AXIS Camera Station Pro

Руководство пользователя

О программе

AXIS Camera Station Pro является системой управления видеонаблюдением, обеспечивающей комплексное наблюдение, запись и администрирование видеопотоков с сетевых видеокамер Axis. Она предоставляет расширенные функции контроля доступа, управления распределенными объектами и интеграции с другими системами.

Система совместима с последними актуальными версиями AXIS OS, а также с последними версиями каждой ветки долгосрочной поддержки (LTS)*. Дополнительные сведения об AXIS OS приведены на портале *AXIS OS Portal*. Чтобы проверить, какие продукты работают с AXIS Camera Station Pro, см. *Compatible products (Совместимые продукты)*.

*Компания стремится обеспечивать совместимость с более ранними версиями AXIS OS при условии коммерческой целесообразности.

Параметры доступа

AXIS Camera Station Pro Сервер – управляет всеми данными, передаваемых с камер, видеокодеров и дополнительных устройств в вашей системе. Сведения о системных требованиях и планировании емкости см. в *Аппаратные требования* в *AXIS Camera Station Pro – Руководство по установке и миграции*.

AXIS Camera Station Pro Клиент – 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*.

AXIS Camera Station Pro мобильное приложение – 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.

Видеоруководства

Дополнительные подробные примеры использования системы см. в *видеоруководствах 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

Ниже приведены некоторые разделы, которые могут вас заинтересовать:

- *Подключить к серверу, on page 8*
- *Настроить устройства, on page 47*
- *Настройка хранилища, on page 77*
- *Настройка записи и событий, on page 82*
- *Настройка подключенных сервисов, on page 128*
- *Настройка сервера, on page 132*
- *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

Ниже приведены некоторые разделы, которые могут вас заинтересовать:

- *Руководство по началу работы с AXIS Camera Station Pro для операторов*
- *Подключить к серверу, on page 8*
- *Настройка клиентского ПО, on page 123*
- *Просмотр в реальном времени, on page 13*
- *Воспроизведение записей, on page 25*
- *Экспорт записей, on page 27*
- *Памятки AXIS Camera Station Pro — просмотр и экспорт*

Краткое руководство по началу работы

В настоящем руководстве последовательно рассматриваются все действия, необходимые для включения и запуска системы.

Прежде чем начать, убедитесь в следующем:

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

Для администраторов:

1. *Запуск системы управления видео*
2. *Добавить устройства*
3. *Настройка способа записи, on page 5*

Для операторов:

1. *Просмотреть живое видео, on page 6*
2. *Просмотр записей, on page 6*
3. *Экспорт записей, on page 6*
4. *Воспроизведение и проверка записей в приложении AXIS File Player, on page 6*

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 для запуска процесса лицензирования. Дополнительные сведения см. в разделах *Управление подключенными сервисами, on page 128* 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

Страница **Add devices (Добавить устройства)** открывается при первом запуске AXIS Camera Station Pro. AXIS Camera Station Pro выполняет поиск подключенных устройств в сети и выводит на экран список найденных устройств. См. *Добавить устройства*.

1. Выберите из списка камеры, которые нужно добавить. Если не удается найти камеру, нажмите кнопку **Manual search (Поиск вручную)**.
2. Нажмите **Добавить**.
3. Выберите один из двух вариантов: **Быстрая настройка** или **Конфигурация AXIS Site Designer**. Нажмите **Next** ("Далее"). См. *Импорт проектов Site Designer, on page 51*.
4. Используйте параметры по умолчанию и убедитесь, что для метода записи задано значение **None (Нет)**. Щелкните **Установить**.

Настройка способа записи

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

2. Выберите камеру.
3. Включите функцию **Motion detection (Обнаружение движения)** или **Continuous (Непрерывная)** или обе.
4. Нажмите **Применить**.

Просмотреть живое видео

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

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 25*.

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 кнопку **Export... (Экспорт...)**.

Для получения дополнительных сведений см. *Экспорт записей, on page 27*.

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)**. Появится страница результатов проверки.

Примечание

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

Конфигурация сети

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

Настройки прокси клиента

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

Параметры прокси-сервера на сервере

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

NAT и межсетевой экран

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

Дополнительные сведения см. в разделах *Список портов для AXIS Camera Station Pro, on page 218* и *Configure the firewall to allow access to AXIS Secure Remote Access in the AXIS Camera Station Pro Troubleshooting guide (Настройка брандмауэра для разрешения доступа к AXIS Secure Remote Access в руководстве по устранению неполадок AXIS Camera Station Pro)*.

Настройка порта сервера

Сервер AXIS Camera Station Pro использует порты 29202 (TCP), 29204 (мобильная связь) и 29205 (мобильная потоковая передача) для связи между сервером и клиентом. При необходимости порты можно изменить с помощью приложения AXIS Camera Station Pro Service Control.

Примечание

Меняйте порты только в том случае, если собираетесь использовать AXIS Camera Station без Axis Secure Remote Access 2 или других наших облачных сервисов.

Дополнительные сведения см. в разделе *Общее* или *Часто задаваемые вопросы*.

Рекомендации по обеспечению безопасности

Во избежание несанкционированного доступа к камерам и записям рекомендуется придерживаться следующих правил.

- 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. Служба Windows® Active Directory обеспечивает высокий уровень безопасности.

Подключить к серверу

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

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 8*.

Axis Secure Remote Access – См. *Войти в AXIS Secure Remote Access, on page 9*.

Axis Secure Remote Access 2 – См. *Вход в систему с помощью AXIS Secure Remote Access 2, on page 9*.

Примечание

При первом подключении к серверу клиент проверяет идентификатор сертификата сервера. Чтобы убедиться, что вы подключаетесь к правильному серверу, вручную сверьте идентификатор сертификата с тем, который отображается в AXIS Camera Station Pro Service Control. См. *Общее, on page 218*.

Для обеспечения соединения между клиентом и сервером они должны иметь одинаковую версию. При несоответствии версий при подключении к локальной системе или системе с пробросом портов, что может вызвать проблемы совместимости, клиент может загрузить корректную версию для соответствия версии сервера. После этого клиент переключается на соответствующую версию.

Обновление клиентов систем, подключенных через Secure Remote Access, необходимо выполнять вручную. Для подключения клиента к нескольким серверам каждый сервер должен иметь ту же версию. По умолчанию ярлык клиента использует последнюю версию.

Рекомендуем использовать **Kerberos** для проверки подлинности пользователей клиента AXIS Camera Station, дополнительные сведения см. в разделе *Аутентификация с использованием Kerberos в руководстве по усилению защиты системы AXIS Camera Station Pro*.

Список серверов	Чтобы подключиться к серверам из списка серверов, выберите один из раскрывающегося меню **Server list (Список серверов)**. Выберите для составления или изменения списков серверов. 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 на всех подключенных серверах, 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 в списке нет нужного сервера, щелкните , чтобы обновить список 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. Доступны следующие варианты 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 в полночь первого числа каждого месяца.

Сведения о том, как активировать Axis Secure Remote Access 2, см. в разделе *Axis Secure Remote Access 2, on page 130*.

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. Откройте на мобильном устройстве страницу *axis.com/products/axis-camera-station/overview* и скачайте 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. Подробнее об этом можно узнать в *Руководстве пользователя по мобильному приложению AXIS Camera Station Mobile*.

Войти в AXIS Secure Remote Access

Внимание

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

Что это означает для вашей системы AXIS Camera Station Pro?

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

Примечание

- При попытке подключения к серверу с помощью Axis Secure Remote Access сервер не может автоматически обновить клиент.
- Если прокси-сервер находится между сетевым устройством и сервером AXIS Camera Station Pro, необходимо настроить прокси-сервер в Windows на сервере AXIS Camera Station Pro для доступа к серверу с помощью AXIS Secure Remote Access.

1. Перейдите по ссылке **Войти в службу AXIS Secure Remote Access**.
2. Введите учетные данные My Axis. См. *Axis Secure Remote Access*.
3. Нажмите **Sign in (Войти)**.
4. Нажмите **Grant (Предоставить)**.

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.

AXIS Camera Station Pro Клиент

При первом запуске AXIS Camera Station Pro открывается страница «Добавить устройства» на вкладке «Конфигурация». См. *Добавить устройства*.

Вкладки

Просмотр в реальном времени	Просмотр видео в режиме реального времени с подключенных камер. См. *Просмотр в реальном времени*.
Записи	поиск, воспроизведение и экспорт записей. См. *Записи*.
Умный поиск 1	Поиск важных событий на видеозаписи с помощью функции поиска движущихся объектов. 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 44*.
Конфигурация	администрирование и обслуживание подключенных устройств, а также настройка параметров клиента и серверов. См. *Конфигурация*.
Горячие клавиши	список горячих клавиш для выполнения определенных действий. См. *Горячие клавиши*.
Журналы	журналы для регистрации сигналов тревоги, событий и аудита. См. *Журналы*.
Контроль доступа	Конфигурирование и управление владельцами карт, группами, дверями, зонами и правилами доступа в системе. См. *Контроль доступа, on page 187*.
Интеллектуальный поиск 2	Использование расширенных фильтров для поиска транспортных средств и людей на основе их характеристик. См. *Интеллектуальный поиск 2, on page 37*.
Контроль работоспособности системы	Отслеживание данных о работоспособности из одной или из нескольких систем AXIS Camera Station Pro. См. *System Health Monitoring BETA, on page 199*.
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	Открытие параметров, относящихся к справке. Чтобы узнать, какая версия клиента **используется, выберите** Справка > О программе AXIS Camera Station Pro.
Выйти из системы	Отключение от сервера и выход из клиентской программы AXIS Camera Station Pro.
Закрыть	Выход из клиентской программы AXIS Camera Station Pro с ее закрытием.

Строка заголовка

? или F1	Откройте справку.
⛶	Введите полноэкранный режим.
⛶ или ESC	Выход из полноэкранного режима.

Строка состояния

В строке состояния отображается представленная ниже информация:

- При рассогласовании по времени между клиентом и сервером появляется предупреждающий значок. Чтобы исключить проблемы, связанные с привязкой ко времени, всегда следите за тем, чтобы время на клиенте было синхронизировано со временем сервера.
- Состояние подключения серверов — это количество подключенных серверов. См. *Состояние соединения*.
- Статус лицензии показывает количество нелицензированных устройств. См. .
- Для службы безопасного удаленного доступа показывается, какой объем данных остался еще неиспользованным или каково превышение в текущем месяце относительно того объема, который предусмотрен для вашего уровня обслуживания. См. *Axis Secure Remote Access*.
- При наличии новой версии, если вы вошли в систему с учетной записью администратора, отобразится уведомление **AXIS Camera Station Pro update available (Доступно обновление)**. См. *Обновить AXIS Camera Station Pro, on page 136*.

Тревоги и Задачи

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

Просмотр в реальном времени

При живом просмотре отображаются виды, камеры и живые видео с подключенных камер, а при подключении к нескольким серверам AXIS Camera Station Pro отображаются все виды и камеры подключенных серверов, сгруппированные по имени сервера.

Виды обеспечивают доступ ко всем камерам и прочим устройствам, добавленным в AXIS Camera Station Pro. Вид может представлять собой одну или несколько камер, последовательность объектов, карту или веб-страницу. 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 21*

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

Сведения о настройке живого просмотра см. в разделе *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 правой кнопкой мыши камеры, виды или видеофрагменты 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 новый мультиэкран, последовательность, вид с камеры, веб-страницу или папку.
✎	Редактирование вида или имени камеры. Сведения об изменении настроек камеры см. в *Изменение настроек камеры*
🗑	Удалите вид. Для удаления вида потребуются разрешения на изменение вида и всех дополнительных видов. Для получения информации о том, как удалить камеры из AXIS Camera Station Pro, см. раздел *Камеры, on page 54*.
🔒	Являясь администратором, вы может заблокировать вид и запретить операторам и наблюдателям перемещать или изменять данный вид.

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 стоп-кадров, которая указана в разделе **Configuration (Конфигурация) > Client (Клиент) > Settings (Настройки)**. Примечание Для съемки стоп-кадров Axis Camera Station Pro обычно использует видеопоток, то есть снимок имеет то же разрешение, что и видеопоток. Однако для панорамных камер и камер "рыбий глаз", которые используют сшивку или компенсацию оптических искажений, стоп-кадр создается прямо с экрана на стороне клиента. Это может привести к снижению разрешения, особенно при съемке с нескольких камер, когда каждое изображение на экране выглядит меньше.
Добавить стоп-кадр в экспорт	Чтобы добавить стоп-кадр в список экспорта на вкладке Export (Экспорт), 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 PTZ-камер и для камер, у которых в веб-интерфейсе камеры активирована функция цифрового PTZ-управления. 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. Другой вариант: для увеличения нажмите CTRL и (+), для уменьшения нажмите CTRL и (-).
Изменение размера области наблюдения	Чтобы увеличить выбранный участок изображения, нарисуйте прямоугольник вокруг масштабируемой области. Чтобы уменьшить участок, воспользуйтесь колесиком мыши. Чтобы увеличить участок вблизи центра изображения, начертите прямоугольник правой кнопкой мыши.
Панорамирование и наклон	Щелкните изображение, где требуется выполнить направление камеры. Для непрерывного панорамирования и наклона при просмотре изображения в реальном времени установите

	курсор в центре изображения, чтобы вывести на экран навигационную стрелку. Затем нажмите кнопку мыши, удерживая ее в нажатом положении, чтобы выполнить панорамирование в направлении, указанном навигационной стрелкой. Для более интенсивного панорамирования и наклона изображения нажмите кнопку мыши, удерживая ее в нажатом положении, пока навигационная стрелка не станет длиннее.
Настройка фокуса	Чтобы настроить фокус камеры, щелкните изображение правой кнопкой мыши и выберите **Set focus (Настроить фокус)**. Нажмите **AF**, чтобы сфокусировать камеру автоматически. Для настройки фокуса вручную выберите элементы со стороны **Вблизи** и со стороны **Вдали**. Кнопка **Ближе** смещает фокусировку камеры ближе к камере. Если выбрать **Вдали**, то фокус переместится на дальние объекты.
Область предустановки фокуса	Чтобы добавить или удалить область предустановки фокуса, щелкните изображение правой кнопкой мыши и выберите **Focus recall zone (Область предустановки фокуса)**.
Автослежение Вкл./Выкл.	Чтобы включить или выключить автослежение для PTZ-камеры Axis с настроенной функцией автослежения, щелкните изображение правой кнопкой мыши и выберите **Autotracking on/off (Включить/выключить 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 предустановленное положение, перетащите вид изображения в нужное положение, щелкните правой кнопкой мыши и последовательно выберите пункты **Presets > Add preset (Предустановки > Добавить предустановку)**.

Абсолютное перемещение PTZ	Доступно для устройств ONVIF, поддерживающих абсолютное позиционирование PTZ. Используется для перемещения камеры в точные координаты с целью повторяемого позиционирования. Для использования функции абсолютного перемещения PTZ щелкните правой кнопкой мыши по камере в режиме живого просмотра и выберите **Absolute PTZ Move (Абсолютное перемещение PTZ)**. Выберите систему координат: **Generic (Стандартная)** — 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

Являясь администратором, вы можете отключить механический 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 мультиэкран и нажмите значок  .
	Указывает текущую запись в живом просмотре.
	Указывает, что обнаружено движение.

	Для воспроизведения текущей записи наведите курсор на изображение и щелкните **Instant replay (Мгновенный повтор)**. Откроется вкладка Recordings (Записи) и воспроизведутся последние 5 секунд записи.
ЗАПИСЬ	Чтобы вручную выполнить запись из режима живого просмотра, наведите на изображение курсор и нажмите **REC (Запись)**. Кнопка становится желтой, что указывает на то, что запись выполняется. Чтобы остановить запись, нажмите **REC** еще раз.

О настройке параметров записи в ручном режиме (разрешение, сжатие и частота кадров) см. раздел *Способ записи*. Более подробные сведения о записи и воспроизведении можно найти в разделе *Воспроизведение записей*.

Примечание

Администраторы могут отключить функцию записи вручную 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 55*.

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 126*.

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 режиме мультиэкрана можно просматривать виды с камер, последовательности, веб-страницы, карты и другие виды.

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 «Живой просмотр» нажмите значок  .
2. Выберите пункт **Новый мультиэкран**.
3. Введите название для разделенного вида.
4. В раскрывающемся меню **Template (Шаблон)** выберите нужный шаблон.
5. Перетащите один или несколько видов, аудиозон или камер на сетку.
6. Нажмите кнопку **Save view (Сохранить вид)**, чтобы сохранить мультиэкранный вид на текущем сервере.

Установить точку наблюдения	Чтобы задать рамку главной области наблюдения, щелкните по ней правой кнопкой мыши и выберите пункт **Set hotspot (Задать главную область наблюдения)**. Если щелкнуть другой рамку она откроется в главной области наблюдения. Главные области наблюдения особенно полезно выделять, когда используется мультиэкранный вид с разными по размеру рамками, среди которых одна большая и несколько маленьких. Главной областью наблюдения обычно является самая большая рамка.
Профиль потока	Чтобы задать профиль потока для данной камеры, щелкните правой кнопкой мыши камеру в ячейке мультиэкрана и выберите **Stream profile (Профиль потока)**, см. *Профили потоков*.

Добавить разделенный вид

Панель управления дверью в мультиэкранном режиме

Если дверь была вами настроена, вы можете помогать владельцам карт и отслеживать состояние двери и последние операции в мультиэкранном режиме.

1. Добавьте дверь. См. *Добавление двери, on page 156*.
2. Добавьте панель управления дверью к мультиэкранному виду, см. *Мультиэкранный режим, on page 18*.

Панель управления	Чтобы просмотреть подробную информацию о двери, ее состоянию и состоянию блокировки, откройте вкладку **Dashboard (Панель управления)**. На вкладке панели управления отображаются следующие сведения: • События контроля доступа с информацией о владельце карты (включая, например, его фотографию), когда владелец карты проводит картой перед считывателем. • 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), щелкните значок .
Доступ	Чтобы предоставить доступ вручную, нажмите кнопку **Access (Доступ)**. После чего происходит разблокировка двери таким же образом, как если бы кто-либо предоставил свои реквизиты для входа (обычно это означает, что она автоматически блокируется по истечении заданного времени).
Зафиксировать	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

Панель аналитики AXIS Data Insights Dashboard представляет аналитические данные, полученные от ваших 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 184*.
2. На вкладке Live view (Живой просмотр) нажмите значок +.
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	Отображение данных из сценария подсчета количества пересечений 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

Можно использовать интерфейсы оповещения, чтобы делать объявления в режиме реального времени, вызывать абонентов или воспроизводить аудиофайлы с аудиоустройств. Для этого требуется интеграция с AXIS Audio Manager Pro. Для получения дополнительной информации см. раздел *Настройка AXIS Audio Manager Pro, on page 179*.

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 полностью соответствуют аудиозонам, 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 переключения между видами.

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 «Живой просмотр» нажмите значок +.
2. Выберите **Новая последовательность**.
3. Введите название последовательности.
4. Перетащите один или несколько видов или камер в последовательность видов.
5. Расположите виды в том порядке, который вам требуется для последовательности.
6. Для каждого вида можно также задать свою длительность показа.
7. Для камер с функциями PTZ) выберите **предустановленные позиции PTZ** из раскрывающегося списка. См. *Предварительные установки PTZ*.
8. Нажмите **Save view (Сохранить вид)**, чтобы сохранить соответствующую последовательность на текущем сервере.

Длительность пребывания	Длительность показа представляет собой время в секундах, в течение которого отображается данный вид, после чего происходит переключение на следующий вид. Этот параметр можно задать отдельно для каждого вида.

Добавить последовательность

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 — это импортированное изображение, где вы можете размещать виды с камер, изображения в мультиэкранном режиме, аудиозоны, последовательности, веб-страницы, другие карты, а также 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.

В виде карты доступны также любые кнопки. 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 «Живой просмотр» нажмите значок +.
2. Выберите **Новая карта**.
3. Задайте имя карте
4. Нажмите **Choose image (Выбрать изображение)** и найдите нужный файл карты. Максимальный размер файла 20 Мб; поддерживаются форматы BMP, JPG, PNG, GIF.
5. Перетащите на данную карту виды, камеры, другие устройства и двери.
6. Нажмите значок на карте, чтобы изменить параметры.
7. Нажмите **Add label (Добавить обозначение)**, введите имя обозначения и задайте размер, угол поворота, стиль и цвет обозначения.

Примечание

Одновременно можно также изменять некоторые параметры для нескольких значков и обозначений.

8. Нажмите **Save view (Сохранить вид)**, чтобы сохранить соответствующую карту на текущем сервере.

	Физическое состояние двери, если для двери настроен дверной монитор.
	физическое состояние замка, если для двери не настроен дверной монитор.
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	Этот параметр доступен только для камер и других устройств. Включите этот параметр, если на карте должна отображаться зона охвата устройства. Можно изменить **диапазон**, **ширину**, **направление** и цвет зоны охвата. Включите функцию **Flash (Мигание)**, если требуется, чтобы зона охвата мигала, когда камера ведет запись по обнаружению движения или по другим правилам действий. На странице настроек клиента можно глобально отключить мигание зон охвата для всех устройств, см. раздел *Настройки клиента, on page 123*.
Удалить	Нажмите значок , чтобы удалить значок с карты.

Добавление карты

Запуск трансляции звука с карты

Веб-страница

Вид «Веб-страница» отображает страницу из Интернета. Веб-страницу можно добавить, к примеру, в мультиэкранный вид или в последовательность.

Чтобы добавить веб-страницу:

1. На вкладке «Живой просмотр» нажмите значок +.
2. Выберите пункт **New webpage (Новая веб-страница)**.
3. Введите имя для веб-страницы.
4. Введите полный URL-адрес для данной 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

Вкладка «Записи» служит для поиска, воспроизведения и экспорта записей. На этой вкладке содержится, а также имеются две панели, на которых можно выполнять поиск видов, изображений, инструментов воспроизведения и камер подключенных серверов, сгруппированных по имени сервера, см. раздел *Просмотр в реальном времени*.

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

О том, как изменить способ записи и ее настройки, включая разрешение, сжатие и частоту кадров, см. в разделе *Способ записи*.

Примечание

Записи из AXIS Camera Station Pro невозможно удалять вручную. Чтобы удалить старые записи, необходимо изменить срок их хранения в разделе **Configuration > Storage > Selection (Конфигурация > Устройство хранения > 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

Используйте шкалу времени для навигации по воспроизведению и определения времени выполнения записи. Красная линия на шкале времени показывает, что запись выполнена при обнаружении движения. Линия синего цвета на шкале времени показывает, что запись была активирована правилом действия. 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. В записи перемещайте шкалу времени (прокручивая), чтобы получить обзор содержимого и найти конкретные случаи.

Поиск записей

	Щелкните, чтобы выбрать дату и время на шкале времени.
	Используйте фильтр, чтобы настроить, какой тип записей будет отображаться на шкале времени.
	Используйте для поиска сохраненных закладок, см. раздел *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 для поиска записей, см. раздел *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 вверх или вниз, чтобы увеличить или уменьшить масштаб изображения, переместите вид, чтобы увидеть другие части изображения. Чтобы увеличить какую-либо часть, поместите курсор на нужный участок и выполните прокрутку для масштабирования.

Закладки

Примечание

- Вы не можете удалить заблокированную запись, пока не разблокируете ее вручную.
- Система удаляет заблокированные записи, когда вы удаляете соответствующую камеру из приложения AXIS Camera Station Pro.

	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 закладки, ее описание, а также разблокируйте или заблокируйте данную запись.
	Удалите закладку. Чтобы удалить несколько закладок, выберите их, нажмите и удерживайте клавишу CTRL или SHIFT.
Запретить удаление записи	Выберите или снимите флажок, чтобы заблокировать или разблокировать запись.

Добавление закладок

1. Перейти к записи.
2. На шкале времени камеры можно увеличить, уменьшить масштаб или установить соответствующий маркер в нужном местоположении.
3. Нажмите .
4. Введите имя и описание закладки. Чтобы можно было легко найти и опознать закладку, используйте в описании ключевые слова.
5. Выберите **Запретить удаление записи**, чтобы заблокировать запись.

Примечание

Заблокированную запись удалить невозможно. Чтобы разблокировать видеозапись, отключите данный параметр или удалите закладку.

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

Категории событий

Присвойте категории записям, чтобы облегчить поиск событий определенных типов, таких как нападение или остановка движения:

1. На вкладке "Запись" найдите запись, которой нужно назначить категорию событий.
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**.

Если присвоить событию категорию, оно станет оранжевым на временной шкале, а выбранные категории появятся на миниатюре для предварительного просмотра записи.

Для получения дополнительных сведений см. *Настроить категории событий, on page 92*.

Экспорт записей

На вкладке **Export (Экспорт)** может выполняться экспорт записей в локальное или сетевое хранилище. Здесь также содержится соответствующая информацию и можно выполнить предварительный просмотр записи. Имеется также можно экспортировать несколько файлов одновременно, при этом может выбираться их формат — .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 приложении AXIS File Player можно изменять скорость воспроизведения записей в форматах .mp4 and .mkv, однако не в формате ASF.

Прежде чем начать, убедитесь, что у вас есть разрешение на выполнение экспорта. См. *Разрешение на экспорт для пользователей, on page 31*.

Экспорт записей

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 кнопку **Export (Экспорт)**.
4. Выберите папку, в которую нужно экспортировать записи.
5. Нажмите кнопку **OK**. Задача экспорта записей отобразится на вкладке **Tasks (Задачи)**.

Папка экспорта содержит следующие элементы:

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

Экспорт записей

Вкладка **Recordings (Записи)**	
	Для выбора нескольких записей, щелкните и переместите маркеры выбора для задания местоположения начала и конца.
	Чтобы выполнить экспорт записей между маркерами выбора, щелкните .
Добавить записи	Для экспорта одной записи щелкните ее правой кнопкой мыши и выберите **Export > Add recordings (Экспорт > Добавление в список экспорта)**.
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)**.

Вкладка **Recordings (Записи)**	
Удалить записи	Для удаления записи из списка экспорта щелкните ее правой кнопкой мыши и выберите **Export > Remove recordings (Экспорт > 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. *Изменение записей (редакция) перед экспортом, on page 31*.
	Для изменения примечания к записи выберите запись и щелкните  .
	Для удаления записи из списка экспорта выберите ее и щелкните  .
Перейти к экспортированию	Если отображается вкладка **Incident report (Отчет об инцидентах)**, то для перехода на вкладку **Export (Экспорт)** выберите **Switch to export (Перейти к экспорту)**.
Предпочтительный профиль потока	Выберите профиль потока в поле **Preferred stream profile (Предпочтительный профиль потока)**.
Предварительный просмотр	Для предварительного просмотра записи щелкните эту запись в списке экспорта, чтобы воспроизвести ее. Несколько записей можно просмотреть, только если они получены с одной камеры.
Сохранить	Если нужно сохранить список экспорта в файл, нажмите кнопку **Save (Сохранить)**.
Загрузить	Если требуется включить ранее сохраненный список экспорта, щелкните **Load (Загрузить)**.
Название экспортируемого содержимого	Вы можете задать пользовательское имя для экспортируемой папки и файлов или оставить поле пустым, чтобы использовать стандартную схему именования в AXIS Camera Station Pro.

Вкладка **Export (Экспорт)**	
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	Для добавления снимка, перетащите шкалу времени в режиме предварительного просмотра в определенное место. Щелкните правой кнопкой мыши предварительный просмотр и выберите **Add snapshot (Добавить моментальный снимок)**.

Расширенные настройки	
Включая примечания	Чтобы отправить примечания к записям, выберите **Включить примечания**. Примечания будут доступны в виде файла .txt в папке экспорта, а также в виде закладки в данной записи в проигрывателе AXIS File Player.
Include AXIS File Player (Включить AXIS File Player)	Чтобы отправить AXIS File Player вместе с экспортируемыми записями, нажмите **Включить AXIS File Player**.
Create playlist (.asx) (Создать список воспроизведения (.asx))	Чтобы создать список воспроизведения в формате .asx для проигрывателя Windows Media Player, выберите **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 параметр доступен только для записей в формате ASF. См. *Воспроизведение и проверка экспортированных записей, on page 32*.
Экспорт в ZIP-файл	Для экспорта в ZIP-файл выберите **Export to Zip file (Экспорт в ZIP-файл)** и задайте пароль для создаваемого ZIP-файла.

Расширенные настройки	
Export format (Формат экспорта)	В раскрывающемся меню **Export format (Формат экспорта)** выберите формат, в который требуется экспортировать записи. Если выбрать формат MP4, звук в формате G.711 или G.726 не будет включен в экспортируемые записи.
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` для использования M-JPEG для формата M-JPEG и использования H.264 для других форматов.

Разрешение на экспорт для пользователей

Чтобы экспортировать записи или создавать отчеты об инцидентах, необходимо иметь соответствующее разрешение. Это разрешение может быть для одного из этих действий или для обоих действий. При выборе на вкладке **Recordings (Записи)** откроется подключенная вкладка экспорта.

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

Изменение записей (редакция) 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. Чтобы отрегулировать размер, перейдите в раздел **Bounding box options > Size (Параметры прямоугольной рамки > Размер)**.
5. Переместите прямоугольную рамку и поместите ее поверх объекта.
6. Перейдите к пункту **Bounding box options > Fill (Параметры прямоугольной рамки > Заполнение)** и установите значение **Pixelated (Пикселизация)** или **Black (Темный)**.
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 окончание, щелкните правой кнопкой мыши элемент, имеющий ромбовидную форму, в последнем ключевом кадре и выберите **Set end (Установить окончание)**. Это приведет к удалению ключевых кадров после конечной точки.

Примечание

В видео можно добавить несколько ограничивающих прямоугольных рамок. Если прямоугольные рамки накладываются друг на друга, то перекрываемая часть заполнится цветом в следующем порядке — от черного к пикселизированному и заканчивая прозрачным.

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. раздел *Размытие движущегося объекта, on page 31*.
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)**. Для выбранных прямоугольных рамок устанавливается значение **Clear (Прозрачный)** и для не выбранных — **Pixelated (Пикселизация)**.

Создать прямоугольники

Чтобы создать прямоугольные рамки из аналитических данных, включите аналитические данные камеры. См. *Профили потоков, on page 55*.

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 закрывают движущийся объект и при необходимости отрегулируйте 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 камеры*.

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 воспроизведутся автоматически.
3. В приложении AXIS File Player щелкните для отображения примечаний в записях.
4. Проверьте цифровую подпись в приложении AXIS File Player для записей с выбранным параметром **Add digital signature (Добавить цифровую подпись)**.
   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, если установлена защита с помощью пароля.
   4.3. Чтобы просмотреть результаты проверки, щелкните **Verify (Проверить)**.

Экспорт отчетов об инцидентах

Экспорт отчетов об инцидентах в локальное или сетевое хранилище может выполняться на вкладке Incident report (Отчет об инцидентах). Здесь вы можете включать записи, моментальные снимки и примечания в свои отчеты об инцидентах.

Прежде чем начать, убедитесь, что у вас есть разрешение на выполнение экспорта. См. *Разрешение на экспорт для пользователей, on page 31*.

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 27*.
3. Щелкните **Switch to incident report (Перейти к отчету об инцидентах)**, чтобы перейти на вкладку отчета об инциденте.
4. Выберите пункт **Create report (Создать отчет)**.
5. Выберите папку, в которую требуется сохранить отчет об инцидентах.
6. Нажмите кнопку **OK**. Задача отчета об инцидентах экспорта отображается на вкладке **Tasks (Задачи)**.

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. *Изменение записей (редакция) перед экспортом, on page 31*.
	Для изменения примечания к записи выберите запись и щелкните  .
	Для удаления записи из списка экспорта выберите ее и щелкните  .
Перейти к отчету об инцидентах	Если открыта вкладка **Export (Экспорт)**, для выполнения изменения перейдите на вкладку **Incident report (Отчет об инцидентах)**, щелкните **Switch to incident report (Перейти к отчету об инцидентах)**.
Предпочтительный профиль потока	Выберите профиль потока в раскрывающемся списке **Preferred stream profile (Предпочтительный профиль потока)**.
Предварительный просмотр	Для предварительного просмотра записи щелкните эту запись в списке экспорта, после чего она начнет воспроизводиться. Несколько записей можно просмотреть, только если они получены с одной камеры.
Сохранить	Если нужно сохранить отчет об инцидентах в файл, нажмите кнопку **Save (Сохранить)**.
Загрузить	Если требуется включить ранее сохраненный отчет об инцидентах, щелкните **Load (Загрузить)**.
Описание	Поле **Description (Описание)** автоматически заполняется предустановленными данными из шаблона Description (Описание). Вы также можете добавить дополнительную информацию, которую требуется включить в отчет об инцидентах.
Категория	Выберите категорию, которой принадлежит отчет.
Reference ID (Ссылочный идентификатор)	**Reference ID (Ссылочный идентификатор)** создается автоматически, и при необходимости его можно изменить вручную. Ссылочный идентификатор является уникальным и указывает конкретный отчет об инцидентах.
Включая примечания	Чтобы включить примечания к записям и моментальные снимки, выберите **Include notes (Включить примечания)**. Примечания будут доступны в виде файла .txt в папке экспорта, а

	также в виде закладки в данной записи в проигрывателе 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` для использования M-JPEG для формата M-JPEG и использования H.264 для других 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	Для добавления снимка, переместите шкалу времени в режиме предварительного просмотра в определенное место. Щелкните правой кнопкой мыши предварительный просмотр и выберите **Add snapshot (Добавить моментальный снимок)**.

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 из раскрывающегося списка **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 курсор на изображение, передающееся с камеры в реальном времени.
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 функцию умного поиска 1, чтобы найти компоненты записи, движущиеся в определенной области изображения.

Чтобы увеличить скорость поиска, выберите **Include analytics data (Включить данные аналитики)** в профили потоков. 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 **фильтр Short-lived objects (Кратковременно присутствующие объекты)** и **фильтр Small objects (Мелкие объекты)**, чтобы отфильтровать нежелательные результаты.
5. Выберите время начала, окончания и дату поиска. Чтобы выбрать диапазон дат, используйте клавишу SHIFT.
6. Нажмите **Поиск**.

Результаты поиска отобразятся на вкладке **Results (Результаты)**. Если требуется экспортировать записи, щелкните правой кнопкой мыши соответствующие один или несколько результатов.

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.

При включении функции умного поиска 2 для камеры Axis, приложение AXIS Camera Station Pro начинает записывать метаданные с этой камеры. В функции умного поиска 2 используются метаданные для классификации объектов в сцене, а также предоставляется возможность использовать фильтры для поиска интересных моментов.

