

AXIS P3265-LVE-3 License Plate Verifier Kit

Índice

Início.....	4
Encontre o dispositivo na rede.....	4
Suporte a navegadores.....	4
Abra a interface web do dispositivo.....	4
Criar uma conta de administrador.....	4
Senhas seguras.....	5
Certifique-se de que o software do dispositivo não foi violado.....	5
Visão geral da interface Web.....	5
Configuração básica.....	6
Recomendações de montagem da câmera.....	6
Assistente de configuração.....	8
Fluxo livre.....	8
Controle de acesso.....	9
Acesso às configurações do aplicativo.....	10
Ajuste a área de interesse.....	10
Selecionar região.....	11
Ajuste das configurações de captura de imagem.....	11
Configuração de armazenamento de eventos.....	11
Instalação.....	13
Modo de visualização.....	13
Configure seu dispositivo.....	14
Para usuários do AXIS Camera Station.....	14
Configurar o AXIS License Plate Verifier.....	14
Configurações básicas.....	14
Ajuste da imagem.....	14
Reduza o tempo de processamento de imagens com o modo de baixa latência.....	14
Seleção do modo de exposição.....	15
Compensação da distorção de barril.....	15
Verifique a resolução de pixels.....	15
Exibição e gravação de vídeo.....	16
Redução de largura de banda e armazenamento.....	16
Configurar o armazenamento de rede.....	16
Como gravar e assistir vídeo.....	17
Verifique se o firmware não foi manipulado com o vídeo.....	17
Configuração de regras de eventos.....	17
Gravar vídeo quando a câmera detectar uma placa de licença.....	17
Acionar uma notificação quando a lente da câmera for manipulada.....	18
Áudio.....	18
Adição de áudio à sua gravação.....	18
Adicione capacidade de áudio ao seu produto usando portcast.....	19
Gerenciar listas.....	20
Adicionar placa de licença detectada à lista.....	20
Adicionar descrições a placas de licença.....	20
Personalização de nomes de listas.....	21
Importação de números de placas de licença na lista de permissão.....	22
Compartilhamento de listas de placas de licença com outras câmeras.....	23
Agendar listas.....	24
Configurações adicionais.....	25
Configurar sobreposição de texto.....	25
Detecção de placas de licença em condições de pouca iluminação.....	25
Permitir menos caracteres nas placas de licença.....	25
Permitir somente correspondências exatas de placas de licença.....	25
Permitir o desvio de mais de um caractere ao comparar placas de licença.....	25

Fornecer acesso limitado aos operadores	26
Configuração de uma conexão segura	26
Fazer backup e restaurar configurações de aplicativos.....	26
Limpar todos os eventos.....	26
Usar portas virtuais para acionar ações.....	26
Cenário de entrada e saída de veículos	28
Abertura de uma barreira para veículos conhecidos usando um módulo de relé.....	28
Abertura de uma barreira para veículos conhecidos usando a E/S da câmera.....	29
Recebimento de notificação sobre um veículo não autorizado.....	30
Cenário de controle de acesso de veículos	31
Conexão a um controlador de porta	31
Conectar ao AXIS Secure Entry	33
Cenário de livre fluxo com medição de velocidade	35
Configurar o cenário.....	35
Pesquisar eventos específicos.....	37
Exportar e compartilhar resultados da pesquisa	37
Integração	38
Use perfis para enviar eventos por push para vários servidores	38
Informações sobre eventos push para software de outros fabricantes	38
Envio de imagens de placas de licença para um servidor.....	39
Integração direta com 2N.....	40
Integração ao Genetec Security Center.....	40
A interface Web.....	43
Saiba mais	44
Tecnologia de ponta a ponta	44
Pareamento de radar.....	44
Pareamento de alto-falante.....	44
Área de visualização.....	44
AXIS Image Health Analytics.....	44
Especificações	46
Visão geral do produto.....	46
Indicadores de LED	46
Slot de cartão SD	47
Botões	47
Botão de controle	47
Conectores	47
Conector de rede	47
Conector de áudio	47
Conector de E/S.....	47
Solução de problemas.....	49
Redefinição para as configurações padrão de fábrica	49
Opções do AXIS OS.....	49
Verificar a versão atual do AXIS OS	49
Atualizar o AXIS OS	50
Problemas técnicos e possíveis soluções.....	50
.....	53
Considerações sobre desempenho	54
Entre em contato com o suporte	54
Cibersegurança.....	55
Gerenciamento de vulnerabilidades.....	55
Notificações de segurança.....	55
Ciclo de vida seguro do produto.....	55

Início

Encontre o dispositivo na rede

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

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

Suporte a navegadores

O dispositivo pode ser usado com os seguintes navegadores:

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

✓: Recomendado

*: Compatível com limitações

Abra a interface web do dispositivo

1. Abra um navegador e digite o endereço IP ou o nome de host do dispositivo Axis.
Se você não souber o endereço IP, use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede.
2. Digite o nome de usuário e a senha. Se você acessar o dispositivo pela primeira vez, você deverá criar uma conta de administrador. Consulte *Criar uma conta de administrador, on page 4*.

Para obter descrições de todos os recursos e configurações na interface Web de dispositivos com AXIS OS, consulte *Ajuda da interface Web do AXIS OS*.

Criar uma conta de administrador

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

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

Importante

O dispositivo não possui conta padrão. Se você perder a senha da sua conta de administrador, deverá redefinir o dispositivo. Consulte *Redefinição para as configurações padrão de fábrica, on page 49*.

Senhas seguras

Importante

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

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

Para proteger seus dados, recomendamos enfaticamente que você:

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

Certifique-se de que o software do dispositivo não foi violado

Para certificar-se de que o dispositivo tenha o AXIS OS original ou para assumir o controle total do dispositivo após um ataque de segurança:

1. Restauração das configurações padrão de fábrica. Consulte *Redefinição para as configurações padrão de fábrica, on page 49*.
Após a redefinição, uma inicialização segura garantirá o estado do dispositivo.
2. Configure e instale o dispositivo.

Visão geral da interface Web

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



Interface Web de um dispositivo Axis

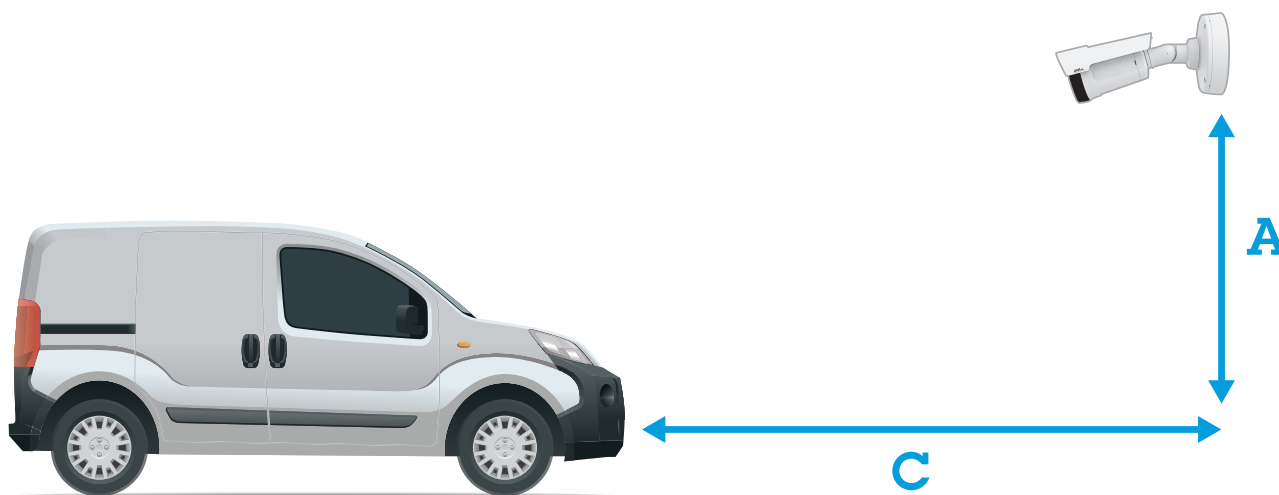
Configuração básica

Estas instruções de configuração são válidas para todos os cenários:

- 1.
- 2.
3. *Ajuste a área de interesse, on page 10*
4. *Selecionar região, on page 11*
5. *Configuração de armazenamento de eventos, on page 11*

Recomendações de montagem da câmera

- Ao selecionar o local de montagem, lembre-se de que luz do sol direta pode distorcer a imagem, por exemplo, durante o nascer e o pôr do sol.
- A altura de montagem de uma câmera em um cenário de **Access control (Controle de acesso)** deve ser metade da distância entre o veículo e a câmera.
- A altura de montagem de uma câmera em um cenário de **Free flow (Fluxo livre)** (reconhecimento de placas de licença em tráfego lento) deve ser inferior à metade da distância entre o veículo e a câmera.



Distância de captura de controle de acesso: 2-7 m (6,6-23 pés). Este exemplo baseia-se no AXIS P3265-LVE-3 License Plate Verifier Kit.

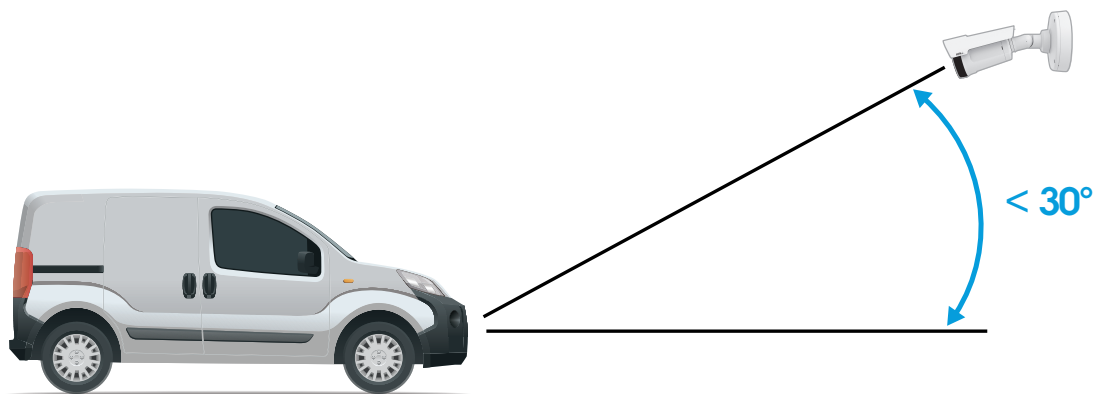
Distância de captura: (C)	Altura de montagem (A)
2,0 m (6,6 pés)	1,0 m (3,3 pés)
3,0 m (9,8 pés)	1,5 m (4,9 pés)
4,0 m (13 pés)	2,0 m (6,6 pés)
5,0 m (16 pés)	2,5 m (8,2 pés)
7,0 m (23 pés)	3,5 m (11 pés)

Distância de captura de fluxo livre: 7-20m (23-65 pés). Este exemplo baseia-se no AXIS P1465-LE-3 License Plate Verifier Kit.

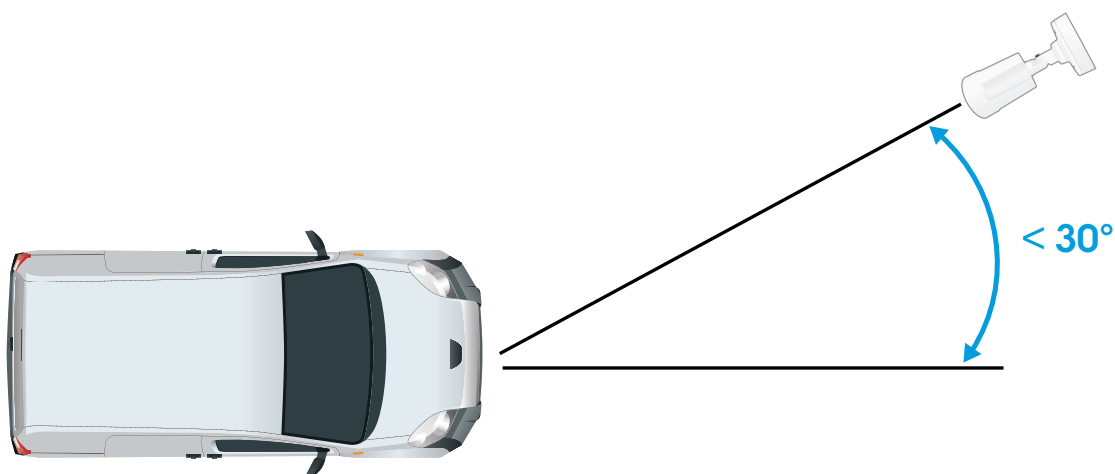
Distância de captura (C)	Altura de montagem (A)
7,0 m (23 pés)	3,0 m (9,8 pés)
10,0 m (33 pés)	4,0 m (13 pés)

15,0 m (49 pés)	6,0 m (19,5 pés)
20,0 m (65 pés)	10,0 m (33 pés)

- O ângulo de montagem da câmera não deve ser maior que 30° em nenhuma direção.

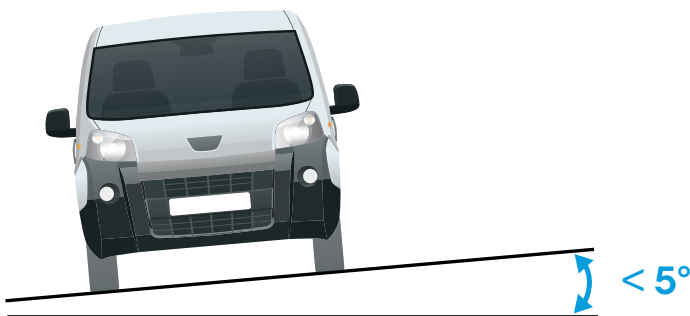


Ângulo de montagem a partir do lado.



Ângulo de montagem a partir de cima.

- A imagem da placa não deve estar inclinada mais do que 5° na horizontal. Se a imagem estiver inclinada em mais de 5°, recomendamos ajustar a câmera para que a placa seja exibida horizontalmente na transmissão ao vivo.



Ângulo de rolagem.

Assistente de configuração

Ao executar o aplicativo pela primeira vez, configure as opções **Free flow (Fluxo livre)** ou **Access control (Controle de acesso)** usando o assistente de configuração. Caso deseje alterar posteriormente, vá para **Settings > Maintenance (Configurações > Manutenção)** e, em **Setup assistant (Assistente de configuração)**, pressione **Start (Iniciar)**.

Fluxo livre

No modo de Fluxo livre, o aplicativo pode detectar e ler placas de licença em trânsito de baixa velocidade em vias de acesso mais largas, centros urbanos e em áreas fechadas, como campi, portos ou aeroportos. Isso permite a busca forense de LPR e eventos acionados de LPR em um VMS.

