AXIS P1445-LE-3 License Plate Verifier Kit

Manual do Usuário

Índice

Sobre o produto 4
Início 5
Configuração básica 5
Recomendações de montagem da câmera 5
Assistente de configuração 7
Fluxo livre 7
Controle de acesso 8
Como acessar a página Web do produto 9
Criar uma conta de administrador 9
Senhas seguras 10
Instalação 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 12
Instalação 13
Modo de visualização 13
Gerenciar listas 14
Adicionar placa de licença detectada à lista 14
Adicionar descrições a placas de licença 14
Personalização de nomes de listas 14
Importação de números de placas de licença na lista de permissão 14
Compartilhamento de listas de placas de licença com outras câmeras 15
Agendar listas 15
Configurações adicionais 16
Configurar sobreposição de texto 16
Detecção de placas de licença em condições de pouca iluminação 16
Permitir menos caracteres nas placas de licença 16
Permitir somente correspondências exatas de placas de licença 16
Permitir o desvio de mais de um caractere ao comparar placas de licença 16
Fornecer acesso limitado aos operadores 17
Configuração de uma conexão segura 17
Limpar todos os eventos 17
Usar portas virtuais para acionar ações 17
Cenário de entrada e saída de veículos 19
Abertura de uma barreira para veículos conhecidos usando um módulo de relé 19
Abertura de uma barreira para veículos conhecidos usando a E/S da câmera 20
Recebimento de notificação sobre um veículo não autorizado 21
Cenário de controle de acesso de veículos 22
Conexão a um controlador de porta 22
Conectar ao AXIS Secure Entry 24
Integração 26
Use perfis para enviar eventos por push para vários servidores 26
Informações sobre eventos push para software de outros fabricantes 26
Envio de imagens de placas de licença para um servidor 26
Integração direta com 2N 27
Integração ao Genetec Security Center 28
A interface Web 30
..... 30
Status 30
..... 31
..... 31
Vídeo 32

Instalação 34
Imagem 36
Stream 42
Sobreposições 45
Áreas de visualização 47
Máscaras de privacidade 47
Áudio 47
Configurações do dispositivo 47
Stream 48
Clipes de áudio 48
Gravações 49
Apps 50
..... 50
Sistema 50
Hora e local 50
Rede 52
Segurança 56
Contas 60
Eventos 62
MQTT 67
Armazenamento 70
SIP 72
Perfis de stream 76
ONVIF 77
Metadados de analíticos 80
Detectores 80
Saída de vídeo 81
Configurações de energia 81
Acessórios 81
Edge-to-edge 82
Logs 83
Configuração simples 84
Manutenção 85
Especificações 86
Visão geral do produto 86
..... 86
Indicadores de LED 86
Slot de cartão SD 86
Botões 87
Botão de controle 87
Conectores 87
Conector de rede 87
Conector de áudio 87
Conector de E/S 87
Limpeza do dispositivo 89
Solução de problemas 90
..... 90
Para usuários do AXIS Camera Station 90
Configurar o AXIS License Plate Verifier 90
Problemas técnicos, dicas e soluções 90
Redefinição para as configurações padrão de fábrica 93
Atualizar o AXIS OS 93
Considerações sobre desempenho 94

Sobre o produto

O AXIS P1445-LE-3 License Plate Verifier Kit consiste em uma AXIS P1445-LE Network Camera e um aplicativo pré-instalado AXIS License Plate Verifier, o que faz dele um kit para o gerenciamento automatizado da entrada e saída de veículos. O AXIS P1445-LE-3 usa uma lista de permissão e uma lista de bloqueio para verificar o acesso às áreas controladas, como os estacionamentos.

Início

Configuração básica

Estas instruções de configuração são válidas para câmeras que não são vendidas como um kit com o AXIS License Plate Verifier

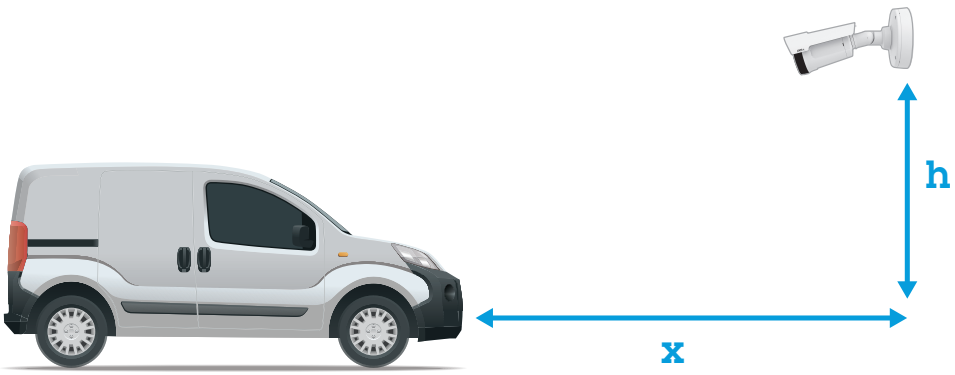
1.
2.

Estas instruções de configuração são válidas para todos os cenários:

1.
2.
3.
4.
5.

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.



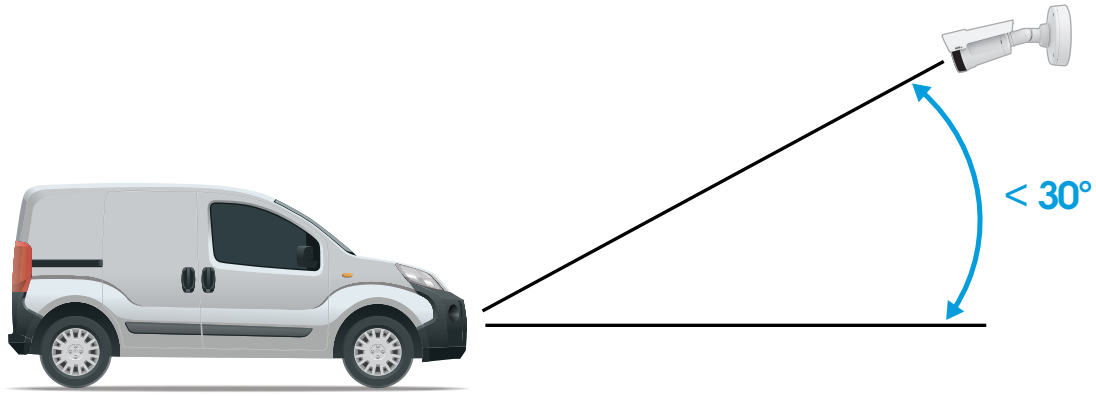
Distância de captura de **controle de acesso**: 2-7 m (6,6-23 pés). Este exemplo baseia-se no AXIS P3265-LVE-3 License Plate Verifier Kit.

Distância de captura: (x)	Altura de montagem (y)
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)

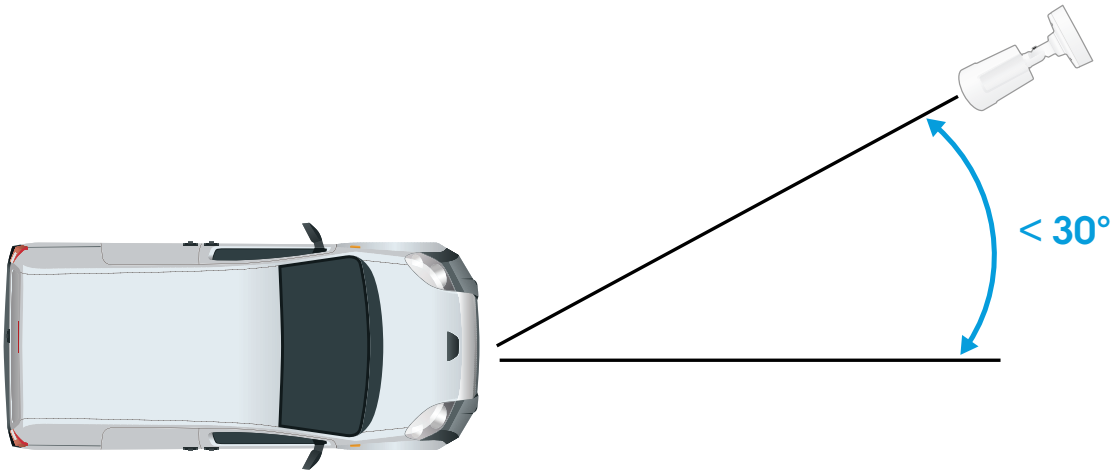
Distância de captura de **fluxo livre**: 7-20m (23-65 pés). Este exemplo baseia-se no AXIS P1465-LE-3 License Plate Verifier Kit.

Distância de captura (x)	Altura de montagem (y)
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.

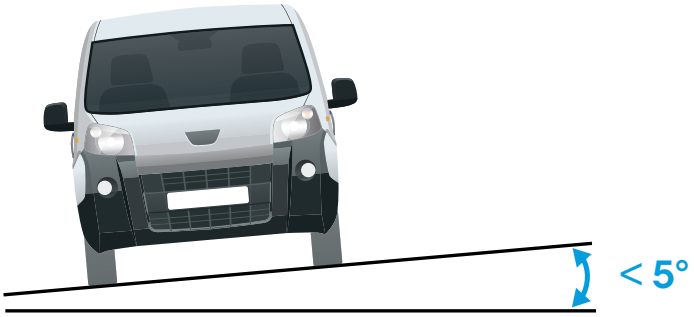


Ângulo de montagem a partir do lado.



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 no stream em tempo real.



Inclinação horizontal.

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. Se desejar fazer alterações posteriormente, ela poderá ser encontrada na guia **Settings (Configurações)** no **Setup assistant (Assistente de configuração)**.

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 .
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 .
    - **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 .
4. Arraste os pontos de ancoragem para ajustar a área de interesse. Consulte .
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: .

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)**.

Como acessar a página Web do produto

Se você não souber o endereço IP do seu produto, use o AXIS IP Utility ou o AXIS Device Manager para localizar o produto na rede. Ambos os aplicativos são grátis e podem ser baixados de *axis.com/support*

Os seguintes navegadores são recomendados:

- Chrome™
- Firefox®

1. Inicie o navegador da Web.
2. Insira o endereço IP ou o nome de host do produto Axis no campo de endereço do navegador.
3. Insira o nome de usuário e a senha. Se esta for a primeira vez que você acessa o produto, você deverá configurar a senha de root primeiro.
4. Se esta for a primeira vez que você acessa o produto, você será solicitado a fazer algumas configurações iniciais. Quando estiver pronto, a página de exibição ao vivo do produto será aberta em seu navegador.

Para obter mais informações sobre como descobrir e atribuir endereços IP, consulte o documento Como atribuir um endereço IP e acessar o dispositivo na página do produto em *axis.com*

Criar uma conta de administrador

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

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

Importante

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

Senhas seguras

Importante

Os dispositivos Axis enviam a senha definida inicialmente na forma de texto plano via rede. Para proteger seu dispositivo após o primeiro login, configure uma conexão HTTPS segura e criptografada e altere a senha.

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.

Instalação do aplicativo

Observação

As câmeras P1445-LE-3, P3245-LE-3 e P1455-LE-3 são fornecidas com o AXIS License Plate Verifier pré-instalado no firmware.

Observação

Para instalar o aplicativo no dispositivo, você precisará de direitos de administrador.

1. Vá para a página Web do dispositivo.
2. Vá para **Settings > Apps (Configurações > Aplicativos)**.
3. Clique em **Add (Adicionar)** para carregar o arquivo do aplicativo (.eap) na câmera.

Para ativar a licença, você precisará de uma chave de licença que é gerada pelo código da licença e do número de série do dispositivo Axis. Se você não tiver uma chave de licença no computador, faça o seguinte:

1. Vá para *axis.com/support/license-key-registration#/registration*
2. Insira o número de série e o código da licença.
3. Salve o arquivo da chave da licença no computador. Navegue para selecionar o arquivo e clique em **Activate (Ativar)**.

