AXIS S3008 Recorder

Руководство пользователя

Сведения об устройстве

AXIS S3008 Recorder — это компактное сетевое устройство видеозаписи с встроенным коммутатором POE для облегчения монтажа. Устройство оснащено жестким диском, специально предназначенным для охранного видеонаблюдения. Кроме того, в устройстве есть USB-порт для удобного экспорта видеоматериалов. Видеорегистратор поставляется в трех моделях — с жестким диском на 2 ТБ, 4 ТБ или 8 ТБ.

Сколько камер можно подключить к видеорегистратору?

К POE коммутатору видеорегистратора можно подключить до восьми камер.

Какой объем мощности видеорегистратор может подавать на камеры?

Ниже указаны ограничения для питания по технологии Power over Ethernet (PoE):

- Видеорегистратор может подавать питание на 8 устройств по технологии PoE.
- Общий доступный объем мощности составляет:
  - 2 ТБ и 4 ТБ: 65 Вт
  - 8 ТБ: 60 Вт
- Каждый сетевой порт поддерживает до 15,4 Вт (PoE, класс 3) на порте PoE (питающее устройство) и 12,95 Вт на стороне камеры (питаемое устройство).
- Коммутатор распределяет мощность PoE с учетом класса PoE подключенного устройства.

Поддержка браузеров

Windows®

- Chrome™ (рекомендуется)
- Firefox®
- Edge®

OS X®

- Chrome™ (рекомендуется)
- Safari®

Прочие

- Chrome™
- Firefox®

Более подробная информация об использовании данного устройства содержится в руководстве пользователя на веб-странице *Документация | Axis Communications*.
Подробнее о рекомендуемых браузерах см. на веб-странице
Браузеры, поддерживаемые операционной системой Axis OS | Axis Communications.

Начало работы

Для просмотра видео откройте веб-версию данного документа.

www.axis.com/products/online-manual/63362#t10153931_ru

Видеорегистратор AXIS S3008 Recorder следует использовать с ПО для управления видео AXIS Companion версии 4.

Начало работы с AXIS Companion

Примечание.

Во время установки системы требуется доступ к Интернету.

Обзор установки:

1. *Регистрация учетной записи MyAxis на стр. 3*
2. *Установка оборудования на стр. 4*
3. *Установка приложения для компьютера на стр. 4*
4. *Создание объекта на стр. 5*
5. *Установка мобильного приложения на стр. 6*

Результат установки системы:

- На всех устройствах Axis обновлено **встроенное ПО**.
- Задан **пароль** для устройств.
- Разрешена **видеозапись** с настройками по умолчанию.
- Разрешен **удаленный доступ**.

Регистрация учетной записи MyAxis

Учетную запись **MyAxis** можно зарегистрировать на странице *axis.com/my-axis/login*.

Для повышения безопасности учетной записи MyAxis активируйте многофакторную проверку подлинности. Многофакторная проверка подлинности — это система безопасности с дополнительным уровнем верификации, подтверждающим личность пользователя.

Активировать многофакторную проверку подлинности:

1. Перейдите на страницу *http://auth.axis.com/user-center/account/security-settings*.
2. Включите **2–Step verification (Двухэтапная проверка)**.

Вы перейдете на страницу входа в систему.

3. Войдите в систему, используя свои учетные данные **MyAxis**.

Многофакторная проверка подлинности включена.

Вход при активной многофакторной проверке подлинности:

1. Войдите в учетную запись **MyAxis**.

Вам придет электронное письмо.

2. Откройте электронное письмо и нажмите кнопку **Authenticate (Подтвердить)**.

Если вы не получили электронное письмо, проверьте папку нежелательной почты. Если письма там нет, обратитесь в службу технической поддержки.

Установка оборудования

1. Установите оборудование камеры.
2. Подключите видеорегистратор к вашей сети через порт локальной сети.

Примечание.

Если видеорегистратор отсутствует, для записи видео требуется камера с установленной картой SD.

3. Подключите камеры к коммутатору PoE, встроенному в видеорегистратор, или к внешнему коммутатору PoE.
4. Подключите компьютер к той же сети, в которой находится видеорегистратор.
5. Подключите источник питания к видеорегистратору.

Важно!

Сначала необходимо подключить шнур питания к видеорегистратору, а затем подсоединить шнур питания к розетке электросети.

6. Подождите несколько минут, пока видеорегистратор и камеры загрузятся, прежде чем продолжить.

⚠ОСТОРОЖНО

Чтобы видеорегистратор не перегревался, его нужно установить в хорошо проветриваемом месте и предусмотреть достаточно свободного пространства вокруг него.

Установка приложения для компьютера

1. Перейдите на страницу *axis.com/products/axis-companion* и нажмите **Download (Скачать)**, чтобы скачать приложение AXIS Companion для компьютера с операционной системой Windows.
2. Выполните вход, используя *учетную запись MyAxis*.
3. Прочтите лицензионное соглашение и выберите один из предлагаемых вариантов, чтобы перейти к следующему шагу.
4. Сохраните файл в любую папку.
5. Откройте файл и нажмите **Run (Выполнить)**, чтобы начать установку.
6. Чтобы разрешить приложению вносить изменения на устройстве, нажмите **Yes (Да)**.
7. Выберите язык и нажмите **OK**.
8. Следуйте инструкциям мастера установки.

Создание объекта

Для просмотра видео откройте веб-версию данного документа.

www.axis.com/products/online-manual/63362#t10112114_ru

Объект — это единая «точка входа» в систему охранного видеонаблюдения некоторого физического объекта. Например, объект может представлять все камеры в одном магазине. С помощью одной учетной записи MyAxis можно вести наблюдение за несколькими объектами.

Примечание.

Если вы использовали более раннюю версию AXIS Companion, в вашей системе могут присутствовать устройства, которые не поддерживаются в AXIS Companion версии 4. К примеру, не поддерживаются сетевые хранилища (NAS) сторонних производителей, а также устаревшие устройства Axis, встроенное ПО которых невозможно обновить до версии 5.50 или более поздней версии. Мастер сообщит вам о любых подобных проблемах и поможет в их разрешении.

Примечание.

Объекты, созданные в AXIS Companion более ранней версии, чем версия 4, не появятся в списке объектов. Дополнительную информацию можно найти в «Руководстве по миграции» (доступно на веб-странице поддержки).

1. Запустите приложение AXIS Companion на компьютере.
2. Выполните вход, используя *учетную запись MyAxis*.
3. Нажмите **Get started (Начать работу)**.
4. Присвойте объекту имя и введите название своей компании.
5. Нажмите **Next (Далее)**.
6. Выберите устройства, которые нужно добавить к объекту.

   Для выбора устройства, защищенного паролем, потребуется ввести пароль.

