

AXIS Camera Station S2216 Mk II Appliance

Содержание

Начало работы.....	4
Установка устройства.....	5
Примеры настройки.....	5
Настройка в независимой сети видеонаблюдения.....	5
Настройка в существующей сети.....	6
Подключите коммутатор напрямую к корпоративной сети.....	7
Настройка устройства.....	9
Первоначальная настройка устройства видеозаписи Axis.....	9
Подключить к серверу.....	9
Подключение к удаленному серверу.....	10
Войти в AXIS Secure Remote Access.....	10
Настройка AXIS Camera Station Pro.....	11
Запуск системы управления видео.....	11
Добавить устройства.....	11
Настройка способа записи.....	12
Просмотреть живое видео.....	12
Просмотр записей.....	12
Добавление закладок.....	12
Экспорт записей.....	12
Воспроизведение и проверка записей в приложении AXIS File Player.....	13
Конфигурация сети.....	13
Настройка порта сервера.....	13
Рекомендации по обеспечению безопасности.....	13
Лицензирование системы в режиме онлайн.....	14
Лицензирование системы в автономном режиме.....	14
Управление локальными учетными записями пользователей Windows®.....	15
Создание учетной записи пользователя.....	15
Создание учетной записи администратора.....	15
Создание локальной группы пользователей.....	15
Удаление учетной записи пользователя.....	16
Изменение пароля учетной записи пользователя.....	16
Создание дискеты сброса пароля для учетной записи пользователя.....	16
Управление учетными записями пользователей AXIS Camera Station Pro.....	17
Права доступа пользователей.....	17
Добавление пользователей или групп.....	17
Права доступа пользователей или групп.....	18
Управление устройством.....	21
Обновление сертификатов функции «Безопасная загрузка».....	21
Проверка состояния сертификата.....	21
Рекомендуемые действия.....	22
Обновление сертификата через BIOS.....	22
Обновление сертификата через Windows Update.....	22
Проверка текущей версии BIOS.....	23
Обновление BIOS.....	23
Обновление Windows®.....	23
Настройка параметров обновления Windows®.....	23
Добавление дополнительного накопителя.....	24
Удаление передней панели.....	24
Установка жесткого диска.....	25
Добавление нового ресурса хранения записей.....	25
Создание тома RAID.....	25
Запуск тома RAID в Microsoft Windows®.....	26

Управление встроенным коммутатором.....	27
Сведения о встроенном коммутаторе	27
Вход на страницу управления коммутатором.....	27
Выполняемая конфигурация	27
Общее представление	27
Управление питанием	28
Выделить мощность.....	29
Включение и выключение PoE.....	30
Обзор сети.....	30
Блокировка и разблокировка портов	31
Параметры.....	31
Настройка сетевых параметров.....	31
Настройка даты и времени.....	32
Настройка сервера DHCP.....	32
Настройка SNMP.....	32
Обслуживание	32
Обновить встроенное ПО.....	32
Перезагрузка коммутатора	33
Резервное копирование настроек коммутатора	33
Восстановление настроек коммутатора	33
Управлять сертификатами	33
Изменить пароль.....	33
Настройка параметров Интернета	34
Сброс к заводским установкам	34
Журналы	34
Создание отчетов коммутатора	34
Технические характеристики	35
Обзор продукции.....	35
Передняя и задняя.....	35
Светодиодные индикаторы	35
Поиск и устранение неисправностей	37
Сброс параметров сервера.....	37
Выполнение восстановления системы.....	37
.....	37
Устранение неполадок с AXIS Camera Station Pro.....	38
Нужна дополнительная помощь?.....	39
Полезные ссылки.....	39
Связаться со службой поддержки	39

Начало работы

Стандартная процедура настройки сервера видеозаписи AXIS Camera Station Pro:

1. *Установка устройства.*
2. Первоначальная настройка Windows®: После установки устройства вам будет предложено выполнить некоторые действия для настройки региона, языка, раскладки клавиатуры, учетной записи администратора, а также пароля.
3. Первоначальная настройка устройства видеозаписи Axis: После первоначальной настройки Windows открывается программа AXIS Recorder Toolbox, где вам будет предложено выполнить несколько шагов по настройке основных и обязательных параметров, таких как имя компьютера, дата и время и используемая сеть. См. *Первоначальная настройка устройства видеозаписи Axis, on page 9.*
4. Настройте ОС Windows®. Рекомендуемые действия:
 - Обновите Windows® до последней версии. См. *Обновление Windows®, on page 23.*
 - Создайте стандартную учетную запись пользователя. См. *Создание учетной записи пользователя, on page 15*
5. Обновите AXIS Camera Station Pro до последней версии.
 - Если система подключена к сети, откройте приложение AXIS Recorder Toolbox и щелкните **Update AXIS Camera Station Pro (Обновить AXIS Camera Station Pro).**
 - Если система работает в автономном режиме, перейдите на сайт *axis.com* и загрузите последнюю версию.
6. Запустите клиент AXIS Camera Station Pro.
7. *Подключение к серверу AXIS Camera Station Pro.*
8. *Настройка AXIS Camera Station Pro, on page 11.*

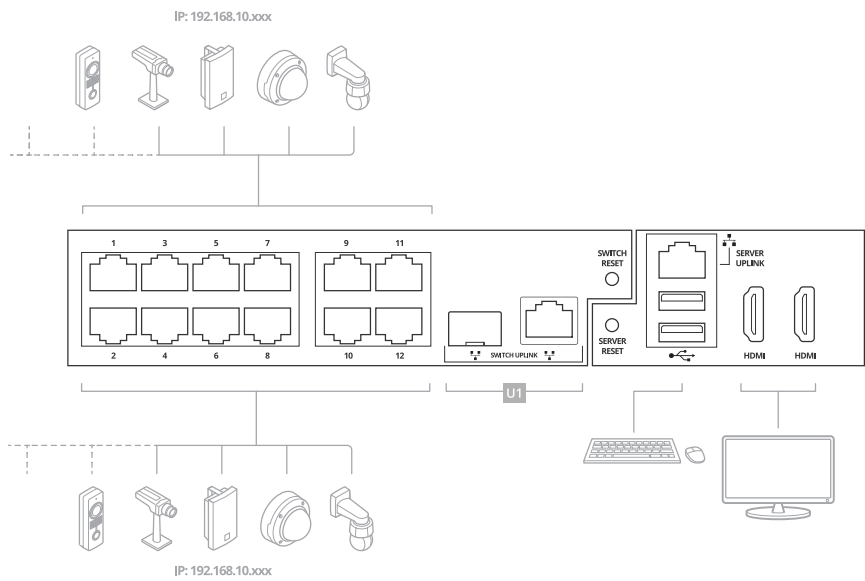
Установка устройства

Инструкции по установке устройства см. в руководстве по установке, которое входит в комплект поставки или на странице технической поддержки устройства *axis.com*.

Примеры настройки

Настройка в независимой сети видеонаблюдения

Можно создать независимую сеть для видеонаблюдения без подключений к другой внешней сети. Эта настройка выполняется автоматически. По умолчанию DHCP-сервер встроенного коммутатора включен. При подключении камер к PoE-портам камеры включаются, получают IP-адрес и становятся доступными в ПО AXIS Camera Station Pro.



Уровень сложности	Базовая авторизация
Преимущества	Выделенная сеть для охранного видеонаблюдения без подключений к другой внешней сети. Автоматическая установка
Ограничения	Пропускная способность Бюджет мощности PoE Отсутствие возможности удаленного доступа
Необходимые действия	Изменение пароля по умолчанию для встроенного коммутатора Регистрация лицензии на AXIS Camera Station Pro

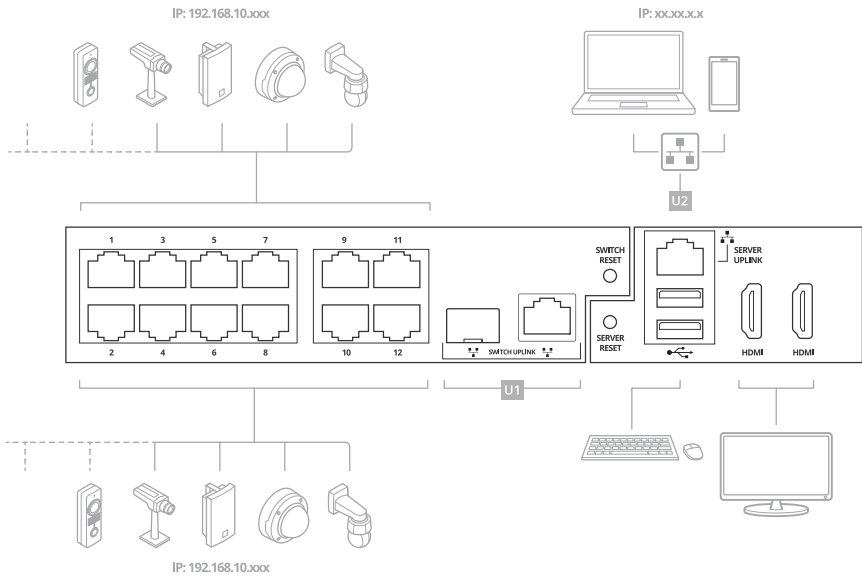
Используемые разъемы	Порты PoE Ethernet Порты USB 2.0 (для клавиатуры и мыши) Разъемы DisplayPort™ или HDMI
НЕ используемые разъемы	Порт для связи с коммутатором Порт для связи с сервером Порт USB 3.2 (передняя сторона) Универсальный аудиоразъем (передняя сторона)

Настройка в существующей сети

Можно создать сеть видеонаблюдения в существующей сети. Это означает, что сеть видеонаблюдения будет отделена от существующей сети.

Примечание

При использовании дополнительного видеорегистратора, например видеорегистратора AXIS S30 Recorder, устройство не направляет сетевые данные из сети видеонаблюдения в сеть сервера для выполнения записи. Видеорегистраторы AXIS S30 Recorders необходимо подключать к той же сети, что и камеры.

