

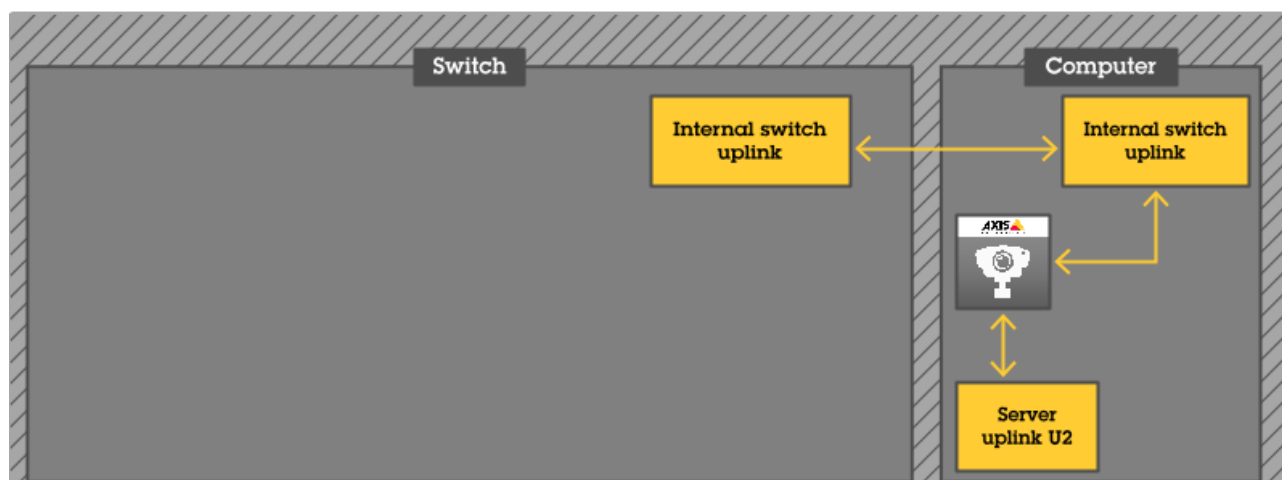
AXIS Camera Station S2108 Appliance

Сведения об устройстве

Видеосервер AXIS Camera Station S2108 Appliance — это надежное решение «все в одном» со встроенным управляемым коммутатором PoE для записи видео в системах видеонаблюдения с поддержкой разрешения до 4K. Видеорегистраторы предварительно настраиваются и поставляются с программным обеспечением для управления видеонаблюдением AXIS Camera Station, включая лицензии и все необходимое системное ПО. AXIS Camera Station имеет наглядный пользовательский интерфейс, который предоставляет доступ ко всем преимуществам линейки камер для видеонаблюдения и других IP-устройств Axis. Благодаря размещению операционной системы на твердотельном накопителе (SSD) и 5-летней гарантии на оборудование этот видеосервер представляет собой надежное решение для систем видеонаблюдения.

Видеосервер AXIS Camera Station S2108 Appliance состоит из двух компонентов:

- **Коммутатор:** Встроенный коммутатор Power over Ethernet (PoE).
- **Компьютер:** На компьютер предварительно загружено программное обеспечение, необходимое для создания решения для охранного видеонаблюдения, в том числе ПО для управления видео AXIS Camera Station.

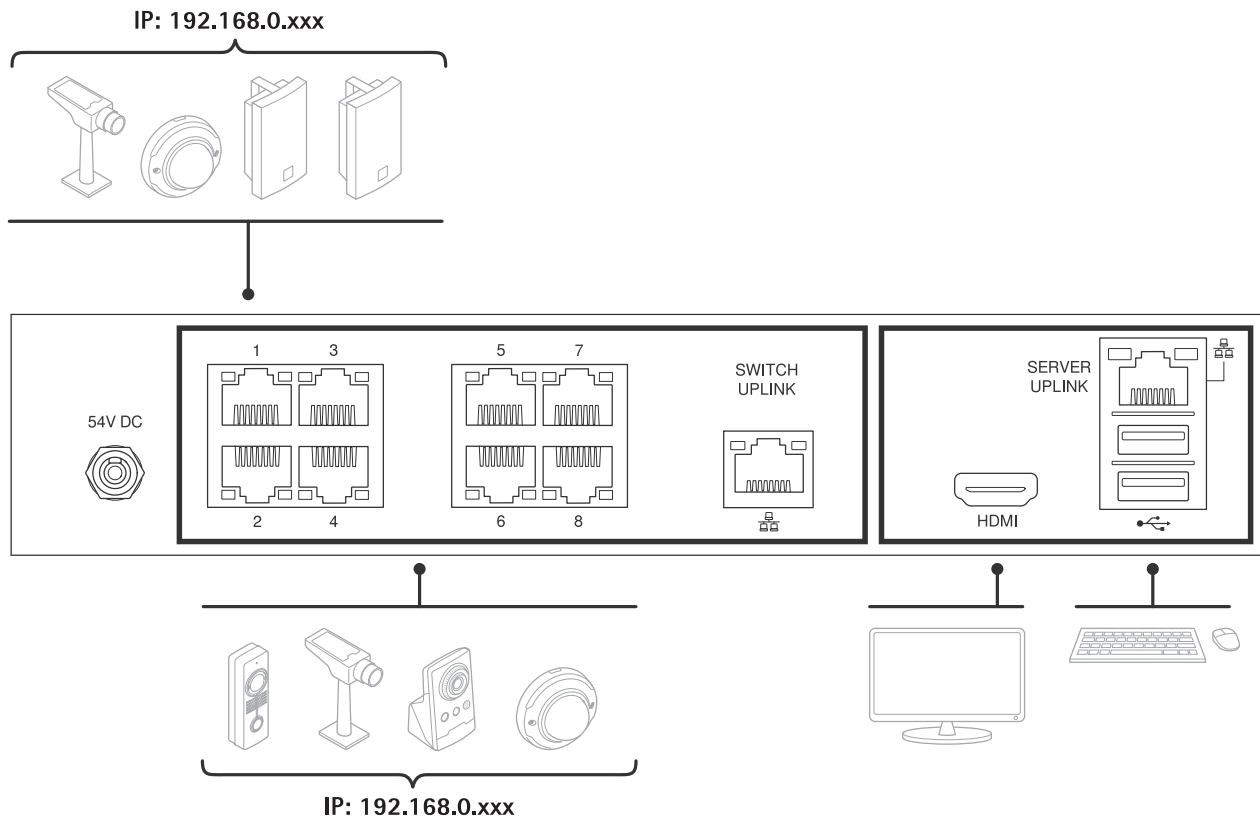


- Коммутатор и компьютер — это два разных компонента.
- Коммутатор и компьютер взаимодействуют через внутренние разъемы восходящей связи: один на плате питания коммутатора, а другой — на системной плате компьютера.
- Порт канала восходящей связи сервера — это внешний сетевой интерфейс, который может подключаться к действующей сети.
- Устройства, подключаемые к порту канала восходящей связи сервера, не могут обмениваться данными с устройствами, подключенными к коммутатору напрямую.
- Устройства, подключаемые к порту канала восходящей связи сервера, могут обмениваться данными с устройствами, подключенными к коммутатору с помощью ПО AXIS Camera Station.

