



# Охранная панель AX PRO

Руководство пользователя

## **Правовая информация**

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. Все права защищены.

### **О руководстве**

Руководство содержит инструкции для использования и управления продуктом. Изображения, графики и вся другая информация предназначена только для ознакомления. Этот документ может быть изменен без уведомления, в связи с обновлением прошивки и по другим причинам. Последнюю версию настоящего документа можно найти на веб-сайте (<https://www.hikvision.com/>).

Используйте этот документ под руководством профессионалов, обученных работе с продуктом.

### **Торговые марки**

**HIKVISION**

и другие торговые марки Hikvision и логотипы являются интеллектуальной собственностью Hikvision в различных юрисдикциях.

Другие торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

### **Правовая информация**

ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ДАННОЕ РУКОВОДСТВО, ПРОДУКТ, АППАРАТУРА, ПРОГРАММНОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», СО ВСЕМИ ОШИБКАМИ И НЕТОЧНОСТЯМИ. HIKVISION НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, КАСАТЕЛЬНО УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ СООТВЕТСТВИЯ УКАЗАННЫМ ЦЕЛЯМ. ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА НЕСЕТ ПОЛЬЗОВАТЕЛЬ. HIKVISION НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД ПОТРЕБИТЕЛЕМ ЗА КАКОЙ-ЛИБО СЛУЧАЙНЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ, ВКЛЮЧАЯ УБЫТКИ ИЗ-ЗА ПОТЕРИ ПРИБЫЛИ, ПЕРЕРЫВА В ДЕЯТЕЛЬНОСТИ ИЛИ ПОТЕРИ ДАННЫХ ИЛИ ДОКУМЕНТАЦИИ, ПО ПРИЧИНЕ НАРУШЕНИЯ УСЛОВИЙ КОНТРАКТА, ТРЕБОВАНИЙ (ВКЛЮЧАЯ ХАЛАТНОСТЬ), УДОВЛЕТВОРИТЕЛЬНОСТИ КАЧЕСТВА ИЛИ ИНОГО, В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ HIKVISION БЫЛО ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ПРОДУКТА С ДОСТУПОМ В ИНТЕРНЕТ НЕСЕТ ПОЛЬЗОВАТЕЛЬ; HIKVISION НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА НЕНОРМАЛЬНУЮ РАБОТУ ОБОРУДОВАНИЯ, ПОТЕРЮ ИНФОРМАЦИИ И ДРУГИЕ ПОСЛЕДСТВИЯ, ВЫЗВАННЫЕ КИБЕР АТАКАМИ, ВИРУСАМИ ИЛИ ДРУГИМИ ИНТЕРНЕТ РИСКАМИ; ОДНАКО, HIKVISION ОБЕСПЕЧИВАЕТ СВОЕВРЕМЕННУЮ ТЕХНИЧЕСКУЮ ПОДДЕРЖКУ, ЕСЛИ ЭТО НЕОБХОДИМО. ВЫ ОБЯЗУЕТЕСЬ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В СООТВЕТСТВИИ С ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, А ТАКЖЕ НЕСЕТЕ ПОЛНУЮ ОТВЕТСТВЕННОСТЬ ЗА ЕГО СОБЛЮДЕНИЕ. В ЧАСТНОСТИ, ВЫ НЕСЕТЕ ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ДАННОГО ПРОДУКТА ТАКИМ ОБРАЗОМ, ЧТОБЫ НЕ НАРУШАТЬ ПРАВА ТРЕТЬИХ ЛИЦ, ВКЛЮЧАЯ ПРАВА НА ПУБЛИЧНОСТЬ, ПРАВА НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ, ЗАЩИТУ ДАННЫХ И ДРУГИЕ ПРАВА КАСАТЕЛЬНО НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ. ВЫ ОБЯЗУЕТЕСЬ НЕ ИСПОЛЬЗОВАТЬ ЭТОТ ПРОДУКТ В ЗАПРЕЩЕННЫХ ЦЕЛЯХ, ВКЛЮЧАЯ РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ,

## **Охранная панель AX PRO • Руководство пользователя**

РАЗРАБОТКУ ИЛИ ПРОИЗВОДСТВО ХИМИЧЕСКОГО ИЛИ БИОЛОГИЧЕСКОГО ОРУЖИЯ, ЛЮБУЮ ДЕЯТЕЛЬНОСТЬ, СВЯЗАННУЮ С ЯДЕРНЫМИ ВЗРЫВЧАТЫМИ ВЕЩЕСТВАМИ, НЕБЕЗОПАСНЫМ ЯДЕРНЫМ ТОПЛИВНЫМ ЦИКЛОМ ИЛИ НАРУШАЮЩУЮ ПРАВА ЧЕЛОВЕКА. В СЛУЧАЕ КАКИХ-ЛИБО КОНФЛИКТОВ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.




### **Защита данных**

Во время использования устройства личные данные будут собираться, храниться и обрабатываться. При разработке устройств Hikvision соблюдаются принципы конфиденциальности в целях защиты данных. Например, устройства с функциями распознавания лиц разработаны таким образом, что сохраняемые биометрические данные защищены шифрованием; в устройствах с функцией идентификации по отпечатку пальца будут сохранены только шаблоны отпечатка пальца и, таким образом, изображение отпечатка пальца не подлежит реконструкции.

Поскольку данные находятся под вашим контролем, сбор, хранение, обработку и передачу данных необходимо выполнять в соответствии с применимыми законами и требованиями по защите данных. Также необходимо выполнять действия по безопасности для защиты личных данных, такие как разумный административный и физический контроль безопасности, периодические обзоры и оценки эффективности мер безопасности.

## Условные обозначения

В настоящем документе используются следующие символы.

Символ	Описание
 <b>Предупреждение</b>	Указывает на опасную ситуацию, которая, если не удастся ее избежать, может привести к летальному исходу или серьезным травмам.
 <b>Предостережение</b>	Указывает на потенциально опасную ситуацию, которая, если не удастся ее избежать, может привести к повреждению оборудования, потере данных, ухудшению рабочих характеристик, либо к получению неожиданных результатов.
 <b>Примечание</b>	Предоставляет дополнительную информацию, чтобы подчеркнуть или дополнить важные пункты основного текста.

## Регулирующая информация

EN 50131-1:2006 + A1:2009 + A2:2017

Уровень безопасности: 2

EN 50131-3:2009

Категория защиты

EN 50131-6:2017

окружающей среды: II DP2

EN 50131-5-3:2017

EN 50131-10: 2014




EN 50136-2: 2013





### Примечание

При использовании несовместимых настроек необходимо удалить маркировку соответствия EN50131.

### Соответствие стандартам ЕС

	<p>Данный продукт и — если применимо — также и поставляемые принадлежности отмечены знаком «CE» и, следовательно, согласованы с европейскими стандартами, перечисленными под директивами 2014/30/EC EMC, 2014/53/EC и 2011/65/EC RoHS.</p>
	<p>2012/19/EC (директива WEEE). Продукты, отмеченные данным знаком, запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Для надлежащей переработки верните этот продукт своему местному поставщику при покупке эквивалентного нового оборудования или утилизируйте его в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: <a href="http://www.recyclethis.info">www.recyclethis.info</a></p>
	<p>2006/66/EC (директива о батареях): данный продукт оснащен батареей, которую запрещено выбрасывать в коллекторы несортированного мусора в Европейском союзе. Подробная информация о батарее изложена в документации продукта. Батарея помечена символом, который может включать буквенное обозначение, сообщающее о наличии кадмия (Cd), свинца (Pb) или ртути (Hg). Для надлежащей утилизации возвратите батарею своему поставщику или утилизируйте её в специально предназначенных точках сбора. За дополнительной информацией обратитесь по адресу: <a href="http://www.recyclethis.info">www.recyclethis.info</a></p>

	<p><b>Предупреждение</b> Это продукт класса А. В домашних условиях этот продукт может создавать радиопомехи, и в этом случае пользователю может потребоваться принять необходимые меры по их устранению.</p>
	<p><b>Информация о FCC</b> Обратите внимание, что изменения или модификации, не одобренные явно стороной, ответственной за соответствие, может привести к аннулированию полномочий пользователя по работе с данным оборудованием.</p> <p>Соответствие FCC: Это оборудование прошло испытания и соответствует регламенту для цифрового устройства класса В, применительно к части 15 Правил FCC. Данный регламент разработан для того, чтобы обеспечить необходимую защиту от вредных помех, возникающих при использовании оборудования в коммерческой среде. Это оборудование генерирует, использует, и может излучать радиоволны на разных частотах и, если устройство установлено и используется не в соответствии с инструкцией, оно может создавать помехи для радиосигналов. Тем не менее, нет никакой гарантии, что помехи не возникнут в каких-либо конкретных случаях установки. Если оборудование создает вредные помехи для приема радио- или телевизионных сигналов, что может быть определено путем включения и выключения оборудования, пользователю рекомендуется попытаться устранить помехи одним или несколькими способами, а именно:</p> <ul style="list-style-type: none"><li>— Изменить ориентацию или местоположение приемной антенны.</li><li>— Увеличить расстояние между оборудованием и приемником.</li><li>— Подключить оборудование к розетке в цепи, отличной от той, к которой подключен приемник.</li><li>— Обратиться к дилеру или опытному радио / телемастеру.</li></ul> <p>Данное оборудование следует устанавливать и эксплуатировать на расстоянии не менее 20 см между источником излучения и пользователем.</p> <p><b>Условия FCC</b> Это устройство соответствует требованиям части 15 правил FCC. Эксплуатация допускается при соблюдении следующих двух условий:</p>

# Содержание

Правовая информация .....	2
Условные обозначения.....	3
Регулирующая информация .....	4
Содержание .....	6
Раздел 1 Введение.....	9
1.1 Описание системы.....	9
1.2 Спецификации.....	10
1.3 Внешний вид устройства.....	14
Раздел 2 Запуск устройства .....	17
2.1 Инициализация устройства.....	17
2.2 Установка устройства .....	18
Раздел 3 Управление пользователями .....	20
3.1 Управление пользователями.....	20
3.2 Журнал доступа.....	23
Раздел 4 Настройка параметров устройства .....	25
4.1 Настройка с помощью Hik-Proconnect.....	25
4.2 Настройка параметров с помощью Hik-Connect .....	41
4.3 Настройка параметров с помощью веб-клиента .....	48
4.3.2 Управление устройством .....	62
4.3.3 Настройки области .....	70
4.3.4 Управление видео.....	72
4.3.5 Управление разрешениями .....	74
4.3.6 Техническое обслуживание .....	75
4.3.7 Настройка системы.....	77
4.3.8 Диагностика состояния .....	89
4.4 Направление отчетности для ЧОП / ПЦН .....	90
Раздел 5 Общие операции .....	94
5.1 Постановка на охрану .....	94
5.2 Снятие с охраны .....	95
5.3 Управление системой с помощью SMS .....	95
А. Поиск неисправностей .....	96
А.1 Ошибка связи .....	96

## Охранная панель AX PRO • Руководство пользователя

A.1.1	Конфликт IP-адресов .....	96
A.1.2	Веб-страница недоступна .....	96
A.1.3	Отсутствие подключения к Hik-Connect.....	96
A.1.4	Часто пропадает подключение к IP-камере.....	96
A.1.5	Не удалось добавить устройство в приложение.....	97
A.1.6	Информация о тревоге не передается в приложение / iVMS-4200 / ЧОП / ПЦН .....	97
A.2	Взаимоисключаемые функции .....	97
A.2.1	Невозможно войти в режим регистрации .....	97
A.3	Ошибки зоны .....	97
A.3.1	Отсутствует подключение к зоне .....	97
A.3.2	Зона с контролем вскрытия .....	98
A.3.3	Срабатывание тревоги в зоне / Неисправность .....	98
A.4	Проблемы при постановке на охрану .....	98
A.4.1	Сбой постановки на охрану (когда процесс постановки на охрану не запускается) ..	98
A.5	Сбой операции .....	98
A.5.1	Не удается войти в тестовый режим .....	98
A.5.2	После операции сброса тревоги отчет об устранении тревоги на панели не формируется .....	99
A.6	Ошибка отправки электронного письма .....	99
A.6.1	Не удается отправить тестовое письмо .....	99
A.6.2	Не удается отправить письмо .....	99
A.6.3	Не удается отправить письмо в Gmail .....	99
A.6.4	Не удается отправить письмо на QQ или Foxmail .....	100
A.6.5	Не удается отправить письмо в Yahoo.....	100
A.6.6	Настройка параметров почты Таблица А-1 .....	101
B.	Типы входных сигналов .....	102
C.	Тип вывода .....	105
D.	Типы событий .....	106
E.	Уровни доступа.....	107
F.	Сигнал.....	109
G.	Код SIA и CID .....	110
H.	Коммуникационная матрица и команды устройства .....	117



## Раздел 1 Введение

### 1.1 Описание системы

Охранная панель AX Pro 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 мАч, время работы в режиме ожидания 12 часов.

## 1.2 Спецификации

<b>AX PRO E</b>		
<b>Емкость</b>	Области	8
	Зоны	До 48 (до 48 внутренних извещателей)
	Выход	
	Считыватель карт (брелоков)	До 8
	Клавиатура	
	Звуковой оповещатель	4 (2 внутри помещений + 2 снаружи помещений)
	Ретранслятор	2
	Брелок	16
	Метки	16
<b>Пользователь</b>	Установщик	1
	Администратор	1
	Обычный пользователь	14
<b>Технические характеристики беспроводного подключения</b>	Частота радиосвязи	433 МГц
	Тип беспроводной связи	Двусторонняя беспроводная передача
	Беспроводная охранная система	Скачкообразная смена частоты, шифрование 128 AES
<b>Функциональные особенности</b>	Голосовое предупреждение	√
	Приложение для работы	√
	Приложение для работы	√
	Веб-сервер для обслуживания (автономная настройка)	√
	Записи журнала событий	5000, включая 1000 обязательных
	Поддержка PIR-датчика со встроенной камерой (PIRCAM)	√
<b>Сетевые интерфейсы</b>	Ethernet	Auto 10/100M Ethernet
	Wi-Fi	802.11 b/g/n (2.4 ГГц)
<b>Оповещение ЧОП / ПЦН</b>	Протоколы	SIA DC09 (SIA уровень 2, ID контакта), ISUP, ISAPI (SDK) Hik-IP Receiver и Hik-IP Receiver Pro (Sur-Gard и Ademco 685)
<b>Облачный сервис</b>	Служба Hik-ProConnect	√
	Служба Hik-Connect	√
<b>Автоматизация</b>	Переключатель	√
	Реле	√
	Управляемая розетка	√
<b>Питание</b>	Напряжение сети	От 100 до 240 В, 50/60 Гц 0.3 А (макс.)
	Емкость батареи <sup>д</sup>	4520 мАч
	Время работы батареи в режиме ожидания <sup>е</sup>	До 12 ч
	Тип батареи	Встроенная литиевая-ионная батарея Модель: 765965

## Охранная панель AX PRO • Руководство пользователя

<b>Питание</b>	Энергопотребление	С привязкой к тревоге: 405 мА Без привязки к тревоге: 340 мА
	Ток при питании от батареи	340 мА
	Время заряда батареи	4 ч до 80 %
	Предупреждение о низком напряжении	3.55 В
<b>Обслуживание</b>	Обслуживаемые детали отсутствуют	
<b>Требования к среде</b>	Рабочая температура	От -10 до +50 °С От -10 до +40 °С (сертифицированная температура)
	Относительная влажность	От 10 до 90 % (без конденсата)
<b>Размеры и масса</b>	Размеры	170.0 x 170.0 x 38.6 мм (6.7 x 6.7 x 1.5")
	Масса	557.5 г
<b>Сертификаты</b>	CE/CB	✓
	ROHS/REACH/WEEE	✓
	FCC	✓
	RCM	✓
<b>b</b>	Беспроводная охранная панель AX Pro совместима с протоколом SIA IP Reporting (UDP / TCP-2013) согласно ANSI / SIA DC-09-2013: отчет о тревожном событии по интернет протоколу. Охранная панель поддерживает токены (протоколы) <b>ADM-CID</b> и <b>SIA-DCS</b> , определенные в SIA DC-07-2001.04, в которых будет добавлен знак «*» перед именем токена, например, <b>*ADM-CID</b> и <b>*SIA-DCS</b> , если данные и отметки времени передачи сообщений зашифрованы по стандарту AES. Поддержка AES-128, AES-192 и AES-256.	
<b>d</b>	Номинальные значения.  Фактическая емкость может незначительно отличаться. Фактическая емкость батареи для каждого отдельного устройства может незначительно превышать или быть ниже номинального значения. Удаление батареи может привести к повреждению устройства. Для замены или ремонта батареи обратитесь к установщику.	
<b>e</b>	При подключенном Wi-Fi, GPRS / 3G / 4G LTE, подключенном ЧОП / ПЦН (интервал опроса: 1800 с), появляется доступ к 8 входам и 1 клавиатуре, а также доступ к облачному сервису.	