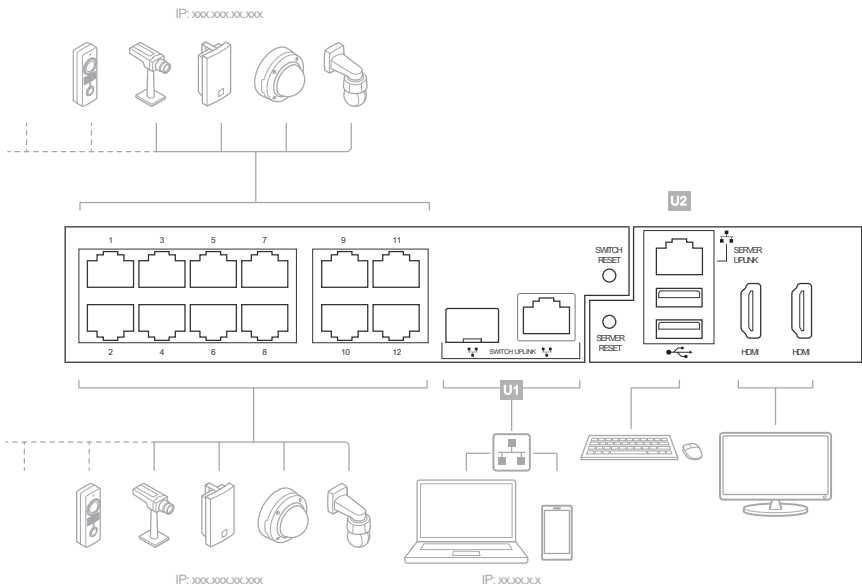


Уровень сложности	Расширенный набор
Преимущества	Возможность использовать клиент AXIS Camera Station Pro для подключения к видеосерверам серии S22 по сети. Разделение сети
Ограничения	Возможно, потребуется обеспечить соблюдение требований корпоративных сетевых политик
Необходимые действия	Изменение пароля по умолчанию для встроенного коммутатора Регистрация лицензии на AXIS Camera Station Pro

Используемые разъемы	Порты PoE Ethernet Порт Ethernet — связь с сервером для подключения к сети Порты USB 2.0 (для клавиатуры и мыши) (дополнительно) Дополнительно: разъемы DisplayPort™ или HDMI
НЕ используемые разъемы	Порт для связи с коммутатором Порт USB 3.2 (передняя сторона) Универсальный аудиоразъем (передняя сторона)

Подключите коммутатор напрямую к корпоративной сети

Такая конфигурация интегрирует систему непосредственно в существующую корпоративную сеть, обеспечивая доступ к камерам и их мониторинг из любой точки сети.



Уровень сложности	Расширенный набор
Преимущества	Доступ к камерам осуществляется из корпоративной сети, а для мониторинга можно использовать сервер SNMP.
Ограничения	Возможно, потребуется обеспечить соблюдение требований корпоративных сетевых политик
Необходимые действия	Выключите протокол DHCP на коммутаторе Присвойте коммутатору статический IP-адрес из корпоративной сети Настройте для внутреннего сетевого адаптера компьютера DHCP-адрес или статический IP-адрес в корпоративной сети Измените пароль коммутатора по умолчанию.

	Настройка и регистрация AXIS Camera Station Pro
Используемые разъемы	Порты PoE Ethernet Порт для связи с коммутатором (U1) Порты USB 2.0 (для клавиатуры и мыши) (дополнительно) Дополнительно: разъемы DisplayPort™ или HDMI
НЕ используемые разъемы	Порт для связи с компьютером (U2) Порт USB 3.2 (передняя сторона) Универсальный аудиоразъем (передняя сторона)

Настройка устройства

Первоначальная настройка устройства видеозаписи Axis

После настройки Windows® автоматически запустится программа AXIS Recorder Toolbox и откроется мастер настройки при первом запуске Setup Assistant. В помощь этого мастера вы настроите несколько базовых параметров, необходимых для последующего управления устройством в AXIS Recorder Toolbox.

Примечание

Это настройки сервера. Чтобы изменить настройки коммутатора, перейдите на страницу управления коммутатором. См. *Параметры, on page 31*

1. Выберите тему **Light (Светлая)** или **Dark (Темная)** и нажмите кнопку **Next (Далее)** (если это доступно для вашего устройства).
2. При необходимости измените имя компьютера и нажмите кнопку **Next (Далее)**.
3. В разделе **Date and time (Дата и время)** настройте следующие параметры и нажмите **Next (Далее)**.
 - Выберите часовой пояс.
 - Чтобы настроить NTP-сервер, выберите **NTP server (NTP-сервер)** и введите адрес NTP-сервера.
 - Для настройки вручную выберите **Manual (Вручную)**, затем введите дату и время.
4. В разделе **Network settings (Настройки сети)** настройте следующие параметры и нажмите **Next (Далее)**.
 - Параметры **Use automatic IP settings (DHCP) (Использовать автоматическую настройку IP-адреса (DHCP))** и **Use automatic DNS settings (Использовать автоматическую настройку DNS-сервера)** по умолчанию включены.
 - Если устройство подключено к сети с DHCP-сервером, автоматически отображаются назначенные сервером IP-адрес, маска подсети, шлюз и предпочитаемый DNS.
 - Если устройство не подключено к сети или в ней нет DHCP-сервера, введите ручную соответствующие IP-адрес, маску подсети, шлюз и предпочитаемый DNS-сервер.
5. Нажмите **Finish ("Завершить")**. Если имя компьютера было изменено, AXIS Recorder Toolbox предложит перезагрузить устройство.

Подключить к серверу

Клиент AXIS Camera Station S2216 Mk II Appliance позволяет подключаться к одному или нескольким серверам различными способами:

Последние использовавшиеся серверы – Подключитесь к серверам, использованным в предыдущем сеансе.

Этот компьютер – Подключитесь к серверу, установленному на том же компьютере, что и клиент.

Удаленный сервер – См. *Подключение к удаленному серверу, on page 10*.

Примечание

- При первом подключении к серверу клиент проверяет идентификатор сертификата сервера. Чтобы убедиться, что подключение выполняется к правильному серверу, сравните идентификатор сертификата с идентификатором, отображаемым в AXIS Camera Station S2216 Mk II ApplianceService Control (Управление сервисом).

Список серверов	Чтобы подключиться к серверам из списка серверов, выберите один из раскрывающегося меню Server list (Список серверов) . Выберите  для составления или изменения списков серверов.
Импортировать список серверов	Чтобы импортировать список серверов, экспортированный из AXIS Camera Station, нажмите Import server list (Импортировать список серверов) и найдите файл .msl.
Удалить сохраненные пароли	Чтобы удалить сохраненные имена пользователей и пароли на всех подключенных серверах, нажмите Delete saved passwords (Удалить сохраненные пароли) .
Изменить настройки клиента проху	Если не удастся подключиться к серверу, возможно, необходимо обновить настройки прокси-сервера клиента. Нажмите Change client proxy settings (Изменить параметры прокси-сервера для клиента) .

Подключение к удаленному серверу

1. Выберите **Удаленный сервер**.
2. Выберите сервер в раскрывающемся списке **Remote server (Удаленный сервер)** или введите IP-адрес или адрес DNS. Если сервер отсутствует в списке, нажмите , чтобы обновить список всех доступных удаленных серверов. Если сервер настроен на подключение клиентских узлов через порт, отличный от заданного по умолчанию порта 55754, введите IP-адрес, а за ним — номер порта, например 192.168.0.5:46001.
3. Выполните одно из следующих действий:
 - Выберите **Log in as current user (Войти как текущий пользователь)**, чтобы войти в систему как текущий пользователь Windows®.
 - Снимите флажок **Log in as current user (Войти как текущий пользователь)** и нажмите **Log in (Войти)**. Выберите **Other user (Другой пользователь)** и введите другое имя пользователя и пароль, чтобы войти в систему с другими учетными данными.

Войти в AXIS Secure Remote Access

Внимание

Чтобы улучшить безопасность и функциональность, мы обновляем **Axis Secure Remote Access** версии 1 до **Axis Secure Remote Access** версии 2. Поддержка текущей версии будет прекращена 1 декабря 2025 года. Настоятельно рекомендуем до этого момента перейти на **Axis Secure Remote Access 2**.

Что это означает для вашей системы **AXIS Camera Station S2216 Mk II Appliance**?

- После 1 декабря 2025 года вы не сможете удаленно получать доступ к системе с помощью **Axis Secure Remote Access 1**.
- Чтобы использовать **Axis Secure Remote Access 2**, установите **AXIS Camera Station Pro 6.8**. До 1 марта 2026 года это обновление бесплатно предоставляется всем пользователям **AXIS Camera Station 5**.

Примечание

- При попытке подключения к серверу с помощью Axis Secure Remote Access сервер не может автоматически обновить клиент.
 - Если прокси-сервер находится между сетевым устройством и сервером AXIS Camera Station S2216 Mk II Appliance, необходимо настроить прокси-сервер в Windows на сервере AXIS Camera Station S2216 Mk II Appliance для доступа к серверу с помощью AXIS Secure Remote Access.
1. Перейдите по ссылке **Войти в службу AXIS Secure Remote Access**.
 2. Введите учетные данные My Axis.
 3. Нажмите **Sign in (Войти)**.
 4. Нажмите **Grant (Предоставить)**.

Настройка AXIS Camera Station Pro

Прежде чем начать, убедитесь в следующем:

- Выполните настройку сети с учетом особенностей вашей системы. См. *Конфигурация сети*.
- При необходимости настройте порты сервера. См. *Настройка порта сервера*.
- Примите во внимание аспекты безопасности. См. *Рекомендации по обеспечению безопасности*.

Выполнив необходимую настройку, вы можете приступать к работе с AXIS Camera Station Pro.

1. *Запуск системы управления видео*
2. *Добавить устройства*
3. *Настройка способа записи, on page 12*
4. *Просмотреть живое видео, on page 12*
5. *Просмотр записей, on page 12*
6. *Добавление закладок, on page 12*
7. *Экспорт записей, on page 12*
8. *Воспроизведение и проверка записей в приложении AXIS File Player, on page 13*

Запуск системы управления видео

Чтобы запустить клиент AXIS Camera Station Pro, дважды щелкните его значок. При первом запуске клиент пытается войти на сервер AXIS Camera Station Pro, установленный на том же компьютере, что и клиент.

Можно подключиться к нескольким серверам AXIS Camera Station Pro разными способами.

Добавить устройства

При первом запуске AXIS Camera Station S2216 Mk II Appliance открывается страница **Add devices (Добавление устройств)**, на которой выполняется поиск устройств в сети для последующего добавления.

