

Контроллер доступа с распознаванием лиц Web 5.0

Руководство пользователя



V1.2.2

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.

Инструкции по технике безопасности

В руководстве могут встречаться следующие сигнальные слова.

Сигнальные слова	Значение:
 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.
 ESD	Электростатически чувствительные устройства. Указывает на устройство, чувствительное к электростатическому разряду.
 ELECTRIC SHOCK	Указывает на опасно высокое напряжение. Будьте осторожны, избегайте контакта с электричеством.
 LASER RADIATION	Указывает на опасность лазерного излучения. Будьте осторожны и избегайте воздействия лазерного луча.
 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
V1.2.2	Обновлены настройки прав доступа к учету посещаемости.	Июнь 2024 г.
V1.2.1	Обновлены настройки домофона, настройки контроля доступа и более.	Май 2024 г.
V1.2.0	Обновлены настройки связи, параметры 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 или оператор данных, вы можете собирать персональные данные других лиц, такие как их лицо, аудиозаписи, отпечатки пальцев и номерные знаки автомобилей. Вам необходимо соблюдать местные законы и правила защиты конфиденциальности, чтобы защитить законные права и интересы других людей, внедряя меры, которые включают, помимо прочего: предоставление четкой и видимой идентификации для информирования людей о наличии зоны видеонаблюдения и предоставление необходимой контактной информации.

О руководстве пользователя

- Данное руководство носит исключительно справочный характер. Между руководством и другими документами могут быть обнаружены незначительные различия. продукт.

- Мы не несем ответственности за убытки, понесенные в результате эксплуатации продукта способами, не предусмотренными законом.

- Соблюдение требований руководства. •

Руководство будет обновляться в соответствии с последними законами и нормативными актами соответствующих юрисдикций.

Для получения подробной информации см. бумажное руководство пользователя, воспользуйтесь нашим CD-ROM, отсканируйте QR-код или посетите наш официальный сайт. Руководство предназначено только для ознакомления. Между электронной и бумажной версиями могут быть незначительные различия.

- Все дизайнерские решения и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта.

Возможно, будут некоторые расхождения между фактическим продуктом и руководством. Пожалуйста, свяжитесь со службой поддержки клиентов для получения последней версии программы и дополнительной документации. • Возможны ошибки в печати или расхождения в описании

функций, операций и технических данных. В случае возникновения каких-либо сомнений или споров мы оставляем за собой право окончательного толкования.

- Если руководство (в формате PDF) не открывается, обновите программное обеспечение для чтения или попробуйте другое распространенное

программное обеспечение для чтения. • Все товарные знаки, зарегистрированные товарные знаки и названия компаний, упомянутые в руководстве, являются собственностью их владельцев.

соответствующих владельцев.

- В случае возникновения каких-либо проблем, пожалуйста, посетите наш веб-сайт, свяжитесь с поставщиком или службой поддержки клиентов. с использованием

устройства. • В случае возникновения каких-либо неясностей или разногласий мы оставляем за собой право окончательного разъяснения.

Важные меры предосторожности и предупреждения

В этом разделе представлена информация о правильном обращении с устройством, предотвращении опасностей и предотвращении повреждения имущества. Внимательно прочтите перед использованием устройства и соблюдайте инструкции по его использованию.

Требования к транспорту



Транспортировка, использование и хранение устройства должны осуществляться в пределах допустимых условий влажности и температуры.

Требования к хранению



Храните устройство в условиях допустимой влажности и температуры.

Требования к установке



- Не подключайте адаптер питания к устройству, когда адаптер включен. • Строго соблюдайте местные правила и стандарты электробезопасности. Убедитесь, что напряжение окружающей среды соответствует нормам. Стабильна и соответствует требованиям к электропитанию устройства.
- Не подключайте устройство к двум или более типам источников питания во избежание его повреждения. Устройство.
- Неправильное использование батареи может привести к возгоранию или взрыву. • Пожалуйста, соблюдайте требования к электропитанию устройства.
- ◇ Ниже приведены требования к выбору адаптера питания. • Источник питания должен соответствовать требованиям IEC 60950-1 и IEC 62368-1. стандарты.
- Напряжение должно соответствовать требованиям SELV (Safety Extra Low Voltage) и не превышать стандарты ES-1.
- Если мощность устройства не превышает 100 Вт, блок питания должен соответствовать требованиям LPS и быть не выше PS2.
- ◇ Мы рекомендуем использовать адаптер питания, входящий в комплект поставки устройства.
- ◇ При выборе адаптера питания необходимо учитывать требования к источнику питания (например, номинальное напряжение), указанные на этикетке устройства.



- Персонал, работающий на высоте, должен принимать все необходимые меры для обеспечения личной безопасности, включая ношение каски и страховочных ремней.
- Не размещайте устройство в местах, подверженных воздействию солнечных лучей или вблизи источников тепла. • Берегите устройство от влаги, пыли и саж. • Установите устройство на устойчивую поверхность, чтобы предотвратить его падение. • Установите устройство в хорошо проветриваемом месте и не препятствуйте его вентиляции.

- Используйте адаптер или блок питания, предоставленный производителем. • Используйте сетевые кабели, рекомендованные для данного региона и соответствующие номинальной мощности.

технические характеристики.

- Устройство относится к электроприборам класса I. Убедитесь, что источник питания устройства соответствует требованиям. подключено к розетке с защитным заземлением.

Эксплуатационные требования



- Перед использованием проверьте правильность подключения блока питания. • Перед включением устройства заземлите его на защитный контакт. • Не отключайте шнур питания сбоку устройства, пока адаптер включен. • Эксплуатируйте устройство в пределах номинального диапазона входной и выходной мощности. • Используйте устройство при допустимых условиях влажности и температуры. • Не допускайте попадания жидкости на устройство и убедитесь, что на нем нет предметов, наполненных жидкостью.

- Не разбирайте устройство без инструкции специалиста. •

Данное изделие является профессиональным оборудованием. •

Устройство не подходит для использования

в местах, где могут находиться дети.

Оглавление

Предисловие.....	Я
Важные меры предосторожности и предупреждения.....	III
1 Обзор.....	1
2 Локальные операции.....	2
2.1 Основная процедура настройки.....	2
2.2 Общие значки.....	2
2.3 Экран ожидания.....	3
2.4 Инициализация.....	4
2.5 Вход в систему.....	4
2.6 Сброс пароля.....	5
2.7 Способы разблокировки.....	6
2.7.1 Разблокировка с помощью карт.....	6
2.7.2 Разблокировка по лицу.....	6
2.7.3 Разблокировка по паролю пользователя.....	6
2.7.4 Разблокировка по паролю администратора.....	6
2.7.5 Разблокировка по QR-коду.....	6
2.7.6 Разблокировка по отпечатку пальца.....	7
2.7.7 Разблокировка с помощью временного пароля.....	7
2.8 Управление пользователями.....	7
2.8.1 Добавление пользователей.....	7
2.8.2 Просмотр информации о пользователях.....	10
2.8.3 Настройка пароля разблокировки администратора.....	11
2.9 Управление контролем доступа.....	11
2.9.1 Настройка метода разблокировки.....	11
2.9.2 Настройка сигнализации.....	14
2.9.3 Настройка состояния двери.....	16
2.9.4 Настройка интервала времени проверки.....	16
2.10 Управление посещаемостью.....	17
2.10.1 Настройка отделов.....	17
2.10.2 Настройка смен.....	18
2.10.3 Настройка планов работы в праздничные дни.....	20
2.10.4 Настройка графиков работ.....	21
2.10.5 Настройка режимов учета посещаемости.....	24
2.11 Настройки связи.....	27
2.11.1 Настройка сети.....	27
2.11.2 Настройка последовательного порта.....	30
2.11.3 Настройка Wiegand.....	32

2.12 Системные настройки.....	33	2.12.1
Настройка времени.....	33	2.12.2 Настройка параметров интерфейса.....
Настройка громкости.....	35	2.12.3 Настройка
Настройка языка.....	38	2.12.4 Настройка языка.....
Настройки экрана.....	38	2.12.5 Настройки экрана.....
(Необязательно) Настройка параметров отпечатка пальца.....	39	2.12.6
Восстановление заводских настроек.....	39	2.12.7
Перезагрузка устройства.....	39	2.12.8
2.13 Настройки функций.....	39	
2.14 Управление USB-устройствами.....	43	
Экспорт на USB-накопитель.....	43	2.14.1
Импорт с USB-накопителя.....	43	2.14.2
Обновление системы.....	43	2.14.3
2.15 Управление документацией.....	44	
2.16 Информация о системе.....	44	2.16.1 Объем данных для просмотра.....
Версия устройства просмотра.....	44	2.16.2
3 Веб-операции.....	45	
Инициализация.....	45	
Вход в систему.....	45	3.2
Сброс пароля.....	46	3.3
Главная страница.....	46	
Управление персоналом.....	47	
Настройка контроля доступа.....	51	
Настройка параметров контроля доступа.....	51	3.6.1
Настройка сигналов тревоги.....	55	3.6.2
Настройка связи сигналов тревоги (необязательно).....	57	3.6.3
Настройка связи событий тревоги.....	58	3.6.4
Настройка распознавания лиц.....	59	3.6.5
Настройка параметров карты.....	63	3.6.6
Настройка QR-кода.....	65	3.6.7
Настройка расписаний.....	66	3.6.8
Настройка конфиденциальности.....	68	3.6.9
Настройка модулей расширения.....	68	3.6.10
Настройка функций портов.....	69	3.6.11
Настройка сравнения бэкэндов.....	69	3.6.12
3.7 Настройка внутренней связи.....	70	
Использование устройства в качестве SIP-сервера.....	70	3.7.1
Использование VTO в качестве SIP-сервера.....	78	3.7.2

3.7.3 Использование платформы в качестве SIP-сервера.....	80
3.7.4 Простой режим.....	83
3.8 Настройка учета посещаемости.....	85
3.8.1 Настройка отделов.....	85
3.8.2 Настройка смен.....	85
3.8.3 Настройка праздничных дней.....	88
3.8.4 Настройка графиков работы.....	88
3.8.5 Настройка режимов учета рабочего времени.....	91
3.9 Настройка аудио и видео.....	93
3.9.1 Настройка видео.....	93
3.9.2 Настройка звуковых подсказок.....	101
3.9.3 Настройка обнаружения движения.....	102
3.9.4 Настройка локального кодирования.....	103
3.10 Настройки связи.....	104
3.10.1 Сетевые настройки.....	104
3.10.2 Настройка RS-485.....	114
3.10.3 Настройка Wiegand.....	116
3.11 Настройка системы.....	117
3.11.1 Управление пользователями.....	117
3.11.2 Настройка времени.....	120
3.11.3 Настройка сочетаний клавиш.....	122
3.12 Персонализация.....	124
3.12.1 Добавление ресурсов.....	124
3.12.2 Настройка тем.....	125
3.13 Центр управления.....	128
3.13.1 Диагностика одним щелчком мыши.....	128
3.13.2 Информация о системе.....	129
3.13.3 Объем данных.....	129
3.13.4 Журналы просмотра.....	129
3.13.5 Управление конфигурацией.....	131
3.13.6 Техническое обслуживание.....	132
3.13.7 Обновление системы.....	132
3.13.8 Расширенное техническое обслуживание.....	133
3.14 Настройки безопасности (необязательно)	133
3.14.1 Состояние безопасности.....	133
3.14.2 Настройка HTTPS.....	134
3.14.3 Атака Защита.....	135
3.14.4 Установка сертификата устройства.....	138
3.14.5 Установка сертификата доверенного центра сертификации.....	141
3.14.6 Шифрование данных.....	142

3.14.7 Предупреждение о безопасности.....	143
3.14.8 Аутентификация безопасности.....	143
4 Настройка Smart PSS Lite.....	145
4.1 Установка и вход в систему.....	145
4.2 Добавление устройств.....	145
4.2.1 Добавление устройств по одному.....	145
4.2.2 Добавление устройств партиями.....	146
4.3 Управление пользователями.....	148
4.3.1 Настройка типа карты.....	148
4.3.2 Добавление пользователей.....	148
4.3.3 Назначение прав доступа.....	153
4.3.4 Назначение прав на учет посещаемости.....	154
4.4 Управление доступом.....	156
4.4.1 Дистанционное открывание и закрывание двери.....	156
4.4.2 Настройка «Всегда открыто» и «Всегда закрыто».....	157
4.4.3 Мониторинг состояния двери.....	157
Приложение 1 Важные моменты распознавания лиц.....	159
Приложение 2 Важные моменты работы домофона.....	162
Приложение 3 Важные моменты регистрации отпечатков пальцев Инструкции.....	163
Приложение 4. Важные моменты сканирования QR-кода.....	165
Приложение 5 Рекомендации по безопасности.....	166

1. Обзор

Устройство представляет собой панель контроля доступа, поддерживающую 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. Оно 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.

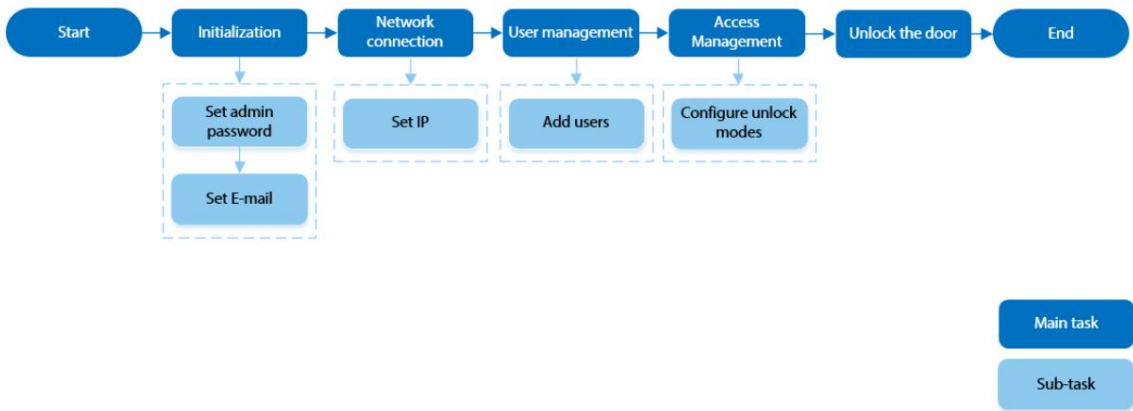
- Конфигурация может отличаться в зависимости от модели продукта, пожалуйста, ориентируйтесь на фактическую конфигурацию продукта.
- Для выполнения настроек устройства без сенсорного экрана должны быть подключены к мыши. Данное руководство В качестве примера используется устройство с сенсорным экраном.
- 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 элементы интерфейса могут не отображаться из-за ограниченного пространства. Нажмите и удерживайте текст в течение 3 секунд, и он отобразится.

2.1 Процедура базовой настройки

Рисунок 2-1. Базовая процедура настройки.



2.2 Общие значки

Таблица 2-1. Описание значков.

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

2.3 Экран ожидания

Дверь можно разблокировать 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.



- Если в течение 30 секунд не будет никаких действий, устройство перейдет в режим ожидания. • Данное руководство носит исключительно справочный характер. Возможны незначительные различия в отображении экрана в режиме ожидания в данном руководстве и на самом устройстве.

Рисунок 2-2. Экран ожидания

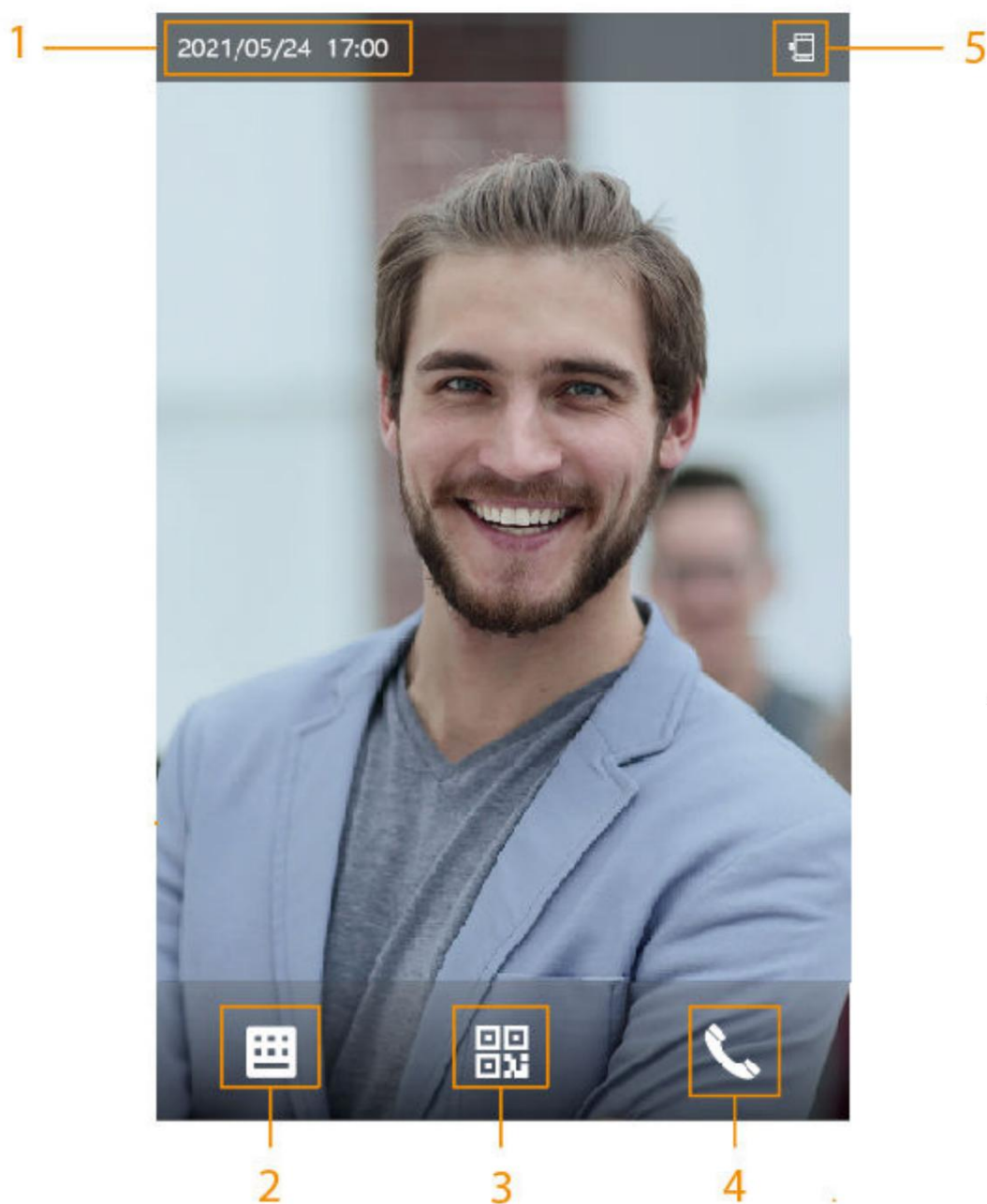


Таблица 2-2. Описание главного экрана.

Нет.	Имя	Описание
1	Дата и время	Текущая дата и время.
2	Пароль	Введите пароль пользователя или пароль администратора или Временный пароль для разблокировки двери.
3	QR-код	Нажмите на значок QR-кода и отсканируйте QR-код, чтобы разблокировать доступ. дверь.  Для моделей, имеющих автономный модуль QR-кода или Подключает модуль расширения для QR-кодов. Значок не будет отображаться. отображается. Вы можете просто разместить свой QR-код перед ним. линза устройства или модуля расширения, это будет Автоматическое сканирование.
4	Домофон	• Когда устройство функционирует как сервер, оно может вызывать VTO и VTH. • Когда платформа управления функционирует как сервер, устройство может вызывать VTO, VTS и платформа управления. • При работе с DMSS, он может вызывать DMSS.
5	Отображение состояния	Отображает состояние Wi-Fi, сети, модуля расширения, USB. и многое другое. Модули Wi-Fi и расширения — это лишь некоторые из них. Доступно на некоторых моделях.  Вы можете нажать, чтобы перейти к экрану точки доступа Wi-Fi. Для получения более подробной информации, см. раздел "2.11.1.4 Настройка точки доступа Wi-Fi"

2.4 Инициализация

При первом использовании или после восстановления заводских настроек необходимо выбрать язык на устройстве. Затем установите пароль и адрес электронной почты для учетной записи администратора. Вы можете использовать учетную запись администратора. Для входа в главное меню устройства и его веб-страницу необходимо иметь соответствующую учетную запись.



- Если вы забыли пароль администратора, отправьте запрос на его восстановление на зарегистрированный адрес электронной почты.
- Пароль должен состоять из 8–32 непустых символов и содержать как минимум два типа символов. символы среди заглавных, строчных букв, цифр и специальных символов (за исключением ' ' ; : &).

2.5 Вход в систему

Для настройки устройства войдите в главное меню. Доступны только учетные записи администратора и администратора. Вы можете войти в главное меню устройства. При первом использовании войдите в систему под учетной записью администратора. Главный экран меню, после чего вы можете создать другие учетные записи администратора.

Справочная информация

- Административный аккаунт: Может войти в главное меню устройства, но не имеет доступа к двери. права доступа.

- Учетная запись администратора: может войти в главное меню устройства и имеет доступ 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.

- Проклад карты: Войдите в главное меню, проведя картой.
- Пароль: Введите идентификатор пользователя и пароль учетной записи администратора.
- Администратор: Введите пароль администратора для входа в главное меню.

2.6 Сброс пароля

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

Процедура

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

Шаг 2 Нажмите на «Администратор», а затем один раз нажмите на пустое место на экране.

Шаг 3. Нажмите «Забыли пароль».

Шаг 4. Прочитайте подсказку на экране, а затем нажмите Enter.

Шаг 5. Нажмите на QR-код, а затем отсканируйте QR-код.

Шаг 6. Отправьте результаты сканирования на указанный адрес электронной почты.

Вы получите код безопасности на свой электронный адрес.



- После сканирования QR-кода вы получите код безопасности на связанный с вами адрес электронной почты. Адрес. Используйте защитный код в течение 24 часов после его получения. В противном случае он станет недействительным.
- 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.

Шаг 7. Введите защитный код.



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

Шаг 8. Нажмите «Далее».

Шаг 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, цифры и специальные символы (за исключением ' " ; : &).

Шаг 10. Нажмите OK.

2.7 Методы разблокировки

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

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 с помощью пароля пользователя

Введите логин и пароль, чтобы открыть дверь.

Процедура

Шаг 1. Коснитесь экрана ожидания.

Шаг 2. Нажмите «Разблокировать по паролю», а затем введите идентификатор пользователя и пароль.

Шаг 3. Нажмите ОК.

2.7.4 Разблокировка с помощью пароля администратора

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

Предварительные требования

Пароль администратора настроен. Подробности см. в разделе "2.8.3 Настройка пароля разблокировки администратора".

Процедура

Шаг 1. Коснитесь экрана ожидания.

Шаг 2. Нажмите «Разблокировать с помощью пароля администратора», а затем введите пароль администратора.

Шаг 3. Нажмите .



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

2.7.5 Разблокировка с помощью QR-кода

Процедура

Шаг 1. На экране ожидания коснитесь .





Значок QR-кода отображается только после того, как вы перейдете в раздел «Функции» > «Ярлык интерфейса распознавания лиц», чтобы включить QR-код.

Шаг 2. Разместите QR-код перед объективом.

2.7.6 Разблокировка по отпечатку пальца

Приложите палец к сканеру отпечатков пальцев. Эта функция доступна только в некоторых моделях.

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 «Разблокировать с помощью временного пароля».

Шаг 3. Введите временный пароль, а затем нажмите .

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 Добавление пользователей

Процедура

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

Шаг 2. Настройте параметры интерфейса.

Рисунок 2-3. Добавление нового пользователя.

Create User

No.

3

Name

Face

0

Card

0

Password

User Permiss...

User

Period

255-Default

Holiday Plan

255-Default

Validity Period

2037-12-31

User Type

General User

Таблица 2-3. Описание параметров.

Параметр	Описание
Нет.	Номер подобен идентификационному номеру сотрудника, который может состоять из цифр, букв и т.д. и их комбинации, а также максимальная длина Номер равен 30 символам.
Имя	Имя может содержать до 32 символов (включая (цифры, символы и буквы).

Параметр	Описание
FP	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. • Мы не рекомендуем устанавливать первый отпечаток пальца в качестве отпечатка для принудительного снятия. • Один пользователь может установить только один принудительный отпечаток пальца. • Функция распознавания отпечатков пальцев доступна, если устройство поддерживает подключение модуля расширения для распознавания отпечатков пальцев.
Лицо	Расположите лицо внутри рамки, и изображение лица будет автоматически захвачено. Вы можете зарегистрироваться повторно, если вас не устраивает результат.
Карта	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.  • Эта функция доступна только на некоторых моделях. • Один пользователь может установить только одну карту принуждения.
Пароль	Введите пароль пользователя. Максимальная длина пароля — 8 цифр. Пароль принудительного вызова добавляет 1 к последней цифре пароля разблокировки. Например, если пароль пользователя — 12345, то пароль принудительного вызова будет 12346; если пароль пользователя — 789, то пароль принудительного вызова будет 780. Сигнализация принудительного вызова сработает при использовании пароля принудительного вызова для разблокировки двери.
Разрешение пользователя	• Пользователь : Пользователи имеют доступ только к дверям или возможность учета рабочего времени. разрешения. • Администратор : Администраторы могут настраивать устройство, помимо разрешений доступа к дверям и учета рабочего времени.
Период	В течение заданного периода люди могут открывать дверь или отмечать посещаемость. Подробную информацию о настройке периодов см. в разделе "3.6.8.1 Настройка временных периодов".
План на отпуск	В течение установленного праздничного дня люди могут открывать дверь или отмечать присутствие. Подробную информацию о настройке периодов см. в разделе «3.6.8.2 Настройка планов праздничных дней».
Срок действия	Укажите дату, когда истекает срок действия разрешений на доступ к двери и учет рабочего времени данного лица.

Параметр	Описание
Тип пользователя	- Обычный пользователь : Обычные пользователи могут открыть дверь. - Пользователь из черного списка : Когда пользователи из черного списка разблокируют При открытии двери сработает сигнализация о заблокированном списке. • Гостевой пользователь : Гости могут разблокировать дверь в течение определенного времени. В течение определенного периода времени или на определенное количество раз. После истечения определенного периода или окончания времени разблокировки, открыть дверь уже невозможно. - Патрульный пользователь : Патрульные пользователи могут отмечать посещаемость. Устройство, но у них нет 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.  Эта функция не работает, если включена удаленная проверка. - Пользователь 1/Пользователь 2 : То же самое, что и для обычных пользователей пользователи.
Отделение	Выберите отделы, что полезно при настройке расписаний отделов. Инструкции по созданию отделов см. в разделе "2.10.1 Настройка отделов".  Эта функция доступна только на некоторых моделях.
Режим расписания	- Расписание отдела: Примените расписание отдела к пользователь. - Личное расписание: Применяйте личное расписание к пользователь. Инструкции по настройке личных или departmental графиков см. в разделе "2.10.4 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 .



2.8.2 Просмотр информации о пользователе

Процедура

Шаг 1. В главном меню выберите «Управление персоналом» > «Список пользователей» или выберите «Пользователи» > «Администратор».
Список.

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.

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.

2.8.3 Настройка пароля разблокировки администратора

Дверь можно открыть, введя только пароль администратора. Этот пароль не ограничен типами пользователей. Для одного устройства разрешен только один пароль разблокировки администратора.

Процедура

Шаг 1. На главном экране меню выберите Пользователь > Разблокировать пароль администратора.

Шаг 2. Нажмите «Пароль разблокировки администратора», а затем введите пароль.

Шаг 3. Включите функцию разблокировки администратора.

2.9 Управление контролем доступа

Вы можете настроить параметры дверей, такие как режим разблокировки, связь с сигнализацией и расписание работы дверей. Доступные режимы разблокировки могут различаться в зависимости от модели изделия.