### **Примечание**

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

Приоритет сообщения и индикации совпадает.

Охранная панель AX PRO 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.

---

## Охранная панель AX PRO • Руководство пользователя

### Инструкция RSSI для периферийных устройств

Соответствие требованиям стандарта EN 50131-5-3 4.2.2.

Уровень	Значение	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.

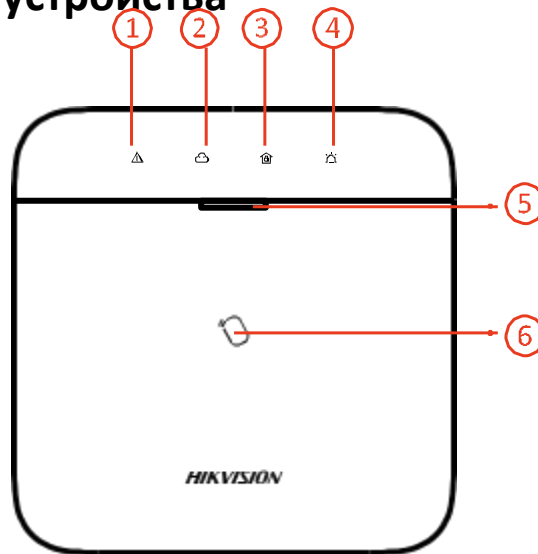
### Параметры уведомлений AX PRO

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

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

### 1.3 Внешний вид устройства

Передняя панель



**Таблица 1-2 Описание передней панели**

№	Название	Описание
1	Индикатор предупреждения	<p>Сплошной оранжевый: в состоянии снятия с охраны LED-индикатор отображает тревогу (например, экстренный вызов, тревога зоны, тревога саботажа и т. д.) и предупреждения о неисправности (сбой в работе, сбой соединения и т. д.).</p> <hr/> <p><b>Примечание</b></p> <ul style="list-style-type: none"> <li>Индикатор или голосовые предупреждения не будут выдаваться на какие-либо действия, выполненные пользователями уровня 1. Уведомления будут выдаваться только когда пользователь уровня 1 представляет или использует действительные карты или метки.</li> <li>Устройство запросит подробную информацию о тревоге или неисправности, когда авторизованные пользователи</li> </ul>
2	Индикатор соединения	<p><b>Горит зеленым:</b> панель привязана к учетной записи Hik-Connect.  <b>Выключено:</b> панель не привязана к учетной записи Hik-Connect.</p>
3	LED-индикатор постановки на охрану / снятия с охраны	<p>Горит синим в течение 5 с: под охраной  Дважды мигает зеленым: снят с охраны</p>

## Охранная панель AX PRO • Руководство пользователя

№	Название	Описание
		<b>Примечание</b> Если индикатор постановки на охрану горит постоянно, светодиод горит синим при постановке на охрану и не горит при снятии с охраны. Функция не соответствует стандарту EN.
4	Индикатор тревоги	<b>Мигает красным:</b> тревожное событие ( <b>Горит красным:</b> саботаж устройства <b>Выключен:</b> отсутствие тревоги
5	Индикатор питания	<b>Горит зеленым:</b> питание включено <b>Выключен:</b> питание отключено
6	Отметка текущей области	<b>Примечание</b> Спектр подключаемых устройств варьируется в зависимости от модели устройства.

### Интерфейсы и компоненты

Снимите заднюю крышку: некоторые компоненты и интерфейсы находятся на задней панели.

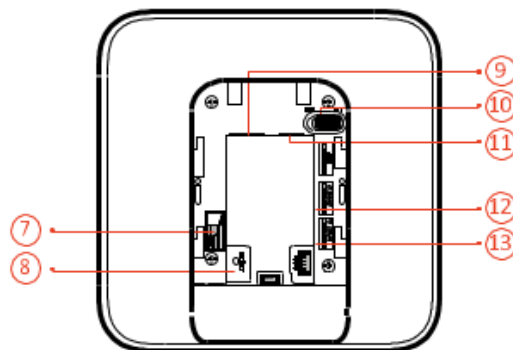





Таблица 1-3 Описание задней панели

№	Описание
7	Тампер
8	Кнопка сброса настроек

## Охранная панель AX PRO • Руководство пользователя

№	Описание
	<hr/>  <b>Примечание</b> Перезагрузите устройство, LED-индикатор питания мигнет 3 раза, удерживайте кнопку сброса в течение 5 секунд. Голосовая подсказка уведомит о результате операции. <hr/> Нажмите кнопку, чтобы переключить режимы STA и Hotspot.
9	Интерфейс питания
10	Переключатель питания
11	Сетевой интерфейс
	Слот для SIM-карты 1
12	<hr/>  <b>Примечание</b> Функция GPRS или 3G / 4G (реализована со встроенным слотом для SIM-карты) зависит от модели устройства. <hr/>
	Слот для SIM-карты 2
13	<hr/>  <b>Примечание</b> Функция GPRS или 3G / 4G (реализована со встроенным слотом для SIM-карты) зависит от модели устройства. <hr/>



## Раздел 2 Запуск устройства

### 2.1 Инициализация устройства

При инициализации устройства с помощью Hik-ProConnector, необходимо добавить охранную панель AX Pro 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.

#### 1. Подключение устройства к сети.

Подключите устройство к сети Ethernet и включите устройство.

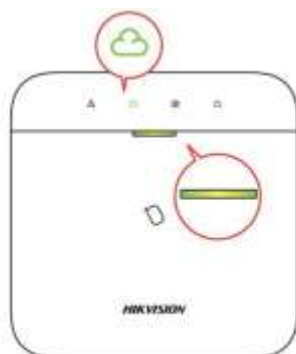


---

#### Примечание

Пока устройство включено, LED-индикаторы питания и связи горят зеленым светом.

---



#### 2. Создание объекта

Откройте 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.

### 3. Добавление устройства

Откройте объект. Нажмите **Add Device** («Добавить устройство») и сканируйте QR-код на этикетке панели.

Охранная панель будет добавлена на объект, 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-ProConnect и в локальный веб-клиент можно войти с использованием учетной записи установщика Hik-ProConnect.

---

#### Примечание

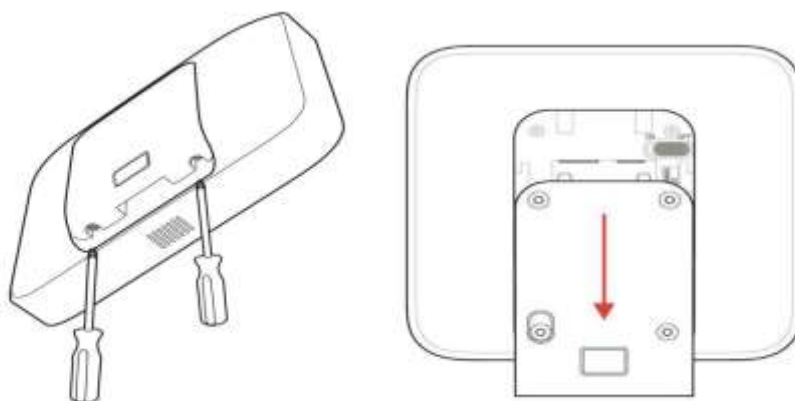
При инициализации устройства с помощью Hik-Connect создание объекта не требуется. Загрузите и войдите в приложение, затем добавьте устройство путем сканирования QR-кода или введите серийный номер устройства вручную.

---

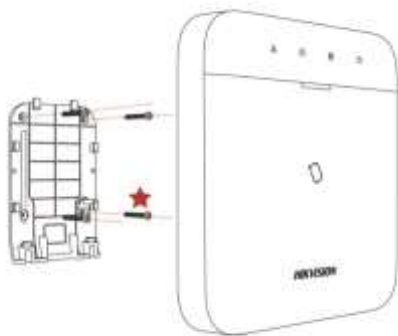
## 2.2 Установка устройства

### Шаги

1. Ослабьте винты на задней крышке, чтобы снять крышку. Сдвиньте заднюю крышку вниз и снимите ее с панели AX PRO.



2. Прикрепите заднюю крышку к месту установки с помощью прилагаемых винтов. Прикрепите панель AX PRO к задней крышке и затяните винты на задней крышке, чтобы завершить установку.



---

### **Примечание**

- «Красная звезда»: винт с защитой от несанкционированного доступа. Закручивать винт с защитой от несанкционированного доступа обязательно.
- Не требуется регулировка.
- Только для использования в охраняемых помещениях.

---

### **Примечание**

Перед подключением и установкой периферийного устройства проверьте уровень радиосигнала. Просмотрите индикатор мощности радиосигнала на периферийном устройстве.

---

## Раздел 3 Управление пользователями

### 3.1 Управление пользователями

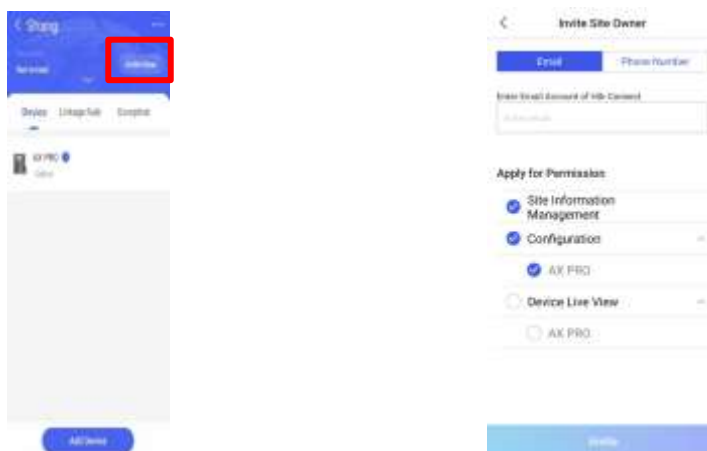
---

#### 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.
- 

#### 3.1.1 Приглашение администратора

Администратор также является владельцем объекта в службе Hik-ProConnect.



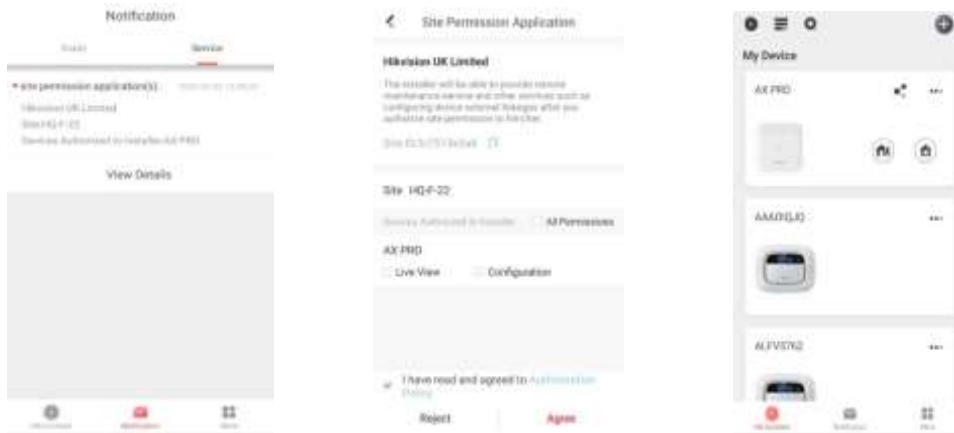
После завершения начальной настройки установщик должен пригласить владельца объекта и запросить разрешение на управление объектом и настройку устройства из учетной записи администратора. Учетная запись администратора будет учетной записью конечного пользователя в службе Hik-Connect.

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.

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.

## Охранная панель AX PRO • Руководство пользователя

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



### 3.1.2 Отмена доступа установщика

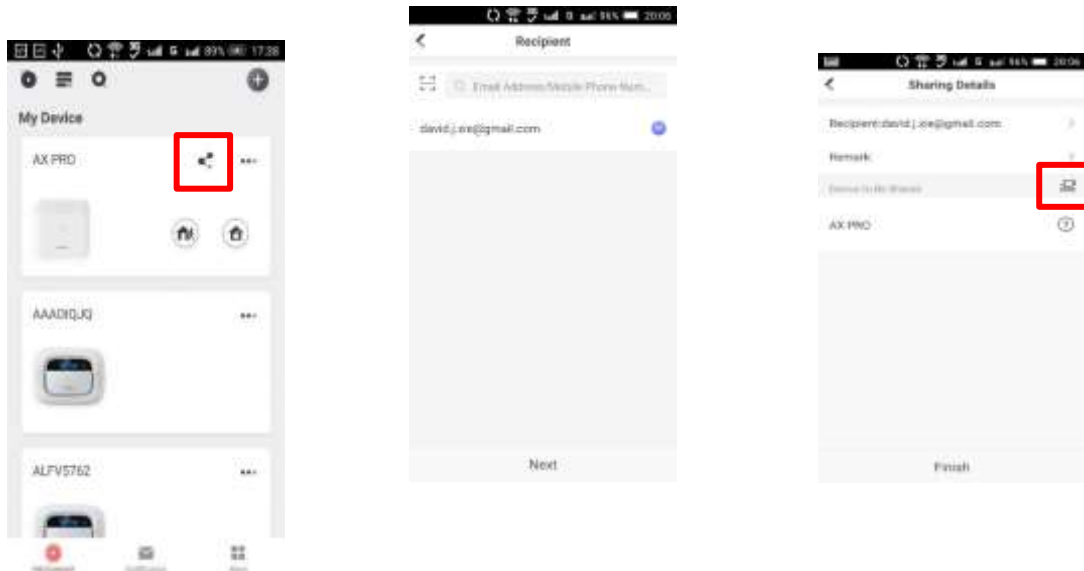
Администратор может отменить авторизацию установщика.


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.

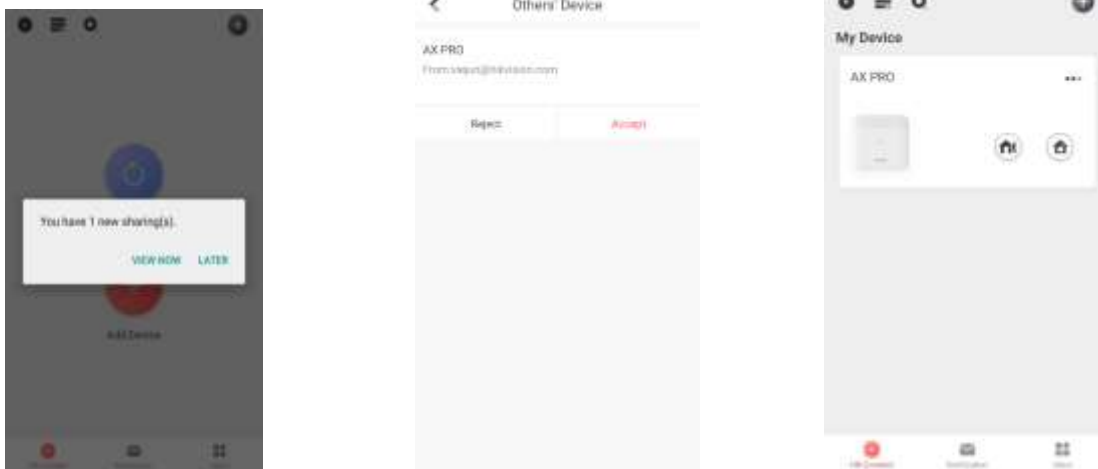


### 3.1.3 Добавление оператора

Администратор может поделиться устройством с другими операторами.



