Контроллер охранной сигнализации

Руководство пользователя

ZHEJIANG DAHUA VISION TECHNOLOGY CO.LTD.

Версия 2.0.1

Важные меры предосторожности и предупреждения

В настоящем разделе описываются правила надлежащего обращения с устройством и меры по предотвращению опасностей, включая опасность причинения ущерба имуществу. Внимательно ознакомьтесь с содержимым данного раздела перед использованием устройства и соблюдайте указанные требования при работе с ним.

Требования к эксплуатации

- Перед использованием убедитесь, что источник питания устройства работает должным образом.
- Запрещается отсоединять шнур питания от устройства при включенном питании.
- Параметры электропитания устройства должны находиться в рекомендованном диапазоне.
- Транспортируйте, используйте и храните устройство при допустимых условиях влажности и температуры.
- Не допускайте попадания брызг или капель жидкости на устройство. Убедитесь, что на устройстве нет никаких предметов, наполненных жидкостью, которая может попасть внутрь устройства.
- Не разбирайте устройство.

Требования к установке

- Перед подачей питания сначала подключите блок питания к устройству.
- Строго соблюдайте местные стандарты электробезопасности и убедитесь, что напряжение в месте установки стабильно и соответствует требованиям к питанию устройства.
- Не подключайте устройство более чем к одному источнику питания. В противном случае устройство может быть повреждено.

- Соблюдайте все меры безопасности и используйте все необходимые при высотных работах средства защиты.
- Не подвергайте устройство воздействию прямого солнечного света или излучению источников тепла.
- Не устанавливайте устройство во влажных, пыльных или задымленных местах.
- Устанавливайте устройство в хорошо проветриваемом месте и не закрывайте вентиляционные отверстия устройства.
- Используйте только сетевой адаптер или блок питания, поставленный производителем устройства.
- Блок питания устройства должен соответствовать классу ES1 по стандарту IEC 62368-1 и иметь мощность не более чем для класса PS2. Рекомендованные параметры электропитания указываются на этикетке данного устройства.
- Электроприборы класса I следует подключать в розетки с защитным заземлением.

Введение

Общая информация

В настоящем руководстве пользователя описаны функции и работа контроллера охранной сигнализации (далее "устройство"). Внимательно ознакомьтесь с этим руководством перед использованием устройства. Сохраните настоящее руководство, чтобы при необходимости обращаться к нему в будущем.

Инструкции по технике безопасности

В руководстве могут встречаться следующие сигнальные слова.

Сигнальные слова	Значение
DANGER	Указывает на высокую потенциальную опасность, которая, если ее не предотвратить, может привести к гибели или к серьезным травмам.
WARNING	Указывает на среднюю или низкую потенциальную опасность, которая, если ее не предотвратить, может привести к травмам легкой или средней степени тяжести.
CAUTION	Указывает на потенциальную опасность, которая, если ее не предотвратить, может привести к причинению ущерба имуществу, потере данных, ухудшению рабочих характеристик или иным непредсказуемым результатам.
TIPS	Приводятся рекомендации, помогающие пользователю решить проблему или сэкономить время.
NOTE	Приводится дополнительная информация в качестве пояснения и добавления к тексту.

Информация об изменениях в документе

Версия	История изменений	Дата публикации
Версия 2.0.1	• Обновлена функция базовой настройки устройства. • Обновлена функция просмотра состояния. • Обновлена настройка функций контроллера. • Обновлена функция настройки проводной сети.	Апрель 2023 года
Версия 2.0.0	• Добавлены сетевые настройки. • Добавлены события и описания сбоев постановки на охрану. • Добавлены коды и описания событий протокола SIA.	Ноябрь 2022 года
Версия 1.1.0	• Добавлены действия в приложениях COS Pro и DMSS. • Добавлено управление пользователями. • Обновлены изображения. • Обновлены описания параметров.	Февраль 2022 года
Версия 1.0.0	Первая редакция	Октябрь 2021 года

Уведомление о защите конфиденциальности

В качестве пользователя устройства или контролера данных вы можете собирать персональные данные других людей, в частности, изображения лиц, отпечатки пальцев и автомобильные номера. Вы обязаны соблюдать требования соответствующих местных законов и нормативных актов о защите конфиденциальности для обеспечения законных прав и интересов других людей путем принятия мер, включающих, помимо прочего, следующее: использование четких и хорошо заметных обозначений зоны видеонаблюдения для информирования людей о ее существовании, а также предоставление необходимой контактной информации.

О настоящем руководстве

- Настоящее руководство носит исключительно справочный характер. Указанные в руководстве параметры могут незначительно отличаться от реальных параметров продукта.
- Мы не несем ответственности за убытки, возникшие в результате эксплуатации продукта способами, которые не отвечают требованиям настоящего руководства.
- Руководство будет обновляться на основании законов и нормативных актов соответствующих юрисдикций. Для получения более подробной информации обратитесь к печатной версии руководства по эксплуатации или к версии на CD-ROM, либо отсканируйте QR-код или посетите наш официальный сайт. Настоящее руководство носит исключительно справочный характер. Между электронной и печатной версиями могут иметь место незначительные расхождения.
- Любые конструктивные элементы и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления продукта могут стать причиной некоторых расхождений между параметрами реального продукта и информацией, изложенной в руководстве. Последнюю версию программного обеспечения и дополнительную документацию можно получить в службе поддержки клиентов.
- Существует вероятность ошибок печати или отклонений в описании функций, операций и технических данных. При возникновении каких-либо сомнений или разногласий мы оставляем за собой право окончательной трактовки.
- Если руководство (в формате PDF) не открывается, обновите установленное программное обеспечение для чтения файлов или попробуйте другое общедоступное программное обеспечение.
- Все товарные знаки, зарегистрированные товарные знаки и названия компаний в настоящем руководстве являются собственностью соответствующих владельцев.
- В случае появления любых проблем при использовании устройства посетите наш веб-сайт или обратитесь к поставщику или в службу поддержки.
- В случае каких-либо сомнений или противоречий мы оставляем за собой право окончательной трактовки.

Содержание

1 Вступление

1.1 Обзор

Контроллер охранной сигнализации – центральное устройство в системе безопасности, предназначенное для управления работой всех подключенных периферийных устройств. Если система безопасности обнаружит присутствие, проникновение или попытку проникновения постороннего в охраняемую зону, контроллер получит сигналы тревоги от извещателей, а затем предупредит пользователей.

1.2 Технические характеристики

В этом разделе приведены технические характеристики устройства. Пожалуйста, выберите те, которые соответствуют вашей модели.

Таблица 1-1 Технические характеристики

Тип	Параметр	Описание
Порты	Сеть	1 порт Ethernet RJ-45 (10/100 Мбит/с)
	GSM	Одна SIM-карта (GSM: 900/1800 МГц); две SIM-карты в режиме ожидания
	LTE	Одна SIM-карта (GSM: 900/1800 МГц, WCDMA: B1/B5/B8, LTE-FDD: B1/B3/B5/B7/B8/B20, LTE-TDD: B38/B40/B41); две SIM-карты в режиме ожидания
	Батарея	Разъем батареи 12 В
	Световой индикатор	1 для нескольких состояний (тревога, постановка / снятие с охраны, подключение к сети и неисправность)
	Кнопки	1 сброса, 1 питания, 1 точка доступа
	Звуковая сигнализация	Встроено
	Противокражная сигнализация	1 порт противокражной сигнализации на корпусе для панели управления сигнализацией
Функции	Оповещение по SMS	Тревоги SMS-сообщениями (до 5 телефонных номеров) Доступно только в определенных моделях.
	Уведомление телефонным вызовом	Есть (до 5 телефонных номеров) Доступно только в определенных моделях.
	Связывание с видео	Есть
	Сетевой протокол	TCP/IP, в том числе PPTP, L2TP, DHCP, UPNP, NTP

Тип	Параметр	Описание	
	Дистанционное обновление	Облачное обновление	
	Способ настройки	Мобильное приложение	
	Способ постановки на охрану и снятия с охраны	Приложение, пульт, брелок, расписание	
	Количество периферийных устройств	Максимально 150 каналов беспроводных периферийных устройств (6 оповещателей, 64 беспроводных брелока, 4 ретранслятора и 8 пультов)	
	Зоны	32 зоны (комнаты)	
	Управление питанием	Автоматическое переключение между основным и резервным питанием.	
		Сигнализация потери основного питания	
		Сигнализация потери батареи и неисправности напряжения батареи	
	Журналы событий	До 400	
	Защита настроенных параметров от сбоя питания	Есть	
	Управление пользователями	Максимально 8 пользователей: 1 монтажная организация, 1 администратор, 6 обычных пользователей.	
	Запросы	Запрос push-сообщений, состояния устройства и версии программы. Определение уровня сигнала.	
Радиоканал	Несущая частота	DHI-ARA3000H-FW2 (868) / DHI-ARA3000H-GW2 (868) / DHI-ARA3000H-W2 (868): 868 МГц ~ 868.6 МГц	DHI-ARA3000H-FW2 / DHI-ARA3000H-GW2 / DHI-ARA3000H-W2: 433.1 МГц ~ 434.6 МГц
	Дальность передачи сигнала	DHI-ARA3000H-FW2 (868) / DHI-ARA3000H-GW2 (868) / DHI-ARA3000H-W2 (868): до 2000 м на открытом пространстве	DHI-ARA3000H-FW2 / DHI-ARA3000H-GW2 / DHI-ARA3000H-W2: до 1200 м на открытом пространстве
	Мощность передатчика	DHI-ARA3000H-FW2 (868) / DHI-ARA3000H-GW2 (868) / DHI-ARA3000H-W2 (868): ограничение 25 мВт	DHI-ARA3000H-FW2 / DHI-ARA3000H-GW2 / DHI-ARA3000H-W2: ограничение 10 мВт
	Тип связи	Двухсторонний	
	Шифрование	AES128	
	Псевдослучайная перестройка рабочей частоты	Есть	

Тип	Параметр	Описание
	Обнаружение радиочастотных помех	Проверка проводится раз в 60 секунд, если помехи продолжаются более 30 секунд, система сообщает о радиочастотных помехах.
	Wi-Fi	2.4 ГГц
Питание	Тип источника питания	Тип A
	Основной источник питания	12 В (DC), 1.5 A
	Емкость батареи	2 × 3.6 В, 2150 мА*ч
	Время работы от батареи	До 12 ч При соблюдении следующих условий время работы может достигать 12 часов: • подключается к Wi-Fi, GPRS / 3G / 4G • подключается к панели управления с интервалом подтверждения 1800 секунд • подключается к 8 входам и 1 оповещателю • подключается к облаку
	Тип батареи	Тип батареи: встроенный литиевый аккумулятор; тип аккумулятора: 18650
	Максимальный ток	3.5 A
	Потребляемая мощность	До 15 Вт
	Потребляемый ток	Нормальный режим: 220 мА; тревога: 300мА
	Порог низкого заряда батареи	3.5 В (DC)
	Порог восстановления батареи	3.7 В (DC)
	Напряжение выключения	<3.358 В
	Время зарядки батареи	Примерно 15 ч до 80%
Взаимодействие со сторонними платформами	Категория системы охранной сигнализации	DP2 / SP2 (LAN / Wi-Fi и GPRS / 4G)
	Подтверждение операции	Сквозное
	Протоколы	SIA-DC09

Тип	Параметр	Описание	
	Приоритетный путь передачи	Локальная сеть / Wi-Fi (EN 50136-2)	
	Альтернативный путь передачи	GPRS / 4G	
	Оборудования оповещения	C/E/F	
Сертификаты		DHI-ARA3000H-FW2 (868) / DHI-ARA3000H-GW2 (868) / DHI-ARA3000H-W2 (868): EN 50131-1:2006 + A1:2009 + A2:2017 + A3:2020 EN 50131-3:2009 EN 50131-6:2017 EN 50131-5-3:2017 EN 50131-10:2014 EN 50136- 2:2013 Класс безопасности 2 Класс условий эксплуатации II CE	DHI-ARA3000H-FW2 / DHI-ARA3000H-GW2 / DHI-ARA3000H-W2: FCC CE

Таблица 1-2 Категория оборудования охранной сигнализации

Категория оборудования охранной сигнализации	Частота опроса	Протоколы	Линия связи			Одновременное использование линий связи
			Телефонная линия	2G / 3G	IP	
SP2	25 ч	Стандартный	√			Только отмеченная линия связи
SP3	30 мин	Стандартный		√	√	Только одна из двух отмеченных линий связи
SP4	3 мин	Шифрованный		√	√	Только одна из двух отмеченных линий связи
SP5	90 с	Шифрованный		√	√	Только одна из двух отмеченных линий связи
DP1	25 ч	Стандартный	√	√	√	Только две из трех отмеченных линий связи
DP2	30 мин	Стандартный	√	√	√	Только две из трех отмеченных линий связи
DP3	3 мин	Шифрованный		√	√	Две отмеченных линии связи
DP4	90 с	Шифрованный		√	√	Две отмеченных линии связи

Оборудование охранной сигнализации – ATE (Alarm transmission equipment) в соответствии со стандартом EN 50136-1.

SPx (Одиночный путь): Значение, указывающее уровень эффективности, достигаемый при использовании одной линии связи, в соответствии со стандартом EN 50136-1.

DPx (Двойной путь): Значение, указывающее уровень эффективности, достигаемый при использовании двух линий связи, в соответствии со стандартом EN 50136-1.

Частота опроса: Время между опросами устанавливается на основе стандарта для каждого уровня эффективности. Частота опроса – это максимальное время, доступное для сообщения о сбое передачи сигналов тревоги устройства. Устройства охранной сигнализации для соответствия этому требованию регулярно сообщают о своем состоянии с помощью специальной функции тестирования.

Протоколы: Здесь указывается уровень безопасности протоколов, которые будут использоваться для уведомления о сбоях. Стандартные протоколы и голосовые протоколы зашифрованы. Протоколы высокого уровня безопасности шифруются с помощью 128-битного или 256-битного ключа шифрования AES.

Линии связи: используемые линии связи.

Линии связи: указывает количество и тип линий связи, которые будут использоваться в зависимости от категории оборудования охранной сигнализации.

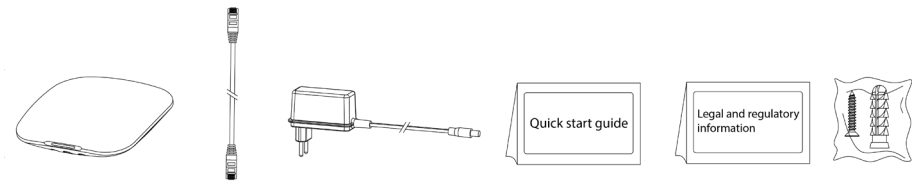
Таблица 1-3 Технические характеристики

Технические характеристики	**Описание**
Классификация вспомогательного управляющего оборудования	Тип A
Класс условий эксплуатации	II
Напряжение питания	12 В (DC), 1.5 A
Размеры продукта	163 мм × 163 мм × 32 мм
Размеры в упаковке	219 мм × 187 мм × 91 мм
Рабочая температура	От -10°C до +50°C От -10°C до +40°C (сертифицированная температура)
Влажность	10% ~ 90% (относительная)
Масса нетто	0.38 кг
Масса брутто	0.8 кг
Корпус	Поликарбонат, АБС-пластик

1.3 Комплектация

Проверьте содержимое упаковки в соответствии со следующим списком. Если вы обнаружите отсутствие или повреждение содержимого упаковки, обратитесь в службу поддержки клиентов.

