат.
Расшифровка карты DESFire	Информация на карте DESFire может быть прочитана, если одновременно включены функции «Включить карту DESFire» и «Расшифровка карты DESFire» .  • Эта функция доступна только в моделях, поддерживающих IC-карты. • Убедитесь, что карта DESFire включена.

2.10.7 Настройка аутентификации по PIN-коду

Процедура

Шаг 1. Выберите «Контроль доступа» > «Аутентификация по PIN-коду».

Шаг 2. Включите или выключите аутентификацию по PIN-коду.

По умолчанию аутентификация по PIN-коду отключена. Если она включена, дверь можно открыть только с помощью пароля.



После включения аутентификации по PIN-коду вы можете напрямую ввести пароль для подтверждения, не вводя идентификатор пользователя.

2.10.8 Настройка блокировки Lock2

Процедура

Шаг 1. Выберите «Контроль доступа» > «Заблокировать 2».

Шаг 2. Включите или отключите Lock2.



Если вы включите блокировку 2, входной сигнал тревоги будет переключен на датчик двери 2 и кнопку разблокировки 2. Изменения вступят в силу после перезапуска.

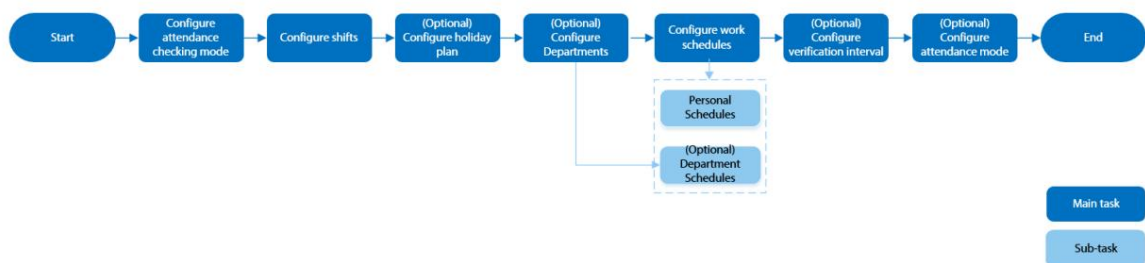
2.11 Управление посещаемостью

Система учета рабочего времени поддерживает управление посещаемостью как на самом устройстве, так и в Smart PSS Lite. В этом разделе настройка учета рабочего времени на устройстве используется только в качестве примера.



Эта функция доступна только на некоторых моделях (устройствах серии 4,3 дюйма).

Рисунок 2-22. Блок-схема конфигурации учета рабочего времени.



2.11.1 Настройка смен

Настройте смены, чтобы определить правила учета рабочего времени. Сотрудники должны приходить на работу к назначенному времени начала смены и уходить к ее окончанию, за исключением случаев, когда они решают работать сверхурочно.

Процедура

Шаг 1. Выберите «Учет посещаемости» > «Настройка смены».

Шаг 2. Выберите смену.



Нажмите, чтобы просмотреть другие смены. Вы можете настроить до 24 смен.

Шаг 3. Настройте параметры смены.

Рисунок 2-23. Настройка смены.

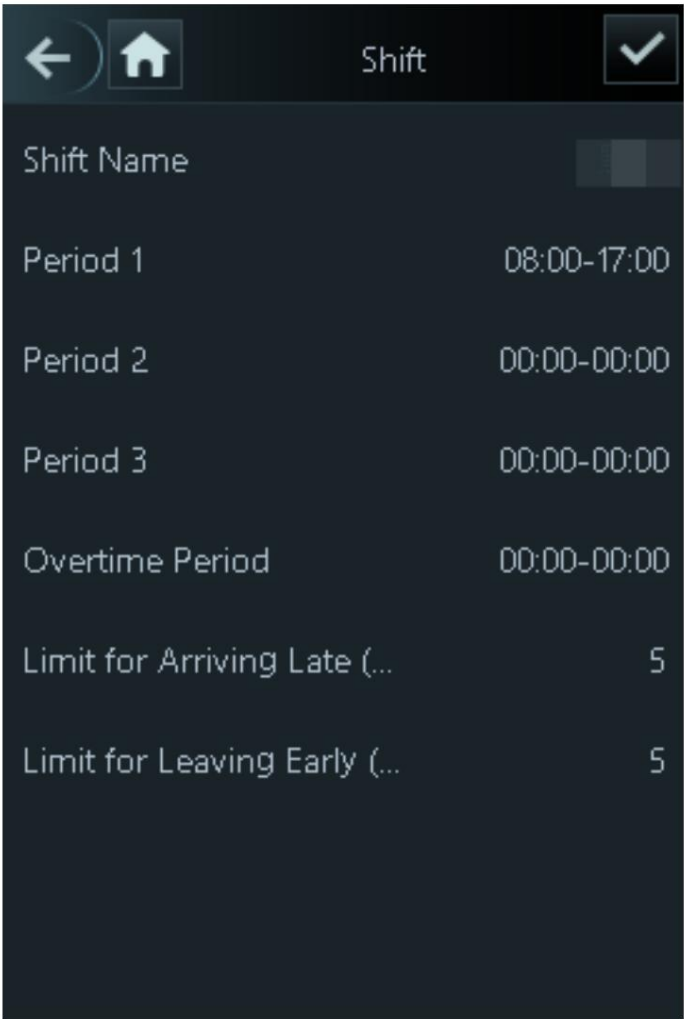


Таблица 2-8. Описание параметров переключения.

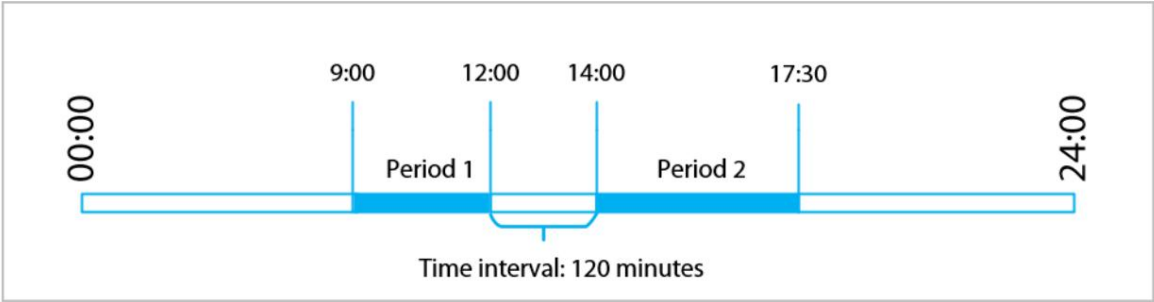
Параметр	Описание
Название смены	Введите название смены.

Параметр	Описание
Период 1	Укажите временной диапазон, в течение которого сотрудники могут отмечать начало и конец рабочего дня. Необходимо настроить как минимум один период. • Если вы установили только один период учета рабочего времени, сотрудники должны отмечать начало и конец рабочего дня в установленное время, чтобы избежать ошибок в их табелях учета рабочего времени. Например, если вы установили период с 08:00 до 17:00, сотрудники должны отметить начало рабочего дня до 08:00 и конец рабочего дня с 17:00 и далее. • Если вы установили 2 периода учета рабочего времени, эти 2 периода не могут быть использованы. Периоды частично совпадают. Сотрудники должны отмечать время прихода и ухода за оба периода. • Если вы зададите 3 периода, они не должны перекрываться. Сотрудники должны отмечать начало и конец рабочего дня для двух смежных периодов.  Последний период может охватывать несколько дней. Если период сверхурочной работы является последним, вы можете настроить его таким образом, чтобы он охватывал несколько дней.
Период 2	
Период 3	
Период сверхурочной работы	Сотрудники, отмечающие время прихода и ухода с работы в течение установленного периода, будут считаться работающими сверх своего обычного рабочего времени.
Ограничение на опоздание (мин)	Сотрудникам может быть предоставлено определенное время для того, чтобы они могли немного опоздать на работу и немного раньше уйти. Например, если обычное время начала работы — 08:00, то допустимый период в 5 минут может быть установлен для сотрудников, прибывших к 08:05, чтобы их не считали опоздавшими.
Ограничение на досрочный отъезд (мин)	

Если вы настраиваете несколько периодов, обратитесь к приведенным ниже инструкциям для выполнения функции учета рабочего времени.

- Если интервал времени между двумя периодами четный, можно разделить его на 2 и отнести первую половину интервала к первому периоду в качестве времени окончания работы. Вторую половину интервала следует отнести ко второму периоду в качестве времени начала работы.

Рисунок 2-24. Временной интервал (четное число).



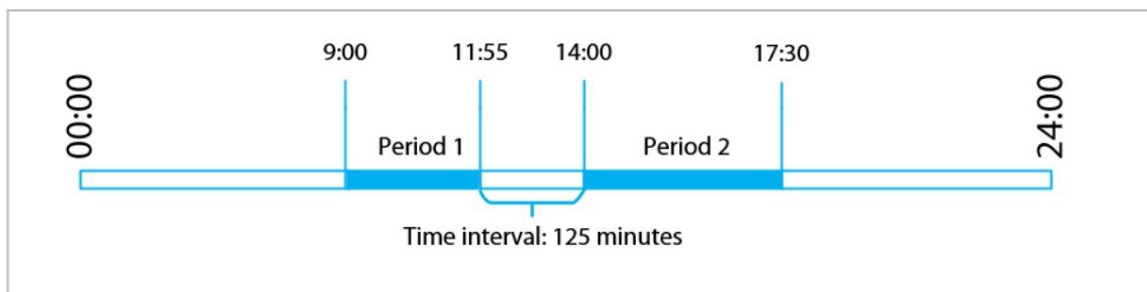
Например: если интервал составляет 120 минут, то время окончания работы в период 1 — с 12:00 до 12:59, а время начала работы в период 2 — с 13:00 до 14:00.



Если сотрудник несколько раз отмечает свой уход в течение первого периода, будет действовать самое позднее время, а если он несколько раз отмечает свой приход в течение второго периода, будет действовать самое раннее время.

- Если интервал времени между двумя периодами нечетный, то наименьшая часть интервала будет отнесена к первому периоду и будет являться временем окончания работы. Наибольшая часть интервала будет отнесена ко второму периоду и будет являться временем начала работы.

Рисунок 2-25. Временной интервал (нечетное число).



Например: если интервал составляет 125 минут, то время окончания первого периода — с 11:55 до 12:57, а время начала второго периода — с 12:58 до 14:00. Первый период длится 62 минуты, а второй — 63 минуты.



Если сотрудник несколько раз отмечает свой уход в течение первого периода, будет действовать самое позднее время, а если он несколько раз отмечает свой приход в течение второго периода, будет действовать самое

раннее время. • Если период только один, и вы не отмечаете свой приход или уход к установленному времени, то считается отсутствующим в течение 1 дня.

- Если периодов несколько, и вы не отмечаете время начала или окончания работы в установленное время. Если вы не отметились при приходе или уходе с работы в установленное время (2 или более периодов), это считается отсутствием на 1 день. Присутствие в сверхурочное время не меняет статус отсутствия.

человек.

Если вы настроили последний период таким образом, чтобы он охватывал несколько дней, обратитесь к приведенным ниже инструкциям для выполнения функции учета рабочего времени.

- Если второй день — обычная смена, посещаемость соответствует обычному графику.
- Если второй день — праздничный день, вы можете отметить свой уход в любое время в течение 24 часов. праздничный день.



Все данные о времени прихода и ухода указаны с точностью до секунды. Например, если обычное время начала работы установлено на 8:05 утра, сотрудник, отметившийся в 8:05:59 утра, не будет считаться опоздавшим. Однако сотрудник, прибывший в 8:06 утра, будет отмечен как опоздавший на 1 минуту.

Шаг 4. Нажмите.



2.11.2 Настройка планов отпусков

Настройте планы отпусков, чтобы установить периоды, когда посещаемость не будет отслеживаться.

Процедура

Шаг 1. Выберите «Учет посещаемости» > «Настройка смен» > «Праздничные дни».

Шаг 2. Нажмите, чтобы добавить планы на отпуск.

Шаг 3. Настройте параметры.

Рисунок 2-26. Создание планов на праздники.

←

Holiday Plan

✓

Attendance Holiday No.

1

Attendance Holiday

Start Time

2023-06-08

End Time

2023-06-08

Таблица 2-9. Описание параметров.

Параметр	Описание
Выходной день, связанный с посещаемостью.	Номер праздника.
Выходной день, связанный с посещаемостью	Название праздника.
Время начала	Время начала и окончания праздника.
Конец времени	

Шаг 4. Нажмите ✓

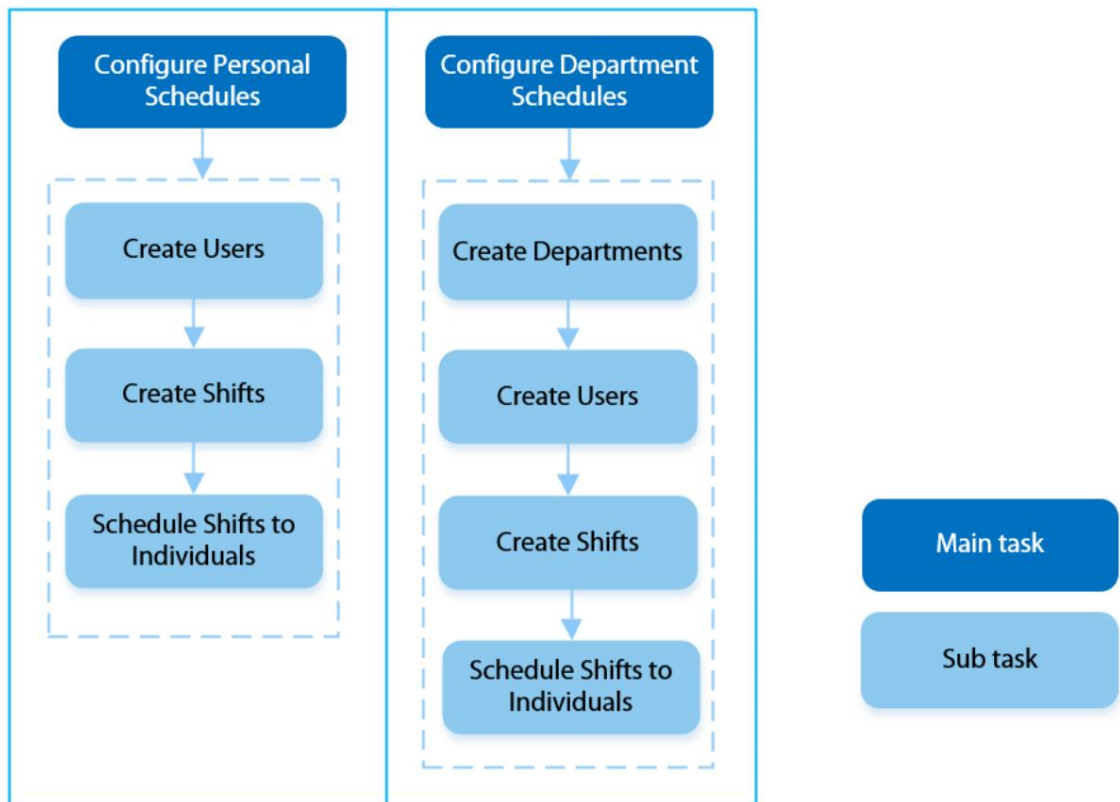
2.11.3 Настройка графиков работы

График работы обычно включает в себя количество дней в месяц и количество часов в день, в течение которых сотрудник должен находиться на рабочем месте. Можно создавать различные типы графиков работы для разных сотрудников или отделов, и в этом случае сотрудники должны следовать установленному графику.

Справочная информация

Для настройки личного или departmental-графика обратитесь к блок-схеме.

Рисунок 2-27. Настройка графиков работы.



Процедура

Шаг 1. Выберите «Учет посещаемости» > «Настройка расписания».

Шаг 2. Составьте рабочие графики для отдельных сотрудников.

1. Нажмите «Личное расписание».
2. Введите идентификатор пользователя, а затем нажмите .
3. В календаре выберите день, а затем выберите смену.

Смена запланирована на этот день.



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

- 0 означает разрыв.
- Цифры от 1 до 24 указывают количество predetermined shifts. Инструкции по настройке смен см. здесь.
См. раздел "2.11.1 Настройка смен".
- 25 означает командировку. • 26 означает отпуск.

Рисунок 2-28. График изменений для отдельных лиц.



4. Нажмите

Шаг 3. Составьте графики работы для отделов.

- 1. Нажмите «Расписание отдела».
- 2. Выберите отдел, а затем выберите смены на неделю.

График смен составлен на неделю.



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

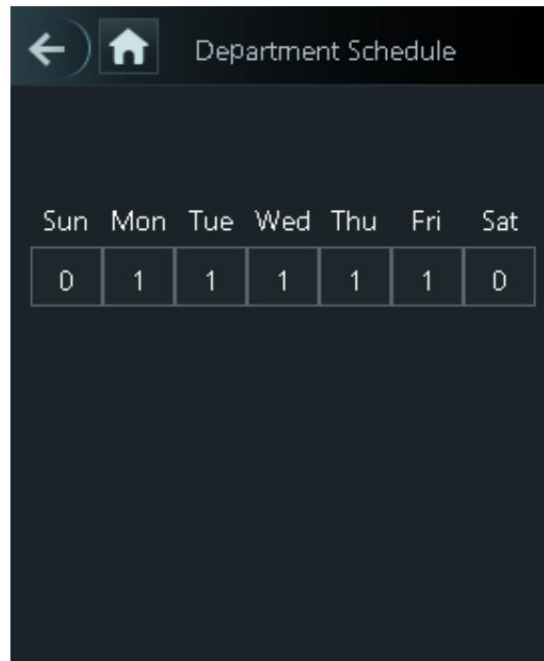
• 0 означает отдых. •

От 1 до 24 указывает номер predetermined смен. Инструкции по настройке смен см. в разделе "2.11.1 Настройка смен". • 25

означает командировку. • 26

означает отпуск.

Рисунок 2-29. График смен в отделе.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
0	1	1	1	1	1	0



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

Шаг 4. Нажмит 

2.11.4 Настройка режимов учета посещаемости

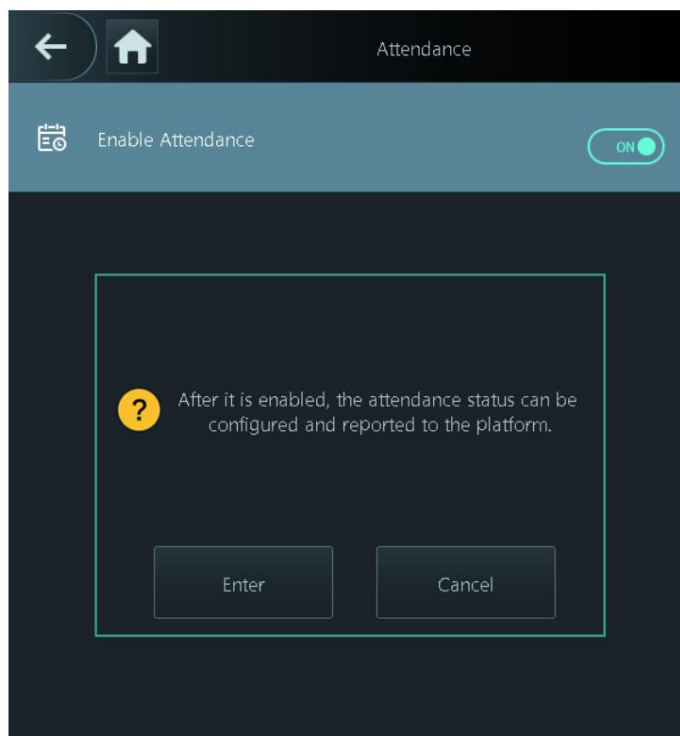
При регистрации начала и окончания рабочего дня вы можете установить режимы учета посещаемости, определяющие статус присутствия.

Процедура

Шаг 1. На главном экране меню нажмите «Посещаемость» .

Шаг 2. Включите функцию.

Рисунок 2-30. Включение учета посещаемости.



Шаг 3. Нажмите «Настройки режима», а затем выберите режим учета посещаемости.

Данные о посещаемости также будут синхронизированы с платформой управления.

Рисунок 2-31 Режим учета посещаемости



Таблица 2-10 Режим посещаемости

Параметр	Описание
Автоматический/Ручной режим	После этого на экране автоматически отобразится статус посещаемости. Вы можете отмечать время прихода и ухода, а также изменять данные о посещаемости вручную. статус.
Автоматический режим	После этого на экране автоматически отобразится ваш статус присутствия. Отмечайте время прихода и ухода.
Ручной режим	При регистрации начала и окончания рабочего дня вы можете вручную выбрать свой статус присутствия.
Фиксированный режим	При регистрации начала или окончания рабочего дня на экране отобразится заранее заданное значение. Статус посещаемости постоянно.

Шаг 4. Настройте параметры режима учета посещаемости.

Рисунок 2-32 Автоматический режим/ручной режим

Auto/Manual Mode	
Check In	06:00-09:59
Break Out	10:00-12:59
Break In	13:00-15:59
Check Out	16:00-20:59
Overtime Check In	00:00-00:00
Overtime Check Out	00:00-00:00

Рисунок 2-33. Фиксированный режим

Fixed Mode	
Check In	✓
Break Out	
Break In	
Check Out	
Overtime Check In	
Overtime Check Out	

Таблица 2-11 Параметры режима посещаемости

Параметры	Описание
Регистрироваться	Отметьте время начала вашего обычного рабочего дня.
Разразиться	Отметьте о завершении работы, когда начнется ваш перерыв.
Вламываться	Отметьте время окончания перерыва.
Проверить	Отметьте о завершении рабочего дня, когда он закончится.
Регистрация на сверхурочную работу	Отмечайте начало сверхурочной работы.
Оплата сверхурочных	Отметьте о завершении работы, когда закончится ваш сверхурочный период.

2.12 Видеодомофон

2.12.1 Настройка видеодомофона

Процедура

Шаг 1. Войдите в главное меню.

Шаг 2. Нажмите «Видеодомофон».

Включите функцию «Вызов» или «Дверной звонок», и на главном экране отобразятся соответствующие значки быстрого доступа (вызов или дверной звонок).

Шаг 3. Настройте параметры вызова или дверного звонка.

- Вызов : Установите «Вызов» или «Дверной звонок» в качестве способа вызова, выберите значки для вызова, а затем настройте параметры.

Таблица 2-12. Описание типов звонков.

Параметр	Описание
Тип вызова	 Вызов с клавиатуры: коснитесь значка вызова на главном экране, введите номер комнаты и совершите звонок.  Центр управления вызовами: Нажмите на значок вызова на главном экране, чтобы позвонить в центр управления.  Вызов в один клик: коснитесь значка вызова на экране ожидания, чтобы позвонить в указанную комнату.  Если модульное устройство подключено к модулю расширения с кнопкой дверного звонка, то функции вызова, выполняемые кнопкой дверного звонка, описываются следующим образом.  Вызов с клавиатуры: Вы можете указать номер комнаты с помощью клавиатуры, а затем нажать кнопку дверного звонка на модуле расширения, чтобы позвонить по указанному номеру комнаты.  Центр управления вызовами/Вызов в один клик: Нажмите кнопку дверного звонка на модуле расширения, чтобы позвонить в систему VTS или по указанному номеру комнаты.

- Дверной звонок : Установите «Вызов» или «Дверной звонок» в качестве дверного звонка, выберите значки для дверного звонка, а затем настройте параметры.



При подключении модульного устройства к внешнему модулю расширения с кнопкой дверного звонка функция дверного звонка работает в соответствии с указанными здесь настройками.

Таблица 2-13. Описание параметров дверного звонка.

Параметр	Описание
Звуковой сигнал локального устройства.	Нажмите на значок на главном экране, и устройство издаст звуковой сигнал.
Внешний дверной звонок	Включите эту функцию, а затем нажмите на значок дверного звонка на главном экране; прозвучит внешний дверной звонок.  • Доступно только на некоторых моделях. • Если функциональный порт 1 не настроен на дверной звонок, при включении внешнего дверного звонка нажмите OK во всплывающем окне. Настройте выходной порт сигнализации на функцию дверного звонка.
Настройка мелодии звонка	Настройте мелодию звонка. Доступны 2 типа мелодий звонка на выбор.
Время звонка (сек.)	Настройте время звонка. По умолчанию оно составляет 3 секунды.

2.12.2 Настройка SIP-сервера

Процедура

Шаг 1. Войдите в главное меню.

Шаг 2. Нажмите «Видеодомофон».

Шаг 3. Включите или выключите SIP-сервер.

После включения SIP-сервера это устройство работает как SIP-сервер.



Изменение настроек SIP-сервера приведет к удалению добавленных устройств с веб-страницы.

2.12.3 Настройка локального кода

Настройте область видео и предварительного просмотра для домофона.



- Поддерживается только на некоторых моделях.
- При использовании с VTN отключение локального кода может привести к невозможности получения предварительного просмотра изображения.

Процедура

Шаг 1. Войдите в главное меню.

Шаг 2. Выберите Видеодомофон > Местный код.

Функция «Локальный код» включена по умолчанию.

Шаг 3. Нажмите «Местоположение», перетащите зеленую рамку выделения на изображении в любое желаемое положение.

а затем нажмите



2.13 Настройки связи

Настройте сеть, порт RS-485 и порт Wiegand.



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

2.13.1 Настройка сети

Настройте IP-адрес, автоматическую регистрацию, облачный сервис, Wi-Fi и точки доступа Wi-Fi.

2.13.1.1 Настройка IP-адреса

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

Процедура

Шаг 1. В главном меню выберите «Связь» > «Сетевые настройки» > «IP-настройки».

Шаг 2. Установите IP-адрес.

Рисунок 2-34 IP-адрес



Таблица 2-14. Параметры конфигурации IP.

Параметр	Описание
IP-адрес/Маска подсети/По умолчанию Врата	IP-адрес, маска подсети и IP-адрес шлюза должны находиться в одном сетевом сегменте.
Предпочитаемый DNS	IP-адрес DNS-сервера.
Альтернативный DNS	Альтернативный IP-адрес DNS-сервера.

Параметр	Описание
MAC	MAC-адрес устройства.
DHCP	Это аббревиатура от Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста). При включении DHCP устройству автоматически будет назначен IP-адрес, маска подсети и шлюз.

2.13.1.2 Настройка автоматической регистрации

Добавьте устройство в платформу управления, чтобы вы могли управлять им непосредственно на этой платформе.

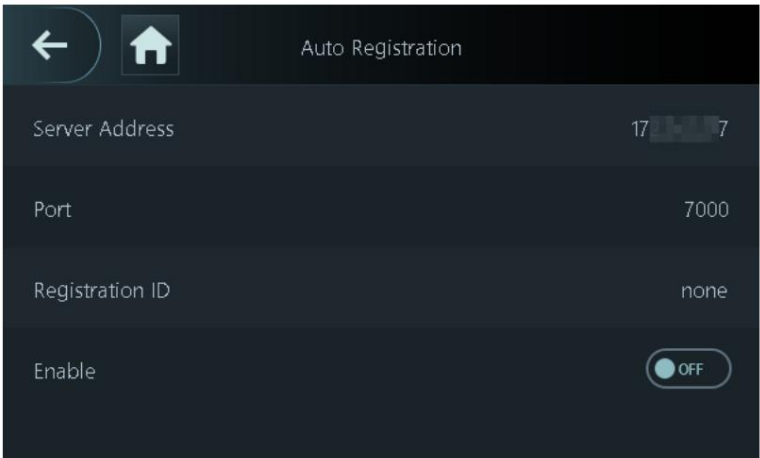
Процедура

Шаг 1. В главном меню выберите «Связь» > «Сетевые настройки» > «Автоматическая регистрация».



Чтобы избежать угроз безопасности и потери данных, необходимо контролировать права доступа к платформе управления.

Рисунок 2-35 Активная регистрация



Шаг 2. Включите функцию автоматической регистрации и задайте параметры.

Таблица 2-15 Регистрация автомобиля

Параметр	Описание
Адрес сервера	IP-адрес платформы управления.
Порт	Номер порта платформы управления.
Идентификатор регистрации	Введите идентификатор устройства (определяется пользователем).  При добавлении устройства на платформу управления регистрационный идентификатор, который вы вводите на платформе управления, должен соответствовать регистрационному идентификатору, определенному на устройстве.

2.13.1.3 Настройка облачного сервиса

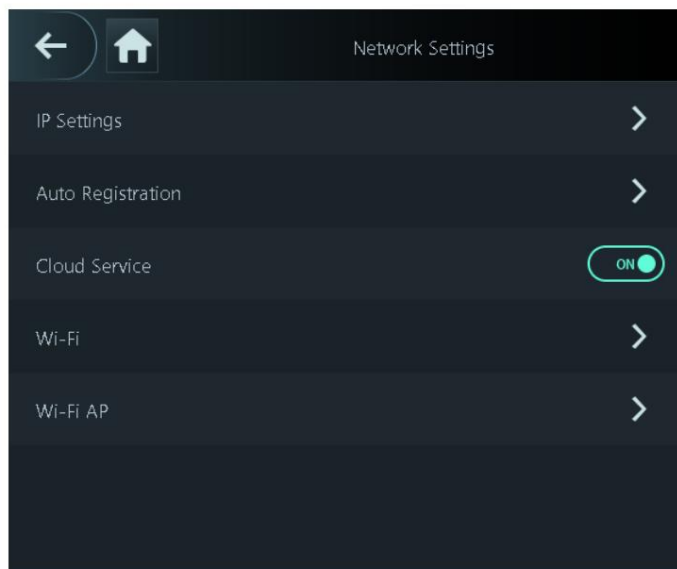
Процедура

Шаг 1. В главном меню выберите «Связь» > «Сетевые настройки».

Шаг 2. Включите облачный сервис.

Управляйте устройствами без подключения к DDNS, настраивайте сопоставление портов и развертывайте транзитные серверы.

Рисунок 2-36. Облачный сервис.



2.13.1.4 Настройка Wi-Fi

Вы можете подключить устройство к сети через сеть Wi-Fi.

Справочная информация



Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. В главном меню выберите «Связь» > «Сетевые настройки» > «Wi-Fi».

Шаг 2. Включите Wi-Fi.



- Функция Wi-Fi доступна только на некоторых моделях.
- Точка доступа Wi-Fi и функция Wi-Fi не могут быть включены одновременно.
- После включения Wi-Fi подождите около 1 минуты для подключения к сети.

Шаг 3. Нажмите, чтобы  выполнить поиск доступных беспроводных сетей.

Рисунок 2-37 Список Wi-Fi



Шаг 4. Выберите беспроводную сеть, введите пароль, а затем нажмите .



Если система не обнаруживает сеть Wi-Fi, нажмите +, чтобы ввести название и пароль сети Wi-Fi.

Результаты

Когда телефон и устройство подключены к одной и той же сети Wi-Fi, введите IP-адрес в браузере для доступа к устройству. Вы также можете использовать свой телефон для сканирования QR-кода на экране подробной информации о сети Wi-Fi, чтобы получить доступ к устройству.

Связанные операции

- Коснитесь подключенной сети Wi-Fi, чтобы просмотреть SSID, IP-адрес, маску подсети, шлюз и другую информацию о сети.
- DHCP: На экране подробной информации о Wi-Fi по умолчанию включен DHCP, и IP-адрес определяется автоматически. Если вы отключите DHCP, вы сможете ввести IP-адрес вручную.

2.13.1.5 Настройка точки доступа Wi-Fi

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

Процедура

Шаг 1. В главном меню выберите «Связь» > «Сетевые настройки» > «Точка доступа Wi-Fi».

Шаг 2. Включите точку доступа Wi-Fi.

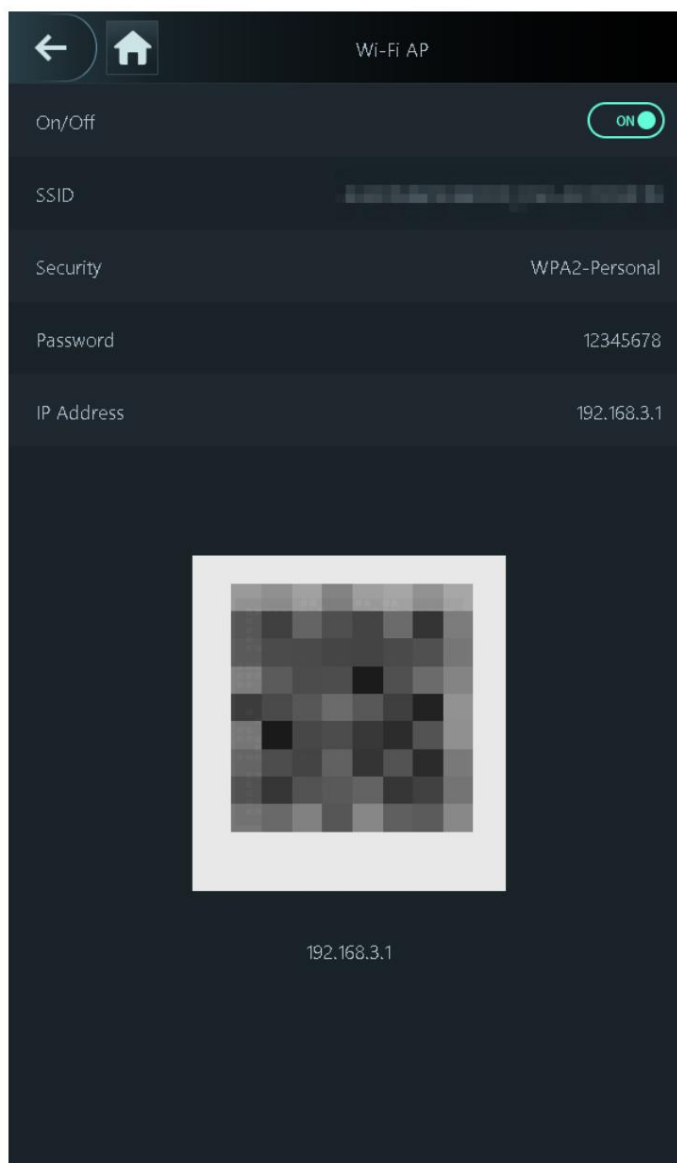
Вы можете настроить безопасность точки доступа Wi-Fi.

Выберите «Нет», чтобы напрямую подключиться к точке доступа Wi-Fi. Выберите «WPA2-Персональный», чтобы настроить пароль и подключиться к точке доступа Wi-Fi, используя этот пароль.



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

Рисунок 2-38. Подключение к точке доступа Wi-Fi.



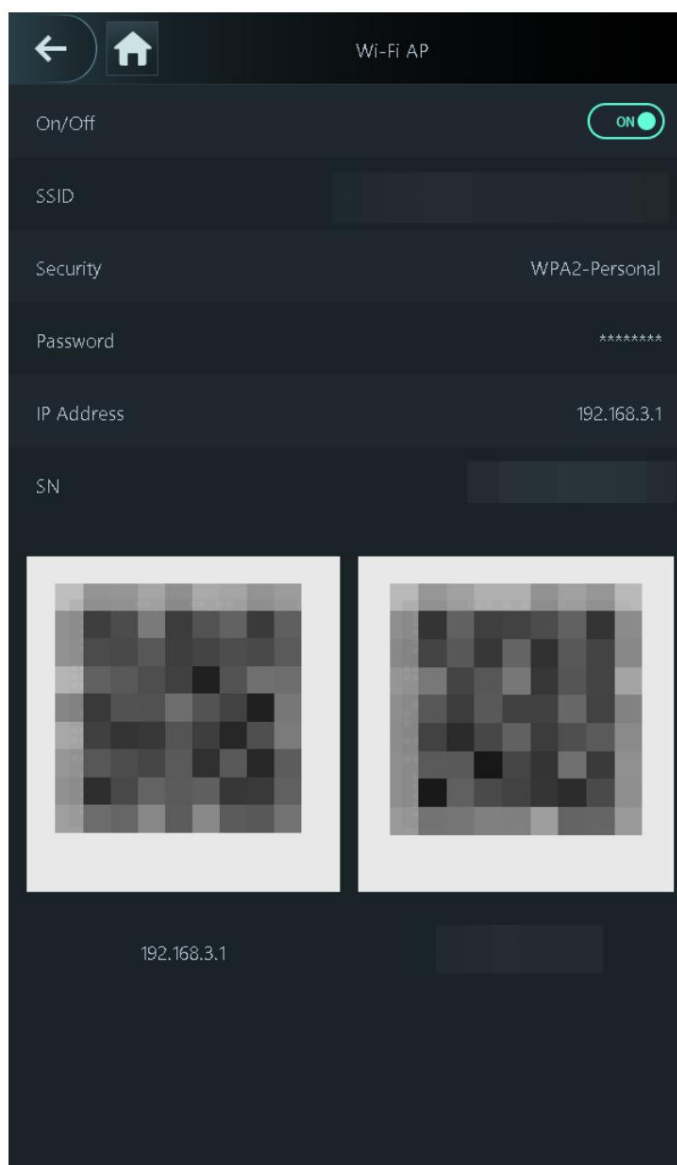
Связанные операции

Также вы можете коснуться правого угла на экране ожидания, чтобы просмотреть состояние точки доступа Wi-Fi. Если вы хотите настроить параметры, сначала войдите в главное меню. QR-код справа используется для добавления контроллера доступа при использовании с другими приложениями.



На некоторых моделях QR-код, расположенный справа, отображается.

Рисунок 2-39 Точка доступа Wi-Fi



2.13.2 Настройка RS-485

Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. В главном меню выберите «Связь» > «Настройки RS-485».

Шаг 2. Выберите внешнее устройство.

Рисунок 2-40. Тип внешнего устройства.

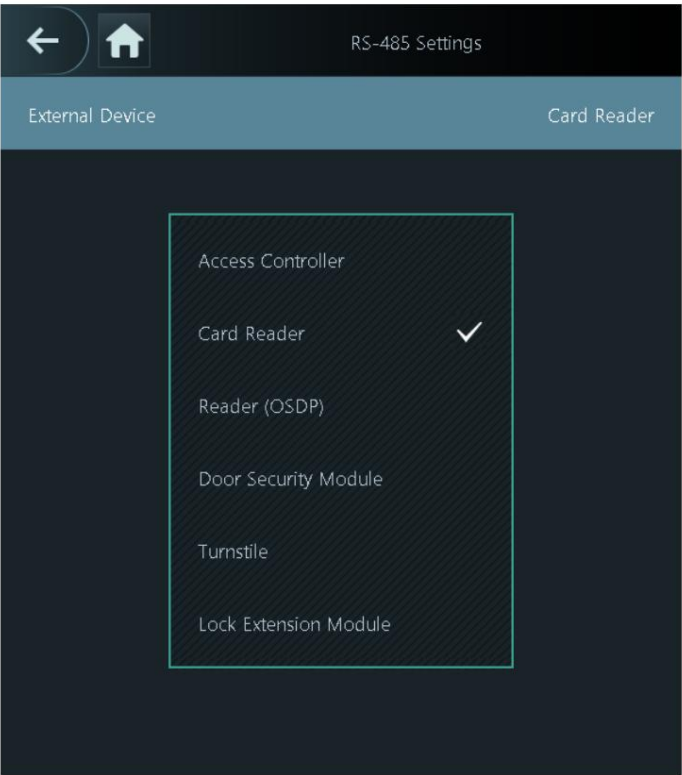


Таблица 2-16. Описание порта.

Внешнее устройство	Описание
Контроллер доступа	Устройство функционирует как считыватель карт и отправляет данные другим внешним контроллерам доступа для управления доступом. Тип выходных данных: • Номер карты : Передайте номер карты контроллеру доступа для аутентификации и разблокировки двери. Если номер карты, переданный этим устройством, совпадает с номером карты в контроллере доступа, аутентификация контроля доступа считается успешной. • Нет .: Передайте идентификатор пользователя контроллеру доступа для аутентификации и разблокировки двери. Если идентификатор пользователя, переданный этим устройством, совпадает с идентификатором пользователя в контроллере доступа, аутентификация контроля доступа считается успешной.  • После успешной проверки на устройстве данные будут переданы контроллеру доступа. Результат проверки, отображаемый на устройстве, соответствует результату, полученному от контроллера доступа. • Если проверка на устройстве не пройдена, данные не будут переданы контроллеру доступа, и результат на устройстве будет считаться неудовлетворительным.

Внешнее устройство	Описание
Считыватель карт	Устройство функционирует как контроллер доступа и подключается к внешнему считывателю карт.
Читатель (OSDP)	Устройство подключено к считывателю карт на основе OSDP-протокол.
Модуль безопасности двери	После активации модуля безопасности кнопка выхода из двери, управление замком и функция пожарной сигнализации устройства перестают работать. - Для разблокировки замка дверного модуля безопасности на устройстве можно подтвердить личность с помощью распознавания лица, карты, отпечатка пальца и пароля. - Вы можете провести картой через подключенную карту RS-485. Для разблокировки замка модуля безопасности двери используйте считыватель или кнопку выхода.  Замок, подключенный к модулю управления безопасностью двери, нельзя заблокировать дистанционно.
Турникет	Когда устройство подключено к турникету, а плата управления доступом турникета подключена к внешнему модулю QR-кода или модулю считывания карт, плата передает данные для проверки на турникет.
Модуль расширения замка	Когда контроллер доступа подключен к внешнему модулю расширения замка, при выборе опции «Модуль расширения замка» локальный замок разблокируется после проверки идентификации на локальном устройстве, а дополнительный замок — после проверки идентификации на внешнем считывателе карт. После выбора модуля расширения замка вы можете выбрать канал 2 на странице «Параметры контроля доступа и сигналы тревоги» на веб-странице контроллера доступа.
Запасной аккумулятор	Устройство подключается к запасному аккумулятору, и текущий уровень заряда батареи отображается в процентах.  Запасной аккумулятор поддерживается только на некоторых моделях.

2.13.3 Настройка Bluetooth

Процедура

Шаг 1. В главном меню выберите «Связь» > «Настройки Bluetooth».

Шаг 2. Включите Bluetooth.

2.13.4 Настройка Wiegand

Устройство поддерживает как входной, так и выходной режимы Wiegand.



Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. В главном меню выберите «Связь» > «Настройки Wiegand».

Шаг 2. Выберите Wiegand.

- При подключении внешнего считывателя карт к устройству выберите вход Wiegand .



Если устройство подключается к стороннему устройству через входной порт Wiegand, и номер карты, считываемый устройством, отображается в обратном порядке по отношению к фактическому номеру карты, в этом случае можно включить функцию инверсии номера карты .

- Выберите выход Wiegand, если устройство работает как считыватель карт и вам это необходимо. Подключите его к контроллеру или другому терминалу доступа.

Рисунок 2-41. Выход Wiegand.



Таблица 2-17. Описание выходных данных Wiegand.

Параметр	Описание
Тип выходного сигнала Wiegand	Выберите формат Wiegand для считывания номеров карт или идентификационных номеров. • Wiegand26 : считывает 3 байта или 6 цифр. • Wiegand34 : считывает 4 байта или 8 цифр. • Wiegand66 : считывает 8 байтов или 16 цифр.
Ширина импульса	Введите ширину импульса и интервал между импульсами на выходе Wiegand.
Интервал пультса	
Тип выходных данных	Выберите тип выходных данных. • Нет : Система выводит данные на основе идентификатора пользователя. Данные Формат — шестнадцатеричный или десятичный. • Номер карты : Система выводит данные на основе первого номера карты пользователя.

2.13.5 Настройки безопасности

Процедура

Шаг 1. В главном меню выберите «Связь» > «Сетевые настройки» > «Настройки безопасности».

Шаг 2. Включите или выключите функции.

- HTTPS: Hypertext Transfer Protocol Secure (HTTPS) — это протокол для безопасной передачи гипертекста. Обмен данными по компьютерной сети. Если включен HTTPS, для доступа к командам CGI будет использоваться HTTPS; в противном случае будет использоваться HTTP.



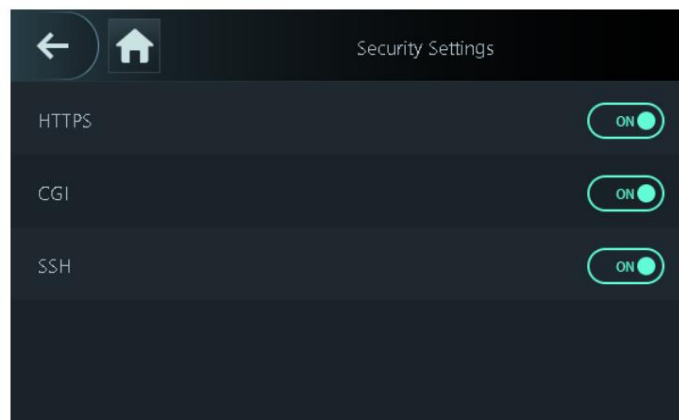
При включении HTTPS устройство автоматически перезагрузится. • CGI: Common

Gateway Interface (CGI) предлагает стандартный протокол для веб-серверов.

Запуск программ аналогичен запуску консольных приложений на сервере, который динамически генерирует веб-страницы. CGI включен по умолчанию.

- SSH: Secure Shell (SSH) — это криптографический сетевой протокол для работы в сети. Защищенное предоставление услуг по незащищенной сети. После включения этой функции передаваемые данные будут зашифрованы.

Рисунок 2-42 Настройки безопасности



2.14 Биометрия

2.14.1 Настройка параметров лицевой панели

Параметры распознавания лица могут различаться в зависимости от модели устройства.

Справочная информация



Мы рекомендуем вам корректировать эти параметры под руководством профессионалов.

Процедура

Шаг 1. В главном меню выберите «Биометрия» > «Параметры лица».

Шаг 2. Настройте параметры лица, а затем нажмите .



Таблица 2-18. Описание параметров лица.

Имя	Описание
Порог распознавания лиц	Настройте уровень точности распознавания лиц. Более высокий порог означает более высокую точность и меньший процент ложных срабатываний.  Если пороговое значение слишком низкое, например, равно 0, то частота ложных срабатываний будет чрезвычайно высокой. Обратите внимание.
Максимальный угол распознавания лиц Отклонение	Задайте максимальный угол, под которым можно расположить лицо для распознавания. Чем больше значение, тем шире диапазон углов наклона грани. Если угол наклона грани выходит за пределы заданного диапазона, она может быть обнаружена неправильно.
Уровень защиты от подделки	После включения эта функция предотвращает использование фотографий, видео, масок и других заменителей для получения несанкционированного доступа. После включения этой функции рамка с лицом не отображается при проверке подлинности неживого объекта.
Иллюминатор	• Включить: Подсветка включается в условиях низкой освещенности. • Выключить: Подсветка постоянно выключена.  Эта функция доступна только на некоторых моделях.
Интервал между полями для заполнения (сек)	Если после первого успешного распознавания перед объективом остается то же лицо, устройство повторно выполнит распознавание лица через определенный промежуток времени.
Неверный интервал между предъявлениями лиц (сек)	Если после первой неудачной попытки распознавания перед объективом остается то же лицо, устройство повторно выполнит распознавание лица через определенный промежуток времени. Если вы укажете 0, лицо не будет распознано, и записи о разблокировке не будут созданы.
Расстояние распознавания	Расстояние между лицом и линзой.
Режим маски	• Не обнаружено : Маска не обнаружена во время распознавания лица. • Предупреждение о маске : Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, но доступ будет разрешен. • Требуется маска : Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, и доступ будет запрещен.
Порог распознавания маски	Чем выше пороговое значение, тем точнее будет распознавание лица, когда человек носит маску, и тем ниже будет частота ложных срабатываний.

Имя	Описание
Оптимизация моментальных снимков	После включения этой функции можно отфильтровать снимки низкого качества из записей о разблокировке.  • Функция распознавания лиц и распознавание нескольких лиц не могут быть включены одновременно. • Эта функция доступна на некоторых моделях.
Удаление повторяющихся граней	После включения этой функции для регистрации и распознавания поддерживается только одно лицо на человека. При регистрации или выдаче лица поддерживается обнаружение дубликатов лиц.
Чувствительность к сходству лиц	
Проверьте качество изображения лица.	Если качество лица, зарегистрированного при добавлении человека, ниже заданного значения чувствительности, рекомендуется повторно загрузить изображение лучшего качества с заданными параметрами чувствительности качества изображения лица.
качества с заданными параметрами	
Бесплатный доступ с помощью Face	Разблокируется после распознавания зарегистрированного лица.
Улучшение снимков лица	После включения этой функции снимки в записях разблокировки отображаются в улучшенном виде.  Эту функцию и распознавание нескольких лиц нельзя включить одновременно.
Украшение	Улучшите качество захваченных изображений лиц.
Включить обнаружение шлема	Обнаруживает защитные каски. Дверь не откроется, если человек не в каске.
Распознавание нескольких лиц	Обнаруживает от 4 до 6 изображений лиц одновременно. Кодовая разблокировка невозможна, дверь откроется только после успешной проверки одного из людей.  Количество поддерживаемых изображений лиц может различаться в зависимости от модели устройства.
Ночной режим	В условиях недостаточного освещения на экране в режиме ожидания отображается белое фоновое изображение для повышения яркости при проверке лица или QR-кода.
Подсветка смарт-экрана	После включения этой функции, в выключенном состоянии экран будет загораться при обнаружении лица.

2.14.2 Настройка параметров отпечатка пальца

Настройте точность обнаружения отпечатков пальцев. Чем выше значение, тем выше порог сходства и точность.

Справочная информация



Эта функция доступна только на некоторых моделях, и некоторые из них поддерживают подключение к модулю расширения для распознавания отпечатков пальцев.

Процедура

Шаг 1. В главном меню выберите «Системные настройки» > «Настройки параметров отпечатка пальца».

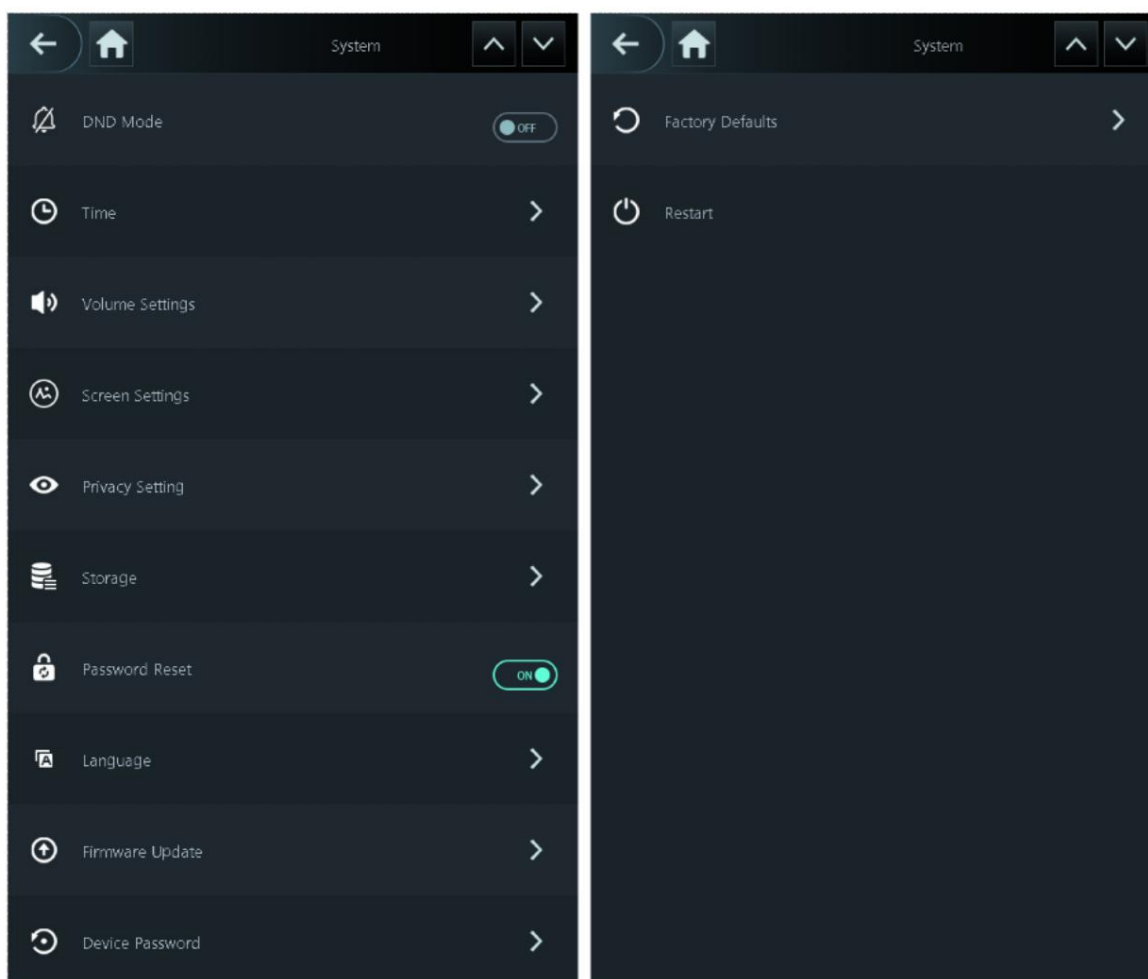
Шаг 2. Нажмите или   чтобы изменить значение.

2.15 Системные настройки

Параметры могут различаться в зависимости от модели устройства.

Кран  или  Переключить страницы.

Рисунок 2-43 Системные настройки



2.15.1 Настройка режима «Не беспокоить»

В течение заданного времени при подтверждении личности на устройстве голосовые подсказки не воспроизводятся. Можно установить до 4 таких периодов.

Процедура

Шаг 1. В главном меню нажмите «Система».

Шаг 2. Включите режим «Не беспокоить».

Шаг 3. Нажмите «Режим «Не беспокоить»», чтобы настроить периоды.

2.15.2 Настройка времени

Настройте системное время, например, дату, время и NTP.
Процедура

- Шаг 1. В главном меню выберите Система > Время.
- Шаг 2. Настройка системного времени.

Рисунок 2-44 Время

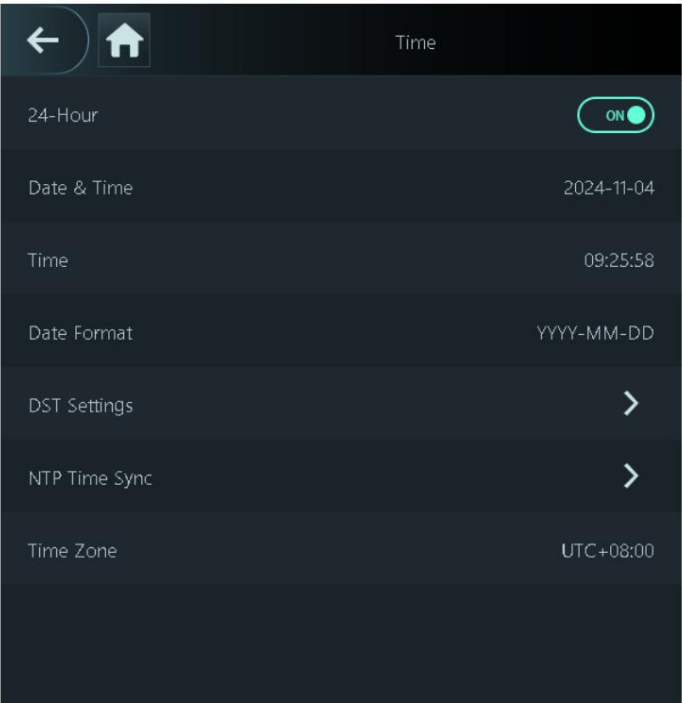


Таблица 2-19. Описание временных параметров.

Параметр	Описание
Круглосуточная система	Время отображается в 24-часовом формате.
Дата и время	Назначьте дату.
Время	Установите время.
Формат даты	Выберите формат даты.
Настройка летнего времени	1. Нажмите «Настройки летнего времени» и включите эту функцию. 2. Выберите дату или неделю из списка «Тип перехода на летнее время» . 3. Введите время начала и время окончания. 4. Нажмите 

Параметр	Описание
Синхронизация времени NTP	Сервер сетевого протокола времени (NTP) — это устройство, специально предназначенное для синхронизации времени со всеми клиентскими компьютерами. Если ваш компьютер настроен на синхронизацию со временем на сервере в сети, ваши часы будут показывать то же время, что и на сервере. Когда администратор меняет время (например, в связи с переходом на летнее время), все клиентские компьютеры в сети также обновляются. 1. Нажмите «Проверка NTP», а затем включите её. 2. Настройте параметры. • Адрес сервера : Введите IP-адрес NTP-сервера, и устройство автоматически синхронизирует время с NTP-сервер. • Порт : Введите порт NTP-сервера. • Интервал : Введите интервал синхронизации времени.
Часовой пояс	Выберите часовой пояс.

