AXIS Camera Station Pro

Руководство пользователя

О программе

AXIS Camera Station Pro — решение для управления видео, предназначенное для мониторинга, записи и управления видеопотоками с сетевых камер Axis. Система поддерживает контроль доступа, управление несколькими охраняемыми объектами, интеграцию с AXIS Audio Manager, а также интеграцию с системами сторонних производителей.

Оно совместимо со всеми поддерживаемыми версиями AXIS OS в ветках Active, Long-Term Support (LTS) и Product Specific Support (PSS)*. Дополнительную информацию см. в примечаниях к выпуску AXIS Camera Station Pro или на *портале AXIS OS*. Чтобы проверить, какие продукты работают с AXIS Camera Station Pro, см. *Compatible products (Совместимые продукты)*.

*Поддержка совместимости с более ранними версиями AXIS OS осуществляется при наличии коммерческой целесообразности.

Параметры доступа

Сервер AXIS Camera Station Pro – управляет обменом данными между камерами, видеокодерами и дополнительными устройствами в системе. Сведения о системных требованиях и планировании емкости см. в *Аппаратные требования* в *AXIS Camera Station Pro – Руководство по установке и миграции*.

Клиент AXIS Camera Station Pro – обеспечивает доступ к записям, живому видео, журналам и настройкам. Его можно установить на любом компьютере, обеспечив тем самым удаленный просмотр и управление из любого места через Интернет или корпоративную сеть.

Веб-клиент для AXIS Camera Station – обеспечивает доступ к записям и живому видео AXIS Camera Station Pro в вашем веб-браузере. Подробную информацию см. в *Руководстве пользователя веб-клиента для AXIS Camera Station*.

Откройте мобильное приложение AXIS Camera Station Pro – обеспечивает доступ к записям и живому видео на нескольких системах. Приложение можно установить на устройствах с операционной системой Android и iOS, чтобы иметь возможность удаленного просмотра видео из разных местоположений.

Варианты загрузки

Перейдите на *страницу загрузки AXIS Camera Station Pro*, чтобы загрузить, обновить или бесплатно использовать его в течение 90 дней.

- **Бесплатная полнофункциональная 90-дневная пробная версия**: бесплатно используйте AXIS Camera Station Pro в течение 90 дней. Лицензия не требуется.
- **Обновление только клиента — автономный режим**: обновляет клиент — часть AXIS Camera Station Pro, с которой вы непосредственно взаимодействуете. Используйте этот вариант, если необходимо обновить только клиент, но не сервер.
- **Обновление клиента и сервера — автономный режим**: сжатый пакет обновления для клиента и сервера. После загрузки распакуйте ZIP-файл, чтобы получить доступ к файлам .msi и .cab, затем запустите файл .msi для начала обновления.
- **Обновление клиента и сервера — онлайн**: автоматически загружает, распаковывает и устанавливает обновление. Запустите файл .exe и следуйте инструкциям на экране. Во время установки компьютер должен оставаться подключенным к Интернету.
- **Мобильное приложение для iOS**: мобильное приложение AXIS Camera Station Pro для iPhone и iPad. Доступно в App Store.
- **Мобильное приложение для Android**: мобильное приложение AXIS Camera Station Pro для телефонов и планшетов Android. Доступно в Google Play.

Видеоруководства

Более подробные примеры использования системы см. в обучающих видеороликах по *AXIS Camera Station Pro*.

Функции системы

Более подробное описание возможностей системы см. в *Руководстве по функциям AXIS Camera Station Pro*.

Новые возможности?

Для доступа к новым функциям в каждом выпуске AXIS Camera Station Pro перейдите в раздел *Что нового в AXIS Camera Station Pro*.

Полезные ссылки для администратора

- *Подключить к серверу, on page 9*
- *Настроить устройства, on page 49*
- *Настройка хранилища, on page 80*
- *Настройка записи и событий, on page 86*
- *Настройка подключенных сервисов, on page 131*
- *Настройка сервера, on page 133*
- *Настройка безопасности, on page 144*

Дополнительные руководства

- *Веб-клиент для AXIS Camera Station*
- *Руководство интегратора AXIS Camera Station Pro*
- *Мобильное приложение AXIS Camera Station*
- *Учебные видеоруководства по AXIS Camera Station Pro*
- *Руководство по устранению неполадок AXIS Camera Station Pro*
- *Руководство по усилению безопасности системы AXIS Camera Station Pro*

Полезные ссылки для оператора

- *Подключить к серверу, on page 9*
- *Настройка клиентского ПО, on page 125*
- *Просмотр в реальном времени, on page 13*
- *Воспроизведение записей, on page 27*
- *Экспорт записей, on page 30*

Краткое руководство по началу работы

Воспользуйтесь этим руководством для настройки и запуска системы.

Прежде чем начать, убедитесь в следующем:

- Настройте сеть для установки. См. *Конфигурация сети*.
- При необходимости настройте порты сервера. См. *Настройка порта сервера*.
- Убедитесь, что система защищена. См. *Рекомендации по обеспечению безопасности*.

Для администраторов:

1. *Запуск системы управления видео*
2. *Добавить устройства*
3. *Настройка способа записи, on page 7*

Для операторов:

1. *Просмотреть живое видео, on page 7*
2. *Просмотр записей, on page 7*
3. *Экспорт записей, on page 7*
4. *Воспроизведение и проверка записей в приложении AXIS File Player, on page 7*

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.

После открытия клиента он попросит выполнить лицензирование вашей системы. Нажмите кнопку **License now (Получить лицензию сейчас)**, чтобы перейти на страницу **Manage licences (Управление лицензиями)**, где можно зарегистрировать сервер вместе с организацией. Дополнительные сведения см. в разделах *Управление подключенными сервисами, on page 131* и *Управление лицензиями, on page 142*.
Для получения доступа к подключенным службам, таким как веб-клиент VMS, службы контроля работоспособности системы и онлайн-лицензирования, необходимо зарегистрировать систему и подключить ее к организации.

Существуют разные способы подключения к нескольким серверам AXIS Camera Station Pro. См. *Подключить к серверу*.

Добавить устройства

При первом запуске AXIS Camera Station Pro открывается страница **Add devices (Добавить устройства)**, на которой выполняется поиск устройств в сети для их последующего добавления. См. *Добавить устройства*.

1. Выберите устройства, которые необходимо добавить, из списка. Если устройство не удается найти, нажмите **Manual search (Ручной поиск)** или используйте ввод для фильтрации.
2. Нажмите **Добавить**.
3. Нажмите **Close (Закрыть)**, 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. *Импорт проектов AXIS Site Designer, on page 53*.
   3.2. Установите флажок **Add image overlay for date, time, and text (Добавить наложение даты, времени и текста на изображение)**, чтобы добавить наложения на все 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 (Срок хранения)** и **Recording storage (Хранилище записей)**, затем нажмите **Finish (Готово)**, чтобы применить конфигурацию.

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.

Для получения дополнительных сведений см. *Просмотр в реальном времени, on page 13*.

Просмотр записей

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

Для получения дополнительных сведений см. *Записи, on page 27*.

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)**

Для получения дополнительных сведений см. *Экспорт записей, on page 30*.

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 подтвердить, что запись получена именно с той камеры, которая ее создала, и что она не была изменена. 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, сервер и подключенные сетевые устройства находятся в разных сетях, перед использованием AXIS Camera Station Pro настройте параметры прокси-сервера или брандмауэра.

Настройки прокси клиента

Если между клиентом и сервером находится прокси-сервер, настройте параметры прокси-сервера 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 клиент и сервер разделены NAT или брандмауэром, настройте их таким образом, чтобы обеспечить прохождение HTTP-порта, TCP-порта и порта потоковой передачи, указанных в AXIS Camera Station Pro Service Control. При необходимости обратитесь за помощью к администратору сети.

Для получения дополнительных сведений см. *Список портов для AXIS Camera Station Pro, on page 224*.

Настройка порта сервера

Сервер AXIS Camera Station Pro использует порты 29202 (TCP) и 29204 (HTTPS) для обмена данными между сервером и клиентом. При необходимости порты можно изменить в AXIS Camera Station Pro Service Control.

Примечание

Изменяйте порты только в том случае, если планируется использовать AXIS Camera Station Pro без Axis Secure Remote Access v2 или других облачных сервисов Axis.

Дополнительную информацию см. в *Общие настройки сервера* или разделе *FAQ (Часто задаваемые вопросы)*.

Рекомендации по обеспечению безопасности

Чтобы предотвратить несанкционированный доступ к камерам и записям:

- Используйте надежные пароли для всех сетевых устройств (камер, видеокодеров и дополнительных устройств).
- Установите сервер AXIS Camera Station Pro, камеры, видеокодеры и дополнительные устройства в защищенной сети, отделенной от офисной сети. Вы можете установить клиент AXIS Camera Station Pro на компьютере в другой сети, например в сети с доступом в Интернет.
- Убедитесь, что у всех пользователей надежные пароли.

Подключить к серверу

Клиент AXIS Camera Station Pro 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 9*.

Axis Secure Remote Access 2 – См. *Вход в систему с помощью AXIS Secure Remote Access 2, on page 10*.

Примечание

- При первом подключении к серверу клиент проверяет идентификатор сертификата сервера. Чтобы убедиться, что вы подключаетесь к нужному серверу, сравните идентификатор сертификата с идентификатором, отображаемым в Service Control AXIS Camera Station Pro. Для получения дополнительных сведений см. *Общие настройки сервера, on page 224*.
- Версии клиента и сервера должны совпадать. Если при подключении к локальной системе или системе с перенаправлением портов обнаружено несоответствие версий, клиент может загрузить нужную версию для соответствия версии сервера, а затем переключиться на нее.
- Для подключения клиента к нескольким серверам каждый сервер должен иметь ту же версию. По умолчанию ярлык клиента использует последнюю версию.

Список серверов	Чтобы подключиться к серверам из списка серверов, выберите сервер в раскрывающемся списке **Server list (Список серверов)**. Выберите для составления или изменения списков серверов. См. *Списки серверов*.
Импортировать список серверов	Чтобы импортировать список серверов, экспортированный из AXIS Camera Station Pro, нажмите **Import server list (Импортировать список серверов)** и найдите файл .msl. См. *Списки серверов*.
Удалить сохраненные пароли	Чтобы удалить сохраненные имена пользователей и пароли для всех подключенных серверов, нажмите **Delete saved passwords (Удалить сохраненные пароли)**.

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 29202, 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.

Вход в систему с помощью AXIS Secure Remote Access 2

1. Перейдите по ссылке **Вход в систему с помощью AXIS Secure Remote Access 2**.
2. Введите учетные данные My Axis.
3. Нажмите **Sign in (Войти)**.
4. Выберите организацию и щелкните **OK**.
5. Выберите нужный сервер для подключения.
6. Введите учетные данные вашего сервера для входа.

Примечание

Учетные данные сервера отличаются от данных учетной записи My Axis.

Строка состояния внизу клиента AXIS Camera Station Pro содержит сведения об использовании Axis Secure Remote Access 2. В разделе **Data used this month (Данные, использованные в этом месяце)** указан общий объем переданных данных, использованных организацией за месяц. Счетчик сбрасывается первого числа каждого месяца в полночь.

Включение Axis Secure Remote Access 2 на мобильных устройствах

Вход на сервер через Axis Secure Remote Access 2 с мобильного устройства (iOS и Android):

1. Перейдите на страницу *axis.com/products/axis-camera-station/overview* и загрузите приложение AXIS Camera Station Mobile.
2. Установите и запустите приложение.
3. Войдите в Axis Secure Remote Access 2 с помощью учетной записи My Axis.
4. Выберите нужный сервер для подключения.
5. Введите учетные данные вашего сервера для входа.

Примечание

- Учетные данные сервера отличаются от данных учетной записи My Axis.
- Прежде чем войти в систему с помощью учетной записи My Axis, необходимо получить приглашение присоединиться к организации в качестве пользователя.

В мобильном приложении отображается общий объем переданных данных, использованных организацией за месяц. Дополнительную информацию см. в руководстве пользователя приложения *AXIS Camera Station Mobile*.

Настройки прокси клиента

Если прокси-сервер находится между клиентом AXIS Camera Station Pro и сервером AXIS Camera Station Pro, необходимо настроить параметры прокси-сервера в Windows на клиентском компьютере. Обратитесь в службу поддержки Axis для получения дополнительной информации.

Клиент AXIS Camera Station Pro

Вкладки

Просмотр в реальном времени	Просмотр видео в режиме реального времени с подключенных камер. См. *Просмотр в реальном времени*.
Записи	Выполняйте поиск, воспроизводите и экспортируйте записи. См. *Записи*.
Умный поиск 1	Находите события в записях с помощью поиска движения. См. *Умный поиск 1*.
Поиск данных	Поиск данных из внешнего источника или системы и отслеживание того, что именно произошло во время каждого события. См. *Поиск данных, on page 46*.
Конфигурация	Управляйте подключенными устройствами и настраивайте параметры клиента и сервера. См. *Конфигурация*.
Горячие клавиши	Просматривайте и настраивайте сочетания клавиш. См. *Горячие клавиши*.
Журналы	журналы для регистрации сигналов тревоги, событий и аудита. См. *Журналы*.
Контроль доступа	Настраивайте и управляйте держателями карт, группами, дверями, зонами и правилами доступа в системе. См. *Контроль доступа, on page 193*.
Интеллектуальный поиск 2	Использование расширенных фильтров для поиска транспортных средств и людей на основе их характеристик. См. *Интеллектуальный поиск 2, on page 39*.
Контроль работоспособности системы	Отслеживание данных о работоспособности из одной или из нескольких систем AXIS Camera Station Pro. См. *System Health Monitoring БЕТА, on page 205*.
Оповещения живого просмотра	при запуске действия «Живой просмотр» камера или вид автоматически переходит на вкладку «Оповещения при живом просмотре». См. *Создание действий живого просмотра*.
Оповещения записи	Чтобы открыть вкладку «Оповещения при записи», выберите на вкладке «Тревоги» или «Журналы» один сигнал тревоги и нажмите **Перейти к записям**. См. *Тревоги* и *Журналы*.

Главное меню

	Открытие главного меню.
Серверы	Подключение к новому серверу AXIS Camera Station Pro и просмотр списков серверов и

	состояния подключений для всех серверов. См. *Настройка сервера*.
Действия	Включение или остановка вручную записи и изменение состояния портов ввода-вывода. См. *Запись в ручном режиме* и *Мониторинг портов ввода-вывода*.
Помощь	Получайте доступ к справке и вариантам поддержки. Чтобы узнать, какая версия клиента **используется, выберите** Справка > О программе AXIS Camera Station Pro.
Выйти из системы	Выполняйте выход из системы и отключение от сервера.
Закрыть	Выход из клиентской программы AXIS Camera Station Pro с ее закрытием.

Строка заголовка

? или F1	Открыть справку.
	Перейти в полноэкранный режим.
или ESC	Выйти из полноэкранного режима.

Строка состояния

- Значок предупреждения указывает на несоответствие времени на клиенте и сервере. Убедитесь, что время на них синхронизировано, чтобы избежать проблем с временной шкалой.
- Состояние подключения серверов — это количество подключенных серверов. См. *Состояние соединения*.
- Статус лицензии показывает количество нелицензированных устройств. См. *Управление лицензиями*.
- Использование Secure Remote Access вер.2 показывает объем данных, использованных за текущий месяц.
- **AXIS Camera Station Pro доступно обновление** уведомляет о наличии обновления, то есть новой доступной версии. Отображается только при входе в систему с правами администратора. См. *Обновить AXIS Camera Station Pro, on page 137*.

Тревоги и Задачи

- На вкладках «Тревоги» и «Задачи» отображаются сработавшие события и системные тревоги. См. *Тревоги* и *Задачи*.

Просмотр в реальном времени

В режиме живого просмотра отображается видео с подключенных камер в реальном времени. При подключении к нескольким серверам AXIS Camera Station Pro отображаются все представления и камеры, сгруппированные по имени сервера.

Виды обеспечивают доступ ко всем камерам и прочим устройствам, добавленным в AXIS Camera Station Pro. Представление может состоять из одной или нескольких камер, последовательности элементов, карты или веб-страницы. При живом просмотре виды обновляются автоматически при добавлении или удалении устройств из системы.

С интеграцией AXIS Audio Manager Pro вы также можете настраивать и добавлять аудиозоны с интерфейсами оповещения в режиме живого просмотра. Для получения дополнительной информации см. раздел *Использование интерфейсов оповещения в мультиэкранном режиме, on page 22*

Доступ к видам имеют все пользователи. Сведения о правах доступа пользователей см. в разделе *Права доступа пользователей, on page 144*.

Для настройки режима живого просмотра см. *Настройки клиента*.

Несколько мониторов

Чтобы открыть вид на другом экране, выполните следующие действия:

1. Откройте вкладку **Live view (Живой просмотр)**.
2. Выберите из списка одну или несколько камер, видов или последовательностей.
3. Перетащите их на другой экран.

Чтобы открыть вид на мониторе, подключенном к видеодекодеру Axis:

1. Откройте вкладку **Live view (Живой просмотр)**.
2. Выберите из списка одну или несколько камер, видов или последовательностей.
3. Щелкните выбранный элемент правой кнопкой мыши и выберите **Show on AXIS T8705 (Показать на AXIS T8705)** или **Show on AXIS D1110 (Показать на AXIS D1110)** в зависимости от используемого видеодекодера.

Примечание

- AXIS T8705 поддерживает только камеры Axis.
- AXIS D1110 поддерживает до 9 потоков на одном мультиэкране.

Управление видами в режиме живого просмотра

+	Добавьте новое представление с разделением экрана, последовательность, представление с камеры, карту, веб-страницу или папку.
✎	Редактирование вида или имени камеры. Для редактирования настроек камеры см. *Изменение настроек камеры*.
🗑	Удалите вид. Для удаления вида потребуются разрешения на изменение вида и всех дополнительных видов. Для удаления камер из AXIS Camera Station Pro см. *Камеры, on page 56*.
🔒	Администратор может заблокировать представление, чтобы запретить операторам перемещать его или изменять его.

Управление изображением в режиме живого просмотра

Перейти	Чтобы перейти к виду с камеры, щелкните правой кнопкой мыши одно из изображений мультиэкранного вида и выберите **Navigate (Перейти)**.
Сделать стоп-кадр	Чтобы получить стоп-кадр, щелкните изображение правой кнопкой мыши и выберите **Сделать стоп-кадр**. Система сохраняет стоп-кадр в папке, указанной в **Configuration (Конфигурация) > Client (Клиент) > Settings (Настройки)**. Примечание AXIS Camera Station Pro обычно использует видеопоток при создании стоп-кадров, поэтому разрешение стоп-кадра совпадает с разрешением видеопотока. Однако для поворотных камер и камер с объективом типа «рыбий глаз», для которых требуется сшивка или компенсация оптических искажений, стоп-кадр создается на стороне клиента непосредственно из изображения на экране. Это может привести к снижению разрешения изображений, особенно в представлениях с несколькими камерами, где изображение с каждой камеры занимает меньшую часть экрана.
Добавить стоп-кадр в экспорт	Чтобы добавить стоп-кадр в список экспорта, щелкните изображение правой кнопкой мыши и выберите **Add snapshot to Export (Добавить стоп-кадр в экспорт)**.
Показать на	Чтобы открыть вид на другом экране, щелкните правой кнопкой мыши изображение и выберите **Показать на**.
Использовать механическое управление позиционером (PTZ)	Доступно для камер PTZ и камер с настроенной цифровой функцией PTZ в веб-интерфейсе камеры. Чтобы воспользоваться функцией механического PTZ-управления, нажмите правой кнопкой мыши на изображение и выберите **Использовать механическое PTZ-управление**. С помощью мыши можно осуществлять масштабирование, панорамирование и наклон.
Зум	увеличение и уменьшение изображения с помощью колесика мыши. Или нажмите Ctrl + [+], чтобы увеличить масштаб, и Ctrl + [-], чтобы уменьшить масштаб.
Изменение размера области наблюдения	Чтобы увеличить определенную область, выделите ее прямоугольной областью. Чтобы уменьшить участок, воспользуйтесь колесиком мыши. Чтобы увеличить участок вблизи центра изображения, начертите прямоугольник правой кнопкой мыши.
Панорамирование и наклон	Щелкните изображение в точке, куда необходимо направить камеру. Для непрерывного поворота и наклона переместите курсор в центр изображения, чтобы отобразить стрелку навигации. Нажмите и

	удерживайте кнопку мыши, чтобы выполнять панорамирование в направлении стрелки. Для ускорения панорамирования и наклона нажмите и удерживайте кнопку мыши, чтобы увеличить длину стрелки навигации.
Настройка фокуса	Чтобы настроить фокус для устройства AXIS, щелкните правой кнопкой мыши по изображению и выберите **Set focus (Установить фокус)**. Используйте шкалы **Near** и **Far** для ручной настройки фокуса либо нажмите **AF** для автоматической фокусировки. Чтобы настроить фокус для устройства ONVIF, щелкните правой кнопкой мыши по изображению и выберите **Set focus (Установить фокус)**. Выберите **Focus mode (Режим фокусирования)**. Диалоговое окно изменяется в зависимости от выбранного режима: • **Absolute (Абсолютное положение)**: задайте положение фокуса, введя значение и нажав **Apply (Применить)**. • **Relative (Относительное положение)**: регулируйте фокус пошагово. Используйте **Near** для объектов, расположенных близко к камере, и **Far** для более удаленных объектов. • **Continuous (Непрерывное)**: перемещайте фокус с помощью **Nearer (Ближе)** или **Further (Дальше)** и после завершения нажмите **Stop (Остановить)**. • Для автоматической фокусировки нажмите **AF**.
Область предустановки фокуса	Чтобы добавить или удалить зону возврата фокуса, щелкните изображение правой кнопкой мыши и выберите **Focus recall zone (Зона возврата фокуса)**.
Автослежение Вкл./Выкл.	Чтобы включить или отключить автослежение для PTZ-камеры Axis с настроенным AXIS PTZ Autotracking, щелкните изображение правой кнопкой мыши и выберите **Autotracking on/off (Включить/отключить автослежение)**.
Предустановки	Чтобы перейти в предустановленное положение, щелкните изображение правой кнопкой мыши, выберите **Предустановки**, а затем выберите соответствующее предустановленное положение. Создание предустановленных положений описано в разделе *Предварительные установки PTZ*.
Добавить предустановку	Чтобы добавить предустановку, переместите изображение в нужное положение, щелкните правой кнопкой мыши и выберите **Presets (Предустановки) > Add preset (Добавить предустановку)**.

Абсолютное перемещение PTZ	Доступно для устройств ONVIF, поддерживающих абсолютное позиционирование PTZ. Используйте этот параметр для перемещения камеры в точные, воспроизводимые координаты. Чтобы использовать Absolute PTZ (Абсолютное положение PTZ), щелкните камеру в режиме живого просмотра правой кнопкой мыши и выберите **Absolute PTZ Move (Перемещение PTZ в абсолютное положение)**. Выберите систему координат: **Generic (Общая)** для стандартных координат или **Spherical (Сферическая)** для координат в градусах. Введите значения положения панорамирования, наклона и зума, задайте скорость перемещения и нажмите **OK** или **Send (Отправить)**.
Профиль потока	Чтобы задать профиль потока, щелкните изображение правой кнопкой мыши и выберите **Stream profile (Профиль потока)**. См. *Профили потоков*.

Добавление цифровых предустановленных положений

Управление функциями PTZ

Примечание

Администратор может отключить механическое управление PTZ для пользователей. См. *Права доступа пользователей*.

Запись видео и мгновенное воспроизведение в режиме живого просмотра

	Чтобы перейти на вкладку Recordings (Записи), выберите камеру или представление с разделением экрана и нажмите .
	Указывает текущую запись в живом просмотре.
	Указывает, что обнаружено движение.

	Чтобы воспроизвести текущую запись, наведите указатель мыши на изображение и нажмите **Instant replay (Мгновенное воспроизведение)**. Откроется вкладка Recordings (Записи) и воспроизведутся последние 5 секунд записи.
ЗАПИСЬ	Чтобы вручную начать запись в режиме живого просмотра, наведите указатель мыши на изображение и нажмите **REC**. Кнопка становится желтой, указывая на то, что запись выполняется. Чтобы остановить запись, нажмите **REC** еще раз.

Для настройки параметров ручной записи, таких как разрешение, сжатие и частота кадров, см. *Способ записи*. Более подробные сведения о записи и воспроизведении можно найти в разделе *Воспроизведение записей*.

Примечание

Администратор может отключить функцию ручной записи для пользователей. См. *Права доступа пользователей*.

Звук при живом просмотре

Звуковое сопровождение доступно, если камера поддерживает передачу звука и если звук включен в том профиле, который задействован для живого просмотра.

Перейдите к пункту **Configuration > Devices > Stream profiles (Конфигурация > Устройства > Профили потока)** и настройте звук для камеры. См. *Профили потоков, on page 57*.

Volume (Громкость)	Чтобы изменить громкость в виде, наведите курсор на изображение, затем на кнопку динамика, а затем используйте ползунок для изменения громкости. Чтобы отключить или включить звук, нажмите кнопку .
Слушать только этот вид	Чтобы отключить звук в других видах и прослушивать только этот вид, наведите курсор на изображение и нажмите кнопку .
Говорить через громкоговоритель	Чтобы сказать что-либо через настроенный громкоговоритель в режиме полного дуплекса, наведите курсор на изображение и нажмите кнопку .
Переговорная кнопка	Чтобы сказать что-либо через настроенный громкоговоритель в симплексном и полудуплексном режимах, наведите курсор на изображение и нажмите и удерживайте кнопку . Чтобы отобразить кнопку **Push-to-talk (Переговорная кнопка)** для всех дуплексных режимов, включите параметр **Use push-to-talk for all duplex modes (Использовать переговорную кнопку для всех дуплексных режимов)** в разделе **Configuration > Client > Streaming > Audio (Конфигурация > Клиент > Потоковая передача > Звук)**. См. *Потоковая передача, on page 129*.

Примечание

Являясь администратором, вы можете отключить звук для пользователей. См. *Права доступа пользователей*.

Экранная панель управления в режиме живого просмотра

Примечание

Для экранной панели управления требуется встроенное программное обеспечение версии 7.40 или более поздней.

	Для доступа к имеющимся функциям камеры в окне живого просмотра нажмите значок .

Мультиэкранный режим

Мультиэкранный режим позволяет отображать несколько видов в одном окне. В мультиэкранном представлении можно использовать представления камер, последовательности, веб-страницы, карты и другие мультиэкранные представления.

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro к вашей вкладке мультиэкранного режима можно добавить любой вид, камеру, устройство или аудиозону с других серверов.

Чтобы добавить мультиэкран:

1. На вкладке **Live view (Живой просмотр)** нажмите +.
2. Выберите пункт **Новый мультиэкран**.
3. Введите название для разделенного вида.
4. Выберите макет в раскрывающемся списке **Template (Шаблон)**.
5. Перетащите камеры или представления из боковой панели в сетку либо дважды щелкните элемент, чтобы добавить его в первую доступную ячейку.
6. Нажмите **Save view (Сохранить вид)**.

Чтобы изменить камеру или представление в сетке, выберите его. В разделе **Select item to configure (Выберите элемент для настройки)** можно:

- Нажать **Remove (Удалить)**, чтобы удалить элемент из сетки.
- Выбрать **PTZ preset (предустановленное положение PTZ)** в раскрывающемся списке.

Чтобы добавить область обзора:

- Выберите кадр и нажмите **Set hotspot (Задать область обзора)** в разделе **Hotspot (Область обзора)**.

Чтобы автоматически отображать в области обзора видеопотоки, активированные триггером:

- Выберите **Dynamic hotspot content (Динамическое содержимое области обзора)** и настройте параметры. Дополнительные сведения см. в разделе *Динамическая область наблюдения, on page 18*.

Чтобы задать профиль потока для камеры:

- Щелкните ее правой кнопкой мыши в режиме просмотра сетки и выберите **Stream profile (Профиль потока)**. См. раздел *Профили потоков, on page 57*.

Динамическая область наблюдения

Используйте динамические точки доступа для одновременного мониторинга нескольких событий. При срабатывании правил действий видеопотоки автоматически отображаются в точке доступа. Например, если движение обнаружено у трех разных входов, все три представления с камер отображаются одновременно.

Точка доступа автоматически изменяет сетку в зависимости от количества активных представлений. В каждом представлении отображается таймер обратного отсчета, по истечении которого представление исчезает.

Примечание

Для камер, активированных действиями просмотра в реальном времени с сохранением состояния, обратный отсчет начинается после прекращения действия. Для остальных камер и представлений обратный отсчет начинается сразу.

Создание динамической точки доступа

Чтобы добавить новое представление с динамической точкой доступа:

1. На вкладке **Live view (Живой просмотр)** нажмите +.
2. Нажмите **Add hotspot (Добавить точку доступа)**.
3. Выберите **Dynamic hotspot content (Динамическое содержимое точки доступа)**.
4. Настройте параметры:
   - **Number of split view cells (Количество ячеек разделенного представления)**: количество ячеек в сетке, даже если активные представления отсутствуют. Диапазон: от 1 до 144.
   - **Countdown in seconds (Обратный отсчет в секундах)**: время отображения каждого активированного представления. Установите значение 0, чтобы представления отображались до их удаления вручную. Диапазон: от 0 до 999.
   - **Seconds remaining when countdown appears in view (Количество секунд до отображения обратного отсчета)**: определяет, когда на экране появляется таймер обратного отсчета. Установите значение 0, чтобы таймер отображался постоянно. Обратите внимание, что отображение таймера использует системные ресурсы. Диапазон: от 0 до 999.
   - **Mute audio on incoming views (Отключать звук во входящих представлениях)**: новые потоки запускаются без звука. Вы можете включать в них звук по-отдельности.
   - **Allow adding views with click on view (Разрешить добавление представлений щелчком)**: позволяет вручную добавлять представления в точку доступа, щелкая по ним, наряду с активированными представлениями.
   - **Allow adding views with hotkey (Разрешить добавление представлений с помощью горячей клавиши)**: позволяет использовать сочетания клавиш для добавления заданных представлений в точку доступа, наряду с активированными представлениями.
5. Нажмите **Save view (Сохранить вид)**.

Чтобы добавить динамическую точку доступа в существующее представление:

1. На вкладке **Live view (Живой просмотр)** нажмите **Edit view (Изменить представление)**.
2. Нажмите **Add hotspot (Добавить точку доступа)**.
3. Выберите **Dynamic hotspot (Динамическая точка доступа)**.
4. Настройте параметры, описанные выше в шаге 4.
5. Нажмите **Save view (Сохранить вид)**.

Примечание

Существующую точку доступа можно преобразовать в динамическую, изменив ее настройки на вкладке **Live view (Живой просмотр)**.

Управление представлениями

Каждая ячейка динамической точки доступа содержит:

- **Индикатор обратного отсчета**: показывает оставшееся время до исчезновения представления.
- **Кнопка паузы**: приостанавливает обратный отсчет, чтобы дольше отображать представление.
- **Кнопка закрытия**: немедленно удаляет представление из точки доступа.

- **Индикатор мигания**: рамка обратного отсчета мигает при повторном срабатывании для представления.

Эти элементы управления скрыты при развертывании ячейки на весь экран или переходе в режим воспроизведения. Дважды щелкните любую ячейку, чтобы развернуть ее на весь экран. В развернутом представлении обратный отсчет автоматически приостанавливается. Динамическая точка доступа продолжает обновляться в фоновом режиме. При возврате к представлению в виде сетки отображаются активные представления.

Примечание

При переходе в режим воспроизведения видеопотоки с камер фиксируются и не обновляются. Перейдите обратно в режим живого просмотра, чтобы возобновить обычную работу.

Панель управления дверью в мультиэкранном режиме

Если дверь настроена, можно помогать держателям карт, а также отслеживать состояние двери и замка и последние операции в режиме разделенного экрана.

1. Добавьте дверь. См. *Добавьте дверь, on page 158*.
2. Добавьте панель управления дверью к мультиэкранному виду, см. *Мультиэкранный режим, on page 18*.

Панель управления	Чтобы просмотреть сведения о двери и состояние замка, откройте вкладку **Dashboard (Панель мониторинга)**. На вкладке панели управления отображаются следующие сведения: • События контроля доступа с данными и фотографиями держателей карт, например при предъявлении держателем карты. • Сигналы тревоги с информацией о причине тревоги (дверь открыта слишком долго и т. п.). • Последняя операция.
	Чтобы добавить событие в закладки и сделать его доступным на вкладке **Transactions (Операции)**, нажмите .
Доступ	Чтобы предоставить доступ вручную, нажмите кнопку **Access (Доступ)**. Это разблокирует дверь так, как если бы кто-то предъявил свои учетные данные. Дверь автоматически снова запирается через заданное время.
Lock (Заблокировать)	Чтобы вручную заблокировать дверь, нажмите кнопку **Lock (Заблокировать)**.
Отпереть	Чтобы вручную разблокировать дверь, нажмите кнопку **Unlock (Разблокировать)**. Дверь будет оставаться разблокированной до тех пор, пока вы снова не заблокируете ее вручную.

Блокировать	Чтобы предотвратить доступ к двери, нажмите **Lockdown (Блокирование)**.
Транзакции	Чтобы просмотреть последние операции и сохраненные операции, откройте вкладку **Transactions (Операции)**.

Контроль за дверью и оказание помощи владельцам карт с помощью панели управления дверью

Панель аналитики AXIS Data Insights Dashboard в режиме мультиэкрана

AXIS Data Insights Dashboard отображает данные аналитики с устройств в виде графиков и диаграмм. Для добавления панели аналитики к мультиэкрану:

1. Настройка панели управления. См. *Панель аналитики AXIS Data Insights Dashboard, on page 188*.
2. На вкладке **Live view (Просмотр в реальном времени)** нажмите +.
3. Выберите пункт **Новый мультиэкран**.
4. Разверните папку **Dashboards (Панели управления)**.
5. Перетащите панель управление в требуемую ячейку сетки.
6. Нажмите **Save view (Сохранить вид)**.

Панели управления	
Audio Analytics	Отображение данных о событиях AXIS Audio Analytics.
Подсчет количества пересечений	Отображает данные сценария подсчета пересечений линии AXIS Object Analytics.
Станд.	Отображение данных из всех поддерживаемых источников.
Состояние изображения	Отображение данных о событиях AXIS Image Health Analytics.
Подсчет посетителей для области	Отображение данных о подсчете посетителей из AXIS Object Analytics.
Подсчет входящих и выходящих посетителей	Отображение данных из сценария подсчета количества пересечений AXIS Object Analytics, а также данных AXIS People Counter и AXIS P8815-2 3D People Counter.
Мониторинг качества воздуха	Отображает данные о качестве воздуха в помещении в реальном времени с соответствующих датчиков AXIS.
Мониторинг качества воздуха – подробный	Отображает агрегированные данные с датчиков качества воздуха AXIS.

Использование интерфейсов оповещения в мультиэкранном режиме

Интерфейсы оповещения можно использовать для трансляции объявлений в реальном времени, выполнения вызовов или воспроизведения аудиофайлов с аудиоустройств. Для этого требуется интеграция с AXIS Audio Manager Pro. Для получения дополнительной информации см. раздел *Настройка AXIS Audio Manager Pro, on page 183*.

Для использования интерфейсов оповещения:

1. редактируйте или добавьте новый вид в мультиэкранном режиме.
2. Перетащите одну или несколько аудиозон на сетку, чтобы превратить ее в интерфейс оповещения.

Примечание

Аудиозоны в AXIS Camera Station Pro идентичны зонам, настроенным на сервере AXIS Audio Manager Pro.

3. Выберите **Speak (Говорить)**, **Call (Вызвать)**, или **Play a file (Воспроизведение файла)**:
   - **Speak** (Говорить) — одностороннее объявление (например, трансляция голосового сообщения).
   - **Call** (Вызов) — двусторонняя связь, например для общения через переговорное устройство.
   - **Play a file (Воспроизвести файл)** — воспроизведение аудиофайла с сервера AXIS Audio Manager Pro через громкоговорители.

последовательно.

Последовательность автоматически переключает представления.

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro к вашей последовательности можно добавить любой вид, камеру или устройство с других серверов.

Чтобы добавить последовательность:

1. На вкладке **Live view (Живой просмотр)** нажмите +.
2. Выберите **Новая последовательность**.
3. Введите название последовательности.
4. Перетащите один или несколько видов или камер в последовательность видов.
5. Расположите представления в нужном порядке.
6. Нажмите представление, чтобы изменить его настройки.
7. Нажмите **Save view (Сохранить вид)**.

Предустановка положений PTZ	Для камер с функцией PTZ выберите предустановленное положение PTZ, в которое должна переместиться камера при активации этого представления.
Длительность пребывания	Количество секунд, в течение которых отображается каждое представление перед переключением на следующее. Этот параметр можно задать отдельно для каждого вида.

Примечание

- Нельзя добавить представление последовательности в другое представление последовательности.
- Нельзя напрямую добавлять представления компонентов с удаленного сервера. В качестве обходного решения сначала добавьте представление компонента в одно мультиэкранное представление, а затем добавьте это мультиэкранное представление с удаленного сервера.
- Воспроизведение на временной шкале может работать некорректно. При воспроизведении отображаются все камеры последовательности, но одновременно активна только одна камера.

Использование панели последовательности

При просмотре последовательности в нижней части окна отображается панель, позволяющая вручную управлять воспроизведением:

- Используйте клавиши [>] и [<] для перехода к следующему или предыдущему обзору.
- Используйте **Hold (Удерживать)** или **Continue (Продолжить),** чтобы приостановить или возобновить воспроизведение последовательности.
- Обратный отсчет показывает, сколько секунд осталось до следующего автоматического переключения.
- Щелкните последовательность правой кнопкой мыши, чтобы скрыть панель.
- Когда последовательность открыта на вкладке **Recording (Запись)**, она автоматически переходит в **режим Hold (Удержание)**, и перемещаться по ней можно только вручную с помощью кнопок «Далее» и «Назад».

Вид с камеры

Вид с камеры отображает видео в реальном времени с одной камеры. Виды с камер могут использоваться в мультиэкранном режиме для последовательного просмотра и в виде карт.

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro в списке отображаются все камеры со всех подключенных серверов.

Как добавить вид с камеры:

1. Щелкните значок + на вкладке «Живой просмотр» или «Записи».
2. Выберите **Новый вид с камеры**.
3. В раскрывающемся меню выберите камеру и нажмите **OK**.

Карта

Карта представляет собой импортированное изображение, на которое можно размещать представления камер, мультиэкранные представления, аудиозоны, последовательности, веб-страницы, другие карты и двери. Карта обеспечивает визуальный обзор и способ, позволяющий находить отдельные устройства и осуществлять к ним доступ. Для больших установок можно создать несколько карт и расположить их на обзорной карте.

Кнопки действий также доступны в режиме просмотра карты. См. *Создание триггеров для кнопок действий*.

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro к вашей вкладке карты можно добавить любой вид, камеру или устройство с других серверов.

Чтобы добавить карту:

1. На вкладке **Live view (Живой просмотр)** нажмите +.
2. Выберите **Новая карта**.

3. Задайте имя карте
4. Нажмите **Choose image (Выбрать изображение)** и найдите нужный файл карты. Размер файла не должен превышать 20 МБ. Поддерживаются форматы BMP, JPG, PNG и GIF.
5. Перетащите на данную карту виды, камеры, другие устройства и двери.
6. Нажмите значок на карте, чтобы изменить его настройки.
7. Нажмите **Add label (Добавить обозначение)**, введите имя обозначения и задайте размер, угол поворота, стиль и цвет обозначения.
8. Нажмите **Save view (Сохранить вид)**.

Примечание

- Одновременно можно также изменять некоторые параметры для нескольких значков и обозначений.
- При редактировании карты с нее удаляются все устройства, к которым у вашей учетной записи пользователя нет доступа.
- Нельзя напрямую добавлять представления компонентов с удаленного сервера. В качестве обходного решения сначала добавьте представление компонента в одно мультиэкранное представление, а затем добавьте это мультиэкранное представление с удаленного сервера на карту.

Настройки значков

Нажмите значок на карте, чтобы открыть его настройки.

	Физическое состояние двери, если для двери настроен дверной монитор.
	физическое состояние замка, если для двери не настроен дверной монитор.
	Красный предупреждающий треугольник указывает на несанкционированные действия на двери, считывающем устройстве или дверном контроллере.
Значок	Выберите значок, который должен использоваться. Этот параметр доступен только для камер и других устройств.
Объем	Измените размер значка с помощью ползунка.
Цвет	Нажмите значок , чтобы изменить цвет значка.
Название	Включите этот параметр, если должно отображаться имя значка. Выберите **Bottom (Внизу)** или **Top (Вверху)**, чтобы задать расположение имени значка.
Зона охвата	Доступно для поддерживаемых устройств. Включите этот параметр, если на карте должна отображаться зона охвата устройства. Можно изменить **диапазон**, **ширину**, **направление** и цвет зоны охвата. Включите параметр **Flash (Мигание)**, чтобы область обзора мигала при запуске записи по обнаружению движения или другим правилам действий. Чтобы отключить мигание областей обзора для всех устройств, см. *Настройки клиента, on page 126*.

Стрелка направления	Отображает стрелки, указывающие направление области обзора каждой камеры. Вы можете отобразить стрелки с зонами охвата или без них.
Показать индикаторы записи	Определяет, какие индикаторы записи отображаются на значке. Включите параметр **Small indicators (Малые индикаторы)**, чтобы отображать индикаторы в компактном виде. С помощью отдельных переключателей можно показать или скрыть индикаторы **Recording (Запись), Motion detected (Обнаружено движение)**, **Object detected (Обнаружен объект)** и **Action rule active (Правило действий активно).** Этот параметр хранится на сервере, поэтому его конфигурация используется всеми клиентами.
Идентификатор	Метка содержит текст, размер, угол поворота и цвет. Также можно включить подчеркивание и курсив для текста метки.
Удалить	Нажмите значок , чтобы удалить значок с карты.

Перемещение по карте

Масштабирование и перемещение
- Вы можете масштабировать и перемещать карту с помощью мыши, клавиатуры или джойстика. В настоящее время сенсорное управление не поддерживается.

Использование мыши.
- Увеличение и уменьшение изображения с помощью колесика мыши.
- При масштабировании перетаскивайте курсор, чтобы перемещаться по карте.

Использование клавиатуры.
- Нажмите Ctrl + [+], чтобы увеличить, и Ctrl + [-], чтобы уменьшить.
- Для поворота и наклона используйте комбинацию клавиш Ctrl + клавиши со стрелками.

Использование джойстика.
- Поверните головку джойстика, чтобы увеличить или уменьшить масштаб.
- Наклоняйте джойстик для поворота и наклона.

Сделать моментальный снимок
- Нажмите правой кнопкой мыши по карте, чтобы открыть контекстное меню. Можно сохранить снимок карты на диск или добавить его на вкладку **Export (Экспорт).** На снимке карта сохраняется в текущем виде, включая все текущие состояния камер и индикаторов.

Веб-страница

Вид "Веб-страница" отображает страницу из Интернета. Например, веб-страницу можно добавить в представление с разделением экрана или в последовательность.

Чтобы добавить веб-страницу:

1. На вкладке **Live view (Живой просмотр)** нажмите .
2. Выберите **New web page (Новая веб-страница)**.
3. Задайте имя карте
4. Введите URL веб-страницы.

5. Нажмите кнопку **OK**.

Папки

Используйте папки для распределения элементов по категориям в системе навигации в виде дерева. Папки могут содержать мультиэкранные виды, последовательности, виды с камер, карты, веб-страницы и другие папки.

Чтобы добавить папку:

1. Щелкните значок + на вкладке «Живой просмотр» или «Записи».
2. Выберите **Новая папка**.
3. Введите имя папки и нажмите **OK**.

Записи

На вкладке **Recordings (Записи)** можно искать, воспроизводить и экспортировать записи. Вкладка состоит из основного представления и двух панелей, в которых можно найти представления, изображения, инструменты воспроизведения и камеры с подключенных серверов, сгруппированные по имени сервера. См. *Просмотр в реальном времени*.

В основном представлении можно управлять изображением так же, как в режиме живого просмотра. Дополнительные сведения см. в разделе *Управление изображением в режиме живого просмотра, on page 14*.

Чтобы изменить способ записи и такие параметры, как разрешение, сжатие и частоту кадров, см. *Способ записи*.

Примечание

Записи из AXIS Camera Station Pro невозможно удалять вручную. Чтобы удалить старые записи, измените срок хранения в **Configuration > Storage > Selection (Конфигурация > Хранилище > Выбор)**.

Воспроизведение записей

Одновременное воспроизведение записей с нескольких камер возможно, когда маркер воспроизведения установлен на нескольких записях на временной шкале.

Вы можете одновременно отображать живое и записанное видео при использовании нескольких мониторов.

Временная шкала воспроизведения

Когда курсор наводится на запись на шкале времени, отображаются тип и время записи. Для получения улучшенного вида и поиска записей, можно увеличивать, уменьшать масштаб и перетаскивать шкалу времени. Воспроизведение временно приостанавливается при перетаскивании шкалы времени и возобновляется, если вы ее отпустите. Перемещайтесь по временной шкале, чтобы получить обзор содержимого и найти определенные моменты.

- Красная линия обозначает запись по детектору движения.
- Синяя линия обозначает запись, запущенную правилом действия.

Поиск записей

	Щелкните, чтобы выбрать дату и время на шкале времени.
	Отфильтруйте типы записей, отображаемые на временной шкале.
	Используйте , чтобы найти сохраненные закладки. См. *Закладки*.
	Нажмите, чтобы открыть список записей и закладок, созданных с помощью нательной камеры Axis. Здесь вы можете искать по дате и времени, методу активации записи, а также по любым категориям и заметкам, которые пользователь камеры добавил в AXIS Body Worn Assistant.
Умный поиск 1	Используйте Умный поиск 1 для поиска записей. См. *Умный поиск 1*.

Воспроизведение записей

	Воспроизвести запись.
	Приостановить запись.
	Выполняет быстрый переход к началу текущей записи или к предыдущей записи или событию. Щелкните правой кнопкой мыши, чтобы перейти к записям, событиям или и к тому, и другому.
	Выполняет быстрый переход к началу следующей записи или событию. Щелкните правой кнопкой мыши, чтобы перейти к записям, событиям или и к тому, и другому.
	Выполняет переход к предыдущему кадру записи. Приостановите запись, чтобы использовать данную функцию. Щелкните правой кнопкой мыши, чтобы указать, сколько кадров следует пропустить (до 20 кадров).
	Выполняет переход к следующему кадру записи. Приостановите запись, чтобы использовать данную функцию. Щелкните правой кнопкой мыши, чтобы указать, сколько кадров следует пропустить (до 20 кадров).
	Измените скорость воспроизведения, используя коэффициенты в выпадающем меню.
	Выключите звук. Эта функция имеется только у записей со звуком.
Ползунок регулировки звука	Сдвиньте, чтобы изменить громкость звука. Эта функция имеется только у записей со звуком.
Показать все метаданные нательного устройства	Показывает метаданные для нательной системы и отображает заметки и категории из AXIS Body Worn Assistant.
Панорамирование, наклон и зум	Щелкните изображение и прокрутите колесо мыши, чтобы увеличить или уменьшить изображение. Чтобы увеличить определенную область, перед прокруткой поместите указатель мыши на нее.

Закладки

Примечание

- Вы не можете удалить заблокированную запись, пока не разблокируете ее вручную.
- Защищенные записи удаляются при удалении связанной камеры из системы.

	Щелкните, чтобы показать все закладки. Чтобы отфильтровать закладки, нажмите данный значок.
	Добавление новой закладки.
	Означает, что эта запись заблокирована. Запись включает в себя не менее 2,5 минут видео до и после закладки.

	Измените имя и описание закладки либо защитите запись от удаления или снимите защиту.
	Удалите закладку. Чтобы удалить несколько закладок, выделите их, удерживая клавишу Ctrl или Shift, и нажмите **Remove (Удалить)**.
Запретить удаление записи	Установите этот флажок, чтобы защитить запись от удаления. Снимите флажок, чтобы снять защиту.

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 снять защиту записи, снимите флажок **Prevent recording deletion (Запретить удаление записи)** или удалите закладку.

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

Категории событий

Назначайте категориям записи, чтобы упростить поиск записей определенных типов событий. Перед началом убедитесь, что у вас есть соответствующие права пользователя. См. раздел *Права доступа пользователей или групп, on page 146*.

Назначение категорий событий

1. На вкладке **Recordings (Записи)** найдите запись, которой необходимо назначить категорию.
2. Щелкните запись на временной шкале правой кнопкой мыши и выберите **Categorize event (Классифицировать событие)**.
3. Добавьте одну или несколько категорий.
4. Нажмите кнопку **OK**.

При категоризации события выбранные категории отображаются на миниатюре предварительного просмотра записи. Если для категории задан цвет, он отображается на временной шкале.

Удаление категорий событий

1. На вкладке **Recordings (Записи)** найдите запись, из которой необходимо удалить категории.
2. Щелкните запись на временной шкале правой кнопкой мыши и выберите **Categorize event (Классифицировать событие)**.
3. В списке назначенных категорий выберите категорию, которую нужно удалить.
4. Выберите пункт **Remove (Удалить)**.
5. Повторите шаги 3–4 для каждой категории, которую требуется удалить.
6. Нажмите кнопку **OK**.

Примечание

Кнопка **Remove (Удалить)** доступна только при наличии разрешения на удаление категорий или при выборе в списке неназначенной категории.

Для получения дополнительных сведений см. *Настроить категории событий, on page 96*.

Экспорт записей

На вкладке **Export (Экспорт)** можно экспортировать записи на локальное устройство хранения или в сетевое расположение. Здесь также можно просмотреть сведения о записи и ее предварительный просмотр. Можно одновременно экспортировать несколько файлов в форматах ASF, MP4 и MKV.

Для воспроизведения записей используется проигрыватель Windows Media (.asf) или AXIS File Player (.asf, .mp4, .mkv). Проигрыватель AXIS File Player — это бесплатное ПО для воспроизведения видео и звука, не требующее установки.

Примечание

В AXIS File Player можно изменять скорость воспроизведения записей в форматах MP4 и MKV, но не в формате ASF.

Прежде чем начать, убедитесь, что у вас есть разрешение на выполнение экспорта. См. *Разрешение на экспорт для пользователей, on page 33*.

Чтобы экспортировать запись:

1. На вкладке **Recordings (Записи)** выберите камеру или вид.
2. Добавьте записи в список экспорта. Записи на шкале времени, не включенные в экспорт, имеют полосатую расцветку.
   2.1. Нажмите значок , чтобы отобразить маркеры выбора.
   2.2. Перемещайте эти маркеры, чтобы выбрать записи, которые требуется экспортировать.
   2.3. Нажмите , чтобы открыть вкладку **Export (Экспорт)**.
3. Нажмите на **Export...(Экспорт)**
4. Выберите папку, в которую нужно экспортировать записи.
5. Нажмите кнопку **OK**. Задача экспорта отображается на вкладке **Tasks (Задачи)**.

Папка экспорта содержит следующие элементы:

- Записи в выбранном формате.
- TXT-файл с примечаниями, если выбран параметр **Include notes (Включить примечания)**.
- Проигрыватель AXIS File Player, если был выбран параметр **Include AXIS File Player (Включить AXIS File Player)**.
- Файл списка воспроизведения ASX, если выбран параметр **Create playlist (.asx) (Создать список воспроизведения (.asx))**.

Экспорт записей

Вкладка Recordings (Записи)	
	Чтобы выбрать несколько записей, нажмите и переместите маркеры выделения в нужные начальную и конечную точки.
	Чтобы экспортировать записи между маркерами выделения, нажмите .
Добавить записи	Чтобы добавить отдельную запись, щелкните ее правой кнопкой мыши и выберите **Export (Экспорт) > Add recordings (Добавить записи)**.
Добавить записи событий	Для добавления всех записей, произошедших во время события, щелкните запись правой кнопкой мыши и выберите **Export > Add event recordings (Экспорт > Добавить записи событий)**.
Удалить записи	Чтобы удалить отдельную запись из списка экспорта, щелкните ее правой кнопкой мыши и выберите **Export (Экспорт) > Remove recordings (Удалить записи)**.
Удалить записи	Для удаления из списка экспорта всех записи между маркерами выбора щелкните правой кнопкой мыши за пределами записи и выберите **Export > Remove recordings (Экспорт > Удалить записи)**.

Вкладка Export (Экспорт)	
Звук	Чтобы убрать звук из экспортированной записи, снимите флажок в столбце **Audio (Звук)**. Чтобы всегда включать звук в экспортированные записи, перейдите в раздел **Configuration** > **Server** > **Settings** > **Export (Настройка > Сервер > Параметры > Экспорт)** и выберите **Include audio when adding recordings to export (Добавить звук при добавлении записей для экспорта)**.
	Чтобы изменить запись, выберите ее и щелкните . См. *Редактирование записей перед экспортом, on page 33*.
	Для изменения примечания к записи выберите запись и щелкните .
	Чтобы удалить запись из списка экспорта, выберите ее и нажмите .
Перейти к экспортированию	Если открыта вкладка **Incident report (Отчет об инциденте)**, нажмите **Switch to export (Перейти к экспорту)**, чтобы вернуться на вкладку **Export (Экспорт)**.
Предпочтительный профиль потока	Выберите профиль потока в поле **Preferred stream profile (Предпочтительный профиль потока)**.

Вкладка Export (Экспорт)	
Предварительный просмотр	Для предварительного просмотра записи щелкните эту запись в списке экспорта, чтобы воспроизвести ее. Предварительный просмотр нескольких записей доступен только для записей с одной и той же камеры.
Сохранить	Чтобы сохранить список экспорта в файл, нажмите **Save (Сохранить)**.
Загрузить	Чтобы добавить ранее сохраненный список экспорта, нажмите **Load (Загрузить)**.
Название экспортируемого содержимого	Введите пользовательское имя для экспортируемой папки и файлов или оставьте поле пустым, чтобы использовать соглашение об именовании по умолчанию в AXIS Camera Station Pro.
Добавить имя камеры и метку времени	Выберите эту опцию, чтобы добавить имя камеры и метку времени к имени экспортируемой папки и файлов.
Настройка времени начала и окончания	Для настройки времени начала и окончания записи перейдите на шкалу времени в предварительном просмотре и настройте время начала и окончания. На шкале времени отображается до тридцати минут записи до и после выбранной записи.
Добавить моментальный снимок	Чтобы добавить стоп-кадр, перетаскивайте временную шкалу в окне предварительного просмотра в нужное место расположения, нажмите правой кнопкой мыши на области предварительного просмотра и выберите пункт**Add snapshot (Добавить стоп-кадр)**.

Расширенные настройки	
Включая примечания	Выберите **Include notes (Включить примечания)**, чтобы добавить примечания к записям в виде TXT-файла в экспортируемую папку и закладки в AXIS File Player.
Include AXIS File Player (Включить AXIS File Player)	Чтобы добавить AXIS File Player к экспортируемым записям, выберите **Include AXIS File Player (Включить AXIS File Player)**.
Create playlist (.asx) (Создать список воспроизведения (.asx))	Чтобы создать список воспроизведения в формате ASX для использования в Windows Media Player, выберите **Create playlist (.asx) (Создать список воспроизведения (.asx))**. Записи будут воспроизводиться в том порядке, в котором они записывались.
Добавить цифровую подпись	Чтобы предотвратить несанкционированные действия с изображением, выберите **Add digital signature (Добавить цифровую подпись)**. Данный

Расширенные настройки	
	параметр доступен только для записей в формате ASF. См. *Воспроизведение и проверка экспортированных записей, on page 35*.
Экспорт в ZIP-файл	Чтобы экспортировать в ZIP-файл, выберите **Export to Zip file (Экспортировать в ZIP-файл)** и при необходимости введите пароль.
Export format (Формат экспорта)	В раскрывающемся списке **Export format (Формат экспорта)** выберите формат для экспорта записей.. При выборе формата MP4 экспортируемые записи не содержат звук в формате G.711 или G.726.
Edited video encoding (Формат редактируемого видео)	Для отредактированных видео можно задать формат кодирования видео `Automatic`, `H.264` или `M-JPEG` в разделе **Edited video encoding (Формат редактируемого видео)**. Выберите `Automatic`(Автоматически), чтобы использовать M-JPEG для формата M-JPEG и H.264 для всех остальных форматов.

Разрешение на экспорт для пользователей

Для экспорта записей или создания отчетов об инцидентах необходимы соответствующие разрешения.

Можно иметь разрешение на выполнение одной из этих операций или обеих. При выборе на вкладке **Recordings (Записи)** откроется подключенная вкладка экспорта.

Чтобы настроить разрешения, перейдите в раздел *Права доступа пользователей, on page 144*.

Редактирование записей перед экспортом

Размытие движущегося объекта

1. На вкладке **Export (Экспорт)** или **Incident report (Отчет об инцидентах)** выберите запись и щелкните .
2. Переместите шкалу времени к первому появлению движущегося объекта, который требуется покрыть.
3. Щелкните **Bounding boxes > Add (Прямоугольные рамки > Добавить)**, чтобы добавить новую прямоугольную рамку.
4. Перейдите в **Bounding box options > Size (Параметры прямоугольной рамки > Размер)**, чтобы изменить размер.
5. Переместите прямоугольную рамку и поместите ее поверх объекта.
6. Перейдите в **Bounding box options > Fill (Параметры прямоугольной рамки > Заливка)** и выберите **Pixelated (Пикселизированная)** или **Black (Черная)**.
7. При воспроизведении записи щелкните объект правой кнопкой мыши и выберите **Add key frame (Добавить ключевой кадр)**.
8. Чтобы добавить несколько ключевых кадров подряд, переместите прямоугольную рамку таким образом, чтобы она перекрывала объект при воспроизведении записи.
9. Переместите шкалу времени и убедитесь, что прямоугольная рамка покрывает объект на протяжении всей записи.

10. Чтобы задать конечную точку, щелкните правой кнопкой мыши ромбовидный маркер последнего ключевого кадра и выберите **Set end (Задать конечную точку)**. Это приведет к удалению ключевых кадров после конечной точки.

Примечание

В видео можно добавить несколько ограничивающих прямоугольных рамок. Если прямоугольные рамки перекрываются, для области перекрытия используется заливка в следующем порядке: Black (Черная), Pixelated (Пикселизированная), затем Clear (Прозрачная).

Удалить все	Чтобы удалить все прямоугольные рамки, выберите **Bounding boxes > Remove all (Прямоугольные рамки > Удалить все)**.
Удалить ключевой кадр	Чтобы удалить ключевой кадр, щелкните по нему правой кнопкой мыши и выберите пункт **Remove key frame (Удалить ключевой кадр)**.

Отображение движущегося объекта с размытым фоном

1. Создайте прямоугольную рамку. См. *Размытие движущегося объекта, on page 33*.
2. Перейдите к пункту **Bounding box options > Fill (Параметры прямоугольной рамки > Заполнение)** и установите значение **Clear (Прозрачное)**.
3. Перейдите в раздел **Video background (Фон видео)** и установите значение **Pixelated (Пикселизация)** или **Black (Темный)**.

Пикселизировать все, кроме этого	Выберите несколько прямоугольных рамок, щелкните правой кнопкой мыши и выберите **Pixelate all but this (Пикселизировать все, кроме этого)**. Выбранные прямоугольные рамки становятся **прозрачными**, а невыбранные — **пикселизированными**.

Создать прямоугольники

Чтобы создать прямоугольные рамки на основе данных аналитики, убедитесь, что аналитика камеры включена. См. *Профили потоков, on page 57*.

1. На вкладке **Export (Экспорт)** или **Incident report (Отчет об инцидентах)** щелкните значок .
2. Выберите **Generate bounding boxes (Создание прямоугольных рамок)**.
3. Убедитесь, что прямоугольные рамки охватывают движущийся объект. При необходимости скорректируйте их.
4. Выберите заливки для прямоугольных рамок или фона видео.

Улучшенный монтаж видео с помощью приложения AXIS Video Content Stream

Для повышения эффективности редактирования видео рекомендуется установить приложение AXIS Video Content Stream 1.0 на камеры с версией прошивки от 5.50 до 9.60. При добавлении такой камеры в систему AXIS Camera Station Pro автоматически инициирует процесс установки данного приложения. См. *Установка приложений для камер*.

Изменение записей перед экспортом

Воспроизведение и проверка экспортированных записей

Чтобы предотвратить несанкционированные действия с изображением, можно добавить цифровую подпись к экспортированным записям с паролем или без него. Для проверки цифровой подписи и наличия изменений в записи используйте AXIS File Player.

1. Перейдите в папку с экспортированными записями. Когда экспортированный ZIP-файл защищен паролем, введите пароль, чтобы открыть папку.
2. Откройте AXIS File Player. Экспортированные записи воспроизводятся автоматически.
3. В AXIS File Player нажмите , чтобы просмотреть примечания к записи.
4. Чтобы проверить цифровую подпись записей, экспортированных с помощью **Add digital signature (Добавить цифровую подпись)**:
   4.1. Перейдите в **Tools (Инструменты) > Verify digital signature (Проверить цифровую подпись)**.
   4.2. Выберите **Validate with password (Проверка с паролем)** и введите пароль, если установлена защита с помощью пароля.
   4.3. Чтобы просмотреть результаты проверки, щелкните **Verify (Проверить)**.

Экспорт отчетов об инцидентах

На вкладке **Incident report (Отчет об инциденте)** можно экспортировать отчеты об инцидентах на локальное устройство хранения или в сетевое расположение. В отчеты об инцидентах можно включать записи, снимки и примечания.

Прежде чем начать, убедитесь, что у вас есть разрешение на выполнение экспорта. См. *Разрешение на экспорт для пользователей, on page 33*.

Отчеты об инцидентах

Создание отчетов об инцидентах

1. На вкладке **Recordings (Записи)** выберите камеру или вид.
2. Добавьте записи в список экспорта. См. *Экспорт записей, on page 30*.
3. Нажмите **Switch to incident report (Перейти к отчету об инциденте)**, чтобы перейти на вкладку **Incident report (Отчет об инциденте)**.
4. Выберите пункт **Create report (Создать отчет)**.
5. Выберите папку, в которую требуется сохранить отчет об инцидентах.

6. Нажмите кнопку **OK**. Задание экспорта отчета об инциденте отображается на вкладке **Tasks (Задания)**.

Папка экспорта содержит следующие элементы:

- AXIS File Player.
- Записи в выбранном формате.
- Файл в формате .txt, если был выбран параметр **Include notes (Включить примечания)**.
- Отчет об инцидентах.
- Список воспроизведения, если выполняется экспорт нескольких записей.

Звук	Чтобы убрать звук из экспортированной записи, снимите флажок в столбце **Audio (Звук)**. Чтобы всегда включать звук в экспортированные записи, перейдите в раздел **Configuration** > **Server** > **Settings** > **Export (Настройка > Сервер > Параметры > Экспорт)** и выберите **Include audio when adding recordings to export (Добавить звук при добавлении записей для экспорта)**.
	Чтобы изменить запись, выберите ее и щелкните . См. *Редактирование записей перед экспортом, on page 33*.
	Для изменения примечания к записи выберите запись и щелкните .
	Чтобы удалить запись из списка экспорта, выберите запись и нажмите .
Перейти к отчету об инцидентах	Если открыта вкладка **Export (Экспорт)**, нажмите **Switch to incident report (Перейти к отчету об инциденте)**, чтобы перейти на вкладку **Incident report (Отчет об инциденте)**.
Предпочтительный профиль потока	Выберите профиль потока в раскрывающемся списке **Preferred stream profile (Предпочтительный профиль потока)**.
Предварительный просмотр	Чтобы просмотреть запись, нажмите ее в списке экспорта для воспроизведения. Предварительный просмотр нескольких записей доступен только для записей с одной и той же камеры.
Сохранить	Чтобы сохранить отчет об инциденте в файл, нажмите **Save (Сохранить)**.
Загрузить	Чтобы загрузить ранее сохраненный отчет об инциденте, нажмите **Load (Загрузить)**.
Описание	Поле **Description (Описание)** автоматически заполняется предварительно заданными данными из шаблона описания. В отчет об инциденте также можно добавить дополнительную информацию.
Категория	Выберите категорию, которой принадлежит отчет.
Reference ID (Ссылочный идентификатор)	Автоматически создается **Reference ID (Идентификатор)**. При необходимости его можно

	изменить вручную. Идентификатор является уникальным и позволяет идентифицировать отчет об инциденте.
Включая примечания	Выберите **Include notes (Включить примечания)**, чтобы добавить примечания к записям в виде TXT-файла в экспортируемую папку и закладки в AXIS File Player.
Edited video encoding (Формат редактируемого видео)	Для отредактированных видео можно задать формат кодирования видео `Automatic`, `H.264` или `M-JPEG` в разделе **Edited video encoding (Формат редактируемого видео)**. Выберите `Automatic`(Автоматически), чтобы использовать M-JPEG для формата M-JPEG и H.264 для всех остальных форматов.
Настройка времени начала и окончания	Для настройки времени начала и окончания записи перейдите на шкалу времени в предварительном просмотре и настройте время начала и окончания. На шкале времени отображается до тридцати минут записи до и после выбранной записи.
Добавить моментальный снимок	Чтобы добавить снимок, переместите временную шкалу в области предварительного просмотра в нужное положение, щелкните область предварительного просмотра правой кнопкой мыши и выберите **Add snapshot (Добавить стоп-кадр)**.

Запись в ручном режиме

Примечание

Когда выполнятся подключение к нескольким серверам AXIS Camera Station Pro, вы можете вручную запускать и останавливать запись на любом подключенном сервере. Для этого выберите сервер в раскрывающемся списке **Selected server (Выбранный сервер)**.

Чтобы вручную включить и остановить запись из главного меню:

1. Выберите ☰ > **Actions (Действия)** > **Record manually (Запись вручную)**.
2. Выберите одну или несколько камер.
3. Щелкните **Start (Пуск)**, чтобы начать запись.
4. Чтобы остановить запись, нажмите **Stop (Стоп)**.

Чтобы вручную включить и остановить запись в режиме **Live view (Живой просмотр)**.

1. Перейдите к пункту **Live view (Живой просмотр)**.
2. Наведите указатель мыши на рамку живого просмотра камеры.
3. Чтобы запустить запись, щелкните **REC (Запись)**. При выполнении записи в рамке вида отображается красный индикатор.
4. Чтобы остановить запись, щелкните **REC (Запись)**.

Умный поиск 1

Используйте Умный поиск 1, чтобы найти фрагменты записи, в которых движение происходило в заданной области.

Чтобы ускорить поиск, выберите **Include analytics data (Включать данные аналитики)** в настройках профиля потока. См. *Профили потоков*.