2.9.1 Настройка метода разблокировки

2.9.1.1 Настройка комбинаций разблокировки

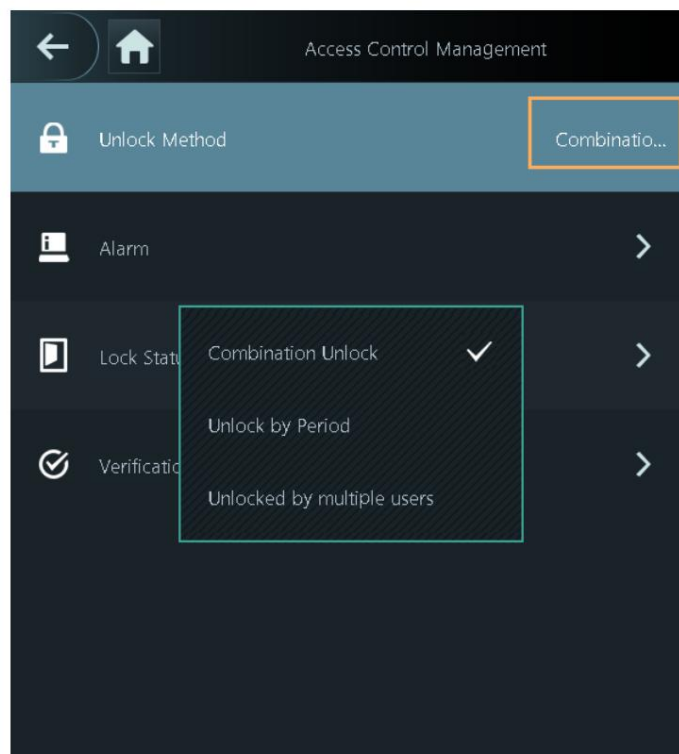
Для разблокировки двери используйте карту, отпечаток пальца, распознавание лица, пароль или их комбинации. Доступные режимы разблокировки могут различаться в зависимости от модели устройства.

Процедура

Шаг 1. Выберите «Управление контролем доступа» > «Способ разблокировки».

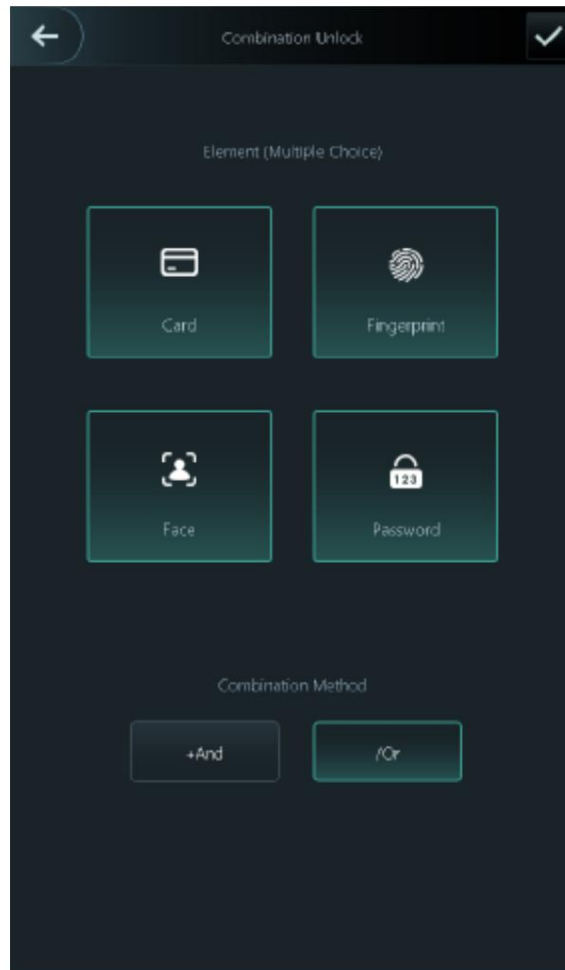
Шаг 2. Нажмите «Комбинированная разблокировка», и выберите комбинацию для разблокировки из списка.

Рисунок 2-4. Комбинированная разблокировка.



Шаг 3. Нажмите «Способ разблокировки» и выберите способ разблокировки.

Рисунок 2-5. Комбинированный метод.



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, что  сохранить изменения.

2.9.1.2 Настройка разблокировки по периоду

Процедура

Шаг 1. Выберите «Управление контролем доступа» > «Способ разблокировки».

Шаг 2. Нажмите на правую область «Способ разблокировки». , а затем выберите в списке пункт «Разблокировать по периоду» .

Подробную информацию о настройке разблокировки по периодам см. в разделе "3.6.1.2 Настройка методов разблокировки".

Шаг 3. Нажмите, что  сохранить изменения.

2.9.1.3 Настройка разблокировки для нескольких пользователей

Процедура

Шаг 1. Выберите «Управление контролем доступа» .

Шаг 2. Нажмите на правую часть списка «Метод разблокировки» , а затем выберите «Разблокировать для нескольких пользователей» .

Подробную информацию о настройке разблокировки по периодам см. в разделе "3.6.1.2 Настройка методов разблокировки".

Шаг 3. Нажмите, чтобы  сохранить изменения.

2.9.2 Настройка сигналов тревоги

Сигнализация сработает при несанкционированном доступе к входу или выходу.

Процедура

Шаг 1. Выберите «Управление контролем доступа» > «Сигнализация».

Шаг 2. Включите этот тип сигнализации.



Типы сигналов тревоги могут различаться в зависимости от модели изделия.

Рисунок 2-6 Сигнализация

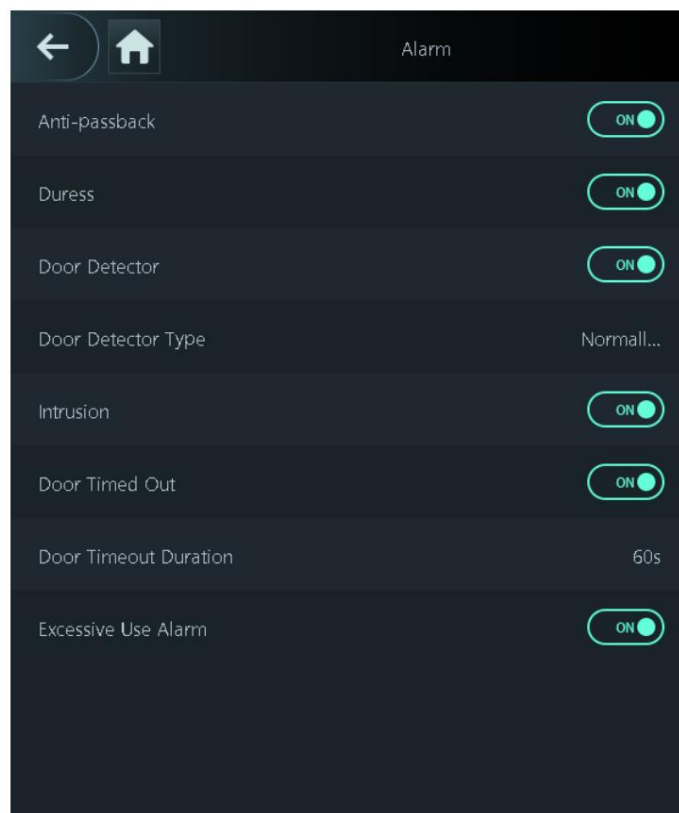


Таблица 2-4. Описание параметров тревоги.

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.
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: датчик находится в замкнутом состоянии, когда дверь или окно закрыты. - Нормально разомкнутый: Разомкнутая цепь создается, когда окно или дверь фактически закрыто.
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 неlegalной карты, которая будет гореть в течение определенного времени.

2.9.3 Настройка состояния двери

Процедура

Шаг 1. На главном экране меню выберите «Управление контролем доступа» > «Настройка состояния блокировки».

Шаг 2. Установите состояние двери.

Рисунок 2-7. Состояние блокировки.

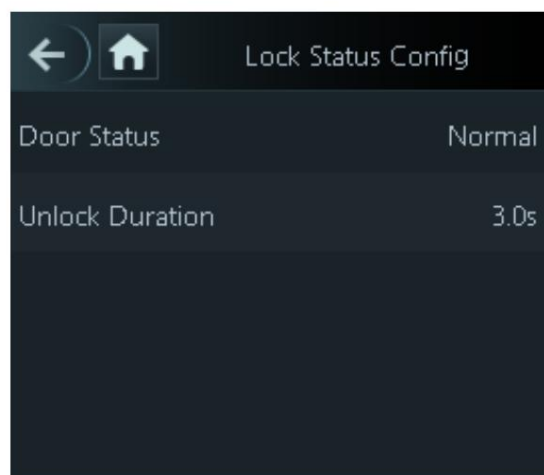


Таблица 2-5. Описание параметров.

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.

2.9.4 Настройка интервала времени 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.

Процедура

Шаг 1. Выберите «Управление контролем доступа» > «Интервал проверки (сек)».

Шаг 2. Введите временной интервал, а затем нажмите .



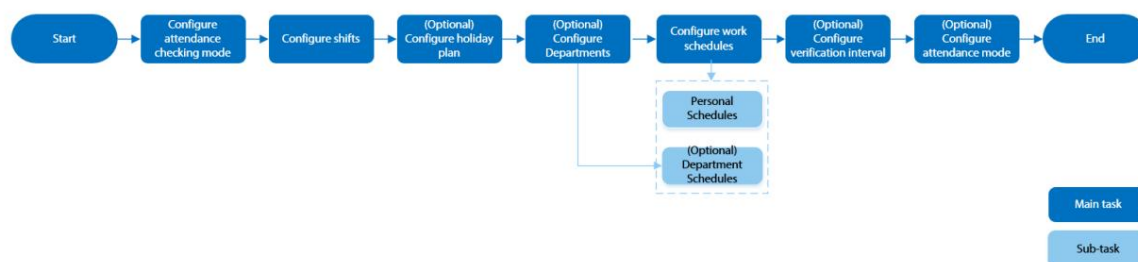
2.10 Управление посещаемостью

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 2-8. Блок-схема конфигурации учета рабочего времени.



2.10.1 Настройка отделов

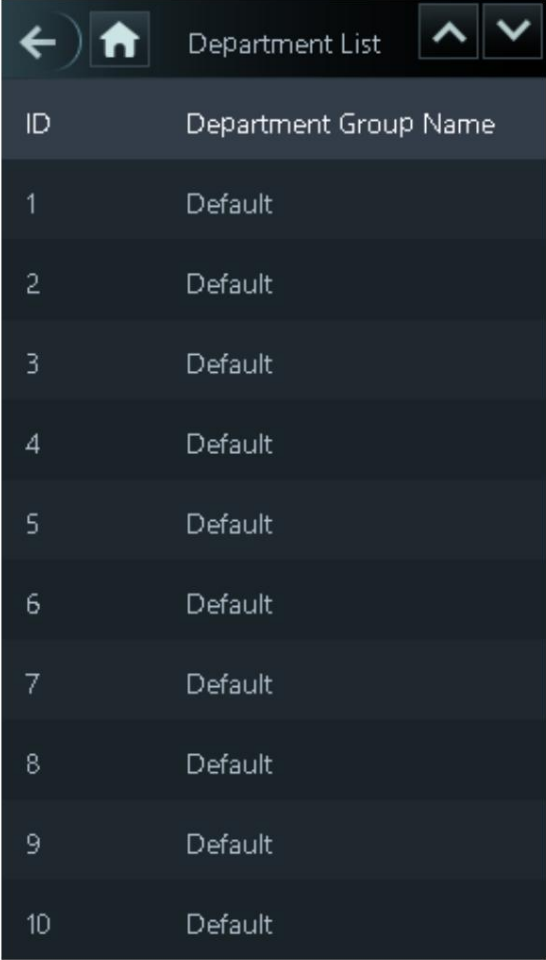
Процедура

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

Шаг 2. Выберите отдел, а затем переименуйте его.

По умолчанию существует 20 отделов. Рекомендуем переименовать их.

Рисунок 2-9. Создание 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 . 

2.10.2 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 2-10. Создание смен.

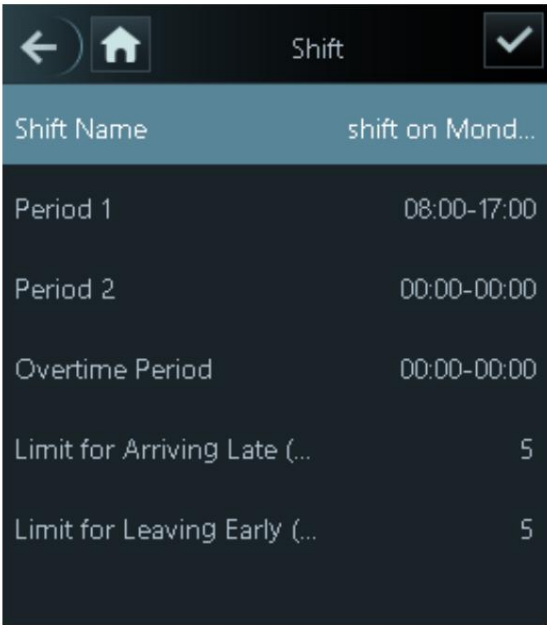
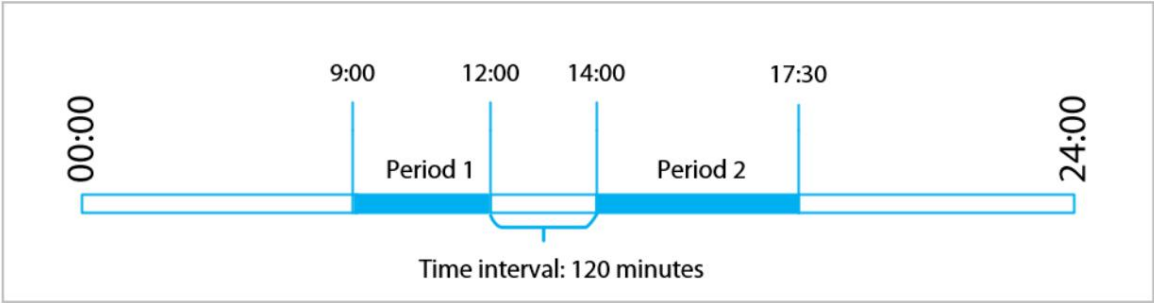


Таблица 2-6. Описание параметров сдвига.

Параметр	Описание
Название смены	Введите название смены.
Период 1	Укажите временной промежуток, в течение которого сотрудники могут отмечать начало и конец рабочего дня.
Период 2	Если вы установите только один период учета рабочего времени, сотрудники должны отмечать начало и конец рабочего дня в установленное время, чтобы избежать ошибок в их таблице учета рабочего времени. Например, если вы установите 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 установите два периода посещаемости, эти два периода не могут перекрываться. Сотрудники должны отмечать время прихода и ухода с работы в оба периода.
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 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 2-11. Временной интервал (четное число).



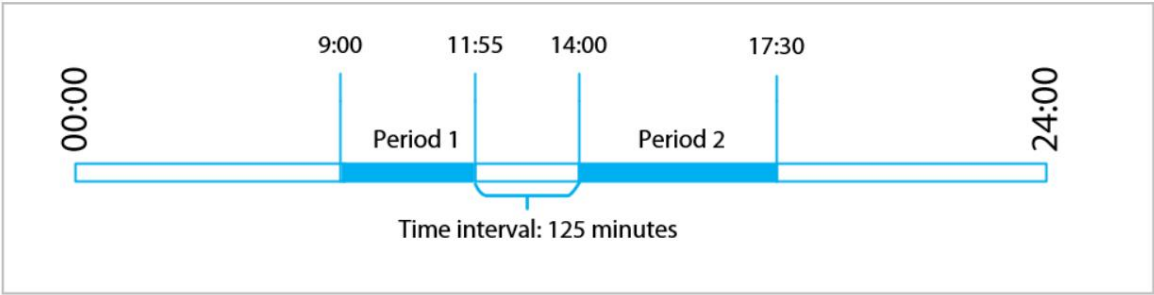
Например: если интервал составляет 120 минут, то время окончания работы в период 1 — с 12:00 до 12:59, а время начала работы в период 2 — с 13:00 до 14:00.



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 2-12. 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.



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. 

2.10.3 Настройка планов на время праздников

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 2-13. Составление планов на праздники.

←

Holiday Plan

✓

Attendance Holiday No.

1

Attendance Holiday

Start Time

2023-06-08

End Time

2023-06-08

Таблица 2-7. 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. ✓

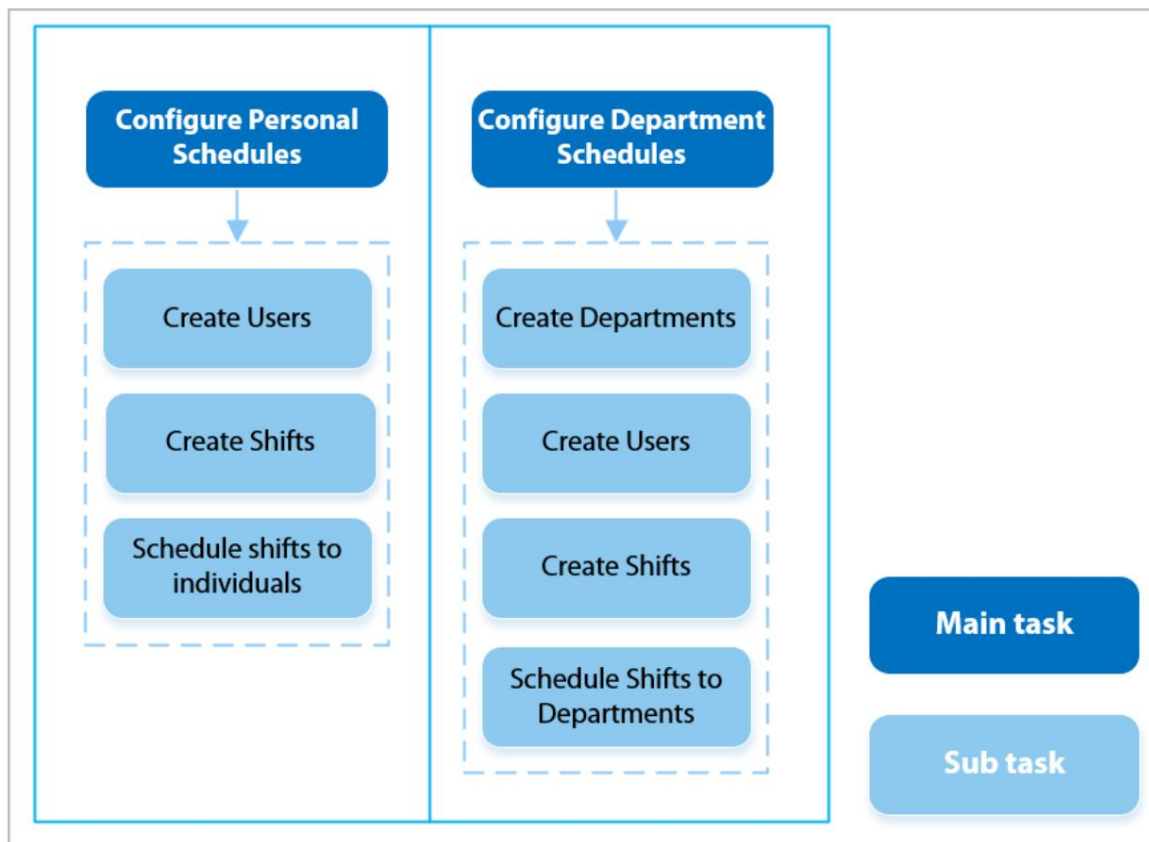
2.10.4 Настройка графиков работы

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.

Рисунок 2-14. 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 перерыв. •

Цифры от 1 до 24 указывают количество заданных смен. Инструкции по настройке смен см. здесь.

См. раздел "2.10.2 Настройка смен".

• 25 означает командировку. • 26

означает отпуск.

Рисунок 2-15. Изменения в расписании для отдельных лиц.

Day	Mon	Tue	Wed	Thu	Fri	Sat
28	29	30	31	1	1	0
0	1	1	1	1	1	0
0	1	1	1	1	1	0
0	1	1	1	1	1	0
0	1	1	1	1	1	1
2	3	4	5	6	7	8

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.

• 0 означает отдых. •

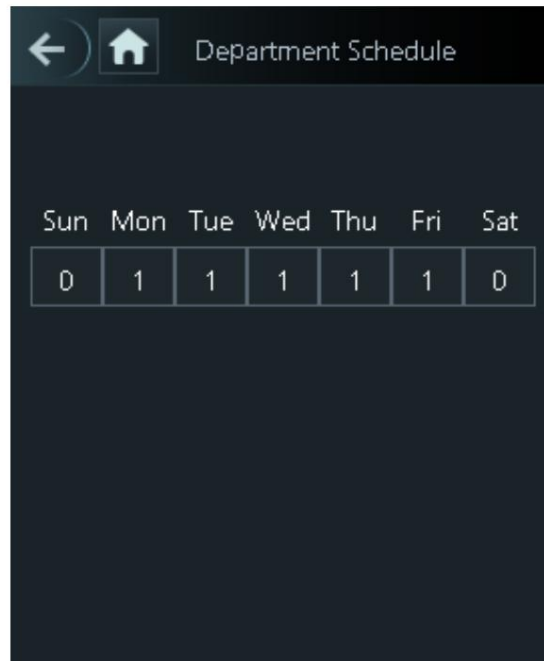
От 1 до 24 указывает количество заданных смен. Инструкции по настройке смен см. в разделе "2.10.2

Настройка смен". • 25 означает

командировку. • 26 означает

отпуск.

Рисунок 2-16. График смен в отделе.



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

Шаг 4. Нажмит ☒

2.10.5 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 локальный или удаленный режим, а затем выберите режим учета посещаемости.

Данные о посещаемости также будут синхронизированы с платформой управления.

Рисунок 2-17 Режим учета посещаемости

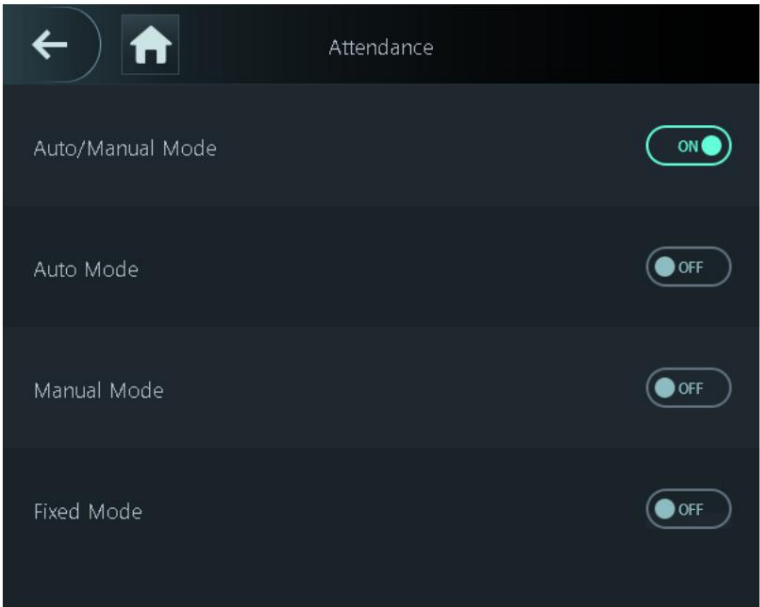


Таблица 2-8 Режим посещаемости

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 определенное время. Статус посещаемости постоянно.

Шаг 3. Выберите режим учета посещаемости.

Шаг 4. Настройте параметры режима учета посещаемости.

Рисунок 2-18 Автоматический режим/ручной режим

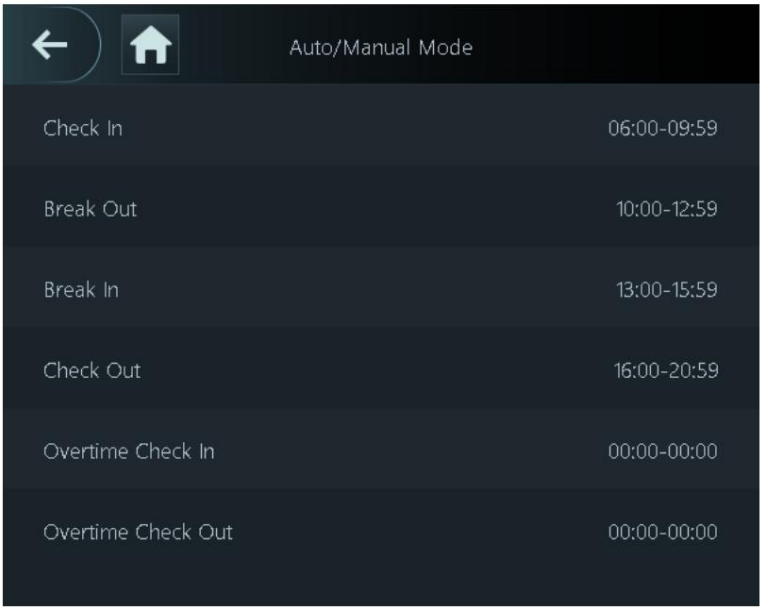


Рисунок 2-19. Фиксированный режим.

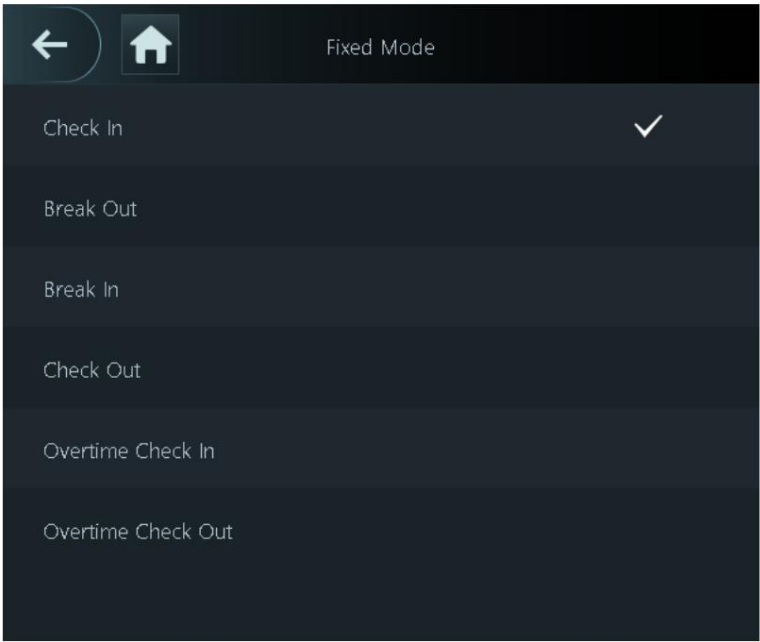


Таблица 2-9 Параметры режима посещаемости

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

2.11 Настройки связи

Настройте сеть, последовательный порт и порт Wiegand для подключения устройства к сети.



В зависимости от модели устройства, последовательный порт и порт Wiegand могут отличаться.

2.11.1 Настройка сети

2.11.1.1 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 «Настройки связи» > «Сеть» > «IP-адрес».

Шаг 2. Установите IP-адрес.

Рисунок 2-20. Конфигурация IP-адреса.

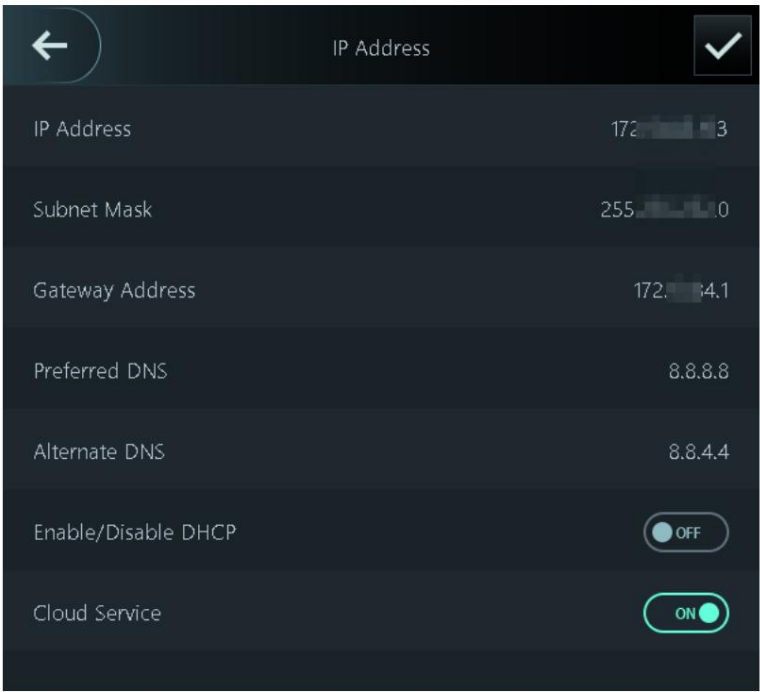


Таблица 2-10 Параметры конфигурации IP

Параметр	Описание
IP-адрес/Маска подсети/Шлюз Адрес	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
Включить/отключить 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.
Облачный сервис	Управляйте устройствами без подключения к DDNS, настраивайте сопоставление портов и развертывайте транзитные серверы.