Примеры настройки

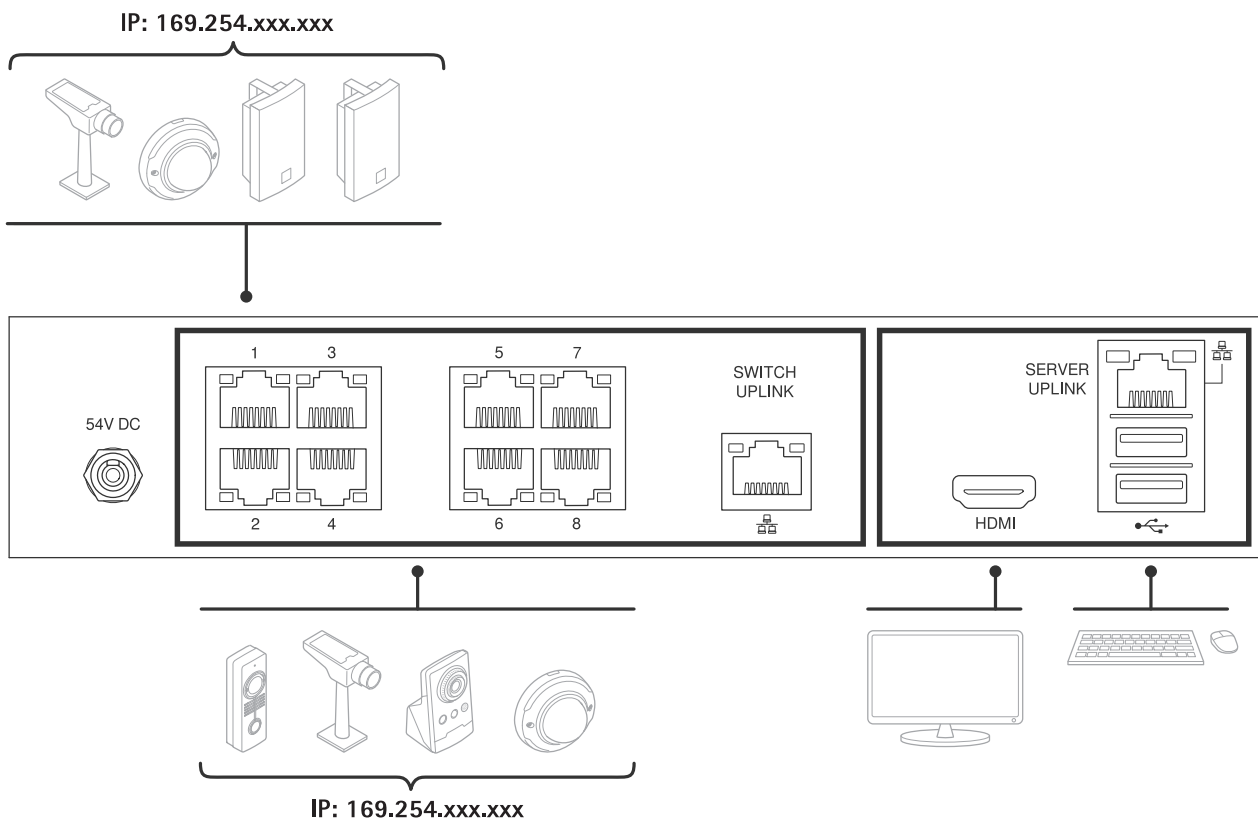
Назначение статических адресов каждому устройству

Можно создать независимую сеть, назначив статические IP-адреса каждому устройству и серверу AXIS S2108 Appliance. Эта сеть будет использовать подключения к другой внешней сети только в тех случаях, когда параметры сетей совпадают. Компьютер по-прежнему будет иметь доступ к сети Интернет через сервер исходящей связи. Сразу после подключения устройств к портам PoE, на которых присутствует питание, они принимают локальный адрес, и для них потребуется набор статических IP-адресов, соответствующий параметрам, заданным на сервере AXIS S2108 Appliance.