Примечание.

При наличии неподдерживаемых устройств можно нажать **Read more (Подробнее)**, чтобы выяснить, почему эти устройства не поддерживаются.

7. Нажмите **Next (Далее)**.
8. Введите пароль.

   Этот пароль будет использоваться в мобильном приложении AXIS Companion для доступа к веб-страницам устройств или при работе в автономном режиме.
9. Нажмите **Next (Далее)**.
10. На странице **Ready to install (Готово к установке)** может отображаться список камер, для которых требуется выполнить восстановление. В этом случае нажмите ссылку **Restore device (Восстановить устройство)** и устраните имеющуюся проблему на веб-странице устройства.

11. Нажмите **Finish (Готово)** и подождите, пока AXIS Companion настраивает камеры.

Примечание.

Процесс настройки может длиться несколько минут.

Видеоруководства по началу работы можно найти на странице *AXIS Companion — Учебные руководства*.

Установка мобильного приложения

Мобильное приложение AXIS Companion можно использовать для настройки системы и управления ею из любого места. Уведомления, отправляемые в режиме реального времени, будут оповещать вас о любых подозрительных действиях. Вы также можете просматривать и экспортировать видеозаписи.

1. Перейдите на страницу App Store или Google Play.
2. Найдите и скачайте приложение **AXIS Companion 4**.
3. Выполните вход в AXIS Companion, используя свою *учетную запись MyAxis*.

Дополнительную информация о том, как использовать приложение, можно найти на странице *AXIS Companion — Учебные руководства*.

Интерфейс устройства

Показать или скрыть основное меню.

Доступ к справке по продукту.

Изменить язык.

Установка светлой или темной темы.

Просмотр информации о пользователе, который вошел в систему.

Элементы контекстного меню:

- **Analytics data (Данные аналитики)**. Нажмите «Принять», чтобы разрешить передачу неперсональных данных просмотра веб-страниц.
- **Feedback (Обратная связь)**. Отправка отзывов, которые помогут нам повысить удобство работы пользователей.
- **Legal (Юридическая информация)**. Просмотр информации о файлах cookie и лицензиях.
- **About (О системе)**. Просмотр информации об устройстве, включая версию встроенного ПО и серийный номер.

Состояние видеорегистратора

Status (Состояние)

Allocated PoE (Выделенная мощность PoE). Количество Ватт (Вт), выделенных в данный момент времени.

Total PoE consumption (Общая потребляемая мощность PoE). Количество потребляемых Ватт (Вт).

Keep PoE active during recorder restart (Не деактивировать PoE во время перезапуска видеорегистратора). Включите подачу питания на подключенные устройства во время перезапуска устройства видеозаписи.

Used space (Использованное пространство). Использованное пространство в процентах.

Free space (Свободное пространство). Доступное для записей пространство в процентах.

Free space (Свободное пространство). Доступное пространство на диске отображается в мегабайтах (МБ), гигабайтах (ГБ) или терабайтах (ТБ).

Disk status (Состояние диска). Текущее состояние диска.

Disk temperature (Температура диска). Текущая температура.

Ports (Порты)

У каждого порта есть индивидуальный номер и индивидуальные настройки.

PoE. Включите или выключите PoE для каждого порта. Когда устройство подключено, отображаются следующие данные.

- **Allocated power (Выделенная мощность)**. Количество Ватт (Вт), выделенных в данный момент времени.
- **Mac**. Адрес контроля доступа к носителю информации (MAC-адрес) подключенного устройства.

Приложения

Add app (Добавить приложение): Нажмите, чтобы установить новое приложение.

Find more apps (Найти другие приложения): Нажмите, чтобы перейти на страницу обзора приложений Axis.

⋮ Элементы контекстного меню:

- **App log (Журнал приложений)**. Нажмите, чтобы просмотреть журнал событий приложения. Журнал полезен при обращении в службу поддержки.
- **Activate license with a key (Активировать лицензию ключом)**. Если приложению требуется лицензия, необходимо активировать ее. Используйте этот параметр, если у устройства нет доступа к Интернету. Если у вас нет лицензионного ключа, перейдите по адресу *axis.com/applications*. Для формирования лицензионного ключа потребуется код лицензии и серийный номер устройства Axis.
- **Activate license automatically (Активировать лицензию автоматически)**. Если приложению требуется лицензия, необходимо активировать ее. Используйте этот параметр, если у устройства есть доступ в Интернет. Для активации лицензии необходимо иметь лицензионный ключ.
- **Deactivate the license (Деактивация лицензии)**. Деактивируйте лицензию, чтобы использовать ее на другом устройстве. Деактивация лицензии означает ее удаление с этого устройства. Для деактивации лицензии требуется доступ в Интернет.
- **Delete (Удалить)**. Удалите приложение с устройства навсегда. Если сначала не деактивировать лицензию, она останется активной.

Примечание.

Производительность устройства может снизиться при одновременном запуске нескольких приложений.

Start (Пуск). Запустить или остановить приложение.

Open (Открыть). Нажмите, чтобы получить доступ к настройкам приложения. Доступные настройки зависят от типа приложения. В некоторых приложениях нет раздела настроек.

Система

Дата и время

Формат времени зависит от языковых настроек веб-браузера.

Примечание.

Рекомендуется синхронизировать дату и время устройства с NTP-сервером.

Synchronization (Синхронизация). Выберите способ синхронизации даты и времени устройства.

- **Automatic date and time (NTP server using DHCP) (Автоопределение даты и времени (NTP-сервер, использующий DHCP))**. Синхронизация с NTP-сервером, подключенным к серверу DHCP.
- **Automatic date and time (manual NTP server) (Автоопределение даты и времени (через NTP-сервер вручную))**. Синхронизация с выбранным вами NTP-сервером.
  - **Primary NTP server (Основной NTP-сервер)** и **Secondary NTP server (Резервный NTP-сервер)**. Введите IP-адрес одного или двух NTP-серверов. При использовании двух NTP-серверов устройство синхронизирует и подстраивает свое время на основании вводимых данных на обоих серверах.
- **Custom date and time (Пользовательская настройка даты и времени)**. Установка даты и времени вручную. Нажмите **Get from system (Получить из системы)**, чтобы однократно получить настройки даты и времени с вашего компьютера или мобильного устройства.

Time zone (Часовой пояс). Выберите часовой пояс, который будет использоваться. Время будет автоматически корректироваться с учетом летнего времени и зимнего времени.

Примечание.

Система использует настройки даты и времени во всех записях, журналах и системных параметрах.

