AXIS Perimeter Defender

AXIS Perimeter Defender

AXIS Perimeter Defender PTZ Autotracking

Руководство пользователя

Содержание

AXIS Perimeter Defender

AXIS Perimeter Defender

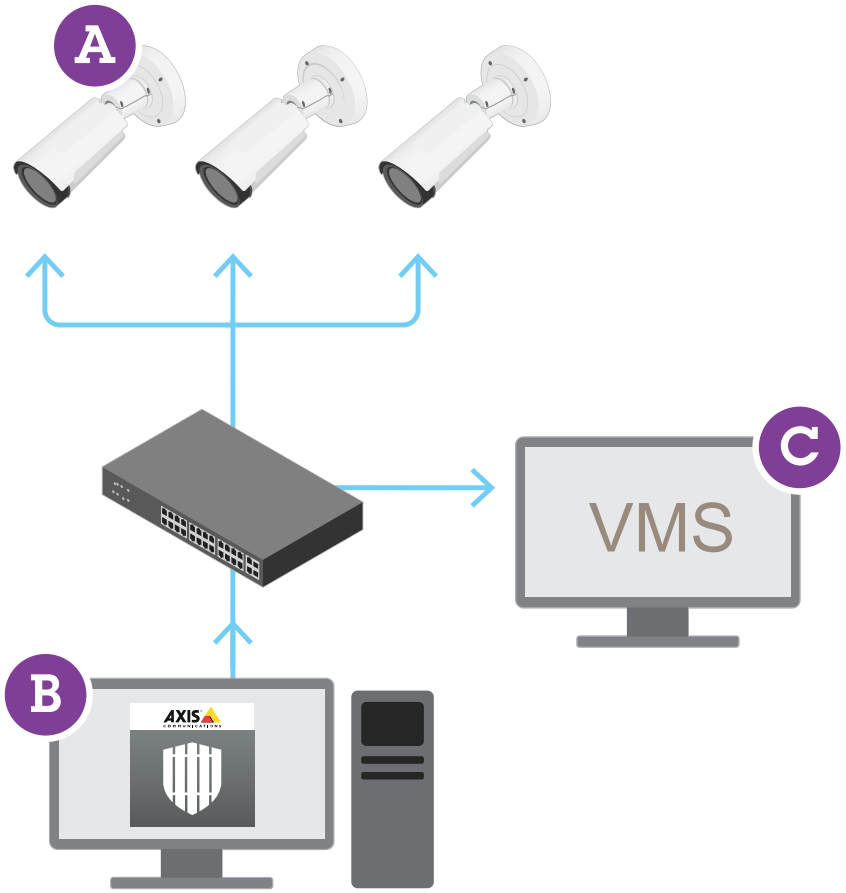
AXIS Perimeter Defender

AXIS Perimeter Defender представляет собой приложение для охранного видеонаблюдения и защиты периметра. Оно идеально подходит для защиты периметра в тех случаях, когда требуется высокая надежность, если необходимо усилить систему физического контроля доступа и обеспечить надежное обнаружение вторжений.

AXIS Perimeter Defender в первую очередь предназначается для защиты «охраняемых территорий», например участков вдоль забора на границе. Термин «охраняемая зона» обозначает зону, в которой не предполагается присутствие людей.

Используйте AXIS Perimeter Defender на открытом воздухе для следующих целей:

- Обнаружение движущихся людей.
- Обнаружение движущихся транспортных средств без разделения на их типы.



Тепловизионные камеры AXIS Q1951-E и AXIS Q1952-E Thermal Camera могут запускать приложение в режиме калибровки, в режиме на основе технологии искусственного интеллекта или в обоих режимах. Если вы решили запустить приложение

AXIS Perimeter Defender

только в режиме на основе технологии искусственного интеллекта, то процесс монтажа камеры станет более гибким, и вам не придется выполнять калибровку камер.

AXIS Perimeter Defender включает в себя интерфейс рабочего стола (B), откуда вы устанавливаете и настраиваете приложение на камерах (A). Затем можно настроить систему для отправки сигналов тревоги в программное обеспечение для управления видео (C).

AXIS Perimeter Defender PTZ Autotracking — это плагин для приложения AXIS Perimeter Defender, использующий тот же интерфейс рабочего стола. Используя плагин, можно сопрягать фиксированную камеру оптического диапазона или тепловизионную камеру с PTZ-камерой Axis Q-line. После этого можно выполнять непрерывное обнаружение сцены с помощью фиксированной камеры, в то время как PTZ-камера будет выполнять автоматическое отслеживание с приближением обнаруженных объектов.

Важно!

Для AXIS Perimeter Defender PTZ Autotracking требуется выполнять калибровку как фиксированных, так и PTZ-камер.

AXIS Perimeter Defender предлагает следующие типы сценариев обнаружения:

- **Вторжение**: запускает сигнал тревоги, когда человек или транспортное средство входит в определенную зону на земле (с любого направления и с любой траекторией).
- **Бесцельное блуждание:** запускает сигнал тревоги, когда человек или транспортное средство остается в определенной на земле зоне дольше заранее заданного времени в секундах.
- **Пересечение зоны**: запускает сигнал тревоги, когда человек или транспортное средство проходит через две и более зоны, определенных на земле, в указанной последовательности.
- **Выполнение заданных условий**: запускает сигнал тревоги, когда человек или транспортное средство входит в зону, определенную на земле, без предварительного прохождения через другую зону или зоны, определенные на земле.

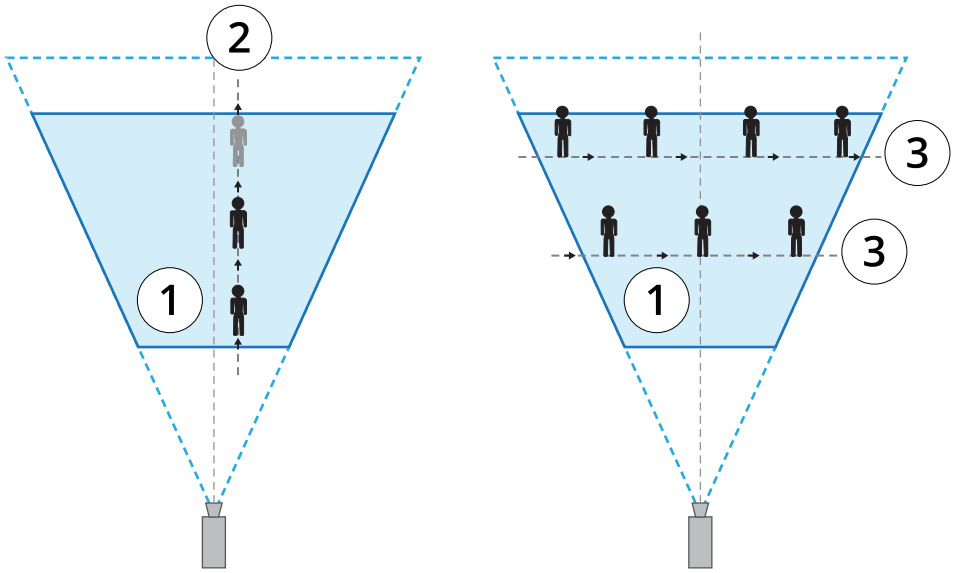
Как это работает?

Обнаружение объектов

AXIS Perimeter Defender может обнаруживать движущихся людей или транспортные средства. Для обнаружения:

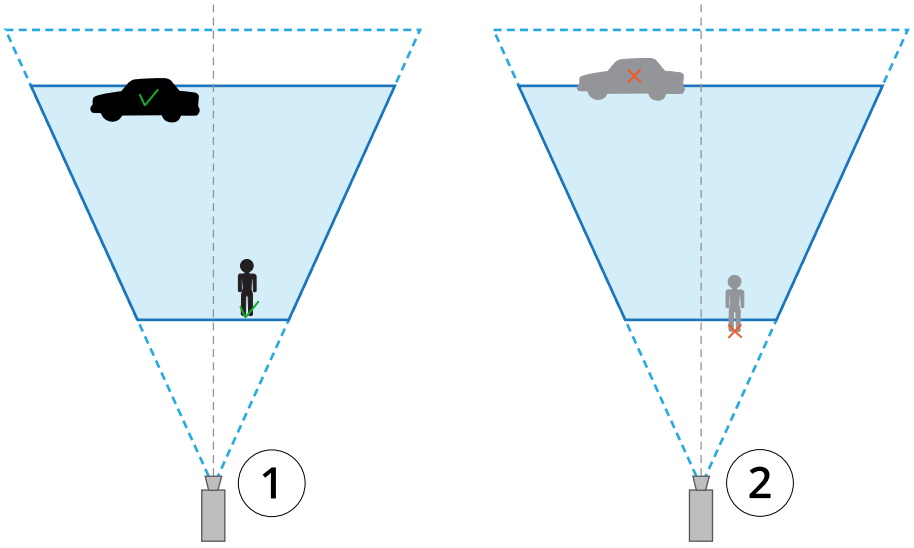
- человек или транспортное средство должны быть полностью видны в зоне обнаружения, по крайней мере в течение трех секунд.
- длина транспортного средства не должна превышать 12 метров. (В режиме на основе технологии искусственного интеллекта максимальная длина не предусмотрена.)
- движение людей или транспортных средств должны быть заметным из той точки, в которой установлена камера. Это означает, что вероятность обнаружения человека, движущегося в направлении камеры или от камеры по прямой линии, ниже, чем в случае, когда человек движется перпендикулярно полю обзора камеры.

AXIS Perimeter Defender



1 *Зона обнаружения*
2 *Человек уходит от камеры*
3 *Люди перемещаются перпендикулярно полю зрения камеры*

- точка обнаружения должна находиться внутри зоны обнаружения. Точка обнаружения человека находится у его ног, а у транспортного средства — по центру.



1 *Точка обнаружения внутри зоны обнаружения*
2 *Точка обнаружения за пределами зоны обнаружения*

После обнаружения AXIS Perimeter Defender продолжает отслеживать человека или транспортное средство, даже если они частично скрыты, например, когда тело человека скрыто за автомобилем, и видна только его голова.

Если обнаруженный человек или транспортное средство замирает на несколько секунд, AXIS Perimeter Defender прекращает его отслеживание. Если они начинают двигаться снова менее чем через 15 секунд, приложение продолжит отслеживание. Если человек находился на пересечении зон, то правильное срабатывание сценария не гарантируется.

AXIS Perimeter Defender

Как работает модуль PTZ Autotracking?

В AXIS Perimeter Defender PTZ Autotracking фиксированная камера работает совместно с PTZ-камерой. Когда фиксированная камера обнаруживает движущихся людей или транспортные средства, она отправляет данные о местоположении объектов на сопряженную с ней PTZ-камеру. Благодаря этому, PTZ-камера может автоматически:

- отслеживать объекты, и
- настраивать уровень зума, чтобы оставлять все объекты в поле зрения

до тех пор, пока объекты находятся в поле зрения фиксированной камеры.

Условия, при которых обнаружение может происходить с опозданием или не происходить вообще

- Туман
- Прямой свет, направленный на камеру
- Недостаточное освещение
- Излишнее количество шумов на изображении

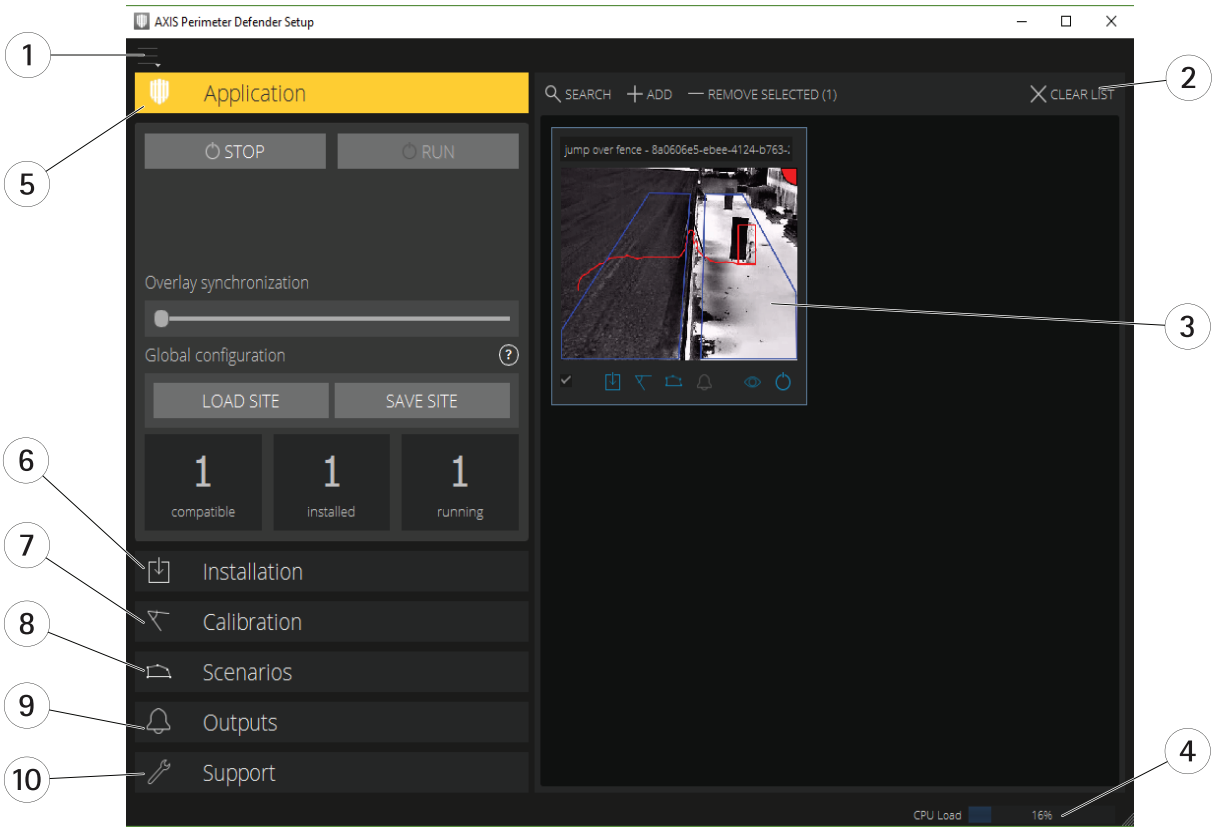
Потенциальные ситуации ложного срабатывания

- Частично скрытые люди или транспортные средства. Например, небольшой фургон, который появляется из-за стены, может выглядеть как человек, поскольку его видимая часть высокая и узкая.
- Насекомые на объективе камеры. Обратите внимание, что круглосуточные камеры с инфракрасной подсветкой привлекают насекомых и пауков.
- Свет автомобильных фар в сочетании с сильным дождем.
- Животные, размер которых близок к размеру человека, особенно если на вкладке **Scenarios (Сценарии)** были выбраны дополнительные типы приближения «ползком (или низко пригнувшись к земле)» или «перекатывание».
- Сильный свет, вызывающий тени.

Интерфейс пользователя

Интерфейс AXIS Perimeter Defender позволяет, например, калибровать устройства, настраивать сценарии и выполнять действия для нескольких устройств. Удаленная настройка позволяет конфигурировать систему из любого места, где есть возможность сетевого подключения.