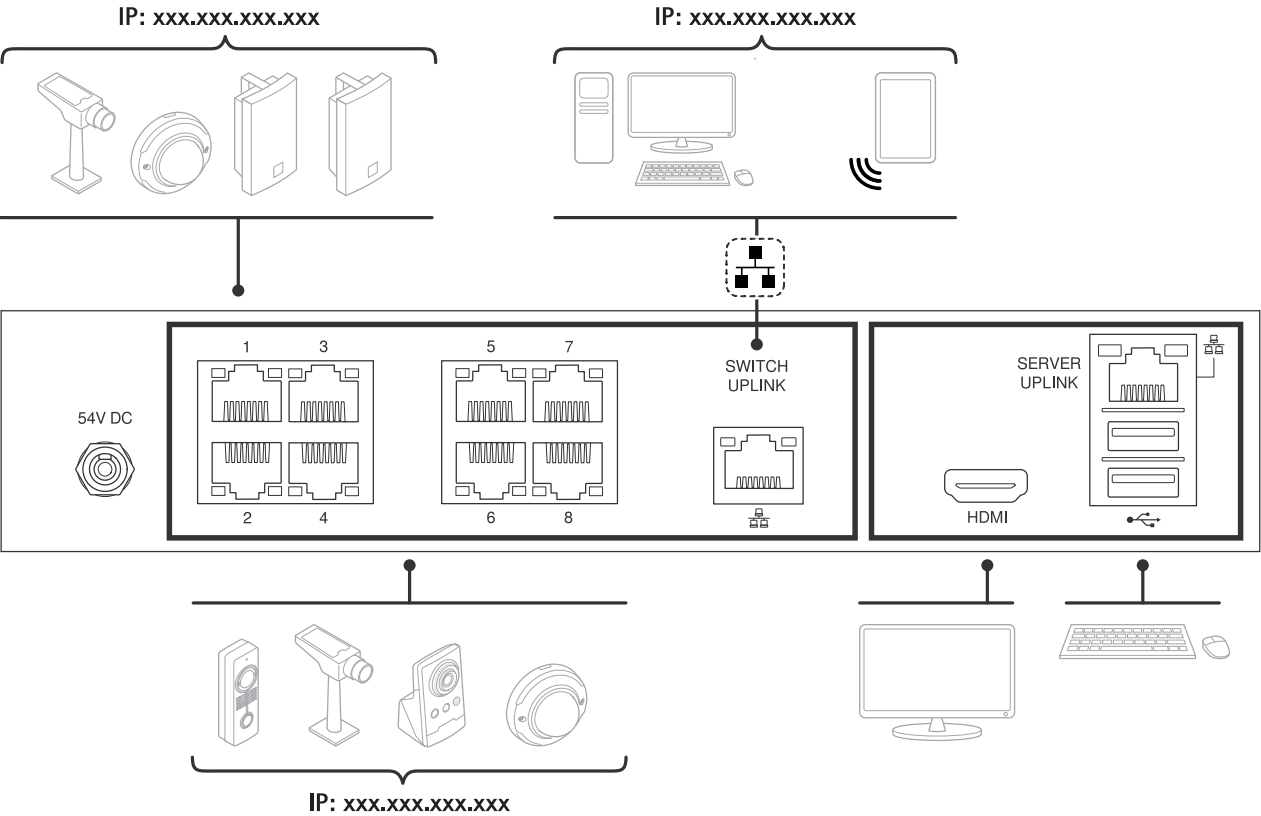
Использование локального адреса

Можно создать независимую сеть, используя локальный адрес для каждого устройства и сервера AXIS S2108 Appliance. Такая сеть не будет иметь возможности взаимодействия с другой внешней сетью. Компьютер по-прежнему будет иметь доступ к сети Интернет через сервер исходящей связи. После подсоединения устройств к активным портам PoE они получают локальный адрес и становятся видимыми для AXIS Camera Station на сервере AXIS S2108 Appliance.



Использование DHCP-сервера из другой сети

Чтобы подключиться к серверу AXIS S2108 Appliance, а также к присоединенным устройствам, необходимо подключить существующую сеть и DHCP-сервер к коммутатору каналов исходящей связи. В результате все подключенные устройства будут иметь IP-адреса, заданные в диапазоне адресов DHCP-сервера. Если данная сеть имеет доступ в Интернет, то он будет доступен и для сервера AXIS S2108 Appliance. В противном случае компьютер по-прежнему будет иметь независимый доступ к сети Интернет через сервер исходящей связи. После подсоединения устройств к активным портам PoE, они получают адрес DHCP, при условии, что DHCP-сервер активен.



Начало работы

Стандартная процедура настройки сервера видеозаписи AXIS Camera Station:

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 15*
4. Настройте ОС Windows®. Рекомендуемые действия:
 - Обновите Windows® до последней версии. См. .
 - Создайте стандартную учетную запись пользователя. См. *Создание учетной записи пользователя, on page 21*.
5. Обновите AXIS Camera Station до последней версии.
 - Если система подключена к сети, откройте приложение AXIS Recorder Toolbox и щелкните **Update AXIS Camera Station (Обновить AXIS Camera Station)**.
 - Если система работает в автономном режиме, перейдите на сайт *axis.com* и загрузите последнюю версию.
6. Запустите клиент AXIS Camera Station.
7. *Подключение к серверу AXIS Camera Station*
8. *Настройка ПО AXIS Camera Station, on page 17*

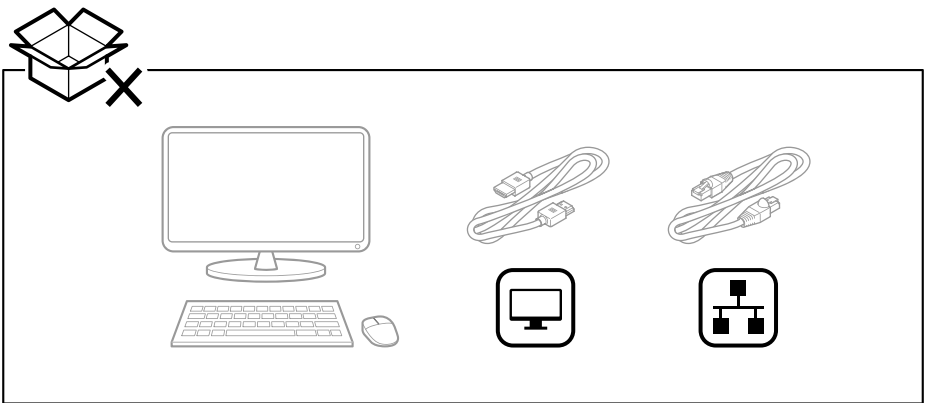
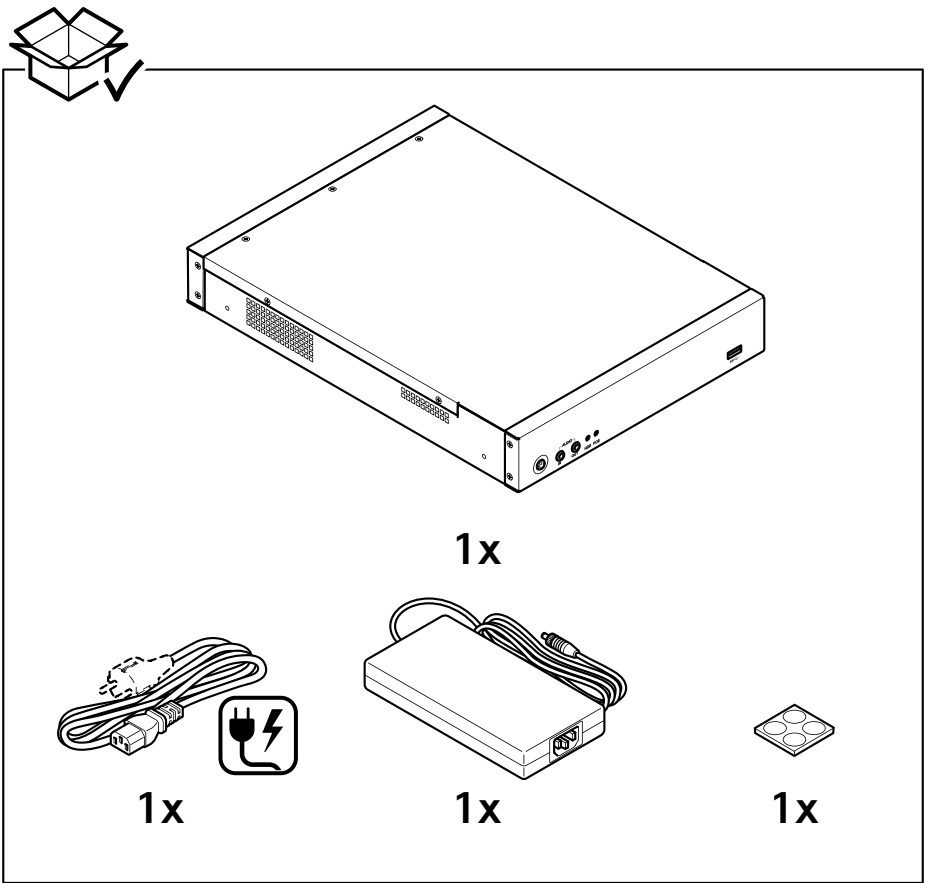
Установка устройства