Примечание

Для использования функции умного поиска 2 требуется следующее:

- Потоковая передача метаданных аналитики по протоколу RTSP.
- AXIS Video Content Stream на камерах с операционной системой AXIS OS версии до 9.60. См. *Установка приложений для камеры, on page 71*.
- Синхронизация времени между сервером AXIS Camera Station Pro и камерами.

Примечание

Общие рекомендации:

- Мы рекомендуем использовать непрерывную запись. Применение функции обнаружения движения может привести к отсутствию необходимых видео при обнаружении объектов.
- Мы рекомендуем использовать формат H.264, если требуется просматривать записи в результатах поиска.
- Убедитесь, что условия освещения соответствуют техническим характеристикам камеры для выполнения оптимальной классификации цветов. При необходимости используйте дополнительное освещение.

Последовательность операций

1. *Настройка «Умного поиска 2», on page 180*
2. Настройка синхронизации времени между сервером AXIS Camera Station Pro и камерами. См. *Синхронизация времени, on page 75*.
3. Создайте фильтр или загрузите существующий фильтр. См. *Поиск с помощью фильтров, on page 37*.
4. Работа с результатами поиска. См. *Результаты умного поиска, on page 42*.

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 много времени, попробуйте использовать следующие способы ускорения:

- Включите фоновую обработку 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.
- Чтобы сократить объем данных, задайте область, а также направление, размер и продолжительность объекта.

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 из обрезанных изображений людей с низким разрешением и сравнивает их с другими представлениями.Когда два представления похожи, вы получаете совпадение по вашему поиску. Поиск по сходству не использует биометрические данные для идентификации человека, но может, например, распознавать общую форму и цвет одежды человека в определенный момент.
Поиск произвольного текста	Функция поиска произвольного текста позволяет использовать естественный язык для написания поискового запроса (только английский). См. *Поиск произвольного текста, on page 40*.
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 необходимые точки.
Пересечение линии	Для выполнения фильтрации по пересечению линии, щелкните **Line crossing (Пересечение линии)**, выберите камеру и включите параметр **Filter by line crossing on this camera (Фильтрация по пересечению черты на этой камере)**.

	Скорректируйте линию на изображении и добавьте или удалите необходимые точки.
Размер и длительность	Для выполнения фильтрации по размеру и длительности, щелкните **Size and duration (Размер и длительность)**, выберите камеру и включите **Filter by size and duration on this camera (Фильтрация по размеру и длительности на этой камере)**. Задайте минимальную ширину и высоту объекта в процентах от общих размеров изображения. Задайте минимальную длительность в секундах.
Скорость	Для выполнения фильтрации по скорости, щелкните **Speed (Скорость)**, выберите камеру и включите параметр **Filter by speed on this camera (Фильтрация по скорости на этой камере)**. Укажите диапазон скоростей для включения в фильтр. Примечание Фильтр скорости доступен для устройств, которые способны определять скорость, например для радаров и камер.
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 кнопку  , 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, щелкните  , выберите имеющийся 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

Функция поиска произвольного текста позволяет использовать естественный язык для написания поискового запроса.

Примечание

- Для поиска произвольного текста требуется не менее 16 ГБ ОЗУ.
- Для поиска произвольного текста требуется подключение к Интернету.
  - Функция поиска произвольного текста использует подключение к Интернету для загрузки модели ИИ с сайта axis.com (при первой настройке функции и при обновлении модели).
  - 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.
  - Функция поиска произвольного текста всю обработку выполняет локально на вашем сервере, **не** подключаясь к Интернету для отправки видео, изображений и текстовых 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.

Чтобы выполнить поиск произвольного текста:

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}`

Подробно опишите объект, используя несколько ключевых слов. 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 разговаривали с человеком, не являющимся специалистом в сфере видеонаблюдения. Например:

Запрос	Комментарий
Желтый пикап, припаркованный у дерева	Правильно
Автомобиль без водителя, номерной знак: CHY67F, класс: пикап, цвет: желтый, местоположение: рядом с толстым 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 на магазине: “Танцующим медведям вход воспрещен”
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 оценки каждого поискового запроса система использует модель обработки текстов на естественных языках, а также настраиваемый список запрещенных поисковых категорий и слов.

Чтобы разблокировать или заблокировать слово, отправьте нашей команде анонимный отзыв через пользовательский интерфейс функции “Умный поиск”.

Примечание

- Функция поиска произвольного текста поддерживает только английский язык.
- Функция поиска произвольного текста понимает статические изображения. Получить с помощью функции поиска произвольного текста хороший результат для таких действий, как падение, бег или кража, может быть сложно, поскольку требуются больше контекста.
- Функция поиска произвольного текста использует обрезанные изображения, т. е. они могут не включать окружающее пространство. Результаты могут быть менее точными при использовании таких ключевых слов, как город, городской, парк, сад, озеро или пляж.
- Подробные сведения о функции поиска произвольного текста, включая ограничения и рекомендации по использованию, см. в техническом обзоре *Функция поиска произвольного текста в AXIS Camera Station Pro*.

Результаты умного поиска

	Чтобы сгруппировать обнаружения, которые, скорее всего, относятся к одному и тому же событию, можно сгруппировать их по интервалам времени. Выберите интервал из раскрывающегося меню  .
Самый последний 	При использовании умного поиска 2 результаты поиска отображаются 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. При установке высокой степени достоверности сомнительные результаты классификации игнорируются.
Столбцы 	Чтобы настроить размер миниатюрных изображений в результатах поиска, нажмите **Columns (Столбцы)** и измените количество столбцов.
Вид Detection (Обнаружение)	Чтобы показать обрезанный вид обнаруженного объекта в виде миниатюрного изображения, выберите вид **Detection (Обнаружение)**.

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.
- Камеры для ношения на теле не поддерживаются.
- Радар может обнаруживать только человека и другое транспортное средство. Включить фоновую классификацию на сервере для радара нельзя.
- Корректная классификация объектов при работе с тепловизионными камерами не гарантируется.
- При использовании функции умного поиска 2 не производится обнаружение движущихся объектов, когда изменяется предустановленное положение PTZ, а также в течение короткого периода перекалибровки после изменения положения.

- 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 представляет собой систему или устройство, генерирующее данные, которые могут использоваться для получения дополнительной информации о том, что произошло в ходе события. Для получения дополнительных сведений см. *Внешние источники данных, on page 75*. Приведем несколько примеров:

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

Чтобы изменить время, в течение которого AXIS Camera Station Pro будет хранить внешние данные, перейдите в раздел **Configuration > Server > Settings > External data (Конфигурация > Сервер > Настройки > 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 задайте дополнительные фильтры. Фильтры зависят от типа источников данных.
5. Введите подходящие ключевые слова в поле поиска. См. *Оптимизация поиска, on page 45*.
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.

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	Контроль доступа — это пример компонента, который производит данные. Используйте этот параметр, если вы хотите включить данные только из этого конкретного компонента. Функция контроля доступа позволяет фильтровать события по дверям, зонам, владельцам карт и типам событий.
Third party (Данные сторонних производителей)	Используйте этот параметр, если вы хотите включить данные сторонних производителей, отличные от настроенных компонентов.

В зависимости от источника данных могут быть получены разные элементы в результатах поиска. Приведем несколько примеров:

Результаты поиска	
Сервер	Сервер, на который отправляются данные события. Отображается только при подключении к нескольким серверам.
Местонахождение	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: Автомобиль.

Чтобы экспортировать результаты поиска в файл PDF или в текстовый файл, щелкните **Download search result (Загрузить результат поиска)**. Можно изменить порядок и ширину столбцов в результатах поиска, чтобы улучшить макет таблицы на выходном файле PDF. 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: – “дверь 1“ и “Дверь открыта силой“

	– “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“
Для фильтрации чисел в пределах столбца используйте символы >, >=, < и <=.	• Поиск по запросы `[Max speed] > 28` возвращает результаты, содержащие число больше 28 в столбце Max speed (Максимальная скорость). • Поиск по запросу `[Average speed] < = 28` возвращает результаты, содержащие число меньше или равное 28 в столбце Average speed (Средняя скорость).
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, содержащие точное совпадение “ABC123“ только в столбце Cardholder (Владелец карты).

Конфигурация

На вкладке «Конфигурация» осуществляется управление и обслуживание подключенных устройств, а также для настройки параметров клиента и серверов. Щелкните + 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 адресами IPv4.
- 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:

- сетевую камеру
- видеокодер с одним или несколькими видеопортами
- дополнительное устройство, не являющееся камерой, например аудиоустройство ввода-вывода, сетевой громкоговоритель или дверной контроллер
- переговорное устройство

Применительно к устройствам можно выполнять следующие действия:

- 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*.
- Изменить настройки профилей потока, связанные с разрешением, форматом и т. д. 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 75*.

Добавить устройства

Примечание

- Зоны просмотра рассматриваются системой как отдельные камеры. Прежде чем использовать область наблюдения, ее надо создать в камере. См. *Использование зон просмотра*.
- Когда вы добавляете устройство, это устройство синхронизирует свое время с сервером AXIS Camera Station Pro.
- Не рекомендуется использовать в имени хоста специальные символы, например å, ä или ö.

1. Поиск устройств, видеопотоков или предварительно записанного видео.
   - *Поиск устройств, on page 49*
   - *Поиск видеопотоков, on page 49*
   - *Поиск предварительно записанных видеозаписей, on page 50*

2. *Добавление устройств, видеопотоков или предварительно записанных видеозаписей, on page 50*

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)	AXIS Camera Station Pro Сервер пытается получить доступ к устройству.
Недоверенный сертификат устройства	AXIS Camera Station Pro не может подтвердить, что сертификат HTTPS на устройстве подписан надежным издателем. 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 может определить, какие учетные данные следует 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.
Установить пароль	Учетная запись и пароль привилегированного пользователя не настроены, или устройство по-прежнему использует пароль по умолчанию. Перейдите по ссылке, чтобы установить пароль для привилегированного пользователя. • Введите свой пароль или щелкните **Generate (Создать)** чтобы получить пароль. Рекомендуется просмотреть сформированный пароль и скопировать его. • Выберите, чтобы использовать этот пароль для всех устройств с состоянием `Set password`.
Модель не поддерживается	AXIS Camera Station Pro не поддерживает данную модель устройства.
Устаревшая прошивка	Встроенное ПО устройства устарело, и вам необходимо обновить его, прежде чем вы сможете добавить устройство.

Неисправное устройство	Параметры устройства, полученные приложением AXIS Camera Station Pro, повреждены.
Установка ориентации по наклону	Щелкните данную ссылку, чтобы в зависимости от того, как установлена камера, выбрать соответствующую ориентацию по наклону: Ceiling (Потолок), Wall (Стена) или Desk (Письменный стол). Отдельные модели камер нуждаются в настройке ориентации по наклону.
Неподдерживаемое устройство стороннего производителя	AXIS Camera Station Pro не поддерживает данное устройство стороннего производителя.
Can only be used with AXIS Companion (Может использоваться только с приложением AXIS Companion)	Данное устройство предназначено только для AXIS Companion.

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. Откройте меню **Конфигурация > Устройства > 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, используемый 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 **OK**.

Поиск видеопотоков

Вы можете добавлять видеопотоки, которые поддерживают следующее:

- 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. Откройте меню **Конфигурация > Устройства > 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

Предварительно записанные видео в формате MKV можно добавить в AXIS Camera Station Pro.

Требования к файлу MKV:

- 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 60*.
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. Откройте меню **Конфигурация > Устройства > Добавить устройства**.
3. Чтобы изменить название устройства, щелкните это название в списке и введите новое.
4. Выберите устройства, видеопотоки или предварительно записанное видео. Нажмите **Добавить**.
5. Укажите, следует ли, по возможности, использовать для устройств имена хостов вместо IP-адресов.
6. Выберите **Quick configuration (Быстрая настройка)**, если требуется настроить основные параметры.
   Если выполняется импорт проекта Site Designer, см. раздел *Импорт проектов Site Designer*.
7. Выберите параметры **Retention time (Время хранения записей)**, **Recording storage (Хранение записей)** и **Recording method (Способ записи)**.

Примечание

Если выбрать параметр хранения записей **Automatic (Автоматически)**, каждой камере будет по возможности назначено хранилище объемом не менее 32 ГБ на диске, отличном от системного. Система автоматически выбирает хранилища с доступным объемом не менее 15 ГБ, затем хранилища,

к которым назначено меньшее количество камер для записи, и, наконец, любые хранилища, уже установленные в AXIS Camera Station Pro.

8. Нажмите **Install (Установить)**. AXIS Camera Station Pro автоматически активирует протокол HTTPS на поддерживающих его устройствах.

Импорт проектов 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, используя код доступа или загруженный файл настройки Site Designer.

Импорт проекта, разработанного в Site Designer, в AXIS Camera Station Pro:

1. Создайте код доступа к проекту своего объекта или загрузите файл проекта.
   1.1. Войдите на страницу *http://sitedesigner.axis.com*, используя учетную запись MyAxis.
   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 имеет подключение к Интернету. Или нажмите **Download settings file (Загрузить файл параметров)**, если сервер не имеет подключения к Интернету.
2. В клиенте AXIS Camera Station Pro перейдите к пункту **Configuration > Devices > Add devices (Конфигурация > Устройства > Добавить устройства)**.
3. Выберите камеры и нажмите **Добавить**.
4. Выберите **Конфигурация Site Designer** и нажмите **Далее**.
5. Выберите **Код доступа** и введите этот код. Или выберите **Choose file (Выбрать файл)** и выполните поиск загруженного файла установки Site Designer.
6. Нажмите **Импорт**. При импорте AXIS Camera Station Pro пытается сопоставить проект Site Designer с выбранными камерами по IP-адресу или названию устройства. Если эта попытка завершилась неудачно, можно выбрать нужную камеру в раскрывающемся меню.
7. Щелкните **Установить**.

AXIS Camera Station Pro выполняет импорт следующих настроек из проекта Site Designer:

	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	✓	✓
Запись с активацией по движению: расписание и профиль записи, включая параметры частоты кадров, разрешения, кодирования видео и сжатия		✓

	Кодеры, видеодекодеры, дверные контроллеры, радар-детекторы и громкоговорители	Камеры, переговорные устройства и устройства серии F/FA
Непрерывная запись: 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 был определен только один из профилей записи или если в проекте Site Designer имеется два одинаковых профиля записи, AXIS Camera Station Pro задает для профиля средний уровень.
- Если в проекте Site Designer были определены оба профиля записи, AXIS Camera Station Pro задает для профиля непрерывной записи средний уровень, а для записи по движению — высокий.
- AXIS Camera Station Pro оптимизирует соотношение сторон. Это означает, что разрешение может отличаться в импортированном проекте и проекте Site Designer.
- AXIS Camera Station Pro Если устройство имеет встроенный микрофон или громкоговоритель, в могут задаваться параметры звука. Чтобы использовать внешнее аудиоустройство, необходимо вручную включить его после установки.
- AXIS Camera Station Pro В настройки звука не применяются к переговорным устройствам, даже если эти настройки в Site Designer отличаются. В переговорных устройствах звук всегда включен 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 49*.

Сведения о поддержке устройств сторонних производителей см. в *последней технической статье*.

AXIS Camera Station Pro поддерживает следующие функции для устройств сторонних производителей в соответствии со стандартами IEC62676-2-31 и IEC62676-2-32:

- 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

- При подсчете общего количества камер, разрешенных лицензией AXIS Camera Station Pro, все зоны просмотра одной сетевой камеры учитываются как одна камера.
- Количество добавляемых камер зависит от лицензии.
- Каждая лицензия на ПО AXIS Camera Station Pro разрешает использовать определенное количество камер.

Чтобы использовать области просмотра в AXIS Camera Station Pro, необходимо сначала включить 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. Порядок активации зон просмотра является различным в зависимости от модели камеры и версии встроенного ПО. Чтобы узнать, где находится та или иная настройка, нажмите **Help (Справка)**.

Замена устройства

Можно заменить устройство, сохранив при этом существующую конфигурацию, а также записи. Количество видеопотоков, настроенных на новой камере, должно совпадать с настройками старой камеры.

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)** для подтверждения успешной замены устройства. Нажмите кнопку **OK**.
7. Если замененное устройство использовало облачное хранилище, перезапустите службу на сервере AXIS Camera Station Pro и включите облачное хранилище для устройства в My Systems. См. *Включение облачного хранилища для отдельных камер*.
8. Проверьте правильность настроек нового устройства, также убедитесь, что устройство работает нормально. 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 к пункту **Configuration > Devices > Cameras (Конфигурация > Устройства > Камеры)** для просмотра списка всех камер, добавленных в систему.

На этой странице можно сделать следующее:

- Щелкните 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. Выполняя это, AXIS Camera Station Pro удаляет все записи, включая заблокированные, связанные с удаленными камерами.

Изменение настроек камеры

Чтобы изменить настройки камеры:

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

Включено	Чтобы предотвратить 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 к пункту **Configuration > Devices > Other devices (Конфигурация > Устройства > Другие устройства)**, чтобы просмотреть список устройств, не поддерживающих возможности видео. В данный список входят дверные контроллеры, звуковые устройства и модули ввода-вывода.

Подробную информацию о поддерживаемых устройствах см. на сайте *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.
- Удалите устройства.

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. Чтобы открыть страницу «Профили потока», откройте меню **Configuration > Devices > Stream profiles (Конфигурация > Устройства > Профили потока)**. На данной странице отображается список всех камер.

В режиме живого просмотра и в настройках видеозаписи 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

Для профиля потока установлено значение **Automatic (Автоматически)** в режиме живого видео и записи по умолчанию, что означает, что профиль потока автоматически изменяется на **High (Высокий)**, **Medium (Средний)** или **Low (Низкий)** в зависимости от доступного размера видеопотока.

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. Этот параметр доступен 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 видеокамер поддерживают кодеки **H.264** и **M-JPEG**. Кодек H.264 требует меньшей пропускной способности сети и объема дискового пространства по сравнению с M-JPEG. Некоторые видеокамеры также поддерживают **H.265**, обеспечивающий несколько более высокую степень сжатия, но требующий увеличенных вычислительных ресурсов. Камеры последнего поколения поддерживают кодек AV1, обеспечивающий эффективное сжатие и ряд новых функций, в том числе включаемые и отключаемые накладки. Дополнительные сведения 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, характеристик 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 5 камер используют один и тот же источник аудио, камера-источник может быть перегружена и работать менее эффективно.

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.
		Выкл.	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)**. Профиль оптимизации хранения использует продвинутые алгоритмы сжатия для дополнительной экономии места по сравнению со стандартным профилем Zipstream. Этот профиль позволяет еще сильнее снизить битрейт даже в динамичных сценах с большим количеством движения. • Формат ASF не поддерживает B-кадры, которые используются этой функцией. • Функция не влияет на видео, записанное на видеорегистраторы серии AXIS S30. • Для 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:	включать передачу звука с микрофона для одного или двух видеопотоков. звук можно включить для живого просмотра и видеозаписей, только для живого просмотра или только для видеозаписей.

При подключении к AXIS Audio Manager Pro можно выбирать аудиоустройства с сервера AXIS Audio Manager Pro как связанные аудиоустройства для камеры. Для получения дополнительной информации см. раздел *Настройка AXIS Audio Manager Pro, on page 179*.

Расширенный набор

Включить данные аналитики	Чтобы разрешить сбор данных для функции умного поиска при потоковой передаче видео, выберите **Include analytics data (Включить данные аналитики)**. Этот параметр доступен только для устройств Axis, которые поддерживают функцию работы с аналитическими данными. Сбор данных для *Умный поиск 1*может замедлять передачу видеопотока при просмотре живого видео.
Использовать FFmpeg	Для улучшения совместимости с устройствами сторонних производителей выберите **Use FFmpeg (Использовать FFmpeg)**, чтобы разрешить потоковую передачу в формате FFmpeg. Этот параметр доступен только для устройств сторонних производителей.

Показать индикаторы объектов функции автоматического слежения с помощью PTZ-камеры	Чтобы на экране живого просмотра отображались индикаторы объектов, обнаруживаемых PTZ-камерой, выберите **Show PTZ autotracking object indicators (Показывать индикаторы объектов функции автослежения с помощью PTZ)** и задайте время буфера видеопотока (можно установить значение до 2000 мс). Этот параметр доступен только для PTZ-камеры Axis с функцией автоматического слежения с помощью PTZ-камеры (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 включайте конфиденциальную информацию в пользовательские настройки.

Чтобы **задать индивидуальные настройки профиля** для разрешения, частоты кадров, сжатия, видеоформата и звука, выберите камеру, которую требуется настроить. Можно настроить сразу несколько камер одной модели с одинаковыми возможностями настройки. См. *Параметры конфигурации*.

Порядок **индивидуальной настройки параметров профиля для записей** см. в разделе *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

В режиме живого просмотра или записи можно использовать аудиосигнал с других устройств (не с камеры или с дополнительного устройства) с видеосигналом от 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 звук для просмотра в режиме реального времени или для 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 в настройках изображения сразу же начинают действовать.

Чтобы настроить параметры изображения:

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

Настройки 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. Регулировка баланса белого позволяет получать изображения одинакового цвета независимо от цветовой температуры источника освещения. При выборе варианта **Автоматически** или **Авто** камера сама идентифицирует источник света и автоматически компенсирует его цветность. Если результат неудовлетворителен, выберите вручную вариант, соответствующий источнику 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) Если в кадре присутствует яркое пятно света (например, лампа), из-за которого остальные части изображения кажутся слишком темными, включите данный параметр.

Dynamic contrast (wide dynamic range) (Динамическая контрастность, широкий динамический диапазон). Включите данный параметр, чтобы использовать широкий динамический диапазон и оптимизировать экспозицию при наличии значительного контраста между освещенными и затемненными участками изображения. Динамический контраст регулируется движком. Динамический контраст рекомендуется включать при наличии интенсивной фоновой подсветки. При низкой освещенности динамический контраст следует отключать.

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.

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

Панорамирование, наклон и зум (PTZ) – это способность камеры панорамировать (сдвигать влево-вправо), наклонять (сдвигать вверх-вниз), увеличивать и уменьшать изображение.

Откройте меню **Конфигурация > Устройства > Предустановки PTZ**, чтобы увидеть список камер, которые поддерживают PTZ-управление. 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);
- фиксированные камеры, у которых включено цифровое PTZ-управление.

Цифровое PTZ-управление активируется с помощью встроенной страницы конфигурации камеры. Подробнее см. руководство по эксплуатации камеры. Чтобы открыть страницу конфигурации, перейдите на страницу управления устройствами, выберите камеру и перейдите по ссылке в столбце Address (Адрес).

Предустановленные положения для PTZ можно настроить в AXIS Camera Station Pro, а также на странице конфигурации камеры. Рекомендуется настраивать предустановленные положения для 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. PTZ-перемещения записываются, и их можно видеть в окне живого просмотра.
- Если предустановленное положение для PTZ настроено в AXIS Camera Station Pro, то можно просматривать полный видеопоток с камеры. PTZ-перемещения при этом не записываются, и их нельзя видеть в окне живого просмотра.

Примечание

Если в камере активирована постановка запросов управления в очередь, PTZ-управление использовать невозможно. Сведения о том, что такое очередность управления и как она включается-отключается, изложены в руководстве по эксплуатации 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 **OK**.

Чтобы удалить предустановку, выберите предустановку и нажмите **Удалить**. Предустановленное положение будет удалено из AXIS Camera Station Pro и из камеры.

Управление устройствами

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

Чтобы открыть страницу «Управление устройствами», выберите в меню **Конфигурация > Устройства > Управление**.

Если в разделе *Настройки обновления встроенного ПО, on page 129* настроена автоматическая проверка на наличие новых версий встроенного ПО, при наличии новых версий встроенного ПО, доступных для устройств, отображается ссылка. Перейдите по этой ссылке для обновления версий встроенного ПО. См. *обновлять встроенное программное обеспечение;.*

Если в разделе *Обновить AXIS Camera Station Pro, on page 136* настроена автоматическая проверка на наличие новых версий программного обеспечения, при наличии новой версии AXIS Camera Station Pro отображается ссылка. Перейдите по этой ссылке, чтобы установить новую версию AXIS Camera Station Pro.

Откроется список устройств, добавленных в AXIS Camera Station Pro. 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. Чтобы изменить порядок столбцов, потяните столбец за заголовок и перетащите.

Список устройств содержит следующую информацию:

- **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.
- **MAC-адрес:** MAC-адрес устройства.
- **Статус:** Состояние устройства.
  - **OK:** стандартное состояние для устройства, с которым установлена связь.
  - **Maintenance (Обслуживание).** Ведется техническое обслуживание, и устройство временно недоступно.
  - **Недоступно:** не удается установить связь с устройством.
  - **Not accessible over set hostname (Недоступно с использованием заданного имени хоста).** Не удается установить соединение с устройством через указанное имя хоста.
  - **Сервер недоступен^** не удается установить соединение с сервером, к которому подключено устройство.
  - **Введите пароль:** нет подключения к устройству, пока не будут введены действующие учетные данные. Перейдите по ссылке, чтобы указать действительные учетные данные пользователя. Если устройство поддерживает зашифрованные соединения, пароль отправляется зашифрованным по умолчанию.
  - **Set password (Установите пароль):** Учетная запись и пароль привилегированного пользователя не настроены, или устройство по-прежнему использует пароль по умолчанию. Перейдите по ссылке, чтобы установить пароль для привилегированного пользователя.
    - Введите свой пароль или нажмите **Generate (Создать)**, чтобы автоматически создать пароль длиной, которая допустима на устройстве. Рекомендуется просмотреть автоматически сформированный пароль и скопировать его.
    - Выберите, чтобы использовать этот пароль для всех устройств с состоянием `Set password`.
    - Выберите **Enable HTTPS (Включить HTTPS)**, чтобы активировать протокол HTTPS, если устройство его поддерживает.
  - **Тип пароля: без шифрования:** соединение с устройством не установлено, поскольку ранее устройство подключалось с использованием зашифрованного пароля. Из соображений безопасности AXIS Camera Station Pro не позволяет использовать незашифрованные

пароли для устройств, если ранее для них использовались зашифрованные пароли. Для устройств, поддерживающих шифрование, тип соединения настраивается на странице конфигурации устройства.

- **Certificate error (Ошибка сертификата).** Произошла ошибка, связанная с сертификатом устройства.
- **Certificate about to expire (Срок действия сертификата заканчивается).** Срок действия сертификата устройства истекает.
- **Certificate has expired (Срок действия сертификата истек).** Истек срок действия сертификата устройства.
- **HTTPS certificate not trusted (Недоверенный сертификат HTTPS).** Сертификат HTTPS на устройстве не является доверенным для AXIS Camera Station Pro. Перейдите по ссылке, чтобы выдать новый сертификат HTTPS.
- **HTTP failed (Не удалось применить HTTP).** не удается установить связь с устройством по протоколу HTTP.
- **HTTPS failed (Не удалось применить HTTPS).** Не удается установить связь с устройством по протоколу HTTPS.
- **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:** 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 74*.
- **Имя хоста:** Имя хоста устройства, если оно имеется. Перейдите по ссылке, чтобы открыть страницу конфигурации устройства. Имя хоста отображается в виде полностью определенного имени домена. См. *Вкладка конфигурации устройства, on page 74*.
- **Производитель:** производитель устройства.
- **Модель:** модель устройства.
- **Встроенное ПО:** текущая версия встроенного ПО устройства.
- **DHCP:** если устройство подключено к серверу, использующему DHCP.
- **HTTPS.** Состояние HTTPS устройства. Сведения о состоянии HTTPS см. в *Безопасность, on page 72*.
- **IEEE 802.1X.** Состояние IEEE 802.1X устройства. Сведения о состоянии IEEE 802.1X см. в *Безопасность, on page 72*.
- **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. *Управление пользователями*.
- Обновить встроенное ПО на устройствах. См. *обновлять встроенное программное обеспечение;*.
- Установить дату и время на устройствах. См. *Установите время и дату*.
- Перезапустить устройства.
- Произвести сброс устройств, то есть восстановить заданные по умолчанию заводские настройки большинства параметров, включая пароль. Не сбрасываются значения следующих параметров: загруженные приложения для камер, протокол загрузки (DHCP или статический), статический IP-адрес, заданный по умолчанию маршрутизатор, маска подсети, системное время.

Примечание

- Во избежание несанкционированного доступа настоятельно рекомендуется задать пароль после сброса параметров устройства.
- 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 перезапустите службу на сервере AXIS Camera Station Pro и включите облачное хранилище для устройства в My Systems. См. *Включение облачного хранилища для отдельных камер*.
- Установить на устройства приложение для камеры. См. *Установка приложений для камеры*.
- Перезагрузить устройства, если их параметры были изменены на странице конфигурации устройства.
- Задать конфигурацию устройств. См. *Настроить устройства*.
- Управлять пользователями. См. *Управление пользователями*.
- Управлять сертификатами. См. *Безопасность, on page 72*.
- Собирать данные с устройств. См. *Сбор данных об устройствах*.
- Выберите, чтобы использовать IP-адрес или имя хоста. См. *Подключение, on page 73*.
- Добавить ярлыки к устройствам. См. *Теги*.
- Ввести учетные данные для устройства. Щелкните устройство правой кнопкой мыши и выберите **Дополнительно > Ввести учетные данные для устройства**, чтобы ввести пароль для данного устройства.
- Перейти на вкладку конфигурации устройства и настроить устройство. См. *Вкладка конфигурации устройства, on page 74*.

Назначение IP-адресов

AXIS Camera Station Pro может назначать IP-адреса нескольким устройствам. Новые IP-адреса могут быть получены автоматически от сервера DHCP или они могут быть взяты 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 выберете одно устройство для назначения IP-адреса, нажмите **Дополнительно**, чтобы открыть страницу «Назначить IP-адрес».
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 «Текущий IP-адрес» отображается текущий IP-адрес, маска подсети и маршрутизатор по умолчанию.
   - Измените параметры в разделе «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 74*.

- Сведения о настройке устройств см. в разделе *Способы настройки*.
- Сведения о том, как создать файл конфигурации, см. в разделе *Создание файла конфигурации*.
- Сведения о том, какие настройки можно скопировать, см. в разделе *Параметры конфигурации*.

Способы настройки

Существуют разные способы настройки устройств. Система управления устройствами AXIS Device Management будет пытаться сконфигурировать все устройства в соответствии с выбранным способом. См. *Настроить устройства*.

Использование конфигурации выбранного устройства

Примечание

Этот способ доступен только для настройки одного устройства на основе существующих настроек или их части.

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Щелкните правой кнопкой мыши одно устройство и выберите **Настроить устройства > Настроить**.
3. Выберите параметры, которые нужно применить. См. *Параметры конфигурации, on page 66*.
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 **Настроить устройства > 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 параметры, которые нужно применить. См. *Параметры конфигурации, on page 66*.
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. Созданный на основе настроек выбранного устройства файл конфигурации можно применять к устройствам других моделей или с другими версиями встроенного ПО, даже если некоторые параметры существуют не на всех устройствах.

Если некоторые параметры не существуют или их нельзя применить, то задача получит статус «Ошибка», который отобразится на вкладке «Задачи» в нижней части окна клиентского ПО AXIS Camera Station Pro. Чтобы просмотреть информацию о параметрах, применить которые оказалось невозможно, щелкните по задаче правой кнопкой и выберите Показать.

Примечание

Этот способ предназначен только для опытных пользователей.

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Щелкните устройства правой кнопкой мыши и выберите **Настроить устройства > Настроить**.
3. Для перехода к файлу конфигурации нажмите **Файл конфигурации**. О том, как создать файл конфигурации, см. в разделе *Создание файла конфигурации, on page 66*.
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. Эти настройки можно впоследствии применить для других устройств. Сведения о том, как использовать файл конфигурации, см. в разделе *Способы настройки*.

Отображаемые параметры — это настройки устройств, к которым можно получить доступ с помощью системы управления устройствами 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 встроенных устройств контролируют их работу. Общая информация о параметрах содержится в руководстве пользователя, которое можно найти на сайте *www.axis.com*

Примечание

- К настройке параметров допускаются только опытные пользователи.
- Не все параметры устройства доступны на странице управления устройствами AXIS Device Management.

В некоторые текстовые поля можно вставлять переменные. Переменные заменяются текстом, прежде чем они будут применены к устройству. Чтобы вставить переменную, щелкните правой кнопкой мыши текстовое поле и выберите:

- **Введите серийный номер устройства:** эта переменная будет заменена серийным номером устройства, к которому применяется файл конфигурации.
- **Введите название устройства:** эта переменная будет заменена названием устройства, которое используется при применении файла конфигурации. Название устройства можно найти в столбце «Название» на странице управления устройствами. Чтобы переименовать устройство, перейдите на страницу «Камеры» или «Другие устройства».
- **Введите имя сервера:** эта переменная будет заменена на имя сервера, который используется при применении файла конфигурации. Имя сервера можно найти в столбце «Сервер» на странице управления устройствами. Чтобы переименовать сервер, используйте приложение AXIS Camera Station Pro Service Control.
- **Введите часовой пояс сервера:** эта переменная будет заменена на часовой пояс POSIX для сервера, который используется при применении файла конфигурации. Переменную можно использовать с параметром часового пояса POSIX для установки правильного часового пояса всех устройств в сети с серверами 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

- **Профили потока.** Профиль потока — это заранее настроенный профиль конфигурации живого просмотра с заданными параметрами кодирования видео, изображения и звука. Профили потока можно переносить с одного устройства на другое.
- **Окна детектора движения.** Окна детектора движения служат для настройки определенных зон в области наблюдения 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.

Управление пользователями

Выберите в меню **Конфигурация > Устройства > Управление**; при этом откроется страница «Управление устройствами», на которой предусмотрено управление пользователями устройств.

Когда вы задаете пароль или удаляете пользователей для нескольких устройств, некоторые пользователи могут быть отмечены значком  . Это говорит о том, что они есть не на всех устройствах. Каждый пользователь упоминается только один раз, даже если на разных устройствах он имеет разные роли.

Примечание

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

Установить 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. На

устройствах с более старыми версиями встроенного ПО пароли рекомендуется задавать отдельно на каждом устройстве.

- 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 назначить пароль пользователям 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 свой пароль или нажмите **Generate (Создать)**, чтобы создать надежный пароль.
5. Нажмите **OK**.

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 «Установка пароля».
4. Выберите права доступа пользователя в раскрывающемся списке для поля **Роль**:
   - **Администратор:** неограниченный доступ к устройству.
   - **Оператор:** доступ к видеопотоку, к событиям и ко всем параметрам, кроме системных.
   - **Наблюдатель:** доступ к видеопотоку.
5. Чтобы пользователь мог управлять панорамированием, наклоном и зумом в режиме живого просмотра, установите флажок **Включить PTZ-управление**.
6. Нажмите **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 надо удалить из раскрывающегося списка для поля **Пользователь**.
4. Нажмите **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. Чтобы найти в списке конкретных пользователей, воспользуйтесь полем **Ввести данные для поиска**.

