AXIS Perimeter Defender

AXIS Perimeter Defender

AXIS Perimeter Defender PTZ Autotracking

Manual do Usuário

AXIS Perimeter Defender

Sumário

AXIS Perimeter Defender

AXIS Perimeter Defender

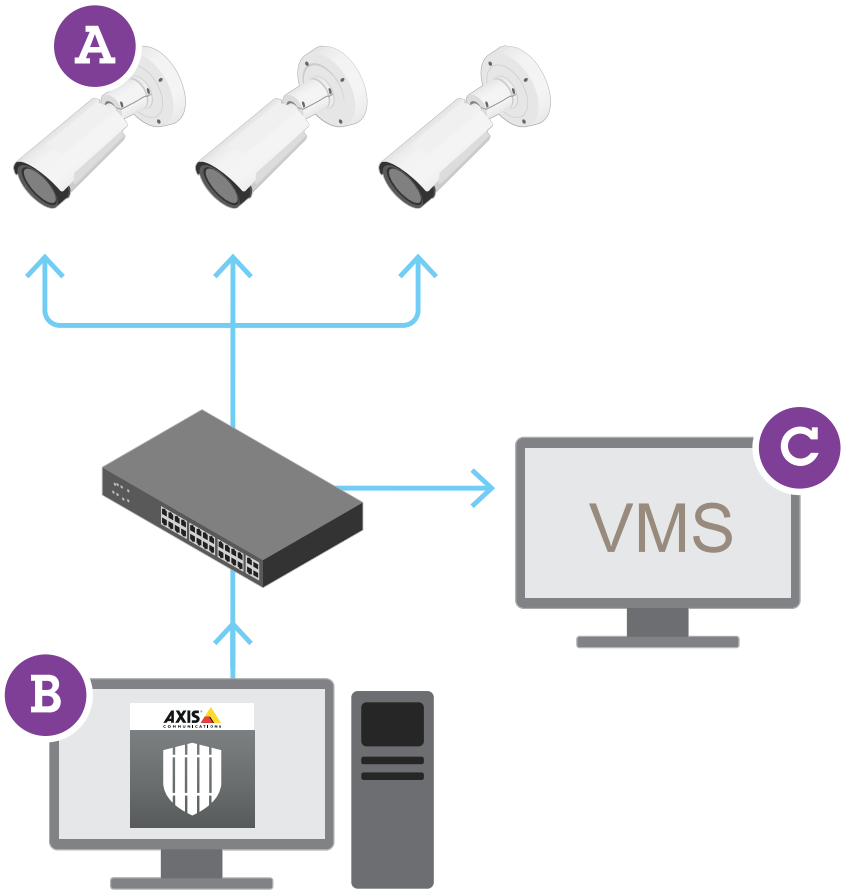
AXIS Perimeter Defender

O **AXIS Perimeter Defender** é um aplicativo para vigilância e proteção de perímetro. Ele é ideal para proteção de perímetro de alta segurança onde haja uma necessidade de reforçar o sistema de controle de acesso físico com detecção de invasão confiável.

O AXIS Perimeter Defender foi projetado principalmente para a chamada proteção de zona estéril, por exemplo, ao longo de uma cerca marcando uma divisa. O termo zona estéril refere-se a uma área onde as pessoas não deveriam estar.

Use o AXIS Perimeter Defender em uma área externa para:

- Detectar pessoas em movimento.
- Detectar veículos em movimento, sem discriminar entre tipos de veículo.



As AXIS Q1951-E e AXIS Q1952-E Thermal Cameras podem executar o aplicativo no modo de calibração, no modo AI ou em ambos os modos combinados. Se você optar por operar as câmeras somente no modo AI, a montagem das câmeras será mais flexível e você não precisará calibrá-las.

AXIS Perimeter Defender

O AXIS Perimeter Defender consiste em uma interface para desktop (B) de onde você pode instalar e configurar o aplicativo nas câmeras (A). Em seguida, você pode configurar o sistema para enviar alarmes para o Software de Gerenciamento de Vídeo (C).

O **AXIS Perimeter Defender PTZ Autotracking** é um plug-in para o aplicativo AXIS Perimeter Defender, usando a mesma interface para desktop. Com o plug-in, você emparelha uma câmera visual ou térmica fixa com uma câmera PTZ Axis Q-line. Em seguida, você pode manter a cobertura de detecção contínua de uma cena com a câmera fixa enquanto a câmera PTZ rastreia automaticamente e fornece uma visão aproximada dos objetos detectados.

Importante

O AXIS Perimeter Defender PTZ Autotracking requer a calibração de câmeras fixas e PTZs.

O AXIS Perimeter Defender oferece os seguintes tipos de cenários de detecção:

- **Invasão**: aciona um alarme quando uma pessoa ou um veículo entra em uma zona definida no solo (de qualquer direção e com qualquer trajetória).
- **Vadiagem**: aciona um alarme quando uma pessoa ou um veículo permanece em uma zona definida no solo por mais de um número predefinido de segundos.
- **Cruzamento de zonas**: aciona um alarme quando uma pessoa ou um veículo passa por duas ou mais zonas definidas no solo em uma determinada sequência.
- **Condicional**: aciona um alarme quando uma pessoa ou um veículo entra numa zona definida no solo sem primeiro passar por outra zona ou zonas definidas no solo.

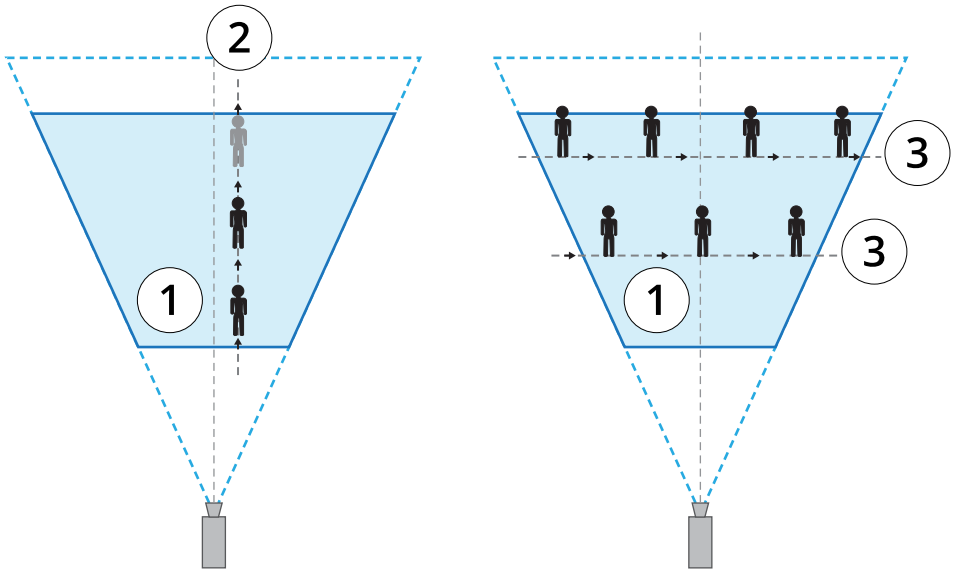
Como isso funciona?

Detecção de objetos

O AXIS Perimeter Defender pode detectar pessoas ou veículos em movimento. Para ser detectado(a):

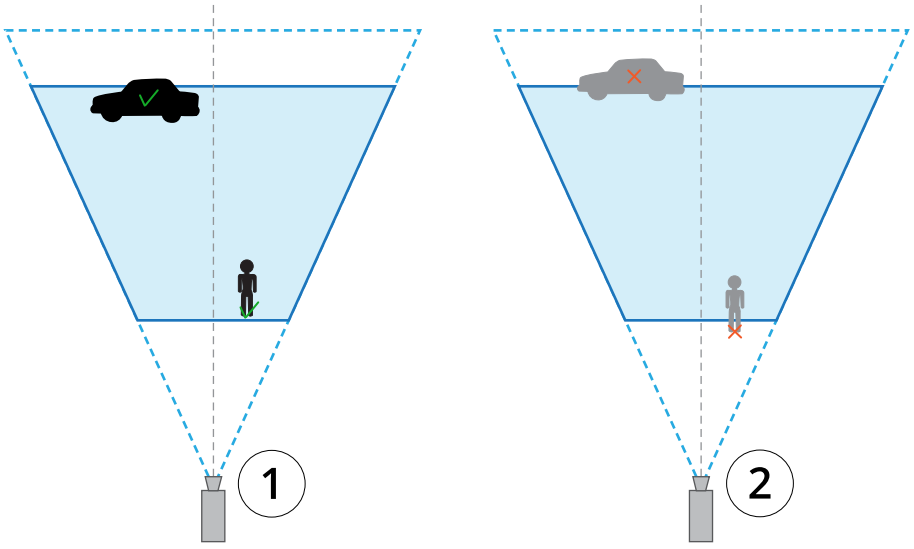
- uma pessoa ou veículo deve estar inteiramente visível na zona de detecção durante pelo menos três segundos.
- um veículo pode ter até 12 metros (39,4 pés) de comprimento. (Com o modo AI, não há comprimento máximo).
- pessoas ou veículos devem estar visivelmente em movimento do ponto de vista da câmera. Isso significa que a taxa de detecção de uma pessoa que se aproxima ou se afasta da câmera em uma linha reta é menor do que para uma pessoa que caminha perpendicularmente ao campo de visão da câmera.

AXIS Perimeter Defender



1 *Zona de detecção*
2 *Uma pessoa se afasta da câmara*
3 *As pessoas andam perpendiculares ao campo de visão da câmera*

- o ponto de detecção deve estar dentro da zona de detecção. O ponto de detecção de uma pessoa está em seus pés, e o de um veículo está em seu centro.



1 *Ponto de detecção dentro da zona de detecção*
2 *Ponto de detecção fora da zona de detecção*

Uma vez detectado, o AXIS Perimeter Defender continuará a rastrear a pessoa ou o veículo, mesmo que esteja parcialmente oculto, por exemplo, quando o corpo de uma pessoa estiver escondido atrás de um carro e apenas a cabeça da pessoa estiver visível.

Se uma pessoa ou veículo detectado parar de se mover por alguns segundos, o AXIS Perimeter Defender interromperá o seu rastreamento. Se eles começarem a se mover novamente após menos de 15 segundos, o aplicativo continuará a rastreá-los. Se a pessoa estiver em uma área de cruzamento de zona, não haverá nenhuma garantia de que o cenário será acionado corretamente.

AXIS Perimeter Defender

Como funciona o PTZ Autotracking?

No AXIS Perimeter Defender PTZ Autotracking, uma câmera fixa e uma câmera PTZ trabalham juntas. Quando a câmera fixa detecta pessoas ou veículos em movimento, ela envia os dados de localização dos objetos para a câmera PTZ emparelhada. Isso torna possível que a câmera PTZ automaticamente:

- siga os objetos, e
- ajuste o nível de zoom para manter todos os objetos em vista

desde que os objetos estejam dentro do campo de visão da câmera fixa.

Condições em que as detecções podem ser atrasadas ou perdidas

- Nevoeiro
- Luz direta que brilha na câmera
- Luz inadequada
- Imagem excessivamente barulhenta

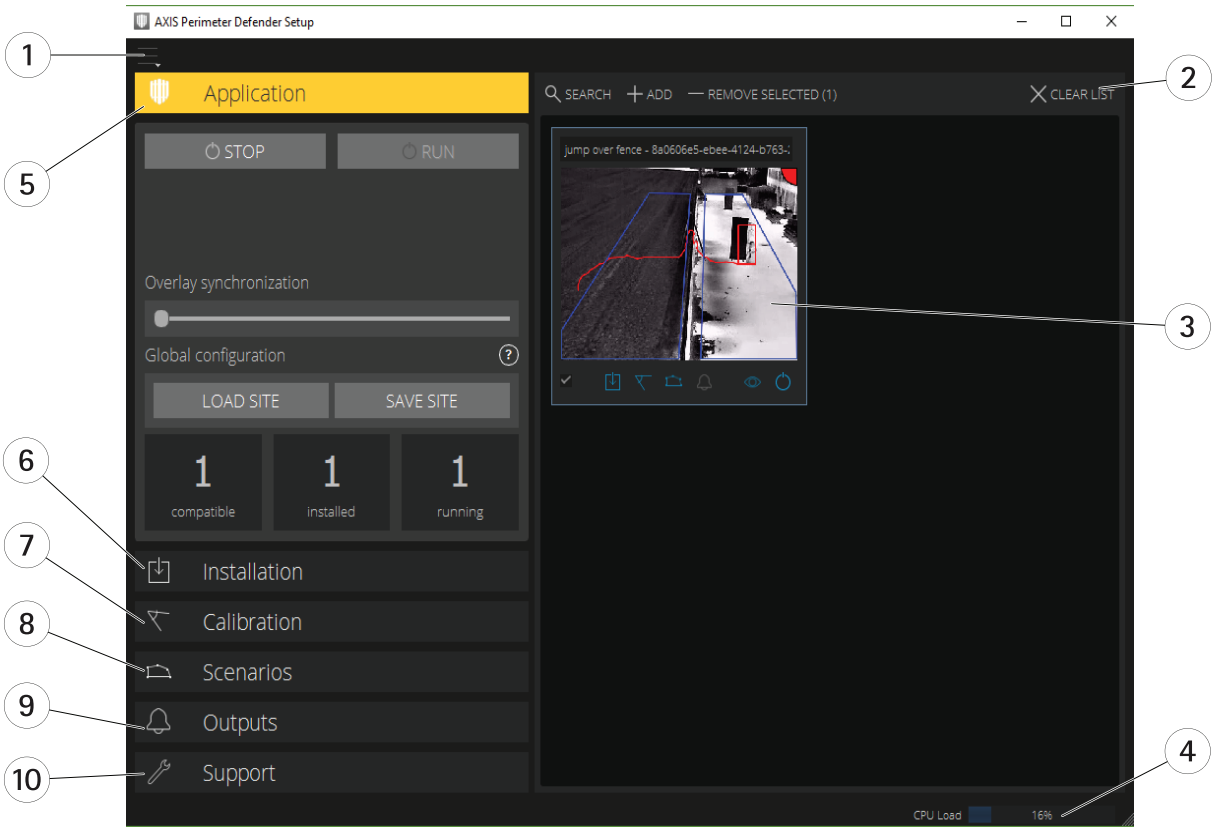
Situações que podem acionar alarmes falsos

- Pessoas ou veículos parcialmente escondidos. Por exemplo, uma pequena van exibida atrás de uma parede pode parecer uma pessoa, pois a parte visível é alta e estreita.
- Insetos na lente da câmera. Observe que as câmeras diurnas e noturnas com manchas infravermelhas atraem insetos e aranhas.
- Uma combinação de faróis de carro e chuva pesada.
- Animais de tamanho humano, especialmente se os tipos de aproximação adicionais, agachamento/rastejo ou rolagem de troncos, forem selecionados na guia **Cenários**.
- Luz forte causando sombras.