1. Выберите устройства, которые необходимо добавить, из списка. Если устройство не удастся найти, нажмите **Manual search (Ручной поиск)** или используйте ввод для фильтрации.
2. Нажмите **Добавить**.
3. Нажмите **Close (Заккрыть)**, чтобы пропустить настройку и продолжить позже. Чтобы продолжить настройку сразу:
 - 3.1. Выберите: **Quick configuration (Быстрая настройка)** или **Site Designer configuration (Конфигурация AXIS Site Designer)**. Для получения дополнительных сведений см. .
 - 3.2. Выберите **Add image overlay for date, time, and text (Добавить наложение изображения с датой, временем и текстом)**, чтобы добавить экранные наложения на камеры Axis, для которых они еще не настроены.

- 3.3. Нажмите **Next** ("Далее").
- 3.4. Выберите предпочтительный режим записи **Recording method**.
- 3.5. Нажмите **Next** (Далее).
- 3.6. Выберите **Retention time** (Время хранения) и **Recording storage** (Хранилище записи) и нажмите **Finish** (Готово) для применения конфигурации.

Настройка способа записи

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Выберите камеру.
3. Включите функцию **Motion detection** (Обнаружение движения) или **Continuous** (Непрерывная) или обе.
4. Нажмите **Применить**.

Просмотреть живое видео

1. Откройте вкладку **Live view** (Живой просмотр).
2. Выберите камеру для просмотра видео в реальном времени.

Просмотр записей

1. Откройте вкладку **Recordings** (Записи).
2. Выберите камеру, с которой вы хотите просмотреть записи.

Добавление закладок

1. Перейти к записи.
2. На шкале времени можно увеличить, уменьшить масштаб или установить соответствующий маркер в нужном местоположении.
3. Нажмите .
4. Введите имя и описание закладки. Используйте ключевые слова, чтобы упростить поиск закладки.
5. Выберите **Запретить удаление записи**, чтобы заблокировать запись.

Примечание

Чтобы разблокировать запись, снимите флажок **Prevent recording deletion** (Запретить удаление записи) или удалите закладку.

6. Щелкните **ОК**, чтобы сохранить закладку.

Экспорт записей

1. Откройте вкладку **Recordings** (Записи).
2. Выберите камеру, с которой вы хотите экспортировать записи.
3. Нажмите значок  для отображения маркеров выбора.
4. Перетаскивая маркеры, выберите записи, которые требуется экспортировать.
5. Нажмите , чтобы открыть вкладку **Export** (Экспорт).
6. Нажмите на **Export...** (Экспорт)

Воспроизведение и проверка записей в приложении AXIS File Player

1. Перейдите в папку с экспортированными записями.
2. Дважды щелкните значок приложения AXIS File Player.
3. Нажмите , чтобы показать заметки к записи.
4. Для проверки цифровой подписи:
 - 4.1. Перейдите в меню Tools (Инструменты) > Verify digital signature (Проверка цифровой подписи).
 - 4.2. Выберите Validate with password (Проверка с паролем) и введите пароль.
 - 4.3. Нажмите Verify (Проверить), чтобы просмотреть результаты проверки.

Примечание

- Цифровая подпись отличается от подписанного видео. Подписанное видео позволяет проследить происхождение записи до камеры, с которой она была получена, и убедиться, что запись не подвергалась изменениям. Дополнительные сведения см. в разделе *Видео с цифровой подписью* и в руководстве пользователя камеры.
- Если сохраненные файлы не связаны с базой данных AXIS Camera Station (неиндексированные файлы), их необходимо конвертировать, чтобы воспроизводить в AXIS File Player. Чтобы получить помощь в конвертировании файлов, обратитесь в службу технической поддержки Axis.

Конфигурация сети

Настройте параметры прокси-сервера или межсетевого экрана перед использованием AXIS Camera Station S2216 Mk II Appliance, если клиент, сервер и подключенные сетевые устройства находятся в разных сетях.

Настройки прокси клиента

Если между клиентом и сервером используется прокси-сервер, настройте параметры прокси в Windows на компьютере клиента. Обратитесь в службу поддержки Axis для получения дополнительной информации.

Параметры прокси-сервера на сервере

Если прокси-сервер находится между сетевым устройством и сервером, необходимо настроить параметры прокси-сервера в Windows на сервере. Обратитесь в службу поддержки Axis для получения дополнительной информации.

NAT и межсетевой экран

Если между клиентом и сервером находится устройство NAT или межсетевой экран, настройте его таким образом, чтобы через него могли проходить HTTP-порт, TCP-порт и порт потоковой передачи, указанные в AXIS Camera Station S2216 Mk II Appliance Service Control (Управление сервисом). При необходимости обратитесь за помощью к сетевому администратору.

Настройка порта сервера

Сервер AXIS Camera Station S2216 Mk II Appliance использует порты 55752 (HTTP), 55754 (TCP), 55756 (мобильная связь) и 55757 (мобильная потоковая передача) для связи между сервером и клиентом. При необходимости порты можно изменить с помощью приложения AXIS Camera Station Service Control.

Рекомендации по обеспечению безопасности

Для предотвращения несанкционированного доступа к камерам и записям:

- Используйте надежные пароли для всех сетевых устройств (камер, видеокодеров и дополнительных устройств).
- Установите сервер AXIS Camera Station S2216 Mk II Appliance, камеры, видеокодеры и дополнительные устройства в защищенной сети, отделенной от офисной сети. Вы можете

установить клиент AXIS Camera Station S2216 Mk II Appliance на компьютере в другой сети, например в сети с доступом в Интернет.

- Убедитесь, что у всех пользователей надежные пароли.

Лицензирование системы в режиме онлайн

Обратите внимание, что для использования автоматического лицензирования необходимо зарегистрировать систему и привязать ее к организации.

1. Перейдите к пункту **Configuration > Licenses > Management** (Конфигурация > Лицензии > Управление).
2. Убедитесь, что включена опция **Automatic licensing** (Автоматическое лицензирование).
3. Нажмите кнопку **Register...** (Регистрация).
4. Войдите в свою учетную запись **My Axis** и следуйте отображаемым на экране инструкциям.
5. Нажмите **Go to AXIS License Manager** (Перейти в AXIS License Manager) для управления лицензиями. Дополнительные сведения см. в *руководстве пользователя My Systems* на сайте help.axis.com.

Лицензирование системы в автономном режиме

Для лицензирования системы в ручном режиме:

1. Перейдите к пункту **Configuration > Licenses > Management** (Конфигурация > Лицензии > Управление).
2. Деактивируйте опцию **Automatic licensing** (Автоматическое лицензирование).
3. Нажмите кнопку **Export system file...** (Экспортировать системный файл) и сохраните файл на свой компьютер.

Примечание

Для доступа к **AXIS License Manager** требуется интернет-соединение. Если ваш клиентский компьютер не подключен к Интернету, скопируйте системный файл на компьютер с доступом в сеть.

4. Откройте *AXIS License Manager*.
5. В **AXIS License Manager**:
 - 5.1. Выберите нужную организацию или создайте новую при необходимости. Дополнительные сведения см. в *руководстве пользователя My Systems* на сайте help.axis.com.
 - 5.2. Перейдите в раздел **System setup** (Настройка системы).
 - 5.3. Нажмите **Upload system file** (Загрузить системный файл).
 - 5.4. Нажмите **Upload system file** (Загрузить системный файл) повторно и укажите путь к вашему системному файлу.
 - 5.5. Нажмите **Upload system file** (Загрузить системный файл).
 - 5.6. Нажмите **Download license file** (Скачать файл лицензии).
6. Вернитесь в клиентское приложение **AXIS Camera Station S2216 Mk II Appliance**.
7. Нажмите **Import license file...** (Импортировать файл лицензии...) и выберите свой файл лицензии.
8. Нажмите **Go to AXIS License Manager** (Перейти в AXIS License Manager) для управления лицензиями.

Управление локальными учетными записями пользователей Windows®

Создание учетной записи пользователя

Чтобы обеспечить безопасность ваших личных данных и информации, для каждой локальной учетной записи рекомендуется создать пароль.

Внимание

После создания пароля для локальной учетной записи сохраните его где-нибудь, чтобы не забыть. Для локальных учетных записей восстановить утерянный пароль невозможно.

1. Откройте меню **Настройки > Учетные записи > Другие пользователи > Добавить другого пользователя** и нажмите **Добавить учетную запись**.
2. Нажмите кнопку **I don't have this person's sign-in information (У меня нет учетных данных этого пользователя)**.
3. Нажмите **Add a user without a Microsoft account (Добавить пользователя без учетной записи Майкрософт)**.
4. Введите имя пользователя, пароль и подсказку для пароля.
5. Нажмите **Next (Далее)** и следуйте инструкциям.

Создание учетной записи администратора

1. Перейдите в раздел **Settings > Accounts > Other people (Параметры > Учетные записи > Другие пользователи)**.
2. Перейдите к учетной записи, которую вы хотите изменить, и выберите пункт **Change account type (Изменить тип учетной записи)**.
3. Перейдите в раздел **Account type (Тип учетной записи)** и выберите **Administrator (Администратор)**.
4. Нажмите кнопку **ОК**.
5. Перезапустите устройство и войдите в систему, используя новую учетную запись администратора.

Создание локальной группы пользователей

1. Перейдите в раздел **Computer Management (Управление компьютером)**.
2. Перейдите в раздел **Local Users and Groups > Group (Локальные пользователи и группы > Группа)**.
3. Щелкните правой кнопкой мыши **Group (Группа)** и выберите **New Group (Создать группу)**.
4. Введите имя и описание группы.
5. Добавление членов группы:
 - 5.1. Нажмите **Добавить**.
 - 5.2. Нажмите **Дополнительно**.
 - 5.3. Найдите учетные записи пользователей, которые нужно добавить в группу, и нажмите кнопку **ОК (ОК)**.
 - 5.4. Нажмите кнопку **ОК (ОК)** еще раз.
6. Нажмите **Create (Создать)**.

Удаление учетной записи пользователя

Внимание

При удалении учетной записи пользователя она удаляется с экрана входа в систему. Вы также удаляете все файлы, настройки и данные программ, сохраненные для этой учетной записи пользователя.

1. Перейдите в раздел **Settings > Accounts > Other people** (Параметры > Учетные записи > Другие пользователи).
2. Перейдите к учетной записи, которую вы хотите удалить, и нажмите **Remove** (Удалить).

Изменение пароля учетной записи пользователя

1. Войдите в систему, используя учетную запись администратора.
2. Перейдите в раздел **User Accounts > User Accounts > Manage another account in sequence** (Учетные записи пользователей > Учетные записи пользователей > Управление другой учетной записью в последовательности).
Вы увидите список со всеми учетными записями пользователей на устройстве.
3. Выберите учетную запись пользователя, чей пароль вы хотите изменить.
4. Нажмите кнопку **Change the password** (Изменить пароль).
5. Введите новый пароль и нажмите **Change password** (Изменить пароль).