Чтобы использовать Умный поиск 1:

1. Щелкните значок + и откройте вкладку **Smart search 1 (Умный поиск 1)**.
2. Выберите камеру, которую требуется найти.
3. Настройте область детекции. К форме области можно добавить до 20 точек. Чтобы удалить точку, щелкните ее правой кнопкой мыши.
4. Используйте фильтры **Short-lived objects (Кратковременно появляющиеся объекты)** и **Small objects (Мелкие объекты)**, чтобы отфильтровать нежелательные результаты.
5. Выберите диапазон даты и времени для поиска. Удерживайте клавишу Shift, чтобы выбрать диапазон дат.
6. Нажмите **Поиск**.

Результаты поиска отобразятся на вкладке **Results (Результаты)**. Щелкните правой кнопкой мыши один или несколько результатов, чтобы экспортировать записи.

Фильтр Short-lived objects (Кратковременно присутствующие объекты)	Минимальное время, в течение которого объект должен находиться в области детекции, чтобы он был включен в результаты поиска.
Фильтр Small objects (Мелкие объекты)	Минимальный размер объекта, при котором он должен включаться в результаты поиска.

Умный поиск 1

Интеллектуальный поиск 2

Используйте умный поиск 2 для поиска движущихся людей и транспортных средств в записях.

Примечание

Для использования функции умного поиска 2 требуется следующее:

- Потоковая передача метаданных аналитики по протоколу RTSP.
- AXIS Video Content Stream на камерах с ОС AXIS версии более ранней, чем 9.60. См. *Установка приложений для камер, on page 74*.
- Синхронизация времени между сервером AXIS Camera Station Pro и камерами.

При включении Умного поиска 2 для камеры Axis AXIS Camera Station Pro начинает записывать метаданные с этой камеры и использовать их для классификации объектов в сцене. Это позволяет использовать фильтры для поиска интересующих объектов.

Примечание

- Рекомендуется использовать непрерывную запись, поскольку при обнаружении движения могут возникать обнаружения без видеозаписи.
- Используйте формат H.264, если необходимо просматривать записи в результатах поиска.
- Для оптимальной классификации цветов убедитесь, что условия освещения соответствуют техническим характеристикам камеры. При необходимости используйте дополнительное освещение.

Последовательность операций

1. *Настройка «Умного поиска 2», on page 183*
2. Настройка синхронизации времени между сервером AXIS Camera Station Pro и камерами. См. *Синхронизация времени, on page 79*.
3. Создайте фильтр или загрузите существующий фильтр. См. *Поиск с помощью фильтров, on page 39*.
4. Работа с результатами поиска. См. *Результаты умного поиска, on page 44*.

Поиск с помощью фильтров

1. Перейдите к пункту **Configuration > Smart search 2 > Settings (Конфигурация > Умный поиск 2 > Настройки)** и выберите камеры, которые требуется использовать в умном поиске 2.
2. Щелкните значок + и откройте вкладку **Smart search 2 (Умный поиск 2)**.
3. Определите критерии поиска.
4. Нажмите **Поиск**.

Если поиск занимает больше времени, чем ожидалось, попробуйте выполнить одно или несколько следующих действий для его ускорения:

- Включите фоновую классификацию на сервере для важных или часто используемых камер.
- Примените для камер входящие фильтры, чтобы уменьшить количество нерелевантных обнаружений.
- Сократите временной диапазон поиска.
- Уменьшите количество камер, на которых выполняется поиск.
- Задайте область, направление движения объекта, размер и продолжительность, чтобы сократить объем данных.

Камеры	Чтобы ограничить поиск по камере, щелкните **Cameras (Камеры)** и выберите камеры, которые требуется включить в поиск.
Интервал поиска	Чтобы ограничить поиск по времени, нажмите **Search interval (Интервал поиска)** и выберите диапазон времени, конкретный временной интервал за несколько дней или создайте пользовательский интервал.
Человек	Чтобы обнаружить людей, щелкните **Object characteristics** > **Pre-classified (Характеристики объекта > Предварительно классифицированные**, выберите **Person (Человек)** и цвета одежды. Можно выбрать несколько цветов.
Автомобиль	Чтобы обнаружить транспортные средства, щелкните **Object characteristics** > **Pre-classified (Характеристики объекта > Предварительно классифицированные)** и выберите тип и цвет автомобиля. Можно выбрать несколько типов и цветов транспортных средств.
Визуальное сходство	Можно использовать изображение для поиска визуально похожих людей. Откройте контекстное меню в пункте результата поиска и выберите **Use as visual similarity reference (Использовать для поиска визуально похожего человека)**. Затем нажмите **Search (Поиск)**. Примечание Поиск по сходству создает абстрактные представления на основе обрезанных изображений людей с низким разрешением и сравнивает их с другими представлениями. Если два представления сходны, соответствующий объект отображается в результатах поиска. При поиске по сходству биометрические данные не используются для идентификации человека; например, система может распознавать общую форму человека и цвет его одежды.
Поиск произвольного текста	Полнотекстовый поиск позволяет описать на естественном языке, что необходимо найти в записях (только на английском языке). См. *Поиск произвольного текста, on page 42*.
Область	Для выполнения фильтрации по области, щелкните **Area (Область)**, выберите камеру и включите параметр **Filter by area on this camera (Фильтрация по области на этой камере)**. Отрегулируйте область детекции на изображении и добавьте или удалите точки, если необходимо.
Пересечение линии	Для фильтрации по пересечению линии нажмите **Line crossing (Пересечение линии)**, выберите камеру и включите **Filter by line crossing on this camera (Фильтровать по пересечению линии на этой камере)**. Измените положение линии на

	изображении и при необходимости добавьте или удалите точки.
Объем	Для фильтрации по размеру нажмите **Size (Размер)**, выберите камеру и включите **Filter by size on this camera (Фильтровать по размеру на этой камере)**. Задайте минимальную высоту и ширину объекта в процентах от общих размеров изображения.
Длительность	Для выполнения фильтрации по длительности, щелкните **Duration (Длительность)**, выберите камеру и включите параметр **Filter by duration on this camera (Фильтрация по длительности на этой камере)**. Задайте минимальную длительность в секундах.
Скорость	Для фильтрации по скорости нажмите **Speed (Скорость)**, выберите камеру и включите **Filter by speed on this camera (Фильтровать по скорости на этой камере)**. Укажите диапазон скорости, который необходимо включить в фильтр. Примечание Фильтр по скорости доступен для радаров и фьюжн-камер, поддерживающих обнаружение скорости.
Обнаружения неизвестных объектов	Для включения обнаружений, которые умный поиск 2 классифицирует как неизвестные, выберите **Object characteristics (Характеристики объекта)**, а затем **Unknown object detections (Обнаружения неизвестных объектов)**.
	Чтобы сохранить фильтр, нажмите , введите имя фильтра и нажмите **Save (Сохранить)**. Нажмите **Share with other users (Поделиться с другими пользователями)**, чтобы сделать фильтр доступным для других пользователей. Чтобы заменить существующий фильтр, нажмите , выберите существующий фильтр и нажмите **Replace (Заменить)**.

	Чтобы загрузить результаты недавнего поиска, нажмите > **Recent searches (Недавний поиск)** и выберите поиск. Для загрузки сохраненного фильтра нажмите > **Saved filters (Сохраненные фильтры)** и выберите фильтр. Для загрузки фильтра, предоставленного другим пользователем, нажмите > **Shared filters (Совместно используемые фильтры)** и выберите фильтр.
	Чтобы сбросить фильтр, щелкните , а затем нажмите **Reset (Сброс)**.

Поиск произвольного текста

Полнотекстовый поиск позволяет описать на естественном языке, что необходимо найти в записях.

Примечание

- Для поиска произвольного текста требуется не менее 16 ГБ ОЗУ.
- Для поиска произвольного текста требуется подключение к Интернету.
  - При первоначальной настройке полнотекстовый поиск использует подключение к Интернету для загрузки модели ИИ с сайта axis.com, а также при обновлении модели компанией Axis.
  - Функция поиска произвольного текста раз в неделю подключается к облачным сервисам Axis и проверяет, нужно ли обновить модели ИИ для выполнения норм и требований, которые скоро вступят в силу. В случае неудачной попытки подключения вы не сможете использовать поиск произвольного текста, пока система снова не установит подключение.
  - Полнотекстовый поиск выполняет всю обработку локально на сервере и **не** использует подключение к Интернету для передачи видео, изображений или текстов запросов.

Чтобы включить функцию поиска произвольного текста:

1. Откройте вкладку **Configuration (Конфигурация)**.
2. Выберите **Smart search 2 (Умный поиск 2)** > **Settings (Параметры)**.
3. Под надписью Free text search (Поиск произвольного текста) выберите **Use free text search (Использовать поиск произвольного текста)**. Система загрузит нужные файлы с сайта axis.com.

Для поиска:

1. Откройте вкладку **Smart search 2 (Умный поиск 2)**.
2. Щелкните **Object characteristics (Характеристики объекта)**.
3. Щелкните **Free text (Произвольный текст)**.
4. Щелкните **Show (Показать)**, чтобы ознакомиться с информацией о назначении, ограничениях и ответственном использовании.
5. Выберите элементы, которые нужно включить в поиск/исключить из поиска.
6. Нажмите **Поиск**.

Инструкции по составлению поисковых запросов

Мы рекомендуем использовать для запросов следующий формат:

`{person, vehicle or other object} + {specific action or attributes of the person, vehicle, or object}`

Опишите объект с помощью нескольких ключевых признаков. Например:

Запрос	Комментарий
Женщина в красном свитере и черной шапке	Правильно
Женщина в красном	Слишком расплывчато
Женщина ростом 156 см в бордовом кардигане с желтыми вставками и черной панаме с коричневой каймой в стиле конца 80-х	Слишком подробно

Опишите ситуацию так, как если бы вы рассказывали о ней человеку, не имеющему опыта в области видеонаблюдения. Например:

Запрос	Комментарий
Желтый пикап, припаркованный у дерева	Правильно
Беспилотное транспортное средство, номерной знак: CHY67F, класс: пикап, цвет: желтый, положение: рядом с высоким тополем.	Похоже на полицейский отчет

Ключевые слова, которые функция поиска произвольного текста с большой вероятностью сможет понять:

Ключевое слово	Пример
object_class	Человек, автомобиль, велосипед, животное
Цвет	Желтый
Погода	Солнечный
Известные бренды (марки автомобилей, логотипы)	Грузовик службы UPS

Плохие ключевые слова:

Ключевое слово	Пример
Текст	Вывеска магазина с надписью «Вход танцующим медведям запрещен»
Воспринимаемые эмоции	Сердитый мужчина
Подсчет	14 человек слоняются на площади
Региональный жаргон	Красный пылесос

Модерация поисковых запросов

Поисковые запросы, содержащие оскорбительные, опасные или недоброжелательные выражения, могут быть заблокированы для сохранения безопасной и уважительной среды. Для анализа каждого поискового запроса наша система использует модель обработки естественного языка и специальный список запрещенных категорий и слов.

Если вы не согласны с блокировкой слова или хотите предложить новое слово, можно отправить анонимный отзыв через пользовательский интерфейс интеллектуального поиска. Отзыв будет передан нашей команде для рассмотрения.

Примечание

- Функция поиска произвольного текста поддерживает только английский язык.
- Функция поиска произвольного текста понимает статические изображения. Для таких действий, как падение, бег или кража, получить точные результаты может быть сложно, поскольку для их распознавания требуется дополнительный контекст.
- Полнотекстовый поиск использует обрезанные изображения, которые могут не содержать окружающую обстановку. Результаты могут быть менее точными при использовании таких ключевых слов, как город, городской, парк, сад, озеро или пляж.
- Более подробную информацию о функции полнотекстового поиска, включая ее ограничения и рекомендации по использованию, см. в нашем информационном документе *Free-text search in AXIS Camera Station Pro.*

Результаты умного поиска

	Чтобы сгруппировать обнаруженные объекты, которые, вероятно, относятся к одному событию, объедините их по временным интервалам. Выберите интервал из раскрывающегося меню .
Самый последний	Умный поиск 2 отображает результаты поиска в порядке убывания, начиная с последних обнаружений. Выберите **Earliest first (Самые ранние)**, чтобы отобразить вначале самые старые обнаружения.
Confidence level (Уровень достоверности)	Для дополнительной фильтрации результатов поиска нажмите **Confidence level (Уровень достоверности)** и задайте степень доверия к результатам. Высокий уровень достоверности позволяет отфильтровать классификации с низкой степенью уверенности.
Столбцы	Чтобы настроить размер миниатюрных изображений в результатах поиска, нажмите **Columns (Столбцы)** и измените количество столбцов.
Вид Detection (Обнаружение)	Чтобы отображать обрезанное изображение обнаруженного объекта в виде эскиза, выберите **Detection view (Представление обнаружения)**.

Ограничения

- Функция "Умный поиск 2" поддерживает только основную (не обрезанную) зону просмотра.
- Функция "Умный поиск 2" поддерживает только режимы съемки без кадрирования.
- Использование функции "Умный поиск 2" с зеркальными и повернутыми потоками камер для устройств с ARTPEC-7 или выше и версией прошивки ниже 10.6 может вызвать некоторые проблемы.

- Высокая или существенно меняющаяся сетевая задержка может вызывать проблемы с синхронизацией времени и влиять на классификацию объектов, обнаруживаемых на основе метаданных аналитики.
- Точность классификации объектов по типу и точность обнаружения объектов ухудшаются, если качество изображения будет низким, например, из-за высокого уровня сжатия, плохих погодных условий (сильный дождь, снег и т. п.), а также низкого разрешения камеры, сильных искажений, большой области обзора камеры или чрезмерных вибраций.
- При использовании умного поиска 2 могут не обнаруживаться мелкие и удаленные объекты.
- Классификация по цвету не будет работать в темноте или с ИК-подсветкой.
- Нательные камеры не поддерживаются.
- Радар обнаруживает только людей и другие транспортные средства. Включить фоновую классификацию на сервере для радара невозможно.
- Результаты классификации объектов для тепловизионных камер могут быть непредсказуемыми.
- Умный поиск 2 не обнаруживает движущиеся объекты при изменении предустановленной позиции PTZ и в течение короткого периода после ее изменения.
- После изменения положения PTZ фильтры на основе пересечения линии и области не перенастраиваются соответствующим образом автоматически.

Поиск данных

Поиск данных позволяет находить данные из внешнего источника. Источник — это система или устройство, генерирующее данные о событиях. Для получения дополнительных сведений см. *Внешние источники данных, on page 78*.
Например:

- Событие, инициируемое системой контроля доступа.
- Номерной знак, считанный приложением AXIS License Plate Verifier.
- Скорость, зафиксированная AXIS Speed Monitor.

Чтобы изменить срок хранения внешних данных в AXIS Camera Station Pro, перейдите в **Configuration (Конфигурация) > Server (Сервер) > Settings (Настройки) > External data (Внешние данные)**.

Чтобы выполнить поиск данных:

1. Щелкните + и выберите **Data search (Поиск данных)**.
2. Выберите интервал поиска .
3. Выберите источник данных из раскрывающегося списка.
4. Нажмите **Search options (Параметры поиска)** и примените дополнительные фильтры. Доступные фильтры зависят от типа источника данных.
5. Введите подходящие ключевые слова в поле поиска. См. *Оптимизация поиска, on page 47*.
6. Нажмите **Поиск**.

Средство поиска данных добавляет закладки к данным, сгенерированным из источника, если настройка осуществлялась вами с использованием вида. Щелкните требуемый элемент данных в списке, чтобы перейти к записи, связанной с событием.

Временной интервал	
Live (Живой)	Чтобы выполнить поиск данных в режиме реального времени, выберите в качестве интервала **Live (Живой)**. При поиске данных могут отображаться не более 3000 событий в режиме живого просмотра. Режим живого просмотра времени не поддерживает операторы поиска.
Последний час – последние 30 дней	Для поиска данных за предустановленный период времени выберите один из доступных вариантов: последний час, 4 часа, 12 часов, 24 часа, 48 часов, 7 дней или 30 дней.
Настраиваемая	Для поиска данных за определенный период выберите **Custom (Пользовательские)** и задайте дату и время начала и окончания.

Результаты поиска можно фильтровать по типам источников:

Тип источника данных	
All data (Все данные)	Этот параметр включает данные как из внутренних компонентов, так и из внешних источников.

Контроль доступа	Используйте этот параметр, чтобы включить данные только из этого компонента. Функция контроля доступа позволяет фильтровать события по дверям, зонам, владельцам карт и типам событий.
Third-party (Сторонние)	Используйте этот параметр, чтобы включить данные из сторонних источников, отличных от настроенных компонентов.

В зависимости от источника данных в результатах поиска могут отображаться разные элементы. Например:

Результаты поиска	
Сервер	Сервер, на который отправляются данные о событиях. Отображается только при подключении к нескольким серверам.
Место расположения	Имя двери и имя дверного сетевого контроллера с IP-адресом.
Enter speed (Введите скорость)	Скорость (в километрах или милях в час), при которой объект входит в зону обнаружения движения радаром (RMD).
Классификация	Классификация объекта. Например: Vehicle (Транспортное средство).

Чтобы экспортировать результаты поиска в файл PDF или в текстовый файл, щелкните **Download search result (Загрузить результат поиска)**. Можно изменить порядок столбцов и их ширину, чтобы улучшить представление таблицы в выходном PDF-файле. Файл PDF содержит до 10 столбцов.

Оптимизация поиска

Для получения более точных результатов можно использовать следующие операторы поиска:

Для фиксации только точных совпадений, заключите ключевые слова в кавычки `" "`.	• Поиск по запросу `"door 1"` возвращает результаты, содержащие "door 1". • Поиск по запросу `door 1` возвращает результаты, содержащие и "door", и "1".
Используйте оператор `AND`, чтобы находить совпадения, содержащие все ключевые слова.	• Поиск по запросу `door AND 1` возвращает результаты, содержащие и "door", и "1". • Поиск по запросу `"door 1" AND "door forced open"` возвращает результаты, содержащие и "door 1", и "door forced open".
Используйте оператор `OR` либо `|`, чтобы искать совпадения, содержащие любое ключевое слово.	• Поиск по запросу `"door 1" OR "door 2"` возвращает результаты, содержащие "door 1" или "door 2". • Поиск по запросу `door 1 OR door 2` возвращает результаты, содержащие "door" или "1" или "2".
Используйте круглые скобки `( )` с оператором `AND` или `OR`.	• Поиск по запросу `(door 1 OR door 2) AND "Door forced open"` возвращает результаты, содержащие одно из следующих значений: – "door 1" и "door forced open"

	– “дверь 2" и "Дверь открыта силой" • Поиск по запросу `door 1 AND (door (forced open OR open too long))` возвращает результаты, содержащие одно из следующих значений: – "door 1" и "door forced open" – "door 1" и "door open too long"
Используйте >, >=, <или <= для фильтрации числовых значений в определенном столбце.	• Поиск по запросу `[Max speed] > 28` возвращает результаты, содержащие в столбце Max speed значение, превышающее 28. • Поиск по запросу `[Average speed] < = 28` возвращает результаты, содержащие в столбце Average speed значение, меньшее или равное 28.
Используйте оператор `CONTAINS` для поиска текста в конкретном столбце.	• Поиск по запросу `[Cardholder] CONTAINS Oscar` возвращает результаты, содержащие "Oscar" в столбце Cardholder (Владелец карты). • Поиск по запросу `[Door] CONTAINS "door 1"` возвращает результаты, содержащие "door 1" в столбце Door (Дверь).
Используйте оператор = для поиска точных совпадений в конкретном столбце.	Поиск по запросу `[CardholderId] = ABC123` возвращает результаты, соответствующие значению «ABC123», только в столбце Cardholder.

Конфигурация

На вкладке Configuration (Конфигурация) можно управлять подключенными устройствами и настраивать параметры клиента и серверов. Нажмите + и выберите **Configuration (Конфигурация)**, чтобы открыть вкладку **Configuration (Конфигурация)**.

Настроить устройства

В AXIS Camera Station Pro термин «устройство» означает сетевое устройство с IP-адресом. Термин «камера» означает источник видео, такой как сетевая камера или видеопорт (с подключенной аналоговой камерой) многопортового видеокодера. Например, 4-портовый видеокодер представляет собой одно устройство с четырьмя камерами.

Примечание

- AXIS Camera Station Pro поддерживает только устройства с IPv4-адресами.
- Некоторые видеокодеры имеют по одному IP-адресу на каждый видеопорт. В этом случае AXIS Camera Station Pro рассматривает каждый видеопорт как одно устройство с одной камерой.

В AXIS Camera Station Pro могут использоваться следующие устройства:

- Сетевая камера.
- Видеокодер с одним или несколькими видеопортами.
- Вспомогательное устройство, не являющееся камерой, например устройство ввода-вывода, сетевой динамик или дверной контроллер.
- Переговорное устройство.

Здесь можно:

- Добавить камеры и устройства, не имеющие возможностей видеосъемки. См. *Добавить устройства*.
- Изменить настройки подключенных камер. См. *Камеры*.
- Изменить настройки устройств, которые не являются камерами. См. *Другие устройства*.
- Изменять профили потоков, включая разрешение, формат и другие параметры. См. *Профили потоков*.
- Внести изменения в настройки изображения в режиме реального времени. См. *Конфигурация изображения*.
- Добавить или удалить предустановленные положения PTZ. См. *Предварительные установки PTZ*.
- Управление и обслуживание подсоединенных устройств. См. *Управление устройствами*.
- Создавать внешние источники данных. См. *Внешние источники данных, on page 78*.

Добавить устройства

Примечание

- Зоны просмотра рассматриваются системой как отдельные камеры. Прежде чем использовать область наблюдения, ее надо создать в камере. См. *Использование зон просмотра*.
- При добавлении устройства его время синхронизируется с сервером AXIS Camera Station Pro.
- Не рекомендуется использовать в имени хоста специальные символы, например å, ä или ö.

1. Найдите устройства, видеопотоки или предварительно записанные видеозаписи.
   - *Поиск устройств, on page 51*
   - *Поиск видеопотоков, on page 52*
   - *Поиск предварительно записанных видеозаписей, on page 52*
2. *Добавление устройств, видеопотоков или предварительно записанных видеозаписей, on page 52*

Перед добавлением устройства необходимо устранить все проблемы, отображаемые в столбце состояния устройства.

(пусто)	Если состояние отсутствует, устройство можно добавить в AXIS Camera Station Pro.
Communicating (Обмен данными)	Сервер AXIS Camera Station Pro пытается получить доступ к устройству.
Недоверенный сертификат устройства	AXIS Camera Station Pro не может проверить, что HTTPS-сертификат устройства подписан доверенным центром сертификации. Нажмите на ссылку, чтобы выпустить новый сертификат HTTPS, или укажите AXIS Camera Station Pro, чтобы доверять существующему.
Закончился срок действия полномочий на сертификацию	Удостоверяющий центр, выдавший сертификат устройства, больше не считается действительным. Нажмите на ссылку, чтобы выпустить новый сертификат HTTPS, или укажите AXIS Camera Station Pro, чтобы доверять существующему.
Несоответствие адреса в сертификате устройства	Адрес устройства не совпадает с адресом, указанным в сертификате. Нажмите на ссылку, чтобы выпустить новый сертификат HTTPS, или укажите AXIS Camera Station Pro, чтобы доверять существующему.
Ошибка связи	AXIS Camera Station Pro не удается установить связь с устройством.
Введите пароль	AXIS Camera Station Pro не знает, какие учетные данные использовать для доступа к устройству. Перейдите по ссылке, чтобы ввести имя пользователя и пароль учетной записи администратора на устройстве. По умолчанию AXIS Camera Station Pro будет использовать введенные имя пользователя и пароль на всех устройствах, где существует такой пользователь.
Set password (Установите пароль):	Учетная запись root и пароль не настроены либо на устройстве по-прежнему используется пароль по умолчанию. Перейдите по ссылке, чтобы установить пароль для привилегированного пользователя. • Введите пароль или нажмите **Generate (Создать)**, чтобы сгенерировать пароль. Рекомендуется сохранить копию сгенерированного пароля. • Установите этот флажок, чтобы использовать данный пароль для всех устройств со статусом `Set password` (Задать пароль). • Если на устройстве действует политика паролей, индикатор политики паролей показывает, соответствует ли пароль ее требованиям. Дополнительные сведения см. в разделе *Управлять пользователями, on page 71*.

Модель не поддерживается	AXIS Camera Station Pro не поддерживает данную модель устройства.
Устаревшая прошивка	Встроенное ПО устройства устарело. Обновите его перед добавлением устройства.
Неисправное устройство	Параметры устройства, полученные приложением AXIS Camera Station Pro, повреждены.
Установка ориентации по наклону	Перейдите по ссылке, чтобы выбрать ориентацию наклона: Ceiling (Потолок), Wall (Стена) или Desk (Стол) — в зависимости от способа установки камеры. В некоторых моделях камер необходимо осуществить настройки угла наклона.
Неподдерживаемое устройство ONVIF	AXIS Camera Station Pro не поддерживает это стороннее устройство.
Неподдерживаемое устройство	AXIS Camera Station Pro не поддерживает этот тип устройства.

Примечание

Новые сертификаты HTTPS выдаются AXIS Camera Station Pro и обновляются автоматически.

Поиск устройств

Чтобы найти устройства, которые не указаны в списке, выполните следующие действия.

1. Перейдите в **Configuration (Конфигурация)> Devices (Устройства)> Add devices (Добавить устройства)**.
2. Нажмите **Отмена**, чтобы остановить выполняемый в сети поиск.
3. Нажмите кнопку **Manual search (Поиск вручную)**.
4. Чтобы найти несколько устройств в одном или нескольких диапазонах IP-адресов:
   4.1. Выберите **Search one or more IP ranges (Поиск в одном или нескольких диапазонах IP-адресов)**.
   4.2. Введите диапазон IP-адресов. Например: 192.168.10.*, 192.168.20-22.*, 192.168.30.0-50
   - Используйте подстановочный знак для всех адресов в группе.
   - Используйте дефис для выбора диапазона адресов.
   - Для разделения нескольких диапазонов используйте запятую.

   4.1. Чтобы изменить порт 80, заданный по умолчанию, введите диапазон портов. Например: 80, 1080-1090
   - Используйте дефис для выбора диапазона портов.
   - Для разделения нескольких диапазонов используйте запятую.

   4.1. Нажмите **Поиск**.
5. Чтобы найти одно или несколько конкретных устройств:
   5.1. Выберите **Enter one or more hostnames or IP addresses (Ввести одно или несколько имен хостов или IP-адресов)**.
   5.2. Введите имена хостов или IP-адреса, разделяя их запятыми.
   5.3. Нажмите **Поиск**.
6. Нажмите кнопку **OK**.

Поиск видеопотоков

Можно добавлять видеопотоки, поддерживающие следующие параметры:

- Протокол: RTSP, HTTP, HTTPS
- Кодирование видеоизображения: M-JPEG для протоколов HTTP и HTTPS, H.264 для протокола RTSP
- Кодирование звука: AAC и G.711 для протокола RTSP

Поддерживаемые схемы URL-адресов видеопотоков:

- `rtsp://<address>:<port>/<path>`
  Например: `rtsp://<address>:554/axis-media/media.amp`
- `http://<address>:80/<path>`
  Например: `http://<address>:80/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`
- `https://<address>:443/<path>`
  Например: `https://<address>:443/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

1. Перейдите в **Configuration (Конфигурация)> Devices (Устройства)> Add devices (Добавить устройства)**.
2. Нажмите кнопку **Enter stream URLs (Ввести URL-адреса потоков)** и введите один или несколько URL-адресов потоков, разделяя их запятыми.
3. Нажмите **Добавить**.

Поиск предварительно записанных видеозаписей

В AXIS Camera Station Pro можно добавлять предварительно записанные видео в формате .mkv.

Особые требования:

- Кодирование видеоизображения: M-JPEG, H.264, H.265
- Кодирование звука: AAC

1. Создайте папку **PreecordedVideos** в папке `C:\ProgramData\Axis Communications\AXIS Camera Station Server`.
2. Добавьте в папку файл в формате MKV.
3. Чтобы компенсировать оптические искажения в предварительно записанном видео, добавьте в папку файл с расширением .dewarp и с таким же именем, как у файла MKV. Для получения дополнительных сведений см. *Конфигурация изображения, on page 63*.
4. Перейдите к пункту **Configuration > Devices > Add devices (Конфигурация > Устройства > Добавить устройства)** и включите параметр **Include prerecorded video (Добавить видеозаписи)**. Вы можете выполнять поиск видеозаписей в зависимости от типа используемой системы.

Добавление устройств, видеопотоков или предварительно записанных видеозаписей

1. В мультисерверной системе выберите сервер из раскрывающегося списка **Selected server (Выбранный сервер)**.
2. Перейдите в **Configuration (Конфигурация)> Devices (Устройства)> Add devices (Добавить устройства)**.
3. Выберите устройства, видеопотоки или предварительно записанное видео. Нажмите **Добавить**.
4. Нажмите **Close (Закрыть)**, чтобы пропустить настройку и выполнить ее позже. Чтобы продолжить настройку:
   4.1. Выберите **Quick configuration (Быстрая настройка)**, чтобы настроить основные параметры. Если вы импортируете проект AXIS Site Designer, выберите **Site Designer**

configuration (Конфигурация Site Designer). Для получения дополнительных сведений см. *Импорт проектов AXIS Site Designer*.

4.2. Выберите **Add image overlay (Добавить наложение изображения)**, чтобы добавить на камеры Axis наложения с датой, временем и текстом, если они еще не добавлены.

4.3. Нажмите **Next (Далее)**.

4.4. Выберите предпочтительный режим записи **Recording method**.

4.5. Нажмите **Next (Далее)**.

4.6. Выберите **Retention time (Срок хранения)** и **Recording storage (Хранилище записей)**, затем нажмите **Finish (Готово)**, чтобы применить конфигурацию.

Импорт проектов AXIS Site Designer

AXIS Site Designer представляет собой интерактивное средство разработки, помогающее создать объект, оснащенный устройствами Axis вместе с соответствующими принадлежностями.

Создав объект в AXIS Site Designer, вы можете импортировать настройки проекта в AXIS Camera Station Pro. Доступ к проекту можно получить с помощью кода доступа или загруженного файла установки.

Чтобы импортировать проект AXIS Site Designer в AXIS Camera Station Pro:

1. Сгенерируйте код доступа или загрузите файл проекта:
   1.1. Войдите на *http://sitedesigner.axis.com* с помощью учетной записи My Axis.
   1.2. Выберите проект и перейдите на страницу проекта.
   1.3. Нажмите **Share (Общий)**.
   1.4. Нажмите **Generate code (Создать код)**, если сервер AXIS Camera Station Pro подключен к Интернету, или **Download settings file (Загрузить файл настроек)**, если подключение отсутствует.
2. В клиенте AXIS Camera Station Pro перейдите к пункту **Configuration > Devices > Add devices (Конфигурация > Устройства > Добавить устройства)**.
3. Выберите устройства и нажмите **Add (Добавить)**.
4. Выберите **Конфигурация Site Designer** и нажмите **Далее**.
5. Выберите **Код доступа** и введите этот код. Чтобы использовать загруженный файл установки, выберите **Choose file (Выбрать файл)**.
6. Нажмите **Import (Импортировать)**. AXIS Camera Station Pro пытается сопоставить проект с выбранными устройствами по IP-адресу или названию продукта. Если сопоставить устройства не удалось, выберите нужные устройства в раскрывающемся списке.
7. Нажмите **Next (Далее)**.
8. Выберите предпочтительный режим записи **Recording method**. Эти настройки применяются к камерам, конфигурация которых не соответствует проекту.
9. Нажмите **Next (Далее)**.
10. Выберите **Retention time (Срок хранения)** и **Recording storage (Хранилище записей)**, затем нажмите **Finish (Готово)**, чтобы применить конфигурацию.

AXIS Camera Station Pro импортирует из проекта AXIS Site Designer следующие настройки:

	Кодеры, видеодекодеры, дверные контроллеры, радар-детекторы и громкоговорители	Камеры, переговорные устройства и устройства серии F/FA
Расписания с именем и периодами времени	✓	✓
Карты с именем, цвет значка, расположение значка и имя элемента	✓	✓
Название	✓	✓
Описание	✓	✓
Непрерывная запись: расписание и профиль записи, включая параметры частоты кадров, разрешения, кодирования видео и сжатия		✓
Запись с активацией по движению: расписание и профиль записи, включая параметры частоты кадров, разрешения, кодирования видео и сжатия		✓
Степень сжатия по технологии Zipstream		✓
Настройки звука для живого просмотра и записей		✓
Срок хранения записей		✓

Примечание

- Если в проекте AXIS Site Designer задан один из профилей записи или определены два одинаковых профиля записи, AXIS Camera Station Pro устанавливает для профиля значение Medium (Средний).
- Если в проекте AXIS Site Designer заданы оба профиля записи, AXIS Camera Station Pro устанавливает для непрерывной записи значение Medium (Средний), а для записи по детектору движения — High (Высокий).
- AXIS Camera Station Pro оптимизирует соотношение сторон, поэтому разрешение может отличаться от указанного в проекте AXIS Site Designer.
- AXIS Camera Station Pro может задать настройки аудио, если устройство оснащено встроенным микрофоном или динамиком. Чтобы использовать внешнее аудиоустройство, включите его после установки.
- AXIS Camera Station Pro не применяет настройки аудио к переговорным устройствам, даже если настройки в AXIS Site Designer отличаются. На переговорных устройствах аудио всегда включено, но только в режиме живого просмотра.

Добавление устройств сторонних производителей

Устройства сторонних производителей можно добавить в AXIS Camera Station Pro таким же образом, как и устройства Axis. См. *Добавить устройства*.

Примечание

Устройства сторонних производителей можно также добавлять в AXIS Camera Station Pro в качестве видеопотоков. См. *Поиск видеопотоков, on page 52*.

AXIS Camera Station Pro поддерживает следующие функции сторонних устройств в соответствии с IEC 62676-2-31 и IEC 62676-2-32:

- Обнаружение камер
- Кодирование видеоизображения: M-JPEG, H.264
- Кодирование звука: G.711 (однонаправленный, от устройства к AXIS Camera Station Pro)
- Один профиль видео на камеру
- Просмотр в реальном времени
- Непрерывная запись и запись в ручном режиме
- Воспроизведение
- Экспорт записей
- Триггеры событий на устройстве
- PTZ-камера

Использование зон просмотра

Некоторые модели камер поддерживают зоны просмотра. В AXIS Camera Station Pro зоны просмотра перечислены на странице **добавления устройств** как отдельные камеры. См. *Добавить устройства*.

Примечание

- Все области обзора в сетевой камере учитываются как одна камера в общем количестве камер, разрешенном лицензией AXIS Camera Station Pro.
- Количество камер, которые можно добавить, зависит от лицензии.

Чтобы использовать области обзора в AXIS Camera Station Pro, сначала включите их в камере:

1. Перейдите в меню **Конфигурация > Устройства > Камеры**.
2. Выбрав камеру, перейдите по ссылке в столбце «Адрес».
3. На странице конфигурации камеры введите имя пользователя и пароль для входа в систему.
4. Нажмите **Help (Справка)**, чтобы получить инструкции о расположении этого параметра. Расположение параметра зависит от модели камеры и версии встроенного ПО.

Замена устройства

Можно заменить устройство с сохранением существующей конфигурации и записей. Количество настроенных видеопотоков на новой камере должно совпадать с количеством видеопотоков на старой камере.

Для замены устройства:

1. Если заменяемое устройство использует облачное хранилище, откройте **Cloud storage (Облачное хранилище)** в My Systems и отключите для устройства облачное хранилище.
2. Откройте вкладку **Configuration (Настройка)** и выберите **Devices (Устройства)** > **Management (Управление)**.
3. Выберите устройство, которое необходимо заменить, после чего нажмите .

4. В диалоговом окне **Replace device (Замена устройств)** выберите устройство для замены старого устройства.
5. Нажмите **Finish** ("Завершить").
6. Появится диалоговое окно **Replaced device (Замененное устройство)** с подтверждением успешной замены устройства. Нажмите кнопку **OK**.
7. Если на замененном устройстве использовалось облачное хранилище, перезапустите службу на сервере AXIS Camera Station Pro. Затем включите облачное хранилище для устройства в разделе My Systems (Мои системы). См. *Включение облачного хранилища для отдельных камер*.
8. Проверьте конфигурацию нового устройства, чтобы убедиться в правильности настроек и нормальной работе устройства. Если нужно,
   8.1. Измените настройки предустановки PTZ на устройстве.
   8.2. Добавьте все удаленные порты ввода-вывода и обновите соответствующие правила действий.
   8.3. Измените настройки параметров движения, если старая камера использовала встроенный видеодетектор движения вместо приложения видеодетектора движения ACAP.
   8.4. Вставьте SD-карту или отключите **Failover recording (Резервная запись)** в настройках выбора хранилища, если старая камера использовала резервную запись.

Камеры

Перейдите в **Configuration (Конфигурация) > Devices (Устройства) > Cameras (Камеры)**, чтобы просмотреть список всех камер, добавленных в систему.

На этой странице можно сделать следующее:

- Нажмите адрес камеры, чтобы открыть ее веб-интерфейс. Для этого требуется, чтобы между клиентом AXIS Camera Station Pro и устройством не было NAT или межсетевого экрана.
- Изменение настроек параметров камеры. См. *Изменение настроек камеры*.
- Удалите камеры. При этом также удаляются все записи, связанные с удаленными камерами, в том числе защищенные от удаления.

Изменение настроек камеры

Чтобы изменить настройки камеры:

1. Перейдите в меню **Конфигурация > Устройства > Камеры**.
2. Выбрав камеру, нажмите **Изменить**.

Включено	Чтобы запретить запись и просмотр видеопотока, снимите флажок **Enabled (Включено)**. Вы по-прежнему можете настраивать запись и режим живого просмотра.
Канал	Если для многопортовых видеокодеров доступно поле **Channel (Канал)**, выберите номер порта. Если для зон просмотра доступно поле **Channel (Канал)**, выберите номер, соответствующий данной зоне просмотра.

Другие устройства

Перейдите в **Configuration (Конфигурация) > Devices (Устройства) > Other devices (Другие устройства)**, чтобы просмотреть список устройств без функций видеонаблюдения. В данный список входят дверные контроллеры, звуковые устройства и модули ввода-вывода.

Сведения о поддерживаемых продуктах см. на *www.axis.com*. См. *Использование аудиосигнала с других устройств*.

На этой странице можно сделать следующее:

- Щелкните адрес устройства, чтобы открыть его веб-интерфейс. Для этого требуется, чтобы между клиентом AXIS Camera Station Pro и устройством не было NAT или межсетевого экрана.
- Измените настройки устройства, такие как его имя, адрес и пароль.
- Удаление устройств.

Изменение других настроек устройства

Чтобы изменить название устройства, не являющегося камерой:

1. Откройте меню **Конфигурация > Устройства > Другие устройства**.
2. Выбрав устройство, нажмите **Изменить**.
3. Введите новое название устройства.

Профили потоков

Профиль потока представляет собой группу настроек, влияющих на видеопоток, таких как разрешение, формат видео, частота кадров и сжатие. Перейдите в **Configuration (Конфигурация) > Devices (Устройства) > Stream profiles (Профили потоков)**, чтобы открыть страницу **Stream profiles (Профили потоков)**. На странице отображается список всех камер.

В режиме живого просмотра и в настройках записи доступны следующие профили:

Высокая – Оптимальный вариант для наивысшего качества и разрешения.

Средняя – Вариант с оптимальным соотношением высокого качества и производительности.

Низкая – вариант для оптимальной производительности.

Примечание

По умолчанию для живого просмотра и записей установлен профиль потока **Automatic (Автоматически)**. Профиль потока автоматически изменяется на **High (Высокий)**, **Medium (Средний)** или **Low (Низкий)** в зависимости от доступного объема видеопотока.

Просмотр профилей потоков на камере

AXIS Camera Station Pro автоматически добавляет профили потока в камеру, чтобы вы могли проводить настройку правил записи прямо на ней. Профили отображаются в веб-интерфейсе камеры в разделе **Stream profiles (Профили потоков)** и именуются по шаблону «имя камеры_уровень профиля», например Camera 1_ACS_Pro_High.

Профили в камере добавляются или обновляются в следующих случаях:

- Камера добавлена в систему AXIS Camera Station Pro.
- Профили потоков изменяются в разделе AXIS Camera Station Pro.
- Запускается ночное обновление системы.

При удалении камеры из AXIS Camera Station Pro профили потока, созданные AXIS Camera Station Pro, удаляются с камеры.

Примечание

Профили потока в форматах M-JPEG или MPEG-4 не добавляются в систему камеры.

Изменение профилей потока

1. Перейдите к пункту **Configuration > Devices > Streaming profiles (Конфигурация > Устройства > Профили потока)** и выберите камеры, которые требуется настроить.

2. В разделе **Video profiles (Профили видео)** настройте разрешение, формат видео, частоту кадров и сжатие.
3. В разделе **Audio (Звук)** настройте микрофон и громкоговоритель.
4. В разделе **Advanced (Дополнительно)** настройте аналитические данные, потоковую передачу FFmpeg, индикаторы объектов автоматического слежения PTZ и индивидуальные настройки потока. Эти настройки доступны не для всех продуктов.
5. Нажмите **Применить**.

Видеопрофили

Видеокодер	• Доступные варианты зависят от настроек видеокодера на устройстве. Доступно только для устройств сторонних производителей. • Конфигурация видеокодера может использоваться только для одного профиля видео. • Если устройство имеет только одну конфигурацию кодера, доступным является только профиль **Medium (Средний)**.
Разрешение	Доступные варианты зависят от модели камеры. При более высоком разрешении изображение содержит больше деталей, но требуется большая пропускная способность сети и больше места на ресурсе хранения.
Формат	Доступные варианты зависят от модели камеры. Большинство камер поддерживают **H.264** и **M-JPEG**. H.264 требует меньше пропускной способности сети и места в хранилище, чем M-JPEG. Некоторые камеры также поддерживают **H.265**, обеспечивающий несколько более высокую степень сжатия, но требующий большей вычислительной мощности. Камеры последнего поколения поддерживают кодек AV1, обеспечивающий эффективное сжатие и ряд новых функций, в том числе включаемые и отключаемые накладки. Дополнительную информацию об AV1 см. на *странице продукта AV1*. Чтобы проверить, поддерживает ли ваша камера AV1, см. *страницу совместимых камер*.
Частота кадров	Фактическая частота кадров зависит от модели камеры, состояния сети и конфигурации компьютера.
Сжатие	При меньшей степени сжатия улучшается качество изображения, но требуется большая пропускная способность сети и больше места на ресурсе хранения.

Примечание

- Только камеры со встроенным ПО версии 5 и выше отображаются в выпадающих списках для аудио.
- Если более пяти камер используют один и тот же источник аудио, это может привести к перегрузке исходной камеры и снижению производительности.

Zipstream

Коэффициент сжатия	Уровень Zipstream определяет уровень снижения битрейта в потоке H.264 или H.265 в режиме реального времени. Этот параметр доступен только для устройств Axis, поддерживающих технологию Zipstream.	**По умолчанию**	Используйте параметр Zipstream, настроенный с помощью веб-интерфейса устройства.
		Off (Выкл.)	None (Нет)
		Низкая	По большей части без видимого эффекта.
		Средняя	Видимый эффект в отдельных сценах: меньше помех чуть хуже проработаны детали в областях не представляющих особого интереса.
		Высокая	Видимый эффект во многих сценах: меньше помех хуже проработаны детали в областях не представляющих особого интереса.
		Очень высокая	Преобладающий видимый эффект: меньше помех хуже проработаны детали в областях не представляющих особого интереса.
		Предельно высокая	Видимый эффект в большинстве сцен: меньше помех хуже проработаны детали в областях не представляющих особого интереса.

Оптимизировать для хранения данных	Технология Zipstream обеспечивает оптимизацию видеопотока для хранилища с помощью профиля **Optimize for storage (Оптимизировать для хранения данных)**. Этот профиль использует более современные средства сжатия для уменьшения объема данных в хранилище по сравнению с настройкой Zipstream по умолчанию и позволяет дополнительно снизить битрейт даже в сценах с высокой интенсивностью движения. • Формат ASF не поддерживает B-кадры, используемые этой функцией. • Эта функция не влияет на видеозаписи, сохраняемые на рекордерах серии AXIS S30. • Для работы этой функции требуется AXIS OS 11.7.59 или более поздней версии.		

Звук

Микрофон:	чтобы связать микрофон с камерой, выберите пункт **Built-in microphone or line in (Встроенный микрофон или линейный вход)** или микрофон другого устройства. См. *Использование аудиосигнала с других устройств*.
Динамик:	Чтобы связать громкоговоритель с камерой, выберите пункт **Built-in speaker or line out (Встроенный громкоговоритель или линейный выход)** или громкоговоритель другого устройства. Говорить при этом нужно в микрофон, подключенный к компьютеру. См. *Использование аудиосигнала с других устройств*.
Включать микрофон при работе в режимах:	Включите аудио с микрофона для одного или двух потоков. Можно включить аудио для просмотра в реальном времени и записей, только для просмотра в реальном времени или только для записей.

При подключении к AXIS Audio Manager Pro можно также выбрать аудиоустройства на сервере AXIS Audio Manager Pro в качестве аудиоустройства, связанного с камерой. Для получения дополнительной информации см. раздел *Настройка AXIS Audio Manager Pro, on page 183*.

Расширенный набор

Включить данные аналитики	Чтобы разрешить сбор данных для функции умного поиска при потоковой передаче видео, выберите **Include analytics data (Включить данные аналитики)**. Доступно только для устройств Axis, поддерживающих данные аналитики. Сбор данных для *Умный поиск 1* может замедлять передачу видеопотока при просмотре живого видео.
Использовать FFmpeg	Для повышения совместимости с устройствами сторонних производителей выберите **Use FFmpeg (Использовать FFmpeg)**, чтобы включить потоковую передачу FFmpeg. Доступно только для устройств сторонних производителей.

Показать индикаторы объектов функции автоматического слежения с помощью PTZ-камеры	Чтобы отображать в режиме просмотра в реальном времени индикаторы объектов, обнаруженных PTZ-камерой, выберите **Show PTZ autotracking object indicators (Показывать индикаторы объектов автоматического сопровождения PTZ)** и установите время буферизации видеопотока до 2000 мс. Доступно только для PTZ-камер Axis с поддержкой AXIS PTZ Autotracking. Полный порядок действий по настройке функции автоматического слежения с помощью PTZ-камеры в AXIS Camera Station Pro см. в разделе *Настройка автоматического слежения с помощью PTZ (AXIS PTZ Autotracking)*.
Настройка потока	Чтобы настроить параметры потока для определенного профиля, введите для этого профиля настройки, разделенные знаком `&`. Например, введите `overlays=off&color=0`, чтобы скрыть наложения на соответствующей камере. Пользовательские настройки переопределяют любые существующие настройки. Не указывайте конфиденциальную информацию в пользовательских настройках.

Чтобы **настроить в профиле** разрешение, частоту кадров, сжатие, формат видео и аудио для профиля, выберите настраиваемую камеру. Можно настроить сразу несколько камер одной модели с одинаковыми возможностями настройки. См. *Параметры конфигурации*.

Порядок индивидуальной настройки параметров профиля для записей см. *Способ записи*.

Разрешение и частоту кадров в режиме живого просмотра можно **ограничить для снижения нагрузки на сеть**, например если подключение между клиентом AXIS Camera Station Pro и сервером AXIS Camera Station Pro является медленным. Использование полосы пропускания описывается в разделе *Потоковая передача*.

Использование аудиосигнала с других устройств

Для живого просмотра или записи можно использовать аудио с других некамерных или вспомогательных устройств вместе с видео с сетевой камеры или видеокодера.

1. Добавьте дополнительное устройство (не камеру) в AXIS Camera Station Pro. См. *Добавить устройства*.
2. Настройте камеру на использование аудиосигнала с этого устройства. См. *Профили потоков*.
3. Включите аудио для живого просмотра или записи. См. *Профили потоков*.

Следующие примеры можно найти в *видеоруководствах AXIS Camera Station Pro*.

- Настройка звуковых устройств и живая трансляция объявлений.
- Создание кнопки действия для ручного воспроизведения звука при обнаружении движения.
- Автоматическое воспроизведение аудиоклипа при обнаружении движения.
- Добавление аудиоклипа в громкоговоритель и ПО AXIS Camera Station Pro.

Конфигурация изображения

Вы можете задать параметры изображения для камер, подключенных к AXIS Camera Station Pro.

Примечание

Изменения конфигурации изображения вступают в силу немедленно.

Чтобы настроить параметры изображения:

1. Перейдите в **Configuration (Конфигурация) > Devices (Устройства) > Image configuration (Конфигурация изображения)**. AXIS Camera Station Pro отображает список всех камер.
2. Выберите камеру, чтобы в режиме реального времени отображать видеопоток под списком. Чтобы найти нужную камеру в списке, воспользуйтесь полем **Ввести данные для поиска**.
3. Задайте нужные параметры изображения:

Яркость – Регулировка яркости изображения. Более высокие значения соответствуют более высокой яркости.

Уровень цветности – Регулировка насыщенности цвета. Выберите меньшее значение, чтобы уменьшить насыщенность цвета. Уровень цветности 0 соответствует черно-белому изображению. Максимальное значение соответствует максимальной насыщенности цвета.

Резкость – Регулировка уровня четкости, применяемого к изображению. Увеличение резкости может увеличивать уровень шума изображения, особенно при низкой освещенности. При высокой настройке резкости также возможно возникновение артефактов вокруг областей с высоким контрастом, например, у резких краев. При меньшей настройке резкости снижается уровень шума, однако изображение становится менее резким.

Контраст – Регулировка контраста изображения.

Баланс белого – В раскрывающемся списке выберите подходящий уровень баланса белого. Баланс белого используется для обеспечения постоянства цветов изображения независимо от цветовой температуры источника света. При выборе варианта **Автоматически** или **Авто** камера сама идентифицирует источник света и автоматически компенсирует его цветность. Если результат неудовлетворительный, выберите параметр, соответствующий типу источника света. Доступные варианты зависят от модели камеры.

Повернуть изображение – Регулировка поворота изображения в градусах.

Автоматический поворот изображения – Включите, чтобы автоматически отрегулировать поворот изображения.

Mirror image (Зеркальный образ). – Включите зеркальное отражение изображения.

Backlight compensation (Компенсация фоновой засветки) – Включите этот параметр, если яркий источник света, например лампа, приводит к слишком сильному затемнению других областей изображения.

Динамический контраст (Сверхширокий динамический диапазон) – Включите этот параметр для улучшения экспозиции при значительном контрасте между светлыми и темными областями изображения. Используйте ползунок для настройки уровня. Отключите этот параметр при слабом освещении.

Custom dewarp settings (Пользовательские настройки компенсации оптических искажений). – При необходимости можно импортировать файл с расширением .dewarp, который содержит параметры объектива, данные об оптических центрах и ориентации по наклону камеры. Нажмите кнопку **Reset (Сброс)**, чтобы восстановить исходные значения параметров.

Чтобы настроить пользовательские параметры компенсации оптических искажений:

1. Создание dewarp-файла, содержащего следующие параметры:
   - Требуется: `RadialDistortionX`, `RadialDistortionY`, `RadialDistortionZ` и `TiltOrientation`. Параметр `TiltOrientation` может иметь значение `wall`, `desk` или `ceiling`.
   - Дополнительно: `OpticalCenterX` и `OpticalCenterY`. Если хотите задать оптические центры, обязательно укажите значение обоих параметров.
2. Нажмите кнопку **Import (Импорт)** и перейдите к dewarp-файлу.

Ниже приведен пример dewarp-файла:

```
RadialDistortionX=-43.970703 RadialDistortionY=29.148499 RadialDistortionZ=715.732193
TiltOrientation=Desk OpticalCenterX=1296 OpticalCenterY=972
```

Предварительные установки PTZ

Поворот, наклон и зум (PTZ) — это возможность поворачивать камеру влево и вправо, наклонять ее вверх и вниз, а также увеличивать и уменьшать изображение.

Перейдите в **Configuration > Devices > PTZ presets (Конфигурация > Устройства > Предустановки PTZ)**. AXIS Camera Station Pro отображает список камер с поддержкой PTZ. Чтобы просмотреть все доступные для камеры предустановленные положения, щелкните камеру. Чтобы обновить список предустановленных положений, нажмите **Refresh (Обновить)**.

К таким камерам относятся:

- PTZ-камеры, т. е. камеры со встроенными механизмами панорамирования, наклона и зума (PTZ);
- Стационарные камеры с включенным цифровым PTZ.
- Камеры ONVIF с поддержкой предустановок PTZ.

Цифровой PTZ можно включить на встроенной странице конфигурации камеры. Дополнительную информацию см. в руководстве пользователя камеры. Чтобы открыть страницу конфигурации, перейдите на страницу управления устройствами, выберите камеру и нажмите ссылку в столбце **Address (Адрес)**.

Предустановленные положения для PTZ можно настроить в AXIS Camera Station Pro, а также на странице конфигурации камеры. Рекомендуется настраивать предустановки PTZ в AXIS Camera Station Pro.

- Если предустановленное положение для PTZ настроено на странице конфигурации камеры, то можно просматривать только изображение области, соответствующей предустановленному положению. Перемещения PTZ в режиме живого просмотра отображаются и записываются.
- Если предустановленное положение для PTZ настроено в AXIS Camera Station Pro, то можно просматривать полный видеопоток с камеры. Перемещения PTZ в режиме живого просмотра не отображаются и не записываются.

Примечание

PTZ нельзя использовать, когда включена очередь управления камерой. Информацию об очереди управления и ее включении и отключении см. в руководстве пользователя камеры.

Чтобы добавить предустановку:

1. Откройте меню **Конфигурация > Устройства > Предустановки PTZ** и выберите камеру в списке.
2. В случае камеры с механическим PTZ-управлением переместите камеру в нужное положение для получения нужного вида с помощью элементов PTZ-управления. В случае камер с цифровым PTZ-управлением установите нужный масштаб (зум) с помощью колесика мыши и перетащите вид с камеры в нужное положение.
3. Нажмите **Добавить** и введите название новой предустановленной позиции.
4. Нажмите кнопку **OK**.

- Чтобы удалить предустановку, выберите ее и нажмите **Remove (Удалить)**. Предустановка будет удалена как из AXIS Camera Station Pro, так и из камеры.

Управление устройствами

Страница управления устройствами содержит средства для администрирования и обслуживания устройств, подключенных к AXIS Camera Station Pro.

Перейдите в **Configuration (Конфигурация) > Devices (Устройства) > Management (Управление)**, чтобы открыть страницу **Manage devices (Управление устройствами)**.

Если в настроена автоматическая проверка наличия новых версий встроенного ПО в *Настройки обновления встроенного ПО, on page 131*, при наличии новых версий встроенного ПО для устройств

отображается ссылка. Перейдите по этой ссылке для обновления версий встроенного ПО. См. *обновлять встроенное программное обеспечение;.*

Если в *Обновить AXIS Camera Station Pro, on page 137* настроена автоматическая проверка наличия новых версий программного обеспечения, при наличии новой версии AXIS Camera Station Pro отображается ссылка. Нажмите ссылку, чтобы установить новую версию.

AXIS Camera Station Pro отображает список всех добавленных устройств. Чтобы найти устройства в списке, воспользуйтесь полем **Ввести данные для поиска**. Чтобы скрыть или показать столбцы, щелкните правой кнопкой мыши строку заголовков и выберите, какие столбцы показывать. Перетаскивайте заголовки столбцов, чтобы изменить порядок их отображения.

Список устройств содержит следующую информацию:

- **Name (Имя)**: имя устройства или список всех связанных имен камер, если устройство является видеокодером с несколькими подключенными камерами или сетевой камерой с несколькими областями просмотра.
- **MAC address (MAC-адрес)**: MAC-адрес устройства.
- **Status (Состояние)**: состояние устройства.
  - **OK:** стандартное состояние для устройства, с которым установлена связь.
  - **Maintenance (Техническое обслуживание)**: устройство находится на техническом обслуживании и временно недоступно.
  - **Not accessible (Недоступно)**: невозможно установить соединение с устройством.
  - **Not accessible over set hostname (Недоступно по заданному имени узла)**: невозможно установить соединение с устройством по его имени узла.
  - **Server not accessible (Сервер недоступен)**: невозможно установить соединение с сервером, к которому подключено устройство.
  - **Enter password (Введите пароль)**: устройство недоступно до ввода действительных учетных данных. Перейдите по ссылке, чтобы указать действительные учетные данные пользователя. Если устройство поддерживает зашифрованные соединения, пароль отправляется зашифрованным по умолчанию.
  - **Set password (Задать пароль)**: учетная запись root и пароль не настроены либо на устройстве по-прежнему используется пароль по умолчанию. Перейдите по ссылке, чтобы установить пароль для привилегированного пользователя.
    - Введите пароль или нажмите **Generate (Создать)**, чтобы автоматически сгенерировать пароль максимальной длины, допустимой для устройства. Рекомендуется сохранить копию сгенерированного пароля.
    - Выберите, чтобы использовать этот пароль для всех устройств с состоянием `Set password`.
    - Установите флажок **Enable HTTPS (Включить HTTPS)**, чтобы включить HTTPS, если устройство поддерживает этот протокол.
  - **Password type: unencrypted (Тип пароля: незашифрованный)**: соединение с устройством не устанавливается, поскольку ранее для подключения к нему использовался зашифрованный пароль. В целях безопасности AXIS Camera Station Pro не позволяет использовать незашифрованные пароли для устройств, для подключения к которым ранее использовались зашифрованные пароли. Для устройств, поддерживающих шифрование, тип соединения настраивается на странице конфигурации устройства.
  - **Certificate error (Ошибка сертификата):** на устройстве произошла ошибка, связанная с сертификатом.
  - **Certificate about to expire (Срок действия сертификата подходит к концу):** срок действия сертификата на устройстве скоро истечет.
  - **Certificate has expired (Срок действия сертификата истек):** срок действия сертификата на устройстве истек.

  - **HTTPS certificate not trusted (HTTPS-сертификат не является доверенным):** HTTPS-сертификат на устройстве не является доверенным для AXIS Camera Station Pro. Перейдите по ссылке, чтобы выдать новый сертификат HTTPS.
  - **HTTP failed (Ошибка HTTP)**: невозможно установить HTTP-соединение с устройством.
  - **HTTPS failed (Ошибка HTTPS)**: невозможно установить HTTPS-соединение с устройством.
  - **HTTP and HTTPS failed (ping or UDP OK) (Не удалось применить HTTP и HTTPS (Ping или UDP OK).** Не удается установить связь с устройством по протоколам HTTP и HTTPS. Устройство отвечает на команду ping и по протоколу User Datagram Protocol (UDP).
- **Адрес (Address)**: адрес устройства. Перейдите по ссылке, чтобы открыть страницу конфигурации устройства. На ней отображается IP-адрес или имя хоста в зависимости от того, что из этого используется при добавлении устройства. См. *Вкладка конфигурации устройства, on page 78*.
- **Hostname (Имя узла)**: имя узла устройства, если оно доступно. Перейдите по ссылке, чтобы открыть страницу конфигурации устройства. Имя хоста отображается в виде полностью определенного имени домена. См. *Вкладка конфигурации устройства, on page 78*.
- **Manufacturer (Производитель)**: производитель устройства.
- **Model (Модель)**: модель устройства.
- **Firmware (Встроенное ПО)**: версия встроенного ПО, используемая устройством в настоящее время.
- **DHCP**: указывает, подключено ли устройство к серверу по протоколу DHCP.
- **HTTPS.** Состояние HTTPS устройства. Сведения о состоянии HTTPS см. в *Безопасность, on page 75*.
- **IEEE 802.1X.** Состояние IEEE 802.1X устройства. Сведения о состоянии IEEE 802.1X см. в *Безопасность, on page 75*.
- **Server (Сервер)**: сервер AXIS Camera Station Pro, к которому подключено устройство.
- **Теги:** ярлыки, добавленные к устройству (по умолчанию скрыты).
- **Понятное имя в UPnP:** имя в системе UPnP (по умолчанию скрыто). Это описательное имя, используемое для облегчения поиска устройства.

На устройствах можно выполнять следующие действия:

- Назначить IP-адрес устройствам. См. *Назначение IP-адресов*.
- Назначить пароль устройствам. См. *Управлять пользователями*.
- Обновить встроенное ПО на устройствах. См. *обновлять встроенное программное обеспечение;*.
- Перезапустить устройства.
- Восстановление устройств выполняет сброс большинства настроек к заводским значениям по умолчанию, включая пароль. Следующие параметры не сбрасываются: загруженные приложения для камер, протокол загрузки (DHCP или статический), статический IP-адрес, шлюз по умолчанию, маска подсети и системное время.

Примечание

- Чтобы предотвратить несанкционированный доступ, после восстановления устройства всегда задавайте новый пароль.
- Если сбрасываемое устройство использует облачное хранилище, откройте **Cloud storage (Облачное хранилище)** в My Systems и перед сбросом устройства отключите для него облачное хранилище. После сброса устройства перезапустите службу на сервере AXIS Camera Station Pro и включите облачное хранилище для устройства в My Systems (Мои системы). См. *Включение облачного хранилища для отдельных камер*.
- Установить на устройства приложение для камеры. См. *Установка приложений для камер*.
- После изменения настроек на странице конфигурации устройства повторно загрузите список устройств.
- Настроить устройства. См. *Настроить устройства*.

- Управлять пользователями. См. *Управлять пользователями*.
- Управлять сертификатами. См. *Безопасность, on page 75*.
- Сбор данных об устройствах. См. *Сбор данных об устройствах*.
- Выберите, чтобы использовать IP-адрес или имя хоста. См. *Подключение, on page 77*.
- Добавить ярлыки к устройствам. См. *Теги*.
- Ввести учетные данные для устройства. Щелкните устройство правой кнопкой мыши и выберите **Advanced (Дополнительно) > Enter device credentials (Ввести учетные данные устройства)**, чтобы ввести пароль устройства.
- Перейти на вкладку конфигурации устройства и настроить устройство. См. *Вкладка конфигурации устройства, on page 78*.

Назначение IP-адресов

AXIS Camera Station Pro может назначать IP-адреса нескольким устройствам. Новые IP-адреса можно автоматически получать с DHCP-сервера или назначать из диапазона IP-адресов.

Назначение IP-адресов

1. Откройте меню **Конфигурация > Устройства > Управление** и выберите устройства, которые нужно настроить.
2. Нажмите значок или щелкните правой кнопкой мыши и выберите **Назначить IP-адрес**.
3. Если некоторые из выбранных устройств невозможно настроить, например, по причине их недоступности, то откроется диалоговое окно Invalid devices (Недопустимые устройства). Нажмите кнопку **Continue (Продолжить)**, чтобы пропустить устройства, которые нельзя настроить.
4. Если вы выбираете одно устройство для назначения IP-адреса, нажмите **Advanced (Дополнительно)**, чтобы открыть страницу **Assign IP address (Назначение IP-адреса)**.
5. Выберите **Получить IP-адреса автоматически (DHCP)**, если хотите, чтобы устройства автоматически получали IP-адреса от сервера DHCP.
6. Выберите **Назначить следующий диапазон IP-адресов** и укажите диапазон IP-адресов, маску подсети и маршрутизатор по умолчанию.
   Чтобы задать диапазон IP-адресов:
   - Используйте подстановочные символы. Например: 192.168.0.* или 10.*.1.*
   - Вводите первый и последний IP-адреса диапазона через дефис. Например: 192.168.0.10-192.168.0.20 (такой диапазон адресов можно также сократить до 192.168.0.10-20) или 10.10-30.1.101
   - Сочетайте подстановочные символы и обозначение диапазона. Например: 10.10-30.1.*
   - Для разделения нескольких диапазонов используйте запятую. Например: 192.168.0.*,192.168.1.10-192.168.1.20

Примечание

Чтобы можно было назначить диапазон IP-адресов, выбранные устройства должны быть подключены к одному серверу AXIS Camera Station Pro.

7. Нажмите **Next (Далее)**.
8. Проверьте текущие и новые IP-адреса. Чтобы изменить IP-адрес, выберите устройство и нажмите **Изменить IP-адрес**.
   - В разделе **Current IP address (Текущий IP-адрес)** отображаются текущий IP-адрес, маска подсети и шлюз по умолчанию.
   - Измените параметры в разделе **New IP address (Новый IP-адрес)** и нажмите **OK**.
9. Задав все новые IP-адреса, нажмите **Закончить**.

Настроить устройства

Некоторые параметры можно настроить одновременно на нескольких устройствах, скопировав параметры с одного устройства или применив файл конфигурации.

Примечание

Чтобы настроить все параметры на одном устройстве, перейдите на страницу конфигурации устройства. См. *Вкладка конфигурации устройства, on page 78*.

- Сведения о настройке устройств см. в *Способы настройки*.
- Сведения о создании файла конфигурации см. в *Создание файла конфигурации*.
- Сведения о параметрах, которые можно копировать, см. в *Параметры конфигурации*.

Способы настройки

Существуют разные способы настройки устройств. AXIS Device Management настраивает все устройства в соответствии с параметрами, указанными в методе. См. *Настроить устройства*.

Использование конфигурации выбранного устройства

Примечание

Этот метод доступен только для одного устройства и повторно использует некоторые или все его существующие настройки.

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Щелкните устройство правой кнопкой мыши и выберите **Configure Devices (Настроить устройства) > Configure (Настроить)**.
3. Выберите настройки, которые необходимо применить. См. *Параметры конфигурации, on page 70*.
4. Нажмите **Далее**, чтобы проверить применяемые настройки.
5. После нажатия кнопки **Готово** эти настройки будут применены к выбранному устройству.

Копирование конфигурации с другого устройства

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Щелкните устройства правой кнопкой мыши и выберите **Configure Devices (Настроить устройства) > Configure (Настроить)**. Можно выбрать устройства разных моделей и с разным встроенным ПО.
3. Нажмите **Устройство**, чтобы отобразить конфигурации устройств, которые можно использовать повторно.
4. Выберите устройство, параметры которого нужно скопировать, и нажмите **OK**.
5. Выберите настройки, которые необходимо применить. См. *Параметры конфигурации, on page 70*.
6. Нажмите **Далее**, чтобы проверить применяемые настройки.
7. После нажатия кнопки **Готово** эти настройки будут применены к выбранным устройствам.

Использование файла конфигурации

В файле конфигурации содержатся настройки одного устройства. Файл конфигурации можно использовать для настройки одновременно несколько устройств, а также для повторной настройки устройства, если, например, для него был выполнен сброс к заводским настройкам по умолчанию. Файл конфигурации, созданный на одном устройстве, можно применять к устройствам других моделей или с другими версиями встроенного ПО, даже если некоторые настройки отсутствуют на отдельных устройствах.

