Охранная панель

Руководство пользователя

Содержание

Раздел 1 Установка **5**
1.1 Типичные сцены 5
1.2 Предостережения 5
1.3 Часто задаваемые вопросы по установке 6
Глава 2 Введение **7**
Описание системы 7
Раздел 3 Запуск устройства **10**
3.1 Управление разрешениями 10
3.2 Активация 11
3.2.1 Активация через LAN или SIM-карту (4G / GPRS) 11
3.2.2 Активация через Wi-Fi 13
3.3 Отмена привязки устройства 19
3.3.1 Отмена привязки устройства к собственной учетной записи 19
3.3.1 Отмена привязки устройства к сторонней учетной записи 19
Раздел 4 Управление пользователями **22**
4.1 Управление пользователями 22
4.1.1 Приглашение администратора 22
4.1.2 Отмена доступа установщика 23
4.1.3 Добавление оператора 24
4.1.4 Удаление оператора 25
4.1.5 Отключение службы Hik-Connect 26
4.1.6 Приглашение установщика 26
4.2 Журналы доступа 27
Раздел 5 Настройка параметров **28**
5.1 Настройка с помощью Hik-ProConnect 28
5.1.1 Использование приложения Hik-ProConnect 28
5.1.2 Использование портала Hik-ProConnect 46
5.2 Настройка параметров с помощью Hik-Connect 50
5.3 Настройка параметров с помощью веб-клиента 71
5.3.1 Настройки связи 72

5.3.2 Управление устройствами 86
5.3.3 Параметры области 98
5.3.4 Управление видео 98
5.3.5 Управление разрешениями 100
5.3.6 Обслуживание 102
5.3.7 Параметры системы 106
5.3.8 Проверка статуса 117
5.4 Уведомление в ЧОП / ПЦН 118
5.4.1 Настройка ATS приемопередатчика ЧОП / ПЦН 118
5.4.2 Настройка ATS приемопередатчика панели 119
5.4.3 Тестирование сигнализации 121
Раздел 6 Общие операции 122
6.1 Постановка на охрану 122
6.2 Снятие с охраны 123
6.3 Управление SMS 123
A.Поиск неисправностей 124
A.1 Сбой связи 124
A.1.1 Конфликт IP-адресов 124
A.1.2 Веб-страница недоступна 124
A.1.3 Hik-Connect не в сети 124
A.1.4 Частое отключение IP-камеры 124
A.1.5 Ошибка добавления устройства в приложение 124
A.1.6 Информация о тревоге не передается в приложение / 124
iVMS-4200 / ЧОП / ПЦН 124
A.2 Взаимоисключаемые функции 125
A.2.1 Невозможно войти в режим регистрации 125
A.3 Ошибки зоны 125
A.3.1 Отсутствует подключение к зоне 125
A.3.2 Зона с контролем вскрытия 125
A.3.3 Срабатывание тревоги в зоне / неисправность 125
A.4 Проблемы при постановке на охрану 125

A.4.1 Сбой постановки на охрану (когда процесс постановки на охрану не запускается). 125
A.5 Сбой операции. 125
A.5.1 Не удается войти в тестовый режим 125
A.5.2 После операции сброса тревоги отчет об устранении тревоги на панели не формируется 126
A.6 Ошибка отправки электронного письма. 126
A.6.1 Не удается отправить тестовое письмо. 126
A.6.2 Не удается отправить письмо. 126
A.6.3 Не удается отправить письмо в Gmail 126
A.6.4 Не удается отправить письмо на QQ или Foxmail. 127
A.6.5 Не удается отправить письмо в Yahoo 127
A.6.6 Настройка параметров почты..... 127
Таблица B. Типы входов 129
Таблица C. Типы выходов 132
D.Типы событий 133
E.Уровни доступа 134
F.Сигнал 135
F.1 Обнаружение неисправностей ATP / ATS 135
F.1 Категория ATS. 135
G.Код SIA и CID 137

Раздел 1 Установка

1.1 Типичные сцены

Местоположение установки:

1. Охранная панель
2. Ретранслятор
3. ИК-датчик
4. Звуковой оповещатель
5. Магнитоконтактный датчик

1.2 Предостережения

1. Избегайте установки устройства на металлические поверхности.
2. Избегайте размещения устройства непосредственно на земле.
3. Запрещается использовать металлические покрытия для устройства.
4. Избегайте препятствий в радиусе 50 см вокруг устройства, за исключением поверхности установки.
5. Ретранслятор необходимо установить между контрольной панелью и периферийным устройством.
6. Перед установкой проверьте уровень сигнала. Зеленый индикатор показывает, что место подходит для установки устройства (не закрывайте датчик руками при проверке уровня сигнала).
7. Для устройств рекомендуется вертикальная установка.

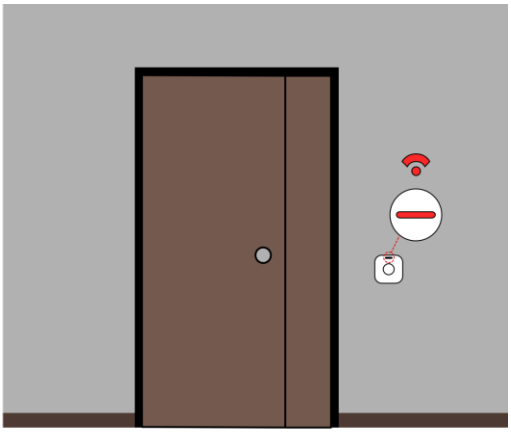
1.3 Часто задаваемые вопросы по установке

Вопрос 1.

Почему при установке передается хороший сигнал, а при фактическом использовании качество сигнала снижается?

Ответы:

Проверьте, не меняется ли рабочая среда во время установки и фактического использования. Например, проблема может быть вызвана препятствиями в виде закрытых дверей или окон.



Вопрос 2.

После завершения установки периферийное устройство отключается.

Ответы:

- Отрегулируйте положение панели управления и проверьте уровень мощности сигнала для установки.
- Установите ретранслятор между автономным периферийным устройством и панелью управления.
- Проверьте соответствие мерам предосторожности.

Глава 2 Введение

Описание системы

Охранная панель является беспроводной охранной системой, предназначенной для помещений, требующих защиты от вторжения. Система поддерживает LAN / Wi-Fi в качестве основной сети передачи. Подходит для применения в различных сценариях, таких как мониторинг объектов: офисов, фабрик, магазинов, складских помещений и т. д.

- Инновационная технология беспроводной двусторонней передачи Tri-X.
- Двусторонняя связь с шифрованием AES-128.
- Псевдослучайная перестройка рабочей частоты (FHSS) используется для снижения уровня помех, предотвращения подслушивания и обеспечения множественного доступа с кодовым разделением (CDMA).
- Голосовое сопровождение для оповещения о тревогах, индикации состояния системы, оповещения о выполняемых операциях и т. д.
- Настройка через веб-клиент, мобильный клиент и Convergence Cloud.
- Тревожные уведомления в сообщения или через телефонные звонки.
- Просмотр видео в режиме реального времени с Hik-Connect и отправка видео тревожных событий по электронной почте, Hik-ProConnect и Hik-Connect.
- Загрузка отчетов о тревогах в ARC.
- Протокол SIA-DC09, поддержка Contact ID и формата данных SIA.
- Резервная литиевая батарея 4520 мА·ч, время работы в режиме ожидания 12 часов.

Примечание

ISUP5.0: интернет-протокол конфиденциальности, который используется для доступа к сторонней платформе, поддерживающий загрузку отчетов о тревогах, управление охранной панелью и загрузку коротких видео.

Приоритет сообщения и индикации совпадает. Охранная панель загружает сообщения и включает индикаторы синхронно.

Примечание

Протокол стандарта DC-09:

ADM-CID: метод представления данных DC-09 — это CID, который не зашифрован и предназначен только для загрузки отчета о тревоге.

*ADC-CID: метод представления данных DC-09 — CID, который зашифрован и предназначен только для загрузки отчета о тревоге.

SIA-DCS: метод представления данных DC-09 — DCS (также именуемый как протокол SIA), который не зашифрован и предназначен только для загрузки отчета о тревоге.

* SIA-DCS: метод представления данных DC-09 — DCS (также именуемый как протокол SIA), который зашифрован и предназначен только для загрузки отчета о тревоге.

Инструкция RSSI для периферийных устройств

Соответствие требованиям стандарта EN 50131-5-3 4.2.2.

Уровень сигнала	**Значение RSSI**	**Индикатор**	**Примечание**
Сильный	> 120	Зеленый	Нажмите ОК для запуска установки
Средний	От 81 до 120	Желтый	Нажмите ОК для запуска установки
Слабый	От 60 до 80	Красный	Не рекомендуется, но может работать
Недействительный	От 0 до 59	Красный (мигает)	Не подходит для установки, не может работать в нормальном режиме

Примечание

Устанавливайте периферийные устройства только в том случае, если уровень сигнала выше 80. Для более эффективного функционирования системы установите уровень 120 и выше.

Параметры уведомлений

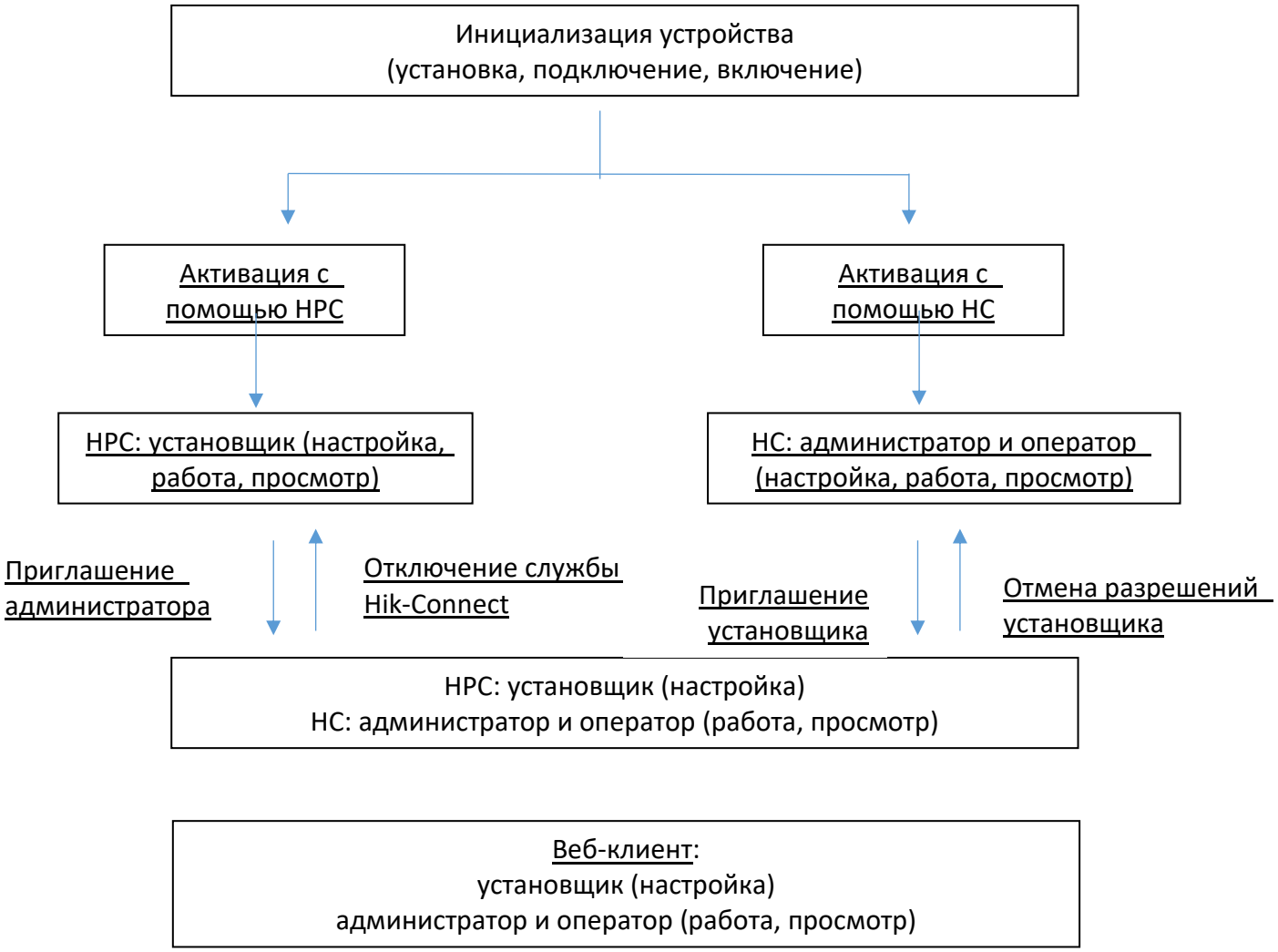
Панель подходит для следующих требований к уведомлениям вместе с необходимыми звуковыми оповещателями.

Системы уведомления	I&HAS уровень 2		
	Параметры		
	C	E	F
Автономное устройство предупреждения	2	1	Опционально
ATS	DP1	Опционально	DP2

Раздел 3 Запуск устройства

3.1 Управление разрешениями

Для активации устройства можно использовать HPC (Hik-ProConnect, APP) или HC (Hik-Connect, APP). После активации можно управлять устройством, передавая разрешения между приложениями. Также можно использовать учетную запись и пароль всех учетных записей для входа в веб-клиент и настройки устройства.



Подробные сведения приведены в ***Раздел 4 Управление пользователями***.

3.2 Активация

При инициализации устройства с помощью Hik-ProConnect or Hik-Connect, необходимо добавить охранную панель в учетную запись установщика. После завершения всех первоначальных настроек и тестирования администратору будет направлено приглашение и передано право собственности. Выполните следующие шаги для инициализации беспроводной охранной системы.
Активировать устройство можно через Wi-Fi, LAN или SIM-карту (4G / GPRS).

3.2.1 Активация через LAN или SIM-карту (4G / GPRS)

Шаг 1 Создайте объект (только для HPC)
Загрузите Hik-ProConnect и войдите в систему с учетной записью установщика.

Объект — это место, где установлена охранная система. Создайте объект, на который можно будет добавить устройство, указав его имя и адрес. Владелец объекта — конечный пользователь, обычно считающийся администратором.

Шаг 2 Подключите устройство к сети
Подключите устройство к сети Ethernet с помощью LAN или SIM-карты и включите устройство.

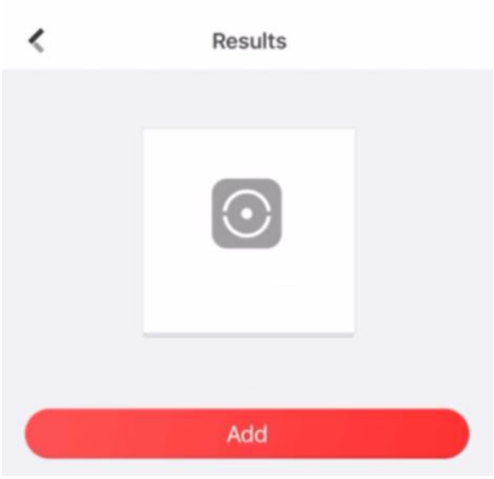
Примечание
- Пока устройство включено, LED-индикаторы питания и связи горят зеленым светом.
- Как только устройство подключится к сети, LED-индикатор станет гореть зеленым.
- Проверьте подключение SIM-карты к сети.

Шаг 3 Добавьте устройство
1. Откройте объект (только для HPC).

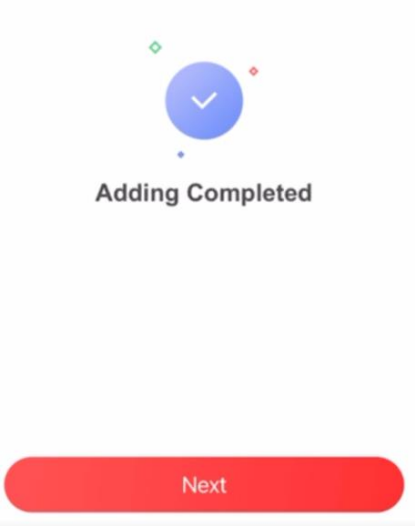
Примечание
При инициализации устройства с помощью Hik-Connect создание объекта не требуется.

2. Нажмите + и сканируйте QR-код на этикетке панели.

3. Нажмите **Add** («Добавить»).



4. Нажмите **Next** («Далее»). Здесь можно отредактировать параметры устройства или пропустить этот шаг, чтобы начать использовать устройство.



Охранная панель будет добавлена на объект, (HPC: созданный и управляемый учетной записью установщика, что также означает, что учетная запись установщика была создана в панели.

После этого установщик может выполнять настройку и тестирование панели перед развертыванием. В службу Hik-Connect и в локальный веб-клиент можно войти с использованием учетной записи установщика Hik-ProConnect.

Примечание

При инициализации устройства с помощью Hik-Connect создание объекта не требуется. Загрузите и войдите в приложение, затем добавьте устройство путем сканирования QR-кода или введите серийный номер устройства вручную.

3.2.2 Активация через Wi-Fi

Шаг 1 Создайте объект (только для HPC)
Загрузите Hik-ProConnect и войдите в систему с учетной записью установщика.

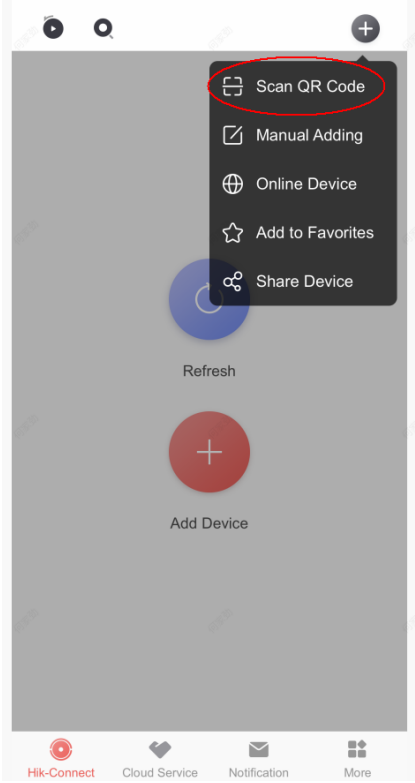
Объект — это место, где установлена охранная система. Создайте объект, на который можно будет добавить устройство, указав его имя и адрес. Владелец объекта — конечный пользователь, обычно считающийся администратором.

Шаг 2 Настройте сеть в приложении
1. Загрузите Hik-Connect / Hik-ProConnect и войдите в систему.

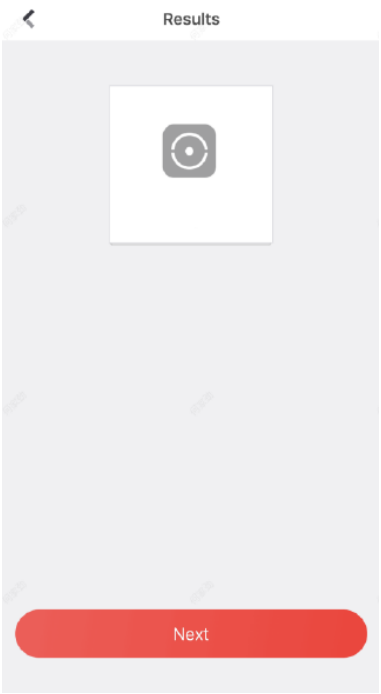
2. Включите охранную панель.

3. Подключите телефон к домашней сети Wi-Fi. Проверьте работу сети Wi-Fi и стабильность сигнала.

4. Откройте HC или HPC, нажмите **+**, затем выберите **Scan QR Code** («Сканирование QR-кода»).

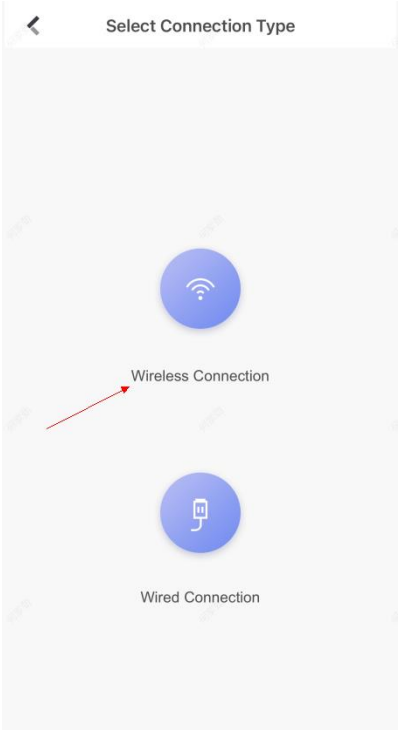


5. Отсканируйте QR-код на обратной стороне охранной панели и дождитесь результата.

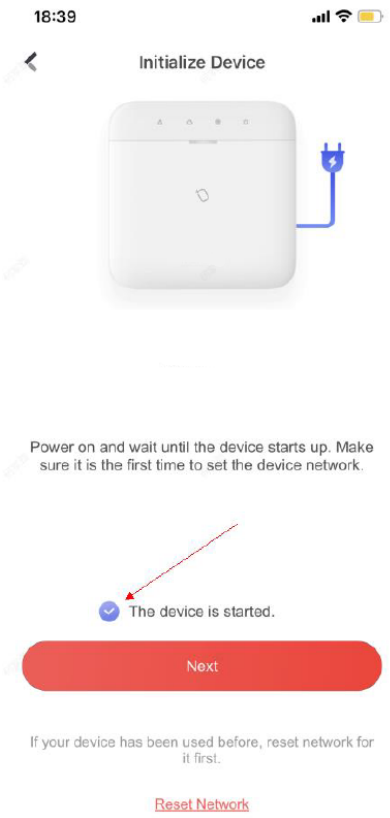


6. Нажмите **Next** («Далее»).

7. Нажмите **Wireless Connection** («Беспроводное соединение»).



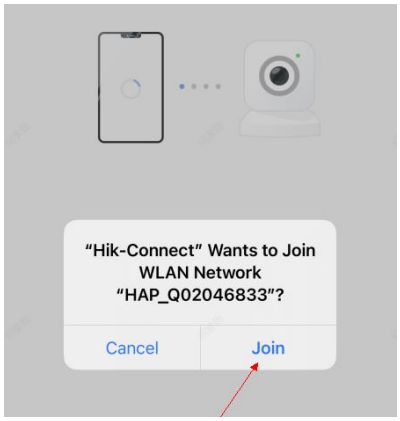
8. Поставьте галочку **The device is started** («Устройство запущено»). Нажмите **Next** («Далее»).



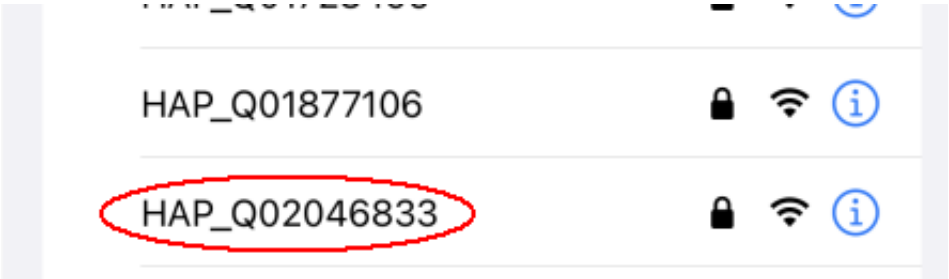
9. Приложение автоматически заполнит страницу домашним Wi-Fi, используемым в настоящее время мобильным телефоном, как показано на рисунке ниже. После подтверждения пароля Wi-Fi нажмите **Next** («Далее»).

10. Нажмите **Connect to a Network** («Подключить к сети»).

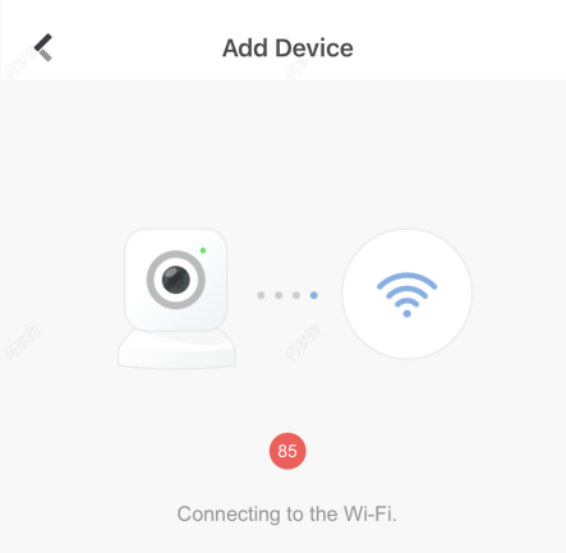
11. Нажмите **Join** («Присоединиться»). Мобильный телефон отключит домашний Wi-Fi. После установления связи с охранной панелью мобильный телефон автоматически переключится обратно на домашний Wi-Fi.



Как показано на рисунке выше, во время обмена информацией подключаться к Wi-Fi можно с именем «HAP_serial number» (серийный номер панели).

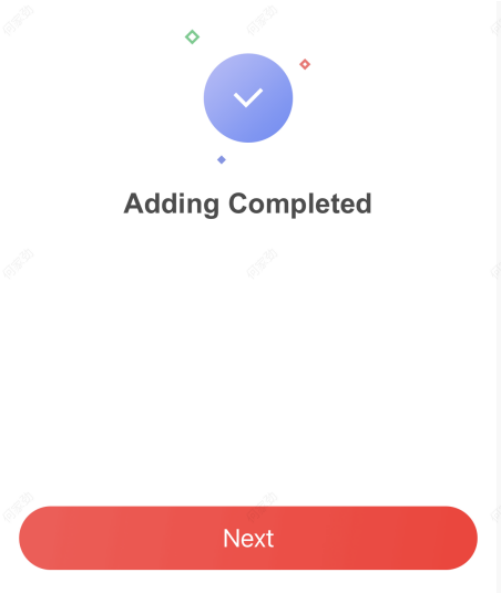


12. После того, как панель управления передаст сообщение **Exit hotspot mode** («Выход из режима точки доступа»), появится следующая страница.

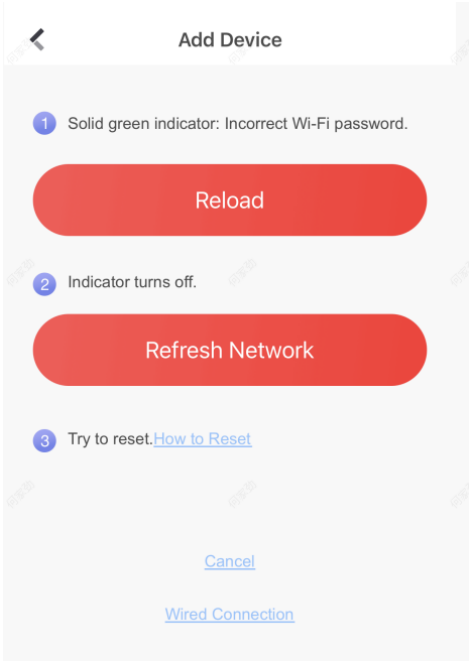


13. Дождитесь, пока устройство подключится к домашнему Wi-Fi и войдите в облачное хранилище EZVIZ.

(1) При достижении стабильного сигнала домашнего Wi-Fi, панель управления успешно войдет в облачное хранилище EZVIZ и завершит привязку до окончания обратного отсчета.

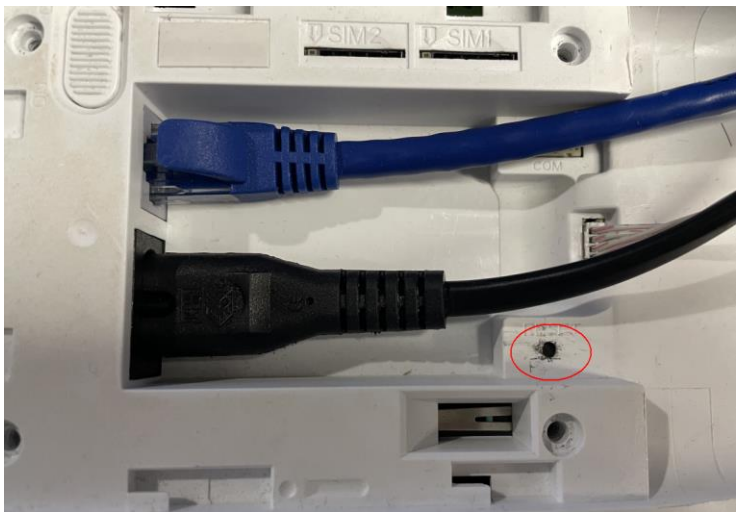


(2) Если сигнал домашнего Wi-Fi нестабилен, панель управления может не подключиться к облачному хранилищу EZVIZ до окончания обратного отсчета, и появится следующая страница:



Проверьте корректность пароля домашней сети Wi-Fi, нажмите **Refresh Network** («Обновить сеть»). Панель управления введет новый обратный отсчет. Дождитесь установления соединения.

Чтобы изменить домашний Wi-Fi, следует сначала изменить домашний Wi-Fi, затем нажать **RESET** («Сброс») на задней панели управления (отмечена на рисунке ниже). Прослушайте голосовое сообщение **Enter hotspot mode** («Войти в режим точки доступа»), нажмите **Reload** («Перезагрузить»). Интерфейс вернется к шагу 9. После этого можно снова настроить параметры сети.



Примечание

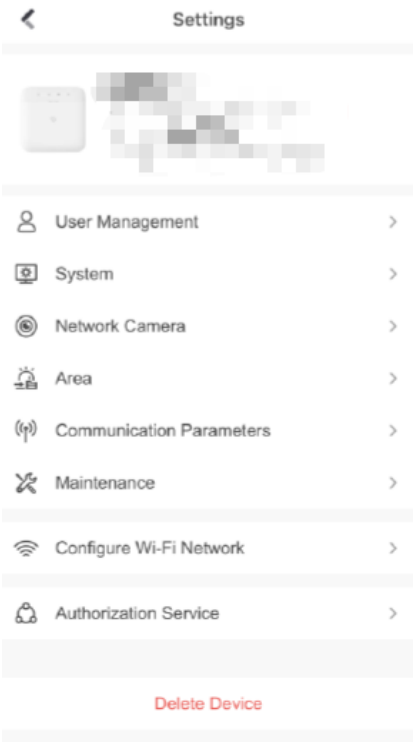
Как только устройство подключится к сети, LED-индикатор станет гореть зеленым .

3.3 Отмена привязки устройства

3.3.1 Отмена привязки устройства к собственной учетной записи

Когда устройство привязано к учетной записи, удалить его можно напрямую.

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек охранной панели.
2. Нажмите .
3. Нажмите **Delete Device** («Удалить устройство»).

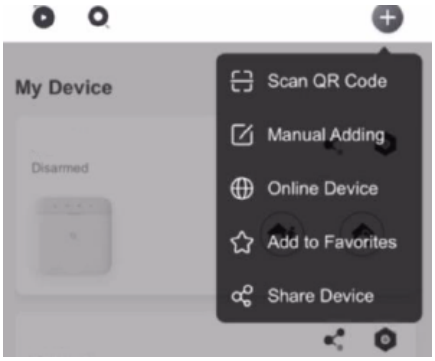


3.3.1 Отмена привязки устройства к сторонней учетной записи

Возьмите панель управления.

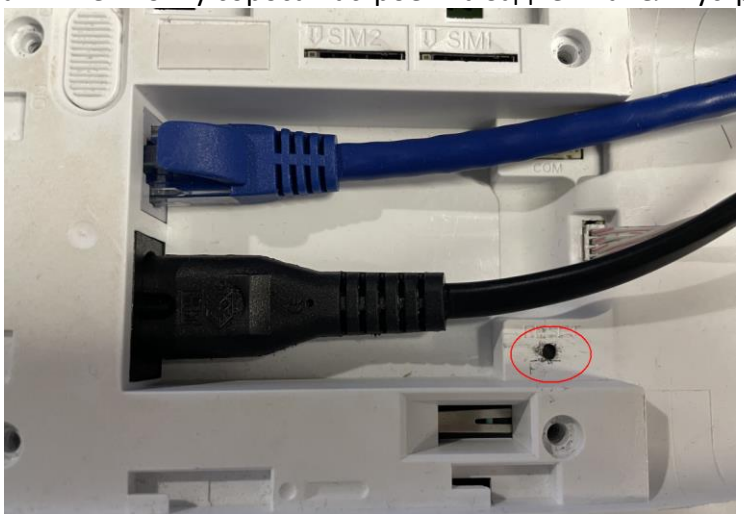
Телефон и устройство должны находиться в одном сегменте сети.

1. Откройте НС / НРС и нажмите **+**.
2. Нажмите **Scan QR Code** («Сканировать QR-код»).

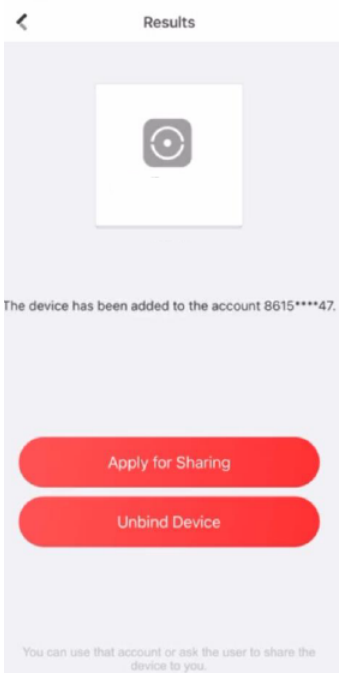


3. Сканируйте QR-код на этикетке устройства.

4. Дважды быстро нажмите кнопку сброса настроек на задней панели устройства.



5. Нажмите **Unbind Device** («Отмена привязки устройства»).



5. Введите проверочный код и нажмите **Finish** («**Завершить»)**.

Привязка устройства к учетной записи будет отменена. После этого устройство можно добавить в свою учетную запись.

Раздел 4 Управление пользователями

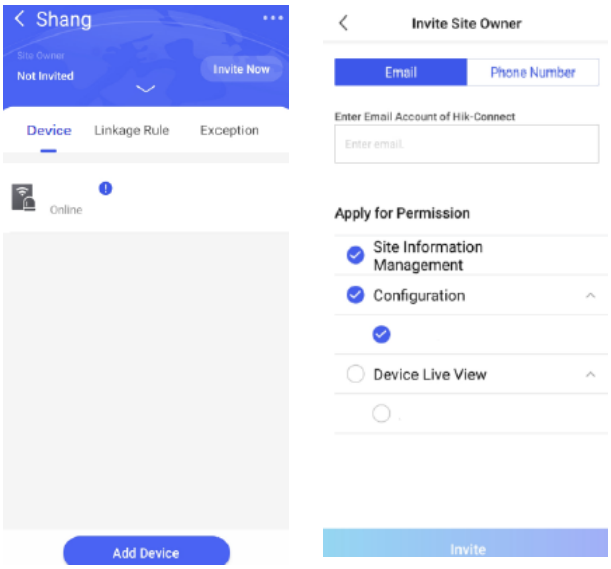
4.1 Управление пользователями

Примечание

- Пользователи могут быть созданы в клиентском ПО.
- Имя и пароль сетевого пользователя (веб-клиента и пользователя приложения) могут содержать от 1 до 32 символов и от 8 до 16 символов соответственно.

4.1.1 Приглашение администратора

Администратор также является владельцем объекта в службе Hik-ProConnect.



После завершения начальной настройки установщик должен пригласить владельца объекта и запросить разрешение на управление объектом и настройку устройства из учетной записи администратора. Учетная запись администратора будет учетной записью конечного пользователя в службе Hik-Connect.

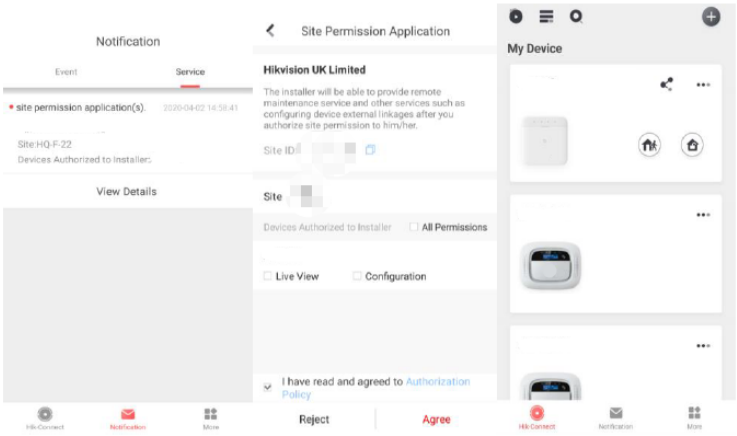
1. Нажмите кнопку **Invite Now** («Пригласить сейчас») и введите адрес электронной почты или номер телефона, чтобы передать право собственности на объект администратору. В то же время установщик должен запросить разрешение от владельца объекта, в частности, разрешения на настройку и управление объектом.
2. Опционально. Поставьте галочку **Allow Me to Disable Hik-Connect Service** («Разрешить отключение службы Hik-Connect»).

Примечание

- Если флажок установлен, после передачи объекта клиенту и одобрения запроса клиентом, можно отключить Hik-Connect для устройств, которые не были переданы клиенту без его / ее разрешения. Если служба Hik-Connect отключена, клиент не сможет работать на этих устройствах через мобильный клиент Hik-Connect.

3. Откройте приложение Hik-Connect и войдите в систему под учетной записью администратора. Запрос на услуги установщика будет получен на странице уведомления. Откройте подробные сведения об уведомлении, чтобы принять службу установщика и разрешения на настройку. Панель управления и другие устройства на объекте будут отображаться в списке устройств.

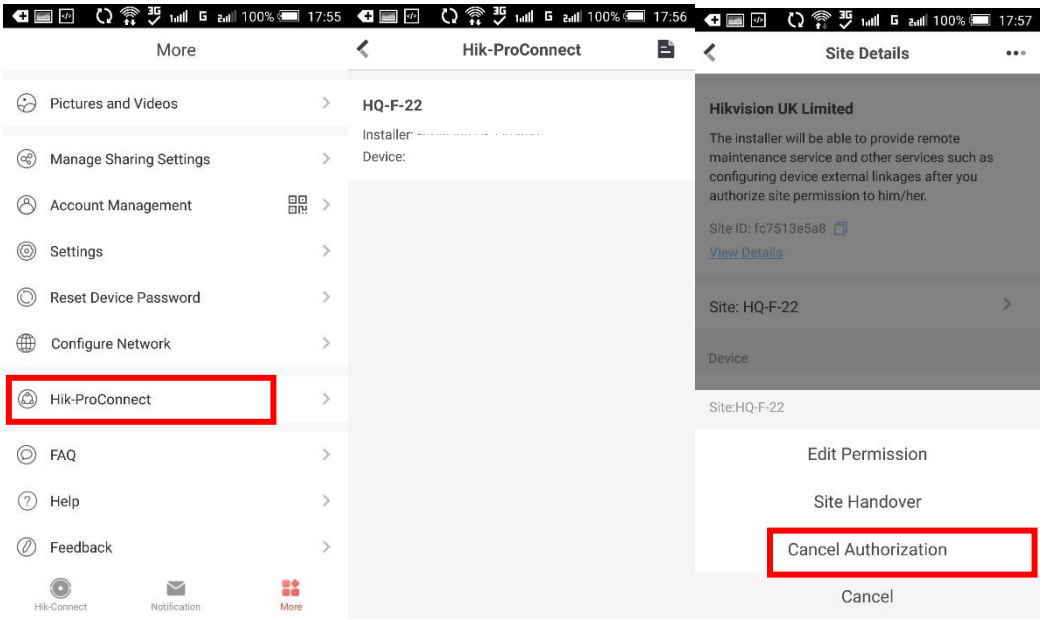
Учетная запись администратора будет добавлена в панель управления, которую можно использовать для входа в приложение Hik-Connect и локальный веб-клиент.