2.15.3 Настройка тома

Процедура

Шаг 1. В главном меню выберите Система > Настройки громкости.

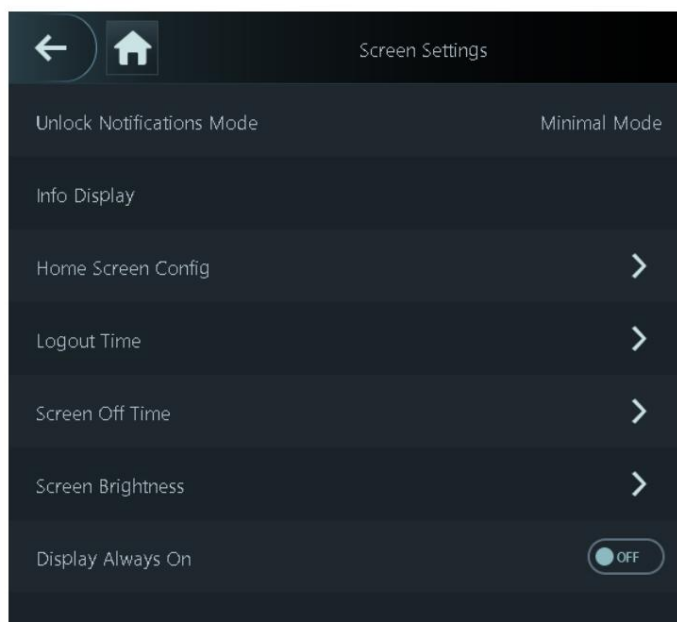
Шаг 2. Настройте параметры.

Таблица 2-20. Описание параметров.

Параметры	Описание
Объем устройства	Нажмите на регулятор громкости, а затем  или  для регулировки громкости.
Громкость домофона	
Громкость микрофона	
Звук касания экрана	При включении этой функции устройства с сенсорным экраном будут издавать звук касания, а устройства без сенсорного экрана — звук щелчка мыши.

2.15.4 Настройка параметров экрана

Рисунок 2-45 Настройки экрана



2.15.4.1 Настройка режима уведомлений о разблокировке

Настройте режим отображения для проверки идентификации. По умолчанию это минимальный режим .



При выборе общего режима в разделе «Персонализация» > «Реклама» > «Тема» отображается этот параметр. Подробную информацию о настройке персонализации см. в разделе «3.13 Персонализация».

Процедура

Шаг 1. Выберите Система > Настройки экрана.

Шаг 2. Нажмите «Разблокировать режим уведомлений» , чтобы выбрать нужный режим.

Рисунок 2-46. Разблокировка режима уведомлений.

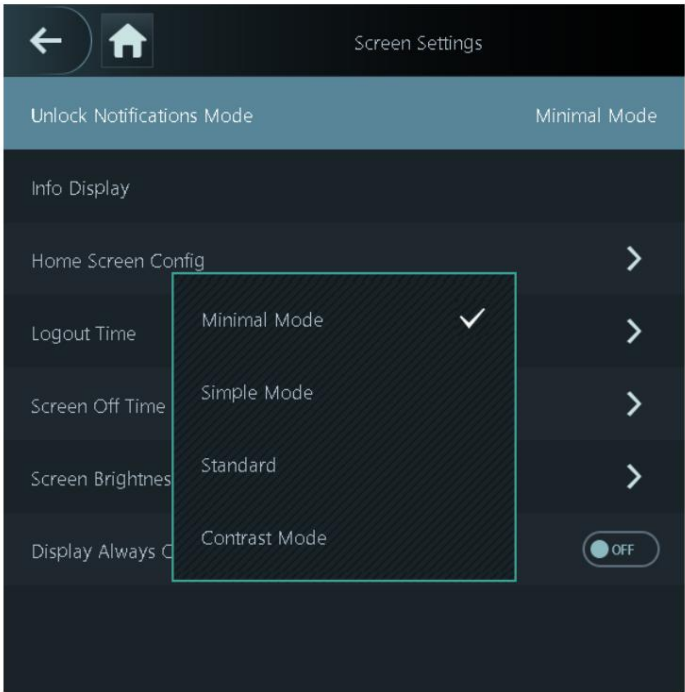


Таблица 2-21. Описание режима уведомлений о разблокировке.

Параметр	Описание
Минимальный режим	Система выводит на экран сообщение «Проверка пройдена успешно» или «Авторизация не выполнена» .
Простой режим	После предоставления доступа отображается идентификатор пользователя, имя и время проверки, а после отказа в доступе — сообщение «Не авторизовано» и время авторизации.
Стандарт	После предоставления доступа отображается зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время проверки, а после отказа в доступе — сообщение «Не авторизовано» и время проверки.
Режим контрастности	После предоставления доступа отображается захваченное изображение лица и зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время авторизации, а после отказа в доступе отображается сообщение «Доступ не авторизован» .

Результаты

После успешного подтверждения личности отображаются следующие всплывающие подсказки.

Рисунок 2-47 Минимальный режим

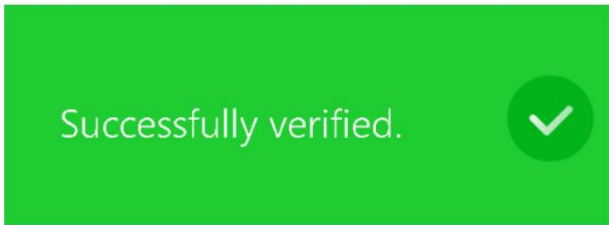


Рисунок 2-48 Простой режим



Рисунок 2-49 Стандарт

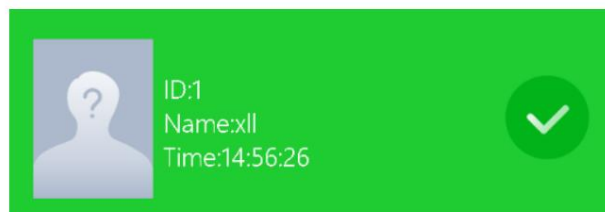
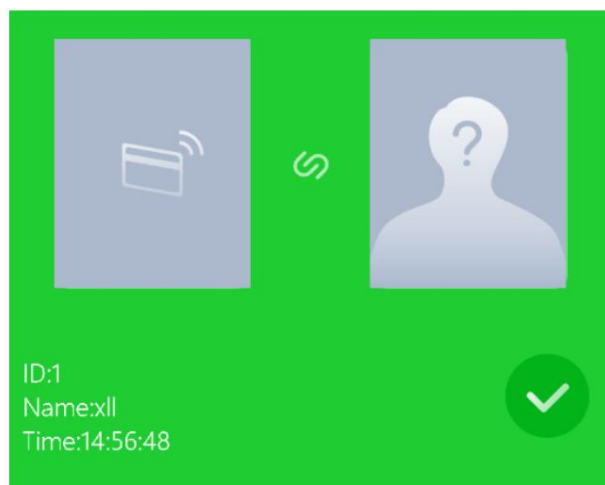


Рисунок 2-50. Режим контрастности.



2.15.4.2 Настройка отображения информации

Процедура

Шаг 1. Выберите Система > Настройки экрана.

Шаг 2. Нажмите «Информационный дисплей», введите информацию, а затем нажмите 

Результаты

При выборе общего режима в разделе «Персонализация» > «Реклама» > «Тема» информация о настроенном устройстве отображается в правом верхнем углу главного экрана. Этот параметр отображается.

2.15.4.3 Настройка главного экрана

Настройте функции, которые будут отображаться на экране в режиме ожидания.

Справочная информация



Поддерживаемые функции могут различаться в зависимости от модели устройства.

Процедура

- Шаг 1. Выберите Система > Настройки экрана > Конфигурация главного экрана.
- Шаг 2. Включите или выключите функции, которые будут отображаться на экране в режиме ожидания.

Рисунок 2-51. Конфигурация главного экрана.

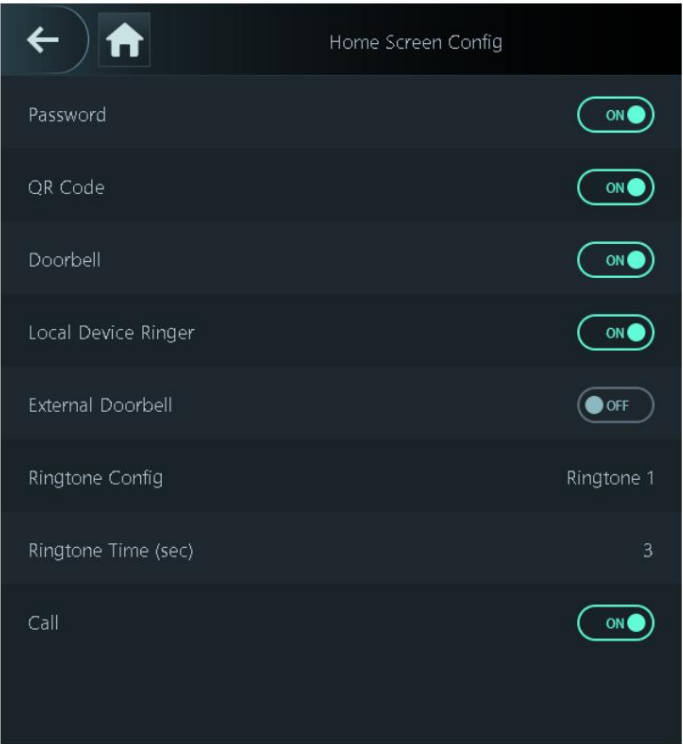


Таблица 2-22. Описание параметров.

Параметр	Описание
Пароль	В режиме ожидания отображается значок способа разблокировки по паролю. экран.
QR-код	Значок QR-кода отображается на экране ожидания. Эта функция недоступна. Доступно для устройств с автономным модулем QR-кода.

Параметр	Описание
Дверной звонок	После включения функции дверного звонка на экране ожидания отображается значок дверного звонка. - Локальный звонок устройства: коснитесь значка звонка на экране ожидания. Устройство зазвонит. - Внешний дверной звонок: Если вы выбрали «Дверной звонок» в разделе «Контроль доступа» > «Конфигурация портов» на веб-странице устройства, включите «Внешний дверной звонок». Коснитесь дверного звонка на экране ожидания, и прозвучит подключенный внешний дверной звонок.  ◇ Эта функция доступна только на некоторых моделях. ◇ Если вы не выберете функцию «Дверной звонок» в разделе «Контроль доступа» > «Настройка портов», то при включении внешнего дверного звонка нажмите «Подтвердить» на экране запроса, и порт будет настроен как функция дверного звонка. - Настройка мелодии звонка: выберите мелодию звонка. - Время звонка (сек.): установите время звонка (1-30 секунд). Значение по умолчанию равно 3.
Вызов	Значок вызова отображается на экране ожидания.

2.15.4.4 Настройка времени выхода из системы

Если на каком-либо экране не выполняются никакие действия и время превышает заданное значение, система переходит в режим ожидания.

Процедура

Шаг 1. Выберите Система > Настройки экрана > Время выхода из системы.

Шаг 2. Нажмите + или —, чтобы изменить время выхода из системы.



Время выхода из системы должно быть короче времени выключения экрана.

Например, если

установить время выхода из системы на 15 секунд, а время выключения экрана на 30 секунд, то после 15 секунд бездействия система переходит в режим ожидания. Если система продолжает бездействовать еще 15 секунд (общее время бездействия достигает 30 секунд), экран системы выключается.

2.15.4.5 Настройка времени выключения экрана

Процедура

Шаг 1. Выберите Система > Настройки экрана > Время выключения экрана.

Шаг 2. Нажмите + или — для регулировки времени.

2.15.4.6 Настройка яркости экрана

Процедура

Шаг 1. Выберите Система > Настройки экрана > Яркость экрана.

Шаг 2. Нажмите + или — для регулировки яркости.

2.15.4.7 Настройка функции «Всегда включенный дисплей»

Процедура

Шаг 1. Выберите Система > Настройки экрана > Дисплей всегда включен.

Шаг 2 Нажмите , а затем нажмите OK , чтобы активировать функцию.



При включении функции Display Always On яркость экрана по умолчанию равна 1 в выключенном режиме.

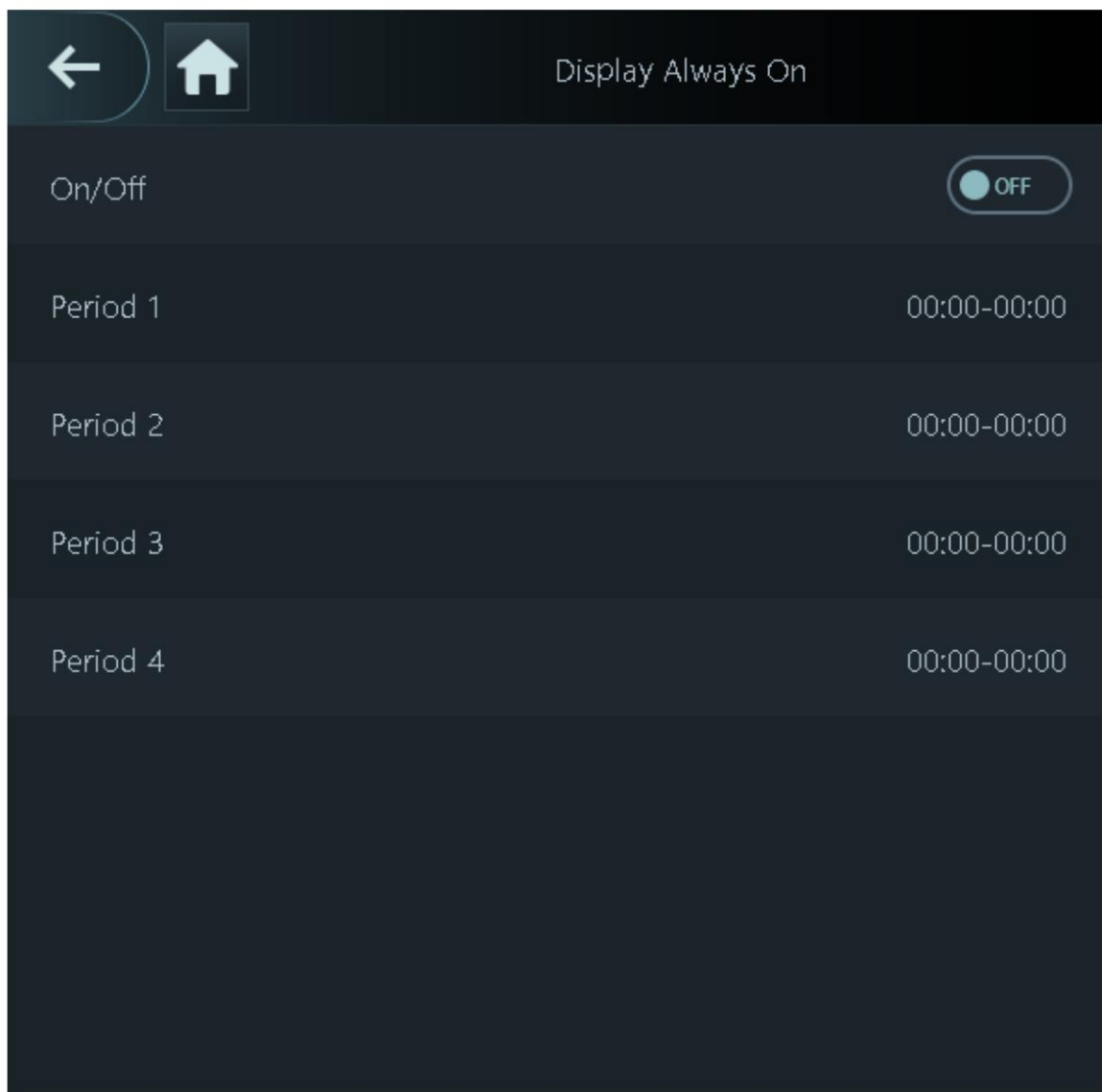
Шаг 3. Нажмите «Дисплей всегда включен» , чтобы настроить периоды, а затем нажмите «Применить».

После включения этой функции экран всегда будет включен в течение заданного периода времени.



Чтобы продлить срок службы экрана, мы рекомендуем ограничить время его работы до 8 часов в день.

Рисунок 2-52 Всегда включено



2.15.5 Настройка параметров конфиденциальности

Процедура

Шаг 1. Выберите Система > Настройки конфиденциальности.

Шаг 2. Настройте параметры.

- Снимок лица для проверки: изображения лиц будут автоматически считываться при разблокировке устройства. дверь.
- Снимок тревоги: При включении этой функции снимки будут создаваться при срабатывании сигнализации. Обратная передача данных, принуждение, черный список и несанкционированные чрезмерные попытки. По умолчанию отключено.
- Регистрация изображения: Если эта функция включена, устройство локально сохраняет изображения лиц, полученные при добавлении пользователей. После отключения эта функция не сохраняет изображения лиц, полученные локально при добавлении пользователей, а только значения характеристик лица.



Эта функция поддерживается на некоторых моделях.

- Очистить все снимки: Удалить все автоматически сделанные фотографии во время разблокировки.

2.15.6 Управление хранилищем

Для экспорта или импорта информации о пользователе можно использовать USB-накопитель.



- Перед экспортом данных убедитесь, что USB-кабель подключен к устройству. Во избежание сбоев не...
Извлеките USB-накопитель или выполните любые другие действия с устройством во время процесса.
- Вы можете использовать USB-накопитель для экспорта информации с одного устройства на другое. Импорт изображений лиц через USB-накопитель запрещен.

2.15.6.1 Экспорт на USB

Вы можете экспортировать данные с устройства на USB-накопитель. Экспортированные данные зашифрованы и не подлежат редактированию.

Процедура

Шаг 1. Выберите Система > Хранилище > Экспорт с USB.

Шаг 2. Выберите тип данных, которые хотите экспортировать, и нажмите OK.



- При экспорте данных в Excel их можно редактировать. • USB-накопитель поддерживает формат FAT32, объем памяти составляет от 4 ГБ до 128 ГБ.

При экспорте персональная информация, черты лица, данные карт и отпечатки пальцев шифруются.

2.15.6.2 Импорт с USB-накопителя

Вы можете импортировать данные с USB-накопителя на устройство.

Справочная информация



Мы рекомендуем импортировать данные между устройствами одной модели и одной версии. В противном случае возможна потеря данных.

Процедура

Шаг 1. Выберите Система > Хранилище > Импорт с USB.

Шаг 2. Выберите тип данных, которые хотите экспортировать, и нажмите OK.

2.15.7 Настройка сброса пароля

В главном меню нажмите «Система», а затем включите функцию «Сброс пароля». После включения этой функции, если вы забудете пароль, вы сможете использовать указанный адрес электронной почты для получения кода безопасности и сброса пароля. Эта функция включена по умолчанию.

2.15.8 Настройка модуля расширения

Справочная информация

- После выбора модуля расширения с функцией «Карта+Дверной звонок» или «Карта+Кнопка+Дверной звонок» механическая кнопка на модуле расширения выполняет практически ту же функцию, что и значок «Вызов/ Дверной звонок» на сенсорном экране. Функции механической кнопки описаны ниже.
- ◇ Когда значок «Вызов /Дверной звонок» на сенсорном экране настроен на функцию вызова:
 - Если тип вызова — вызов с клавиатуры: Если для модуля расширения не указан номер комнаты, по умолчанию вызов поступит на номер администратора. Если для модуля указан пользовательский номер комнаты, то нажатие кнопки дверного звонка на модуле расширения в интерфейсе вызова вызовет на указанный номер.
 - Если тип вызова — вызов администратора / вызов одним нажатием: Нажатие механической кнопки на Модуль расширения инициирует звонок администратору или по указанному номеру комнаты одним нажатием кнопки.
- ◇ Когда на сенсорном экране в настройках вызова /дверного звонка выбрана функция дверного звонка, механическая кнопка также функционирует как дверной звонок.



- Внешние модули расширения поддерживаются только модульными устройствами.
- Разные устройства поддерживают разные типы модулей расширения.
- После восстановления заводских настроек устройства данная конфигурация останется неизменной.

Процедура

Шаг 1. Войдите в главное меню.

Шаг 2. Система подключения.

Шаг 3 Модуль расширения подключения , Выберите внешний модуль расширения, а затем нажмите ОК.

- Перезапустите контроллер доступа, и  Значок отображается в правом верхнем углу главного экрана. Это означает, что настройка прошла успешно.
- Перезапустите контроллер доступа, и  Значок отображается в правом верхнем углу главного экрана. Это означает, что выбранный модуль расширения не соответствует тому, который фактически подключается к контроллеру доступа.
- Если вы выберете «НЕТ» для модуля расширения, значок состояния в правом верхнем углу не отобразится.

2.15.9 Настройка языка

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

2.15.10 Настройка сброса защиты от несанкционированного доступа

В главном меню выберите Система > Сброс защиты от несанкционированного доступа, а затем включите эту функцию.

Операция сброса настроек после вскрытия: В течение 5 минут после включения устройства нажмите кнопку защиты от вскрытия 5 раз подряд в течение 8 секунд. На экране ожидания устройства отобразится запрос на сброс к заводским настройкам. Нажмите «Подтвердить» или нажмите и удерживайте кнопку защиты от вскрытия в течение 3 секунд или дольше. Устройство перезагрузится. Все настройки и информация будут восстановлены до заводских значений по умолчанию.

2.15.11 Обновление системы

Обновите систему устройства через USB.

Процедура

Шаг 1. Переименуйте файл обновления в "update.bin", поместите его в корневой каталог USB-накопителя, а затем вставьте USB-накопитель в устройство.

Шаг 2. В главном меню выберите Система > Обновление микропрограммы.

Шаг 3. Нажмите OK.

Устройство перезагрузится после завершения обновления.



Не выключайте устройство во время обновления.

2.15.12 Настройка пароля устройства

2.15.12.1 Смена пароля

Процедура

Шаг 1. Выберите Система > Пароль устройства > Изменить пароль.

Шаг 2. Введите старый пароль, новый пароль, подтвердите пароль и нажмите OK.

2.15.12.2 Изменение зарезервированной информации

Указанный адрес электронной почты используется для получения кода безопасности, необходимого для сброса пароля.

Процедура

Шаг 1. Выберите Система > Пароль устройства > Изменить зарезервированную информацию.

Шаг 2. Введите адрес электронной почты, а затем нажмите OK.

2.15.13 Восстановление заводских настроек



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

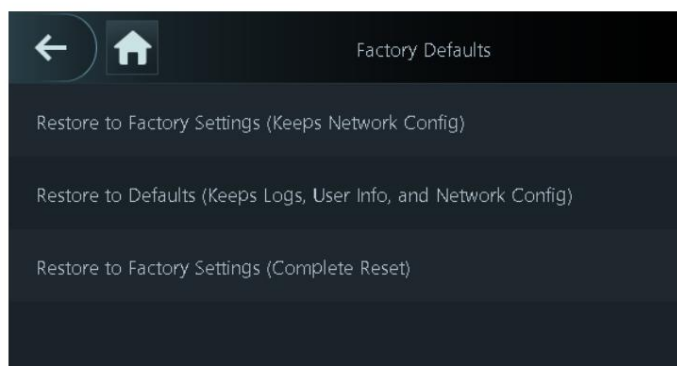
Восстановление с помощью программного обеспечения

1. В главном меню выберите Система > Заводские настройки.

2. При необходимости восстановите заводские настройки.

- Восстановление заводских настроек (с сохранением сетевой конфигурации): Сбрасывает все настройки, кроме сетевой конфигурации и типа модуля расширения (для модульных устройств).
- Восстановление настроек по умолчанию (с сохранением журналов, информации о пользователе и сетевой конфигурации): Сбрасывает все настройки и данные, кроме информации о пользователе, журналов, сетевой конфигурации и типа модуля расширения (для модульных устройств).
- Восстановление заводских настроек (полный сброс): Сбрасывает все параметры конфигурации.

Рисунок 2-53 Заводские настройки по умолчанию



Восстановление через оборудование

Устройство поддерживает кнопку защиты от взлома и кнопку сброса.

- Кнопка защиты от вскрытия: Если в течение 5 минут после включения устройства нажать кнопку защиты от вскрытия 5 раз за 8 секунд, на экране устройства появится соответствующее сообщение. Нажмите «ОК» или нажмите кнопку защиты от вскрытия один раз, и устройство перезагрузится. Все настройки и информация будут восстановлены до заводских значений.
- Отверстие для сброса: Чтобы сбросить устройство, необходимо замкнуть его, вставив штырь в отверстие.
 - ◇ Если вы хотите выполнить частичный сброс и сохранить информацию о пользователе, журналы и IP-конфигурации, PIN-код необходимо удерживать в течение 500 мс.
 - ◇ Для полного сброса настроек штифт необходимо удерживать вставленным в течение 5 секунд.



Отверстие для сброса настроек доступно на некоторых моделях.

2.15.14 Перезагрузка устройства

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

2.16 Информация об устройстве

Вы можете просмотреть объем данных и версию устройства.

2.16.1 Объем данных для просмотра

В главном меню выберите «Информация об устройстве» > «Объем памяти». Вы можете просмотреть объем памяти для каждого типа данных.

2.16.2 Версия устройства просмотра

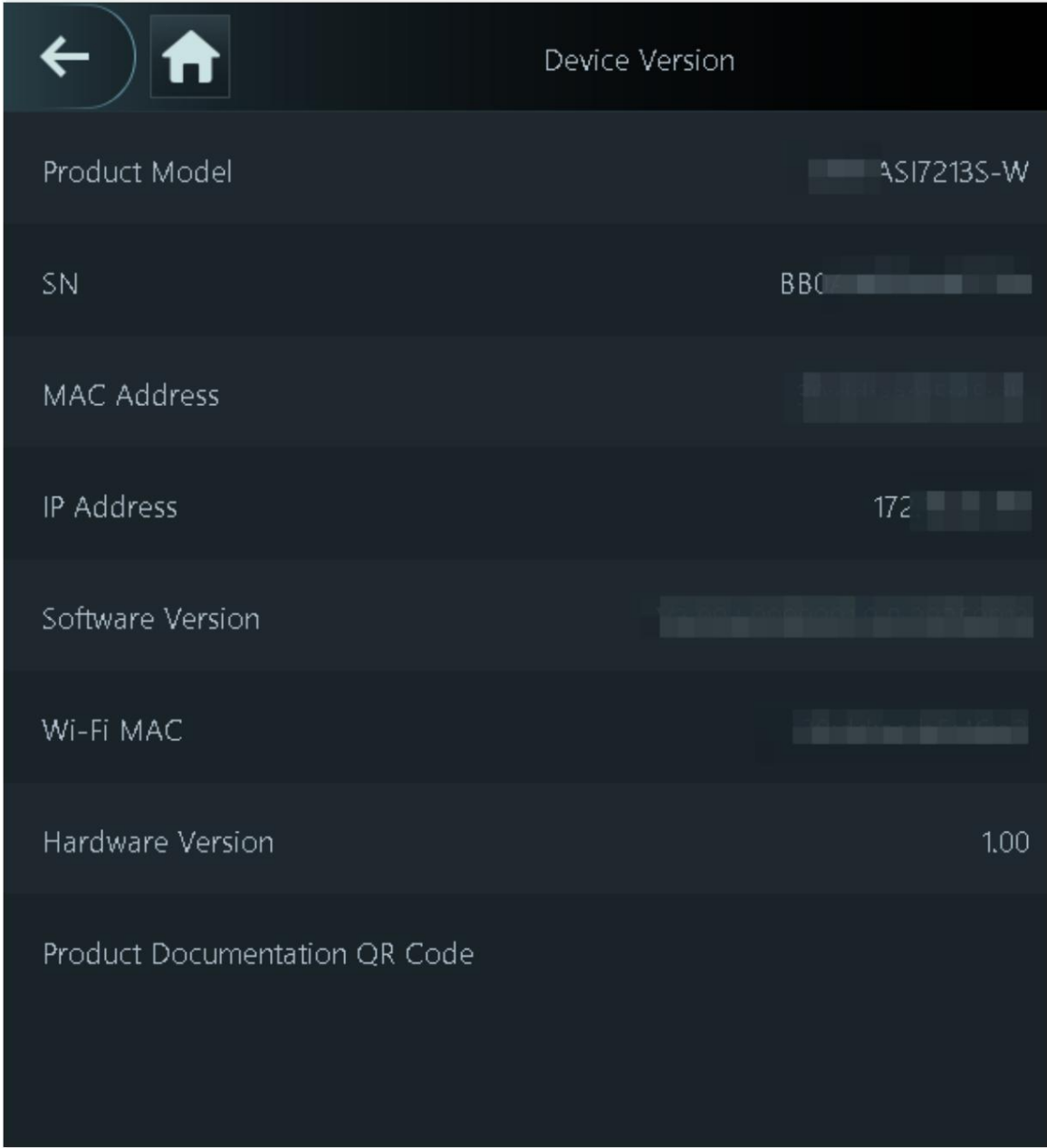
В главном меню выберите «Информация об устройстве» > «Версия устройства». Вы можете просмотреть версию устройства, такую как модель, серийный номер, версия программного обеспечения и многое другое.

Нажмите на QR-код «Документация к продукту», отсканируйте QR-код телефоном, чтобы просмотреть документацию к продукту.



Эта функция доступна только на некоторых моделях.

Рисунок 2-54. Версия устройства.



3 Веб-операции

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



Настройки веб-браузера различаются в зависимости от модели устройства.

3.1 Инициализация

Инициализируйте устройство при первом входе на веб-страницу или после сброса устройства до заводских настроек.

Предварительные требования

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

Процедура

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



Мы рекомендуем 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.



- Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа следующих символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' ').
- Установите надежный пароль, следуя подсказкам о его надежности.
- Сохраните пароль в безопасном месте после инициализации и регулярно меняйте его для повышения уровня безопасности.

3.2 Вход в систему

Процедура

Шаг 1. Откройте браузер, введите IP-адрес устройства в адресную строку и нажмите кнопку.

Нажмите клавишу Enter.

Шаг 2. Введите имя пользователя и пароль.



- Имя администратора по умолчанию — admin, а пароль — тот, который вы установили во время инициализации. Мы рекомендуем регулярно менять пароль администратора для повышения безопасности.
- Если вы забыли пароль для входа в систему администратора, вы можете нажать «Забыли пароль?» Сбросить пароль.

Шаг 3. Нажмите «Войти».

3.3 Сброс пароля

Если вы забыли пароль администратора, сбросьте его через связанный адрес электронной почты. Если адрес электронной почты для сброса пароля не был указан, вам необходимо связаться с местным дилером или службой технической поддержки.

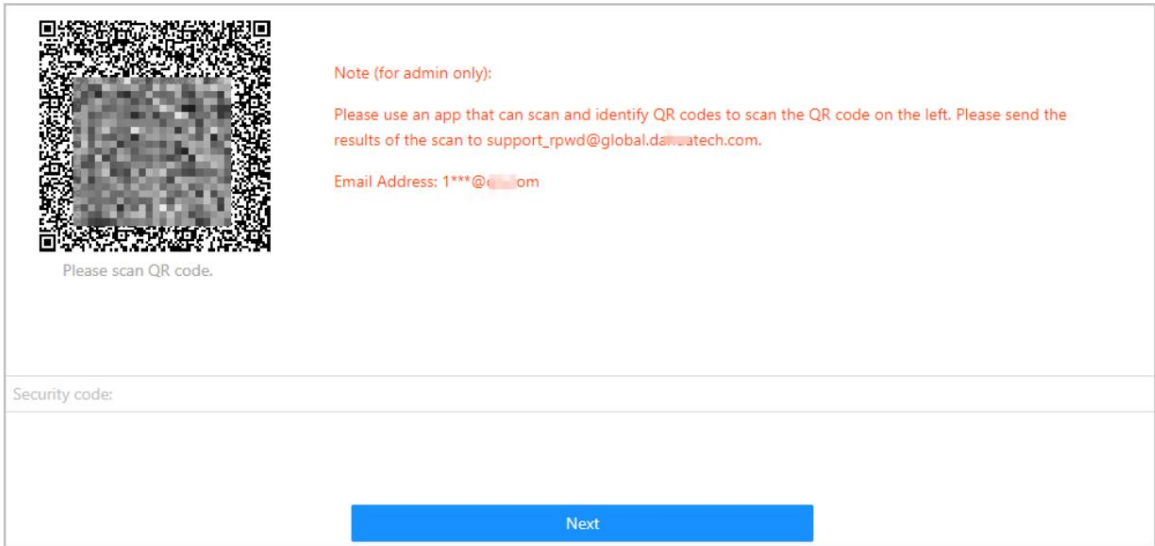
Процедура

Шаг 1. На странице входа нажмите «Забыли пароль».

Шаг 2. Внимательно прочтите подсказку на экране, а затем нажмите ОК.

Шаг 3. Отсканируйте QR-код, и вы получите защитный код.

Рисунок 3-1. 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.dawatech.com.

Email Address: 1***@****.com

Security code:

Next



- При сканировании одного и того же QR-кода будет сгенерировано до двух защитных кодов. Если защитный код недействителен, обновите QR-код и отсканируйте его снова.
- После сканирования QR-кода вы получите защитный код на связанный с ним адрес электронной почты. Адрес. Используйте защитный код в течение 24 часов после его получения. В противном случае он станет недействительным.
- Если неверный код безопасности будет введен 5 раз подряд, учетная запись администратора будет заблокирована на 5 минут.

Шаг 4. Введите защитный код.

Шаг 5. Нажмите «Далее».

Шаг 6. Сбросьте и подтвердите пароль.



Пароль должен состоять из 8–32 непустых символов и содержать как минимум два из следующих типов символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; : &).

Шаг 7. Нажмите ОК.

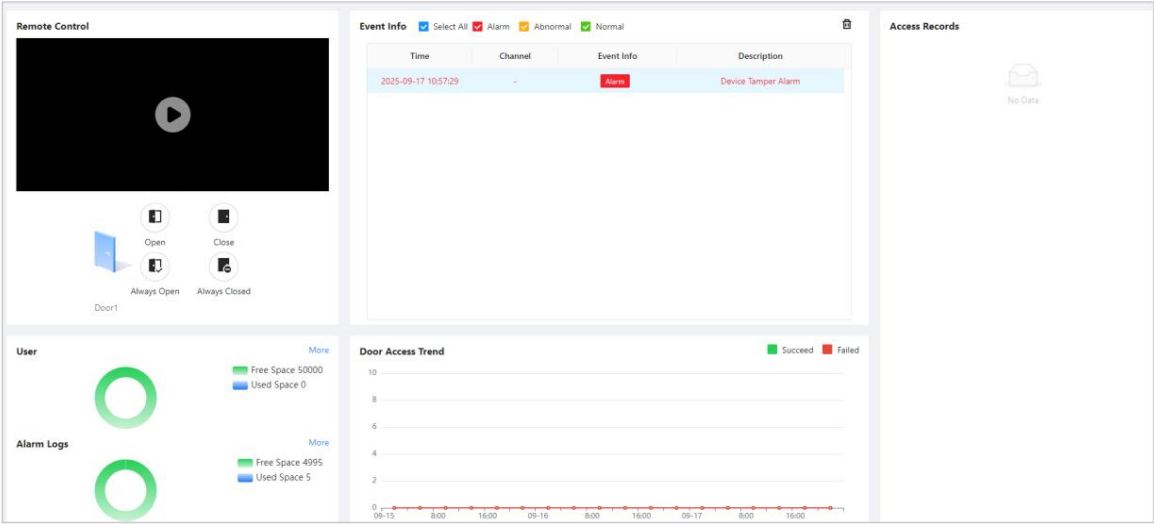
3.4 Мониторинг доступа

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



• Для первого использования, пожалуйста, загрузите и установите плагин в соответствии с инструкциями. • Вы также можете щелкнуть значок веб-сервиса в верхнем левом углу, чтобы просмотреть мониторинг доступа. страница.

Рисунок 3-2. Мониторинг доступа.



Пульт дистанционного управления

- Нажмите «Открыть» или «Закрыть» рядом с дверью, чтобы дистанционно управлять ею. • Нажмите «Всегда открыто» или «Всегда закрыто» , чтобы дистанционно управлять дверью. Нажмите «Восстановить» , чтобы вернуть дверь в нормальное состояние.
- Нажмите  для предварительного просмотра изображения на экране и выполнения соответствующих операций.

Таблица 3-1. Описание значков на экране пульта дистанционного управления.

Иконки	Описание
	Сделайте снимок.
	Начните запись видео.
	Включите звук в видео.
	Включите функцию внутренней связи.
	Увеличьте изображение.

Тенденция в сфере доступа к дверям

Отображается динамика обращений за последние 3 дня. Зеленый цвет означает успешный доступ, красный — неудачный.

Доступ к записям

Отображаются записи о доступе в режиме реального времени, включая изображение, информацию о пользователе, метод проверки и время проверки.

Информация о мероприятии

В разделе «Информация о событии» выберите тип события, чтобы просмотреть события. Нажмите  чтобы завершить все события.

Журналы действий пользователей и тревожных сигналов

Просмотрите информацию о помещениях пользователей и журналы аварийных сигналов. Нажмите «Подробнее», чтобы просмотреть подробную информацию.

3.5 Главная страница

Чтобы перейти на главную страницу, нажмите на кнопку в верхнем левом углу веб-страницы.

Рисунок 3-3 Главная страница

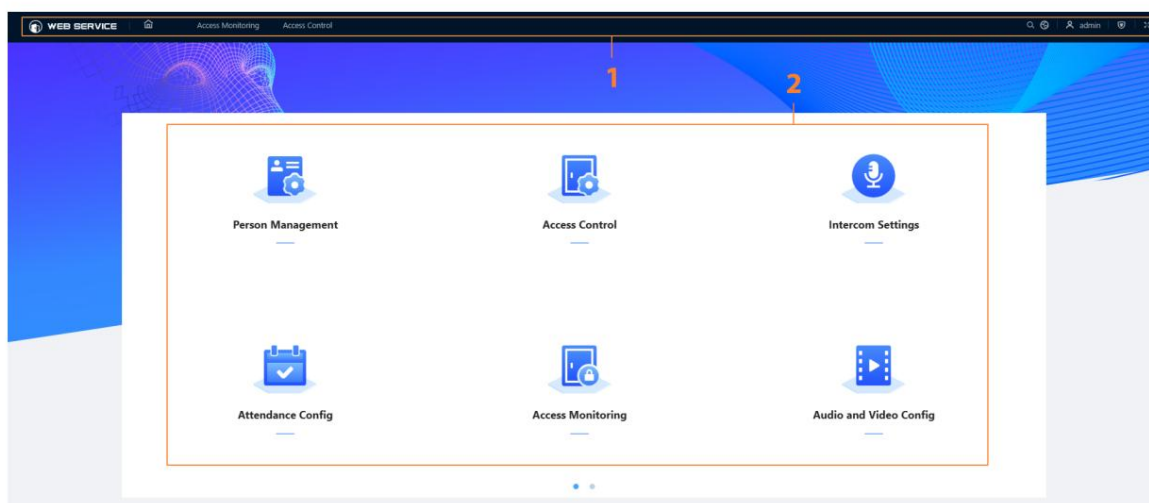


Таблица 3-2. Описание главной страницы

Нет.	Описание
1	 : Перейти на главную страницу.  Поиск функциональных меню по ключевым словам.  : Выберите язык на устройстве.  Выйдите из системы или перезагрузите устройство.  : Перейдите на страницу «Безопасность» .  Отсканируйте QR-код с помощью телефона, чтобы посмотреть товар. документы.  Эта функция доступна только на некоторых моделях.  : Отображение в полноэкранном режиме.
2	Главное меню.

3.6 Управление персоналом

Процедура

Шаг 1. На главной странице выберите «Управление персоналом» , а затем нажмите «Добавить».

Шаг 2. Настройка информации о пользователе.

Рисунок 3-4. Основная информация.

Basic Info

* ID

12

Validity Period

Forever

* User Type

General User

* General Plan

255-Default

Permission Type

Unlock and Attendance

Verification Mode

Same as Device

Custom

Combination Meth...

And

Or

Name

1

* Permission

User

* Times Used

Unlimited

* Holiday Plan

255-Default

Email

* Unlock Method

Card

Face

Password

Bluetooth Card

Fingerprint

Таблица 3-3. Описание основной информации.

Параметр	Описание
Имя	Идентификатор пользователя аналогичен идентификатору сотрудника и может состоять из цифр, букв и их комбинаций, при этом максимальная длина числа составляет 30 символов.
Отделение	Добавьте пользователей в отдел. Если сотруднику назначен график работы отдела, он будет следовать установленному графику. Инструкции по созданию отдела см. в разделе «2.8.1 Настройка отделов».
Режим расписания	- Расписание отдела: Назначьте пользователю расписание отдела. Подробности см. здесь. См. раздел "2.11.3 Настройка графиков работы". - Персональное расписание: Назначьте пользователю персональное расписание. Подробности см. в разделе "2.11.3 Настройка графиков работы".  - Эта функция доступна только на некоторых моделях. - Если вы установите здесь режим расписания на «расписание отдела», то персональное расписание, настроенное для пользователя в разделе «Учет посещаемости > Настройка расписания > Персональное расписание», будет недействительным.
Срок действия	Укажите дату, когда истекает срок действия разрешений на доступ к двери и учет рабочего времени данного лица.
Разрешение	- Пользователь : Пользователи имеют только права доступа к дверям или учета рабочего времени. - Администратор : Администраторы могут настраивать устройство, помимо доступа к дверям и т. д. Разрешения на посещение.
Тип пользователя	- Обычный пользователь : Обычные пользователи могут открыть дверь. - Пользователь из черного списка : Когда пользователи из черного списка открывают дверь, служба Персонал получит уведомление. - Гостевой пользователь : Гости могут открыть дверь в течение определенного периода времени или на определенное количество раз. По истечении установленного периода или по истечении времени разблокировки, открыть дверь будет невозможно. - Патрульный пользователь : Патрульные пользователи могут отмечать посещаемость на устройстве, но они не имеют доступа к двери. - VIP-пользователь : Когда VIP-пользователь открывает дверь, обслуживающий персонал получает... уведомление. - Другой пользователь : После открытия двери она останется открытой еще на 5 секунд. - Пользователь 1 / Пользователь 2: Аналогично обычным пользователям.
Количество использований	Установите лимит времени разблокировки для гостевых пользователей. После истечения этого лимита они не смогут открыть дверь.
Генеральный план	В течение установленного периода люди могут открывать дверь или отмечать присутствие.  Вы можете выбрать несколько тарифных планов.

Параметр	Описание
План на отпуск	В дни установленных праздников посетители могут открывать двери или отмечать присутствие.  Вы можете выбрать более одного праздника.
Тип разрешения	- Открытие и учет присутствия: У пользователя есть разрешение на учет присутствия, и он может открыть дверь, используя настроенные методы проверки. - Учет присутствия: У пользователя есть только разрешение на учет присутствия, и он не может открыть дверь. После успешной проверки личности пользователя создается одна запись о неудачной попытке открытия.
Режим проверки	Настройте режим проверки для пользователя. Вы можете использовать режим, совпадающий с режимом устройства, или настроить свой собственный. - Аналогично устройству: Режим работы идентичен режиму работы устройства. - Пользовательский: После выбора пользовательского режима отобразятся «Метод комбинации» и «Метод разблокировки». Выберите необходимый метод комбинации и метод разблокировки. - Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы открыть дверь. - И ещё: используйте все выбранные способы разблокировки, чтобы открыть дверь.  - Настраиваемый режим проверки действителен только для локального устройства. Он не может использоваться во внешних считывателях карт. - Если пользовательский режим проверки отличается от режима устройства, приоритет отдается пользовательскому режиму.

Рисунок 3-5. Учетные данные доступа.

Access Credentials

Face

Not Added

Upload

Local Collec...

 Supports jpg,jpeg,png image formats.

> Password

Not Added

> Card

Not Added

> Fingerprint

Not Added

> Bluetooth Card

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

Not Added

Add

Add More

Cancel

Таблица 3-4. Описание учетных данных доступа.

Параметр	Описание
Лицо	• Загрузка: Нажмите «Загрузить», чтобы загрузить изображение лица. Каждый пользователь может добавить не более 2 изображений лица. После загрузки вы можете просмотреть или удалить изображение лица.  Изображение лица должно быть в формате jpg, jpeg, png и иметь размер менее 100 КБ. • Локальный сбор: Используйте камеру устройства или USB-камеру для сбора изображений лица. Вы можете просмотреть или удалить изображение лица после того, как сделаете снимок. 1. Нажмите «Локальная коллекция». 2. Нажмите «Изменить», чтобы выбрать устройство сбора данных. 3. Нажмите «Начать создание снимка», чтобы получить изображение лица. 4. Нажмите «Добавить».
Пароль	Введите пароль пользователя. Максимальная длина пароля — 8 цифр. Пароль принудительного вызова — это пароль разблокировки + 1. Например, если пароль пользователя — 12345, то пароль принудительного вызова будет 12346. Сигнализация принудительного вызова сработает при использовании пароля принудительного вызова для разблокировки двери.

Параметр	Описание
Карта	 Эта функция доступна только на некоторых моделях. - Введите номер карты вручную. - Нажмите «Добавить». - Введите номер карты и нажмите «Добавить». - Считывание номера происходит автоматически через устройство считывания регистрационных данных или Устройство. - Нажмите «Добавить» , а затем нажмите «Изменить» , чтобы выбрать устройство для чтения регистрационных данных или устройство». - Прочитайте карточку. - Для считывания удостоверений личности и идентификационных карт нажмите «Считать карту», а затем проведите картой по считывателю. На экране отображается 60-секундный обратный отсчет, напоминающий о необходимости провести картой, после чего система автоматически считает номер карты. Если 60-секундный отсчет истек, нажмите кнопку «Считать карту» еще раз, чтобы начать новый отсчет. - Для считывания карты Desfire поместите карту на устройство, а затем нажмите кнопку «Считать карту». Если на карту Desfire уже записан номер карты, он будет считан и отображен здесь. Если карта пуста, то сначала необходимо записать номер карты. Номер карты будет автоматически сгенерирован на компьютере и записан на карту. - Нажмите «Добавить». Пользователь может зарегистрировать максимум 5 карт. Введите номер карты или проведите картой по считывателю, после чего устройство считает информацию о карте. Вы можете включить функцию «Карта принуждения» . Сигнализация сработает, если для разблокировки двери будет использована карта принуждения.  : Установить карту принуждения.  : Изменить номер карты.  Один пользователь может установить только одну принудительную карту.

Параметр	Описание
Отпечаток пальца	Регистрация отпечатков пальцев. Пользователь может зарегистрировать до 3 отпечатков пальцев, и вы можете назначить один из них в качестве отпечатка для вызова помощи. Сигнализация сработает, когда отпечаток пальца будет использован для разблокировки двери. Регистрация отпечатков пальцев осуществляется с помощью считывателя отпечатков или самого устройства. 1. Нажмите «Добавить» , а затем нажмите «Изменить» , чтобы выбрать устройство для чтения регистрационных данных или Устройство. 2. Прижмите палец к сканеру в соответствии с инструкциями на экране. 3. Нажмите «Добавить».  • Функция сканирования отпечатков пальцев доступна только на некоторых моделях. • Мы не рекомендуем устанавливать первый отпечаток пальца в качестве принудительных. Отпечаток пальца. • Один пользователь может установить только один принудительный отпечаток пальца. • Функция отпечатка пальца доступна, если устройство поддерживает подключение модуля отпечатков пальцев.
Bluetooth-карта	 Функция Bluetooth доступна только на некоторых моделях. Вы можете выбрать вариант «Запрос по электронной почте» или «Запрос с помощью регистрационного кода». • Запрос по электронной почте : подходит для тех, кто впервые использует Bluetooth-карту. Запрос. Вы можете запросить до 5 Bluetooth-карт, используя адрес электронной почты, зарегистрированный в DMSS.  Перед использованием этой функции необходимо ввести зарезервированный адрес электронной почты. 1. Настройте адрес электронной почты, зарегистрированный в DMSS. 2. Нажмите «Запрос по электронной почте», после чего можно будет получить Bluetooth-карты. по запросу. • Запрос через регистрационный код : подходит, если у вас уже есть карта Bluetooth и вы хотите использовать ее на другом контроллере доступа, поддерживающем функцию Bluetooth. 1. Скопируйте код регистрации Bluetooth из DMSS. 2. Нажмите «Запросить с помощью регистрационного кода», а затем введите код. 3. Нажмите OK.

Шаг 3. Нажмите «Добавить».

Вы можете нажать кнопку «Добавить ещё» , чтобы добавить других пользователей.

Связанные операции

- Импорт информации о пользователе
 - Нажмите «Экспорт шаблона» , загрузите шаблон и введите в него информацию о пользователе. Поместите изображения лиц и шаблон в одну папку, а затем нажмите «Импорт шаблона» , чтобы импортировать папку.



За один раз можно импортировать до 10 000 пользователей.

◆

Нажмите «Экспорт информации о пользователе», чтобы экспортировать информацию о пользователях партиями. Вы можете нажать «Импорт информации о пользователе» на веб-странице другого устройства для переноса данных. • Экспорт информации о пользователе: •

Очистить: удалить всех пользователей. •

Обновить: обновить список пользователей. • Поиск: поиск

по имени пользователя или идентификатору пользователя. • Нажмите «Записи о картах Bluetooth», чтобы просмотреть записи о картах Bluetooth. Для пользователей, которым не удалось выпустить карты, вы можете перевыпустить карты здесь.



Вы можете выпускать карты партиями на устройствах, поддерживающих функцию Bluetooth.

3.7 Настройка контроля доступа

3.7.1 Параметры контроля доступа

3.7.1.1 Настройка основных параметров

Процедура

- Шаг 1. Выберите «Контроль доступа» > «Параметры контроля доступа».
- Шаг 2. В разделе «Основные настройки» укажите основные параметры контроля доступа.

Рисунок 3-6. 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

▼

Unlock Notifications Mode

Minimal Mode

▼

Verification Interval

0

s (0-180)

Card Swiping Interval

0

s (0-86400)

Public Password

☐

Tamper Reset

☒

Lock 2

☐

Таблица 3-5. Описание основных параметров.

Параметр	Описание
Имя	Название двери.

Параметр	Описание
Состояние двери	Установите статус двери. - Обычный режим: Дверь будет запирается и отпираться в соответствии с вашими настройками. - Всегда открыта: дверь всегда остается незапертой. • Всегда закрыта: дверь всегда остается запертой.
Обычно открытый период	При выборе «Обычный» вы можете выбрать временной шаблон из выпадающего списка. Дверь остается открытой или закрытой в течение заданного времени. Подробную информацию о настройке общих планов и планов на праздничные дни см. в разделе «3.7.6 Настройка периодов».
Обычно закрытый период	 Если период работы обычно открыт и период закрытия конфликтуют, то период работы обычно открыт имеет приоритет над периодом закрытия. • Если генеральный план конфликтует с планом праздников, то план праздников имеет приоритет над генеральным планом.
Разблокировать режим уведомлений	Отображает уведомление на экране, когда пользователь подтверждает свою личность на устройстве. - Минимальный режим: система выводит на экран сообщение «Успешно проверено» или «Не авторизовано» . • Простой режим: после предоставления доступа отображается идентификатор пользователя, имя и время проверки. После отказа в доступе отображается сообщение «Не авторизовано» и время авторизации. - Стандартный режим: отображает зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время проверки после предоставления доступа. Отображает сообщение «Не авторизовано» и время проверки после отказа в доступе. • Контрастный режим: отображает захваченное изображение лица и Зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время авторизации после предоставления доступа. Отображается сообщение «Не авторизовано» и время авторизации после отказа в доступе.
Интервал проверки	Если вы подтверждаете свою личность несколько раз в течение определенного периода времени, действительной будет считаться только самая ранняя проверка, и дверь не откроется после второй или последующих проверок. С момента, когда дверь не открывается, вам необходимо дождаться истечения заданного интервала времени проверки, прежде чем пытаться подтвердить свою личность снова.
Интервал считывания карты	При первой проверке с помощью карты вы, как правило, можете открыть дверь или отметить присутствие, и записи будут сгенерированы. В течение заданного периода, если вы повторно проведете картой для проверки, вы не сможете открыть дверь или отметить присутствие, и записи не будут сгенерированы. Пожалуйста, проверьте идентификацию по истечении заданного периода.  Интервал считывания карты имеет приоритет над интервалом проверки.
Открытый пароль	После включения функции публичного пароля настройте пароль. Вы можете использовать публичный пароль для разблокировки двери без ввода идентификатора пользователя. Для одного устройства поддерживается только один публичный пароль.

Параметр	Описание
Сброс защиты от несанкционированного доступа	При включении этой функции можно восстановить заводские настройки с помощью кнопки защиты от взлома на задней панели устройства. Операция сброса настроек после вскрытия: В течение 5 минут после включения устройства нажмите кнопку защиты от вскрытия 5 раз подряд в течение 8 секунд. На экране ожидания устройства отобразится запрос на сброс к заводским настройкам. Нажмите «Подтвердить» или нажмите и удерживайте кнопку защиты от вскрытия в течение 3 секунд или дольше. Устройство перезагрузится. Все настройки и информация будут восстановлены до заводских значений по умолчанию.
Замок 2	После включения входной порт сигнализации будет переключен на порт датчика двери 2 и порт кнопки выхода 2.

Шаг 3. Нажмите «Применить».

3.7.1.2 Настройка методов разблокировки

Для разблокировки двери можно использовать несколько способов, таких как отпечаток пальца, карта и пароль.

Вы также можете комбинировать их, чтобы создать свой собственный способ разблокировки.

Процедура

Шаг 1. Выберите «Контроль доступа» > «Параметры контроля доступа».

Шаг 2. В настройках разблокировки выберите режим разблокировки.

- Разблокировка комбинации

1. Выберите «Разблокировка комбинацией» в списке режимов разблокировки .
2. Выберите «Или» или «И».
 - ◇ Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы открыть дверь.
 - ◇ И ещё: используйте все выбранные способы разблокировки, чтобы открыть дверь.
3. Выберите способы разблокировки, а затем настройте остальные параметры.

Рисунок 3-7. Настройки разблокировки.

The screenshot shows the 'Unlock Settings' window with the following configurations:

- Unlock Method:** Combination Unlock
- Combination Method:** Or (selected), And
- Unlock Method (Multi-select):** Card, Fingerprint, Face, Password (all checked)
- PIN Code Authentication:** Disabled (toggle off)
- Door Unlocked Duration:** 3.0 s (range 0.2-600)
- Remote Verification:** Enabled (toggle on)
- Remote Verification Unlock Period:** General Plan: Disabled, Holiday Plan: Disabled
- Unlock Code:** Empty field with a copy icon

Таблица 3-6. Описание настроек разблокировки.