Если некоторые настройки отсутствуют или не могут быть применены, на вкладке **Tasks (Задачи)** в нижней части клиента AXIS Camera Station Pro для задачи отображается состояние **Error (Ошибка)**. Щелкните задачу правой кнопкой мыши и выберите **Show (Показать)**, чтобы просмотреть сведения о настройках, которые не удалось применить.

Примечание

Этот способ предназначен только для опытных пользователей.

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Щелкните устройства правой кнопкой мыши и выберите **Configure Devices (Настроить устройства) > Configure (Настроить)**.
3. Для перехода к файлу конфигурации нажмите **Файл конфигурации**. Сведения о создании файла конфигурации см. в *Создание файла конфигурации, on page 70*.
4. Выберите в проводнике файл .cfg и нажмите на **Открыть**.
5. Нажмите **Далее**, чтобы проверить применяемые настройки.
6. После нажатия кнопки **Готово** эти настройки будут применены к выбранным устройствам.

Создание файла конфигурации

В файле конфигурации содержатся настройки одного устройства. После этого можно применить эти настройки к другим устройствам. Сведения об использовании файла конфигурации см. в разделе *Способы настройки*.

Отображаемые настройки — это настройки устройств, доступные через AXIS Device Management. Чтобы найти нужную настройку, воспользуйтесь полем **Ввести данные для поиска**.

Чтобы создать файл конфигурации:

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Выберите устройство, для которого нужно создать файл конфигурации.
3. Щелкните правой кнопкой мыши и выберите **Настроить устройства > Создать файл конфигурации**.
4. Выберите параметры, которые нужно включить в файл, и задайте для них требуемые значения. См. *Параметры конфигурации*.
5. Нажмите **Далее**, чтобы проверить настройки.
6. Чтобы создать файл конфигурации, нажмите кнопку **Готово**.
7. Нажмите **Сохранить**, чтобы сохранить выбранные настройки в файл .cfg.

Параметры конфигурации

При настройке устройств речь может идти о настройке параметров, правил действий и о дополнительных настройках устройств.

Параметры

Параметры — это внутренние настройки, определяющие поведение устройства. Общие сведения о параметрах см. в руководстве пользователя соответствующего продукта на *www.axis.com*

Примечание

- К настройке параметров допускаются только опытные пользователи.
- Не все параметры устройств доступны в AXIS Device Management.

В некоторые текстовые поля можно вставлять переменные. Перед применением к устройству переменные заменяются текстом. Чтобы вставить переменную, щелкните правой кнопкой мыши текстовое поле и выберите:

- **Insert device serial number variable (Вставить переменную серийного номера устройства)**: заменяется серийным номером устройства, к которому применяется файл конфигурации.
- **Insert device name variable (Вставить переменную имени устройства)**: заменяется именем устройства, указанным при применении файла конфигурации. Имя устройства можно найти в столбце **Name (Имя)** на странице **Device management (Управления устройствами)**. Чтобы

переименовать устройство, перейдите на страницу **Cameras (Камеры)** или **Other devices (Другие устройства)**.

- **Insert server name variable (Вставить переменную имени сервера)**: заменяется именем сервера, используемого при применении файла конфигурации. Имя сервера можно найти в столбце **Server (Сервер)** на странице **Device management (Управления устройствами)**. Чтобы переименовать сервер, перейдите в AXIS Camera Station Pro Service Control.
- **Insert server time zone variable (Вставить переменную часового пояса сервера)**: заменяется часовым поясом сервера в формате POSIX, используемого при применении файла конфигурации. Эту переменную можно использовать с параметром часового пояса POSIX, чтобы задать правильный часовой пояс для всех устройств в сети, в которой серверы находятся в разных часовых поясах.

Правила действия

Правила действия можно переносить с одного устройства на другое. Изменять правила действий должны только опытные пользователи. Для получения общих сведений о правилах действий см. *Правила действия*.

Дополнительные настройки

- **Stream profiles (Профили потоков)**: профиль потока — предварительно настроенный профиль конфигурации живого просмотра для параметров кодирования видео, изображения и звука. Профили потока можно переносить с одного устройства на другое.
- **Motion detection windows (Зоны обнаружения движения)**: зоны обнаружения движения определяют конкретные области поля зрения камеры. Обычно при любом обнаружении движения (и остановки движения) в заданных областях генерируется сигнал тревоги. Окна обнаружения движения можно переносить с одного устройства на другое.

Управлять пользователями

Перейдите в **Configuration (Конфигурация) > Devices (Устройства) > Management (Управление)**, чтобы управлять пользователями устройств.

При задании пароля или удалении пользователей для нескольких устройств пользователи, отсутствующие на всех устройствах, обозначаются с помощью . Каждый пользователь отображается только один раз, даже если на разных устройствах ему назначены разные роли.

Примечание

Учетные записи относятся к конкретным устройствам и не связаны с учетными записями пользователей AXIS Camera Station Pro.

Политика паролей

Некоторые устройства предъявляют определенные требования к паролям. Если одно или несколько выбранных устройств используют политику паролей, вместо индикатора надежности пароля отображается индикатор соответствия политике, показывающий, соответствует ли пароль действующим требованиям.

- Если политика паролей не применяется или устройство использует стандарт ONVIF, отображается обычный индикатор надежности пароля.
- Если выбрано несколько устройств с разными политиками, пароль должен соответствовать требованиям всех этих политик.
- Если пароль не соответствует требованиям, отображается состояние **Non-compliant (Не соответствует требованиям)**. Наведите курсор на значок информации, чтобы просмотреть конкретные требования:

Политика длины пароля – Пароль должен содержать не менее 15 символов.

Политика сложности пароля – Пароль должен содержать не менее 12 символов и включать как минимум одну прописную букву, одну строчную букву, одну цифру и один специальный символ.

Обе политики – Пароль должен соответствовать требованиям как к длине, так и к сложности.

Set password (Установите пароль):

Примечание

- Устройства с версией встроенного ПО 5.20 и выше поддерживают пароли длиной до 64 знаков. Устройства с более ранними версиями встроенного ПО поддерживают 8-значные пароли. Для устройств с более ранними версиями микропрограммы рекомендуется задавать пароли отдельно.
- При задании пароля на нескольких устройствах, поддерживающих разную длину пароля, пароль должен соответствовать минимально поддерживаемой длине.
- Во избежание несанкционированного доступа и в целях повышения безопасности настоятельно рекомендуется защитить паролями все устройства, добавленные в систему AXIS Camera Station Pro.

В паролях можно использовать следующие символы:

- Буквы A–Z, a–z
- Цифры 0–9
- Пробел, запятая (,), точка (.), двоеточие (:), точка с запятой (;)
- !, ", #, $, %, &, ', (, +, *, -,), /, <, >, =, ?, [, \, ^, -, `, {, |, ~, @,], }

Чтобы задать пароль для пользователей на устройствах:

1. Перейдите в раздел **Configuration > Devices > Management > Manage devices (Конфигурация > Устройства > Управление > Управление устройствами)**.
2. Выберите устройства и нажмите . Можно также выбрать устройства правой кнопкой мыши, а затем открыть **User Management > Set password (Управление пользователями > Установка пароля)**.
3. Выберите пользователя.
4. Введите пароль или нажмите **Generate (Создать)**, чтобы автоматически создать надежный пароль.
5. Нажмите кнопку **OK**.

Примечание

Если установлен флажок **Use this password for all devices without a factory default password (Использовать этот пароль для всех устройств без заводского пароля по умолчанию)**, пароль будет применен ко всем устройствам со статусом **Set password (Задать пароль)**. Если длина пароля превышает максимальную длину, поддерживаемую устройством, вы получите соответствующее уведомление до открытия диалогового окна и сможете выбрать продолжение без этих устройств.

Добавить пользователя

Чтобы добавить в AXIS Camera Station Pro локальных пользователей или пользователей Active Directory, сделайте следующее:

1. Перейдите в раздел **Configuration > Devices > Management > Manage devices (Конфигурация > Устройства > Управление > Управление устройствами)**.
2. Выберите устройства правой кнопкой мыши, а затем перейдите в раздел **User Management > Add user (Управление пользователями > Добавить пользователя)**.
3. Введите имя пользователя, пароль и подтвердите пароль. Список допустимых символов см. выше в разделе **Set password (Задать пароль)**.
4. Выберите права доступа пользователя в раскрывающемся списке **Role (Роль)**:
   - **Administrator (Администратор)**: полный доступ к устройству.
   - **Operator (Оператор)**: доступ к видеопотоку, событиям и всем настройкам, кроме System Options (Параметры системы).
   - **Viewer (Наблюдатель)**: доступ только к видеопотоку.

5. Установите флажок **Enable PTZ control (Разрешить управление PTZ)**, чтобы предоставить пользователю возможность управлять поворотом, наклоном и зумом в режиме живого просмотра.
6. Нажмите кнопку **OK**.

Удалить пользователя

Для удаления пользователей с устройств:

1. Перейдите в раздел **Configuration > Devices > Management > Manage devices (Конфигурация > Устройства > Управление > Управление устройствами)**.
2. Выберите устройства правой кнопкой мыши, а затем перейдите в раздел **User Management > Remove user (Управление пользователями > Удалить пользователя)**.
3. Выберите пользователя, которого необходимо удалить, в раскрывающемся списке **User (Пользователь)**.
4. Нажмите кнопку **OK**.

Список пользователей

Чтобы в списке отображались все пользователи на устройствах, а также их права доступа:

1. Перейдите в раздел **Configuration > Devices > Management > Manage devices (Конфигурация > Устройства > Управление > Управление устройствами)**.
2. Выберите устройства правой кнопкой мыши, а затем перейдите в раздел **User Management > List users (Управление пользователями > Список пользователей)**.
3. Используйте поле **Type to search (Введите текст для поиска)**, чтобы найти пользователя в списке.

обновлять встроенное программное обеспечение;

Встроенное ПО — это программное обеспечение, определяющее функциональность устройства Axis. Поддержание встроенного ПО в актуальном состоянии обеспечивает наличие на устройстве новейших функций и улучшений.

Новое встроенное ПО можно загрузить с помощью AXIS Camera Station Pro или импортировать с жесткого диска или карты памяти. Версии встроенного ПО, доступные для загрузки, обозначаются текстом **(Download)** после номера версии. Версии встроенного ПО, которые доступны на локальном клиенте, отображаются со словом **(Файл)** после номера версии.

При обновлении встроенного ПО можно выбрать тип обновления:

- **Standard (Стандартный)**: обновить до выбранной версии встроенного ПО с сохранением существующих значений настроек.
- **Factory default (Заводские настройки)**: обновить до выбранной версии встроенного ПО и сбросить все настройки до заводских значений.

Чтобы обновить встроенное ПО:

1. Откройте меню **Конфигурация > Устройства > Управление** и выберите устройства, которые нужно настроить.
2. Нажмите значок или щелкните правой кнопкой мыши и выберите **Обновить встроенное ПО**.
3. Если некоторые из выбранных устройств невозможно настроить, например, по причине их недоступности, то откроется диалоговое окно **Invalid devices (Недопустимые устройства)**. Нажмите кнопку **Continue (Продолжить)**, чтобы пропустить устройства, которые нельзя настроить.
4. Во время обновления встроенного ПО устройство недоступно. Щелкните **Да**, чтобы продолжить. Если вы больше не хотите видеть это сообщение, выберите **Do not show this dialog again (Больше не показывать это диалоговое окно)** и нажмите **Yes (Да)**.
5. В диалоговом окне **Upgrade firmware (Обновление встроенного ПО)** отображаются модель устройства, количество устройств каждой модели, текущая версия встроенного ПО, доступные для обновления версии встроенного ПО и тип обновления. По умолчанию устройства в списке

предварительно выбраны, если доступны новые версии встроенного ПО для загрузки, а для каждого устройства предварительно выбрана последняя версия встроенного ПО.

5.1. Для обновления списка версий встроенного ПО, доступного для скачивания, нажмите кнопку **Проверить наличие обновлений**. Чтобы найти один или несколько файлов встроенного ПО, которые хранятся в локальном клиентском модуле, нажмите кнопку **Обзор**.

5.2. Выберите устройства, версии встроенного ПО, до которых требуется выполнить обновление, и тип обновления.

5.3. Нажмите **OK**, чтобы приступить к обновлению устройств в списке.

Примечание

По умолчанию обновление встроенного ПО выполняется одновременно для всех выбранных устройств. Порядок обновления можно изменить. См. *Настройки обновления встроенного ПО*.

Установка приложений для камер

Приложениями для камер называется программное обеспечение, которое можно загрузить и установить на сетевую видеотехнику Axis. Приложения расширяют функциональные возможности устройства, например обеспечивают обнаружение, распознавание, отслеживание или подсчет объектов.

Отдельные приложения можно установить непосредственно из AXIS Camera Station Pro. Другие приложения сначала нужно скачать из раздела нашего сайта *www.axis.com/global/en/products/analytics-and-other-applications* или с сайта разработчика приложений.

Приложения устанавливаются на устройства, совместимые с платформой AXIS Camera Application. Отдельным приложениям требуются конкретные версии встроенного ПО или модели камер.

Если для приложения требуется лицензия, файл лицензионного ключа можно установить одновременно с приложением или позднее на странице конфигурации устройства.

Чтобы получить файл с лицензионным ключом, код лицензии, предоставляемый вместе с приложением, нужно в обязательном порядке зарегистрировать по адресу *www.axis.com/se/sv/products/camera-applications/license-key-registration#/registration*

Если установить приложение не удалось, проверьте на сайте *www.axis.com* модель устройства и версию встроенного ПО на совместимость с платформой AXIS Camera Application Platform.

Доступные программные приложения для камер

Видеодетектор движения AXIS Video Motion Detection 4 – Приложение служит для обнаружения движущихся объектов в зоне наблюдения. Для этого приложения лицензия не требуется. Его можно устанавливать на камеры с микропрограммой версии 6.50 и выше. Вы также можете ознакомиться с заметками о выпуске для встроенного ПО ваших устройств, чтобы убедиться в том, что используемая версия поддерживает Video Motion Detection 4.

AXIS Video Motion Detection 2 – Приложение служит для обнаружения движущихся объектов в зоне наблюдения. Для этого приложения лицензия не требуется. Его можно устанавливать на камеры с микропрограммой версии 5.60 и выше.

AXIS Video Content Stream – Приложение, позволяющее камерам Axis передавать данные отслеживания движения в AXIS Camera Station Pro. Оно может быть установлено на камеру со встроенным ПО версии от 5.50 до 9.59. AXIS Video Content Stream можно использовать только с AXIS Camera Station Pro.

Другие приложения – Любое приложение, которое необходимо установить. Прежде чем начать установку приложения, его нужно загрузить на локальный компьютер.

Установка приложений для камеры:

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Выберите камеры, на которые необходимо установить приложения. Щелкните значок или нажмите правую кнопку мыши и выберите в меню **Установить приложение для камеры**.
3. Выберите приложение для камеры, которое необходимо установить. Если вы хотите установить другие приложения, нажмите кнопку **Обзор** и перейдите к нужному файлу приложения на локальном компьютере. Нажмите **Next (Далее)**.
4. После установки приложения можно выбрать вариант **Разрешить перезапись приложения**, что позволит переустановить приложение, или вариант **Разрешить возврат к предыдущей версии**, чтобы можно было установить предыдущую версию приложения.

Примечание

При понижении версии или перезаписи приложения его настройки на устройствах будут сброшены.

5. Если для приложения требуется лицензия, откроется диалоговое окно **Install licenses (Установка лицензий)**.
   5.1. Нажмите **Да**, чтобы начать установку лицензии, затем нажмите **Далее**.
   5.2. Нажмите кнопку **Обзор** и перейдите к файлу лицензии, затем нажмите **Далее**.

Примечание

Для установки AXIS Video Motion Detection 2, AXIS Video Motion Detection 4 и AXIS Video Content Stream лицензия не требуется.

6. Проверьте информацию и нажмите **Готово**. В процессе установки состояние камеры меняется с `OK` на `Maintenance`, а затем вновь на `OK` (после окончания установки).

Безопасность

Центр сертификации (CA) AXIS Camera Station Pro автоматически подписывает и распространяет сертификаты клиента и сервера на устройства при включении HTTPS или IEEE 802.1X. ЦС игнорирует предустановленные сертификаты. Сведения о том, как настраивать сертификаты, см. в разделе *Сертификаты, on page 148*.

Управление сертификатами HTTPS или IEEE 802.1X

Примечание

Прежде чем включать IEEE 802.1X, убедитесь, что время на устройствах Axis синхронизировано со временем в AXIS Camera Station Pro.

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Щелкните устройства правой кнопкой мыши:
   - Выберите **Security (Безопасность) > HTTPS > Enable/Update (Включить/обновить)**, чтобы включить HTTPS или обновить настройки HTTPS для устройств.
   - Выберите **Security (Безопасность) > IEEE 802.1X > Enable/Update (Включить/обновить)**, чтобы включить IEEE 802.1X или обновить настройки IEEE 802.1X для устройств.
   - Выберите **Security (Безопасность) > HTTPS > Disable (Отключить)**, чтобы отключить HTTPS для устройств.
   - Выберите **Security (Безопасность) > IEEE 802.1X > Disable (Отключить)**, чтобы отключить IEEE 802.1X для устройств.
   - Выберите **Сертификаты...**, чтобы получить обзор, удалить сертификаты или получить подробную информацию о конкретном сертификате.

Примечание

Если один и тот же сертификат установлен на нескольких устройствах, он отображается как один элемент. При удалении сертификата он удаляется со всех устройств, на которых установлен.

Состояние HTTPS и IEEE 802.1X

Состояние HTTPS и IEEE 802.1X отображается на странице Device management (Управление устройствами).

	Статус	Описание
HTTPS	On (Вкл.)	AXIS Camera Station Pro использует HTTPS для подключения к устройству.
	Off (Выкл.)	AXIS Camera Station Pro использует HTTP для подключения к устройству.
	Неизвестно	Устройство недоступно.
	Неподдерживаемое встроенное ПО	HTTPS не поддерживается, поскольку версия встроенного ПО устройства слишком старая.
	Неподдерживаемое устройство	HTTPS не поддерживается этой моделью устройства.
IEEE 802.1X	Включено	Протокол IEEE 802.1X включен на устройстве.
	отключена	IEEE 802.1X не активирован, но готов к активации на устройстве.
	Неподдерживаемое встроенное ПО	IEEE 802.1X не поддерживается, поскольку версия встроенного ПО устройства слишком старая.
	Неподдерживаемое устройство	IEEE 802.1X не поддерживается этой моделью устройства.

Сбор данных об устройствах

Этот параметр обычно используется для устранения неисправностей. Используйте его для создания ZIP-файла с отчетом о сборе данных для определенного расположения на устройствах.

Чтобы собрать данные об устройстве:

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Щелкните устройства правой кнопкой мыши и выберите **Сбор данных об устройстве**.
3. В разделе **Data source on selected devices (Источник данных на выбранных устройствах)**:
   - Нажмите **Предустановка** и выберите одно из значений в раскрывающемся списке обычно используемых команд.

   Примечание

   Некоторые предустановленные наборы параметров работают не на всех устройствах. Например, состояние PTZ не поддерживается аудиоустройствами.

   - Нажмите **Задается пользователем** и укажите полный URL-адрес для источника собираемых данных на выбранных серверах.
4. В разделе **Save as (Сохранить как)** укажите имя файла и расположение папки для ZIP-файла с данными.
5. Выберите **Автоматически открывать папку после сбора данных** — при выборе этого варианта указанная папка будет открываться по окончании сбора данных.
6. Нажмите кнопку **OK**.

Подключение

Для связи с устройствами по IP-адресу или имени узла:

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Выберите устройства, щелкните правой кнопкой мыши и выберите **Connection (Подключение)**.
   - Чтобы подключиться к устройствам, используя IP-адрес, выберите **Use IP (Использовать IP-адрес)**.
   - Чтобы подключиться к устройствам, используя имя хоста, выберите **Use hostname (Использовать имя хоста)**.
   - Для изменения учетных данных, адреса или настроек порта выберите **Edit (Изменить)**.

Теги

Теги помогают организовать устройства на странице **Device management (Управление устройствами)**. Устройство может иметь несколько тегов.

Устройствам можно присваивать теги по модели, расположению или другим критериям. Например, если устройства помечены тегами по модели камеры, можно быстро найти и обновить все камеры этой модели.

Присвоение тега устройствам:

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Щелкните устройство правой кнопкой мыши и выберите **Присвоить теги устройствам**.
3. Выберите **Use existing tag (Использовать существующий тег)** и выберите тег либо выберите **Create a new tag (Создать новый тег)** и введите его название.
4. Нажмите кнопку **OK**.

Чтобы удалить тег у устройства:

1. Откройте меню **Configuration (Конфигурация) > Devices (Устройства) > Management (Управление)** и нажмите значок вверху справа.
2. В папке **Tags (Теги)** выберите тег. Будут показаны все устройства, отмеченные с этим тегом.
3. Выберите устройства, щелкните их правой кнопкой мыши и выберите **Untag devices (Удалить теги с устройств)**.
4. Нажмите кнопку **OK**.

Управление тегами:

1. Откройте меню **Configuration (Конфигурация) > Devices (Устройства) > Management (Управление)** и нажмите значок вверху справа.
2. На странице **Device tags (Теги устройств)**:
   - Щелкните правой кнопкой мыши пункт **Теги** и выберите **Новый тег**.
   - Чтобы переименовать тег, щелкните правой кнопкой мыши, выберите **Переименовать тег** и введите новое название тега.
   - Чтобы удалить тег, щелкните правой кнопкой мыши и выберите **Удалить**.
   - Нажмите , чтобы закрепить страницу **Device tags (Теги устройств)**.
   - Нажмите тег, чтобы отобразить все связанные с ним устройства, или нажмите **All devices (Все устройства)**, чтобы отобразить все устройства, подключенные к AXIS Camera Station Pro.
   - Нажмите **Предупреждения/Ошибки**, чтобы показать устройства, требующие внимания, например, устройства, к которым нет доступа.

Вкладка конфигурации устройства

Чтобы настроить все параметры для одного устройства:

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Щелкните по адресу или имени хоста устройства, чтобы перейти на вкладку конфигурации устройства.
3. Измените параметры. Сведения о настройке устройства см. в руководстве пользователя устройства.
4. Закройте вкладку. Устройство перезагружается для применения изменений в AXIS Camera Station Pro.

Ограничения

- Автоматическая аутентификация сторонних устройств не поддерживается.
- Мы не можем гарантировать полную поддержку сторонних устройств.
- Вкладка конфигурации устройства с активными видеопотоками увеличивает нагрузку и может повлиять на производительность сервера.

Внешние источники данных

Внешним источником данных является система или источник, которые создают данные, позволяющие отследить, что именно произошло во время каждого события. См. *Поиск данных, on page 46*.

Перейдите в **Configuration (Конфигурация) > Devices (Устройства) > External data sources (Внешние источники данных)**, чтобы просмотреть список всех внешних источников данных. Чтобы упорядочить список по содержимому столбца, щелкните по заголовку этого столбца.

Наименование	Описание
Название	Имя внешнего источника данных.
Исходный ключ	Уникальный идентификатор внешнего источника данных.
Вид	Вид, с которым связан внешний источник данных.
Сервер	Сервер, к которому подключен источник данных. Отображается только при подключении к нескольким серверам.

Внешний источник данных добавляется автоматически, когда:

- При создании двери в разделе **Configuration > Access control > Doors and zones (Конфигурация > Контроль доступа > Двери и зоны)**.
  Полное описание рабочего процесса настройки дверного сетевого контроллера Axis в AXIS Camera Station Pro см. в разделе *Настройка сетевого дверного контроллера Axis*.
- При получении первого события устройством, которое настроено для работы с AXIS License Plate Verifier.
  Полное описание рабочего процесса настройки AXIS License Plate Verifier в AXIS Camera Station Pro см. в разделе *Настройка AXIS License Plate Verifier*.

Если для внешнего источника данных настроено представление, данные, созданные источником данных, автоматически добавляются в закладки на временной шкале представления на вкладке **Data search (Поиск данных)**. Чтобы связать источник данных с видом с камеры:

1. Перейдите к пункту **Configuration > Devices > External data sources (Конфигурация > Устройства > Внешние источники данных)**.
2. Выберите внешний источник данных и нажмите **Edit (Изменить)**.

3. Выберите вид в раскрывающемся списке **View (Вид)**.
4. Нажмите кнопку **OK**.

Синхронизация времени

Перейдите в **Configuration > Devices > Time synchronization (Конфигурация > Устройства > Синхронизация времени)**, чтобы открыть страницу **Time synchronization (Синхронизация времени)**.

AXIS Camera Station Pro отображает список всех добавленных устройств. Щелкните правой кнопкой мыши по строке заголовка и выберите столбцы для отображения. Перетаскивайте заголовки столбцов, чтобы изменить порядок их отображения.

Список устройств содержит следующую информацию:

- **Name (Имя)**: имя устройства или список всех связанных имен камер, если устройство является видеокодером с несколькими подключенными камерами или сетевой камерой с несколькими областями просмотра.
- **Адрес (Address)**: адрес устройства. Перейдите по ссылке, чтобы открыть страницу конфигурации устройства. На ней отображается IP-адрес или имя хоста в зависимости от того, что из этого используется при добавлении устройства. См. *Вкладка конфигурации устройства, on page 78*.
- **MAC address (MAC-адрес)**: MAC-адрес устройства.
- **Model (Модель)**: модель устройства.
- **Enabled (Включено)**: указывает, включена ли синхронизация времени.
- **NTP source (Источник NTP)**: источник NTP, настроенный для устройства.
  - **Static (Статический)**: серверы NTP устройства задаются вручную в полях **Primary NTP server (Основной сервер NTP)** и **Secondary NTP server (Вторичный сервер NTP)**.
  - **DHCP:** Устройство получает NTP-сервер динамически из сети. **Поля Primary NTP server (Основной NTP-сервер)** и **Secondary NTP server (Резервный NTP-сервер)** недоступны при выборе **DHCP**.
- **Primary NTP server (Основной сервер NTP)**: основной сервер NTP, настроенный для устройства. Доступно только при выборе варианта **Static (Статический)**.
- **Secondary NTP server (Вторичный сервер NTP)**: вторичный сервер NTP, настроенный для устройства. Доступно только для устройств Axis, которые поддерживают резервный NTP-сервер и при выбранном варианте **Static (Статический)**.
- **Server time offset (Смещение времени сервера)**: разница во времени между устройством и сервером.
- **UTC time (Время UTC)**: всемирное координированное время на устройстве.
- **Synced (Синхронизировано)**: указывает, применены ли настройки синхронизации времени. Доступно только для устройств со встроенным ПО версии 9.1 или более поздней.
- **Time to next sync (Время до следующей синхронизации)**: время, оставшееся до следующей синхронизации.

Служба времени Windows (W32Time) использует протокол сетевого времени (NTP) для синхронизации даты и времени для сервера AXIS Camera Station Pro. Отображается следующая информация:

- **Server (Сервер)**: сервер AXIS Camera Station Pro, на котором запущена служба времени Windows.
- **Status (Состояние)**: состояние службы времени Windows. `Running` или `Stopped`.
- **NTP server (Сервер NTP)**: сервер NTP, настроенный для службы времени Windows.

Настройка синхронизации времени

1. Перейдите в раздел **Configuration > Devices > Time synchronization (Конфигурация > Устройства > Синхронизация времени)**.

2. Выберите устройства и укажите опцию **Enable time synchronization (Включить синхронизацию времени)**.
3. Выберите источник NTP**Static (Статический)** или **DHCP**.
4. Если выбран вариант **Static (Статический)**, настройте основной и вторичный серверы NTP.
5. Нажмите **Применить**.

Отправлять тревогу, если разница во времени между сервером и устройством превышает 2 секунды.	Выберите этот параметр, чтобы получать тревогу, если разница во времени между сервером и устройством превышает 2 секунды.
Set the time zone manually through the device interface (Настроить часовой пояс вручную через интерфейс устройства)	Выберите этот параметр, если вы не хотите использовать часовой пояс сервера, а предпочитаете установить другой часовой пояс для местоположения устройства. В этом случае вам необходимо вручную настроить часовой пояс через веб-интерфейс устройства.

Настройка хранилища

Перейдите в **Configuration (Конфигурация) > Storage (Хранилище) > Management (Управление)**, чтобы открыть страницу **Manage storage (Управление хранилищем)**. Здесь отображается обзор локального и сетевого хранилища в AXIS Camera Station Pro.

Список	
Место расположения	Путь к ресурсу хранения и его имя.
Выделено	Максимальный объем пространства ресурса хранения, отведенный для записей.
Используется	Объем пространства ресурса хранения, в данный момент занятый записями.

Список	
Статус	Состояние ресурса хранения. Возможные значения статуса: • **OK** • **Storage full (Хранилище заполнено)**: хранилище заполнено. Система перезаписывает самые старые, незаблокированные записи. • **Unavailable (Недоступно)**: информация о хранилище в настоящее время недоступна. Например, это может произойти, если сетевое хранилище удалено или отключено. • **Intruding data (Посторонние данные)**: другие приложения используют пространство хранилища, выделенное для AXIS Camera Station Pro. Или имеются записи без подключения к базе данных, так называемые неиндексированные записи, которые находятся в дисковом пространстве, выделенном для AXIS Camera Station Pro. • **No permissions (Нет разрешений)**: у пользователя нет разрешения на чтение или запись в хранилище. • **Low space (Мало свободного места)**: на диске доступно менее 15 ГБ свободного места, что AXIS Camera Station Pro считает недостаточным. Чтобы предотвратить ошибки или повреждения, AXIS Camera Station Pro выполняет принудительную очистку независимо от расположения ползунка хранилища для защиты накопителя. В процессе принудительной очистки AXIS Camera Station Pro предотвращает запись до тех пор, пока не будет доступно более 15 ГБ памяти. • **Insufficient capacity (Недостаточная емкость)**: общий объем диска составляет менее 32 ГБ, что недостаточно для AXIS Camera Station Pro. Устройства видеозаписи AXIS OS Recorders, поддерживающие RAID, также могут иметь следующие статусы: • **Online (В сети)**: RAID-массив работает надлежащим образом. Предусмотрено резервирование на случай отказа одного из физических дисков в системе RAID. • **Degraded (Работа с ограничениями)**: один из физических дисков RAID-массива неисправен. Запись и воспроизведение записей из хранилища по-прежнему возможны, но резервирование отсутствует. При поломке другого физического диска состояние RAID-массива меняется на **Failure (Сбой)**. Рекомендуется как можно раньше заменить поврежденный физический диск. После замены поврежденного диска состояние RAID-массива меняется с **Degraded (Ухудшилось)** на **Syncing (Синхронизация)**. • **Syncing (Синхронизация)**: выполняется синхронизация дисков RAID. Запись и воспроизведение записей из хранилища возможны, но в случае отказа физического диска резервирование отсутствует. После синхронизации физических дисков в системе RAID происходит резервирование, а состояние RAID меняется на **Online (В сети)**. Внимание Не извлекайте диск RAID во время синхронизации. Это может привести к сбою в работе диска. • **Failure (Отказ)**: несколько физических дисков RAID-массива вышли из строя. При этом происходит потеря всех записей в

Список	
	хранилище, и запись возможна только после того, как вы замените сломанные физические диски.
Сервер	Сервер, на котором расположен локальный ресурс хранения или сетевое хранилище.

Общее представление	
Используется	Объем пространства ресурса хранения, который в данный момент занят записями. Если файл находится в каталоге записей, но не проиндексирован в базе данных, этот файл учитывается в этой категории **Other data (Другие данные)**. См. *Управление хранением данных, on page 82*.
Свободно	Объем пространства ресурса хранения, оставшийся на устройстве хранения. Это тот же объем пространства, что и "Space free" (Свободно:) в свойствах Windows для устройства хранения.
Другие данные	Объем пространства хранилища, занятый файлами, отличными от индексированных записей, поэтому неизвестный для . AXIS Camera Station Pro Other data (Другие данные) = общая емкость - используемое пространство - свободное пространство.
Общая емкость	Общий объем пространства ресурса хранения. Это тот же объем пространства, что и "Total size" (Общий размер) в свойствах Windows для устройства хранения.
Выделено	Объем пространства ресурса хранения, который AXIS Camera Station Pro может использовать для записей. Чтобы изменить объем выделенного пространства, используйте ползунок и нажмите **Apply (Применить)**.

Сетевое устройство хранения	
Путь	Путь к сетевому хранилищу.
Имя пользователя	Имя пользователя, которое используется для подключения к сетевому хранилищу.
Пароль	Соответствующий имени пользователя пароль, который используется для подключения к сетевому хранилищу.

Управление хранением данных

Перейдите в **Configuration (Конфигурация) > Storage (Хранилище) > Management (Управление)**, чтобы открыть страницу **Manage storage (Управление хранилищем)**. Здесь можно указать папку для хранения записей. Чтобы предотвратить заполнение хранилища, задайте максимальный процент общей емкости, который может использовать AXIS Camera Station Pro. Для повышения безопасности и расширения свободного пространства можно добавить дополнительный локальный ресурс хранения и сетевые диски.

Примечание

- При подключении к нескольким серверам AXIS Camera Station Pro выберите сервер из выпадающего меню **Selected server (Выбранный сервер)** для управления хранилищем.
- Если служба использует системную учетную запись для входа в систему, невозможно добавить

сетевые диски, связанные с общими папками на других компьютерах. См. *Нет доступа к сетевому хранилищу*.

- Локальный ресурс хранения или сетевое хранилище невозможно удалить, если в камерах настроена запись на этот ресурс либо данный ресурс содержит записи.

Добавление локального ресурса хранения или общего сетевого диска

1. Откройте меню **Конфигурация > Устройство хранения > Управление**.
2. Нажмите **Добавить**.
3. Чтобы добавить локальное хранилище, выберите **Local storage (Локальное хранилище)** и выберите расположение хранилища в раскрывающемся списке.
4. Чтобы добавить общий сетевой диск, выберите **Shared network drive (Общий сетевой диск)** и введите путь. Например: \\ip_address\share.
5. Нажмите **OK** и введите имя пользователя и пароль для общего сетевого диска.
6. Нажмите кнопку **OK**.

Удаление локального ресурса хранения или общего сетевого диска

Чтобы удалить локальное хранилище или общий сетевой диск, выберите его в списке хранилищ и нажмите **Remove (Удалить)**.

Перемещение записей в новую папку

1. Откройте меню **Конфигурация > Устройство хранения > Управление**.
2. Выберите локальное хранилище или общий сетевой диск из списка ресурсов хранения.
3. Во вкладке **Overview (Обзор)** введите имя папки в поле **Move recordings to a new folder (Переместить записи в новую папку)**, чтобы изменить место хранения записей. Существующие записи будут перемещены из предыдущей папки в новую.
4. Нажмите **Применить**.

Изменение емкости ресурса хранения

1. Откройте меню **Конфигурация > Устройство хранения > Управление**.
2. Выберите локальное хранилище или общий сетевой диск из списка ресурсов хранения.
3. Во вкладке **Overview (Обзор)** переместите ползунок, чтобы задать максимальное пространство, которое может использовать AXIS Camera Station Pro.
4. Нажмите **Применить**.

Примечание

- Мы рекомендуем оставлять не занятым не менее 5% свободного места на диске для оптимальной производительности.
- Минимальный объем хранилища, добавляемого в AXIS Camera Station Pro, составляет 32 ГБ, при этом должно быть доступно не менее 15 ГБ свободного места.
- Если доступно менее 15 ГБ свободного места, AXIS Camera Station Pro автоматически удаляет старые записи для освобождения места.

Сбор неиндексированных файлов

Неиндексированные файлы могут составлять существенную часть сегмента **Другие данные** на ресурсе хранения. К неиндексированным файлам относятся любые данные в папке с видеозаписями, которые не входят в текущую базу данных. Такой файл может содержать видеозаписи, оставшиеся от предыдущих установок, или данные, которые были потеряны при использовании точки восстановления.

Система не удаляет собранные файлы, а собирает их и помещает в папку **Non-indexed files (Неиндексированные файлы)** в хранилище записей. В зависимости от конфигурации этот ресурс хранения может располагаться либо на том же компьютере, что и клиент, либо на удаленном сервере. Для доступа к папке **Non-indexed files (Неиндексированные файлы)** необходим доступ к серверу. AXIS Camera

Station Pro сначала систематизирует данные по серверам, а затем по устройствам, подключенным к соответствующему серверу.

Можно найти потерянную запись или журнал либо удалить содержимое для освобождения места.

Чтобы собрать неиндексированные файлы для проверки или удаления:

1. Откройте меню **Конфигурация > Устройство хранения > Управление**.
2. Выберите локальное хранилище или общий сетевой диск из списка ресурсов хранения.
3. В разделе **Collect non-indexed files (Сбор неиндексированных файлов)** нажмите **Collect (Собрать)**, чтобы запустить задачу.
4. После завершения задачи перейдите в **Alarms and Tasks (Тревоги и задачи) > Tasks (Задачи)** и дважды щелкните задачу, чтобы просмотреть результат.

Выбор устройств хранения для подключения

Примечание

Записи хранятся в виде ACSM-файлов. Перед воспроизведением их необходимо конвертировать. Чтобы получить помощь в конвертировании файлов, обратитесь в службу технической поддержки Axis.

Перейдите в **Configuration > Storage > Selection (Конфигурация > Хранилище > Выбор)**, чтобы открыть страницу **Select storage (Выбор хранилища)**. На этой странице отображается список всех камер в AXIS Camera Station Pro. Здесь можно указать, сколько дней хранить записи для определенных камер. После выбора камеры информацию о хранилище можно просмотреть в разделе **Recording Storage (Хранилище записей)**. Одновременно можно настраивать сразу нескольких камер.

Название	Имя устройства или список имен всех связанных с ним камер, если устройство представляет собой видеокодер с несколькими подключенными камерами или сетевую камеру с несколькими зонами просмотра.
Адрес	Адрес устройства. Перейдите по ссылке, чтобы открыть страницу конфигурации устройства. На ней отображается IP-адрес или имя хоста в зависимости от того, что из этого используется при добавлении устройства. См. *Вкладка конфигурации устройства, on page 78*.
MAC-адрес	MAC-адрес устройства.
Изготовитель	производитель устройства.
Модель	модель устройства.
Используемое пространство устройства хранения	Объем пространства ресурса хранения, в данный момент занятый записями.
Место расположения	Путь к ресурсу хранения и его имя.
Время хранения записей	Время хранения, заданное для камеры.
Самая старая запись	Время самой старой записи с камеры, находящейся в хранилище.
Воспроизведение с SD-карты	Указывает, настроена ли камера на непосредственное воспроизведение записей с SD-карты в AXIS Camera Station Pro, без копирования записей на сервер.
Резервная запись	Указывает, использует ли камера резервную запись при отказе.
Копирование на сервер ACS Pro	Указывает, копируются ли записи с SD-карты на AXIS Camera Station Pro.

Резервная запись	Указывает, использует ли камера резервную запись.
Сервер	Сервер, на котором расположен локальный ресурс хранения или сетевое хранилище.

Настройки хранилища для каждой камеры были заданы при добавлении камер в AXIS Camera Station Pro. Чтобы изменить настройки хранения для камеры:

1. Откройте меню **Конфигурация > Устройство хранения > Выбор**.
2. Выберите камеру для изменения настроек хранения.
3. В разделе **Recording storage (Хранилище записей)** задайте место хранения и время хранения.
4. В разделе **SD card storage (Хранилище на SD-карте)** при необходимости выберите **Playback of SD card recordings (Воспроизведение записей с SD-карты)**, **Failover recording (Резервная запись)** и **Copy SD card recordings to ACS Pro server (Копировать записи с SD-карты на сервер ACS Pro)**.
5. Нажмите **Применить**.

Хранение записей Примечание • Для использования хранилища на SD-карте устройство должно поддерживать VAPIX и использовать SD-карту Axis. • Функции SD-карты не работают с M-JPEG. • Записи на SD-карте не удаляются AXIS Camera Station Pro. Срок их хранения определяется параметром времени хранения записей на SD-карте в камере.	
Сохранить на	Выберите расположение хранилища для записей в раскрывающемся списке. Возможные варианты: локальный ресурс хранения и созданное сетевое хранилище.
Время хранения записей	• **Unlimited (Неограниченно)**: хранить записи до заполнения хранилища. • **Limited (Ограниченный)**: задайте максимальное количество дней хранения записей. Примечание Если место, выделенное на ресурсе хранения для AXIS Camera Station Pro, будет заполнено, записи могут быть удалены до истечения указанного количества дней.
Максимальное количество дней хранения записей	Укажите срок хранения записей в днях.

Накопитель на SD-карте	
Воспроизведение записей с SD-карты	Включите этот параметр, чтобы воспроизводить записи непосредственно с SD-карты камеры в AXIS Camera Station Pro, не копируя их на сервер. Записи с SD-карты, отображаемые на временной шкале, также можно экспортировать. Для использования этой функции требуется AXIS OS 5.60 или более поздней версии.
Резервная запись	Выберите этот параметр, чтобы сохранять записи на SD-карту камеры при потере соединения с AXIS Camera Station Pro. Доступно для камер с SD-картой и встроенным ПО версии 5.20 или более поздней.
Копирование записей с SD-карты на сервер ACS	Выберите этот параметр, чтобы скопировать все записи с SD-карты камеры на сервер. Используйте **Schedule (Расписание)**, чтобы задать время копирования записей. По умолчанию установлено значение **Always (Всегда)**.

Настройка записи и событий

При добавлении камер в AXIS Camera Station Pro система автоматически настраивает запись по детектору движения или непрерывную запись. Позже можно изменить способ записи в соответствии с вашими потребностями. См. *Способ записи, on page 92*.

Запись по детекции движения

Детекцию движения можно использовать со всеми сетевыми камерами и видеокодерами Axis. Запись только при обнаружении движения позволяет значительно сэкономить место в хранилище по сравнению с непрерывной записью. При выполнении настройки на экране **Recording method (Способ записи)** можно включить и настроить параметр **Motion detection (Обнаружение движения)**. Например, можно настроить параметры, если камера обнаруживает слишком много или слишком мало движущихся объектов или если размер записываемых файлов слишком велик для доступного пространства в хранилище.

Чтобы настроить запись при обнаружении движения:

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Выберите камеру.
3. Установите флажок **Motion detection (Обнаружение движения)**.
4. Нажмите **Motion settings (Настройки обнаружения движения)**, чтобы настроить параметры обнаружения движения, например количество обнаруживаемых объектов. Доступные параметры различаются в зависимости от камеры; см. *Настройка встроенного видеодетектора движения* и *Изменение настроек AXIS Video Motion Detection 2 и 4*.
5. Выберите профиль в раскрывающемся списке **Profile (Профиль)**. По умолчанию выбран профиль **High (Высокое качество)**.
6. Выберите расписание или нажмите **New schedule... (Новое расписание...)**, чтобы создать пользовательское расписание.
7. Задайте время предварительного и последующего буфера и период срабатывания.
8. Нажмите **Применить**.

Примечание

Для настройки записи при обнаружении движения можно также использовать правила действий. Перед использованием правил действий убедитесь, что параметр **Motion detection (Обнаружение движения)** отключен в разделе **Recording method (Метод записи)**.

Профиль	Чтобы уменьшить размер записи используйте более низкое разрешение. Чтобы изменить параметры профиля, ознакомьтесь с разделом *Профили потоков*.
Расписание	Расписание записей. Чтобы снизить нагрузку на пространство хранилища, осуществляйте запись только в определенные периоды времени.
Категория события	Категория событий, к которой должна относиться запись, при наличии.
Буфер перед тревогой	Число секунд до обнаружения движения для включения в запись.
Буфер после тревоги	Число секунд после обнаружения движения для включения в запись.
Период действия триггера	Задает минимальный интервал между двумя срабатываниями, чтобы уменьшить количество следующих друг за другом записей. Если в течение этого интервала происходит другое срабатывание, запись продолжается, а отсчет интервала начинается заново.
Уведомления	При обнаружении движения камерой отправляется уведомление. **Mobile app (Мобильное приложение)** отправляет push-уведомление в мобильное приложение AXIS Camera Station. **Server alarm (Тревога сервера)** формирует тревогу в AXIS Camera Station Pro.

Настройка детектора движения

Обнаружение объектов

Запись по обнаружению объектов выполняется при обнаружении и классификации объектов (например, людей или транспортных средств) с помощью AXIS Object Analytics. Рекомендуется использовать эту функцию совместно с обнаружением движения или непрерывной записью, чтобы не пропустить события. AXIS Object Analytics поддерживает до 10 сценариев на камеру.

Примечание

Для использования функции требуется камера с прошивкой версии 12.4.26 или новее, наличие одного сенсора и установленное приложение AXIS Object Analytics ACAP.

Для использования функции обнаружения объектов:

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Выберите камеру.
3. Установите флажок **Object detection (Обнаружение объектов)**.
4. Настройте параметры. Дополнительные сведения см. в таблице ниже.
5. Нажмите **Применить**.

- События обнаружения объектов отображаются на временной шкале розовым цветом.

Параметры обнаружения объектов...	Нажмите, чтобы открыть веб-интерфейс AXIS Object Analytics и настройку типов объектов (люди, транспортные средства), инициирующих запись, чтобы задать минимальный размер объекта, определить зоны обнаружения и настроить время нахождения объекта в зоне.
Профиль	Выберите профиль в раскрывающемся списке **Profile (Профиль)**. По умолчанию используется профиль **High (Высокий)**. Чтобы уменьшить размер записи используйте более низкое разрешение. Чтобы изменить параметры профиля, ознакомьтесь с разделом *Профили потоков*.
Расписание	Задайте расписание записей. Чтобы снизить нагрузку на пространство хранилища, осуществляйте запись только в определенные периоды времени.
Категория события	При необходимости можно выбрать категорию события, к которой должна относиться запись. Дополнительную информацию см. в разделе *Категории событий, on page 29*.
Буфер перед тревогой	Задайте число секунд до обнаружения объектов для включения в запись.
Буфер после тревоги	Задайте число секунд после обнаружения объектов для включения в запись.
Период действия триггера	Задайте минимальный интервал между срабатываниями триггера, чтобы сократить количество следующих друг за другом записей. Если в течение этого интервала произойдет повторное срабатывание, запись продолжится, а отсчет интервала срабатывания начнется заново.
Уведомления	Отправляет уведомление при обнаружении объекта с помощью AXIS Object Analytics. **Mobile app (Мобильное приложение)** отправляет push-уведомление в мобильное приложение AXIS Camera Station. В AXIS Camera Station Pro формируется **Сигнал тревоги сервера**.

Непрерывная запись и запись по расписанию

Непрерывная запись сохраняет изображения без перерывов и требует больше места в хранилище, чем другие варианты записи. Чтобы уменьшить размер файлов, рассмотрите возможность использования записи при обнаружении движения.

Чтобы выполнять непрерывную запись:

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Выберите камеру.
3. Установите флажок **Continuous (Непрерывная запись)**.
4. Настройте параметры. Дополнительные сведения см. в таблице ниже.
5. Нажмите **Применить**.

Профиль	Выберите профиль в раскрывающемся списке **Profile (Профиль)**. По умолчанию выбран профиль **High (Высокое качество)**. Чтобы уменьшить размер записи используйте более низкое разрешение. Чтобы изменить параметры профиля, ознакомьтесь с разделом *Профили потоков*.
Расписание	Задайте расписание записей. Чтобы снизить нагрузку на пространство хранилища, осуществляйте запись только в определенные периоды времени.
средний битрейт	Включите этот параметр, чтобы установить максимальный объем хранилища.. Система отображает значение среднего битрейта, рассчитанного на основе заданного максимального объема хранилища и срока хранения. Максимальный средний битрейт составляет 50000 Кбит/с. См. *Настройка среднего битрейта, on page 92*.

Запись в ручном режиме

Порядок настройки параметров записи в ручном режиме:

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Выберите камеру.
3. Установите флажок **Manual (Вручную)**.
4. Настройте параметры. Дополнительные сведения см. в таблице ниже.
5. Нажмите **Применить**.

Профиль	Выберите профиль в раскрывающемся списке **Profile (Профиль)**. По умолчанию выбран профиль **High (Высокое качество)**. Чтобы уменьшить размер записи используйте более низкое разрешение. Чтобы изменить параметры профиля, ознакомьтесь с разделом *Профили потоков*.
Категория события	При необходимости можно выбрать категорию события, к которой должна относиться запись.
Буфер перед тревогой	Задайте количество секунд до нажатия кнопки записи, которые будут включены в запись.
Буфер после тревоги	Задайте количество секунд после остановки записи, которые будут включены в запись.
Создание закладки при записи	Добавляет сведения о закладке при каждом запуске ручной записи. Закладки помогают находить и идентифицировать конкретные записи позднее. Этот параметр применяется только к операторам и администраторам и по умолчанию отключен.
Максимальная продолжительность	Задайте максимальную длительность каждой записи, без учета времени предварительного и последующего буфера. Установите значение 0 для неограниченной длительности.

Дополнительную информацию о ручной записи см. в *Запись в ручном режиме*.

Rule-triggered recording (Запись по правилу)

Запись, активируемая правилом, запускается и останавливается в соответствии с правилом, созданным в разделе Action rules (Правила действий). Вы можете использовать правила, например, для создания записей, активируемых сигналами от портов ввода-вывода или событиями устройств. Правило может содержать несколько триггеров.

Инструкции по созданию записи по правилу см. в *Правила действия*.

Примечание

При использовании правила для настройки включения записи по обнаружению движения, не забудьте отключить этот режим во избежание двойной записи.

Резервная запись

Используйте запись при отказе соединения для сохранения записей на SD-карту камеры при потере соединения с AXIS Camera Station Pro.

AXIS Camera Station Pro автоматически выбирает метод записи при отказе в зависимости от версии встроенного ПО камеры:

- **Встроенное ПО версии 11.11.42 или более поздней**: запись при отказе соединения начинается каждый раз, когда камера теряет связь с сервером.
- **Более ранние версии встроенного ПО**: запись при отказе соединения начинается только при неожиданной потере соединения. Плановые перезапуски сервера не запускают запись при отказе соединения.

Инструкции по настройке записи при отказе соединения см. в разделе *Выбор устройств хранения для подключения, on page 84*.

Примечание

- При обновлении, если ранее была включена **запись при отказе соединения**, параметр **Copy SD card recordings to ACS Pro server (Копировать записи с SD-карты на сервер ACS Pro)** включается автоматически.
- Записи на SD-карте не удаляются с помощью AXIS Camera Station Pro. Срок их хранения определяется параметром срока хранения записей на SD-карте в камере.
- Включение записи при отказе соединения перезаписывает существующую конфигурацию записи при отказе соединения для этой камеры на других серверах.
- Для одного представления камеры запись при отказе соединения может быть одновременно активна только для одного сервера AXIS Camera Station Pro.

После восстановления соединения, если включен параметр **Copy SD card recordings to ACS Pro server (Копировать записи с SD-карты на сервер ACS Pro)**, записи копируются на сервер и отмечаются темно-серым цветом на временной шкале. Камера использует предварительный и последующий буфер длительностью 20 секунд, однако по-прежнему могут возникать короткие разрывы продолжительностью от 1 до 4 секунд.

Способы записи	
Обнаружение движения с буфером перед тревогой	Если соединение потеряно более чем на 20 секунд, камера непрерывно записывает на SD-карту до восстановления соединения или до заполнения SD-карты.
Обнаружение движения без буфера перед тревогой	• Если соединение потеряно более чем на 20 секунд, и запись по событию движения в данный момент не производится, резервная запись не начинается. • Если соединение потеряно более чем на 20 секунд, и запись по событию движения в данный момент производится, резервная запись начинается и продолжается до восстановления соединения или заполнения SD-карты.
Непрерывная запись	Если соединение потеряно более чем на 20 секунд, камера непрерывно записывает на SD-карту до восстановления соединения или до заполнения SD-карты.

Используйте SD-карту для резервной записи

Резервная запись

Резервную запись можно включить на устройстве, на котором используется AXIS S3008 Recorder для хранения записей. После включения устройство автоматически начинает непрерывную запись при потере соединения между AXIS Camera Station Pro и записывающим устройством. Для резервной записи устройство использует профиль потока Medium (Средний).

Примечание

- Для работы этой функции требуется AXIS Camera Station 5.36 или более поздней версии, встроенное ПО AXIS S3008 Recorder версии 10.4 или более поздней и встроенное ПО устройства Axis версии 5.50 или более поздней.
- Если в момент запуска резервной записи уже выполняется непрерывная запись, начинается новая непрерывная запись. Система создает дубликаты потока на видеорегистраторе.

Для включения резервной записи:

1. Убедитесь, что вы добавили AXIS S3008 Recorder и устройства и выбрали записывающее устройство в качестве хранилища записей для устройства. См. *Настройка видеорегистраторов AXIS OS Recorder*.
2. Откройте меню **Конфигурация > Устройство хранения > Выбор**.
3. Выберите устройство и пункт **Fallback recording (Резервная запись)**.
4. Нажмите **Применить**.

Способ записи

AXIS Camera Station Proавтоматически настраивает запись по детектору движения или непрерывную запись при добавлении устройств.

Флажок указывает способ записи, используемый устройством. Порядок настройки параметров профиля видео и аудио см. в разделе *Профили потоков*.

Для изменения способа записи:

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Выберите одно или несколько устройств.
   Для устройств одной и той же модели можно одновременно настраивать несколько устройств.
3. На странице **Recording method (Способ записи)** включите или отключите способ записи.

Примечание

Обнаружение движения в зонах просмотра не поддерживается.

Настройка среднего битрейта

В режиме усреднения битрейт автоматически регулируется на протяжении длительного времени. Это позволяет обеспечить заданную целевую скорость передачи данных и хорошее качество видео с учетом указанного объема хранилища.

Примечание

- Этот параметр доступен только для непрерывной записи. Камеры должны поддерживать среднюю скорость передачи данных и иметь встроенное ПО версии 9.40 или более поздней.
- Параметры среднего битрейта влияют на качество выбранного профиля потока.

1. Перейдите в **Configuration (Конфигурация) > Storage (Хранилище) > Selection (Выбор)** и убедитесь, что для камеры задан ограниченный срок хранения записей.
2. Перейдите к пункту **Configuration > Devices > Stream profiles (Конфигурация > Устройства > Профили потока)** и проверьте, что в качестве формата, используемого для непрерывной записи, используется формат H.264 или H.265.
3. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
4. Выберите камеру и активируйте пункт **Continuous (Непрерывная)**.
5. В разделе **Video settings (Параметры видео)** выберите настроенный вами профиль видеопотока.
6. Включите параметр **Average bitrate (Средний битрейт)** и задайте значение для параметра **Max storage (Макс. объем устройства хранения)**. Система отображает значение среднего битрейта, рассчитанного на основе заданного максимального объема хранилища и срока хранения. Максимальный средний битрейт составляет 50 000 Кбит/с.

Примечание

Max storage (Максимальный объем устройства хранения) — это максимальное место, доступное для записей в течение срока хранения. Это гарантирует только то, что объем записей не превысит указанное пространство, но не гарантирует наличие достаточного места для хранения записей.

7. Нажмите **Применить**.

Редактирование настроек детектора движения

Если ваше устройство использует AXIS Object Analytics, вы можете изменить параметры записи по движению в соответствующем разделе.

Примечание

Для AXIS Object Analytics в AXIS Camera Station Pro требуется AXIS OS 12.4.

1. Откройте вкладку **Configuration (Конфигурация)**.

2. Перейдите к пункту **Recording and events** > **Recording method** (Конфигурация > Записи и события > Способ записи).
3. Выберите камеру, которую требуется настроить.
4. Включите параметр **Motion detection (Детектор движения)**.
5. Нажмите **Motion settings (Параметры движения)**.

Подробную информацию по конфигурированию аналитического модуля *AXIS Object Analytics* см. в соответствующем руководстве пользователя.

Изменение настроек AXIS Video Motion Detection 2 и 4

AXIS Video Motion Detection 2 и AXIS Video Motion Detection 4 — приложения для камер, предназначенные для устройств с поддержкой AXIS Camera Application Platform. Если на камере установлено приложение AXIS Video Motion Detection 2 или 4, то производится обнаружение движения в области детекции. Для AXIS Video Motion Detection 2 требуется встроенное ПО версии 5.60 или более поздней, а для AXIS Video Motion Detection 4 требуется встроенное ПО версии 6.50 или более поздней. Вы также можете ознакомиться с заметками о выпуске для встроенного ПО ваших устройств, чтобы убедиться в том, что используемая версия поддерживает Video Motion Detection 4.

Если при добавлении камер в AXIS Camera Station Pro выбрать запись по движению, AXIS Video Motion Detection 2 и AXIS Video Motion Detection 4 устанавливаются на камеры с необходимой версией микропрограммы. Камеры без необходимой версии встроенного ПО используют встроенную функцию обнаружение движения. Приложение можно установить в ручном режиме, перейдя на страницу управления устройствами. См. *Установка приложений для камер*.

Используя AXIS Video Motion Detection 2 и 4, можно создать:

- **Область детекции**: область записи, в которой камера обнаруживает движущиеся объекты. При использовании данной функции игнорируются объекты за пределами области детекции. Данная область отображается в виде многоугольника поверх видеоизображения. Эта область может иметь от 3 до 20 вершин (углов).
- **Исключаемая область**: область внутри области интереса, в которой движущиеся объекты игнорируются.
- **Фильтры игнорирования:** позволяют создавать фильтры для игнорирования движущихся объектов, обнаруженных приложением. Старайтесь использовать как можно меньше фильтров и тщательно настраивайте их, чтобы не допустить игнорирования важных объектов. Использовать и настраивать фильтры следует по одному.
  - **Фильтр кратковременно присутвующих объектов**: игнорирует объекты, которые появляются в кадре только на короткое время. Например, свет фар проезжающего автомобиля, а также быстро перемещающиеся тени. Задайте минимальное время, в течение которого объект должен отображаться на изображении, чтобы возник сигнал тревоги. Отсчет времени начинается с момента обнаружения объекта приложением. Фильтр задерживает формирование тревоги и не запускает ее, если объект исчезает из кадра в течение заданного времени.
  - **Фильтр мелких объектов**: этот фильтр игнорирует мелкие объекты, такие как животные. Задайте ширину и высоту объекта в процентах от общих размеров изображения. Фильтр игнорирует объекты, размеры которых меньше заданной ширины и высоты, и не запускает сигнал тревоги. Размеры соответствующего объекта должны быть меньше и по значению ширины, и по значению высоты, чтобы фильтр игнорировал его.
  - **Фильтр качающихся объектов**: игнорирует объекты, перемещающиеся лишь на небольшое расстояние, например колышущуюся листву, флаги и их тени. Задайте расстояние в процентах от общего размера изображения. Фильтр игнорирует объекты, диапазон перемещений которых меньше, чем расстояние между центром эллипса и концом одной из стрелок. Эллипс служит в качестве меры перемещения и применяется к любому движущемуся объекту на изображении независимо от расположения этого эллипса.

Как настроить параметры движения:

Примечание

Эти настройки применяются непосредственно к камере.

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Выберите камеру с AXIS Video Motion Detection 2 или AXIS Video Motion Detection 4 и нажмите **Motion Settings (Настройки обнаружения движения)**.
3. Измените область наблюдения.
4. Измените область исключения.
5. Создайте фильтры, позволяющие игнорировать объекты.
6. Нажмите **Применить**.

Добавление новой вершины	Чтобы добавить новую вершину в область детекции, щелкните линию между двумя вершинами.
Удаление вершины	Чтобы удалить вершину из области детекции, щелкните ее и нажмите **Remove Point (Удалить вершину)**.
Добавление области исключения	Чтобы создать область исключения, щелкните **Add Exclude Area (Добавить область исключения)** и щелкните линию между двумя вершинами.
Удаление области исключения	Чтобы удалить область исключения, нажмите **Удалить область исключения**.
Фильтр Short lived objects (Кратковременно присутствующие объекты)	Чтобы использовать фильтр кратковременных объектов, установите флажок **Short lived objects filter (Фильтр кратковременно присутствующих объектов)** и с помощью ползунка **Time (Время)** задайте минимальное время, в течение которого объект должен находиться в кадре для формирования сигнала тревоги.
Фильтр Small objects (Мелкие объекты)	Чтобы использовать фильтр для мелких объектов, выберите **Small objects filter (Фильтр мелких объектов)** и задайте размер игнорируемых объектов с помощью ползунков **Width (Ширина)** и **Height (Высота)**.
Фильтр Swaying objects (Качающиеся объекты)	Чтобы использовать фильтр качающихся объектов, установите флажок **Swaying objects filter (Фильтр качающихся объектов)** и с помощью ползунка **Distance (Расстояние)** настройте размер эллипса.

Настройка встроенного видеодетектора движения

При использовании встроенного обнаружения движения камера обнаруживает движение в одной или нескольких зонах включения и игнорирует все остальные движения. Зона наблюдения — это область, в которой обнаруживается движение. Можно использовать несколько зон включения и исключения, а также размещать зону исключения внутри зоны включения, чтобы игнорировать определенное движение.

Чтобы добавить или изменить зону наблюдения:

Примечание

Эти настройки применяются непосредственно к камере.

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.

2. Выберите камеру со встроенным детектором движения и нажмите **Параметры движения**.
3. В разделе работы с окнами нажмите **Add (Удалить)**.
4. Выберите **Include (Включить)**.
5. Чтобы просматривать только редактируемую область, выберите **Show selected window (Показывать выбранную область)**.
6. Измените местоположение и размер фигуры на видеоизображении. Это зона наблюдения.
7. Настройте параметры **Object size (Размер объекта)**, **History (История)** и **Sensitivity (Чувствительность)**.
8. Чтобы использовать предустановленные параметры, выберите **Low (Низкая)**, **Moderate (Средняя)**, **High (Высокая)** или **Very High (Очень высокая)**. **Низкий** — обнаружение крупных объектов с короткой историей. **Повышенный** — обнаружение мелких объектов с продолжительной историей.
9. Перейдите в раздел **Activity (Активность)** и проверьте обнаруженное движение в зоне наблюдения. Пики красного цвета указывают на движение. Используйте поле **Activity (Активность)** для корректировки значений параметров **Object size (Размер объекта)**, **History (История)** и **Sensitivity (Чувствительность)**.
10. Нажмите кнопку **OK**.

Размер предметов, от которых	берется размер объекта относительно размера всего участка. На верхнем уровне камера обнаруживает только очень крупные объекты. На нижнем уровне она обнаруживает даже очень мелкие объекты.
История	Задается длительность пребывания объекта в пределах заданной области, чтобы определить, можно ли считать его неподвижным. При высоком значении объект вызывает обнаружение движения в течение длительного времени. При низком значении объект вызывает обнаружение движения в течение короткого времени. Если в заданной области не должны появляться посторонние объекты, выберите очень большую величину длительности пребывания объекта в этой области (большое значение параметра «История»). Этот триггер обнаруживает движение, если объект присутствует в данной области.
Чувствительность	разница в освещенности фона и объекта. При высокой чувствительности камера обнаруживает обычно окрашенные объекты на обычном фоне. При низкой чувствительности она обнаруживает только очень яркие объекты на темном фоне. Чтобы обнаруживать только мигающий свет, выберите низкую чувствительность. В остальных случаях рекомендуем использовать высокую чувствительность.

Чтобы добавить и изменить область исключения:

1. В окне **Edit Motion Detection (Настройка обнаружения движения)** нажмите **Add (Добавить)** в разделе **Window (Область)**.
2. Выберите **Exclude (Исключить)**.
3. Измените местоположение и размер затемненной фигуры на видеоизображении.
4. Нажмите кнопку **OK**.

Чтобы удалить зону наблюдения или область исключения:

1. На экране **Edit Motion Detection (Изменение параметров обнаружения движения)** выберите область, которую требуется удалить.
2. Выберите пункт **Remove (Удалить)**.
3. Нажмите кнопку **OK**.

Настроить категории событий

Категории событий упрощают поиск записей определенного типа. Чтобы создать категорию событий:

1. Перейдите в меню **Configuration (Конфигурация)** > **Recording and events (Записи и события)** > **Event categories (Категории событий)**.
2. Щелкните **New (Новое)**.
3. Введите название категории событий.
4. Вы также можете задать цвет и пользовательское время хранения записей для категории событий.
5. Нажмите **Применить**.

Название	Рекомендуется использовать для категории название, соответствующее типу события (например, нападение или остановка на дороге).
Время хранения записей	Для каждой категории событий можно установить отдельное время хранения, которое переопределяет время хранения, заданное по умолчанию для камеры. Особое время хранения для категории событий применяется только в том случае, если оно превышает время, заданное по умолчанию.

Для получения дополнительных сведений см. *Категории событий, on page 29*.

Порты ввода/вывода

Многие камеры и видеокодеры имеют порты ввода-вывода для подключения внешних устройств. Некоторые дополнительные устройства также могут иметь порты ввода/вывода.

Имеется два вида портов ввода-вывода:

Входной порт – Используйте для подключения устройств, которые могут изменять состояние сигнальной цепи с разомкнутого на замкнутое и наоборот. Например, дверные и оконные датчики, дымовые пожарные извещатели, стеклянные пожарные извещатели, PIR (пассивные инфракрасные детекторы).

Выходной порт – Используйте для подключения таких устройств как реле, двери, замки, сигнализаторы. Приложение AXIS Camera Station Pro может управлять устройствами, подключенными к выходным портам.

Примечание

- При подключении к нескольким серверам AXIS Camera Station Pro можно выбрать любой подключенный сервер в раскрывающемся списке **Selected server (Выбранный сервер)** для добавления портов ввода-вывода и управления ими.
- Администраторы могут отключить для пользователей доступ к портам ввода/вывода. См. *Права доступа пользователей*.

Правила действий используют порты ввода/вывода в качестве триггеров или действий. Триггеры используют входные сигналы. Например, когда AXIS Camera Station Pro получает сигнал от устройства, подключенного к входному порту, выполняются заданные действия. Действия используют выходные

порты. Например, при активации правила AXIS Camera Station Pro может активировать или деактивировать устройство, подключенное к порту вывода. См. *Правила действия*.

Сведения о подключении устройств и настройке портов ввода-вывода см. в руководстве пользователя или руководстве по установке соответствующего продукта Axis. Порты некоторых устройств могут действовать как входные, так и как выходные порты.

Управление портами вывода можно осуществлять вручную. См. *Мониторинг портов ввода-вывода*.