1. Selecione **Free flow (Fluxo livre)** e clique em **Next (Avançar)**.
2. Selecione a rotação de imagem correspondente à forma como a câmera está montada.
3. Selecione o número de áreas de interesse. Observe que uma área pode detectar placas em ambas as direções.
4. Selecione a região em que a câmera está localizada.
5. Selecione o tipo de captura.
 - **License plate crop (Recorte de placa de licença)** salva somente a placa de licença.
 - **Vehicle crop (Recorte de veículo)** salva o veículo capturado inteiro.
 - **Frame downsized 480x270 (Quadro reduzido para 480 x 270)** salva a imagem inteira e reduz a resolução para 480 x 270.
 - **Full frame (Quadro inteiro)** salva a imagem inteira na resolução máxima.
6. Arraste os pontos de ancoragem para ajustar a área de interesse. Consulte *Ajuste a área de interesse, on page 10*.
7. Ajuste a direção da área de interesse. Clique na seta e gire-a para definir a direção. A direção determina como o aplicativo registra veículos que entram ou saem da área.
8. Clique em **Next (Avançar)**.
9. Na lista suspensa **Protocol (Protocolo)**, selecione um dos seguintes protocolos:
 - TCP
 - HTTP POST
10. No campo **Server URL (URL do servidor)**, digite o endereço e a porta do servidor no seguinte formato:
127.0.0.1:8080

11. No campo **Device ID (ID do dispositivo)**, digite o nome do dispositivo ou deixe-o como está.
12. Em **Event types (Tipos de eventos)**, selecione uma ou mais das seguintes opções:
 - **New (Nova)** significa a primeira detecção de uma placa de licença.
 - **Update (Atualização)** é uma correção de um caractere em uma placa previamente detectada ou quando uma direção é detectada à medida que a placa se move e é rastreada ao longo da imagem.
 - **Lost (Perdido)** é o último evento rastreado da placa de licença antes dela sair da imagem. Ele também contém a direção da placa.
13. Para ativar o recurso, selecione **Send event data to server (Enviar dados de eventos para o servidor)**.
14. Para reduzir a largura de banda ao usar HTTP POST, você pode selecionar **Do not to send images through HTTP POST (Não enviar imagens via HTTP POST)**.
15. Clique em **Next (Próximo)**.
16. Se você já possui uma lista de placas registradas, escolha a opção de importar como uma **blocklist (lista de bloqueio)** ou **allowlist (lista de permissão)**.
17. Clique em **Finish (Concluir)**.

Controle de acesso

Use o assistente de configuração para configurar de forma rápida e fácil. Você pode selecionar **Skip (Pular)** para sair da guia a qualquer momento.

1. Selecione **Access control (Controle de acesso)** e clique em **Next (Avançar)**.
2. Selecione o tipo de controle de acesso que será usado:
 - **Internal I/O (E/S interna)** se você deseja manter o gerenciamento de listas na câmera. Consulte *Abertura de uma barreira para veículos conhecidos usando a E/S da câmera, on page 29*.
 - **Controller (Controlador)** se você deseja conectar um controlador de porta. Consulte .
 - **Relay (Relé)** se você deseja conectar a um módulo de relé. Consulte .
3. Na lista suspensa **Barrier mode (Modo de barreira)**, em **Open from lists (Abrir a partir de listas)**, selecione **Allowlist (Lista de permissão)**.
4. Na lista suspensa **Vehicle direction (Direção do veículo)** selecione **out (saindo)**.
5. Na lista suspensa **ROI (Região de interesse)**, selecione a área de interesse que gostaria de usar ou se deseja usar a área inteira.
6. Clique em **Next (Próximo)**.

Na página **Image settings (Configurações da imagem)**:

1. Selecione o número de áreas de interesse.
2. Selecione a região em que a câmera está localizada.
3. Selecione o tipo de captura. Consulte *Ajuste das configurações de captura de imagem, on page 11*.
4. Arraste os pontos de ancoragem para ajustar a área de interesse. Consulte *Ajuste a área de interesse, on page 10*.
5. Ajuste a direção da área de interesse. A direção determina como o aplicativo registra veículos que entram ou saem da área.
6. Clique em **Next (Avançar)**.

Na página **Event data (Dados de eventos)**:

Observação

Para obter configurações detalhadas, consulte: *Informações sobre eventos push para software de outros fabricantes, on page 38*.

1. Na lista suspensa **Protocol (Protocolo)**, selecione um dos seguintes protocolos:

- TCP
 - HTTP POST
2. No campo **Server URL (URL do servidor)**, digite o endereço e a porta do servidor no seguinte formato:
127.0.0.1:8080.
 3. No campo **Device ID (ID do dispositivo)**, digite o nome do dispositivo ou deixe-o como está.
 4. Em **Event types (Tipos de eventos)**, selecione uma ou mais das seguintes opções:
 - **New (Nova)** significa a primeira detecção de uma placa de licença.
 - **Update (Atualização)** é uma correção de um caractere em uma placa previamente detectada ou quando uma direção é detectada à medida que a placa se move e é rastreada ao longo da imagem.
 - **Lost (Perdido)** é o último evento rastreado da placa de licença antes dela sair da imagem. Ele também contém a direção da placa.
 5. Para ativar o recurso, selecione **Send event data to server (Enviar dados de eventos para o servidor)**.
 6. Para reduzir a largura de banda ao usar HTTP POST, você pode selecionar **Do not to send images through HTTP POST (Não enviar imagens via HTTP POST)**.
 7. Clique em **Next (Avançar)**.

Na página **Import list from a .csv file (Importar lista de um arquivo .csv)**:

1. Se você já possui uma lista de placas registradas, escolha a opção de importar como uma **blocklist (lista de bloqueio)** ou **allowlist (lista de permissão)**.
2. Clique em **Finish (Concluir)**.

Acesso às configurações do aplicativo

1. Na interface Web da câmera, vá para **Apps (Aplicativos)**, inicie o aplicativo e clique em **Open (Abrir)**.

Ajuste a área de interesse

A área de interesse é a área na visualização ao vivo onde o aplicativo procura placas de licença de veículos. Para obter o melhor desempenho, mantenha a área de interesse a menor possível. Para ajustar a área de interesse, faça o seguinte:

1. Vá para **Settings (Configurações)**.
2. Clique em **Image (Imagem)**.
3. Clique em 1:1 para aplicar zoom na área onde deseja monitorar o tráfego ou gerenciar o controle de acesso.
4. Para melhorar a verificação e as imagens capturadas, clique em **AF (Foco automático)**.
5. Para que a câmera foque automaticamente nos veículos, clique em **AF (Foco automático)**. Para definir o foco manualmente, ajuste-o com o controle deslizante.
6. Clique em **Area of interest (Área de interesse)** para exibi-la na área de exibição.
7. Para mover a área de interesse, clique em qualquer lugar da área para selecionar e arraste para onde as placas de licença forem mais visíveis. Certifique-se de que a região de interesse permaneça na posição depois de ter salvo as configurações.
8. Para ajustar a área de interesse, clique em qualquer lugar na área para selecionar e arraste os pontos de ancoragem destacados em azul.
 - Para redefinir a área de interesse, clique no botão de redefinição no canto inferior esquerdo, próximo ao ícone numérico.
 - Para adicionar pontos de ancoragem, clique em um dos pontos de ancoragem escuros. O ponto de ancoragem se tornará amarelo, mostrando que pode ser manipulado. Novos pontos escuros são adicionados automaticamente ao lado do ponto de ancoragem amarelo. O número máximo de pontos de ancoragem amarelos é oito.

9. Clique em qualquer lugar fora da área de interesse para salvar suas alterações.
10. Para obter uma resposta de direção correta no **Event log (Log de eventos)**, gire a seta para corresponder à direção de condução.
 - 10.1. Clique no ícone de seta.
 - 10.2. Selecione o ponto de ancoragem e gire a seta para que ela se alinhe à direção de condução.
 - 10.3. Clique fora da área de interesse para salvar as alterações.

Observe que uma área pode detectar placas em ambas as direções. O feedback de direção será exibido na coluna **Direction (Direção)**.

11. Para verificar se a sua área de interesse é suficientemente ampla para obter os melhores resultados, utilize o contador de pixels.
 - Para exibir o contador de pixels, clique no ícone da calculadora.
 - Para ajustar a área total do contador de pixels, arraste o canto inferior direito da área destacada em amarelo.
 - Para mover a área do contador de pixels, clique em qualquer lugar da área e arraste-a para onde desejar.
- Para adicionar uma segunda área de interesse, clique em + ao lado de 1.
- Se você estiver usando uma câmera independente, o aplicativo poderá definir as configurações recomendadas para o reconhecimento da placa de licença.
 1. Clique no ícone da varinha mágica e as configurações serão otimizadas para o reconhecimento de placas de licença.
 2. Clique no botão do menu ao lado da varinha mágica para visualizar os valores definidos.

Selecionar região

1. Vá para **Settings > Recognition (Configurações > Reconhecimento)**.
2. Na lista suspensa **Region (Região)**, selecione sua região.

Ajuste das configurações de captura de imagem

1. Vá para **Settings (Configurações) > Image (Imagem)**.
2. Para alterar a resolução das imagens capturadas, vá para **Image resolution (Resolução da imagem)**.
3. Para alterar a rotação da imagem capturada, vá para **Rotation (Rotação)**

Configuração de armazenamento de eventos

Um evento consiste em aspectos como imagem capturada, placa de licença, número da área de interesse, direção do veículo, no acesso e data e hora.

Este exemplo de caso de uso explica como armazenar eventos de números de placas de licença na lista de permissão por 30 dias.

Requisitos:

- Câmera fisicamente instalada e conectada à rede.
 - AXIS License Plate Verifier pronto e em execução na câmera.
 - Armazenamento interno ou em um cartão SD instalado na câmera.
1. Vá para **Settings > Storage (Configurações > Armazenamento)**.
 2. Em **Retain events (Reter eventos)**, selecione **Allowlisted (Na lista de permissão)**.
 3. Em **Retention period (Período de retenção)**, selecione **30 days (30 dias)**.
 4. Para alterar a forma como as imagens capturadas são salvas, vá para **Save full frame (Salvar quadro inteiro)**:

- **License plate crop (Recorte de placa de licença)** salva somente a placa de licença.
- **Vehicle crop (Recorte de veículo)** salva o veículo capturado inteiro.
- **Frame downsized 480x270 (Quadro reduzido para 480 x 270)** salva a imagem inteira e reduz a resolução para 480 x 270.
- **Full frame (Quadro inteiro)** salva a imagem inteira na resolução máxima.

Observação

Para detectar um cartão SD inserido quando o aplicativo está em execução, é necessário reiniciar o aplicativo. Se um cartão SD estiver instalado na câmera, o aplicativo escolherá automaticamente o cartão SD como armazenamento padrão.

O AXIS License Plate Verifier usa a memória interna das câmeras para economizar até 1.000 eventos usando os recortes da placa de licença como quadro. Se você usar quadros maiores, a quantidade de eventos que você poderá salvar poderá variar.

Um cartão SD pode salvar até 100.000 eventos usando qualquer tipo de quadro.

Instalação

Modo de visualização

O modo de visualização é ideal para os instaladores durante o ajuste fino da exibição da câmera durante a instalação. Não há necessidade de login para acessar a exibição da câmera no modo de visualização. Ele está disponível somente no estado padrão de fábrica por um tempo limitado ao alimentar o dispositivo.



Para assistir a este vídeo, vá para a versão Web deste documento.

Este vídeo demonstra como usar o modo de visualização.

Configure seu dispositivo

Para usuários do AXIS Camera Station

Configurar o AXIS License Plate Verifier

Quando um dispositivo é configurado com o AXIS License Plate Verifier, ele é considerado uma fonte de dados externa no sistema de gerenciamento de vídeo. Você pode conectar uma exibição à fonte de dados, procurar placas de licença capturadas pelo dispositivo e exibir a imagem relacionada.

Observação

- Isso requer o AXIS Camera Station 5.38 ou posterior.
 - O AXIS License Plate Verifier requer uma licença.
1. Baixe e instale o aplicativo no dispositivo.
 2. Configure o aplicativo. Consulte o *Manual do Usuário do AXIS License Plate Verifier*.
 3. Para uma instalação existente do AXIS Camera Station, renove o certificado do servidor que é usado para se comunicar com o cliente. Consulte *Renovação de certificado*.
 4. Ative a sincronização de hora para usar o servidor do AXIS Camera Station como servidor NTP. Consulte *Configurações do servidor*.
 5. Adicione o dispositivo ao AXIS Camera Station. Consulte *Adicionar dispositivos*.
 6. Quando o primeiro evento é recebido, uma fonte de dados é adicionada automaticamente em **Configuration > Devices > External data sources** (**Configuração > Dispositivos > Fontes de dados externas**).
 7. Conecte a fonte de dados a uma exibição. Consulte *Fontes de dados externas*.
 8. Pesquise as placas de licença capturadas pelo dispositivo. Consulte *Pesquisa de dados*.
 9. Clique em  para exportar os resultados da pesquisa para um arquivo .txt.

Configurações básicas

Defina a posição de montagem

1. Vá para **Video > Installation > Mounting position** (**Vídeo > Instalação > Posição de montagem**).
2. Clique em **Change** (**Alterar**).
3. Selecione uma posição de montagem e clique em **Save and restart** (**Salvar e reiniciar**).

Defina a frequência da linha de alimentação

1. Vá para **Video > Installation > Power line frequency** (**Vídeo > Instalação > Frequência da linha de alimentação**).
2. Selecione uma frequência de linha de alimentação e clique em **Save and restart** (**Salvar e reiniciar**).

Ajuste da imagem

Esta seção contém instruções sobre como configurar um dispositivo.

Reduza o tempo de processamento de imagens com o modo de baixa latência

Você pode otimizar o tempo de processamento de imagens da sua transmissão ao vivo ativando o modo de baixa latência. A latência na sua transmissão ao vivo é reduzida para um mínimo. Quando você usa um modo de latência baixa, a qualidade da imagem é menor do que o normal.

1. Vá para **System > Plain config** (**Sistema > Configuração simples**).
2. Selecione **ImageSource** na lista suspensa.

3. Vá para **ImageSource/I0/Sensor > Low latency mode (ImageSource/I0/Sensor > Modo de baixa latência)** e selecione **On (Ativado)**.
4. Clique em **Salvar**.