A interface do usuário

A interface do AXIS Perimeter Defender permite que você, por exemplo, calibre dispositivos, configure cenários e execute ações para vários dispositivos. A configuração remota permite a configuração de qualquer lugar onde há uma conexão de rede.

AXIS Perimeter Defender



1 *Configurações da interface na página 7*
2 *Manuseie dispositivos. Consulte Adicionar dispositivos na página 17.*
3 *Visualização ao vivo na página 8*
4 *Indicador de carga da CPU. Consulte Carga da CPU na página 12.*
5 *Guia Aplicativo na página 9*
6 *Guia Instalação na página 10*
7 *Guia Calibração na página 10*
8 *Guia Cenários na página 10*
9 *Guia Saída na página 11*
10 *Guia Suporte na página 11*

Configurações da interface

O menu de configurações da interface contém:

Configurações de pasta –
Caminho de configuração do dispositivo: Selecione onde armazenar arquivos temporários e vídeo de calibração.
Caminho de configuração do site: Selecione onde armazenar arquivos de configuração de caminhos de carregamento.

Senhas da câmera – Verifique as senhas usadas e adicione a nova senha. As senhas não são armazenadas quando o usuário sai do aplicativo.

Gerenciar pacotes de clipes de demonstração – Importe ou remova clipes de demonstração.

Ativar o modo de taxa de quadros máxima – Altere a taxa de quadros na visualização ao vivo. Consulte *Carga da CPU na página 12*.

Exibir pés e polegadas – Alterne entre unidades métricas e imperiais.

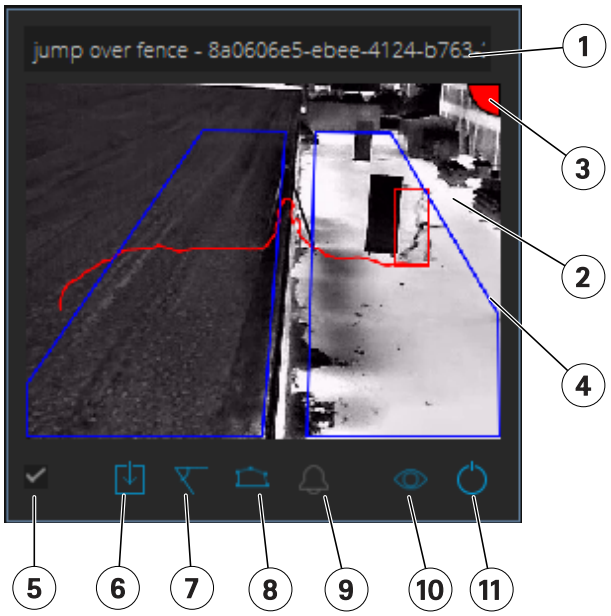
Alterar idioma – Altere o idioma no aplicativo.

AXIS Perimeter Defender

Sobre – Consulte o número de versão do AXIS Perimeter Defender Setup.

Visualização ao vivo

Cada dispositivo conectado obtém uma visualização ao vivo na interface principal. A visualização ao vivo fornece o status do dispositivo e o acesso rápido às funções principais.



1. Nome do dispositivo – Clique para editar o nome do dispositivo. Ele sempre inclui o endereço IP e o número MAC do dispositivo. Mova o mouse sobre o nome para mostrar a taxa de proporção usada para análise, que fornece a cobertura máxima do campo de visão e para ver se o dispositivo está em uma conexão remota.

2. Imagem ao vivo – No modo de visão geral, a taxa de quadros é 1 fps. Clique duas vezes para maximizar a imagem e aumentar a taxa de quadros para 8 fps.

3. Status do alarme – O status do alarme só será visível se a sobreposição estiver ativa e o AXIS Perimeter Defender estiver instalado, configurado e em execução. Cinza significa que a funcionalidade de alarme não está ativa ou que as definições de configuração estão carregando. Verde significa que a funcionalidade de alarme está ativa. Vermelho significa que um alarme foi acionado.

4. Zonas de detecção – As zonas de detecção estarão visíveis somente se a sobreposição estiver ativa e o AXIS Perimeter Defender estiver instalado, configurado e em execução.

5. Caixa de seleção – Para selecionar vários dispositivos, use esta caixa de seleção.

6. Status de instalação e botão de acesso rápido – Mova o mouse para mostrar a versão do AXIS Perimeter Defender instalada no dispositivo. Se o ícone for substituído por , isso significa que uma versão mais recente está disponível. Clique para abrir a guia Instalação para o dispositivo. Cinza significa que o dispositivo não está instalado. Laranja significa que o dispositivo está instalado, mas não tem uma licença válida. Azul significa que o dispositivo está instalado com uma licença válida.

7. Status de calibração e botão de acesso rápido – Clique para abrir a guia Calibração para o dispositivo. Cinza significa que o dispositivo não está calibrado. Azul significa que o dispositivo está calibrado.

8. Status de cenários e botão de acesso rápido – Clique para abrir a guia Cenários para o dispositivo. Cinza significa que nenhum cenário está definido. Azul significa que pelo menos um cenário está definido.

9. Status de saídas e botão de acesso rápido – Clique para abrir a guia Saída para o dispositivo. Cinza significa que nenhuma saída está configurada. Azul significa que pelo menos uma saída está configurada.

AXIS Perimeter Defender

10. Status de sobreposição e botão de alternância – Clique para ativar e desativar a sobreposição. Cinza significa que a sobreposição está inativa. Azul significa que a sobreposição está ativa. A sobreposição é mostrada como uma caixa delimitadora ao redor de objetos detectados, bem como uma "trilha de caracol" exibindo a trajetória dos objetos.

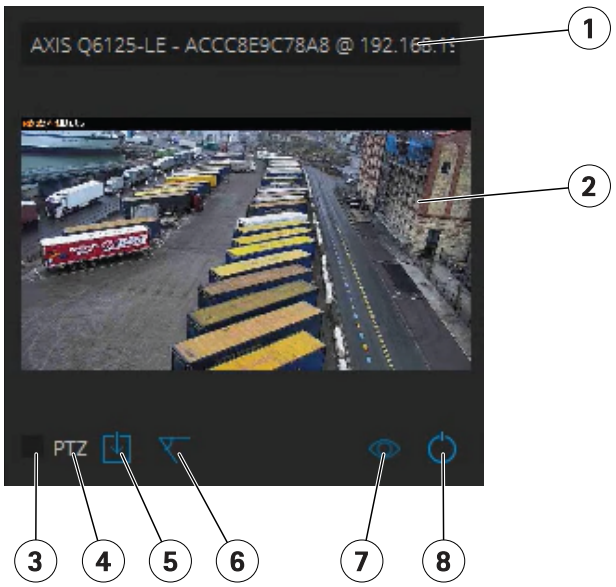
11. Status de execução e botão de alternância – Clique para executar/parar o aplicativo no dispositivo. Cinza significa que o aplicativo está parado. Azul significa que está em execução.

Observação

A sobreposição só estará disponível se uma conexão direta do dispositivo ao computador do usuário estiver disponível, ou seja, se nenhum firewall ou similar impedir a conexão com a porta de sobreposição no dispositivo.

Visualização ao vivo - PTZ Autotracking

A visualização ao vivo para dispositivos que possuem o AXIS Perimeter Defender PTZ Autotracking instalado difere ligeiramente da visualização ao vivo regular.



1 *Nome do dispositivo*
2 *Imagem ao vivo*
3 *Caixa de seleção*
4 *Indica que o dispositivo usa o AXIS Perimeter Defender PTZ Autotracking*
5 *Status de instalação e botão de acesso rápido*
6 *Status de calibração e botão de acesso rápido*
7 *Status de sobreposição e botão de alternância*
8 *Status de execução e botão de alternância*

Guia Aplicativo

- **Executar** – Inicia a análise nos dispositivos selecionados.
- **Parar** – Para a análise nos dispositivos selecionados.
- **Carregar site** – Carrega um site salvo anteriormente, ou seja, dispositivos e seus respectivos arquivos de configuração
- **Salvar site** – Salva o site atual, ou seja, salva todas as informações do dispositivo e seus respectivos arquivos de configurações

AXIS Perimeter Defender

- **Sincronização de sobreposição** - Controle sobre a sincronização de sobreposição de metadados do AXIS Perimeter Defender. Esse controle deslizante controla o atraso entre a sobreposição de metadados e as imagens recebidas para compensar o fluxo de imagem mais lento comparado aos metadados. O valor do controle deslizante indica o atraso definido para a câmera atualmente selecionada. Se houver mais de uma câmera conectada, o valor indicado será o da primeira câmera selecionada. Alterar o valor do controle deslizante muda o atraso para todas as câmeras selecionadas.

Você também pode ver o número de dispositivos compatíveis adicionados, o número total de dispositivos com o AXIS Perimeter Defender instalado e o número de dispositivos nos quais a análise está sendo executada.

Guia Instalação

- **Aplicativo: Instalar** — Instala o aplicativo nos dispositivos selecionados.
- **Aplicativo: Desinstalar** — Desinstala o aplicativo dos dispositivos selecionados.
- **Licença: Instalar** — Instala a licença nos dispositivos selecionados.

Guia Calibração

- **Automática** — Executa uma calibração automática dos dispositivos selecionados.
- **Manual** — Executa uma calibração manual dos dispositivos selecionados.

Guia Cenários

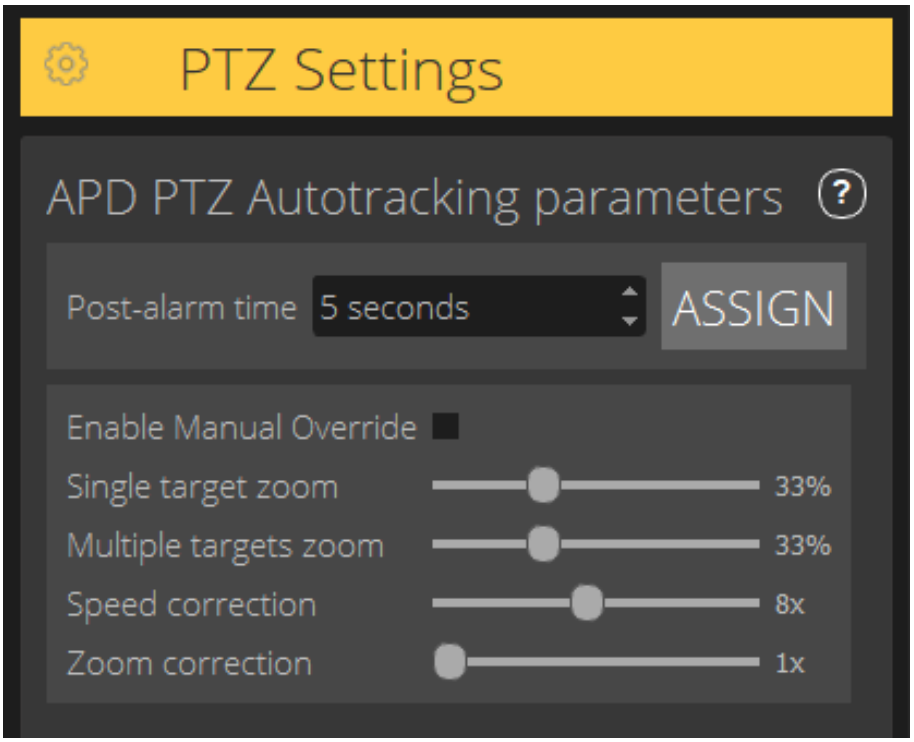
- **Parâmetros globais** — aplicam-se a todos os cenários.
- **Cenários avançados** — cria cenários de invasão, vadiagem, cruzamento de zona e condicionais.

Guia Configurações de PTZ

Observação

Esta guia só será mostrada se você tiver o plug-in AXIS Perimeter Defender PTZ Autotracking.

AXIS Perimeter Defender



- **Tempo pós-alarme** – Defina o tempo antes que a câmera PTZ retorne à sua posição inicial, após o objeto rastreado sair de vista.
- **Ativar substituição manual** – Quando selecionada, o operador poderá assumir o controle da câmera PTZ com um joystick, nas VMs ou na página da câmera.
- **Zoom de alvo único** – Ajuste o nível de zoom para rastrear um único alvo. Um valor mais alto possibilita uma melhor identificação, mas também aumenta o risco de perder objetos que se movam rapidamente.
- **Zoom de vários alvos** – Ajuste o nível de zoom para rastrear vários alvos.
- **Correção de velocidade** – Ajuste a velocidade de rastreamento para manter objetos em movimento rápido centralizados na imagem da câmera PTZ. Observe que um valor alto pode levar à instabilidade de rastreamento.
- **Correção de zoom** – Um valor mais alto aumenta o zoom para objetos que estão próximos à borda do campo de visão da câmera PTZ.

Guia Saída

- **Configurar** — Abre a página da Web do dispositivo para criar e configurar alarmes.
- **Testar alarme** — Testa o alarme configurado para o dispositivo.
- **Tempo pós-alarme: Atribuir** — Define o tempo pós-alarme.

Guia Suporte

- **Carregar** — Carrega a configuração de backup para dispositivos selecionados. Isso será especialmente útil para restaurar rapidamente após uma falha de dispositivo ou desinstalação acidental. A configuração inclui:
  - Licença
  - Parâmetros

- Calibração e cenários
- Vídeo de calibração

- **Salvar** — Cria um backup da configuração dos dispositivos selecionados.
- **Limpar** — Apaga a calibração e os cenários dos dispositivos selecionados. Isso será útil se as câmeras forem movidas, pois as zonas de calibração e detecção não serão mais válidas.
- **Exibir log do aplicativo** — Exibe o log interno do AXIS Perimeter Defender.
- **Exportar log de suporte** — Gera um arquivo de suporte que contém informações detalhadas. Sempre inclua esse arquivo com uma solicitação de suporte.

Carga da CPU

O indicador de carga da CPU representa a carga atual da CPU do computador em tempo real. Uma carga de CPU muito alta pode resultar em um computador ou aplicativo que não responde. Certifique-se de fechar outros aplicativos ao usar o AXIS Perimeter Defender Setup para maximizar sua alocação de CPU. Se a carga da CPU for muito alta e você tentar adicionar um dispositivo, o sistema emitirá um aviso.

Os dispositivos adicionados consomem recursos da CPU do computador host para decodificar streams de vídeo da câmera e exibi-los. Para limitar o impacto no computador host, os streams de vídeo de dispositivos adicionados são exibidos em uma taxa de quadros reduzida (aproximadamente 1 fps) por padrão. A taxa de quadros normal (aproximadamente8 fps) é restaurada quando os streams são maximizados ou durante o processo de calibração.