2.11.1.2 Настройка автоматической регистрации

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

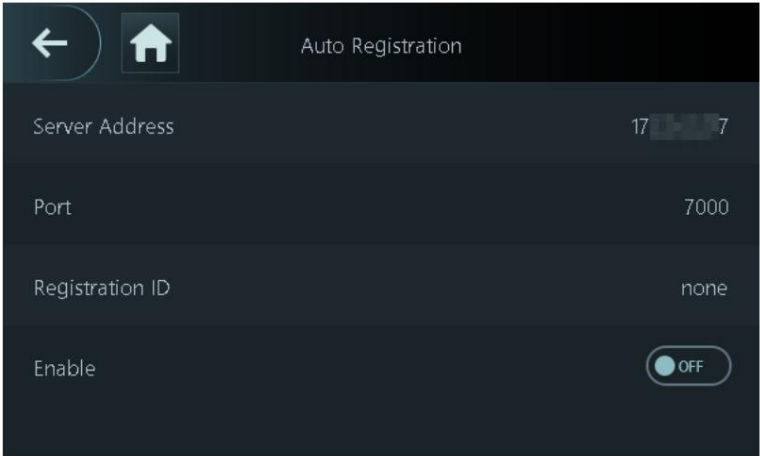
Процедура

Шаг 1. В главном меню выберите «Настройки связи» > «Сеть» > «Автоматическая регистрация».



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

Рисунок 2-21 Активная регистрация



Шаг 2. Включите функцию автоматической регистрации и задайте параметры.

Таблица 2-11 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.

2.11.1.3 Настройка Wi-Fi

Вы можете подключить устройство к сети через Wi-Fi.

Справочная информация



Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. В главном меню выберите «Настройки связи» > «Сеть» > «Wi-Fi».

Шаг 2. Включите Wi-Fi.



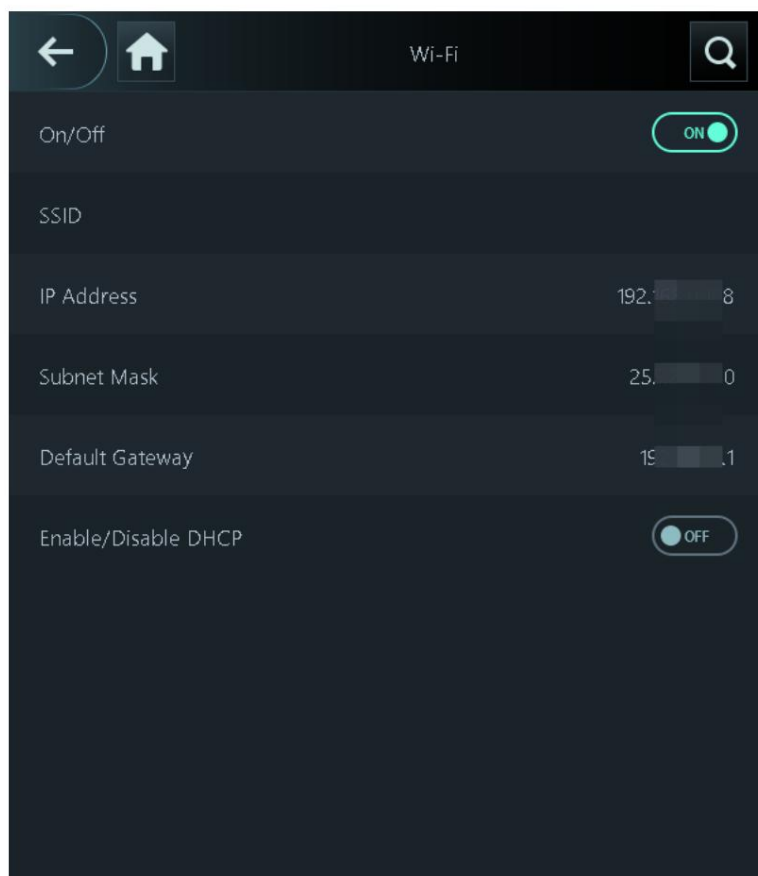
- Функция Wi-Fi доступна только на некоторых моделях.
- Точка доступа Wi-Fi и функция Wi-Fi не могут быть включены одновременно.
- После включения Wi-Fi подождите около 1 минуты для подключения к сети.

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

Шаг 4. Выберите беспроводную сеть и введите пароль.

Если система не обнаруживает сеть Wi-Fi, нажмите SSID, чтобы ввести название сети Wi-Fi.

Рисунок 2-22. Подключение к Wi-Fi.



Связанные операции

Включить/отключить DHCP: Включите эту функцию, и устройству будет автоматически присвоен Wi-Fi-адрес.

2.11.1.4 Настройка точки доступа Wi-Fi

Эта функция доступна только на некоторых моделях.

Процедура

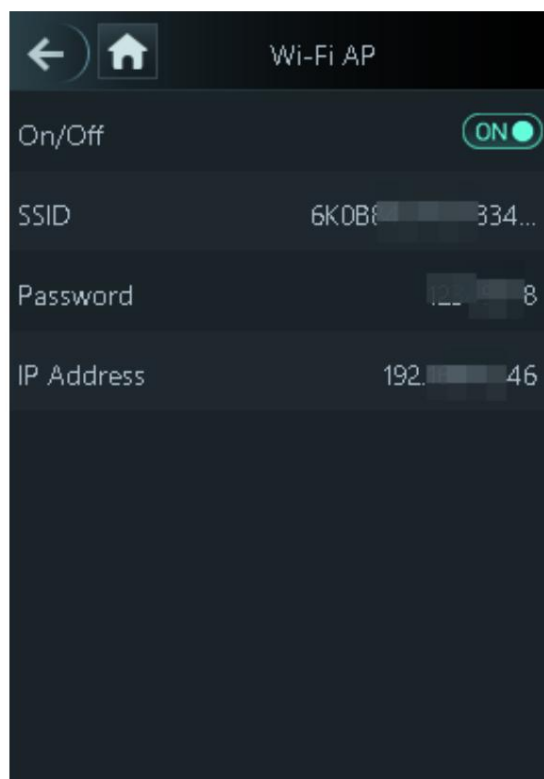
Шаг 1. В главном меню выберите «Настройки связи» > «Сеть» > «Точка доступа Wi-Fi».

Шаг 2. Включите точку доступа Wi-Fi.



Одновременное включение точки доступа Wi-Fi и функции Wi-Fi невозможно.

Рисунок 2-23. Подключение к точке доступа Wi-Fi.



Результаты

Для доступа к веб-странице устройства используйте свой компьютер, чтобы подключиться к точке доступа Wi-Fi устройства.

2.11.2 Настройка последовательного порта

Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. В главном меню выберите «Настройки связи» > «Последовательный порт».

Шаг 2. Выберите внешнее устройство.

Рисунок 2-24. Тип внешнего устройства.

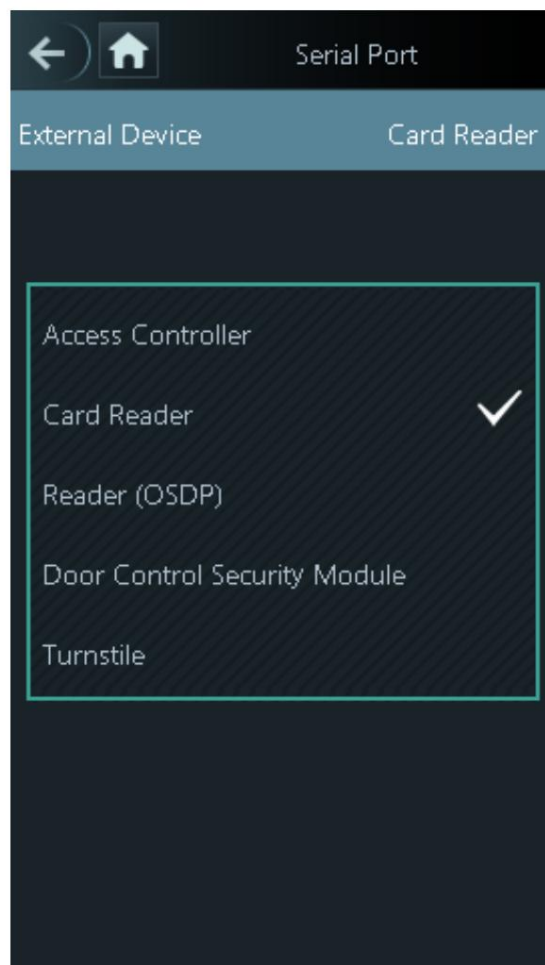


Таблица 2-12. Описание порта.

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: Выводит данные на основе номера карты, когда пользователи проводят картой через считыватель для разблокировки дверей; выводит данные на основе первого номера карты пользователя, когда пользователи используют другие способы разблокировки. • Нет: Выводит данные на основе идентификатора пользователя.
Считыватель карт	Устройство функционирует как контроллер доступа и подключается к внешнему считывателю карт.
Читатель (OSDP)	Устройство подключено к считывателю карт, работающему по протоколу OSDP.
Модуль безопасности управления дверью	После активации модуля безопасности кнопка выхода из двери, управление замком и связь устройства с противопожарной системой перестают работать, но кнопка выхода из двери и управление замком, подключенные к модулю безопасности, начинают работать.

Внешнее устройство	Описание
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.

2.11.3 Настройка Wiegand

Устройство поддерживает как входной, так и выходной режимы Wiegand.



Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. На веб-странице выберите «Настройки связи» > «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 2-25. Выход Wiegand.



Таблица 2-13. 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 пульса	
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.

2.12 Системные настройки

2.12.1 Настройка времени

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

Процедура

Шаг 1. В главном меню выберите «Системные настройки» > «Время».

Шаг 2. Настройка системного времени.

Рисунок 2-26 Время



Таблица 2-14. 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. Нажми ☒

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.

2.12.2 Настройка параметров лицевой панели

Параметры распознавания лица могут различаться в зависимости от модели устройства.

Процедура

Шаг 1. В главном меню выберите «Системные настройки» > «Настройка параметров лица».

Шаг 2. Настройте параметры лица, а затем нажмите .



Рисунок 2-27 Параметр лица

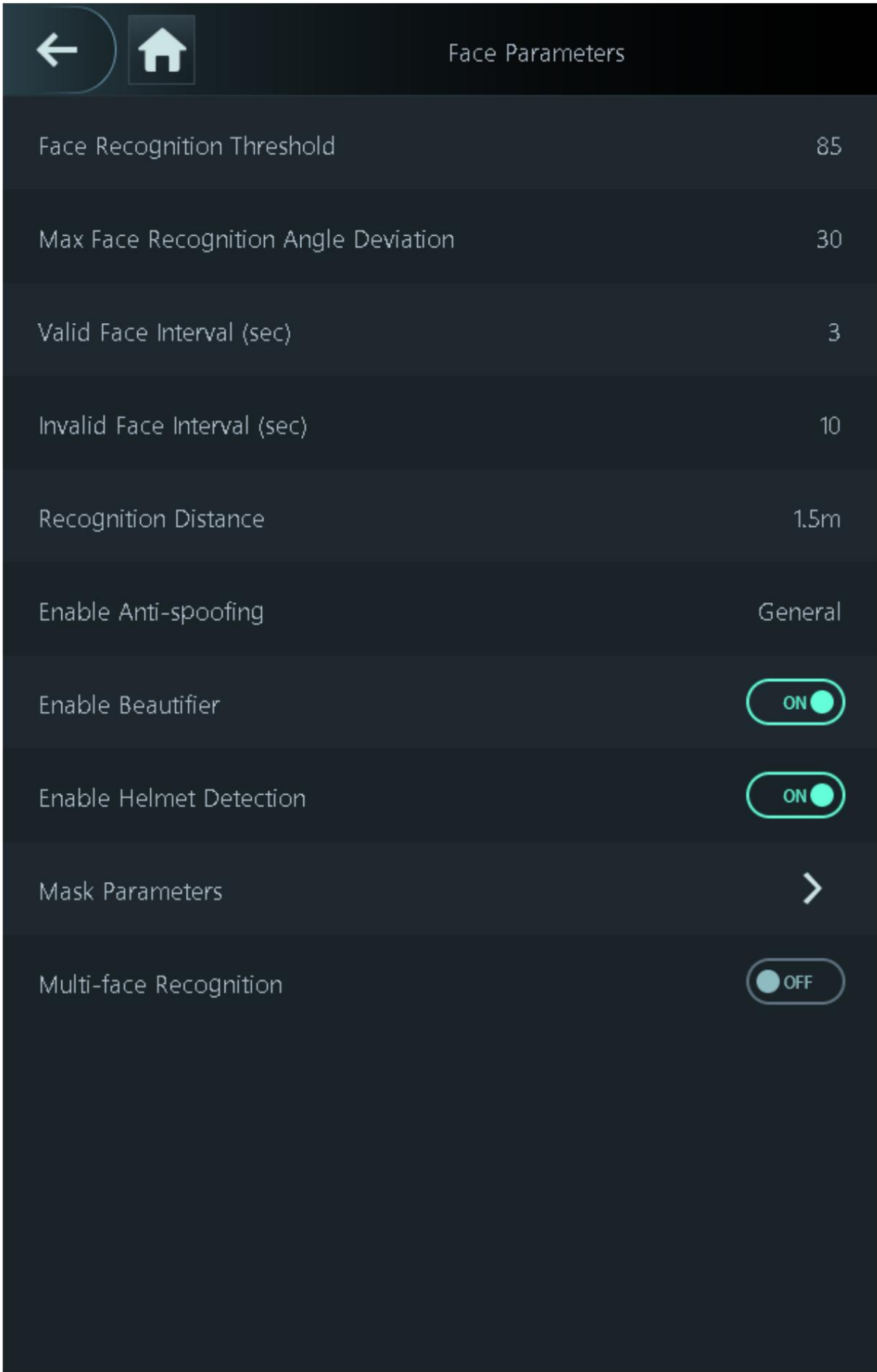


Таблица 2-15. Описание параметров лица.

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.
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.
Расстояние распознавания	Расстояние между лицом и линзой.
Включить защиту от подделки	Это предотвращает возможность использования фотографий, видеозаписей, масок и других заменителей для получения несанкционированного доступа.
Включить улучшение внешнего вида	Улучшите качество захваченных изображений лиц.
Включить обнаружение шлема	Обнаруживает защитные шлемы. Дверь не откроется для людей без шлема.
Параметры маски	- Режим маски: - Не распознается : Маска не распознается во время распознавания лица. - Напоминание о маске : маска распознается в процессе распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, но ему все равно будет разрешен доступ. - Вход без защитной маски запрещен : маска определяется при распознавании лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, и доступ будет запрещен. - Порог распознавания маски: Чем выше порог, тем точнее будет распознавание лица, когда человек носит маску, и тем ниже будет частота ложных срабатываний.
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.

Имя	Описание
Режим подсветки	• Авто: Подсветка включается в условиях низкой освещенности. • Отключено: Подсветка постоянно выключена.  Эта функция доступна только на некоторых моделях.

2.12.3 Регулировка громкости

Процедура

Шаг 1. В главном меню выберите «Системные настройки» > «Настройки громкости».

Шаг 2. Настройте параметры.

Таблица 2-16. Описание параметров.

Параметры	Описание
Громкость звукового сигнала	а затем нажмите  и  , чтобы отрегулировать громкость.
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.

2.12.4 Настройка языка

Измените язык на устройстве. В главном меню выберите «Системные настройки» > «Язык» и выберите язык, подходящий для вашего устройства.

2.12.5 Настройки экрана

Настройте время выключения дисплея и время выхода из системы.

Процедура

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

Шаг 2. Нажмите «Время выхода»  Нажмите «Настройки выключения экрана» или «Настройки яркости экрана», а затем выберите соответствующий пункт. 
или  отрегулируйте время или яркость экрана.

- Время выхода из системы: Система возвращается в режим ожидания через заданное время. бездействие.
- Настройки выключения экрана: система возвращается в режим ожидания, а затем экран выключается после заданного периода бездействия.

Например, если время выхода из системы установлено на 15 секунд, а время выключения экрана — на 30 секунд, система вернется в режим ожидания через 15 секунд, а затем экран выключится еще через 15 секунд.



Время выхода из системы должно быть меньше времени выключения экрана.

2.12.6 (Необязательно) 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.

2.12.7 Восстановление заводских настроек

Процедура

Шаг 1. В главном меню выберите «Системные настройки» > «Заводские настройки».

Шаг 2. При необходимости восстановите заводские настройки.

- Сброс к заводским настройкам : Сбрасывает все конфигурации и данные, кроме настроек IP-адреса и... тип модуля расширения.
- Восстановление настроек по умолчанию (за исключением информации о пользователе и журналов) : Сбрасывает все настройки. Настройки, за исключением информации о пользователе и журналов.

2.12.8 Перезагрузка устройства

В главном меню выберите «Системные настройки» > «Перезагрузка», и устройство будет перезагружено.

2.13 Настройки функций

На главном экране меню выберите «Функции».



Функционал может различаться в зависимости от модели изделия.

Рисунок 2-28 Функции

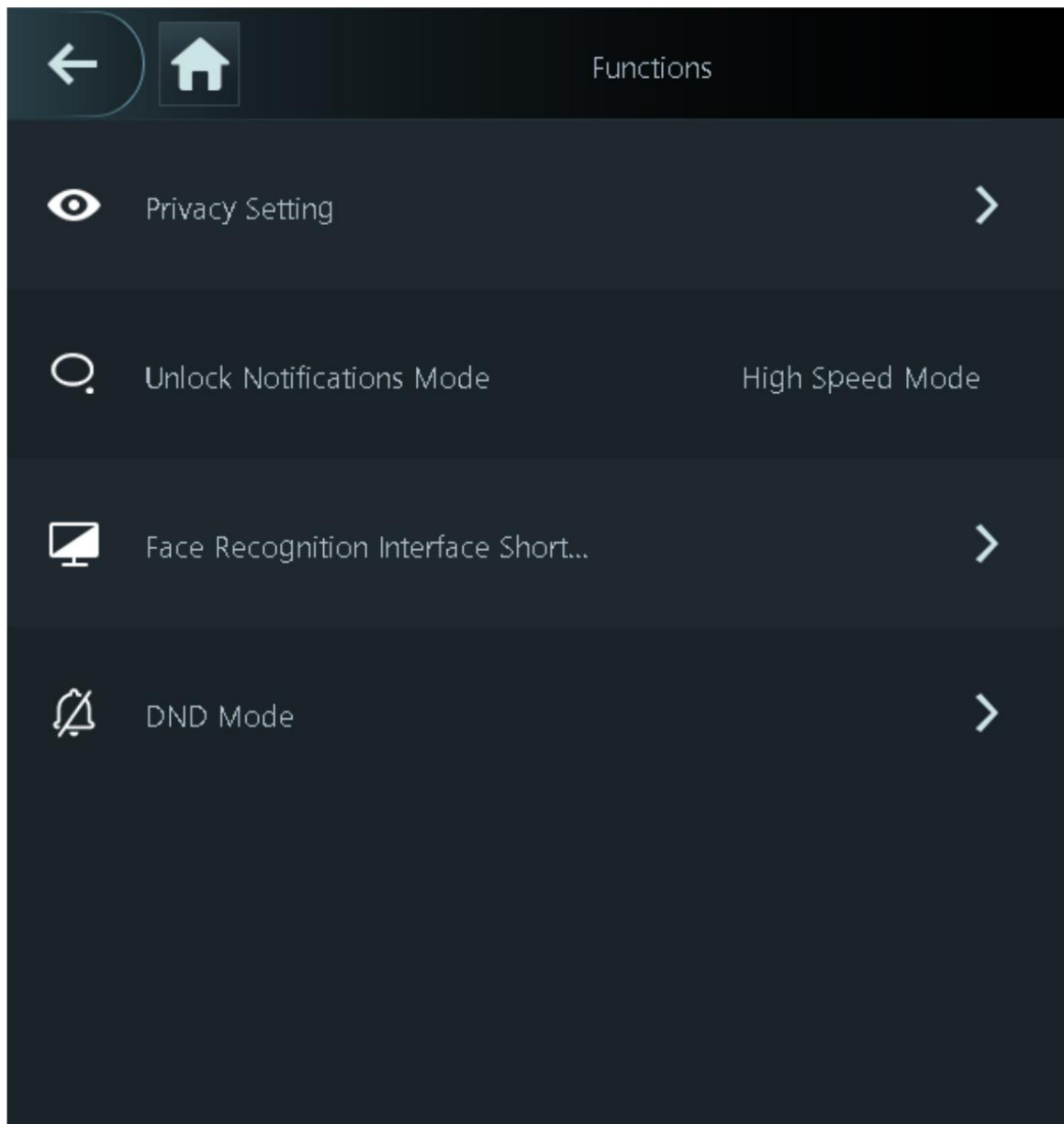


Таблица 2-17. Описание функций.

Параметр	Описание
Приватные настройки	• Сброс пароля: Пароль можно сбросить, включив эту функцию. • Включение HTTPS: Протокол HTTPS (Hypertext Transfer Protocol Secure) — это протокол для безопасной связи в 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. • Включить CGI: Common Gateway Interface (CGI) предлагает стандартный протокол для веб-серверов, позволяющий выполнять программы аналогично тому, как консольные приложения работают на сервере, динамически генерирующем веб-страницы. CGI включен по умолчанию. • Включить SSH: Secure Shell (SSH) — это криптографический сетевой протокол для безопасной работы сетевых служб в незащищенной сети. После включения этой функции передаваемые данные будут зашифрованы. • Изображение отпечатка пальца: Изображение отпечатка пальца отображается, когда Разблокировка осуществляется с помощью отпечатка пальца.  Эта функция доступна только на некоторых моделях. • Захват: Изображения лиц будут автоматически фиксироваться при открытии двери. • Очистить все снимки: Удалить все автоматически сделанные фотографии.
Push-уведомления	Отображает уведомление на экране, когда пользователь подтверждает свою личность на устройстве. • Высокоскоростной режим: система выдает сообщение «Проверено успешно» или на экране отображается сообщение «Не авторизовано». • Простой режим: отображает идентификатор пользователя, имя и время проверки. После предоставления доступа отображается сообщение «Не авторизовано», а после отказа в доступе — время авторизации. • Стандартный режим: Отображает зарегистрированное изображение лица пользователя, идентификатор пользователя, Имя и время проверки после предоставления доступа отображаются, а после отказа в доступе — «Не авторизовано» и время проверки. • Контрастный режим: отображает захваченное изображение лица и зарегистрированное изображение лица пользователя, идентификатор пользователя, имя и время авторизации после предоставления доступа, а также отображает сообщение «Не авторизовано» после отказа в доступе.

Параметр	Описание
Интерфейс распознавания лиц Быстрый доступ	Выберите методы проверки личности на экране ожидания. • Пароль: его значок отображается на экране ожидания. • QR-код: его значок отображается на экране ожидания.  Эта функция доступна только на некоторых моделях. • Дверной звонок: его значок отображается на экране ожидания. ◇ Локальный звонок устройства: Нажмите на значок звонка на экране ожидания, устройство зазвонит. ◇ Настройка мелодии звонка: Выберите мелодию ◇ звонка. Время звонка (сек): Установите время звонка (1-30 секунд). Значение по умолчанию — 3. ◇ Сигнализация: Нажмите на значок звонка, и внешнее тревожное устройство зазвонит.  Эта функция доступна только на некоторых моделях. Если кабель сигнализации и кабель дверного звонка используются совместно, убедитесь, что функциональный интерфейс установлен на «Дверной звонок». Подробнее см. раздел «3.6.11 Настройка функций порта». • Вызов: его значок отображается на экране ожидания. • Тип вызова: ◇ Номер комнаты: Нажмите на значок вызова в режиме ожидания и введите номер комнаты, чтобы совершить звонок. ◇ Центр управления вызовами: в режиме ожидания коснитесь значка вызова, а затем позвоните в центр управления. ◇ Настраиваемая комната для звонка: коснитесь значка вызова на экране ожидания, чтобы позвонить в предварительно заданную комнату.  Вы можете звонить только в DMSS в этом типе вызова. • SIP-сервер: Вы можете включить SIP, чтобы настроить устройство на работу с SIP-сервером.
Модуль расширения	Выберите модуль расширения, и устройство перезагрузится. • В левом углу экрана в режиме ожидания отображается сообщение об успешной настройке. • В правом углу экрана в режиме ожидания отображается сообщение о неудачной настройке.  • Модуль расширения доступен только для некоторых моделей. • Модуль расширения не поддерживает горячую замену. • Конфигурация модуля расширения остается неизменной. Ничего не изменилось даже после восстановления системы до заводских настроек.
Режим «Не беспокоить»	В течение установленного времени при подтверждении личности на устройстве голосовые подсказки не воспроизводятся. Можно установить до 4 таких периодов.

2.14 Управление USB

Для обновления устройства, а также для экспорта или импорта информации о пользователях или записей о посещаемости через USB можно использовать USB-накопитель.



- 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.
- Вы можете использовать USB-накопитель для экспорта информации с одного устройства на другое. Импорт изображений лиц через USB-накопитель запрещен.
- Импорт/экспорт данных о посещаемости доступен только на некоторых моделях.

2.14.1 Экспорт на USB

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

Процедура

Шаг 1. В главном меню выберите «Управление USB» > «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.

2.14.2 Импорт с USB-накопителя

Вы можете импортировать данные с USB-накопителя на устройство.

Процедура

Шаг 1. В главном меню выберите «Управление USB» > «Импорт с USB».

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

2.14.3 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 «Управление USB» > «Обновление USB».

Шаг 3. Нажмите OK.

Устройство перезагрузится после завершения обновления.



Не выключайте устройство во время обновления.

2.15 Управление документацией

В главном меню выберите «Управление записями» > «Поиск записей разблокировки». Отобразятся записи разблокировки. Вы можете искать записи по идентификатору пользователя.

2.16 Информация о системе

Вы можете просмотреть объем данных и версию устройства.

2.16.1 Объем данных для просмотра

В главном меню выберите «Информация о системе» > «Объем памяти», чтобы просмотреть объем памяти для каждого типа данных.

2.16.2 Версия устройства просмотра

В главном меню выберите «Информация о системе» > «Версия устройства». Там вы сможете просмотреть версию устройства, например, серийный номер, версию программного обеспечения и многое другое.

Связанные операции

Нажмите на QR-код с информацией о продукте, отсканируйте QR-код телефоном, чтобы просмотреть документацию на продукт.



Эта функция доступна только на некоторых моделях.

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 указанный адрес электронной почты.

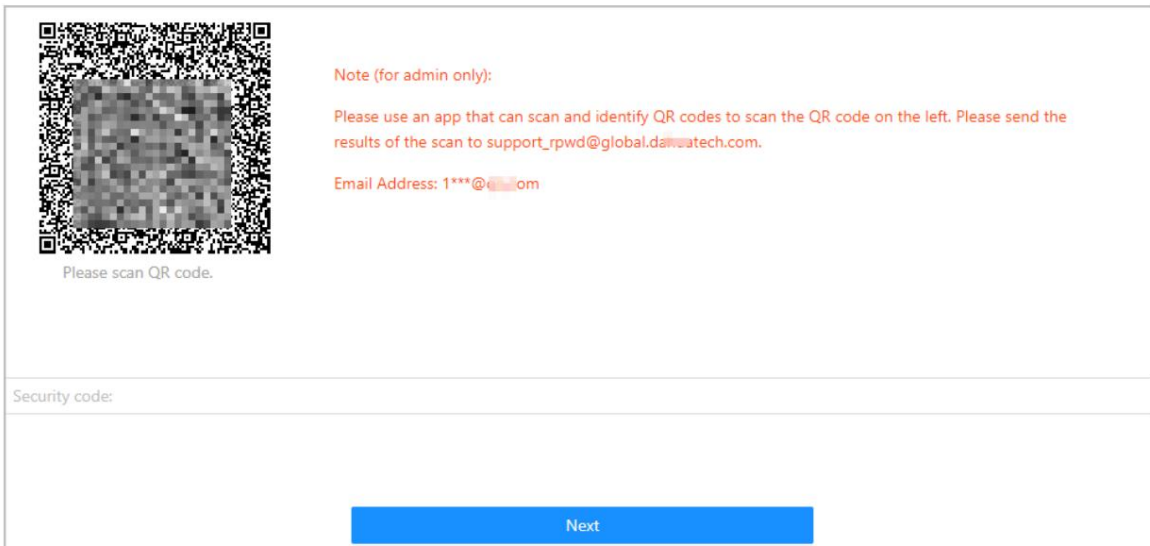
Процедура

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.



- 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 Главная страница

Главная страница отображается после успешного входа в систему.