Seleção do modo de exposição

Para melhorar a qualidade da imagem em cenas de monitoramento específicas, use os modos de exposição. Os modos de exposição permitem que você controle a abertura, a velocidade do obturador e o ganho. Vá para **Video > Image > Exposure (Vídeo > Imagem > Exposição)** e selecione entre os seguintes modos de exposição:

- Para a maioria dos casos de uso, selecione a exposição **Automatic (Automática)**.
- Para ambientes com determinada iluminação artificial, por exemplo, iluminação fluorescente, selecione **Sem cintilação**.
Selecione a mesma frequência da linha de alimentação.
- Para ambientes com determinadas iluminações artificiais e luz brilhante, por exemplo, áreas externas com iluminação fluorescente e sol durante o dia, selecione **Redução de cintilação**.
Selecione a mesma frequência da linha de alimentação.
- Para manter as configurações de exposição atuais, selecione **Hold current (Manter atuais)**.

Compensação da distorção de barril

A distorção de barril é um fenômeno no qual as linhas retas parecem mais tortas mais próximas às extremidades do quadro. Um campo de visão amplo frequentemente cria distorções de barril em uma imagem. A correção de distorção de barril compensa esse tipo de distorção.

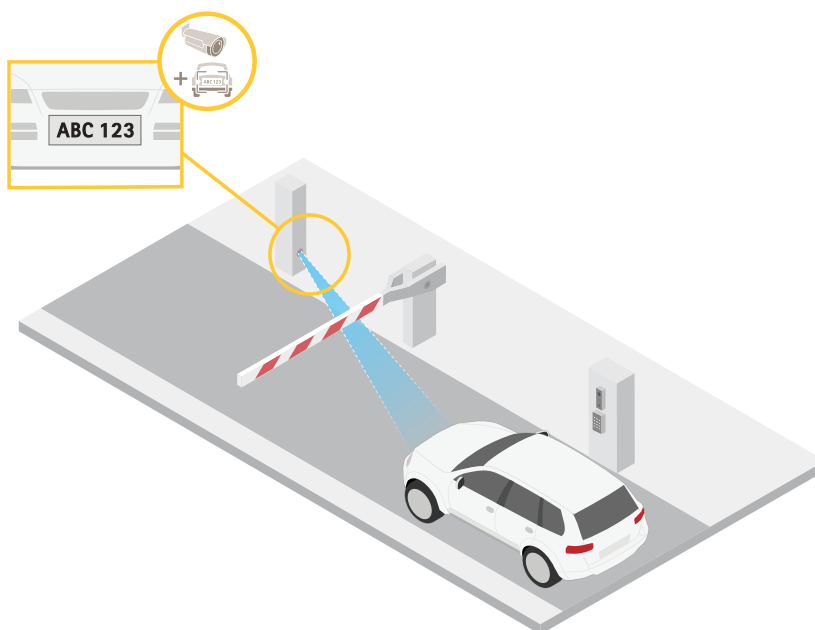
Observação

A correção de distorção de barril afeta a resolução da imagem e o campo de visão.

1. Vá para **Video > Installation > Image correction (Vídeo > Instalação > Correção da imagem)**.
2. Ative a opção **Barrel distortion correction (BDC) (Correção de distorção cilíndrica (BDC))**.

Verifique a resolução de pixels

Para verificar que uma parte definida da imagem contém pixels suficientes, por exemplo, para reconhecer placas de licença, você pode usar o contador de pixels.



1. Vá para **Video > Image (Vídeo > Imagem)**.

2. Clique em .
3. Clique em  para **Pixel counter (Contador de pixels)**.
4. Na vista ao vivo da câmera, ajuste o tamanho e posição do retângulo ao redor da área de interesse, por exemplo, onde você espera que as placas de licença apareçam.
5. Você pode ver o número de pixels para cada lado do retângulo e decidir se os valores são suficientes para as suas necessidades.

Exibição e gravação de vídeo

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

Redução de largura de banda e armazenamento

Importante

A redução da largura de banda pode levar à perda de detalhes na imagem.

1. Vá para **Video > Stream (Vídeo > Fluxo)**.
2. Clique em  na visualização ao vivo.
3. Selecione **Video format (Formato de vídeo) AV1** se o dispositivo for compatível com ele. Caso contrário, selecione **H.264**.
4. Vá para **Video > Stream > General (Vídeo > Fluxo > Geral)** e aumente **Compression (Compactação)**.
5. Vá para **Video > Stream > Zipstream (Vídeo > Fluxo > Zipstream)** e siga um ou mais dos seguintes procedimentos:

Observação

As configurações do Zipstream são usadas para todos os codificadores de vídeo, exceto MJPEG.

- Selecione a **Strength (Intensidade)** da Zipstream que deseja usar.
- Ative **Optimize for storage (Otimizar para armazenamento)**. Esse recurso só poderá ser usado se o software de gerenciamento de vídeo oferecer suporte a quadros B.
- Ative o **Dynamic FPS (FPS dinâmico)**.
- Ative **Dynamic GOP (Grupo de imagens dinâmico)** e defina um valor alto para **Upper limit (Limite superior)** do comprimento de GOP.

Observação

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

Configurar o armazenamento de rede

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

1. Vá para **System > Storage (Sistema > Armazenamento)**.
2. Clique em  **Add network storage (Adicionar armazenamento de rede)** em **Network storage (Armazenamento de rede)**.
3. Digite o endereço IP do servidor host.
4. Digite o nome do local compartilhado no servidor host em **Network share (Compartilhamento de rede)**.
5. Digite o nome de usuário e a senha.
6. Selecione a versão SMB ou deixe em **Auto**.

7. Selecione **Add share without testing (Adicionar compartilhamento sem testar)** se você experimentar problemas de conexão temporários ou se o compartilhamento ainda não tiver sido configurado.
8. Clique em **Adicionar**.

Como gravar e assistir vídeo

Gravar vídeo diretamente da câmera

1. Vá para **Video > Stream (Vídeo > Fluxo)**.
2. Para iniciar uma gravação, clique em .

Se você não configurou nenhum armazenamento, clique em  e em . Para obter instruções sobre como configurar o armazenamento de rede, consulte *Configurar o armazenamento de rede, on page 16*

3. Para interromper a gravação, clique em  novamente.

Assista ao vídeo

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

Verifique se o firmware não foi manipulado com o vídeo

Com o vídeo assinado, é possível garantir que ninguém manipulou o vídeo gravado pela câmera.

1. Vá para **Video > Stream > General (Vídeo > Fluxo > Geral)** e ative **Signed video (Vídeo assinado)**.
2. Grave vídeos diretamente no dispositivo ou utilize o AXIS Camera Station Pro ou outro software de gerenciamento de vídeo compatível. Para obter instruções sobre o AXIS Camera Station Pro, consulte o *manual do usuário do AXIS Camera Station Pro*.
3. Exporte o vídeo gravado.
4. Utilize a ferramenta *Axis Signed Media Verifier* para verificar a gravação.

Configuração de regras de eventos

Você pode criar regras para fazer com que o dispositivo realize ações quando certos eventos ocorrem. Uma regra consiste em condições e ações. As condições podem ser usadas para acionar as ações. Por exemplo, o dispositivo pode iniciar uma gravação ou enviar um email quando detecta movimento ou mostrar um texto de sobreposição enquanto o dispositivo está gravando.

Para saber mais, consulte *Comece a utilizar regras para eventos*.

Gravar vídeo quando a câmera detectar uma placa de licença

Este exemplo explica como configurar o dispositivo para iniciar a gravação no cartão SD quando a câmera detecta um objeto. A gravação incluirá cinco segundos antes da detecção e um minuto após o término da detecção.

Antes de começar:

- Certifique-se de ter um cartão SD instalado.

Certifique-se de que o verificador da placa de licença AXIS esteja em execução:

1. Vá para **Apps > AXIS License Plate Verifier**.
2. Inicie o aplicativo se ele ainda não estiver em execução.
3. Certifique-se de ter configurado o aplicativo de acordo com suas necessidades.

Crie uma regra:

1. vá para **System > Events (Sistema > Eventos)** e adicione uma regra.

2. Digite um nome para a regra.
3. Na lista de condições, em **Application (Aplicativo)**, selecione **ALPV.PlateInView**.
4. Na lista de ações, em **Recordings (Gravações)**, selecione **Record video while the rule is active (Gravar vídeo enquanto a regra estiver ativa)**.
5. Na lista de opções de armazenamento, selecione **SD_DISK**.
6. Selecione uma câmera e um perfil de fluxo.
7. Defina o tempo do pré-buffer como 5 segundos.
8. Defina o tempo do pós-buffer como 1 minuto.
9. Clique em **Salvar**.

Accionar uma notificação quando a lente da câmera for manipulada

Este exemplo explica como configurar uma notificação por email quando a lente da câmera for pintada com tinta em spray, encoberta ou desfocada.

Ativar a detecção de manipulação:

1. Vá para **System > Detectors > Camera tampering (Sistema > Detectores > Manipulação da câmera)**.
2. Defina um valor para **Trigger delay (Retardo do acionador)**. O valor indica o tempo que deve ser transcorrido antes que um email seja enviado.
3. Ative **Trigger on dark images (Acionar em imagens escuras)** para detectar se a lente é borrifada, coberta ou tirada significativamente de foco.

Adicionar um destinatário de email:

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

Crie uma regra:

12. Acesse **System > Events > Rules (Sistema > Eventos > Regras)** e adicione uma regra:
13. Digite um nome para a regra.
14. Na lista de condições, em **Video (Vídeo)**, selecione **Tampering (Manipulação)**.
15. Na lista de ações, em **Notifications (Notificações)**, selecione **Send notification to email (Enviar notificação para email)** e, em seguida, selecione o destinatário na lista.
16. Digite uma linha de assunto e a mensagem do email.
17. Clique em **Salvar**.

Áudio

Adição de áudio à sua gravação

Ative o áudio:

1. Vá para **Video > Stream > Audio (Vídeo > Fluxo > Áudio)** e inclua áudio.
2. Se o dispositivo tiver mais de uma fonte de entrada, selecione a correta em **Source (Fonte)**.

3. Vá para **Audio > Device settings** (Áudio > Configurações do dispositivo) e ative a fonte de entrada correta.

Edite o perfil de fluxo que é usado para a gravação:

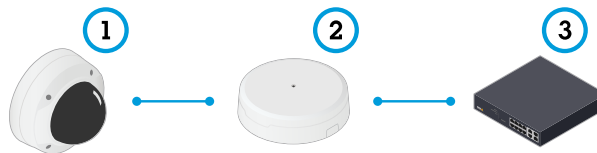
4. Vá para **System > Stream profiles** (Sistema > Perfis de fluxo) e selecione o perfil de fluxo.
5. Selecione **Include audio** (Incluir áudio) e ative-a.
6. Clique em **Salvar**.

Adicione capacidade de áudio ao seu produto usando portcast

Com a tecnologia portcast, você pode adicionar recursos de áudio ao seu produto. Ele permite a comunicação de áudio e E/S digitalmente via cabo de rede entre a câmera e a interface.

Para adicionar capacidade de áudio ao seu dispositivo de vídeo em rede Axis, conecte o dispositivo de áudio Axis e a interface de E/S compatíveis entre seu dispositivo e o switch PoE responsável por fornecer a alimentação.

1. Conecte o dispositivo de vídeo em rede Axis (1) e o dispositivo portcast Axis (2) com um cabo PoE.
2. Conecte o dispositivo portcast Axis (2) e o switch PoE (3) com um cabo PoE.



- 1 Dispositivo de vídeo em rede Axis
- 2 Dispositivo portcast Axis
- 3 Switch

Assim que os dispositivos estiverem conectados, uma guia de áudio se tornará visível nas configurações para seu dispositivo de vídeo em rede Axis. Vá para a guia **Audio** (Áudio) e ative a opção **Allow audio** (Permitir áudio).

Consulte o manual do usuário do dispositivo portcast Axis para obter mais informações.

Gerenciar listas

Adicionar placa de licença detectada à lista

Uma placa de licença pode ser adicionada diretamente a uma lista após ser detectada pelo aplicativo.

1. Clique em Home (Início).
2. Vá para Live (Ao vivo).
3. Clique no ícone de seta na placa registrada na lista.
4. Clique em **Append plate to list (Adicionar placa à lista)**.
5. Selecione a lista à qual deseja adicionar a placa de licença na caixa de diálogo.
6. Clique em **Append (Anexar)**.

Observação

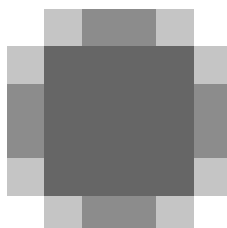
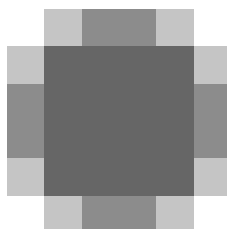
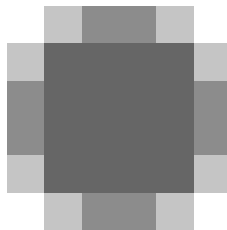
Certifique-se de que os símbolos <, > e & não sejam usados na placa de licença ou na descrição.

Adicionar descrições a placas de licença

Para adicionar uma descrição a uma placa de licença na lista:

- Vá para List management (Gerenciamento de listas).

- Selecione a placa de licença, clique em



e, em seguida, selecione **Edit (Editar)** no menu suspenso.

- Digite as informações relevantes no campo **Description (Descrição)**.
- Clique em **Salvar**.

Observação

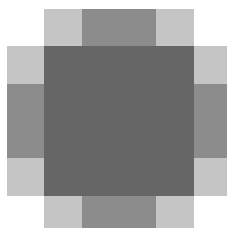
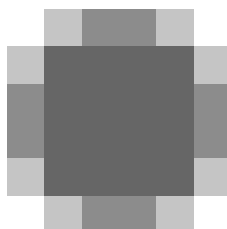
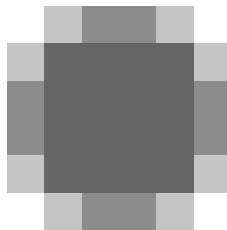
Certifique-se de que os símbolos <, > e &t não sejam usados em placas de licença ou descrições.

Personalização de nomes de listas

Você pode alterar o nome de qualquer uma das listas para ajustá-lo ao seu caso de uso específico.

1. Vá para **List management (Gerenciamento de listas)**.

2. Clique em



ao lado da lista que deseja alterar.

3. Selecione **Edit (Editar)**.
4. Digite o nome da lista.
5. Clique em **Submit (Enviar)**.

O novo nome da lista será atualizado em todas as configurações existentes.

Importação de números de placas de licença na lista de permissão

Você pode importar números de placas de licença na lista de permissão a partir de um arquivo .csv no computador. Além do número da placa de licença, você também pode adicionar comentários para cada número de placa no arquivo .csv.