Добавить порты ввода-вывода

Чтобы добавить порты ввода-вывода:

1. Перейдите в меню **Конфигурация > Записи и события > Порты ввода-вывода**.
2. Чтобы просмотреть список портов ввода/вывода, которые можно добавить, нажмите **Add (Добавить)**.
3. Выберите соответствующий порт и нажмите **OK**.
4. Проверьте информацию в разделах **Type (Тип)** и **Device (Устройство)**. При необходимости обновите.
5. Введите название в поля **Port (Порт)**, **Active State (Активное состояние)** и **Inactive State (Неактивное состояние)**. Данные имена также отображаются в правилах действий, журналах и контроля ввода/вывода.
6. Для выходных портов можно задать исходное состояние, в которое они должны переходить при подключении AXIS Camera Station Pro к устройству. Выберите **On startup set to (При запуске установить в)** и выберите исходное состояние в раскрывающемся списке **State (Состояние)**.

Изменить	Чтобы изменить порт, выберите его и нажмите **Edit (Изменить)**. В диалоговом окне измените сведения о порте и нажмите **OK**.
Удалить	Чтобы удалить порт, выберите его и нажмите **Remove (Удалить)**.
Перезагрузка портов ввода/вывода	Если вы настроили порты ввода-вывода на странице конфигурации устройства, нажмите **Reload I/O Ports (Повторно загрузить порты ввода-вывода)**, чтобы обновить список.

Мониторинг портов ввода-вывода

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro можно выбрать любой подключенный сервер в раскрывающемся списке **Selected server (Выбранный сервер)** для контроля портов ввода-вывода.

Управление портами вывода можно осуществлять вручную:

1. Выберите > **Actions (Действия) > I/O Monitoring (Мониторинг портов ввода-вывода)**.
2. Выберите выходной порт.
3. Щелкните **Change state (Изменить состояние)**.

Правила действия

Используйте правила действий для автоматического реагирования на события. Например, отправляйте электронное письмо, когда камера обнаруживает движение вне рабочего времени, взаимодействуйте с устройствами, подключенными к портам ввода-вывода, и оповещайте операторов о важных событиях.

Каждое правило имеет триггеры (события, активирующие правило), действия (что происходит при срабатывании) и необязательное расписание. При активации триггеров правило выполняет все действия.

Примечание

- При подключении к нескольким серверам AXIS Camera Station Pro можно создать и управлять правилами действий на любом из подключенных серверов. Для этого надо выбрать нужный сервер в раскрывающемся списке **Selected Server (Выбранный сервер)**.
- Действия, доступные для устройств стороннего производителя, могут различаться на разных устройствах. Для некоторых из этих действий требуется дополнительная настройка устройства.

Создайте новое правило действия

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New... (Новое...)**.
3. Дайте правилу название в поле **Название**.
4. В разделе **Schedule (Расписание)**, выберите **Always (Всегда)** или **Custom schedule (Расписание пользователя)** , чтобы выбрать расписание из раскрывающегося списка. Также можно создать новое расписание или изменить существующее.
5. В разделе **Triggers (Триггеры)** нажмите **Add...(Добавить)**, выберите тип триггера, выполните настройку и нажмите **OK**. См. *Добавление триггеров* для получения дополнительной информации.
6. В разделе **Actions (Действия)** нажмите **Add... (Добавить...)**, выберите тип действия, настройте его и нажмите **OK**. См. *Добавление действий* для получения дополнительной информации.
7. Нажмите **Применить**.
   - Правило автоматически включается при его сохранении.

Изменить	Чтобы изменить существующее правило, выберите его и нажмите **Edit (Изменить)**.
Копировать	Чтобы скопировать существующее правило, выберите его и нажмите **Copy... (Копировать...)**.
Удалить	Чтобы удалить правило, выберите его и нажмите **Remove (Удалить)**.

Настроить несколько правил действий

При выборе нескольких правил отображаются только те триггеры и действия, которые совпадают во всех выбранных правилах. Все внесенные изменения применяются ко всем выбранным правилам.

- Перейдите в меню **Конфигурация > Записи и события > Правила действия.**
- Выберите несколько правил.
- Доступные изменения:
  - Добавление триггеров или действий, применяемых ко всем выбранным правилам.
  - Удаление общих триггеров или действий из всех выбранных правил.
  - Изменение расписания для всех выбранных правил.
- Нажмите **Применить**.

Примечание

При выборе нескольких правил редактирование отдельных триггеров или действий невозможно. Если изменения приведут к некорректной конфигурации хотя бы одного правила, применить их будет невозможно.

Добавление триггеров

Триггеры активируют правила, и одно правило может иметь несколько триггеров. Правило остается активным, пока активен хотя бы один из триггеров. Если требуется, чтобы все триггеры были активными для данного правила, выберите **All triggers must be active simultaneously to trigger the actions (Для запуска действий должны быть одновременно активированы все инициирующие события)**. Если этот параметр используется с импульсными триггерами, увеличьте период срабатывания триггера. Импульсные триггеры — это триггеры, действующие немедленно.

Доступны следующие триггеры:

Детектор движения – Движение, зарегистрированное в определенной области, активирует триггер обнаружения движения. См. *Создание триггеров с помощью детектора движения, on page 99*.

всегда включена – Этот триггер будет всегда включен. Например, вы можете объединить этот триггер с расписанием, которое всегда включено, и действием записи с низким профилем, чтобы получить вторую непрерывную запись, подходящую для устройств с ограниченной производительностью.

Просмотр в реальном времени – Триггер живого просмотра срабатывает, когда пользователь открывает видеопоток конкретной камеры. Вы можете использовать это, например, чтобы с помощью светодиодов камеры дать знать людям, находящимся рядом с ней, что кто-то наблюдает за ними через эту камеру. См. *Создание триггеров живого просмотра, on page 100*.

Ошибка и событие системы – Триггер системного события и ошибки активируется при возникновении ошибок записи, заполнении хранилища, сбое подключения к сетевому хранилищу или потере соединения с одним или несколькими устройствами. См. *Создание триггеров на основе системных событий и сбоев, on page 100*.

Ввод/Вывод – Триггер ввода/вывода (I/O) активируется при поступлении сигнала тревоги на порт ввода/вывода устройства, например от подключенной двери, коммутатора или детектора дыма. См. *Создание триггеров ввода-вывода, on page 101*. По возможности рекомендуется использовать триггеры событий устройства вместо триггеров входов/выходов.

Событие устройства – Этот триггер использует события, поступающие непосредственно с камеры или вспомогательного устройства. Используйте этот триггер, если в AXIS Camera Station Pro нет подходящего триггера. См. *Создать триггеры по событиям на устройстве, on page 102*.

Кнопка действия – Используйте кнопки действия для запуска и остановки действий в режиме живого просмотра. Для разных правил можно использовать одну кнопку. См. *Создание триггеров для кнопок действий, on page 107*.

Событие AXIS Entry Manager – Данный триггер активируется, когда AXIS Camera Station Pro получает сигналы от дверей, настроенных в AXIS Entry Manager. Например, двери были принудительно открыты, открывались слишком долго или в случае запрещенного доступа. См. *Создание триггеров событий AXIS Entry Manager, on page 109*.

Внешний HTTPS – Внешний триггер HTTPS позволяет внешним приложениям активировать события в AXIS Camera Station Pro посредством обмена данными по протоколу HTTPS. См. *Создание внешних HTTPS-триггеров, on page 109*.

Создание триггеров с помощью детектора движения

Триггер обнаружение движения активируется, когда камера обнаруживает движение в зоне наблюдения. Поскольку обнаружение выполняется камерой, дополнительная нагрузка на AXIS Camera Station Pro не возникает.

Примечание

Не используйте триггеры обнаружения движения для запуска записи, если на камере уже включена запись при обнаружении движения. Прежде чем использовать триггеры обнаружения движения, отключите запись движения. Чтобы отключить запись движения, перейдите к пункту **Configuration > Recording and events > Recording method (Конфигурация > Записи и события > Способ записи)**.

Чтобы создать триггер обнаружения движения:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Добавить** и выберите **Детектор движения**.
4. Нажмите кнопку **OK**.
5. В диалоговом окне:
   5.1. Выберите камеру, которая должна обнаруживать движение.
   5.2. Задайте минимальный интервал между срабатываниями триггера, чтобы сократить количество следующих друг за другом записей. Если в течение этого интервала произойдет повторное срабатывание, запись продолжится, а отсчет интервала срабатывания начнется заново.
   5.3. Задайте параметры обнаружения движения, нажав **Параметры движения**. Доступные параметры зависят от модели камеры. См. *Настройка встроенного видеодетектора движения* и *Изменение настроек AXIS Video Motion Detection 2 и 4*.
6. Нажмите кнопку **OK**.

Создание триггеров живого просмотра

Триггер живого просмотра срабатывает, когда пользователь открывает видеопоток конкретной камеры. Вы можете использовать это, например, чтобы с помощью светодиодов камеры дать знать людям, находящимся рядом с ней, что кто-то наблюдает за ними через эту камеру.

Чтобы создать триггер живого просмотра:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Добавить** и выберите **Живой просмотр**.
4. Нажмите кнопку **OK**.
5. Выберите камеру для триггера.
6. Нажмите кнопку **OK**.

Создание триггеров на основе системных событий и сбоев

Выберите одно или несколько системных событий и сбоев, которые можно использовать в качестве триггеров. Примеры системных событий: ошибки записи, заполнение хранилища, сбой подключения к сетевому хранилищу и потеря соединения с одним или несколькими устройствами.

Чтобы создать триггер на основе системного события и сбоя:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Добавить** и выберите **Системное событие и сбой**.
4. Нажмите кнопку **OK**.
5. Выберите системное событие или сбой для создания триггера.
6. Нажмите кнопку **OK**.

При ошибке записи	Если выбрать **При ошибке записи**, то триггер активируется при возникновении ошибок во время записи, например, если прекращается передача потокового видео с камеры.
При заполнении ресурса хранения	Если выбрать **On full storage (При заполнении ресурса хранения)**, триггер будет срабатывать при

	заполнении ресурса хранения, используемого для записи.
При отсутствии связи с сетевым ресурсом хранения	Выберите **On no contact with network storage (При отсутствии связи с сетевым хранилищем)**, чтобы активировать триггер при возникновении проблемы с доступом к сетевому хранилищу.
При потери связи с камерой	Выберите **On lost connection to camera (При потере соединения с камерой)**, чтобы активировать триггер при возникновении проблемы с подключением к камерам.. • Выберите **All (Все)**, чтобы включить все камеры, добавленные в AXIS Camera Station Pro. • Выберите **Selected (Выбранные)** и нажмите **Cameras (Камеры)** для отображения списка всех камер, добавленных в AXIS Camera Station Pro. Используйте **Select all (Выбрать все)** или **Deselect all (Отменить выбор всех)**, чтобы выбрать все камеры или снять выделение со всех камер.

Создание триггеров ввода-вывода

Триггер ввода/вывода (I/O) активируется при поступлении сигнала тревоги на порт ввода/вывода устройства, например от подключенной двери, коммутатора или детектора дыма.

Примечание

- Прежде чем использовать триггер ввода/вывода, добавьте в AXIS Camera Station Pro соответствующий порт ввода/вывода. См. *Порты ввода/вывода*.
- По возможности рекомендуется использовать триггеры событий устройства вместо триггеров входов/выходов. Для получения дополнительных сведений см. *Создать триггеры по событиям на устройстве, on page 102*.

Чтобы создать триггер ввода-вывода:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Добавить** и выберите **Ввод/вывод**.
4. Нажмите кнопку **OK**.
5. В разделе **Trigger port and state (Инициирующий порт и состояние)** настройте порт ввода-вывода и параметры триггера.
6. Нажмите кнопку **OK**.

Инициирующий порт и состояние	
Порт ввода/вывода	В разделе **I/O port (Порт ввода-вывода)** выберите порт ввода или вывода.
Состояние триггера	В поле **Trigger state (Состояние триггера)** выберите состояние порта ввода-вывода, при котором триггер будет срабатывать. Перечень возможных состояний зависит от настройки порта.
Период действия триггера	Задайте минимальный интервал между двумя последовательными срабатываниями, чтобы избежать запуска записей подряд. Если в течение этого интервала произойдет повторное срабатывание, запись продолжится, а отсчет интервала срабатывания начнется заново.

Создать триггеры по событиям на устройстве

Этот триггер использует события, поступающие непосредственно с камеры или вспомогательного устройства. Используйте этот вариант, если в AXIS Camera Station Pro отсутствует подходящий триггер. Набор событий зависит от модели камеры. Для каждого события необходимо настроить один или несколько фильтров. Фильтры представляют собой условия, которые должны быть выполнены для срабатывания триггера события устройства. Дополнительные сведения о событиях и фильтрах для устройств Axis можно найти в документации VAPIX® на страницах *axis.com/partners* и *axis.com/vapix*

Чтобы создать триггер по событию на устройстве:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Добавить** и выберите **Событие на устройстве**.
4. Нажмите кнопку **OK**.
5. В разделе **Configure device event trigger (Настроить триггер в виде события устройства)** настройте инициирующее событие.

Примечание

Перечень возможных событий зависит от выбранного устройства. Устройства сторонних производителей могут потребовать дополнительной настройки для поддержки многих из этих событий.

6. В разделе **Filters (Фильтры)** выберите фильтры.
7. В разделе **Activity (Активность)** просмотрите изменение состояния триггера события устройства с течением времени. События бывают зависящими и не зависящими от предыстории. Ступенчатый график указывает на событие с состоянием. Прямая линия с импульсами указывает на событие без состояния.
8. Нажмите кнопку **OK**.

Настроить запуск по событию для устройства	
Устройство	В меню **Device (Устройство)** выберите камеру или дополнительное устройство.
Событие	В меню **Event (Событие)** выберите событие для использования в качестве триггера.
Период действия триггера	Задайте минимальный интервал между двумя последовательными срабатываниями, чтобы избежать запуска записей подряд. Если в течение этого интервала произойдет повторное срабатывание, запись продолжится, а отсчет интервала срабатывания начнется заново.

Примеры событий устройств

Категория	**Событие устройства**
Усилитель	Перегрузка усилителя
Управление звуком	Состояние цифрового сигнала
Источник звука	Детектор звука
Авторизация	Доступ предоставлен
	Запрос на доступ отклонен
Вызов	State (Состояние)
	Изменение состояния
	Качество сети
	Состояние учетной записи SIP
	Входящее видео
Корпус	Корпус открыт
Устройство	Защита от перегрузки по току в цепи питания через кольцо
Датчики устройства	Система готова
	Матрица PIR
Контроль за состоянием устройств	Система готова
Дверной датчик	Дверь открыта силой
	Обнаружены несанкционированные действия с дверью
	Дверь заперта
	Дверь открыта слишком долго
	Положение двери
	Дверь отперта
Буфер событий	Начало
Система регистрации событий	Пропущенные сигналы тревоги

	Пропущенные события
	Тревога
Вентилятор	Статус
Изменение глобальной сцены	Служба изображения
Сбой оборудования	Сбой устройства хранения
	Неисправность вентилятора
Обогреватель	Статус
Входные порты	Виртуальный вход
	Входной цифровой порт
	Ручной запуск
	Контролируемый входной порт
	Цифровой выходной порт
	Внешний вход
Light (Свет)	Статус
Изменение состояния освещения	Статус
СМИ	Изменение профиля
	Изменение конфигурации
Непрерывное наблюдение	Контрольный сигнал
Детектор движения с зонами	Движение
Сеть	Разрыв сетевого подключения Применимо только к событиям, используемым устройством, и неприменимо к событиям, используемым в AXIS Camera Station Pro.
	Добавление адреса
	Удаление адреса
Движение PTZ	Движение PTZ на канале <имя канала>
Предварительные установки PTZ	Достижение предустановленного положения PTZ на канале <имя канала>
Контроллер PTZ	Автослежение
	Очередь доступа к PTZ-управлению
	Ошибка PTZ
	PTZ готово
Конфигурация записи	Создание записи
	Удаление записи
	Отслеживание конфигурации

	Конфигурация записи
	Конфигурация задания записи
Удаленная камера	Состояние VAPIX
	Положение PTZ
Расписание	Импульс
	Интервал
	Запланированное событие
State (Состояние)	Активный
Хранилище	Неисправность устройства хранения
	Ведется запись
Системное сообщение	Ну удалось выполнить действие
Защита от несанкционированных действий	Обнаружен наклон
	Обнаружен удар
Датчики температуры	Рабочая температура выше допустимой
	Рабочая температура ниже допустимой
	В пределах рабочей температуры
	Рабочая температура выше или ниже допустимой
Триггер	Реле и выходы
	Цифровой вход
Видеодетектор движения	VMD 4: профиль <имя профиля>
	VMD 4: любой профиль
Видеодетектор движения Video Motion Detection 3	VMD 3
Источник видео	Тревога по движению
	Доступ к видеопотоку в режиме реального времени
	Дневной и ночной режимы видеонаблюдения
	Несанкционированные действия с камерой
	Уменьшение среднего битрейта
	Подключен источник видео

События устройства для сетевого дверного контроллера Axis

Событие устройства	Запуск правила действия
Авторизация	
Доступ предоставлен	Система предоставила доступ владельцу карты, когда он идентифицировал себя с использованием своих учетных данных.

ПИН-код под принуждением	Кто-то использовал свой PIN-код под принуждением. Это событие можно использовать, например, для активации скрытого сигнала тревоги.
Запрос на доступ отклонен	Система отказала в доступе владельцу карты, когда он идентифицировал себя с использованием своих учетных данных.
Двойной свайп	Владелец карты дважды провел свою карту. Двойное проведение карты позволяет владельцу карты изменить текущее состояние двери. В качестве примера, с его помощью можно отпереть дверь вне обычного графика.
Детектор защиты от передачи доступа	Кто-то использовал учетные данные, принадлежащие владельцу карты, который вошел в зону перед ним.
Авторизация с использованием правила двух человек	
Запрос доступа находится на рассмотрении	Первый из двух владельцев карт идентифицировал себя с помощью учетных данных.
Доступ предоставлен	Система предоставила доступ последнему владельцу карты, когда он идентифицировал себя с использованием своих учетных данных.
Корпус	
Корпус открыт	Когда корпус сетевого дверного контроллера снят или открыт. В частности, это можно использовать для отправки уведомления администратору о том, что корпус вскрыт для проведения техобслуживания или что кто-либо взломал корпус.
Контроль за состоянием устройств	
Система готова	Система находится в состоянии готовности. В частности, устройство Axis может распознавать состояние системы и отправлять уведомление администратору о начале работы системы. Выберите **Yes (Да)**, чтобы запускать правило действия, когда система находится в состоянии готовности. Правило может срабатывать только после запуска всех необходимых служб, например системы событий.
Дверной датчик	
Дверь открыта силой	Дверь открыта силой.
Обнаружены несанкционированные действия с дверью	Система обнаруживает следующие события: • корпус устройства открыт или закрыт; • движение устройства; • снятие подключенного считывающего устройства со стены; • попытка несанкционированных действий в отношении подключенного датчика положения двери, считывающего устройства или устройства REX. Для использования этого триггера включите **Supervised input (Контролируемый вход)** и проверьте установку оконечных резисторов на соответствующих входных портах дверного разъема.
Дверь заперта	Дверной замок закрыт.
Дверь открыта слишком долго	Дверь открыта слишком долго.

Положение двери	Дверной монитор указывает, что дверь открыта или закрыта.
Дверь отперта	Дверной замок остается незакрытым. Например, это состояние можно использовать, когда посетителям разрешено открывать дверь без предъявления учетных данных.
Входные порты	
Виртуальный вход	Изменяется состояние одного из виртуальных входных сигналов. Это событие может использоваться клиентом, например, руководителем, для инициирования различных действий. Выберите входной порт, переход которого в активное состояние должен запускать правило действия.
Входной цифровой порт	Изменяется состояние входного цифрового порта. Используйте этот триггер для запуска различных действий, например отправки уведомления или мигания индикатора состояния. Выберите входной порт, активное состояние которого должно запускать правило действия, или выберите **Any (Любой)**, если нужно, чтобы правило действия запускалось, когда любой входной порт становится активным.
Ручной запуск	Активирует ручной запуск. Используйте этот триггер для запуска или остановки правила действия вручную с помощью API-интерфейса VAPIX.
Внешний вход	Вход чрезвычайной ситуации активен или неактивен.
Сеть	
Разрыв сетевого подключения	Сеть теряет соединение. Применимо только к событиям устройства, но не к событиям, используемым AXIS Camera Station Pro.
Добавление адреса	Добавляется новый IP-адрес.
Удаление адреса	IP-адрес удален.
Расписание	
Запланированное событие	Изменяется состояние по предварительно заданному расписанию. Используйте этот параметр для записи видео в определенные периоды времени, например в рабочие часы или по выходным. Выберите расписание в раскрывающемся меню **Schedule (Расписание)**.
Системное сообщение	
Ну удалось выполнить действие	Когда не удается выполнить правило действия и появляется системное сообщение о сбое действия.
Триггер	
Цифровой вход	Физический цифровой входной порт активен или неактивен.

Создание триггеров для кнопок действий

Используйте кнопки действий для запуска и остановки действий в режиме живого просмотра. Кнопки действий находятся в нижней части окна живого просмотра или на карте. Можно использовать одну кнопку для нескольких камер и карт; для одной камеры или карты может быть несколько кнопок действий. Можно изменить расположение кнопок камеры при добавлении или редактировании кнопки действия для камеры.

Существует два вида кнопок действий:

Командные кнопки – Используется для запуска действия вручную. Используйте командные кнопки для выполнения действий, для которых не требуется кнопка остановки действия. Командная кнопка имеет надпись и всплывающую подсказку. Название кнопки — текст на кнопке. Наведите указатель мыши на кнопку, чтобы отобразилась всплывающая подсказка.

Пример: создайте кнопку для активации выхода на заданное время, формирования сигнала тревоги и отправки сообщения электронной почты.

Кнопки-переключатели – Используется для ручного запуска и остановки действия. Такая кнопка имеет два состояния: нажата и отпущена. При нажатии кнопка меняет состояние с одного на другое. По умолчанию кнопки-переключатели запускают действие, когда находятся во включенном состоянии, но также можно настроить запуск действия в выключенном состоянии.
Кнопка-переключатель имеет надпись в нажатом состоянии, надпись в отпущенном состоянии и всплывающую подсказку. Надписи в нажатом и отпущенном состоянии — это тексты, которые отображаются на кнопке, когда она нажата и отпущена соответственно. Наведите указатель мыши на кнопку, чтобы отобразилась всплывающая подсказка.

Пример: создайте кнопку для открытия и закрытия дверей, используя действие с выходом и установив для импульса значение «as long as any trigger is active (пока активен любой триггер)».

Чтобы создать триггер для кнопки действия:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Добавить** и выберите **Кнопка действия**.
4. Нажмите кнопку **OK**.
5. Выберите **Создать новую кнопку** или **Использовать существующую кнопку**. Нажмите **Next (Далее)**.
6. Если вы выбрали **Create new button (Создать новую кнопку)**:
   6.1. Выберите **Командная кнопка** или **Кнопка-переключатель**. Если вы хотите использовать кнопку-переключатель, которая будет запускать действие при отпускании кнопки, выберите **Запуск при отпускании кнопки**.
   6.2. Нажмите **Next (Далее)**.
   6.3. Добавьте метки и всплывающую подсказку для этой кнопки.

Примечание

Буква или число после первого знака подчеркивания в метке кнопки действия служит клавишей доступа к этой кнопке действия. Нажмите Alt и клавишу доступа, чтобы активировать кнопку действия. Например, если кнопке действия присвоено имя A_BC, то в режиме живого просмотра это имя изменится на ABC. Нажмите Alt + B, чтобы активировать кнопку действия.

7. Если вы выбрали **Use existing button (Использовать существующую кнопку)**:
   7.1. Найдите нужную кнопку или нажмите ее.
   7.2. Если выбрана существующая кнопка-переключатель, необходимо выбрать **Trigger on toggle (Срабатывание при включении)** или **Trigger on untoggle (Срабатывание при выключении)**.
   7.3. Нажмите **Next (Далее)**.
   7.4. Измените метки и всплывающую подсказку для этой кнопки.
8. В раскрывающемся меню выберите камеру или карту.
9. Чтобы добавить кнопку к нескольким камерам или картам, нажмите **Добавить к нескольким камерам** или **Добавить к нескольким картам**.
10. Если для камеры задано несколько кнопок действий, нажмите **Arrange (Расположить)**, чтобы изменить порядок расположения кнопок. Нажмите кнопку **OK**.

11. Нажмите **Next (Далее)**.

Создание триггеров событий AXIS Entry Manager

AXIS Camera Station Pro активирует триггер при получении сигналов от дверей, настроенных в AXIS Entry Manager. Например, двери были принудительно открыты, открывались слишком долго или в случае запрещенного доступа.

Примечание

Триггер события AXIS Entry Manager доступен, только если в AXIS Camera Station Pro добавлен сетевой дверной контроллер AXIS A1001 Network Door Controller.

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и выберите **AXIS Entry Manager event (Событие Axis Entry Manager)**.
4. Нажмите кнопку **OK**.
5. Выберите событие и дверь для активации триггера.
6. Нажмите кнопку **OK**.

Создание внешних HTTPS-триггеров

Внешний триггер HTTPS позволяет внешним приложениям активировать события в AXIS Camera Station Pro посредством обмена данными по протоколу HTTPS. Этот триггер поддерживает только обмен данными по протоколу HTTPS и требует действительных имени пользователя AXIS Camera Station Pro с указанием домена и пароля для HTTPS-запросов.

Следующие запросы поддерживаются HTTP-методом GET*. Также возможно использовать POST с данными JSON, указанными в теле запроса.

Примечание

- Запросы внешнего HTTPS-триггера можно тестировать только в Google Chrome.
- Внешний HTTPS-триггер использует те же порты, что и приложение для просмотра с мобильного телефона, см. «Порт мобильной связи» и «Мобильный порт для передачи видеопотока», описанные в разделе *Общие настройки сервера*.
- Активировать триггер с идентификатором "trigger1": `https://[address]:29204/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Деактивировать триггер с идентификатором "trigger1": `https://[address]:29204/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Активировать триггер с идентификатором "trigger1" и через 30 секунд автоматически деактивировать его: `https://[address]:29204/Acs/Api/TriggerFacade/ActivateDeactivateTrigger?{"triggerName":"trigger1","deactivateAfterSeconds":"30"}`

Примечание

Таймер автоматической деактивации отменяется, если этому триггеру отправляется любая другая команда.

- Активировать и сразу деактивировать триггер с идентификатором "trigger1" (импульс): `https://[address]:29204/Acs/Api/TriggerFacade/PulseTrigger?{"triggerName":"trigger1"}`

Чтобы создать внешний HTTPS-триггер:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. нажмите **New (Создать)**.
3. Нажмите **Добавить** и выберите **Внешний HTTPS**.
4. Нажмите кнопку **OK**.

5. Введите название триггера в поле **Trigger name (Имя триггера)**.
6. Просмотрите пример URL, в котором используется тот же адрес сервера, с помощью которого клиент выполнил вход. URL-адреса функционируют только после выполнения правила действия.
7. Нажмите кнопку **OK**.

Действия, предусмотренные для внешних HTTPS-триггеров

- Запросы активации и деактивации триггера подходят для действий, которые запускают и останавливают запись.
- Запросы импульсной активации и деактивации триггера подходят для таких действий как **подача сигнала тревоги** или **отправка сообщения по электронной почте**.

Создание триггеров Smart search 2

Чтобы создать триггер Smart search 2:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и выберите **Smart search 2**.
4. Нажмите кнопку **OK**.
5. Выберите и настройте триггер:
   - Чтобы создать фильтр умного поиска для использования как триггер, см. раздел *Триггеры, on page 185*.
   - Выберите **High processing delay (Высокая задержка обработки)**, чтобы активировать триггер, когда обработка обнаружений в Smart Search 2 занимает более одной минуты.
6. Нажмите кнопку **OK**.

Создание триггеров AXIS Audio Manager

Чтобы создать триггер AXIS Audio Manager:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и выберите **Audio manager (Аудиоменеджер)**.
4. Нажмите кнопку **OK**.
5. Выберите и настройте триггер.
6. Нажмите кнопку **OK**.

Состояние устройства изменено	Выберите **Device status changed (Изменение состояния устройства)**, чтобы активировать триггер при переходе устройства в состояние «в сети» или «не в сети».
Состояние воспроизведения изменено	Выберите **Playback status changed (Статус воспроизведения изменен)**, чтобы активировать триггер при старте или остановке воспроизведения.

Включение и выключение целевого объекта	Выберите **Target enabled or disabled (Целевое устройство включено или отключено)**, чтобы активировать триггер при включении или отключении целевого устройства.
Настройка громкости изменена	Выберите **Volume controller volume changed (Изменение уровня громкости)**, чтобы активировать триггер при изменении параметров громкости.

Добавление действий

Одно правило может иметь несколько действий. Действия выполняются при срабатывании правила.

Доступны следующие действия:

Запись – Запускает запись с камеры. См. *Создание действия «Запись»*.

Поднять тревогу – Отправляет сигнал тревоги всем подключенным клиентам AXIS Camera Station Pro. См. *Создание действий подачи сигналов тревоги*.

Задать выходной сигнал – Устанавливает состояние выходного порта. Используйте это действие для управления устройством, подключенным к выходному порту, например для включения освещения или запирания двери. См. *Создание действий для выходных портов*.

Отправка письма по электронной почте – Отправляет сообщение электронной почты одному или нескольким получателям. См. *Создание действий отправки электронной почты*.

Просмотр в реальном времени – Открывает режим просмотра в реальном времени для выбранной камеры, представления или предустановленной позиции во всех подключенных клиентах AXIS Camera Station Pro. Действие Live view (Живой просмотр) также можно использовать, чтобы восстановить свернутые на панели задач окна клиентов или вывести их поверх других открытых приложений. См. *Создание действий живого просмотра*.

Отправить HTTP-уведомление – Отправляет HTTP-запрос на камеру, дверной контроллер или внешний веб-сервер. См. *Создание действий для отправки HTTP-уведомлений*.

Сирена и освещение – Запускает сирену и световую индикацию на совместимом устройстве в соответствии с предварительно настроенным профилем. См. *Создание действий для сирены и освещения, on page 117*.

Virtual I/O (Виртуальный вход/выход) – Активирует определенный виртуальный входной порт устройства. См. *Создание действий виртуального ввода/вывода, on page 117*

Система AXIS Entry Manager – Предоставляет доступ, разблокирует или блокирует дверь, подключенную к контроллеру двери, настроенному с помощью AXIS Entry Manager. См. *Создание действий AXIS Entry Manager, on page 118*.

Отправить уведомление мобильного приложения – Отправляет пользовательское сообщение в мобильное приложение AXIS Camera Station. См. *Создание действий для отправки уведомления мобильному приложению, on page 118*.

Включение или выключение правил – Включает или отключает другие правила действий. См. *Создать действие, которое включает и выключает другие правила действий., on page 119*.

Отправить на видеодекодер – Отправляет представление на видеодекодер для отображения на мониторе в течение заданного времени. См. *Создайте действие, которое отправляет вид на видеодекодер, on page 119*

Контроль доступа – Включает действия с дверями и зонами в AXIS Camera Station Secure Entry. См. *Создание действий контроля доступа, on page 120*.

Создание действия «Запись»

Действие «Запись» включает запись с выбранной камеры. Открывайте и воспроизводите записи на вкладке **Recordings (Записи)**.

Чтобы создать действие «Запись»:

1. Укажите место сохранения записей: перейдите в **Configuration (Конфигурация) > Storage (Хранилище) > Selection (Выбор)**.
2. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
3. Щелкните **New (Новое)**.
4. Для создания триггера нажмите **Добавить**. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
5. Нажмите **Добавить** и выберите **Запись**.
6. Нажмите кнопку **OK**.
7. В разделе **Camera (Камера)** выберите камеру, с которой необходимо вести запись.
8. В разделе **Video setting (Параметры видео)** настройте профиль, буфер перед тревогой и буфер после тревоги.
9. В разделе **Event setting (Настройка события)** при необходимости выберите категорию события для записи.
10. Нажмите кнопку **OK**.

Настройки видео	
Профиль	Выберите профиль в раскрывающемся меню **Profile (Профиль)**. Чтобы изменить параметры профиля, ознакомьтесь с разделом *Профили потоков*.
Буфер перед тревогой	Задайте число секунд до обнаружения движения для включения в запись.
Буфер после тревоги	Задайте количество секунд, которые необходимо добавить к записи после завершения действия.

Создание действий подачи сигналов тревоги

Действие подачи сигнала тревоги заключается в отправке сигнала тревоги на все подключенные клиенты AXIS Camera Station Pro. Сигнал тревоги отображается на вкладке **Alarms (Сигналы тревоги)** и в виде уведомления на панели задач. К сигналу тревоги можно прикрепить файл с процедурами обработки сигналов тревоги. Этот файл доступен при переходе на вкладки **Тревоги** и **Журналы**.

Чтобы создать действие подачи сигнала тревоги:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Добавить** и выберите **Подать сигнал тревоги**.
5. Нажмите кнопку **OK**.
6. В разделе **Alarm message (Сообщение о сигнале тревоги)** настройте заголовок, описание и длительность.
7. Настройте **Alarm procedure (Процедуру обработки сигнала тревоги)**.
   7.1. Выберите **On alarm show alarm procedure (При сигнале тревоги показывать процедуру обработки сигнала тревоги)**.

7.2. Нажмите **Upload (Загрузить)** и выберите файл.

7.3. Нажмите **Preview (Предварительный просмотр)**, чтобы просмотреть файл.

7.4. Нажмите кнопку **OK**.

Сообщение тревоги	
Заголовок	Введите заголовок сообщения о тревоге. Заголовок отображается в разделе **Alarms (Сигналы тревоги)** на вкладке **Alarms (Сигналы тревоги)**, а также в уведомлении на панели задач.
Описание	Введите описание тревоги. Описание отображается в разделе **Alarms > Description (Сигналы тревоги > Описание)** на вкладке **Alarms (Сигналы тревоги)** и в уведомлении на панели задач.
Duration (s) (Длительность, с)	Задайте длительность всплывающих уведомлений от 1 до 600 секунд.

Создание действий для выходных портов

Выходное действие устанавливает состояние порта вывода. Используйте этот параметр для управления устройством, подключенным к порту вывода, например для включения освещения или запирания двери.

Примечание

Прежде чем применить действие для выходного порта, необходимо добавить порт вывода в AXIS Camera Station Pro. См. *Порты ввода/вывода*.

Чтобы создать действие для выходного порта:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Добавить** и выберите **Создать действие на выходе**.
5. Нажмите кнопку **OK**.
6. В разделе **Output port (Порт вывода)** выберите порт вывода.
7. В разделе **State on action (Состояние при действии)** выберите состояние, в которое необходимо установить порт. Доступные параметры зависят от конфигурации порта.
8. Выберите **Pulse (Импульс)**, чтобы задать продолжительность нахождения порта вывода в новом состоянии.

Примечание

Чтобы порт оставался в новом состоянии после выполнения действия, снимите флажок **Импульс**.

9. Нажмите кнопку **OK**.

До тех пор пока активен какой либо триггер	Чтобы порт оставался в новом состоянии в течение всего времени, пока активны триггеры в правиле, выберите **До тех пор, пока активен какой-либо триггер**.
Сохранять состояние в течение фиксированного времени	Чтобы порт оставался в новом состоянии в течение заданного времени, выберите **Keep the state for a fixed time (Сохранять состояние в течение заданного времени)** и укажите количество секунд.

Создание действий отправки электронной почты

Действие отправки электронной почты служит для отправки сообщения по электронной почте одному или нескольким получателям. Вы можете вложить в электронную почту стоп-кадры с камер.

Примечание

Для отправки сообщений электронной почты необходимо сначала настроить SMTP-сервер. См. *Параметры сервера*.

Чтобы создать действие отправки электронной почты:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Добавить** и выберите **Отправить сообщение по электронной почте**.
5. Нажмите кнопку **OK**.
6. В разделе **Recipients (Получатели)** добавьте адреса электронной почты:
   6.1. Введите адрес электронной почты в поле **New Recipient (Новый получатель)** и выберите **Кому (To)**, **Копия (Cc)** или **Скрытая копия (Bcc)**.
   6.2. Нажмите **Добавить**.
7. В разделе **Contents (Содержание)** введите тему и сообщение электронной почты.
8. В разделе **Advanced (Дополнительно)** настройте вложения, количество сообщений электронной почты, а также интервалы.
9. Нажмите кнопку **OK**.

Расширенный набор	
Присоединить моментальный снимок	Чтобы прикрепить снимки в формате JPG с камер, выберите **Attach snapshots (Прикреплять снимки)** и нажмите **Cameras (Камеры).** Появляется список всех камер, зарегистрированных для работы с ПО AXIS Camera Station Pro. Нажмите **Select all (Выбрать все)**, чтобы выбрать все камеры, или **Deselect all (Отменить выбор всех)**, чтобы снять выделение.
Отправлять одно электронное письмо для каждого события	Чтобы не отправлять несколько сообщений электронной почты об одном и том же событии, выберите **Send one email for each event (Отправлять одно сообщение электронной почты для каждого события)**.
Не отправлять следующее сообщение в течение	Чтобы сообщения электронной почты не отправлялись слишком часто, выберите **Don't send another email for (Не отправлять другое сообщение электронной почты в течение)** и задайте минимальный интервал между сообщениями в раскрывающемся списке.

Создание действий живого просмотра

Действие Live view (Живой просмотр) открывает выбранную камеру, представление или предустановленное положение на вкладке **Live view (Живой просмотр)** во всех подключенных клиентах AXIS Camera Station Pro. Если на вкладке **Live view (Живой просмотр)** отображается мультиэкранное представление с областью обзора, камера, выбранная в действии Live view (Живой просмотр),

отображается в области обзора. Для получения дополнительных сведений о главных областях наблюдения см. раздел *Мультиэкранный режим*.

Действие Live view (Живой просмотр) также можно использовать, чтобы восстановить открытые клиенты AXIS Camera Station Pro с панели задач или вывести их поверх других открытых приложений.

Чтобы создать действие живого просмотра:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Добавить** и выберите **Живой просмотр**.
5. Нажмите кнопку **OK**.
6. В разделе **Live view actions (Действия живого просмотра)** настройте содержимое, отображаемое при активации действия.
7. В разделе **Shown in (Показано в)** настройте способ отображения выбранного вида.
8. В разделе **Bring to front (На передний план)** выберите **On trigger bring application to front (При срабатывании выводить приложение на передний план)**, чтобы при запуске действия восстановить открытые клиенты AXIS Camera Station Pro с панели задач или вывести их поверх других открытых приложений.
9. Нажмите кнопку **OK**.

Действия просмотра живого видео	
Вид	Выберите **View (Представление)**, затем выберите представление в раскрывающемся списке.
Камера	Выберите **Camera (Камера)**, затем выберите камеру в раскрывающемся списке. Если камера поддерживает PTZ и имеет предустановленное положение, выберите **Go to preset (Перейти к предустановленному положению)** и выберите область в раскрывающемся списке, чтобы открыть предустановленное положение.
Действия нет	Выберите **No action (Без действия)**, если не требуется открывать представление.

Shown in (Показано в)	
Вкладка оповещений в режиме реального времени	Выберите вкладку **Live alert (Живое оповещение)**, чтобы открыть выбранный просмотр или вид с камеры на вкладке **живого оповещения**.
Главная область наблюдения	Выберите пункт **Hotspot in view (Главная область наблюдения)** и выберите вид с главной областью наблюдения в раскрывающемся меню. Если при срабатывании действия область обзора отображается в режиме живого просмотра, в ней появляется представление камеры.

Пример:
В этом примере в одном правиле действий используются два действия Live view (Живой просмотр).

1. Создайте действие живого просмотра, чтобы перейти к виду с главной областью наблюдения на вкладке **Live alert (Живое оповещение)**.

1.1. В разделе **Live view actions (Действия живого просмотра)** выберите **View (Просмотр)**.

1.2. Выберите **Hotspot view (Главная область наблюдения)**.

1.3. В разделе **Show in (Показать в)** выберите вкладку **Live alert (Живое оповещение)**.

1.4. Выберите **On trigger bring application to front (При срабатывании триггера переместить окно приложения наверх)**.

2. Создайте еще одно действие Live view (Живой просмотр), которое переходит к представлению с областью обзора и отображает представление камеры в области обзора.

2.1. В разделе **Live view actions (Действия живого просмотра)** выберите **Camera (Камера)**, а затем представление камеры.

2.2. В разделе **Show in (Показать в)** выберите **Hotspot in view (Главная область наблюдения)**.

2.3. Выберите **Hotspot view (Главная область наблюдения)**.

Создание действий для отправки HTTP-уведомлений

HTTP-уведомление подразумевает отправку HTTP-запроса получателю. Получателем может быть камера, дверной контроллер, внешний веб-сервер или любой сервер, способный принимать HTTP-запросы. Например, с помощью HTTP-уведомлений можно включать или отключать функцию на камере либо открывать, закрывать, запирать или отпирать дверь, подключенную к дверному контроллеру.

Поддерживаются методы GET, POST и PUT.

Примечание

Для отправки HTTP-уведомлений получателям за пределами локальной сети может потребоваться изменить параметры прокси-сервера AXIS Camera Station Pro. Обратитесь в службу поддержки Axis для получения дополнительной информации.

Чтобы создать действие для отправки HTTP-уведомлений:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Добавить** и выберите **Отправить HTTP-уведомление**.
5. Нажмите кнопку **OK**.
6. **URL** — введите адрес получателя и сценарий обработки запроса. Например: `https://192.168.254.10/cgi-bin/notify.cgi`.
7. Установите флажок **Требуется аутентификация**, если необходима аутентификация получателя. Введите имя пользователя и пароль.
8. Выберите способ аутентификации.
9. Для вывода дополнительных параметров на экран нажмите **Дополнительно**.
10. Нажмите кнопку **OK**.

Метод аутентификации	
Дайджест-авторизация	Рекомендуется выбрать этот вариант, поскольку он обеспечивает наилучшую защиту от перехвата данных.
Дайджест-авторизация с резервной базовой аутентификацией	Выберите этот параметр, если вы не знаете, какой способ аутентификации поддерживается устройством.

Расширенный набор	
Способ	В раскрывающемся списке **Method (Метод)** выберите метод HTTP.
Тип содержимого	В случае выбора метода POST или PUT выберите тип контента в раскрывающемся меню **Content type (Тип контента)**.
Основной текст	Для методов POST и PUT введите тело запроса в поле **Body (Тело)**.
Данные инициирующего события	В раскрывающемся меню также можно вставить предустановленные данные инициирующего события.

Данные инициирующего события	
Тип	Инициирующее событие, которое активировало данное правило действия.
Идентификатор источника	Указывает источник, вызвавший срабатывание правила действий. Чаще всего это камера или устройство другого типа. Источник может отсутствовать для некоторых типов.
Source name (Имя источника)	Имя источника, вызвавшего срабатывание правила действий. Чаще всего это камера или устройство другого типа. Источник может отсутствовать для некоторых типов.
Время (UTC)	Дата и время активации правила действия в формате UTC.
Время (местное)	Дата и время сервера на момент активации правила действия.

Создание действий виртуального ввода/вывода

Используйте действия виртуального ввода для активации определенного порта виртуального входа на устройстве. Каждый порт устройства можно использовать для одного действия.

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Add (Добавить)** и выберите **Virtual I/O (Виртуальный вход/выход)**.
5. Нажмите кнопку **OK**.
6. Выберите устройство и порт, который необходимо активировать.
7. Нажмите кнопку **OK**.

Создание действий для сирены и освещения

Действие сирены и освещения запускает шаблон работы сирены и освещения сетевой светозвуковой сирены AXIS D4100-E Network Strobe Siren в соответствии с заданным профилем.

Примечание

Для использования этого действия необходимо настроить профиль на странице конфигурации устройства.

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Add (Добавить)** и выберите **Siren and light (Сирена и освещение)**.
5. Нажмите кнопку **OK**.
6. Выберите устройство в раскрывающемся меню **Device (Устройство)**.
7. Выберите профиль в раскрывающемся меню **Profile (Профиль)**.
8. Нажмите кнопку **OK**.

Создание действий AXIS Entry Manager

Действие AXIS Entry Manager предоставляет доступ, разблокирует или блокирует дверь, подключенную к дверному контроллеру, настроенному с помощью AXIS Entry Manager.

Примечание

Действие AXIS Entry Manager доступно, только если в AXIS Camera Station Pro доступен сетевой дверной контроллер AXIS A1001 Network Door Controller.

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Add (Добавить)** и выберите **Axis Entry Manager**.
5. Нажмите кнопку **OK**.
6. Выберите действие и дверь, для которой оно будет выполняться.
7. Нажмите кнопку **OK**.

Создание действий для отправки уведомления мобильному приложению

Действие отправки уведомления мобильному приложению отправляет пользовательское сообщение в мобильное приложение AXIS Camera Station Mobile. Можно нажать полученное уведомление, чтобы перейти к определенному представлению с камеры. См. *Руководство пользователя по мобильному приложению AXIS Camera Station Mobile*.

Чтобы создать действие отправки уведомления мобильного приложения:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Add (Добавить)** и выберите **Send mobile app notification (Отправить уведомление мобильного приложения)**.
5. Нажмите кнопку **OK**.
6. В поле **Message (Сообщение)** введите сообщение, которое будет отображаться в мобильном приложении.
7. В разделе **Click notification and go to (Нажатие на уведомление и переход)** настройте содержимое, отображаемое при нажатии на уведомление.
8. Нажмите кнопку **OK**.

Щелкните уведомление и перейдите в	
Камера	Выберите представление с камеры, которое будет отображаться при нажатии на уведомление.
По умолчанию	Выберите **Default (По умолчанию)**, чтобы при нажатии на уведомление перейти на начальную страницу мобильного приложения.

Создать действие, которое включает и выключает другие правила действий.

Используйте это действие, например, чтобы отключить обнаружение движения в офисе, когда сотрудник прикладывает карту доступа к считывателю.

Чтобы создать действие включения или отключения правил:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Add (Добавить)** и выберите **Turn rules on or off (Включение или выключение правил)**.
5. Нажмите кнопку **OK**.
6. Выберите одно или несколько правил действий.
7. Выберите, необходимо ли включить или отключить выбранные правила действий.
8. Введите задержку, чтобы добавить интервал между срабатыванием и изменением состояния.
9. Выберите **Return to the previous state when the trigger is no longer active (Вернуться в предыдущее состояние, когда срабатывание прекращается)**, если не требуется сохранять измененное состояние правила действий после прекращения срабатывания. В приведенном выше примере это означает, что обнаружение движения снова включается, когда сотрудник убирает карту доступа со считывателя.
10. Нажмите кнопку **OK**.

Создать новую закладку

Действие добавления закладки добавляет закладку к записи в момент срабатывания правила действий.

Чтобы создать действие «Закладка»:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Add (Добавить)** и выберите **Add bookmark (Добавить закладку)**.
5. Нажмите кнопку **OK**.
6. Настройте закладку, введя имя и, при необходимости, описание.
7. Нажмите кнопку **OK**.

Создайте действие, которое отправляет вид на видеодекодер

Используйте это действие, чтобы отправить вид на видеодекодер для отображения на мониторе в течение заданного времени.

Чтобы создать действие отправки на видеодекодер:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.

2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Add (Добавить)** и выберите **Send to video decoder (Отправить на видеодекодер)**.
5. Нажмите кнопку **OK**.
6. В разделе **Decoder (Декодер)** выберите видеодекодер, на который будет отправлен вид.
7. На странице **View (Вид)** выберите камеру или вид для отправки.
8. В поле **Duration (Продолжительность)** введите время отображения представления в секундах.
9. Нажмите кнопку **OK**.

Создание действий контроля доступа

Действие контроля доступа может выполнять следующие операции в AXIS Camera Station Secure Entry:

- **Действия с дверями**: предоставить доступ, заблокировать, разблокировать, сбросить или перевести выбранные двери в режим блокировки.
- **Действия с зонами**: заблокировать, разблокировать, сбросить или перевести в режим блокировки выбранные двери в выбранных зонах.
- **Действия с правилами доступа**: включить или отключить правила доступа.

Примечание

Действие контроля доступа доступно только в AXIS Camera Station Secure Entry.

Чтобы создать действие контроля доступа:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Add (Добавить)** и выберите **Access control (Контроль доступа)**.
5. Нажмите кнопку **OK**.
6. Для выполнения действий с дверями:
   6.1. В разделе **Access control (Контроль доступа)** выберите **Door actions (Действия с дверями)**.
   6.2. В разделе **Configure action (Настройка действия)** выберите двери и действие.
7. Для выполнения действий с зонами:
   7.1. В разделе **Access control (Контроль доступа)** выберите **Zone actions (Действия с зонами)**.
   7.2. В разделе **Configure action (Настройка действия)** выберите зоны, типы дверей и действие.
8. Для включения или выключения правил доступа:
   8.1. В разделе **Access control (Контроль доступа)** выберите **Action rule actions (Действия с правилом действия)**.
   8.2. В разделе **Configure action (Настройка действия)** выберите правило доступа, которое нужно включить или отключить.
   8.3. В разделе **Action (Действие)**, выберите **Enable (Включить)** или **Disable (Выключить)**.
9. Нажмите кнопку **OK**.

- Чтобы сохранять отчеты для данного действия, нажмите **Save report** (Сохранить отчет) и задайте настройки отчета.

Создавать действия AXIS Audio Manager

Действие AXIS Audio Manager управляет воспроизведением аудио и настройками громкости на подключенных аудиоустройствах.

Чтобы создать действие AXIS Audio Manager:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Нажмите **Add (Добавить)** и настройте триггер. Нажмите **Next (Далее)**. См. *Добавление триггеров*.
4. Нажмите **Add (Добавить)** и выберите **Audio manager (Аудиоменеджер)**.
5. Нажмите кнопку **OK**.
6. Выберите и настройте действие, которое необходимо выполнить.
7. Нажмите кнопку **OK**.

Действия AXIS Audio Manager	
Воспроизвести аудиофайл	Выберите **Play audio file (Воспроизвести аудиофайл)** для воспроизведения выбранного аудиофайла. Можно также настроить параметры воспроизведения, например количество повторов, приоритет и визуальный профиль.
Остановить аудиофайл	Выберите **Stop audio file (Остановить аудиофайл)**, чтобы остановить воспроизведение аудио.
Включить или отключить целевое устройство	Выберите **Enable or disable target (Включить или отключить целевое устройство)**, чтобы включить или отключить устройства.
Отключить звук	Выберите **Mute volume (Отключить звук)** для отключения регулятора громкости.
Установить уровень громкости	Выберите **Set volume (Задать громкость)**, чтобы установить громкость регулятора громкости. Значение может быть положительным или отрицательным.
Смещение уровня громкости	Выберите **Offset volume (Изменить громкость относительно текущего значения)**, чтобы изменить громкость относительно текущего уровня. Введите положительное значение для увеличения громкости или отрицательное для ее уменьшения.

Расписания

На странице Schedules (Расписания) представлены все расписания, которые можно применять к записи, правилам действий и таким компонентам, как AXIS Secure Entry. Некоторые расписания автоматически создаются во время установки с помощью AXIS Site Designer.

Можно создавать и редактировать пользовательские ежедневные и еженедельные расписания, а также расписания переопределения. Расписания-переопределения всегда являются дневными, но могут применяться как к дневным, так и к недельным расписаниям в особые даты, например, в праздничные дни.

Вкладка **Schedules** (Расписания) — это основное представление, в котором можно управлять всеми ежедневными и еженедельными расписаниями.

- **Name (Имя)**: название расписания.
- **Type (Тип)**: указывает, является ли расписание ежедневным или еженедельным.

- **In use (Используется)**: указывает, используется ли расписание в данный момент компонентом, правилом записи или правилом действия.
- **Override schedules (Расписания переопределения)**: список расписаний переопределения, применяемых к этому расписанию.

Вкладка **Override schedules (Расписания переопределения)** является основным представлением для управления расписаниями переопределения. Здесь можно увидеть, какие ежедневные и еженедельные расписания переопределяет каждое из них.

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro можно добавлять расписания и управлять ими на любом из подключенных серверов. Выберите сервер в раскрывающемся списке **Selected server (Выбранный сервер)**, чтобы управлять расписаниями.

Управление ежедневными и еженедельными расписаниями

Чтобы управлять ежедневными и еженедельными расписаниями, перейдите на вкладку **Schedules** (Расписания).

Чтобы создать новое ежедневное или еженедельное расписание, нажмите **New schedule** (Новое расписание).

Чтобы удалить расписание, выберите его в списке и нажмите **Delete** (Удалить). Перед удалением убедитесь, что расписание не используется.

Создайте или выберите ежедневное либо еженедельное расписание, чтобы просмотреть подробные сведения о нем.

- Если выбрано ежедневное расписание, нажмите **Add dates** (Добавить даты), чтобы добавить к нему новый диапазон дат. К одному ежедневному расписанию можно добавить несколько диапазонов дат.
- Чтобы добавить временной интервал, нажмите **+** или дважды щелкните строку.
- Чтобы изменить диапазон дат или временной интервал, щелкните его левой кнопкой мыши.
- Чтобы добавить приоритетное расписание, выберите его в раскрывающемся меню и нажмите **Add** (Добавить). Чтобы удалить приоритетное расписание, выберите его в списке и нажмите **Remove** (Удалить).
- Нажмите **Apply** (Применить), чтобы сохранить изменения.

Управление приоритетными расписаниями

- Чтобы управлять приоритетными расписаниями, перейдите на вкладку **Override schedules** (Приоритетные расписания).
- Нажмите **Add dates (Добавить даты)**, чтобы добавить в расписание новый диапазон дат. К одному приоритетному расписанию можно добавить несколько диапазонов дат.
- Чтобы добавить временной интервал, нажмите **+** или дважды щелкните строку.
- Чтобы изменить диапазон дат или временной интервал, щелкните его левой кнопкой мыши.
- Нажмите **Apply** (Применить), чтобы сохранить изменения.

Примеры правил действий

Пример: Взломана дверь

Взломана дверь

В этом примере показано, как настроить правило действия в AXIS Camera Station Pro, которое запускает запись и тревогу при принудительном открытии входной двери.

Прежде чем начать, потребуется выполнить следующее:

- Установите сетевой дверной контроллер Axis. См. *Добавить устройства, on page 49*.
- Настроить дверной контроллер. См. раздел *Добавьте дверь, on page 158*.

Создайте правило действия:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Добавьте событие Принудительное открытие двери в качестве триггера:
   3.1. Нажмите **Добавить** и выберите **Событие на устройстве**.
   3.2. Нажмите кнопку **OK**.
   3.3. В разделе **Configure device event trigger (Настроить триггер в виде события устройства)** настройте параметры инициирующего события.
   3.4. В разделе **Filters (Фильтры)** настройте параметры фильтра.
   3.5. В разделе **Activity (Срабатывание)** убедитесь, что триггер отображается как срабатывание на линии сигнала.
   3.6. Нажмите кнопку **OK**.
4. Нажмите **Next (Далее)**.
5. Добавьте действие записи:
   5.1. Нажмите **Добавить** и выберите **Запись**.
   5.2. Нажмите кнопку **OK**.
   5.3. Выберите камеру в раскрывающемся меню **Camera (Камера)**.
   5.4. В разделе **Video setting (Параметры видео)** настройте профиль, буфер перед тревогой и буфер после тревоги.
   5.5. Нажмите кнопку **OK**.
6. Добавьте подачу сигнала тревоги в качестве действия:
   6.1. Нажмите **Добавить** и выберите **Подать сигнал тревоги**.
   6.2. Нажмите кнопку **OK**.
   6.3. В разделе **Alarm message (Сообщение о тревоге)** введите название и описание сигнала тревоги. Например: «The main entrance is forced open» («Входная дверь принудительно открыта»).
   6.4. Нажмите кнопку **OK**.
7. Нажмите **Next (Далее)** и выберите **Always (Всегда)** в качестве расписания.
8. Нажмите **Finish** ("Завершить").

Настроить запуск по событию для устройства	
Устройство	Выберите сетевой дверной контроллер Axis из раскрывающегося меню **Device (Устройство)**.
Событие	Выберите **Door > Door forced (Дверь > Дверь открыта силой)** в раскрывающемся меню **Event (Событие)**.
Период действия триггера	Задайте параметр **Trigger period (Период действия триггера)** равным 10 секунд.

Фильтры	
Имя двери	Выберите дверь из раскрывающегося меню **Door name (Имя двери)**.
Состояние двери	Выберите **Forced (Открыта силой)** из раскрывающегося меню **Door status (Состояние двери)**.

Настройки видео	
Профиль	Выберите **High (Высокое качество)** в раскрывающемся списке **Profile (Профиль)**.
Буфер перед тревогой	Задайте параметр **Prebuffer (Буфер перед тревогой)** равным 3 секунды.
Буфер после тревоги	Задайте параметр **Postbuffer (Буфер после тревоги)** равным 5 секунд.

Пример: При входе важного лица

При входе важного лица

В этом примере показано, как создать правило действия в AXIS Camera Station Pro, которое воспроизводит приветственное сообщение и вызывает лифт при входе важного лица.

Прежде чем начать, потребуется выполнить следующее:

- Установите сетевой дверной контроллер Axis и добавьте держателей карт. См. *Настройте контроль доступа, on page 154* и *Контроль доступа, on page 193*.
- Установите сетевое аудиоустройство Axis и свяжите его с камерой. См. *Профили потоков, on page 57*.
- Установить сетевой релейный модуль ввода-вывода AXIS A9188 Network I/O Relay Module, подключить входы-выходы к лифту и добавить порты ввода-вывода сетевого релейного модуля ввода-вывода в AXIS Camera Station Pro. См. *Порты ввода/вывода, on page 96*.

Создайте правило действия:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **New (Новое)**.
3. Добавьте событие устройства в качестве триггера:
   3.1. Нажмите **Добавить** и выберите **Событие на устройстве**.
   3.2. Нажмите кнопку **OK**.
   3.3. В разделе **Configure device event trigger (Настроить триггер в виде события устройства)** настройте параметры события.
   3.4. В разделе **Filters (Фильтры)** настройте параметры фильтра.
   3.5. В разделе **Activity (Срабатывание)** убедитесь, что триггер отображается как срабатывание на линии сигнала.
   3.6. Нажмите кнопку **OK**.
4. Нажмите **Next (Далее)**.
5. Добавьте действие Send HTTP notification (Отправить уведомление HTTP) для воспроизведения приветственного сообщения:
   5.1. Нажмите **Add (Добавить)** и выберите **Send HTTP notification (Отправить HTTP-уведомление)**.
   5.2. Нажмите кнопку **OK**.

5.3. В поле **URL (URL-адрес)** введите URL-адрес аудиоклипа с приветственным сообщением.

5.4. Выберите **Authentication required (Требуется проверка подлинности)** и введите имя пользователя и пароль для аудиоустройства.

5.5. Нажмите кнопку **OK**.

6. Добавьте действие Set output (Задать выход):

6.1. Нажмите **Добавить** и выберите **Создать действие на выходе**.

6.2. Нажмите кнопку **OK**.

6.3. В раскрывающемся списке **Output port (Порт выхода)** выберите порт выхода модуля ввода-вывода, подключенного к лифту.

6.4. Из раскрывающегося меню **State on action (Состояние при действии)** выберите состояние модуля ввода-вывода для вызова лифта.

6.5. Выберите **Pulse (Импульс)** и задайте длительность 60 секунд.

6.6. Нажмите кнопку **OK**.

7. Нажмите **Next (Далее)** и выберите **Always (Всегда)** в качестве расписания.

8. Нажмите **Finish** ("Завершить").

Настроить запуск по событию для устройства	
Устройство	Выберите сетевой дверной контроллер Axis из раскрывающегося меню **Device (Устройство)**.
Событие	Выберите **Authorization > Access request granted (Авторизация > Доступ предоставлен)** в раскрывающемся меню **Event (Событие)**.
Период действия триггера	Задайте параметр **Trigger period (Период действия триггера)** равным 10 секунд.

Фильтры	
Имя двери	Выберите дверь из раскрывающегося меню **Door name (Имя двери)**.
Сторона двери	Выберите сторону двери из раскрывающегося меню **Door side (Сторона двери)**.
Номер карты	Выберите **Card number (Номер карты)** и введите номер карты человека.

Настройка клиентского ПО

Перейдите в меню **Конфигурация > Клиент**, чтобы:

- Изменение параметров, относящихся к клиенту, например темы оформления и языка. См. *Настройки клиента, on page 126*.
- Изменение параметров, относящихся к пользователю, например уведомлений и параметров запуска. См. *Настройки пользователя, on page 127*.
- Изменение параметров потоковой передачи, относящихся к производительности клиента, например масштабирования видео и аппаратного декодирования. См. *Потоковая передача, on page 129*.

Настройки клиента

Эти настройки будут применены ко всем пользователям AXIS Camera Station Pro на компьютере.
Перейдите в **Configuration (Конфигурация) > Client (Клиент) > Client settings (Настройки клиента)**.

Тема	
System (Системная), Light (Светлая), Dark (Темная)	Выберите оформление для данного клиента. **System (Системная)** — значение по умолчанию при новой установке. Если выбрана **System (Системная)**, тема оформления соответствует теме оформления Windows.

Общее	
Запускать приложение при загрузке Windows	Включите этот параметр, чтобы автоматически запускался AXIS Camera Station Pro при запуске Windows.

Просмотр в реальном времени	
Показывать названия камер в живых просмотрах	Отображает имена камер в режиме живого просмотра.
	Включите **Show recording indicators in live views and maps (Показывать индикаторы записи в режиме живого просмотра и на картах)**, чтобы отображать индикатор записи при обнаружении движения или при запуске записи правилом действий.
	Включите **Show event indicators in live views and maps (Показывать индикаторы событий в режиме живого просмотра и на картах)**, чтобы отображать индикатор записи при обнаружении движения или при запуске записи правилом действий.

Карты	
Разрешить мигание зон охвата для всех карт	Включите или отключите этот параметр, чтобы управлять миганием зон покрытия на всех картах. Этот глобальный параметр не влияет на локальный параметр на уровне карты. См. *Карта, on page 23*.

Язык
Измените язык клиента AXIS Camera Station Pro. Перезапустите клиент, чтобы изменения вступили в силу.

Обратная связь	
Выберите этот параметр, если требуется, чтобы анонимные данные об использовании клиента передавались в компанию Axis Communications (это поможет нам улучшить приложение и сделать его более удобным для вас).	Передача анонимных данных в компанию Axis для повышения качества обслуживания пользователей. Чтобы изменить этот параметр для сервера, см. *Параметры сервера, on page 133*.

Настройки пользователя

Эти настройки применяются к пользователю AXIS Camera Station Pro, выполнившему вход. Перейдите в **Configuration > Client > User settings (Конфигурация > Клиент > Настройки пользователя)**.

Система навигации	
Представление системы навигации в виде дерева	Включено по умолчанию. Отображает представления, камеры или и то и другое в области навигации.
Показать в системе навигации	В раскрывающемся списке выберите, что отображать: представления, камеры или и то и другое.
Показывать путь навигации при навигации в окне просмотра	Активируйте этот параметр, чтобы показать путь навигации поверх вида при навигации в мультиэкранном режиме.

Уведомления	
Выводить уведомления о тревоге на панель задач	Включите этот параметр, чтобы при возникновении тревоги отображалось уведомление на панели задач Windows.
Выводить уведомления о задачах на панель задач	Включите этот параметр, чтобы при добавлении или выполнении задания отображалось уведомление на панели задач Windows.
Показывать уведомления на странице управления устройствами	Включите этот параметр, чтобы показывать уведомления о доступности для скачивания новой версии прошивки.
Показывать окно уведомлений видеодомофона	Включите этот параметр, чтобы при нажатии кнопки вызова на подключенной системе переговорного устройства отображалось окно уведомления.

Моментальный снимок	
Показывать сообщение после создания моментального снимка	Включите этот параметр, чтобы выводить сообщение, когда кто-либо делает моментальный снимок.
Открыть папку с моментальными снимками после создания моментального снимка	Включите этот параметр, чтобы открывать папку с моментальными снимками, когда кто-либо делает моментальный снимок.
Обзор	Нажмите **Browse (Обзор)**, чтобы выбрать папку для сохранения стоп-кадров.

Ввод в эксплуатацию	
Запуск в полноэкранном режиме	Включите этот параметр, чтобы запустить AXIS Camera Station Pro в полноэкранном режиме.
Запоминать последние вкладки	Включите этот параметр, чтобы AXIS Camera Station Pro запускалось с теми же открытыми вкладками, представлениями и представлениями камер, которые были открыты при последнем закрытии.
Запоминать последние мониторы	Включите этот параметр, чтобы запускать AXIS Camera Station Pro на том же мониторе, где окно было закрыто при запуске в предыдущий раз.

Примечание

- Система сохраняет виды и виды с камер для каждой вкладки. Система запоминает их только при повторном подключении клиента к тому же серверу.
- Динамические виды, которые вы перетаскиваете на окно живого просмотра, никогда не запоминаются системой.
- При подключении к нескольким серверам с разными пользователями система не поддерживает функцию **Remember last used tabs (Запоминать последние использованные вкладки)**.

Звук при тревоге	
Без звука	Выберите этот параметр, чтобы при возникновении тревоги звук не воспроизводился.
Зуммерный сигнал	Выберите этот параметр, чтобы при возникновении тревоги воспроизводился звуковой сигнал.
Звуковой файл	Выберите этот параметр и нажмите **Browse (Обзор)**, чтобы при возникновении тревоги использовать пользовательский звуковой файл. Поддерживается любой формат файла, совместимый с Windows Media Player.
Воспроизведение	Нажмите для проверки звука.

Звук при входящем вызове	
Без звука	Выберите этот параметр, чтобы при поступлении вызова звук не воспроизводился.
Зуммерный сигнал	Выберите этот параметр, чтобы при поступлении вызова воспроизводился звуковой сигнал.
Звуковой файл	Выберите этот параметр и нажмите **Browse (Обзор)**, чтобы при поступлении вызова использовать пользовательский звуковой файл. Поддерживается любой формат файла, совместимый с Windows Media Player.
Воспроизведение	Нажмите для проверки звука.

Особенности конструкции	
Показать интеллектуальный поиск 1	Отображается по умолчанию. Отключите этот параметр, чтобы скрыть Умный поиск 1.

Показывать окна с предупреждениями	
Предупреждение о недействительном сертификате	Включите этот параметр, чтобы при обнаружении недействительного сертификата отображалось предупреждение.

Потоковая передача

Перейдите в **Configuration (Конфигурация) > Client (Клиент) > Streaming (Потоковая передача)**, чтобы настроить параметры потоковой передачи.