4.1.2 Отмена доступа установщика

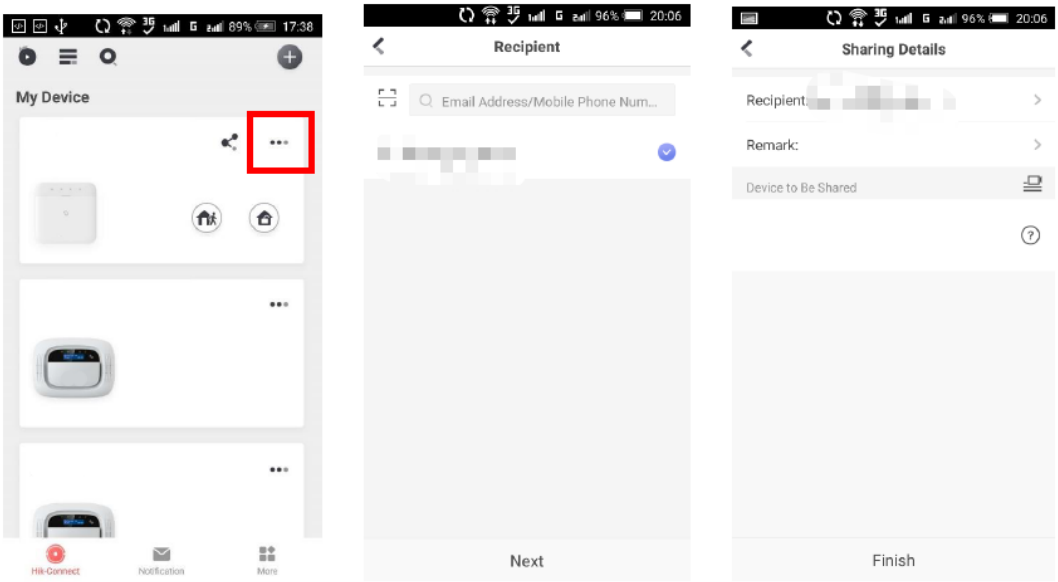
Администратор может отменить авторизацию установщика.

1. Войдите на страницу **More** («Показать еще») и нажмите Hik-ProConnect. Все объекты, управляемые службой Hik-ProConnect, будут перечислены на странице.
2. Нажмите на кнопки выбора в правом верхнем углу страницы сведений об объекте и нажмите **Cancel Authorization** («Отменить авторизацию») в меню подсказки.
3. Подтвердите операцию, чтобы отменить авторизацию установщика. После отмены авторизации для доступа к системе установщик должен снова подать запрос на получение авторизации.



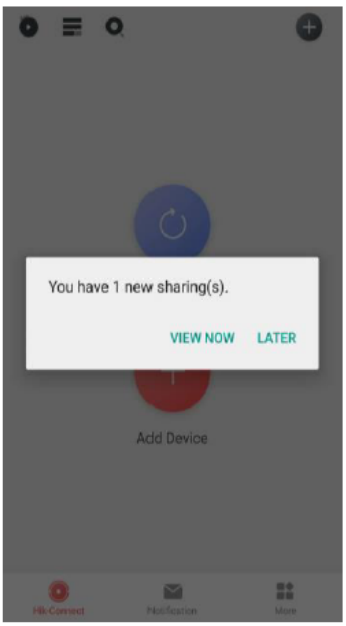
4.1.3 Добавление оператора

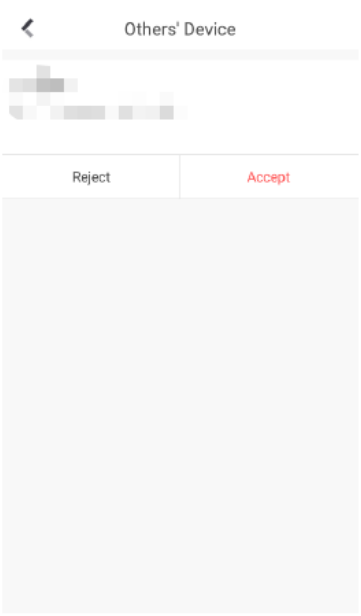
Администратор может поделиться устройством с другими операторами.

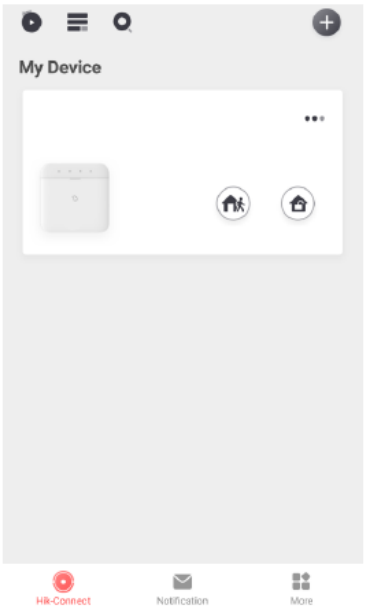


1. Нажмите  («Поделиться») в списке устройств.
2. Войдите в учетную запись оператора Hik-Connect.

   Администратор также может выбрать, к какому устройству будет предоставлен общий доступ.







Сообщение о совместном использовании будет отправлено на учетную запись оператора, и оператор сможет прочитать сообщение в приложении Hik-Connect.

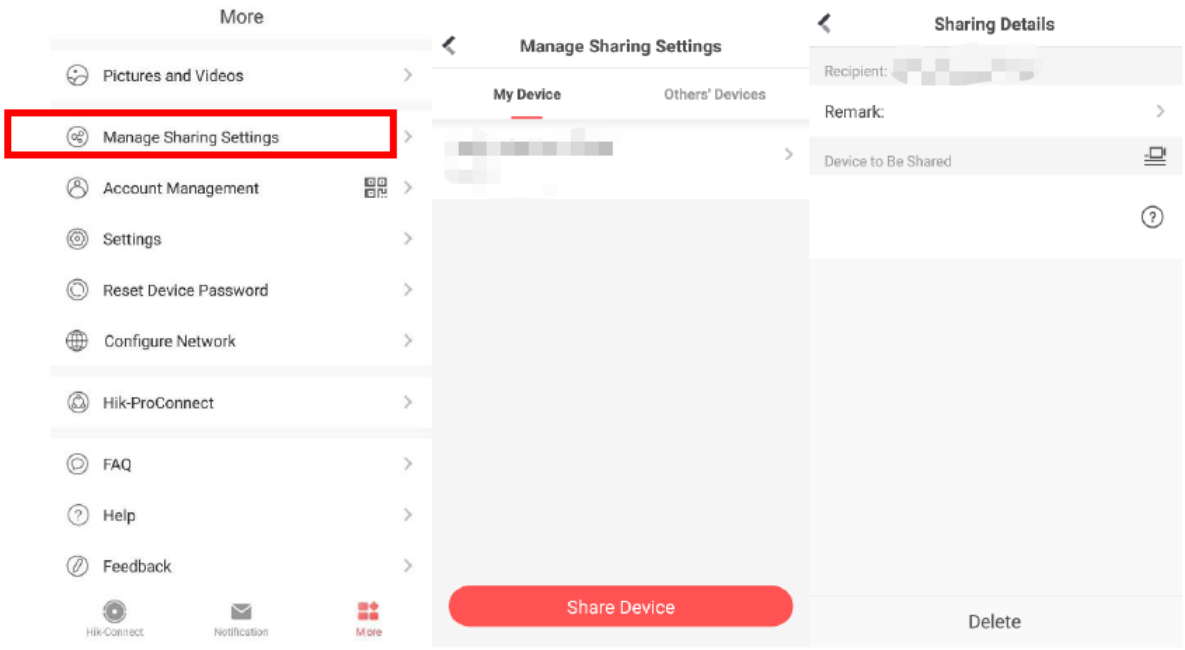
3. Примите приглашение, и устройство появится в списке устройств.

Учетная запись оператора будет добавлена в панель управления, которую можно использовать для входа в приложение Hik-Connect и локальный веб-клиент.

4.1.4 Удаление оператора

Пользователь-администратор может удалить оператора.

1. Войдите на страницу **More** («Показать еще») и нажмите **Manage Sharing Settings** («Управление настройками общего доступа»).
2. Удалите выбранного оператора или исключите его из устройства.



4.1.5 Отключение службы Hik-Connect

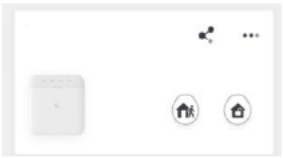
Примечание

- Объект должен быть арендным.
- Установщик на стороне HPC должен установить флажок **Allow Me to Disable Hik-Connect Service** («Разрешить отключать службу Hik-Connect») при приглашении администратора, и администратор на стороне HC также принимает этот параметр.

Перейдите на вкладку **Device** («Устройство»), чтобы отключить службу Hik-Connect для одного устройства или всех устройств на этом объекте, нажав или установив переключатель службы Hik-Connect в положение «Выкл.». Также можно удалить устройства из учетной записи Hik-Connect конечного пользователя без авторизации конечного пользователя.

4.1.6 Приглашение установщика

1. В HC нажмите в списке устройств.



2. Нажмите **Share with Installer** («Поделиться с установщиком») и введите адрес электронной почты.
3. Нажмите **OK**.

4. Нажмите → **Share with Installer** → **Share QR Code** («Поделиться с установщиком → Поделиться QR-кодом»).
5. В HPC выберите объект и нажмите **Add Device** («Добавить устройство»).
6. Сканируйте QR-код.
7. В HC пользователь получит приложение для авторизации устройства. Перейдите на страницу приложения и нажмите **Agree** («Согласен»).
8. Перейдите в меню **Cloud Service** → **Device Authorization** → → **Authorize More Devices** («Облачная служба → Авторизация устройства → Авторизовать больше устройств»).
9. Выберите устройства и разрешения.
10. Нажмите **OK**, и устройства будут авторизованы для установщика и добавлены на объект.

4.2 Журналы доступа

Установщику и операторам охранной панели назначены разные уровни доступа, определяющие системные функции, которые может выполнять отдельный пользователь. Для разных ролей пользователей с определенным уровнем доступа предусмотрены различные журналы записей доступа.

Журналы доступа для установщиков (уровень доступа 3)

- **Служба Hik-ProConnect**
  Hik-ProConnect — это сервис для установщиков, который используется для удаленного управления охранными системами клиентов, расположенными на различных объектах. Панели управления можно добавить в учетную запись установщика в сервисе Hik-ProConnect и управлять ими на объектах.
- **Локальный веб-клиент**
  Перейдите по IP-адресу устройства, который можно узнать с помощью инструмента SADP. Установщик может войти в систему с учетной записью службы Hik-ProConnect после добавления панели.
- **Другие записи**
  PIN-коды клавиатуры и теги также могут быть назначены установщикам на определенном уровне доступа для выполнения ключевых операций.

Журналы доступа для администратора и операторов (уровень доступа 2)

- **Служба Hik-Connect**
  Сервис Hik-Connect может использоваться конечными пользователями для доступа к устройствам и управления ими.
- **Локальный веб-клиент (для администратора)**
  Как только панель добавлена к учетной записи конечного пользователя в службе

  Hik-Connect, учетная запись Hik-Connect может использоваться для входа во встроенный веб-клиент. Операторы не могут войти в веб-клиент.
- **Другие записи**
  PIN-коды клавиатуры и теги также могут быть назначены конечным пользователям на определенном уровне доступа для выполнения ключевых операций.

Раздел 5 Настройка параметров

5.1 Настройка с помощью Hik-ProConnect

5.1.1 Использование приложения Hik-ProConnect

Установщик может использовать Hik-Proconnect для настройки охранной панели, в частности, для активации, регистрации устройства и т. д.

Загрузка и вход в Hik-ProConnect

Загрузите мобильный клиент Hik-ProConnect и выполните вход в систему перед началом работы с охранной панелью.

Шаги

1. Загрузите мобильный клиент Hik-ProConnect.
2. Опционально. Зарегистрируйте новую учетную запись, если мобильный клиент Hik-ProConnect используется впервые.

Примечание

- Подробная информация представлена в *Руководстве пользователя мобильного клиента Hik-ProConnect.*
- Для регистрации понадобится код приглашения. Обратитесь в службу технической поддержки.

3. Запустите и войдите в клиент.

Добавление охранной панели в мобильный клиент

Добавьте охранную панель в мобильный клиент перед другими операциями. **Шаги**

1. Включите охранную панель.
2. Создайте или выполните поиск на сайте.
   - Нажмите **+**, задайте название объекта, часовой пояс, адрес, город, страну / провинцию /регион и нажмите **OK**, чтобы создать объект.
   - Введите название объекта в области поиска и нажмите на значок поиска, чтобы выполнить поиск по объекту.
3. Нажмите на вкладку **Add Device** («Добавить устройство»).
   - Нажмите **Scan QR Code** («Сканировать QR-код»), чтобы перейти на соответствующую страницу. Сканируйте QR-код на панели.

     Примечание

     Обычно QR-код находится на этикетке на задней крышке панели.

Нажмите **Manual Adding** («Добавление вручную»), чтобы перейти на соответствующую страницу. Введите серийный номер устройства и проверочный код для добавления устройства.

4. Активируйте устройство.

Добавление периферийных устройств на охранную панель

Добавьте периферийные устройства на панель.

Шаги

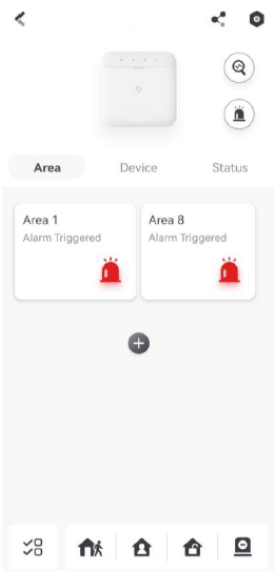
1. Выберите объект.
2. Выберите устройство управления (охранную панель).
3. Нажмите на иконку **+**.
   - Сканируйте QR-код на панели периферийного устройства.
   - Нажмите для перехода на страницу ввода вручную. Введите серийный номер устройства и выберите тип устройства для добавления устройства.

Основная страница

Здесь можно просматривать неисправности, ставить и снимать области с охраны, просматривать состояние устройства и т. д.

На странице списка устройств, выберите охранную панель и выполните вход в систему

(при необходимости), чтобы перейти на страницу настроек охранной панели.



Активация тревоги

Нажмите для выбора **Audible Panic Alarm** («Тревога экстренного вызова») или **Silent Panic Alarm** («Беззвучная сигнализации экстренного вызова»).

Просмотр неисправностей

Нажмите для просмотра неисправностей.

Управление параметрами области

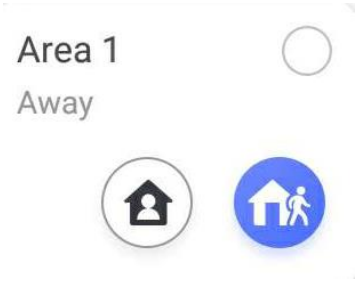
Нажмите **+**, чтобы добавить область.

Выберите область, чтобы вернуться на страницу управления устройством. Подробная информация представлена в разделе ***Настройка расписания снятия / постановки на охрану.***

Постановка на охрану / снятие с охраны

При необходимости можно поставить область на охрану или снять область с охраны. На странице списка устройств, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу области.

Операции в одной зоне



- **Away Arming («Полная постановка на охрану»):** нажмите , чтобы активировать режим охраны одной области при выходе из области. После выхода людей из области, включите режим постановки на охрану при выходе из области, чтобы поставить все зоны на охрану после установленного времени.
- **Stay Arming («Частичная охрана»):** нажмите , чтобы активировать частичный режим охраны. Во время нахождения посетителей в зоне обнаружения, включите режим постановки на охрану, чтобы включить обнаружение несанкционированных вторжений по всему периметру.

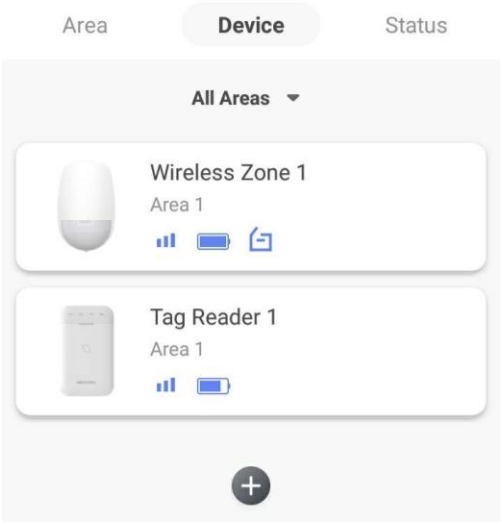
Операции в нескольких зонах

- Выбор областей. Нажмите , чтобы выбрать области, которыми вы хотите управлять. Если не выбрать области, следующие операции будут применены ко всем областям.
- **Away Arming** («Полная постановка на охрану»): нажмите , чтобы активировать режим полной постановки на охрану выбранных областей. После выхода людей из области, включите режим постановки на охрану при выходе из области, чтобы поставить все зоны на охрану после установленного времени.
- **Stay Arming** («Частичная охрана»): нажмите , чтобы активировать режим охраны всех областей. Во время нахождения посетителей в зоне обнаружения, включите режим постановки на охрану, чтобы включить обнаружение несанкционированных вторжений по всему периметру (например, датчик обнаружения по периметру, магнитоконтактный датчик и датчик, срабатывающий на движение штор на балконе) во всех зонах всех областей. В это время датчики внутри зоны обнаружения блокируются (например, ИК-датчики). Тревога не сработает при перемещении посетителей внутри зоны. **Disarming**
- **(«Снятие с охраны»):** нажмите для снятия охраны всех областей.
  В режиме снятия с охраны тревога в зонах всех областей не будет срабатывать, в том числе при обнаружении тревожных событий.

- **Silent Panic Alarm** («Беззвучная тревога экстренного вызова»): нажмите , чтобы включить беззвучную тревогу экстренного вызова для всех областей.

Управление зоной

1. Нажмите **Device** («Устройство»), чтобы просмотреть связанные зоны.



2. Нажмите +, чтобы добавить новую зону.
3. Выберите зоны, чтобы перейти на страницу управления.
   Здесь можно просматривать состояние устройства (например, температуру, состояние батареи и т. д.).
4. Нажмите в правом верхнем углу, чтобы перейти на страницу настроек зоны.
5. Выберите тип зоны.

   Instant Zone («Зона мгновенного срабатывания»)

   Данный тип зоны немедленно вызовет тревожное событие при постановке на охрану.

   Delayed Zone («Зона отсроченного срабатывания»)

   Задержка при выходе. Задержка при выходе дает время для выхода из защищенной зоны без срабатывания тревоги.

   Задержка входа. Задержка срабатывания на входе дает время для входа в защищенную зону для отключения системы без срабатывания тревоги.

   Если система включена или активирована повторно, система обеспечивает время задержки для входа / выхода. Обычно эта функция применяется на маршруте входа / выхода (например, входная дверь / главный вход), который является основным для постановки системы на охрану / снятия с охраны с помощью рабочей клавиатуры.

Примечание

- В соответствии со стандартом EN50131-1, таймер не должен превышать 45 секунд.
- Настройте **Stay Arm Delay Time** («Время задержки постановки на охрану») для зоны задержки.

Follow Zone («Зона слежения»)

При обнаружении тревожного события во время задержки входа в систему зона действует как зона отсроченного срабатывания. В других случаях — действует как зона мгновенного срабатывания.

Примечание

Для зоны можно выбрать два типа триггера (по времени срабатывания и по статусу зоны). Если выбран тип состояния зоны, настройте правило срабатывания триггера (постановка на охрану / снятие с охраны).

Disabled Zone («Зона отключенного предупреждения»)

Зона отключена, любое тревожное событие будет игнорировало. Обычно используется для отключения неисправных детекторов.

24 Hours Zone («Зона с круглосуточным оповещением»)

Зона активна все время со звуковым сигналом / сиреной при срабатывании тревоги. Обычно используется в пожароопасных зонах, оборудованных детекторами дыма и датчиками температуры.

Timeout Zone («Зона заданного периода времени»)

Зона активна все время. Данный тип зоны используется для мониторинга и сообщения активного статуса зоны. Уведомления о статусе зоны будут направлены по истечении заданного времени (от 1 до 599) секунд. Можно использовать в местах, оборудованных магнитоконтактными датчиками, которые требуют доступа только на короткий период (например, дверца шкафа пожарного гидранта или дверца другого внешнего защитного ящика).

6. Поставьте галочку **Cross zone («Пересечение зоны»)**, **Silent Alarm («Зона беззвучной сигнализации»)** и т. д.

Примечание

Некоторые модели не поддерживают эту функцию. Опирайтесь на характеристики конкретной зоны.

Режимы охраны

Если зона является общественной зоной (зона принадлежит более чем одной области), вы можете установить режим охраны.

И Зона будет поставлена на охрану, когда все выбранные зоны поставлены на охрану. Зона будет снята с охраны, когда любая из связанных областей снимается с охраны.

ИЛИ Зона будет поставлена на охрану, когда любая из связанных областей поставлена на охрану. Зона будет снята с охраны, когда все связанные области снимаются с охраны.

Когда зона находится в состоянии тревоги, снятые с охраны области, связанные с этой зоной, не могут быть поставлены на охрану.

Stay Arm Bypass («Частичная охрана»)

Зона будет автоматически исключена во время постановки на охрану.

Cross Zone («Пересечение зоны»)

PD6662 не включен: необходимо установить временной интервал.

При срабатывании тревоги первой зоны система начнет отсчет времени после восстановления зоны. Если тревога второй зоны сработает в течение установленного времени, обе зоны будут выдавать тревогу. В противном случае тревога не сработает. Если первая зона не будет восстановлена, обе зоны будут выдавать тревоги при срабатывании второй зоны даже по истечении установленного времени.

PD6662 включен: необходимо установить временной интервал.

Первая зона подаст сигнал при срабатывании тревоги. Если сработает тревога второй зоны до восстановления первой зоны, система сообщит о подтверждении тревоги. Если первая зона восстановлена, система начнет отсчет времени.

Если тревога второй зоны сработает в течение установленного времени, система сообщит о подтверждении тревоги.

Если первая зона восстановлена, система начнет отсчет времени. Если вторая зона не сработает в течение установленного времени, система не будет выводить какую-либо информацию.

Forbid Bypass on Arming («Запрет обхода при постановке на охрану»)

Если функция включена, при постановке на охрану обход зоны будет недоступен.

Chime («Сигнал»)

Включите дверной звонок. Обычно используется для магнитоконтактных датчиков.

Silent Panic Alarm («Беззвучная тревога экстренного вызова»)

Если функция включена, при срабатывании тревоги будет загружен только отчет, звук издаваться не будет.

Double Knock («Функция двойного срабатывания»)

Если функция включена, можно установить временной интервал. Устройство выдаст тревогу, если датчик срабатывает дважды или непрерывно в течение определенного периода времени.

Sounder Delay Time («Время задержки звукового оповещателя»)

Звуковой оповещатель сработает сразу или по истечении установленного времени.

Управление пользователями

Установщики (пользователи Hik-ProConnect) могут управлять пользователями. Администратор может добавлять, редактировать и удалять пользователей, а также назначать новые права новым пользователям.

Шаги

Примечание

Предусмотрено три типа пользователей для охранной панели: администратор (или владелец), оператор и установщик (или настройщик). Пользователи каждого типа имеют разные права на доступ к функциям охранной панели.

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек охранной панели.
2. Нажмите **Next** («Далее»), чтобы пригласить пользователя.

Примечание
Получатель должен принять приглашение.

3. Нажмите → **User Management** → **User** («Управления пользователями → Пользователи»).
4. Выберите пользователя, чтобы перейти на страницу управления пользователями.
5. Опционально. При необходимости выполните следующие действия.

User Permission («Разрешения пользователя»)	Выберите целевого пользователя из списка, затем нажмите **Edit** («Изменить»), чтобы настроить разрешения для целевого пользователя. **Примечание** Данная операция доступна только администраторам.
Set Linked Areas («Настройка привязанной области»)	Если целевой пользователь является оператором, выберите целевого пользователя из списка, затем нажмите **Linked Areas** («Связанные области»), чтобы настроить область, связанную с целевым пользователем. **Примечание** Данная операция доступна только администраторам.
Change Keypad Password («Изменение пароля клавиатуры»)	Если целевой пользователь является администратором, установщиком или оператором, выберите целевого пользователя из списка, затем нажмите **Change Keypad Password** («Изменить пароль клавиатуры»), чтобы установить пароль клавиатуры для целевого пользователя.
Change Duress Password («Изменение пароля принуждения»)	Если целевой пользователь является администратором или оператором, выберите целевого пользователя из списка, затем нажмите **Change Duress Password** («Изменить пароль принуждения»), чтобы настроить пароль принуждения для пользователя. **Примечание** Если установлен код принуждения, введите код принуждения на клавиатуре, чтобы поставить на охрану и снять с охраны зону (зоны) и загрузить сигнал тревоги принудительного действия.
Automation Control («Управление системой автоматического управления и контроля»)	Администратор, установщик или оператор могут управлять модулем реле, настенным выключателем и интеллектуальной розеткой.

Примечание

- Возможность изменения настроек и объем разрешений зависят от типа пользователя.
- Здесь можно просматривать привязанные карты/метки и брелоки пользователя без возможности изменения настроек.

Управление картами / метками

После добавления карт / меток в охранную панель можно провести карту / метку, чтобы поставить или снять с охраны все датчики, добавленные в определенные области охранной панели, или отключить тревожные уведомления.

Примечание

ID / PIN-код тега представляет собой 32-битное целое число, например, 42949672956.

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. **User Management** → **Card / Tag** («Управление пользователями → Карты / метки»), чтобы перейти на страницу управления картами / метками.
3. Нажмите **+**, чтобы добавить метку.
4. Услышав голосовую подсказку **Swipe Tag** («Считайте карту»), поднесите метку в область считывания карты на охранной панели.
   - Сигнал бипера означает, что метка успешно распознана.
   - Метка будет отображаться на странице управления картами / метками.
5. Опционально. Выберите метку, чтобы перейти на страницу настроек.
6. Нажмите **Edit** («Изменить») для изменения наименования метки.

Примечание

- Пропустите этот шаг, если выполнен вход в качестве установщика. Возможность редактирования наименования метки доступна только для администратора.
- Наименование должно содержать от 1 до 32 символов.

7. Включите функцию **Enable Tag** («Активировать метку»).
8. Выберите привязанного пользователя.
9. Выберите тип метки.

Примечание

Тип разрешения метки зависит от типа привязанного пользователя.

Работа с метками

Проведите метку, чтобы поставить область на охрану / снять область с охраны.

Патрульные метки

Проведите меткой для загрузки записи в систему.

10. Опционально. Нажмите **Delete** («Удалить»), чтобы удалить метку.

Информация об устройстве

При необходимости можно изменить язык и выбрать часовой пояс.

Шаги

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **System** → **Configuration** («Система → Настройки»), чтобы перейти на страницу настроек времени.
3. Выберите язык устройства и часовой пояс.
4. При необходимости включите функцию DST (переход на летнее время).

   DST

   Переход на летнее время (DST) — это практика перевода часов вперед при более продолжительном дневном свете, чтобы по вечерам было больше дневного света и по утрам меньше.

Управление системой

Шаги

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **System** → **System Options** → **System Management** («Система → Параметры системы → Управление системой»), чтобы открыть страницу.

Forced Auto Arm («Принудительная автоматическая постановка на охрану»)

Если опция включена и в зоне присутствуют активные неисправности, зона будет исключена автоматически при постановке на охрану.

Примечание

Необходимо отключить функцию постановки на охрану на странице дополнительных настроек. При наличии неисправности постановка панели на охрану не будет выполнена.

Forced Arming («Принудительная постановка на охрану»)

Если опция включена и в зоне присутствуют активные неисправности, зона будет исключена при постановке на охрану.

System Status Report («Отчет о состоянии системы»)

Если опция включена, устройство автоматически загрузит отчет при изменении статуса панели.

Voice Prompt («Голосовое предупреждение»)

Если опция включена, панель включит текстовое голосовое предупреждение. Здесь можно установить подробную подсказку: **подсказка об ошибке при постановке на охрану, подсказка об ошибке при снятии с охраны, подсказка об ошибке, когда охрана активирована, подсказка об ошибке, когда охрана отключена, голосовое предупреждение при тревоге.**

System Volume («Громкость системы»)

Доступный диапазон громкости системы: от 0 до 10.

Audible Tamper Alarm («Тревога тампера»)

Если опция включена, при тревоге саботажа будет срабатывать бипер.

Alarm Duration («Длительность тревоги»)

Длительность тревоги на охранной панели.

Wireless Supervision Loss («Ошибка беспроводного управления»)

Настройте максимальную продолжительность интервала опроса. Система сообщит о неисправности, если продолжительность превышает установленное значение.

Bypass on Re-Arm («Обход зоны при повторной постановке на охрану»)

Если функция включена, зона с неисправностью будет автоматически исключена при повторной постановке на охрану.

Jamming Sensitivity Settings («Настройки чувствительности к помехам»)

Устройство обнаружит радиочастотные помехи и отправит push-сообщения, когда создаются помехи для радиосигналов. Настройте чувствительность обнаружения.

Fault LED Stay On When Armed («LED-индикатор неисправности остается включенным при постановке на охрану»)

Когда система поставлена на охрану, индикатор неисправности горит непрерывно.

Arm LED Stay On («LED-индикатор постановки на охрану остается включенным»)

LED-индикатор постановки на охрану горит непрерывно.

Hik-Connect Indicator («Индикатор Hik-Connect»)

Включите индикатор Hik-Connect.

Motion Detector Restore («Восстановление датчиков движения»)

К датчикам движения относятся все ИК-датчики.

Power Save Mode («Режим энергосбережения»)

Если режим энергосбережения включен и отключен основной источник питания, Wi-Fi переходит на низкое энергопотребление, отключается 4G, не выполняется считывание метки, не горит LED-индикатор, отключены голосовые подсказки.

PD6662

Включите стандарт PD6662. Несоответствующие стандарту функции не будут работать.

Проверка неисправности

Система определяет, следует или не следует производить диагностику неисправностей, перечисленных на странице. Система будет диагностировать только выбранную неисправность.

Шаги

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Перейдите на вкладку → **System** → **System Options** → **System Fault Check** («Система → Параметры системы → Проверка неисправности»).

Detect Network Camera Disconnection («Обнаружение отключения IP-камеры»)

Если опция включена, сработает тревожный сигнал при отключении IP-камеры.

Panel Battery Fault Check («Проверка неисправности батареи»)

Если опция включена, устройство будет загружать события, когда батарея отключена или разряжена.

LAN Fault Check («Проверка неисправности LAN»)

Если опция включена, сработает тревожный сигнал при разрыве или сбоях проводной сети.

Wi-Fi Fault Check («Проверка неисправности Wi-Fi»)

Если опция включена, сработает тревожный сигнал при разрыве или сбоях подключения Wi-Fi.

Cellular Network Fault Check («Проверка неисправности сотовой сети»)

Если опция включена, сработает тревожный сигнал при разрыве или сбоях сотовой сети.

Main Power Lost («Тревога потери питания»)

Если опция включена, тревога сработает при отключении IP-камеры.

AC Power Loss Delay («Потеря питания переменного тока»)

Система проводит проверку неисправности по истечении заданного времени после отключения питания переменного тока. В соответствии со стандартом EN 50131-3 продолжительность проверки должна составлять 10 с.

Параметры постановки на охрану

Настройте расширенные параметры доступа.

Шаги

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **System** → **System Options** → **Arm Options** («Система → Параметры системы
2. Параметры постановки на охрану»), чтобы открыть страницу.

Также можно настроить следующие параметры:

Arm with Faults («Постановка на охрану с условием подтверждения неисправностей»)

Отметьте неисправности в списке **Enable Arming with Fault list** («»Включить постановку на охрану при обнаружении неисправности»), и устройство не остановит процедуру постановки на охрану при обнаружении неисправности.

Early Alarm («Тревога по истечении времени задержки»)

Если функция включена и зона поставлена на охрану, при возникновении тревожного события, тревога сработает по истечении времени задержки.

Примечание

Данная тревога сработает только после срабатывания зоны с задержкой.

3. Нажмите **Save** («Сохранить»).

Режим регистрации

Шаги

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **System** → **System Options** → **Enrollment Mode** («Система → Параметры системы → Режим регистрации»), чтобы открыть страницу.
3. Нажмите на иконку **Enter the Enrollment Mode** («Перейти в режим регистрации»). Зарегистрировать периферийное устройство можно посредством активации.

IP-камера

Добавление камер на охранную панель

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Network Camera** → **Network Camera Channel** («IP-камера → Канал IP-камеры»), чтобы перейти на страницу.
3. Нажмите **Add Channel** («Добавить канал»).
4. Введите IP-адрес, номер порта, имя пользователя и пароль камеры.
5. Нажмите **Save** («Сохранить»).
6. Опционально: нажмите **Edit** («Изменить») или **Delete** («Удалить»), чтобы изменить параметры или удалить выбранную камеру.

Настройка параметров видео

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Network Camera** → **Event Video Settings** («IP-камера → Параметры видео по событию»), чтобы перейти на соответствующую страницу.
3. Выберите камеру и настройте параметры видео.

   Stream Type («Тип потока»)

   Main Stream («Основной поток»): используется при записи и предварительном просмотре в формате HD, имеет высокое разрешение, скорость кодового потока и качество изображения.

   Sub-Stream («Дополнительный поток»): используется для передачи по сети и предварительного просмотра изображений в виде потокового видео с возможностью более низкого разрешения, скорости передачи данных и качества изображения.

   Bitrate Type («Тип битрейта»)

   Выберите тип битрейта: **Constant** («Постоянный») или **Variable** («Переменный»).

   Resolution («Разрешение»)

   Выберите разрешение видеовыхода.

   Bitrate («Битрейт»)

   Чем выше значение, тем лучше качество видео, но требуется большая пропускная способность.

Настройка расписания снятия / постановки на охрану

Шаги

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Area** («Область»), чтобы перейти на страницу.
2. Выберите область из списка, включите ее и выберите связанные области.
3. Включите функцию автоматической постановки на охрану/ снятия с охраны и задайте время автоматической постановки на охрану / снятия с охраны. Также можно настроить время задержки снятия с охраны, время задержки входа, время задержки выхода, время задержки звукового оповещателя, исключение выходных и праздничных дней.

Auto Arm («Автоматическая постановка на охрану»)

Включите автоматическую постановку под охрану в заданное время.

Auto Arm Time («Длительность автоматической постановки под охрану»)

Установите расписание для автоматической постановки на охрану.

Auto Disarm («Автоматическое снятие с охраны»)

Включите автоматическое снятие с охраны в заданное время.

Auto Disarm Time («Время автоматического снятия с охраны»)

Настройте расписание для автоматического снятия с охраны.

Late to Disarm («Задержка снятия с охраны»)

Разрешите устройству отправлять уведомления на смартфон или планшет, чтобы напоминать пользователю о снятии области с охраны, если область находится под охраной после заданного времени.

Примечание

Активируйте функцию уведомления с помощью панели на веб-клиенте меню **Communication Parameters** → **Event Communication** («Параметры связи → Связь по событию») перед активацией функции **Late to Disarm** («Задержка снятия с охраны»).

Late to Disarm Time («Время задержки снятия с охраны»)

Задайте время, указанное в пункте **Late to Disarm** («Задержка снятия с охраны»)

Auto Arm Sound Prompt («Звуковое предупреждение автоматической постановки на охрану»)

После отключения бипер не будет подавать звуковой сигнал перед автоматической постановкой на охрану.

Weekend Exception («Исключение выходных дней»)

Если функция включена, указанные выше режимы не будут активны в выходные дни.

Holiday Exception («Исключения в праздничные дни»)

Если функция включена, режимы постановки и снятия с охраны не будут активны в праздничные дни. После включения необходимо настроить расписание выходных дней.

Примечание

Можно настроить до 6 групп праздничных дней.

Связь

Проводная сеть

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Перейдите на вкладку **Communication → Wired Network** («Связь → Параметры проводной сети»).
3. Настройте параметры.
   – Автоматические настройки: включите **DHCP** и настройте HTTP-порт.
   – Настройки вручную: отключите **DHCP** и настройте IP-адрес, маску подсети, адрес шлюза, адрес DNS-сервера.
4. Опционально. Установите корректный адрес DNS-сервера, если устройству необходимо подключиться к серверу Hik-Connect через доменное имя.
5. Нажмите **Save** («Сохранить»).

Сотовая сеть передачи данных

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Перейдите на вкладку → **Communication Parameters** → **Cellular Data Network Settings** («Параметры связи → Параметры сотовой сети передачи данных»).
3. Включите **Cellular Data Network** («Сотовая сеть передачи данных»).
4. Нажмите, чтобы выбрать SIM-карту. Нажмите **Parameter Configuration → Edit Icon** («Настройка параметров → Изменить значок») и настройте параметры, в том числе, имя пользователя, пароль доступа, APN, MTU и PIN-код.
5. Нажмите **Save** («Сохранить»).
6. Включите **Data Usage Limit** («Ограничение использования данных»).
7. Измените **Data Used This Month** («Данные, используемые в этом месяце») и **Data Limited per Month** («Данные, ограниченные в месяц»).

Access Number («Номер доступа»). Введите номер для связи с оператором.

Примечание

Номер доступа требуется ввести только пользователю SIM-карты частной сети.

User Name («Имя пользователя»)

Введите имя пользователя в соответствующее поле.

Access Password («Пароль доступа»)

Введите пароль пользователя в соответствующее поле.

APN

Запросите информацию APN у оператора сети и введите информацию в соответствующее поле.

Data Usage Limit («Ограничение использования данных»)

Включите функцию и настройте порог данных в месяц. При превышении порогового значения сработает тревога, которая будет загружена в центр тревог и мобильный клиент.