обновлять встроенное программное обеспечение;

Встроенное ПО - это программное обеспечение, которое определяет функциональность продукта Axis. Использование актуальной версии встроенного ПО гарантирует поддержку новейших функций и усовершенствований.

Новую версию встроенного ПО можно загрузить с помощью AXIS Camera Station Pro или импортировать из файла на жестком диске или карте памяти. Версии встроенного ПО, которые доступны для скачивания, отображаются со словом **(Загрузить)** 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:

- **Стандарт:** Обновление до выбранной версии встроенного ПО и сохранение существующих значений параметров.
- **Factory default (Заводские настройки по умолчанию)** Обновление до выбранной версии встроенного ПО с последующим сбросом всех настроек заводским установкам по умолчанию.

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. Увидев сообщение «Устройство недоступно для обновления встроенного ПО», нажмите **Да**, чтобы продолжить. Если вы подтвердили информацию и не хотите, чтобы такое сообщение появлялось в будущем, выберите **Больше не показывать это сообщение**, затем нажмите **Да**.
5. В диалоговом окне Upgrade firmware (Обновление встроенного ПО) приводится модель устройства, количество устройств каждой модели, существующая версия встроенного ПО, доступные версии встроенного ПО для обновления и тип обновления. Когда появляются для скачивания новые версии встроенного ПО, по умолчанию будут выбраны все устройства в списке и для каждого устройства будет предложена свежая 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, которых требуется обновить, а также 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*.

Установите время и дату

Настройки даты и времени ваших устройств Axis можно синхронизировать со временем на сервере или с NTP-сервером, либо можно задавать их вручную.

Установка даты и времени на устройствах

1. Выберите в меню **Конфигурация > Устройства > Управление**.
2. Выберите устройство и щелкните значок или щелкните правой кнопкой мыши и выберите **Set date and time (Задать дату и время)**.
3. Элемент экрана **Время на устройстве** показывает текущую дату и время для устройства Axis. Если выбрать несколько устройств, то элемент экрана **Время на устройстве** будет недоступен.
4. Выберите часовой пояс.
   - В раскрывающемся списке **Часовой пояс** выберите часовой пояс для устройства Axis.
   - Если ваше устройство находится в регионе, где существует переход на летнее время, установите флажок **Автоматический переход на летнее время**.

Примечание

Часовой пояс можно задать при выборе способа установки времени: **Синхронизировать с NTP-сервером** или **Задать вручную**.

5. В разделе выбора способа установки времени:
   - Выберите **Synchronize with server computer time (Синхронизировать с временем на сервере)**, если хотите, чтобы дата и время на вашем устройстве были синхронизированы с часами на сервере, то есть на том компьютере, где установлен сервер AXIS Camera Station Pro.
   - Выберите **Синхронизировать с NTP-сервером**, если хотите синхронизировать дату и время на вашем устройстве с NTP-сервером. Введите IP-адрес, DNS или имя хоста NTP-сервера в соответствующее поле.
   - Выберите **Задать вручную**, чтобы установка даты и времени производилась в ручном режиме.
6. Нажмите **OK**.

Установите время и дату

Установка приложений для камеры

Приложениями для камер называется программное обеспечение, которое можно загрузить и установить на сетевую видеотехнику Axis. Приложения расширяют функциональные возможности устройств, например, за счет обнаружения, распознавания, слежения или подсчета.

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 приложение лицензируется, файл с лицензионным ключом можно установить вместе с приложением. Его также можно установить позже, открыв страницу конфигурации соответствующего 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. Приложение, не требующее лицензии, можно установить на камеры со встроенным ПО, начиная с версии 6.50. 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. Приложение, не требующее лицензии, можно установить на камеры со встроенным ПО, начиная с версии 5.60.

AXIS Video Content Stream – Приложение, с помощью которого камеры Axis могут отправлять данные отслеживания движущихся объектов в AXIS Camera Station Pro. Оно может быть установлено на камеру со встроенным ПО версии от 5.50 до 9.59. Приложение AXIS Video Content Stream может использоваться только в сочетании с AXIS Camera Station Pro.

Другие приложения – Любое приложение, которое вы хотите 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 вы хотите установить программные приложения. Щелкните значок  или нажмите правую кнопку мыши и выберите в меню **Установить приложение для камеры**.
3. Выберите программное приложение, которое вы хотите установить на камеры. 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

переход на более раннюю версию или переустановка приводит к сбросу настроек приложения на устройстве.

5. Если для работы приложения требуется лицензия, то откроется диалоговое окно установки 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 приложений AXIS Video Motion Detection 2, AXIS Video Motion Detection 4 или AXIS Video Content Stream лицензии не требуются.

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 (ЦС) AXIS Camera Station Pro автоматически подписывает и распространяет сертификаты клиентов и серверов на устройства при включении HTTPS или IEE 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 > HTTPS > Enable/Update (Безопасность > HTTPS > Активировать/обновить)**, чтобы включить HTTPS или обновить параметры HTTPS для устройств.
   - Выберите **Security > IEEE 802.1X > Enable/Update (Безопасность > IEEE 802.1X > Активировать/обновить)**, чтобы включить IEEE 802.1X или обновить параметры IEEE 802.1X для устройств.
   - Выберите **Security > HTTPS > Disable (Безопасность > HTTPS > Отключить)**, чтобы отключить HTTPS для устройств.
   - Выберите **Security > IEEE 802.1X > Disable (Безопасность > IEEE 802.1X > 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 в списке однократно. Если удалить этот сертификат, он будет удален со всех устройств, на которых он установлен.

Состояние HTTPS и IEEE 802.1X

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

	Статус	**Описание**
HTTPS	Вкл.	AXIS Camera Station Pro использует протокол HTTPS для подключения к устройству.
	Выкл.	AXIS Camera Station Pro использует протокол HTTP для подключения к устройству.
	неизвестно	Устройство недоступно.
	Неподдерживаемое встроенное ПО	HTTPS не поддерживается, так как на устройстве установлено устаревшее встроенное ПО.
	Неподдерживаемое устройство	HTTPS не поддерживается этой моделью устройства.

IEEE 802.1X	Включено	Протокол IEEE 802.1X включен на устройстве.
	отключена	Протокол IEEE 802.1X не активирован, но готов к активации на устройстве.
	Неподдерживаемое встроенное ПО	IEEE 802.1X не поддерживается, так как на устройстве установлено устаревшее встроенное ПО.
	Неподдерживаемое устройство	IEEE 802.1X не поддерживается этой моделью устройства.

Сбор данных об устройствах

Эта функция обычно используется при устранении неполадок. С ее помощью создается ZIP-файл с отчетом о сборе данных для определенного местоположения на выбранных 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 «Источник данных о выбранных устройствах»:
   - Нажмите **Предустановка** и выберите одно из значений в раскрывающемся списке обычно используемых команд.

   Примечание

   Некоторые предустановки работают не на всех устройствах. Например, состояние PTZ не работает на аудиоустройствах.
   - Нажмите **Задается пользователем** и укажите полный URL-адрес для источника собираемых данных на выбранных серверах.
4. В разделе «Сохранить как» укажите имя файла и место расположения папки для ZIP-файла с собранными данными.
5. Выберите **Автоматически открывать папку после сбора данных** — при выборе этого варианта указанная папка будет открываться по окончании сбора данных.
6. Нажмите **OK**.

Подключение

Для обмена данными с устройствами с использованием IP-адреса или имени хоста:

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 используются для упорядочения устройств на странице управления устройствами. Устройство может иметь несколько тегов.

Теги, например, могут быть добавлены согласно модели или расположения. Если тег обозначает определенную модель камеры, вы сможете быстрой 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 **Использовать существующий ярлык** и выберите ярлык или выберите **Создать новый ярлык** и введите имя нового ярлыка
4. Нажмите **OK**.

Чтобы удалить тег у устройства:

1. Откройте меню **Configuration (Конфигурация) > Devices (Устройства) > Management (Управление)** и нажмите значок вверху справа.
2. Выберите тег в папке тегов. Будут показаны все устройства, отмеченные с этим тегом.
3. Выберите устройства Щелкните правой кнопкой мыши и выберите **Отменить теги устройств**.
4. Нажмите **OK**.

Управление тегами:

1. Откройте меню **Configuration (Конфигурация) > Devices (Устройства) > Management (Управление)** и нажмите значок вверху справа.
2. Перейдите на страницу «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**.
   - Чтобы закрепить страницу тегов устройств, нажмите значок .
   - Щелкнув тег, вы увидите все устройства, имеющие этот тег; щелкнув «Все устройства», вы увидите все устройства, связанные с системой 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 том, как настроить устройство, см. в руководстве пользователя данного устройства.
4. Закройте вкладку. Устройство будет перезагружено, чтобы изменения гарантированно вступили в силу в AXIS Camera Station Pro.

Ограничения

- Автоматическая проверка подлинности для устройств сторонних производителей не поддерживается.
- Общая поддержка для устройств сторонних производителей не гарантируется.
- Вкладка конфигурации устройства с активными видеопотоками увеличивает нагрузку и может повлиять на производительность серверного компьютера.

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 44*.

Перейдите к пункту **Configuration > Devices > External data sources (Конфигурация > Устройства > Внешние источники данных)**. Отобразится 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 в следующих случаях:

- При создании двери в разделе **Configuration > Access control > Doors and zones (Конфигурация > Контроль доступа > Двери и зоны)**.
  Полное описание рабочего процесса настройки сетевого дверного контроллера AXIS A1601 Network Door Controller в AXIS Camera Station Pro см. в разделе *Настройка сетевого дверного контроллера AXIS A1601 Network Door Controller*.
- 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 внешний источник данных настроен с видом с камеры, то создаваемые этим источником данные автоматически отмечаются как закладки на шкале времени этого вида с камеры 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 меню **Configuration > Devices > Time synchronization (Конфигурация > Устройства > Синхронизация времени)** для открытия страницы синхронизации времени.

Откроется список устройств, добавленных в AXIS Camera Station Pro. Щелкните правой кнопкой мыши по строке заголовка и выберите столбцы для отображения. Чтобы изменить порядок столбцов, потяните столбец за заголовок и перетащите.

Список устройств содержит следующую информацию:

- **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 74*.
- **MAC-адрес:** MAC-адрес устройства.
- **Модель:** модель устройства.
- **Включено:** Показывает, включена ли синхронизация времени.
- **Источник NTP:** Источник NTP, настроенный для устройства.
  - **Static (Статический):** NTP-серверы на устройстве указываются вручную в полях **Primary NTP server (Основной NTP-сервер)** и **Secondary NTP server (Резервный NTP-сервер)**.
  - **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**.
- **Основной NTP-сервер:** Основной NTP-сервер, настроенный для данного устройства. Доступно только при выборе варианта **Static (Статический)**.
- **Резервный NTP-сервер:** Резервный NTP-сервер, настроенный для данного устройства. Доступно только для устройств Axis, которые поддерживают резервный NTP-сервер и при выбранном варианте **Static (Статический)**.
- **Смещение времени сервера:** Разница во времени между устройством и сервером.
- **UTC time (Время UTC):** Всемирное координированное время на устройстве.
- **Синхронизировано:** Отображается в случае фактического применения настроек синхронизации времени. Доступно только на устройствах со встроенным ПО версии 9.1 или более поздней.
- **Время до следующей синхронизации:** Оставшееся время 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:

- **Сервер:** Сервер AXIS Camera Station Pro, на котором работает служба времени Windows.
- **Статус:** Состояние службы времени Windows. `Running` или `Stopped`.
- **NTP-сервер:** 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 резервный NTP-сервер.
5. Нажмите **Применить**.

Отправить сигнал тревоги, когда разница во времени между сервером и устройством превышает 2 секунды	Выберите эту опцию для получения сигнала тревоги, если разница во времени между сервером и устройством превысит 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

Чтобы открыть страницу «Управление хранением данных», выберите в меню **Конфигурация > Устройство хранения > Управление**. На странице «Управление хранилищем» представлен обзор локального хранилища и сетевого хранилища, существующего в AXIS Camera Station Pro.

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

Список	
Статус	Состояние ресурса хранения. Возможные значения статуса: • **OK** • **Storage full (Ресурс хранения заполнен).** Ресурс хранения заполнен. Система перезаписывает самые старые, незаблокированные записи. • **Недоступен:** Информация ресурса хранения в данный момент недоступна. Например, это может произойти, если сетевое хранилище удалено или отключено. • **Недопустимое переполнение:** Данные из других приложений используют дисковое пространство, 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. • **Нет полномочий:** У пользователя нет разрешения на чтение или запись в хранилище. • **Low space (Недостаточно места)** На диске меньше 15 ГБ свободного места, что AXIS Camera Station Pro считает слишком низким значением. 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 (Нехватка емкости)** Общий размер диска составляет менее 32 ГБ, чего недостаточно для AXIS Camera Station Pro. Устройства видеозаписи AXIS OS Recorders, поддерживающие RAID, также могут иметь следующие статусы: • **Online (Онлайн):** Система RAID работает, как следует. Резервирование в случае, если один из физических дисков в системе RAID будет недоступен. • **Degraded (Ухудшилось)** Один из физических дисков в системе RAID поврежден. Можно записывать и воспроизводить записи из хранилища, но резервирование недоступно. 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)** Дисковые RAID-массивы синхронизируются. Можно записывать и воспроизводить записи из хранилища, но при этом не будет резервирования, если физический диск сломается. 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 (Сбой)** Сбой в работе нескольких физических дисков в системе RAID. 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	
Used (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. раздел «Сбор неиндексированных файлов» в *Управление хранением данных, on page 79*.
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 ресурса хранения, занимаемый файлами, которые не являются проиндексированными записями и поэтому неизвестны для AXIS Camera Station Pro. Other data (Другие данные) = Total capacity (Общая емкость) – Used space (Использованное пространство) – Free space (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

Чтобы открыть страницу «Управление хранением данных», выберите в меню **Конфигурация > Устройство хранения > Управление**. На этой странице можно задать папку для хранения записей. Чтобы предотвратить заполнение хранилища, установите максимальный процент от 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 вход в службу выполнен с использованием системной учетной записи, добавлять общие папки на других компьютерах в качестве сетевых дисков невозможно. 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 локальный ресурс хранения, выберите **Local storage (Локальный ресурс хранения)** и выберите ресурс хранения из раскрывающегося меню.
4. Чтобы использовать общий сетевой диск, нажмите **Общий сетевой ресурс** и укажите к нему 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 локальный ресурс хранения или общий сетевой диск, выберите в списке ресурсов хранения нужный локальный ресурс хранения или общий сетевой диск 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.
- Емкость ресурса хранения, добавленного в AXIS Camera Station Pro, должна составлять не меньше 32 ГБ, из которых должно быть свободно по меньшей мере 15 ГБ.
- Если останется менее 15 ГБ свободного места, система AXIS Camera Station Pro автоматически начнет удалять старые записи, чтобы освободить место.

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.

Заметим, что собранные файлы не удаляются, а помещаются в папку **Non-indexed files (Неиндексированные файлы)** на ресурсе хранения, используемом для записи. 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 **Неиндексированные файлы** необходимо иметь доступ к этому серверу. AXIS Camera Station Pro размещает данные в папках в порядке их обнаружения, сначала по серверу, а затем по устройствам, подключенным к этому конкретному серверу.

Вы можете выбрать либо поиск конкретной потерянной записи или журнала, либо просто удаление содержимого, чтобы освободить место.

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 выполнение задачи.
4. По окончании перейдите на вкладку **Alarms and Tasks > Tasks («Тревоги и задачи > Задачи»** и дважды щелкните выполненную задачу, чтобы увидеть 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.

Чтобы открыть страницу «Выбор устройства хранения», откройте в меню **Конфигурация > Устройство хранения > Выбор**. На этой странице представлен список всех камер, добавленных в AXIS Camera Station Pro, и здесь можно указать срок хранения записей (в днях) для каждой конкретной камеры. После того как параметры заданы, информацию о хранении можно увидеть в меню «Устройства хранения 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 74*.
MAC-адрес	MAC-адрес устройства.
Изготовитель	производитель устройства.
Модель	модель устройства.
Используемое пространство устройства хранения	Объем пространства ресурса хранения, в данный момент занятый записями.
Местонахождение	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.
Резервная запись	Показывает, включена ли резервная запись для камеры.

Резервная запись	Показывает, включена ли резервная запись для камеры.
Сервер	Сервер, на котором расположен локальный ресурс хранения или сетевое хранилище.

Решение по хранению для каждой камеры настраивается тогда, когда камеру добавляют 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. Нажмите **Применить**.

Хранение записей	
Сохранить на	Выберите в раскрывающемся меню ресурс хранения, на который будут сохраняться записи. Возможные варианты: локальный ресурс хранения и созданное сетевое хранилище.
Резервная запись	Выберите, чтобы сохранять записи на SD-карту камеры в случае утери соединения между AXIS Camera Station Pro и камерой. После восстановления связи резервные записи переносятся в AXIS Camera Station Pro. Примечание Эта функция может использоваться только для камер с установленной картой памяти SD и встроенным ПО версии 5.20 или более поздней.
Без ограничений	Выберите это значение для времени хранения записей, чтобы они хранились до тех пор, пока не заполнится ресурс хранения.
Ограниченное	Выберите это значение и задайте максимальный срок хранения записей в днях. 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.

Настройка записи и событий

Когда выполняется добавление камер, AXIS Camera Station Pro автоматически настраивает параметры записи при обнаружении движения или непрерывной записи. Позже можно будет изменить способ записи в соответствии со своими потребностями, перейдите в раздел *Способ записи, on page 88*.

Запись по детекции движения

Функция обнаружения движения может использоваться со всеми сетевыми камерами и видеокодерами Axis. Запись видео только при обнаружении движения существенно экономит 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 соответствующие параметры, если камера обнаруживает слишком много или слишком мало движущихся объектов или если размер записанных файлов слишком велик по отношению к месту, доступному 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. Щелкните **Motion settings (Параметры движения)** для настройки параметров обнаружения движения, например количества обнаруживаемых объектов. Доступные параметры зависят от модели камеры, см. *Настройка встроенного видеодетектора движения* т *Изменение настроек AXIS Video Motion Detection 2 и 4*.
5. Выберите в раскрывающемся меню пункт **Profile (Профиль)** (по умолчанию используется значение **High (Высокий)**).
6. Выберите расписание или нажмите **New schedule... (Новое расписание)** для создания нового пользовательского расписания.
7. Задайте временные параметры предварительного и последующего буфера, а также период срабатывания триггера.
8. Нажмите **Применить**.

Примечание

Для настройки записи при обнаружении движения можно также использовать правила действий. Прежде чем использовать правила действий, обязательно отключите параметр **Motion detection (Обнаружение движения)** при выполнении настройки на экране **Recording method (Способ записи)**.

Профиль	Чтобы уменьшить размер записи используйте более низкое разрешение. Чтобы изменить параметры профиля, ознакомьтесь с разделом *Профили потоков*.
Расписание	Расписание, по которому должны выполняться записи. 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	Интервал времени между двумя последовательными срабатываниями триггера, чтобы уменьшить количество последовательно производимых записей. Если в этом интервале происходит дополнительное срабатывание триггера, запись продолжается, и период действия триггера начинается заново.
Поднять тревогу	Включает тревогу при обнаружении движения камерой.

Настройка детектора движения

Обнаружение объектов

Запись по обнаружению объектов выполняет захват видео при обнаружении и классификации типов объектов, таких как люди и транспортные средства, модулем AXIS Object Analytics. Рекомендуется использовать данную функцию совместно с обнаружением движения или непрерывной записью, чтобы не пропустить события. AXIS Object Analytics поддерживает до 10 сценариев на одну камеру.

Примечание

Для работы этой функции камера должна иметь версию микропрограммного обеспечения 12.4.26 или выше, один сенсор и установленный 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.

Настройки обнаружения объектов...	Нажмите, чтобы открыть веб-интерфейс AXIS Object Analytics и настроить типы объектов (люди, транспортные средства), которые инициируют запись, задать минимальный размер объекта, определить зоны обнаружения и настроить параметры времени пребывания в зоне.
Профиль	Выберите в раскрывающемся меню пункт **Profile (Профиль)** (по умолчанию используется значение **High (Высокий)**). Чтобы уменьшить размер записи используйте более низкое разрешение. Чтобы изменить параметры профиля, ознакомьтесь с разделом *Профили потоков*.
Расписание	Установка расписания, по которому должны выполняться записи. 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. Дополнительные сведения см. в разделе *Категории событий, on page 27*.
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 интервал времени между двумя последовательными срабатываниями триггера, чтобы уменьшить количество последовательно производимых записей. Если в этом интервале происходит дополнительное срабатывание триггера, запись продолжается, и период действия триггера начинается заново.
Поднять тревогу	Выберите этот параметр, чтобы формировать тревогу при обнаружении объекта модулем AXIS Object Analytics.

Непрерывная запись и запись по расписанию

При непрерывной записи происходит непрерывное сохранение изображений, поэтому требуется больше места в хранилище, чем при других вариантах записи. Для уменьшения размера файла можно использовать возможность 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)** для использования непрерывной записи.
4. Настройте параметры. Дополнительные сведения см. в таблице ниже.
5. Нажмите **Применить**.

Профиль	Выберите в раскрывающемся меню пункт **Profile (Профиль)** (по умолчанию используется значение **High (Высокий)**). Чтобы уменьшить размер записи используйте более низкое разрешение. Чтобы изменить параметры профиля, ознакомьтесь с разделом *Профили потоков*.
Расписание	Установка расписания, по которому должны выполняться записи. Чтобы снизить нагрузку на пространство хранилища, осуществляйте запись только в определенные периоды времени.
средний битрейт	Включите и задайте 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 88*.

Запись в ручном режиме

Сведения о выполнении записи вручную см. в разделе *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 в раскрывающемся меню пункт **Profile (Профиль)** (по умолчанию используется значение **High (Высокий)**). 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	Выберите, чтобы добавлять сведения закладки 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.

Запись по правилам

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.

Для создания записи по правилу см. раздел *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 режим резервной записи, чтобы записи сохранялись при потере соединения с AXIS Camera Station Pro. Когда активирована резервная запись, камера сохраняет видеозаписи на свою SD-карту, если соединение отсутствует более 20 секунд. В камере должна быть установлена SD-карта, и функция должна быть активирована. Резервная запись возможна только с записями формата H.264.

Для включения резервной записи:

1. Откройте меню **Конфигурация > Устройство хранения > Выбор**.
2. Выберите камеру, поддерживающую резервную запись.
3. Выберите **Failover recording (Резервная запись)**.
4. Нажмите **Применить**.

Примечание

- Перезапуск сервера AXIS Camera Station Pro не инициирует выполнение резервной записи. Например, при запуске средства обслуживания баз данных перезапустите AXIS Camera Station Pro Service Control или перезагрузите компьютер, на котором установлен сервер.
- Включение резервной записи перезаписывает любую существующую конфигурацию резервирования для этой камеры на других серверах.
- Резервная запись может быть активна только на одном сервере AXIS Camera Station Pro одновременно для каждого видеоканала.

После восстановления соединение AXIS Camera Station Pro автоматически импортирует резервные записи и помечает их темно-серым цветом на шкале времени.

Камера использует 20-секундный предбуфер и постбуфер для минимизации разрывов записи, но короткие разрывы длительностью около 1–4 секунд все же могут появляться. Для резервных записей всегда используется профиль потока высокого качества. Аудиосигнал включается, если он активирован на камере и является частью потока до включения режима резервной записи.

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.

Примечание

Устройства с версией AXIS OS ранее 11.11.42 используют устаревший метод резервной записи. Основные отличия:

- камера начинает резервную запись через 10 секунд после потери соединения.
- Камера использует 10-секундный буфер внутренней памяти вместо 20-секундного предбуфера и постбуфера.

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 резервной записи устройство автоматически начинает непрерывную запись в случае потери связи между AXIS Camera Station Pro и видеорегистратором. Устройство использует средний профиль потока для резервной записи.

Примечание

- Для этого требуется AXIS Camera Station 5.36 или более поздней версии, встроенное ПО AXIS S3008 Recorder 10.4 или более поздней версии, встроенное ПО устройства AXIS 5.50 или более поздней версии.
- Если непрерывная запись выполняется при инициировании резервной записи, начинается новая непрерывная запись. Система создает дубликаты потока на видеорегистраторе.

Для включения резервной записи:

1. Убедитесь, что вы добавили AXIS S3008 Recorder и соответствующие устройства и задали видеорегистратор 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 Pro Когда выполняется добавление устройств, автоматически настраивает параметры записи при обнаружении движения или непрерывной записи.

Установленный флажок в списке показывает, какой способ записи используется 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 экране **Recording method (Способ записи)** включите или выключите требуемый способ.

Примечание

Обнаружение движения в зонах просмотра не поддерживается.

Настройка среднего битрейта

В режиме усреднения битрейт автоматически регулируется на протяжении длительного времени. Благодаря этому можно достичь требуемого значения битрейта и обеспечить хорошее качество видео с учетом указанной емкости хранилища.

Примечание

- Этот параметр доступен только для непрерывной записи. Кроме того, камеры должны поддерживать функцию усреднения битрейта и на них должно быть установлено встроенное ПО версии 9.40 или более поздней версии.
- Параметры среднего битрейта влияют на качество выбранного профиля потока.

1. Перейдите к пункту **Configuration > Storage > Selection (Конфигурация > Устройство хранения > Выбор)** и убедитесь, что для камеры задан ограниченный срок хранения.
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. Этот параметр гарантирует только, что объем записей не превысят заданный объем пространства, но не гарантирует, что для записей достаточно места.

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

Приложения для камер AXIS Video Motion Detection 2 и 4 можно установить на устройства, поддерживающие платформу 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 систему AXIS Camera Station Pro выбрано включение записи по обнаружению движения, то приложения AXIS Video Motion Detection 2 и 4 требуется устанавливать только на камеры со встроенным ПО требуемой версии. 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 камеры*.

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

- **Область наблюдения**: Область выполнения 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).
- **Область исключения**: зона внутри области детекции, в которой будут игнорироваться движущиеся объекты.

- **Фильтры, позволяющие игнорировать объекты**: создаются фильтры, позволяющие не обращать внимания на движущиеся объекты, обнаруженные приложением. Старайтесь использовать как можно меньше фильтров и тщательно настраивайте их, чтобы не допустить игнорирования важных объектов. Использовать и настраивать фильтры следует по одному.
  - **Кратковременно присутствующие объекты**: данный фильтр позволяет не обращать внимания на объекты, возникающие на изображении лишь на короткое время. Например, пучки света от проезжающего мимо автомобиля и быстро движущиеся тени. Задайте минимальное время, в течение которого объект должен отображаться на изображении, чтобы возник сигнал тревоги. Время начинает отсчитываться с того момента, когда приложение обнаружило данный объект. Фильтр задерживает подачу сигналов тревоги и не запускает их, если объект исчезает с изображения в течение заданного времени.
  - **Мелкие объекты**: фильтр позволяет игнорировать объекты небольшого размера, включая мелких животных. Задайте ширину и высоту объекта в процентах от общих размеров изображения. Данный фильтр игнорирует объекты, размеры которых не превышают заданную ширину и высоту, и не запускает сигналы тревоги. Размеры соответствующего объекта должны быть меньше и по значению ширины, и по значению высоты, чтобы фильтр игнорировал его.
  - **Качающиеся объекты**: этот фильтр позволяет игнорировать объекты, перемещение которых происходит в ограниченном диапазоне расстояний, например, качание листвы деревьев, развевающиеся флаги и движение их теней. 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

Задаваемые здесь настройки изменяют настройки камеры.

1. Перейдите в меню **Конфигурация > Записи и события > Способ записи**.
2. Используя AXIS Video Motion Detection 2 или 4, выберите камеру и нажмите **Параметры 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 для кратковременно присутствующих объектов, выберите **Short lived objects filter (Фильтр кратковременно присутствующих объектов)** и задайте с помощью ползунка **Time (Время)** минимальное время, в

	течение которого объект должен присутствовать на изображении, чтобы запустить сигнал 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 для качающихся объектов, выберите **Swaying objects filter (Фильтр качающихся объектов)** и задайте размер эллипса с помощью ползунка **Distance (Расстояние)**.

Настройка встроенного видеодетектора движения

С помощью встроенной функции обнаружения движения камера фиксирует движение в одной или нескольких зонах наблюдения и игнорирует все остальные движения. Зона наблюдения — это область, в которой обнаруживается движение. Область исключения можно разместить внутри зоны наблюдения, чтобы игнорировать движение. Может использоваться несколько зон наблюдения и областей исключения.

Чтобы добавить или изменить зону наблюдения:

Примечание

Задаваемые здесь настройки изменяют настройки камеры.

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 видеть только изменяемую область, выберите **Show selected window (Показать выбранное окно)**.
6. Измените местоположение и размер фигуры на видеоизображении. Это зона наблюдения.
7. Отрегулируйте параметры **Object size (Размер объекта)**, **History (История)** и **Sensitivity manually (Чувствительность вручную)**.
8. Использование заранее заданных параметров. Выберите **Low (Низкий)**, **Moderate (Умеренный)**, **High (Высокий)** или **Very High (Очень высокий)**. **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. На верхнем уровне обнаружение движения выполняется после длительного пребывания объекта в пределах заданной области. На нижнем уровне обнаружение движения выполняется после кратковременного пребывания объекта в заданной области. 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. На экране **Edit Motion Detection (Изменение параметров обнаружения движения)** щелкните **Add (Добавить)** в разделе работы с окнами.
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 **OK**.

Настроить категории событий

Категории событий облегчают поиск записей определенного типа, таких как нападение или остановка движения. Чтобы создать категорию событий:

1. Перейдите в меню **Configuration (Конфигурация)** > **Recording and events (Записи и события)** > **Event categories (Категории событий)**.
2. Щелкните **Новая**.
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 27*.

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 добавлять порты ввода-вывода и управлять ими на любом из подключенных серверов. Для этого надо выбрать нужный сервер в раскрывающемся меню **Selected Server (Выбранный сервер)**.
- 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*.

Информацию 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 внесите изменения.

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, когда AXIS Camera Station Pro подключается к устройству. Выберите **On startup set to (Задать при запуске)**, а затем выберите исходное состояние в раскрывающемся меню **State (Состояние)**.

Изменить	Чтобы изменить порт, выберите его и нажмите **Изменить**. В появившемся диалоговом окне обновите сведения о порте и нажмите **OK**.
Удалить	Чтобы удалить порт, выберите его и нажмите **Удалить**.
Перезагрузка портов ввода/вывода	Если порты ввода/вывода настраиваются на странице конфигурации устройства, нажмите **Reload I/O Ports (Перезагрузить порты ввода-вывода)**, чтобы обновить соответствующий список.

Мониторинг портов ввода-вывода

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro можно отслеживать порты ввода-вывода. Для этого надо выбрать нужный сервер в раскрывающемся меню **Selected Server (Выбранный сервер)**.

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. Устройство может потребовать дополнительной настройки для поддержки многих из этих действий.

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. Перейдите в меню **Schedule (Расписание)**, выберите**Always (Всегда)** или **Custom schedule (Пользовательское расписание)** , чтобы выбрать расписание из раскрывающегося меню. Можно создать новое или изменить уже существующее.
5. В меню **Triggers (Триггеры)** нажмите **Add... (Добавить)**, выберите тип триггера, настройте его и нажмите **OK**. Подробнее см. *Добавление триггеров*.
6. В меню **Actions (Действия)** нажмите **Add... (Добавить)**, выберите тип действия, настройте его и нажмите **OK**. Подробнее см. *Добавление действий*.
7. Нажмите **Применить**.
   - Правило автоматически включается при его сохранении.

Изменить	Чтобы изменить имеющееся правило, выберите правило и нажмите **Изменить**.
Копировать	Чтобы скопировать имеющееся правило, выберите правило и нажмите **Copy... (Копировать)...**.
Удалить	Для удаления правила выберите правило и нажмите **Remove (Удалить)**.

Настройка нескольких правил действий

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

- Перейдите в меню **Конфигурация > Записи и события > Правила действия.**
- Выберите несколько правил.
- Выполните изменения:
  - Добавьте триггеры или действия, которые будут применяться ко всем выбранным правилам.
  - Удалите общие триггеры или действия из всех выбранных правил.
  - Измените расписание для всех выбранных правил.
- Нажмите **Применить**.

Примечание

При выборе нескольких правил невозможно редактировать отдельные триггеры или действия. Если внесенные изменения делают какое-либо правило недействительным, применить их невозможно.

Добавление триггеров

Триггеры активируют правила. В свою очередь, 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)**. При использовании этой настройки в импульсных триггерах увеличьте период действия 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 96*.

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 97*.

Ошибка и событие системы – Триггер системных событий и ошибок активируется при возникновении ошибки записи, переполнении хранилища, потере связи с сетевым накопителем или при разрыве связи с одним или несколькими устройствами. См. *Создание триггеров на основе системных событий и сбоев, on page 97*.

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 98*. Мы рекомендуем по возможности использовать триггеры по событиям устройства, а не триггеры ввода/вывода.

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 99*.

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 105*.

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 106*.

Внешний HTTPS – Внешний HTTPS-триггер позволяет внешним приложениям инициировать события в AXIS Camera Station Pro по протоколу HTTPS. См. *Создание внешних HTTPS-триггеров, on page 106*.

Создание триггеров с помощью детектора движения

Триггер обнаружение движения активируется, когда камера обнаруживает движение в зоне наблюдения. Поскольку камера обрабатывает обнаружение, она не добавляет нагрузки, связанной с обработкой, на AXIS Camera Station Pro.

Примечание

Не используйте триггеры обнаружения движения совместно с записью движения в камере. 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 **Новая**.
3. Нажмите **Добавить** и выберите **Детектор движения**.
4. Нажмите кнопку **OK**.
5. На всплывающем экране:
   5.1. Выберите камеру, которая должна обнаруживать движение.
   5.2. Задайте интервал времени между двумя последовательными срабатываниями триггера, чтобы уменьшить количество последовательно производимых записей. Если в этом интервале происходит дополнительное срабатывание триггера, запись продолжается, и период действия триггера начинается 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 **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 **Новая**.
3. Нажмите **Добавить** и выберите **Живой просмотр**.
4. Нажмите кнопку **OK**.
5. Выберите камеру для триггера.
6. Нажмите **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 включают ошибки записи, заполненное хранилище, сбой связи с сетевым хранилищем и потерю связи 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 **Новая**.
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	Если выбрать **On no contact with network storage (При отсутствии связи с сетевым ресурсом хранения)**, триггер будет срабатывать при проблемах с доступом к сетевому ресурсу хранения.
При потери связи с камерой	Если выбрать **On lost connection to camera (При потере связи с камерой)**, триггер будет срабатывать при проблемах связи с одной или несколькими камерами. • 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. Укажите **Select all (Выбрать все)** для выбора всех камер или **Deselect all (Отменить выбор)** для отмены выбора 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 используйте триггеры событий на устройстве, а не триггеры ввода/вывода. Триггеры событий на устройстве обеспечивают повышенный уровень удобства для пользователей. Для получения дополнительных сведений см. *Создать триггеры по событиям на устройстве, on page 99*.