Создание дискеты сброса пароля для учетной записи пользователя

Дискету сброса пароля рекомендуется создавать на USB-накопителе. С помощью этой дискеты может выполняться сброс пароля. Без дискеты сброса пароля выполнение процедуры сброса пароля невозможно.

Примечание

Если используется Windows® 10 или более поздняя версия этой системы, вы можете добавить контрольные вопросы в свою локальную учетную запись, на случай если вы забудете свой пароль. В этом случае не потребуется создавать дискету сброса пароля. Чтобы сделать это, перейдите в меню **Start** (Пуск) и выберите **Settings > Sign-in options > Update your security questions** (Параметры > Параметры входа > Обновить контрольные вопросы).

1. Войдите в устройство, используя локальную учетную запись пользователя. Для подключенной учетной записи дискету сброса пароля создать невозможно.
2. Вставьте пустой USB-накопитель в устройство.
3. В поле поиска Windows® введите **Create a password reset disk** (Создание дискеты сброса пароля).
4. В помощнике настройки забытых паролей нажмите кнопку **Next** (Далее).
5. Выберите нужный USB-накопитель и нажмите **Next** (Далее).
6. Введите свой текущий пароль и нажмите **Next** (Далее).
7. Следуйте инструкциям на экране.
8. Извлеките USB-накопитель и сохраните его в безопасном месте. При изменении пароля создавать новую дискету не требуется (даже при многократном изменении пароля).

Управление учетными записями пользователей AXIS Camera Station Pro

Права доступа пользователей

Перейдите в Configuration (Конфигурация) > Security (Безопасность) > User permissions (Разрешения пользователя), чтобы увидеть пользователей и группы в AXIS Camera Station S2216 Mk II Appliance.

Примечание

Администраторы компьютера, на котором работает сервер AXIS Camera Station S2216 Mk II Appliance, автоматически получают права администратора в AXIS Camera Station S2216 Mk II Appliance. Права доступа группы администраторов нельзя изменить или удалить.

Перед добавлением пользователя или группы убедитесь, что они зарегистрированы на локальном компьютере или имеют учетную запись пользователя Windows® Active Directory. Чтобы добавить пользователя или группу, см. *Добавление пользователей или групп*.

Если пользователь входит в группу, ему предоставляется наивысший уровень прав, назначенный либо непосредственно пользователю, либо группе. Например, пользователь, имеющий доступ к камере X и одновременно входящий в группу с доступом к камерам Y и Z, получает доступ ко всем трем камерам.

	Тип записи: индивидуальный пользователь.
	Указывает на групповой тип записи.
Название	Имя пользователя в том виде, как оно отображается на локальном компьютере или в Active Directory.
Домен	Домен, к которому относится пользователь или группа.
Тип доступа	Роль доступа, назначенная пользователю или группе. Возможные значения роли: администратор, оператор и наблюдатель.
Сведения	Подробная информация о пользователе в том виде, как она отображается на локальном компьютере или в Active Directory.
Сервер	Сервер, к которому относится пользователь или группа.

Добавление пользователей или групп

Доступ к AXIS Camera Station S2216 Mk II Appliance могут получать пользователи и группы Microsoft Windows® и Active Directory. Чтобы добавить пользователя в AXIS Camera Station S2216 Mk II Appliance, добавьте пользователей или группу в Windows®.

Чтобы добавить пользователя в Windows® 10 и 11:

- Нажмите клавиши Windows + X и выберите **Computer Management (Управление компьютером)**.
- В окне **Computer Management (Управление компьютером)** перейдите к разделу **Local Users and Groups (Локальные пользователи и группы) > Users (Пользователи)**.
- Щелкните правой кнопкой мыши **Users (Пользователи)** и выберите **New User (Новый пользователь)**.
- Во всплывающем диалоговом окне введите данные нового пользователя и снимите флажок **User must change password at next login (Пользователь должен изменить пароль при следующем входе)**.
- Нажмите **Create (Создать)**.

Если вы используете домен Active Directory, обратитесь к администратору сети.

Добавление пользователей или групп

1. Перейдите в меню **Configuration (Конфигурация) > Security (Безопасность) > User permissions (Разрешения пользователей)**.
2. Нажмите **Добавить**. Доступные пользователи и группы отображаются в списке.
3. В разделе **Scope (Область действия)** укажите, где нужно искать пользователей и группы.
4. В разделе **Show (Отображение)** можно задать отображение пользователей или групп. Если пользователей или групп слишком много, результаты поиска могут не отображаться. Используйте фильтр, чтобы сузить результаты поиска.
5. Выберите пользователей или группы и нажмите **Добавить**.

Область действия	
Сервер	Выберите для поиска пользователей или групп на локальном компьютере.
Домен	Выберите для поиска пользователей или групп Active Directory.
Выбранный сервер	При подключении к нескольким серверам AXIS Camera Station S2216 Mk II Appliance выберите сервер, на котором необходимо выполнить поиск пользователей или групп.

Настройка пользователя или группы

1. Выберите пользователя или группу в списке.
2. В разделе **Role (Роль)** выберите **Administrator (Администратор)**, **Operator (Оператор)** или **Viewer (Наблюдатель)**.
3. Если выбрать пункт **Operator (Оператор)** или **Viewer (Наблюдатель)**, вы сможете настроить права доступа пользователей или групп. См. *Права доступа пользователей или групп*.
4. Нажмите **Save ("Сохранить")**.

Удаление пользователя или группы

1. Выберите пользователя или группу.
2. Выберите пункт **Remove (Удалить)**.
3. В появившемся диалоговом окне нажмите **ОК**, чтобы подтвердить удаление пользователя или группы.

Права доступа пользователей или групп

Пользователю или группе можно назначить одну из трех ролей. О том как определить роль для пользователя или группы, см. *Добавление пользователей или групп*.

Администратор – Полный доступ ко системе, включая доступ к живому просмотру и видеозаписям со всех камер, доступ ко всем портам ввода-вывода и режимам видеонаблюдения. Эта роль необходима для доступа к настройкам системы.

Оператор – Выберите камеры, виды и порты ввода/вывода, чтобы предоставить доступ к просмотру видео в реальном времени и архивных записей. Оператор имеет полный доступ ко всем функциям AXIS Camera Station S2216 Mk II Appliance за исключением системных настроек.

Наблюдатель – Доступ к живому видео с выбранных камер, портов ввода-вывода и видов. У наблюдателя нет доступа к видеозаписям и системным настройкам.

Камеры

Пользователи или группы, которым назначена роль **Operator (Оператор)** или **Viewer (Наблюдатель)**, имеют следующие права.

Доступ	разрешен доступ к камере и всем функциям камеры.
Видео	разрешен доступ к живому видео с этой камеры.
Прослушать звук	Разрешить прослушивание звука с камеры.
Воспроизведение голоса	Разрешить голосовое вещание через камеру.
Запись в ручном режиме	Разрешить ручной запуск и остановку записи.
Механическое управление позиционером (PTZ)	разрешен доступ к механическому PTZ-управлению. Доступно только для камер с механическим PTZ.
Приоритет PTZ-управления	Задать приоритет PTZ-управления. Чем меньше значение, тем выше приоритет. Приоритет не назначен, 0. Администратор обладает самым высоким приоритетом. Если PTZ-камерой управляет пользователь с ролью более высокого приоритета, остальные пользователи не могут управлять этой камерой в течение 10 секунд (по умолчанию). Доступно только для камер с механическим PTZ, для которых выбран параметр Mechanical PTZ (Механическое PTZ-управление) .

Виды

Пользователи или группы, которым назначена роль **Operator (Оператор)** или **Viewer (Наблюдатель)**, имеют следующие права. Можно выбрать несколько видов и задать права доступа.

Доступ	Разрешить доступ к видам в AXIS Camera Station S2216 Mk II Appliance.
Изменить	Разрешает редактирование видов в AXIS Camera Station S2216 Mk II Appliance.

Вводы/выводы

Пользователи или группы, которым назначена роль **Operator (Оператор)** или **Viewer (Наблюдатель)**, имеют следующие права.

Доступ	разрешен полный доступ к порту ввода-вывода.
Считывание	Разрешает просматривать состояние порта ввода/вывода без возможности его изменения.
Запись	Разрешает изменять состояние порта ввода/вывода.

Система

Невозможно настроить права доступа, выделенные в списке серым цветом. Флажок означает, что пользователь или группа имеет данное право по умолчанию.

Пользователи или группы, которым назначена роль **Operator (Оператор)**, имеют следующие права. Для роли **Viewer (Наблюдатель)** также доступна функция **Take snapshots (Сделать снимок)**.

Сделать снимок	Разрешает создавать снимки в режиме живого просмотра и при просмотре записей.
Экспорт записей	Позволяет экспортировать записи.
Создать отчет об инцидентах	Позволяет создавать отчеты об инцидентах.
Prevent access to recordings older than (Запрещен доступ к записям старше, чем)	Запрещает доступ к записям старше указанного периода времени (в минутах). Пользователи не могут найти эти записи при поиске.
Доступ к сигналам тревоги, задачам и журналам	Получение уведомлений о сигналах тревоги и разрешение доступа к панели Alarms and tasks (Тревоги и задачи) и вкладке Logs (Журналы) .
Доступ к данным поиска	Разрешить поиск данных, чтобы отслеживать, что произошло во время события.
Добавление категорий к событиям	Разрешить добавление категорий к событиям на вкладке Recordings (Записи) .
Удаление категорий из события	Разрешить удаление категорий из событий на вкладке Recordings (Записи) .

Контроль доступа

Пользователи или группы, которым назначена роль **Operator (Оператор)**, имеют следующие права. Для роли **Viewer (Наблюдатель)** также доступен пункт **Access Management (Управление доступом)**.

Настройка контроля доступа	Позволяет настраивать двери и зоны, профили идентификации, форматы карт и ПИН-коды, зашифрованный обмен данными и многосерверные функции.
Контроль доступа	Позволяет управлять доступом и осуществлять доступ к настройкам Active Directory.

Пользователи или группы, которым назначена роль **Viewer (Наблюдатель)**, имеют следующие права.

Контроль работоспособности системы

Пользователи или группы, которым назначена роль **Operator (Оператор)**, имеют следующие права. Для роли **Viewer (Наблюдатель)** также доступен пункт **Доступ к контролю работоспособности системы**.