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

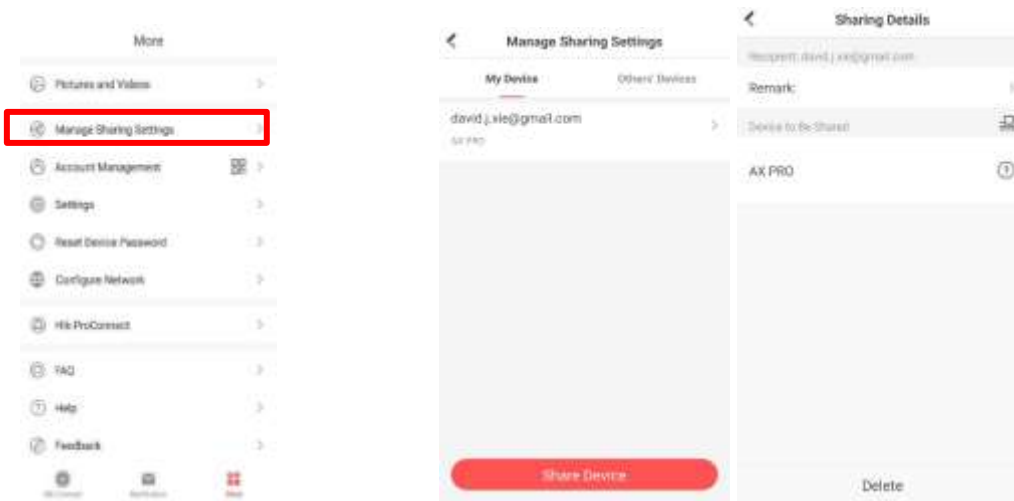
3. Примите приглашение, и устройство появится в списке устройств.

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

### 3.1.4 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.



## 3.2 Журнал доступа

Установщику и операторам AX PRO 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.
- **Передача записей**  
PIN-коды клавиатуры и теги также могут быть назначены установщику на определенном уровне доступа для выполнения ключевых операций.

**Журналы доступа для администратора и операторов (уровень доступа 2)**

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



## Раздел 4 Настройка параметров устройства

### 4.1 Настройка с помощью Hik-Proconnect

#### 4.1.1 Использование приложения Hik-Proconnect

Установщик может использовать Hik-Proconnect для настройки AX PRO, 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 AX PRO.

##### 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 AX PRO в мобильный клиент

Добавьте AX PRO в мобильный клиент перед другими операциями.

##### Шаги

1. Включите охранную панель AX PRO.
2. Создайте или выполните поиск на сайте.
  - Нажмите **+**, задайте название объекта, часовой пояс, адрес, город, страну / область / 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 AX PRO.



##### Примечание

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

---

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 AX PRO

Добавьте периферийное устройство на AX PRO.

#### Шаги

1. Выберите объект.
2. Выберите устройство управления (AX PRO).
3. Нажмите на иконку +.
  - Нажмите **Scan QR Code** («Сканировать QR-код»), чтобы перейти на соответствующую страницу. Сканируйте QR-код на панели периферийного устройства.
  - Нажмите **Manual Adding** («Добавление вручную»), чтобы перейти на соответствующую страницу. Введите серийный номер устройства и проверочный код для добавления устройства.

### Управление пользователями

Установщики (пользователи Nik-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 AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
  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.

### Linked Areas («Настройка привязанной области»)

Если целевой пользователь является оператором, выберите целевого пользователя из списка и нажмите **Linked Areas** («Привязанные области»), чтобы настроить области, привязанные к целевому пользователю.

---

 **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 настроить пароль клавиатуры для пользователя.

### Change Duress Password («Изменение пароля принуждения»)

Если целевой пользователь является администратором, 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 тревогу принуждения.

### 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 AX PRO 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 AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
  2. Нажмите  → **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» («Проведите 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.

---

### Operation Tag («Метки действия»)

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

### Patrol Tag («Патрульные метки»)


Проведите меткой для загрузки записи в систему.

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

### Параметры системы

#### Настройка параметров системы

Настройте часовой пояс и параметры перехода на летнее время.


На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO. Нажмите  → **System** → **Configuration** («Система → Настройки»), чтобы перейти на страницу настроек времени. Нажмите, чтобы выбрать часовой пояс.

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

### Параметры системы

Настройте параметры системы.

#### Управление параметрами

На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO. Перейдите на вкладку  → **System** → **System Options** → **System Management** («Система → Параметры системы → Управление системой») для перехода на соответствующую страницу.

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

Если опция включена и в зоне присутствуют активные неисправности, зона будет исключена автоматически.

#### System Status Report («Отчет о состоянии системы»)

Переключатель загрузки системных отчетов.

#### Voice Prompt («Голосовое предупреждение»)

Если опция включена, панель AX PRO включит текстовое голосовое предупреждение.

#### Audible Tamper Alarm («Тревога тампера»)

Если опция включена, при тревоге саботажа будет срабатывать бипер.

Если опция отключена, периферийные устройства сообщают об открытии крышки, но не выдают тревогу.

#### System Volume («Громкость системы»)

Доступный диапазон громкости системы: от 0 до 10.

#### Panel Lockup Button («Кнопка блокировки панели»)

Если опция включена, установщик может использовать кнопку блокировки, чтобы заблокировать AX PRO. После блокировки пользователи не могут управлять устройством и получать сообщения.

#### Panel Alarm Duration («Длительность тревоги»)

Настройте длительность тревоги на охранной панели.


### **Polling Loss Times («Интервал опроса»)**

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»)**

После обхода зона снова перейдет в режим охраны, если неисправность восстановится.

### **Проверка неисправности**

На странице объекта выберите AX PRO. Перейдите на вкладку  → **System** → **System Options** → **Panel Fault Check** («Система → Параметры системы → Проверка неисправности»).

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

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

### **Battery Fault Check («Проверка неисправности батареи»)**

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

### **LAN Fault Check («Проверка неисправности LAN»)**

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

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

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


### **Cellular Fault Check («Проверка неисправности сотовой сети»)**

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

### **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.

### **Инструкции по настройке параметров системы**

На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO. Нажмите  → **System** → **System Options** → **Arm Options** («Система → Параметры системы → Параметры постановки на охрану»).

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

Если опция включена, при возникновении неисправности во время процедуры постановки на охрану можно остановить постановку на охрану вручную.


### **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.

### **Early Alarm Time («Интервал срабатывания тревоги»)**

Когда функция включена, необходимо настроить интервал срабатывания тревоги. Тревога сработает по истечении заданного времени.


### Режим регистрации

1. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
2. Нажмите  → **System** → **System Options** → **Enrollment Mode** («Система → Параметры системы → Режим регистрации»).
3. Нажмите на иконку **Enter the Enrollment Mode** («Перейти в режим регистрации»).
4. Следуйте инструкциям, чтобы добавить устройство.
5. Нажмите на иконку **Exit the Enrollment Mode** («Выйти из режима регистрации»).

### IP-камера


#### Добавление камер на охранную панель AX PRO

##### Шаги

1. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
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 AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
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»)

Основной поток: используется при записи и предварительном просмотре в формате HD, имеет высокое разрешение, скорость кодированного потока и качество изображения.

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**

1. Настройте расписание для автоматической постановки на охрану / снятия с охраны определенной зоны.
2. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
3. Нажмите  → **Area** («Область») для перехода на соответствующую страницу.
4. Выберите область из списка, включите ее и выберите связанные области.
5. 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 («Время автоматической постановки на 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**

Включите функцию уведомления панели управления в веб-клиенте **Communication Parameters** → **Event Communication** («Параметры связи → Сообщение о событии») перед включением режима задержки снятия с охраны.

---

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

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

### **Weekend Exception («Исключение выходных дней»)**

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

### **Excepted Holiday (Исключение праздничных дней»)**

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.

---




## Настройка параметров связи

### Сотовая сеть передачи данных

Введите краткое описание своей задачи (необязательно).


#### Шаги

1. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
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 **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»).

### Push-уведомления

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


#### Шаги

1. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
2. Перейдите на вкладку  → **Communication Parameters** → **Push Notification(s)** («Параметры связи → Параметры Push-уведомлений»).
3. Нажмите **Phone Call and SMS** («Телефонный вызов и SMS-сообщения»).
4. Нажмите + или + **Add Phone Number** («Добавить номер телефона»), чтобы ввести номер телефона.
5. Выберите добавленный номер телефона, чтобы включить телефонный вызов и SMS-сообщения в соответствии с вашими потребностями.
6. (для телефонного вызова) Настройте **Numbers of Calling** («Номера вызова»).
7. (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»).
8. Проверьте уведомления.

### Пункт централизованного наблюдения (ЧОП / ПЦН)

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

#### Шаги

1. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
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.

### **Тревога зоны / тревога 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.

### **Gas Alarm («Тревога утечки газа»)**

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 AX PRO.

### **Smart Alarm Notification («Уведомления об интеллектуальных тревогах»)**


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

---

### Обслуживание устройства

Перезагрузите устройство при необходимости.

#### Шаги

1. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
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.
3. Нажмите **Maintenance** → **Reboot Device**(«Обслуживание → Перезагрузка устройства»). Панель AX PRO будет перезагружена.


### Управление устройством

Введите краткое описание своей концепции (необязательно). С этого этапа начинается разработка концепции.

#### Зоны

Настройте параметры зоны на соответствующей странице.

#### Шаги

1. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
2. Выберите зону на вкладке **Device** («Устройства»).
3. На начальной странице нажмите  и приступите к аутентификации.
4. Нажмите **Edit** («Изменить») для изменения наименования 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**

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.

Для зоны с задержкой на выходе можно настроить параметры задержки на вход / выход.

#### **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.

#### **24h Silent Panic Zone («Зона беззвучной сигнализации 24 часа в сутки»)**

Данный тип зоны активен 24 часа и используется для устройств экстренного вызова или устройств удержания, не для датчиков дыма или датчиков разбития стекла.

#### **Panic Zone («Зона тревоги»)**

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

#### **Fire Zone («Зона датчиков пожарной сигнализации»)**

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

#### **Gas Zone («Зона датчиков утечки газа»)**

Зона активна все время со звуковым сигналом / звуковым оповещателем при срабатывании тревоги. Обычно он используется в помещениях, оборудованных детекторами утечки газа (например, на кухне).

#### **Medical Zone («Зона медицинской деятельности»)**

Зона активна все время со звуковым сигналом / звуковой оповещателем при срабатывании тревоги. Обычно используется в местах, оборудованных тревожными кнопками.

#### **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).

#### **Key Zone («Ключевая зона»)**

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.

#### **Disabled Zone («Зона отключенного предупреждения»)**

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

6. Включите функции: **Stay Arm Bypass** («Частичная охрана»), **Chime** («Сигнал»), **Double Knock** («Двойное срабатывание»), **Silent Alarm** («Зона беззвучной сигнализации») и другие функции в соответствии с фактическими потребностями.



### Примечание


- Некоторые модели не поддерживают эту функцию. Опирайтесь на характеристики конкретной зоны.
- Зоны разных типов имеют разные параметры.

7. Настройте частоту опроса.
8. Опционально: нажмите **Delete** («Удалить»), чтобы удалить устройство.

### Клавиатура

Настройте параметры клавиатуры, зарегистрированной в панели AX PRO.


#### Шаги

1. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
2. Выберите клавиатуру на вкладке устройств.
3. На начальной странице нажмите  и приступите к аутентификации.
4. Нажмите **Edit** («Изменить») для изменения наименования клавиатуры.
5. Поставьте галочку **Enable Keyfob** («Включить клавиатуру»).
6. Выберите привязанных пользователей.
7. Нажмите на вкладку **Function Key Settings** («Настройки функциональных клавиш»), чтобы настроить функции для отдельных и комбинированных клавиш.
8. Опционально: нажмите **Delete** («Удалить»), чтобы удалить устройство.

### Звуковой оповещатель


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

#### Шаги

1. На странице объекта, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
2. Выберите звуковой оповещатель на вкладке устройств.
3. На начальной странице нажмите  и приступите к аутентификации.
4. Нажмите **Edit** («Изменить») для изменения наименования звукового оповещателя.
5. Выберите привязанные области.
6. Настройте время срабатывания и громкость тревоги.
7. Включите LED-индикатор постановки на охрану / снятия с охраны, бипер постановки на охрану / снятия с охраны, индикатор тревоги в соответствии с фактическими потребностями.
8. Настройте цикл Heartbeat.
9. Опционально: нажмите **Delete** («Удалить»), чтобы удалить устройство.

#### 4.1.2 Использование портала Hik-ProConnect






Для охранной панели AX Pro 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 AX Pro) и переключить настройки языка в панели AX Pro.

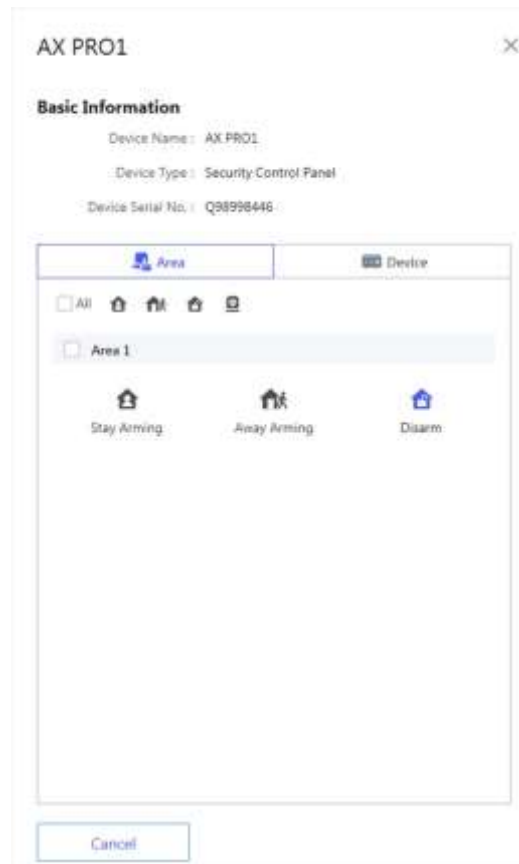
Нажмите вкладку  **Site** («Объекты») для перехода на страницу списка объектов, затем выберите наименование объекта, чтобы перейти на страницу сведений об объекте.

### **Удаленное управление AX Pro**


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

**Таблица 4-3 Описание операции**

	<b>Описание операции</b>
Частичная охрана определенной зоны	Выберите вкладку <b>Area</b> («Область»), затем нажмите <b>Stay Arming</b> («Частичная охрана»), чтобы поставить область на частичную охрану.
Полная охрана определенной области	Выберите вкладку <b>Area</b> («Область»), затем нажмите <b>Away Arming</b> («Полная охрана»).
Снятие охраны с определенной области	Выберите вкладку <b>Area</b> («Область»), затем нажмите <b>Disarm</b> («Снятие с охраны»).
Частичная охрана нескольких областей	Выберите вкладку <b>Area</b> («Область»), затем выберите области и нажмите  .
Полная охрана нескольких областей	Выберите вкладку <b>Area</b> («Область»), затем выберите области и нажмите  .
Снятие нескольких областей с охраны	Выберите вкладку <b>Area</b> («Область»), затем выберите области и нажмите  .
Отключение тревожных уведомлений нескольких областей	Выберите вкладку <b>Area</b> («Область»), затем выберите области и нажмите  .
Фильтр периферийного устройства по области	Выберите вкладку <b>Device</b> («Устройство»), затем нажмите  и выберите область, чтобы отображались только периферийные устройства, связанные с выбранной областью, или выберите <b>All</b> («Все»), чтобы отобразить все периферийные устройства, связанные со всеми областями.
Управляющее реле	Перейдите на вкладку <b>Device</b> («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 <b>Device</b> «Устройство», затем выберите зону (например, датчик) и <b>Bypass</b> («Обход»), чтобы обойти зону.