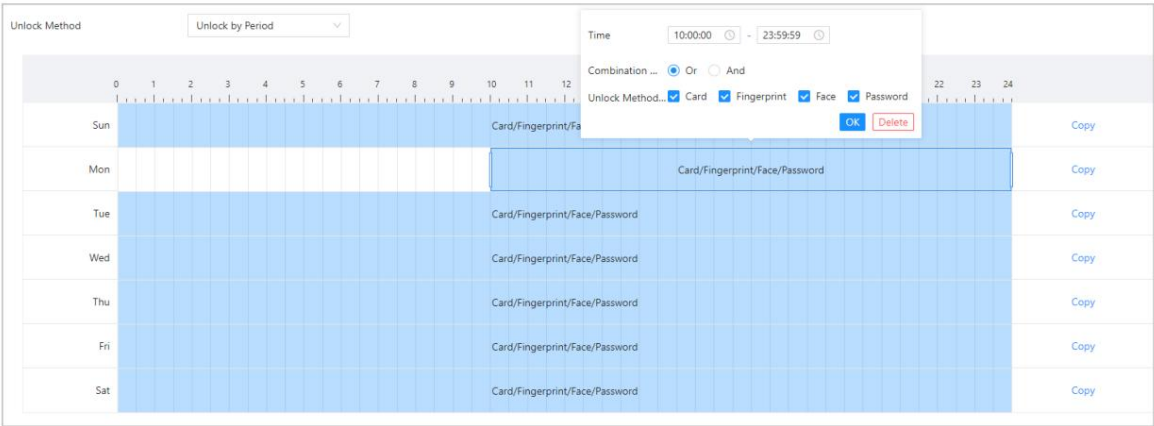
Параметр	Описание
Способ разблокировки (выбор нескольких вариантов)	Способы разблокировки могут различаться в зависимости от модели продукта.
Аутентификация по ПИН-коду	При включенной аутентификации по PIN-коду вы можете открыть дверь, используя только пароль.
Продолжительность открытия двери	После того, как человеку будет предоставлен доступ, дверь останется открытой в течение определенного времени, чтобы он мог пройти. Это время варьируется от 0,2 до 600 секунд.
Удалённая проверка	Откройте дверь дистанционно. После включения функции выберите общий тарифный план и тарифный план для отдыха.
Код разблокировки	Настройте код разблокировки, состоящий максимум из 6 цифр. Устройство стороннего пользователя может выполнить удаленную разблокировку с помощью этого кода.  Данная функция действительна только для локальной блокировки.

- Разблокировка по периодам
 - В списке «Режим разблокировки» выберите «Разблокировка по периоду».
 - Перетащите ползунок, чтобы отрегулировать временной период для каждого дня.



Вы также можете нажать кнопку «Копировать», чтобы применить настроенный период времени к другим дням.
 - Выберите способ комбинации и способ разблокировки на определенный период времени, а затем настройте остальные параметры.

Рисунок 3-8. Разблокировка по периодам.



- Разблокируется несколькими пользователями.
 - Если добавлена только одна группа, дверь откроется только после того, как количество людей в группе, предоставивших доступ, сравняется с заданным допустимым числом.
 - Если добавлено более одной группы, дверь откроется только после того, как количество людей в каждой группе, предоставивших доступ, сравняется с заданным допустимым числом.
 - В списке «Режим разблокировки» выберите «Разблокировка несколькими пользователями».
 - Нажмите «Добавить», чтобы добавить группы.
 - Выберите способ разблокировки и пользователей, укажите допустимый номер, а затем нажмите ОК.

- ◇ Вы можете добавить до 4 групп.
- ◇ Методы разблокировки поддерживают только связь «или».
- ◇ Указанное число означает количество людей в каждой группе, которым необходимо подтвердить свою личность на устройстве, прежде чем дверь откроется. Например, если для группы установлено число 3, то для открытия двери необходимо, чтобы любые 3 человека из этой группы подтвердили свою личность.

Допустимое число не может превышать количество пользователей в списке пользователей.

Рисунок 3-9 Добавить группу

Add [X]

No.

Unlock Method ...

Valid No.

Select Person [Q]

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

Selected People

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

[OK] [Cancel]

Шаг 3. Нажмите «Применить».

3.7.2 Сигнализация

3.7.2.1 Настройка сигнализации

Сигнал тревоги сработает при возникновении нештатной ситуации доступа.

Процедура

Шаг 1. Выберите «Контроль доступа» > «Сигнализация» > «Сигнализация».

Шаг 2 (необязательно) Выберите направляющую двери.

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

- Дверной канал 1: Замок подключается извне через порт дверного замка устройства.

- Дверной канал 2: Замок подключается извне к модулю расширения, который соединен с устройством через порт RS-485.

Рисунок 3-10. Выберите канал.

Door Channel

1

▼

Шаг 3. Настройка параметров сигнализации.

Рисунок 3-11 Сигнализация

Duress Alarm

☒

Anti-passback

☒

Door Detector

☒

☐ NC ☒ NO

Intrusion Alarm

☐

Unlock Timeout Alarm

☐

Excessive Attempts Ala...

☒

Buzzer

☐ Enable

Duration

15

s (1-1800)

Link Alarm Output

☐ Enable

Duration

15

s (1-1800)

Tamper Alarm

☒

Buzzer

☒ Enable

Duration

3

s (1-1800)

Link Alarm Output

☐ Enable

Duration

15

s (1-1800)

Apply

Refresh

Default

Таблица 3-7. Описание параметров тревоги.

Параметр	Описание
Сигнал тревоги	Сигнализация сработает при использовании карты принудительного вызова, пароля принудительного вызова или отпечатка пальца для разблокировки двери.

Параметр	Описание
Защита от повторного прохода	Пользователи должны подтвердить свою личность как при входе, так и при выходе; в противном случае сработает сигнализация. Это помогает предотвратить передачу карты доступа другому лицу для входа. При включенной функции защиты от повторного прохода владелец карты должен покинуть охраняемую зону через считыватель на выходе, прежде чем система предоставит доступ другому лицу. - Если человек входит после получения разрешения, а выходит без разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен. - Если человек входит без разрешения и выходит после получения разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен.  Если к устройству можно подключить только один замок, проверка на самом устройстве по умолчанию означает направление входа, а проверка на внешнем считывателе карт — направление выхода. Вы можете изменить эту настройку на платформе управления.
Детектор двери	При подключении дверного датчика к вашему устройству сигнализация может срабатывать при ненормальном открытии или закрытии дверей. Существует два типа дверных датчиков: нормально замкнутый (NC) и нормально разомкнутый (NO) датчик. - NC: Датчик находится в замкнутом состоянии, когда дверь или окно закрыто. - NET: Разомкнутая цепь образуется, когда окно или дверь фактически закрыты.
охранная сигнализация	Если дверь открывается ненормально, сработает охранная сигнализация, которая будет гореть в течение определенного времени.  Датчик открытия двери и система охранной сигнализации должны быть включены одновременно.
Сигнализация об истечении времени разблокировки	Если дверь остается незапертой дольше заданного времени, сработает сигнализация об истечении времени ожидания, которая будет действовать в течение заданного времени.
Тайм-аут разблокировки	 Датчик открытия двери и функция автоматического закрытия двери должны быть включены одновременно.
Сигнализация о чрезмерном употреблении	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании неlegalной карты, которая будет гореть в течение определенного времени.
Сигнализация о несанкционированном доступе	Сигнализация о попытке взлома срабатывает при нажатии кнопки обнаружения взлома.

Шаг 4. Нажмите «Применить».

3.7.2.2 (Необязательно) Настройка связи между сигналами тревоги

Вы можете настроить связь между сигналами тревоги.

Процедура

Шаг 1. Выберите «Контроль доступа» > «Сигнализация» > «Настройки связи с сигнализацией».



- Если устройство добавлено в платформу управления, настройки сигнализации будут изменены. синхронизировано с платформой.
- Эта функция доступна только на моделях, имеющих вход и выход для сигнализации. порты.
- Количество входных и выходных портов сигнализации различается в зависимости от модели. продукт.



Шаг 2. Нажмите для настройки сигнализации.

Рисунок 3-12. Связь сигналов 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. Придумайте название для зоны тревоги.

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

- NC: Вход сигнализации находится в нормально замкнутом (NC) состоянии, когда сигнал тревоги не сработал. Сработала сигнализация. Размыкание нормально замкнутой цепи приводит к срабатыванию сигнализации.
- НЕТ: Когда сигнализация не сработала, входное устройство сигнализации находится в нормально разомкнутом (НО) состоянии. Замыкание цепи приводит к срабатыванию сигнализации.

Шаг 5 Если вы хотите связать контроль доступа с моментом срабатывания пожарной сигнализации, включите функцию «Связывание контроля доступа».



Эта функция вступает в силу только после включения функции Link Fire Safety Control .

Шаг 6. Выберите режим соединения.

- **Интенсивное выполнение:** Когда сигнал пожарной тревоги исчезает, дверь остается в текущем состоянии. При желании вы можете вручную изменить ее состояние на предыдущее.
- **Слабое выполнение:** Когда сигнал пожарной тревоги исчезает, дверь автоматически возвращается в предыдущее состояние.

Шаг 7. Выберите тип канала.

- **НЕТ:** Дверь автоматически открывается при срабатывании пожарной сигнализации.
- **НЕТ:** Дверь автоматически закрывается при срабатывании пожарной сигнализации.

Шаг 8. Нажмите OK.

3.7.2.3 Настройка связи между событиями тревоги

Процедура

Шаг 1. Выберите «Контроль доступа» > «Сигнализация» > «Связывание событий тревоги».

Шаг 2. Настройте связи между событиями тревоги, а затем нажмите «Применить».

Рисунок 3-13. Связь событий тревоги.

Alarm Type	Linkage Status	Buzzer	Link Alarm Output	Buzzer Duration	Link Alarm Output Duration
Intrusion Alarm Linkage	☒	☐ Enable	☒ Enable	15 s (1-1800)	15 s (1-1800)
Unlock Timeout Alarm Linkage	☒	☐ Enable	☒ Enable	Custom Time 15 s (1-1800)	Custom Time 15 s (1-1800)
Max Use Alarm Link	☒	☐ Enable	☒ Enable	15 s (1-1800)	15 s (1-1800)
Tamper Alarm Linkage	☒	☒ Enable	☐ Enable	3 s (1-1800)	15 s (1-1800)

Buttons: Apply, Refresh, Default

Таблица 3-8. Связь событий тревоги.

Параметр	Описание
Связь с охранной сигнализацией	Если дверь откроется ненормально, сработает охранная сигнализация. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении вторжения. Вы можете настроить продолжительность сигнала тревоги. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает охранная сигнализация. Вы можете настроить продолжительность тревоги.
Сигнализация об истечении времени разблокировки Связь	Если дверь остается незапертой дольше заданного времени, сработает сигнализация об истечении времени ожидания, которая будет действовать в течение заданного времени. • Звуковой сигнал: Звуковой сигнал срабатывает при истечении времени ожидания разблокировки. Вы можете настроить продолжительность сигнала. ◇ Настраиваемое время: Настройте продолжительность. Контроллер доступа будет издавать звуковой сигнал в соответствии с заданным периодом. ◇ До тех пор, пока дверь не закроется: контроллер доступа будет издавать звуковой сигнал до тех пор, пока дверь не закроется. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнал тревоги об истечении времени разблокировки. Вы можете настроить продолжительность сигнала тревоги.
Ссылка на оповещение о максимальном использовании	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании нелегальной карты, которая будет гореть в течение определенного времени. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении чрезмерного использования. Длительность срабатывания сигнала можно настроить. • Выходной сигнал тревоги: Внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнал тревоги об истечении времени разблокировки. Вы можете настроить продолжительность сигнала тревоги.
Связь сигнализации о несанкционированном доступе	Сигнализация о попытке взлома срабатывает, когда кто-то пытается физически повредить устройство. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении попытки взлома. Вы можете настроить продолжительность сигнала тревоги. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнализация о несанкционированном доступе. Вы можете настроить продолжительность срабатывания сигнализации.

3.7.3 Настройка параметров лица

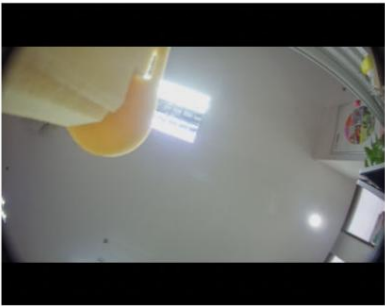
Настройте параметры распознавания лиц. Параметры распознавания лиц могут различаться в зависимости от модели устройства.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Параметры распознавания лиц».

Рисунок 3-14. Параметры распознавания лиц.



Recognition

Exposure

Target Filter

Min Size 64 * 64

Draw Target Clear

Detection Area

Detection Area Clear

Apply

Refresh

Default

Face Recognition Threshold 85 (0-100)

Max Face Recognition Angl... 30 (0-90)

Anti-spoofing Level ☐ Close ☒ General ☐ High ☐ Ultra High

Valid Face Interval (sec) 3 (1-60)

Invalid Face Interval (sec) 10 (0-60)

Recognition Distance 1.5m

Mask mode Not Detect

Mask Recognition Threshold 75 (0-100)

Snapshot Optimization ☐

Remove Duplicate Faces ☐

Face Similarity Sensitivity 85 (0-100)

Verify Face Image Quality ☒

Face Image Quality Sensitivi... 60 (0-100)

Free Access with Face ☐

Face Snapshot Enhancement ☐

Beautifier ☐

Enable Helmet Detection ☐

Multi-face Recognition ☐

Night Mode ☒

Smart Screen Light Up ☒

Шаг 3. Настройте параметры.

Таблица 3-9. Описание параметров лица.

Имя	Описание
Порог распознавания лиц	Настройте уровень точности распознавания лиц. Более высокий порог означает более высокую точность и меньший процент ложных срабатываний.  Если пороговое значение слишком низкое, например, равно 0, то частота ложных срабатываний будет чрезвычайно высокой. Обратите внимание.
Максимальный угол распознавания лиц Отклонение	Задайте максимальный угол, под которым можно расположить лицо для распознавания. Чем больше значение, тем шире диапазон углов наклона грани. Если угол наклона грани выходит за пределы заданного диапазона, она может быть обнаружена неправильно.
Уровень защиты от подделки	После включения эта функция предотвращает использование фотографий, видео, масок и других заменителей для получения несанкционированного доступа. После включения этой функции рамка с лицом не отображается при проверке подлинности неживого объекта.

Имя	Описание
Иллюминатор	• Включить: Подсветка включается в условиях низкой освещенности. • Выключить: Подсветка постоянно выключена.  Эта функция доступна только на некоторых моделях.
Интервал между полями для заполнения (сек)	Если после первого успешного распознавания перед объективом остается то же лицо, устройство повторно выполнит распознавание лица через определенный промежуток времени.
Неверный интервал между предъявлениями лиц (сек)	Если после первой неудачной попытки распознавания перед объективом остается то же лицо, устройство повторно выполнит распознавание лица через определенный промежуток времени. Если вы укажете 0, лицо не будет распознано, и записи о разблокировке не будут созданы.
Расстояние распознавания	Расстояние между лицом и линзой.
Режим маски	• Не обнаружено : Маска не обнаружена во время распознавания лица. • Предупреждение о маске : Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, но доступ будет разрешен. • Требуется маска : Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, и доступ будет запрещен.
Порог распознавания маски	Чем выше пороговое значение, тем точнее будет распознавание лица, когда человек носит маску, и тем ниже будет частота ложных срабатываний.
Оптимизация моментальных снимков	После включения этой функции можно отфильтровать снимки низкого качества из записей о разблокировке.  • Функция распознавания лиц и распознавание нескольких лиц не могут быть включены одновременно. • Эта функция доступна на некоторых моделях.
Удаление повторяющихся граней	После включения этой функции для регистрации и распознавания поддерживается только одно лицо на человека. При регистрации или выдаче лица поддерживается обнаружение дубликатов лиц.
Чувствительность к сходству лиц	
Проверьте качество изображения лица.	Если качество лица, зарегистрированного при добавлении человека, ниже заданного значения чувствительности, рекомендуется повторно загрузить изображение лучшего качества с заданными параметрами чувствительности качества изображения лица.
качества с заданными параметрами	
Бесплатный доступ с помощью Face	Разблокируется после распознавания зарегистрированного лица.
Улучшение снимков лица	После включения этой функции снимки в записях разблокировки отображаются в улучшенном виде.  Эту функцию и распознавание нескольких лиц нельзя включить одновременно.

Имя	Описание
Украшение	Улучшите качество захваченных изображений лиц.
Включить обнаружение шлема	Обнаруживает защитные каски. Дверь не откроется, если человек не в каске.
Распознавание нескольких лиц	Обнаруживает от 4 до 6 изображений лиц одновременно. Кодовая разблокировка невозможна, дверь откроется только после успешной проверки одного из людей.  Количество поддерживаемых изображений лиц может различаться в зависимости от модели устройства.
Ночной режим	В условиях недостаточного освещения на экране в режиме ожидания отображается белое фоновое изображение для повышения яркости при проверке лица или QR-кода.
Подсветка смарт-экрана	После включения этой функции, в выключенном состоянии экран будет загораться при обнаружении лица.

Шаг 4. Настройте параметры экспозиции.

Рисунок 3-15. Параметры экспозиции.

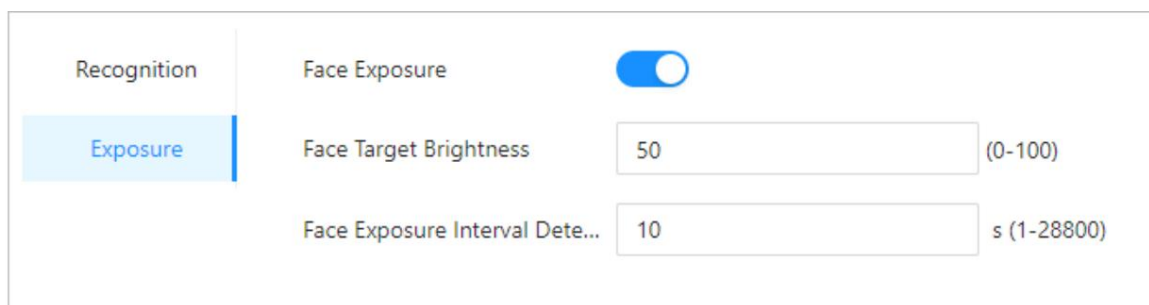


Таблица 3-10. Описание параметров воздействия.

Параметр	Описание
Открытое лицо	После включения функции экспозиции лица, лицо будет экспонироваться с заданной яркостью для четкого отображения изображения.
Яркость мишени лица	
Обнаружение интервала экспозиции лица	Лицо будет показано лишь один раз в течение определенного промежутка времени.

Шаг 5. Нарисуйте область обнаружения лица.

1. Область обнаружения кликов .
2. Щелкните правой кнопкой мыши, чтобы нарисовать область обнаружения, а затем отпустите левую кнопку мыши, чтобы завершить рисование.

Лицо в заданной области будет обнаружено.

Шаг 6. Нарисуйте целевой размер.

1. Нажмите «Нарисовать цель».
2. Нарисуйте прямоугольник распознавания лица, чтобы определить минимальный размер обнаруженного лица.

Только если размер лица превышает заданный размер, устройство может его распознать.

Шаг 7. Нарисуйте область обнаружения.

Шаг 8. Нажмите ОК.

3.7.4 Настройки карты

3.7.4.1 Настройка параметров карты



Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройки карты» > «Настройки карты».

Шаг 3. Настройте параметры карты.

Рисунок 3-16. Параметры карты.

Card Settings

M1 Card

☒

M1 Card Encryption & Verification

☐

FeliCa Card

☒

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 3-11. Описание параметров карты.

Элемент	Параметр	Описание
Настройки карты	Карта M1	При включении этой функции карту M1 можно считать.  Эта функция доступна только на некоторых моделях.
	Шифрование карты M1 и Проверка	При включении этой функции можно считать только зашифрованную IC-карту.  Убедитесь, что карта M1 активирована.
	FeliCa Card	При включении этой функции карту FeliCa можно считать.  Эта функция доступна только на некоторых моделях.
	Удостоверение личности	При включении этой функции можно считать данные удостоверения личности. включено.  Эта функция доступна только на некоторых моделях.
	Блокировка NFC-карт	После включения этой функции разблокировка с помощью дубликата NFC-карты будет исключена.  - Эта функция доступна только на моделях. - Убедитесь, что карта M1 включена. - Функция NFC доступна только на некоторых моделях телефонов.
	Карта DESFire	При включении этой функции устройство может считывать номер карты DESfire.  - Эта функция доступна только на моделях. - Поддерживаются только IC-карты. - Поддерживается только шестнадцатеричный формат.

Элемент	Параметр	Описание
	Расшифровка карты DESFire	Информация на карте DESFire может быть прочитана, если одновременно включены функции «Включить карту DESFire» и «Расшифровка карты DESFire» .  • Эта функция доступна только на моделях, которые поддерживают IC-карты. • Убедитесь, что карта DESFire включена.
Система номеров карт	Система номеров карт	При подключении считывателя карт Wiegand выберите десятичный или шестнадцатеричный формат для номера карты. Система нумерации карт одинакова как для ввода, так и для вывода номера карты.
DESFire Card Write	Устройство сбора данных	Выберите устройство, поместите карту в считыватель, введите номер карты, а затем нажмите «Записать» , чтобы записать номер карты на карту. 
	Номер карты	• Необходимо включить функцию карты DESFire и функцию расшифровки карты DESFire. • Поддерживается только шестнадцатеричный формат. • Поддерживается до 8 символов.

Шаг 4. Нажмите «Применить».

3.7.4.2 Настройка параметров правил использования карт доступа

Платформа по умолчанию поддерживает 5 типов форматов Wiegand. Вы также можете добавить собственные форматы Wiegand.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройки карт» > «Настройки правил доступа по картам».

Шаг 3. Нажмите «Добавить», а затем настройте новые форматы Wiegand.

Рисунок 3-17. 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 3-12. Описание формата Wiegand.

Параметр	Описание
Формат Виганда	Название формата Wiegand.
Всего бит	Введите общее количество битов.
Код объекта	Нажмите кнопку «Добавить», а затем введите начальный и конечный биты кода объекта.
Номер карты	Нажмите кнопку «Добавить», а затем введите начальный и конечный биты номера карты.
Код четности	1. Нажмите «Добавить». 2. Введите бит начала и бит конца четности. 3. Введите бит начала и бит конца нечетной четности.

Шаг 4. Нажмите OK.

Связанные операции

- Вы также можете нажать «Добавить протокол» , чтобы импортировать файл Wiegand на платформу. • Код учреждения: Если эта функция включена, и на странице «Управление персоналом» для системы номеров карт установлен десятичный формат , код учреждения и номер карты преобразуются в десятичный формат отдельно, а затем объединяются.
- HID26: Если функция включена:
 - ◇ Поддерживается только Wiegand 26.
 - ◇ Платформа поддерживает отображение данных карты только в десятичном формате.
 - ◇ Номер карты должен состоять из 5 символов, а код учреждения — не более чем из 3 символов. При ручном вводе номера карты система автоматически добавит ведущий ноль к фиксированной длине числа. Например, если введенный вами номер карты содержит менее 5 символов, например:

56, ведущий ноль добавляется для фиксации длины числа в 5 символов, например, 00056, и еще один 0 добавляется для обозначения кода объекта. Таким образом, окончательный номер карты будет 000056.

3.7.4.3 Настройка пользовательской конверсии

При считывании карт сторонних производителей с помощью встроенного считывателя устройства, внешнего считывателя карт RS-485 или внешнего считывателя карт Wiegand, если фактический номер карты не совпадает ни с одним номером карты в системе, можно настроить пользовательское преобразование номера карты, чтобы гарантировать, что преобразованный номер карты будет соответствовать номеру карты в системе.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройки карты» > «Пользовательская конверсия».

Шаг 3. Включите функцию преобразования, а затем выберите режим сопоставления.

- Автоматическое сопоставление: Используйте встроенное правило преобразования устройства для конвертации номера карты.
 - 1. Выберите тип ввода.
 - ◇ Ввод с устройства: проведите картой по устройству, чтобы считать карту.
 - ◇ Ввод RS-485: Проведите картой по подключенному считывателю карт RS-485, чтобы считать карту.
 - ◇ Ввод Wiegand: Проведите картой по подключенному считывателю карт Wiegand, чтобы считать карту.
 - 2. Считайте номер карты через устройство или введите номер карты до конвертации, а затем введите номер карты после конвертации.
 - 3. Нажмите «Автоматический поиск».
 - ◇ Если номера карт успешно совпали, вы можете нажать кнопку «Экспорт», чтобы экспортировать правило и импортировать его на другое устройство для быстрого переключения правил сопоставления.
 - ◇ Если номера карт не совпадают, это означает, что в системе отсутствует правило сопоставления. Вам необходимо настроить скрипт правила сопоставления и выбрать «Импорт правила преобразования», чтобы импортировать правило на устройство.
 - ◇ Если вам необходимо изменить правило сопоставления, нажмите «Изменить правило сопоставления».

Рисунок 3-18. Автоматическое сопоставление (сопоставление успешно выполнено).

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

- Импорт правила преобразования: Импортируйте другие правила для преобразования номера карты.

Нажмите «Загрузить файл». , Выберите файл с правилами, а затем нажмите «Открыть».

Рисунок 3-19. Правило конвертации импорта.

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.

3.7.5 Настройка QR-кода

Процедура

Шаг 1. На веб-странице выберите «Контроль доступа» > «Настройки карты».

Рисунок 3-20 QR-код

Enable QR Code Exposure ☒

QR Code Brightness

-

+

50

QR Code Exposure Interval (sec)

2

(1-28800)

QR Code Validity Period (min)

10

(0-1440)

Apply

Refresh

Default

Таблица 3-13 Параметры QRR-кода

Параметры	Описание
Включить отображение QR-кода	QR-код будет отображаться с заданной яркостью, и QR-код можно обнаружить и четко прочитать.
Яркость QR-кода	

Параметры	Описание
Интервал показа QR-кода (сек)	QR-код будет показан только один раз в течение заданного интервала времени.
Срок действия QR-кода (мин)	После генерации QR-кода срок его действия будет определяться в течение определенного времени, после чего он истечет.  Сроки действия QR-кодов в QR Code Validity Period, DSS Pro и Dolyнк имеют приоритет друг над другом. Это означает, что платформа, которая последней внесла изменения во время действия кода, будет иметь приоритет над своей последней конфигурацией, а первоначальный срок действия будет аннулирован.

3.7.6 Настройка периодов

Настройте временные интервалы и планы на периоды отпусков, а затем определите, когда пользователь имеет право открывать двери.

3.7.6.1 Настройка общего плана

Вы можете настроить до 128 периодов времени (от №0 до №127). В каждом периоде необходимо настроить расписание доступа к двери на целую неделю. Люди могут открыть дверь только в запланированное время.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройка периода» > «Общий план».

Шаг 3. Нажмите «Добавить».

1. Укажите номер тарифного плана и название тарифного плана.
2. Перетащите ползунок времени, чтобы настроить время для каждого дня.
3. (Необязательно) Нажмите «Копировать», чтобы скопировать конфигурацию на оставшиеся дни.

Рисунок 3-21. Настройка общего плана.

Add [X]

No.

General Plan Name

Time Plan

Time - [OK] [Delete]

	0	1	2	3	4	5	6	7	8	9	10	11	
Sun													Copy
Mon													Copy
Tue													Copy
Wed													Copy
Thu													Copy
Fri													Copy
Sat													Copy

[OK] [Cancel]

Шаг 4. Нажмите OK.

3.7.6.2 Настройка плана отпусков

Вы можете настроить до 128 групп праздников (от №0 до №127), и в каждую группу праздников можно добавить до 16 праздников. После этого вы можете назначить настроенные группы праздников плану праздников. Пользователи могут открывать дверь только в течение времени, указанного в плане праздников.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Настройка периода» > «План отпусков».

Шаг 3. Нажмите «Управление праздниками», а затем нажмите «Добавить».

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

Рисунок 3-22. Добавить группу праздников.

Add [X]

No.

Holiday Group Name

Holiday Group Config

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

2. Нажмите «Добавить», , Добавьте праздник в группу праздников, а затем нажмите ОК.

Рисунок 3-23. Добавление праздника в группу праздников.

Edit [X]

Holiday Name

* Period →

Шаг 4. Нажмите ОК.

Шаг 5. Нажмите «Управление планами», а затем нажмите «Добавить».

1. Выберите номер для плана отдыха, а затем введите для него название.
2. Выберите группу праздников, а затем перетащите ползунок, чтобы настроить время для каждого дня.

Поддерживается добавление до 4 временных интервалов в течение дня.

Рисунок 3-24. Добавить план отпуска.

Шаг 6. Нажмите OK.

3.7.7 Настройка модулей расширения

Для устройств, поддерживающих подключение модулей расширения, укажите тип модуля, который поддерживает данное устройство.

Справочная информация



- Тип модуля расширения может отличаться в зависимости от модели устройства.
- Настройки модуля расширения сохраняются после восстановления заводских настроек устройства.

Процедура

Шаг 1. На веб-странице выберите «Контроль доступа» > «Модуль расширения».

Шаг 2. Выберите тип модуля, который поддерживает устройство.

Шаг 3. Нажмите «Применить».

Настройки вступают в силу после перезагрузки устройства.

-  В правом углу экрана в режиме ожидания отображается сообщение об успешной настройке. В
-  правом углу экрана в режиме ожидания отображается сообщение о том, что тип настроенного вами модуля расширения не соответствует фактическому модулю расширения, подключенному к устройству.
- Если выбрано

«Нет» и к устройству не подключен модуль расширения,
Значок модуля расширения отображаться не будет.

3.7.8 Настройки конфиденциальности

Процедура

Шаг 1. На веб-странице выберите «Контроль доступа» > «Настройки конфиденциальности».

Шаг 2. Включите необходимую функцию.

- Снимок лица для проверки: изображения лиц будут автоматически считываться при разблокировке устройства. дверь.
- Снимок тревоги: При включении этой функции снимки будут создаваться при срабатывании сигнализации. Обратная передача данных, принуждение, черный список и несанкционированные чрезмерные попытки. По умолчанию отключено.
- Регистрация изображения: Если эта функция включена, устройство локально сохраняет изображения лиц, полученные при добавлении пользователей. После отключения эта функция не сохраняет изображения лиц, полученные локально при добавлении пользователей, а только значения характеристик лица.



Эта функция поддерживается на некоторых моделях.

- Сохранение лица на карту: После включения этой функции информация о лице сохраняется на картах, а не в устройстве. При подтверждении личности требуется провести картой по считывателю, чтобы сопоставить черты лица с данными на карте.



После включения этой функции, если вы просто зарегистрируете лицо и сохраните его на карте, вам потребуется добавить эту карту для обычного использования.

Шаг 3. Нажмите «Применить».

3.7.9 Настройка функций порта

Некоторые порты могут функционировать как разные порты, и вы можете настроить их на разные порты в зависимости от фактических потребностей.



- Эта функция доступна только на некоторых моделях.

Расположение портов может отличаться в зависимости от модели изделия.

Процедура

Шаг 1. На веб-странице выберите «Контроль доступа» > «Настройка портов».

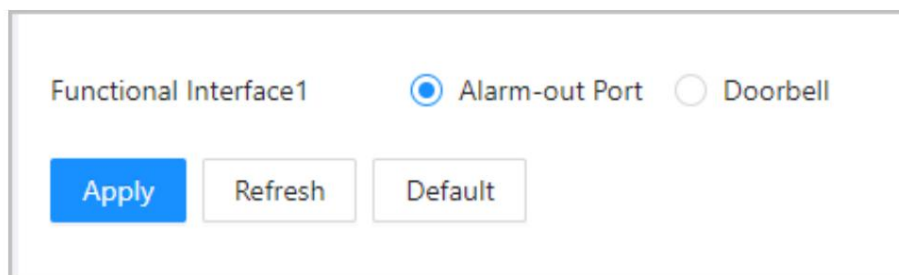
Шаг 2. Выберите тип порта.



Если кабель сигнализации и кабель дверного звонка используются совместно, настройте интерфейс на подключение к дверному звонку, чтобы гарантировать срабатывание звонка.

Шаг 3. Нажмите «Применить».

Рисунок 3-25. Настройка портов.



3.7.10 Настройка параметров управления лифтом

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Управление лифтом».

Шаг 3. Активируйте функцию, а затем выберите способ проверки.

- Удалённая проверка: Идентификаторы проверяются на контроллере лифта.
- Локальная проверка: Идентификаторы проверяются на контроллере доступа.

Рисунок 3-26. Настройка параметров управления лифтом.

Enable ☒

Remote Verification ☐ Remote Verification ☒ Local Verification

IP Address	Port	Lift Control Duration (sec)	Enable	Connection Status	Operation
[Redacted]	5000	0	☐	Test	
[Redacted]	5000	0	☐	Test	
[Redacted]	5000	0	☐	Test	
[Redacted]	5000	0	☐	Test	
[Redacted]	5000	0	☐	Test	
[Redacted]	5000	0	☐	Test	
[Redacted]	5000	0	☐	Test	
[Redacted]	5000	0	☐	Test	

Location

Lift No.



Шаг 4. Щелкните рядом с контроллером лифта, чтобы настроить параметры, а затем включите контроллер лифта.



К одному контроллеру доступа можно подключить до 8 контроллеров лифтов.

Рисунок 3-27. Настройка параметров.

Edit

IP Address

192

168

1

2

Port

5000

(1-65535)

Username

admin

Password

••••••••••••••••

Lift Control Duration (sec)

0

(0-999)

OK

Cancel

Таблица 3-14. Описание параметров устройства.

Параметр	Описание
IP-адрес	Введите IP-адрес контроллера лифта.
Порт	По умолчанию номер порта равен 5000.
Имя пользователя/Пароль	Введите имя пользователя и пароль контроллера лифта.
Продолжительность управления лифтом (сек)	Настройте продолжительность управления лифтом. Значение варьируется от 0 до 999 секунд. Приоритет длительности следующий: контроллер доступа или дверная станция > контроллер лифта > модуль управления лифтом. Например, если вы задаете длительность на контроллере доступа и модуле управления лифтом, приоритет будет иметь длительность, заданная на контроллере доступа.

Шаг 5. Настройте местоположение.

- Внутренний лифт: Лифтом можно управлять только по номеру лифта. Выберите номер лифта. По умолчанию — 1.
- Внешний лифт: Лифт можно вызвать и управлять им. Укажите этаж, на котором находится лифт.
Контроллер доступа. По умолчанию значение равно 1. Диапазон значений от -10 до 128.
- Выберите номер лифта из вариантов 1 или 2.

Шаг 6. Нажмите «Применить».

3.7.11 Настройка сравнения на стороне бэкэнда

Перед настройкой убедитесь, что устройство подключено к сторонней платформе через SDK. Вы можете напрямую передавать данные, такие как QR-код или номер карты, на стороннюю платформу для проверки данных, вместо проверки данных на самом устройстве.

Выберите «Контроль доступа» > «Сравнение серверных частей».

Рисунок 3-28. Сравнение бэкэндов.

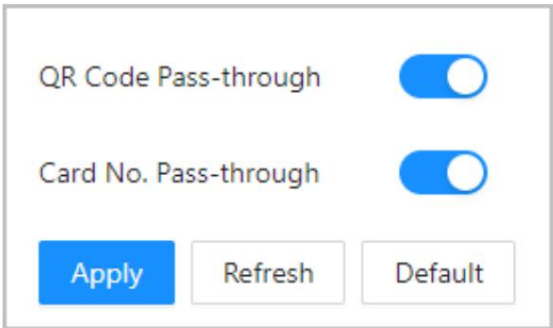


Таблица 3-15. Сравнение бэкэндов.

Параметры	Описание
Пропуск QR-кода	После активации отсканированный QR-код передается на стороннюю платформу для проверки данных.
Номер карты. Передача данных.	После активации номер карты передается на стороннюю платформу для проверки данных.

3.7.12 Настройка разблокировки режима от первого лица

Доступ к дверям возможен только после того, как через них пройдут указанные вами лица. Если указано несколько лиц, то доступ к дверям возможен после того, как через них пройдет любое из указанных лиц.

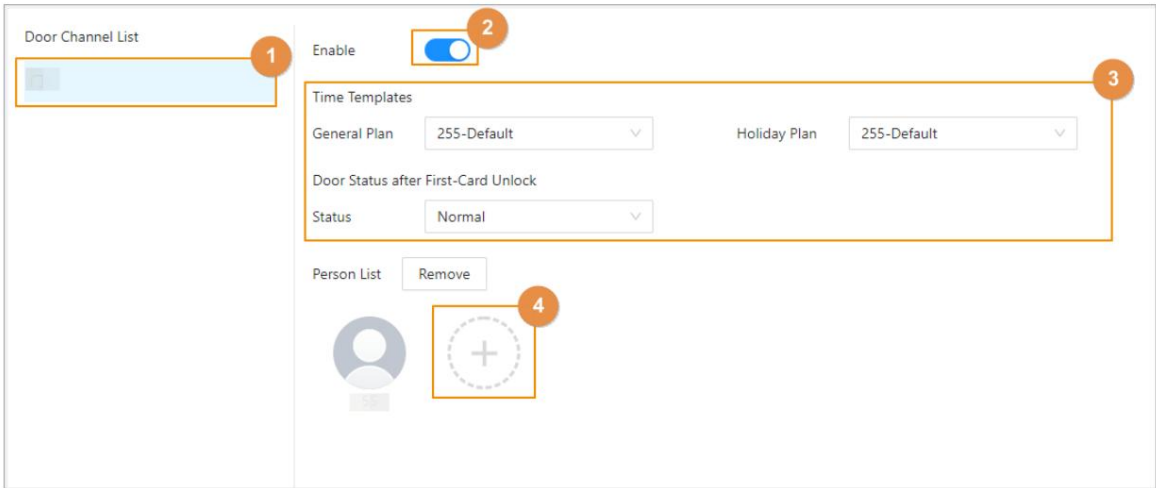
Предварительные требования

- Персонажей можно назначать в качестве персонажей от первого лица только в том случае, если у них есть права доступа к дверям.
- В качестве первого пользователя могут быть назначены только обычные пользователи. • После подтверждения личности первым пользователем, если устройство перезагрузится, первому пользователю необходимо будет пройти повторную проверку. Идентификация снова.
 - После включения этой функции сотрудники патрульной службы могут в обычном режиме отмечать время начала и окончания работы.

Процедура

- Шаг 1. Выберите «Контроль доступа» > «Разблокировка от первого лица».
- Шаг 2. Выберите дверной канал, а затем активируйте функцию.

Рисунок 3-29. Разблокировка от первого лица.



Шаг 3. Настройте параметры.

Таблица 3-16. Описание параметров.

Параметр	Описание
Временные шаблоны	Выберите период действия этого правила.
Состояние двери после первой карты Разблокировать	- Обычный режим : Другие лица должны подтвердить свою личность. проходить. - Круглосуточно открыто : любой желающий может пройти без проверки документов, удостоверяющих личность.
Список лиц	Нажмите кнопку «+» , чтобы выбрать одного или нескольких человек, и они получат доступ к дверям.

Шаг 4. Нажмите «Применить».

3.7.13 Настройка защиты от повторной передачи

Пользователи должны подтвердить свою личность как при входе, так и при выходе; в противном случае сработает сигнализация о невозможности повторной передачи карты. Это предотвращает передачу карты доступа другому лицу для обеспечения доступа. При включении функции предотвращения повторной передачи карты владелец карты должен покинуть охраняемую зону, прежде чем система предоставит доступ другому лицу.

- Если человек входит после получения разрешения и выходит без разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен. • Если человек выходит без разрешения после получения разрешения, сработает сигнализация.

Когда они пытаются войти снова, доступ одновременно блокируется.

Процедура

Шаг 1. Выберите «Контроль доступа» > «Защита от повторного прохода».

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

Укажите время, когда будет сброшен статус защиты от повторного прохода для всего персонала.

Шаг 3. Выберите общий план и план отдыха.

Система предотвращения повторного прохода действует в течение установленного времени.

Шаг 4. В группе устройств нажмите «Добавить», а затем выберите устройство для чтения карт.

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

Рисунок 3-30. Защита от обратного прохода.

Enable ☒

Reset Time min (5-300)

Time Templates

General Plan Holiday Plan

Anti-passback Group Config [?](#)

Entry Group

/Reader 1
[Remove](#)

Exit Group

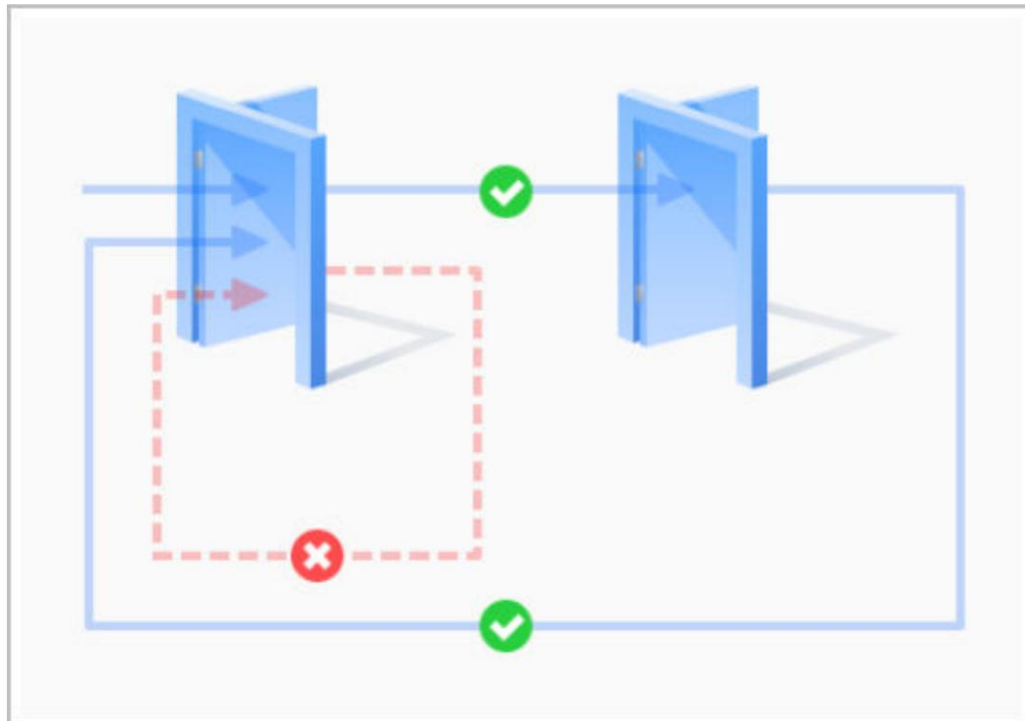
/Reader 2
[Remove](#)

Шаг 6. Нажмите «Применить».

Результаты

Номер группы указывает последовательность считывания карт. Карту необходимо использовать в соответствии с определенной последовательностью групп. Например, в группе входа необходимо провести картой через считыватель, а затем через считыватель в группе выхода. Пока вы проводите картой в соответствии с установленной последовательностью, система работает корректно.

Рисунок 3-31. Функция защиты от повторного прохода.



3.8 Настройка домофона

Устройство может функционировать как дверная станция для реализации видеодомофонной системы.



Функция внутренней связи доступна только на некоторых моделях.

3.8.1 Использование устройства в качестве SIP-сервера

3.8.1.1 Настройка SIP-сервера

Когда устройство функционирует как SIP-сервер, оно может подключать до 500 VTN.

Процедура

Шаг 1. Выберите «Настройки домофона» > «SIP-сервер».

Шаг 2. Включите SIP-сервер.



При изменении состояния SIP-сервера настройки устройства будут автоматически восстановлены до заводских значений.

Рисунок 3-32 SIP-сервер

Local SIP Server

☒

Port

5060

SIP No.

8001

Registration Password

●●●●●●●●●●●●●●●●

SIP Domain

VDP

Apply

Refresh

Default

Шаг 3. Нажмите «Применить».

3.8.1.2 Настройка локальных параметров

Если устройство функционирует как SIP-сервер, настройте параметры устройства.

Процедура

Шаг 1. Выберите «Настройки домофона» > «Конфигурация локального устройства».

Шаг 2. Настройте параметры.

Рисунок 3-33. Основные параметры

Device Type

Door Station

No.

8001

Group Call

☐

Management Center

888888

Apply

Refresh

Default

Таблица 3-17. Описание основных параметров.

Параметр	Описание
Тип устройства	Выберите дверную станцию.
Нет.	Невозможно установить.

Параметр	Описание
Групповой звонок	При включении функции группового вызова дверной пульт одновременно звонит на главный VTH и на внутренние номера. Настройка вступает в силу после перезагрузки дверного пульта.
Центр управления	Номер телефона центра управления по умолчанию: 888888 + номер VTS. Чтобы узнать номер VTS, перейдите в раздел « Настройки проекта » > « Общие » в центре управления.

Шаг 3. Нажмите «Применить».

3.8.1.3 Настройки устройства

Войдите на веб-страницу, затем выберите «Настройки домофона» > «Настройки устройства». Доступны 2 режима на выбор.

- Отключите автономную конфигурацию устройства : если это устройство используется в качестве SIP-сервера, необходимо добавить VTH, VTS и другие дверные станции для видеодомофонов.
- Включение автономной настройки устройств : поддерживает настройку IP-адреса, SIP-сервера, серийного номера и другой информации для устройств VTO, станций ограждения, VTH и VTS в сети, а также распространяет информацию о конфигурации на устройства VTO в сети для обеспечения быстрой интеграции в сеть.

Рисунок 3-34 Настройки устройства



3.8.1.3.1 Отключение автономной конфигурации устройства

Убедитесь, что функция «Настройка автономного устройства» отключена. Нажмите «Добавить» , чтобы настроить параметры, а затем нажмите «ОК».

Добавление VTO

Установите тип устройства как VTO.

Рисунок 3-35 ВТО

Add
X

Device Type
VTO

* No.
Please enter

* Registration Password
.....

Building No.

Unit No.

* IP Address
192 . 168 . 11 . 1

* Username
Please enter

* Password
Please enter

OK
Cancel

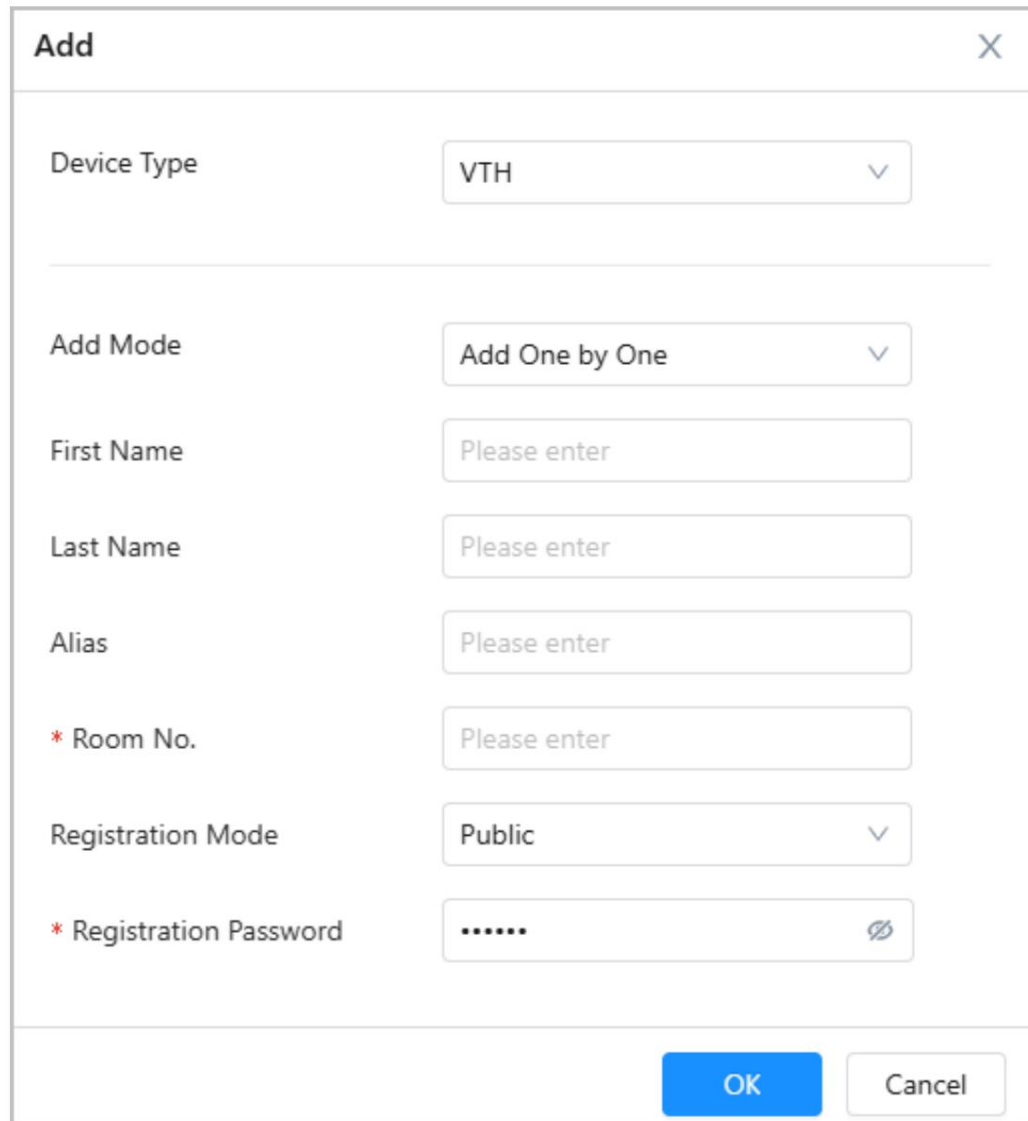
Таблица 3-18. Добавление конфигурации ВТО.

Параметр	Описание
Тип устройства	Выберите дверную станцию.
Нет.	Чтобы посмотреть номер дверной станции, перейдите на экран «Устройство». Затем введите номер дверной станции на этой странице.
Регистрация Пароль	Оставьте значения по умолчанию.
Здание №	Невозможно настроить.
Номер блока	
IP-адрес	IP-адрес добавленной дверной станции.
Имя пользователя	Имя пользователя и пароль, используемые для входа на веб-страницу Добавлена дверная станция.
Пароль	

Добавление VTH

Установите тип устройства как VTH.

Рисунок 3-36. Складывайте по одному.



The image shows a software dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains several input fields and dropdown menus for adding a VTH device. The fields are arranged vertically and separated by a horizontal line. The "Device Type" dropdown is set to "VTH". The "Add Mode" dropdown is set to "Add One by One". The "First Name", "Last Name", "Alias", and "* Room No." fields are empty text boxes with the placeholder text "Please enter". The "Registration Mode" dropdown is set to "Public". The "* Registration Password" field is a password input box with masked characters "*****" and a toggle icon for visibility. At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).

Field	Value
Device Type	VTH
Add Mode	Add One by One
First Name	Please enter
Last Name	Please enter
Alias	Please enter
* Room No.	Please enter
Registration Mode	Public
* Registration Password	*****

Рисунок 3-37. Добавлять партиями.

Add

Device Type

VTH

Add Mode

Add in Batches

Floors in Unit

5

Rooms on Each Floor

4

First Room No. on 1st Floor

101

First Room No. on 2nd Floor

201

OK

Cancel

Таблица 3-19. Описание добавления VTH.

Добавить параметр режима	Описание	
Добавить единицу один	Имя	Укажите имя, фамилию и псевдоним для идентификации VTH.
	Фамилия	
	Псевдоним	
	Номер комнаты.	Укажите номер комнаты для VTH. • Номер комнаты состоит из 1-5 цифр и должен совпадать с номером комнаты, указанным в VTH. • Если система включает в себя основной и вспомогательный VTH, то основной Номер комнаты в главном виртуальном доме (VTH) заканчивается на "-0", а номера комнат в поддоме — на "-1", "-2", "-3". Например, главный виртуальный дом может быть "101-0", а поддоме — "101-1", "101-2". • Если поддомеев нет, номер комнаты не обязательно должен заканчиваться на "-0". Например, "101", "102".
	Регистрация Режим	Используется для сигнализации взаимодействия в системе SIP. Оставьте значение по умолчанию.
	Регистрация Пароль	

Добавить параметр	режима	Описание	
Добавлять партиями	Этажи в квартире	Количество этажей на единицу жилья варьируется от 1 до 99.	Например, если на каждом этаже 10 комнат, и начальный номер комнаты на первом этаже равен 100, то начальный номер комнаты на втором этаже должен быть 111 или позже.
	Комнаты на каждом Пол	Количество комнат на этаже варьируется от 1 до 99.	
	Комната номер один на 1-м этаже	Начальный номер комнаты варьируется от 1 до 99999.	
	Комната номер один на 2-м этаже	Начальный номер комнаты на втором этаже должен основываться на начальном номере комнаты на первом этаже, скорректированном в соответствии с количеством комнат на этаже.	

Добавление VTS

Установите тип устройства как VTS.

Рисунок 3-38 Добавить VTS

Таблица 3-20. Описание добавления VTS.

Параметр	Описание
Номер BTC.	Введите 888888+ номер VTS, который может содержать до 9 цифр. Номер системы управления движением (VTS) можно найти в разделе «Локальные > Номер VTS» системы VTS.
IP-адрес	IP-адрес добавленного BTC.
Пароль для регистрации	Оставьте значение по умолчанию.

Связанные операции

Таблица 3-21. Описание связанных операций.

Операция	Описание
Импорт устройства информация	В этот раздел можно импортировать информацию об устройствах, экспортированную с других устройств. устройство. 1. Нажмите «Импорт» , введите зашифрованный пароль, а затем нажмите «ОК». 2. Нажмите «Обзор» . Выберите файл, а затем нажмите «Открыть». 3. Нажмите ОК.
Экспортное устройство информация	Нажмите «Экспорт» , введите пароль шифрования, указанный в поле, и нажмите «ОК».
Удалить	• Удалять по одному: нажмите  , а затем нажмите ОК. Удалять группами: выберите устройства для удаления, нажмите «Удалить»,  , и затем нажмите «ОК». • Очистить все устройства: Нажмите « Очистить» , а затем нажмите ОК.
Редактировать	Нажмите  для редактирования информации об устройстве.
Позвоните в VTH	Нажмите  Чтобы вызвать соответствующий VTH, нажмите.  чтобы завершить работу домофона.

3.8.1.3.2 Включение автономной конфигурации устройства

Убедитесь, что функция « Настройка устройства в автономном режиме» включена. После включения этой функции...
VTO отправляет информацию из файла конфигурации, чтобы упростить работу устройств, находящихся в автономном режиме, что были добавлены параметры для быстрого подключения к сети. Нажмите « Добавить» для настройки параметров, а затем нажмите хорошо.

Добавление блока VTO

Установите тип устройства как Unit VTO. Отправьте файл конфигурации в VTO вместе с соответствующим содержимым. серийный номер в сети. После включения питания VTO автоматически получает при необходимости настраивает параметры и регистрируется на SIP-сервере.

Рисунок 3-39. Добавить блок VTO.

Add

*

Device Type

Unit VTO

▼

Device Name

Please enter

*

Device SN

Please enter

*

Username

admin

*

Login Password

Please enter

*

IP Address

.

.

.

*

Subnet Mask

.

.

.

*

Default Gateway

.

.

.

*

Port

(1025-65534)

*

Room No./Devic...

Please enter

*

Management C...

888888

*

Main VTO

Yes

▼

*

SIP Server IP

.

.

.

*

SIP Port

5060

(1025-65534)

*

Registration Pas...

.....

SIP Server Userna...

admin

SIP Server Passwo...

Please enter

*

Server Type

Device

▼

First Name

Please enter

Last Name

Please enter

OK

Cancel

Таблица 3-22. Описание блока VTO.

Параметр	Описание
Серийный номер устройства	Введите серийный номер (SN) с этикетки VTO. Информация о конфигурации будет отправлена на VTO вместе с соответствующим серийным номером в сети.
Имя пользователя	Введите имя пользователя и пароль VTO.
Пароль для входа	
IP-адрес	Введите сетевые параметры VTO.
Маска подсети	
Шлюз по умолчанию	
Порт	
Номер комнаты/Номер устройства	Введите номер устройства в разделе «Локальные настройки» на веб-странице VTO.
Центр управления	Укажите номер, по которому VTO будет звонить в центр управления. По умолчанию это 8888888, или вы можете ввести 8888888 + номер VTS. 8888888: Когда устройство выступает в роли SIP-сервера, оно вызывает все VTS в рамках одного SIP-сервера; когда платформа выступает в роли SIP-сервера, она вызывает группу управления вызовами, настроенную на платформе. 8888888+VTS No: Вызов определенного VTS в рамках одного SIP-сервера.  Чтобы увидеть номер VTS, перейдите в раздел «Номер» > «Локальный» в локальном интерфейсе VTS.
Главный VTO	Если это основной VTO, выберите ДА. Если это суб-VTO, выберите НЕТ. Одновременно информация о VTO отправляется на VTN внутри сети, и VTN получает разрешение на добавление соответствующего основного или вспомогательного VTO.
IP-адрес SIP-сервера	Введите IP-адрес SIP-сервера.
SIP-порт	• 5080, когда платформа выступает в качестве SIP-сервера. • 5060, когда устройство выступает в качестве SIP-сервера.
Пароль для регистрации	Оставьте значение по умолчанию.
Имя пользователя SIP-сервера	Необязательный.
Пароль SIP-сервера	 В случае, если для параметра Main VTO установлено значение No, а Server Type — Device, и Sub VTO хочет получить информацию о пользователях от Main VTO, и Main VTO может искать записи о разблокировке и записи о тревогах в Sub VTO, введите имя пользователя и пароль VTO, который выступает в качестве SIP-сервера.