A estrutura do arquivo .csv deve parecer com esta: `license plate, date, description`

Exemplo:

Somente placa de licença: `AXIS123`

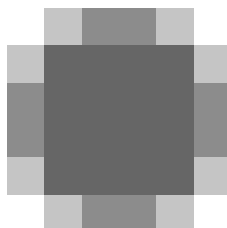
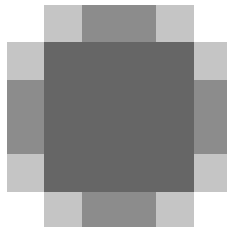
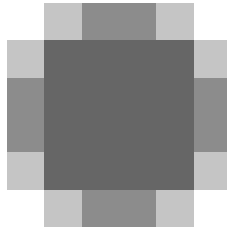
Placa de licença + descrição: `AXIS123, , John Smith`

Placa de licença + data + descrição: `AXIS123, 2022-06-08, John Smith`

Observação

Certifique-se de que os símbolos <, > e & não sejam usados em placas de licença ou descrições.

1. Vá para List management (Gerenciamento de listas).
2. Clique em



ao lado de Allowlist (Lista de permissão) e selecione Import (Importar) no menu suspenso.

3. Navegue para selecionar um arquivo. csv no computador.
4. Clique em OK.
5. Verifique se os números de placas de licença importados aparecem no campo Allowlist (Lista de permissão).

Compartilhamento de listas de placas de licença com outras câmeras

Você pode compartilhar as listas de placas de placas com outras câmeras na rede. A sincronização substituirá todas as listas de placas de licenças atuais nas outras câmeras.

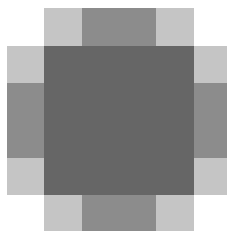
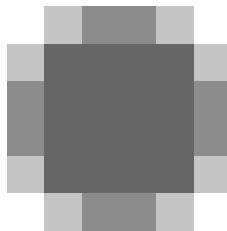
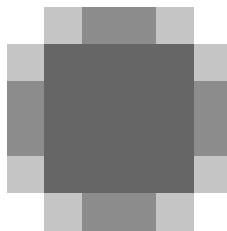
1. Vá para List management > List synchronization (Gerenciamento de listas > Sincronização de listas).
2. Em Remote connected devices (Dispositivos conectados remotamente), digite o endereço IP, nome de usuário e senha.
3. Clique em Adicionar.

4. Clique em **Synchronize list (Sincronizar lista)**.
5. Verifique se a data e a hora em **Last sync (Última sincronização)** são atualizadas de acordo.

Agendar listas

As listas podem ser agendadas para que estejam ativas somente em determinados horários durante determinados dias da semana. Para agendar uma lista:

- Vá para **List management (Gerenciamento de listas)**.
- Clique em



ao lado da lista que deseja alterar.

- Selecione **Schedule (Programação)** no menu suspenso.
- Selecione a hora de início e de término e o dia em que a lista deve estar ativa.
- Clique no botão próximo a **Enabled (Ativada)** para continuar.
- Clique em **Salvar**.

Configurações adicionais

Configurar sobreposição de texto

Uma sobreposição de texto mostra as seguintes informações de eventos na visualização ao vivo: `weekday`, `month`, `time`, `year`, `license plate number`.

1. Vá para **Settings (Configurações) > Image (Imagem)**.
2. Ative a opção **Text overlay (Sobreposição de texto)**.
3. Selecione uma das seguintes opções: **Timestamp and license plate (Data e hora e placa de licença)** ou **License plate only (Placa somente)**.
4. Defina a **Overlay duration (Duração da sobreposição)** como um valor entre 1 e 9 segundos.
5. Verifique se a sobreposição aparece na visualização ao vivo.

Detecção de placas de licença em condições de pouca iluminação

Cada detecção recebe uma pontuação do algoritmo, denominada limiar de confiança. As detecções com pontuação inferior ao valor do nível selecionado não são mostradas na lista de eventos.

Para cenas com pouca luz, é possível definir um limiar de confiança mais baixo, o que permitirá a detecção de mais placas.

1. Vá para **Settings > Recognition (Configurações > Reconhecimento)**.
2. Ajuste o controle deslizante em **Confidence threshold (Limiar de confiança)**.
3. Verifique se o algoritmo detecta as placas de licença conforme esperado.

Permitir menos caracteres nas placas de licença

O aplicativo possui um número mínimo padrão de caracteres para detectar uma placa de licença. O número mínimo padrão de caracteres é cinco. Você pode configurar o aplicativo para detectar placas de licença com menos caracteres.

1. Vá para **Settings > Recognition (Configurações > Reconhecimento)**.
2. Em **Number of characters (Número de caracteres)**, ajuste ou controle deslizante para definir o número mínimo de caracteres que deseja permitir.
3. Verifique se o aplicativo detecta as placas de licença conforme esperado.

Permitir somente correspondências exatas de placas de licença

O algoritmo de correspondência permite automaticamente um desvio de um caractere ao comparar a placa de licença detectada com a lista de permissão ou a lista de bloqueio. No entanto, alguns cenários necessitam de uma correspondência exata de todos os caracteres da placa de licença.

1. Vá para **List management (Gerenciamento de listas)**.
2. Clique para ativar **Strict matching (Correspondência estrita)**.
3. Verifique se o aplicativo compara as placas de licença conforme esperado.

Permitir o desvio de mais de um caractere ao comparar placas de licença

O algoritmo de correspondência permite automaticamente um desvio de um caractere ao comparar a placa de licença detectada com a lista de permissão ou a lista de bloqueio. No entanto, você pode permitir o desvio de mais de um caractere.

1. Vá para **Settings > Recognition (Configurações > Reconhecimento)**.
2. Em **Allowed character deviation (Desvio de caractere permitido)**, selecione o número de caracteres que podem ser diferentes.

3. Verifique se o aplicativo compara as placas de licença conforme esperado.

Fornecer acesso limitado aos operadores

Os operadores podem ter acesso limitado ao aplicativo usando um URL. Dessa forma, eles só têm acesso a Event log (Registro de eventos) e List management (Gerenciamento de listas). O URL pode ser encontrado em Settings > User rights (Configurações > Direitos de usuário).

Configuração de uma conexão segura

Para proteger a comunicação e os dados entre dispositivos, por exemplo, entre a câmera e o controlador de porta, configure uma conexão segura com HTTPS usando certificados.

1. Vá para Settings (Configurações) > Security (Segurança).
2. Em HTTPS, selecione Self-signed (Autoassinado) ou CA-signed (Assinado pela CA).

Observação

Saiba mais sobre HTTPS e como usá-lo em .

Fazer backup e restaurar configurações de aplicativos

Você pode fazer backup e restaurar as configurações feitas no aplicativo relacionadas à captura de imagens, segurança, detecção e integração. Se algo errado ocorrer, agora você poderá restaurar as configurações das quais criou um backup.

Para fazer backup das configurações do aplicativo:

- Vá para Settings > Maintenance (Configurações > Manutenção).
- Clique em Download backup configuration (Baixar configuração de backup).

Um arquivo JSON será baixado para sua pasta de downloads.

Para restaurar as configurações do aplicativo:

- Vá para Settings > Maintenance (Configurações > Manutenção).
- Clique em Restore configuration (Restaurar configuração).

Selecione o arquivo JSON que contém o backup.

As configurações são restauradas automaticamente.

Limpar todos os eventos

Após configurar o aplicativo, talvez seja uma boa ideia limpar os registros de qualquer imagem ou placa capturada durante o processo de configuração.

Para limpar todas as imagens e placas do banco de dados:

Vá para Settings > Maintenance (Configurações > Manutenção).

- Clique em Clear all recognition results (Limpar todos os resultados do reconhecimento).
- Clique em Sim.

Usar portas virtuais para acionar ações

As portas virtuais podem ser usadas junto com o controle de acesso para acionar qualquer tipo de ação. Este exemplo explica como configurar o AXIS License Plate Verifier juntamente com a porta de E/S da câmera para exibir uma sobreposição de texto usando uma porta virtual.

Requisitos:

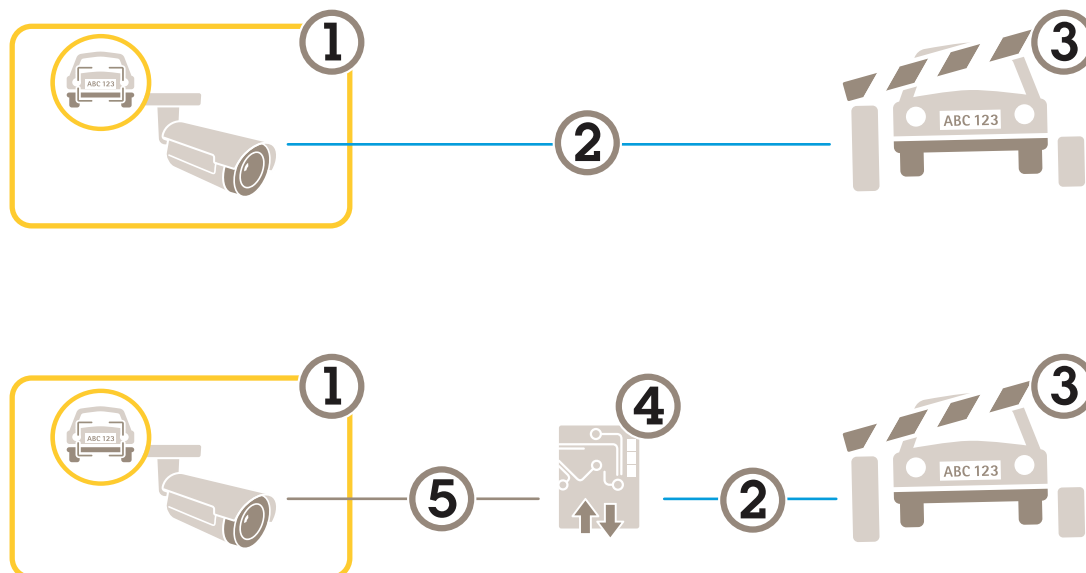
- Câmera fisicamente instalada e conectada à rede.
- AXIS License Plate Verifier pronto e em execução na câmera.
- Cabos conectados entre a barreira e a porta de E/S da câmera.

- Configuração básica pronta. Consulte .
- 1. Vá para a página Web do aplicativo e selecione a guia **Settings (Configurações)**.
- 2. Vá para **Access control (Controle de acesso)**.
- 3. Em **Access control (Controle de acesso)**, selecione **Internal I/O (E/S interna)**.
- 4. Selecione a **I/O output # (Saída de E/S #)**.
- 5. Selecione uma porta na lista suspensa **Virtual port (Porta virtual)**.
- 6. Em **Barrier mode (Modo de barreira)**, selecione **Open to all (Aberto a todos)**.
- 7. Em **Vehicle direction (Direção do veículo)**, selecione **Any (Qualquer uma)**.
- 8. Selecione a **Area of interest (Área de interesse)** que deseja utilizar.
- 9. Na página Web da câmera, vá para **System > Events (Sistema > Eventos)**.
- 10. Clique em **Add rule (Adicionar regra)**.
- 11. Em **Condition (Condição)**, selecione **Virtual input is active (A entrada virtual está ativa)** e o número da porta que você selecionou.
- 12. Em **Action (Ação)**, selecione **Use overlay text (Usar texto de sobreposição)**.
- 13. Selecione um **Video channels (Canais de vídeo)**.
- 14. Digite o texto que deseja exibir.
- 15. Adicione a duração do texto.
- 16. Clique em **Salvar**.
- 17. Vá para **Video > Overlays (Vídeo > Sobreposições)**.
- 18. Vá para **Overlays (Sobreposições)**.
- 19. Selecione **Text (Texto)** no menu suspenso e clique em **+**.
- 20. Digite **#D** ou selecione o modificador na lista suspensa **Modifiers (Modificadores)**.
- 21. Verifique se a sobreposição de texto é exibida quando um veículo entra na região de interesse na visualização ao vivo.

Cenário de entrada e saída de veículos

No cenário da entrada e saída de veículos, o aplicativo lê a placa do veículo capturada pela câmera e a verifica em relação a uma lista de números de placas autorizadas ou não autorizadas armazenadas na câmera.

Esse cenário requer o aplicativo incorporado em uma câmera com suporte a E/S ou um módulo de relé de E/S conectado para abrir e fechar a barreira.



Duas configurações possíveis para o cenário de entrada e saída de veículos.

- 1 Câmera Axis com o AXIS License Plate Verifier
- 2 Comunicação de E/S
- 3 Barreira
- 4 Módulo de relé de E/S Axis
- 5 Comunicação IP

Abertura de uma barreira para veículos conhecidos usando um módulo de relé

Esse caso de uso de exemplo explica como configurar o AXIS License Plate Verifier juntamente com um módulo de relé para abrir uma cancela para um veículo conhecido dirigindo através de uma região de interesse (ROI) específica para, digamos, uma área de estacionamento.

Requisitos:

- Câmera fisicamente instalada e conectada à rede.
 - AXIS License Plate Verifier pronto e em execução na câmera.
 - Cabos conectados entre a barreira e o módulo de relé.
 - Configuração básica pronta. Consulte *Configuração básica*, on page 6.
1. Vá para a página Web da câmera, selecione **Settings (Configurações)** e abra o AXIS License Plate Verifier.
 2. Acesse a página Web do módulo de relé e certifique-se de que a porta do relé esteja conectada à porta de E/S da câmera.
 3. Copie o endereço IP do módulo do relé.
 4. Volte para o AXIS License Plate Verifier.
 5. Acesse **Settings (Configurações) > Access control (Controle de acesso)**.
 6. Vá para **Type (Tipo)** e selecione **Relay (Relé)** na lista suspensa.
 7. Na lista suspensa **I/O output (Saída de E/S)**, selecione a porta de E/S que está conectada à barreira.

8. Na lista suspensa **Barrier mode (Modo de barreira)**, selecione **Open from lists (Abrir a partir de listas)** e marque a opção **Allowlist (Lista de permissão)**.
9. Na lista suspensa **Vehicle direction (Direção do veículo)** selecione **in (entrando)**.
10. Na lista suspensa **ROI (Região de interesse)**, selecione a área de interesse que cobre a faixa de trânsito.
11. Insira as seguintes informações:
 - o endereço IP do módulo de relé no formato 192.168.0.0
 - o nome de usuário do módulo de relé
 - a senha do módulo de relé
12. Para garantir que a conexão funcione, clique em **Connect (Conectar)**.
13. Para ativar a conexão, clique em **Turn on integration (Ativar integração)**.
14. Vá para a guia **List management (Gerenciamento de listas)**.
15. Insira o número da placa no campo **Allowlist (Lista de permissão)**.