Масштабирование видео	
Наилучшее масштабирование	Выберите этот параметр, чтобы вписать видео в доступное пространство без обрезки и изменения соотношения сторон.
Заполнить область видео (части видеоизображения могут быть обрезаны)	Выберите этот параметр, чтобы заполнить доступное пространство видеоизображением. Если соотношение сторон доступного пространства отличается от соотношения сторон видео, система обрезает видео для соответствия доступному пространству.

Аппаратное декодирование	
Режим	• **Automatic (Автоматически)**: видеокарта используется для декодирования потоков с разрешением выше 3840 × 2160 при 25 кадрах/с (также обозначается как 4K или UHD). • **On (Вкл.)**: видеокарта используется для декодирования потоков с разрешением выше 1920 × 1080 при 25 кадрах/с (также обозначается как 1080p или HD). • **Off (Выкл.)**: AXIS Camera Station Pro использует ЦП для декодирования видео.
Видеокарта	Выберите видеокарту в раскрывающемся меню.

Поддерживаемые видеокарты	Технология декодирования
NVIDIA	PureVideo
AMD	Unified Video Decoder (UVD)
Intel	Intel Quick Sync Video (QSV)

Примечание

- При аппаратном декодировании видеокарта используется для декодирования видео. Высокопроизводительная видеокарта позволяет повысить производительность и снизить загрузку ЦП при аппаратном декодировании, особенно при потоковой передаче видео высокого разрешения. Аппаратное декодирование поддерживает только потоки H.264 и AV1.
- Камеры с разрешением ниже 1080p не могут использовать аппаратное декодирование, даже если оно включено.
- Если видеокарта не поддерживает декодирование 4K, аппаратное декодирование работает только с потоками 1080p, даже если оно включено.
- Для аппаратного декодирования используется только одна видеокарта, даже если в системе установлено несколько видеокарт.

Использование трафика	
Всегда использовать профиль потока «Низкий» для этого клиента	Включите этот параметр, чтобы использовать профиль потока с низким разрешением для живого просмотра. См. *Профили потоков*. Этот параметр влияет на видео H.264 и M-JPEG и снижает потребление пропускной способности.
Приостанавливать видеопотоки на неактивных вкладках	Активируйте этот параметр, чтобы приостанавливать видеопотоки на неактивных вкладках. Это снижает потребление пропускной способности.

PTZ (поворот, наклон, зум)	
Первым кликом выбирать зону просмотра, а не запускать PTZ	Включите этот параметр, чтобы первый щелчок в представлении выбирал его. Последующие щелчки используются для управления PTZ.

Звук	
Push-to-talk release delay (ms) (Задержка после отпускания переговорной кнопки (мс))	Задает в миллисекундах продолжительность передачи звука с микрофона после отпускания кнопки **Push-to-talk (Нажать и говорить)**.
Использовать переговорную кнопку для всех дуплексных режимов	Активируйте этот параметр, чтобы использовать режимы push-to-talk в симплексном, полудуплексном и полнодуплексном режимах.
Всегда разрешать звук для переговорных устройств	Включите этот параметр, чтобы прослушивать переговорные устройства и говорить через них, даже если текущих вызовов нет.

Мгновенный повтор	
Длительность воспроизведения (сек)	Задайте время воспроизведения в диапазоне от 1 до 600 секунд, чтобы вернуться назад по временной шкале и воспроизвести запись.

Настройка подключенных сервисов

Управление подключенными сервисами

Подключенные службы предоставляют доступ к следующим функциям:

- Веб-клиент для AXIS Camera Station
- Управление устройствами
- Автоматическое управление лицензиями
- Контроль работоспособности системы

Для доступа к этим службам необходимо зарегистрировать систему и подключить ее к организации. Для получения дополнительных сведений см. *Регистрация системы в организации, on page 131*.

Статус	На карточке состояния отображается состояние подключения между сервером и подключенными службами, а также название организации, в которой зарегистрирована система.
Отключить	При отключении сервера он остается зарегистрированным в организации.
Управление лицензиями	Включите опцию **License management (Управление лицензиями)** для автоматической синхронизации ваших лицензий. Система передает изменения лицензий в AXIS License Manager и получает обновленный статус лицензий. Отключите **License management (Управление лицензиями)**, чтобы управлять лицензиями вручную, например если система не подключена к Интернету. Дополнительную информацию см. в разделе Manage licenses (Управление лицензиями). Для получения дополнительных сведений см. *Управление лицензиями, on page 142*.
Синхронизация системы	Активируйте опцию **Synchronize system (Синхронизация системы)** для автоматической синхронизации ваших устройств и видов с веб-клиентом AXIS Camera Station и системой управления AXIS Device Manager.

Регистрация системы в организации

Для регистрации системы:

1. Перейдите в меню **Configuration (Конфигурация)** > **Connected services (Подключенные сервисы)** > **Management (Управление)**.
2. Нажмите **Register (Регистрация)** и следуйте инструкциям на экране.

Дополнительную информацию о регистрации системы см. в *руководстве по установке и миграции AXIS Camera Station Pro*.

Настройки обновления встроенного ПО

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro можно задавать параметры обновления встроенного ПО на любом из подключенных серверов. Для этого надо выбрать нужный сервер в раскрывающемся меню **Selected Server (Выбранный сервер)**.

1. Перейдите в меню **Конфигурация > Подключенные сервисы > Параметры обновления встроенного ПО**.
2. В разделе **Automatic check for updates (Проверять наличие обновлений автоматически)** настраивается частота и способ проверки обновлений.
3. В разделе **Upgrade order (Последовательность обновления)** настраивается последовательность обновления устройств.

Автоматический поиск обновлений	
Проверить наличие обновлений	Выберите **Every start-up (При каждом запуске)**, чтобы проверять наличие доступных версий встроенного ПО при каждом запуске сервера. По умолчанию для AXIS Camera Station Pro установлено значение **Never (Никогда)**.
Проверить сейчас	Нажмите для проверки доступных версий встроенного ПО на сервере.

Порядок обновления	
параллельно;	Выберите для одновременного обновления всех устройств. В этом случае обновление будет выполнено быстрее, чем для варианта **Sequential (Последовательно)**, но при этом все устройства одновременно будут переведены в автономный режим (офлайн).
Последовательный	Выберите для последовательного обновления устройств одного за другим. На это требуется больше времени, но при этом устройства не будут одновременно находиться в офлайн-режиме. Выберите **Cancel remaining upgrades if one device fails (Отменить оставшиеся обновления при сбое одного устройства)**, чтобы остановить последовательное обновление.

Активация автоматической проверки встроенного ПО

Axis Secure Remote Access 2

Axis Secure Remote Access v2 позволяет подключаться к серверу AXIS Camera Station Pro через зашифрованное интернет-соединение.

Примечание

Служба Axis Secure Remote Access v2 доступна для AXIS Camera Station Pro 6.8 или более поздних версий.

Чтобы включить функцию Axis Secure Remote Access 2:

1. Зарегистрируйте сервер в организации. См. *Регистрация системы в организации, on page 131*.

2. Выполните вход с помощью Axis Secure Remote Access v2. См. *Вход в систему с помощью AXIS Secure Remote Access 2, on page 10*.

Чтобы ограничить доступ только серверами AXIS Camera Station Pro:

1. Перейдите на страницу **Организация > Пользователи** в разделе My Systems.
2. Выберите пользователя, чей доступ нужно настроить.
3. Нажмите **Роли и доступ**.
4. Назначьте роль **ACS Pro Secure Remote Access**. Эта роль ограничивает доступ только к серверам AXIS Camera Station Pro, без доступа к другим функциям Axis My Systems.

После регистрации можно управлять разрешениями доступа, назначая пользователям роли в организации в Axis My Systems. Дополнительную информацию о правах доступа пользователей AXIS Camera Station Pro см. в *Права доступа пользователей, on page 144*.

Облачное хранилище данных

AXIS Camera Station Cloud Storage — лицензируемая служба для хранения записей в облаке. Дополнительную информацию см. в *руководстве пользователя AXIS Camera Station Cloud Storage*.

Внимание

AXIS Camera Station Cloud Storage работает только с AXIS Camera Station Pro версии 6.18 или более ранней. Перед обновлением рекомендуется экспортировать записи в локальное хранилище. При обновлении до версии более новой, чем 6.18, служба облачного хранилища перестанет работать, и все данные, хранящиеся в облаке, будут потеряны. Обновления безопасности для версии 6.18 будут выпускаться до восстановления поддержки облачного хранилища в одной из последующих версий.

Перед использованием службы облачного хранилища необходимо зарегистрировать систему в подключенных службах. После регистрации системы можно управлять облачным хранилищем камер в разделе My Systems (Мои системы).

Настройка сервера

Параметры сервера

Перейдите в **Configuration (Конфигурация) > Server (Сервер) > Settings (Настройки)**.

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro выберите нужный сервер в раскрывающемся списке **Selected server (Выбранный сервер)**, чтобы настроить его параметры.

Экспорт	
Включить звук при добавлении записей для экспорта	Выберите для включения звука при добавлении записи в список экспорта.

Журналы
Укажите количество дней хранения сигналов тревоги, событий и журналов аудита. Задайте значение от 7 до 1000 дней. Чтобы непрерывно записывать журналы в файл в режиме реального времени для использования со сторонними системами, такими как Splunk, Elastic или SIEM-система, выберите **Write audit logs to file (Записывать журналы аудита в файл)**, **Write event logs to file (Записывать журналы событий в файл)** или оба параметра. Сервер записывает записи журнала в файл `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Server\Logs`. Файлы имеют текстовый формат и не включаются в отчеты о системе.

Файл	Описание
`AcsService.exe.audit.log.export`	Записи журнала аудита
`AcsService.exe.event.log.export`	Записи журнала событий

Внешние данные
Укажите, сколько дней должны храниться внешние данные. Задайте значение от 1 до 1000 дней.

SMTP-серверы

Добавьте SMTP-серверы для отправки сообщений электронной почты при возникновении системных сигналов тревоги или срабатывании правила действий.

Чтобы добавить SMTP-сервер:

1. В разделе **SMTP servers (SMTP-серверы)** нажмите кнопку **Add (Добавить)**.
2. В разделе **Server (Сервер)** настройте адрес сервера, порт, проверку подлинности и протокол TLS.
3. В разделе **Sender (Отправитель)** введите адрес электронной почты и имя, которые будут отображаться в качестве данных отправителя.

Сервер	
Адрес	Введите адрес SMTP-сервера.
Порт	Введите номер порта. 587 — это порт по умолчанию для SMTP-подключений по протоколу TLS.
Использовать TLS	Выберите, если SMTP-сервер использует TLS. По умолчанию используется протокол TLS.
Использовать проверку подлинности	Если сервер требует имя пользователя и пароль, установите соответствующий флажок и введите учетные данные.

Изменить	Чтобы изменить параметры SMTP-сервера, выберите нужный сервер и нажмите **Изменить**.
Удалить	Чтобы удалить SMTP-сервер, выберите его и нажмите **Удалить**. В диалоговом окне нажмите **Yes (Да)**, чтобы удалить сервер.

Проверить все...	Чтобы протестировать SMTP-сервер, выберите его и нажмите **Test all... (Проверить все...)**. В диалоговом окне введите адрес электронной почты в поле **Recipient (Получатель)** и нажмите **OK**, чтобы отправить тестовое сообщение. При тестировании SMTP-сервера выдается список результатов и рекомендуемых действий.
Стрелки	Выберите сервер и с помощью стрелок установите порядок. Система обращается к серверам в указанном порядке.

Результаты тестирования сервера	
OK	Соединение с SMTP-сервером установлено. Убедитесь, что получатели получили тестовое сообщение.
Неизвестная ошибка	При отправке электронной почты произошла непредвиденная ошибка. Проверьте работоспособность SMTP-сервера.
Нет контакта	AXIS Camera Station Pro не удается получить доступ к SMTP-серверу. Убедитесь, что SMTP-сервер работает, а маршрутизаторы и прокси-серверы между AXIS Camera Station Pro и SMTP-сервером разрешают передачу трафика.
Ошибка конфигурации	Запрошено использование TLS, но сервер не поддерживает StartTLS, не поддерживает аутентификацию или не имеет совместимого механизма аутентификации.
Ошибка подтверждения установления связи по протоколу TLS/SSL	При согласовании TLS/SSL произошла ошибка, например из-за недействительного сертификата сервера.
Требуется аутентификация	Для отправки электронной почты серверу требуется проверка подлинности.
Ошибка проверки подлинности	Неверные учетные данные.
Соединение прервано	Соединение было установлено, но затем потеряно.

Системная тревога

Системный сигнал тревоги возникает при потере камерой соединения, отказе в доступе к хранилищу записей, неожиданном завершении работы сервера или возникновении ошибок записи. Можно настроить отправку уведомлений о системных сигналах тревоги по электронной почте.

Примечание

Для отправки сообщений по электронной почте необходимо сначала добавить в систему SMTP-сервер.

Чтобы отправить сообщение по электронной почте при подаче сигнала тревоги в системе:

1. Выберите **Send email on system alarm to the following recipients (Отправлять сообщения электронной почты при системных сигналах тревоги следующим получателям)**, чтобы настроить уведомления о системных сигналах тревоги по электронной почте.
2. В разделе **Recipients (Получатели)**:
   2.1. Выберите требуемое поле адреса (**To (Кому)**, **Cc (Копия)** или **Bcc (Скрытая копия)**).

2.2. Введите адрес электронной почты.

2.3. Нажмите **Add (Добавить)**, чтобы сохранить адрес электронной почты в поле **Recipients (Получатели)**.

Подключение устройства	
По возможности используйте имена хостов вместо IP для вновь добавленных устройств	По возможности используйте имена узлов вместо IP-адресов при добавлении новых устройств. Если имя узла отсутствует, используется IP-адрес.
Продолжать использовать имена хостов, даже если они стали недоступными	Для подключения используйте имя хоста. Чтобы автоматически переключиться на IP-адрес, снимите флажок. Можно вручную выбрать имя хоста или IP-адрес для подключения к устройствам. См. *Подключение, on page 77*.

Язык	
Изменить язык сервера	Изменяет язык AXIS Camera Station Pro Service Control и AXIS Camera Station Secure Entry. Например, для системных сигналов тревоги, сообщений журнала аудита и внешних данных на вкладке **Data search (Поиск данных)**. Перезапустите сервер, чтобы изменения вступили в силу.

Нательные камеры	
Диск **Папка**	Выберите диск и папку для хранения отклоненного содержимого из системы нательных камер. Дополнительную информацию см. в разделе *Передача записей в хранилище отклоненного содержимого в Руководстве пользователя для нательного решения Axis*.
Количество дней хранения отклоненного содержимого из нательной системы.	Задает количество дней хранения отклоненного содержимого из системы нательных камер.

Обратная связь	
Отправить анонимные данные об использовании сервера в компанию Axis Communications	Установите этот флажок, чтобы передавать Axis анонимные данные для улучшения приложения и взаимодействия с пользователем. Чтобы изменить этот параметр для клиента, см. *Настройки клиента, on page 126*.

Расширенные настройки

Изменяйте эти параметры только по указанию службы технической поддержки Axis. Чтобы изменить расширенные настройки:

1. Введите настройку и ее значение.
2. Нажмите **Добавить**.

Чтобы включить ведение журнала отладки на стороне сервера для устранения неисправностей, установите флажок **Enable server side debug logging (Включить ведение журнала отладки на стороне сервера)**. Этот параметр увеличивает объем используемого дискового пространства. Файл `log4net.config` в каталоге **ProgramData** имеет приоритет над этим параметром.

Дополнительную информацию см. в разделе *Advanced server setting in the AXIS Camera Station Pro Troubleshooting guide (Расширенные настройки сервера в руководстве по устранению неполадок AXIS Camera Station Pro)*.

Компоненты

Компоненты — это программные модули, расширяющие возможности системы. На странице **Components (Компоненты)** можно управлять компонентами и просматривать их состояние.

Просмотр списка установленных компонентов:

1. Перейдите к пункту **Configuration > Server > Components (Конфигурация > Сервер > Компоненты)**.
2. Включите функцию **Show components (Показать компоненты)**.

Примечание

Компоненты рассматриваются как расширенные настройки. Просматривайте и настраивайте компоненты только после консультации со службой поддержки Axis.

Обновить AXIS Camera Station Pro

Чтобы обновить AXIS Camera Station Pro:

1. Перейдите к пункту **Configuration > Server > General (Конфигурация > Сервер > Обновить)**.
2. Нажмите **Upload and install... (Загрузить и установить...)**.

Примечание

- После начала обновления, вручную или по расписанию, отменить его невозможно.
- Запуск запланированных обновлений осуществляется автоматически.
- В мультисерверных системах последним всегда обновляйте локальный сервер.
- При обновлении локального сервера клиент и Service Control (Управление службой) временно закрываются. Во время обновления индикатор выполнения не отображается. Оставьте серверный компьютер включенным до тех пор, пока и клиент, и сервер не перезапустятся.

Отчет об инцидентах

При включении разрешений на создание отчетов об инцидентах можно создавать отчеты об инцидентах, содержащие записи, снимки и примечания. См. *Экспорт отчетов об инцидентах, on page 35*.

Чтобы настроить параметры отчетов об инцидентах:

1. Перейдите в меню **Configuration > Server > Incident report (Конфигурация > Сервер > Отчет об инцидентах)**.
2. В разделе **Location (Место расположения)** выберите место хранения отчетов об инцидентах.
3. В раскрывающемся списке **Export format (Формат экспорта)** выберите формат для экспорта записей.
4. В разделе **Categories (Категории)** добавьте или удалите категории, чтобы нужным образом сгруппировать отчеты об инцидентах. Если категории заданы как переменная в пути к каталогу сервера, они становятся именами папок в расположении экспорта.
   4.1. Введите название категории в поле, например Accident (Аварийная ситуация) или Theft (Кража).
   4.2. Нажмите **Добавить**.
   4.3. Чтобы удалить категорию, выберите ее и нажмите **Remove (Удалить)**.
5. В разделе **Description template (Шаблон описания)** введите сведения, которые будут отображаться в поле **Description (Описание)** при формировании отчетов об инцидентах. Например: «Reported by: [name, email, phone number] (Сообщил: [имя, адрес электронной почты, номер телефона])».

6. Нажмите **Применить**.

Место расположения	
Путь к директории сервера	Введите путь к каталогу для сохранения отчетов об инцидентах в папке на компьютере. В качестве переменных можно использовать имя сервера, категорию или имя пользователя. Например: `C:\Reports\$(Server Name)\$(Category)\$(User Name)\`.
Путь к сетевой папке	Выберите, чтобы сохранить отчеты об инцидентах в папку на сетевом накопителе. Введите путь к каталогу или используйте учетные данные для сетевого накопителя. Этот сетевой ресурс должен быть доступен с сервера AXIS Camera Station Pro. Инструкции по добавлению ресурса хранения для хранения записей см. в разделе *Управление хранением данных*.

Export format (Формат экспорта)	
ASF	Выберите **Add digital signature (Добавить цифровую подпись)**, чтобы предотвратить изменение изображений. См. раздел «Цифровая подпись» в *Экспорт записей*. Цифровую подпись также можно защитить паролем, выбрав параметр **Use password (Использовать пароль)**.
MP4	Экспортированные записи не включают звук в формате G.711 или G.726.

Запланированный экспорт

Перейдите в **Configuration > Server > Scheduled export (Конфигурация > Сервер > Запланированный экспорт)**, чтобы создать расписания для экспорта записей.

В запланированное время AXIS Camera Station Pro экспортирует все записи, созданные после предыдущего экспорта. Если с момента предыдущего экспорта прошла более чем неделя или предыдущего экспорта не было, включаются только записи за последнюю неделю. Чтобы экспортировать более ранние записи, откройте вкладку **Recordings (Записи)** и выполните экспорт вручную. См. *Экспорт записей*.

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro выберите любой сервер в раскрывающемся списке **Selected server (Выбранный сервер)**, чтобы управлять запланированным экспортом.

Запланированный экспорт записей

1. В разделе **Scheduled export (Запланированный экспорт)** выберите **Enable scheduled export (Включить запланированный экспорт)**.
2. В разделе **Cameras (Камеры)** выберите камеры, с которых надо экспортировать записи. По умолчанию система выбирает все камеры в списке. Снимите флажок **Use all cameras (Использовать все камеры)** и выберите конкретные камеры из списка.
3. В разделе **Export (Экспорт)** укажите путь для хранения записей, формат и необходимость создания списка воспроизведения.
4. В разделе **Weekly schedule (Недельное расписание)** выберите время и дни для экспорта записей.
5. Нажмите **Применить**.

Экспорт	
Путь к директории сервера	Чтобы сохранить записи в папке на компьютере, выберите или введите путь к каталогу.
Путь к сетевой папке	Выберите, чтобы сохранить записи в папку на сетевом накопителе. Введите путь к каталогу или используйте учетные данные для сетевого накопителя. Этот сетевой ресурс должен быть доступен с сервера AXIS Camera Station Pro. Инструкции по добавлению ресурса хранения для хранения записей см. в разделе *Управление хранением данных*.
Создать список воспроизведения (.asx)	Выберите, чтобы создать список воспроизведения в формате ASX для проигрывателя Windows Media Player. Записи будут воспроизводиться в том порядке, в котором они записывались.
Export format (Формат экспорта)	Выберите формат для экспорта записей. **ASF** – выберите **Add digital signature (Добавить цифровую подпись)**, чтобы предотвратить несанкционированные действия в отношении изображений. См. раздел «Цифровая подпись» в *Экспорт записей*. Цифровую подпись также можно защитить паролем, выбрав параметр **Use password (Использовать пароль)**. **MP4** – экспортированные записи не включают звук в формате G.711 или G.726.

Microsoft Windows 2012 Server

Чтобы экспортировать записи с сервера под управлением Microsoft Windows Server 2012, установите Desktop Experience:

1. Перейдите в меню **Пуск > Администрирование > Управление сервером** и откройте окно «Диспетчер сервера».
2. Открыв меню **Управление > Добавить правила и функции**, запустите мастер настройки ролей и функций.
3. В разделе **Features Summary (Функции)** выберите **User Interfaces and Infrastructure (Пользовательские интерфейсы и инфраструктура)**.
4. Выберите **Desktop Experience (Возможности рабочего стола)** и нажмите **Next (Далее)**.
5. Щелкните **Установить**.

Параметры WebRTC

Веб-клиент AXIS Camera Station использует протокол WebRTC для взаимодействия с сервером.

Включить TURN	Включает локальный сервер TURN на сервере AXIS Camera Station Pro, позволяя использовать один порт для обмена данными WebRTC. Это упрощает настройку брандмауэра.
Prioritize TURN (Приоритет TURN)	Выберите этот параметр, чтобы WebRTC использовал только кандидатов ретрансляции.

Новое соединение

Перейдите в ☰ > **Servers (Серверы) > New connection (Новое подключение)**, чтобы подключиться к серверу AXIS Camera Station Pro. См. *Подключить к серверу*.

Состояние соединения

Перейдите в ☰ > **Servers (Серверы) > Connection status (Состояние подключения)**, чтобы просмотреть состояние подключения всех серверов.

Используйте ползунок рядом с именем сервера, чтобы подключиться к серверу или отключиться от него.

Код статуса	Описание	Возможные решения
Подключение	Клиент пытается установить соединение с сервером.	
Подключено	При подключении к этому серверу клиент использует TCP.	
Подключено (Axis Secure Remote Access v2)	Клиент подключен к этому серверу с помощью Axis Secure Remote Access вер.2.	
Подключено (HTTP)	Клиент подключен к серверу по протоколу HTTP. Такое соединение менее эффективно, чем подключение по протоколу TCP; кроме того, оно медленнее при подключении сразу к нескольким серверам.	
Отключение	Клиент отключается от этого сервера .	
Отключено	Клиент не подключен к этому серверу.	
Переподключение	Клиент потерял соединение с этим сервером и пытается восстановить подключение.	
Ошибка при пересоединении	Сервер найден, но права пользователя или пароль могли измениться.	• Добавьте пользователя в диалоговом окне **User permission (Разрешения пользователей)**. • Проверьте имя пользователя и пароль.
Отмена входа в систему	Вход в систему отменен пользователем.	
Неверное имя пользователя или пароль	Введите правильные учетные данные, пройдя по ссылке в столбце **Action (Действие)**.	
Пользователь не авторизован на этом сервере	Сервер не авторизует пользователя для входа.	Добавьте пользователя в диалоговом окне **User permission (Разрешения пользователей)**.

Проверка безопасности завершилась ошибкой	Сбой проверки безопасности, связанной с WCF.	Синхронизируйте время UTC на компьютерах клиента и сервера.
Нет связи с серверным компьютером	Компьютер сервера не ответил по указанному адресу.	• Убедитесь, что сеть работает правильно. • Убедитесь, что сервер запущен.
Нет работающего сервера	Компьютер, на котором работает сервер, доступен, но сервер не запущен.	Запустите сервер.
Ошибка связи	Ошибка подключения к серверу.	• Проверьте, доступен ли компьютер, работающий как сервер. • Убедитесь, что сеть нормально функционирует. • Убедитесь, что сервер запущен.
Недопустимое имя хоста	DNS не может преобразовать имя хоста в IP-адрес.	• Убедитесь, что имя узла указано правильно. • Убедитесь, что DNS может разрешить имя узла.
Подключение к этому серверу уже установлено	Соединение клиента с сервером уже установлено.	Удалите двойной ввод сервера.
Сервер отличается от ожидаемого	По этому адресу ответил другой сервер, а не ожидаемый.	Обновите сервер, указав правильный сервер.
Версия клиента (x) несовместима с версией сервера (y)	Клиентское ПО устарело или, наоборот, слишком новое, по сравнению с серверным ПО.	Установите одинаковую версию AXIS Camera Station Pro на компьютерах клиента и сервера.
Сервер перегружен	Нет отклика от сервера из-за проблем с производительностью.	Убедитесь, что компьютер сервера и сеть не перегружены.

Для просмотра видео откройте веб-версию данного документа.

Несколько серверов

Списки серверов

Серверы AXIS Camera Station Pro можно организовать в виде списков. Один и тот же сервер может находиться в нескольких списках. Можно импортировать, экспортировать и использовать списки серверов в других клиентах AXIS Camera Station Pro.

Перейдите в > **Servers (Серверы) > Server lists (Списки серверов)**.

В списке **Recent connections (Недавние подключения)** по умолчанию отображаются серверы, использовавшиеся в предыдущем сеансе. **Недавние подключения** удалить невозможно.

	Выберите список серверов и нажмите , чтобы удалить его.
New server list (Новый список серверов)	Нажмите , чтобы добавить новый список серверов и присвоить ему имя.
Добавить	Чтобы добавить сервер в список серверов, выберите список и нажмите **Add (Добавить)**. Введите необходимую информацию.
Экспорт списков	Нажмите для экспорта всех списков серверов в виде файла .msl. Можно импортировать списки серверов для подключения к серверам. См. *Подключить к серверу*.
Изменить	Чтобы изменить сервер, выберите его и нажмите **Edit (Изменить)**. За один раз можно изменить только один сервер.
Удалить	Чтобы удалить сервер из списка серверов, выберите его и нажмите **Remove (Удалить)**.
Rename a list (Переименовать список)	Дважды щелкните список и введите новое имя.

Организация серверов в списках серверов

Configure switch (Настройка коммутатора)

Если используется устройство серии AXIS Camera Station S22 Appliance, его можно настроить из AXIS Camera Station Pro. Перейдите в **Configuration (Конфигурация) > Switch (Коммутатор) > Management (Управление)** и введите учетные данные для открытия страницы управления коммутатором. Инструкции по настройке коммутатора см. в руководстве пользователя AXIS Camera Station S22 Appliance на сайте *axis.com*.

Примечание

AXIS Camera Station Pro может подключаться только к https://192.168.0.1/, то есть к IP-адресу коммутатора, заданному по умолчанию.

Управление лицензиями

Страница «Управление лицензиями» отображает текущее состояние ваших лицензий.

Пробный период	При установке AXIS Camera Station Pro вам предоставляется 90-дневный пробный период. В течение этого периода система полностью работоспособна. Можно настроить систему и проверить все функции до приобретения лицензий.
Проверьте свои лицензии	Если срок действия лицензии системы истек без автоматического продления, AXIS License Manager предоставляет 30-дневный льготный период.
Требуется лицензия	Система имеет полную лицензию до самой ранней даты истечения срока действия.
Изменения, внесенные в систему, требуют синхронизации лицензии	При добавлении устройств в лицензированную систему AXIS Camera Station Pro пытается синхронизировать изменения с AXIS License Manager для обновления статуса лицензии системы. При автоматическом лицензировании этот процесс может быть незаметным. При использовании ручного лицензирования, если повторная синхронизация не выполняется в течение 60 дней, лицензия системы становится недействительной.
Нет лицензий	Система остается работоспособной, но с ограниченным функционалом. Запись и правила действий продолжают работать, и существующие записи не будут утеряны. Следующие функции не будут работать: • Потоковая передача в реальном времени • Воспроизведение записей • Мгновенное воспроизведение • Стоп-кадры • Экспорт записей

Лицензировать систему можно двумя способами:

Автоматическое лицензирование (для онлайн-систем) – Система автоматически передает изменения, влияющие на количество лицензий, в AXIS License Manager и получает новый статус лицензии. Требуется подключение к Интернету. Для получения дополнительных сведений см. *Лицензирование системы в режиме онлайн, on page 143*.

Ручное лицензирование (для офлайн-систем) – При выборе этого варианта необходимо вручную экспортировать файл системы, загрузить его в AXIS License Manager и импортировать новую лицензию. При каждом изменении системы, влияющем на количество лицензий, этот процесс необходимо повторять. Выбирайте ручной вариант, если предпочитаете управлять лицензиями самостоятельно или если система не имеет выхода в Интернет. Для получения дополнительных сведений см. *Лицензирование системы в автономном режиме, on page 144*.

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 Pro.
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.

Настройка безопасности

Права доступа пользователей

Перейдите к пункту **Configuration (Конфигурация) > Security (Безопасность) > User permissions (Права доступа пользователей)**, чтобы увидеть пользователей и группы в AXIS Camera Station Pro.

Примечание

Администраторы компьютера, на котором работает сервер AXIS Camera Station Pro, автоматически получают права администратора системы в AXIS Camera Station Pro. 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. раздел *Добавление пользователей или групп*.

Если пользователь входит в состав группы, ему предоставляются права наиболее высокой роли, назначенной либо непосредственно пользователю, либо группе. Например, если пользователю предоставлен доступ к камере X и при этом он входит в группу с доступом к камерам Y и Z, то он 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. Допустимые значения: Administrator (Администратор), Operator (Оператор) и Viewer (Средство просмотра).
Сведения	Подробные сведения о пользователе в том виде, в котором они отображаются на локальном компьютере или в Active Directory.
Сервер	Сервер, к которому относится пользователь или группа.

Добавление пользователей или групп

Доступ к AXIS Camera Station Pro могут получать пользователи и группы Microsoft Windows® и Active Directory. Чтобы добавить пользователя в AXIS Camera Station Pro, 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 в **Local Users and Groups (Локальные пользователи и группы)** > **Users (Пользователи)**.
- Щелкните **Users (Пользователи)** правой кнопкой мыши 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 для сужения результатов поиска.
5. Выберите пользователей или группы и нажмите **Add (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 Pro выберите сервер, на котором требуется 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 **OK**, чтобы подтвердить удаление пользователя или группы.

Права доступа пользователей или групп

Пользователю или группе можно назначить одну из трех ролей. Информацию о том, как определить роль для пользователя или группы, см. в разделе *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 конфигурации системы.

Оператор – Выберите камеры, виды и порты ввода-вывода для получения доступа к живому видео и видеозаписям. Оператор имеет полный доступ ко всем функциям AXIS Camera Station Pro 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	Разрешает вручную запускать и останавливать запись.

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-управлением, когда 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 Pro.
Изменить	Позволяет редактировать представления в AXIS Camera Station Pro.

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	Позволяет просматривать состояние порта ввода-вывода без возможности его изменения.
Запись	Позволяет 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	Позволяет создавать снимки в режиме живого просмотра и при воспроизведении 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.

AXIS Audio Manager Pro

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

Доступ к настройкам компонентов AXIS Audio Manager Pro	Позволяет выполнить конфигурирование AXIS Audio Manager Pro в AXIS Camera Station Pro и доступ к интерфейсу сервера AXIS Audio Manager Pro. Доступно только для роли Operator (Оператор).
Доступ к интерфейсу AXIS Audio Manager Pro	Позволяет получить доступ к интерфейсу сервера AXIS Audio Manager Pro. Доступно только для роли Viewer (Обозреватель).

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 настраивать параметры контроля работоспособности системы.
Доступ к контролю работоспособности системы	Позволяет получить доступ к контролю работоспособности системы.

Сертификаты

Для управления настройками сертификатов сервера AXIS Camera Station Pro и подключенных устройств перейдите в **Configuration (Конфигурация) > Security (Безопасность) > Certificates (Сертификаты)**.

Сведения о включении, удалении и просмотре сертификатов HTTPS и IEEE 802.1X см. в *Безопасность, on page 75*.

AXIS Camera Station Pro можно использовать в качестве:

- **Root certificate authority (CA) (Корневой центр сертификации (CA))**: AXIS Camera Station Pro использует собственный корневой сертификат для выпуска сертификатов сервера без участия других корневых центров сертификации.
- **Intermediate certificate authority (Промежуточный центр сертификации)**: импортируйте сертификат CA и его закрытый ключ в AXIS Camera Station Pro, чтобы подписывать и выпускать сертификаты сервера для устройств Axis. Это может быть корневой сертификат или сертификат промежуточного центра сертификации.

Примечание

При удалении AXIS Camera Station Pro выполняется удаление сертификатов ЦС из раздела «Центры доверенных корневых сертификатов Windows». При этом импортированные сертификаты ЦС удалены не будут; их необходимо удалить вручную.

Центр сертификации (ЦС)

Центр сертификации предоставляет возможность использовать протоколы HTTPS и IEEE 802.1X на устройствах без каких-либо сертификатов клиента или сервера. Сертификат ЦС AXIS Camera Station Pro может автоматически создавать, подписывать и устанавливать сертификаты клиента/сервера на устройствах при использовании протокола HTTPS или IEEE 802.1X. Можно использовать AXIS Camera Station Pro в качестве корневого ЦС или импортировать сертификат ЦС и позволить AXIS Camera Station Pro действовать в качестве промежуточного ЦС. Система генерирует корневой ЦС при установке сервера.

Импорт	Нажмите, чтобы импортировать существующий сертификат центра сертификации (CA) и его закрытый ключ. AXIS Camera Station Pro сохраняет пароль сертификата.
Создать	Нажмите кнопку для создания нового открытого и закрытого ключа, а также самозаверяющего сертификата ЦС, действительного в течение 10 лет. При создании нового центра сертификации он заменяет все сертификаты компонентов и перезапускает компоненты.
Вид	Нажмите, чтобы просмотреть подробные сведения о сертификате ЦС.

Экспорт	Нажмите, чтобы экспортировать CA в файл. Вы можете экспортировать его двумя способами: • **Без закрытого ключа**: сохраняет сертификат в формате .cer или .crt. Если требуется установить только открытый сертификат в другие системы, которые должны доверять сертификатам, подписанным AXIS Camera Station Pro. • **С закрытым ключом:** сохраняет CA в формате PKCS#12 (.pfx или .p12). Если необходимо импортировать CA на другой сервер AXIS Camera Station Pro. Импорт сертификатов формата .cer или .crt обратно в AXIS Camera Station Pro невозможен.
Срок действия (дней) подписанных сертификатов сервера/клиента	Задайте срок действия автоматически созданных сертификатов клиента/сервера. Максимальный срок действия составляет 1 095 дней (три года). CA не подписывает сертификаты, срок действия которых истекает позже срока действия самого CA.

Создание корневого ЦС

При запуске AXIS Camera Station Pro ищет ЦС. Если CA не найден, автоматически создает корневой CA. Включает в себя самозаверяющий корневой сертификат, а также закрытый ключ, защищенный паролем. AXIS Camera Station Pro сохраняет пароль, но не делает его видимым. Сертификат ЦС, созданный ПО AXIS Camera Station Pro, действителен в течение 10 лет.

Чтобы вручную создать новый ЦС для замены старого, см. *Замена ЦС, on page 151*.

Если выполнить обновление с версии 5.45 или более ранней, на устройстве с установленным вручную сертификатом AXIS Camera Station Pro автоматически использует существующий корневой CA для установки нового сертификата после истечения срока действия вручную установленного сертификата.

Примечание

При создании сертификата ЦС он добавляется в раздел «Доверенные корневые сертификаты Windows».

Импорт центра сертификации

При установке сертификата CA от другого центра сертификации можно использовать AXIS Camera Station Pro в качестве промежуточного центра сертификации. Импортируйте существующий CA, содержащий сертификат и закрытый ключ, чтобы разрешить AXIS Camera Station Pro подписывать сертификаты от имени этого CA. Файл должен быть в формате PKCS#12, сертификат должен содержать базовое ограничение (2.5.29.19), указывающее, что он является сертификатом CA, а также должен использоваться в течение срока действия. Чтобы импортировать CA вместо существующего, см. *Замена ЦС, on page 151*.

Примечание

- Если для импортированного ЦС не требуется пароль, то при каждом запросе на ввод пароля будет открываться диалоговое окно. Например, если вы используете HTTPS или IEEE на устройстве либо добавляете устройство. Чтобы продолжить, нажмите **OK**.
- При импорте сертификата ЦС он добавляется в раздел «Доверенные корневые сертификаты Windows».
- При импорте промежуточного сертификата ЦС корневой сертификат должен уже присутствовать в хранилище сертификатов Windows. Если корневой сертификат отсутствует, импорт завершается

ошибкой и отображается сообщение об ошибке. AXIS Camera Station Pro продолжает использовать предыдущий CA.

- После удаления AXIS Camera Station Pro необходимо вручную удалить импортированные сертификаты ЦС из раздела «Центры доверенных корневых сертификатов Windows».

Замена ЦС

Чтобы заменить ЦС, который выдает подписанные сертификаты, используемые на устройствах с HTTPS-подключением:

1. Перейдите в раздел **Configuration > Security > Certificates > HTTPS (Конфигурация > Безопасность > Сертификаты > HTTPS)**.
2. Выключите параметр **Validate device certificate (Проверять сертификат устройства)**.
3. В разделе **Certificate authority (Центр сертификации)** нажмите кнопку **Generate (Создать)** или **Import (Импортировать)**.
4. Введите пароль и нажмите **OK**.
5. Выберите срок действия (число дней) подписанных сертификатов клиента/сервера.
6. Выберите в меню **Конфигурация > Устройства > Управление**.
7. Щелкните устройства правой кнопкой мыши и выберите **Security > HTTPS > Enable/Update (Безопасность > HTTPS > Активировать/обновить)**.
8. Перейдите в меню **Configuration (Конфигурация) > Security (Безопасность) > Certificates (Сертификаты)> HTTPS** и включите **Validate device certificate (Проверять сертификат устройства)**.

Создание пользовательского сертификата

AXIS Camera Station Pro позволяет создавать пользовательские сертификаты, подписанные собственным центром сертификации. Такие сертификаты можно применять, например, для внешних HTTPS-точек. Обратите внимание, что по истечении срока действия эти сертификаты потребуется обновлять вручную. Процесс создания пользовательского сертификата:

1. Перейдите в раздел **Configuration** > **Security** > **Certificates** (Конфигурация > Безопасность > Сертификаты).
2. В разделе **Issue custom certificate (Создать пользовательский сертификат)** нажмите **Issue certificate... (Создать сертификат)**.
3. Заполните необходимые данные сертификата и подтвердите, нажав **OK**.

Создание сертификата	
Общее имя (CN)	Идентификатор владельца сертификата. Обычно в качестве CN указывается полное доменное имя (FQDN) или IP-адрес, на котором будет установлен сертификат.
Пароль закрытого ключа	Пароль для защиты закрытого ключа сертификата.
Срок действия (дни)	Период действия сертификата в днях.
Аутентификация сервера	Выберите этот параметр, если сертификат используется на сервере для подтверждения его подлинности. Как правило, устройства и другие конечные точки, к которым AXIS Camera Station Pro подключается по HTTPS, считаются серверами, поэтому для их сертификатов следует использовать аутентификацию сервера.
Аутентификация клиента	Выберите этот параметр, если сертификат используется на клиенте для подтверждения

Создание сертификата	
	подлинности клиента перед подключением к серверу. Например, устройства, запрашивающие доступ к сети с контролем доступа по стандарту IEEE 802.1X, должны предъявлять такой сертификат.
Организация (O)	Название организации, которой принадлежит сертификат.
Коды страны (C)	Код страны владельца сертификата.
DNS SAN	Альтернативные DNS-имена. Дополнительные полные доменные имена (FQDN) для идентификации владельца сертификата. При создании сертификата общее имя (CN) автоматически добавляется в список DNS SAN. Можно ввести несколько адресов, разделенных запятыми, например, address-1.com,address-2.com.
IP SAN	Альтернативные IP-адреса (IP SAN). Дополнительные IP-адреса для идентификации владельца сертификата. Если в качестве общего имени (CN) указан IP-адрес, то он автоматически попадет в список IP SAN. Можно указать несколько адресов через запятую, например: 192.168.1.1,192.168.1.2.

HTTPS

По умолчанию AXIS Camera Station Pro проверяет сертификат HTTPS-сервера на каждом подключенном устройстве и не подключается к устройству с недействительным сертификатом. Сертификат сервера должен быть подписан активным CA в AXIS Camera Station Pro или проверен с помощью хранилища сертификатов Windows. AXIS Camera Station Pro также проверяет соответствие адреса в сертификате HTTPS устройства адресу, используемому для связи с устройством, если включен параметр **Validate device address (Проверять адрес устройства)**.

Камеры со встроенным ПО версии 7.20 или выше поставляются с предварительно настроенной конфигурацией, включающей самозаверяющий сертификат. Эти сертификаты не являются доверенными. Вместо этого создайте или импортируйте ЦС, чтобы позволить AXIS Camera Station Pro выпускать новые сертификаты для устройств при использовании HTTPS.

Проверить сертификат	Включите, чтобы подключаться только к устройствам с действительным сертификатом. Без проверки сертификатов могут подключаться устройства с недействительными сертификатами.
Проверка адреса устройства	Отключите этот параметр для более стабильной работы в сетях DHCP, в которых не используются имена узлов. Включите эту опцию, чтобы проверять соответствие адресов для обеспечения дополнительной безопасности. Рекомендуется включать этот параметр только в сетях, где устройства преимущественно используют имена узлов или статические IP-адреса.

Примечание

- Если защищенное соединение (HTTPS) недоступно, вы можете выпустить новый сертификат HTTPS. См. *Добавить устройства, on page 49*
- Для использования HTTPS требуется встроенное ПО версии 5.70 или выше — для видеоустройств и встроенное ПО версии 1.25 или выше — для устройств контроля доступа и аудиоустройств.

Ограничения

- Порты, не являющиеся портами по умолчанию (кроме 443), не поддерживаются.
- Для всех сертификатов в установочном пакете должен использоваться один и тот же пароль.
- Операции с сертификатами по незашифрованным каналам, например **Basic**, не поддерживаются. Установите для устройств значение **Encrypted & unencrypted (Зашифрованное и незашифрованное)** или **Encrypted only (Только зашифрованное)**, чтобы разрешить обмен данными по протоколу **Digest**.
- Нельзя включить HTTPS на сетевых коммутаторах AXIS T85 PoE+ Network Switch Series.

IEEE 802.1X

При аутентификации AXIS Camera Station Pro IEEE 802.1X supplicant — это сетевое устройство Axis, которое пытается подключиться к локальной сети. Аутентифицирующей стороной выступает сетевое устройство, например коммутатор Ethernet или беспроводная точка доступа. Сервер проверки подлинности обычно представляет собой хост, на котором работает программное обеспечение, поддерживающее протоколы RADIUS и EAP.

Для включения IEEE 802.1X необходимо импортировать сертификат ЦС по проверке подлинности IEEE 802.1X. Сертификат ЦС по проверке подлинности IEEE 802.1X и сертификат клиента IEEE 802.1X устанавливаются при включении или обновлении IEEE 802.1X. Сертификат для аутентификации можно получить из внешнего источника, например с сервера аутентификации IEEE 802.1X, или непосредственно создать в AXIS Camera Station Pro. Этот сертификат устанавливается на каждом устройстве Axis для проверки сервера аутентификации.

Примечание

Для использования сертификатов IEEE 802.1X требуется встроенное ПО версии 5.50 или выше — для видеоустройств и встроенное ПО версии 1.25 или выше — для устройств контроля доступа и аудиоустройств.

Настройка IEEE 802.1X:

1. Перейдите в раздел **Configuration > Security > Certificates (Конфигурация > Безопасность > Сертификаты)**.
2. В раскрывающемся списке **EAPOL Version (Версия EAPOL)** выберите версию расширяемого протокола аутентификации (EAP), которую необходимо использовать.
3. В раскрывающемся списке **EAPOL Version (Версия EAPOL)** выберите версию расширяемого протокола аутентификации (EAP), которую необходимо использовать.
4. Если выбран вариант **Custom (Пользовательский)**, введите текст, который будет использоваться в качестве идентификатора EAP.
5. Нажмите **Import (Импорт)** и выберите файл сертификата ЦС для проверки подлинности IEEE 802.1X.
6. В раскрывающемся списке **Common name (Общее имя)** выберите **Device IP address (IP-адрес устройства)** или **Device EAP identity (Идентификатор EAP устройства)** в качестве общего имени сертификатов, создаваемых для каждого устройства.
7. Выберите в меню **Конфигурация > Устройства > Управление**.
8. Щелкните устройства правой кнопкой мыши и выберите **Security > IEEE 802.1X > Enable/Update (Безопасность > IEEE 802.1X > Активировать/обновить)**.

Ограничения

- В случае устройств с несколькими сетевыми адаптерами (например, беспроводных камер) протокол IEEE 802.1X можно включить только для первого адаптера, которым обычно является адаптер проводной сети.
- Устройства, у которых отсутствует параметр `Network.Interface.I0.dot1x.Enabled`, не поддерживаются. Например: AXIS P39 Series, AXIS T85 Series и AXIS T87 Video Decoder
- Операции с сертификатами по незашифрованным каналам, например **Basic**, не поддерживаются. Установите для устройств значение **Encrypted & unencrypted (Зашифрованное и незашифрованное)** или **Encrypted only (Только зашифрованное)**, чтобы разрешить обмен данными по протоколу **Digest**.

Предупреждение об окончании срока действия сертификата

Предупреждение появляется, когда срок действия сертификата уже истек или скоро истекает. Для некоторых сертификатов также запускается системный сигнал тревоги. Это правило относится ко всем сертификатам клиента и сервера, сертификатам ЦС устройств, установленным AXIS Camera Station Pro, к сертификату ЦС AXIS Camera Station Pro и сертификату IEEE 802.1X. Предупреждение отображается в виде сообщения в разделе **Status (Состояние)** на странице **Device management (Управление устройством)**, а также в виде значка в списке **Installed certificates (Установленные сертификаты)**.

В разделе **Certificate expiration warning (Предупреждение об истечении срока действия сертификата)** укажите, за сколько дней до истечения срока действия AXIS Camera Station Pro должно отображать предупреждение.

Продление сертификата

Продление действия сертификата между сервером и устройствами

Сертификаты клиента и сервера, созданные AXIS Camera Station Pro автоматически, автоматически обновляются за семь дней до появления предупреждения об истечении срока действия. Для этого на устройстве должна быть включена функция HTTPS или IEEE 802.1X. Для ручного обновления или изменения сертификата см. *Безопасность, on page 75*.

Продление действия сертификата между сервером и клиентом

Новый сертификат сервера можно создать на вкладке **Certificates (Сертификаты)** в AXIS Camera Station Pro Service Control. Указания о том, как это сделать, см. в разделе *Сертификаты, on page 238*.

Сброс пароля

1. Перейдите в раздел **Configuration > Security > Certificates (Конфигурация > Безопасность > Сертификаты)**.
2. Отключите **Validate device certificate (Проверять сертификат устройства)**, чтобы устройства, использующие сертификаты CA, оставались доступными.
3. В разделе **Certificate authority (Центр сертификации)** нажмите кнопку **Generate (Создать)** и введите свой пароль.
4. В разделе **Certificate authority (Центр сертификации)** нажмите **Export (Экспорт)**, чтобы сохранить сертификат ЦС локально.
5. Перейдите в раздел **Configuration > Devices > Management (Конфигурация > Устройства > Управление)** и включите HTTPS на выбранных устройствах.
6. Включите параметр **Validate device certificate (Проверять сертификат устройства**.

Настройте контроль доступа

Если вы добавили в свою систему дверной сетевой контроллер Axis, оборудование контроля доступа можно настроить в AXIS Camera Station версии 6.x или более поздней версии.

Полное описание рабочего процесса настройки дверного сетевого контроллера Axis в AXIS Camera Station Pro см. в разделе *Настройка сетевого дверного контроллера Axis*.

Примечание

Прежде чем приступать к настройке, обязательно выполните следующее:

- Обновите версию AXIS OS контроллера в **Configuration (Конфигурация) > Devices (Устройства) > Management (Управление)**.
- Установите дату и время для контроллера в разделе **Configuration > Devices > Management (Конфигурация > Устройства > Управление)**.
- Активируйте протокол HTTPS на контроллере в разделе **Configuration > Devices > Management (Конфигурация > Устройства > Управление)**.

Рабочий процесс настройки контроля доступа

1. Инструкции по редактированию предварительно заданных профилей идентификации или созданию нового профиля см. в *Профили идентификации, on page 174*.
2. Чтобы использовать пользовательскую настройку для форматов карт и длины PIN-кода, см. *Форматы карт и ПИН-коды, on page 176*.
3. Добавьте дверь и примените профиль идентификации к двери. См. *Добавьте дверь, on page 158*.
4. Настройте дверь:
   - *Add a door position sensor (Добавление датчика положения двери), on page 165*
   - *Add an emergency sensor (Добавление датчика аварийной ситуации), on page 167*
   - *Добавление считывающего устройства, on page 168*
   - *Добавление REX-устройства, on page 171*
5. Добавьте зону и добавьте двери в зону. См. *Добавление зоны, on page 171*.

Совместимость программного обеспечения устройств для дверных контроллеров

Внимание

При обновлении AXIS OS на дверном контроллере учитывайте следующее:

- **Поддерживаемые версии AXIS OS**: перечисленные ниже поддерживаемые версии AXIS OS применяются только при обновлении с исходной рекомендуемой версии AXIS Camera Station Pro и при наличии в системе настроенной двери. Если система не соответствует этим условиям, необходимо обновить ее до рекомендуемой версии AXIS OS для конкретной версии AXIS Camera Station Pro.
- **Минимальная поддерживаемая версия AXIS OS**: самая старая установленная в системе версия AXIS OS определяет минимальную поддерживаемую версию AXIS OS с ограничением в две предыдущие версии. Предположим, вы используете версию AXIS Camera Station Pro 6.5 и обновляете все устройства до рекомендуемой версии AXIS OS 12.0.86.2. После этого версия AXIS OS 12.0.86.2 становится минимальной поддерживаемой версией системы в дальнейшем.
- **Обновление до версии AXIS OS выше рекомендуемой**: предположим, вы обновили систему до версии AXIS OS, более новой, чем рекомендуемая для определенной версии AXIS Camera Station Pro. После этого вы всегда можете без проблем выполнить откат до рекомендуемой версии AXIS OS, если она находится в пределах ограничений поддержки, установленных для версии AXIS Camera Station Pro.
- **Будущие рекомендации по AXIS OS:** всегда используйте рекомендуемую версию AXIS OS для соответствующей версии AXIS Camera Station Pro, чтобы обеспечить стабильность системы и полную совместимость.
- **Изменение ветки**: для перехода с ветки 10.12.xx на ветку 11.0.xx или более позднюю требуется восстановление заводских настроек.

В таблице ниже приведены минимальные и рекомендуемые версии AXIS OS для каждой версии AXIS Camera Station Pro:

Версия AXIS Camera Station	Минимальная версия AXIS OS	Рекомендуемая версия AXIS OS
Pro 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

Двери и зоны

Перейдите в раздел **Configuration > Access control > Doors and zones (Конфигурация > Контроль доступа > Двери и зоны > Зоны)**, чтобы получить обзор и настроить двери и зоны.

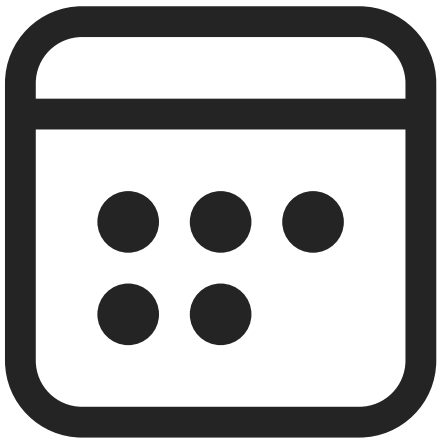
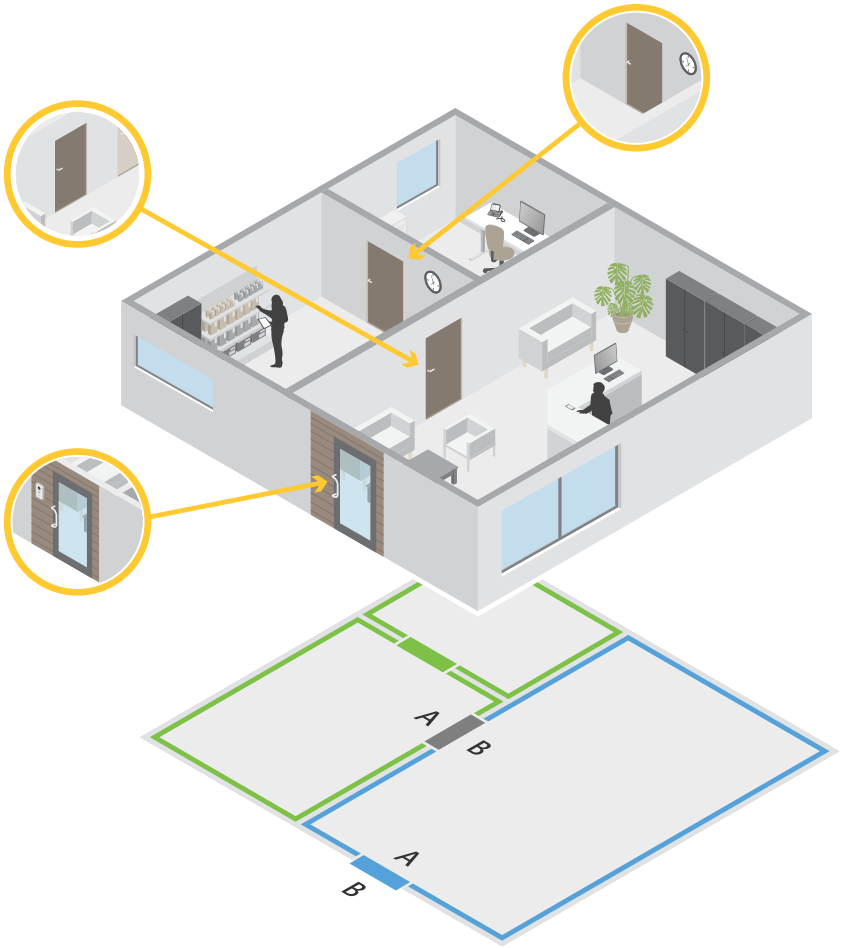
 Действия в ручном режиме	Задайте состояние двери вручную. Выберите один из следующих вариантов): **Reset (Сбросить)** (соблюдение правил системы), **Grant access (Предоставить доступ)**, (разблокировка двери на 7 секунд), **Unlock (Разблокировать)**, (оставить дверь незапертой), **Lock (Заблокировать)**, (оставить дверь запертой) или **Lockdown (Блокировка)**, (вход и выход запрещены).
 **Расписания отпирания**	Задайте расписание для автоматического отпирания дверей в определенное время. В остальное время двери остаются запертыми. Чтобы первый человек вручную открывал дверь перед активацией графика, включите функцию **First person in** (Первый входящий человек).
Профиль идентификации	Изменить профиль идентификации для дверей.

Схема контактов	Посмотреть схему контактов контроллера, связанную с дверью. Чтобы распечатать таблицу PIN-кодов, нажмите **Print (Печать)**.
Защищенный канал	Включение или выключение защищенного канала OSDP Secure Channel для конкретного считывателя.

Двери	
Название	Имя двери.
Тип	Тип конфигурации двери.
Устройство	Устройство, подключенное к двери.
IP-адрес	IP-адрес дверного контроллера, подключенного к двери.
Сторона A	Зона, в которой находится сторона A двери.
Сторона B	Зона, в которой находится сторона B двери.
Профиль идентификации	Профиль идентификации, применяемый к двери.
Батарея	Состояние батареи дверного контроллера.
Статус	Состояние двери. • **Online (В сети)**: дверь находится в сети и работает исправно. • **Reader offline (Считывающее устройство не в сети)**: Считывающее устройство в конфигурации двери не в сети. • **Reader error (Ошибка считывающего устройства)**: считыватель не поддерживает защищенный канал или эта функция отключена для считывающего устройства. • **Old firmware (Старая версия встроенного ПО)**: на устройстве установлена устаревшая версия встроенного ПО. Для оптимальной производительности и безопасности обновите встроенное ПО.
Зоны	
Название	Имя зоны.
Количество дверей	Количество дверей, включенных в зону.
Уровень безопасности	Уровень безопасности для данной зоны.

Пример конфигурации дверей и зон



- Имеется две зоны: зеленая и синяя.
- Имеется три двери: зеленая, синяя и коричневая.
- Зеленая дверь — это внутренняя дверь в зеленой зоне.
- Синяя дверь — это дверь по периметру, относящаяся только к синей зоне.
- Коричневая дверь — это дверь по периметру, принадлежащая зеленой и синей зонам.

Добавьте дверь

Примечание

- Для дверного контроллера можно настроить одну дверь с двумя замками либо же две двери с одним замком в каждой. Мультиконтроллеры поддерживают дополнительные конфигурации замков.
- Если у контроллера двери нет дверей и используется новая версия AXIS Camera Station Pro со старой версией встроенного ПО контроллера двери, система не позволяет добавить дверь. При этом система позволяет добавлять новые двери в системные контроллеры со старой версией встроенного ПО, если в системе уже имеется существующая дверь.

Чтобы добавить дверь:

1. Перейдите в **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
2. Нажмите + . **Add (Добавить)** и выберите тип двери в раскрывающемся списке.

Типы дверей	
Дверной датчик	Обычная дверь с контролем состояния двери, поддерживающая замки и считывающие устройства. Требуется дверной контроллер.
Этаж	Тип двери для управления лифтом, обеспечивающий аутентификацию доступа к этажам лифта с использованием считывающих устройств для идентификационных карт. Подробнее см. в разделе *Добавить этаж BETA, on page 166*.
Контролируемая дверь	Дверь, которая может сообщать, открыта она или закрыта. Подробнее см. в разделе *Добавление двери с мониторингом, on page 166*.
Беспроводная сеть	Дверь, которую можно настроить с беспроводными замками и коммуникационными хабами ASSA ABLOY Aperio®. Подробнее см. в разделе *Добавление беспроводной блокировки, on page 163*.
Выделенная дверь	Заполнитель двери, который можно добавить в систему без выбора аппаратного обеспечения.

3. Введите имя двери и выберите контроллер двери в раскрывающемся списке **Device (Устройство)** для привязки к двери. Контроллер отображается неактивным, если добавить еще одну дверь невозможно, контроллер находится вне сети или HTTPS не включен.
4. Нажмите **Next (Далее)**, чтобы перейти к странице конфигурации двери.
5. Выберите порт реле из раскрывающегося меню **Primary lock (Главная блокировка)**.
6. Чтобы настроить два замка двери, выберите порт реле из раскрывающегося меню **Secondary lock (Вторичная блокировка)**.
7. Выберите профиль идентификации. См. *Профили идентификации, on page 174*.
8. Настройте дверь, добавив датчики или считыватели в разделах **Sensors (Датчики)**, **Side A (Сторона A)** и **Side B (Сторона B)**.
9. Настройте параметры конкретной двери. См. *Настройки двери, on page 160*.
10. Настройка уровня безопасности. См. *Уровень безопасности двери, on page 161*.
11. Нажмите **Save (Сохранить)**.

Копирование конфигурации двери:

1. Перейдите в **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
2. Нажмите **+ Add (Добавить)**.
3. Введите имя двери и выберите контроллер двери в раскрывающемся списке **Device (Устройство)** для привязки к двери.
4. Нажмите **Next (Далее)**.
5. Выберите существующую конфигурацию двери из раскрывающегося меню **Copy configuration (Копировать конфигурацию)**. Отображаются подключенные двери, и контроллер становится серым, если он был настроен с двумя дверями или одной дверью с двумя замками.
6. Если необходимо, измените параметры.
7. Нажмите **Save (Сохранить)**.

Добавление и настройка дверей и зон

Настройки двери

Чтобы изменить параметры двери:

1. Перейдите к пункту **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
2. Выберите дверь, которую требуется изменить.
3. Нажмите кнопку **Edit (Изменить)**.
4. В разделе **Door settings (Настройки двери)** измените любые параметры и нажмите **Save (Сохранить)**.

Время доступа (с)	Задайте время в секундах, в течение которого дверь остается незапертой после предоставления доступа. Дверь снова запирается при закрытии, даже если заданное время еще не истекло.
Open-too-long time (sec) (Время «открыта слишком долго» (с))	Действительно только при настроенном датчике состояния двери. Задайте время в секундах, в течение которого дверь может оставаться открытой. Если по истечении заданного времени дверь остается открытой, срабатывает тревога о слишком длительном открытии двери. Настройте правило действия, определяющее реакцию системы на это событие.
Длительное время доступа (сек)	Задайте время в секундах, в течение которого дверь остается незапертой после предоставления доступа держателям карт, для которых включен этот параметр. Этот параметр имеет приоритет над стандартным временем доступа.
Long open-too-long time (sec) (Длительное время «открыта слишком долго» (с))	Действительно только при настроенном датчике состояния двери. Задайте время в секундах, в течение которого дверь может оставаться открытой для держателей карт, для которых включен **Long access time (Увеличенное время доступа)**. Переопределяет стандартное время слишком длительного открытия двери.
Время задержки повторного запирания (мс)	Задайте время в миллисекундах, в течение которого дверь остается незапертой после ее открытия или закрытия.
Повторная блокировка	• **After opening (После открытия)**: действительно только при добавленном датчике состояния двери. • **After closing (После закрытия)**: действительно только при добавленном датчике состояния двери.

Дверь открыта силой	Выберите, должна ли система формировать системную тревогу при принудительном открытии двери. Требуется датчик положения двери (DPS).
Дверь открыта слишком долго	Выберите, должна ли система формировать системную тревогу, если дверь остается открытой слишком долго.

Чтобы удалить дверь:

1. Перейдите к пункту **Configuration > Access control > Doors and zones > Doors (Конфигурация > Контроль доступа > Двери и зоны > Двери)**.
2. Выберите дверь в списке.
3. Нажмите **Remove** (Удалить) и подтвердите.

Действия в ручном режиме

Вы можете вручную выполнять следующие действия с дверями и зонами:

Сброс – Возвращает к настроенным системным правилам.

Предоставить доступ – Разблокировка двери или зоны на 7 секунд, а затем повторная блокировка.

Отпереть – Дверь остается разблокированной до выполнения сброса.

Lock (Заблокировать) – Обеспечивает блокировку двери до тех пор, пока система не предоставит доступ владельцу карты.

Блокировать – Никто не войдет и не выйдет, пока вы не сбросите или не разблокируете систему.

Чтобы выполнить действие вручную:

1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.
2. Выберите дверь или зону.
3. Нажмите на любое действие в ручном режиме.

Уровень безопасности двери

К двери можно добавить следующую функцию безопасности:

Правило двух человек – Правило двух человек требует введения учетных данных двумя людьми для получения доступа.

Двойной свайп – Двойное прикладывание карты позволяет держателю карты изменить текущее состояние двери. Например, с его помощью можно запереть или разблокировать дверь вне установленного расписания, что удобнее разблокировки двери через систему. Двойное прикладывание карты не влияет на существующее расписание. Например, если по расписанию дверь должна запираться в конце рабочего дня, а сотрудник выходит на обеденный перерыв, дверь все равно запрется согласно расписанию.

Уровень безопасности можно настроить при добавлении новой двери или применить его к существующей двери.

Для добавления **правила двух человек** к существующей двери:

1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.
2. Выберите дверь, для которой нужно настроить уровень безопасности.

3. Нажмите кнопку **Edit** (Изменить).
4. Нажмите **Security level (Уровень безопасности)**.
5. Включение **правила двух человек.**
6. Нажмите **Применить.**

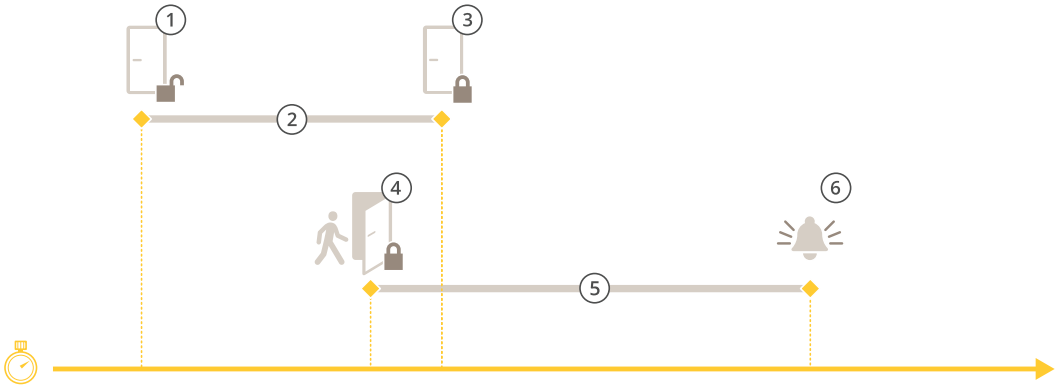
Правило двух человек	
Сторона A и **сторона B**	Выберите, с какой стороны двери будет использоваться правило.
Расписания	Выберите время, в которое будет действовать правило.
Время тайм-аута (в секундах)	Тайм-аут — максимально допустимый интервал между прикладываниями карты или другими действительными предъявлениями учетных данных.