Сеть

IPv4 and IPv6 (IPv4 и IPv6)

IPv4

- **Automatic IP (DHCP) and DNS (DHCP) (Автоматический IP-адрес (DHCP) и DNS (DHCP))**: Рекомендуемый параметр для большинства сетей. Текущие настройки обновляются автоматически.
- **Automatic IP (DHCP) and manual DNS (Автоматическое назначение IP-адреса (DHCP) и назначение DNS вручную)**: Обратитесь к администратору сети, чтобы задать настройки вручную. Текущие автоматические настройки обновляются автоматически.
- **Manual IP and DNS (Назначение IP-адреса и DNS вручную)**: Обратитесь к администратору сети, чтобы задать настройки вручную.

IP address (IP-адрес). Укажите уникальный IP-адрес устройства. В изолированных сетях можно случайным образом назначать статические IP-адреса при условии, что каждый адрес является уникальным. Во избежание конфликтов настоятельно рекомендуется обратиться к администратору сети, прежде чем назначить статический IP-адрес.

Subnet mask (Маска подсети). Укажите маску подсети.

Router (Маршрутизатор). Укажите IP-адрес маршрутизатора (шлюза), который по умолчанию используется для подключения устройств, находящихся в разных сетях и разных сегментах сети.

Hostname (Имя хоста). Введите имя хоста.

Search domains (Поиск по доменам). При использовании неполного имени хоста нажмите **Add search domain (Добавить поисковый домен)** и введите домен, в котором будет осуществляться поиск имени хоста, используемого устройством.

DNS servers (DNS-серверы). Нажмите **Add DNS server (Добавить DNS-сервер)** и введите IP-адрес основного DNS-сервера. Этот сервер обеспечивает преобразование имен хостов в IP-адреса в вашей сети.

IPv6

Assign IPv6 automatically (Назначить IPv6 автоматически). Выберите этот пункт, чтобы сетевой маршрутизатор автоматически назначил IP-адрес устройству.

Friendly name (Понятное имя)

Bonjour®. Включите этот параметр, чтобы разрешить автоматическое обнаружение в сети.

Bonjour name (Имя для протокола Bonjour). Введите понятное имя, которое будет отображаться в сети. Имя по умолчанию включает в себя название и MAC-адрес устройства.

Use UPnP® (Использовать UPnP®). Включите этот параметр, чтобы разрешить автоматическое обнаружение в сети.

UPnP name (Имя в службе UPnP). Введите понятное имя, которое будет отображаться в сети. Имя по умолчанию включает в себя название и MAC-адрес устройства.

One-click cloud connection (Подключение к облаку одним щелчком)

Подключение к облаку в одно нажатие (O3C) совместно с сервисом O3C обеспечивает простой и безопасный доступ через Интернет к живому и записанному видео отовсюду, где бы вы ни находились. Дополнительные сведения см. на странице *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (Разрешить O3C):

- **One-click (Одно нажатие)**. Значение по умолчанию. Нажмите и удерживайте нажатой кнопку управления, чтобы подключиться к службе O3C через Интернет. После нажатия кнопки управления необходимо зарегистрировать устройство в службе O3C в течение 24 часов. В противном случае, устройство будет отключено от службы O3C. После регистрации будет активирован параметр **Always (Всегда)** и устройство будет постоянно подключено к службе O3C.

- **Always (Всегда)**. Устройство будет постоянно пытаться подключиться к службе O3C через Интернет. После регистрации устройство будет постоянно подключено к службе O3C. Используйте этот вариант, если кнопка управления находится вне досягаемости.
- **No (Нет)**. Отключает службу O3C.

Proxy settings (Настройки прокси-сервера): Если требуется, задайте параметры прокси-сервера для подключения к серверу HTTP.

Host (Хост). Укажите адрес прокси-сервера.

Port (Порт). Введите номер порта, используемого для получения доступа.

Login (Логин) и **Password (Пароль)**. При необходимости введите имя пользователя и пароль для прокси-сервера.

Authentication method (Способ проверки подлинности).

- **Basic (Базовая)**. Этот способ является самой совместимой схемой проверки подлинности для протокола HTTP. Метод **Digest (Дайджест-авторизация)** безопаснее, так как в данном случае имя пользователя и пароль передаются серверу без шифрования.
- **Digest (Дайджест-авторизация)**. Этот способ является более безопасным, так как при его использовании пароль всегда передается по сети в зашифрованном виде.
- **Auto (Автоматически)** Этот вариант позволяет устройству выбирать способ проверки подлинности автоматически в зависимости от поддерживаемого способа. Приоритет отдается способу **Digest (Дайджест-авторизация)**, а не **Basic (Базовая)**.

Owner authentication key (OAK) (Ключ аутентификации владельца (OAK)): Нажмите **Get key (Получить ключ)**, чтобы получить ключ авторизации владельца. Это возможно только в том случае, если устройство подключено к Интернету без межсетевого экрана или прокси-сервера.

Connected clients (Подключенные клиенты)

В списке отображаются все клиенты, подключенные к устройству.

Update (Обновление). Нажмите, чтобы обновить список.

Безопасность

Сертификаты

Сертификаты служат для проверки подлинности устройств в сети. Устройство поддерживает два типа сертификатов:

- **Сертификаты клиента/сервера**
  Сертификат клиента/сервера удостоверяет подлинность устройства. Он может быть самозаверяющим или может быть выдан Центром сертификации (ЦС). Самозаверяющий сертификат дает ограниченную защиту, и его можно использовать до получения сертификата, выданного Центром сертификации.
- **Сертификаты ЦС**
  Сертификат, выданный Центром сертификации (ЦС), можно использовать для подтверждения подлинности сертификата узла, например для идентификации сервера проверки подлинности, когда устройство подключается к сети, защищенной по стандарту IEEE 802.1X. Устройство поставляется с несколькими предустановленными сертификатами ЦС.

Поддерживаются следующие форматы:

- Форматы сертификатов: .PEM, .CER и .PFX
- Форматы закрытых ключей: PKCS#1 и PKCS#12

Важно!

При сбросе параметров устройства к заводским установкам все сертификаты удаляются. Любые предустановленные сертификаты ЦС будут установлены повторно.

Фильтрация сертификатов в списке.

+ **Add certificate (Добавление сертификата)**. Нажмите эту кнопку, чтобы добавить сертификат.

⋮ Элементы контекстного меню:

- **Certificate information (Информация о сертификате)**. Просмотр свойств установленного сертификата.
- **Delete certificate (Удалить сертификат)**. Удаление сертификата.
- **Create certificate signing request (Создать запрос подписи сертификата)**. Создание запроса на подписание сертификата для его отправки в регистрационный орган и подачи заявления на получение цифрового удостоверения личности.

IEEE 802.1x

IEEE 802.1x — стандарт для технологии контроля доступа в сеть с использованием портов, обеспечивающий проверку подлинности проводных и беспроводных сетевых устройств. Стандарт IEEE 802.1x основан на протоколе EAP (Extensible Authentication Protocol).