Importante

Ativar o modo de taxa de quadros máxima pode levar a uma interface que não responde se você se conectar a um grande número de câmeras ou quando você usa um computador de baixa potência.

Demonstração do AXIS Perimeter Defender

Para fins de demonstração, o AXIS Perimeter Defender e o AXIS Perimeter Defender PTZ Autotracking vêm pré-instalados com alguns clipes de demonstração que podem ser usados para demonstrar as análises sem a necessidade de uma câmera ativa instalada. Os clipes de demonstração mostram os tipos de resultado de detecção e rastreamento automático que podem ser esperados em diferentes ambientes.

1. Vá para **Aplicativo > Adicionar > Clipes de demonstração** e execute um ou mais dos seguintes procedimentos:
   - Filtre clipes de demonstração de acordo com seus tipos.
   - Selecione pelo menos um clipe de demonstração.
2. Para adicionar os clipes de demonstração, clique em **Adicionar clipes de demonstração selecionados**.

Uma vez adicionados, os clipes de demonstração serão exibidos como streams de vídeo padrão na interface. A calibração está disponível e a análise já está ativada para que o usuário veja imediatamente os resultados de análise e rastreamento automático no stream de vídeo. A análise e o rastreamento automático podem ser interrompidos ou iniciados ao clicar no status de execução na visualização ao vivo ou nos botões **Executar** ou **Parar** no painel esquerdo.

A calibração e o emparelhamento podem ser modificados e refeitos. Da mesma forma, os cenários de detecção podem ser adicionados, removidos e modificados.

A guia **Suporte** no painel esquerdo tem um botão **Limpar** que permite reverter a calibração e os cenários para os valores originais. Não é possível remover completamente a calibração.

Introdução

O processo de instalação do AXIS Perimeter Defender e AXIS Perimeter Defender PTZ Autotracking difere ligeiramente.

Como começar a usar o AXIS Perimeter Defender

Você deve percorrer as etapas a seguir para que seu site funcione com o AXIS Perimeter Defender:

1. Monte a câmera. Consulte *Montagem da câmera na página 13*.
2. Baixe e instale o software no seu computador. Consulte *Instale o software no computador na página 16*.
3. Conecte aos seus dispositivos. Consulte *Adicionar dispositivos na página 17*.
4. Instale o AXIS Perimeter Defender em cada dispositivo. Consulte *Instalar software em dispositivos na página 18*.

Observação

Não é necessário calibrar dispositivos que operam somente no modo AI. Para operar dispositivos no modo de calibração e no modo AI, é necessário calibrá-los.

5. Calibre os dispositivos. Consulte *Calibrar - AXIS Perimeter Defender na página 19*.
6. Defina as regras para o que deve acionar alarmes ao adicionar cenários. Consulte *Definir cenários na página 27*.
7. Configure os alarmes a serem enviados. Consulte *Definir saídas na página 31*.

Introdução ao AXIS Perimeter Defender PTZ Autotracking

Você deve percorrer as etapas a seguir para que seu site funcione com o AXIS Perimeter Defender PTZ Autotracking:

1. Monte as câmeras. Consulte *Montagem da câmera na página 13* e *Monte a câmera PTZ. na página 15*.
2. Baixe e instale o software no seu computador. Consulte *Instale o software no computador na página 16*.
3. Conecte aos seus dispositivos. Consulte *Adicionar dispositivos na página 17*.
4. Instale a versão do AXIS Perimeter Defender 2.5.0 ou posterior na câmera fixa e o AXIS Perimeter Defender PTZ Autotracking na câmera PTZ. Consulte *Instalar software em dispositivos na página 18*.
5. Calibre os dispositivos e configure cenários. Consulte *Calibrar - PTZ Autotracking na página 26*.
6. Emparelhe os dispositivos. Consulte *Emparelhar as câmaras - PTZ Autotracking na página 30*.
7. Configure os alarmes a serem enviados. Consulte *Definir saídas na página 31*.

Montagem da câmera

Sobre a ferramenta de design

Para especificar o posicionamento da câmera no site, recomendamos que você use a ferramenta Design para o AXIS Perimeter Defender. Ele leva em conta as câmeras Axis e os requisitos do AXIS Perimeter Defender. A ferramenta ajuda a decidir:

- Altura de montagem da câmera
- Ângulo de inclinação
- Distância mínima de detecção
- Distância máxima de detecção

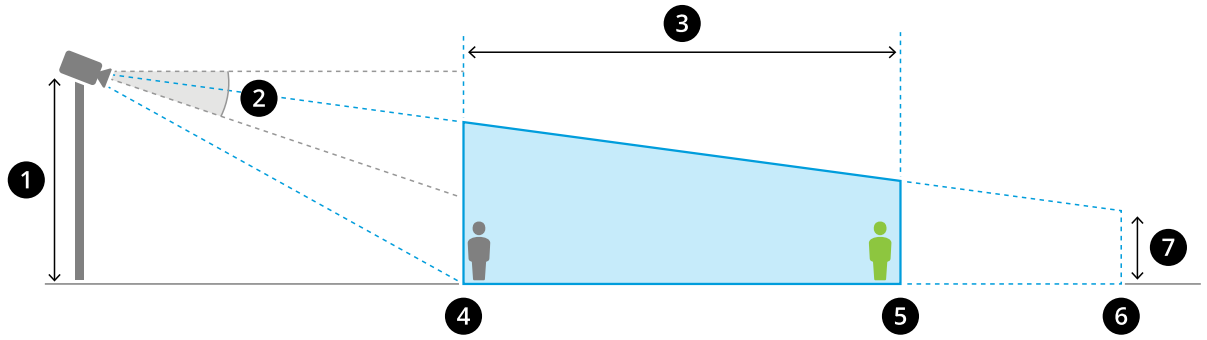
Introdução

Para baixar a ferramenta, vá para *axis.com/products/axis-perimeter-defender*

Recomendações para montagem da câmera

Observação

Somente para câmeras que operam no modo AI, recomendações de montagem podem ser encontradas no aplicativo.



Uma câmera montada corretamente.

1 *Altura de montagem*
2 *Tilt*
3 *Zona de detecção*
4 *Distância mínima de detecção*
5 *Distância máxima de detecção*
6 *Distância do campo de visão*
7 *Elevação do campo de visão*

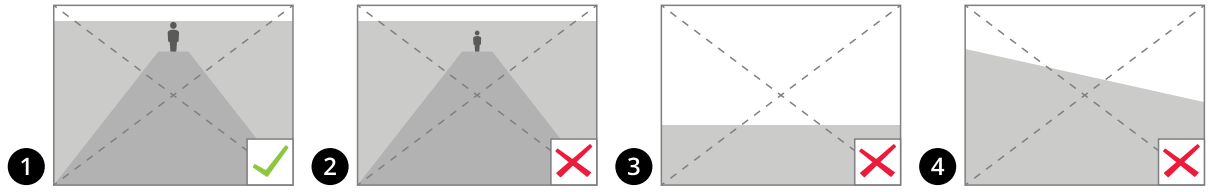
Altura do objeto na distância máxima de detecção – Para que uma pessoa em pé seja detectada na distância máxima de detecção, a altura em pixels deve ser pelo menos 5% da altura total da imagem (3,5% para câmeras térmicas). Por exemplo, se a altura da imagem visualizada for 576 pixels, a altura de uma pessoa em pé no final da zona de detecção deverá ser pelo menos 28 pixels (20 pixels na imagem térmica).

Altura do objeto na distância mínima de detecção – Para que uma pessoa em pé seja detectada na distância mínima de detecção, a altura do pixel não pode ser superior a 60% da altura total da imagem.

Altura do objeto ao operar no modo AI – Quando o aplicativo é executado no modo AI, os objetos precisam ter o tamanho igual ou maior do que o avatar para ser detectado.

Ângulo de inclinação – A câmera deve ser suficientemente orientada para o chão para que o centro da imagem fique sob a linha do horizonte. Monte a câmera para que a distância mínima de detecção seja maior do que a metade da altura de montagem da câmera (distância de detecção mínima > altura de montagem da câmera/2).

Ângulo de rolagem – O ângulo de rolagem da câmera deve ser quase igual a zero.



1 *A altura do objeto, o ângulo de inclinação e o ângulo de rolagem são adequados.*
2 *A altura do objeto na distância máxima de detecção é inferior a 5% da altura da imagem (3,5% para câmeras térmicas).*

3 *O centro da imagem está acima da linha do horizonte.*
4 *O ângulo de rolagem da câmera não é quase igual a zero.*

A distância máxima de detecção depende dos seguintes fatores:

- Tipo e modelo da câmera
- Lente da câmera. Um alcance focal maior permite uma distância mais longa de detecção.
- O tamanho mínimo do pixel que um ser humano deve cobrir na imagem a ser detectada. A altura do pixel de uma pessoa em pé deve ser pelo menos 5% da altura da imagem para câmeras visuais e 3,5% para câmeras térmicas.
- Tempo
- Iluminação
- Carga da câmera

Ao montar a câmera, considere:

- vibrações. O aplicativo tolera pequenas vibrações da câmera, mas você obtém o melhor desempenho quando a câmera não está sujeita a vibrações.
- campo de visão. O campo de visão da câmera deve ser corrigido.

Requisitos de cena

Observação

Somente para câmeras que operam no modo AI, requisitos de cena podem ser encontradas no aplicativo.

A zona de detecção deve fornecer as seguintes condições:

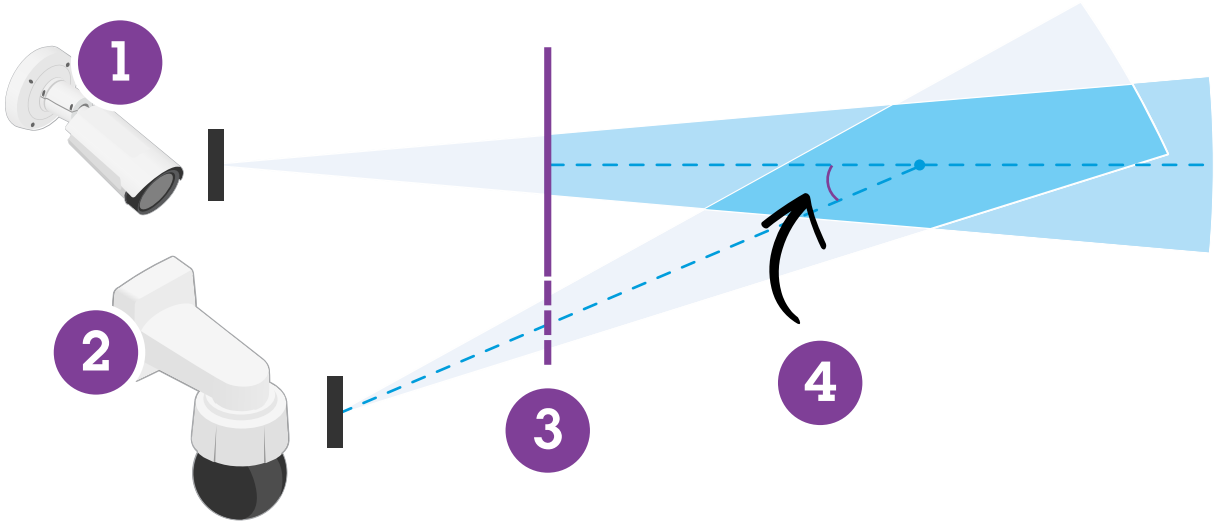
- Visão clara
- O chão deve ser plano ou ter apenas uma ligeira inclinação
- Iluminação não acionada por movimento
- Visão clara
- Para câmeras visuais, o nível de iluminação e configurações de imagem deve ser suficiente para fornecer contraste suficiente entre pessoas e veículos e o fundo.
  - Quando você usa uma câmera dia e noite Axis com iluminação artificial, recomendamos pelo menos 50 Lux em toda a zona de detecção.
  - Ao usar pontos IR externos, recomendamos uma distância de detecção máxima de 80 m e que a faixa de pontos IR seja mais do que duas vezes a distância máxima de detecção.
  - Ao usar iluminação IR interna, a distância de detecção máxima estará limitada a 20 m, dependendo da câmera e do ambiente.
- Para câmeras térmicas, deverá haver um alto contraste entre o fundo e o primeiro plano

Para otimizar o desempenho de detecção, o AXIS Perimeter Defender aprende automaticamente a diferença entre dia e noite e usa essas informações para aperfeiçoar os algoritmos de detecção. O ajuste fino leva cerca de 24 horas, o que significa que a detecção ideal durante o dia e a noite será atingida após executar o aplicativo por esse tempo.

Monte a câmera PTZ.

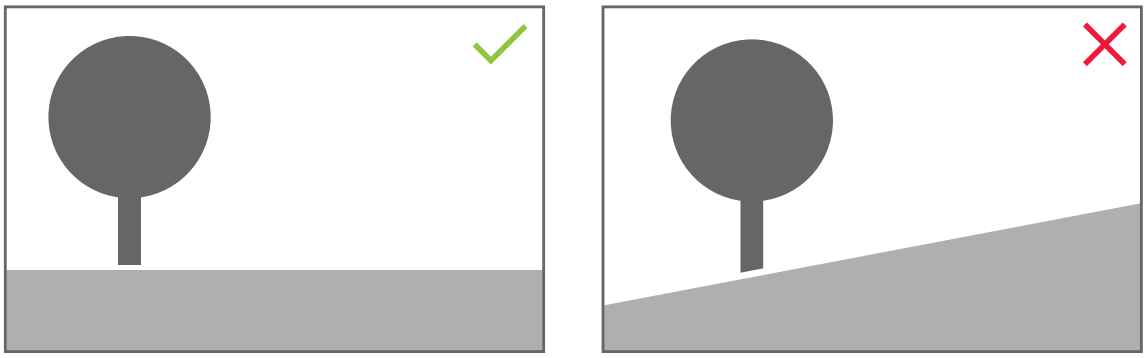
Este capítulo descreve como montar a câmera PTZ em relação à câmera fixa. Para obter instruções sobre como montar a câmera fixa, consulte *Montagem da câmera na página 13*.

Introdução



1 *Câmera de rede fixa*
2 *Câmera de rede PTZ*
3 *Distância mínima de detecção*
4 *Ângulo entre as câmeras*

- A posição predefinida inicial da câmara PTZ deve abranger mais de 60% da zona de detecção da câmara fixa.
- Para ser rastreada pela câmera PTZ, uma pessoa em pé deve cobrir mais de 4% da altura da imagem da câmera PTZ.
- A câmera PTZ deve ser colocada antes da distância mínima de detecção da câmera fixa (C).
- O ângulo entre a câmara fixa e a câmara PTZ deve ser inferior a 30° (D).



- O chão deve estar plano.

Instale o software no computador

1. Baixe o software AXIS Perimeter Defender de *axis.com/products/axis-perimeter-defender*
2. Instale o software no seu computador.