Рисунок 1-1 Комплектация



1 2 3 4 5 6

Таблица 1-4 Комплектация

№	Наименование	Количество	№	Наименование	Количество
1	Контроллер охранной сигнализации	1	5	Юридическая и нормативная информация	1
2	Кабели	1	6	Комплект винтов	1
3	Блок питания	1	7	Зажим для фиксации провода	1
4	Краткое руководство пользователя	1	–	–	–

2 Конструкция

2.1 Внешний вид устройства

Рисунок 2-1 Внешний вид устройства

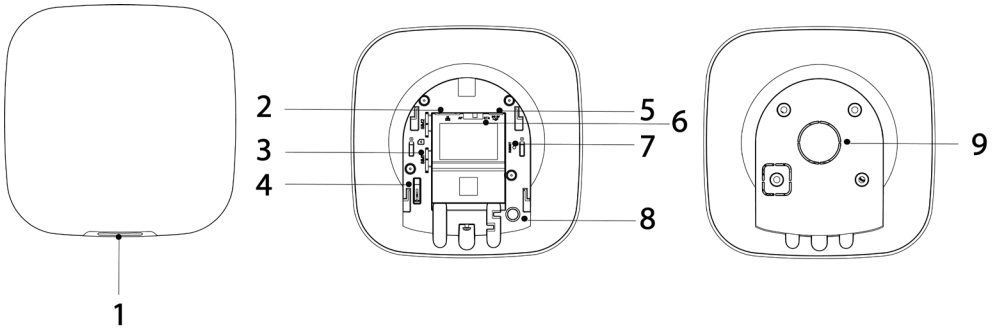


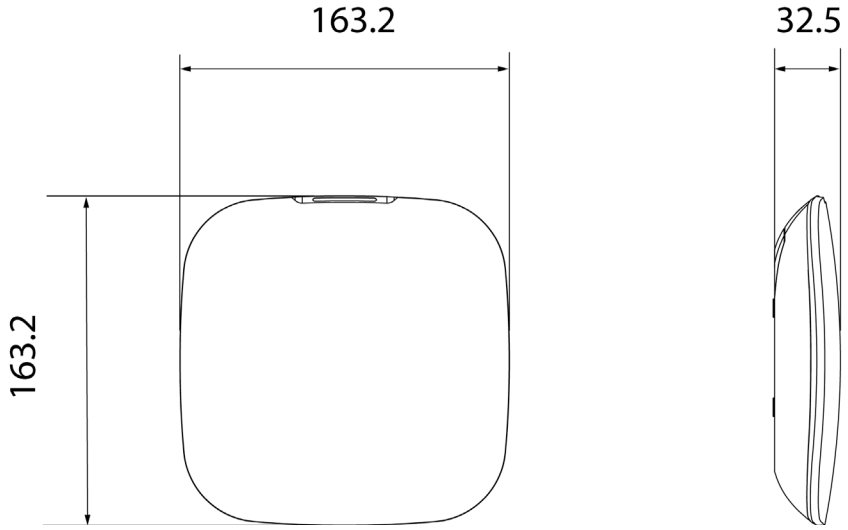
Таблица 2-1 Конструкция

№	Наименование	Описание
1	Индикатор	• Медленно мигает зеленым цветом: режим пониженной чувствительности. • Мигает зеленым цветом: контроллер запускается. • Постоянно светится желтым цветом: не удалось подключиться к облаку. • Постоянно светится зеленым цветом: режим снятия с охраны. • Постоянно светится синим цветом: режим постановки на охрану. • Мигает красным цветом: получено тревожное событие. • Мигает желтым цветом: обнаружена неисправность. • Мигает синим цветом: запущено конфигурирование через точку доступа или контроллер выполняет сопряжение с периферийными устройствами. • Быстро мигает синим цветом: режим регистрации карты.
2	Разъем кабеля Ethernet	Используется для подключения контроллера к сети Ethernet.

№	Наименование	Описание
3	Отсек для micro SIM 1/2	Установите основную карту в первый отсек, а резервную карту – во второй отсек. ● Поддержка двух SIM-карт в режиме ожидания. ● SIM-карты позволяют контроллеру использовать сотовую связь и отправлять уведомления о тревогах. ● SIM-карты не будут работать, пока не будет завершена настройка сети. ● Функция SIM-карт доступна только на определенных моделях.
4	Противокражная кнопка	Когда противокражная кнопка отпущена, срабатывает противокражная сигнализация.
5	Разъем кабеля питания	Используется для подключения кабеля питания
6	Точка доступа	Включите точку доступа, телефон подключится к точке доступа контроллера, а затем синхронизируйте имя пользователя и пароль Wi-Fi с контроллером.
7	Кнопка сброса	Нажмите и удерживайте кнопку в течение 10 секунд, чтобы перезапустить контроллер и восстановить заводские настройки по умолчанию.
8	Кнопка включения / выключения питания	Нажмите и удерживайте кнопку в течение 2 секунд, чтобы включить или выключить контроллер.
9	Задняя крышка	Если задняя крышка будет открыта, сработает противокражная сигнализация.

2.2 Размеры

Рисунок 2-2 Размеры, мм



3 Включение

3.1 Пользователи

Пользователи могут быть созданы только в приложениях DMSS и Dolynk Care. Распределите пользователей по разным ролям, чтобы они могли иметь разные уровни доступа для работы с устройствами.

Уровень доступа пользователей

Таблица 3-1 Уровень доступа пользователей

Пользователь	Уровень доступа
Администратор DMSS	L2
Обычный пользователь DMSS	L2
Монтажная организация	L3

- Монтажная организация: Монтажные организации предоставляют конечным пользователям услуги по эксплуатации и техническому обслуживанию. Эта роль должна запрашивать права доступа у конечного пользователя (администратор DMSS) на управление устройством. Они могут получать такие права, как настройка устройства и управление пользователями.
- Администратор DMSS: Администратор – конечный пользователь. Эта роль не может быть изменена, и у нее есть права доступа, такие как настройка устройства и управление пользователями. Администратор DMSS не имеет права на настройку устройства, когда монтажные организации сдают ему контроллер в пользование или когда он передает монтажной организации в управление контроллер.
- Обычный пользователь DMSS: Это пользователи, которым администратор DMSS предоставляет общий доступ к устройствам через приложение DMSS. Эта роль может быть изменена, и у нее есть только базовые права доступа, такие как просмотр состояния устройства, а также постановка на охрану и снятие с охраны комнат.

Схема последовательности действий

Ниже описан процесс передачи в управление устройств и предоставления общего доступа к устройствам в приложениях DMSS и Dolynk Care. Монтажные организации и конечные пользователи могут следить за процессом предоставления общего доступа к устройствам и передачи их в управление.

Рисунок 3-1 Схема последовательности действий (пользователь DMSS)

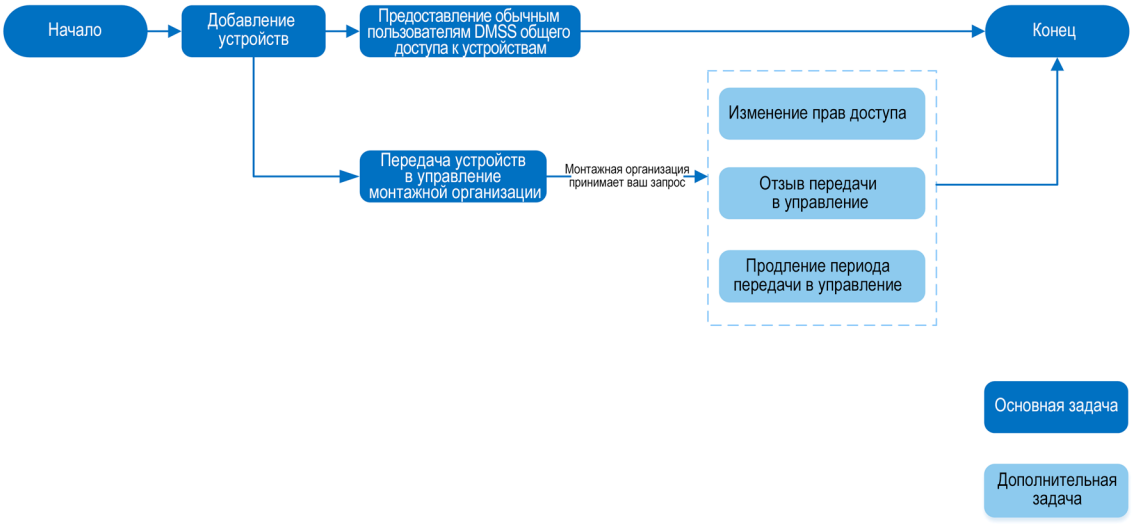
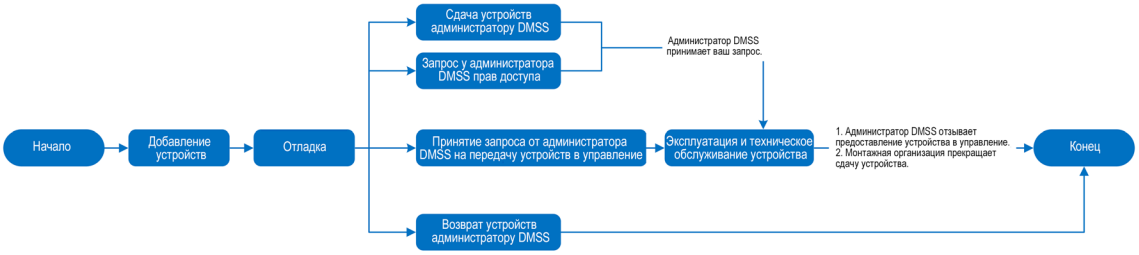


Рисунок 3-2 Схема последовательности действий (монтажная организация)



3.2 Работа с устройством

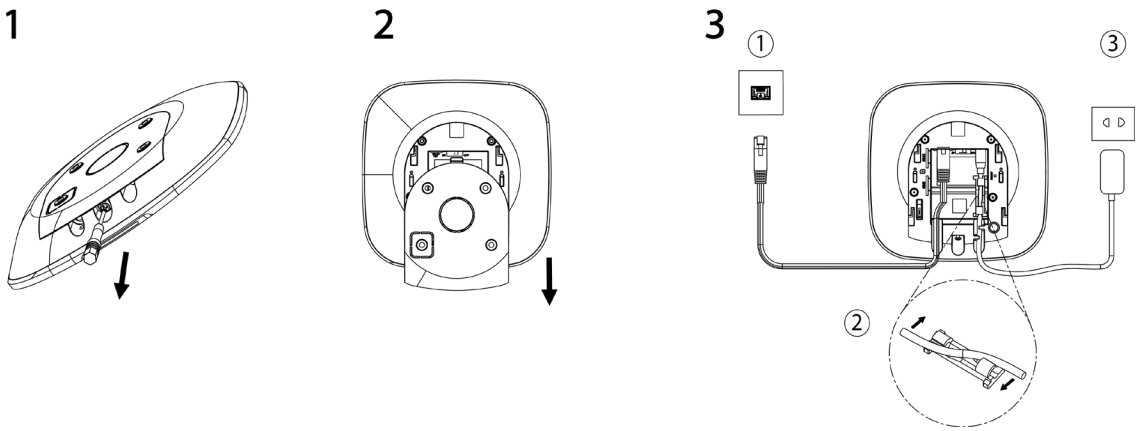
Следуйте инструкциям ниже, чтобы включить беспроводную систему охранной сигнализации.

Рисунок 3-3 Работа с устройством

Включение

Подключите контроллер к сети и включите его.

Рисунок 3-4 Включение



Добавление устройств

1. Добавьте контроллер в приложение Dolynk Care и DMSS.
2. Добавьте периферийные устройства на контроллер.

Монтаж контроллера

Для установки контроллера мы рекомендуем использовать саморезы с дюбелями. Не размещайте контроллер в следующих местах:

- на улице
- вблизи металлических предметов, которые вызывают ослабление и экранирование радиосигнала
- местах со слабым сигналом GSM
- вблизи источников радиопомех, на расстоянии менее 1 метра от маршрутизатора и кабелей питания
- местах, где температура и влажность превышают допустимые пределы

Рисунок 3-5 Монтаж

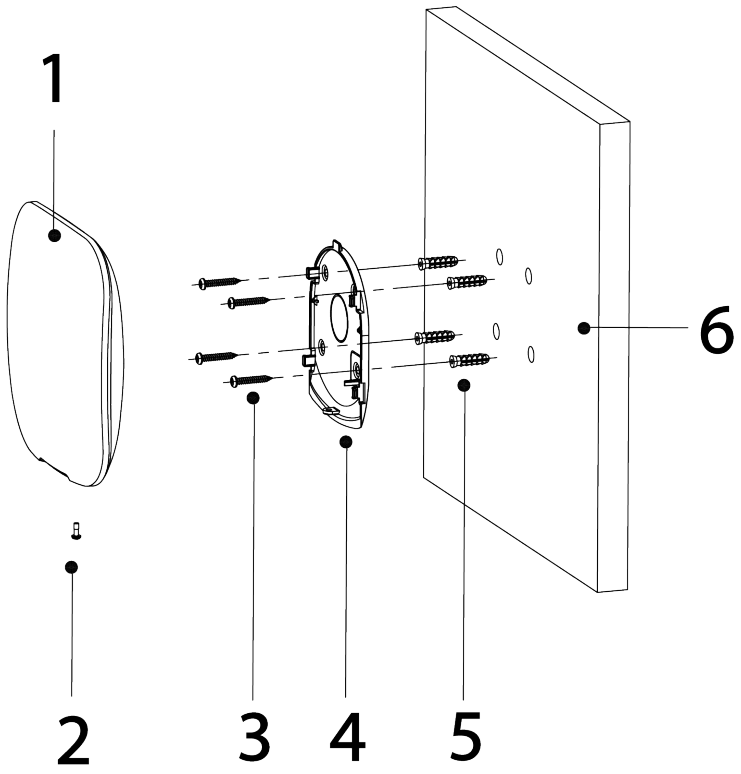


Таблица 3-2 Принадлежности для монтажа

№	Наименование	№	Наименование
1	Контроллер	4	Монтажная пластина
2	Винт M3 × 8 мм с потайной головкой	5	Дюбель
3	Саморез ST4 × 25 мм	6	Стена

1. Выберите положение отверстий для винтов, а затем просверлите их.
2. Вставьте дюбели в отверстия
3. Прикрепите монтажную пластину к стене, а затем совместите отверстия для винтов на пластине с дюбелями.

4. Закрепите монтажную пластину саморезами ST4 × 25 мм.
5. Вставьте контроллер охранной сигнализации в монтажную пластину сверху вниз.
6. Закрепите контроллер и монтажную пластину винтами с потайной головкой M3 × 8 мм.

Настройка контроллера

Настройте контроллер в приложении Dolynk Care и DMSS.

Постановка на охрану

Вы можете использовать пульт, брелок и приложение для постановки вашей системы на охрану. После отправки команды постановки на охрану в приложение Dolynk Care и DMSS система проверит свое состояние. Если в системе произошел сбой, вам нужно будет выбрать, включать ли ее принудительно. Подробная информация о периферийных устройствах приведена в соответствующем руководстве пользователя устройства.

4 Работа с приложением Dolynk Care для монтажных организаций

Приложение Dolynk Care предназначено для того, чтобы помочь монтажным организациям оказывать конечным пользователям профессиональные услуги по эксплуатации и техническому обслуживанию. Оно предоставляет такие функции, как управление оборудованием, эксплуатация и контроль исправности устройств, работа с переданными в управление устройствами и т.п. Подробная информация приведена в руководстве пользователя приложения Dolynk Care.

Изображения интерфейсов приведены только для справки и могут отличаться от фактических.

4.1 Авторизация в Dolynk Care

При первом использовании вам необходимо создать аккаунт. В этом руководстве пользователя в качестве примера описан порядок действий для пользователей iOS.