Для получения доступа к сети, защищенной IEEE 802.1x, сетевые устройства должны пройти проверку подлинности. Проверка подлинности выполняется сервером проверки подлинности. Как правило, это RADIUS-сервер, примерами которого являются FreeRADIUS и сервер Microsoft для проверки подлинности в Интернете (IAS).

Сертификаты

Если сертификат ЦС не был настроен, проверка сертификата сервера будет отключена и устройство будет проверять собственную подлинность независимо от того, к какой сети оно подключено.

При использовании сертификата в установке Axis устройство и сервер аутентификации авторизуются с помощью цифровых сертификатов через протокол EAP-TLS.

Чтобы обеспечить устройству доступ к сети, защищенной с помощью сертификатов, на устройстве должен быть установлен подписанный клиентский сертификат.

Client certificate (Сертификат клиента): Выберите сертификат клиента для использования IEEE 802.1x. Сервер проверки подлинности использует сертификат для подтверждения подлинности сервера аутентификации.

CA certificate (Сертификат ЦС): Выберите сертификат ЦС для проверки удостоверения сервера проверки подлинности. Если сертификат не выбран, устройство попытается пройти проверку подлинности независимо от того, к какой сети оно подключено.

EAP identity (Идентификатор EAP). Введите удостоверение пользователя, связанное с сертификатом клиента.

EAPOL version (Версия EAPOL). Выберите версию протокола EAPOL, используемую в сетевом коммутаторе.

Use IEEE 802.1x (Использовать IEEE 802.1x): Выберите этот пункт, чтобы использовать протокол IEEE 802.1x.

Custom-signed firmware certificate (Сертификат для встроенного ПО с пользовательской подписью)

Для установки тестового встроенного ПО или другого пользовательского встроенного ПО от компании Axis на устройстве необходимо использовать сертификат для встроенного ПО с пользовательской подписью. Сертификат проверяет, одобрено ли встроенное ПО как владельцем устройства, так и компанией Axis. Встроенное ПО может работать только на определенном устройстве, которое идентифицируется по его уникальному серийному номеру и идентификатору микросхемы. Сертификаты для встроенного ПО с пользовательской подписью может создавать только компания Axis, поскольку она является владельцем ключа для подписания таких сертификатов.

Нажмите **Install (Установить)**, чтобы установить сертификат. Перед установкой встроенного ПО необходимо установить сертификат.

Пользователи

+ **Add user (Добавление пользователя)**. Щелкните, чтобы добавить нового пользователя. Можно добавить до 100 пользователей.

Username (Имя пользователя). Введите уникальное имя пользователя.

New password (Новый пароль). Введите пароль для пользователя. Длина паролей должна составлять от 1 до 64 символов. В пароле можно использовать только печатные ASCII-символы (с кодами от 32 до 126), например буквы, цифры, знаки пунктуации и некоторые другие символы.

Repeat password (Повторите ввод пароля). Введите тот же самый пароль еще раз.

Role (Роль).

- **Administrator (Администратор)**. Имеет неограниченный доступ ко всем настройкам. Администраторы также могут добавлять, обновлять и удалять других пользователей.
- **Operator (Оператор)**. Эти пользователи обладают правом доступа ко всем настройкам, кроме следующих:
  - Все **System (Системные)** настройки.
  - Добавление приложений.
- **Viewer (Наблюдатель)**. У наблюдателя есть доступ к следующему:
  - Просмотр видеопотока и создание моментальных снимков на его основе.
  - Просмотр и экспорт записей.
  - Доступ к PTZ-управлению: поворот, наклон и зум.

⋮ Элементы контекстного меню:

Update user (Обновить пользователя): Изменение свойств пользователя.

Delete user (Удалить пользователя): Удаление пользователя. Привилегированного пользователя удалить нельзя.

Anonymous users (Анонимные пользователи)

Allow anonymous viewers (Разрешить анонимный просмотр). Включите этот параметр, чтобы любой пользователь мог получить доступ к устройству в качестве наблюдателя, не выполняя вход в учетную запись.

Allow anonymous PTZ operators (Разрешить PTZ-управление анонимным операторам). Включите этот параметр, чтобы анонимные пользователи могли выполнять поворот, наклон и зум изображения.

Накопитель

Onboard storage (Встроенный накопитель)

Hard drive (Жесткий диск)

- **Free (Свободно)**: Свободный объем дискового пространства.
- **Status (Состояние)**: Указывает, подключен диск или нет.
- **File system (Файловая система)**: Файловая система, используемая диском.
- **Encrypted (Зашифровано)**: Указывает, зашифрован диск или нет.
- **Temperature (Температура)**: Текущая температура оборудования.
- **Overall heath test (Общая проверка работоспособности)**: Результат после проверки работоспособности диска.

Tools (Инструменты)

- **Check (Проверить)**: Проверка устройства хранения на наличие ошибок и попытка его автоматического восстановления.
- **Repair (Восстановить)**: Восстановить устройство хранения. Активные записи будут приостановлены во время восстановления. Восстановление устройства хранения может привести к потере данных.
- **Format (Форматировать)**: Удалить все записи и отформатировать устройство хранения. Выберите файловую систему.
- **Encrypt (Шифровать)**: Шифрование хранящихся на устройстве данных.

- **Decrypt (Расшифровать)**: Расшифровка хранящихся на устройстве данных. Все файлы на устройстве хранения будут удалены.
- **Change password (Изменить пароль)**: Изменение пароля для выполнения шифрования диска. Изменение пароля не влияет на текущие записи.
- **Use tool (Использовать инструмент)**: Нажмите, чтобы запустить выбранный инструмент

Unmount (Отключить): Щелкните перед отключением устройства от системы. Все текущие записи будут остановлены.

Write protect (Защита от записи): Включите защиту от записи, чтобы защитить устройство хранения от перезаписи.

Auto format (Автоматическое форматирование): Диск будет автоматически отформатирован с использованием файловой системы ext4.

Журналы

Отчеты и журналы

Reports (Отчёты)

- **View the device server report (Просмотр отчета сервера устройства)**. Нажмите, чтобы показать информацию о статусе устройства (в открывающемся окне). В отчет сервера автоматически добавляется журнал доступа.
- **Download the device server report (Загрузить отчет сервера устройства)**. Нажмите, чтобы скачать отчет сервера. При скачивании отчета сервера создается файл ZIP, который содержит полный отчет сервера в виде текстового файла в формате UTF-8, а также моментальный снимок текущего изображения живого просмотра. При обращении в службу поддержки всегда прикладывайте файл ZIP с отчетом сервера.
- **Download the crash report (Загрузить отчет о сбоях в работе сервера)**. Нажмите, чтобы скачать архив с подробной информацией о состоянии сервера. Отчет об отказах системы содержит сведения, включенные в отчет сервера, а также подробную информацию для отладки. Этот отчет может содержать конфиденциальную информацию, например трассировку сети. Для формирования отчета может потребоваться несколько минут.