Data Used This Month («Данные, использованные в месяц»)

Используемые данные будут накапливаться и отображаться в данном текстовом поле.

Push-уведомления

Настройте параметры push-уведомлений, чтобы уведомления о тревоге были направлены на мобильный телефон.

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости),чтобы перейти на страницу настроек .
2. Перейдите на вкладку → **Communication Parameters → Push Notification(s)** («Параметры связи → Параметры Push-уведомлений»).
3. Включите уведомления о целях.

Zone Alarm / Lid Opened («Тревога зоны / открытия крышки»)

Устройство будет отправлять push-уведомления, когда срабатывает тревога в зоне или при открытии крышки.

Примечание

Необходимо настроить время интервала фильтрации событий для телефонных вызовов.

Peripherals Lid Opened («Открытие крышки периферийного устройства»)

Устройство будет отправлять push-уведомления, при открытии крышки любого периферийного устройства.

Panel Lid Opened («Открытие крышки панели»)

Устройство будет отправлять push-уведомления при открытии крышки панели управления.

Panic Alarm («Тревога экстренного вызова»)

Устройство будет отправлять push-уведомления, при срабатывании тревоги экстренного вызова в зоне, на клавиатуре или на брелоке.

Medical Alarm («Тревога экстренной медицинской помощи»)

Устройство будет отправлять push-уведомления при срабатывании тревоги экстренной медицинской помощи.

Fire Alarm («Пожарная тревога»)

Устройство будет отправлять push-уведомления при срабатывании тревоги утечки газа.

Panel Status («Состояние панели»)

Устройство будет отправлять push-уведомления при изменении состояния панели.

Zone Status («Статус зоны»)

Устройство будет отправлять уведомления при изменении статуса зоны.

Peripherals Status («Состояния периферийных устройств»)

Устройство будет отправлять push-уведомления при изменении статуса любого периферийного устройства.

Panel Operation («Операции панели»)

Устройство будет отправлять push-уведомления, когда пользователь работает с охранной панелью.

Smart Alarm Event («События интеллектуальной тревоги»)

Устройство будет отправлять push-уведомления при срабатывании тревоги на тепловизионных камерах.

5. Нажмите **Phone Call and SMS** («Телефонный вызов и SMS-сообщения»).
6. Нажмите **+ Add Phone Number** («Добавить номер телефона»), чтобы ввести номер телефона.
7. Выберите добавленный номер телефона, чтобы включить телефонный вызов и SMS-сообщения в соответствии с вашими потребностями.
8. (для телефонного вызова) Настройте **Numbers of Calling** («Номера вызова»).
9. (для SMS-сообщений) Настройте **Arming Permission («Разрешение на постановку на охрану**»), **Disarming Permission («Разрешение на снятие с охраны»)** и **Alarm Clearing Permission («Разрешение на сброс тревоги для областей»).**

General Hint («Общая подсказка»)

Введите **Common Voice** («Голосовое сообщение»). При срабатывании тревоги настроенный контент будет добавлен в начало сообщения, отправляемого системой. Можно импортировать **Common Voice** («Голосовое предупреждение»). При срабатывании тревоги настроенное голосовое предупреждение будет добавлено в начало содержимого телефона, набранного системой.

Примечание

Поддерживается только формат WAV до 512 КБ и 15 с.

10. Проверьте уведомления.

Пункт централизованного наблюдения (ЧОП / ПЦН)

Настройте параметры центра тревог: тревоги будут отправляться в настроенный центр тревог.

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости), на страницу настроек.
2. Перейдите на вкладку → **Communication Parameters → Alarm Receiving Center (ARC)** («Настройка параметров → ЧОП / ПЦН») для перехода на соответствующую страницу.
3. Выберите ЧОП / ПЦН и включите его.

Protocol Type («Тип протокола»)

Выберите **Protocol Type** («Тип протокола»): ADM-CID, ISUP, SIA-DCS, *SIA-DCS, *ADM-CID или CSV-IP, чтобы настроить режим загрузки.

Companies («Компания»)

Выберите компанию поддержки: **None** («Отсутствует»), **Hungary-Multi Alarm Receiving Company** («ЧОП / ПЦН в Венгрии») или **French Alarm Receiving Company** («ЧОП / ПЦН во Франции»).

Address Type («Тип адреса»)

Укажите тип адреса: **IP Address** («IP-адрес») или **Domain Name** («Доменное имя»). Введите адрес сервера / доменное имя, номер порта и код учетной записи.

Transmission Mode («Режимы передачи»)

Выберите режим передачи TCP или UDP. Протокол UDP рекомендуется стандартом SIA DC-09.

Retry Timeout Period («Период ожидания повторной попытки»)
По истечении выбранного времени система повторит попытку передачи.
Attempts («Попытки»)
Задайте количество повторных попыток.
Polling Option («Вариант опроса»)
Настройте частоту опроса в диапазоне от 10 до 3888000 секунд.
Periodic Test («Периодическая диагностика»)
Введите интервал периодической проверки.
GMT («Среднее время по Гринвичу»)
Включите среднее время по Гринвичу.

Настройки облачного сервиса

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Communication Parameters** → **Cloud Service Settings** («Параметры связи→ Настройки облачного сервиса»), чтобы открыть страницу.
3. Выберите **Communication Mode** («Режим связи»).
   Auto («Автоматич.»)
   Система автоматически выберет режим связи в соответствии с последовательностью проводной сети, сети Wi-Fi и сотовой сети передачи данных. Только когда текущая сеть отключена, устройство подключится к другой сети.
   Wired Network & Wi-Fi Priority («Приоритет проводной сети и сети Wi-Fi»)
   Порядок приоритета подключения: проводная сеть, Wi-Fi, сотовая сеть передачи данных.
   Wired &Wi-Fi («Проводная сеть и сеть Wi-Fi»)
   В первую очередь система выберет проводную сеть. Если проводная сеть не обнаружена, будет выбрана сеть Wi-Fi.
   Cellular Data Network («Сотовая сеть передачи данных»)
   Система выберет только сотовую сеть передачи данных.
4. Включите **Periodic Test** («Периодическая проверка»). Введите интервал периодической проверки.
5. Нажмите **Save** («Сохранить»).

Уведомление по Email

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Communication Parameters** → **Notification by Emails** («Параметры связи→ Уведомление по электронной почте»), чтобы войти на страницу.
3. Включите **Email**.
4. Введите имя отправителя, адрес электронной почты отправителя, адрес SMTP-сервера, порт SMTP, имя пользователя и пароль.
5. Выберите тип шифрования: **None** («Отсутствует»), SSL или TLS.

6. Активация **Server Authentication («Аутентификация сервера»)**.
7. Введите имя получателя и адрес электронной почты получателя. Нажмите **Test Receiver Email Address** («Проверить адрес электронной почты получателя»), чтобы проверить правильность адреса электронной почты.
8. Нажмите **Save** («Сохранить»).

Настройка параметров FTP

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Communication Parameters** → **FTP Settings** («Параметры связи → Настройки FTP»), чтобы открыть страницу.
3. Выберите **Preferred FTP** («Предпочитаемый FTP») или **Alternated FTP** («Альтернативный FTP») и включите FTP.
4. Настройте параметры FTP.

FTP Type («Тип FTP»)

Настройте тип FTP: предпочтительный или альтернативный.

Protocol Type («Тип протокола»)

Можно выбрать FTP и SFTP. Загрузка файлов зашифрована с помощью протокола SFTP.

Server Address and Port («Адрес сервера и номер порта»)

Адрес FTP сервера и соответствующий номер порта.

User Name and Password («Имя пользователя и пароль»)

Пользователю FTP необходимо иметь разрешение для загрузки изображений. Если FTP сервер разрешает анонимным пользователям загружать изображения, можно выбрать режим **Anonymous** («Анонимный»), чтобы скрыть информацию об устройстве во время загрузки.

Directory Structure («Структура директорий»)

Путь сохранения захваченных изображений в FTP сервере.

4. Нажмите **Save** («Сохранить»).

NAT

Universal Plug и Play (UPnP ™) – это сетевая архитектура, обеспечивающая совместимость сетевого оборудования, программного обеспечения и других устройств. Протокол UPnP позволяет легко подключать устройства и упрощает реализацию сетей в домашних и корпоративных средах.

Если функция включена, не требуется настраивать проброс портов для каждого порта, камера подключается к WAN через роутер.

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости),чтобы перейти на страницу настроек.
2. Нажмите → **Communication Parameters** → **NAT** («Параметры связи→ NAT»), чтобы открыть страницу.

3. Передвиньте ползунок, чтобы включить функцию UPnP.
4. Опционально. Выберите тип сопоставления **Manual** («Вручную») и задайте порт HTTP и порт службы.
5. Нажмите **Save** («Сохранить»), чтобы завершить настройку.

Служба внутренней связи

Настройте службу внутренней связи для оповещателя.

Перед началом

В первую очередь необходимо зарегистрировать оповещатель внутренней связи.

Только один оповещатель может быть установлен в качестве оповещателя внутренней связи.

Шаги

1. Нажмите **Communication** → **Intercom Service** («Связь → Служба внутренней связи»), чтобы войти на страницу.
2. Сдвиньте ползунок для включения функции.
3. Задайте тип внутренней связи.

   SIP-сервер

   Панель управления будет использовать сервер ПОП / ПЦН и SIP.

   IP Receiver Pro

   В панели управления будет отображаться облачный сервис.
4. Выберите оповещатель и нажмите **Save** («Сохранить»).

Техническое обслуживание устройств

Перезагрузите устройство.

Шаги

1. На странице объекта, выберите охранную панель и выполните вход в систему (при необходимости),чтобы перейти на страницу настроек.
2. Нажмите → **Maintenance** → **Device Maintenance** («Обслуживание → Обслуживание устройства»), чтобы перейти на соответствующую страницу.
3. Нажмите кнопку **Test** («Диагностика»), затем нажмите **Start Walk Test** («Запустить диагностику»), чтобы проверить корректность работы устройства.
4. Нажмите **Maintenance** → **Reboot Device** («Обслуживание → Перезагрузка устройства»). Панель будет перезагружена.
5. Нажмите → **Maintenance** → **Device Maintenance** («Обслуживание → Обслуживание устройства»), чтобы перейти на соответствующую страницу.

Охранная панель обновится до последней версии.

5.1.2 Использование портала Hik-ProConnect

Для охранной панели можно выполнять различные операции, включая постановку / снятие с охраны, отключение тревожных уведомлений, обход зоны и т.д., а также удаленно настраивать панель управления на портале. Также можно подать заявку на получение PIN-кода (необходим для обновления прошивки) и переключить язык охранной панели.

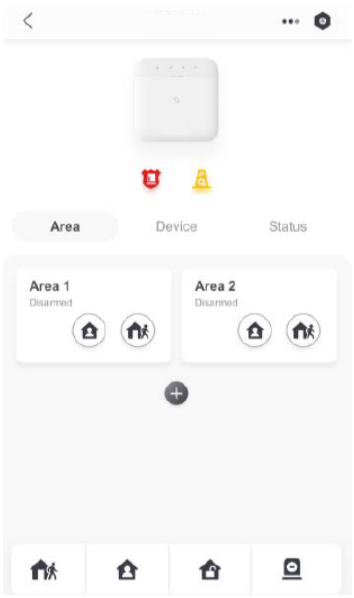
Нажмите вкладку **Site** («Объекты») для перехода на страницу списка объектов, затем выберите наименование объекта, чтобы перейти на страницу сведений об объекте.

Удаленное управление охранной панелью

Выберите охранную панель, чтобы открыть панель управления. После этого доступны следующие операции.

Таблица 4-3 Описание операции

Операции	Описание операции
Частичная охрана определенной зоны	Выберите вкладку **Area** («Область»), затем нажмите **Stay Arming** («Частичная охрана»), чтобы поставить область под частичную охрану.
Полная охрана определенной области	Выберите вкладку **Area** («Область»), затем нажмите **Away Arming** («Полная охрана»).
Снятие охраны с определенной области	Выберите вкладку **Area** («Область»), затем нажмите **Disarm** («Снятие с охраны»).
Частичная охрана нескольких областей	Выберите вкладку **Area** («Область»), затем выберите области и нажмите .
Полная охрана нескольких областей	Выберите вкладку **Area** («Область»), затем выберите области и нажмите .
Снятие нескольких областей с охраны	Выберите вкладку **Area** («Область»), затем выберите области и нажмите .
Отключение тревожных уведомлений нескольких областей	Выберите вкладку **Area** («Область»), затем выберите области и нажмите .
Фильтр периферийного устройства по области	Выберите вкладку **Device** («Устройство»), затем нажмите и выберите область, чтобы отображались только периферийные устройства, связанные с выбранной областью, или выберите **All** («Все»), чтобы отобразить все периферийные устройства, связанные со всеми областями.
Управляющее реле	Перейдите на вкладку **Device** («Устройство»), затем выберите беспроводной выходной расширитель для отображения связанных с ним сирен, а затем выберите сирену (-ы), чтобы включить / выключить их.
Обход зоны	Нажмите на вкладку **Device** «Устройство», затем выберите зону (например, датчик) и **Bypass** «Обход», чтобы обойти зону.



Удаленная настройка охранной панели

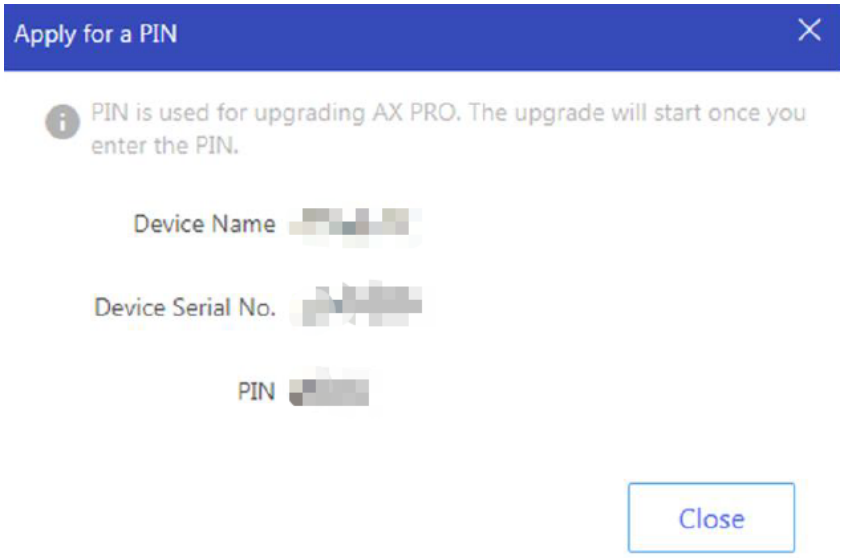
Можно нажать для перехода в веб-интерфейс охранной панели для конфигурации устройства.

Примечание

Подробная информация о конфигурации охранной панели представлена в руководстве пользователя устройства.

Подача заявки на получение PIN-кода

Можно нажать • • • → для открытия окна Apply for a PIN («Подача заявки на получение PIN-кода»), тогда отобразится PIN-код.

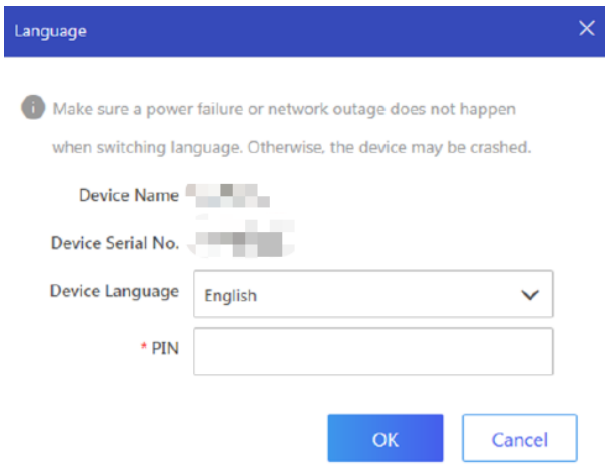


Переключение языка

Примечание

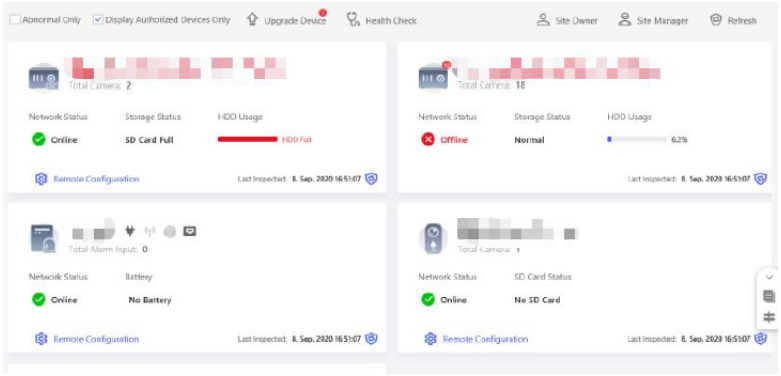
В первую очередь необходимо подать заявку на получение PIN-кода.

Можно нажать ••• → ⇆ для открытия окна **Language** («Язык»), затем настройте язык на устройстве и введите PIN-код.

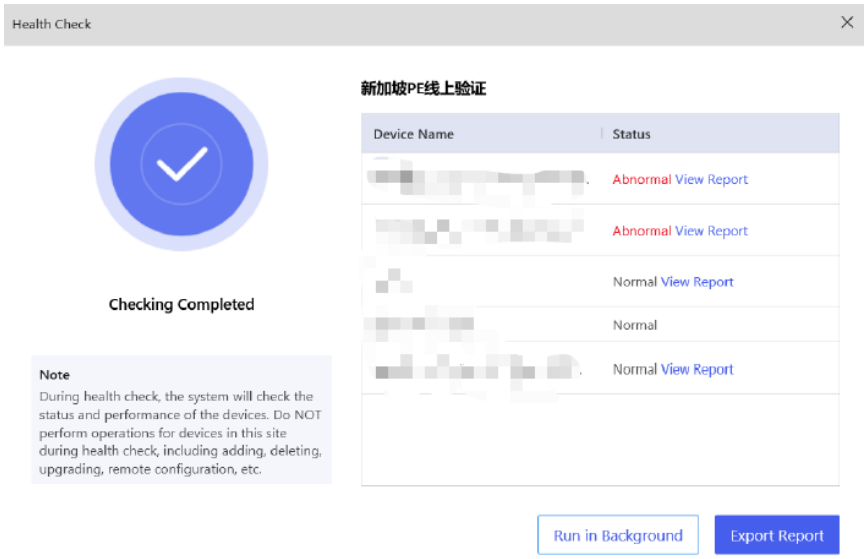


Мониторинг состояния

1. Войдите на веб-сайт портала Hik-ProConnect и нажмите **Health Monitoring** → **Health Status** («Мониторинг состояния → Состояние»), чтобы перейти на соответствующую страницу.
2. Выберите объект.



3. Нажмите **Health Check** («Проверка состояния устройства»), затем нажмите **Check Now** («Запустить проверку»). По завершении проверки можно просматривать состояние устройств и отчеты. При необходимости можно экспортировать отчет.



4. Нажмите , чтобы просмотреть актуальное состояние устройства.

5.2 Настройка параметров с помощью Hik-Connect

Оператор может использовать Hik-Connect для управления устройством, например, для постановки на охрану / снятия с охраны, управления пользователями и т. д.

Загрузка и вход в мобильный клиент

Загрузите мобильный клиент Hik-Connect и войдите в систему перед началом работы с охранной панелью.

Шаги

1. Загрузите мобильный клиент Hik-Connect.
2. Опционально. Зарегистрируйте новую учетную запись, если мобильный клиент Hik-Connect используется впервые.

Примечание

Подробная информация представлена в *Руководстве пользователя мобильного клиента Hik-Connect.*

3. Запустите и войдите в клиент.

Добавление охранной панели в мобильный клиент

Добавьте охранную панель в мобильный клиент перед другими операциями.

Шаги

1. Включите охранную панель.
2. Выберите способ добавления.

Нажмите **+** → **Scan QR Code** («Сканировать QR-код»), чтобы перейти на соответствующую страницу. Сканируйте QR-код на панели.

Примечание

Обычно QR-код находится на этикетке на задней крышке панели.

Нажмите **+** → **Manual Adding** («Добавление вручную»), чтобы перейти на страницу добавления устройства. Введите серийный номер устройства при добавлении домена Hik-Connect.

3. Для поиска устройства нажмите .
4. Нажмите **Add** («Добавить»).
5. Введите проверочный код и нажмите **OK**.
6. После завершения добавления введите псевдоним устройства и нажмите **Save** («Сохранить»).
7. Опционально. Нажмите → **Delete Device** («Удалить устройство»), чтобы удалить устройство.
8. Опционально. Нажмите → , чтобы изменить имя устройства.

Добавление периферийных устройств на охранную панель

Добавьте периферийные устройства на охранную панель.

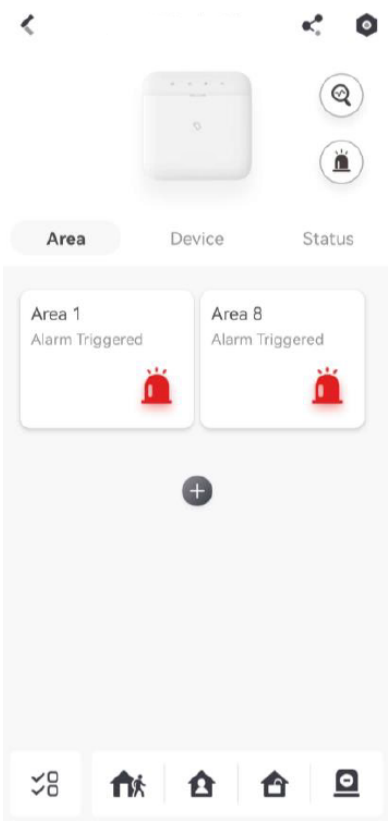
Шаги

1. Выберите устройство управления (охранную панель).
2. Нажмите +.
   - Нажмите **Scan QR Code** («Сканировать QR-код»), чтобы перейти на соответствующую страницу. Сканируйте QR-код на панели периферийного устройства.
   - Нажмите для перехода на страницу ввода вручную. Введите серийный номер устройства и выберите тип устройства для добавления устройства.

Основная страница

Здесь можно просматривать неисправности, ставить и снимать области с охраны, просматривать состояние устройства и т. д.

На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек .



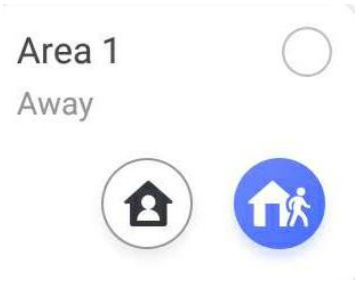
Активация тревоги
Нажмите для выбора **Audible Panic Alarm** («Тревога экстренного вызова») или **Silent Panic Alarm** («Беззвучная сигнализации экстренного вызова»).

Просмотр неисправностей
Нажмите для просмотра неисправностей.

Управление параметрами области
Нажмите **+**, чтобы добавить область.
Выберите область, чтобы вернуться на страницу управления устройством. Подробная информация представлена в разделе ***Настройка расписания снятия / постановки на охрану***.

Постановка на охрану / снятие с охраны
При необходимости можно поставить область на охрану или снять область с охраны.
На странице списка устройств, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу области.

Операции в одной зоне



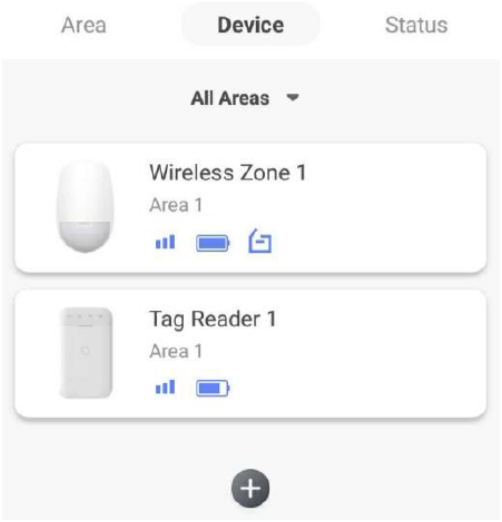
- **Away Arming** («Полная постановка на охрану»): нажмите , чтобы активировать режим охраны одной области при выходе из области. После выхода людей из области, включите режим постановки на охрану при выходе из области, чтобы поставить все зоны на охрану после установленного времени.
- **Stay Arming («Частичная охрана»):** нажмите , чтобы активировать частичный режим охраны. Во время нахождения посетителей в зоне обнаружения, включите режим постановки на охрану, чтобы включить обнаружение несанкционированных вторжений по всему периметру.

Операции в нескольких зонах

- Выбор областей. Нажмите , чтобы выбрать области, которыми вы хотите управлять. Если не выбрать области, следующие операции будут применены ко всем областям.
- **Away Arming** («Полная постановка на охрану»): нажмите , чтобы активировать режим полной постановки на охрану выбранных областей. После выхода людей из области, включите режим постановки на охрану при выходе из области, чтобы поставить все зоны на охрану после установленного времени.
- **Stay Arming** («Частичная охрана»): нажмите , чтобы активировать режим охраны всех областей. Во время нахождения посетителей в зоне обнаружения, включите режим постановки на охрану, чтобы включить обнаружение несанкционированных вторжений по всему периметру (например, датчик обнаружения по периметру, магнитоконтактный датчик и датчик, срабатывающий на движение штор на балконе) во всех зонах всех областей. В это время датчики внутри зоны обнаружения блокируются (например, ИК-датчики). Тревога не сработает при перемещении посетителей внутри зоны.
- **Disarming («Снятие с охраны»):** нажмите для снятия с охраны всех областей. В режиме снятия с охраны тревога в зонах всех областей не будет срабатывать, в том числе при обнаружении тревожных событий.
- **Silent Panic Alarm** («Беззвучная тревога экстренного вызова»): нажмите , чтобы включить беззвучную тревогу экстренного вызова для всех областей.

Управление зоной

1. Нажмите **Device** («Устройство»), чтобы просмотреть связанные зоны.



2. Нажмите +, чтобы добавить новую зону.
3. Выберите зоны, чтобы перейти на страницу управления. Здесь можно просматривать состояние устройства (например, температуру, состояние батареи и т. д.).
4. Нажмите в правом верхнем углу, чтобы перейти на страницу настроек зоны.
5. Выберите тип зоны.

Instant Zone («Зона мгновенного срабатывания»)

Данный тип зоны немедленно вызовет тревожное событие при постановке на охрану.

Delayed Zone («Зона отсроченного срабатывания»)

Задержка при выходе. Задержка при выходе дает время для выхода из защищенной зоны без срабатывания тревоги.

Задержка входа. Задержка срабатывания на входе дает время для входа в защищенную зону для отключения системы без срабатывания тревоги.

Если система включена или активирована повторно, система обеспечивает время задержки для входа / выхода. Обычно эта функция применяется на маршруте входа / выхода (например, входная дверь / главный вход), который является основным для постановки системы на охрану / снятия с охраны с помощью рабочей клавиатуры.

Примечание

- В соответствии со стандартом EN50131-1, таймер не должен превышать 45 секунд.
- Настройте **Stay Arm Delay Time** («Время задержки постановки на охрану») для зоны задержки.

Follow Zone («Зона слежения»)

При обнаружении тревожного события во время задержки входа в систему зона действует как зона отсроченного срабатывания. В других случаях — действует как зона мгновенного срабатывания.

Примечание

Для зоны можно выбрать два типа триггера (по времени срабатывания и по статусу зоны). Если выбран тип состояния зоны, настройте правило срабатывания триггера (постановка на охрану / снятие с охраны).

Disabled Zone («Зона отключенного предупреждения»)

Зона отключена, любое тревожное событие будет игнорировало. Обычно используется для отключения неисправных детекторов.

24 Hours Zone («Зона с круглосуточным оповещением»)

Зона активна все время со звуковым сигналом / сиреной при срабатывании тревоги. Обычно используется в пожароопасных зонах, оборудованных детекторами дыма и датчиками температуры.

Timeout Zone («Зона заданного периода времени»)

Зона активна все время. Данный тип зоны используется для мониторинга и сообщения активного статуса зоны. Уведомления о статусе зоны будут направлены по истечении заданного времени (от 1 до 599) секунд. Можно использовать в местах, оборудованных магнитоконтактными датчиками, которые требуют доступа только на короткий период (например, дверца шкафа пожарного гидранта или дверца другого внешнего защитного ящика).

6. Поставьте галочку **Cross zone («Пересечение зоны»)**, **Silent Alarm («Зона беззвучной сигнализации»)** и т. д.

Примечание

Некоторые модели не поддерживают эту функцию. Опирайтесь на характеристики конкретной зоны.

Режимы охраны

Если зона является общественной зоной (зона принадлежит более чем одной области), вы можете установить режим охраны.

И Зона будет поставлена на охрану, когда все выбранные зоны поставлены на охрану. Зона будет снята с охраны, когда любая из связанных областей снимается с охраны.

ИЛИ Зона будет поставлена на охрану, когда любая из связанных областей поставлена на охрану. Зона будет снята с охраны, когда все связанные области снимаются с охраны.

Когда зона находится в состоянии тревоги, снятые с охраны области, связанные с этой зоной, не могут быть поставлены на охрану.

Stay Arm Bypass («Частичная охрана»)

Зона будет автоматически исключена во время постановки на охрану.

Cross Zone («Пересечение зоны»)

PD6662 не включен: необходимо установить временной интервал.

При срабатывании тревоги первой зоны система начнет отсчет времени после восстановления зоны. Если тревога второй зоны сработает в течение установленного времени, обе зоны будут выдавать тревогу. В противном случае тревога не сработает. Если первая зона не будет восстановлена, обе зоны будут выдавать тревоги при срабатывании второй зоны даже по истечении установленного времени.

PD6662 включен: необходимо установить временной интервал.
Первая зона подаст сигнал при срабатывании тревоги. Если сработает тревога второй зоны до восстановления первой зоны, система сообщит о подтверждении тревоги.
Если первая зона восстановлена, система начнет отсчет времени. Если тревога второй зоны сработает в течение установленного времени, система сообщит о подтверждении тревоги.
Если первая зона восстановлена, система начнет отсчет времени. Если вторая зона не сработает в течение установленного времени, система не будет выводить какую-либо информацию.

Forbid Bypass on Arming («Запрет обхода при постановке на охрану»)
Если функция включена, при постановке на охрану обход зоны будет недоступен.

Chime («Сигнал»)
Включите дверной звонок. Обычно используется для магнитоконтактных датчиков.

Silent Panic Alarm («Беззвучная тревога экстренного вызова»)
Если функция включена, при срабатывании тревоги будет загружен только отчет, звук издаваться не будет.

Double Knock («Функция двойного срабатывания»)
Если функция включена, можно установить временной интервал. Устройство выдаст тревогу, если датчик срабатывает дважды или непрерывно в течение определенного периода времени.

Sounder Delay Time («Время задержки звукового оповещателя»)
Звуковой оповещатель сработает сразу или по истечении установленного времени.

7. При необходимости привяжите PIRCAM или камеру к зоне.
8. Нажмите **OK**.

Просмотр статуса

Нажмите **Status** («Статус»), чтобы просмотреть статус периферийных устройств.

Обход зоны

Когда зона поставлена на охрану, можно исключить определенную зону по своему желанию.

Перед началом

Привяжите датчик к определенной зоне.

Шаги

1. На странице списка устройств, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу области.
2. Перейдите в меню **Devices** (Устройства»).
3. Выберите зону на вкладке **Device** («Устройства»).
4. Нажмите для перехода на страницу настроек.
5. Включите **Bypass** («Обход»). Зона перейдет в режим обхода.
   Bypass Status («Состояние обхода»)
   Датчик не будет обнаруживать тревоги и отправлять уведомления о тревогах пользователю.

Управление пользователями

Администратор и установщики могут настраивать параметры пользователей. Администратор может добавлять, редактировать и удалять пользователей, а также назначать новые права новым пользователям.

Шаги

Примечание

Предусмотрено три типа пользователей для охранной панели: администратор (или владелец), оператор и установщик (или настройщик). Пользователи каждого типа имеют разные права на доступ к функциям охранной панели.

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите для перехода на страницу настроек.
3. Выберите пользователя, которого хотите пригласить.
   - Сканируйте QR-код, чтобы пригласить пользователя.
   - Введите адрес электронной почты / номер мобильного телефона получателя.
   - Выберите пользователя из списка.
4. Нажмите **Next** («Далее»), чтобы пригласить пользователя.

Примечание

Получатель должен принять приглашение.

5. Нажмите → **User Management** → **User** («Управления пользователями → Пользователи»).
6. Выберите пользователя, чтобы перейти на страницу информации о пользователях.
7. Опционально. При необходимости выполните следующие действия.

Разрешения пользователя	Выберите целевого пользователя из списка, затем нажмите , чтобы настроить разрешения для целевого пользователя. **Примечание** Данная операция доступна только администраторам.
Настройка привязанной области	Если целевой пользователь является оператором, выберите целевого пользователя из списка, затем нажмите **Linked Areas** («Связанные области»), чтобы настроить область, связанную с целевым пользователем. **Примечание** Данная операция доступна только администраторам.
Изменение пароля клавиатуры	Если целевой пользователь является администратором, установщиком или оператором, выберите целевого пользователя из списка, затем нажмите **Change Keypad Password** («Изменить пароль клавиатуры»), чтобы настроить пароль клавиатуры для пользователя.

Примечание

Пароль (PIN-код) должен содержать от 4 до 6 цифр. Можно использовать любые цифры в диапазоне от 10 000 до 100 000 без ограничений на комбинацию цифр.
После добавления клавиатуры можно добавить ПИН-код (пароль клавиатуры) в меню пользователя. Нажмите на поле ввода: можно ввести от 4 до 6 цифр. Это правило одинаково для каждого пользователя.

Изменение пароля принуждения

Если целевой пользователь является администратором или оператором, выберите целевого пользователя из списка, затем нажмите **Change Duress Password** («Изменить пароль принуждения»), чтобы настроить пароль принуждения для пользователя.

Примечание

Если установлен код принуждения, введите код принуждения на клавиатуре, чтобы поставить на охрану и снять с охраны зону (зоны) и загрузить сигнал тревоги принудительного действия.

Управление системой автоматического управления и контроля

Администратор, установщик или оператор могут управлять модулем реле, настенным выключателем и интеллектуальной розеткой.

Примечание

- Возможность изменения настроек и объем разрешений зависят от типа пользователя.
- Здесь можно просматривать привязанные карты / метки и беспроводные брелоки пользователя без возможности изменения настроек.

8. Опционально. (Опция доступна только для администратора) нажмите **+** для добавления пользователя.

Управление картами / метками

После добавления карт / меток в охранную панель можно провести карту / метку, чтобы поставить или снять с охраны все датчики, добавленные в определенные области охранной панели, или отключить тревожные уведомления.

Шаги

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек .
2. Нажмите → **User Management** → **Card / Tag** («Управление пользователями → Карты / метки»), чтобы перейти на страницу управления картами / метками.

3. Нажмите + для добавления карты / метки.
4. Услышав голосовую подсказку **Swipe Tag** («Считайте карту»), поднесите карту / метку в область считывания карты / метки на охранной панели.
   - Сигнал бипера означает, что карта / метка успешно распознана.
   - Метка будет отображаться на странице управления картами / метками.
5. Опционально. Выберите карту / метку, чтобы перейти на страницу настроек.
6. Нажмите , чтобы изменить имя метки.

Примечание

- Пропустите этот шаг, если выполнен вход в качестве установщика. Возможность редактирования наименования метки доступна только для администратора.
- Наименование должно содержать от 1 до 32 символов.

7. Поставьте галочку **Enable Card / Tag** («Активировать карту / метку»).
8. Выберите привязанного пользователя.
9. Выберите тип метки.

Примечание

Тип разрешения метки зависит от типа привязанного пользователя.

Работа с метками

Проведите метку, чтобы поставить область на охрану / снять область с охраны.

Патрульные метки

Проведите меткой для загрузки записи в систему.

10. Опционально. Нажмите **Delete** («Удалить»), чтобы удалить метку.

Информация об устройстве

При необходимости можно изменить язык и выбрать часовой пояс.

Шаги

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **System** → **Configuration** («Система → Настройки»), чтобы перейти на страницу настроек времени.
3. Выберите язык устройства и часовой пояс.
4. При необходимости включите функцию DST (переход на летнее время).

DST

Переход на летнее время (DST) — это практика перевода часов вперед при более продолжительном дневном свете, чтобы по вечерам было больше дневного света и по утрам меньше.

Управление системой

Шаги

1. На странице списка устройств, выберите охранную панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **System** → **System Options** → **System Management** («Система → Параметры системы → Управление системой»), чтобы открыть страницу.

Forced Auto Arm («Принудительная автоматическая постановка на охрану»)

Если опция включена и в зоне присутствуют активные неисправности, зона будет исключена автоматически при постановке на охрану.

Примечание

Необходимо отключить функцию постановки на охрану на странице дополнительных настроек. При наличии неисправности постановка панели на охрану не будет выполнена.

Forced Arming («Принудительная постановка на охрану»)

Если опция включена и в зоне присутствуют активные неисправности, зона будет исключена при постановке на охрану.

System Status Report («Отчет о состоянии системы»)

Если опция включена, устройство автоматически загрузит отчет при изменении статуса панели.

Voice Prompt («Голосовое предупреждение»)

Если опция включена, панель включит текстовое голосовое предупреждение. Здесь можно установить подробную подсказку: **подсказка об ошибке при постановке на охрану, подсказка об ошибке при снятии с охраны, подсказка об ошибке, когда охрана активирована, подсказка об ошибке, когда охрана отключена, голосовое предупреждение при тревоге.**

System Volume («Громкость системы»)

Доступный диапазон громкости системы: от 0 до 10.

Audible Tamper Alarm («Тревога тампера»)

Если опция включена, при открытии крышки будет срабатывать бипер.

Alarm Duration («Длительность тревоги»)

Длительность тревоги на охранной панели.

Wireless Supervision Loss («Ошибка беспроводного управления»)

Настройте максимальную продолжительность интервала опроса. Система сообщит о неисправности, если продолжительность превышает установленное значение.

Bypass on Re-Arm («Обход зоны при повторной постановке на охрану»)

Если функция включена, зона с неисправностью будет автоматически исключена при повторной постановке на охрану.

Jamming Sensitivity Settings («Настройки чувствительности к помехам»)

Устройство обнаружит радиочастотные помехи и отправит push-сообщения, когда создаются помехи для радиосигналов. Настройте чувствительность обнаружения.

Fault LED Stay On When Armed («LED-индикатор неисправности остается включенным при постановке на охрану»)

Когда система поставлена на охрану, индикатор неисправности горит непрерывно.

Arm LED Stay On («LED-индикатор постановки на охрану остается включенным»)

LED-индикатор постановки на охрану горит непрерывно.