Параметр	Описание
Тип сервера	Вы можете выбрать устройство на сервере, Частный SIP-сервер и сторонний SIP-сервер устройств. • Устройство : Устройство выступает в качестве SIP-сервера. • Частный SIP-сервер : Частная платформа выступает в качестве SIP-сервера. • Сторонний SIP-сервер : Сторонняя платформа выступает в качестве SIP-сервера. сервер.

Станция установки ограждения

Установите тип устройства как «Станция ограждения». Отправьте файл конфигурации станции ограждения на VTN. в сети, и, следовательно, VTN может добавлять суб-VTO. До 20 VTO и станций ограждения. Конфигурацию можно отправить.

Рисунок 3-40. Ограждение. Станция

Add

* Device Type

Fence Station

* Username

admin

* Login Password

Please enter

* IP Address

* Room No./Devic...

Please enter

* Registration Pas...

.....

OK

Cancel

Таблица 3-23. Описание станции ограждения.

Параметр	Описание
Имя пользователя	Введите имя пользователя и пароль, которые вы использовали для входа в систему ограждения. станция.
Пароль для входа	
IP-адрес	Введите IP-адрес станции ограждения.

Параметр	Описание
Номер комнаты/Устройство	Введите номер устройства станции ограждения, который можно найти в Локальные настройки на веб-странице станции ограждения.
Пароль для регистрации	Оставьте значение по умолчанию.

Добавление VTH

Установите тип устройства как «Станция ограждения». Отправьте файл конфигурации станции ограждения на VTH. в сети. После включения VTH он автоматически получает соответствующий сигнал. настраивает конфигурацию и регистрируется на SIP-сервере.

Рисунок 3-41 VTH

Add

*

Device Type

VTH

▼

Device Name

Please enter

*

Device SN

Please enter

*

Username

admin

*

Login Password

Please enter

🔒

*

IP Address

.

.

.

*

Subnet Mask

.

.

.

*

Default Gateway

.

.

.

*

Port

(1025-65534)

*

Room No./Devic...

Please enter

*

Management C...

888888

*

SIP Server IP

.

.

.

*

SIP Port

5060

(1025-65534)

*

Registration Pas...

.....

🔒

First Name

Please enter

Last Name

Please enter

Alias

Please enter

OK

Cancel

Таблица 3-24. Описание добавления VTH.

Параметр	Описание
Серийный номер устройства	Введите серийный номер, указанный на этикетке VTH.
Имя пользователя	Введите имя пользователя и пароль, которые вы использовали для входа в VTH.
Пароль для входа	
IP-адрес	Введите сетевые параметры VTH, которые могут быть автоматически синхронизированы после включения VTH.
Маска подсети	
Шлюз по умолчанию	
Порт	
Номер комнаты/Номер устройства	Введите номер устройства VTH.
Центр управления	Настройте номер, по которому VTO будет звонить в центр управления. По умолчанию это 888888, или вы можете ввести 888888 + номер VTS. • 888888: Когда устройство выступает в роли SIP-сервера, оно вызывает все VTS в рамках одного SIP-сервера; когда платформа выступает в роли SIP-сервера, она вызывает группу управления вызовами, настроенную на платформе. • 888888+VTS No: Вызов определенного VTS в рамках одного SIP-сервера.  Чтобы увидеть номер VTS, перейдите в раздел «Номер» > «Локальный» в локальном интерфейсе VTS.
IP-адрес SIP-сервера	Введите IP-адрес SIP-сервера.
SIP-порт	• 5080, когда платформа выступает в качестве SIP-сервера. • 5060, когда устройство выступает в качестве SIP-сервера.
Пароль для регистрации	Оставьте значение по умолчанию.

Добавление VTS

Установите тип устройства как VTS. Если устройство выступает в качестве SIP-сервера, добавьте информацию о регистрации SIP VTS для регистрации VTS в VTO.

Номер комнаты/номер устройства : введите 888888 + номер VTS, который может содержать до 9 цифр.

Рисунок 3-42 VTS

Add

*

Device Type

VTS

*

Room No./Devic...

Please enter

*

Registration Pas...

.....

OK

Cancel

Связанные операции

Таблица 3-25. Описание связанных операций.

Операция	Описание
Импорт устройства информация	В этот раздел можно импортировать информацию об устройствах, экспортированную с других устройств. 1. Нажмите «Импорт» , введите зашифрованный пароль, а затем нажмите «ОК». 2. Нажмите «Обзор» . , Выберите файл, а затем нажмите «Открыть». 3. Нажмите ОК.
Экспортное устройство информация	Нажмите «Экспорт» , введите пароль шифрования, указанный в поле, и нажмите «ОК».
Удалить	• Удалять по одному: нажмите  , а затем нажмите ОК. Удалять группами: выберите устройства для удаления, нажмите «Удалить», , и затем нажмите «ОК». • Очистить все устройства: Нажмите « Очистить» , а затем нажмите ОК.
Редактировать	Нажмите  для редактирования информации об устройстве.
Позвоните в VTH	Нажмите  Чтобы вызвать соответствующий VTH, нажмите.  чтобы завершить работу домофона.

3.8.2 Использование VTO в качестве SIP-сервера

3.8.2.1 Настройка SIP-сервера

Используйте другой VTO в качестве SIP-сервера.

Процедура

Шаг 1. Выберите «Настройки домофона» > «SIP-сервер».

Шаг 2. Выберите устройство в поле «Тип сервера».



Не включайте SIP-сервер.

Шаг 3. Настройте параметры, а затем нажмите ОК.

Рисунок 3-43. Использование VTO в качестве SIP-сервера.

SIP Server

Server Type

Device

IP/Domain Name

192.168.1.1

Port

5060

Username

8001

Registration Password

SIP Domain

VDP

SIP Server Username

SIP Server Password

Apply

Refresh

Default

Таблица 3-26. Конфигурация SIP-сервера.

Параметр	Описание
IP-адрес/доменное имя	IP-адрес или доменное имя VTO.
Порт	По умолчанию используется код 5060, когда VTO работает в качестве SIP-сервера.
Имя пользователя	Оставьте их по умолчанию.
Пароль для регистрации	
Домен SIP	ВДП.
Имя пользователя SIP-сервера	Имя пользователя и пароль для входа на SIP-сервер.
Пароль SIP-сервера	

Шаг 4. Нажмите «Применить».

3.8.2.2 Настройка локальных параметров

Настройте параметры устройства при использовании другого VTO в качестве SIP-сервера.

Процедура

Шаг 1. Выберите «Настройки домофона» > «Конфигурация локального устройства».

Шаг 2. Настройте параметры.

Рисунок 3-44. Настройка параметров.

Device Type

Door Station

No.

8001

Management Center

888888

Apply

Refresh

Default

Таблица 3-27. Описание параметров.

Параметр	Описание
Тип устройства	Выберите дверную станцию.
Нет.	Номер ВТО. • Номер должен состоять из 4 цифр. Первые 2 цифры должны быть 80, а последние 2 цифры начинаются с 01. Например, 8001. • Если в одном подразделении существует несколько регистрационных номеров транспортных средств (VTO), номер VTO не может повторяться.
Центр управления	Номер телефона для связи с центром управления — 888888. Оставьте его значением по умолчанию.

Шаг 3. Нажмите «Применить».

3.8.3 Использование платформы в качестве SIP-сервера

3.8.3.1 Настройка SIP-сервера

Платформа управления используется в качестве SIP-сервера.

Процедура

Шаг 1. Выберите «Настройки домофона» > «SIP-сервер».

Шаг 2. В поле «Тип сервера» выберите «Частный SIP-сервер» .



Не включайте SIP-сервер.

Рисунок 3-45. Альтернативный сервер.

Local SIP Server

Server Type

Private SIP Server

Server Address

192.168.1.111

Port

5080

SIP No.

8001

Registration Password

••••••••••••••••

SIP Domain

VDP

Device as Alternate Server

Alternate IP

Alternate Server Username

admin

Alternate Server Password

••••••••••••••••

Alternate VTS IP

0

.

0

.

0

.

0

Таблица 3-28. Конфигурация SIP-сервера.

Параметр	Описание
Адрес сервера	IP-адрес платформы.
Порт	По умолчанию используется порт 5080, когда платформа работает в режиме SIP-сервера.
Пароль для регистрации. Оставьте значения по умолчанию.	
Домен SIP	Оставьте значение по умолчанию.
Альтернативный IP-адрес	В случае, если платформа не отвечает, в качестве SIP-сервера будет использоваться альтернативный сервер. • Если вы включите функцию «Дополнительный сервер» , вы настроите устройство. в качестве альтернативного сервера. • Если вы хотите, чтобы другой VTO функционировал в качестве альтернативного сервера, вам необходимо ввести IP-адрес, имя пользователя и пароль этого VTO. В этом случае не включайте функцию «Альтернативный сервер» . • Мы рекомендуем установить основной VTO в качестве резервного сервера.
Альтернативный сервер	После настройки альтернативного сервера, если платформа управления не отвечает, альтернативный сервер будет активирован, чтобы обеспечить взаимодействие VTO и VTH. • Если включена опция «Альтернативный сервер» , устройство устанавливается в качестве альтернативного сервера. сервер. • Если опция «Альтернативный сервер» не включена, введите IP-адрес альтернативного сервера. укажите сервер, его имя пользователя и пароль, чтобы установить VTO в качестве альтернативного сервера. Мы рекомендуем установить основной VTO в качестве резервного сервера.
Имя пользователя	
Пароль	
Альтернативный сервер	Мы рекомендуем установить основной VTO в качестве резервного сервера.
Альтернативный VTS IP	Введите IP-адрес альтернативного VTS. Если платформа управления не отвечает, будет активирован альтернативный VTS, чтобы обеспечить взаимодействие VTO, VTH и VTS.

Шаг 3. Нажмите «Применить».

3.8.3.2 Настройка локальных параметров

Настройте параметры устройства, если платформа используется в качестве SIP-сервера.

Процедура

Шаг 1. Выберите «Настройки домофона» > «Конфигурация локального устройства».

Шаг 2. Настройте параметры.

Рисунок 3-46. Основной параметр

The screenshot shows a configuration window with the following fields and values:

- Device Type:** Door Station (dropdown menu)
- Building No.:** 0 (text input with a checkbox to its right)
- Unit No.:** 0 (text input with a checkbox to its right)
- No.:** 8001 (text input)
- Management Center:** 888888 (text input)

At the bottom of the window are three buttons: **Apply** (blue), **Refresh** (white), and **Default** (white).

Таблица 3-29. Описание параметров.

Параметр	Описание
Тип устройства	Выберите станцию ограждения или дверную станцию в зависимости от места установки.
Здание №	Установите флажок и введите номер здания, в котором установлен дверной блок.
Номер блока	Установите флажок, а затем введите номер устройства, в котором установлена дверная станция.
Нет.	• Номер должен состоять из 4 цифр. Первые 2 цифры должны быть 80, а последние 2 цифры начинаются с 01. Например, 8001. • Если в одном подразделении существует несколько ВТО, номер ВТО не может быть повторено.
Центр управления	Номер телефона по умолчанию при звонке оператора ВТО в службу ВТС — 888888. Оставьте значение по умолчанию.

Шаг 3. Нажмите «Применить».

После настройки имя пользователя на странице «Домофон > SIP» автоматически обновляется. Убедитесь, что имя пользователя совпадает с номером вызова при добавлении устройства на платформу управления.

3.8.3.3 Управление регистрацией

Когда платформа управления работает в качестве SIP-сервера, вы можете просматривать и управлять всеми устройствами, зарегистрированными на SIP-сервере.

Процедура

Шаг 1. Выберите «Настройки домофона» > «Управление регистрацией».

Шаг 2. Вы можете просматривать и редактировать устройства.

Рисунок 3-47. Просмотр и управление устройствами.

Add Refresh							
No.	Client IP	Device Type	Analog Indoor Monitor Start No.	Analog Indoor Monitor End No.	Long No. of the Device	Operation	
1					8001		

3.8.4 Настройка параметров вызова

3.8.4.1 Звонок

Настройка функции вызова устройства. В этом разделе описывается добавление VTH или VTS в режим телефонной книги для прямого вызова VTH или VTS на устройстве.

Справочная информация

После включения функции на экране ожидания отображается значок вызова. Вы можете выбрать один из 3 типов вызовов. Настройки соответствуют настройкам в разделе «Персонализация > Настройки экрана > Настройки ярлыков».

Таблица 3-30. Описание типов звонков.

Тип	Описание
Вызов с клавиатуры	- Стандартный режим : коснитесь значка вызова на экране ожидания, введите номер комнаты, а затем коснитесь значка вызова, чтобы позвонить в комнату. - Телефонная книга : Настройте содержимое на веб-странице. Коснитесь значка вызова на экране ожидания, и добавленный VTH или VTS отобразится на экране. Вы можете нажать на значок, чтобы вызвать VTH или VTS. Список вызовов отображается в соответствии с вашими настройками на веб-странице.
Управление звонками Центр	Нажмите на значок вызова на экране ожидания, чтобы позвонить в центр управления.
Звонок в один клик	- Укажите номер комнаты и нажмите «Применить». - Нажмите на значок вызова на экране ожидания, чтобы позвонить в указанную комнату.

Процедура

Шаг 1. На веб-странице выберите «Настройки домофона» > «Настройка вызовов».

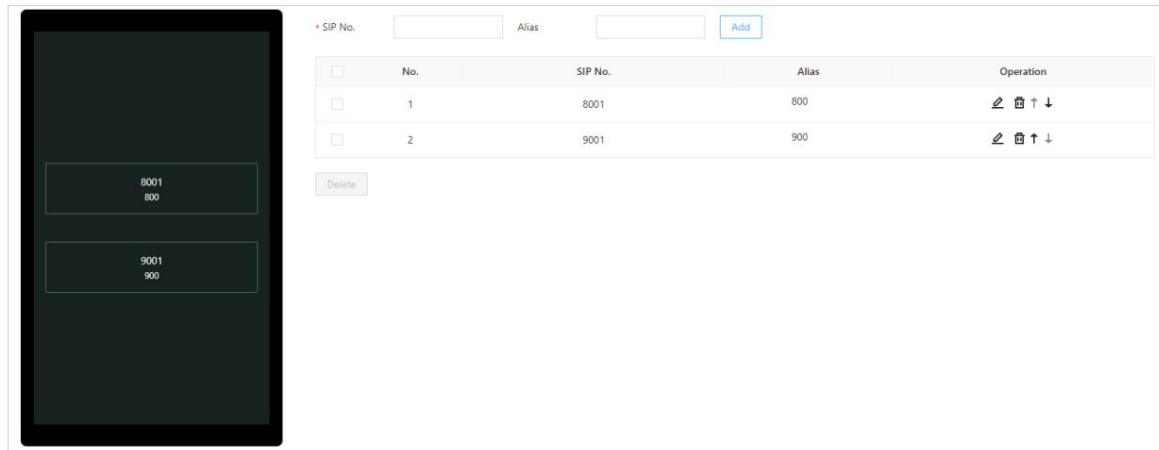
Шаг 2. Включите функцию вызова или дверной звонок , а затем выберите опцию «Вызов» или «Дверной звонок» в качестве способа вызова.

Выберите тип вызова «Вызов с клавиатуры» и режим «Телефонная книга» . Предварительный просмотр отобразится слева, а добавленный VTH или VTS — справа.



- Окно предварительного просмотра списка вызовов различается в зависимости от модели устройства.
- Устройства с горизонтальным экраном диагональю 4,3 дюйма не поддерживают предварительный просмотр списка вызовов.
- Соответствующий тип устройства отображается только в том случае, если устройство установлено в качестве SIP-сервера, и на странице настроек устройства к SIP-серверу добавлены VTH и VTS.

Рисунок 3-48. Тип колл-центра и режим телефонной книги.



Шаг 3. Добавьте VTH и VTS.

Если у VTH есть добавочные номера (например, 9901-0, 9901-1 и 9901-2), а SIP-номер — 9901, то вы можете просто позвонить на этот SIP-номер, и одновременно будут вызваны номера 9901-0, 9901-1 и 9901-2.

- Добавление одного устройства: введите SIP-номер и нажмите «Добавить».

Добавление устройств партиями: если локальное устройство настроено как SIP-сервер, поддерживается пакетное добавление. Перед добавлением устройств партиями необходимо сначала добавить VTH и VTS в разделе «Управление устройствами».

1. Нажмите «Пакетное добавление».

2. Выберите добавленный VTS или VTH, а затем нажмите ОК.

Связанные операции

- Нажмите  чтобы изменить псевдоним устройства.
- Нажмите  чтобы удалить устройство.
- Чтобы изменить порядок устройств, нажмите на них, или просто перетащите устройства в окне предварительного просмотра.

3.8.4.2 Дверной звонок

Установите параметр «Вызов» или «Дверной звонок» в качестве «Дверной звонок», а затем настройте параметры.

Рисунок 3-49. Быстрый вызов настроек.

Password

QR Code

Call or Doorbell

Call or Doorbell

CallDoorbell

Icon

Call Type

One-Click Call

Room No.

9901

Apply

Refresh

Default

Таблица 3-31. Описание параметров.

Параметр	Описание
Локальный звонок устройства.	Нажмите на значок дверного звонка на главном экране устройства, и он зазвонит.
Внешний дверной звонок	Нажмите на значок дверного звонка на главном экране устройства, и внешний дверной звонок зазвонит.  • Функция доступна только на некоторых моделях. • Если функциональный порт 1 не настроен на дверной звонок, при включении внешнего подключения... Для вызова дверного звонка нажмите кнопку ОК во всплывающем окне. Установите выходной порт сигнализации в режим дверного звонка.
Настройка мелодии звонка	Настройте мелодию звонка. Доступны 2 типа мелодий звонка на выбор.
Время звонка (сек.)	Настройте время звонка. По умолчанию оно составляет 3 секунды.

3.9 Настройка учета посещаемости

Эта функция доступна только на некоторых моделях.

3.9.1 Настройка отделов

Процедура

Шаг 1. Выберите «Настройки посещаемости» > «Настройки отдела».

Шаг 2. Нажмите, чтобы  переименовать отдел.

По умолчанию существует 20 отделов. Рекомендуем переименовать их.

Рисунок 3-50. Создание отделов.

Default

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

Связанные операции

Вы можете нажать кнопку «По умолчанию» , чтобы восстановить настройки отделов по умолчанию.

3.9.2 Настройка смен

Настройте смены, чтобы определить правила учета рабочего времени. Сотрудники должны начинать работу в запланированное время и заканчивать ее в запланированное время, за исключением случаев, когда они выбирают работу сверхурочно.

Процедура

Шаг 1. Выберите «Настройки посещаемости» > «Настройки смен».

Шаг 2. Нажмите, чтобы  настроить смену.

Рисунок 3-51. Настройка смены.

Edit Shift

X

* 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 3-32. Описание параметров сдвига.

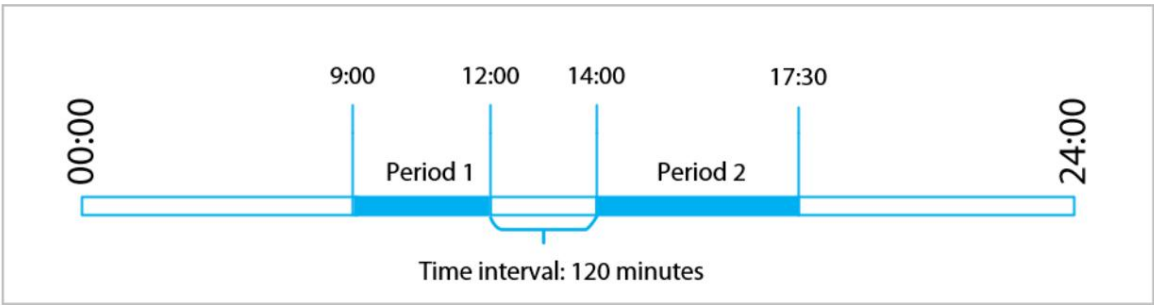
Параметр	Описание
Название смены	Введите название смены.

Параметр	Описание
Период 1	Укажите временной диапазон, в течение которого сотрудники могут отмечать начало и конец рабочего дня. Необходимо настроить как минимум один период. • Если вы установили только один период учета рабочего времени, сотрудники должны отмечать начало и конец рабочего дня в установленное время, чтобы избежать ошибок в их табелях учета рабочего времени. Например, если вы установили период с 08:00 до 17:00, сотрудники должны отметить начало рабочего дня до 08:00 и конец рабочего дня с 17:00 и далее. • Если вы установили 2 периода учета рабочего времени, эти 2 периода не могут быть использованы. Периоды частично совпадают. Сотрудники должны отмечать время прихода и ухода за оба периода. • Если вы зададите 3 периода, они не должны перекрываться. Сотрудники должны отмечать начало и конец рабочего дня для двух смежных периодов.  Последний период может охватывать несколько дней. Если период сверхурочной работы является последним, вы можете настроить его таким образом, чтобы он охватывал несколько дней.
Период 2	
Период 3	
Период сверхурочной работы	Сотрудники, отмечающие время прихода и ухода с работы в течение установленного периода, будут считаться работающими сверх своего обычного рабочего времени.
Ограничение на опоздание (мин)	Сотрудникам может быть предоставлено определенное время для того, чтобы они могли немного опоздать на работу и немного раньше уйти. Например, если обычное время начала работы — 08:00, то допустимый период в 5 минут может быть установлен для сотрудников, прибывших к 08:05, чтобы их не считали опоздавшими.
Ограничение на досрочный отъезд (мин)	

Если вы настраиваете несколько периодов, обратитесь к приведенным ниже инструкциям для выполнения функции учета рабочего времени.

- Если интервал времени между двумя периодами четный, можно разделить его на 2 и отнести первую половину интервала к первому периоду в качестве времени окончания работы. Вторую половину интервала следует отнести ко второму периоду в качестве времени начала работы.

Рисунок 3-52. Временной интервал (четное число).



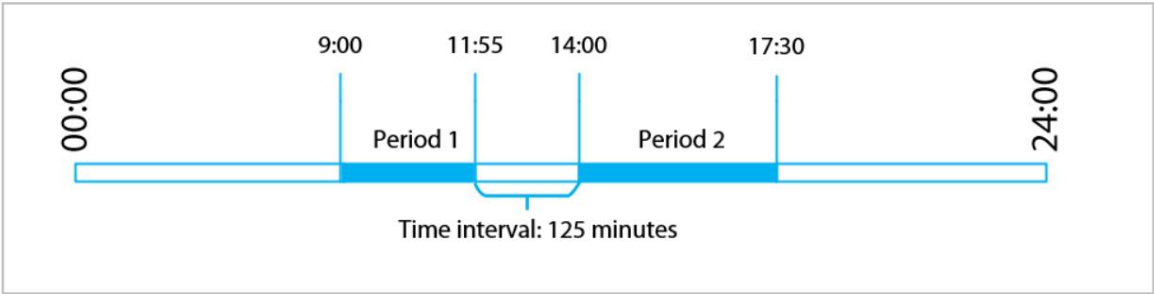
Например: если интервал составляет 120 минут, то время окончания работы в период 1 — с 12:00 до 12:59, а время начала работы в период 2 — с 13:00 до 14:00.



Если сотрудник несколько раз отмечает свой уход в течение первого периода, будет действовать самое позднее время, а если он несколько раз отмечает свой приход в течение второго периода, будет действовать самое раннее время.

- Если интервал времени между двумя периодами нечетный, то наименьшая часть интервала будет отнесена к первому периоду и будет являться временем окончания работы. Наибольшая часть интервала будет отнесена ко второму периоду и будет являться временем начала работы.

Рисунок 3-53. Временной интервал (нечетное число).



Например: если интервал составляет 125 минут, то время окончания первого периода — с 11:55 до 12:57, а время начала второго периода — с 12:58 до 14:00. Первый период длится 62 минуты, а второй — 63 минуты.



Если сотрудник несколько раз отмечает свой уход в течение первого периода, будет действовать самое позднее время, а если он несколько раз отмечает свой приход в течение второго периода, будет действовать самое раннее время. • Если

период только один, и вы не отмечаете свой приход или уход к установленному времени, то
Считается отсутствующим в течение 1 дня.

- Если периодов несколько, и вы не отмечаете время начала или окончания работы в установленное время.
Если вы не отметились при приходе или уходе с работы в установленное время (2 или более периодов), это считается отсутствием на 1 день. Присутствие в сверхурочное время не меняет статус отсутствия.

человек.

Если вы настроили последний период таким образом, чтобы он охватывал несколько дней, обратитесь к приведенным ниже инструкциям для выполнения функции учета рабочего времени.

- Если второй день — обычная смена, посещаемость соответствует обычному графику.
- Если второй день — праздничный день, вы можете отметить свой уход в любое время в течение 24 часов.
праздничный день.



Все данные о времени прихода и ухода указаны с точностью до секунды. Например, если обычное время начала работы установлено на 8:05 утра, сотрудник, отметившийся в 8:05:59 утра, не будет считаться опоздавшим. Однако сотрудник, прибывший в 8:06 утра, будет отмечен как опоздавший на 1 минуту.

Шаг 3. Нажмите ОК.

Похожие операции. Вы можете нажать

«По умолчанию», чтобы восстановить заводские настройки переключения передач.

3.9.3 Настройка праздников

Настройте планы отпусков, чтобы установить периоды, когда посещаемость не будет отслеживаться.

Процедура

Шаг 1. Выберите «Настройки посещаемости» > «Настройки смен» > «Праздничные».

Шаг 2. Нажмите «Добавить», чтобы добавить планы на отпуск.

Шаг 3. Настройте параметры.

Рисунок 3-54. Составьте планы на праздники.

Add Attendance Holiday

* Attendance Holiday ...

1

* Attendance Holiday

Attendance Holiday for October

* Time

2023-10-01 → 2023-10-07

OK

Cancel

Таблица 3-33. Описание параметров.

Параметр	Описание
Выходной день, связанный с посещаемостью.	Номер праздника.
Выходной день, связанный с посещаемостью	Название праздника.
Время начала	Время начала и окончания праздника.
Конец времени	

Шаг 4. Нажмите OK.

3.9.4 Настройка графиков работы

График работы обычно включает в себя количество дней в месяц и количество часов в день, в течение которых сотрудник должен находиться на рабочем месте. Можно создавать различные типы графиков работы для разных сотрудников или отделов, и в этом случае сотрудники должны следовать установленному графику.

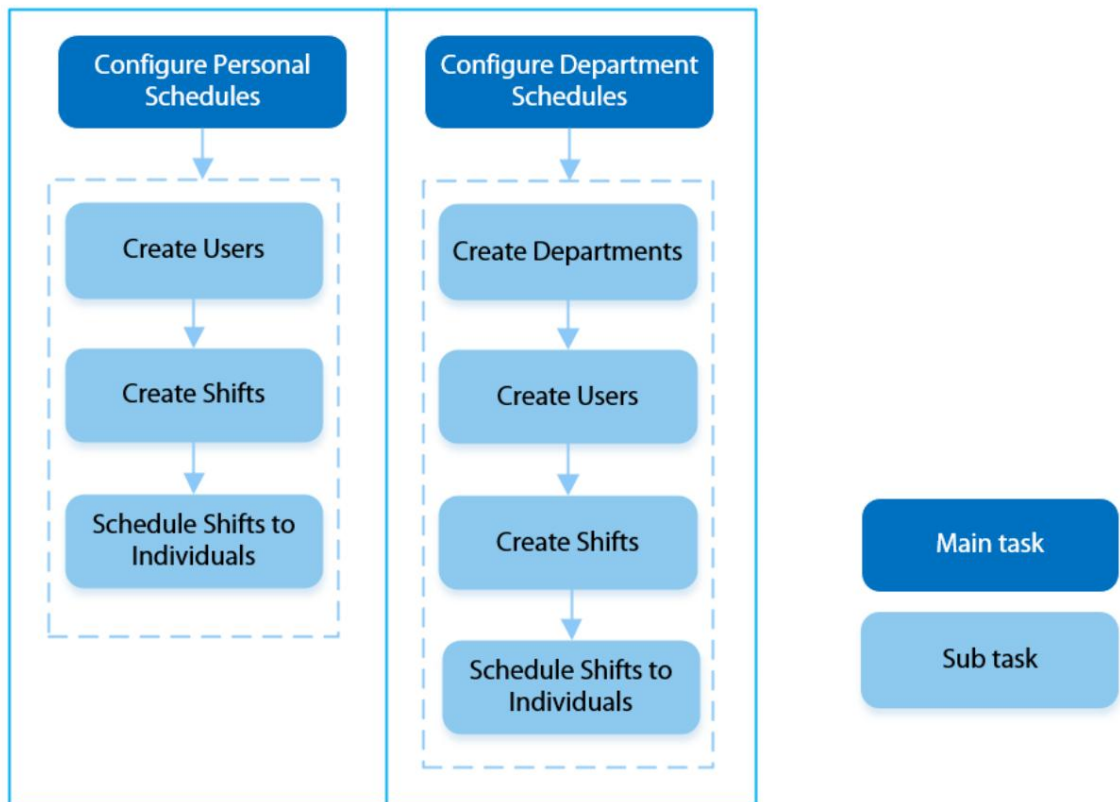
Справочная информация

Для настройки личного или departmental-графика обратитесь к блок-схеме.



При настройке расписания не должно быть перекрывающихся временных периодов в один и тот же день, а также в предыдущий или последующий день.

Рисунок 3-55. Настройка графиков работы.



Процедура

Шаг 1. Выберите «Настройки посещаемости» > «Настройки расписания».

Шаг 2. Составьте рабочие графики для отдельных сотрудников.

1. Нажмите «Личное расписание».
2. Выберите человека из списка.
3. В календаре выберите день, а затем выберите смену.

Вы также можете нажать кнопку «Настроить пакетную обработку», чтобы запланировать смены на несколько дней.

Рисунок 3-56. Личное расписание.



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

• 0 означает перерыв. •

От 1 до 24 указывает номер predetermined смен. Инструкции по настройке смен см. в разделе "2.11.1 Настройка смен". • 25

означает командировку. • 26

означает отпуск.

Шаг 3. Составьте графики работы для отделов.

1. Нажмите «Расписание отдела».

2. Выберите отдел из списка отделов.

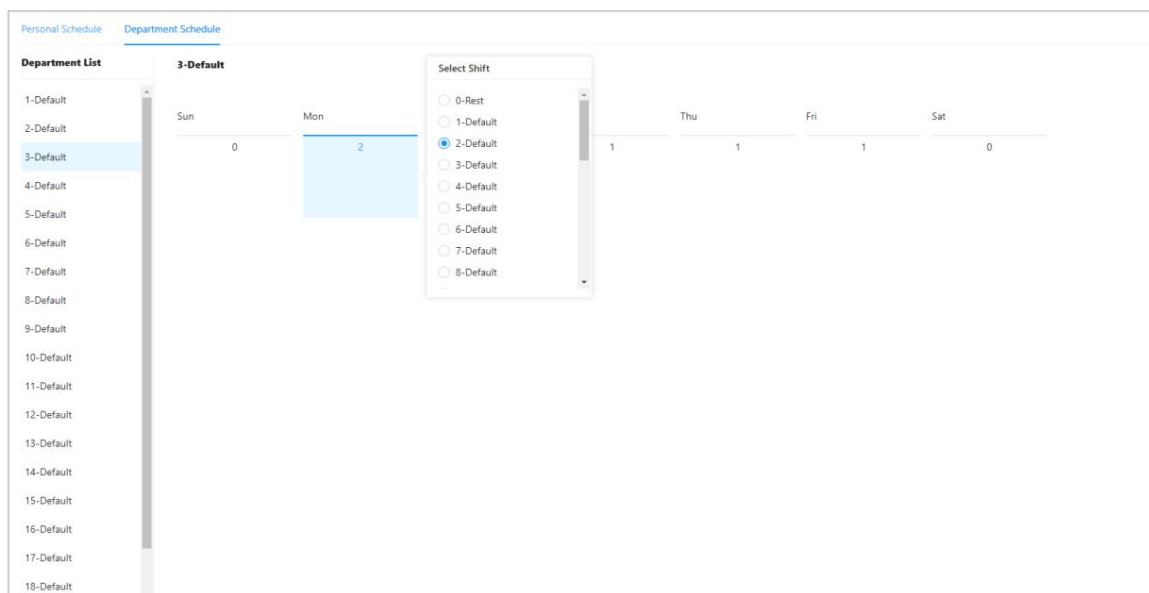
3. В календаре выберите день, а затем выберите смену.

• 0 означает отдых.

• Цифры от 1 до 24 указывают количество predetermined смен. Инструкции по настройке смен см. в разделе "2.11.1 Настройка смен". • 25 означает командировку.

• 26 означает отпуск.

Рисунок 3-57. График смен в отделе.



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

3.9.5 Экспорт журнала посещаемости

Вы можете экспортировать записи о разблокировке и записи о посещаемости.

Процедура

Шаг 1. Выберите «Настройки посещаемости» > «Отчеты о посещаемости».

Шаг 2. Выберите тип, укажите дату, а затем нажмите «Экспорт».

- Для устройства контроля доступа вы можете выбрать тип в разделе «Записи разблокировки». , 1 месяц
Посещаемость и аномальная посещаемость.
- Для устройства учета посещаемости вы можете выбрать тип из разделов «Учет посещаемости», , 1
«Ежемесячная посещаемость» и «Нештатная посещаемость».
- Если вы выберете «Отчет о посещаемости за 1 месяц», то получите персональный отчет о посещаемости или подробный отчет о посещаемости.
Отчет и сводка посещаемости экспортируются одновременно.



Экспортированные файлы имеют формат XML.

Рисунок 3-58 Экспорт записи

3.9.6 Настройка режимов учета посещаемости

Процедура

- Шаг 1. Выберите «Настройки посещаемости» > «Настройки посещаемости».
- Шаг 2. Включите локальную регистрацию посещаемости, а затем установите режим регистрации посещаемости.
- Шаг 3. Настройка режимов учета посещаемости.

Рисунок 3-59 Режимы посещаемости

Local Attendance

Mode Settings

Auto/Manual ModeAuto ModeManual ModeFixed 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 3-34 Режим посещаемости

Параметр	Описание
Автоматический/Ручной режим	После регистрации начала и окончания рабочего дня на экране автоматически отображается статус посещаемости, но вы также можете изменить свой статус посещаемости вручную. • Регистрация начала работы: Отметьте начало вашего обычного рабочего дня. • Регистрация окончания работы: Отметьте окончание работы, когда начинается ваш перерыв. • Регистрация начала работы: Отметьте окончание работы, когда заканчивается ваш перерыв. • Регистрация окончания работы: Отметьте окончание работы, когда заканчивается ваш обычный рабочий день. • Регистрация начала сверхурочной работы: Отметьте начало вашего сверхурочного периода. • Регистрация окончания сверхурочной работы: Отметьте окончание вашего сверхурочного периода.

Параметр	Описание
Автоматический режим	На экране автоматически отображается ваш статус присутствия после того, как вы отмечаете начало или конец рабочего дня. • Регистрация начала работы: Отметьте начало вашего обычного рабочего дня. • Регистрация окончания работы: Отметьте окончание работы, когда начинается ваш перерыв. • Регистрация начала работы: Отметьте окончание работы, когда заканчивается ваш перерыв. • Регистрация окончания работы: Отметьте окончание работы, когда заканчивается ваш обычный рабочий день. • Регистрация начала сверхурочной работы: Отметьте начало вашего сверхурочного периода. • Регистрация окончания сверхурочной работы: Отметьте окончание вашего сверхурочного периода.
Ручной режим	При регистрации начала и окончания рабочего дня вы можете вручную выбрать свой статус присутствия.
Фиксированный режим	При регистрации начала или окончания рабочего дня 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 восстановить предыдущие настройки.
- По умолчанию: Восстановить заводские настройки учета посещаемости.

3.10 Настройка аудио и видео

3.10.1 Настройка видео

Процедура

Шаг 1. Выберите «Настройка аудио и видео» > «Видео».

Шаг 2. Настройте битрейт.

Рисунок 3-60 Битрейт

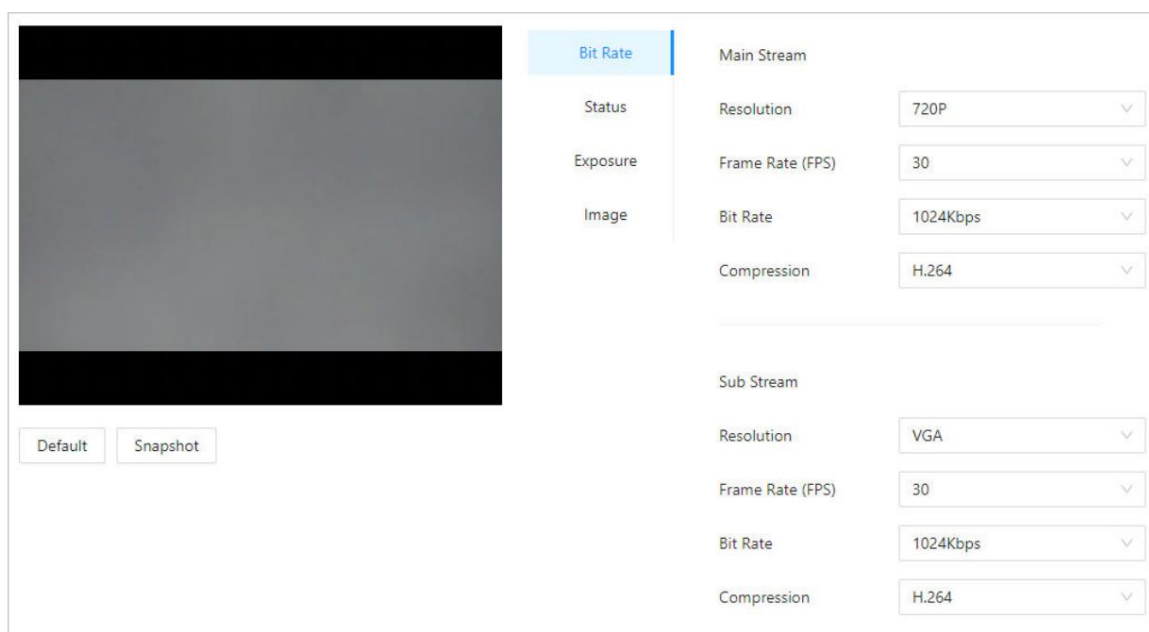


Таблица 3-35. Описание скорости передачи данных.

Параметр		Описание
Основной формат	Разрешение	Когда устройство функционирует как VTO и подключается к VTH, ограничение на размер получаемого потока VTH составляет 720p. При изменении разрешения на 1080p это может повлиять на работу функций вызова и мониторинга.
	Частота кадров (FPS)	Количество кадров (или изображений) в секунду.
	Битрейт	Объем данных, передаваемых по интернет-соединению за определенный промежуток времени. Выберите подходящее значение в зависимости от скорости вашей сети.
	Сжатие	Стандарт сжатия видео, обеспечивающий хорошее качество видео при более низких битрейтах.
Подпоток	Разрешение	Дополнительный поток поддерживает D1, VGA и QVGA.
	Частота кадров (FPS)	Количество кадров (или изображений) в секунду.
	Битрейт	Это показатель объема данных, передаваемых по интернет-соединению за определенный промежуток времени.
	Сжатие	Стандарт сжатия видео, обеспечивающий хорошее качество видео при более низких битрейтах.

Шаг 3. Настройте статус.

Рисунок 3-61. Статус

The image shows a settings interface with a sidebar on the left containing four options: Bit Rate, Status (highlighted in blue), Exposure, and Image. The main content area is titled 'Status' and contains the following settings:

- Scene Mode:** A dropdown menu set to 'Auto'.
- Day/Night:** A dropdown menu set to 'Color'.
- Compensation Mode:** A dropdown menu set to 'WDR'.
- Brightness:** A horizontal slider with a blue knob, ranging from a minus sign to a plus sign, with the value '30' displayed on the right.
- Video Standard:** A dropdown menu set to 'NTSC'.

Таблица 3-36. Описание параметров состояния.

Параметр	Описание
Режим сцены	Оттенок изображения различается в зависимости от режима съемки. • Закрыть : Функция режима сцены отключена. • Авто : Система автоматически регулирует режим сцены в зависимости от... на основе фоточувствительности. • Солнечный : В этом режиме оттенок изображения будет уменьшен. • Ночной : В этом режиме оттенок изображения будет увеличен.
День/Ночь	Режим «День/Ночь» влияет на компенсацию освещенности в разных ситуациях. • Авто : Система автоматически регулирует дневной/ночной режим в зависимости от светочувствительности. • Цветной : В этом режиме изображения получаются цветными. • Черно-белый : В этом режиме изображения отображаются в черно-белом цвете.
Режим компенсации	• Отключить : Компенсация выключена. • BLC : Компенсация подсветки автоматически увеличивает освещенность темных участков изображения, когда яркий свет, падающий сзади, заслоняет их. • WDR : Система затемняет светлые участки и компенсирует темные, создавая баланс для улучшения общего качества изображения. • HLC : Компенсация подсветки (HLC) — это технология, используемая в Камеры видеонаблюдения/IP-камеры предназначены для обработки изображений, снятых при освещении, например, фарами или прожекторами. Датчик изображения камеры обнаруживает яркие источники света в видео и уменьшает экспозицию в этих местах для повышения общего качества изображения.
Видеостандарт	Выберите один из стандартов: PAL или NTSC.

Шаг 4. Настройте параметры экспозиции.

Рисунок 3-62. Воздействие

Bit Rate

Status

Exposure

Image

Anti-flicker

Outdoor

Exposure Mode

Manual

Shutter

Custom Range

Shutter Range

0

-

20

(0-40)ms

Gain

0

-

80

(0-100)

Exposure Compensation

-

+

50

3D NR

NR Level

-

+

50

Таблица 3-37. Описание параметров воздействия.

Параметр	Описание
Защита от мерцания	Установите функцию подавления мерцания, чтобы уменьшить мерцание и снизить неравномерность цветопередачи. КОНТАКТ. • 50 Гц : При частоте электросети 50 Гц воздействие составляет Автоматическая регулировка в зависимости от яркости окружающей среды для предотвращения появления горизонтальных линий. • 60 Гц : При частоте электросети 60 Гц экспозиция Автоматическая регулировка в зависимости от яркости окружающего освещения для уменьшения появления горизонтальных линий. • На улице : При выборе режима «На улице» можно выбрать режим экспозиции. переключилось.

Параметр	Описание
Режим экспозиции	Вы можете настроить экспозицию для регулировки яркости изображения. • Автоматический режим : Устройство автоматически регулирует яркость изображений, исходя из окружающей обстановки. • Приоритет выдержки : Устройство регулирует яркость изображения в соответствии с заданным диапазоном выдержки. Если изображение недостаточно яркое, но значение выдержки достигло верхнего или нижнего предела, устройство автоматически отрегулирует значение усиления для достижения оптимального уровня яркости. • Ручной режим : Вы можете вручную отрегулировать усиление и значение выдержки для регулировки яркости изображения.  ◇ При выборе пункта «На открытом воздухе» в списке «Защита от мерцания» можно выбрать режим приоритета выдержки . ◇ Режим экспозиции может отличаться в зависимости от модели устройства.
Затвор	Затвор — это элемент, пропускающий свет в течение определенного времени. Чем больше выдержка, тем короче время экспозиции и тем темнее изображение. Вы можете выбрать диапазон выдержек или добавить собственный диапазон.
Прирост	При установке диапазона значений усиления качество видео улучшится.
Контакт Компенсация	Видео станет ярче, если отрегулировать значение компенсации экспозиции.
3D NR	При включении функции 3D-шумоподавление (RD) можно уменьшить видеошум, чтобы обеспечить более высокое разрешение видео.
Уровень NR	При включении этой функции можно установить уровень детализации изображения. Более высокий уровень детализации означает более четкое изображение.

Шаг 5. Настройте образ.

Рисунок 3-63 Изображение

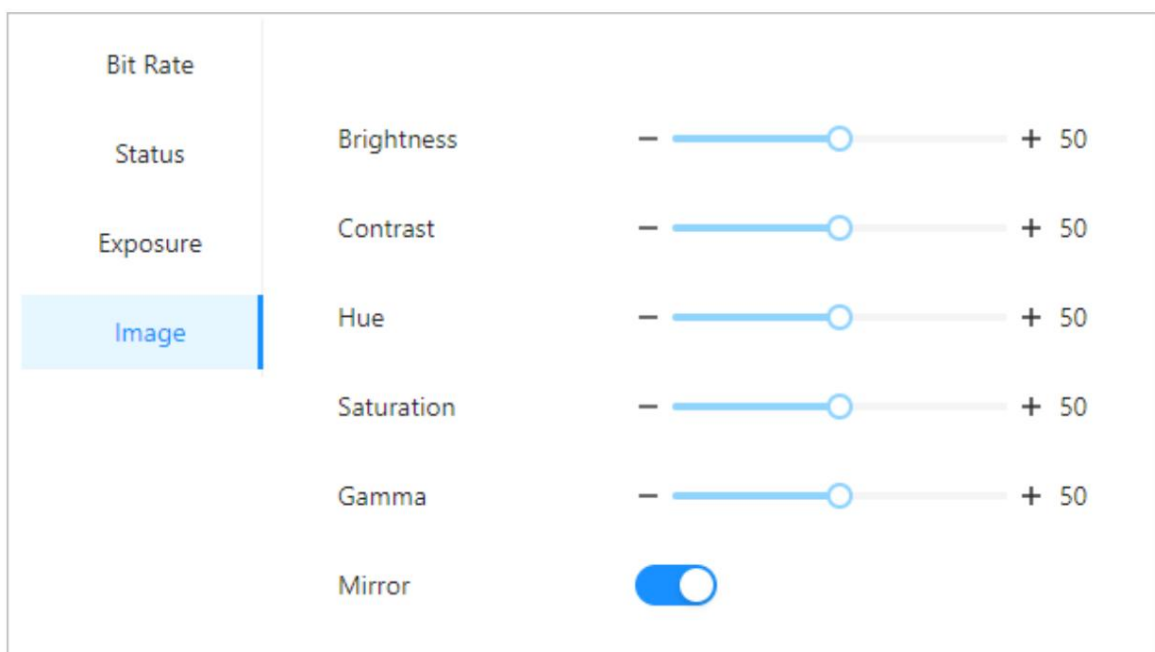


Таблица 3-38. Описание изображения.

Параметр	Описание
Яркость	Яркость изображения. Чем выше значение, тем ярче изображение.
Контраст	Контраст — это разница в яркости или цвете, которая позволяет различить объект. Чем выше значение контраста, тем больше будет цветовой контраст.
Оттенок	Относится к интенсивности или насыщенности цвета. Описывает яркость цвета или его чистоту.
Насыщенность	Насыщенность цвета указывает на интенсивность цвета в изображении. Чем выше насыщенность, тем насыщеннее цвет, например, тем больше в нем красного или синего.  Значение насыщенности не изменяет яркость изображения.
Гамма	Изменяйте яркость и контрастность изображения нелинейным способом. Чем выше значение, тем ярче изображение.
Зеркало	При включении этой функции изображения будут отображаться с перевернутыми левой и правой сторонами. Экран устройства не поддерживает настройку и всегда отображает зеркальное изображение.

Связанные операции

- По умолчанию: Нажмите «По умолчанию», и параметры на этой странице будут восстановлены до значений по умолчанию.
- Снимок экрана: Нажмите «Снимок экрана», чтобы сделать снимок экрана текущего устройства.

3.10.2 Настройка аудиоподсказок

Настройте звуковые подсказки во время подтверждения личности.

Процедура

Шаг 1. Выберите «Настройка аудио и видео» > «Аудио».

Шаг 2. Настройте параметры звука.

Device Volume

+ 80

Intercom Volume

+ 80

Microphone Volume

+ 90

Key Sound

☐

Audio Collection

Enable

Only supports MP3 files that are less than 100 KB with a sampling rate of 16K.

Audio File

Audio Type	Audio File	Modify
Successfully verified.	-	
Failed to verify.	-	
Not wearing face mask.	-	

DND Mode

☐

Apply

Refresh

Default

Параметры	Описание
Объем устройства	Регулируйте громкость динамика, когда устройство не находится в режиме внутренней связи.
Громкость домофона	Отрегулируйте громкость динамика, когда устройство находится в режиме внутренней связи.
Громкость микрофона	Установите громкость микрофона.
Ключевой звук	При включении этой функции сенсорные устройства будут выдавать Звук касания и устройства без сенсорного экрана будут имитировать работу мыши. Щелчок.
Аудиоколлекция	Если эта функция включена, звук из микрофона устройства будет Запись производилась в режиме реального времени и во время видеозаписи.
Аудиофайл	Вы можете загружать аудиофайлы на устройство.
Режим «Не беспокоить»	В течение установленного времени при подтверждении вашей учетной записи голосовые подсказки не звучат. Идентификатор устройства. Можно установить до 4 периодов.

Шаг 3. Нажмите, чтобы загрузить аудиофайлы на платформу для каждого типа аудио.

Поддерживаются только MP3-файлы размером менее 20 КБ с частотой дискретизации 16 кГц.

Шаг 4. Нажмите «Применить».

3.10.3 Настройка обнаружения движения

При обнаружении движущихся объектов и достижении заданного порогового значения экран включится.

Справочная информация



Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. Выберите «Настройки аудио и видео» > «Настройки обнаружения движения».

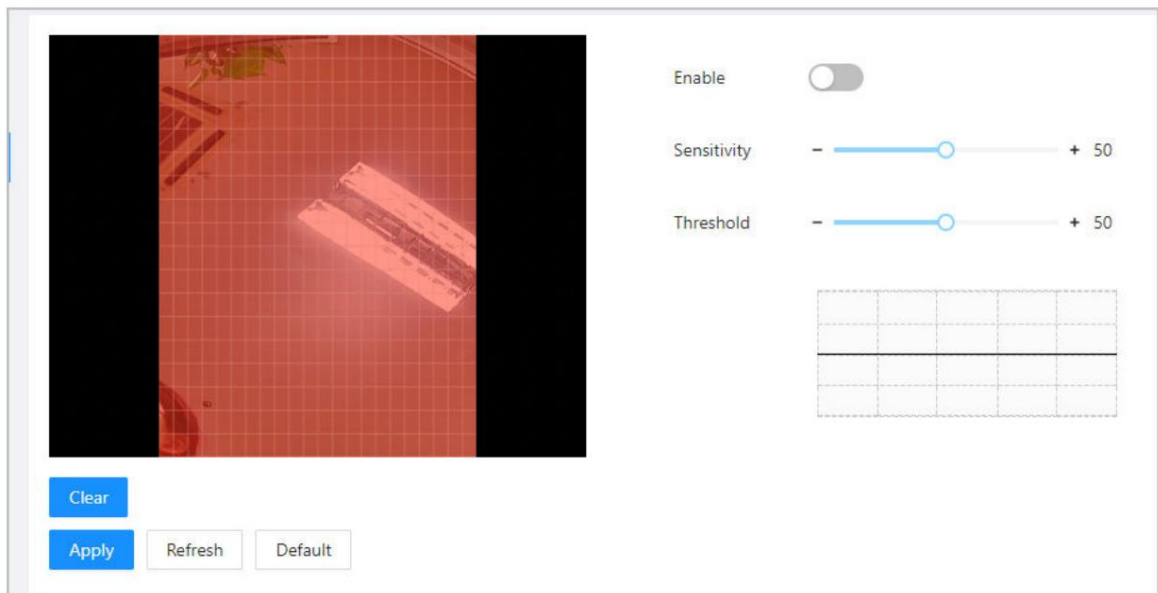
Шаг 2. Включите функцию обнаружения движения.

Шаг 3 Нажмите и удерживайте левую кнопку мыши, затем нарисуйте область обнаружения в красной зоне.



- Область обнаружения движения отображается красным цветом.
- Чтобы удалить существующую область обнаружения движения, нажмите «Очистить».
- Если вы нарисуете область обнаружения движения в стандартной области обнаружения движения, она не будет использоваться для обнаружения движения.

Рисунок 3-65. Зона обнаружения движения.



Шаг 4. Настройте параметры.

- Чувствительность: Восприимчивость к окружающей среде. Чем выше чувствительность, тем легче сработать тревога.
- Порог: Процент площади движущегося объекта, находящейся в зоне обнаружения движения. Более высокий порог означает более легкое срабатывание сигнализации.

Шаг 5. Нажмите «Применить».

Функция обнаружения движения срабатывает при отображении красных линий; при отсутствии срабатывания отображаются зеленые линии.

3.10.4 Настройка локального кода

Настройте область просмотра в видеообращении и предварительном просмотре.

Справочная информация



• Эта функция доступна только на некоторых моделях. • Эта функция включена по умолчанию при работе с VTN. Предварительный просмотр может быть недоступен, если эта функция отключена.

Процедура

Шаг 1. Войдите на веб-страницу.

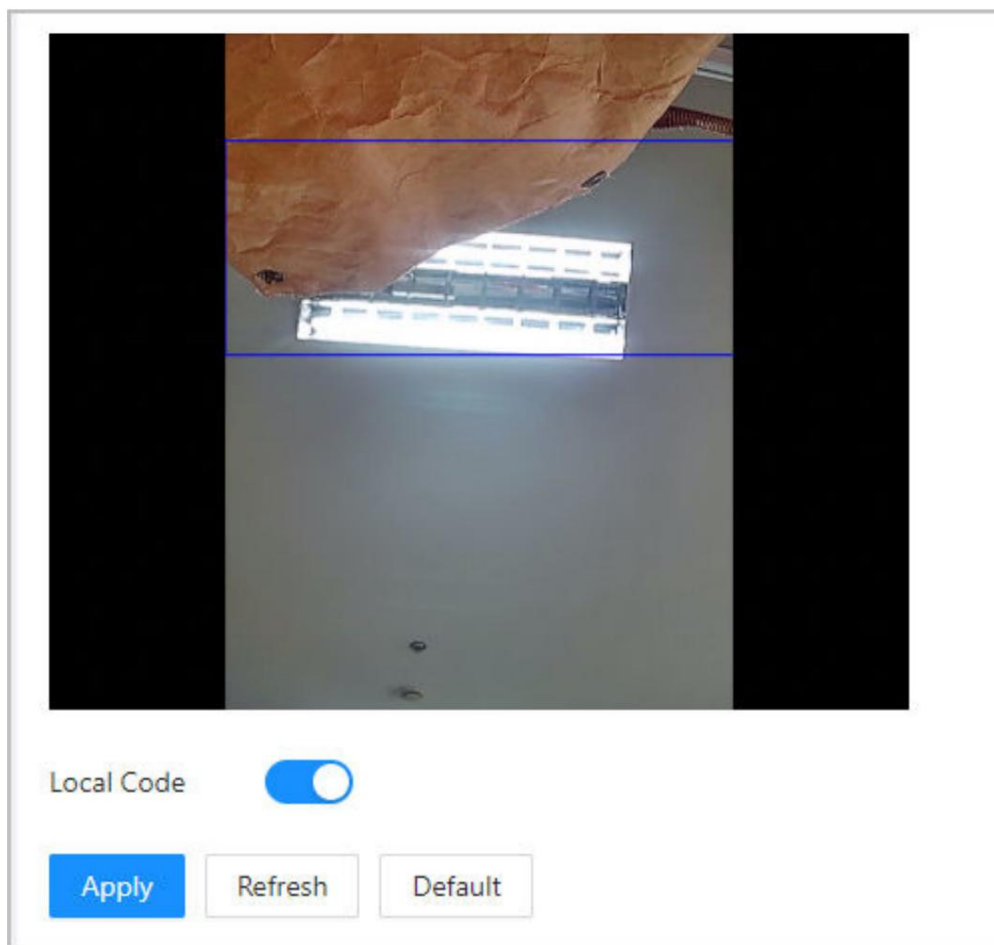
Шаг 2. Выберите «Настройка аудио и видео» > «Локальный код».