### Удаленная настройка AX Pro

Нажмите  для перехода в веб-интерфейс охранной панели и настройки параметров устройства.

---

#### Примечание

Подробная информация о настройке параметров охранной панели представлена в руководстве пользователя устройства.

---

### Подача заявки на получение PIN-кода

Нажмите  → , чтобы открыть окно **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.

---

Нажмите **• • •** → , чтобы открыть окно **Language** («Язык»), затем настройте язык на устройстве и введите PIN-код.

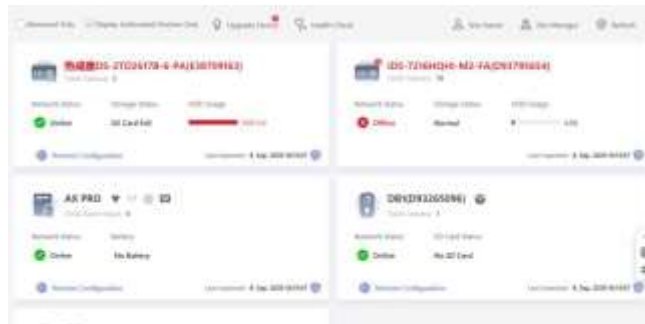


### Мониторинг состояния

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

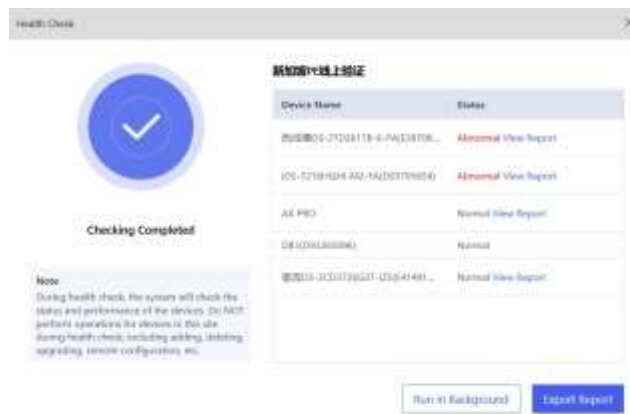


2. Выберите объект.



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.

## 4.2 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 AX PRO.

#### 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 AX PRO в мобильный клиент

Добавьте охранную панель AX PRO в мобильный клиент перед другими операциями.

#### Шаги

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

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







#### Примечание

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

---

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

3. Нажмите , чтобы выполнить поиск на устройстве.
4. Нажмите **Add** («Добавить») на странице результатов.
5. Введите проверочный код и нажмите **OK**.
6. После завершения добавления введите псевдоним устройства и нажмите **Save** («Сохранить»).
7. Опционально: нажмите  → **Delete** («Удалить»), чтобы удалить устройство.
8. Опционально: нажмите  → , чтобы изменить имя устройства.

### Добавление периферийных устройств на AX PRO

Добавьте периферийное устройство на AX PRO.



#### Шаги

1. Выберите устройство управления (AX PRO).
2. Нажмите +.
  - Нажмите **Scan QR Code** («Сканировать QR-код»), чтобы перейти на соответствующую страницу. Сканируйте QR-код на панели периферийного устройства.
  - Нажмите **Manual Adding** («Добавление вручную»), чтобы перейти на соответствующую страницу. Введите серийный номер устройства и проверочный код для добавления устройства.

### Управление картами / метками

После добавления карт / меток в AX PRO 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 AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
2. Нажмите  → **User Management** → **Card / Tag** («Управление пользователями → Карты / метки»), чтобы перейти на страницу / метками.
3. Нажмите + для добавления карты / метки.
4. Услышав голосовую подсказку «Swipe Tag» («Проведите 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.

---

#### **Operation Tag («Метки действия»)**

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

#### **Patrol Tag («Патрульные метки»)**

Проведите меткой для загрузки записи в систему.

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

### 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 AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
2. Нажмите  для перехода на страницу настроек общего доступа.
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 управления пользователями.
7. 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.

#### **Linked Areas** («Привязанные области»)

Если целевой пользователь является оператором, выберите целевого пользователя из списка и нажмите **Linked Areas** («Привязанные области»), чтобы настроить области, привязанные к целевому пользователю.

### **Примечание**

#### **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 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. Эти правила применяются для каждого пользователя.

**Change Duress Password («Изменение пароля принуждения»)** Если целевой пользователь является администратором, 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 тревогу принуждения.

**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.

---

8. Опционально: (опция доступна только для администратора) нажмите + для добавления пользователя.


## **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 AX PRO 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.

Датчик не будет обнаруживать тревоги и отправлять уведомления о тревогах пользователю.





### Постановка на охрану / снятие с охраны

При необходимости можно поставить область на охрану или снять область с охраны. На странице списка устройств, выберите панель AX PRO 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.
- **Disarm** («Снятие с охраны»): нажмите значок **Away Arming** («Снятие с охраны»), чтобы снять область с охраны. В режиме снятия с охраны тревога в зонах области не будет срабатывать, в том числе при обнаружении тревожных событий.

#### Операции во всех зонах

- **Away** («При выходе»): нажмите , чтобы активировать режим охраны всех областей 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** («При пребывании посетителей»): 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, PIR-датчики). Тревога не сработает при перемещении посетителей внутри зоны.
- **Disarm** («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.
- **Silence Alarm** («Отключение тревожных уведомлений»): нажмите , чтобы отключить тревожные уведомления для всех областей. Здесь можно очистить все тревоги, вызванные зонами области.

### 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.

### Wi-Fi-соединение

Подключите охранную панель AX PRO к Wi-Fi через приложение.

### Шаги


1. На странице списка устройств, выберите AX PRO и выполните вход в систему (при необходимости), чтобы перейти на страницу настроек AX PRO.
2. Нажмите  → **Configure Wi-Fi Network** («Настройка сети Wi-Fi»).
3. Следуйте приведенным ниже инструкциям, чтобы переключить AX PRO 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»).

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

### Обслуживание устройства

Перезагрузите устройство при необходимости.

#### Шаги

- На странице списка устройств, выберите панель AX PRO и выполните вход в систему (при необходимости), чтобы перейти на соответствующую страницу.
- Нажмите  → **Maintenance** → **Reboot Device** («Обслуживание → Перезагрузка устройства»). Панель AX PRO будет перезагружена.

## 4.3 Настройка параметров с помощью веб-клиента

#### Шаги

- Подключите устройство к Ethernet.
- Найдите IP-адрес устройства с помощью клиентского ПО и ПО SADP.
- Введите найденный IP-адрес в адресную строку.



#### Примечание

- При использовании мобильного браузера IP-адрес по умолчанию: **192.168.8.1**.
- При прямом подключении сетевого кабеля к компьютеру IP-адрес по умолчанию: 10.22.98.113.

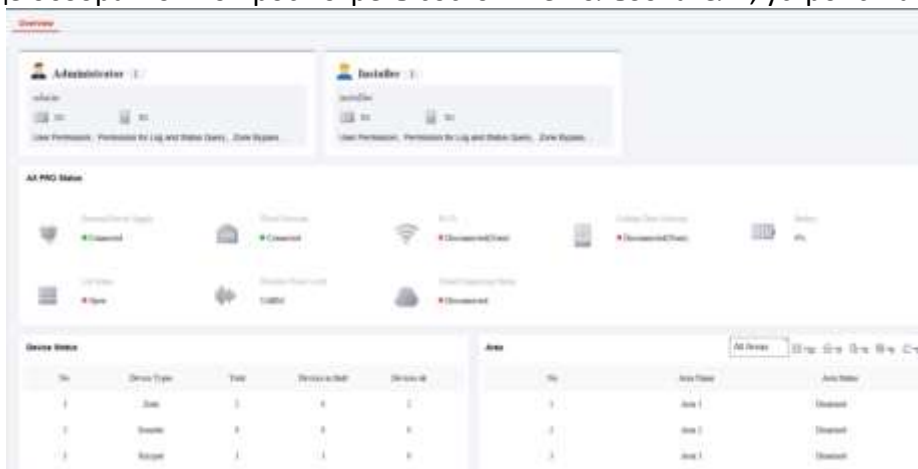
- Для входа используйте имя пользователя и пароль активации.



#### Примечание

- Подробная информация приведена в разделе *Активация*.
- Вход в веб-клиент доступен только администраторам и установщикам.

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





### 4.3.1 Настройки связи

#### Проводная сеть

Настройте IP-адрес устройства и другие параметры сети.

#### Шаги

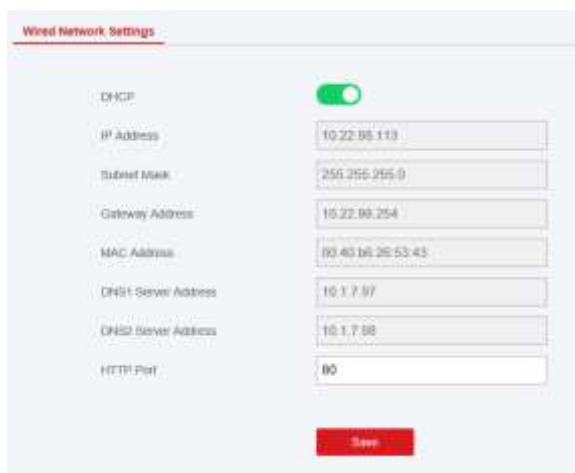
---

##### 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 → Сеть Wi-Fi»).

## Охранная панель AX PRO • Руководство пользователя

Status of STA/AP Swit...

Switch Mode: STA Mode

Wi-Fi

SSID Wi-Fi: NETGEAR01

Wi-Fi Password: [Empty]

Encryption Mode: WPA2-personal

Network List

Name	Channel	Signal S.	Encryption Mode	Operative
NETGEAR01	11	35	WPA2-personal	Disconnect
HAP_Q02731701	11	70	WPA2-personal	Connect
HAP_Q01790103	11	60	WPA2-personal	Connect
HAP_Q02030875	11	39	WPA2-personal	Connect
HUAWEI-B011-8E54	8	89	WPA2-personal	Connect
HAP_Q01877075	11	58	WPA2-personal	Connect
HAP_Q58895531	11	56	WPA2-personal	Connect

Save

### 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. Выберите **WLAN**, чтобы перейти на страницу WLAN.

Wi-Fi Settings: **WLAN**

DHCP:

IP Address: 192.168.1.28

Subnet Mask: 255.255.255.0

Gateway Address: 192.168.1.1

MAC Address: ac:9c:32:5a:43:40

DNS1 Server Address: 192.168.1.1

DNS2 Server Address: [Empty]

Save

### 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

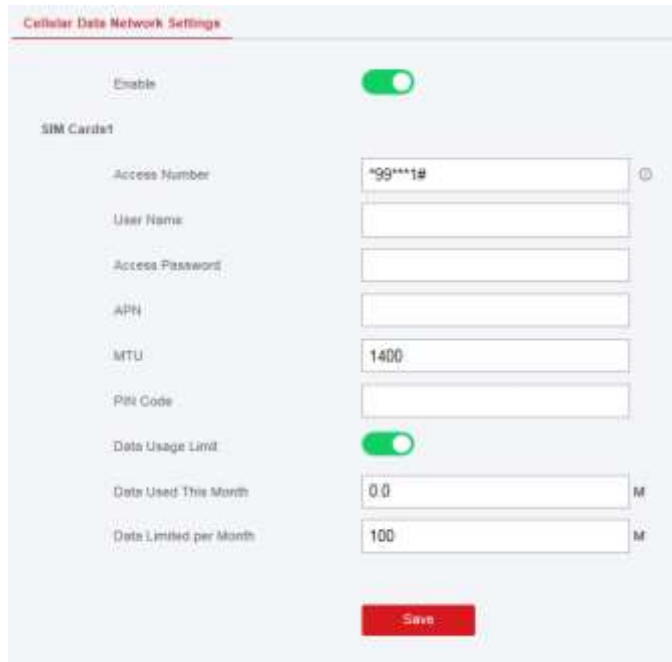
Настройте параметры сотовой сети, если используется SIM-карта. Используя сотовую сеть, устройство может загружать уведомления о тревожных событиях в центр тревог.

#### Перед началом

Вставьте SIM-карту в слот для SIM-карты.

#### Шаги

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



Cellular Data Network Settings

Enable

SIM Cardset

Access Number \*99\*\*\*1# ⓘ

User Name

Access Password

APN

MTU 1400

PIN Code

Data Usage Limit

Data Used This Month 0.0 M

Data Limited per Month 100 M

Save

2. Поставьте галочку **Wireless Dial** («Беспроводная связь»).

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.

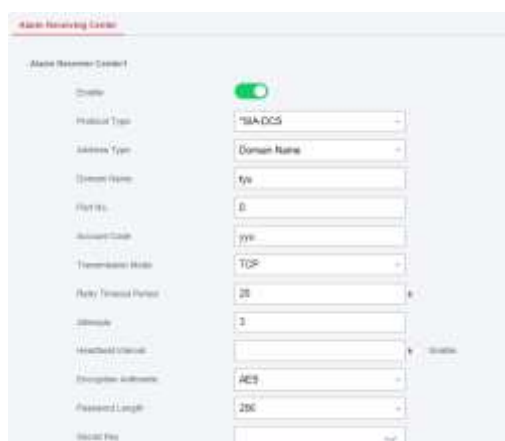
4. Нажмите **Save** («Сохранить»).

### **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 центр тревог для настройки параметров и сдвиньте ползунок, чтобы активировать выбранный центр тревог.
- 

 **Примечание**

Если активирован центр тревог 1, можно настроить центр тревог 2 для резервного копирования и редактирования параметров канала.

---

3. Выберите **Protocol Type**(«Тип протокола»): **ADM-CID, ISUP, SIA-DCS, \*SIA-DCS** или **\*ADM-CID**, 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 центра тревог: по IP-адресу или доменному имени и введите IP-адрес / доменное имя, номер порта, код учетной записи, время ожидания, время повторной загрузки и интервал подтверждения.

---

 **Примечание**

Настройте цикл Heartbeat в диапазоне от 10 до 3888000 секунд.

---

**ISUP**: нет необходимости настраивать параметры протокола ISUP.

**\*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, период ожидания повторной попытки, попытки, цикл Heartbeat, параметры шифрования, длину пароля и секретный ключ.

---

 **Примечание**

Настройте цикл Heartbeat в диапазоне от 10 до 3888000 секунд.

Для параметров шифрования: панель поддерживает формат шифрования для защиты информации в соответствии с DC-09, AES-128, AES-192 и AES-256 поддерживаются при настройке центра тревог (ЧОП / ПЦН).

Для секретного ключа: если используется зашифрованный формат DC-09, ключ должен быть установлен при настройке ЧОП / ПЦН. ЧОП / ПЦН выдаст ключ в автономном режиме, который будет использоваться для шифрования сообщений в целях обеспечения безопасности.

---

3. Нажмите **Save** («Сохранить»).