Observação

As portas de entrada físicas de 1 a 8 no módulo de relé correspondem às portas de 1 a 8 na lista suspensa. No entanto, as portas de relé de 1 a 8 no módulo de relé correspondem às portas de 9 a 16 na lista suspensa. Isso será válido mesmo se o módulo de relé tiver apenas 8 portas.

16. Verifique se o aplicativo identificará o número da placa na lista de permissão como um veículo conhecido e se a barreira abrirá conforme o esperado.

Abertura de uma barreira para veículos conhecidos usando a E/S da câmera

Este exemplo explica como configurar o AXIS License Plate Verifier juntamente com a porta de E/S da câmera para abrir uma barreira para um veículo conhecido que está entrando, por exemplo, em um estacionamento.

Requisitos:

- Câmera fisicamente instalada e conectada à rede.
 - AXIS License Plate Verifier pronto e em execução na câmera.
 - Cabos conectados entre a barreira e a porta de E/S da câmera.
 - Configuração básica pronta. Consulte .
1. Vá para a página da Web do aplicativo, acesse **Home (Início)** e, em seguida, adicione placas de licença detectadas a uma lista. Consulte *Adicionar placa de licença detectada à lista, on page 20*
 2. Para editar as listas diretamente, vá para **List management (Gerenciamento de listas)**.
 3. Insira os números das placas autorizadas no campo **Allowlist (Lista de permissão)**.
 4. Vá para **Settings (Configurações)**.
 5. Em **Access control (Controle de acesso)**, selecione **Internal I/O (E/S interna)**.
 6. Selecione a **I/O output # (Saída de E/S #)**.
 7. Em **Barrier mode (Modo de barreira)**, selecione **Open from lists (Abrir a partir de listas)** e, em seguida, marque **Allowlist (Lista de permissão)**.
 8. Na lista suspensa **Vehicle direction (Direção do veículo)** selecione **in (entrando)**.
 9. Em **Area of interest (Área de interesse)**, selecione a área de interesse que gostaria de usar ou se deseja usar a área inteira.
 10. Verifique se o aplicativo identificará o número da placa na lista de permissão como um veículo conhecido e se a barreira abrirá conforme o esperado.

Observação

Você pode alterar o nome de qualquer uma das listas para ajustá-lo ao seu caso de uso específico.

Recebimento de notificação sobre um veículo não autorizado

Este exemplo explica como configurar o aplicativo para que um evento que aciona uma notificação possa ser criado na câmera.

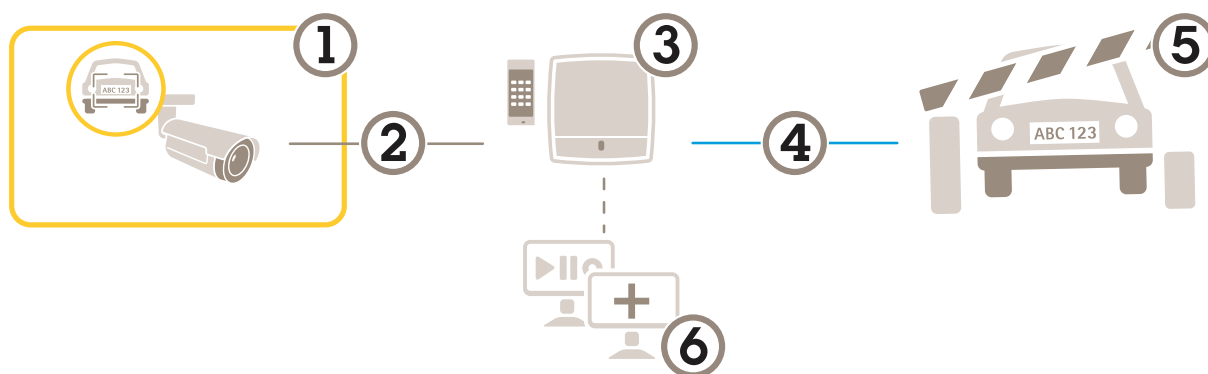
Requisitos:

- Configuração básica pronta. Consulte a *Configuração básica, on page 6*.
- 1. Vá para **List management (Gerenciamento de listas)**.
- 2. Insira o número da placa no campo **Blocklist (Lista de bloqueio)**.
- 3. Vá para a página Web da câmera.
- 4. Vá para **Settings (Configurações) > Events (Eventos)** e configure uma regra de ação com o aplicativo como uma condição e com uma notificação como uma ação.
- 5. Verifique se o aplicativo identificará o número da placa adicionada como um veículo não autorizado e se a regra de ação será executada conforme o esperado.

Cenário de controle de acesso de veículos

No cenário de controle de acesso de veículos, o aplicativo pode ser conectado a um controlador de portas em rede Axis para configuração de regras de acesso, criação de agendamentos para tempos de acesso e controle do acesso de veículos não apenas de funcionários, mas também, por exemplo, de visitantes e fornecedores.

Por backup, use um sistema de acesso que envolva um controlador de porta e um leitor de cartões. Para configurar o controlador de portas e o leitor de cartões, consulte a documentação do usuário em axis.com



- 1 Câmera Axis com o AXIS License Plate Verifier
- 2 Comunicação IP
- 3 Controlador de portas em rede Axis com leitor de cartões
- 4 Comunicação de E/S
- 5 Barreira
- 6 Software de terceiros opcional

Conexão a um controlador de porta

Neste exemplo nós conectaremos a câmera a um controlador de porta em rede, o que significa que a câmera funcionará como um sensor. A câmera encaminha as informações para o controlador que, por sua vez, analisa as informações e aciona os eventos.

Observação

Ao alternar entre o AXIS License Plate Verifier e AXIS Entry Manager, certifique-se de atualizar as páginas da Web para obter acesso a todos os parâmetros.

Requisitos:

- Câmera e controlador de porta fisicamente instalados e conectados à rede.
- AXIS License Plate Verifier pronto e em execução na câmera.
- Configuração básica pronta. Consulte *Configuração básica*, on page 6.



Como configurar e executar o aplicativo com o AXIS A1001 Door Controller.

Configuração de hardware no AXIS Entry Manager

1. Vá para AXIS Entry Manager e inicie uma nova configuração de hardware em **Setup (Configuração)**.
2. Na configuração de hardware, renomeie o controlador de porta em rede para "Gatecontroller".
3. Clique em **Next (Próximo)**.
4. Em **Configure locks connected to this controller (Configurar fechaduras conectadas a este controlador)**, desmarque a opção **Door monitor (Monitor de portas)**.

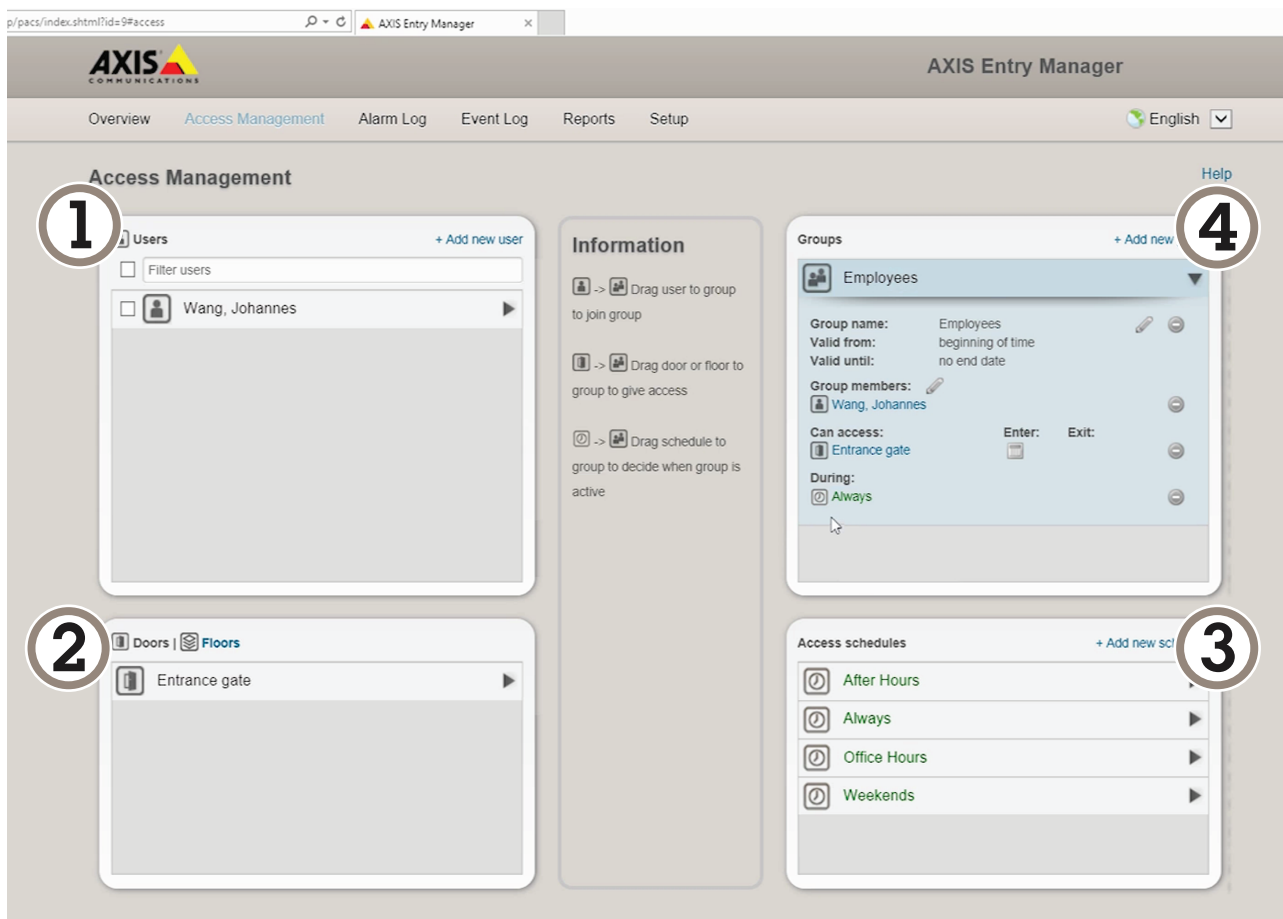
5. Clique em **Next** (Próximo).
6. Em **Configure readers connected to this controller** (Configurar leitores conectados a este controlador), desmarque a opção **Exit reader** (Sair do leitor).
7. Clique em **Finish** (Concluir).

Configuração no AXIS License Plate Verifier

1. Acesse a página Web do AXIS License Plate Verifier.
2. Acesse **Settings (Configurações) > Access control (Controle de acesso)**.
3. Vá para **Type (Tipo)** e selecione **Controller (Controlador)** na lista suspensa.
4. Insira as seguintes informações:
 - o endereço IP do controlador, no formato 192.168.0.0
 - o nome de usuário para o controlador
 - a senha do controlador.
5. Clique em **Conectar**.
6. Se a conexão for bem-sucedida, "Gatecontroller" será exibido na lista suspensa **Network Door Controller name (Nome do controlador de porta em rede)**. Selecione "Gatecontroller".
7. Na lista suspensa **Reader name (Nome do leitor)**, selecione o leitor conectado à porta "Gatecontroller", por exemplo, "Reader entrance". Esses nomes podem ser alterados no AXIS Entry Manager.
8. Para ativar a conexão, selecione **Turn on integration (Ativar integração)**.
9. Insira um dos números da placa de licença do usuário – ou use o padrão – no campo de teste e clique em **Test integration (Testar integração)**. Verifique se o teste foi concluído com êxito.

Configure usuários, grupos, portas e agendamentos no AXIS Entry Manager

1. Vá para o AXIS Entry Manager.
2. Vá para **Access Management (Gerenciamento de acesso)**.
3. Vá para **Doors > Add identification type (Portas > Adicionar tipo de identificação)**.
4. Na lista suspensa **Credentials needed (Credenciais necessárias)**, selecione **License plate only (Placa somente)**.
5. Para definir limites para quando o tipo de identificação pode ser usado, arraste e solte um **Schedule (Agendamento)** na porta.
6. Adicione usuários e, para cada usuário, adicione a credencial **License plate (Placa de licença)**.
7. Clique em **Add credential (Adicionar credencial)** novamente e insira as informações da placa.
8. Clique em **Add new group (Adicionar novo grupo)** e insira as informações.
9. Para adicionar usuários a um grupo, arraste e solte **Users (Usuários)** no grupo de usuários.
10. Para conceder acesso aos usuários, arraste e solte a **Door (Porta)** no grupo de usuários.
11. Para limitar o tempo de acesso, arraste e solte um **Schedule (Agendamento)** no grupo de usuários.



Visão geral da interface do usuário do AXIS Entry Manager.

- 1 Usuários
- 2 Portas
- 3 Programações
- 4 Grupos de usuários

Conectar ao AXIS Secure Entry

Este exemplo descreve a conexão de um controlador de porta Axis ao AXIS Camera Station e ao AXIS Secure Entry com AXIS Licence Plate Verifier.

Requisitos:

- Câmera e controlador de porta fisicamente instalados e conectados à rede.
- AXIS License Plate Verifier pronto e em execução na câmera.
- Cliente do AXIS Camera Station versão 5.49.449 ou superior.
- Configuração básica pronta. Consulte *Configuração básica*, on page 6.

No AXIS Camera Station, consulte *Adicionar um leitor*.

No app AXIS License Plate Verifier:

1. Na guia Settings (Configurações), vá para Configuration wizard (Assistente de configuração) e clique em Start (Iniciar).
2. Selecione Access Control (Controle de acesso).
3. Selecione Secure Entry (Entrada segura) e clique em Next (Avançar).

No AXIS Camera Station:

4. Digite o endereço IP do controlador de porta, disponível na lista de dispositivos em AXIS Camera Station>Configuration>Other Devices (AXIS Camera Station > Configuração > Outros dispositivos).

5. Para adicionar uma chave de autenticação, vá para **AXIS Camera Station>Configuration>Encrypted communication** (AXIS Camera Station > Configuração > Comunicação criptografada).
6. Vá para **External Peripheral Authentication Key** (Chave de autenticação de periférico externo) e clique em **Show authentication key** (Mostrar chave de autenticação).
7. Clique em **Copy key** (Copiar chave).

No app **AXIS License Plate Verifier**:

8. Vá para **Authentication key** (Chave de autenticação) no assistente de configuração e cole a chave.
9. Clique em **Conectar**.
10. Selecione o **Door controller name** (Nome do controlador de porta) no menu suspenso.
11. Selecione o **Reader name** (Nome do leitor) no menu suspenso.
12. Marque a opção **Turn on integration** (Ativar integração).
13. Clique em **Next** (Próximo).
14. Ajuste a área de interesse. Consulte *Ajuste a área de interesse, on page 10*.
15. Clique em **Next** (**Avançar**) duas vezes e, em seguida, em **Finish** (**Concluir**).