Настройка контроля работоспособности системы	Позволяет настройку контроля работоспособности системы.
Доступ к контролю работоспособности системы	Позволяет получить доступ к контролю работоспособности системы.

Управление устройством

Обновление сертификатов функции «Безопасная загрузка».

Microsoft прекращает использование сертификатов функции «Безопасная загрузка» 2011 года в июне 2026 года и заменяет их новыми сертификатами 2023 года. Чтобы обеспечить безопасную работу регистратора, установите сертификаты 2023 года до этого срока.

Для установки сертификатов 2023 года требуется Windows 10 LTSC (Long-Term Servicing Channel) или Windows 11 LTSC. Если ваше устройство находится на гарантии, но работает под управлением Windows 10 SAC (Semi-Annual Channel) вместо версии LTSC, обратитесь в службу технической поддержки Axis. Специалисты сообщают, можно ли обновить систему до версии LTSC перед обновлением BIOS или изменением сертификатов.

Примечание

После июня 2026 года устройства без сертификатов 2023 года продолжат работать в обычном режиме, однако не будут получать новые средства защиты для раннего этапа загрузки, включая обновления Windows Boot Manager и списки отзыва сертификатов для устранения новых уязвимостей.

Проверка состояния сертификата

Чтобы убедиться, что сертификаты 2023 года установлены и загрузчик Windows обновлен, воспользуйтесь одним из следующих способов:

Способ 1:

1. Откройте Редактор реестра.
2. См. раздел HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing.
3. Проверьте значение UEFICA2023Status. Если значение равно Updated, сертификат 2023 года установлен.

 (Default)	REG_SZ	(value not set)
 BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
 ConfidenceLevel	REG_SZ	No Data Observed - Action Required
 ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
 LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
 UEFICA2023Status	REG_SZ	Updated
 WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

Способ 2:

1. Откройте Windows Security (Безопасность Windows).
2. Перейдите в раздел Device security (Безопасность устройства).
3. В разделе Secure boot (Безопасная загрузка) проверьте сообщение о состоянии. Если сертификат актуален, отображается следующее сообщение: Secure Boot is on and all required certificate updates have been applied. No further certificate changes are needed (Безопасная загрузка включена, и все необходимые обновления сертификатов применены. Дополнительное обновление сертификатов не требуется).

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

Примечание

Приложение «Безопасность Windows» отображает состояние сертификата только в том случае, если на устройстве установлено накопительное обновление Windows от 14 апреля 2026 года или более поздней версии. Если сообщение о состоянии сертификата отсутствует, установите последнее обновление Windows или воспользуйтесь способом 1.

Рекомендуемые действия

При обновлении BIOS сертификаты 2023 года сохраняются во встроенном ПО на постоянной основе. Это наиболее надежный способ, и мы рекомендуем использовать его, даже если сертификаты уже были установлены через Windows Update.

Внимание

Если установить сертификаты только через Windows Update, а затем выполнить сброс ключей функции «Безопасная загрузка» в BIOS к заводским настройкам, сертификаты будут утрачены, и устройство не сможет загрузиться при включенной функции «Безопасная загрузка». Перед сбросом ключей функции «Безопасная загрузка» обновите BIOS, чтобы сертификаты были сохранены в микропрограмме на постоянной основе.

Обновление сертификата через BIOS

Установите версию BIOS, указанную для вашей модели, или более позднюю версию. Эти версии можно загрузить со страницы продукта на Axis.com:

Модель	Минимальная версия BIOS
AXIS S2208	отмена
AXIS S2212	отмена
AXIS S2216	отмена
AXIS S2224	отмена
AXIS S2108	Z218-004
AXIS S2208 Mk II	Z670-005
AXIS S2212 Mk II	Z671-005
AXIS S2216 Mk II	Z672-005
AXIS S2224 Mk II	Z673-005

Обновление сертификата через Windows Update

Если обновление BIOS для вашей модели пока недоступно, сертификаты 2023 года можно получить через Windows Update.

Внимание

Сертификаты, установленные таким способом, сохраняются в текущей базе данных безопасной загрузки, а не во встроенном ПО. Если выполнить сброс ключей безопасной загрузки в BIOS к заводским настройкам, сертификаты будут удалены, и устройство может не загрузиться при включенной функции безопасной загрузки Secure Boot. Установите обновление BIOS сразу после того, как оно станет доступно для вашей модели, даже если вы уже воспользовались этим способом.

Чтобы использовать этот способ:

1. Убедитесь, что на устройстве установлена Windows 10 LTSC или Windows 11 LTSC.
2. Установите все обновления Windows, выпущенные 14 апреля 2026 года или позднее.
3. Перейдите в Windows Security (Безопасность Windows) > Device security (Безопасность устройства) > Secure Boot (Безопасная загрузка)

4. Если после установки последних обновлений сертификат не обновился, проверьте значение реестра **UEFICA2023Status**. Если устройство по-прежнему не соответствует требованиям для автоматического обновления, обновите BIOS или обратитесь в службу технической поддержки Axis.

Внимание

Не выполняйте ручную отзвук сертификата 2011 года, пока не убедитесь, что все носители восстановления, среды загрузки и драйверы в вашей среде подписаны сертификатом 2023 года. Преждевременный отзвук сертификата 2011 года приведет к тому, что устройство не сможет загрузиться при включенной функции безопасной загрузки.

Проверка текущей версии BIOS

Чтобы проверить текущую версию BIOS:

1. Включите устройство и быстро нажимайте клавишу **DEL**, пока не появится логотип Axis.
2. Номер версии отображается как первый элемент в разделе **Main (Главная)**.

Обновление BIOS

Следуйте инструкциям, приведенным в руководстве по обновлению BIOS, доступном на странице загрузки файла BIOS.

Обновление Windows®

Система Windows® периодически проверяет наличие обновлений. Когда доступно обновление, устройство автоматически загружает это обновление, но его необходимо установить вручную.

Примечание

Во время запланированного перезапуска системы видеозапись прерывается.

Чтобы проверить наличие обновлений вручную:

1. Откройте меню **Настройки > Обновление Windows**.
2. Нажмите **Check for updates (Проверить наличие обновлений)**.

Настройка параметров обновления Windows®

Можно изменить способ и время обновления Windows® в соответствии с вашими потребностями.

Примечание

Все выполняющиеся записи останавливаются во время выполнения запланированного в расписании перезапуска системы.

1. Откройте приложение **Run (Выполнить)**.
 - Перейдите в раздел **Windows System > Run (Система Windows > Выполнить)** или
2. Введите **gpedit.msc** и нажмите **OK**. Откроется редактор локальных групповых политик.
3. Перейдите в раздел **Computer Configuration > Administrative Templates > Windows Components > Windows Update (Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Центр обновления Windows)**.
4. Настройте необходимые параметры (см. пример).

Пример:

Чтобы обновления автоматически загружались и устанавливались без вмешательства пользователя, а также чтобы при необходимости устройство перезагружалось самостоятельно во вне рабочее время, используйте следующую конфигурацию:

1. Откройте параметр **Always automatically restart at the scheduled time (Всегда автоматически перезагружаться в запланированное время)** и выберите значение:
 - 1.1. Включено

- 1.2. The restart timer will give users this much time to save their work (minutes) (Таймер перезагрузки предоставит пользователям столько времени для сохранения работы (в минутах)): 15.
- 1.3. Нажмите кнопку OK.
2. Откройте параметр Configure Automatic Updates (Настройка автоматического обновления) и выберите значение:
 - 2.1. Включено
 - 2.2. Configure Automatic updates (Настройка автоматического обновления): Автоматическое скачивание и установка по расписанию
 - 2.3. Schedule Install day (День установки по расписанию): Каждое воскресенье
 - 2.4. Schedule Install time (Время установки по расписанию): 00:00
 - 2.5. Нажмите кнопку OK.
3. Откройте параметр Allow Automatic Updates immediate installation (Разрешить немедленную установку автоматических обновлений) и выберите значение:
 - 3.1. Включено
 - 3.2. Нажмите кнопку OK.

Добавление дополнительного накопителя

Потребность в хранении может отличаться. Необходимость установки дополнительных накопителей зависит от времени хранения данных или записей с высоким разрешением. В этом разделе описана процедура установки дополнительного жесткого диска на устройстве серии AXIS S22.

Примечание

Следуйте приведенным ниже инструкциям, чтобы добавить дополнительный накопитель в соответствующее устройство AXIS S22. Инструкции приводятся на условиях "как есть", и компания Axis Communications AB не несет ответственности за потерю данных и/или неправильную настройку при выполнении любого из этих действий. Прежде чем приступать к их выполнению, необходимо создать резервную копию всех критически важных для бизнеса данных, что является стандартной мерой предосторожности в таких случаях. Приводимый далее порядок увеличения емкости накопителей не будет поддерживаться службой технической поддержки Axis.

Примечание

Чтобы избежать электростатического разряда, при работе с внутренними компонентами системы рекомендуется использовать антистатический коврик и антистатическую ленту.

Гарантия

Подробную информацию о гарантии можно найти на веб-странице www.axis.com/support/warranty.



Для просмотра видео откройте веб-версию данного документа.

Удаление передней панели

1. Открутите два винта с барашком с каждой стороны рамки.
2. Удаление передней панели.

Установка жесткого диска

▲ ОСТОРОЖНО

- Используйте только жесткие диски, которые были протестированы и одобрены для использования с AXIS серии S22.
 - Устанавливая жесткий диск, убедитесь, что носитель жесткого диска вставлен до упора. Щелчок свидетельствует о фиксации носителя жесткого диска.
 - Отключите шнур питания перед установкой жесткого диска.
1. Выключите систему и убедитесь в том, что питание выключено.
 2. Отсоедините шнур питания.
 3. Нажмите кнопку разблокировки на лицевой панели носителя жесткого диска и откройте ручку носителя жесткого диска.
 4. Вытяните носитель жесткого диска за ручку.
 5. Вставьте жесткий диск в носитель для жесткого диска.
 6. Четырьмя винтами закрепите жесткий диск на носителе.
 7. Вставьте носитель жесткого диска в гнездо для жесткого диска и доведите его до положения, в котором он соединится с задней платой.
 8. Закройте ручку держателя жесткого диска, чтобы зафиксировать жесткий диск на месте.
 9. Снова установите переднюю рамку.
 10. Запустите систему.