Hik-Connect Indicator («Индикатор Hik-Connect»)

Включите индикатор Hik-Connect.

Motion Detector Restore («Восстановление датчиков движения»)

К датчикам движения относятся все ИК-датчики.

Режим энергосбережения

Если режим энергосбережения включен и отключен основной источник питания, Wi-Fi переходит на низкое энергопотребление, отключается 4G, не выполняется считывание метки, не горит LED-индикатор, отключены голосовые подсказки.

PD6662

Включите стандарт PD6662. Несоответствующие стандарту функции не будут работать.

Проверка неисправности

Система определяет, следует или не следует производить диагностику неисправностей, перечисленных на странице. Система будет диагностировать только выбранную неисправность.

Шаги

1. На странице списка устройств, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Перейдите на вкладку → **System** → **System Options** → **System Fault Check** («Система → Параметры системы → Проверка неисправности»).

Detect Network Camera Disconnection («Обнаружение отключения IP-камеры»)

Если опция включена, сработает тревожный сигнал при отключении IP-камеры.

Panel Battery Fault Check («Проверка неисправности батареи»)

Если опция включена, устройство будет загружать события, когда батарея отключена или разряжена.

LAN Fault Check («Проверка неисправности LAN»)

Если опция включена, сработает тревожный сигнал при разрыве или сбоях проводной сети.

Wi-Fi Fault Check («Проверка неисправности Wi-Fi»)

Если опция включена, сработает тревожный сигнал при разрыве или сбоях подключения Wi-Fi.

Cellular Network Fault Check («Проверка неисправности сотовой сети»)

Если опция включена, сработает тревожный сигнал при разрыве или сбоях сотовой сети.

Main Power Lost («Тревога потери питания»)

Если опция включена, тревога сработает при отключении IP-камеры.

Power Save Mode («Потеря питания переменного тока»)

Система проводит проверку неисправности по истечении заданного времени после отключения питания переменного тока.

В соответствии со стандартом EN 50131-3 продолжительность проверки должна составлять 10 с.

Параметры постановки на охрану

Настройте расширенные параметры доступа.

Шаги

1. На странице списка устройств, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **System** → **System Options** → **Arm Options** («Система → Параметры системы
2. Параметры постановки на охрану»), чтобы открыть страницу.

Также можно настроить следующие параметры:

Arm with Faults («Постановка на охрану с условием подтверждения неисправностей»)

Отметьте неисправности в списке **Enable Arming with Fault list** («»Включить постановку на охрану при обнаружении неисправности»), и устройство не остановит процедуру постановки на охрану при обнаружении неисправности.

Early Alarm («Тревога по истечении времени задержки»)

Если функция включена и зона поставлена на охрану, при возникновении тревожного события, тревога сработает по истечении времени задержки.

Примечание

Данная тревога сработает только после срабатывания зоны с задержкой.

3. Нажмите **Save** («Сохранить»).

Режим регистрации

Шаги

1. На странице списка устройств, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **System** → **System Options** → **Enrollment Mode** («Система → Параметры системы → Режим регистрации»), чтобы открыть страницу.
3. Нажмите на иконку **Enter the Enrollment Mode** («Перейти в режим регистрации»). Зарегистрировать периферийное устройство можно посредством активации.

IP-камера

Здесь можно добавить, редактировать и удалить каналы IP-камер.

Шаги

1. На странице списка устройств, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Network Camera** → **Network Camera Channel** («IP-камера → Канал IP-камеры»), чтобы перейти на страницу.
3. Нажмите **+ Add Channel** («Добавить канал») и введите IP-адрес, имя пользователя и пароль, чтобы добавить канал.
4. Выберите камеру. Здесь можно просмотреть параметры камеры или нажать **Delete** («Удалить»), чтобы удалить ее.
5. Нажмите , чтобы изменить параметры.

Настройка параметров видео

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Network Camera** → **Event Video Settings** («IP-камера → Параметры видео по событию»), чтобы перейти на соответствующую страницу.
3. Выберите камеру и настройте параметры видео.

Stream Type («Тип потока»)

Main Stream («Основной поток»): используется при записи и предварительном просмотре в формате HD, имеет высокое разрешение, скорость кодового потока и качество изображения.

Sub-Stream («Дополнительный поток»): используется для передачи по сети и предварительного просмотра изображений в виде потокового видео с возможностью более низкого разрешения, скорости передачи данных и качества изображения.

Bitrate Type («Тип битрейта»)

Выберите тип битрейта: **Constant** («Постоянный») или **Variable** («Переменный»).

Resolution («Разрешение»)

Выберите разрешение видеовыхода.

Bitrate («Битрейт»)

Чем выше значение, тем лучше качество видео, но требуется большая пропускная способность.

Before Alarm («Перед сигналом тревоги»)

Продолжительность записи до срабатывания тревоги.

After Alarm («После сигнала тревоги»)

Продолжительность записи после срабатывания тревоги.

Настройка расписания снятия / постановки на охрану

Шаги

1. На странице списка устройств, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Area** («Область»), чтобы перейти на страницу.
2. Выберите область из списка, включите ее и выберите связанные области.
3. Включите функцию автоматической постановки на охрану/ снятия с охраны и задайте время автоматической постановки на охрану / снятия с охраны. Также можно настроить время задержки снятия с охраны, время задержки входа, время задержки выхода, время задержки звукового оповещателя, исключение выходных и праздничных дней.

Auto Arm («Автоматическая постановка на охрану»)

Включите автоматическую постановку под охрану в заданное время.

Auto Arm Time («Длительность автоматической постановки под охрану»)

Установите расписание для автоматической постановки на охрану.

Auto Disarm («Автоматическое снятие с охраны»)

Включите автоматическое снятие с охраны в заданное время.

Auto Disarm Time («Время автоматического снятия с охраны»)

Настройте расписание для автоматического снятия с охраны.

Late to Disarm («Задержка снятия с охраны»)

Разрешите устройству отправлять уведомления на смартфон или планшет, чтобы напоминать пользователю о снятии области с охраны, если область находится под охраной после заданного времени.

Примечание

Активируйте функцию уведомления с помощью панели на веб-клиенте меню **Communication Parameters** → **Event Communication** («Параметры связи → Связь по событию») перед активацией функции **Late to Disarm** («Задержка снятия с охраны»).

Late to Disarm Time («Время задержки снятия с охраны»)

Задайте время, указанное в пункте **Late to Disarm** («Задержка снятия с охраны»)

Auto Arm Sound Prompt («Звуковое предупреждение автоматической постановки на охрану»)

После отключения бипер не будет подавать звуковой сигнал перед автоматической постановкой на охрану.

Weekend Exception («Исключение выходных дней»)

Если функция включена, указанные выше режимы не будут активны в выходные дни.

Holiday Exception («Исключения в праздничные дни»)

Если функция включена, режимы постановки и снятия с охраны не будут активны в праздничные дни. После включения необходимо настроить расписание выходных дней.

Примечание

Можно настроить до 6 групп праздничных дней.

Связь

Проводная сеть

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Перейдите на вкладку **Communication → Wired Network** («Связь → Параметры проводной сети»).
3. Настройте параметры.
   – Автоматические настройки: включите **DHCP** и настройте HTTP-порт.
   – Настройки вручную: отключите **DHCP** и настройте IP-адрес, маску подсети, адрес шлюза, адрес DNS-сервера.
4. Опционально. Установите корректный адрес DNS-сервера, если устройству необходимо подключиться к серверу Hik-Connect через доменное имя.
5. Нажмите **Save** («Сохранить»).

Сотовая сеть передачи данных

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек .
2. Перейдите на вкладку → **Communication Parameters** → **Cellular Data Network Settings** («Параметры связи → Параметры сотовой сети передачи данных»).
3. Включите **Cellular Data Network** («Сотовая сеть передачи данных»).
4. Нажмите, чтобы выбрать SIM-карту. Нажмите **Parameter Configuration → Edit Icon** («Настройка параметров → Изменить значок») и настройте параметры, в том числе, имя пользователя, пароль доступа, APN, MTU и PIN-код.
5. Нажмите **Save** («Сохранить»).
6. **Включите Data Usage Limit («Ограничение использования данных**»).
7. Измените **Data Used This Month** («Данные, используемые в этом месяце») и **Data Limited per Month** («Данные, ограниченные в месяц»).

Access Number («Номер доступа»)

Введите номер для связи с оператором.

Примечание

Номер доступа требуется ввести только пользователю SIM-карты частной сети.

User Name («Имя пользователя»)

Введите имя пользователя в соответствующее поле.

Access Password («Пароль доступа»)

Введите пароль пользователя в соответствующее поле.

APN

Запросите информацию APN у оператора сети и введите информацию в соответствующее поле.

Data Usage Limit («Ограничение использования данных»)

Включите функцию и настройте порог данных в месяц. При превышении порогового значения сработает тревога, которая будет загружена в центр тревог и мобильный клиент.

Data Used This Month («Данные, использованные в месяц»)

Используемые данные будут накапливаться и отображаться в данном текстовом поле.

Push-уведомления

Настройте параметры push-уведомлений, чтобы уведомления о тревоге были направлены на мобильный телефон.

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Перейдите на вкладку → **Communication Parameters** → **Push Notification(s) («Параметры связи → Параметры Push-уведомлений»).**
3. Выберите ЧОП / ПЦН или приложение.
4. Включите уведомления о целях.

Zone Alarm / Lid Opened («Тревога зоны / открытия крышки»)

Устройство будет отправлять push-уведомления, когда срабатывает тревога в зоне или при открытии крышки.

Примечание

Необходимо настроить время интервала фильтрации событий для телефонных вызовов.

Peripherals Lid Opened («Открытие крышки периферийного устройства»)

Устройство будет отправлять push-уведомления, при открытии крышки любого периферийного устройства.

Panel Lid Opened («Открытие крышки панели»)

Устройство будет отправлять push-уведомления при открытии крышки панели управления.

Panic Alarm («Тревога экстренного вызова»)

Устройство будет отправлять push-уведомления, при срабатывании тревоги экстренного вызова в зоне, на клавиатуре или на брелоке.

Medical Alarm («Тревога экстренной медицинской помощи»)

Устройство будет отправлять push-уведомления при срабатывании тревоги экстренной медицинской помощи.

Fire Alarm («Пожарная тревога»)

Устройство будет отправлять push-уведомления при срабатывании тревоги утечки газа.

Panel Status («Состояние панели»)

Устройство будет отправлять push-уведомления при изменении состояния панели.

Zone Status («Статус зоны»)

Устройство будет отправлять уведомления при изменении статуса зоны.

Peripherals Status («Состояния периферийных устройств»)

Устройство будет отправлять push-уведомления при изменении статуса любого периферийного устройства.

Panel Operation («Операции панели»)

Устройство будет отправлять push-уведомления, когда пользователь работает с охранной панелью.

Smart Alarm Event («События интеллектуальной тревоги»)

Устройство будет отправлять push-уведомления при срабатывании тревоги на тепловизионных камерах.

5. Нажмите **Phone Call and SMS** («Телефонный вызов и SMS-сообщения»).
6. Нажмите **+ Add Phone Number** («Добавить номер телефона»), чтобы ввести номер телефона.
7. Выберите добавленный номер телефона, чтобы включить телефонный вызов и SMS-сообщения в соответствии с вашими потребностями.
8. (для телефонного вызова) Настройте **Numbers of Calling** («Номера вызова»).
9. (для SMS-сообщений) Настройте **Arming Permission («Разрешение на постановку на охрану**»), **Disarming Permission («Разрешение на снятие с охраны»)** и **Alarm Clearing Permission («Разрешение на сброс тревоги для областей»).**

Общая подсказка

Введите **Common Voice** («Голосовое сообщение»). При срабатывании тревоги настроенный контент будет добавлен в начало сообщения, отправляемого системой. Можно импортировать **Common Voice** («Голосовое предупреждение»). При срабатывании тревоги настроенное голосовое предупреждение будет добавлено в начало содержимого телефона, набранного системой.

Примечание

Поддерживается только формат WAV до 512 КБ и 15 с.

10. Проверьте уведомления.

Пункт централизованного наблюдения (ЧОП / ПЦН)

Настройте параметры центра тревог: тревоги будут отправляться в настроенный центр тревог.

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Перейдите на вкладку → **Communication Parameters → Alarm Receiving Center (ARC) («Настройка параметров → ЧОП / ПЦН»)** для перехода на соответствующую страницу.
3. Выберите ЧОП / ПЦН и включите его.

Protocol Type («Тип протокола»)

Выберите **Protocol Type** («Тип протокола»): ADM-CID, ISUP, SIA-DCS, *SIA-DCS, *ADM-CID или CSV-IP, чтобы настроить режим загрузки.

Companies («Компания»)

Выберите компанию поддержки: **None** («Отсутствует»), **Hungary-Multi Alarm Receiving Company** («ЧОП / ПЦН в Венгрии») или **French Alarm Receiving Company** («ЧОП / ПЦН во Франции»).

Address Type («Тип адреса»)

Укажите тип адреса: **IP Address** («IP-адрес») или **Domain Name** («Доменное имя»). Введите адрес сервера / доменное имя, номер порта и код учетной записи.

Transmission Mode («Режимы передачи»)

Выберите режим передачи TCP или UDP. Протокол UDP рекомендуется стандартом SIA DC-09.

Retry Timeout Period («Период ожидания повторной попытки»)

По истечении выбранного времени система повторит попытку передачи.

Attempts («Попытки»)

Задайте количество повторных попыток.

Polling Option («Вариант опроса»)

Настройте частоту опроса в диапазоне от 10 до 3888000 секунд.

Periodic Test («Периодическая диагностика»)

Введите интервал периодической проверки.

GMT («Среднее время по Гринвичу»)

Включите среднее время по Гринвичу.

Настройки облачного сервиса

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Communication Parameters** → **Cloud Service Settings** («Параметры связи→ Настройки облачного сервиса»), чтобы открыть страницу.
3. Выберите **Communication Mode** («Режим связи»).
   Auto («Автоматич.»)
   Система автоматически выберет режим связи в соответствии с последовательностью проводной сети, сети Wi-Fi и сотовой сети передачи данных. Только когда текущая сеть отключена, устройство подключится к другой сети.
   Wired Network & Wi-Fi Priority («Приоритет проводной сети и сети Wi-Fi»)
   Порядок приоритета подключения: проводная сеть, Wi-Fi, сотовая сеть передачи данных.
   Wired &Wi-Fi («Проводная сеть и сеть Wi-Fi»)
   В первую очередь система выберет проводную сеть. Если проводная сеть не обнаружена, будет выбрана сеть Wi-Fi.
   Cellular Data Network («Сотовая сеть передачи данных»)
   Система выберет только сотовую сеть передачи данных.
4. Включите **Periodic Test** («Периодическая проверка»). Введите интервал периодической проверки.
5. Нажмите **Save** («Сохранить»).

Уведомление по Email

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Communication Parameters** → **Notification by Emails** («Параметры связи→ Уведомление по электронной почте»), чтобы войти на страницу.
3. Включите **Email**.
4. Введите имя отправителя, адрес электронной почты отправителя, адрес SMTP-сервера, порт SMTP, имя пользователя и пароль.
5. Выберите тип шифрования: **None** («Отсутствует»), SSL или TLS.
6. Активация **Server Authentication («Аутентификация сервера»)**.
7. Введите имя получателя и адрес электронной почты получателя. Нажмите **Test Receiver Email Address** («Проверить адрес электронной почты получателя»), чтобы проверить правильность адреса электронной почты.
8. Нажмите **Save** («Сохранить»).

Настройка параметров FTP

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Communication Parameters** → **FTP Settings** («Параметры связи → Настройки FTP»), чтобы открыть страницу.
3. Выберите **Preferred FTP** («Предпочитаемый FTP») или **Alternated FTP** («Альтернативный FTP») и включите FTP.
4. Настройте параметры FTP.

   FTP Type («Тип FTP»)

   Настройте тип FTP: предпочтительный или альтернативный.

   Protocol Type («Тип протокола»)

   Можно выбрать FTP и SFTP. Загрузка файлов зашифрована с помощью протокола SFTP.

   Server Address and Port («Адрес сервера и номер порта»)

   Адрес FTP сервера и соответствующий номер порта.

   User Name and Password («Имя пользователя и пароль»)

   Пользователю FTP необходимо иметь разрешение для загрузки изображений. Если FTP сервер разрешает анонимным пользователям загружать изображения, можно выбрать режим **Anonymous** («Анонимный»), чтобы скрыть информацию об устройстве во время загрузки.

   Directory Structure («Структура директорий»)

   Путь сохранения захваченных изображений в FTP сервере.
4. Нажмите **Save** («Сохранить»).

NAT

Universal Plug и Play (UPnP ™) – это сетевая архитектура, обеспечивающая совместимость сетевого оборудования, программного обеспечения и других устройств. Протокол UPnP позволяет легко подключать устройства и упрощает реализацию сетей в домашних и корпоративных средах.

Если функция включена, не требуется настраивать проброс портов для каждого порта, камера подключается к WAN через роутер.

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Communication Parameters** → **NAT** («Параметры связи→ NAT»), чтобы открыть страницу.
3. Передвиньте ползунок, чтобы включить функцию UPnP.
4. Опционально. Выберите тип сопоставления **Manual** («Вручную») и задайте порт HTTP и порт службы.
5. Нажмите **Save** («Сохранить»), чтобы завершить настройку.

Служба внутренней связи

Настройте службу внутренней связи для оповещателя.

Перед началом

В первую очередь необходимо зарегистрировать оповещатель внутренней связи.

Только один оповещатель может быть установлен в качестве оповещателя внутренней связи.

Шаги

1. Нажмите **Communication** → **Intercom Service** («Связь → Служба внутренней связи»), чтобы войти на страницу.
2. Сдвиньте ползунок для включения функции.
3. Задайте тип внутренней связи.
   SIP-сервер
   Панель управления будет использовать сервер ПОП / ПЦН и SIP.
   IP Receiver Pro
   В панели управления будет отображаться облачный сервис.
4. Выберите оповещатель и нажмите **Save** («Сохранить»).

Техническое обслуживание устройств

Перезагрузите устройство.

Шаги

1. На странице объекта, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Maintenance → Reboot Device («Обслуживание → Перезагрузка устройства»**), чтобы перейти на соответствующую страницу. Панель будет перезагружена.
3. Нажмите → **Maintenance** → **Device Upgrade** («Обслуживание → Обновление устройства»), чтобы проверить версию системы.

Панель обновится до последней версии.

4. Опционально. Нажмите → **Maintenance** → **Remote Log Collection («Обслуживание → Удаленный сбор журналов»)**, чтобы включить эту функцию.
   Удаленный сбор журналов предназначен для получения журналов, относящихся к устройству. Когда эта функция включена, наша служба технической поддержки сможет удаленно собирать журналы, относящиеся к устройству, и загружать их на наш сервер для устранения неполадок. Настройте необходимый срок действия. Данная функция будет отключена по истечении установленного срока действия.

Wi-Fi-соединение

Подключите охранную панель к Wi-Fi через приложение.

Шаги

1. На странице списка устройств, выберите панель и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек.
2. Нажмите → **Configure Wi-Fi Network** («Настройка сети Wi-Fi»).
3. Следуйте приведенным ниже инструкциям, чтобы переключить панель в режим точки доступа. Нажмите **Next** («Далее»).
4. Выберите стабильное Wi-Fi-соединение для подключения устройства.
5. Вернитесь на страницу настроек, введите пароль Wi-Fi и нажмите **Next** («Далее»).

6. Нажмите **Connect to a Network** («Подключить к сети») и дождитесь подключения.
   После завершения подключения панель предложит выйти из режима точки доступа и автоматически переключится в режим станции (STA).

Проверка тревожных уведомлений

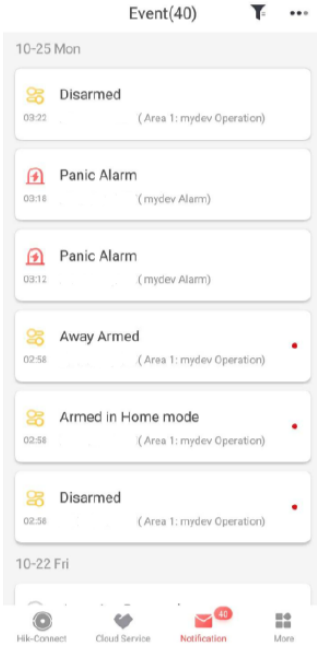
Уведомления о тревожных событиях будут направлены при срабатывании тревоги.
Информацию о тревоге можно просмотреть в мобильном клиенте.

Перед началом

- Убедитесь, что зона связана с датчиком.
- Убедитесь, что зона не исключена.
- Убедитесь, что функция **Silence Alarm** («Отключение тревожных уведомлений») не активна.

Шаги

1. Нажмите **Notification** («Уведомления») в мобильном клиенте, чтобы перейти на соответствующую страницу.
   Все уведомления о тревожных событиях будут перечислены на странице уведомлений.
2. Выберите тревогу для просмотра подробных сведений.



3. Опционально. Если зона связана с камерой, можно просматривать видео при срабатывании тревоги.
4. Опционально. Нажмите , чтобы начать поиск событий по датам или устройствам.

5.3 Настройка параметров с помощью веб-клиента

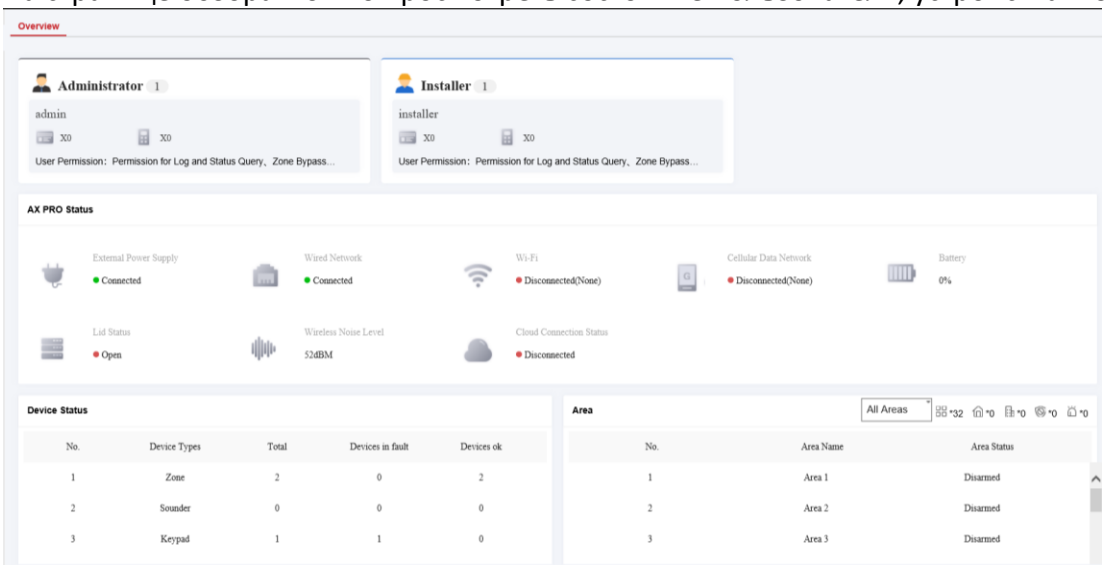
Шаги

1. Подключите устройство к Ethernet.
2. Найдите IP-адрес устройства с помощью клиентского ПО и ПО SADP.
3. Введите найденный IP-адрес в адресную строку.
4. Для входа используйте имя пользователя и пароль активации.

Примечание

- Вход в веб-клиент доступен только администраторам и установщикам.
- Имя пользователя и пароль те же, что и при активации через Hik-Connect или Hik-ProConnect.

На странице обзора можно просмотреть состояние пользователя, устройства и области.



5.3.1 Настройки связи

Проводная сеть

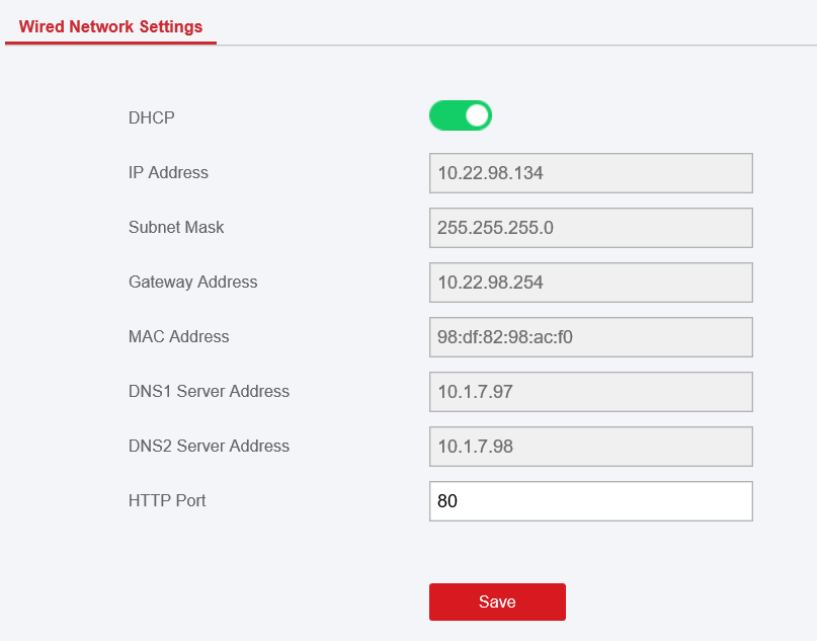
Настройте IP-адрес устройства и другие параметры сети.

Шаги

Примечание

Доступный функционал зависит от модели устройства.

1. Перейдите на вкладку **Communication → Wired Network** («Связь → Параметры проводной сети»).



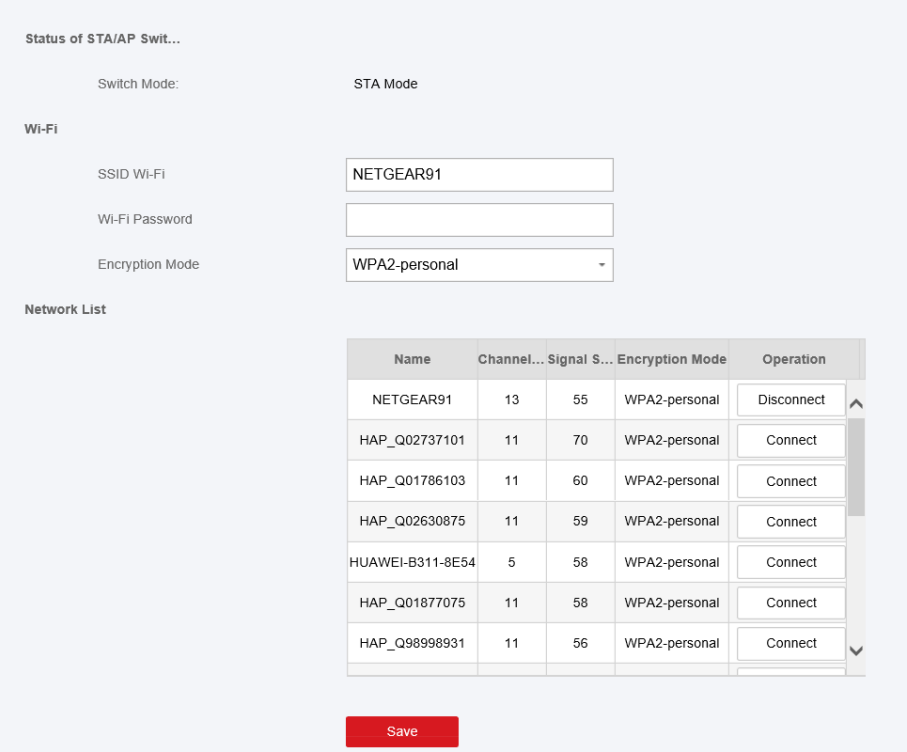
2. Настройте параметры.
– Автоматические настройки: включите **DHCP** и настройте HTTP-порт.
– Настройки вручную: отключите **DHCP** и настройте IP-адрес, маску подсети, адрес шлюза, адрес DNS-сервера.
3. Опционально. Установите корректный адрес DNS-сервера, если устройству необходимо подключиться к серверу Hik-Connect через доменное имя.
4. Нажмите **Save** («Сохранить»).

Wi-Fi

Настройте параметры Wi-Fi, если поблизости присутствуют безопасные и надежные сети Wi-Fi.

Шаги

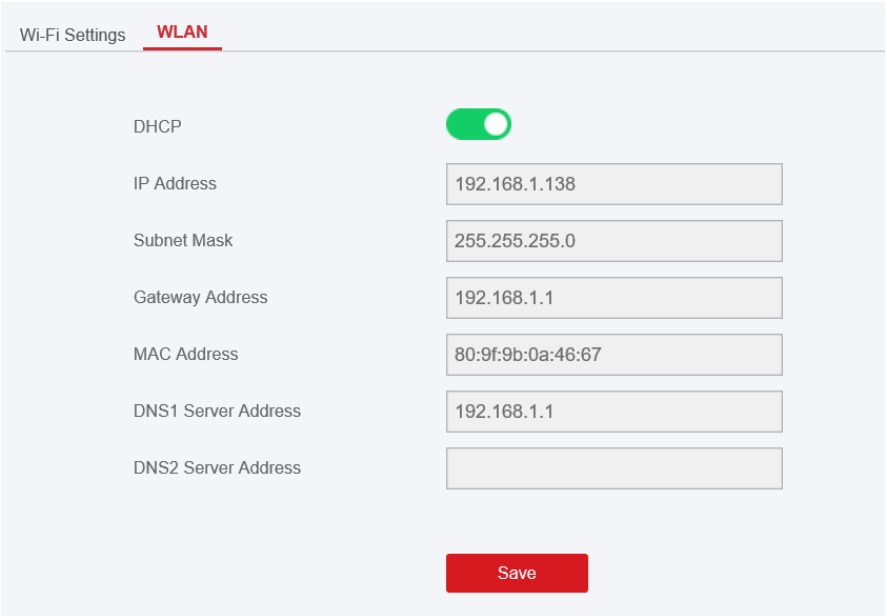
1. Перейдите на вкладку **Communication → Wi-Fi («Связь → Wi-Fi»).**



2. Подключитесь к сети Wi-Fi.

– Подключение вручную: введите **SSID Wi-Fi** и **пароль Wi-Fi**, выберите режим шифрования и нажмите **Save** («Сохранить»).
– Выберите из списка сетей: выберите сеть Wi-Fi из списка. Нажмите **Connect** («Подключиться»), введите пароль Wi-Fi и нажмите **Connect** («Подключиться»).

3. Нажмите **WLAN**, чтобы перейти на страницу WLAN.



4. Настройте IP-адрес, маску подсети, адрес шлюза и адрес DNS-сервера.

Примечание

Включите DHCP, чтобы устройство получило параметры Wi-Fi автоматически.

5. Нажмите **Save** («Сохранить»).

Сотовая сеть

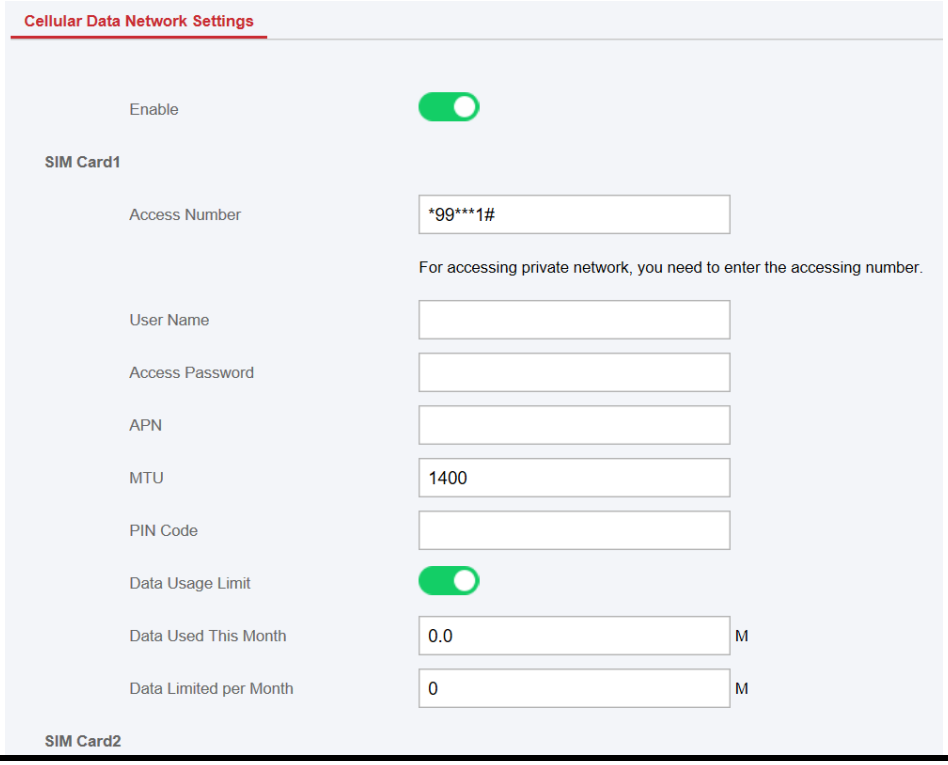
Настройте параметры сотовой сети, если используется SIM-карта. Используя сотовую сеть, устройство может загружать уведомления о тревожных событиях в центр тревог.

Перед началом

Вставьте SIM-карту в слот для SIM-карты.

Шаги

1. Перейдите на вкладку **Communication → Cellular Data Network** («Параметры связи → Параметры сотовой сети»).



Примечание

Номер доступа требуется ввести только пользователю SIM-карты частной сети.

2. Включите функцию.
3. Настройте параметры сотовой сети.

Access Number («Номер доступа»)

Введите номер для связи с оператором.

Примечание

Номер доступа требуется ввести только пользователю SIM-карты частной сети.

User Name («Имя пользователя»)

Введите имя пользователя в соответствующее поле.

Access Password («Пароль доступа»)

Введите пароль пользователя в соответствующее поле.

APN

Запросите информацию APN у оператора сети и введите информацию в соответствующее поле.

Data Usage Limit («Ограничение использования данных»)

Включите функцию и настройте порог данных в месяц. При превышении порогового значения сработает тревога, которая будет загружена в центр тревог и мобильный клиент.

Data Used This Month («Данные, использованные в месяц»)

Используемые данные будут накапливаться и отображаться в данном текстовом поле.

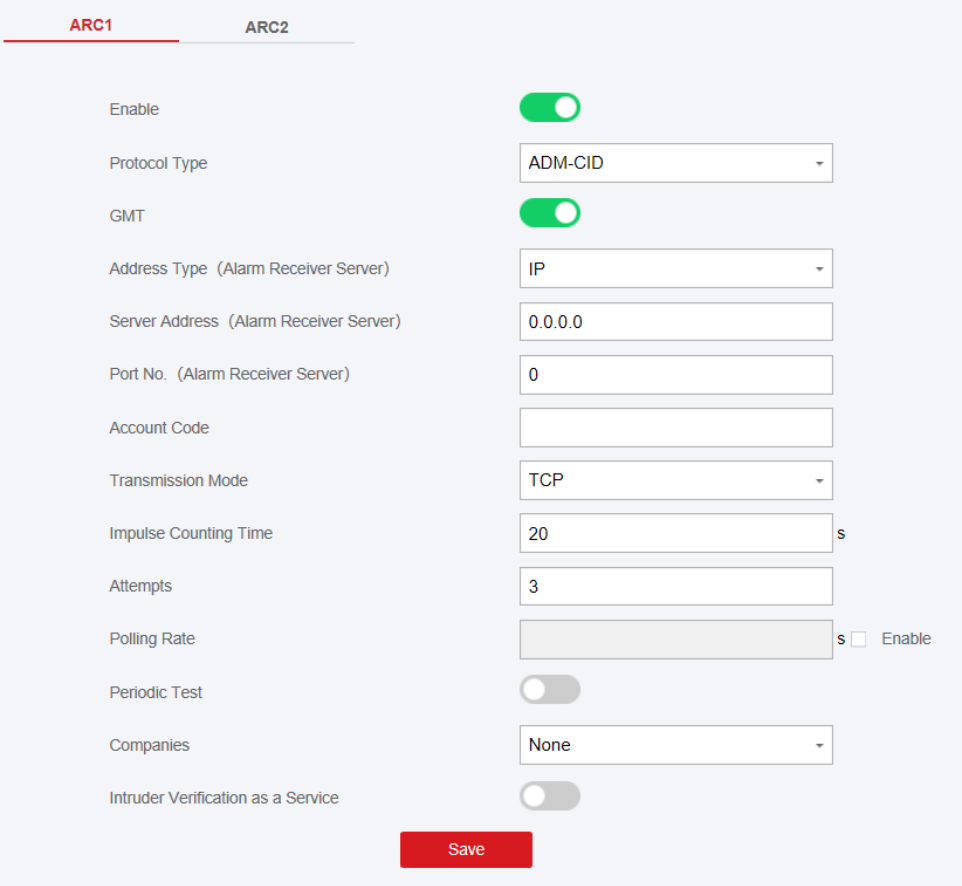
4. Нажмите **Save** («Сохранить»).

Центр тревог (ЧОП / ПЦН)

Настройте параметры центра тревог: тревоги будут отправляться в настроенный центр тревог (ЧОП / ПЦН).

Шаги

1. Нажмите **Communication** → **Alarm Receiving Center** («Связь → Центр тревог») для перехода на страницу центра тревог.



2. Выберите 1 или 2 ЧОП / ПЦН для настройки параметров и сдвиньте ползунок, чтобы активировать выбранный центр тревог.

Примечание
Если ЧОП / ПЦН 1 включен, можно установить ЧОП / ПЦН 2 в качестве резервного канала и отредактировать параметры канала.

3. Выберите **Protocol Type** («Тип протокола»): **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, ***ADM-CID** или **CSV-IP**, чтобы настроить режим загрузки.

Примечание
Протокол стандарта DC-09
ADM-CID: метод представления данных DC-09 — это CID, который не зашифрован и предназначен только для загрузки отчета о тревоге.
* ADM-CID: метод представления данных DC-09 — CID, который зашифрован и предназначен только для загрузки отчета о тревоге.
SIA-DCS: метод представления данных DC-09 — DCS (также именуемый как протокол SIA), который не зашифрован и предназначен только для загрузки отчета о тревоге.
* SIA-DCS: метод представления данных DC-09 — DCS (также именуемый как протокол SIA), который зашифрован и предназначен только для загрузки отчета о тревоге.

ADM-CID или **SIA-DCS:** выберите тип ЧОП / ПЦН: **IP** («IP-адрес») или **Domain name** («Доменное имя») и введите адрес IP-адрес, номер порта, код учетной записи, время подсчета импульсов, количество попыток, частоту опроса.

Примечание
Настройте частоту опроса в диапазоне от 10 до 3888000 секунд.