Cenário de livre fluxo com medição de velocidade

Em um cenário de livre fluxo com medição de velocidade, a câmera é pareada com um radar Axis por meio da tecnologia edge-to-edge. A câmera cobre duas faixas e lê as placas de licença dos veículos que passam, e o radar pareado cobre as mesmas duas faixas para medir a velocidade dos veículos. Além disso, o aplicativo *AXIS Speed Monitor* pode visualizar a velocidade máxima em cada faixa por meio de sobreposições na visualização ao vivo da câmera.

Para saber mais sobre edge-to-edge, consulte *Tecnologia de ponta a ponta*, on page 44.

Requisitos:

- Um kit de câmera Axis License Plate Verifier e *AXIS D2210-VE Radar* instalado e conectado à rede

Configurar o cenário

Configure o cenário em quatro etapas: primeiro configure a câmera, depois emparelhe e configure o radar e, por fim, use o *AXIS Speed Monitor* para adicionar sobreposições.

Antes de começar:

- Certifique-se de que a câmera e o radar estejam direcionados para a mesma área de interesse.
- Certifique-se de que a câmera e o radar estejam com o tempo sincronizado. Para verificar o status, vá para **Installation > Time sync status (Instalação > Status de sincronização de horário)** em cada dispositivo.
- Certifique-se de que a segunda área de exibição da câmera (**View area 2 (Área de exibição 2)**) não seja usada, já que o radar a usará após o pareamento.

Configurar a câmera:

1. Configure a câmera de acordo com as instruções fornecidas em *Configuração básica*, on page 6.
2. Selecione o fluxo livre ao seguir o assistente de configuração. Para obter mais informações, consulte *Fluxo livre*, on page 8.

Emparelhar o câmera com um radar:

1. Na interface Web da câmera, vá para **System > Edge-to-edge > Radar pairing (Sistema > Edge-to-edge > Pareamento de radar)**.
2. Insira o nome de host, o nome de usuário e a senha do radar.
3. Clique em **Connect (Conectar)** para parear os dispositivos.
Quando a conexão for estabelecida, as configurações do radar estarão disponíveis na interface Web da câmera.

Observação

A resolução padrão do radar emparelhado é 1280x720. Mantenha a resolução padrão do radar na interface web da webcam e se for adicioná-lo a um VMS.

Configurar o radar:

1. Na interface Web da câmera, vá para **Radar > Scenarios (Radar > Cenários)**.
2. Adicione um cenário de radar que cubra uma faixa e outro cenário de radar que cubra a outra faixa.
3. Em ambos os cenários, selecione **Movement in area (Movimento na área)**, acione em **Vehicles (Veículos)** e defina um **Speed limit (Limite de velocidade)**.
Para obter mais informações, vá para *Add scenarios (Adicionar cenários)* no manual do usuário do *AXIS D2210-VE Radar*.

Observação

Se desejar adicionar sobreposições contendo informações da placa de licença por meio do *AXIS License Plate Verifier*, adicione-as antes de adicionar sobreposições no *AXIS Speed Monitor*.

Use o *AXIS Speed Monitor* para adicionar sobreposições de velocidade:

1. Baixe e instale o *AXIS Speed Monitor* em sua câmera.

2. Adicione uma sobreposição para cada faixa, a qual mostrará a velocidade máxima na visualização ao vivo da câmera.
Para instruções de instalação e configuração, vá para o *manual do usuário do AXIS Speed Monitor*.

Pesquisar eventos específicos

Use o recurso de pesquisa para procurar eventos usando vários critérios.

1. Vá para a página da Web do aplicativo e selecione a página **Search (Pesquisar)**.
2. Selecione a data nos menus de calendário **From (De)** e **To (Até)**.
3. Clique no menu suspenso **AOI (Área de interesse)** para selecionar qual área de interesse deve ser incluída na pesquisa.
4. Selecione **Direction (Direção)** para filtrar por entrada ou saída.
5. Insira a placa de licença no campo **Plate (Placa)** se desejar procurar por uma placa.
6. Para localizar placas de licença pertencentes a um país específico, selecione um país na lista suspensa **Country (País)**.
7. Para filtrar imagens com base na exibição do veículo, selecione **Front (Dianteira)** ou **Rear (Traseira)** na lista suspensa **Vehicle view (Exibição do veículo)**.
8. Para filtrar os resultados da pesquisa com base na marca, modelo, tipo ou cor do veículo, selecione o que você está procurando nos menus suspensos **Vehicle details (Detalhes do veículo)**.
9. Clique em **Apply filters (Aplicar filtros)** para exibir os resultados da pesquisa.

Exportar e compartilhar resultados da pesquisa

Para exportar qualquer resultado de pesquisa como um arquivo CSV com as estatísticas daquele momento, clique em **Export (Exportar)** para salvar os resultados como um arquivo CSV.

Para copiar a API como um link que pode ser usado para exportar dados para sistemas de terceiros, clique em **Copy search link (Copiar link de pesquisa)**.

Integração

Use perfis para enviar eventos por push para vários servidores

Com perfis, você pode enviar por push um evento para diferentes servidores usando protocolos diferentes ao mesmo tempo. Para usar perfis:

1. Vá para **Integration (Integração)** e para a página **Push events (Eventos de push)**.
2. Selecione **Profile 1 (Perfil 1)**.
3. Configure a regra. Consulte *Informações sobre eventos push para software de outros fabricantes, on page 38*.
4. Testar a regra.
5. Selecione uma nova guia de perfil para configurar uma nova regra.

Informações sobre eventos push para software de outros fabricantes

Observação

O aplicativo envia as informações do evento no formato JSON. Para obter mais informações, *faça login usando sua conta MyAxis*, acesse a *AXIS VAPIX Library* e selecione **AXIS License Plate Verifier**

Com esse recurso, você pode integrar software de outros fabricantes ao enviar os dados de eventos via TCP ou HTTP POST.

Antes de começar:

- A câmera deverá estar fisicamente instalada e conectada à rede.
 - O **AXIS License Plate Verifier** deverá estar pronto e em execução na câmera.
1. Vá para **Integration (Integração) > Push events (Eventos de push)**.
 2. Selecionar um perfil vazio
 3. Na lista suspensa **Protocol (Protocolo)**, selecione **HTTP POST**.
 4. No campo **Server URL (URL do servidor)**, digite o endereço e a porta do servidor no seguinte formato:
127.0.0.1:8080
 5. Digite o nome de usuário e a senha.
 6. Caso esteja utilizando um proxy, ative-o e insira o nome de host, nome de usuário e senha.
 7. No campo **Device ID (ID do dispositivo)**, digite o nome do dispositivo ou deixe-o como está.
 8. Selecione a direção para acionar eventos de push em **Push conditions (Condições de push)**.
 9. Em **LPR Event types (Tipos de eventos de LPR)**, selecione uma ou mais das seguintes opções:
 - **New (Nova)** significa a primeira detecção de uma placa de licença.
 - **Update (Atualização)** é uma correção de um caractere em uma placa previamente detectada ou quando uma direção é detectada à medida que a placa se move e é rastreada ao longo da imagem.
 - **Lost (Perdido)** é o último evento rastreado da placa de licença antes dela sair da imagem. Ele também contém a direção da placa.
 - **Conditional (Condicional)** aciona um evento para um objeto quando as condições são atendidas.
 10. Para reduzir a largura de banda ao usar HTTP POST, você pode selecionar **Do not to send images (Não enviar imagens)**.
 11. Ative **Event buffer (Buffer de eventos)** para armazenar eventos no buffer caso o servidor fique indisponível e enviá-los quando o servidor voltar a ficar disponível.
 12. Para incluir o recorte da placa de licença do veículo, além da imagem, caso tenha escolhido em **Retention settings (Configurações de retenção)**, selecione **Send two images (Enviar duas imagens)**.

13. Para enviar os eventos no formato multipart em vez de base64, selecione **Multipart**.
14. Clique em **Test (Testar)** para testar a integração usando uma placa de licença virtual.
15. Para ativar o recurso, selecione **Activate (Ativar)**.

Observação

Para enviar eventos via HTTP POST, você pode usar um cabeçalho de autorização, em vez de um nome de usuário e uma senha, acessar **Auth-Header (Cabeçalho de autorização)** e adicionar um caminho para uma API de autenticação.

Envio de imagens de placas de licença para um servidor

Com esse recurso, você pode enviar imagens de placas de licença para um servidor via FTP.

Antes de começar:

- A câmera deverá estar fisicamente instalada e conectada à rede.
 - O AXIS License Plate Verifier deverá estar pronto e em execução na câmera.
1. Vá para **Integration (Integração) > Push events (Eventos de push)**.
 2. Na lista suspensa **Protocol (Protocolo)**, selecione **FTP**.
 3. No campo **Server URL (URL do servidor)**, digite o endereço do servidor no seguinte formato: `ftp://10.21.65.77/LPR`.
 4. Digite o nome de usuário e a senha para o servidor FTP.
 5. Selecione os modificadores de caminho e nome para os nomes de arquivos.
 6. No campo **Device ID (ID do dispositivo)**, digite o nome do dispositivo. Uma pasta com este nome será criada para as imagens. As imagens são criadas usando o seguinte formato: `timestamp_area of interest_direction_carID_license plate text_country.jpg`.
 7. Selecione a direção para acionar eventos de push em **Push conditions (Condições de push)**.
 8. Em **Event types (Tipos de eventos)**, selecione uma ou mais das seguintes opções:
 - **New (Nova)** significa a primeira detecção de uma placa de licença.
 - **Update (Atualização)** é uma correção de um caractere em uma placa previamente detectada ou quando uma direção é detectada à medida que a placa se move e é rastreada ao longo da imagem.
 - **Lost (Perdido)** é o último evento rastreado da placa de licença antes dela sair da imagem. Ele também contém a direção da placa.
 - **Conditional (Condicional)** aciona um evento para um objeto quando as condições são atendidas.

Observação

A direção é incluída somente no nome do arquivo quando as opções **Lost (Perdido)** ou **Update (Atualizado)** são selecionadas.

9. Clique em **Test (Testar)** para testar a integração usando uma placa de licença virtual.
10. Para ativar o recurso, clique em **Activate (Ativar)**.

Observação

Observe que a imagem varia dependendo do tipo de modo de captura selecionado. Consulte *Ajuste das configurações de captura de imagem*, on page 11.

Observação

Se os eventos push falharem, o aplicativo reenviará ao servidor até os 100 primeiros eventos que falharam. Ao usar o FTP para enviar eventos para um servidor Windows, não use %c para nomear as imagens que fornecem data e hora. Isso se deve ao fato de o Windows não aceitar a nomenclatura configurada pela função %c para data e hora. Observe que isso não é um problema quando se usa um servidor Linux.

Integração direta com 2N

Este exemplo descreve a integração direta com um dispositivo IP 2N.

Configure uma conta em seu dispositivo 2N:

1. Vá para o 2N IP Verso.
2. Vá para **Services (Serviços) > HTTP API (API HTTP) > Account 1 (Conta 1)**.
3. Selecione **Enable account (Ativar conta)**.
4. Selecione **Camera access (Acesso à câmera)**.
5. Selecione **License plate recognition (Reconhecimento de placas de licença)**.
6. Copie o endereço IP.

No app AXIS License Plate Verifier:

1. Vá para **Integration (Integração) > Direct integration (Integração direta)**.
2. Selecione **2N IP Device (Dispositivo IP 2N)**.
3. Adicione o endereço IP ou URL ao dispositivo 2N.
4. Digite seu nome de usuário e senha.
5. Selecione **Connection type (Tipo de conexão)**.
6. Selecione o motivo do uso da barreira em **Barrier is used for (A barreira é usada para)**.
7. Clique em **Enable integration (Permitir integração)**.
8. Selecione a direção dos veículos.
9. Para ativar o recurso, selecione **Activate (Ativar)**.

Para verificar se a integração está funcionando:

1. Vá para o 2N IP Verso.
2. Vá para **Status > Events (Eventos)**.

Integração ao Genetec Security Center

Este exemplo descreve a configuração de uma integração direta ao Genetec Security Center.

No Genetec Security Center:

1. Vá para **Overview (Visão geral)**.
2. Certifique-se de que **Database (Banco de dados)**, **Directory (Diretório)** e **License (Licença)** estejam online. Se não estiverem, execute todos os serviços Genetec e SQLEXPRESS no Windows.
3. Vá para **Genetec Config Tool > Plugins**.
4. Clique em **Add an entity (Adicionar uma entidade)**.
5. Vá para **Plugin (Plug-in)** e selecione **LPR plugin (Plug-in LPR)**.
6. Clique em **Next (Próximo)**.
7. Clique em **Next (Próximo)**.
8. Clique em **Next (Próximo)**.
9. Selecione o plug-in LPR que você adicionou e vá para **Data sources (Fontes de dados)**.

Em **ALPR reads API (ALPR lê API)**:

10. Marque **Enabled (Ativada)**.
11. Em **Name (Nome)**, digite: **Plug-in REST API**.
12. Em **API path prefix (Prefixo do caminho da API)**, digite: **lpr**.
13. Em **REST port (Porta REST)**, selecione **443**.

14. Em WebSDK host (Host WebSDK), digite: localhost.
15. Em WebSDK port (Porta WebSDK), selecione 443.
16. Marque a opção Allow self signed certificates (Permitir certificados autoassinados).

Em Security Center events data source (Fonte de dados de eventos do Security Center):

17. Marque Enabled (Ativada).
18. Em Name (Nome), digite Security Center Lpr Events (Eventos de Lpr do Security Center).
19. Em Processing frequency (Frequência de processamento), selecione 5 sec (5 segundos) no menu suspenso.
20. Vá para a guia Data sinks (Coletores de dados).
21. Clique em +.
22. Em Type (Tipo), selecione Database (Banco de dados).
23. Selecione e configure o banco de dados:
 - Marque Enabled (Ativada).
 - Em Source (Fonte), marque Plugin REST API (API REST do plug-in) e Native ALPR Events (Eventos ALPR nativos).
 - Em Name (Nome), digite Reads DB (Lê banco de dados).
 - Em Include (Incluir), marque Reads (Leituras), Hits (Acertos) e Images (Imagens).
 - Vá para a guia Resources (Recursos).
 - Clique em Delete the database (Excluir o banco de dados) e, em seguida, Create a database (Criar um banco de dados).

Create an API user: (Criar um usuário da API:)

24. Vá para Config Tool > User Management (Ferramenta de configuração (Gerenciamento de usuários)).
25. Clique em Add an entity (Adicionar uma entidade).
26. Selecione User (Usuário).
27. Digite um nome de usuário e uma senha. Deixe os outros campos inalterados.
28. Selecione o usuário adicionado e vá para a guia Privileges (Privilégios).
29. Marque para permitir tudo sob Application privileges (Privilégios de aplicativos).
30. Marque para permitir Third-party ALPR reads API (ALPR de terceiros lê API).
31. Clique em Aplicar.