Чтобы создать триггер ввода-вывода:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
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 интервал времени между двумя последовательными срабатываниями триггера, определив значение для параметра **Trigger period (Период действия триггера)**, чтобы уменьшить количество последовательно производимых записей. Если в этом интервале происходит дополнительное срабатывание триггера, запись продолжается, и период действия триггера начинается заново.

Создать триггеры по событиям на устройстве

Этот триггер использует события, поступающие непосредственно с камеры или вспомогательного устройства. Используйте этот триггер, если в AXIS Camera Station Pro нет подходящего триггера. События разных камер отличаются друг от друга, и для них необходимо задать один или несколько фильтров. Фильтры — это условия, при выполнении которых срабатывает триггер по событию на устройстве. 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 **Новая**.
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)** отображается текущее состояние триггера по событию на устройстве как функция времени. События бывают зависящими и не зависящими от предыстории. Активность события, зависящего от предыстории, отображается функцией в виде ступеньки. Активность события, не зависящего от предыстории, отображается прямой линией с импульсами, когда срабатывает триггер этого события.
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 интервал времени между двумя последовательными срабатываниями триггера, определив значение для параметра **Trigger period (Период действия триггера)**, чтобы уменьшить количество последовательно производимых записей. Если в этом интервале происходит дополнительное срабатывание триггера, запись продолжается, и период действия триггера начинается 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	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
Освещение	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
Состояние	Активный
Хранение данных	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 A1601 Network Door Controller

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 **Да** для активации правила действия, когда устройство находится в состоянии готовности. Обратите внимание, что правило может быть активировано, только если запущены все необходимые службы, например система обработки событий.
Дверной датчик	
Дверь открыта силой	Дверь открыта силой.
Обнаружены несанкционированные действия с дверью	Когда система обнаруживает следующее: • Открыт или закрыт корпус устройства. • Движение устройства. • Снятие подключенного считывателя со стены • Несанкционированные действия с подключенным дверным монитором, считывателем или устройством обработки запросов на выход. Для использования этого триггера обязательно включите параметр Supervised inputs (Контролируемые входы), а также установите оконечные резисторы на соответствующих контактах входных портов 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, если имеются посетители, которым необходимо разрешить открывать дверь без предоставления 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 для отправки уведомления или запуска мигания светодиодного 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	Потеряно сетевое подключение. Применимо только к событиям, используемым устройством, и неприменимо к событиям, используемым в 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 для видеозаписи в определенный период времени, например в рабочее время или в выходные дни. 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. При добавлении или изменении кнопки действия можно расположить рядом несколько кнопок для одной 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. Для вывода всплывающей подсказки наведите курсор мыши на кнопку.

Пример: Создайте кнопку для активации выходного порта в заранее определенное время, для подачи сигнала тревоги и отправки уведомления по электронной почте.

Кнопки-переключатели – Служит для запуска и остановки действия вручную. Такая кнопка имеет два состояния: нажата и отпущена. При нажатии кнопка меняет состояние с одного на другое. По умолчанию кнопки-переключатели запускают действие в нажатом состоянии, однако также можно запускать действие при отпускании кнопки.

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. Для вывода всплывающей подсказки наведите курсор мыши на кнопку.

Пример: Создайте кнопку для открытия и закрытия дверей (чтобы задать длительность интервала активности порта вывода, установите длительность импульса «Пока активен какой-либо триггер»).

Чтобы создать триггер для кнопки действия:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
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 клавишу 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 клавиши ALT + B, и кнопка действия активируется.

7. Если вы выбрали **Use existing button (Использовать существующую кнопку)**:
   7.1. Найдите кнопку или нажмите кнопку, которую вы хотите использовать.
   7.2. Если вы хотите использовать существующую кнопку-переключатель, то необходимо выбрать один из двух вариантов **Trigger on toggle (Запуск при нажатии кнопки)** или **Trigger on untoggle (Запуск при отпускании кнопки)**.

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 данный 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 **Новая**.
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 HTTPS-триггер позволяет внешним приложениям инициировать события в AXIS Camera Station Pro по протоколу HTTPS. Этот триггер поддерживает только протокол HTTPS, причем в запросе HTTPS необходимо указать актуальное имя пользователя AXIS Camera Station Pro, включая доменное имя и пароль.

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 *Общее*.
- 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. Проверьте пробный URL-адрес, в котором используется тот же адрес сервера, который используется клиентом при входе в систему. URL-адреса функционируют только после выполнения правила действия.
7. Нажмите **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 **Новая**.
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 181*.
   - Выберите **High processing delay (Высокая задержка обработки)**, чтобы активировать триггер, когда Smart search 2 обрабатывает объекты обнаружения дольше одной минуты.
6. Нажмите кнопку **OK**.

создать триггер аудиоменеджера;

Для создания триггера в Audio manager (Аудиоменеджер):

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
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 (Статус устройства изменен)**, чтобы активировать триггер при изменении статуса устройства (например, устройство стало онлайн или офлайн).
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 (Целевой объект включен или отключен)**, чтобы активировать триггер при включении или отключении целевого объекта.
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 начинаются при активации правила.

Доступны следующие действия:

Запись – это действие включает запись с камеры. См. *Создание действия «Запись»*.

Поднять тревогу – Данное действие означает подачу сигнала тревоги на все подключенные клиенты AXIS Camera Station Pro. См. *Создание действий подачи сигналов тревоги*.

Задать выходной сигнал – Это действие задает состояние порта вывода. Используйте его для управления устройством, подключенным к выходному порту, например, можно включить свет или заблокировать дверь. См. *Создание действий для выходных портов*.

Отправка письма по электронной почте – действие предусматривает отправку сообщения по электронной почте одному или нескольким получателям. См. *Создание действий отправки электронной почты*.

Просмотр в реальном времени – Это действие открывает живой просмотр для конкретной камеры, вида или предустановленной позиции во всех подключенных клиентах AXIS Camera Station Pro. Действие просмотра живого видео также можно использовать для развертывания окон открытых клиентов AXIS Camera Station Pro из панели задач или для перемещения клиентов на передний план относительно других открытых приложений. См. *Создание действий живого просмотра*.

Отправить HTTP-уведомление – данное действие предусматривает передачу HTTP-запроса камере, дверному контроллеру или внешнему веб-серверу. См. *Создание действий для отправки HTTP-уведомлений*.

Сирена и освещение – Данное действие активирует сигнал тревоги и световую индикацию на совместимом устройстве в соответствии с предварительно настроенным профилем. См. *Создание действий для сирены и освещения, on page 115*.

Virtual I/O (Виртуальный вход/выход) – Данное действие активирует назначенный виртуальный входной порт на устройстве. См. *Создание действий виртуального ввода/вывода, on page 115*

Система AXIS Entry Manager – данное действие позволяет предоставить доступ либо отпереть или запереть дверь, которая подключена к дверному контроллеру, настроенному с помощью AXIS Entry Manager. См. *Создание действий AXIS Entry Manager, on page 116*.

Отправить уведомление мобильного приложения – Данное действие отправляет пользовательское сообщение в мобильное приложение AXIS Camera Station. См. *Создание действий для отправки уведомления мобильному приложению, on page 116*.

Включение или выключение правил – Используйте это действие для включения или выключения других правил действий. См. *Создать действие, которое включает и выключает другие правила действий., on page 116*.

Отправить на видеодекодер – Используйте этот вид, чтобы отправить данные на видеодекодер для отображения на мониторе в течение заданного времени. См. *Создайте действие, которое отправляет вид на видеодекодер, on page 117*

Контроль доступа – данное действие включает действия с дверями и действия с зонами в AXIS Camera Station Secure Entry. См. *Создание действий контроля доступа, on page 117*.

Создание действия «Запись»

Действие «Запись» включает запись с выбранной камеры. Для доступа к записи и для ее воспроизведения используется вкладка **Recordings (Записи)**.

Чтобы создать действие «Запись»:

1. Укажите расположение для сохранения записи в разделе **Configuration > Storage > Selection (Конфигурация > Устройство хранения > Выбор)**.
2. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
3. Щелкните **Новая**.
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 (Настройки события)** выпри необходимости можно выбрать категорию события, к которой должна относиться запись.
10. Нажмите **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	Выберите время в секундах, в течение которого продолжается запись после прекращения триггера действия.

Создание действий подачи сигналов тревоги

Действие подачи сигнала тревоги заключается в отправке сигнала тревоги на все подключенные клиенты AXIS Camera Station Pro. Тревога отображается на вкладке **Alarms (Сигналы тревоги)** и в уведомлении на панели задач. К сигналу тревоги можно приложить файл с указаниями о необходимых действиях в случае 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 **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 тревоге)** настройте заголовок, описание, а также длительность.
7. В разделе **Alarm procedure (Действия при тревоге)**.
   7.1. Выберите **Показывать действия при тревоге**.
   7.2. Нажмите **Upload (Загрузить)** и выберите в проводнике нужный файл.
   7.3. Нажмите **Предварительный просмотр**, чтобы открыть загруженный файл в окне предварительного просмотра.
   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 продолжительность отображения в диапазоне от 1 до 600 секунд для всплывающих сигналов тревоги.

Создание действий для выходных портов

Выходное действие устанавливает состояние порта вывода. Это применяется для управления устройством, подключенным к выходному порту, например, можно включить свет или заблокировать дверь.

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 **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 варианты зависят от конфигурации порта.
8. Выберите **Импульс**, чтобы задать длительность пребывания порта 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 фиксированного времени, выберите второй вариант и задайте время в секундах.

Создание действий отправки электронной почты

Действие отправки электронной почты служит для отправки сообщения по электронной почте одному или нескольким получателям. К сообщению электронной почты можно приложить моментальные снимки 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 **Новая**.
3. Для создания триггера нажмите **Добавить**. Нажмите **Next** ("Далее"). См. *Добавление триггеров*.
4. Нажмите **Добавить** и выберите **Отправить сообщение по электронной почте**.
5. Нажмите кнопку **OK**.
6. Добавьте получателей в меню **Recipients (Получатели)**:
   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 кнопку **Add (Добавить)**, чтобы добавить адрес электронной почты в поле **Recipients (Получатели)**.
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 **OK**.

Расширенный набор	
Присоединить моментальный снимок	Чтобы отправить моментальные снимки с камер (в формате jpg) в виде вложений в уведомления, отправляемые по электронной почте, выберите **Attach snapshots (Приложить снимки)** и нажмите **Cameras (Камеры)**. Появляется список всех камер, зарегистрированных для работы с ПО AXIS Camera Station Pro. Укажите **Select all (Выбрать все)** для выбора всех камер или **Deselect all (Отменить выбор)** для отмены выбора всех камер.
Отправлять одно электронное письмо для каждого события	Чтобы предотвратить отправку нескольких сообщений по электронной почте для одного и того же события, выберите **Отправлять одно сообщение для каждого события**.
Не отправлять следующее сообщение в течение	Чтобы предотвратить отправку сообщений по электронной почте через слишком малые интервалы времени, выберите **Don't send another email for (Не отправлять следующее сообщение в течение)** и задайте минимальное время между отправкой сообщений, выбрав его в раскрывающемся меню.

Создание действий живого просмотра

Действие живого просмотра открывает вкладку **Live view (Живой просмотр)** с конкретной камерой, видом или предустановленной позицией. Вкладка **Live view (Живой просмотр)** открывается во всех подключенных клиентах AXIS Camera Station Pro. Если на вкладке **Live view (Живой просмотр)** отображается мультиэкран с главной областью наблюдения, то камера, выбранная в действии живого просмотра, будет загружена в эту главную область. Для получения дополнительных сведений о главных областях наблюдения см. раздел *Мультиэкранный режим*.

Действие просмотра живого видео также можно использовать для развертывания окон открытых клиентов AXIS Camera Station Pro из панели задач или для перемещения клиентов на передний план относительно других открытых приложений.

Чтобы создать действие живого просмотра:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
3. Для создания триггера нажмите **Добавить**. 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, что должно отображаться при активном действии.
7. В разделе **Shown in (Показано в)** настройте способ отображения выбранного вида.
8. Чтобы развернуть открытые клиенты AXIS Camera Station Pro **Bring to front (Вынести на передний план)** из панели задач или переместить окна клиентских приложений поверх других открытых приложений при запуске действия живого просмотра, выберите в соответствующей части окна **On trigger bring application to front (При срабатывании триггера переместить окно приложения наверх)**.
9. Нажмите кнопку **OK**.

Действия просмотра живого видео	
Вид	Чтобы открыть какой-то вид, нажмите **View (Вид)** и выберите в раскрывающемся меню требуемую область наблюдения.
Камера	Чтобы открыть вид с камеры, нажмите **Camera (Камера)** и выберите в раскрывающемся меню нужную камеру. Если для камеры заданы предустановленные позиции PTZ, выберите **Go to preset (Перейти к предустановке)**, затем выберите одну область в раскрывающемся меню, чтобы открыть предустановленную позицию.
Действия нет	Если не нужно открывать никакой вид, выберите **No action (Действие не требуется)**.

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 главная область наблюдения видима в режиме живого просмотра, то при запуске действия будет отображаться вид с камеры в главной области наблюдения.

Пример:
Чтобы открыть вкладку **Live view (Живой просмотр)**, перейдите в вид главной области наблюдения и отобразите вид с камеры в главной области наблюдения, настройте два действия живого просмотра в том же правиле действия:

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 другое действие живого просмотра, чтобы перейти в вид главной области наблюдения, и отобразите вид с камеры в главной области наблюдения.
   2.1. В разделе **Live view actions (Действия живого просмотра)** выберите пункт **Camera (Камера)** и выберите вид с 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. HTTP-уведомления можно использовать, например, для включения или отключения отдельных функций камеры

или для того, чтобы открыть, закрыть, запереть или отпереть дверь, подключенную к дверному контроллеру.

Поддерживаются методы GET, POST и PUT.

Примечание

Для отправки HTTP-уведомлений получателям, находящимся за пределами локальной сети, может потребоваться настройка параметров прокси-сервера для 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 **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 использовать данный параметр, поскольку он обеспечивает максимальную защиту от несанкционированного 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 (Способ)** выберите тип HTTP-уведомлений.
Тип содержимого	В случае выбора метода POST или PUT выберите тип контента в раскрывающемся меню **Content type (Тип контента)**.
Основной текст	При использовании метода POST или PUT введите тело запроса в поле **Body (Тело)**.
Данные инициирующего события	В раскрывающемся меню также можно вставить предустановленные данные инициирующего события. См. подробнее ниже.

Данные инициирующего события	
Тип	Инициирующее событие, которое активировало данное правило действия.
Идентификатор источника	Представляет собой идентификатор источника, запускающего правило действия, зачастую это будет камера либо устройство другого типа. Идентификаторы источника для разных источников могут отличаться.
Source name (Имя источника)	Представляет собой имя источника, запускающего правило действия, зачастую это будет камера либо устройство другого типа. Имена источника для разных источников могут отличаться.
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/вывода для активации определенного порта виртуального ввода на устройстве. Каждый порт устройства можно использовать для одного действия.

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 для активации.
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 **Новая**.
3. Для создания триггера нажмите **Добавить**. 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

С помощью действия AXIS Entry Manager можно предоставить доступ к двери либо отпереть или запереть дверь, которая подключена 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 **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 должно быть выполнено действие.
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. Щелкнув по поступившему уведомлению, можно перейти к определенному виду 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 **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 (Нажать уведомление и перейти)** можно настроить, что будет отображаться при нажатии на уведомление.
8. Нажмите **OK**.

Щелкните уведомление и перейдите в	
Камера	В раскрывающемся меню **Camera (Камера)** выберите вид с камеры , который должен отображаться при нажатии на уведомление в мобильном приложении.
По умолчанию	Выберите **Default (По умолчанию)**, чтобы перейти на домашнюю страницу мобильного приложения при выборе уведомления в мобильном приложении.

Создать действие, которое включает и выключает другие правила действий.

Используйте функцию Turn rules on or off (Включение или выключение правил), например, если нужно отключить функцию обнаружения движения в офисе, когда сотрудник проводит карту доступа перед считывающим устройством.

Чтобы создать действие для включения и выключения правил:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 действия.
7. Выберите этот параметр, чтобы включить или отключить выбранные правила действия.
8. Если между инициирующим событием и изменением состояния должно пройти какое-то время, задайте задержку.
9. Выберите **Return to the previous state when the trigger is no longer active (Вернуться к предыдущему состоянию после того, как инициирующее событие станет неактивным)**, если требуется, чтобы выбранное правило действия оставалось не измененным при неактивном инициирующем событии. В приведенном выше примере функция обнаружения движения включается сразу после того, как сотрудник убирает карту доступа со считывающего устройства.
10. Нажмите **OK**.

Создать новую закладку

Чтобы создать действие «Закладка»:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 этот вид, чтобы отправить данные на видеодекодер для отображения на мониторе в течение заданного времени.

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 разделе **Duration (Продолжительность)** введите время в секундах, в течение которого будет отображаться вид.
9. Нажмите **OK**.

Создание действий контроля доступа

Действие контроля доступа позволяет выполнять следующие действия в системе AXIS Camera Station Secure Entry:

- **Действия с дверями:** предоставление доступа, запирание, отпирание или блокировка выбранных дверей.
- **Действия с зонами:** запирание, отпирание или блокировка выбранных дверей в выбранных зонах.
- **Действия с правилом доступа:** Включение или выключение правила доступа.

Примечание

Действие контроля доступа доступно только для системы AXIS Camera Station Secure Entry.

Для создания действия контроля доступа:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
3. Для создания триггера нажмите **Добавить**. 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)**, затем выберите **Enable (Включить)** или **Disable (Выключить)**.
9. Нажмите кнопку **OK**.

создать действия аудиоменеджера;

Для создания действия в Audio manager (Аудиоменеджер):

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
3. Для создания триггера нажмите **Добавить**. 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 аудиоменеджера	
Воспроизвести аудиофайл	Выберите **Play audio file (Воспроизвести аудиофайл)** для воспроизведения выбранного аудиофайла.
Включить или отключить целевое устройство	Выберите **Enable or disable target (Включить или отключить устройство)**, чтобы включить или отключить устройства.

Действия аудиоменеджера	
Отключить звук	Выберите **Mute volume (Отключить звук)** для отключения регулятора громкости.
Установить уровень громкости	Выберите **Set volume (Установить громкость)**, чтобы установить новый уровень громкости.
Смещение уровня громкости	Выберите **Offset volume (Сместить громкость)**, чтобы увеличить или уменьшить громкость относительно текущего уровня.

Расписания

На странице "Schedules" (Расписания) содержатся все расписания, которые можно использовать для записи, правил действия и компонентов, например AXIS Secure Entry. AXIS Site Designer создает некоторые расписания во время установки.

Расписания позволяют создавать и изменять настраиваемые ежедневные и еженедельные, а также специальные приоритетные расписания, которые используются вместо ежедневного или еженедельного расписания в определенные 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, какое это расписание: ежедневное или еженедельное.
- **In use (Используется)**: Указывает, используют ли сейчас расписание компонент, правило записи или правило действия.
- **Override schedules (Приоритетные расписания)**: Перечисляет, какие приоритетные расписания используются для данного расписания.

Вкладка **Override schedules** (Приоритетные расписания) — это основное представление, в котором можно управлять приоритетными расписаниями и просмотреть ежедневные и еженедельные расписания, для которых они используются.

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 меню **Selected server (Выбранный сервер)** для управления 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). Прежде чем удалить расписание, убедитесь, что оно 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 период времени, нажмите **+** или дважды щелкните строку.
- Чтобы изменить диапазон дат или период времени, 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 к расписанию новый диапазон дат. К одному приоритетному расписанию можно добавить несколько диапазонов дат.
- Чтобы добавить период времени, нажмите **+** или дважды щелкните строку.
- Чтобы изменить диапазон дат или период времени, щелкните его левой кнопкой мыши.
- Нажмите **Apply** (Применить), чтобы сохранить изменения.

Примеры правил действий

Пример: Взломана дверь

Взломана дверь

В этом примере будет показано, как настроить правило действия в AXIS Camera Station Pro так, чтобы при открытии входной двери силой запускалась видеозапись и подавался сигнал тревоги.

Прежде чем начать, потребуется выполнить следующее:

- Установить сетевой дверной контроллер AXIS A1601 Network Door Controller. См. *Добавить устройства, on page 47*.
- Настроить дверной контроллер. См. раздел *Добавление двери, on page 156*.

Создайте правило действия:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
3. Добавьте триггер по событию «Дверь открыта силой».
   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 (Активность)** убедитесь, что активность триггера отражается на сигнальной линии.
   3.6. Нажмите кнопку **OK**.
4. Нажмите **Next** (“Далее“).
5. Добавьте действие «Запись».
   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. Пример: «Принудительно открыта дверь главного входа».

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 A1601 Network Door Controller 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 (Высокий)** в раскрывающемся меню **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 будет показано, как настроить правило действия в AXIS Camera Station Pro так, чтобы при входе важного человека воспроизводилось приветственное сообщение и вызывался лифт.

Прежде чем начать, потребуется выполнить следующее:

- Установить и настроить сетевой дверной контроллер AXIS A1601 Network Door Controller и добавить владельцев карт. См. *Настройте контроль доступа, on page 153* и *Контроль доступа, on page 187*.
- Установить сетевое аудиоустройство Axis и связать его с камерой. См. *Профили потоков, on page 55*.
- 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 93*.

Создайте правило действия:

1. Перейдите в меню **Конфигурация > Записи и события > Правила действия**.
2. Щелкните **Новая**.
3. Добавьте триггер по событию на устройстве.
   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 (Активность)** убедитесь, что активность триггера отражается на сигнальной линии.
   3.6. Нажмите кнопку **OK**.
4. Нажмите **Next** ("Далее").
5. Добавьте действие Send HTTP Notification (Отправить HTTP-уведомление), чтобы запускалось воспроизведение 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 (Установить выход).
   6.1. Нажмите **Добавить** и выберите **Создать действие на выходе**.
   6.2. Нажмите кнопку **OK**.
   6.3. В раскрывающемся меню **Output port (Выходной порт)** выберите выходной порт 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 продолжительность удержания состояния порта равной 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 A1601 Network Door Controller 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 важного человека.

Настройка клиентского ПО

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

- Изменить параметры клиента, например, тему и язык. См. *Настройки клиента, on page 123*.
- Изменить параметры пользователя, например, уведомления и параметры запуска. См. *Настройки пользователя, on page 124*.
- Изменить такие клиентские настройки потоковой передачи видео как масштабирование видео и аппаратное декодирование. См. *Потоковая передача, on page 126*.

Настройки клиента

Эти настройки будут применены ко всем пользователям AXIS Camera Station Pro на компьютере. Чтобы настроить параметры клиента **, перейдите в меню** Configuration > Client > Client settings (Конфигурация > Клиент > Настройки клиента) AXIS Camera Station Pro.

Тема	
System (Системная), Light (Светлая), Dark (Темная)	Выберите оформление для данного клиента. Для новых установок по умолчанию используется тема **System** (Системная). Если выбран вариант **System** (Системная), будет использоваться светлая или темная тема в зависимости от текущих настроек системы Windows.

Общее	
Запускать приложение при загрузке Windows	Активируйте этот параметр, чтобы автоматически запускать AXIS Camera Station Pro при каждом запуске Windows.

Просмотр в реальном времени	
Показывать названия камер в живых просмотрах	Отображение названия камеры в живом просмотре.
	Для отображения записей всех типов включите параметр **Show recording indicators in live views and maps (Показывать индикаторы записи в живом просмотре и на картах)**.
	Для отображения записей, активированных при обнаружении движения, или записей, запущенных в соответствии с правилом действий, включите параметр **Show event indicators in live views and maps (Показывать индикаторы событий в живом просмотре и на картах)**.

Карты	
Разрешить мигание зон охвата для всех карт	Используется для общего выключения или включения мигания всех зон охвата через меню **Flash (Мигание)**. Эта глобальная настройка не влияет на локальную настройку на уровне карты. См. *Карта, on page 22*.

Язык
Изменение языка клиента AXIS Camera Station Pro. Изменение вступает в силу после перезапуска клиента.

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. Порядок изменения параметров сервера см. в разделе *Параметры сервера, on page 132*.

Настройки пользователя

Эти настройки применяются к пользователю AXIS Camera Station Pro, вошедшему в систему. Чтобы настроить параметры клиента **, перейдите в меню** Configuration > Client > User settings (Конфигурация > Клиент > Настройки пользователя) AXIS Camera Station Pro.

Система навигации	
Представление системы навигации в виде дерева	Включается по умолчанию для отображения панели навигации в виде дерева с различными видами и камерами.
Показать в системе навигации	Выберите для отображения видов и/или камер в раскрывающемся меню.
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 активации сигнала тревоги на панели задач Windows отображалось уведомление.
Выводить уведомления о задачах на панель задач	Включите этот параметр, чтобы отобразить уведомление на панели задач Windows, когда кто-либо добавляет задачу или ее окончание.
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 показать окно уведомлений, когда кто-либо нажимает кнопку вызова в подключенной системе переговорной связи.

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 хранения моментальных снимков.

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 при запуске AXIS Camera Station Pro открывались вкладки, виды и виды с камер, которые были открыты при последнем закрытии этого приложения AXIS Camera Station Pro.
Запоминать последние мониторы	Включите этот параметр, чтобы запускать AXIS Camera Station Pro на том же мониторе, где окно AXIS Camera Station Pro было закрыто при запуске в предыдущий раз.

Примечание

- Система сохраняет виды и виды с камер для каждой вкладки. Система их запомнит, только если клиент в следующий раз подключается к тому же серверу.
- Запоминать вкладки, чтобы запомнить мониторы, виды и виды с камер.
- 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 пункт, если тревога не должна сопровождаться звуковым сигналом.
Зуммерный сигнал	Выберите этот пункт, если тревога должна сопровождаться типичным звуковым сигналом зуммера.
Звуковой файл	Выберите и нажмите **Browse (Обзор)**, чтобы найти звуковой файл, если вы подготовили особое звуковое сопровождение для тревоги. Можно использовать любой формат файлов, поддерживаемый проигрывателем Windows Media Player.
Воспроизведение	Нажмите для проверки звука.

Звук при входящем вызове	
Без звука	Выберите этот пункт, если входящий вызов не должен сопровождаться звуковым сигналом.
Зуммерный сигнал	Выберите этот пункт, если входящий вызов должен сопровождаться типичным звуковым сигналом зуммера.
Звуковой файл	Выберите и нажмите **Browse (Обзор)**, чтобы найти звуковой файл, если вы подготовили особое звуковое сопровождение для входящего вызова. Можно использовать любой формат файлов, поддерживаемый проигрывателем Windows Media Player.
Воспроизведение	Нажмите для проверки звука.

Особенности конструкции	
Показать интеллектуальный поиск 1	По умолчанию отображается Умный поиск 1. Выключите, чтобы скрыть эту функцию.

Показывать окна с предупреждениями	
Предупреждение о недействительном сертификате	Включите, чтобы при необходимости показывать это предупреждение.

Потоковая передача

Чтобы настроить параметры видеопотока в клиенте **, перейдите в меню** Configuration > Client > Streaming (Конфигурация > Клиент > Потоковая передача) AXIS Camera Station Pro.

Масштабирование видео	
Наилучшее масштабирование	Выберите опцию для отображения видео на всем доступном пространстве, без искажения пропорций и без обрезки изображения.
Заполнить область видео (части видеоизображения могут быть обрезаны)	Выберите опцию, чтобы подогнать видео под доступное пространство и сохранить пропорции. Если у свободного места на экране и у видеоизображения разные соотношения сторон, то система обрежет видео.

Аппаратное декодирование	
Режим	• **Automatic (Автоматически)** Использует видеокарту (если поддерживается) для декодирования потоков с разрешением выше 3840 x 2160p при 25 кадр/с (стандарт 4K или UHD). • **On (Вкл.)** Использует видеокарту (если поддерживается) для декодирования потоков с разрешением выше 1920 x 1080p при 25 кадр/с (стандарт 1080p или HD). • **Off (Выкл.)** Аппаратное декодирование отключено, при этом AXIS Camera Station Pro использует центральный процессор для декодирования видео.
Видеокарта	Выберите видеокарту в раскрывающемся меню.

Примечание

- Для аппаратного декодирования используется видеокарта компьютера, позволяющая декодировать видео. Если у вас высокопроизводительная видеокарта, то аппаратное декодирование — это хороший способ увеличить производительность и снизить нагрузку на ЦП, особенно при потоковой передаче видео с высоким разрешением. Аппаратное декодирование поддерживает стандарты M-JPEG и H.264.
- Камеры с разрешением ниже 1080p не могут использовать аппаратное декодирование, даже если соответствующая функция включена **On (Вкл.)**.
- Если используемая видеокарта не поддерживает декодирование 4K, то аппаратное декодирование будет работать только для потоков с разрешением 1080p, даже если функция аппаратного декодирования включена **On**.

Использование трафика	
Всегда использовать профиль потока «Низкий» для этого клиента	Активируйте этот режим, чтобы использовать низкий профиль потока для живого просмотра. См. *Профили потоков*. Данная настройка влияет на видео в форматах H.264 и M-JPEG и уменьшает нагрузку на сеть.
Приостанавливать видеопотоки на неактивных вкладках	Активируйте этот параметр, чтобы приостанавливать видеопотоки на неактивных вкладках. Это позволяет уменьшить нагрузку на сеть.

PTZ (поворот, наклон, зум)	
Первым кликом выбирать зону просмотра, а не запускать PTZ	Включите этот параметр, чтобы активировать выбор вида при первом нажатии в пределах вида. Последующие клики по зоне просмотра будут запускать PTZ-управление.

Звук	
Push-to-talk release delay (ms) (Задержка после отпускания переговорной кнопки (мс))	Задайте время в миллисекундах, в течение которого необходимо сохранить передачу звука с микрофона после отпускания переговорной кнопки **Push-to-talk**.
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	Активируйте этот параметр, чтобы переговариваться через переговорные устройства даже при отсутствии входящего вызова.

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 сервисы открывают доступ к следующим возможностям:

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

Для использования подключенных сервисов необходимо зарегистрировать вашу систему и привязать ее к организации. Для получения дополнительных сведений см. *Регистрация системы в организации, on page 129*.

Статус	Карточка состояния отображает статус соединения между вашим сервером и подключенными сервисами, а также название организации, к которой вы присоединены или в которой зарегистрированы.
Отключить	При отключении подключенного сервера он по-прежнему остается зарегистрированным в организации.

Управление лицензиями	Включите опцию **License management (Управление лицензиями)** для автоматической синхронизации ваших лицензий. При этом система будет передавать в AXIS License Manager изменения, влияющие на количество лицензий, и получать обновленный статус лицензий. Отключите **Управление лицензиями**, если требуется управлять лицензиями вручную, например, при отсутствии интернет-подключения у вашей системы. 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.

Дополнительные сведения о факторах, которые необходимо учесть при регистрации системы, см. *в* Руководстве по установке и миграции для 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)** в раскрывающемся меню для проверки наличия новых версий встроенного ПО при каждом запуске системы на сервере. По умолчанию для AXIS Camera Station Pro задано 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 2 позволяет подключаться к серверу AXIS Camera Station Pro с помощью надежного зашифрованного интернет-соединения.

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 129*.
2. Войдите в систему с помощью Axis Secure Remote Access 2. См. *Войти в AXIS Secure Remote Access*.

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**. Она разрешает доступ только к серверам AXIS Camera Station Pro, не позволяя использовать другие функции Axis в разделе My Systems.

После регистрации вы можете дополнительно управлять правами доступа, назначая роли пользователей организации с помощью Axis My Systems. Дополнительные сведения о правах доступа пользователей AXIS Camera Station Pro см. в разделе *Права доступа пользователей, on page 144*.

Axis Secure Remote Access

Внимание

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

Что это означает для вашей системы AXIS Camera Station Pro?

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

Средство безопасного удаленного доступа Axis Secure Remote Access позволяет подключаться к своему серверу AXIS Camera Station Pro с помощью надежного зашифрованного интернет-соединения. Безопасный удаленный доступ к камерам Axis Secure Remote Access обеспечивается независимо от переадресации портов в маршрутизаторе.

Примечание

- Служба Axis Secure Remote Access доступна только для AXIS Camera Station 5.12 или более поздних версий.
- При подключении к нескольким серверам AXIS Camera Station Pro выберите любой сервер в раскрывающемся меню **Selected server (Выбранный сервер)** для настройки Axis Secure Remote Access.

Включение безопасного удаленного доступа Axis Secure Remote Access

Чтобы пользоваться безопасным удаленным доступом Axis Secure Remote Access, нужно войти в свою учетную запись My Axis. Безопасный удаленный доступ Axis Secure Remote Access необходимо включить вручную. Эта функция позволяет выполнить удаленный вход на сервер, см. раздел *Подключить к серверу*.

1. Перейдите в меню **Конфигурация > Подключенные сервисы > Axis Secure Remote Access**.
2. В разделе My Axis account (Учетная запись My Axis) введите свои учетные My Axis.
3. Нажмите **Применить**.
4. Для включения удаленного доступа нажмите **Enable (Включить)** в окне Axis Secure Remote Access.

Включение безопасного удаленного доступа Axis Secure Remote Access на мобильных устройствах

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

1. Откройте на мобильном устройстве страницу *axis.com/products/axis-camera-station/overview* и скачайте приложение AXIS Camera Station Mobile.
2. Установите и запустите приложение.
3. Войдите в Axis Secure Remote Access, используя ту же учетную запись My Axis, которую вы использовали для активации удаленного доступа.
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.

В мобильном приложении отображается общий объем переданных данных для учетной записи My Axis за месяц. Подробнее об этом можно узнать в *Руководстве пользователя по мобильному приложению AXIS Camera Station Mobile*.

Использование безопасного удаленного доступа Axis Secure Remote Access

Использование службы Axis Secure Remote Access отображается в строке состояния в нижней части окна клиентского ПО AXIS Camera Station Pro. Для получения обзорной информации об использования безопасного удаленного подключения перейдите по ссылке.

Уровень обслуживания	отображается уровень обслуживания для вашей подписки на Axis Secure Remote Access.
Данные, использованные в этом месяце	объем данных, использованных в текущем месяце. Счетчик сбрасывается в полночь первого числа каждого месяца.
Превышение	Показывает объем данных за текущий месяц, превышающий установленный объем для вашего уровня обслуживания. Данная функция доступна только в случае ее активации для вашей подписки.
Соединения	Показывает серверы, подключенные с помощью Secure Remote Access.