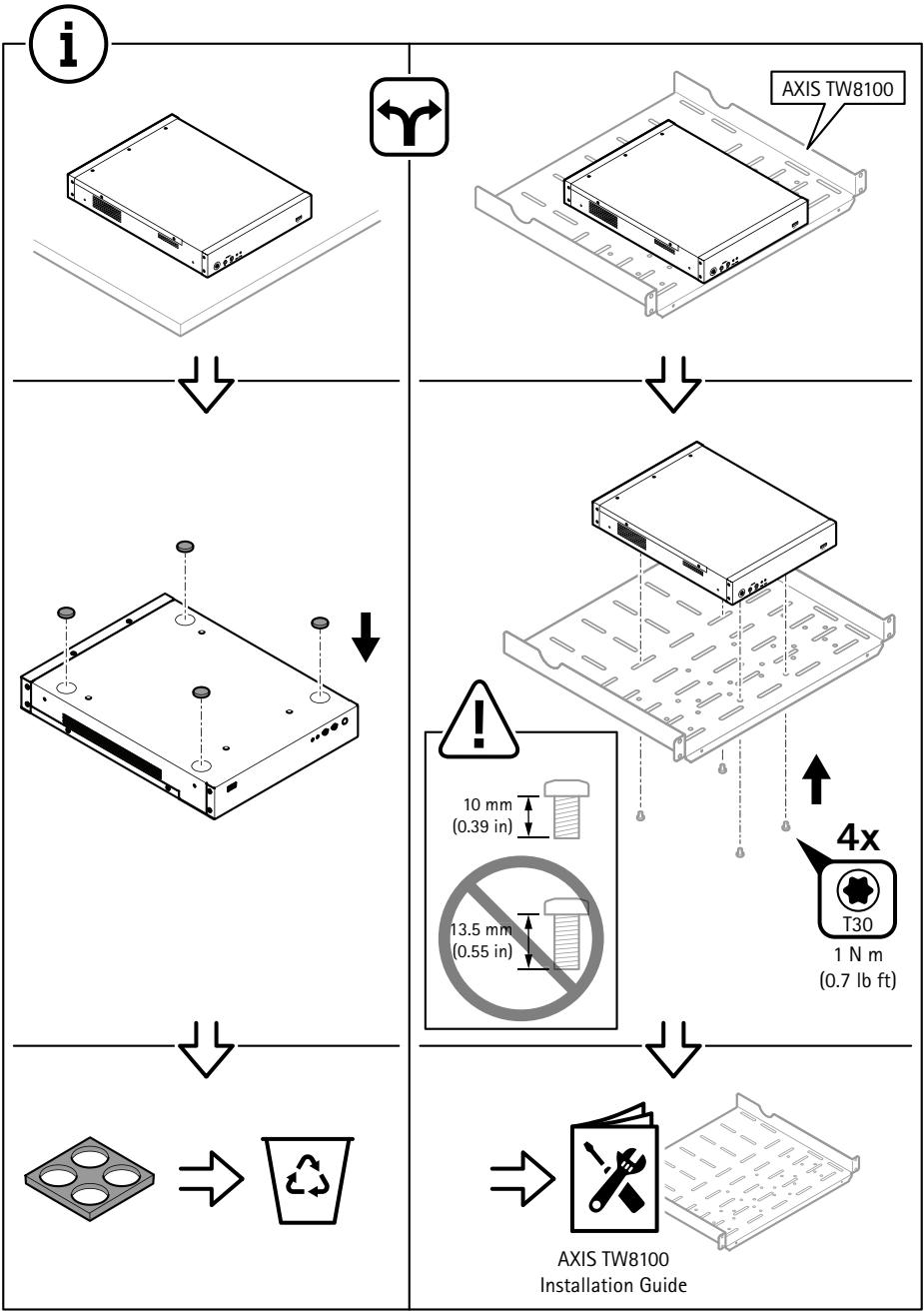
Перед установкой

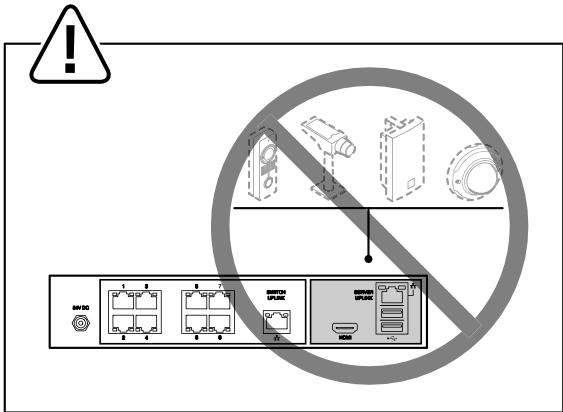
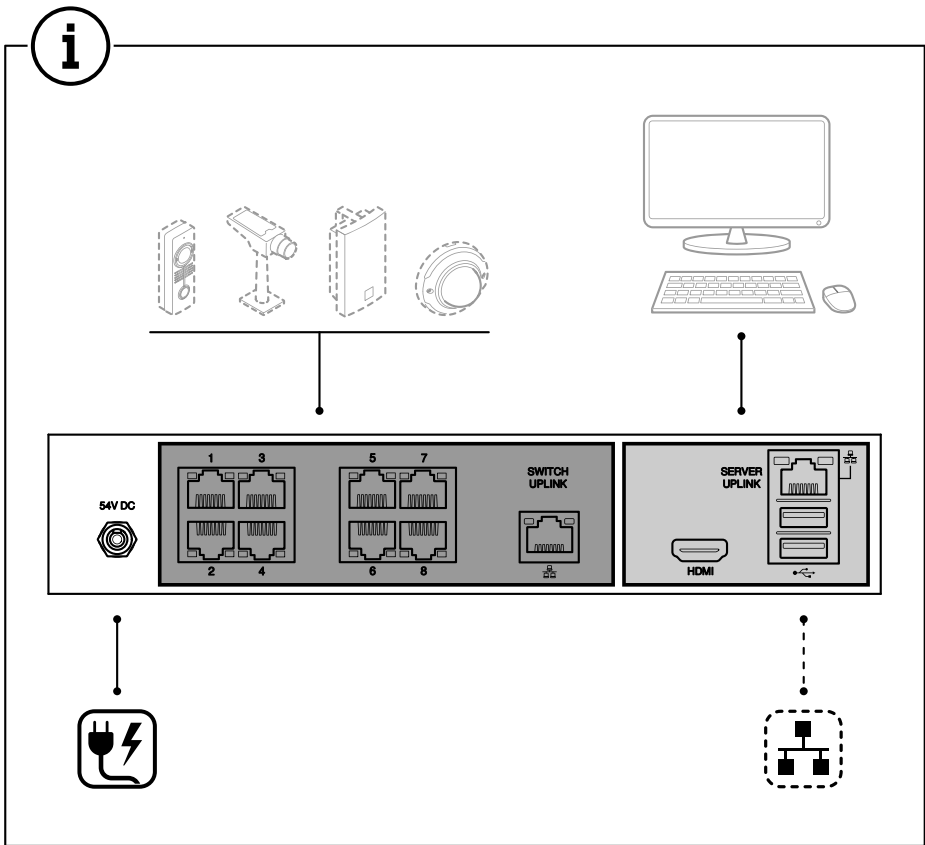
- Подготовьте дополнительные принадлежности, необходимые для установки: монитор, мышь, клавиатуру и сетевой кабель.
- Ознакомьтесь с информацией об использовании разных учетных записей пользователей.