AXIS Perimeter Defender



1 *Параметры интерфейса на стр. 7*
2 *Управление устройствами. См. Добавление устройств на стр. 18.*
3 *Живой просмотр на стр. 8*
4 *Индикатор нагрузки процессора. См. Нагрузка на процессор на стр. 12.*
5 *Вкладка Application (Приложение) на стр. 9*
6 *Вкладка Installation (Установка) на стр. 10*
7 *Вкладка Calibration (Калибровка) на стр. 10*
8 *Вкладка Scenarios (Сценарии) на стр. 10*
9 *Вкладка Output (Выход) на стр. 11*
10 *Вкладка Support (Поддержка) на стр. 12*

Параметры интерфейса

Меню параметров интерфейса содержит:

Настройки папки –
Путь к файлу конфигурации устройства: Выберите место для хранения временных файлов и калибровочного видео.
Путь к файлу конфигурации объекта: Выберите, где хранить файлы конфигурации из путей загрузки.

Пароли для камер – Просмотр используемых паролей и добавление нового пароля. Пароли не сохраняются после выхода пользователя из приложения.

Управление пакетами демороликов – Импорт или удаление демороликов.

Активировать режим с полной частотой кадров – Изменение частоты кадров при живом просмотре. См. *Нагрузка на процессор на стр. 12.*

Отображать футы и дюймы – Переключение между метрическими единицами измерения и единицами британской системы.

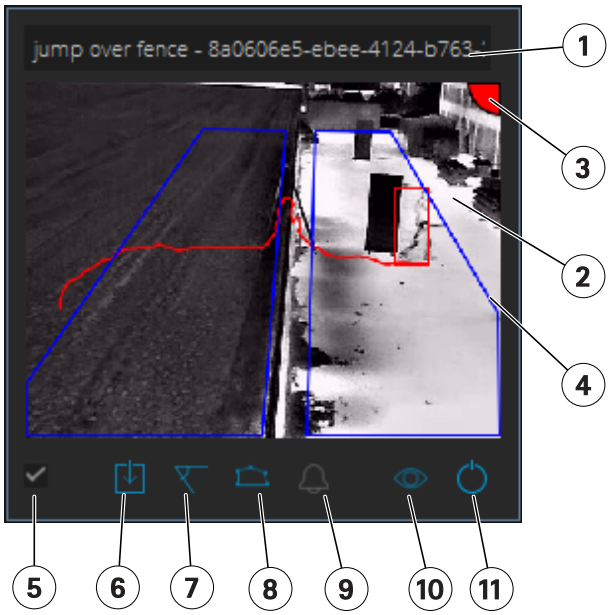
Изменить язык – Изменение языка приложения.

AXIS Perimeter Defender

О программе – Отображение номера версии AXIS Perimeter Defender Setup.

Живой просмотр

Каждое подключенное устройство поддерживает живой просмотр через главный интерфейс. Живой просмотр позволяет отслеживать состояние устройства и открывает быстрый доступ к основным функциям.



1. Название устройства – Нажмите для изменения имени устройства. Имя устройства всегда включает в себя IP и MAC-адрес устройства. Наведите курсор на имя устройства, чтобы увидеть используемое для анализа соотношение сторон, обеспечивающее максимальный угол обзора, а также наличие активного удаленного подключения.

2. Живое изображение – В режиме обзора используется частота кадров 1 кадр/с. Дважды щелкните мышью, чтобы максимально увеличить размер изображения и увеличить частоту кадров до 8 кадр/с.

3. Состояние сигнализации – Состояние сигнализации отображается только при активном наложении и при наличии установленного, настроенного и работающего приложения AXIS Perimeter Defender. Серый цвет означает, что функция сигнализации не активна или что выполняется загрузка настроек конфигурации. Зеленый цвет означает, что функция сигнализации активна. Красный цвет указывает на срабатывание сигнализации.

4. Зоны обнаружения – Зоны обнаружения отображаются только при активном наложении и при наличии установленного, настроенного и работающего приложения AXIS Perimeter Defender.

5. Флажок выбора – Используйте этот флажок для выбора нескольких устройств.

6. Состояние установки и кнопка быстрого доступа – Наведите курсор для просмотра версии AXIS Perimeter Defender, установленной на устройстве. Если вместо значка отображается , это указывает на наличие более новой версии. Нажмите, чтобы открыть вкладку Installation (Установка) для устройства. Серый цвет означает, что устройство не установлено. Оранжевый цвет означает, что устройство установлено, но не имеет действительной лицензии. Синий цвет означает, что устройство установлено и имеется действительная лицензия.

7. Состояние калибровки и кнопка быстрого доступа – Нажмите, чтобы открыть вкладку Calibration (Калибровка) для устройства. Серый цвет означает, что устройство не откалибровано. Синий цвет означает, что устройство откалибровано.

8. Статус сценариев и кнопка быстрого доступа – Нажмите, чтобы открыть вкладку Scenarios (Сценарии) для устройства. Серый цвет означает, что сценарий не определен. Синий цвет означает, что определен по крайней мере один сценарий.

AXIS Perimeter Defender

9. Состояние выходов и кнопка быстрого доступа – Нажмите, чтобы открыть вкладку Output (Выход) для устройства. Серый цвет означает, что выходы не настроены. Синий цвет означает, что настроен по крайней мере один выход.

10. Кнопка переключения статуса наложения – Нажмите для включения и отключения наложения. Серый цвет означает, что наложение неактивно. Синий цвет означает, что наложение активно. Наложение отображается в виде прямоугольника вокруг обнаруженных объектов, а также следа, повторяющего траекторию объектов.

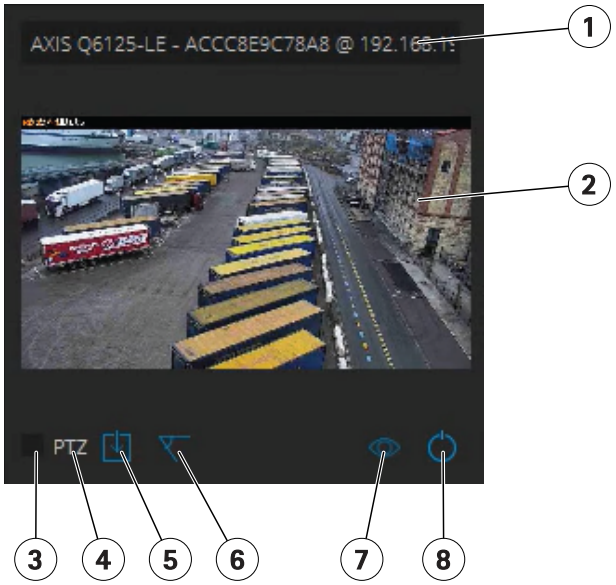
11. Кнопка переключения статуса работы – Нажмите, чтобы запустить/остановить приложение на устройстве. Серый цвет означает, что приложение остановлено. Синий цвет означает, что приложение работает.

Примечание.

Наложение доступно только в том случае, если доступно прямое подключение с устройства к компьютеру пользователя, то есть если брандмауэр или другая система не препятствуют подключению к порту наложения устройства.

Живой просмотр — PTZ Autotracking

Живой просмотр для устройств, на которых установлен плагин AXIS Perimeter Defender PTZ Autotracking, немного отличается от обычного живого просмотра.



1 *Название устройства*
2 *Живое изображение*
3 *Флажок выбора*
4 *Указывает, что устройство использует AXIS Perimeter Defender PTZ Autotracking*
5 *Состояние установки и кнопка быстрого доступа*
6 *Состояние калибровки и кнопка быстрого доступа*
7 *Кнопка переключения статуса наложения*
8 *Кнопка переключения статуса работы*

Вкладка Application (Приложение)

- **Run (Выполнить)** — запуск интеллектуальных приложений видеоаналитики на выбранных устройствах.
- **Stop (Остановить)** — остановка выполнения интеллектуальных приложений видеоаналитики на выбранных устройствах.
- **Load Site (Загрузить объект)** — загрузка сохраненного ранее объекта, т.е. устройств и их файлов конфигурации

AXIS Perimeter Defender

- **Save Site (Сохранить объект)** — сохранение текущего объекта, т.е. сохранение информации о всех устройствах и соответствующих файлов конфигурации
- **Overlay synchronization (Синхронизации наложения)** — управление синхронизацией наложения метаданных AXIS Perimeter Defender. Этот слайдер управляет задержкой между наложением метаданных и получением изображений, чтобы компенсировать более низкую скорость передачи потокового изображения по сравнению с метаданными. Значение слайдера указывает на задержку, установленную для текущей выбранной камеры. Если подключено более одной камеры, указанное значение является значением первой выбранной камеры. Изменение значения ползунка изменяет задержку для всех выбранных камер.

Кроме этого, вы можете видеть количество добавленных совместимых устройств, общее количество устройств, на которых установлено приложение AXIS Perimeter Defender, и количество устройств, на которых выполняются приложения видеоаналитики.

Вкладка Installation (Установка)

- **Application (Приложение): Install (Установить)** — Install the application on the selected device(s) (Установить приложение на выбранных устройствах).
- **Application (Приложение): Uninstall (Удалить)** — Uninstall the application on the selected device(s) (Удалить приложение с выбранных устройств).
- **Licence (Лицензия): Install (Установить)** — Install licence on the selected device(s) (Установить лицензию на выбранных устройствах).

Вкладка Calibration (Калибровка)

- **Automatic (Автоматическая)** — проведение автоматической калибровки выбранных устройств.
- **Manual (Ручная)** — проведение ручной калибровки выбранных устройств.

Вкладка Scenarios (Сценарии)

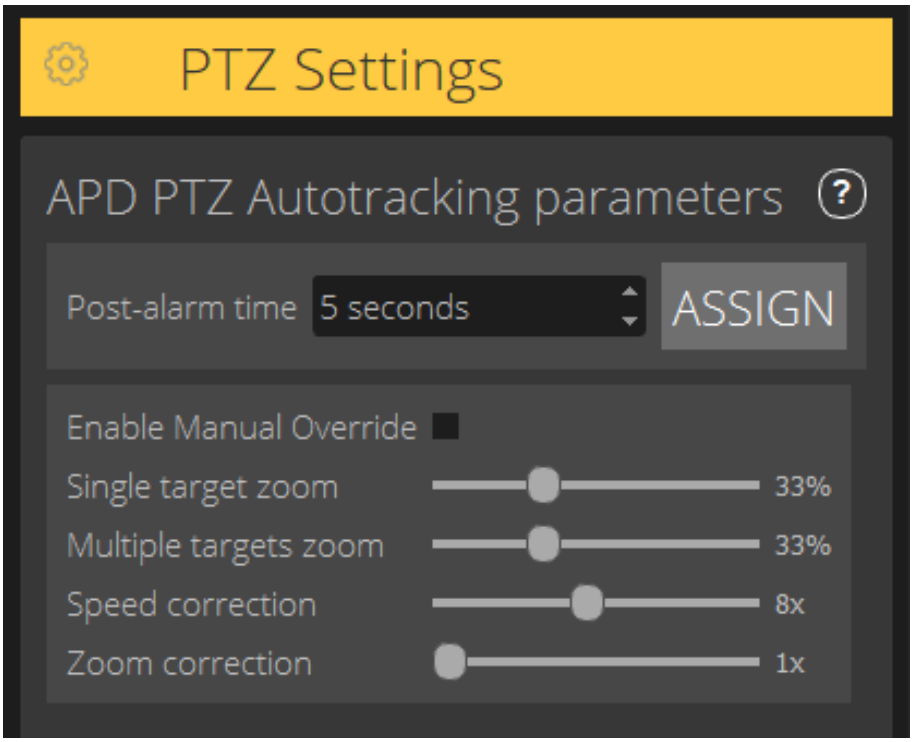
- **Global parameters (Глобальные параметры)** — применяются ко всем сценариям.
- **Advanced scenarios (Расширенные сценарии)** — создание сценариев обнаружения вторжения, бесцельного блуждания, пересечения зоны и условного сценария.

Вкладка PTZ settings (Параметры PTZ)

Примечание.

Эта вкладка отображается только при наличии плагина AXIS Perimeter Defender PTZ Autotracking.

AXIS Perimeter Defender



- **Post-alarm time (Время после начала сигнала тревоги)** — задайте время, предшествующее возврату камеры в начальное положение после выхода отслеживаемого объекта из поля зрения.
- **Enable manual override (Включить приоритет ручного режима)** — при проверке оператор сможет управлять PTZ-камерой с помощью джойстика, в ПО для управления видео или на веб-странице камеры.
- **Single target zoom (Зумирование одиночного объекта)** — настройте уровень зумирования для отслеживания одиночного объекта. Более высокое значение дает больше возможностей для идентификации, но также увеличивает риск потери быстро движущихся объектов.
- **Multiple targets zoom (Зумирование нескольких объектов)** — отрегулируйте зумирование для отслеживания нескольких объектов.
- **Speed correction (Коррекция скорости** — настройте скорость отслеживания, чтобы удерживать быстро движущиеся объекты по центру изображения PTZ-камеры. Обратите внимание, что высокое значение может привести к нестабильному отслеживанию.
- **Zoom correction (Коррекция зумирования)** — более высокое значение увеличивает масштабирование для объектов, которые находятся близко к краю поля зрения PTZ-камеры.

Вкладка Output (Выход)

- **Configure (Настройка)** — открытие веб-страницы устройства для создания и настройки сигналов тревоги.
- **Test alarm (Тестовый сигнал тревоги)** — тестирование сигнала тревоги, настроенного для устройства.
- **Post-alarm time: Assign (Время после начала сигнала тревоги: назначить)** — установить время после начала сигнала тревоги.

Вкладка Support (Поддержка)

- **Load (Загрузка)** — загрузка резервной конфигурации для выбранных устройств. Эта функция особенно полезна для быстрого восстановления после сбоя устройства или после случайной деинсталляции. Конфигурация включает в себя следующие элементы:
  - Лицензия
  - Параметры
  - Калибровка и сценарии
  - Калибровочный видеоролик
- **Save (Сохранить)** — создание резервной копии конфигурации выбранных устройств.
- **Clear (Очистить)** — удаление результатов калибровки и сценариев с выбранных устройств. Эта функция будет полезной после перемещения камер, в этом случае зоны калибровки и обнаружения изменятся.
- **View application log (Просмотр журнала приложения)** — просмотр внутреннего журнала AXIS Perimeter Defender.
- **Export support log (Экспорт журнала поддержки)** — создание файла поддержки с подробной информацией. Обязательно прилагайте этот файл к запросу на поддержку.

Нагрузка на процессор

Индикатор загрузки процессора указывает текущую нагрузку на процессор компьютера в режиме реального времени. Слишком высокая нагрузка на процессор может привести к тому, что компьютер или приложение не будут отвечать на запросы. Убедитесь в том, что при использовании AXIS Perimeter Defender Setup другие приложения закрыты, это позволит наиболее эффективно использовать ресурсы процессора. Если нагрузка на процессор слишком высокая и вы пытаетесь добавить устройство, то система выдает предупреждение.

Добавленные устройства используют ресурсы компьютерного процессора для декодирования видеопотоков с камеры и их отображения. Чтобы ограничить воздействие на компьютер, видео потоки от добавленных устройств по умолчанию отображаются со сниженной частотой кадров (примерно 1 кадр/с). Нормальная частота кадров (приблизительно 8 кадр/с) восстанавливается при развертывании видеопотоков или в процессе калибровки.

Важно!

Включение режима с полной частотой кадров может привести к зависанию интерфейса при подключении к большому количеству камер или при использовании недостаточно мощного компьютера.

Отображение демонстрационного ролика AXIS Perimeter Defender

Для демонстрационных целей AXIS Perimeter Defender и AXIS Perimeter Defender PTZ Autotracking поставляется с предварительно загруженными демонстрационными роликами, которые можно использовать для демонстрации аналитики без подключенных активных камер. Демонстрационные ролики показывают виды обнаружения и автоматического отслеживания результатов, которые можно ожидать в различных средах применения.