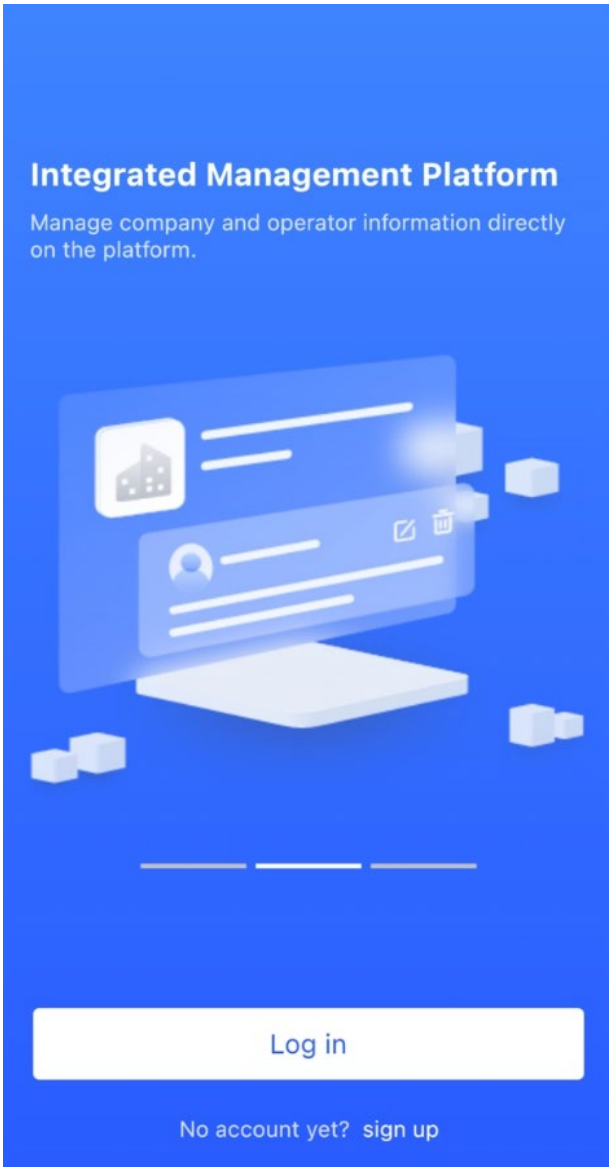
Порядок действий

Шаг 1 Найдите Dolynk Care в App Store, чтобы загрузить мобильное приложение.

Пользователи Android могут перейти в Google Play, чтобы найти и загрузить мобильное приложение.

Шаг 2 Нажмите на смартфоне , чтобы открыть мобильное приложение.

Рисунок 4-1 Авторизация



Шаг 3 Создайте аккаунт.

1. На странице **Вход (Login)** нажмите **Нет аккаунта? Зарегистрироваться (No account yet? sign up)**.
2. На странице **Регистрация (Register)** Заполните нужные поля.
   - **Имя компании (Company Name)**: Введите имя вашей компании.
   - **Адрес страны (Country Address)**: Выберите страну / район, провинцию / штат и город вашей компании.
   - **Адрес (Address)**: Введите полный адрес вашей компании.
   - **Код приглашения (Invitation Code)**: Введите пригласительный код, который можно получить у реселлера или торгового представителя.
   - **E-mail (Email)**: Введите ваш адрес e-mail.
   - **Пароль (Password)**: Введите пароль.
   - **Код подтверждения (Verification Code)**: Нажмите **Отправить (Send)**, и на указанный адрес e-mail придет код подтверждения. Введите этот код в поле **Код подтверждения (Verification Code)**.
3. Ознакомьтесь с Политикой конфиденциальности (Privacy Policy) и

Пользовательским соглашением (User Agreement), а затем установите флажок **Я прочитал и согласен с политикой конфиденциальности и пользовательским соглашением (I have read and agree to Privacy Policy and User Agreement)**.

4. Нажмите **Зарегистрироваться (Register)**, и затем приложение вернется к экрану входа в систему.

Шаг 4 Введите ваш адрес e-mail и пароль, затем нажмите кнопку **Войти (Log in)**.

- Для новых клиентов требуется одобрение заявки на регистрацию аккаунта. Получение электронного письма с подтверждением аккаунта займет 1-3 дня. После этого вы можете войти в приложение под своим аккаунтом.
- Некоторым аффилированным клиентам не требуется получать одобрение для регистрации аккаунта Dolynk Care. Они могут напрямую войти в приложение после регистрации.

4.2 Добавление устройств

Монтажная организация может добавлять устройства в приложение Dolynk Care для управления и технического обслуживания. Перед добавлением устройств убедитесь, что устройство подключено к источнику питания и сети. Вы можете добавить в приложение устройства сигнализации, включая контроллеры и множество периферийных устройств.

4.2.1 Добавление контроллера

Контроллер может быть добавлен либо в **Режиме объекта (Site mode)**, либо в **Режиме устройства (Device mode)**. Если вы добавляете в **Режиме устройства (Device mode)**, вам сначала нужно выбрать объект. Операции для этих двух режимов аналогичны. В этом разделе в качестве примера показана настройка в **Режиме устройства (Device mode)**.

- Перед добавлением контроллера убедитесь, что контроллер подключен к источнику питания и сети.
- Убедитесь, что на вашем телефоне включена функция Wi-Fi.

4.2.1.1 Добавление по серийному номеру или QR-коду

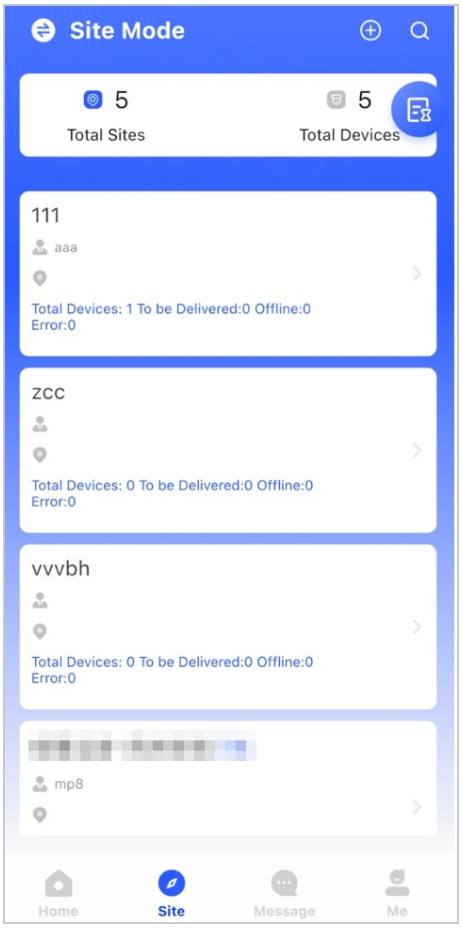
Вы можете добавить контроллер, отсканировав QR-код устройства или вручную введя серийный номер устройства в беспроводной или проводной сети.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите 

, затем перейдите на страницу **Объект (Site)**.

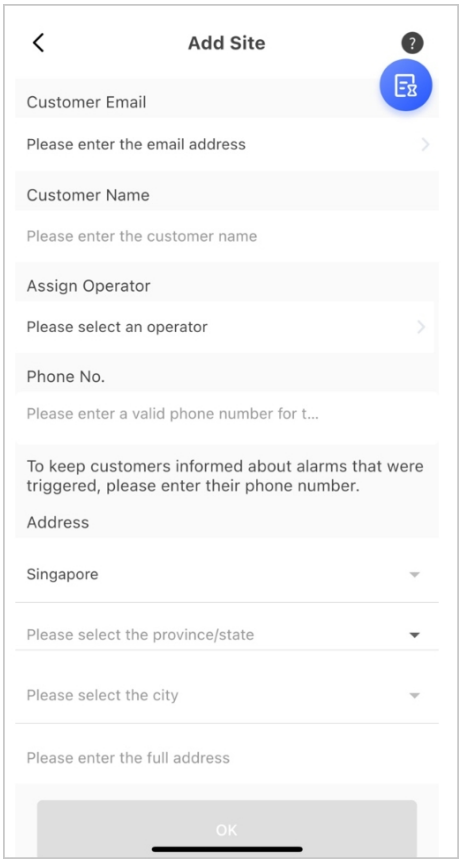
Рисунок 4-2 Объект



Шаг 2 Нажмите ⊕ для добавления нового объекта.

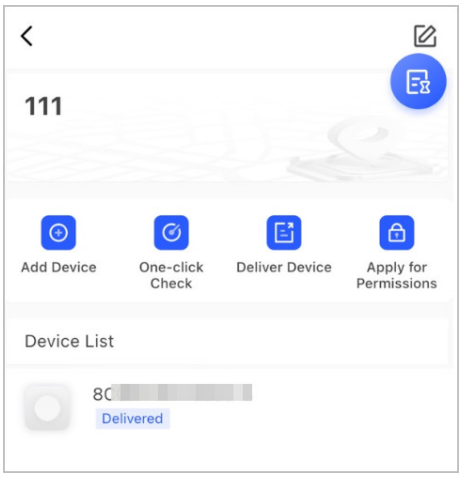
Введите информацию об объекте, а затем нажмите **OK**, чтобы создать объект.

Рисунок 4-3 Добавление объекта



Шаг 3 На странице созданного **Объекта (Site)** нажмите **Добавить устройство (Add Device)**.

Рисунок 4-4 Добавление устройства



Шаг 4 Отсканируйте QR-код устройства или нажмите **Добавить вручную (Manually Add)**, чтобы вручную ввести серийный номер устройства.

Шаг 5 Выберите объект, затем нажмите **OK**.

Шаг 3 На странице **Добавление устройства (Add Device)** выберите тип устройства.

Шаг 3 Подключитесь к беспроводной или проводной сети.

- **Беспроводное подключение**

1) Нажмите **Беспроводное (Wireless)** в правом верхнем углу, после чего произойдет переключение на **Проводное (Wired)**.
2) Введите пароль для Wi-Fi, к которому подключен ваш телефон, а затем нажмите **Подключиться (Connect)**.

3) Следуйте инструкциям на странице, а затем нажмите **Далее (Next)**.
4) Дождитесь сопряжения.

Если это не удалось, повторите описанные выше действия.

- Проводное подключение **(Wired)**

1) Нажмите **Проводное (Wireless)** в правом верхнем углу, после чего произойдет переключение на **Беспроводное (Wired)**.
2) Подключите устройство к источнику питания и сети, а затем нажмите **Далее (Next)**.

Если это не удалось, повторите описанные выше действия.

Шаг 8 Если добавляемый контроллер неинициализирован, введите пароль и подтвердите его еще раз, а затем нажмите **Инициализировать устройство (Initialize the device)**, чтобы завершить инициализацию.

Step 9 Нажмите **Готово (Completed)**, после чего вы сможете просмотреть устройство в списке устройств.

4.2.1.2 Добавление поиском в локальной сети

Вы можете выполнять поиск устройств и добавлять их. Убедитесь, что ваш смартфон и другие устройства подключены к одной сети.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите 

на странице **Объект (Site)**.

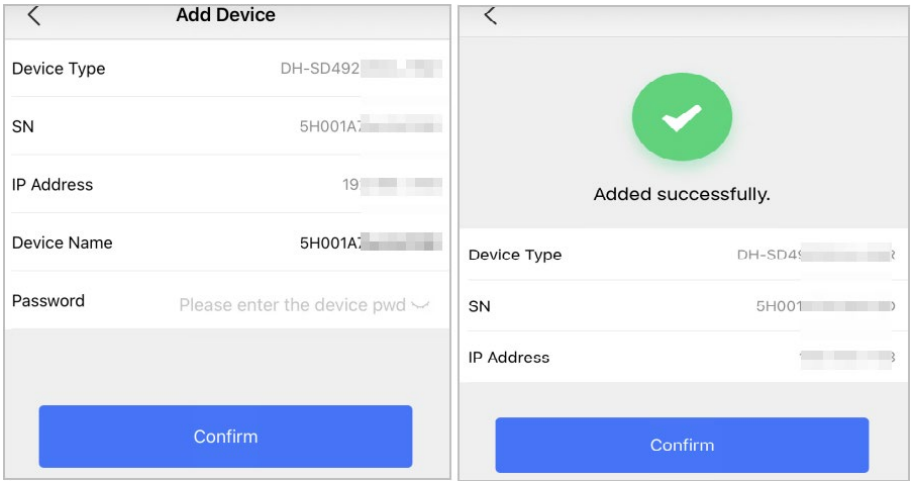
Шаг 2 Выберите объект и нажмите Добавить устройство **(Add Device)**, чтобы добавить устройство.

Рисунок 4-5 Добавление устройства

Шаг 3 Нажмите Поиск в локальной сети **(LAN Searching)**.

Step 4 На странице **Добавить устройство Add Device** введите пароль устройства, а затем нажмите **Подтвердить (Confirm)**.

Рисунок 4-6 Подтверждение добавления устройства



4.2.1.3 Добавление через настройку точки доступа

Вы можете добавить контроллер через настройку точки доступа.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите Site, затем перейдите на страницу **Объект (Site)**.

Шаг 2 Выберите объект и нажмите **Добавить устройство (Add Device)**, чтобы добавить устройство.

Рисунок 4-7 Добавление устройства

Шаг 3 Отсканируйте QR-код устройства или нажмите **Добавить вручную (Manually Add)**, чтобы вручную ввести серийный номер устройства.

Шаг 4 На странице **Добавить устройство (Add Device)** выберите **Контроллер охранной сигнализации (Alarm Station)**.

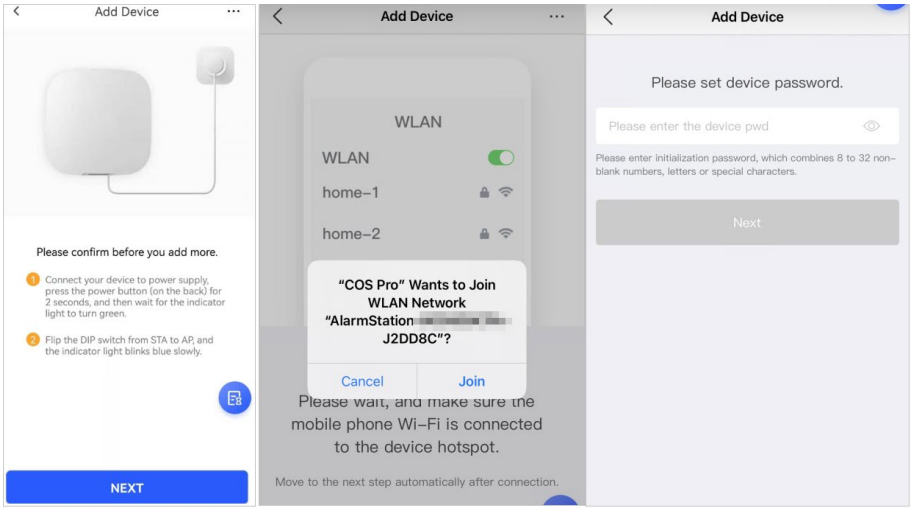
Рисунок 4-8 Выбор контроллера охранной сигнализации

Шаг 5 Следуйте инструкциям на экране и переключите DIP-переключатель с STA на AP.

Шаг 6 Нажмите **Присоединиться (Join)** для подключения к точке доступа устройства.

Шаг 7 Установите пароль устройства для инициализации устройства, а затем нажмите **Далее (Next)**.

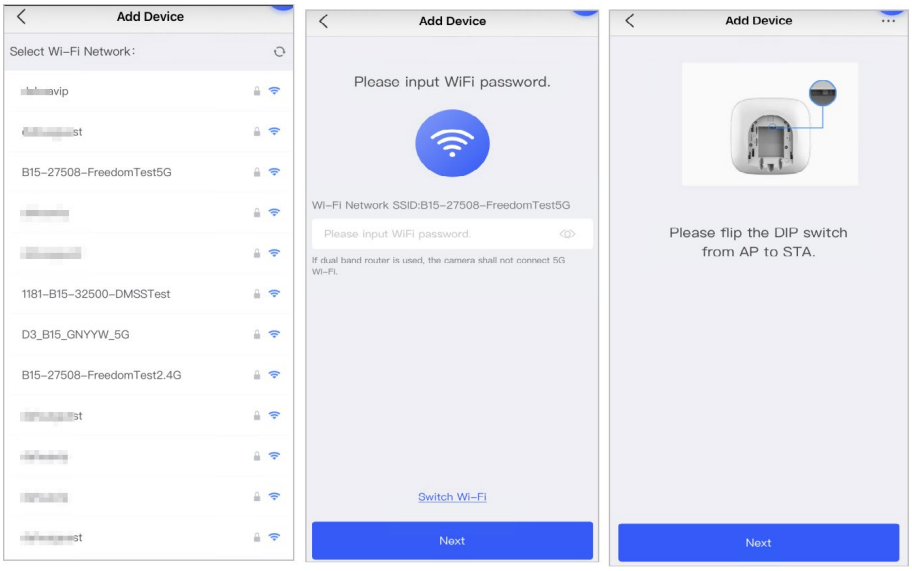
Рисунок 4-9 Добавление через настройку точки доступа



Шаг 8 Подключение к сети.