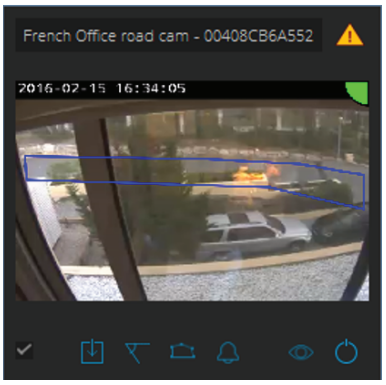
Adicionar dispositivos

Você pode adicionar dispositivos ao aplicativo AXIS Perimeter Defender de três maneiras diferentes:

- Automaticamente através de uma verificação de rede. Consulte *Adicionar dispositivos automaticamente na página 17*.
- Manualmente, especificando as configurações de conexão. Consulte *Adicionar dispositivos manualmente na página 17*.
- Automaticamente carregando um site salvo anteriormente. Consulte *Carregar um site existente na página 18*.

Ao adicionar um dispositivo, você verá uma lista de todos os outros aplicativos instalados no dispositivo. Recomendamos que você interrompa quaisquer aplicativos não essenciais, pois eles usam os recursos da CPU da câmera, o que afeta o desempenho do AXIS Perimeter Defender e pode impedir a instalação correta.

Se um dispositivo não tiver recursos de CPU suficientes, por exemplo, porque outros aplicativos estão em execução, o AXIS Perimeter Defender diminuirá a taxa de quadros. Se a taxa de quadros estiver abaixo de 5 quadros por segundo, um triângulo de advertência amarelo será exibido ao lado do nome do dispositivo na visualização ao vivo. Quando você move o mouse sobre o triângulo, a taxa de quadros atual é exibida.



Observação

Uma taxa de quadros abaixo de 5 fps pode diminuir significativamente o desempenho analítico de vídeo. Isso pode resultar em detecções perdidas e falsas.

Para obter mais informações, consulte *Carga da CPU na página 12*.

Adicionar dispositivos automaticamente

Importante

A funcionalidade de pesquisa não funciona em redes, ou seja, a configuração do AXIS Perimeter Defender só poderá encontrar dispositivos que estejam conectados à mesma sub-rede que o cliente que executa o software. Para adicionar dispositivos conectados a uma sub-rede diferente, adicione-os manualmente. A funcionalidade de pesquisa também poderá falhar se os roteadores ou switches de rede estiverem configurados para filtrar multicast.

1. Para varrer dispositivos na rede circundante, vá para **Aplicativo** e clique em **Pesquisar**.

   Quando você faz uma pesquisa pela primeira vez e não há senhas disponíveis, uma caixa de diálogo de senha é aberta. Caso contrário, a senha disponível será usada para se conectar aos dispositivos.

2. Selecione dispositivos e clique em **Adicionar dispositivos selecionados**.

   Se a senha estiver correta, uma imagem estática será exibida para guiar o usuário ao selecionar dispositivos.

Adicionar dispositivos manualmente

1. Vá para **Aplicativo** e clique em **Adicionar**.

2. Insira o seguinte:
   - O endereço IP ou o nome de host do dispositivo.
   - A senha de root do dispositivo, pois o AXIS Perimeter Defender requer acesso root.
   - A porta HTTP usada para se conectar. A porta padrão é 80.
   - Um nome opcional para o dispositivo para facilitar o reconhecimento.
   - Se o dispositivo estiver em uma rede remota para a qual a conexão pode ser lenta, selecione **Dispositivo na rede remota**. Conexões lentas não configuradas como remotas podem levar ao não funcionamento ou a calibrações ruins.

   Observação

   Para conexões remotas, o usuário deve ser capaz de se conectar ao dispositivo por meio de HTTP. Certifique-se de configurar a porta HTTP corretamente. A configuração remota poderá falhar quando a conexão não tiver largura de banda suficiente ou estável.

3. Clique em **OK**.

Observação

Se isso não funcionar para adicionar uma câmara por nome de host, verifique as configurações de rede e DNS ou adicione o dispositivo usando o respectivo endereço IP.

Carregar um site existente

Para carregar uma configuração de site salva anteriormente:

1. Vá para **Aplicativo** e clique em **Carregar site**.
2. Navegue para selecionar o arquivo de configuração do site e clique em **Abrir**. A visualização ao vivo será exibida automaticamente.

Instalar software em dispositivos

Você precisa instalar o AXIS Perimeter Defender em cada dispositivo.

Se você desejar verificar qual versão do AXIS Perimeter Defender está instalada em um dispositivo, mova o mouse sobre **Status da instalação** na visualização ao vivo.

Se um dispositivo não tiver o AXIS Perimeter Defender instalado, todos os ícones na visualização ao vivo estarão cinzas.

Instalar o software em um dispositivo

1. Vá para **Instalação**.
2. Selecione os dispositivos onde você deseja instalar o aplicativo.
3. Selecione a versão mais recente disponível do AXIS Perimeter Defender e clique em **Instalar**.

   O AXIS Perimeter Defender está agora instalado nos dispositivos selecionados e será iniciado automaticamente.
4. Procure uma licença e execute um dos seguintes procedimentos:
   - Se você estiver instalando em um único dispositivo: selecione o arquivo de licença para o dispositivo.
   - Se você estiver instalando em vários dispositivos: selecione a pasta onde os arquivos de licença são armazenados.
5. Clique em **Instalar**.

Calibrar - AXIS Perimeter Defender

Calibração

Observação

Não é necessário calibrar dispositivos que operam somente no modo AI. Para operar dispositivos no modo de calibração e no modo AI, é necessário calibrá-los.

Para que o AXIS Perimeter Defender interprete corretamente a cena, você deve calibrar todos os dispositivos. Durante a calibração, você introduz pontos de referência que fornecem informações de profundidade e altura para o processador. Você também define a zona de interesse.

A calibração consiste em duas tarefas:

1. Executar uma calibração:
   - automática — recomendada na maioria dos casos. Consulte *Executar uma calibração automática na página 19*.
   - manual — recomendada se a calibração automática falhar em uma câmera, para ajuste fino, ou quando for impraticável fazer uma caminhada pela cena e houver objetos de altura conhecida na cena. Um exemplo disso é um perímetro remoto com uma linha de cerca que consiste em um número de mourões uniformemente espaçados de uma altura consistente. Consulte *Execute uma calibração manual na página 24*.
2. Verificar os resultados da calibração. Consulte *Verifique a qualidade da calibração na página 21*.

Para acelerar a configuração de um site grande, você pode calibrar vários dispositivos simultaneamente. É possível executar a calibração automática ou manualmente, assim como para uma única câmera. Considere o seguinte antes de calibrar vários dispositivos simultaneamente:

- O número máximo de dispositivos que você pode instalar e configurar simultaneamente depende da potência da CPU e da memória disponível em seu computador. Muitos dispositivos no AXIS Perimeter Defender Setup podem causar falhas. Quando o aviso de sobrecarga da CPU aparecer, instale e configure um subconjunto dos dispositivos usando o recurso para gravação de site.
- A calibração automática de vários dispositivos requer mais recursos de CPU e RAM do que um único dispositivo. Em sistemas com especificações fracas, isso pode fazer com que o computador não responda por algum tempo ou causar uma falha no aplicativo. Em caso de acidente, os vídeos capturados ainda estarão disponíveis para serem usados posteriormente para uma única calibração da câmera.

Observação

- O AXIS Perimeter Defender oferece suporte a diferentes proporções de imagem de acordo com a resolução máxima fornecida pela câmera. Como resultado, você precisará refazer todas as calibrações anteriores se alterar a resolução. No entanto, se você alterar a resolução de stream na página da Web da câmera, não será necessário recalibrar.
- Recomendamos que você use a mesma proporção de imagem no AXIS Perimeter Defender e nas VMs, para certificar-se de que as informações exibidas caiam no conteúdo da imagem. Para descobrir a taxa de proporção, mova o mouse sobre o nome da câmera na visualização ao vivo.
- Se uma câmera se mover após a calibração, você precisará recalibrá-la para que os resultados analíticos sejam corretos.

Executar uma calibração automática

Com a calibração automática, você pode calibrar uma ou mais câmeras ao deixar uma pessoa percorrer a cena de vigilância. A câmera coleta automaticamente as informações necessárias para se calibrar.

Para realizar uma calibração automática bem-sucedida:

- Não calibre quando houver muitas pessoas no campo de visão.
- Não calibre quando houver muitos veículos passando no campo de visão.
- Não calibre quando houver outros objetos em movimento no campo de visão. Por exemplo, árvores ou bandeiras se movendo ao vento.

- Não calibre uma câmara que não tenha sido instalada paralela ao solo.
- A pessoa que percorre a cena deve ser capaz de cobrir todo o campo de visão de frente para trás. Se isso não for possível, será melhor mudar para a calibração manual.
- Se a câmera estiver em uma rede remota, mas não conectada como remota, a pessoa que percorrer a cena deverá andar por cerca de 5 minutos para garantir que imagens suficientes sejam capturadas. Isso ocorre porque a taxa de quadros é geralmente menor para dispositivos em redes remotas.

1. Vá para **Calibração**.
2. Selecione os dispositivos que deseja calibrar.
3. Clique em **Automático**.
4. Defina a hora de início da gravação. A captura deverá começar pelo menos 10 segundos antes da pessoa que percorre a cena entrar no campo de visão.
5. Defina a duração da gravação. Considere que:
   - deverá haver tempo suficiente para que a pessoa caminhe para frente e para trás por toda a cena.
   - a duração do vídeo afeta o cálculo da calibração.
6. Insira a altura (cm) da pessoa que está andando pela cena e clique em **Capturar**.

   Para reutilizar um vídeo capturado anteriormente, clique em **Usar captura anterior**.
7. Deixe a pessoa andar pela cena de acordo com as seguintes instruções:
   - Caminhe em um zigue-zague que abranja o máximo possível da zona de detecção de frente para trás da cena. Recomendamos um caminho em V pelo campo de visão.
   - Permaneça quase sempre totalmente visível da cabeça aos pés no campo de visão.
   - Caminhe lentamente em linhas retas.
   - Mantenha uma postura vertical o tempo todo.
   - Pause por 1-2 segundos antes de mudar de direção.

Um exemplo de uma sequência de caminhada.

8. Verifique se a calibração automática foi bem-sucedida confirmando que a pessoa foi detectada com precisão. Consulte *Verifique a qualidade da calibração na página 21*.
9. Para salvar a calibração, clique em **Aceitar**.

   Para executar uma nova calibração, clique em **Novo**.

   Para executar uma calibração manual, clique em **Manual**.

Após aceitar a calibração, as bordas azuis indicarão a zona de detecção máxima. A zona de detecção máxima é a maior área que pode ser monitorada. Fora dessa área, invasores podem ser detectados, mas isso não é garantido.

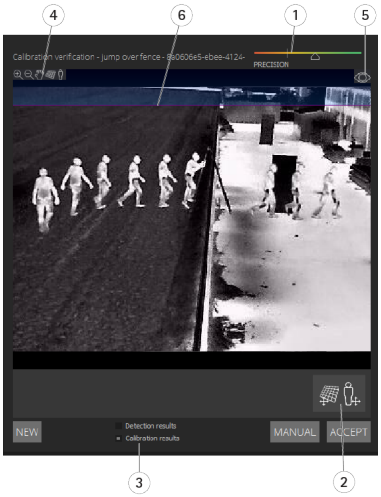
Verifique a qualidade da calibração

Depois de uma calibração, você deve ver a pessoa que atravessou a cena em vários lugares diferentes. Se a pessoa não estiver visível, a calibração automática terá falhado e precisará ser refeita.

Existem várias maneiras de verificar a qualidade da calibração:

- Verifique o indicador de precisão de calibração. Ele reflete um nível de precisão calculado automaticamente que mede o quão bem a pessoa cobriu a cena e o quão bem ela foi detectada. Se o indicador de precisão estiver na zona vermelha, a calibração terá falhado e não será possível clicar em **Aceitar**. Consulte *Execute uma calibração manual na página 24*.
- Você pode usar a ferramenta de grade. Consulte *Use a grade para verificar a calibração na página 22*.
- Você pode usar a ferramenta de avatar. Consulte *Use o avatar para verificar a calibração na página 23*.
- Você pode verificar os resultados da detecção. Consulte *Use os resultados de detecção para verificar a calibração na página 24*.

Introdução



1 *Indicador de precisão de calibração*
2 *Ferramentas de grade e avatar*
3 *Exibição dinâmica ou estática*
4 *Modificadores de exibição*
5 *Alternar entre a imagem de calibração e a visualização ao vivo*
6 *Linha do horizonte*

A linha do horizonte representa a extremidade visível do chão na cena. Quando você define cenários, não é possível colocar zonas de cenário na área azul acima da linha do horizonte, pois isso está acima do solo e as zonas de cenário estão, por definição, no solo.

Use a grade para verificar a calibração

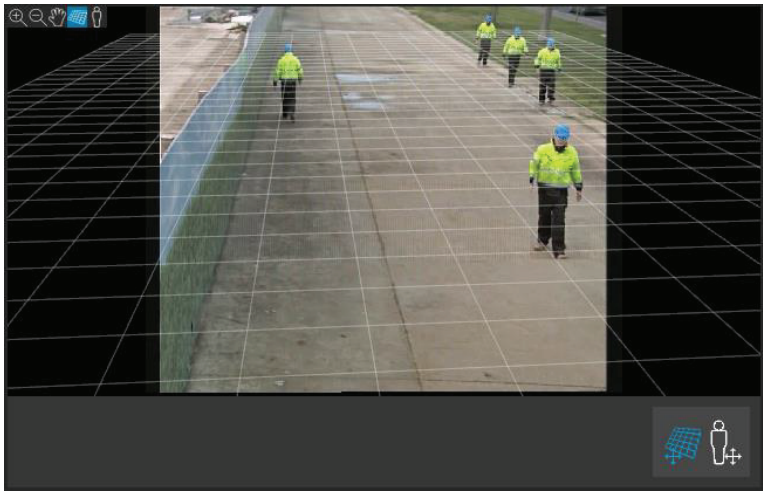
A grade deve corresponder a uma grade quadrada no chão. Você pode alternar a exibição da grade ao clicar no ícone de modificação de exibição de grade.