1. Выберите **Application (Приложение) > Add (Добавить) > Demo Clips (Демонстрационные ролики)** и выполните одно или несколько из указанных ниже действий:
   - Отфильтруйте демонстрационные ролики по их типу.
   - Выберите хотя бы один демонстрационный ролик.
2. Для добавления демонстрационных роликов нажмите **Add Selected Demo Clips (Добавить выбранные демонстрационные ролики)**.

После добавления демонстрационные ролики отображаются в виде стандартных видеопотоков в интерфейсе. В этом случае пользователь сразу видит результаты работы аналитики и автоматического отслеживания на отображаемом видео. Аналитику и автоматическое отслеживание можно останавливать и запускать по нажатию рабочего статуса в режиме живого просмотра либо кнопок **Run (Запуск)** или **Stop (Остановка)** на левой панели.

AXIS Perimeter Defender

Калибровку и сопряжение можно менять и выполнять повторно. Аналогичным образом, можно добавлять, удалять или изменять сценарии обнаружения.

На вкладке **Support (Поддержка)** на левой панели предусмотрена кнопка **Clear (Очистить)**, которая позволяет вернуть калибровку и сценарии к исходным значениям. Полностью удалить калибровку невозможно.

Начало работы

Процесс установки AXIS Perimeter Defender и AXIS Perimeter Defender PTZ Autotracking имеет незначительные отличия.

Начало работы с AXIS Perimeter Defender

Для запуска AXIS Perimeter Defender на объекте вам необходимо будет выполнить следующие шаги:

1. Установка камеры. См. *Установка камеры на стр. 14*.
2. Загрузка и установка приложения на компьютере. См. *Установка программного обеспечения на компьютере на стр. 18*.
3. Подключение к устройствам. См. *Добавление устройств на стр. 18*.
4. Установка AXIS Perimeter Defender на каждом устройстве. См. *Установка программного обеспечения на устройствах на стр. 20*.

Примечание.

Устройства, работающие только в режиме на основе технологии искусственного интеллекта, калибровать не требуется. Чтобы устройства работали в режиме калибровки и в режиме на основе технологии искусственного интеллекта одновременно, необходимо откалибровать их.

5. Калибровка устройств. См. *Калибровка — AXIS Perimeter Defender на стр. 20*.
6. Определите правила срабатывания сигналов тревоги путем добавления сценариев. См. *Определение сценариев на стр. 28*.
7. Настройка отправляемых сигналов тревоги. См. *Настройка выходов на стр. 33*.

Начало работы с AXIS Perimeter Defender PTZ Autotracking

Для запуска AXIS Perimeter Defender PTZ Autotracking на объекте вам необходимо будет выполнить следующие шаги:

1. Установка камер. См. *Установка камеры на стр. 14* и *Установка PTZ-камеры на стр. 17*.
2. Загрузка и установка приложения на компьютере. См. *Установка программного обеспечения на компьютере на стр. 18*.
3. Подключение к устройствам. См. *Добавление устройств на стр. 18*.
4. Установка AXIS Perimeter Defender версии 2.5.0 или более поздней версии на фиксированную камеру, и AXIS Perimeter Defender PTZ Autotracking на PTZ-камеру. См. *Установка программного обеспечения на устройствах на стр. 20*.
5. Калибровка устройств и настройка сценариев. См. *Калибровка — PTZ Autotracking на стр. 27*.
6. Сопряжение устройств. См. *Сопряжение камер — PTZ Autotracking на стр. 31*.
7. Настройка отправляемых сигналов тревоги. См. *Настройка выходов на стр. 33*.

Установка камеры

Сведения о средстве разработки

Для правильного размещения камеры на объекте рекомендуется использовать средство разработки для AXIS Perimeter Defender. Этот инструмент учитывает требования, выдвигаемые камерами и системой AXIS Perimeter Defender. Это средство поможет вам правильно выбрать:

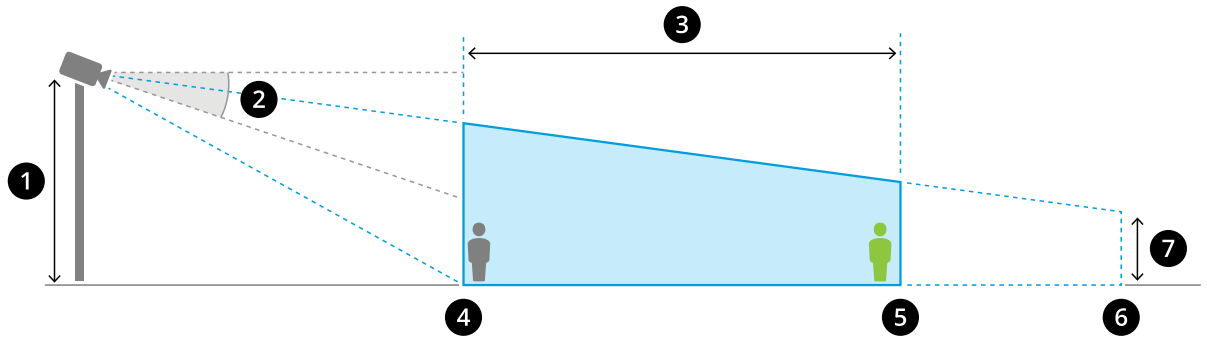
- Высоту установки камеры
- Угол поворота по вертикали
- Минимальное расстояние обнаружения
- Максимальное расстояние обнаружения

Для загрузки инструмента воспользуйтесь ссылкой *axis.com/products/axis-perimeter-defender*

Рекомендации по установке камеры

Примечание.

Для камер, которые работают только в режиме на основе технологии искусственного интеллекта, рекомендации по монтажу см. в приложении.



Правильно установленная камера.

1 *Высота монтажа*
2 *Наклон*
3 *Зона обнаружения*
4 *Минимальное расстояние обнаружения*
5 *Максимальное расстояние обнаружения*
6 *Расстояние области обзора*
7 *Высота области обзора*

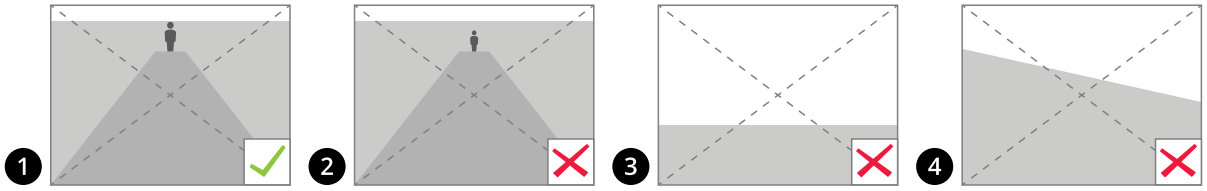
Высота объекта на максимальном расстоянии обнаружения – Для обнаружения стоящего человека на максимальном расстоянии обнаружения высота в пикселях должна составлять не менее 5 % от общей высоты изображения (3,5 % для тепловизионных камер). Например, если высота показываемого изображения составляет 576 пикселей, то высота человека, стоящего в конце зоны обнаружения, должна быть не менее 28 пикселей (20 пикселей для тепловизионной камеры).

Высота объекта на минимальном расстоянии обнаружения – Для обнаружения неподвижно стоящего человека на минимальном расстоянии обнаружения высота пикселя не должна превышать 60 % от общей высоты изображения.

Высота объекта при работе в режиме на основе технологии искусственного интеллекта – При запуске приложения в режиме на основе технологии искусственного интеллекта объекты должны быть того же размера, что и размер аватара, который требуется обнаружить.

Угол поворота по вертикали – Камера должна быть достаточно наклонена вниз, чтобы центр изображения находился ниже линии горизонта. Установите камеру таким образом, чтобы минимальное расстояние обнаружения было больше, чем половина высоты установки камеры (минимальное расстояние обнаружения > высота установки камеры / 2).

Угол вращения – Угол вращения камеры должен быть близким к нулю.



1 *Высота объекта, угол наклона и угол вращения выбраны правильно.*
2 *Высота объекта на максимальном расстоянии обнаружения составляет менее 5 % от высоты изображения (3,5 % для тепловизионных камер).*
3 *Центр изображения находится над линией горизонта.*
4 *Угол вращения камеры существенно отличается от нулевого.*

Максимальное расстояние обнаружения зависит от следующих факторов:

- Тип и модель камеры
- Объектив камеры. С увеличением фокусного расстояния увеличивается расстояние обнаружения.
- Минимальный размер пикселя, занимаемого человеком на изображении, для успешного обнаружения. Высота в пикселях для обнаружения стоящего человека должна составлять не менее 5 % от высоты изображения для камер оптического диапазона и не менее 3,5 % для тепловизионных камер.
- Погода
- Освещение
- Нагрузка от камеры

При установке камеры необходимо учесть следующие факторы:

- вибрации. Приложение допускает небольшие вибрации камеры, однако максимальная производительность достигается при полном отсутствии вибраций камеры.
- угол обзора. Угол обзора камеры должен быть фиксированным.

Требования к сцене

Примечание.

Для камер, которые работают только в режиме на основе технологии искусственного интеллекта, требования к сцене см. в приложении.

Зона обнаружения должна отвечать следующим условиям:

- Хорошая видимость
- Земля должна быть ровной или с небольшим наклоном
- При движении не происходит автоматическое включение освещения
- Хорошая видимость
- Для камер оптического диапазона уровень освещения и настройки изображения должны обеспечивать достаточный контраст между людьми/транспортными средствами и фоном.
    - При использовании камер Axis для круглосуточной работы с искусственным освещением рекомендуется обеспечить уровень освещенности не менее 50 люкс во всей зоне обнаружения.

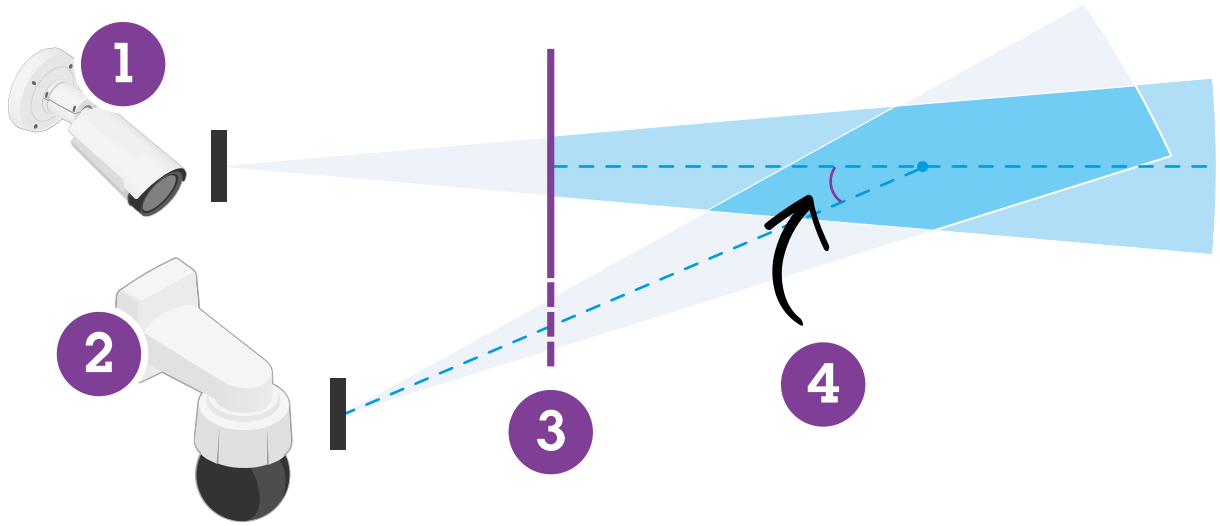
- При использовании внешних ИК-осветителей рекомендованное максимальное расстояние обнаружения составляет 80 м, при этом дальность ИК-осветителей должна быть в два и более раза выше, чем максимальное расстояние обнаружения.
- При использовании встроенного ИК-освещения максимальное расстояние обнаружения ограничено 20 м в зависимости от камеры и окружающих условий.

- При использовании тепловизионных камер необходимо обеспечить высокий контраст между фоном и передним планом

Для оптимальной производительности обнаружения AXIS Perimeter Defender автоматически распознает разницу между светлым и темным временем суток и использует эту информацию для точной настройки алгоритмов обнаружения. Точная настройка занимает около 24 часов, т.е. оптимальное обнаружение в круглосуточном режиме достигается через сутки.

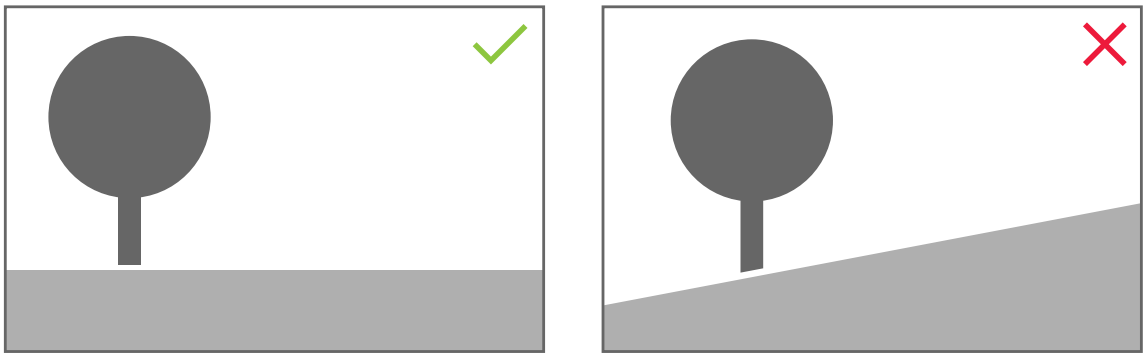
Установка PTZ-камеры

В этой главе описывается процедура установки PTZ-камеры по отношению к фиксированной камере. Указания по монтажу фиксированной камеры см. в разделе *Установка камеры на стр. 14*.



1 *Фиксированная сетевая камера*
2 *Сетевая PTZ-камера*
3 *Минимальное расстояние обнаружения*
4 *Угол между камерами*

- В заданном начальном положении PTZ-камера должна охватывать более 60% зоны обнаружения фиксированной камеры.
- Для отслеживания PTZ -камерой стоящий человек должен занимать более 4% от высоты изображения PTZ-камеры.
- PTZ-камера должна быть размещена до минимального расстояния обнаружения фиксированной камеры (C).
- Угол между фиксированной камерой и PTZ-камерой должен быть меньше 30° (D).



- Земля должна быть ровной.

Установка программного обеспечения на компьютере

1. Скачайте приложение AXIS Perimeter Defender по ссылке *axis.com/products/axis-perimeter-defender*
2. Установите программное обеспечение на компьютер.

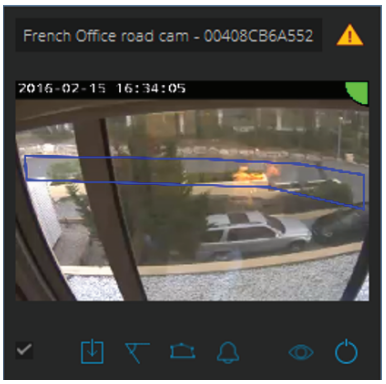
Добавление устройств

Добавлять устройства в приложение AXIS Perimeter Defender можно тремя разными способами:

- Автоматически путем сканирования сети. См. *Автоматическое добавление устройств на стр. 19*.
- Вручную, указывая настройки соединения. См. *Добавить устройства вручную на стр. 19*.
- Автоматически путем загрузки ранее сохраненного объекта. См. *Загрузить существующий объект на стр. 19*.