No app AXIS License Plate Verifier:

1. Vá para Integration > Direct integration (Integração > Integração direta).
2. Selecione Genetec Security Center.
3. Em URL/IP, digite seu endereço de acordo com este modelo: `https://server-address/api/V1/lpr/lpringestion/reads`.
4. Digite o nome de usuário e a senha do Genetec.
5. Selecione Connection type (Tipo de conexão).
6. Para ativar o recurso, selecione Activate (Ativar).
7. Clique em Test (Testar) para testar a integração usando uma placa de licença virtual.
8. Caso tenha escolhido HTTPS, vá para a guia Settings (Configurações).
9. Em Security > HTTPS (Segurança > HTTPS).
10. Selecione Self-signed (Autoassinado) ou CA-signed (Assinado por CA) dependendo das configurações no Genetec Security Center.

No Genetec Security Center:

1. Vá para Genetec Security desk.
2. Em Investigation (Investigação), clique em Reads (Leituras).
3. Vá para a guia Reads (Leituras).
4. Filtre o resultado de acordo com suas necessidades.
5. Clique em Generate report (Gerar relatório).

Observação

Você também pode ler a documentação da Genetec sobre integração de plug-ins de ALPR de terceiros. *Isso pode ser feito aqui (requer registro).*

A interface Web

Para ler sobre todos os recursos e configurações disponíveis na interface Web de dispositivos com AXIS OS, vá para *Ajuda da interface Web do AXIS OS*.

Saiba mais

Tecnologia de ponta a ponta

Ponta a ponta é uma tecnologia que faz com que os dispositivos IP se comuniquem diretamente uns com os outros. Ela oferece funcionalidade de emparelhamento inteligente entre, por exemplo, câmeras Axis e produtos de áudio ou radar Axis.

Observação

Certifique-se de que os dispositivos emparelhados executem a mesma versão do AXIS OS.

Para obter mais informações, consulte o white paper "Edge-to-edge technology" (Tecnologia de ponta a ponta) em whitepapers.axis.com/edge-to-edge-technology.

Pareamento de radar

Com o pareamento de radar de ponta a ponta, você pode conectar sua câmera a um radar Axis compatível e aproveitar recursos integrados de radar, como detecção de velocidade.

O pareamento de radar é uma configuração unidirecional em que você pareia uma câmera com um radar e usa a câmera para configurar e manter ambos os dispositivos. Quando pareado, você pode acessar as configurações do radar e criar regras para eventos específicos de radar diretamente na interface Web da câmera. A câmera também se identificará para o VMS como uma câmera com funcionalidade de radar integrada.

Além disso, o stream de radar é visualizado na segunda área de exibição da câmera, chamada **área de exibição 2**. Os metadados produzidos pelo radar estão disponíveis por meio do segundo canal de produtor de metadados da câmera, chamado **canal 2**.

Pareamento de alto-falante

O pareamento de alto-falantes edge-to-edge permite usar um alto-falante em rede Axis como se ele fizesse parte da câmera. Após o pareamento, os recursos do alto-falante são integrados à interface Web da câmera e o alto-falante em rede atua como um dispositivo de saída de áudio que permite reproduzir clipes de áudio e transmitir o som pela câmera.

A câmera se identificará para o VMS como uma câmera com saída de áudio integrada e redirecionará qualquer áudio reproduzido para o alto-falante.

Área de visualização

Uma área de exibição é uma parte recortada da exibição completa. Você pode transmitir e armazenar áreas de exibição em vez da visão total para minimizar as necessidades de largura de banda e armazenamento. Se você ativar o PTZ para uma área de exibição, poderá aplicar pan, tilt e zoom nessa área. Com o uso de áreas de exibição, você pode remover partes da visão total, por exemplo, o céu.

Ao configurar uma área de exibição, recomendamos que você defina a resolução do fluxo de vídeo como o mesmo tamanho ou menor do que o tamanho da área de exibição. Se você definir a resolução do fluxo de vídeo como maior que o tamanho da área de exibição, isso significa que o vídeo será expandido digitalmente após a captura pelo sensor, o que exige mais largura de banda sem adicionar informações de imagem.

Observação

Se você parear a câmera com um radar de ponta a ponta, o stream de radar será visualizado na segunda área de exibição da câmera.

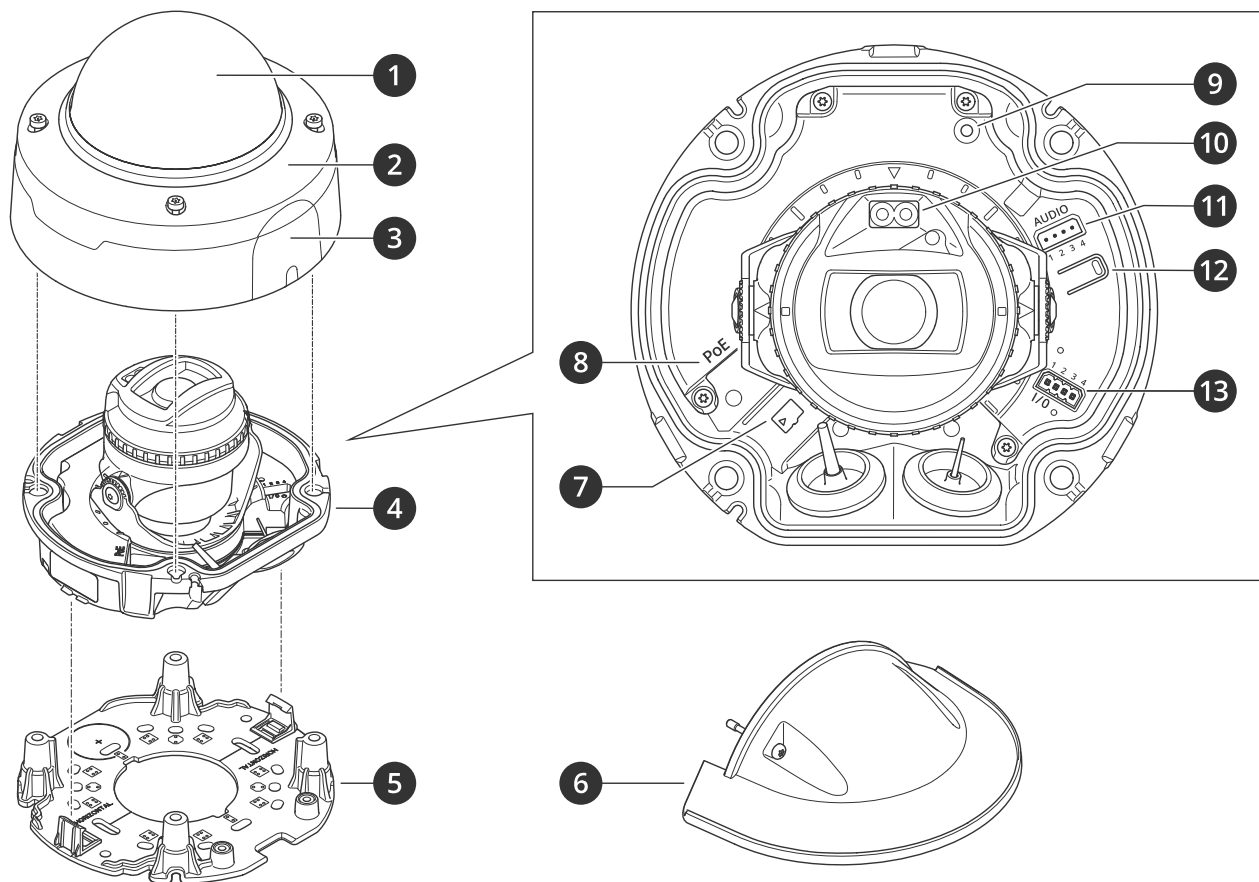
AXIS Image Health Analytics

O AXIS Image Health Analytics é um aplicativo baseado em IA que pode ser usado para detectar degradação da imagem ou tentativas de manipulação. O aplicativo analisa e aprende o comportamento da cena para detectar desfoque ou subexposição na imagem, ou para detectar uma visão obstruída ou redirecionada. É possível configurar o aplicativo para enviar eventos para qualquer uma dessas detecções e acionar ações por meio do sistema de eventos da câmera ou de software de terceiros.

Para saber mais sobre como o aplicativo funciona, consulte o *Manual do Usuário do AXIS Image Health Analytics*.

Especificações

Visão geral do produto



- 1 Dome
- 2 Cobertura dome
- 3 Tampa
- 4 Unidade da câmera
- 5 Suporte de montagem
- 6 Proteção climática
- 7 Entrada para cartão de memória SD
- 8 Conector de rede (PoE)
- 9 LED indicador de status
- 10 LED IR
- 11 Conector de áudio
- 12 Botão de controle
- 13 Conector de E/S

Indicadores de LED

LED de estado	Indicação
Apagado	Conexão e operação normais.
Verde	Permanece aceso em verde por 10 segundos para operação normal após a conclusão da inicialização.
Âmbar	Aceso durante a inicialização. Pisca durante uma atualização do software do dispositivo ou redefinição para o padrão de fábrica.
Âmbar/Vermelho	Pisca em âmbar/vermelho quando a conexão de rede não está disponível ou foi perdida.

Slot de cartão SD

OBSERVAÇÃO

- Risco de danos ao cartão SD. Não use ferramentas afiadas, objetos de metal ou força excessiva para inserir ou remover o cartão SD. Use os dedos para inserir e remover o cartão.
- Risco de perda de dados ou gravações corrompidas. Desmonte o cartão SD pela interface web do dispositivo antes de removê-lo. Não remova o cartão SD com o produto em funcionamento.

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

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



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

Botões

Botão de controle

O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte *Redefinição para as configurações padrão de fábrica, on page 49*.

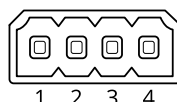
Conectores

Conector de rede

Conector Ethernet RJ45 com Power over Ethernet (PoE).

Conector de áudio

Bloco de terminais com 4 pinos para entrada e saída de áudio.



Função	Pino	Observações
GND	1	Terra
Ring power	2	12 V para fonte externa
entrada para microfone/linha	3	Microfone (analogico ou digital) ou entrada de áudio (mono). Polarização de microfone de 5 V disponível.
Saída de linha	4	Saída de áudio nível de linha (mono). Pode ser conectada a um sistema de anúncio ao público (PA) ou a um alto-falante ativo com amplificador embutido.

Conector de E/S

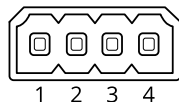
Use o conector de E/S com dispositivos externos em combinação com, por exemplo, detectores de movimento, acionadores de eventos e notificações de alarmes. Além do ponto de referência de 0 V CC e da alimentação (saída CC de 12 V), o conector do terminal de E/S fornece a interface para:

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

Entrada supervisionada – Permite detectar manipulações em entradas digitais.

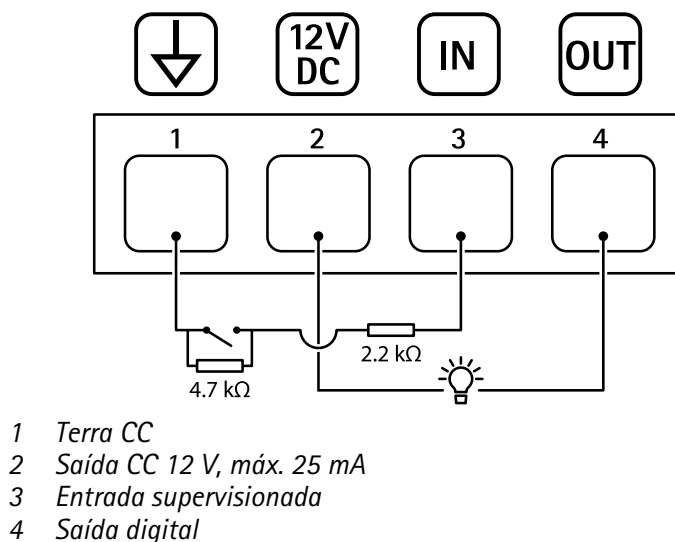
Saída digital – Para conectar dispositivos externos, como relés e LEDs. Os dispositivos conectados podem ser ativados pela interface de programação de aplicativos VAPIX®, por meio de um evento ou via interface web do dispositivo.

Bloco de terminais com 4 pinos



Função	Pino	Observações	Especificações
Terra CC	1		0 V CC
Saída CC	2	 Pode ser usada para alimentar equipamentos auxiliares. Observação: esse pino pode ser usado somente como saída de energia.	12 V CC Carga máx. = 25 mA
Entrada digital ou entrada supervisionada	3	Conecte o pino 1 para ativar ou mantenha-o flutuante (desconectado) para desativar. Para usar a entrada supervisionada, instale resistores de terminação. Veja o diagrama de conexão para obter informações de como conectar os resistores.	0 a 30 V CC máx.
Saída digital	4	Conectado internamente ao pino 1 (terra CC) quando ativo, flutuante (desconectado) quando inativo. Se usada com uma carga indutiva (por exemplo, um relé), conecte um diodo em paralelo à carga para proporcionar proteção contra transientes de tensão.	0 a 30 V CC máx., dreno aberto, 100 mA

Exemplo:



Solução de problemas

Redefinição para as configurações padrão de fábrica

⚠ AVISO

 Este produto emite radiação óptica potencialmente perigosa. Isso pode ser perigoso para os olhos. Não olhe diretamente para a lâmpada em operação.

Importante

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

Observação

A câmera foi pré-configurada com o AXIS License Plate Verifier. Se redefinir o padrão de fábrica, você manterá a chave de licença. Não será necessário reinstalar o aplicativo após uma redefinição de fábrica.

Para redefinir o produto para as configurações padrão de fábrica:

1. Desconecte a alimentação do produto.
2. Mantenha o botão de controle pressionado enquanto reconecta a alimentação. Consulte *Visão geral do produto*, on page 46.
3. Mantenha o botão de controle pressionado por cerca de 15 a 30 segundos até que o indicador do LED de estado pisque com a cor âmbar.
4. Solte o botão de controle. O processo estará concluído quando o indicador do LED de estado ficar verde. O produto foi então redefinido para as configurações padrão de fábrica. Se não houver um servidor DHCP disponível na rede, o endereço IP padrão será 192.168.0.90.
5. Use as ferramentas de software de instalação e gerenciamento para atribuir um endereço IP, definir a senha e acessar o dispositivo.
As ferramentas de software de instalação e gerenciamento estão disponíveis nas páginas de suporte em axis.com/support.