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:

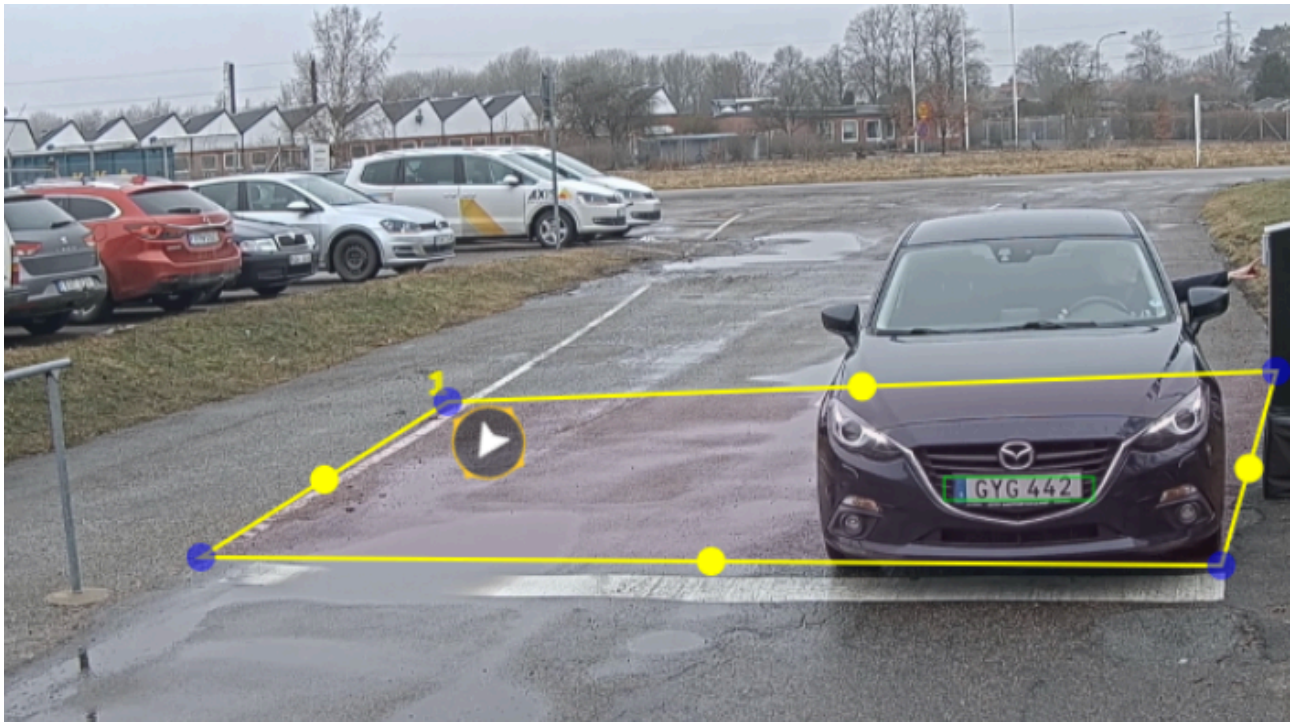
1. Vá para **Settings (Configurações)**.
2. Clique em **Edit area of interest (Editar área de interesse)**.
3. Para aprimorar a verificação e as imagens capturadas, vá para **Zoom** e ajuste o controle deslizante de acordo com as suas necessidades.
4. Para que a câmera foque automaticamente nos veículos, clique em **Autofocus (Foco automático)**. Para definir o foco manualmente, vá para **Focus (Foco)** e ajuste-o com o controle deslizante.
5. Para mover a área de interesse, clique em qualquer lugar da área e arraste-a para onde as placas de licença sejam mais visíveis. Se você deslocar a área de interesse para fora da visualização ao vivo, ela retornará automaticamente para a posição padrão. Certifique-se de que a região de interesse permaneça na posição depois de ter salvado as configurações.
6. Para ajustar a área de interesse, clique em qualquer lugar na área e arraste os pontos de ancoragem destacados em azul.
   - Para redefinir a área de interesse, clique com o botão direito dentro da área e selecione **Reset (Redefinir)**.

- Para adicionar pontos de ancoragem, clique em um dos pontos de ancoragem amarelos. O ponto de ancoragem se tornará azul, mostrando que pode ser manipulado. Novos pontos amarelos são adicionados automaticamente ao lado do ponto de ancoragem azul. O número máximo de pontos de ancoragem azuis é oito.

7. Clique em qualquer lugar fora da área de interesse para salvar suas alterações.
8. Para obter uma resposta de direção correta no **Event log (Log de eventos)**, gire a seta para corresponder à direção de condução.
   8.1. Clique no ícone de seta.
   8.2. Selecione o ponto de ancoragem e gire a seta para que ela se alinhe à direção de condução.
   8.3. 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)**.

- Para adicionar uma segunda área de interesse, selecione **2** no menu suspenso **Area of interest (Área de interesse)**.



Exemplo com uma área de interesse.

Observação

- Se você estiver usando uma câmera independente, o aplicativo poderá definir as configurações recomendadas para o reconhecimento da placa de licença.
  1. Clique em **Recommended LPR settings (Configurações de LPR recomendadas)**. Você verá uma tabela onde as configurações atuais e as configurações recomendadas são diferentes.
  2. Clique em **Update settings (Atualizar configurações)** para que o app altere as configurações dos valores recomendados.

Selecionar região

1. Vá para **Settings (Configurações)** > **Image (Imagem)**.
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 **Resolution (Resolução)**.
3. Para alterar a rotação da imagem capturada, vá para **Image rotation (Rotação da imagem)**.
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.

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 (Configurações)** > **Events (Eventos)**.
2. Em **Save events (Salvar eventos)**, selecione **Allowlisted (Na lista de permissão)**.
3. Em **Delete events after (Excluir eventos após)**, selecione **30 days (30 dias)**.

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.

Para alterar as configurações de captura de imagem, vá para **Settings > Image (Configurações > Imagem)**. 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.



Este vídeo demonstra como usar o modo de visualização.

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 na guia **Event log (Log de eventos)**.
2. Vá para **Latest Event (Último evento)**.
3. Clique em **Add to list (Adicionar à lista)** próximo à placa de licença que deseja adicionar.
4. Selecione a lista à qual deseja adicionar a placa de licença no menu suspenso de listas.
5. Clique em **Append (Anexar)**.

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 que deseja editar e clique no ícone de caneta.
- Digite as informações relevantes no campo **Description (Descrição)**, na parte superior da lista.
- Clique no ícone de disco para salvar.

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. Vá para o menu de listas da lista que deseja alterar.
3. Selecione **Rename (Renomear)**.
4. Digite o nome da lista.

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`

1. Vá para **List management (Gerenciamento de listas)**.
2. Vá para o menu de contexto ao lado de **Allowlist (Lista de permissão)** e selecione **Import from file (Importar de arquivo)**.
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 (Gerenciamento de listas)**.
2. Em **Camera synchronization (Sincronização da câmera)**, digite o endereço IP, o nome de usuário e a senha.
3. Clique em **+**.
4. Clique em **Camera synchronization (Sincronização da câmera)**.
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)**.
- Vá para o menu de listas da lista que deseja agendar.
- Selecione **Schedule (Agendar)** no menu pop-up.
- 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. Defina a **Overlay duration (Duração da sobreposição)** como um valor entre 1 e 9 segundos.
4. Selecione a data, a hora e a placa de licença (**Datetime + LP (Data e hora + PL)**) ou apenas a placa de licença (**LP (PL)**).
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 pelo algoritmo. Isso é chamado de nível de sensibilidade (parâmetro de confiança). As detecções com pontuação inferior ao valor do nível selecionado não são mostradas na lista de eventos.

Para cenas com iluminação reduzida, é possível baixar o nível de sensibilidade.

1. Vá para **Settings (Configurações)** > **Detection parameters (Parâmetros de detecção)**.
2. Ajuste o controle deslizante sob **Sensitivity level (Nível de sensibilidade)**. Para evitar detecções falsas, recomendamos reduzir o valor do limite em 0,05 de cada vez.
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 (Configurações)** > **Detection parameters (Parâmetros de detecção)**.
2. No campo **Minimum number of characters (Número mínimo de caracteres)**, digite 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 (Configurações)** > **Detection parameters (Parâmetros de detecção)**.

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 **Enable HTTPS (Ativar HTTPS)**.
3. Selecione **Self-signed (Autoassinado)** ou **CA-signed (Assinado pela CA)**.

Observação

Saiba mais sobre HTTPS e como usá-lo em .

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 .

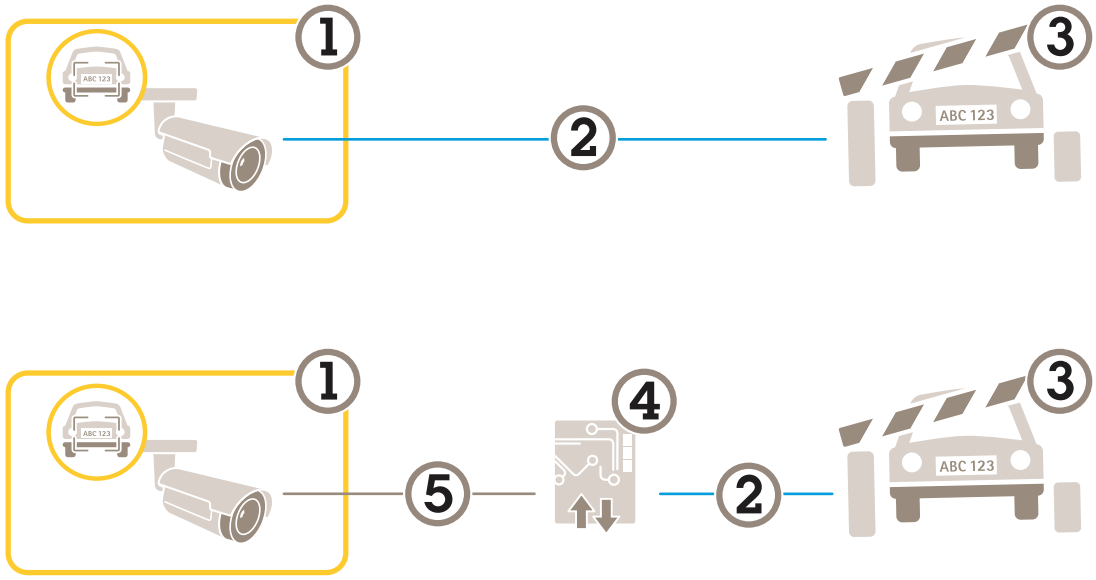
1. Vá para a página Web do aplicativo e selecione a guia **Settings (Configurações)**.
2. Vá para **Access control (Controle de acesso)**.
3. Em **Access control (Controle de acesso)**, selecione a lista suspensa **Type (Tipo)** e, em seguida, **Internal I/O (E/S interna)**.
4. Selecione a **I/O output # (Saída de E/S #)**.
5. Selecione uma porta na lista suspensa **Virtual port (Porta virtual)**.
6. Na lista suspensa **Barrier mode (Modo de barreira)**, selecione **Open to all (Abrir para todos)**.
7. Na lista suspensa **Vehicle direction (Direção do veículo)** selecione **any (qualquer)**.
8. Na lista suspensa **ROI (Região de interesse)**, selecione a área de interesse que gostaria de usar ou se deseja usar a área inteira.

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 .

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 .