ISUP, CSV-IP или FSK: нет необходимости настраивать параметры протокола.
***SIA-DCS** или ***ADM-CID** Выберите тип центра тревог: по IP-адресу или доменному имени и введите IP-адрес / доменное имя, номер порта, код учетной записи, время подсчета импульсов, попытки, частоту опроса, параметры шифрования, длину пароля и т. д.

Примечание
Настройте частоту опроса в диапазоне от 10 до 3888000 секунд.

4. Нажмите **Save** («Сохранить»).

Функция PIRCAM для загрузки изображений или видео.

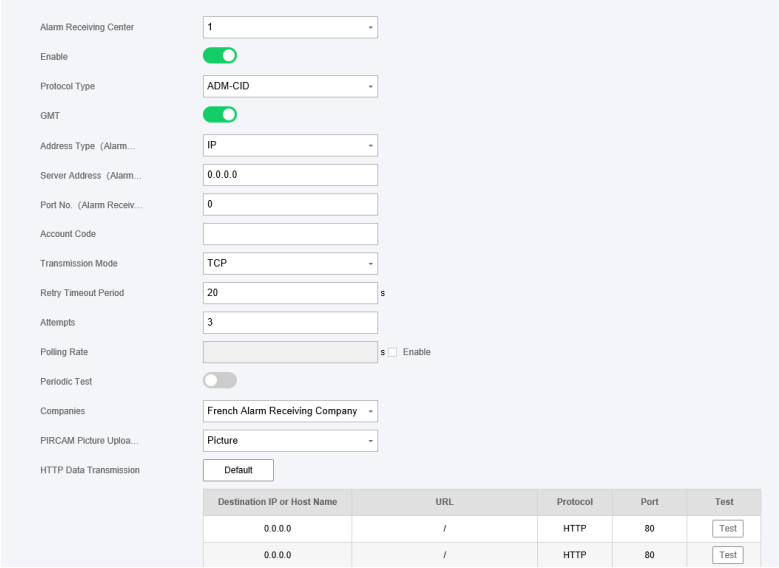
Включите функцию PIRCAM для загрузки изображений или видео.

1. Загрузка изображений
   Можно загрузить от 1 до 20 изображений.

(1) Нажмите **Communication → Alarm Receiving Center** («Связь → ЧОП / ПЦН»), чтобы перейти на страницу ЧОП / ПЦН.
(2) Сдвиньте ползунок, чтобы включить выбранный центр тревог.
(3) Выберите **Protocol Type** («Тип протокола»): **SIA-DCS.**

(4) Выберите **Companies** («Компании»): **French Alarm Receiving Company** («Французская компания, выступающая в качестве ЧОП / ПЦН»).

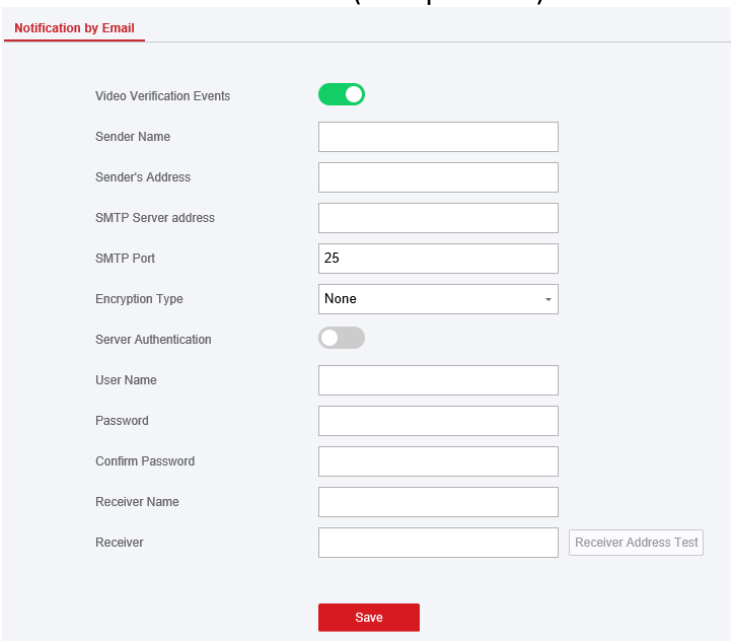
(5) Нажмите **Save** («Сохранить»).



(6) Настройте параметры SMTP или FTP.

Настройте параметры SMTP:

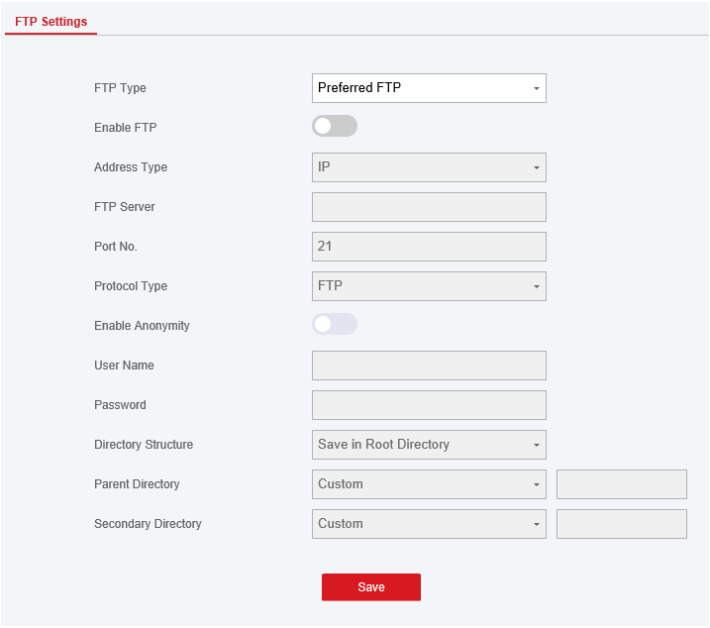
Нажмите **Communication** → **Notification by Email** («Связь → Уведомления по Email»). Включите **Video Verification Events** («События видеоверификации») и настройте соответствующие параметры. Подробная информация представлена в разделе *Уведомления по Email.* Нажмите **Save** («Сохранить»).



Настройте параметры FTP:

Перейдите на вкладку **Communication → FTP** («Связь → FTP»), чтобы перейти на страницу настройки параметров FTP.

Сдвиньте ползунок, чтобы включить FTP, и настройте соответствующие параметры. Подробная информация представлена в разделе *FTP.* Нажмите **Save** («Сохранить»).



2. Загрузка видео

   Видео будут загружены, когда PIRCAM настроена на захват более двух изображений.

   (1) Нажмите **Communication → Alarm Receiving Center** («Связь → ЧОП / ПЦН»), чтобы перейти на страницу ЧОП / ПЦН.

   (2) Сдвиньте ползунок, чтобы включить выбранный центр тревог.

   (3) Выберите **Protocol Type** («Тип протокола»): **SIA-DCS.**

   (4) Нажмите **Save** («Сохранить»).

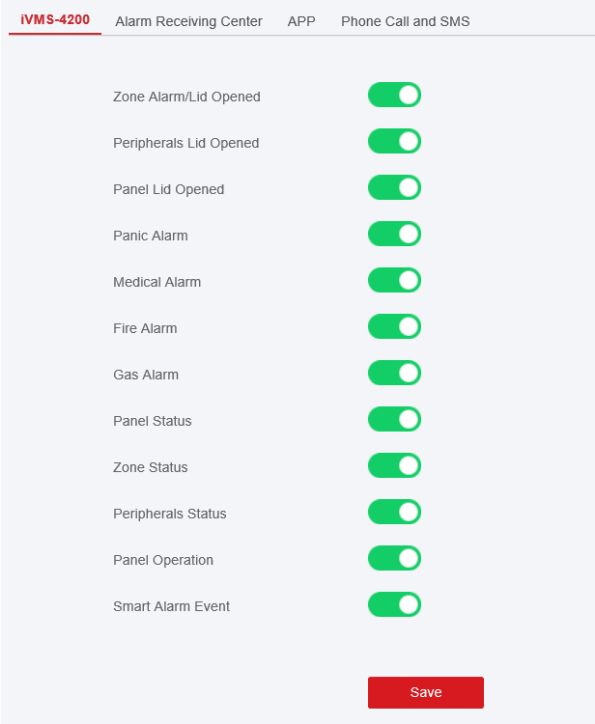
   (5) Настройте параметры SMTP или FTP аналогично параметрам для загрузки изображений.

Push-уведомления

Настройте параметры push-уведомлений, чтобы уведомления о тревоге были направлены в клиентское ПО, центр тревог, облачное хранилище или мобильный клиент.

Шаги

1. Перейдите на вкладку **Communication → Event Types Notification** («Связь → Уведомления о типе события»).



2. Включите уведомления о целях.

Zone Alarm / Lid Opened («Тревога зоны / открытия крышки»)

Устройство будет отправлять push-уведомления при срабатывании тревоги зоны (в веб-клиенте, программном клиенте или мобильном клиенте) или тревоги периферийных устройств зоны.

Peripherals Lid Opened («Открытие крышки периферийного устройства»)

Устройство будет отправлять push-уведомления при открытии крышки любого периферийного устройства.

Panel Lid Opened («Открытие крышки панели»)

Устройство будет отправлять push-уведомления при открытии крышки панели управления.

Panic Alarm («Тревога экстренного вызова»)

Устройство будет отправлять уведомления при срабатывании тревоги экстренного вызова на клавиатуре или на брелоке.

Medical Alarm («Тревога экстренной медицинской помощи»)

Устройство будет отправлять push-уведомления при срабатывании тревоги экстренной медицинской помощи на клавиатуре.

Fire Alarm («Пожарная тревога»)

Устройство будет отправлять push-уведомления при срабатывании пожарной тревоги на клавиатуре или при нажатии пользователем клавиши пожарной тревоги на клавиатуре.

Gas Alarm («Тревога утечки газа»)

Устройство будет отправлять push-уведомления при срабатывании тревоги утечки газа на клавиатуре.

Panel Status («Состояние панели»)

Устройство будет отправлять push-уведомления при изменении состояния панели.

Zone Status («Статус зоны»)

Устройство будет отправлять push-уведомления при изменении статуса зоны.

Peripherals Status («Состояния периферийных устройств»)

Устройство будет отправлять push-уведомления при изменении статуса любого периферийного устройства.

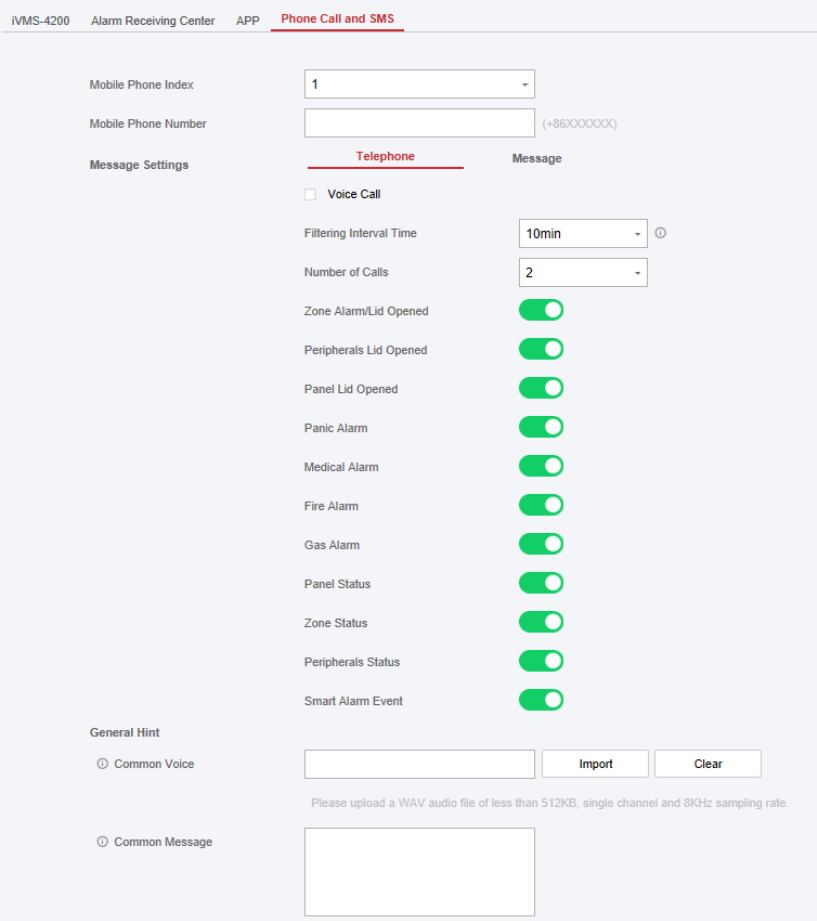
Panel Operation («Операции панели»)

Устройство отобразит уведомления, когда пользователь управляет устройством.

Smart Alarm Event («События интеллектуальной тревоги»)

Устройство будет отправлять push-уведомления при срабатывании тревоги на IP-камерах.

3. **Опционально.** Выберите номер ЧОП / ПЦН перед настройкой параметров.
4. **Опционально.** Чтобы уведомления о тревоге отправлялись в мобильный клиент, следует настроить параметры **Phone Call and SMS** («Телефонный вызов и SMS-сообщения»).



(1) Настройте **Mobile Phone Index** («Индекс мобильного телефона») и **Mobile Phone Number** («Номер мобильного телефона»).
(2) Проверьте **Voice Call** («Голосовой вызов») на странице телефона.
(3) Выберите **Filtering Interval Time** («Время интервала фильтрации») и **Number of Calls** («Количество вызовов»).
(4) Выберите SMS на странице сообщений.
(5) Выберите области, для которых разрешены постановка на охрану, снятие с охраны или сброс тревоги.

General Hint («Общая подсказка»)

Можно импортировать **Common Voice** («Голосовое предупреждение»). При срабатывании тревоги настроенное голосовое предупреждение будет добавлено в начало содержимого телефона, набранного системой.

Примечание

Поддерживается только формат WAV до 512 КБ и 15 с.

Введите **Common Voice** («Голосовое сообщение»). При срабатывании тревоги настроенный контент будет добавлен в начало сообщения, отправляемого системой.

5. Нажмите **Save** («Сохранить»).

Примечание

Для отправки уведомлений на мобильный телефон:

- Нажмите *, чтобы завершить вызов.
- При вводе номера мобильного телефона необходимо добавить проверочный код.

Облачный сервис

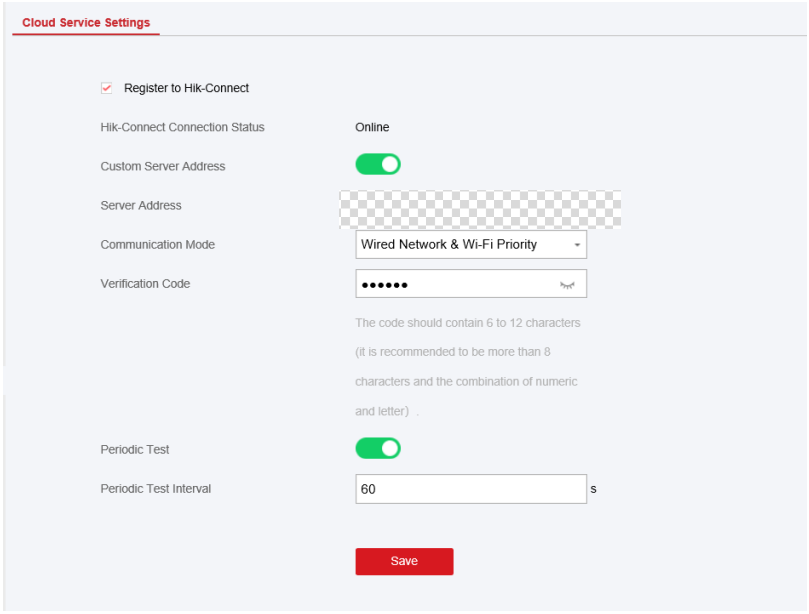
Чтобы зарегистрировать устройство в мобильном клиенте для удаленной настройки, необходимо предварительно настроить
параметры регистрации мобильного клиента.

Перед началом

- Подключите устройство к сети через проводное соединение, коммутируемое соединение или соединение Wi-Fi.
- Настройте IP-адрес устройства, маску подсети, шлюз и DNS-сервер в локальной сети.

Шаги

1. Перейдите на вкладку **Communication** → **Cloud Service** («Связь → Облачный сервис») для перехода на страницу регистрации в Hik-Connect.



2. Поставьте галочку **Register to Hik-Connect** («Зарегистрировать в Hik-Connect»).

Примечание

По умолчанию на устройстве включена служба Hik-Connect.

Статус устройства можно просмотреть на сервере Hik-Connect (www.hik-connect.com).

3. Включите **Custom Server Address** («Настраиваемый адрес сервера»).
   Адрес сервера будет отображаться в текстовом поле **Server Address** («Адрес сервера»).
4. Выберите режим связи из раскрывающегося списка.
   Wired Network & Wi-Fi Priority («Приоритет проводной сети и сети Wi-Fi»)
   Порядок приоритета подключения: проводная сеть, Wi-Fi, сотовая сеть передачи данных.

Wired &Wi-Fi («Проводная сеть и сеть Wi-Fi»)

В первую очередь система выберет проводную сеть. Если проводная сеть не обнаружена, будет выбрана сеть Wi-Fi.

Cellular Data Network («Сотовая сеть передачи данных»)

Система выберет только сотовую сеть передачи данных.

5. Опционально. Измените проверочный код.

Примечание

- По умолчанию в текстовом поле отображается проверочный код.
- Проверочный код должен содержать от 6 до 12 букв или цифр. По соображениям безопасности предлагается использовать 8-значный пароль, содержащий два или более символов следующего типа: буквы верхнего и нижнего регистра и цифры.

6. Включите **Periodic Test** («Периодическая проверка»). Введите интервал периодической проверки.
7. Нажмите **Save** («Сохранить»).

Уведомление по Email

Видео тревожного события или событие можно отправить на указанную электронную почту.

Шаги

1. Нажмите **Communication** → **Notification by Email** («Связь → Уведомление по Email»), чтобы перейти на страницу.
2. Выберите **Email 1** или **Email 2**. (**Email 2** является резервным для **Email 1**)
3. Включите **Video Verification Events («События видеоверификации»)** и **Server Authentication («Серверная аутентификация»)**.
4. Введите информацию об отправителе.

Примечание

Для отправки писем рекомендуется использовать Gmail и Hotmail.

Тревожное видео будет прикреплено к электронному письму только если зона связана с IP-камерой.

5. Введите информацию о получателе.
6. Нажмите **Receiver Address Test** («Проверка адреса получателя») и проверьте корректность адреса.
7. Нажмите **Save** («Сохранить») для сохранения настроек.

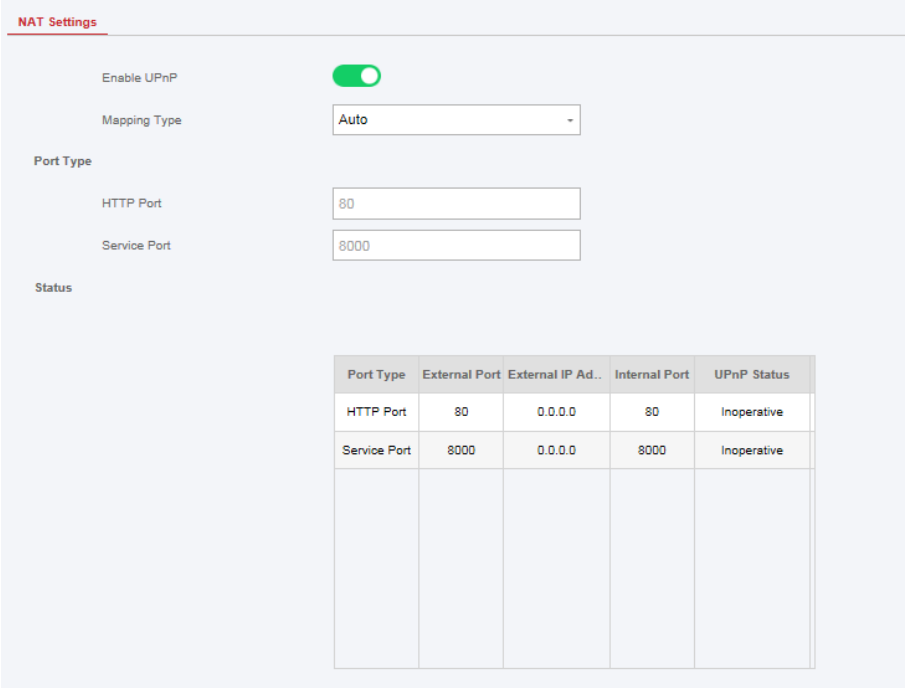
NAT

Universal Plug и Play (UPnP ™) – это сетевая архитектура, обеспечивающая совместимость сетевого оборудования, программного обеспечения и других устройств. Протокол UPnP позволяет легко подключать устройства и упрощает реализацию сетей в домашних и корпоративных средах.

Если функция включена, не требуется настраивать проброс портов для каждого порта, камера подключается к WAN через роутер.

Шаги

1. Перейдите на вкладку **Communication → NAT («Связь → NAT»).**



2. Передвиньте ползунок, чтобы включить функцию UPnP.
3. Опционально. Выберите тип сопоставления **Manual** («Вручную») и задайте порт HTTP и порт службы.
4. Нажмите **Save** («Сохранить»), чтобы завершить настройку.

FTP

Настройте FTP-сервер на сохранение тревожного видео.

Шаги

1. Перейдите на вкладку **Communication → FTP («Связь → FTP»).**
2. Настройте параметры FTP.

FTP Type («Тип FTP»)

Настройте тип FTP: предпочтительный или альтернативный.

Protocol Type («Тип протокола»)

Можно выбрать FTP и SFTP. Загрузка файлов зашифрована с помощью протокола SFTP.

FTP Server and Port No. («FTP-сервер и номер порта»)

Адрес FTP сервера и соответствующий номер порта.

User Name and Password («Имя пользователя и пароль»)

Пользователю FTP необходимо иметь разрешение для загрузки изображений. Если FTP сервер разрешает анонимным пользователям загружать изображения, можно выбрать режим **Anonymous** («Анонимный»), чтобы скрыть информацию об устройстве во время загрузки.

Directory Structure («Структура директорий»)

Путь сохранения захваченных изображений в FTP сервере.

Служба внутренней связи

Настройте службу внутренней связи для оповещателя.

Перед началом

В первую очередь необходимо зарегистрировать оповещатель внутренней связи.

Только один оповещатель может быть установлен в качестве оповещателя внутренней связи.

Шаги

1. Нажмите **Communication** → **Intercom Service** («Связь → Служба внутренней связи»), чтобы войти на страницу.
2. Сдвиньте ползунок для включения функции.
3. Задайте тип внутренней связи.

   SIP-сервер

   Панель управления будет использовать сервер ПОП / ПЦН и SIP.

   IP Receiver Pro

   В панели управления будет отображаться облачный сервис.
4. Выберите оповещатель и нажмите **Save** («Сохранить»).

5.3.2 Управление устройствами

В этом разделе представлена информация об управлении зарегистрированными периферийными устройствами, в том числе, датчиком, звуковым оповещателем, клавиатурой и т. д.

Зоны

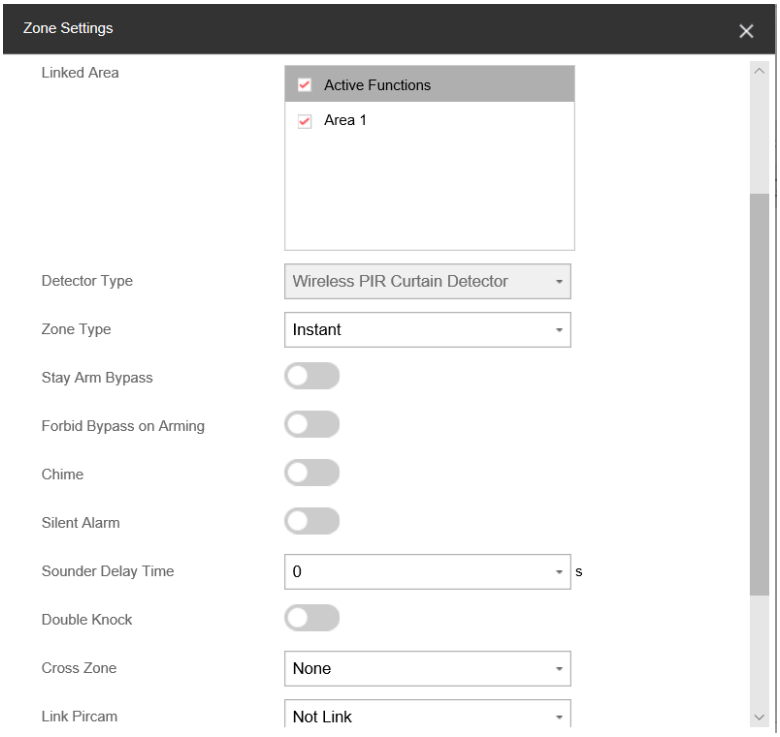
Настройте параметры зоны на соответствующей странице.

Шаги

1. Перейдите на вкладку **Device** → **Zone** («Устройства → Зоны»).

Zone	Device Number	Name	Main Device	Channel No	Device Types	Silent Alarm	Chime	Linked Camera	Operation
1	3	Wireless Zone 1	/	/	Instant	Disable	Disable	/	
2	4	Wireless Zone 2	/	/	Instant	Disable	Disable	/	

2. Выберите зону и нажмите для перехода на страницу настроек зоны.



3. Измените наименование зоны.
4. Активируйте привязанные области.

Примечание

- В списке будут отображаться только активированные зоны.
- Новое добавленное периферийное устройство по умолчанию связано с областью 1.

5. Выберите тип зоны.

Instant Zone («Зона мгновенного срабатывания»)

Данный тип зоны немедленно вызовет тревожное событие при постановке на охрану.

Delayed Zone («Зона отсроченного срабатывания»)

Задержка при выходе. Задержка при выходе дает время для выхода из защищенной зоны без срабатывания тревоги.

Задержка входа. Задержка срабатывания на входе дает время для входа в защищенную зону для отключения системы без срабатывания тревоги.

Если система включена или активирована повторно, система обеспечивает время задержки для входа/выхода. Обычно эта функция применяется на маршруте входа/выхода (например, входная дверь/главный вход), который является основным для постановки системы на охрану/снятия с охраны с помощью рабочей клавиатуры.

Примечание

- Настройте 2 разных периода времени: **System Options** → **Schedule & Time** («Параметры системы → Расписание и таймер»).
- В соответствии со стандартом EN50131-1, таймер не должен превышать 45 секунд.
- Настройте **Stay Arm Delay Time** («Время задержки постановки на охрану») для зоны задержки.

Panic Zone («Зона тревоги»)

Зона активна все время. Обычно применяется в местах, оборудованных тревожной кнопкой, датчиком дыма и извещателем разбития стекла.

Follow Zone («Зона слежения»)

При обнаружении тревожного события во время задержки входа в систему зона действует как зона отсроченного срабатывания. В других случаях — действует как зона мгновенного срабатывания.

Keyswitch Zone («Переключение между зонами»)

Связанная область будет поставлена на охрану после срабатывания тревоги и снята с охраны после восстановления нормального состояния. В случае тревоги саботажа операция постановки и снятия с охраны не сработает.

Примечание

Для зоны можно выбрать два типа триггера (по времени срабатывания и по статусу зоны). Если выбран тип состояния зоны, настройте правило срабатывания триггера (постановка на охрану / снятие с охраны).

Disabled Zone («Зона отключенного предупреждения»)

Зона отключена, любое тревожное событие будет игнорировало. Обычно используется для отключения неисправных детекторов.

24 Hours Zone («Зона с круглосуточным оповещением»)

Зона активна все время со звуковым сигналом / сиреной при срабатывании тревоги. Обычно используется в пожароопасных зонах, оборудованных детекторами дыма и датчиками температуры.

Timeout Zone («Зона заданного периода времени»)

Зона активна все время. Данный тип зоны используется для мониторинга и сообщения активного статуса зоны. Уведомления о статусе зоны будут направлены по истечении заданного времени (от 1 до 599 секунд). Можно использовать в местах, оборудованных магнитоконтактными датчиками, которые требуют доступа только на короткий период (например, дверца шкафа пожарного гидранта или дверца другого внешнего защитного ящика).

6. Поставьте галочку **Cross zone («Пересечение зоны»)**, **Silent Alarm («Зона беззвучной сигнализации»)** и т. д.

Примечание

Некоторые модели не поддерживают эту функцию. Опирайтесь на характеристики конкретной зоны.

Arm Mode («Режимы охраны»)

Если зона является общественной зоной (зона принадлежит более чем одной области), вы можете установить режим охраны.

И Зона будет поставлена на охрану, когда все выбранные зоны поставлены на охрану. Зона будет снята с охраны, когда любая из связанных областей снимается с охраны.

ИЛИ Зона будет поставлена на охрану, когда любая из связанных областей поставлена на охрану. Зона будет снята с охраны, когда все связанные области снимаются с охраны.

Когда зона находится в состоянии тревоги, снятые с охраны области, связанные с этой зоной, не могут быть поставлены на охрану.

Stay Arm Bypass («Частичная охрана»)

Зона будет автоматически исключена во время постановки на охрану.

Cross Zone («Пересечение зоны»)

PD6662 не включен: необходимо установить временной интервал.

При срабатывании тревоги первой зоны система начнет отсчет времени после восстановления зоны. Если тревога второй зоны сработает в течение установленного времени, обе зоны будут выдавать тревогу. В противном случае тревога не сработает. Если первая зона не будет восстановлена, обе зоны будут выдавать тревоги при срабатывании второй зоны даже по истечении установленного времени.

PD6662 включен: необходимо установить временной интервал.

Первая зона подаст сигнал при срабатывании тревоги. Если сработает тревога второй зоны до восстановления первой зоны, система сообщит о подтверждении тревоги. Если первая зона восстановлена, система начнет отсчет времени. Если тревога второй зоны сработает в течение установленного времени, система сообщит о подтверждении тревоги.

Если первая зона восстановлена, система начнет отсчет времени. Если вторая зона не сработает в течение установленного времени, система не будет выводить какую-либо информацию.

Forbid Bypass on Arming («Запрет обхода при постановке на охрану»)

Если функция включена, при постановке на охрану обход зоны будет недоступен.

Chime («Сигнал»)

Включите дверной звонок. Обычно используется для магнитоконтактных датчиков.

Silent Panic Alarm («Беззвучная тревога экстренного вызова»)

Если функция включена, при срабатывании тревоги будет загружен только отчет, звук издаваться не будет.

Double Knock («Функция двойного срабатывания»)

Если функция включена, можно установить временной интервал. Устройство выдаст тревогу, если датчик срабатывает дважды или непрерывно в течение определенного периода времени.

Sounder Delay Time («Время задержки звукового оповещателя»)

Звуковой оповещатель сработает сразу или по истечении установленного времени.

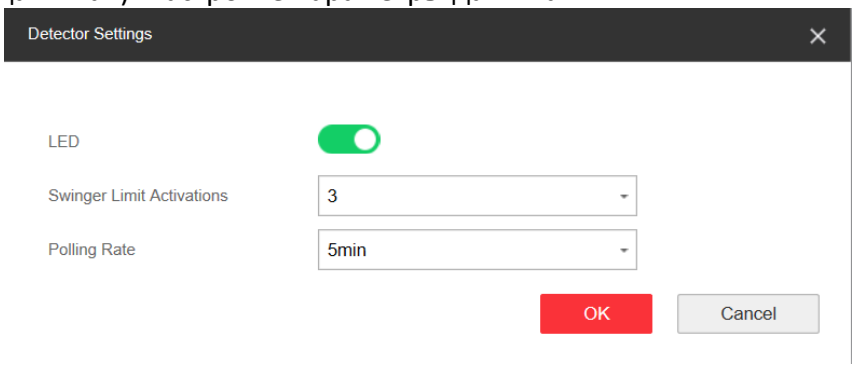
7. При необходимости привяжите PIRCAM или камеру к зоне.
8. Нажмите **OK**.

Примечание

После добавления передатчика нажмите **Device** → **Zone** → **Enroll** («Устройство → Зона → Зарегистрировать»), чтобы добавить зону проводного соединения. Выберите **Relate Mode** («Режим связи») как **Wired** («Проводное соединение»); **Device Source** («Источник устройства») как **Single** («Один передатчик») или **Multi Transmitter** («Несколько передатчиков»), **Channel** («Канал») и нажмите **OK**.

После настройки зоны перейдите на вкладку: **Maintenance** → **Device Status** → **Zone Status** («Обслуживание → Состояние устройства → Состояние зоны»), чтобы просмотреть состояние зоны.

9. Опционально. Нажмите **Device** → **Zone** («Устройство → Зона») и выберите **Detector Settings** («Настройки датчика»). Настройте параметры датчика.

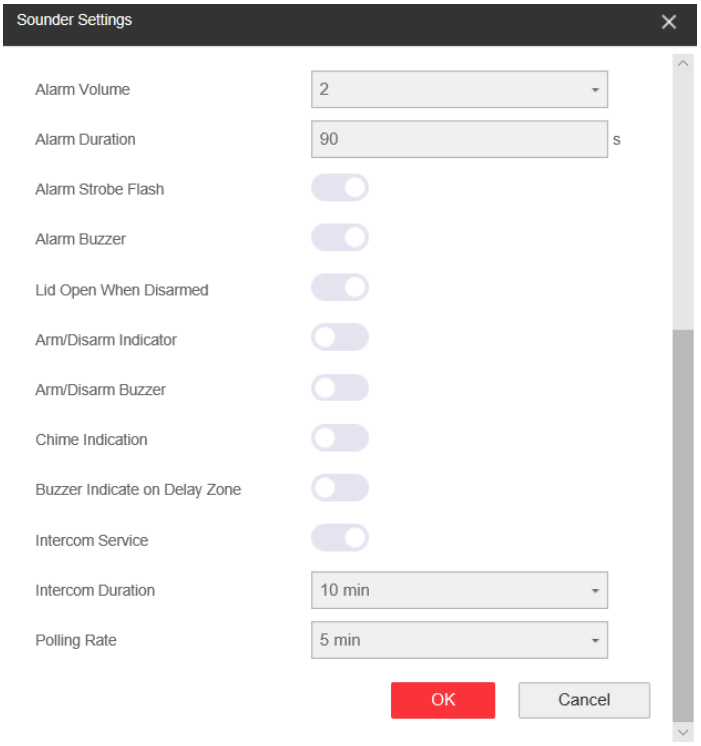


Звуковой оповещатель

Звуковой оповещатель регистрируется в панели через модуль беспроводного приемника, а беспроводной звуковой оповещатель с частотой 868 МГц может быть зарегистрирован в гибридной панели через беспроводной приемник, который использует адрес 9.

Шаги

1. Перейдите на вкладку **Device** → **Sounder** («Устройства → Звуковой оповещатель»).
2. Нажмите для перехода на страницу настроек звукового оповещателя.



3. Настройте имя тревоги, уровень громкости и продолжительность сигнала.

Примечание

Доступный диапазон громкости тревога: от 0 до 3 (функция зависит от модели устройства).
Доступный диапазон длительности тревоги: от 10 до 900 с.

4. Выберите связанную область.

Примечание

- В списке будут отображаться только активированные зоны.
- Новое добавленное периферийное устройство по умолчанию связано с областью 1.

5. Здесь можно включить: **Alarm Strobe Flash** («Стробоскоп»), **Alarm Buzzer** («Зуммер тревоги»), **Lid Open When Disarmed** («Открытие крышки при снятии с охраны»), **Arm / Disarm LED Indicator** («LED-индикатор постановки / снятия с охраны») и **Arm / Disarm Buzzer** («Зуммер постановки / снятия с охраны»).

Alarm Strobe Flash («Стробоскоп»)

Включите стробоскоп.

Alarm Buzzer («Зуммер тревоги»)

Включите тревогу.

Lid Open When Disarmed («Открытие крышки при снятии с охраны»)

Когда связанная область снята с охраны, периферийное устройство подаст сигнал об открытии крышки, а также сработает оповещатель.

Arm/Disarm LED Indicator («LED-индикатор постановки / снятия с охраны»)

Включите LED-индикатор постановки / снятия с охраны.

Arm / Disarm Buzzer («Бипер постановки на охрану / снятия с охраны»)
Включите зуммер постановки / снятия с охраны.
Chime Indicator («Индикатор звукового сигнала»)
Включите звуковой сигнал.
Buzzer Indicator on Delay Zone («Индикатор зуммера в зоне задержки»)
При задержке при входе или при выходе из зоны, в дополнение к панели управления, сирена также издаст тревогу.
Intercom Service («Служба внутренней связи»)
Включите службу внутренней связи. Только один оповещатель может включить эту функцию.

6. Настройте **Polling Rate** («**Частота опроса»)**.
7. При необходимости включите функцию **Enroll Wireless Sounder («Зарегистрировать звуковой оповещатель»).**
8. Нажмите **OK**.

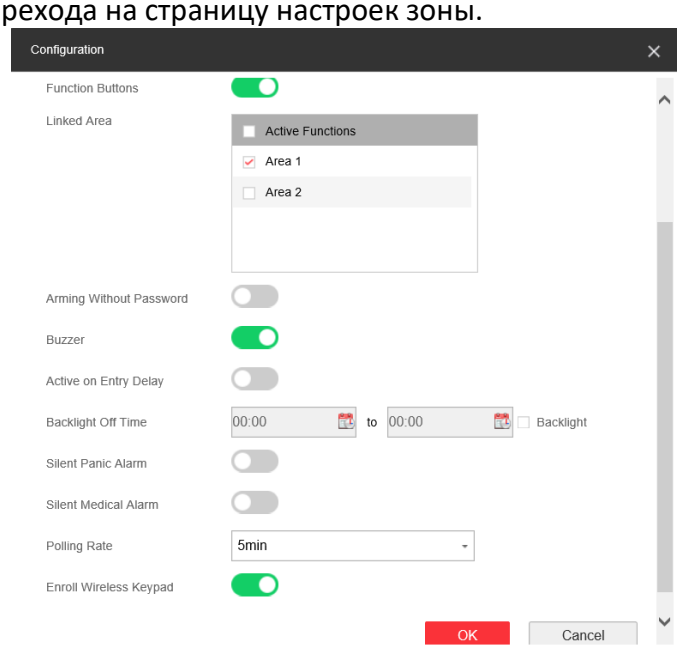
Примечание
После настройки оповещателя, перейдите на вкладку **Maintenance** → **Device Status** → **Sounder Status** («Обслуживание → Состояние устройства → Состояние звукового оповещателя»), для просмотра статуса оповещателя.

Клавиатура

Настройте параметры клавиатуры, зарегистрированной в панели.