Logs (Журналы)

- **View the system log (Просмотр журнала системных событий)**. Нажмите, чтобы показать информацию о системных событиях, таких как запуск устройства, предупреждения и важные сообщения.
- **View the access log (Просмотр журнала запросов на получение доступа)**. Нажмите, чтобы отобразить все неудачные попытки доступа к устройству, например при использовании неверного пароля для входа в систему.

Network trace (Трассировка сети)

Важно!

Файл трассировки сети может содержать конфиденциальную информацию, например сертификаты или пароли.

В файле трассировки сети регистрируются совершаемые в сети операции, что может помочь в поиске и устранении неполадок. Выберите продолжительность трассировки в секундах или минутах и нажмите **Download (Загрузить)**.

Remote system log (Удаленный системный журнал)

Системный журнал (syslog) — это стандартный способ регистрации сообщений. С его помощью можно разделить программное обеспечение, которое генерирует сообщения, систему, в которой они хранятся, и программное обеспечение, которое сообщает о них и анализирует их. Каждое сообщение помечается кодом объекта, обозначающим тип программного обеспечения, создавшего сообщение. Также сообщению назначается уровень серьезности.

+ **Server (Сервер)**. Нажмите, чтобы добавить новый сервер.

Host (Хост). Введите имя хоста или IP-адрес сервера.

Format (Форматировать): Выберите формат сообщений в системном журнале.

- RFC 3164
- RFC 5424

Protocol (Протокол). Выберите протокол и порт для использования:

- UDP (по умолчанию используется порт 514)
- TCP (по умолчанию используется порт 601)
- TLS (по умолчанию используется порт 6514)

Severity (Степень серьезности). Выберите, какие сообщения будут отправляться при срабатывании триггера.

CA certificate set (Набор сертификатов ЦС). Просмотр текущих настроек или добавление сертификата.

SSH-сервер

Secure Shell (SSH) (Протокол безопасной оболочки). Включите этот параметр, чтобы разрешить пользователю безопасно войти в систему и выполнять в сети службы оболочки и сети.

Обслуживание

Restart (Перезапуск). Перезапуск устройства. Это не повлияет на какие-либо текущие параметры. Работающие приложения перезапустятся автоматически.

Restore (Восстановить). Возврат *большинства* настроек к заводским установкам. После этого необходимо перенастроить устройство и приложения, переустановить все приложения, которые не были предустановлены, и воссоздать любые события и предустановленные положения PTZ.

Важно!

Единственными настройками, которые сохраняются после восстановления, являются следующие:

- Boot protocol (DHCP or static) (Протокол загрузки (DHCP или статический))
- Static IP address (Статический IP-адрес)
- Default router (Маршрутизатор по умолчанию)
- Subnet mask (Маска подсети)
- Параметры 802.1X
- Параметры O3C

Factory default (Заводские установки). Возврат *всех* настроек к заводским установкам. После этого необходимо сбросить IP-адрес, чтобы обеспечить возможность доступа к устройству.

Примечание.

Чтобы гарантировать то, что на вашем устройстве выполняется установка только проверенного встроенного ПО, все встроенное ПО для устройств Axis сопровождается цифровой подписью. Это еще больше повышает общий минимальный уровень кибербезопасности устройств Axis. Для получения дополнительной информации см. технический документ «Встроенное ПО с цифровой подписью, режим безопасной загрузки и защита закрытых ключей» на веб-сайте *axis.com*.

Firmware upgrade (Обновление встроенного ПО). Обновление до новой версии встроенного ПО. Новые выпуски встроенного ПО могут содержать улучшенную функциональность, исправление ошибок или совершенно новые функции. Рекомендуется всегда использовать самую последнюю версию. Чтобы скачать последнюю версию, перейдите на страницу *axis.com/support*.

В ходе обновления можно выбрать один из трех вариантов:

- **Standard upgrade (Стандартное обновление)**. Обновление до новой версии встроенного ПО.
- **Factory default (Заводские установки)**. Обновление и возврат всех настроек к заводским установкам по умолчанию. При выборе этого варианта после выполнения обновления вернуться к предыдущей версии встроенного ПО будет нельзя.
- **Autorollback (Автооткат)**. Обновление и подтверждение обновления в течение указанного срока. Если не выполнить подтверждение, устройство вернется к предыдущей версии встроенного ПО.

Firmware rollback (Откат встроенного ПО). Выполнение отката к установленной ранее версии встроенного ПО.

Расширенные настройки

Выделение мощности

Устройство видеозаписи резервирует определенное количество электроэнергии для каждого порта. Общая зарезервированная мощность не может превышать общий бюджет мощности. Если видеорегистратор попытается зарезервировать больше энергии, чем доступно, то порт не включится. Этот способ гарантирует подачу питания все на подсоединенные устройства.

Мощность PoE можно распределять между подключенными устройствами следующими способами:

- **Класс PoE** — каждый порт автоматически определяет мощность, зарезервированную в соответствии с классом PoE подсоединенного устройства.
- **LLDP** — каждый порт определяет зарезервированную мощность, обмениваясь данными PoE через протокол LLDP.

Примечание.

Распределение мощности с помощью LLDP работает только на поддерживаемых устройствах со встроенным ПО версии 9.80 или более поздней, а также для видеорегистратора AXIS S3008 Recorder со встроенным ПО версии 10.2 или более поздней.