Importante

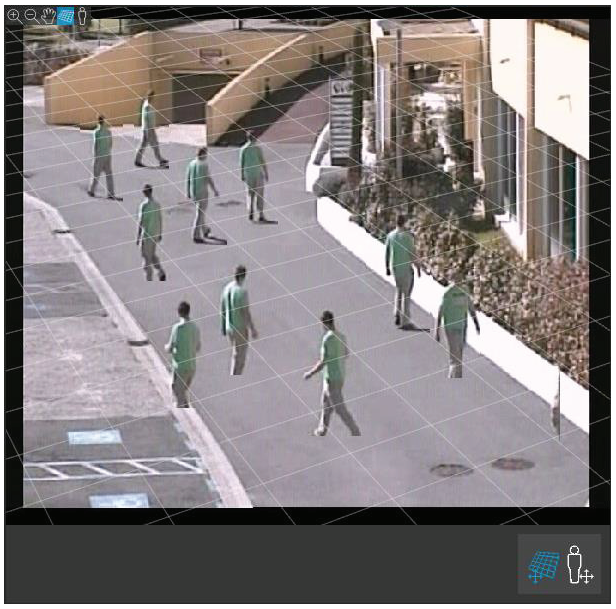
A grade não afeta a calibração, ela é uma ferramenta para verificar se a calibração está correta.

Você pode ativar a grade arrastando-a no painel de visualização. Tente alinhá-la com alguma estrutura na cena para ver se o resultado parece razoável.

Se a grade estiver paralela ao chão, não tiver uma inclinação estranha e, após a aplicação da rotação necessária, estiver paralela a artefatos de fabricação humana que sejam paralelos no mundo real, a calibração estará satisfatória.



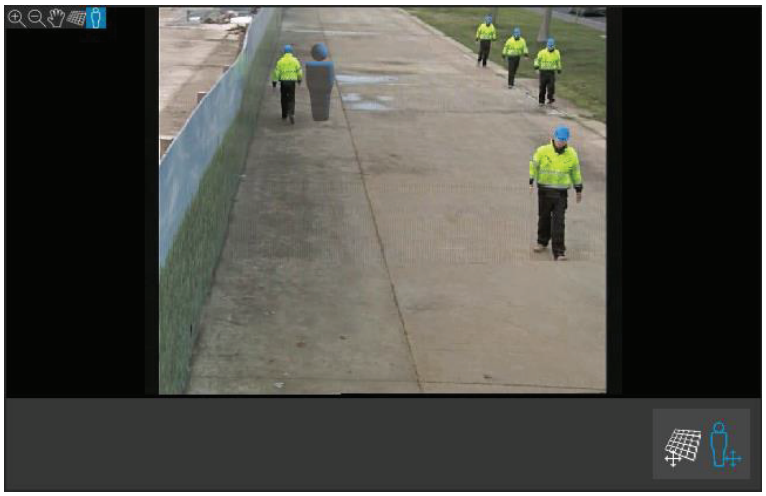
Um exemplo onde a grade está corretamente alinhada com os acostamentos.



Um exemplo onde a grade não está corretamente alinhada com os acostamentos.

Use o avatar para verificar a calibração

O avatar permite que você coloque um avatar 3D de pessoa com altura média na cena. Você pode alternar a exibição do avatar ao clicar no ícone de modificação de visualização de avatar.



Seu tamanho no painel de exibição corresponde ao tamanho de uma pessoa média nessa posição de acordo com a calibração atual. Ao mover o avatar, você pode verificar se seu tamanho está razoável em relação a outros objetos ou pessoas na cena. Você deve verificar o avatar em diferentes posições, pois ele pode ser dimensionado de forma correta em uma posição, mas de forma incorreta em outra na imagem.

Use os resultados de detecção para verificar a calibração

Você pode usar os resultados de detecção para verificar como seria o desempenho do AXIS Perimeter Defender com a calibração atual se ele tivesse recebido as imagens de vídeo de caminhada da pessoa como um stream ao vivo.

1. Alterne de **Resultados de calibração** para **Resultados de detecção**.
2. Verifique as detecções das pessoas ou veículos que entram na cena de vigilância:
   - Se a calibração estiver boa, as pessoas serão marcadas com retângulos vermelhos e os veículos com retângulos azuis.
   - Se pessoas ou veículos frequentemente não forem marcados, provavelmente a calibração automática terá falhado.
   - Uma zona vermelha mostra a zona limite de detecção de acordo com a calibração calculada, ou seja, a zona onde os pré-requisitos na altura humana na imagem não são respeitados. Nessa zona, a detecção pode falhar devido ao tamanho do alvo.

Observação

- Se a calibração calculada estiver errada, a zona vermelha também estará errada.
- Se a pessoa estiver muito longe, ela poderá não ser marcada. Um tamanho mínimo é necessário para que a detecção funcione. Para obter mais informações, consulte *Montagem da câmera na página 13*.
- Revisar os resultados da detecção pode não funcionar em câmeras conectadas remotamente, pois a captura pode ter uma taxa de quadros muito baixa. Isso não significa que a configuração falhou. Use o avatar e a grade para verificar a calibração em vez disso.

Execute uma calibração manual

Se você não tiver tentado uma calibração automática, será necessário capturar um vídeo curto e criar uma imagem composta antes de executar uma calibração manual. Siga as mesmas etapas para uma calibração automática (*Executar uma calibração automática na página 19*), mas selecione **Manual** em vez de **Automática** na guia **Calibração**. Para criar a imagem composta depois de capturar um vídeo:

- mova o controle deslizante para navegar no clipe de vídeo

- em posições-chave, clique no ícone da câmera para adicionar imagens à composição

Certifique-se de que a imagem composta reflita a seção transversal completa da cena: frente, trás, esquerda e direita.

Quando você tem uma imagem composta, criada manual ou automaticamente, é possível continuar a calibração manual.

O mecanismo de calibração calibra ao estimar:

- o horizonte
- a forma como as linhas verticais se espalham, ou ventilam, na imagem
- a escala da cena

Ao executar uma calibração manual, é necessário fornecer essas informações ao mecanismo de calibração por meio de elementos de calibração. Há três tipos de elementos de calibração:

- Os **bastões de pessoas** são usados para marcar a altura conhecida de uma pessoa média em várias posições na cena. Se você já tiver tentado executar uma calibração automática, é muito provável que a imagem exibida no painel do editor mostre várias instâncias da mesma pessoa. Coloque os bastões de pessoas do chão para cima para marcar a altura e a direção da pessoa em uma ou mais posições. Um bastão de pessoa deve começar no chão e ser vertical no mundo real. O comprimento de um bastão de pessoa no mundo real deve corresponder à altura indicada ao lado do botão **Pessoa** no painel do editor. Os bastões de pessoa são marcados com um símbolo azul-claro semitransparente.

  Como melhor posicionar um bastão de pessoa

  - Recomendamos que você coloque um bastão em uma pessoa com os pés próximos.
  - Se você colocar um bastão em uma pessoa em pé no chão com os pés separados, coloque o ponto mais baixo no chão a meio caminho entre os saltos da pessoa.
  - Alinhe o bastão com o torso da pessoa. No entanto, ela estiver se inclinando em alguma direção, geralmente, para frente ao andar, tente compensar a inclinação ao posicionar o bastão mais verticalmente. Use quaisquer pistas na cena para orientá-lo, por exemplo, árvores, cercas ou postes de iluminação.
  - Para a escala da cena, pelo menos um bastão de pessoa com a altura da pessoa correspondente é necessário. Se não houver pessoa visível na cena, você poderá adicionar um bastão de pessoa em algum outro objeto vertical de altura conhecida, por exemplo, um mourão de 3 m, e definir a altura da pessoa como a altura do objeto.

- **Linhas horizontais paralelas (linhas H)** são usadas para marcar linhas horizontais e paralelas conhecidas na cena. Essas linhas podem estar no chão ou em uma parede ou ambos, mas todas elas devem ser paralelas. Se você adicionar linhas H, será necessário adicionar pelo menos duas. Você pode colocá-las nos lados ou nas marcações em uma estrada reta, em um conjunto de trilhas retas da estrada de ferro, em alguma estrutura visível em uma parede, ou nas partes superiores e inferiores de uma fileira de mourões. As linhas H são marcadas em azul-claro.

- As **linhas verticais (linhas V)** são usadas para marcar linhas verticais conhecidas na cena. Uma linha V deve marcar alguma estrutura vertical no mundo real. Isso pode ser, por exemplo, um mourão, o canto de um edifício, ou uma placa. Uma linha V não precisa começar no chão. As linhas em V são marcadas em azul-escuro. Observe que as linhas V são muito sensíveis, pois uma pequena mudança de orientação pode alterar drasticamente a calibração. Como regra geral, as linhas V devem inclinar-se para a direita no lado direito da imagem e deixadas no lado esquerdo.

1 *Bastões de pessoa*
2 *Linhas verticais (linhas V)*
3 *Linhas horizontais paralelas (linhas H)*
4 *Ferramentas de grade e avatar*

Número de elementos de calibração

Geralmente, quando você adiciona bastões de pessoa, linhas H e V na cena, quanto mais itens melhor. O mecanismo de calibração pode calibrar com muito poucas linhas, mas, geralmente, a qualidade da calibração começa a melhorar conforme as linhas e os bastões desenhados aumentam. Ao adicionar bastões de pessoa, recomendamos que você coloque ambos perto e longe, à esquerda e direita.

Estruturas verticais na imagem

Segundo *Recomendações para montagem da câmera na página 14*, todas as câmeras devem apontar ligeiramente para baixo. Como resultado, todas as estruturas verticais no mundo real parecem ventilar como uma cauda de pavão na imagem. Isso significa que todos os bastões de pessoa e linhas V devem inclinar para a borda da imagem. Um bastão na metade direita da imagem deve inclinar para a direita e um bastão à esquerda deve inclinar para a esquerda. Pelo menos um dos bastões de pessoa ou linhas V colocados devem estar "inclinados corretamente" para que a calibração funcione.

O indicador de precisão fornece feedback visual sobre o nível e a qualidade dos detalhes que foram adicionados à cena. Para calibrações manuais bem-sucedidas, as marcações devem cobrir a cena da frente para trás e da esquerda para a direita. Isso é identificado por um indicador de precisão verde.

Qualidade da calibração

A qualidade da calibração pode ser verificada com os manipuladores de grade ou avatar. Consulte *Verifique a qualidade da calibração na página 21*. Como alternativa, clique em **Revisar**. Isso mostra o resultado da execução do AXIS Perimeter Defender no vídeo capturado usando a calibração manual atual.

Calibrar - PTZ Autotracking

Importante

Para alcançar bons resultados, a calibração deve ser de alta qualidade. Siga atentamente as orientações e instruções.

Observação

Você pode calibrar ambas as câmeras ao mesmo tempo, ou uma de cada vez.

1. Selecione a câmera fixa e a câmera PTZ.

2. Vá para **Calibração** e clique em **Configurar posição PTZ**. Um pop-up com a visão da câmera fixa é mostrado.

   A câmera PTZ vai executar pan, tilt e zoom por um curto período de tempo quando o aplicativo for iniciado.

3. Verifique se as visões das duas câmeras estão alinhadas entre si.

   Se não estiverem, clique na imagem da visualização ao vivo para ajustar o modo de exibição da câmera PTZ até que ele corresponda à visão da câmera fixa. Certifique-se de que não haja rolo.

4. Clique em **Configurar posição da PTZ**.

   Se o botão não estiver visível, mova o pop-up com a visão da câmera fixa.

5. Clique em **Automático**.

6. Realize uma calibração automática de acordo com as instruções em *Executar uma calibração automática na página 19*.

7. Use o avatar para verificar a qualidade da calibração para a câmera fixa. Consulte *Use o avatar para verificar a calibração na página 23*.

   Se a qualidade for boa o suficiente, clique em **Aceitar**.

   Se a qualidade não for boa o suficiente, use o vídeo da calibração automática para fazer uma calibração manual. Clique em **Manual** e siga as instruções em *Execute uma calibração manual na página 24*.

8. Em **Cenários**, defina as regras para o que deve acionar alarmes. Consulte *Definir cenários na página 27*.

9. Em **Calibração**, clique em **Revisar** na visualização ao vivo da câmera PTZ.

10. Use o avatar para verificar a qualidade da calibração para a câmera PTZ. Consulte *Use o avatar para verificar a calibração na página 23*.

    Se a qualidade for boa o suficiente, clique em **Aceitar**.

    Se a qualidade não for boa o suficiente, use o vídeo da calibração automática para fazer uma calibração manual. Clique em **Manual** e siga as instruções em *Execute uma calibração manual na página 24*.

11. Emparelhe as câmeras. Consulte *Emparelhar as câmaras - PTZ Autotracking na página 30*.

Definir cenários

Cenários

O AXIS Perimeter Defender inclui cenários de zona estéril comuns que você pode configurar para proteger e monitorar áreas sensíveis. Na etapa de calibração, a zona de detecção máxima foi criada para fornecer um cenário padrão do tipo invasão/vadiagem. Nessa etapa, você pode definir cenários de detecção mais sofisticados de três tipos diferentes:

- invasão/vadiagem. Consulte *Configurar o cenário de invasão/vadiagem na página 28*
- cruzamento de zonas. Consulte *Configurar o cenário de cruzamento de zona na página 28*
- condicional. Consulte *Configurar o cenário condicional na página 29*

Se o símbolo **!** for exibido por um nome de cenário, isso significará que a configuração do cenário não estará completa. O problema mais comum é que sua zona de detecção ainda não foi definida.

Parâmetros globais

Os parâmetros globais que você definiu na interface do usuário se aplicam a todos os cenários.

Tipo de câmera - Para câmeras visuais, selecione **Cor-dia-noite**. Para câmeras térmicas, o tipo de câmera é automaticamente definido como térmico.

Observação

- Tipos de abordagem adicionais podem aumentar o risco de alarmes falsos, por exemplo, causados por animais.
- Não há suporte a tipos de abordagem adicionais para dispositivos que operam somente no modo AI.

Tipos de abordagem adicionais – Selecione aqueles que você deseja cobrir com seu cenário de detecção.

Mitigação avançada – Para dispositivos com o modo AI, marque a opção **AI** para ativá-lo. Você poderá usar a opção **Headlights/vehicles in scene (Faróis/veículos na cena)** se a cena contiver veículos, faróis ou efeitos de faróis, como reflexos. Se você usar essa configuração, o desempenho às vezes poderá ser reduzido em condições normais. Por padrão, todos os cenários devem conter veículos e, portanto, faróis. Você pode usar **Insects/droplets on lens (Insetos/gotículas na lente)** para ignorar acionadores causados por chuva ou insetos e reduzir a quantidade de alarmes falsos.

Sensibilidade – Para aumentar a sensibilidade do sistema, mova o controle deslizante para a direita. Uma maior sensibilidade reduz o risco de detecções perdidas, mas aumenta o risco de falsos alarmes.

Filtragem de tamanho-alvo – Para dispositivos com o modo AI, você pode filtrar objetos menores que o tamanho-alvo.

Parâmetros de duração

Para cada cenário que você criar, defina parâmetros de duração.

Presença mínima na zona – Defina a hora em que um objeto deve permanecer em uma zona para que ela seja ativada.