Для добавления **двойного свайпа** к существующей двери:

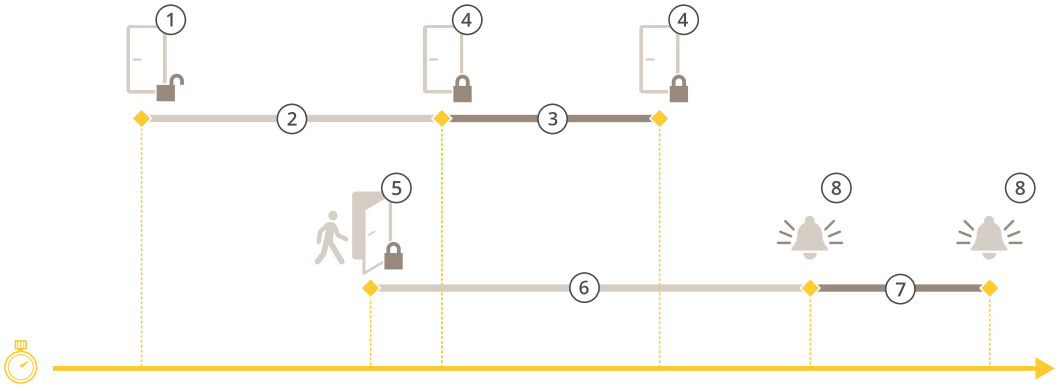
1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.
2. Выберите дверь, для которой нужно настроить уровень безопасности.
3. Нажмите кнопку **Edit** (Изменить).
4. Нажмите **Security level (Уровень безопасности)**.
5. Для включения функции **двойного свайпа**.
6. Нажмите **Применить.**
7. Для применения **двойного свайпа** к владельцу карты.
   7.1. Откройте вкладку **Access Management (Управление доступом)**.
   7.2. Нажмите ⋮ рядом с владельцем карты для редактирования и выберите **Edit (Изменить)**.
   7.3. Нажмите **More (Дополнительно)**.
   7.4. Выберите **Allow double-swipe (Разрешить двойной свайп)**.
   7.5. Нажмите **Применить.**

Двойной свайп	
Время тайм-аута (в секундах)	Тайм-аут — максимально допустимый интервал между прикладываниями карты или другими действительными предъявлениями учетных данных.

Параметры времени



1 Доступ предоставлен — замок отпирается
2 Время доступа
3 No action taken - lock stays locked (Действие не выполняется — замок остается запертым)
4 Выполнено действие (открыта дверь) — замок запирается или остается незапертым до закрытия двери
5 Время до подачи сигнала тревоги «Открыта слишком долго»
6 Сигнал тревоги «Открыта слишком долго» выключается



1 Доступ предоставлен — замок отпирается
2 Время доступа
3 2+3: Длительное время доступа
4 No action taken - lock stays locked (Действие не выполняется — замок остается запертым)
5 Выполнено действие (открыта дверь) — замок запирается или остается незапертым до закрытия двери
6 Время до подачи сигнала тревоги «Открыта слишком долго»
7 6+7: Длительное время до подачи сигнала тревоги «Открыта слишком долго»
8 Сигнал тревоги «Открыта слишком долго» выключается

Добавление беспроводной блокировки

AXIS Camera Station Pro поддерживает беспроводные замки и коммуникационные концентраторы ASSA ABLOY Aperio®. Беспроводная блокировка подключается к системе через концентратор Aperio, подсоединенный к разъему RS485 дверного контроллера. Для одного дверного контроллера можно подключить до 16 беспроводных блокировок.

Примечание

- Для выполнения настройки требуется, чтобы на дверном контроллере Axis была установлена AXIS OS версии 11.6.16.1 или более поздней.
- Для выполнения настройки требуется, чтобы для AXIS Door Controller Extension имелась действительная лицензия.
- Время на дверном контроллере Axis и сервере AXIS Camera Station Pro должно быть синхронизировано.
- Прежде чем начать работу, необходимо выполнить сопряжение блокировок Aperio с концентратором Aperio, используя прикладное средство с поддержкой технологии ASSA ABLOY.
- К каждому разъему RS485 можно подключить только один сетевой концентратор Aperio. Подключение нескольких устройств по одной линии не поддерживается.
- В автономном режиме беспроводные замки не выполняют расписания разблокировки.

1. Выполните доступ к дверному контроллеру.
   1.1. Откройте меню **Конфигурация > Устройства > Другие устройства**.
   1.2. Откройте веб-интерфейс дверного контроллера, подключенного к концентратору Aperio.
2. Включите AXIS Door Controller Extension.
   2.1. В веб-интерфейсе контроллера двери перейдите в раздел **Apps (Приложения)**.
   2.2. Откройте контекстное меню AXIS Door Controller Extension .
   2.3. Щелкните **Activate license with a key (Активировать лицензию ключом)** и выберите нужную лицензию.
   2.4. Включите **AXIS Door Controller Extension**.
3. Подключите беспроводную блокировку к дверному контроллеру через концентратор.
   3.1. В веб-интерфейсе дверного контроллера выберите **Access control > Wireless locks (Контроль доступа > Беспроводные блокировки)**.
   3.2. Нажмите **Connect communication hub (Подключить концентратор)**.
   3.3. Введите имя концентратора и нажмите **OK**.
   3.4. Нажмите **Connect wireless lock (Подключить беспроводную блокировку)**.
   3.5. Выберите адрес и возможности добавляемой блокировки замка и нажмите кнопку **Save (Сохранить)**.
4. Добавьте и настройте дверь с беспроводной блокировкой.
   4.1. В AXIS Camera Station Pro перейдите к пункту **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
   4.2. В разделе **Doors (Двери)** нажмите **Add (Добавить)**.
   4.3. В качестве **Door type (Тип двери)** выберите **Wireless door (Беспроводная дверь)** и дверной контроллер, подключенный к коммуникационному концентратору Aperio.
   4.4. Нажмите **Next (Далее)**.
   4.5. Выберите **Wireless lock (Беспроводная блокировка)**.

4.6. Определите стороны двери A и B и добавьте нужные датчики. Дополнительную информацию вы найдете по адресу *Двери и зоны, on page 156*.

4.7. Нажмите **Save (Сохранить)**.

После подключения беспроводного замка в обзоре дверей отображаются уровень заряда его аккумулятора и состояние.

Уровень заряда аккумулятора	Action (Действие)
Хорошо	None (Нет)
Низкая	Замок работает нормально, однако аккумулятор следует заменить до того, как его уровень заряда достигнет критического значения.
Критические ошибки	Замените аккумулятор. Блокировка, возможно, работает неправильно.

Состояние замка	Action (Действие)
Дистанционное обучение	None (Нет)
Заклинивание замка	Устраните любые механические проблемы с замком.

Add a door position sensor (Добавление датчика положения двери)

Датчик положения двери — это переключатель, отслеживающий физическое состояние двери. К двери можно добавить датчик положения двери и настроить способ его подключения.

1. Перейдите на страницу конфигурации двери. См. *Добавьте дверь, on page 158*.
2. В разделе **Sensors (Датчики)** нажмите **Add (Добавить)**.
3. Выберите **Door position sensor (Датчик положения двери)**.
4. Выберите порт ввода-вывода, к которому вы хотите подключить дверной монитор.
5. В разделе **Door open if (Дверь открыта, если)** выберите способ подключения цепей дверного монитора.
6. Чтобы изменения в состоянии дискретного входа до его перехода в новое стабильное состояние игнорировались, задайте параметр **Debounce time (Время устранения дребезга)**.
7. Чтобы при разрыве соединения между контроллером двери и датчиком положения двери срабатывало событие, включите **Supervised input (Контролируемый вход)**. См. *Контролируемые входы, on page 173*.

Дверь открыта, если	
Цепь разомкнута	Цепь дверного монитора является нормально замкнутой. Дверной монитор отправляет сигнал открытия двери при размыкании цепи. Когда цепь замкнута, дверной монитор отправляет сигнал, означающий, что дверь закрыта.
Цепь замкнута	Цепь дверного монитора является нормально разомкнутой. Дверной монитор отправляет сигнал открытия двери при замыкании цепи. Дверной монитор отправляет сигнал закрытия двери при размыкании цепи.

Добавление двери с мониторингом

Дверь с мониторингом – это тип двери, который позволяет отслеживать ее состояние (открыта или закрыта). Например, такую функцию можно использовать для противопожарной двери, на которой замок не нужен, однако требуется контроль положения двери.

Дверь с мониторингом отличается от обычной двери с дверным монитором. Обычная дверь с дверным монитором поддерживает замки и устройства считывания и при этом требует наличия дверного контроллера. Дверь с мониторингом поддерживает один датчик положения, но требует только сетевого модуля ввода-вывода, подключенного к дверному контроллеру. К одному сетевому модулю ввода-вывода можно подключить до пяти датчиков положения двери.

Примечание

Для двери с мониторингом требуется сетевой модуль ввода-вывода AXIS A9210 с последней версией прошивки, включая приложение AXIS Monitoring Door ACAP.

Настройка двери с мониторингом:

1. Установите AXIS A9210 и обновите его до последней версии AXIS OS.
2. Установите датчики положения двери.
3. В AXIS Camera Station Pro выберите **Configuration** > **Access control** > **Doors and zones** (Конфигурация > Управление доступом > Двери и зоны).
4. Нажмите **Add door (Добавить дверь)**.
5. Введите имя.
6. В разделе **Type (Тип)** выберите **Monitoring door (Дверь с мониторингом)**.
7. В разделе **Device (Устройство)** выберите ваш сетевой модуль ввода-вывода.
8. Нажмите **Next (Далее)**.
9. В разделе **Sensors (Датчики)** нажмите **Add (Добавить)** и выберите **Door position sensor (Датчик положения двери)**.
10. Выберите порт ввода-вывода, к которому подключен датчик положения двери.
11. Нажмите **Добавить**.

Добавить этаж BETA

Этаж — это тип двери, который используется для управления доступом к этажам лифта. При добавлении этажа вы создаете ресурс лифта, который группирует все этажи для этого лифта. Каждый этаж использует считывающее устройство для карт внутри кабины лифта для аутентификации пользователей перед предоставлением доступа к этому этажу.

Прежде чем начать, потребуется выполнить:

- Подключенный к системе дверной контроллер, поддерживающий сеть, такой как *A1610*, *A1710-B*, or *A1810-B*.
- Модуль расширения реле *A9910 I/O Relay Expansion Module*, если требуется дополнительное количество реле. Для добавления модуля к контроллеру см. раздел .

Примечание

Эта функция находится в стадии Бета и в настоящее время поддерживает до 16 этажей и считывающих устройств для карт.

Чтобы настроить этаж:

1. Перейдите в **Configuration > Access control > Doors and zones (Конфигурация > Контроль доступа > Двери и зоны)**.
2. Нажмите **Add (Добавить)** и выберите **Floor (Этаж)** BETA.
3. Введите имя для этажа.

4. Выберите ваш контроллер.
5. Во вкладке **Elevator (Лифт)** выберите существующий лифт и нажмите **Create new elevator (Создать новый лифт)**, чтобы добавить новый, а затем введите имя.
6. В разделе **Side A (Сторона A)** выберите **Card reader (Считывающее устройство для карт)** и конфигурируйте считывающее устройство. **Side B (Сторона Б)** не подлежит конфигурации по соображениям безопасности.
7. Нажмите **Save and add new (Сохранить и добавить новый)**, чтобы добавить дополнительные этажи к тому же лифту. Конфигурация лифта и считывающего устройства остается неизменной для следующего этажа. Этот параметр доступен только при наличии реле в контроллере.
8. Нажмите **Save (Сохранить)** после добавления этажа. Этажи отображаются в формате «Название лифта — Название этажа», например: «West Side — Floor 1»

Примечание

- Считывающие устройства, используемые на нескольких этажах, можно редактировать только на первом этаже, на котором они были добавлены.
- Лифты автоматически удаляются, когда удаляются все связанные с ними этажи.

Add an emergency sensor (Добавление датчика аварийной ситуации)

Вы можете добавить и настроить аварийный вход для инициирования действия, которое блокирует или разблокирует дверь. Можно также настроить способ подключения цепи.

1. Перейдите на страницу конфигурации двери. См. *Добавьте дверь, on page 158*.
2. В разделе **Sensors (Датчики)** нажмите **Add (Добавить)**.
3. Выберите **Emergency input (Вход чрезвычайной ситуации)**.
4. В разделе **Emergency state (Чрезвычайная ситуация)** выберите способ подключения цепи.
5. Чтобы изменения в состоянии дискретного входа до его перехода в новое стабильное состояние игнорировались, задайте параметр **Debounce time (ms) (Время устранения дребезга (мс))**.
6. Выберите **Emergency action (Действие при чрезвычайной ситуации)**, которое должно запускаться при поступлении на дверь сигнала чрезвычайной ситуации.

Аварийное состояние	
Цепь разомкнута	Ко входу чрезвычайной ситуации подключена нормально замкнутая цепь. Сигнал чрезвычайной ситуации отправляется на вход чрезвычайной ситуации, когда цепь размыкается.
Цепь замкнута	Ко входу чрезвычайной ситуации подключена нормально разомкнутая цепь. Сигнал чрезвычайной ситуации отправляется на вход чрезвычайной ситуации, когда цепь замыкается.

Аварийное действие	
Отпереть дверь	Дверь отпирается при получении сигнала чрезвычайной ситуации.
Запереть дверь	Дверь запирается при получении сигнала чрезвычайной ситуации.

Добавление IP-считывателя

В качестве считывателя можно использовать сетевой интерком Axis или другое IP-устройство. Перед назначением устройства на дверь нужно добавить его в AXIS Camera Station Pro.

Примечание

Перед началом работы убедитесь, что IP-считыватель включен и подключен к той же сети, что и AXIS Camera Station Pro.

1. Перейдите в **Configuration (Конфигурация)> Devices (Устройства)> Add devices (Добавить устройства)**.
2. Выберите IP-считыватель из списка обнаруженных устройств и нажмите **Add (Добавить)**.
3. При появлении запроса введите учетные данные устройства.

После добавления устройства его можно назначить на дверь. См. *Добавление считывающего устройства, on page 168*.

Добавление считывающего устройства

Можно настроить дверной контроллер на несколько проводных считывающих устройств. Вы можете добавить считывающее устройство только с одной стороны или с обеих сторон двери.

Если применить к считывателю пользовательскую настройку форматов карт или длины PIN-кода, она отображается в **Card formats (Форматы карт)** в разделе **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**. См. *Двери и зоны, on page 156*.

Примечание

- К дверному контроллеру можно добавить до 16 считывающих устройств Bluetooth. Дополнительные сведения см. в разделе *Добавление считывающего Bluetooth-устройства, on page 169*.
- Если в качестве IP-считывателя используется сетевое переговорное устройство Axis, система использует конфигурацию PIN-кода, заданную на веб-странице устройства.

1. Перейдите на страницу конфигурации двери. См. *Добавьте дверь, on page 158*.
2. Для одной стороны двери нажмите **Add (Добавить)**.
3. Выберите **Card reader (Устройство для считывания карт)**.
4. Выберите **Reader type (Тип считывающего устройства)**.
5. Для использования пользовательской длины PIN-кода для этого считывателя.
   5.1. Нажмите **Дополнительно**.
   5.2. Включите параметр **Custom PIN length (Пользовательская длина PIN-кода)**.
   5.3. Задайте параметры **Min PIN length (Минимальная длина PIN-кода)**, **Max PIN length (Максимальная длина PIN-кода)** и **End of PIN character (Последний знак PIN-кода)**.
6. Использование пользовательского формата карты для данного считывателя:
   6.1. Нажмите **Дополнительно**.
   6.2. Включите параметр **Custom card formats (Пользовательские форматы карт)**.
   6.3. Выберите требуемые форматы карт для считывающего устройства. Если формат карты с такой же битовой длиной уже используется, необходимо сначала деактивировать этот формат. Если настройка формата карты отличается от настроек, заданных в системе, в клиенте отображается значок предупреждения.
7. Нажмите **Добавить**.
8. Чтобы добавить считывающее устройство с другой стороны двери, повторите эту процедуру.

Сведения об установке AXIS Barcode Reader см. в *Установка считывателя штрих-кодов AXIS, on page 179*.

Тип считывателя карт	
OSDP RS485, полудуплекс	Для считывателей RS485 выберите **OSDP RS485 half duplex (OSDP RS485, полудуплекс** и порт считывателя.
Wiegand	В случае считывателей, использующих протоколы Wiegand, выберите **Wiegand** и порт считывателя.
Считыватель IP-адресов	В случае IP-считывателей выберите **IP reader (IP-считыватель)** и выберите устройство из раскрывающегося меню. Сетевые переговорные устройства Axis можно использовать в качестве IP-считывающих устройств.

Wiegand	
Контрольный индикатор	Выберите **Single wire (Однопроводной)** или **Dual wire (R/G) (Двухпроводной (кр/зел))**. Считыватели с управлением двумя светодиодами используют разные провода для красного и зеленого цветов.
Оповещение о несанкционированном доступе	Выберите состояние цепи, при котором активируется вход контроля вскрытия считывающего устройства. • **Open circuit (Разомкнутая цепь)**: считывающее устройство передает двери сигнал вскрытия при разомкнутой цепи. • **Closed circuit (Замкнутая цепь)**: считывающее устройство передает двери сигнал вскрытия при замкнутой цепи.
Время устранения дребезга для обнаружения несанкционированных действий	Чтобы изменения в состоянии входа сигнала несанкционированного доступа до его перехода в новое стабильное состояние игнорировались, задайте параметр **Tamper debounce time (Время устранения дребезга для обнаружения несанкционированных действий)**.
Контролируемый вход	Включите параметры, чтобы при прерывании соединения между дверным контроллером и считывающим устройством инициировалось событие. См. *Контролируемые входы, on page 173*.

Добавление считывающего Bluetooth-устройства

С помощью сетевого Bluetooth-считывающего устройства AXIS A4612 можно расширить возможности проводного подключения дверных контроллеров Axis. К одному дверному контроллеру можно подключить до 16 таких считывающих устройств. Каждый считыватель способен управлять замком двери, кнопкой выхода (REX) и датчиком положения двери (DPS).

Для добавления и использования этих считывающих устройств дополнительные лицензии не требуются.

Чтобы добавить AXIS A4612 Network Bluetooth Reader к двери:

1. Убедитесь, что AXIS A4612 сопряжен с контроллером двери. См. *Используйте приложение AXIS Mobile Credential в качестве данных доступа по Bluetooth, on page 170*.
2. Перейдите на страницу конфигурации двери. См. раздел *Добавьте дверь, on page 158*.

3. На одной из сторон двери нажмите **Add (Добавить)**, затем **Card reader (Считывающее устройство для карт)**.
4. Выберите **IP-считыватель**, затем выберите сопряженный AXIS A4612 из выпадающего списка. Если это считывающее устройство используется для сопряжения учетных данных, установите для него признак использования для сопряжения. Нажмите **Добавить**.
5. На вкладке **Overview (Обзор)** измените профиль идентификации. Вы можете выбрать профили **Tap in app (Касание в приложении)** или **Touch reader (Касание считывателя)**, если AXIS A4612 установлен только с одной стороны двери, а с другой используется кнопка выхода (REX).

Используйте приложение AXIS Mobile Credential в качестве данных доступа по Bluetooth

В этом примере показано, как добавить в систему считывающее устройство Bluetooth AXIS A4612, чтобы владельцы карт могли открывать двери с помощью приложения AXIS Mobile Credential.

1. Установите считывающее устройство Bluetooth и подключите его к дверному контроллеру.
2. Добавьте считывающее устройство Bluetooth в веб-интерфейс дверного контроллера.
   2.1. Войдите в интерфейс дверного контроллера и перейдите в раздел **Peripherals (Периферийные устройства)** > **Readers (Считывающие устройства)**.
   2.2. Нажмите **Add reader (Добавить считывающее устройство)**.
   2.3. Введите необходимые данные в диалоговом окне **Add Bluetooth reader (Добавить считывающее устройство Bluetooth)**.
   2.4. Нажмите **Добавить**.
3. Добавьте считывающее устройство Bluetooth к двери в AXIS Camera Station Pro.
   3.1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.
   3.2. Выберите дверь, к которой нужно добавить считывающее устройство Bluetooth, и нажмите **Edit (Редактировать)**.
   3.3. Нажмите **Add (Добавить)** со стороны двери, где расположен Bluetooth-считыватель.
   3.4. Выберите **Card reader (Устройство для считывания карт)**.
   3.5. В разделе **Add IP reader (Добавить IP-считыватель)** выберите **IP-считыватель**.
   3.6. В разделе **Select IP reader (Выбрать IP-считыватель)** выберите считывающее устройство Bluetooth.
   3.7. Нажмите **Добавить**.
4. Выберите считывающее устройство Bluetooth для сопряжения. Это нужно сделать как минимум для одного считывающего устройства Bluetooth в вашей системе.
   4.1. Выберите только что добавленное считывающее устройство Bluetooth.
   4.2. Нажмите кнопку **Edit** (Изменить).
   4.3. В разделе **Edit bluetooth reader (Выбрать считывающее устройство bluetooth)** выберите **Use this reader for pairing (Использовать это считывающее устройство для сопряжения)**.
   4.4. Нажмите **Применить**.
5. Выберите профиль идентификации **Tap in app (Активация в приложении)** или **Touch reader (Сенсорное считывающее устройство)**. Для получения дополнительных сведений см. *Профили идентификации, on page 174*.
6. Добавьте мобильный пропуск для владельца карты. См. *Добавить учетные данные, on page 195*.
7. Выполните сопряжение мобильного пропуска со считывающим устройством:
   7.1. Поднесите мобильный телефон держателя карты к Bluetooth-считывателю с включенным режимом сопряжения.
   7.2. Следуйте инструкциям из электронного письма, отправленного владельцу карты.

Добавление REX-устройства

С одной или обеих сторон двери можно добавить устройство запроса на выход (REX). В качестве REX-устройства может использоваться пассивный ИК-датчик, REX-кнопка или толкающий рычаг.

1. Перейдите на страницу конфигурации двери. См. *Добавьте дверь, on page 158*.
2. Для одной стороны двери нажмите **Add (Добавить)**.
3. Выберите **REX-устройство**.
4. Выберите порт ввода-вывода, к которому необходимо подключить устройство REX. Если доступен только один порт, он выбирается автоматически.
5. В пункте **Action (Действие)** выберите действие, которое будет запускаться при приеме сигнала REX дверью.
6. В разделе **REX active (REX активен)** выберите способ подключения цепей дверного монитора.
7. Чтобы изменения в состоянии дискретного входа до его перехода в новое стабильное состояние игнорировались, задайте параметр **Debounce time (ms) (Время устранения дребезга (мс))**.
8. Чтобы при разрыве соединения между дверным контроллером и устройством REX срабатывало событие, включите **Supervised input (Контролируемый вход)**. См. *Контролируемые входы, on page 173*.

Action (Действие)	
Отпереть дверь	Выберите, чтобы отпереть дверь при приеме сигнала REX.
None (Нет)	Выберите этот параметр, чтобы не выполнять никаких действий при получении дверью сигнала REX.

REX активен	
Цепь разомкнута	Выберите этот вариант в случае нормально замкнутой цепи REX. Устройство REX отправляет сигнал, когда цепь размыкается.
Цепь замкнута	Выберите этот вариант в случае нормально разомкнутой цепи REX. Устройство REX отправляет сигнал, когда цепь замыкается.

Добавление зоны

Зона — это конкретная физическая зона с группой дверей. Можно создавать зоны и добавлять в зоны двери. Различают двери двух типов:

- **Perimeter door (Дверь периметра)**: держатели карт входят в зону или выходят из нее через эту дверь.
- **Internal door (Внутренняя дверь)**: внутренняя дверь в пределах зоны.

Примечание

Дверь по периметру может принадлежать двум зонам. Внутренняя дверь может принадлежать только одной зоне. Обзор см. в разделе *Пример конфигурации дверей и зон, on page 158*.

1. Перейдите к пункту **Configuration > Access control > Doors and zones > Zones (Конфигурация > Контроль доступа > Двери и зоны > Зоны)**.
2. Нажмите + **Add zone (Добавить зону)**.
3. Введите имя зоны.

4. Нажмите **Add door (Добавить дверь)**.
5. Выберите двери для добавления в зону и нажмите **Add (Добавить)**.
6. По умолчанию дверь настраивается как дверь по периметру. Чтобы изменить тип двери, выберите **Internal door (Внутренняя дверь)** в раскрывающемся меню.
7. По умолчанию для двери периметра сторона A является стороной входа в зону. Чтобы изменить сторону, выберите **Leave (Выход)** в раскрывающемся меню.
8. Для удаления двери из зоны выберите нужную дверь и нажмите **Remove (Удалить)**.
9. Нажмите **Save (Сохранить)**.

Чтобы изменить параметры зоны:

1. Перейдите к пункту **Configuration > Access control > Doors and zones > Zones (Конфигурация > Контроль доступа > Двери и зоны > Зоны)**.
2. Выберите зону из списка.
3. Нажмите кнопку **Edit (Изменить)**.
4. Измените значения параметров и нажмите **Save (Сохранить)**.

Чтобы удалить зону:

1. Перейдите к пункту **Configuration > Access control > Doors and zones > Zones (Конфигурация > Контроль доступа > Двери и зоны > Зоны)**.
2. Выберите зону из списка.
3. Выберите пункт **Remove (Удалить)**.
4. Нажмите **Да**.

Уровень безопасности зон

К зоне можно добавить следующую функцию безопасности:

Запрет на повторный проход – Предотвращает проход людей с использование тех же реквизитов для входа, которые были введены другими людьми, выполнившими вход в зону до них. Перед повторным использованием учетных данных человек должен выйти из области.

Примечание

- При наличии запрета на повторный проход мы рекомендуем использовать датчики положения дверей на всех дверях в зоне, чтобы убедиться, что пользователь открыл дверь, воспользовавшись своей картой.
- Если контроллер двери переходит в автономный режим, функция запрета на повторный проход продолжает работать при условии, что все двери в зоне относятся к одному и тому же контроллеру. Однако, если двери в зоне принадлежат разным контроллерам, перешедшим в автономный режим, функция запрета на повторный проход перестает работать.

Уровень безопасности можно настроить при добавлении новой зоны или применить его к существующей зоне. Чтобы добавить уровень безопасности к существующей зоне, выполните следующие действия:

1. Перейдите к пункту **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Doors and zones (Двери и зоны)** >.
2. Выберите зону, для которой нужно настроить уровень безопасности.
3. Нажмите кнопку **Edit** (Изменить).
4. Нажмите **Security level (Уровень безопасности)**.
5. Включите необходимые функции безопасности для зоны.
6. Нажмите **Применить**.

Запрет на повторный проход	
Log violation only (Soft) (Только нарушение в журнале (мягкое))	Выберите этот параметр, чтобы разрешить второму человеку войти с использованием тех же учетных данных, что и первый человек. Данный вариант приводит только к подаче сигнала тревоги в системе.
Deny access (Hard) (Запрет доступа (строгий))	Выберите этот параметр, чтобы запретить второму человеку входить с использованием тех же учетных данных, что и первый человек. Данный вариант также приводит к подаче сигнала тревоги в системе.
Время тайм-аута (в секундах)	Время до тех пор, пока система не позволит пользователю повторно войти в систему. Введите 0, чтобы отключить тайм-аут. В этом случае защита от повторного прохода действует до тех пор, пока пользователь не покинет зону. Используйте значение тайм-аута, равное 0, с параметром **Deny access (Hard) (Запрет доступа (строгий))**, только когда все двери в зоне имеют считывающие устройства с обеих сторон.

Контролируемые входы

Контролируемые входы могут инициировать событие при разрыве соединения с дверным контроллером.

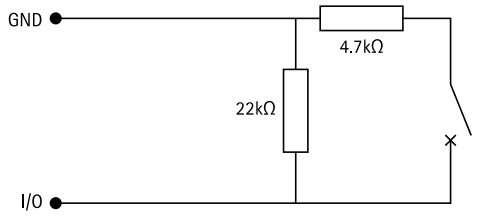
- Соединение между дверным контроллером и дверным монитором. См. *Add a door position sensor (Добавление датчика положения двери), on page 165*.
- Соединение между дверным контроллером и считывающим устройством, которое использует протоколы Wiegand. См. *Добавление считывающего устройства, on page 168*.
- Соединение между дверным контроллером и устройством REX. См. *Добавление REX-устройства, on page 171*.

Для использования контролируемых входов:

1. Установите резисторы на концах линии как можно ближе к периферийному устройству в соответствии со схемой подключения.
2. Перейдите на страницу конфигурации считывающего устройства, дверного монитора или REX-устройства и включите параметр **Supervised input (Контролируемый вход)**.
3. Если вы следовали схеме параллельного соединения, выберите **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Параллельное соединение с параллельным резистором 22 кОм и последовательным резистором 4,7 кОм)**.
4. Если вы следовали схеме последовательного подключения, выберите **Serial first connection (Последовательное соединение)** и укажите значение резистора, выбрав его в раскрывающемся меню **Resistor values (Значения резистора)**.

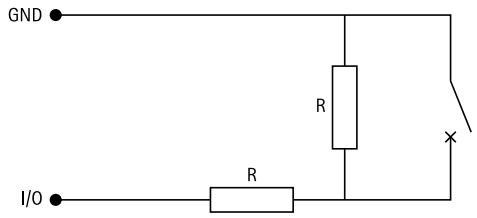
Параллельное соединение

Значение резистора должно быть 4,7 кОм и 22 кОм.



Сначала последовательное соединение

Значение резистора должно быть одинаковым и находиться в диапазоне 1-10 кОм.



Профили идентификации

Профиль идентификации представляет собой комбинацию типов идентификации и расписаний. Вы можете применить профиль идентификации к одной или нескольким дверям, чтобы установить, как и когда владелец карты может получить доступ к двери.

Примечание

Вы должны использовать динамический QR-код и PIN-код совместно.

Чтобы создать, изменить или удалить профили идентификации, перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)**.

Доступные профили идентификации:

Карта – Для открытия двери владелец карты должен провести карту перед считывателем.

Карта и PIN-код – Для открытия двери владелец карты должен провести карту перед считывателем и ввести PIN-код.

ПИН-код – Для открытия двери владелец карты должен ввести PIN-код.

Карта или PIN-код – Для открытия двери владелец карты должен провести карту перед считывателем или ввести PIN-код.

QR-код – Чтобы получить доступ к двери, владельцы карты должны продемонстрировать камере код QR Code®. Профиль идентификации QR-кода можно использовать как для статических, так и для динамических QR-кодов.

Номерной знак а/м – Владелец карты должен подъехать к камере на автомобиле с одобренным номерным знаком.

Активация в приложении – Владелец карты должен активировать учетные данные в мобильном приложении AXIS Camera Station, находясь в зоне действия считывающего устройства Bluetooth.

Сенсорное считывающее устройство – Владелец карты должны прикоснуться к Bluetooth-считывателю, имея при себе мобильный телефон с цифровым пропуском.

*QR Code — охраняемый товарный знак Denso Wave Incorporated в Японии и других странах.

Создание профиля идентификации

1. Перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)**.
2. Нажмите + **Create identification profile (Создать профиль учетных данных)**.
3. Введите имя профиля идентификации.
4. Выберите **Include facility code for card validation (Включить код объекта для проверки карты)**, чтобы использовать код объекта в качестве одного из полей проверки учетных данных. Это поле доступно, только если вы активировали параметр **Facility code (Код объекта)** в разделе **Access management > Settings (Управление доступом > Настройки)**.

5. Для стороны A нажмите **Add (Добавить)**, выберите тип идентификации и расписание.
   - Чтобы требовать от держателей карт использование более чем одного типа идентификации, выберите несколько типов в одной строке.
   - Чтобы разрешить владельцам карт использовать любой из типов, снова нажмите **Add (Добавить)** и добавьте еще одну строку.
6. Для стороны B нажмите **Add (Добавить)**, выберите тип идентификации и расписание.
7. Нажмите кнопку **OK**.

Настройка профилей идентификации

Редактирование профиля идентификации

1. Перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)**.
2. Выберите профиль идентификации и нажмите значок .
3. Чтобы изменить имя профиля идентификации, введите новое имя.
4. Внесите требуемые изменения для данной стороны двери.
5. Чтобы изменить профиль идентификации для другой стороны двери, повторите предыдущие действия.
6. Нажмите кнопку **OK**.

Изменить профиль идентификации	
×	Чтобы удалить тип идентификации и соответствующее расписание.
Тип идентификации	Чтобы изменить тип идентификации, выберите один или несколько типов из раскрывающегося меню **Identification type (Тип идентификации)**.
Расписание	Чтобы изменить расписание, выберите одно или несколько расписаний из раскрывающегося меню **Schedule (Расписание)**.
Добавить	Чтобы добавить тип идентификации и соответствующее расписание, нажмите **Add (Добавить)** и задайте типы идентификации и расписания.

Удаление профиля идентификации

1. Перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)**.
2. Выберите профиль идентификации и нажмите значок .

3. Если этот профиль идентификации применен к двери, выберите для двери другой профиль идентификации.
4. Нажмите кнопку **OK**.

Сброс предустановленного формата карты

1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. Для сброса формата карты к схеме полей по умолчанию нажмите значок .

Форматы карт и ПИН-коды

Формат карты определяет способ интерпретации считывателем данных с карты. Доступны предварительно заданные форматы карт, которые можно использовать или редактировать, а также можно создавать пользовательские форматы карт

Перейдите в раздел **(Конфигурация > Контроль доступа > Форматы карт и PIN-коды)** для создания, редактирования или активации форматов карт. Можно также настроить PIN-код.

Пользовательские форматы карт могут содержать следующие поля данных, используемые для проверки учетных данных.

Номер карты – Подмножество двоичных данных учетных данных, кодируемых в виде десятичных или шестнадцатеричных чисел. Номер карты служит для идентификации конкретной карты или владельца карты.

Код объекта – Подмножество двоичных данных учетных данных, кодируемых в виде десятичных или шестнадцатеричных чисел. Код объекта служит для идентификации конкретного конечного заказчика или объекта.

Конфигурация PIN-кода

1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. В разделе **PIN configuration (Конфигурация PIN-кода)** нажмите значок .
3. Задайте параметры **Min PIN length (Минимальная длина PIN-кода)**, **Max PIN length (Максимальная длина PIN-кода)** и **End of PIN character (Последний знак PIN-кода)**.
4. Нажмите кнопку **OK**.

Создание формата карты

1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. Щелкните **Add card format (Добавить формат карты)**.
3. Введите имя формата карты.
4. В поле **Bit length (Длина в битах)** введите количество битов от 1 до 256.
5. Если порядок следования битов в данных, получаемых от считывателя карт, нужно менять на обратный, выберите пункт **Invert bit order (Инвертировать порядок битов)**.
6. Если порядок следования байтов данных, получаемых от считывателя карт, нужно менять на обратный, выберите пункт **Invert byte order (Инвертировать порядок байтов)**. Этот параметр доступен, только если указанная битовая длина кратна восьми.
7. Выберите и настройте поля данных, которые должны быть активны в формате карты. В формате карты должно быть активно поле **Card number (Номер карты)** или **Facility code (Код объекта)**.
8. Нажмите кнопку **OK**.

9. Чтобы активировать формат карты, установите флажок перед его именем.

Примечание

- Нельзя одновременно активировать два формата карт с одинаковой длиной в битах. Например, если вы определили два 32-битных формата карт, только один из них может быть активным. Деактивируйте один формат карты, чтобы активировать другой.
- Вы можете активировать и деактивировать форматы карт, только если для данного дверного контроллера был настроен хотя бы один считыватель.
- Предустановленные форматы карт можно редактировать, но нельзя удалить. Чтобы отменить изменения в предустановленном формате, нажмите значок сброса, чтобы восстановить настройки по умолчанию. Созданные вами форматы карт можно удалять.

ⓘ	Чтобы увидеть пример выходных данных после инвертирования порядка битов, нажмите значок ⓘ.
Фокусное расстояние	Задайте диапазон битов данных для поля данных. Диапазон должен быть в пределах заданного вами значения параметра **Bit length (Длина в битах)**.
Выходной формат	Выберите выходной формат данных для поля данных. **Десятичная система:** также известна как позиционная система счисления с основанием 10; состоит из цифр от 0 до 9. **Шестнадцатеричная система**: (или позиционная система счисления с основанием 16) использует 16 уникальных символов, а именно цифры 0-9 и буквы a-f.
Битовый порядок поддиапазона	Выберите порядок следования битов. **Little endian (Младший порядок байтов)**: первым передается младший (наименее значащий) бит. **Big endian (Старший порядок байтов)**: первым передается старший (наиболее значащий) бит.

Настройка форматов карт

Редактирование формата карты

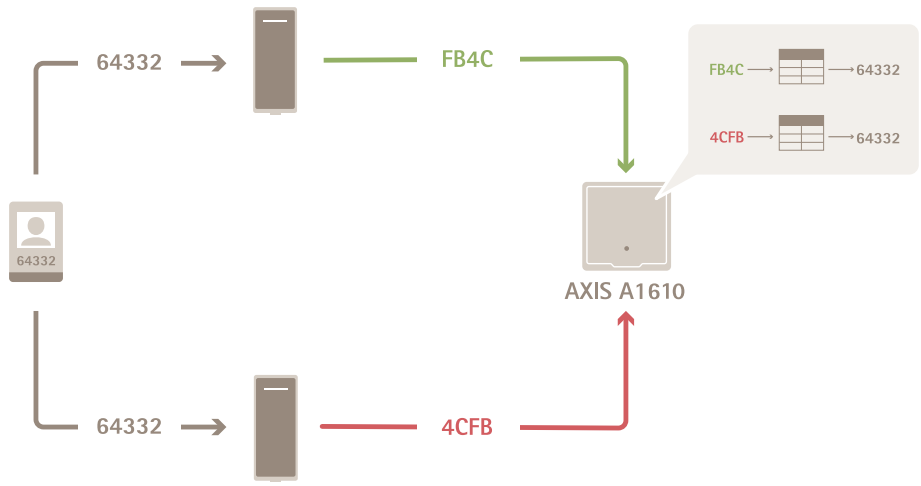
1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. Выберите формат карты и нажмите значок .
3. Если вы редактируете предопределенный формат карты, вы можете редактировать только **Инвертирование порядка битов** и **Инвертирование порядка байтов**.
4. Нажмите кнопку **OK**.

Можно удалить только пользовательские форматы карт. Чтобы удалить пользовательский формат карты:

1. Перейдите к пункту **Configuration > Access Control > Card formats and PIN (Конфигурация > Контроль доступа > Форматы карт и PIN-коды)**.
2. Выберите пользовательский формат карты, нажмите значок и **Yes (Да)**.

Настройка параметров форматов карт

Общее представление



- Номер карты в десятичном формате: `64332`.
- Одно считывающее устройство преобразует номер карты в шестнадцатеричное число `FB4C`. Другое считывающее устройство преобразует его в шестнадцатеричное число `4CFB`.
- Сетевой дверной контроллер AXIS A1610 Network Door Controller принимает число `FB4C` и преобразует его в десятичное число `64332` в соответствии с настройками формата карт, которые применяются к считывающему устройству.
- Сетевой дверной контроллер AXIS A1610 Network Door Controller принимает число `4CFB`, инвертирует порядок байтов, получая число `FB4C`, и преобразует его в десятичное число `64332` в соответствии с настройками формата карт, которые применяются к считывающему устройству.

Инвертировать порядок битов

После инвертирования порядка следования битов данные карты, полученные от считывающего устройства, читаются справа налево бит за битом.

Инвертировать порядок байтов

Группа из восьми битов составляет один байт. После инвертирования порядка следования байтов данные карты, полученные от считывающего устройства, читаются справа налево байт за байтом.

Стандартный 26-битный формат карты Wiegand

1 *Ведущий бит контроля четности*
2 *Код объекта*
3 *Номер карты*
4 *Конечный бит контроля четности*

Зашифрованная связь

Защищенный канал OSDP

AXIS Camera Station Secure Entry поддерживает передачу данных по защищенному каналу по протоколу OSDP (OSDP Secure Channel), что обеспечивает возможность шифрования данных, которыми контроллер обменивается со считывателями Axis.

Чтобы включить OSDP Secure Channel для всей системы:

1. Перейдите в меню **Configuration > Access control > Encrypted communication (Конфигурация > Контроль доступа > Зашифрованная связь)**.
2. Введите основной ключ шифрования и нажмите **OK**.
3. Включите параметр **OSDP Secure Channel (Защищенный канал OSDP Secure Channel)**. Этот параметр доступен только после ввода основного ключа шифрования:
4. По умолчанию основной ключ шифрования используется для создания ключа защищенного канала OSDP. Чтобы вручную задать ключ для OSDP Secure Channel:
   4.1. В разделе **OSDP Secure Channel (Защищенный канал OSDP Secure Channel)** нажмите значок .
   4.2. Снимите флажок **Use main encryption key to generate OSDP Secure Channel key (Использовать основной ключ шифрования для формирования ключа для OSDP Secure Channel)**.
   4.3. Введите ключ для OSDP Secure Channel и нажмите **OK**.

Сведения о том, как включить или отключить функцию OSDP Secure Channel для конкретного считывателя, см. в разделе *Двери и зоны*.

Считыватель штрих-кодов AXIS

Считыватель штрих-кодов AXIS Barcode Reader — это приложение, которое можно установить на камерах Axis. Дверной контроллер Axis использует внешний ключ аутентификации периферийных устройств для предоставления доступа и аутентификации AXIS Barcode Reader и AXIS License Plate Verifier. Полный порядок настройки AXIS License Plate Verifier в AXIS Camera Station Pro см. в разделе

Установка считывателя штрих-кодов AXIS

1. Загрузите файл установки приложения с веб-сайта *axis.com*.
2. Перейдите на веб-страницу вашего переговорного устройства или камеры Axis.
3. Установите приложение.

4. Активируйте лицензию.
5. Запустите приложение.
6. Мы рекомендуем изменить следующую настройку камеры для повышения точности QR.
   6.1. Перейдите к настройкам камеры.
   6.2. В разделе **Image > Exposure (Изображение > Экспозиция)** переместите ползунок **Blur-noise trade-off (Оптимум между размытием и шумом)** в среднее положение.

Настройка считывателя штрих-кодов AXIS

1. Чтобы изменить профиль идентификации QR-кода перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)** и нажмите . См. *Профили идентификации*.
2. Добавьте дверь. См. раздел *Добавление двери*.
3. Выберите **QR** в качестве профиля идентификации для данной двери. См. *Настройка параметров двери*.
4. Добавьте считыватель штрих-кодов. См. *Добавление считывающего устройства*.
   4.1. Для одной стороны двери нажмите **Add reader (Добавить считыватель)**.
   4.2. Выберите **AXIS Barcode Reader (Считыватель штрих-кодов AXIS)** в раскрывающемся списке **Reader type (Тип считывающего устройства)**. Введите имя и нажмите кнопку **OK**.

Создать подключение с дверным контроллером

1. В AXIS Camera Station Pro:
   1.1. Перейдите в меню **Configuration > Access control > Encrypted communication (Конфигурация > Контроль доступа > Зашифрованная связь)**.
   1.2. В разделе **External Peripheral Authentication Key (Ключ проверки подлинности внешнего периферийного оборудования)** нажмите **Show authentication key (Показать ключ проверки подлинности)** и **Copy key (Копировать ключ)**.
2. В веб-интерфейсе устройства, где работает считыватель штрихкодов AXIS Barcode Reader, выполните следующие действия:
   2.1. Откройте приложение AXIS Barcode Reader.
   2.2. Если сертификат сервера не настроен в AXIS Camera Station Pro, включите **Ignore server certificate validation (Игнорировать проверку сертификата сервера)**. Дополнительные сведения см. в разделе *Сертификаты*.
   2.3. Если сертификат сервера не настроен в AXIS Camera Station Pro, включите **Ignore server certificate validation (Игнорировать проверку сертификата сервера)**. Дополнительные сведения см. в разделе *Сертификаты*.
   2.4. Включите **AXIS Camera Station Secure Entry**.
   2.5. Нажмите **Add (Добавить)**, введите IP-адрес дверного контроллера и вставьте ключ для проверки подлинности.
   2.6. Выберите считывающее устройство, выполняющее считывание штрих-кодов из раскрывающегося меню двери.

Мультисерверная БЕТА-ВЕРСИЯ

В мультисерверной системе можно использовать глобальных владельцев карт и группы владельцев карт на основном сервере также и на подключенных подсерверах.

Примечание

- Одна система может поддерживать до 64 подсерверов.
- Для этого требуется AXIS Camera Station 5.47 или более поздней версии.
- Для этого основной сервер и подсерверы должны быть расположены в одной сети.
- На основном сервере и на подсерверах необходимо настроить брандмауэр Windows таким образом, чтобы он разрешал входящие TCP-соединения на порт Secure Entry. По умолчанию это порт 55767. Сведения о настройке портов см. в *Общие настройки сервера, on page 224*.
- Подключение вспомогательного сервера к основному серверу приводит к замене его ключа считывающего устройства, что делает все существующие учетные данные Bluetooth недействительными. Чтобы избежать этого, создавайте учетные данные Bluetooth на основном сервере, а не на вспомогательном.

Последовательность операций

1. Настройте сервер в качестве подсервера и создайте файл конфигурации. См. *Создание файла конфигурации на подсервере, on page 181*.
2. Настройте сервер в качестве основного сервера и импортируйте файл конфигурации для подсерверов. См. *Импорт файла конфигурации на основной сервер, on page 181*.
3. Настройте глобального владельца карты и группы владельцев карт на основном сервере. См. *Добавление владельца карты, on page 193* и *Добавление группы, on page 198*.
4. Просмотр и наблюдение за глобальными владельцами карт и группами владельцев карт с подсервера. См. *Контроль доступа, on page 193*.

Создание файла конфигурации на подсервере

1. На подсервере перейдите в раздел **Configuration > Access Control > Multi Server (Конфигурация > Контроль доступа > Мультисерверная система)**.
2. Нажмите **Sub server (Подсервер)**.
3. Нажмите **Generate (Сформировать)**. Создается файл конфигурации в формате .json.
4. Нажмите **Download (Скачать)** и выберите путь для сохранения файла.

Импорт файла конфигурации на основной сервер

1. На основном сервере перейдите в раздел **Configuration > Access Control > Multi Server (Конфигурация > Контроль доступа > Мультисерверная система)**.
2. Нажмите **Main server (Основной сервер)**.
3. Нажмите + **Add (Добавить)** и перейдите к файлу конфигурации, созданному на подсервере.
4. Введите имя сервера, IP-адрес и номер порта для подсервера.
5. Нажмите **Import (Импорт)** для добавления подсервера.
6. Состояние подсервера отображается как `Connected`.

Отзыв подсервера

Отозвать подсервер можно только до того, как файл конфигурации будет импортирован на основной сервер.

1. На основном сервере перейдите в раздел **Configuration > Access Control > Multi Server (Конфигурация > Контроль доступа > Мультисерверная система)**.
2. Нажмите **Sub server (Подсервер)** и выберите **Revoke server (Отозвать сервер)**.
   Теперь можно настроить этот сервер в качестве основного сервера или в качестве подсервера.

Удаление подсервера

После импорта файла конфигурации подсервера он подключается к основному серверу.

Для удаления подсервера:

1. С основного сервера:
   1.1. Перейдите к пункту **Access management > Dashboard (Управление доступом > Панель управления)**.
   1.2. Измените глобальных владельцев карт и группы на локальных владельцев карт и группы.
   1.3. Перейдите в раздел **Configuration > Access control > Multi server (Конфигурация > Контроль доступа > Мультисерверная система)**.
   1.4. Нажмите **Main server (Основной сервер)** для вывода на отображение списка подсерверов.
   1.5. Выберите подсервер и нажмите **Delete (Удалить)**.
2. С подсервера:
   – Перейдите в раздел **Configuration > Access control > Multi server (Конфигурация > Контроль доступа > Мультисерверная система)**.
   – Нажмите **Sub server (Подсервер)** и выберите **Revoke server (Отозвать сервер)**.

Настройки Active Directory[БЕТА]

Примечание

Для доступа к AXIS Camera Station Pro используются учетные записи Microsoft Windows, а также пользователи и группы Active Directory. Процедура добавления пользователей в Windows может отличаться в зависимости от используемой версии. Дополнительную информацию см. на сайте *support.microsoft.com*. Если вы используете домен Active Directory, обратитесь к администратору сети.

При первом открытии страницы настроек Active Directory можно выполнить импорт пользователей Microsoft Active Directory владельцам карт в AXIS Camera Station Pro. См. *Импорт пользователей Active Directory, on page 182*.

После начальной настройки на странице параметров Active Directory появятся следующие параметры.

- Создание групп владельцев карт и управление ими на основе групп в Active Directory.
- Настройка запланированной синхронизации между Active Directory и системой управления доступом.
- Выполнение синхронизации вручную для обновления всех владельцев карт, импортированных из Active Directory.
- Управление сопоставлением данных между данными пользователя из Active Directory и свойствами держателя карты.

Импорт пользователей Active Directory

Для импортирования пользователей Active Directory владельцам карт в AXIS Camera Station Pro:

1. Перейдите в меню **Configuration (Конфигурация)** > **Access control (Контроль доступа)** > **Active Directory settings (Настройки Active Directory)**[БЕТА].
2. Щелкните **Set up import (Настроить импорт)**.
3. Для выполнения этих трех действий следуйте инструкциям на экране.
   3.1. Выберите пользователя из Active Directory для использования его в качестве шаблона для сопоставления данных.
   3.2. Сопоставьте данные пользователя из базы данных Active Directory со свойствами владельца карты.
   3.3. Создайте новую группу владельцев карт в системе управления доступом и выберите, какие группы Active Directory требуется импортировать.

Изменение импортированных данных пользователей невозможно, однако вы можете добавить учетные данные для импортированного владельца карты, см. раздел *Добавить учетные данные, on page 195*.

Внимание

Если отключить пользователя в Active Directory, AXIS Camera Station Pro безвозвратно удаляет держателя карты и все связанные с ним данные, включая историю. Это действие нельзя отменить. Чтобы заблокировать доступ держателя карты без потери его данных, приостановите его учетную запись в AXIS Camera Station Pro вместо отключения пользователя в Active Directory.

Настройка AXIS Audio Manager Pro

Можно подключиться к серверу AXIS Audio Manager Pro и использовать подключенные к нему аудиоустройства в AXIS Camera Station Pro.

Для этой настройки требуется AXIS Camera Station Pro 6.12 или более поздней версии, а также AXIS Audio Manager Pro 5.0 или более поздней версии. Оба сервера должны быть настроены либо на одном сервере, либо на разных компьютерах в одной сети.

Внимание

Если AXIS Camera Station Pro и AXIS Audio Manager Pro работают на одном сервере, по умолчанию оба используют порт 443. Чтобы избежать проблем с подключением, настройте один из них на использование другого порта.

Изменить порт в AXIS Camera Station Pro можно через < *Общие настройки сервера, on page 224*. Инструкции по изменению порта в AXIS Audio Manager Pro приведены в *AXIS Audio Manager Pro — Руководство пользователя*.

Начало работы с AXIS Audio Manager Pro в AXIS Camera Station Pro

1. В AXIS Audio Manager Pro:
   1.1. Откройте **System settings (Системные настройки)** > **API access (Доступ к API)**.
   1.2. Включите API и введите имя пользователя и пароль.
2. В AXIS Camera Station Pro:
   2.1. Перейдите в **Configuration (Конфигурация)** > **AXIS Audio Manager Pro** и нажмите **Connect (Подключить)**, чтобы установить соединение с сервером AXIS Audio Manager Pro.
   2.2. В появившемся окне введите:**Server URL (URL сервера)**, **API username (Имя пользователя API)**, и **API password (Пароль API)** вашего сервера AXIS Audio Manager Pro и нажмите **Connect (Подключить)**.

После установления подключения можно:

- Смотреть **Server status (Статус сервера)** AXIS Audio Manager Pro и **Device status (Статус устройств)** подключенных аудиоустройств.
- Открывать вкладку AXIS Audio Manager Pro для доступа к веб-интерфейсу сервера.
- Использовать новые аудиофункции в AXIS Camera Station Pro.

Для получения дополнительной информации см. раздел *AXIS Audio Manager Pro, on page 215*.

Примечание

Во избежание проблем, связанных с сертификатами, лучше создать или получить сертификат в доверенном центре сертификации, загрузить его в AXIS Audio Manager Pro и добавить в список доверенных сертификатов сервера AXIS Camera Station Pro. Подробнее см. в разделе *AXIS Audio Manager Pro — Руководство пользователя*.

Настройка «Умного поиска 2»

С помощью Умного поиска 2 можно задать фильтры для поиска интересующих людей и транспортных средств в записях с камер Axis.

Сведения о требованиях и ограничениях, а также инструкции по применению функции «Интеллектуальной поиск 2» см. в разделе *Интеллектуальный поиск 2, on page 39*.

1. Перейдите к пункту **Configuration > Smart search 2 (Конфигурация > Умный поиск 2) > Settings (Настройки)**.
2. В разделе **Cameras (Камеры)**:
   2.1. Выберите камеры для отправки метаданных в функцию «Умный поиск 2».
   2.2. Чтобы разрешить классификацию на сервере в фоновом режиме для камеры, выберите пункт **Allow (Разрешить)** в столбце **Background server classification (Фоновая классификация на сервере)**.
   Это увеличит нагрузку на сервер, но в то же время сделает эту функцию более удобной для пользователей.
   2.3. Чтобы ограничить количество обнаружений, сохраняемых на сервере, в разделе **Filter (Фильтр)** нажмите ⚙ и создайте фильтры для параметров **Area (Область)**, **Size and duration (Размер и длительность)** и **Swaying objects (Качающиеся объекты)**.
   Эти фильтры позволяют исключить области, небольшие объекты, объекты, появляющиеся только на очень короткое время, а также качающиеся объекты, например листву.
   Фильтры умного поиска используют любые существующие фильтры настроек движения в качестве отправной точки.
3. В разделе **Storage (Устройство хранения)**:
   – Выберите накопитель и папку для хранения обнаруженных объектов и нажмите **Apply (Применить)**.
   – Установите предельный объем хранилища и нажмите кнопку **Apply (Применить)**. После исчерпания заданного лимита хранилища самые старые обнаруженные объекты будут удалены.
4. Выберите **Include periods with missing metadata (Включать периоды без метаданных)**, чтобы отображать результаты, для которых метаданные не записывались.
5. Выберите **Allow the server to classify detections when you start a search (Разрешить серверу классифицировать обнаружения при начале поиска)** для получения более детализированных результатов поиска, включая обнаружения, которые не были классифицированы камерой. Для более быстрого поиска оставьте этот параметр выключенным.

Фоновая классификация на сервере	
	Состояние классификации на сервере за последний час, когда классификация на сервере происходит медленно. Отображается, если классифицировано менее 95 % обнаружений.
	Состояние классификации на сервере за последний час, когда классификация на сервере происходит медленно. Отображается, если классифицировано менее 50 % обнаружений.

Триггеры

Фильтры интеллектуального поиска можно настроить в качестве триггеров в правилах действий. Чтобы создать триггер умного поиска:

1. Перейдите в **Configuration (Конфигурация)** > **Smart search 2** > **Triggers (Триггеры)**.
2. Нажмите **Create (Создать)**.
3. Настройте фильтры. Дополнительную информацию о фильтрах умного поиска см. в разделе *Поиск с помощью фильтров, on page 39*.
4. Нажмите **Next (Далее)**.
5. Настройте уровень **Confidence (Достоверность)** для объектов обнаружения. Более высокий уровень достоверности отфильтровывает классификации с низкой степенью уверенности, уменьшая количество обнаружений.
6. Нажмите **Next (Далее)**.
7. Введите имя для триггера и нажмите **Save (Сохранить)**.

Примечание

- Обычно функции Умный поиск 2 требуется несколько секунд после выхода объекта из поля зрения камеры для анализа видеозаписи и подтверждения обнаружения. Например, если в правиле действий задано срабатывание при обнаружении красного автомобиля, действие сработает через несколько секунд после выхода объекта из поля зрения камеры.
- Опция **Visual similarity (Визуальное сходство)** недоступна для триггеров Smart search 2.
- Создание триггера для камеры позволяет серверу обрабатывать обнаружения объектов, даже если для этой камеры отключена опция **Enable background processing (Включить фоновую обработку)**.
- **Периоды задержки обнаружения** — это периоды высокой задержки обработки, из-за которых правила действий срабатывают с задержкой. Если это происходит часто, измените конфигурацию фильтра триггера, уменьшив количество камер, и используйте фильтры камеры, такие как пересечение линии, область, размер и продолжительность, чтобы уменьшить задержку обработки.

Чтобы использовать триггер Smart search 2 в правиле действий, см. раздел *Создание триггеров Smart search 2, on page 110*.

Настройка приложения System Health Monitoring БЕТА

Примечание

- При подключении к нескольким серверам AXIS Camera Station Pro можно настроить модуль System Health Monitoring на любом из этих серверов. Для этого выберите сервер из раскрывающегося меню **Selected server (Выбранный сервер)**.
- Если вы управляете системами, расположенными в разных сетях, служба контроля работоспособности сервера в My Systems обеспечивает эти же функциональные возможности, но через использование облака.

Параметры

Облачное соединение	Если сервер зарегистрирован в организации, данные о состоянии системы можно просматривать из любого места. Если подключение еще не установлено, нажмите **Manage (Управление)** и следуйте инструкциям на экране.
Частота получения данных	Выберите более низкую частоту передачи данных, чтобы устранить предупреждения об устаревших данных или общие проблемы с производительностью. В конфигурации с несколькими системами рекомендуется использовать для подсистемы такое же или более высокое значение, как для родительской системы. • **Low (Низкая)** — для систем более чем со 100 устройствами. • **Medium (Средняя)** — для систем с 25–100 устройствами. • **High (Высокая)** — для систем менее чем с 25 устройствами.

Уведомления

Для отправки уведомлений по электронной почте:

1. Настройте сервер SMTP и адрес электронной почты для отправки уведомлений. См. *Параметры сервера, on page 133*
2. Настройте адреса электронной почты для получения уведомлений. См. *Настройка получателей электронной почты, on page 186*.
3. Настройте правила уведомлений. См. *Настройка правил уведомлений., on page 186*.

Настройка получателей электронной почты

1. Выберите **Configuration > System Health Monitoring > Notifications (Конфигурация > Контроль работоспособности системы > Уведомления)**.
2. В разделе **Email recipients (Получатели электронной почты)** введите адрес электронной почты и нажмите **Save (Сохранить)**. Для добавления нескольких получателей электронной почты повторите процедуру.
3. Для проверки SMTP-сервера нажмите **Send test email (Отправить тестовое сообщение по электронной почте)**. Появится сообщение с подтверждением отправки тестового сообщения электронной почты.

Настройка правил уведомлений.

По умолчанию включены два правила уведомлений.

Отключение системы – отправка уведомления в случае, когда одиночная или многосистемная конфигурация находится в состоянии отключения дольше обычного.

Отключение устройства – Отправка уведомления, если устройство, указанное в System Health Monitoring (Контроль работоспособности системы), находится в состоянии отключения дольше обычного.

1. Выберите **Configuration > System Health Monitoring > Notifications (Конфигурация > Контроль работоспособности системы > Уведомления)**.

2. В разделе **Notification rules (Правила уведомлений)** включите или отключите правила уведомлений.
3. В разделе **Applied rules (Примененные правила)** отображается список систем и устройств и применяемых к ним правил уведомлений.

Мультисистема

Приложение System Health Monitoring позволяет отслеживать данные о работоспособности нескольких вспомогательных систем из основной системы.

1. Во вспомогательной системе создайте конфигурацию системы. См. *Сформировать конфигурацию системы, on page 187*.
2. В основной системе загрузите системную конфигурацию. См. *Получить данные из других систем, on page 187*.
3. Повторите указанные выше шаги в других вспомогательных системах.
4. Отслеживайте данные о работоспособности нескольких систем из основной системы. См. *System Health Monitoring BETA, on page 205*.

Сформировать конфигурацию системы

1. Выберите **Configuration > System Health Monitoring > Multisystem (Конфигурация > Контроль работоспособности системы > Многосистемность)**.
2. Нажмите **Generate (Сформировать)**.
3. Нажмите **Copy (Копировать)**, чтобы скопировать конфигурацию для загрузки в основную систему.
4. Для просмотра подробных сведений о конфигурации системы нажмите **Show details (Показать подробности)**.
5. Чтобы повторно создать конфигурацию системы, сначала нажмите **Delete (Удалить)**, чтобы удалить существующую конфигурацию.

После загрузки конфигурации системы в основную систему сведения об основной системе отображаются в разделе **Systems with access (Системы с доступом)**.

Получить данные из других систем

После создания и копирования конфигурации вторичной системы ее можно загрузить в основную систему.

1. В основной системе перейдите в меню **Configuration > System Health Monitoring > Multisystem (Конфигурация > Контроль работоспособности системы > Многосистемность)**.
2. Нажмите **Paste (Вставить)**, чтобы добавить скопированные сведения вторичной системы.
3. Проверьте IP-адрес хоста и нажмите **Add (Добавить)**.
   Вспомогательная система отображается в списке **Available systems (Доступные системы)**.

Настройка аналитики

Панель аналитики AXIS Data Insights Dashboard

Панель аналитики AXIS Data Insights Dashboard представляет аналитические данные, полученные от ваших устройств, в виде графиков и диаграмм. На странице конфигурации AXIS Data Insights Dashboard отображаются все поддерживаемые приложения и настроенные сценарии на устройствах в вашей системе. Перейдите в раздел **Analytics (Аналитика)** > **Data Insights Dashboard (Панель мониторинга анализа данных)**, чтобы:

- Просмотрите список камер и источников данных, на которых запущены поддерживаемые приложения.
- Просмотрите список поддерживаемых приложений и сценариев для каждого устройства или источника данных. Поддерживаются следующие приложения и сценарии:
  - AXIS Object Analytics: подсчет пересечений линии и подсчет людей в области
  - AXIS Audio Analytics
  - AXIS Image Health Analytics
  - AXIS People Counter
  - AXIS P8815-2 3D Counter
  - Датчики качества воздуха AXIS (мониторинг качества воздуха)

  Примечание

  Можно хранить до 100 МБ данных, поэтому время хранения ограничено. Например, датчик качества воздуха, который контролирует все 12 типов данных, может хранить записи около 430 дней.
- Выбрать сценарии для отображения на панели мониторинга.
- Помечайте сценарии, чтобы фильтровать данные на панели мониторинга, например для группировки камер, расположенных в одном месте.

Примечание

Чтобы отобразить данные подсчета количества пересечений AXIS Object Analytics на панели **In and Out counting (Подсчет входящих и выходящих посетителей)**, выберите направление **In (Входящие)** или **Out (Выходящие)** в поле **Direction (Направление)**.

- Отслеживать статус сценариев.

Включить	Включите переключатель в столбце **Include (Включить)**, чтобы данные сценария отображались на панели мониторинга.
Теги	Выберите метки из выпадающего списка в столбце **Tags (Метки)**, чтобы прикрепить их к сценарию.

Чтобы добавить новый тег:

1. Откройте вкладку **Tags (Теги)**.
2. Задайте имя тега
3. Нажмите стрелку.

Примечание

- Для зашифрованных подключений AXIS Data Insights Dashboard требуется TLS версии 1.2 или более поздней на сервере Windows.
- AXIS Data Insights Dashboard переопределяет существующие настройки MQTT на камере в следующих случаях:
  - На камере не настроен MQTT-клиент.

  - Сценарий вручную включается для камеры, подключенной к другому серверу AXIS Camera Station Pro.
- При подключении к AXIS Data Insights Dashboard клиент MQTT на камере выделяется для AXIS Data Insights Dashboard.
- Камеры и сервер AXIS Camera Station Pro должны находиться в одной сети.
- Для оптимальной производительности рекомендуется использовать сервер с объемом ОЗУ не менее 16 ГБ для запуска AXIS Data Insights Dashboard в AXIS Camera Station Pro.
- Максимальный объем хранимых данных составляет 100 МБ, что ограничивает время хранения. Например:
  - Расчетное время хранения данных при подсчете заполненности парковки, оборудованной четырьмя камерами, каждая из которых круглосуточно обнаруживает пять подклассов транспортных средств, например автомобили и велосипеды, составляет 260 дней.
  - Подсчет людей в торговом помещении, оборудованном восемью камерами, при непрерывном потоке людей в течение 12 часов обеспечивает расчетное время хранения данных около 1270 дней.
  - При использовании на камере сценария подсчета пересечений линии с шестью классами и непрерывном подсчете в течение 24 часов расчетное время хранения данных составляет около 860 дней.

Подробнее о добавлении панели мониторинга в мультиэкранный режим см. в разделе *Панель аналитики AXIS Data Insights Dashboard в режиме мультиэкрана, on page 21*.

Включение панели AXIS Data Insights Dashboard

License Plate Verifier

На странице License plate verifier (Проверка номерных знаков) можно просматривать состояние AXIS License Plate Verifier на камерах и объединять камеры в группы для упрощения управления списками.

Вкладка **Cameras** (Камеры) содержит перечень всех подключенных устройств с установленным AXIS License Plate Verifier:

- **Camera (Камера)**: имя камеры.
- **Version (Версия)**: версия AXIS License Plate Verifier, установленная на камере.
- **Status (Состояние)**: текущее состояние AXIS License Plate Verifier.
- **Latest event (Последнее событие)**: время последнего события, зафиксированного камерой.
- **Allowed (Разрешенные)**: количество номерных знаков в списке Allowed (Разрешенные) камеры.
- **Blocked (Заблокированные)**: количество номерных знаков в списке Blocked (Заблокированные) камеры.
- **Custom (Пользовательские)**: количество номерных знаков в списке Custom (Пользовательские) камеры.
- **Group (Группа)**: группа, к которой относится камера.

На вкладке **Groups (Группы)** отображаются все группы камер и камеры, входящие в каждую группу. На этой вкладке можно сделать следующее:

- Нажать **New...** (Новая), чтобы добавить новую группу.

- Нажать **Delete** (Удалить), чтобы удалить существующую группу.
- Переименовать выбранную группу в поле **Group name** (Название группы)
- Нажмите **Add... (Добавить...)**, чтобы добавить камеру в выбранную группу.
- Нажать **Remove** (Удалить), чтобы удалить камеру из группы

Вы можете создавать общие списки для сгруппированных камер. Дополнительную информацию см. в разделе *Управление номерными знаками, on page 214*.

Настройка нательных камер

Подключение системы нательных камер

Подключите систему нательных камер к AXIS Camera Station Pro для передачи записей и метаданных с нательных камер.

1. Перейдите в **Configuration (Конфигурация) > Body worn (Нательные камеры) > Connect a body worn system (Подключить систему нательной камеры)**.
2. В разделе **Connection method** выберите желаемый способ подключения:
   - **Прямое подключение**: введите IP-адрес и учетные данные Body Worn Manager.
   - **Создание файла подключения**: создайте файл конфигурации для загрузки в Body Worn Manager.