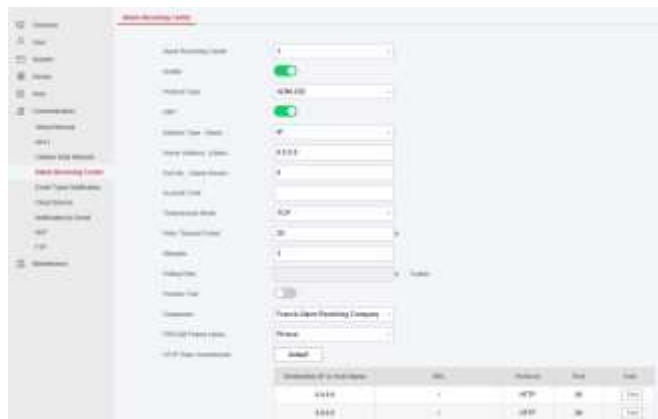
### **Примечание**

Включите функцию PIRCAM для загрузки изображений или видео.

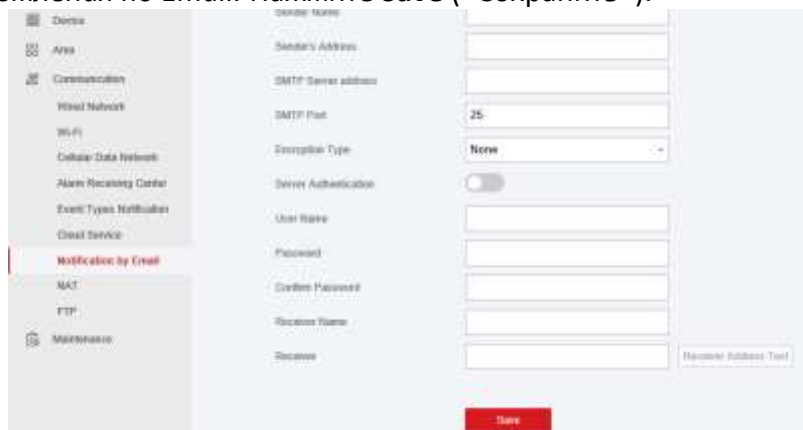
#### 1. Загрузка изображений

Можно загрузить от 1 до 20 изображений.

- (1) Нажмите **Communication** → **Alarm Receiving Center**(«Связь → Центр тревог»), чтобы перейти на страницу Центра тревог.
- (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 центра тревог»).
- (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»).



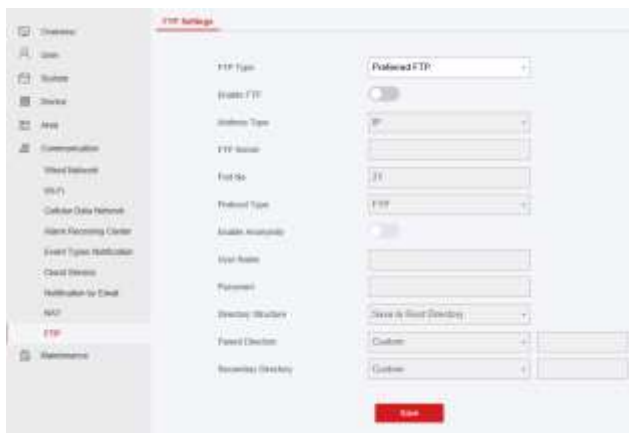
## Охранная панель AX PRO • Руководство пользователя

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.

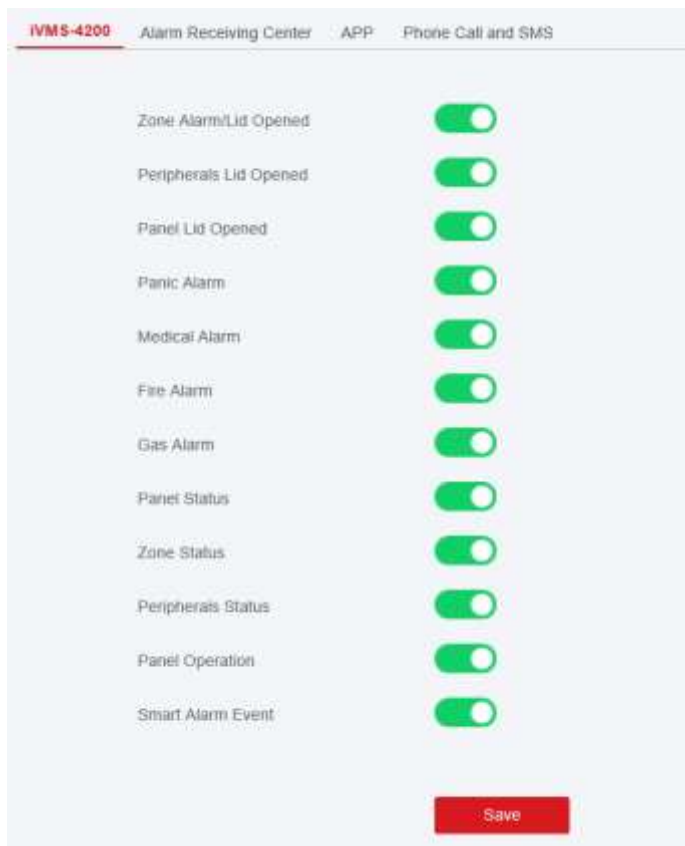
- (1) Нажмите **Communication** → **Alarm Receiving Center** («Связь → Центр тревог») для перехода на страницу центра тревог.
- (2) Сдвиньте ползунок, чтобы включить выбранный центр тревог.
- (3) Выберите **Protocol Type** («Тип протокола»): **SIA-DCS**.
- (4) Нажмите **Save** («Сохранить»).
- (5) Настройте параметры SM TP или FTP аналогично параметрам загрузки фотографий.

## 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.

#### **Примечание**

Чтобы уведомления о тревоге отправлялись в мобильный клиент, следует настроить **Mobile Phone Index** («Индекс мобильного телефона»), **Mobile Phone Number** («Номер мобильного телефона») и поставить галочку **Notification Type** («Тип уведомления»).

#### **Примечание**

Для уведомления о сообщениях в центре тревог выберите индекс центра перед остальными настройками.

### 3. Нажмите **Save** («Сохранить»).



**Результат**

**Таблица 4-1 Параметры уведомлений**

Опционально	Уведомление
iVMS-4200	<p>Тревога зоны и тревога открытия крышки</p> <p>Крышка беспроводного устройства открыта</p> <p>Уведомления о несанкционированном доступе</p> <p>Уведомления о тревоге экстренного вызова</p> <p>Уведомления о тревоге экстренной медицинской помощи</p> <p>Уведомления о тревоге утечки газа</p> <p>Уведомления о пожарной тревоге</p> <p>Уведомления об управлении панелью</p> <p>Уведомления о состоянии системы</p> <p>Уведомления о состоянии датчика</p>
Центр тревог (ЧОП / ПЦН)	<p>Центр тревог 1 и 2 зоны</p> <p>Тревога зоны и тревога открытия крышки</p> <p>Крышка беспроводного устройства открыта</p> <p>Уведомления о несанкционированном доступе</p> <p>Уведомления о тревоге экстренного вызова</p> <p>Уведомления о тревоге экстренной медицинской помощи</p> <p>Уведомления о тревоге утечки газа</p> <p>Уведомления о пожарной тревоге</p> <p>Уведомления об управлении панелью</p> <p>Уведомления о состоянии системы</p> <p>Уведомления о состоянии датчика</p> <p>Уведомления о статусе беспроводного устройства</p>
Облачный сервис	<p>Тревога зоны и тревога открытия крышки</p> <p>Крышка беспроводного устройства открыта</p> <p>Уведомления о несанкционированном доступе</p> <p>Уведомления о тревоге экстренного вызова</p> <p>Уведомления о тревоге экстренной медицинской помощи</p>

## Охранная панель AX PRO • Руководство пользователя

Опционально	Уведомление
	Уведомления о тревоге утечки газа Уведомления о пожарной тревоге Уведомления об управлении панелью Уведомления о состоянии системы Уведомления о состоянии датчика Уведомления о статусе беспроводного устройства
Мобильный телефон	Индекс мобильного телефона от 1 до 8 Номер мобильного телефона Тип уведомления SMS и голосовой вызов Тревога зоны и тревога открытия крышки (настройка времени фильтрации) Крышка беспроводного устройства открыта Уведомления о несанкционированном доступе Уведомления о тревоге экстренного вызова Уведомления о тревоге экстренной медицинской помощи Уведомления о тревоге утечки газа Уведомления о пожарной тревоге Уведомления об управлении панелью Уведомления о состоянии системы Уведомления о состоянии датчика Уведомления о статусе беспроводного устройства

### Примечание

Для отправки уведомлений на мобильный телефон:

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

### Облачный сервис

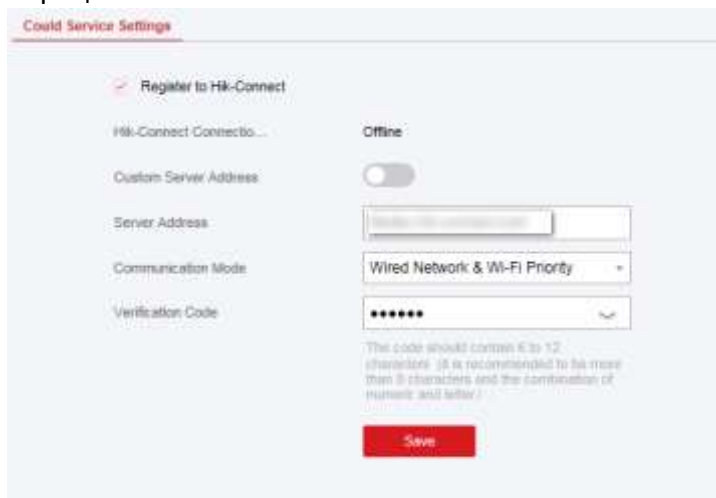
Чтобы зарегистрировать устройство в мобильном клиенте для удаленной настройки, необходимо предварительно настроить параметры регистрации мобильного клиента.

### 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](http://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.

#### **Auto** («Автоматический»)

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.

#### 5. Опционально: измените пароль аутентификации.

---

##### **Примечание**

- По умолчанию в текстовом поле отображается пароль аутентификации.
  - Пароль аутентификации 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. 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. Нажмите на блок, чтобы включить функцию об отправке события видеоверификации.
  3. 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.

---

#### 4. Введите информацию о получателе.

#### 5. Нажмите **Receiver Address Test** («Проверка адреса получателя») и проверьте корректность адреса.

#### 6. Нажмите **Save** («Сохранить»).

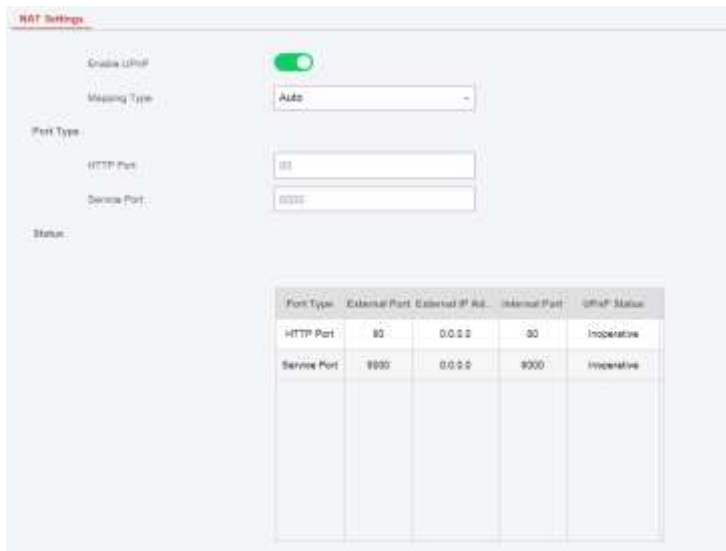
### NAT

Universal Plug and 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 **Port Mapping Type** («Тип проброса портов»): **Manual** («Вручную»).
4. Настройте порт HTTP и порт службы.
5. 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.

#### FTP Protocol («Протокол FTP»)

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.

## 4.3.2 Управление устройством

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»).



2. Выберите зону и нажмите **Edit** («Редактировать»), чтобы перейти на страницу настройки параметров 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. При необходимости можно настроить задержку включения режима ожидания для зоны отсроченного срабатывания.

### **Panic Zone («Зона тревоги»)**

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

### **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 работает.

---

#### **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 игнорировано. 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.

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.

---

7. Задайте **Sounder Delay Time**(«**Время задержки звукового оповещателя**»). Звуковой оповещатель сработает сразу или по истечении установленного времени.
8. При необходимости привяжите камеру к зоне.
9. Нажмите **ОК**.


### **Примечание**

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

## **Звуковой оповещатель**

Звуковой оповещатель регистрируется в панели AX PRO через модуль беспроводного приемника, а беспроводной звуковой оповещатель с частотой 868 МГц может быть зарегистрирован в гибридной панели AX PRO 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.

Sounder	<input type="text" value="1"/>
Name	<input type="text" value="Sounder 1"/>
Volume	<input type="text" value="2"/>
Enroll Wireless Sounder	<input checked="" type="checkbox"/>
Serial No.	<input type="text" value="Q00007031"/>
Area	<div><input checked="" type="checkbox"/> Active Functions <input checked="" type="checkbox"/> Area1 <input checked="" type="checkbox"/> Area2 <input checked="" type="checkbox"/> Area3</div>
Sounder Type	<input type="text" value="Internal"/>
Alarm LED Indicator	<input checked="" type="checkbox"/>
Alarm Buzzer	<input checked="" type="checkbox"/>
Arm/Disarm LED Indicator	<input checked="" type="checkbox"/>



## Охранная панель AX PRO • Руководство пользователя

Polling Rate	<input type="text" value="5min"/>
Alarm Duration	<input type="text" value="90"/> s

3. Задайте название и громкость оповещателя.

### **Примечание**

Доступный диапазон громкости оповещателя: от 0 до 3 (функция зависит от модели устройства).

4. Поставьте галочку **Enroll Wireless Sounder**(«Зарегистрировать беспроводной оповещатель») и настройте серийный номер оповещателя.

5. Выберите связанную область.

### **Примечание**

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

6. Включите LED-индикатор постановки на охрану / снятия с охраны, бипер постановки на охрану / снятия с охраны, индикатор тревоги и т.д.

7. Настройте **Polling Rate** («Частота опроса») и **Alarm Duration** («Длительность тревоги»).

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 AX PRO.

### **Шаги**

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



3. Задайте наименование зоны.
4. Поставьте галочку, чтобы включить функцию зуммера, беззвучную сигнализацию экстренного вызова, беззвучную сигнализацию тревоги экстренной медицинской помощи и кнопки клавиатуры.
5. Поставьте галочку, чтобы включить функцию постановки на охрану без пароля.
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 оповещателя, перейдите на вкладку **Maintenance** → **Device Status** → **Keypad Status** («Обслуживание → Состояние устройства → Состояние клавиатуры»), для просмотра статуса клавиатуры.
- Настройте пароль клавиатуры на странице **User** → **User Management** → **Operation** («Пользователь → Управление пользователями → Операции»).

## Автоматизация

Настройте параметры релейных выходов, зарегистрированных в панели AX PRO.

### 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 релейного устройства.
3. Нажмите , чтобы изменить информацию о реле.

Event Type	Parameter Setting
<input type="checkbox"/> Alarm	Activation Mode: Pulse
<input type="checkbox"/> Schedule	Pulse Duration: 5
<input type="checkbox"/> Ann	
<input type="checkbox"/> Alarm	
<input type="checkbox"/> Silence Alarm	
<input type="checkbox"/> Fault	
<input checked="" type="checkbox"/> Manual	

## Охранная панель AX PRO • Руководство пользователя

- 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 частоту опроса.
  - Активируйте или снимите защиту от скачков напряжения / тока.
  - Настройте событие для срабатывания.
  - Настройте 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.