Zona estreita – Se a zona é estreita e pode ser atravessada em 1 – 2 segundos, há o risco de alarmes perdidos. Esse comportamento pode ser minimizado com a funcionalidade **Narrow zone (Zona estreita)**. Observe que não é possível combinar com **Min presence in zone (Presença mínima na zona)**.

Configurar o cenário de invasão/vadiagem

O cenário de invasão/vadiagem foi projetado para acionar um alarme quando um objeto entra em uma determinada zona e nela permanece por mais tempo do que o tempo predefinido.

O cenário padrão criado na etapa de calibração é do tipo invasão/vadiagem e usa a zona de detecção máxima. Para usar esse cenário como está, clique em **Aceitar** na guia **Cenários**.

Para alterar o cenário padrão:

1. Vá para **Cenários > Cenários avançados**.
2. Altere a zona de detecção predefinida:
   - Para mover os pontos existentes na zona de detecção, clique e arraste-os com o mouse.
   - Para criar pontos adicionais, clique em qualquer um dos segmentos existentes e arraste com o mouse.
3. Em **Detectar**, selecione o tipo de objeto a ser detectado.
4. Em **Parâmetros de duração**, se você não desejar que um objeto acione um alarme assim que ele entrar na zona, defina o tempo de vadiagem em **Presença mínima na zona**.
5. Se a zona for estreita e puder ser atravessada em 1 – 2 segundos e você mesmo assim quiser que os alarmes sejam acionados, selecione **Narrow zone (Zona estreita)**. Essa configuração não pode ser combinada à opção **Min presence in zone (Presença mínima na zona)**. Para obter mais informações, consulte *Parâmetros de duração na página 28*.
6. Para carregar as alterações na câmera e voltar para a exibição principal, clique em **Aceitar**.

Configurar o cenário de cruzamento de zona

O cenário de cruzamento de zonas foi projetado para acionar um alarme quando um objeto passa por duas zonas de detecção em uma determinada sequência.

Importante

O cenário de cruzamento de zona possui a seguinte limitação: se o objeto que acionar o cenário parar de se mover por alguns segundos na zona de origem antes de passar para a zona final, o cenário não será acionado.

Em **Parâmetros de duração**, você pode definir um tempo de presença mínimo para cada uma das zonas no cenário. Se T_A for o tempo mínimo na zona de origem e T_B na zona final, um alarme só será disparado se o objeto permanecer por mais tempo que T_A na zona de origem e, em seguida, mais que T_B na zona final.

1. Vá para **Cenários > Cenários avançados**.
2. Clique em **Novo** e selecione **Cruzamento de zona**.
3. Crie duas zonas de detecção separadas por pelo menos um metro (3 pés 3 3/8 polegadas):
   - Para criar uma zona de detecção, clique várias vezes na imagem.
   - Para concluir a zona, clique com o botão direito do mouse na imagem.
4. Para especificar a direção de cruzamento proibida, clique em **Selecionar origem** e, em seguida, clique em uma das zonas.
5. Em **Detectar**, selecione o tipo de objeto a ser detectado.
6. Em **Parâmetros de duração**, se você não desejar que uma zona seja ativada assim que um objeto entrar, defina a **Presença mínima em** para uma ou ambas as zonas.
7. Se a zona for estreita e puder ser atravessada em 1 – 2 segundos e você mesmo assim quiser que os alarmes sejam acionados, selecione **Narrow zone (Zona estreita)**. Essa configuração não pode ser combinada à opção **Min presence in zone (Presença mínima na zona)**. Para obter mais informações, consulte *Parâmetros de duração na página 28*.
8. Para carregar as alterações na câmera e voltar para a exibição principal, clique em **Aceitar**.

Configurar o cenário condicional

O cenário condicional foi projetado para acionar um alarme quando um objeto entra em uma determinada zona sem primeiro passar por outras.

Em **Parâmetros de duração**, você pode definir um tempo de presença mínimo para cada uma das zonas no cenário. Se T_A for o tempo mínimo na zona autorizada e T_B na zona de invasão, um alarme só será disparado se o objeto:

- permanecer por mais tempo que T_B na zona de invasão sem ter entrado primeiro na zona autorizada.
- permanecer por tempo inferior a T_A na zona autorizada, entrar e permanecer por mais tempo que T_B na zona de invasão.

Nenhum alarme será disparado se o objeto:

- não entrar ou permanecer por menos tempo que T_B na zona de invasão.
- permanecer por mais tempo que T_A na zona autorizada, entrar na zona de invasão (independentemente do tempo que o objeto permanecer).

1. Vá para **Cenários > Cenários avançados**.
2. Clique em **Novo** e selecione **Condicional**.
3. Crie duas ou mais zonas de detecção separadas por pelo menos um metro (3 pés 3 3/8 polegadas):
   - Para criar uma zona de detecção, clique várias vezes na imagem.
   - Para concluir a zona, clique com o botão direito do mouse na imagem.
4. Para especificar a direção de cruzamento permitida, clique em **Selecionar zona de invasão** e clique em uma das zonas.
5. Em **Detectar**, selecione o tipo de objeto a ser detectado.

6. Em **Parâmetros de duração**, se você não desejar que uma zona seja ativada assim que um objeto entrar, defina a **Presença mínima em** para uma ou ambas as zonas.

7. Se a zona for estreita e puder ser atravessada em 1 – 2 segundos e você mesmo assim quiser que os alarmes sejam acionados, selecione **Narrow zone (Zona estreita)**. Essa configuração não pode ser combinada à opção **Min presence in zone (Presença mínima na zona)**. Para obter mais informações, consulte *Parâmetros de duração na página 28*.

8. Para carregar as alterações na câmera e voltar para a exibição principal, clique em **Aceitar**.

Emparelhar as câmaras - PTZ Autotracking

Na configuração do AXIS Perimeter Defender PTZ Autotracking, você deve emparelhar a câmera fixa e a câmera PTZ entre si para garantir que um objeto em movimento seja rastreado de maneira eficiente pela câmera PTZ.

Se você tiver executado uma calibração automática, será possível *Executar um emparelhamento automático na página 30* das duas câmeras. Caso contrário, você precisará *Executar um emparelhamento manual na página 30*.

Executar um emparelhamento automático

No vídeo de emparelhamento, as linhas vermelhas representam a pessoa e a caixa delimitadora laranja representa a imagem ampliada da câmera PTZ.

1. Em **Calibração > Revisão do emparelhamento PTZ**, verifique os vídeos de emparelhamento das duas câmeras:
   - verifique se as linhas vermelhas nas duas imagens estão alinhadas ao longo do vídeo
   - verifique se as linhas vermelhas sempre vão dos pés à cabeça da pessoa
   - verifique se a pessoa está sempre centralizada dentro da caixa delimitadora laranja no vídeo da câmera PTZ
2. Se as condições na etapa 1 forem atendidas, selecione **Revisão de emparelhamento interativa**.

   Se as condições não forem atendidas, clique em **Manual** e siga as etapas em *Executar um emparelhamento manual na página 30*.
3. Mova o controle deslizante para navegar no clipe de vídeo. Verifique se:
   - as linhas azuis nas duas imagens estão alinhadas em todo o vídeo
   - verifique se a pessoa está sempre centralizada dentro da caixa delimitadora laranja no vídeo da câmera PTZ
4. Se houver cenas em que a caixa delimitadora laranja esteja ausente:

   4.1 Ative o avatar na imagem da câmera fixa.

   4.2 Use o controle deslizante para avançar e retroceder no vídeo. Coloque o avatar na pessoa exibida pela câmera fixa, e verifique se o ponto vermelho está nos pés da pessoa na imagem da câmera PTZ.
5. Se houver cenas em que o emparelhamento automático não tenha adicionado linhas azuis, clique em **Manual** e adicione linhas vermelhas manualmente à pessoa. Consulte *Executar um emparelhamento manual na página 30* para obter instruções detalhadas.
6. Clique em **Aceitar** e **Sair**.

Executar um emparelhamento manual

Ao executar um emparelhamento manual, você adiciona linhas vermelhas verticais dos pés à cabeça da pessoa que atravessou a cena de vigilância na etapa de calibração. Você precisa adicionar linhas em todo o vídeo, para cobrir toda a cena.

Se você já tiver executado um emparelhamento automático, o vídeo já conterá linhas azuis.

Remova as linhas azuis e vermelhas que:

- não comecem nos pés da pessoa
- não percorra todo o caminho até a cabeça da pessoa
- não tem uma linha correspondente na imagem da câmera PTZ

Para remover uma linha, clique nela e pressione EXCLUIR.

1. Mova o controle deslizante para navegar até uma imagem no clipe de vídeo onde a pessoa está visível.
2. Adicione uma linha vermelha à pessoa na imagem da câmera fixa. Comece a linha nos pés da pessoa. A linha obterá um número de identificação.
3. Adicione uma linha vermelha correspondente ao mesmo objeto na imagem da câmera PTZ. Verifique se o número de identificação corresponde ao da imagem da câmera fixa.
4. Repita os passos 1–3 até cobrir a cena inteira.

   Quando o clipe de vídeo contiver um número suficiente de linhas para um emparelhamento válido:

   - o botão **Aceitar** se tornará ativo
   - uma caixa delimitadora laranja é mostrada na imagem da câmera PTZ
5. Verifique se a pessoa está sempre centralizada na caixa delimitadora laranja. Se houver cenas onde ela não esteja, adicione mais linhas vermelhas.
6. Ative o avatar na imagem da câmera fixa.
7. Mova o controle deslizante para navegar no clipe de vídeo. Use o avatar para verificar se:

   - na imagem da câmera fixa, o tamanho do avatar corresponde ao tamanho da pessoa, em diferentes posições
   - na imagem da câmera PTZ, o ponto vermelho está nos pés da pessoa
   - na imagem da câmera PTZ, a pessoa está sempre centralizada dentro da caixa delimitadora laranja
8. Clique em **Aceitar**. Se o botão estiver inativo, você precisará adicionar mais linhas vermelhas primeiro.
9. Clique em **Sair**.

Definir saídas

Para fazer com que o AXIS Perimeter Defender emita alarmes quando ele detecta uma invasão, você precisa definir regras para ele. O sistema pode enviar alarmes para, por exemplo, um VMS.

O AXIS Perimeter Defender pode enviar alarmes por meio de diferentes interfaces.

Do próprio aplicativo:

- Notificações de alarme de texto simples ou XML sobre TCP/IP
- Streams de metadados XML sobre HTTP multipartes

Do dispositivo:

- Notificações de texto livre básico para alarmes sobre TCP/IP
- Saídas elétricas (contatos secos ou molhados)
- Notificações via email
- Upload para FTP de imagens de alarme

Você pode ativar várias interfaces ao mesmo tempo.

Introdução

Para obter informações mais detalhadas, consulte *Saídas na página 33*.

Para definir regras para o envio de alarmes a partir do dispositivo:

1. Vá para **Outputs (Saídas)** e clique em **Configure (Configurar)**. A página da Web do dispositivo será aberta em um navegador da Web.
2. Crie uma nova regra de ação.
3. Na lista de acionadores, selecione **Aplicativos**, **AXISPerimeterDefender** e o cenário para acionar a ação.

Observação

Para acionar a mesma ação para todos os cenários definidos, selecione **ALL_SCENARIOS**.

4. Na lista de ações, selecione a ação a ser executada quando a condição for atendida.
5. Clique em **OK**.

Para obter informações mais detalhadas sobre como criar regras de ação, consulte o manual do usuário do dispositivo.

Configuração avançada

Saídas

Notificações de alarme XML/texto

Essa interface permite que um destinatário TCP/IP receba um XML mais completo e descritivo ou uma mensagem de texto para cada alarme. Com relação à interface de texto livre, a interface XML/texto oferece as seguintes vantagens:

- Uma notificação é enviada no início do alarme, no final do alarme e a cada 10 segundos durante o alarme.
- Marca de data e hora: as notificações de início e fim de alarme contêm uma marca de data/hora que é sincronizada com o relógio da câmera e fornece a hora exata dos eventos.
- Tipo de alarme: O AXIS Perimeter Defender oferece suporte a vários tipos de alarmes, consulte *Definir cenários na página 27*. As notificações de XML/texto contêm as informações do tipo de alarme acionado. Preste atenção: o cenário de "cruzamento de zona" tem o tipo "passagem" e o cenário de vadiagem tem o tipo "presença"
- Zonas envolvidas na geração de alarmes; onde cada cenário do AXIS Perimeter Defender está associado a uma ou mais zonas, as notificações de XML/texto incluem qual zona está associada ao alarme (ou seja, para um alarme de invasão, a zona de invasão na qual uma pessoa foi detectada)

Com relação à interface de texto livre, a interface XML/texto fornece as seguintes limitações:

- O texto da mensagem é fixo e não há campos de texto livre.
- Cada câmera oferece suporte a apenas um destinatário por vez.

O destinatário das notificações de XML/texto recebe quatro tipos de mensagens:

- O AXIS Perimeter Defender envia uma mensagem CONNECTION_TEST quando a notificação XML é configurada para verificar se a comunicação com o destinatário funciona conforme o esperado.
- Quando o AXIS Perimeter Defender aciona um alarme, ele envia uma mensagem ALARM_START.
- Durante a duração do alarme, o AXIS Perimeter Defender envia várias mensagens de "alarme em andamento", uma a cada 10 segundos. Todas essas mensagens têm a mesma marca GUID, idêntica da mensagem ALARM_START e mensagens ALARM_STOP relacionadas ao mesmo alarme
- No final do alarme, o AXIS Perimeter Defender envia um alarme ALARM_STOP.

Para obter explicações sobre o formato dessas mensagens, em formato XML e texto, consulte *Exemplos de formato XML e texto na página 33*.

Exemplos de formato XML e texto

O formato XML é o formato padrão para as notificações TCP/IP. No entanto, se o tamanho da notificação for importante, um formato de texto, gerando mensagens mais curtas, poderá ser usado. Para selecionar o formato do texto, a opção **Não usar XML para parâmetro de alarmes** deve ser selecionada na página de configuração do AXIS Perimeter Defender.