Шаги

1. Нажмите **Device** → **Keypad** («Устройство → Клавиатура») для перехода на соответствующую страницу.
2. Нажмите для перехода на страницу настроек зоны.



3. Настройте наименование зоны.

4. Поставьте галочку, чтобы включить функцию зуммера, беззвучную сигнализацию экстренного вызова, беззвучную сигнализацию тревоги экстренной медицинской помощи и кнопки клавиатуры.
5. Включить функцию постановки на охрану без пароля и активации при задержке на вход.
6. Поставьте галочку **Enable** («Включить») в поле **Back-light Off Time** («Время выключения подсветки») и настройте продолжительность отключения подсветки.
7. Настройте частоту опроса.
8. Выберите связанную область.

Примечание

- В списке будут отображаться только активированные зоны.
- Новое добавленное периферийное устройство по умолчанию связано с областью 1.

9. Можно отменять регистрацию клавиатуры или оставить активной. Если привязка активна, устройство будет удалено.
10. Нажмите **OK**.

Примечание

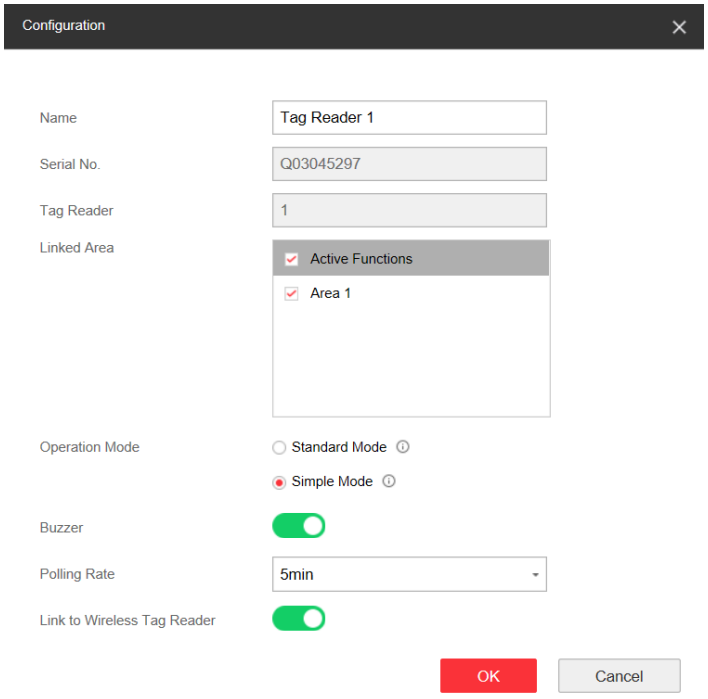
- После настройки клавиатуры, перейдите на вкладку **Maintenance** → **Device Status** → **Keypad Status** («Обслуживание → Состояние устройства → Состояние клавиатуры»).
- Настройте пароль клавиатуры на странице **User** → **User Management** → **Operation** («Пользователь → Управление пользователями → Операции»).

Считыватель карт (брелоков)

Настройте параметры считывателя карт (брелоков).

Шаги

1. Нажмите **Device** → **Automation** («Устройство → Автоматизация») для перехода на соответствующую страницу.
2. Нажмите **Enroll** («Зарегистрировать»), введите серийный номер для добавления считывателя.
3. Нажмите ⚙ для редактирования параметров считывателя карт (брелоков).



4. Измените наименование устройства.
5. Активируйте привязанные области.
6. Выберите режим работы.

   Standard Mode («Стандартный режим»)

   Выбор области и подтверждение неисправности поддерживаются при считывании метки для постановки или снятия с охраны.

   Simple Mode («Обычный режим»)

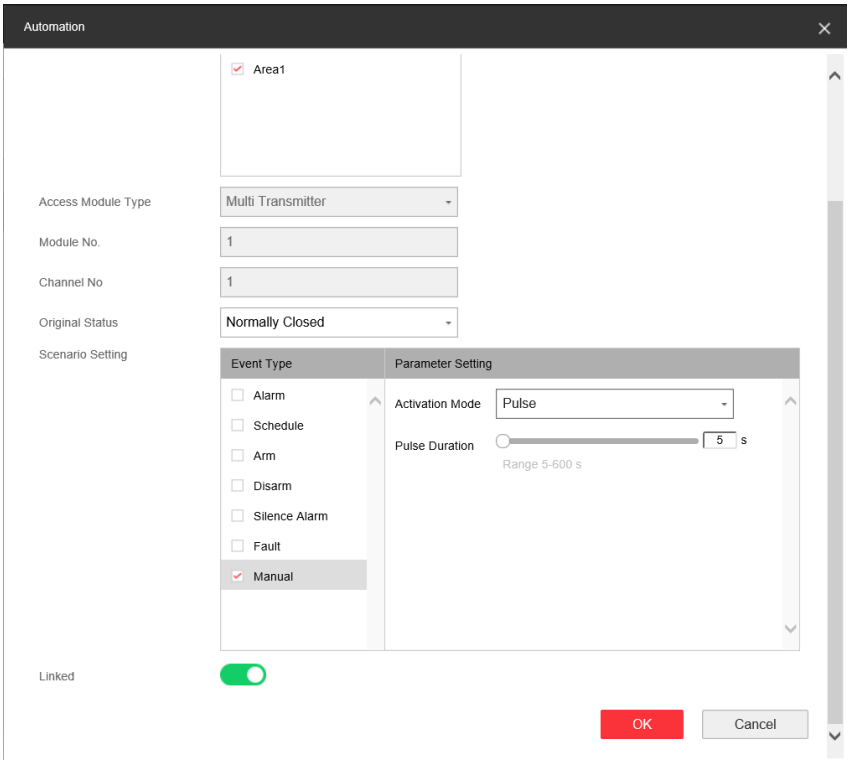
   Выбор номера области и подтверждение неисправности при считывании метки для постановки или снятия с охраны.
7. При необходимости включите бипер. Если бипер отключен, при считывании метки звуковой сигнал не будет издаваться.
8. Установите частоту опроса.
9. **Опционально.** Включите **Link to Wireless Tag Reader** («Привязать к беспроводному считывателю»).
10. Нажмите **OK**.

Автоматизация

Настройте параметры релейных выходов, зарегистрированных в панели.

Шаги

1. Нажмите **Device** → **Automation** («Устройство → Автоматизация») для перехода на соответствующую страницу.
2. Нажмите **Enroll** («Зарегистрировать»), введите серийный номер и выберите тип устройства для добавления устройства релейного вывода.
3. Нажмите ⚙ для редактирования информации о реле.



- Задайте наименование выходного релейного устройства.
- Выберите связанную область для вывода.

Примечание

- В списке будут отображаться только активированные зоны.
- Новое добавленное периферийное устройство по умолчанию связано с областью 1.
- Данная функция реализована не во всех реле.

- Состояние по умолчанию: **Normally Closed** («Всегда закрыто») или **Normally Opened** («Всегда открыто»).
- Настройте событие для срабатывания.
- Настрйоте активацию после срабатывания.
- Активируйте или отключите подключение к релейному выходному устройству. Если привязка активна, устройство будет удалено.

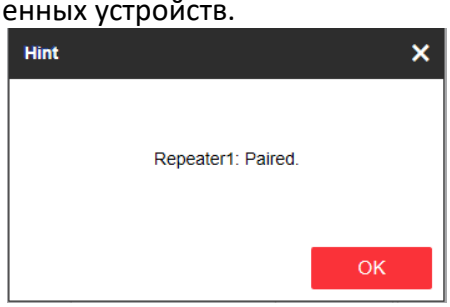
Ретранслятор

Ретранслятор может усиливать сигналы между панелью управления и периферийными устройствами.

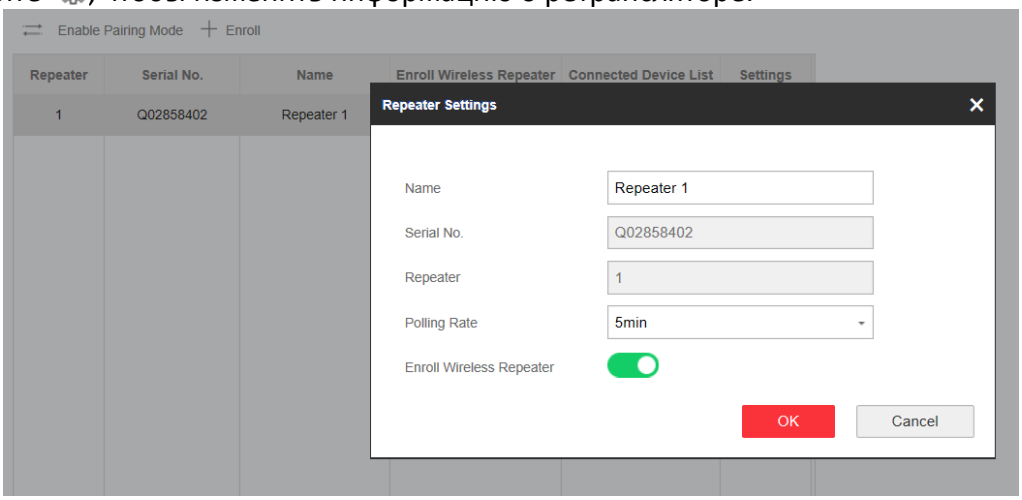
Шаги

1. Перейдите на вкладку **Device** → **Repeater** («Устройство → Ретранслятор»).
2. Нажмите **Enroll** («Зарегистрировать»), введите серийный номер и выберите тип устройства для добавления ретранслятора.
3. Нажмите **Enter Paring Mode** («Войти в режим сопряжения»), чтобы ретранслятор перешел в режим сопряжения устройств.

4. При большом расстоянии между периферийным устройством и панелью управления ретранслятор можно использовать в качестве станции передачи для сопряжения. Режим сопряжения длится 3 минуты и не может быть прерван. После успешного сопряжения отобразится список подключенных устройств.

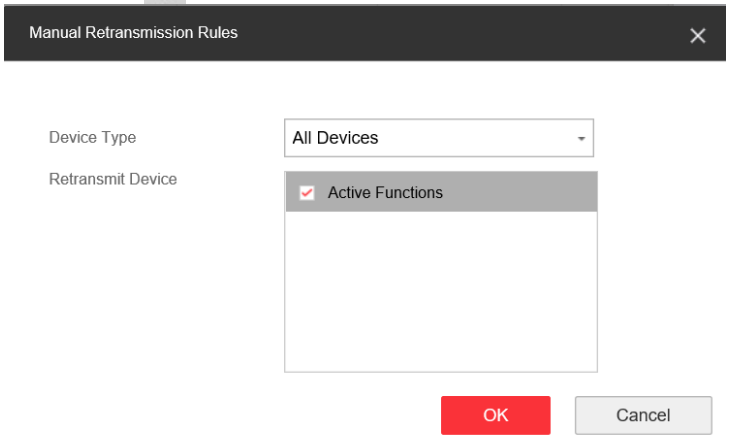


5. Нажмите , чтобы изменить информацию о ретрансляторе.



- Задайте наименование ретранслятора.
- Настройте частоту опроса ретранслятора.
- Активируйте или отмените регистрацию ретранслятора. Если привязка активна, устройство будет удалено.

6. Нажмите , чтобы перейти на страницу правил повторной передачи вручную.



- Выберите **Device Type** («**Тип устройства»)**.

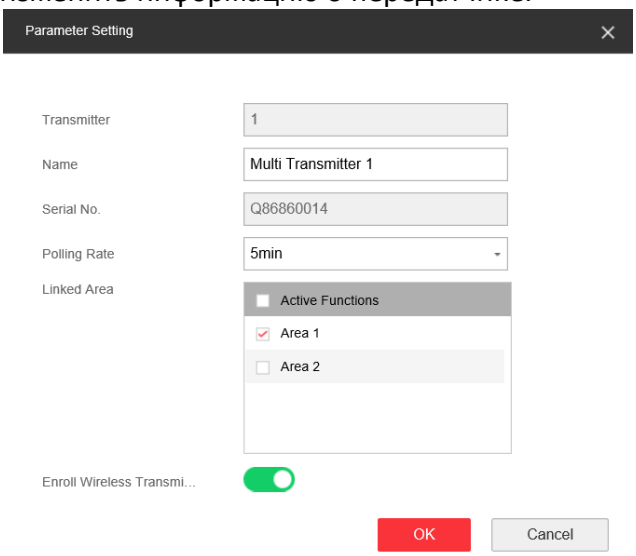
- Проверьте активные функции.
- Нажмите **OK**, после чего устройства можно будет повторно передать вручную.

Передатчик

Настройте параметры передатчика.

Шаги

1. Перейдите на вкладку **Device** → **Transmitter** («Устройство → Передатчик»).
2. Нажмите **Enroll** («Зарегистрировать»), введите серийный номер и выберите модель устройства для добавления передатчика.
3. Нажмите , чтобы изменить информацию о передатчике.



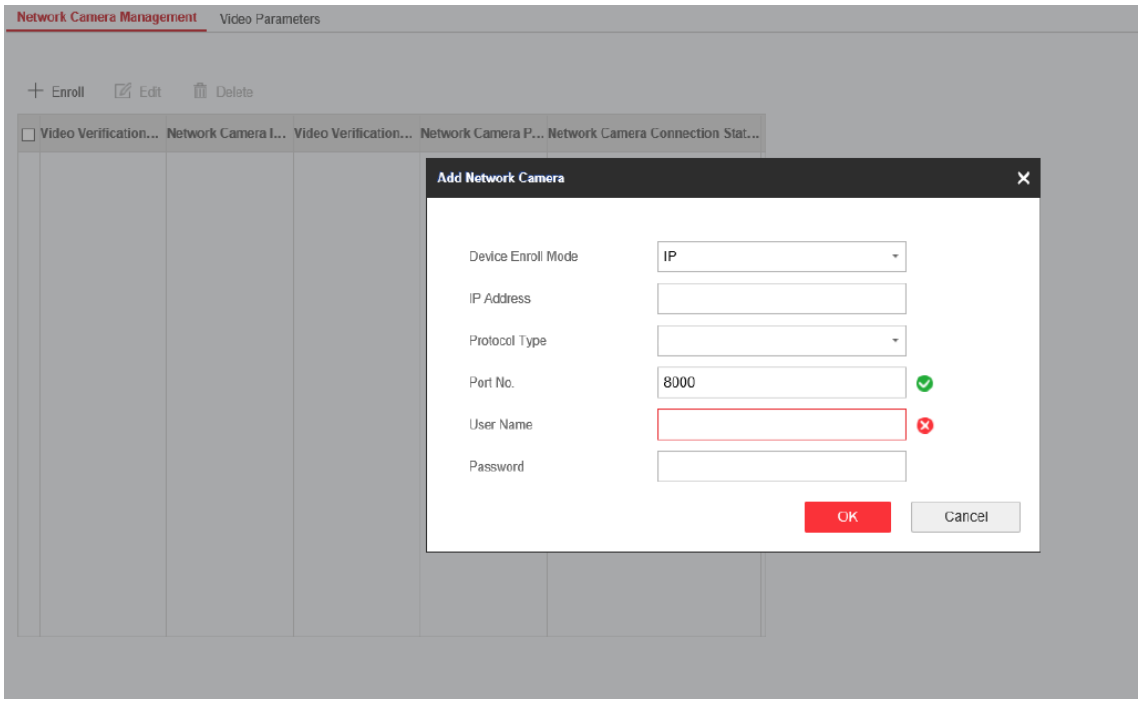
4. Задайте наименование передатчика.
5. Настройте частоту опроса передатчика.
6. Поставьте галочку **Enroll Wireless Transmission** («Регистрация беспроводного передатчика»).
7. Нажмите **OK**.

IP-камера

В систему можно добавить IP-камеры.

Шаги

1. Нажмите **Device** → **Camera** («Устройство → Камера») для перехода на соответствующую страницу.
2. Нажмите **Enroll** («Зарегистрировать»), введите IP-адрес, имя пользователя и пароль для добавления камеры.



3. Нажмите для редактирования информации о камере.

Нажмите Edit, чтобы изменить информацию о камере, или нажмите Delete, чтобы удалить камеру.

5.3.3 Параметры области

Настройка основных параметров

Зоны можно привязать к выбранной области.

Шаги

1. Перейдите на вкладку **Area** → **Basic Settings** («Область → Настройка основных параметров») для перехода на соответствующую страницу.
2. Выберите область.
3. Нажмите **Enable** («Включить»).
4. Нажмите **Edit Linked Zone** («Редактировать связанную зону») и **Edit Linked Peripheral** («Редактировать связанное периферийное устройство»), чтобы проверить связанные зоны или периферийные устройства.
5. Нажмите **Save** («Сохранить»), чтобы завершить настройку.

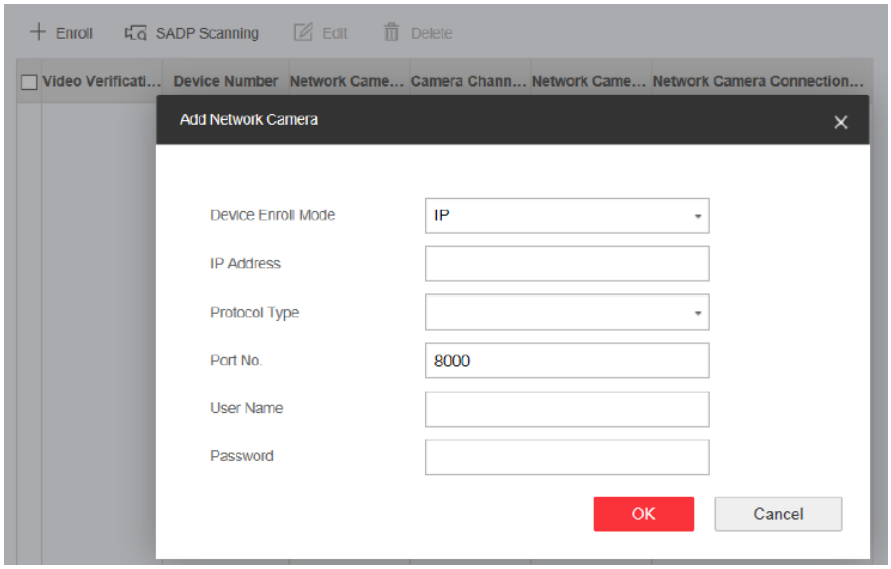
5.3.4 Управление видео

В охранную панель можно добавить 2 IP-камеры и связать камеру с выбранной зоной для видеонаблюдения. Получать и просматривать видео о событии можно через клиентское ПО и по электронной почте.

Добавление камер на охранную панель

Шаги

1. Нажмите **Device** → **Network Camera** («Устройство → IP-камера») для перехода на страницу управления камерой.



2. Нажмите **Enroll** («Зарегистрировать») и введите основную информацию о камере, в частности, IP-адрес и номер порта, и выберите тип протокола.
3. Введите имя пользователя и пароль камеры.

   Сканирование с помощью ПО SADP

   Сканируйте все IP-камеры в одной локальной сети. После сканирования отобразится список камер. Также можно вручную добавить камеры в список.
4. Нажмите **OK**.
5. Опционально. Нажмите **Edit** («Изменить») или **Delete** («Удалить»), чтобы изменить параметры или удалить выбранную камеру.

Привязка камеры к определенной зоне

Шаги

1. Перейдите на вкладку **Device** → **Zone** («Устройства → Зоны»).
2. Выберите зону, в которой необходимо включить видеонаблюдение, и нажмите ⚙.
3. Выберите **Link Camera** («Привязать камеру»).
4. Нажмите **OK**.

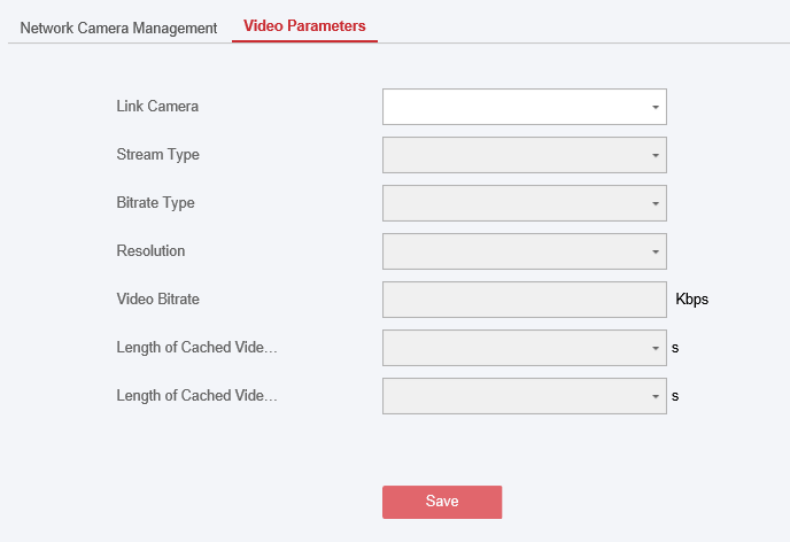
Примечание

Тревожное видео будет прикреплено к электронному письму только если зона связана с IP-камерой.

Настройка параметров видео

Шаги

1. Нажмите **Device → Network Camera → Video Parameters** («Устройство → IP-камера → Параметры видео») для перехода на соответствующую страницу.



2. Выберите камеру и настройте параметры видео.

Stream Type («Тип потока»)

Main Stream («Основной поток»): используется при записи и предварительном просмотре в формате HD, имеет высокое разрешение, скорость кодового потока и качество изображения.

Sub-Stream («Дополнительный поток»): используется для передачи по сети и предварительного просмотра изображений в виде потокового видео с возможностью более низкого разрешения, скорости передачи данных и качества изображения.

Bitrate Type («Тип битрейта»)

Выберите тип битрейта: **Constant** («Постоянный») или **Variable** («Переменный»).

Resolution («Разрешение»)

Выберите разрешение видеовыхода.

Video Bitrate («Битрейт видео»)

Чем выше значение, тем лучше качество видео, но требуется большая пропускная способность.

5.3.5 Управление разрешениями

Добавление / изменение / удаление брелока

При необходимости можно добавить брелок на панель. Это позволит управлять панелью с помощью брелока. Также можно редактировать информацию о брелоке или удалить брелок из охранной панели.

Шаги

1. Нажмите **Device** → **Keyfob** («Устройство → Брелок»), чтобы перейти на страницу управления брелоком.
2. Нажмите **Enroll** («Зарегистрировать») и нажмите любую клавишу на брелоке.
3. Настройте параметры брелока.

Name («Название»)

Задайте наименование для брелока.

Permission Settings («Настройки разрешений»)

Отметьте разные разрешения, чтобы назначить их для пользователей.

Single Key Settings («Настройки клавиши»)

Выберите клавиши из раскрывающегося списка, чтобы настроить функции клавиш I и II.

Combination Keys Settings («Настройки комбинированных клавиш»)

Выберите клавиши из раскрывающегося списка, чтобы настроить функции комбинированных клавиш.

4. Нажмите **OK**.
5. Опционально. Нажмите , чтобы изменить информацию о брелоке.
6. Опционально. Удалите один брелок или отметьте несколько брелоков и нажмите **Delete** («Удалить»), чтобы удалить брелоки в пакетном режиме.

Примечание

Связь беспроводных устройств, таких как брелок, обозначается серийным номером, который будет зашифрован во время передачи. Серийный номер начинается с символа от Q до Z, далее следуют 8 цифр, например, Q02235774. Максимальное число: 100000000 (10 в степени 8 [цифр]).

Добавление / изменение / удаление меток

Добавьте метку в охранную панель и используйте ее для постановки на охрану / снятия зоны с охраны. Также можно редактировать информацию о метке или удалить ее из панели.

Примечание

Связь между метками обозначается серийным номером, который будет зашифрован во время передачи. Серийный может содержать до 32 цифр. Максимальное число: 4, 294, 967, 296.

Шаги

1. Нажмите **Device** → **Tag** («Устройство → Метка»), чтобы перейти на страницу управления.
2. Нажмите **Enroll** («Зарегистрировать») и поместите метку в область меток панели.
3. Задайте наименование для метки во всплывающем окне.
4. Выберите тип метки и связанную область.
5. Выберите разрешения для метки.

Примечание

Необходимо предоставить как минимум 1 разрешение для метки.

6. Нажмите **OK**, информация о метке отобразится в списке.

Примечание

Метка поддерживает не менее 20 тысяч серийных номеров.

7. Опционально. Нажмите , чтобы изменить наименование метки.
8. Опционально. Удалите одну метку или отметьте несколько меток и нажмите **Delete** («Удалить»), чтобы удалить метки в пакетном режиме.

5.3.6 Обслуживание

Информация об устройстве

Здесь можно просмотреть наименование устройства и другую информацию.

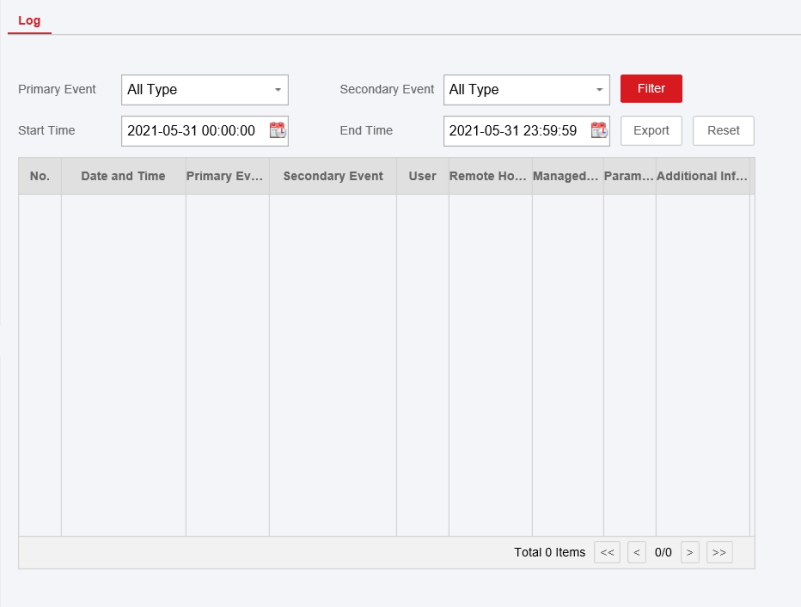
Перейдите на вкладку **Maintenance → Device Information** («Техническое обслуживание → Информация об устройстве»).
Здесь можно просмотреть модель, серийный номер, версию прошивки устройства, веб-версию или нажать **About → View Licenses** («Информация о программе → Просмотреть лицензии»), чтобы просмотреть лицензии на исходное ПО.

Перейдите в меню **System → System settings** («Система → Системные настройки»), чтобы изменить имя устройства.

Локальный поиск записей журнала

Здесь можно выполнить поиск журнала на устройстве.

Перейдите на вкладку **Maintenance→ Log** («Система → Поиск в локальном журнале»), чтобы перейти на соответствующую страницу.



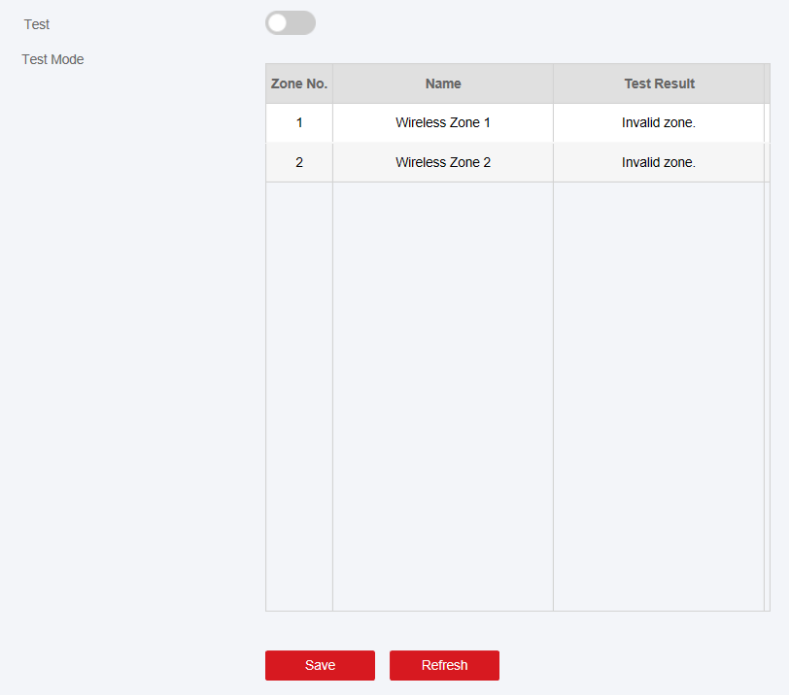
Выберите событие и второстепенный тип из раскрывающегося списка, настройте время начала и окончания записей журнала и нажмите **Filter** («Фильтровать»). Фильтрованная информация журнала будет отображаться в списке.
Нажмите **Reset** («Очистить»), чтобы сбросить все условия поиска.

Диагностика

Охранная панель поддерживает проведение полной диагностики.

Шаги

1. Перейдите в меню **Maintenance → Device Maintenance Test** («Техническое обслуживание → Обслуживание устройства → Диагностика»), чтобы включить функцию.



Примечание

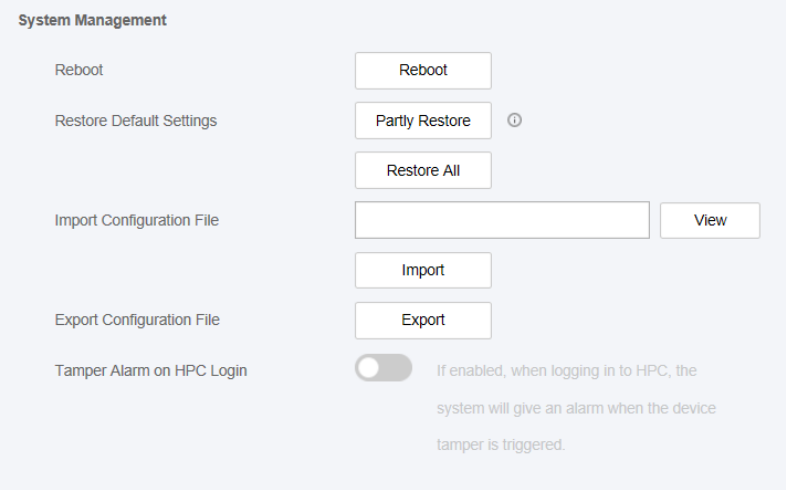
В режим диагностики можно перейти только когда все датчики работают исправно.

2. Поставьте галочку **Test** («Диагностика»), чтобы запустить диагностику.
3. Нажмите **Save** («Сохранить»), чтобы завершить настройку.
4. Включите датчики в каждой зоне.
5. После этого можно просмотреть результаты диагностики.

Обслуживание системы

Перезагрузите устройство, восстановите настройки по умолчанию, импортируйте / экспортируйте файл конфигурации или обновите устройство удаленно.

Выберите устройство и нажмите в клиентском ПО или введите IP-адрес устройства в адресной строке веб-браузера. Нажмите **Maintenance** → **Device Maintenance** → **Maintenance** («Система → Обслуживание системы»), чтобы перейти на страницу обновления и обслуживания системы.



Reboot («Перезагрузка устройства»)

Нажмите **Reboot** («Перезагрузка») для перезагрузки устройства.

Restore Default Settings («Восстановление настроек по умолчанию»)

Нажмите **Partly Restore** («Восстановить часть настроек по умолчанию») и устройство вернется к настройкам по умолчанию, за исключением параметров администратора, параметров проводной сети, параметров Wi-Fi, параметров датчиков и параметров беспроводного устройства.

Нажмите **Restore All** («Восстановить настройки по умолчанию») для сброса всех параметров до значений по умолчанию.

Import Configuration File («Импорт файла конфигурации»)

Нажмите **View** («Просмотреть»), чтобы выбрать файл конфигурации на ПК, и нажмите **Import Configuration File** («Импортировать файл конфигурации»), чтобы импортировать параметры конфигурации на устройство. Для импорта файла конфигурации необходимо ввести пароль, настроенный во время экспорта.

Export Configuration File («Экспорт файла конфигурации»)

Нажмите **Export Configuration File** («Экспортировать файл конфигурации»), чтобы экспортировать параметры конфигурации устройства на ПК. Для экспорта файла конфигурации требуется пароль, который будет использоваться для шифрования файла.

Tamper Alarm on HPC Login («Тревога несанкционированного доступа при входе в систему HPC»)

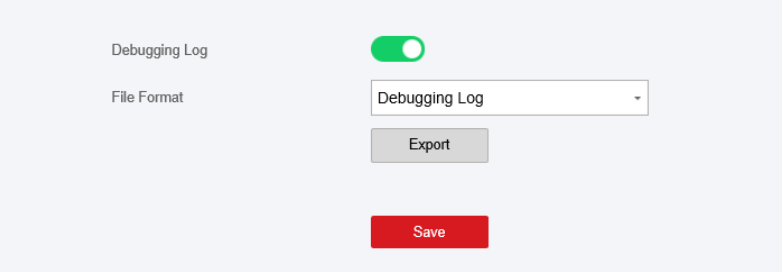
После включения этой функции при входе в систему с учетной записи установщика срабатывает тревога открытия крышки устройства (тревога тампера). (По умолчанию тревога открытия крышки устройства (тревога тампера) не будет срабатывать при входе в систему с учетной записи установщика.)

Экспорт файла

Файл отладки можно экспортировать на ПК.

Шаги

1. Перейдите на вкладку **Maintenance → Device Maintenance → Export File** («Техническое обслуживание → Обслуживание устройства → Экспортировать файл»).



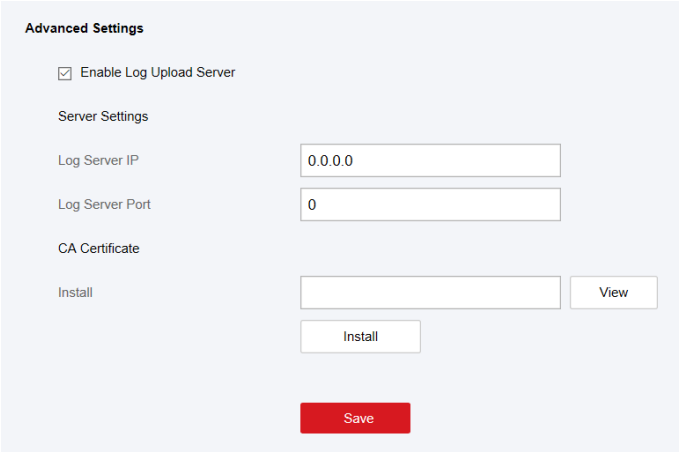
2. Сдвиньте ползунок для включения функции.
3. Нажмите **Export** («Экспортировать»), чтобы сохранить файл отладки на ПК.

Журнал проверки безопасности

Можно добавить сервер проверки безопасности в систему. Устройство будет загружать веб-журналы на сервер.

Шаги

2. Нажмите **System Maintenance → Device Maintenance → Security Audit Log** («Обслуживание системы → Обслуживание устройства → Журнал проверки безопасности»), чтобы перейти на соответствующую вкладку.



3. Установите галочку в поле **Enable Log Upload Server** («Включить сервер загрузки журналов»).
4. Введите **Server IP address** («IP-адрес сервера») и **Server Port** («Порт сервера»).
5. Нажмите **View** («Просмотреть»), чтобы выбрать сертификат.

Примечание

Допускаются такие форматы, как ca.crt, ca-chan.crt, private.txt.

6. Нажмите **Install** («Установить»).
7. Нажмите **Save** («Сохранить»).

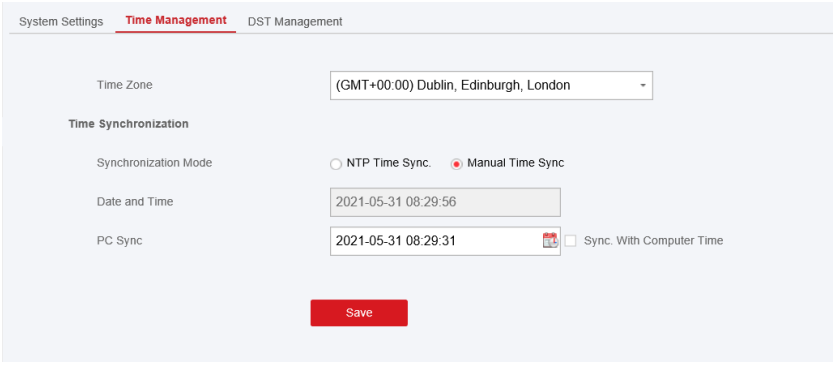
5.3.7 Параметры системы

Настройки времени

Настройте часовой пояс для синхронизации времени устройства и параметры перехода на летнее время. Устройство поддерживает синхронизацию времени через сервер Hik-Connect Guarding Vision.

Управление временем

Нажмите **System → System Settings → Time Management** («Система → Параметры системы → Управление временем»), чтобы перейти на соответствующую страницу.



Выберите часовой пояс из выпадающего списка.

Можно синхронизировать время устройства вручную с помощью NTP-сервера. Установите флажок **NTP Time Sync.** («Синхронизация времени с NTP-сервером»), введите адрес сервера и номер порта, затем настройте интервал синхронизации.

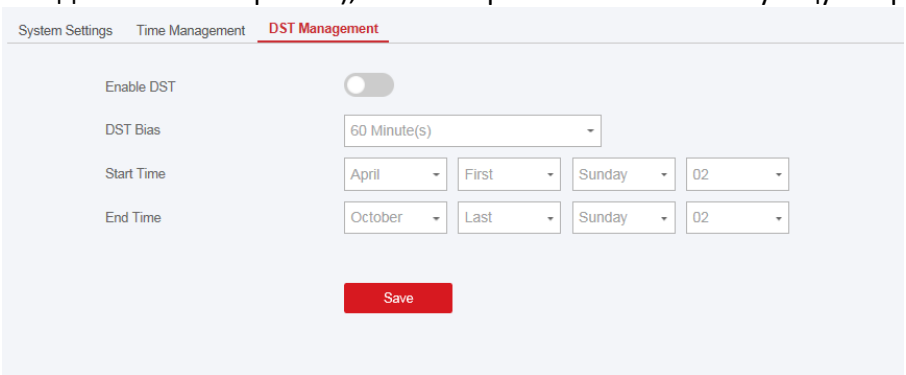
Можно синхронизировать время устройства вручную. Также можно нажать **Sync. with Computer Time** («Синхронизировать со временем ПК»), чтобы синхронизировать время устройства со временем компьютера.

Примечание

При синхронизации времени вручную или при синхронизации со временем ПК система записывает журнал **SDK Synchronization** («Синхронизация SDK»).

Настройки перехода на летнее время

Нажмите **System → System Settings → DST Management** («Система → Параметры системы → Настройки перехода на летнее время»), чтобы перейти на соответствующую страницу.