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

1. Vá para a página da Web do aplicativo, selecione a guia **Event log (Log de eventos)** e, em seguida, adicione placas de licença detectadas a uma lista. Consulte
2. Para editar as listas diretamente, vá para a guia **List management (Gerenciamento de listas)**.
3. Insira os números das placas autorizadas no campo **Allowlist (Lista de permissão)**.
4. Vá para a guia **Settings (Configurações)**.
5. Em **Access control (Controle de acesso)**, selecione a lista suspensa **Type (Tipo)** e, em seguida, **Internal I/O (E/S interna)**.
6. Selecione a **I/O output # (Saída de E/S #)**.
7. 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)**.
8. Na lista suspensa **Vehicle direction (Direção do veículo)** selecione **in (entrando)**.
9. Na lista suspensa **ROI (Região 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:

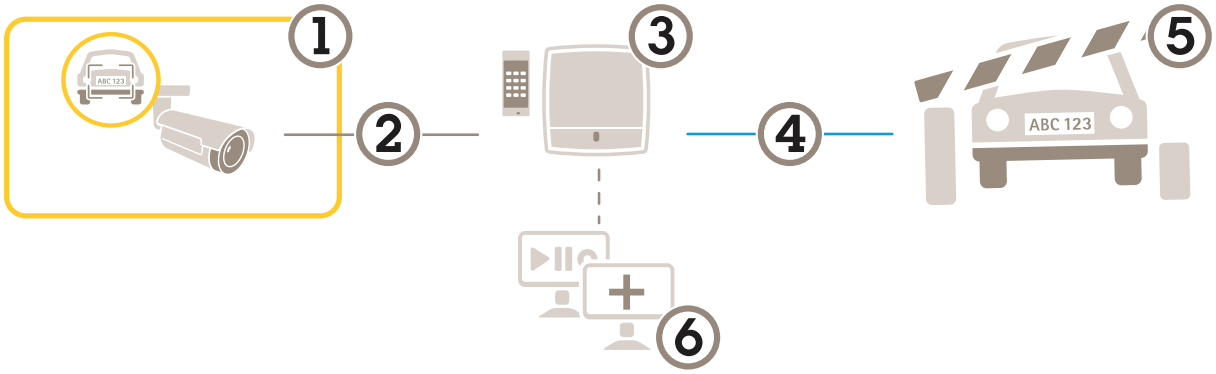
- Configuração básica pronta. Consulte a .

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 .

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

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)**.

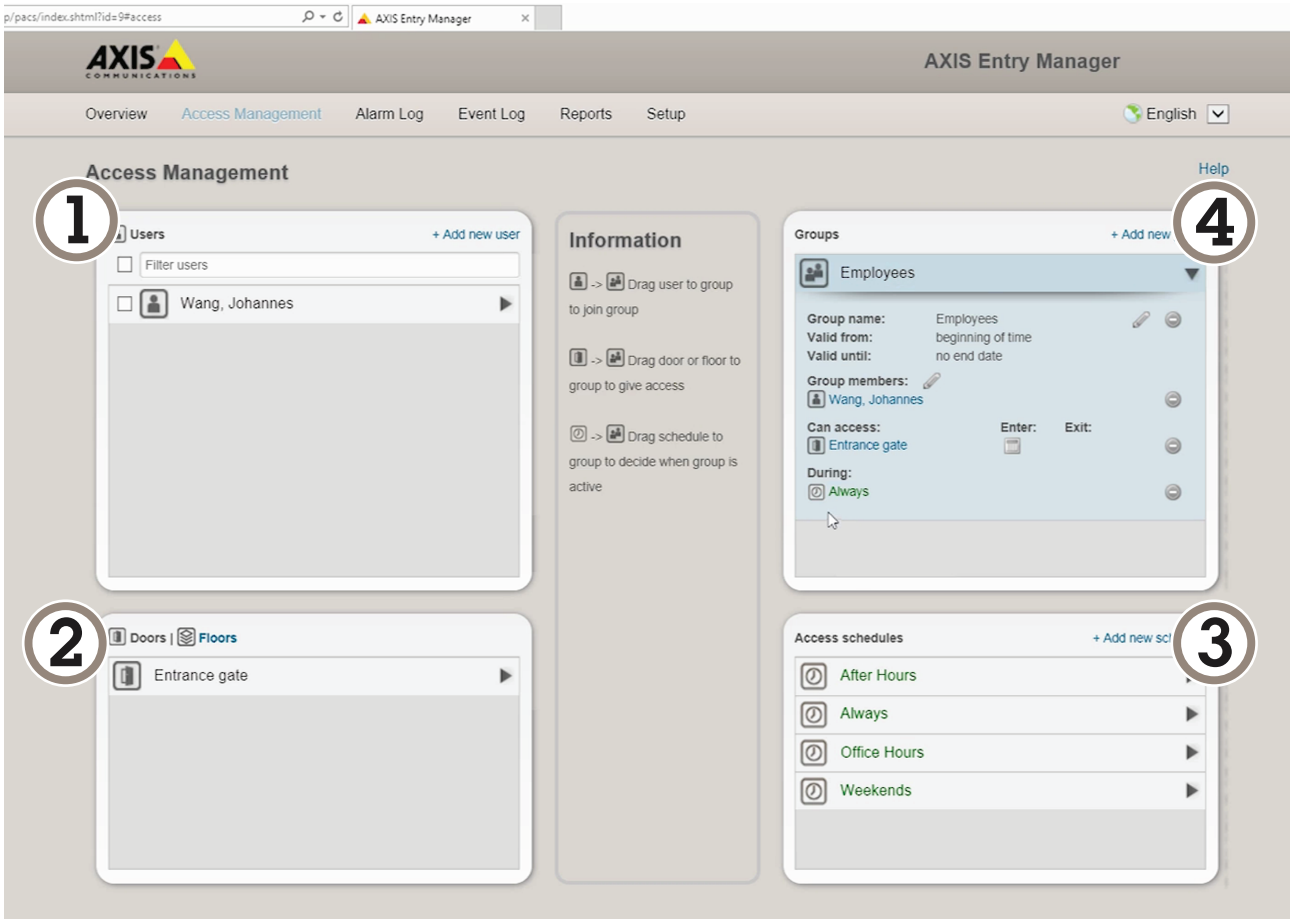
5. Clique em **Next** (Próximo).
6. Em **Configure readers connected to this controller (Configurar leitores conectados a este controlador)**, desmarque a opção **Exit reader (Sair do leitor)**.
7. Clique em **Finish (Concluir)**.

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 .

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 .
15. Clique em **Next (Avançar)** duas vezes e, em seguida, em **Finish (Concluir)**.

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. Selecione um perfil no menu suspenso **Profiles (Perfis)**.
2. Configure a regra. Consulte .
3. Clique em "Salvar".
4. Selecione um novo perfil no menu suspenso **Profiles (Perfis)**.

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. Na lista suspensa **Protocol (Protocolo)**, selecione um dos seguintes protocolos:
   - TCP
   - HTTP POST
     - Digite o nome de usuário e a senha.
3. No campo **Server URL (URL do servidor)**, digite o endereço e a porta do servidor no seguinte formato: `127.0.0.1:8080`
4. No campo **Device ID (ID do dispositivo)**, digite o nome do dispositivo ou deixe-o como está.
5. 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.
6. Para ativar o recurso, selecione **Send event data to server (Enviar dados de eventos para o servidor)**.
7. 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)**.
8. Clique em **Salvar**.

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 o campo **Auth-Header (Cabeçalho de autorização)** e adicionar um caminho a 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. 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.
5. Digite o nome de usuário e a senha para o servidor FTP.
6. Selecione os modificadores de caminho e nome para os nomes de arquivos.
7. Clique em **Pronto**.
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.

   Observação

   A direção é incluída somente no nome do arquivo quando as opções **Lost (Perdido)** ou **Update (Atualizado)** são selecionadas.
9. Para ativar o recurso, selecione **Send event data to server (Enviar dados de eventos para o servidor)**.
10. Clique em **Salvar**.

Observação

Observe que a imagem varia dependendo do tipo de modo de captura selecionado. Consulte .

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. Adicione o endereço IP ou URL ao dispositivo 2N.

3. Selecione **Connection type (Tipo de conexão)**.
4. Selecione o motivo do uso da barreira em **Barrier is used for (A barreira é usada para)**.
5. Digite seu nome de usuário e senha.
6. Clique em **Enable integration (Permitir integração)**.
7. Clique em **Salvar**.

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 cerificados 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 a guia **Integration (Integração)**.
2. Selecione **Genetec Security Center** na lista suspensa.
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. Clique em **Enable integration (Permitir integração)**.
6. Vá para a guia **Settings (Configurações)**.
7. Em **Security > HTTPS (Segurança > HTTPS)**.
8. 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 alcançar a interface Web do dispositivo, digite o endereço IP do dispositivo em um navegador da Web.

Observação

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

 Mostre ou oculte o menu principal.

 Acesse as notas de versão.

 Acesse a ajuda do produto.

 Altere o idioma.

 Defina o tema claro ou escuro.

 O menu de usuário contém:

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

 O menu de contexto contém:

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

Status

Status de sincronização de horário

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

NTP settings (Configurações de NTP): Exiba e atualize as configurações de NTP. Leva você para a página **Date and time (Data e hora)** na qual é possível alterar as configurações de NTP.

Informações do dispositivo

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

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

RAM use (Uso de RAM): Percentual de RAM utilizado.

CPU use (Uso de CPU): Percentual de CPU utilizado.

GPU use (Uso de GPU): Percentual de GPU utilizado.

GPU bus use (Uso do barramento da GPU): Percentual do barramento da GPU utilizado.

Decoding process (Processo de decodificação): Status atual do processo de decodificação, Running (Em execução) ou Stopped (Parado).

Endereço IP: O endereço IP do dispositivo.

Date and time (Data e hora): A data e a hora do dispositivo.

Gravação em andamento

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

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

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

Clientes conectados

Mostra o número de conexões e os clientes conectados.

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

Vídeo

Clique para reproduzir o stream de vídeo ao vivo.

Clique para congelar o stream de vídeo ao vivo.

Clique para obter uma captura instantânea do stream de vídeo ao vivo. O arquivo é salvo na pasta "Downloads" do seu computador. O nome do arquivo de imagem é [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]. O tamanho real do instantâneo depende da compactação que é aplicada do mecanismo de navegador da Web específico no qual o instantâneo é recebido. Portanto, o tamanho do instantâneo pode variar com a configuração de compactação real que é configurada no dispositivo.

Clique para mostrar as portas de saída de E/S. Use a chave para abrir ou fechar o circuito de uma porta, por exemplo, com o intuito de testar dispositivos externos.

Clique para ativar ou desativar manualmente a iluminação IR.

Clique para ativar ou desativar manualmente a luz branca.

Clique para acessar os controles na tela:

- **Predefined controls (Controles predefinidos)**: ative para usar os controles na tela disponíveis.
- **Custom controls (Controles personalizados)**: Clique em **Add custom control (Adicionar controle personalizado)** para adicionar um controle na tela.

Inicia o lavador. Quando a sequência é iniciada, a câmera se move para a posição configurada para receber o spray de lavagem. Quando toda a sequência de lavagem é concluída, a câmera retorna para sua posição anterior. Esse ícone só é visível quando o lavador está conectado e configurado.

Inicia o limpador.

Clique e selecione uma posição predefinida para ir para a posição predefinida na visualização ao vivo. Ou clique em **Setup (Configuração)** para ir para a página da posição predefinida.

Adiciona ou remove uma área de recuperação de foco. Quando uma área de recuperação de foco é adicionada, a câmera salva as configurações de foco naquela faixa de pan/tilt específica. Quando você define uma área de recuperação de foco e a câmera entra nessa área na visualização ao vivo, a câmera recupera o foco salvo anteriormente. É suficiente cobrir metade da área para a câmera recuperar o foco.

Clique para selecionar um guard Tour e, em seguida, clique em **Start (Iniciar)** para executar o guard tour. Ou clique em **Setup (Configuração)** para ir para a página guard tours.

Clique para ativar manualmente o aquecedor durante um período selecionado.

Clique para iniciar uma gravação contínua do stream de vídeo ao vivo. Clique novamente para parar a gravação. Se uma gravação estiver em andamento, ela será retomada automaticamente depois de uma reinicialização.

Clique para exibir o armazenamento configurado para o dispositivo. Para configurar o armazenamento, você deve estar conectado como administrador.