Шаг 3. Выберите «Включить», чтобы активировать функцию.

Шаг 4. Перетащите прямоугольник в указанное место.

В рамке указана область предварительного просмотра во время видеоконференции.

Рисунок 3-66 Локальное кодирование



Шаг 5. Нажмите «Применить».

3.11 Настройки связи

3.11.1 Сетевые настройки

3.11.1.1 Настройка TCP/IP

Необходимо настроить IP-адрес устройства, чтобы обеспечить его связь с другими устройствами.

Процедура

~~Шаг 1.~~ Выберите «Настройки связи» > «Настройки сети» > «TCP/IP».

~~Шаг 2.~~ Настройте параметры.

Рисунок 3-67 TCP/IP

NIC

NIC 1

Mode

☐ DHCP

☒ Static

MAC Address

90 : 02 : : 51 : 9f

IP Version

IPv4

IP Address

172 . . 103

Subnet Mask

255 . . 0

Default Gateway

172 . . 1

Preferred DNS

8 . . 8

Alternate DNS

8 . . 4

MTU

1500

Transmission Mode

☒ Multicast

☐ Unicast

Apply

Refresh

Default

Таблица 3-40. Описание TCP/IP.

Параметр	Описание
Режим	• Статический режим: Введите IP-адрес, маску подсети и шлюз вручную. • DHCP: расшифровывается как Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста). При включении DHCP устройство будет автоматически Назначается с указанием IP-адреса, маски подсети и шлюза.
MAC-адрес	MAC-адрес устройства.
IP-версия	IPv4 или IPv6.

Параметр	Описание
IP-адрес	Если вы установите режим «Статический», настройте IP-адрес, маску подсети и шлюз.
Маска подсети	
Шлюз по умолчанию	 - IPv6-адрес представляется в шестнадцатеричном формате. • Для версий IPv6 не требуется установка масок подсети. - IP-адрес и шлюз по умолчанию должны совпадать. сегмент сети.
Предпочитаемый DNS	Укажите IP-адрес предпочтительного DNS-сервера.
Альтернативный DNS	Укажите IP-адрес альтернативного DNS-сервера.
MTU	MTU (Maximum Transmission Unit) — это максимальный размер данных, которые могут быть переданы в одном сетевом пакете в компьютерных сетях. По умолчанию он равен 1500.
Режим передачи	- Многоадресная рассылка: идеально подходит для видеозвонков. - Одноадресная передача: идеально подходит для групповых звонков.

Шаг 3. Нажмите ОК.

3.11.1.2 Настройка Wi-Fi



- Одновременное включение Wi-Fi и точки доступа Wi-Fi невозможно. •
- Функция Wi-Fi доступна только на некоторых моделях.

Процедура

Шаг 1. Выберите «Настройки связи» > «Настройки сети» > «Wi-Fi».

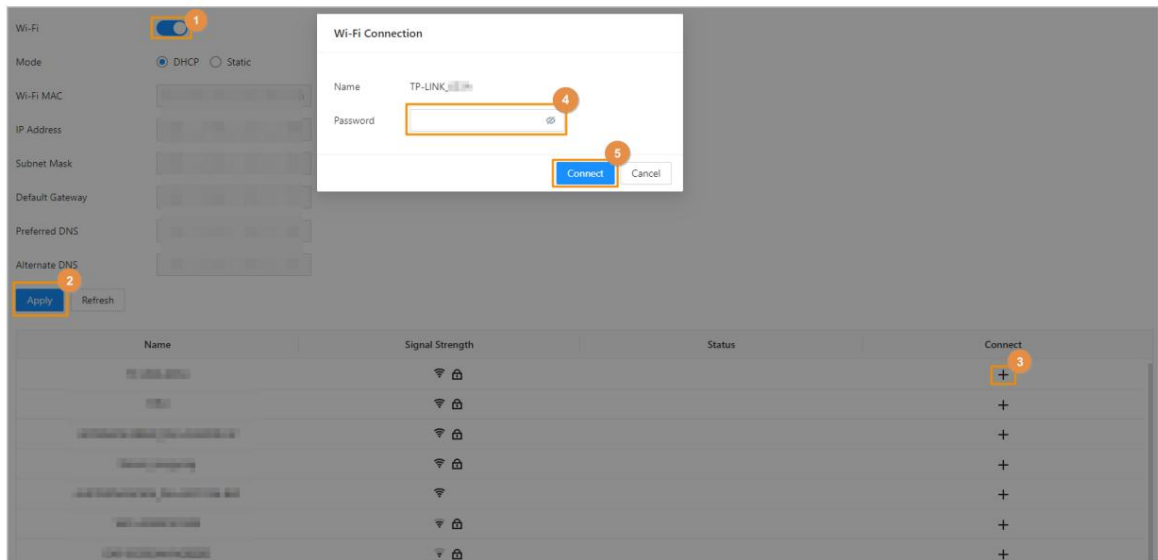
Шаг 2. Включите Wi-Fi, а затем нажмите «Применить».

Отображаются все доступные сети Wi-Fi.

Шаг 3. Нажмите кнопку «+», а затем введите пароль от сети Wi-Fi.

Wi-Fi подключен.

Рисунок 3-68 Wi-Fi



Шаг 4 (необязательно) Добавьте Wi-Fi вручную.

Если сеть Wi-Fi не обнаружена, вы можете добавить её вручную.

1. Нажмите «Добавить».

2. Введите название и пароль сети Wi-Fi, а затем нажмите «Подключиться».

Результаты

После успешного подключения статус Wi-Fi отображается как «Подключено» .



Если подключены как Wi-Fi, так и проводная сеть, приоритет будет отдаваться Wi-Fi.

Связанные операции

Вы можете вручную изменить IP-адрес сети Wi-Fi. • DHCP:

Включите эту функцию и нажмите «Применить», устройству будет автоматически назначена сеть Wi-Fi-адрес.

- Статический режим: Включите эту функцию, вручную введите Wi-Fi-адрес, затем нажмите «Применить», и устройство подключится к Wi-Fi.

3.11.1.3 Настройка точки доступа Wi-Fi



- Функция Wi-Fi доступна в некоторых моделях.
- 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 функцию, а затем нажмите «Применить».

Рисунок 3-69 Точка доступа Wi-Fi

The screenshot shows a configuration window for a Wi-Fi access point. It contains the following elements:

- Enable:** A toggle switch that is currently turned off.
- SSID:** A text input field containing a blurred network name.
- Security:** A dropdown menu showing a blurred security protocol.
- Password:** A text input field containing a blurred password.
- IP Address:** A text input field containing a blurred IP address.
- QR Code:** A square QR code located below the IP address field, used for quick connection.
- Buttons:** Three buttons at the bottom: 'Apply' (blue), 'Refresh' (white), and 'Default' (white).

Результаты

После включения вы сможете подключиться к Wi-Fi устройства через свой телефон и войти на веб-страницу устройства на своем телефоне.

3.11.1.4 Настройка порта

Вы можете одновременно ограничить доступ к устройству через веб-страницу, настольное приложение и мобильное приложение.

Процедура

Шаг 1. Выберите «Настройки связи» > «Настройки сети» > «Порт».

Шаг 2. Настройте порты.



За исключением параметров Max Connection и RTSP Port, для вступления изменений в силу после изменения остальных параметров необходимо перезагрузить устройство.

Рисунок 3-70. Настройка портов.

Max Connection	50	(1-50)
TCP Port	3777	(1025-65535)
HTTP Port	80	
HTTPS Port	443	
RTSP Port	554	
Apply Refresh Default		

Таблица 3-41. Описание портов.

Параметр	Описание
Максимальное соединение	Вы можете установить максимальное количество клиентов (например, веб-страниц, настольных компьютеров и мобильных устройств), которые могут одновременно получать доступ к устройству.
TCP-порт	Значение по умолчанию — 37777.
HTTP-порт	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 «Применить».

3.11.1.5 Настройка базового сервиса

Для подключения устройства к сторонней платформе включите функции CGI и ONVIF.

Процедура

Шаг 1. Выберите «Настройки связи» > «Сетевые настройки» > «Основные службы».

Шаг 2. Настройка базовой службы.

Рисунок 3-71. Базовое обслуживание.

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 3-42. Описание основных параметров обслуживания.

Параметр	Описание
SSH	SSH, или протокол Secure Shell, — это протокол удалённого администрирования, позволяющий пользователям получать доступ к удалённым серверам, управлять ими и изменять их через Интернет.
Поиск по многоканальной/широковещательной рассылке	Поиск устройств с использованием многоадресного или широковещательного протокола.
CGI	Общий интерфейс шлюза (CGI) представляет собой точку пересечения между веб-серверами, через которую возможен стандартизированный обмен данными между внешними приложениями и серверами.
ОНВИФ	ONVIF расшифровывается как Open Network Video Interface Forum (Форум открытых сетевых видеоинтерфейсов). Его цель — обеспечить стандарт для взаимодействия между различными IP-устройствами безопасности. Эти стандартизированные спецификации ONVIF представляют собой своего рода общий язык, который все устройства могут использовать для обмена данными.
Аварийное техническое обслуживание	Она включена 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 использованием методов аутентификации Digest, DES и открытого текста, что повышает безопасность устройства. • Совместимый режим: поддерживает доступ к устройству с использованием методов аутентификации Digest, DES и открытого текста, но с пониженным уровнем безопасности.
Частный протокол	Платформа добавляет устройства по частному протоколу.

Параметр	Описание
TLSv1.1	TLSv1.1 означает Transport Layer Security версии 1.1. TLS — это криптографический протокол, предназначенный для обеспечения безопасной и аутентифицированной связи в компьютерной сети.  Протокол TLSv1.1 отключен по умолчанию. Фактически, вместо TLSv1.1 используется TLSv1.2.
ЛЛДП	LLDP — это аббревиатура от Link Layer Discovery Protocol (протокол обнаружения канального уровня), протокола канального уровня. Он позволяет сетевым устройствам, таким как коммутаторы, маршрутизаторы или серверы, обмениваться информацией о своих идентификационных данных и возможностях друг с другом. Протокол LLDP помогает сетевым администраторам лучше понимать топологию сети и предоставляет стандартизированный способ автоматизации обнаружения и сопоставления соединений между сетевыми устройствами. Это упрощает настройку сети, устранение неполадок и оптимизацию производительности.

Шаг 3. Нажмите «Применить».

3.11.1.6 Настройка облачного сервиса

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

Процедура

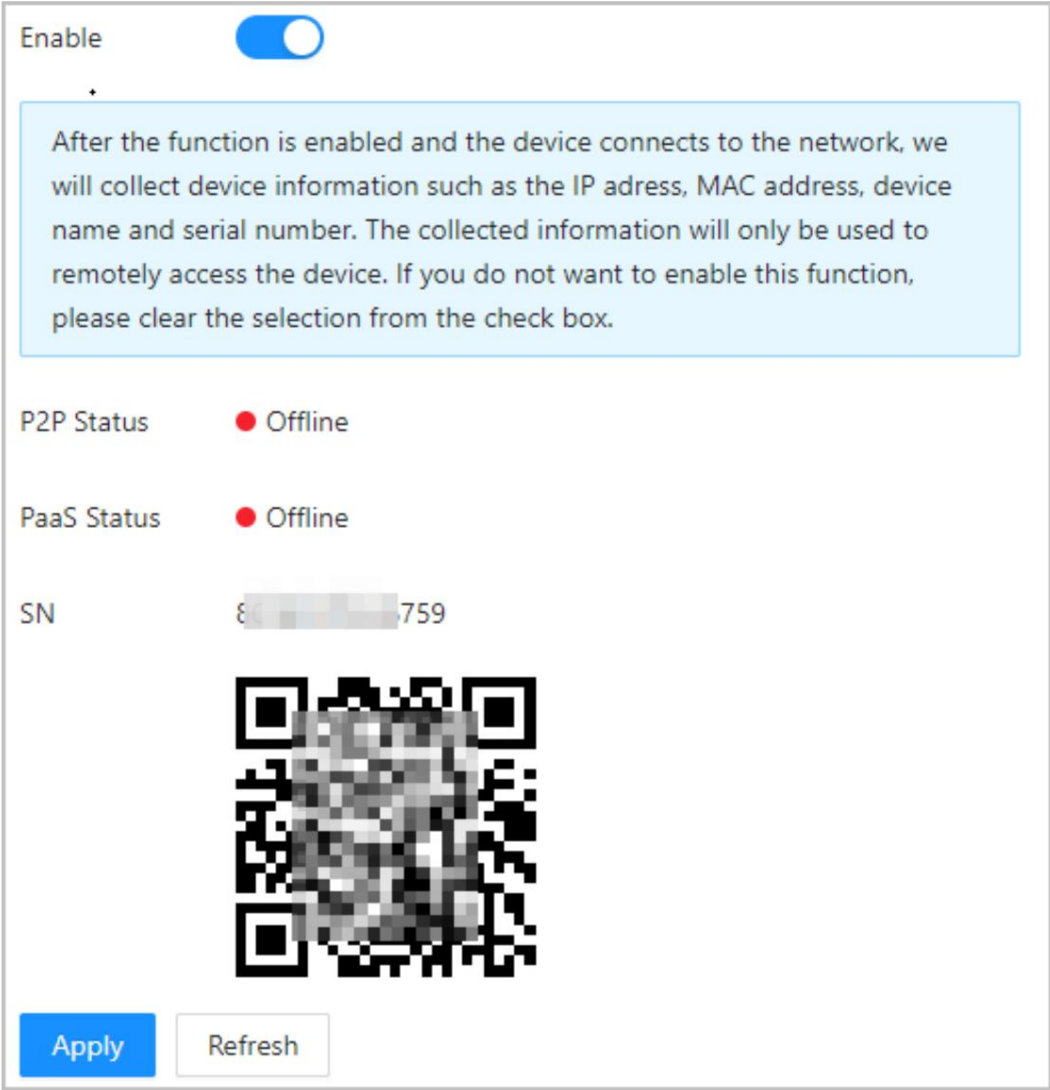
Шаг 1. На главной странице выберите «Настройки связи» > «Настройки сети» > «Облако».

Услуга.

Шаг 2. Включите функцию облачного сервиса.

Облачный сервис становится доступным, если P2P-сети и PaaS-платформы подключены к сети.

Рисунок 3-72. Облачный сервис.



Шаг 3. Нажмите «Применить».

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

3.11.1.7 Настройка автоматической регистрации SDK

Автоматическая регистрация позволяет добавлять устройства в 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 главной странице выберите «Настройки сети» > «Автоматическая регистрация SDK».

Шаг 2. Включите функцию автоматической регистрации и настройте параметры.

Рисунок 3-73. Регистрация автомобиля.

Enable

Status

Offline

Server Address

172.5.2.27

Port

7000

(1-65535)

Registration ID

none

Apply

Refresh

Default

Таблица 3-43. Описание автоматической регистрации.

Параметр	Описание
Статус	Отображает статус подключения автоматической регистрации.
Адрес сервера	IP-адрес или доменное имя сервера.
Порт	Порт сервера, используемого для автоматической регистрации.
Идентификатор регистрации	Идентификатор регистрации устройства (определяется пользователем). Добавление устройства в систему. для управления путем ввода регистрационного идентификатора на платформе.

Шаг 3. Нажмите «Применить».

3.11.1.8 Настройка автоматических регистров CGI

Подключитесь к сторонней платформе через протокол CGI.

Справочная информация



Поддерживается только IPv4.

Процедура

Шаг 1. На главной странице выберите «Настройки связи» > «Сетевые настройки» > «Автоматический CGI».

Регистрация.

Шаг 2. Включите эту функцию, а затем настройте параметры.



Шаг 3. Нажмите , а затем настройте параметры.

Рисунок 3-74 Автоматическая регистрация CGI

Edit

X

Enable

Device ID

none

Address Type

Host IP

▼

Host IP

10

Port

60005

HTTPS

Username

Password

OK

Cancel

Таблица 3-44. Описание автоматической регистрации.

Параметр	Описание
Идентификатор устройства	Поддерживает до 32 байт, включая китайские иероглифы, цифры, буквы и другие данные. специальные символы.
Тип адреса	Поддерживаются 2 способа регистрации.
IP-адрес хоста	• IP-адрес хоста: Введите IP-адрес сторонней платформы. • Доменное имя: Введите доменное имя сторонней платформы.
Доменное имя	
HTTPS	Доступ к сторонней платформе осуществляется через HTTPS. HTTPS обеспечивает безопасность. Обмен данными по компьютерной сети.
Имя пользователя/Пароль	Введите имя пользователя и пароль устройства.

Шаг 4. Нажмите OK.

3.11.1.9 Настройка автоматической загрузки

Передавайте информацию о пользователях и разблокируйте записи через платформу управления.

Процедура

Шаг 1. На главной странице выберите «Настройки связи» > «Сетевые настройки» > «Авто». Загрузить.

Шаг 2 (необязательно) Включите отправку информации о пользователе.

При обновлении информации о пользователе или добавлении новых пользователей устройство автоматически передаст информацию о пользователе на платформу управления.

Шаг 3. Включите режим загрузки по протоколу HTTP.

Шаг 4. Нажмите «Добавить», а затем настройте параметры.

Рисунок 3-75 Автоматическая загрузка

Push Person Info

Upload Mode

HTTP

Enable

Add

Delete

	No.	IP/Domain Name	Port	HTTPS	Path	Authenti- cation	Event Type	Test	Delete
☐	1	192.168.1.108	80	☐	/		Person Info, Unlock Reco...	Test	

Apply

Refresh

Default

Таблица 3-45. Описание параметров.

Параметр	Описание
IP-адрес/доменное имя.	IP-адрес или доменное имя платформы управления.
Порт	Порт платформы управления.
HTTPS	Доступ к платформе управления осуществляется через HTTPS. HTTPS обеспечивает безопасность связи в компьютерной сети.
Аутентификация	Включите аутентификацию учетной записи при доступе к платформе управления. Для входа в систему необходимы имя пользователя и пароль.
Тип события	Выберите тип события, которое будет отправлено на платформу управления. • Перед использованием этой функции включите функцию «Передача информации о человеке». • Информация о человеке может быть передана только на одну платформу управления, а записи о разблокировке — на несколько платформ управления.

Шаг 5. Нажмите «Применить».

3.11.1.10 Настройка таблицы маршрутизации

Если устройство одновременно подключено к сети 4G и проводному соединению, или одновременно к сети Wi-Fi и проводному соединению, вы можете настроить таблицу маршрутизации для доступа к проводной сети устройства в пределах локальной сети.



Эта функция доступна только на устройствах, поддерживающих 4G или Wi-Fi.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Настройки связи» > «Сетевые настройки» > «Таблица маршрутизации».

Шаг 3. Нажмите «Добавить», настройте параметры, а затем нажмите «Добавить».

После добавления устройства, находящиеся в IP-сегменте, смогут получить доступ к текущему устройству через проводную сеть.

Например, если IP-адрес в TCP/IP настроен как 172.16.24.5, а IP-адрес компьютера А — 192.168.1.8, добавьте его в таблицу маршрутизации, как показано на рисунке ниже. После добавления компьютер А сможет напрямую получить доступ к адресу 172.16.24.5.



Можно добавить до 5 таблиц.

Рисунок 3-76. Добавьте таблицу маршрутизации.

Add

NIC

NIC 1

No.

1

* IP Segment

192 . 168 . 0 . 0

* Subnet Mask

255 . 255 . 0 . 0

* Gateway

192 . 168 . 0 . 1

Basic Network

IP Address

172.12.85.100

Subnet Mask

255.255.252.0

Gateway

172.12.85.1

OK

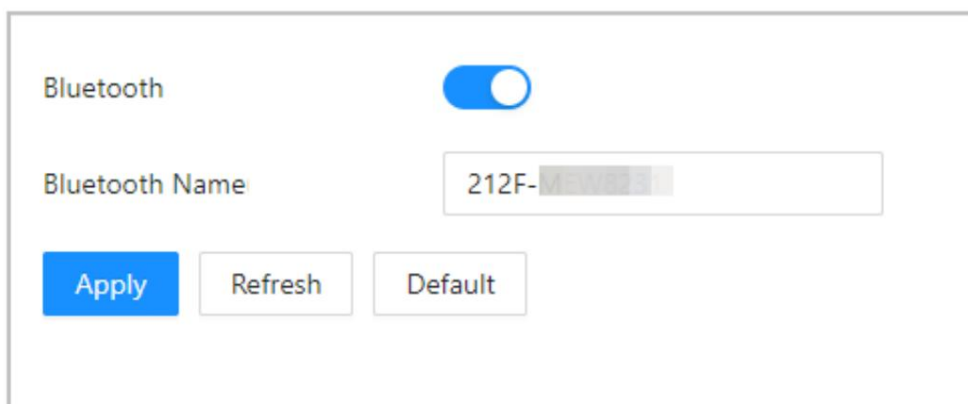
Cancel

3.11.2 Настройки Bluetooth

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

- Шаг 1. Выберите «Настройки связи» > «Настройки Bluetooth».
- Шаг 2. Включите или выключите Bluetooth, настройте имя Bluetooth.

Рисунок 3-77 Bluetooth



Шаг 3. Нажмите «Применить».

Результаты

Дверь можно разблокировать через Bluetooth с помощью приложения DMSS.

3.11.3 Настройка RS-485

Настройте параметры RS-485, если вы подключаете внешнее устройство к порту RS-485.

Процедура

Шаг 1. Выберите «Настройки связи» > «Настройки RS-485».

Шаг 2. Настройте параметры.

Рисунок 3-78. Настройка параметров.

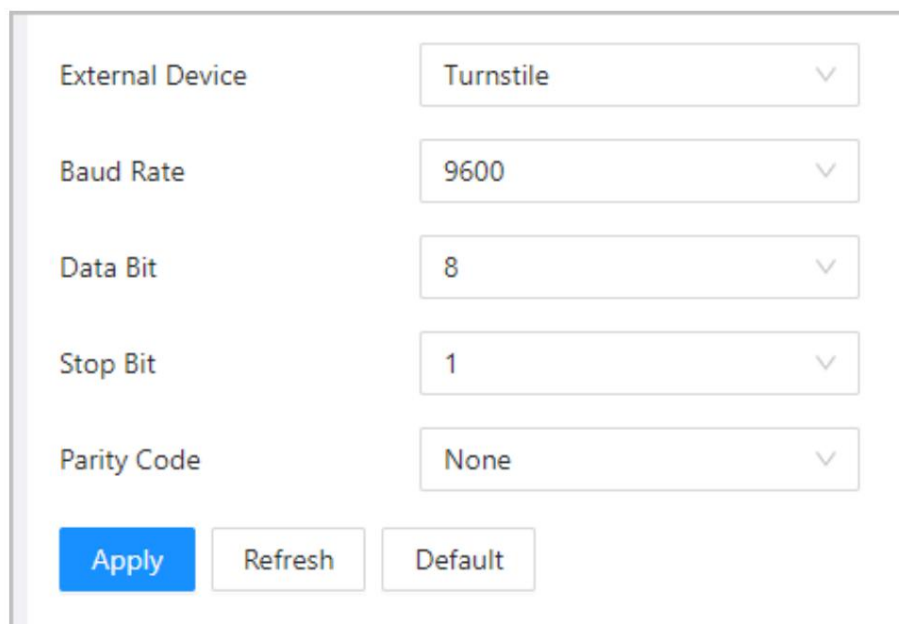


Таблица 3-46. Настройка параметров RS-485.

Параметр	Описание
Внешнее устройство	• Контроллер доступа Выберите «Контроллер доступа», если устройство функционирует как считыватель карт и отправляет данные другим внешним контроллерам доступа для управления доступом. Тип выходных данных: ◇ Номер карты : Передайте номер карты контроллеру доступа для аутентификации и разблокировки двери. Если номер карты, переданный этим устройством, совпадает с номером карты в контроллере доступа, аутентификация контроля доступа считается успешной. ◇ Нет. : Передайте идентификатор пользователя контроллеру доступа для аутентификации и разблокировки двери. Если идентификатор пользователя, переданный этим устройством, совпадает с идентификатором пользователя в контроллере доступа, аутентификация контроля доступа считается успешной. • Считыватель карт: Устройство функционирует как контроллер доступа и подключается к внешнему считывателю карт. • Считыватель (OSDP): Устройство подключается к считывателю карт на основе протокола OSDP. протокол. • Модуль безопасности управления дверью: После включения модуля безопасности кнопка выхода, замок и функция пожарной сигнализации не работают. • Турникет: Когда устройство подключается к турникету, происходит доступ. Контроллерная плата турникета подключается к внешнему модулю QR-кода или модулю считывания карт, после чего плата передает данные для проверки на турникет. • Режим расширения замка: Если контроллер доступа подключен к внешнему модулю расширения замка и выбран режим «Модуль расширения замка», локальный замок разблокируется после подтверждения идентификации на локальном устройстве, а дополнительный замок — после подтверждения идентификации на внешнем считывателе карт. После выбора модуля расширения замка вы можете выбрать канал 2 на странице «Параметры контроля доступа и сигналы тревоги» на веб-странице контроллера доступа. • Запасная батарея: Устройство подключается к запасной батарее, и текущий Уровень заряда батареи отображается в процентах.  Запасной аккумулятор поддерживается только на некоторых моделях.
Бит данных	Количество бит, используемых для передачи фактических данных в последовательном канале связи. Это двоичные цифры, несущие передаваемую информацию.
Стоп Бит	После данных передается бит, а также необязательные биты четности, указывающие на конец передачи данных. Это позволяет приемнику подготовиться к передаче следующего байта данных и обеспечивает синхронизацию в протоколе связи.
Код четности	После битов данных отправляется дополнительный бит для обнаружения ошибок передачи. Он помогает проверить целостность передаваемых данных, обеспечивая наличие определенного количества логических старших или младших битов.

Шаг 3. Нажмите «Применить».

3.11.4 Настройка Wiegand

Поддерживает доступ к устройствам Wiegand. Настройте режим и режим передачи в соответствии с вашими реальными устройствами.

Процедура

Шаг 1. Выберите «Настройки связи» > «Wiegand».

Шаг 2. Выберите тип Wiegand, а затем настройте параметры.

- При подключении внешнего считывателя карт к устройству выберите вход Wiegand .



Если устройство подключается к стороннему устройству через входной порт Wiegand, и номер карты, считываемый устройством, отображается в обратном порядке по отношению к фактическому номеру карты, в этом случае можно включить функцию инверсии номера карты .

- Выберите выход Wiegand, если устройство функционирует как считыватель карт и вам необходимо подключить его к другому контроллеру доступа.

Рисунок 3-79. Выход Wiegand.

Wiegand

☐ Wiegand Input ☒ Wiegand Output

Wiegand Output Type

Wiegand34

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.

Output Data Type

☒ Card Number ☐ No.

Apply

Refresh

Default

Таблица 3-47. Описание выходных данных Wiegand.

Параметр	Описание
Тип выходного сигнала Wiegand	Выберите формат Wiegand для считывания номеров карт или идентификационных номеров. • Wiegand26 : считывает 3 байта или 6 цифр. • Wiegand34 : считывает 4 байта или 8 цифр. • Wiegand66 : считывает 8 байтов или 16 цифр.
Ширина импульса	Введите ширину импульса и интервал между импульсами на выходе Wiegand.

Параметр	Описание
Интервал пульса	
Тип выходных данных	Выберите тип выходных данных. • Нет.: Выводит данные на основе идентификатора пользователя. Формат данных — шестнадцатеричный или десятичный. • Номер карты: Выводит данные на основе первой карты пользователя. число.

Шаг 3. Нажмите «Применить».

3.12 Настройка системы

3.12.1 Управление пользователями

Вы можете добавлять или удалять пользователей, изменять пароли пользователей, а также указывать адрес электронной почты для сброса пароля в случае его забытия.

3.12.1.1 Добавление администраторов

Вы можете добавить новые учетные записи администраторов, после чего они смогут войти на веб-страницу устройства.

Процедура

Шаг 1. На главной странице выберите Система > Учетная запись.

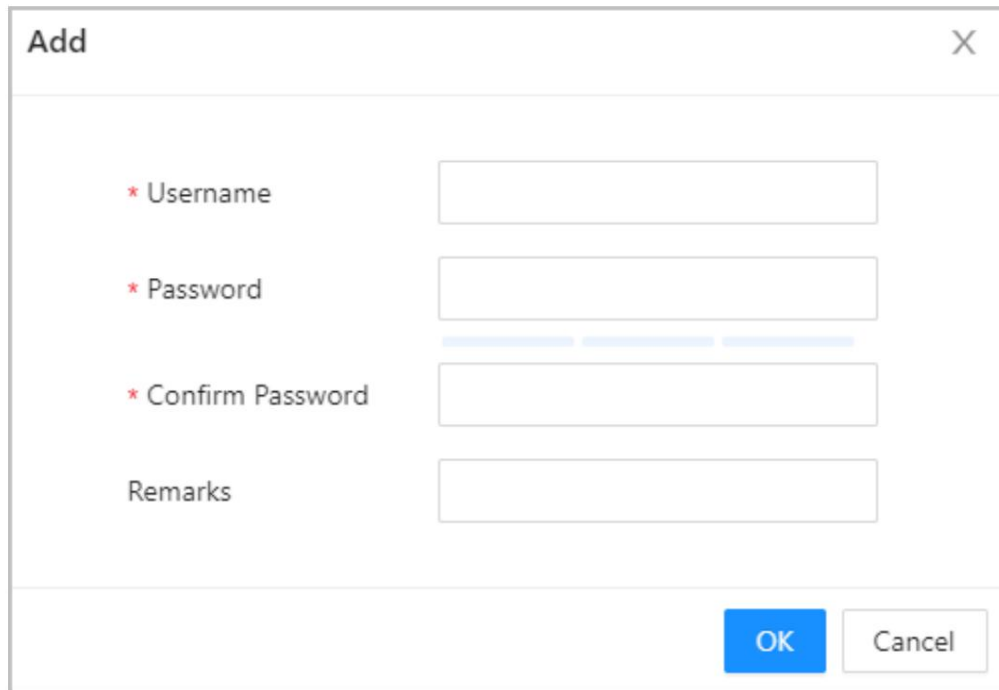
Шаг 2. Нажмите «Добавить» и введите информацию о пользователе.



- Имя пользователя не может совпадать с именем существующей учетной записи. Имя пользователя может содержать до 31 символа и допускает только цифры, буквы, подчеркивания, символы середины строки, точки или символ @.
- Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа следующих символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' ' ; &).

Установите надежный пароль, следуя подсказкам по проверке уровня защиты.

Рисунок 3-80. Добавление администраторов.



The image shows a dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there are four input fields arranged vertically. The first three fields are labeled with a red asterisk and the text "Username", "Password", and "Confirm Password" respectively. The fourth field is labeled "Remarks". Below the input fields, there are two buttons: a blue "OK" button and a white "Cancel" button with a grey border.

Шаг 3. Нажмите OK.



Изменить пароль может только администратор, и удалить учетную запись администратора невозможно.

3.12.1.2 Добавление пользователей ONVIF

Справочная информация

Форум открытых сетевых видеоинтерфейсов (ONVIF) — это глобальный открытый отраслевой форум, созданный для разработки глобального открытого стандарта для интерфейса физических IP-устройств безопасности, обеспечивающего совместимость с продукцией различных производителей. Идентификация пользователей ONVIF проверяется с помощью протокола ONVIF. Пользователем ONVIF по умолчанию является администратор.

Процедура

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

Шаг 2. Нажмите «Добавить», а затем настройте параметры.

Рисунок 3-81. Добавить пользователя ONVIF.

Add

*

Username

*

Password

*

Confirm Password

*

Group

OK

Cancel

Таблица 3-48. Описание пользователя ONVIF.

Параметр	Описание
Имя пользователя	Имя пользователя не может совпадать с именем существующей учетной записи. Имя пользователя может содержать до 31 символа и допускает только цифры, буквы, подчеркивания, символы середины строки, точки или символ @.
Пароль	Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа следующих символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; &).
Группа	Существует три группы разрешений, представляющие разные уровни доступа. • Администратор: Вы можете просматривать и управлять другими учетными записями пользователей в ONVIF. Диспетчер устройств. • Оператор: Вы не можете просматривать или управлять другими учетными записями пользователей в Диспетчере устройств ONVIF. • Пользователь: Вы не можете просматривать или управлять другими учетными записями пользователей и системными журналами в Диспетчере устройств ONVIF.

Шаг 3. Нажмите OK.

3.12.1.3 Сброс пароля

Если вы забыли пароль, восстановите его через указанный адрес электронной почты.

Процедура

Шаг 1. Выберите Система > Учетная запись.

Шаг 2. Введите адрес электронной почты и установите время истечения срока действия пароля.

Шаг 3. Включите функцию сброса пароля.

Рисунок 3-82 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

Password Expires in Days



Если вы забыли пароль, вы можете получить коды безопасности на привязанный адрес электронной почты для его сброса.

Шаг 4. Нажмите «Применить».

3.12.1.4 Просмотр пользователей онлайн

Вы можете просмотреть список пользователей, которые в данный момент авторизованы на веб-странице. На главной странице выберите Система > Пользователи онлайн.

3.12.2 Настройка времени

Процедура

Шаг 1. На главной странице выберите Система > Время.

Шаг 2. Настройте время на платформе.

Рисунок 3-83 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 3-49. Описание настроек времени.

Параметр	Описание
Время	• Ручная настройка: Введите время вручную или нажмите «Синхронизировать время» , чтобы синхронизировать время с компьютером. • NTP: Устройство автоматически синхронизирует время с NTP-сервером. сервер. ◇ Сервер : Введите домен NTP-сервера. ◇ Порт : Введите порт NTP-сервера. ◇ Интервал : Введите время с указанием интервала синхронизации.
Формат времени	Выберите формат времени.
Часовой пояс	Введите часовой пояс.

Параметр	Описание
летнее время	1. (Необязательно) Включите летнее время. 2. В поле «Тип» выберите «Дата» или «Неделя» . 3. Настройте время начала и окончания перехода на летнее время.

Шаг 3. Нажмите «Применить».

3.13 Персонализация

Настройте темы оформления и добавьте видео- или графическую рекламу на устройство.



- Функция доступна на некоторых моделях. •

Декодирование видео, содержащего В-кадры, отправленные с платформы, не поддерживается.

- Изображения с глубиной цвета 1 не могут быть обработаны.
- Анализ полупрозрачных изображений не поддерживается. •

Разные устройства поддерживают разные разрешения рекламы.

3.13.1 Реклама

3.13.1.1 Добавление ресурсов

Добавьте изображения или видео для отображения на экране устройства в режиме ожидания.

Процедура

Шаг 1. На главной странице выберите «Персонализация» > «Реклама» > «Рекламные ресурсы».

Шаг 2. Добавьте видео или изображения.

Рисунок 3-84. Добавьте видео или изображения.

Video

The video size must not exceed 100M. Supported formats: AVI,DAV,MP4. We recommend the resolution for full-screen advertisements be 800*1200 and for other advertisements be 800*800.

Upload

No.	Name	Operation
1		
2		
3		
4		
5		

Picture

The image size must not exceed 2M. Supported formats: PNG,JPG,BMP. We recommend the resolution for full-screen advertisements is 800*1200 and for other advertisements is 800*800.

+

Upload

• Добавляйте видео.

1. Нажмите «Загрузить».

2. Нажмите «Обзор» , Выберите видеофайл и нажмите «Далее».

Видео автоматически загружается на платформу после перекодирования.

Вы можете загрузить до 5 видеофайлов.

Поддерживает форматы DAV, AVI, MP4. Размер видеофайла должен быть менее 100 МБ.

Поддерживается загрузка видеофайлов только в последних версиях Firefox и Chrome.

• Добавьте изображения.

1. Нажмите +.
2. Выберите изображение из локальной памяти и загрузите его.



Поддерживаются форматы PNG, JPG, BMP. Размер изображения должен быть менее 2 МБ.

Связанные операции

Нажмите, чтобы удалить загруженные изображения или видео.



Используемые видео- и видеоматериалы удалить невозможно.

3.13.1.2 Настройка тем оформления

Процедура

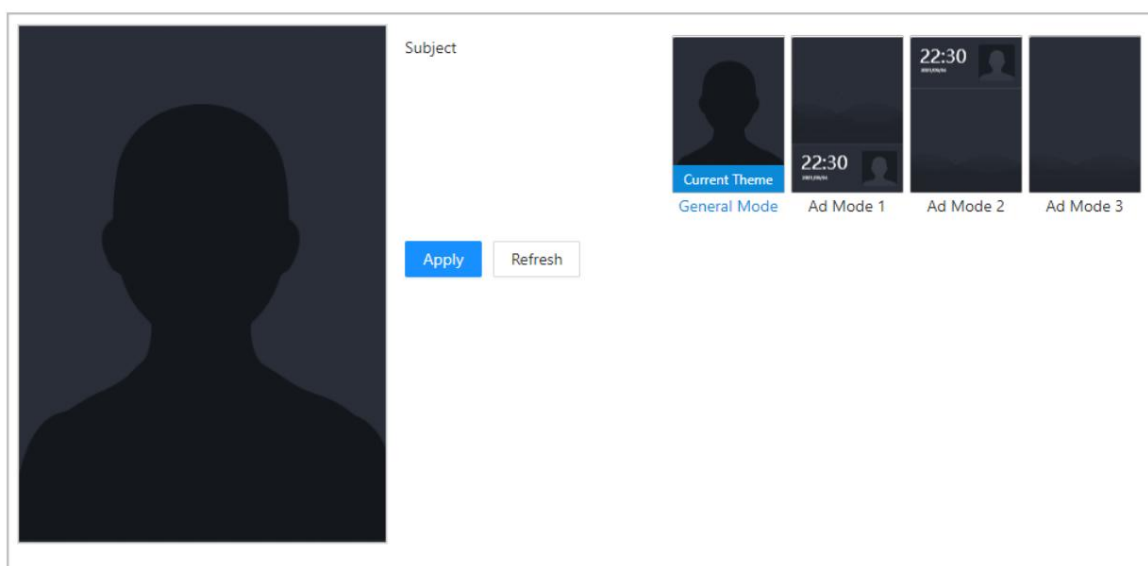
Шаг 1. На главной странице выберите «Персонализация» > «Реклама» > «Тема».

Шаг 2. Выберите тему.

Если вы выберете общую тему оформления, нажмите «Применить». Если вы выбрали тему для рекламы, выполните шаги 3 и 4, а затем нажмите «Применить».

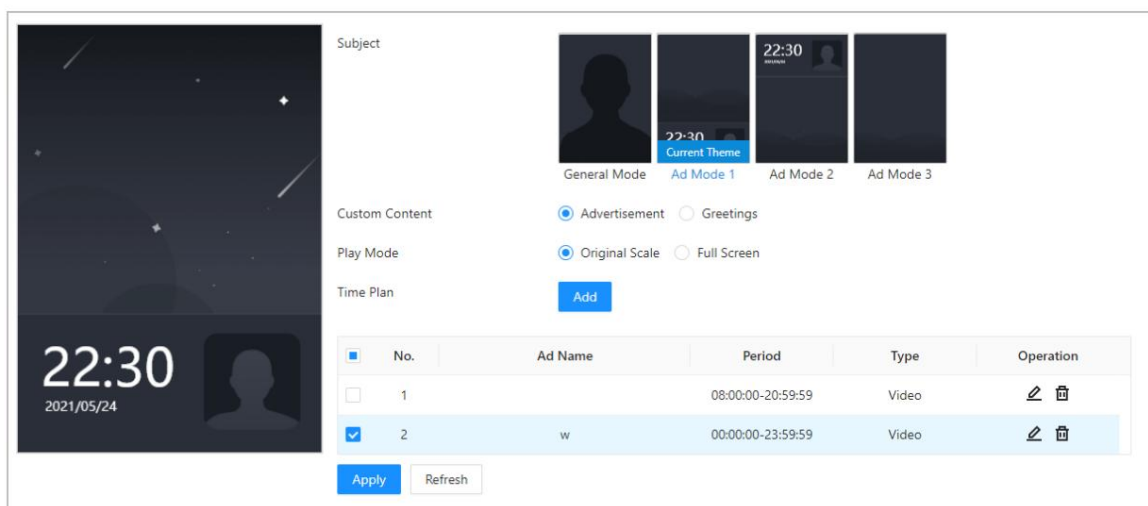
- Общая тема : Отображает изображение лица в полноэкранном режиме.
- Режим рекламы 1 : В верхней области отображается реклама, а в нижней — время и окно распознавания лица.
- Режим рекламы 2 : В верхней области отображается время и окно распознавания лица, а в нижней — реклама.
- Режим рекламы 3 : На экране отображается реклама, значки быстрого доступа не отображаются. При проверке лица экран распознавания не отображается, а отображается результат проверки. Настройки такие же, как в режиме рекламы 1.

Рисунок 3-85 Тема

**Шаг 3. Настройка отображения рекламы.**

1. Выберите «Реклама» в разделе «Пользовательский контент».

Рисунок 3-86 Режим рекламы



2. Выберите режим отображения.

- Исходный масштаб: Воспроизводит изображение и видео в исходном размере.

- Полноэкранный режим: Воспроизводит изображение и видео в полноэкранном режиме.

3. Нажмите «Добавить», чтобы добавить расписание.

Вы можете добавить до 10 расписаний.

4. Введите название рекламного объявления.

5. Выберите временной интервал, тип файла и сам файл.

6. Введите продолжительность, выберите добавленные ресурсы и нажмите «Применить».

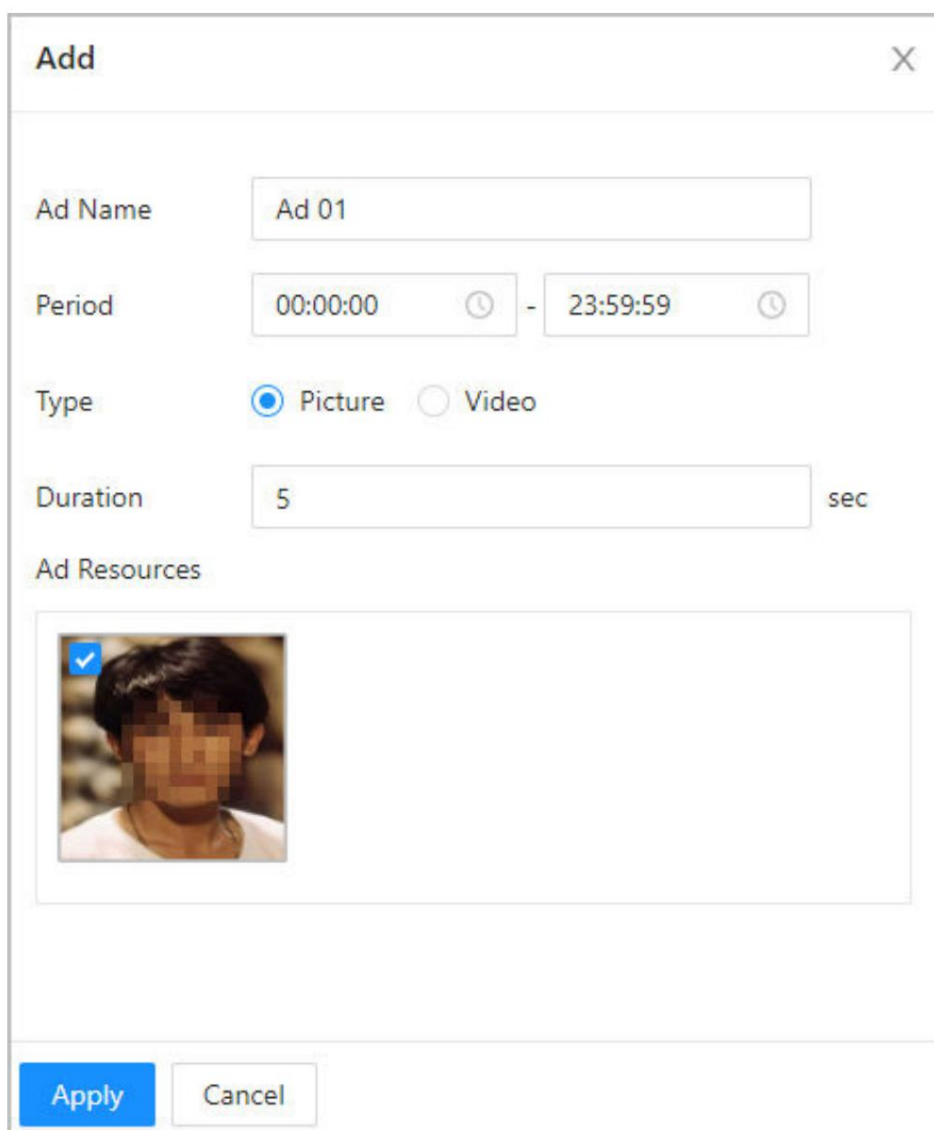
Убедитесь, что вы добавили ресурсы через раздел Персонализация > Реклама > Ресурсы рекламы.

- Установите продолжительность воспроизведения одного изображения в цикле.

Длительность варьируется от 1 до 20 секунд, по умолчанию составляет 5 секунд.

- При выборе видеороликов вы можете изменить их порядок.

Рисунок 3-87. Добавить расписания.



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Ad Name:** A text input field containing "Ad 01".
- Period:** Two time selection fields. The first shows "00:00:00" with a clock icon, followed by a minus sign, and the second shows "23:59:59" with a clock icon.
- Type:** Two radio buttons. "Picture" is selected (indicated by a blue dot), and "Video" is unselected.
- Duration:** A text input field containing "5", followed by the unit "sec".
- Ad Resources:** A section containing a list of resources. One resource is visible, showing a thumbnail image of a person's face with a blue checkmark in the top left corner, indicating it is selected.
- Buttons:** At the bottom, there are two buttons: "Apply" (blue) and "Cancel" (white with a grey border).

Шаг 4. Настройка приветствий.

1. Выберите «Приветствие» в разделе «Пользовательский контент».

2. Выберите шаблон.

3. Введите заголовок и подзаголовок.

Рисунок 3-88 Приветствия

The screenshot shows the Windows Hello interface for setting a greeting screen. The interface is divided into two main sections: a preview on the left and configuration options on the right.

Preview (Left): A dark-themed screen with the text "Welocme home" and "Good night". A clock shows "22:30" and the date "2021/05/24". A silhouette of a person is visible in the bottom right corner.

Configuration Options (Right):

- Subject:** A dropdown menu showing "General Mode", "Ad Mode 1", "Ad Mode 2", and "Ad Mode 3". "Ad Mode 1" is selected.
- Custom Content:** Radio buttons for "Advertisement" and "Greetings". "Greetings" is selected.
- Template:** A dropdown menu showing "Current Templa...", "Galaxy", "Mist", and "Dream". "Current Templa..." is selected.
- Content:** A text input field with the placeholder "Please edit your content below."
- Title:** A text input field with the value "Welocme home".
- Subtitle:** A text input field with the value "Good night".
- Buttons:** "Apply" and "Refresh".

3.13.2 Настройки экрана

3.13.2.1 Настройка режима Always-On

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Персонализация» > «Настройки экрана» > «Настройка постоянной работы».

Шаг 3. Включите функцию, а затем нажмите OK.

После включения этой функции экран всегда будет включен в течение заданного периода времени.

- Когда устройство переходит в режим выключения экрана, экран остается постоянно включенным с уровнем яркости, соответствующим уровню 1 в настройках яркости экрана в главном меню устройства.

Во всех остальных режимах яркость соответствует значению, заданному в настройках яркости экрана в главном меню устройства.



Чтобы продлить срок службы экрана, мы рекомендуем ограничить время его работы до 8 часов в день.

Шаг 4. Настройте период, а затем нажмите «Применить».

Рисунок 3-89. Дисплей всегда включен.

Display Always On ☒

i To help extend the lifespan of your screen, we recommend you limit the time it stays on to no more than 8 hours a day.

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

3.13.2.2 Настройка отображения информации

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Персонализация» > «Настройки экрана» > «Информационное отображение».

Шаг 3. Введите информацию об устройстве, а затем нажмите «Применить».

На странице «Персонализация > Реклама > Тема» при выборе «Общий режим» информация о настроенном устройстве отображается в правом верхнем углу главного окна. экран.

Рисунок 3-90. Настройка информации об устройстве.

i It will only take effect in general mode.

Device Info test

Apply Refresh Default

3.13.2.3 Настройка сочетаний клавиш

Процедура

Шаг 1. На веб-странице выберите «Персонализация» > «Настройки экрана» > «Настройки ярлыков».

Шаг 2. Настройте параметры сочетания клавиш.

Рисунок 3-91. Быстрый вызов настроек.

Password	☒
QR Code	☒
Call or Doorbell	☒
Call or Doorbell	☒ Call ☐ Doorbell
Icon	☒  ☐ 
Call Type	One-Click Call ▼
Room No.	9901
Apply Refresh Default	

Рисунок 3-92. Настройки ярлыка дверного звонка.

Password

QR Code

Call or Doorbell

Call or Doorbell

Call

Doorbell

Icon

Local Device Ringer

External Doorbell

Ringtone Config

Ringtone 1

Ringtone Time (sec)

3

(1-30)

Apply

Refresh

Default

Таблица 3-50. Описание параметров.

Параметр	Описание
Пароль	На экране ожидания отображается значок способа разблокировки по паролю.
QR-код	Значок QR-кода отображается на экране ожидания. Эта функция недоступна. Доступно для устройств с автономным модулем QR-кода.
Позвоните или вставьте дверь.	Включите функцию, и на главном экране отобразится соответствующее сообщение.
Икона	Значок быстрого доступа. Вы можете выбрать «Вызов» и «Дверной звонок», а также значок для выбранная вами функция.  Когда модульное устройство подключается к внешнему модулю расширения с Кнопка дверного звонка, функция дверного звонка соответствует настройкам. здесь .

Параметр	Описание	
Тип вызова	• Вызов с клавиатуры: Доступны 2 режима. ◇ Стандартный способ: коснитесь значка вызова на экране ожидания, введите номер комнаты, а затем коснитесь значка вызова, чтобы позвонить в комнату. ◇ Телефонная книга: настройте содержимое на веб-странице. Коснитесь значка вызова на экране ожидания, и добавленный VTN или VTS отобразится на экране. Вы можете коснуться значка, чтобы позвонить в VTN или VTS. Список вызовов отображается в соответствии с вашими настройками на веб-странице. • Центр управления вызовами: Нажмите на значок вызова на экране ожидания, чтобы позвонить. Центр управления. • Звонок в один клик 1. Укажите номер комнаты и нажмите «Применить». 2. Нажмите на значок вызова на экране ожидания, чтобы позвонить в указанную комнату.  Звонки в DMSS можно совершать только в рамках этого типа вызова.	
Локальный звонок устройства	Нажмите на значок дверного звонка на главном экране устройства, и он зазвонит.	 Доступно только при выборе варианта «Вызов» или «Дверной звонок» в качестве варианта «Дверной звонок».
Внешний дверной звонок	Нажмите на значок дверного звонка на главном экране устройства, и внешний дверной звонок зазвонит.  • Эта функция доступна только на некоторых моделях. • Если функциональный порт 1 не настроен на дверной звонок, то при Чтобы включить внешний дверной звонок, нажмите OK во всплывающем окне. Установите выходной порт сигнализации на функцию дверного звонка.	
Настройка мелодии звонка	Настройте мелодию звонка. Доступны 2 типа мелодий звонка на выбор.	
Время звонка (сек.)	Настройте время звонка. По умолчанию оно составляет 3 секунды.	

3.14 Центр управления

3.14.1 Диагностика одним щелчком мыши

Система автоматически диагностирует конфигурацию и состояние устройства для повышения его производительности.

Процедура

Шаг 1. На главной странице выберите Центр обслуживания > Диагностика в один клик.

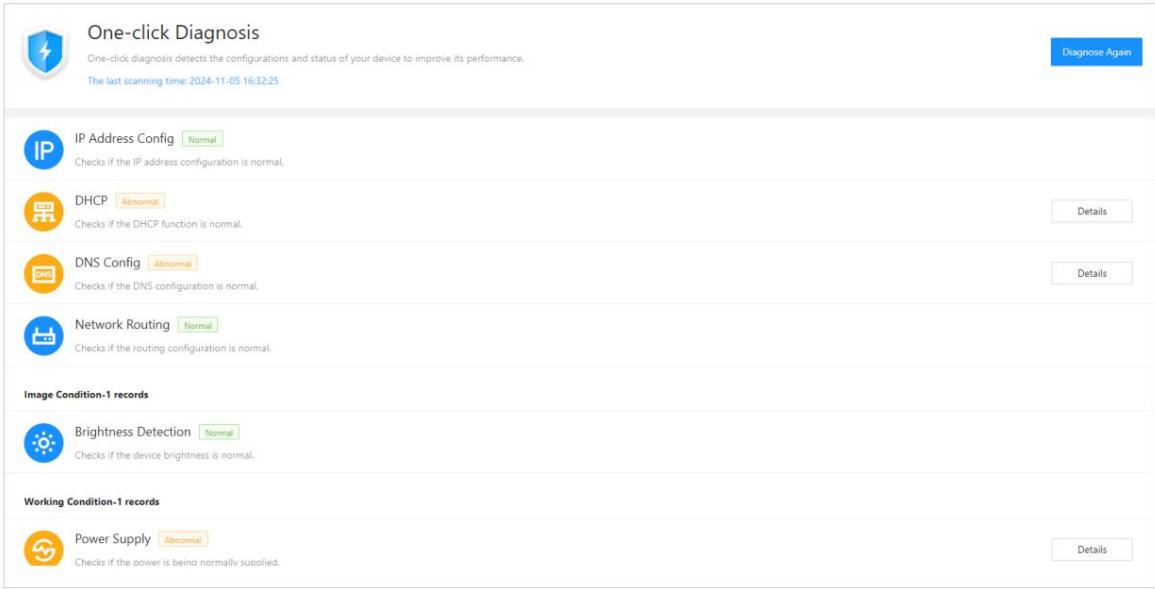
Шаг 2. Нажмите «Диагностика».

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

Шаг 3 (необязательно) Нажмите «Подробности», чтобы просмотреть сведения об аномальных элементах.

Вы можете проигнорировать отклонение или оптимизировать его. Вы также можете нажать «Провести повторную диагностику» , чтобы повторно выполнить автоматическую диагностику.

Рисунок 3-93. Диагностика одним щелчком мыши.



3.14.2 Информация о системе

3.14.2.1 Просмотр информации о версии

На веб-странице выберите Центр обслуживания > Информация о системе > Версия, и вы сможете просмотреть информацию о версии устройства.

3.14.2.2 Просмотр юридической информации

На главной странице выберите Центр обслуживания > Информация о системе > Юридическая информация, и вы сможете ознакомиться с лицензионным соглашением на программное обеспечение, политикой конфиденциальности и уведомлением об использовании программного обеспечения с открытым исходным кодом.

3.14.3 Объем данных

Вы можете увидеть, сколько пользователей, карточек и изображений лиц может хранить устройство.

Войдите на веб-страницу и выберите Центр обслуживания > Емкость хранилища данных.

3.14.4 Журналы просмотров

Просматривайте журналы, такие как системные журналы, журналы администратора и записи о разблокировке.

3.14.4.1 Системные журналы

Поиск и просмотр системных журналов.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр технического обслуживания > Журнал > Журнал.

Шаг 3. Выберите временной диапазон и тип журнала, а затем нажмите «Поиск».

Связанные операции

• Нажмите «Экспорт», чтобы экспортировать найденные журналы на локальный компьютер. •

Нажмите «Зашифровать резервную копию журнала», а затем введите пароль. Экспортированный файл можно будет открыть только после ввода пароля. • Нажмите, чтобы

просмотреть  подробную информацию о журнале.

3.14.4.2 Разблокировка записей

Найдите записи о разблокировке и экспортируйте их.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр обслуживания > Журнал > Разблокировать записи.

Функция «Сохранять записи разблокировки» включена по умолчанию. После её отключения записи разблокировки не могут быть сохранены на устройстве.

Шаг 3. Выберите временной диапазон и тип, а затем нажмите «Поиск».

Для загрузки журнала нажмите кнопку «Экспорт» .

Связанные операции

• Нажмите «Экспорт», чтобы экспортировать записи о разблокировке на свой компьютер.

• Нажмите  для просмотра собранного изображения лица.

• Нажмите  для просмотра изображения лица, полученного в ходе верификации.