Рисунок 3-2. Главная страница

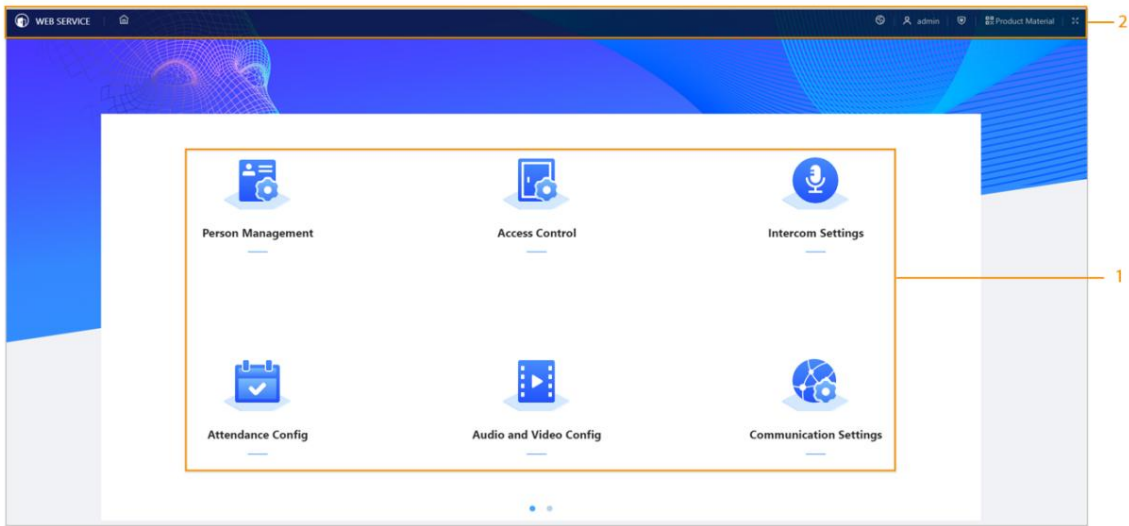


Таблица 3-1. Описание главной страницы

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

3.5 Управление персоналом

Процедура

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

Шаг 2. Настройка информации о пользователе.

Рисунок 3-3. Добавление пользователей.

Add

Basic Info

* User ID

* Department

1-

Validity Period

2037-12-31 23:59:59

* User Type

General User

* Period

255-Default

Name

* Schedule Mode

Department Schedule

* Permission

User

* Times Used

Unlimited

* Holiday Plan

255-Default

Verification Mode

Face

Not Added

+
Upload

The image size must not exceed 100KB. Supported formats: jpg.

> Password

Not Added

> Card

Not Added

Add

Add More

Cancel

Таблица 3-2. Описание параметров.

Параметр	Описание
ID пользователя	Идентификатор пользователя похож на идентификатор сотрудника, который может состоять из цифр, буквы, их сочетания и максимальная длина Число состоит из 30 символов.
Имя	Имя может содержать до 32 символов (включая (цифры, символы и буквы).

48

Параметр	Описание
Отделение	Добавьте пользователей в отдел. Если сотруднику назначен график работы отдела, он будет следовать установленному графику. Инструкции по созданию отдела см. в разделе "2.10.1 Настройка отделов".
Режим расписания	• График работы отдела: Назначьте пользователю график работы отдела. Подробности см. в разделе «2.10.4 Настройка графиков работы». • Персональное расписание: Назначьте пользователю персональное расписание. Подробности см. в разделе «2.10.4 Настройка рабочих расписаний».  ◇ 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 прав доступа к дверям и учета рабочего времени.
Тип пользователя	• Обычный пользователь : Обычные пользователи могут открыть дверь. • Пользователь из черного списка : Когда пользователи из черного списка открывают дверь, обслуживающий персонал получает уведомление. • Гостевой пользователь : Гости могут открыть дверь в течение определенного времени. В течение определенного периода времени или на определенное количество раз. После истечения определенного периода или окончания времени разблокировки, открыть дверь уже невозможно. • Патрульный пользователь : Патрульные пользователи могут отмечать посещаемость. Устройство, но у них нет доступа к двери. • VIP-пользователь : Когда VIP-пользователь открывает дверь, обслуживающий персонал получает уведомление. • Другой пользователь : После разблокировки двери она останется незапертой еще на 5 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.
Период	В течение установленного периода люди могут открывать дверь или отмечать присутствие.  Вы можете выбрать несколько периодов.

Параметр	Описание
План на отпуск	В дни установленных праздников посетители могут открывать двери или отмечать присутствие.  Вы можете выбрать более одного праздника.
Лицо	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.
Карта	 Эта функция доступна только на некоторых моделях. - Введите номер карты вручную. - Нажмите «Добавить». - Введите номер карты, затем нажмите «Добавить». • Номер будет считан автоматически с помощью считывателя регистрации или устройства. - Нажмите  , а затем нажмите «Изменить», чтобы выбрать «Добавить устройство для регистрации» или «Устройство». - Нажмите «Прочитать карту», а затем проведите картой по считывателю. читатель. На экране отображается 60-секундный обратный отсчет, напоминающий о необходимости провести картой, после чего система автоматически считывает номер карты. Если 60-секундный отсчет истек, нажмите кнопку «Считать карту» еще раз, чтобы начать новый отсчет. - Нажмите «Добавить». 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.  : Установить карту принуждения.  : Изменить номер карты.  Один пользователь может установить только одну принудительную карту.
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
FP	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 , а затем нажмите «Изменить», чтобы выбрать «Добавить устройство для регистрации» или «Устройство». 2. Приложите палец к сканеру в соответствии с инструкциями на экране. 3. Нажмите «Добавить».  • Функция распознавания отпечатков пальцев доступна только на некоторых моделях. • Не рекомендуется устанавливать первый отпечаток пальца в качестве принудительных. • Один пользователь может установить только один принудительный отпечаток пальца. • Функция распознавания отпечатков пальцев доступна, если устройство поддерживает подключение модуля распознавания отпечатков пальцев.

Шаг 3. Нажмите OK.

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 информации о пользователе», чтобы импортировать папку.



За один раз можно импортировать до 10 000 пользователей.

- Очистить: Удалить всех пользователей.
- Обновить: Обновить список пользователей. •

Поиск: Поиск по имени пользователя или идентификатору пользователя.

3.6 Настройка контроля доступа

3.6.1 Настройка параметров контроля доступа

3.6.1.1 Настройка основных параметров

Процедура

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

Шаг 2 В разделе «Основные настройки» укажите основные параметры контроля доступа.

Рисунок 3-4. Основные параметры

Basic Settings			
Name	Door1		
Door Status	☒ Normal ☐ Always Closed ☐ Always Open		
Normally Open Period	Period	Disabled	Holiday Plan Disabled
Normally Closed Period	Period	Disabled	Holiday Plan Disabled
Unlock Notifications Mode	High Speed Mode		
Verification Interval	0	s (0-180)	

Таблица 3-3. Описание основных параметров.

Параметр	Описание
Имя	Название двери.
Состояние двери	Установите статус двери. - Обычный режим: Дверь будет открываться и закрываться 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 периодов и планов на праздничные дни см. в разделе «3.6.8 Настройка расписаний».
Период обычного закрытия	 - Если период открытого состояния конфликтует с периодом закрытого состояния, то период открытого состояния имеет приоритет над периодом закрытого состояния. - Если периоды совпадают с планами на отпуск, планы на отпуск переносятся на более поздний срок. приоритет над периодами.
Уведомление о разблокировке	Отображает уведомление на экране, когда пользователь подтверждает свою личность на устройстве. - Высокоскоростной режим: система выводит на экран сообщение «Проверено успешно» или «Авторизация не выполнена» . - Простой режим: отображает идентификатор пользователя, имя и время проверки после предоставления доступа; отображает «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 «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; отображает «Не авторизовано» 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.

Шаг 3. Нажмите «Применить».

3.6.1.2 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 3-5. Настройки разблокировки.

Unlock Settings

Unlock Method

Combination Unlock

Combination Method

☒ Or
 ☐ And

Unlock Method (Multi-select)

☒ Card
 ☒ Fingerprint
 ☒ Face
 ☒ Password

Door Unlocked Duration

s (0.2-600)

Remote Verification

☐

Apply

Refresh

Default

Таблица 3-4. Описание настроек разблокировки.

Параметр	Описание
Способ разблокировки (множественный выбор)	Способы разблокировки могут различаться в зависимости от модели продукта.
Продолжительность открытия двери	После того, как человеку будет предоставлен доступ, дверь останется незапертой в течение определенного времени, чтобы он мог пройти. Это время варьируется от 0,2 до 600 секунд.
Тайм-аут разблокировки	Если включены датчик открытия двери и сигнализация о превышении времени разблокировки, то сработает сигнализация о превышении времени разблокировки, если дверь останется незапертой дольше заданного времени.
Удалённая проверка	Откройте дверь дистанционно.

• Разблокировка по периодам

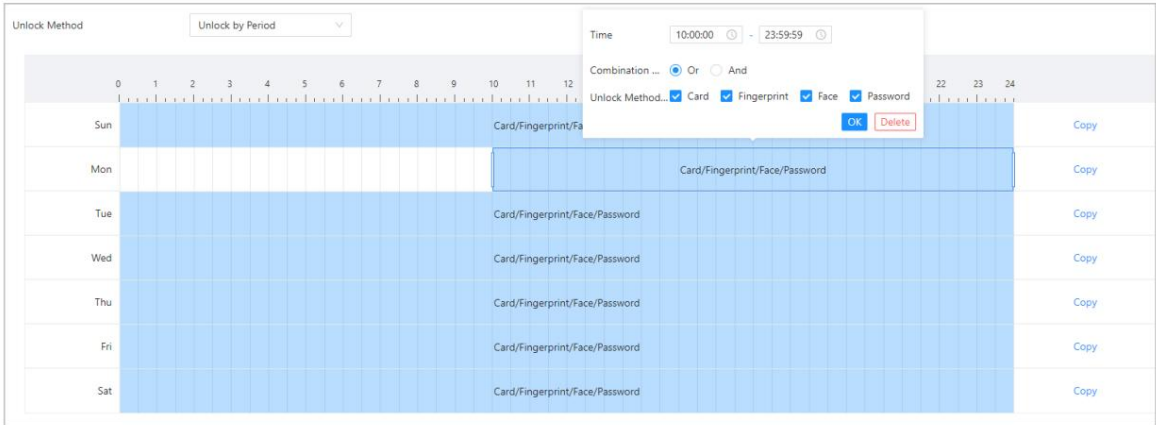
1. В списке «Режим разблокировки» выберите «Разблокировка по периоду».
2. Перетащите ползунок, чтобы отрегулировать временной период для каждого дня.



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

3. Выберите способ разблокировки на указанный период времени, а затем настройте остальные параметры.

Рисунок 3-6. Разблокировка по периодам.



• Разблокируется несколькими пользователями.

1. В списке «Режим разблокировки» выберите «Разблокировка несколькими пользователями».
2. Нажмите «Добавить», чтобы добавить группы.
3. Выберите способ разблокировки, действительный номер и список пользователей.
 - ◇ 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.



- ◇ Вы можете добавить до 4 групп.
- ◇ 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.

Шаг 3. Нажмите «Применить».

3.6.2 Настройка сигналов тревоги

Сигнал тревоги сработает при возникновении нештатной ситуации доступа.

Процедура

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

Шаг 2. Настройка параметров сигнализации.

Рисунок 3-7 Сигнализация

Duress Alarm

Anti-passback

Door Detector

Normally Closed

Normally Open

Intrusion Alarm

Unlock Timeout Alarm

Unlock Timeout

60

s (1-9999)

Excessive Use Alarm

Apply

Refresh

Default

Таблица 3-5. 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. - Нормально замкнутый: Датчик находится в замкнутом состоянии, когда Дверь или окно закрыты. - Нормально разомкнутая цепь: разомкнутая цепь создается, 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 нелегальной карты, которая будет гореть в течение определенного времени.

Шаг 3. Нажмите «Применить».

3.6.3 Настройка связи между системами оповещения (необязательно)

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 оповещений будут синхронизированы 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, чтобы настроить оповещение.

Рисунок 3-8. Связь сигналов тревоги.

Шаг 3. Придумайте название для зоны тревоги.

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

- Нормально замкнутый: Вход сигнализации находится в нормально замкнутом (НЗ) состоянии, когда сигнализация не сработала. Размыкание нормально замкнутой цепи приводит к срабатыванию сигнализации.
- Нормально разомкнутый: Устройство входа сигнализации находится в нормально разомкнутом (НО) состоянии, когда Сигнализация не сработала. Замыкание цепи приводит к срабатыванию сигнализации.

Шаг 5 Если вы хотите связать контроль доступа с сигналом пожарной тревоги, 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.

- Нормально открытый: Дверь автоматически открывается при срабатывании пожарной сигнализации.
- Нормально закрытый: Дверь автоматически закрывается при срабатывании пожарной сигнализации.

Шаг 8. Нажмите OK.

3.6.4 Настройка связи между событиями тревоги

Процедура

Шаг 1. В главном меню выберите «Контроль доступа» > «Сигнализация» > «Связывание событий тревоги».

Шаг 2. Настройка связей между событиями тревоги.

Рисунок 3-9. Связь событий тревоги.

Linkage Type	Linkage Status	Message	Buzzer	Link Alarm Out	Buzzer Duration	Link Alarm Out Duration
Intrusion Alarm Linkage	Enabled	Please enable Intrusion Alarm.	Enabled	Enabled	15 s (1-1800)	15 s (1-1800)
Unlock Timeout Alarm Linkage	Enabled	Please enable Unlock Timeout Alarm.	Enabled	Enabled	15 s (1-1800)	15 s (1-1800)
Excessive Use Alarm Linkage	Enabled	Please enable Excessive Use Alarm.	Enabled	Enabled	15 s (1-1800)	15 s (1-1800)
Tamper Alarm Linkage	Enabled		Enabled	Enabled	3 s (1-1800)	15 s (1-1800)

Buttons: Apply, Refresh, Default

Таблица 3-6. 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 тревоги. • Локальный выходной сигнал тревоги: Внешнее устройство сигнализации генерирует сигналы тревоги. Когда срабатывает сигнал тревоги об истечении времени разблокировки. Вы можете настроить продолжительность сигнала тревоги.
Сигнализация о чрезмерном употреблении Связь	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. • Локальный 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. • Локальный выходной сигнал тревоги: Внешнее устройство сигнализации генерирует сигналы тревоги при срабатывании сигнала о несанкционированном доступе. Вы можете настроить продолжительность сигнала тревоги.

3.6.5 Настройка распознавания лиц

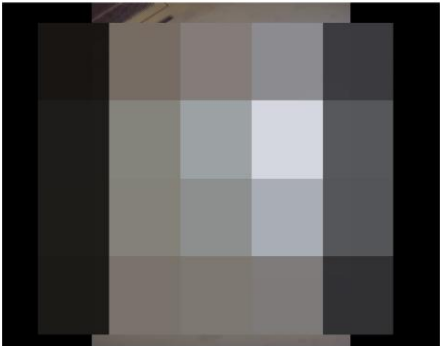
Настройте параметры распознавания лиц. Параметры распознавания лиц могут различаться в зависимости от модели устройства.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите «Контроль доступа» > «Распознавание лиц».

Рисунок 3-10. Параметры распознавания лиц.



Recognition

Exposure

Face Recognition Threshold85(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(1-60)

Recognition Distance1.5 meters

Mask modeDo Not Detect

Face Mask Threshold75(0-100)

Beautifier

☒

Enable Helmet Detection

☒

Multi-face Recognition

☐

Night Mode

☒

Screen Light Up for Face

☒

Target Filter

Min Size256 * 256

Draw TargetClear

Detection Area

Detection AreaClear

ApplyRefreshDefault

Шаг 3. Настройте параметры.

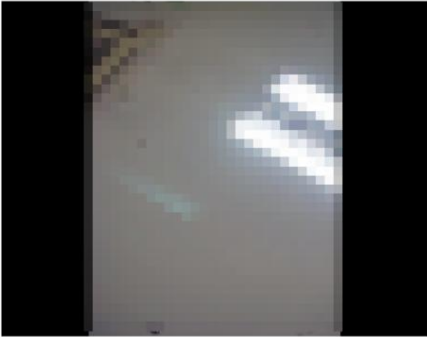
Таблица 3-7. Описание параметров лица.

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	Это предотвращает возможность использования фотографий, видеозаписей, масок и других заменителей для получения несанкционированного доступа.
Иллюминатор	• Авто: Подсветка включается в условиях низкой освещенности. • Отключено: 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.

Имя	Описание
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.
Расстояние распознавания	Расстояние между лицом и линзой.
Режим маски	• Не обнаружено : Маска не обнаружена во время распознавания лица. • Напоминание о маске : Маска обнаружена во время распознавания лица. Если человек не носит маску, система напомнит ему о необходимости надеть маску, но доступ будет разрешен. • Нет авторизации без маски : Маска не обнаружена. Обнаружено в процессе распознавания лиц. Если человек не носит маску, система напомнит ему о необходимости надеть маску, и доступ будет запрещен.
Порог ношения маски для лица	Чем выше пороговое значение, тем точнее будет распознавание лица, когда человек носит маску, и тем ниже будет частота ложных срабатываний.
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 экрана для лица	В выключенном состоянии экран загорится при обнаружении лица.

Шаг 4. Настройте параметры экспозиции.

Рисунок 3-11. Параметры экспозиции.



Recognition

Exposure

Channel No.

1

Face Exposure

☒

Face Target Brightness

50

(0-100)

Face Exposure Interval Dete...

10

s (1-28800)

Target Filter

Min Size

256

*

256

Draw Target

Clear

Detection Area

Detection Area

Clear

Apply

Refresh

Default

Таблица 3-8. Описание параметров воздействия.

Параметр	Описание
Номер канала	• Канал 1 — режим белого света. • Канал 2 — режим инфракрасного света.
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 с заданным интервалом.

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.

3.6.6 Настройка параметров карты

Справочная информация



Эта функция доступна только на некоторых моделях.

Процедура

Шаг 1. Войдите на веб-страницу.

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

Шаг 3. Настройте параметры карты.

Рисунок 3-12. Параметры карты.

Card Settings

IC Card

☒

IC Card Encryption & Verification

☒

Block NFC Cards

☒

Enable 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

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

Card Number

Write

Таблица 3-9. Описание параметров карты.

Элемент	Параметр	Описание
Настройки карты	IC-карта	При включении этой функции карту IC можно считать.  Эта функция доступна только на некоторых моделях.
	Шифрование IC-карт и Проверка	При включении этой функции зашифрованную карту можно будет прочитать.  Убедитесь, что IC-карта активирована.
	Блокировка NFC-карт	После включения этой функции разблокировка с помощью дубликата NFC-карты будет исключена.  - Эта функция доступна только на моделях. - Убедитесь, что поддержка IC-карт включена . - Функция NFC доступна только на некоторых моделях телефонов.
	Включить карту Defire	При включении этой функции устройство может считывать номер карты Defire.  - Эта функция доступна только на моделях - Поддерживаются только 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 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.

Элемент	Параметр	Описание
DESFire Card Write	Номер карты	Приложите карту к считывателю, вставьте карту. номер, а затем нажмите «Написать» , чтобы записать карту. номер карты.  • Необходимо включить функцию карты Desfire. • Поддерживается только шестнадцатеричный формат. • Поддерживает до 8 символов.

Шаг 4. Нажмите «Применить».

3.6.7 Настройка QR-кода

Процедура

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

Рисунок 3-13 QR-код

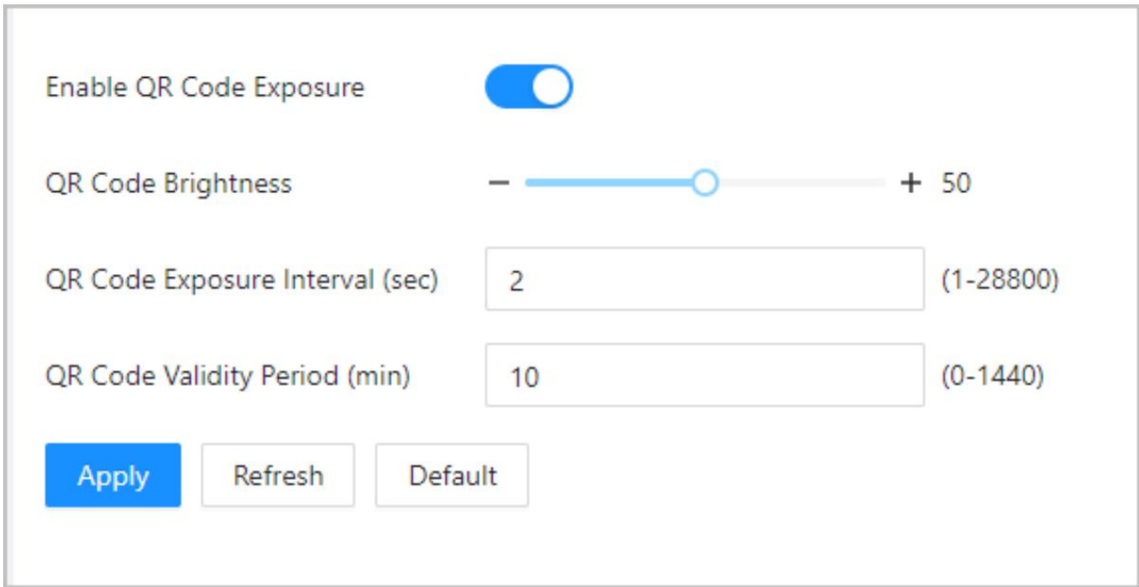


Таблица 3-10 Параметры QRR-кода

Параметры	Описание
Включить отображение QR-кода	QR-код будет отображаться с заданной яркостью, и QR-код можно обнаружить и четко прочитать.
Яркость QR-кода	
Интервал показа QR-кода (сек)	QR-код будет показан только один раз в течение заданного периода времени. интервал.
Срок действия QR-кода (мин)	После генерации QR-кода и подтверждения его действительности. Срок действия кодов ограничен определенным периодом, после чего они истекают.

3.6.8 Настройка расписаний

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

3.6.8.1 Настройка временных периодов

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» > «Период».

Шаг 3. Нажмите «Добавить».

Рисунок 3-14. Настройка временных периодов.

The screenshot shows a web application window titled "Add" with a close button (X) in the top right corner. Inside the window, there are three main sections:

- No.:** A dropdown menu showing the value "2".
- Period Name:** A text input field containing "period XX".
- Time Plan:** A grid interface for setting access times. At the top of the grid is a horizontal timeline with markers from 0 to 9. A pop-up window titled "Time" is open, showing a time range from "00:00:00" to "23:59:59" with "OK" and "Delete" buttons. The grid itself has rows for the days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and columns for the hours (0-9). A blue shaded area covers the time plan for Monday through Saturday, starting from the 00:00:00 mark. To the right of each row is a "Copy" button.

At the bottom right of the "Add" window are "OK" and "Cancel" buttons.

Шаг 4. Перетащите ползунок времени, чтобы настроить время для каждого дня.

Шаг 5 (необязательно) Нажмите «Копировать», чтобы скопировать конфигурацию на оставшиеся дни.

Шаг 6. Нажмите OK.

3.6.8.2 Настройка планов на время праздников

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».

Шаг 4. Выберите номер для группы праздников, а затем введите название группы.

Рисунок 3-15. Добавить группу праздников.

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

Шаг 5. Нажмите «Добавить», а затем добавьте праздник в группу праздников.

Шаг 6. Нажмите OK.

Рисунок 3-16. Добавление праздника в группу праздников.

Шаг 7. Нажмите «Управление планами», а затем нажмите «Добавить».

Шаг 8. Выберите номер для плана отпусков, а затем введите для него название.

Шаг 9. Выберите группу праздников, а затем перетащите ползунок, чтобы настроить время для каждого дня.

Поддерживается добавление до 4 временных интервалов в течение дня.

Рисунок 3-17. Добавить план отпуска.

Шаг 10. Нажмите OK.

3.6.9 Настройки конфиденциальности

Процедура

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

Шаг 2. Включите функцию создания моментальных снимков.

Изображения лиц будут автоматически фиксироваться, когда люди откроют дверь.

Рисунок 3-18. Включить создание моментальных снимков.

Шаг 3. Нажмите «Применить».

3.6.10 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.

-  Если в правом углу устройства отображается сообщение «Настройка вступила в силу», это означает, 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.

3.6.11 Настройка функций порта

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

Справочная информация



• 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».

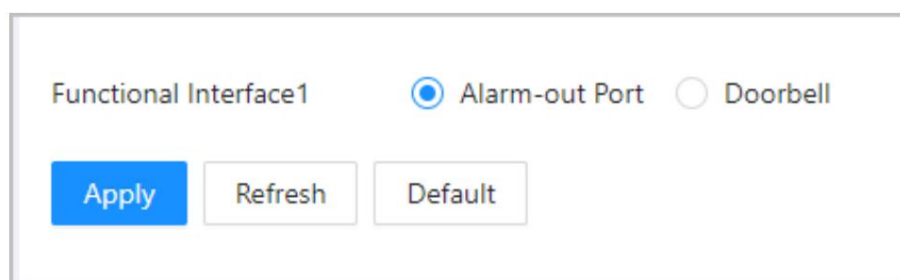
Шаг 2. Выберите тип порта.



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 3-19. Настройка портов.



3.6.12 Настройка сравнения на стороне бэкэнда

Передавайте данные, такие как QR-код или номер карты, непосредственно на стороннюю платформу для проверки данных, вместо проверки данных на самом устройстве.

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

Рисунок 3-20. Сравнение бэкэндов.

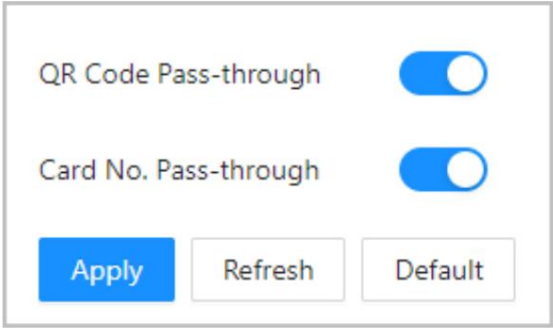


Таблица 3-11. Сравнение бэкэндов.

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 Настройка домофона

Устройство может функционировать как дверная станция для реализации видеодомофонной системы.



Функция внутренней связи доступна только на некоторых моделях.

3.7.1 Использование устройства в качестве SIP-сервера

3.7.1.1 Настройка SIP-сервера

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

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 3-21. Использование устройства 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

Шаг 3. Нажмите «Применить».

3.7.1.2 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 3-22. Основные параметры

Device Type

Door Station

No.

8001

Group Call

☐

Management Center

888888

Apply

Refresh

Default

Таблица 3-12. Описание основных параметров.

Параметр	Описание
Тип устройства	Выберите дверную станцию.
Нет.	Невозможно установить.
Групповой звонок	При включении функции группового вызова дверной пульт одновременно звонит на главный VTN 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».

3.7.1.3 Добавление дверной станции

Когда устройство функционирует как SIP-сервер, необходимо добавить дверную станцию к SIP-серверу, чтобы обеспечить возможность связи между ними.

Процедура

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

Шаг 2. Нажмите «Добавить», а затем настройте дверную станцию.

Рисунок 3-23. Добавить дверную станцию.

Add

X

Device Type

Door Station

▼

* No.

Please enter

* Registration Password

.....

🔑

Building No.

Unit No.

* IP Address

127.0.0.1

* Username

Please enter

* Password

Please enter

🔑

OK

Cancel

Таблица 3-13. Добавление конфигурации VTO.

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 значение 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	

Шаг 3. Нажмите ОК.

3.7.1.4 Добавление VTH

Когда устройство функционирует как SIP-сервер, вы можете добавить все VTH в одном блоке на SIP-сервер, чтобы обеспечить возможность их связи друг с другом.

Справочная информация



- Если есть основной VTH и добавочный номер, сначала необходимо включить функцию группового вызова, а затем добавить основной VTH и добавочный номер на странице управления VTH. Инструкции по включению функции группового вызова см. в разделе «3.7.1.2 Настройка локальных параметров».
- Добавление расширения невозможно, если не добавлены основные VTH.

Процедура

Шаг 1. На главной странице выберите «Настройки домофона» > «Настройки устройства».

Шаг 2. Добавьте VTH.

- Добавляйте по одному.
 1. Нажмите «Добавить».
 2. Настройте параметры, а затем нажмите ОК.

Рисунок 3-24. Складывайте по одному.

Add

X

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

.....

🔑

OK

Cancel

Таблица 3-14 Информация о номере

Параметр	Описание
Имя	Введите название VTH, чтобы вам было проще различать VTH.
Фамилия	
Псевдоним	

Параметр	Описание
Номер комнаты.	Введите номер комнаты ветеринарной клиники. ◇ Номер комнаты состоит из 1-5 цифр и должен соответствовать номеру комнаты, указанному в настройках VTH. ◇ Если есть основной виртуальный домофон (VTH) и его филиалы, то номер комнаты основного VTH заканчивается на -0, а номер комнаты филиала — на -1, -2 или -3. Например, основной VTH — 101-0, а номер комнаты филиала — 101-1, 101-2 и т.д. ◇ Если функция группового вызова не включена, номер комнаты в формате 9901-xx установить невозможно.
Номер комнаты.	Введите номер комнаты ветеринарной клиники. ◇ Номер комнаты состоит из 1-5 цифр и должен соответствовать номеру комнаты, указанному в настройках VTH. ◇ Если есть основной виртуальный домофон (VTH) и его филиалы, то номер комнаты основного VTH заканчивается на -0, а номер комнаты филиала — на -1, -2 или -3. Например, основной VTH — 101-0, а номер комнаты филиала — 101-1, 101-2 и т.д. ◇ Если функция группового вызова не включена, номер комнаты в формате 9901-xx установить невозможно.
Режим регистрации	Оставьте их по умолчанию.
Пароль для регистрации	

• Добавляйте партиями.