Облачное хранилище данных

AXIS Camera Station Cloud Storage — это лицензионная услуга, которая позволяет хранить записи в облаке. Дополнительную информацию см. *AXIS Camera Station Cloud Storage — Руководство пользователя*.

Прежде чем вы сможете использовать службу облачного хранения, вам необходимо зарегистрировать свою систему в подключенных службах. После регистрации системы вы можете управлять облачным хранилищем для ваших камер в разделе My Systems (Мои системы).

Настройка сервера

Параметры сервера

Выберите в меню **Configuration > Server > Settings (Конфигурация > Сервер > Параметры)**, чтобы задать общие настройки сервера AXIS Camera Station Pro.

Примечание

При подключении к нескольким серверам AXIS Camera Station Pro выберите любой сервер в раскрывающемся меню **Selected server (Выбранный сервер)** для настройки параметров сервера.

Хранение данных	
После запуска сервера передайте право собственности на папки с записями администраторам и ограничьте доступ к ним для администраторов.	При первой установке AXIS Camera Station Pro этот параметр выбран. При обновлении AXIS Camera Station Pro этот параметр не выбран.

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

Журналы
Укажите, сколько дней должны храниться тревоги, события и аудиты. Задайте значение от 7 до 1000 дней.

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

SMTP-серверы

Добавление SMTP-серверов для отправки сообщений электронной почты при подаче сигнала тревоги в системе или при активации правила настройки событий.

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, которое будет отображаться в электронной почте 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	Выберите, если для данного сервера требуется ввести имя пользователя и пароль. Введите имя пользователя и пароль для доступа к серверу.

Изменить	Чтобы изменить параметры SMTP-сервера, выберите нужный сервер и нажмите **Изменить**.
Удалить	Чтобы удалить SMTP-сервер, выберите его и нажмите **Удалить**. В появившемся диалоговом окне нажмите **Да**, чтобы подтвердить удаление сервера.
Проверить все...	Чтобы протестировать SMTP-сервер, выберите его и нажмите **Test all... (Проверить все...)**. В появившемся диалоговом окне введите адрес электронной почты в поле **Recipient (Получатель)** и нажмите **OK**. При тестировании SMTP-сервера выдается список результатов и рекомендуемых действий.
Стрелки	Выберите сервер и с помощью стрелок измените порядок размещения серверов в списке. Серверы используются системой в порядке перечисления.

Результаты тестирования сервера	
OK	успешное подключение к SMTP-серверу. Проверьте, дошло ли до получателей тестовое сообщение по электронной почте.
Неизвестная ошибка	при отправке сообщения по электронной почте произошел непредвиденный сбой. Проверьте работоспособность SMTP-сервера.
Нет контакта	AXIS Camera Station Pro не может получить доступ к SMTP-серверу. Убедитесь, что SMTP-сервер работает правильно и что в настройках всех маршрутизаторов и прокси-серверов между AXIS Camera Station Pro и SMTP-сервером разрешен соответствующий трафик.
Ошибка конфигурации	Запрос TLS отправлен, но сервер не поддерживает StartTLS, сервер не поддерживает проверку подлинности или отсутствует совместимый механизм проверки подлинности.
Ошибка подтверждения установления связи по протоколу TLS/SSL	Ошибка при согласовании TLS/SSL, например недействительный сертификат сервера.
Требуется аутентификация	Для отправки электронной почты серверу требуется проверка подлинности.
Ошибка проверки подлинности	Неверные реквизиты для входа.
Соединение прервано	Соединение было установлено, но затем потеряно.

Системная тревога

Системная тревога возникает при потере связи с камерой, при отказе в доступе к хранилищу для записи, при неожиданном отключении сервера или при сбое в процессе записи. Можно отправлять по электронной почте уведомления о системных сигналах тревоги.

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 **Отправить сообщение по электронной почте при системной тревоге следующим получателям**, чтобы активировать отправку сообщений по электронной почте при возникновении сигнала тревоги в системе.
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 **Добавить**, чтобы добавить адрес электронной почты в поле **Получатели**.

Подключение устройства	
Продолжать использовать имена хостов, даже если они стали недоступными	Для подключения используйте имя хоста. Чтобы автоматически переключиться на подключение с помощью IP-адреса, снимите флажок. Можно вручную выбрать имя хоста или IP-адрес для подключения к устройствам. См. *Подключение, on page 73*.

Язык	
Изменить язык сервера	Изменение имени AXIS Camera Station Pro Service Control и AXIS Camera Station Secure Entry. Например: системные сигналы тревоги, сообщения журнала аудита, внешние данные на вкладке **Data search (Поиск данных)**. Изменение вступает в силу после перезапуска.

Нательные камеры	
Диск **Папка**	Выберите диск и папку для отклоненного содержимого из нательной системы. 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.	Это время хранения отклоненного содержимого.

Обратная связь	
Отправить анонимные данные об использовании сервера в компанию Axis Communications	Выберите, чтобы улучшить работу приложения и повысить его удобство для пользователей. Порядок изменения параметров клиента см. в разделе *Настройки клиента, on page 123*.

Расширенные настройки

Изменять эти настройки следует только по указанию службы поддержки Axis. Чтобы изменить расширенные настройки:

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

Чтобы включить ведение журнала отладки для устранения неисправностей, выберите **Enable server side debug logging (Включить ведение журнала отладки на стороне сервера)**. Эта настройка использует больше места на диске, также ее переопределяет значение, заданное в файле `log4net.config` в папке **ProgramData**.

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. Страница компонентов позволяет управлять компонентами и просматривать их статус.

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. Показывать компоненты и управлять ими можно только после того, как вы связались со службой поддержки Axis.

Обновить AXIS Camera Station Pro

Чтобы получить последнюю версию AXIS Camera Station Pro:

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

Примечание

- После запуска 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 управление службой временно закрываются. Во время обновления пользовательский интерфейс или индикатор выполнения отображаться не будут. Оставьте серверный компьютер включенным до тех пор, пока и клиент, и сервер не перезапустятся.

Отчет об инцидентах

Если разрешение на создание отчета об инцидентах включено, вы можете создавать отчеты об инцидентах, включая записи, моментальные снимки и примечания об инцидентах. См. *Экспорт отчетов об инцидентах, on page 33*.

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 меню **Export format (Формат экспорта)** выберите формат, в который вы хотите экспортировать записи.
4. В разделе **Categories (Категории)** добавьте или удалите категории, чтобы нужным образом сгруппировать отчеты об инцидентах. Категорией может быть имя папки в каталоге экспорта, если вы зададите категорию в качестве переменной в пути к каталогу на сервере.
   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: Автор отчета: <Insert your name, mail, and phone number (Введите свое имя, адрес электронной почты и номер телефона)>.
6. Нажмите **Применить**.

Местонахождение	
Путь к директории сервера	Выберите или введите путь к каталогу на сервере, чтобы отчеты об инцидентах сохранялись 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	Если выбран этот параметр, можно выбрать пункт **Add digital signature (Добавить цифровую подпись)**, чтобы использовать цифровую подпись, делающую невозможным вмешательство в изображение. 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

Чтобы задать расписание экспорта записей, перейдите в меню **Configuration > Server > Scheduled export (Конфигурация > Сервер > Запланированный экспорт)**

В выбранное время будут экспортироваться все записи, накопленные со времени выполнения предыдущей операции экспорта. Если предыдущий экспорт был выполнен более недели назад, либо если предыдущий экспорт отсутствует, будут экспортироваться только записи, возраст которых не превышает одну 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 можно добавлять экспорт по расписанию и управлять таким экспортом на любом из подключенных серверов. Для этого надо выбрать нужный сервер в раскрывающемся меню **Selected Server (Выбранный сервер)**.

Запланированный экспорт записей

1. Чтобы активировать экспорт по расписанию, 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. Система по умолчанию выбирает все перечисленные камеры. 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 недели, когда должен производиться экспорт 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 использовать цифровую подпись для защиты от изменения изображения. 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 2008 Server

Для экспорта записей с сервера, работающего под управлением ОС Microsoft Windows 2008 Server, необходимо установить компонент Desktop Experience:

1. Перейдите в меню **Пуск > Администрирование > Управление сервером** и откройте окно «Диспетчер сервера».
2. В разделе **Features Summary (Функции)** нажмите **Add features (Добавить функции)**.
3. Выберите **Desktop Experience (Возможности рабочего стола)** и нажмите **Next (Далее)**.
4. Щелкните **Установить**.

Microsoft Windows 2012 Server

Для экспорта записей с сервера, работающего под управлением ОС Microsoft Windows 2012 Server, необходимо установить компонент 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	Данная опция включает локальный TURN-сервер на сервере AXIS Camera Station Pro. Выберите **Enable TURN (Активировать TURN)**, если вы хотите, чтобы коммуникация WebRTC могла осуществляться через единственный порт, что упрощает настройку брандмауэра.
Prioritize TURN (Приоритет TURN)	Отметьте эту опцию, если вы хотите, чтобы WebRTC рассматривал только ретранслируемых кандидатов для установления соединения.

Новое соединение

Перейдите к пункту ☰ **> Servers > New connection (Серверы > Новое соединение)**, чтобы подключиться к серверу AXIS Camera Station Pro. См. *Подключить к серверу*.

Состояние соединения

Перейдите в меню ☰ **> Servers > Connection status (Серверы > Состояние соединения)** для отображения списка с указанием состояний соединения всех серверов.

Используйте ползунок перед именем сервера, чтобы подключиться или отключиться от сервера.

Коды состояния	Описание	Возможные решения
Подключение	Клиент пытается установить соединение с сервером.	
Подключено	Клиент подключен к серверу по протоколу TCP.	
Подключено (с помощью Secure Remote Access)	Клиент подключен к этому серверу с помощью Secure Remote Access.	
Подключено (по 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 разрывает соединение с сервером.	
Отключено	Отсутствует соединение между клиентом и сервером.	
Переподключение	Клиент пытается восстановить разорванное соединение с сервером.	

Ошибка при пересоединении	Клиенту не удалось восстановить разорванное соединение с сервером. Сервер найден, но, возможно, были изменены права доступа или пароль пользователя.	• Укажите пользователя в диалоговом окне полномочий. • 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.	Укажите пользователя в диалоговом окне полномочий.
Проверка безопасности завершилась ошибкой	Не удалось проверить защиту по WCF. Обязательно синхронизируйте время UTC на клиентском и серверном компьютере.	
Нет связи с серверным компьютером	Нет отклика от серверного компьютера по указанному адресу.	• Убедитесь, что сеть нормально функционирует. • Убедитесь, что сервер работает.
Нет работающего сервера	Компьютер, на котором установлен сервер, доступен, однако сервер на нем не работает.	Запустите сервер.
Ошибка связи	Ошибка подключения к серверу. Проверьте, доступен ли компьютер, работающий как сервер.	• Убедитесь, что сеть нормально функционирует. • Убедитесь, что сервер работает.
Недопустимое имя хоста	DNS не может преобразовать имя хоста в IP-адрес.	• Убедитесь, что имя хоста введено без ошибок. • Проверьте полноту информации, передающейся на DNS.
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.	Обновите список серверов для подключения к нужному серверу.
Версия клиента (x) несовместима с версией сервера (y)	Клиентское ПО устарело или, наоборот, слишком новое, по сравнению с серверным ПО.	Проследите за установкой на клиентском и на серверном компьютерах одной и той же версии ПО AXIS Camera Station Pro.
Сервер перегружен	Нет отклика от сервера из-за проблем с производительностью.	Проверьте, не перегружены ли сеть и компьютер, на котором установлен сервер.

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.

Чтобы открыть диалоговое окно со списками серверов, выберите > **Servers (Серверы) > Server lists (Списки серверов)**.

По умолчанию отображается список **Recent connections (Недавние подключения)** — в нем представлены серверы, с которыми устанавливалось соединение в ходе предыдущего сеанса. **Недавние подключения** удалить невозможно.

	Выберите список серверов и щелкните .
+ Новый список серверов	Нажмите, чтобы составить новый список серверов, а затем дайте новому списку название.
Добавить	Для добавления сервера в список серверов выберите нужный список и нажмите кнопку Add (Добавить). Введите необходимую информацию.
Экспорт списков	Нажмите для экспорта всех списков серверов в виде файла .msl. Для входа на серверы можно импортировать список серверов. См. *Подключить к серверу*.
Изменить	Чтобы изменить сервер, выберите его и нажмите **Edit (Изменить)**. За один раз можно изменить только один сервер.
Удалить	Для удаления серверов из списка выберите их и нажмите **Remove (Удалить)**.
Переименовать сервер	Нажмите список серверов два раза и введите новое название списка.

Организация серверов в списках серверов

Configure switch (Настройка коммутатора)

При наличии устройства серии S22 Appliance AXIS Camera Station можно настроить его из AXIS Camera Station Pro. Для открытия страницы управления коммутатором на клиенте **перейдите в раздел** Configuration > Switch > Management (Конфигурация > Коммутатор > Управление) AXIS Camera Station Pro и введите свои реквизиты для входа. Инструкции по настройке коммутатора см. в руководстве пользователя AXIS Camera Station S22 Appliance на сайте *axis.com*.

Примечание

AXIS Camera Station Pro может соединиться только с адресом https://192.168.0.1/ (это принимаемый по умолчанию IP-адрес коммутатора).

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 времени система полностью функциональна, что позволяет настроить ее и опробовать все возможности перед приобретением лицензий.
Проверьте свои лицензии	Если срок действия лицензии системы истекает без автоматического продления, AXIS License Manager предоставляет дополнительный 30-дневный льготный период.
Требуется лицензия	Система полностью лицензирована и работоспособна до наиболее ранней даты истечения срока действия.
Изменения, внесенные в систему, требуют синхронизации лицензии	При добавлении устройств в лицензированную систему AXIS Camera Station Pro пытается синхронизировать эти изменения с AXIS License Manager для переоценки статуса лицензии. При автоматическом лицензировании этот процесс может быть незаметным. Однако при ручном лицензировании, если не синхронизировать изменения с AXIS License Manager в течение 60 дней, система перейдет в нелицензированное состояние.
Нет лицензий	Система остается работоспособной, но с ограниченным функционалом. Запись и правила действий продолжают работать, и существующие записи не будут утеряны. Следующие функции работать не будут: • Потоки живого видео • Воспроизведение записей • Мгновенное воспроизведение • Стоп-кадры • Экспорт записей

Лицензирование системы возможно двумя способами:

Автоматическое лицензирование (для онлайн-систем) – При данном варианте система автоматически передает в AXIS License Manager изменения, влияющие на количество лицензий, и получает обновленный

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 ручном лицензировании необходимо вручную экспортировать файл системы, загрузить его в AXIS License Manager и импортировать новую лицензию обратно в систему. Эту процедуру нужно повторять после любых изменений, влияющих на количество лицензий. 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 143*.

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 > Security > User permissions (Конфигурация > Безопасность > Права доступа пользователей)**, чтобы увидеть пользователей и группы, существующие в AXIS Camera Station Pro.

Примечание

Администраторы компьютера, на котором работает сервер AXIS Camera Station Pro, автоматически получают права администратора системы AXIS Camera Station Pro. Права доступа группы администраторов нельзя изменить или удалить.

Прежде чем добавлять пользователя или группу, необходимо зарегистрировать этого пользователя или группу на локальном компьютере или получить учетную запись Windows® Active Directory. Чтобы добавить пользователя или группу, см. *Добавление пользователей или групп*.

Если пользователь входит в группу, то он получает максимальные для данной роли права, которые назначаются отдельному человеку или группе. Если пользователю предоставляются индивидуальные права, то он также получает права доступа, предусмотренные для группы. Например, пользователь получает индивидуальный доступ к камере X. Пользователь также является членом группы, имеющей доступ к камерам Y и Z. Таким образом, пользователь будет иметь доступ к камерам X, Y и Z.

	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 в отношении прав доступа, предоставляемая пользователю или группе. Возможные значения роли: администратор, оператор и наблюдатель.
Сведения	Подробная информация о пользователе в том виде, как она отображается на локальном компьютере или в Active Directory.
Сервер	Сервер, к которому относится пользователь или группа.

Добавление пользователей или групп

Доступ к AXIS Camera Station 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 к разделу **Local Users and Groups (Локальные пользователи и группы)** > **Users (Пользователи)**.
- Щелкните правой кнопкой мыши на **Users (Пользователи)** и выберите **New User (Новый пользователь)**.
- Во всплывающем диалоговом окне введите данные нового пользователя и снимите флажок **User must change password at next login (Пользователь должен изменить пароль при следующем входе)**.
- Нажмите **Create (Создать)**.

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

Добавление пользователей или групп

1. Перейдите в меню **Configuration (Конфигурация) > Security (Безопасность) > User permissions (Разрешения пользователей)**.
2. Нажмите **Добавить**.
   Доступные пользователи и группы содержатся 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 найдено слишком много пользователей или групп, результаты поиска не отображаются. Воспользуйтесь функцией фильтра.
5. Выберите пользователей или группы и нажмите **Добавить**.

Область действия	
Сервер	Выберите для поиска пользователей или групп на локальном компьютере.
Домен	Выберите для поиска пользователей или групп Active Directory.
Выбранный сервер	При подключении к нескольким серверам AXIS Camera Station Pro выберите сервер в раскрывающемся меню **Selected server (Выбранный сервер)**.

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. О том как определить роль для пользователя или группы, см. *Добавление пользователей или групп*.

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

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	разрешен запуск и остановка записей вручную.
Механическое управление позиционером (PTZ)	разрешен доступ к механическому PTZ-управлению. Доступно только для камер с механическим PTZ-управлением.
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	Разрешить изменение видов 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	разрешено просматривать состояние порта ввода-вывода. Пользователь не может менять состояние порта.
Запись	разрешено менять состояние порта ввода-вывода.

Система

Невозможно настроить права доступа, выделенные в списке серым цветом. Если напротив названия права установлен флажок, это значит, что пользователь или группа обладают этим правом 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	Разрешить делать снимки в режимах живого просмотра и записи.
Экспорт записей	Разрешить 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). При поиске пользователь не будет получать результатов старше указанного времени.
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.

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	Только для оператора. Позволяет выполнить конфигурирование AXIS Audio Manager Pro в AXIS Camera Station Pro и доступ к интерфейсу сервера AXIS Audio Manager Pro.
Доступ к интерфейсу AXIS Audio Manager Pro	Только для наблюдателя. Позволяет получить доступ к интерфейсу сервера AXIS Audio Manager Pro.

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	Разрешить настройку системы контроля работоспособности системы.
Доступ к контролю работоспособности системы	Разрешить доступ к системе контроля работоспособности системы.

Сертификаты

Для управления настройками сертификатов между сервером AXIS Camera Station Pro и устройствами выберите **Configuration > Security > Certificates (Конфигурация > Безопасность > Сертификаты)**.

Дополнительные сведения о включении, удалении и просмотре сертификатов HTTPS и IEEE 802.1X см. в разделе *Безопасность, on page 72*.

AXIS Camera Station Pro может выполнять одну из указанных ниже функций.

- **Корневой центр сертификации (ЦС).** Использование AXIS Camera Station Pro в качестве корневого центра сертификации. Выступая в данном качестве, AXIS Camera Station Pro использует свой собственный корневой сертификат для выдачи сертификатов сервера, при этом какие-либо другие корневые ЦС в этом процессе участия не принимают.
- **Промежуточный центр сертификации.** При таком сценарии необходимо импортировать сертификат ЦС и его закрытый ключ в AXIS Camera Station Pro для подписи и выдачи сертификатов сервера для устройств Axis. Этот сертификат ЦС может быть корневым сертификатом либо сертификатом промежуточного ЦС.

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 для импорта существующего сертификата ЦС и его закрытого ключа. AXIS Camera Station Pro сохраняет свой пароль.
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 приводит к перезапуску всех компонентов.
Вид	Нажмите, чтобы просмотреть подробные сведения о сертификате ЦС.

Экспорт	Нажмите, чтобы экспортировать CA в файл. Вы можете экспортировать его двумя способами: • **Без личного 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 личным 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). Обратите внимание, что ЦС не подписывает сертификаты, действительные после истечения срока действия.

Создание корневого ЦС

При запуске AXIS Camera Station Pro ищет ЦС. Если он отсутствует, автоматически генерируется корневой ЦС. 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 150*.

При обновлении с версии 5.45 или более ранней, в которой используется установленный вручную сертификат на устройстве, AXIS Camera Station Pro автоматически установит новый сертификат, используя существующий корневой ЦС, когда срок действия сертификата, установленного вручную, истечет.

Примечание

При создании сертификата ЦС он добавляется в раздел «Доверенные корневые сертификаты Windows».

Импорт центра сертификации

При установке сертификата ЦС из другого центра сертификации вы можете использовать AXIS Camera Station Pro в качестве промежуточного ЦС. Импортируйте существующий ЦС, состоящий из сертификата и закрытого ключа, чтобы позволить AXIS Camera Station Pro подписывать сертификаты от имени этого ЦС. Файл должен быть в формате PKCS#12, а сертификат должен иметь основное ограничение (2.5.29.19), указывающее на то, что это сертификат ЦС, который должен использоваться в течение срока его действия. Чтобы импортировать ЦС для замены существующего, см. раздел *Замена ЦС, on page 150*.

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 кнопку **OK**.
- При импорте сертификата ЦС он добавляется в раздел «Доверенные корневые сертификаты Windows».
- 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 (Проверка сертификата 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 раздел **Configuration (Конфигурация) > Security (Безопасность) > Certificates (Сертификаты) > HTTPS** и включите **Validate device certificate (Проверить 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	Включите эту опцию, если сертификат будет использоваться для подтверждения подлинности сервера. Как правило, для устройств и других конечных точек, с которыми AXIS Camera Station Pro взаимодействует по HTTPS, применяются серверные сертификаты с включенной аутентификацией сервера.
Аутентификация клиента	Активируйте этот параметр, если сертификат будет использоваться клиентом для подтверждения своей личности перед подключением к серверу. Например, устройства, запрашивающие доступ к сети с контролем

Создание сертификата	
	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 валидирует подпись действующего сертификата сервера HTTPS на каждом подключенном устройстве и не подключается к устройству, если его сертификат не валидирован. Сертификат сервера должен быть подписан действующим ЦС в AXIS Camera Station Pro или валидирован посредством хранилища сертификатов Windows. AXIS Camera Station Pro также проверяет соответствие адреса в сертификате HTTPS устройства адресу, используемому для обмена данными с устройством, если активирован параметр **Validate device address (Проверка адреса устройства)**.

Камеры со встроенным ПО версии 7.20 или выше поставляются с предварительно настроенной конфигурацией, включающей самозаверяющий сертификат. Эти сертификаты не будут 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 разрешить подключение только для устройств с действительным сертификатом. Без проверки сертификата вы разрешаете доступ к устройствам с недействительным сертификатом.
Проверка адреса устройства	Отключите для стабильной работы в сетях DHCP без использования имен хостов. Включите эту опцию, чтобы проверять соответствие адресов для обеспечения дополнительной безопасности. Рекомендуется включать эту настройку только в тех сетях, где устройства в основном обмениваются данными с использованием имени хоста, или устройства имеют статический IP-адрес.

Примечание

- Если защищенное соединение (HTTPS) недоступно, вы можете выпустить новый сертификат HTTPS. См. *Добавить устройства, on page 47*
- 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 (т. е. типа «Базовый») не поддерживаются. Чтобы была возможна связь для дайджест-проверки подлинности, для устройств должен быть установлен режим «Encrypted & unencrypted» («С шифрование и без шифрования») или «Encrypted only» («Только с шифрованием»).
- Нельзя включить HTTPS на сетевых коммутаторах AXIS T85 PoE+ Network Switch Series.

IEEE 802.1X

Для проверки подлинности AXIS Camera Station Pro IEEE 802.1X запрашивающая сторона заявляет сетевое устройство Axis, которое требуется подключить 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 от внешнего источника, например с сервера аутентификации по стандарту IEEE 802.1X, или непосредственно в AXIS Camera Station Pro. Этот сертификат будет установлен на каждом устройстве Axis и будет использоваться 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 меню **EAPOL Version (Версия EAPOL)** выберите, какую версию протокола EAP (Extensible Authentication Protocol) вы хотите использовать.
3. В раскрывающемся меню **EAP identity (Идентификатор EAP)** выберите использование MAC-адреса устройства, имени хоста устройства или пользовательского текста.
4. Если выбран вариант **Custom (Настроить)**, введите в поле **Custom (Настроить)** любой текст, который будет служить идентификатором EAP.
5. Нажмите **Import (Импорт)** и выберите файл сертификата ЦС для проверки подлинности IEEE 802.1X.
6. В раскрывающемся меню **Common name (Общее имя)** выберите использование **Device IP address (IP-адрес устройства)** или **Device EAP identity (EAP-идентификатор устройства)** в качестве общего имени в отдельных сертификатах, которые создаются для каждого устройства, когда AXIS Camera Station Pro выступает в качестве центра сертификации.
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 без параметра `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 (т. е. типа «Базовый») не поддерживаются. Чтобы была возможна связь для дайджест-проверки подлинности, для устройств должен быть установлен режим «Encrypted & unencrypted» («С шифрование и без шифрования») или «Encrypted only» («Только с шифрованием»).

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 окончании срока действия сертификата)** укажите, за сколько дней до истечения срока действия AXIS Camera Station Pro пришлет соответствующее уведомление.

Продление сертификата

Продление действия сертификата между сервером и устройствами

Клиентские или серверные сертификаты устройства, генерируемые AXIS Camera Station Pro, автоматически обновляются в течение 7 дней до того, как будет отображаться предупреждение об истечении срока действия. Для этого вы должны включить на устройстве протокол HTTPS или IEEE 802.1X. Если вы хотите обновить или продлить сертификат вручную, см. раздел *Безопасность, on page 72*.

Продление действия сертификата между сервером и клиентом

Новый серверный сертификат можно сгенерировать во вкладке Certificates (Сертификаты) в панели управления службой AXIS Camera Station Pro. Указания о том, как это сделать, см. в разделе *Сертификаты, on page 236*.

Сброс пароля

1. Перейдите в раздел **Configuration > Security > Certificates (Конфигурация > Безопасность > Сертификаты)**.
2. Отключите параметр **Validate device certificate (Проверка сертификата устройства)**, чтобы обеспечить доступность устройств, использующих сертификаты удостоверяющего центра (CA).
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 (Проверка сертификата 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 AXIS OS контроллера через меню **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. Чтобы изменить существующий предустановленный профиль идентификации или создать новый профиль идентификации, см. *Профили идентификации, on page 171*.
2. Чтобы использовать пользовательскую настройку для форматов карт и длины PIN-кода, см. *Форматы карт и ПИН-коды, on page 173*.
3. Добавьте дверь и примените профиль идентификации к двери. См. *Добавление двери, on page 156*.
4. Настройте дверь.
   - *Добавление дверного монитора, on page 163*
   - *Добавить вход чрезвычайной ситуации, on page 164*
   - *Добавление считывающего устройства, on page 165*
   - *Добавление REX-устройства, on page 167*
5. Добавьте зону и добавьте двери в зону. См. *Добавление зоны, on page 168*.

Совместимость программного обеспечения устройств для дверных контроллеров

Внимание

При обновлении AXIS OS на дверном контроллере следует помнить следующее:

- **Поддерживаемые версии AXIS OS:** Поддерживаемые версии AXIS OS, перечисленные ниже применимы только при обновлении с изначально рекомендованной версии AXIS Camera Station Pro и если в системе имеется дверь. Если система не соответствует этим условиям, необходимо обновить ее до версии AXIS OS, рекомендованной на сайте для конкретной версии AXIS Camera Station Pro.
- **Минимальная поддерживаемая версия AXIS OS:** Самая старая версия AXIS OS, установленная в системе, определяет минимально поддерживаемую версию AXIS OS, но не более чем на две версии ниже текущей. Предположим, вы используете AXIS Camera Station Pro версии 6.5 и обновили все устройства до рекомендуемой версии AXIS OS 12.0.86.2. Тогда версия AXIS OS 12.0.86.2 становится минимально поддерживаемой версией для вашей системы в дальнейшем.
- **Обновление до версии AXIS OS, превышающей рекомендованную:** Предположим, вы обновили AXIS OS до версии , превышающей рекомендованную для конкретной версии AXIS Camera Station Pro. При этом вы всегда можете понизить версию обратно до рекомендованной версии AXIS OS, если она находится в пределах поддержки , установленной для версии AXIS Camera Station Pro.
- **Рекомендации по AXIS OS на будущее:** Для обеспечения стабильности и полной совместимости системы всегда следуйте рекомендациям для версии AXIS OS в соответствии с версией AXIS Camera Station Pro.

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 6.13	12.5.68.1	12.6.102.1
Pro 6.12	12.2.63.13	12.6.94.1
Pro 6.11	12.0.101.4	12.5.68.1

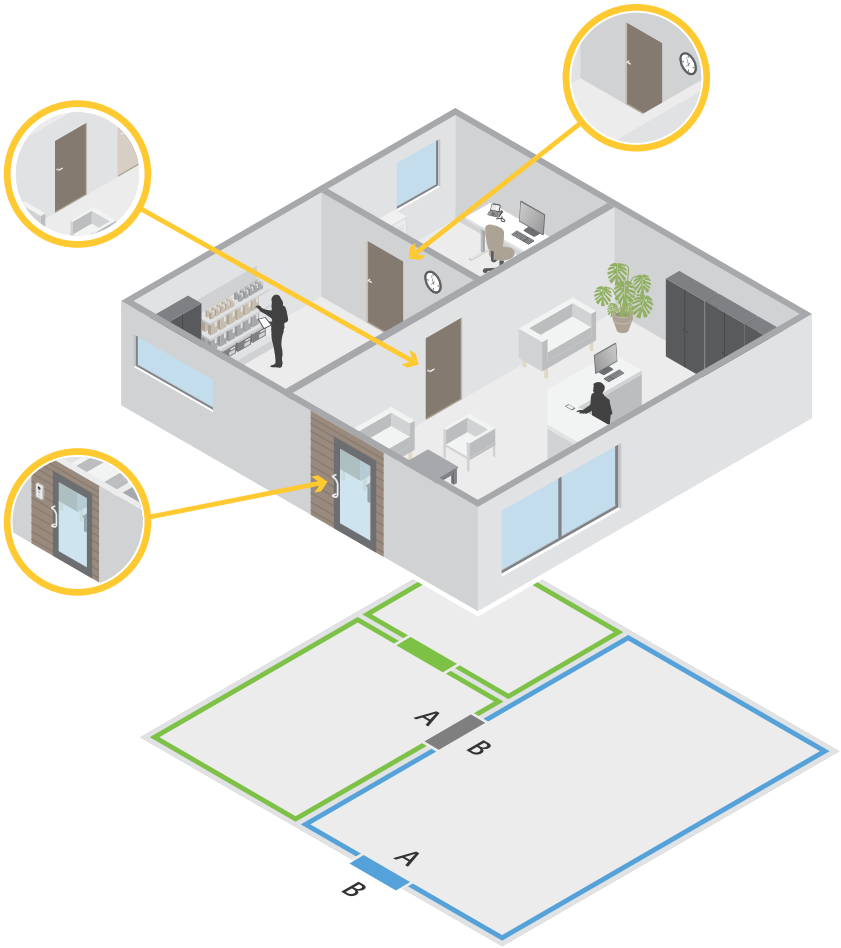
Двери и зоны

Перейдите в раздел **Configuration > Access control > Doors and zones (Конфигурация > Контроль доступа > Двери и зоны > Зоны)**, чтобы получить обзор и настроить двери и зоны.

Схема контактов	Посмотреть схему контактов контроллера, связанную с дверью. Если схему контактов нужно распечатать, нажмите **Print (Печать)**.
Профиль идентификации	Изменить профиль идентификации для дверей.
Защищенный канал	Включение или выключение защищенного канала OSDP Secure Channel для конкретного считывателя.

Двери	
Название	Имя двери.
Дверной контроллер	Дверной контроллер, к которому подключена дверь.
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.
Форматы карт и ПИН-коды	Показывает тип формата карты или длину PIN-кода.
Статус	Состояние двери. • **Online (Онлайн):** Дверь находится в режиме онлайн и работает корректно. • **Reader offline (Считыватель в автономном режиме):** считыватель в конфигурации двери находится в автономном режиме. • **Reader error (Ошибка считывателя):** Считыватель в конфигурации двери не поддерживает защищенный канал, или защищенный канал выключен для считывателя.
Зоны	
Название	Имя зоны.
Количество дверей	Количество дверей, включенных в зону.

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.

Добавление двери

Примечание

- Для дверного контроллера можно настроить одну дверь с двумя замками либо же две двери с одним замком в каждой.
- Если дверной контроллер не имеет дверей, и вы используете новую версию AXIS Camera Station Pro со старой прошивкой на дверном контроллере, система не позволит вам добавить дверь. Однако система разрешает добавлять новые двери на системные контроллеры со старой прошивкой при наличии уже существующей двери.

Создание новой конфигурации двери для добавления двери:

1. Перейдите в **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
2. Нажмите + **Add door (Добавить дверь)** и выберите дверь в раскрывающемся списке.

Типы дверей	
Дверной датчик	Обычная дверь с контролем состояния двери, поддерживающая замки и считывающие устройства. Требуется дверной контроллер.
Беспроводная сеть	Дверь, которую можно настроить с беспроводными замками и коммуникационными хабами ASSA ABLOY Aperio®. Подробнее см. в разделе *Добавление беспроводной блокировки, on page 161*.
Контролируемая дверь	Дверь, которая может сообщать, открыта она или закрыта. Подробнее см. в разделе *Добавление двери с мониторингом, on page 163*.
Выделенная дверь	Дверь, которую можно добавить как резервное устройство в системе без необходимости выбора оборудования.
Этаж	Тип двери для управления лифтом с аутентификацией доступа с помощью считывающего устройства. Для получения дополнительной информации см. раздел *Добавление этажа для управления лифтом BETA, on page 164*.

3. Введите имя двери и выберите контроллер двери в раскрывающемся списке **Device (Устройство)** для привязки к двери. Контроллер отображается серым цветом, когда вы не можете добавить другую дверь, когда он находится в режиме офлайн либо если HTTPS не активен.
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 171*.
8. Настройте параметры двери. См. *Настройки двери, on page 158*.
9. *Добавление дверного монитора, on page 163*
10. *Добавить вход чрезвычайной ситуации, on page 164*
11. *Добавление считывающего устройства, on page 165*
12. *Добавление REX-устройства, on page 167*
13. Настройка уровня безопасности. См. *Уровень безопасности двери, on page 159*.
14. Нажмите **Сохранить**.

Чтобы добавить дверь, скопируйте существующую конфигурации двери:

1. Перейдите в **Configuration (Конфигурация) > Access control (Контроль доступа) > Doors and zones (Двери и зоны)**.
2. Нажмите + **Add door (Добавить дверь)**.
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 **Сохранить**.