1) Выберите Wi-Fi.
   Убедитесь, что ваш смартфон и другие устройства подключены к одной сети.
2) Введите пароль Wi-Fi, нажмите **Далее (Next)**.
3) Переключите DIP-переключатель из положения AP в положение STA, нажмите **Далее (Next)**.
4) Дождитесь завершения настройки сети устройством.

Рисунок 4-10 Подключение к сети



Шаг 9 Нажмите **Готово (Completed)**.

4.2.2 Добавление периферийных устройств

Вы можете подключить к контроллеру множество периферийных устройств. В качестве примера в этом разделе рассматривается добавление магнитоконтактного извещателя. Дополнительные сведения о добавлении периферийных устройств см. в руководствах пользователя соответствующих периферийных устройств.

К контроллеру можно добавить до 6 оповещателей, 64 брелоков, 4 ретранслятора и 8 пультов.

Порядок действий

Шаг 1 На странице контроллера нажмите ⊕ в правом верхнем углу, а затем отсканируйте QR-код в нижней части магнитоконтактного извещателя.

Шаг 2 Нажмите **Далее (Next)**.

Шаг 3 Следуйте инструкциям на странице и включите магнитоконтактный извещатель, а затем нажмите **Далее (Next)**, чтобы добавить его на контроллер.

Шаг 4 Дождитесь сопряжения.

Шаг 5 Измените имя магнитоконтактного извещателя и выберите зону, а затем нажмите **Готово (Completed)**.

- Удаление периферийных устройств: Перейдите на экран контроллера, выберите устройство из списка периферийных устройств и смахните его влево для удаления.
- Можно создать до 32 зон для одного контроллера.

4.3.2 Управление пользователями

4.3.1 Добавление администраторов DMSS

Монтажная организация может добавить администраторов DMSS, предоставив им доступ к устройствам или приняв их запрос на передачу устройств в управление.

Справочная информация

В соответствии с сертификационными требованиями EN 50131 администратор DMSS не имеет права на настройку устройства, когда монтажные организации сдают им контроллер в пользование или когда они передают в управление контроллер монтажной организации.

4.3.1.1 Сдача устройства в пользование администраторам DMSS

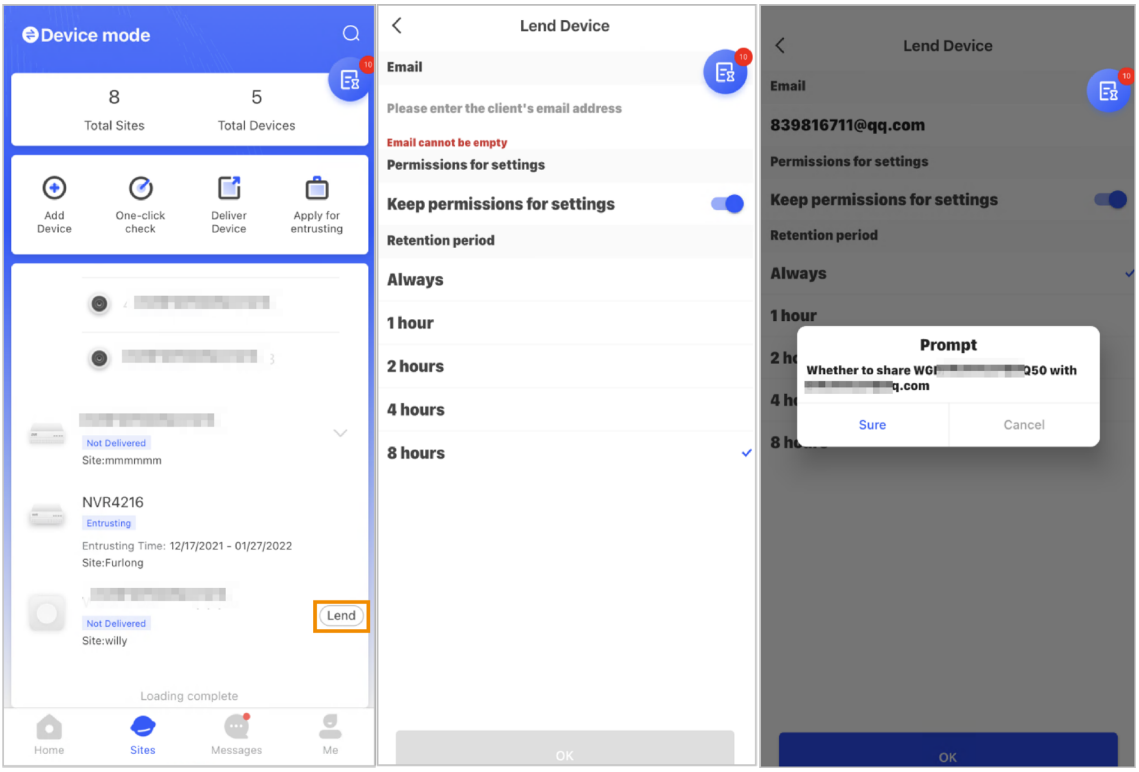
В соответствии с сертификационными требованиями EN 50131 монтажная организация может сдать контроллер в пользование администратору DMSS. После этого монтажной организации необходимо запрашивать права у администратора DMSS, на такие как действия, как настройка устройства, постановка на охрану и снятие с охраны, а также управление пользователями.

Убедитесь, что контроллер не был добавлен в другие аккаунты.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите Site, затем перейдите на страницу **Объект (Site)**.

Рисунок 4-11 Сдача контроллера в пользование администратору DMSS



Шаг 2 Нажмите в верхнем левом углу для переключения в **Режим устройств (Device mode)**.

Шаг 3 В списке устройств выберите контроллер, нажмите **Сдать в пользование (Lend)** в правом углу контроллера.

Шаг 4 Введите адрес e-mail администратора DMSS.

Шаг 5 Включите **Сохранить право на настройку (Reserve Configuration Permissions)** и выберите время, в течение которого право на настройку будет оставаться за вами.

Шаг 6 Нажмите **Подтвердить**.

Шаг 7 На экране нажмите **Личное сообщение (Personal Message)**, вы сможете просмотреть сообщения, чтобы узнать, согласился ли администратор DMSS принять ваш запрос на предоставление устройства в пользование.

Сообщение опредоставлении устройства в пользование будет отправлено в аккаунт администратора DMSS, и администратор DMSS сможет прочитать сообщение в приложении DMSS.

4.3.1.2 Принятие запросов на передачу в управление

Монтажная организация может принять запрос администратора DMSS на передачу в управление для предоставления услуг эксплуатации и обслуживания для пользователей.

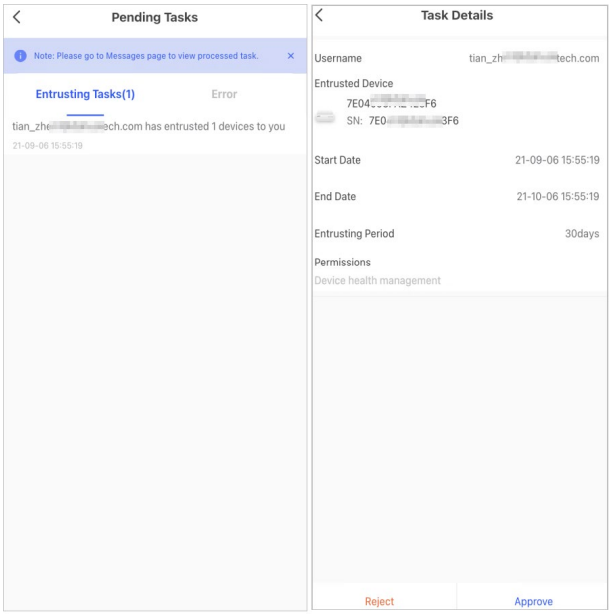
Порядок действий

Шаг 1 На **Главной странице (Home)**, выберите **Незавершенные задачи > Просмотр передачи в управление (Pending Task > Entrusting Review)**.

Шаг 2 На странице **Незавершенные задачи (Pending Task)**, выберите задачу, чтобы

просмотреть сведения о задаче и обработать запросы на передачу в управление.

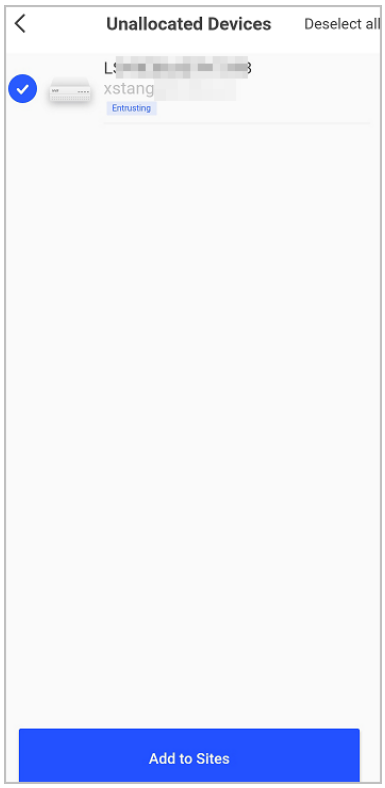
Рисунок 4-12 Обработка задач передачи в управление



- Для подтверждения

1) Нажмите **Подтвердить (Approve)**, а затем перейдите на страницу **Неназначенные устройства (Unallocated Devices)**.
2) Выберите устройства, которые нужно назначить или нажмите **Выбрать все (Select all)**, а затем нажмите **Добавить на объект (Add to Sites)**.

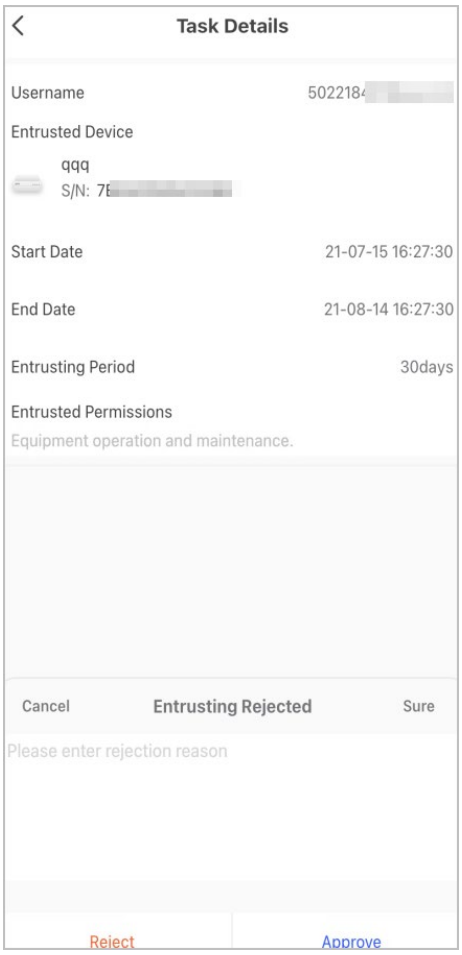
Рисунок 4-13 Добавление устройства на объект



3) На странице **Объекты (Sites)**, выберите объект или добавьте новый.
4) Нажмите **ОК**, чтобы подтвердить перемещение этого устройства на выбранный объект.

- Для отклонения: нажмите **Отклонить (Reject)**, введите причины отклонения, а затем нажмите **Верно (Sure)**.

Рисунок 4-14 Отклонение



4.3.2 Удаление пользователей

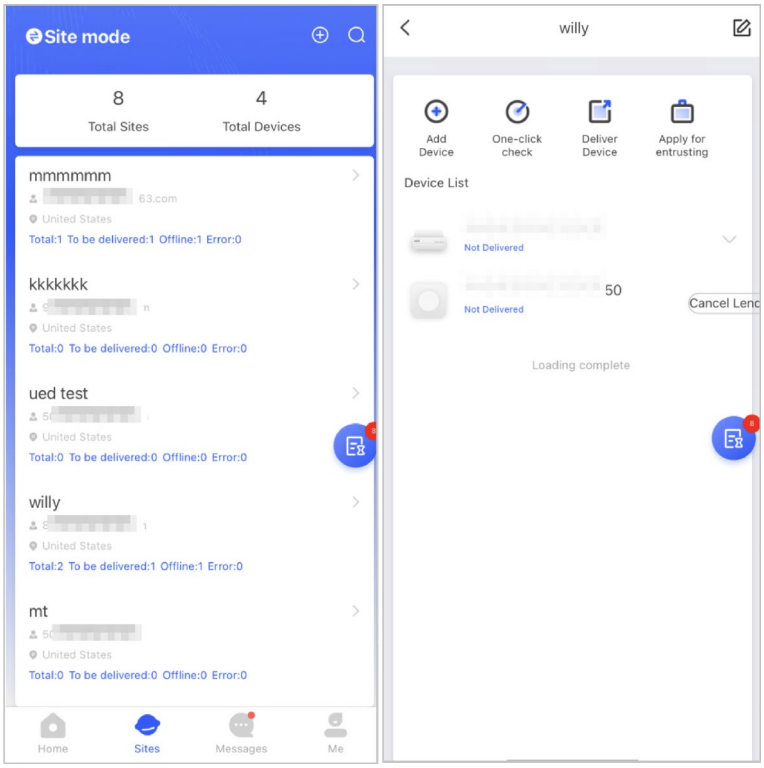
4.3.2.1 Отмена сдачи устройств в пользование

Монтажная организация может удалить администратора DMSS, отменив сдачу им контроллера в пользование.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите , затем перейдите на страницу **Объект (Site)**.

Рисунок 4-15 Сдача контроллера в пользование администратору DMSS



Шаг 2 Нажмите в верхнем левом углу для переключения в **Режим объектов (Site mode)**.

Шаг 3 В списке объектов выберите объект с устройством, которое вы предоставляете администратору DMSS, затем выберите контроллер и нажмите **Отменить сдачу в пользование (Cancel Lend)**.

Сообщение будет отправлено в аккаунт администратора DMSS, и администратор DMSS сможет прочитать сообщение в приложении DMSS.

4.3.2.2 Удаление устройств

Монтажная организация может удалять администраторов DMSS, удалив устройства.

- Убедитесь, что монтажная организация отменила сдачу устройств в пользование администратору DMSS.
- Монтажная организация может удалить всех пользователей DMSS, если администратор DMSS предоставил общий доступ к устройствам обычным пользователям DMSS.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите , затем перейдите на страницу **Объект (Site)**.

Шаг 2 Нажмите в верхнем левом углу для переключения в **Режим устройств (Device mode)**.

Шаг 3 В списке устройств выберите нужное устройство.

Шаг 4 На странице контроллера нажмите , затем нажмите **Удалить (Delete)**, чтобы удалить устройство.

4.4 Запрос прав у администратора DMSS

Монтажные организации могут добавить контроллер непосредственно в приложение Dolynk Care, чтобы предоставлять администраторам DMSS услуги по эксплуатации и техническому обслуживанию устройств. У вас есть ограниченные по времени права, включая права на настройку устройства и управление пользователями, и вам необходимо повторно подать заявку на получение прав по истечении срока их действия.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите , затем перейдите на страницу **Объект (Site)**.

Шаг 2 Нажмите в верхнем левом углу для переключения в **Режим устройств (Device mode)**.

Шаг 3 В списке устройств выберите нужное устройство.

Шаг 4 На странице **Контроллер (Hub)** выберите > **Настройки контроллера (Hub Setting)**, нажмите на любой параметр, который вы хотите настроить, и затем появится приглашение с напоминанием о необходимости запросить права у администратора DMSS.

Шаг 5 Нажмите **Верно (Sure)**.

Шаг 6 Выберите часы действия прав, затем нажмите **Подтвердить (Confirm)**.

Шаг 7 На странице, нажмите **Личное сообщение (Personal Message)**, вы сможете просмотреть сообщения, чтобы узнать, согласился ли администратор DMSS выдать вам права доступа.

Сообщение с запросом будет отправлено в аккаунт администратора DMSS, и администратор DMSS сможет прочитать сообщение в приложении DMSS.

4.5 Возврат устройств администратору DMSS

После установки и настройки устройств вы можете вернуть их администратору DMSS. Устройства не в сети и устройства, которые вы передали в управление, не могут быть возвращены.

Требования сертификации EN 50131 не будут соблюдаться, если монтажная организация вернет контроллер администратору DMSS.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите , затем перейдите на страницу **Объект (Site)**.

Шаг 2 Нажмите в верхнем левом углу для переключения в **Режим объектов (Site mode)**.

Шаг 3 В списке объектов выберите объект с устройствами, которые необходимо вернуть администратору DMSS.

Шаг 4 Нажмите , а затем перейдите на страницу **Вернуть устройства (Deliver devices)**.

Одновременно может быть возвращено не более 5 устройств.

Шаг 5 Введите адреса e-mail администратора DMSS, а затем нажмите **Верно (Sure)** чтобы просмотреть результаты возврата. Для устройств, которые не удалось вернуть администратору DMSS, перейдите на страницу **Сбой (Failed)**, чтобы выполнить повторный возврат.

Если клиенты используют аккаунт Imou, то их устройства не будут успешно возвращены. При этом на **Главной странице (Home)** появится сообщение о том, что у аккаунта нет соответствующих прав доступа. Пожалуйста, попросите клиента обновить аккаунт в приложении DMSS. Подробная информация приведена в *руководстве пользователя приложения DMSS*.

4.6 Эксплуатация и техническое обслуживание устройства

Монтажные организации могут предоставлять услуги по эксплуатации и техническому обслуживанию устройств, такие как проверка состояния работоспособности устройств, удаленная настройка устройств и исправление ошибок.

4.6.1 Проверка состояния работоспособности устройства

Вы можете проверять сетевое состояние устройств в режиме реального времени, а также проверять работоспособность устройств по одному или все сразу. В этом разделе в качестве примера используется вариант групповой проверки.

Справочная информация

Настройки можно найти в **Режиме объекта (Site mode)** и **Режиме устройства (Device mode)**. Операции для этих двух режимов аналогичны. В этом разделе в качестве примера показана настройка в **Режиме устройства (Device mode)**.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите , затем перейдите на страницу **Объект (Site)**.

Шаг 2 Нажмите в верхнем левом углу для переключения в **Режим устройств (Device mode)**.

Шаг 3 Нажмите .

Шаг 4 Выберите устройства, которые вы хотите проверить, а затем нажмите **X выбранных устройств (X devices selected)**. **Начать проверку состояния устройств (Start Health Check)**.

Для выбора всех устройств, нажмите **Выбрать все (Select all)**.

Шаг 5 Просмотрите результаты проверки, затем нажмите **OK**.

Устройства не в сети не могут быть проверены.

4.6.2 Основные настройки устройства

После добавления устройств, включая контроллер охранной сигнализации и периферийные устройства, вы можете просматривать и редактировать общую информацию об устройстве.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите Site, затем перейдите на страницу **Объект (Site)**.

Шаг 2 Нажмите в верхнем левом углу для переключения в **Режим устройств (Device mode)**.

Шаг 3 В списке устройств выберите нужное устройство.

Шаг 4 На экране контроллера нажмите , чтобы просмотреть и отредактировать общую информацию об устройстве.

Таблица 4-1 Описание параметров

Параметр	Описание
Состояние контроллера (Hub Status)	Подробная информация приведена в разделе «Настройка контроллера».
Настройки контроллера (Hub Setting)	Подробная информация приведена в разделе «4.6.2.2 Просмотр статуса состояния».
Настройки сети (Network Configuration)	Нажмите **Настройки сети (Network Configuration)**, чтобы просмотреть текущую информацию о вашей сети.
Time Zone (Часовой пояс)	Нажмите **Часовой пояс (Time Zone)**, чтобы выбрать свой часовой пояс, и при необходимости включите DST (переход на летнее время). • **Часовой пояс (Time Zone)**: Выберите часовой пояс, в котором работает контроллер. • **DST (переход на летнее время)**: Выберите дату или неделю, а затем выберите время начала и окончания.
Общий доступ к устройствам (Device Sharing)	Нажмите **Общий доступ к устройствам (Device Sharing)**, чтобы поделиться состоянием контроллера с другими пользователями.

Параметр	Описание
Облачное обновление (Cloud Update)	Обновление прошивки устройства по сети Обновление запрещено, если контроллер поставлен на охрану или уровень заряда батареи низкий.
Журналы (Logs)	Устройство и журнал приложения • Журнал устройства: Выберите **Журнал > Журнал устройства (Log > Device log)**, чтобы просмотреть журналы тревог устройства. Вы также можете нажать на странице **Журнал устройства (Device log)**, чтобы отправить журналы тревог на указанный адрес e-mail. • Журнал приложения (App log): Выберите **Журнал > Журнал приложения (Log > App log)**, чтобы просмотреть журналы тревог приложения Dolynk Care. Вы также можете нажать на странице **Журнал устройства (App log)**, чтобы отправить журналы тревог на указанный адрес e-mail.
Руководство пользователя (User's Manual)	Нажмите **Руководство пользователя (User's Manual)**, чтобы получить руководство пользователя контроллера охранной сигнализации.

4.6.2.1 Настройка контроллера

На странице **Контроллера (Hub)**, выберите > **Настройки контроллера (Hub Setting)**, чтобы настроить параметры контроллера.

Таблица 4-2 Описание параметров контроллера

Параметр	Описание
Управление пользователями (User Manager)	Вы можете добавлять, изменять или удалять пользователей пульта, когда он снят с охраны. • **Добавление пользователей**: Нажмите ⊕ для добавления пользователя. Введите свое имя пользователя, пароль и пароль под принуждением, а затем выберите права на постановку на охрану и снятие с охраны для комнаты. ◇ Пароль и пароль под принуждением должны состоять из 4-6 цифр. ◇ Пароль под принуждением необязателен. ◇ Можно создать до 32 пользователей. Первый созданный пользователь по умолчанию является администратором. Ему доступны все права доступа. • Удаление пользователя: выберите пользователя, а затем смахните влево, чтобы удалить его. Пользователь с правами администратора должен быть удален последним. • **Изменение информации о пользователе:** Нажмите на пользователя, которого вам нужно отредактировать, и затем вы сможете изменить информацию о пользователе, включая имя пользователя, пароль, пароль под принуждением, права на постановку на охрану и снятие с охраны. • **Добавление карты доступа**: Нажмите ⊕ в правом верхнем углу страницы с информацией о пользователе, чтобы добавить карту доступа для пользователя. Нажмите любую клавишу, чтобы активировать пульт, а затем поместите карту доступа рядом с областью считывания карт на пульте, чтобы перейти к процессу связывания карты доступа с пользователем в течение 30 секунд. Если информация о карте успешно распознана, идентификатор карты отобразится на странице информации о пользователе, а затем пульт подаст один звуковой сигнал. После сохранения конфигураций карта будет иметь права пользователя. Можно связать с пользователем до 8 карт. • **Удаление карты доступа**: Выберите карту доступа, а затем проведите пальцем влево, чтобы удалить ее.

Параметр	Описание
Глобальные постановка на охрану или снятие с охраны (Global Arming/Disarming)	Включите или выключите все извещатели во всех зонах одним нажатием.
Постановка на охрану или снятие с охраны по расписанию (Schedule Arming/Disarming)	Вы можете ставить на охрану зоны или снимать их с охраны по расписанию. • **Зона (Area)**: Выберите зону, в которой работает контроллер. • **Настройка команд (Command setting)**: выберите нужный режим постановки на охрану, нажав **В присутствии (Home)**, **В отсутствие (Away)** или **Снятие с охраны (Disarm)**. • **Время (Time)**: Выберите период времени, в котором работает контроллер. • **Повторить (Repeat)**: Скопируйте расписание постановки или снятия с охраны. • **Принудительная постановка на охрану (Force Armed)**: Вы можете включить систему при возникновении ошибок в зонах.
Настройка звукового сигнала (Ringtone Setting)	Звуковой сигнал при входе в режим постановки на охрану или выходе из него.
Светодиодный индикатор (LED Indicator)	**Светодиодный индикатор (LED Indicator)** включен по умолчанию. • Если **Светодиодный индикатор (LED Indicator)** отключен, он будет оставаться выключенным независимо от того, нормально ли работает контроллер или нет. • Эта функция доступна только в приложении DMSS версии 1.96 или более новой для контроллера с прошивкой версии V1.001.0000000.4.R.211014 или более новой.
Управление телефонными номерами (Phone Number Management)	Нажмите **Добавить (Add)** в правом верхнем углу страницы, чтобы добавить телефонный номер для получения события, а затем выберите тип события, для которого необходимо отправить SMS. Типы событий включают в себя тревогу, неисправность, операции и то, связан ли тревога с телефонным вызовом. После добавления вы можете смахнуть влево, чтобы проверить телефонные вызовы и SMS-сообщения или проверить текущий телефонный номер. Вы также можете смахнуть влево, чтобы удалить телефонный номер. Нажмите на телефонный номер, чтобы перейти на страницу редактирования телефонного номера, а затем вы можете изменить номер и выбрать тип события, для которого необходимо отправить SMS. Только устройства с 2G / 4G поддерживают эту функцию.
Тестовый режим (Test Mode)	Нажмите **Старт (Start)**, чтобы проверить состояние периферийных устройств, подключаемых к контроллеру в различных зонах, а затем нажмите **Стоп (Stop)**, чтобы завершить проверку.

Параметр	Описание
Режим пониженной чувствительности (Reduced Sensitivity Mode)	Включите **Режим пониженной чувствительности (Reduced Sensitivity Mode)**, и тогда мощность передачи контроллера будет уменьшена. Функция доступна только в приложении DMSS версии 1.97 или более новой для контроллера с прошивкой версии V1.001.0000000.6.R.211215 или более новой.
Соединение с облаком (Cloud Service Connection)	Установите интервал проверки связи между сервером и контроллером в диапазоне от 150 до 900 секунд (по умолчанию 150 секунд). Если D-cloud обнаружит, что время отсутствия связи с контроллером превышает 150 секунд, оно сообщит пользователю о состоянии контроллера через приложение. Функция доступна только в приложении DMSS версии 1.96 или более новой для контроллера с прошивкой версии V1.001.0000000.6.R.211215 или более новой.
Интервал опроса (Heartbeat)	Настройте интервал опроса извещателей контроллером. Настройки определяют, как часто контроллер взаимодействует с периферийными устройствами и как быстро обнаруживается потеря соединения. • **Интервал опроса извещателя (Detector Ping Interval)**: Частота опроса подключенных периферийных устройств, управляемых контроллером, настраивается в диапазоне от 12 секунд до 300 секунд (по умолчанию 60 секунд). Чем короче интервал опроса извещателя, тем короче срок службы батареи. • **Количество потерянных пакетов при определении сбоя подключения (Number of undelivered packets to determine connection failure)**: Лимит потерянных пакетов настраивается в диапазоне от 3 до 60 (по умолчанию 15 пакетов). ◇ Чем меньше это число, тем чаще обнаруживается и сообщается о состоянии периферийных устройств, которые не в сети. ◇ Если контроллер постоянно теряет соединение с периферийными устройствами и не может опросить их о состоянии, он сообщит системе их состояние не в сети.

Параметр	Описание
Связывание оповещателя с противокражной сигнализацией (Link Siren for Tamper)	• **Связать оповещатель с противокражной сигнализацией (Link Siren for Tampe)**: При постановке на охрану, когда включена функция **Связать оповещатель с противокражной сигнализацией (Link Siren for Tamper)**, контроллер подключит звуковой сигнал тревоги. Оповещатель подаст сигнал тревоги, когда крышки контроллера и периферийных устройств будут открыты. • **Всегда активен (Always Active)**: Настройте связывание звукового оповещателя при снятии с охраны. По умолчанию это отключено. После включения функции **Всегда активен (Always Active)**, когда включена функция **Связать оповещатель с противокражной сигнализацией (Link Siren for Tamper)**, контроллер будет связывать звуковой сигнал тревоги как в состоянии постановки на охрану, так и в состоянии снятия с охраны. Это не соответствует требованиям сертификации EN50131-1.
Диагностика системы (System Integrity Check)	При включении этой функции контроллер охранной сигнализации перед постановкой на охрану проведет диагностику всех извещателей. Диагностика включает проверку уровня зарядки батареи, противокражных тревог и подключений. При обнаружении ошибок будут показаны предупреждения. • На брелоке индикатор мигает зеленым, а затем становится красным. • В приложении появится тревожное сообщение. • Пульт подает звуковой сигнал в течение 1 секунды, индикатор постановки на охрану и снятия с охраны мигает зеленым в течение 2 секунд, а затем переходит в нормальное состояние.
Платформа (CMS)	Введите IP-адрес, порт и идентификатор устройства, а затем вы можете зарегистрировать контроллер на DSS Pro или конвертере. Функция доступна только в приложении DMSS версии 1.96 или более новой для контроллера с прошивкой версии V1.001.0000000.6.R.211215 или более новой.

Центр обработки тревог (Alarm Center)	Включите **Станцию мониторинга (Monitoring Station)**, а затем установите параметры протокола SIA для центра обработки тревог (ARC). • **Основной IP-адрес (Preferred IP address)**: Введите IP-адрес и номер порта платформы центра обработки тревог. • **Альтернативный IP-адрес (Alternative IP address)**: Введите альтернативный IP-адрес и номер порта платформы центра обработки тревог.  ◇ Сообщения будут отправляться на альтернативный IP-адрес только в том случае, если основной IP-адрес не сможет получить сообщение. ◇ Если включен **Интервал опроса (Heartbeat interval)**, система сама определит, следует ли отправлять сообщение на основной или альтернативный IP-адрес. • **Протокол IP (IP Protocol)**: По умолчанию выбран **TCP**. • **Интервал опроса (Heartbeat interval)**: Установите интервал опроса в диапазоне от 0 секунд до 24 часов (по умолчанию 60 секунд).  0 секунд означает, что **Интервал опроса (Heartbeat interval)** отключен. • **Аккаунт платформы (Central account)**: Введите номер аккаунта, созданный центром обработки тревог, который будет использоваться для идентификации контроллера при отправке информации в центр обработки тревог. • **Шифрование (Encryption)**: Контроллер использует формат шифрования для обеспечения информационной безопасности при настройке центра обработки тревог. По умолчанию установлен **AES 128**. • **Загрузка события (Upload event)**: Нажмите  рядом с событием, чтобы загрузить его. ◇ **Тревога (Alarm)**: Тревожное сообщение ◇ **Ошибка (Error)**: Сбой питания, пониженное напряжение батареи, противокражная тревога и отключение от сети. ◇ **Событие (Event)**: Невозможность использования периферийных устройств, добавление или удаление периферийных устройств, а также добавление или удаление пользователей. ◇ **Постановка / снятие с охраны (Arm/Disarm)**: Отправка уведомлений о постановке на охрану или снятии с охраны системы. • **Проверка связи (Communication Test)**: Поддерживает **Ручное**

Параметр	Описание
	тестирование (Manual Test) и **Тестирование по расписанию (Scheduled Test)**. ◇ **Ручное тестирование (Manual Test)**: При ручном тестировании возможно проверить являются ли основные и альтернативные настройки центров обработки тревог рабочими. Если тест прошел успешно, центр может получить тестовое событие. ◇ **Тестирование по расписанию (Scheduled Test)**: Тестирование по расписанию отключено по умолчанию. После включения контроллер регулярно сообщает о периодическом тестовом событии.
Контроль неисправностей (Fault Check)	• **Сбой основного источника питания (Main Power Failure)**: По умолчанию включено. После отключения, когда основной источник питания контроллера выходит из строя, контроллер не будет уведомлять об этом. • **Противокражная сигнализация контроллера охранной сигнализации (Alarm Hub Tamper)**: По умолчанию включено. После отключения, когда крышка контроллера открыта, контроллер не будет уведомлять об этом. • **Связь с облачной платформой (Connections to Cloud Platform)**: По умолчанию включено. После отключения, когда не будет связи между контроллером и облачной платформой, контроллер не будет уведомлять об этом. • **Обнаружение ошибок проводного подключения и Wi-Fi (Wired Network and Wi-Fi Error Detection)**: По умолчанию включено. После отключения, когда проводное подключение и Wi-Fi контроллера выходят из строя, контроллер не будет уведомлять об этом. • **Глушение радиосигнала (RF Jamming)**: По умолчанию включено. После отключения, когда контроллер обнаруживает глушение радиосигнала, он не будет уведомлять об этом, но событие можно просмотреть в журнале. Отключение любой из этих функций приведет к тому, что система не будет соответствовать стандарту EN50131-1, и соответствующие сообщения об ошибках отправляться не будут.