1. Нажмите «Добавить в пакетном режиме».

2. Настройте параметры.

3. Нажмите «Добавить».

Рисунок 3-25. Добавление партии.

Таблица 3-15. Добавлять партиями.

Параметр	Описание
Этажи в квартире	Количество этажей здания варьируется от 1 до 99.
Комнаты на каждом этаже	Количество комнат на каждом этаже варьируется от 1 до 99.
Комната номер один на 1-м этаже	Первая комната на первом этаже.
Комната номер один на 2-м этаже	Номер первой комнаты на 2-м этаже равен первой цифре номера первой комнаты на 1-м этаже плюс 1. Например, если номер первой комнаты на первом этаже — 101, то номер первой комнаты на 2-м этаже должен быть 201.

3.7.1.5 Добавление системы VTS

Когда устройство функционирует как SIP-сервер, вы можете добавить VTS к SIP-серверу, чтобы обеспечить возможность совершения звонков друг другу.

Процедура

Шаг 1. На главной странице выберите «Настройки домофона» > «Настройки устройства».

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

Рисунок 3-26. Управление VTS.

Add

Device Type

VTS

* VTS No.

Please enter

* IP Address

* Registration Password

.....

OK

Cancel

Таблица 3-16 Параметры VTS

Параметр	Описание
Номер VTS.	Введите 888888+ номер VTS, который может содержать до 9 цифр. Для получения номера VTS перейдите на экран «Устройство» в системе VTS.
IP-адрес	IP-адрес системы VTS.
Пароль для регистрации	Оставьте значение по умолчанию.

Шаг 3. Нажмите OK.

3.7.2 Использование VTO в качестве SIP-сервера

3.7.2.1 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 OK.

Рисунок 3-27. Используйте 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 3-17. 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».

3.7.2.2 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 3-28. Настройка параметров.

Device Type

Door Station

No.

8001

Management Center

888888

Apply

Refresh

Default

Таблица 3-18. Описание параметров.

Параметр	Описание
Тип устройства	Выберите дверную станцию.
Номер.	Номер VTO.  • 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».

3.7.3 Использование платформы в качестве SIP-сервера

3.7.3.1 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 3-29. Используйте платформу управления в качестве SIP-сервера.

SIP Server

Server Type

Private SIP Server

IP/Domain Name

192.168.1.1

Port

5080

Alternate IP

0.0.0.0

Username

8001

Alternate Server Username

admin

Registration Password

.....

Alternate Server Password

.....

SIP Domain

VDP

Alternate VTS IP

0 . 0 . 0 . 0

SIP Server Username

Alternate Server

SIP Server Password

Apply

Refresh

Default

Таблица 3-19. Конфигурация SIP-сервера.

Параметр	Описание
IP-адрес/доменное имя	IP-адрес или доменное имя платформы.
Порт	По умолчанию используется порт 5080, когда платформа работает в режиме SIP-сервера.
Имя пользователя	Оставьте их по умолчанию.
Пароль для регистрации	
Домен SIP	Оставьте значение по умолчанию.
Имя пользователя SIP-сервера	Имя пользователя и пароль для входа на платформу.
Пароль SIP-сервера	
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.

Параметр	Описание
Альтернативный сервер Имя пользователя	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.
Альтернативный сервер Пароль	
Альтернативный сервер	
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».

3.7.3.2 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 3-30. Основной параметр

Device Type

Door Station

Building No.

0

Unit No.

0

No.

8001

Management Center

888888

Apply

Refresh

Default

Таблица 3-20. Описание параметров.

Параметр	Описание
Тип устройства	Выберите станцию ограждения или дверную станцию в зависимости от места установки.

Параметр	Описание
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.

3.7.3.3 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 3-31. 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	 	

3.7.4 Простой режим

Вызов VTH или VTS одним нажатием кнопки на устройстве.

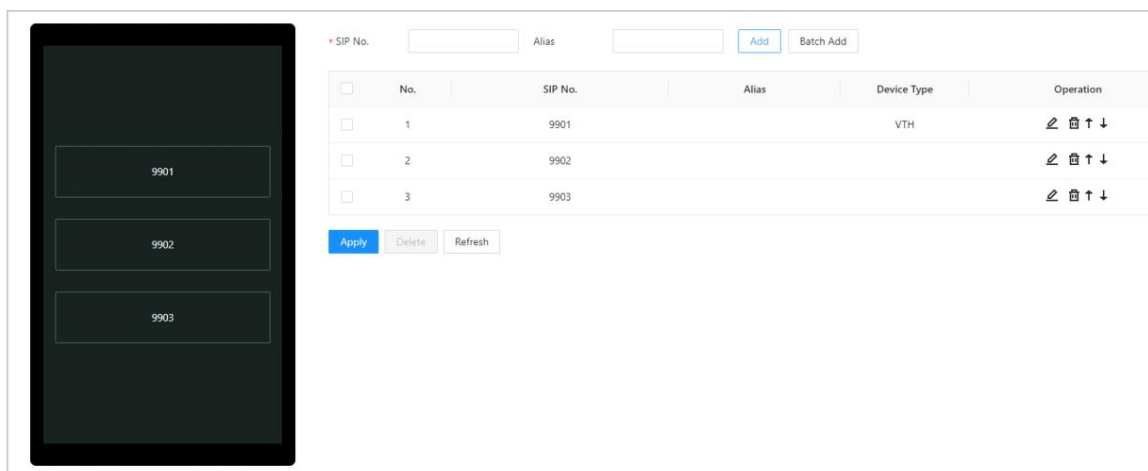
Процедура

Шаг 1. На веб-странице выберите «Настройки домофона» > «Простой режим».



- 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 3-32 Простой режим



Шаг 2. Добавляйте VTH и VTS по одному или партиями.

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.

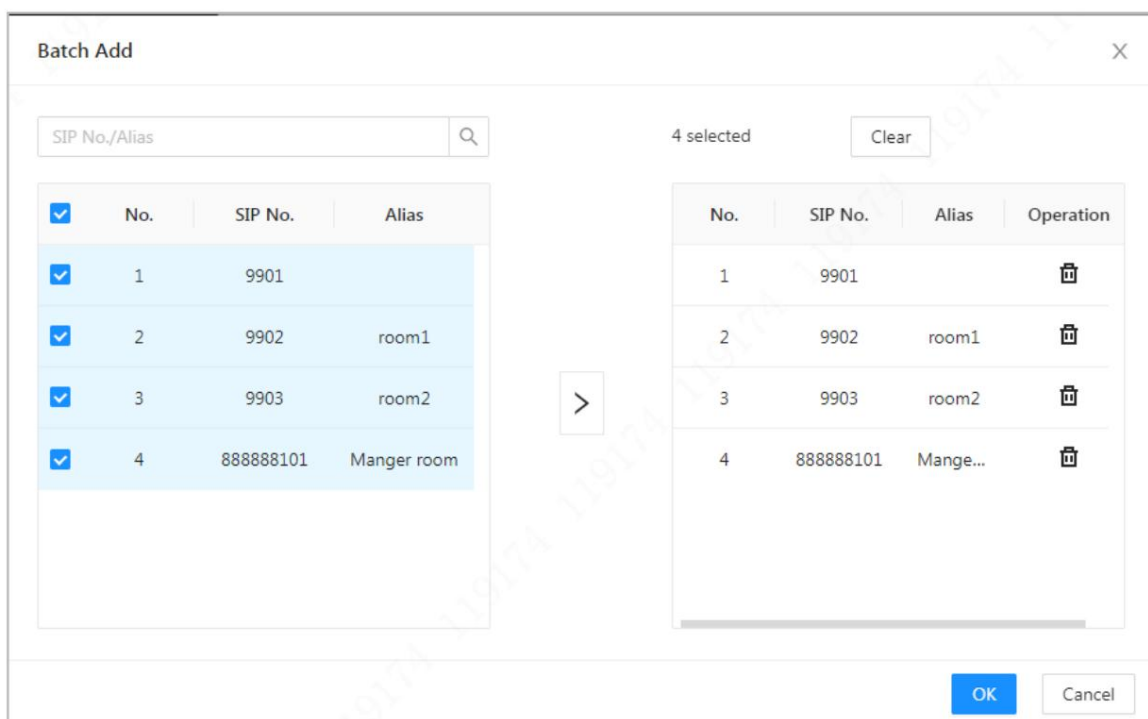
• Добавляйте по одному: введите SIP-номер и нажмите «Добавить». • Добавляйте

партиями: эта функция доступна только в том случае, если устройство установлено в качестве SIP-сервера, а VTH и VTS добавлены к SIP-серверу на странице настроек устройства.

1. Нажмите «Пакетное добавление».

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

Рисунок 3-33. Добавлять партиями.



Шаг 3 (необязательно) Нажмите . Вы можете изменить порядок устройств или просто перетащить их в окне предварительного просмотра.

Связанные операции

- Нажмите, чтобы отредактировать псевдоним устройства.
- Нажмите, чтобы удалить устройство.

3.8 Настройка учета посещаемости

Эта функция доступна только на некоторых моделях.

3.8.1 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 3-34. 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.

3.8.2 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 3-35. Создание сдвигов.

Edit Shift

X

* Shift No.

1

* Shift Name

* Period 1

08:00:00 → 17:00:00

⌚

* Period 2

00:00:00 → 00:00:00

⌚

* Overtime Period

00:00:00 → 00:00:00

⌚

* Limit for Arriving Late

5

min (0-99)

* Limit for Leaving Early

5

min (0-99)

OK

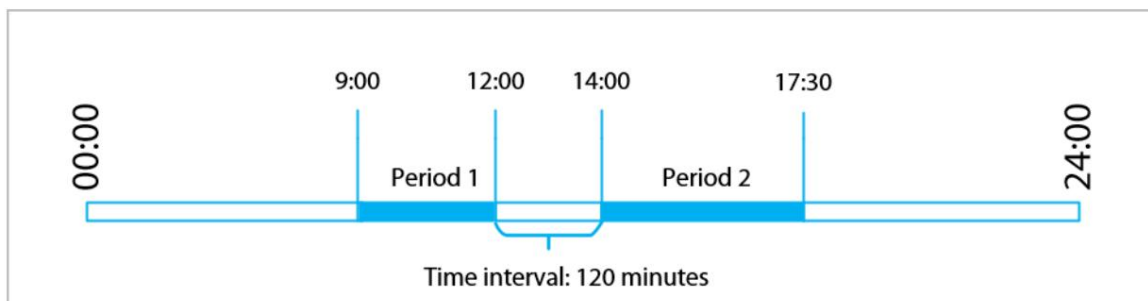
Cancel

Таблица 3-21. Описание параметров переключения.

Параметр	Описание
Название смены	Введите название смены.
Период 1	Укажите временной промежуток, в течение которого сотрудники могут отмечать начало и конец рабочего дня.
Период 2	Если вы установите только один период учета рабочего времени, сотрудники должны отмечать начало и конец рабочего дня в установленное время, чтобы избежать ошибок в их таблице учета рабочего времени. Например, если вы установите 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 установите два периода посещаемости, эти два периода не могут перекрываться. Сотрудники должны отмечать время прихода и ухода с работы в оба периода.
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 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 3-36. Временной интервал (четное число).



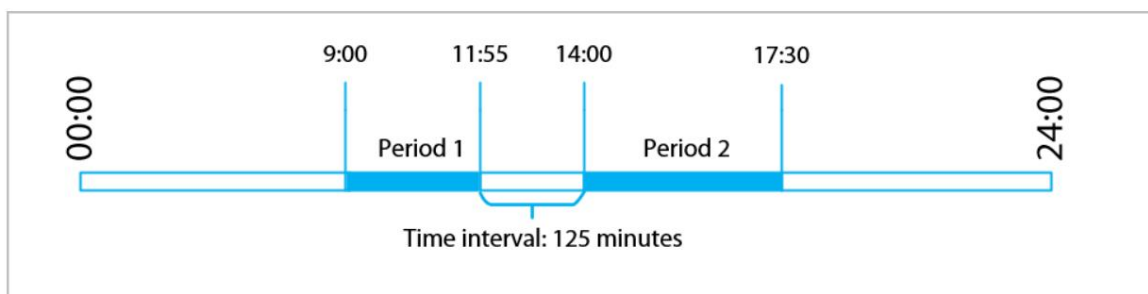
Например: если интервал составляет 120 минут, то время окончания работы в период 1 — с 12:00 до 12:59, а время начала работы в период 2 — с 13:00 до 14:00.



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 3-37. 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.



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.

Связанные операции

Вы можете нажать кнопку «По умолчанию», чтобы восстановить заводские настройки переключения передач.

3.8.3 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 3-38. Создание планов на праздники.

Add Attendance Holiday

* Attendance Holiday ...

1

* Attendance Holiday

Attendance Holiday for October

* Time

2023-10-01 → 2023-10-07

OK

Cancel

Таблица 3-22. 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.

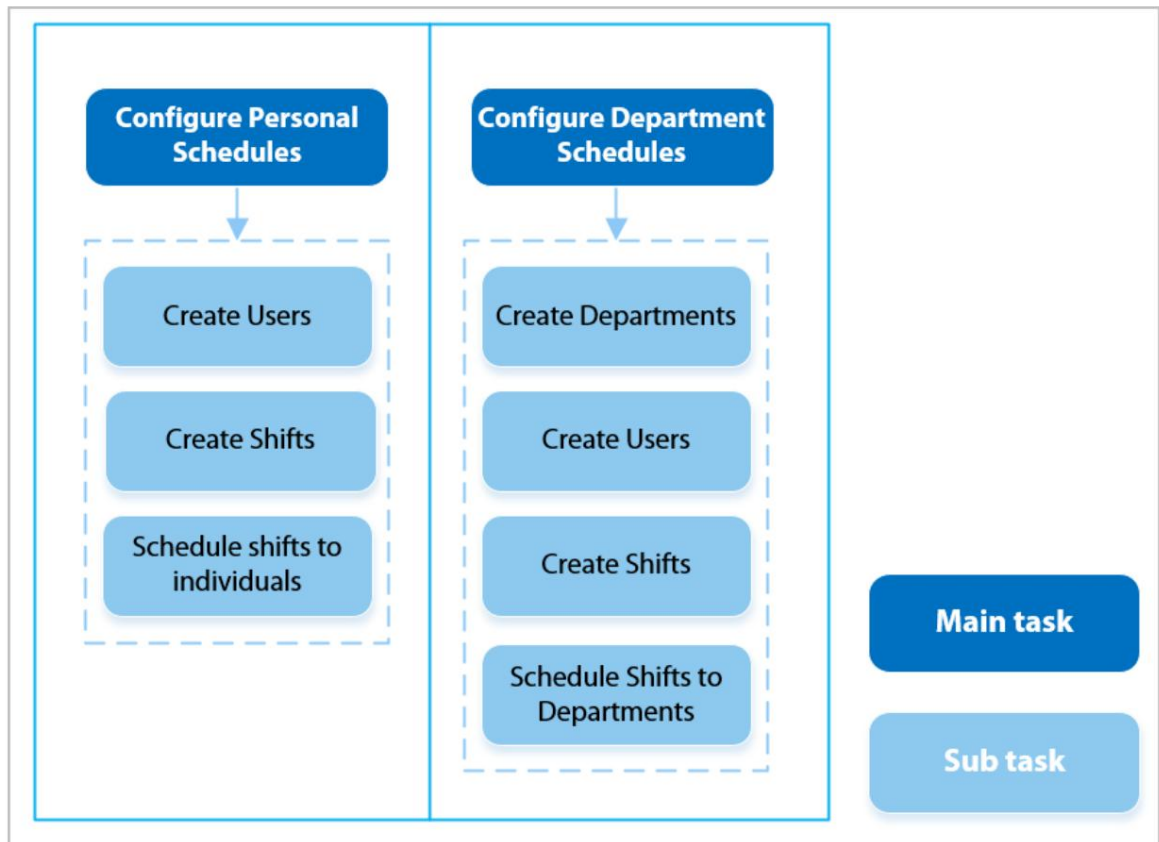
3.8.4 Настройка графиков работы

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.

Рисунок 3-39. 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 3-40. Личное расписание.



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

• 0 означает перерыв. •

От 1 до 24 указывает количество заданных смен. Инструкции по настройке смен см. в разделе "2.10.2 Настройка смен". • 25 означает командировку. • 26 означает отпуск.

Шаг 3. Составьте графики работы для отделов.

1. Нажмите «Расписание отдела».

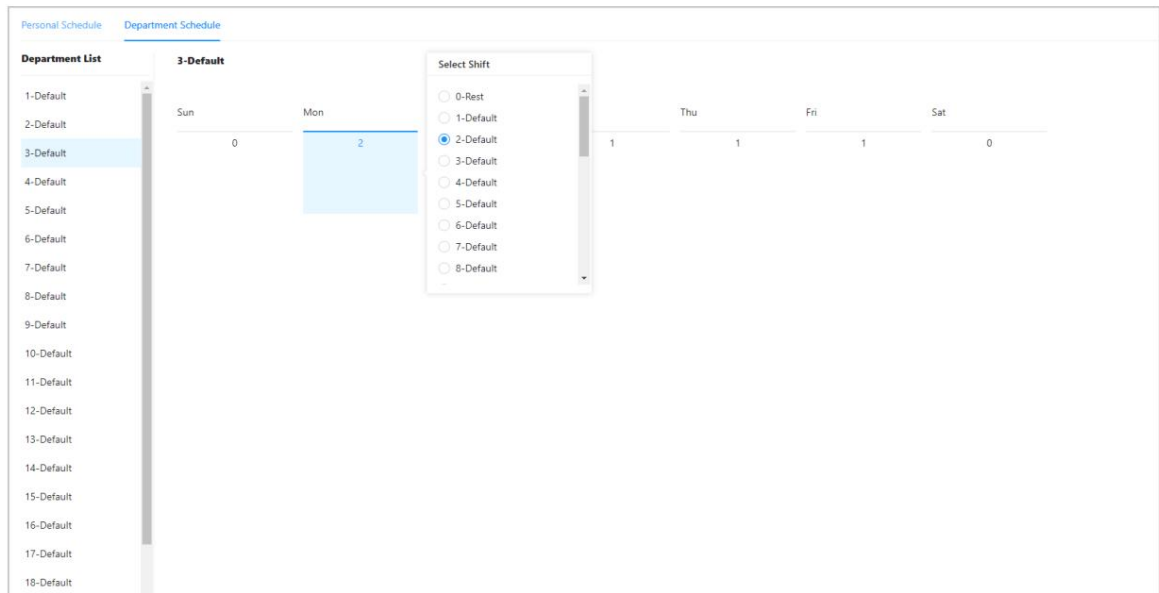
2. Выберите отдел из списка отделов.

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

• 0 означает отдых.

• Цифры от 1 до 24 указывают количество заданных смен. Инструкции по настройке смен см. в разделе "2.10.2 Настройка смен". • 25 означает командировку. • 26 означает отпуск.

Рисунок 3-41. График смен в отделе.



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

3.8.5 Настройка режимов учета посещаемости

Процедура

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

Шаг 2. Введите интервал проверки.

Если сотрудник несколько раз отмечает время прихода и ухода в течение установленного интервала, будет считаться действительным самое раннее время.

Шаг 3. Включите локальный или удаленный режим, а затем выберите режим учета посещаемости.

Шаг 4. Настройка режимов учета посещаемости.

Рисунок 3-42 Режимы посещаемости

Local or Remote

Mode Settings

Auto/Manual Mode

Auto ModeManual ModeFixed 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

Apply

Refresh

Default

Таблица 3-23 Режим 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. • Начало работы: Отметьте начало вашего обычного рабочего дня. • Окончание работы: Отметьте окончание вашей работы, когда начнется ваш перерыв. • Начало работы: Отметьте окончание вашей работы, когда закончится ваш перерыв. • Окончание работы: Отметьте окончание вашей обычной работы. • Начало работы после сверхурочной работы: Отметьте начало вашего сверхурочного периода. • Окончание работы после 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. • Начало работы: Отметьте начало вашего обычного рабочего дня. • Окончание работы: Отметьте окончание вашей работы, когда начнется ваш перерыв. • Начало работы: Отметьте окончание вашей работы, когда закончится ваш перерыв. • Окончание работы: Отметьте окончание вашей обычной работы. • Начало работы после сверхурочной работы: Отметьте начало вашего сверхурочного периода. • Окончание работы после 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 5. 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.

3.9 Настройка аудио и видео

3.9.1 Настройка видео

На главной странице выберите «Настройка аудио и видео» > «Видео», а затем настройте параметры видео.

Справочная информация • Номер

- канала: Канал 1 предназначен для настройки изображения в видимом свете. Канал 2 предназначен для настройки изображения в инфракрасном свете.
- По умолчанию: Восстановить настройки по умолчанию.
- Снимок: Сделать снимок текущего изображения.

3.9.1.1 Настройка канала 1

Процедура

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

Шаг 2. Выберите 1 из списка номеров каналов.

Шаг 3. Настройте битрейт.

Рисунок 3-43 Курс даты

Channel No. 1

Bit Rate

Status

Exposure

Image

Main Stream

Resolution 720P

Frame Rate (FPS) 25

Bit Rate 2Mbps

Compression H.264

Sub Stream

Resolution VGA

Frame Rate (FPS) 25

Bit Rate 1024Kbps

Compression H.264

Default Snapshot

Таблица 3-24. 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 через интернет-соединение за определенный промежуток времени. Выберите подходящую пропускную способность 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 4. Настройте статус.

Статус рисунка 3-44

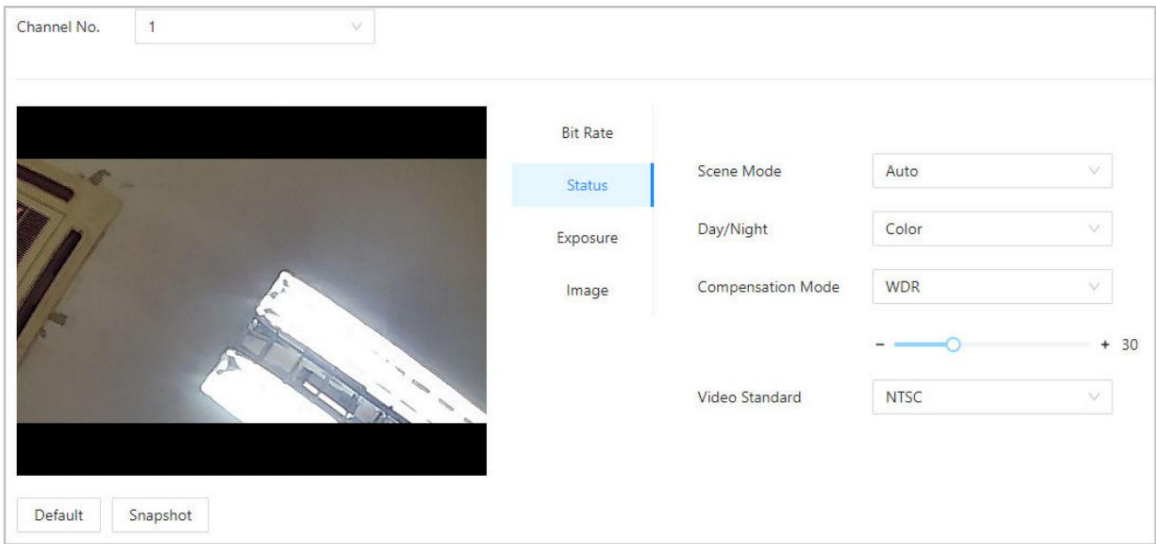


Таблица 3-25. Описание параметров состояния.

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.

Шаг 5. Настройте параметры экспозиции.

Рисунок 3-45. 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 3-26. 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 виде шум, 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 6. Настройте образ.

Рисунок 3-46 Изображение

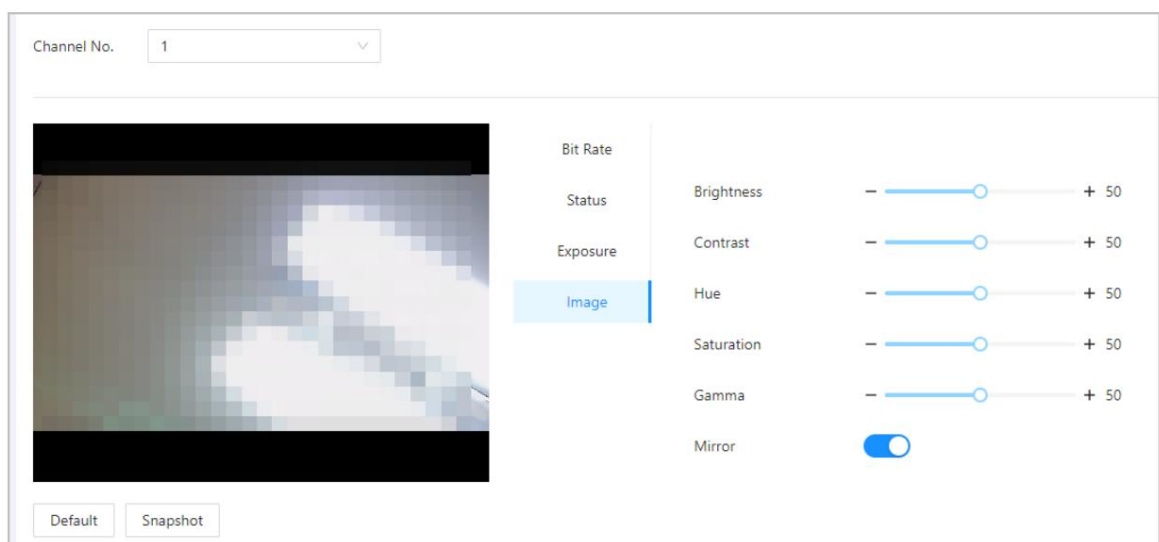


Таблица 3-27. Описание изображения.

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.
Зеркало	При включении этой функции изображения будут отображаться с перевернутыми левой и правой сторонами.

3.9.1.2 Настройка канала 2

Процедура

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

Шаг 2. Выберите 2 из списка номеров каналов .

Шаг 3. Настройте статус видео.



Мы рекомендуем включать функцию WDR, когда лицо находится под контровым светом.

Рисунок 3-47. Состояние конфигурации.

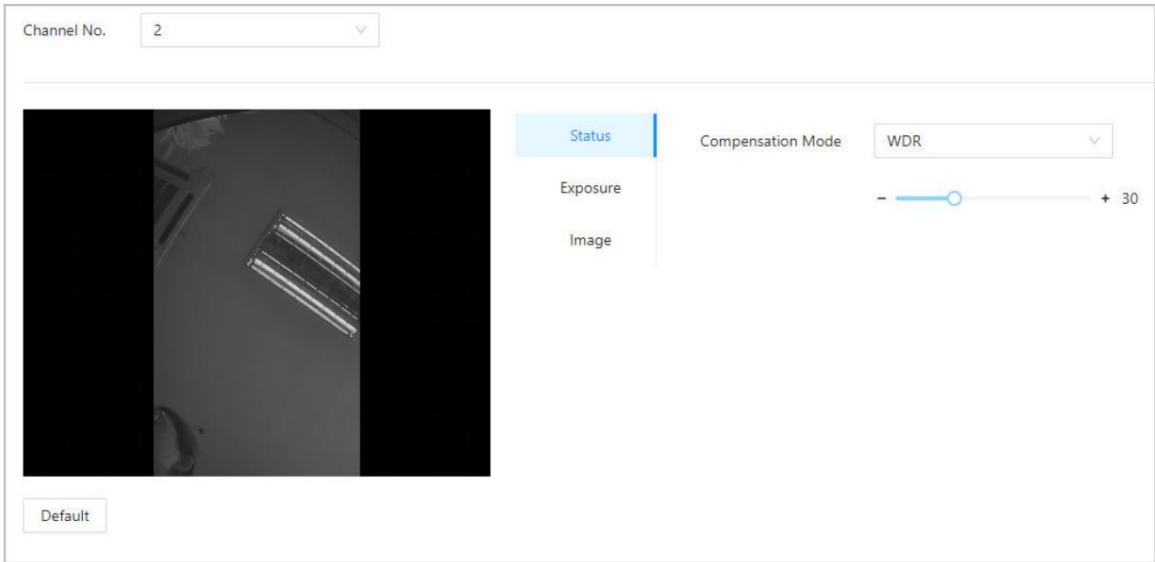


Таблица 3-28. Описание статуса.