Чтобы изменить параметры двери:

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 кнопку **Edit (Изменить)**.
4. Измените значения параметров и нажмите **Save (Сохранить)**.

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. Выберите пункт **Remove (Удалить)**.
4. Нажмите **Да**.

Добавление и настройка дверей и зон

Настройки 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)**.

Время доступа (с)	Задайте время (количество секунд), в течение которого дверь должна оставаться отпертой после предоставления доступа. Дверь будет оставаться отпертой, пока она не будет открыта или пока не истечет заданное время. Дверь блокируется при закрытии, даже если время доступа еще не истекло.
Open-too-long time (sec) (Время «открыта слишком долго» (с))	Действует, только если настроен дверной монитор. Установите количество секунд, в течение которых дверь остается отпертой. Если дверь открыта по истечении установленного времени, это вызывает сигнал тревоги, соответствующий событию «Открыта слишком долго». Задайте правило действия, чтобы определить, какое действие будет запускаться событием «Открыта слишком долго».

Длительное время доступа (сек)	Задайте время (количество секунд), в течение которого дверь должна оставаться отпертой после предоставления доступа. Длительное время доступа применяется вместо заданной длительности доступа для владельцев карт, для которых включен этот параметр.
Long open-too-long time (sec) (Длительное время «открыта слишком долго» (с))	Действует, только если настроен дверной монитор. Установите количество секунд, в течение которых дверь остается отпертой. Если дверь открыта по истечении установленного времени, это вызывает сигнал тревоги, соответствующий событию «Открыта слишком долго». Длительное время до подачи сигнала тревоги «Открыта слишком долго» применяется вместо заданного времени «открыта слишком долго» для владельцев карт, если активирована настройка **Длительное время доступа**.
Время задержки повторного запирания (мс)	Настройте время в миллисекундах, в течение которого дверь остается незапертой после ее открытия или закрытия.
Повторная блокировка	• **После открытия:** Действует, только если добавлен дверной монитор. • **After closing (После закрытия):** Действует, только если добавлен дверной монитор.
Дверь открыта силой	Выберите, будет ли система подавать сигнал тревоги, если дверь была открыта силой.
Дверь открыта слишком долго	Выберите, будет ли система подавать сигнал тревоги, если дверь оставалась открытой слишком долго.

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 проведение карты позволяет владельцу карты изменить текущее состояние двери. Например, с помощью этой функции можно заблокировать или разблокировать дверь вне установленного расписания, что удобнее, чем вручную менять статус двери в системе. Двойной свайп не влияет на существующее расписание. Например, если расписание предусматривает блокировку двери при закрытии, и сотрудник уходит на обеденный перерыв, дверь все равно будет заблокирована согласно расписанию.

Можно настроить уровень безопасности при добавлении новой двери или для уже 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**.

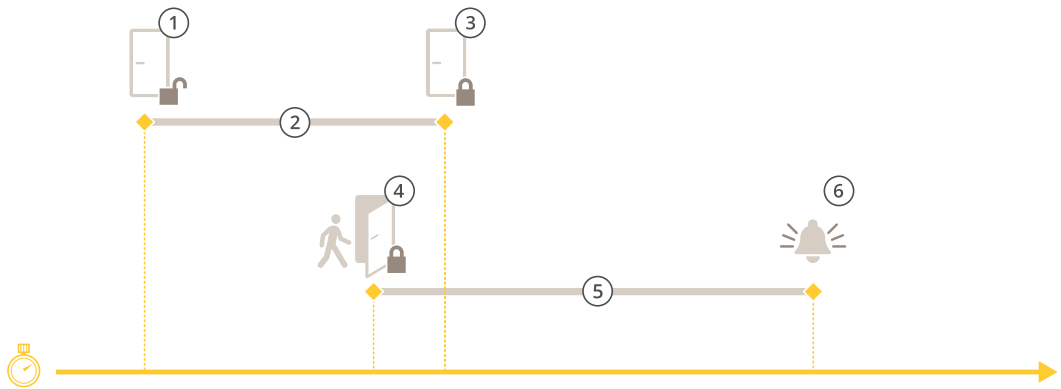
Правило двух человек	
Сторона A и сторона B	Выберите, с какой стороны двери будет использоваться правило.
Расписания	Выберите время, в которое будет действовать правило.
Время тайм-аута (в секундах)	Тайм-аут — это максимально допустимое время между считываниями карт или вводом других действительных учетных 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**.

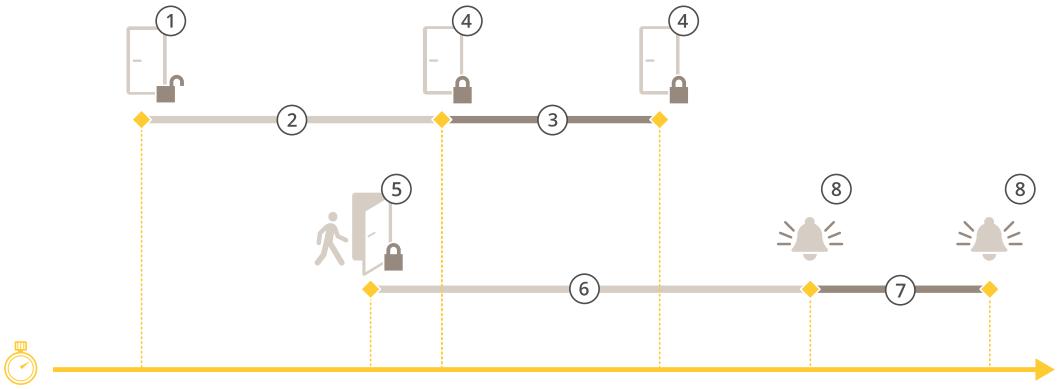
Двойной свайп	
Время тайм-аута (в секундах)	Тайм-аут — это максимально допустимое время между считываниями карт или вводом других действительных учетных данных.

Параметры времени



1 Доступ предоставлен — замок отпирается

2 *Время доступа*
3 *Никаких действий не предпринято — замок запирается*
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 *Никаких действий не предпринято — замок запирается*
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 ASSA ABLOY Aperio® беспроводные блокировки и концентраторы. Беспроводная блокировка подключается к системе через концентратор Aperio, подсоединенный к разъему RS485 дверного контроллера. Для одного дверного контроллера можно подключить до 16 беспроводных блокировок.

Для просмотра видео откройте веб-версию данного документа.

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.
- Необходимо синхронизировать время на дверном контроллере Axis и на сервере AXIS Camera Station Pro.
- Прежде чем начать работу, необходимо выполнить сопряжение блокировок Aperio с концентратором Aperio, используя прикладное средство с поддержкой технологии ASSA ABLOY.
- Если беспроводные блокировки находятся в автономном режиме, они не будут следовать расписанию отпирания.

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. Нажмите **Add door (Добавить дверь)**.
   4.3. Выберите дверной контроллер, подключенный к концентратору Aperio, выберите **Wireless door (Дверь с беспроводным управлением)** в качестве значения **Door type (Тип двери)**.
   4.4. Нажмите **Next** (“Далее“).
   4.5. Выберите **Wireless lock (Беспроводная блокировка)**.
   4.6. Определите стороны двери A и B и добавьте нужные датчики. Дополнительные сведения см. в разделе *Двери и зоны, on page 155*.
   4.7. Нажмите **Сохранить**.

Подключив беспроводную блокировку, можно посмотреть уровень заряда аккумулятора и его состояние в обзоре дверей.

Уровень заряда аккумулятора	Действие
Хорошо	Нет
Низкая	Блокировка работает как положено, но следует заменить аккумулятор до того, как уровень его заряда станет критическим.
Критические ошибки	Замените аккумулятор. Блокировка, возможно, работает неправильно.

Состояние замка	Действие
Дистанционное обучение	Нет
Заклинивание замка	Устраните любые механические проблемы с замком.

Добавление дверного монитора

Дверной монитор — это датчик положения двери, который контролирует физическое состояние двери. Можно добавить дверной монитор к двери и настроить способ его подключения.

1. Перейдите на страницу конфигурации двери. См. *Добавление двери, on page 156*.
2. В разделе **Sensors (Датчики)** нажмите **Add (Добавить)**.
3. Выберите **Door monitor sensor (Датчик дверного монитора)**.
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 прерывании соединения между дверным контроллером и дверным монитором инициировалось событие, включите параметр **Supervised input (Контролируемый вход)**. См. *Контролируемые входы, on page 170*.

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**.

Добавление этажа для управления лифтом 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 инструкций по подключению вашего модуля к контроллеру см.

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 (Конфигурация) > Access control (Контроль доступа) > Doors and zones (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. Обратите внимание, что эта опция доступна только в том случае, если ваш контроллер оснащен реле.
8. Нажмите **Save (Сохранить)** после добавления этажа. Названия этажей отображаются в формате «Название лифта — Название этажа». Например: «Западная сторона — Этаж 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.

Добавить вход чрезвычайной 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. *Добавление двери, on page 156*.
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 считывающего устройства

Можно настроить дверной контроллер на использование двух проводных считывающих устройств. Вы можете добавить считывающее устройство только с одной стороны или с обеих сторон двери.

Если к считывающему устройству применена пользовательская настройка для форматов карт или длины PIN-кода, это наглядно отображается в столбце **Card Formats (Форматы карт)** в разделе **Configuration > Access control > Doors and zones (Конфигурация > Контроль доступа > Двери и зоны)**. См. *Двери и зоны, on page 155*.

Примечание

- Также к одному контроллеру можно подключить до 16 Bluetooth-считывателей. Подробнее см. в разделе *Добавление считывающего Bluetooth-устройства, on page 167*.
- Если вы используете систему сетевой видеосвязи Axis в качестве IP-считывателя, система использует конфигурацию PIN-кода, заданную на веб-странице устройства.

1. Перейдите на страницу конфигурации двери. См. *Добавление двери, on page 156*.
2. Для одной стороны двери нажмите **Add (Добавить)**.
3. Выберите **Card reader (Устройство для считывания карт)**.
4. Выберите **Reader type (Тип считывающего устройства)**.
5. Использование пользовательской настройки длины PIN-кода для данного 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. Значок предупреждения отображается в клиенте, когда настройка формата карты отличается от настройки, заданной в конфигурации системы.

7. Нажмите **Добавить**.

8. Для добавления считывающего устройства на другой стороне двери еще раз повторите эту процедуру.

Для получения информации о настройке считывателя штрих-кодов AXIS см. раздел *Настройка считывателя штрих-кодов AXIS*.

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. Сведения о требованиях и поддерживаемых устройствах см. в разделе *Считыватель IP-адресов, on page 167*.

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 активное состояние входа сигнала несанкционированного доступа (взлома) для считывателя. • **Open circuit (Разомкнутая цепь)**: Считывающее устройство отправляет на дверь сигнал несанкционированного доступа (взлома), когда цепь разомкнута. • **Closed circuit (Замкнутая цепь)**: Считывающее устройство отправляет на дверь сигнал несанкционированного доступа (взлома), когда цепь замкнута.
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 170*.

Добавление считывающего Bluetooth-устройства

Вы можете использовать AXIS A4612 Network Bluetooth Reader для расширения лимита проводных дверей в контроллерах доступа Axis. Контроллер может управлять до 16 такими считывателями, каждому из которых может быть назначена своя дверь. Каждый считыватель способен управлять замком двери, кнопкой выхода (REX) и датчиком положения двери (DPS).

Добавление и использование этих считывающих устройств не требует дополнительной лицензии.

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 191*.
2. Перейдите на страницу конфигурации двери. См. раздел *Добавление двери, on page 156*.
3. Для одной стороны двери нажмите **Add (Добавить)**, затем **Card reader (Устройство для считывания карт)**.
4. Выберите **IP-считыватель**, затем выберите сопряженный AXIS A4612 из выпадающего списка. Если это считывающее устройство будет использоваться для сопряжения учетных данных, отметьте его как предназначенное 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).

Считыватель IP-адресов

В AXIS Camera Station Secure Entry в качестве IP-считывателя можно использовать сетевой домофон Axis.

Примечание

- Для этого требуется AXIS Camera Station 5.38 или более поздней версии и сетевой дверной контроллер AXIS A1601 Network Door Controller со встроенным ПО версии 10.6.0.2 или более поздней версии.
- Для использования домофона в качестве IP-считывателя никакой его специальной настройки не требуется.

Поддерживаемые устройства:

- Сетевой видеодомофон AXIS A8207-VE Network Video Door Station со встроенным ПО версии 10.5.1 или более поздней версии
- Сетевой видеодомофон AXIS A8207-VE Mk II Network Video Door Station со встроенным ПО версии 10.5.1 или более поздней версии
- AXIS I8116-E Network Video Intercom

Добавление REX-устройства

Вы можете по своему усмотрению добавить REX-устройство только с одной стороны двери или с обеих сторон. В качестве REX-устройства может использоваться пассивный ИК-датчик, REX-кнопка или толкающий рычаг.

1. Перейдите на страницу конфигурации двери. См. *Добавление двери, on page 156*.
2. Для одной стороны двери нажмите **Add (Добавить)**.
3. Выберите **REX-устройство**.
4. Выберите порт ввода-вывода, к которому вы хотите подключить REX-устройство. Если доступен только один порт, он будет выбран 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 прерывании соединения между дверным контроллером и REX-устройством инициировалось событие, включите параметр **Supervised input (Контролируемый вход)**. См. *Контролируемые входы, on page 170*.

Действие	
Отпереть дверь	Выберите, чтобы отпереть дверь при приеме сигнала REX.
Нет	Выберите этот вариант, если при поступлении сигнала REX на дверь не должно выполняться никаких действий.

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 по периметру).** Владельцы карт входят в зону через эту дверь и покидают зону через нее же.
- **Internal door (Внутренняя дверь).** Внутренняя дверь внутри зоны.

Примечание

Дверь по периметру может принадлежать двум зонам. Внутренняя дверь может принадлежать только одной зоне.

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. Для двери по периметру по умолчанию устанавливается, что для входа в зону используется сторона двери A. Чтобы изменить сторону, выберите **Leave (Выход)** в раскрывающемся меню.
8. Для удаления двери из зоны выберите нужную дверь и нажмите **Remove (Удалить)**.
9. Нажмите **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. Человек должен будет сначала выйти из зоны, прежде чем он сможет снова использовать свои учетные данные.

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.

Можно настроить уровень безопасности при добавлении новой зоны или для уже существующей зоны. 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 функции безопасности, которые требуется добавить для двери.
6. Нажмите **Применить**.

Запрет на повторный проход	
Log violation only (Soft) (Только нарушение в журнале (мягкое))	Используйте этот параметр, если требуется разрешить второму человеку войти через дверь, используя те же реквизиты для входа, что и первый человек. Данный вариант приводит только к подаче сигнала тревоги в системе.

Deny access (Hard) (Запрет доступа (строгий))	Используйте это параметр, если требуется запретить второму пользователю вход через данную дверь, если он использует те же реквизиты для входа, 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, если тайм-аут использовать не требуется. Это означает, что для зоны установлен запрет на повторный проход до тех пор, пока пользователь не покинет данную 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 вызывать событие при нарушении соединения с дверным контроллером.

- Соединение между дверным контроллером и дверным монитором. См. *Добавление дверного монитора, on page 163*.
- Соединение между дверным контроллером и считывающим устройством, которое использует протоколы Wiegand. См. *Добавление считывающего устройства, on page 165*.
- Соединение между дверным контроллером и устройством REX. См. *Добавление REX-устройства, on page 167*.

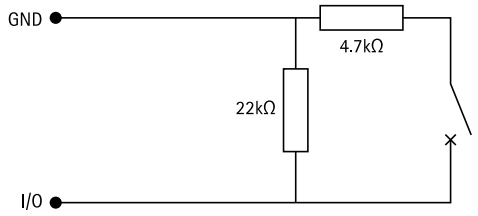
Для использования контролируемых входов:

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 КОм parallel resistor and a 4.7 КОм 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)**.

Схемы подключения

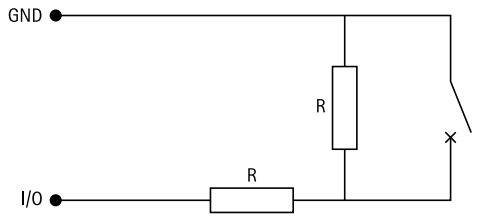
Параллельное соединение

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.



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 незапертой до тех пор, пока вы не выполните сброс.

Зафиксировать – 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, для которой необходимо выполнить действие в ручном режиме.
3. Нажмите на любое действие в ручном режиме.

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.

Типы идентификации — это носители информации об учетных данных, необходимой для доступа к двери. Распространенные типы идентификации — это токены, персональные идентификационные номера (PIN-коды), отпечатки пальцев, определение структуры лица, а также устройства, обрабатывающие запросы на выход (REX-устройства). Тип идентификации может содержать один или несколько типов информации.

Поддерживаемые типы идентификации: Карта, PIN-код, REX, статический QR-код и динамический QR-код.

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)**.

На выбор доступны пять профилей идентификации по умолчанию, которые можно при необходимости изменить или использовать без каких-либо изменений.

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; 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.

Чтобы создать профиль идентификации:

1. Перейдите к пункту **Configuration > Access control > Identification profiles (Конфигурация > Контроль доступа > Профили идентификации)**.
2. Нажмите **Create identification profile (Создать профиль идентификации)**.
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. Настройте профиль идентификации для одной стороны двери.
6. Повторите предыдущие действия для другой стороны двери.
7. Нажмите кнопку **OK**.

Чтобы внести изменения в профиль 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**.

Чтобы удалить профиль 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**.

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.

Настройка профилей идентификации

Форматы карт и ПИН-коды

Формат карты определяет, как данные хранятся в карте. Он представляет собой таблицу перевода для установления соответствия между входящими данными и проверенными данными в системе. Каждому формату карты соответствует свой набор правил, определяющий, как организовано хранение информации на карте. Задавая формат карты, вы сообщаете системе, как интерпретировать информацию, которую контроллер получает от считывателя карт.

На выбор доступно несколько предварительно определенных широко применяемых форматов карт. При необходимости в них можно внести нужные изменения либо можно их использовать без каких-либо изменений. Можно также создать 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.

Чтобы создать формат 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.

ⓘ	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. **Десятичный**: Эта система также широко известна как десятичная система счисления, состоит из цифр 0–9. **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. **Прямой порядок байтов**: Первый бит является наименьшим (наименее значимым). **Обратный порядок байтов**: Первый бит является наибольшим (наиболее значимым).

Чтобы внести изменения в формат 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)**.

Для сброса 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 .

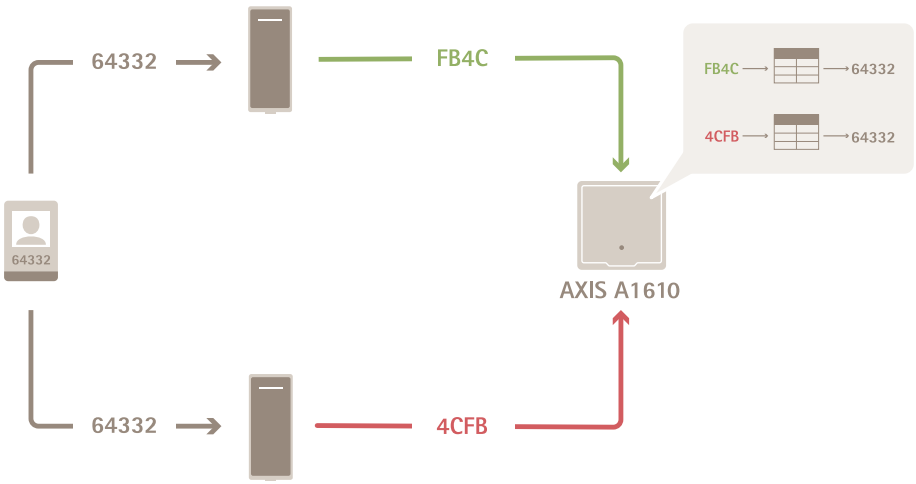
Чтобы настроить длину PIN-кода:

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**.

Настройка форматов карт

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 A1601 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 A1601 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 ключ защищенного канала OSDP Secure Channel генерируется с использованием основного ключа шифрования. 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 может проверять подлинность считывателя штрих-кодов AXIS, используя ключ проверки подлинности для предоставления доступа. Для получения информации о последовательности операций по настройке считывателя штрих-кодов AXIS см. раздел *Настройка считывателя штрих-кодов Axis*.

Чтобы создать подключение между дверным контроллером и считывателем штрих-кодов AXIS, выполните следующие действия:

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. Включите **AXIS Camera Station Secure Entry**.
   2.4. Нажмите **Add (Добавить)**, введите IP-адрес дверного контроллера и вставьте ключ для проверки подлинности.
   2.5. 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. Порт по умолчанию — 55767. Сведения о настройке конфигурации портов см. в разделе *Общее, on page 218*.

Последовательность операций

1. Настройте сервер в качестве подсервера и создайте файл конфигурации. См. *Создание файла конфигурации на подсервере, on page 178*.

2. Настройте сервер в качестве основного сервера и импортируйте файл конфигурации для подсерверов. См. *Импорт файла конфигурации на основной сервер, on page 178*.
3. Настройте глобального владельца карты и группы владельцев карт на основном сервере. См. *Добавление владельца карты, on page 187* и *Добавление группы, on page 192*.
4. Просмотр и наблюдение за глобальными владельцами карт и группами владельцев карт с подсервера. См. *Контроль доступа, on page 187*.

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. Более подробные сведения 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 179*.

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 188*.

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 — AXIS Camera Station Pro и AXIS Audio Manager Pro — должны быть предварительно настроены, либо на одном сервере, либо на разных устройствах в одной сети.

Внимание

Если AXIS Camera Station Pro и AXIS Audio Manager Pro работают на одном и том же сервере, по умолчанию они будут использовать порт 443. Для предотвращения проблем с подключением настройте одно из устройств на использование другого порта.

Изменить порт в AXIS Camera Station Pro можно через < *Общее, on page 218*. 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 задайте 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 соединения вы можете:

- 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 209*.

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 функцией «Умный поиск 2» вы можете настроить несколько фильтров, которые помогут вам легко найти интересующих вас людей и транспортные средства на видеозаписях, полученных с камер Axis.

Сведения о требованиях и ограничениях, а также инструкции по применению функции «Умный поиск 2» см. в разделе *Интеллектуальный поиск 2, on page 37*.

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, сохраненных на сервере, в разделе **Filter (Фильтр)** нажмите ⚙ и создайте фильтры для **Area (Область)**, **Size and duration (Размер и длительность)** и **Swaying objects (Качающиеся объекты)**.

Вы можете использовать данные фильтры для исключения из области детектирования участков сцены, мелких объектов, кратковременно появляющихся объектов, а также качающихся объектов, таких как листва.
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 (Включить периоды без метаданных)** для отображения результатов, указывающих на то, что в течение определенного периода метаданные не были записаны.
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 классифицируется менее 95 % обнаружений.
	Состояние классификации на сервере за последний час, когда классификация на сервере происходит медленно. Отображается, если классифицируется менее 50 % обнаружений.

Триггеры

Можно настроить умные фильтры поиска, чтобы использовать их как триггеры 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 37*.
4. Нажмите **Next** ("Далее").
5. Настройте уровень **Confidence (Достоверность)** для объектов обнаружения. Более высокий уровень достоверности игнорирует неопределенные классификации, что уменьшает количество срабатываний.
6. Нажмите **Next** ("Далее").
7. Введите имя для триггера и нажмите **Save (Сохранить)**.

Примечание

- Smart search 2 обычно требуется несколько секунд после того, как объект покидает поле зрения камеры, чтобы проанализировать запись и подтвердить результат. Например, если настроено правило действий на срабатывание при обнаружении красного автомобиля, действие выполнится

через несколько секунд после того, как автомобиль выйдет из поля зрения камеры и умный поиск подтвердит, что это действительно был красный автомобиль.

- 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)**.
- **Delayed detection periods (Периоды задержки обнаружения)** — это интервалы с высокой задержкой обработки, из-за которых правила действий срабатывают поздно. Если это происходит часто, можно перенастроить фильтр триггера, чтобы включить меньше камер, и использовать фильтры камеры, такие как пересечение линии, область, размер и длительность, чтобы снизить нагрузку.

Чтобы использовать триггер Smart search 2 в правиле действий, см. раздел *Создание триггеров Smart search 2, on page 107*.

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 вы зарегистрировали свой сервер в организации, вы можете просматривать данные о состоянии системы из любой точки. Если вы еще не подключены, нажмите кнопку **Manage (Управление)** и следуйте инструкциям на экране.
Частота получения данных	Выберите более низкую частоту получения данных для устранения предупреждений об устаревших данных или общих проблемах производительности в системе. В многосистемной конфигурации рекомендуется использовать для подсистемы ту же или более высокую настройку, что и для родительской системы. • **Low (Низкая)** — для систем с более чем 100 устройствами. • **Medium (Средняя)** — для систем с 25–100 устройствами. • **High (Высокая)** — для систем с менее чем 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 132*
2. Настройте адреса электронной почты для получения уведомлений. См. *Настройка получателей электронной почты, on page 183*.
3. Настройте правила уведомлений. См. *Настройка правил уведомлений., on page 183*.

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, показывающее, что тестовое электронное сообщение было отправлено.

Настройка правил уведомлений.

По умолчанию активированы два правила уведомления.

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 уведомления)** можно включать или выключать правила уведомления.
3. В меню **Applied rules (Примененные правила)** отображается список систем и устройств, включая применяемое правило уведомления.

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 183*.
2. В основной системе загрузите системную конфигурацию. См. *Получить данные из других систем, on page 184*.
3. Повторите указанные выше шаги в других вспомогательных системах.
4. Отслеживайте данные о работоспособности нескольких систем из основной системы. См. *System Health Monitoring БЕТА, on page 199*.

Сформировать конфигурацию системы

1. Выберите **Configuration > System Health Monitoring > Multisystem (Конфигурация > Контроль работоспособности системы > Многосистемность)**.
2. Нажмите **Generate (Сформировать)**.
3. Нажмите **Copy (Копировать)** для загрузки в основную систему.

4. Для просмотра подробных сведений о конфигурации системы нажмите **Show details (Показать подробности)**.
5. Для повторного создания конфигурации системы нажмите кнопку **Delete (удалить)**, чтобы сначала удалить существующую конфигурацию.

После загрузки системной конфигурации в основную систему основные сведения о системе будут отображаться в разделе **Systems with access (Системы, у которых есть доступ)**.

Получить данные из других систем

После создания и копирования конфигурации вспомогательной 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)** для добавления информации, скопированной из дополнительной 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 функции:
  - AXIS Object Analytics: Подсчет количества пересечений и посетителей для 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.
- Добавить теги к сценариям, чтобы группировать данные на панели, например, объединять камеры по местоположению.

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 работы панели управления AXIS Data Insights на вашем сервере Windows требуются протоколы шифрования соединений TLS версии 1.2 и выше.
- AXIS Data Insights Dashboard переопределяет существующие настройки MQTT на камере в следующих случаях:
  - На камере не настроен MQTT-клиент.
  - Вы вручную активируете сценарий для камеры, подключенной к другому серверу AXIS Camera Station Pro.
- Пока панель AXIS Data Insights Dashboard подключена, MQTT-клиент камеры используется только для взаимодействия с этой панелью.
- Камеры и сервер AXIS Camera Station Pro должны находиться в одной сети.
- Для оптимальной работы панели AXIS Data Insights Dashboard в AXIS Camera Station Pro рекомендуется сервер с минимум 16 ГБ оперативной памяти.
- Максимальный объем хранимых данных составляет 100 МБ, что ограничивает время хранения. Например:
  - Оценка заполняемости парковки, оборудованной четырьмя камерами, каждая из которых настроена на круглосуточное обнаружение пяти подклассов транспортных средств, таких как автомобили и мотоциклы, обеспечивает срок хранения данных 260 дней.
  - Подсчет посетителей в торговом помещении, оборудованном восемью камерами, где поток людей непрерывен в течение 12 часов, обеспечивает около 1270 дней хранения данных.
  - Камера, настроенная на подсчет пересечений линий с шестью классами объектов при стабильном потоке в течение 24 часов, может сохранять данные подсчета примерно за 860 дней.

Подробнее о добавлении панели мониторинга в мультиэкранный режим см. в разделе *Панель аналитики AXIS Data Insights Dashboard в режиме мультиэкрана, on page 20*.

Включение панели AXIS Data Insights Dashboard

License Plate Verifier

Вы можете просматривать состояние AXIS License Plate Verifier ACAP на ваших камерах и группах камер для упрощения управления списками номерных знаков на странице License plate verifier (Проверка номерных знаков).

Вкладка **Cameras** (Камеры) содержит перечень всех подключенных устройств с установленным AXIS License Plate Verifier:

- **Камера**: Название камеры.
- **Версия**: Какая версия AXIS License Plate Verifier установлена на камере.
- **Status (Состояние)**. Текущий статус AXIS License Plate Verifier.
- **Последнее событие**: Время последнего события, зафиксированного камерой.
- **Allowed** (Разрешенные): Количество номерных знаков, включенных в список «Разрешенные» камеры.
- **Blocked** (Заблокированные): Количество номерных знаков, включенных в список «Заблокированные» камеры.
- **Custom (Пользовательский)**. Количество номерных знаков, включенных в список «Пользовательские» камеры.
- **Групповое:** К какой группе принадлежит камера.

Вкладка **Groups** (Группы) содержит перечень всех ваших групп камер и вложенный список камер, входящих 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)
- Нажать **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 208*.

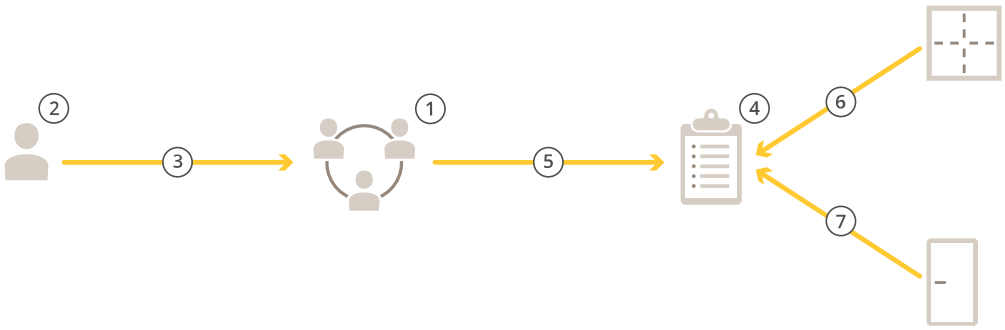
Контроль доступа

На вкладке Access Management (Управление доступом) можно настраивать и управлять следующими объектами, имеющимися в системе: владельцы карт, группы и правила доступа.

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 управления доступом является гибкой, что позволяет разработать рабочий процесс, отвечающий вашим потребностям. Пример рабочего процесса представлен ниже.



1. Добавьте группы. См. *Добавление группы, on page 192*.
2. Добавьте владельцев карт. См. *Добавление владельца карты, on page 187*.
3. Добавьте владельцев карт в группы.
4. Добавьте правила доступа. См. *Добавление правила доступа, on page 193*.
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 владельца карты с учетными данными, которые идентифицируют человека, а также когда и как предоставить ему доступ к дверям.

Можно также сопоставить пользователей в базе данных Active Directory в качестве владельцев карт. См. раздел *Настройки Active Directory^{БЕТА}, on page 179*.

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Cardholder management (Управление владельцами карт)** > **Cardholders (Владельцы карт)** и нажмите **+ Add (Добавить +)**.
3. Введите имя и фамилию владельца карты и нажмите **Next (Далее)**.
4. При желании нажмите **Advanced (Дополнительно)** и выберите необходимые параметры.
5. Добавьте учетные данные владельца карты. См. *Добавить учетные данные, on page 188*
6. Нажмите **Сохранить**.
7. Добавьте владельца карты в группу.
   7.1. В разделе **Groups (Группы)** выберите группу, в которую вы хотите добавить владельца карты, и нажмите **Edit (Изменить)**.

7.2. Нажмите **+ Add (Добавить +)** и выберите владельца карты, которого вы хотите добавить в группу. Можно выбрать несколько владельцев карт.

7.3. Нажмите **Добавить**.

7.4. Нажмите **Сохранить**.

Расширенный набор	
Длительное время доступа	Выберите, чтобы предоставить владельцу карты длительное время доступа и длительное время до подачи сигнала тревоги «Открыта слишком долго» при наличии установленного дверного монитора.
Приостановить владельца карты	Выберите, чтобы приостановить владельца карты.
Разрешить двойной свайп	Выберите, чтобы разрешить владельцу карты переопределять текущее состояние двери. В качестве примера, с его помощью можно отпереть дверь вне обычного графика.
Исключение из блокировки	Выберите если требуется, чтобы владелец карты имел доступ во время блокировки.
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 177*.

Добавление владельцев карт и групп

Добавить учетные данные

Владельцу карты можно назначить следующие типы учетных данных:

- ПИН; PIN-код; ПИН-код
- Карта
- Номерной знак а/м
- QR-код
- Мобильный телефон

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 191*.

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**.

Пример см. в разделе *Использование номерного знака автомобиля в качестве учетных данных, on page 190*.

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. Чтобы использовать PIN-код под принуждением для активации скрытого сигнала тревоги, включите параметр **Duress PIN (PIN-код под принуждением)** и введите PIN-код под принуждением.
4. Нажмите **Добавить**.

Заданный PIN-код действителен всегда. Кроме того, можно настроить так называемый «PIN-код под принуждением», который позволяет открыть дверь, но при этом активирует скрытый сигнал тревоги в системе.

Чтобы добавить данные о мобильном телефоне владельца карты:

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить +)** и выберите **PIN-код**.
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 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 reader(s) (Получить последние считанные данные карты с дверного считывающего устройства)**.

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**.

Чтобы добавить данные QR-кода владельца карты:

Примечание

Использование QR-кода в качестве учетных данных требует, чтобы время на системном контроллере совпадало со временем на камере, на которой работает AXIS Barcode Reader. Рекомендуется использовать один и тот же источник времени для обоих устройств для выполнения идеальной синхронизации времени.

1. В разделе **Credentials (Учетные данные)** нажмите **+ Add (Добавить +)** и выберите **QR-код**.
2. Введите имя для учетных данных.
3. Параметр **Dynamic QR (Динамический QR-код)** по умолчанию включен. Динамический QR-код необходимо использовать вместе с PIN-кодом.
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**.

Дата окончания срока действия	
Действует с	Установите дату и время, когда учетные данные будут действительны.
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 истечения действия учетных данных с момента их последнего использования. Выберите количество дней, месяцев или лет после последнего использования.