В следующей таблице представлены учетные записи пользователей, которые можно использовать для установки, настройки и работы системы Axis.

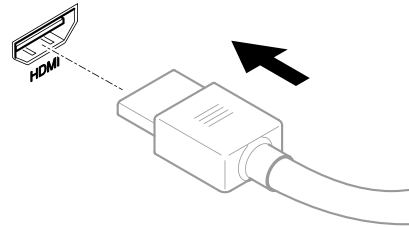
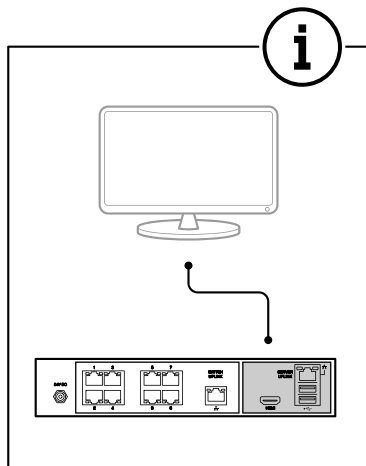
Учетная запись пользователя	Описание	Примечание
MyAxis	Используется для загрузки новейшего программного обеспечения, доступа к лицензионной системе, AXIS Secure Remote Access и System Health Monitoring.	Зарегистрировано с веб-сайта <i>my.axis.com</i> .
Windows®		
Администратор Windows®	Права администратора в Windows®. Мы не рекомендуем использовать эту учетную запись в качестве администратора AXIS Camera Station.	Создано во время первоначальной настройки Windows®.
Пользователь Windows® с правами администратора AXIS Camera Station	Пользователь Windows®, которому предоставлены права администратора в AXIS Camera Station, будет использоваться системным интегратором или системным администратором для настройки или устранения неисправностей.	Создано в настройках Windows®.
Пользователь Windows® с правами оператора или наблюдателя в AXIS Camera Station	Пользователь Windows®, которому предоставлены права оператора или наблюдателя в AXIS Camera Station.	Создано в настройках Windows®.
Устройство		
Администратор устройства	Используется администратором для доступа к камере из системы управления видео или с веб-страницы устройства.	Создано на веб-странице устройства или при добавлении устройства в AXIS Camera Station.



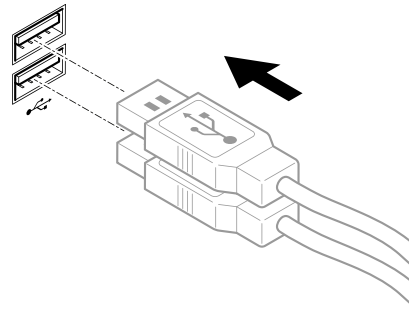
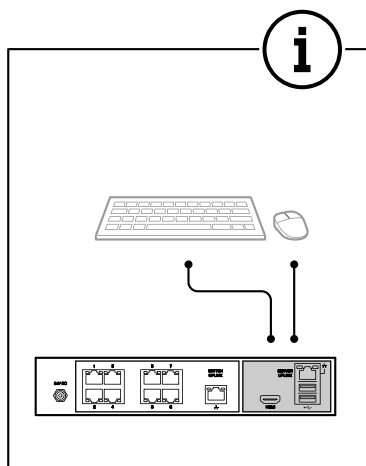




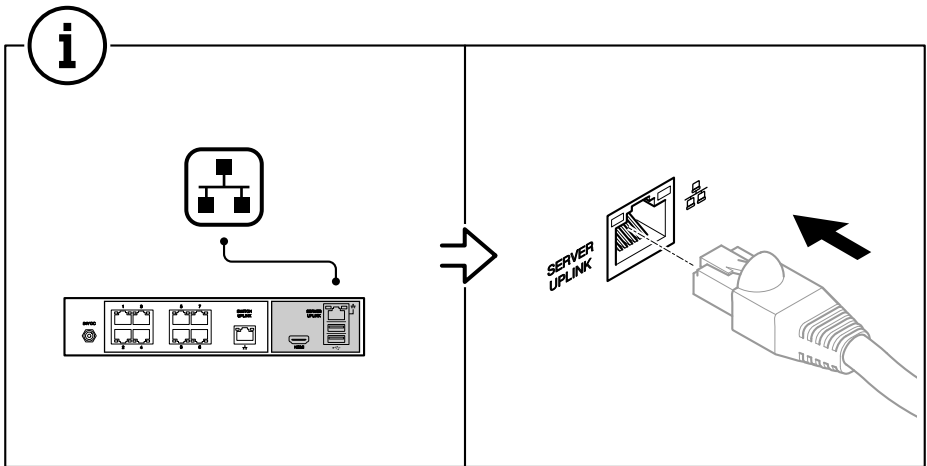
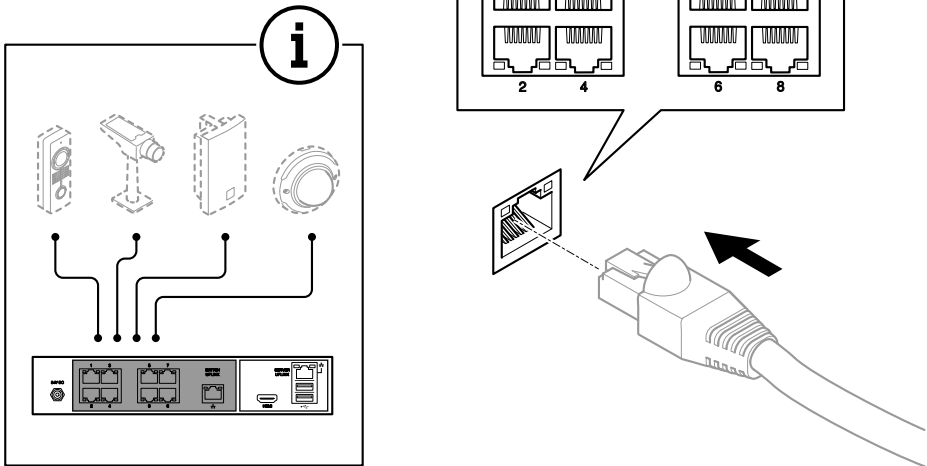
1.1