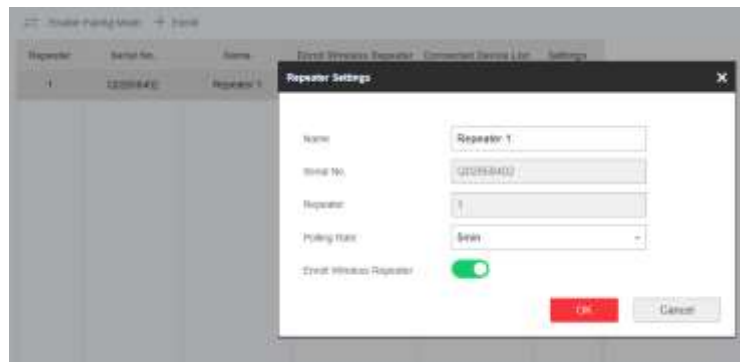
### Шаги

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 Pairing 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.

## Охранная панель AX PRO • Руководство пользователя



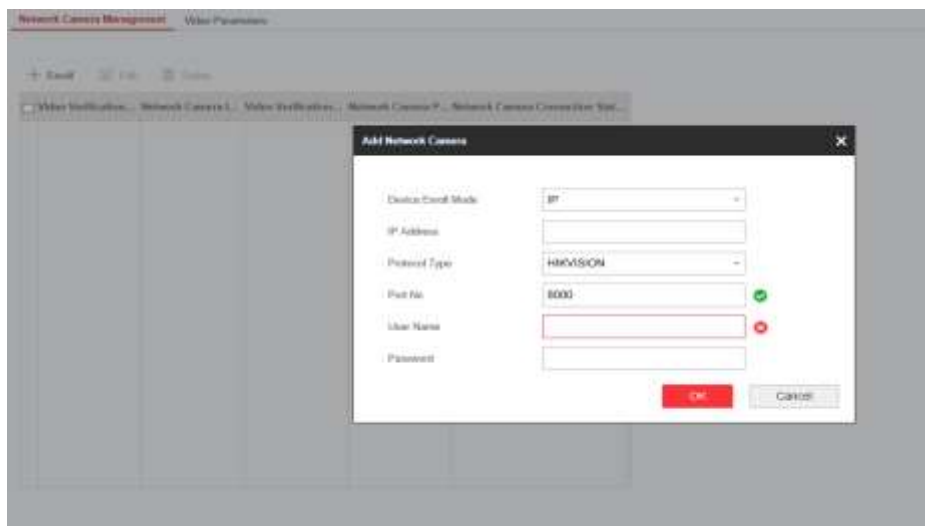
- Задайте наименование ретранслятора.
- Настройте частоту опроса ретранслятора.
- Активируйте или отмените регистрацию ретранслятора. Если привязка активна, устройство будет удалено.



### 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.



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

### 4.3.3 Настройки области

#### Настройка основных параметров

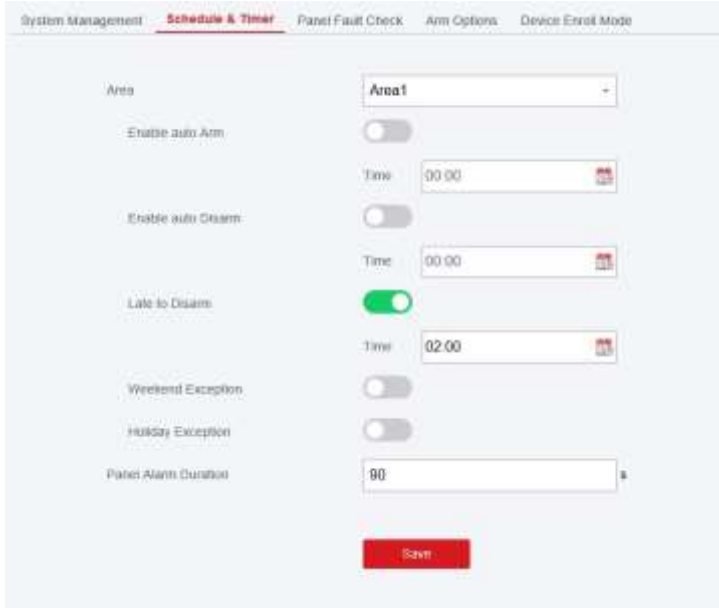
Зоны можно привязать к выбранной области.

##### 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. Поставьте галочку напротив зоны, чтобы выбрать зоны для конкретной области.
5. Нажмите **Save** («Сохранить»), чтобы завершить настройку.

#### Расписание тревог и настройки таймера

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



The screenshot displays the 'Schedule & Timer' configuration page. At the top, there are navigation tabs: 'System Management', 'Schedule & Timer' (selected), 'Panel Fault Check', 'Arm Options', and 'Device Enroll Mode'. The main content area is divided into two columns. The left column lists various settings: 'Area' (set to 'Area1'), 'Enable auto Arm' (disabled), 'Enable auto Disarm' (disabled), 'Late to Disarm' (enabled), 'Weekend Exception' (disabled), 'Holiday Exception' (disabled), and 'Panel Alarm Duration' (set to 90). The right column contains input fields for 'Time' (00:00), 'Time' (00:00), and 'Time' (02:00), each with a calendar icon. A red 'Save' button is located at the bottom center of the page.

##### 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.
  - Если открыта зона общего пользования, зона 1 не поддерживает автоматическую постановку на охрану.
- 

### **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.
  - Если открыта зона общего пользования, зона 1 не поддерживает автоматическое снятие с охраны.
- 

### **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**

Включите функцию уведомления панели управления в веб-клиенте **Communication Parameters → Event Communication** («Параметры связи → Сообщение о событии») перед включением режима задержки снятия с охраны.

---

### **Weekend Exception («Исключения в выходные дни»)**

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.

---

### **Panel Alarm Duration («Длительность тревоги»)**

Длительность тревоги на охранной панели.

### **Примечание**

Доступный диапазон длительности тревоги: от 10 до 900 с.

5. Нажмите **Save** («Сохранить»).

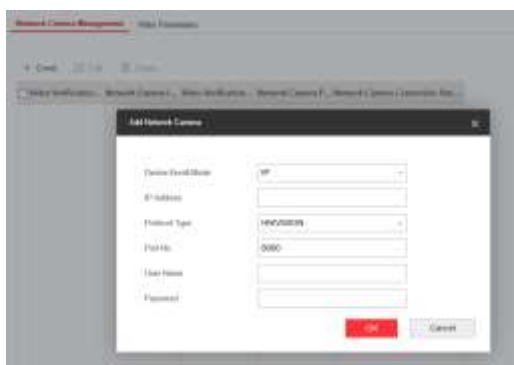
### **4.3.4 Управление видео**

В охранную панель AX PRO 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 AX PRO**

#### **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.

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 **Panel Video Channel No.** («Номер видеоканала панели»).

4. Нажмите **OK**.





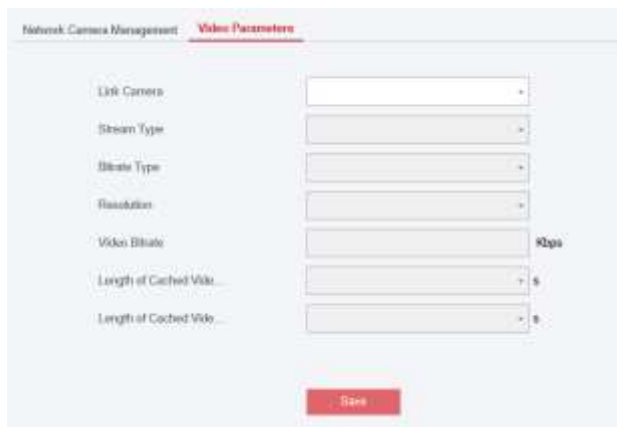
### Примечание

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»)

Основной поток: используется при записи и предварительном просмотре в формате HD, имеет высокое разрешение, скорость кодированного потока и качество изображения.

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.

### **4.3.5 Управление разрешениями**

#### **Добавление / изменение / удаление брелока**

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

##### **Шаги**

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

##### **Name («Наименование»)**

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  для редактирования информации 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 AX PRO и используйте ее для постановки на охрану / снятия зоны с охраны.

Также можно редактировать информацию о метке или удалить ее из панели AX PRO.

---



##### **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 AX PRO.
  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**, и 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.

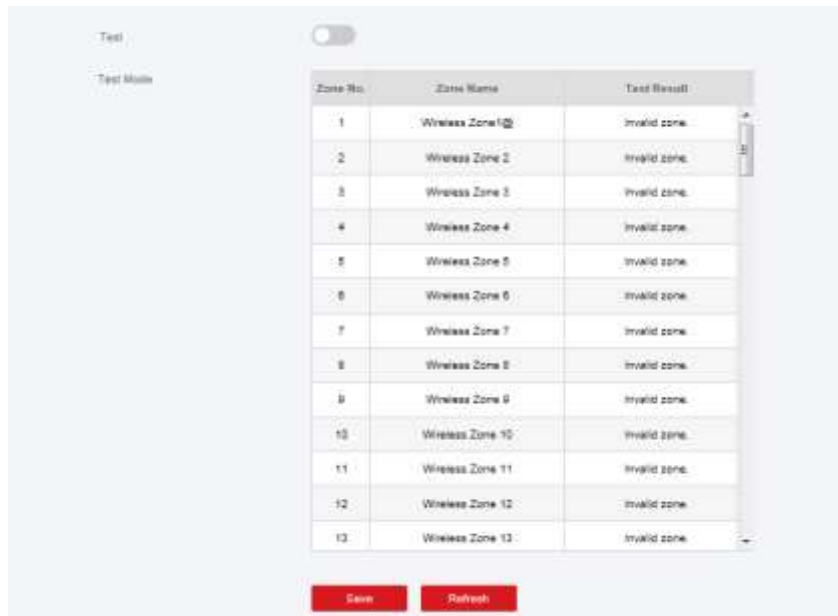
## 4.3.6 Техническое обслуживание

### Диагностика

Охранная панель AX PRO 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.

---

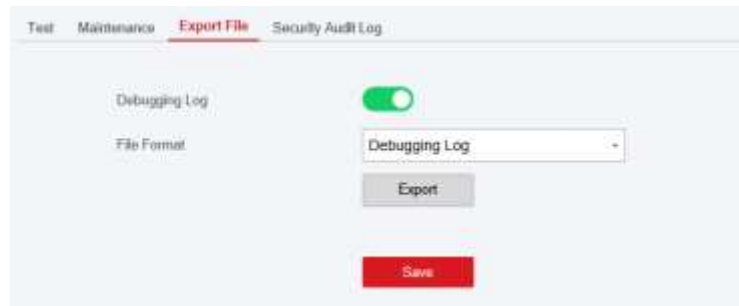
2. Поставьте галочку **Test** («Диагностика»), чтобы запустить диагностику.
3. Нажмите **Save** («Сохранить»), чтобы завершить настройку.
4. Включите датчики в каждой зоне.
5. После этого можно просмотреть результаты диагностики.

### **Экспорт файлов**

Файл отладки можно экспортировать на ПК.

#### **Шаги**

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



2. Поставьте галочку для включения функции.

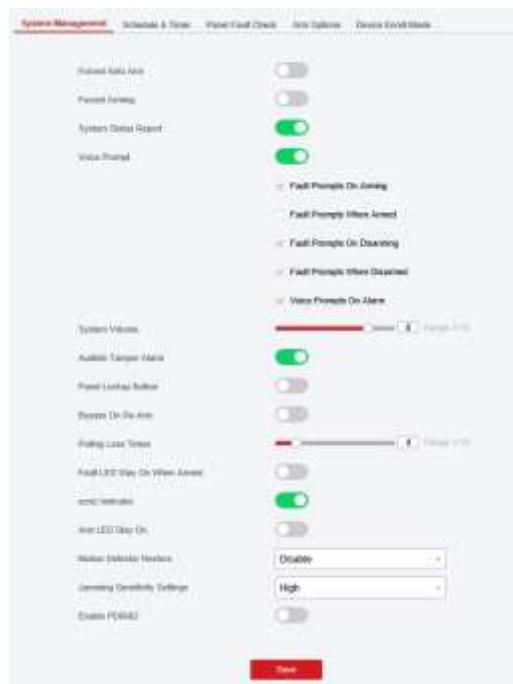
3. Нажмите **Export** («Экспортировать»), чтобы сохранить файл отладки на ПК.

### 4.3.7 Настройка системы

#### 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. В противном случае функция постановки на охрану AX PRO при наличии неисправностей может быть недействительной.

---

### **System Status Report («Отчет о состоянии системы»)**

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

### **Voice Prompt («Голосовое предупреждение»)**

Если опция включена, панель AX PRO включит текстовое голосовое предупреждение.

### **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.

### **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»)**

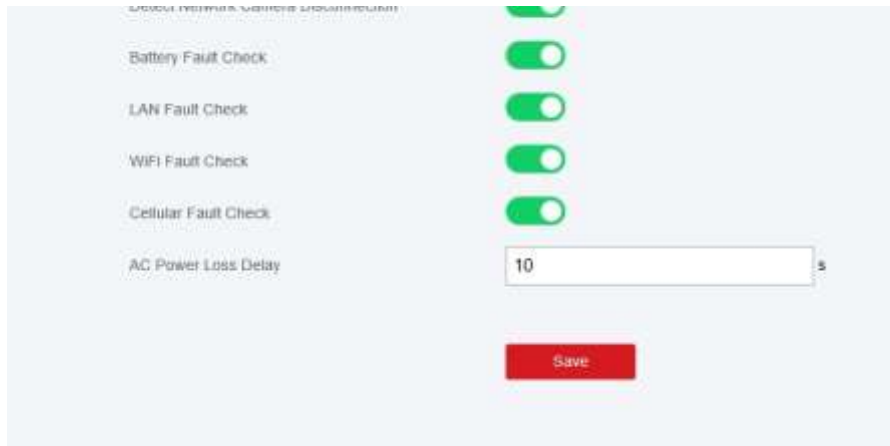
Настройте максимальную продолжительность интервала опроса. Система сообщит о неисправности, если продолжительность превышает установленное значение.

## **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** → **Panel Fault Check** («Система → Параметры системы → Проверка неисправности»).

## Охранная панель AX PRO • Руководство пользователя



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

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

### **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, при разрыве или сбоях проводной сети сработает тревога.

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

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

### **Cellular Fault Check («Проверка неисправности сотовой сети»)**

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

### **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.

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

	Checklist	Arm With Fault
Device Lid Opened	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zone/Peripherals Poll Failure/Offline	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Zone/Peripherals Low Battery	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Zone Triggered	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Main Power Lost	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Communication Fault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Early Alarm:

Early Alarm Time:  s

Также можно настроить следующие параметры:

### **Enable Arming with Fault («Включить постановку на охрану при обнаружении неисправности»)**

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.

### **Enable 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.



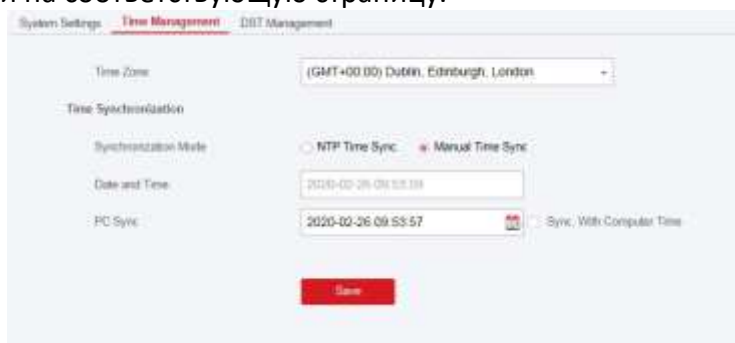


### Настройки времени

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

### Настройки времени

Нажмите **System** → **System Settings** → **Time** («Система → Параметры системы → Время»), 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 компьютера»), чтобы синхронизировать время устройства со временем компьютера.



#### Примечание

При синхронизации времени вручную или при синхронизации со временем компьютера, 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.