Clique para acessar mais configurações:

- **Formato de vídeo**: selecione o formato de codificação que será usado na visualização ao vivo.
- **Autoplay (Reprodução automática)**: ative para reproduzir automaticamente um stream de vídeo sem som sempre que você abrir o dispositivo em uma nova sessão.
- **Client stream information (Informações de stream do cliente)**: ative para exibir informações dinâmicas sobre o stream de vídeo usado pelo navegador que apresenta o stream de vídeo ao vivo. As informações de taxa de bits são diferentes das informações apresentadas em uma sobreposição de texto devido às diferentes fontes de informações. A taxa de bits nas informações do stream do cliente é a taxa de bits do último segundo, proveniente do driver de codificação do dispositivo. A taxa de bits na sobreposição é a taxa de bits média nos últimos 5 segundos, proveniente do navegador. Os dois valores cobrem apenas o stream de vídeo bruto, sem a largura de banda adicional gerada ao ser transportado pela rede via UDP/TCP/HTTP.
- **Adaptive stream (Stream adaptativo)**: ative para adaptar a resolução da imagem à resolução real do cliente de exibição, a fim de aprimorar a experiência do usuário e impedir uma possível sobrecarga do hardware do cliente. O stream adaptativo é aplicado somente ao visualizar o stream de vídeo ao vivo na interface da Web em um navegador. Quando o stream adaptativo está ativado, a taxa de quadros máxima é 30 fps. Se você capturar um instantâneo com o stream adaptativo ativado, será usada a resolução de imagem selecionada pelo stream adaptativo.
- **Level grid (Grade de nível)**: Clique em para exibir a grade de nível. Essa grade ajuda você a decidir se a imagem está alinhada horizontalmente. Clique em para ocultá-la.
- **Pixel counter (Contador de pixels)**: Clique em para mostrar o contador de pixels. Arraste e redimensione a caixa para acomodar sua área de interesse. Você também pode definir o tamanho em pixels da caixa nos campos **Width (Largura)** e **Height (Altura)**.
- **Refresh (Atualizar)**: Clique em para atualizar a imagem estática na visualização ao vivo.
- **Controles de PTZ** : Ative para exibir controles de PTZ na visualização ao vivo.

Clique para mostrar a visualização ao vivo na resolução máxima. Se a resolução máxima for maior que o tamanho da sua tela, use a imagem menor para navegar.

Clique para exibir o stream de vídeo ao vivo em tela cheia. Pressione ESC para sair do modo de tela cheia.

Instalação

Modo de captura : um modo de captura é uma configuração predefinida que determina como a câmera captura as imagens. Quando você altera o modo de captura, várias outras configurações podem ser afetadas, como áreas de exibição e máscaras de privacidade.

Posição de montagem : a orientação da imagem pode mudar de acordo com a montagem da câmera.

Power line frequency (Frequência da linha de alimentação): Para minimizar a cintilação da imagem, selecione a frequência utilizada em sua região. As regiões norte-americanas e o Brasil normalmente usam 60 Hz. O resto do mundo usa principalmente 50 Hz. Se não tiver certeza sobre a frequência da linha de alimentação da sua região, entre em contato com as autoridades locais.

Rotate (Girar): selecione a orientação desejada para a imagem.

Zoom: use o controle deslizante para ajustar o nível de zoom.

Focus (Foco): Use o controle deslizante para definir o foco manualmente.

AF: Clique para fazer a câmera focalizar na área selecionada. Se você não selecionar uma área de foco automático, a câmera focalizará na cena inteira.

Autofocus area (Área de foco automático): Clique em para exibir a área de foco automático. Essa área deve incluir a área de interesse.

Reset focus (Redefinir foco): Clique para que o foco retorne à sua posição original.

Observação

Em ambientes frios, é possível levar vários minutos para que o zoom e o foco fiquem disponíveis.

Correção de imagem

Importante

Nós recomendamos o uso de vários recursos de correção de imagem ao mesmo tempo, pois isso pode gerar problemas de desempenho.

Correção de distorção de barril (BDC) : ative para obter uma imagem mais reta caso ela sofre de distorção em barril. A distorção em barril é um efeito da lente que faz com que a imagem apareça curva e dobrada para fora. Essa condição é vista com mais facilidade quando o zoom da imagem está afastado.

Recortar : Use o controle deslizante para ajustar o nível de correção. Um nível menor significa que a largura da imagem será mantida às custas da altura e da resolução da imagem. Um nível maior significa que a altura e a resolução da imagem são mantidas às custas da largura da imagem.

Remover distorção : Use o controle deslizante para ajustar o nível de correção. Pucker (Franzido) significa que a largura da imagem será mantida às custas da altura e da resolução da imagem. Bloat (Inchado) significa que a altura e a resolução da imagem são mantidas às custas da largura da imagem.

Estabilização da imagem : ative para obter uma imagem mais suave e estável com menos desfoque. Recomendamos usar a estabilização de imagem ambientes em que o dispositivo é montado em um local exposto e sujeito a vibrações, por exemplo, devido a ventos ou tráfego próximo.

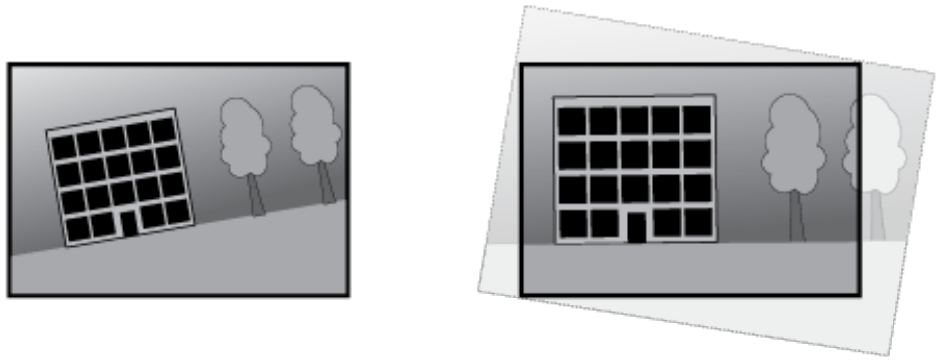
Distância focal : use o controle deslizante para ajustar a distância focal. Um valor mais elevado produz uma ampliação maior e um ângulo de visão mais estreito, enquanto um valor menor diminui a ampliação e amplia o ângulo de visão.

Margem do estabilizador : Use o controle deslizante para ajustar o tamanho da margem do estabilizador, o qual determina o nível de vibração a ser estabilizado. Se o produto estiver montado em um ambiente com muita vibração, mova o controle deslizante para **Max (Máximo)**. O resultado será a captura de uma cena menor. Se o ambiente apresentar menos vibrações, mova o controle deslizante para **Min (Mínimo)**.

Endireitar imagem : ative e use o controle deslizante para endireitar a imagem horizontalmente girando-a e recortando-a digitalmente. Essa funcionalidade é útil quando não é possível montar a câmera perfeitamente nivelada. O ideal é endireitar a imagem durante a instalação.

: Clique para exibir uma grade de apoio na imagem.

: Clique para ocultar a grade.



A imagem antes e depois do endireitamento.

Imagem

Aparência

Perfil de cena : selecione um perfil de cena adequado para seu cenário de monitoramento. Um perfil de cena otimiza as configurações de imagem, incluindo nível de cor, brilho, nitidez, contraste e contraste local, para um ambiente ou uma finalidade específica.

- **Forense**: adequado para fins de monitoramento.
- **Ambientes internos** : adequado para ambientes internos.
- **Ambientes externos** : adequado para ambientes externos.
- **Vívida** : útil para fins de demonstração.
- **Visão geral do tráfego** : adequado para monitorar tráfego de veículos.

Saturação: use o controle deslizante para ajustar a intensidade das cores. Por exemplo, é possível gerar uma imagem em tons de cinza.



Contraste: use o controle deslizante para ajustar a diferença entre claro e escuro.



Brilho: use o controle deslizante para ajustar a intensidade de luz. Isso pode facilitar a visualização dos objetos. O brilho é aplicado após a captura da imagem e não afeta as informações existentes na imagem. Para obter mais detalhes de uma área escura, geralmente é melhor aumentar o ganho ou o tempo de exposição.



Sharpness (Nitidez): use o controle deslizante para fazer com que os objetos na imagem pareçam mais nítidos por meio do ajuste do contraste das bordas. Se você aumentar a nitidez, também aumentará a taxa de bits e, consequentemente, o espaço de armazenamento necessário.



Amplo alcance dinâmico

WDR (Wide Dynamic Range, Amplo Alcance Dinâmico) : ative para tornar visíveis tanto as áreas escuras quanto as áreas claras da imagem.

Contraste local : use o controle deslizante para ajustar o contraste da imagem. Quanto mais alto for o valor, maior será o contraste entre áreas escuras e claras.

Mapeamento de tons : use o controle deslizante para ajustar a quantidade de mapeamento de tons que é aplicada à imagem. Se o valor for definido como zero, somente a correção de gama padrão será aplicada, enquanto um valor mais alto aumentará a visibilidade das partes mais escuras e mais claras da imagem.

Equilíbrio de branco

Quando a câmera detecta qual é a temperatura da cor da luz recebida, ela pode ajustar a imagem para fazer as cores parecerem mais naturais. Se isso não for suficiente, você pode selecionar uma fonte de luz adequada na lista.

A configuração de balanço de branco automático reduz o risco de cintilação das cores adaptando-se a mudanças de forma gradual. Se a iluminação for alterada, ou quando a câmera for ligada pela primeira vez, até 30 segundos poderão ser necessários para a adaptação à nova fonte de luz. Se houver mais de um tipo de fonte de luz em uma cena, ou seja, elas apresentam temperatura de cores diferentes, a fonte de luz dominante atuará como referência para o algoritmo de balanço de branco automático. Esse comportamento poderá ser sobrescrito com a escolha de uma configuração de balanço de branco fixa que corresponda à fonte de luz que você deseja usar como referência.

Light environment (Ambiente de iluminação):

- **Automatic (Automático)**: Identificação e compensação automáticas da cor da fonte de luz. Essa é a configuração recomendada que pode ser usada na maioria das situações.
- **Automático – Ambientes externos** : Identificação e compensação automáticas da cor da fonte de luz. Essa é a configuração recomendada que pode ser usada na maioria das situações de ambientes externos.
- **Personalizado, ambientes internos** : Ajuste de cores fixo para ambientes com alguma iluminação artificial (não fluorescente), bom para temperaturas de cor normais ao redor de 2800 K.
- **Personalizado – ambientes externos** : Ajuste de cores fixo para condições de tempo ensolaradas com temperatura de cor de cerca de 5500 K.
- **Fixed – fluorescent 1 (Fixo – luz fluorescente 1)**: Ajuste de cores fixo para iluminação fluorescente com temperatura de cor de cerca de 4000 K.
- **Fixed – fluorescent 2 (Fixo – luz fluorescente 2)**: Ajuste de cores fixo para iluminação fluorescente com temperatura de cor de cerca de 3000 K.
- **Fixed – indoors (Fixo – ambientes internos)**: Ajuste de cores fixo para ambientes com alguma iluminação artificial (não fluorescente), bom para temperaturas de cor normais ao redor de 2800 K.
- **Fixed – outdoors 1 (Fixo – ambientes externos 1)**: Ajuste de cores fixo para condições de tempo ensolaradas com temperatura de cor de cerca de 5500 K.
- **Fixed – outdoors 2 (Fixo – ambientes externos 2)**: Ajuste de cores fixo para condições de tempo nubladas com temperatura de cor de cerca de 6500 K.
- **Iluminação pública – mercúrio** : ajuste de cores fixo para a emissão ultravioleta das lâmpadas de vapor de mercúrio muito comuns em iluminação pública.
- **Iluminação pública – sódio** : Ajuste de cores fixo para compensar a cor amarelo-alaranjada das lâmpadas de vapor de sódio muito comuns em iluminação pública.
- **Hold current (Manter atuais)**: Mantém as configurações atuais e não compensa por alterações na iluminação.
- **Manual** : fixa o balanço de branco com a ajuda de um objeto branco. Arraste o círculo para um objeto que deseja que a câmera interprete como branco na imagem de visualização ao vivo. Use os controles deslizantes **Red balance (Balanço de vermelho)** e **Blue balance (Balanço de azul)** para ajustar o balanço de branco manualmente.

Modo dia/noite

IR-cut filter (Filtro de bloqueio de infravermelho):

- **Auto**: selecione para ativar e desativar automaticamente o filtro de bloqueio de infravermelho. Quando a câmera está no modo diurno, o filtro de bloqueio de infravermelho é ativado e bloqueia luz infravermelha recebida. No modo noturno, o filtro de bloqueio de infravermelho é desativado e aumenta a sensibilidade da câmera à luz.