При добавлении устройства вы видите список всех других приложений, установленных на устройстве. Рекомендуется остановить работу любых несущественных приложений, поскольку они используют ресурсы процессора камеры, что влияет на производительность AXIS Perimeter Defender и может помешать правильной установке.

Если у устройства недостаточно ресурсов процессора, например, из-за работы других приложений, AXIS Perimeter Defender уменьшает частоту кадров. Если частота кадров ниже 5 кадров в секунду, рядом с именем устройства в режиме живого просмотра отображается желтый предупреждающий треугольник. При наведении курсора на треугольник отображается текущая частота кадров.



Примечание.

Частота кадров ниже 5 кадр/с может значительно снизить производительность видеоаналитики. Это может привести как к пропуску событий, так и к ложным обнаружениям.

Для получения более подробных сведений см. *Нагрузка на процессор на стр. 12*.

Автоматическое добавление устройств

Важно!

Функция поиска не работает по сети, то есть AXIS Perimeter Defender Setup может находить только устройства, подключенные к той же подсети, что и клиент, на котором установлено приложение. Добавление устройств, подключенных к другой подсети, необходимо выполнять вручную. Функция поиска также может не работать, если сетевые маршрутизаторы или коммутаторы настроены для фильтрации многоадресной передачи.

1. Для сканирования устройств в окружающей сети выберите **Application (Приложение)**, а затем нажмите **Search (Поиск)**.

   При первом поиске без настроенных паролей откроется диалог ввода паролей. В противном для подключения к устройствам будет использоваться заданный пароль.

2. Выберите устройства и нажмите **Add selected devices (Добавить выбранные устройства)**.

   Если пароль правильный, появляется статическое изображение с указаниями по выбору устройств для пользователя.

Добавить устройства вручную

1. Выберите **Application (Приложение)**, а затем нажмите **Add (Добавить)**.
2. Введите следующие данные:
   - IP-адрес или имя хоста устройства.
   - Пароль учетной записи root для устройства, поскольку для AXIS Perimeter Defender требуется root-доступ.
   - Порт HTTP, используемый для подключения. По умолчанию используется порт 80.
   - Дополнительное название устройства для удобного распознавания.
   - Если устройство располагается в удаленной сети, подключение к которой может быть медленным, отметьте пункт **Device on remote network (Устройство в удаленной сети)**. Если не установить такую отметку для медленных соединений, то калибровка может не выполняться или выполняться некорректно.

   Примечание.

   При удаленном подключении пользователь должен иметь возможность подключиться к устройству через HTTP. Убедитесь в том, что порт HTTP настроен правильно. В случае недостаточной или нестабильной пропускной способности возможны сбои при удаленном конфигурировании.

3. Нажмите **OK**.

Примечание.

Если не удается добавить камеру по имени хоста, проверьте настройки сети и DNS или добавьте устройство по IP-адресу.

Загрузить существующий объект

Для загрузки ранее сохраненной конфигурации:

1. Выберите **Application (Приложение)**, а затем щелкните **Load site (Загрузить объект)**.
2. Выберите файл конфигурации и щелкните **Открыть**. Автоматически откроется живой просмотр.

Установка программного обеспечения на устройствах

AXIS Perimeter Defender необходимо установить на каждом устройстве.

Для проверки версии AXIS Perimeter Defender, установленной на устройстве, наведите курсор на пункт **Installation status (Состояние установки)** в режиме живого просмотра.

Если приложение AXIS Perimeter Defender на устройстве не установлено, то все значки в режиме живого просмотра будут показаны серым цветом.

Установка программного обеспечения на устройство

1. Выберите **Installation (Установка)**.
2. Выберите устройства, на которых вы хотите установить приложение.
3. Выберите самую последнюю версию AXIS Perimeter Defender и нажмите **Install (Установить)**.

   Приложение AXIS Perimeter Defender будет установлено на выбранные устройства и автоматически запущено.
4. Выберите файл лицензии и выполните одно из следующих действий:
   - В случае установки на одном устройстве: выберите файл лицензии для устройства.
   - В случае установки на нескольких устройствах: выберите папку, в которой хранятся файлы лицензии.
5. Нажмите **Install (Установить)**.

Калибровка — AXIS Perimeter Defender

Калибровка

Примечание.

Устройства, работающие только в режиме на основе технологии искусственного интеллекта, калибровать не требуется. Чтобы устройства работали в режиме калибровки и в режиме на основе технологии искусственного интеллекта одновременно, необходимо откалибровать их.

Чтобы система AXIS Perimeter Defender могла правильно интерпретировать сцену, необходимо откалибровать все устройства. Во время калибровки вы указываете опорные точки, благодаря которым процессор может получать информацию о глубине и высоте. Вы также определяете наблюдаемую зону.

Калибровка состоит из двух задач:

1. Выполнение калибровки:
   - в автоматическом режиме — рекомендуется в большинстве случаев. См. *Выполнение автоматической калибровки на стр. 21*.
   - в ручном режиме — рекомендуется, если автоматическая калибровка камеры не удалась, а также для точной настройки, в случае нецелесообразности тестовых прохождений через зону, либо если в наблюдаемой зоне имеются объекты известной высоты. К примерам можно отнести удаленный периметр с линией забора, состоящей из ряда равномерно расположенных столбов одинаковой высоты. См. *Выполнение ручной калибровки на стр. 25*.
2. Проверка результатов калибровки. См. *Проверка качества калибровки на стр. 22*.

Чтобы ускорить процесс настройки крупных объектов, можно откалибровать несколько устройств одновременно. Калибровку можно выполнять автоматически или вручную, как и для одной камеры. Перед одновременной калибровкой нескольких устройств необходимо учесть следующие факторы:

- Максимальное количество устройств, которые можно установить и настроить одновременно, зависит от мощности процессора и размера памяти, доступной на вашем компьютере. Слишком большое количество устройств в

AXIS Perimeter Defender Setup может привести к сбоям. При появляются предупреждения о перегрузке процессора, устанавливайте и настраивайте отдельные наборы устройств, используя функцию сохранения объекта.

- Автоматическая калибровка нескольких устройств требует больше ресурсов процессора и оперативной памяти, чем калибровка одного устройства. На слабых системах это может привести к зависанию компьютера или к сбою приложения. В случае сбоя уже снятые видеоролики будут доступны для использования при калибровке единичных камер.

Примечание.

- AXIS Perimeter Defender поддерживает различные варианты соотношения сторон изображения в зависимости от максимального разрешения, обеспечиваемого камерой. В этой связи при изменении разрешения необходимо будет повторно выполнять все предыдущие калибровки. Однако, если изменить разрешение потока на веб-странице камеры, то повторная калибровка не потребуется.
- Рекомендуется использовать одинаковое соотношение сторон в AXIS Perimeter Defender и в ПО для управления видео для оптимизации изображения. Для получения подробной информации о соотношении сторон наведите курсор на название камеры в режиме живого просмотра.
- Если камера после калибровки сдвинется, для получения достоверных результатов аналитики потребуется повторная калибровка.

Выполнение автоматической калибровки

Используя автоматическую калибровку, вы можете откалибровать одну или несколько камер по мере того, как человек проходит через зону видеонаблюдения. Камера автоматически собирает информацию, необходимую для калибровки.

Что требуется для успешной автоматической калибровки:

- Не выполняйте калибровку, когда в поле наблюдения находится много людей.
- Не выполняйте калибровку, когда в поле наблюдения находится много проезжающих машин.
- Не выполняйте калибровку, когда в поле наблюдения присутствуют другие движущиеся предметы. Например, раскачивающиеся на ветру деревья или развевающиеся флаги.
- Не откалибруйте камеру, которая не была установлена параллельно земле.
- Человек, который проходит через зону наблюдения, должен пересекать ее на всей протяженности от нижнего до верхнего края. Если это невозможно, лучше выбрать ручную калибровку.
- Если камера находится в удаленной сети, и при этом не подключена как удаленная камера, человек, который проходит через зону наблюдения, должен двигаться в этой зоне на протяжении примерно 5 минут, чтобы система могла собрать нужное количество изображений. Это связано с тем, что частота кадров для устройств в удаленных сетях обычно ниже.

1. Выберите **Calibration (Калибровка)**.
2. Выберите устройства, которые вы хотите откалибровать.
3. Нажмите **Automatic (Автоматическая)**.
4. Установите время начала записи. Запись изображения должна как минимум за 10 секунд до того, как человек, который проходит через зону наблюдения, войдет в поле зрения камеры.
5. Установите продолжительность записи. Примите во внимание следующие факторы:
   - необходимо предусмотреть достаточно времени, чтобы человек мог пройти через всю зону наблюдения туда и обратно;
   - продолжительность видео влияет на калибровочные вычисления.
6. Введите рост (в см) человека, который, проходит через зону наблюдения, и нажмите **Capture (Съемка)**.

   Чтобы использовать уже снятый видеоролик, щелкните **Use previous capture (Использовать предыдущую съемку)**.

7. Попросите человека пройти через зону наблюдения, следуя указанным инструкциям:

   - Человек должен двигаться зигзагами, чтобы охватить как можно больше площади в зоне обнаружения, от начала до конца зоны. Рекомендуется двигаться по V-образной траектории через всю область наблюдения.
   - Человек должен практически всегда в полный рост оставаться в поле зрения камеры.
   - Необходимо идти медленно и прямыми отрезками.
   - Сохраняйте вертикальное положение тела.
   - Перед изменением направления делайте паузы на 1-2 секунды.

Пример схемы прохождения.

8. Убедитесь в правильности выполненной автоматической калибровки, проверив точность обнаружения человека. См. *Проверка качества калибровки на стр. 22*.
9. Для сохранения калибровки нажмите **Accept (Принять)**.

   Для выполнения новой калибровки нажмите **New (Новая)**.

   Для выполнения ручной калибровки нажмите **Manual (Ручная)**.

После подтверждения калибровки синие границы указывают максимальную зону обнаружения. Максимальная зона обнаружения — это самая большая область, в которой можно вести наблюдение. За пределами этой области также возможно обнаружение злоумышленников, но такое обнаружение не гарантируется.

Проверка качества калибровки

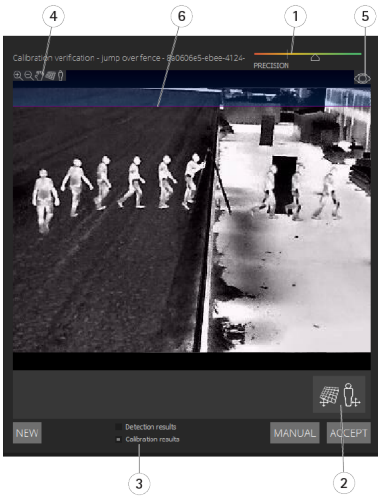
После калибровки вы должны видеть проходящего через зону наблюдения человека в нескольких разных местах. Если человек не виден вообще, автоматическая калибровка не удалась, и ее следует повторить.

Существует несколько способов проверить качество калибровки:

- По индикатору точности калибровки. Он отражает автоматически вычисленный уровень точности, который обозначает охват человека в зоне наблюдения и качество его обнаружения. Если индикатор точности находится в

красной зоне, то калибровка не удалась, и кнопка **Accept (Принять)** будет неактивной. См. *Выполнение ручной калибровки на стр. 25*.

- Можно использовать сетку. См. *Использование сетки для проверки калибровки на стр. 23*.
- Можно использовать аватар. См. *Использование аватара для проверки калибровки на стр. 24*.
- Вы можете проверить результаты обнаружения. См. *Использование результатов обнаружения для проверки калибровки на стр. 25*.



1 *Индикатор точности калибровки*
2 *Инструменты сетки и аватара*
3 *Динамическое или статическое представление*
4 *Инструменты управления представлением*
5 *Переключение между калибровочным изображением и живым просмотром*
6 *Линия горизонта*

Эта линия представляет видимую линию горизонта. При определении сценариев вы не можете располагать зоны наблюдения в синей области над линией горизонта, поскольку эти зоны располагаются над землей, а зоны наблюдения по определению должны находиться на земле.

Использование сетки для проверки калибровки

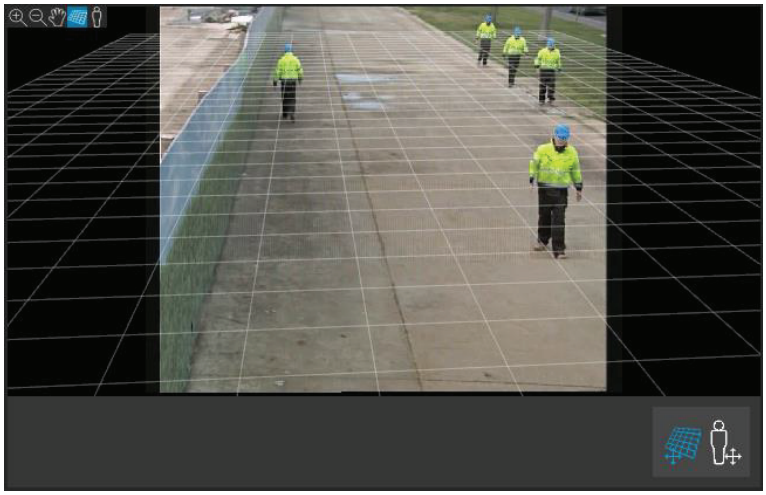
Сетка должна соответствовать квадратной сетке на земле. Вы можете включать и выключать отображение сетки с помощью значка управления сеткой.

Важно!

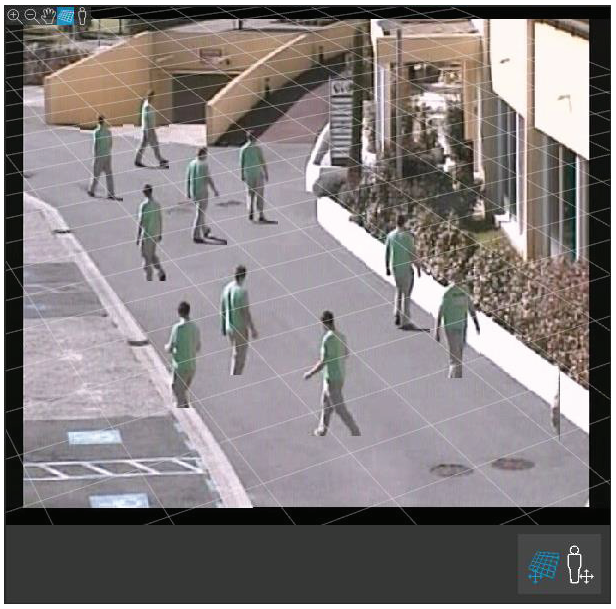
Сетка не влияет на калибровку, этот инструмент просто позволяет убедиться в правильности калибровки.

Сетку можно повернуть, перетащив ее мышью в области предварительного просмотра. Попробуйте совместить ее с какой-нибудь конструкцией на изображении, чтобы оценить корректность результата.

Если сетка параллельна земле, не имеет странного наклона, и если после вращения сетки она располагается параллельно искусственным объектам, которые параллельны в реальном мире, то калибровка выполнена правильно.