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 5*
2. Задайте дату и время для новых устройств с помощью параметра **Synchronize with computer time (Синхронизировать с временем компьютера)**. См. *Установите время и дату, on page 70*.
3. Обновите прошивку на новых устройствах до последней доступной версии. См. *обновлять встроенное программное обеспечение;, on page 69*.

4. Добавьте новую дверь, подключенную к вашему дверному контроллеру. См. *Добавление двери, on page 156*.
   4.1. Добавьте считывающее устройство на **сторону A**. См. *Добавление считывающего устройства, on page 165*.
   4.2. 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.
   4.3. Дополнительно можно также добавить считывающее устройство или устройство, обрабатывающее запросы на выход, на **сторону B**.
   4.4. Нажмите кнопку **OK**.
5. Установите на камеру AXIS License Plate Verifier и выполните активацию. См. руководство пользователя *AXIS License Plate Verifier*.
6. Запустите AXIS License Plate Verifier.
7. Настройте AXIS License Plate Verifier.
   7.1. Перейдите в меню **Configuration > Access control > Encrypted communication (Конфигурация > Контроль доступа > Зашифрованная связь)**.
   7.2. 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)**.
   7.3. Откройте AXIS License Plate Verifier из веб-интерфейса камеры.
   7.4. Не выполняйте настройку.
   7.5. Выберите в меню **Settings (Настройки)**.
   7.6. В разделе **Access control (Контроль доступа)** выберите **Secure Entry** в качестве значения **Type (Тип)**.
   7.7. В поле **IP address (IP-адрес)** введите IP-адрес дверного контроллера.
   7.8. В поле **Authentication key (Ключ проверки подлинности)** вставьте скопированный вами ранее ключ проверки подлинности.
   7.9. Нажмите **Подключить**.
   7.10. В разделе **Door controller name (Имя дверного контроллера)** выберите нужный дверной контроллер.
   7.11. В разделе **Reader name (Имя считывающего устройства)** выберите добавленное вами ранее считывающее устройство.
   7.12. Включите интеграцию.
8. Добавьте владельца карты, которому хотите предоставить доступ. См. *Добавление владельца карты, on page 187*
9. Добавление данных номерного знака для нового владельца карты. См. *Добавить учетные данные, on page 188*
10. Добавление правила доступа. См. *Добавление правила доступа, on page 193*.
    10.1. Добавление расписания.
    10.2. Добавьте владельца карты, которому вы хотите предоставить доступ к номерному знаку.
    10.3. Добавьте дверь со считывающим устройством AXIS License Plate Verifier.

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)** на той стороне двери, где установлено считывающее устройство Bluetooth.
   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 171*.
6. Добавьте мобильный пропуск для владельца карты. См. *Добавить учетные данные, on page 188*.
7. Выполните сопряжение мобильного пропуска со считывающим устройством.
   7.1. Поднесите мобильный телефон владельца карты к считывающему устройству Bluetooth, настроенному для сопряжения.
   7.2. Следуйте инструкциям из электронного письма, отправленного владельцу карты.

Добавление группы

Группы позволяют эффективно управлять множеством владельцев карт и связанными с ними правилами доступа.

1. Откройте вкладку Access management (Управление доступом).
2. Перейдите в раздел **Cardholder management (Управление владельцами карт)** > **Groups (Группы)** и нажмите **+ Add (Добавить +)**.
3. Введите название и, по желанию, инициалы для группы.
4. Выберите **Global group (Глобальная группа)** для просмотра и отслеживания владельца группы на подсерверах. Данная опция доступна только для тех владельцев карт, которые созданы на основном сервере. См. *Мультисерверная БЕТА-ВЕРСИЯ, on page 177*.
5. Добавление в группу владельцев карт:

5.1. Щелкните **+ Добавить**.

5.2. Выберите владельцев карт, которых вы хотите добавить, и нажмите **Add (Добавить)**.

6. Нажмите **Сохранить**.

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 (Владельцы карт)** или **Groups (Группы)** нажмите **+ Add (Добавить +)**.
   5.2. Выберите владельцев карт или группы и нажмите **Add (Добавить)**.
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 **Сохранить**.

Правило доступа, в котором отсутствует один или более компонентов, описанных выше, является неполным. Просмотреть все неполные правила доступа можно на вкладке **Incomplete (Неполные)**.

Для просмотра видео откройте веб-версию данного документа.

Двери

Информацию о действиях, которые выполняются вручную, таких как разблокировка двери, см. в разделе *Действия в ручном режиме, on page 171*.

Зоны

Информацию о действиях, которые выполняются вручную, таких как разблокировка зоны, см. в разделе *Действия в ручном режиме, on page 171*.

Экспорт отчетов о конфигурации системы

Вы можете экспортировать отчеты, содержащие различные типы информации о системе. AXIS Camera Station Pro Экспорт отчета в виде файла со значениями, разделенными запятыми (CSV), и сохранение его в папке загрузки 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 зданиями в определении местонахождения персонала и посетителей после эвакуации. Пункт сбора - это специально отведенное место, где персонал должен отметится во время чрезвычайных ситуаций. Это позволяет сформировать отчет о присутствующих на территории и тех, кто покинул объект. 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 (Сбор/присутствие)**.

4. Назовите отчет
5. Выберите зоны для отчета.
6. Выберите группы для отчета.
7. Если вам нужен отчет о сборе, выберите **Mustering point (Пункт сбора)** и считыватель для пункта сбора.
8. Выберите временные рамки для отчета.
9. Нажмите **Сохранить**.
10. Выберите отчет и нажмите **Run (Выполнить)**.

Состояние отчета о присутствии	Описание
Присутствует	Владелец карты вошел в указанную зону и не вышел из нее до того, как вы запустили отчет.
Не присутствует	Владелец карты вышел из указанной зоны и не входил в нее до того, как вы запустили отчет.

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

Данная функция позволяет импортировать сведения о владельцах карт, группах владельцев карт, учетные данные и фотографии владельцев карт из CSV-файла. Чтобы импортировать фотографии владельцев карт, убедитесь в том, что сервер имеет доступ к фотографиям.

Когда вы импортируете владельца карт, система управления доступом автоматически сохраняет конфигурацию системы, включая все конфигурации оборудования, и удаляет все ранее сохраненные.

Можно также сопоставить пользователей в базе данных Active Directory в качестве владельцев карт. См. раздел *Настройки Active Directory[БЕТА], on page 179*.

Варианты импорта	
Новинка	При выборе этого варианта добавляются новые владельцы карт, а существующие удаляются.
Обновить	При выборе этого варианта обновляются существующие владельцы карт и добавляются новые а владельцы карт.
Добавить	При выборе этого варианта сохраняются существующие владельцы карт и добавляются новые. 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)** и перейдите к файлу CSV. Нажмите кнопку **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. Уникальный идентификатор предотвращает импорт дубликатов личных записей.
Формат номера карты	По умолчанию выбран параметр **Allow both hexadecimal and number (Разрешить шестнадцатеричный и числовой форматы).**

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 (Отмена импорта)** сбрасывает данные владельца карты и всю конфигурацию оборудования до состояния, которое было до импорта последнего владельца карты.

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. Выберите **+ 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

Также необходимо выбрать **Include facility code for card validation (Включить код объекта для проверки карты)** при настройке профилей идентификации. См. *Профили идентификации, on page 171*.

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)**, если хотите 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 сохранить новый шаблон.

Примечание

После того, как шаблон был создан, его нельзя изменить, только переименовать.

Печать бейджей BETA

Вы можете печатать идентификационные бейджи для владельцев карт, используя настроенные шаблоны бейджей. 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.
- Для печати вам необходим принтер, поддерживающий формат карты CR80 и совместимые расходные материалы, такие как плотная картонная бумага.

- Настройте параметры печати в вашем браузере:
  - Установите размер страницы на CR80 или пользовательский размер, соответствующий размерам вашей карты.
  - Установите ориентацию на «Портрет».
  - Отключите поля или установите минимальные.

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 выпадающем списке **Template (Шаблон)** выберите нужный шаблон бейджа.
5. Если у владельца карты имеется несколько учетных данных карты, выберите один из них в выпадающем 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 BETA

Вкладка System Health Monitoring (Контроль работоспособности системы) позволяет отслеживать данные о работоспособности из одной системы или из нескольких систем AXIS Camera Station Pro, расположенных 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 199*.
	Показывает сводку и подробные сведения о записи для каждой камеры с контролируемых систем. См. *Хранение данных, on page 200*.
	Отображает журналы System Health Monitoring для контролируемых систем. См. *Уведомления, on page 201*.

Ограничения

- Мониторинг объема пространства ресурса хранения для записей, выполненных с помощью AXIS S3008 Recorder, не поддерживается.
- Настройки уведомления влияют только на локальный сервер контроля работоспособности системы.
- Записи, за исключением непрерывных записей и записей триггера по движению, будут иметь системную отметку **Нет (None)** в поле типа записи.

Последовательность операций

1. *Настройка приложения System Health Monitoring BETA, on page 182*
   1.1. Настройка уведомлений. См. *Уведомления, on page 182*.
   1.2. Настройка мультисистемы. См. *Мультисистема, on page 183*.
2. Мониторинг данных о работоспособности из систем AXIS Camera Station Pro.
   2.1. *Инвентарная ведомость, on page 199*
   2.2. *Хранение данных, on page 200*
   2.3. *Уведомления, on page 201*

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 BETA** (Контроль работоспособности системы)нажмите  .
2. Для просмотра сводных данных о системе нажмите **AXIS Camera Station**.
   Эта информация отображается на правой панели, включая сведения о системе и сервере.
3. Чтобы просмотреть сводные данные по устройству в системе, нажмите устройство в списке.
   Эта информация отображается на правой панели, включая информацию об устройстве и данные о ресурсе хранения, если в нем содержится видеоисточник.
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 213*.

5. Для загрузки отчета System Health Monitoring:
   5.1. Выберите **System Health Monitoring report (Отчет о контроле работоспособности системы)** в раскрывающемся меню **Create report (Создать отчет)**.
   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.

Хранение данных

На странице Storage (Хранилище) показана сводка по хранилищу и подробные сведения о записи для каждой камеры с контролируемых систем. Чтобы упорядочить список по содержимому столбца, щелкните по заголовку этого столбца.

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 77*.
Местонахождение	Путь к ресурсу хранения и его имя.
Итого	Общий объем пространства ресурса хранения. Это тот же объем пространства, что и "Total size" (Общий размер) в свойствах Windows для устройства хранения.
Выделено	Максимальный объем пространства ресурса хранения, отведенный для записей.
Used (Используется)	Объем пространства ресурса хранения, в данный момент занятый записями.
Последнее обновление	Время последнего обновления информации.

Камера	
Статус	(Пусто). Normal state (Нормальное состояние). Значок предупреждения: Срок хранения не выполнен. Значок информации: Требования к сроку хранения не выполнены из-за недостаточной длительности записи на камеру.
Название	Имя камеры.
Тип записи	Типы записей, применимые к камере.
Задать срок хранения записей	Срок хранения записей, заданный для камеры в разделе **Configuration > Storage > Selection (Конфигурация > Хранилище > Выбор)**.
Текущий срок хранения записей	Количество дней, в течение которых записи с камеры будут оставаться в хранилище.
Самая старая запись	Время самой старой записи с камеры, находящейся в хранилище.
Последняя запись	Время последней записи с камеры, находящейся в хранилище.
Местонахождение	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. Чтобы упорядочить список по содержимому столбца, щелкните по заголовку этого столбца.

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, которое инициировало уведомление. `System down` или `Device down`
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

Вы должны вручную назначить действия в категориях Navigate to cameras («Переход к камерам») и Navigate to views («Переход к видам»).

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 посмотреть, для какого действия назначено это сочетание клавиш. Нажмите клавишу ESC для отмены. Нажмите клавишу ВВОД, чтобы использовать горячую клавишу с автоматическим удалением конфликтующей комбинации.
- 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 значение действия для сочетания клавиш на клавиатуре является пустым, щелкните это пустое значение и добавьте горячую клавишу для данного действия. • Чтобы добавить горячую клавишу с помощью дополнительной цифровой клавиатуры, нажмите Ctrl и еще одну клавишу или 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 добавить горячую клавишу для действия с использованием джойстика или колеса прокрутки, нажмите кнопку джойстика или колеса прокрутки, которую хотите назначить для данного действия.
Изменить горячую клавишу	Щелкните значение действия, заданное на клавиатуре, и измените это значение.
Удалить горячую клавишу	Щелкните значение действия, заданное на клавиатуре, и удалите это значение.
	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	-

Сопоставление горячих клавиш – джойстик	Действие по умолчанию	AXIS TU9002	AXIS T8311
Кнопка 9	Перейти к предыдущей записи		-
Кнопка 10	Воспроизвести/пауза		-
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	-

Сопоставление горячих клавиш – клавиатура	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	-	-	

Сопоставление горячих клавиш – клавиатура	Действие по умолчанию	AXIS TU9003	AXIS T8312
ПЛЮС	Увеличить расстояние фокусировки	+	-
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 журналы живого видео, в том числе живое тревоги, события и журналы аудита. Кроме того, здесь можно выполнять поиск предыдущих журналов. Вы можете настроить срок хранения журналов (в днях) в разделе **Configuration > Server > Settings (Конфигурация > Сервер > Настройки)**.

Time (Время)	Дата и время действия.
Тип	Тип действия: «Тревога», «Событие» или «Аудит».
Категория	Категория действия.
Сообщение	Краткое описание действия.
Пользователь	AXIS Camera Station Pro Пользователь , который выполняет действие.
Компьютер	Компьютер (имя в Windows-домене), на котором установлено приложение AXIS Camera Station Pro.
Пользователь Windows	Пользователь Windows, выполняющий администрирование AXIS Camera Station Pro.
Сервер	Отображается 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) выберите **Search (Поиск)** в разделе **Log search (Поиск журналов)**.
2. В поле «Filter» (Фильтр) введите ключевые слова. Программа AXIS Camera Station Pro выполнит поиск в списке журналов, за исключением столбца **Time (Время)** и отобразит результаты поиска, содержащие все ключевые слова. Сведения о поддерживаемых операторах поиска см. в разделе *Оптимизация поиска, on page 45*.
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 тревог отображается список системных тревог и тревог, связанных с выполнением правил и обнаружением движения. В списке указываются дата и время тревоги, категория тревоги и связанное с ней сообщение. См. *Тревоги*.

	Нажмите тревогу и  , чтобы открыть вкладку Recordings (Записи) и запустить воспроизведение, если для данной тревоги предусмотрена видеозапись.
	Нажмите тревогу и  , чтобы увидеть последовательность действий по сигналу тревоги (отображается, если сигналу тревоги назначена определенная последовательность действий).

	Нажмите тревогу и  , чтобы уведомить другие клиенты, что тревоги приняты к сведению.
	Нажмите тревогу и  , чтобы экспортировать журнал в текстовый файл.

Журнал событий

В журнале событий отображается список событий камер и серверов, в частности, записи, триггеры, 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 аудита регистрируются все действия пользователей, например запущенные вручную записи, запуск и остановка потоковой передачи видео, правила действий, а также созданные двери и владельцы карт. Выберите аудиты и нажмите значок  в панели инструментов, чтобы экспортировать журнал аудита в виде текстового файла.

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. Чтобы отредактировать название списка, нажмите **Edit list name** (Редактировать название списка).
4. Введите новые номерные знаки в столбец License plate (Номерной знак) и описание (если есть) в столбец Description (Описание). Нажмите **Add** (Добавить), чтобы сохранить их в списке.
5. Нажмите **Apply** (Применить), чтобы сохранить изменения.

Чтобы отредактировать или удалить номерной знак, добавленный в список, выберите его и нажмите **Edit** (Редактировать) или **Remove** (Удалить).

AXIS Audio Manager Pro

Вкладка AXIS Audio Manager Pro позволяет открывать интерфейс сервера AXIS Audio Manager Pro прямо из AXIS Camera Station Pro. Подробнее об интерфейсе сервера см. *Руководство пользователя AXIS Audio Manager Pro*.

Вкладка появится 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 179*.

Внимание

Доступ к интерфейсу сервера AXIS Audio Manager Pro через Secure Remote Access v2 невозможен.

Интеграция также позволяет:

- *создать триггер аудиоменеджера;, on page 107*
- *создать действия аудиоменеджера;, on page 118*
- добавлять аудиозоны на карты. См. *Карта, on page 22*.
- *Использование интерфейсов оповещения в мультиэкранном режиме, on page 21*
- Назначьте права пользователей, связанные с AXIS Audio Manager Pro, в AXIS Camera Station Pro См. раздел *Права доступа пользователей или групп, on page 145*.
- Выберите аудиоустройства с сервера AXIS Audio Manager Pro как связанные аудиоустройства для камеры См. *Изменение профилей потока, on page 55*.

Тревоги

Вкладка Alarms (Тревоги) находится в нижней части окна клиентского ПО AXIS Camera Station Pro. На вкладке отображаются сработавшие события и системные 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 236*.

Time (Время)	время возникновения сигнала тревоги.
Категория	категория тревоги, которая вызвала подачу сигнала.
Описание	краткое описание тревоги.
Сервер	Доступно при подключении к нескольким серверам. Сервер AXIS Camera Station Pro, который отправляет сигнал тревоги.
Компонент	компонент, инициирующий сигнал тревоги.
	Show Alarm procedure (Показать действия при тревоге). Отображается только если для тревоги предусмотрена соответствующая последовательность действий.
	Кнопка Go to recordings (Перейти к записям) отображается только если для тревоги предусмотрено включение видеозаписи.
	Подтвердить выбранную тревогу
	Удалить тревогу. Тревога будет удалена только временно, если вы не подтвердите ее перед удалением.

При возникновении сигнала тревоги:

1. Нажмите **Alarms and Tasks (Тревоги и задачи)** в нижней части клиентского ПО AXIS Camera Station Pro и откройте вкладку **Alarms (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. Чтобы уведомить других клиентов о том, что сигналы тревоги были обработаны, выберите сигналы тревоги и нажмите .
6. Для удаления сигналов тревоги из списка выберите их и нажмите .

Задачи

Вкладка Tasks (Задачи) отображается в нижней части клиентского ПО AXIS Camera Station Pro.

Следующие задачи являются персональными и их видят только администраторы и пользователи, которые их запустили.

- Системный отчет
- Создать отчет об инциденте
- Экспорт записей

Администратор может просматривать все задачи (и работать с ними), 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).
- Отменять и перезапускать задачи, запущенные вами. 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.
Пуск	Время начала выполнения задачи.
Сообщение	Состояние задачи или информация о задаче. Возможные состояния: • **Canceling (Идет отмена)**: выполняется удаление информации перед отменой задачи. • **Canceled (Отменено)**: удаление информации завершено, задача отменена. • **Error (Ошибка)**: задача завершена с ошибками, т.е. задачу не удалось выполнить на одном или нескольких устройствах. • **Finished (Завершено)**: задача завершена. • **Finished during lost connection (Завершено во время потери связи):** Отображается в том случае если окончание выполнения задачи совпало с разрывом соединения с сервером. Невозможно определить состояние выполнения задачи. • **Lost connection (Соединение потеряно)**: Отображается если соединение клиента с сервером разорвано во время выполнения задачи. Невозможно определить состояние выполнения задачи. • **Running (Работает)**. задача выполняется. • **Pending (Ожидание)**: Ожидание 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 одно из 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. Все операции, завершившиеся неудачно, необходимо проанализировать и настроить вручную.

Для большинства задач приводятся следующие сведения. Для таких задач, как экспорт записей и формирование системного отчета, дважды щелкните задачу, чтобы открыть папку, в которой хранятся файлы.

MAC-адрес	MAC-адрес обновленного устройства.
Адрес	IP-адрес обновленного устройства.
Сообщение	Информация о состоянии выполнения задачи: • **Finished (Завершено)**: задача успешно выполнена. • **Error (Ошибка)**: не удалось выполнить эту задачу на устройстве. • **Canceled (Отменено)**: задача была отменена до ее 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.

Для просмотра отчета в формате HTML с обзором конфигурации клиентской системы:

1. Откройте меню **Configuration (Конфигурация)** > **Server (Сервер)** > **Diagnostics (Диагностика)**.
2. Нажмите **View client configuration sheet (Просмотр листа конфигурации клиента)**.

Лист конфигурации сервера

Лист конфигурации сервера содержит информацию об общей конфигурации системы, о настройках камер, включая правила действий, о расписаниях, месте хранения видеозаписей, дополнительных устройствах и лицензиях. Отчет полезен при поиске и устранении неполадок, а также при обращении в службу поддержки.

Чтобы просмотреть отчет в формате HTML с обзором конфигурации серверной системы:

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 меню в верхнем правом углу.
2. Выберите пункт **Help** ("Помощь") > **System report** ("Системный отчет").
3. Отредактируйте имя файла, если хотите изменить автоматически сгенерированное имя файла.
4. Нажмите **Обзор**, чтобы выбрать место сохранения системного отчета.
5. Выберите параметры:
   - **Автоматически открывать папку по готовности отчета**, чтобы сразу его видеть.
   - **Включить все базы данных**, чтобы добавить подробную информацию о записях и системных данных.
   - **Включить скриншоты всех мониторов**, чтобы упростить анализ системных отчетов.
6. Нажмите **OK**.

Создать системный отчет

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	Тестируется видеопоток и поток данных, поступающих в хранилище, для текущих системных настроек в AXIS Camera Station Pro. Выход: удовлетворительный или неудовлетворительный результат.
Условия слабой освещенности	тестируется видеопоток и поток данных, поступающих в хранилище, для типичных настроек, используемых при слабом освещении, — например, для заданных параметров усиления сигнала. Выход: удовлетворительный или неудовлетворительный результат.
Стресс-тест	постепенное увеличение объема передаваемого видеопотока и потока данных, поступающих в хранилище, до тех пор, пока не будет достигнуто максимально возможное значение для данной системы. Выход: информация о максимальной производительности 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. По окончании тестирования нажмите **View report (Просмотр отчета)**, чтобы вывести отчет на экран, 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 поле **Последняя операция экспорта** будет создана или обновлена ссылка на файл.
5. Для перехода к файлу откройте ссылку.

Настройки нательной системы

Для подключения к нательный системе необходимо создать файл подключения. См. раздел *Настройка нательной системы Axis*.

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*.

Чтобы создать файл подключения:

1. Перейдите в раздел >**Other (Прочее) > Body worn settings (Параметры нательной системы)**.
2. Чтобы изменить имя объекта по умолчанию, отображаемое в нательной системе, введите новое имя.
3. Нажмите на **Экспорт**.
4. В поле **Последняя операция экспорта** будет создана или обновлена ссылка на файл.
5. Для перехода к файлу откройте ссылку.

Настройка нательной системы Axis

Воспроизведение и экспорт записей с нательных камер Axis

Состояние служб Axis

Чтобы просмотреть статус онлайн-сервисов Axis:

1. Откройте меню **Configuration (Конфигурация)** > **Server (Сервер)** > **Diagnostics (Диагностика)**.
2. Нажмите **Просмотр состояния служб Axis**.

AXIS Camera Station Pro Service Control

Сервер использует AXIS Camera Station Pro Service Control для запуска, остановки и изменения своих 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 правой кнопкой мыши значок и выберите в меню один из следующих вариантов: **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 (Выход)**.

Чтобы открыть Service Control из меню «Пуск»:

Перейдите в меню **Start (Пуск)** и выберите **All Programs > Tools > Service Control (Все программы > Инструменты > Управление службой)**.

	Работает
	Выполняется запуск
	Остановлено

Изменение параметров	Выберите, чтобы иметь возможность изменять настройки сервера.
Восстановить параметры по умолчанию	Нажмите, чтобы восстановить все настройки к исходным значениям по умолчанию.
Пуск	Нажмите для изменения состояния сервера.
Остановить	
Перезапуск	Нажмите для перезапуска сервера.

Общее

В приложении AXIS Camera Station Pro Service Control выберите **Modify settings (Изменить параметры)** и перейдите на вкладку **General (Общие)**, чтобы изменить общие настройки сервера.

Параметры сервера	
Имя сервера	Имя данного сервера. Имя сервера отображается в клиентском ПО. 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. Оставшиеся порты изменятся автоматически.
Разрешить AXIS Camera Station Pro добавлять исключения в брандмауэр Windows	Выберите этот параметр, если хотите разрешить AXIS Camera Station Pro автоматически добавлять исключения в брандмауэр Windows, когда пользователь изменяет диапазон портов.

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. Возможно, нужно будет включить их в межсетевом экране для обеспечения оптимальной производительности и для удобства использования. Номера портов вычисляются на основе основного порта HTTP — 29200.

Взаимодействие «сервер — устройства»

Порт	Номер	Протокол	Вход/выход	Описание
Основные порты HTTP и HTTPS	80 и 443	TCP	Исходящий	Используется для видеопотоков и данных устройства.
Порт Bonjour по умолчанию	5353	UDP	Многоадресная передача (входящая + исходящая)	Используется для обнаружения устройств с помощью

				обнаружения mDNS (Bonjour). Multicast 224.0.0.251. Если не удается выполнить привязку к порту по умолчанию, возможно, он используется другим приложением, которое отказывается сделать его общедоступным. В таком случае будет использован случайный порт. При использовании случайного порта устройства с локальными адресами будет невозможно обнаружить с помощью Bonjour.
Порт SSDP по умолчанию	1900	UDP	Многоадресная передача (входящая + исходящая)	Используется для обнаружения устройств с использованием протокола SSDP (UPNP). Multicast 239.255.255.250.
Порт WS-Discovery по умолчанию	3702	UDP	Многоадресная передача (входящая + исходящая)	Обнаружение веб-служб WS-Discovery, используемое для обнаружения устройств Onvif. Multicast 239.255.255.250.

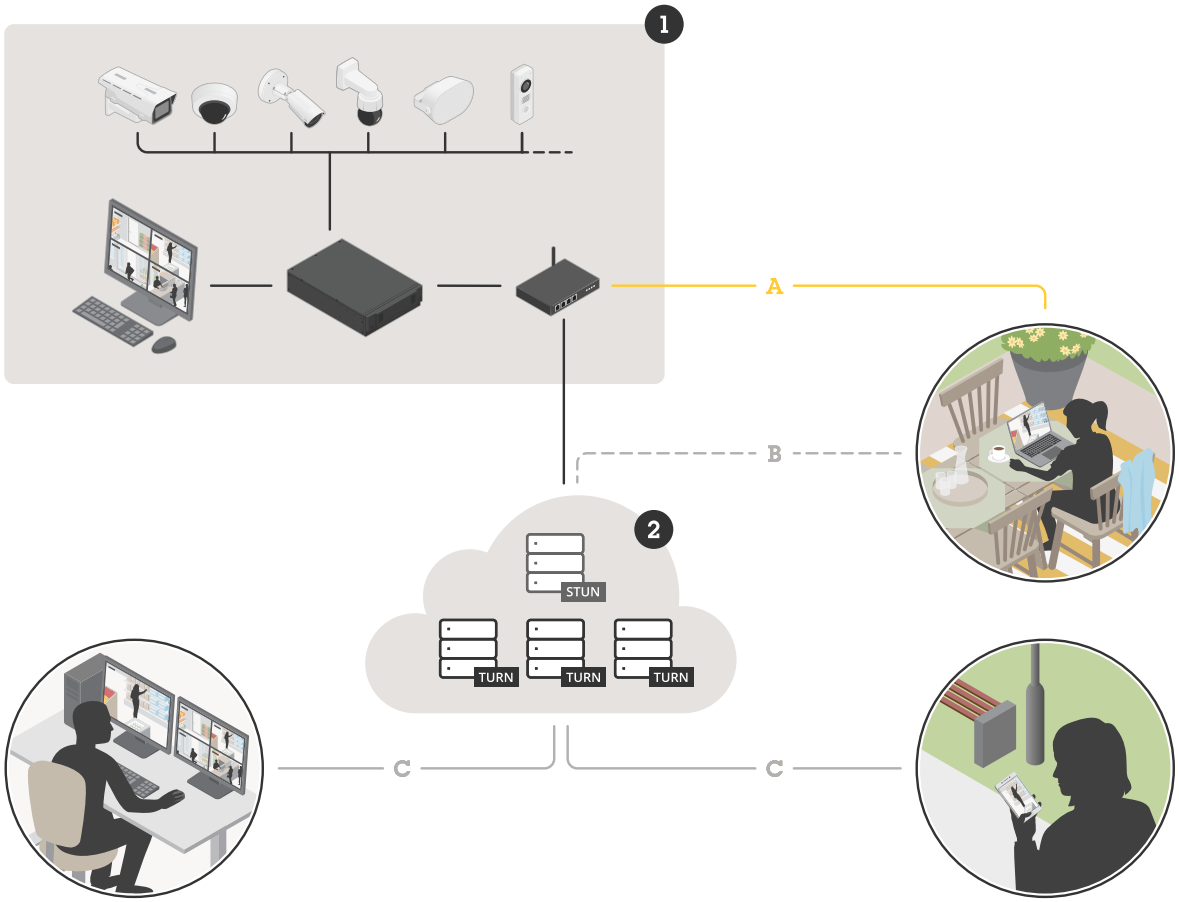
Взаимодействие «клиент — сервер».

Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
Потоковый порт HTTP	29200	TCP	Входящий	Сервер и клиент	Используется для потоковой передачи

					видео, звука и метаданных (шифрование AES).
Основной порт TCP	29202	TCP	Входящий	Сервер и клиент	+2 — смещение относительно потокового порта HTTP. Используется для данных приложения (шифрование TLS 1.2).
Порт веб-сервера API	29204	TCP	Входящий	Сервер и мобильное приложение	+4 — смещение относительно потокового порта HTTP. Используется для данных приложения и видеопотока MP4, передаваемого по протоколу HTTPS.
Медиа-порт API	29205	TCP	Входящий	Сервер и мобильное приложение	+5 — смещение относительно потокового порта HTTP. Используется для передачи видеопотока RTSP по протоколу HTTP.

Порт HTTP локального прокси-сервера	29206	TCP	Входящий	Внутренний обмен данными на сервере	+6 — смещение относительно потокового порта HTTP (ServerPortParser). +2 — смещение относительно порта веб-сервера API (RemoteFacadeBinder). Доступен только внутри системы на серверном компьютере AXIS Camera Station Pro. Обходной порт для неизвестных проблем. Мобильные приложения осуществляют вызовы к модулю SRA, который получает HTTPS, преобразует в HTTP и отправляет на порт HTTP локального прокси-сервера и медиа-порт API.
Порт конечной точки веб-прокси	29207	TCP	Входящий	Сервер и компонент	+7 — смещение относительно потокового порта HTTP. 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 SRA v2 в системе 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 - MyAxis Sign in	https://eu.login.connect.axis.com	443	TCP	Входящие и исходящие
SRA v2 - Обмен данными с облачным сервисом	https://eu.cs.connect.axis.com	443	TCP	Входящие и исходящие
SRA v2 - Обмен данными с API облачного сервиса	https://api.vms.axis.cloud	443	TCP	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

Компонент	Прослушивает интерфейс	Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
Secure Entry	Localhost (127.0.0.1)	Порт веб-сервера	29214	HTTPS	Входящий	Клиент (вкладка Access management (Управление доступом)) и компонент	+14 — смещение относительно потокового порта HTTP. В более ранних системах использовался порт 8081.
Secure Entry	Все (0.0.0.0/INADDR_ANY)	Порт веб-сервера	29215	HTTPS	Входящий	Основной сервер и подсерверы	+15 — смещение относительно потокового порта HTTP. Используется для обмена данными между основным сервером и подсерверами в многосерверных решениях.
Контроль работоспособности системы	Все (0.0.0.0/INADDR_ANY)	Порт веб-сервера	29216	HTTPS	Входящий	Клиент (вкладка System Health	+16 — смещение относительно

Компонент	Прослушивает интерфейс	Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
						Monitoring) и компонент	потокового порта HTTP. Используется для размещения веб-страниц службы мониторинга работоспособности системы System Health Monitoring, а также для обмена данными в многосистемной конфигурации.
Облачная служба контроля работоспособности системы System Health Monitoring Cloud Service	localhost	Порт веб-сервера	29217	HTTPS	Входящий	AXIS Camera Station Pro (веб-страница) и серверный механизм CloudService (плагин)	+17 — смещение относительно потокового порта HTTP. Используется для облачной службы контроля работоспособности системы, обеспечивая контроль работоспособности системы.
Интеллектуальный поиск 2	localhost	Порт веб-сервера	29218	HTTPS	Входящий	Клиент (вкладка Smart search	+18 — смещение относительно

Компонент	Прослушивает интерфейс	Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
						(Умный поиск)) и компонент	потокового порта HTTP. Используется для размещения прикладного программного интерфейса Умного поиска и обслуживания клиентской веб-страницы.
Ядро VMS API	127.0.0.1, ::1	GraphQL API	29219	GraphQL	Входящий	Клиенты VMS API и GraphQL	+19 — смещение относительно потокового порта HTTP. Используется для применения ACS в качестве GraphQL API для клиента
Аутентификация VMS API	127.0.0.1	Аутентификация	29220	gRPC	Входящий	Ядро VMS API и аутентификация	+20 — смещение относительно потокового порта HTTP. Используется ядром VMS API для аутентификации клиентов.
Интерпретатор VMS API acs	127.0.0.1	Интерпретатор ACS	29221	gRPC	Входящий	Ядро VMS API и интерпретатор ACS	+21 — смещение относительно

Компонент	Прослушивает интерфейс	Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
							потокового порта HTTP. Используется ядром API VMS для получения информации о камере.
			29222				Зарезервировано для использования в будущем.
Веб-клиент	localhost	Порт веб-сервера	29223	HTTPS	Входящий	Веб-клиент для VMS API/ Встраиваемый клиент	+23 — смещение относительно потокового порта HTTP. Серверная часть выступает в качестве прокси-сервера перед настраиваемым API VMS.
Встраиваемый клиент	localhost	Порт веб-сервера	29224	HTTPS	Входящий	Клиент, встраиваемый в VMS API/ WebRTC Streamer/ Сигнальный сервер	+24 — смещение относительно потокового порта HTTP. Серверная часть выступает в качестве прокси-сервера перед API VMS.
Конфигурация веб-клиента	localhost	Порт веб-сервера	29225	HTTPS	Входящий	AXIS Camera Station Pro клиент	+25 — смещение относительно

Компонент	Прослушивает интерфейс	Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
						(веб-страница)	потокового порта HTTP. Используется для размещения страницы настройки веб-клиента и серверной части.
Настройка встраиваемого клиента	localhost	Порт веб-сервера	29226	HTTPS	Входящий	AXIS Camera Station Pro клиент (веб-страница)	+26 — смещение относительно потокового порта HTTP. Используется для размещения страницы настройки встраиваемого клиента и серверной части.
			29227				Зарезервировано для использования в будущем.
Локальный генератор конфигураций ICE	localhost	Порт веб-сервера	29228	HTTPS	Входящий	Сигнальный сервер к генератору конфигураций ICE	+28 — смещение относительно потокового порта HTTP. Локальная часть компонента WebRTC.
Настройка локального WebRTC	localhost	Порт веб-сервера	29229	HTTPS	Входящий	AXIS Camera Station Pro клиент (веб-страница)	+29 — смещение относительно потокового порта

Компонент	Прослушивает интерфейс	Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
							HTTP. Используется для размещения страницы настройки WebRTC и серверной части. Локальная часть компонента WebRTC.
Локальный сервер TURN	localhost	порт сервера coturn	29230	UDP	Входящий/исходящий	Встраиваемый клиент/веб-клиент - сервер TURN	+30 — смещение относительно потокового порта HTTP. Используется для "WebRTC с одним портом" в ACS onprem.
			29231				Зарезервировано для использования в будущем.
Локальный IDP IAM	0.0.0.0	IDP_OIDC (общедоступный)	29232	HTTPS	Входящий	Обратный прокси-сервер и локальный IAM	+32 — смещение относительно потокового порта HTTP. Общедоступный порт.
Локальный IDP IAM	0.0.0.0	MTLS (администратор)	29233	HTTPS	Входящий	Сторонние службы	+33 — смещение относительно потокового порта HTTP.