3.14.4.3 История звонков

Просмотреть журналы звонков.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр технического обслуживания > Журнал > История обращений.

3.14.4.4 Журналы аварийных сигналов

Просмотреть журналы тревожных сообщений.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр технического обслуживания > Журнал > Журнал аварийных сигналов.

Шаг 3. Выберите тип и временной диапазон.

Шаг 4. Введите идентификатор администратора, а затем нажмите «Поиск».

3.14.4.5 Журналы администратора

Найдите журналы администратора, используя его идентификатор.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр обслуживания > Журнал > Журнал администратора.

Шаг 3. Введите идентификатор администратора, а затем нажмите «Поиск».

Нажмите «Экспорт», чтобы экспортировать журналы администратора.

3.14.4.6 Управление USB

Экспорт пользовательской информации с/на USB-накопитель.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Центр обслуживания > Журнал > Управление USB.



- Перед экспортом данных или обновлением системы убедитесь, что USB-накопитель вставлен в устройство. Во избежание сбоев не извлекайте USB-накопитель и не выполняйте никаких операций с устройством во время процесса.
- Для экспорта информации с устройства на другие устройства необходимо использовать USB-накопитель. Импорт изображений лиц через USB-накопитель запрещен.

Шаг 3. Выберите тип данных, а затем нажмите «Импорт с USB» или «Экспорт с USB», чтобы импортировать или экспортировать данные.

3.14.5 Центр технического обслуживания

3.14.5.1 Управление конфигурацией

Если для нескольких устройств требуются одинаковые настройки, вы можете задать для них параметры, импортировав или экспортировав файлы конфигурации.

3.14.5.1.1 Экспорт и импорт конфигурационных файлов

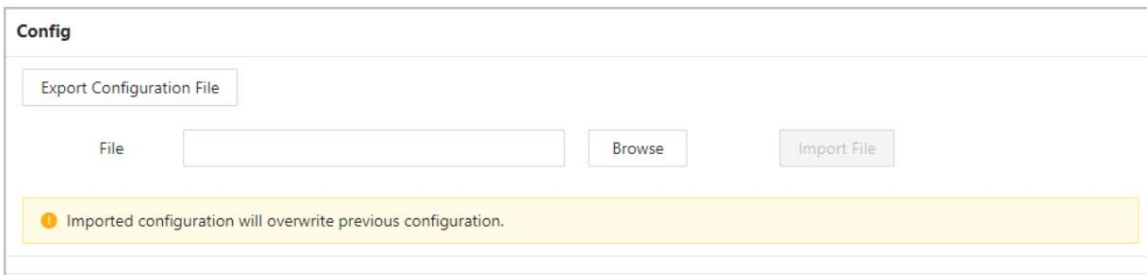
Вы можете импортировать и экспортировать файл конфигурации устройства. Если вы хотите применить одни и те же настройки к нескольким устройствам, вы можете импортировать файл конфигурации на них.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Управление техническим обслуживанием» > «Конфигурация».

Рисунок 3-94. Управление конфигурацией.



Шаг 3. Экспорт или импорт конфигурационных файлов.

- Экспортируйте файл конфигурации.

Нажмите «Экспорт файла конфигурации», чтобы загрузить файл на локальный компьютер.



IP-адрес экспортироваться не будет. •

Импортируйте файл конфигурации.

1. Нажмите кнопку «Обзор», чтобы выбрать файл конфигурации.
2. Нажмите «Импорт конфигурации».



Файлы конфигурации можно импортировать только на устройства одной и той же модели.

3.14.5.1.2 Настройка порогового значения отпечатка пальца

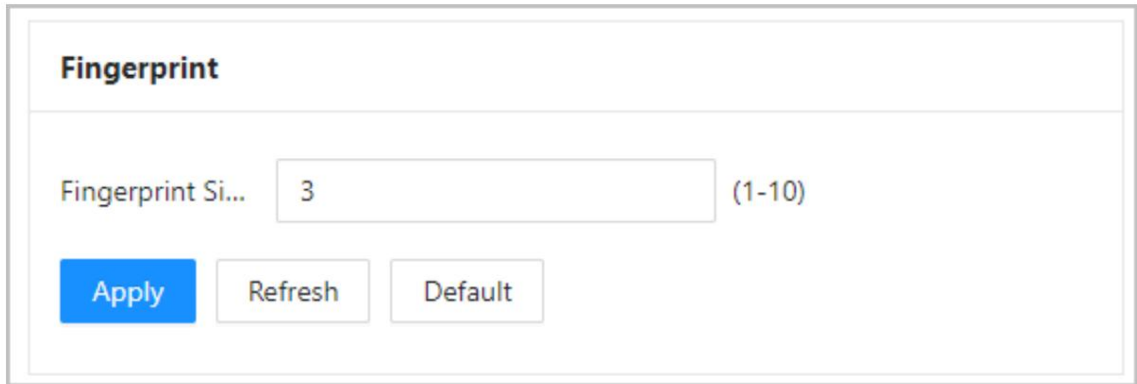
Выберите «Управление техническим обслуживанием» > «Конфигурация». Настройте пороговое значение для отпечатков пальцев в соответствии с фактической ситуацией. Чем больше значение, тем выше точность сопоставления отпечатков пальцев, тем ниже процент ложных срабатываний, но при этом снижается и процент успешных распознаваний.



• Для модульного устройства после подключения модуля расширения с функцией распознавания отпечатков пальцев отображается следующая конфигурация. • Для устройства с функцией распознавания отпечатков пальцев отображается следующая конфигурация.

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

Рисунок 3-95. Пороговое значение отпечатков пальцев.



Fingerprint

Fingerprint Si... (1-10)

Apply Refresh Default

3.14.5.1.3 Восстановление заводских настроек по умолчанию

Процедура

Шаг 1. Выберите «Управление техническим обслуживанием» > «Конфигурация».



Восстановление устройства до заводских настроек приведет к потере данных. Обратите внимание.

Шаг 2. При необходимости восстановите заводские настройки по умолчанию.

- Восстановление заводских настроек (с сохранением сетевой конфигурации) : Сбрасывает все настройки. За исключением сетевой конфигурации устройства. • Восстановление настроек по умолчанию (сохраняет журналы, информацию о пользователе и сетевую конфигурацию) : Сбрасывает настройки устройства. Удаляет все данные, кроме информации о пользователе, журналов и сетевых конфигураций, и вносит изменения в настройки устройства.

3.14.5.2 Техническое обслуживание

Для повышения производительности устройства рекомендуется регулярно перезагружать его в режиме ожидания.

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 «Перезагрузить» , чтобы перезагрузить его немедленно.

3.14.6 Обновление системы



- Используйте правильный файл обновления. Убедитесь, что вы получили правильный файл обновления от технической поддержки.
- Не отключайте источник питания или сеть, а также не перезагружайте и не выключайте устройство. во время обновления.

3.14.6.1 Обновление файла

Процедура

- Шаг 1. На главной странице выберите Система > Обновление.
- Шаг 2. В разделе «Обновление файла» нажмите «Обзор», а затем загрузите файл обновления.



Файл обновления должен быть файлом с расширением .bin.

- Шаг 3. Нажмите «Обновить».
- После завершения обновления устройство перезагрузится.

3.14.6.2 Онлайн-обновление

Процедура

- Шаг 1. На главной странице выберите Система > Обновление.
- Шаг 2 В разделе «Онлайн-обновление» выберите способ обновления.
 - Выберите опцию «Автоматическая проверка обновлений», и устройство автоматически проверит наличие последних версий. Обновление версии.
 - Выберите «Ручная проверка», и вы сразу сможете проверить, установлена ли последняя версия. доступный.
- Шаг 3 (необязательно) Нажмите «Обновить сейчас» , чтобы немедленно обновить устройство.

3.14.7 Расширенное техническое обслуживание

Получение информации об устройстве и захват пакетов данных упростит работу обслуживающего персонала по устранению неполадок.

3.14.7.1 Экспорт

Процедура

- Шаг 1. На главной странице выберите Центр обслуживания > Расширенное обслуживание > Экспорт.
- Шаг 2. Нажмите «Экспорт» , чтобы экспортировать серийный номер, версию микропрограммы, журналы работы устройства и информацию о конфигурации.

3.14.7.2 Захват пакетов

Захват пакетов

- 1. На главной странице выберите Центр обслуживания > Расширенное обслуживание > Захват пакетов.

Рисунок 3-96. Захват пакетов.

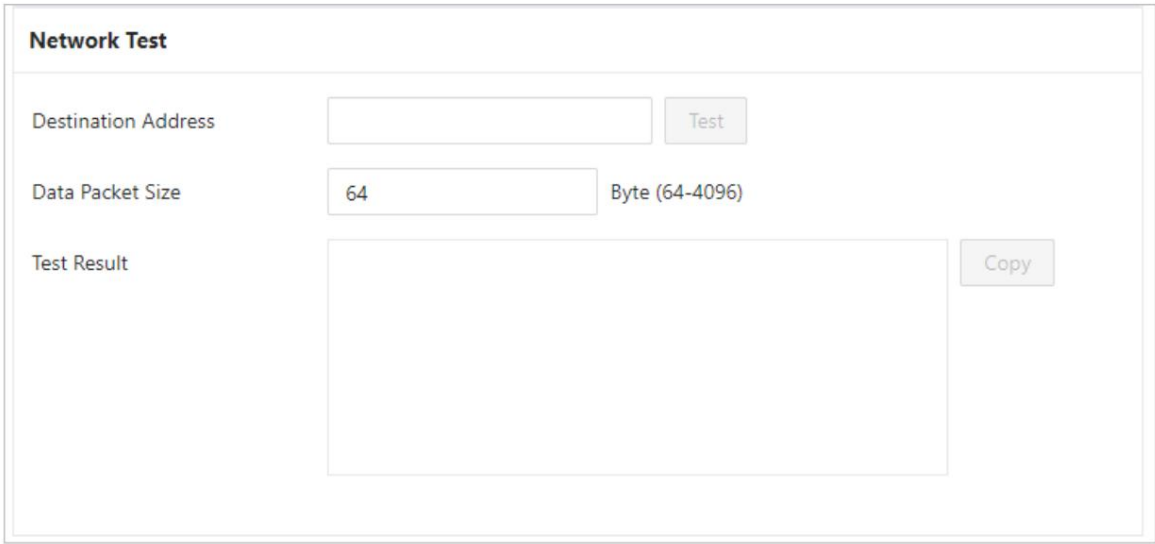
Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	1 166	Optional	Optional	Optional	Optional	0.00MB	►
eth2	1 101	Optional	Optional	Optional	Optional	0.00MB	►

2. Введите IP-адрес, нажмите .
 -  изменения в .
 3. После того, как вы соберете достаточно данных, нажмите .
- Захваченные пакеты автоматически загружаются на ваш локальный компьютер.

Тестирование сети

1. На главной странице выберите Центр обслуживания > Расширенное обслуживание > Захват пакетов.
2. В области «Тестирование сети» введите адрес назначения, а затем настройте размер пакета данных.

Рисунок 3-97. Тест сети.



Network Test

Destination Address

Data Packet Size Byte (64-4096)

Test Result

3. Нажмите «Тест».

Результат отображается в области «Результаты теста». Вы можете скопировать результат.

3.15 Настройки безопасности (необязательно)

3.15.1 Состояние безопасности

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

Справочная информация

- Проверка пользователей и служб: проверка соответствия текущей конфигурации рекомендациям.
- Сканирование модулей безопасности: сканирует состояние работы модулей безопасности, таких как передача аудио- и видеосигнала, доверенная защита, система предупреждения об угрозах и защита от атак, не определяя, включены ли они.

Процедура

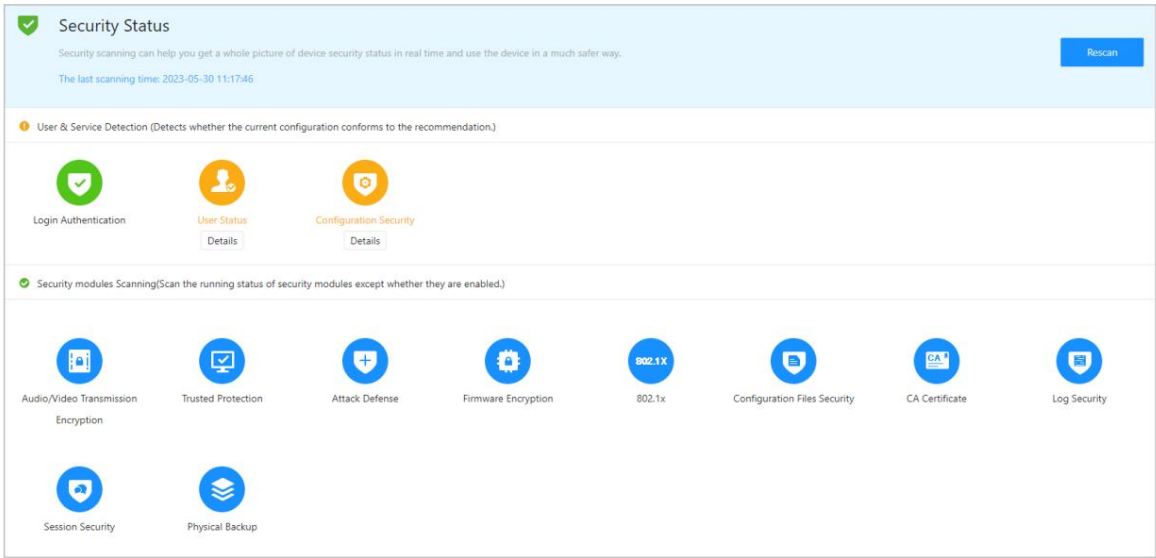
Шаг 1. Выберите >  Состояние безопасности.

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



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

Рисунок 3-98. Состояние безопасности.



Связанные операции

После выполнения сканирования результаты будут отображены разными цветами. Жёлтый цвет указывает на неисправность модулей безопасности, а зелёный — на их исправность.

- Нажмите «Подробности» , чтобы просмотреть подробную информацию о результатах сканирования.
- Нажмите «Игнорировать» , чтобы проигнорировать обнаруженную аномалию, и сканирование не будет выполнено. Обнаруженная аномалия «Игнорируется» будет выделено серым цветом.
- Нажмите «Оптимизировать» , чтобы устранить проблему.

3.15.2 Настройка HTTPS

Создайте сертификат или загрузите аутентифицированный сертификат, после чего вы сможете войти на веб-страницу через HTTPS на своем компьютере. HTTPS обеспечивает безопасность передачи данных по компьютерной сети.

Процедура

Шаг 1. Выберите > Система > Служба > HTTPS.

Шаг 2. Включите службу HTTPS.



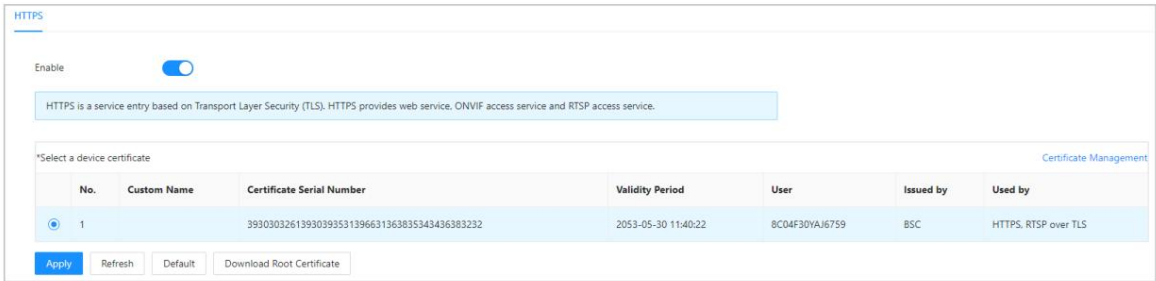
Если включить параметр "Совместимость с TLS v1.1 и более ранними версиями", могут возникнуть риски для безопасности. Обращаем ваше внимание.

Шаг 3. Выберите сертификат.



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

Рисунок 3-99 HTTPS



Шаг 4. Нажмите «Применить».

Введите в веб-браузере «https://IP-адрес: https-порт». Если сертификат установлен, вы сможете успешно войти на веб-страницу. В противном случае веб-страница отобразит сертификат как недействительный или ненадежный.

3.15.3 Атака Защита

3.15.3.1 Настройка брандмауэра

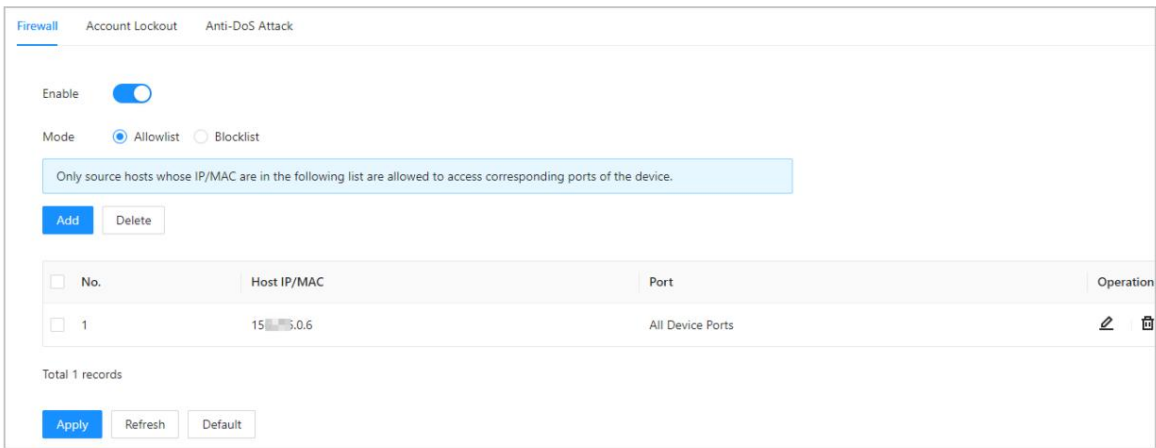
Настройте брандмауэр для ограничения доступа к устройству.

Процедура

Шаг 1. Выберите > Защита от атак > Межсетевой экран.

Шаг 2. Нажмите, чтобы включить функцию брандмауэра.

Рисунок 3-100 Межсетевой экран



Шаг 3. Выберите режим: Список разрешенных и Список заблокированных.

- Список разрешенных адресов : Доступ к устройству разрешен только для IP-адресов/MAC-адресов из списка разрешенных адресов.
- Список заблокированных адресов : Доступ к устройству запрещен для IP-адресов/MAC-адресов из списка заблокированных адресов.

Шаг 4. Нажмите «Добавить» , чтобы ввести IP-адрес.

Рисунок 3-101. Добавить информацию об IP-адресе.

Шаг 5. Нажмите OK.

Связанные операции

- Нажмите, чтобы отредактировать информацию об IP-адресе.
- Нажмите, чтобы удалить IP-адрес.

3.15.3.2 Настройка блокировки учетной записи

Если неверный пароль будет введен заданное 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, указанное для учетной записи администратора и ONVIF. Пользователь будет заблокирован.

Рисунок 3-102 Блокировка учетной записи

- Количество попыток входа: Лимит попыток входа. Если неверный пароль будет введен определенное количество раз, учетная запись будет заблокирована.
- Время

блокировки: Период времени, в течение которого вы не сможете войти в систему после блокировки учетной записи.

Шаг 3. Нажмите «Применить».

3.15.3.3 Настройка защиты от DoS-атак

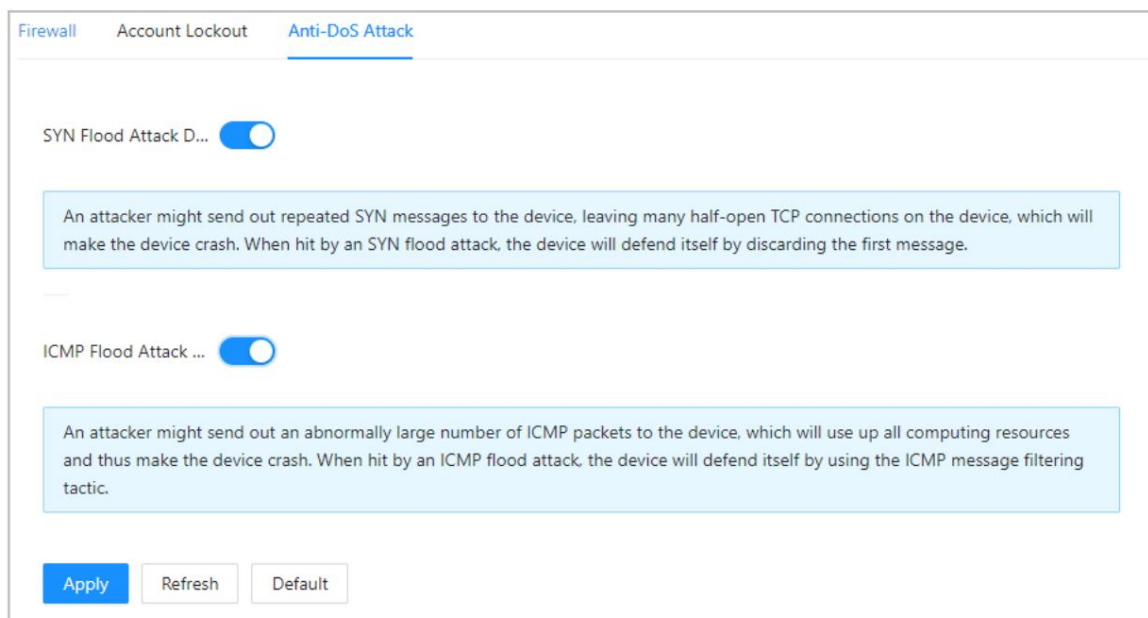
Для защиты устройства от DoS-атак можно включить защиту от SYN-флуд-атак и защиту от ICMP-флуд-атак .

Процедура

Шаг 1. Выберите > Защита от атак > Защита от DoS-атак.

Шаг 2. Включите защиту от SYN-флуд-атак или ICMP-флуд-атак , чтобы защитить устройство от DoS-атаки.

Рисунок 3-103 Защита от DoS-атаки



Шаг 3. Нажмите «Применить».

3.15.4 Сертификат на устанавливаемое устройство

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

3.15.4.1 Создание сертификата

Создайте сертификат для устройства.

Процедура

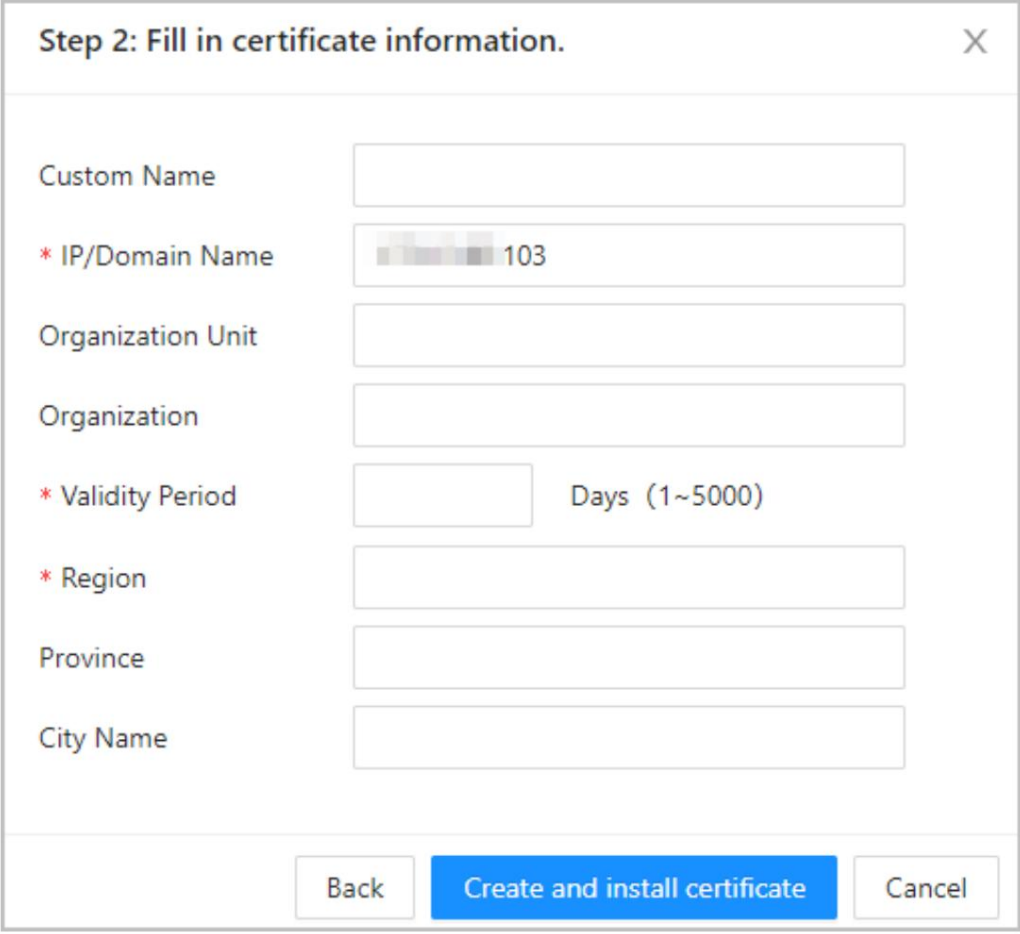
Шаг 1. Выберите > Сертификат центра сертификации > Сертификат устройства.

Шаг 2. Выберите «Установить сертификат устройства».

Шаг 3. Выберите «Создать сертификат». Шаг 4. , и нажмите «Далее».

Введите информацию о сертификате.

Рисунок 3-104 Информация о сертификате




Название региона не может превышать 2 символов. Рекомендуется вводить сокращенное название региона.

Шаг 5. Нажмите «Создать и установить сертификат».

После успешной установки сертификата он отобразится на странице «Сертификаты устройства».

Связанные операции

- На странице «Сертификат устройства» нажмите «Войти в режим редактирования», чтобы изменить имя сертификата.
- Нажмите, чтобы загрузить сертификат.
- Нажмите, чтобы удалить сертификат.

3.15.4.2 Подача заявки на получение и импорт сертификата CA

Импортируйте сертификат стороннего центра сертификации на устройство.

Процедура

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

Шаг 2. Нажмите «Установить сертификат устройства».

Шаг 3. Выберите «Подать заявку на получение сертификата CA и импорт (рекомендуется)», и нажмите «Далее».

Шаг 4. Введите информацию о сертификате.

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

- Регион: Название региона не должно превышать 3 символов. Рекомендуем ввести Сокращенное название региона.

Рисунок 3-105 Информация о сертификате (2)

The screenshot shows a web form titled "Step 2: Fill in certificate information." with a close button (X) in the top right corner. The form contains the following fields and labels:

- * IP/Domain Name**: A text input field containing "172.16.0.03".
- Organization Unit**: A text input field.
- Organization**: A text input field.
- * Region**: A text input field.
- Province**: A text input field.
- City Name**: A text input field.

At the bottom of the form, there are three buttons: "Back", "Create and Download" (highlighted in blue), and "Cancel".

Шаг 5. Нажмите «Создать и загрузить».

Сохраните файл запроса на свой компьютер.

Шаг 6. Обратитесь в сторонний центр сертификации за сертификатом, используя файл запроса.

Шаг 7. Импортируйте подписанный сертификат центра сертификации.

1. Сохраните сертификат центра сертификации на свой компьютер.
2. Нажмите «Установка сертификата устройства».
3. Нажмите кнопку «Обзор», чтобы выбрать сертификат центра сертификации.
4. Нажмите «Импорт и установка».

После успешной установки сертификата он отобразится на странице «Сертификаты устройства».

- Нажмите «Создать заново», чтобы повторно создать файл запроса.
- Нажмите «Импортировать позже», чтобы импортировать сертификат позже.

Связанные операции

- На странице «Сертификат устройства» нажмите «Войти в режим редактирования», чтобы изменить имя сертификата.
- Нажмите, чтобы загрузить сертификат.
- Нажмите, чтобы удалить сертификат.

3.15.4.3 Установка существующего сертификата

Если у вас уже есть файл сертификата и файл закрытого ключа, импортируйте их.

Процедура

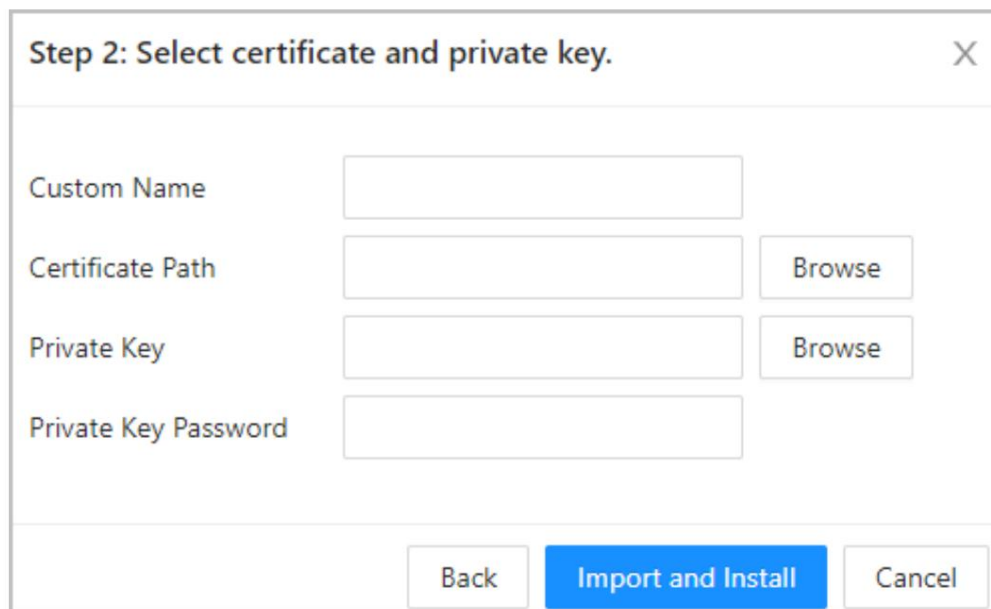
Шаг 1. Выберите Безопасность > Сертификат центра сертификации > Сертификат устройства.

Шаг 2. Нажмите «Установить сертификат устройства».

Шаг 3. Выберите «Установить существующий сертификат». , и нажмите «Далее».

Шаг 4. Нажмите «Обзор» , чтобы выбрать файл сертификата и закрытого ключа, и введите закрытый ключ. пароль.

Рисунок 3-106 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 «Импорт и установка».

После успешной установки сертификата он отобразится на странице «Сертификаты устройства» .

Связанные операции

- На странице «Сертификат устройства» нажмите «Войти в режим редактирования» , чтобы изменить имя сертификата.
- Нажмите  чтобы скачать сертификат.
- Нажмите  чтобы удалить сертификат.

3.15.5 Установка доверенного сертификата центра сертификации

Доверенный сертификат центра сертификации (ЦС) — это цифровой сертификат, используемый для проверки подлинности веб-сайтов и серверов. Например, при использовании протокола 802.1x для коммутаторов требуется сертификат ЦС для подтверждения их подлинности.

Справочная информация: 802.1X — это

протокол сетевой аутентификации, который открывает порты для доступа к сети, когда организация подтверждает личность пользователя и предоставляет ему доступ к сети.

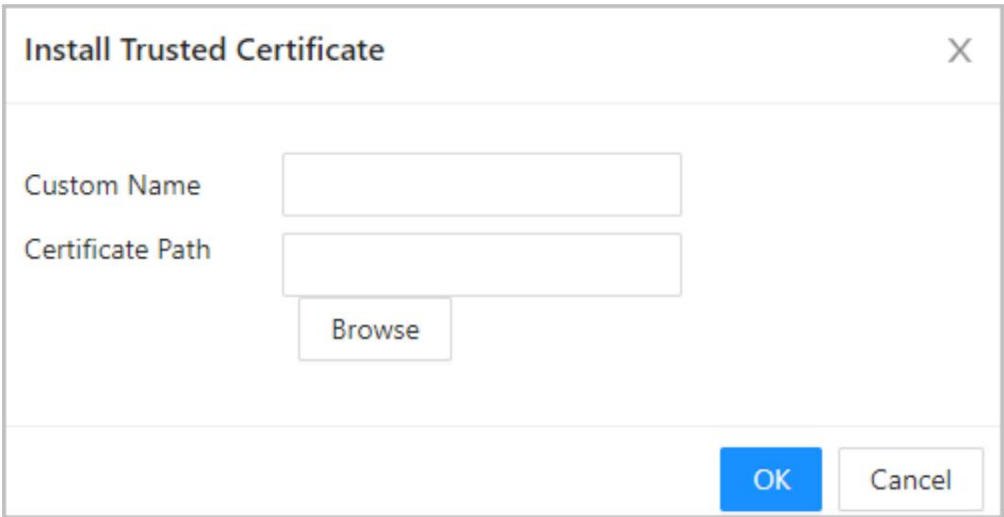
Процедура

Шаг 1. Выберите > Сертификаты >  центра сертификации > Доверенные сертификаты центра сертификации.

Шаг 2. Выберите «Установить доверенный сертификат».

Шаг 3. Нажмите кнопку «Обзор» , чтобы выбрать доверенный сертификат.

Рисунок 3-107. Установите доверенный сертификат.



Шаг 4. Нажмите OK.

После успешной установки сертификата он отображается на странице «Доверенные сертификаты центра сертификации» .

Связанные операции

- На странице «Сертификат устройства» нажмите «Войти в режим редактирования» , чтобы изменить имя сертификата.
- Нажмите  чтобы скачать сертификат.
- Нажмите  чтобы удалить сертификат.

3.15.6 Шифрование данных

Процедура

Шаг 1. Выберите > Шифрование данных.

Шаг 2. Настройте параметры.

Рисунок 3-108 Шифрование данных

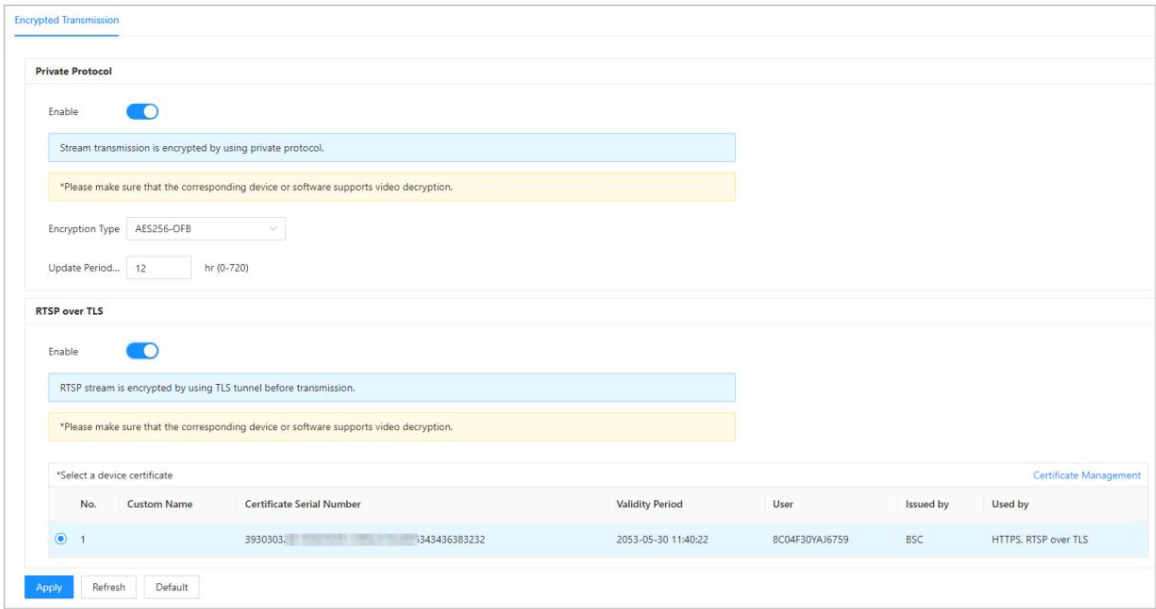


Таблица 3-51. Описание шифрования данных.

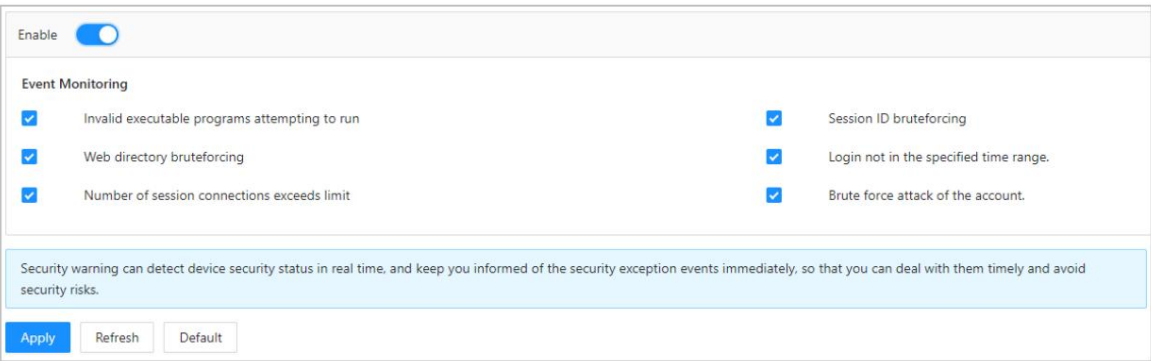
	Параметр	Описание
Частный протокол	Делать возможность	Передача потоков данных осуществляется с использованием частного протокола и шифруется во время передачи.
	Тип шифрования	Оставьте значение по умолчанию.
	Период обновления секретности Ключ	Диапазон значений от 0 ч до 720 ч. 0 означает, что секретный ключ никогда не будет обновляться.
RTSP поверх TLS	Делать возможность	Поток RTSP шифруется во время передачи через туннель TLS.
		Создайте или импортируйте сертификат. Подробности см. в разделе «Управление сертификатами» (раздел 3.15.4 «Установка сертификата устройства»). Установленные сертификаты отображаются в списке.

3.15.7 Предупреждение о безопасности

Процедура

- Шаг 1. Выберите > Предупреждение безопасности.
- Шаг 2. Включите функцию предупреждения системы безопасности.
- Шаг 3. Выберите элементы мониторинга.

Рисунок 3-109. Предупреждение о безопасности.



- Шаг 4. Нажмите «Применить».

3.15.8 Аутентификация безопасности

Процедура

- Шаг 1. Выберите Безопасность > Аутентификация безопасности.
- Шаг 2. Выберите алгоритм хэширования сообщения.
- Шаг 3. Нажмите «Применить».

Рисунок 3-110. Аутентификация безопасности.

Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☒ MD5 ☐ SHA256

Digest Algorithm for ONVIF User Authentication ☒ MD5 ☐ SHA256

4. Работа с телефоном

4.1 Инициализация

Если телефон находится в той же локальной сети, что и контроллер доступа, инициализацию контроллера доступа можно выполнить в первый раз или после восстановления заводских настроек устройства через веб-страницу телефона. В этом разделе рассматривается инициализация телефона через точку доступа Wi-Fi.

Предварительные требования

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



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

Процедура

Шаг 1. Включите контроллер доступа.

Шаг 2. Через 30 секунд после того, как устройство перейдет на экран инициализации, подключитесь к точке доступа Wi-Fi на вашем телефоне. Название точки доступа — серийный номер продукта + модель устройства.

Если вы не подключились к точке доступа Wi-Fi в течение 30 минут, точка доступа будет отключена.

Шаг 3. Откройте браузер на своем телефоне и перейдите по IP-адресу точки доступа (адрес по умолчанию — 192.168.3.1).

Шаг 4. Нажмите «Начать инициализацию».

Шаг 5. Выберите язык.

Шаг 6. Введите и подтвердите пароль, укажите адрес электронной почты, а затем нажмите «Далее».



- Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа следующих символов: заглавные буквы, строчные буквы, цифры и специальные символы (за исключением ' ').
- Установите надежный пароль, следуя подсказкам о его надежности.
- Храните пароль в безопасности после инициализации и регулярно меняйте его для повышения уровня безопасности.
- Если вы хотите сбросить пароль администратора, отсканировав QR-код, вам потребуется указанный адрес электронной почты для получения кода безопасности.

Шаг 7. При необходимости включите автоматическую проверку, а затем нажмите «Выполнено».

4.2 Вход на веб-страницу

Предварительные требования

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

Процедура

Шаг 1. Откройте браузер и введите IP-адрес устройства.

Вы можете войти на веб-страницу тремя следующими способами:

- Телефон и устройство находятся в одной локальной сети. Откройте браузер на телефоне и введите IP-адрес.

- Телефон и устройство находятся в одной локальной сети. Отсканируйте QR-код.
Настройки связи > Сетевые настройки > Wi-Fi на веб-странице вашего телефона.

- Подключите точку доступа устройства к своему телефону. На главном экране устройства коснитесь верхнего правого угла, чтобы перейти к экрану точки доступа Wi-Fi . Отсканируйте QR-код с IP-адресом через браузер на телефоне или введите в браузере телефона IP-адрес, отображаемый на экране точки доступа Wi-Fi .

Также вы можете выбрать «Настройки связи» > «Сетевые настройки» > «Точка доступа Wi-Fi» , чтобы перейти в главное меню.



Wi-Fi и точки доступа Wi-Fi доступны в некоторых моделях.

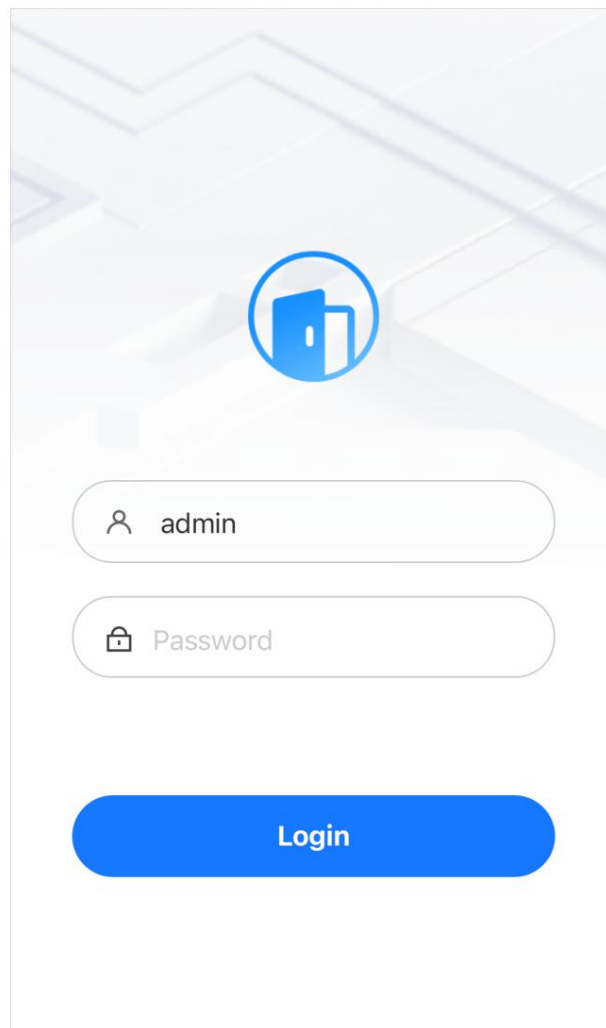
Шаг 2. Введите имя пользователя и пароль.

Нажмите  рядом с паролем, чтобы просмотреть его.



- Имя администратора по умолчанию — admin, а пароль — тот, который вы установили во время инициализации. Мы рекомендуем регулярно менять пароль администратора для повышения безопасности.
- Если вы забыли пароль администратора, вы можете восстановить его через веб-страницу на компьютере. Подробнее см. раздел «3.3 Восстановление пароля».

Рисунок 4-1 Страница входа

The image shows a login page with a light gray background featuring a subtle geometric pattern of overlapping squares. At the top center is a blue circular icon containing a white door symbol. Below this icon are two input fields: the first is labeled 'admin' with a person icon, and the second is labeled 'Password' with a lock icon. At the bottom center is a large, rounded blue button with the word 'Login' in white text.

Шаг 3. Нажмите «Войти».

4.3 Главная страница

Главная страница отображается после успешного входа в систему.

- Нажмите на  в правом верхнем углу веб-страницы, затем нажмите «QR-код документации по продукту», чтобы отсканировать QR-код и получить материалы по продукту, или нажмите «Выход», чтобы выйти из учетной записи.



Документация по продукту доступна для некоторых моделей.

- В разделе «Состояние двери» отображается состояние двери. Вы можете дистанционно открывать или закрывать дверь. Вы также можете настроить статус двери как «Всегда открыта» или «Всегда закрыта».

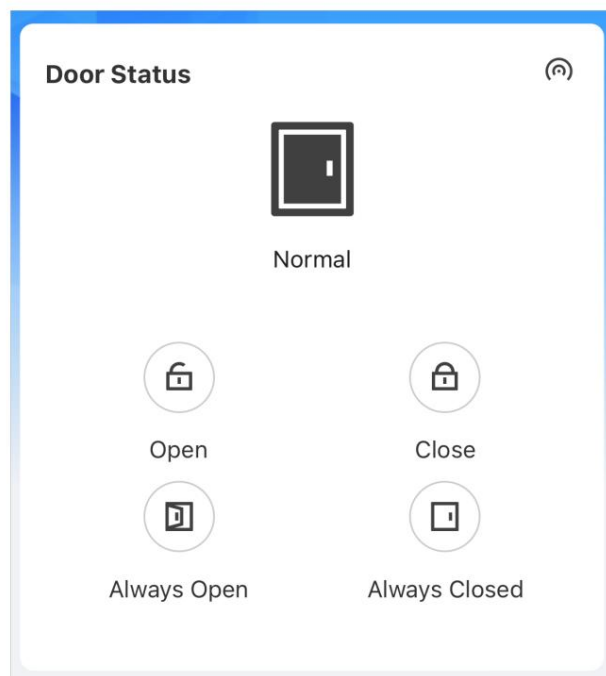


◇ Это означает, что проводная сеть подключена.



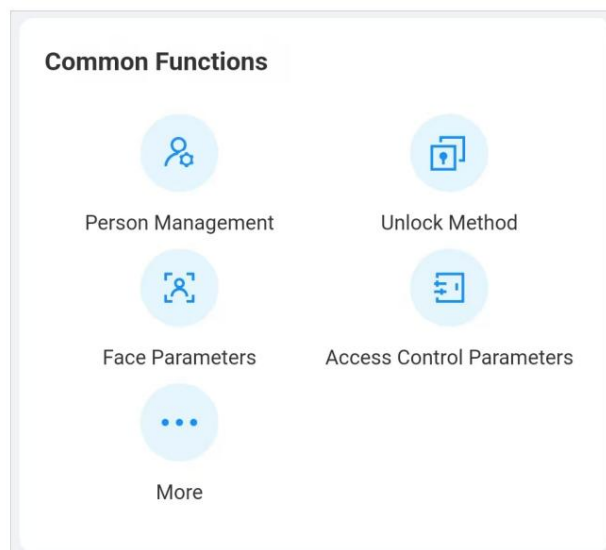
◇ Это означает, что точка доступа Wi-Fi включена.

Рисунок 4-2. Состояние двери.



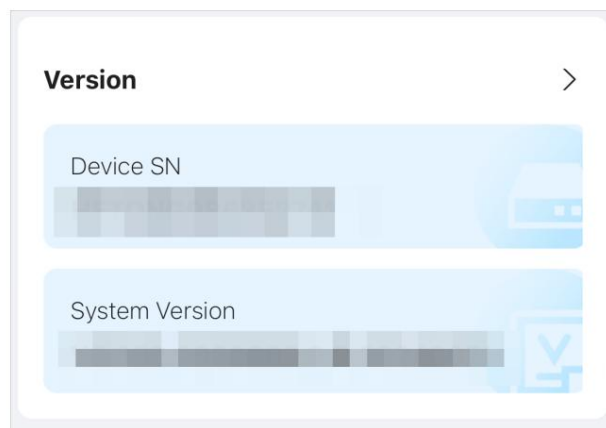
- В разделе «Общие функции» отображается меню настроек устройства. Нажмите «Подробнее», чтобы просмотреть все меню настроек.

Рисунок 4-3. Общие функции



- В разделе «Версия» можно просмотреть серийный номер и информацию о версии. Нажмите > для просмотра. Подробности о версии.

Рисунок 4-4. Версия



4.4 Управление персоналом

Добавьте пользователя и настройте права доступа.

Процедура

Шаг 1. Войдите на веб-страницу, а затем

Шаг 2. Нажмите «Управление персоналом» и нажмите +.

Шаг 3. Настройте информацию о пользователе.

Рисунок 4-5. Добавить человека (1)

A screenshot of a mobile application's 'Basic Info' form for adding a user. The form has a light blue header with the title 'Basic Info'. Below the header, there are two light blue rounded rectangular boxes. The first box is labeled 'Basic Info' and contains two input fields: '* ID' and 'Name'. The second box is labeled 'Access Credentials' and contains four input fields: 'Face', 'Password', 'Card', and 'Fingerprint'. Each of these fields has a right-pointing chevron and a status indicator: '0' for 'Face', 'Card', and 'Fingerprint', and 'Not Added' for 'Password'.

Рисунок 4-6. Добавить человека (2)

Verification Mode

Same as Device

Permission

User

Validity Period

2037-12-31 23:59:59

General Plan

255-Default

Holiday Plan

255-Default

User Type

General User

Times Used

Unlimited

Permission Type

Unlock and Attendance

Таблица 4-1. Описание параметров.

Параметр	Описание
—	Идентификатор пользователя аналогичен идентификатору сотрудника и может состоять из цифр, букв и их комбинаций, при этом максимальная длина числа составляет 30 символов.
Имя	Имя может содержать до 32 символов (включая цифры, символы и буквы).
Лицо	Поддерживается загрузка изображения лица или создание фотографии. Каждый пользователь может добавить не более 2 изображений лица. После загрузки изображение лица можно просмотреть или удалить.  Изображение лица должно быть в формате jpg, jpeg, png и иметь размер менее 100 КБ. После того, как вы сделаете снимок лица, вы сможете просмотреть или удалить его.
Пароль	Настройте пароль пользователя. Максимальная длина пароля — 8 цифр. Пароль принуждения — это пароль разблокировки + 1. Например, если пароль пользователя — 12345, то пароль принуждения будет 12346. Сигнализация принуждения сработает при использовании пароля принуждения для разблокировки двери.

Параметр	Описание
Карта	Нажмите «Добавить», введите номер карты вручную или проведите карту через специальное считывающее устройство. Пользователь может зарегистрировать максимум 5 карт. После успешного добавления нажмите на добавленную карту, вы сможете изменить номер карты, настроить карту как карту принуждения или удалить карту. Если вы включите тревожную сигнализацию, то при использовании карты вызова помощи для разблокировки двери сработает сигнализация.  Один пользователь может установить только одну принудительную карту.
Отпечаток пальца	Регистрация отпечатков пальцев. Пользователь может зарегистрировать до 3 отпечатков пальцев, и вы можете назначить один из них в качестве отпечатка для вызова помощи. Сигнализация сработает, когда отпечаток пальца будет использован для разблокировки двери. 1. Нажмите «Добавить». 2. Прижмите палец к сканеру в соответствии с инструкциями на экране. 3. Нажмите ОК.  • Функция сканирования отпечатков пальцев доступна только на некоторых моделях. • Мы не рекомендуем устанавливать первый отпечаток пальца в качестве принудительных отпечатков пальца. • Один пользователь может установить только один принудительный отпечаток пальца.
Bluetooth-карта	 Функция Bluetooth доступна только на некоторых моделях. Вы можете выбрать вариант «Запрос по электронной почте» или «Запрос с помощью регистрационного кода». • Запрос по электронной почте : подходит для тех, кто впервые использует Bluetooth-карту. Запрос. Вы можете запросить до 5 Bluetooth-карт, используя адрес электронной почты, зарегистрированный в DMSS.  Перед использованием этой функции необходимо ввести зарезервированный адрес электронной почты. 1. Настройте адрес электронной почты, зарегистрированный в DMSS. 2. Нажмите «Запрос по электронной почте», после чего можно будет получить Bluetooth-карты по запросу. • Запрос через регистрационный код : подходит, если у вас уже есть карта Bluetooth и вы хотите использовать ее на другом контроллере доступа, поддерживающем функцию Bluetooth. 1. Скопируйте код регистрации Bluetooth из DMSS. 2. Нажмите «Запросить с помощью регистрационного кода», а затем введите код. 3. Нажмите ОК.

Параметр	Описание
Режим проверки	Настройте режим проверки для пользователя. Вы можете использовать режим, совпадающий с режимом устройства, или настроить свой собственный. • Аналогично устройству : Режим работы идентичен режиму работы устройства. • Пользовательский : После выбора пользовательского режима отобразятся «Метод комбинации» и «Метод разблокировки». Выберите необходимый метод комбинации и метод разблокировки. ◇ Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы открыть дверь. ◇ И ещё: используйте все выбранные способы разблокировки, чтобы открыть дверь.  ◇ Настраиваемый режим проверки действителен только для локального устройства. Он не может использоваться во внешних считывателях карт. ◇ Если пользовательский режим проверки отличается от режима устройства, приоритет отдается пользовательскому режиму.
Разрешение	• Пользователь : Пользователи имеют только права доступа к дверям или учета рабочего времени. • Администратор : Администраторы могут настраивать устройство, помимо доступа к дверям и т. д. Разрешения на посещение.
Срок действия	Укажите дату, когда истекает срок действия разрешений на доступ к двери и учет рабочего времени данного лица.
Генеральный план	В течение установленного периода люди могут открывать дверь или отмечать присутствие.  Вы можете выбрать несколько тарифных планов.
План на отпуск	В дни установленных праздников посетители могут открывать двери или отмечать присутствие.  Вы можете выбрать более одного праздника.
Выберите разрешения блокировки: выберите локальную и внешнюю блокировку по мере необходимости.	
Тип пользователя	• Обычный пользователь : Обычные пользователи могут открыть дверь. • Пользователь из черного списка : Когда пользователи из черного списка открывают дверь, служба Персонал получит уведомление. • Гостевой пользователь : Гости могут открыть дверь в течение определенного периода времени или на определенное количество раз. По истечении установленного периода или по истечении времени разблокировки, открыть дверь будет невозможно. • Патрульный пользователь : Патрульные пользователи могут отмечать посещаемость на устройстве, но они не имеют доступа к двери. • VIP-пользователь : Когда VIP-пользователь открывает дверь, обслуживающий персонал получает... уведомление. • Другой пользователь : Когда он откроет дверь, она останется открытой в течение 5 минут, ещё несколько секунд. • Пользователь 1/Пользователь 2: То же самое, что и для обычных пользователей.
Затраченное время	Установите лимит времени разблокировки для гостевых пользователей. После истечения этого лимита они не смогут открыть дверь.

Параметр	Описание
Отделение	Добавьте пользователей в отдел. Если сотруднику назначен график работы отдела, он будет следовать установленному графику.
Режим расписания	• Расписание отдела: Назначить пользователю расписание отдела. • Личное расписание: Назначить пользователю личное расписание.  ♦ Эта функция доступна только на некоторых моделях. ♦ Если вы установите здесь режим расписания на «расписание отдела», то персональное расписание, настроенное для пользователя в разделе «Учет посещаемости > Настройка расписания > Персональное расписание», будет недействительным.
Тип разрешения	• Открытие и учет присутствия: У пользователя есть разрешение на учет присутствия, и он может открыть дверь, используя настроенные методы проверки. • Учет присутствия: У пользователя есть только разрешение на учет присутствия, и он не может открыть дверь. После успешной проверки личности пользователя создается одна запись о неудачной попытке открытия.

Шаг 4. Нажмите «Добавить».

4.5 Настройка системы

4.5.1 Просмотр информации о версии

На веб-странице выберите «Дополнительно» > «Система» > «Версия», и вы сможете просмотреть информацию о версии устройства.

4.5.2 Управление конфигурацией

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Система > Конфигурация.

Шаг 3. При необходимости восстановите заводские настройки по умолчанию.

- Восстановление заводских настроек (с сохранением сетевой конфигурации) : Сбрасывает все настройки.

За исключением сетевой конфигурации устройства. • Восстановление настроек

по умолчанию (сохраняет журналы, информацию о пользователе и сетевую конфигурацию) : Сбрасывает настройки устройства.