Добавление нового ресурса хранения записей

1. Создайте и отформатируйте новый раздел жесткого диска в Windows:
 - 1.1. Щелкните правой кнопкой мыши меню **Start (Пуск)** и выберите **Disk Management (Управление дисками)**.
 - 1.2. Нажмите **ОК**, если откроется окно **Инициализировать диск**. В противном случае щелкните новый жесткий диск правой кнопкой мыши и выберите **Инициализировать диск**.
 - 1.3. Щелкните правой кнопкой мыши незанятую область на только что инициализированном жестком диске и выберите пункт **Новый простой том**.
 - 1.4. Следуя указаниям мастера, настройте размер тома, назначьте диску букву и отформатируйте раздел.
 - 1.5. Завершите работу мастера, чтобы создать новый простой том.
2. Добавьте новое хранилище в AXIS Camera Station Pro:
 - 2.1. Откройте приложение AXIS Camera Station Pro.
 - 2.2. Откройте меню **Storage (Хранилище) > Management (Управление)**.
 - 2.3. Нажмите **Добавить...**
 - 2.4. Выберите добавленный диск и нажмите **ОК**.
 - 2.5. Откройте меню **Storage (Хранилище) > Selection (Выбор)**.
 - 2.6. Выберите устройства, данные с которых нужно перенести на новый диск.
 - 2.7. В раскрывающемся списке **Store to (Сохранить на)** выберите новый диск и нажмите **Apply (Применить)**.

Подробнее об управлении накопителями см. в *Руководстве пользователя AXIS Camera Station Pro*.

Создание тома RAID

Инструкции по созданию тома RAID см. в онлайн-версии руководства пользователя.

Запуск тома RAID в Microsoft Windows®

Чтобы настроить новый том, выполните следующие действия:

1. Щелкните правой кнопкой мыши меню **Start (Пуск)** и выберите **Disk Management (Управление дисками)**.
2. Во всплывающем меню **"Initialize Disk (Инициализация диска)"** выберите **GPT** и нажмите **OK**.
3. Нажмите незанятый диск и выберите **New Simple Volume (Создать простой том)**.
 - Следуйте инструкциям помощника установки.
4. По окончании работы помощника установки в разделе **Disk Management (Управление дисками)** появится новый том. Закройте окно **Disk Management (Управление дисками)** для использования нового тома в системе.

Управление встроенным коммутатором

Сведения о встроенном коммутаторе

В состав AXIS Camera Station S22 Mk II Appliance входит встроенный коммутатор Power over Ethernet (PoE). Встроенный коммутатор можно настраивать и управлять им.

Коммутатор используется для разделения трафика в сети таким образом, чтобы камеры систем охранного видеонаблюдения и связанный с ними трафик, управляемый коммутатором (порты PoE и порты для связи с коммутатором), не попадали в другие сети.

Управлять питанием коммутатора необходимо согласно следующим правилам:

- Каждый порт может резервировать мощность в соответствии с классом PoE подключенного устройства. Можно вручную задать мощность порта.
- Если фактическое энергопотребление конкретного порта превышает зарезервированный объем для этого порта, то порт отключается.
- Порты отключаются, когда фактическое энергопотребление всех портов превышает общий объем мощности, который способен обеспечить блок питания. После этого порты отключаются в соответствии с приоритетом портов, где меньший номер порта означает более высокий приоритет.

Вход на страницу управления коммутатором

1. Откройте строку меню.
 - В веб-браузере введите IP-адрес коммутатора. По умолчанию: 192.168.10.1
 - В программе AXIS Recorder Toolbox перейдите в раздел **Switch > Open the switch configuration** (Коммутатор > Открыть конфигурацию коммутатора).
2. Войдите в систему, введя имя пользователя и пароль.
 - Ваше имя пользователя `admin`
 - Пароль указан на наклейке, которая находится на устройстве сверху или входит в комплект поставки (самоклеяющаяся наклейка).

Из строки меню выйдите со страницы управления коммутатором.

Выполняемая конфигурация

Выполняемая конфигурация — это набор настроек, которые в данный момент активированы и выполняются на сетевом устройстве. Она отражает текущее состояние устройства и его функционирование в режиме реального времени. Эти изменения не сохраняются в случае перезагрузки устройства.

Пусковая конфигурация, напротив, представляет собой набор настроек, которые записаны в постоянной памяти устройства. Конфигурация загружается и применяется при запуске или перезапуске устройства.

Когда вы вносите изменения через веб-интерфейс и нажимаете **Save (Сохранить)**, изменения применяются к выполняемой конфигурации.

Чтобы сохранить настройки в пусковой конфигурации, щелкните значок **Save (Сохранить)** в верхнем правом углу веб-интерфейса.

Если в выполняемой конфигурации есть несохраненные изменения, значок мигает желтым цветом.

Общее представление

В строке меню щелкните **Overview (Обзор)**.

Общие сведения

Категория	Наименование	Описание
Сводка по портам	Активные порты	Количество используемых портов.
	Порты, использующие PoE	Количество используемых портов, для которых включена функция PoE.
	Заблокированные порты	Количество заблокированных портов.
Энергопотребление	Текущее использование PoE	Мощность PoE в ваттах, потребляемая устройствами, а также процент потребленной мощности PoE от общей выделенной мощности PoE.
	Запрошенная мощность	общая мощность в ваттах и процент мощности, распределенной между устройствами.
Состояние порта	Активный	Порт используется.
	Неактивно	Порт готов к использованию.
	Заблокировано	Порт заблокирован.

Примечание

Щелкните порт, чтобы просмотреть подробные сведения о нем.

Управление питанием

В строке меню щелкните **Power management (Управление питанием)**.

Список портов

Наименование	Описание
Порт	Номер порта, к которому подключено устройство.
PoE	Состояние PoE. Щелкнув значок, можно включить или отключить PoE на порте.
Класс PoE	Класс PoE подсоединенного устройства.
Приоритет	Приоритет распределения мощности подсоединенного устройства. По умолчанию приоритет соответствует номеру порта.
Энергопотребление (Вт)	Мощность в ваттах, потребляемая устройством, подключенным к порту.
Запрошенная мощность (Вт)	Мощность в ваттах, запрошенная устройством, подключенным к порту.
Выделенная мощность (Вт)	Вручную отрегулируйте мощность, выделенную для порта. Доступно, только если в качестве способа распределения мощности выбран параметр Manual (Вручную) .

Выделить мощность

Мощность PoE можно распределять между подключенными устройствами следующими способами:

- **Класс PoE:** Коммутатор распределяет мощность PoE с учетом класса PoE подключенного устройства.
- **Manual (Вручную):** Можно вручную настроить мощность PoE, выделяемую подключенному устройству.
- **LLDP-MED:** коммутатор взаимодействует с подключенным устройством и по мере необходимости динамически распределяет мощность PoE.

Примечание

Метод распределения мощности LLDP-MED поддерживается только для камер с AXIS OS 9.20 или более поздней версии.

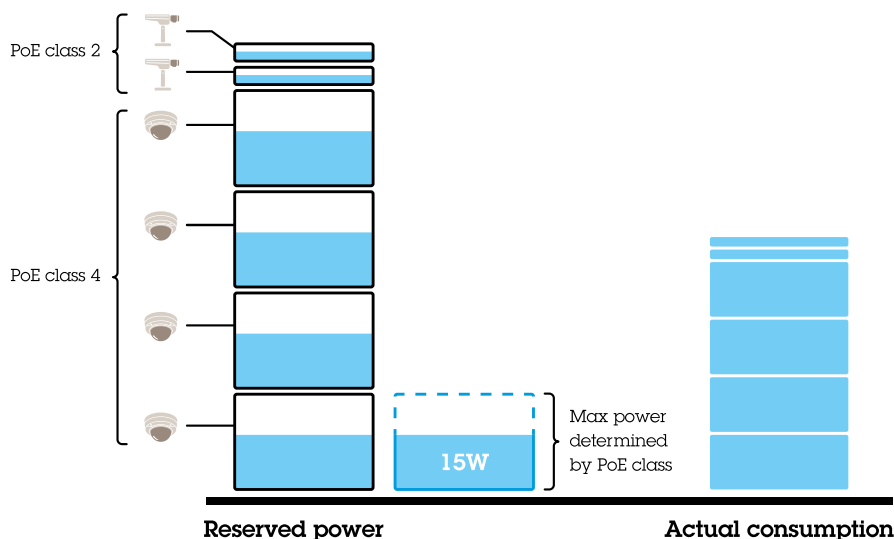
Чтобы изменить способ распределения питания, выполните следующие действия:

1. На странице управления питанием коммутатора перейдите в раздел **Power management (Управление питанием)**.
2. Выберите **PoE Class (Класс PoE)**, **Manual (Вручную)** или **LLDP-MED** в разделе **Allocate power (Выделение мощности)**.
3. Если выбрано значение **Manual (Вручную)**, вы можете изменить мощность для подключенного устройства в столбце **Power allocated (Выделенная мощность)**.
4. Если вы хотите изменить приоритет подключенного устройства, выберите приоритет для этого устройства. Приоритет других устройств изменится автоматически.

Пример:

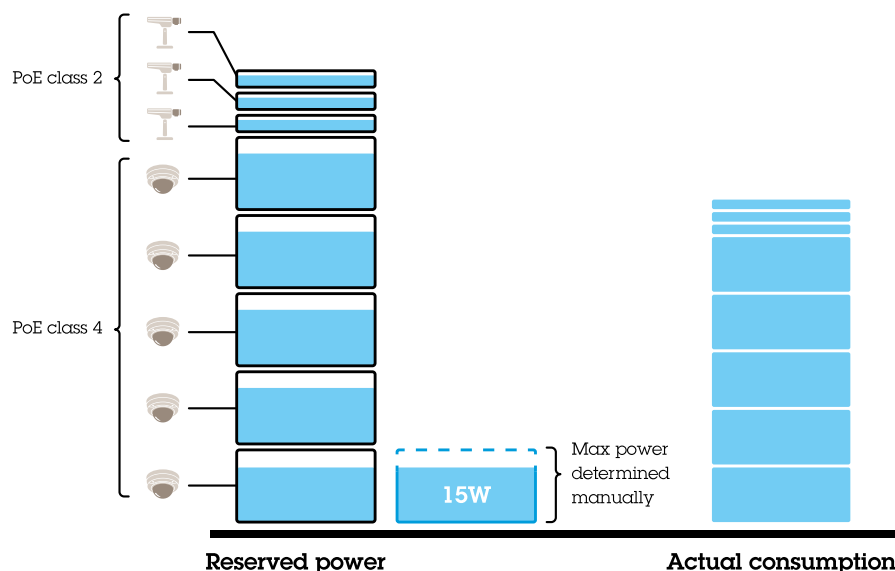
В этом примере общий бюджет мощности коммутатора составляет 135 Вт. Устройство PoE класса 4 запрашивает 30 Вт, но потребляет только 15 Вт. Устройство PoE класса 2 запрашивает 7 Вт, но потребляет только 5 Вт.