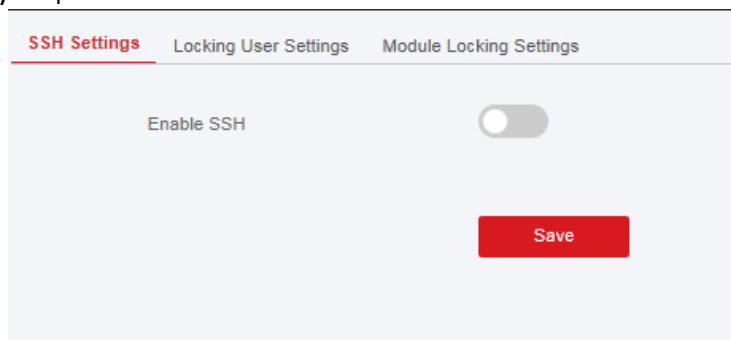
Настройте время начала и окончания DST, а также **DST Bias** («Погрешность DST»).

### 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.

SSH Settings **User Lockout Attempts** Module Locking Settings

Retry Times Before Auto-Lock: 3

Auto-lock Time: 1800 s

No.	IP Address	Unlock
-----	------------	--------

Save Unlock All

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.

### **Locked Duration («Длительность блокировки»)**

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**

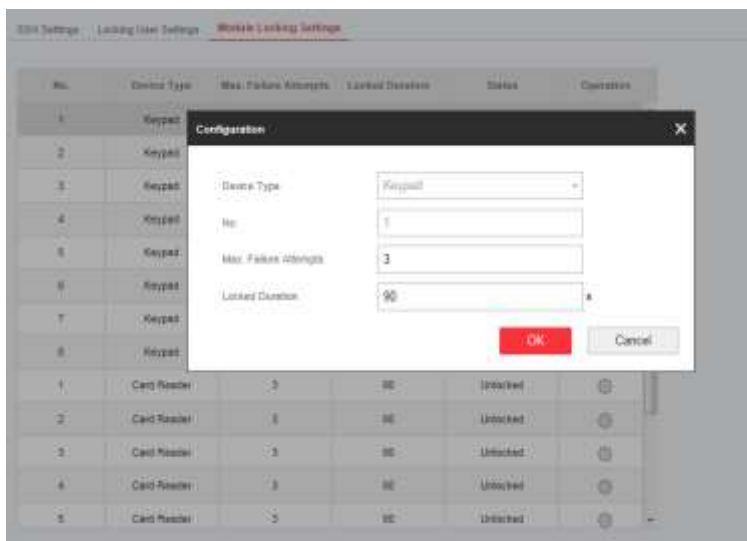
Настройте параметры блокировки модуля, включая максимальное количество попыток ввода учетных данных и длительность блокировки.


## Охранная панель AX PRO • Руководство пользователя

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 значок 
3. Настройте следующие параметры:

#### **Max. Failure Attempts («Максимальное количество неудачных попыток»)**

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


#### **Locked Duration («Длительность блокировки»)**

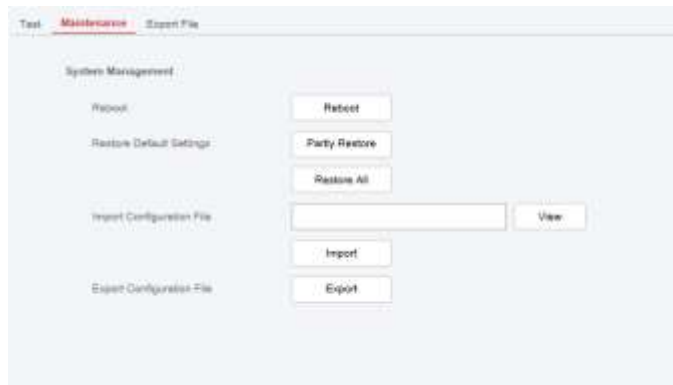
Настройте длительность блокировки клавиатуры. По истечении заданного времени клавиатура будет разблокирована.

4. Нажмите **OK**.
5. Опционально: нажмите **Lock** («Блокировка»), чтобы разблокировать заблокированный модуль.

### 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.

### **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.

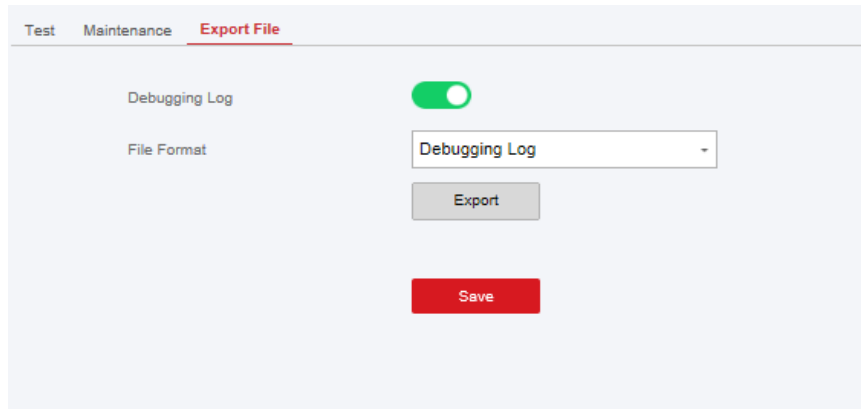
### **Export Configuration File («Экспорт файла конфигурации»)**

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.

## **Экспорт файлов**

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

Включите журнал отладки, чтобы включить функцию.

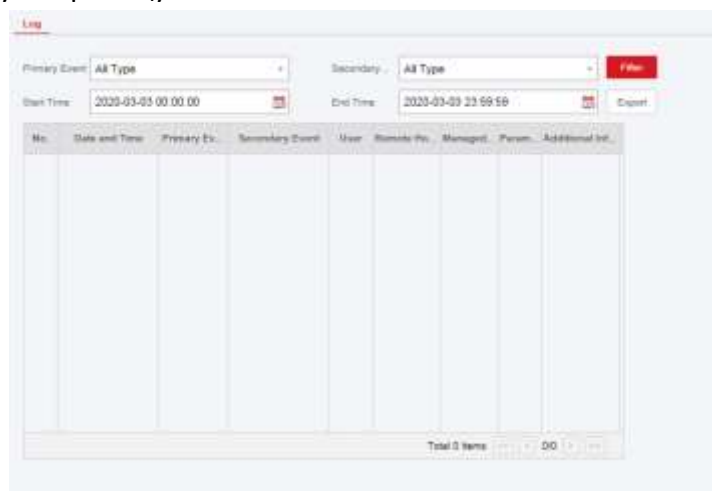


Выберите тип файла, который необходимо экспортировать. Нажмите **Export** («Экспорт»), чтобы экспортировать файл.

### 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 основной тип 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 фильтры»), чтобы сбросить все условия поиска.

### 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.



- **Получение PIN-кода от техподдержки HIKVISION**

Для доступа к локальному веб-клиенту панели управления лучше использовать удаленный рабочий стол.

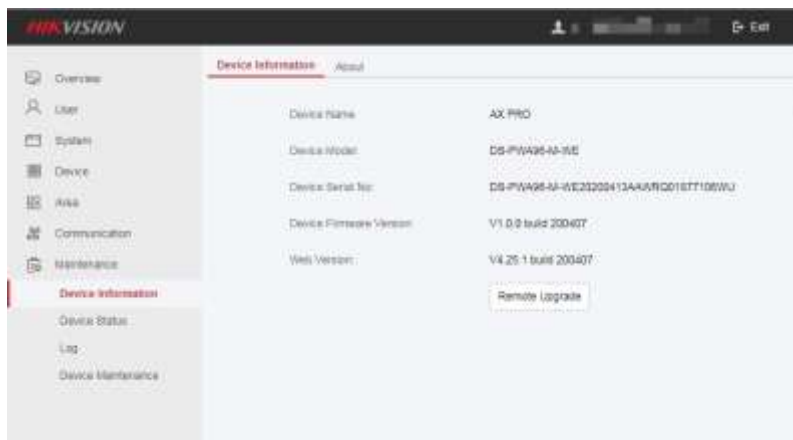
## Охранная панель AX PRO • Руководство пользователя

PIN-код будет авторизован в соответствии со стандартной процедурой техподдержки.

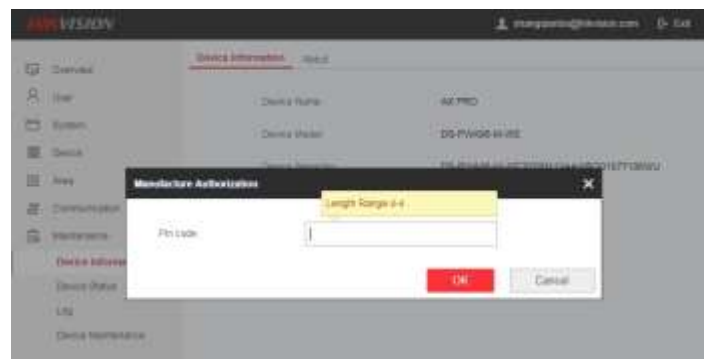
### Обновление прошивки

#### Шаги:

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

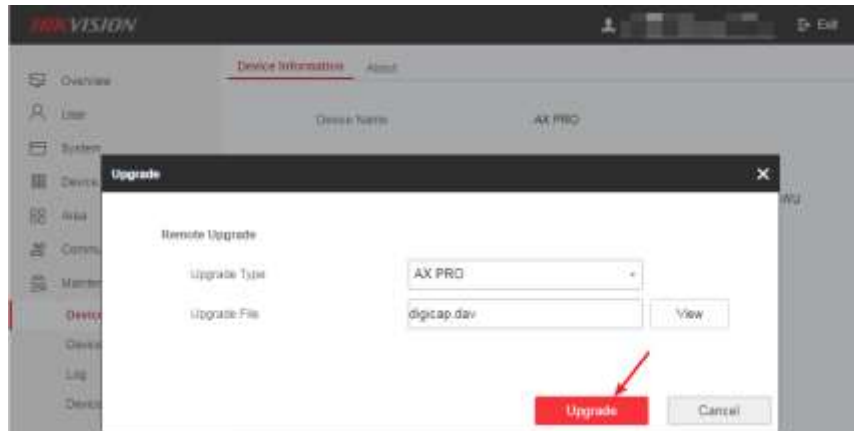


3. Введите PIN-код производителя, чтобы открыть интерфейс обновления.



4. Нажмите **View** («Просмотреть»), чтобы найти файл прошивки с именем digicap.dav.
5. Для завершения нажмите **Upgrade** («Обновить»).





---

### **Примечание**

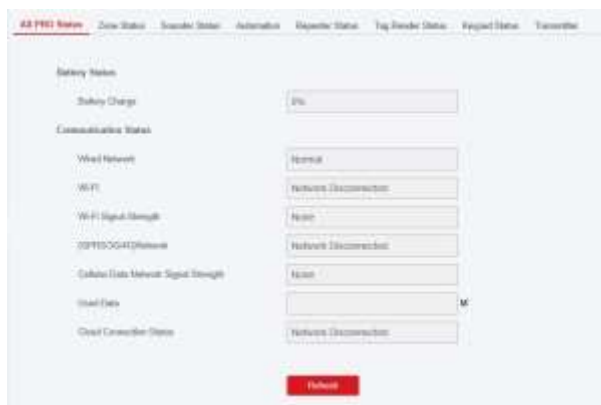
И пользователи, и информация о конфигурации будут сохранены после завершения обновления.

---

### **4.3.8 Диагностика состояния**

После настройки зоны, ретранслятора и других параметров можно посмотреть статус их работы.

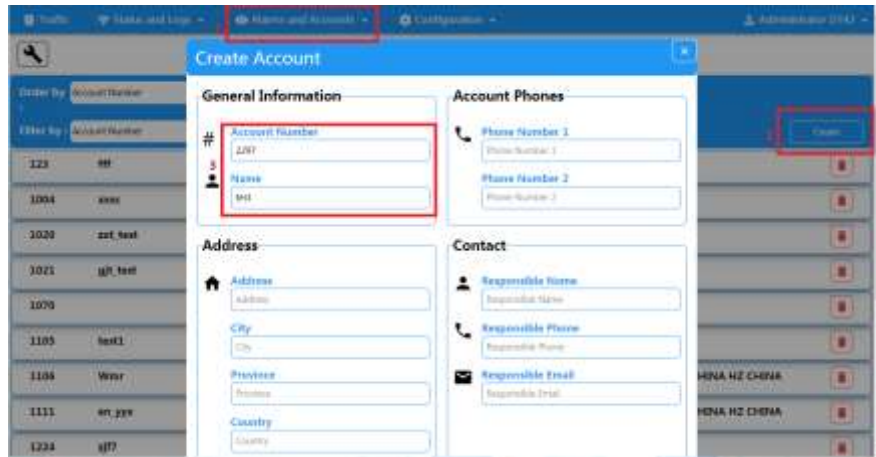
Перейдите на вкладку **Maintenance** → **Device Status** («Обслуживание → Состояние устройства»). Здесь можно просматривать состояние зоны, реле, звукового оповещателя, клавиатуры, считывателя меток, батареи и связи.



- **Zone («Зона»):** здесь можно просматривать состояние зоны, состояние тревоги, емкость батареи детектора и мощность сигнала.
- **Sounder («Звуковой оповещатель»):** здесь можно посмотреть состояние звукового оповещателя, состояние батареи и уровень сигнала.
- **Output («Выход»):** здесь можно посмотреть состояние реле, состояние батареи и уровень сигнала.



## Охранная панель AX PRO • Руководство пользователя



### Настройка ATS приемопередатчика панели:

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.

Address Type	IP
Server Address	115.236.50.3
Port No.	6666
Account Code	2297
Transmission Mode	TCP
Impulse Counting Time	20
Adaptgts	3
Poling Rule	60
Encryption Algorithm	AES
Password Length	128
Secret Key	123456789012345678901234567

= 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.

## Охранная панель AX PRO • Руководство пользователя

= Настройка параметров сервера =

■ <b>Тип адреса</b> — IP-адрес — Доменное имя
■ <b>Адрес сервера / доменное имя</b>
■ <b>№ порта</b> 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 =

■ <b>Код учетной записи</b> Введите назначенную учетную запись, предоставленную ЧОП / ПЦН.
---

= Настройка параметров протокола SIA DC-09 =

■ <b>Режимы передачи</b> — TCP — UDP Для передачи данных поддерживаются протоколы TCP и UDP. Протокол UDP рекомендуется стандартом SIA DC-09.
■ <b>Настройка подключения</b> <ul style="list-style-type: none"><li>○ <b>Время подсчета импульсов / период ожидания повторной попытки</b> Настройте время ожидания ответа получателя. Повторная передача будет выполнена при истечении установленного периода для приемопередатчика.</li><li>○ <b>Попытки</b> Настройте максимальное количество попыток повторной передачи.</li><li>○ <b>Частота опроса</b> Настройте интервал между двумя опросами в реальном времени, поставить галочку <b>Enable</b> («Включить»).</li></ul>
■ <b>Настройки шифрования</b> <ul style="list-style-type: none"><li>○ <b>Алгоритмы шифрования</b> — AES</li><li>○ <b>Длина пароля</b> — 128 — 192 — 256</li><li>○ <b>Секретный ключ</b> Настройте длину ключа шифрования и введите ключ, предоставленный ЧОП / ПЦН.</li></ul>

### Тестирование сигнализации

Активируйте тревогу экстренного видео с панели управления.

Войдите в приемник. Нажмите **Traffic** («Трафик»), чтобы просмотреть все полученные сообщения.