Параметр	Описание
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.

Шаг 4. Настройте параметры экспозиции.

Рисунок 3-48. Параметр экспозиции.

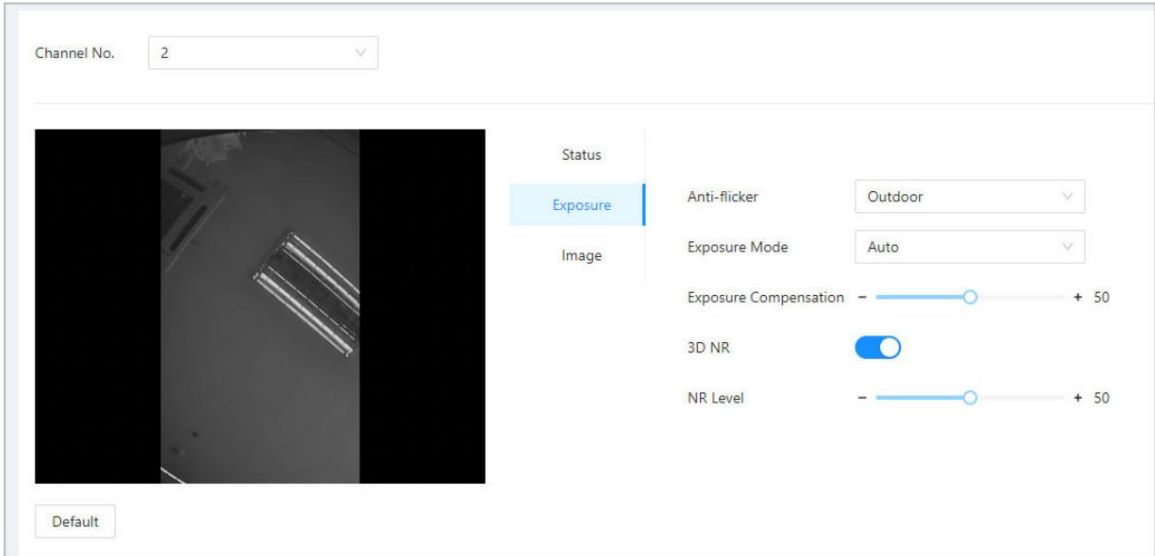


Таблица 3-29. Описание параметров воздействия.

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.
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 параметры изображения.

Рисунок 3-49 Параметры изображения

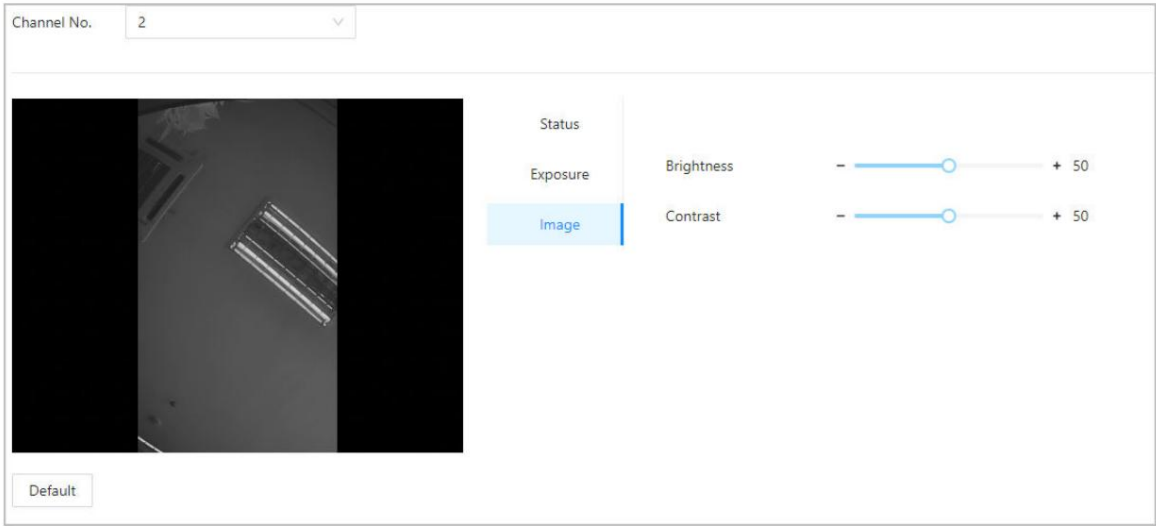


Таблица 3-30. Описание изображения.

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.

3.9.2 Настройка аудиоподсказок

Настройте звуковые подсказки во время подтверждения личности.

Процедура

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

Шаг 2. Настройте параметры звука.

Рисунок 3-50. Настройка параметров звука.

Speaker Volume

80

(0-100) ?

Microphone Volume

90

(0-100) ?

Screen Tap Sound

Audio Collection

Enable

Only supports MP3 files that are less than 20 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

Таблица 3-31. Описание параметров.

Параметры	Описание
Спикер	Установите громкость динамика.
Громкость микрофона	Установите громкость микрофона.
Звук касания экрана	При включении этой функции сенсорные устройства будут выдавать Звук касания и устройства без сенсорного экрана будут имитировать работу мыши. Щелчок.
Аудиоколлекция	В этом случае запись звука во время видеозвонка производиться не будет. Функция не активирована.
Аудиофайл	Нажмите «Загрузить аудиофайлы на платформу».
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».

3.9.3 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».

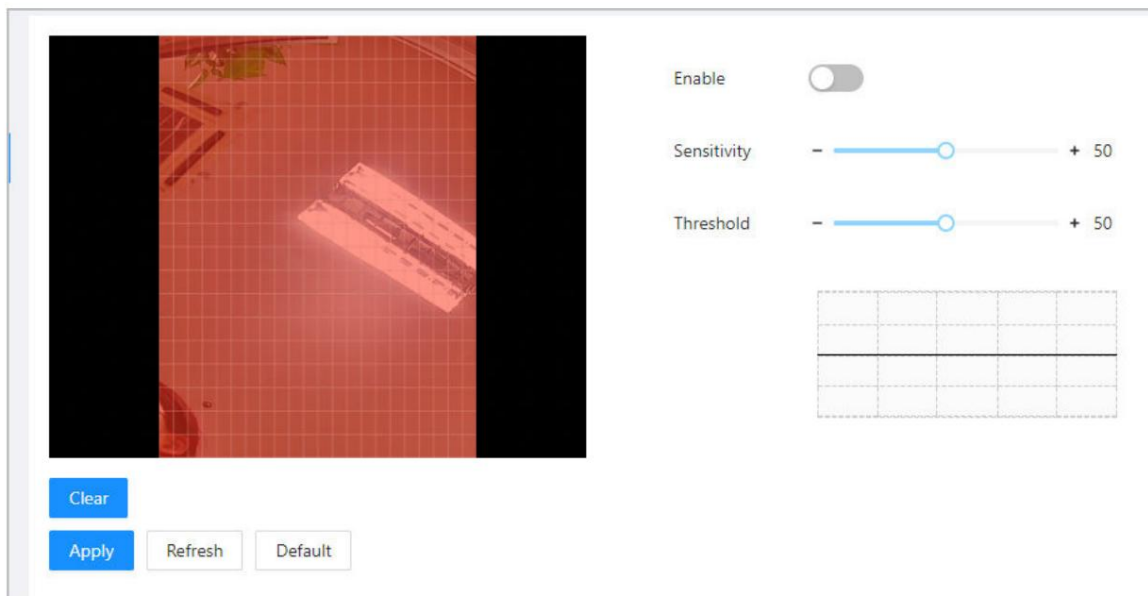
Шаг 2. Включите функцию обнаружения движения.

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 3-51. 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.

3.9.4 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 при отключении этой функции.

Процедура

Шаг 1. Войдите на веб-страницу.

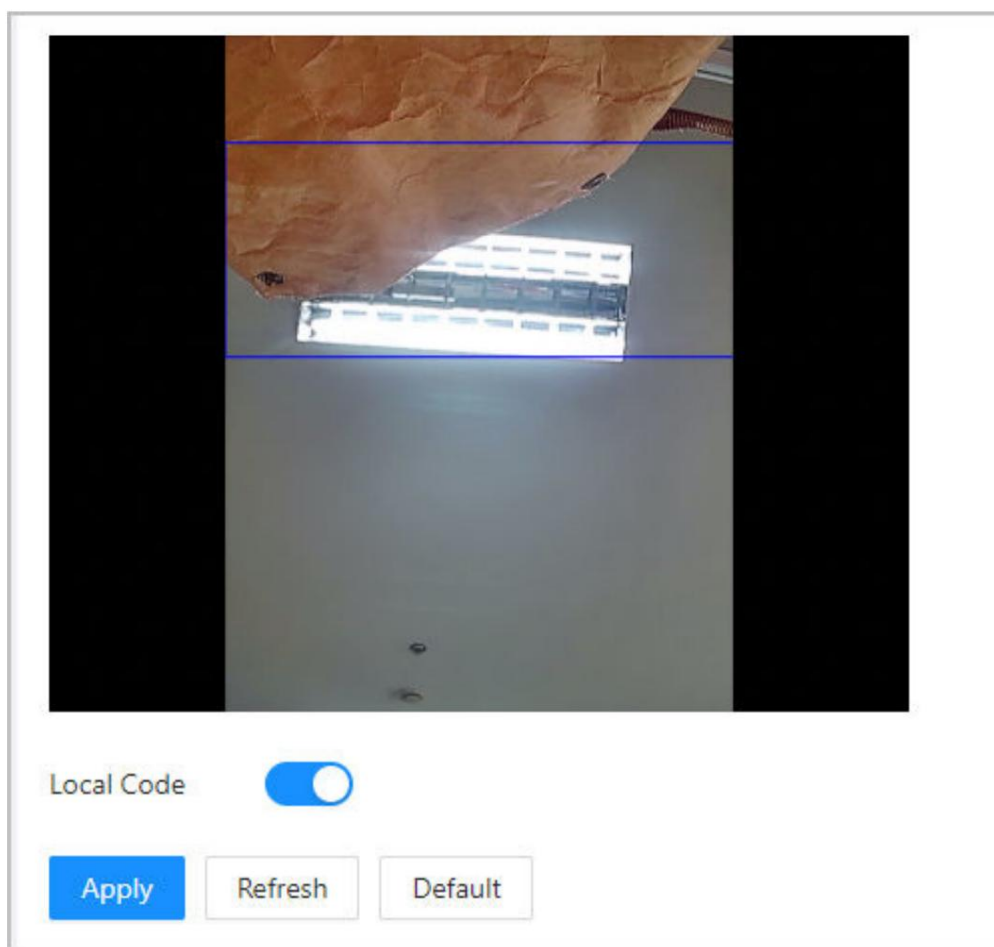
Шаг 2. Выберите «Настройка аудио и видео» > «Локальный код».

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

Шаг 4. Перетащите прямоугольник в указанное место.

В рамке указана область предварительного просмотра во время видеоконференции.

Рисунок 3-52 Локальное кодирование



Шаг 5. Нажмите «Применить».

3.10 Настройки связи

3.10.1 Сетевые настройки

3.10.1.1 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 3-53 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 3-32. 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, который может быть передан в одном сетевом пакете в компьютерных сетях. Более высокое значение MTU может повысить эффективность передачи данных по сети за счет уменьшения количества пакетов и связанных с этим сетевых накладных расходов. Если устройство на пути следования по сети не может обрабатывать пакеты определенного размера, это может привести к фрагментации пакетов или ошибкам передачи. В сетях Ethernet обычно используется значение MTU 1500 байт. Однако в некоторых случаях, например, при использовании PPPoE или VPN, могут потребоваться меньшие значения MTU для соответствия требованиям конкретных сетевых протоколов или служб. Ниже приведены рекомендуемые значения MTU для справки: 1500: Максимальное значение для пакетов Ethernet, также является значением по умолчанию. Это типичная настройка для сетевых подключений без PPPoE и VPN, некоторых маршрутизаторов, сетевых адаптеров и коммутаторов. 1492: Оптимальное значение для PPPoE 1468: Оптимальное значение для DHCP. 1450: Оптимальное значение для VPN.
Режим передачи	- Многоадресная рассылка: идеально подходит для видеозвонков. - Одноадресная передача: идеально подходит для групповых звонков.

Шаг 3. Нажмите OK.

3.10.1.2 Настройка Wi-Fi

Процедура

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

Шаг 2. Включите Wi-Fi.

Отображаются все доступные сети Wi-Fi.

Рисунок 3-54 Wi-Fi

Name	Signal Strength	Status	Connect
TP-LINK_CB8C	📶		+
DAHUA_Wireless	📶		+



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

Шаг 3. Нажмите  а затем введите пароль от сети Wi-Fi.

Wi-Fi подключен.

Связанные операции

- 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.

3.10.1.3 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.

Рисунок 3-55. Настройка портов.

Max Connection

1000

(1-1000)

TCP Port

37777

(1025-65534)

HTTP Port

80

HTTPS Port

443

RTSP Port

554

Apply

Refresh

Default



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

Таблица 3-33. 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».

3.10.1.4 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 3-56. 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 3-34. 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.  При включении протокола TLSv1.1 могут возникнуть риски безопасности. Просим принять это к сведению.
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».

3.10.1.5 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 3-57. Облачный сервис.

Enable



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

P2P Status

 Offline

PaaS Status

 Offline

SN

8 759



Apply

Refresh

Шаг 3. Нажмите «Применить».

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

3.10.1.6 Настройка автоматической регистрации

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».

Шаг 2. Включите функцию автоматической регистрации и настройте параметры.

Рисунок 3-58. Регистрация автомобиля.

Enable

Status

Offline

Server Address

172.5.2.7

Port

7000

(1-65535)

Registration ID

none

Apply

Refresh

Default

Таблица 3-35. 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».

3.10.1.7 Настройка активных 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» > «CGI active».
регистры.

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

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

Рисунок 3-59 Активная регистрация CGI

Edit

Enable

Device ID

none

Address Type

Host IP

Host IP

10 . . 10

Port

60005

HTTPS

OK

Cancel

Таблица 3-36. Описание автоматической регистрации.

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

Шаг 4. Нажмите «Применить».

3.10.1.8 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 3-60 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 3-37. 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 потребуется имя пользователя и пароль.
Чётный тип	Выберите тип события, которое будет отправлено на платформу управления. • Перед использованием этой функции включите функцию «Отправка информации о человеке». • Информация о человеке может быть отправлена только одному человеку. Платформа управления и записи о разблокировке могут передаваться на несколько платформ управления.

Шаг 5. Нажмите «Применить».

3.10.2 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 3-61. Настройка параметров.

External Device

Turnstile

Baud Rate

9600

Data Bit

8

Stop Bit

1

Parity Code

None

Apply

Refresh

Default

Таблица 3-38. Настройка формата Wiegand.

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: Выводит данные на основе номера карты, когда пользователь проводит картой для разблокировки двери; выводит данные на основе первого номера карты пользователя при использовании других способов разблокировки. ◇ №: Выводит данные на основе идентификатора пользователя. • 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: Кнопка выхода, замок и противопожарная система не работают после включения модуля безопасности. • Турникет: Когда устройство подключается к турникету, а плата контроллера доступа турникета подключается к внешнему модулю QR-кода или модулю считывания карт, плата передает данные для проверки на турникет.
Бит данных	Количество бит, используемых для передачи фактических данных в последовательном канале связи. Оно представляет собой двоичные цифры, несущие передаваемую информацию.

Параметр	Описание
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».

3.10.3 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 3-62. 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 3-39. 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 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».

3.11 Настройка системы

3.11.1 Управление пользователями

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

3.11.1.1 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.

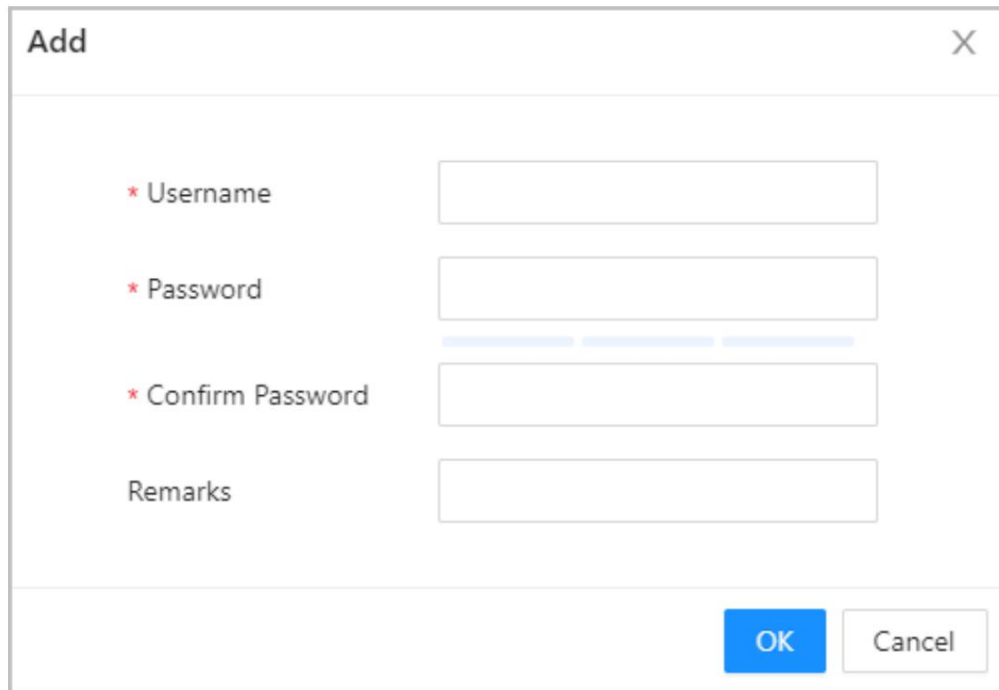
Шаг 2. Нажмите «Добавить» и введите информацию о пользователе.



- 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 3-63. 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 followed by the text: "Username", "Password", and "Confirm Password". The fourth field is labeled "Remarks". At the bottom right of the dialog, 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.

3.11.1.2 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 3-64. Добавить пользователя ONVIF.

Add

*

Username

*

Password

*

Confirm Password

*

Group

OK

Cancel

Таблица 3-40. 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 диспетчере устройств ONVIF. • Оператор: Вы не можете просматривать или управлять другими учетными записями пользователей в диспетчере устройств ONVIF. • Пользователь: Вы не можете просматривать или управлять учетными записями других пользователей и системными журналами в диспетчере устройств ONVIF.

Шаг 3. Нажмите OK.

3.11.1.3 Сброс пароля

Если вы забыли пароль, восстановите его через связанный 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 3-65 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».

3.11.1.4 Просмотр пользователей онлайн

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

3.11.2 Настройка времени

Процедура

Шаг 1. На главной странице выберите Система > Время.

Шаг 2. Настройте время на платформе.

Рисунок 3-66. Настройки даты.

Time and Time Zone



Date :

2023-05-30 Tuesday

Time :

16:18:35

Time

☒ Manually Set ☐ NTP

System Time

2023-05-30 16:18:35 

Sync PC

Time Format

YYYY-MM-DD 

24-Hour 

Time Zone

(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi 

DST

Enable

☐

Type

☒ Date ☐ Week

Start Time

01-01 00:00 

End Time

01-02 00:00 

Apply

Refresh

Default

Таблица 3-41. 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.
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».

3.11.3 Настройка сочетаний клавиш

Процедура

Шаг 1. На веб-странице выберите Система > Настройки ярлыков.

Шаг 2. Настройте параметры сочетания клавиш.

Рисунок 3-67 Настройки сочетаний клавиш

Password ☒
 QR Code ☒
 Doorbell ☒
 Local Device Ringer ☒
 Ringtone Config Ringtone 1 ▾
 Ringtone Time (sec) 3 (1-30)
 Call ☒
 Call Type Call Room ▾
 Mode Standard ▾
 Apply Refresh Default

Таблица 3-42. Описание параметров.

Параметр	Описание
Пароль	В режиме ожидания отображается значок способа разблокировки по паролю. экран.
QR-код	Значок QR-кода отображается на экране в режиме ожидания. Эта функция недоступна для устройств с автономным модулем QR-кода.
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. - Настройка мелодии звонка: выберите мелодию звонка • Время звонка (сек.): установите время звонка (1-30 секунд). Значение по умолчанию равно 3. Эта функция доступна только на некоторых моделях.
Вызов	Значок вызова отображается на экране ожидания.

Параметр	Описание
Тип вызова	• Номер комнаты: В режиме ожидания коснитесь значка вызова и введите номер комнаты для совершения звонка. • Центр управления вызовами: в режиме ожидания коснитесь значка вызова. а затем позвоните в центр управления. • Настройка номера комнаты: введите номер комнаты, после чего вы можете нажать на значок вызова на экране ожидания, чтобы позвонить по заранее заданному номеру комнаты.  Звонки в DMSS можно совершать только в рамках этого типа вызова.

3.12 Персонализация

Настройте темы оформления и добавьте видео- или графические ресурсы на устройство.

3.12.1 Добавление ресурсов

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

Справочная информация



Эта функция доступна только на некоторых моделях.

Процедура

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

Шаг 2. Добавьте видео или изображения.

Рисунок 3-68. Добавьте видео или изображения.

Video

● Supports AVI,DAV,MP4. Video size must be less than 100M.

Upload

No.	Name	Operation
1	A...p.dav	

Picture

● Supports PNG,JPG,BMP. Image size must be less than 2M.

+

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 локального хранилища 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.

3.12.2 Настройка тем оформления

Справочная информация



Эта функция доступна только на некоторых моделях.

Процедура

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

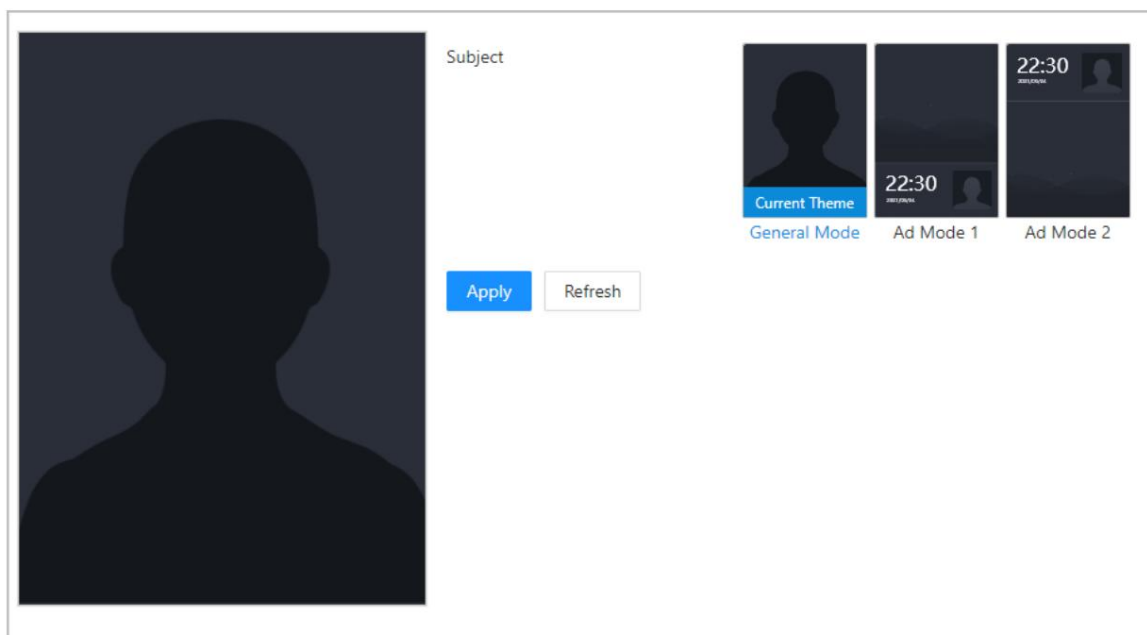
Шаг 2. Выберите тему.

- 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 — рекламные объявления.

Рисунок 3-69 Тема

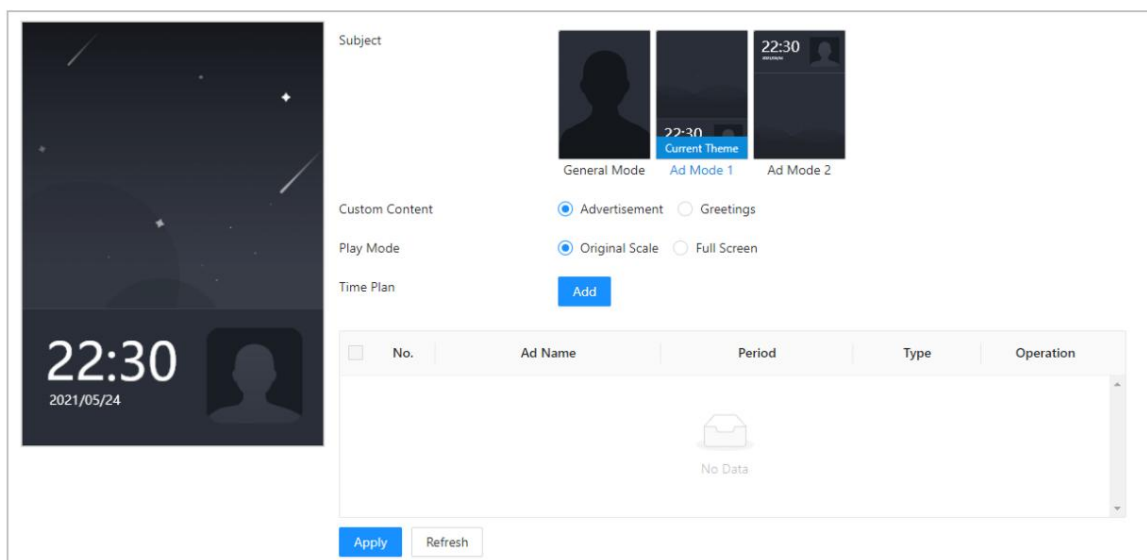


Шаг 3. Выберите голосовую подсказку для успешной проверки личности.

Шаг 4. Настройка отображения рекламы.

1. Выберите режим рекламы 1 или режим рекламы 2, а затем выберите «Реклама».

Рисунок 3-70 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 и нажмите «Применить».

Установите продолжительность воспроизведения одного изображения в цикле. Диапазон значений — от 1 до 20 секунд, по умолчанию — 5 секунд.

Рисунок 3-71. Добавить расписания.

Add

Ad Name

Ad 01

Period

00:00:00

-

23:59:59

Type

☒ Picture

☐ Video

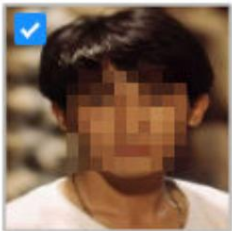
Duration

5

sec

Ad Resources

☒



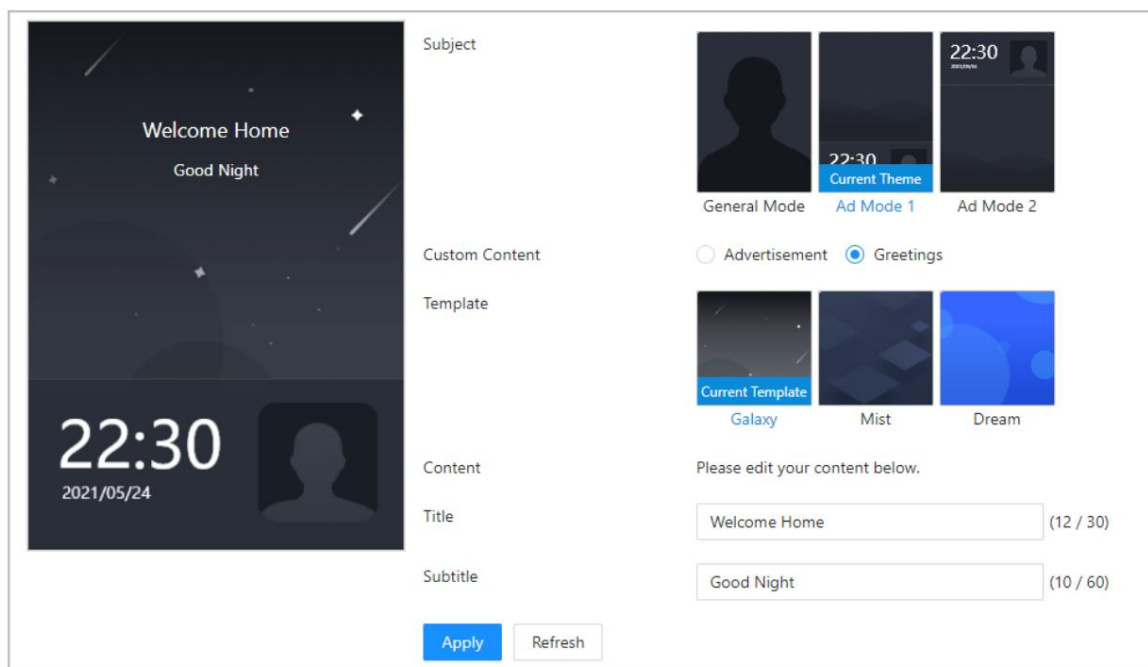
Apply

Cancel

Шаг 5. Настройка приветствий.