Примечание

Прежде чем создавать файл подключения, необходимо сначала обновить сертификат сервера, если изменился IP-адрес сервера или программа AXIS Camera Station была обновлена с версии, предшествующей версии 5.33. Инструкции по обновлению сертификата см. в разделе *Сертификаты, on page 148*.

Если выбрано **Connect directly (Прямое подключение):**

3. В разделе **Configure direct connection (Конфигурация прямого подключения)** введите **IP address (IP-адрес)**, **User name (Имя пользователя)** и **Password (Пароль)** для входа в Body Worn Manager.

1. При необходимости измените имя системы **AXIS Camera Station system name**. Это имя идентифицирует назначение для копируемых и передаваемых записей.
2. При необходимости завершите все существующие подключения, выбрав **End existing connections**. Загрузите новый файл подключения в каждый контроллер AXIS Body Worn System.
3. Нажмите **Подключить**.

Если выбрано **Generate connection file (Создать файл подключения)**:

4. В разделе **Generate connection file (Создать файл подключения)** при необходимости измените **AXIS Camera Station system name (Имя системы AXIS Camera Station)**. Это помогает определить, куда копируются или переносятся записи.
   4.1. При необходимости завершите все существующие подключения, выбрав **End existing connections**. Загрузите новый файл подключения в каждый контроллер AXIS Body Worn System.
   4.2. Нажмите **Export (Экспортировать)** и сохраните файл подключения.
   4.3. Загрузите файл подключения в систему AXIS Body Worn System.

Настройка нательной системы Axis

Воспроизведение и экспорт записей с нательных камер Axis

Стоп-кадры

Автоматический экспорт стоп-кадров из закладок нательной камеры выполняется в папку при передаче записей в AXIS Camera Station Pro.

1. Перейдите на **Configuration (Конфигурация)> Body worn (Нательные камеры) > Snapshots (Стоп-кадры)**.
2. В поле **Storage location (Место хранения)** введите путь к папке для сохранения стоп-кадров.
3. Нажмите **Применить**.
4. Включите функцию**Snapshot export (Экспорт стоп-кадров)**.

Интеграция CAD

Интеграция с системой Computer-aided Dispatch (CAD) позволяет автоматически классифицировать записи с носимых камер на основе данных диспетчеризации.

Для настройки интеграции:

1. Перейдите в **Configuration (Конфигурация)> Body worn (Нательные камеры)> CAD integration (Интеграция с CAD)**.
2. Нажмите **Set up integration (Настроить интеграцию)**.
3. Выберите формат файла (CSV или XML) и нажмите **Next (Далее)**.
4. Включите параметр **Shared network drive (Общий сетевой диск)**, если файл CAD расположен на сетевом общем ресурсе.
5. Укажите путь к папке с CAD-файлом, имя файла (только для CSV), а также разделитель столбцов.
6. Нажмите **Next (Далее)**.
7. Сопоставьте каждое поле с соответствующим идентификатором, как он задан в CAD-файле:
   - **Officer name (Имя сотрудника)**: должен совпадать с именами виртуальных камер в AXIS Camera Station Pro. Если имя не совпадает, его необходимо изменить в Body Worn Manager, а не в AXIS Camera Station Pro.
   - **Event ID**: уникальный идентификатор диспетчерского события.
   - **Call category**: категория записи. Если категория отсутствует, она будет создана автоматически.
   - **Время отправки**: время начала в формате RFC 3339, например «2025-11-25T09:49:17 +01:00».
   - **Clearance time**: время окончания в формате RFC 3339.
   - **Case number**: номер дела, связанный с диспетчерским событием. Столбец должен присутствовать в файле, но значение может быть пустым.
8. Нажмите **Finish (Завершить)**, затем **Apply (Применить)**.
9. Для просмотра записей нажмите + и выберите **CAD recordings (Записи CAD)**, чтобы отобразить все автоматически классифицированные записи. Можно фильтровать записи по времени или имени сотрудника.

Примечание

Если новые категории создаются автоматически, для них необходимо вручную задать сроки хранения.

Ограничения
Информация может быть утрачена в следующих случаях:

- AXIS Camera Station Pro или соответствующий компонент не запущен.
- Экспортируемые файлы превышают 1 ГБ.
- Требуется обновление сетевых учетных данных.

Настройки нательной системы

Настройте места сохранения записей с нательных камер.

Хранение записей
Выберите расположение по умолчанию для хранения записей с носимых камер для новых пользователей системы:

1. Перейдите в **Configuration (Конфигурация) > Body worn (Нательные камеры) > Body worn settings (Настройки нательных камер)**.
2. В **Recording storage (Хранилище записей)** выберите диск из выпадающего списка **Disk (Диск)**.
3. Нажмите **Save (Сохранить)**.

Хранилище отклоненных записей
Выберите место сохранения для отклоненного контента от нательной системы:

1. В разделе **Rejected recordings storage (Хранилище отклоненных записей)** выберите диск в раскрывающемся списке **Disk (Диск)** и введите **Folder name (Имя папки).**
2. Установите количество дней хранения отклоненного контента в параметре **Number of days to keep rejected content from the body worn system (Количество дней хранения отклоненного контента из системы нательных камер)**.
3. Нажмите **Save (Сохранить)**.

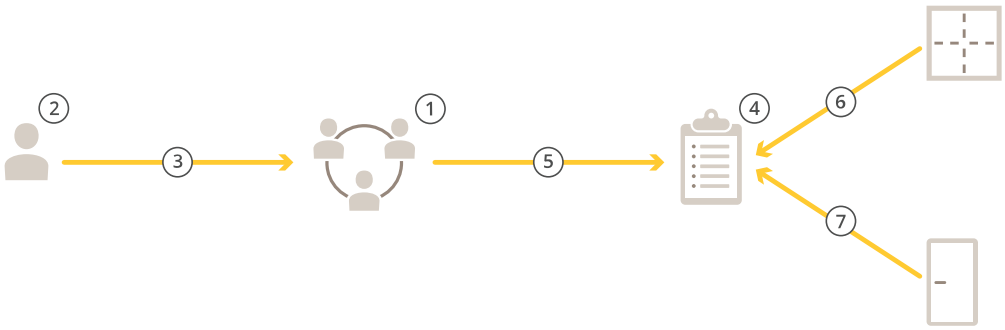
Контроль доступа

Используйте вкладку **Access management (Управление доступом)** для настройки и управления держателями карт, группами и правилами доступа в системе.

Полное описание рабочего процесса настройки дверного сетевого контроллера Axis в AXIS Camera Station Pro см. в разделе *Настройка сетевого дверного контроллера Axis*.

Рабочий процесс управления доступом

Структура системы управления доступом является гибкой, поэтому можно разработать рабочий процесс в соответствии с вашими потребностями. Пример рабочего процесса:



1. *Добавление группы, on page 198*.
2. *Добавление владельца карты, on page 193*.
3. Добавьте владельцев карт в группы.
4. *Добавление правила доступа, on page 198*.
5. Примените группы к правилам доступа.
6. Примените зоны к правилам доступа.
7. Примените двери к правилам доступа.

Добавление владельца карты

Владелец карты — это человек с уникальным идентификатором, зарегистрированным в системе. Настройте держателя карты, указав учетные данные, идентифицирующие человека, а также определив, когда и каким образом ему разрешен доступ через двери.

Пользователей из базы данных Active Directory также можно сопоставить с держателями карт. См. *Настройки Active Directory[БЕТА], on page 182*.

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в **Cardholder management (Управление держателями карт)** > **Cardholders (Держатели карт)** и нажмите **Add (Добавить)**.
3. Введите имя и фамилию владельца карты. При необходимости можно добавить дополнительные сведения о владельце карты.
   - В поле **Email** (Электронная почта) введите адрес электронной почты владельца карты.
   - В поле **Groups** (Группы) выберите группы, в которые вы хотите добавить владельца карты.
   - В поле **Access rules** (Правила доступа) выберите правила доступа, которые будут применяться ко владельцу карты.

4. Чтобы добавить фотографию, нажмите **Cardholder picture** (Фотография владельца карты) и выберите подходящий вариант:
   - **Upload** (Загрузить файл), чтобы добавить изображение со своего устройства.
   - **Capture** (Сделать снимок), чтобы сделать снимок с помощью камеры.

   Примечание

   Поддерживаемые форматы изображения: JPG, PNG или GIF. Размер изображений автоматически изменяется до максимального значения 700×700 пикселей, затем файлы конвертируются в формат JPG.
5. Нажмите на кнопку **Advanced** (Расширенные настройки), чтобы настроить дополнительные параметры.
6. Добавьте учетные данные владельца карты. См. *Добавить учетные данные, on page 195*.
7. Нажмите **Save (Сохранить)**.
8. Чтобы распечатать пропуска, выберите одного или нескольких держателей карт и нажмите **Print Badge**BETA (Печать пропуска BETA). Дополнительную информацию см. в разделе *Печать бейджа BETA, on page 204*.

Вы можете найти владельца карты по имени или фамилии, используя строку поиска. Чтобы фильтровать список по источнику, нажмите **Filter** (Фильтр) выберите **Local** (Локально), **Global** (Глобально), **AD** или **Center** (Центр).

Расширенный набор	
Длительное время доступа	Выберите этот параметр, чтобы предоставить держателю карты увеличенное время доступа и увеличенное время допустимого открытия двери при наличии установленного датчика состояния двери.
Приостановить владельца карты	Выберите, чтобы приостановить владельца карты. Этот параметр временно отменяет все права доступа держателя карты.
Разрешить двойной свайп	Выберите, чтобы разрешить владельцу карты переопределять текущее состояние двери. Например, держатель карты может использовать этот параметр для разблокировки двери вне установленного расписания.
Исключение из блокировки	Выберите этот параметр, чтобы предоставить держателю карты доступ при блокировке.
Снять запрет на проход в обратном направлении	Выберите, чтобы снять для владельца карты запрет на повторный проход. Запрет прохода в обратном направлении предотвращает повторное использование реквизитов для входа другими людьми. Первый человек должен сначала выйти из области, только после этого его реквизиты для входа могут быть использованы снова.
Глобальный владелец карты	Выберите для активации просмотра и мониторинга владельца карты на подсерверах. Данная опция доступна только для тех владельцев карт, которые созданы на основном сервере. См. *Мультисерверная БЕТА-ВЕРСИЯ, on page 180*.

Добавление владельцев карт и групп

Добавить учетные данные

Владельцу карты можно назначить следующие типы учетных данных:

- *Учетные данные на основе QR-кода, on page 195*
- *PIN-код, on page 196*
- *Мобильный пропуск, on page 196*
- *Учетные данные карты, on page 196*
- *Учетные данные номерного знака, on page 197*

Дата окончания срока действия	
Действует с	Задайте дату и время, начиная с которых учетные данные становятся действительными.
Действует до	Выберите вариант из раскрывающегося меню.

Действует до	
Нет даты окончания	Срок действия учетных данных никогда не истечет.
Дата	Установите конкретную дату и время истечения срока действия учетных данных.
С момента первого использования	Выберите срок истечения действия учетных данных с момента их первого использования. Выберите количество дней, месяцев или лет или количество раз после первого использования.
С момента последнего использования	Выберите срок действия учетных данных после последнего использования. Выберите количество дней, месяцев или лет после последнего использования.

Учетные данные на основе QR-кода

Примечание

Для использования QR-кодов в качестве учетных данных необходимо синхронизировать время на системном контроллере и камере с AXIS Barcode Reader. Для синхронизации времени рекомендуется использовать один и тот же источник времени для обоих устройств.

Чтобы добавить данные QR-кода владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить +)** и выберите **QR-код**.
2. Введите имя для учетных данных.
3. Параметр Динамический QR-код включен по умолчанию. Его необходимо использовать вместе с учетными данными PIN-код.

4. Установите даты начала и окончания действия учетных данных.
5. Для автоматической отправки QR-кода по электронной почте после сохранения владельца карты, выберите **Send QR code to cardholder when credential is saved (Отправить QR-код владельцу карты при сохранении учетных данных)**.
6. Нажмите **Добавить**.

PIN-код

Чтобы добавить PIN-код для владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **Add (Добавить)** и выберите **PIN-код**.
2. Введите PIN-код.
3. При необходимости для активации скрытой тревоги с отдельным PIN-кодом включите **Duress PIN (PIN-код принуждения)** и задайте PIN-код принуждения.
4. Задайте даты **Valid from (Действует с)** and **Valid to (Действует до)** для учетных данных.
5. Нажмите **Добавить**.

Мобильный пропуск

Примечание

Держатель карты должен иметь адрес электронной почты для получения мобильных учетных данных.

Чтобы добавить данные о мобильном телефоне владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **Add (Добавить +)** и выберите **Mobile credential (Данные о мобильном телефоне)**.
2. Введите имя для учетных данных.
3. Установите даты начала и окончания действия учетных данных.
4. Выберите опцию **Send the mobile credential to the cardholder after saving (Отправить цифровой пропуск владельцу карты после сохранения)**. Владелец карты получит сообщение электронной почты с инструкциями по активации.
5. Нажмите **Добавить**.

Пример см. в разделе . *Используйте приложение AXIS Mobile Credential в качестве данных доступа по Bluetooth, on page 170*.

Учетные данные карты

Чтобы добавить данные о мобильном телефоне владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **Add (Добавить)** и выберите **Card (Карта)**.
2. Чтобы вручную ввести данные карты, введите имя карты, номер карты и длину в битах.

Примечание

Длина в битах настраивается, только если вы создаете формат карты с определенной битовой длиной, которой еще нет в системе.

3. Чтобы автоматически получить данные последней использованной карты:
   3.1. Выберите дверь в раскрывающемся меню **Select reader (Выбрать считыватель)**.
   3.2. Проведите карту через считыватель, подключенный к этой двери.
   3.3. Нажмите **Get last swiped card data from the door's readers (Получить последние считанные данные карты с дверных считывающих устройств)**.

Примечание

Чтобы получить данные с карты, можно использовать считывающее USB-устройство 2N для настольных компьютеров. Более подробную информацию см. в разделе *Настройка считывающего USB-устройства 2N для настольных компьютеров*.

4. Введите код объекта. Это поле доступно, только если вы активировали параметр **Facility code (Код объекта)** в разделе **Access management > Settings (Управление доступом > Настройки)**.
5. Установите даты начала и окончания действия учетных данных.
6. Нажмите **Добавить**.

Учетные данные номерного знака

Чтобы добавить данные номерного знака владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите + **Add (Добавить)** и выберите **License plate (Номерной знак)**.
2. Введите название для учетных данных, описывающее транспортное средство.
3. Введите номерной знак автомобиля для транспортного средства.
4. Установите даты начала и окончания действия учетных данных.
5. Нажмите **Добавить**.

Использование номерного знака автомобиля в качестве учетных данных

В этом примере показано, как предоставить доступ, используя номерной знак автомобиля в качестве учетных данных, с помощью дверного контроллера и камеры с AXIS License Plate Verifier.

1. Добавьте дверной контроллер и камеру к AXIS Camera Station Pro. См. *Добавить устройства, on page 6*.
2. Обновите прошивку на новых устройствах до последней доступной версии. См. *обновлять встроенное программное обеспечение;, on page 73*.
3. Добавьте новую дверь, подключенную к вашему дверному контроллеру. См. *Добавьте дверь, on page 158*.
   3.1. Добавьте считывающее устройство на **сторону A**. См. *Добавление считывающего устройства, on page 168*.
   3.2. В разделе **Door settings (Настройка параметров двери)** выберите **AXIS License Plate Verifier** в качестве значения **Reader type (Тип считывающего устройства)** и введите имя для считывающего устройства.
   3.3. Дополнительно можно также добавить считывающее устройство или устройство, обрабатывающее запросы на выход, на **сторону B**.
   3.4. Нажмите кнопку **OK**.
4. Установите на камеру AXIS License Plate Verifier и выполните активацию. См. руководство пользователя *AXIS License Plate Verifier*.
5. Запустите AXIS License Plate Verifier.
6. Настройте AXIS License Plate Verifier.
   6.1. Перейдите в меню **Configuration > Access control > Encrypted communication (Конфигурация > Контроль доступа > Зашифрованная связь)**.
   6.2. В разделе **External Peripheral Authentication Key (Ключ проверки подлинности внешнего периферийного оборудования)** нажмите **Show authentication key (Показать ключ проверки подлинности)** и **Copy key (Копировать ключ)**.
   6.3. Откройте AXIS License Plate Verifier из веб-интерфейса камеры.
   6.4. Пропустите мастер настройки.
   6.5. Выберите в меню **Settings (Настройки)**.

6.6. В разделе **Access control (Контроль доступа)** выберите **Secure Entry** в качестве значения **Type (Тип)**.

6.7. В поле **IP address (IP-адрес)** введите IP-адрес дверного контроллера.

6.8. В поле **Authentication key (Ключ аутентификации)** вставьте скопированный ранее ключ аутентификации.

6.9. Нажмите **Подключить**.

6.10. В разделе **Door controller name (Имя дверного контроллера)** выберите нужный дверной контроллер.

6.11. В разделе **Reader name (Имя считывающего устройства)** выберите добавленное вами ранее считывающее устройство.

6.12. Включите интеграцию.

7. Добавьте держателя карты, которому необходимо предоставить доступ. См. *Добавление владельца карты, on page 193*
8. Добавление данных номерного знака для нового владельца карты. См. *Добавить учетные данные, on page 195*
9. Добавление правила доступа. См. *Добавление правила доступа, on page 198*.

9.1. Добавление расписания.

9.2. Добавьте держателя карты, которому необходимо предоставить доступ к номерным знакам.

9.3. Добавьте дверь со считывающим устройством AXIS License Plate Verifier.

Добавление группы

Группы позволяют совместно управлять держателями карт и их правилами доступа.

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в **Cardholder management (Управление держателями карт)** > **Groups (Группы)** и нажмите **Add (Добавить)**.
3. Введите название и, по желанию, инициалы для группы.
4. Выберите **Global group (Глобальная группа)**, чтобы просматривать держателей карт на подчиненных серверах и отслеживать их состояние. Данная опция доступна только для тех владельцев карт, которые созданы на основном сервере. См. *Мультисерверная БЕТА-ВЕРСИЯ, on page 180*.
5. Добавление в группу владельцев карт:

5.1. Нажмите **Add (Добавить)**.

5.2. Выберите владельцев карт, которых вы хотите добавить, и нажмите **Add (Добавить)**.

6. Нажмите **Save (Сохранить)**.
7. Чтобы распечатать пропуска для всех держателей карт в группе, выберите группу и нажмите **Print Badge**BETA (Печать пропускаBETA). Дополнительную информацию см. в разделе *Печать бейджа BETA, on page 204*.

Добавление правила доступа

Правило доступа определяет условия, которые должны быть выполнены для предоставления доступа.

Правило доступа состоит из следующих элементов:

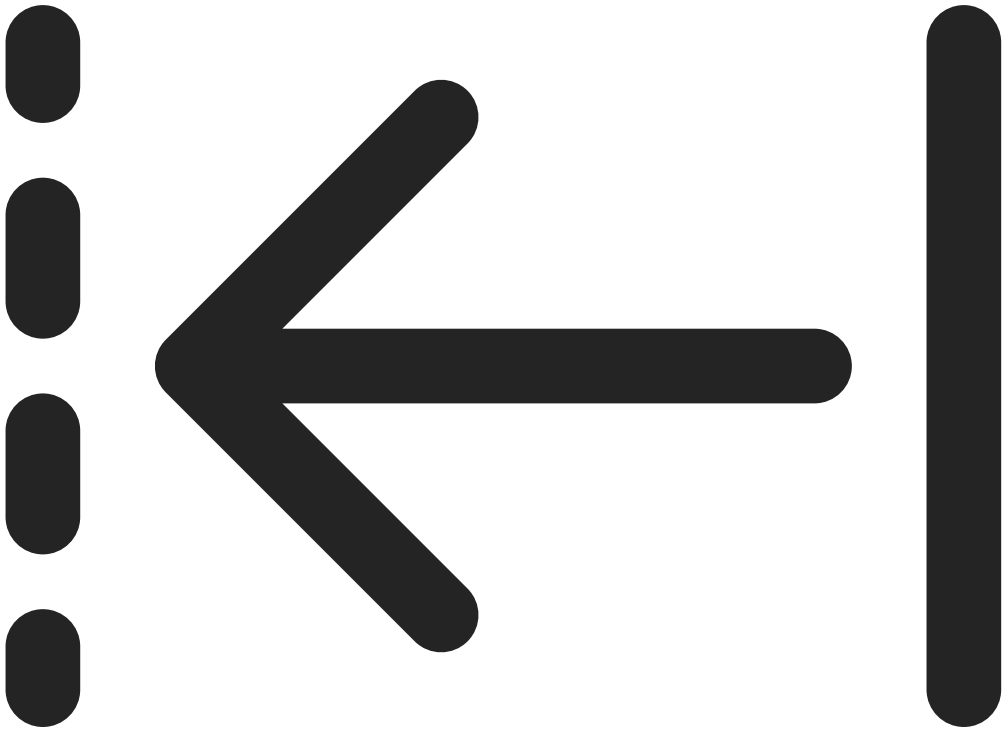
Владельцы карт и группы владельцев карт – кому следует предоставлять доступ.

Двери и зоны – где применяется правило доступа.

Расписания – когда следует предоставлять доступ.

Чтобы добавить правило доступа:

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Cardholder management (Управление владельцами карт)**.
3. В разделе **Access rules (Правила доступа)**



нажмите **Add (Добавить)**.

4. Введите имя правила доступа и нажмите **Next (Далее)**.
5. Настройка владельцев карт и групп:
   5.1. В разделе **Cardholders (Держатели карт)** или **Groups (Группы)** нажмите **Add (Добавить)**.
   5.2. Выберите владельцев карт или группы и нажмите **Add (Добавить)**.
   5.3. Вы также можете перетащить запись владельца карты или группу прямо в поле правила доступа, чтобы применить правило к нужным пользователям. Правила доступа, на которые можно перетащить элементы, выделяются. Если вы перетаскиваете сразу нескольких владельцев карт или групп, будет показано количество перемещаемых объектов.
6. Настройка дверей и зон:

6.1. В разделе **Doors (Двери)** или **Zones (Зоны)** нажмите **Add (Добавить)**.

6.2. Выберите двери или зоны и нажмите **Добавить (Add)**.

7. Настройка расписаний:

7.1. В разделе **Schedules (Расписания)** нажмите **Add (Добавить)**.

7.2. Выбрав одно или несколько расписаний, нажмите **Add (Добавить)**.

8. Нажмите **Save (Сохранить)**.

Правило доступа, в котором отсутствует один или более компонентов, описанных выше, является неполным. Просмотреть все неполные правила доступа можно на вкладке **Incomplete (Неполные)**.

Экспорт отчетов о конфигурации системы

Можно экспортировать отчеты, содержащие различные типы информации о системе. AXIS Camera Station Pro экспортирует отчеты в виде CSV-файла с разделителями-запятыми и сохраняет их в папке загрузок по умолчанию. Для экспорта отчета:

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Reports (Отчеты)** > **System configuration (Конфигурация системы)**.
3. Выберите отчеты, которые вы хотите экспортировать, и нажмите **Download (Загрузить)**.

Подробный отчет о владельцах карты	Включает информацию о владельцах карт, об учетных данных, о проверке карт и о последней операции.
Отчет о доступе владельцев карты	Включает информацию о владельце карты, а также информацию о группах владельцев карт, о правилах доступа, дверях и зонах, с которыми связан владелец карты.
Отчет о доступе группы владельцев карты	Включает имя группы владельцев карт, а также информацию о владельцах карт, правилах доступа, дверях и зонах, с которыми связана группа владельцев карт.
Отчет о правилах доступа	Включает имя правила доступа, а также информацию о владельцах карт, группах владельцев карт, дверях и зонах, с которыми связано правило доступа.
Отчет о доступе к двери	Включает имя двери, а также информацию о владельцах карт, группах владельцев карт, правилах доступа и зонах, с которыми связана дверь.
Отчет о доступе к зоне	Включает имя зоны, а также информацию о владельцах карт, группах владельцев карт, правилах доступа и дверях, с которыми связана зона.

Создание отчетов о действиях владельцев карт

Отчет о присутствии содержит список владельцев карт в определенной зоне в данный момент времени.

В отчете о сборе указываются владельцы карт в определенной зоне. Это помогает определить, кто находится в безопасности во время чрезвычайных ситуаций. Помогает управляющим зданий находить сотрудников и посетителей после эвакуации. Место сбора — назначенное считывающее устройство, на котором персонал отмечается в чрезвычайных ситуациях. Система формирует отчет о лицах, находящихся на территории и за ее пределами. Система отмечает владельцев карт как отсутствующих до тех пор, пока они не зарегистрируются в пункте сбора или пока кто-нибудь вручную не отметит, что они в безопасности.

Как для отчетов о сборе, так и для отчетов о присутствии требуется определить зоны отслеживания владельцев карт.

Создать и запустить отчет о сборе или присутствии:

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Reports (Отчеты)** > **Cardholder activity (Действия владельцев карт)**.
3. Нажмите **Add (Добавить)** и выберите **Roll call / Mustering (Перекличка / Сбор персонала)**.
4. Назовите отчет
5. Выберите зоны для отчета.
6. Выберите группы для отчета.
7. Если требуется отчет о сборе персонала, выберите **Mustering point (Место сбора)** и считывающее устройство.
8. Выберите временные рамки для отчета.
9. Нажмите **Save (Сохранить)**.
10. Выберите отчет и нажмите **Run (Выполнить)**.

Состояние отчета о присутствии	Описание
Присутствует	Держатель карты вошел в указанную зону и не вышел из нее до формирования отчета.
Не присутствует	Держатель карты вышел из указанной зоны и не вошел в нее снова до формирования отчета.

Состояние отчета о сборе	Описание
В безопасности	Владелец карты провел своей картой по считывателю в пункте сбора.
Отсутствуют	Владелец карты не провел карту по считывателю в пункте сбора.

Импорт и экспорт

Импорт владельцев карт

Этот параметр позволяет импортировать держателей карт, группы, учетные данные и фотографии из CSV-файла. Чтобы импортировать фотографии владельцев карт, убедитесь в том, что сервер имеет доступ к фотографиям.

При импорте держателей карт система управления доступом автоматически сохраняет конфигурацию системы, включая всю конфигурацию оборудования, и удаляет ранее сохраненную конфигурацию.

Пользователей из базы данных Active Directory также можно сопоставить с держателями карт. См. *Настройки Active Directory[БЕТА], on page 182*.

Варианты импорта	
Новинка	Удаляет существующих держателей карт и добавляет новых.
Обновить	Обновляет существующих держателей карт и добавляет новых.
Добавить	Сохраняет существующих держателей карт и добавляет новых. Номера карт и идентификаторы владельцев карт уникальны, они могут быть использованы только один раз.

1. На вкладке **Access management (Управление доступом)** нажмите **Import and export (Импорт и экспорт)**.
2. Нажмите **Import cardholders (Импорт владельцев карт)**.
3. Выберите **New (Новые)**, **Update (Обновить)** или **Add (Добавить)**.
4. Нажмите **Next (Далее)**.
5. Нажмите **Choose a file (Выбрать файл)**, найдите CSV-файл и нажмите **Open (Открыть)**.
6. Введите разделитель столбцов, выберите уникальный идентификатор и нажмите **Next (Далее)**.
7. Назначьте каждому столбцу заголовок.
8. Нажмите **Импорт**.

Настройки импорта	
Первая строка является заголовком	Выберите в том случае, если CSV-файл содержит заголовок столбца.
Разделитель столбцов	Введите формат разделителя столбцов для файла CSV.
Уникальный идентификатор	Для идентификации владельца карты по умолчанию система использует **Cardholder ID (Идентификатор владельца карты).** Можно также использовать его имя и фамилию или адрес электронной почты. Используйте этот параметр, чтобы предотвратить импорт дублирующихся записей о сотрудниках.
Формат номера карты	Параметр **Allow both hexadecimal and number (Разрешить шестнадцатеричные и числовые значения)** по умолчанию включен.

экспорт владельцев карт

Эта команда экспортирует имеющиеся в системе данные владельцев карт в файл в формате CSV.

1. На вкладке **Access management (Управление доступом)** нажмите **Import and export (Импорт и экспорт)**.
2. Нажмите **Export cardholders (Экспорт владельцев карт)**.
3. Выберите место расположения загрузки и нажмите **Save (Сохранить)**.

AXIS Camera Station Pro обновляет фотографии владельцев карт в папке `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` при изменении конфигурации.

Отмена импорта

Система автоматически сохраняет свою конфигурацию при импорте владельцев карт. Параметр **Undo import (Отменить импорт)** восстанавливает данные держателей карт и всю конфигурацию оборудования в состояние, в котором они находились до последнего импорта.

1. На вкладке **Access management (Управление доступом)** нажмите **Import and export (Импорт и экспорт)**.
2. Нажмите **Undo import (Отмена импорта)**.
3. Нажмите **Да**.

Настройка параметров управления доступом

Чтобы настроить поля данных владельцев карт, которые должны использоваться в панели управления, предназначенной для управления доступом:

1. На вкладке **Access management (Управление доступом)** нажмите **Settings (Настройки)** > **Custom cardholder fields (Пользовательские поля держателя карты)**.
2. Нажмите **+ Add (Добавить)** и введите имя. Можно добавить до 6 пользовательских полей.
3. Нажмите **Добавить**.

Чтобы разрешить использование кода объекта для проверки вашей системы контроля доступа:

1. На вкладке **Access management (Управление доступом)** нажмите **Settings (Настройки)** > **Facility code (Код объекта)**.
2. Выберите **Facility code on (Вкл. код объекта)**.

Примечание

При настройке профилей идентификации также необходимо выбрать **Include facility code for card validation (Учитывать код объекта при проверке карты)**. См. *Профили идентификации, on page 174*.

Чтобы отредактировать шаблон электронного письма для отправки QR-кода или мобильных учетных данных:

1. На вкладке **Access management (Управление доступом)** нажмите **Настройки** > **Email templates (Шаблоны электронной почты)**.
2. Измените свой шаблон и нажмите **Update (Обновить)**.

Шаблоны бейджей BETA

Вы можете настроить шаблоны бейджей с информацией о владельце карты, фотографиями, логотипами и индивидуальным брендингом. Для создания нового шаблона:

1. Перейдите в **Access management (Управление доступом) > Settings (Настройки) > Badge templates (Шаблоны бейджа)** BETA.
2. Нажмите **Create new template (Создать новый шаблон)**.
3. Введите название в поле **Template name (Название шаблона)**.
4. Выберите **Use as default template for printing (Использовать по умолчанию для печати)**, чтобы сделать этот шаблон шаблоном по умолчанию.
5. Настройте дизайн бейджа:
   - Выберите до пяти текстовых полей для отображения на лицевой стороне, включая любые настраиваемые поля, которые вы создали. При печати на бейдже будут отображаться только заполненные поля.

- Выберите шрифт и цвет для текста.
- Добавьте цвет фона или изображение.
- Загрузите логотип вашей организации.
- Для оборотной стороны добавьте либо цвет фона, либо изображение.

6. Нажмите **Save (Сохранить)**, чтобы сохранить изменения, или **Save as (Сохранить как)**, чтобы создать новый шаблон.

Примечание

После того, как шаблон был создан, его нельзя изменить, только переименовать.

Печать бейджа BETA

Вы можете печатать идентификационные бейджи для владельцев карт, используя настроенные шаблоны бейджей. Кодирование карт в настоящее время не поддерживается. Прежде чем начать, убедитесь в следующем:

- Убедитесь, что у владельца карты есть хотя бы одни учетные данные карты. Вы не можете печатать бейджи для владельцев карт без учетных данных.
- Необходим принтер с поддержкой размера карт CR80 и совместимых материалов для печати, например плотного картона.
- Настройте параметры печати в вашем браузере:
  1. Установите размер страницы на CR80 или пользовательский размер, соответствующий размерам вашей карты.
  2. Установите ориентацию на «Портрет».
  3. Отключите поля или установите для них минимальное значение.

Внимание

Функция Secure Entry (Безопаксный вход) работает с принтерами, для которых доступны драйверы Windows. Работоспособность подтверждена для принтеров серии HID Fargo. Если вам нужен драйвер для принтера, обратитесь к поставщику принтера.

Для печати бейджей:

1. Перейдите в **Access management (Управление доступом) > Cardholder management (Управление владельцами карт) > Cardholders (Владельцы карт)**.
2. Выберите одного или несколько владельцев карт.
3. Нажмите **Print badge (Печатать бейдж)** BETA.
4. Нажмите **Select template (Выбрать шаблон)** и в раскрывающемся списке **Template (Шаблон)** выберите нужный шаблон пропуска.
5. Если у держателя карты несколько учетных данных карты, выберите один вариант в раскрывающемся списке **Card (Карта)**.
6. Нажмите кнопку **Print (Печать)**.

Примечание

Если ваш принтер не поддерживает двустороннюю печать, сначала распечатайте все страницы лицевой стороны, затем переверните стопку карт и загрузите их в лоток снова, чтобы распечатать оборотные страницы.

System Health Monitoring БЕТА

Используйте вкладку System Health Monitoring (Мониторинг состояния системы) для мониторинга состояния одной или нескольких систем AXIS Camera Station Pro в одной сети.

Если вы управляете системами, расположенными в разных сетях, служба контроля работоспособности сервера в My Systems обеспечивает эти же функциональные возможности, но через использование облака.

	Показывает сводку по устройствам и системам, к которым у вас есть доступ. См. *Инвентарная ведомость, on page 205*.
	Показывает сводку и подробные сведения о записи для каждой камеры с контролируемых систем. См. *Хранилище, on page 206*.
	Отображает журналы System Health Monitoring для контролируемых систем. См. *Уведомления, on page 207*.

Ограничения

- Мониторинг свободного места для записей на устройствах серии AXIS S30 и S40 Recorder не поддерживается.
- Настройки уведомления влияют только на локальный сервер контроля работоспособности системы.
- Система помечает записи значением **None (Нет)** в качестве типа записи, за исключением непрерывной записи и записи по детекции движения.

Последовательность операций

1. *Настройка приложения System Health Monitoring БЕТА, on page 185*
   1.1. Настроить уведомления. См. *Уведомления, on page 186*.
   1.2. Настройка мультисистемы. См. *Мультисистема, on page 187*.
2. Мониторинг данных о работоспособности из систем AXIS Camera Station Pro.
   2.1. *Инвентарная ведомость, on page 205*
   2.2. *Хранилище, on page 206*
   2.3. *Уведомления, on page 207*

Инвентарная ведомость

На странице с перечнем устройств представлены сводные данные об устройствах и системах, к которым вы имеете доступ.

1. На вкладке **System Health Monitoring БЕТА** (Контроль работоспособности системы)нажмите .
2. Для просмотра сводных данных о системе нажмите **AXIS Camera Station**.
   На правой панели отображаются сведения о системе и сервере.
3. Чтобы просмотреть сводные данные по устройству в системе, нажмите устройство в списке.
   Если устройство содержит источник видеосигнала, на правой панели отображаются сведения об устройстве и хранилище.
4. Для загрузки системного отчета выберите **AXIS Camera Station system report (Системный отчет AXIS Camera Station)** в раскрывающемся меню **Create report (Создать отчет)**. См. *Системный отчет, on page 219*.
5. Для загрузки отчета System Health Monitoring:

5.1. В раскрывающемся списке **Create report (Создать отчет)** выберите **System Health Monitoring report (Отчет о мониторинге состояния системы)**.

5.2. Чтобы включить базу данных в отчет, выберите **Include all databases (Включить все базы данных)** и нажмите **Download (Загрузить)**.

5.3. Когда отчет будет готов, нажмите для его сохранения.

Хранилище

На странице Storage (Хранилище) показана сводка по хранилищу и подробные сведения о записи для каждой камеры с контролируемых систем. Щелкните заголовок столбца, чтобы выполнить сортировку по этому столбцу.

1. На вкладке **System Health Monitoring** BETA (Контроль работоспособности системы)нажмите .
2. При контроле работоспособности в многосистемной конфигурации выберите систему из раскрывающегося меню.

Краткая информация	
Статус	Состояние ресурса хранения. См. *Настройка хранилища, on page 80*.
Место расположения	Путь к ресурсу хранения и его имя.
Итого	Общий объем пространства ресурса хранения. Соответствует значению Total size (Общий размер), отображаемому в свойствах Windows для расположения хранилища.
Выделено	Максимальный объем пространства ресурса хранения, отведенный для записей.
Используется	Объем дискового пространства, используемого в настоящее время для хранения записей.
Последнее обновление	Время последнего обновления информации.

Камера	
Статус	(пусто): нормальное состояние. Значок предупреждения: срок хранения не соблюдается. Информационный значок: срок хранения не соблюдается, поскольку продолжительность записей с камеры слишком мала.
Название	Имя камеры.
Тип записи	Типы записей, применимые к камере.
Задать срок хранения записей	Срок хранения, заданный для камеры в разделе **Configuration > Storage > Selection (Конфигурация > Хранилище > Выбор)**.
Текущий срок хранения записей	Количество дней, в течение которых записи хранятся в хранилище.
Самая старая запись	Время самой старой записи с камеры в хранилище.
Последняя запись	Время самой последней записи с камеры в хранилище.
Место расположения	Место хранения, используемое камерой.

Камера	
Используемое пространство устройства хранения	Объем дискового пространства, используемого камерой для хранения записей.
Последнее обновление	Время последнего обновления информации.

Уведомления

На странице уведомлений отображаются журналы System Health Monitoring из контролируемых систем. Щелкните заголовок столбца, чтобы выполнить сортировку по этому столбцу.

На вкладке **System Health Monitoring** BETA (Контроль работоспособности системы)нажмите .

История	
Уведомление отправлено	Время отправки уведомления.
Наименование	Показывает имя устройства для уведомлений, инициированных правилом `device down`, или `system` для уведомлений, инициированных правилом `system down`.
Система	Имя системы, в которой произошло событие.
Правило	Правило, вызвавшее уведомление: `System down` (Система недоступна) или `Device down` (Устройство недоступно).
Обнаружено	Время обнаружения проблемы.
Разрешено	Время устранения проблемы.

Горячие клавиши

На вкладке Hotkeys (Горячие клавиши) отображаются доступные сочетания клавиш. Тип горячей клавиши зависит от того, что вы используете для управления AXIS Camera Station Pro.

- Сочетание клавиш на клавиатуре
- Сочетание клавиш на дополнительной цифровой клавиатуре
- Кнопка джойстика
- Кнопка колеса прокрутки

При удалении камеры или вида с подключенного сервера также удаляются и связанные с ними сочетания клавиш.

В системе горячие клавиши сгруппированы по следующим категориям:

- Камера
- Управление устройствами
- Перейти к камере
- Перейти к просмотру
- Навигация
- Предварительные установки PTZ
- Записи
- Последовательности
- Мультиэкранный режим
- Вкладка
- Прочее

Необходимо вручную назначить действия в категориях Navigate to cameras (Переход к камерам) и Navigate to views (Переход к представлениям).

Примечание

- Если при добавлении или изменении сочетания клавиш окажется, что это сочетание клавиш уже используется для другого действия, отобразится значок предупреждения. Наведите указатель мыши на значок предупреждения, чтобы просмотреть действие, вызывающее конфликт. Нажмите ESC, чтобы отменить действие. Нажмите ENTER, чтобы использовать это сочетание клавиш и автоматически удалить конфликтующее сочетание.
- В случае подключения к нескольким серверам в категориях Navigate to cameras («Переход к камерам») и Navigate to views («Переход к видам») также перечислены камеры и виды на подключенных серверах.

Назначить горячую клавишу	Если для действия не задано сочетание клавиш, щелкните пустое поле, чтобы назначить его. • Чтобы назначить сочетание клавиш с помощью клавиатуры, нажмите Ctrl и как минимум еще одну клавишу либо функциональную клавишу F2–F12. • Чтобы добавить горячую клавишу с помощью дополнительной цифровой клавиатуры, нажмите комбинацию цифровых клавиш или одну из функциональных клавиш F1-F5. • Чтобы назначить сочетание клавиш с помощью джойстика или поворотного регулятора (jog dial), нажмите соответствующую кнопку.
Изменить горячую клавишу	Чтобы изменить сочетание клавиш, щелкните его в строке соответствующего действия.
Удалить горячую клавишу	Чтобы удалить сочетание клавиш, щелкните его в строке соответствующего действия.
	Щелкните значок , чтобы напечатать таблицу значений горячих клавиш.
	Щелкните значок , чтобы сбросить настройки всех горячих клавиш к исходным значениям.

Клавиши панели управления системы видеонаблюдения

Сопо-ставле-ние горячих клавиш – джойстик	Действие по умолчанию	AXIS TU9002	AXIS T8311
Кнопка 1	Переход к предустановке 1	J1	J1
Кнопка 2	Переход к предустановке 2	J2	J2
Кнопка 3	Переход к предустановке 3	J3	J3
Кнопка 4	Переход к предустановке 4	J4	J4
Кнопка 5	Имитация левой кнопки мыши	J5	L
Кнопка 6	Имитация левой правой кнопки	J6	R
Кнопка 7	Выбрать предыдущую ячейку на мультиэкранном виде	Вверху слева	-
Кнопка 8	Выбрать следующую ячейку на мультиэкранном виде	Вверху справа	-
Кнопка 9	Перейти к предыдущей записи		-

Сопо-ставле-ние горячих клавиш – джойстик	Действие по умолчанию	AXIS TU9002	AXIS T8311
Кнопка 10	Воспроизвести/пауза	▶/II	-
Кнопка 11	Перейти к следующей записи	▶|	-
Кнопка 12	Добавить закладку	⚑	-
Кнопка 13	Переключать функцию кольца трансфокации между цифровым зумом и скоростью воспроизведения	M1	-
Кнопка 14	Переключение живой просмотр/запись	M2	-
Кнопка 15	Кадр назад	Левый верхний переключатель	-
Кнопка 16	Кадр вперед	Правый верхний переключатель	-

Сопо-ставле-ние горячих клавиш – клавиа-тура	Действие по умолчанию	AXIS TU9003	AXIS T8312
A	Открыть виды	⊞	⊞
B	Переход к следующей камере или виду	🎥	🎥
ALT+B	Переход к предыдущей камере или представлению	Alt+🎥	-
ВКЛАДКА	Переход к следующей вкладке	⇄	-
ALT+TAB	Переход к предыдущей вкладке	Alt+⇄	-
C	-	-	✣
D	-	-	🕒
E	-	-	🛠
ПЛЮС	Увеличить расстояние фокусировки	+	-

Сопоставление горячих клавиш – клавиатура	Действие по умолчанию	AXIS TU9003	AXIS T8312
МИНУС	Уменьшить расстояние фокусировки	-	-
F2	Открыть горячие клавиши	F2	F2
F4	Открыть журналы	F4	F4
F5	Открыть конфигурацию	F5	F5
F10	Автофокусировка	F10	-

Сопоставление горячих клавиш – поворотный переключатель	Действие по умолчанию	AXIS T8313
Колесо 1	Показать или скрыть маркер экспорта	L
Колесо 2	Добавить закладку	
Колесо 3	Перейти к предыдущей записи	
Колесо 4	Воспроизвести/Пауза	
Колесо 5	Перейти к следующей записи	
Колесо 6	Переключение живой просмотр/запись	R

Примечание

Джойстик AXIS T8311 Video Surveillance Joystick не поддерживает кнопки джойстика 7–10.

Журналы

По умолчанию на вкладке **Logs (Журналы)** отображаются текущие сигналы тревоги, события и журналы аудита. Кроме того, здесь можно выполнять поиск предыдущих журналов. Количество дней хранения журналов можно настроить в **Configuration (Конфигурация) > Server (Сервер) > Settings (Настройки)**.

Time (Время)	Дата и время действия.
Тип	Тип действия: сигнал тревоги, событие или запись в журнале аудита.
Категория	Категория действия.
Сообщение	Краткое описание действия.
Пользователь	Пользователь AXIS Camera Station Pro, выполнивший действие.
Компьютер	Компьютер (имя в Windows-домене), на котором установлено приложение AXIS Camera Station Pro. Это значение предоставляется клиентом и не может быть независимо проверено сервером.
Пользователь Windows	Пользователь Windows, осуществляющий администрирование AXIS Camera Station Pro. Это значение предоставляется клиентом и не может быть независимо проверено сервером. В колонке User (Пользователь) отображается аутентифицированный пользователь.
Сервер	Доступно только при подключении к нескольким серверам. Сервер, на котором происходит действие.
Компонент	Компонент, на основе которого создается журнал.

Search logs (Журналы поиска)

1. На вкладке **Logs (Журналы)** нажмите **Search (Поиск)** в разделе **Log search (Поиск в журналах)**.
2. Введите ключевые слова в поле фильтра. AXIS Camera Station Pro выполняет поиск в списке журналов, исключая поле **Time (Время)**, и отображает результаты, содержащие все указанные ключевые слова. Сведения о поддерживаемых операторах поиска см. в разделе *Оптимизация поиска, on page 47*.
3. Выберите **Alarms (Сигналы тревоги)**, **Audits (Аудиты)** или **Events (События)** в разделе **Filter (Фильтр)**.
4. Выберите в календаре дату или диапазон дат.
5. В раскрывающихся меню выберите время **начала** и **окончания** записи.
6. Нажмите **Поиск**.

Журнал тревог

В журнале **Alarms (Сигналы тревоги)** отображаются системные сигналы тревоги, а также сигналы тревоги, сформированные правилами и функцией обнаружения движения. В списке указываются дата и время тревоги, категория тревоги и связанное с ней сообщение. См. *Тревоги*.

	Нажмите сигнал тревоги и , чтобы открыть вкладку **Recordings (Записи)** и начать воспроизведение, если сигнал тревоги содержит запись.
	Нажмите тревогу и , чтобы увидеть последовательность действий по сигналу тревоги

	(отображается, если сигналу тревоги назначена определенная последовательность действий).
	Нажмите сигнал тревоги и , чтобы уведомить другие клиенты о подтверждении сигнала тревоги.
	Нажмите тревогу и , чтобы экспортировать журнал в текстовый файл.

Журнал событий

В журнале **Events (События)** отображаются в виде списка события камер и сервера, например записи, срабатывания триггеров, сигналы тревоги, ошибки и системные сообщения. В списке указывается дата и время события, категория события и сообщение, связанное с событием. Выберите события и нажмите значок в панели инструментов, чтобы экспортировать журнал событий в виде текстового файла.

Журнал аудита

В журнале **Audit (Аудит)** регистрируются все действия пользователей, например запущенные вручную записи, запуск и остановка потоковой передачи видео, правила действий, а также созданные двери и владельцы карт. Выберите записи аудита и нажмите на панели инструментов, чтобы экспортировать их в текстовый файл.

Управление номерными знаками

Для управления списками номерных знаков в AXIS Camera Station Pro откройте вкладку **License plate management** (Управление номерными знаками).

На этой вкладке можно редактировать три списка номерных знаков для отдельных камер или групп камер:

1. Выберите группу или камеру из списков **Groups** (Группы) и **Cameras** (Камеры).
2. Выберите список для редактирования. По умолчанию три списка, которые можно редактировать, называются **Allow list** (Список разрешенных адресов), **Block list** (Список заблокированных адресов) или **Custom list** (Пользовательский список).
3. Внесите изменения в список:
   - Чтобы отредактировать название списка, нажмите **Edit list name** (Редактировать название списка).
   - Чтобы добавить новый номерной знак, введите его в столбце License plate (Номерной знак) и при необходимости добавьте описание в столбце Description (Описание). Нажмите **Добавить**.
   - Чтобы изменить или удалить существующий номерной знак, выберите его и нажмите **Edit (Изменить)** или **Remove (Удалить)**.
   - Чтобы импортировать список номерных знаков из CSV-файла, нажмите **Import (Импорт)** и выберите файл. При этом текущий список будет перезаписан. Чтобы сохранить его копию, сначала экспортируйте список.
   - Чтобы экспортировать список номерных знаков в CSV-файл, нажмите **Export (Экспорт)**.
4. Нажмите **Apply (Применить)**, чтобы сохранить изменения.

Примечание

После применения изменений AXIS Camera Station Pro берет на себя управление списками номерных знаков для этой группы или камеры. Каждую ночь список на камере обновляется в соответствии со списками, сохраненными в AXIS Camera Station Pro, при этом все номерные знаки, сохраненные непосредственно на камере, перезаписываются.

AXIS Audio Manager Pro

Используйте вкладку **AXIS Audio Manager Pro** для непосредственного доступа к интерфейсу сервера AXIS Audio Manager Pro из AXIS Camera Station Pro. Подробнее об интерфейсе сервера см. *Руководство пользователя AXIS Audio Manager Pro*.

Вкладка отображается только после подключения к серверу AXIS Audio Manager Pro в AXIS Camera Station Pro. Для получения дополнительной информации см. раздел *Настройка AXIS Audio Manager Pro, on page 183*.

Внимание

Доступ к интерфейсу сервера AXIS Audio Manager Pro через Secure Remote Access v2 невозможен.

Интеграция также позволяет:

- *Создание триггеров AXIS Audio Manager, on page 110*.
- *Создавать действия AXIS Audio Manager, on page 120*.
- добавлять аудиозоны на карты. См. *Карта, on page 23*.
- *Использование интерфейсов оповещения в мультиэкранном режиме, on page 22*.
- Назначьте права пользователей, связанные с AXIS Audio Manager Pro, в AXIS Camera Station Pro См. раздел *Права доступа пользователей или групп, on page 146*.
- Выберите аудиоустройства с сервера AXIS Audio Manager Pro как связанные аудиоустройства для камеры См. *Изменение профилей потока, on page 57*.

Тревоги

В нижней части клиента AXIS Camera Station Pro находится вкладка Alarms (Сигналы тревоги), на которой отображаются сработавшие события и системные сигналы тревоги. Сведения о создании сигналов тревоги см. в разделе *Правила действия*. Информацию о сигнале тревоги «Требуется обслуживание базы данных» см. в разделе *Обслуживание базы данных, on page 238*.

Time (Время)	время возникновения сигнала тревоги.
Категория	категория тревоги, которая вызвала подачу сигнала.
Описание	краткое описание тревоги.
Сервер	Отображается при подключении к нескольким серверам. Сервер AXIS Camera Station Pro, отправивший сигнал тревоги.
Компонент	компонент, инициирующий сигнал тревоги.
	Отображает процедуру обработки сигнала тревоги. Доступно только если сигнал тревоги содержит процедуру обработки.
	Переходит к записям. Доступно только если сигнал тревоги содержит запись.
	Подтвердить выбранную тревогу
	Удалить тревогу. Сигнал тревоги удаляется только временно, если перед этим его не подтвердить.

При возникновении сигнала тревоги:

1. Нажмите **Alarms and Tasks (Сигналы тревоги и задачи)** в нижней части клиента AXIS Camera Station Pro и откройте вкладку **Alarms (Сигналы тревоги)**.
2. Для сигналов тревоги с записью, выберите сигнал тревоги и нажмите для перехода к записи на вкладке **Recording alerts (Оповещения при записи)**.
3. Для тревог без записи откройте вкладку с живым просмотром и дважды щелкните тревогу, чтобы показать запись за время тревоги на вкладке **Recording alerts (Оповещение при записи)**.
4. Для сигналов тревоги с действиями в случае тревоги выберите сигнал тревоги и нажмите , чтобы открыть действия в случае тревоги.
5. ЧЧтобы уведомить другие клиенты о подтверждении сигналов тревоги, выберите нужные сигналы и нажмите .
6. Для удаления сигналов тревоги из списка выберите их и нажмите .

Задачи

В нижней части клиента AXIS Camera Station Pro находится вкладка Tasks (Задачи).

Следующие задачи являются персональными и видны только администраторам и пользователям, которые их запустили:

- Системный отчет
- Создать отчет об инциденте
- Экспорт записей

Если вы являетесь администратором, вы можете просматривать и выполнять все задачи, запущенные любым пользователем, включая персональные задачи.

Если вы являетесь оператором или наблюдателем, то можете:

- Просматривать все задачи, запущенные вами, а также задачи, запущенные другими пользователями (но не личные задачи этих пользователей).
- Отменяйте или повторно запускайте задачи, которые вы запустили. Вы можете только повторно сформировать отчет об инцидентах и экспортировать задачи записи.
- Просматривать результат всех задач в списке.
- Удалять все завершенные задачи из списка. Это касается только локального клиента.

Название	Название задачи.
Start (Запустить)	Время начала выполнения задачи.
Сообщение	Отображает состояние или сведения о задаче. Возможные состояния: • **Canceling (Отмена)**: выполняется очистка перед отменой задачи. • **Canceled (Отменена)**: очистка завершена, задача отменена. • **Error (Ошибка)**: задача завершилась с ошибкой на одном или нескольких устройствах. • **Finished (Завершена)**: задача выполнена. • **Finished during lost connection (Завершена при потере соединения)**: задача была выполнена при отсутствии соединения с сервером. Состояние задачи невозможно определить. • **Lost connection (Соединение потеряно)**: во время выполнения задачи клиент потерял соединение с сервером. Состояние задачи невозможно определить. • **Running (Выполняется)**: задача выполняется. • **Pending (Ожидает)**: ожидает завершения другой задачи.
Собственник	Пользователь, который инициировал задачу.
Прогресс	Отображает ход выполнения задачи.
Сервер	Отображается при подключении к нескольким серверам. Показывает сервер AXIS Camera Station Pro, который выполняет задачу.

Для работы с одной или несколькими задачами:

1. Нажмите **Alarms and Tasks (Тревоги и задачи)** в нижней части клиентского ПО AXIS Camera Station Pro и нажмите вкладку **Tasks (Задачи)**.

2. Выберите задачи и нажмите одну из кнопок действий

	Нажмите для открытия диалогового окна с результатом выполнения задачи.
	Нажмите, чтобы отменить выполнение задачи.
	Нажмите для удаления задач из списка.
	Если задача завершилась с ошибкой при экспорте записей или создании отчета об инцидентах, нажмите, чтобы повторить попытку выполнить эту задачу.

Результат выполнения задачи

Если задача выполнялась на нескольких устройствах, то в диалоговом окне выводятся результаты ее выполнения применительно к каждому устройству. Проверьте и вручную настройте все операции, завершившиеся с ошибкой.

Для большинства задач приводятся следующие сведения. Для таких задач, как **Export recordings (Экспорт записей)** и **System report (Отчет о системе)**, дважды щелкните задачу, чтобы открыть папку с сохраненными файлами.

MAC-адрес	MAC-адрес обновленного устройства.
Адрес	IP-адрес обновленного устройства.
Сообщение	Сведения о выполнении задачи: • **Finished (Завершена)**: задача успешно выполнена. • **Error (Ошибка)**: не удалось выполнить задачу на устройстве. • **Canceled (Отменена)**: задача была отменена до завершения.
Описание	Сведения о задаче.

В зависимости от типа задачи указываются следующие сведения:

Новый адрес	Новый IP-адрес, назначенный устройству.
Правила действия	Версия встроенного ПО и наименование устройства.
Сведения	Серийный номер и IP-адрес замененного устройства, а также серийный номер и IP-адрес нового устройства.
Reference ID (Ссылочный идентификатор)	Ссылочный идентификатор отчета об инцидентах.

Создание отчетов

Лист конфигурации клиента

Лист конфигурации клиента полезен при устранении неполадок и при обращении в службу поддержки.

Чтобы просмотреть HTML-обзор конфигурации системы клиента:

1. Откройте меню **Configuration (Конфигурация)** > **Server (Сервер)** > **Diagnostics (Диагностика)**.
2. Нажмите **View client configuration sheet (Просмотр листа конфигурации клиента)**.

Лист конфигурации сервера

Лист Server configuration (Конфигурация сервера) содержит сведения об общей конфигурации, настройках камер, включая правила действий, расписания, хранилище записей, вспомогательные устройства и лицензии. Отчет полезен при поиске и устранении неполадок, а также при обращении в службу поддержки.

Чтобы просмотреть HTML-обзор конфигурации системы сервера:

1. Откройте меню **Configuration (Конфигурация)** > **Server (Сервер)** > **Diagnostics (Диагностика)**.
2. Нажмите **View server configuration sheet (Просмотр листа конфигурации сервера)**.

Системный отчет

Системный отчет представляет собой файл .zip, содержащий файлы параметров и журнала, которые помогают сотрудникам службы поддержки Axis при анализе вашей системы.

Обращаясь в службу поддержки клиентов, всегда прикладывайте системный отчет.

Для создания системного отчета:

1. Перейдите в **> Help (Справка) > System report (Системный отчет)**.
2. При необходимости измените имя файла, чтобы заменить автоматически сгенерированное имя.
3. Нажмите **Browse... (Обзор...)**, чтобы выбрать место сохранения системного отчета.
4. Выберите параметры:
   - Выберите **Automatically open folder when report is ready (Автоматически открывать папку после подготовки отчета)**, чтобы сразу открыть его.
   - **Включить все базы данных**, чтобы добавить подробную информацию о записях и системных данных.
   - **Include screenshots of all monitors (Добавьте снимки экрана всех мониторов)**, чтобы помочь при анализе системного отчета.
5. Нажмите кнопку **OK**.

Создать системный отчет

Примечание

- Если сервер не запускается, можно собрать упрощенный системный отчет на вкладке **Tools (Инструменты)** в AXIS Camera Station Service Control.
- Если клиент не может войти на сервер, служба поддержки Axis может запросить журналы клиента. Они находятся в папке, соответствующей версии клиента: `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Client 6.xx`.
- В зависимости от проблемы также может потребоваться собрать журналы событий Windows. Для этого откройте Просмотр событий, перейдите в **Windows Logs (Журналы Windows)**, затем щелкните правой кнопкой мыши **Application (Приложение)** и выберите **Save all events as (Сохранить все события как)**. То же самое выполните для **System (Система)**.

В этих случаях службе поддержки Axis также потребуются обычные журналы сервера для анализа.

AXIS Installation Verifier

AXIS Installation Verifier — это инструментальное средство, с помощью которого инициируется тестирование системы после установки, чтобы убедиться в полноценной работе всех установленных в системе устройств. Тестирование занимает около 20 минут.

Проверки	
Нормальные условия	Проверка потоковой передачи и хранения данных с использованием текущих настроек системы в AXIS Camera Station Pro. Результаты отображаются как «Пройден» или «Не пройден».
Условия слабой освещенности	Проверка потоковой передачи и хранения данных с использованием настроек, оптимизированных для типичных условий слабого освещения. Результаты отображаются как «Пройден» или «Не пройден».
Стресс-тест	Проверка с постепенным увеличением объема передаваемых и сохраняемых данных до достижения системой предельной производительности. В результатах отображается максимальная производительность системы.

Примечание

- Тестировать можно только устройства, совместимые с платформой AXIS Camera Application Platform 2 (ACAP 2) и более поздних версий.
- Во время проверки AXIS Camera Station Pro переходит в режим обслуживания, и все операции видеонаблюдения становятся временно недоступны.

Запуск тестирования:

1. Откройте меню **Configuration (Конфигурация)** > **Server (Сервер)** > **Diagnostics (Диагностика)**.
2. Нажмите **Open AXIS installation verifier... (Открыть AXIS Installation Verifier...)**.
3. Нажмите **Пуск**.
4. После завершения проверки нажмите **View report (Просмотреть отчет)**, чтобы открыть отчет, или **Save report (Сохранить отчет)**, чтобы сохранить его.

Список ресурсов

Вы можете экспортировать список ресурсов для своей системы управления видео. В списке ресурсов указывается название, тип, модель, состояние и серийный номер следующих категорий оборудования:

- Все подключенные серверы

- Все подключенные устройства
- Клиентский терминал, откуда вы экспортируете список ресурсов при подключении к нескольким терминалам.

Чтобы экспортировать список ресурсов:

1. Перейдите к пункту > **Other > Asset list (Прочее > Список ресурсов)**.
2. Нажмите на **Экспорт**.
3. Выберите местоположение файла и нажмите **Сохранить**.
4. В разделе **Latest export (Последний экспорт)** появляется ссылка на файл или обновляется существующая ссылка.
5. Для перехода к файлу откройте ссылку.

Состояние служб Axis

Чтобы просмотреть статус онлайн-сервисов Axis:

1. Откройте меню **Configuration (Конфигурация)** > **Server (Сервер)** > **Diagnostics (Диагностика)**.
2. Нажмите **Просмотр состояния служб Axis**.

Управление службами AXIS Camera Station Pro

Сервер использует управление службами AXIS Camera Station Pro для запуска, остановки служб и изменения их настроек. Оно запускается автоматически после завершения установки. Если компьютер сервера перезагружается, Service Control автоматически перезапускается примерно через 2 минуты. Значок в области уведомлений Windows отображает состояние службы.

Щелкните значок правой кнопкой мыши и выберите **Open AXIS Camera Station Service Control (Открыть AXIS Camera Station Service Control)**, **Start Service (Запустить службу)**, **Stop Service (Остановить службу)**, **Restart Service (Перезапустить службу)** или **Exit (Выйти)**.

Чтобы открыть Service Control из меню «Пуск»:

Перейдите в меню **Start (Пуск)** и выберите **All Programs (Все программы) > Tools (Служебные программы) > Service Control (Управление службами)**.

	Running (Работает).
	Выполняется запуск
	Остановлено

Изменение параметров	Выберите этот параметр, чтобы изменить настройки сервера.
Восстановить параметры по умолчанию	Нажмите, чтобы восстановить все настройки к исходным значениям по умолчанию.
Start (Запустить)	Нажмите для изменения состояния сервера.
Остановить	
Перезапуск	Нажмите для перезапуска сервера.

Общие настройки сервера

В приложении AXIS Camera Station Pro Service Control выберите **Modify settings (Изменить параметры)** и перейдите на вкладку **General (Общие)**, чтобы изменить общие настройки сервера.

Имя сервера	Имя данного сервера. Имя сервера отображается в программном клиенте. По умолчанию имя сервера совпадает с именем компьютера. Это имя не изменится, если вы измените имя компьютера.
Порт веб-клиента	Веб-клиент AXIS Camera Station использует этот порт.
Диапазон портов	Укажите диапазон портов. Остальные порты изменяются автоматически.
Разрешить AXIS Camera Station Pro добавлять исключения в брандмауэр Windows	Выберите этот параметр, чтобы разрешить AXIS Camera Station Pro автоматически добавлять исключения в брандмауэр Windows при изменении диапазона портов пользователем.

Примечание

- Если между сервером и клиентскими узлами установлен NAT, межсетевой экран и т. п., то их нужно настроить на обеспечение доступа к указанным портам.
- Номера портов не должны выходить за пределы диапазона 1024-65534.

Список портов для AXIS Camera Station Pro

В таблицах ниже указаны порты и протоколы, используемые AXIS Camera Station Pro. Для обеспечения оптимальной производительности и удобства работы может потребоваться разрешить эти порты в брандмауэре. Номера портов рассчитываются относительно основного порта HTTP 29200. В некоторых разделах указаны обязательные и необязательные порты. Для работы AXIS Camera Station Pro обязательные порты должны быть всегда открыты. Если необязательные порты запрещены, соответствующие функции работать не будут.

Взаимодействие «сервер — устройства»

Обязательные				
Порт	**Номер**	**Протокол**	**Направление**	**Описание**
Основной порт HTTP и HTTPS	443	HTTPS	Исходящий	Используется для активации лицензий, загрузки микропрограмм и работы

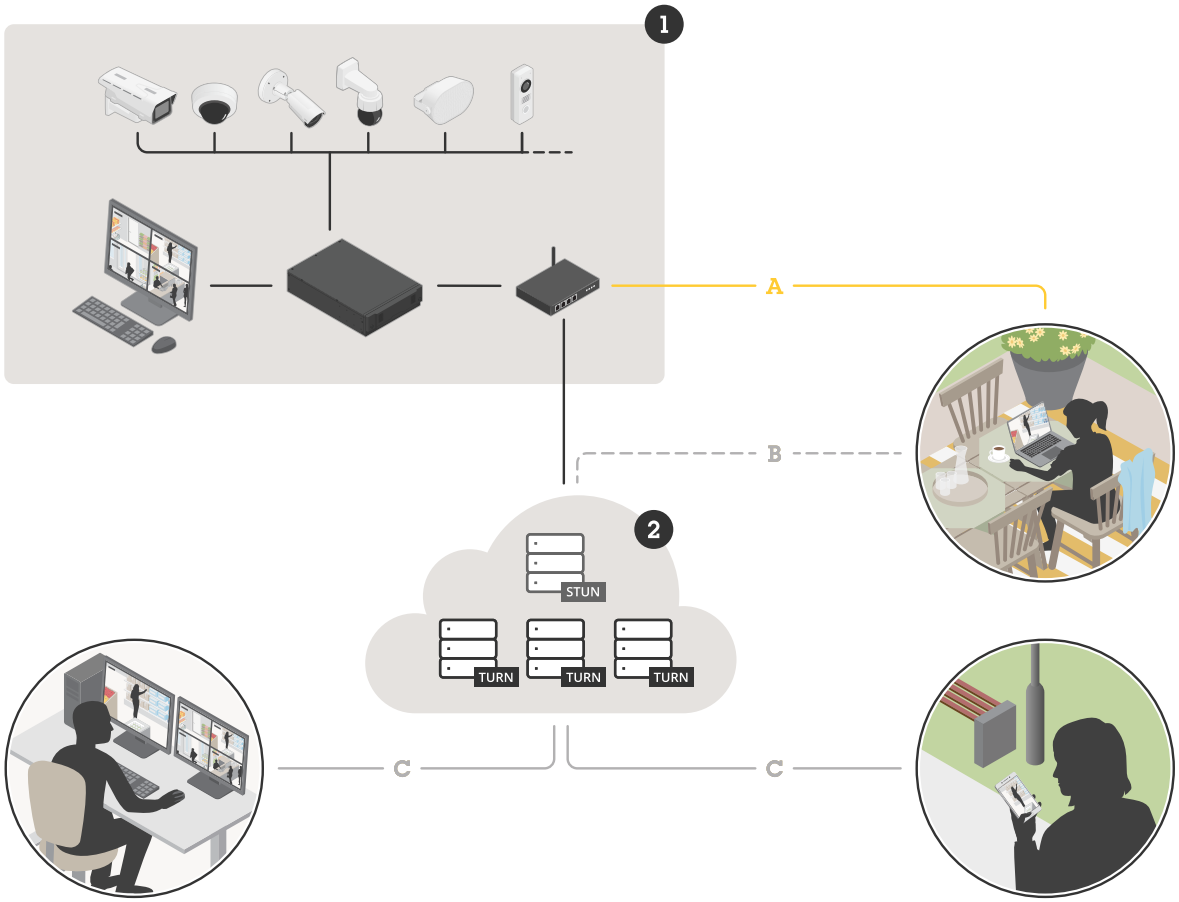
				подключенных служб.
Опция				
Порт WS-Discovery по умолчанию	3702	UDP	Входящие и исходящие	Веб-службы WS-Discovery, используемые для обнаружения устройств ONVIF. Multicast 239.255.255.250.
Порт Bonjour по умолчанию	5353	UDP	Входящие и исходящие	Используется для обнаружения устройств с помощью mDNS (Bonjour). Multicast 224.0.0.251. Если порт по умолчанию недоступен, возможно, он уже используется другим приложением, которое не предоставляет к нему совместный доступ. В этом случае вместо него используется случайный порт. Обратите внимание, что устройства с локальными адресами канала не обнаруживаются через Bonjour при использовании случайного порта.