Observação

- Alguns dispositivos têm filtros de passagem de infravermelho no modo noturno. O filtro de passagem de infravermelho aumenta a sensibilidade à luz infravermelha, mas bloqueia a luz visível.
- **On (Ativado)**: selecione para ativar o filtro de bloqueio de infravermelho. A imagem está em cores, mas com sensibilidade reduzida à luz.
- **Off (Desativada)**: selecione para desativar o filtro de bloqueio de infravermelho. A imagem permanece em preto e branco para uma maior sensibilidade à luz.

Threshold (Limite): use o controle deslizante para ajustar o limiar de luz em que a câmera alterna do modo diurno para o modo noturno.

- Mova o controle deslizante em direção a **Bright (Brilho)** para reduzir o limite para o filtro de bloqueio de infravermelho. A câmera alternará para o modo noturno mais cedo.
- Mova o controle deslizante em direção a **Dark (Escuro)** para aumentar o limite do filtro de bloqueio de infravermelho. A câmera alternará para o modo noturno mais tarde.

Luz IV

se o seu dispositivo não tiver iluminação integrada, esses controles estarão disponíveis somente quando você conectar um acessório Axis compatível.

Allow illumination (Permitir iluminação): ative para que a câmera use a luz integrada no modo noturno.

Synchronize illumination (Sincronizar iluminação): ative para sincronizar automaticamente a iluminação com a luz do ambiente. A sincronização entre dia e noite funcionará somente se o Filtro de bloqueio de infravermelho estiver configurado como **Auto** ou **Desativado**.

Ângulo de iluminação automático : Ligue para usar o ângulo de iluminação automático. Desligue para definir o ângulo de iluminação manualmente.

Ângulo de iluminação : use o controle deslizante para definir manualmente o ângulo de iluminação, por exemplo, se o ângulo tiver que ser diferente do ângulo de visão da câmera. Se a câmera tiver um ângulo de visão amplo, você poderá reduzir o ângulo de iluminação, o que é equivalente a uma posição de aproximação maior. Isso resultará em cantos escuros na imagem.

Comprimento de onda IR : selecione o comprimento de onda desejado para a luz IR.

Luz branca

Allow illumination (Permitir iluminação) : Ative para que a câmera use luz branca no modo noturno.

Synchronize illumination (Sincronizar iluminação) : ative para sincronizar automaticamente a luz branca com a luz do ambiente.

Exposição

selecione um modo de exposição para reduzir efeitos irregulares altamente variáveis na imagem, por exemplo, cintilação produzida por diferentes tipos de fontes de iluminação. Recomendamos o uso do modo de exposição automática, ou o uso da mesma frequência da sua rede elétrica.

Exposure mode (Modo de exposição):

- **Automatic (Automático)**: a câmera ajusta a abertura, o ganho e o obturador automaticamente.
- **Abertura automática** : A câmera ajusta a abertura e o ganho automaticamente. O obturador é fixo.
- **Obturador automático** : A câmera ajusta o obturador e o ganho automaticamente. A abertura é fixa.
- **Hold current (Manter atuais)**: Trava as configurações de exposição atuais.
- **Sem cintilação** : a câmera ajusta a abertura e o ganho automaticamente, e usa somente as seguintes velocidades de obturador: 1/50 s (50 Hz) e 1/60 s (60 Hz).
- **Sem cintilação 50 Hz** : a câmera ajusta a abertura e o ganho automaticamente, e usa a velocidade de obturador de 1/50 s.
- **Sem cintilação 60 Hz** : a câmera ajusta a abertura e o ganho automaticamente, e usa a velocidade de obturador de 1/60 s.
- **Redução de cintilação** : o mesmo que sem cintilação, mas a câmera pode usar velocidades de obturador superiores a 1/100 s (50 Hz) e 1/120 s (60 Hz) para cenas mais claras.
- **Redução de cintilação 50 Hz** : o mesmo que sem cintilação, mas a câmera pode usar velocidades de obturador superiores a 1/100 s para cenas mais claras.
- **Redução de cintilação 60 Hz** : o mesmo que sem cintilação, mas a câmera pode usar velocidades de obturador superiores a 1/120 s para cenas mais claras.
- **Manual** : A abertura, o ganho e o obturador são fixos.

Zona de exposição : Use zonas de exposição para otimizar a exposição em uma parte selecionada da cena, por exemplo, a área na frente de uma porta de entrada.

Observação

As zonas de exposição estão relacionadas à imagem original (sem rotação), e os nomes das zonas aplicam-se à imagem original. Isso significa que, por exemplo, se o stream de vídeo for girado em 90°, a zona **superior** se tornará a zona **direita** e a **esquerda** passará a ser a **inferior** no stream.

- **Automatic (Automático)**: opção adequada para a maioria das situações.
- **Center (Centro)**: usa uma área fixa no centro da imagem para calcular a exposição. A área tem tamanho e posição fixos na visualização ao vivo.
- **Máximo** : usa a visualização ao vivo inteira para calcular a exposição.
- **Superior** : usa uma área com tamanho e posição fixos na parte superior da imagem para calcular a exposição.
- **Inferior** : usa uma área com tamanho e posição fixos na parte inferior da imagem para calcular a exposição.
- **Esquerda** : usa uma área com tamanho e posição fixos na parte esquerda da imagem para calcular a exposição.

- **Direita** : usa uma área com tamanho e posição fixos na parte direita da imagem para calcular a exposição.
- **Spot (Pontual)**: usa uma área com tamanho e posição fixos na visualização ao vivo para calcular a exposição.
- **Custom (Personalizada)**: usa uma área na visualização ao vivo para calcular a exposição. É possível ajustar o tamanho e a posição da área.

Max shutter (Obturador máximo): selecione a velocidade do obturador para proporcionar a melhor imagem. Velocidades de obturador mais lentas (exposição mais longa) podem causar desfoque quando há movimento. Velocidades muito altas podem afetar a qualidade da imagem. O obturador máximo trabalha em conjunto com o ganho máximo para aprimorar a imagem.

Max gain (Ganho máximo): selecione o ganho máximo adequado. Se você aumentar o ganho máximo, o nível de visibilidade dos detalhes em imagens escuras aumentará, mas o nível de ruído também aumentará. O aumento no ruído também pode resultar no aumento do uso de largura de banda e de requisitos de capacidade de armazenamento. Se você definir o ganho máximo como um valor elevado, as imagens poderão diferir bastante se as condições de iluminação forem muito diferentes entre o dia e a noite. O ganho máximo trabalha em conjunto com o obturador máximo para aprimorar a imagem.

Exposição adaptativa ao movimento : Selecione para reduzir o desfoque por movimento em condições de pouca iluminação.

Blur-noise trade-off (Compromisso desfoque/ruído): use o controle deslizante para ajustar a prioridade entre desfoque por movimento e ruído. Se desejar priorizar a largura de banda reduzida e obter menos ruído às custas de detalhes em objetos móveis, mova o controle deslizante para **Low noise (Ruído baixo)**. Se desejar priorizar a preservação de detalhes em objetos móveis às custas de ruído e largura de banda, mova o controle deslizante para **Low motion blur (Desfoque por movimento baixo)**.

Observação

Você pode alterar a exposição mediante o ajuste do tempo de exposição ou do ganho. Se você aumentar o tempo de exposição, obterá mais desfoque por movimento. Se aumentar o ganho, obterá mais ruído. Se você ajustar o **Blur-noise trade-off (Compromisso desfoque/ruído)** para **Low noise (Ruído baixo)**, a exposição automática priorizará tempos de exposição mais longos em relação ao ganho crescente, bem como o contrário se você ajustar o compromisso para **Low motion blur (Desfoque por movimento baixo)**. O ganho e o tempo de exposição eventualmente atingirão seus valores máximos em condições de pouca iluminação, independentemente da prioridade definida.

Travar abertura : ative para manter o tamanho da abertura definido pelo controle deslizante **Aperture (Abertura)**. Desative para permitir que a câmera ajuste automaticamente o tamanho da abertura. Por exemplo, você pode bloquear a abertura para cenas com condições de iluminação permanentes.

Abertura : Use o controle deslizante para ajustar o tamanho da abertura, ou seja, a quantidade de luz que passa pela lente. A fim de possibilitar que mais luz entre no sensor e, assim, produzir uma imagem mais clara em condições de pouca luz, mova o controle deslizante para **Open (Aberta)**. Uma abertura mais ampla também reduz a profundidade do campo, o que significa que objetos muito próximos ou muito afastados da câmera poderão aparecer fora de foco. Para aumentar a região da imagem em foco, mova o controle deslizante para **Closed (Fechada)**.

Exposure level (Nível de exposição): use o controle deslizante para ajustar a exposição da imagem.

Remoção de névoa : ative para detectar os efeitos de névoa e removê-los automaticamente para produzir uma imagem mais clara.

Observação

Recomendamos que você não ative **Defog (Remoção de névoa)** em cenas com baixo contraste, grandes variações de nível de luz, ou quando o foco automático estiver ligeiramente desativado. Isso pode afetar a

qualidade da imagem, por exemplo, aumentando o contraste. Além disso, o excesso de luz pode afetar negativamente a qualidade da imagem quando a remoção de névoa está ativa.

Óptica

Compensação de temperatura : Ative para que a posição do foco seja corrigida de acordo com a temperatura na óptica.

Compensação de IR : Ative se desejar que a posição de foco seja corrigida quando o filtro de bloqueio de infravermelho estiver desativado e houver luz infravermelha.

Calibrate zoom and focus (Calibrar zoom e foco): Clique para redefinir a óptica e as configurações de zoom e foco para a posição padrão de fábrica. Isso será necessário se a parte óptica perder a calibração durante o transporte ou se o dispositivo tiver sido exposto a vibrações extremas.

Stream

Geral

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

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

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

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

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

Zipstream

Zipstream é uma tecnologia de redução da taxa de bits otimizada para videomonitoramento, que reduz a taxa de bits média em um stream H.264 ou H.265 em tempo real. A Axis Zipstream aplica uma taxa de bits elevada em cenas com muitas regiões de interesse, por exemplo, em cenas que contêm objetos móveis. Quando a cena é mais estática, a Zipstream aplica uma taxa de bits inferior, reduzindo a necessidade de armazenamento. Para saber mais, consulte *Redução da taxa de bits com Axis Zipstream*

Selecione a **Strength (Intensidade)** da redução de taxa de bits:

- **Off (Desativada)**: sem redução da taxa de bits.
- **Baixa**: Não há degradação de qualidade visível na maioria das cenas. Essa é a opção padrão e pode ser usada em todos os tipos de cenas para reduzir a taxa de bits.
- **Medium (Média)**: efeitos visíveis em algumas cenas com menos ruído e nível de detalhes ligeiramente inferior em regiões de menos interesse (por exemplo, quando não houver movimento).
- **Alta**: efeitos visíveis em algumas cenas com menos ruído e nível de detalhes inferior em regiões de menos interesse (por exemplo, quando não houver movimento). Recomendamos esse nível para dispositivos conectados à nuvem e dispositivos que usam armazenamento local.
- **Higher (Mais alto)**: efeitos visíveis em algumas cenas com menos ruído e nível de detalhes inferior em regiões de menos interesse (por exemplo, quando não houver movimento).
- **Extreme (Extrema)**: efeitos visíveis na maioria das cenas. A taxa de bits é otimizada para minimizar o armazenamento.

Optimize for storage (Otimizar para armazenamento): Ative-a para minimizar a taxa de bits enquanto mantém a qualidade. A otimização não se aplica ao stream mostrado no cliente Web. Esse recurso só poderá ser usado se seu VMS oferecer suporte a quadros B. Ativar a opção **Optimize for storage (Otimizar para armazenamento)** também ativa o **Dynamic GOP (Grupo de imagens dinâmico)**.

Dynamic FPS (FPS dinâmico) (quadros por segundo): ative para que a largura de banda varie com base no nível de atividade na cena. Mais atividade exigirá mais largura de banda.

Lower limit (Limite inferior): insira um valor para ajustar a taxa de quadros entre FPS mínimo e o fps padrão do stream com base na movimentação na cena. Nós recomendamos que você use o limite inferior em cenas com movimentação muito baixa, em que o fps pode cair para 1 ou menos.