Выделение мощности по классу PoE



Мощность, запрошенная каждым устройством, определяется классом PoE. Коммутатор может подавать питание на четыре устройства PoE класса 4, а также на два устройства PoE класса 2. Общий объем запрашиваемой мощности составляет $(4 \times 30) + (2 \times 7) = 134$ Вт. Фактическая потребляемая мощность составляет $(4 \times 15) + (2 \times 5) = 70$ Вт. Таким образом, все подключенные устройства гарантированно получат необходимый объем мощности и в этом случае приоритет менее важен.

Распределение мощности вручную



Запрашиваемая мощность задается вручную и составляет 20 Вт для устройств PoE класса 4. Коммутатор может подавать питание на пять устройств PoE класса 4, а также на три устройства PoE класса 2. Общий объем запрашиваемой мощности составляет $(5 \times 20) + (3 \times 7) = 121$ Вт. Фактическая потребляемая мощность составляет $(5 \times 15) + (3 \times 5) = 90$ Вт. Таким образом, все подключенные устройства гарантированно получают необходимый объем мощности и в этом случае приоритет менее важен.

Включение и выключение PoE

Включение PoE на порте

1. В строке меню щелкните **Overview (Обзор)**.
2. В столбце PoE нажмите , чтобы включить PoE на определенном порте.

Выключение PoE на порте

1. В строке меню щелкните **Overview (Обзор)**.
2. В столбце PoE нажмите , чтобы выключить PoE на определенном порте.

Включение/выключение PoE для всех портов

1. В строке меню щелкните **Power management (Управление питанием)**.
2. Чтобы выключить PoE для всех портов, в раскрывающемся меню **PoE ports state (Состояние портов PoE)** выберите **Turn off all (Выключить все)**.
3. Чтобы включить PoE для всех портов, в раскрывающемся меню **PoE ports state (Состояние портов PoE)** выберите **Turn on all (Включить все)**.

Обзор сети

Обзор сети содержит подробную информацию о состоянии сетевого трафика для каждого порта.

Порты PoE

Наименование	Описание
Порт	Номер порта, к которому подключено устройство.
Устройство	Имя устройства, подключенного к порту.
IP-адрес	IP-адрес устройства, подключенного к порту.
MAC-адрес	MAC-адрес устройства, подключенного к порту.

Прием	Текущая скорость передачи (в мегабитах в секунду) для входящих данных на порте.
Отправка	Текущая скорость передачи (в мегабитах в секунду) для исходящих данных на порте.
Пакет отправлен	Количество пакетов данных, переданных коммутатором в сеть.
Пакет получен	Количество пакетов данных, полученных коммутатором из сети.
Пакет потерян	Количество и процент пакетов данных, которые не достигли пункта назначения из-за проблем в сети.
Блокировка	Показывает, заблокирован ли порт. Чтобы заблокировать или разблокировать порт, щелкните значок.

Блокировка и разблокировка портов

Можно заблокировать MAC-адрес для порта таким образом, чтобы проходил только трафик, поступающий с этого MAC-адреса. Это повышает безопасность и предотвращает несанкционированное подключение пользователями ноутбука или других устройств к сети охранного видеонаблюдения.

Привязка MAC-адреса к порту

1. В строке меню щелкните **Network overview (Обзор сети)**.
2. В столбце **Lock (Привязать)** щелкните , чтобы привязать определенный порт.

Отсоединение MAC-адреса от порта

1. В строке меню щелкните **Network overview (Обзор сети)**.
2. В столбце **Lock (Привязать)** щелкните , чтобы отсоединить определенный порт.

Привязка или отсоединение всех портов

1. В строке меню щелкните **Network overview (Обзор сети)**.
2. Чтобы привязать все порты, в раскрывающемся меню **Lock ports (Привязать порты)** выберите **Lock all (Привязать все)**.
3. Чтобы отсоединить все порты, в раскрывающемся меню **Lock ports (Привязать порты)** выберите **Unlock all (Отсоединить все)**.

Параметры

Настройка сетевых параметров

Можно изменить IP-адрес коммутатора. Однако для большинства камер рекомендуется использовать настройки по умолчанию. Причина заключается в том, что сеть охранного видеонаблюдения обычно изолируется от других сетей, например от корпоративной локальной сети. В этом случае сеть охранного видеонаблюдения используется только для управления устройствами видеонаблюдения и сбора данных с установленного на сервере ПО для управления видео.

1. В строке меню выберите **Settings (Настройки) > Network settings (Настройки сети)**.
2. Введите тип соединения, IP-адрес, маску подсети, шлюз, основной сервер DNS, вспомогательный сервер DNS и имя хоста.

Примечание

Настройки по умолчанию: статический IP-адрес 192.168.10.1 и маска подсети 255.255.255.0.

3. Нажмите **Сохранить**.

Настройка даты и времени

1. В строке меню выберите **Settings (Настройки) > Date and time (Дата и время)**.
2. Выберите страну и часовой пояс.
3. Чтобы задать время вручную, выберите **Manual (Вручную)** и настройте время вручную.
4. Чтобы настроить NTP-сервер, выберите **NTP server (NTP-сервер)** и введите адрес NTP-сервера.

Примечание

NTP-сервер работает только в том случае, если коммутатор подключен к сети и для него настроен доступ в Интернет.

5. Нажмите **Сохранить**.

Настройка сервера DHCP

Коммутатор можно настроить так, чтобы он использовал внутренний DHCP-сервер для назначения IP-адресов подключенным устройствам. Если канал связи с коммутатором используется, чтобы разрешить устройствам осуществлять доступ или принимать запросы от внешних приложений, необходимо задать шлюз и DNS-адреса.

1. В строке меню выберите **Settings (Настройки) > DHCP Server (сервер DHCP)**.
2. Выберите **Enable DHCP server (Включить DHCP-сервер)**.
3. Введите начальный IP-адрес, конечный IP-адрес, маску подсети, шлюз, основной сервер DNS, вспомогательный сервер DNS, продолжительность аренды и доменное имя.
4. Нажмите **Сохранить**.

Настройка SNMP

1. В строке меню выберите **Settings (Настройки) > SNMP**.
2. Укажите имя сервера, контактное лицо и место, используемое для SNMP-подключения.
3. Если вы хотите использовать SNMPV1 или SNMPV2c, выберите пункт **SNMPV1 / SNMPV2c** и укажите сообщество только для чтения.
4. Если вы хотите использовать SNMPV3, выберите **SNMPV3 (MD5)** и введите имя пользователя и пароль.

Примечание

В настоящее время поддерживается только проверка подлинности MD5, применяемая для SNMP.

5. Нажмите **Сохранить**.

Обслуживание

Обновить встроенное ПО

1. В строке меню выберите **Maintenance (Обслуживание) > Update firmware (Обновить встроенное ПО)**.
2. Перетащите файл встроенного ПО или нажмите кнопку **Browse (Обзор)** и перейдите к файлу встроенного ПО.
3. Нажмите **Upload (Загрузить)**.
4. После обновления встроенного ПО перезагрузите коммутатор.

Перезагрузка коммутатора

Внимание

Во время перезагрузки коммутатора все подключенные устройства временно теряют связь с коммутатором, включая PoE.

1. В строке меню выберите **Maintenance (Обслуживание) > Reboot switch (Перезагрузка коммутатора)**.
2. Нажмите **Reboot (Перезагрузить)** и выберите **Yes (Да)**.
3. Когда коммутатор перезагрузится через несколько минут, введите ваши имя пользователя и пароль для входа в систему.

Резервное копирование настроек коммутатора

Примечание

Имя пользователя и пароль добавляются в файл резервной копии.

1. В строке меню выберите **Maintenance (Обслуживание) > Backup and restore (Резервное копирование и восстановление)**.
2. Нажмите **Create a backup file (Создать файл резервной копии)**. Резервная копия будет создана в формате .bin и сохранена в папке **Downloads (Загрузки)**.

Восстановление настроек коммутатора

Примечание

Чтобы можно было восстановить настройки коммутатора необходимо предварительно создать файл с резервной копией настроек.

1. В строке меню выберите **Maintenance (Обслуживание) > Backup and restore (Резервное копирование и восстановление)**.
2. Перетащите файл резервной копии или нажмите кнопку **Browse (Обзор)** и перейдите к файлу резервной копии.
3. Нажмите **Upload (Загрузить)**.

Восстановление коммутатора из файла резервного копирования может занять несколько минут. После восстановления настроек будет выполнена автоматическая перезагрузка коммутатора и потребуются повторный вход в систему.

Управлять сертификатами

1. В строке меню выберите **Maintenance (Обслуживание) > Manage certificates (Управлять сертификатами)**.
2. Нажмите  и перейдите к файлу с закрытым ключом.
3. Нажмите  и перейдите к файлу с сертификатом.
4. Нажмите  и перейдите к файлу с пакетом ЦС.
5. Нажмите **Сохранить**.
6. Перезагрузите коммутатор.

Изменить пароль

Заданный по умолчанию пароль для коммутатора можно изменить на выбранный вам пароль.

Внимание

Выберите пароль, который вам будет легко запомнить. Если вы забыли пароль, см. *Сброс к заводским установкам, on page 34*, чтобы восстановить пароль по умолчанию.

1. В строке меню выберите **Maintenance (Обслуживание) > Change password (Изменить пароль)**.
2. Введите текущий пароль и новый пароль в соответствии с инструкциями.
3. Нажмите **Сохранить**.

Настройка параметров Интернета

1. В строке меню выберите **Maintenance (Обслуживание) > Web settings (Настройки Интернета)**.
2. Введите номер порта.

Примечание

- Если вы изменили номер порта, обязательно запишите новый номер. Если вы забыли новый номер порта, см. *Сброс к заводским установкам, on page 34*, чтобы восстановить номер порта по умолчанию.
- Мы рекомендуем включить протокол HTTPS.

Сброс к заводским установкам

Нажмите кнопку сброса и удерживайте ее пять секунд, чтобы восстановить для коммутатора заводские установки по умолчанию.

Также можно сбросить настройки коммутатора через веб-интерфейс:

1. В строке меню выберите **Maintenance (Обслуживание) > Reset to factory default settings (Восстановить заводские установки по умолчанию)**.
2. Нажмите **Reset (Сброс)** и выберите **Yes (Да)**.