Компонент	Прослушивает интерфейс	Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
							Порт администратора.
Локальный IDP IAM	127.0.0.1	ТОКЕНИЗАТОР	29234	HTTPS	Входящий	Сторонние службы	+34 — смещение относительно потокового порта HTTP. Порт токенизатора.
WebRTC	localhost	API для адаптации	29235	HTTPS	Входящий	Облачный компонент	+35 — смещение относительно потокового порта HTTP. Служит для настройки облачного подключения webrtc во время адаптации. Входит в состав компонента WebRTC.
OpenTelemetry	127.0.0.1	gRPC-порт	29236	gRPC	Входящий	Сторонние службы	+36 — смещение относительно потокового порта HTTP.
OpenTelemetry	127.0.0.1	Порт HTTP	29237	HTTPS	Входящий	Сторонние службы	+37 — смещение относительно потокового порта HTTP.
Audio Manager Pro		Порт веб-сервера	29238	HTTPS	Входящий	Сервисы и компоненты интеграции	+38 — смещение относительно

Компонент	Прослушивает интерфейс	Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
						сторонних разработчиков	потокового порта HTTP.
			29239				Зарезервировано для использования в будущем.
			29240				Зарезервировано для использования в будущем.
Data Insights Dashboard	localhost	2dpc/3dpc push Приемник	29241	HTTPS	Входящий (внешний)	Получатель push-сообщений (post), содержащих данные подсчета из 2dpc и 3dpc. Внутренний: база данных, брокер Mosquitto	+41 — смещение относительно потокового порта HTTP.
Data Insights Dashboard	0.0.0.0	Брокер Mosquitto	29242	MQTTS	Входящий (внешний) Исходящий (внешний)	Получатель сообщений о событиях камеры. При необходимости можно объединить брокеры MQTT (многие к одному, например, с помощью темы. Дублирование базы данных и	+42 — смещение относительно потокового порта HTTP.

Компонент	Прослушивает интерфейс	Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
						балансировка нагрузки доступны для профессиональных сервисов при настройке объекта) Внутренний: Приемник	
			29243				Зарезервировано для использования в будущем.
Брокер NATS	127.0.0.1	NATS	29244	NATS	Входящий	Между AXIS Camera Station Pro и компонентами, а также между самими компонентами	+44 — смещение относительно потокового порта HTTP.
OpenTelemetry	127.0.0.1	Порт HTTP	29245	HTTP;	Входящий	Конечная точка мониторинга для получения метрик из коллектора OpenTelemetry	+45 — смещение относительно потокового порта HTTP.
Обратный прокси-сервер (ReverseProxyPortInternal)	Все (0.0.0.0/INADDR_ANY)	Резервный порт обратного прокси-сервера, используемый хостом периферийного устройства	29248	HTTPS	Входящий	Пограничный хост и обратный прокси-сервер	+48 — смещение относительно потокового порта HTTP.

Другие порты

Порт	Номер	Протокол	Вход/выход	Обмен данными между	Описание
Internet HTTPS	80 и 443	TCP	Исходящий	Клиент и сервер к Интернету	Используется для активации лицензии, скачивания встроенного ПО, подключенных услуг и т. д.
Порт потоковой передачи TCP сервера	29198	TCP	Входящий	Сервер и устройство	-2 — смещение относительно потокового порта HTTP.
Состояние обновления порта UDP	15156	UDP	Входящий + Исходящий	Управление серверами и службами	AXIS Camera Station Pro Приложение Service Control прослушивает порт, после чего сервер делает широковеща-тельную рассылку о состоянии текущего обновления.

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

База данных архивируется каждый вечер и перед каждым обновлением системы. 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 указать 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

- Записи в базе данных не хранятся, вместо этого укажите путь для их хранения в разделе **Configuration > Storage (Конфигурация > Устройство хранения)**. Создавайте резервные копии записей отдельно.
- Настройки сервера и базы данных в AXIS Camera Station Pro Service Control не сохраняются.

Резервное копирование системы

Система автоматически сохранит резервную копию в папке, указанной на вкладке **Database (База данных)**, см. *Настройки базы данных, on page 233*. Резервная копия системы содержит как основные файлы базы данных, так и дополнительные файлы базы данных, см. *Файлы базы данных, on page 232*.

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 если вы используете компонент. Например, AXIS Camera Station Secure Entry или умный поиск. • **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. • **Умный поиск**: Эта папка содержит файл базы данных умного поиска smartSearch-backup-yyyyMMddHHmmssfff.sqlite3.
backup_summary.json	в этих файлах содержится подробная информация о резервной копии.
_cluster_yyyyMMddHHmmssfff.dbcbackup	Этот файл содержит логическую резервную копию кластера базы данных PostgreSQL, включающую общекластерные данные, такие как роли и табличные пространства.

Служебное резервное копирование

Укажите папку для хранения служебных резервных копий на вкладке **Database (База данных)**, см. *Настройки базы данных, on page 233*. 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.
- Вручную из AXIS Camera Station Pro Service Control при выполнении обслуживания базы данных. См. *Обслуживание базы данных, on page 236*.
- Автоматически с помощью запланированной задачи обслуживания базы данных, настроенной в планировщике заданий Windows. См. *Инструменты, on page 238*.

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.

Резервное копирование в ручном режиме можно выполнить двумя способами:

- **Способ 1:**перейдите в папку `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` и создайте копию файлов базы данных. Затем выполните резервное копирование кластера базы данных PostgreSQL:
  1. Откройте терминал с правами администратора в каталоге, в котором требуется сохранить резервную копию.
  2. Выполните команду `C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" backup -cluster`
  3. Резервная копия сохраняется в папке с именем **yyyyMMddHHmmssfff** в каталоге, в котором был открыт терминал.
- **Способ 2:** создайте отчет о системе со всеми включенными базами данных и скопируйте файлы резервной копии базы данных. Обязательно выберите **Include all databases (Включить все базы данных)**. См. *Системный отчет, on page 213*.

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. Дополнительные сведения о резервном копировании базы данных см. в разделе *Создайте резервную копию базы данных, on page 233*.

Примечание

Записи в базе данных не хранятся, вместо этого укажите путь для их хранения в разделе **Configuration > Storage (Конфигурация > Устройство хранения)**. Создавайте резервные копии 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 233*.
3. Извлеките файлы.
4. Восстановите кластер базы данных PostgreSQL:
   4.1. Откройте терминал с правами администратора в распакованной папке.
   4.2. Выполните команду `"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 доверие 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`.

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 Service Control и нажмите **Start (Пуск)**, чтобы запустить службу.

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 238*.

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 в редких случаях принудительного сжатия.

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 – Исключите базу данных из поиска вирусов, так как некоторые антивирусные программы могут повредить базу данных. Если используется внешняя система резервного копирования, не создавайте резервную копию текущей и 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 проверяйте оперативную память на ошибки с помощью утилиты диагностики памяти Windows Memory Diagnostic.

Сертификаты

Во вкладке **Certificates (Сертификаты)** можно управлять серверными сертификатами 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, при этом используются только алгоритмы RSA с ключами длиной не менее 2048 бит.

Примечание

При импорте сертификата в формате PEM с промежуточными сертификатами, все промежуточные сертификаты должны содержаться в одном файле с расширением .cer. Если вы создаете собственные сертификаты, см. раздел *Подготовка промежуточных сертификатов к импорту, on page 237*.

Текущий сертификат

Отображает информацию о действующем серверном сертификате, используемом для ручной проверки корректности подключения клиента к 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 конец другого и измените имя в первой строке на combined_cert.cer:
```
combined_cert.cer
———BEGIN CERTIFICATE———
MIIFTDCCB....
———END CERTIFICATE———
———BEGIN CERTIFICATE———
MIIE+zCCA+OgA.....
———END CERTIFICATE———
```
3. Сохраните файл.

Инструменты

В управлении службой AXIS Camera Station Pro Service Control выберите **Modify settings (Изменить параметры)** и перейдите на вкладку **Tools (Инструменты)**, чтобы запустить процесс обслуживания базы данных и создать частичный системный отчет.

Обслуживание БД

- Откройте управление службами AXIS Camera Station Pro Service Control.
- Нажмите **Tools (Инструменты)**.
- Нажмите **Run (Выполнить)** в разделе **Database maintainer (Обслуживание базы данных)**.
- Будет показано ожидаемое время остановки базы данных. Щелкните **Да**, чтобы продолжить. Запущенный процесс отменить невозможно.

Примечание

- AXIS Camera Station Pro На время обслуживания сервер и все текущие операции записи останавливаются. После завершения технического обслуживания сервер автоматически запускается.
- Не выключайте компьютер во время технического 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 настроить триггер задачи и указать, когда и как часто нужно запускать обслуживание базы данных.

Системный отчет

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. Для создания полного системного отчета выберите  **> Help > System report (Справка > Системный отчет)** в клиенте AXIS Camera Station Pro.

Чтобы создать частичный системный отчет:

1. Нажмите **Выполнить**.
2. Выберите и введите запрашиваемую информацию в диалоговом окне.
3. Нажмите **Создать отчет**.

Средство создания системного отчета	
Имя файла	Введите имя файла для системного отчета.
Папка	Выберите место сохранения отчета сервера.
Автоматически открывать папку по готовности отчета	После выбора папка будет автоматически открываться, когда системный отчет будет готов.
Включить файл базы данных в отчет	Выберите для включения базы данных в системный отчет. База данных AXIS Camera Station Pro содержит информацию о записях и другие данные, необходимые для правильной работы системы.

Ведение журнала сети

- Перейдите по ссылке, чтобы загрузить приложение для анализа сетевых протоколов.
- После установки можно будет запускать это приложение с помощью кнопки **Пуск**.

Поиск и устранение неисправностей

Об этом руководстве

В этом руководстве описаны возможные неисправности AXIS Camera Station Pro и способы их устранения. Неисправности отсортированы по разделам для удобства поиска, например, разделы «Звук» или «Живой просмотр». Для каждой неисправности описано возможное решение.

Подробнее

Посетите сайт *axis.com/support*, где размещены:

- Ответы на типичные вопросы
- Аппаратные требования
- Обновленное программное обеспечение
- Пособия, учебные материалы и другая полезная информация

Перезапустите службу сервера.

Перезапуск службы сервера AXIS Camera Station Pro может решить некоторые общие проблемы.

Примечание

- Перезапуск службы сервера может занять некоторое время. Отменить перезапуск нельзя.
- Во время перезапуска службы сервер недоступен.
- Во время перезапуска службы все подключенные устройства теряют связь с сервером.

Для перезапуска службы сервера:

1. Откройте меню **Configuration (Конфигурация)** > **Server (Сервер)** > **Diagnostics (Диагностика)**.
2. Нажмите **Restart AXIS Camera Station server service... (Перезапуск службы сервера AXIS Camera Station...)**.

Служба AXIS Camera Station Pro

Служба AXIS Camera Station Pro часто перезапускается

Сервер может быть перегружен, из-за чего увеличивается очередь задач; также возможно повреждение баз данных.

- Проверьте панель управления ресурсами в вашей системе и убедитесь в том, что AXIS Camera Station Pro или любое другое приложение не используют слишком много системных ресурсов.
- Выполните обслуживание базы данных, см. раздел *Обслуживание базы данных* в AXIS Camera Station Pro руководстве пользователя.

Если приведенные выше решения не помогли, обратитесь за помощью в службу поддержки Axis. См. раздел *Порядок отправки запроса о решении проблемы в службу поддержки, on page 257*.

Устройства в системе управления видео

Неполадки общего характера

Не удается установить связь с камерой	
Системе управления видео не удается установить связь с камерой. Перечисленные камеры не добавлены.	1. Убедитесь в том, что камера подключена к сети, что на ней присутствует питание и что камера работает. 2. Еще раз попытайтесь добавить камеру в меню **Configuration > Add devices (Конфигурация > Добавить устройства)**.

Установка отменена	
Пользователь отменил установку. Перечисленные камеры не добавлены.	Чтобы добавить новые камеры, войдите в меню **Конфигурация > Добавить устройства**.

Не удалось установить пароль для камеры	
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

Если перед добавлением устройства в AXIS Camera Station Pro оно использовалось в другой системе,

- выполните сброс устройства к заводским установкам по умолчанию.

Если в систему управления видео не удается добавить устройство, попробуйте добавить его в приложение AXIS Device Manager.

Вы можете добавить другую модель устройства, отличную от той, которую вы хотите добавить:

- Если устройство было недавно выпущено на рынок или в нем установлена новая версия встроенного ПО, может возникнуть проблема с совместимостью. Всегда используйте последнюю версию ПО AXIS Camera Station Pro.

Если не удается добавить устройство другой модели:

- Найдите неисправность в камере и устраните ее, см. *axis.com/support/troubleshooting*.

Не удается обновить встроенное ПО устройства через AXIS Camera Station Pro

Если не удается обновить камеру через ее веб-интерфейс, выполните следующие действия:

- Найдите неисправность в камере и устраните ее, см. *axis.com/support/troubleshooting*.

Не удается обновить встроенное ПО на всех устройствах:

- Проверьте сетевое подключение.
- Если проблема не связана с сетью, обратитесь за помощью в службу поддержки Axis. См. раздел *Порядок отправки запроса о решении проблемы в службу поддержки, on page 257*.

Не удается обновить встроенное ПО на устройствах определенных моделей:

- Возможно, возникла проблема с совместимостью, обратитесь в службу поддержки Axis. См. раздел *Порядок отправки запроса о решении проблемы в службу поддержки, on page 257*.

Устройства не найдены

Система управления видео автоматически выполняет поиск в сети подключенных камер и видеокодеров, однако не находит камеры.

- Убедитесь, что камера имеет сетевое подключение и 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. Перейдите к разделу *Параметры прокси-сервера на клиенте* в AXIS Camera Station Pro руководстве пользователя.
  - Если между клиентом и сервером находится NAT или система безопасности, измените параметры NAT или системы безопасности. Убедитесь в том, что порт HTTP, порт TCP (протокол управления передачей) и порт потоковой передачи, указанные в AXIS Camera Station Service Control, не заблокированы системой безопасности или NAT. Полный список портов см. в разделе *Список портов для AXIS Camera Station Pro, on page 218*.
  - Если между сервером и устройствами находится прокси-сервер, измените настройки прокси-сервера. См. раздел «Настройки прокси» в разделе *Общие сведения о Service Control* в руководстве пользователя AXIS Camera Station Pro.
- Для добавления камер вручную перейдите в раздел *Добавление устройств* в руководстве пользователя AXIS Camera Station Pro.

Повторяющееся сообщение "Повторное подключение к камере через 15 секунд"

Возможные проблемы:

- Перегрузка сети.
- Камера недоступна. Убедитесь, что камера имеет сетевое подключение и питание.
- 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.
- Измените настройки видео и звука, например, путем оптимизации параметров профиля для работы в режиме экономии трафика.

Записи

Более подробную информацию о проблемах с производительностью, влияющих на запись и воспроизведение, см. в разделе *Просмотр в реальном времени, on page 245*.

Неполадки общего характера

Непрерывная запись не включена	
Для указанных в списке камер не включена непрерывная запись.	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	
Системе не удается настроить хранилище записей.	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 удалось установить приложение AXIS Video Content Stream	
Это сообщение об ошибке выводится, если приложение AXIS Video Content Stream не удалось установить на совместимую с ним камеру.	1. Чтобы установить приложение вручную, откройте меню **Configuration > Devices > Management (Конфигурация > Устройства > Управление)**. 2. Выберите камеру и нажмите  .

Запись не запускается

Если запись не запускается или останавливается через несколько секунд после запуска, это означает, что на диске не осталось места или имеется слишком много посторонних данных.

- Проверьте **Recording Storage (Хранилище записей)** в Server Configuration Sheet (Лист конфигурации сервера) на предмет наличия свободного места и отсутствия посторонних данных.
- Увеличьте лимит хранилища для системы управления видео.
- Выделите больше пространства для хранения. Перейдите в раздел *Настройка хранения данных* в AXIS Camera Station Pro руководстве пользователя.

Пробелы в записи во время непрерывной записи

Наряду с пробелами в записи выдаются оповещения об **Ошибках записи**. Пробел может возникнуть по следующим причинам:

- Перегрузка сервера
- Проблема с сетью
- Перегрузка камеры
- Перегрузка диска

Проверьте наличие пробелов в записи на других камерах. Если это происходит не на всех камерах, это может указывать на перегрузку камеры. Задайте себе следующие вопросы, чтобы определить причину:

- Как часто возникает пробел: каждый час или каждый день?
- Какова длительность пробела: несколько секунд или несколько часов?
- В какое время возникает пробел?

Возможные решения:

- В диспетчере задач проверьте использование аппаратных ресурсов, обращая внимание на возможное избыточное использование. При наличии признаков избыточного использования дисков добавьте дополнительные диски и перенастройте несколько камер для записи на новые диски.
- Уменьшите объем данных, записываемых на диск (параметры видео, Zipstream, FPS, разрешение). Следует помнить о пропускной способности, рассчитываемой AXIS Site Designer, см. *axis.com/support/tools/axis-site-designer*.

Дополнительные сведения см. в разделе *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).

Более подробную информацию см. в разделе *Воспроизведение и проверка экспортированных записей* в руководстве пользователя AXIS Camera Station Pro.

Примечание

Проигрыватель AXIS File Player автоматически откроет все записи, находящиеся в одной папке с проигрывателем.

Записи исчезают

Система сохраняет записи только в течение определенного срока, заданного в днях. Чтобы изменить срок в днях, откройте меню **Конфигурация > Устройство хранения > Выбор**.

Если ресурс хранения заполнен, система удалит записи до истечения указанного срока хранения. Чтобы избежать переполнения хранилища, попробуйте сделать следующее:

- 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)**.
  - Для записи используйте формат H. 264, поскольку формат M-JPEG требует значительно больше пространства хранения.
  - Для дополнительного уменьшения размера записей используйте Zipstream.

Проблемы с резервной записью

После восстановления подключения не выполняется резервная запись на сервер.

Причина	Решение
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.	• Убедитесь, что вы синхронизировали NTP для будущих записей. • Синхронизируйте время камеры с сервером или настройте одинаковый NTP-сервер на камере и сервере.

Отказоустойчивая запись на AXIS Camera Station Pro не будет работать в следующих случаях:

- Управляемое выключение сервера.
- Кратковременные (менее 10 секунд) сбои в подключении.

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	При использовании встроенной видеокарты не рекомендуется использовать более двух мониторов на каждую видеокарту. 1. Откройте средство диагностики DirectX (выполните поиск по запросу «dxdiag» на компьютере) 2. Убедитесь в том, что AXIS Camera Station Pro поддерживает используемую дискретную видеокарту. Примечание Вы не можете запустить клиент на виртуальной машине.

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	Может возникать проблема, особенно при использовании некоторых камер серии M. • Измените поток на тот же профиль потока или выберите более низкое разрешение. См. раздел *Streaming profiles (Профили потока)* в AXIS Camera Station Pro руководстве пользователя. • Измените поток на тот же профиль потока или выберите более низкое разрешение. См. раздел *Streaming profiles (Профили потока)* в AXIS Camera Station Pro руководстве пользователя.

Перегрузка сервера	
Необычное использование ЦП/ОЗУ в момент, совпадающий с временем возникновения проблемы	Убедитесь, что параллельно не запущены другие ресурсоемкие приложения, нагружающие ЦП/ОЗУ.

Проблема с сетью	
Необычное использование полосы пропускания в момент, совпадающий с временем возникновения проблемы.	Убедитесь, что параллельно не запущены другие приложения, загружающие полосу пропускания.
Достаточная происканная способность / Удаленная или локальная сеть	• 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 оно включено, см. раздел «Аппаратное декодирование» в теме *Потоковая передача* в AXIS Camera Station Pro руководстве пользователя.

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 серверный отчет по камере, см. *axis.com/support/troubleshooting*.
- Убедитесь в том, что установленное антивирусное программное обеспечение не блокирует поток живого видео.

- Предоставьте разрешения для папок и процессов AXIS Camera Station Pro, см. раздел *Часто задаваемые вопросы*.
- Убедитесь в том, что межсетевой экран не блокирует подключение на определенных портах, см. раздел *Общие сведения о Service Control* в AXIS Camera Station Pro руководстве пользователя.
- Убедитесь, что установлен компонент «Возможности рабочего стола» для поддерживаемых версий ОС Windows Server. См. раздел *Scheduled export (Запланированный экспорт)* в AXIS Camera Station Pro руководстве пользователя.
- Проверьте, работает ли видеопоток с более низким разрешением.

Если приведенные выше решения не помогли, обратитесь за помощью в службу поддержки Axis *Порядок отправки запроса о решении проблемы в службу поддержки, on page 257*.

Хранение данных

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 удалось установить приложение AXIS Video Motion Detection	
Не удалось установить AXIS Video Motion Detection 2 или 4. Запись по обнаружению движения будет производиться с помощью встроенной функции обнаружения движения.	Чтобы установить приложение вручную, см. раздел *Установка приложений для камеры* в руководстве пользователя AXIS Camera Station Pro.

Не удалось получить текущие настройки обнаружения движения	
Системе управления видео не удается получить параметры обнаружения движения с камеры. Запись по обнаружению движения будет производиться с помощью встроенной функции обнаружения движения.	Чтобы установить приложение вручную, см. раздел *Установка приложений для камеры* в руководстве пользователя AXIS Camera Station Pro.

Не настроен детектор движения	
Не удается настроить детектор движения в указанных камерах.	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.

Детектор движения не включен	
На перечисленных камерах запись при обнаружении движения не включена.	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 описываются возможные решения проблемы, при которой видеодетектор обнаруживает слишком много или слишком мало движущихся объектов.

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. раздел *Изменение настроек AXIS Video Motion Detection 2 и 4* в AXIS Camera Station Pro руководстве пользователя.
Встроенный видеодетектор движения	Возможна настройка окон включения и исключения. См. раздел *Настройка встроенного видеодетектора движения* в AXIS Camera Station Pro руководстве пользователя.

Регулировка периода срабатывания

Период действия триггера — это интервал времени между двумя последовательными срабатываниями триггера. Эта настройка используется для того, чтобы уменьшить количество последовательно производимых записей. Запись продолжается, если в течении этого периода триггер срабатывает повторно. Если срабатывает еще один триггер, то с этого момента начинается новый период срабатывания.

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 нет звукового сопровождения, проверьте следующее:

- 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 (Звук)** выберите микрофон в раскрывающемся меню **Microphone (Микрофон)**.
5. В раскрывающемся меню **Use microphone for (Использовать микрофон для)** укажите, когда следует использовать звук.
6. Если применимо, выберите громкоговоритель в раскрывающемся меню **Speaker (Громкоговоритель)**.

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. Дополнительные сведения см. в разделе *Stream profiles (Профили потока)* в AXIS Camera Station Pro руководстве пользователя.

Нет звука при воспроизведении

Воспроизведение записи со звуковым сопровождением возможно лишь при условии, что в профиле, который использовался при записи, был включен звук.

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 подключении к нескольким серверам запускается клиентское ПО, при

этом состояние подключения отображается в строке состояния. Подробнее о состоянии соединения см. в разделе *Состояние соединения* в AXIS Camera Station Pro руководстве пользователя.

Неправильное имя пользователя или пароль	Неправильно введены имя пользователя и пароль при попытке подключиться к указанному серверу.	• Проверьте написание или воспользуйтесь другой учетной записью. • Убедитесь в том, что пользователь имеет 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 при этом входящий в локальную группу администраторов данного сервера, должен обязательно использовать права администратора при запуске клиента. • Сведения о правах доступа пользователей см. в разделе *Настройка прав доступа* пользователей в руководстве пользователя AXIS Camera Station Pro.
Пользователь не имеет полномочий для входа на этот сервер	Пользователь не может использовать AXIS Camera Station Pro на указанном сервере.	Укажите пользователя в диалоговом окне полномочий.
Не удается проверить безопасность сообщения	Во время установки защищенного соединения с сервером произошел сбой, вызванный, скорее всего, отсутствием синхронизации времени на клиенте или на сервере.	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	Не удается установить соединение клиентского узла с сервером.	• Проверьте, подключен ли серверный компьютер к сети. • Проверьте, работает ли серверный компьютер. • Проверьте, правильно ли настроен брандмауэр. • Проверьте написание адреса сервера. • Проверьте параметры прокси клиента.
Сервер не отвечает	Соединение клиентского узла с сервером установлено, но, как выяснилось, серверное ПО AXIS Camera Station Pro не работает.	Проверьте, к тому ли компьютеру вы подключаетесь и запущено ли на нем серверное ПО AXIS Camera Station Pro.

Клиенту не удается подключиться к серверу	Клиент не может подключиться к серверу и отображается сообщение об ошибке.	Проверьте правильность настройки сети. • Убедитесь, что используемая операционная система поддерживается. Полный список поддерживаемых операционных систем см. в *заметках о выпуске*. • В Service Control убедитесь в том, что сервер AXIS Camera Station Pro работает. 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. • Проверьте, имеется ли между сервером и клиентом прокси-сервер. – Настройте прокси-сервер в приложении Service Control. – Настройте параметры прокси-сервера клиента на странице входа в систему, выберите **Change proxy settings (Изменить параметры прокси-сервера)**. – Настройте параметры прокси-сервера в разделе параметров Интернета Windows и задайте для него параметр по умолчанию в разделе **Change Proxy settings (Изменить параметры прокси-сервера)**.
Не удается подключиться к серверу	При подключении к серверу произошел неожиданный сбой.	• Проверьте правильность адреса и порта сервера AXIS Camera Station Pro. • Проверьте, не блокируется ли подключение к серверу межсетевым экраном, антивирусной программой или NAT. Дополнительные сведения см. в разделе *Configure the firewall to allow access to AXIS Secure Remote Access (Настройка брандмауэра для разрешения доступа к AXIS Secure Remote Access)*. • Проверьте работоспособность сервера через AXIS Camera Station Pro Service Control. – Откройте AXIS Camera Station Pro Service Control, см. раздел *AXIS Camera Station Service Control* в AXIS Camera Station Pro руководстве пользователя. – 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	Клиент не распознаёт введенный IP-адрес.	• Проверьте, подключен ли серверный компьютер к сети. • Проверьте правильность адреса и порта сервера AXIS Camera Station Pro. • Проверьте, не блокируется ли подключение к серверу межсетевым экраном, антивирусной программой или NAT. Дополнительные сведения см. в разделе *Configure the firewall to allow access to AXIS Secure Remote Access (Настройка брандмауэра для разрешения доступа к AXIS Secure Remote Access)*.
На сервере и клиенте установлены разные версии ПО	Версия клиентского ПО AXIS Camera Station Pro новее версии серверного ПО.	Обновите серверное ПО до той же версии, что и клиентское ПО.
	Версия серверного ПО AXIS Camera Station Pro новее версии клиентского ПО.	Обновите клиентское ПО до той же версии, что и серверное ПО.
Не удалось подключиться к серверу. Сервер перегружен.	Нет отклика от сервера из-за проблем с производительностью.	Проверьте, не перегружены ли сеть и компьютер, на котором установлен сервер.
Локальный сервер AXIS Camera Station Pro не работает	Вы установили соединение через меню **This computer (Этот компьютер)**, однако не работает установленный сервер AXIS Camera Station Pro.	Используйте Service Control для запуска AXIS Camera Station Pro или выберите удаленный сервер для входа в систему.
На данном компьютере не установлен сервер AXIS Camera Station Pro.	Вы устанавливаете соединение через меню **This computer (Этот компьютер)**, однако на этом компьютере не установлено серверное ПО.	Установите серверное ПО AXIS Camera Station Pro или выберите другой сервер.
Выбранный список серверов пуст	Список серверов, выбранный для входа в систему, оказался пустым.	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 раздел **Configuration (Настройка)** и убедитесь в том, что активирована опция **Automatic licensing (Автоматическое лицензирование)**, см. раздел *Управление лицензиями* в руководстве пользователя AXIS Camera Station Pro.
- Убедитесь в том, 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 пользователей домена найти не удалось, нужно сменить учетную запись для входа в сервисную систему:

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 взаимодействовать с устройством, пока не устранена ошибка сертификата.

Возможные ошибки		
Сертификат не найден	Если сертификат устройства был удален.	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	Сертификат устройства был изменен за пределами AXIS Camera Station Pro. Это может означать, что устройство подверглось несанкционированному доступу и модификации.	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

При наличии центра сертификации в AXIS Camera Station Pro без сохраненного пароля появится следующий сигнал тревоги.

Необходимо предоставить пароль для сертификата центра сертификации. Дополнительные сведения см. в руководстве пользователя.

Устранить эту проблему можно тремя разными способами:

- 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 раздел **Configuration (Конфигурация) > Security (Безопасность) > Certificates (Сертификаты) > Devices (Устройства)**.
2. В разделе HTTPS отключите параметр **Validate device certificate (Проверить 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 раздел **Configuration (Конфигурация) > Security (Безопасность) > Certificates (Сертификаты) > Devices (Устройства)** и включите **Validate device certificate (Проверить 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 раздел **Configuration (Конфигурация) > Security (Безопасность) > Certificates (Сертификаты) > Devices (Устройства)**.
2. В разделе HTTPS отключите параметр **Validate device certificate (Проверить 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 раздел **Configuration (Конфигурация) > Security (Безопасность) > Certificates (Сертификаты) > Devices (Устройства)** и включите **Validate device certificate (Проверить 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 происходить, когда служба времени Windows не может установить соединение с сервером NTP.

- Для решения проблемы проверьте следующее:
- Настройки брандмауэра должны быть корректными.
- Устройство должно находиться в сети, имеющей доступ к серверу NTP.

Для получения поддержки обратитесь к системному администратору.

На устройстве обнаружена разница во времени

Устройство не синхронизировано по времени с сервером. Запись содержит отметку времени о получении сервером, а не отметку времени о записи на устройстве.

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 в том, что устройство может получить доступ к указанному NTP-серверу.
   2.3. Перезагрузите устройство в меню **Configuration > Devices > Management (Конфигурация > Устройства > Управление)**.
3. Если смещение времени сервера составляет меньше 2 секунд, устройство, возможно, не отправляет достаточно данных для синхронизации времени.
   3.1. Снимите флажок **Send alarm when the time difference between server and device is larger than 2 seconds (Отправить сигнал тревоги, когда разница во времени между сервером и устройством превышает 2 секунды)** для отключения сигналов тревоги.

Для получения поддержки 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

В случае возникновения неисправностей, которые не могут быть устранены с использованием этого руководства, обратитесь в онлайн-службу технической поддержки Axis, см. раздел *Онлайн-служба технической поддержки Axis*. Чтобы служба поддержки могла лучше понять имеющуюся проблему и предложить ее решение, необходимо предоставить следующую информацию:

- Четкое описание того, как можно воспроизвести проблему или обстоятельств, при которых возникает проблема.
- Время возникновения проблемы и имя или IP-адрес неисправной камеры.
- AXIS Camera Station Pro Системный отчет , сформированный непосредственно после возникновения проблемы. Системный отчет должен быть сформирован из клиента или сервера, на которых была воспроизведена проблема.
- По возможности приложите скриншоты или записи со всех мониторов, которые демонстрируют проблему. Активируйте функцию накладываемой информации для отладки при создании моментальных снимков или при выполнении записи.
- При необходимости включите файлы базы данных. Исключите их, чтобы ускорить загрузку.

Некоторые проблемы требуют дополнительной информации, которую служба поддержки запрашивает при необходимости.

Примечание

Если размер файла превышает 100 МБ, например, файл трассировки сети или файл базы данных, отправьте файл с использованием надежной службы общего доступа к файлам, которой вы доверяете.

Дополнительная информация	
Журналы на уровне отладки	Иногда может потребоваться включить создание журнала на уровне отладки для сбора дополнительных сведений. Это делается только по запросу инженера службы поддержки Axis. За инструкциями обращайтесь в *онлайн-службу технической поддержки Axis.*
Накладываемая информация для отладки режима «Живой просмотр»	В некоторых случаях может потребоваться предоставление снимков экрана с накладываемой информацией или видеоизображений, показывающих изменение значений в интересующий вас момент времени. Для добавления накладываемой информации выполните следующие действия: • Нажмите клавиши Ctrl и i один раз, чтобы отобразить накладываемую информацию в режиме живого просмотра. • Нажмите клавиши Ctrl и i два раза, чтобы добавить отладочную информацию. • Нажмите клавиши Ctrl и i три раза, чтобы скрыть накладку.
Трассировка сети	Если об этом попросит инженер службы поддержки, сгенерируйте трассировки сети при создании отчета о системе. Трассировки сети, полученные в момент возникновения проблемы, если ее можно воспроизвести. К этим данным относятся: • Полученная с камеры трассировка сети, продолжительностью 60 секунд

Дополнительная информация	
	(применимо только к камерам со встроенным ПО версии 5.20 и более поздней) Используйте следующую команду VAPIX, чтобы при необходимости изменить логин, IP-адрес и продолжительность (в секундах): `http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60` • Полученная с сервера трассировка сети, продолжительностью 10–30 секунд, демонстрирующая обмен данными между сервером и камерой.
Файлы базы данных	В случае, когда нам требуется изучить или вручную восстановить работу базы данных. Выберите **Include database in the report (Добавить базу данных в отчет)**, перед тем как будет сформирован системный отчет.
Снимки экрана	Используйте снимки экрана, если проблема связана с интерфейсом пользователя в живом просмотре. Например, если вам необходимо показать временную шкалу для записей, или если проблема сложно поддается описанию.
Записи экрана	Используйте записи экрана, если сложно описать проблему на словах, то есть когда для воспроизведения проблемы необходимо выполнить много действий в пользовательском интерфейсе.

T10196821_ru

2026-01 (M24.3)