1. Выберите «Приветствие» в разделе «Пользовательский контент».
2. Выберите шаблон.
3. Введите заголовок и подзаголовок.

Рисунок 3-72 Приветствия



4. Нажмите «Применить».

3.13 Центр управления

3.13.1 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.

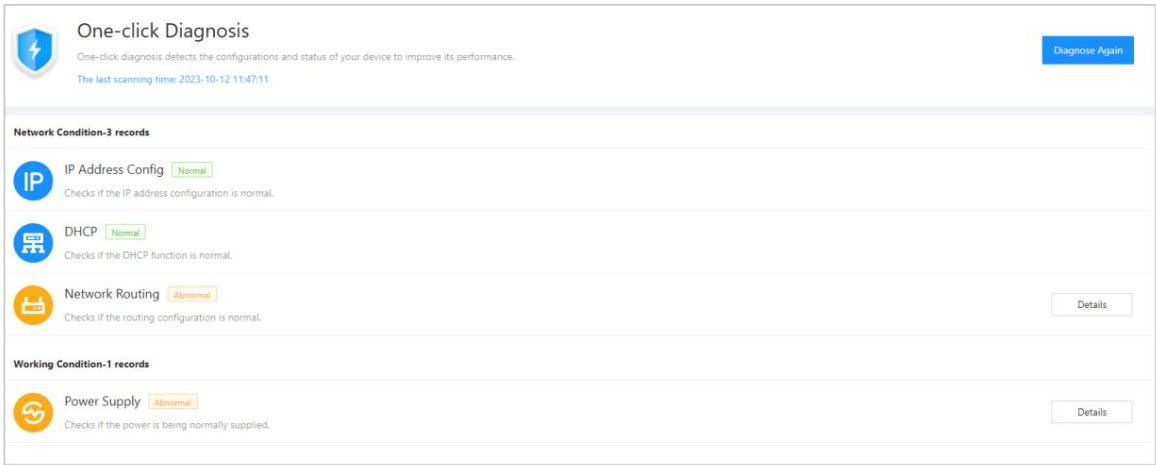
Шаг 2. Нажмите «Диагностика».

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 3-73. Диагностика одним щелчком мыши.



3.13.2 Информация о системе

3.13.2.1 Просмотр информации о версии

На веб-странице выберите Система > Версия, и вы сможете просмотреть информацию о версии устройства.

3.13.2.2 Просмотр юридической информации

На главной странице выберите «Система» > «Юридическая информация», и вы сможете ознакомиться с лицензионным соглашением на программное обеспечение, политикой конфиденциальности и уведомлением об открытом исходном коде.

3.13.3 Объем данных

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

Войдите на веб-страницу и выберите «Объем данных».

3.13.4 Журналы просмотра

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

3.13.4.1 Системные журналы

Просмотр и поиск системных журналов.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите 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  подробности журнала.

3.13.4.2 Разблокировка записей

Найдите записи о разблокировке и экспортируйте их.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Журнал > Разблокировать записи.

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

Для загрузки журнала нажмите кнопку «Экспорт» .

3.13.4.3 История звонков

Просмотреть журналы звонков.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Журнал > История звонков.

3.13.4.4 Журналы аварийных сигналов

Просмотреть журналы тревожных сообщений.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Журнал > Журнал тревог.

Шаг 3. Выберите тип и временной диапазон.

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

3.13.4.5 Журналы администратора

Найдите журналы администратора, используя его идентификатор.

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Журнал > Журнал администратора.

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

Нажмите «Экспорт», чтобы экспортировать журналы администратора.

3.13.4.6 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.

3.13.5 Управление конфигурацией

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

3.13.5.1 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 Система > Конфигурация.

Рисунок 3-74. 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.

3.13.5.2 Восстановление заводских настроек по умолчанию

Процедура

Шаг 1. Выберите Система > Конфигурация.



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

Шаг 2. При необходимости восстановите заводские настройки по умолчанию.

- Сброс к заводским настройкам : Сбрасывает все параметры устройства и удаляет все данные.
- Восстановление настроек по умолчанию (кроме информации о пользователе и журналов) : Сбрасывает параметры устройства.

Устройство удаляет все данные, кроме информации о пользователе и журналов.

3.13.6 Техническое обслуживание

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

Процедура

Шаг 1. Войдите на веб-страницу.

Шаг 2. Выберите Система > Обслуживание.

Шаг 3. Установите время, а затем нажмите «Применить».

Устройство перезагрузится в запланированное время, или вы можете нажать кнопку «Перезагрузить» , чтобы перезагрузить его немедленно.

3.13.7 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.

3.13.7.1 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.

3.13.7.2 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 версий.

- Выберите «Ручная проверка», и вы сразу сможете проверить, установлена ли последняя версия. доступный.

Шаг 3 (необязательно) Нажмите «Обновить сейчас» , чтобы немедленно обновить устройство.

3.13.8 Расширенное техническое обслуживание

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

3.13.8.1 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.

3.13.8.2 Захват пакетов

Процедура

Шаг 1. На главной странице выберите Центр обслуживания > Расширенное обслуживание > Пакет.
Захватывать.

Рисунок 3-75. 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	►

Шаг 2. Введите IP-адрес, нажмите .

 изменения в . 

Шаг 3. После того, как вы собрали достаточно данных, нажмите .

Захваченные пакеты автоматически загружаются на ваш локальный компьютер.

3.14 Настройки безопасности (необязательно)

3.14.1 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

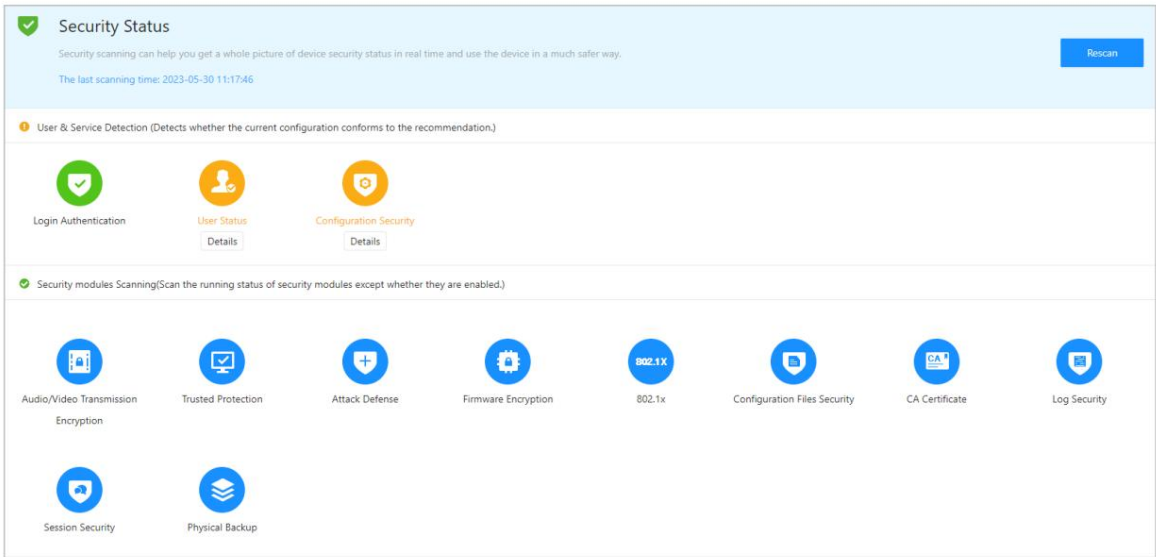
Шаг 1. Выберите >  Состояние безопасности.

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



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

Рисунок 3-76. 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 она не будет сканироваться. Обнаруженная аномалия «Игнорируется» будет выделено серым цветом.
- Нажмите «Оптимизировать», чтобы устранить проблему.

3.14.2 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 >  Системная служба > HTTPS.

Шаг 2. Включите службу HTTPS.



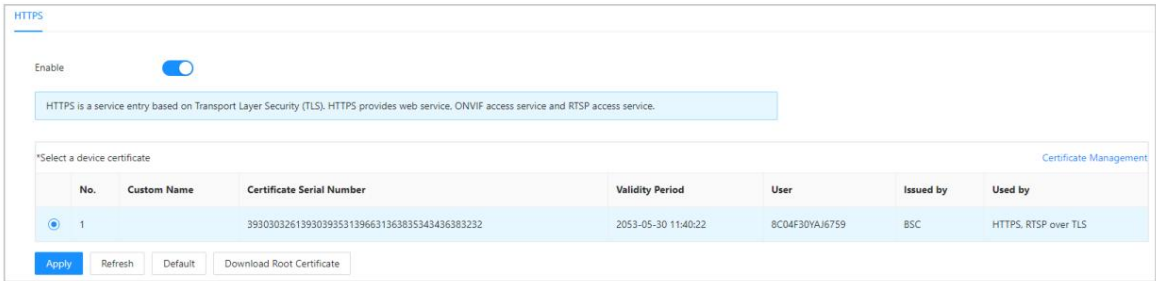
Если включить параметр "Совместимость с TLS v1.1 и более ранними версиями", могут возникнуть риски для безопасности. Обращаем ваше внимание.

Шаг 3. Выберите сертификат.



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

Рисунок 3-77 HTTPS



Шаг 4. Нажмите «Применить».

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

3.14.3 Атака Защита

3.14.3.1 Настройка брандмауэра

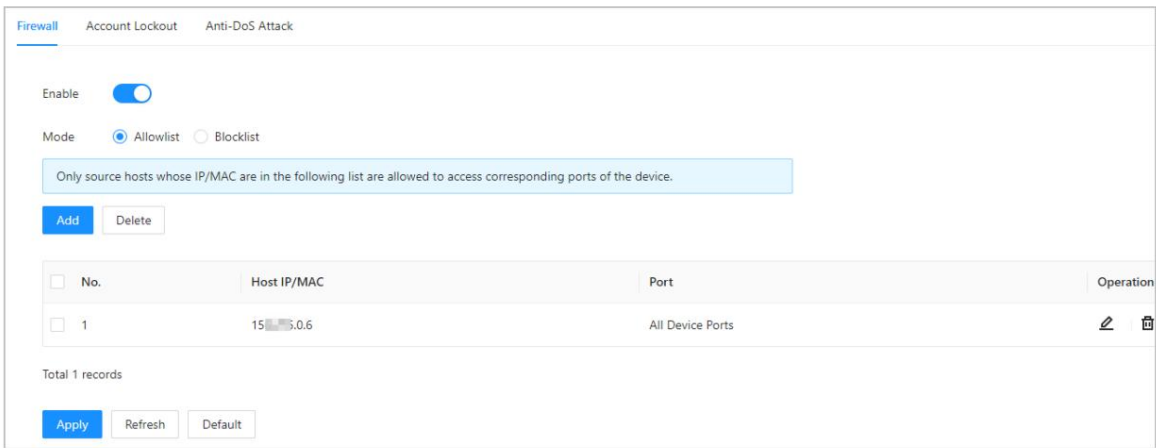
Настройте брандмауэр для ограничения доступа к устройству.

Процедура

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

Шаг 2. Нажмите, чтобы включить функцию брандмауэра.

Рисунок 3-78 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 3-79. Добавить информацию об IP-адресе.

The 'Add' dialog box is shown with the following fields and controls:

- Add Mode:** A dropdown menu with 'IP' selected.
- IP Version:** A dropdown menu with 'IPv4' selected.
- IP Address:** A text input field with three dots (.) as a placeholder.
- All Device Ports:** A toggle switch that is currently turned on (blue).
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Шаг 5. Нажмите OK.

Связанные операции

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

3.14.3.2 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 3-80 Блокировка учетной записи

Firewall **Account Lockout** Anti-DoS Attack

Device Account

Login Attempt 5time(s) ▾

Lock Time 5 min

Apply Refresh Default

- 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».

3.14.3.3 Настройка защиты от DoS-атак

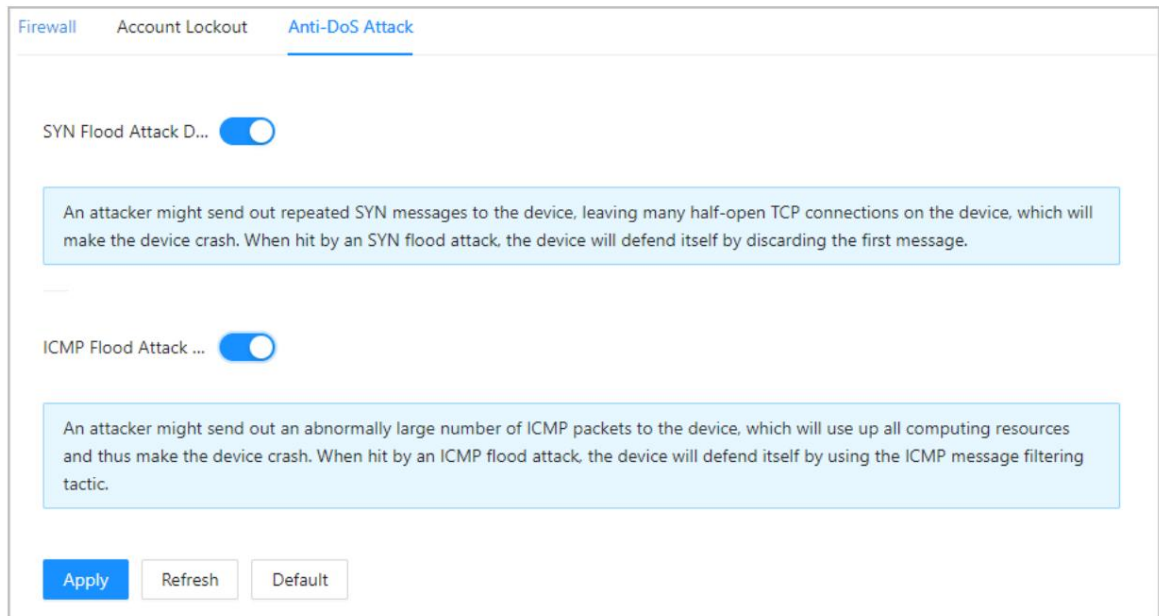
Для защиты устройства от DoS-атак можно включить защиту от SYN-флуд-атак и защиту от ICMP-флуд-атак .

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 3-81. Защита от DoS-атаки.



Шаг 3. Нажмите «Применить».

3.14.4 Сертификат на устанавливаемое устройство

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

3.14.4.1 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 3-82. 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.

3.14.4.2 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 3-83 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 "17[redacted]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.

3.14.4.3 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 3-84. Сертификат и закрытый ключ.

The image shows a Windows-style dialog box titled "Step 2: Select certificate and private key." with a close button (X) in the top right corner. Inside the dialog, there are four labeled input fields arranged vertically: "Custom Name", "Certificate Path", "Private Key", and "Private Key Password". To the right of the "Certificate Path" and "Private Key" fields are "Browse" buttons. At the bottom of the dialog, there are three buttons: "Back", "Import and Install" (which is highlighted in blue), and "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.

3.14.5 Установка сертификата доверенного 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.

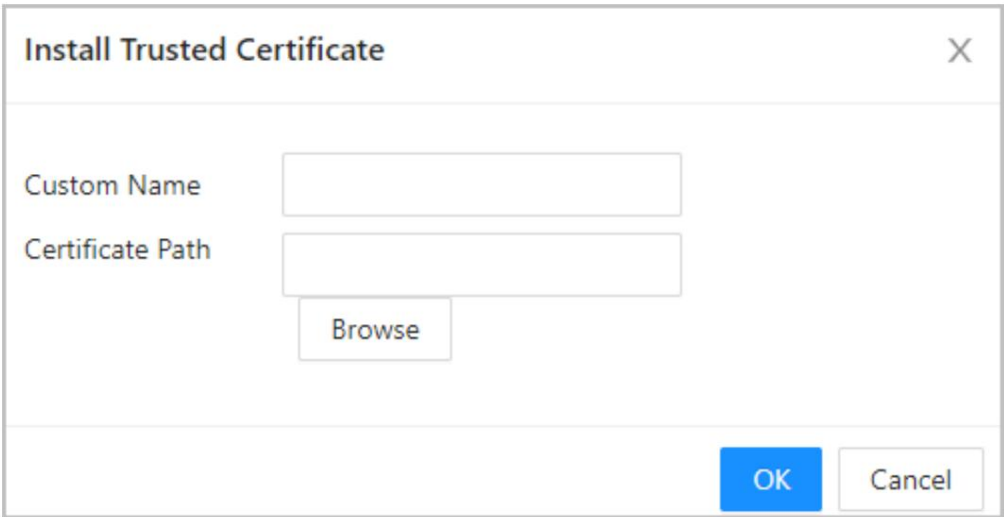
Процедура

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 3-85. 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.

3.14.6 Шифрование данных

Процедура

Шаг 1. Выберите > Шифрование данных.

Шаг 2. Настройте параметры.

Рисунок 3-86 Шифрование данных

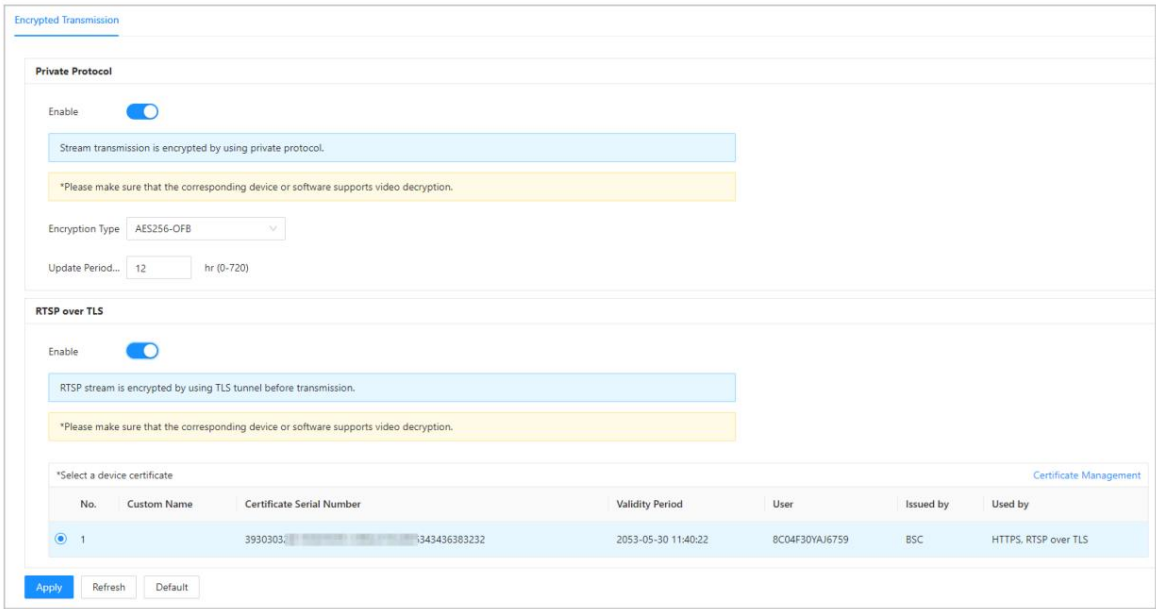


Таблица 3-43. Описание шифрования данных.

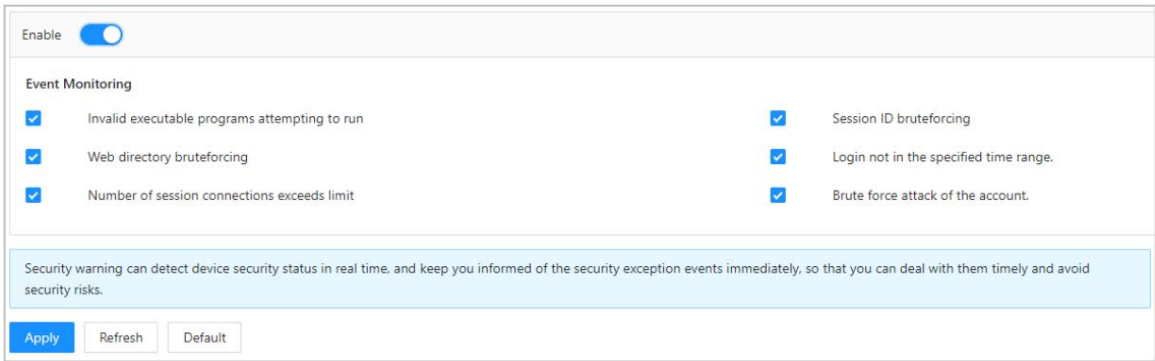
	Параметр	Описание
Частный протокол	Дать возможность	Передача потоков данных осуществляется с использованием частного протокола и шифруется во время передачи.
	Тип шифрования	Оставьте значение по умолчанию.
	Период обновления секретности Ключ	Диапазон значений от 0 ч до 720 ч. 0 означает, что секретный ключ никогда не будет обновляться.
RTSP поверх TLS	Дать возможность	Поток RTSP шифруется во время передачи через туннель TLS.
		Создайте или импортируйте сертификат. Подробности см. в разделе «Управление сертификатами» в разделе «3.14.4 Установка сертификата устройства». Установленные сертификаты отображаются в списке.

3.14.7 Предупреждение о безопасности

Процедура

- Шаг 1. Выберите > Предупреждение безопасности.
- Шаг 2. Включите функцию предупреждения системы безопасности.
- Шаг 3. Выберите элементы мониторинга.

Рисунок 3-87. Предупреждение о безопасности.



- Шаг 4. Нажмите «Применить».

3.14.8 Аутентификация безопасности

Процедура

- Шаг 1. Выберите Безопасность > Аутентификация безопасности.
- Шаг 2. Выберите алгоритм хэширования сообщения.
- Шаг 3. Нажмите «Применить».

Рисунок 3-88. Аутентификация безопасности.

Digest Algorithm for Authentication

Digest Algorithm for User Authentication ☒ MD5 ☐ SHA256

Digest Algorithm for ONVIF User Authentication ☒ MD5 ☐ SHA256

4 конфигурации 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.

4.1 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 забывания.

Шаг 3. Введите ваше имя пользователя и пароль для входа в Smart PSS Lite.

4.2 Добавление устройств

Необходимо добавить устройство в Smart PSS Lite. Добавлять их можно группами или по отдельности.

4.2.1 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 4-1. Добавление устройств.

Add Device

Device Name:

*

Method to add:

IP/Domain

IP/Domain:

*

Port:

*

37777

User Name:

*

Password:

*

Add and Continue

Add

Cancel

Таблица 4-1. 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.

4.2.2 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».

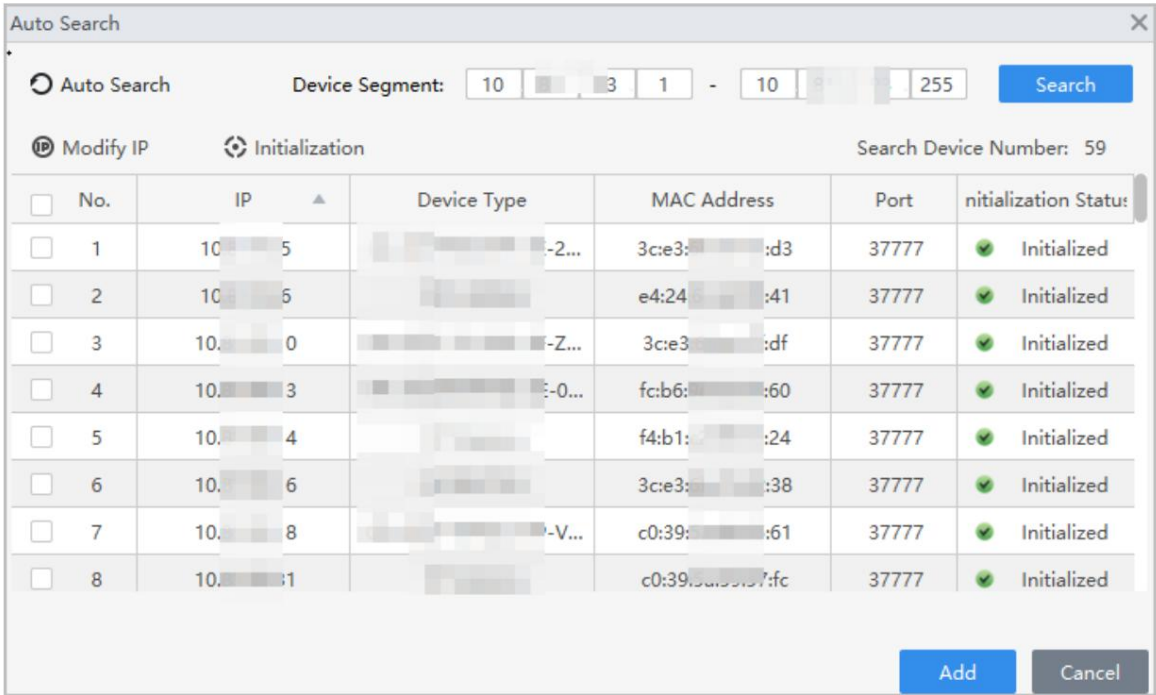
Шаг 2. Выберите метод поиска.

- 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 4-2. Поиск устройств.



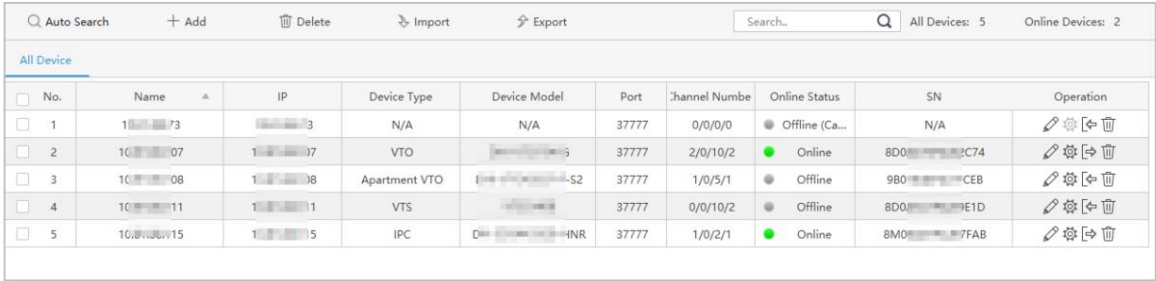
Шаг 3. Нажмите «Устройства», а затем нажмите «Добавить».

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 4-3. Добавленные устройства.



4.3 Управление пользователями

Добавляйте пользователей, назначайте им карточки и настраивайте их права доступа.

4.3.1 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 OK.

4.3.2 Добавление пользователей

4.3.2.1 Добавление пользователей по одному

Процедура

Шаг 1. Выберите «Кадры» > «Менеджер по кадрам» > «Добавить».

Шаг 2. Введите основную информацию о сотрудниках.

1. Выберите «Основные сведения».
2. Добавьте основную информацию о сотрудниках.
3. Сделайте снимок экрана или загрузите изображение, а затем нажмите «Готово».



- Номер карты может быть считан автоматически или введен вручную. Для автоматического считывания номера карты выберите считыватель карт рядом с полем «Номер карты», а затем поместите карту на считыватель. Номер карты будет считан автоматически.

- Вы можете выбрать несколько USB-камер для съемки фотографий.

- Установите пароль

Нажмите «Добавить», чтобы добавить

пароль. • Настройте карту

а. Щелкните, чтобы выбрать устройство или эмитента карты в качестве считывателя карт.

б. Добавьте карты. в. После добавления вы можете выбрать карту в качестве основной или принудительной, заменить карту новой или удалить карту.

г. Нажмите, чтобы отобразить QR-код карты.



QR-код карты может отображаться только при вводе 8-значного номера карты в шестнадцатеричном формате.

Настройка отпечатка пальца

- а. Щелкните, чтобы выбрать «Устройство» или «Сканер отпечатков пальцев» в качестве устройства для сбора отпечатков пальцев. б. Добавьте отпечаток пальца. Выберите «Добавить» > «Добавить отпечаток пальца», а затем трижды подряд прижмите палец к сканеру.

Рисунок 4-4. Добавьте основную информацию.

Add User

Basic Info | Extended information | Permission

User ID: *

Name: *

Department: Default Company

User Type: General User

Validity Time: 2022/11/29 0:00:00 2032/11/29 23:59:59 3654 Days

Times Used: Unlimited

Take Snapshot Upload Picture Image Size: 0-100 KB

Take Snapshot Upload Picture Image Size: 0-100 KB

Take Snapshot Upload Picture Image Size: 0-100 KB

Password Add ! For the 2nd-generation access controller, 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
☐		

Add More Finish Cancel

Шаг 3. Нажмите «Дополнительная информация», чтобы добавить расширенные данные о персонале, а затем нажмите «Готово», чтобы сохранить.