Dynamic GOP (Grupo de imagens dinâmico): ative para ajustar dinamicamente o intervalo entre quadros I com base no nível de atividade na cena.

Upper limit (Limite superior): insira um comprimento de GOP máximo, ou seja, o número máximo de quadros P entre dois quadros I. Um quadro I é um quadro de imagem autônomo independente de outros quadros.

Controle de taxa de bits

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

Orientação

Mirror (Espelhar): Ative para espelhar a imagem.

Áudio

Include (Incluir): ative para usar áudio no stream de vídeo.

Source (Fonte) : selecione a fonte de áudio que deseja usar.

Estéreo : ative para incluir áudio integrado, ou áudio de um microfone externo.

Sobreposições

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

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

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

- **Transparência**: defina a transparência de toda a sobreposição.
- **Transparência do segundo plano**: defina a transparência apenas do plano de fundo da sobreposição.
- **Pontos**: ative para adicionar um ponto à linha do gráfico quando os dados forem atualizados.
- **Eixo Y**
  - **Label (Rótulo)**: insira o rótulo de texto para o eixo Y.
  - **Escala dinâmica**: ative para que a escala se adapte automaticamente aos valores dos dados. desative para inserir manualmente valores para uma escala fixa.
  - **Limiar mínimo de alarme** e **Limiar máximo de alarme**: esses valores adicionarão linhas de referência horizontais ao gráfico de barras, facilitando a visualização quando o valor dos dados estiver muito alto ou muito baixo.

Áreas de visualização

: Clique para criar uma área de exibição.

Clique na área de exibição para acessar as configurações.

Nome: insira um nome para a área de exibição. O comprimento máximo é 64 caracteres.

Aspect ratio (Proporção): selecione a proporção desejada. A resolução será ajustada automaticamente.

PTZ: Ative para usar a funcionalidade pan, tilt e zoom na área de exibição.

Máscaras de privacidade

: Clique para criar uma máscara de privacidade.

Privacy masks (Máscaras de privacidade): clique para mudar a cor de todas as máscaras de privacidade ou excluir todas as máscaras permanentemente.

Mask x (Máscara x): clique para renomear, desativar ou excluir permanentemente a máscara.

Áudio

Configurações do dispositivo

Entrada: ative ou desative a entrada de áudio. Mostra o tipo de entrada.

Permitir extração de stream : ative para permitir a extração de streams.

Tipo de entrada : selecione o tipo de entrada; por exemplo, microfone interno ou linha.

Tipo de alimentação : selecione o tipo de alimentação para a entrada.

Aplicar alterações : Aplique sua seleção.

Echo cancellation (Cancelamento de eco) : Ative para remover ecos durante uma comunicação bidirecional.

Controles de ganho separados : ative para ajustar o ganho separadamente para cada tipo de entrada.

Controle de ganho automático : ative para adaptar dinamicamente o ganho às alterações no som.

Gain (Ganho): use o controle deslizante para mudar o ganho. Clique no ícone de microfone para silenciar ou remover o silenciamento.

Saída: mostra o tipo de saída.

Gain (Ganho): use o controle deslizante para mudar o ganho. Clique no ícone de alto-falante para silenciar ou remover o silenciamento.

Stream

Codificação: selecione a codificação que será usada para o streaming da fonte de entrada. Você só poderá escolher a codificação se a entrada de áudio estiver ativada. Se a entrada de áudio estiver desativada, clique em **Enable audio input (Ativar entrada de áudio)** para ativá-la.

Clipes de áudio

Adicionar clipe: Adicione um novo clipe de áudio. É possível usar arquivos .au, .mp3, .opus, .vorbis, .wav.

Executar o clipe de áudio.

Parar de executar o clipe de áudio.

O menu de contexto contém:

- **Rename (Renomear)**: Altere o nome do clipe de áudio.
- **Create link (Criar link)**: crie um URL que reproduz o clipe de áudio no dispositivo. Especifique o volume e o número de vezes para reproduzir o clipe.
- **Download (Baixar)**: baixe o clipe de áudio em seu computador.
- **Excluir**: exclua o clipe de áudio do dispositivo.

Gravações

Clique para filtrar as gravações.

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

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

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

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

Armazenamento: mostra gravações com base no tipo de armazenamento.

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

Inicie uma gravação no dispositivo.

Escolha o dispositivo de armazenamento que será usado para salvar.

Pare uma gravação no dispositivo.

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

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

Reproduza a gravação.

Pare a execução da gravação.

Mostre ou oculte informações sobre a gravação.

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

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

Clique para excluir uma gravação.

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

Apps

Adicionar app: Instale um novo aplicativo.

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

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

Permitir apps com privilégios de root : Ative para permitir que aplicativos com privilégios de root tenham acesso total ao dispositivo.

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

Observação

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

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

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

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

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

Sistema

Hora e local

Data e hora

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

Observação

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

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

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

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

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

Observação

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

Local do dispositivo

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

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

Rede

IPv4

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

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

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

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

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

Observação

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

IPv6

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

Nome de host

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

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

Servidores DNS

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

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

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

HTTP e HTTPS

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

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

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

Observação

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

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

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

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

Protocolos de descoberta de rede

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

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

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

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

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

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

Proxies globais

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

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

Formatos permitidos para proxies http e https:

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

Observação

Reinicie o dispositivo para aplicar as configurações de proxy global.

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

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

Conexão com a nuvem com apenas um clique

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

Allow O3C (Permitir O3C):

- **Um clique**: Esta é a configuração padrão. Pressione e mantenha pressionado o botão de controle no dispositivo para conectar a um serviço O3C via Internet. Você precisa registrar o dispositivo com o serviço O3C dentro de 24 horas após pressionar o botão de controle. Caso contrário, o dispositivo se desconectará do serviço O3C. Após o dispositivo ser registrado, a opção **Always (Sempre)** será ativada e seu dispositivo Axis permanecerá conectado ao serviço O3C.
- **Sempre**: O dispositivo tenta constantemente conectar a um serviço O3C pela Internet. Uma vez registrado, o dispositivo permanece conectado ao serviço O3C. Use essa opção se o botão de controle do dispositivo estiver fora de alcance.
- **Não**: Desativa o serviço O3C.

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

Host: Insira o endereço do servidor proxy.

Porta: Insira o número da porta usada para acesso.

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

Authentication method (Método de autenticação):

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

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

SNMP

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

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

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

Observação

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

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

Segurança

Certificados

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

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

Os seguintes formatos são aceitos:

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

Importante

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

Adicionar certificado : Clique para adicionar um certificado.

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

O menu de contexto contém:

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

Secure keystore (Armazenamento de chaves seguro) :

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

Controle de acesso à rede e criptografia

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificados

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

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

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

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

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

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

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

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

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

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

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

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

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

Impedir ataques de força bruta

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

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

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

Firewall

Activate (Ativar): Ative o firewall.

Default Policy (Política padrão): Selecione o estado padrão do firewall.

- **Permitir:** Permite todas as conexões ao dispositivo. Essa opção é definida por padrão.
- **Deny (Negar):** Nega todas as conexões ao dispositivo.

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

- **Endereço**: Insira um endereço no formato IPv4/IPv6 ou CIDR ao qual deseja permitir ou negar o acesso.
- **Protocol (Protocolo)**: Selecione um protocolo ao qual deseja permitir ou negar acesso.
- **Porta**: Insira um número de porta ao qual deseja permitir ou negar o acesso. Você pode adicionar um número de porta entre 1 e 65535.
- **Policy (Política)**: Selecione a política da regra.

: Clique para criar outra regra.

Adicionar regras: Clique para adicionar as regras que você definiu.

- **Time in seconds (Tempo em segundos):** Defina um limite de tempo para testar as regras. O limite de tempo padrão está definido como 300 segundos. Para ativar as regras imediatamente, defina o tempo como 0 segundo.
- **Confirm rules (Confirmar regras):** Confirme as regras e o limite de tempo. Se você definiu um limite de tempo superior a 1 segundo, as regras permanecerão ativas nesse período. Se tiver definido o tempo para 0, as regras estarão ativas imediatamente.

Pending rules (Regras pendentes): Uma visão geral das regras testadas mais recentes que você ainda não confirmou.

Observação

As regras com limite de tempo são exibidas em **Active rules (Regras ativas)** até que o temporizador exibido acabe ou até serem confirmados. Se elas não forem confirmadas, elas serão exibidas em **Pending rules (Regras pendentes)** assim que o temporizador chegar em zero e o firewall será revertido às configurações definidas anteriormente. Se você as confirmar, elas substituirão as regras ativas atuais.

Confirm rules (Confirmar regras): Clique para ativar as regras pendentes.

Active rules (Regras ativas): Uma visão geral das regras que você está executando no dispositivo.

: Clique para excluir uma regra ativa.

: Clique para excluir todas as regras, pendentes e ativas.

Certificado do AXIS OS com assinatura personalizada

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

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

O menu de contexto contém:

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

Contas

Contas

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

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

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

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

Privileges (Privilégios):

- **Administrator (Administrador)**: Tem acesso irrestrito a todas as configurações. Os administradores também podem adicionar, atualizar e remover outras contas.
- **Operator (Operador)**: Tem acesso a todas as configurações, exceto:
  - Todas as configurações do **System (Sistema)**.
- **Viewer (Visualizador)**: Tem acesso a:
  - Assistir e capturar instantâneos de um stream de vídeo.
  - Assistir e exportar gravações.
  - Pan, tilt e zoom; com **acesso de conta usuário PTZ**.

O menu de contexto contém:

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

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

Acesso anônimo

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

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

Contas SSH

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

- **Restrict root access (Restringir o acesso de root)**: Ative essa opção para restringir funcionalidade que requer acesso root.
- **Enable SSH (Ativar SSH)**: Ative para usar o serviço SSH.

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

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

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

Comentário: Insira um comentário (opcional).

O menu de contexto contém:

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

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

Virtual host (Host virtual)

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

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

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

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

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

O menu de contexto contém:

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

Disabled (Desativado): o servidor está desativado.

Configuração de OpenID

Importante

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

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

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

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

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

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

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

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

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

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

Segredo do cliente: Insira a senha OpenID novamente

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

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

Eventos

Regras

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

Observação

Você pode criar até 256 regras de ação.

Adicionar uma regra: Crie uma regra.

Nome: Insira um nome para a regra.

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

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

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

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

Adicionar uma condição: clique para adicionar uma condição.

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

Destinatários

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

Observação

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

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

Observação

É possível criar até 20 destinatários.

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

Nome: insira um nome para o destinatário.

Tipo: selecione na lista:

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

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

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

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

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

Observação

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

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

Testar: clique para testar a configuração.

O menu de contexto contém:

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

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

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

Programações

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

Adicionar agendamento: clique para criar um cronograma ou pulso.

Acionadores manuais

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

MQTT

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

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

Saiba mais sobre MQTT no *Portal do AXIS OS*.

ALPN

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

Cliente MQTT

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

Status: Mostra o status atual do cliente MQTT.

Broker

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

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

Porta: Insira o número da porta.

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

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

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

Senha: Insira uma senha para o nome de usuário.

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

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

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

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

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

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

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

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

Mensagem de conexão

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

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

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

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

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

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

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

Mensagem de Último desejo e testamento

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

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

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

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

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

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

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

Publicação MQTT

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

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

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

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

Adicionar condição: clique para adicionar uma condição.

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

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

QoS: selecione o nível desejado para a publicação MQTT.

Assinaturas MQTT

Adicionar assinatura: clique para adicionar uma nova assinatura MQTT.

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

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

Subscription type (Tipo de assinatura):

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

QoS: selecione o nível desejado para a assinatura MQTT.

Armazenamento

Armazenamento de rede

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

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

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

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

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

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

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

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

Ferramentas

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

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

Armazenamento interno

Importante

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

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

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

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

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

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

Ferramentas

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

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

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

Armazenamento interno

Disco rígido

- **Livre**: a quantidade de espaço livre em disco.
- **Status**: se o disco está montado ou não.
- **File system (Sistema de arquivos)**: o sistema de arquivos usado pelo disco.
- **Encrypted (Criptografado)**: se o disco está criptografado ou não.
- **Temperature (Temperatura)**: a temperatura atual do hardware.
- **Teste geral de saúde**: O resultado depois de verificar a saúde do disco.