удаляет все данные, кроме информации о пользователе, журналов и сетевых конфигураций, и вносит изменения в настройки устройства.

4.5.3 Техническое обслуживание

Для повышения производительности устройства рекомендуется регулярно перезагружать его в режиме ожидания.

Процедура

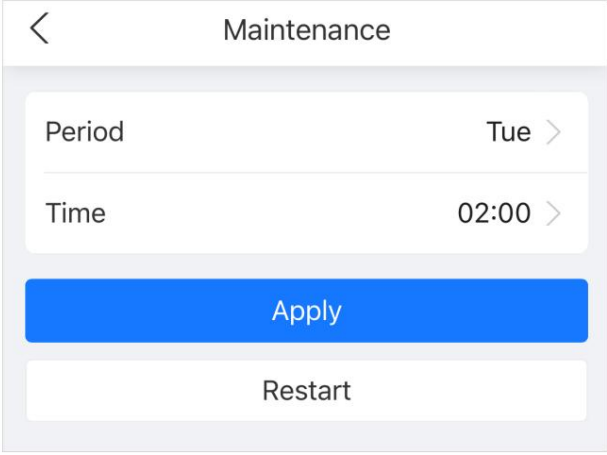
Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Система > Обслуживание.

Шаг 3. Установите время, а затем нажмите «Применить».

Устройство перезагрузится в запланированное время, или вы можете нажать «Перезагрузить», чтобы перезагрузить его немедленно.

Рисунок 4-7. Техническое обслуживание.



The screenshot shows a mobile application interface titled "Maintenance". At the top left is a back arrow icon. Below the title, there are two settings: "Period" set to "Tue" and "Time" set to "02:00", both with right-pointing chevron icons. Below these settings are two buttons: a blue "Apply" button and a white "Restart" button with a grey border.

4.5.4 Настройка времени

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Система > Время.

Шаг 3. Настройте время.

Рисунок 4-8. Настройка параметров времени.

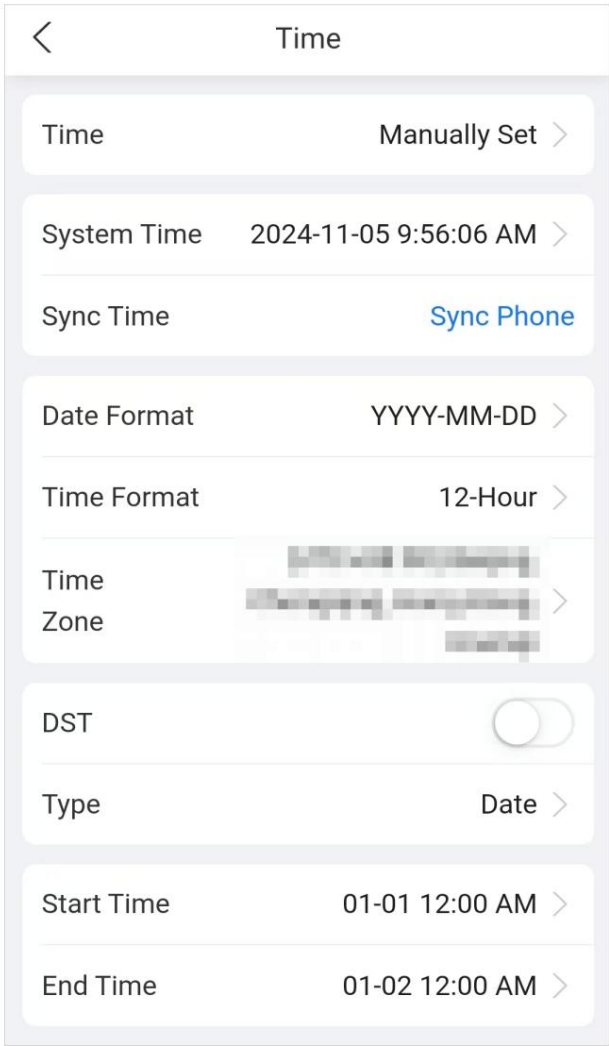


Таблица 4-2. Описание настроек времени.

Параметр	Описание
Время	• Ручная настройка: Введите время вручную или нажмите «Синхронизировать телефон», чтобы синхронизировать время с телефоном. • NTP: Устройство автоматически синхронизирует время с NTP-сервером. сервер. ◇ Сервер : Введите домен NTP-сервера. ◇ Порт : Введите порт NTP-сервера. ◇ Интервал : Введите время с указанием интервала синхронизации.
Формат даты	Выберите формат даты и формат времени.
Формат времени	
Часовой пояс	Выберите часовой пояс.
летнее время	1. (Необязательно) Включите летнее время. 2. Выберите «Дата» или «Неделя» в качестве типа. 3. Настройте время начала и окончания перехода на летнее время.

Шаг 4. Нажмите «Применить».

4.5.5 Объем данных

Вы можете увидеть, сколько пользователей, карт, изображений лиц, отпечатков пальцев, журналов, записей разблокировки и другой информации может хранить устройство.

Войдите на веб-страницу и выберите «Дополнительно» > «Система» > «Объем данных».

4.5.6 Язык

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

4.6 Настройка учета посещаемости

Эта функция доступна только на некоторых моделях.

4.6.1 Настройка отделов

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройка посещаемости > Настройки отдела.

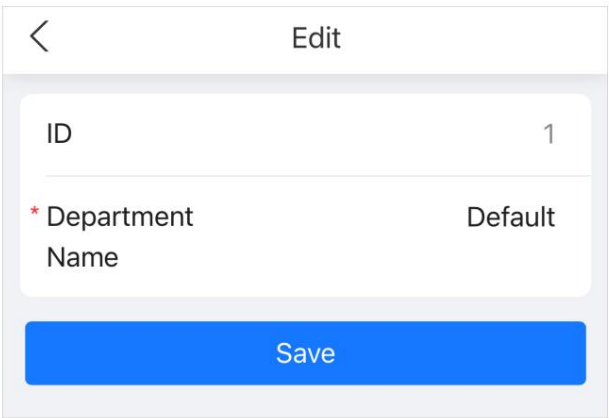
Рисунок 4-9. Настройки отдела.



Шаг 3. Коснитесь отдела, чтобы переименовать его, а затем коснитесь «Сохранить».

По умолчанию существует 20 отделов. Рекомендуем переименовать их.

Рисунок 4-10. Переименуйте отдел.



Связанные операции

Вы можете нажать  восстановить настройки отделов по умолчанию.

4.6.2 Настройка смен

Настройте смены, чтобы определить правила учета рабочего времени. Сотрудники должны начинать работу в запланированное время и заканчивать ее в запланированное время, за исключением случаев, когда они выбирают работу сверхурочно.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройка посещаемости > Настройка смены > Смена.

Рисунок 4-11 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. Нажмите клавишу Shift, чтобы настроить параметры переключения, а затем нажмите «Сохранить».

Рисунок 4-12. 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 4-3. Описание параметров сдвига.

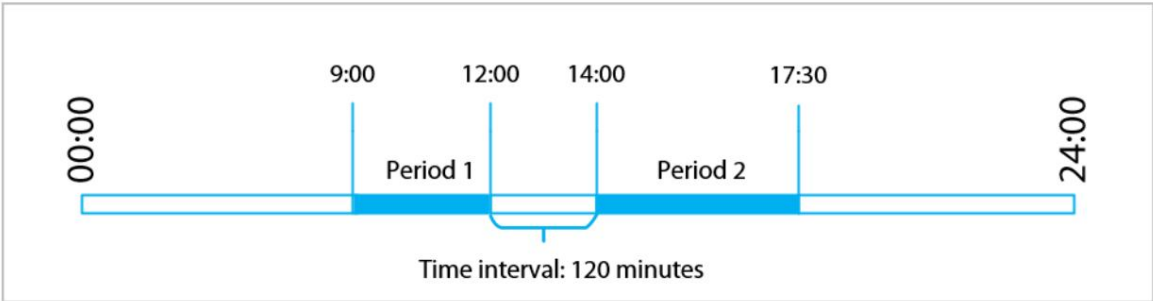
Параметр	Описание
Название смены	Введите название смены.
Период 1	Укажите временной диапазон, в течение которого сотрудники могут отмечать начало и конец рабочего дня. Необходимо настроить как минимум один период. • Если вы установили только один период учета рабочего времени, сотрудники должны отмечать начало и конец рабочего дня в установленное время, чтобы избежать ошибок в их табелях учета рабочего времени. Например, если вы установили период с 08:00 до 17:00, сотрудники должны отметить начало рабочего дня до 08:00 и конец рабочего дня с 17:00 и далее. • Если вы установили 2 периода учета рабочего времени, эти 2 периода не могут быть использованы. Периоды частично совпадают. Сотрудники должны отмечать время прихода и ухода за оба периода. • Если вы зададите 3 периода, они не должны перекрываться. Сотрудники должны отмечать начало и конец рабочего дня для двух смежных периодов.  Последний период может охватывать несколько дней. Если период сверхурочной работы является последним, вы можете настроить его таким образом, чтобы он охватывал несколько дней.
Период 2	
Период 3	

Параметр	Описание
Период сверхурочной работы	Сотрудники, отмечающие время прихода и ухода с работы в течение установленного периода, будут считаться работающими сверх своего обычного рабочего времени.
Ограничение на опоздание (мин)	Сотрудникам может быть предоставлено определенное время для того, чтобы они могли немного опоздать на работу и немного раньше уйти. Например, если обычное время начала работы — 08:00, то допустимый период в 5 минут может быть установлен для сотрудников, прибывших к 08:05, чтобы их не считали опоздавшими.
Ограничение на досрочный отъезд (мин)	

Если вы настраиваете несколько периодов, обратитесь к приведенным ниже инструкциям для выполнения функции учета рабочего времени.

- Если интервал времени между двумя периодами четный, можно разделить его на 2 и отнести первую половину интервала к первому периоду в качестве времени окончания работы. Вторую половину интервала следует отнести ко второму периоду в качестве времени начала работы.

Рисунок 4-13. Временной интервал (четное число).



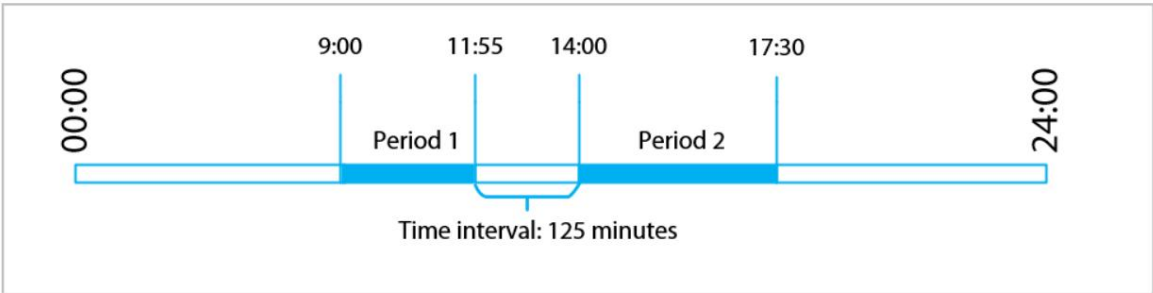
Например: если интервал составляет 120 минут, то время окончания работы в период 1 — с 12:00 до 12:59, а время начала работы в период 2 — с 13:00 до 14:00.



Если сотрудник несколько раз отмечает свой уход в течение первого периода, будет считаться действительным самое позднее время, а если он несколько раз отмечает свой приход в течение второго

периода, будет считаться действительным самое раннее время. • Если интервал времени между двумя периодами нечетный, то наименьшая часть интервала будет отнесена к первому периоду и будет считаться временем ухода. Наибольшая часть интервала будет отнесена ко второму периоду и будет считаться временем прихода.

Рисунок 4-14. Временной интервал (нечетное число).



Например: если интервал составляет 125 минут, то время окончания первого периода — с 11:55 до 12:57, а время начала второго периода — с 12:58 до 14:00. Первый период длится 62 минуты, а второй — 63 минуты.



Если сотрудник несколько раз отмечает свой уход в течение первого периода, будет действовать самое позднее время, а если он несколько раз отмечает свой приход в течение второго периода, будет действовать самое раннее время. • Если

период только один, и вы не отмечаете свой приход или уход к установленному времени, то
Считается отсутствующим в течение 1 дня.

- Если периодов несколько, и вы не отмечаете время начала или окончания работы в установленное время.

Если вы не отметились при приходе или уходе с работы в установленное время в течение 2 или более периодов, это считается отсутствием на 1 день. Присутствие в сверхурочное время не меняет статус отсутствия.

Если вы настроили последний период таким образом, чтобы он охватывал несколько дней, обратитесь к приведенным ниже инструкциям для выполнения функции учета рабочего времени.

- Если второй день — обычная смена, посещаемость соответствует обычному графику. • Если второй день — праздничный день, вы можете отметить свой уход в любое время в течение 24 часов.
праздничный день.



Все данные о времени прихода и ухода указаны с точностью до секунды. Например, если обычное время начала работы установлено на 8:05 утра, сотрудник, отметившийся в 8:05:59 утра, не будет считаться опоздавшим. Однако сотрудник, прибывший в 8:06 утра, будет отмечен как опоздавший на 1 минуту.

Связанные операции

Вы можете нажать  восстановить заводские настройки переключения передач.

4.6.3 Настройка праздников

Настройте планы отпусков, чтобы установить периоды, когда посещаемость не будет отслеживаться.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройка посещаемости > Настройка смен > Праздники.

Шаг 3. Нажмите +, чтобы добавить планы на отпуск.

Шаг 4. Настройте параметры, а затем нажмите «Сохранить».

Рисунок 4-15. Добавьте праздник.

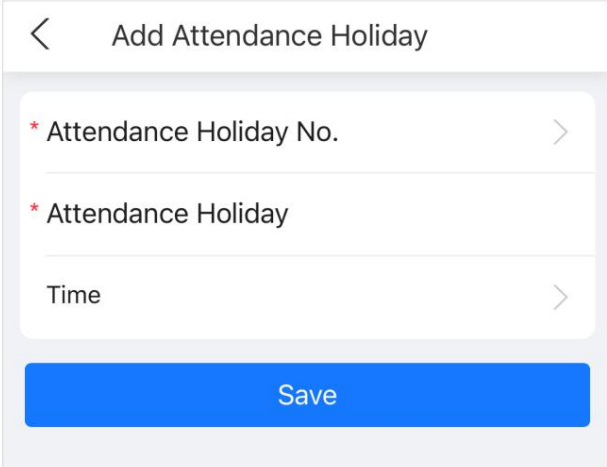


Таблица 4-4. Описание параметров.

Параметр	Описание
Выходной день, связанный с посещаемостью.	Номер праздника.
Выходной день, связанный с посещаемостью	Название праздника.
Время	Время начала и окончания праздника.

Шаг 5. Нажмите ОК.

4.6.4 Настройка графиков работы

График работы обычно включает в себя количество дней в месяц и количество часов в день, в течение которых сотрудник должен находиться на рабочем месте. Можно создавать различные типы графиков работы для разных сотрудников или отделов, и в этом случае сотрудники должны следовать установленному графику.

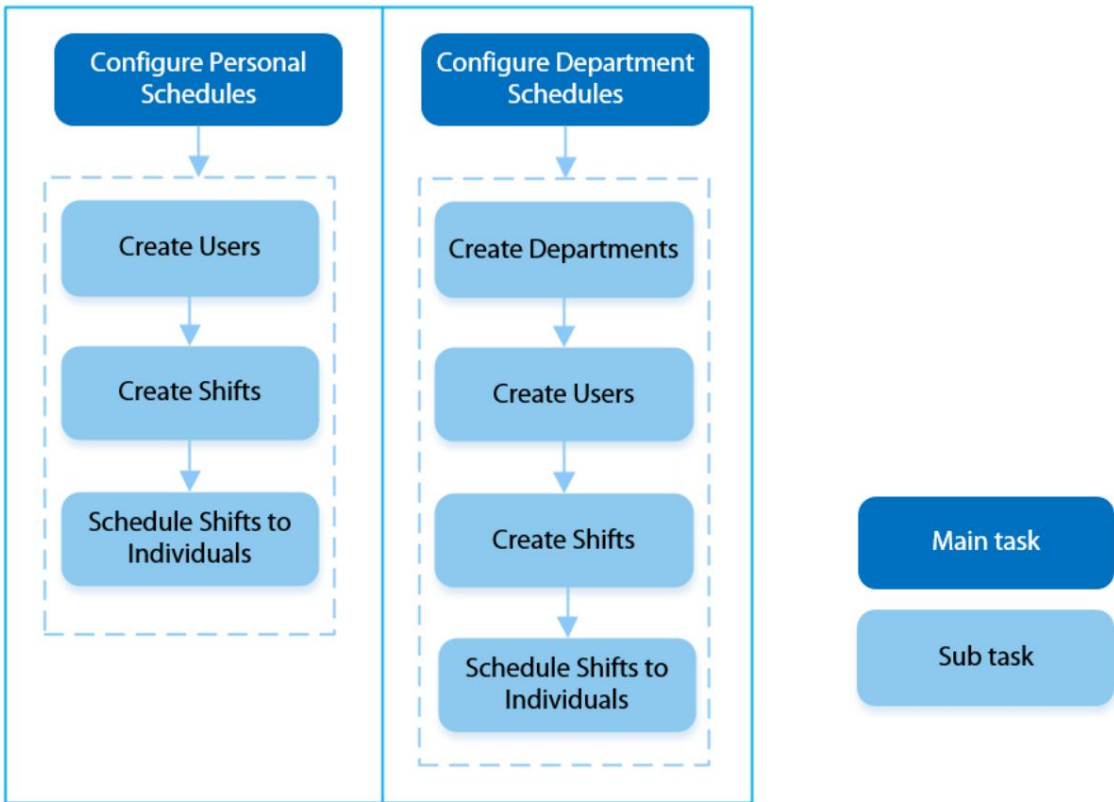
Справочная информация

Для настройки личного или departmental-графика обратитесь к блок-схеме.



При настройке расписания не должно быть перекрывающихся временных периодов в один и тот же день, а также в предыдущий или последующий день.

Рисунок 4-16. Настройка графиков работы.



Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройка посещаемости > Настройка расписания.

Шаг 3. Составьте рабочие графики для отдельных сотрудников.

1. Нажмите «Личное расписание».
2. Выберите человека из списка.



После того, как вы настроите режим расписания как «Персональное расписание» при добавлении человека, этот человек отобразится в списке пользователей.

3. В календаре выберите день, а затем выберите смену.



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

• 0 означает перерыв. •

От 1 до 24 указывает количество предопределенных смен. • 25

означает командировку. • 26

означает отпуск.

Шаг 4. Составьте графики работы для отделов.

1. Нажмите «Расписание отдела».
2. Выберите отдел из списка отделов.
3. В календаре выберите день, а затем выберите смену.

Рисунок 4-17. Расписание отдела.

1-Default						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
0	1	1	1	1	1	0

Cancel
Select Shift
OK

- 0-Rest
- 1-Default
08:00:00-17:00:00 00:00:00-00:00:00 ✓
- 2-Default
08:00:00-17:00:00 00:00:00-00:00:00
- 3-3
08:00:00-17:00:00 00:00:00-00:00:00
- 4-4
08:00:00-17:00:00 00:00:00-00:00:00

• 0 означает отдых.

- Цифры от 1 до 24 обозначают количество predetermined смен.
- 25 означает командировку.
- 26 означает отпуск.



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

4.6.5 Настройка режимов учета посещаемости

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройка посещаемости > Настройка посещаемости.

Шаг 3. Включите локальную регистрацию посещаемости, а затем настройте режим учета посещаемости.

Рисунок 4-18. Конфигурация посещаемости.

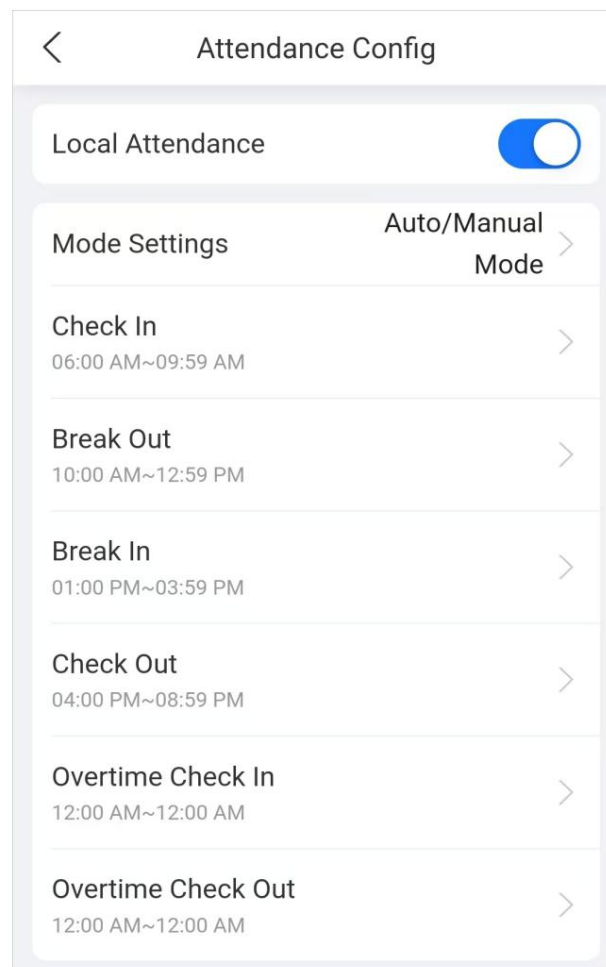


Таблица 4-5. Описание параметров посещаемости.

Параметр	Описание
Автоматический/Ручной режим	На экране автоматически отображается статус присутствия после того, как вы отметили начало или конец рабочего дня, но вы также можете изменить свой статус присутствия вручную. • Регистрация начала работы: Отметьте начало вашего обычного рабочего дня. • Регистрация окончания работы: Отметьте окончание работы, когда начинается ваш перерыв. • Регистрация начала работы: Отметьте окончание работы, когда заканчивается ваш перерыв. • Регистрация окончания работы: Отметьте окончание работы, когда заканчивается ваш обычный рабочий день. • Регистрация начала сверхурочной работы: Отметьте начало вашего сверхурочного периода. • Регистрация окончания сверхурочной работы: Отметьте окончание вашего сверхурочного периода.
Автоматический режим	На экране автоматически отображается ваш статус присутствия после того, как вы отмечаете начало или конец рабочего дня. • Регистрация начала работы: Отметьте начало вашего обычного рабочего дня. • Регистрация окончания работы: Отметьте окончание работы, когда начинается ваш перерыв. • Регистрация начала работы: Отметьте окончание работы, когда заканчивается ваш перерыв. • Регистрация окончания работы: Отметьте окончание работы, когда заканчивается ваш обычный рабочий день. • Регистрация начала сверхурочной работы: Отметьте начало вашего сверхурочного периода. • Регистрация окончания сверхурочной работы: Отметьте окончание вашего сверхурочного периода.
Ручной режим	При регистрации начала и окончания рабочего дня вы можете вручную выбрать свой статус присутствия.
Фиксированный режим	При регистрации начала или окончания рабочего дня на экране постоянно будет отображаться заданный статус посещаемости.

Шаг 4. Нажмите «Применить».

4.7 Настройка контроля доступа

4.7.1 Настройка методов разблокировки

Для разблокировки двери можно использовать несколько способов, таких как отпечаток пальца, Bluetooth, карта и пароль. Вы также можете комбинировать их, чтобы создать свой собственный способ разблокировки.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Нажмите «Способ разблокировки» в главном меню или выберите «Дополнительно» > «Контроль доступа» > «Разблокировать».

Метод.

Шаг 3 (необязательно) Настройте способ ввода комбинации клавиш и способ разблокировки, а затем нажмите.

Применять.

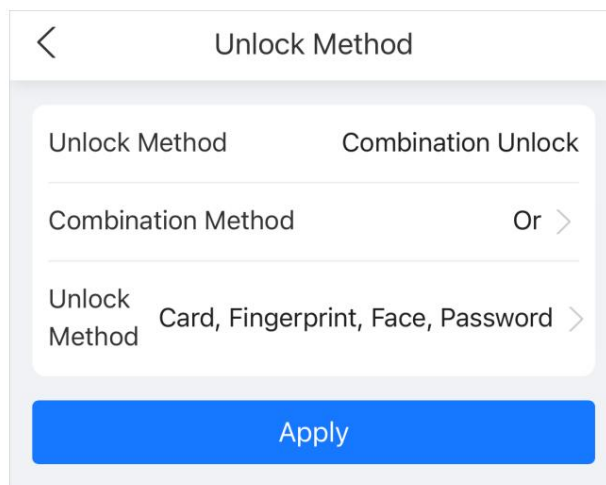
• Комбинированный метод

- ◇ Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы открыть дверь.
- ◇ И ещё: используйте все выбранные способы разблокировки, чтобы открыть дверь.

• Способ разблокировки

Выберите способ разблокировки в соответствии с поддерживаемыми возможностями устройства.

Рисунок 4-19. Способ разблокировки.



4.7.2 Настройка параметров лицевой панели

Настройте параметры распознавания лиц. Параметры распознавания лиц могут различаться в зависимости от модели устройства.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. В главном меню нажмите «Параметры лица» или выберите «Дополнительно» > «Контроль доступа» > «Параметры лица».

Шаг 3. Настройте параметры, а затем нажмите «Применить».

Рисунок 4-20 Настройка параметров лица (1)

Face Parameters	
Face Recognition Threshold	85
Max Face Recognition Angle Deviation	30
Anti-spoofing Level	General >
Valid Face Interval (sec)	3
Invalid Face Interval (sec)	10
Recognition Distance	1.5 meters >
Mask mode	Not Detect >
Face Mask Threshold	75

Рисунок 4-21 Настройка параметров лица (2)

Snapshot Optimization	☐
Remove Duplicate Faces	☐
Face Similarity Sensitivity	85
Verify Face Image Quality	☒
Face Image Quality Sensitivity	60
Free Access with Face	☐
Face Snapshot Enhancement	☐
Beautifier	☐
Enable Helmet Detection	☐

4.7.3 Настройка параметров контроля доступа

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. В главном меню нажмите «Параметры контроля доступа» или выберите «Дополнительно» > «Контроль доступа» > «Параметры контроля доступа».

Шаг 3. Настройте основные параметры контроля доступа, а затем нажмите «Применить».

Рисунок 4-22 Параметры контроля доступа (1)

Name	Door1
Door Status	Normal >
Unlock Notifications Mode	Minimal Mode >
Verification Interval	0 s
Card Swiping Interval	0 s (0-86400)
Public Password	☐
Tamper Reset	☒
Lock 2	☐

Рисунок 4-23 Параметры контроля доступа (2)

Normally Open Period	
General Plan	Disabled >
Holiday Plan	Disabled >
Normally Closed Period	
General Plan	Disabled >
Holiday Plan	Disabled >

Рисунок 4-24 Параметры контроля доступа (3)

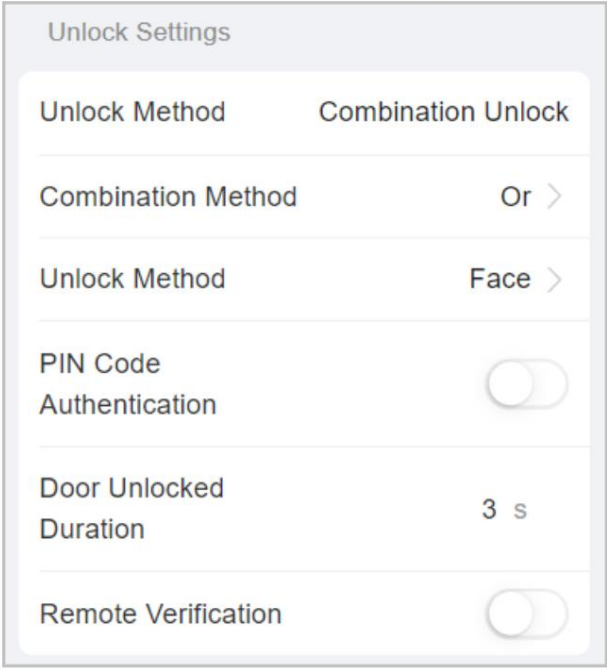


Таблица 4-7. Описание параметров контроля доступа.

Параметр		Описание
Основные настройки	Имя	Название двери.
	Состояние двери	Установите статус двери. • Нормальный режим: Дверь будет открыта и закрыта в соответствии с вашими настройками. • Всегда открыто: Дверь остается незапертой все время. • Всегда закрыто: Дверь остается запертой все время.
	Разблокировать уведомления Режим	Отображает уведомление на экране, когда пользователь подтверждает свою личность на устройстве. • Минимальный режим: система выводит на экран сообщение «Проверено успешно» или «Авторизация не выполнена» . • Простой режим: отображает идентификатор пользователя, имя и Время проверки после предоставления доступа. Отображается сообщение «Не авторизовано» и время авторизации после отказа в доступе. • Стандартный режим: отображает зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время проверки после предоставления доступа. Отображает сообщение « Не авторизовано» и время проверки после отказа в доступе. • Контрастный режим: отображает полученное изображение лица и зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время авторизации после предоставления доступа. Отображает сообщение «Доступ не авторизован» и время авторизации после отказа в доступе.

Параметр		Описание
	Интервал проверки	Если вы подтверждаете свою личность несколько раз в течение установленного периода, действительной будет считаться только самая ранняя проверка, и дверь не откроется после второй или последующих проверок. С момента, когда дверь не открывается, вам необходимо дождаться истечения заданного интервала времени проверки, прежде чем пытаться подтвердить свою личность снова.
	Проведение картой Интервал	При первой проверке с помощью карты вы, как правило, можете открыть дверь или отметить присутствие, и записи будут сгенерированы. В течение заданного периода, если вы повторно проведете картой для проверки, вы не сможете открыть дверь или отметить присутствие, и записи не будут сгенерированы. Пожалуйста, проверьте идентификацию по истечении заданного периода.  Интервал считывания карты имеет приоритет над интервалом проверки.
	Открытый пароль	После включения функции публичного пароля настройте пароль. Вы можете использовать публичный пароль для разблокировки двери без ввода идентификатора пользователя. Для одного устройства поддерживается только один публичный пароль.
	Сброс защиты от несанкционированного доступа	При включении этой функции можно восстановить заводские настройки с помощью кнопки защиты от взлома на задней панели устройства.
	Сброс защиты от несанкционированного доступа	После включения входной порт сигнализации будет переключен на порт датчика двери 2 и порт кнопки выхода 2.
Обычно открыто Период	Генеральный план/ План на отпуск	При выборе «Обычный» вы можете выбрать временной шаблон из выпадающего списка. Дверь остается открытой или закрытой в течение заданного времени. Подробную информацию о настройке общих планов и планов на праздничные дни см. в разделе «3.7.6 Настройка периодов».
Обычно закрыто Период	Генеральный план/ План на отпуск	 • Когда обычно открытый период конфликтует с - В период, обычно закрытый, период, обычно открытый, имеет приоритет над периодом, обычно закрытым. • В случае конфликта генерального плана с планом праздников, план праздников имеет приоритет над генеральным планом.
Разблокировать настройки	Способ разблокировки	Комбинированная разблокировка по умолчанию. Подробную информацию о других методах разблокировки см. в разделе "3.7.1.2 Настройка методов разблокировки".

Параметр		Описание
	Комбинация Метод	- Или: Воспользуйтесь одним из выбранных способов разблокировки, чтобы Откройте дверь. - И: Используйте все выбранные способы разблокировки, чтобы открыть дверь.
	Способ разблокировки	Способы разблокировки могут различаться в зависимости от модели продукта.
	ПИН-код Аутентификация	При включенной аутентификации по PIN-коду вы можете открыть дверь, используя только пароль.  Если эта функция включена, вводить идентификатор пользователя не требуется. Удалённая проверка не поддерживается.
	Дверь открыта Продолжительность	После того, как человеку будет предоставлен доступ, дверь останется открытой в течение определенного времени, чтобы он мог пройти. Его продолжительность варьируется от 0,2 до 600 секунд.
	Удалённая проверка. Откройте дверь дистанционно.	

Шаг 4. Нажмите «Применить».

4.7.4 Настройка сигналов тревоги

Сигнал тревоги сработает при возникновении нештатной ситуации доступа.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Контроль доступа > Сигнализация.

Шаг 3 (необязательно) Выберите направляющую двери.

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

Шаг 4. Настройте параметры сигнализации, а затем нажмите «Применить».

Рисунок 4-25. Настройки сигнализации.

Duress Alarm

Anti-passback

Door Detector

Door Detector Status

NO

Intrusion Alarm

Buzzer: Disabled

Disabled

Link Alarm Output: Disabled

Unlock Timeout Alarm

Buzzer: Disabled

Disabled

Link Alarm Output: Disabled

Excessive Attempts Alarm

Buzzer: Disabled

Enable

Link Alarm Output: Disabled

Tamper Alarm

Buzzer: Enable, Duration: 3 s

Enable

Link Alarm Output: Disabled

Apply

Таблица 4-8. Описание параметров аварийной сигнализации.

Параметр	Описание
Сигнал тревоги	Сигнализация сработает при срабатывании карты принудительного вызова. Для разблокировки двери используется пароль или отпечаток пальца принуждения.

229

Параметр	Описание
Защита от повторного прохода	Пользователи должны подтвердить свою личность как при входе, так и при выходе; в противном случае сработает сигнализация. Это помогает предотвратить передачу карты доступа другому лицу для входа. При включенной функции защиты от повторного прохода владелец карты должен покинуть охраняемую зону через считыватель на выходе, прежде чем система предоставит доступ другому лицу. - Если человек входит после получения разрешения, а выходит без разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен. - Если человек входит без разрешения и выходит после получения разрешения, при повторной попытке входа сработает сигнализация, и доступ будет запрещен.  Если к устройству можно подключить только один замок, проверка на самом устройстве по умолчанию означает направление входа, а проверка на внешнем считывателе карт — направление выхода. Вы можете изменить эту настройку на платформе управления.
Детектор двери	При подключении дверного датчика к вашему устройству сигнализация может срабатывать при ненормальном открытии или закрытии дверей. Существует два типа дверных датчиков: нормально замкнутый (NC) и нормально разомкнутый (NO) датчик. - NC: Датчик находится в замкнутом состоянии, когда дверь или Окно закрыто. - NET: Разомкнутая цепь образуется, когда окно или дверь фактически закрыты.
охранная сигнализация	Если дверь открывается ненормально, сработает охранная сигнализация, которая будет гореть в течение определенного времени.  Датчик открытия двери и система охранной сигнализации должны быть включены одновременно.
Сигнализация об истечении времени разблокировки	Если дверь остается незапертой дольше заданного времени, сработает сигнализация об истечении времени ожидания, которая будет действовать в течение заданного времени.
Тайм-аут разблокировки	 Датчик открытия двери и функция автоматического закрытия двери должны быть включены одновременно.
Сигнал тревоги о чрезмерном количестве попыток	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании неlegalной карты, которая будет гореть в течение определенного времени.
Сигнализация о несанкционированном доступе	Сигнализация о несанкционированном доступе срабатывает при нажатии кнопки защиты от взлома на устройстве.

4.7.5 Настройка связи между системами оповещения (необязательно)

Вы можете настроить связь между сигналами тревоги.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Контроль доступа > Настройка связи с сигнализацией.

Шаг 3. Выберите зону для настройки сигнализации.

Рисунок 4-26. Связь сигналов тревоги.

Alarm-in Port 1	
Name	Zone1
Alarm Input Type	NO >
Link Fire Safety Control	☐
Alarm-out Port ☐	
Duration	30 s
Alarm Output Channel	1 >
Access Control Linkage ☐	
Linkage Mode	Weak Execution >
When the heat alarm signal disappears, the door will automatically return to the normal authentication mode.	
Local Lock	NO >
External Lock	NO >

Шаг 4. Придумайте название для зоны тревоги.

Шаг 5. Включите функцию Link Fire Safety Control и выберите тип устройства ввода сигнала тревоги.

- NC: Вход сигнализации находится в нормально замкнутом (NC) состоянии, когда сигнал тревоги не сработал.
Сработала сигнализация. Размыкание нормально замкнутой цепи приводит к срабатыванию сигнализации.
- НЕТ: Когда сигнализация не сработала, входное устройство сигнализации находится в нормально разомкнутом (НО) состоянии. Замыкание цепи приводит к срабатыванию сигнализации.

Шаг 6. Если вы хотите связать управление доступом с срабатыванием пожарной сигнализации, включите функцию «Управление доступом». Связь.



Эта функция вступает в силу только после включения функции Link Fire Safety Control .

Шаг 7. Выберите режим соединения.

- Интенсивное выполнение: Когда сигнал пожарной тревоги исчезает, дверь остается в текущем состоянии. При желании вы можете вручную изменить ее состояние на предыдущее.
- Слабое выполнение: Когда сигнал пожарной тревоги исчезает, дверь автоматически возвращается в предыдущее состояние.

Шаг 8. Выберите тип блокировки: локальная или внешняя.

- НЕТ: Дверь автоматически открывается при срабатывании пожарной сигнализации.
- НЕТ: Дверь автоматически закрывается при срабатывании пожарной сигнализации.

Шаг 9. Нажмите OK.

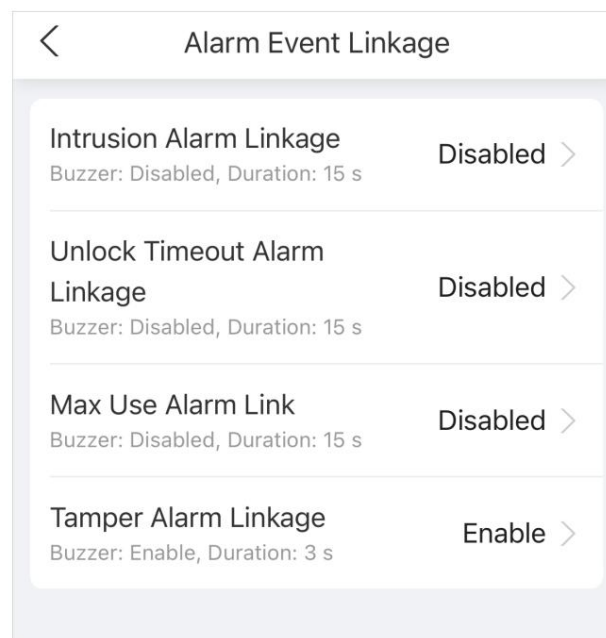
4.7.6 Настройка связи между событиями тревоги

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Контроль доступа > Связывание событий тревоги.

Рисунок 4-27. Связь событий тревоги.



Шаг 3. Коснитесь ссылки, чтобы настроить связь с тревожной системой, а затем нажмите OK.

Таблица 4-9. Связь событий тревоги.

Параметр	Описание
Связь с охранной сигнализацией	Если дверь откроется ненормально, сработает охранная сигнализация. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении вторжения. Вы можете настроить продолжительность сигнала тревоги. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает охранная сигнализация. Вы можете настроить продолжительность тревоги.
Сигнализация об истечении времени разблокировки Связь	Если дверь остается незапертой дольше заданного времени, сработает сигнализация об истечении времени ожидания, которая будет действовать в течение заданного времени. • Звуковой сигнал: Звуковой сигнал срабатывает при истечении времени ожидания разблокировки. Вы можете настроить продолжительность сигнала. ◇ Настраиваемое время: Настройте продолжительность. Контроллер доступа будет издавать звуковой сигнал в соответствии с заданным периодом. ◇ До тех пор, пока дверь не закроется: контроллер доступа будет издавать звуковой сигнал до тех пор, пока дверь не закроется. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнал тревоги об истечении времени разблокировки. Вы можете настроить продолжительность сигнала тревоги.
Ссылка на оповещение о максимальном использовании	Если неверный пароль или карта будут использованы 5 раз подряд в течение 60 секунд, сработает сигнализация о чрезмерном использовании нелегальной карты, которая будет гореть в течение определенного времени. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении чрезмерного использования. Длительность срабатывания сигнала можно настроить. • Выходной сигнал тревоги: Внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнал тревоги об истечении времени разблокировки. Вы можете настроить продолжительность сигнала тревоги.
Связь сигнализации о несанкционированном доступе	Сигнализация о попытке взлома срабатывает, когда кто-то пытается физически повредить устройство. • Звуковой сигнал: Звуковой сигнал срабатывает при обнаружении попытки взлома. Вы можете настроить продолжительность сигнала тревоги. • Выходной сигнал тревоги: внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнализация о несанкционированном доступе. Вы можете настроить продолжительность срабатывания сигнализации.

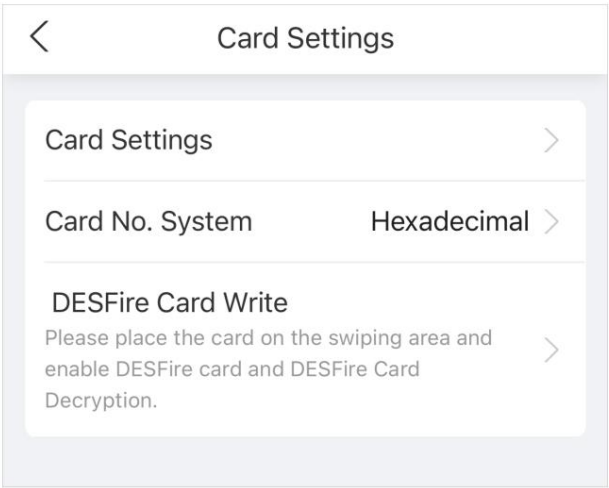
4.7.7 Настройка параметров карты

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Контроль доступа > Настройки карты.

Рисунок 4-28 Настройки карты



Шаг 3. Нажмите «Настройки карты» , настройте параметры карты, а затем нажмите «Применить».

Рисунок 4-29 Параметры карты

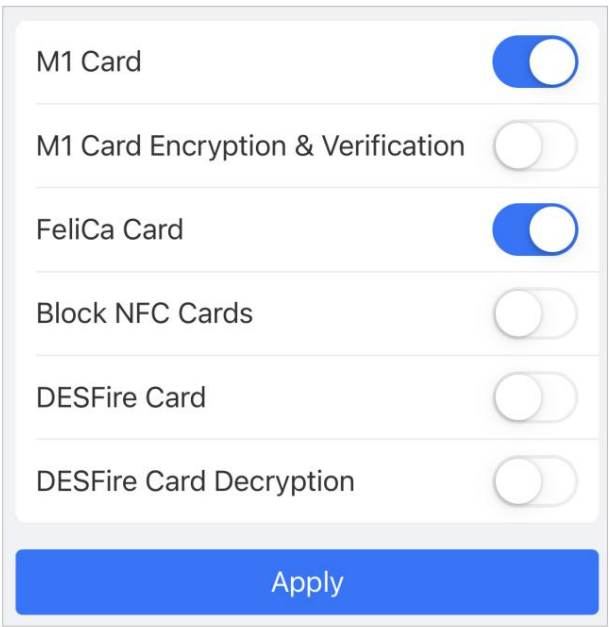


Таблица 4-10. Описание параметров карты.

Параметр	Описание
Карта M1	При включении этой функции карту M1 можно считать. Эта функция доступна только на некоторых моделях.
Шифрование и проверка карт M1	При включении этой функции можно считать только зашифрованную IC-карту. Убедитесь, что карта M1 активирована.

Параметр	Описание
FeliCa Card	При включении этой функции карту FeliCa можно считать.  Эта функция доступна только на некоторых моделях.
Удостоверение личности	При включении этой функции удостоверение личности можно считать.  Эта функция доступна только на некоторых моделях.
Блокировка NFC-карт	После включения этой функции разблокировка с помощью дубликата NFC-карты будет исключена.  • Эта функция доступна только в моделях, поддерживающих IC-карты. • Убедитесь, что карта M1 активирована. • Функция NFC доступна только на некоторых моделях телефонов.
Карта DESFire	При включении этой функции устройство может считывать номер карты DESFire.  • Эта функция доступна только в моделях, поддерживающих IC-карты. Поддерживается только шестнадцатеричный формат.
Расшифровка карты DESFire	Информация на карте DESFire может быть прочитана, если одновременно включены функции «Включить карту DESFire» и «Расшифровка карты DESFire».  • Эта функция доступна только в моделях, поддерживающих IC-карты. • Убедитесь, что карта DESFire включена.

Шаг 4. Нажмите «Система номеров карт», выберите формат, а затем нажмите «Применить».

При подключении считывателя карт Wiegand выберите десятичный или шестнадцатеричный формат для номера карты. Система нумерации карт одинакова как для ввода, так и для вывода номера карты.

Шаг 5. Нажмите кнопку «Записать на карту DESFire».

Поместите карту в считывающее устройство, введите номер карты, а затем нажмите кнопку «Записать», чтобы записать номер карты на карту.



• Необходимо включить функцию карты DESFire и функцию расшифровки карты DESFire. • Поддерживается только шестнадцатеричный формат. • Поддерживается до 8 символов.

4.7.8 Настройки конфиденциальности

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Дополнительно» > «Контроль доступа» > «Настройки конфиденциальности».

Шаг 3. Включите необходимую функцию.

- Снимок лица для проверки: изображения лиц будут автоматически считываться при разблокировке устройства. дверь.
- Снимок тревоги: При включении этой функции снимки будут создаваться при срабатывании сигнализации.
Обратная передача данных, принуждение, черный список и несанкционированные чрезмерные попытки. По умолчанию отключено.
- Сохранение лица на карту: После включения этой функции информация о лице сохраняется на картах, а не в устройстве. При подтверждении личности требуется провести картой по считывателю, чтобы сопоставить черты лица с данными на карте.



После включения этой функции, если вы просто зарегистрируете лицо и сохраните его на карте, вам потребуется добавить эту карту для обычного использования.

Шаг 4. Нажмите «Применить».

4.7.9 Настройка функций порта

Некоторые порты могут функционировать как разные порты, и вы можете настроить их на разные порты в зависимости от фактических потребностей.



- Эта функция доступна только на некоторых моделях.
- Расположение портов может отличаться в зависимости от модели изделия.

Процедура

Шаг 1. Войдите на веб-страницу.

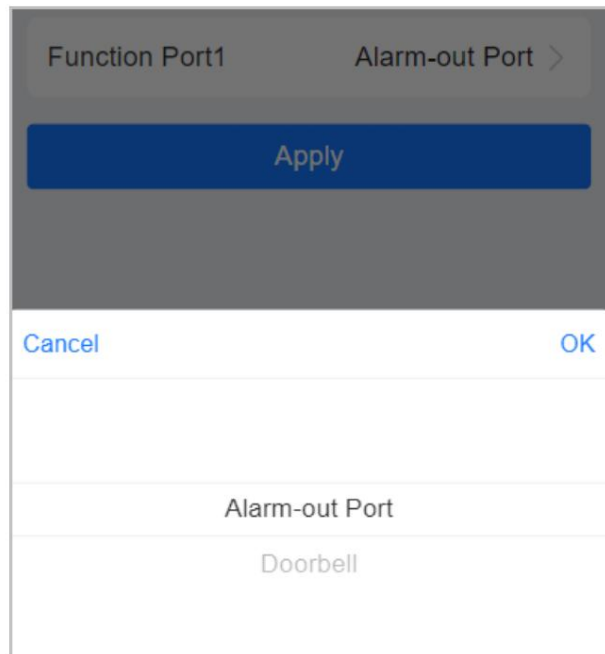
Шаг 2. Выберите Дополнительно > Контроль доступа > Настройка портов.

Шаг 3. Выберите тип порта.



Если кабель сигнализации и кабель дверного звонка используются совместно, настройте интерфейс на подключение к дверному звонку, чтобы гарантировать срабатывание звонка.

Рисунок 4-30. Настройка портов.



Шаг 4. Нажмите «Применить».

4.7.10 Настройка параметров экрана

Настройте период постоянного отображения экрана и информацию об устройстве, которая отображается на экране, когда тема оформления выбрана в режиме «Общий режим».

Процедура

Шаг 1. Войдите на веб-страницу.

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

Шаг 3. Настройте постоянно включенный экран и отображение информации.

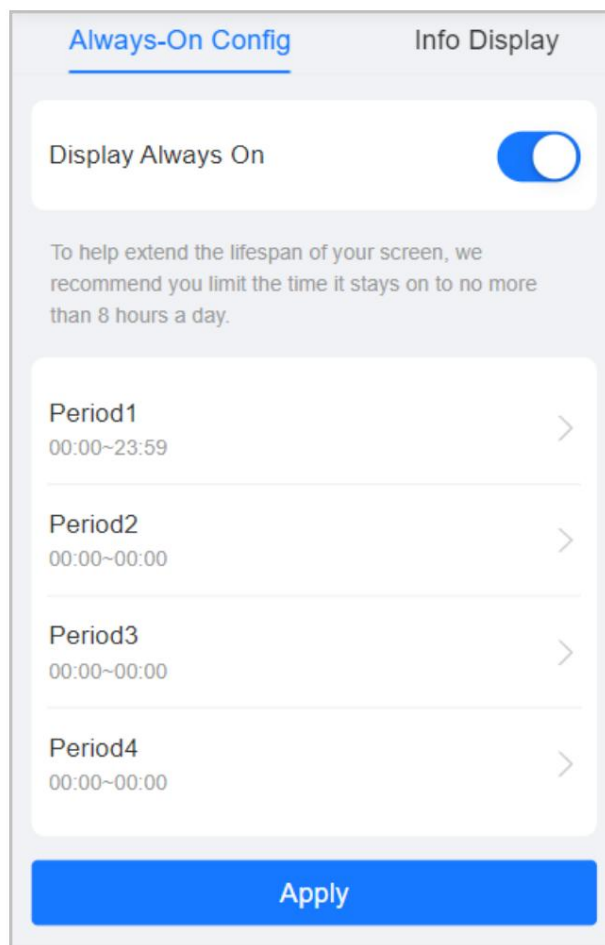
- Режим постоянной работы : экран всегда включен в течение заданного периода времени.

1. Нажмите «Настройка постоянной работы».
2. Включите функцию, а затем нажмите ОК.
3. Выберите период, укажите время начала и окончания, а затем нажмите ОК.
4. Нажмите «Применить».



Чтобы продлить срок службы экрана, мы рекомендуем ограничить время его работы до 8 часов в день.

Рисунок 4-31. Дисплей всегда включен.

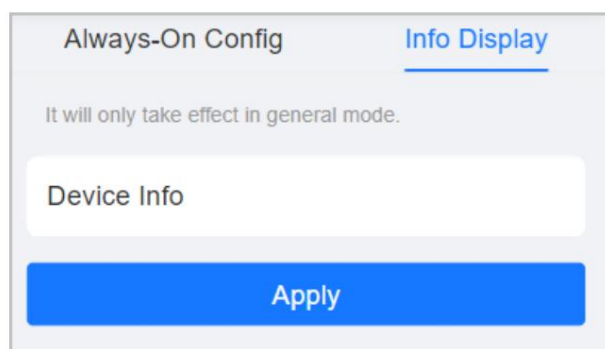


- Отображение информации : На странице «Персонализация > Реклама > Тема »

На компьютере, если вы выберете «Общий режим», информация о настроенном устройстве отобразится в правом верхнем углу главного экрана.

Нажмите «Информация на дисплее» , введите данные устройства, а затем нажмите «Применить».

Рисунок 4-32. Отображение информации.



4.8 Настройки связи

4.8.1 Настройка TCP/IP

Необходимо настроить IP-адрес устройства, чтобы обеспечить его связь с другими устройствами.

Процедура

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

Рисунок 4-33 TCP/IP

TCP/IP

NIC

NIC 1 >

Mode

Static >

MAC Address

IP Version

IPv4 >

* IP Address

* Subnet Mask

* Default Gateway

* Preferred DNS

* Alternate DNS

MTU

1500

Transmission Mode

Multicast >

Таблица 4-11. Описание TCP/IP.

Параметр	Описание
Режим	• Статический: Введите IP-адрес, маску подсети и шлюз вручную. • DHCP: Расшифровывается как Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста). При включении DHCP устройству автоматически будут присвоены IP-адрес, маска подсети и шлюз.
MAC-адрес	MAC-адрес устройства.
IP-версия	IPv4 или IPv6.

Параметр	Описание
IP-адрес	Если вы установите режим «Статический», настройте IP-адрес, маску подсети и шлюз.
Маска подсети	
Шлюз по умолчанию	 - IPv6-адрес представляется в шестнадцатеричном формате. • Для версий IPv6 не требуется установка масок подсети. - IP-адрес и шлюз по умолчанию должны совпадать. сегмент сети.
Предпочитаемый DNS	Укажите IP-адрес предпочтительного DNS-сервера.
Альтернативный DNS	Укажите IP-адрес альтернативного DNS-сервера.
MTU	MTU (Maximum Transmission Unit) — это максимальный размер данных, которые могут быть переданы в одном сетевом пакете в компьютерных сетях. По умолчанию он равен 1500.
Режим передачи	- Многоадресная рассылка: идеально подходит для видеозвонков. - Одноадресная передача: идеально подходит для групповых звонков.

4.8.2 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 сети Wi-Fi.



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

Шаг 4. Нажмите на Wi-Fi, а затем введите пароль.

Wi-Fi подключен.

Шаг 5 (необязательно) Добавьте Wi-Fi вручную.

Если сеть Wi-Fi не обнаружена, вы можете добавить её вручную.

- Нажмите «Добавить».
- Введите название и пароль сети Wi-Fi, а затем нажмите «Подключиться».

Результаты

После успешного подключения статус Wi-Fi отображается как «Подключено» .



Если подключены как Wi-Fi, так и проводная сеть, приоритет будет отдаваться Wi-Fi.

Связанные операции

Вы можете вручную изменить IP-адрес сети Wi-Fi.

- DHCP: Включите эту функцию и нажмите «Применить», устройству автоматически будет назначена сеть Wi-Fi. адрес.

- Статический режим: Включите эту функцию, вручную введите Wi-Fi-адрес, затем нажмите «Применить», и устройство подключится к Wi-Fi.

4.8.3 Настройка точки доступа Wi-Fi



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

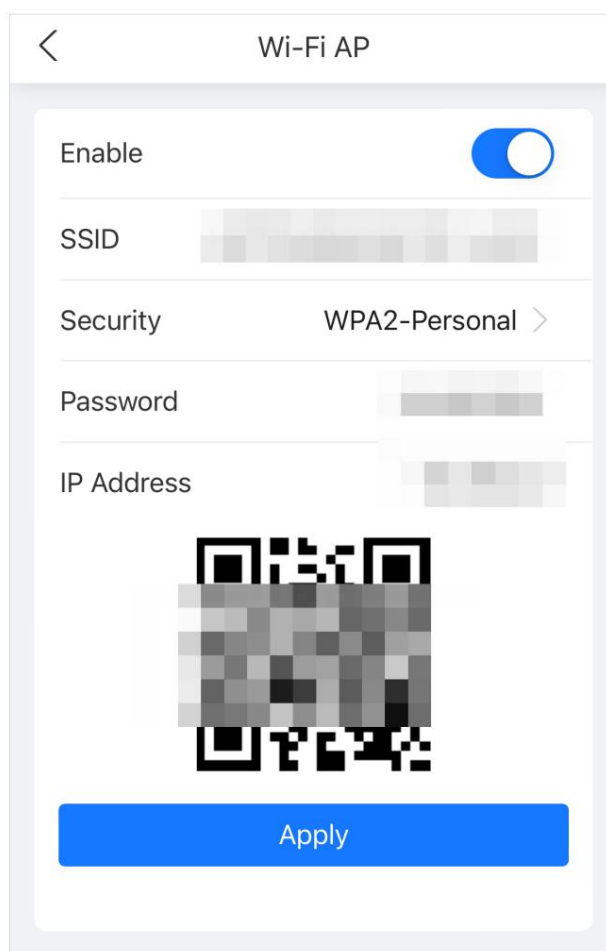
Процедура

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 4-34 Точка доступа Wi-Fi



4.8.4 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 становится доступным, если P2P-сети и PaaS-платформы подключены к сети.

Шаг 4. Нажмите «Применить».

4.8.5 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 4-35. Регистрация автомобиля.