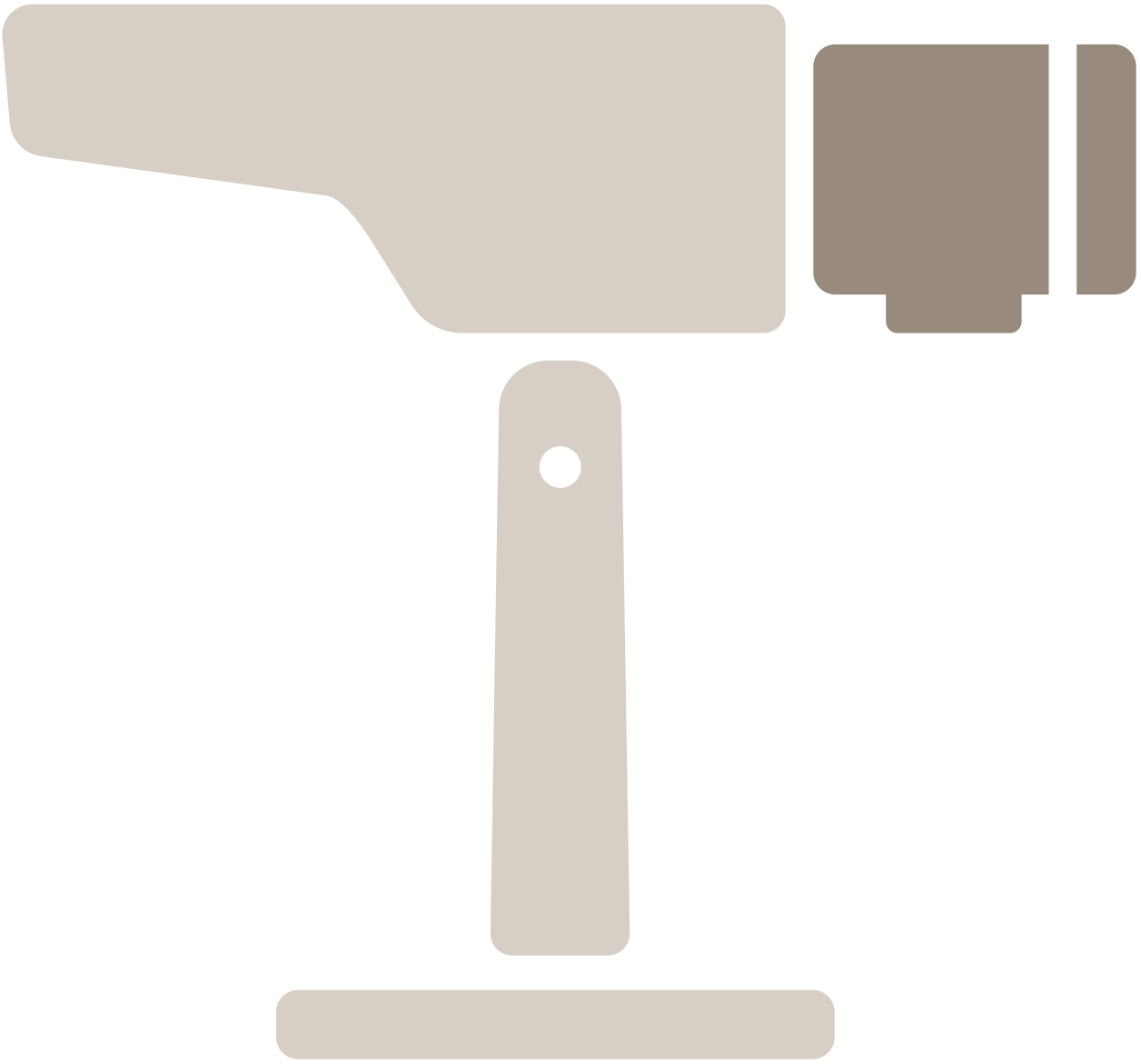
Протокол LLDP всегда активен в видеорегистраторе AXIS S3008 Recorder, но его необходимо активировать на подключенном устройстве. Если протокол LLDP выключен или не поддерживается на подключенном устройстве, то вместо него будет использоваться резервирование класса PoE.

Чтобы включить протокол LLDP на устройстве PoE, выполните следующие действия:

1. Откройте веб-страницу устройства.
2. Перейдите в меню **Settings (Настройки)** > **System (Система)** > **Plain config (Простая конфигурация)** > **Network (Сеть)**.
3. В разделе **LLDP POE** установите флажок **LLDP Send Max PoE**.

Пример

В этом примере видеорегистратор AXIS S3008 Recorder имеет общий бюджет мощности 65 Вт.



Устройство класса 2 PoE. Требует 7 Вт мощности, но фактически потребляет 5 Вт.

Устройство класса 3 PoE. Требует 15,5 Вт мощности, но фактически потребляет 7,5 Вт.

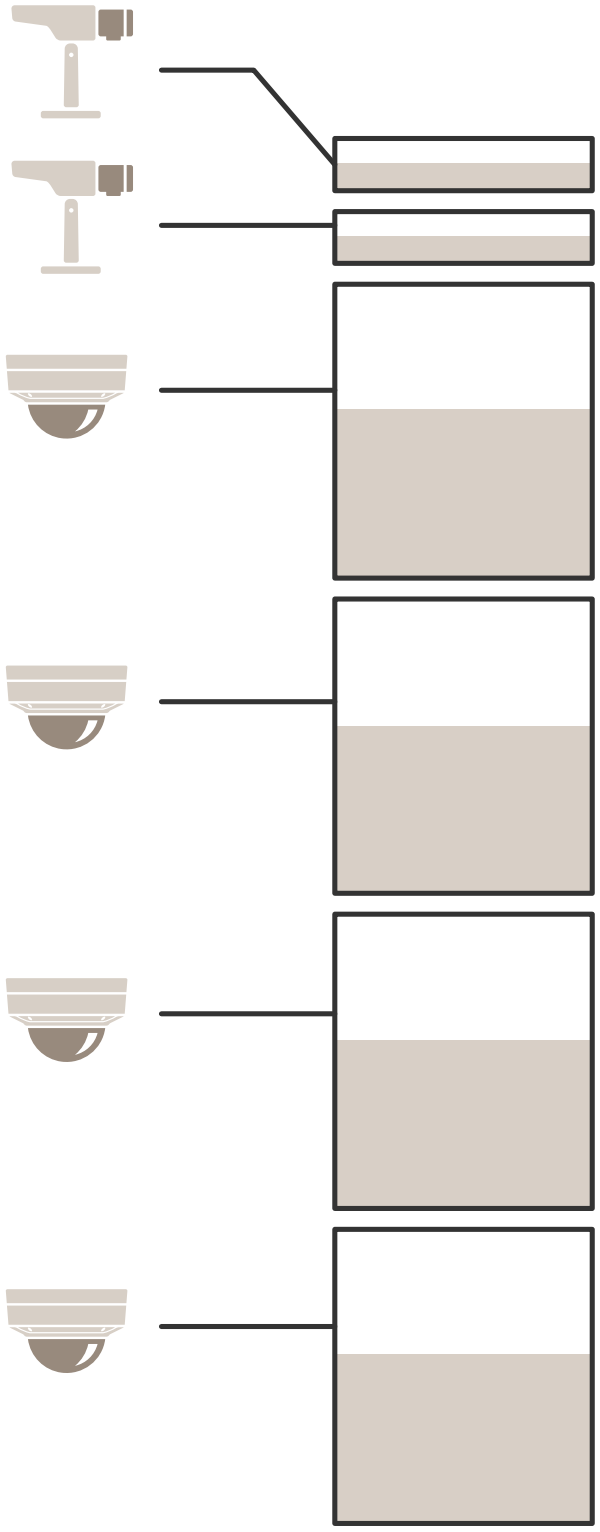
Зарезервированный объем.

