

## AXIS D2110-VE Security Radar

**Руководство пользователя**

# AXIS D2110-VE Security Radar

## Содержание

---

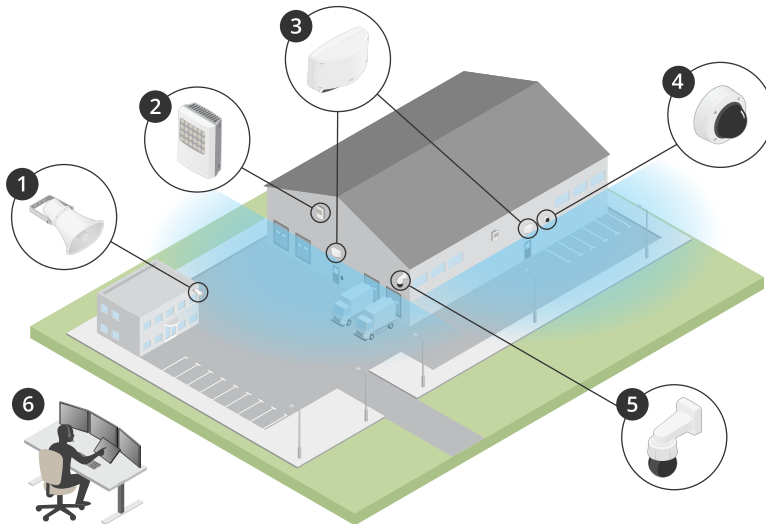
<b>Общие сведения о решении</b> .....	3
Профили радара .....	3
Выбор места установки .....	3
Установка нескольких радаров .....	4
Область охвата .....	4
<b>Профиль наблюдения за областью</b> .....	5
Примеры установки .....	5
Диапазон области обнаружения .....	6
Практические примеры наблюдения за областью .....	7
<b>Профиль наблюдения за дорогой</b> .....	9
Примеры установки для наблюдения за дорогой .....	9
Диапазон обнаружения на дороге .....	9
Практические примеры наблюдения за дорогой .....	10
<b>Начало работы</b> .....	12
Поиск устройства в сети .....	12
Откройте веб-страницу устройства .....	12
Обзор веб-страницы .....	13
<b>Настройка устройства</b> .....	14
Калибровка радара .....	14
О зонах обнаружения .....	14
Просмотр и запись видео .....	16
Настройка правил для событий .....	17
Инструкции .....	18
<b>Проверьте установку</b> .....	23
Проверка установки радара .....	23
Проверка радара .....	23
Завершение проверки .....	26
<b>Интерфейс устройства</b> .....	27
Состояние .....	27
Видео .....	28
Записи .....	30
Приложения .....	31
Система .....	31
Обслуживание .....	48
<b>Устранение неполадок</b> .....	49
Сброс к заводским установкам .....	49
Проверка текущей версии встроенного ПО .....	49
Обновление встроенного ПО .....	49
Технические проблемы, советы и решения .....	50
Рекомендации по увеличению производительности .....	51
<b>Рекомендации по очистке</b> .....	52
<b>Характеристики</b> .....	53
Общий вид устройства .....	53
Слот для SD-карты .....	54
Кнопки .....	54
Разъемы .....	54

# AXIS D2110-VE Security Radar

## Общие сведения о решении

---

### Общие сведения о решении



- 1 Рупорный громкоговоритель C1310-E Horn Speaker
- 2 Дверной контроллер
- 3 Охранный радар D2110-VE Security Radar
- 4 Фиксированная купольная камера
- 5 PTZ-камера
- 6 Центр охранного видеонаблюдения

### Профили радара

#### Примечание.

Чтобы можно было использовать профили радара, устройство должно иметь встроенное ПО версии не ниже 10.11. Для обновления встроенного ПО устройства перейдите на веб-сайт .

Руководство пользователя организовано таким образом, чтобы вы могли получить помощь по использованию радара в зависимости от того, какую задачу вы решаете. Для охранного радара AXIS D2110-VE Security Radar предусмотрено два профиля:

- Профиль наблюдения за областью для отслеживания крупных и мелких объектов, движущихся со скоростью ниже 55 км/ч.
- Профиль наблюдения за дорогой для отслеживания транспортных средств, движущихся со скоростью до 105 км/ч.

Любая информация в данном руководстве пользователя, которая не относится конкретно к профилю наблюдения за областью или профилю наблюдения за дорогой, является общей для обоих профилей и может использоваться независимо от того, какой из этих профилей применяется.

### Выбор места установки

- Радар предназначен для мониторинга открытых пространств. Любой сплошной объект (стена, забор, дерево, большой куст и т. п.) в зоне покрытия создает позади себя «слепую» зону («радиолокационную тень»).

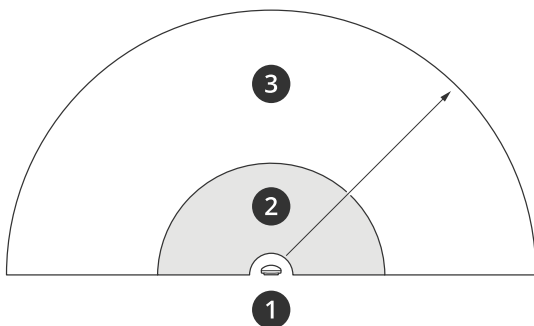
# AXIS D2110-VE Security Radar

## Общие сведения о решении

- Установите радар на устойчивом столбе или на стене в таком месте, где нет других объектов или сооружений. Объекты, расположенные слева или справа от радара на расстоянии до 1 м и способные отражать радиоволны, будут влиять на работу радара.
- Металлические объекты в пределах области обзора вызывают отражения, влияющие на способность радара классифицировать объекты.
- Не допускайте, чтобы более трех радаров были направлены друг на друга.
- Если более трех радаров будут установлены на небольшом расстоянии друг от друга, то возможны взаимные помехи. О том, как избежать помех от других радаров AXIS D2110-VE Security Radar, см. в разделе *Установка нескольких радаров на стр. 4*.

## Установка нескольких радаров

Радиоволны распространяются за пределы области обнаружения и могут создавать помехи для других радаров, находящихся на расстоянии до 350 м.



- 1 Радар
- 2 Область обнаружения
- 3 Область взаимного влияния

### Примечание.

Чтобы избежать помех в случае установки более двух радаров в одной зоне взаимного влияния, перейдите к пункту **Settings > Radar > General (Настройки > Радар > Общие)** и задайте **Number of neighboring radars (Количество соседних радаров)** в разделе **Coexistence (Взаимное влияние)** равным 2.

Если в области взаимного влияния радара работает больше двух близко расположенных радаров, характеристики радара ухудшаются. Сокращается дальность обнаружения, радар неправильно классифицирует объекты, возникают ложные тревоги из-за взаимных помех между радаром.

Чем больше радаров работают в пределах одной области взаимного влияния, тем выше вероятность и степень серьезности этих проблем. Также это зависит от особенностей среды применения и от того, куда направлен радар: в сторону ограждений, зданий или соседних радаров.

Если в системе принципиально важно использовать более двух радаров, см. раздел *Примеры установки на стр. 5*.

## Область охвата

Модель AXIS D2110-VE обеспечивает охват в горизонтальной плоскости на 180°. Площадь области обнаружения составляет 5600 м<sup>2</sup> при обнаружении людей и 11 300 м<sup>2</sup> при обнаружении транспортных средств.

### Примечание.

Оптимальная область охвата достигается при установке радара на высоте 3,5–4 м. От высоты установки также зависит размер «слепой» зоны под радаром.

# AXIS D2110-VE Security Radar

## Профиль наблюдения за областью

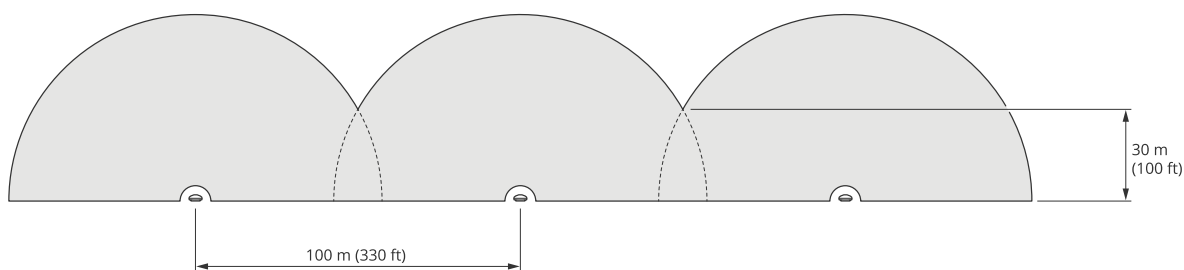
### Профиль наблюдения за областью

Профиль наблюдения за областью лучше всего использовать для объектов, движущихся со скоростью до 55 км/ч. Этот профиль позволяет определить, является ли объект человеком, автомобилем или неизвестным объектом. Можно настроить правило для активации события при обнаружении любого из этих объектов. Если требуется отслеживать только транспортные средства, используйте *Профиль наблюдения за дорогой на стр. 9*.

### Примеры установки

#### Охват периметра

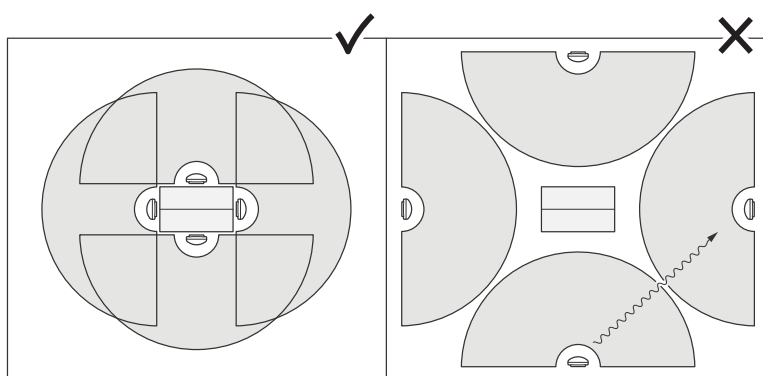
Чтобы создать виртуальное ограждение, можно установить несколько радаров рядом друг с другом. Мы рекомендуем устанавливать их на расстоянии 100 м друг от друга.



#### Охват пространства вокруг здания

Чтобы охватить территорию вокруг здания, установите радары на стенах здания так, чтобы они были направлены не на стены здания, а в противоположные стороны. В этом случае радары можно разместить рядом друг с другом, взаимных помех они создавать не будут.

Если же более трех радаров будут направлены в сторону здания (т. е. внутрь территории), они будут излучать радиоволны в направлении друг друга и взаимные помехи в этом случае будут выше.



#### Охват области

Чтобы охватить обширную открытую территорию, с помощью двух мачтовых креплений установите радары на столбе, направив их в противоположные друг от друга стороны.

#### Примечание.

Когда два радара устанавливаются так близко друг от друга, они находятся в одной зоне взаимного влияния.

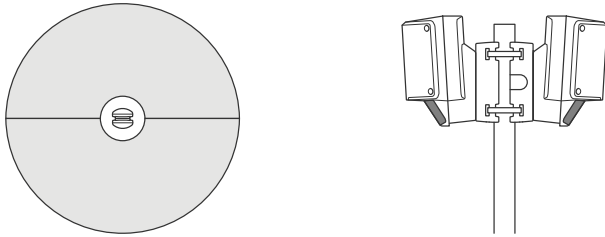
# AXIS D2110-VE Security Radar

## Профиль наблюдения за областью

Выход PoE одного радара можно использовать для питания второго радара, однако третий радар таким способом подключить не получится.

### Примечание.

Выход PoE радара действует, если для питания радара используется инжектор на 60 Вт.



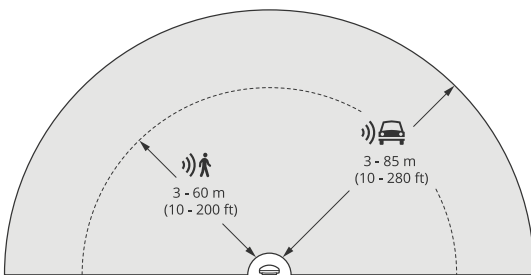
## Диапазон области обнаружения

Диапазон обнаружения — это диапазон расстояний, в пределах которого устройство может отследить объект и инициировать сигнал тревоги. Этот диапазон простирается от **ближней границы обнаружения** (насколько близко к устройству может производиться обнаружение) до **дальней границы обнаружения** (насколько далеко от устройства может производиться обнаружение).

Профиль наблюдения за областью оптимизирован для обнаружения людей, однако он также позволяет отслеживать транспортные средства и другие объекты, движущиеся со скоростью до 55 км/ч (погрешность определения скорости составляет +/- 2 км/ч).

В случае установки на оптимальной высоте обеспечиваются следующие диапазоны обнаружения:

- 3–60 м при обнаружении человека;
- 3–85 м при обнаружении транспортного средства.



### Примечание.

- Если радар установлен на другой высоте, укажите фактическую высоту на веб-странице устройства при калибровке радара.
- Дальность обнаружения зависит от условий в месте ведения наблюдения.
- На дальность обнаружения влияют соседние радары.
- Дальность обнаружения зависит от типа объекта.

Дальность обнаружения измерялась при следующих условиях:

- Дальность измерялась на уровне земли.

# AXIS D2110-VE Security Radar

## Профиль наблюдения за областью

- В качестве объекта выступал человек ростом 170 см.
- Человек ходил прямо перед радаром.
- Значения измеряются, когда человек входит в зону обнаружения.
- Чувствительность радара была установлена на **Medium (Средняя)**.

Высота монтажа	Наклон 0°	Наклон 10°	Наклон 20°
2,5 м	3,0–60 м	Не рекомендуется	Не рекомендуется
3,5 м	3,0–60 м	Не рекомендуется	Не рекомендуется
4,5 м	4,0–60 м	Не рекомендуется	Не рекомендуется
5,5 м	7,5–60 м	Не рекомендуется	Не рекомендуется
6,5 м	7,5–60 м	5,5–60 м	Не рекомендуется
8 м	Не рекомендуется	9–60 м	7,5–30 м
10 м	Не рекомендуется	15–60 м	9–35 м
12 м	Не рекомендуется	23–60 м	13–38 м
14 м	Не рекомендуется	27–60 м	17–35 м
16 м	Не рекомендуется	Не рекомендуется	25–50 м

## Практические примеры наблюдения за областью

### Охват зоны плавательного бассейна

На территорию общественного бассейна несколько раз проникали посторонние лица в нерабочее время. По этическим соображениям владельцы бассейна не могут установить систему охранного видеонаблюдения. Они решили установить радар и выбрать для него профиль **Area monitoring profile (Профиль наблюдения за областью)**. Радар установлен на здании и охватывает весь бассейн, а также большую часть территории вокруг него. В случае обнаружения человека, когда бассейн закрыт (между 20:00 и 06:00), радар запускает воспроизведение предупреждающего сообщения с использованием громкоговорителя.

### Охват пространства вокруг здания

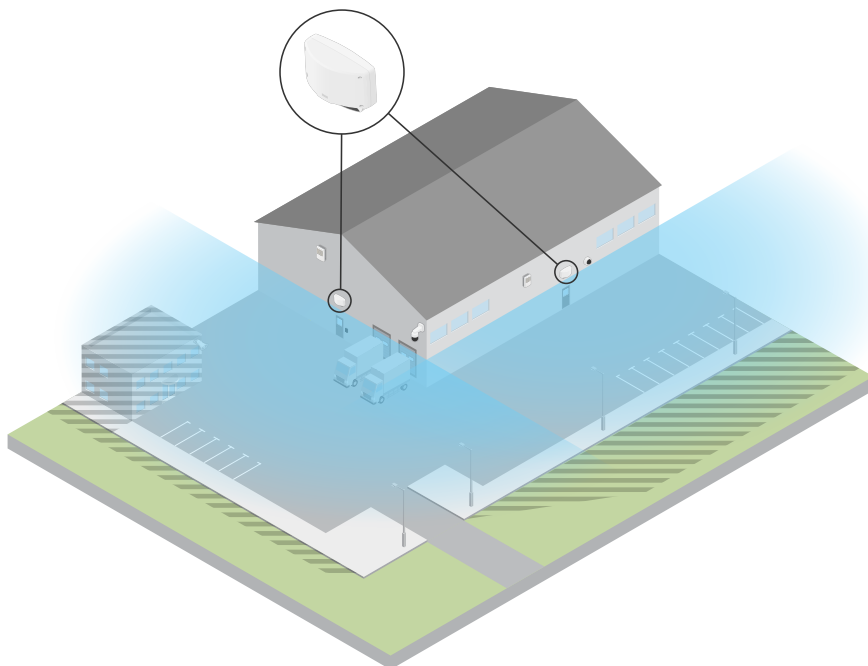
Завод по производству химреактивов принял решение усилить безопасность за счет применения радаров, охватывающих территорию вокруг здания с особо важным цехом. Система безопасности уже оснащена камерами, тепловизорами и дверными контроллерами. Радары могут инициировать события, по которым камеры начинают отслеживать перемещения нарушителя, увеличивают изображение и начинают вести видеозапись для фиксации всех действий. Кроме того, начинают мигать проблесковые маячки, подключенные к тепловизионным камерам, чтобы нарушитель знал, что территория охраняется.

# AXIS D2110-VE Security Radar

## Профиль наблюдения за областью

---

Дверные контроллеры не дают нарушителю проникнуть в закрытые зоны. Благодаря радарам система защиты начинает действовать задолго до того, как нарушитель оказывается рядом с особо охраняемым цехом.