Exemplo

Uma mensagem CONNECTION_TEST no formato XML é semelhante a este exemplo:

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="1"
         TYPE="CONNECTION_TEST"
         SENDER_IP="192.168.1.40"
         SENDER_PORT="0">
```

```
  <REFERENTIAL>45</REFERENTIAL>
</KEENEO_MESSAGE>
```

- VERSION é a versão interna da sintaxe e do protocolo XML.
- ID é uma identidade numérica para a mensagem. Os IDs não são garantidos como exclusivos nem progressivos.
- TYPE é o tipo da mensagem, aqui "CONNECTION_TEST". O tipo de mensagem determina as submarcas da mensagem (nenhum para mensagens do tipo "CONNECTION_TEST").
- SENDER_IP é o endereço IP da câmera AXIS enviando a notificação XML.
- SENDER_PORT é sempre zero; a câmera não pode receber mensagens.
- REFERENTIAL é o ID numérico associado à câmera

Se o formato de texto for escolhido, as mensagens de notificação conterão 7 campos cada, separados pelo caractere "pipe" "|". Se um campo não puder ser especificado (por exemplo, ele não fizer sentido para esse tipo de mensagem), ele será substituído por "-".

Os sete campos são, do primeiro ao último (entre parênteses, o campo XML correspondente quando o formato é XML):

1. O ID numérico da mensagem (atributo "ID" do cabeçalho XML "KEENEO_MESSAGE").
2. O endereço IPv4 da câmera (atributo "SENDER_IP" do cabeçalho XML "KEENEO_MESSAGE").
3. O número referencial associado à instância do AXIS Perimeter Defender (marca "REFERENTIAL").
4. O tipo de mensagem (atributo "TYPE" do cabeçalho XML "KEENEO_MESSAGE").
5. O tipo de alarme (marca "TYPE").
6. O nome do cenário que acionou o alarme (marca "SCENARIO_NAME").
7. A marca de data/hora (marca "TIMESTAMP"). O formato de marca de data/hora é o mesmo para o formato XML.

A mensagem CONNECTION_TEST anterior no formato TEXT é:

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

Exemplo

Uma mensagem ALARM_START no formato XML é semelhante a este exemplo:

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

- O cabeçalho da mensagem é igual à mensagem "CONNECTION_TEST".
- O tipo de mensagem é "ALARM_START" e tem um conjunto de submarcas.
  - REFERENTIAL é o ID numérico associado à câmera.

- TYPE é o tipo de alarme acionado pelo AXIS Perimeter Defender, "INTRUSION" neste exemplo. Outros tipos possíveis são "PRESENCE", "PASSAGE" e "CONDITIONAL".
- SCENARIO_NAME é o nome do cenário que disparou o alarme, conforme definido na interface de configuração. Consulte *Configurar o cenário de invasão/vadiagem na página 28*
- EXTRA_DATA carrega o nome da zona (ou lista de nomes de zona) envolvidos com o alarme, como a zona de invasão.
- TIMESTAMP é a data e hora do início do alarme, no formato AAAA-MM-DDTHH: mm: SS. zzz, onde:

  – AAAA é o ano com 4 dígitos, como 2014.

  – MM é o número do mês com 2 dígitos, como 01 para janeiro.

  – DD é o número do dia com 2 dígitos, como 03 para o 3º.

  – 'T' é uma letra fixa

  – HH é a hora em formato de 24 horas, de 00 a 23

  – mm são os minutos com 2 dígitos, de 00 a 59

  – ss são os segundos com 2 dígitos, de 00 a 59

  – zzz são os milissegundos com 3 dígitos, de 000 a 999.

  O AXIS Perimeter Defender usa a data e a hora internas da câmera para gerar a marca de data e hora do alarme. Portanto, é importante sincronizar a câmera com algum tipo de relógio externo.
- GUID é um identificador exclusivo e constante para todas as mensagens relacionadas ao mesmo alarme (portanto, ALARM_START, ALARM_IN_PROGRESS e ALARM_STOP)

Este é o equivalente, no formato de texto, da mensagem ALARM_START:

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

Exemplo

Uma mensagem ALARM_IN_PROGRESS no formato XML é semelhante a este exemplo:

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

- O cabeçalho da mensagem é igual à mensagem "CONNECTION_TEST" e "ALARM_START".
- O tipo de mensagem é "ALARM_IN_PROGRESS" e tem um conjunto de submarcas.
  - REFERENTIAL é o ID numérico associado à câmera.
  - TYPE é o tipo de alarme acionado pelo AXIS Perimeter Defender, o mesmo do ALARM_START correspondente.
  - SCENARIO_NAME é o nome do cenário que acionou o alarme, o mesmo do ALARM_START correspondente.
  - O GUID é o mesmo do ALARM_START correspondente.

A mensagem ALARM_IN_PROGRESS correspondente no formato TEXT:

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

Exemplo

Uma mensagem ALARM_STOP no formato XML é semelhante a este exemplo:

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

- O cabeçalho da mensagem é igual às mensagens anteriores.
- O tipo de mensagem é "ALARM_STOP" e tem o mesmo conjunto de subtipos da mensagem ALARM_START.

A mensagem ALARM_IN_PROGRESS correspondente no formato TEXT:

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

A conexão TCP/IP é sempre fechada após cada mensagem. Portanto, o destinatário deverá manter o soquete de escuta sempre aberto para conseguir receber mais notificações.

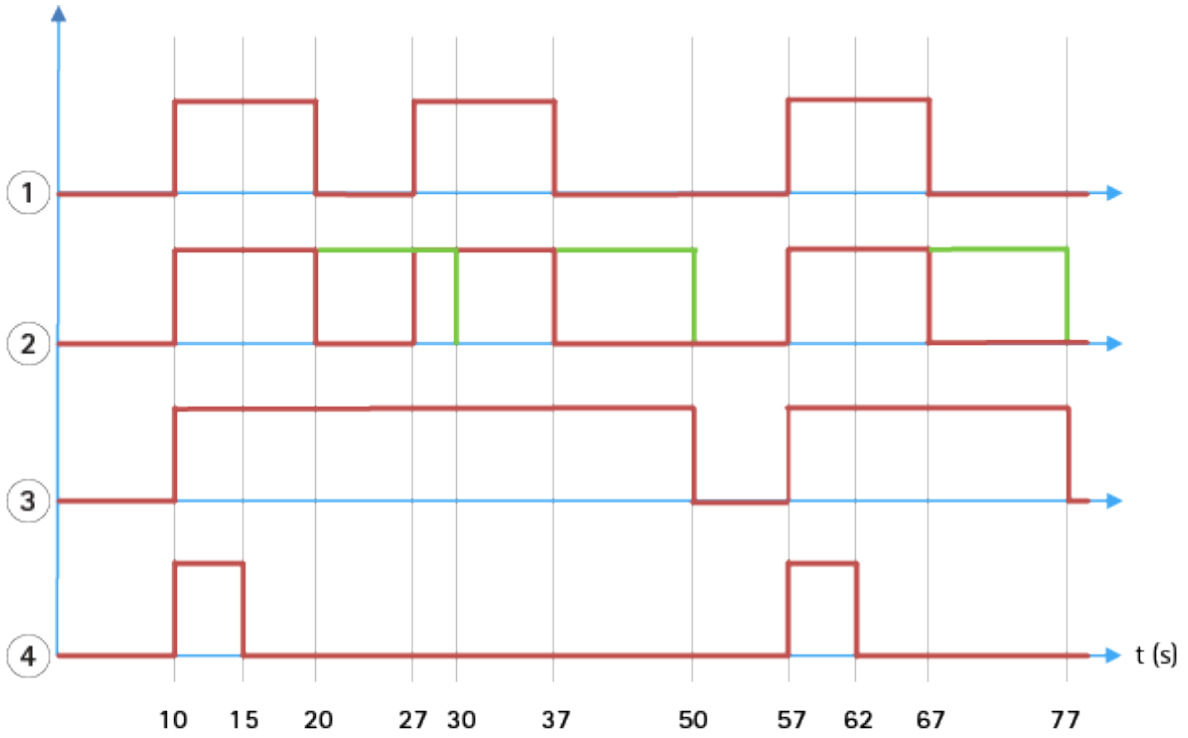
Erros de comunicação

Se o destinatário remoto de notificações XML não estiver acessível, por exemplo, devido a uma desconexão de rede, o AXIS Perimeter Defender iniciará o buffer de alarmes não entregues interna e periodicamente (pelo menos 10 segundos) e tentará entregá-los novamente. Após um número consecutivo de falhas na entrega de novas mensagens (falhas ao tentar entregar novamente uma mensagem do buffer não conta para isso), o AXIS Perimeter Defender declara o destinatário como "permanentemente offline" e para enviando notificações XML para o destinatário. O número de falhas consecutivas é fixado em 20, aproximadamente correspondendo a 4 ou 5 alarmes de invasão com uma duração média de 40 segundos cada. O AXIS Perimeter Defender iniciará novamente o envio de notificações para o mesmo destinatário se um dos seguintes eventos ocorrer:

- O AXIS Perimeter Defender for reiniciado.
- O mesmo valor do parâmetro "URL de streaming de alarme" for salvo novamente.

Tempo pós-alarme

O AXIS Perimeter Defender possui o conceito de "tempo pós-alarme". Isso é definido como o intervalo de tempo depois que um alarme para, durante o qual, se outro alarme for acionado, ambos os alarmes serão mesclados em um único.



1 *Três alarmes acionados pelo AXIS Perimeter Defender nos tempos 10, 27 e 57. Cada alarme tem uma duração de 10 segundos, ou seja, um intruso levou 10 segundos para atravessar a zona de invasão.*
2 *Um tempo pós-alarme de 10 segundos é adicionado.*
3 *Alarmes usando notificações XML e metadados XML.*
4 *Alarmes usando notificações por email, upload de imagens para FTP, contatos elétricos e notificações TCP/IP básicas.*

(2) Observe como um tempo pós-alarme de 10 segundos (em verde) aumenta a duração de cada alarme, levando assim à fusão (mesclagem) de dois alarmes separados por 10 segundos ou menos.

(3) Você pode ver o número de alarme resultante e a duração como gerados pelo AXIS Perimeter Defender através de notificações XML e metadados XML. O tempo pós-alarme pode ser usado para obter menos alarmes mais longos em vez de vários, mais curtos e consecutivos.

(4) Para notificações por email, upload de imagens para FTP, contatos elétricos e notificações TCP/IP básicas, o resultado do uso de um tempo pós-alarme de 10 segundos é diferente. Essas notificações consideram somente o início do alarme, e negligenciam a parada do alarme. Assim, não há nenhuma noção de "duração do alarme" quando você usa essas notificações e, consequentemente, o tempo pós-alarme não altera a duração da notificação propriamente dita. Ele sempre é corrigido para o valor escolhido pelo usuário ao configurar a notificação. Assim, quando os alarmes consecutivos são fundidos em um por causa do tempo pós-alarme, somente uma notificação é emitida. Você pode ver que o AXIS Perimeter Defender mescla os dois primeiros alarmes, enviando assim apenas uma notificação. Portanto, notificações por email, upload de imagens para FTP, contatos elétricos e notificações TCP/IP básicas notificam apenas para dois deles. O gráfico mostra uma duração fixa de 5 segundos para essas notificações.

Como configurar o tempo pós-alarme

1. Abra o AXIS Perimeter Defender Setup.
2. Vá para **Saídas** .
3. Altere a configuração **Tempo pós-alarme**. O valor padrão é 7 segundos.
4. Clique em **Atribuir**.

Metadados

Sobreposição de metadados integrada

A sobreposição de metadados integrada é um recurso que pode desenhar detecções de análise para streams ao vivo selecionados diretamente na câmera. As detecções são sobreposições gráficas na forma de caixas delimitadoras e linhas de trajetória. Os streams são selecionados com base em suas resoluções e, se o dispositivo tiver suporte a áreas de exibição, em uma área de exibição. Os metadados integrados são exibidos na visualização ao vivo e durante a reprodução de material gravado.

Sobreposições de metadados integradas em streams selecionados

Por exemplo, você pode configurar o aplicativo para adicionar sobreposições em todos os streams com resolução 640x480. Nesse caso, somente os streams com essa resolução terão a sobreposição e os outros ficarão sem modificações.

Sobreposições de metadados integradas em áreas de exibição selecionadas

Quando houver suporte, você também poderá indicar uma área de exibição junto com a resolução. Por exemplo, você pode optar por ter sobreposições em streams obtidos da área de exibição número 3 na resolução 1280x720. Nesse caso, somente os streams que correspondam a essa configuração terão as sobreposições, e outros streams permanecerão não modificados incluindo aqueles buscados da área de exibição 3, mas em uma resolução diferente, e aqueles buscados em 1280x720, mas não da área de exibição 3.

Adicionar metadados integrados ao stream de vídeo

Observação

Esta função só está disponível em dispositivos com firmware 7.30 ou posterior.

Este exemplo explica como ativar sobreposições de metadados integrados em todos os streams de vídeo com resolução 640x480. Os streams de vídeo com qualquer outra resolução permanecem inalterados.

1. Selecione a câmera no painel com visualizações ao vivo.
2. Vá para **Saídas > Sobreposição de metadados integrada**.
3. Selecione **Ativada**.
4. Na lista suspensa, selecione a resolução 640x480.
5. Clique em **Aplicar**.
6. Certifique-se de que os metadados sejam exibidos na visualização ao vivo para essa resolução.

Integração do VMS

O AXIS Perimeter Defender integra-se perfeitamente aos seguintes sistemas de gerenciamento de vídeo (VMS):

- Security Center da Genetec™
- XProtect® da Milestone

Para obter informações sobre as versões do VMS com suporte, consulte *axis.com/products/axis-perimeter-defender/support-and-documentation*

Os alarmes acionados pelo AXIS Perimeter Defender são automaticamente convertidos em eventos no VMS que, por sua vez, pode acionar um vasto conjunto de ações e aproveitar todo o potencial do VMS. Simultaneamente, os metadados ao vivo gerados pelo AXIS Perimeter Defender são enviados para o VMS para visualização ao vivo e gravação. Portanto, os metadados também estarão disponíveis ao reproduzir as sequências de vídeo gravadas no modo de reprodução.

Um sistema automatizado de detecção de invasão foi projetado para acionar alarmes e fornecer dados que ajudam a informar a intervenção de segurança. Isso pode incluir fornecer um prompt para um dispositivo móvel ou exibir o evento de alarme dentro de uma VMS talvez com o assunto que criou o evento de alarme realçado na tela.

Integração de eventos padrão

O AXIS Perimeter Defender aproveita e estende as interfaces e recursos nativos do ACAP para o envio de alarmes e informações complementares para dispositivos externos ou VMS. A saída de eventos pelo AXIS Perimeter Defender pode ser traduzida em mensagens para as VMs, conectando as regras de ação a elas.

Os seguintes canais de alarme da câmara para as VMS estão disponíveis:

- Notificações de texto livre básicas para alarmes (TCP/IP)
- Saídas elétricas (contatos secos ou molhados)
- Notificações via email
- Upload para FTP de imagens de alarme

Essas integrações podem ser configuradas na câmera. Consulte *Tempo pós-alarme na página 36*.

Pontes VMS

Para os seguintes sistemas de gerenciamento de vídeo, fornecemos módulos de integração pré-desenvolvidos, denominados "pontes":

- Milestone XProtect® 2014 e 2016 Corporate/Expert/Enterprise/Professional/Express. As edições Enterprise/Professional/Express não oferecem suporte a metadados (sem visualização ao vivo ou reprodução de metadados)
- Genetec™ Service Center 5,3 e 5,4 Pro/Enterprise/SV32/SV16

As pontes fornecem duas integrações:

- Criação de eventos de alarme personalizados no VMS, combinando a saída de eventos pelo AXIS Perimeter Defender.
- Exibição de sobreposições de alarme, ou caixas delimitadoras, em cima de material de vídeo ao vivo e gravado (exceto para as edições Milestone XProtect® Enterprise/Professional/Express).

Você precisa baixar e instalar as pontes VMS como aplicativos separados. Para obter mais informações sobre como instalar e configurar essas pontes, consulte o manual do usuário para a ponte específica.

Criação de uma regra no AXIS Camera Station

Esta seção explica como integrar o AXIS Perimeter Defender com o sistema de eventos do Axis Camera Station. Você aprenderá a:

- Configurar uma regra AXIS Camera Station a ser acionada em caso de invasão.
- Verificar se a configuração foi feita corretamente.