Ferramentas

- **Check (Verificar)**: verifique se há erros no dispositivo de armazenamento e tente repará-lo automaticamente.
- **Repair (Reparar)**: repare o dispositivo de armazenamento. As gravações ativas serão interrompidas durante o reparo. Reparar um dispositivo de armazenamento pode resultar em perda de dados.
- **Format (Formatar)**: Apague todas as gravações e formate o dispositivo de armazenamento. Escolha um sistema de arquivos.
- **Encrypt (Criptografar)**: criptografa os dados armazenados.
- **Decrypt (Descriptografar)**: descriptografa os dados armazenados. O sistema apagará todos os arquivos no dispositivo de armazenamento.
- **Change password (Alterar senha)**: altere a senha de criptografia do disco. Alterar a senha não interrompe as gravações em andamento.
- **Use tool (Usar ferramenta)**: Clique para executar a ferramenta selecionada

Unmount (Desmontar) : Clique antes de desconectar o dispositivo do sistema. Isso interromperá todas as gravações em andamento.

Write protect (Proteção contra gravação): Ative para impedir que o dispositivo de armazenamento seja sobrescrito.

Autoformat (Formatação automática) : o disco será formatado automaticamente com o sistema de arquivos ext4.

SIP

Definições

O Session Initiation Protocol (SIP) é usado para as sessões de comunicação interativa entre os usuários. As sessões podem incluir elementos de áudio e vídeo.

SIP setup assistant (Assistente de configuração de SIP): Clique para definir e configurar o SIP passo a passo.

Enable SIP (Ativar SIP): marque esta opção para possibilitar o início e o recebimento de chamadas SIP.

Permitir chamadas recebidas: Marque esta opção para permitir o recebimento de chamadas de outros dispositivos SIP.

Tratamento da chamada

- **Tempo limite da chamada**: Defina a duração máxima de uma tentativa de chamada se ninguém atender.
- **Incoming call duration (Duração da chamada recebida)**: defina a duração máxima de uma chamada recebida (máx. 10 minutos).
- **End calls after (Encerrar chamadas após)**: defina a duração máxima de uma chamada (máx. 60 minutos). Selecione **Infinite call duration (Duração de chamada infinita)** se não quiser limitar a duração de uma chamada.

Portas

O número da porta deverá ser entre 1024 e 65535.

- **Porta SIP**: a porta de rede usada para comunicação SIP. O tráfego de sinalização por essa porta não é criptografado. O número da porta padrão é 5060. Insira um número de porta diferente, se necessário.
- **Porta TLS**: a porta de rede usada para comunicação SIP criptografada. O tráfego de sinalização por meio dessa porta é criptografado com o Transport Layer Security (TLS). O número da porta padrão é 5061. Insira um número de porta diferente, se necessário.
- **Porta de início de RTP**: a porta de rede usada para o primeiro stream de mídia RTP em uma chamada SIP. O número da porta de início padrão é 4000. Alguns firewalls bloqueiam o tráfego RTP em determinados números de porta.

NAT traversal

Use o NAT (Network Address Translation) traversal quando o dispositivo estiver localizado em uma rede privada (LAN) e você quiser torná-lo disponível na parte externa de rede.

Observação

Para o NAT traversal funcionar, o roteador deve oferecer suporte a ele. O roteador também deverá oferecer suporte a UPnP®.

Cada protocolo de NAT traversal pode ser usado separadamente ou em diferentes combinações, dependendo do ambiente de rede.

- **ICE**: O protocolo ICE (Interactive Connectivity Establishment) aumenta as chances de encontrar o caminho mais eficiente para uma comunicação bem-sucedida entre dispositivos. Se você também ativar o STUN e o TURN, poderá melhorar as chances do protocolo ICE.
- **STUN**: O STUN (Session Traversal Utilities for NAT) é um protocolo de rede cliente-servidor que permite que o dispositivo determine se ele está localizado atrás de um NAT ou firewall e, em caso afirmativo, obtenha o endereço IP público mapeado e o número da porta alocada para conexões a hosts remotos. Insira o endereço do servidor STUN, por exemplo, um endereço IP.
- **TURN**: O TURN (Traversal Using Relays around NAT) é um protocolo que permite que um dispositivo atrás de um roteador NAT ou firewall receba dados de outros hosts via TCP ou UDP. Insira o endereço e as informações de login do servidor TURN.

Áudio e vídeo

- **Audio codec priority (Prioridade do codec de áudio)**: Selecione pelo menos um codec de áudio com a qualidade de áudio desejada para as chamadas SIP. Arraste e solte para alterar a prioridade.

Observação

Os codecs selecionados deve corresponder ao codec do destinatário da chamada, pois o codec do destinatário é decisivo quando uma chamada é feita.

- **Audio direction (Direção do áudio)**: selecione as direções de áudio permitidas.
- **H.264 packetization mode (Modo de pacotes H.264)**: Selecione o modo de pacotes a ser usado.
  - **Auto**: (Recomendado) O dispositivo decide qual modo de pacote será usado.

  - **None (Nenhuma)**: Nenhum modo de pacotes é definido. Este modo é frequentemente interpretado como modo **0**.
  - **0**: Modo não entrelaçado.
  - **1**: Modo de unidade NAL única.
- **Direção do vídeo**: selecione as direções de vídeo permitidas.

Adicionais

- **UDP-to-TCP switching (Alternância de UDP para TCP)**: selecione para permitir que as chamadas alternem temporariamente os protocolos de transporte de UDP (User Datagram Protocol) para TCP (Transmission Control Protocol). O motivo da comutação é evitar fragmentação, e a mudança poderá ocorrer se uma solicitação estiver dentro de 200 bytes da unidade máxima de transmissão (MTU) ou for superior a 1.300 bytes.
- **Allow via rewrite (Permitir via regravação)**: selecione para enviar o endereço IP local em vez de endereço IP público do roteador.
- **Allow contact rewrite (Permitir regravação de contato)**: selecione para enviar o endereço IP local em vez de endereço IP público do roteador.
- **Register with server every (Registrar com o servidor a cada)**: defina a frequência na qual você deseja que o dispositivo se registre com o servidor SIP para contas SIP existentes.
- **DTMF payload type (Tipo de carga DTMF)**: altera o tipo de carga padrão para DTMF.
- **Max retransmissions (Máximo de retransmissões)**: defina o número máximo de vezes que o dispositivo tenta se conectar ao servidor SIP antes de parar de tentar.
- **Seconds until failback (Segundos até a contingência)**: defina o número de segundos até que o dispositivo tente se reconectar ao servidor SIP primário após ter feito a contingência para um servidor SIP secundário.

Contas

Todas as contas SIP atuais estão listadas em **SIP accounts (Contas SIP)**. Para contas registradas, o círculo colorido permite saber o status.

A conta foi registrada com êxito no servidor SIP.

Há um problema com a conta. Possíveis motivos podem ser falha de autorização, credenciais de conta incorretas ou o servidor SIP não consegue encontrar a conta.

A conta **peer to peer (default) (ponto a ponto (padrão))** é uma conta criada automaticamente. Você poderá excluí-la se criar pelo menos mais uma conta e configurá-la como padrão. A conta padrão é sempre usada quando uma chamada à VAPIX® Application Programming Interface (API) é feita sem que a conta SIP de origem seja especificada.

Adicionar conta: clique para criar uma conta SIP.

- **Active (Ativa)**: Selecione para poder usar a conta.
- **Tornar padrão**: Selecione para tornar esta a conta padrão. Deve haver uma conta padrão, e somente uma conta padrão pode existir.
- **Answer automatically (Atender automaticamente)**: Selecione para atender automaticamente a uma chamada recebida.
- **Priorizar IPv6 sobre IPv4** : Selecione para priorizar endereços IPv6 em vez de endereços IPv4. Isso é útil quando você conecta a contas ponto a ponto ou nomes de domínio que resolvem tanto em endereços IPv4 quanto IPv6. Só é possível priorizar IPv6 para nomes de domínio mapeados em endereços IPv6.
- **Nome**: Insira um nome descritivo. Isso pode ser, por exemplo, um nome e sobrenome, uma função ou um local. O nome não é exclusivo.
- **ID de usuário**: insira o número exclusivo do ramal ou telefone atribuído ao dispositivo.
- **Ponto a ponto**: use para direcionar chamadas para outro dispositivo SIP na rede local.
- **Registrada**: Use para fazer chamadas para dispositivos SIP fora da rede local através de um servidor SIP.
- **Domain (Domínio)**: Se disponível, insira o nome do domínio público. Ele será mostrado como parte do endereço SIP nas chamadas feitas para outras contas.
- **Senha**: insira a senha associada à conta SIP para autenticação no servidor SIP.
- **ID de autenticação**: Insira o ID de autenticação usado para autenticar no servidor SIP. Se ele for o mesmo que o ID de usuário, não será necessário inserir o ID de autenticação.
- **ID do chamador**: o nome apresentado para o destinatário das chamadas do dispositivo.
- **Registrador**: insira o endereço IP do registrador.
- **Modo de transporte**: selecione o modo de transporte de SIP para a conta: UPD, TCP ou TLS.
- **TLS version (Versão do TLS)** (somente com o modo de transporte TLS): Selecione a versão de TLS que deve ser utilizada. As versões **v1.2** e **v1.3** são as mais seguras. **Automatic (Automático)** seleciona a versão mais segura com a qual o sistema pode lidar.
- **Media encryption (Criptografia de mídia)** (somente com o modo de transporte TLS): Selecione o tipo de criptografia de mídia (áudio e vídeo) em chamadas SIP.
- **Certificate (Certificado)** (somente com o modo de transporte TLS): Selecione um certificado.
- **Verify server certificate (Verifique o certificado do servidor)** (somente com o modo de transporte TLS): Marque para verificar o certificado do servidor.
- **Secondary SIP server (Servidor SIP secundário)**: ative se quiser que o dispositivo tente se registrar em um servidor SIP secundário se o registro no servidor SIP primário falhar.
- **SIP secure (SIP seguro)**: Selecione para usar o Secure Session Initiation Protocol (SIPS). O SIPS usa o modo de transporte TLS para criptografar o tráfego.

- **Proxies**
  - **Proxy**: clique para adicionar um proxy.
  - **Prioritize (Priorizar)**: Se você adicionou dois ou mais proxies, clique para priorizá-los.
  - **Server address (Endereço do servidor)**: insira o endereço IP do servidor proxy SIP.
  - **Username (Nome de usuário)**: Se necessário, insira o nome de usuário do servidor proxy SIP.
  - **Senha**: Se necessário, insira a senha para o servidor proxy de SIP.
- **Vídeo**
  - **View area (Área de exibição)**: Selecione a área de exibição que será usada nas chamadas com vídeo. Se você selecionar nenhum, o modo de exibição nativo será usado.
  - **Resolução**: selecione a resolução que será usada nas chamadas com vídeo. A resolução afeta a largura de banda necessária.
  - **Taxa de quadros**: selecione o número de quadros por segundo para as chamadas com vídeo. A taxa de quadros afeta a largura de banda necessária.
  - **Perfil H.264**: selecione o perfil que será usado nas chamadas com vídeo.

Testar chamada

Conta SIP: selecione a conta que realizará a chamada.

Endereço SIP: Insira um endereço SIP e clique em para realizar uma chamada de teste e verificar se a conta está funcionando.

Perfis de stream

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

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

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

Nome: adicione um nome para seu perfil.

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

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

Resolução: Consulte para obter uma descrição desta configuração.

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

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

Zipstream : Consulte para obter uma descrição desta configuração.

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

FPS dinâmico : Consulte para obter uma descrição desta configuração.

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

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

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

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

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

Incluir áudio : Consulte para obter uma descrição desta configuração.

ONVIF

Contas ONVIF

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

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

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

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

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

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

Role (Função):

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

O menu de contexto contém:

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

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

Perfis de mídia ONVIF

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

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

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

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

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

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

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

Observação

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

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

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

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

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

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

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

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

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

Metadados: Selecione os metadados para incluir na sua configuração.