После сброса коммутатор перезагрузится автоматически.

Журналы

В строке меню щелкните **Logs (Журналы)**, чтобы просмотреть список журналов. Щелкните заголовок столбца, чтобы отсортировать его в алфавитном порядке.

Наименование	Описание
Time (Время)	Дата и время, когда произошло событие журнала.
Уровень	Уровень серьезности, отображаемый в виде предупреждений (значки).
Пользователь	Пользователь, инициировавший событие журнала.
IP-адрес	IP-адрес пользователя, инициировавшего событие журнала.
Сервис	Служба, с которой связано событие журнала. Возможные значения: Desktop, Network, System, NTPD, Storage, DHCP и т. д.
Событие	Описание события в журнале.

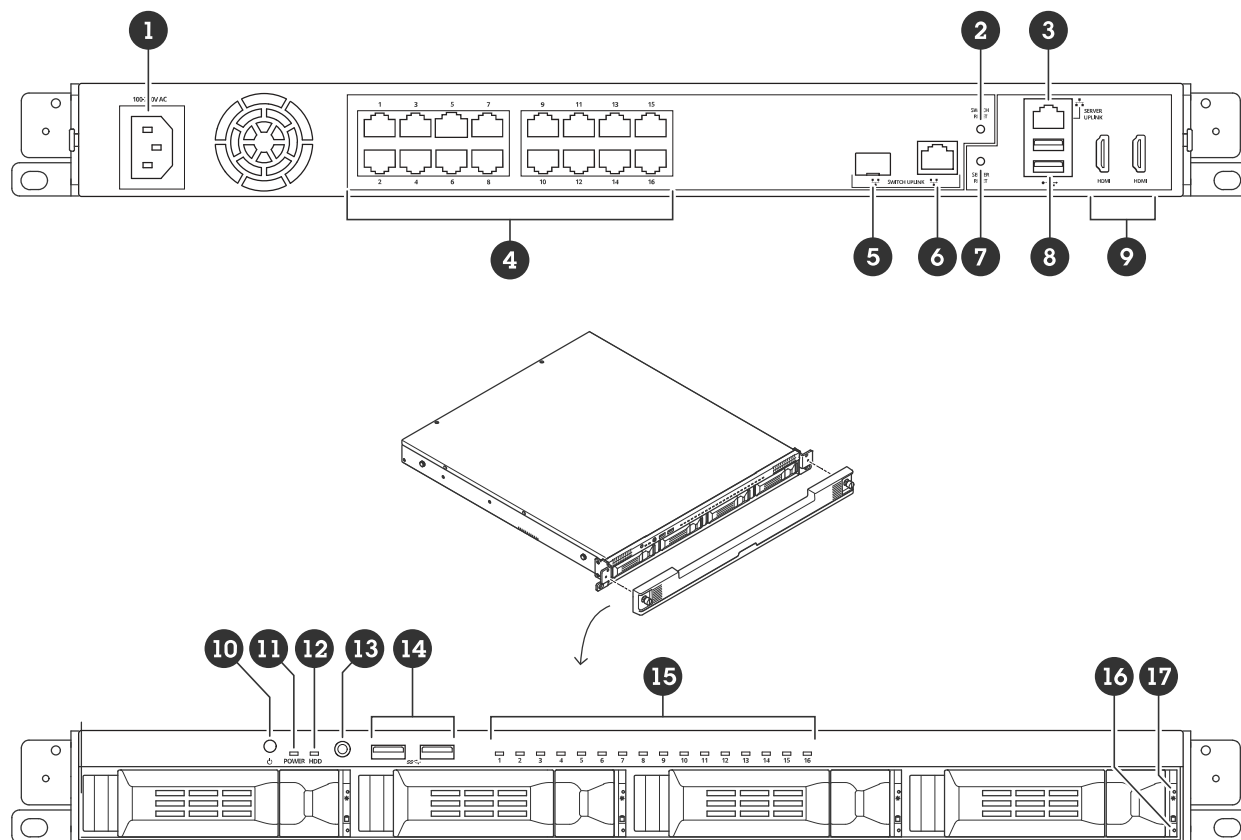
Создание отчетов коммутатора

На странице журнала щелкните **Export (Экспорт)**, чтобы создать текстовый файл с данными коммутатора, включая записи журнала.

Технические характеристики

Обзор продукции

Передняя и задняя



- 1 Разъем питания
- 2 Кнопка сброса коммутатора
- 3 1 порт GbE Ethernet – связь с сервером
- 4 1 порт GbE PoE Ethernet
- 5 1 порт GbE Ethernet – связь с коммутатором (SFP)
- 6 1 порт GbE Ethernet – связь с коммутатором (RJ45)
- 7 Кнопка сброса сервера
- 8 Порты USB 2.0
- 9 Порты HDMI
- 10 Кнопка питания
- 11 Светодиодный индикатор питания
- 12 Светодиодный индикатор работы жесткого диска
- 13 Универсальный аудиоразъем
- 14 Порты USB 3.2
- 15 Индикатор состояния портов PoE Ethernet
- 16 Светодиодный индикатор работы жесткого диска
- 17 Индикатор состояния жесткого диска

Светодиодные индикаторы

Передние СИД-индикаторы

Кнопка питания	Светодиодный индикатор питания	Индикация
Не нажата	Выкл.	Компьютер и коммутатор выключены
	Желтый	Компьютер включен, а коммутатор выключен
	Желтый (мигает)	Компьютер включен, а коммутатор загружается
	Зеленый	Компьютер включен, а коммутатор завершил загрузку
Нажата	0 с	Включается коммутатор и компьютер (если выключены)
	До оранжевого мигания (3 с)	Коммутатор инициирует корректное выключение
	До красного мигания (6 с)	Компьютер и коммутатор инициируют корректное выключение
	Пока не начнет постоянно светиться красным (9 с)	Компьютер инициирует некорректное выключение, коммутатор инициирует корректное выключение

Индикатор	Цвет	Индикация
Жесткий диск	Зеленый (мигает)	Работа жесткого диска
	Красный	Возможная неисправность жесткого диска
Состояние порта PoE Ethernet	Зеленый	Состояние связи
	Желтый	Запитываемое устройство, без состояния связи
	Красный	Превышение бюджета питания PoE
Состояние жесткого диска	Зеленый	Жесткий диск установлен
	Красный	Возможная неисправность жесткого диска

Задние индикаторы

Скорость и активность сети	Цвет	Индикация
Правый индикатор	Желтый	10/100 Мбит/с
	Зеленый	1000 Мбит/с
Левый индикатор	Зеленый	Подключение PoE в порядке
	Красный	Превышение бюджета питания PoE

Поиск и устранение неисправностей

Сброс параметров сервера

Для сброса параметров сервера можно использовать кнопку сброса сервера. Сброс параметров сервера займет более одного часа.

1. Выключите питание устройства.
2. Нажмите и удерживайте кнопку сброса сервера в течение 5 секунд. Будет запущена среда восстановления Windows® RE.
3. Выберите пункт Troubleshoot (Диагностика).
4. Выберите Reset your PC (Сброс параметров компьютера).
5. Выберите Keep my files (Сохранить мои файлы) или Remove everything (Удалить все). При выборе пункта Keep my files (Сохранить мои файлы) необходимо указать учетные данные администратора.
6. Следуйте инструкциям, отображаемым на экране.
7. Сервер перезагрузится и начнет процедуру восстановления заводских установок Windows®.



Сброс параметров сервера к заводским установкам по умолчанию

Выполнение восстановления системы

Если на устройстве произошел полный отказ системы, то для восстановления системы Windows® необходимо использовать образ для восстановления. Чтобы загрузить комплект AXIS Network Video Recorder Recovery Kit, обратитесь в службу технической поддержки Axis и сообщите серийный номер своего устройства.

Примечание

AXIS Network Video Recorder Recovery Kit доступен в двух вариантах:

- sb11 — для устройств, которые все еще используют сертификат 2011 года.
- sb23 — для устройств, перешедших на сертификат 2023 года.

Перед загрузкой Recovery Kit проверьте статус сертификата и выберите соответствующий вариант. При выборе неправильного варианта установка не позволит создать загрузочный носитель, и процедуру потребуется повторить с использованием правильного образа. Это не приведет к повреждению устройства.

Если на устройстве уже установлен сертификат 2023 года, вариант sb11 по-прежнему можно безопасно использовать, при условии что сертификат 2011 года не был отозван вручную. После его отзыва будет работать только вариант sb23.

Для восстановления системы:

1. Загрузите комплект AXIS Network Video Recorder Recovery Kit и инструмент AXIS Network Video Recorder Recovery: ISO to USB Tool.
2. Вставьте USB-накопитель в компьютер.
 - Используйте USB-накопители со свободным пространством от 16 ГБ.
 - USB-накопитель будет отформатирован, и все имеющиеся на нем данные будут удалены.

3. Запустите инструмент AXIS Network Video Recorder Recovery: ISO to USB Tool и следуйте инструкциям на экране.
Запись данных на USB-накопитель займет 10 до 15 минут. Не извлекайте USB-накопитель до завершения процесса.
4. После завершения работы инструмента AXIS Network Video Recorder Recovery: ISO to USB Tool вставьте USB-накопитель в устройство.
5. Запустите устройство.
6. При появлении экрана-заставки Axis нажмите клавишу F12.
7. Щелкните **UEFI: USB Drive (UEFI: USB-накопитель)**.
8. Перейдите к USB-накопителю и нажмите клавишу ВВОД. Система загружается в AXIS Network Video Recorder Recovery Kit.
9. Нажмите **Reinstall Operating System (Переустановить операционную систему)**.
Процесса восстановления займет от 10 до 15 минут. Подробные инструкции см. в скачанных файлах комплекта восстановления.

Устранение неполадок с AXIS Camera Station Pro

Инструкции по устранению неполадок в работе AXIS Camera Station Pro см. в *Руководстве пользователя AXIS Camera Station Pro*.

Нужна дополнительная помощь?

Полезные ссылки

- *Руководство пользователя ПО AXIS Camera Station Pro*
- *Войти в AXIS Secure Remote Access*
- *Вход в систему с помощью AXIS Secure Remote Access 2*
- *Что следует добавить в список разрешений антивирусной программы для AXIS Camera Station*

Связаться со службой поддержки

Если вам нужна дополнительная помощь, перейдите на страницу axis.com/support.

T10207038_ru

2026-07 (M5.2)

© 2024 – 2026 Axis Communications AB