Фактически потребляемая мощность.

Выделение мощности по классу PoE

Зарезервированный объем

Фактически потребляемая мощность



- Каждый порт резервирует мощность в соответствии с классом PoE устройства.
- Видеорегистратор может подавать питание на три устройства PoE класса 2, а также на два устройства PoE класса 4.
- Общая зарезервированная мощность составляет (2 x 15,5) + (4 x 7) =59 Вт.
- Фактически потребляемая мощность составляет (2 x 7,5) + (4 x 5) = 35 Вт.

Выделение мощности по протоколу LLDP

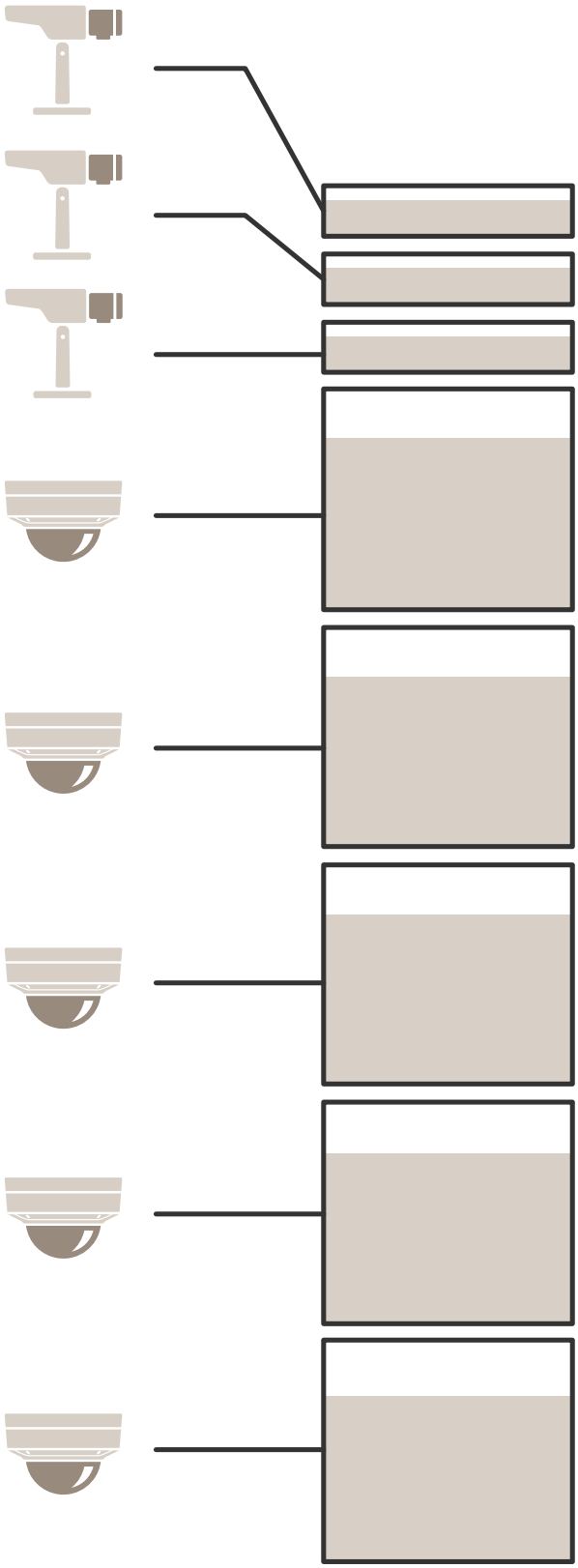
Примечание.

При выделении мощности по протоколу LLDP выделяется избыточный объем мощности для ситуации потери питания в сетевом кабеле.

Класс PoE	1	2	3
Максимальная мощность для камеры	3.84	6.49	12.95
Потеря питания в кабеле	0.14	0.41	1.92
Мощность, необходимая для видеорегистратора	3.98	6.90	14.87
Макс. мощность для класса	4.00	7.00	15.40
Зарезервированная мощность на видеорегистраторе	4 Вт	7 Вт	15,5 Вт

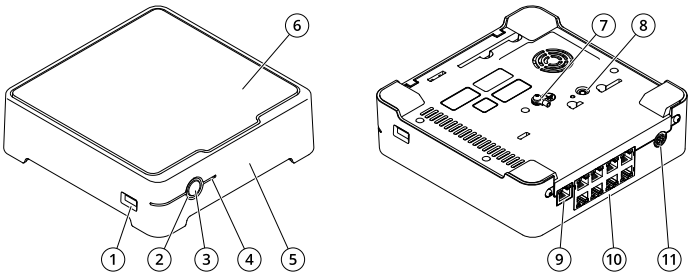
Зарезервированный объем

Фактически потребляемая мощность



- Макс. мощность, определяемая подключенным устройством.
- Каждый порт резервирует мощность в соответствии с максимально потребляемой устройством мощностью через PoE.
- Видеорегистратор может подавать питание на 8 устройств, если требования к максимальной мощности этих устройств остаются в заданных пределах.
- Общая мощность, резервируемая 8 устройствами PoE класса 3 по протоколу LLDP, составляет (8 x 7,5) = 60 Вт.
- Фактическая мощность, потребляемая 8 устройствами PoE класса 3 по протоколу LLDP, составляет (8 x 7) = 56 Вт.
- Таким образом, более экономное распределение бюджета мощности PoE позволяет подключить больше устройств.

Обзор продукта



1 *USB-порт*
2 *СИД-индикатор состояния*
3 *Кнопка питания*
4 *СИД жесткого диска*
5 *Звуковой сигнал тревоги*
6 *Жесткий диск*
7 *Заземление*
8 *Кнопка управления*
9 *Порт LAN*
10 *Порт PoE (8 шт.)*
11 *Вход питания*

Поиск и устранение неисправностей

СИД-индикатор состояния предоставляет следующую информацию:

СИД-индикатор состояния	Индикация
Зеленый	Видеорегистратор включен и работает нормально.
Оранжевый	Происходит запуск видеорегистратора или обновление встроенного ПО. Подождите, пока СИД не станет зеленым.
Красный	Это может означать, что превышен бюджет мощности PoE. Если устройство было только что подключено к видеорегистратору, попытайтесь отключить повторно. Дополнительные сведения об ограничениях мощности PoE см. в разделе *Какой объем мощности видеорегистратор может подавать на камеры? на стр. 2* .

СИД на жестком диске предоставляет следующую информацию:

СИД жесткого диска	Индикация
Зеленый	СИД мигает зеленым, когда данные записываются на жесткий диск.
Красный	Произошла ошибка записи. Для получения более подробной информации перейдите в раздел **System (Система)** > **Storage (Хранилище)**.