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

PTZ : Selecione as configurações PTZ para a sua configuração.

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

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

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

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

Metadados de analíticos

Produtores de metadados

Lista os aplicativos que transmitem metadados e os canais utilizados por eles.

Producer (Produtor): O aplicativo que produz os metadados. Abaixo do aplicativo há uma lista dos tipos de metadados que o aplicativo transmite do dispositivo.

Canal: O canal usado pelo aplicativo. Selecione para ativar o stream de metadados. Desmarque por motivos de compatibilidade ou gerenciamento de recursos.

Detectores

Manipulação da câmera

O detector de manipulação da câmera gera um alarme quando a cena mudar, por exemplo, quando a lente foi coberta, borrifada ou gravemente desfocada, e o tempo em **Trigger delay (Retardo do acionador)** se esgotou. O detector de manipulação só será ativado quando a câmera ficar parada por pelo menos 10 segundos. Nesse período, o detector configura um modelo de cena para usar como comparação a fim de detectar manipulação nas imagens atuais. Para que o modelo de cena seja configurado corretamente, verifique se a câmera está focalizada, se as condições de iluminação estão corretas e se a câmera não está apontada para uma cena sem contornos visíveis, por exemplo, uma parede vazia. O aplicativo de manipulação da câmera pode ser usado como condição para disparar ações.

Retardo do acionador: insira o tempo mínimo durante o qual as condições de manipulação deverão ficar ativas para que o alarme seja acionado. Isso pode ajudar a prevenir alarmes falsos causados por condições conhecidas que afetam a imagem.

Trigger on dark images (Acionar em imagens escuras): É muito difícil gerar alarmes quando a lente da câmera está borrifada ou pintada, visto que é impossível diferenciar esse evento de outras situações em que a imagem escurece de forma legítima, por exemplo, quando as condições de iluminação mudam. Ative esse parâmetro para gerar alarmes para todos os casos em que a imagem se tornar escura. Quando estiver desativado, o dispositivo não gerará alarmes se a imagem ficar escura.

Observação

Para detecção de tentativas de manipulação em cenas estáticas e não lotadas.

Detecção de áudio

Essas configurações estão disponíveis para cada entrada de áudio.

Sound level (Nível sonoro): ajuste o nível sonoro para um valor entre 0 e 100, em que 0 é o mais sensível e 100 é o menos sensível. Use o indicador de atividade como guia ao definir o nível sonoro. Ao criar eventos, você pode usar o nível sonoro como uma condição. Você pode optar por acionar uma ação se o nível sonoro ultrapassar, ficar abaixo ou passar pelo valor definido.

Detecção de impactos

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

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

Saída de vídeo

Configurações de energia

Configurações de energia

Desligamento com atraso : Ative se desejar definir um atraso antes que a energia seja desligada.

Tempo de atraso : Defina um tempo de atraso entre 1 e 60 minutos.

Modo de economia de energia : Ative para colocar o dispositivo no modo de economia de energia. Quando o modo de economia de energia é acionado, o alcance da iluminação IR é reduzido.

Set power configuration (Definir configuração de alimentação): Altere a configuração de energia selecionando uma opção de classe PoE diferente. Clique em **Save and restart (Salvar e reiniciar)** para salvar a alteração.

Observação

Se você definir a configuração de energia como PoE classe 3, recomendamos selecionar **Low power profile (Perfil de baixo consumo)** se o dispositivo possuir essa opção.

Dynamic power mode (Modo de potência dinâmica): Ative-o para reduzir o consumo de energia quando o dispositivo estiver inativo.

Acessórios

Portas de E/S

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

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

Detecção automática

Nome: Edite o texto para renomear a porta.

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

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

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

Observação

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

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

Edge-to-edge

Pareamento

O pareamento de permite usar um alto-falante ou microfone de rede Axis compatível como se ele fizesse parte da câmera. Uma vez pareado, o alto-falante de rede age como um dispositivo de saída de áudio no qual você pode reproduzir clipes de áudio e transmitir som por meio da câmera. O microfone de rede captará sons da área ao redor e o disponibilizará como um dispositivo de entrada de áudio que pode ser usado em streams de mídia e gravações.

Importante

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

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

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

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

Senha: Insira a senha do usuário.

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

Pareamento de microfone  : Selecione para parear um microfone.

Clear fields (Limpar campos): Clique para limpar todos os campos.

Connect (Conectar): Clique para estabelecer conexão com o alto-falante ou microfone.

Logs

Relatórios e logs

Relatórios

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

Logs

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

Rastreamento de rede

Importante

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

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

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

Acesse o sistema remotamente

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

Servidor: Clique para adicionar um novo servidor.

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

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

- Axis
- RFC 3164
- RFC 5424

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

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

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

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

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

Configuração simples

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

Manutenção

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

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

Importante

As únicas configurações que permanecem salvas após a restauração são:

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

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

Observação

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

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

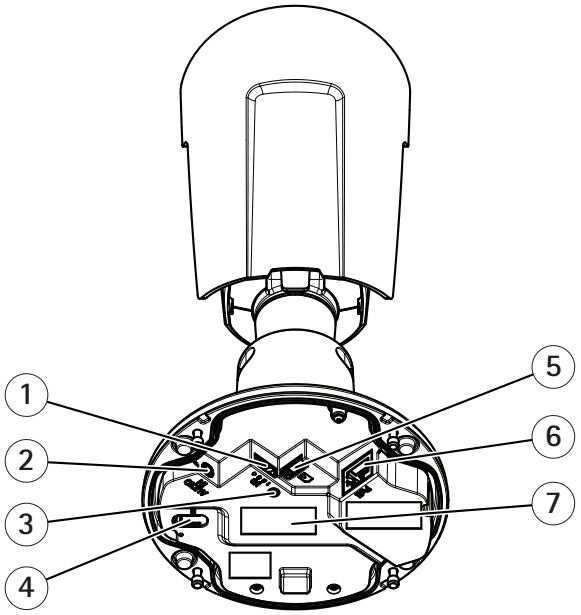
Ao atualizar, é possível escolher entre três opções:

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

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

Especificações

Visão geral do produto



1 *Conector de E/S*
2 *Conector de áudio*
3 *LED indicador de status*
4 *Botão de controle*
5 *Entrada para cartão microSD*
6 *Conector de rede*
7 *Número de peça (P/N) e número de série (S/N)*

Indicadores de LED

LED de estado	Indicação
Apagado	Conexão e operação normais.
Verde	Aceso em verde por 10 segundos para operação normal após a conclusão da inicialização.
Âmbar	Aceso durante a inicialização. Pisca durante a atualização do firmware ou durante a redefinição para os padrões de fábrica.
Âmbar/Vermelho	Pisca em âmbar/vermelho quando a conexão de rede não está disponível ou foi perdida.
Vermelho	Falha na atualização do firmware.

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 dipositivo é compatível com cartões microSD/microSDHC/microSDXC.

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

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

Botões

Botão de controle

O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte .

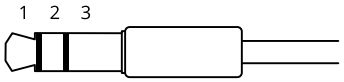
Conectores

Conector de rede

Conector Ethernet RJ45 com Power over Ethernet (PoE).

Conector de áudio

- **Entrada de áudio** – Entrada de 3,5 mm para um microfone mono ou um sinal mono de entrada de áudio (o canal esquerdo é usado de um sinal estéreo).



Entrada de áudio

1 Ponta	2 Anel	3 Luva
Microfone não equalizado (com ou sem alimentação de eletreto) ou entrada de áudio	Alimentação de eletreto, se selecionada	Terra

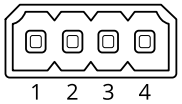
Conector de E/S

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 VCC e da alimentação (saída CC de 12 V), o conector do terminal de E/S fornece a interface para:

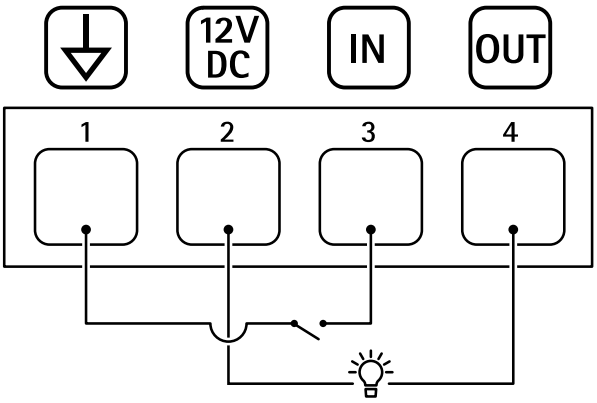
Entrada digital – Para conectar dispositivos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas/janelas e detectores de quebra de vidros.

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



Exemplo:



1 Terra CC
2 Saída CC 12 V, máx. 25 mA
3 Entrada digital
4 Saída digital

Limpeza do dispositivo

OBSERVAÇÃO

- Evite limpar o dispositivo sob luz solar direta ou em temperaturas elevadas, visto que isso pode causar manchas.

1. Para evitar manchas, seque o dispositivo com um pano limpo e macio.

Solução de problemas

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 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.

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.

Problemas técnicos, dicas e soluções

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

Problemas ao atualizar o AXIS OS

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

Problemas na configuração do endereço IP

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

O dispositivo não pode ser acessado por um navegador

Não é possível fazer login	Quando o HTTPS estiver ativado, certifique-se de que o protocolo correto (HTTP ou HTTPS) seja usado ao tentar fazer login. Talvez seja necessário digitar manualmente `http` ou `https` no campo de endereço do navegador. Se a senha da conta root for perdida, o dispositivo deverá ser restaurado para as configurações padrão de fábrica. Consulte .
O endereço IP foi alterado pelo DHCP	Os endereços IP obtidos de um servidor DHCP são dinâmicos e podem mudar. Se o endereço IP tiver sido alterado use o AXIS IP Utility ou o AXIS Device Manager para localizar o dispositivo na rede. Identifique o dispositivo usando seu modelo ou número de série ou nome de DNS (se um nome tiver sido configurado). Se necessário, um endereço IP estático poderá ser atribuído manualmente. Para obter instruções, vá para *axis.com/support*.
Erro de certificado ao usar IEEE 802.1X	Para que a autenticação funcione corretamente, as configurações de data e hora no dispositivo Axis deverão ser sincronizadas com um servidor NTP. Vá para **System > Date and time (Sistema > Data e hora)**.

O dispositivo está acessível local, mas não externamente

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

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

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

Problemas com streaming

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 da placa para obter informações adicionais.
Taxa de quadros inferior à esperada	• Consulte . • 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. • A taxa de quadros por segundo máxima depende da frequência da rede pública (60/50 Hz) à qual o dispositivo Axis está conectado.

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

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

Redefinição para as configurações padrão de fábrica

Importante

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

Observação

A câmera foi pré-configurada com o AXIS License Plate Verifier. Se você redefinir o padrão de fábrica, será necessário reinstalar a chave de licença. Consulte .

Para redefinir o produto para as configurações padrão de fábrica:

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

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

Atualizar o AXIS OS

Importante

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

Observação

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

1. Baixe o arquivo do AXIS OS para seu computador, o qual está disponível gratuitamente em *axis.com/ /support/device-software*.
2. Faça login no dispositivo como um administrador.
3. Vá para **Maintenance (Manutenção) > AXIS OS upgrade (Atualização do AXIS OS)** e clique em **Upgrade (Atualizar)**.

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

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

Considerações sobre desempenho

Ao configurar seu sistema, é importante considerar como várias configurações e situações afetam o desempenho. Alguns fatores afetam a quantidade de largura de banda (a taxa de bits) necessária, outros podem afetar a taxa de quadros e alguns afetam ambos. Se a carga na CPU atingir o valor máximo, isso também afetará a taxa de quadros.

Os seguintes fatores importantes devem ser considerados:

- 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 números elevados de clientes H.264 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 simultâneo a streams de vídeo Motion JPEG e H.264 afeta a taxa de quadros e a largura de banda.
- 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, especificamente se houver streaming 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.

T10126900_pt

2024-11 (M26.2)

© 2018 – 2024 Axis Communications AB