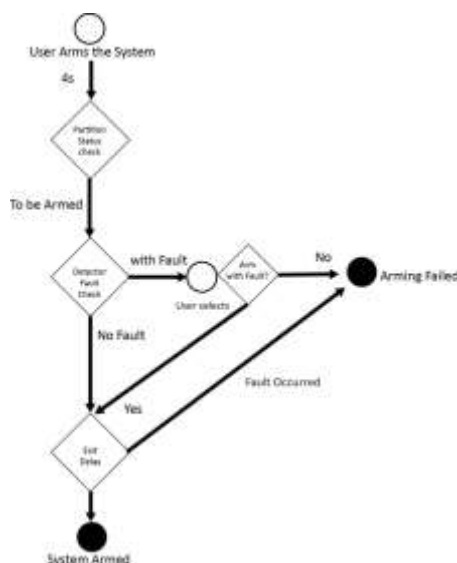
## Раздел 5 Общие операции

### 5.1 Постановка на охрану

Для постановки системы на охрану можно использовать: клавиатуру, брелок, метку, клиентское программное обеспечение, мобильный клиент.

После отправки команды постановки на охрану в AX PRO система проверит состояние извещателя. Если детектор неисправен, можно поставить систему на охрану с неисправным датчиком или остановить операцию.

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



#### Уровень доступа постановки на охрану

Пользователь на уровне 2 или 3 имеет разрешение на поставку системы на полную или частичную охрану.

#### Идентификация постановки на охрану

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

### **Причина сбоя постановки на охрану**

- Сработал детектор саботажа (кроме детектора на пути к выходу).
- Сработало устройство тревожной сигнализации.
- Сработала тревога детектора саботажа.
- Исключение связи
- Исключение основного источника питания
- Исключение резервной батареи
- Ошибка приема тревоги
- Неисправность звукового оповещателя
- Низкий заряд батареи брелока
- Другое

### **Постановка на охрану при обнаружении неисправности**

При обнаружении неисправности, пользователь на уровне 2 имеет право поставить систему на охрану (принудительная постановка на охрану).

Принудительная постановка на охрану влияет только на текущую операцию постановки на охрану. Принудительная постановка на охрану будет записана в журнал событий.

## **5.2 Снятие с охраны**

Снять систему с охраны можно с помощью: клавиатуры, брелока, метки, клиентского программного обеспечения или мобильного клиента.

### **Индикаторы снятия с охраны**

Индикатор постановки на охрану / снятия с охраны мигает 30 секунд, пока пользователь успешно снимает систему с охраны при входе / выходе.

Система сообщит о результате снятия с охраны после завершения операции.

### **Продолжительность задержки на вход**

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

### **Тревога по истечении времени задержки**

Если тревога вторжения или тревога саботажа возникает в точке входа / выхода, когда AX PRO находится в состоянии задержки на вход, панель AX PRO перейдет в режим тревоги по истечении времени задержки

Можно установить длительность интервал задержки: (> 30 с).

Панель AX PRO будет сообщать о тревоге, только если тревожное событие длится в течение установленного интервала с добавлением задержки на вход.

## **5.3 Управление системой с помощью SMS**

Управлять системой безопасности можно с помощью SMS, как показано ниже.

Формат SMS для постановки на охрану / снятия с охраны / выключения тревоги:

{Команда} + {Тип операции} + {Цель}

Команда: 2 цифры, 00 - снятие с охраны, 01 - постановка на охрану, 02 - постановка на охрану, 03 - отключение тревоги тип работы: 1- зона действия

Цель: не более 3 цифр, 0 - операция для всех областей, 1 - операция для области 1 (зона 1).

Все остальное можно вывести по аналогии.

## **А. Поиск неисправностей**

### **А.1 Ошибка связи**

#### **А.1.1 Конфликт IP-адресов**

Описание неисправности:

IP-адрес, который панель автоматически получает или назначает, совпадает с IP-адресом других устройств, что приводит к конфликтам IP-адресов.

Решение:

Найдите текущий доступный IP-адрес через ping. Измените IP-адрес и войдите повторно.

#### **А.1.2 Веб-страница недоступна**

Описание неисправности:

Отображается недоступная страница в веб-браузере.

Решение:

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

#### **А.1.3 Отсутствие подключения к Hik-Connect**

Описание неисправности:

Веб-страница показывает отсутствие подключения к Hik-Connect.

Решение:

Ошибка сетевой конфигурации панели, отсутствует доступ к внешней сети.

#### **А.1.4 Часто пропадает подключение к IP-камере**

Описание неисправности:

Система сообщает о нескольких событиях отключения и подключения IP-камеры.

Решение:

Проверьте корректность подключения к сети или к интерфейсу просмотра с камеры в режиме реального времени.



### **A.1.5 Не удалось добавить устройство в приложение**

Описание неисправности:

При использовании приложения для добавления устройств появляется сообщение о том, что устройство не может быть добавлено, устройство не может быть найдено и т. д.

Решение:

Проверьте веб-страницу: активно ли подключение к Hik-Connect.

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

Описание неисправности:

После срабатывания тревоги, приложение / iVMS-4200 / ЧОП / ПЦН не получает сообщение о тревоге.

Решение:

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

Обеспечьте кнопку контролем вскрытия на извещателе.

### **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.

## **А.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.

## **А.6 Ошибка отправки электронного письма**

### **А.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.

### **А.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).

### **А.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»).

## **А.6.6 Таблица А-1 Настройка параметров почты**

**Настройка параметров почты**

<b>Тип почты</b>	<b>Почтовый сервер</b>	<b>SMTP-порт</b>	<b>Поддерживаемые протоколы</b>
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)

**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 Для имени пользователя в Outlook и Hotmail требуются полные имена, а для других адресов электронной почты требуется префикс перед @.

## **В. Типы входных сигналов**

**Таблица В-1 Типы входных сигналов**

<b>Типы вводных сигналов</b>	<b>Операции</b>
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 в зоне X.
Зона периметра	После постановки системы на охрану при обнаружении тревожного события тревога срабатывает незамедлительно. Звуковое оповещение: 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 в зоне 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.

## Охранная панель AX PRO • Руководство пользователя

Типы входных сигналов	Операции
	Звуковое оповещение: включите звук и звуковой оповещатель системы. Голосовая подсказка: пожарная тревога в зоне X.
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. Звуковое оповещение: включите звук и звуковой оповещатель системы. Голосовая подсказка: срабатывает бипер.
Тревога детектора саботажа	После постановки системы на охрану при обнаружении тревожного события тревога срабатывает незамедлительно. Звуковое оповещение: 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 AX PRO поставлена на охрану.

## Охранная панель AX PRO • Руководство пользователя

Под охраной	<p>Когда зона поставлена на охрану: Голосовое предупреждение об обнаружении неисправности. Далее можно устранить неисправность в соответствии с голосовой подсказкой.</p> <ul style="list-style-type: none"><li>● Звуковое оповещение для постановки на охрану с помощью метки или брелока.</li><li>● Голосовое предупреждение об обнаружении неисправности. Далее можно устранить неисправность в соответствии с голосовой подсказкой.</li></ul> <p>В клиентском ПО отображается сообщение о неисправности. Устранить ошибку можно через клиентское программное обеспечение или мобильный клиент.</p> <p>Голосовая подсказка: постановка на охрану выполнена / Ошибка автоматической постановки на охрану.</p>
-------------	---



## С. Тип вывода

Таблица С-1 Тип вывода

Тип вывода	Активный	Восстановленный
Постановка на охрану	Постановка панели АХ PRO на охрану.	После настроенной задержки вывода.
Снятие с охраны	Снятие панели АХ PRO 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 АХ PRO 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	x/√	√	√	√	√
Событие, угрожающее безопасности жизни	x/√	√	√	√	√
Уведомления о состоянии системы	x/√	√	x	x	x
Уведомление панели управления	x/√	√	x	x	x

## **Е. Уровни доступа**

<b>Уровень</b>	<b>Описание</b>
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 Е-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	Нет	Да <sup>d</sup>	Да <sup>d</sup>
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**

<sup>a</sup> При условии предварительного разрешения от пользователя на уровне 2.

<sup>б</sup> При условии предварительного разрешения от пользователя на уровне 2 и 3.

<sup>d</sup> 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.

## Охранная панель AX PRO • Руководство пользователя

- 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**

### **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.

	<b>TN</b>	<b>Максимальное время</b>
<b>Ошибка первичного ATP / восстановление ATP</b>	LAN/WiFi	10 мин
<b>Ошибка вторичного ATP / восстановление ATP</b>	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.

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

### **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

**Таблица F-1 Код SIA и CID**

<b>Код SIA</b>	<b>Код CID</b>	<b>Описание</b>
MA	1100	Тревога экстренной медицинской помощи
MH	3100	Тревога экстренной медицинской помощи устранена
BA	1130	Тревога взлома
BH	3130	Тревога взлома устранена
FA	1110	Пожарная тревога
FH	3110	Пожарная тревога устранена
HA	1121	Тревога принудительного действия
HA	1122	Беззвучная сигнализация экстренного
HN	3122	Беззвучная сигнализация экстренного
—	1780	Тревога тайм-аута
BH	3780	Тревога тайм-аута устранена
PA	1120	Тревога экстренного вызова
PH	3120	Тревога экстренного вызова устранена
BA	1133	Тревога 24 часа в сутки
BH	3133	Тревога 24 часа в сутки устранена
BA	1134	Тревога входа / выхода из области
BH	3134	Тревога входа / выхода из области
TA	1137	Тревога саботажа устройства
TR	3137	Тревога саботажа устройства устранена
GA	1151	Тревога утечки газа
GH	3151	Тревога утечки газа устранена
AT	1301	Тревога потери питания
AR	3301	Тревога потери питания устранена
YT	1302	Тревога низкого заряда батареи
YR	3302	Тревога потери питания устранена
RN	1305	Сброс настроек панели управления

## Охранная панель AX PRO • Руководство пользователя

Код SIA	Код CID	Описание
YM	1311	Неисправность батареи
YR	3311	Неисправность батареи
YI	1312	Тревога перегрузки
YJ	3312	Тревога перегрузки устранена
YP	1319	Тревога перенапряжения
YQ	3319	Тревога перенапряжения
XT	1338	Тревога низкого заряда
XR	3338	Тревога низкого заряда батареи ретранслятора
AT	1342	Тревога потери питания
AR	3342	Тревога потери питания
YM	1311	Тревога отключения
YR	3311	Тревога отключения батареи
ES (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	1341 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Тревога саботажа расширителя
EJ (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	3341 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Тревога саботажа расширителя устранена
TA	1334	Тревога саботажа
TR	3334	Тревога саботажа беспроводного ретранслятора
TA	1321	Тревога саботажа беспроводной сирены
TR	3321	Тревога саботажа беспроводной сирены устранена

## Охранная панель AX PRO • Руководство пользователя

UY	1321	Беспроводная сирена отключена
UJ	3321	Подключение беспроводной сирены
ES (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	1341 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Тревога саботажа беспроводного устройства
EJ (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	3341 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Тревога саботажа беспроводного устройства устранена
XT	1338	Тревога низкого заряда батареи беспроводного устройства
XR	3338	Тревога низкого заряда батареи беспроводного устройства устранена
ET (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	1333 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Беспроводное устройство отключено
ER (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	3333 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Беспроводное устройство подключено
LT	1351	Ошибка основного канала АТР
LR	3351	Ошибка основного канала АТР устранена
LT	1352	Ошибка резервного канала АТР
LR	3352	Ошибка резервного канала АТР устранена
TA	1383	Тревога саботажа датчика
TR	3383	Тревога саботажа датчика устранена
OP	1401	Снятие с охраны



## Охранная панель AX PRO • Руководство пользователя

CL	3401	Полная постановка на охрану
OA	1403	Автоматическое снятие с охраны
CA	3403	Автоматическая постановка на охрану
BC	1406	Тревога сброшена
1409	CS	Снятие с охраны при переключении между зонами
3409	OC	Постановка на охрану при переключении между зонами
CL	3441	Частичная охрана
CT	1452	Задержка снятия с охраны
CD	1455	Ошибка автоматической
BB	1570	Тревога обхода зоны
BU	3570	Тревога обхода зоны устранена
RP	1602	Отправка периодических отчетов
TS	1607	Переход в тестовый режим
TE	3607	Выход из тестового режима
LB	1627	Вход в режим разработки
LX	1628	Выход из режима разработки
BA	1131	Тревога вторжения
BH	3131	Тревога вторжения устранена
BA	1131	Тревога пересечения линии
BH	3131	Тревога пересечения линии
BA	1134	Обнаружение входа в область
FA	1112	Пожарная тревога
FH	3112	Пожарная тревога устранена
KS	1158	Предварительная тревога
KR	3158	Предварительная тревога повышенной температуры устранена
1159	ZS	Предварительная тревога
ZR	3159	Предварительная тревога пониженной температуры устранена

## Охранная панель AX PRO • Руководство пользователя

KA	1158	Тревога повышенной температуры
KH	3158	Тревога повышенной температуры
ZA	1159	Тревога пониженной температуры
ZH	3159	Тревога пониженной температуры устранена
EA	1134	Обнаружение выхода из области
PA (для распознавания клавиатуры, номер пользователя брелока начинается с 901)	1120 (для распознавания клавиатуры, номер пользователя брелока начинается с 901)	Тревога экстренного вызова с клавиатуры / брелока
FA	1110	Пожарная тревога 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
/	/	Считыватель карт (брелоков)
/	/	Считыватель карт (брелоков)
UY	1381	Беспроводной датчик отключен
UJ	3381	Беспроводной датчик
XT	1384	Тревога низкого заряда
XR	3384	Тревога низкого заряда батареи беспроводного датчика устранена

## Охранная панель AX PRO • Руководство пользователя

ET (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	1333 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Расширитель отключен
ER (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	3333 (серийный номер модуля вывода начинается с 1, модуля клавиатуры: с 101, считывателя тегов: с 201)	Расширитель подключен
UY	1334	Беспроводной ретранслятор
UJ	3334	Беспроводной ретранслятор
XT	1384	Тревога низкого заряда
XR	3384	Тревога низкого заряда
NT	1350	Сотовая сеть передачи данных
NR	3350	Сотовая сеть передачи данных
NT	1350	Сбой Wi-Fi
NR	3350	Wi-Fi подключен
XQ	1344	Исключение радиосигнала
XH	3344	Исключение радиосигнала устранено
NT	1350	Превышение сетевого потока
XT	1384	Тревога низкого заряда батареи брелока
XR	3384	Тревога низкого заряда батареи брелока устранена
NT	1350	Конфликт IP-адресов
NR	3350	Конфликт IP-адресов устранен
NT	1350	Исключение проводной сети
NR	3350	Исключение проводной сети устранено
/	/	Ошибка отправки email
/	/	IP-камера отключена

## Охранная панель AX PRO • Руководство пользователя

/	/	IP-камера подключена
/	3250	Патруль
/	1306	Датчик удален
/	3306	Датчик добавлен
/	1306	Расширитель удален
/	1306	Расширитель добавлен
/	1306	Беспроводной ретранслятор
/	3306	Добавлен беспроводной ретранслятор
/	1306	Беспроводная сирена удалена
/	3306	Добавлена беспроводная сирена
/	1306	Беспроводное устройство удалено
/	3306	Добавлено беспроводное устройство

## Н. Коммуникационная матрица и команды устройства

Сканируйте приведенный ниже QR-код, чтобы просмотреть документ коммуникационной матрицы охранной панели AXPRO.



### Гарантии защиты конфиденциальной информации пользователей

- Команда отладки или `zhimakaimen` используется для управления доступом к файловой системе для обеспечения безопасности устройства. Чтобы получить разрешение, обратитесь в службу технической поддержки.
- Учетные записи предусмотрены для: администратора, установщика, специалиста

### Описание конфиденциальной информации пользователя

Пароль	Пароль учетной записи устройства, используемый для входа в систему.
Имя пользователя	Имя учетной записи устройства, которое используется для входа в систему.
IP-адрес и порт устройства	IP-адрес и порт устройства используются для поддержки связи сетевых служб. Подробная информация представлена в разделе <i>Коммуникационная матрица</i> .
Журнал	Используется для записи информации об операциях устройства и хранения записей операций.
Информация из базы данных	Используется для записи информации.

# Охранная панель AX PRO • Руководство пользователя