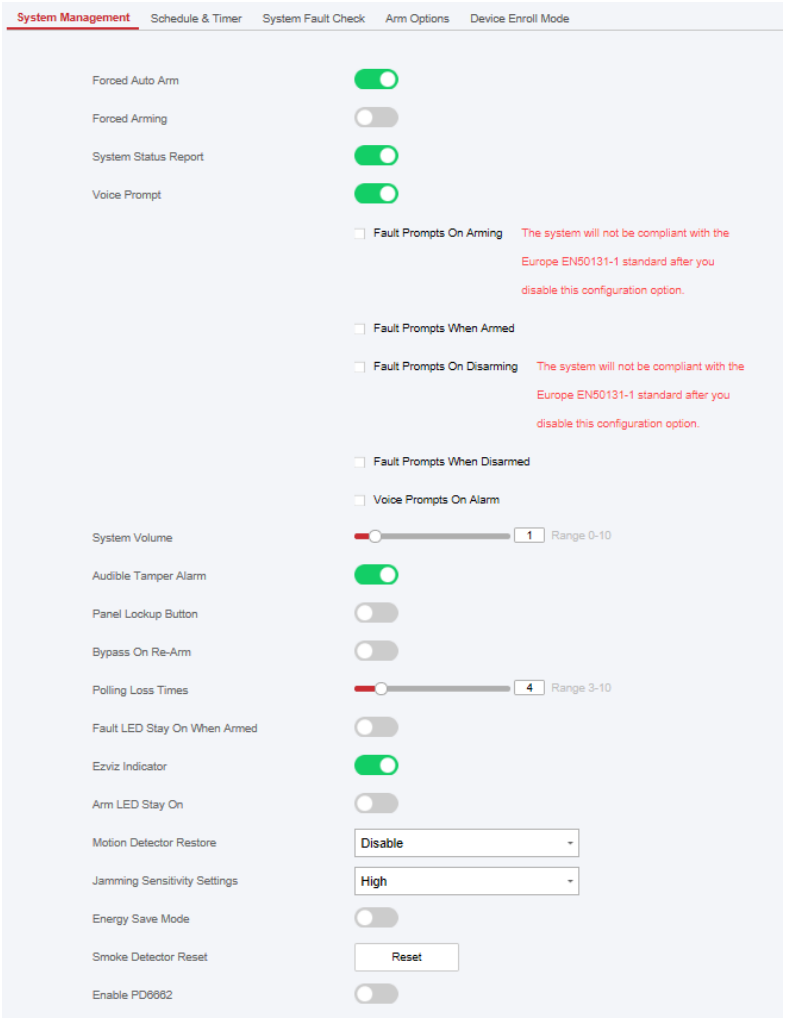


Настройте время начала и окончания DST, а также **DST Bias** («Погрешность DST»).

Управление разрешениями

Настройте параметры разрешений.

Нажмите **System** → **System Options** → **System Management** («Система → Параметры системы → Управление системой»), чтобы перейти на соответствующую страницу.



Forced Auto Arm («Принудительная автоматическая постановка на охрану»)

Если опция включена и в зоне присутствуют активные неисправности, зона будет исключена автоматически при постановке на охрану.

Примечание

Необходимо отключить функцию постановки на охрану на странице дополнительных настроек. При наличии неисправности постановка панели на охрану не будет выполнена.

Forced Arming («Принудительная постановка на охрану»)

Если опция включена и в зоне присутствуют активные неисправности, зона будет исключена при постановке на охрану.

System Status Report («Отчет о состоянии системы»)

Если опция включена, устройство автоматически загрузит отчет при изменении статуса панели.

Voice Prompt («Голосовое предупреждение»)

Если опция включена, панель включит текстовое голосовое предупреждение. **System Volume («Громкость системы»)**

Доступный диапазон громкости системы: от 0до 10

Audible Tamper Alarm («Тревога тампера»)

Если опция включена, при тревоге саботажа будет срабатывать бипер.

Panel Lockup Button («Кнопка блокировки панели»)

Включение / отключение кнопки блокировки панели управления.

Bypass on Re-Arm («Обход зоны при повторной постановке на охрану»)

Если функция включена, зона с неисправностью будет автоматически исключена при повторной постановке на охрану.

Polling Loss Times («Интервал опроса»)

Настройте максимальную продолжительность интервала опроса. Система сообщит о неисправности, если продолжительность превышает установленное значение.

Fault LED Stay On When Armed («LED-индикатор неисправности остается включенным при постановке на охрану»)

Когда система поставлена на охрану, индикатор неисправности горит непрерывно.

Ezviz Indicator («Индикатор EZVIZ»)

Включите индикатор EZVIZ.

Arm LED Stay On («LED-индикатор постановки на охрану остается включенным»)

LED-индикатор постановки на охрану горит непрерывно.

Motion Detector Restore («Восстановление датчиков движения»)

К датчикам движения относятся все ИК-датчики.

Jamming Sensitivity Settings («Настройки чувствительности к помехам»)

Устройство обнаружит радиочастотные помехи и отправит push-сообщения, когда создаются помехи для радиосигналов. Настройте чувствительность обнаружения.

Energy Save Mode («Режим энергосбережения»)

Если режим энергосбережения включен и отключен основной источник питания, Wi-Fi переходит на низкое энергопотребление, отключается 4G, не выполняется считывание метки, не горит LED-индикатор, отключены голосовые подсказки.

Enable PD6662 («Включение PD6662»)

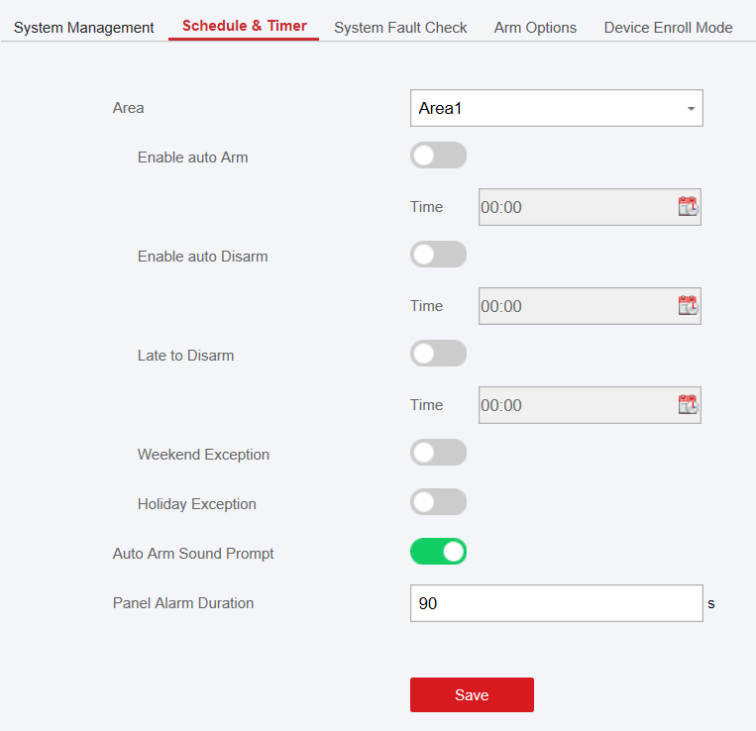
Включите стандарт PD6662. Несоответствующие стандарту функции не будут работать.

Расписание тревог и настройки таймера

При необходимости можно настроить расписание тревог. Зона будет поставлена / снята с охраны в соответствии с настроенным расписанием.

Шаги

1. Нажмите **System**→ **System Options** → **Schedule & Timer** («Система → Параметры системы → Расписание и таймер»), чтобы перейти на соответствующую страницу.



2. Выберите область.
3. Задайте необходимые параметры.

Auto Arm («Автоматическая постановка на охрану»)

Включите функцию и задайте время начала постановки на охрану. Зона будет поставлена на охрану в установленное время.

Примечание

- Время автоматической постановки на охрану и время автоматического снятия с охраны не могут совпадать.
- Бипер издает длительный звуковой сигнал за 2 минуты до запуска автоматической постановки на охрану и короткий звуковой сигнал за 1 минуту до автоматической постановки на охрану.
- Также можно включить принудительную постановку на охрану на странице **System Options** («Параметры системы»). Когда функция включена, система будет поставлена на охрану даже при наличии неисправности.

Auto Disarm («Автоматическое снятие с охраны»)

Включите функцию и настройте время начала снятия с охраны. Зона будет снята с охраны в установленное время.

Примечание

- Время автоматической постановки на охрану и время автоматического снятия с охраны не могут совпадать.

Late to Disarm («Задержка снятия с охраны»)

Включите функцию и настройте время. При срабатывании тревоги по истечении заданного времени, сотрудник / посетитель будет считаться опоздавшим.

Примечание

Активируйте функцию уведомления с помощью панели в меню **Communication Parameters** → **Event Communication** («Параметры связи → Связь по событию») перед активацией функции **Late to Disarm** («Задержка снятия с охраны»).

Weekend Exception («Исключение выходных дней»)

Если функция включена, зона не будет поставлена на охрану в выходные дни.

Holiday Exception («Исключения в праздничные дни»)

Если функция включена, режимы постановки и снятия с охраны не будут активны в праздничные дни. После включения необходимо настроить расписание выходных дней.

Примечание

Можно настроить до 6 групп праздничных дней.

Auto Arm Sound Prompt («Звуковое предупреждение автоматической постановки на охрану»)

После отключения бипер не будет подавать звуковой сигнал перед автоматической постановкой на охрану.

Panel Alarm Duration («Длительность тревоги»)

Длительность тревоги на охранной панели.

Примечание

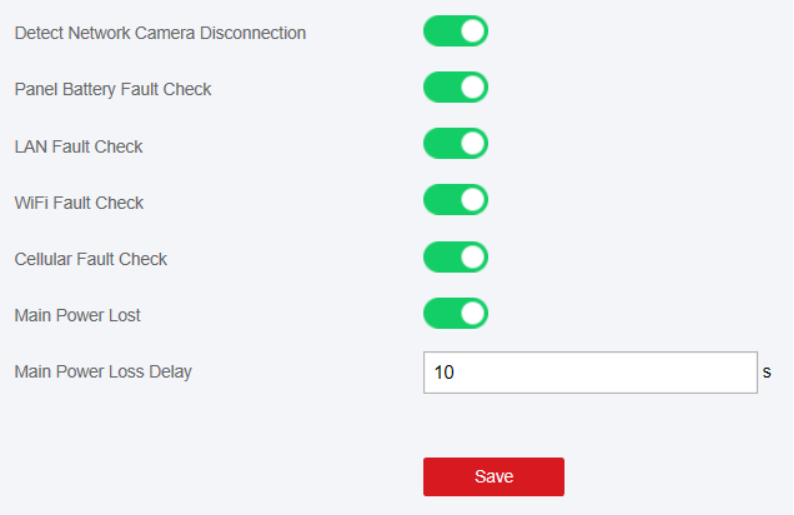
Доступный диапазон длительности тревоги: от 10 до 900 с.

5. Нажмите **Save** («Сохранить»).

Fault Check («Проверка неисправности»)

Система определяет, следует или не следует производить диагностику неисправностей, перечисленных на странице. Система будет диагностировать только выбранную неисправность.

Перейдите на вкладку **System → System Options → System Fault Check** («Система → Параметры системы → Проверка неисправности»).



Detect Network Camera Disconnection («Обнаружение отключения IP-камеры»)

Если опция включена, сработает тревожный сигнал при отключении IP-камеры.

Panel Battery Fault Check («Проверка неисправности батареи»)

Если опция включена, устройство будет загружать события, когда батарея отключена или разряжена.

LAN Fault Check («Проверка неисправности LAN»)

Если опция включена, сработает тревожный сигнал при разрыве или сбоях проводной сети.

Wi-Fi Fault Check («Проверка неисправности Wi-Fi»)

Если опция включена, сработает тревожный сигнал при разрыве или сбоях подключения Wi-Fi.

Cellular Network Fault Check («Проверка неисправности сотовой сети»)

Если опция включена, сработает тревожный сигнал при разрыве или сбоях сотовой сети.

Main Power Lost («Тревога потери питания»)

Если опция включена, тревога сработает при отключении IP-камеры.

Main Power Loss Delay («Потеря основного питания»)

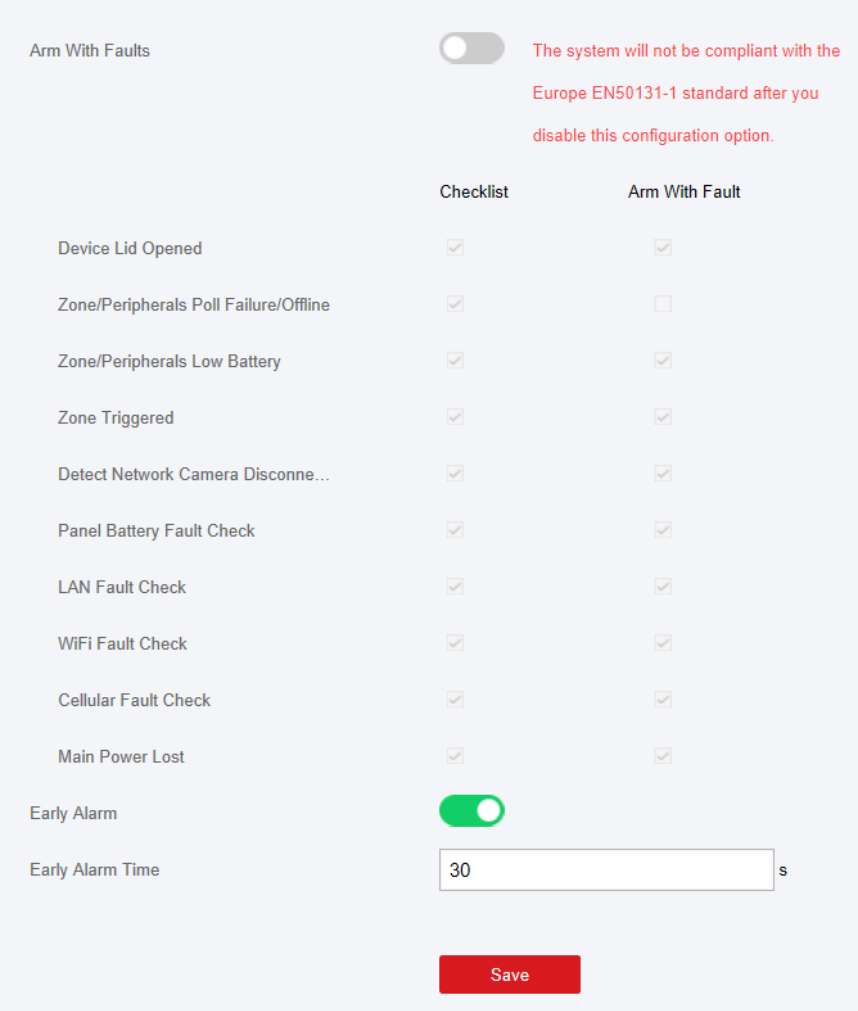
Система проводит проверку неисправности по истечении заданного времени после отключения питания переменного тока.

В соответствии со стандартом EN 50131-3 продолжительность проверки должна составлять 10 с.

Параметры постановки на охрану

Настройте расширенные параметры доступа.

Нажмите **System → System Options → Arm Options** («Система → Параметры системы → Параметры постановки на охрану»), чтобы перейти на соответствующую страницу.



Также можно настроить следующие параметры:

Arm with Faults («Постановка на охрану с условием подтверждения неисправностей»)

Отметьте неисправности в списке **Enable Arming with Fault list** («Включить постановку на охрану при обнаружении неисправности»), и устройство не остановит процедуру постановки на охрану при обнаружении неисправности.

Fault Checklist («Контрольный список неисправностей»)

Система проверит наличие неисправностей в контрольном списке устройства во время процедуры постановки на охрану.

Early Alarm («Тревога по истечении времени задержки»)

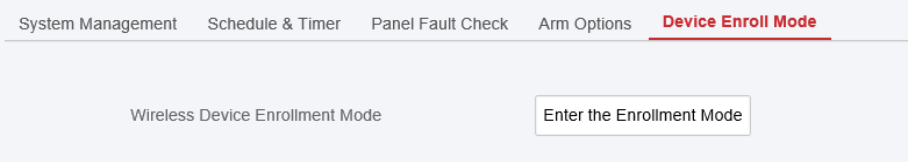
Если функция включена и зона поставлена на охрану, при возникновении тревожного события, тревога сработает по истечении времени задержки.

Примечание

Данная тревога сработает только после срабатывания зоны с задержкой.

Режим регистрации устройства

Нажмите **Enter the Enrollment Mode** («Войти в режим регистрации»), чтобы панель перешла в режим регистрации.

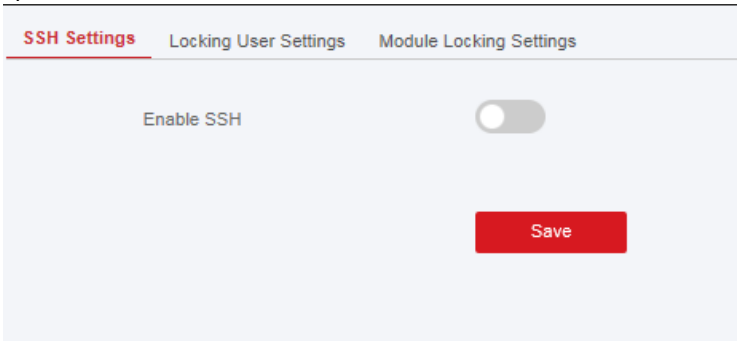


Настройки безопасности

Настройка параметров SSH

Включите или отключите протокол SSH по мере необходимости.

Нажмите **System → System Security → SSH Settings** («Система → Параметры безопасности → Параметры SSH»), чтобы перейти на страницу настроек SSH. Здесь можно включить или отключить функцию SSH.



Параметры блокировки

Устройство будет заблокировано в течение 90 секунд после 3 неудачных попыток ввода учетных данных (время можно настроить в поле **Retry Time before Auto-Lock** («Интервал для повторной попытки перед автоматической блокировкой»)) через минуту.

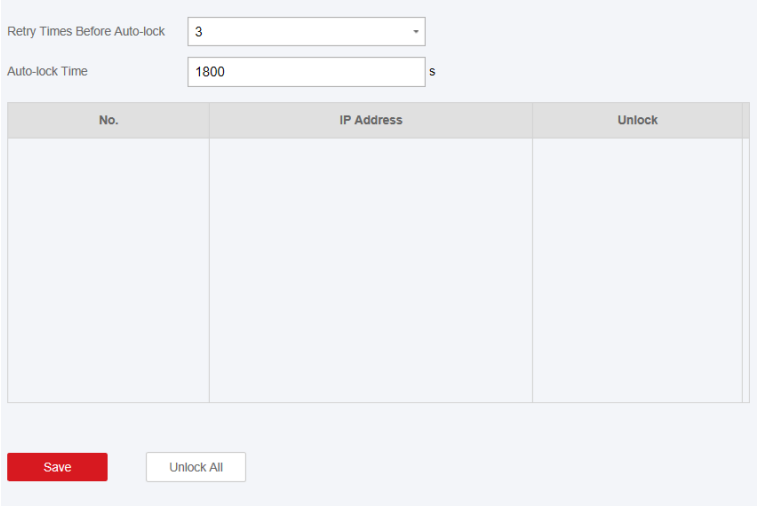
Здесь можно просмотреть заблокированного пользователя или разблокировать пользователя и настроить длительность блокировки пользователя.

Примечание

Для соответствия EN, система будет непрерывно записывать один и тот же журнал только 3 раза.

Шаги

1. Перейдите на вкладку **System → System Security → User Lockout Attempts** («Система → Безопасность системы → Параметры блокировки»), чтобы перейти на страницу настроек блокировки пользователя.



2. Настройте следующие параметры.

Retry Time before Auto-Lock («Интервал для повторной попытки перед автоматической блокировкой»)

Если пользователь последовательно вводит неверный пароль более указанного времени, учетная запись будет заблокирована.

Примечание

Администратор имеет на две попытки больше, по сравнению с настроенным значением.

Auto-lock Time («Интервал перед автоматической блокировкой»)

Настройте длительность блокировки учетной записи.

Примечание

Доступная длительность блокировки составляет: от 5 до 1800 с.

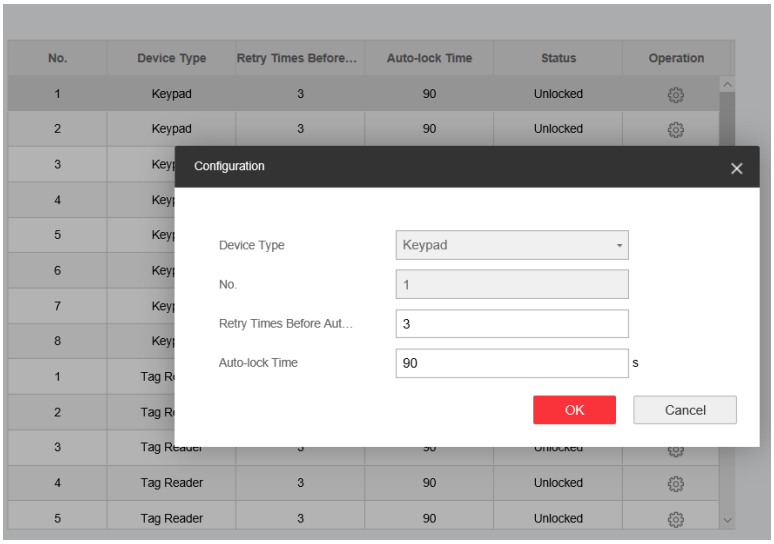
3. Нажмите , чтобы разблокировать учетную запись, или нажмите **Unlock All** («Разблокировать все»), чтобы разблокировать всех заблокированных пользователей в списке.
4. Нажмите **Save** («Сохранить»).

Настройки блокировки модуля

Настройте параметры блокировки модуля, включая максимальное количество попыток ввода учетных данных и длительность блокировки. Модуль будет заблокирован на заданный период времени при неудачной аутентификации модуля за указанное количество попыток.

Шаги

1. Перейдите на вкладку **System** → **System Security** → **Module Locking Settings** («Система → Безопасность системы → Параметры блокировки модуля»), чтобы перейти на страницу настроек блокировки модуля.



2. Выберите модуль из списка и нажмите .
3. Настройте следующие параметры:

   Retry Time before Auto-Lock («Интервал для повторной попытки перед автоматической блокировкой»)

   При превышении заданного количества неудачных попыток, клавиатура будет заблокирована на настроенное время.

   Auto-lock Time («Интервал перед автоматической блокировкой»))

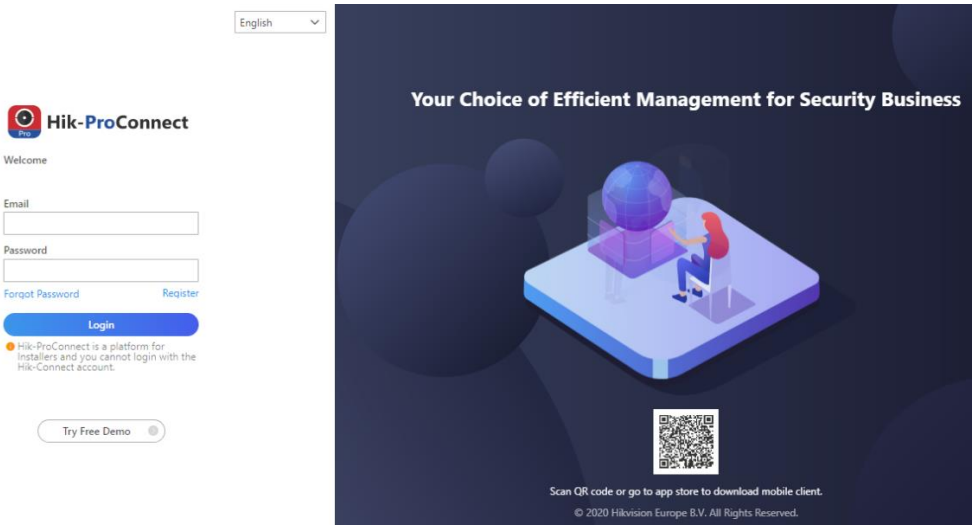
   Настройте длительность блокировки клавиатуры. По истечении заданного времени клавиатура будет разблокирована.
4. Нажмите **OK**.
5. Опционально. Нажмите **Lock** («Блокировка»), чтобы разблокировать заблокированный модуль.

Обновление устройства

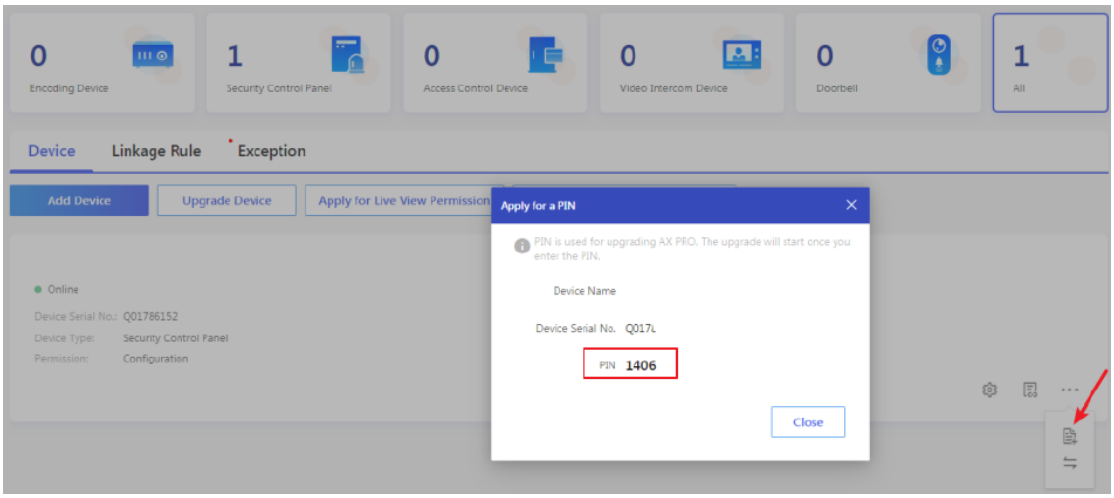
Получение PIN-кода производителя

Чтобы обновить устройство, для аутентификации необходим PIN-код производителя. PIN-код производителя можно получить только через службу Hik-ProConnect, что означает, что установщик, авторизованный администратором на уровне доступа 2, получил разрешение на доступ уровня 4. PIN-код производителя можно использовать только один раз.

- **Получение PIN-кода от службы Hik-ProConnect**



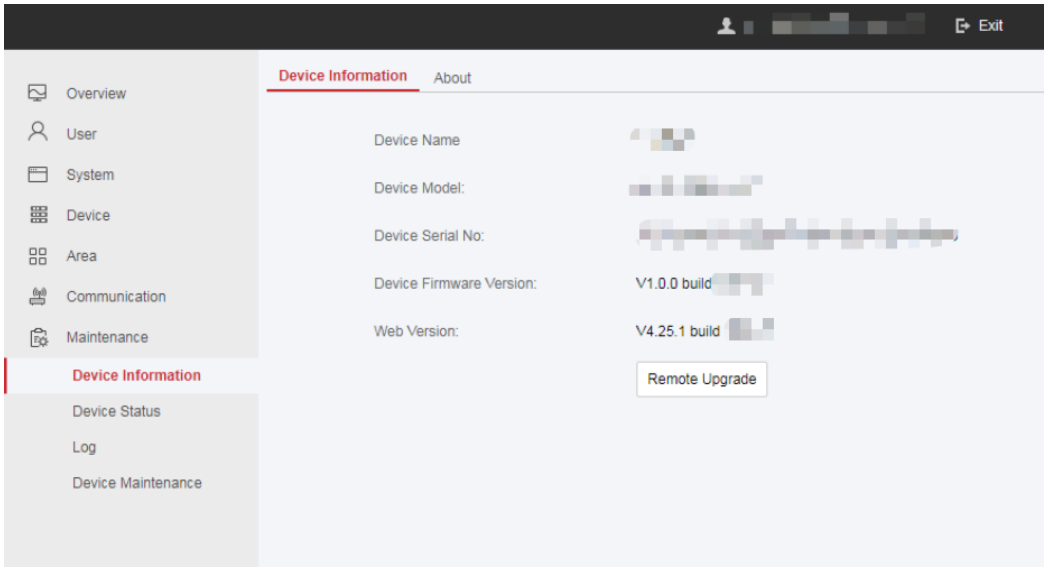
Войдите в систему с учетной записью установщика и перейдите на страницу устройства, которое необходимо обновить. Нажмите **More Menu** («Дополнительное меню») в правом нижнем углу страницы и примените PIN-код.



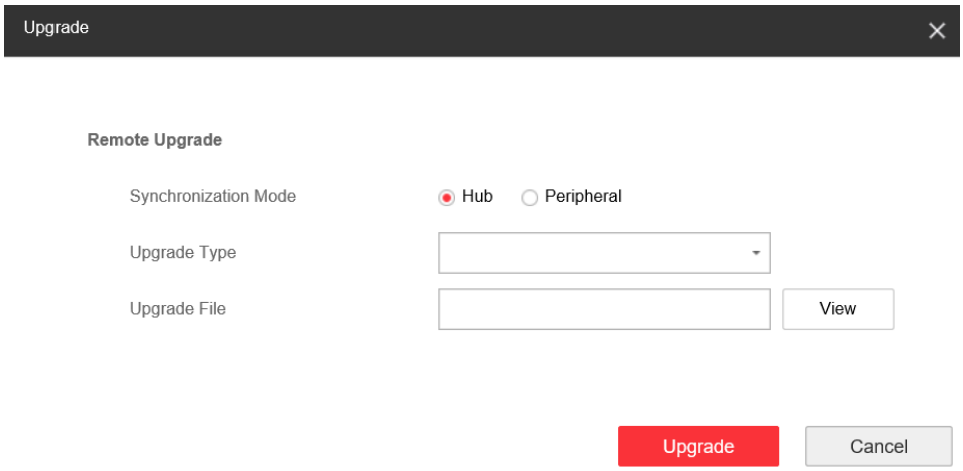
Обновление прошивки

Шаги

1. Перейдите на вкладку **Maintenance** → **Device Information** («Техническое обслуживание → Информация об устройстве»).
2. Нажмите **Remote Upgrade** («Удаленное обновление»).



3. Выберите хаб или периферийное устройство для обновления и выберите тип обновления.
4. Нажмите **View** («Просмотреть»), чтобы найти файл прошивки с именем digicap.dav.
5. Для завершения нажмите **Upgrade** («Обновить»).

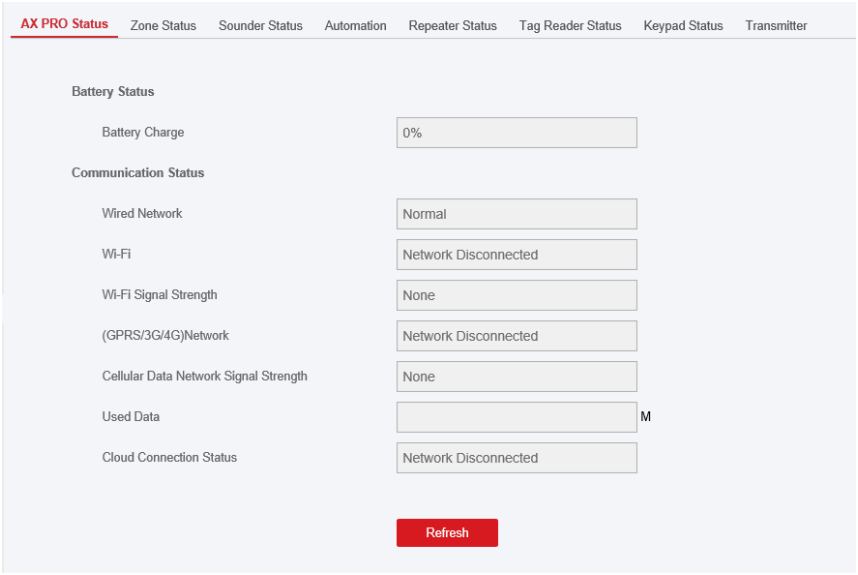


Примечание

И пользователи, и информация о конфигурации будут сохранены после завершения обновления.

5.3.8 Проверка статуса

Проверка статуса доступна после настройки зоны, ретранслятора и других параметров. Перейдите на вкладку **Maintenance** → **Device Status** («Обслуживание → Состояние устройства»). Здесь можно просмотреть состояние охранной панели, зоны, оповещателя, ретранслятора, клавиатуры, считывателя тегов, брелока и передатчика.



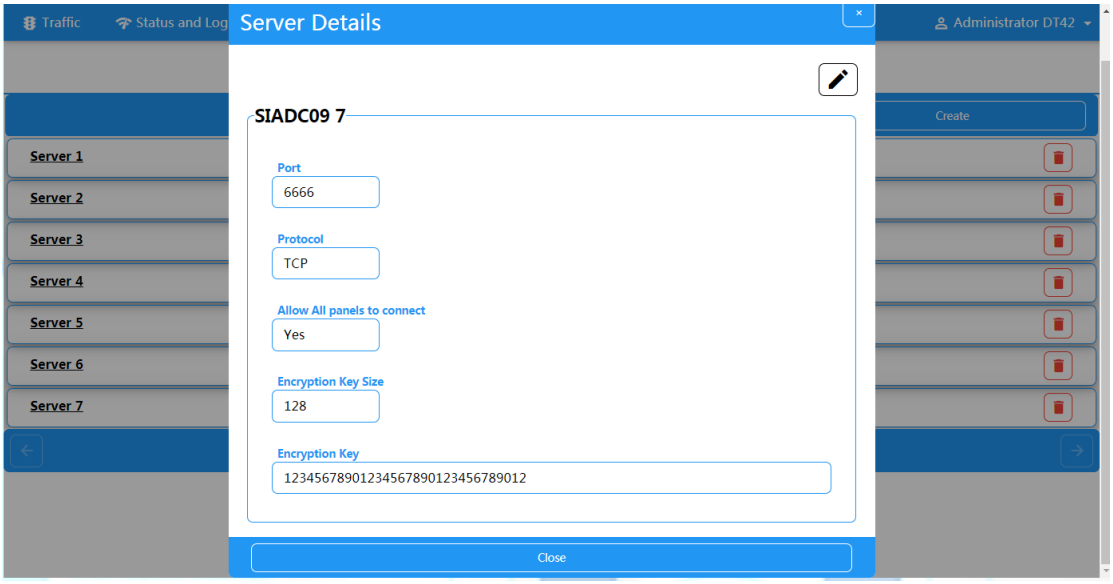
5.4 Уведомление в ЧОП / ПЦН

Беспроводная панель управления разработана со встроенным приемопередатчиком в соответствии с рекомендациями EN 50131-10 и EN 50136-2. Категория DP2 имеет первичный сетевой интерфейс LAN / Wi-Fi и вторичный сетевой интерфейс GPRS или 3G / 4G LTE. По мере доступности, ATS всегда использует сетевой интерфейс LAN / Wi-Fi, для экономии использования мобильных данных. Вторичный сетевой интерфейс обеспечивает отказоустойчивость и надежность при сбоях в электросети.

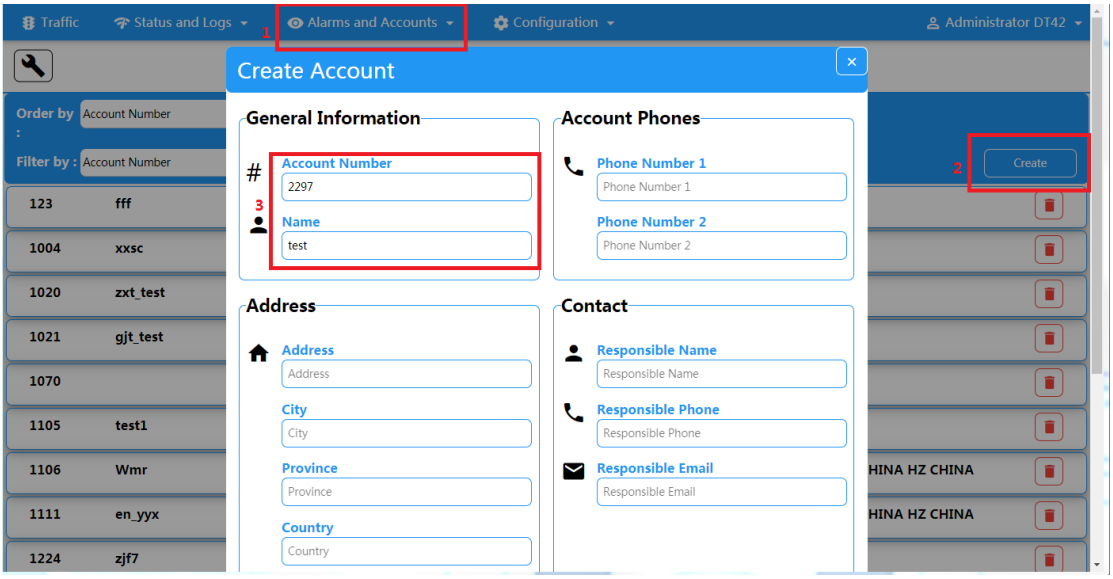
5.4.1 Настройка ATS приемопередатчика ЧОП / ПЦН

Шаги

1. Войдите в веб-клиент ЧОП / ПЦН.
2. Перейдите на вкладку **Configuration→ IP Reception** («Настройка параметров → Прием IP-адресов») и создайте принимающий сервер, как показано ниже.



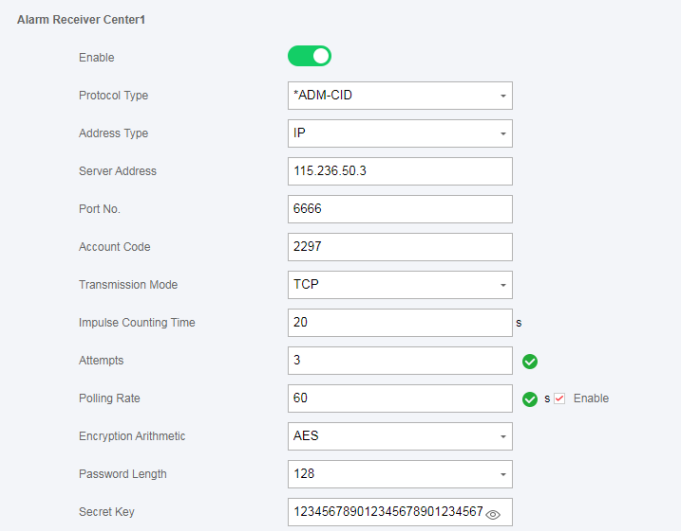
3. Нажмите **Alarms and Accounts** → **Accounts Management** («Тревоги и учетные записи → Управление учетными записями») и назначьте учетную запись для панели, как показано ниже.