Взаимодействие «клиент — сервер».

Требуются все порты					
Порт	**Номер**	**Протокол**	**Направление**	**Обмен данными между**	**Описание**
Основной порт HTTP и потоковый порт HTTP	29200	HTTP	Входящий	Сервер ACS и клиент ACS	Вспользуется для передачи видеопотока, аудиопотока и потока метаданных

					(шифрование AES).
Основной порт TCP	29202	TCP	Входящий	Сервер ACS и клиент ACS	Используется только для переключателя клиентов начиная с версии 6.17. Ранее это был основной TCP-порт.
Порт веб-сервера ACS API	29204	HTTPS	Входящий	Сервер ACS и мобильное приложение	Используется для передачи данных приложения и потоковой передачи видео MP4 по протоколу HTTPS.
Порт HTTP локального прокси-сервера	29206	TCP	Входящий	Внутри сервера ACS	Мобильные приложения отправляют запросы модулю SRA, который принимает HTTPS-запросы, преобразует их в HTTP и перенаправляет на локальный HTTP-порт прокси-сервера.
Порт конечной точки веб-прокси	29207	TCP	Входящий	Сервер ACS и компоненты	Используется для безопасного обмена данными между компонентом и устройствами.

Домены и сетевые порты для функции защищенного удаленного доступа Secure Remote Access v2 (SRA v2)



Изображение: Обзор решения Axis Secure Remote Access v2 в AXIS Camera Station Pro

1. Контролируемый объект в локальной сети с локальным клиентом просмотра
   - A — Удаленное соединение (прямое, peer-to-peer)
   - B — Временное соединение STUN/TURN с сервисами Axis Cloud Connected Services

Название или тип	Адрес	Номер порта.	Протокол	Направление
SRA v2 - My Axis Sign in	eu.login.connect.axis.com	443	TCP	Входящие и исходящие
SRA v2 - Обмен данными с облачным сервисом	eu.cs.connect.axis.com	443	TCP	Входящие и исходящие
SRA v2 - Обмен данными с API облачного сервиса	api.vms.axis.cloud	443	TCP	Входящие и исходящие
Компонент Uplink	acspro.mysystems.axis.com	443	-	Входящие и исходящие
EdgeHost component	75.2.119.140	443, 8443	-	Входящие и исходящие

EdgeHost component	99.83.133.42	443, 8443	-	Входящие и исходящие
EdgeHost component	cep.connect.axis.com	443, 8443	-	Входящие и исходящие

2. Axis Cloud Connected Services (облачные подключаемые сервисы Axis)
   – C — Удаленное соединение TURN с Axis Cloud Connected Services

Название или тип	Адрес	Номер порта.	Протокол	Направление
Обмен через P2P-прокси и компонент WebRTC	wss://signaling.prod.webrtc.connect.axis.com	443	TCP	Входящие и исходящие
Обмен через P2P-прокси и компонент WebRTC	https://*.turn.prod.webrtc.connect.axis.com	443, 3478, 5349, 49152-65535	TCP	Входящие и исходящие

Зарезервировано для компонентов системы

Обязательные						
Компонент	**Прослушивает интерфейс**	**Номер**	**Протокол**	**Направление**	**Обмен данными между**	**Описание**
Локальный сервер сигнализации WebRTC	localhost	29227	WSS	Входящий	Встраиваемый клиент, веб-клиент и WebRTC Streamer с сервером сигнализации	Входит в состав локального компонента WebRTC.
Настройка локального WebRTC	localhost	29229	HTTPS	Входящий	Клиент ACS (веб-страница)	Используется для размещения страницы настройки WebRTC и серверной части. Входит в состав локального компонента WebRTC.
Локальный сервер TURN	Все (0.0.0.0/INADDR_ANY)	29230	UDP	Входящие и исходящие	Встраиваемый клиент / веб-клиент с TURN-сервером	Используется для режима «WebRTC через один порт» в локальной системе ACS.

Локальный IDP IAM	0.0.0.0	29232	HTTPS	Входящий	Обратный прокси-сервер и local-iam, клиент ACS для Windows и local-iam	Общедоступный порт IDP_OIDC.
Локальный IDP IAM	0.0.0.0	29233	HTTPS	Входящий	Сторонние службы	Порт администратора mTLS.
Локальный IDP IAM	127.0.0.1	29234	HTTPS	Входящий	Сторонние службы	Порт токенизатора.
WebRTC	localhost	29235	HTTPS	Входящий	Облачный компонент	Используется при первоначальной настройке для конфигурирования облачного подключения WebRTC. Входит в состав компонента WebRTC.
API службы	127.0.0.1	29244	NATS	Входящий	Между ACS и компонентами, а также между самими компонентами по протоколу NATS.	Брокер NATS.
Опция						
Secure Entry (AC-MSM)	127.0.0.1	29214	HTTPS (WS)	Входящий	Клиент ACS (веб-страница) и компонент	Настраивается с использованием базового порта ACS. В более ранних системах использовался порт 8081.
Secure Entry (AC-MSM)	Все (0.0.0.0/ INADDR_ ANY)	29215	HTTPS (WS)	Входящий	Компоненты Secure Entry на разных охраняемых объектах	Настраивается с использованием

						базового порта ACS.
Контроль работоспособности системы	Все (0.0.0.0/ INADDR_ ANY)	29216	HTTPS	Входящий	ACS (веб-страница), серверная часть SHM (компонент)	Используется для размещения веб-страницы System Health Monitoring и обмена данными в многосистемной конфигурации.
Облачная служба System Health Monitoring / Cloud Service	localhost	29217	HTTPS	Входящий	ACS (веб-страница) и серверная часть Cloud Service (компонент)	Используется для работы облачных служб.
Интеллектуальный поиск 2	localhost	29218	HTTPS	Входящий	Клиент ACS (вкладка веб-страницы Smart Search) и серверная часть Smart Search (компонент)	Используется для размещения API Smart Search и обслуживания веб-страницы клиента.
VMS API	127.0.0.1, ::1	29219	GraphQL	Входящий	Клиенты VMS API и GraphQL	Используется для предоставления клиентам доступа к ACS через GraphQL API.
Веб-клиент	localhost	29223	HTTPS	Входящий	Веб-клиент для VMS API/ Встраиваемый клиент	Серверная часть выступает в роли прокси-сервера перед VMS API.
Встраиваемый клиент	localhost	29224	HTTPS	Входящий	Встраиваемый клиент в VMS API, WebRTC Streamer и Signaling Server	Серверная часть выступает в роли прокси-сервера перед VMS API.

Конфигурация веб-клиента	localhost	29225	HTTPS	Входящий	Клиент ACS (веб-страница)	Используется для размещения веб-страницы и серверной части конфигурации веб-клиента.
Конфигурация встраиваемого клиента	localhost	29226	HTTPS	Входящий	Клиент ACS (веб-страница)	Используется для размещения веб-страницы и серверной части конфигурации встраиваемого клиента.
OpenTelemetry	127.0.0.1	29236	gRPC	Входящий	Сторонние сервисы (ACS и другие компоненты)	gRPC-порт.
OpenTelemetry	127.0.0.1	29237	HTTPS	Входящий	Сторонние сервисы (ACS и другие компоненты)	Порт HTTP.
Audio Manager		29238	HTTPS	Входящий	Службы и компоненты интеграции сторонних производителей	Порт веб-сервера.
Data Insights Dashboard	localhost	29241	HTTPS	Входящий		Порт веб-сервера получателя.
Data Insights Dashboard	0.0.0.0	29242	MQTTS	Входящие и исходящие	Получатель сообщений о событиях камеры	Брокер Mosquitto.
OpenTelemetry	127.0.0.1	29245	HTTP	Входящий	Конечная точка мониторинга для получения метрик из коллектора	Порт HTTP.

					OpenTele-metry	
Умный поиск 2	localhost	29247	gRPC	Входящий	Ядро API VMS и преобраз-ователь Умный поиск	Преобраз-ователь Умный поиск.
Шлюз API	0.0.0.0	29248	HTTPS	Входящий	Пограничный узел и шлюз API	Резервный порт шлюза API, используемый пограничным узлом.
Шлюз API	0.0.0.0	29250	HTTPS	Входящий	Клиенты ACS и шлюз API	Резервный порт для HTTP- и HTTPS-трафика на портах 80 и 443. Отличается от +48 тем, что в +48 используются сертификаты компонентов, а здесь — сертификаты сервера.
Контроль работоспо-собности системы	127.0.0.1	29251	gRPC	Входящий	Сервер ACS и, возможно, другие компоненты к коллектору SHM	Используется источниками данных о состоянии системы для передачи данных в коллектор SHM.

Контроль работоспособности системы	127.0.0.1	29252	HTTPS	Входящий	Сервер ACS и, возможно, другие компоненты к коллектору SHM	Используется источниками данных о состоянии системы для передачи данных в коллектор SHM.
AXIS Body Worn Live	127.0.0.1	29254	TCP	Входящий	Сервер потоковой передачи в реальном времени, принимающий HTTPS-запросы от сервера ACS	Сервер потоковой передачи в реальном времени.

Другие порты

Обязательные

Порт	Номер	Протокол	Направление	Обмен данными между	Описание
Порт HTTP	80	HTTP	Исходящий	Сервер ACS и устройства, а также клиент ACS и сервер ACS ↔ Интернет	Используется для активации лицензий, загрузки микропрограмм и работы подключенных служб.
Порт HTTP	80	HTTP	Входящий	Клиент ACS и сервер ACS	Используется для видеопотоков и данных устройства.
Порт HTTPS	443	TCP	Входящий	Клиенты ACS и сервер ACS	Используется для видеопотоков и данных устройства.
Состояние обновления порта UDP	15156	UDP	Входящие и исходящие	Сервер ACS и ACS Service Control	ACS Service Control прослушивает этот порт, а сервер ACS передает сведения о ходе выполняемого обновления.

PostgreSQL	29210	TCP	Входящие и исходящие	PostgreSQL и любой пользователь	В настоящее время к пользователям относятся Data Insights Dashboard, компонент AXIS Audio Manager Pro и компонент AXIS Body Worn.
Опция					
Бортовые службы	29253	UDP	Входящий	Приемник GNSS и компонент бортовых сервисов	
Порт HTTP	80	HTTP	Исходящий	Сервер ACS и устройства, а также клиент ACS и сервер ACS с Интернетом	Используется для активации лицензии, скачивания встроенного ПО, подключенных услуг и т. д.
Порт HTTP	80	HTTP	Входящий	Клиент ACS и сервер ACS	Используется для видеопотоков и данных устройства.

База данных

Файлы базы данных

Основные файлы базы данных

AXIS Camera Station Pro хранит основные файлы базы данных в папке `C:\ProgramData\AXIS Communications\AXIS Camera Station Server`.

Для AXIS Camera Station версии до 5.13 используется только один файл базы данных:. **ACS.FDB**.

Для AXIS Camera Station версии 5.13 или более поздних версий используются три файла базы данных:

- **ACS.FDB**: Этот главный файл базы данных содержит конфигурацию системы, включая устройства, представления, разрешения, события и профили видеопотока.
- **ACS_LOGS.FDB**: Этот файл базы данных журналов содержит ссылки на журналы.
- **ACS_RECORDINGS.FDB**: В этом файле базы данных записей содержатся метаданные и ссылки на записи. Место хранения записей указано в меню **Configuration > Storage (Конфигурация > Хранение)**. Этот файл необходим AXIS Camera Station Pro для отображения записей на временной шкале во время воспроизведения.

Дополнительные файлы базы данных

SecureEntry.db – Файл базы данных AXIS Secure Entry содержит все данные контроля доступа, за исключением фотографий владельцев карт. Он хранится в папке `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\INTERNAL\main_db`.

smartSearch.sqlite3 – Файл базы данных умного поиска содержит конфигурацию камеры и сохраненные фильтры поиска. Он хранится в папке `C:\ProgramData\Axis Communications\AXIS Smart Search\data`.

Настройки базы данных

Система каждую ночь создает резервную копию базы данных, а также перед каждым обновлением. В приложении AXIS Camera Station Pro Service Control выберите **Modify settings (Изменить параметры)** и перейдите на вкладку **Database (База данных)**, чтобы изменить настройки резервного копирования.

Папка для резервного копирования	Нажмите **Browse (Обзор)** и выберите папку, куда будут сохраняться резервные копии. Перезапустите сервер AXIS Camera Station Pro, чтобы изменения вступили в силу. Если указан неправильный путь к папке резервного копирования или AXIS Camera Station Pro не имеет доступа к сетевому ресурсу, резервная копия сохраняется в папке `C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup`.
Срок хранения резервных копий в днях	Укажите срок хранения резервных копий. Можно задать любое значение от 1 до 30. Срок, заданный по умолчанию – 14 дней.
Ход процесса обновления	Для просмотра подробных сведений о последнем обновлении базы данных нажмите кнопку **View Details (Просмотреть подробности)**. В состав этих сведений входят события, которые произошли после последнего перезапуска приложения AXIS Camera Station Pro Service Control.

Создайте резервную копию базы данных

База данных содержит информацию о записях и другие метаданные, необходимые для обеспечения нормальной работы системы.

Внимание

- База данных не содержит записей. Укажите расположение хранилища в **Configuration (Конфигурация) > Storage (Хранилище)** и создайте резервную копию записей отдельно.
- Настройки сервера и базы данных в AXIS Camera Station Pro Service Control не сохраняются.

Резервное копирование системы

Система автоматически сохраняет резервную копию системы в папке, указанной на вкладке **Database (База данных)**. См. *Настройки базы данных, on page 235*. Резервная копия системы содержит как основные файлы базы данных, так и дополнительные файлы базы данных. См. *Файлы базы данных, on page 234*.

Файлы резервной копии	
`System_YYYY-MM-DD-HH-mm-SSSS.zip`	Резервная копия, создание которой было запущено ночью.
`PreUpgrade_YYYY-MM-DD-HH-mm-SSSS.zip`	Резервная копия, создание которой было запущено перед обновлением базы данных.
`User_YYYY-MM-DD-HH-mm-SSSS.zip`	Резервная копия, создание которой было запущено перед удалением хранилища.

В ZIP-файле содержатся следующие файлы:

ACS	Эта папке содержит основные файлы базы данных `ACS.FDB`, `ACS_LOGS.FDB` и `ACS_RECORDINGS.FDB`.
Компоненты	Эта папка доступна только при использовании компонента, например AXIS Camera Station Secure Entry или Умного поиска. • **webrtc**: эта папка содержит файлы конфигурации WebRTC. • **ACMSM**: эта папка содержит файл базы данных AXIS Camera Station Secure Entry `SecureEntry.db` и фотографии владельцев карт. • **smartsearch**: эта папка содержит файл базы данных умного поиска `smartSearch-backup-yyyyMMddHHmmssfff.sqlite3`.
`backup_summary.json`	Этот файл содержит более подробную информацию о резервной копии.
`_cluster_yyyyMMddHHmmssfff.dbcbackup`	Данный файл содержит логическую резервную копию кластера базы данных PostgreSQL, включая общие данные кластера, такие как роли и табличные пространства.

Служебное резервное копирование

На вкладке **Database (База данных)** укажите папку для хранения резервных копий при обслуживании. См. *Настройки базы данных, on page 235*. Служебная резервная копия содержит основные файлы базы данных, причем каждый файл помещается в отдельную папку `PreMaintenance_YYYY-MM-DD-HH-mm-SSSS`.

Запуск может выполняться различными способами:

- Автоматически во время обновления AXIS Camera Station Pro.
- При ручном запуске **Database maintainer (Средство обслуживания базы данных)** из AXIS Camera Station Pro Service Control. См. *Обслуживание базы данных, on page 238*.
- Автоматически с помощью запланированной задачи обслуживания базы данных, настроенной в планировщике заданий Windows. См. *Инструменты, on page 239*.

Резервное копирование вручную

Примечание

При резервном копировании вручную выполняется резервное копирование только основных файлов базы данных. При этом не выполняется резервное копирование дополнительных файлов базы данных, например файлов базы данных умного поиска.

Существует два способа выполнить резервное копирование вручную:

- **Способ 1:** перейдите в папку `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` и создайте копию файлов базы данных. Затем выполните резервное копирование кластера PostgreSQL:
  1. Откройте терминал с правами администратора в каталоге, где требуется сохранить резервную копию.

2. Выполните команду "C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" backup -cluster
3. Резервная копия будет сохранена в каталоге с именем **yyyyMMddHHmmssfff** в директории, из которой был открыт терминал.

- **Вариант 2**: создайте системный отчет и выберите **Include all databases (Включить все базы данных)**, чтобы включить файлы резервных копий базы данных. См. *Системный отчет, on page 219*.

Восстановление базы данных

Если произошел сбой базы данных из-за отказа оборудования или других проблем, то ее можно восстановить, взяв одну из сохраненных резервных копий. По умолчанию система хранит файлы резервных копий в течение 14 дней. Дополнительную информацию о резервном копировании базы данных см. в *Создайте резервную копию базы данных, on page 235*.

Примечание

База данных не содержит записей. Укажите расположение хранилища в **Configuration (Конфигурация) > Storage (Хранилище)** и создайте резервную копию записей отдельно.

Чтобы восстановить базу данных:

1. Откройте службу AXIS Camera Station Pro Service Control и остановите ее, нажав **Stop** (Остановить).
2. Перейдите к файлам резервной копии базы данных. См. *Создайте резервную копию базы данных, on page 235*.
3. Извлеките файлы.
4. Восстановление кластера базы данных PostgreSQL:
   4.1. Откройте терминал с правами администратора в распакованном каталоге.
   4.2. Выполните "C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" restore -backup-file _cluster_yyyyMMddHHmmssfff.dbcbackup
   4.3. При появлении запроса нажмите **y**, чтобы подтвердить, что вы доверяете источнику файла резервной копии.
5. В разархивированной папке найдите следующие файлы базы данных в папке **ACS** и скопируйте их в папку C:\ProgramData\AXIS Communications\AXIS Camera Station Server\.
   - **ACS.FDB** — для восстановления базы данных необходимо скопировать этот файл.
   - **ACS_LOGS.FDB** — скопируйте данный файл, если нужно восстановить журналы.
   - **ACS_RECORDINGS.FDB** — вы можете скопировать данный файл, если хотите восстановить записи.
6. Если вы используете AXIS Camera Station Secure Entry, выполните инструкции в файле RESTORE_INSTRUCTIONS.txt, который находится в папке C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db.
7. Если вы используете Умный поиск, скопируйте файл **smartSearch-backup-yyyyMMddHHmmssfff.sqlite3** из smartsearch в папку C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Smart Search\data и измените его имя на **smartSearch.sqlite3**.
8. Если вы используете веб-клиент для управления видеонаблюдением, скопируйте все файлы из webrtc в папку C:\ProgramData\Axis Communications\AXIS Camera Station\Components\WebRTC.
9. Вернитесь в AXIS Camera Station Pro панель управления службой и нажмите **Запустить** .

Обслуживание базы данных

Если отображается сигнал `Database maintenance is required` или если система неожиданно выключилась, например, после сбоя электропитания, необходимо выполнить обслуживание базы данных.

Чтобы начать обслуживание базы данных см. *Инструменты, on page 239*.

Примечание

AXIS Camera Station Secure Entry использует DB Janitor для монитора экрана; дисплей уменьшает файлы базы данных, если это необходимо. Система контроля доступа становится временно недоступной при принудительном уменьшении размера базы данных.

База данных лучших практик

Во избежание проблем помните о следующем:

Проверяйте диск на наличие ошибок – Ошибки диска могут приводить к порче базы данных. С помощью утилиты chkdsk (Проверка диска) или аналогичной проверьте на поврежденные секторы жесткий диск, на котором расположена база данных. Регулярно запускайте chkdsk.

Антивирусное программное обеспечение и внешние резервные копии – Не выполняйте проверку базы данных на наличие вирусов, поскольку некоторые антивирусные программы могут повредить ее. При использовании внешней системы резервного копирования не выполняйте резервное копирование активной базы данных. Вместо этого создайте резервную копию файлов, расположенных в папке резервного копирования.

Сбой питания – К повреждению базы данных может привести неожиданное отключение компьютера, например, из-за сбоя электропитания. Для ответственных установок используйте источники бесперебойного питания (ИБП).

Нехватка места – База данных может быть испорчена, если закончится место на жестком диске. Чтобы этого не случилось, устанавливайте сервер AXIS Camera Station Pro на специально выделенный компьютер а достаточным объемом памяти. Требования к аппаратному обеспечению см. по ссылке *axis.com/products/axis-camera-station/hardware-guidelines*.

Повреждение ОЗУ – Регулярно запускайте Windows Memory Diagnostic для проверки оперативной памяти на наличие ошибок.

Сертификаты

Используйте вкладку **Certificates (Сертификаты)** для управления сертификатами сервера для AXIS Camera Station Pro. Вы можете просматривать сведения о текущем сертификате сервера, проверять срок действия, генерировать и импортировать новые сертификаты, экспортировать действующий сертификат. Серверные сертификаты хранятся в C:\ProgramData\Axis Communications\AXIS Camera Station Server\certs.

Сертификат сервера

Создать	Создание нового самозаверяющего серверного сертификата. Создание нового сертификата заменяет ранее используемый сервером сертификат. Для вступления изменений в силу требуется перезапуск сервера.
Импорт...	Импорт серверного сертификата из файла. Поддерживаются форматы файлов PEM и PFX/PKCS12. Поддерживаются только ключи RSA длиной не менее 2048 бит.

Примечание

При импорте сертификата с промежуточными сертификатами в формате PEM все промежуточные сертификаты должны находиться в файле .cer. При создании собственных сертификатов см. раздел *Подготовка промежуточных сертификатов к импорту, on page 239*.

Текущий сертификат

Отображает сведения о текущем сертификате сервера. Используйте этот параметр для ручной проверки подключения клиента к правильному серверу.

Вид	Позволяет просмотреть подробную информацию о текущем сертификате сервера.
Экспорт...	Позволяет экспортировать сертификат сервера в файл PFX.

Создание нового серверного сертификата

- Нажмите клавишу Windows + S, введите и откройте службу управления AXIS Camera Station Pro (AXIS Camera Station Pro Service Control).
- Перейдите во вкладку **Certificates (Сертификаты)**, нажмите **Generate (Создать)** для генерации нового серверного сертификата.
- Перезапустите сервер, чтобы применить новый серверный сертификат.

Подготовка промежуточных сертификатов к импорту

Для импорта серверного сертификата с промежуточными сертификатами в AXIS Camera Station Pro необходимо объединить их в один файл:

1. Откройте серверный сертификат и промежуточный сертификат в Блокноте (Notepad). Структура содержимого каждого сертификата будет следующей:
```
cert.cer
——BEGIN CERTIFICATE——
MIIFTDCCB....
——END CERTIFICATE——
```
2. Скопируйте содержимое одного сертификата и вставьте его в другой, а первую строку измените на combined_cert.cer:
```
combined_cert.cer
——BEGIN CERTIFICATE——
MIIFTDCCB....
——END CERTIFICATE——
——BEGIN CERTIFICATE——
MIIE+zCCA+OgA.....
——END CERTIFICATE——
```
3. Сохраните файл.

Инструменты

В Service Control AXIS Camera Station Pro выберите **Modify settings (Изменить настройки)**, затем нажмите **Tools (Инструменты)** для выполнения обслуживания базы данных, создания частичного отчета о состоянии системы, включения сетевого журналирования или сброса центра сертификации.

Обслуживание БД

Запуск Database maintainer (Средство обслуживания базы данных):

1. Откройте управление службами AXIS Camera Station Pro Service Control.

2. Нажмите **Tools (Инструменты)**.
3. Нажмите **Run (Выполнить)** в разделе **Database maintainer (Обслуживание базы данных)**.
4. Отображается предполагаемое время простоя. Щелкните **Да**, чтобы продолжить. Запущенный процесс отменить невозможно.

Примечание

- AXIS Camera Station ProBo время обслуживания сервер AXIS Camera Station Pro и все выполняемые записи останавливаются. После завершения технического обслуживания сервер автоматически запускается.
- Не выключайте компьютер во время обслуживания.
- Для обслуживания базы данных требуются права администратора в системе Windows.
- Если обслуживание базы данных не привело к восстановлению базы данных, обратитесь в службу технической поддержки Axis.

Если отображается сигнал «Требуется обслуживание базы данных» или если система неожиданно выключилась, например, после сбоя электропитания, необходимо выполнить обслуживание базы данных.

Также можно запланировать автоматический запуск обслуживания базы данных: для этого в планировщике заданий Windows нужно включить задание «Задача обслуживания базы данных AXIS Camera Station Pro». Можно изменить условие срабатывания, чтобы настроить время и периодичность запуска Database maintainer (Средство обслуживания базы данных).

Ведение журнала сети

Запуск регистрации сетевого трафика:

1. Откройте управление службами AXIS Camera Station Pro Service Control.
2. Нажмите **Tools (Инструменты)**.
3. В разделе **Network logging (Регистрация сетевого трафика)** перейдите по ссылке, чтобы загрузить приложение для анализа сетевых протоколов.
4. После установки нажмите **Start... (Запустить...)**, чтобы запустить приложение.

Частичный отчет о системе

Частичный системный отчет — это архивированный файл в формате .zip, содержащий файлы параметров и журнала, которые помогают сотрудникам службы поддержки клиентов Axis проанализировать вашу систему. Обращаясь в службу поддержки клиентов, всегда прикладывайте системный отчет.

Сведения о создании полного отчета о системе см. в разделе *Системный отчет, on page 219*.

Чтобы создать частичный системный отчет:

1. Откройте AXIS Camera Station Pro Service Control.
2. Нажмите **Tools (Инструменты)**.
3. В разделе **Partial system report (Частичный отчет о системе)** нажмите **Run... (Выполнить...)**.
4. Выберите и введите запрашиваемую информацию в диалоговом окне.
5. Нажмите **Создать отчет**.

Сброс центра сертификации

Нажмите **Reset (Сбросить)**, чтобы создать новый центр сертификации и перезапустить службу.

- После перезапуска сервиса вы сможете войти в систему и при необходимости импортировать пользовательский центр сертификации.

Поиск и устранение неисправностей

Об этом руководстве

В этом руководстве описаны возможные неисправности AXIS Camera Station Pro и способы их устранения. Для удобства поиска проблемы сгруппированы по темам. Например, темой может быть Audio (Звук) или Live view (Живой просмотр). Для каждой проблемы предлагается решение.

Дополнительные материалы, включая требования к аппаратному обеспечению, обновления программного обеспечения и учебные руководства, см. на странице *axis.com/support*.

При возникновении общих проблем перед дальнейшим устранением неполадок попробуйте перезапустить службу сервера AXIS Camera Station Pro:

1. Откройте меню **Configuration (Конфигурация)** > **Server (Сервер)** > **Diagnostics (Диагностика)**.
2. Нажмите **Restart AXIS Camera Station server service... (Перезапуск службы сервера AXIS Camera Station...)**.

Примечание

Перезапуск службы сервера может занять некоторое время; отменить перезапуск невозможно. Сервер недоступен, а все подключенные устройства теряют соединение во время его перезапуска.

Служба AXIS Camera Station Pro

Служба часто перезапускается

Сервер может быть перегружен, что приводит к увеличению очереди задач и может также вызвать повреждение баз данных.

- Проверьте, не использует ли AXIS Camera Station Pro или другое приложение большое количество ресурсов.
- Запустите Database maintainer (Средство обслуживания базы данных). См. *Обслуживание базы данных, on page 238*.

Если ни одно из приведенных выше решений не помогает, обратитесь в службу поддержки Axis. Выберите *Порядок отправки запроса о решении проблемы в службу поддержки, on page 257*.

Устройства в системе управления видео

Неполадки общего характера

Перечисленные камеры не добавлены, поскольку VMS не может связаться с камерой.	1. Убедитесь, что камера подключена к сети, на нее подается питание и она работает. 2. Еще раз попытайтесь добавить камеру в меню **Configuration > Add devices (Конфигурация > Добавить устройства)**.
Перечисленные камеры не добавлены, поскольку пользователь отменил установку.	Чтобы добавить новые камеры, войдите в меню **Конфигурация > Добавить устройства**.
Не удалось задать пароль для указанных камер	1. Чтобы задать пароль вручную, откройте меню **Configuration > Devices > Management (Конфигурация > Устройства > Управление)**. 2. Нажмите камеру правой кнопкой мыши, а затем выберите **User Management > Set password (Управление пользователями > Установка пароля)**.

Не удается добавить устройство

До добавления в AXIS Camera Station Pro устройство использовалось в другой системе.	• Выполните сброс устройства до заводских настроек. • Попробуйте добавить устройство в AXIS Device Manager.
Попробуйте добавить устройство в AXIS Device Manager.	Это может быть проблема совместимости. Используйте последнюю версию AXIS Camera Station Pro.
Невозможно добавить другую модель устройства.	Устранение неполадок камеры см. на странице *axis.com/support/troubleshooting*.

Не удается обновить встроенное ПО устройства через AXIS Camera Station Pro

Не удается обновить встроенное ПО на всех устройствах	Устранение неполадок камеры см. на странице *axis.com/support/troubleshooting*.
Убедитесь в наличии сетевого соединения	• Убедитесь в наличии сетевого соединения. • Если проблема не связана с сетью, обратитесь в службу поддержки Axis. Выберите *Порядок отправки запроса о решении проблемы в службу поддержки, on page 257*.
Не удается обновить встроенное ПО на устройствах определенных моделей	Это может быть проблема совместимости. Связаться со службой технической Axis. Выберите *Порядок отправки запроса о решении проблемы в службу поддержки, on page 257*.

Устройства не найдены

Система управления видео автоматически выполняет поиск подключенных камер и видеокодеров в сети, но ничего не обнаружила.

- Убедитесь, что камера подключена к сети и получает питание.
- Если клиент, сервер или камеры находятся в разных сетях, выполните настройку параметров прокси-сервера и межсетевого экрана.
  - Если между клиентом и сервером находится прокси-сервер, измените параметры прокси-сервера.
  - Если между клиентом и сервером находится NAT или система безопасности, измените параметры NAT или системы безопасности. Разрешите прохождение через систему безопасности или NAT HTTP-порта, TCP-порта (Transmission Control Protocol) и порта потоковой передачи, указанных в AXIS Camera Station Service Control (Управление службой AXIS Camera Station). Полный список портов см. в разделе *Список портов для AXIS Camera Station Pro, on page 224*.
- Добавьте камеры вручную. Перейдите в *Добавить устройства, on page 6*.

Повторяющееся сообщение "Повторное подключение к камере через 15 секунд"

Возможные проблемы:

- Перегрузка сети.
- Камера недоступна. Убедитесь, что камера подключена к сети.

- Возникли проблемы с видеокартой.

Возможные способы устранения проблем с видеокартой:

- Установите последнюю версию драйвера видеокарты.
- Установите видеоадаптер с большим объемом видеопамяти и большей производительностью.
- Используйте центральный процессор для рендеринга видеоизображения. Выберите ее в разделе **Graphics card (Графическая карта)** в настройках **Hardware decoding (Аппаратное декодирование)**. Этот параметр находится в разделе **Configuration > Client > Streaming (Конфигурация > Клиент > Потоковая передача)**.
- Настройте параметры видео и аудио. Например, оптимизируйте параметры профиля для работы с низкой пропускной способностью.

Записи

Неполадки общего характера

Непрерывная запись не включена.	1. Для включения непрерывной записи перейдите в меню **Configuration > Recording and events > Recording method (Конфигурация > Записи и события > Способ записи)**. 2. Выберите камеру и активируйте пункт **Continuous (Непрерывная)**.
Не удается выполнить запись на указанный диск	1. Чтобы использовать другой ресурс хранения, перейдите в раздел **Configuration > Storage > Management (Конфигурация > Устройство хранения > Управление)**. 2. Добавьте накопитель и настройте параметры хранения для камер.
Не удается установить приложение AXIS Video Content Stream.	1. Чтобы установить приложение вручную, откройте меню **Configuration > Devices > Management (Конфигурация > Устройства > Управление)**. 2. Выберите камеру и нажмите .

Запись не запускается

Если запись не начинается или прекращается через несколько секунд, диск заполнен или на нем слишком много посторонних данных.

- В листе конфигурации сервера в разделе **Recording Storage (Хранилище записей)** проверьте наличие свободного места и отсутствие посторонних данных.
- Увеличьте лимит хранилища для системы управления видео.
- Выделите больше пространства для хранения. См. *Настройка хранилища, on page 80*.

Пробелы в записи во время непрерывной записи

Разрывы записей вызывают тревоги с меткой **Recording errors (Ошибки записи)**. Пробел может возникнуть по следующим причинам:

- Перегрузка сервера

- Проблема с сетью
- Перегрузка камеры
- Перегрузка диска

Проверьте, возникают ли разрывы записей на всех камерах. Если разрывы возникают не на всех камерах, это может указывать на перегрузку камеры. Используйте следующие вопросы для определения причины:

- Как часто возникает разрыв — каждый час или каждый день?
- Какова продолжительность разрыва — секунды или часы?
- В какое время возникает пробел?

Возможные решения:

- В диспетчере задач сервера проверьте, не используется ли какой-либо аппаратный ресурс с нагрузкой выше обычной. Если имеются признаки чрезмерной нагрузки на диск, добавьте диски и перенесите запись некоторых камер на новые диски.
- Уменьшите объем данных, записываемых на диск (настройки видео, Zipstream, частота кадров, разрешение). Учитывайте пропускную способность, рассчитанную с помощью AXIS Site Designer; см. *axis.com/support/tools/axis-site-designer*.

Дополнительную информацию вы найдете по адресу *Живой просмотр и воспроизведение, on page 245*.

Невозможно воспроизвести экспортированные записи

Если экспортированные записи не воспроизводятся в проигрывателе Windows Media, проверьте формат файла. Для воспроизведения экспортированных записей используется проигрыватель Windows Media (.asf) или AXIS File Player (.asf, .mp4, .mkv).

Дополнительную информацию см. в разделе *Воспроизведение и проверка записей в приложении AXIS File Player, on page 7*.

Примечание

Проигрыватель AXIS File Player автоматически откроет все записи, находящиеся в одной папке с проигрывателем.

Записи исчезают

Система сохраняет записи только в течение указанного количества дней. Чтобы изменить срок в днях, откройте меню **Конфигурация > Устройство хранения > Выбор**.

Если хранилище заполнено, система может удалить записи до окончания установленного срока хранения. Чтобы предотвратить заполнение хранилища, выполните следующие действия:

- Увеличьте емкость ресурса хранения. Откройте меню **Конфигурация > Устройство хранения > Управление**.
- Изменение объема хранилища, отведенного для AXIS Camera Station Pro. Откройте меню **Конфигурация > Устройство хранения > Управление**.
- Уменьшите объем файлов видеозаписей, изменив, например, разрешение или частоту кадров. Откройте меню **Configuration > Devices > Stream profiles (Конфигурация > Устройства > Профили потока)**.
  - Используйте для записи формат видео H.264. Формат M-JPEG требует значительно больше места в хранилище.
  - Используйте Zipstream, чтобы дополнительно уменьшить размер записей.

Проблемы с резервной записью

Недостаточно пропускной способности для передачи записи между камерой и сервером	Увеличьте пропускную способность сети.
Во время отключения камера не выполняла запись на SD-карту	• Просмотрите отчет сервера о камере. См. *axis.com/support/troubleshooting*. • Убедитесь, что SD-карта работает правильно и на ней есть записи.
Время камеры изменилось/сместилось с момента отключения	• Обязательно настройте NTP для будущих записей. • Синхронизируйте время камеры с сервером или используйте на камере тот же NTP-сервер, что и на сервере.

Примечание

Запись при отказе сервера не работает при управляемом завершении работы сервера или разрывах соединения продолжительностью менее 10 секунд.

Просмотр в реальном времени

Живой просмотр и воспроизведение

В этом разделе описаны возможные решения таких проблем как потеря кадров или графические сбои в клиенте AXIS Camera Station Pro.

Оборудование клиента	
Убедитесь, что установлена последняя версия драйвера для видеокарты и сетевого адаптера	1. Откройте средство диагностики DirectX (выполните поиск по запросу «dxdiag» на компьютере). 2. На веб-сайте изготовителя проверьте, что версия драйвера является самой последней для используемой операционной системы. 3. Убедитесь, что клиент и сервер работают на одном и том же компьютере. 4. Попробуйте запустить клиент на специально выделенном компьютере.
Проверьте количество мониторов	Мы не рекомендуем использовать более двух мониторов на одну графическую карту. Примечание Запуск клиента на виртуальной машине не поддерживается.
Графическая карта не поддерживает формат кодирования, заданный в **Configuration (Конфигурация) > Devices (Устройства) > Stream Profiles (Профили потоков)**	• Убедитесь, что графическая карта поддерживает формат кодирования используемых потоков. • Попробуйте использовать другие форматы кодирования. • Если поддерживаемый формат кодирования работает неправильно на нескольких камерах, убедитесь, что драйверы графической карты обновлены.

Подключенные устройства	
Одновременно подключено много клиентов	В зависимости от типового варианта использования, убедитесь, что система соответствует требованиям и следуйте рекомендациям по оборудованию. См. *Server requirements in the AXIS Camera Station Pro Installation and migration guide (Требования к серверу в руководстве по установке и миграции AXIS Camera Station Pro)*.
Камера подключена к другой системе управления видео, а не к AXIS Camera Station Pro	Отключите камеру от другого клиента и сбросьте настройки камеры по умолчанию, прежде чем подключать ее к AXIS Camera Station Pro.
Одна камера использует много различных потоков, особенно потоков с высоким разрешением	Это может быть проблемой, особенно для некоторых камер серии M-Line или многосенсорных камер. • Измените поток на тот же профиль потока или выберите более низкое разрешение. См. раздел *Профили потоков, on page 57*.

Перегрузка сервера	
Необычно высокая загрузка ЦП или ОЗУ, соответствующая времени возникновения проблемы	Убедитесь, что одновременно не работает другое приложение, потребляющее ресурсы ЦП или ОЗУ.

Проблема с сетью	
Необычное использование полосы пропускания в момент, совпадающий с временем возникновения проблемы.	Убедитесь, что одновременно не работает другое приложение, потребляющее большой объем пропускной способности сети.
Достаточная пропускная способность удаленной или локальной сети	• Просмотрите топологию вашей сети. • Проверьте работоспособность всех сетевых устройств (коммутатор/маршрутизатор/сетевой адаптер/кабель), используемых между камерами, сервером и клиентом.

Нет видео в режиме живого просмотра

Видео с заведомо исправной камеры не отображается в режиме живого просмотра.

- Отключите аппаратное декодирование. По умолчанию аппаратное декодирование установлено в режим **Auto (Автоматически)**. См. раздел Hardware decoding (Аппаратное декодирование) в разделе *Потоковая передача, on page 129*.
- Если установлено антивирусное ПО, оно может блокировать живые потоки или папки и процессы AXIS Camera Station Pro. См. часто задаваемые вопросы *FAQ*.

Другие возможные решения:

- Если вы не можете просматривать живое видео через веб-интерфейс либо если веб-интерфейс не работает, выполните поиск и устранение неполадок камеры. Перейдите на страницу *axis.com/support/troubleshooting*.
- Создайте отчет о состоянии сервера камер. Перейдите на страницу *axis.com/support/troubleshooting*.
- Убедитесь, что брандмауэр не блокирует соединения через определенные порты. См. раздел *Общие настройки сервера, on page 224*.

- Убедитесь, что Desktop Experience установлен в поддерживаемых версиях ОС Windows Server. См. раздел *Запланированный экспорт, on page 138*.
- Убедитесь, что поток с более низким разрешением работает правильно.

Если ничего из перечисленного не помогло, перейдите в *Порядок отправки запроса о решении проблемы в службу поддержки, on page 257*.

Производительность аппаратного декодирования

Воспользуйтесь этим руководством по устранению неисправностей, если во время живого просмотра наблюдаются задержки, рывки или прерывистое воспроизведение, высокая загрузка оборудования процессами ЦП либо часто появляется сообщение «Повторное подключение к камере».

1. Обновите драйверы графического адаптера. Устаревшие драйверы — наиболее распространенная причина проблем с аппаратным ускорением. Перейдите на веб-сайт производителя (NVIDIA, AMD или Intel) и загрузите последнюю версию драйвера для используемой модели графического процессора.
2. Настройте режим аппаратного декодирования. Перейдите в **Configuration (Конфигурация) > Client (Клиент) > Streaming (Потоковая передача)**:
   - Если выбран режим **Automatic (Автоматически)** или **On (Вкл.)** и возникают проблемы, установите значение **Off (Выкл.)**. Если производительность повысилась, возможно, производительности графического процессора недостаточно для обработки текущего количества потоков. См. шаг 6.
   - Если выбран режим **Off (Выкл.)** и загрузка процессора высокая, попробуйте установить **Automatic (Автоматически)** или **On (Вкл.)**, если используется достаточно производительный графический процессор.
3. Контролируйте использование системных ресурсов. Откройте Диспетчер задач Windows (Ctrl + Shift + Esc) и перейдите на вкладку **Performance (Производительность)**:
   - Если при отключенном аппаратном декодировании загрузка процессора стабильно превышает ~80 %, это может указывать на недостаточную производительность системы для обработки текущего количества потоков или их разрешения.
   - Если при включенном аппаратном декодировании выделенная память графического процессора почти полностью занята, это указывает на ограничение производительности графического процессора.
4. Чтобы снизить нагрузку на систему, уменьшите количество одновременно отображаемых камер или переключите камеры на профили потоков с более низким разрешением.
5. Убедитесь, что камеры передают видеопоток в формате H.264 или AV1. Для других кодеков аппаратное декодирование не используется.
6. Оцените возможности графического процессора. Даже если графический процессор поддерживает аппаратное декодирование, он может иметь ограничения по разрешению или частоте кадров. Если используется большое количество потоков высокого разрешения, ознакомьтесь с *требованиями к клиенту AXIS Camera Station Pro* и при необходимости используйте графический процессор с большим объемом видеопамяти и более высокой производительностью декодирования.
7. Если ни одно из приведенных выше решений не помогло, обратитесь в *службу технической поддержки Axis* и подготовьте следующую информацию:
   - Конфигурация оборудования системы (ЦП, ГП, ОЗУ).
   - Версия операционной системы.
   - Версия драйвера графического адаптера.
   - Версия AXIS Camera Station Pro.
   - Подробное описание симптомов и действий, необходимых для их воспроизведения.

Хранилище

Нет доступа к сетевому хранилищу

Если для входа в службу AXIS Camera Station Pro используется учетная запись локальной системы, добавлять сетевые хранилища, ссылаясь на общие папки на других компьютерах, невозможно.

Изменение учетной записи для входа в службу:

1. Откройте **Панель управления Windows**.
2. Поиск служб.
3. Нажмите **View local services (Просмотр локальных служб)**.
4. Нажмите правой кнопкой AXIS Camera Station Pro и выберите **Properties (Свойства)**.
5. Перейдите на вкладку **Log on (Войти)**.
6. Измените выбор **Локальная учетная запись системы** на **Данная учетная запись**.
7. Выберите пользователя с доступом к службе Windows Active Directory.

Сетевое хранилище отсутствует

Убедитесь, что компьютер и сервер, на которых запущено ПО для управления видео, относятся к тому же домену, что и сетевой накопитель.

Не удается повторно подключиться к сетевому хранилищу с новым именем пользователя и паролем

Если подключение к сетевому хранилищу требует авторизации, то важно отключить это сетевое хранилище от всех текущих соединений, прежде чем менять свое имя пользователя и пароль.

Изменение имени пользователя и пароля для сетевого хранилища с последующим повторным подключением:

1. Отключите сетевое хранилище от всех текущих соединений.
2. измените имя пользователя и пароль.
3. Откройте меню **Configuration > Storage > Management (Конфигурация > Устройство хранения > Управление)** и повторно подключитесь к сетевому хранилищу, используя новое имя пользователя и пароль.

Детектор движения

Неполадки общего характера

Не удается установить приложение AXIS Video Motion Detection.	Для установки приложения вручную перейдите в раздел *Установка приложений для камер, on page 74*.
Не удается получить текущие параметры обнаружения движения.	Восстановите заводские настройки камеры: 1. Выберите в меню **Конфигурация > Устройства > Управление**. 2. Щелкните правой кнопкой мыши неисправную камеру и выберите **Restore the camera to factory settings (Восстановить заводские настройки камеры)**. Во время сброса камера недоступна. Настройки IP-адреса и HTTPS не изменяются. После завершения сброса в столбце состояния отображается **Set**

	password (Задать пароль). Нажмите **Set password (Задать пароль)**, чтобы повторно подключить камеру к серверу.
Не настроен детектор движения	1. Чтобы настроить функцию обнаружения движения вручную, войдите в меню **Конфигурация > Записи и события > Способ записи**. 2. Выберите камеру и нажмите **Motion settings (Параметры движения)** для настройки детектора движения.
Обнаружение движения не включено.	1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**. 2. Выберите камеру и включите параметр **Motion detection (Детектор движения)**, чтобы при обнаружении движения начиналась запись.

Видеодетектор движения обнаруживает слишком много или слишком мало движущихся объектов

В этом разделе описаны возможные решения проблем, связанных с увеличением или уменьшением количества обнаружений в записях при использовании Video Motion Detection.

Настройка параметров движения

Вы можете выбрать настройки обнаружения движения для настройки области, в которой отслеживаются движущиеся объекты.

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Выбрав камеру, нажмите **Параметры движения**.
3. Выберите параметры в зависимости от прошивки камеры.

AXIS Video Motion Detection 2 и 4	Можно настроить область детекции. См. *Изменение настроек AXIS Video Motion Detection 2 и 4, on page 93*.
Встроенный видеодетектор движения	Возможна настройка окон включения и исключения. См. *Настройка встроенного видеодетектора движения, on page 94*.

Регулировка периода срабатывания

Период срабатывания — интервал между двумя последовательными срабатываниями. Используйте этот параметр, чтобы уменьшить количество последовательных записей. Если в течение этого интервала происходит дополнительное срабатывание, запись продолжается, а период срабатывания начинается заново.

Чтобы изменить период срабатывания:

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Выберите камеру.
3. В разделе **Advanced (Дополнительно)** настройте значение **Trigger period (Период действия триггера)** в секундах.

Правила действия

Неожиданные события с триггером ввода/вывода

Если примерно в 1:15 появляются неожиданные события ввода/вывода, замените существующие триггеры ввода-вывода на триггеры по событиям устройства.

Звук

Нет звука в режиме живого просмотра

Если в режиме живого просмотра отсутствует звук, выполните следующие действия:

- Передает ли камера изображение со звуковым сопровождением.
- Оснащен ли компьютер звуковой картой и включена ли она.
- Проверьте, настроен ли активный профиль на работу со звуком.
- Имеет ли пользователь полномочия просмотра изображения со звуком.

Настройте профили для передачи звука

1. Откройте меню **Configuration > Devices > Stream profiles (Конфигурация > Устройства > Профили потока)**.
2. Выберите камеру.
3. Выберите **MPEG-4** или **H.264** в пункте **Format (Формат)** меню параметров видеопрофиля.
4. В разделе **Audio (Аудио)** выберите микрофон в раскрывающемся списке **Microphone (Микрофон)**.
5. В раскрывающемся списке **Use microphone for (Использовать микрофон для)** выберите, когда использовать аудио.
6. При необходимости выберите динамик в раскрывающемся списке **Speaker (Динамик)**.
7. Нажмите кнопку **OK**.

Проверьте и измените права доступа пользователя

Примечание

Выполнение следующих действий возможно только с полномочиями администратора системы AXIS Camera Station Pro.

1. Перейдите в меню **Configuration (Конфигурация) > Security (Безопасность) > User permissions (Разрешения пользователей)**.
2. Выберите пользователя или группу.
3. Выберите **Audio listen (Прослушивать звук)** или **Audio speak (Воспроизведение голоса)** для требуемого устройства.
4. Нажмите **Применить**.

Нет звука при просмотре последовательности

Включить и выключить звук можно в профилях потоков. Дополнительную информацию см. в разделе *Профили потоков, on page 57*.

Нет звука при воспроизведении

Звук доступен при воспроизведении, если включить аудио в профиле, используемом для записи.

Примечание

Видео в формате M-JPEG не поддерживает звук. Выберите другой видеоформат.

Чтобы использовать звук в видеозаписях:

1. Перейдите в раздел **Configuration > Devices > Stream profiles (Конфигурация > Устройства > Профили потока)** для настройки требуемого формата видео для видеопрофиля.
2. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
3. Выберите камеру.
4. Выберите настроенный профиль в раскрывающемся меню **Profile (Профиль)**.
5. Нажмите **Применить**.

Записи по правилам

Порядок добавления звукового сопровождения в уже существующее правило:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Выбрав правило, нажмите **Правка**.
3. Нажмите **Next (Далее)** для перехода к разделу **Actions (Действия)**.
4. Выберите действие **Record (Запись)** и нажмите **Edit (Изменить)**.
5. Выберите профиль, использующий звук.
6. Нажмите **Закончить** для сохранения.

Войти в систему

Не удается войти в систему или подключиться к серверу

В этом разделе рассказывается о проблемах, возникающих при входе в систему с одним сервером или при подключении к этому серверу. При входе в систему на нескольких серверах клиент запускается и отображает состояние подключения в строке состояния. Дополнительные сведения о состоянии подключения см. в разделе *Состояние соединения, on page 140*.

Неправильное имя пользователя или пароль	• Проверьте написание или воспользуйтесь другой учетной записью. • Убедитесь, что у пользователя есть права доступа к серверу AXIS Camera Station Pro. • Часы на серверной и клиентской части AXIS Camera Station Pro должны быть синхронизированы. Кроме того, пользователям домена нужно проверить синхронизацию часов доменного сервера с часами сервера и клиента. • Пользователь, не добавленный на сервер, но входящий в локальную группу администраторов, должен запускать клиент от имени администратора. • Сведения о правах доступа пользователей см. в разделе *Права доступа пользователей, on page 144*.
Пользователь не авторизован для входа на сервер.	Добавьте пользователя в диалоговом окне **User permissions (Разрешения пользователей)**.
Не удается проверить безопасность сообщения	Значения времени UTC на клиенте и на сервере должны быть синхронизированы. Настройте время на клиентском узле и на сервере таким образом, чтобы разница не превышала 3 часа.
Нет связи с сервером	• Убедитесь, что компьютер сервера может подключиться к сети. • Проверьте, работает ли серверный компьютер. • Проверьте, правильно ли настроен брандмауэр.

	• Проверьте написание адреса сервера. • Проверьте параметры прокси клиента.
Сервер не отвечает	Проверьте, к тому ли компьютеру вы подключаетесь и запущено ли на нем серверное ПО AXIS Camera Station Pro.
Клиенту не удается подключиться к серверу	Проверьте правильность настройки сети: • Убедитесь, что используемая операционная система поддерживается. Полный список поддерживаемых операционных систем см. в *примечаниях к выпуску.* • В Service Control убедитесь, что сервер AXIS Camera Station Pro запущен, или при необходимости запустите сервер. • Убедитесь, что клиент и сервер подключены к одной и той же сети. Если это не так, клиент должен использовать внешний IP-адрес сервера. • На компьютере сервера настройте параметры прокси-сервера в разделе Свойства обозревателя Windows. • На странице входа в систему настройте параметры прокси-сервера клиента, выбрав **Change proxy settings (Изменить параметры прокси-сервера)**. • На компьютере клиента настройте параметры прокси-сервера клиента в разделе Свойства обозревателя Windows.
Не удается подключиться к серверу	• Убедитесь, что адрес и порт сервера AXIS Camera Station Pro указаны правильно. Убедитесь, что диапазон портов правильно настроен в Service Control. • Убедитесь, что NAT, брандмауэр или антивирусное ПО не блокирует подключение к серверу. См. раздел *Домены и сетевые порты для функции защищенного удаленного доступа Secure Remote Access v2 (SRA v2), on page 227* для получения дополнительной информации. • Проверьте работоспособность сервера через AXIS Camera Station Pro Service Control. – Откройте Service Control AXIS Camera Station Pro, см. *Управление службами AXIS Camera Station Pro, on page 222*. – Обратите внимание на состояние сервера, отображаемое на вкладке **General (Общие)**. Если состояние отображается как **Stopped (Остановлен)**, запустите сервер нажатием на **Start (Пуск)**.
Сервер не найден	• Проверьте, подключен ли серверный компьютер к сети. • Убедитесь, что адрес и порт сервера AXIS Camera Station Pro указаны правильно. • Убедитесь, что NAT, брандмауэр или антивирусное ПО не блокирует подключение к серверу. • Убедитесь, что настройки DNS вашего клиента указаны правильно. • Убедитесь, что на вашем DNS-сервере есть запись с именем хоста и IP-адресом сервера.
Не удалось подключиться к серверу	Убедитесь, что компьютер сервера и сеть не перегружены.

На сервере и клиенте установлены разные версии ПО	Обновите серверное ПО до той же версии, что и клиентское ПО.
Локальный сервер AXIS Camera Station Pro не работает	Используйте Service Control, чтобы запустить AXIS Camera Station Pro, или выберите удаленный сервер для входа в систему.
На этом компьютере не установлен сервер AXIS Camera Station Pro	Установите сервер AXIS Camera Station Pro или выберите другой сервер.
Выбранный список серверов пуст	Добавьте серверы в список, перейдя по ссылке **Edit (Изменить)** рядом со списком серверов для выбора.

Лицензии

Проблемы с регистрацией лицензии

При отказе в автоматической регистрации попробуйте выполнить следующие действия:

- Убедитесь в том, что система зарегистрирована для организации.
- Перейдите в **Configuration (Конфигурация)** и убедитесь, что **Automatic licensing (автоматическое лицензирование)** включено. См. раздел *Управление лицензиями, on page 142*.
- Убедитесь, что время на сервере установлено правильно.

Дополнительные сведения см. *в руководстве по установке и переходу на AXIS Camera Station Pro*.

Пользователи

Не удается найти пользователей домена

Если поиск пользователя домена завершается ошибкой, измените учетную запись для входа в службу:

1. Откройте **Панель управления Windows**.
2. Поиск служб.
3. Нажмите **View local services (Просмотр локальных служб)**.
4. Нажмите правой кнопкой AXIS Camera Station Pro и выберите **Properties (Свойства)**.
5. Перейдите на вкладку **Log on (Вход)**.
6. Измените выбор **Локальная учетная запись системы** на **Данная учетная запись**.
7. Выберите пользователя с доступом к службе Windows Active Directory.

Ошибки сертификата

AXIS Camera Station Pro не может обмениваться данными с устройством до устранения ошибки сертификата.

Возможные ошибки	
Сертификат не найден	Если вам известна причина, нажмите **Repair (Восстановить)**. Если вы подозреваете несанкционированный доступ, сначала выясните причину, и только потом восстанавливайте сертификат. Чтобы просмотреть подробные сведения о сертификате, нажмите **Advanced (Дополнительно)**. Возможно, сертификат был удален по одной из следующих причин: • Устройство было возвращено к заводским настройкам. • Отключена защищенная связь по протоколу HTTPS. • Устройство подверглось несанкционированному доступу и модификации.
Недоверенный сертификат	Если вам известна причина, нажмите **Trust This Device (Доверять этому устройству)**. В противном случае сначала выясните причину, и только потом отмечайте сертификат как доверенный. Чтобы просмотреть подробные сведения о сертификате, нажмите **Advanced (Дополнительно)**.

Отсутствует пароль для центра сертификации

Если в AXIS Camera Station Pro имеется центр сертификации без сохраненного пароля, отображается следующая тревога:

Необходимо предоставить пароль для сертификата центра сертификации. Дополнительные сведения см. в руководстве пользователя.

Эту проблему можно устранить одним из трех способов:

- Включите HTTPS на устройстве
- Импортируйте существующий центр сертификации
- Создайте новый центр сертификации

Для включения HTTPS на устройстве:

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. В списке щелкните правой кнопкой мыши на устройстве и выберите **Security (Безопасность) > HTTPS > Enable/Update (Активировать/обновить)**.
3. Щелкните **Да**, чтобы подтвердить.
4. Введите пароль для центра сертификации.
5. Нажмите кнопку **OK**.

Чтобы импортировать существующий центр сертификации, выполните следующие действия:

1. Перейдите в **Configuration (Конфигурация)> Security (Безопасность) > Certificates (Сертификаты) > Devices (Устройства)**.
2. В разделе HTTPS отключите параметр **Validate device certificate (Проверять сертификат устройства)**.
3. В разделе **Certificate authority (Центр сертификации)** нажмите кнопку **Import (Импортировать)**.

4. Введите пароль и нажмите **OK**.
5. Выберите срок действия (число дней) подписанных сертификатов клиента/сервера.
6. Выберите в меню **Конфигурация > Устройства > Управление**.
7. Щелкните устройства правой кнопкой мыши и выберите **Security > HTTPS > Enable/Update (Безопасность > HTTPS > Активировать/обновить)**.
8. Перейдите в меню **Configuration (Конфигурация) > Security (Безопасность) > Certificates (Сертификаты)> Devices (Устройства)** и включите **Validate device certificate (Проверять сертификат устройства)**.

Примечание

AXIS Camera Station Pro потеряет подключение к устройствам, и некоторые системные компоненты перезапустятся.

Чтобы разрешить AXIS Camera Station Pro создание нового центра сертификации:

1. Перейдите в **Configuration (Конфигурация)> Security (Безопасность) > Certificates (Сертификаты) > Devices (Устройства)**.
2. В разделе HTTPS отключите параметр **Validate device certificate (Проверять сертификат устройства)**.
3. В разделе **Certificate authority (Центр сертификации)** нажмите кнопку **Generate (Создать)**.
4. Введите пароль и нажмите **OK**.
5. Выберите срок действия (число дней) подписанных сертификатов клиента/сервера.
6. Выберите в меню **Конфигурация > Устройства > Управление**.
7. Щелкните устройства правой кнопкой мыши и выберите **Security > HTTPS > Enable/Update (Безопасность > HTTPS > Активировать/обновить)**.
8. Перейдите в меню **Configuration (Конфигурация) > Security (Безопасность) > Certificates (Сертификаты)> Devices (Устройства)** и включите **Validate device certificate (Проверять сертификат устройства)**.

Примечание

AXIS Camera Station Pro потеряет подключение к устройствам, и некоторые системные компоненты перезапустятся.

Синхронизация времени

Служба времени Windows не запущена

Служба времени Windows и сервер NTP не синхронизированы. Это может быть связано с тем, что служба времени Windows не может связаться с сервером NTP.

- Убедитесь, что сервер NTP доступен.
- Убедитесь, что параметры брандмауэра настроены правильно.
- Убедитесь, что устройство подключено к сети, через которую доступен сервер NTP.

Для получения поддержки обратитесь к системному администратору.

На устройстве обнаружена разница во времени

Устройство не синхронизировано по времени с сервером. Для записи используется временная метка времени получения записи сервером, а не времени ее записи устройством.

1. Перейдите в раздел **Configuration > Devices > Time synchronization (Конфигурация > Устройства > Синхронизация времени)** и проверьте смещение времени на устройстве.
2. Если смещение времени сервера превышает 2 секунды:
   2.1. Выберите **Enable time synchronization (Включить синхронизацию времени)**.

2.2. Убедитесь, что устройство может подключиться к указанному серверу NTP.

2.3. Перезагрузите устройство в меню **Configuration > Devices > Management (Конфигурация > Устройства > Управление)**.

3. Если смещение времени сервера составляет менее 2 секунд, устройство может передавать недостаточно данных для синхронизации времени.

3.1. Снимите флажок **Send alarm when the time difference between server and device is larger than 2 seconds (Отправлять тревогу, если разница во времени между сервером и устройством превышает 2 секунды)**, чтобы отключить тревоги.

Для получения поддержки обратитесь в службу поддержки Axis.

Secure Remote Access 2

Не удается локально подключиться к облачным службам

Устранение проблем с подключением к облачным службам:

1. Откройте AXIS Camera Station Pro и перейдите в **Configuration** > **Connected services** > **Management** (Конфигурация > Подключенные службы > Управление).
2. Убедитесь, что индикатор **Status (Состояние)** зеленый. Если это не так, проверьте подключение к Интернету.
3. Если проблема сохраняется, обратитесь в службу поддержки Axis.

Не удается удаленно подключиться к облачным службам

В AXIS Camera Station Pro:

1. Откройте **Menu (Меню)** > **Help (Справка)** и щелкните **Status of Axis services (Состояние служб Axis)**. Откроется страница состояния *https://status.axis.com*, где можно проверить уведомления о техническом обслуживании или запланированных периодах недоступности.
2. В разделе Axis Camera Station Pro откройте раскрывающийся список, чтобы проверить наличие доступа к облачным службам.
3. Убедитесь, что ваша учетная запись My Axis приглашена в соответствующую организацию.

В мобильном приложении AXIS Camera Station Pro:

1. Откройте **More (Еще)** > **Help (Справка)** и щелкните **Status of Axis services (Состояние служб Axis)**. Откроется страница состояния *https://status.axis.com*, где можно проверить уведомления о техническом обслуживании или запланированных периодах недоступности.
2. Убедитесь в наличии устойчивого подключения к Интернету. Чтобы идентифицировать причину проблемы, попробуйте провести тестирование на другом мобильном устройстве.
3. Убедитесь, что ваша учетная запись My Axis приглашена в соответствующую организацию.

Если проблема сохраняется, обратитесь в службу поддержки Axis.

Общие проблемы, связанные с потерей пакетов, задержкой или неправильной маршрутизацией

1. Проверьте наличие доступа к Интернету. Основные используемые порты 80 и 443 также должны быть открыты для исходящего трафика.
2. В зависимости от маршрутизатора может потребоваться открыть следующие дополнительные домены с портами:
   - https://eu.login.connect.axis.com с портом 433
   - https://eu.cs.connect.axis.com с портом 433
   - https://api.vms.axis.cloud с портом 433

- wss://signaling.prod.webrtc.connect.axis.com с портом 433
- https://*.turn.prod.webrtc.connect.axis.com с портами 443, 3478, 5349 и 49152-65535

Примечание

Звездочка (*) — это комбинация из идентификатора региона и нестатического идентификатора сервера.

Для получения дополнительной помощи обратитесь в службу поддержки Axis.

Техническая поддержка

Техническая поддержка предоставляется пользователям лицензионной версии ПО AXIS Camera Station Pro.

Чтобы обратиться в службу технической поддержки, выберите **> Help > Online Support (Справка > Онлайн-поддержка)** или перейдите по ссылке *axis.com/support*.

При обращении в службу техподдержки рекомендуем прикладывать системный отчет и снимки экрана.

Для создания системного отчета выберите **> Справка (Help) > Системный отчет (System report)**.

Порядок отправки запроса о решении проблемы в службу поддержки

Если возникли проблемы, которые невозможно решить с помощью этого руководства, передайте их специалистам службы поддержки через *онлайн-справочную службу Axis*. Чтобы служба поддержки могла лучше понять имеющуюся проблему и предложить ее решение, необходимо предоставить следующую информацию:

- Четкое описание способов воспроизведения проблемы или условий, при которых она возникает.
- Время возникновения проблемы и, если применимо, имя или IP-адрес затронутой камеры.
- System report (системный отчет) AXIS Camera Station Pro, созданный непосредственно после возникновения проблемы. Системный отчет должен быть сформирован из клиента или сервера, на которых была воспроизведена проблема. Если проблема возникает повторно предсказуемым образом, включите ведение журнала отладки для сервера и клиента, чтобы более полно зафиксировать проблему. После завершения не забудьте отключить ведение журнала отладки.

В некоторых случаях служба поддержки может запросить дополнительную информацию.

Примечание

Если размер файла превышает 1 ГБ, например если это сетевой трассировочный файл или файл базы данных, используйте надежный сервис безопасного обмена файлами для отправки файла.

Дополнительная информация	
Debug-level logs (Журналы уровня отладки)	Журналы уровня отладки по умолчанию отключены, поскольку размер файла журнала ограничен. Если вы включили ведение журналов уровня отладки, не забудьте отключить его после создания системного отчета. Server (Сервер): **Configuration (Конфигурация) > Server (Сервер) > Settings (Настройки) > Enable debug logging (Включить ведение журнала отладки)** Client (Клиент): **Configuration (Конфигурация) > Client (Клиент) > Settings (Настройки) > Enable debug logging (Включить ведение журнала отладки)**
Накладка отладочной информации в режиме живого просмотра и воспроизведения	При возникновении проблемы с живым просмотром или воспроизведением полезно предоставить запись экрана с отображением

Дополнительная информация	
	отладочной информации. Запись должна охватывать весь экран, включая системные часы, чтобы мы могли сопоставить проблему с записями в журналах. • Нажмите Ctrl + I один раз, чтобы отобразить информацию поверх изображения при просмотре в реальном времени. • Нажмите Ctrl + I два раза, чтобы добавить отладочную информацию. • Нажмите Ctrl + I три раза, чтобы скрыть отладочную информацию.
Файлы базы данных	Используйте это, если необходимо проверить базу данных или выполнить ее восстановление вручную. Выберите **Include database in the report (Добавить базу данных в отчет)**, перед тем как будет сформирован системный отчет. Добавляйте этот файл при возникновении проблем с запуском службы AXIS Camera Station.
Снимки экрана	При добавлении снимков экрана захватывайте весь экран, чтобы предоставить больше контекста. Если полноэкранный снимок недостаточно информативен, укажите стрелками область, на которой необходимо сосредоточить внимание.
Записи экрана	Используйте записи экрана, если проблему сложно описать словами, например если для ее воспроизведения требуется выполнить множество действий в пользовательском интерфейсе.
Recording files (Файлы записей)	Служба поддержки может попросить предоставить примеры файлов .acsm и .acsi, которые AXIS Camera Station использует для хранения записей. Это относится к проблемам с воспроизведением или экспортом записей, а также к проблемам с AXIS File Player. Эти файлы можно найти в расположении хранилища, выбранном для каждой камеры.

T10196821_ru

2026-07 (M33.8)

© 2023 – 2026 Axis Communications AB