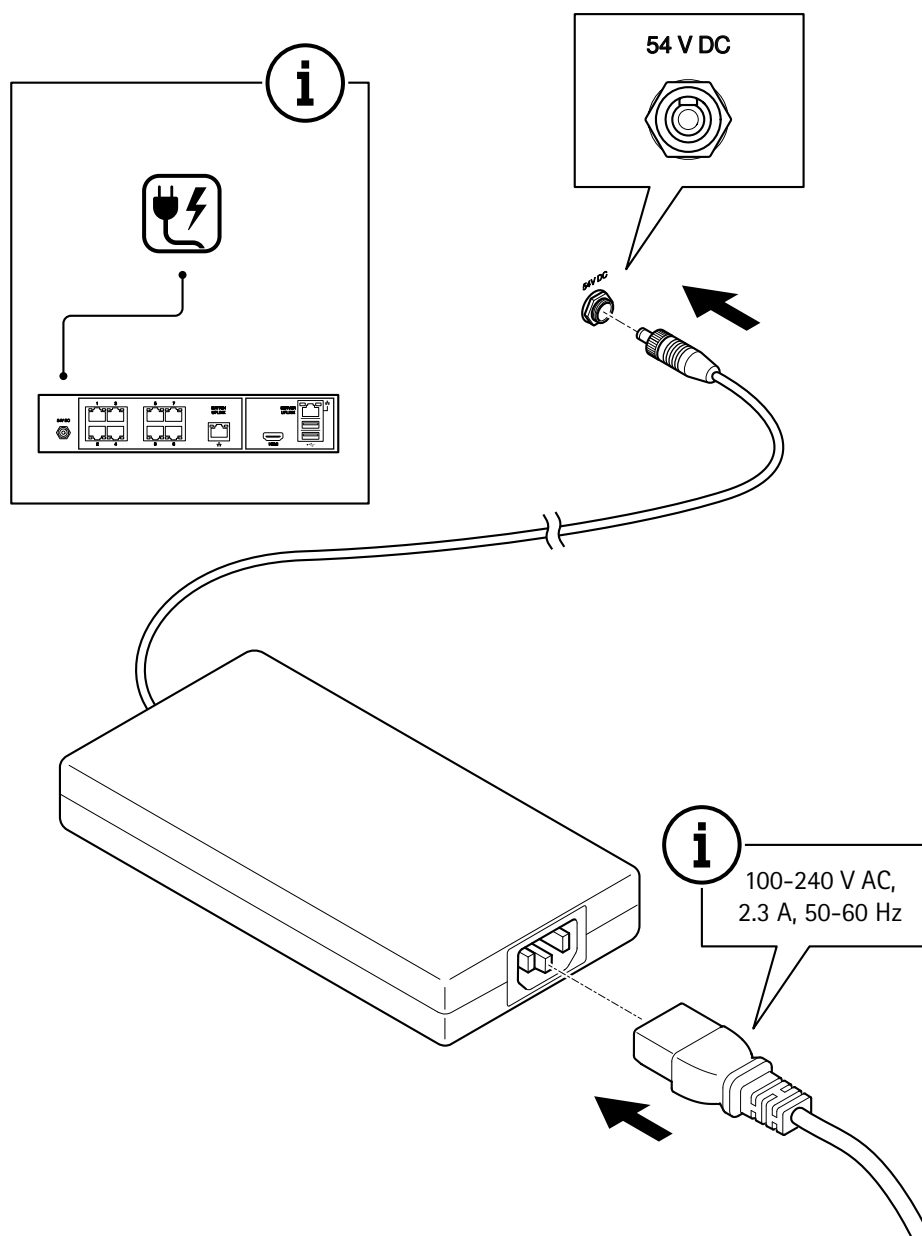
1.2



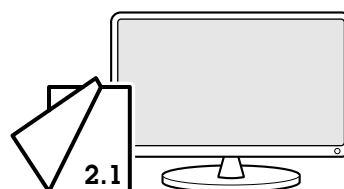
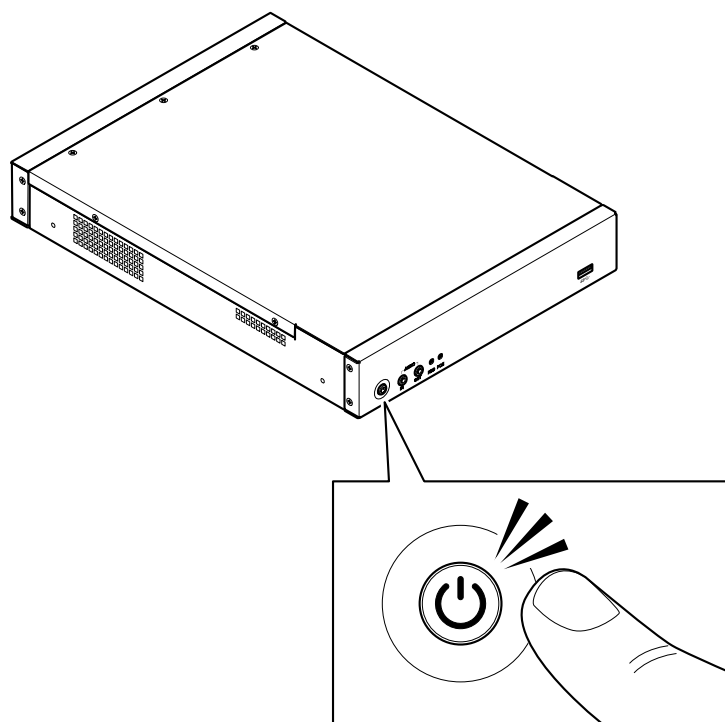
1.3



1.4



1.5



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 помощью этого мастера вы настроите несколько базовых параметров, необходимых для последующего управления устройством в AXIS Recorder Toolbox.

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 отображается 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.

Войдите на сервер

Используя клиент AXIS Camera Station, вы можете подключиться к нескольким серверам или к одному серверу, установленному на локальном компьютере или где-либо еще в сети. Можно подключаться к серверам AXIS Camera Station и использовать разные способы подключения:

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 16*.

AXIS Secure Remote Access – См. *Войти в AXIS Secure Remote Access, on page 16*.

Примечание

При первом подключении к серверу клиент проверяет идентификатор сертификата сервера. Чтобы убедиться, что вы подключаетесь к правильному серверу, вручную сверьте идентификатор сертификата с тем, который отображается в AXIS Camera Station Service Control.