4.6.2.2 Просмотр состояния

На странице **Контроллер (Hub)**, выберите > **Состояние контроллера (Hub Status)**, чтобы просмотреть состояние контроллера.

Таблица 4-3 Состояние контроллера

Параметр	Описание
Уровень сигнала GSM / LTE (GSM/LTE Signal Strength)	Уровень сигнала мобильной сети для активной SIM-карты. ● : Очень низкий. ● : Низкий. ● : Средний. ● : Высокий. ● : Нет.
Уровень сигнала Wi-Fi (Wi-Fi Signal Strength)	Состояние подключения контроллера к интернету через Wi-Fi. Для большей надежности мы рекомендуем устанавливать контроллер в местах с уровнем сигнала не менее 2 делений. ● : Очень низкий. ● : Низкий. ● : Средний. ● : Высокий. ● : Нет.
Уровень заряда батареи (Battery Level)	Показывает оставшийся заряд батареи. ● : Полный заряд. ● : Достаточный заряд. ● : Средний заряд. ● : Низкий заряд.
Противокражная сигнализация (Anti-tampering)	Режим противокражной сигнализации периферийного устройства, который реагирует на открытие корпуса.
Состояние основного источника питания (Main Power Status)	Показывает состояние основного источника питания.
Состояние подключения GSM / LTE (GSM/LTE Connection Status)	Состояние подключения контроллера к Интернету через сотовую связь, Wi-Fi и Ethernet. ● : Подключено. ● : Отключено.
Состояние подключения Wi-Fi (Wi-Fi Connection Status)	
Состояние подключения сетевого кабеля (Network Cable Connection Status)	
Состояние SIM-карты (SIM Card Status)	Состояние подключения SIM-карты. ● : SIM-карта 1 активна ● : SIM-карта 2 активна ● : Нет SIM-карты.
Версия прошивки (Program Version)	Версия прошивки контроллера

4.6.3 Просмотр оценок

После удаленной настройки устройств и устранения ошибок клиенты оценят, как операторы справились с устранением ошибок и поддержанием работоспособности устройств. Аккаунт администратора может просматривать подробную информацию об ошибках, такую как тип ошибки, время возникновения ошибки, предложения и действия, имя оператора и оценки.

Порядок действий

Шаг 1 На экране, нажмите **Уведомления об ошибках**.

Шаг 2 В списке сообщений нажмите на сообщение, чтобы просмотреть подробную информацию о сообщении, включая имя пользователя клиента, имя пользователя оператора, сведения об устройстве, сведения об ошибке, сведения об устранении ошибки и рейтинг.

4.6.4 Исправление ошибок

Вы можете исправить ошибки после проверки неисправных устройств. Ошибки обнаруживаются двумя способами, включая автоматический отчет устройства и ручную проверку.

Порядок действий

Шаг 1 На **Главной странице (Home)** выберите **Незавершенные задачи > Исправление ошибок (Pending Task > Error Fixing)**.

Шаг 2 В списке ошибок выберите задачу с ошибкой, а затем нажмите **Начать обработку (Start processing)**.

Шаг 3 Исправьте ошибку в соответствии с предложениями.

Шаг 4 Нажмите **Ошибка исправлена (Error Fixed)**, если ошибка исправлена, а затем дождитесь подтверждения от клиента.

Клиенты будут уведомлены о состоянии исправления ошибок. Если они подтвердят, что ошибка была исправлена, им будет предложено оценить качество обслуживания.

5 Функции DMSS для конечных пользователей

Приложение DMSS предоставляет профессиональные услуги видеонаблюдения для конечных пользователей. Администраторы DMSS могут совместно использовать контроллер с обычными пользователями DMSS и передать его в управление обслуживающей организации. Периферийные устройства, входящие в комплект поставки контроллера, можно передать в общий доступ или в управление. Чтобы самостоятельно передать в общий доступ или в управление контроллер, вам необходимо установить последнюю версию приложения DMSS.

Изображения интерфейсов приведены только для справки и могут отличаться от фактических.

5.1 Авторизация в DMSS

Система безопасности настраивается и управляется с помощью приложения DMSS. Вы можете воспользоваться приложением DMSS под iOS или Android. В этом разделе в качестве примера описан порядок действий для пользователей iOS.

Убедитесь, что вы установили последнюю версию приложения.

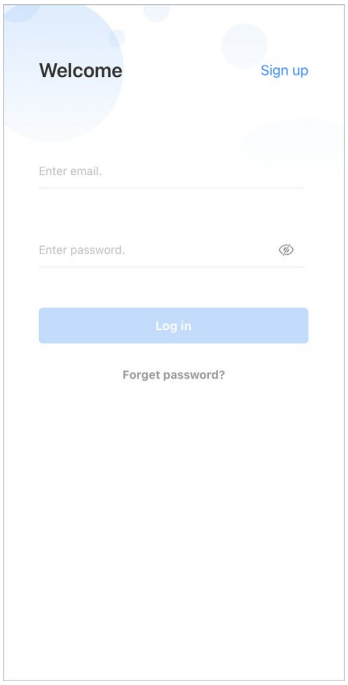
Порядок действий

Шаг 1 Найдите DMSS в App Store, а затем загрузите приложение.

Пользователи Android могут перейти в Google Play, чтобы загрузить мобильное приложение.

Шаг 2 Нажмите на смартфоне ⊕, чтобы открыть мобильное приложение.

Рисунок 5-1 Авторизация



Шаг 3 Создайте аккаунт.

1) На странице **Вход (Login)** нажмите **Зарегистрироваться (Sign up)**.
2) Введите адрес e-mail и пароль.

Нажмите чтобы отобразить пароль, и значок изменится на .

3) Прочтите документы **Пользовательское соглашение (User Agreement)** и **Политика конфиденциальности (Privacy Policy)** и отметьте пункт **Мною прочитаны и принимаются (I have read and agree to)**.
4) Нажмите **Получить код подтверждения (Get verification code)**, и на указанный адрес e-mail придет код подтверждения. Введите этот код.

Срок действия полученного кода подтверждения – 60 секунд. По истечении этого времени код подтверждения становится недействительным.

5) Нажмите **OK**.

Шаг 4 На странице **Вход (Login)** введите адрес e-mail и пароль, затем нажмите **Войти (Log in)**.

Чтобы изменить пароль, выберите **Мои сведения > Управление аккаунтами > Изменить пароль (Me > Account Management > Modify Password)**.

5.2 Добавление устройств

Конечные пользователи могут добавить устройства охранной сигнализации в приложение

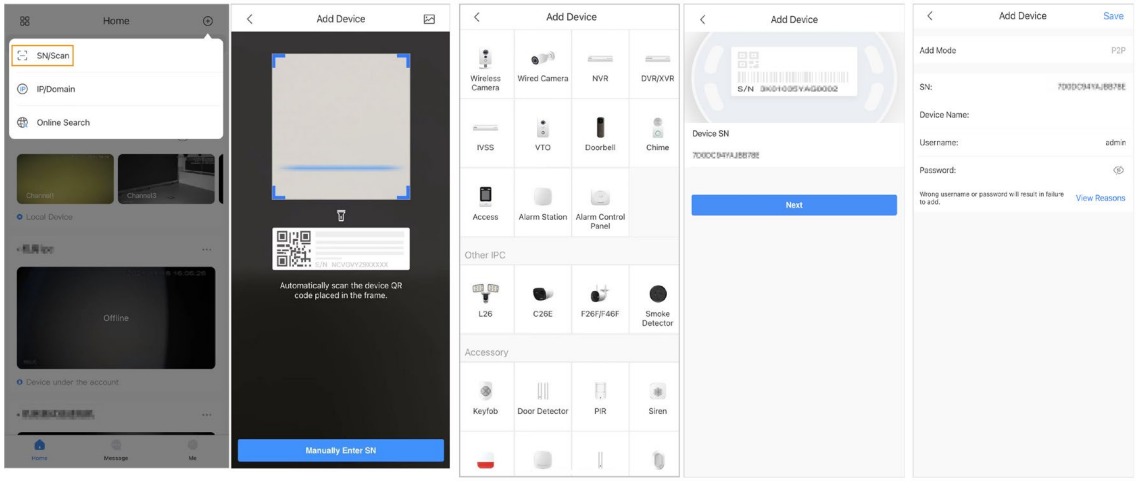
DMSS.

5.2.1 Добавление контроллера

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите ⊕, а затем выберите **Серийный номер / Сканировать (SN/Scan)**.

Рисунок 5-2 Добавление по серийному номеру / QR-коду



Шаг 2 Добавление устройства.

- Отсканируйте QR-код устройства напрямую или нажмите 🖼 и импортируйте изображение QR-кода, чтобы добавить устройство.
- Нажмите **Ручной ввод серийного номера (Manually Enter SN)**, а затем введите серийный номер устройства, чтобы вручную добавить устройство.

Шаг 3 Выберите тип устройства, а затем нажмите **Далее (Next)**.

Нажмите **Далее (Next)**, если система автоматически определит тип устройства.

Шаг 4 На странице **Добавить устройство (Add Device)** измените название устройства, введите имя пользователя и пароль устройства, а затем нажмите **Сохранить (Save)**.

5.2.2 Добавление периферийных устройств

Для конечных пользователей вы можете добавить в контроллер несколько периферийных устройств. Операции по добавлению периферийных устройств в DMSS такие же, как и в Dolynk Care.

5.3 Основные настройки контроллера

На экране контроллера нажмите ⚙, после чего вы сможете просматривать и редактировать общую информацию о контроллере. Основная информация об устройстве, отображаемая в

приложении DMSS, такая же, как и в приложении Dolynk Care.

5.4 Настройка сети

В меню **Общие настройки (General Config)** на странице **Сведения об устройстве (Device Details)** нажмите **Настройкиа сети (Network Configuration)**, а затем вы можете выбрать тип сети для контроллера: проводная сеть, беспроводная сеть или сотовая сеть.

5.4.1 Настройка проводной сети

Порядок действий

Шаг 1 Выберите **Настройки сети > Настройка проводной сети (Network Settings > Wired Network Config)**.

Шаг 2 Настройте параметры подключения к проводной сети.

Таблица 5-1 Описание параметров проводной сети

Параметр	Описание
DHCP	Когда в сети есть DHCP-сервер, вы можете включить **DHCP** и тогда контроллер будет получать динамический IP-адрес автоматически.
IP-адрес (IP Address)	Установите IP-адрес вручную: установите IP-адрес, маску подсети, шлюз по умолчанию, DNS и MAC-адрес вручную для контроллера.
Маска подсети (Subnet Mask)	
Шлюз (Gateway)	
DNS	
DNS 2	
MAC-адрес (MAC Address)	

5.4.2 Настройка сети Wi-Fi

Порядок действий

Шаг 1 Выберите **Настройки сети > Настройка сети Wi-Fi Network Settings > Wi-Fi Network Configuration**.

Шаг 2 Выберите доступную сеть Wi-Fi в данной зоне, а затем введите пароль для подключения к сети.

5.4.3 Настройка сотовой сети

Порядок действий

Шаг 1 Выберите **Настройки сети > Сотовая сеть** > **Network Settings > Cellular**.

Шаг 2 Настройте параметры сотовой сети.

Таблица 5-2. Описание параметров сотовой сети

Параметр	Описание
Сотовая сеть (Cellular)	Нажмите напротив **Сотовая сеть (Cellular)**, чтобы включить сотовую связь.
Приоритет (Priority)	Нажмите напротив **Приоритет (Priority)** чтобы установить сотовую связь в качестве приоритетной при выборе сети.
SIM 1	• Поддержка двух SIM-карт в режиме ожидания. • SIM-карты позволяют контроллеру использовать сотовые данные и отправлять уведомления о тревогах.
SIM 2	
Имя точки доступа (APN)	Имя точки доступа (APN) – это название настроек, считываемых вашим устройством для настройки шлюза между сотовой сетью вашего оператора и общедоступным Интернетом.
Режим аутентификации (Auth Mode)	Режим аутентификации в сотовой сети.
Имя пользователя (Username)	Имя пользователя и пароль в сотовой сети.
Пароль (Password)	
Контактный номер (Dial Number)	Номер, по которому звонит контроллер.
Использование мобильных данных (Mobile Data Usage)	Просмотр использования мобильных данных.
Сброс статистики (Reset Statistics)	Сбросьте статистику использования мобильных данных, чтобы перезапустить подсчет.

5.5 Управление пользователями

5.5.1 Добавление пользователя

Администраторы DMSS могут добавить как монтажные организации, так и обычных пользователей DMSS.

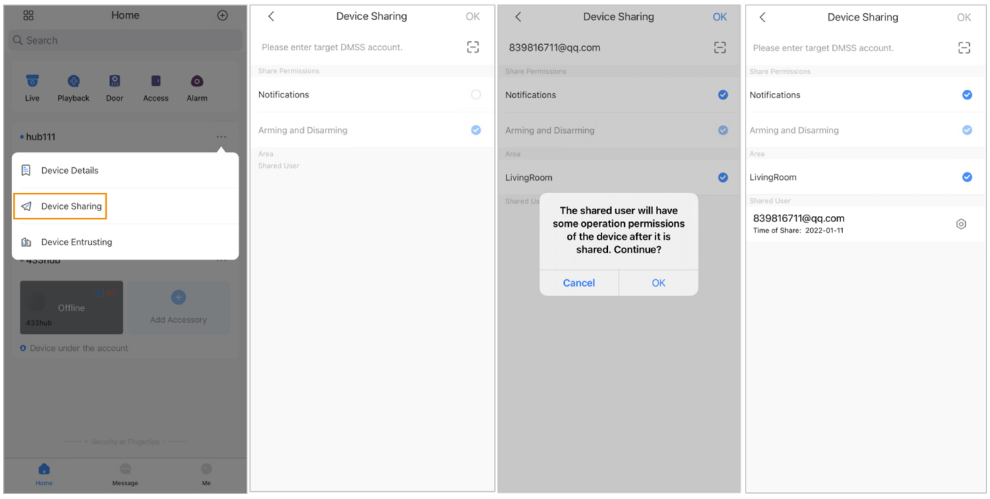
5.5.1.1 Добавление обычного пользователя DMSS

Вы можете перейти в > **Сведения об устройстве (Device Details)** > или > **Сведения об устройстве > Общий доступ к устройствам (Device Details > Device Sharing)**, чтобы предоставить общий доступ к устройству. Эти методы сходны. В этом разделе в качестве примера используется предоставление общего доступа через > **Общий доступ к устройствам (Device Sharing)**.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите напротив устройства, а затем нажмите **Общий доступ к устройствам (Device Sharing)**.

Рисунок 5-3 Общий доступ к устройствам



Шаг 2 На странице **Общий доступ к устройствам (Device Sharing)** дайте общий доступ к устройству пользователю, введя его аккаунт DMSS или отсканировав QR-код.

Шаг 3 Выберите нужные права доступа для пользователя.

Шаг 4 Нажмите **OK**.

Аккаунт, которому вы предоставили общий доступ к устройству, появится в разделе **Пользователи с общим доступом** на странице **Общий доступ к устройствам (Device Sharing)**.

5.5.1.2 Добавление монтажной организации

Администраторы DMSS могут добавить монтажные организации, передав им устройства в управление. Вы можете передать в управление монтажной организации устройства по одному или все сразу.

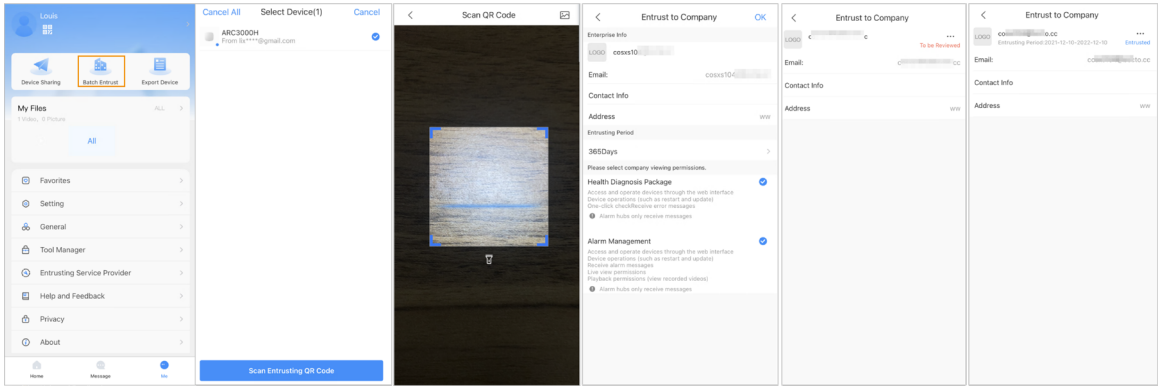
5.5.1.2.1 Групповая передача устройств в управление

Вы можете передать в управление организации все устройства сразу.

Порядок действий

Шаг 1 На **Главной странице (Home)**, выберите **Мои сведения > Групповая передача в управление (Me > Batch Entrust)**.

Рисунок 5-4 Групповая передача в управление



Шаг 2 На странице **Выбор устройств (Select Device)** выберите устройства, которые

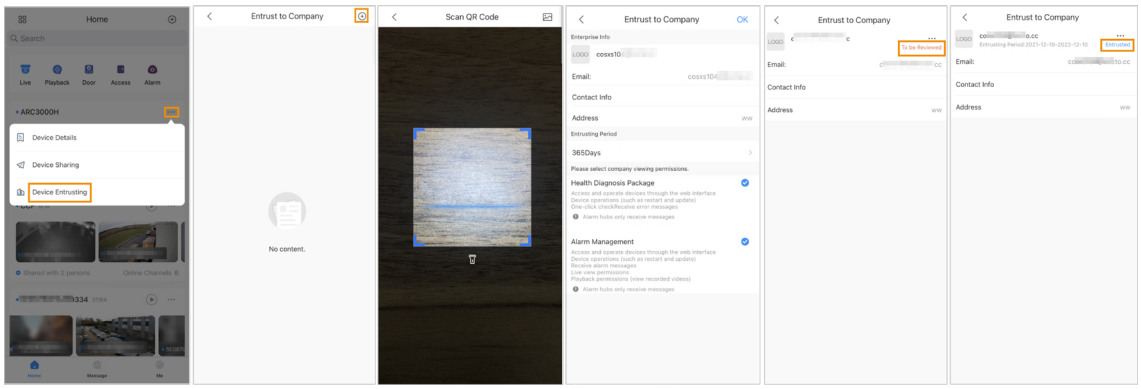
необходимо передать в управление, а затем передайте их организации. Процесс групповой передачи устройств в управление такой же, как и для одного устройства.

5.5.1.2.2 Передача устройств в управление по одному

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите ••• напротив устройства, а затем нажмите **Передача в управление (Device Entrusting)**.

Рисунок 5-5 Передача устройства в управление



Шаг 2 На странице **Передача организации** нажмите ⊕, а затем отсканируйте соответствующий QR-код монтажной организации или нажмите и импортируйте изображение QR-кода, чтобы передать в управление устройство монтажной организации.

Вы можете запросить у монтажных организаций их QR-коды.

Шаг 3 На странице **Передача организации (Entrust to Company)** выберите периоды действия и права на просмотр для организации, а затем нажмите **ОК**.

- Вы должны выбрать по крайней мере одно право на просмотр в **Пакете диагностики работоспособности (Health Diagnosis Package)** и **Обработки тревог (Alarm Management)**.
- Информация об организации будет автоматически распознана после того, как вы отсканируете QR-код монтажной организации.

Шаг 4 Просмотрите информацию о передаче в управление на странице **Передача организации (Entrust to Company)**.

После успешной передачи в управление состояние **На проверке (To be Reviewed)** изменится на **Передано (Delivered)**.

После успешной отправки запроса на передачу в управление на **Главной странице (Home)** появится соответствующее сообщение. Вам нужно дождаться ответа от монтажникамонтажной организации, который будет показан на странице **Мои сведения > Почтовый ящик > Личные сообщения (Me > Mailbox > Personal)**.

Сопутствующие действия

- Чтобы изменить права доступа, перейдите на страницу **Передача организации (Entrust to Company)**, а затем нажмите **Изменить права доступа (Change Permissions)**.
- Чтобы отозвать права доступа, выданные при передаче в управление, перейдите на страницу **Передача организации (Entrust to Company)**, а затем нажмите **Отозвать (Withdraw)**.
- Чтобы продлить периоды действия передачи в управление, перейдите на страницу **Передача организации (Entrust to Company)**, а затем нажмите **Продлить (Renew)**.

5.5.2 Удаление пользователей

Администраторы DMSS могут удалить как монтажные организации, так и обычных пользователей DMSS.

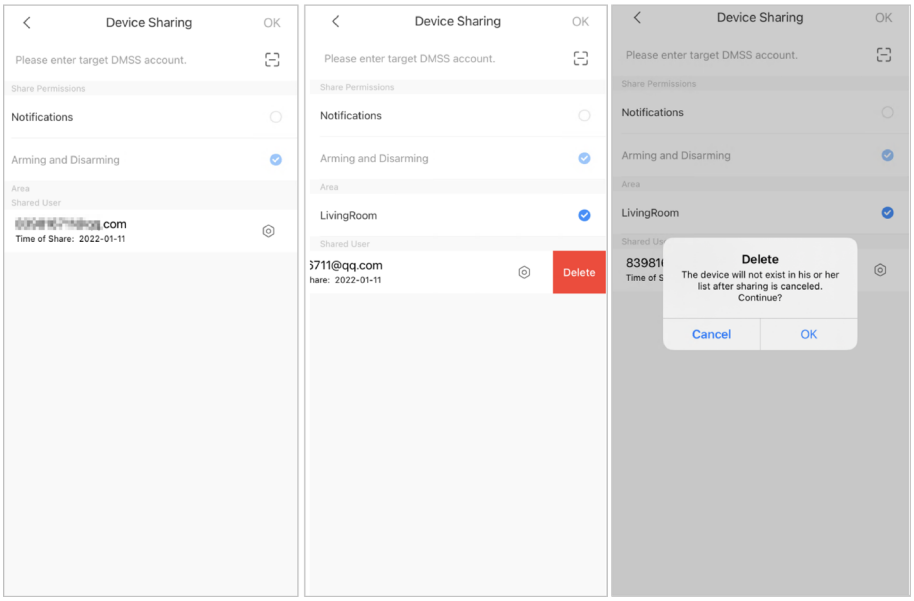
5.5.2.1 Отмена общего доступа к устройствам

Как администратор DMSS, вы можете удалить обычных пользователей DMSS, отменив предоставление им общего доступа к устройствам на странице **Общий доступ к устройствам (Device Sharing)**. В этом разделе в качестве примера используются метод через ••• > **Общий доступ к устройствам (Device Sharing)**.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите ••• напротив устройства, а затем нажмите **Общий доступ к устройствам (Device Sharing)**.

Рисунок 5-6 Общий доступ к устройствам



Шаг 2 В списке аккаунтов на странице **Общий доступ к устройствам (Device Sharing)** выберите аккаунт, смахните блок влево, а затем нажмите **Удалить (Delete)**.

Шаг 3 Нажмите **OK** для отмены доступа.

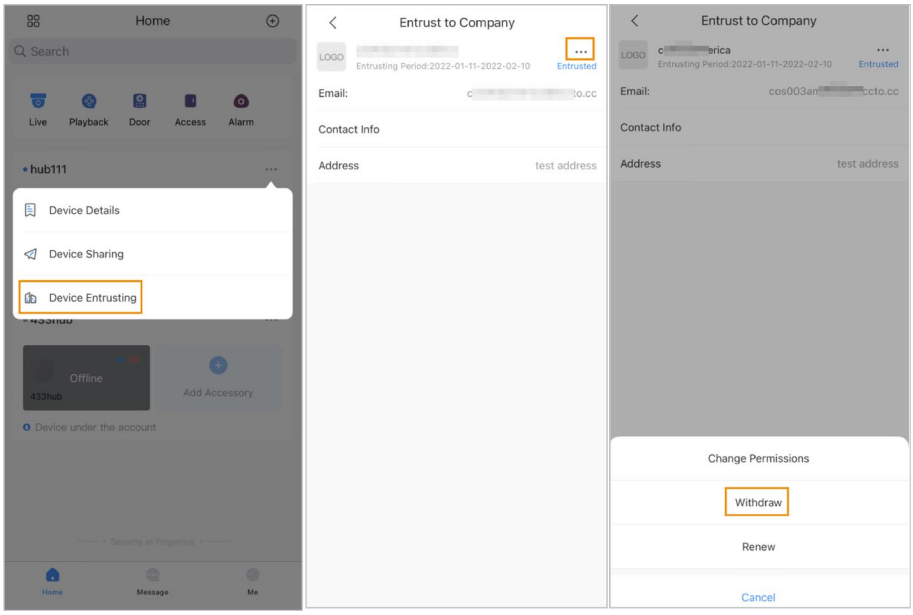
5.5.2.2 Отмена передачи в управление приложению

Как администратор DMSS вы можете удалить монтажную организацию, отменив передачу в управление приложению.

Порядок действий

Шаг 1 На **Главной странице (Home)** нажмите ••• напротив устройства, а затем нажмите **Передача устройств (Device Entrusting)**.

Рисунок 5-7 Отмена передачи в управление приложению



Шаг 2 На странице **Передача устройств (Device Entrusting)** выберите ••• > **Отозвать (Withdraw)**, а затем нажмите **OK**.

На аккаунт монтажной организации будет отправлено сообщение. После того, как монтажная организация прочтет сообщение и одобрит ваш запрос на отмену передачи в управление приложению в Dolynk Care, отмена будет завершена.

5.5.2.3 Удаление устройств

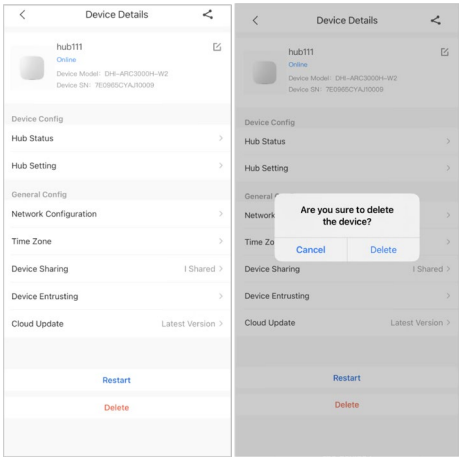
Как администратор DMSS вы можете удалить как монтажные организации, так и обычных пользователей DMSS, удалив устройства.

Администратор DMSS не может удалить монтажную организацию, если она предоставляет общий доступ к устройствам.

Порядок действий

Шаг 1 На **Главной странице (Home)** выберите ••• > **Сведения об устройстве (Device Details)**.

Рисунок 5-8 Удаление устройства



Шаг 2 На странице **Сведения об устройстве (Device Details)** нажмите **Удалить (Delete)**.

Шаг 3 Нажмите **Удалить (Delete)**, чтобы удалить устройство.

6 Основные действия

Пользователь уровня 2 или 3 имеет права на постановку на охрану и снятие с охраны. В этом разделе в качестве примера используется работа конечного пользователя с DMSS.

Подготовка

- Перед выполнением настройки убедитесь, что вы добавили контроллер.
- Контроллер должен иметь стабильное подключение к Интернету.
- Контроллер должен быть снят с охраны.

Справочная информация

Вы можете управлять контроллерами охранной сигнализации и периферийными устройствами, а также выполнять такие операции, как постановка на охрану и снятие с охраны, настройка устройств охранной сигнализации.

Порядок действий

Шаг 1 На странице контроллера нажмите **Периферийное устройство**, чтобы добавить периферийные устройства. Подробная информация о добавлении периферийных устройств приведена в соответствующем руководстве пользователя устройства.

Шаг 2 Постановка на охрану и снятие с охраны извещателей в отдельной зоне или во всех зонах осуществляется вручную или по расписанию.

- Одиночная постановка на охрану и снятие с охраны: Постановка на охрану и снятие с охраны извещателей в одной зоне.
- Глобальная постановка на охрану и снятие с охраны: Постановка на охрану и снятие с охраны извещателей во всех зонах.
- Ручная постановка на охрану и снятие с охраны: Постановка системы на охрану с помощью приложения DMSS, пульта или брелока.
- Постановка на охрану и снятие с охраны по расписанию: Постановка на охрану и снятие с охраны извещателей по расписанию.

6.1 Одиночная постановка на охрану и снятие с охраны

Вы можете поставить на охрану и снять с охраны извещатели в одной зоне.

Порядок действий

Шаг 1 На странице контроллера нажмите **Зона (Area)**.

Шаг 2 Коснитесь зоны, а затем выберите во всплывающем окне **В присутствии (Home)**, **В отсутствие (Away)**, **Снятие с охраны (Disarm)** и **Отключить (Disable)**.

- **В присутствии (Home)**: Постановка на охрану при нахождении внутри охраняемой зоны.
- **В отсутствие (Away)**: Режим, позволяющий ставить систему сигнализации на охрану при уходе из охраняемой зоны.
- **Снятие с охраны (Disarm)**: Снятие системы безопасности с охраны. Действие, противоположное постановке системы на охрану.

- **Отключение (Disable)**: Закрывает текущую страницу.

6.2 Глобальные постановка на охрану или снятие с охраны

Подготовка

Убедитесь, что вы включили функцию **Глобальные постановка на охрану или снятие с охраны (Global Arming/Disarming)**. На странице контроллера выберите > **Настройки контроллера (Hub Setting)**, а затем включите **Глобальные постановка на охрану или снятие с охраны (Global Arming/Disarming)**.

Справочная информация

Вы можете поставить на охрану и снять с охраны извещатели во всех зонах.

Порядок действий

Шаг 1 Перейдите на страницу контроллера

Шаг 2 Выберите **В присутствии (Home)**, **В отсутствие (Away)**, **Снятие с охраны (Disarm)** на верхней части страницы.

6.3 Постановка на охрану или снятие с охраны вручную

Вы можете поставить систему на охрану с помощью приложения DMSS или брелока.

- Для постановки на охрану или снятия с охраны извещателей в отдельной зоне или во всех зонах см. разделы «Однократные постановка на охрану или снятие с охраны» и «Глобальные постановка на охрану или снятие с охраны».
- Чтобы управлять с помощью брелока и пульта, вам необходимо сначала назначить брелоку и пульту права на управление зонами. Подробная информация приведена в руководстве пользователя соответствующего брелока и пульта.

6.4 Постановка на охрану или снятие с охраны по расписанию

Вы можете настроить расписание постановки на охрану или снятия с охраны извещателей. Вы можете настроить расписания постановки на охрану, включая зоны постановки на охрану, режимы и периоды.

Порядок действий

Шаг 1 На странице контроллера выберите > **Настройки контроллера > Постановка на охрану или снятие с охраны по расписанию (Hub Setting > Scheduled Arming/Disarming)**.

Шаг 2 На странице **Постановка на охрану или снятие с охраны по расписанию**

(Scheduled Arming/Disarmin) нажмите **Добавить (Add)**, а затем настройте расписания постановки на охрану.