Звуковой сигнал раздается по следующим причинам:

- Бюджет мощности PoE превышен. Если устройство было только что подключено к видеорегистратору, попытайтесь отключить повторно. Дополнительные сведения об ограничениях мощности PoE см. в разделе *Какой объем мощности видеорегистратор может подавать на камеры? на стр. 2* .

Примечание.

Звуковой сигнал можно отключить, быстро нажав кнопку питания.

Видеорегистратор выключается:

- Устройство сильно перегрелось.

Кнопка питания

- Чтобы выключить видеорегистратор, нажмите и удерживайте кнопку питания до тех пор, пока не будет воспроизведен короткий звуковой сигнал.
- Чтобы отключить звуковой сигнал, нажмите кнопку питания.

Кнопка управления

Кнопка управления предназначена для выполнения следующих действий.

- Сброс параметров изделия к заводским установкам по умолчанию. См. раздел *Аппаратный сброс видеорегистратора на стр. 28*.
- Подключение к службе видеохостинга AXIS Video Hosting System (AVHS). Для подключения нажмите и удерживайте кнопку примерно 3 секунды, пока СИД-индикатор состояния не начнет мигать зеленым цветом.

Технические проблемы, советы и решения

Проблема	Решение
Отсутствуют видеозаписи.	См. раздел *Устранение неполадок общего характера на стр. 27*.
Не удается подключиться к камерам.	См. раздел *Устранение неполадок общего характера на стр. 27*.
Отображается уведомление об ошибке: «No contact» («Нет соединения»).	См. раздел *Устранение неполадок общего характера на стр. 27*.
Мои объекты не отображаются в мобильном приложении.	Убедитесь, что у вас установлено мобильное приложение AXIS Companion версии 4.

Устранение неполадок общего характера

Перед перезагрузкой, настройкой или сбросом ваших устройств рекомендуется сохранить системный отчет.

См. раздел *Сохранение системного отчета на стр. 29*.

1. Убедитесь, что на камеры и видеорегистратор подается электропитание.
2. Убедитесь установлено подключение к Интернету.
3. Убедитесь, что сеть работает.
4. Убедитесь, что камеры подключены к той же сети, что и компьютер (если только не используется удаленное подключение).

По-прежнему не работает?

5. Убедитесь, что в камерах и в видеорегистраторе используется встроенное ПО последней версии и что для приложения AXIS Companion на компьютере установлены все необходимые обновления.

   См. раздел *Обновление встроенного ПО на стр. 28*.
6. Перезапустите приложение AXIS Companion на компьютере.
7. Перезапустите камеры и видеорегистратор.

По-прежнему не работает?

8. Выполните аппаратный сброс камер и видеорегистратора, чтобы полностью вернуть их к заводским установкам по умолчанию.

   См. разделы и *Аппаратный сброс видеорегистратора на стр. 28*.
9. После сброса вновь добавьте камеры к своему объекту.

По-прежнему не работает?

10. Обновите видеокарту с помощью новейших драйверов.

По-прежнему не работает?

11. Сохраните системный отчет и обратитесь в *службу технической поддержки Axis*.

    См. раздел *Сохранение системного отчета на стр. 29*.

Обновление встроенного ПО

Обновления встроенного ПО открывают доступ к новым и улучшенным возможностям и функциям, а также к усовершенствованиям системы безопасности.

1. Откройте на веб-страницу главного устройства.
2. Перейдите в раздел **System (Система)** > **Maintenance (Обслуживание)** и выберите пункт **Upgrade (Обновить)** в разделе **Firmware upgrade (Обновление встроенного ПО)**.
3. Следуйте инструкциям, отображаемым на экране.

Аппаратный сброс видеорегистратора

⚠ВНИМАНИЕ!

Перемещайте видеорегистратор очень осторожно, когда он включен. Резкие движения или удары могут повредить жесткий диск.

⚠ВНИМАНИЕ!

При аппаратном сборе сохраненный пароль шифрования для жесткого диска будет удален. Если вы забудете пароль шифрования для зашифрованного жесткого диска, то это приведет к полной потере всех записей.

Примечание.

Аппаратный сброс приведет к сбросу всех параметров, включая IP-адрес.

1. Выключите видеорегистратор:

   Нажимайте кнопку питания на передней панели видеорегистратора в течение 4–5 секунд, пока не раздастся звуковой сигнал.
2. Подождите, пока видеорегистратор выключится, затем переверните его, чтобы получить доступ к кнопке управления.
3. Нажмите кнопку управления и не отпускайте ее. Нажмите и отпустите кнопку питания для запуска видеорегистратора. Отпустите кнопку управления через 15–30 секунд, когда СИД-индикатор начнет мигать желтым цветом.
4. Медленно установите видеорегистратор на место.
5. Процесс будет завершен, когда индикатор состояния начнет светиться зеленым цветом. Произошел сброс параметров устройства к заводским установкам по умолчанию. Если в сети нет сервера DHCP, используется IP-адрес по умолчанию `192.168.0.90`
6. Выполните сброс камер, подключенных к видеорегистратору. См. раздел .
7. Если жесткий диск зашифрован, его необходимо подключить вручную после сброса видеорегистратора:

   7.1 Откройте веб-страницу устройства.

   7.2 Перейдите в раздел **System (Система)** > **Storage (Хранилище)** и нажмите **Mount (Подключить)**.

   7.3 Введите пароль шифрования, используемый при шифровании жесткого диска.

Не удается войти в систему на веб-странице устройства

Если вы задали пароль для устройства во время его настройки и позже добавили это устройство на свой объект, то не сможете войти на веб-страницу устройства с помощью заданного пароля. Это связано с тем, что программное обеспечение AXIS Companion изменяет пароли всех устройств на объекте.

Чтобы войти в устройство на вашем объекте, введите имя пользователя **root** и пароль вашего объекта.

Удаление всех записей

1. Перейдите на веб-страницу устройства и выберите **System (Система)** > **Storage (Хранилище)**.
2. Выберите **Format (Форматировать)**, а затем — **Use tool (Использовать инструмент)**.

Примечание.

Эта процедура удаляет все записи с жесткого диска, но конфигурация видеорегистратора и объекта не меняется.

Сохранение системного отчета

1. В приложении AXIS Companion перейдите в меню > **Save system report (Сохранение системного отчета)**.
2. При отправке нового обращения в службу поддержки Axis приложите системный отчет.

Нужна дополнительная помощь?

Полезные ссылки

- *Руководство пользователя AXIS Companion*

Связаться со службой технической поддержки

Обратитесь в службу поддержки на странице *axis.com/support*.

Руководство пользователя
AXIS S3008 Recorder
© Axis Communications AB, 2020 - 2021
Версия M12.2
Дата: Октябрь 2021
Артикул T10152902