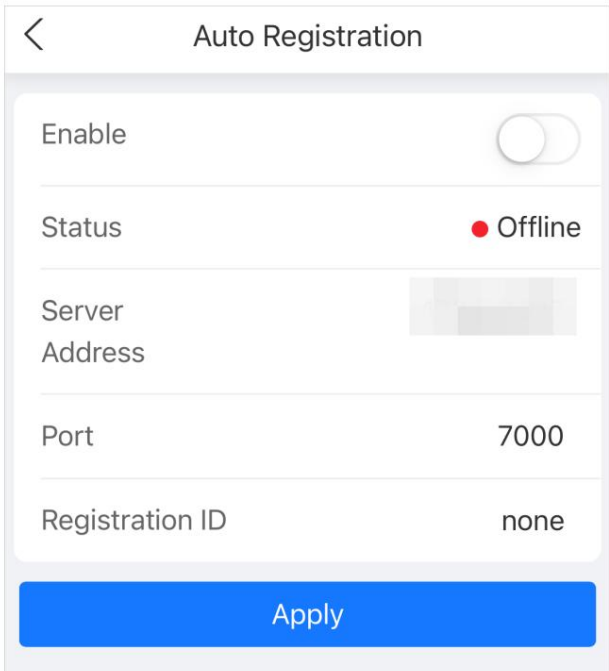


Таблица 4-12. Описание автоматической регистрации.

Параметр	Описание
Статус	Отображает статус подключения автоматической регистрации.
Адрес сервера	IP-адрес или доменное имя сервера.
Порт	Порт сервера, используемого для автоматической регистрации.
Идентификатор регистрации	Идентификатор регистрации устройства (определяемый пользователем). Добавление устройства в систему управления осуществляется путем ввода идентификатора регистрации на платформе.

4.8.6 Настройка Wiegand

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройки связи > Wiegand.

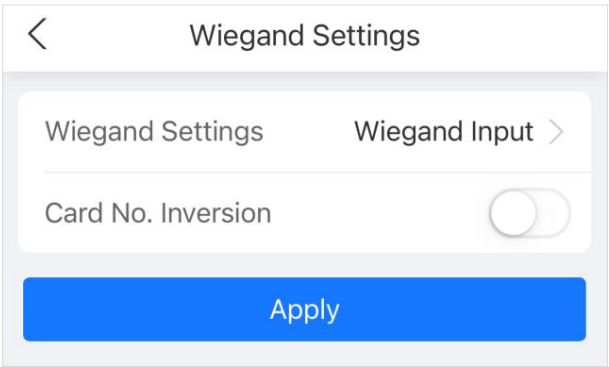
Шаг 3. Выберите тип Wiegand, настройте параметры, а затем нажмите «Применить».

- При подключении внешнего считывателя карт к устройству выберите вход Wiegand .



Если устройство подключается к стороннему устройству через входной порт Wiegand, и номер карты, считываемый устройством, отображается в обратном порядке по отношению к фактическому номеру карты, в этом случае можно включить функцию инверсии номера карты .

Рисунок 4-36. Вход Wiegand.



- Выберите выход Wiegand, если устройство функционирует как считыватель карт и вам необходимо подключить его к другому контроллеру доступа.

Рисунок 4-37. Выход Wiegand.

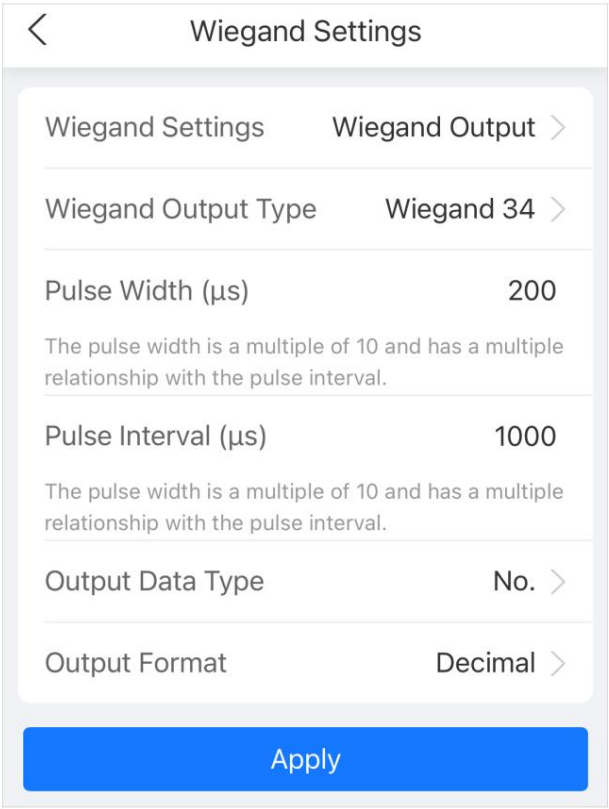


Таблица 4-13. Описание выходных данных Wiegand.

Параметр	Описание
Тип выходного сигнала Wiegand	Выберите формат Wiegand для считывания номеров карт или идентификационных номеров. ◇ Wiegand26 : считывает 3 байта или 6 цифр. ◇ Wiegand34 : Считывает 4 байта или 8 цифр. ◇ Wiegand66 : Считывает 8 байтов или 16 цифр.
Ширина импульса	Введите ширину импульса и интервал между импульсами на выходе Wiegand.
Интервал пульта	
Тип выходных данных	Выберите тип выходных данных. ◇ Нет.: Выводит данные на основе идентификатора пользователя. Формат данных — шестнадцатеричный или десятичный. ◇ Номер карты : Выводит данные на основе первого номера карты пользователя.

4.8.7 Настройка RS-485

Настройте параметры RS-485, если вы подключаете внешнее устройство к порту RS-485.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройки связи > Настройки RS-485.

Шаг 3. Настройте параметры, а затем нажмите «Применить».

Параметры могут различаться в зависимости от типа внешнего устройства. На следующем рисунке в качестве примера используется контроллер доступа .

Рисунок 4-38 Настройки RS-485

RS-485 Settings

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 >

Apply

Таблица 4-14. Настройка параметров RS-485.

Параметр	Описание
Внешнее устройство	• Контроллер доступа Выберите «Контроллер доступа», если устройство функционирует как считыватель карт и отправляет данные другим внешним контроллерам доступа для управления доступом. Тип выходных данных: ◇ Номер карты : Передайте номер карты контроллеру доступа для аутентификации и разблокировки двери. Если номер карты, переданный этим устройством, совпадает с номером карты в контроллере доступа, аутентификация контроля доступа считается успешной. ◇ Нет. : Передайте идентификатор пользователя контроллеру доступа для аутентификации и разблокировки двери. Если идентификатор пользователя, переданный этим устройством, совпадает с идентификатором пользователя в контроллере доступа, аутентификация контроля доступа считается успешной. • Считыватель карт: Устройство функционирует как контроллер доступа и подключается к внешнему считывателю карт. • Считыватель (OSDP): Устройство подключается к считывателю карт на основе протокола OSDP. • Модуль безопасности управления дверью: После включения модуля безопасности кнопка выхода, замок и функция пожарной сигнализации не работают. • Турникет: Когда устройство подключается к турникету, происходит доступ. Контроллерная плата турникета подключается к внешнему модулю QR-кода или модулю считывания карт, после чего плата передает данные для проверки на турникет. • Режим расширения замка: Если контроллер доступа подключен к внешнему модулю расширения замка и выбран режим «Модуль расширения замка», локальный замок разблокируется после подтверждения идентификации на локальном устройстве, а дополнительный замок — после подтверждения идентификации на внешнем считывателе карт. После выбора модуля расширения замка вы можете выбрать канал 2 на странице «Параметры контроля доступа и сигналы тревоги» на веб-странице контроллера доступа. • Запасная батарея: Устройство подключается к запасной батарее, и текущий уровень заряда батареи отображается в процентах.  Запасной аккумулятор поддерживается только на некоторых моделях.
Бит данных	Количество бит, используемых для передачи фактических данных в последовательном канале связи. Это двоичные цифры, несущие передаваемую информацию.
Стоп Бит	После данных передается бит, а также необязательные биты четности, указывающие на конец передачи данных. Это позволяет приемнику подготовиться к передаче следующего байта данных и обеспечивает синхронизацию в протоколе связи.
Код четности	После битов данных отправляется дополнительный бит для обнаружения ошибок передачи. Он помогает проверить целостность передаваемых данных, обеспечивая наличие определенного количества логических старших или младших битов.

4.8.8 Настройка Bluetooth

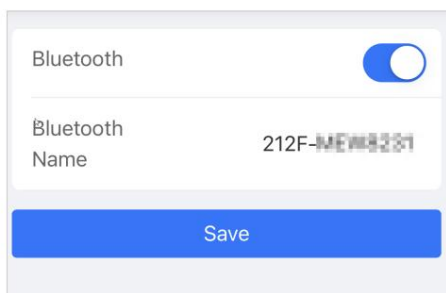
Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Связь» > «Настройки Bluetooth».

Шаг 3. Включите или выключите Bluetooth.

Рисунок 4-39 Bluetooth



Шаг 4. Нажмите «Сохранить».

Результаты

Дверь можно разблокировать через Bluetooth с помощью приложения DMSS.

4.9 Настройка аудиоподсказок

Настройте звуковые подсказки во время подтверждения личности.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Настройки аудио и видео > Аудио.

Шаг 3. Настройте параметры звука, а затем нажмите «Применить».

Рисунок 4-40. Настройка параметров звука.

Device Volume80
Only enter a multiple of 10.

Intercom Volume80
Only enter a multiple of 10.

Microphone Volume90
Only enter a multiple of 10.

Key Sound

Audio CollectionEnable >

DND Mode

DND Mode

Apply

Таблица 4-15. Описание параметров.

Параметры	Описание
Объем устройства	Регулируйте громкость динамика, когда устройство не находится в режиме внутренней связи.
Громкость домофона	Отрегулируйте громкость динамика, когда устройство находится в режиме внутренней связи.
Громкость микрофона	Установите громкость микрофона.
Ключевой звук	При включении этой функции сенсорные устройства будут выдавать Звук касания и устройства без сенсорного экрана будут имитировать касание мыши. звук.
Аудиоколлекция	Если эта функция включена, звук из микрофона устройства будет Запись производилась в режиме реального времени и во время видеозаписи.
Режим «Не беспокоить»	В течение установленного времени при подтверждении вашей учетной записи голосовые подсказки не звучат. Идентификатор устройства. Можно установить до 4 периодов.

4.10 Журналы просмотров

Просматривайте журналы, такие как системные журналы, записи о разблокировке и журналы тревожных сигналов.

4.10.1 Системные журналы

Просмотр и поиск системных журналов.

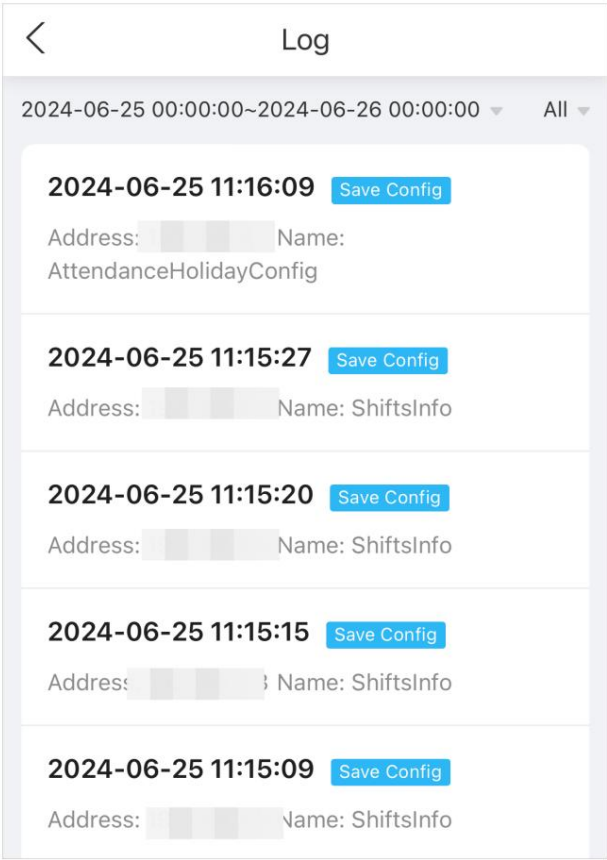
Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Журнал > Журнал.

Шаг 3. Выберите время и тип записи.

Рисунок 4-41. Журналы



4.10.2 Разблокировка записей

Найдите записи о разблокировке.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Дополнительно» > «Журнал» > «Разблокировать записи».

Шаг 3. Выберите время и тип записи.

Шаг 4. Нажмите на запись, чтобы просмотреть подробности.

4.10.3 История звонков

Найдите историю звонков.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Журнал > История звонков.

4.10.4 Журналы аварийных сигналов

Просмотреть журналы тревожных сообщений.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Дополнительно > Журнал > Журнал тревог.

Шаг 3. Выберите время и тип записи.

5 конфигураций Smart PSS Lite

В этом разделе описывается, как управлять устройством и настраивать его с помощью Smart PSS Lite. Подробную информацию см. в руководстве пользователя Smart PSS Lite.

5.1 Установка и вход в систему

Установите и войдите в Smart PSS Lite. Подробную информацию см. в руководстве пользователя Smart PSS Lite.

Процедура

Шаг 1. Получите программный пакет Smart PSS Lite у службы технической поддержки, а затем установите и запустите программное обеспечение в соответствии с инструкциями.

Шаг 2 При первом входе в систему выполните инициализацию Smart PSS Lite, включая установку пароля и контрольных вопросов.



Установите пароль для первого использования, а затем настройте контрольные вопросы для сброса пароля в случае его забвения.

Шаг 3. Введите ваше имя пользователя и пароль для входа в Smart PSS Lite.

5.2 Добавление устройств

Необходимо добавить устройство в Smart PSS Lite. Добавлять их можно группами или по отдельности.

5.2.1 Добавление устройств по одному

Вы можете добавлять устройства по одному, вводя их IP-адреса или доменные имена.

Процедура

Шаг 1. На странице «Диспетчер устройств» нажмите «Добавить».

Шаг 2. Настройте параметры устройства.

Рисунок 5-1. Добавление устройств.

Add Device

Device Name:

*

Method to add:

IP/Domain

IP/Domain:

*

Port:

*

37777

User Name:

*

Password:

*

Add and Continue

Add

Cancel

Таблица 5-1. Параметры добавления IP-блоков.

Параметр	Описание
Название устройства	Для удобства идентификации рекомендуем присваивать устройствам названия, указывающие на зону наблюдения.
Способ добавления	Выберите IP-адрес/домен. • IP/Домен: Введите IP-адрес или доменное имя устройства. • SN: Введите серийный номер устройства.
Порт	Введите номер порта; по умолчанию это 37777. Фактический номер порта может отличаться в зависимости от модели.
Имя пользователя	Введите имя пользователя устройства.
Пароль	Введите пароль устройства.

Шаг 3. Нажмите «Добавить».

Вы можете нажать «Добавить и продолжить» , чтобы добавить больше устройств.

5.2.2 Добавление устройств партиями

Справочная информация



- Мы рекомендуем добавлять устройства с помощью автоматического поиска, если вам необходимо добавлять устройства партиями в пределах одного сетевого сегмента или если сетевой сегмент известен, но точные IP-адреса устройств неизвестны.
- Закрывайте ConfigTool и DSS при настройке устройств; в противном случае вы можете не найти нужное устройство. все устройства.

Процедура

Шаг 1. На странице «Диспетчер устройств» нажмите «Автопоиск».

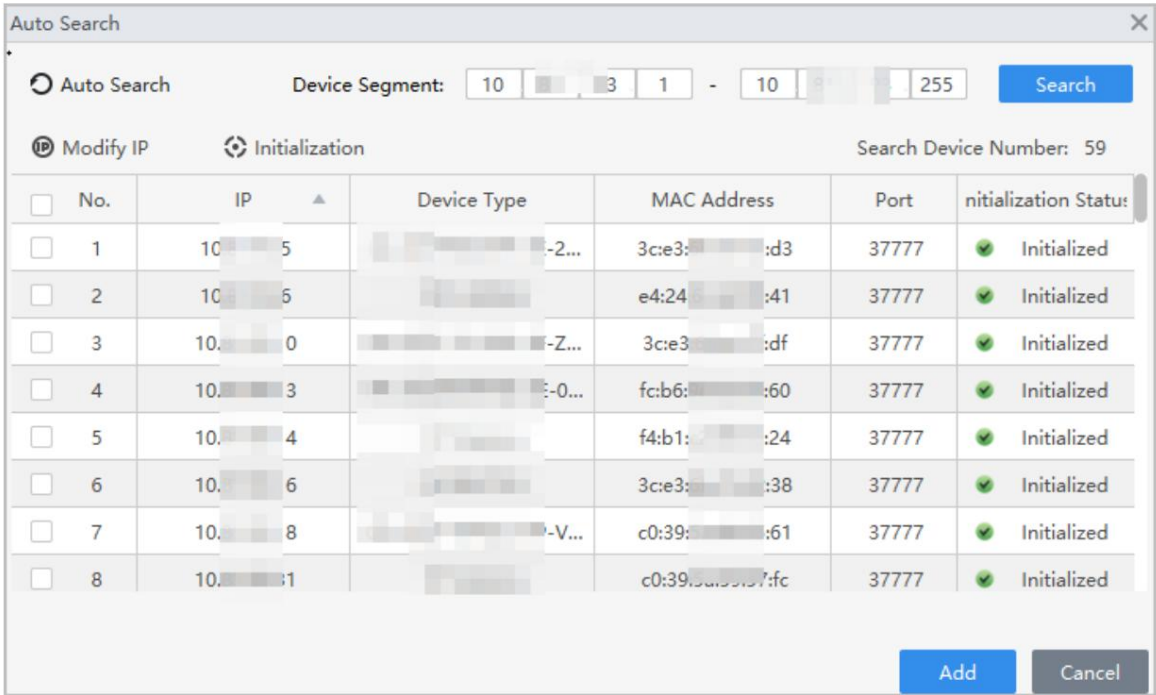
Шаг 2. Выберите метод поиска.

- Автоматический поиск: Введите имя пользователя и пароль устройства. Система автоматически выполнит поиск устройств, находящихся в той же сети, что и ваш компьютер.
- Поиск по сегменту устройства: Введите имя пользователя и пароль устройства, а затем укажите начальный и конечный IP-адреса. Система автоматически выполнит поиск устройств в этом диапазоне IP-адресов.



Вы можете выбрать оба метода, чтобы система автоматически искала устройства как в сети, к которой подключен ваш компьютер, так и в других сетях.

Рисунок 5-2. Поиск устройств.



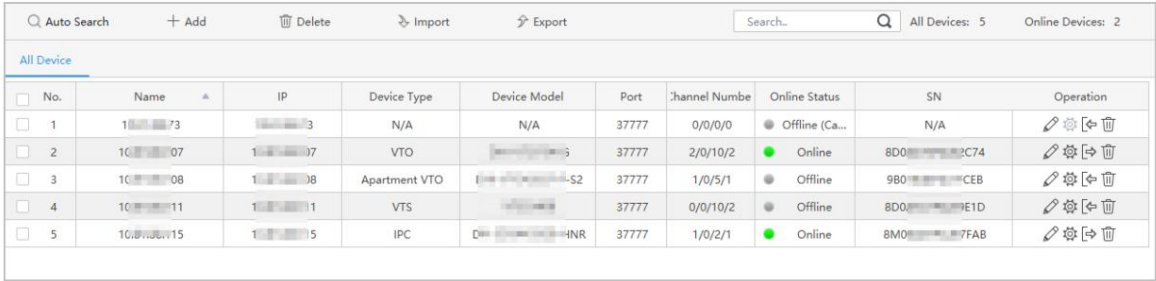
Шаг 3. Нажмите «Устройства», а затем нажмите «Добавить».

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

Результаты

После успешного добавления устройства отображаются на этой странице.

Рисунок 5-3. Добавленные устройства.



5.3 Управление пользователями

Добавляйте пользователей, назначайте им карточки и настраивайте их права доступа.

5.3.1 Настройка типа карты

Перед назначением карт пользователям необходимо указать их тип. Например, если назначенная карта является удостоверением личности, установите тип карты на «Удостоверение личности».

Процедура

Шаг 1. Войдите в Smart PSS Lite.

Шаг 2. Щелкните «Доступ к решению» > «Менеджер по персоналу» > «Пользователь».

Шаг 3. В поле «Тип выпуска карты» выберите тип карты.



Убедитесь, что тип карты совпадает с фактически выданной картой; в противном случае номер карты не будет считан.

Шаг 4. Нажмите ОК.

5.3.2. Увеличение штата сотрудников

5.3.2.1 Пополнение персонала по одному человеку

Процедура

Шаг 1. Выберите «Персонал» > «Управление персоналом», а затем нажмите «Добавить».

Шаг 2. Введите основные данные о сотрудниках.

1. Нажмите вкладку «Основная информация».

2. Добавьте основную информацию о персонале.

3. Нажмите «Сделать снимок» или «Загрузить изображение», чтобы установить фотографию профиля.

4. Настройте проверку личности.

• Установите пароль.

Нажмите «Добавить», чтобы добавить пароль.



◇ Для устройств второго поколения установите личный пароль; для устройств более ранних поколений установите пароль карты.

◇ Новый пароль должен состоять из 6–8 цифр. • Настройте

карты.

а. Щелкните , чтобы выбрать Устройство или Эмитент карты в качестве считывателя карт.

б. Нажмите «Добавить», чтобы добавить карточки, а затем нажмите

«ОК». с. Управляйте карточками.

◇ Нажмите  или , чтобы установить карту в качестве основной или принудительной.

◇ Нажмите , чтобы изменить номер карты.

◇ Нажмите , чтобы удалить карту.

◇ Нажмите , чтобы отобразить QR-код карты.



QR-код карты может отображаться только при вводе 8-значного номера карты в шестнадцатеричном формате.

- Настройте отпечатки пальцев.
 - а. Щелкните, чтобы выбрать «Устройство» или «Сканер отпечатков пальцев» в качестве устройства для сбора отпечатков пальцев.
 - б. Добавьте отпечатки пальцев.

Выберите «Добавить» > «Добавить отпечаток пальца», а затем трижды подряд приложите один из пальцев к сканеру.

Рисунок 5-4. Добавьте основную информацию.

Add User

Basic Info

More Info

Person ID:

*

1

Name:

*

Department:

Default Company

Person Type:

Normal User

Effective Time:

2024/8/28 0:00:00

2034/8/28 23:59:59

3653 Day

Times Used:

Unlimited

Profile Picture

Take Snapshot

Upload Picture

Image size: 0-100 KB

Face1

Take Snapshot

Upload Picture

Image size: 0-100 KB

Face2

Take Snapshot

Upload Picture

Image size: 0-100 KB

Password

Add

For the second-generation access control device, it is the person password.

Otherwise it is the card password.

Card

Add

The card number must be added if non-2nd generation access controller is used.

Fingerprint

+

Add

Delete

☐	Fingerprint Name	Operation

Palm Vein

+

Add

Delete

☐	HandPrint Name	Operation

Add More

Complete

Cancel

Шаг 3. Нажмите вкладку «Подробнее», чтобы добавить дополнительную информацию о персонале.

Рисунок 5-5. Добавьте дополнительную информацию.

Add User

Basic Info

More Info

Details

Gender: ☒ Male ☐ Female

Credential Type: ID Card

Title: Mr.

Credential No.:

Date of Birth: 1985/3/15

Organization:

Phone No.:

Occupation:

Email:

Employment Date: 2024/8/27 15:33:56

Communication A...

Termination Date: 2034/8/28 15:33:56

Admin: ☒

Remarks:

Add More

Complete

Cancel

Шаг 4. Нажмите «Завершить».

Связанные операции

- Нажмите  Изменить информацию или добавить дополнительные сведения в список персонала.
- Нажмите  Удалить всю информацию о персонале.
- Нажмите  чтобы заблокировать карты, после чего их нельзя будет использовать в обычном режиме.
- Нажмите  чтобы разблокировать карты, после чего их можно будет использовать в обычном режиме.

5.3.2.2 Набор персонала партиями

Процедура

- Шаг 1. Выберите «Персонал» > «Управление персоналом».
- Шаг 2. Нажмите «Пакетное обновление», а затем «Пакетное добавление».
- Шаг 3. Выберите тип устройства, а затем установите начальное количество и число карт.
- Шаг 4. Укажите отдел, срок действия и срок истечения действия карт.
- Шаг 5. Нажмите «Прочитать номер карты».
- Шаг 6. Поместите карты в устройство для выдачи карт или в устройство для считывания карт.

Номера карт будут считаны или заполнены автоматически.

Шаг 7. Нажмите OK.

Рисунок 5-6. Добавление персонала партиями.

5.3.3 Назначение прав доступа

Создайте группу разрешений, представляющую собой набор прав доступа к дверям, а затем свяжите пользователей с этой группой, чтобы они могли разблокировать двери, связанные с этой группой разрешений.

Процедура

Шаг 1. Нажмите «Доступ к решению» > «Менеджер по персоналу» > «Разрешения».

Шаг 2. Нажмите  .

Шаг 3. Введите название группы, примечания (необязательно) и выберите временной шаблон.

Шаг 4. Выберите методы проверки и двери.

Шаг 5. Нажмите OK.

Рисунок 5-7. Создание группы разрешений.

The screenshot shows the 'Add Permission Group' dialog box. On the left, a table lists existing permission groups. The dialog itself has a 'Related Information' tab and a 'Basic Info' section. Numbered callouts indicate the following steps:

- Click the '+' icon to add a new group.
- Enter a 'Group Name' (e.g., 'Permission Group4') and a 'Remark'.
- Select a 'Time Template' (e.g., 'Full-day Time Te').
- Select verification methods: Card, Fingerprint, Password, and Face.
- Select devices from the 'All Device' list (e.g., 'Door 1').
- Click the 'OK' button to save the group.

Шаг 6. Щелкните по группе разрешений.

Шаг 7. Выберите пользователей, чтобы связать их с группой разрешений.

Рисунок 5-8. Добавление пользователей в группу разрешений.

The screenshot shows the 'Add Person' dialog box. On the left, a table lists existing permission groups. The dialog has a 'Permission Group1' section and a 'User List' section. Numbered callouts indicate the following steps:

- Click the '+' icon to add a new user.
- Select users from the 'User List' (e.g., 'Default Company(2)', 'Mary', 'Tom').
- Click the 'OK' button to save the users.

Шаг 8. Нажмите OK.

Пользователи, входящие в эту группу разрешений, могут разблокировать дверь после подтверждения личности.

5.3.4 Назначение прав доступа к отметкам о посещении

Создайте группу разрешений, которая будет представлять собой набор прав доступа к учету рабочего времени, а затем свяжите сотрудников с этой группой, чтобы они могли отмечать время прихода и ухода с помощью определенных методов проверки.

Процедура

Шаг 1. Войдите в систему Smart PSS Lite.

Шаг 2. Щелкните «Решение доступа» > «Менеджер по персоналу» > «Настройка разрешений».

Шаг 3. Нажмите.  .

Шаг 4. Введите название группы, примечания (необязательно) и выберите временной шаблон.

Шаг 5. Выберите устройство контроля доступа.

Шаг 6. Нажмите ОК.

Рисунок 5-9. Создание группы разрешений.

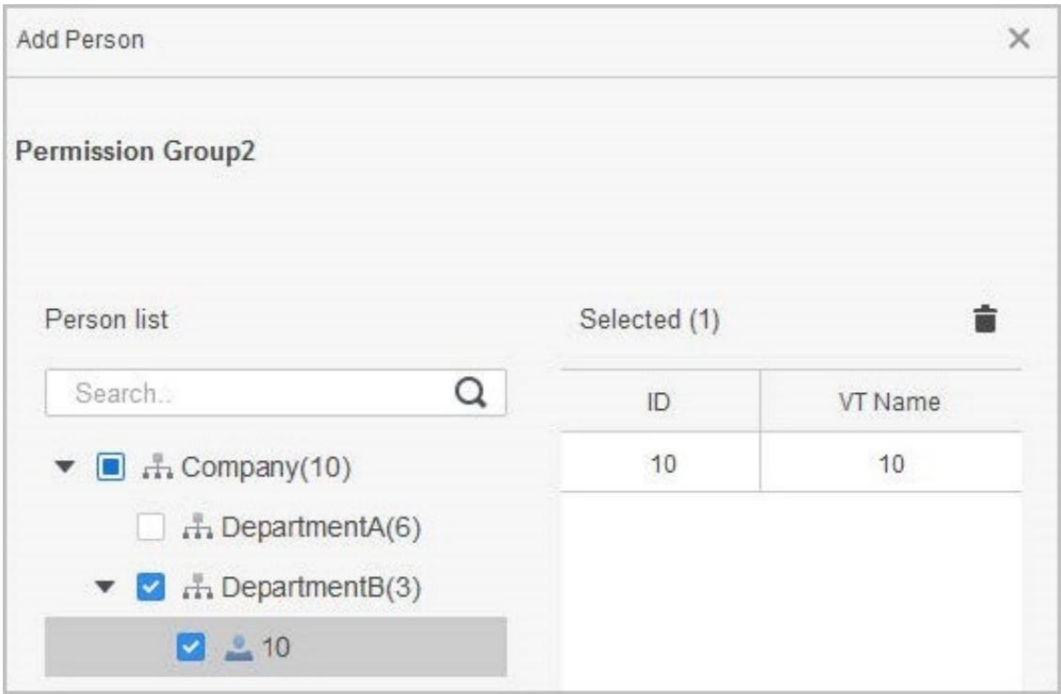


- Система учета рабочего времени поддерживает регистрацию прихода/ухода с помощью пароля, а также распознавание лиц.
Система учета рабочего времени по картам и отпечаткам пальцев.
- На некоторых моделях доступна система учета рабочего времени с использованием карт и отпечатков пальцев.

Шаг 7. Щелкните по добавленной вами группе разрешений.

Шаг 8. Выберите пользователей, чтобы связать их с группой разрешений.

Рисунок 5-10. Добавление пользователей в группу разрешений.



Шаг 9. Нажмите OK.

5.4 Управление доступом

5.4.1 Дистанционное открывание и закрывание двери

С помощью платформы вы можете удаленно контролировать и управлять дверью. Например, вы можете дистанционно открывать или закрывать дверь.

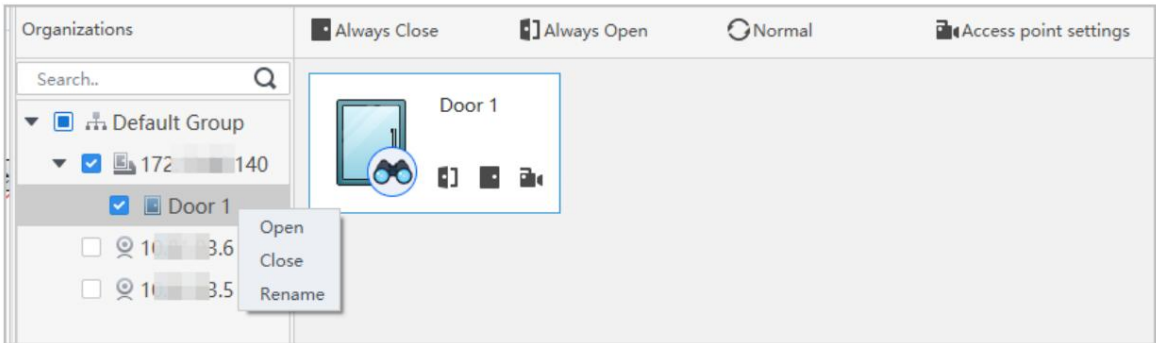
Процедура

Шаг 1. На главной странице нажмите «Решение Access» > «Менеджер Access» .

Шаг 2. Дистанционное управление дверью.

- Выберите дверь, щелкните правой кнопкой мыши и выберите «Открыть» или «Заккрыть» , чтобы открыть или закрыть дверь.

Рисунок 5-11 Открытая дверь



- : Откройте или закройте дверь.
- : Просмотрите видео с двери в режиме реального времени.

Связанные операции

- Фильтрация событий: выберите тип события в разделе «Информация о событии», и в списке событий отобразятся выбранные события.
Тип события, например, тревожные события и нештатные ситуации. • Блокировка

обновления событий: Нажмите  Чтобы заблокировать список событий, после этого обновление списка событий прекратится. Нажмите  разблокировать.

- Удаление событий: Нажмите , чтобы удалить все события из списка.

5.4.2 Настройка «Всегда открыто» и «Всегда закрыто»

После установки параметра "всегда открыта" или "всегда закрыта" дверь остается открытой или закрытой постоянно.

Процедура

Шаг 1 На главной странице нажмите «Решение Access» > «Менеджер Access» .

Шаг 2 Нажмите «Всегда открыто» или «Всегда закрыто» , чтобы открыть или закрыть дверь.

Рисунок 5-12. Всегда открыто или закрыто.



Дверь будет оставаться открытой или закрытой постоянно. Вы можете нажать кнопку «Нормальный» , чтобы восстановить нормальный режим работы системы контроля доступа, после чего дверь будет открываться или закрываться в зависимости от настроенных методов проверки.

5.4.3 Мониторинг состояния двери

Процедура

Шаг 1. На главной странице нажмите «Решение Access» > «Менеджер Access» .

Шаг 2. Выберите устройство в дереве устройств, щелкните по нему правой кнопкой мыши и выберите «Запустить Real-».

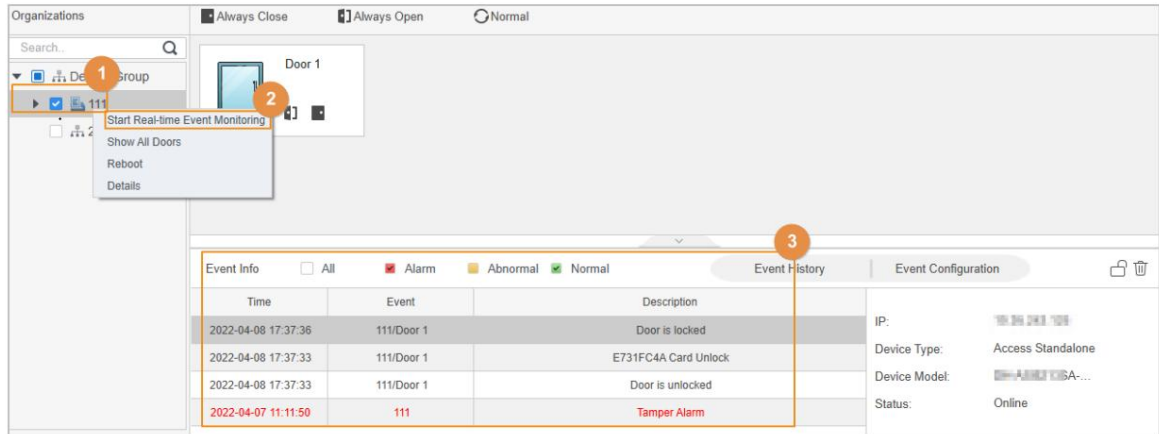
Мониторинг событий по времени.

События контроля доступа в режиме реального времени будут отображаться в списке событий.



Нажмите кнопку «Остановить мониторинг», и события контроля доступа в реальном времени отображаться не будут.

Рисунок 5-13. Состояние двери монитора.



Связанные операции • Показать

все двери: Отображает все двери, управляемые устройством. • Перезагрузка:

Перезапускает устройство.

• Подробная информация: Просмотр сведений об устройстве, таких как IP-адрес, модель и состояние.

Приложение 1. Важные особенности лица. Регистрация

Перед регистрацией

- Очки, головные уборы и борода могут повлиять на эффективность распознавания лиц. • Не закрывайте брови, когда носите головной убор. • Не меняйте сильно форму бороды во время использования устройства; в противном случае распознавание лиц может быть нарушено.

неудача.

- Держите лицо в чистоте. •

Держите устройство на расстоянии не менее 2 метров от источника света и не менее 3 метров от других источников света. окна или двери; в противном случае подсветка и прямые солнечные лучи могут повлиять на эффективность распознавания лиц контроллером доступа.

Во время регистрации

- Вы можете зарегистрировать лица через устройство или через платформу. Для регистрации через
 - Расположите голову по центру рамки для фотосъемки. Будет сделано фотоизображение лица. автоматически.



- Не трясите головой или телом, иначе регистрация может не удался. • Избегайте одновременного появления двух лиц в кадре.

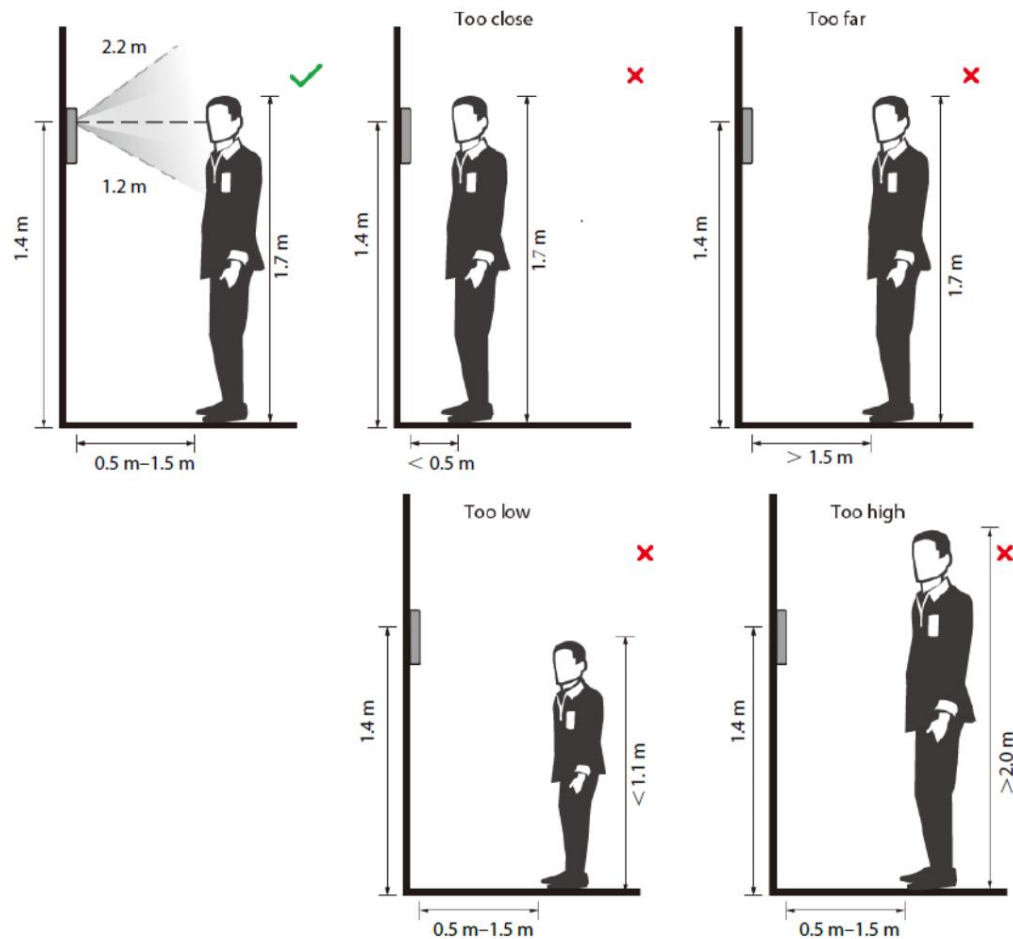
Положение лица

Если ваше лицо находится не в правильном положении, точность распознавания лиц может снизиться.



Положение лица, показанное ниже, приведено только для справки и может отличаться от фактического.

Приложение, Рисунок 1-1. Правильное положение лица.



Требования к лицам

- Убедитесь, что лицо чистое, а лоб не закрыт волосами. • Не носите очки, шляпы, густую бороду или другие украшения для лица, которые влияют на внешний вид лица. запись.
- Смотрите на экран с открытыми глазами, без мимики, и направьте лицо в центр камеры. • При записи лица или распознавании лиц не располагайте лицо слишком близко или слишком далеко от камеры.

Приложение, Рисунок 1-2. Положение головы.



Приложение, Рисунок 1-3 Расстояние между гранями



- При импорте изображений лиц через платформу управления убедитесь, что изображение разрешение находится в диапазоне от 150 × 300 пикселей до 600 × 1200 пикселей. Рекомендуется, чтобы разрешение было больше 500 × 500 пикселей, размер изображения был меньше 100 КБ, а имя изображения и идентификатор человека совпадали.
- Убедитесь, что лицо занимает более 1/3, но не более 2/3 всей площади изображения, а соотношение сторон не превышает 1:2.

Приложение 2. Важные моменты внутренней связи. Операция

Устройство может функционировать как VTO для реализации функции внутренней связи.

Предварительные требования

Функция внутренней связи настраивается на устройстве.

Процедура

Шаг 1. На экране ожидания коснитесь . 

Шаг 2. Введите номер комнаты, а затем нажмите 

Приложение 3. Важные моменты, касающиеся отпечатков пальцев.

Инструкции по регистрации

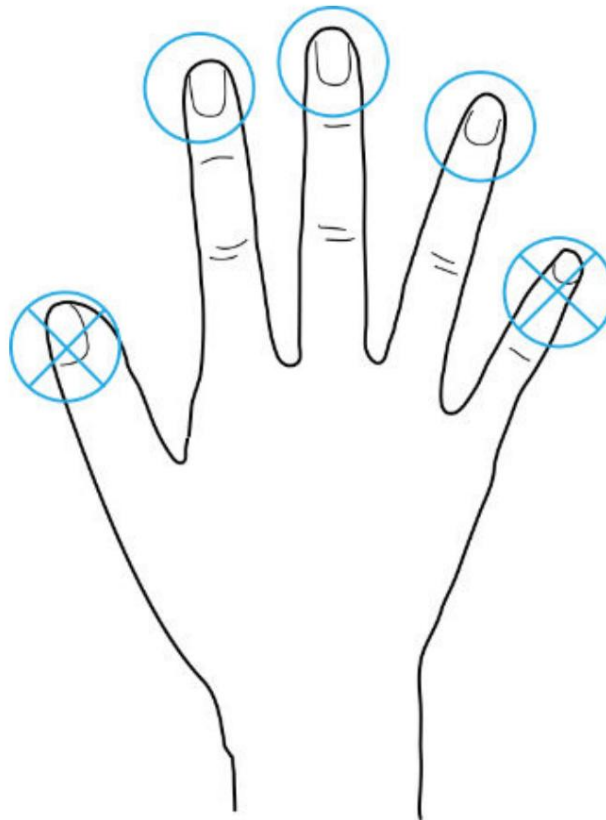
При регистрации отпечатков пальцев обратите внимание на следующие моменты:

- Убедитесь, что ваши пальцы и поверхность сканера чистые и сухие.
- Прижмите палец к центру сканера отпечатков пальцев.
- Не размещайте датчик отпечатков пальцев в местах с интенсивным освещением, высокой температурой и высокой температурой. влажность.
- Если отпечатки пальцев нечеткие, используйте другие способы разблокировки.

Рекомендуется использовать пальцы.

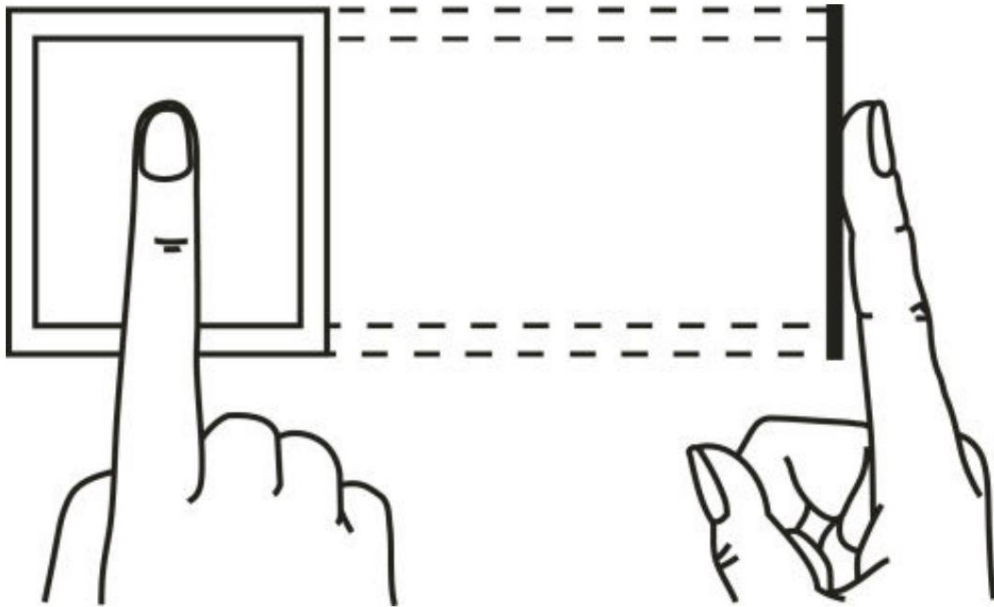
Рекомендуется использовать указательные, средние и безымянные пальцы. Большие пальцы и мизинцы будет сложно разместить в центре записи.

Приложение, Рисунок 3-1. Рекомендуемые пальцы.

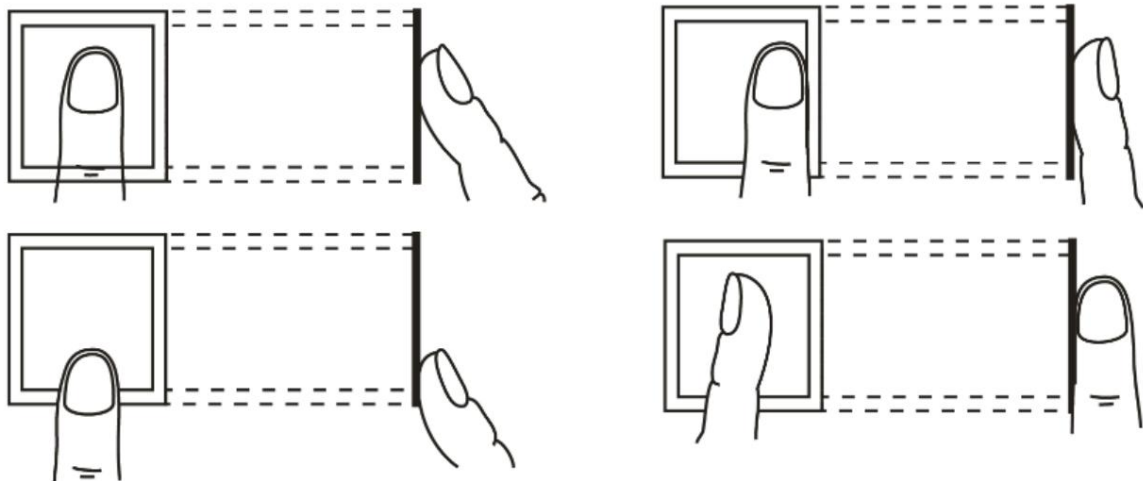


Как приложить отпечаток пальца к сканеру

Приложение, Рисунок 3-2. Правильное размещение.



Приложение, Рисунок 3-3. Неправильное размещение.



Приложение 4. Важные моменты, касающиеся QR-кода.

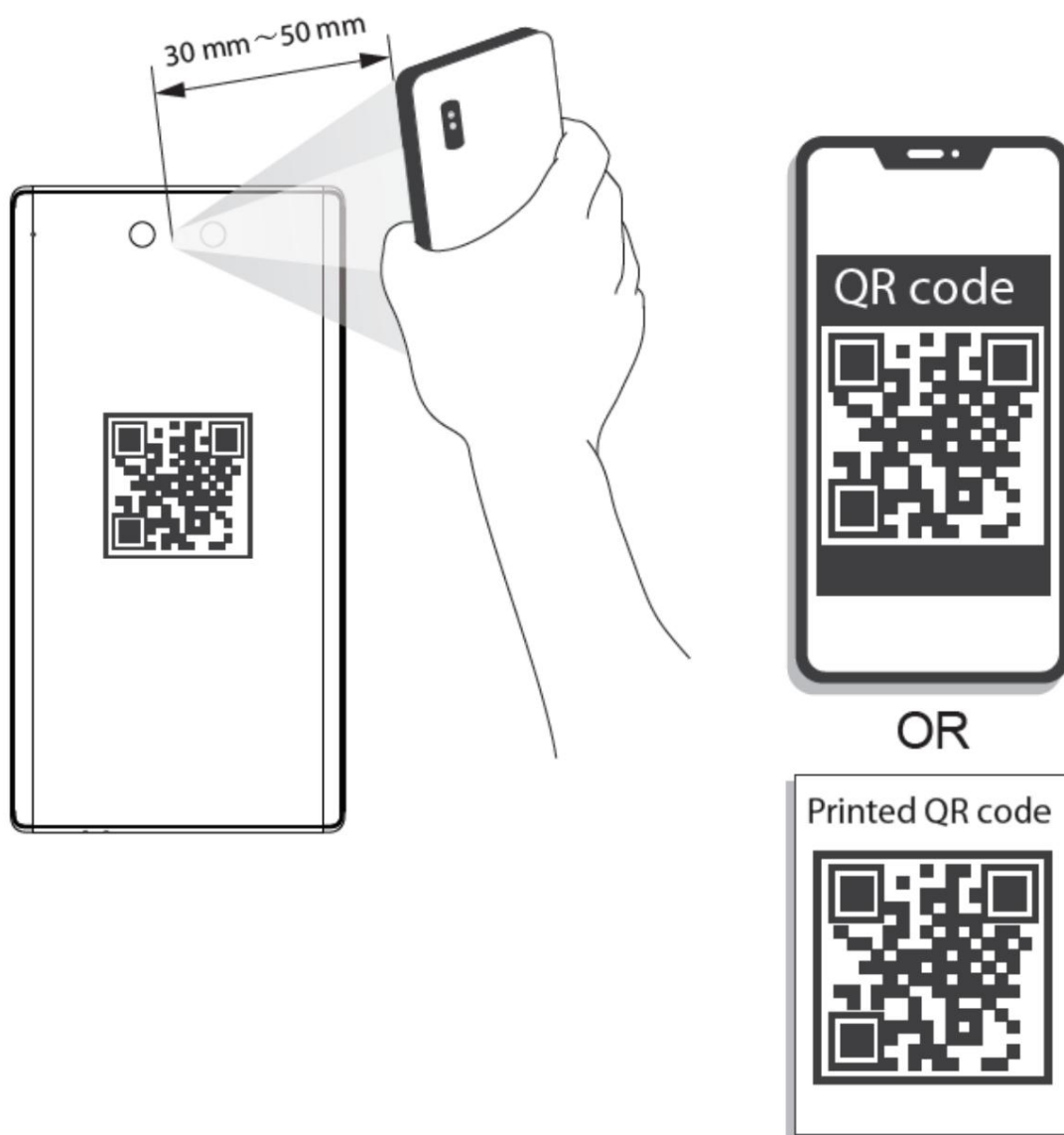
Сканирование

Разместите QR-код на телефоне на расстоянии 30–50 мм от сканирующего объектива. Поддерживаются QR-коды размером более 30 мм × 30 мм и размером менее 128 байт.



- Расстояние обнаружения QR-кода зависит от количества байтов и размера QR-кода. • Убедитесь, что QR-код выровнен относительно объектива, и избегайте попадания прямых солнечных лучей.

Приложение, Рисунок 4-1. Сканирование QR-кода.



Приложение 5. Рекомендации по безопасности.

Управление учетными записями

1. Используйте сложные пароли.

Для установки паролей воспользуйтесь следующими рекомендациями:

- Длина не должна быть меньше 8 символов;
- Включать как минимум два типа символов: прописные и строчные буквы, цифры и символы;
- Не содержать название счета или название счета в обратном порядке;
- Не использовать непрерывные символы, такие как 123, abc и т. д.;
- Не использовать повторяющиеся символы, такие как 111, aaa и т. д.

2. Периодически меняйте пароли.

Рекомендуется периодически менять пароль устройства, чтобы снизить риск его угадывания или взлома.

3. Распределите учетные записи и права доступа надлежащим образом.

Добавляйте пользователей в соответствии с требованиями к обслуживанию и управлению и назначайте им минимальные наборы прав доступа.

4. Включите функцию блокировки учетной записи.

Функция блокировки учетной записи включена по умолчанию. Рекомендуется оставить ее включенной 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 для сброса пароля.

Устройство поддерживает функцию сброса пароля. Чтобы снизить риск использования этой функции злоумышленниками, при изменении информации, пожалуйста, своевременно вносите необходимые корректировки. При настройке контрольных вопросов рекомендуется не использовать легко угадываемые ответы.

Конфигурация службы

1. Включите HTTPS.

Рекомендуется включить протокол HTTPS для доступа к веб-сервисам через защищенные каналы.

2. Зашифрованная передача аудио и видео.

Если ваши аудио- и видеоданные очень важны или конфиденциальны, рекомендуется использовать функцию зашифрованной передачи, чтобы снизить риск перехвата ваших аудио- и видеоданных во время передачи.

3. Отключите некритичные службы и используйте безопасный режим.

Если в этом нет необходимости, рекомендуется отключить некоторые службы, такие как SSH, SNMP, SMTP, UPnP, точки доступа и т. д., чтобы уменьшить поверхность атаки.

При необходимости настоятельно рекомендуется выбирать безопасные режимы, включая, помимо прочего, следующие сервисы:

- SNMP: Выберите SNMP v3 и настройте надежное шифрование и пароли аутентификации.
- SMTP: Выберите TLS для доступа к серверу почтовых ящиков.
- FTP: Выберите SFTP и настройте сложные пароли.
- Точка доступа: Выберите режим шифрования WPA2-PSK и настройте сложные пароли.

4. Измените порты HTTP и других служб по умолчанию.

Рекомендуется изменить порт по умолчанию для HTTP и других служб на любой порт в диапазоне от 1024 до 65535, чтобы снизить риск его подбора злоумышленниками.

Сетевая конфигурация

1. Включить список разрешенных .

Рекомендуется включить функцию списка разрешенных IP-адресов и разрешить доступ к устройству только IP-адресам из этого списка. Поэтому обязательно добавьте IP-адрес вашего компьютера и IP-адрес совместимого устройства в список разрешенных.

2. Привязка MAC-адреса

Рекомендуется привязать IP-адрес шлюза к MAC-адресу устройства, чтобы снизить риск подмены ARP-адреса.

3. Создайте безопасную сетевую среду.

Для повышения уровня безопасности устройств и снижения потенциальных киберрисков рекомендуется следующее:

- Отключите функцию переадресации портов маршрутизатора, чтобы избежать прямого доступа к устройствам внутренней сети из внешней сети;
- Разделите сеть в соответствии с фактическими потребностями: если между двумя подсетями нет потребности в обмене данными, рекомендуется использовать VLAN, шлюзы и другие методы для разделения сети с целью достижения сетевой изоляции;
- Внедрить систему аутентификации доступа 802.1x для снижения риска несанкционированного доступа терминалов к частной сети.

Аудит безопасности

1. Проверьте пользователей сети.

Рекомендуется регулярно проверять пользователей в сети, чтобы выявлять нелегальных пользователей.

2. Проверьте журнал устройства.

Просмотрев журналы, вы можете узнать об IP-адресах, которые пытались войти в систему устройства, и о ключевых операциях авторизованных пользователей.

3. Настройка сетевого журнала

Из-за ограниченной емкости памяти устройств объем сохраняемых журналов ограничен. Если вам необходимо сохранять журналы в течение длительного времени, рекомендуется включить функцию сетевого журнала, чтобы обеспечить синхронизацию важных записей с сервером сетевого журнала для трассировки.

Безопасность программного обеспечения

1. Своевременно обновляйте прошивку.

В соответствии со стандартными отраслевыми требованиями, для обеспечения актуальности функций и безопасности устройства необходимо своевременно обновлять его прошивку до последней версии. Если устройство подключено к общедоступной сети, рекомендуется включить функцию автоматического обнаружения онлайн-обновлений, чтобы своевременно получать информацию об обновлениях прошивки, выпущенных производителем.

2. Своевременно обновляйте клиентское программное обеспечение.

Рекомендуется загрузить и использовать последнюю версию клиентского программного обеспечения.

Физическая защита

Рекомендуется обеспечить физическую защиту устройств (особенно устройств хранения данных), например, разместить устройство в специально отведенном машинном помещении и шкафу, а также установить систему контроля доступа.

а также внедрена система управления ключами для предотвращения повреждения оборудования и других периферийных устройств (например, USB-накопителей, последовательных портов) посторонними лицами.