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	Возможно, вам придется изменить настройки прокси-сервера клиента для подключения к серверу. 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 S2108 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 S2108 Appliance, необходимо настроить прокси-сервер в Windows на сервере AXIS Camera Station S2108 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 ПО AXIS Camera Station

В настоящем руководстве будут последовательно рассмотрены все основные действия, необходимые для запуска системы.

Прежде чем начать, убедитесь в следующем:

- Выполните настройку сети с учетом особенностей вашей системы. См. *Конфигурация сети, on page 19*.
- При необходимости настройте порты сервера. См. *Настройка порта сервера, on page 19*.
- Примите во внимание аспекты безопасности. См. *Рекомендации по обеспечению безопасности*.

Выполнив необходимую настройку, вы можете приступить к работе с Axis Camera Station:

1. *Запуск системы управления видео, on page 17*
2. *Добавить устройства, on page 17*
3. *Настройка способа записи, on page 17*
4. *Просмотреть живое видео, on page 18*
5. *Просмотр записей, on page 18*
6. *Добавление закладок, on page 18*
7. *Экспорт записей, on page 18*
8. *Воспроизведение и проверка записей в приложении AXIS File Player, on page 18*

Запуск системы управления видео

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

Можно подключаться к разным серверам AXIS Camera Station и использовать разные способы подключения.

Добавить устройства

При первом запуске AXIS Camera Station открывается страница Add devices (Добавить устройства). AXIS Camera Station выполняет поиск подключенных устройств в сети и выводит на экран список найденных устройств.

1. Выберите из списка камеры, которые нужно добавить. Если не удастся найти камеру, нажмите кнопку **Manual search** (Поиск вручную).
2. Нажмите **Добавить**.
3. Выберите один из двух вариантов: Быстрая настройка или Конфигурация AXIS Site Designer. Нажмите **Next** ("Далее").
4. Используйте параметры по умолчанию и убедитесь, что для метода записи задано значение **None** (Нет). Щелкните **Установить**.

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

Если клиент AXIS Camera Station Client, сервер AXIS Camera Station Server и подключенные сетевые устройства находятся в разных сетях, перед использованием AXIS Camera Station настройте параметры прокси-сервера или межсетевого экрана.

Настройки прокси клиента

Если между клиентом и сервером находится прокси-сервер, настройте параметры прокси-сервера на клиенте.

1. Откройте клиент AXIS Camera Station.
2. Нажмите **Change client proxy settings (Изменить параметры прокси-сервера для клиента)**.
3. Измените параметры прокси-сервера для клиента.
4. Нажмите кнопку **ОК**.

Параметры прокси-сервера на сервере

Если между сетевыми устройствами и сервером находится прокси-сервер, настройте параметры прокси-сервера на сервере.

1. Откройте приложение AXIS Camera Station Service Control.
2. Выберите **Modify settings (Изменить параметры)**.
3. В разделе Proxy settings (Параметры прокси) используйте значение по умолчанию **System account internet option (Свойства браузера системной учетной записи)** или выберите **Use manual proxy settings (Использовать параметры прокси, заданные вручную)**.
4. Нажмите **Сохранить**.

NAT и межсетевой экран

Если между клиентом и сервером находится NAT, межсетевой экран или аналогичные системы, настройте параметры NAT или межсетевого экрана так, чтобы порту HTTP, порту TCP и порту потоковой передачи, указанным в настройках AXIS Camera Station Service Control, было разрешено передавать данные через межсетевой экран или NAT. За инструкциями по настройке NAT или межсетевого экрана обратитесь к администратору сети.

Настройка порта сервера

Сервер AXIS Camera Station 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 S2108 Appliance, камеры, видеокодеры и дополнительные устройства в защищенной сети, отделенной от офисной сети. Вы можете установить клиент AXIS Camera Station S2108 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

И клиент, и сервер AXIS Camera Station должны быть подключены к Интернету.

1. Перейдите на вкладку **Конфигурация > Лицензии > Управление**.
2. Убедитесь в том, что параметр **Manage licenses online (Управлять лицензиями в режиме онлайн)** активирован.
3. Выполните вход, используя учетную запись **My Axis**.
4. Лицензионный ключ создается автоматически и отображается в разделе **License keys (Лицензионные ключи)**.
5. Если вы приобрели лицензионные ключи по отдельности, введите свой лицензионный ключ в разделе **Add license key (Добавить лицензионный ключ)**.
6. Нажмите **Добавить**.
7. На клиенте AXIS Camera Station убедитесь, что ваши лицензионные ключи отображаются в разделе **Configuration > Licenses > Keys (Конфигурация > Лицензии > Ключи)**.

Лицензирование системы в автономном режиме

1. Перейдите на вкладку **Конфигурация > Лицензии > Управление**.
2. Отключите функцию **Manage licenses online (Управлять лицензиями в режиме онлайн)**.
3. Нажмите **Экспортировать системный файл**.
4. Сохраните системный файл на USB-накопителе.
5. Выполните вход, используя учетную запись **My Axis**.
6. Нажмите **Upload system file (Загрузить системный файл)**, чтобы загрузить системный файл с USB-накопителя.
7. Лицензионный ключ создается автоматически и отображается в разделе **License keys (Лицензионные ключи)**.
8. Если вы приобрели лицензионные ключи по отдельности, введите свой лицензионный ключ в разделе **Add license key (Добавить лицензионный ключ)**.
9. Нажмите **Добавить**.
10. В разделе **License keys (Лицензионные ключи)** нажмите **Download license file (Скачать файл лицензии)** и сохраните этот файл на USB-накопителе.
11. В клиенте AXIS Camera Station перейдите в раздел **Configuration > Licenses > Management (Конфигурация > Лицензии > Управление)**.
12. Нажмите **Import license file (Импортировать файл лицензии)** и выберите файл лицензии на USB-накопителе.
13. Убедитесь, что ваши лицензионные ключи отображаются в разделе **Configuration > Licenses > Keys (Конфигурация > Лицензии > Ключи)**.

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. Перейдите в раздел **Settings > Accounts > Other people > Add someone else to this PC** (Параметры > Учетные записи > Другие пользователи > Добавить пользователя для этого компьютера).
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 **OK**.
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 **OK (OK)**.
 - 5.4. Нажмите кнопку **OK (OK)** 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

Права доступа пользователей

Перейдите в Configuration (Конфигурация) > Security (Безопасность) > User permissions (Разрешения пользователя), чтобы увидеть пользователей и группы в AXIS Camera Station S2108 Appliance.