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

Opções do AXIS OS

A Axis oferece o gerenciamento de software de dispositivo de acordo com a trilha ativa ou com as trilhas de suporte de longo prazo (LTS). Estar na trilha ativa significa que você obtém acesso contínuo a todos os recursos de produtos mais recentes, enquanto as trilhas de LTS fornecem uma plataforma fixa com versões periódicas voltadas principalmente para correções de erros e atualizações de segurança.

Usar os AXIS OS da trilha ativa é recomendado se você deseja acessar os recursos mais recentes ou se você usa as ofertas de sistema ponta a ponta Axis. As trilhas de LTS são recomendados se você usa integrações de outros fabricantes, as quais podem não ser continuamente validadas com a trilha ativa mais recente. Com o LTS, os produtos podem manter a segurança cibernética sem apresentar quaisquer alterações funcionais significativas nem afetar quaisquer integrações existentes. Para obter informações mais detalhadas sobre a estratégia de software de dispositivos Axis, acesse axis.com/support/device-software.

Verificar a versão atual do AXIS OS

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

Para verificar a versão atual do AXIS OS:

1. Vá para a interface Web do dispositivo > **Status**.

2. Em Device info (Informações do dispositivo), consulte a versão do AXIS OS.

Atualizar o AXIS OS

Importante

- Ao atualizar o software do dispositivo, suas configurações pré-definidas e personalizadas serão salvas. A Axis Communications AB não pode garantir que as configurações sejam salvas, mesmo que os recursos estejam disponíveis na nova versão do AXIS OS.
- A partir do AXIS OS 12.6, é necessário instalar todas as versões LTS entre a versão atual do seu dispositivo e a versão de destino. Por exemplo, se a versão atual do software do dispositivo instalada for AXIS OS 11.2, é necessário instalar a versão LTS AXIS OS 11.11 antes de poder atualizar o dispositivo para o AXIS OS 12.6. Para obter mais informações, consulte *Guia do ciclo de vida do AXIS OS: Caminho de atualização*.
- Certifique-se de que o dispositivo permaneça conectado à fonte de alimentação ao longo de todo o processo de atualização.

Observação

- Quando você atualiza o dispositivo com a versão mais recente do AXIS OS na trilha ativa, o produto recebe a última funcionalidade disponível. Sempre leia as instruções de atualização e notas de versão disponíveis com cada nova versão antes de atualizar. Para encontrar a versão do AXIS OS e as notas de versão mais recentes, vá para axis.com/support/device-software.
1. Baixe o arquivo do AXIS OS para seu computador, o qual está disponível gratuitamente em axis.com/support/device-software.
 2. Faça login no dispositivo como um administrador.
 3. Vá para **Maintenance (Manutenção) > AXIS OS upgrade (Atualização do AXIS OS)** e clique em **Upgrade (Atualizar)**.

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

Você pode usar o AXIS Device Manager para atualizar vários dispositivos ao mesmo tempo. Descubra mais em axis.com/products/axis-device-manager.

Problemas técnicos e possíveis soluções

Problemas ao atualizar o AXIS OS

A atualização do AXIS OS falhou

Se a atualização falhar, o dispositivo recarregará a versão anterior. O motivo mais comum é que o arquivo de incorreto do AXIS OS foi carregado. Verifique se o nome do arquivo do AXIS OS corresponde ao seu dispositivo e tente novamente.

Problemas após a atualização do AXIS OS

Se você tiver problemas após a atualização, reverta para a versão instalada anteriormente na página **Maintenance (Manutenção)**.

Problemas na configuração do endereço IP

Não é possível definir o endereço IP

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

Problemas com o acesso ao dispositivo

Não é possível fazer login ao acessar o dispositivo em um navegador

Quando o HTTPS estiver ativado, certifique-se de utilizar o protocolo correto (HTTP ou HTTPS) ao tentar fazer login. Talvez seja necessário digitar manualmente `http` ou `https` no campo de endereço do navegador.

Caso tenha perdido a senha da conta root, será necessário redefinir o dispositivo para as configurações padrão de fábrica. Para obter instruções, consulte *Redefinição para as configurações padrão de fábrica, on page 49*.

O endereço IP foi alterado pelo DHCP

Os endereços IP obtidos de um servidor DHCP são dinâmicos e podem mudar. Se o endereço IP tiver sido alterado use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede. Identifique o dispositivo usando seu modelo ou número de série ou nome de DNS (se um nome tiver sido configurado).

Se necessário, é possível atribuir um endereço IP estático de forma manual. Para obter instruções, vá para axis.com/support.

Erro de certificado ao usar IEEE 802.1X

Para que a autenticação funcione corretamente, as configurações de data e hora no dispositivo Axis deverão ser sincronizadas com um servidor NTP. Vá para **System > Date and time (Sistema > Data e hora)**.

O navegador não é compatível

Para obter uma lista dos navegadores recomendados, consulte *Suporte a navegadores, on page 4*.

Não é possível acessar o dispositivo externamente

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

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

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

Problemas com a transmissão

H.264 multicast acessível somente a clientes locais

Verifique se seu roteador oferece suporte a multicasting ou se as configurações do roteador entre o cliente e o dispositivo precisam ser ajustadas. Poderá ser necessário aumentar o valor do TTL (Time To Live).

Sem H.264 multicast exibido no cliente

Verifique com seu administrador de rede se os endereços de multicast usados pelo dispositivo Axis são válidos para sua rede.

Verifique com seu administrador de rede se há um firewall impedindo a visualização.

Renderização ruim de imagens H.264

Verifique se sua placa gráfica está usando o driver mais recente. Normalmente, é possível baixar os drivers mais recentes do site do fabricante.

A saturação de cores é diferente entre H.264 e Motion JPEG

Modifique as configurações da sua placa gráfica. Consulte a documentação do adaptador para obter mais informações.

Taxa de quadros inferior à esperada

- Consulte *Considerações sobre desempenho, on page 54*.
- Reduza o número de aplicativos em execução no computador cliente.
- Limite o número de visualizadores simultâneos.
- Verifique junto ao administrador de rede se há largura de banda suficiente disponível.
- Reduza a resolução da imagem.
- Faça login na interface Web do dispositivo e defina um modo de captura que priorize a taxa de quadros. Se você alterar o modo de captura para priorizar a taxa de quadros, poderá reduzir a resolução máxima dependendo do dispositivo usado e dos modos de captura disponíveis.

Não é possível selecionar a codificação H.265 na visualização ao vivo.

Os navegadores da Web não oferecem suporte à decodificação H.265. Use um aplicativo ou sistema de gerenciamento de vídeo que ofereça suporte à decodificação H.265.

Problemas com MQTT

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

O firewall bloqueia o tráfego que utiliza a porta 8883, uma vez que é considerado inseguro.

Em alguns casos, o servidor/broker pode não fornecer uma porta específica para a comunicação MQTT. Ainda será possível usar MQTT em uma porta normalmente usada para tráfego HTTP/HTTPS.

- Se o servidor/broker suporta WebSocket/WebSocket Secure (WS/WSS), geralmente na porta 443, use este protocolo em vez do MQTT. Verifique com o provedor do servidor/broker para saber se o WS/WSS é suportado e qual porta e caminho base devem ser usados.
- Se o servidor/corretor suportar ALPN, o uso do MQTT poderá ser negociado em uma porta aberta, como a 443. Verifique com seu provedor de servidor/corretor se há suporte para ALPN e qual protocolo e porta ALPN usar.

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

Veículos desconhecidos marcados como aceitos

Se o aplicativo permitir a entrada de veículos com placas que não estejam na lista de permissão, uma razão provável é que a comparação permite a variação de um caractere.

Por exemplo, se **AXI S1234** estiver na lista de permissão, o aplicativo aceitará **AXI SI234**.

Da mesma forma, se **AXIS 1234** estiver na lista de permissão, o aplicativo aceitará **AXI 1234**.

Vá para *Configurações adicionais*, on page 25 para definir os caracteres permitidos.

A conexão entre o aplicativo e controlador ou o módulo de relé não funciona

Certifique-se de que o controlador ou o módulo de relé permita tráfego de dados por HTTP. Para saber como alterar essa configuração, acesse o manual do usuário do dispositivo correspondente.

Problemas com pareamento de radares

Não consigo parear a câmera com o radar.	Certifique-se de que a segunda área de exibição da câmera (View area 2 [Área de exibição 2]) não seja usada, pois o radar será atribuído a ela automaticamente. Se a segunda área de exibição for usada, vá para Video > View areas (Vídeo > Áreas de exibição) para removê-la e, em seguida, tente parear os dispositivos novamente.
Os veículos em movimento na exibição da câmera não estão sincronizados com as sobreposições de velocidade ou com as faixas na visão do radar	Certifique-se de que a câmera e o radar estejam com o tempo sincronizado. Para verificar o status, vá para Status > Time sync status (Status > Status de sincronização de horário) na interface Web de cada dispositivo. Se o status mostrar Synchronized: No (Sincronizado: não), clique em NTP settings (Configurações de NTP) e selecione uma fonte de horário para sincronizar o dispositivo. Use a mesma fonte de hora para ambos os dispositivos.
A segunda área de exibição da câmera não mostra o stream de radar corretamente	A resolução padrão do radar após o emparelhamento de borda a borda é 1280x720, tanto na interface web da webcam quanto em um VMS. Se você selecionar outra resolução, o stream do radar aparecerá incorretamente. Para ajustar a resolução do radar, vá para Video > Stream > General (Vídeo > Stream > Geral) na interface Web da câmera e selecione View area 2 (Área de exibição 2).

Problemas com sobreposições	
As sobreposições que adicionei por meio da interface Web da câmera desaparecem após o pareamento com o radar	Se você adicionou mais de uma área de exibição na câmera, quaisquer sobreposições anteriormente adicionadas desaparecerão da interface Web da câmera. Como o radar ocupará a segunda área de exibição após o pareamento, todas as sobreposições existentes na interface Web da câmera desaparecerão. As sobreposições desaparecerão somente da interface Web. Você ainda pode solicitar um stream contendo as sobreposições, por exemplo, em um VMS.
As sobreposições de placas de licença que eu adicionei no AXIS License Plate Verifier não aparecem	Se você adicionou sobreposições que mostram a velocidade do veículo no AXIS Speed Monitor e, em seguida, ativou sobreposições de placas de licença no AXIS License Plate Verifier, as sobreposições de placas de licença não são exibidas. Ative as sobreposições no AXIS License Plate Verifier antes de adicionar sobreposições de velocidade por meio do AXIS Speed Monitor.

Considerações sobre desempenho

Ao configurar seu sistema, é importante considerar como diferentes configurações e situações afetam o desempenho. Alguns fatores afetam a largura de banda (taxa de bits), outros afetam a taxa de quadros e alguns afetam ambos.

Os fatores mais importantes a serem considerados são:

- Alta resolução de imagem ou níveis de compactação menores geram imagens com mais dados que, por sua vez, afetarão a largura de banda.
- Girar a imagem na GUI poderá aumentar a carga sobre a CPU do produto.
- O acesso por um grande número de clientes H.264/H.265/AV1 unicast ou Motion JPEG pode afetar a largura de banda.
- A exibição simultânea de diferentes streams (resolução, compactação) por diferentes clientes afeta a taxa de quadros e a largura de banda.
Use streams idênticos sempre que possível para manter uma alta taxa de quadros. Perfis de stream podem ser usados para garantir que streams sejam idênticos.
- O acesso a streams de vídeo com diferentes codecs afeta simultaneamente a taxa de quadros e a largura de banda. Para obter o desempenho ideal, use streams com o mesmo codec.
- O uso pesado de configurações de eventos afeta a carga da CPU do produto que, por sua vez, impacta a taxa de quadros.
- Usar HTTPS pode reduzir a taxa de quadros, especialmente se houver transmissão de Motion JPEG.
- A utilização pesada da rede devido à infraestrutura ruim afeta a largura de banda.
- A exibição em computadores clientes com desempenho ruim reduz o desempenho percebido e afeta a taxa de quadros.
- Executar vários aplicativos AXIS Camera Application Platform (ACAP) simultaneamente pode afetar a taxa de quadros e o desempenho geral.

Entre em contato com o suporte

Se precisar de ajuda adicional, acesse axis.com/support.

Cibersegurança

A segurança cibernética oferece suporte a um ciclo de vida de produto bem-sucedido com riscos minimizados. Você pode encontrar informações e documentação detalhadas sobre nossa abordagem de segurança cibernética em axis.com/about-axis/cybersecurity. Siga as diretrizes de segurança cibernética abaixo para receber notificações de segurança de produtos da Axis e para configurar seu produto para um ciclo de vida e desativação seguros.

No *Axis Trust Center*, você pode encontrar informações sobre como a Axis implementa a conformidade de segurança, a transparência, a proteção de dados e a privacidade.

Gerenciamento de vulnerabilidades

A Axis é uma *Autoridade de numeração de vulnerabilidades e exposições comuns (CVE) (CNA)*. Para minimizar seu risco de exposição, seguimos os padrões do setor ao identificar e resolver vulnerabilidades em nossos dispositivos, software e serviços. Consulte axis.com/vulnerability-management para obter informações sobre nossa política de gerenciamento de vulnerabilidades ou para relatar uma vulnerabilidade.

Notificações de segurança

Assine os e-mails de notificação de segurança da Axis em axis.com/security-notification-service. Enviaremos a você informações sobre vulnerabilidades, avisos de segurança correspondentes e outros assuntos relacionados à segurança de seu produto Axis.

Ciclo de vida seguro do produto

A Axis minimiza os riscos durante toda a vida útil de nossos produtos por meio do gerenciamento seguro do ciclo de vida. Use nossos guias para aumento do nível de proteção em help.axis.com para configurar e operar com mais segurança seus produtos Axis e para encontrar informações sobre:

Uso seguro desde o primeiro uso – Os produtos Axis são pré-configurados com alta proteção padrão para permitir a inicialização segura e a comunicação criptografada desde o início.

Uso pretendido e erros comuns de configuração – Nossos guias fornecem informações sobre o uso pretendido dos produtos Axis, incluindo erros comuns de configuração e usos indevidos relevantes para a segurança que devem ser evitados.

Gerenciamento de vulnerabilidades e transparência da cadeia de suprimentos – Uma lista de materiais de software (SBOM) é publicada com cada versão de software em axis.com para divulgar vulnerabilidades e aumentar a transparência da cadeia de suprimentos.

Descomissionamento e exclusão segura de dados – Para desativar um produto com segurança quando ele chegar ao fim de seu ciclo de vida, redefina-o para as configurações padrão de fábrica. Isso apaga suas configurações, dados armazenados e informações confidenciais.

T10191705_pt

2026-07 (M16.2)

© 2023 – 2026 Axis Communications AB