5.4.2 Настройка ATS приемопередатчика панели

Шаги

1. Войдите в систему, используя учетную запись установщика из локального веб-клиента.
2. Перейдите на вкладку **Communication**→ **Alarm Receiving Center (ARC)** («Связь → ЧОП / ПЦН») и включите ЧОП / ПЦН.



- **= Настройки протокола =**

Тип протокола

— ADM-CID
— SIA-DCS
— *ADM-CID
— *SIA-DCS

Выберите токен, поддерживаемый получателем в ЧОП / ПЦН. Выберите токен со знаком «*», чтобы повысить безопасность связи.

- **= Настройка параметров сервера =**

■ ***Тип адреса***

— IP-адрес
— Доменное имя

■ ***Адрес сервера / доменное имя***

■ ***№ порта***

Введите IP-адрес или доменное имя, по которому можно связаться с приемопередатчиком ЧОП / ПЦН. Введите номер порта сервера, предоставленного ЧОП / ПЦН.

- **= Настройка параметров учетной записи =**

■ ***Код учетной записи***

Введите назначенную учетную запись, предоставленную ЧОП / ПЦН.

- **= Настройка параметров протокола SIA DC-09 =**

■ ***Режимы передачи***

— TCP
— UDP

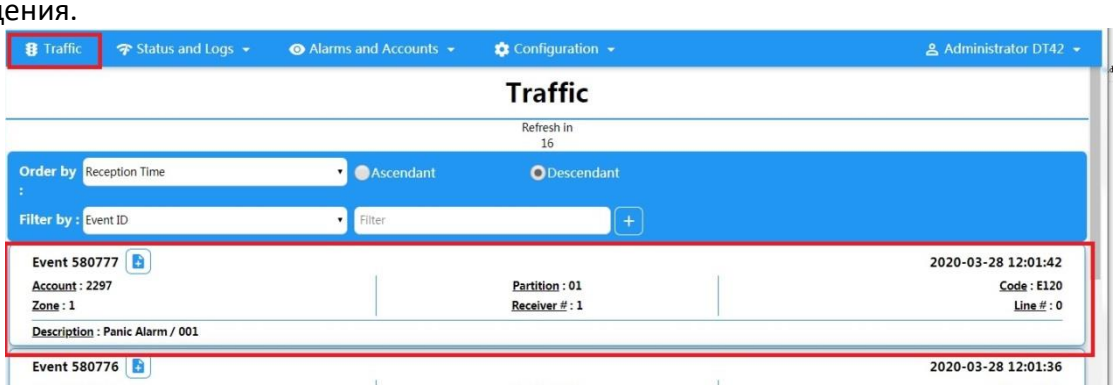
Для передачи данных поддерживаются протоколы TCP и UDP. Протокол UDP рекомендуется стандартом SIA DC-09.

- ***Настройка подключения***
  - ***Время подсчета импульсов / период ожидания повторной попытки***
    Настройте время ожидания ответа получателя. Повторная передача будет выполнена при истечении установленного периода для приемопередатчика.
  - ***Попытки***
    Настройте максимальное количество попыток повторной передачи.
  - ***Частота опроса***
    Настройте интервал между двумя опросами в реальном времени, поставить галочку **Enable** («Включить»).

- ***Настройки шифрования***
  - ***Алгоритмы шифрования***
    — — AES
  - ***Длина пароля***
    — 128
    — 192
    — 256
  - ***Секретный ключ***
    Настройте длину ключа шифрования и введите ключ, предоставленный ЧОП / ПЦН.

5.4.3 Тестирование сигнализации

Активируйте тревогу экстренного видео с панели управления.
Войдите в приемник. Нажмите **Traffic** («Трафик»), чтобы просмотреть все полученные сообщения.



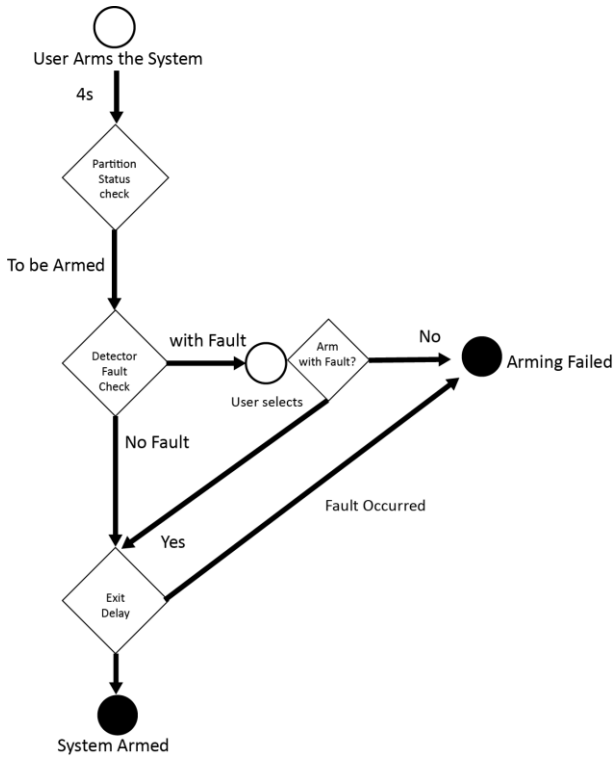
Раздел 6 Общие операции

6.1 Постановка на охрану

Для постановки системы на охрану можно использовать клавиатуру, брелок, метку, клиентское ПО, мобильный клиент.

После того, как команда постановки на охрану будет отправлена в панель, система проверит состояние извещателя. Если извещатель неисправен, при необходимости систему можно поставить на охрану с учетом неисправности.

Когда система поставлена на охрану, панель через 5 секунд запросит результат и загрузит отчет о постановке на охрану.



Access level of Arming («Уровень доступа при постановке на охрану»)

Пользователь уровня доступа 2 или 3 имеет разрешения на постановку системы на охрану или частичную постановку на охрану.

Arming Indication («Индикация постановки на охрану»)

Индикатор постановки / снятия с охраны горит синим в течение 5 секунд.

Reason of Arming Failure («Причина сбоя постановки на охрану»)

- Срабатывание охранного датчика (кроме датчика на выходе)
- Срабатывание тревоги экстренного вызова
- Тревога саботажа
- Исключение связи
- Исключение основного источника питания
- Исключение резервной батареи
- Ошибка получения тревоги

- Ошибка звукового оповещателя
- Низкий заряд батареи брелока
- Другое

Постановка на охрану с условием подтверждения неисправностей

Когда постановка на охрану остановлена по ошибке, пользователь уровня доступа 2 имеет право поставить систему на охрану с условием подтверждения неисправностей (принудительная постановка на охрану).

Принудительная постановка на охрану действует только на текущую операцию постановки на охрану.

Операция принудительной постановки на охрану будет записана в журнале событий.

6.2 Снятие с охраны

Снять систему с охраны можно с помощью клавиатуры, брелока, тега, клиентского ПО или мобильного клиента.

Disarming Indication («Индикатор снятия с охраны»)

Индикатор постановки / снятия с охраны мигает 30 с, в то время как пользователь успешно снимает систему с охраны на пути входа / выхода.

После завершения операции система выдаст результат снятия с охраны.

Entry Delay Duration («Продолжительность задержки на вход»)

В соответствии со стандартом EN50131-1, таймер не должен превышать 45 секунд.

Early Alarm («Тревога по истечении времени задержки»)

Если срабатывает тревога вторжения или несанкционированного доступа на пути входа / выхода, когда AX Hybrid PRO находится в состоянии задержки на вход, охранная панель переходит в режим предварительной тревоги.

Также можно настроить продолжительность ранней тревоги (> 30 с).

Охранная панель выдаст тревогу только в том случае, если тревожное событие длится дольше совокупного времени предварительной тревоги и задержки на вход.

6.3 Управление SMS

Управлять системой безопасности можно с помощью SMS, команда показана ниже.

Формат SMS для постановки на охрану / снятия с охраны / отключения тревожных уведомлений:

{Команда} + {Тип операции} + {Цель}

Команда: 2 цифры, 00 снятие с охраны, 01 полная охрана, 02 - частичная охрана,

03 - отключение тревоги

Тип операции: 1- операции области

Цель: Не более 3-х цифр, 0 операция для всех областей, 1 - операция для области 1 (зона 1), остальное можно вывести по аналогии.

A. Поиск неисправностей

A.1 Сбой связи

A.1.1 Конфликт IP-адресов

Описание неисправности:

IP-адрес, автоматически полученный или установленный панелью, совпадает с IP-адресом других устройств. Это вызывает конфликт IP-адресов.

Решение:

Поиск текущего доступного IP-адреса через ping. Измените IP-адрес и снова войдите в систему.

A.1.2 Веб-страница недоступна

Описание неисправности:

Используйте браузер для доступа к веб-страницам.

Решения

1. Проверьте соединение сетевого кабеля и работу сети панели.
2. Порт панели был изменен. Добавьте порт к веб-адресу для дальнейшего доступа.

A.1.3 Hik-Connect не в сети

Описание неисправности:

Веб-страница показывает, что сетевое подключение к Hik-Connect недоступно.

Решение:

Ошибка конфигурации сети панели, невозможно получить доступ к сети Интернет.

A.1.4 Частое отключение IP-камеры

Описание неисправности:

Система сообщает о нескольких записях событий отключения и подключении IP-камеры.

Решение:

Проверьте сетевое соединение или работу камеры в режиме реального времени.

A.1.5 Ошибка добавления устройства в приложение

Описание неисправности:

При добавлении устройств с использованием APP появляется сообщение о невозможности добавления / поиска устройства и т. д.

Решение:

Проверьте веб-страницу: присутствует ли сетевое соединение службы Hik-Connect.

A.1.6 Информация о тревоге не передается в приложение / iVMS-4200 / ЧОП / ПЦН

Описание неисправности:

Приложение / iVMS-4200 / ЧОП / ПЦН не получает тревожное сообщение после срабатывания тревоги.

Решение:

Сообщение: «уведомления о тревоге и взломе» отключены. Необходимо включить «уведомления о тревоге и взломе».

A.2 Взаимоисключаемые функции

A.2.1 Невозможно войти в режим регистрации

Описание неисправности:
Нажмите функциональную клавишу панели, клавиша подсказки недействительна.
Решение:
Панель находится в режиме **Hotspot** («Точка доступа»). Переведите панель в режим **Station** («Станция»), затем попробуйте снова войти в режим регистрации.

A.3 Ошибки зоны

A.3.1 Отсутствует подключение к зоне

Описание неисправности:
Просмотрите состояния зон, подключение к которым отсутствует.
Решение:
Проверьте, нет ли сообщения о низком заряде батареи извещателя. Замените батарею извещателя.

A.3.2 Зона с контролем вскрытия

Описание неисправности:
Просмотрите состояния зон с контролем вскрытия.
Решение:
Удерживайте кнопку контроля вскрытия извещателя.

A.3.3 Срабатывание тревоги в зоне / неисправность

Описание неисправности:
Просмотрите состояния зон, в которых сработала тревога / обнаружена неисправность.
Решение:
Перезапустите извещатель.

A.4 Проблемы при постановке на охрану

A.4.1 Сбой постановки на охрану (когда процесс постановки на охрану не запускается)

Описание неисправности:
Постановка на охрану не выполняется.
Решение:
Функция **Forced Arming** («Принудительная постановка на охрану») не запускается автоматически, и при возникновении неисправности в зоне постановка на охрану не будет выполнена. Включите принудительную постановку на охрану или верните зону в нормальное состояние.

A.5 Сбой операции

A.5.1 Не удается войти в тестовый режим

Описание неисправности:
Не удается включить тестовый режим, выводится сообщение: **A fault in the zone** («Неисправность в зоне»).

Решение:
Проверьте наличие неисправности: состояние зоны, состояние тревоги или подключение зоны к источнику питания.

A.5.2 После операции сброса тревоги отчет об устранении тревоги на панели не формируется

Описание неисправности:
После операции сброса тревоги отчет об устранении тревоги на панели не формируется.
Решение:
При отсутствии тревоги отчет о сбросе тревог не будет загружен.

A.6 Ошибка отправки электронного письма

A.6.1 Не удается отправить тестовое письмо

Описание неисправности:
При настройке информации о почте нажмите **Test inbox** («Проверить почтовый ящик») и появляется сообщение: проверка не пройдена.
Решение:
Настройка параметров почтового ящика выполнена некорректно. Измените параметры настройки почтового ящика, как показано в таблице 1/1.

A.6.2 Не удается отправить письмо

Описание неисправности:
Проверьте журнал исключений панели. Появляется сообщение об ошибке: **Mail sending failure** («Ошибка при отправке почты»).
Решение:
Почтовый сервер имеет ограничение доступа. Войдите в почтовый ящик и снимите блокировку (при наличии).

A.6.3 Не удается отправить письмо в Gmail

Описание неисправности:
Почтовый ящик получателя: Gmail. Нажмите **Test Inbox** («Проверить папку «Входящие»»), появится сообщение: проверка не пройдена.
1. Google запрещает доступ к Gmail с помощью приложений / устройств, которые не соответствуют стандартам безопасности компании.
Решение:
Войдите на сайт (https://www.google.com/settings/security/lesssecureapps) и поставьте галочку для **Start using access of application not safe enough** («Предоставить доступ с небезопасных устройств»). После этого с устройств можно будет отправлять электронные письма.
2. Gmail использует CAPTCHA для аутентификации.
Решение: Перейдите по ссылке ниже, затем нажмите **Continue** («Продолжить») (https://accounts.google.com/b/0/displayunlockcaptcha).

A.6.4 Не удается отправить письмо на QQ или Foxmail

Описание неисправности:

Почтовый ящик получателя: QQ или foxmail. Нажмите **Test Inbox** («Проверить папку «Входящие»»), появится сообщение: проверка не пройдена.

1. Имя пользователя или пароль от учетной записи QQ указаны неверно.

Решение:

Пароль, необходимый для входа в учетную запись QQ, не является паролем, используемым для обычного входа в систему. Конкретный путь: Перейдите на вкладку **Email account → Device → Account** («Учетная запись электронной почты → Устройство → Учетная запись), чтобы сгенерировать код авторизации. Используйте код авторизации в качестве пароля для входа в систему.

2. Для открытия страницы требуется разрешение на вход по SMTP.

A.6.5 Не удается отправить письмо в Yahoo

Описание неисправности:

Почтовый ящик получателя: Yahoo. Нажмите **Test Inbox** («Проверить папку «Входящие»»), появится сообщение: проверка не пройдена.

1. На почтовом ящике установлены слишком высокие параметры безопасности.

Решение:

Зайдите в почтовый ящик и включите режим: **Less secure sign-in** («Разрешить менее безопасный вход»).

A.6.6 Настройка параметров почты

Настройка параметров почты

Тип почты	Почтовый сервер	Порт HTTP	Поддерживаемые протоколы
Gmail	smtp.gmail.com	587	TLS/STARTTLS (TLS)
Outlook	smtp.office365.com	587	STARTTLS (TLS)
Hotmail	smtp.office365.com	587	STARTTLS (TLS)
QQ	smtp.qq.com	587	STARTTLS (TLSv1.2)
Yahoo	smtp.mail.yahoo.com	587	STARTTLS (TLSv1.2)
126	smtp.126.com	465	SSL/TLS
Sina	smtp.sina.com	25/465/587	SSL/TLS/STARTTLS (SSL/TLS)

Тип почты	Почтовый сервер	Порт HTTP	Поддерживаемые протоколы

Примечание

Информация о настройке почты:

- Порт SMTP по умолчанию используется порт 25 без шифрования или порт 465, если используется протокол SSL / TLS. Порт 587 в основном используется для протокола STARTTLS.
  Режим протокола STARTTLS обычно используется по умолчанию при выборе TLS.
- Имя пользователя. В качестве имени пользователя в Outlook и Hotmail требуются полные имена, а для других адресов электронной почты требуется префикс перед @.

Таблица B. Типы входов

Таблица B-1 Типы входов

Типы входов	Операции
Зона мгновенного срабатывания	После постановки системы на охрану при обнаружении тревожного события тревога срабатывает незамедлительно. Запуск звукового ответа системы и звукового оповещателя. Голосовая подсказка: тревога зоны X.
Зона периметра	После постановки системы на охрану при обнаружении тревожного события тревога срабатывает незамедлительно. Звуковой ответ: включите звук и звуковой оповещатель системы. Существует настраиваемый интервал между выходом тревоги и сирены, который позволяет проверять тревоги и отменять вывод сигнала сирены в течение этого интервала. Голосовая подсказка: сработал периметральный датчик в зоне X.
Зона отсроченного срабатывания	Система дает время для выхода / входа в защищенную зону без срабатывания тревоги. Звуковое оповещение: включите звук и звуковой оповещатель системы. Голосовая подсказка: тревога зоны X.
Зона слежения	При обнаружении тревожного события во время задержки входа в систему зона действует как зона отсроченного срабатывания. В других случаях — действует как зона мгновенного срабатывания. Звуковое оповещение: включите звук и звуковой оповещатель системы. Голосовая подсказка: зона X запускает действия по тревоге.
Зона беззвучной сигнализации 24 часа в сутки	Зона активна все время со звуковым сигналом / звуковым оповещателем при срабатывании тревоги. Звуковое оповещение: звук в системе отключен (включая голосовые подсказки или оповещатели).
Зона тревоги	Зона активна все время. Звуковое оповещение: включите звук и звуковой оповещатель системы. Голосовая подсказка: тревога экстренного вызова в зоне X.
Зона датчиков пожарной сигнализации	Зона активна все время со звуковым сигналом / звуковым оповещателем при срабатывании тревоги. Звуковое оповещение: включите звук и звуковой оповещатель системы. Голосовая подсказка: пожарная тревога в зоне X.

Типы входов	Операции
Зона датчиков утечки газа	Зона активна все время со звуковым сигналом / звуковым оповещателем при срабатывании тревоги. Звуковое оповещение: включите звук и звуковой оповещатель системы. Голосовая подсказка: тревога утечки газа в зоне X.
Зона медицинской деятельности	Зона активна все время со звуковым сигналом / звуковой оповещателем при срабатывании тревоги. Звуковое оповещение: включите звук и звуковой оповещатель системы. Голосовая подсказка: тревога экстренной помощи в зоне X.
Зона заданного периода времени	Зона активна все время. Данный тип зоны используется для мониторинга и сообщения активного статуса зоны. Уведомления о статусе зоны будут направлены по истечении заданного времени (от 1 до 599 сек).
Зона отключенного предупреждения	Тревожные выходы не будут активированы при срабатывании датчика или тампера в зоне. Звуковое оповещение: звук в системе отключен (включая голосовые подсказки или оповещатели).
Виртуальная зона (клавиатура / брелок)	После постановки системы на охрану при обнаружении тревожного события тревога срабатывает незамедлительно. Звуковой ответ: включите звук и звуковой оповещатель системы. Голосовая подсказка: срабатывает бипер.
Тревога тампера	После постановки системы на охрану при обнаружении тревожного события тревога срабатывает незамедлительно. Звуковой ответ: включите звук и звуковой оповещатель системы. Голосовая подсказка: тревога саботажа в зоне X.
Привязка	Запустите связанное устройство при возникновении события. Пример: реле, связанные с расширителем выходов, будут активированы, когда панель поставлена на охрану.
Постановка на охрану	Когда зона поставлена на охрану: голосовое предупреждение об обнаружении неисправности. Далее можно устранить неисправность в соответствии с голосовой подсказкой. ● Звуковое оповещение для постановки на охрану с помощью метки или брелока. ● Голосовое предупреждение об обнаружении неисправности. Далее можно устранить неисправность в соответствии с голосовой подсказкой.

В клиентском ПО отображается сообщение о неисправности.

Устранить ошибку можно через клиентское программное обеспечение или мобильный клиент.

Голосовая подсказка. Постановка на охрану выполнена / Ошибка автоматической постановки на охрану.

Таблица C. Типы выходов

Таблица C-1 Тип вывода

Тип вывода	Активный	Восстановление
Постановка на охрану	Постановка панели на охрану	После настроенной задержки вывода
Снятие с охраны	Снятие панели с охраны	После настроенной задержки вывода
Параметры тревоги	Когда происходит тревожное событие. Тревожный выход будет активирован после заданной задержки на выход / вход	По истечении заданной задержки вывода снимите панель с охраны или отключите тревогу
Привязка зоны	При возникновении тревожного события связанное реле будет выдавать тревогу	По истечении настроенной продолжительности тревоги
Выполнение операций вручную	Включение реле вручную	По истечении времени срабатывания или отключите реле вручную

D. Типы событий

Таблица D-1 Типы событий

Типы событий	Настраиваемый	По умолчанию 1 (уведомление клиентского ПО)	По умолчанию 2 (ЧОП / ПЦН 1/2)	По умолчанию 3 (мобильный клиент)	По умолчанию 4 (телефон)
Тревожное событие и тревога тампера	×/√	√	√	√	√
Событие, угрожающее безопасности жизни сотрудника / посетителя	×/√	√	√	√	√
Уведомления о состоянии системы	×/√	√	×	×	×
Уведомление панели управления	×/√	√	×	×	×

E. Уровни доступа

Уровень	Описание
1	Доступ разрешен для неограниченного круга лиц.
2	Доступ разрешен для пользователей со стороны оператора и администратора; например, для клиентов (пользователи систем).
3	Доступ разрешен для пользователя со стороны установщика; например, для специалиста по охранной сигнализации.

Таблица E-1 Разрешения согласно уровню доступа

Функции	Разрешения		
	1	2	3
Постановка на охрану	Нет	Да	Есть
Снятие с охраны	Нет	Да	Есть
Восстановление / очистка тревог	Нет	Да	Есть
Вход в тестовый режим	Нет	Да	Есть
Обход зоны / снятие зоны с охраны / Принудительная постановка на охрану	Нет	Да	Есть
Добавление / изменение кода подтверждения	Нет	Есть[d]	Есть[d]
Добавление / редактирование пользователя уровня 2 и кода подтверждения	Нет	Да	Есть
Добавление / редактирование параметров настройки	Нет	Нет	Да
Замена ПО и прошивки	Нет	Нет	Нет

Примечание

[a] При условии предварительного разрешения от пользователя на уровне 2.

[b]При условии предварительного разрешения от пользователя на уровне 2 и 3.

[d]Пользователи могут редактировать только свой собственный код пользователя.

- Пользователь с уровнем доступа 2 может назначить разрешение входа контроллера для пользователя с уровнем доступа 3 на странице настроек.
- Пользователь с уровнем доступа 2 может назначить разрешение для пользователя с уровнем доступа 3, если пользователю с уровнем доступа 3 необходимо удаленно войти в систему контроллера.
- При обходе контроллера, пользователь с уровнем доступа 3 может войти в систему контроллера без назначения полномочий от пользователя с уровнем доступа 2.
- При обходе контроллера, пользователь с уровнем доступа 3 может войти в систему контроллера без назначения полномочий от пользователя с уровнем доступа 2.
- Пользователь с уровнем доступа 4 может войти в контроллер только в том случае, если пользователь с уровнем доступа 2 или уровень 3 назначил разрешения для пользователя с уровнем доступа 4.

F. Сигнал

F.1 Обнаружение неисправностей ATP / ATS

Неисправности ATP будут обнаружены, когда сетевой кабель панели отключен или путь передачи к приемопередатчику приемного центра, расположенного в ЧОП / ПЦН, заблокирован где-то посередине пути. Уведомление о неисправности ATS будет сообщено при обнаружении сбоев ATP на обоих путях передачи. Ошибка будет устранена, как только сетевой кабель будет подключен и восстановлен путь передачи к приемопередатчику центра приема. Уведомление об устранении неисправности ATS появится сразу после обнаружения в системе.

Временные характеристики обнаружения сбоев и восстановления ATP показаны в таблице ниже.

	TN	Максимальное время обнаружения
Ошибка первичного ATP / восстановление ATP	LAN/Wi-Fi	10 мин
Ошибка вторичного ATP / восстановление ATP	GPRS	60 мин.
	3G/4G LTE	20 мин (при отказе первичного ATP)

Сигнал всегда будет передаваться от первичного ATP, когда он находится в рабочем состоянии. В противном случае он будет автоматически переключен на вторичный путь передачи, который работает в данный момент. Уведомления о первичных и вторичных сбоях ATP, а также об устранении неисправности будут направлены в ЧОП / ПЦН. Уведомления также будут записаны в обязательную память журнала, рассчитанную на 1000 записей, размещенную в энергонезависимой флэш-памяти, а также в журнал неисправностей ATS. Подробности отчетов и записей журнала перечислены в таблице ниже.

	Код события при сигнализации	Описание журнала событий
Ошибка первичного ATP / восстановление ATP	E351 / R351	Ошибка пути к локальной сети / восстановление пути к локальной сети
Ошибка вторичного ATP / восстановление ATP	E352 / R352	Ошибка пути к мобильной сети / восстановление пути к мобильной сети
Сбой ATP / восстановление	-	Сбой ATP
Сбой / восстановление основного сетевого интерфейса	E351 / R351	Ошибка пути к локальной сети / восстановление пути к локальной сети
Сбой / восстановление вторичного сетевого интерфейса	E352 / R352	Ошибка пути к мобильной сети / восстановление пути к мобильной сети

F.1 Категория ATS

Категория ATS в AXPRO: DP2. Пока включен ЧОП / ПЦН. Контрольная панель загрузит отчет о тревоге в ЧОП / ПЦН через основной путь (LAN или Wi-Fi) или резервный путь (3G / 4G). Если панель управления корректно подключена к локальной сети или Wi-Fi, в качестве пути передачи выбирается основной путь. В случае сбоя подключения по основному пути, путь будет переключен на 3G / 4G. И если соединение основного пути будет восстановлено, путь будет переключен обратно на LAN или Wi-Fi.

Панель управления постоянно проверяет состояние подключения и генерирует журналы ошибок передачи для любого пути.
Когда оба пути недействительны, панель управления определяет неисправность ATS.

G. Код SIA и CID

Примечание

Приведенный ниже код предназначен для передачи данных с охранной панели в ЧОП / ПЦН по протоколу DC09.

Таблица F-1 Код SIA и CID

Код SIA	Код CID	Описание операции
MA	1100	Тревога экстренной медицинской помощи
MH	3100	Тревога экстренной медицинской помощи устранена
BA (Датчик протечки воды: WA)	1130 (Датчик протечки воды: 1154)	Тревога взлома
BH (Датчик протечки воды: WH)	3130 (Датчик протечки воды: 3154)	Тревога взлома устранена
FA (Тепловой извещатель: KA)	1111 (Тепловой извещатель: 1114)	Пожарная тревога
FH (Тепловой извещатель: KH)	3111 (Тепловой извещатель: 3114)	Пожарная тревога устранена
HA	1121	Тревога принудительного действия
HA	1122	Беззвучная сигнализация экстренного вызова
HH	3122	Беззвучная сигнализация экстренного вызова устранена
AA	1123	Тревога экстренного вызова
CH	3123	Беззвучная тревога экстренного вызова устранена
	1133	Тревога 24 часа в сутки
	3133	Тревога 24 часа в сутки устранена
	1133	Тревога 24 часа в сутки
	3133	Тревога 24 часа в сутки устранена
BA	1130	Тревога тайм-аута
BH	3130	Тревога тайм-аута устранена
PA	1120	Тревога экстренного вызова
PH	3120	Беззвучная тревога экстренного вызова устранена
BA	1130	Тревога взлома
BH	3130	Тревога взлома устранена

Код SIA	Код CID	Описание операции
BA	1131	Тревога проникновения через периметр
BH	3131	Тревога проникновения через периметр устранена
AD	1132	Тревога несанкционированных вторжений
CK	3132	Тревога несанкционированных вторжений устранена
BA (Датчик протечки воды: WA)	1130 (Датчик протечки воды: 1154)	Тревога 24 часа в сутки
BH (Датчик протечки воды: WH)	3130 (Датчик протечки воды: 3154)	Тревога 24 часа в сутки устранена
BA (Датчик протечки воды: WA)	1130 (Датчик протечки воды: 1154)	Тревога взлома
BH (Датчик протечки воды: WH)	3130 (Датчик протечки воды: 3154)	Тревога взлома устранена
TA	1137	Тревога открытия крышки панели
TR	3137	Тревога открытия крышки панели устранена
BV	1139	Подтвержденная тревога
BW	3139	Подтвержденная тревога устранена
		Тревога разомкнутой цепи
		Тревога разомкнутой цепи устранена
AF	1142	Тревога короткого замыкания
CN	3142	Тревога короткого замыкания устранена
TA	1144	Внешний зонд отключен
TR	3144	Внешний зонд подключен
AG	1148	Тревога перемещения устройства
CO	3148	Тревога перемещения устройства устранена
	1149	Тревога при обнаружения маскировки
	3149	Тревога при обнаружения маскировки устранена
GA	1162	Тревога утечки газа
GH	3162	Тревога утечки газа устранена
AH	1207	Тревога зоны раннего предупреждения

Код SIA	Код CID	Описание операции
CP	3207	Тревога зоны раннего предупреждения устранена
AT	1301	Тревога потери питания
AR	3301	Тревога потери питания устранена
YT	1302	Низкий заряд батареи
YR	3302	Тревога низкого заряда батареи устранена
ZY	1305	Сброс до заводских настроек
YM Отсутствует батарея передатчика Дальность ИК-подсветки 301~	1311 Отсутствует батарея передатчика Дальность ИК-подсветки 301~	Тревога отключения батареи
YR Отсутствует батарея передатчика Дальность ИК-подсветки 301~	3311 Отсутствует батарея передатчика Дальность ИК-подсветки 301~	Тревога отключения батареи устранена
YI	1312	Тревога перегрузки
YJ	3312	Тревога перегрузки устранена
YP	1319	Тревога перенапряжения
YQ	3319	Тревога перенапряжения устранена
AI	1333	Исключение расширителя
CQ	3333	Тревога саботажа расширителя устранена
AJ	1336	Принтер отключен
CR	3336	Принтер подключен
XT	1384	Низкий заряд батареи
XR	3384	Тревога низкого заряда батареи устранена
		Низкое напряжение расширителя
		Нормальное напряжение расширителя
YP	1301	Тревога потери питания
YQ	3301	Тревога потери питания устранена
YM	1311	Тревога отключения батареи
YR	3311	Тревога отключения батареи устранена
TA (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	1144 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Тревога открытия крышки панели

Код SIA	Код CID	Описание операции
TR (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	3144 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Тревога открытия крышки панели устранена
YP Питание передатчика (AC) отключено Дальность ИК-подсветки 301~	1301 Питание передатчика (AC) отключено Дальность ИК-подсветки 301~	Тревога потери питания расширителя
YQ Питание передатчика (AC) отключено Дальность ИК-подсветки 301~	3301 Питание передатчика (AC) отключено Дальность ИК-подсветки 301~	Тревога потери питания расширителя устранена
TA	1144	Тревога открытия крышки панели
TR	3144	Тревога открытия крышки панели устранена
TA	1144	Тревога открытия крышки панели
TR	3144	Тревога открытия крышки панели устранена
XL	1381	Состояние устройства «Не в сети»
XC	3381	Устройство восстановлено
TA (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	1144 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	Тревога открытия крышки панели
TR (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	3144 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	Тревога открытия крышки панели устранена
XT (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	1384 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	Низкий заряд батареи
XR (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	3384 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	Тревога низкого заряда батареи устранена

Код SIA	Код CID	Описание операции
XL (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	1381 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	Состояние устройства «Не в сети»
XC (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	3381 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	Устройство восстановлено
LT	1351	Неисправность основного сигнального тракта
LR	3351	Неисправность основного сигнального тракта устранена
LT	1352	Неисправность сигнального тракта резервного копирования
LR	3352	Неисправность сигнального тракта резервного копирования устранена
AM	1354	Телефонная линия отключена
CU	3354	Телефонная линия подключена
AN	1382	Ошибка контроля шины
CV	3382	Ошибка контроля шины устранена
TA	1144	Тревога открытия крышки панели
TR	3144	Тревога открытия крышки панели устранена
		Тревога разомкнутой цепи зоны
		Тревога разомкнутой цепи зоны устранена
OP	1401	Снятие с охраны
CL	3401	Под охраной
OA	1403	Автоматическое снятие с охраны
CA	3403	Автоматическая постановка на охрану
BC	1406	Тревожные уведомления устранены
CW	3408	Мгновенная постановка на охрану
CS	1409	Снятие с охраны при переключении между зонами
OC	3409	Постановка на охрану при переключении между зонами
NL	3441	Постановка на охрану в домашнем режиме
CX	3442	Принудительная постановка на охрану

Код SIA	Код CID	Описание операции
		Включить вывод по расписанию
		Выключить вывод по расписанию
CT	1452	Задержка снятия с охраны
CD	1455	Ошибка автоматической постановки на охрану
		Ошибка включения выхода
		Ошибка отключения выхода
		Ошибка автоматического снятия с охраны
		Изменение сети
QB	1570	Обход
QU	3570	Тревога обхода зоны устранена
AU	1574	Обход группы
CZ	2574	Тревога обхода группы устранена
AV	1601	Проверка отчета вручную
RP	1602	Отправка периодических отчетов
TS	1607	Диагностика включена
TE	3607	Диагностика отключена
AW	1617	Проверка телефонного соединения
LB	1627	Режим разработки
LX	1628	Выход из режима разработки
BA	1131	Обнаружение вторжения
BH	3131	Тревога обнаружения вторжения устранена
BA	1131	Тревога пересечения линии
BH	3131	Тревога пересечения линии устранена
		Тревога ИК-датчика
		Тревога ИК-датчика устранена
AY	1775	Тревога внезапного роста интенсивности звука
DE	3775	Тревога внезапного роста интенсивности звука устранена
AZ	1776	Тревога внезапного спада интенсивности звука
DF	3776	Тревога внезапного спада интенсивности звука устранена
		Ошибка аудиовхода
		Ошибка аудиовхода устранена
BA	1131	Тревога пересечения линии
BH	3131	Тревога пересечения линии устранена

Код SIA	Код CID	Описание операции
BA	1134	Обнаружение входа в область
EA	1134	Тревога устранена
FA	1112	Пожарная тревога
FH	3112	Пожарная тревога устранена
KS	1158	Предварительная тревога повышенной температуры
KR	3158	Предварительная тревога повышенной температуры устранена
ZS	1159	Предварительная тревога пониженной температуры
ZR	3159	Предварительная тревога пониженной температуры устранена
KA	1158	Тревога повышенной температуры
KH	3158	Тревога повышенной температуры устранена
ZA	1159	Тревога пониженной температуры
ZH	3159	Тревога пониженной температуры устранена
EA	1134	Обнаружение выхода из области
PA (номер пользователя клавиатуры начинается с 101, брелока: с 901)	1120 (номер пользователя клавиатуры начинается с 101, брелока: с 901)	Тревога экстренного вызова
FA	1110	Пожарная тревога с клавиатуры / брелока
		Тревога взлома с клавиатуры / брелока
CI	1454	Ошибка постановки на охрану
MA	1100	Тревога экстренной медицинской помощи с клавиатуры / брелока
DK	1501	Клавиатура заблокирована
DO	3501	Клавиатура разблокирована
		Тревога отсутствия на месте
BE	1910	Клавиатура отключена
DH	3910	Клавиатура подключена
BF	1911	Реле KBUS отключено
DI	3911	Реле KBUS подключено
		KBUS GP/K отключено
		KBUS GP/K подключено
		KBUS MN/K отключено
		KBUS MN/K подключено

Код SIA	Код CID	Описание операции
DK	1501	Считыватель карт (брелоков) заблокирован
DO	3501	Считыватель карт (брелоков) разблокирован
BD	1865	Метка не зарегистрирована
XL	1381	Состояние устройства «Не в сети»
XC	3381	Устройство восстановлено
XT	1384	Низкий заряд батареи
XR	3384	Тревога низкого заряда батареи устранена
XL (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	1381 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Состояние устройства «Не в сети»
XC (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	3381 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Устройство восстановлено
XL	1381	Состояние устройства «Не в сети»
XC	3381	Устройство восстановлено
BI	1918	Сбой передатчика радиолокационной станции
DL	3918	Сбой передатчика радиолокационной станции устранен
XT	1384	Низкий заряд батареи
XR	3384	Тревога низкого заряда батареи устранена
NT	1350	Сбой сотовой сети
NR	3350	Сбой сотовой сети устранен
NT	1350	Исключение SIM-карты
NR	3350	Исключение SIM-карты восстановлено
NT	1350	Сбой сети
NR	3350	Сбой сети устранен
XQ	1344	Обнаружено глушение
XH	3344	Глушение устранено
NT	1350	Достигнут лимит данных
XT	1384	Низкий заряд батареи
XR	3384	Тревога низкого заряда батареи устранена
NT	1350	IP-адрес уже используется

Код SIA	Код CID	Описание операции
NR	3350	Конфликт IP-адресов устранен
NT	1350	Сбой сети
NR	3350	Сбой сети устранен
BA	1131	Запуск тревоги обнаружения движения
BH	3131	Остановка тревоги обнаружения движения
BJ	1941	Устройство заблокировано
DM	3941	Тревога блокировки устройства устранена
		Потеря видеосигнала
		Видеосигнал восстановлен
		Несоответствие формата ввода / вывода
		Несоответствие формата ввода / вывода устранено
		Исключение видеовхода
		Исключение видеовхода устранено
		Переполнение накопителя
		Накопитель пуст
		Исключение HDD
		Исключение накопителя устранено
		Ошибка загрузки изображения
BQ	1948	Ошибка отправки email
BR	1949	IP-камера отключена
DS	3949	IP-камера подключена
		Проверка команды
		Сообщение ответа
BU	1962	Сообщение о пожарной тревоге
DT	3962	Сообщение о пожарной тревоге завершено
BV	1963	Сообщение о тревоге принудительного действия
DU	3963	Сообщение о тревоге принудительного действия завершено
BW	1964	Сообщение о тревоге экстренной помощи
DV	3964	Сообщение о тревоге экстренной помощи завершено
DW	3250	Сигнал патрулирования

Код SIA	Код CID	Описание операции
BX	1970	BUS-запрос
BY	1971	Регистрация BUS-шины
BZ	1973	Снятие с охраны одной зоны
DX	3973	Постановка на охрану одной зоны
CA	1974	Тревога одной зоны сброшена
CB	1306	Устройство удалено
DY	3306	Устройство зарегистрировано
CC	1976	Сообщение об операциях
DZ	3976	Сообщение об операциях завершено
CD	1306	Устройство удалено
EA	3306	Устройство зарегистрировано
CE	1306	Устройство удалено
EB	3306	Устройство зарегистрировано
CF	1306	Устройство удалено
EC	3306	Устройство зарегистрировано
CG	1306 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	Устройство удалено
ED	3306 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201, передатчика: с 301)	Устройство зарегистрировано
JA	1461	Неверный пароль
NT	1350	Состояние устройства «Не в сети»
YM	1311	Исчерпание мощности