Рисунок 4-5. Дополнительная информация.

The screenshot shows a 'Add User' dialog box with three tabs: 'Basic Info', 'Extended information' (selected), and 'Permission'. The 'Extended information' tab contains a 'Details' section with the following fields:

- Gender: ☒ Male ☐ Female
- ID Type:
- Title:
- ID No.:
- Date of Birth:
- Company:
- Tel:
- Occupation:
- Email:
- Employment Date:
- Mailing Address:
- Termination Date:
- Administrator: ☒
- Remark:

At the bottom right, there are three buttons: 'Add More', 'Finish', and 'Cancel'.

Шаг 4. Настройка прав доступа.

1. Нажмите  .
2. Введите название группы, примечания (необязательно) и выберите временной шаблон.
3. Выберите методы проверки и двери.

Шаг 5. Настройка разрешений. Подробности см. в разделе «4.3.3 Назначение прав доступа».

1. Выберите группу.
2. Введите название группы, примечания (необязательно) и выберите временной шаблон.
3. Выберите методы проверки и двери.
4. Нажмите OK.

Рисунок 4-6. Настройка групп разрешений.

Add Permission Group

Basic Info

Group Name
Permission Group4

Remark:

Time Templ...
Full-day Time Te

Verification Method:
☒ Card
☒ Fingerprint
☒ Password
☒ Face

All Device
Selected (1)

Search..

☒ Default Group

☒ 172.16.1.140

☒ Door 1

172.16.1.140-Door 1

OK
Cancel

Шаг 6. Нажмите «Готово».



После завершения добавления вы можете щелкнуть, чтобы изменить информацию или добавить подробности в список сотрудников.

4.3.2.2 Добавление пользователей пакетами

Процедура

Шаг 1. Нажмите «Менеджер по персоналу» > «Пакетное обновление» > «Пакетное добавление».

Шаг 2. Выберите эмитента карты или устройство из списка устройств , а затем настройте параметры.

Рисунок 4-7. Добавление пользователей партиями.

Batch Add

Device

Card Issuer

Read C...

Start No.:

* 3789

Quantity:

* 20

Department:

Default Company

Validity Period:

2023/9/25 0:00:00

Expiration Time:

2029/9/25 23:59:59

Issue Card

ID	Card No.
3789	
3790	
3791	
3792	
3793	
3794	
3795	
3796	
3797	
3798	
3799	

OK

Cancel

Таблица 4-2. Параметры добавления пользователей партиями.

Параметр	Описание
Начальный номер	Идентификатор пользователя начинается с заданного вами числа.
Количество	Количество пользователей, которых вы хотите добавить.
Отделение	Выберите отдел, к которому принадлежит пользователь.
Время действия/Время истечения срока действия	Пользователи могут разблокировать дверь в течение установленного периода времени.

Шаг 3. Нажмите «Прочитать номер карты» и проведите картой по считывателю.

Номер карты будет считан автоматически.

Шаг 4. Нажмите ОК.

4.3.3 Назначение прав доступа

Создайте группу разрешений, представляющую собой набор разрешений доступа к дверям, а затем свяжите пользователей с ними. группа, чтобы пользователи могли открывать двери, связанные с этой группой разрешений.

Процедура

Шаг 1. Нажмите «Доступ к решению» > «Менеджер по персоналу» > «Разрешения».

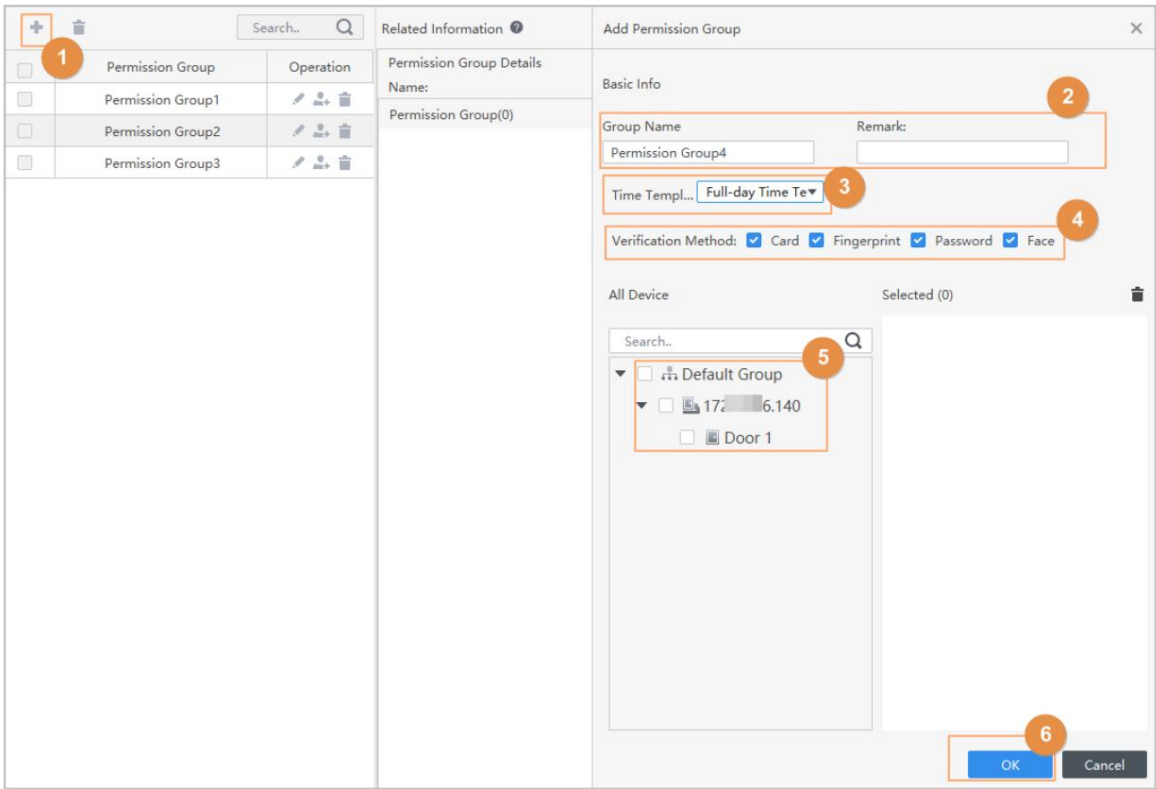
Шаг 2. Нажмите.  .

Шаг 3. Введите название группы, примечания (необязательно) и выберите временной шаблон.

Шаг 4. Выберите методы проверки и двери.

Шаг 5. Нажмите ОК.

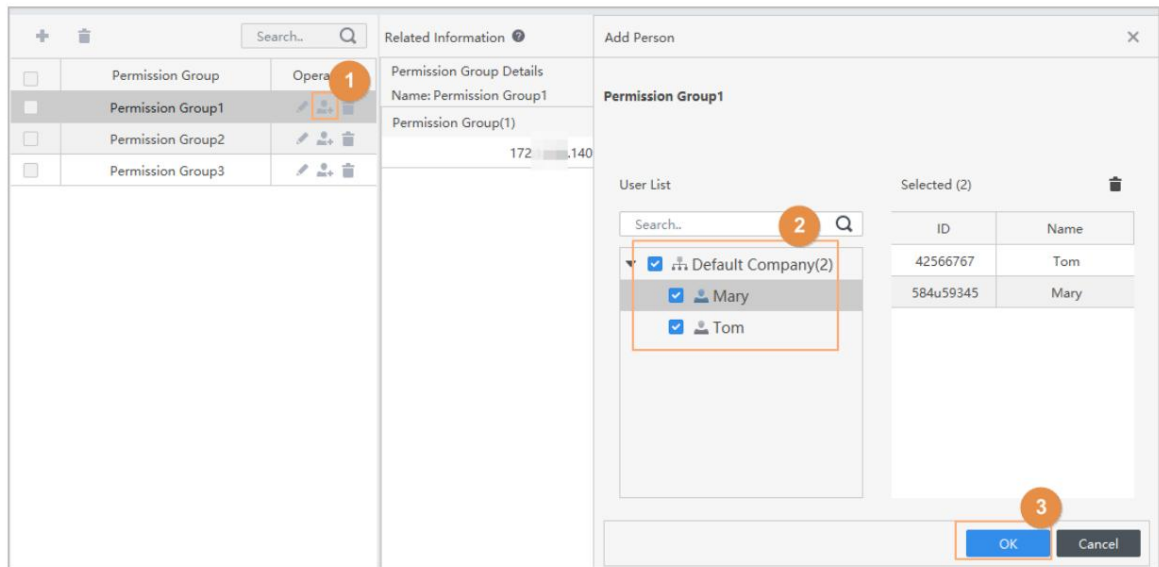
Рисунок 4-8. Создание группы разрешений.



Шаг 6. Щелкните по группе разрешений.

Шаг 7. Выберите пользователей, чтобы связать их с группой разрешений.

Рисунок 4-9. Добавление пользователей в группу разрешений.



Шаг 8. Нажмите OK.

Пользователи, входящие в эту группу разрешений, могут разблокировать дверь после подтверждения личности.

4.3.4 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 OK.

Рисунок 4-10. Создание группы разрешений.

Add Access Group

Basic Info

Group Name: Remark:

Permission Group3

Time Template: All Day Time Template

All Device

Search...

Default Group

1 3

Door 1

Selected (0)

OK Cancel

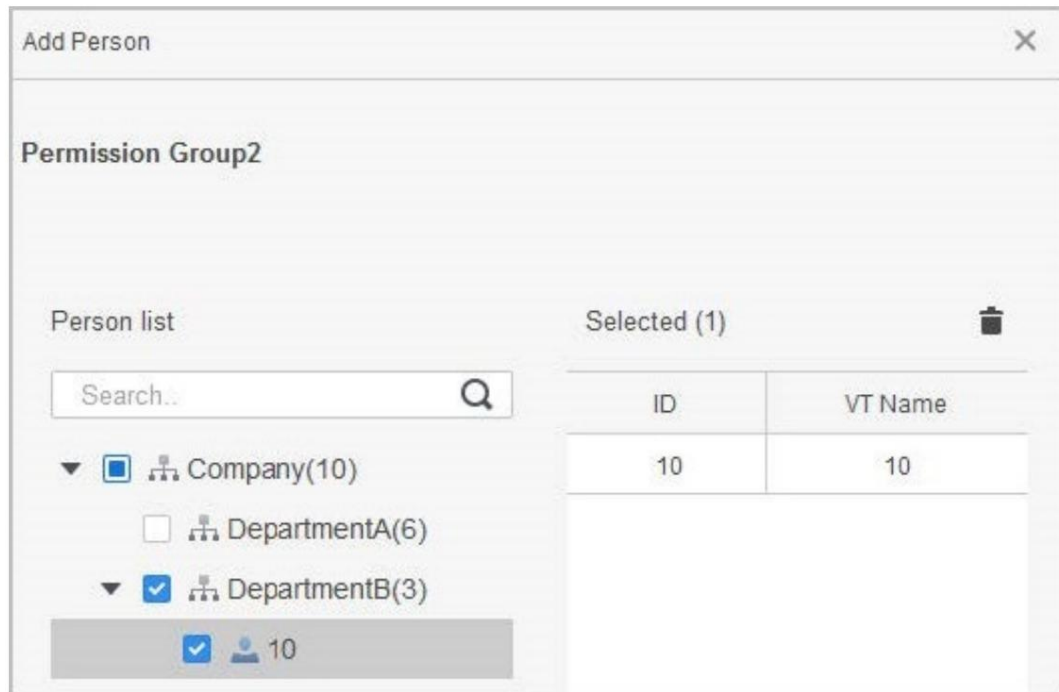


- Система учета рабочего времени поддерживает регистрацию прихода/ухода с помощью пароля, а также распознавание лиц.
Система учета рабочего времени по картам и отпечаткам пальцев.
- На некоторых моделях доступна система учета рабочего времени с использованием карт и отпечатков пальцев.

Шаг 7. Щелкните по добавленной вами группе разрешений.

Шаг 8. Выберите пользователей, чтобы связать их с группой разрешений.

Рисунок 4-11. Добавление пользователей в группу разрешений.



Шаг 9. Нажмите OK.

4.4 Управление доступом

4.4.1 Дистанционное открытие и закрытие двери

С помощью платформы вы можете удаленно контролировать и управлять дверью. Например, вы можете дистанционно открывать или закрывать дверь.

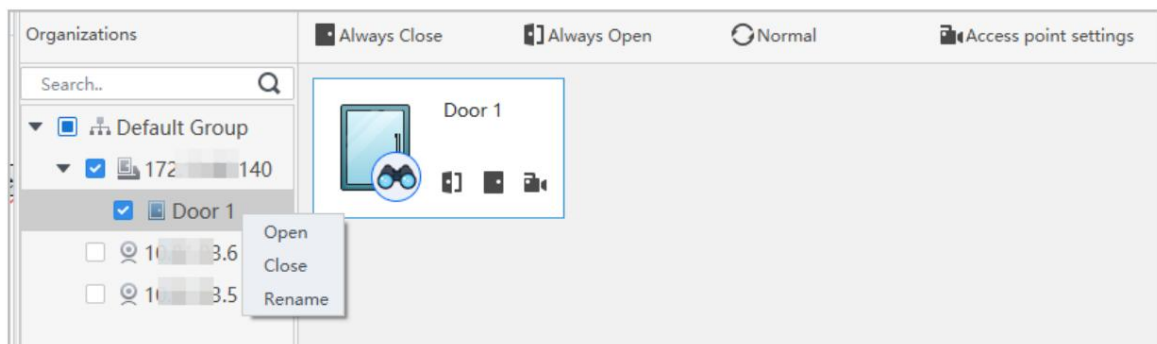
Процедура

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 4-12 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.

4.4.2 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 4-13. 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.

4.4.3 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-».

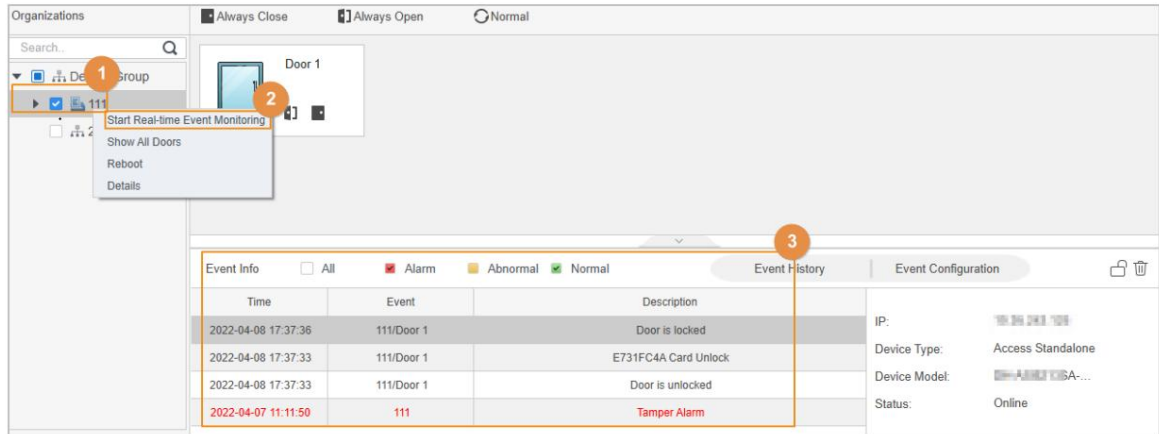
Мониторинг событий по времени.

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 4-14. 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 удалась. • Избегайте одновременного появления двух лиц в кадре.

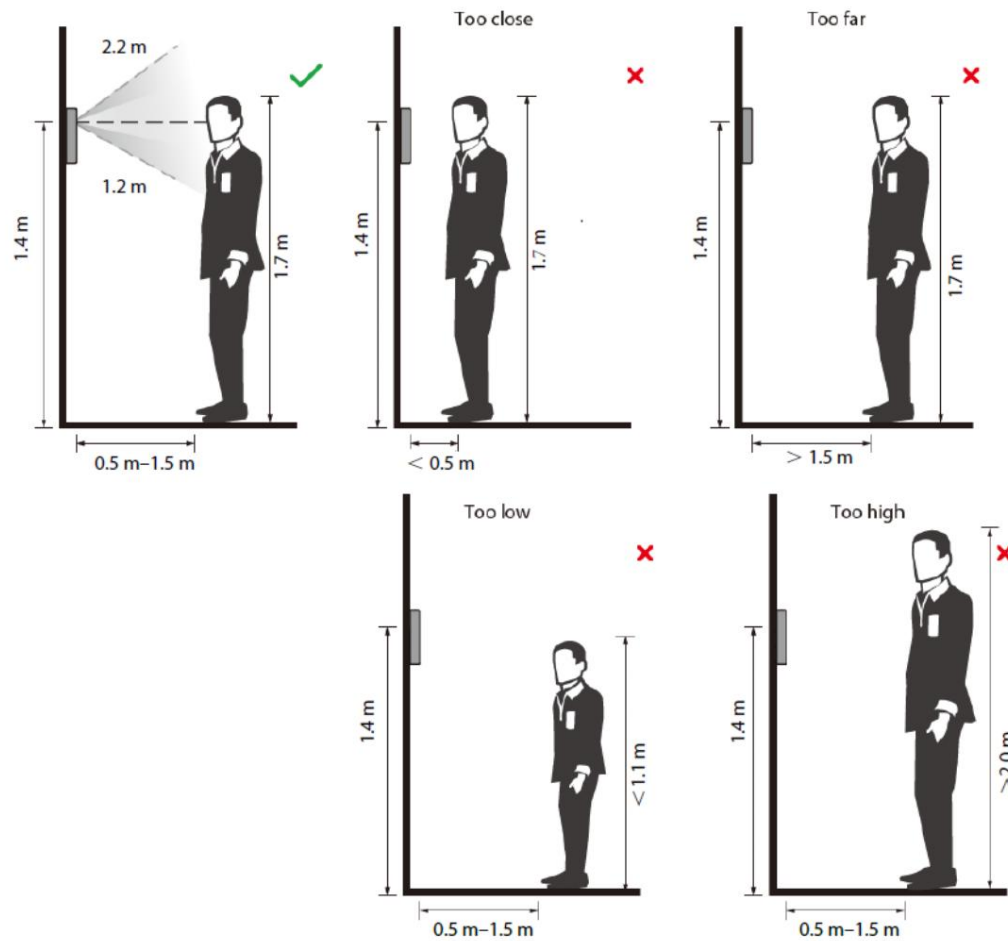
Положение лица

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 границами

Good



Too Close



Too Far



- 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 и VTO.

Процедура

Шаг 1. На экране ожидания коснитесь . 

Шаг 2. Войдите в комнату «Нет», а затем нажмите .

Приложение 3. Важные моменты, касающиеся отпечатков пальцев.

Инструкции по регистрации

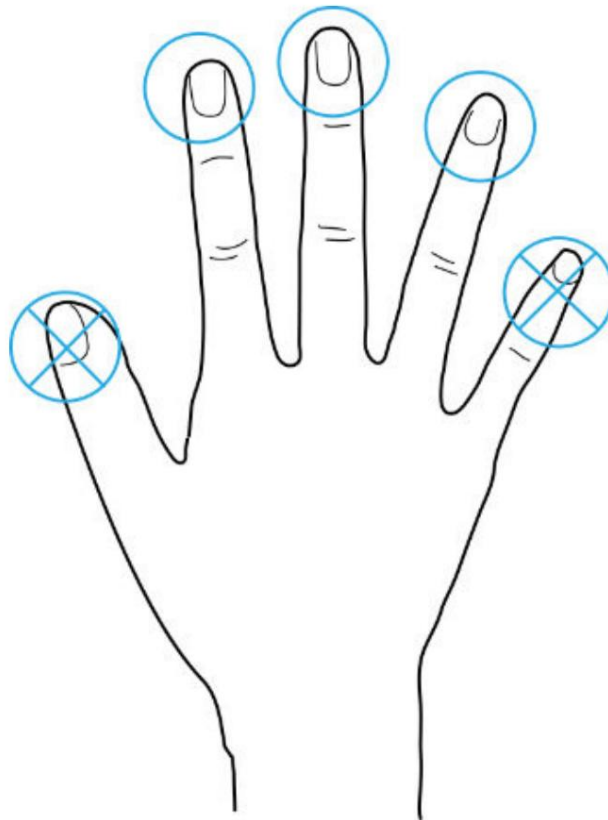
При регистрации отпечатков пальцев обратите внимание на следующие моменты:

- 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 влажностью.
- Если отпечатки пальцев нечеткие, используйте другие способы разблокировки.

Рекомендуется использовать пальцы.

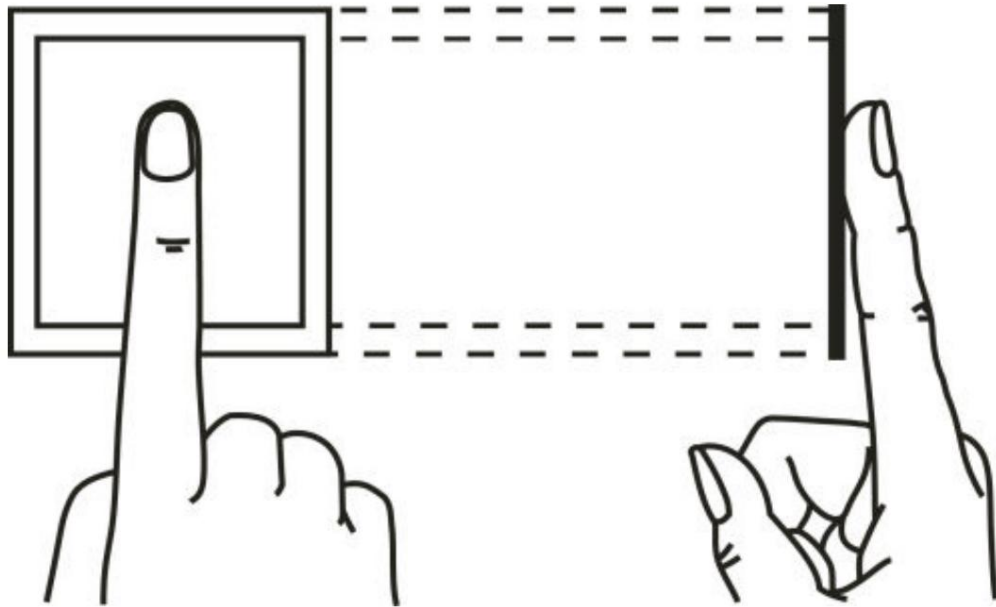
Рекомендуется использовать указательные, средние и безымянные пальцы. Большие пальцы и мизинцы будет сложно разместить в центре записи.

Приложение, Рисунок 3-1. Рекомендуемые пальцы.

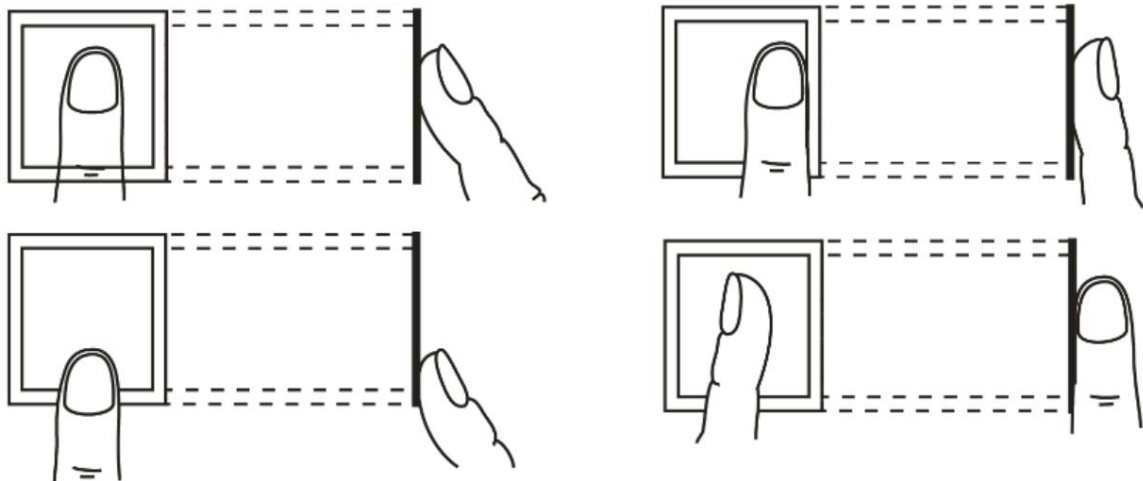


Как приложить отпечаток пальца к сканеру

Приложение, Рисунок 3-2. Правильное размещение.



Приложение, Рисунок 3-3. Неправильное размещение.



Приложение 4. Важные моменты, касающиеся QR-кода.

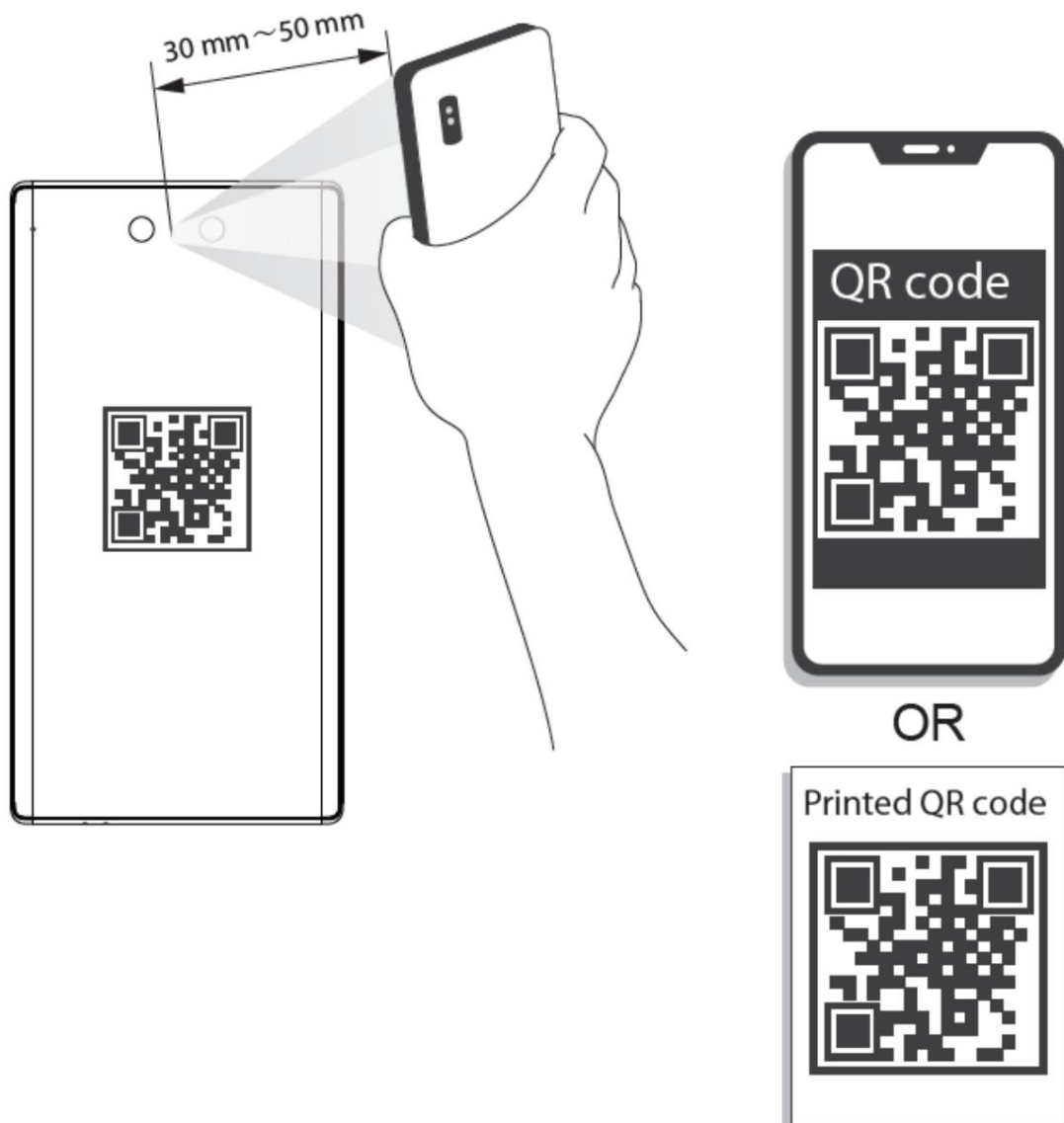
Сканирование

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. Включите 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 вашего 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 критически 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.