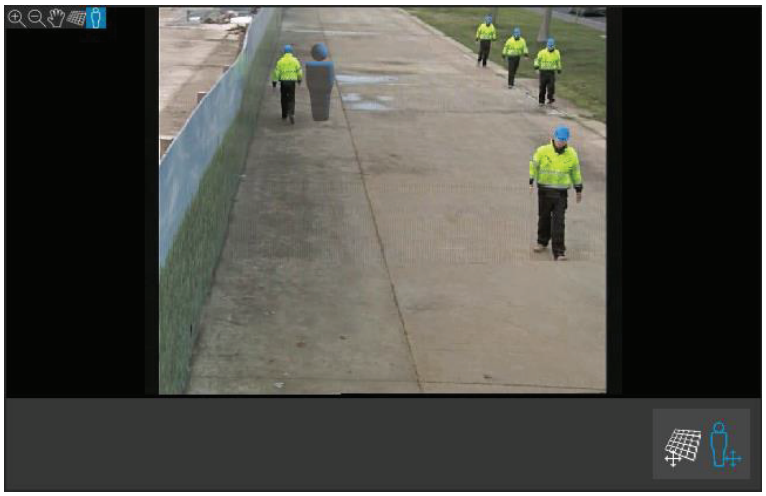
Пример правильного размещения сетки по обочинам дороги.



Пример неправильного размещения сетки по обочинам дороги.

Использование аватара для проверки калибровки

Эта функция позволяет разместить на изображении 3D-аватар человека среднего роста. Включать и выключать отображение аватара можно по нажатию значка управления аватаром.



Размер аватара на панели представления соответствует размеру среднего человека в этом положении в соответствии с текущей калибровкой. Перемещая аватар, вы можете убедиться, что его размер является достоверным по отношению к другим объектам или людям на изображении. Проверять аватар нужно в разных позициях, поскольку его размер может быть правильным в одной позиции и некорректным в другой.

Использование результатов обнаружения для проверки калибровки

Можно использовать результаты обнаружения для проверки работы AXIS Perimeter Defender с текущей калибровкой, если поток снятого живого видео содержит кадры, на которых запечатлен движущийся человек.

1. Переключитесь с **результатов калибровки** на **результаты обнаружения**.
2. Обратите внимание на обнаружение людей или транспортных средств, въезжающих в зону видеонаблюдения:
   - Если калибровка выполнена правильно, люди будут отмечены красными прямоугольниками, а транспортные средства — синими прямоугольниками.
   - Если люди или транспортные средства часто упускаются, то с большой долей вероятности автоматическая калибровка выполнена некорректно.
   - Красная зона показывает зону ограничения обнаружения в соответствии с калибровочными вычислениями, то есть зону, в которой требования к росту человека на изображении не соблюдаются. В этой зоне обнаружение может выполняться некорректно из-за отклонений в размерах отслеживаемой цели.

Примечание.

- Если калибровочные вычисления выполнены неправильно, то красная зона также будет указана некорректно.
- Если человек находится слишком далеко, то отметить его не удастся. Для правильной работы обнаружения должны быть соблюдены требования к минимальному размеру. Для получения более подробных сведений см. *Установка камеры на стр. 14*.
- Проверка результатов обнаружения на удаленно подключенных камерах может не работать из-за слишком низкой частоты кадров. Это не является признаком неправильной настройки. Вместо этого для проверки калибровки используйте аватар и сетку.

Выполнение ручной калибровки

Если вы еще не проводили автоматическую калибровку, то перед ручной калибровкой необходимо снять короткое видео и создать составное изображение. Выполните те же шаги, что и для автоматической калибровки (*Выполнение автоматической калибровки на стр. 21*), при этом выбирайте пункт **Manual (Ручная)** вместо пункта **Automatic (Автоматическая)** на вкладке **Calibration (Калибровка)**. Для создания составного изображения после съемки видео:

- перемещайте ползунок для выбора
- ключевых точек видеоролика; нажимайте значок камеры для добавления снимков в составное изображение

Составное изображение должно отражать весь диапазон сцены: спереди, сзади, слева и справа.

После ручного или автоматического создания составного изображения можно продолжить ручную калибровку.

Механизм калибровки проверяет следующие параметры:

- горизонт
- распределение или расхождение вертикальных линий на изображении
- масштаб сцены

При выполнении ручной калибровки необходимо ввести эту информацию в механизм калибровки, используя элементы управления калибровкой. Существует три типа элементов управления калибровкой:

- **Маркировочные линии**, обозначающие средний рост человека в разных точках сцены. Если вы уже проводили автоматическую калибровку, то с большой долей вероятности изображение, показанное на панели редактора, уже содержит несколько копий одного и того же человека. Установите маркировочные линии в соответствии с ростом и направлением людей, показанных в одной или нескольких точках сцены. Маркировочная линия должна начинаться от земли и в реальном мире должна быть вертикальной. Длина маркировочной линии в реальном мире должна соответствовать высоте, указанной рядом с кнопкой **Person (Человек)** на панели редактора. Маркировочные линии отмечены полупрозрачным голубым символом.

  Как лучше всего размещать маркировочную линию

  - Рекомендуется размещать маркировочную линию на человеке, ноги которого расположены близко друг к другу.
  - Если устанавливать линию на человеке, стоящем на земле с расставленными ногами, то нижняя точка должна располагаться на земле на одинаковом расстоянии между пятками.
  - Линия должна проходить вдоль туловища человека. Однако, если человек наклонен в любом направлении, обычно это будет наклон вперед во время ходьбы, попробуйте компенсировать такой наклон, разместив линию ближе к вертикали. Используйте любые ориентиры на изображении, например, деревья, заборы или фонарные столбы.
  - Для определения масштаба сцены необходимо указать как минимум одну маркировочную линию, обозначающую рост человека. Если на изображении нет людей, можно добавить маркировочную линию на любой другой вертикальный объект известной высоты, например, на стойку забора высотой 3 м, отметив рост человека на этом объекте.

- **Параллельные горизонтальные линии** (горизонтальные элементы) используются для обозначения известных горизонтальных и параллельных линий сцены. Эти линии могут располагаться на земле и/или на стене, при этом они обязательно должны быть параллельными. Необходимо добавить не менее двух горизонтальных элементов. Вы можете разместить их по бокам изображения, вдоль разметки на прямых участках дороги, вдоль прямых железнодорожных путей, вдоль видимых конструкций на стенах, либо вдоль верхних и нижних точек на заборных столбах. Горизонтальные линии отмечены голубым цветом.

- **Вертикальные линии** используются для обозначения известных вертикальных линий на изображении. Вертикальная линия должна обозначать некоторую вертикальную структуру в реальном мире. Это может быть, например, столб забора, угол здания или знак. Вертикальная линия не обязательно должна начинаться от земли. Вертикальные линии отмечены синим цветом. Обратите внимание, что вертикальные линии существенно влияют на чувствительность, так как даже небольшое изменение ориентации может кардинально повлиять на калибровку. Как правило, вертикальные линии должны иметь видимый уклон вправо на правой стороне изображения и уклон влево на левой стороне изображения.

1 *Маркировочные линии*
2 *Вертикальные линии*
3 *Параллельные горизонтальные линии*
4 *Инструменты сетки и аватара*

Количество элементов калибровки

Как правило, чем больше количество добавленных маркировочных линий, горизонтальных и вертикальных линий, тем лучше результаты калибровки. Механизм калибровки может откалибровать систему всего по нескольким линиям, но обычно с увеличением количества добавленных линий возрастает и качество калибровки. Маркировочные линии, обозначающие рост людей, рекомендуется размещать внизу, вверху, слева и справа на изображении.

Вертикальные структуры на изображении

В соответствии с *Рекомендации по установке камеры на стр. 15*, все камеры должны быть направлены с легким наклоном вниз. В результате все вертикальные в реальном мире структуры на изображении будут казаться расходящимися. Это означает, что все маркировочные линии, обозначающие рост человека, а также вертикальные линии должны наклоняться ближе к краю изображения. Линия в правой половине изображения должна иметь наклон вправо, а линия в левой половине — наклон влево. Для надлежащей калибровки как минимум одна из указанных маркировочных или вертикальных линий должна иметь правильный наклон.

Индикатор точности визуально показывает уровень и качество деталей, добавленных на изображении. Для успешной ручной калибровки линии должны быть добавлены в ближней, дальней, левой и правой части изображения. Это можно проследить по зеленому индикатору точности.

Качество калибровки

Качество калибровки можно проверить с помощью сетки или аватара. См. *Проверка качества калибровки на стр. 22*. Также можно воспользоваться кнопкой **Review (Проверка)**. Это позволит увидеть результат работы AXIS Perimeter Defender на снятом видеоролике с использованием текущей ручной калибровки.

Калибровка — PTZ Autotracking

Важно!

Для достижения хороших результатов требуется качественная калибровка камеры. Внимательно следуйте инструкциям.

Примечание.

Можно откалибровать обе камеры одновременно или по очереди.

1. Выберите фиксированную камеру и PTZ-камеру.
2. Выберите **Calibration (Калибровка)** и нажмите **Setup PTZ position (Настройка положения PTZ)**. Отображается всплывающее окно, содержащее изображение с фиксированной камеры.

   При запуске приложения PTZ-камера в течение некоторого времени будет выполнять панорамирование, наклон и зумирование.
3. Убедитесь, что изображения с двух камер совмещены друг с другом.

   Если это не так, щелкните по изображению в режиме живого просмотра и отрегулируйте вид с PTZ-камеры так, чтобы он соответствовал виду с фиксированной камеры. Убедитесь в том, что изображение не повернуто.
4. Нажмите **Setup PTZ position (Настройка положения PTZ)**.

   Если кнопка не видна, переместите всплывающее окно, содержащее изображение с фиксированной камеры.
5. Нажмите **Automatic (Автоматическая)**.
6. Выполните автоматическую калибровку в соответствии с инструкциями в разделе *Выполнение автоматической калибровки на стр. 21*.
7. Используйте аватар для проверки качества калибровки фиксированной камеры. См. *Использование аватара для проверки калибровки на стр. 24*.

   Если качество достаточно хорошее, нажмите **Accept (Принять)**.

   Если качество недостаточно хорошее, используйте видео из автоматической калибровки, для выполнения калибровки вручную. Нажмите **Manual (Ручная)** и следуйте инструкциям, указанным в разделе *Выполнение ручной калибровки на стр. 25*.
8. В разделе **Scenarios (Сценарии)** задайте правила для событий, инициирующих сигналы тревоги. См. *Определение сценариев на стр. 28*.
9. В разделе **Calibration (Калибровка)** нажмите **Review (Проверка)** в живом просмотре с PTZ-камеры.
10. Используйте аватар для проверки качества калибровки PTZ-камеры. См. *Использование аватара для проверки калибровки на стр. 24*.

    Если качество достаточно хорошее, нажмите **Accept (Принять)**.

    Если качество недостаточно хорошее, используйте видео из автоматической калибровки, для выполнения калибровки вручную. Нажмите **Manual (Ручная)** и следуйте инструкциям, указанным в разделе *Выполнение ручной калибровки на стр. 25*.
11. Выполните сопряжение камер. См. *Сопряжение камер — PTZ Autotracking на стр. 31*.

Определение сценариев

Сценарии

AXIS Perimeter Defender использует стандартные сценарии охраняемой территории, которые можно настроить для защиты и мониторинга нужных зон. На этапе калибровки для используемых по умолчанию сценариев обнаружения вторжения/бесцельного блуждания была задана максимальная зона обнаружения. На этом этапе можно настраивать более сложные сценарии обнаружения трех различных типов:

- обнаружение вторжения/бесцельного блуждания. См. *Настройка сценария обнаружения вторжения/бесцельного блуждания на стр. 29*

- пересечение зоны. См. *Настройка сценария пересечения зоны на стр. 30*.
- выполнение заданных условий. См. *Настройка условного сценария на стр. 30*

Если рядом с названием сценария отображается символ **!**, это означает, что настройка сценария не завершена. Чаще всего это означает, что зона обнаружения еще не определена.

Глобальные параметры

Глобальные параметры, установленные в пользовательском интерфейсе, применяются ко всем сценариям.

Тип камеры – Для камер оптического диапазона выберите **Color – Day-Night (Цветное изображение в режимах «день/ночь»)**. Для тепловизионных камер тип камеры будет установлен автоматически.

Примечание.

- Дополнительные типы передвижения могут увеличить риск ложных срабатываний, например, вызванных животными.
- Дополнительные типы передвижения не поддерживаются устройствами, которые работают только в режиме на основе технологии искусственного интеллекта.

Дополнительные типы передвижения – Выберите типы передвижения, которые вы хотите включить в сценарий обнаружения.

Расширенная компенсация – Для устройств, работающих в режиме на основе технологии искусственного интеллекта, установите флажок **AI (ИИ)**, чтобы включить его. Если в кадре присутствуют транспортные средства, фары или световые эффекты от фар, например отражения, можно использовать параметр **Headlights/vehicles in scene (Фары/транспортные средства в сцене)**. При использовании данного параметра в некоторых случаях могут ухудшаться рабочие характеристики в нормальных условиях. По умолчанию во всех сценариях предусмотрено присутствие транспортных средств и, следовательно, света их фар. Чтобы игнорировать капли дождя или насекомых и сократить число ложных тревог, можно использовать параметр **Insects/droplets on lens (Насекомые/капли на объективе)**.

Чувствительность – Чтобы увеличить чувствительность системы, переместите ползунок вправо. Более высокая чувствительность снижает риск пропуска вторжений, однако повышает вероятность ложных срабатываний.

Фильтрация объектов по целевому размеру – Для устройств, работающих в режиме на основе технологии искусственного интеллекта, можно фильтровать объекты, размер которых меньше целевого размера.

Параметры продолжительности

Для каждого создаваемого сценария можно установить параметры продолжительности.

Минимальное время присутствия в зоне – Установите время, в течение которого объект должен находиться в зоне для активации.

Узкая зона распознавания движения – В случае узкой зоны, которую можно пересечь за 1–2 секунды, существует риск пропуска сигналов тревоги. Снизить вероятность пропуска сигналов тревоги можно с помощью функции **Narrow zone (Узкая зона)**. Обратите внимание, что эту функцию нельзя сочетать с параметром **Min presence in zone (Минимальное время присутствия в зоне)**.

Настройка сценария обнаружения вторжения/бесцельного блуждания

Сценарий обнаружения вторжения/бесцельного блуждания для активации сигнала тревоги, когда объект входит в определенную зону и остается в этой зоне дольше определенного времени.

На этапе калибровки был создан сценарий обнаружения вторжения/бесцельного блуждания, этот сценарий использует максимальную зону обнаружения. Чтобы использовать имеющийся сценарий без изменений, нажмите кнопку **Accept (Принять)** на вкладке **Scenarios (Сценарии)**.

Чтобы изменить сценарий по умолчанию:

1. Выберите **Scenarios (Сценарии) > Advanced scenarios (Расширенные сценарии)**.
2. Измените зону обнаружения по умолчанию:

- Чтобы переместить существующие точки в зоне обнаружения, нажмите и перетащите их с помощью мыши.
- Чтобы создать дополнительные точки, нажмите на любой из существующих сегментов и перетащите с помощью мыши.

3. В разделе **Detect (Обнаружение)** выберите тип обнаруживаемых объектов.
4. В разделе **Duration parameters (Параметры длительности)**, если вы не хотите, чтобы объект вызвал сигнал тревоги, как только он войдет в зону, установите время бесцельного блуждания в пункте **Min presence in zone (Минимальное время присутствия в зоне).**
5. Если сигнал тревоги должен подаваться для узкой зоны, которую можно пересечь за 1–2 секунды, выберите **Narrow zone (Узкая зона)**. Этот параметр нельзя использовать в комбинации с параметром **Min presence in zone (Минимальное время присутствия в зоне)**. Для получения более подробных сведений см. *Параметры продолжительности на стр. 29*.
6. Чтобы загрузить изменения в камеру и вернуться к основному представлению нажмите **Accept (Принять)**.

Настройка сценария пересечения зоны

Сценарий пересечения зоны предназначен для запуска сигнала тревоги при прохождении объекта через две зоны обнаружения в заданной последовательности.

Важно!

Сценарий пересечения зоны имеет следующее ограничение: если объект, запускающий сценарий, замирает на нескольких секунд в начальной зоне перед переходом в конечную зону, то сценарий срабатывать не будет.

В разделе **Duration parameters (Параметры длительности)** можно задать минимальное время присутствия для каждой из зон в сценарии. Если T_A — это минимальное время в начальной зоне и T_B — в конечной зоне, то сигнал тревоги срабатывает только если объект остается дольше, чем T_A в начальной зоне, а затем дольше, чем T_B в конечной зоне.

1. Выберите **Scenarios (Сценарии) > Advanced scenarios (Расширенные сценарии)**.
2. Нажмите **New (Новый)** и выберите **Zone-crossing (Пересечение зоны)**.
3. Создайте две зоны обнаружения, отстоящие друг от друга на расстоянии не менее одного метра:
   - Чтобы создать зону обнаружения, щелкните изображение несколько раз.
   - Чтобы завершить зону, щелкните изображение правой кнопкой.
4. Чтобы указать запрещенное направление пересечения, нажмите **Select origin (Выбрать исходную зону)**, после чего нажмите одну из зон.
5. В разделе **Detect (Обнаружение)** выберите тип обнаруживаемых объектов.
6. В разделе **Duration parameters (Параметры длительности)**, если вы не хотите активировать зону сразу после появления в ней объекта, задайте параметр **Min presence in (Минимальное время присутствия)** для одной или обеих зон.
7. Если сигнал тревоги должен подаваться для узкой зоны, которую можно пересечь за 1–2 секунды, выберите **Narrow zone (Узкая зона)**. Этот параметр нельзя использовать в комбинации с параметром **Min presence in zone (Минимальное время присутствия в зоне)**. Для получения более подробных сведений см. *Параметры продолжительности на стр. 29*.
8. Чтобы загрузить изменения в камеру и вернуться к основному представлению нажмите **Accept (Принять)**.

Настройка условного сценария

Условный сценарий предназначен для запуска сигнала тревоги при входе объекта в определенную зону без предварительного прохождения через другие зоны.

В разделе **Duration parameters (Параметры длительности)** можно задать минимальное время присутствия для каждой из зон в сценарии. Если T_A — это минимальное время в разрешенной зоне и T_B — в зоне вторжения, то сигнал тревоги срабатывает только в том случае, если объект:

- остается в зоне вторжения дольше, чем T_B без предварительного появления в разрешенной зоне.
- находится меньше, чем T_A в разрешенной зоне, затем входит и остается дольше, чем T_B в зоне вторжения.

Сигнализация не срабатывает, если объект:

- не входит в зону вторжения или находится в зоне вторжения меньше, чем T_B .
- остается в разрешенной зоне дольше, чем T_A , после чего входит в зону вторжения (независимо от того, как долго объект остается в этой зоне).

1. Выберите **Scenarios (Сценарии) > Advanced scenarios (Расширенные сценарии)**.
2. Нажмите **New (Новый)** и выберите **Conditional (Условный)**.
3. Создайте две или более зон обнаружения, отстоящие друг от друга на расстоянии не менее одного метра:
   - Чтобы создать зону обнаружения, щелкните изображение несколько раз.
   - Чтобы завершить зону, щелкните изображение правой кнопкой.
4. Чтобы указать допустимое направление пересечения, нажмите **Select intrusion zone (Выбрать зону вторжения)**, после чего нажмите одну из зон.
5. В разделе **Detect (Обнаружение)** выберите тип обнаруживаемых объектов.
6. В разделе **Duration parameters (Параметры длительности)**, если вы не хотите активировать зону сразу после появления в ней объекта, задайте параметр **Min presence in (Минимальное время присутствия)** для одной или обеих зон.
7. Если сигнал тревоги должен подаваться для узкой зоны, которую можно пересечь за 1–2 секунды, выберите **Narrow zone (Узкая зона)**. Этот параметр нельзя использовать в комбинации с параметром **Min presence in zone (Минимальное время присутствия в зоне)**. Для получения более подробных сведений см. *Параметры продолжительности на стр. 29*.
8. Чтобы загрузить изменения в камеру и вернуться к основному представлению нажмите **Accept (Принять)**.

Сопряжение камер — PTZ Autotracking

При настройке AXIS Perimeter Defender PTZ Autotracking необходимо выполнить сопряжение фиксированной камеры и PTZ-камеры для эффективного отслеживания движущегося объекта PTZ-камерой.

Если вы выполнили автоматическую калибровку, можно провести *Выполнение автоматического сопряжения на стр. 31* двух камер. В противном случае необходимо *Выполнение ручного сопряжения на стр. 32*.

Выполнение автоматического сопряжения

В видеоролике для сопряжения красные линии обозначают человека, а оранжевый прямоугольник обозначает увеличенное изображение PTZ-камеры.

1. В разделе **Calibration (Калибровка) > PTZ Pairing review (Просмотр сопряжения PTZ)** проверьте видеоролики для сопряжения на обеих камерах:
   - убедитесь, что красные линии на двух изображениях выровнены по всему видео
   - убедитесь, что красные линии всегда идут от ног к голове человека
   - убедитесь, что человек всегда располагается по центру в ограничивающем прямоугольнике в видео PTZ-камеры

2. Если условия в шаге 1 выполнены, выберите **Interactive pairing review (Проверка интерактивного сопряжения)**.

   Если условия не выполнены, нажмите **Manual (Ручная)** и выполните процедуры, указанные в разделе *Выполнение ручного сопряжения на стр. 32*.

3. Перемещайте ползунок для выбора. Выполните следующие проверки:

   - синие линии на двух изображениях должны быть совмещены по всему видео
   - человек всегда располагается по центру в ограничивающем прямоугольнике в видео PTZ-камеры

4. Если есть сцены, где отсутствует оранжевый прямоугольник:

   4.1 Активируйте аватар на изображении с фиксированной камеры.

   4.2 Используйте ползунок для навигации. Поместите аватар на человека на изображении с фиксированной камеры и убедитесь, что красная точка находится у ног человека в изображении с PTZ-камеры.

5. Если есть сцены, где автоматическое сопряжение не привело к добавлению синих линий, нажмите **Manual (Ручная)** и вручную добавить красные линии на изображение человека. Подробные инструкции см. в разделе *Выполнение ручного сопряжения на стр. 32*.

6. Нажмите **Accept (Принять)** и **Exit (Выход)**.

Выполнение ручного сопряжения

При выполнении ручного сопряжения вы добавляете вертикальные красные линии от ног к голове человека, который прошел через сцену наблюдения во время калибровки. Вам нужно добавить строки по всему видео, чтобы охватить всю сцену.

Если вы уже выполнили автоматическое сопряжение, видео уже содержит синие линии.

Удалите синие и красные линии, которые:

- не начинаются у ног человека
- не доходят до головы человека
- не имеют соответствующей линии на изображении с PTZ-камеры

Чтобы удалить линию, выделите ее и нажмите DELETE (УДАЛИТЬ).

1. Переместите ползунок для навигации по видеоролику с изображением человека.
2. Поместите красную линию на человека на изображении с фиксированной камеры. Начинайте линию у ног человека. Линия получает идентификационный номер.
3. Добавьте соответствующую красную линию на том же объекте на изображении с PTZ-камеры. Убедитесь, что идентификационный номер совпадает с номером на изображении с фиксированной камеры.
4. Повторяйте шаги 1-3, пока вы не будет покрыта вся сцена.

   Если видеоролик содержит достаточное количество строк для нормального сопряжения:

   - кнопка **Accept (Принять)** становится активной
   - на изображении с PTZ-камеры отображается оранжевый прямоугольник

5. Убедитесь, что человек всегда находится по центру оранжевого прямоугольника. Если есть сцены, где человек находится не по центру, добавьте больше красных линий.
6. Активируйте аватар на изображении с фиксированной камеры.
7. Перемещайте ползунок для выбора. Используйте аватар, чтобы выполнить следующие проверки:

- на изображении с фиксированной камеры размер аватара соответствует размеру человека в разных положениях
- на изображении с PTZ-камеры красная точка находится у ног человека
- на изображении с PTZ-камеры человек всегда располагается по центру в ограничивающем прямоугольнике

8. Нажмите **Accept (Принять)**. Если кнопка неактивна, то добавьте больше красных линий.
9. Нажмите **Exit (Выход)**.

Настройка выходов

Чтобы AXIS Perimeter Defender мог выводить сигналы тревоги при обнаружении вторжения, необходимо определить правила вывода. Система может отправлять сигналы тревоги, например, в систему управления видео.

AXIS Perimeter Defender может посылать сигналы тревоги через различные интерфейсы.

Из самого приложения:

- Сигнал тревоги в формате XML или простого текста через TCP/IP
- Потоки метаданных XML через многопакетный HTTP

С устройства:

- Основные текстовые уведомления для сигналов тревоги по TCP/IP
- Электрические выходы (сухие или влажные контакты)
- Уведомления по электронной почте
- Загрузка изображений на FTP при срабатывании сигналов тревоги

Можно активировать несколько интерфейсов одновременно.

Для получения более подробной информации см. *Выходные порты на стр. 34*.

Для определения правил отправки сигналов тревоги с устройства:

1. Выберите **Outputs (Выходы)** и нажмите **Configure (Настройка)**. В браузере откроется веб-страница устройства.
2. Создайте новое правило действия.
3. В списке инициирующих событий выберите **Applications (Приложения)**, затем выберите **AXISPerimeterDefender** и сценарий для вызова действия.

Примечание.

Чтобы вызвать одно и то же действие для всех определенных сценариев, выберите **ALL_SCENARIOS**.

4. Из списка действий выберите действие для выполнения при соблюдении условия.
5. Нажмите **OK**.

Более подробную информацию о создании правил действий можно найти в руководстве пользователя устройства.

Advanced configuration (Расширенная конфигурация)

Выходные порты

Сигналы тревоги в формате XML/текстовом формате

Этот интерфейс позволяет получать по протоколу TCP/IP более полное и информативное сообщение в формате XML или в текстовом формате при каждом сигнале тревоги. Что касается интерфейса свободного текста, то XML/текстовый интерфейс предлагает следующие преимущества:

- Уведомление отправляется в начале сигнала тревоги, в конце сигнала тревоги и каждые 10 секунд в процессе подачи сигнала тревоги.
- Метка времени: уведомления о начале сигнала тревоги и о завершении сигнала тревоги содержат метку времени, синхронизируемую с часами камеры; эта метка времени позволяет отслеживать точную дату и время событий.
- Тип сигнала тревоги: AXIS Perimeter Defender поддерживает несколько типов сигнала тревоги, см. *Определение сценариев на стр. 28*. Уведомления XML/текстовые уведомления содержат информацию о типе возникшего сигнала тревоги. Обратите внимание: сценарий пересечения зоны относится к типу «passage (прохождение)» , а сценарий обнаружения бесцельного блуждания — к типу «presence (присутствие)»
- Зоны, участвующие в генерации сигнала тревоги; если каждый сценарий AXIS Perimeter Defender связан с одной или несколькими зонами, уведомления в формате XML/текстовом формате информируют о том, какая зона связана с сигналом тревоги (т.е. для сигнала тревоги при вторжении это будут зоны вторжения, в которой обнаружен человек)

Что касается интерфейса свободного текста, то XML/текстовый интерфейс имеет следующие ограничения:

- В сообщениях содержится фиксированный текст, нет свободных текстовых полей.
- За один раз камера может отправлять сообщение только одному получателю.

Получатель уведомлений XML/текстовых уведомлений получает четыре типа сообщений:

- AXIS Perimeter Defender отправляет сообщение CONNECTION_TEST, если настроены уведомления в формате XML, для проверки связи с получателем.
- Когда AXIS Perimeter Defender инициирует сигнал тревоги, будет отправлено сообщение ALARM_START.
- В период подачи сигнала тревоги AXIS Perimeter Defender отправляет несколько сообщений «сигнал тревоги активен», по одному сообщению каждые 10 секунд. Все эти сообщения имеют один и тот же тег GUID, идентичный сообщению ALARM_START и сообщениям ALARM_STOP, связанным с тем же сигналом тревоги
- После завершения сигнала тревоги AXIS Perimeter Defender отправляет уведомление ALARM_STOP.

Подробное объяснение формата этих сообщений, включая информацию о формате XML и о текстовом формате, см. в разделе *Примеры формата XML и текстового формата на стр. 34*.

Примеры формата XML и текстового формата

Формат XML — это формат по умолчанию для уведомлений через TCP/IP. Тем не менее, если важен размер уведомления, можно использовать текстовый формат для генерации коротких сообщений. Для использования текстового формата необходимо выбрать параметр **Do not use XML for alarms (Не использовать XML для сигналов тревоги)** на странице конфигурации AXIS Perimeter Defender.

Пример

Сообщение CONNECTION_TEST в формате XML выглядит следующим образом:

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
```

```
          ID="1"
          TYPE="CONNECTION_TEST"
          SENDER_IP="192.168.1.40"
          SENDER_PORT="0">
  <REFERENTIAL>45</REFERENTIAL>
</KEENEO_MESSAGE>
```

- VERSION — это внутренняя версия синтаксиса и протокола XML.
- ID — это числовой индикатор сообщения. Уникальность и прогрессивность идентификаторов не гарантируется.
- TYPE — это тип сообщения, здесь CONNECTION_TEST. Тип сообщения определяет субтеги сообщения (отсутствуют для сообщений типа CONNECTION_TEST).
- SENDER_IP — это IP-адрес камеры Axis, отправляющей XML-уведомление.
- Значение SENDER_PORT всегда равно нулю; камера не может принимать входящие сообщения.
- REFERENTIAL — это числовой идентификатор, назначенный для камеры.

При выборе текстового формата сообщения уведомлений содержат по 7 полей, разделенных вертикальной чертой «|». Если значение поля указать не удается (например, оно не имеет смысла для данного типа сообщения), оно заменяется на символ «-».

Семь полей, от первого до последнего (в скобках указывается соответствующее поле XML, если выбран формат XML):

1. Числовой идентификатор сообщения (признак "ID" в заголовке сообщения XML "KEENEO_MESSAGE").
2. iPv4-адрес камеры (признак"SENDER_IP" в заголовке сообщения XML "KEENEO_MESSAGE").
3. Справочный номер, связанный с экземпляром AXIS Perimeter Defender (тег REFERENTIAL).
4. Тип сообщения (признак TYPE в заголовке сообщения XML "KEENEO_MESSAGE").
5. Тип сигнала тревоги (тег "TYPE").
6. Название сценария, вызвавшего тревогу (тег "SCENARIO_NAME").
7. Метка времени (тег "TIMESTAMP"). Формат метки времени такой же, как и для формата XML.

Предыдущее сообщение CONNECTION_TEST в текстовом формате будет выглядеть следующим образом.

```
1|192.168.1.40|45|CONNECTION_TEST|-|-|-
```

Пример

Сообщение ALARM_START в формате XML имеет следующий вид:

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xmlns:xsd="http://www.w3.org/2001/XMLSchema"
          VERSION="5.0.0"
          ID="9999"
          TYPE="ALARM_START"
          SENDER_IP="192.168.1.40"
          SENDER_PORT="0">
  <REFERENTIAL>0</REFERENTIAL>
  <TYPE>INTRUSION</TYPE>
  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>
  <EXTRA_DATA>zone=testzone</EXTRA_DATA>
  <TIMESTAMP>2014-03-01T21:24:12.114</TIMESTAMP>
  <GUID>77acddf9-e0d4-402e-a497-231aeee22788</GUID>
</KEENEO_MESSAGE>
```

- Заголовок сообщения такой же, как и в сообщении "CONNECTION_TEST".

- Тип сообщения — "ALARM_START", используется несколько субтегов.
  - REFERENTIAL — это числовой идентификатор, назначенный для камеры.
  - TYPE — это тип тревоги, сгенерированной AXIS Perimeter Defender, в этом примере "INTRUSION". Другие возможные типы: "PRESENCE", "PASSAGE" и "CONDITIONAL".
  - SCENARIO-NAME — это название сценария, который вызвал тревогу, как это определено в интерфейсе конфигурации. См. *Настройка сценария обнаружения вторжения/бесцельного блуждания на стр. 29*.
  - EXTRA_DATA содержит название зоны (или список названий зон), связанных с сигналом тревоги, например, зона вторжения.
  - TIMESTAMP — это дата и время появления аварийного сигнала в формате YYYY-MM-DDTHH:mm:ss.zzz, где:

    - YYYY это обозначение года из 4 цифр, например, 2014.

    — MM содержит обозначение месяца из 2 цифр, например, 01 — январь.

    — DD содержит обозначение дня из 2 цифр, например 03 — 3-е число.

    — 'T' — это фиксированный символ

    — HH обозначает часы в 24-часовом формате, от 00 до 23

    — обозначает минуты, от 00 до 59

    — ss обозначает секунды, от 00 до 59

    — zzz обозначает миллисекунды, от 000 до 999.

    AXIS Perimeter Defender использует внутреннюю дату и время камеры для генерации метки времени сигнализации, поэтому важно синхронизировать камеру с какими-то внешними часами.
  - GUID — это уникальный идентификатор, который является постоянным для всех сообщений, связанных одним сигналом тревоги (ALARM_START, ALARM_IN_PROGRESS and ALARM_STOP)

Это эквивалентно в текстовом формате сообщения ALARM_START:

```
9999|192.168.1.40|0|ALARM_START|INTRUSION|Intrusion-0|2014-03-01T21:24:12.114
```

Пример

Сообщение ALARM_IN_PROGRESS в формате XML выглядит следующим образом:

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="9999"
         TYPE="ALARM_IN_PROGRESS"
         SENDER_IP="192.168.1.40"
         SENDER_PORT="0">
  <REFERENTIAL>0</REFERENTIAL>
  <TYPE>INTRUSION</TYPE>
  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>
  <GUID>77acddf9-e0d4-402e-a497-231aeee22788</GUID>
</KEENEO_MESSAGE>
```

- Заголовок сообщения такой же, как и в сообщении "CONNECTION_TEST" и "ALARM_START".
- Тип сообщения "ALARM_IN_PROGRESS", используется несколько субтегов.
  - REFERENTIAL — это числовой идентификатор, назначенный для камеры.
  - TYPE — это тип сигнала тревоги, инициализированного AXIS Perimeter Defender, совпадает с ALARM_START.

- SCENARIO_NAME — это название сценария, который инициализировал сигнал тревоги, совпадает с ALARM_START.
- GUID совпадает с ALARM_START.

Соответствующее сообщение ALARM_IN_PROGRESS в формате TEXT:

```
9999|192.168.1.40|0|ALARM_IN_PROGRESS|INTRUSION|Intrusion-0|-
```

Пример

Сообщение ALARM_STOP в формате XML выглядит следующим образом:

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="9999"
         TYPE="ALARM_STOP"
         SENDER_IP="192.168.1.40"
         SENDER_PORT="0">
  <REFERENTIAL>0</REFERENTIAL>
  <TYPE>INTRUSION</TYPE>
  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>
  <EXTRA_DATA>zone=testzone</EXTRA_DATA>
  <TIMESTAMP>2014-03-01T21:24:26.304</TIMESTAMP>
  <GUID>77acddf9-e0d4-402e-a497-231aeee22788</GUID>
</KEENEO_MESSAGE>
```

- Заголовок сообщения такой же, как и в предыдущих сообщениях.
- Тип сообщения ALARM_STOP, используется тот же набор подтипов, что и для сообщения ALARM-START.

Соответствующее сообщение ALARM_IN_PROGRESS в формате TEXT:

```
9999|192.168.1.40|0|ALARM_STOP|INTRUSION|Intrusion-0|2014-03-01T21:24:26.304
```

После каждого сообщения связь по протоколу TCP/IP разрывается. Таким образом, прослушивающий сокет у получателя должен всегда быть открытым, чтобы иметь возможность получать следующие уведомления.

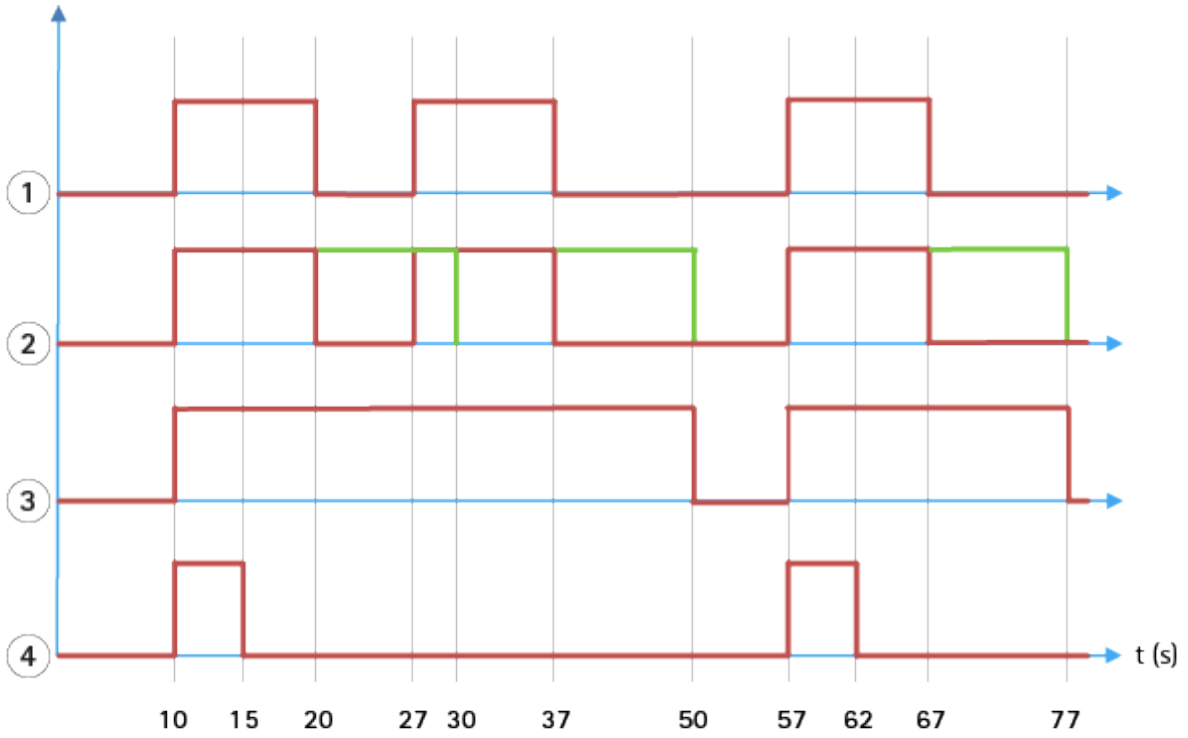
Ошибки связи

Если удаленный получатель уведомлений в формате XML недоступен, например, из-за отключения сети, AXIS Perimeter Defender начинает буферизировать недоставленные сигналы тревоги во внутренней памяти и периодически (как минимум каждые 10 секунд) пытается доставить их повторно. После последовательного количества сбоев в доставке новых сообщений (сбои при попытке повторной доставки сообщения из буфера не учитываются), AXIS Perimeter Defender относит получателя к «постоянно отключенным» и останавливает отправку XML-уведомлений получателю. Количество последовательных сбоев составляет 20, что примерно соответствует 4 или 5 сигналам тревоги при вторжении средней продолжительности 40 секунд каждый. AXIS Perimeter Defender начинает отправлять уведомления тому же получателю снова, если происходит одно из следующих событий:

- Перезапуск AXIS Perimeter Defender.
- Происходит повторное сохранение того же параметра «Alarm streaming url (url для передачи сигнала тревоги)».

Время после начала сигнала тревоги

AXIS Perimeter Defender использует такой параметр как «время после начала сигнала тревоги». Это интервал времени после прекращения сигнала тревоги, в течение которого, если возникает другой сигнал тревоги, оба сигнала объединяются в один уникальный сигнал.



1 *Система AXIS Perimeter Defender выдала три сигнала тревоги с метками времени 10, 27 и 57. Каждый сигнал тревоги имеет продолжительность 10 секунд, т.е. злоумышленнику потребовалось 10 секунд, чтобы пересечь зону вторжения.*
2 *Добавляется время после начала сигнала тревоги, равное 10 секундам.*
3 *Сигналы тревоги с использованием уведомлений XML и метаданных XML.*
4 *Сигналы тревоги с отправкой уведомлений по электронной почте, загрузкой изображений на ftp, срабатыванием электрических контактов и базовыми уведомлениями по протоколу TCP/IP.*

(2) Обратите внимание, как время после начала сигнала тревоги, составляющее 10 секунд (показано зеленым цветом), увеличивает продолжительность каждого сигнала тревоги, что приводит к слиянию двух сигналов тревоги, период между которыми не превышает 10 секунд.

(3) Полученный в итоге номер сигнала тревоги и его продолжительность AXIS Perimeter Defender указывает в XML-уведомлениях и в метаданных XML. Время после начала сигнала может быть использовано для получения меньшего количества более длинных сигналов тревоги вместо нескольких, более коротких сигналов тревоги, следующих друг за другом.

(4) Для сигналов тревоги с отправкой уведомлений по электронной почте, загрузкой изображений на ftp, срабатыванием электрических контактов и базовыми уведомлениями по протоколу TCP/IP результаты добавления времени после начала сигнала тревоги, равного 10 секундам, будут отличаться. Эти уведомления учитывают только начало сигнала тревоги и не учитывают его окончание. Таким образом, при использовании этих уведомлений отсутствует понятие «продолжительность сигнала тревоги», следовательно, время после начала сигнала тревоги не изменяет продолжительность самого уведомления. Продолжительность всегда будет равна фиксированному значению, выбранному пользователем при настройке уведомления. Таким образом, когда последовательные сигналы тревоги сливаются в один из-за использования времени после начала сигнала тревоги, то будет отправлено только одно уведомление. Как видно, AXIS Perimeter Defender объединяет первые два сигнала тревоги и в итоге отправляет только одно уведомление. Таким образом, сигналы тревоги с отправкой уведомлений по электронной почте, загрузкой изображений на ftp, срабатыванием электрических контактов и базовыми уведомлениями по протоколу TCP/IP информируют только о двух из них. На графике отображается фиксированная продолжительность этих уведомлений, равная 5 секундам.

Как настроить время после начала сигнала тревоги

1. Перейдите к настройкам AXIS Perimeter Defender.

2. Выберите **Outputs (Выходы)**.
3. Измените значение параметра **Post-alarm time (Время после начала сигнала тревоги)**. По умолчанию используется значение, равное 7 секундам.
4. Нажмите **Assign (Назначить)**.

Метаданные

Встроенное наложение метаданных

Встроенное наложение метаданных — это функция, которая может накладывать аналитику обнаружения на выбранные живые потоки видео непосредственно в камере. Используются графические наложения в виде прямоугольных рамок и траекторий. Потоки выбираются с учетом разрешения и, если устройство поддерживает зоны просмотра, с учетом зоны просмотра. Встроенные метаданные отображаются как в режиме живого просмотра, так и во время воспроизведения записанного материала.

Встроенные метаданные на отдельных потоках

Например, можно настроить приложение для добавления наложений на все потоки с разрешением 640x480. В этом случае наложение будет присутствовать только на потоках с этим разрешением, а остальные потоки останутся без изменений.

Встроенные метаданные на выбранных зонах просмотра

Если система поддерживает данную функцию, вместе с разрешением вы также можете указать зону просмотра. Например, можно добавлять наложения на потоки, взятые из зоны просмотра номер 3 в разрешении 1280x720. В этом случае только потоки, соответствующие этой конфигурации, будут использовать наложения; другие потоки останутся без изменений, включая потоки, взятые из зоны просмотра номер 3 в другом разрешении, и потоки с разрешением 1280x720, полученные из зоны просмотра, отличной от зоны номер 3.

Добавление встроенных метаданных в видеопоток

Примечание.

Эта функция доступна только на устройствах с прошивкой версии 7.30 или более поздней версии.

В этом примере рассмотрим наложение встроенных метаданных на все видеопотоки с разрешением 640x480. Видеопотоки с любым другим разрешением остаются без изменений.

1. Выберите камеру на панели живых просмотров.
2. Выберите **Outputs (Выходы) > Burnt-in Metadata Overlay (Наложение метаданных на видео)**.
3. Выберите **Enabled (Включено)**.
4. В раскрывающемся списке выберите разрешение 640x480.
5. Нажмите **Apply (Применить)**.
6. Убедитесь, что метаданные отображаются в живом просмотре для этого разрешения.

Интеграция с ПО для управления видео

AXIS Perimeter Defender легко интегрируется со следующими системами управления видео (VMS):

- Security Center от Genetec™
- XProtect® от Milestone

Подробную информацию о поддерживаемых версиях ПО для управления видео см. по ссылке *axis.com/products/axis-perimeter-defender/support-and-documentation*

Сигналы тревоги, сгенерированные AXIS Perimeter Defender, автоматически преобразуются в события в ПО для управления видео, что, в свою очередь, может вызывать различные последующие действия для полного использования всех возможностей ПО. Одновременно с этим «живые» метаданные, сгенерированные приложением AXIS Perimeter Defender, отправляются в ПО для управления видео для живого отображения и записи. Таким образом, метаданные также доступны при воспроизведении записанных видео последовательностей в режиме воспроизведения.

Автоматизированная система обнаружения вторжения предназначена для запуска сигналов тревоги и предоставления информации, которая помогает информировать о нарушении безопасности. Это может предполагать отправку уведомления на мобильное устройство или отображение сигнала тревоги в системе управления видео, в некоторых случаях субъект, инициировавший событие сигнализации, будет иметь выделение на экране.

Стандартная интеграция событий

AXIS Perimeter Defender использует и расширяет родные интерфейсы и функции ACAP для отправки сигналов тревоги и дополнительной информации на внешние устройства или в системы управления видео. События, выводимые через AXIS Perimeter Defender, могут быть преобразованы в сообщения для систем управления видео с применением определенных правил действий.

Доступны следующие каналы передачи сигналов тревоги с камеру в систему управления видео:

- Основные текстовые уведомления для сигналов тревоги (TCP/IP)
- Электрические выходы (сухие или влажные контакты)
- Уведомления по электронной почте
- Загрузка изображений на FTP при срабатывании сигналов тревоги

Эти интеграции можно настраивать на камере. См. *Время после начала сигнала тревоги на стр. 37*.