### Охват обширной открытой территории

На парковке возле небольшого торгового центра участились случаи кражи вещей из салонов автомобилей в нерабочее время. В штате есть охранники, которые дежурят посменно, но в магазине посчитали, что нужно усилить охрану в ночное время, не неся при этом дополнительных затрат на наем дополнительного персонала. Было решено установить два охранных радара в режиме **Area monitoring profile** (Профиль наблюдения за областью) рядом друг с другом и направить их в противоположные друг от друга стороны, чтобы охватить целиком всю зону парковки. В соответствии с настройками радары оповещают дежурного охранника о подозрительных действиях на территории, благодаря чему охранник может оперативно оценить обстановку, взглянув на монитор, и принять необходимые меры. Также можно установить рупорный громкоговоритель для воспроизведения предупреждающего сообщения по сигналу с радаров с целью отпугнуть воришек.



# AXIS D2110-VE Security Radar

## Профиль наблюдения за дорогой

---

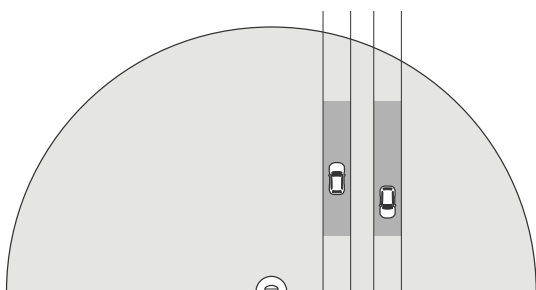
### Профиль наблюдения за дорогой

Профиль *Road monitoring profile* (Профиль наблюдения за дорогой) лучше всего использовать для отслеживания транспортных средств, движущихся со скоростью до 105 км/ч, на территории города, в закрытых зонах и на пригородных дорогах. Этот режим не следует использовать для обнаружения людей и объектов других типов. Если нужно отслеживать не автомобили, а другие объекты, для радара следует выбрать режим *Профиль наблюдения за областью на стр. 5*.

### Примеры установки для наблюдения за дорогой

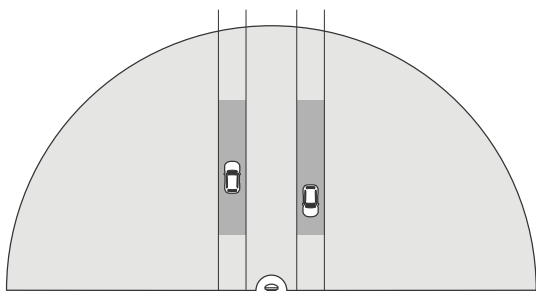
#### Установка сбоку от дороги

Для наблюдения за автомобилями, движущимися по дороге, радар можно установить сбоку от дороги. Радар обеспечит охват до 10 м в направлении, перпендикулярном направлению дороги.



#### Установка в центре

Для этого варианта установки требуется стабильная конструкция. Радар может быть установлен на столбе посреди дороги или на мосту над дорогой. Радар обеспечит тогда охват до 10 м с обеих сторон в направлении, перпендикулярном направлению дороги. Таким образом, установка радара в центре позволяет охватить более обширный участок дороги.



#### Примечание.

При использовании профиля *Road Monitoring Profile* (Профиль наблюдения за дорогой) радар рекомендуется устанавливать на высоте от 3 м до 8 м.

### Диапазон обнаружения на дороге

Диапазон обнаружения — это диапазон расстояний, в пределах которого устройство может отследить объект и инициировать сигнал тревоги. Этот диапазон простирается от **ближней границы обнаружения** (насколько близко к устройству может производиться обнаружение) до **дальней границы обнаружения** (насколько далеко от устройства может производиться обнаружение).

# AXIS D2110-VE Security Radar

## Профиль наблюдения за дорогой

Этот профиль оптимизирован для обнаружения транспортных средств и обеспечивает точность определения скорости  $\pm 2$  км/ч, когда скорость автомобилей не превышает 105 км/ч.

Когда радар установлен на оптимальной высоте, обеспечиваются следующие диапазоны обнаружения:

- 25–70 м при скорости движения автомобилей 60 км/ч;
- 30–60 м при скорости движения автомобилей 105 км/ч.

### Примечание.

Наличие более двух радаров в пределах одной зоны взаимного влияния ведет к сужению диапазона обнаружения примерно на 10 % (ближняя граница) и 20 % (дальняя граница).

## Практические примеры наблюдения за дорогой

### Регулирование движения транспорта в зонах с низкой скоростью движения

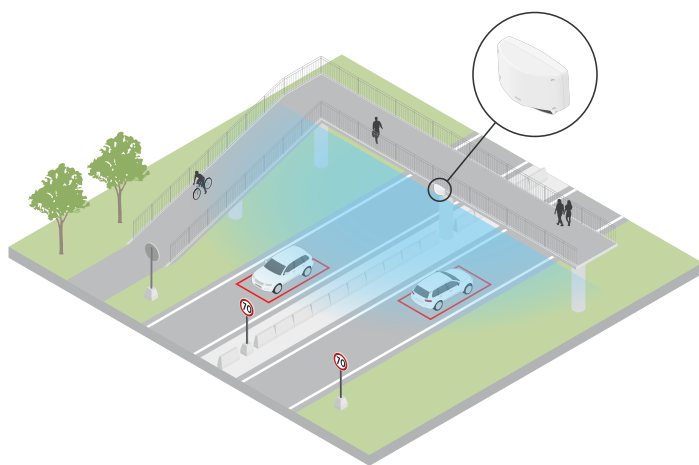
На территории промышленного комплекса с протяженной дорогой между двумя складами установили радар, чтобы обеспечивать соблюдение ограничения скорости в 60 км/ч. При работе в режиме **Road monitoring profile (Профиль наблюдения за дорогой)** радар может обнаруживать, когда транспортное средство в зоне обнаружения превышает эту скорость. В этом случае радар активирует событие, при котором водителю и управляющему отправляются соответствующие уведомления по электронной почте. Это дисциплинирует водителей, и они более строго соблюдают скоростной режим.

### Предотвращение проезда по закрытой дороге

Небольшая дорога, ведущая к старому карьеру, была закрыта, но некоторые водители продолжали ей пользоваться, и власти решили установить охранный радар в режиме **Road monitoring profile (Профиль наблюдения за дорогой)**. Радар установлен на обочине, и его охвата хватает на всю ширину дороги. Когда какой-либо автомобиль въезжает в зону включения, радар включает проблесковый маячок, который предупреждает водителей о необходимости покинуть дорогу. Он также отправляет сообщение службе охраны, и при необходимости на место выезжает наряд.

### Соблюдение скоростного режима на дороге

На дороге, проходящей через небольшой городок, было зафиксировано несколько случаев превышения скорости. Чтобы добиться соблюдения ограничения скорости в 70 км/ч, управление дорожного движения установило на мосту, который пересекает дорогу, охранный радар в режиме **Road monitoring profile (Профиль наблюдения за дорогой)**. Теперь они могут контролировать скорость движения транспортных средств и определять, когда вдоль дороги нужно расставить патрули для контроля движения.



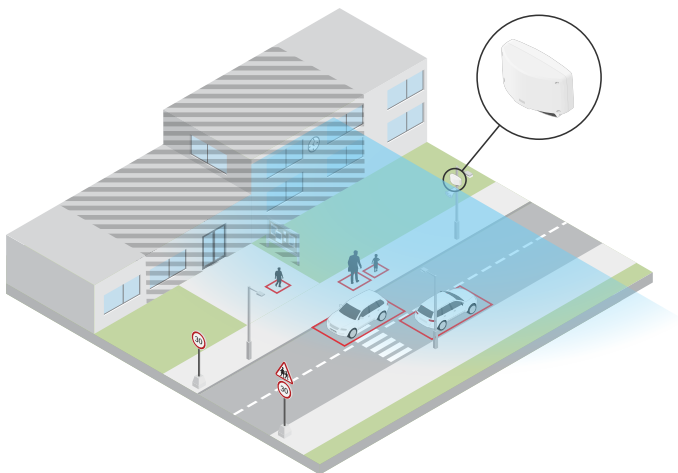
### Охрана территории и обеспечение дорожной безопасности

## AXIS D2110-VE Security Radar

### Профиль наблюдения за дорогой

---

Сотрудники школы выявили две проблемы безопасности, которые они хотели бы разрешить. Это проникновение посторонних лиц на территорию школы в течение учебного дня и движение автомобилей со скоростью выше максимально допустимой (20 км/ч) по дороге, расположенной рядом со школой. Радар устанавливается на столбе рядом с пешеходной дорожкой. Был выбран *Профиль наблюдения за областью на стр. 5*, поскольку в этом случае радар способен отслеживать как людей, так и транспортные средства, которые движутся со скоростью ниже 55 км/ч. Теперь сотрудники школы могут отслеживать людей, приходящих и уходящих в течение учебного дня, а также могут активировать громкоговоритель, чтобы предупреждать пешеходов, когда проезжающий автомобиль едет слишком быстро.



# AXIS D2110-VE Security Radar

## Начало работы

### Начало работы

#### Поиск устройства в сети

Для поиска устройств Axis в сети и назначения им IP-адресов в Windows® можно использовать приложение AXIS IP Utility или AXIS Device Manager. Оба эти приложения можно бесплатно скачать на странице [axis.com/support](http://axis.com/support).

Дополнительные сведения о поиске устройств и назначении IP-адресов см. в документе *How to assign an IP address and access your device (Как назначить IP-адрес и получить доступ к устройству)*.

#### Поддержка браузеров

Это устройство можно использовать со следующими браузерами:

	Chrome™	Firefox®	Edge™	Safari®
Windows®	Рекомендуется	Рекомендуется	✓	
macOS®	Рекомендуется	Рекомендуется	✓	✓
Linux®	Рекомендуется	Рекомендуется	✓	
Другие операционные системы	✓	✓	✓	✓*

\* Чтобы использовать веб-интерфейс AXIS OS с iOS 15 или iPadOS 15, перейдите к пункту **Settings > Safari > Advanced > Experimental Features (Настройки > Safari > Дополнительно > Экспериментальные функции)** и отключите *NSURLSession Websocket*.

#### Откройте веб-страницу устройства

1. Откройте браузер и введите IP-адрес или имя хоста устройства Axis.  
Если вы не знаете IP-адрес, используйте программу AXIS IP Utility или приложение AXIS Device Manager, чтобы найти устройство в сети.
2. Введите имя пользователя и пароль. Если доступ к устройству производится в первый раз, необходимо задать пароль для учетной записи root. См. *Установка нового пароля для учетной записи root* на стр. 12.

#### Установка нового пароля для учетной записи root

По умолчанию для учетной записи администратора используется имя пользователя root. Для учетной записи root пароль по умолчанию не установлен. Пароль задается при первом входе в устройство.

1. Введите пароль. Соблюдайте инструкции по созданию надежных паролей. См. *Безопасные пароли* на стр. 12.
2. Введите пароль еще раз для подтверждения.
3. Нажмите **Добавить пользователя**.

#### Важно!

Если вы потеряете пароль для учетной записи root, перейдите к разделу *Сброс к заводским установкам* на стр. 49 и следуйте инструкциям.

#### Безопасные пароли

#### Важно!

Устройства Axis передают первоначально установленный пароль по сети в текстовом виде. Чтобы защитить свое устройство, после первого входа в систему настройте безопасное зашифрованное HTTPS-соединение, а затем измените пароль.

# AXIS D2110-VE Security Radar

## Начало работы

---

Пароль устройства — это основное средство защиты ваших данных и сервисов. Для устройств Axis не предусмотрена собственная политика использования паролей, так как эти устройства могут входить в состав систем разного типа и назначения.

Для защиты данных мы настоятельно рекомендуем соблюдать указанные ниже правила.

- Используйте пароль длиной не менее 8 символов. Желательно создать пароль с помощью генератора паролей.
- Никому не сообщайте пароль.
- Периодически меняйте пароль — хотя бы раз в год.

## Обзор веб-страницы

В этом видеоролике представлены общие сведения об интерфейсе устройства.



Для просмотра видео откройте веб-версию данного документа.

[help.axis.com/?&pid=45364&section=webpage-overview](http://help.axis.com/?&pid=45364&section=webpage-overview)

*Веб-интерфейс устройства Axis*

# AXIS D2110-VE Security Radar

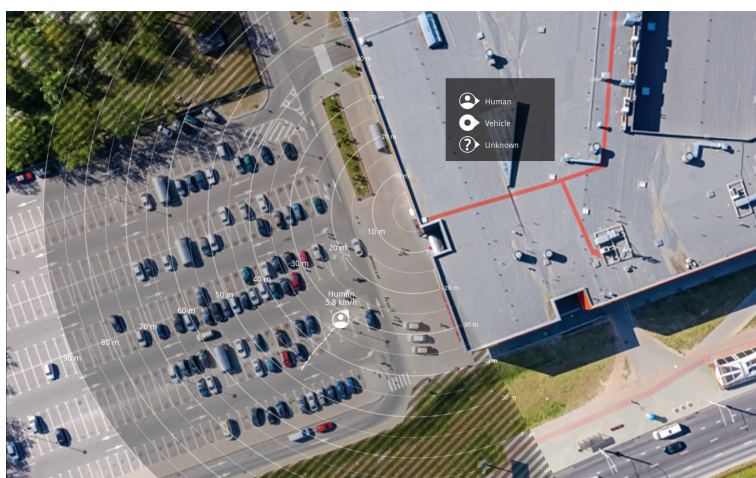
## Настройка устройства

### Настройка устройства

#### Калибровка радара

Радар готов к работе сразу после установки. В окне живого просмотра по умолчанию будут отображаться зона покрытия радара и любое обнаруженное движение. Вы сразу можете начать добавлять зоны обнаружения и правила действий.

Если радар установлен на высоте 3,5 м над землей, то больше ничего делать не нужно. Если радар установлен на другой высоте, его необходимо откалибровать, чтобы компенсировать отличие в высоте установки.



Чтобы оператору было проще определять местоположение движущихся объектов, можно загрузить карту объекта (например, план местности или аэрофотоснимок) с изображением зоны, охватываемой радаром.

Требования к изображению:

- Поддерживаются форматы JPEG и PNG.
- Изображение в радаре можно обрезать.
- Изображение в радаре можно повернуть на угол  $\pm 35^\circ$ .
- Ориентация не играет роли, так как форма охватываемой радаром области во время калибровки будет перемещаться, подстраиваясь под изображение.

После загрузки карты объекта ее нужно откалибровать, чтобы реальная область охвата радара точно совпала с этой областью на карте (по положению, направлению и масштабу).

Калибровка выполняется в веб-интерфейсе при щелчке по карте объекта. Вам не требуется физический доступ к объекту.

#### Калибровка радара

1. Для настройки радара перейдите в раздел **Settings > Radar > Calibration (Настройки > Радар > Калибровка)**, нажмите **Start (Пуск)** и следуйте инструкциям, приведенным в пошаговом руководстве.

#### О зонах обнаружения

Чтобы определить области, в которых должно обнаруживаться движение, можно добавить несколько зон обнаружения. В разных зонах можно инициировать разные действия.

Различают зоны двух типов:

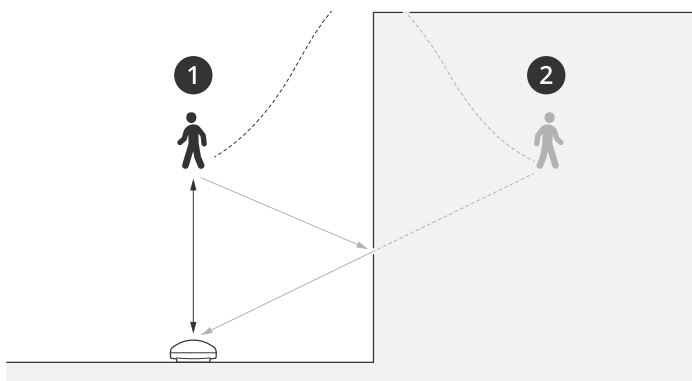
# AXIS D2110-VE Security Radar

## Настройка устройства

- **Include zone (Зона включения)** – это область, в которой движущиеся объекты будут активировать правила. Зона включения по умолчанию охватывает всю область, покрываемую радаром.
- **Exclude zone (Зона исключения)** – это область, в которой движущиеся объекты игнорируются. Используйте зоны исключения, если внутри зоны включения имеются области с большой частотой ложных тревог.

### Удаление ненужных отражений

Объекты из радиолокационно-отражающих материалов, такие как металлические крыши, ограждения, транспортные средства и даже кирпичные стены, могут нарушать работу радара. Они могут создавать отражения, вызывающие видимые обнаружения, которые может быть трудно отличить от реальных обнаружений.



- 1 Фактическое обнаружение
- 2 Обнаружение с отражением

Чтобы избежать нежелательных обнаружений, настройте зону исключения.

### Добавление зоны включения

1. Перейдите к пункту **Settings > RMD zones (Настройки > RMD-зоны)** и нажмите **+**.
2. Выберите **Include zone (Включить зону)**.
3. Выберите **⚙️**, чтобы изменить параметры зоны. Дополнительные сведения можно найти во встроенной справке устройства.
4. Измените форму зоны включения (см. *Изменение зоны обнаружения на стр. 16*).

### Изменение зоны включения

Выберите **⚙️**, чтобы изменить зону включения.

- Для настройки диапазона скорости, на который будет активироваться зона включения, выполните следующие действия:
  - В разделе **Trigger between (Включение между)** с помощью ползунков установите требуемый диапазон скорости. Устройство будет включаться при перемещении объекта со скоростью в пределах этого диапазона.
  - Нажмите кнопку **Invert (Обратить)**, чтобы устройство включалось, когда объект перемещается ниже и выше заданного диапазона скорости.
- Чтобы увидеть влияние изменения на зону включения:


# AXIS D2110-VE Security Radar

## Настройка устройства

---

- Щелкните Test alarm (Тестовый сигнал тревоги).

### Добавление зоны исключения



1. Перейдите к пункту Settings > RMD zones (Настройки > RMD-зоны) и нажмите .
2. Выберите Exclude zone (Исключить зону).
3. Измените форму зоны исключения (см. *Изменение зоны обнаружения на стр. 16*).

### Изменение зоны обнаружения

Перемещая зону и изменяя ее форму с помощью мыши, можно добиться, чтобы зона охватывала нужную часть карты объекта.

- Чтобы добавить вершину, щелкните границу зоны. Перетащите вершину в нужное положение.
- Чтобы удалить вершину, щелкните по ней правой кнопкой мыши.
- Чтобы переместить вершину, щелкните ее и перетащите в новое положение.
- Для перемещения зоны расположите указатель внутри нее и перетащите зону в новое положение.

### Добавление детектора пересечения линии

1. Перейдите к пункту Settings > RMD zones (Настройки > RMD-зоны) и нажмите .
2. Выберите Crossline detection (Детектор пересечения линии).
3. Изменение линии:
  - Чтобы переместить линию, щелкните по линии и перетащите ее.
  - Чтобы переместить точку, щелкните по точке и перетащите ее.
  - Чтобы добавить новую точку, щелкните по линии.
  - Чтобы удалить точку, щелкните по ней правой кнопкой мыши.
4. Чтобы изменить направление обнаружения и другие параметры, нажмите значок .

Дополнительные сведения можно найти во встроенной справке устройства.


## Просмотр и запись видео

В этом разделе приводятся инструкции по настройке устройства. Более подробную информацию о потоковой передаче и хранении видео см. в разделе .

### Уменьшение требуемой пропускной способности канала связи и требуемой емкости системы хранения

#### Важно!

Уменьшение требований к пропускной способности канала передачи требует снижения битрейта видеопотока, т. е. количества битов видеоданных, передаваемых за единицу времени. Уменьшение битрейта, однако, может приводить к потере деталей изображения.

1. Перейдите к пункту Video > Stream (Видео > Поток).
2. Нажмите значок  в режиме живого просмотра.



# AXIS D2110-VE Security Radar


## Настройка устройства

---

3. Выберите Video format (Формат видео) H.264.
4. Перейдите к пункту Video > Stream > General (Видео > Поток > Общие) и увеличьте Compression (Сжатие).
5. Перейдите к пункту Video > Stream > H.264 and H.265 encoding (Видео > Поток > Кодирование H.264 и H.265) и выполните одно или несколько следующих действий:
  - Выберите уровень Zipstream, который нужно использовать.
  - Включите параметр Dynamic FPS (Динамическая частота кадров).
  - Включите параметр Dynamic GOP (Динамическая регулировка параметра GOP) и задайте большое значение длины GOP в параметре Upper limit (Верхний предел).


### Настройка сетевого хранилища данных



Для хранения записей в сети необходимо настроить сетевой накопитель данных.


1. Перейдите к пункту System > Storage (Система > Хранилище).
2. Нажмите  Добавить сетевой накопитель в разделе Сетевой накопитель.
3. Введите IP-адрес сервера, содержащего устройство хранения.
4. Введите имя общего сетевого ресурса на сервере в разделе Network Share (Сетевой ресурс).
5. Введите имя пользователя и пароль.
6. Выберите версию протокола SMB или оставьте значение Auto (Автоматически).
7. Если подключение временно невозможно или сетевой ресурс еще не настроен, выберите флажок **Добавить ресурс**, даже если проверка соединения завершится сбоем.
8. Нажмите кнопку **Добавить**.

### Запись и просмотр видео

Запись видео непосредственно с камеры

1. Перейдите к пункту Video > Image (Видео > Изображение).
2. Чтобы начать запись, нажмите значок .

Если устройство хранения еще не настроено, нажмите  и . Инструкции по настройке сетевого накопителя см. в разделе *Настройка сетевого хранилища данных на стр. 17*

3. Чтобы остановить запись, нажмите значок  еще раз.

Просмотр видео

1. Перейдите к пункту Recordings (Записи).
2. Нажмите значок  для нужной записи в списке.

### Настройка правил для событий

Для получения более подробной информации ознакомьтесь с нашим руководством *Начало работы с правилами для событий*.

# AXIS D2110-VE Security Radar

## Настройка устройства

---

### Запуск действия

1. Перейдите в раздел **System > Events (Система > События)** и добавьте правило. Правило определяет, в какой момент устройство будет выполнять определенные действия. Правила можно настроить как запланированные, повторяющиеся или запускаемые вручную события.
2. Введите имя в поле **Name (Имя)**.
3. С помощью параметра **Condition (Условие)** выберите условие, которое должно выполняться для запуска действия. Если для одного правила задано несколько условий, действие запускается, только если соблюдаются все эти условия.
4. С помощью параметра **Action (Действие)** выберите действие, которое должно выполнить устройство при соблюдении условий.

#### Примечание.

Если в активное правило вносятся изменения, оно должно быть снова включено, чтобы изменения вступили в силу.

### Запуск сигнала тревоги при открытии корпуса

В этом примере объясняется, как сделать так, чтобы камера подавала сигнал тревоги, когда кто-то открывает ее корпус.

#### Добавьте получателя:

1. Перейдите к пункту **Система > События > Получатели** и нажмите **Добавить получателя**.
2. Введите имя получателя уведомления.
3. Выберите **Email (Электронная почта)**.
4. Введите адрес электронной почты получателя.
5. В камере нет собственного почтового сервера, поэтому для отправки сообщений по электронной почте она должна войти на другой сервер электронной почты. Введите данные вашего поставщика услуг электронной почты в остальных полях.
6. Для отправки проверочного письма нажмите **Test (Проверка)**.
7. Нажмите **Save (Сохранить)**.

#### Создайте правило:

8. Перейдите к пункту **Настройки > События > Правила** и добавьте правило.
9. Введите имя правила.
10. В списке условий выберите **Casing open (Вскрытие корпуса)**.
11. В списке действий выберите **Send notification to email (Отправить уведомление по электронной почте)**.
12. Выберите получателя из списка.
13. Введите тему и текст сообщения электронной почты.
14. Нажмите **Save (Сохранить)**.

## Инструкции

### Как записывать данные радара при обнаружении движения

В этом примере поясняется, как настроить радар так, чтобы он начинал запись на карту SD при обнаружении движения, захватив 5-секундный интервал, предшествующий моменту обнаружения движения, и прекращал запись через минуту.

Запись будет содержать карту (план этажа, карту территории и т. п.) с траекторией движения объекта.

# AXIS D2110-VE Security Radar

## Настройка устройства

---

Создайте правило:

1. Перейдите к пункту **Settings > System > Events** (Настройки > Система > События) и добавьте правило.
2. Введите имя правила.
3. В списке условий выберите зону включения в разделе **Radar motion** (Радарный детектор движения). Порядок настройки зоны включения см. в разделе *Добавление зоны включения на стр. 15*.
4. В списке действий выберите **Record video** (Запись видео).
5. Задайте время, предшествующее моменту обнаружения, равным 5 с.
6. Задайте время после момента обнаружения равным 60 с.
7. В списке вариантов устройств хранения выберите **SD card** (Карта SD).
8. Нажмите кнопку **Save** (Сохранить).

### Как записывать видео с камеры при обнаружении движения

В этом примере объясняется, как настроить радар и камеру так, чтобы камера начинала запись на карту SD при обнаружении радаром движения, захватив 5-секундный интервал, предшествующий моменту обнаружения движения, и прекращала запись через минуту.

Подключите устройства:

1. Соедините выходной порт ввода-вывода радара со входным портом ввода-вывода камеры с помощью кабеля.

Настройте порт ввода-вывода радара:

2. Перейдите к пункту **Settings > System > I/O ports** (Настройки > Система > Порты ввода-вывода), настройте порт ввода-вывода в качестве выхода и выберите нормальное состояние.

Создайте правило в радаре:

3. Перейдите к пункту **Settings > System > Events** (Настройки > Система > События) и добавьте правило.
4. Введите имя правила.
5. В списке условий выберите зону включения в разделе **Radar motion** (Радарный детектор движения). Порядок настройки зоны включения см. в разделе *Добавление зоны включения на стр. 15*.
6. В списке действий выберите **Toggle I/O while the rule is active** (Переключать ввод-вывод, пока правило активно), а затем выберите порт, подключенный к камере.
7. Нажмите кнопку **Save** (Сохранить).

Настройте порт ввода-вывода камеры:

8. Перейдите к пункту **Settings > System > I/O ports** (Настройки > Система > Порты ввода-вывода), настройте порт ввода-вывода в качестве входа и выберите нормальное состояние.

Создайте правило в камере:

9. Перейдите к пункту **Settings > System > Events** (Настройки > Система > События) и добавьте правило.
10. Введите имя правила.
11. В списке условий выберите **Digital Input** (Цифровой вход), а затем выберите порт, который должен запускать данное правило.
12. В списке действий выберите **Record video** (Запись видео).
13. Выберите существующий профиль потока или создайте новый.

# AXIS D2110-VE Security Radar

## Настройка устройства

---

14. Задайте время, предшествующее моменту обнаружения, равным 5 с.
15. Задайте время после момента обнаружения равным 60 с.
16. В списке вариантов устройств хранения выберите **SD card (Карта SD)**.
17. Нажмите кнопку **Save (Сохранить)**.

### Как настроить включение освещения при обнаружении движения

Включение света при проникновении нарушителя в зону обнаружения может иметь отпугивающий эффект, а также повысит качество видеозаписи, создаваемой с помощью оптической камеры.

В этом примере объясняется, как настроить радар и осветитель так, чтобы осветитель включался, когда радар обнаруживает движение, и выключался через одну минуту.

Подключите устройства:

1. Подсоедините один из кабелей осветителя к источнику питания через порт реле радара. Другой кабель осветителя подсоедините непосредственно к источнику питания.

Настройте порт реле радара:

2. Перейдите к пункту **Settings > System > I/O ports (Настройки > Система > Порты ввода-вывода)** и выберите **Open circuit (Разомкнутая цепь)** в качестве нормального состояния.

Создайте правило в радаре:

3. Перейдите к пункту **Settings > System > Events (Настройки > Система > События)** и добавьте правило.
4. Введите имя правила.
5. В списке триггеров выберите зону включения в разделе **Radar motion (Радарный детектор движения)**. Порядок настройки зоны включения см. в разделе *Добавление зоны включения на стр. 15*.
6. В списке условий выберите **Toggle I/O once (Переключить вход-выход один раз)**, а затем выберите порт реле.
7. Выберите **Active (Активный)**.
8. Задайте продолжительность с помощью параметра **Duration (Длительность)**.
9. Нажмите кнопку **Save (Сохранить)**.

### Как управлять PTZ-камерой с помощью радара

Информацию о положениях объектов, получаемую от радара, можно использовать для отслеживания этих объектов с помощью PTZ-камеры.

Это можно сделать двумя способами:

- Используйте встроенную функцию **Radar autotracking (Автоматическое слежение с использованием радара)**. Используйте этот параметр, если у вас есть одна PTZ-камера и один радар, смонтированные очень близко друг к другу. При выборе этого параметра создается комплексное решение, в котором радар непосредственно управляет камерой.
  1. Перейдите в меню **Settings > System > Radar autotracking (Настройки > Система > Автоматическое слежение с использованием радара)**.
  2. Введите IP-адрес, имя пользователя и пароль для PTZ-камеры.
  3. Нажмите **Connect (Подключиться)** и следуйте инструкциям.

# AXIS D2110-VE Security Radar

## Настройка устройства

---

### Примечание.

Камера должна быть установлена непосредственно над радаром или под ним.

Это приложение не использует зоны включения в радаре. Оно использует для обнаружения движения всю охватываемую радаром территорию, кроме зон исключения.

- Если нужно использовать несколько камер с несколькими радаром, воспользуйтесь приложением **AXIS Radar Autotracking for PTZ для Windows®**. Скачайте приложение AXIS Radar Autotracking for PTZ с веб-сайта [axis.com](http://axis.com) и установите его на своем сервере с ПО для управления видеонаблюдением (или на другом компьютере, имеющем доступ к камере и радару), следуя инструкциям в приложении.

Это серверное решение, которое подходит для разных конфигураций системы:

- Управление несколькими PTZ-камерами с помощью одной радара.
- Управление одной PTZ-камерой с помощью нескольких радаров.
- Управление несколькими PTZ-камерами с помощью нескольких радаров.
- Управление одной PTZ-камерой с помощью одного радара, если они установлены в разных положениях, охватывающих одну и ту же область.

### Как минимизировать частоту ложных тревог

Если ложные тревоги возникают слишком часто, можно отфильтровать некоторые типы движения или объекты, изменить область покрытия или отрегулировать чувствительность обнаружения. Опытным путем определите настройки, которые дают наилучшие результаты в ваших условиях.

- Регулировка чувствительности обнаружения:

Перейдите к пункту **Settings > Radar > Detection (Настройки > Радар > Обнаружение)** и выберите более низкую чувствительность с помощью параметра **Detection sensitivity (Чувствительность обнаружения)**. Это снизит риск ложных тревог, но может привести к тому, что радар не будет реагировать на некоторые движущиеся объекты. Настройка чувствительности влияет на все зоны.

- **Low (Низкий)**. Используйте это значение чувствительности, если в зоне много металлических объектов или крупных автомобилей. Для слежения за объектами и их классификации объектов может потребоваться больше времени. Это может привести к сокращению диапазона обнаружения, особенно для быстро движущихся объектов.
- **High (Высокий)**. Используйте это значение чувствительности при наличии открытой территории без металлических объектов перед радаром. Это приведет к увеличению диапазона обнаружения людей.

- Измените зоны включения и исключения:

Если в зоне включения присутствуют твердые поверхности, например металлическая стена, то вследствие отражений может многократно обнаруживаться один и тот же физический объект. В этом случае измените зону включения (см. *Изменение зоны обнаружения на стр. 16*) или добавьте зону исключения, маскирующую все, что находится позади поверхности (см. *Добавление зоны исключения на стр. 16*).

- Отфильтруйте некоторые виды движения:

Перейдите к пункту **Settings > Radar > Detection (Настройки > Радар > Обнаружение)** и выберите **Ignore swaying objects (Игнорировать качающиеся объекты)**. Этот параметр позволяет минимизировать количество ложных тревог, вызываемых движением веток деревьев, кустов и флагов в зоне покрытия.

- Примените фильтрацию по времени:

Перейдите к пункту **Settings > RMD zones (Настройки > RMD-зоны)** и выберите зону, параметры которой нужно изменить.

Активируйте параметр **Short-lived object (Кратковременно существующий на изображении объект)** и задайте время задержки, по истечении которого радар будет сигнализировать тревогу после начала отслеживания объекта.

# AXIS D2110-VE Security Radar

## Настройка устройства

---

Отсчет времени начинается с момента обнаружения объекта радаром, а не с момента входа объекта в зону наблюдения, указанную параметром «Include zone» (Включить зону).

- Отфильтруйте объекты некоторых типов:

Радар классифицирует каждый объект по характеристикам отражения («эха») от этого объекта. Если он не может определить тип объекта, то объект классифицируется как **Unknown (Неизвестный)**.

Перейдите к пункту **Settings > RMD zones (Настройки > RMD-зоны)** и выберите зону, параметры которой нужно изменить.

Чтобы детектор не срабатывал при обнаружении объектов определенного типа, включите фильтр и исключите типы объектов, которые не должны инициировать события в данной зоне.

# AXIS D2110-VE Security Radar

## Проверьте установку

---

### Проверьте установку

#### Проверка установки радара

##### Примечание.

Этот тест помогает проверить правильность установки, выполненной в текущих условиях. На повседневную эффективность установки могут повлиять изменения в сцене.

Радар готов к использованию сразу после установки, однако перед началом работы с ним рекомендуется выполнить соответствующую проверку. Это может повысить точность радара и поможет выявить любые проблемы, связанные с установкой или наличием мешающих объектов в сцене (деревья, отражающие поверхности и т. п.).

Перед началом проверки в первую очередь выполните *Калибровка радара на стр. 14*.

Проверку рекомендуется выполнять в следующих случаях:

- В сцене имеются объекты, которые вы хотите исключить, чтобы соответствующие зоны могли содержать определенные объекты, такие как качающиеся ветки или металлические поверхности.
- Вы объединяете радар с PTZ-камерой и хотите настроить функцию **Radar autotracking** (Автоматическое слежение с использованием радара).
- Изменилась высота установки радара.

#### Проверка радара

##### Проверьте отсутствие ложных обнаружений

1. Убедитесь в том, что зона включения радара закрыта от человеческих действий.
2. Подождите несколько минут, чтобы убедиться, что радар не обнаруживает каких-либо статических объектов в зонах с включенным радарным детектором движения (RMD).
3. Если нежелательных обнаружений нет, можно пропустить шаг 4.
4. Если имеются нежелательные обнаружения, узнайте, как выполняется фильтрация определенных типов движений или объектов, изменение покрытия или регулировка чувствительности детектора в разделе *Как минимизировать частоту ложных тревог на стр. 21*.

##### Проверка правильности символа и направления перемещения при приближении к радару спереди

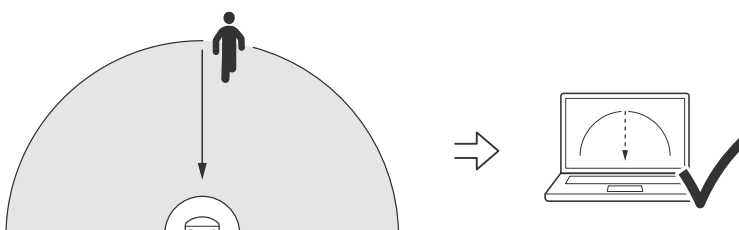
1. Перейдите в веб-интерфейс радара и выберите запись сеанса. Для получения справки по этим действиям перейдите в раздел *Запись и просмотр видео на стр. 17*.
2. Начинайте с расстояния 60 м перед радаром и продвигайтесь прямо по направлению к радару.
3. Проверьте сеанс в веб-интерфейсе радара. Символ для классификации человека должен появиться, когда вы будете обнаружены.

# AXIS D2110-VE Security Radar

## Проверьте установку

---

4. Убедитесь в том, что веб-интерфейс радара отображает правильное направление перемещения.



### Проверка правильности символа и направления перемещения при пересечении зоны радара

1. Перейдите в веб-интерфейс радара и выберите запись сеанса. Для получения справки по этим действиям перейдите в раздел *Запись и просмотр видео на стр. 17*.
2. Начните с расстояния 60 м от радара и продвигайтесь прямо через зону радара.
3. Убедитесь в том, что веб-интерфейс радара отображает символ для классификации человека.

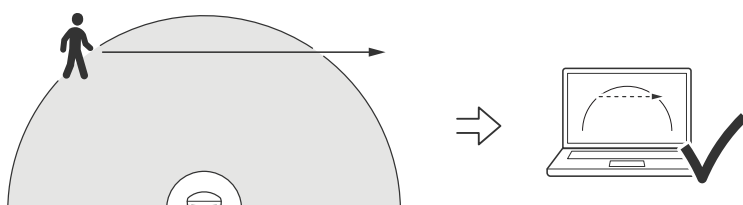


# AXIS D2110-VE Security Radar

## Проверьте установку

---

4. Убедитесь в том, что веб-интерфейс радара отображает правильное направление перемещения.



Создайте таблицу, подобную приведенной ниже, чтобы сохранить данные проверки.

Тест	Успех/неудача	Комментарий
1. Проверка отсутствия нежелательных обнаружений, когда зона является чистой		
2а. Проверьте, что обнаружен объект с правильным символом для «человека» при приближении к радару спереди		

# AXIS D2110-VE Security Radar

## Проверьте установку

---

2b. Проверьте, что направление перемещения является правильным при приближении к радару спереди		
3a. Проверьте, что объект обнаружен с правильным символом для «человека» при пересечении зоны радара		
3b. Проверьте, что направление перемещения является правильным при пересечении зоны радара		

### Завершение проверки

После завершения первой части проверки необходимо выполнить следующие тесты для завершения процесса проверки.

1. Убедитесь, что вы правильно настроили радар и следовали инструкциям.
2. Для дальнейшей проверки *Калибровка радара на стр. 14*.
3. Задайте для радара зону для включения для триггера при обнаружении соответствующего объекта. По умолчанию буфер перед тревогой установлен в две секунды, но при необходимости его величину можно изменить в веб-интерфейсе.
4. Задайте, чтобы радар *Как записывать данные радара при обнаружении движения на стр. 18* при обнаружении соответствующего объекта.
5. Задайте продолжительность следа равной одному часу, чтобы она наверняка превышала время, которое уйдет на то, что вы покинете свое местоположение, обойдете область охранного видеонаблюдения, а затем вернитесь в исходное местоположение. Продолжительность следа позволит в течение заданного времени выполнять слежение в режиме живого просмотра радара; после окончания проверки этот режим можно отключить.
6. Пройдите по границе области покрытия радара и убедитесь, что отслеживание, выполненное в системе, соответствует маршруту, по которому вы прошли.
7. Если результаты проверки являются неудовлетворительными, необходимо выполнить повторную калибровку карты объекта и повторить проверку.

# AXIS D2110-VE Security Radar















## Интерфейс устройства

### Интерфейс устройства

Чтобы перейти к интерфейсу устройства, введите IP-адрес устройства в веб-браузере.

#### Примечание.

Поддержка функций и параметров, описанных в данном разделе, зависит от конкретного устройства.

-  Показать или скрыть основное меню.
-  Доступ к справке по продукту.
-  Изменить язык.
-  Установка светлой или темной темы.
-  Меню пользователя содержит:
  -  Информацию о пользователе, который вошел в систему.
  -  Изменить пользователя : Выход текущего пользователя и вход в систему нового пользователя.
  -  Выход: Выход текущего пользователя.
-  Контекстное меню содержит следующие команды:
  -  **Analytics data (Данные аналитики)**. Нажмите «Принять», чтобы разрешить передачу неперсональных данных просмотра веб-страниц.
  -  **Feedback (Обратная связь)**. Отправка отзывов, которые помогут нам повысить удобство работы пользователей.
  -  **Legal (Юридическая информация)**. Просмотр информации о файлах cookie и лицензиях.
  -  **About (О системе)**. Просмотр информации об устройстве, включая версию встроенного ПО и серийный номер.
  -  **Старый интерфейс устройства**: Измените интерфейс устройства на старый интерфейс устройства.

### Состояние

#### Синхронизация по NTP

Отображение информации о синхронизации по протоколу NTP, в том числе о том, синхронизировано ли устройство с NTP-сервером, и о том, сколько времени осталось до следующей синхронизации.

**NTP settings (Параметры NTP)**. Нажмите для перехода на страницу **Date and time (Дата и время)**, где можно изменить параметры NTP.

#### Информация об устройстве

Отображение информации об устройстве, включая его серийный номер и версию встроенного ПО.

**Upgrade firmware (Обновить встроенное ПО)**. Нажмите для перехода на страницу **Maintenance (Обслуживание)**, где можно выполнить обновление встроенного ПО.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

### Видео



Нажмите для воспроизведения живого видеопотока.



Нажмите для постановки воспроизведения живого видеопотока на паузу.



Нажмите для создания стоп-кадра живого видеопотока. Файл изображения сохраняется в папку Downloads (Загрузки) на компьютере под именем [snapshot\_ГГГГ\_ММ\_ДД\_ЧЧ\_ММ\_СС.jpg]. Фактический размер файла стоп-кадра зависит от механизма сжатия, применяемого в конкретном веб-браузере, с помощью которого создается стоп-кадр, поэтому он может не соответствовать настройкам сжатия в устройстве.



Нажмите для отображения выходных портов ввода-вывода. Используйте переключатель для размыкания или замыкания цепи порта, например, чтобы проверить работу внешних устройств.



Нажмите, чтобы вручную включить или выключить ИК-подсветку.



Щелкните, чтобы получить доступ к экранным элементам управления:

- **Predefined controls (Предустановленные элементы управления):** Включите этот параметр, чтобы можно было использовать доступные на экране элементы управления.
- **Custom controls (Пользовательские элементы управления):** Нажмите элемент управления, чтобы добавить экранный элемент управления. **+** Добавить пользовательский



Нажмите, чтобы вручную включить обогреватель на выбранный период времени.



Нажмите, чтобы начать непрерывную запись живого видеопотока. Чтобы остановить запись, нажмите еще раз. Если ведется запись, она автоматически возобновляется после перезагрузки.



Нажмите для отображения хранилища, настроенного для устройства. Для настройки хранилища необходимо войти в систему в качестве администратора.







Нажмите для доступа к дополнительным параметрам:


- **Video format (Формат видео).** Выберите формат кодирования видео, используемый для живого просмотра. В случае выбора формата со сжатием видео возрастут нагрузка на процессор и расходование памяти.
- **Client stream information (Информация о потоке клиента).** Включите для отображения динамической информации о видеопотоке, используемом браузером, в котором отображается живой видеопоток. Информация о битрейте отличается от информации, отображаемой в текстовом наложении, так как используются разные источники информации. В информации о потоке клиента отображается значение битрейта за последнюю секунду, которое поступает от кодека, работающего в устройстве. В накладываемом тексте отображается среднее значение битрейта за последние 5 секунд, и это значение поступает от веб-браузера. Оба значения учитывают только сам видеопоток и не учитывают служебную информацию, добавляемую при передаче видеопотока по сети по протоколу UDP/TCP/HTTP и создающую дополнительную нагрузку на сеть.
- **Adaptive stream (Адаптивный поток).** Включите эту функцию, если нужно, чтобы разрешение изображения подстраивалось под фактическое разрешение дисплея клиента. Это сделает работу пользователя более удобной и предотвратит возможную перегрузку оборудования клиента. Адаптивный поток применяется только при просмотре живого видеопотока в веб-интерфейсе в браузере. Когда включен адаптивный поток, частота кадров не может быть больше 30 кадров/с. Для стоп-кадра, создаваемого при включенном адаптивном потоке, используется разрешение изображения, выбранное адаптивным потоком.

# AXIS D2110-VE Security Radar


## Интерфейс устройства


- **Level grid (Сетка уровня).** Для отображения сетки уровня нажмите значок . Сетка помогает точнее определить, выровнено ли изображение по горизонтали. Чтобы скрыть сетку, нажмите значок .
- **Счетчик пикселей:** Нажмите , чтобы показать счетчик пикселей. Перетащите и измените размер отображаемой зоны так, чтобы она включала нужную область. Можно также задать размер отображаемой зоны в пикселях, указав нужные значения в полях **Width (Ширина)** и **Height (Высота)**.
- **Refresh (Обновить).** Чтобы обновить неподвижное изображение в режиме живого просмотра, нажмите значок .

**1:1** Нажмите для просмотра живого видео с максимальным разрешением. Если максимальное разрешение больше разрешения экрана, используйте изображение меньшего размера для навигации по изображению.

 Нажмите для просмотра живого видеопотока в полноэкранном режиме. Нажмите клавишу ESC для выхода из полноэкранного режима.

### Установка

**Capture mode (Режим съемки)**  : Режим съемки — это предустановленная конфигурация, определяющая, как камера создает изображения. Изменение режима съемки может повлиять на множество других параметров, таких как зоны просмотра и маски закрытых зон.




**Mounting position (Положение установки)**  : Ориентация изображения может меняться в зависимости от того, как установлена камера.

**Power line frequency (Частота электросети).** Выберите частоту электросети, которая используется в вашем регионе, чтобы минимизировать мерцание изображения. В Америке используется частота 60 Гц. В большинстве остальных стран мира используется частота 50 Гц. Если вы точно не знаете, какая частота электросети используется в вашем регионе, обратитесь в соответствующие местные органы.

### Наложения



**+** : Нажмите, чтобы добавить накладку. Выберите тип наклейки из раскрывающегося списка:

- **Text (Текст).** Выберите этот вариант для отображения текста: текст встраивается в живое изображение, а также виден на всех видах, записях и стоп-кадрах. Можно ввести собственный текст, а также включить предварительно настроенные модификаторы для автоматического отображения информации, такой как время, дата и частота кадров.

-  : Нажмите, если нужно добавить модификатор даты %F для отображения даты в формате гggg-мм-дд.
-  : Нажмите, если нужно добавить модификатор времени %X для отображения времени в 24-часовом формате чч:мм:сс.
- **Модификаторы:** Нажмите, если нужно выбрать любой из модификаторов, отображаемых в списке, и добавить его в текстовое поле. Например, модификатор %a показывает день недели.
- **Size (Размер).** Выберите нужный размер шрифта.
- **Appearance (Вид изображения).** Выберите цвет текста и фоновый цвет, например белый текст на черном фоне (по умолчанию).
-  : Выберите положение наклейки на изображении.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

- **Image (Изображение).** Выберите этот вариант, если поверх видео должно отображаться статическое изображение. Можно использовать файлы с расширением BMP, PNG, JPEG или SVG. Чтобы загрузить изображение, нажмите **Images (Изображения)**. Перед загрузкой изображения можно выбрать следующее:
  - **Scale with resolution (Сохранение пропорций разрешения).** Выберите этот параметр, если нужно, чтобы масштаб накладываемого изображения автоматически приводился в соответствие с разрешением видео.
  - **Use transparency (Использовать прозрачность).** Выберите этот параметр и введите шестнадцатеричное значение RGB для данного цвета. Используйте формат RRGGBB. Примеры шестнадцатеричных значений: FFFFFFFF для белого цвета, 000000 для черного цвета, FF0000 для красного цвета, 6633FF для синего цвета и 669900 для зеленого цвета. Это возможно только для изображений в формате BMP.
- **Streaming indicator (Индикатор потоковой передачи)** . Выберите этот вариант, если поверх видео должна отображаться анимация. Даже если изображение будет статичным из-за отсутствия движения в сцене, анимация будет показывать, что передается живой видеопоток.
  - **Appearance (Вид изображения).** Выберите цвет анимации и фоновый цвет, например красная анимация на прозрачном фоне (по умолчанию).
  - **Size (Размер).** Выберите нужный размер шрифта.
  -  : Выберите положение наклейки на изображении.


## Записи



Нажмите, чтобы отфильтровать записи.

**From (После).** Показать записи, сделанные после определенного момента времени.

**To (До).** Показать записи, сделанные до определенного момента времени.

**Source (Источник)** . Показать записи в привязке к источнику видео.

**Event (Событие).** Показать записи в привязке к событиям.

**Storage (Хранилище).** Показать записи в привязке к типу устройства хранения.



Нажмите для воспроизведения записи.



Нажмите, чтобы остановить запись.



Нажмите для отображения дополнительной информации и параметров записи.

**Set export range (Установить диапазон экспорта).** Если нужно экспортировать только часть записи, укажите время начала и конца этого фрагмента.



Нажмите, чтобы удалить запись.

**Export (Экспорт).** Нажмите, чтобы экспортировать запись (или ее часть).


### Приложения

**Добавить приложение:** Нажмите, чтобы установить новое приложение.

**Find more apps (Найти другие приложения):** Нажмите, чтобы перейти на страницу обзора приложений Axis.



Контекстное меню содержит следующие команды:

- **App log (Журнал приложений).** Нажмите, чтобы просмотреть журнал событий приложения. Журнал полезен при обращении в службу поддержки.
- **Activate license with a key (Активировать лицензию ключом).** Если приложению требуется лицензия, необходимо активировать ее. Используйте этот параметр, если у устройства нет доступа к Интернету. Если у вас нет лицензионного ключа, перейдите по адресу [axis.com/applications](http://axis.com/applications). Для формирования лицензионного ключа потребуется код лицензии и серийный номер устройства Axis.
- **Activate license automatically (Активировать лицензию автоматически).** Если приложению требуется лицензия, необходимо активировать ее. Используйте этот параметр, если у устройства есть доступ в Интернет. Для активации лицензии необходимо иметь лицензионный ключ.
- **Deactivate the license (Деактивация лицензии).** Деактивируйте лицензию, чтобы использовать ее на другом устройстве. Деактивация лицензии означает ее удаление с этого устройства. Для деактивации лицензии требуется доступ в Интернет.
- **Settings (Настройки)**  : Настройте параметры.
- **Delete (Удалить).** Удалите приложение с устройства навсегда. Если сначала не деактивировать лицензию, она останется активной.

**Примечание.**

Производительность устройства может снизиться при одновременном запуске нескольких приложений.

**Start (Пуск).** Запустить или остановить приложение.

**Open (Открыть).** Нажмите, чтобы получить доступ к настройкам приложения. Доступные настройки зависят от типа приложения. В некоторых приложениях нет раздела настроек.

### Система

#### Дата и время

Формат времени зависит от языковых настроек веб-браузера.

**Примечание.**

Рекомендуется синхронизировать дату и время устройства с NTP-сервером.

**Synchronization (Синхронизация).** Выберите способ синхронизации даты и времени устройства.

- **Automatic date and time (manual NTS KE servers) (Автоопределение даты и времени (вручную для серверов NTS KE)).** Синхронизируйте с надежными NTP-серверами установки ключа, подключенными к DHCP-серверу.
  - **Manual NTS KE servers (Вручную для серверов NTS KE).** Введите IP-адрес одного или двух NTP-серверов. При использовании двух NTP-серверов устройство синхронизирует и подстраивает свое время на основании вводимых данных на обоих серверах.
- **Automatic date and time (NTP servers using DHCP) (Автоопределение даты и времени (NTP-серверы, использующие DHCP)).** Синхронизация с NTP-серверами, подключенными к серверу DHCP.
  - **Fallback NTP servers (Резервные NTP-серверы).** Введите IP-адрес одного или двух резервных серверов.
- **Automatic date and time (manual NTP server) (Автоопределение даты и времени (через NTP-серверы вручную)).** Синхронизация с выбранным вами NTP-сервером.
  - **Manual NTP servers (Через NTP-серверы вручную).** Введите IP-адрес одного или двух NTP-серверов. При использовании двух NTP-серверов устройство синхронизирует и подстраивает свое время на основании вводимых данных на обоих серверах.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

- **Custom date and time (Пользовательская настройка даты и времени).** Установка даты и времени вручную. Нажмите **Get from system (Получить из системы)**, чтобы однократно получить настройки даты и времени с вашего компьютера или мобильного устройства.
- Time zone (Часовой пояс).** Выберите часовой пояс, который будет использоваться. Время будет автоматически корректироваться с учетом летнего времени и зимнего времени.

**Примечание.**

Система использует настройки даты и времени во всех записях, журналах и системных параметрах.

### Сеть

#### IPv4

**Assign IPv4 automatically (Назначить IPv4 автоматически).** Выберите этот пункт, чтобы сетевой маршрутизатор автоматически назначил IP-адрес устройству. Рекомендуется автоматическое назначение IP-адреса (DHCP) для большинства сетей.

**IP address (IP-адрес).** Укажите уникальный IP-адрес устройства. В изолированных сетях можно случайным образом назначать статические IP-адреса при условии, что каждый адрес является уникальным. Во избежание конфликтов настоятельно рекомендуется обратиться к администратору сети, прежде чем назначить статический IP-адрес.

**Маска подсети:** Введите маску подсети, чтобы определить, какие адреса входят в локальную сеть. Любой адрес за пределами локальной сети проходит через маршрутизатор.

**Router (Маршрутизатор).** Укажите IP-адрес маршрутизатора (шлюза), который по умолчанию используется для подключения устройств, находящихся в разных сетях и разных сегментах сети.

#### IPv6

**Assign IPv6 automatically (Назначить IPv6 автоматически).** Выберите этот пункт для включения протокола IPv6, чтобы сетевой маршрутизатор автоматически назначил IP-адрес устройству.

#### Hostname (Имя хоста)

**Assign hostname automatically (Назначить имя хоста автоматически).** Выберите этот пункт, чтобы сетевой маршрутизатор мог автоматически назначать имя хоста устройству.

**Hostname (Имя хоста).** Введите имя хоста вручную, чтобы использовать его в качестве альтернативного способа доступа к устройству. Имя хоста используется в отчете сервера и в системном журнале. Допустимые символы: A-Z, a-z, цифры 0-9 и «-».

#### DNS-серверы

**Assign DNS automatically (Назначить DNS автоматически).** Выберите этот пункт, чтобы сетевой маршрутизатор мог автоматически назначить домены поиска и адреса DNS-серверов для устройства. Рекомендуется автоматическое назначение DNS (DHCP) для большинства сетей.

**Search domains (Поиск по доменам).** При использовании неполного имени хоста нажмите **Add search domain (Добавить поисковый домен)** и введите домен, в котором будет осуществляться поиск имени хоста, используемого устройством.

**DNS-серверы.** Нажмите **Add DNS server (Добавить DNS-сервер)** и введите IP-адрес DNS-сервера. Этот сервер обеспечивает преобразование имен хостов в IP-адреса в вашей сети.

#### HTTP and HTTPS (HTTP и HTTPS).



# AXIS D2110-VE Security Radar

## Интерфейс устройства

**Allow access through (Разрешить доступ через).** Выберите этот вариант, если пользователю разрешено подключаться к устройству через HTTP, HTTPS или оба протокола HTTP and HTTPS (HTTP и HTTPS).

HTTPS – это протокол, обеспечивающий шифрование запросов страниц от пользователей и страниц, возвращаемых веб-сервером. Обмен зашифрованной информацией регулируется использованием сертификатов HTTPS, которые гарантируют надежность и безопасность сервера.

Чтобы на устройстве можно было использовать протокол HTTPS, необходимо установить сертификат HTTPS. Для создания и установки сертификатов перейдите в меню **System > Security (Система > Безопасность)**.

**Примечание.**

При просмотре зашифрованных веб-страниц по протоколу HTTPS возможно снижение производительности, особенно если вы запрашиваете страницу в первый раз.

**HTTP port (Порт HTTP).** Введите номер HTTP-порта, который будет использоваться. Допустимыми вариантами являются порт 80 или любой порт в диапазоне 1024–65535. Если вы вошли в систему от имени администратора, можете ввести любой порт в диапазоне 1–1023. Если используете порт в этом диапазоне, вы получите предупреждение.

**HTTPS port (Порт HTTPS).** Введите номер HTTPS-порта, который будет использоваться. Допустимыми вариантами являются порт 443 или любой порт в диапазоне 1024–65535. Если вы вошли в систему от имени администратора, можете ввести любой порт в диапазоне 1–1023. Если используете порт в этом диапазоне, вы получите предупреждение.

**Certificate (Сертификат).** Выберите сертификат, чтобы включить протокол HTTPS для данного устройства.

### Friendly name (Понятное имя)

**Bonjour®.** Включите этот параметр, чтобы разрешить автоматическое обнаружение в сети.

**Bonjour name (Имя для протокола Bonjour).** Введите понятное имя, которое будет отображаться в сети. Имя по умолчанию включает в себя название и MAC-адрес устройства.

**Use UPnP® (Использовать UPnP®).** Включите этот параметр, чтобы разрешить автоматическое обнаружение в сети.

**UPnP name (Имя в службе UPnP).** Введите понятное имя, которое будет отображаться в сети. Имя по умолчанию включает в себя название и MAC-адрес устройства.

### One-click cloud connection (Подключение к облаку одним щелчком)

Подключение к облаку в одно нажатие (ОЗС) совместно с сервисом ОЗС обеспечивает простой и безопасный доступ через Интернет к живому и записанному видео отовсюду, где бы вы ни находились. Дополнительные сведения см. на странице [axis.com/end-to-end-solutions/hosted-services](http://axis.com/end-to-end-solutions/hosted-services).

#### Allow ОЗС (Разрешить ОЗС):

- **One-click (Одно нажатие).** Значение по умолчанию. Нажмите и удерживайте нажатой кнопку управления, чтобы подключиться к службе ОЗС через Интернет. После нажатия кнопки управления необходимо зарегистрировать устройство в службе ОЗС в течение 24 часов. В противном случае, устройство будет отключено от службы ОЗС. После регистрации будет активирован параметр **Always (Всегда)** и устройство будет постоянно подключено к службе ОЗС.
- **Always (Всегда).** Устройство будет постоянно пытаться подключиться к службе ОЗС через Интернет. После регистрации устройство будет постоянно подключено к службе ОЗС. Используйте этот вариант, если кнопка управления находится вне досягаемости.
- **No (Нет).** Отключает службу ОЗС.

**Proxy settings (Настройки прокси-сервера):** Если требуется, задайте параметры прокси-сервера для подключения к серверу HTTP.

**Host (Хост).** Укажите адрес прокси-сервера.

**Port (Порт).** Введите номер порта, используемого для получения доступа.

**Login (Логин) и Password (Пароль).** При необходимости введите имя пользователя и пароль для прокси-сервера.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

Authentication method (Способ проверки подлинности).

- **Basic (Базовая).** Этот способ является самой совместимой схемой проверки подлинности для протокола HTTP. Метод **Digest (Дайджест-авторизация)** безопаснее, так как в данном случае имя пользователя и пароль передаются серверу без шифрования.
- **Digest (Дайджест-авторизация).** Этот способ является более безопасным, так как при его использовании пароль всегда передается по сети в зашифрованном виде.
- **Auto (Автоматически)** Этот вариант позволяет устройству выбирать способ проверки подлинности автоматически в зависимости от поддерживаемого способа. Приоритет отдается способу **Digest (Дайджест-авторизация)**, а не **Basic (Базовая)**.

**Owner authentication key (OAK) (Ключ аутентификации владельца (OAK)):** Нажмите **Get key (Получить ключ)**, чтобы получить ключ авторизации владельца. Это возможно только в том случае, если устройство подключено к Интернету без межсетевого экрана или прокси-сервера.

### SNMP

Протокол SNMP (Simple Network Management Protocol) позволяет осуществлять удаленное управление сетевыми устройствами.

**SNMP:** Выберите версию SNMP для использования.

- **v1 and v2c (v1 и v2c).**
  - **Read community (Сообщество для чтения).** Укажите имя сообщества с уровнем доступа только для чтения ко всем поддерживаемым объектам SNMP. Значение по умолчанию: **public**.
  - **Write community (Сообщество для записи).** Укажите имя сообщества с уровнем доступа для чтения и записи ко всем поддерживаемым объектам SNMP (кроме объектов, доступных только для чтения). Значение по умолчанию: **write**.
  - **Activate traps (Активировать ловушки).** Включите данный параметр, чтобы активировать отчеты по ловушкам. Ловушки используются устройством для отправки сообщений системе управления при важных событиях или изменениях состояния. В интерфейсе устройства можно настроить ловушки для протоколов SNMP v1 и v2c. Ловушки автоматически отключаются, если вы перейдете на SNMP v3 или отключите SNMP. При использовании протокола SNMP v3 ловушки нужно настраивать с помощью приложения управления SNMP v3.
  - **Адрес ловушки.** Укажите адрес или имя хоста, присвоенные серверу управления.
  - **Trap community (Сообщество ловушки).** Укажите сообщество, которое будет использоваться при отправке устройством сообщения ловушки в систему управления.
  - **Traps (Ловушки):**
    - **Cold start (Холодный запуск).** При запуске устройства отправляется сообщение ловушки.
    - **Warm start (Горячий запуск).** При изменении настроек SNMP отправляется сообщение ловушки.
    - **Link up (Соединение установлено).** Отправка сообщения ловушки при изменении статуса «соединение не установлено» на «соединение установлено».
    - **Authentication failed (Проверка подлинности не пройдена).** Отправка сообщения ловушки при неудачной попытке авторизации.

#### Примечание.

Все ловушки AXIS Video MIB включаются при включении ловушек SNMP v1 и v2c. Дополнительные сведения см. в разделе *Axis OS Portal > SNMP*.

- **v3: SNMP v3** — это более надежная версия протокола, обеспечивающая шифрование и надежные пароли. Для использования протокола SNMP v3 рекомендуется активировать протокол HTTPS, чтобы использовать HTTPS для передачи пароля. Это также поможет предотвратить несанкционированный доступ к незашифрованным ловушкам протоколов SNMP v1/v2c. При использовании протокола SNMP v3 ловушки нужно настраивать с помощью приложения управления SNMP v3.
  - **Password for the account "initial" (Пароль для учетной записи initial):** Введите пароль SNMP для учетной записи с именем initial. Хотя пароль можно отправить без активации HTTPS, мы так поступать не рекомендуем. Пароль SNMP v3 можно задать лишь один раз, при этом рекомендуется включить протокол HTTPS. После установки пароля поле для ввода пароля больше не отображается. Для повторной установки пароля необходимо выполнить сброс устройства к заводским установкам.

### Connected clients (Подключенные клиенты)

# AXIS D2110-VE Security Radar

## Интерфейс устройства

В списке отображаются все клиенты, подключенные к устройству.

**Update (Обновление).** Нажмите, чтобы обновить список.

### Безопасность

#### Сертификаты

Сертификаты служат для проверки подлинности устройств в сети. Устройство поддерживает два типа сертификатов:

- **Сертификаты клиента/сервера**  
Сертификат клиента/сервера удостоверяет подлинность устройства. Он может быть самоверяющим или может быть выдан Центром сертификации (ЦС). Самоверяющий сертификат дает ограниченную защиту, и его можно использовать до получения сертификата, выданного Центром сертификации.
- **Сертификаты ЦС**  
Сертификат, выданный Центром сертификации (ЦС), можно использовать для подтверждения подлинности сертификата узла, например для идентификации сервера проверки подлинности, когда устройство подключается к сети, защищенной по стандарту IEEE 802.1X. Устройство поставляется с несколькими предустановленными сертификатами ЦС.

Поддерживаются следующие форматы:

- Форматы сертификатов: .PEM, .CER и .PFX
- Форматы закрытых ключей: PKCS#1 и PKCS#12

#### Важно!

При сбросе параметров устройства к заводским установкам все сертификаты удаляются. Любые предустановленные сертификаты ЦС будут установлены повторно.



Фильтрация сертификатов в списке.



**Add certificate (Добавление сертификата).** Нажмите эту кнопку, чтобы добавить сертификат.



Контекстное меню содержит следующие команды:

- **Certificate information (Информация о сертификате).** Просмотр свойств установленного сертификата.
- **Delete certificate (Удалить сертификат).** Удаление сертификата.
- **Create certificate signing request (Создать запрос подписи сертификата).** Создание запроса на подписание сертификата для его отправки в регистрационный орган и подачи заявления на получение цифрового удостоверения личности.

#### IEEE 802.1x

IEEE 802.1x — стандарт для технологии контроля доступа в сеть с использованием портов, обеспечивающий проверку подлинности проводных и беспроводных сетевых устройств. Стандарт IEEE 802.1x основан на протоколе EAP (Extensible Authentication Protocol).

Для получения доступа к сети, защищенной IEEE 802.1x, сетевые устройства должны пройти проверку подлинности. Проверка подлинности выполняется сервером проверки подлинности. Как правило, это RADIUS-сервер, примерами которого являются FreeRADIUS и сервер Microsoft для проверки подлинности в Интернете (IAS).

#### Сертификаты

Если сертификат ЦС не был настроен, проверка сертификата сервера будет отключена и устройство будет проверять собственную подлинность независимо от того, к какой сети оно подключено.

При использовании сертификата в установке Axis устройство и сервер аутентификации авторизуются с помощью цифровых сертификатов через протокол EAP-TLS.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

Чтобы обеспечить устройству доступ к сети, защищенной с помощью сертификатов, на устройстве должен быть установлен подписанный клиентский сертификат.

**Client certificate (Сертификат клиента):** Выберите сертификат клиента для использования IEEE 802.1x. Сервер проверки подлинности использует сертификат для подтверждения подлинности сервера аутентификации.

**CA certificate (Сертификат ЦС):** Выберите сертификат ЦС для проверки удостоверения сервера проверки подлинности. Если сертификат не выбран, устройство попытается пройти проверку подлинности независимо от того, к какой сети оно подключено.

**EAP identity (Идентификатор EAP).** Введите удостоверение пользователя, связанное с сертификатом клиента.

**EAPOL version (Версия EAPOL).** Выберите версию протокола EAPOL, используемую в сетевом коммутаторе.

**Use IEEE 802.1x (Использовать IEEE 802.1x):** Выберите этот пункт, чтобы использовать протокол IEEE 802.1x.

### Prevent brute-force attacks (Предотвращение атак методом подбора)

**Blocking (Блокировка):** Включите, чтобы блокировать атаки методом подбора пароля. При таких атаках злоумышленник пытается угадать данные для входа в систему или ключи шифрования, перебирая разные варианты.

**Blocking period (Период блокировки):** Введите количество секунд, в течение которых будет блокироваться атака методом подбора пароля.

**Blocking conditions (Блокирующие условия):** Введите количество сбоев проверки подлинности в секунду, вызывающее блокировку. Можно задать количество ошибок, разрешенных как на уровне страницы, так и на уровне устройства.

### Фильтр IP-адресов

**Use filter (Использовать фильтры):** Выберите этот пункт, чтобы отфильтровать IP-адреса, которым разрешен доступ к устройству.

**Policy (Политика):** Укажите, следует ли **Allow (Разрешить)** доступ или **Deny (Запретить)** доступ для определенных IP-адресов.

**Адреса:** Введите IP-адреса, которым разрешен или запрещен доступ к устройству. Можно также использовать формат CIDR.

### Custom-signed firmware certificate (Сертификат для встроенного ПО с пользовательской подписью)

Для установки тестового встроенного ПО или другого пользовательского встроенного ПО от компании Axis на устройстве необходимо использовать сертификат для встроенного ПО с пользовательской подписью. Сертификат проверяет, одобрено ли встроенное ПО как владельцем устройства, так и компанией Axis. Встроенное ПО может работать только на определенном устройстве, которое идентифицируется по его уникальному серийному номеру и идентификатору микросхемы. Сертификаты для встроенного ПО с пользовательской подписью может создавать только компания Axis, поскольку она является владельцем ключа для подписания таких сертификатов.

Нажмите **Install (Установить)**, чтобы установить сертификат. Перед установкой встроенного ПО необходимо установить сертификат.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

### Пользователи



**Add user (Добавить пользователя).** Нажмите, чтобы добавить нового пользователя. Можно добавить до 100 пользователей.

**Username (Имя пользователя).** Введите уникальное имя пользователя.

**New password (Новый пароль).** Введите пароль для пользователя. Длина паролей должна составлять от 1 до 64 символов. В пароле можно использовать только печатные ASCII-символы (с кодами от 32 до 126), например буквы, цифры, знаки пунктуации и некоторые другие символы.

**Repeat password (Повторите ввод пароля).** Введите тот же самый пароль еще раз.

**Role (Роль).**

- **Administrator (Администратор).** Имеет неограниченный доступ ко всем настройкам. Администраторы также могут добавлять, обновлять и удалять других пользователей.
- **Operator (Оператор).** Эти пользователи обладают правом доступа ко всем настройкам, кроме следующих:
  - Все System (Системные) настройки.
  - Добавление приложений.
- **Viewer (Наблюдатель).** Не может изменять настройки.



Контекстное меню содержит следующие команды:

**Update user (Обновить пользователя):** Изменение свойств пользователя.

**Delete user (Удалить пользователя).** Удаление пользователя. Пользователя root удалить нельзя.

### Anonymous users (Анонимные пользователи)

**Allow anonymous viewers (Разрешить анонимный просмотр).** Включите этот параметр, если нужно, чтобы любой человек мог получить доступ к устройству в качестве зрителя, не выполняя вход в учетную запись.

**Allow anonymous PTZ operators (Разрешить PTZ-управление анонимным операторам).** Включите этот параметр, чтобы анонимные пользователи могли выполнять поворот, наклон и зум изображения.

### События

#### Правила

Правило — это набор условий, которые должны быть выполнены, чтобы устройство совершило действие. В списке отображаются все настроенные на данный момент правила в устройстве.

#### Примечание.

Можно создать до 256 правил действия.



**Добавить правило.** Нажмите, чтобы создать правило.

**Name (Имя).** Введите имя для правила.

**Wait between actions (Ожидание между действиями).** Введите минимальное время (чч:мм:сс), которое должно пройти, чтобы правило могло быть вновь активировано. Этот параметр можно использовать, например, для правила, активируемого при наступлении условий дневной/ночной съемки, чтобы исключить частое срабатывание правила из-за небольших изменений в освещенности во время восхода или заката солнца.

**Condition (Условие).** Выберите условие из списка. Чтобы устройство выполнило то или иное действие, должно быть удовлетворено заданное условие. Если задано несколько условий, то для запуска соответствующего действия необходимо соблюдение всех условий. Сведения об особых условиях см. в разделе *Начало работы с правилами для событий*.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

Use this condition as a trigger (Использовать это условие в качестве триггера). Выберите этот параметр, если нужно, чтобы это первое условие выступало лишь в качестве запускающего триггера. Это означает, что после активации правило будет оставаться активным до тех пор, пока удовлетворяются все остальные условия, независимо от состояния первого условия. Если этот параметр не выбран, правило будет оставаться активным, пока удовлетворяются все условия.

Invert this condition (Инvertировать это условие). Выберите этот параметр, если нужно использовать условие, противоположное выбранному.



Добавить условие. Нажмите, чтобы добавить дополнительное условие.

Action (Действие). Выберите действие из списка и введите требуемую информацию. Сведения об особых действиях см. в разделе *Начало работы с правилами для событий*.

### Получатели

Можно настроить устройство так, чтобы оно уведомляло определенных получателей об определенных событиях или отправляло им файлы. Список содержит всех получателей, настроенных в устройстве на данный момент, включая различную информацию об их конфигурации.

#### Примечание.

Можно создать до 20 получателей.



Добавить получателя. Нажмите, чтобы добавить получателя.

Name (Имя). Введите имя получателя.

Type (Тип). Выберите нужный тип в списке.

- FTP
  - Host (Хост). Введите IP-адрес или имя хоста сервера. В случае ввода имени хоста убедитесь, что в разделе System > Network > IPv4 and IPv6 (Система > Сеть > IPv4 и IPv6) указан DNS-сервер.
  - Port (Порт). Введите номер порта, используемый FTP-сервером. Значение по умолчанию — 21.
  - Folder (Папка). Введите путь к каталогу, в котором будут храниться файлы. Если данного каталога еще нет на FTP-сервере, при загрузке файлов отобразится сообщение об ошибке.
  - Username (Имя пользователя). Введите имя пользователя для входа в систему.
  - Password (Пароль). Введите пароль для входа в систему.
  - Use temporary file name (Использовать временное имя файла). Выберите этот параметр, если для загружаемых файлов должны использоваться временные имена, генерируемые автоматически. По завершении загрузки файлам присваиваются требуемые имена. Если загрузка будет прервана по какой-либо причине, никакие файлы повреждены не будут. Однако могут остаться временные файлы. Таким образом, вы будете знать, что файлы с требуемыми именами не повреждены.
  - Use passive FTP (Использовать пассивный режим FTP). При нормальных условиях устройство просто отправляет на целевой FTP-сервер запрос на установление соединения для передачи данных. Устройство само инициирует установление FTP-соединений с целевым сервером для управления и передачи данных. Обычно это необходимо, если между устройством и целевым FTP-сервером установлен межсетевой экран.
- HTTP
  - URL. Введите сетевой адрес HTTP-сервера и сценарий обработки запроса. Пример: `http://192.168.254.10/cgi-bin/notify.cgi`.
  - Username (Имя пользователя). Введите имя пользователя для входа в систему.
  - Password (Пароль). Введите пароль для входа в систему.
  - Proxy (Прокси-сервер). Если для подключения к HTTP-серверу используется прокси-сервер, включите этот параметр и введите требуемую информацию.
- HTTPS
  - URL. Введите сетевой адрес HTTPS-сервера и сценарий обработки запроса. Пример: `https://192.168.254.10/cgi-bin/notify.cgi`.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

- **Validate server certificate (Проверка сертификата сервера).** Выберите этот параметр, если требуется проверка сертификата, созданного HTTPS-сервером.
- **Username (Имя пользователя).** Введите имя пользователя для входа в систему.
- **Password (Пароль).** Введите пароль для входа в систему.
- **Proxy (Прокси-сервер).** Если для подключения к HTTPS-серверу используется прокси-сервер, включите этот параметр и введите требуемую информацию.
- **Network storage (Сетевое хранилище)**

Можно добавить сетевое хранилище, например NAS (сетевое устройство хранения данных), и использовать его в качестве получателя для хранения файлов. Файлы сохраняются в формате Matroska (MKV).

  - **Host (Хост).** Введите IP-адрес или имя хоста сетевого хранилища данных.
  - **Share (Общий ресурс).** Введите имя общего ресурса на хосте.
  - **Folder (Папка).** Введите путь к каталогу, в котором будут храниться файлы.
  - **Username (Имя пользователя).** Введите имя пользователя для входа в систему.
  - **Password (Пароль).** Введите пароль для входа в систему.
- **SFTP**
  - **Host (Хост).** Введите IP-адрес или имя хоста сервера. В случае ввода имени хоста убедитесь, что в разделе **System > Network > IPv4 and IPv6 (Система > Сеть > IPv4 и IPv6)** указан DNS-сервер.
  - **Port (Порт).** Введите номер порта, используемый SFTP-сервером. Значение по умолчанию — 22.
  - **Folder (Папка).** Введите путь к каталогу, в котором будут храниться файлы. Если данного каталога еще нет на SFTP-сервере, при загрузке файлов отобразится сообщение об ошибке.
  - **Username (Имя пользователя).** Введите имя пользователя для входа в систему.
  - **Пароль:** Введите пароль для входа в систему.
  - **Тип SSH с открытым ключом хоста (MD5):** Введите отпечаток открытого ключа удаленного хоста (строка из 32 шестнадцатеричных символов). Клиент SFTP поддерживает SFTP-серверы, использующие протокол SSH-2 с ключами хоста типа RSA, DSA, ECDSA и ED25519. Наиболее предпочтителен метод RSA; остальные методы в порядке убывания предпочтения: ECDSA, ED25519 и DSA. Обязательно введите правильный ключ хоста MD5, который используется вашим SFTP-сервером. Хотя устройство Axis поддерживает хэш-ключи как MD5, так и SHA-256, мы рекомендуем использование ключа SHA-256, поскольку он обеспечивает более высокую безопасность, чем ключ MD5. Для получения более подробной информации о настройке SFTP-сервера с устройством Axis, перейдите на [портал AXIS OS Portal](#).
  - **Тип SSH с открытым ключом хоста (SHA256):** Введите отпечаток открытого ключа удаленного хоста (строка из 43 символов в формате Base64). Клиент SFTP поддерживает SFTP-серверы, использующие протокол SSH-2 с ключами хоста типа RSA, DSA, ECDSA и ED25519. Наиболее предпочтителен метод RSA; остальные методы в порядке убывания предпочтения: ECDSA, ED25519 и DSA. Обязательно введите правильный ключ хоста MD5, который используется вашим SFTP-сервером. Хотя устройство Axis поддерживает хэш-ключи как MD5, так и SHA-256, мы рекомендуем использование ключа SHA-256, поскольку он обеспечивает более высокую безопасность, чем ключ MD5. Для получения более подробной информации о настройке SFTP-сервера с устройством Axis, перейдите на [портал AXIS OS Portal](#).
  - **Use temporary file name (Использовать временное имя файла).** Выберите этот параметр, если для загружаемых файлов должны использоваться временные имена, генерируемые автоматически. По завершении загрузки файлам присваиваются требуемые имена. Если загрузка будет прервана по какой-либо причине, никакие файлы повреждены не будут. Однако могут остаться временные файлы. Таким образом вы будете знать, что все файлы с необходимым вам именем не повреждены.
- **SIP**
  - **Из учетной записи SIP:** Выберите нужный тип в списке.
  - **На SIP-адрес:** Введите SIP-адрес.
- **Эл. почта**
  - **Send email to (Получатель электронной почты).** Введите адрес электронной почты для отправки сообщений. Можно ввести несколько адресов, разделяя их запятыми.
  - **Send email from (Отправитель электронной почты).** Введите адрес электронной почты отправляющего сервера.
  - **Username (Имя пользователя).** Введите имя пользователя для сервера электронной почты. Оставьте это поле пустым, если почтовый сервер не требует проверки подлинности.
  - **Password (Пароль).** Введите пароль для сервера электронной почты. Оставьте это поле пустым, если почтовый сервер не требует проверки подлинности.
  - **Email server (SMTP) (Сервер электронной почты (SMTP)).** Введите имя SMTP-сервера, например: smtp.gmail.com, smtp.mail.yahoo.com.
  - **Port (Порт).** Введите номер порта SMTP-сервера, используя значения в диапазоне 0–65535. Значение по умолчанию — 587.
  - **Encryption (Шифрование).** Чтобы использовать шифрование, выберите SSL или TLS.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

- **Validate server certificate (Проверка сертификата сервера).** Если используется шифрование, выберите этот параметр для проверки подлинности устройства. Сертификат может быть самозаверяющим или может быть выдан центром сертификации (ЦС).
- **POP authentication (Проверка подлинности POP).** Если требуется, включите этот параметр и введите имя POP-сервера, например: pop.gmail.com.

### Примечание.

Некоторые поставщики услуг электронной почты применяют фильтры безопасности, из-за которых пользователи не могут получать или просматривать вложения большого объема, получать письма по расписанию и т. п. Поинтересуйтесь политикой безопасности выбранного поставщика услуг электронной почты, чтобы избежать блокирования учетной записи электронной почты или пропуска ожидаемых сообщений.

- TCP

- **Host (Хост).** Введите IP-адрес или имя хоста сервера. В случае ввода имени хоста убедитесь, что в разделе **System > Network > IPv4 and IPv6 (Система > Сеть > IPv4 и IPv6)** указан DNS-сервер.
- **Port (Порт).** Введите номер порта, используемого для доступа к серверу.

**Test (Проверка).** Нажмите, чтобы проверить настройку.



Контекстное меню содержит следующие команды:

**View recipient (Просмотреть получателя).** Нажмите для просмотра всех сведений о получателе.

**Copy recipient (Копировать получателя).** Нажмите, чтобы скопировать получателя. Скопировав получателя, можно внести изменения для создания нового получателя.

**Delete recipient (Удалить получателя).** Нажмите, чтобы навсегда удалить получателя.

### Расписания

Расписания и импульсы могут использоваться в качестве условий в правилах. Список содержит все расписания и импульсы, настроенные в устройстве на данный момент, включая различную информацию о их конфигурации.



**Добавить расписание.** Нажмите, чтобы создать расписание или импульс.

### Ручной запуск

Ручной запуск используется для запуска правила вручную. Например, ручной запуск можно использовать для проверки действий при установке и настройке устройства.

### MQTT

MQTT (Message Queuing Telemetry Transport) — это стандартный протокол обмена сообщениями для Интернета вещей (IoT). Он был разработан с целью упростить интеграцию IoT и используется в самых разных отраслях для подключения удаленных устройств с небольшим объемом кода и требующих минимальной пропускной способности сети. Клиент MQTT, встроенный в микропрограмму устройства Axis, позволяет упростить интеграцию данных и событий устройства в другие системы, которые не являются системами управления видео (VMS).

Настройте устройство в качестве клиента MQTT. Связь по протоколу MQTT происходит между двумя участниками: клиентом и брокером. Клиенты могут отправлять и принимать сообщения. Брокер отвечает за маршрутизацию сообщений между клиентами.

Более подробно о протоколе MQTT можно узнать на странице *AXIS OS Portal*.

### MQTT client (Клиент MQTT)



# AXIS D2110-VE Security Radar

## Интерфейс устройства

**Connect (Подключение).** Позволяет включить или выключить клиент MQTT.

**Status (Состояние).** Отображает текущее состояние клиента MQTT.

**Broker (Брокер)**

**Host (Хост).** Введите имя хоста или IP-адрес сервера MQTT.

**Protocol (Протокол).** Выберите протокол, который будет использоваться.

**Port (Порт).** Введите номер порта.

- 1883 — это значение по умолчанию для MQTT по протоколу TCP
- 8883 — это значение по умолчанию для MQTT по протоколу SSL
- 80 — это значение по умолчанию для MQTT по протоколу WebSocket
- 443 — это значение по умолчанию для MQTT по протоколу WebSocket Secure

**Username (Имя пользователя).** Введите имя пользователя, которое клиент будет использовать для доступа к серверу.

**Password (Пароль).** Введите пароль для имени пользователя.

**Client ID (Идентификатор клиента).** Введите идентификатор клиента. Идентификатор клиента, передаваемый на сервер, когда клиент подключается к серверу.

**Clean session (Очистка сеанса).** Определяет поведение во время подключения и отключения. Если этот параметр включен, информация о состоянии при подключении и отключении отклоняется.

**Keep alive interval (Интервал поддержания активности соединения).** С помощью параметра Keep alive interval (Интервал поддержания активности соединения) клиент может определять, что сервер больше не доступен, не ожидая долго тайм-аута TCP/IP.

**Timeout (Тайм-аут).** Промежуток времени в секундах, в течение которого должно быть выполнено соединение. Значение по умолчанию: 60

**Префикс темы устройства:** Используется в значениях по умолчанию для раздела в Connect message (Сообщение о подключении) и LWT message (Сообщение «завещания») на вкладке клиента MQTT, а также в условиях публикации на вкладке публикация MQTT.

**Reconnect automatically (Переподключаться автоматически).** Указывает, должен ли клиент автоматически переподключаться при непреднамеренном отключении.

**Connect message (Сообщение о подключении)**

Указывает, следует ли отправлять сообщение при установлении подключения.

**Send message (Отправить сообщение).** Включите этот параметр для отправки сообщений.

**Use default (Использовать по умолчанию).** Выключите этот параметр, если вы хотите ввести собственное сообщение для использования по умолчанию.

**Topic (Тема).** Введите тему для сообщения по умолчанию.

**Payload (Полезные данные).** Введите содержание сообщения по умолчанию.

**Retain (Сохранять).** Выберите, чтобы сохранить состояние клиента для данной темы (**Topic (Тема)**).

**QoS.** Позволяет изменить уровень QoS для потока пакетов.

**Last Will and Testament message (Сообщение последнего распоряжения)**

С помощью параметра Last Will Testament (Завещание) клиент при подключении к брокеру может вместе со своими учетными данными предоставить распоряжение («завещание»). Это позволит брокеру отправить сообщение другим клиентам, если впоследствии данный клиент будет некорректно отключен (например, из-за отсутствия питания). Сообщение «завещания» имеет ту же форму, что и обычное сообщение, и отправляется с использованием тех же механизмов.

**Send message (Отправить сообщение).** Включите этот параметр для отправки сообщений.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

**Use default (Использовать по умолчанию).** Выключите этот параметр, если вы хотите ввести собственное сообщение для использования по умолчанию.

**Topic (Тема).** Введите тему для сообщения по умолчанию.

**Payload (Полезные данные).** Введите содержание сообщения по умолчанию.

**Retain (Сохранять).** Выберите, чтобы сохранить состояние клиента для данной темы (**Topic (Тема)**).

**QoS.** Позволяет изменить уровень QoS для потока пакетов.

### Публикация MQTT

**Use default topic prefix (Использовать префикс темы по умолчанию).** Выберите этот пункт, чтобы использовать префикс темы по умолчанию, который определяется в префиксе темы устройства на вкладке **MQTT client (Клиент MQTT)**.

**Include topic name (Включить имя темы).** Выберите этот пункт, чтобы включить в тему MQTT тему, описывающую соответствующее условие.

**Include topic namespaces (Включить пространство имен).** Выберите этот параметр, если в тему MQTT нужно включить пространства имен темы ONVIF.

**Include serial number (Включить серийный номер):** Выберите этот параметр, если в полезные данные MQTT нужно включить серийный номер устройства.



**Add condition (Добавить условие).** Нажмите, чтобы добавить условие.

**Retain (Сохранять).** Определяет, какие сообщения MQTT отправляются как сохраняемые.

- **None (Нет).** Отправлять все сообщения как несохраняемые.
- **Property (Свойство).** Отправлять в качестве сохраняемых только сообщения с сохранением состояния.
- **All (Все).** Отправлять в качестве сохраняемых сообщения с сохранением и без сохранения состояния.

**QoS.** Выберите требуемый уровень для публикации MQTT.

### MQTT subscriptions (Подписки MQTT)



**Добавить подписку.** Нажмите, чтобы добавить новую подписку MQTT.

**Subscription filter (Фильтр подписок).** Введите тему MQTT, на которую вы хотите подписаться.

**Use device topic prefix (Использовать префикс темы устройства).** Добавьте фильтр подписки в качестве префикса к теме MQTT.

**Subscription type (Тип подписки).**

- **Stateless (Без сохранения состояния).** Выберите этот вариант для преобразования сообщений MQTT в сообщения без сохранения состояния.
- **Stateful (С сохранением состояния).** Выберите этот вариант для преобразования сообщений MQTT в условие. Полезные данные используются в качестве состояния.

**QoS.** Выберите требуемый уровень для подписки MQTT.

### Storage (Устройство хранения)

Network storage (Сетевое хранилище)

# AXIS D2110-VE Security Radar

## Интерфейс устройства

**Добавить сетевой накопитель.** Нажмите, чтобы добавить сетевой ресурс для хранения записей.

- **Адрес.** Введите IP-адрес или имя хоста для хост-сервера, который обычно является сетевым устройством хранения данных (NAS). Рекомендуется настроить на хосте использование статического IP-адреса (а не DHCP, так как динамический IP-адрес может меняться) либо использовать DNS. Имена Windows SMB/CIFS не поддерживаются.
- **Network share (Сетевой ресурс).** Введите имя сетевой папки на хост-сервере. Несколько устройств Axis могут использовать один и тот же сетевой ресурс: у каждого устройства будет своя папка.
- **User (Пользователь).** Если для входа на сервер требуется авторизация, введите имя пользователя. Чтобы войти на определенный сервер домена, введите DOMAIN\username (ДОМЕН\имя пользователя).
- **Password (Пароль).** Если для входа на сервер требуется авторизация, введите пароль.
- **SMB version (Версия SMB).** Выберите версию протокола SMB для подключения к сетевому устройству хранения данных (NAS). Если выбрать вариант **Auto (Автоматически)**, устройство при подключении к NAS будет пытаться автоматически согласовать использование одной из безопасных версий протокола SMB: 3.02, 3.0 или 2.1. Для подключения к старому серверу NAS, не поддерживающему более новые версии, можно выбрать версию 1.0 или 2.0. Более подробно о поддержке протокола SMB в устройствах Axis можно прочитать [здесь](#).
- **Добавить ресурс, даже если проверка соединения завершится сбоем.** Выберите этот параметр, если нужно, чтобы сетевой ресурс был добавлен, даже если проверка соединения завершится ошибкой. Ошибка может произойти, к примеру, если вы не введете пароль, когда его ввод необходим для входа на сервер.

**Remove network storage (Удалить сетевой накопитель).** Нажмите, чтобы удалить подключение к сетевому ресурсу. При этом будут удалены все настройки сетевого ресурса.

**Write protect (Защита от записи).** Активируйте этот параметр чтобы прекратить запись на сетевой ресурс и защитить записи от удаления. Сетевой ресурс с защитой от записи нельзя форматировать.

**Ignore (Игнорировать).** Активируйте этот параметр, чтобы прекратить сохранение записей в сетевом ресурсе.

**Retention time (Срок хранения).** Укажите, как долго требуется хранить записи, чтобы ограничить объем старых записей либо обеспечить соблюдение нормативов, касающихся хранения данных. Если место на сетевом накопителе закончится, старые записи будут удаляться до истечения выбранного периода времени.

### Tools (Инструменты)

- **Test connection (Проверить соединение).** Проверка соединения с сетевым ресурсом.
- **Format (Форматировать).** Позволяет форматировать сетевой ресурс, например, когда необходимо быстро удалить все данные. В качестве файловой системы можно выбрать CIFS.

Чтобы привести в действие выбранный инструмент, нажмите **Use tool (Использовать инструмент)**.

### Встроенный накопитель

#### Важно!

Риск потери данных и повреждения записей. Не извлекайте SD-карту во время работы устройства. Прежде чем извлечь SD-карту, отключите ее.

**Unmount (Отключить).** Нажмите, чтобы безопасно извлечь SD-карту.

**Write protect (Защита от записи).** Включите этот параметр, чтобы прекратить запись на SD-карту и защитить записи от удаления. SD-карту с защитой от записи форматировать нельзя.

**Autoformat (Автоматическое форматирование).** Включите этот параметр для автоматического форматирования любой впервые вставляемой SD-карты. При форматировании на карте создается файловая система ext4.

**Ignore (Игнорировать).** Включите этот параметр, если нужно прекратить сохранение записей на SD-карту. При игнорировании SD-карты устройство больше сможет распознать наличие карты. Этот параметр доступен только для администраторов.

**Retention time (Срок хранения).** Укажите, как долго требуется хранить записи, чтобы ограничить объем старых записей либо обеспечить соблюдение нормативов, касающихся хранения данных. Когда место на SD-карте заканчивается, старые записи будут удаляться до того, как истечет выбранный период времени.

### Tools (Инструменты)

# AXIS D2110-VE Security Radar


## Интерфейс устройства

- **Check (Проверить).** Проверка SD-карты на наличие ошибок. Эта функция работает только для файловой системы ext4.
- **Repair (Восстановить).** Исправление ошибок в файловой системе ext4. Для устранения ошибок на SD-карте, отформатированной с использованием файловой системы VFAT, извлеките SD-карту, вставьте ее в компьютер и запустите программу восстановления диска.
- **Format (Форматировать):** Если необходимо изменить файловую систему или быстро стереть все данные, отформатируйте SD-карту. Доступные типы файловой системы: VFAT и ext4. Рекомендуется использовать формат ext4, поскольку он более устойчив к потере данных при извлечении карты или внезапном отключении питания. Однако для доступа к файловой системе из Windows® потребуется драйвер для файловой системы ext4 стороннего разработчика или соответствующее приложение.
- **Encrypt.** Используйте этот инструмент для форматирования SD-карты и включения шифрования. **Encrypt** удаляет все данные, хранящиеся на SD-карте. После применения инструмента **Encrypt** данные, хранящиеся на SD-карте, защищаются с помощью шифрования.
- **Decrypt.** Используйте этот инструмент для форматирования SD-карты без шифрования. **Decrypt** удаляет все данные, хранящиеся на SD-карте. После применения инструмента **Decrypt** данные, хранящиеся на SD-карте, не защищаются с помощью шифрования.
- **Change password (Изменить пароль).** Изменение пароля, необходимого для шифрования SD-карты.

Чтобы привести в действие выбранный инструмент, нажмите **Use tool (Использовать инструмент)**.

**Триггер по износу:** Задайте значение для уровня износа SD-карты, при котором будет запускаться соответствующее действие. Уровень износа варьируется в диапазоне 0–200 %. Уровень износа новой, еще не использованной SD-карты составляет 0 %. Уровень износа в 100 % указывает, что срок службы SD-карты близок к завершению. При уровне износа 200 % очень высок риск того, что SD-карта будет функционировать неправильно. Мы рекомендуем задавать инициирующее событие для триггера по износу в диапазоне 80–90 %. Благодаря этому у вас будет время для загрузки любых записей, а также для замены SD-карты до ее потенциального износа. Триггер по износу позволяет задать соответствующее событие и получить уведомление до того, как уровень износа достигнет заданного значения.

### Профили потока

Нажмите значок , чтобы создать и сохранить группы параметров видеопотока. Эти параметры можно использовать в различных ситуациях, например при непрерывной записи или при использовании правил действия для запуска записи.

### ONVIF

#### Пользователи ONVIF

ONVIF (Open Network Video Interface Forum) — это международный стандарт интерфейса, нацеленный на то, чтобы конечным пользователям, интеграторам, консультантам и производителям было проще использовать преимущества технологии сетевого видео. Стандарт ONVIF обеспечивает интероперабельность устройств разных производителей, повышает их эксплуатационную гибкость, способствует снижению затрат и дает возможность модернизировать системы в будущем.



Добавить пользователя. Нажмите, чтобы добавить нового пользователя ONVIF.

**Username (Имя пользователя).** Введите уникальное имя пользователя.

**New password (Новый пароль).** Введите пароль для пользователя. Длина паролей должна составлять от 1 до 64 символов. В пароле можно использовать только печатные ASCII-символы (с кодами от 32 до 126), например буквы, цифры, знаки пунктуации и некоторые другие символы.

**Repeat password (Повторите ввод пароля).** Введите тот же самый пароль еще раз.

**Role (Роль).**

- **Administrator (Администратор).** Имеет неограниченный доступ ко всем настройкам. Администраторы также могут добавлять, обновлять и удалять других пользователей.
- **Operator (Оператор).** Эти пользователи обладают правом доступа ко всем настройкам, кроме следующих:

# AXIS D2110-VE Security Radar

## Интерфейс устройства

- Все System (Системные) настройки.
  - Добавление приложений.
  - Media user (Пользователь мультимедиа). Возможен доступ только к видеопотоку.
- ⋮  
Контекстное меню содержит следующие команды:

Update user (Обновить пользователя). Изменение свойств пользователя.

Delete user (Удалить пользователя). Удаление пользователя. Пользователя root удалить нельзя.

При создании пользователя ONVIF автоматически разрешается обмен данными по стандарту ONVIF. Для любой связи с устройством в рамках ONVIF используйте заданные имя пользователя и пароль. Дополнительную информацию можно найти на страницах сообщества разработчиков Axis Developer Community на сайте [axis.com](http://axis.com).

### Медиапрофили ONVIF

Медиапрофиль ONVIF содержит набор конфигураций, которые можно использовать для изменения параметров медиапотока.



Добавить медиапрофиль. Нажмите, чтобы добавить новый медиапрофиль ONVIF.

profile\_x. Щелкните профиль, чтобы внести в него изменения.

### Метаданные аналитики

#### Производители метаданных

Производители метаданных перечисляют каналы, используемые приложениями, а также метаданные, в потоке с которыми они передаются с устройства.

Производитель. Приложение, в котором были произведены метаданные.

Канал. Канал, используемый приложением. Установите этот флажок, чтобы включить поток метаданных. Чтобы отключить поток для совместимости или управления ресурсами, снимите этот флажок.

### Детекторы

#### Shock detection (Обнаружение ударов)

Shock detector (Детектор ударов). Включите этот параметр, если нужно, чтобы устройство подавало сигнал тревоги в случае удара каким-либо предметом или при ином механическом воздействии (например, с целью взлома или вывода из строя).

Sensitivity level (Уровень чувствительности). Перемещая ползунок, установите уровень чувствительности для определения силы удара, при которой должен подаваться сигнал тревоги. При небольшом значении устройство будет подавать сигнал тревоги только при сильном ударе. Высокое значение означает, что устройство будет подавать сигнал тревоги даже при незначительном воздействии.

### Принадлежности

#### Подключение сетевого громкоговорителя

# AXIS D2110-VE Security Radar

## Интерфейс устройства

Связав сетевой громкоговоритель с камерой, можно использовать совместимый сетевой громкоговоритель Axis так, как если бы он был подключен непосредственно к камере. После связывания громкоговоритель будет работать как устройство для вывода звука. С его помощью вы сможете воспроизводить аудиоклипы и передавать звук через камеру.

### Важно!

Чтобы эта функция работала с ПО для управления видео (VMS), необходимо сначала связать камеру с сетевым громкоговорителем, а затем добавить камеру в ваше ПО для управления видео.

**Адрес:** Введите имя хоста или IP-адрес для сетевого громкоговорителя.

**Имя пользователя:** Введите имя пользователя.

**Пароль:** Введите пароль для пользователя.

**Очистить поля:** Нажмите, чтобы очистить все поля.

**Подключение:** Нажмите, чтобы установить подключение к сетевому громкоговорителю.



### I/O ports (Порты ввода-вывода)



Используйте цифровой вход для подключения внешних устройств, способных размыкать и замыкать электрическую цепь, таких как пассивные ИК-датчики, дверные или оконные контакты и детекторы разбивания стекла.

Цифровой выход служит для подключения внешних устройств, например таких как реле и светодиодных индикаторов. Подключенные устройства можно активировать с помощью VAPIX® Application Programming Interface или в интерфейсе устройства.

#### Port (Порт)

**Name (Имя):** Чтобы переименовать порт, измените текст.


**Direction (Направление):**  указывает, что порт является входным портом.  указывает на то, что это порт вывода. Если порт настраиваемый, то нажмите на значки для переключения между входом и выходом.

**Нормальное состояние:** Нажмите  для разомкнутой цепи и  для замкнутой цепи.

**Текущее состояние:** Показывает текущее состояние порта. Вход или выход активен, когда его текущее состояние отличается от нормального. Входная цепь устройства разомкнута, когда вход не подсоединен или при наличии напряжения выше 1 В пост. тока.

#### Примечание.

Во время перезапуска выходная цепь разомкнута. После завершения перезапуска цепь возвращается в обычное положение. При изменении каких-либо параметров на этой странице выходные цепи вернуться в обычное положение, даже если в этот момент будут активны какие-либо триггеры.

**Контролируемый**  : Включите этот параметр для обнаружения и запуска действий при несанкционированных действиях с подключением к цифровым устройствам ввода-вывода. Помимо обнаружения разомкнутых или замкнутых входных цепей, можно также обнаруживать несанкционированные действия с ними (например, при обрыве или замыкании). Реализация этой функции требует дополнительного оборудования (резисторы на концах линии) во внешней петле ввода-вывода.

## Журналы

Отчеты и журналы

# AXIS D2110-VE Security Radar

## Интерфейс устройства

### Reports (Отчеты)

- **View the device server report (Просмотр отчета сервера устройства).** Нажмите, чтобы просмотреть информацию о состоянии устройства (во всплывающем окне). В отчет сервера автоматически добавляется журнал доступа.
- **Download the device server report (Загрузить отчет сервера устройства).** Нажмите, чтобы скачать отчет сервера. При скачивании отчета сервера создается файл ZIP, который содержит полный отчет сервера в виде текстового файла в формате UTF-8, а также моментальный снимок текущего изображения живого просмотра. При обращении в службу поддержки всегда прикладывайте файл ZIP с отчетом сервера.
- **Download the crash report (Загрузить отчет о сбоях в работе сервера).** Нажмите, чтобы скачать архив с подробной информацией о состоянии сервера. Отчет об отказах системы содержит сведения, включенные в отчет сервера, а также подробную информацию для отладки. Этот отчет может содержать конфиденциальную информацию, например трассировку сети. Для формирования отчета может потребоваться несколько минут.

### Logs (Журналы)

- **View the system log (Просмотр журнала системных событий).** Нажмите, чтобы показать информацию о системных событиях, таких как запуск устройства, предупреждения и важные сообщения.
- **View the access log (Просмотр журнала запросов на получение доступа).** Нажмите, чтобы отобразить все неудачные попытки доступа к устройству, например при использовании неверного пароля для входа в систему.

### Network trace (Трассировка сети)

#### Важно!

Файл трассировки сети может содержать конфиденциальную информацию, например сертификаты или пароли.

В файле трассировки сети регистрируются совершаемые в сети операции, что может помочь в поиске и устранении неполадок. Выберите продолжительность трассировки в секундах или минутах и нажмите **Download (Скачать)**.

### Remote system log (Удаленный системный журнал)

Системный журнал (syslog) – это стандартный способ регистрации сообщений. С его помощью можно разделить программное обеспечение, которое генерирует сообщения, систему, в которой они хранятся, и программное обеспечение, которое сообщает о них и анализирует их. Каждое сообщение помечается кодом объекта, обозначающим тип программного обеспечения, создавшего сообщение. Также сообщению назначается уровень серьезности.



**Server (Сервер).** Нажмите, чтобы добавить новый сервер.

**Host (Хост).** Введите имя хоста или IP-адрес сервера.

**Format (Форматировать):** Выберите формат сообщений в системном журнале.

- RFC 3164
- RFC 5424

**Protocol (Протокол).** Выберите протокол и порт для использования:

- UDP (по умолчанию используется порт 514)
- TCP (по умолчанию используется порт 601)
- TLS (по умолчанию используется порт 6514)

**Severity (Степень серьезности).** Выберите, какие сообщения будут отправляться при срабатывании триггера.

**CA certificate set (Набор сертификатов ЦС).** Просмотр текущих настроек или добавление сертификата.

### Простая конфигурация

Простая конфигурация предназначена для опытных пользователей, разбирающихся в настройках устройства Axis. На этой странице можно задать и изменить большинство параметров.

# AXIS D2110-VE Security Radar

## Интерфейс устройства

### Обслуживание

**Restart (Перезапуск).** Перезапуск устройства. Это не повлияет на какие-либо текущие параметры. Работающие приложения перезапустятся автоматически.

**Restore (Восстановить).** Возврат *большинства* настроек к заводским установкам. После этого необходимо перенастроить устройство и приложения, переустановить все приложения, которые не были предустановлены, и воссоздать любые события и предустановленные положения PTZ.

#### Важно!

Единственными настройками, которые сохраняются после восстановления, являются следующие:

- Boot protocol (DHCP or static) (Протокол загрузки (DHCP или статический))
- Статический IP-адрес
- Default router (Маршрутизатор по умолчанию)
- Subnet mask (Маска подсети)
- Параметры 802.1X
- Параметры ОЗС

**Factory default (Заводские установки).** Возврат *всех* настроек к заводским установкам. После этого необходимо сбросить IP-адрес, чтобы обеспечить возможность доступа к устройству.

#### Примечание.

Чтобы гарантировать то, что на вашем устройстве выполняется установка только проверенного встроенного ПО, все встроенное ПО для устройств Axis сопровождается цифровой подписью. Это еще больше повышает общий минимальный уровень кибербезопасности устройств Axis. Для получения дополнительной информации см. технический документ «Встроенное ПО с цифровой подписью, режим безопасной загрузки и защита закрытых ключей» на веб-сайте [axis.com](http://axis.com).

**Firmware upgrade (Обновление встроенного ПО).** Обновление до новой версии встроенного ПО. Новые выпуски встроенного ПО могут содержать улучшенную функциональность, исправление ошибок или совершенно новые функции. Рекомендуется всегда использовать самую последнюю версию. Чтобы скачать последнюю версию, перейдите на страницу [axis.com/support](http://axis.com/support).

В ходе обновления можно выбрать один из трех вариантов:

- **Standard upgrade (Стандартное обновление).** Обновление до новой версии встроенного ПО.
- **Factory default (Заводские установки).** Обновление и возврат всех настроек к заводским установкам по умолчанию. При выборе этого варианта после выполнения обновления вернуться к предыдущей версии встроенного ПО будет нельзя.
- **Autorollback (Автооткат).** Обновление и подтверждение обновления в течение указанного срока. Если не выполнить подтверждение, устройство вернется к предыдущей версии встроенного ПО.

**Firmware rollback (Откат встроенного ПО).** Выполнение отката к установленной ранее версии встроенного ПО.



# AXIS D2110-VE Security Radar

## Устранение неполадок

---

### Устранение неполадок

#### Сброс к заводским установкам

**Важно!**

Сброс к заводским установкам следует использовать с осторожностью. Сброс к заводским установкам приведет к возврату всех параметров (включая IP-адрес) к принимаемым по умолчанию значениям.

Для сброса параметров изделия к заводским установкам:

1. Отсоедините питание устройства.
2. Нажмите и удерживайте кнопку управления, одновременно подключив питание. См. *Общий вид устройства на стр. 53*.
3. Удерживайте кнопку управления в нажатом положении в течение 15–30 секунд, пока индикатор состояния не начнет мигать желтым цветом.
4. Отпустите кнопку управления. Процесс завершен, когда индикатор состояния становится зеленым. Произошел сброс параметров устройства к заводским установкам по умолчанию. Если в сети нет доступного DHCP-сервера, то IP-адресом по умолчанию будет 192.168.0.90.
5. С помощью программных средств для установки и управления назначьте IP-адрес, задайте пароль и получите доступ к устройству.

Программные средства установки и управления доступны на страницах поддержки по адресу [axis.com/support](http://axis.com/support).

Сброс параметров к заводским установкам также можно выполнить на веб-странице устройства. Перейдите к пункту Maintenance (Обслуживание) > Factory default (Заводские установки) и нажмите Default (По умолчанию).

#### Проверка текущей версии встроенного ПО

Функциональность каждого сетевого устройства определяется его встроенным программным обеспечением. При возникновении неполадок рекомендуется в первую очередь проверить текущую версию встроенного ПО. Последняя версия встроенного ПО может содержать исправление, устраняющее определенную проблему.

Чтобы проверить текущую версию встроенного ПО:

1. Перейдите в меню Status (Состояние) в интерфейсе устройства.
2. Версия встроенного ПО отображается в разделе Device info (Информация об устройстве).

#### Обновление встроенного ПО

**Важно!**

При обновлении встроенного ПО предварительно заданные и измененные настройки будут сохранены (при условии наличия тех же функций в новой версии встроенного ПО), однако Axis Communications AB этого не гарантирует.

**Важно!**

Обеспечьте, чтобы устройство было подключено к источнику питания в течение всего процесса обновления.

**Примечание.**

Если для обновления устройства используется последняя версия встроенного ПО действующей ветви обновлений (Active), на устройстве становятся доступны новые функции. Перед обновлением встроенного ПО всегда читайте инструкции и примечания к выпуску, сопровождающие обновление. Последнюю версию встроенного ПО и примечания к выпуску можно найти на странице [axis.com/support/firmware](http://axis.com/support/firmware).

1. Файл встроенного ПО можно бесплатно скачать на компьютер со страницы [axis.com/support/firmware](http://axis.com/support/firmware).

# AXIS D2110-VE Security Radar

## Устранение неполадок

---

2. Войдите в систему устройства в качестве администратора.
3. Перейдите к пункту **Maintenance > Firmware upgrade (Обслуживание > Обновление встроенного ПО)** и нажмите **Upgrade (Обновить)**.

По окончании обновления устройство автоматически перезапустится.

### Технические проблемы, советы и решения

Если вам не удалось найти здесь нужную информацию, перейдите в раздел о поиске и устранении неисправностей на странице [axis.com/support](http://axis.com/support).

#### Проблемы при обновлении встроенного ПО

---

Сбой при обновлении встроенного ПО	Если при обновлении встроенного ПО происходит сбой, устройство загружает предыдущую версию встроенного ПО. Чаще всего сбои происходят из-за того, что загружен неподходящий файл встроенного ПО. Убедитесь, что имя файла встроенного ПО соответствует вашему устройству, и повторите попытку.
Проблемы после обновления встроенного ПО	Если после обновления встроенного ПО возникли какие-либо проблемы, перейдите на страницу <b>Maintenance (Обслуживание)</b> и сделайте откат к предыдущей версии ПО, которая была у вас установлена.

#### Проблемы с заданием IP-адреса

---

Устройство расположено в другой подсети	Если тот IP-адрес, который вы собираетесь назначить устройству, и IP-адрес компьютера, используемого для получения доступа к устройству, расположены в разных подсетях, то вы не сможете настроить IP-адрес. Свяжитесь с сетевым администратором, чтобы получить соответствующий IP-адрес.
IP-адрес используется другим устройством.	Отключите устройство Axis от сети. Запустите команду Ping (в командной строке или сеансе DOS введите ping и IP-адрес устройства): <ul style="list-style-type: none"><li>• Если вы получите следующий ответ: <code>Reply from &lt;IP-адрес&gt;: bytes=32; time=10...</code> – это означает, что данный IP-адрес, возможно, уже используется другим устройством в сети. Получите новый IP-адрес у сетевого администратора и переустановите устройство.</li><li>• Если вы получите следующий ответ: <code>Request timed out</code>, это означает, что данный IP-адрес доступен для использования устройством Axis. В этом случае проверьте все кабели и переустановите устройство.</li></ul>
Возможный конфликт с IP-адресом другого устройства в той же подсети	Прежде чем DHCP-сервер установит динамический адрес, в устройстве Axis используется статический IP-адрес. Это означает, что если такой же статический IP-адрес по умолчанию используется другим устройством, то могут возникнуть проблемы с доступом к устройству.

#### Не удается получить доступ к устройству из браузера

---

Не удается войти в систему	При включенном протоколе HTTPS убедитесь, что при попытке входа используется должный протокол (HTTP или HTTPS). Возможно, придется вручную ввести <code>http</code> или <code>https</code> в адресное поле браузера.  Если утерян пароль для пользователя root, необходимо произвести сброс параметров устройства к заводским установкам по умолчанию. См. <i>Сброс к заводским установкам на стр. 49</i> .
----------------------------	---

# AXIS D2110-VE Security Radar

## Устранение неполадок

---

IP-адрес изменен DHCP-сервером.

IP-адрес, получаемый от DHCP-сервера, является динамическим и может меняться. Если IP-адрес изменился, используйте утилиту AXIS IP Utility или AXIS Device Manager, чтобы найти устройство в сети. Устройство можно идентифицировать по модели, серийному номеру или DNS-имени (если это имя задано).

При необходимости можно вручную назначить статический IP-адрес. Инструкции см. на странице [axis.com/support](http://axis.com/support).

Ошибка сертификата при использовании IEEE 802.1X

Проверка подлинности пройдет должным образом, только если дата и время устройства Axis синхронизируются с NTP-сервером. Перейдите к пункту **System > Date and time (Система > Дата и время)**.

### Устройство доступно локально, но не доступно из внешней сети

---

Для доступа к устройству из внешней сети рекомендуется использовать одно из следующих приложений для Windows®:

- AXIS Companion: бесплатное приложение, которое идеально подходит для небольших систем с базовыми требованиями к охранному видеонаблюдению.
- AXIS Camera Station: бесплатная пробная версия на 30 дней, идеальное решение для систем от небольшого до среднего размера.

Для получения инструкций и загрузки перейдите на страницу [axis.com/vms](http://axis.com/vms).

## Рекомендации по увеличению производительности

В первую очередь необходимо учитывать следующие факторы:

- Интенсивное использование сети из-за низкого качества инфраструктуры увеличивает объем трафика.

# AXIS D2110-VE Security Radar

## Рекомендации по очистке

---

### Рекомендации по очистке

Для удаления с поверхности устройства жирных пятен, смазки или сильных загрязнений можно использовать мягкое моющее средство или мыльный раствор без растворителей.

**ПРИМЕЧАНИЕ.**

Никогда не используйте агрессивные моющие средства, такие как бензин, бензол или ацетон.

1. Для удаления пыли и частиц грязи с поверхности устройства используйте баллончик со сжатым воздухом.
2. Для чистки устройства используйте мягкую ткань, смоченную мягким моющим средством и умеренно теплой водой.
3. Тщательно протрите поверхность сухой тканью.

**Примечание.**

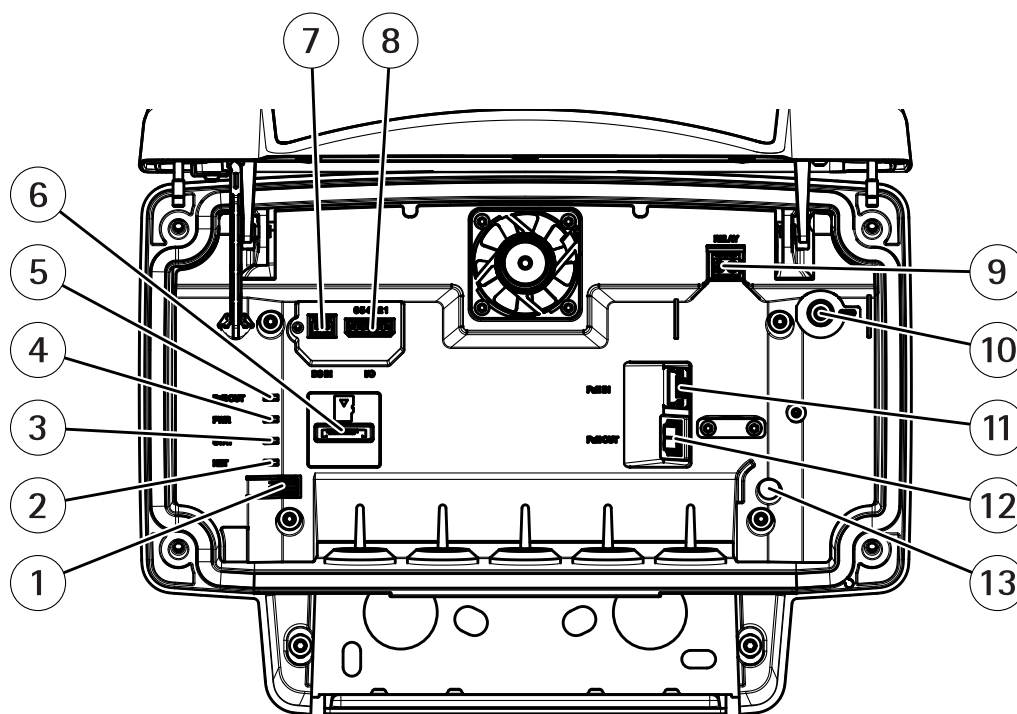
Не производите чистку под прямыми солнечными лучами или при повышенной температуре, так как после высыхания капель воды на поверхности могут остаться пятна.

# AXIS D2110-VE Security Radar

## Характеристики

### Характеристики

#### Общий вид устройства



- 1 Кнопка управления
- 2 Светодиодный индикатор сети
- 3 Светодиодный индикатор состояния
- 4 Светодиодный индикатор питания
- 5 Светодиодный индикатор выхода PoE
- 6 Слот для карты microSD
- 7 Разъем питания (для подключения источника питания пост. тока)
- 8 Разъем ввода-вывода
- 9 Разъем реле
- 10 Винт заземления
- 11 Сетевой разъем (вход PoE)
- 12 Сетевой разъем (выход PoE)
- 13 Датчик несанкционированного доступа

Технические характеристики см. в разделе *Характеристики* на стр. 53.

#### Индикаторы

Индикатор состояния	Индикация
Зеленый	Непрерывно горит зеленым – нормальный режим работы.

Индикатор сети	Индикация
Зеленый	Горит непрерывно – подключение к сети 100 Мбит/с. Мигает – осуществляется обмен данными по сети.

# AXIS D2110-VE Security Radar

## Характеристики

Желтый	Горит непрерывно – подключение к сети 10 Мбит/с. Мигает – осуществляется обмен данными по сети.
Не горит	Сетевое подключение отсутствует.

Индикатор питания	Индикация
Зеленый	Нормальный режим работы.

Светодиодный индикатор выхода PoE	Индикация
Не горит	Выход PoE выключен
Зеленый	Выход PoE включен

## Слот для SD-карты

Рекомендации по выбору карт SD можно найти на сайте [axis.com](http://axis.com).



Логотипы microSD, microSDHC и microSDXC являются товарными знаками компании SD-3C LLC. microSD, microSDHC, microSDXC являются товарными знаками или зарегистрированными товарными знаками компании SD-3C, LLC в США и(или) других странах.

## Кнопки

### Кнопка управления

Чтобы найти кнопку управления, см. раздел *Общий вид устройства на стр. 53*.

Кнопка управления служит для выполнения следующих действий.

- Сброс параметров изделия к заводским установкам. См. *стр. 49*.
- Подключение к сервису системы видеохостинга AXIS (AVHS). См. . Для подключения нажмите и удерживайте кнопку примерно 3 секунды, пока индикатор состояния не начнет мигать зеленым цветом.

## Разъемы

### Сетевой разъем

Разъем RJ45 Ethernet с поддержкой технологии Power over Ethernet Plus (PoE+).

#### **▲ОСТОРОЖНО**

Риск повреждения устройства. Не используйте для питания устройства одновременно PoE и источник питания постоянного тока.

### Сетевой разъем (выход PoE)

Технология Power over Ethernet, IEEE 802.3at, тип 2, макс. 30 Вт

Этот разъем можно использовать для подачи питания на другое устройство с поддержкой PoE, например на видеокамеру, рупорный громкоговоритель или на второй радар.

#### Примечание.

Выход PoE действует, если радар питается от инжектора на 60 Вт (Power over Ethernet, IEEE 802.3bt, тип 3).

# AXIS D2110-VE Security Radar

## Характеристики

### Примечание.

Если радар питается от инжектора на 30 Вт или источника постоянного тока, выход PoE отключен.

### Примечание.

Максимальная общая длина кабеля Ethernet составляет 100 метров для выхода и входа PoE. Кабель можно удлинить с помощью PoE-удлинителя.

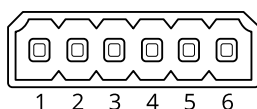
### Разъем ввода-вывода

Используйте разъем ввода-вывода для подключения внешних устройств, например для подачи сигналов тревоги и активации устройств по событиям. Помимо общей цепи 0 В пост. тока и питания (выход пост. тока) разъем ввода-вывода содержит контакты для следующих цепей ввода и вывода:

**Цифровой вход** – Для подключения устройств, которые способны размыкать и замыкать цепь, например пассивные ИК-датчики, дверные/оконные контакты и детекторы разбивания стекла.

**Цифровой выход** – Для подключения внешних устройств, например реле и светодиодных индикаторов. Подключенные устройства можно активировать по событию, с помощью прикладного программного интерфейса (API) VAPIX® или на веб-странице устройства.

6-контактная клеммная колодка

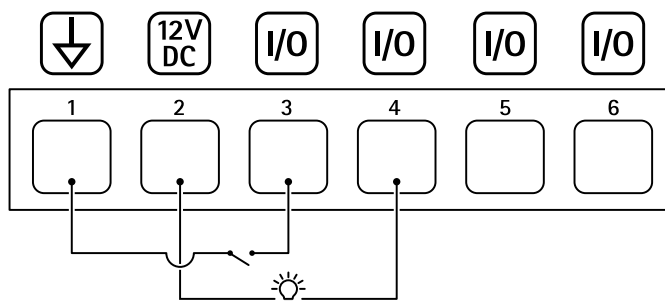


Функция	Контакт	Примечания	Технические характеристики
Заземление пост. тока	1		0 В пост. тока
Выход питания пост. тока	2	Может использоваться для питания дополнительного оборудования. Примечание. Этот контакт может использоваться только для подачи питания на внешние устройства.	12 В пост. тока Макс. нагрузка = 50 мА
Настраиваемый (вход или выход)	3-6	Цифровой вход: для активации подключить к контакту 1, для деактивации оставить свободным (неподключенным).	От 0 до макс. 30 В пост. тока
		Цифровой выход: в активном состоянии соединен с контактом 1 («земля» пост. тока) через внутреннюю цепь, в неактивном состоянии ни с чем не соединен. При подключении индуктивной нагрузки, например реле, параллельно нагрузке следует включить диод для защиты от переходных напряжений.	От 0 до макс. 30 В пост. тока, с открытым стоком, 100 мА

# AXIS D2110-VE Security Radar

## Характеристики

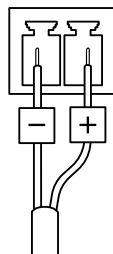
Пример



- 1 *Заземление пост. тока*
- 2 *Выход пост. тока: 12 В, макс. 50 мА*
- 3 *Вход-выход настроен как вход*
- 4 *Вход-выход настроен как выход*
- 5 *Настраиваемый вход-выход*
- 6 *Настраиваемый вход-выход*

### Разъем питания

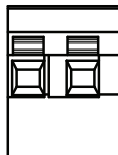
2-контактная клеммная колодка для подвода питания пост. тока. В целях безопасности используйте сверхнизковольтный (SELV) источник питания ограниченной мощности (LPS), у которого либо номинальная выходная мощность не превышает 100 Вт, либо номинальный выходной ток не превышает 5 А.



### ▲ОСТОРОЖНО

Риск повреждения устройства. Не используйте для питания устройства одновременно PoE и источник питания постоянного тока.

### Разъем реле



### ▲ОСТОРОЖНО

Используйте с разъемом реле только одножильные провода.

Функция	Технические характеристики
Тип	Нормально разомкнутый



## AXIS D2110-VE Security Radar

### Характеристики

---

Номинальные параметры	24 В пост. тока / 5 А
Изоляция от других цепей	2,5 кВ