- **Имя (Name)**: Настройте имя для расписаний постановки на охрану.
- **Зона (Area)**: Выберите одну или несколько зон, которые вы хотите поставить на охрану.
- **Настройка команд (Command Setting)**: Выберите из **В присутствии (Home)**, **В отсутствие (Away)**, **Снятие с охраны (Disarm)**.
- **Время (Time)**: Установите время постановки на охрану.

  Чтобы применить время постановки на охрану к другим дням, нажмите **Повторить (Repeat)** и выберите нужные дни.
- **Принудительная поставка на охрану (Forced Arming)**: Выберите при необходимости.

Приложение 1 События сбоя постановки на охрану и их описание

Таблица приложения 1-1 События сбоя постановки на охрану и описание (периферийные устройства)

№	Причина	Описание
1	ModuleLoss	Периферийное устройство не в сети
2	HeartError	Пакеты опроса не отправлялись более 18 минут.
3	Alarm	Круглосуточная тревога.
4	Open	Задняя крышка устройства была открыта.
5	exOpen	Задняя крышка внешнего устройства была открыта.
6	Tamper	Сработала противокражная сигнализация периферийного устройства.
7	LowBattery	Обнаружен низкий заряд батареи устройства.
8	PriPowerLoss	Обнаружен отказ основного источника питания периферийного устройства.
9	BatteryLoss	Обнаружен отказ аккумулятора.
10	OverVoltage	Обнаружено перенапряжение.
11	OverCurrent	Обнаружена перегрузка по току.
12	OverHeat	Обнаружен перегрев
13	FireAlarm	Сработала пожарная сигнализация.
14	MedicalAlarm	Сработала медицинская сигнализация.
15	SOS-Alarm	Сработал экстренная сигнализация SOS.
16	PanicAlarm	Сработала сигнализация тревожной кнопки.
17	Gas-Alarm	Сработала сигнализация утечки газа.
18	IntrusionAlarm	Сработала сигнализация проникновения.
19	HoldUpAlarm	Сработала сигнализация тревожной кнопки.

Таблица приложения 1-2 События сбоя постановки на охрану и описание (контроллер)

№	Причина	Описание
1	SOSAlert	Тревожная сигнализация может быть активирована через приложение DMSS.
2	Tamper	Сработала противокражная сигнализация контроллера.
3	Server Connect Error	Контроллер не в сети
4	SIAServer Connect Error	Произошла ошибка в соединении между контроллером и центром обработки тревог по протоколу SIA.

№	Причина	Описание
5	LowBattery	Обнаружен низкий заряд аккумулятора.
6	MainLoss	Обнаружен отказ основного источника питания.
7	BatteryLoss	Обнаружен отказ аккумулятора.
8	NoGSM	Обнаружены ошибки модуля 2G / 4G.
9	ATS Fault	Обнаружена неисправность системы охранной сигнализации.
10	Cellular Network ATP Fault	Обнаружена ошибка пути передачи сигнала тревоги (сбой сотовой сети).
11	Wired Network/Wi-Fi ATP Fault	Обнаружена ошибка в пути передачи сигнала тревоги (сбой проводной сети или Wi-Fi).

Приложение 2 Коды событий SIA и описание

Таблица приложения 2-1 Коды событий SIA и описание

№	Событие	Код CID	Описание
1	Обнаружение движения	130	130: Тревога взлома.
		133	133: Круглосуточная тревога (сейф)
		134	134: Тревога входа/выхода.
2	Обнаружено действие открытия / Обнаружено действие закрытия	130	130: Тревога взлома.
		133	133: Круглосуточная тревога (сейф)
		134	134: Тревога входа/выхода.
3	Внешний контакт был разомкнут / Внешний контакт был замкнут	130	130: Тревога взлома.
		133	133: Круглосуточная тревога (сейф)
		134	134: Тревога входа / выхода.
4	Тревога открытия под принуждением	121	Тревога открытия под принуждением
5	Была нажата тревожная кнопка	120	Сигнал тревожной кнопки
6	Тревога взлома проникновения	130	130: Тревога взлома.
		133	133: Круглосуточная тревога (сейф)
		134	134: Тревога входа/выхода.
7	Пожарная сигнализация	110	Пожарная сигнализация
8	Обнаружена утечка газа	151	Тревога утечки газа.
9	Была нажата кнопка медицинской тревоги	100	Медицинская тревога.
10	Была нажата тревожная кнопка ограниченного доступа	120	Сигнал тревожной кнопки
11	Извещатель разбития стекла	130	130: Тревога взлома.
		133	133: Круглосуточная тревога (сейф)
		134	134: Тревога входа/выхода.
12	Обнаружен наклон	130	130: Тревога взлома.

№	Событие	Код CID	Описание
		133	133: Круглосуточная тревога (сейф)
		134	134: Тревога входа/выхода.
13	Обнаружен удар	130	130: Тревога взлома.
		133	133: Круглосуточная тревога (сейф)
		134	134: Тревога входа/выхода.
14	Крышка панели управления была открыта / Крышка панели управления была закрыта	137	Противокражная сигнализация.
15	Крышка периферийного устройства была открыта / Крышка периферийного устройства была закрыта	137	Противокражная сигнализация периферийного устройства.
16	Крышка внешнего устройства была открыта / Крышка внешнего устройства была закрыта	137	Противокражная сигнализация периферийного устройства.
17	Обнаружение утечки воды / Утечка воды остановлена	154	Утечка воды.
18	Низкий заряд батареи / Уровень заряда восстановлен	302	Низкий уровень заряда системной батареи.
19	Неисправность батареи / Батарея восстановлена	311	Батарея отсутствует / неисправна.
20	Сбой основного источника питания / Восстановление основного источника питания	301	Потеря переменного тока.
21	Глушение радиосигнала	344	Обнаружение помех радиочастотным приемником.
22	Неисправность системы охранной сигнализации / устранена	350	Проблемы со связью.

№	Событие	Код CID	Описание
23	Путь передачи сигнала тревоги: Сбой проводной сети или Wi-Fi / устранен	350	Проблемы со связью.
24	Путь передачи сигнала тревоги: Сбой сотовой сети / устранен	350	Проблемы со связью.
25	Периферийное соединение потеряно / Периферийное соединение восстановлено	355	Потеря радиоканального контроля
26	Разряжена батарея периферийного устройства / Восстановлен уровень заряда батареи периферийного устройства	302	Низкий уровень заряда системной батареи.
27	Сбой батареи периферийного устройства / Сбой батареи периферийного устройства устранен	311	Батарея отсутствует / неисправна.
28	Сбой основного источника питания периферийного устройства / Сбой основного источника питания периферийного устройства устранен	301	Потеря переменного тока.
29	Сбой соединения RF-HD / Соединение RF-HD восстановлено	354	Не удалось сообщить о событии.
30	Устройство заблокировано и разблокировано	501	Считыватель контроля доступа отключен.
31	Сработала защита от перенапряжения / Защита от перенапряжения восстановлена	319	Перенапряжение источника питания.

№	Событие	Код CID	Описание
32	Сработала защита от перегрузки по току / Восстановлена защита от перегрузки по току	312	Перегрузка источника питания по току.
33	Сработала защита от перегрева / Защита от перегрева восстановлена	318	Перегрев источника питания.
34	Высокая температура / Нормальная температура	158	Высокая температура.
35	Низкая температура / Нормальная температура	159	Низкая температура
36	Постановка на охрану	400 (Приложение)	400: Открыто / закрыто.
		401 (Пульт)	401: Пользователь открыл / закрыл.
		403 (Постановка на охрану по расписанию)	403: Автоматическое открытие / закрытие.
		407 (Брелок)	407: Удаленная постановка на охрану или снятие с охраны.
		408 (Глобальная постановка на охрану)	408: Быстрая постановка на охрану.
37	Снятие с охраны	400 (Приложение)	400 Открыто / закрыто.
		401 (Пульт)	401 Пользователь открыл / закрыл.
		403 (Постановка на охрану по расписанию)	403 Автоматическое открытие / закрытие.
		407 (Брелок)	407 Удаленная постановка на охрану или снятие с охраны.
38	Активирован режим В присутствии	441	Оставлена постановка на охрану
39	Неудачная постановка на охрану	454 (Сбой постановки на охрану)	454 Не удалось закрыть.
		455 (Ошибка постановки на охрану по расписанию)	455 Сбой автоматической постановки на охрану.

№	Событие	Код CID	Описание
		457 (Сбой постановки на охрану с задержкой выхода)	457 Ошибка выхода (пользователь).
40	Постановка на охрану с ошибками.	450	Ошибка открытия / закрытия.
41	Временно деактивирован / активирован	502	Временно деактивирован.
42	Временно отключены уведомления для крышки / Включены уведомления для крышки	503	Временно отключен.
43	Отчет о тестировании был запущен вручную	601	Отчет об испытании вручную.
44	Отчет о периодическом испытании	602	Отчет о периодическом испытании.

Приложение 3 Рекомендации по обеспечению кибербезопасности

Кибербезопасность – это больше, чем просто популярное слово. Она в той или иной мере затрагивает любое устройство, подключенное к Интернету. IP-видеонаблюдение не застраховано от угроз кибербезопасности, но принятие основных мер по защите и укреплению безопасности сетей и сетевых устройств сделает их менее уязвимыми для атак. Ниже приведены несколько советов и рекомендаций от Dahua о том, как создать более защищенную систему безопасности.

Обязательные предосторожности для обеспечения базовой сетевой безопасности устройства:

1. **Используйте надежные пароли**

   Обратите внимание на следующие рекомендации по установке паролей:

   - Длина пароля должна составлять не менее 8 символов.
   - Используйте по меньшей мере два типа символов, к которым относятся буквы верхнего и нижнего регистров, цифры и специальные символы.
   - Не используйте имя аккаунта ни в прямом, ни в обратном порядке.
   - Не используйте символы, идущие по порядку, например, «123», «abc» и т.д.
   - Не используйте идущие подряд одинаковые символы, например, «111», «aaa» и т.д.

2. **Своевременно обновляйте прошивку и клиентское программное обеспечение**

   - В соответствии со стандартной процедурой в индустрии высоких технологий мы рекомендуем обновлять прошивку вашего устройства (например, IP-видеорегистратора, цифрового видеорегистратора, IP-видеокамеры и т.д.), чтобы система была защищена последними обновлениями безопасности и исправлениями ошибок. Когда устройство подключено к общедоступной сети, рекомендуется включить функцию автоматической проверки обновлений, чтобы своевременно получать информацию об обновлениях прошивки, выпущенных производителем.
   - Мы предлагаем вам загрузить и использовать последнюю версию клиентского программного обеспечения.

Желательные, но не обязательные рекомендации для повышения уровня сетевой безопасности вашего устройства:

1. **Физическая защита**

   Мы предлагаем вам обеспечить физическую защиту устройства, особенно это касается устройств хранения. Например, установите устройство в специальное серверное помещение или шкаф для оборудования и организуйте продуманный контроль доступа и ключей, чтобы предотвратить физический доступ к устройству посторонних и повреждение оборудования, несанкционированное подключение съемного накопителя (например, USB-накопителя) или к последовательному порту) и т.д.

2. **Регулярно меняйте пароли**

   Мы рекомендуем регулярно менять пароли, чтобы уменьшить риск угадывания или взлома.

3. **Своевременно введите и обновляйте информацию для сброса пароля**

   Устройство поддерживает функцию сброса пароля. Своевременно введите

соответствующую информацию для сброса пароля, включая адрес e-mail конечного пользователя и контрольные вопросы для сброса пароля. Своевременно обновляйте эту информацию в случае ее изменения. При вводе контрольных вопросов для сброса пароля рекомендуется избегать таких, которые можно легко угадать.

4. **Пользуйтесь функцией блокировки аккаунта**
   Функция блокировки аккаунта включена по умолчанию, и мы рекомендуем вам оставить ее включенной, чтобы гарантировать безопасность аккаунта. Если злоумышленник несколько раз попытается войти в систему с неправильным паролем, соответствующий аккаунт и исходящий IP-адрес будут заблокированы.
5. **Измените порт HTTP по умолчанию и другие служебные порты**
   Мы предлагаем вам изменить порты HTTP и других служб по умолчанию на любое значение в диапазоне от 1024 до 65535, чтобы снизить риск того, что посторонние смогут угадать, какие порты вы используете.
6. **Включите протокол HTTPS**
   Мы предлагаем вам включить протокол HTTPS, чтобы вы подключались к веб-интерфейсу по защищенному каналу связи.
7. **Привязка MAC-адреса**
   Мы рекомендуем вам привязать IP-адрес и MAC-адрес шлюза к устройству, что снизит риск атаки типа ARP-spoofing.
8. **Назначайте аккаунты и права доступа разумно**
   В соответствии с потребностями вашей деятельности и администрирования разумно добавляйте пользователей и назначайте им минимально необходимый набор прав доступа.
9. **Отключите ненужные службы и используйте безопасные протоколы**
   Для снижения рисков рекомендуется отключать такие службы, как SNMP, SMTP, UPnP и т.д., если они не используются.
   Настоятельно рекомендуется использовать безопасные реализации протоколов, включая, помимо прочего, следующие:
   - SNMP: выберите протокол SNMP v3 и настройте надежные пароли шифрования и пароли аутентификации.
   - SMTP: выберите протокол TLS для доступа к почтовому серверу.
   - FTP: выберите протокол SFTP и установите надежные пароли.
   - Точка доступа Wi-Fi: выберите режим шифрования WPA2-PSK и установите надежные пароли.
10. **Шифрование аудио и видео**
    Если содержимое ваших аудио- и видеоданных очень важно или конфиденциально, мы рекомендуем вам использовать функцию шифрования, чтобы снизить риск похищения аудио- и видеоданных во время передачи.
    Внимание: функция шифрования при передаче данных требует вычислительных ресурсов приведет к некоторому снижению эффективности передачи данных.
11. **Аудит безопасности**
    - Проверяйте пользователей, выполнивших вход на устройство: мы предлагаем вам регулярно проверять пользователей, выполнивших вход на устройство, чтобы отслеживать несанкционированный доступ.
    - Проверяйте журналы устройства: просматривая журналы, вы можете узнать IP-адреса, которые использовались для входа на ваши устройства, и отслеживать основные

действия пользователей.

12. **Сетевой журнал**

    Из-за ограниченного объема памяти устройства количество записей в журналах ограничено. Если вам необходимо сохранять записи журнала за длительный период времени, рекомендуется включить функцию сетевого журнала, чтобы обеспечить синхронизацию важных журналов с сервером сетевых журналов для отслеживания.

13. **Создайте безопасную сетевую среду**

    Чтобы эффективнее обеспечить безопасность устройства и снизить потенциальные риски кибербезопасности, мы рекомендуем следующее:

    - Отключите функцию преобразования портов на маршрутизаторе, чтобы исключить прямой доступа к устройствам локальной сети из внешней сети.
    - Сеть должна быть сегментирована и изолирована в соответствии с фактическими потребностями обмена данными в ней. Если нет требований к организации связи между двумя подсетями, предлагается использовать VLAN и другие технологии для сегментирования сети, чтобы добиться изоляции сетей.
    - Используйте протокол контроля доступа и аутентификации 802.1X, чтобы снизить риск несанкционированного доступа в локальных сетях.
    - Включите функцию фильтрации IP-адресов и MAC-адресов, чтобы ограничить диапазон адресов, с которых разрешен доступ к устройству.

Дополнительная информация

Посетите Центр реагирования на чрезвычайные ситуации на официальном веб-сайте Dahua, чтобы ознакомиться с уведомлениями о безопасности и последними рекомендациями по безопасности.

БЕЗОПАСНЕЕ ОБЩЕСТВО, КАЧЕСТВЕННЕЕ ЖИЗНЬ

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Адрес: №1399, улица Биньань, район Биньцзян, Ханчжоу, Китай | Веб-сайт: www.dahuasecurity.com | Почтовый индекс: 310053
E-mail: dhoverseas@dhvisiontech.com | Телефон: +86-571-87688888 28933188