Примечание

Администраторы компьютера, на котором работает сервер AXIS Camera Station S2108 Appliance, автоматически получают права администратора в AXIS Camera Station S2108 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 S2108 Appliance могут получать пользователи и группы Microsoft Windows® и Active Directory. Чтобы добавить пользователя в AXIS Camera Station S2108 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 S2108 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 S2108 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 S2108 Appliance.
Изменить	Разрешает редактирование видов в AXIS Camera Station S2108 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 отзыв 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 ОК.
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 ОК.
3. Откройте параметр Allow Automatic Updates immediate installation (Разрешить немедленную установку автоматических обновлений) и выберите значение:
 - 3.1. Включено
 - 3.2. Нажмите кнопку ОК.

Управление питанием

Общий бюджет мощности коммутатора составляет 105 Вт. Это максимальная мощность, которая может выдаваться на все подключенные устройства.

В большинстве случаев потребление подключенных устройств будет меньше запрашиваемого значения. Для оптимизации энергопотребления контроллер PoE позволяет подключенным устройствам запрашивать до 125 Вт мощности и одновременно с этим ограничивает реальное энергопотребление до 105 Вт.

Например, коммутатор может питать 8 устройств PoE, класса 3.

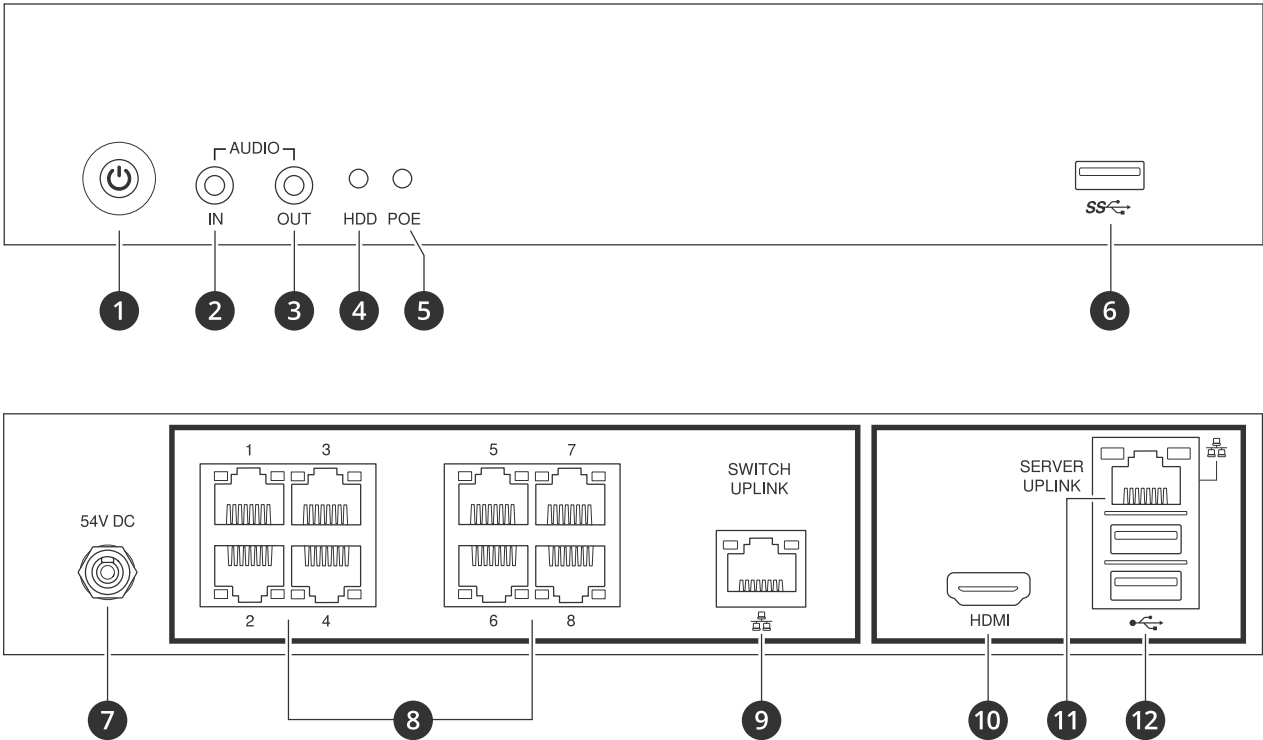
- 1 устройство PoE класса 3 запрашивает мощность 15,4 Вт.
- 8 устройств PoE класса 3 запрашивают мощность $(8 \times 15,4) = 123,2$ Вт. Это не превышает предельное значение 125 Вт, допускаемое контроллером PoE.
- 1 устройство PoE класса 3 обычно потребляет от 10 до 12 Вт.
- 8 устройств PoE класса 3 обычно потребляют от 80 до 96 Вт. Это не превышает общий бюджет мощности 105 Вт.

▲ ВНИМАНИЕ!

- Когда подключенные устройства требуют мощность, превышающую 125 Вт:
 - Последнее подсоединенное устройство не будет запущено.
 - Светодиодный индикатор перегрузки PoE будет непрерывно светиться красным до отключения последнего подсоединенного устройства или до высвобождения мощности PoE путем отсоединения других устройств.
- Когда фактическая мощность потребления подключенных устройств превышает 105 Вт:
 - Последнее подсоединенное устройство будет отключено, после чего будет предпринята попытка перезапуска.
 - Светодиодный индикатор перегрузки PoE светиться не будет.

Обзор продукции

Передняя и задняя стороны



- 1
 Кнопка / светодиодный индикатор питания
- 2
 Вход аудио
- 3
 Выход аудио
- 4
 Светодиодный индикатор работы жесткого диска
- 5
 Индикатор состояния портов PoE
- 6
 Порт USB 3.0
- 7
 Разъем питания
- 8
 Порты PoE
- 9
 Разъем RJ45 коммутатора каналов исходящей связи
- 10
 порт HDMI
- 11
 Разъем RJ45 сервера исходящей связи
- 12
 Порты USB 2.0

Технические характеристики

Передние СИД-индикаторы

Индикатор	Цвет	Индикация
Питание	Зеленый	Сервер ВКЛ.
Жесткий диск	Желтый (мигает)	Работа жесткого диска
	Красный (мигает)	Возможная неисправность жесткого диска
Перегрузка PoE	Красный	Превышение бюджета мощности PoE
	Выкл.	OK

Задние индикаторы

Скорость и активность сети	Цвет	Индикация
Правый индикатор	Желтый	10/100 Мбит/с
	Зеленый ¹	1000 Мбит/с
Левый индикатор	Зеленый (мигает)	Активность сети

1. Только для каналов исходящей связи коммутаторов и каналов восходящей связи серверов.

Поиск и устранение неисправностей

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 AXIS Camera Station

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

Нужна дополнительная помощь?

Полезные ссылки

- *Руководство пользователя AXIS Camera Station*
- *Войти в AXIS Secure Remote Access*
- *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.

T10181903_ru

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB