AXIS D2110-VE Security Radar

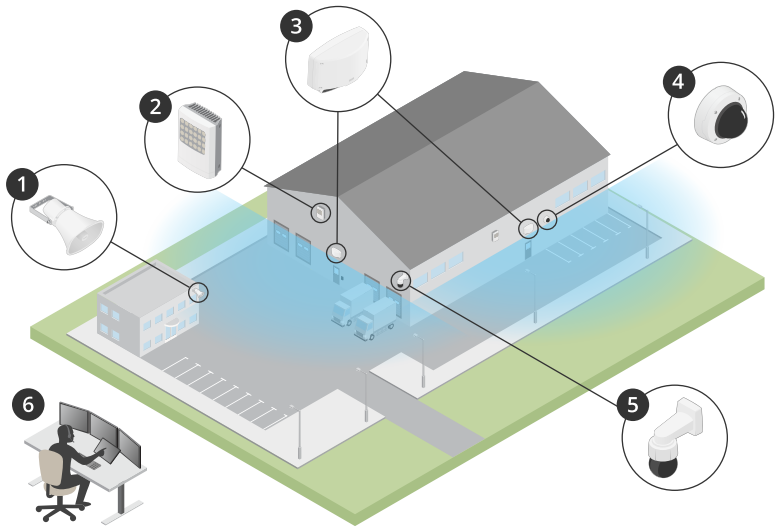
Manual do Usuário

Índice

Visão geral da solução 4
Perfis de radar 4
Onde instalar o produto 4
Área de cobertura 5
Perfil de monitoramento de áreas 6
Instalação de vários radares 6
Instalação de 2 – 3 radares na mesma zona de coexistência 6
Instalação de 4 – 6 radares na mesma zona de coexistência 6
Exemplos de instalação de área 7
Alcance da detecção de área 9
Casos de uso de monitoramento de áreas 11
Perfil de monitoramento de estradas 12
Exemplos de instalação em ruas e estradas 12
Alcance da detecção na estrada 12
Caso de uso de monitoramento de ruas e estradas 13
Início 15
Encontre o dispositivo na rede 15
Suporte a navegadores 15
Abra a interface web do dispositivo 15
Criar uma conta de administrador 15
Senhas seguras 15
Visão geral da interface Web 16
Configure seu dispositivo 17
Definir a altura de montagem 17
Calibrar um mapa de referência 17
Definir zonas de detecção 18
Adicionar cenários 18
Adicionar zonas de exclusão 19
Minimizar alarmes falsos 19
Exibição e gravação de vídeo 20
Redução de largura de banda e armazenamento 20
Configurar o armazenamento de rede 21
Como gravar e assistir vídeo 21
Controlar uma câmera PTZ com o radar 21
Controle uma câmera PTZ com o serviço de rastreamento automático de radar integrado 21
Controle uma câmera PTZ com o Auto-rastreador de Radar AXIS para PTZ 22
Configuração de regras de eventos 23
Acionar uma ação 23
Acionar uma notificação quando a caixa de proteção for aberta 23
Gravar vídeo de uma câmera quando um movimento é detectado 24
Acender uma luz quando um movimento é detectado 24
Enviar um email se alguém cobrir o radar com um objeto metálico 25
A interface Web 26
Status 26
Radar 27
Definições 27
Stream 29
Calibração do mapa 29
Zonas de exclusão 30
Cenários 31
Sobreposições 32
Rastreamento automático PTZ com radar: 34
Gravações 35

Apps 36
Sistema 36
Hora e local 36
Rede 38
Segurança 42
Contas 47
Eventos 50
MQTT 55
Armazenamento 58
Perfis de stream 60
ONVIF 61
Detectores 64
Acessórios 64
Edge-to-edge 64
Logs 66
Configuração simples 68
Manutenção 68
Manutenção 68
solução de problemas 69
Validar sua instalação 70
Validar a instalação do radar 70
Validar o radar 70
Concluir a validação 71
Saiba mais 72
Streaming e armazenamento 72
Formatos de compressão de vídeo 72
Controle de taxa de bits 72
Especificações 75
Visão geral do produto 75
..... 75
Indicadores de LED 75
..... 76
Slot de cartão SD 76
Botões 76
Botão de controle 76
Conectores 76
Conector de rede 76
Conector de rede (PoE out) 76
Conector de E/S 77
Conector de energia 78
Conector do relé 78
Limpeza do dispositivo 79
Solução de problemas 80
Redefinição para as configurações padrão de fábrica 80
Verificar a versão atual do AXIS OS 80
Atualizar o AXIS OS 80
Problemas técnicos, dicas e soluções 81
Considerações sobre desempenho 82

Visão geral da solução



1 *C1310-E Horn Speaker*
2 *Controle de porta*
3 *D2110-VE Security Radar*
4 *Câmera dome fixa*
5 *Câmera PTZ*
6 *Centro de monitoramento*

Perfis de radar

Observação

Para usar perfis de radar, seu dispositivo deverá estar executando o firmware versão 10.11 ou posterior. Vá para para atualizar seu firmware.

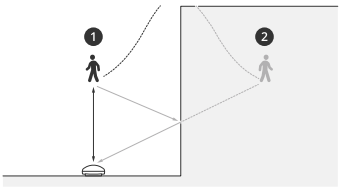
O manual do usuário é configurado para ajudar você a usar seu radar dependendo do que você deseja fazer. O AXIS D2110-VE Security Radar tem dois perfis:

- **Perfil de monitoramento de áreas** para rastrear objetos grandes e pequenos movendo-se em velocidades menores que 55 km/h (34 mph)
- **Perfil de monitoramento de estradas** para rastrear veículos que se movimentam a velocidades de até 105 km/h (65 mph)

Qualquer informação neste manual do usuário que não esteja sob um **Perfil de monitoramento de áreas** ou **Perfil monitoramento de estradas** é comum a ambos os perfis e pode ser consultada independentemente do que você usa.

Onde instalar o produto

- O radar destina-se ao monitoramento de áreas abertas. Qualquer objeto sólido (como uma parede, cerca, árvore ou arbusto grande) na área de cobertura criará um ponto cego (sombra de radar) atrás dele.
- Instale o radar em um poste estável ou em um ponto em uma parede onde não haja outros objetos ou instalações. Os objetos dentro de 1 m (3 pés) à esquerda e à direita do radar que refletem ondas de rádio afetam o desempenho do radar.
- Os objetos de metal no campo de visão causam reflexos que afetam a capacidade do radar de realizar classificações.



1 Detecção real
2 Detecção refletida (trilhas-fantasmas)

Para obter informações sobre como lidar com objetos reflexivos, consulte .

- Se desejar instalar mais de dois radares na mesma zona de coexistência, consulte .

Área de cobertura

O AXIS D2110-VE possui uma cobertura de área horizontal de 180°. A faixa de detecção corresponde a 5.600 m^2 (61.000 $pés^2$) para pessoas e 11.300 m^2 (122.000 $pés^2$) para veículos.

Observação

A cobertura de área ideal se aplica quando o radar é montado em 3,5 – 4 m (11 – 13 pés). A altura de montagem afetará o tamanho do ponto cego abaixo do radar.

Perfil de monitoramento de áreas

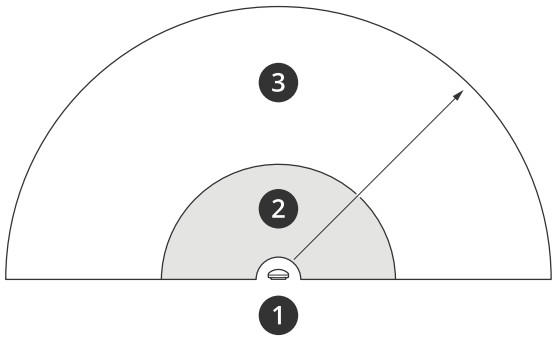
O **perfil de monitoramento de áreas** é otimizado para objetos que se movem a até 55 km/h (34 mph). Esse perfil permite detectar se um objeto é humano, veículo ou desconhecido. Uma regra pode ser configurada para acionar uma ação quando qualquer um desses objetos é detectado. Para rastrear veículos móveis em velocidades mais altas, use o .

Instalação de vários radares

Você pode instalar vários radares para cobrir áreas como os arredores de um edifício ou a zona de buffer do lado de fora de um cerca.

Coexistência

Quando você posiciona mais de dois radares na mesma zona de coexistência, as ondas de rádio dos radares dentro da zona podem causar interferência e afetar o desempenho. O raio da zona de coexistência é de 350 m (380 jardas).



1 Radar
2 Área de detecção
3 Zona de coexistência

Observação

O desempenho do radar na zona de coexistência também pode ser afetado pelo ambiente e/ou pela direção do radar em relação a cercas, edifícios ou radares vizinhos.

Instalação de 2 – 3 radares na mesma zona de coexistência

Quando dois ou três radares são colocados na mesma zona de coexistência, é necessário definir o número de radares vizinhos na interface do dispositivo. Isso ajuda a melhorar o desempenho dos radares e a evitar interferência.

1. Vá para **Radar > Settings > Coexistence (Radar > Configurações > Coexistência)**.
2. Selecione o número de radares vizinhos.

Consulte para obter exemplos de instalações com vários radares.

Instalação de 4 – 6 radares na mesma zona de coexistência

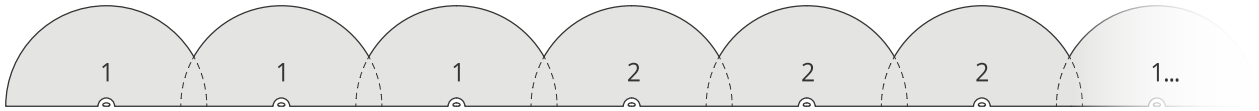
Observação

A opção para instalar até seis radares na mesma zona de coexistência está disponível no firmware versão 11.3.

Ao montar de quatro a seis radares na mesma zona de coexistência, defina primeiro o número de radares vizinhos e, em seguida, adicione cada radar a um grupo. Comece com o radar que está instalado mais longe, por exemplo, o mais afastado à sua esquerda. Adicione os radares em grupos de três e adicione os radares mais próximos uns dos outros no mesmo grupo.

Os radares dentro do grupo se sincronizarão uns aos outros para otimizar o desempenho e evitar interferência entre eles.

1. Vá para **Radar > Settings > Coexistence (Radar > Configurações > Coexistência)**.
2. Defina o número de radares vizinhos como **3–5**.
3. Selecione um grupo para seu radar.



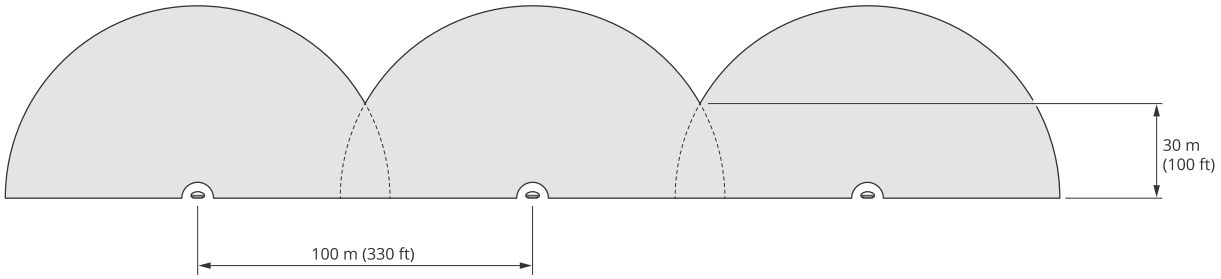
Este é um exemplo de como agrupar vários radares instalados lado a lado na mesma zona de coexistência.

Consulte para obter mais exemplos de instalações com vários radares.

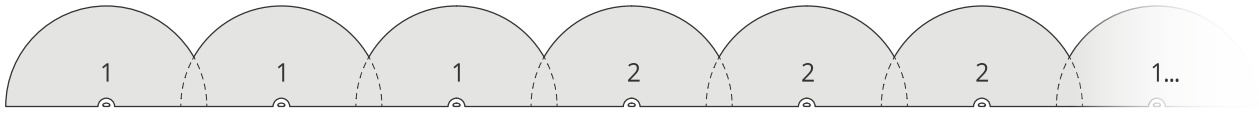
Exemplos de instalação de área

Criação de cercas virtuais com vários radares

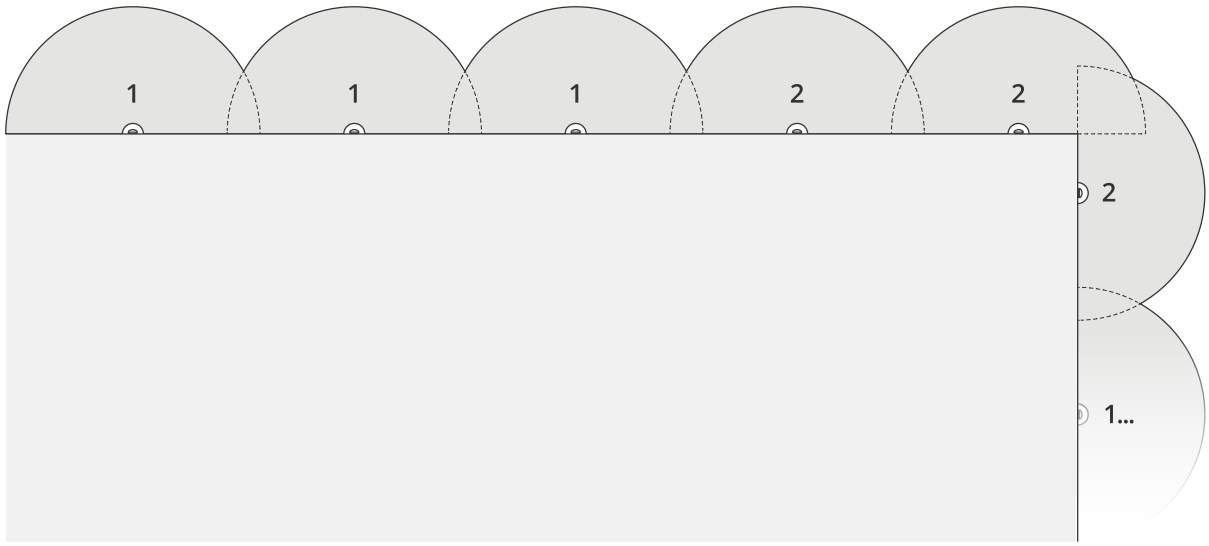
Para criar uma cerca virtual, por exemplo, ao longo ou ao redor de um edifício, é possível colocar vários radares lado a lado. Recomendamos colocá-los com espaçamento de 100 m (330 pés).



Para evitar interferências ao montar mais de dois radares na mesma zona de coexistência, defina o número de radares vizinhos na interface do dispositivo. Além disso, ao montar mais de três radares, adicione cada radar a um grupo.



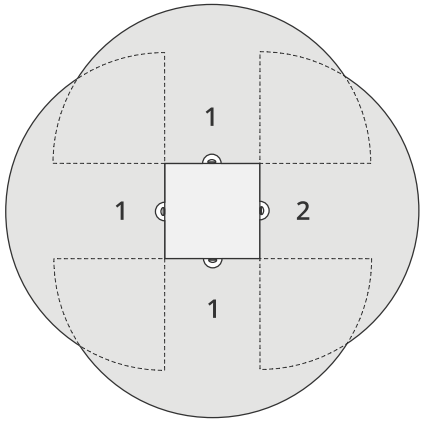
Você também pode ajustar a cerca virtual para cobrir quinas, como ilustrado neste exemplo.



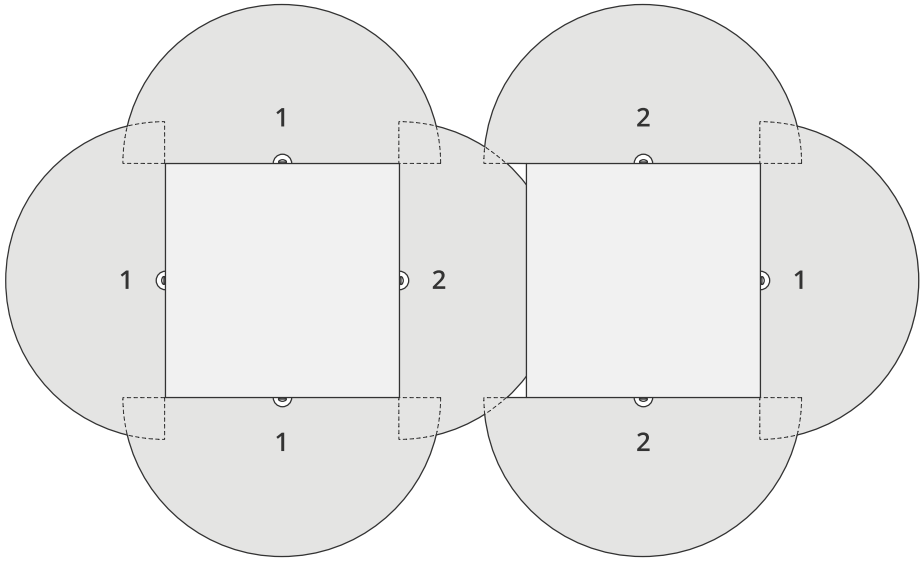
Consulte para obter mais informações sobre radares vizinhos e grupos.

Cobertura de uma área ao redor de um edifício

Para cobrir a área ao redor de um edifício, coloque os radares nas paredes do edifício voltados para fora. Se estiver colocando mais de três radares na mesma zona de coexistência, defina o número de radares vizinhos na interface do dispositivo e adicione cada radar a um grupo, conforme ilustrado neste exemplo.



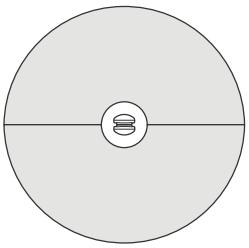
Você também pode cobrir a área ao redor de vários edifícios.

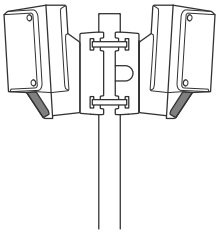


Consulte para obter mais informações sobre radares vizinhos e grupos.

Cobertura de uma área aberta

Para cobrir uma grande área aberta, use dois suportes para montagem em poste para colocar os dois radares um de costas para o outro.



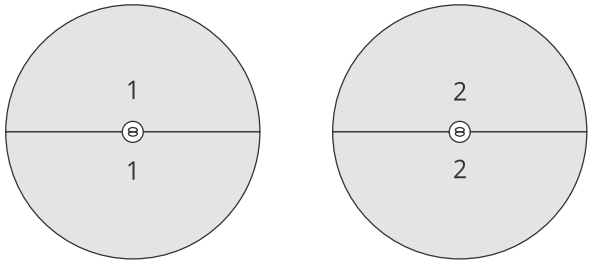


Você pode usar a saída PoE de um radar para alimentar o segundo radar, mas não é possível conectar um terceiro radar dessa forma.

Observação

A saída de PoE no radar é ativada quando o radar é alimentado por um midspan de 60 W.

Se você precisar de várias instalações de costas um para o outro na mesma zona de coexistência, defina o número de radares vizinhos na interface do dispositivo e adicione cada radar a um grupo para evitar interferência. Este é um exemplo de como você pode agrupar seus radares em uma instalação de costas um para o outro.



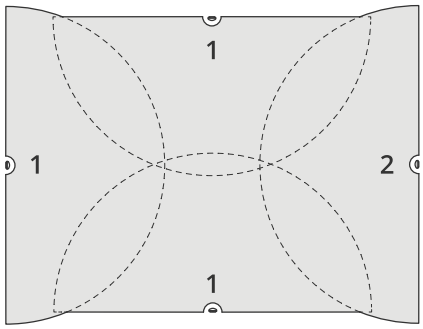
Consulte para obter mais informações sobre radares vizinhos e grupos.

Instalação de vários radares voltados uns para os outros

Em geral, não é recomendável instalar mais de três radares voltados uns para os outros, pois isso aumenta o risco de interferência entre eles. No entanto, em algumas áreas específicas, isso pode ser necessário. Se desejar cobrir um campo de futebol por exemplo, você não poderá colocar os radares no meio do campo.

Se você instalar mais de três radares voltados uns para os outros, a distância mínima de um radar para o outro deverá ser de 40 metros (130 pés). Além disso, é especialmente importante definir o número de radares vizinhos na interface do dispositivo e adicionar cada radar a um grupo. Isso ajudará a melhorar o desempenho dos radares.

Este é um exemplo de como agrupar quatro radares que cobrem um campo.



Consulte para obter mais informações sobre radares vizinhos e grupos.

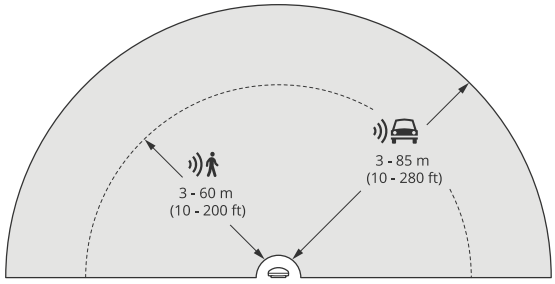
Alcance da detecção de área

O alcance de detecção é a distância na qual um objeto pode ser rastreado e acionar um alarme. Ele é medido de um **limite de detecção próximo** (o quanto perto do dispositivo é possível fazer uma detecção) até um **limite de detecção distante** (o quanto longe do dispositivo é possível fazer uma detecção).

No entanto, o **perfil de monitoramento de áreas** é otimizado para a detecção de pessoas. No entanto, ele também permite que você rastreie veículos e outros objetos se movendo até 55 km/h (34 mph) com precisão de velocidade +/-2 km/h (1,24 mph).

Quando montado na altura de instalação ideal, os intervalos de detecção são:

- **3 – 60 m (10 – 200 pés)** ao detectar uma pessoa
- **3 – 85 m (10 – 280 pés)** ao detectar um veículo



Observação

- Se você instalar o radar em uma altura diferente, insira a altura de montagem real nas páginas Web do produto ao calibrar o radar.
- O alcance de detecção é afetado pela cena.
- O alcance de detecção é afetado por radares vizinhos.
- O alcance de detecção é afetado pelo tipo de objeto.

O alcance de detecção foi medido sob estas condições:

- O alcance foi medido ao longo do solo.
- O objeto era uma pessoa com 170 cm (5 pés 7 pol.) de altura.
- A pessoa estava caminhando diretamente na frente do radar.
- Os valores são medidos quando a pessoa entra na zona de detecção.
- A sensibilidade do radar foi definida como **Medium (Média)**.

Altura de montagem	Tilt de 0°	Inclinação de 10°	Tilt de 20°
2,5 m (8,2 pés)	3,0–60 m (9,8–197 pés)	Não recomendadas	Não recomendadas
3,5 m (11 pés)	3,0–60 m (9,8–197 pés)	Não recomendadas	Não recomendadas
4,5 m (15 pés)	4,0–60 m (13–197 pés)	Não recomendadas	Não recomendadas
5,5 m (18 pés)	7,5–60 m (25–197 pés)	Não recomendadas	Não recomendadas
6,5 m (21 pés)	7,5–60 m (25–197 pés)	5,5–60 m (18–197 pés)	Não recomendadas
8 m (26 pés)	Não recomendadas	9–60 m (30–197 pés)	7,5–30 m (25–98 pés)
10 m (33 pés)	Não recomendadas	15–60 m (49–197 pés)	9–35 m (30–115 pés)
12 m (39 pés)	Não recomendadas	23–60 m (75–197 pés)	13–38 m (43–125 pés)
14 m (36 pés)	Não recomendadas	27–60 m (89–197 pés)	17–35 m (56–115 pés)
16 m (52 pés)	Não recomendadas	Não recomendadas	25–50 m (82–164 pés)

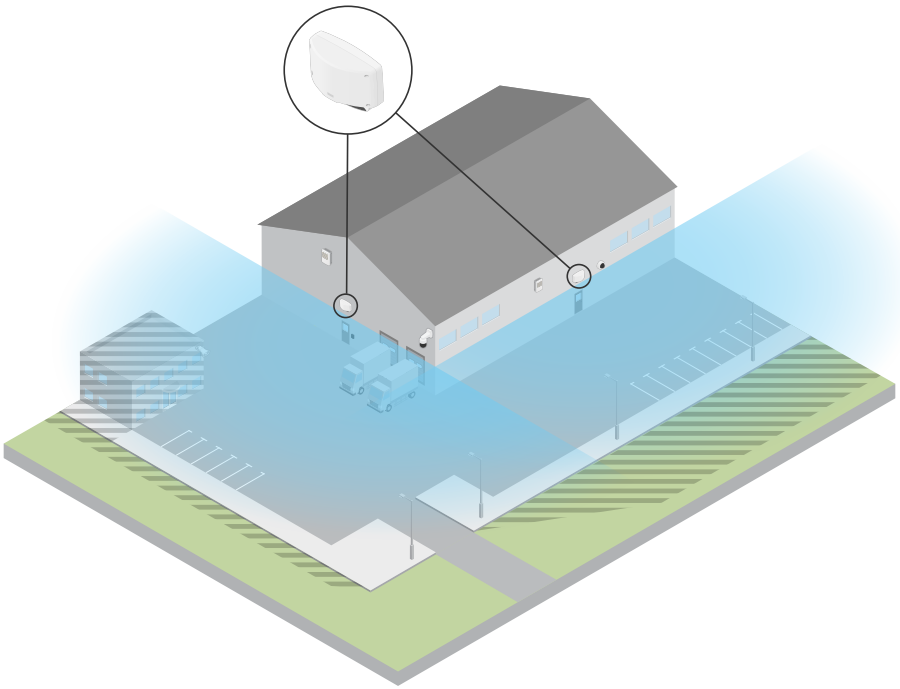
Casos de uso de monitoramento de áreas

Cobertura de área de piscina

Uma piscina pública estava sofrendo uma série de invasões após o horário de funcionamento. Devido à natureza privada dos negócios, os proprietários não podem instalar videomonitoramento. Eles optaram por instalar um radar e configurá-lo no **Area monitoring profile (Perfil de monitoramento de áreas)**. O radar é montado no edifício e cobre toda a piscina, bem como toda a área ao seu redor. Ele aciona um aviso de um alto-falante quando uma pessoa é detectada entre os horários de encerramento às 20h e abertura às 6h do dia seguinte.

Cobertura de uma área ao redor de um edifício

Uma fábrica de produtos químicos adiciona outra camada de segurança ao sistema usando radares para cobrir a área em volta de um prédio sensível. O sistema de segurança já inclui câmeras, câmeras térmicas e controladores de portas. Os radares podem acionar eventos que fazem com que as câmeras acompanhem o invasor, aproximem a imagem e registrem atividades. Os sinalizadores piscantes, vinculados às câmeras térmicas, são acionados para piscar para que o intruso saiba que a área está protegida. E os controladores de portas podem restringir o acesso. Os radares ajudam o sistema de defesa a entrar em ação muito antes que o invasor atinja o prédio protegido.



Cobertura de uma grande área aberta

O número de arrombamentos de veículos em um estacionamento do lado de fora de um pequeno shopping center aumentou fora do horário de funcionamento. Eles contam com a presença de um guarda de segurança nesse horário, mas acham que precisam reforçar a segurança à noite, sem incorrer no custo adicional de contratar mais funcionários. Eles decidiram instalar dois radares de segurança, no **Area monitoring profile (Perfil de monitoramento de áreas)** montados de costas um para o outro para cobrir toda a área do estacionamento. Os radares são configurados para alertar o guarda de segurança sobre comportamentos suspeitos para que eles possam investigar a cena. Eles também poderiam instalar um alto-falante tipo corneta acionado pelos radares para reproduzir um alerta que talvez consiga impedir a ação dos ladrões.

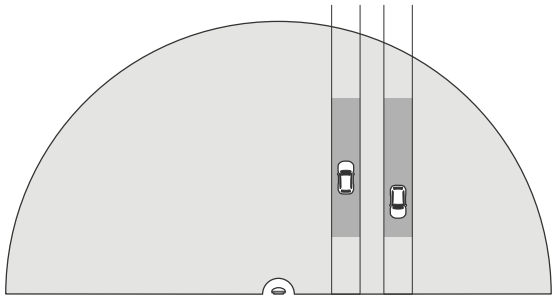
Perfil de monitoramento de estradas

O **Road monitoring profile (Perfil de monitoramento de estradas)** é melhor usado para acompanhar veículos em movimento a até 105 km/h (65 mph) em zonas urbanas, zonas fechadas e em estradas suburbanas. Este modo não deve ser usado para a detecção de pessoas ou outros tipos de objetos. Para rastrear objetos diferentes de veículos, use seu radar no .

Exemplos de instalação em ruas e estradas

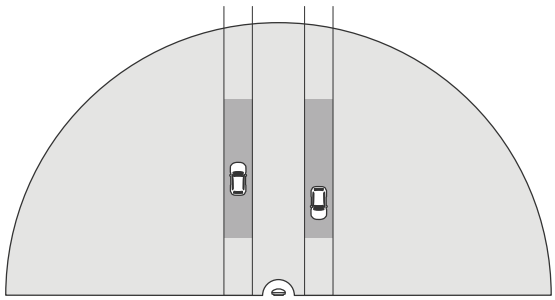
Montagem lateral

Para monitorar veículos viajando ao longo de uma rua ou estrada, você pode montar o radar na lateral da via. O radar fornecerá uma distância de cobertura lateral de 10 m (32 pés).



Montagem central

Essa opção de montagem requer uma posição estável. O radar pode ser montado em um poste no meio da estrada ou em uma ponte acima da estrada. O radar fornecerá uma distância de cobertura lateral de 10 m (32 pés) para ambos os lados do radar. O radar cobre uma distância lateral mais ampla quando é montado no centro.



Observação

Recomenda-se que o radar seja montado a uma altura entre 3 m (10 pés) e 8 m (26 pés) para o **Road monitoring profile (Perfil de monitoramento de estradas)**.

Alcance da detecção na estrada

O alcance de detecção é a distância na qual um objeto pode ser rastreado e acionar um alarme. Ele é medido de um **limite de detecção próximo** (o quanto perto do dispositivo é possível fazer uma detecção) até um **limite de detecção distante** (o quanto longe do dispositivo é possível fazer uma detecção).

Este perfil é otimizado para detecção de veículos e produzirá uma precisão de velocidade de +/-2 km/h (1,24 mph) ao monitorar veículos em movimento a até 105 km/h (65 mph).

Alcance da detecção quando o radar é montado em uma altura de instalação ideal:

- **25 – 70 m (82 – 229 pés)** para veículos em movimento a 60 km/h (37 mph).
- **30 – 60 m (98 – 196 pés)** para veículos em movimento a 105 km/h (65 mph).

Caso de uso de monitoramento de ruas e estradas

Regulando veículos em zonas de baixa velocidade

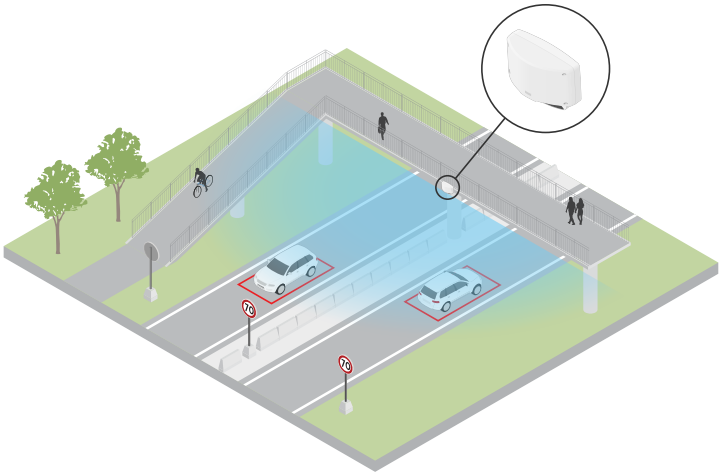
Um complexo industrial com uma grande rua entre dois armazéns instalou um radar para ajudar a reforçar o limite de velocidade de 60 km/h (37 mph). No **Road monitoring profile (Perfil de monitoramento de estradas)**, o radar pode detectar quando um veículo em sua zona de detecção excede essa velocidade. Ele, em seguida, aciona um evento que envia notificações por email para motoristas e gerentes. O lembrete ajuda a aumentar a conformidade com as restrições de velocidade.

Veículos indesejados em uma estrada fechada

Uma pequena estrada para a antiga pedreira foi fechada. No entanto, denúncias de veículos trafegando na estrada fizeram com que as autoridades instalassem um radar de segurança no **Road monitoring profile (Perfil de monitoramento de estradas)**. O radar é montado ao longo da estrada e cobre toda a largura da via. Sempre que um veículo entra no cenário, ele aciona um sinalizador piscante que avisa os motoristas para deixar a estrada. Ele também envia uma mensagem para a equipe de segurança para que eles possam enviar uma unidade, se necessário.

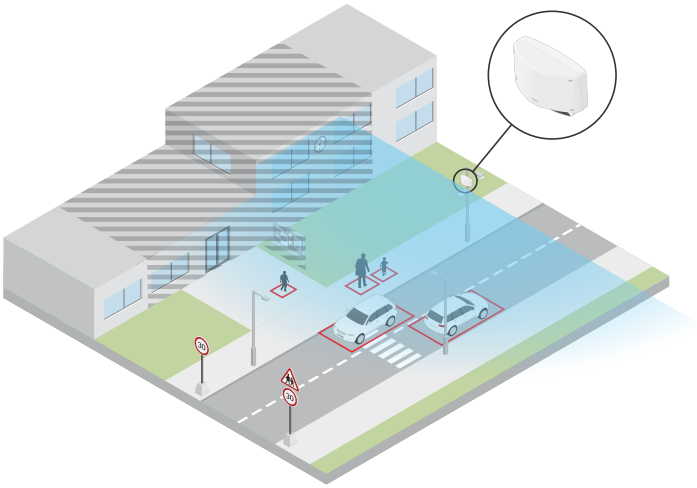
Conscientização de velocidade na estrada

Uma estrada que atravessa uma pequena cidade tem alguns incidentes de excesso de velocidade. Para reforçar o limite de velocidade de 70 km/h (43 mph), o controle de tráfego instalou um radar de segurança no **Road monitoring profile (Perfil de monitoramento de estrada)** em uma ponte que cruza a estrada. Isso permitiu a eles detectar a velocidade em que os veículos estão trafegando e monitorar quando deveriam ter unidades estacionadas ao longo da estrada para controlar o tráfego.



Segurança com pessoas e veículos

A equipe na escola identificou dois problemas de segurança que gostariam de abordar. Eles já experimentaram visitantes indesejados que entram em instalações durante o dia escolar, bem como veículos manipulando a zona de baixa velocidade de 20 km/h (12 mph) fora da escola. O radar é montado em um poste, próximo ao caminho de pedestres. O foi escolhido, pois ele permite que o radar rastreie pessoas e veículos se movendo em velocidades menores que 55 km/h (34 mph). Isso ajuda a equipe a acompanhar as pessoas que entram e saem no horário escolar e permite acionar um alto-falante para avisar os pedestres quando um veículo se aproxima rápido demais.



Início

Encontre o dispositivo na rede

Para encontrar dispositivos Axis na rede e atribuir endereços IP a eles no Windows®, use o AXIS IP Utility ou o AXIS Device Manager. Ambos os aplicativos são grátis e podem ser baixados de *axis.com/support*.

Para obter mais informações sobre como encontrar e atribuir endereços IP, acesse *Como atribuir um endereço IP e acessar seu dispositivo*.

Suporte a navegadores

O dispositivo pode ser usado com os seguintes navegadores:

	Chrome™	Firefox®	Edge™	Safari®
Windows®	recomendada	✓	recomendada	
macOS®	recomendada	✓	recomendada	✓*
Linux®	recomendada	✓	recomendada	
Outros sistemas operacionais	✓	✓	✓	✓

*Não é totalmente compatível. Se tiver problemas com o streaming de vídeo, use um navegador diferente.

Abra a interface web do dispositivo

1. Abra um navegador e digite o endereço IP ou o nome de host do dispositivo Axis.
   Se você não souber o endereço IP, use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede.
2. Digite o nome de usuário e a senha. Se você acessar o dispositivo pela primeira vez, você deverá criar uma conta de administrador. Consulte .

Para obter descrições de todos os controles e opções presentes na interface Web do dispositivo, consulte .

Criar uma conta de administrador

Na primeira vez que fizer login no dispositivo, você deverá criar uma conta de administrador.

1. Insira um nome de usuário.
2. Insira uma senha. Consulte .
3. Insira a senha novamente.
4. Aceite o contrato de licença.
5. Clique em **Add account (Adicionar conta)**.

Importante

O dispositivo não possui conta padrão. Se você perder a senha da sua conta de administrador, deverá redefinir o dispositivo. Consulte .

Senhas seguras

Importante

Use HTTPS (que é ativado por padrão) para definir sua senha ou outras configurações confidenciais pela rede. O HTTPS permite conexões de rede seguras e criptografadas, o que protege dados confidenciais, como senhas.

A senha do dispositivo é a proteção primária para seus dados e serviços. Os dispositivos Axis não impõem uma política de senhas, pois os produtos podem ser usados em vários tipos de instalações.

Para proteger seus dados, recomendamos enfaticamente que você:

- Use uma senha com pelo menos 8 caracteres, preferencialmente criada por um gerador de senhas.
- Não exponha a senha.
- Altere a senha em um intervalo recorrente pelo menos uma vez por ano.

Visão geral da interface Web

Este vídeo oferece uma visão geral sobre a interface Web do dispositivo.

Interface Web de um dispositivo Axis

Configure seu dispositivo

Definir a altura de montagem

Configure a altura de montagem do radar na interface web. Isso ajuda o radar a detectar e medir corretamente a velocidade dos objetos que passam.

Meça a altura do chão até o radar com a maior precisão possível. Para cenas com superfícies desiguais, defina o valor que representa a altura média na cena.

1. Acesse **Radar > Settings > General (Radar > Configurações > Geral)**.
2. Defina a altura sob **Mounting height (Altura de montagem)**.

Calibrar um mapa de referência

Faça upload de um mapa de referência para facilitar a visualização de onde os objetos detectados estão se movendo. Você pode usar uma planta ou uma foto aérea que mostre a área coberta pelo radar. Calibre o mapa para que a cobertura do radar se ajuste à posição, à direção e à escala do mapa, e faça zoom no mapa se estiver interessado em uma parte específica da cobertura do radar.

Você pode usar um assistente de configuração que o orienta passo a passo na calibração do mapa ou editar cada configuração individualmente.

Use o assistente de configuração:

1. Vá para **Radar > Map calibration (Radar > Calibração do mapa)**.
2. Clique em **Assistente de configuração** e siga as instruções.

Para remover o mapa carregado e as configurações que você adicionou, clique em **Redefinir calibração**.

Edite cada configuração individualmente:
O mapa será calibrado gradualmente após o ajuste de cada configuração.

1. Vá para **Radar > Map calibration > Map (Radar > Calibração do mapa > Mapa)**.
2. Selecione a imagem que deseja carregar ou arraste e solte-a na área desenhada.
   Para reutilizar uma imagem de mapa com suas configurações atuais de panning e zoom, clique em **Download map (Baixar mapa)**.
3. Em **Rotate map (Girar mapa)**, use o controle deslizante para girar o mapa na posição.
4. Acesse **Scale and distance on a map (Escala e distância em um mapa)** e clique em dois pontos pré-determinados no mapa.
5. Em **Distance (Distância)**, adicione a distância real entre os dois pontos que você adicionou ao mapa.
6. Acesse **Pan and zoom map (Mapa de pan e zoom)** e use os botões para fazer uma panorâmica da imagem do mapa, ou ampliar e diminuir a imagem do mapa.

Observação

A função de zoom não altera a área de cobertura do radar. Mesmo que partes da cobertura estejam fora de visualização após o zoom, o radar ainda detectará objetos em movimento em toda a área de cobertura. A única maneira de excluir movimentos detectados é adicionar zonas de exclusão. Para obter mais informações, consulte .

7. Acesse **Radar position (Posição do radar)** e use os botões para mover ou girar a posição do radar no mapa.

Para remover o mapa carregado e as configurações que você adicionou, clique em **Redefinir calibração**.

O vídeo mostra um exemplo de como calibrar um mapa de referência em um radar Axis ou em uma câmera de fusão de radar-vídeo.

Definir zonas de detecção

Para determinar onde detectar o movimento, você pode adicionar uma ou mais zonas de detecção. Use zonas diferentes para disparar ações diferentes.

Há dois tipos de zonas:

- Um **scenario (cenário)** (anteriormente chamado de zona de inclusão) é uma área na qual objetos em movimento acionam regras. O cenário padrão é compatível com a área inteira coberta pelo radar.
- Uma **exclude zone (zona de exclusão)** é uma área na qual objetos em movimento serão ignorados. Use zonas de exclusão se houver áreas dentro de um cenário que disparem muitos alarmes indesejados.

Adicionar cenários

Um cenário é uma combinação de condições de acionamento e configurações de detecção, que você pode usar para criar regras no sistema de eventos. Adicione cenários se você deseja criar regras diferentes para diferentes partes da cena.

Adicionar um cenário:

1. vá para **Radar > Scenarios (Radar > Cenários)**.
2. Clique em **Add scenario (Adicionar cenário)**.
3. Digite o nome do cenário.
4. Selecione se deseja acionar em situações em que objetos se movem em uma área ou cruzam uma ou duas linhas.

Acionar em objetos que se movem em uma área:

1. Selecione **Movement in area (Movimento na área)**.
2. Clique em **Next** (Próximo).
3. Selecione o tipo da zona que deve ser incluída no cenário.
   Use o mouse para mover e reformatar a zona de forma que ela abranja a parte desejada da imagem do radar ou mapa de referência.
4. Clique em **Next** (Próximo).
5. Adicionar configurações de detecção.

1. Adicione os segundos antes de acionar em **Ignore short-lived objects (Ignorar objetos de curta duração)**.
2. Selecione o tipo de objeto a ser acionado em **Trigger on object type (Acionar com tipo de objeto)**.
3. Adicione um alcance para o limite de velocidade em **Speed limit (Limite de velocidade)**.

6. Clique em **Next** (Próximo).
7. Defina a duração mínima do alarme sob **Minimum trigger duration (Duração mínima do acionador)**.
8. Clique em **Salvar**.

Acionar quando objetos cruzam uma linha:

1. Selecione **Line crossing (Cruzamento de linha)**.
2. Clique em **Next** (Próximo).
3. Posicione a linha na cena.
   Use o mouse para mover e dimensionar a linha.
4. Para alterar a direção de detecção, ative a opção **Change direction (Alterar direção)**.
5. Clique em **Next** (Próximo).
6. Adicionar configurações de detecção.
   6.1. Adicione os segundos antes de acionar em **Ignore short-lived objects (Ignorar objetos de curta duração)**.

6.2. Selecione o tipo de objeto a ser acionado em **Trigger on object type (Acionar com tipo de objeto)**.

6.3. Adicione um alcance para o limite de velocidade em **Speed limit (Limite de velocidade)**.

7. Clique em **Next** (Próximo).
8. Defina a duração mínima do alarme sob **Minimum trigger duration (Duração mínima do acionador)**. O valor padrão é definido como 2 segundos. Se desejar que o cenário seja acionado toda vez que um objeto cruzar a linha, reduza a duração para 0 segundos.
9. Clique em **Salvar**.

Acionar quando objetos cruzam duas linhas:

1. Selecione **Line crossing (Cruzamento de linha)**.
2. Clique em **Next** (Próximo).
3. Para fazer o objeto cruzar duas linhas para o alarme ser acionado, ative **Require crossing of two lines (Exigir o cruzamento de duas linhas)**.
4. Posicione as linhas na cena.
   Use o mouse para mover e dimensionar a linha.
5. Para alterar a direção de detecção, ative a opção **Change direction (Alterar direção)**.
6. Clique em **Next** (Próximo).
7. Adicionar configurações de detecção.
   7.1. Defina o limite de tempo entre cruzar a primeira e a segunda linhas em **Max time between crossings (Tempo máximo entre cruzamentos)**.

   7.2. Selecione o tipo de objeto a ser acionado em **Trigger on object type (Acionar com tipo de objeto)**.

   7.3. Adicione um alcance para o limite de velocidade em **Speed limit (Limite de velocidade)**.
8. Clique em **Next** (Próximo).
9. Defina a duração mínima do alarme sob **Minimum trigger duration (Duração mínima do acionador)**. O valor padrão é definido como 2 segundos. Se desejar que o cenário seja acionado toda vez que um objeto cruzar as duas linhas, reduza a duração para 0 segundos.
10. Clique em **Salvar**.

Adicionar zonas de exclusão

Zonas de exclusão são áreas na qual objetos em movimento serão ignorados. Adicione zonas de exclusão para ignorar, por exemplo, folhas oscilantes na lateral de uma estrada. Você também pode adicionar zonas de exclusão para ignorar trilhas-fantasmas causadas por materiais reflexivos por radar, por exemplo, uma cerca de metal.

Adicionar uma zona de exclusão:

1. vá para **Radar > Exclude zones (Radar > Zonas de exclusão)**.
2. Clique em **Add exclude zone (Adicionar zona de exclusão)**.
   Use o mouse para mover e reformatar a zona de forma que ela abranja a parte desejada da exibição do radar ou mapa de referência.

Minimizar alarmes falsos

Se você observar muitos alarmes falsos, filtre determinados tipos de movimento ou objetos, altere a cobertura ou ajuste a sensibilidade da detecção. Veja quais configurações funcionam melhor para seu ambiente.

- Ajuste a sensibilidade da detecção do radar:
  Vá para **Radar > Settings > Detection (Radar > Configurações > Detecção)** e selecione uma **Detection sensitivity (Sensibilidade de detecção)** menor. Isso reduz o risco de alarmes falsos, mas também pode fazer com que o radar perca algum movimento.
  A configuração de sensibilidade afeta todas as zonas.

  - **Baixa**: Use essa sensibilidade quando houver muitos objetos de metal ou veículos grandes na área. Mais tempo será necessário para que o radar rastreie e classifique objetos. Isso pode reduzir o alcance de detecção, especialmente para objetos em movimento rápido.
  - **Medium (Média)**: Esta é a configuração padrão.
  - **Alta**: Use essa sensibilidade quando houver um campo aberto sem objetos metálicos na frente do radar. Isso aumentará o alcance de detecção para pessoas.
- Modifique os cenários e zonas de exclusão:
  Se o cenário contiver superfícies rígidas, como uma parede metálica, reflexos poderão causar várias detecções para um único objeto físico. Você pode modificar a forma do cenário ou adicionar uma zona de exclusão que ignora determinadas partes do cenário. Para obter mais informações, consulte e .
- Acionador para objetos que cruzam duas linhas em vez de uma:
  Se um cenário de cruzamento de linhas incluir objetos balançando ou animais se movendo, há o risco de um objeto cruzar a linha e acionar um alarme falso. Nesse caso, você pode configurar o cenário para acionar somente quando um objeto cruzar duas linhas. Para obter mais informações, consulte .
- Filtragem ao movimentar:
  - Vá para **Radar > Settings > Detection (Radar > Configurações > Detecção)** e selecione **Ignore swaying objects (Ignorar objetos balançando)**. Esta configuração minimiza alarmes falsos gerados por árvores, arbustos e mastros de bandeiras na zona de cobertura.
  - Vá para **Radar > Settings > Detection (Radar > Configurações > Detecção)** e selecione **Ignore small objects (Ignorar objetos pequenos)**. Essa configuração está disponível no perfil de monitoramento de área e minimiza alarmes falsos de pequenos objetos na zona de cobertura, como gatos e coelhos.
- Filtragem com base em tempo:
  - vá para **Radar > Scenarios (Radar > Cenários)**.
  - Selecione um cenário e clique em ⋮ para modificar suas configurações.
  - Selecione um valor mais alto em **Seconds until trigger (Segundos até o acionamento)**. Este é o tempo de retardo entre o radar começar a acompanhar um objeto e acionar um alarme. O temporizador começa quando o radar detecta o objeto pela primeira vez, e não quando o objeto entra na zona especificada no cenário.
- Filtragem com base no tipo de objeto:
  - vá para **Radar > Scenarios (Radar > Cenários)**.
  - Selecione um cenário e clique em ⋮ para modificar suas configurações.
  - Para evitar acionar tipos de objetos específicos, desmarque os tipos de objetos que não deveriam acionar eventos no cenário.

Exibição e gravação de vídeo

Esta seção contém instruções sobre como configurar um dispositivo. Para saber mais sobre como o streaming e o armazenamento funcionam, acesse .

Redução de largura de banda e armazenamento

Importante

A redução da largura de banda pode resultar em perda de detalhes na imagem.

1. Vá para **Radar > Stream**.
2. Clique em na visualização ao vivo.
3. Selecione o **Video format (Formato de vídeo) H.264**.
4. Vá para **Radar > Stream > General (Vídeo > Sistema > Geral)** e aumente **Compression (Compactação)**.

Observação

A maioria dos navegadores da Web não oferece suporte à decodificação H.265. Por isso, o dispositivo não é compatível com essa decodificação em sua interface da Web. Em vez disso, você pode usar um aplicativo ou sistema de gerenciamento de vídeo compatível com a decodificação H.265.

Configurar o armazenamento de rede

Para armazenar registros na rede, você precisa configurar o seu armazenamento de rede.

1. Vá para **System > Storage (Sistema > Armazenamento)**.
2. Clique em + **Add network storage (Adicionar armazenamento de rede)** em **Network storage (Armazenamento de rede)**.
3. Digite o endereço IP do servidor host.
4. Digite o nome do local compartilhado no servidor host em **Network share (Compartilhamento de rede)**.
5. Digite o nome de usuário e a senha.
6. Selecione a versão SMB ou deixe em **Auto**.
7. Selecione **Add share without testing (Adicionar compartilhamento sem testar)** se você experimentar problemas de conexão temporários ou se o compartilhamento ainda não tiver sido configurado.
8. Clique em **Adicionar**.

Como gravar e assistir vídeo

Gravar vídeo diretamente do radar

1. Vá para **Radar > Stream**.
2. Para iniciar uma gravação, clique em .

   Se você não configurou nenhum armazenamento, clique em e em . Para obter instruções sobre como configurar o armazenamento de rede, consulte
3. Para interromper a gravação, clique em novamente.

Assista ao vídeo

1. Vá para **Recordings (Gravações)**.
2. Clique em para obter sua gravação na lista.

Controlar uma câmera PTZ com o radar

É possível usar as informações sobre as posições dos objetos do radar para fazer uma câmera PTZ acompanhar objetos. Há duas formas de fazer isso:

- . A opção embutida é adequada quando você tem uma câmera PTZ e radar montados muito de perto.
- . O aplicativo Windows é adequado quando você quer usar várias câmeras PTZ e radares para acompanhar objetos.

Observação

Use um servidor NTP para sincronizar a hora nas câmeras, nos radares e no computador Windows. Se os relógios estiverem fora de sincronismo, você poderá enfrentar atrasos no rastreamento ou rastreamento de fantasmas.

Controle uma câmera PTZ com o serviço de rastreamento automático de radar integrado

O rastreamento automático de radar integrado cria uma solução de ponta a ponta em que o radar controla diretamente a câmera PTZ. Ele é compatível com todas as câmeras PTZ Axis.

Observação

Você pode usar o serviço de rastreamento automático de radar integrado para conectar um radar a uma câmera PTZ. Para uma configuração em que se deseja usar mais de um radar ou câmera PTZ, use o Auto--rastreador de Radar AXIS para PTZ. Para obter mais informações, consulte .

Esta instrução explica como emparelhar o radar com uma câmera PTZ, como calibrar os dispositivos e como configurar o rastreamento de objetos.

Antes de começar:

- Defina a área de interesse e evite alarmes indesejados configurando zonas de exclusão no radar. Certifique-se de excluir zonas com materiais que refletem o radar ou objetos balançando, como folhagens, para impedir que a Câmera PTZ rastreie objetos irrelevantes. Para obter instruções, consulte .

Emparelhe o radar com a câmera PTZ:

1. Vá para **System > Edge-to-edge > Pareamento PTZ**.
2. Insira o endereço IP, nome de usuário e senha para a câmera PTZ.
3. Clique em **Conectar**.
4. Clique em **Configure Radar autotracking (Configurar rastreamento automático por radar)** ou vá para **Radar > Radar PTZ autotracking (Radar > Rastreamento automático PTZ com radar)** para configurar o rastreamento automático com radar.

Calibre o radar e a câmera PTZ:

5. Vá para **Radar > Radar PTZ autotracking (Radar > Rastreamento automático PTZ com radar)**.
6. Para definir a altura de montagem da câmera, vá para **Altura de montagem da câmera**.
7. Para colocar a câmera PTZ de modo panorâmico para que ela aponte na mesma direção do radar, vá para **Alinhamento de panorâmica**.
8. Se você precisar ajustar a inclinação para compensar um terreno irregular, vá para **Deslocamento de inclinação de solo** e adicione um deslocamento em graus.

Configure o rastreamento de PTZ:

9. Vá para **Rastrear** para selecionar se deseja rastrear humanos, veículos e/ou objetos desconhecidos.
10. Para começar a rastrear objetos com a câmera PTZ, ligue o **Rastreamento**.
    O rastreamento ampliará automaticamente um objeto ou grupo de objetos para mantê-los na exibição da câmera.
11. Ligue a **Troca de objeto** se esperar vários objetos que não caberiam na visão da câmera.
    Com essa configuração, o radar dá prioridade aos objetos a serem rastreados.
12. Para determinar quantos segundos rastrear cada objeto, defina o **Tempo de espera do objeto**.
13. Para fazer a câmera PTZ retornar para sua posição inicial quando o radar não estiver mais rastreando objetos, ative a opção **Retornar para posição inicial**.
14. Para determinar por quanto tempo a câmera PTZ deve permanecer na última posição conhecida dos objetos rastreados antes de voltar para a posição inicial, defina o **Tempo limite de retornar para a posição inicial**.
15. Para ajustar o zoom da câmera PTZ, ajuste o zoom no controle deslizante.

Controle uma câmera PTZ com o Auto-rastreador de Radar AXIS para PTZ

O Auto-rastreador de Radar AXIS para PTZ é uma solução baseada em servidor que pode lidar com diferentes configurações ao rastrear objetos:

- Controle várias câmeras PTZ com um radar.
- Controle uma câmera PTZ com vários radares.
- Controle várias câmeras PTZ com vários radares.
- Controle uma câmera PTZ com um radar quando elas são montadas em diferentes posições que cobrem a mesma área.

O aplicativo é compatível com um conjunto específico de câmeras PTZ. Para mais informações, veja *axis.com/ /products/axis-radar-autotracking-for-ptz#compatible-products*.

Baixe o aplicativo e consulte o manual do usuário para obter informações sobre como configurar o aplicativo. Para mais informações, veja *axis.com/products/axis-radar-autotracking-for-ptz/support*.

Configuração de regras de eventos

Para saber mais, consulte nosso guia *Introdução a regras de eventos*.

Acionar uma ação

1. vá para **System > Events (Sistema > Eventos)** e adicione uma regra. A regra define quando o dispositivo executará determinadas ações. Você pode configurar regras como agendadas, recorrentes ou acionadas manualmente.
2. Insira um **Name (Nome)**.
3. Selecione a **Condition (Condição)** que deve ser atendida para acionar a ação. Se você especificar mais de uma condição para a regra, todas as condições deverão ser atendidas para acionar a ação.
4. Selecione qual **Action (Ação)** o dispositivo deverá executar quando as condições forem atendidas.

Observação

Se você fizer alterações em uma regra ativa, a regra deverá ser ativada novamente para que as alterações entrem em vigor.

Acionar uma notificação quando a caixa de proteção for aberta

Este exemplo explica como configurar uma notificação por email quando a caixa de proteção do dispositivo for aberta.

Adicionar um destinatário de email:

1. vá para **System > Events > Recipients (Sistema > Eventos > Destinatários)** e clique em **Add recipient (Adicionar destinatário)**.
2. Digite um nome para o destinatário.
3. Selecione **Email** como o tipo de notificação.
4. Digite o endereço de email do destinatário.
5. Digite o endereço de email do qual a câmera enviará as notificações.
6. Forneça os detalhes de login da conta de email remetente, juntamente com o nome do host SMTP e o número da porta.
7. Para testar a configuração de seu email, clique em **Test (Testar)**.
8. Clique em **Salvar**.

Crie uma regra:

9. Vá para **System > Events > Rules (Sistema > Eventos > Regras)** e clique em **Add a rule (Adicionar uma regra)**.
10. Digite um nome para a regra.
11. Na lista de condições, selecione **Casing open (Caixa aberta)**.
12. Na lista de ações, selecione **Send notification to email (Enviar notificação para email)**.
13. Selecione um destinatário na lista.
14. Digite uma linha de assunto e a mensagem do email.
15. Clique em **Salvar**.

Gravar vídeo de uma câmera quando um movimento é detectado

Este exemplo explica como configurar o radar e uma câmera para que ela comece a gravar no cartão SD cinco segundos antes que o radar identifique movimento e pare um minuto depois.

Conexão dos dispositivos:

1. Conecte um cabo de uma saída de E/S no radar a uma entrada de E/S na câmera.

Configuração da porta de E/S do radar:

2. Vá para **System > Accessories > I/O ports (Sistema > Acessórios > Portas de E/S)**, configure a porta de E/S como uma saída e selecione o estado normal.

Criação de uma regra no radar:

3. vá para **System > Events (Sistema > Eventos)** e adicione uma regra.
4. Digite um nome para a regra.
5. Na lista de condições, selecione um cenário em **Radar motion (Movimento do radar)**.
   Para configurar um cenário, consulte .
6. Na lista de ações, selecione **Toggle I/O while the rule is active (Alternar E/S enquanto a regra estiver ativa)** e, em seguida, selecione a porta que está conectada à câmera.
7. Clique em **Salvar**.

Configure a porta de E/S da câmera:

8. Vá para **System > Accessories > I/O ports (Sistema > Acessórios > Portas de E/S)**, configure a porta de E/S como uma entrada e selecione o estado normal.

Criação de uma regra na câmera:

9. vá para **System > Events (Sistema > Eventos)** e adicione uma regra.
10. Digite um nome para a regra.
11. Na lista de condições, selecione **Digital input is active (A entrada digital está ativa)** e, em seguida, selecione a porta que deve acionar a regra.
12. Na lista de ações, selecione **Record video (Gravar vídeo)**.
13. Na lista de opções de armazenamento, selecione **SD card (Cartão SD)**.
14. Selecione um perfil de stream existente ou crie um novo.
15. Defina o pré-buffer como 5 segundos.
16. Defina o tempo do pós-buffer como 1 minuto.
17. Clique em **Salvar**.

Acender uma luz quando um movimento é detectado

Acender uma luz quando um invasor entra na zona de detecção pode deter, além de melhorar a qualidade da imagem de uma câmera visual gravando a invasão.

Este exemplo explica como configurar o radar e um iluminador para que o iluminador acenda quando o radar identificar movimento e desligue após um minuto.

Conexão dos dispositivos:

1. Conecte um dos cabos do iluminador à fonte de alimentação através da porta de relé no radar. Conecte o outro cabo diretamente entre a fonte de alimentação e o iluminador.

Configuração da porta de relé do radar:

2. Vá para **System > Accessories > I/O ports (Sistema > Acessórios > Portas de E/S)** e selecione **Open circuit (Circuito aberto)** como o estado normal da porta de relé.

Criação de uma regra no radar:

3. vá para **System > Events (Sistema > Eventos)** e adicione uma regra.
4. Digite um nome para a regra.
5. Na lista de condições, selecione um cenário em **Radar motion (Movimento do radar)**.

Para configurar um cenário, consulte .

6. Na lista de ações, selecione **Toggle I/O once (Alternar E/S uma vez)** e, em seguida, selecione a porta de relé.
7. Selecione **Active (Ativa)**.
8. Defina a **Duration (Duração)**.
9. Clique em **Salvar**.

Enviar um email se alguém cobrir o radar com um objeto metálico

Esse exemplo explica como criar uma regra que envia uma notificação por email quando alguém manipula o radar cobrindo-o com um objeto metálico, como folha ou chapa metálica.

Observação

A opção de criar regras para eventos de manipulação de radar está disponível no AXIS OS 11.11.

Adicionar um destinatário de email:

1. vá para **System > Events > Recipients (Sistema > Eventos > Destinatários)** e clique em **Add recipient (Adicionar destinatário)**.
2. Digite um nome para o destinatário.
3. Selecione **Email**.
4. Digite um endereço de email para o qual a mensagem será enviada.
5. A câmera não tem seu próprio servidor de email, portanto, será necessário fazer login em outro servidor de email para poder enviar emails. Preencha as demais informações de acordo com seu provedor de email.
6. Para enviar um email de teste, clique em **Test (Testar)**.
7. Clique em **Salvar**.

Crie uma regra:

8. vá para **System > Events (Sistema > Eventos)** e adicione uma regra.
9. Digite um nome para a regra.
10. Na lista de condições, em **Device status (Status do dispositivo)**, selecione **Radar data failure (Falha de dados do radar)**.
11. Em **Reason (Motivo)**, selecione **Tampering (Manipulação)**.
12. Na lista de ações, em **Notifications (Notificações)**, selecione **Send notification to email (Enviar notificação para email)**.
13. Selecione o destinatário criado.
14. Digite um assunto e uma mensagem para o email.
15. Clique em **Salvar**.

A interface Web

Para alcançar a interface Web do dispositivo, digite o endereço IP do dispositivo em um navegador da Web.

Observação

O suporte aos recursos e às configurações descritas nesta seção variam para cada dispositivo. Este ícone indica que o recurso ou configuração está disponível somente em alguns dispositivos.

Mostre ou oculte o menu principal.

Acesse as notas de versão.

Acesse a ajuda do produto.

Altere o idioma.

Defina o tema claro ou escuro.

O menu de usuário contém:

- Informações sobre o usuário que está conectado.
- **Alterar conta**: Saia da conta atual e faça login em uma nova conta.
- **Desconectar**: Faça logout da conta atual.

 O menu de contexto contém:

- **Analytics data (Dados de analíticos)**: Aceite para compartilhar dados de navegador não pessoais.
- **Feedback (Comentários)**: Compartilhe qualquer feedback para nos ajudar a melhorar sua experiência de usuário.
- **Legal**: veja informações sobre cookies e licenças.
- **About (Sobre)**: veja informações do dispositivo, incluindo versão e número de série do AXIS OS.

Status

Status de sincronização de horário

Mostra as informações de sincronização de NTP, incluindo se o dispositivo está em sincronia com um servidor NTP e o tempo restante até a próxima sincronização.

NTP settings (Configurações de NTP): Exiba e atualize as configurações de NTP. Leva você para a página **Time and location (Hora e local)** na qual é possível alterar as configurações de NTP.

Gravação em andamento

Mostra as gravações em andamento e seu espaço de armazenamento designado.

Gravações: Exibir gravações em andamento e filtradas e suas fontes. Para obter mais informações, consulte

Mostra o espaço de armazenamento no qual a gravação é salva.

Informações do dispositivo

Mostra as informações do dispositivo, incluindo versão e o número de série do AXIS OS.

Upgrade AXIS OS (Atualizar o AXIS OS): atualize o software em seu dispositivo. Abre a página Maintenance (Manutenção), na qual é possível atualizar.

Clientes conectados

Mostra o número de conexões e os clientes conectados.

View details (Exibir detalhes): Exiba e atualize a lista dos clientes conectados. A lista mostra o endereço IP, o protocolo, a porta e o PID/Processo de cada conexão.

Radar

Definições

Geral

Transmissão de radar: Use essa opção para desativar o módulo de radar completamente.

Canal : Se você tiver problemas com vários dispositivos interferindo uns nos outros, selecione o mesmo canal para até quatro dispositivos próximos uns dos outros. Para a maioria das instalações, selecione **Auto** para permitir que os dispositivos negociem automaticamente qual canal usar.

Altura da montagem: insira a altura de montagem para o produto.

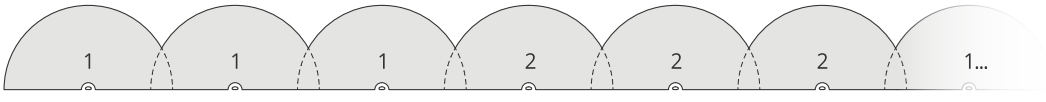
Observação

Seja o mais específico possível ao inserir a altura de montagem. Isso ajuda o dispositivo a visualizar a detecção de radar na posição correta na imagem.

Coexistência

Number of neighboring radars (Número de radares vizinhos): Selecione o número de radares vizinhos que são montados na mesma zona de coexistência. Isso ajudará a evitar interferências. O raio da zona de coexistência é de 350 m (1148 pés).

- **0–1**: Selecione essa opção se você pretende montar um a dois radares na mesma zona de coexistência.
- **2**: Selecione essa opção se você pretende montar três radares na mesma zona de coexistência.
- **3–5**: Selecione essa opção se você pretende montar quatro a seis radares na mesma zona de coexistência.
  - **Groups (Grupos)**: Selecione um grupo (**Group 1 (Grupo 1)** ou **Group 2 (Grupo 2)**) para seu radar. Isso também ajudará a evitar interferências. Recomendamos adicionar três radares em cada grupo e adicionar radares que estão mais próximos uns dos outros no mesmo grupo.



Para obter mais informações, consulte .

Detecção

Detection sensitivity (Sensibilidade da detecção): Selecione o quanto sensível o radar deve ser. Um valor mais alto significa que você obtém um alcance de detecção mais longo, mas também há um risco mais alto de alarmes falsos. Uma sensibilidade mais baixa reduz o número de alarmes falsos, mas pode reduzir o alcance da detecção.

Radar profile (Perfil de radar): Selecione um perfil adequado à sua área de interesse.

- **Area monitoring (Monitoramento de área)**: Rastreie objetos grandes e pequenos movendo-se em velocidades menores em áreas abertas.
  - **Ignorar objetos rotativos estacionários (Ignorar objetos rotativos estacionários)** : Ative-o para minimizar alarmes falsos provenientes de objetos estacionários com movimentos rotativos, como ventiladores ou turbinas.
  - **Ignore small objects (Ignorar objetos pequenos)**: Ative para minimizar alarmes falsos de objetos pequenos, como cães ou coelhos.
  - **Ignore swaying objects (Ignorar objetos balançando)**: Ative para minimizar alarmes falsos causados por objetos balançando, como árvores, arbustos ou mastros de bandeiras.
- **Road monitoring (Monitoramento de vias)**: Acompanhe veículos transitando em velocidades mais altas em zonas urbanas e em estradas suburbanas
  - **Ignorar objetos rotativos estacionários (Ignorar objetos rotativos estacionários)** : Ative-o para minimizar alarmes falsos provenientes de objetos estacionários com movimentos rotativos, como ventiladores ou turbinas.
  - **Ignore swaying objects (Ignorar objetos balançando)**: Ative para minimizar alarmes falsos causados por objetos balançando, como árvores, arbustos ou mastros de bandeiras.

Visualizar

Information legend (Legenda de informações): Ative para mostrar uma legenda que contenha os tipos de objetos que o radar pode detectar e rastrear. Arraste e solte para mover a legenda de informações.

Zone opacity (Opacidade da zona): Selecione o quanto opaca ou transparente a zona de cobertura deve ser.

Grid opacity (Opacidade da grade): Selecione o quanto opaca ou transparente a grade deve ser.

Color scheme (Esquema de cores): Selecione um tema para a visualização de radar.

Rotação : Selecione a orientação preferida da imagem de radar.

Visualização de objetos

Trail lifetime (Duração do rastro): Selecione por quanto tempo o rastro de um objeto rastreado é visível na exibição de radar.

Icon style (Estilo do ícone): Selecione o estilo do ícone dos objetos rastreados no modo de exibição de radar. Para triângulos simples, selecione **Triangle (Triângulo)**. Para símbolos representativos, selecione **Symbol (Símbolo)**. Os ícones apontarão na direção em que os objetos rastreados estão se movendo, independente do estilo.

Show information with icon (Mostrar informações com o ícone): Selecione quais informações serão exibidas ao lado do ícone do objeto rastreado:

- **Object type (Tipo do objeto)**: Mostra o tipo de objeto detectado pelo radar.
- **Classification probability (Probabilidade de classificação)**: Mostra o nível de certeza do radar em relação à classificação correta do objeto.
- **Velocity (Velocidade)**: Mostra o quanto rápido o objeto está se movendo.

Stream

Geral

Resolução: Selecione a resolução de imagem adequada para a cena de monitoramento. Uma resolução maior aumenta a largura de banda e o armazenamento.

Taxa de quadros: para evitar problemas de largura de banda na rede ou reduzir o tamanho do armazenamento, você pode limitar a taxa de quadros a um valor fixo. Se a taxa de quadros for definida como zero, ela será mantida na maior taxa possível sob as condições atuais. Uma taxa de quadros mais alta exige mais largura de banda e capacidade de armazenamento.

P-frames (Quadros P): um quadro P é uma imagem prevista que exibe somente as alterações na imagem do quadro anterior. insira a quantidade desejada de quadros P. Quanto maior for o número, menor será a largura de banda necessária. No entanto, se houver congestionamento na rede, poderá haver deterioração perceptível na qualidade do vídeo.

Compression (Compactação): use o controle deslizante para ajustar a compactação da imagem. Uma compactação alta resulta em taxa de bits e qualidade de imagem menores. Uma compactação baixa aumenta a qualidade da imagem, mas usa mais largura de banda e armazenamento durante a gravação.

— Vídeo assinado : ative para adicionar o recurso de vídeo assinado ao vídeo. O vídeo assinado protege o vídeo contra manipulação ao adicionar assinaturas de criptografia ao vídeo.

Controle de taxa de bits

- **Average (Média)**: selecione para ajustar automaticamente a taxa de bits durante um período mais longo e proporcionar a melhor qualidade de imagem possível com base no armazenamento disponível.
  - Clique para calcular a taxa-alvo de bits com base em armazenamento disponível, tempo de retenção e limite da taxa de bits.
  - **Target bitrate (Taxa-alvo de bits)**: insira a taxa-alvo de bits desejada.
  - **Retention time (Tempo de retenção)**: insira o número de dias que deseja manter as gravações.
  - **Armazenamento**: mostra o armazenamento estimado que pode ser usado para o stream.
  - **Maximum bitrate (Taxa de bits máxima)**: ative para definir um limite para a taxa de bits.
  - **Bitrate limit (Limite da taxa de bits)**: insira um limite para a taxa de bits que seja superior à taxa-alvo de bits.
- **Maximum (Máxima)**: selecione para definir uma taxa de bits máxima instantânea do stream com base na largura de banda da rede.
  - **Maximum (Máxima)**: insira a taxa de bits máxima.
- **Variable (Variável)**: selecione para permitir que a taxa de bits varie de acordo com o nível de atividade na cena. Mais atividade exigirá mais largura de banda. Recomendamos essa opção para a maioria das situações.

Calibração do mapa

Use a calibração de mapa para carregar e calibrar um mapa de referência. O resultado da calibração é um mapa de referência que exibe a cobertura do radar na escala apropriada, o que facilita a visualização de onde os objetos estão se movendo.

Assistente de configuração: Clique para abrir o assistente de configuração que o orienta passo a passo na calibração.

Redefinir calibração: Clique para remover a imagem do mapa atual e a posição do radar no mapa.

Mapa

Upload map (Carregar mapa): Selecione ou arraste e solte a imagem do mapa que você deseja carregar.

Faça o download do mapa: Clique para fazer o download do mapa.

Rotate map (Girar mapa): use o controle deslizante para girar a imagem do mapa.

Escala e distância no mapa

Distance (Distância): Adicione a distância entre os dois pontos que você adicionou ao mapa.

Mapa com panning e zoom

Pan: Clique nos botões para criar uma panorâmica da imagem do mapa.

Zoom: Clique nos botões para aumentar ou diminuir o zoom na imagem do mapa.

Redefinir o panning e o zoom: Clique para remover as configurações de panning e zoom.

Posição do radar

Posição: Clique nos botões para mover o radar no mapa.

Rotação: Clique nos botões para girar o radar no mapa.

Zonas de exclusão

Uma **exclude zone (zona de exclusão)** é uma área na qual objetos em movimento são ignorados. Use zonas de exclusão se houver áreas dentro de um cenário que disparem muitos alarmes indesejados.

: Clique para criar uma nova zona de exclusão.

Para modificar uma zona de exclusão, selecione-a na lista.

Track passing objects (Rastrear objetos móveis): Ative-o para rastrear os objetos que atravessam a zona de exclusão. Os objetos móveis mantêm seus IDs de rastreamento e são visíveis por toda a zona. Objetos que aparecem dentro da zona de exclusão não serão rastreados.

Zone shape presets (Predefinições de formato de zona): Selecione o formato inicial da zona de exclusão.

- **Cover everything (Cobrir tudo)**: Selecione para definir uma zona de exclusão que cubra toda a área de cobertura do radar.
- **Reset to box (Reajustar à caixa)**: Selecione para colocar uma zona de exclusão retangular no meio da área de cobertura.

Para modificar o formato da zona, arraste e solte qualquer um dos pontos nas linhas. Para remover um ponto, clique com o botão direito sobre ele.

Cenários

Um cenário é uma combinação de condições de acionamento, bem como configurações de cena e detecção.

: Clique para criar um novo cenário. É possível criar até 20 cenários.

Triggering conditions (Condições de acionamento): Selecione a condição que acionará alarmes.

- **Movement in area (Movimento na área)**: Selecione se deseja que o cenário acione em caso de objetos se movendo em uma área.
- **Cruzamento de linhas**: Selecione se deseja que o cenário seja acionado em objetos que cruzam uma ou duas linhas.

Scene (Cena): Defina a área ou as linhas no cenário em que objetos móveis acionam alarmes.

- Para **Movement in area (Movimento na área)**, selecione uma das formas predefinidas para modificar a área.
- Para **Line crossing (Cruzamento de linhas)**, arraste e solte a linha na cena. Para criar mais pontos em uma linha, clique em e arraste em qualquer lugar na linha. Para remover um ponto, clique com o botão direito sobre ele.
  - **Require crossing of two lines (Exigir o cruzamento de duas linhas)**: Ative se o objeto precisar passar por duas linhas antes que o cenário dispare um alarme.
  - **Change direction (Alterar direção):** Ative se desejar que o cenário dispare um alarme quando os objetos cruzarem a linha na outra direção.

Detection settings (Configurações de detecção): Defina os critérios de acionamento para o cenário.

- Para **Movement in area (Movimento na área)**:
  - **Ignore short-lived objects (Ignorar objetos de curta duração)**: Defina o retardo em segundos desde o momento em que o radar detecta o objeto até quando o cenário aciona um alarme. Isso pode ajudar a reduzir os alarmes falsos.
  - **Trigger on object type (Acionar com tipo de objeto)**: Selecione o tipo de objeto (pessoa, veículo, desconhecido) para o qual você deseja que o cenário seja acionado.
  - **Speed limit (Limite de velocidade)**: Acione em objetos que estejam se movendo em velocidades dentro de uma faixa específica.
    - **Invert (Inverter)**: Selecione se deseja acionar em velocidades acima e abaixo do limite de velocidade definido.
- Para **Line crossing (Cruzamento de linhas)**:
  - **Ignore short-lived objects (Ignorar objetos de curta duração)**: Defina o retardo em segundos desde o momento em que o radar detecta o objeto até quando o cenário dispara uma ação. Isso pode ajudar a reduzir os alarmes falsos. Esta opção não está disponível para objetos que cruzam duas linhas.
  - **Max time between crossings (Tempo máximo entre cruzamentos)**: Defina o tempo máximo entre os cruzamentos da primeira linha e da segunda linha. Esta opção só está disponível para objetos que cruzam duas linhas.
  - **Trigger on object type (Acionar com tipo de objeto)**: Selecione o tipo de objeto (pessoa, veículo, desconhecido) para o qual você deseja que o cenário seja acionado.
  - **Speed limit (Limite de velocidade)**: Acione em objetos que estejam se movendo em velocidades dentro de uma faixa específica.
    - **Invert (Inverter)**: Selecione se deseja acionar em velocidades acima e abaixo do limite de velocidade definido.

Alarm settings (Configurações de alarme): Defina os critérios do alarme.

- **Minimum trigger duration (Duração mínima do acionador)**: Defina a duração mínima do alarme acionado.

Sobreposições

: clique para adicionar uma sobreposição. Selecione o tipo de sobreposição na lista suspensa:

- **Text (Texto)**: selecione para mostrar um texto integrado à imagem da visualização ao vivo e visível em todas as exibições, gravações e instantâneos. Você pode inserir texto próprio e também pode incluir modificadores pré-configurados para mostrar automaticamente a hora, data, taxa de quadros etc.
  - : clique para adicionar o modificador de data `%F` para mostrar aaaa-mm-dd.
  - : clique para adicionar o modificador de hora `%X` para mostrar hh:mm:ss (formato de 24 horas).
  - **Modifiers (Modificadores)**: clique para selecionar quaisquer modificadores mostrados na lista para adicioná-los à caixa de texto. Por exemplo, `%a` mostra o dia da semana.
  - **Tamanho**: selecione o tamanho de fonte desejado.
  - **Aparência**: selecione a cor do texto e o fundo, por exemplo, texto branco sobre fundo preto (padrão).
  - Selecione a posição da sobreposição na imagem ou clique e arraste a sobreposição para movê-la na visualização ao vivo.
- **Image (Imagem)**: selecione para mostrar uma imagem estática sobre o stream de vídeo. Você pode usar arquivos .bmp, .png, .jpeg e .svg.
  Para carregar uma imagem, clique em **Manage images (Gerenciar imagens)**. Antes de fazer upload de uma imagem, você pode escolher:
  - **Scale with resolution (Dimensionamento com resolução)**: selecione para dimensionar automaticamente a imagem de sobreposição para adequá-la à resolução do vídeo.
  - **Use transparency (Usar transparência)**: selecione e insira o valor hexadecimal RGB para a respectiva cor. Use o formato RRGGBB. Exemplos de valores hexadecimais são: FFFFFF para branco, 000000 para preto, FF0000 para vermelho, 6633FF para azul e 669900 para verde. Somente para imagens .bmp.
- **Anotação de cena** : Selecione para mostrar uma sobreposição de texto no stream de vídeo que permanece na mesma posição, mesmo quando a câmera gira ou inclina em outra direção. Você pode optar por mostrar a sobreposição apenas dentro de determinados níveis de zoom.
  - : clique para adicionar o modificador de data `%F` para mostrar aaaa-mm-dd.
  - : clique para adicionar o modificador de hora `%X` para mostrar hh:mm:ss (formato de 24 horas).
  - **Modifiers (Modificadores)**: clique para selecionar quaisquer modificadores mostrados na lista para adicioná-los à caixa de texto. Por exemplo, `%a` mostra o dia da semana.
  - **Tamanho**: selecione o tamanho de fonte desejado.
  - **Aparência**: selecione a cor do texto e o fundo, por exemplo, texto branco sobre fundo preto (padrão).
  - Selecione a posição da sobreposição na imagem ou clique e arraste a sobreposição para movê-la na visualização ao vivo. A sobreposição é salva e permanece nas coordenadas de panorâmica e inclinação desta posição.
  - **Annotation between zoom levels (%) (Anotação entre níveis de zoom (%))**: Defina os níveis de zoom nos quais a sobreposição será mostrada.

- **Annotation symbol (Símbolo de notação)**: Selecione um símbolo que aparece em vez da sobreposição quando a câmera não está dentro dos níveis de zoom definidos.

- **Indicador de streaming** : selecione para mostrar uma animação sobre o stream de vídeo. A animação indica que o stream de vídeo está ao vivo, mesmo quando a cena não contém nenhum movimento.
  - **Aparência**: selecione a cor da animação e a cor de fundo, por exemplo, animação vermelha em fundo transparente (padrão).
  - **Tamanho**: selecione o tamanho de fonte desejado.
  - Selecione a posição da sobreposição na imagem ou clique e arraste a sobreposição para movê-la na visualização ao vivo.

- **Widget: Linegraph (Widget: Gráfico de linhas)** : mostre um gráfico que mostra como um valor medido muda ao longo do tempo.
  - **Título**: insira um título para o widget.
  - **Modificador de sobreposição**: selecione um modificador de sobreposição como fonte de dados. Se você criou sobreposições MQTT, elas estarão localizadas no final da lista.
  - Selecione a posição da sobreposição na imagem ou clique e arraste a sobreposição para movê-la na visualização ao vivo.
  - **Tamanho**: selecione o tamanho da sobreposição.
  - **Visível em todos os canais**: Desative para mostrar apenas no canal selecionado no momento. Ative para exibir todos os canais ativos.
  - **Intervalo de atualização**: escolha o tempo entre as atualizações de dados.
  - **Transparência**: defina a transparência de toda a sobreposição.
  - **Transparência do segundo plano**: defina a transparência apenas do plano de fundo da sobreposição.
  - **Pontos**: ative para adicionar um ponto à linha do gráfico quando os dados forem atualizados.
  - **Eixo X**
    - **Label (Rótulo)**: insira o rótulo de texto para o eixo X.
    - **Janela de tempo**: insira por quanto tempo os dados são visualizados.
    - **Unidade de tempo**: insira uma unidade de tempo para o eixo X.
  - **Eixo Y**
    - **Label (Rótulo)**: insira o rótulo de texto para o eixo Y.
    - **Escala dinâmica**: ative para que a escala se adapte automaticamente aos valores dos dados. desative para inserir manualmente valores para uma escala fixa.
    - **Limiar mínimo de alarme** e **Limiar máximo de alarme**: esses valores adicionarão linhas de referência horizontais ao gráfico, facilitando a visualização quando o valor dos dados estiver muito alto ou muito baixo.

- **Widget: Medidor** : mostre um gráfico de barras que exibe o valor dos dados medidos mais recentemente.
  - **Título**: insira um título para o widget.
  - **Modificador de sobreposição**: selecione um modificador de sobreposição como fonte de dados. Se você criou sobreposições MQTT, elas estarão localizadas no final da lista.
  - Selecione a posição da sobreposição na imagem ou clique e arraste a sobreposição para movê-la na visualização ao vivo.

- **Tamanho**: selecione o tamanho da sobreposição.
- **Visível em todos os canais**: Desative para mostrar apenas no canal selecionado no momento. Ative para exibir todos os canais ativos.
- **Intervalo de atualização**: escolha o tempo entre as atualizações de dados.
- **Transparência**: defina a transparência de toda a sobreposição.
- **Transparência do segundo plano**: defina a transparência apenas do plano de fundo da sobreposição.
- **Pontos**: ative para adicionar um ponto à linha do gráfico quando os dados forem atualizados.
- **Eixo Y**
  - **Label (Rótulo)**: insira o rótulo de texto para o eixo Y.
  - **Escala dinâmica**: ative para que a escala se adapte automaticamente aos valores dos dados. desative para inserir manualmente valores para uma escala fixa.
  - **Limiar mínimo de alarme** e **Limiar máximo de alarme**: esses valores adicionarão linhas de referência horizontais ao gráfico de barras, facilitando a visualização quando o valor dos dados estiver muito alto ou muito baixo.

Rastreamento automático PTZ com radar:

Emparelhe o radar com uma câmera PTZ para usar rastreamento automático por radar. Para estabelecer a conexão, vá para **System > Edge-to-edge**).

Ajuste as configurações iniciais:

Altura de montagem da câmera: A distância do chão até a altura da câmera PTZ montada.

Alinhamento de pan: Obtenha a panorâmica da câmera PTZ de modo que ela aponte na mesma direção que o radar. Clique no endereço IP da câmera PTZ para acessá-la.

Salvar deslocamento de pan: Clique em para salvar o alinhamento de pan.

Deslocamento da inclinação em relação ao chão: Use o deslocamento da inclinação do chão para ajustar a inclinação da câmera. Se o chão for inclinado, ou se a câmera não estiver montada na horizontal, a câmera poderá apontar muito para cima ou muito para baixo ao rastrear um objeto.

Pronto: Clique em para salvar suas configurações e continue com a configuração.

Configurar o rastreamento automático de PTZ:

Rastreamento: Selecione se deseja rastrear humanos, veículos e/ou objetos desconhecidos.

Rastreamento: Ative para iniciar o rastreamento de objetos com a câmera PTZ. O rastreamento ampliará automaticamente um objeto ou grupo de objetos para mantê-los na exibição da câmera.

Alternância de objetos: Se o radar detecta vários objetos que não cabem na exibição da câmera PTZ, a câmera PTZ rastreará o objeto com a prioridade mais alta fornecida pelo radar e ignorará os demais.

Tempo de retenção do objeto: Determina por quantos a câmera PTZ deve rastrear cada objeto.

Return to home (Retornar para posição inicial): Ative para fazer a câmera PTZ retornar para sua posição inicial quando o radar não estiver mais rastreando objetos.

Tempo limite do retorno para posição inicial: Determina por quanto tempo a câmera PTZ deve permanecer deve permanecer na última posição conhecida dos objetos rastreados antes de voltar para a posição inicial.

Zoom: Use o controle deslizante para fazer o ajuste fino do zoom da câmera PTZ.

Reconfigurar instalação: Clique em para limpar todas as configurações e voltar para a configuração inicial.

Gravações

Ongoing recordings (Gravações em andamento): Mostre todas as gravações em andamento no dispositivo.

● Inicie uma gravação no dispositivo.

Escolha o dispositivo de armazenamento que será usado para salvar.

● Pare uma gravação no dispositivo.

Gravações acionadas serão paradas manualmente ou quando o dispositivo for desligado.

As **gravações contínuas** continuarão até ser interrompidas manualmente. Mesmo se o dispositivo for desligado, a gravação continuará quando o dispositivo iniciar novamente.

Reproduza a gravação.

Pare a execução da gravação.

Mostre ou oculte informações sobre a gravação.

Set export range (Definir faixa de exportação): se você só quiser exportar uma parte da gravação, informe um intervalo de tempo. Observe que, se você trabalha em um fuso horário diferente do local do dispositivo, o intervalo de tempo será baseado no fuso horário do dispositivo.

Encrypt (Criptografar): Selecione para definir uma senha para as gravações exportadas. Não será possível abrir o arquivo exportado sem a senha.

Clique para excluir uma gravação.

Export (Exportar): Exporte a gravação inteira ou uma parte da gravação.

Clique para filtrar as gravações.

From (De): mostra as gravações realizadas depois de determinado ponto no tempo.

To (Até): mostra as gravações até determinado ponto no tempo.

Source (Fonte): mostra gravações com base na fonte. A fonte refere-se ao sensor.

Event (Evento): mostra gravações com base em eventos.

Armazenamento: mostra gravações com base no tipo de armazenamento.

Apps

Adicionar app: Instale um novo aplicativo.

Find more apps (Encontrar mais aplicativos): Encontre mais aplicativos para instalar. Você será levado para uma página de visão geral dos aplicativos Axis.

Permitir apps não assinados : Ative para permitir a instalação de aplicativos não assinados.

Veja as atualizações de segurança nos aplicativos AXIS OS e ACAP.

Observação

O desempenho do dispositivo poderá ser afetado se você executar vários aplicativos ao mesmo tempo.

Use a chave ao lado do nome do aplicativo para iniciar ou parar o aplicativo.

Open (Abrir): Acesse às configurações do aplicativo. As configurações disponíveis dependem do aplicativo. Alguns aplicativos não têm configurações.

O menu de contexto pode conter uma ou mais das seguintes opções:

- **Open-source license (Licença de código aberto)**: Exiba informações sobre as licenças de código aberto usadas no aplicativo.
- **App log (Log do aplicativo)**: Exiba um log dos eventos de aplicativos. Este log é útil quando é necessário entrar em contato com o suporte.
- **Activate license with a key (Ativar licença com uma chave)**: Se o aplicativo exigir uma licença, você deverá ativá-la. Use essa opção se o dispositivo não tiver acesso à Internet.
  Se você não tiver uma chave de licença, acesse *axis.com/products/analytics*. Você precisa de um código de licença e do número de série do produto Axis para gerar uma chave de licença.
- **Activate license automatically (Ativar licença automaticamente)**: Se o aplicativo exigir uma licença, você deverá ativá-la. Use essa opção se o dispositivo tiver acesso à Internet. Um código de licença é necessário para ativar a licença.
- **Deactivate the license (Desativar a licença)**: Desative a licença para substituí-la por outra licença, por exemplo, ao migrar de uma licença de avaliação para uma licença completa. Se você desativar a licença, ela será removida do dispositivo.
- **Settings (Configurações)**: configure os parâmetros.
- **Excluir**: Exclua o aplicativo permanentemente do dispositivo. Se você não desativar a licença primeiro, ela permanecerá ativa.

Sistema

Hora e local

Data e hora

O formato de hora depende das configurações de idioma do navegador da Web.

Observação

Recomendamos sincronizar a data e a hora do dispositivo com um servidor NTP.

Synchronization (Sincronização): Selecione uma opção para sincronização da data e da hora do dispositivo.

- **Automatic date and time (manual NTS KE servers) (Data e hora automáticas (servidores NTS KE manuais))**: Sincronizar com os servidores estabelecimentos de chave NTP seguros conectados ao servidor DHCP.
  - **Manual NTS KE servers (Servidores NTS KE manuais)**: Insira o endereço IP de um ou dois servidores NTP. Quando você usa dois servidores NTP, o dispositivo sincroniza e adapta sua hora com base na entrada de ambos.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **Automatic date and time (NTP servers using DHCP) (Data e hora automáticas (servidores NTP usando DHCP))**: sincronize com os servidores NTP conectados ao servidor DHCP.
  - **Fallback NTP servers (Servidores NTP de fallback)**: insira o endereço IP de um ou dois servidores de fallback.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **Automatic date and time (manual NTP servers) (Data e hora automáticas (servidores NTP manuais))**: sincronize com os servidores NTP de sua escolha.
  - **Manual NTP servers (Servidores NTP manuais)**: Insira o endereço IP de um ou dois servidores NTP. Quando você usa dois servidores NTP, o dispositivo sincroniza e adapta sua hora com base na entrada de ambos.
  - **Max NTP poll time (Tempo máximo da pesquisa NTP)**: selecione o tempo máximo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
  - **Min NTP poll time (Tempo mínimo da pesquisa NTP)**: selecione o tempo mínimo que o dispositivo deve aguardar antes de fazer a pesquisa no servidor NTP para obter um tempo atualizado.
- **Custom date and time (Data e hora personalizadas)**: defina manualmente a data e a hora. Clique em **Get from system (Obter do sistema)** para obter as configurações de data e hora uma vez em seu computador ou dispositivo móvel.

Fuso horário: Selecione qual fuso horário será usado. A hora será ajustada automaticamente para o horário de verão e o horário padrão.

- **DHCP**: Adota o fuso horário do servidor DHCP. O dispositivo deve estar conectado a um servidor DHCP para que você possa selecionar esta opção.
- **Manual**: Selecione um fuso horário na lista suspensa.

Observação

O sistema usa as configurações de data e hora em todas as gravações, logs e configurações do sistema.

Local do dispositivo

Insira o local do dispositivo. Seu sistema de gerenciamento de vídeo pode usar essa informação para posicionar o dispositivo em um mapa.

- **Format (Formatar)**: Selecione o formato a ser usado ao inserir a latitude e a longitude de seu dispositivo.
- **Latitude**: Valores positivos estão ao norte do equador.
- **Longitude**: Valores positivos estão a leste do meridiano de Greenwich.
- **Cabeçalho**: Insira a direção da bússola para a qual o dispositivo está voltado. 0 representa o norte.
- **Label (Rótulo)**: Insira um nome descritivo para seu dispositivo.
- **Save (Salvar)**: Clique em para salvar a localização do dispositivo.

Configurações regionais

Define o sistema de medida em todas as configurações do sistema.

Métrico (m, km/h): Selecione para que a medição de distância seja em metros e a de velocidade em quilômetros por hora.

Padrão dos EUA (ft, mph): Selecione para que a medição de distância seja em pés e a de velocidade em milhas por hora.

Rede

IPv4

Assign IPv4 automatically (Atribuir IPv4 automaticamente): Selecione para permitir que o roteador de rede atribua um endereço IP ao dispositivo automaticamente. Recomendamos utilizar IP (DHCP) automático para a maioria das redes.

Endereço IP: Insira um endereço IP exclusivo para o dispositivo. Endereços IP estáticos podem ser atribuídos aleatoriamente em redes isoladas, desde que cada endereço seja único. Para evitar conflitos, é altamente recomendável entrar em contato o administrador da rede antes de atribuir um endereço IP estático.

Máscara de sub-rede: Insira a máscara de sub-rede para definir quais endereços estão dentro da rede local. Qualquer endereço fora da rede local passa pelo roteador.

Router (Roteador): Insira o endereço IP do roteador padrão (gateway) usado para conectar dispositivos conectados a diferentes redes e segmentos de rede.

Fallback to static IP address if DHCP isn't available (Retornar como contingência para o endereço IP estático se o DHCP não estiver disponível): Selecione se você deseja adicionar um endereço IP estático para usar como contingência se o DHCP não estiver disponível e não puder atribuir um endereço IP automaticamente.

Observação

Se o DHCP não estiver disponível e o dispositivo usar um fallback de endereço estático, o endereço estático será configurado com um escopo limitado.

IPv6

Assign IPv6 automatically (Atribuir IPv6 automaticamente): Selecione para ativar o IPv6 e permitir que o roteador de rede atribua um endereço IP ao dispositivo automaticamente.

Nome de host

Assign hostname automatically (Atribuir nome de host automaticamente): Selecione para permitir que o roteador de rede atribua um nome de host ao dispositivo automaticamente.

Nome de host: Insira o nome de host manualmente para usar como uma maneira alternativa de acessar o dispositivo. O relatório do servidor e o log do sistema usam o nome de host. Os caracteres permitidos são A – Z, a – z, 0 – 9 e -.

Ative as atualizações de DNS dinâmicas: Permita que o dispositivo faça a atualização automática dos registros do servidor de nomes de domínio sempre que o endereço IP for alterado.

Registrar o nome do DNS: Digite um nome de domínio exclusivo que aponte para o endereço IP de seu dispositivo. Os caracteres permitidos são A – Z, a – z, 0 – 9 e -.

TTL: O tempo de vida (TTL) define por quanto tempo um registro DNS permanecerá válido até que precise ser atualizado.

Servidores DNS

Assign DNS automatically (Atribuir o DNS automaticamente): Selecione para permitir que o servidor DHCP atribua domínios de pesquisa e endereços de servidor DNS ao dispositivo automaticamente. Recomendamos utilizar DNS (DHCP) automático para a maioria das redes.

Search domains (Domínios de pesquisa): Ao usar um nome de host que não está totalmente qualificado, clique em **Add search domain (Adicionar domínio de pesquisa)** e insira um domínio para pesquisar o nome de domínio usado pelo dispositivo.

DNS servers (Servidores DNS): Clique em **Add DNS server (Adicionar servidor DNS)** e insira o endereço IP do servidor DNS. Esse servidor fornece a tradução dos nomes de host em endereços IP na sua rede.

HTTP e HTTPS

O HTTPS é um protocolo que fornece criptografia para solicitações de páginas de usuários e para as páginas retornadas pelo servidor Web. A troca de informações de criptografia é regida pelo uso de um certificado HTTPS que garante a autenticidade do servidor.

Para usar HTTPS no dispositivo, é necessário instalar certificado HTTPS. Vá para **System > Security (Sistema > Segurança)** para criar e instalar certificados.

Allow access through (Permitir acesso via): Selecione se um usuário tem permissão para se conectar ao dispositivo via protocolos **HTTP**, **HTTPS** ou **HTTP and HTTPS (HTTP e HTTPS)**.

Observação

Se você exibir páginas da Web criptografadas via HTTPS, talvez haja uma queda no desempenho, especialmente quando uma página é solicitada pela primeira vez.

HTTP port (Porta HTTP): Insira a porta HTTP que será usada. O dispositivo permite a porta 80 ou qualquer porta no intervalo 1024 – 65535. Se você estiver conectado como um administrador, também poderá inserir qualquer porta no intervalo 1 – 1023. Se você usar uma porta nesse intervalo, receberá um aviso.

HTTPS port (Porta HTTPS): Insira a porta HTTPS que será usada. O dispositivo permite a porta 443 ou qualquer porta no intervalo 1024 – 65535. Se você estiver conectado como um administrador, também poderá inserir qualquer porta no intervalo 1 – 1023. Se você usar uma porta nesse intervalo, receberá um aviso.

Certificate (Certificado): Selecione um certificado para ativar o HTTPS para o dispositivo.

Protocolos de descoberta de rede

Bonjour®: Ative para permitir a descoberta automática na rede.

Nome Bonjour: Insira um nome amigável para ser visível na rede. O nome padrão é o nome do dispositivo e seu endereço MAC.

UPnP®: Ative para permitir a descoberta automática na rede.

Nome UPnP: Insira um nome amigável para ser visível na rede. O nome padrão é o nome do dispositivo e seu endereço MAC.

WS-Discovery: Ative para permitir a descoberta automática na rede.

LLDP e CDP: Ative para permitir a descoberta automática na rede. Desligar as configurações LLDP e o CDP pode afetar a negociação de energia PoE. Para resolver quaisquer problemas com a negociação de energia PoE, configure a chave PoE somente para negociação de energia PoE de hardware.

Proxies globais

Http proxy (Proxy Http): Especifique um host proxy global ou um endereço IP de acordo com o formato permitido.

Https proxy (Proxy Https): Especifique um host proxy global ou um endereço IP de acordo com o formato permitido.

Formatos permitidos para proxies http e https:

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

Observação

Reinicie o dispositivo para aplicar as configurações de proxy global.

No proxy (Nenhum proxy): use **No proxy (Nenhum proxy)** para ignorar os proxies globais. Digite uma das opções da lista ou várias opções separadas por vírgula:

- Deixar vazio
- Especificar um endereço IP
- Especificar um endereço IP no formato CIDR
- Especifique um nome de domínio, por exemplo: www.<nome de domínio>.com
- Especifique todos os subdomínios em um domínio específico, por exemplo, .<nome de domínio>.com

Conexão com a nuvem com apenas um clique

O One-Click Cloud Connect (O3C), em conjunto com um serviço O3C, fornece acesso via Internet fácil e seguro a vídeo ao vivo e gravado a partir de qualquer local. Para obter mais informações, consulte *axis.com/end-to-end--solutions/hosted-services*.

Allow O3C (Permitir O3C):

- **One-click (Um clique)**: Esta é a opção padrão. Para conectar ao O3C, pressione o botão de controle no dispositivo. Dependendo do modelo do dispositivo, pressione e solte ou pressione e segure, até que o LED status pisque. Registre o dispositivo no serviço O3C dentro de 24 horas para ativar a opção **Always (Sempre)** e permanecer conectado. Se o dispositivo não for registrado, ele será desconectado do O3C.
- **Sempre**: O dispositivo tenta continuamente estabelecer conexão com um serviço O3C pela Internet. Depois de registrar o dispositivo, ele permanecerá conectado. Use essa opção se o botão de controle estiver fora de alcance.
- **No (Não)**: Desconecta o serviço O3C.

Proxy settings (Configurações de proxy): Se necessário, insira as configurações de proxy para conectar ao servidor proxy.

Host: Insira o endereço do servidor proxy.

Porta: Insira o número da porta usada para acesso.

Login e **Senha**: Se necessário, insira um nome de usuário e uma senha para o servidor proxy.

Authentication method (Método de autenticação):

- **Básico**: Este método é o esquema de autenticação mais compatível para HTTP. Ele é menos seguro do que o método de **Digest**, pois ele envia o nome de usuário e a senha não criptografados para o servidor.
- **Digest**: Esse método é mais seguro porque sempre transfere a senha criptografada pela rede.
- **Auto**: Essa opção permite que o dispositivo selecione o método de autenticação automaticamente dependendo dos métodos suportados. Ela prioriza o método **Digest** sobre o método **Básico**.

Owner authentication key (OAK) (Chave de autenticação do proprietário (OAK): Clique em **Get key (Obter chave)** para buscar a chave de autenticação do proprietário. Isso só será possível se o dispositivo estiver conectado à Internet sem um firewall ou proxy.

SNMP

O Simple Network Management Protocol (SNMP) possibilita o acesso e o gerenciamento remotos de dispositivos de rede.

SNMP: Selecione a versão de SNMP que deve ser utilizada.

- **v1 and v2c (v1 e v2c)**:
  - **Read community (Comunidade de leitura)**: Insira o nome da comunidade que tem acesso somente de leitura a todos os objetos SNMP suportados. O valor padrão é **public**.
  - **Write community (Comunidade de gravação)**: Insira o nome da comunidade que tem acesso de leitura ou gravação em todos os objetos SNMP suportados (exceto objetos somente leitura). O valor padrão é **gravação**.
  - **Activate traps (Ativar interceptações)**: Ative para ativar o relatório de interceptações. O dispositivo usa interceptações para enviar mensagens sobre eventos importantes ou alterações de status para um sistema de gerenciamento. Na interface Web, você pode configurar interceptações para SNMP v1 e v2c. As interceptações serão desativadas automaticamente se você mudar para SNMP v3 ou desativar o SNMP. Se você usa SNMP v3, é possível configurar interceptações via aplicativo de gerenciamento do SNMP v3.
  - **Trap address (Endereço da interceptação)**: Insira o endereço IP ou nome de host do servidor de gerenciamento.
  - **Trap community (Comunidade de interceptação)**: Insira a comunidade que é usada quando o dispositivo envia uma mensagem de interceptação para o sistema de gerenciamento.
  - **Traps (Interceptações)**:
    - **Cold start (Partida a frio)**: Envia uma mensagem de interceptação quando o dispositivo é iniciado.
    - **Link up (Link ativo)**: Envia uma mensagem de interceptação quando um link muda de inativo para ativo.
    - **Link down (Link inativo)**: Envia uma mensagem de interceptação quando um link muda de ativo para inativo.
    - **Falha de autenticação**: Envia uma mensagem de interceptação quando uma tentativa de autenticação falha.

Observação

Todas as interceptações MIB de vídeo Axis são habilitados quando você ativa as interceptações SNMP v1 e v2c. Para obter mais informações, consulte *AXIS OS portal > SNMP*.

- **v3**: O SNMP v3 é uma versão mais segura que fornece criptografia e senhas seguras. Para usar o SNMP v3, recomendamos ativar o HTTPS, pois as senhas serão enviadas via HTTPS. Isso também impede que partes não autorizadas acessem interceptações SNMP v1 e v2c não criptografadas. Se você usa SNMP v3, é possível configurar interceptações via aplicativo de gerenciamento do SNMP v3.
  - **Password for the account "initial" (Senha para a conta "initial")**: Insira a senha do SNMP para a conta chamada "initial". Embora a senha possa ser enviada sem ativar o HTTPS, isso não é recomendável. A senha do SNMP v3 só pode ser definida uma vez e, preferivelmente, quando o HTTPS está ativado. Após a senha ser definida, o campo de senha não será mais exibido. Para definir a senha novamente, o dispositivo deverá ser redefinido para as configurações padrões de fábrica.

Segurança

Certificados

Certificados são usados para autenticar dispositivos em uma rede. O dispositivo oferece suporte a dois tipos de certificados:

- **Certificados cliente/servidor**
  Um certificado cliente/servidor valida a identidade do produto e pode ser autoassinado ou emitido por uma autoridade de certificação (CA). Um certificado autoassinado oferece proteção limitada e pode ser usado antes que um certificado emitido por uma CA tenha sido obtido.
- **Certificados CA**
  Você pode usar um certificado de CA para autenticar um certificado de par, por exemplo, para validar a identidade de um servidor de autenticação quando o dispositivo se conecta a uma rede protegida por IEEE 802.1X. O dispositivo possui vários certificados de CA pré-instalados.

Os seguintes formatos são aceitos:

- Formatos de certificado: .PEM, .CER e .PFX
- Formatos de chave privada: PKCS#1 e PKCS#12

Importante

Se você redefinir o dispositivo para o padrão de fábrica, todos os certificados serão excluídos. Quaisquer certificados de CA pré-instalados serão reinstalados.

Adicionar certificado : Clique para adicionar um certificado. Um guia passo a passo é aberto.

- **Mais** : Mostrar mais campos para preencher ou selecionar.
- **Secure keystore (Armazenamento de chaves seguro)**: Selecione para usar **Trusted Execution Environment (SoC TEE)**, **Secure element** (Elemento seguro) ou **Trusted Platform Module 2.0** para armazenar de forma segura a chave privada. Para obter mais informações sobre qual armazenamento de chaves seguro selecionar, acesse *help.axis.com/axis-os#cryptographic-support*.
- **Tipo da chave**: Selecione o algoritmo de criptografia padrão ou diferente na lista suspensa para proteger o certificado.

O menu de contexto contém:

- **Certificate information (Informações do certificado)**: Exiba as propriedades de um certificado instalado.
- **Delete certificate (Excluir certificado)**: Exclua o certificado.
- **Create certificate signing request (Criar solicitação de assinatura de certificado)**: Crie uma solicitação de assinatura de certificado para enviar a uma autoridade de registro para se aplicar para um certificado de identidade digital.

Secure keystore (Armazenamento de chaves seguro) :

- **Trusted Execution Environment (SoC TEE)**: Selecione para usar o SoC TEE para armazenamento de chaves seguro.
- **Secure element (CC EAL6+) (Elemento seguro (CC EAL6+))**: Selecione para usar o elemento seguro no armazenamento de chaves seguro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Nível 2)**: Selecione para usar TPM 2.0 para armazenamento de chaves seguro.

Controle de acesso à rede e criptografia

IEEE 802.1x

O IEEE 802.1x é um padrão do IEEE para controle de admissão em redes baseado em portas que fornece autenticação segura de dispositivos em rede com e sem fio. O IEEE 802.1x é baseado no EAP (Extensible Authentication Protocol).

Para acessar uma rede protegida pelo IEEE 802.1x, os dispositivos de rede devem se autenticar. A autenticação é executada por um servidor de autenticação, geralmente, um servidor RADIUS (por exemplo, FreeRADIUS e Microsoft Internet Authentication Server).

IEEE 802.1AE MACsec

O IEEE 802.1AE MACsec é um padrão IEEE para segurança de controle de acesso à mídia (MAC) que define a confidencialidade e integridade de dados sem conexão para protocolos independentes de acesso à mídia.

Certificados

Quando configurado sem um certificado de CA, a validação do certificado do servidor é desativada e o dispositivo tenta se autenticar independentemente da rede à qual está conectado.

Ao usar um certificado, na implementação da Axis, o dispositivo e o servidor de autenticação se autenticam com certificados digitais usando EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

Para permitir que o dispositivo acesse uma rede protegida por certificados, é necessário instalar um certificado de cliente assinado no dispositivo.

Authentication method (Método de autenticação): Selecione um tipo de EAP usado para autenticação.

Client certificate (Certificado de cliente): Selecione um certificado de cliente para usar o IEEE 802.1x. O servidor de autenticação usa o certificado para validar a identidade do cliente.

CA certificates (Certificados CA): Selecione certificados CA para validar identidade do servidor de autenticação. Quando nenhum certificado é selecionado, o dispositivo tenta se autenticar independentemente da rede à qual está conectado.

EAP identity (Identidade EAP): Insira a identidade do usuário associada ao seu certificado de cliente.

EAPOL version (Versão EAPOL): Selecione a versão EAPOL que é usada no switch de rede.

Use IEEE 802.1x (Usar IEEE 802.1x): Selecione para usar o protocolo IEEE 802.1 x.

Essas configurações só estarão disponíveis se você usar **IEEE 802.1x PEAP-MSCHAPv2** como método de autenticação:

- **Senha**: Insira a senha para sua identidade de usuário.
- **Peap version (Versão do Peap)**: Selecione a versão do Peap que é usada no switch de rede.
- **Label (Rótulo)**: Selecione 1 para usar a criptografia EAP do cliente; selecione 2 para usar a criptografia PEAP do cliente. Selecione o rótulo que o switch de rede usa ao utilizar a versão 1 do Peap.

Essas configurações só estarão disponíveis se você usar o **IEEE 802.1ae MACsec (CAK estático/chave pré-compartilhada)** como método de autenticação:

- **Nome da chave de associação de conectividade do acordo de chaves**: Insira o nome da associação de conectividade (CKN). Deve ter de 2 a 64 (divisível por 2) caracteres hexadecimais. O CKN deve ser configurado manualmente na associação de conectividade e deve corresponder em ambas as extremidades do link para ativar inicialmente o MACsec.
- **Chave de associação de conectividade do acordo de chaves**: Insira a chave da associação de conectividade (CAK). Ela deve ter 32 ou 64 caracteres hexadecimais. O CAK deve ser configurado manualmente na associação de conectividade e deve corresponder em ambas as extremidades do link para ativar inicialmente o MACsec.

Impedir ataques de força bruta

Blocking (Bloqueio): Ative para bloquear ataques de força bruta. Um ataque de força bruta usa tentativa e erro para adivinhar informações de login ou chaves de criptografia.

Blocking period (Período de bloqueio): Insira o número de segundos para bloquear um ataque de força bruta.

Blocking conditions (Condições de bloqueio): Insira o número de falhas de autenticação permitidas por segundo antes do início do bloco. Você pode definir o número de falhas permitidas em nível de página ou em nível de dispositivo.

Firewall

Firewall: Ative para ativar o firewall.

Default Policy (Política padrão): Selecione como você deseja que o firewall trate as solicitações de conexão não cobertas por regras.

- **ACCEPT (ACEITAR):** Permite todas as conexões com o dispositivo. Essa opção é definida por padrão.
- **DROP (DESCARTAR):** Bloqueia todas as conexões com o dispositivo.

Para criar exceções à política padrão, você pode criar regras que permitem ou bloqueiam conexões com o dispositivo a partir de endereços, protocolos e portas específicos.

+ New rule (+ Nova regra): clique para criar uma regra.

Rule type (Tipo de regra):

- **FILTER (FILTRAR)**: Selecione para permitir ou bloquear conexões de dispositivos que correspondam aos critérios definidos na regra.
  - **Policy (Política)**: Selecione **Accept (Aceitar)** ou **Drop (Descartar)** a regra de firewall.
  - **IP range (Faixa IP)**: Selecione para especificar uma faixa de endereços a serem permitidos ou bloqueados. Use IPv4/IPv6 em **Start (Início)** e **End (Fim)**.
  - **Endereço IP**: Digite um endereço que você deseja permitir ou bloquear. Use o formato IPv4/ /IPv6 ou CIDR.
  - **Protocol (Protocolo)**: Selecione um protocolo de rede (TCP, UDP ou ambos) para permitir ou bloquear. Se você selecionar um protocolo, também deverá especificar uma porta.
  - **MAC**: Digite o endereço MAC de um dispositivo que você deseja permitir ou bloquear.
  - **Port range (Faixa de portas)**: Selecione para especificar a faixa de portas a serem permitidas ou bloqueadas. Adicione-as a **Start (Início)** e **End (Fim)**.
  - **Porta**: Insira um número de porta que você deseje permitir ou bloquear. Os números de portas devem estar entre 1 e 65535.
  - **Traffic type (Tipo de tráfego)**: Selecione um tipo de tráfego que você deseja permitir ou bloquear.
    - **UNICAST**: Tráfego de um único remetente para um único destinatário.
    - **BROADCAST**: Tráfego de um único remetente para todos os dispositivos na rede.
    - **MULTICAST**: Tráfego de um ou mais remetentes para um ou mais destinatários.
- **LIMIT (LIMITAR)**: Selecione para aceitar conexões de dispositivos que correspondam aos critérios definidos na regra, mas aplique limites para reduzir o tráfego excessivo.
  - **IP range (Faixa IP)**: Selecione para especificar uma faixa de endereços a serem permitidos ou bloqueados. Use IPv4/IPv6 em **Start (Início)** e **End (Fim)**.
  - **Endereço IP**: Digite um endereço que você deseja permitir ou bloquear. Use o formato IPv4/ /IPv6 ou CIDR.
  - **Protocol (Protocolo)**: Selecione um protocolo de rede (TCP, UDP ou ambos) para permitir ou bloquear. Se você selecionar um protocolo, também deverá especificar uma porta.
  - **MAC**: Digite o endereço MAC de um dispositivo que você deseja permitir ou bloquear.
  - **Port range (Faixa de portas)**: Selecione para especificar a faixa de portas a serem permitidas ou bloqueadas. Adicione-as a **Start (Início)** e **End (Fim)**.
  - **Porta**: Insira um número de porta que você deseje permitir ou bloquear. Os números de portas devem estar entre 1 e 65535.
  - **Unit (Unidade)**: Selecione o tipo de conexão a ser permitida ou bloqueada.
  - **Period (Período)**: Selecione o período de tempo relacionado a **Amount (Quantidade)**.
  - **Amount (Quantidade)**: Defina o número máximo de vezes que um dispositivo tem permissão para se conectar dentro do período definido em **Period (Período)**. O valor máximo é 65535.

- **Burst (Surto)**: Insira o número de conexões que podem exceder o valor definido em **Amount (Quantidade)** uma vez durante o período definido em **Period (Período)**. Quando o número for atingido, somente a quantidade definida durante o período definido será permitida.
- **Traffic type (Tipo de tráfego)**: Selecione um tipo de tráfego que você deseja permitir ou bloquear.
  - **UNICAST**: Tráfego de um único remetente para um único destinatário.
  - **BROADCAST**: Tráfego de um único remetente para todos os dispositivos na rede.
  - **MULTICAST**: Tráfego de um ou mais remetentes para um ou mais destinatários.

Test rules (Testar regras): Clique para testar as regras que você definiu.

- **Test time in seconds (Tempo de teste em segundos)**: Defina um limite de tempo para testar as regras.
- **Roll back (Reverter)**: Clique para reverter o firewall ao seu estado anterior, antes de testar as regras.
- **Apply rules (Aplicar regras)**: Clique para ativar as regras sem testar. Não recomendamos fazer isso.

Certificado do AXIS OS com assinatura personalizada

Para instalar o software de teste ou outro software personalizado da Axis no dispositivo, certificado do AXIS OS com assinatura personalizada é necessário. O certificado verifica se o software é aprovado pelo proprietário do dispositivo e pela Axis. O software só pode ser executado em um dispositivo específico identificado por seu número de série e ID de chip exclusivos. Somente a Axis pode criar certificados do AXIS OS com assinatura personalizada, pois é a Axis que possui a chave para assiná-los.

Install (Instalar): Clique para instalar o certificado. É necessário instalar o certificado antes de instalar o software.

O menu de contexto contém:

- **Delete certificate (Excluir certificado)**: Exclua o certificado.

Contas

Contas

Adicionar conta: Clique para adicionar uma nova conta. É possível adicionar até 100 contas.

Account (Conta): Insira um nome de conta exclusivo.

New password (Nova senha): Insira uma senha para o nome da conta. As senhas devem conter 1 a 64 caracteres de comprimento. Somente caracteres ASCII imprimíveis (código 32 a 126) são permitidos na senha, por exemplo, letras, números, pontuação e alguns símbolos.

Repeat password (Repetir senha): Insira a mesma senha novamente.

Privileges (Privilégios):

- **Administrator (Administrador)**: Tem acesso irrestrito a todas as configurações. Os administradores também podem adicionar, atualizar e remover outras contas.
- **Operator (Operador)**: Tem acesso a todas as configurações, exceto:
  - Todas as configurações do **System (Sistema)**.
- **Viewer (Visualizador)**: Não tem acesso para alterar as configurações.

O menu de contexto contém:

Update account (Atualizar conta): Edite as propriedades da conta.

Delete account (Excluir conta): Exclua a conta. Não é possível excluir a conta root.

Acesso anônimo

Allow anonymous viewing (Permitir visualização anônima): Ative para permitir que qualquer pessoa acesse o dispositivo como um visualizador sem precisar fazer login com uma conta.

Permitir operação de PTZ anônima : Ative para permitir que usuários anônimos façam pan, tilt e zoom da imagem.

Contas SSH

Adicionar conta SSH: Clique para adicionar uma nova conta SSH.

- **Enable SSH (Ativar SSH)**: Ative para usar o serviço SSH.

Account (Conta): Insira um nome de conta exclusivo.

New password (Nova senha): Insira uma senha para o nome da conta. As senhas devem conter 1 a 64 caracteres de comprimento. Somente caracteres ASCII imprimíveis (código 32 a 126) são permitidos na senha, por exemplo, letras, números, pontuação e alguns símbolos.

Repeat password (Repetir senha): Insira a mesma senha novamente.

Comentário: Insira um comentário (opcional).

O menu de contexto contém:

Update SSH account (Atualizar conta SSH): Edite as propriedades da conta.

Delete SSH account (Excluir conta SSH): Exclua a conta. Não é possível excluir a conta root.

Virtual host (Host virtual)

Add virtual host (Adicionar host virtual): clique para adicionar um novo host virtual.

Enabled (Ativado): selecione para usar este host virtual.

Server name (Nome do servidor): insira o nome do servidor. Use somente números 0 – 9, letras A – Z e hífen (-).

Porta: insira a porta à qual o servidor está conectado.

Tipo: selecione o tipo de autenticação que será usada. Selecione entre **Basic**, **Digest** e **Open ID**.

O menu de contexto contém:

- **Update (Atualizar)**: atualizar o host virtual.
- **Excluir**: excluir o host virtual.

Disabled (Desativado): o servidor está desativado.

Configuração de concessão de credenciais de cliente

Reivindicação de administrador: Insira um valor para a função de administrador.

Verification URI (URI de verificação): Insira o link Web para a autenticação do ponto de extremidade de API.

Reivindicação de operador: Insira um valor para a função do operador.

Exigir reivindicação: Insira os dados que deveriam estar no token.

Reivindicação de visualizador: insira o valor da função de visualizador.

Save (Salvar): Clique para salvar os valores.

Configuração de OpenID

Importante

Se você não puder usar OpenID para fazer login, use as credenciais Digest ou Básicas que você usou quando configurou OpenID para fazer login.

Client ID (ID do cliente): Insira o nome de usuário de OpenID.

Proxy de saída: insira o endereço proxy da conexão OpenID para usar um servidor proxy.

Reivindicação de administrador: Insira um valor para a função de administrador.

URL do provedor: Insira o link Web para a autenticação do ponto de extremidade de API. O formato deve ser https://[inserir URL]/.bem conhecido/openid-configuration

Reivindicação de operador: Insira um valor para a função do operador.

Exigir reivindicação: Insira os dados que deveriam estar no token.

Reivindicação de visualizador: insira o valor da função de visualizador.

Remote user (Usuário remoto): insira um valor para identificar usuários remotos. Isso ajudará a exibir o usuário atual na interface Web do dispositivo.

Scopes (Escopos): Escopos opcionais que poderiam fazer parte do token.

Segredo do cliente: Insira a senha OpenID novamente

Save (Salvar): Clique em para salvar os valores de OpenID.

Ativar OpenID: Ative para fechar a conexão atual e permita a autenticação do dispositivo via URL do provedor.

Eventos

Regras

Uma regra define as condições que fazem com que o produto execute uma ação. A lista mostra todas as regras configuradas no produto no momento.

Observação

Você pode criar até 256 regras de ação.

Adicionar uma regra: Crie uma regra.

Nome: Insira um nome para a regra.

Wait between actions (Aguardar entre ações): insira o tempo mínimo (hh:mm:ss) que deve passar entre ativações de regras. Ela será útil se a regra for ativada, por exemplo, em condições de modo diurno/noturno, para evitar que pequenas mudanças de iluminação durante o nascer e o pôr do sol ativem a regra várias vezes.

Condition (Condição): selecione uma condição na lista. Uma condição deve ser atendida para que o dispositivo execute uma ação. Se várias condições forem definidas, todas elas deverão ser atendidas para acionar a ação. Para obter informações sobre condições específicas, consulte *Introdução às regras de eventos*.

Use this condition as a trigger (Usar esta condição como acionador): selecione para que essa primeira função opere apenas como acionador inicial. Isso significa que, uma vez que a regra for ativada, ela permanecerá ativa enquanto todas as outras condições forem atendidas, independentemente do estado da primeira condição. Se você não marcar essa opção, a regra simplesmente será ativada quando todas as condições forem atendidas.

Invert this condition (Inverter esta condição): marque se você quiser que a condição seja o contrário de sua seleção.

Adicionar uma condição: clique para adicionar uma condição.

Action (Ação): selecione uma ação na lista e insira as informações necessárias. Para obter informações sobre ações específicas, consulte *Introdução às regras de eventos*.

Destinatários

Você pode configurar seu dispositivo para notificar os destinatários sobre eventos ou enviar arquivos.

Observação

Se você configurar seu dispositivo para usar FTP ou SFTP, não altere nem remova o número de sequência exclusivo que é adicionado aos nomes dos arquivos. Se fizer isso, apenas uma imagem por evento poderá ser enviada.

A lista mostra todos os destinatários atualmente configurados no produto, juntamente com informações sobre suas configurações.

Observação

É possível criar até 20 destinatários.

Add a recipient (Adicionar um destinatário): clique para adicionar um destinatário.

Nome: insira um nome para o destinatário.

Tipo: selecione na lista:

- FTP
  - **Host**: insira o endereço IP ou o nome de host do servidor. Se você inserir um nome de host, verifique se um servidor DNS está especificado em **System > Network > IPv4 and IPv6 (Sistema > Rede > IPv4 e IPv6)**.
  - **Porta**: Insira o número da porta usada pelo servidor FTP. O padrão é 21.
  - **Folder (Pasta)**: insira o caminho para o diretório em que deseja armazenar arquivos. Se esse diretório ainda não existir no servidor FTP, você receberá uma mensagem de erro ao fazer upload de arquivos.
  - **Username (Nome de usuário)**: insira o nome de usuário para o login.
  - **Senha**: insira a senha para o login.
  - **Use temporary file name (Usar nome de arquivo temporário)**: marque para carregar arquivos com nomes temporários e gerados automaticamente. Os arquivos serão renomeados para os nomes desejados quando o upload for concluído. Se o upload for cancelado/interrompido, nenhum arquivo será corrompido. No entanto, provavelmente você ainda obterá os arquivos temporários. Dessa forma, você saberá que todos os arquivos com o nome desejado estão corretos.
  - **Use passive FTP (Usar FTP passivo)**: Em circunstâncias normais, o produto simplesmente solicita que o servidor FTP de destino abra a conexão de dados. O dispositivo inicia ativamente as conexões de controle de FTP e dados para o servidor de destino. Isso é normalmente necessário quando há um firewall entre o dispositivo e o servidor FTP de destino.
- HTTP
  - **URL**: Insira o endereço de rede do servidor HTTP e o script que cuidará da solicitação. Por exemplo, http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Nome de usuário)**: insira o nome de usuário para o login.
  - **Senha**: insira a senha para o login.
  - **Proxy**: ative e insira as informações necessárias se houver a necessidade de passar por um servidor proxy para se conectar ao servidor HTTP.
- HTTPS
  - **URL**: Insira o endereço de rede do servidor HTTPS e o script que cuidará da solicitação. Por exemplo, https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Validar certificado do servidor)**: marque para validar o certificado que foi criado pelo servidor HTTPS.
  - **Username (Nome de usuário)**: insira o nome de usuário para o login.
  - **Senha**: insira a senha para o login.
  - **Proxy**: ative e insira as informações necessárias se houver a necessidade de passar por um servidor proxy para se conectar ao servidor HTTPS.
- Armazenamento de rede
  Você pode adicionar armazenamento de rede, como um NAS (Network Attached Storage), e utilizá-lo como destinatário para armazenar arquivos. Os arquivos são armazenados no formato Matroska (MKV).
  - **Host**: Insira o endereço IP ou o nome de host do armazenamento de rede.
  - **Compartilhamento**: Insira o nome do compartilhamento no host.

- **Folder (Pasta)**: insira o caminho para o diretório em que deseja armazenar arquivos.
- **Username (Nome de usuário)**: insira o nome de usuário para o login.
- **Senha**: insira a senha para o login.

- SFTP
  - **Host**: insira o endereço IP ou o nome de host do servidor. Se você inserir um nome de host, verifique se um servidor DNS está especificado em **System > Network > IPv4 and IPv6 (Sistema > Rede > IPv4 e IPv6)**.
  - **Porta**: Insira o número da porta usada pelo servidor SFTP. O padrão é 22.
  - **Folder (Pasta)**: insira o caminho para o diretório em que deseja armazenar arquivos. Se esse diretório ainda não existir no servidor SFTP, você receberá uma mensagem de erro ao fazer upload de arquivos.
  - **Username (Nome de usuário)**: insira o nome de usuário para o login.
  - **Senha**: insira a senha para o login.
  - **SSH host public key type (MD5) (Tipo de chave pública do host SSH [MD5])**: insira a impressão digital da chave pública do host remoto (sequência de 32 dígitos hexadecimais). O cliente SFTP oferece suporte a servidores SFTP que utilizam SSH-2 com os tipos de chave de host RSA, DSA, ECDSA e ED25519. RSA é o método preferido durante a negociação, seguido por ECDSA, ED25519 e DSA. Certifique-se de inserir a chave de host MD5 certa que é usada pelo seu servidor SFTP. Embora o dispositivo Axis ofereça suporte a chaves de hash MD5 e SHA-256, recomenda-se usar a SHA-256 devido à segurança mais forte do que o MD5. Para obter mais informações sobre como configurar um servidor SFTP com um dispositivo Axis, acesse o *Portal do AXIS OS*.
  - **SSH host public key type (SHA256) (Tipo de chave pública do host SSH [SHA256])**: insira a impressão digital da chave pública do host remoto (string codificada em Base64 com 43 dígitos). O cliente SFTP oferece suporte a servidores SFTP que utilizam SSH-2 com os tipos de chave de host RSA, DSA, ECDSA e ED25519. RSA é o método preferido durante a negociação, seguido por ECDSA, ED25519 e DSA. Certifique-se de inserir a chave de host MD5 certa que é usada pelo seu servidor SFTP. Embora o dispositivo Axis ofereça suporte a chaves de hash MD5 e SHA-256, recomenda-se usar a SHA-256 devido à segurança mais forte do que o MD5. Para obter mais informações sobre como configurar um servidor SFTP com um dispositivo Axis, acesse o *Portal do AXIS OS*.
  - **Use temporary file name (Usar nome de arquivo temporário)**: marque para carregar arquivos com nomes temporários e gerados automaticamente. Os arquivos serão renomeados para os nomes desejados quando o upload for concluído. Se o upload for cancelado ou interrompido, nenhum arquivo será corrompido. No entanto, provavelmente você ainda obterá os arquivos temporários. Dessa forma, você saberá que todos os arquivos com o nome desejado estão corretos.

- SIP ou VMS :
  SIP: Selecione para fazer uma chamada SIP.
  VMS: Selecione para fazer uma chamada VMS.
  - **From SIP account (Da conta SIP)**: selecione na lista.
  - **To SIP address (Para endereço SIP)**: Insira o endereço SIP.
  - **Teste**: Clique para testar se suas configurações de chamada funcionam.
- **E-mail**
  - **Enviar email para**: insira o endereço para enviar os emails. Para inserir vários emails, use vírgulas para separá-los.
  - **Enviar email de**: insira o endereço de email do servidor de envio.
  - **Username (Nome de usuário)**: insira o nome de usuário para o servidor de email. Deixe esse campo em branco se o servidor de email não precisar de autenticação.

- **Senha**: insira a senha para o servidor de email. Deixe esse campo em branco se o servidor de email não precisar de autenticação.
- **Email server (SMTP) (Servidor de email (SMTP))**: Insira o nome do servidor SMTP. Por exemplo, smtp.gmail.com, smtp.mail.yahoo.com.
- **Porta**: Insira o número da porta do servidor SMTP usando valores na faixa 0 – 65535. O valor padrão é 587.
- **Criptografia**: para usar criptografia, selecione SSL ou TLS.
- **Validate server certificate (Validar certificado do servidor)**: se você usar criptografia, marque para validar a identidade do dispositivo. O certificado pode ser autoassinado ou emitido por uma Autoridade de Certificação (CA).
- **POP authentication (Autenticação POP)**: Ative para inserir o nome do servidor POP. Por exemplo, pop.gmail.com.

Observação

Alguns provedores de email possuem filtros que impedem que os usuários recebam ou exibam anexos grandes, emails recorrentes e outros semelhantes. Verifique a política de segurança do provedor de email para evitar que sua conta de email seja bloqueada ou que as mensagens que você está esperando não sejam recebidas.

- **TCP**
  - **Host**: insira o endereço IP ou o nome de host do servidor. Se você inserir um nome de host, verifique se um servidor DNS está especificado em **System > Network > IPv4 and IPv6 (Sistema > Rede > IPv4 e IPv6)**.
  - **Porta**: Insira o número da porta usada para acessar o servidor.

Testar: clique para testar a configuração.

O menu de contexto contém:

View recipient (Exibir destinatário): clique para exibir todos os detalhes do destinatário.

Copy recipient (Copiar destinatário): clique para copiar um destinatário. Ao copiar, você pode fazer alterações no novo destinatário.

Delete recipient (Excluir destinatário): clique para excluir o destinatário permanentemente.

Programações

Agendamentos e pulsos podem ser usados como condições em regras. A lista mostra todas os agendamentos e pulsos configurados no momento no produto, juntamente com várias informações sobre suas configurações.

Adicionar agendamento: clique para criar um cronograma ou pulso.

Acionadores manuais

É possível usar o acionador manual para acionar manualmente uma regra. O acionador manual pode ser usado, por exemplo, para validar ações durante a instalação e a configuração do produto.

MQTT

O MQTT (Message Queuing Telemetry Transport) é um protocolo de troca de mensagens padrão para a Internet das Coisas (IoT). Ele foi desenvolvido para integração simplificada com a IoT e é usado em uma ampla variedade de setores para conectar dispositivos remotos com o mínimo de código e largura de banda de rede. O cliente MQTT no software do dispositivo Axis pode simplificar a integração de dados e eventos produzidos no dispositivo a sistemas que não são software de gerenciamento de vídeo (VMS).

Configure o dispositivo como um cliente MQTT. A comunicação MQTT baseia-se em duas entidades, os clientes e o broker. Os clientes podem enviar e receber mensagens. O broker é responsável por rotear mensagens entre os clientes.

Saiba mais sobre MQTT na *Base de conhecimento do AXIS OS*.

ALPN

O ALPN é uma extensão do TLS/SSL que permite a seleção de um protocolo de aplicação durante a fase de handshake da conexão entre o cliente e o servidor. Isso é usado para permitir o tráfego MQTT na mesma porta que é utilizada para outros protocolos, como o HTTP. Em alguns casos, pode não haver uma porta dedicada aberta para a comunicação MQTT. Uma solução nesses casos é usar o ALPN para negociar o uso do MQTT como protocolo de aplicação em uma porta padrão permitida pelos firewalls.

Cliente MQTT

Connect (Conectar): Ative ou desative o cliente MQTT.

Status: Mostra o status atual do cliente MQTT.

Broker

Host: Insira o nome de host ou endereço IP do servidor MQTT.

Protocol (Protocolo): Selecione o protocolo que será usado.

Porta: Insira o número da porta.

- 1883 é o valor padrão para **MQTT sobre TCP**
- 8883 é o valor padrão para **MQTT sobre SSL**
- 80 é o valor padrão para **MQTT sobre WebSocket**
- 443 é o valor padrão para **MQTT sobre WebSocket Secure**

Protocol ALPN: Insira o nome do protocolo ALPN fornecido pelo seu provedor de broker de MQTT. Isso se aplica apenas com MQTT sobre SSL e MQTT sobre o WebSocket Secure.

Username (Nome de usuário): Insira o nome de usuário que será usado pelo cliente para acessar o servidor.

Senha: Insira uma senha para o nome de usuário.

Client ID (ID do cliente): Insira um ID de cliente. O identificador do cliente é enviado para o servidor quando o cliente se conecta a ele.

Clean session (Limpar sessão): Controla o comportamento na conexão e na desconexão. Quando selecionada, as informações de estado são descartadas na conexão e desconexão.

HTTP proxy (Proxy HTTP): Um URL com comprimento máximo de 255 bytes. Deixe o campo vazio se não quiser usar um proxy HTTP.

HTTPS proxy (Proxy HTTPS): Um URL com comprimento máximo de 255 bytes. Deixe o campo vazio se não quiser usar um proxy HTTPS.

Keep alive interval (Intervalo de Keep Alive): Permite que o cliente detecte quando o servidor não está mais disponível sem que seja necessário aguardar o longo tempo limite de TCP/IP.

Timeout (Tempo limite): O intervalo de tempo em segundos para permitir que uma conexão seja concluída. Valor padrão: 60

Device topic prefix (Prefixo do tópico do dispositivo): Usado nos valores padrão para o tópico na mensagem de conexão e na mensagem de LWT na guia **MQTT client (Cliente MQTT)** e nas condições de publicação na guia **MQTT publication (Publicação MQTT)**.

Reconnect automatically (Reconectar automaticamente): Especifica se o cliente deve se reconectar automaticamente após uma desconexão.

Mensagem de conexão

Especifica se uma mensagem deve ser enviada quando uma conexão é estabelecida.

Send message (Enviar mensagem): ative para enviar mensagens.

Use default (Usar padrão): Desative para inserir sua própria mensagem padrão.

Topic (Tópico): insira o tópico para a mensagem padrão.

Payload (Carga): insira o conteúdo para a mensagem padrão.

Retain (Reter): selecione para manter o estado do cliente neste **Topic (Tópico)**

QoS: Altere a camada de QoS para o fluxo do pacote.

Mensagem de Último desejo e testamento

A opção Last Will Testament (LWT) permite que um cliente forneça uma prova juntamente com suas credenciais ao conectar ao broker. Se o cliente se desconectar abruptamente em algum momento mais tarde (talvez porque sua fonte de energia seja interrompida), ele pode permitir que o broker envie uma mensagem para outros clientes. Essa mensagem de LWT tem o mesmo formato que uma mensagem comum e é roteada através da mesma mecânica.

Send message (Enviar mensagem): ative para enviar mensagens.

Use default (Usar padrão): Desative para inserir sua própria mensagem padrão.

Topic (Tópico): insira o tópico para a mensagem padrão.

Payload (Carga): insira o conteúdo para a mensagem padrão.

Retain (Reter): selecione para manter o estado do cliente neste **Topic (Tópico)**

QoS: Altere a camada de QoS para o fluxo do pacote.

Publicação MQTT

Use default topic prefix (Usar prefixo de tópico padrão): selecione para usar o prefixo de tópico padrão, o qual é definido com o uso do prefixo de tópico de dispositivo na guia **MQTT client (Cliente MQTT)**.

Include topic name (Incluir nome do tópico): selecione para incluir o tópico que descreve a condição no tópico MQTT.

Include topic namespaces (Incluir namespaces de tópico): selecione para incluir espaços para nome de tópico ONVIF no tópico MQTT.

Include serial number (Incluir número de série): selecione para incluir o número de série do dispositivo na carga MQTT.

Adicionar condição: clique para adicionar uma condição.

Retain (Reter): define quais mensagens MQTT são enviadas como retidas.

- **None (Nenhuma)**: envia todas as mensagens como não retidas.
- **Property (Propriedade)**: envia somente mensagens stateful como retidas.
- **All (Todas)**: envie mensagens stateful e stateless como retidas.

QoS: selecione o nível desejado para a publicação MQTT.

Assinaturas MQTT

Adicionar assinatura: clique para adicionar uma nova assinatura MQTT.

Subscription filter (Filtro de assinatura): insira o tópico MQTT no qual deseja se inscrever.

Use device topic prefix (Usar prefixo de tópico do dispositivo): adicione o filtro de assinatura como prefixo ao tópico MQTT.

Subscription type (Tipo de assinatura):

- **Stateless**: selecione para converter mensagens MQTT em mensagens stateless.
- **Stateful**: selecione para converter mensagens MQTT em condições. A carga é usada como estado.

QoS: selecione o nível desejado para a assinatura MQTT.

Sobreposições MQTT

Observação

Conecte a um broker de MQTT antes de adicionar modificadores de sobreposição MQTT.

Adicionar modificador de sobreposição: Clique para adicionar um novo modificador de sobreposição.

Topic filter (Filtro de tópicos): Adicione o tópico MQTT que contém os dados que deseja mostrar na sobreposição.

Data field (Campo de dados): Especifique a chave para a carga útil da mensagem que deseja mostrar na sobreposição, supondo que a mensagem esteja no formato JSON.

Modifier (Modificador): Use o modificador resultante ao criar a sobreposição.

- Os modificadores que começam com **#XMP** mostram todos os dados recebidos do tópico.
- Os modificadores que começam com **#XMD** mostram os dados especificados no campo de dados.

Armazenamento

Armazenamento de rede

Ignore (Ignorar): Ative para ignorar o armazenamento de rede.

Add network storage (Adicionar armazenamento de rede): clique para adicionar um compartilhamento de rede no qual você pode salvar as gravações.

- **Endereço**: insira o endereço IP ou nome de host do servidor host, em geral, um NAS (armazenamento de rede). Recomendamos configurar o host para usar um endereço IP fixo (e não DHCP, pois os endereços IP dinâmicos podem mudar) ou então usar DNS. Não há suporte a nomes SMB/CIFS Windows.
- **Network share (Compartilhamento de rede)**: Insira o nome do local compartilhado no servidor host. Vários dispositivos Axis podem usar o mesmo compartilhamento de rede, já que cada dispositivo tem sua própria pasta.
- **User (Usuário)**: se o servidor exigir um login, insira o nome de usuário. Para fazer login em um servidor de domínio específico, digite `DOMAIN\username`.
- **Senha**: Se o servidor exigir um login, digite a senha.
- **SMB version (Versão SMB)**: selecione a versão do protocolo de armazenamento SMB para se conectar ao NAS. Se você selecionar **Auto**, o dispositivo tentará negociar uma das versões seguras de SMB: 3.02, 3.0 ou 2.1. Selecione 1.0 ou 2.0 para se conectar ao NAS antigo que não oferece suporte a versões posteriores. Leia mais sobre o suporte a SMB em dispositivos Axis *aqui*.
- **Add share without testing (Adicionar compartilhamento sem testar)**: selecione para adicionar o compartilhamento de rede mesmo se um erro for descoberto durante o teste de conexão. O erro pode ser, por exemplo, que você não digitou uma senha, embora o servidor precise de uma.

Remove network storage (Remover armazenamento em rede): Clique para desmontar, desvincular e remover a conexão com o compartilhamento de rede. Isso remove todas as configurações do compartilhamento de rede.

Unbind (Desvincular): Clique para desvincular e desconectar o compartilhamento de rede.
Bind (Vincular): Clique para vincular e conectar o compartilhamento de rede.

Unmount (Desmontar): Clique para desmontar o compartilhamento de rede.
Mount (Montar): Clique para montar o compartilhamento de rede.

Write protect (Proteção contra gravação): Ative para parar de gravar no compartilhamento de rede e proteger as gravações contra remoção. Não é possível formatar um compartilhamento de rede protegido contra gravação.

Retention time (Tempo de retenção): Selecione por quanto tempo as gravações serão mantidas para limitar a quantidade de gravações antigas ou atender a regulamentações relativas ao armazenamento de dados. Se o armazenamento de rede ficar cheio, as gravações antigas serão removidas antes do período de tempo selecionado se esgotar.

Ferramentas

- **Test connection (Testar conexão)**: Teste a conexão com o compartilhamento de rede.
- **Format (Formatar)**: formate o compartilhamento de rede, por exemplo, quando for necessário apagar rapidamente todos os dados. CIFS é a opção de sistema de arquivos disponível.

Use tool (Usar ferramenta): Clique para ativar a ferramenta selecionada.

Armazenamento interno

Importante

Risco de perda de dados ou gravações corrompidas. Não remova o cartão SD com o dispositivo em funcionamento. Desmonte o cartão SD antes de removê-lo.

Unmount (Desmontar): Clique para remover com segurança o cartão SD.

Write protect (Proteção contra gravação): Ative essa opção para parar de escrever no cartão SD e proteger as gravações contra remoção. Não é possível formatar um cartão SD protegido contra gravação.

Autoformat (Formatação automática): ative para formatar automaticamente um cartão SD recém-inserido. Ele formata o sistema de arquivos em ext4.

Ignore (Ignorar): ative para parar de armazenar gravações no cartão SD. Quando você ignora o cartão SD, o dispositivo passa a não reconhecer que o cartão existe. A configuração está disponível somente para administradores.

Retention time (Tempo de retenção): selecione por quanto tempo as gravações serão mantidas para limitar a quantidade de gravações antigas ou atender a regulamentações de armazenamento de dados. Quando o cartão SD está cheio, ele exclui gravações antigas antes que o tempo de retenção tenha passado.

Ferramentas

- **Check (Verificar)**: Verifica se há erros no cartão SD.
- **Repair (Reparar)**: Repare erros no sistema de arquivos.
- **Format (Formatar)**: Formate o cartão SD para alterar o sistema de arquivos e apagar todos os dados. Só é possível formatar o cartão SD para o sistema de arquivos ext4. Um driver ou aplicativo de terceiros compatível com ext4 será necessário para acessar o sistema de arquivos no Windows®.
- **Encrypt (Criptografar)**: Use essa ferramenta para formatar o cartão SD e ativar a criptografia. Isso exclui todos os dados armazenados no cartão SD. Todos os novos dados armazenados no cartão SD serão criptografados.
- **Decrypt (Descriptografar)**: Use essa ferramenta para formatar o cartão SD sem criptografia. Isso exclui todos os dados armazenados no cartão SD. Nenhum novo dado armazenado no cartão SD será criptografado.
- **Change password (Alterar senha)**: Altere a senha necessária para criptografar o cartão SD.

Use tool (Usar ferramenta): Clique para ativar a ferramenta selecionada.

Wear trigger (Acionador de uso): Defina um valor para o nível de uso do cartão SD no qual você deseja acionar uma ação. O nível de desgaste varia de 0 a 200%. Um novo cartão SD que nunca foi usado tem um nível de desgaste de 0%. Um nível de desgaste de 100% indica que o cartão SD está próximo de seu tempo de vida esperado. Quando o nível de desgaste atinge 200%, há um alto risco de falha do cartão SD. Recomendamos configurar o acionador de desgaste entre 80 – 90%. Isso permite baixar qualquer gravação, bem como substituir o cartão SD a tempo antes que ele possa se deteriorar. O acionador de desgaste permite a você configurar um evento e obter uma notificação quando o nível de desgaste atingir o valor definido.

Perfis de stream

Um perfil de stream é um grupo de configurações que afetam o stream de vídeo. Você pode usar perfis de stream em situações diferentes, por exemplo, ao criar eventos e usar regras para gravar.

Adicionar perfil de stream: Clique para criar um novo perfil de stream.

Preview (Visualizar): Uma visualização do stream de vídeo com as configurações de perfil de stream selecionadas por você. A visualização é atualizada quando você altera as configurações na página. Se seu dispositivo possuir áreas de exibição diferentes, você poderá alterar a área de exibição na lista suspensa no canto inferior esquerdo da imagem.

Nome: adicione um nome para seu perfil.

Description (Descrição): adicione uma descrição do seu perfil.

Video codec (Codec de vídeo): Selecione o codec de vídeo que deve ser aplicado ao perfil.

Resolução: Consulte para obter uma descrição desta configuração.

Taxa de quadros: Consulte para obter uma descrição desta configuração.

Compression (Compactação): Consulte para obter uma descrição desta configuração.

Zipstream : Consulte para obter uma descrição desta configuração.

Optimize for storage (Otimizar para armazenamento) : Consulte para obter uma descrição desta configuração.

FPS dinâmico : Consulte para obter uma descrição desta configuração.

Grupo de imagens dinâmico : Consulte para obter uma descrição desta configuração.

Mirror (Espelhar) : Consulte para obter uma descrição desta configuração.

Comprimento de GOP dinâmico : Consulte para obter uma descrição desta configuração.

Bitrate control (Controle de taxa de bits): Consulte para obter uma descrição desta configuração.

Incluir sobreposições : Selecione o tipo de sobreposições para incluir. Consulte para obter informações sobre como adicionar sobreposições.

Incluir áudio : Consulte para obter uma descrição desta configuração.

ONVIF

Contas ONVIF

O ONVIF (Open Network Video Interface Forum) é um padrão de interface global que facilita aos usuários finais, integradores, consultores e fabricantes aproveitarem as possibilidades oferecidas pela tecnologia de vídeo em rede. O ONVIF permite interoperabilidade entre produtos de diferentes fornecedores, maior flexibilidade, custo reduzido e sistemas sempre atuais.

Ao criar uma conta ONVIF, você ativa a comunicação ONVIF automaticamente. Use o nome da conta e a senha em toda a comunicação ONVIF com o dispositivo. Para obter mais informações, consulte a Comunidade de desenvolvedores Axis em *axis.com*.

Add accounts (Adicionar contas): Clique para adicionar um nova conta ONVIF.

Account (Conta): Insira um nome de conta exclusivo.

New password (Nova senha): Insira uma senha para o nome da conta. As senhas devem conter 1 a 64 caracteres de comprimento. Somente caracteres ASCII imprimíveis (código 32 a 126) são permitidos na senha, por exemplo, letras, números, pontuação e alguns símbolos.

Repeat password (Repetir senha): Insira a mesma senha novamente.

Role (Função):

- **Administrator (Administrador)**: Tem acesso irrestrito a todas as configurações. Os administradores também podem adicionar, atualizar e remover outras contas.
- **Operator (Operador)**: Tem acesso a todas as configurações, exceto:
  - Todas as configurações do **System (Sistema)**.
  - Adicionando aplicativos.
- **Media account (Conta de mídia)**: Permite acesso apenas ao stream de vídeo.

O menu de contexto contém:

Update account (Atualizar conta): Edite as propriedades da conta.

Delete account (Excluir conta): Exclua a conta. Não é possível excluir a conta root.

Perfis de mídia ONVIF

Um perfil de mídia ONVIF consiste em um conjunto de configurações que podem ser usadas para alterar opções de stream de mídia. Você pode criar novos perfis com seu próprio conjunto de configurações ou usar perfis pré-configurados para uma configuração rápida.

Adicionar perfil de mídia: clique para adicionar um novo perfil de mídia ONVIF.

Nome do perfil: Adicione um nome para o perfil de mídia.

Video source (Origem do vídeo): Selecione a fonte de vídeo para sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista. As configurações na lista suspensa correspondem aos canais de vídeo do dispositivo, incluindo multivisualizações, áreas de visualização e canais virtuais.

Video encoder (Codificador de vídeo): Selecione o formato de codificação de vídeo para sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário na lista e ajuste as configurações de codificação. As configurações na lista suspensa atuam como identificadores/nomes da configuração do codificador de vídeo. Selecione o usuário de 0 a 15 para aplicar suas próprias configurações ou selecione um dos usuários padrão se desejar usar configurações predefinidas para um formato de codificação específico.

Observação

Ative o áudio no dispositivo para obter a opção de selecionar uma fonte de áudio e uma configuração do codificador de áudio.

Fonte de áudio : Selecione a fonte de entrada de áudio para a sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações de áudio. As configuraçãos na lista suspensa correspondem às entradas de áudio do dispositivo. Se o dispositivo tiver uma entrada de áudio, é user0. Se o dispositivo tiver várias entradas de áudio, haverá usuários adicionais na lista.

Codificador de áudio : Selecione o formato de codificação de áudio para a sua configuração.

- **Selecione a configuração**: Seleciione uma configuração definida pelo usuário da lista e ajuste as configurações de codificação de áudio. As configurações na lista suspensa agem como identificadores/ /nomes da configuração do codificador de áudio.

Audio decoder (Decodificador de áudio) : Selecione o formato de decodificação de áudio para a sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações. As configurações na lista suspensa agem como identificadores/nomes da configuração.

Saída de áudio : Selecione o formato da saída de áudio para a sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações. As configurações na lista suspensa agem como identificadores/nomes da configuração.

Metadados: Selecione os metadados para incluir na sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações de metadados. As configuraçãos na lista suspensa agem como identificadores/nomes da configuração de metadados.

PTZ : Selecione as configurações PTZ para a sua configuração.

- **Selecione a configuração**: Selecione uma configuração definida pelo usuário da lista e ajuste as configurações PTZ. As configurações na lista suspensa correspondem aos canais de vídeo do dispositivo com suporte PTZ.

Create (Criar): Clique para salvar suas configurações e criar o perfil.

Cancelar: Clique para cancelar a configuração e limpar todas as configurações.

profile_x: Clique no nome do perfil para abrir e editar o perfil pré-configurado.

Detectores

Detecção de impactos

Shock detector (Detector de impactos): ative para gerar um alarme se o dispositivo for atingido por um objeto ou se for manipulado.

Sensitivity level (Nível de sensibilidade): mova o controle deslizante para ajustar o nível de sensibilidade com o qual o dispositivo deve gerar um alarme. Um valor baixo significa que o dispositivo só gera um alarme se o choque for poderoso. Um valor elevado significa que o dispositivo gerará alarme até mesmo em casos de manipulação leve.

Acessórios

Portas de E/S

Use a entrada digital para conectar dispositivos externos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas ou janelas e detectores de quebra de vidros.

Use a saída digital para conectar dispositivos externos, como relés e LEDs. Você pode ativar dispositivos conectados via interface de programação de aplicativos VAPIX® ou na interface Web.

Detecção automática

Nome: Edite o texto para renomear a porta.

Direção: indica que a porta é uma porta de entrada. indica que é uma porta de saída. Se a porta for configurável, você poderá clicar nos ícones para alternar entre entrada e saída.

Normal state (Estado normal): Clique em para circuito aberto e para circuito fechado.

Current state (Estado atual): Mostra o estado atual da porta. A entrada ou saída é ativada quando o estado atual é diferente do estado normal. Uma entrada no dispositivo tem um circuito aberto quando desconectada ou quando há uma tensão acima de 1 VCC.

Observação

Durante a reinicialização, o circuito de saída é aberto. Quando a reinicialização é concluída, o circuito retorna para a posição normal. Se você alterar qualquer configuração nesta página, os circuitos de saída voltarão para suas posições normais, independentemente de quaisquer acionadores ativos.

Supervisionado : Ative para possibilitar a detecção e o acionamento de ações se alguém manipular a conexão com dispositivos de E/S digitais. Além de detectar se uma entrada está aberta ou fechada, você também pode detectar se alguém a manipulou (ou seja, cortada ou em curto). Supervisionar a conexão requer hardware adicional (resistores de fim de linha) no loop de E/S externo.

Edge-to-edge

Pareamento

O emparelhamento permite usar um dispositivo Axis compatível como se ele fizesse parte do dispositivo principal.

Audio pairing (Emparelhamento de áudio) permite emparelhar com o alto-falante ou microfone da rede. Uma vez pareado, o alto-falante de rede age como um dispositivo de saída de áudio no qual você pode reproduzir

clipes de áudio e transmitir som por meio da câmera. O microfone de rede captará sons da área ao redor e o disponibilizará como um dispositivo de entrada de áudio que pode ser usado em streams de mídia e gravações.

Importante

Para que esse recurso funcione com um software de gerenciamento de vídeo (VMS), você deve primeiro parear a câmera com o alto-falante ou microfone e, em seguida, adicionar a câmera ao seu VMS.

Defina um limiar para "Aguardar entre ações (hh:mm:ss)" na regra do evento quando um dispositivo de áudio pareado em rede é usado na regra de evento com "Detecção de áudio" como condição e "Reproduzir clipes de áudio" como ação. Isso ajudará você a evitar uma detecção de loop se o microfone que captura captar áudio do alto-falante.

Adicionar: Adicione um dispositivo com o qual emparelhar.

Discover devices (Descobrir dispositivos): Clique para localizar dispositivos na rede. Após a rede ser verificada, será exibida uma lista de dispositivos disponíveis.

Observação

A lista mostrará todos os dispositivos Axis encontrados, não apenas os dispositivos que podem ser emparelhados.

Somente dispositivos com o **Bonjour** ativado podem ser encontrados. Para ativar o **Bonjour** em um dispositivo, abra a interface Web do dispositivo e acesse **System > Network > Network discovery protocols (Sistema > Rede > Protocolos de descoberta de rede)**.

Observação

Um ícone de informações será mostrado em dispositivos que já foram emparelhados. Passe o mouse sobre o ícone para obter informações sobre os emparelhamentos que já estão ativos.

Para emparelhar um dispositivo da lista, clique em .

Select pairing type (Selecionar tipo de emparelhamento): Selecione na lista suspensa.

Speaker pairing (Pareamento de alto-falante): Selecione para parear um alto-falante de rede.

Pareamento de microfone : Selecione para parear um microfone.

Endereço: Insira o nome de host ou endereço IP para o alto-falante de rede.

Username (Nome de usuário): Insira o nome de usuário.

Senha: Insira a senha do usuário.

Close (Fechar): Clique para limpar todos os campos.

Connect (Conectar): clique para estabelecer conexão com o dispositivo com o qual deseja emparelhar.

O pareamento com PTZ permite emparelhar um radar com uma câmera PTZ para usar rastreamento automático. O rastreamento automático PTZ com radar faz com que a câmera PTZ rastreie objetos com base em informações do radar sobre as posições dos objetos.

Adicionar: Adicione um dispositivo com o qual emparelhar.

Discover devices (Descobrir dispositivos): Clique para localizar dispositivos na rede. Após a rede ser verificada, será exibida uma lista de dispositivos disponíveis.

Observação

A lista mostrará todos os dispositivos Axis encontrados, não apenas os dispositivos que podem ser emparelhados.

Somente dispositivos com o **Bonjour** ativado podem ser encontrados. Para ativar o **Bonjour** em um dispositivo, abra a interface Web do dispositivo e acesse **System > Network > Network discovery protocols (Sistema > Rede > Protocolos de descoberta de rede)**.

Observação

Um ícone de informações será mostrado em dispositivos que já foram emparelhados. Passe o mouse sobre o ícone para obter informações sobre os emparelhamentos que já estão ativos.

Para emparelhar um dispositivo da lista, clique em .

Select pairing type (Selecionar tipo de emparelhamento): Selecione na lista suspensa.

Endereço: Insira o nome do host ou endereço IP da câmera PTZ.

Username (Nome de usuário): Insira o nome de usuário da câmera PTZ.

Senha: Insira a senha da câmera PTZ.

Close (Fechar): Clique para limpar todos os campos.

Connect (Conectar): Clique em para estabelecer conexão à câmera PTZ.

Configurar rastreamento automático por radar: Clique em para abrir e configurar o rastreamento automático. Você também pode ir para **Radar > Radar PTZ autotracking (Radar > Rastreamento automático PTZ com radar)** para configurá-lo.

Logs

Relatórios e logs

Relatórios

- **View the device server report (Exibir o relatório do servidor de dispositivos)**: Exiba informações sobre o status do produto em uma janela pop-up. O Log de acesso é incluído automaticamente no Relatório do servidor.
- **Download the device server report (Baixar o relatório do servidor de dispositivos)**: Ele cria um arquivo .zip que contém um arquivo de texto do relatório completo do servidor no formato UTF-8, bem como um instantâneo da imagem da visualização ao vivo atual. Inclua sempre o arquivo. zip do relatório do servidor ao entrar em contato com o suporte.
- **Download the crash report (Baixar o relatório de falhas inesperadas)**: Baixe um arquivo com informações detalhadas sobre o status do servidor. O relatório de panes contém informações que fazem parte do relatório do servidor, além de informações de depuração detalhadas. Esse relatório pode conter informações sensíveis, como rastreamentos de rede. A geração do relatório poderá demorar vários minutos.

Logs

- **View the system log (Exibir o log do sistema)**: Clique para mostrar informações sobre eventos do sistema, como inicialização de dispositivos, avisos e mensagens críticas.
- **View the access log (Exibir o log de acesso)**: clique para mostrar todas as tentativas de acessar o dispositivo que falharam, por exemplo, quando uma senha de login incorreta é usada.

Acesse o sistema remotamente

O syslog é um padrão para o registro de mensagens. Ele permite a separação do software que gera mensagens, o sistema que as armazena e o software que as relata e analisa. Cada mensagem é rotulada com um código da instalação que indica o tipo de software que gerou a mensagem e recebe um nível de gravidade.

Servidor: Clique para adicionar um novo servidor.

Host: Insira o nome de host ou endereço IP do servidor.

Format (Formatar): Selecione o formato de mensagem do syslog que será usado.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocolo): Selecione o protocolo que a ser usado:

- UDP (a porta padrão é 514)
- TCP (a porta padrão é 601)
- TLS (a porta padrão é 6514)

Porta: Edite o número da porta para usar uma porta diferente.

Severity (Severidade): Selecione quais mensagens serão enviadas após o acionamento.

Tipo: Selecione o tipo de registros que deseja enviar.

Test server setup (Testar configuração do servidor): Envie uma mensagem de teste para todos os servidores antes de salvar as configurações.

CA certificate set (Certificado CA definido): Consulte as configurações atuais ou adicione um certificado.

Configuração simples

A configuração simples destina-se a usuários avançados com experiência em configuração de dispositivos Axis. A maioria dos parâmetros podem ser definidos e editados nesta página.

Manutenção

Manutenção

Restart (Reiniciar): Reinicie o dispositivo. Isso não afeta nenhuma das configurações atuais. Os aplicativos em execução reiniciam automaticamente.

Restore (Restaurar): Devolve a maioria das configurações para os valores padrão de fábrica. Posteriormente, você deverá reconfigurar o dispositivo e os aplicativos, reinstalar quaisquer apps que não vieram pré-instalados e recriar quaisquer eventos e predefinições.

Importante

As únicas configurações que permanecem salvas após a restauração são:

- Protocolo de inicialização (DHCP ou estático)
- Endereço IP estático
- Roteador padrão
- Máscara de sub-rede
- Configurações 802.1X
- Configurações de O3C
- Endereço IP do servidor DNS

Factory default (Padrão de fábrica): Retorna todas as configurações para os valores padrão de fábrica. Em seguida, você deverá redefinir o endereço IP para tornar o dispositivo acessível.

Observação

Todo software de dispositivo Axis é digitalmente assinado para garantir que somente software verificado seja instalado em seu dispositivo. Esse procedimento aprimora ainda mais o nível de segurança cibernética mínimo dos dispositivos Axis. Para obter mais informações, consulte o white paper "Axis Edge Vault" em *axis.com*.

Atualização do AXIS OS: atualize para uma nova versão do AXIS OS. As novas versões podem conter funcionalidades aprimoradas, correções de falhas ou ainda recursos inteiramente novos. Recomendamos sempre utilizar a versão mais recente do AXIS OS. Para baixar a versão mais recente, vá para *axis.com/support*.

Ao atualizar, é possível escolher entre três opções:

- **Standard upgrade (Atualização padrão)**: atualize para a nova versão do AXIS OS.
- **Factory default (Padrão de fábrica)**: Atualize e retorne todas as configurações para os valores padrão de fábrica. Ao escolher essa opção, você não poderá reverter para a versão anterior do AXIS OS após a atualização.
- **Autorollback (Reversão automática)**: Atualize e confirme a atualização dentro do período definido. Se você não confirmar, o dispositivo reverterá para a versão anterior do AXIS OS.

AXIS OS rollback (Reversão do AXIS OS): reverta para a versão anteriormente instalada do AXIS OS.

solução de problemas

Reset PTR (Redefinir PTR) : redefina o PTR se, por algum motivo, as configurações de **Pan (Panorama)**, **Tilt (Inclinação)** ou **Roll (Rolagem)** não funcionarem como esperado. Os motores de PTR são sempre calibrados em uma nova câmera. No entanto, a calibração poderá ser perdida, por exemplo, se a câmera perder energia ou se os motores forem movidos à mão. Quando você redefine o PTR, a câmera é recalibrada e retorna à sua posição padrão de fábrica.

Calibração : clique em **Calibrate (Calibrar)** para recalibrar os motores pan, tilt e roll às suas posições padrão.

Ping: Para verificar se o dispositivo pode acessar um endereço específico, digite o nome de host ou o endereço IP do host no qual deseja executar o ping e clique em **Iniciar**.

Verificação de porta: Para verificar a conectividade do dispositivo com um endereço IP e uma porta TCP/UDP específicos, digite o nome do host ou o endereço IP e o número da porta que deseja verificar e clique em **Iniciar**.

Rastreamento de rede

Importante

Um arquivo de rastreamento de rede pode conter informações confidenciais, como certificados ou senhas.

Um arquivo de trace de rede pode ajudar a solucionar problemas gravando as atividades na rede.

Trace time (Tempo de trace): Selecione a duração do trace em segundos ou minutos e clique em **Download (Baixar)**.

Validar sua instalação

Validar a instalação do radar

Observação

Este teste ajuda você a validar sua instalação sob as condições correntes. O desempenho diário da sua instalação pode ser afetado por alterações na cena.

O radar está pronto para ser usado assim que é instalado. No entanto, recomendamos realizar uma validação antes de começar a usá-lo. Isso pode aumentar a precisão do radar ajudando você a identificar quaisquer problemas com a instalação ou o gerenciamento de objetos (como árvores e superfícies reflexivas) na cena.

Primeiro, antes de tentar a validação.

É uma boa ideia executar a validação sempre que:

- Houver objetos na cena que você deseja excluir para que as zonas possam conter certos objetos, como vegetação ou superfícies metálicas.
- Você parear o radar com uma câmera PTZ e deseja configurar o **Radar autotracking (Rastreamento automático por radar)**.
- A altura de montagem do radar for alterada.

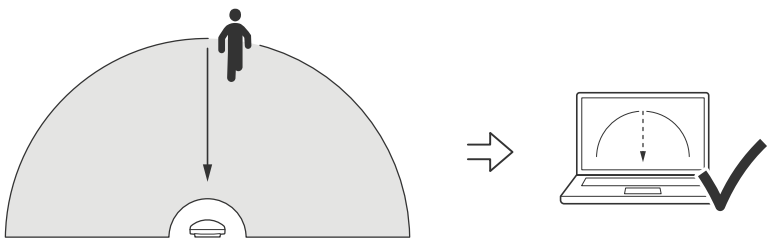
Validar o radar

Verifique se não há detecções falsas

1. Verifique se a zona de detecção está livre de atividade humana.
2. Aguarde alguns minutos para garantir que o radar não esteja detectando objetos estáticos nas zonas de detecção.
3. Se não houver detecções indesejadas, você poderá ignorar a etapa 4.
4. Se houver detecções indesejadas, aprenda a filtrar certos tipos de movimento ou objetos, alterar a cobertura ou ajustar a sensibilidade da detecção em .

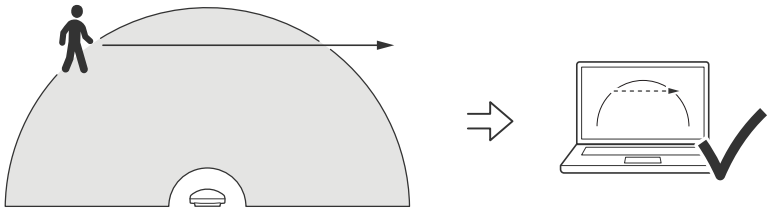
Verificar o símbolo correto e a direção de deslocamento quando o radar é abordado pela frente

1. Acesse a interface da Web do radar e grave a sessão. Para obter ajuda para fazer isso, acesse .
2. Comece a 60 m (197 pés) na frente do radar e caminhe na direção do radar.
3. Verifique a sessão na interface da Web do radar. O símbolo de uma classificação humana deve ser exibido quando você é detectado.
4. Verifique se a interface da Web do radar mostra a direção correta da viagem.



Verificar o símbolo correto e a direção de deslocamento quando o radar é abordado pela frente

1. Acesse a interface da Web do radar e grave a sessão. Para obter ajuda para fazer isso, acesse .
2. Comece a 60 m (197 pés) de largura no radar e caminhe diretamente ao longo da área de cobertura do radar.
3. Verifique se a interface da Web do radar mostra o símbolo para uma classificação humana.
4. Verifique se a interface da Web do radar mostra a direção correta da viagem.



Crie uma tabela semelhante à abaixo para ajudar a gravar os dados da sua validação.

Teste	Aprovado/Reprovado	Comentários
1. Verifique se não há detecções indesejadas quando a área está livre		
2a. Verifique se o objeto é detectado com o símbolo correto para "pessoas" quando o radar é abordado pela frente		
2b. Verifique se a direção do deslocamento está correta quando o radar é abordado pela frente		
3a. Verifique se o objeto é detectado com o símbolo correto para "pessoas" quando o radar é abordado pelo lado		
3b. Verifique se a direção do deslocamento está correta quando o radar é abordado pelo lado		

Concluir a validação

Após concluir a primeira parte da validação com êxito, você deverá executar os testes a seguir para concluir o processo de validação.

1. Certifique-se de ter configurado seu radar e seguido as instruções.
2. Para validação adicional, adicione e calibre um mapa de referência.
3. Defina o cenário de radar para acionar dados quando um objeto apropriado for detectado. Por padrão, **seconds until trigger (segundos até o acionamento)** é definido como dois segundos, mas esse valor pode ser alterado na interface da Web, se necessário.
4. Defina o radar para gravar dados quando um objeto apropriado for detectado.
   Consulte para obter instruções.
5. Defina a **trail lifetime (duração da trilha)** como uma hora para que ela exceda de forma segura o tempo necessário para você se levantar, caminhar pela área de monitoramento e se sentar novamente. A **trail lifetime (duração da trilha)** manterá o rastreamento na visualização ao vivo do radar pelo tempo definido e, após a conclusão da validação, ela poderá ser desativada.
6. Percorra a borda da área de cobertura do radar e certifique-se de que a trilha no sistema coincida com o rota em que você caminhou.
7. Se não estiver satisfeito com os resultados da validação, será necessário recalibrar o mapa de referência e repetir a validação.

Saiba mais

Streaming e armazenamento

Formatos de compressão de vídeo

Decida o método de compactação a ser usado com base em seus requisitos de exibição e nas propriedades da sua rede. As opções disponíveis são:

Motion JPEG

Motion JPEG ou MJPEG é uma sequência de vídeo digital composta por uma série de imagens JPEG individuais. Essas imagens são, em seguida, exibidas e atualizadas a uma taxa suficiente para criar um stream que exibe constantemente movimento atualizado. Para que o visualizador perceba vídeo em movimento, a taxa deve ser pelo menos 16 quadros de imagem por segundo. Vídeo com movimento completo é percebido a 30 (NTSC) ou 25 (PAL) quadros por segundo.

O stream Motion JPEG usa quantidades consideráveis de largura de banda, mas fornece excelente qualidade de imagem e acesso a cada imagem contida no stream.

H.264 ou MPEG-4 Parte 10/AVC

Observação

H.264 é uma tecnologia licenciada. O produto Axis inclui uma licença de cliente de exibição H.264. A instalação de cópias não licenciadas adicionais do cliente é proibida. Para comprar licenças adicionais, entre em contato com seu revendedor Axis.

O H.264 pode, sem compromisso à qualidade da imagem, reduzir o tamanho de um arquivo de vídeo digital em mais de 80% comparado ao formato Motion JPEG e em até 50% comparado a formatos MPEG mais antigos. Isso significa que menos largura de banda de rede e espaço de armazenamento são necessários para um arquivo de vídeo. Ou, veja de outra forma, melhor qualidade de vídeo pode ser obtida para uma determinada taxa de bits.

H.265 ou MPEG-H Parte 2/HEVC

O H.265 pode, sem comprometer a qualidade da imagem, reduzir o tamanho de um arquivo de vídeo digital em mais de 25% em comparação com o H.264.

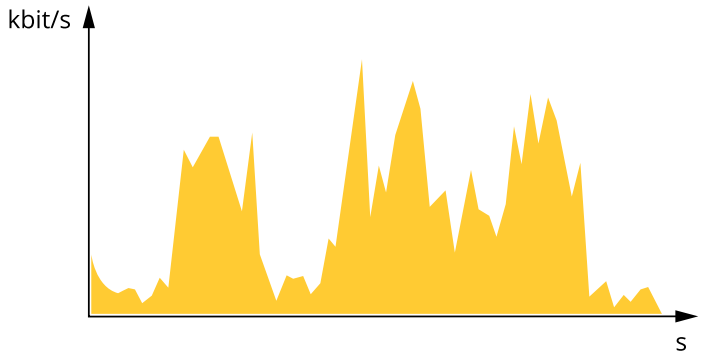
Observação

- H.265 é uma tecnologia licenciada. O produto Axis inclui uma licença de cliente de exibição H.265. A instalação de cópias não licenciadas adicionais do cliente é proibida. Para comprar licenças adicionais, entre em contato com seu revendedor Axis.
- A maioria dos navegadores da Web não oferece suporte à decodificação H.265, por isso a câmera não é compatível com ela em sua interface da Web. Em vez disso, você pode usar um aplicativo ou sistema de gerenciamento de vídeo que ofereça suporte à decodificação H.265.

Controle de taxa de bits

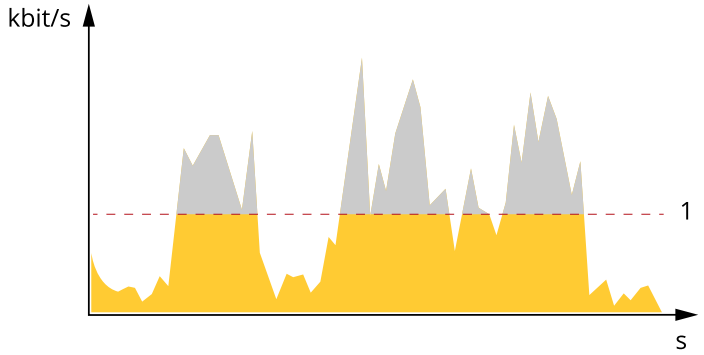
O controle de taxa de bits ajuda você a gerenciar o consumo de largura de banda do stream de vídeo.

Taxa de bits variável (VBR)
A taxa de bits variável permite que o consumo de largura de banda varie com base no nível de atividade na cena. Quanto mais atividade, mais largura de banda será necessária. Com a taxa de bits variável, você garante a qualidade da imagem constante, mas precisa verificar se há margens de armazenamento suficientes.



Taxa de bits Máxima (MBR)

A taxa de bits máxima permite definir uma taxa de bits para lidar com limitações de taxa de bits em seu sistema. Você pode perceber um declínio na qualidade da imagem ou taxa de quadros quando a taxa de bits instantânea é mantida abaixo da taxa de bits alvo especificada. Você pode optar por priorizar a qualidade da imagem ou a taxa de quadros. Recomendamos configurar a taxa de bits alvo com um valor mais alto do que a taxa de bits esperada. Isso proporciona uma margem no caso de haver um alto nível de atividade na cena.

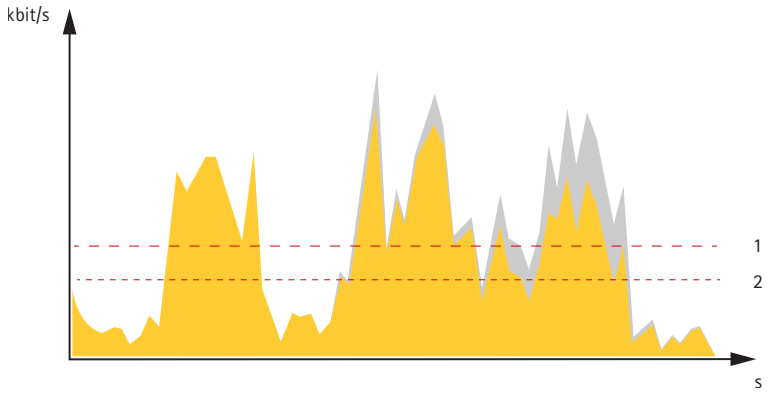


1 Taxa de bits alvo

Taxa de bits média (ABR)

Com a taxa de bits média, a taxa de bits é ajustada automaticamente por um período maior. Isso visa atingir o alvo especificado e fornecer a melhor qualidade de vídeo com base no armazenamento disponível. A taxa de bits é maior em cenas com muita atividade, comparadas a cenas estáticas. Você provavelmente obterá uma melhor qualidade de imagem em cenas com muita atividade se usar a opção de taxa de bits média. Você poderá definir o armazenamento total necessário para o stream de vídeo para um período de tempo especificado (tempo de retenção) quando a qualidade da imagem for ajustada para atender à taxa de bits alvo especificada. Especifique as configurações da taxa de bits média de uma das seguintes formas:

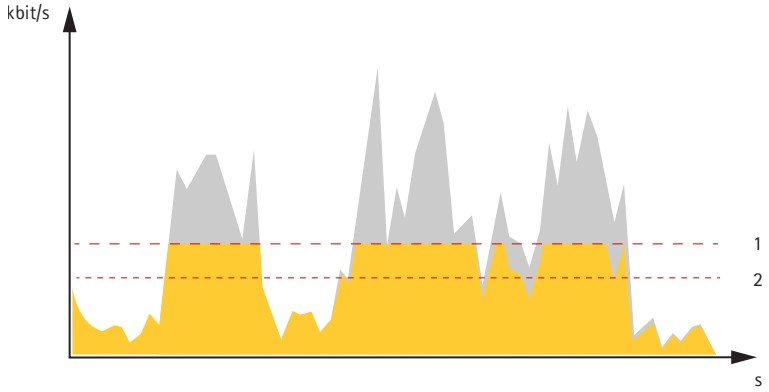
- Para calcular a necessidade de armazenamento estimada, defina a taxa de bits alvo e o tempo de retenção.
- Para calcular a taxa de bits média, com base no armazenamento disponível e no tempo de retenção necessário, use a calculadora de taxa de bits alvo.



1 Taxa de bits alvo

2 Taxa de bits média real

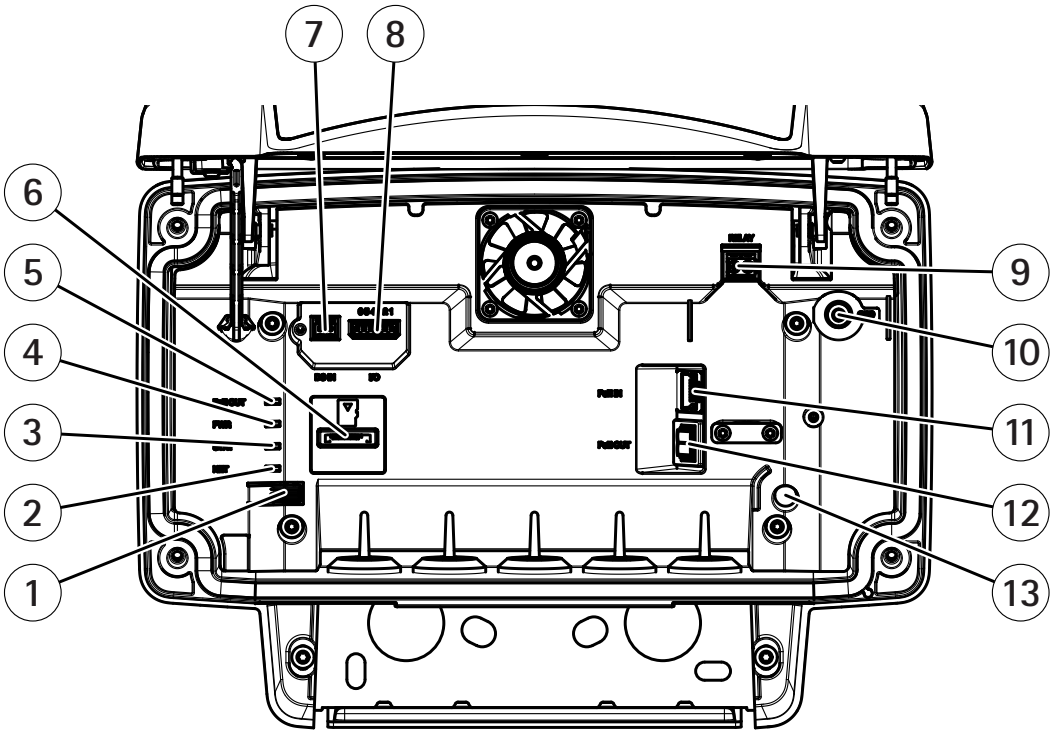
Você também pode ativar a taxa de bits máxima e especificar uma taxa de bits alvo dentro da opção de taxa de bits média.



1 Taxa de bits alvo
2 Taxa de bits média real

Especificações

Visão geral do produto



1 *Botão de controle*
2 *LED de rede*
3 *LED de estado*
4 *LED de energia*
5 *LED da saída PoE*
6 *Entrada para cartão microSD*
7 *Conector de alimentação (CC)*
8 *Conector de E/S*
9 *Conector do relé*
10 *Parafuso de aterramento*
11 *Conector de rede (PoE in)*
12 *Conector de rede (PoE out)*
13 *Sensor do alarme de invasão*

Para especificações técnicas, consulte .

Indicadores de LED

LED de estado	Indicação
Verde	Aceso em verde para operação normal.

LED de rede	Indicação
Verde	Fixo para uma conexão com uma rede de 100 Mbit/s. Pisca para atividade de rede.
Âmbar	Fixo para uma conexão com uma rede de 10 Mbit/s. Pisca para atividade de rede.
Apagado	Sem conexão de rede.

LED de energia	Indicação
Verde	Funcionamento normal.

LED da saída PoE	Indicação
Apagado	Saída PoE desativada
Verde	Saída PoE ativada

Slot de cartão SD

Esse dipositivo é compatível com cartões microSD/microSDHC/microSDXC.

Para obter recomendações sobre cartões SD, consulte *axis.com*.

Os logotipos microSD, microSDHC e microSDXC são marcas comerciais da SD-3C LLC. microSD, microSDHC e microSDXC são marcas comerciais ou registradas da SD-3C, LLC nos Estados Unidos e/ou em outros países.

Botões

Botão de controle

Para obter a localização do botão de controle, consulte .
O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte .
- Conectar a um serviço do AXIS Video Hosting System. Consulte . Para conectar, mantenha o botão pressionado por aproximadamente 3 segundos até o LED de status piscar em verde.

Conectores

Conector de rede

Conector Ethernet RJ45 com Power over Ethernet Plus (PoE+).

⚠ CUIDADO

Risco de danos ao dispositivo. Não ligue o dispositivo usando PoE e CC ao mesmo tempo.

Conector de rede (PoE out)

Power over Ethernet IEEE 802.3at Tipo 2, máx. 30 W

Use esse conector para fornecer energia para outro dispositivo PoE, por exemplo, uma câmera, um alto-falante ou um segundo radar Axis.

Observação

A saída PoE é ativada quando o radar é alimentado por um midspan de 60 W (Power over Ethernet IEEE 802.3 BT, Tipo 3).

Observação

Se o radar é alimentado por um midspan de 30 W ou alimentação CC, a saída PoE é desativada.

Observação

O comprimento máximo do cabo Ethernet é de 100 m no total para a saída PoE e a entrada PoE combinadas. Se desejar, use extensor de PoE para aumentá-lo.

Observação

Se o dispositivo PoE conectado precisar de mais de 30 W, você poderá adicionar um midspan de 60 W entre a porta de saída de PoE no radar e o dispositivo. O midspan alimentará o dispositivo, enquanto que o radar de segurança fornecerá a conexão Ethernet.

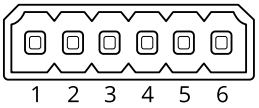
Conector de E/S

Use o conector de E/S com dispositivos externos em combinação com, por exemplo, acionadores de eventos e notificações de alarmes. Além do ponto de referência de 0 V CC e da alimentação (saída CC), o conector do terminal de E/S fornece a interface para:

Entrada digital – Para conectar dispositivos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas/janelas e detectores de quebra de vidros.

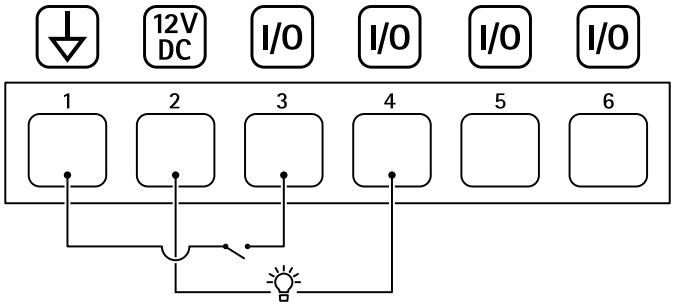
Saída digital – Para conectar dispositivos externos, como relés e LEDs. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativos VAPIX®, por meio de um evento ou via interface web do dispositivo.

Bloco de terminais com 6 pinos



Função	Pino	Observações	Especificações
Terra CC	1		0 V CC
Saída CC	2	⚠ Pode ser usada para alimentar equipamentos auxiliares. Observação: esse pino pode ser usado somente como saída de energia.	12 V CC Carga máxima = 50 mA
Configurável (entrada ou saída)	3–6	Entrada digital – Conecte ao pino 1 para ativar ou deixe aberta (desconectada) para desativar.	0 a 30 V CC máx.
		Saída digital – Conectado internamente ao pino 1 (terra CC) quando ativo, flutuante (desconectado) quando inativo. Se usada com uma carga indutiva (por exemplo, um relé), conecte um diodo em paralelo à carga para proporcionar proteção contra transientes de tensão.	0 a 30 V CC máx., dreno aberto, 100 mA

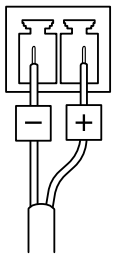
Exemplo:



1 *Terra CC*
2 *Saída CC 12 V, máx. 50 mA*
3 *E/S configurada como entrada*
4 *E/S configurada como saída*
5 *E/S configurável*
6 *E/S configurável*

Conector de energia

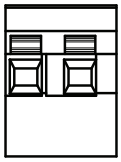
Bloco de terminais com 2 pinos para entrada de energia CC Use uma fonte de energia com limitação compatível com os requisitos de voltagem de segurança extra baixa (SELV) e com potência de saída nominal restrita a ≤100 W ou corrente de saída nominal limitada a ≤ 5 A.



⚠ CUIDADO

Risco de danos ao dispositivo. Não ligue o dispositivo usando PoE e CC ao mesmo tempo.

Conector do relé



⚠ CUIDADO

Use fios rígidos para o conector do relé.

Função	Especificações
Tipo	Normalmente aberto
Tensão nominal	24 VCC/5 A
Isolamento de outros circuitos	2,5 kV

Limpeza do dispositivo

Você pode limpar o dispositivo com água morna e sabão neutro e não abrasivo.

OBSERVAÇÃO

- Produtos químicos abrasivos podem danificar o dispositivo. Não use produtos químicos como limpa-vidros ou acetona para limpar o dispositivo.
- Não borrife detergente diretamente no dispositivo. Borrife o detergente em um pano macio e use-o para limpar o dispositivo.
- Evite limpar o dispositivo sob luz solar direta ou em temperaturas elevadas, visto que isso pode causar manchas.

1. Use ar comprimido para remover qualquer poeira e sujeira solta do dispositivo.
2. Se necessário, limpe o dispositivo com um pano de microfibra macio umedecido com água morna e sabão neutro não abrasivo.
3. Para evitar manchas, seque o dispositivo com um pano limpo e macio.

Solução de problemas

Redefinição para as configurações padrão de fábrica

Importante

A restauração das configurações padrão de fábrica. deve ser feita com muito cuidado. Uma redefinição para os padrões de fábrica restaura todas as configurações, inclusive o endereço IP, para os valores padrão de fábrica.

Para redefinir o produto para as configurações padrão de fábrica:

1. Desconecte a alimentação do produto.
2. Mantenha o botão de controle pressionado enquanto reconecta a alimentação. Consulte .
3. Mantenha o botão de controle pressionado por cerca de 15 a 30 segundos até que o indicador do LED de estado pisque com a cor âmbar.
4. Solte o botão de controle. O processo estará concluído quando o indicador do LED de estado ficar verde. Se nenhum servidor DHCP estiver disponível na rede, o endereço IP do dispositivo terá como padrão um dos seguintes:
   - **Dispositivos com AXIS OS 12.0 e posterior:** Obtido da sub-rede de endereços locais de link (169.254.0.0/16)
   - **Dispositivos com AXIS OS 11.11 e anterior:** 192.168.0.90/24
5. Use as ferramentas de software de instalação e gerenciamento para atribuir um endereço IP, definir a senha e acessar o dispositivo.
   As ferramentas de software de instalação e gerenciamento estão disponíveis nas páginas de suporte em *axis.com/support*.

Você também pode redefinir os parâmetros para as configurações padrão de fábrica na interface Web do dispositivo. Vá para **Maintenance (Manutenção)** > **Factory default (Padrão de fábrica)** e clique em **Default (Padrão)**.

Verificar a versão atual do AXIS OS

O AXIS OS determina a funcionalidade de nossos dispositivos. Durante o processo de solução de um problema, recomendamos que você comece conferindo a versão atual do AXIS OS. A versão mais recente pode conter uma correção que soluciona seu problema específico.

Para verificar a versão atual do AXIS OS:

1. Vá para a interface Web do dispositivo > **Status**.
2. Em **Device info (Informações do dispositivo)**, consulte a versão do AXIS OS.

Atualizar o AXIS OS

Importante

- As configurações pré-configuradas e personalizadas são salvas quando você atualiza o software do dispositivo (desde que os recursos estejam disponíveis no novo AXIS OS), embora isso não seja garantido pela Axis Communications AB.
- Certifique-se de que o dispositivo permaneça conectado à fonte de alimentação ao longo de todo o processo de atualização.

Observação

Quando você atualiza o dispositivo com a versão mais recente do AXIS OS na trilha ativa, o produto recebe a última funcionalidade disponível. Sempre leia as instruções de atualização e notas de versão disponíveis com cada nova versão antes de atualizar. Para encontrar a versão do AXIS OS e as notas de versão mais recentes, vá para *axis.com/support/device-software*.

1. Baixe o arquivo do AXIS OS para seu computador, o qual está disponível gratuitamente em *axis.com/ /support/device-software*.

2. Faça login no dispositivo como um administrador.
3. Vá para **Maintenance (Manutenção) > AXIS OS upgrade (Atualização do AXIS OS)** e clique em **Upgrade (Atualizar)**.

Após a conclusão da atualização, o produto será reiniciado automaticamente.

Problemas técnicos, dicas e soluções

Se você não conseguir encontrar aqui o que está procurando, experimente a seção de solução de problemas em *axis.com/support*.

Problemas ao atualizar o AXIS OS	
Falha na atualização do AXIS OS	Se a atualização falhar, o dispositivo recarregará a versão anterior. O motivo mais comum é que o arquivo de incorreto do AXIS OS foi carregado. Verifique se o nome do arquivo do AXIS OS corresponde ao seu dispositivo e tente novamente.
Problemas após a atualização do AXIS OS	Se você tiver problemas após a atualização, reverta para a versão instalada anteriormente na página **Maintenance (Manutenção)**.

Problemas na configuração do endereço IP	
O dispositivo está localizado em uma sub--rede diferente	Se o endereço IP destinado ao dispositivo e o endereço IP do computador usado para acessar o dispositivo estiverem localizados em sub-redes diferentes, você não poderá definir o endereço IP. Entre em contato com o administrador da rede para obter um endereço IP.
O endereço IP está sendo usado por outro dispositivo	Desconecte o dispositivo Axis da rede. Execute o comando ping (em uma janela de comando/DOS, digite `ping` e o endereço IP do dispositivo): • Se receber: `Reply from <IP address>: bytes=32; time=10...`, isso significa que o endereço IP já pode estar sendo usado por outro dispositivo na rede. Obtenha um novo endereço IP junto ao administrador da rede e reinstale o dispositivo. • Se receber: `Request timed out`, isso significa que o endereço IP está disponível para uso com o dispositivo Axis. Verifique todo o cabeamento e reinstale o dispositivo.
Possível conflito de endereço IP com outro dispositivo na mesma sub-rede	O endereço IP estático no dispositivo Axis é usado antes que o DHCP defina um endereço dinâmico. Isso significa que, se o mesmo endereço IP estático padrão também for usado por outro dispositivo, poderá haver problemas para acessar o dispositivo.

O dispositivo não pode ser acessado por um navegador	
Não é possível fazer login	Quando o HTTPS estiver ativado, certifique-se de que o protocolo correto (HTTP ou HTTPS) seja usado ao tentar fazer login. Talvez seja necessário digitar manualmente `http` ou `https` no campo de endereço do navegador. Se a senha da conta root for perdida, o dispositivo deverá ser restaurado para as configurações padrão de fábrica. Consulte .

O endereço IP foi alterado pelo DHCP	Os endereços IP obtidos de um servidor DHCP são dinâmicos e podem mudar. Se o endereço IP tiver sido alterado use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede. Identifique o dispositivo usando seu modelo ou número de série ou nome de DNS (se um nome tiver sido configurado). Se necessário, um endereço IP estático poderá ser atribuído manualmente. Para obter instruções, vá para *axis.com/support*.
Erro de certificado ao usar IEEE 802.1X	Para que a autenticação funcione corretamente, as configurações de data e hora no dispositivo Axis deverão ser sincronizadas com um servidor NTP. Vá para **System > Date and time (Sistema > Data e hora)**.

O dispositivo está acessível local, mas não externamente

Para acessar o dispositivo externamente, recomendamos que você use um dos seguintes aplicativos para Windows®:

- AXIS Camera Station Edge: grátis, ideal para sistemas pequenos com necessidades básicas de monitoramento.
- AXIS Camera Station 5: versão de avaliação grátis por 30 dias, ideal para sistemas de pequeno a médio porte.
- AXIS Camera Station Pro: versão de avaliação grátis por 90 dias, ideal para sistemas de pequeno a médio porte.

Para obter instruções e baixar o aplicativo, acesse *axis.com/vms*.

Não é possível conectar através da porta 8883 com MQTT sobre SSL.

O firewall bloqueia o tráfego usando a porta 8883, pois é considerada insegura.	Em alguns casos, o servidor/broker pode não fornecer uma porta específica para a comunicação MQTT. Ainda é possível usar MQTT em uma porta normalmente usada para tráfego HTTP/HTTPS. • Se o servidor/broker suporta WebSocket/WebSocket Secure (WS/WSS), geralmente na porta 443, use este protocolo em vez do MQTT. Verifique com o provedor do servidor/broker para saber se o WS/WSS é suportado e qual porta e caminho base devem ser usados. • Se o servidor/corretor suportar ALPN, o uso do MQTT poderá ser negociado em uma porta aberta, como a 443. Verifique com seu provedor de servidor/ /corretor se há suporte para ALPN e qual protocolo e porta ALPN usar.

Considerações sobre desempenho

Ao configurar seu sistema, é importante considerar como várias configurações e situações afetam a quantidade de largura de banda (taxa de bits) necessária.

Os seguintes fatores importantes devem ser considerados:

- A utilização pesada da rede devido à infraestrutura ruim afeta a largura de banda.

T10145149_pt

2025-06 (M31.2)

© 2020 – 2025 Axis Communications AB