VMS-мосты

Для следующих систем управления видео мы предлагаем готовые интеграционные модули, называемые «мостами»:

- Milestone XProtect® 2014 и 2016 Corporate/Expert/Enterprise/Professional/Express. Версии Enterprise/Professional/Express не поддерживают метаданные (в том числе отображение метаданных в режимах живого просмотра и воспроизведения)
- Genetec™ Service Center 5.3 и 5.4 Pro/Enterprise/SV32/SV16

Мосты обеспечивают два вида интеграции:

- Создание пользовательских событий сигнализации в системе управления видео в соответствии с событиями, выводимыми через AXIS Perimeter Defender.
- Отображение наложений сигнала тревоги или прямоугольных рамок поверх живого видео, а также сделанных ранее записей (за исключением версий Milestone XProtect® Enterprise/Professional/Express).

VMS-мосты необходимо скачать и установить в виде отдельных приложений. Более подробную информацию по установке и настройке мостов см. в руководствах к соответствующим мостам.

Создайте правило в AXIS Camera Station

В этом разделе описывается интеграция AXIS Perimeter Defender в систему событий ПО Axis Camera Station. Изучив данный раздел, вы узнаете следующее:

- Как настроить правило для AXIS Camera Station, чтобы оно срабатывало при вторжении.
- Как убедиться в том, что настройка выполнена правильно.

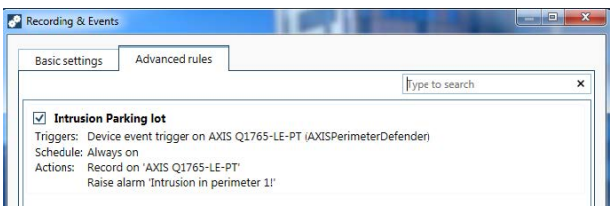
1. Настройте и откалибруйте AXIS Perimeter Defender в программном обеспечении AXIS Perimeter Defender Setup, предназначенном для настройки этого приложения. Справочные сведения об установке и калибровке

AXIS Perimeter Defender можно найти в руководстве пользователя приложения AXIS Perimeter Defender или *на странице данного продукта*.

2. Добавьте камеру в систему AXIS Camera Station, следуя указаниям мастера **Add Camera (Добавление камеры)**.
3. Настройте триггер для события на устройстве:
   - 3.1 Выбрав в меню **Configuration (Конфигурация)** > **Recording & Events (Запись и события)**, откройте вкладку **Advanced rules (Расширенные правила)**.
   - 3.2 Создайте новое правило и выберите триггер **Device Event (Событие на устройстве)**.
   - 3.3 Выберите камеру, на которой установлено приложение AXIS Perimeter Defender.
   - 3.4 В списке **Event (События)** выберите **AXISPerimeterDefender (AXIS Perimeter Defender)**.
   - 3.5 В списке **Feature (Характеристики)** выберите имя настраиваемого вторжения (в данном случае это "Intrusion-1"). Если вы хотите, чтобы правило срабатывало для всех настроенных сценариев, выберите пункт **ALL_SCENARIOS (Все сценарии)**.
   - 3.6 Выберите **Yes (Да)**, если триггер должен активироваться при вторжении. Если будет обнаружено вторжение, то в окне «Активность» отобразится изменение состояния, что позволит убедиться в правильности настройки.
   - 3.7 Чтобы настроить одно или несколько действий, нажмите кнопку **OK (OK)**, а затем **Next (Далее)**.
   - 3.8 В диалоговом окне **Add Action (Добавление действия)** можно добавить одно или несколько действий для данного правила.

В этом примере мы добавляем действие «Включение видеозаписи» и действие «Подача сигнала тревоги».

   - 3.9 Нажмите кнопку **Finish (Готово)**.



В данном примере показано правило для AXIS Camera Station, которое запускает два действия, если произошло вторжение.

4. Смоделируйте вторжение, чтобы проверить правильность срабатывания настроек; для этого можно физически зайти на охраняемую территорию.

Поиск и устранение неисправностей

Для надлежащей работы всех функций необходимо настроить следующие параметры Axis:

- Network (Сеть) / TCP-IP / Basic (Базовые) / Default router (Маршрутизатор по умолчанию)
- Network (Сеть) / TCP-IP / Advanced (Расширенные)/ Domain name (Имя домена)
- Network (Сеть) / TCP-IP / Primary DNS Server (Основной DNS-сервер)
- Network (Сеть) / TCP-IP / Secondary DNS Server (Резервный DNS-сервер)
- Network (Сеть) / TCP-IP / NTP server address (Адрес NTP-сервера)
- Network (Сеть) / TCP-IP / SMTP (email) (Сервер электронной почты (SMTP))
- System Options (Параметры системы) / Date & Time (Дата и время) / Time Zone (Часовой пояс)
- System Options (Параметры системы) / Date & Time (Дата и время) / Synchronize with NTP server (Синхронизировать с NTP-сервером)

Обновление до последней версии

Чтобы воспользоваться последними улучшениями без необходимости повторной калибровки и переопределения сценариев, мы рекомендуем обновляться до последней версии AXIS Perimeter Defender.

1. Скачайте и установите последнюю версию AXIS Perimeter Defender.
2. Нажмите **Install (Установить)**. Мастер установки AXIS Perimeter Defender Setup автоматически выполняет необходимые шаги для завершения установки:
   - Резервное копирование существующей калибровки, сценариев, параметров и лицензии.
   - Установка новой версии.
   - Восстановление лицензии.
   - Восстановление калибровки и сценариев.
   - Восстановление параметров.
   - Если приложение до этого работало, оно будет запущено повторно.

Обновление прошивки камеры

Примечание.

Перед обновлением прошивки камеры сохраните все настройки AXIS Perimeter Defender. Обновление прошивки удаляет приложение и его настройки с камеры. В случае сохранения параметров их можно восстановить с помощью AXIS Perimeter Defender Setup.

1. Используйте AXIS Perimeter Defender Setup для сохранения конфигурации объекта.
2. Обновите прошивку камеры. Для получения инструкций обратитесь к руководству пользователя камеры.
3. Запустите AXIS Perimeter Defender Setup.
4. Используйте опцию загрузки параметров объекта для автоматической загрузки сохраненной конфигурации объекта для каждой обновленной камеры.

Поиск и устранение неисправностей

Устранение неполадок, связанных с установкой

Проблема	Возможная причина	Решение
Windows® выдает сообщение, информирующее о невозможности установки приложения.	Несовместимая операционная система на ноутбуке или на ПК.	Убедитесь в том, что версия ОС Windows® соответствует указанным требованиям.
Windows® выдает сообщение о неправильной установке.	Помощник по совместимости программ Windows® обнаружил возможную проблему при установке.	Подтвердите правильность и продолжите установку.
Ошибка при установке XVID.	Не удается установить XVID из-за наличия на компьютере старых установочных файлов XVID.	Удалите папку XVID в C:\Program Files (x86) и попробуйте установить еще раз.
Программа установки внезапно закрывается после отображения лицензионного соглашения с конечным пользователем. Windows® выдает сообщение об ошибке, сообщающее о нештатном закрытии приложения. Закрыть установщик невозможно.	Известная проблема в пакетах установки приводит к сбою приложения при некоторых обстоятельствах.	Откройте диспетчер задач и остановите все процессы msiexec.exe. Затем остановите процесс установщика и перезапустите установщик.

Устранение неполадок конфигурации

Проблема	Возможная причина	Решение
Проблемы с открытием AXIS Perimeter Defender.	Отсутствуют достаточные пользовательские права в Windows®.	Убедитесь, что у вас есть права администратора.
Функция поиска не находит мои камеры.	Брандмауэр	Брандмауэры и антивирусное программное обеспечение могут иногда блокировать обнаружение камеры. В случае необходимости настройте брандмауэр таким образом, чтобы разрешить сетевой трафик к приложению AXIS Perimeter Defender и от него. Если это не решает проблему, настройте брандмауэр так, чтобы разрешить следующие порты: UDP-порт 5353 и TCP-порт 80.
	Проблемы с IP-адресом	Любое устройство в сети должно иметь уникальный IP-адрес, чтобы иметь возможность связи с другими устройствами. При работе с AXIS Perimeter Defender рекомендуется использовать фиксированные IP-адреса для камер. Убедитесь, что каждое IP-устройство в сети имеет свой собственный IP-адрес и не использует уже занятый IP-адрес.
	Камера недоступна с компьютера пользователя.	Наберите IP-адрес камеры в браузере, чтобы подтвердить ее доступность. Если камера недоступна, то ее установка в сети была выполнена неправильно или компьютер не имеет доступа к камере.

Поиск и устранение неисправностей

Проблема	Возможная причина	Решение
Невозможно добавить камеру.	Неверно заданы параметры подключения камеры, например IP-адрес, пароль или порт HTTP.	Проверьте правильность введенных параметров и повторите попытку.
	Камера не видна с компьютера пользователя.	Наберите IP-адрес камеры в браузере, чтобы подтвердить ее доступность. Если камера недоступна, то ее установка в сети выполнена неправильно, или компьютер не имеет доступа к сети, в которой находится камера.
Потеря видеопотоков в AXIS Perimeter Defender Setup.	Источник видео больше недоступен.	Работа источника видео была прервана, поэтому видеосигнал на дисплее не обновляется.
	Используйте браузер для проверки доступности камеры.	Нажмите на плитку, где должен находиться видеопоток, и измените размер интерфейса; поток видео должен снова появиться.
Автоматическая калибровка не работает или дает плохие результаты.	Не выполнены предварительные требования.	Проверьте выполнение требований к монтажу. См. *Установка камеры на стр. 14*.
	Камера использует вращение.	Откалибровать камеру с вращением невозможно.
	Медленное подключение к камере, которая не настроена в качестве удаленной камеры.	Подключите камеру как удаленное устройство для снижения нагрузки на полосу пропускания.
	В сцене, используемой для автоматической калибровки, присутствуют другие движущиеся объекты, например, автомобили, деревья или другие лица.	Повторите автоматическую калибровку или откалибруйте устройство вручную.
	Поле обзора камеры слишком загромождено, в результате человек, идущий перед камерой, зачастую оказывается виден не полностью.	Откалибруйте устройство вручную.
	Слишком малая область обзора, например вход.	Откалибруйте устройство вручную.
	Снятое видео не было должным образом записано из-за отсутствия места на диске.	Убедитесь в наличии места на диске и что приложению разрешено сохранение видео на компьютер, на котором работает AXIS Perimeter Defender.

Устранение неполадок в работе

Проблема	Возможная причина	Решение
Приложение не работает, конфигурация выполнена правильно.	Прошивка камеры не обновлена.	Убедитесь, что установлена последняя версия прошивки для камеры.

Наложение не отображается AXIS Perimeter Defender Setup при запущенном анализе.	Приложение блокируется после запуска или остановки работы или обновления пакета AXIS Perimeter Defender.	Перезапустите камеру.
	Брандмауэр блокирует подключение к порту входящих соединений метаданных камеры.	Настройте брандмауэр таким образом, чтобы интерфейс конфигурации подключаться к порту входящих соединений метаданных камеры.
	Антивирусная программа блокирует прием наложения.	Настройте антивирус, разрешив получение наложения.
Сигнализация в настроенной на компьютере версии AXIS Perimeter Defender не срабатывает несмотря на работающий анализ и видимое наложение.	Хотя цель находится в зоне обнаружения, она не соответствует условному сценарию, например, не переходит из одной зоны в другую в сценарии пересечения зоны.	Проверьте правильность выбора сценария и условий.
	Плохое обнаружение.	Проверьте выполнение требований к монтажу. См. *Установка камеры на стр. 14*. Также убедитесь, что калибровка выполнена с достаточной точностью, и что настроена достаточная чувствительность.

Поиск и устранение неисправностей, связанных с производительностью системы

Проблема	Возможная причина	Решение
Экранное меню и данные анализа постоянно появляются и исчезают.	Слишком высокая загрузка процессора камеры.	Возможные решения: • Убедитесь, что поток камеры визуализируется только в нужных местах, поскольку каждая визуализация потока камеры увеличивает нагрузку на процессор. • Если активирована запись при срабатывании встроенного датчика движения, попробуйте снизить качество записи, чтобы высвободить ресурсы процессора. • Деактивируйте запись при срабатывании встроенного датчика движения и убедитесь в том, что встроенный датчик движения отключен.
После входа целевого объекта в охраняемую зону срабатывают несколько сигналов тревоги.	Задано слишком короткое время после начала сигнала тревоги .	Отрегулируйте время после начала сигнала тревоги. Выберите AXIS Perimeter Defender Setup (Настройка AXIS Perimeter Defender) > **Outputs (Выходы)**.

Поиск и устранение неисправностей

Проблема	Возможная причина	Решение
Потенциальная цель входит в охраняемую зону, при этом сигнал тревоги не срабатывает — пропуск события.	Недостаточная контрастность объекта на общем фоне.	Проверьте выполнение требований к монтажу. См. *Установка камеры на стр. 14*.
	Недостаточное освещение в зоне обнаружения или недостаточная светочувствительность камеры.	Проверьте выполнение требований к монтажу. См. *Установка камеры на стр. 14*.
	Настроена слишком низкая чувствительность AXIS Perimeter Defender.	Увеличьте чувствительность в глобальных параметрах сценария.
	Изменение положения камеры привело к нарушению калибровки.	Выполните повторную калибровку.
	Калибровка недостаточно точная.	Проверьте калибровку камеры. Перейдите в раздел AXIS Perimeter Defender Setup (Настройка AXIS Perimeter Defender).
	Хотя цель находится в зоне обнаружения, она не соответствует условному сценарию, например, не переходит из одной зоны в другую в сценарии пересечения зоны.	Проверьте правильность выбора сценария и условий.
Цель обнаруживается, но классифицируется неправильно (человек распознается как автомобиль или автомобиль — как человек).	Неправильно выбрана высота, позиция или ориентация камеры.	Проверьте выполнение требований к монтажу. См. *Установка камеры на стр. 14*.
	Камера находится слишком далеко от зоны.	Проверьте выполнение требований к монтажу. См. *Установка камеры на стр. 14*.
	Калибровка недостаточно точная.	Проверьте калибровку камеры. Перейдите в раздел AXIS Perimeter Defender Setup (Настройка AXIS Perimeter Defender).
AXIS Perimeter Defender генерирует сигнал тревоги, когда нет вторжения в охраняемую зону.	Чувствительность анализа слишком высокая.	Уменьшите чувствительность. Перейдите в раздел AXIS Perimeter Defender Setup (Настройка AXIS Perimeter Defender).
	Калибровка недостаточно точная.	Проверьте калибровку камеры. Перейдите в раздел AXIS Perimeter Defender Setup (Настройка AXIS Perimeter Defender).
	Изменение положения камеры привело к нарушению калибровки.	Выполните повторную калибровку.
	Неправильная высота, позиция или ориентация камеры.	Проверьте выполнение требований к монтажу. См. *Установка камеры на стр. 14*.
	Камера движется, например, раскачивается или вибрирует.	Установите камеру в более стабильных условиях.
	Растительность или другие движущиеся объекты, например флаги, находятся близко к камере.	Удалите мешающие предметы из поля зрения камеры. AXIS Perimeter Defender будет игнорировать объекты, которые постоянно находятся в сцене, но не двигаются.

Поиск и устранение неисправностей

Проблема	Возможная причина	Решение
	На объективе камеры или рядом с ним ползают насекомые.	По возможности не допускайте попадания насекомых на объектив камеры или в прилегающие зоны.

Это руководство предназначено для администраторов и пользователей AXIS Perimeter Defender. Данный документ содержит инструкции по использованию и управлению устройством в сети. При использовании данного устройства будет полезен опыт организации локальных сетей.

Заявления о товарных знаках

Руководство пользователя
AXIS Perimeter Defender

Версия M15.5
Дата: Август 2021
Артикул T10068952