1. Configurar e calibrar o AXIS Perimeter Defender no software de instalação do AXIS Perimeter Defender. Para obter ajuda com a instalação e a calibração do AXIS Perimeter Defender, consulte o manual do usuário do AXIS Perimeter Defender ou a *página do produto*.
2. Adicionar a câmera ao AXIS Camera Station com o assistente **Add Camera (Adicionar câmera)**.
3. Configurar um acionador de evento de dispositivo:
    3.1 Vá para **Configuration (Configuração)** > **Recording & Events (Gravação e eventos)** e abra a guia **Advanced rules (Regras avançadas)**.
    3.2 Crie uma nova regra e selecione o acionador **Device Event (Evento do dispositivo)**.
    3.3 Selecione a câmera em que o AXIS Perimeter Defender está instalado.
    3.4 Na lista **Event (Eventos)**, selecione **AXISPerimeterDefender**.
    3.5 Na lista **Feature (Recurso)**, selecione o nome da invasão configurado (no caso "Intrusion-1"). Se você deseja acionar a regra para todos os cenários configurados, selecione **ALL_SCENARIOS**.

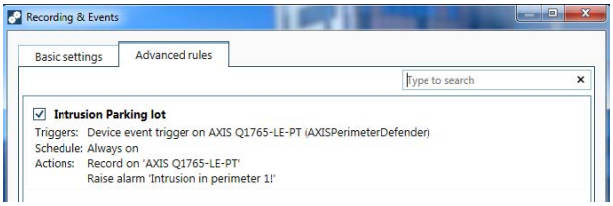
3.6 Selecione **Yes (Sim)** se o acionador precisar ser ativado quando houver uma invasão. Quando uma invasão é detectada, a janela de atividade mostra uma alteração de status que ajuda a verificar se a configuração está correta.

3.7 Clique em **OK** e **Next (Avançar)** para configurar as ações.

3.8 Na caixa de diálogo **Add Action (Adicionar ação)**, você pode adicionar uma ou várias ações para a regra.

Neste exemplo, podemos adicionar uma ação de gravação e uma ação de alarme.

3.9 Clique em **Finish (Concluir)**.



O exemplo mostra uma regra do AXIS Camera Station que aciona duas ações quando uma invasão ocorre.

4. Teste se a configuração está funcionando conforme o esperado simulando uma invasão. Por exemplo, entrando fisicamente na área monitorada.

Solução de problemas

Para que todas as funcionalidades funcionem como o esperado, é obrigatório configurar os seguintes parâmetros do Axis:

- Rede/TCP-IP/Básico/Roteador padrão
- Rede/TCP-IP/Avançado/Nome de domínio
- Rede/TCP-IP/Servidor DNS primário
- Rede/TCP-IP/Servidor DNS secundário
- Rede/TCP-IP/Endereço do servidor NTP
- Rede/TCP-IP/SMTP (email)
- Opções do sistema/Data & hora/Fuso horário
- Opções do sistema/Data e hora/Sincronizar com o servidor NTP

Atualizar para a versão mais recente

Para aproveitar as melhorias mais recentes sem precisar recalibrar e redefinir cenários, recomendamos que você atualize para a versão mais recente do AXIS Perimeter Defender.

1. Baixe e instale a versão mais recente do AXIS Perimeter Defender.
2. Clique em **Instalar**. O AXIS Perimeter Defender Setup executa automaticamente as etapas necessárias para concluir a instalação:
   - Faça backup da calibração, cenários, parâmetros e licença existentes.
   - Instale a nova versão.
   - Restaure a licença.
   - Restaure a calibração e os cenários.
   - Restaure os parâmetros.
   - Se um aplicativo estava sendo executado, ele será reiniciado.

Atualizar firmware da câmera

Observação

Antes de atualizar o firmware da câmera, salve todas as configurações do AXIS Perimeter Defender. A Atualização do firmware remove o aplicativo e suas configurações da câmera. Se as configurações forem salvas, elas poderão ser restauradas usando o AXIS Perimeter Defender Setup.

1. Use o AXIS Perimeter Defender Setup para salvar a configuração do site.
2. Atualize o firmware da câmera. Para obter instruções, consulte o Manual do Usuário da câmera.
3. Inicie o AXIS Perimeter Defender Setup.
4. Use a opção carregar site para carregar automaticamente a configuração do site salvo para cada câmera atualizada.

Solução de problemas

Solução de problemas de instalação

Problema	Razão possível	Solução
Há uma mensagem do Windows® informando que é impossível instalar o software.	O sistema operacional no laptop ou PC não é compatível.	Verifique as correspondências do sistema operacional Windows® especificadas nos requisitos.
Há uma mensagem do Windows® informando que a instalação estava incorreta.	O Assistente de Compatibilidade do Windows® detectou um possível problema na instalação.	Confirme se a instalação está correta de qualquer maneira e prossiga.
A instalação falha durante a instalação do XVID.	A instalação do XVID falha devido à instalação parcial antiga do XVID presente no computador.	Exclua a pasta XVID em C:\Program Files (x86) e tente instalar novamente.
O pacote do instalador trava repentinamente após a exibição do EULA. Há uma mensagem de erro do Windows® informando que o aplicativo foi encerrado de uma maneira incomum. É impossível fechar o instalador.	Um problema conhecido nos instaladores leva a uma falha do aplicativo sob algumas circunstâncias.	Abra o gerenciador de tarefas e encerre todos os processos "msiexec. exe". Em seguida, encerre o processo de instalação e reinicie o instalador.

Solução de problemas de configuração

Problema	Razão possível	Solução
Problemas ao abrir o AXIS Perimeter Defender.	Você não tem direitos de usuário do Windows® suficientes.	Certifique-se de ter direitos de administrador.
A funcionalidade de pesquisa não encontra minhas câmeras.	Firewall	Firewalls e software antivírus podem, ocasionalmente, bloquear a descoberta da câmera. Se necessário, configure o firewall para permitir o tráfego de rede e do AXIS Perimeter Defender. Se isso não resolver o problema, configure o firewall para permitir o acesso às seguintes portas: porta UDP 5353 e porta TCP 80.
	Problemas com o endereço IP	Qualquer dispositivo em uma rede deve ter um endereço IP exclusivo para poder se comunicar com outros dispositivos. Ao usar o AXIS Perimeter Defender, é recomendável usar endereços IP fixos para as câmeras. Certifique-se de que cada dispositivo IP na rede tenha o seu próprio endereço IP e não reutilize um endereço IP já utilizado.
	A câmera não está disponível no computador do usuário.	Em um navegador, vá para o endereço IP da câmera para confirmar se ele está disponível ou não. Se você não puder alcançá-lo, a câmera não foi corretamente instalada na rede ou o computador não tem acesso à câmera.

Solução de problemas

Problema	Razão possível	Solução
Não é possível adicionar uma câmera.	Os parâmetros de conexão da câmera, por exemplo endereço IP, senha ou porta HTTP, estão incorretos.	Verifique se os parâmetros inseridos estão corretos e repita.
	A câmara não pode ser vista a partir do computador do usuário.	Em um navegador, vá para o endereço IP da câmera para confirmar se ele está disponível ou não. Se você não puder acessá-lo, a câmera não foi corretamente instalada na rede ou o computador não tem acesso à rede na qual a câmera está ligada.
Perda de streams de vídeo no AXIS Perimeter Defender Setup.	A fonte de vídeo não está mais disponível.	A fonte de vídeo foi interrompida e não foi atualizada no visor.
	Use um navegador para verificar se a câmera está disponível.	Clique no bloco onde o stream deve estar, redimensione a interface e o stream deverá voltar.
A calibração automática não funciona ou produz resultados ruins.	Os pré-requisitos não são atendidos.	Certifique-se de que os requisitos de montagem sejam atendidos. Consulte *Montagem da câmera na página 13*.
	A câmera tem um rolo.	Não é possível calibrar a câmera com um rolo.
	Conexão lenta com a câmera não configurada como remota.	Conecte a câmera como dispositivo remoto para reduzir os requisitos de largura de banda.
	Há outros objetos em movimento na cena usada para a calibração automática como carros, árvores ou outras pessoas.	Repita a calibração automática ou calibre o dispositivo manualmente.
	O campo de visão está desordenado fazendo com que a pessoa que está andando na frente da câmera fique parcialmente escondida durante muito tempo.	Calibre o dispositivo manualmente.
	O campo de visão é pequeno, por exemplo, em entradas.	Calibre o dispositivo manualmente.
	O vídeo de captura não foi gravado corretamente devido a espaço em disco insuficiente.	Verifique se há espaço em disco adequado e se o aplicativo tem permissão para salvar o vídeo no computador onde a interface do AXIS Perimeter Defender está em execução.

Solução de problemas de operação

Problema	Razão possível	Solução
O aplicativo não é executado mesmo com uma boa configuração.	O firmware da câmara não está atualizado.	Certifique-se de que você tenha o firmware mais recente para a câmera.

A sobreposição não é exibida no AXIS Perimeter Defender Setup mesmo com a análise em execução.	O aplicativo é bloqueado após uma operação de início ou parada ou uma atualização do pacote AXIS Perimeter Defender.	Reinicie a câmera.
	Um firewall está bloqueando a conexão com a porta de escuta de metadados da câmera.	Configure o firewall para permitir que a interface de configuração conecte à porta de escuta de metadados da câmera.
	Um programa antivírus está bloqueando a recepção da sobreposição.	Configure o antivírus para permitir que a sobreposição seja recebida.
Nenhum alarme é acionado na configuração do AXIS Perimeter Defender no computador de configuração, mesmo que a análise esteja em execução e a sobreposição esteja visível.	Embora o alvo esteja na cena, ele não está correspondendo a um cenário condicional, por exemplo, ele não se move de uma zona para outra no cenário de cruzamento de zona.	Certifique-se de que o cenário esteja especificado corretamente, incluindo condições.
	Detecção ruim.	Certifique-se de que os requisitos de montagem sejam atendidos. Consulte *Montagem da câmera na página 13*. Certifique-se também de que a calibração seja suficientemente precisa e que a sensibilidade seja suficientemente alta.

Solução de problemas de desempenho

Problema	Razão possível	Solução
OSD e análise continua a ligar e desligar.	A carga da CPU na câmera é muito alta.	Possíveis soluções: • Certifique-se de que o stream da câmera não seja visualizado em locais desnecessários, pois cada visualização do stream da câmera aumenta a carga da CPU. • Se a gravação na detecção de movimento integrada estiver ativada, tente diminuir a qualidade da gravação para liberar a CPU. • Desative a gravação na detecção de movimento integrada e certifique-se de que a detecção de movimento integrada esteja desativada.
Um alvo entra na zona estéril e faz com que vários alertas sejam gerados.	A duração do tempo pós-alarme é demasiado curta.	Ajuste o tempo pós-alarme. Vá para AXIS Perimeter Defender Setup > **Saídas**.

Solução de problemas

Problema	Razão possível	Solução
Um alvo potencial entra na zona estéril, mas não aciona uma detecção de alerta-perdida.	O contraste do objeto em relação ao plano de fundo na cena é muito baixo.	Certifique-se de que os requisitos de montagem sejam atendidos. Consulte *Montagem da câmera na página 13*.
	Não há iluminação inadequada na cena ou o desempenho da câmera com pouca luz é insuficiente.	Certifique-se de que os requisitos de montagem sejam atendidos. Consulte *Montagem da câmera na página 13*.
	O AXIS Perimeter Defender está com uma configuração de sensibilidade muito baixa.	Aumente a sensibilidade nos parâmetros de cenário global.
	A câmera se moveu tornando a calibração incorreta.	Refaça a calibração.
	A calibração não é suficientemente precisa.	Verifique a calibração da câmera. Vá para o AXIS Perimeter Defender Setup.
	Embora o alvo esteja na cena, ele não está correspondendo a um cenário condicional, por exemplo, ele não se move de uma zona para outra no cenário de cruzamento de zona.	Certifique-se de que o cenário esteja especificado corretamente, incluindo condições.
O alvo foi detectado, mas está classificado incorretamente (pessoa como veículo ou veículo como pessoa).	A altura, posicionamento ou orientação da câmara estão incorretos.	Certifique-se de que os requisitos de montagem sejam atendidos. Consulte *Montagem da câmera na página 13*.
	A câmera está muito longe da zona.	Certifique-se de que os requisitos de montagem sejam atendidos. Consulte *Montagem da câmera na página 13*.
	A calibração não é suficientemente precisa.	Verifique a calibração da câmera. Vá para o AXIS Perimeter Defender Setup.
O AXIS Perimeter Defender gera um alarme quando não há uma invasão na zona estéril.	A sensibilidade da análise é muito alta.	Diminua a sensibilidade. Vá para o AXIS Perimeter Defender Setup.
	A calibração não é suficientemente precisa.	Verifique a calibração da câmera. Vá para o AXIS Perimeter Defender Setup.
	A câmera se moveu tornando a calibração incorreta.	Refaça a calibração.
	Altura, posicionamento ou orientação da câmera incorretos.	Certifique-se de que os requisitos de montagem sejam atendidos. Consulte *Montagem da câmera na página 13*.
	A câmera está se movendo, por exemplo, balançando ou vibrando.	Instale a câmera em um ambiente mais estável.
	Vegetação ou outros objetos em movimento, por exemplo, bandeiras, perto da câmera.	Remova os itens ofensivos do campo de visão da câmera. Os objetos que estão constantemente na cena, mas não perto da câmera, são ignorados pelo AXIS Perimeter Defender.
	Os insetos estão rastejando sobre ou perto da lente da câmera.	Impedir que insetos invadam ou fiquem perto da lente da câmera.

Este manual destina-se a administradores e usuários do AXIS Perimeter Defender. Ele inclui instruções para usar e gerenciar o produto em sua rede. Experiência anterior em networking de uso ao utilizar este produto.

Reconhecimento de marcas comerciais

Manual do Usuário
AXIS Perimeter Defender

Ver. M15.5
Data: Agosto 2021
Nº da peça T10068952