



AXIS I8307-VE Network Intercom

Manual do Usuário

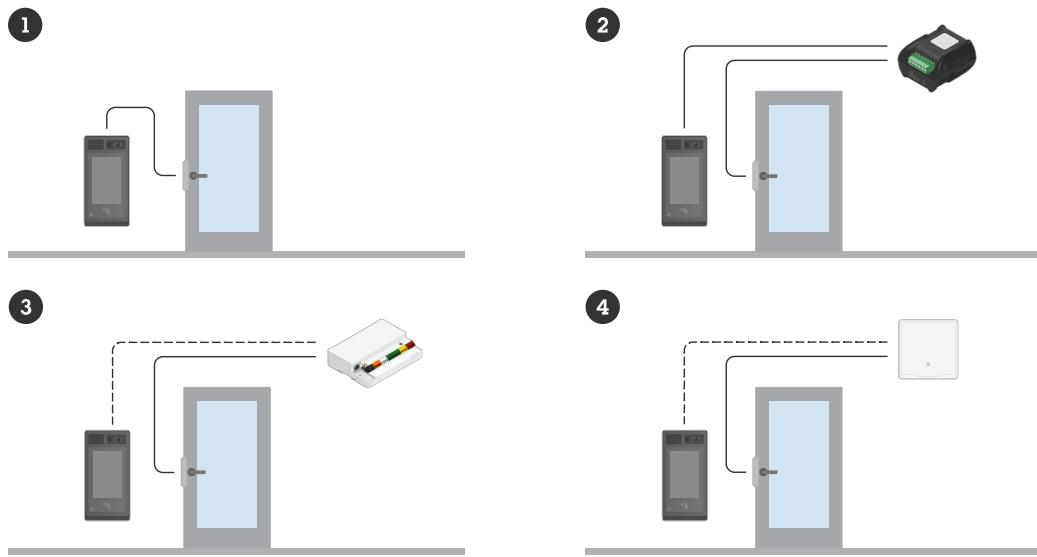
Índice

Visão geral da solução	5
Instalação	6
Modo de visualização	6
Início	7
Encontre o dispositivo na rede	7
Suporte a navegadores	7
Abra a interface web do dispositivo	7
Criar uma conta de administrador	7
Senhas seguras	7
Certifique-se de que o software do dispositivo não foi violado	8
Configure seu dispositivo	9
Configuração de SIP direto (P2P)	9
Configuração de SIP por meio de um servidor (PBX)	9
Criar um contato	10
Adicionar um botão de chamada ao visor	11
Configurar como leitor	11
Use a lista de entradas para permitir que os detentores de credencial abram a porta	11
Configure como leitor de cartão usando um controlador de porta	12
Use dados protegidos em cartões para aumentar a segurança	13
Usar DTMF para mostrar um mapa no visor	13
A interface Web	15
Status	15
Vídeo	16
Instalação	16
Imagem	16
Stream	22
Sobreposições	25
Máscaras de privacidade	27
Comunicação	27
SIP	27
Chamadas no VMS	32
Lista de contatos	32
Chamadas	34
Visor	35
Páginas	35
Geral	36
Protetor de tela	36
Analíticos	37
AXIS Object Analytics	37
Configuração de metadados	37
PTZ	38
Posições predefinidas	38
Modo de ronda	38
Limites	40
Movimento	41
Fila de controle	42
Definições	42
Leitor	42
Conexão	42
Formato da saída	44
Tipos de chip	44
PIN	45
Lista de entradas	45

Áudio.....	47
Configurações do dispositivo.....	47
Stream	47
Clipes de áudio.....	48
Gravações	48
Mídia	49
Apps	50
Sistema.....	50
Hora e local	50
Verificação de configuração.....	52
Rede	52
Segurança.....	57
Contas.....	62
Eventos	65
MQTT	70
Armazenamento	73
Perfis de stream.....	75
ONVIF.....	76
Detectores	79
Configurações de energia	79
Medidor de potência	80
Acessórios.....	80
Logs	81
Configuração simples.....	82
Manutenção	83
Manutenção	83
solução de problemas.....	84
Saiba mais	85
Voice over IP (VoIP)	85
Session Initiation Protocol (SIP).....	85
SIP ponto a ponto (P2PSIP).....	85
Private Branch Exchange (PBX)	86
NAT traversal	87
Configuração de regras de eventos.....	87
Aplicativos	87
Cibersegurança	87
Serviço de notificação de segurança Axis	87
Gerenciamento de vulnerabilidades	87
Operação segura de dispositivos Axis.....	88
Especificações	89
Visão geral do produto.....	89
Indicadores de LED	90
Slot de cartão SD	90
Botões	90
Botão de controle	90
Conectores	90
Conector de rede	90
Conector de áudio	90
Conector do relé.....	91
Conector do leitor.....	91
Conector de E/S.....	92
Conector de energia.....	93
Conexão de equipamentos	94
Um relé alimentado por PoE (12 V).....	94
Dois relés alimentados por PoE (12 V).....	94
Um relé alimentado por PoE (12 V) + um relé alimentado por fonte de alimentação externa	95

Um relé alimentado por PoE (12 V) + um relé de contato livre de potencial	95
Fechadura de 12 V protegida contra falhas alimentada por PoE+ pelo intercomunicador	96
Fechadura protegida contra falhas alimentada por fonte externa	96
Um relé alimentado por PoE (24 V) + um relé de contato livre de potencial	97
Leitor conectado ao controlador de porta usando OSDP	97
Leitor conectado ao controlador de porta usando Wiegand	98
Leitor conectado ao controlador de porta Axis usando leitor VAPIX	98
Solução de problemas	99
Redefinição para as configurações padrão de fábrica	99
Opções do AXIS OS	99
Verificar a versão atual do AXIS OS	99
Atualizar o AXIS OS	100
Problemas técnicos, dicas e soluções	100
Considerações sobre desempenho	102
Entre em contato com o suporte	102
Informações sobre segurança	103
Níveis de perigo	103
Outros níveis de mensagens	103

Visão geral da solução



- 1 *Intercomunicação*
- 2 *Intercomunicador combinado com a AXIS A9801*
- 3 *Intercomunicador combinado com a AXIS A9210*
- 4 *Intercomunicador combinado com sistema de controle de acesso*

Instalação



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

Modo de visualização

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



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

Este vídeo demonstra como usar o modo de visualização.

Início

Encontre o dispositivo na rede

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

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

Suporte a navegadores

O dispositivo pode ser usado com os seguintes navegadores:

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

✓: Recomendado

*: Compatível com limitações

Abra a interface web do dispositivo

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

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

Criar uma conta de administrador

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

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

Importante

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

Senhas seguras

Importante

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

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

Para proteger seus dados, recomendamos enfaticamente que você:

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

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

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

1. Restauração das configurações padrão de fábrica. Consulte .
Após a redefinição, uma inicialização segura garantirá o estado do dispositivo.
2. Configure e instale o dispositivo.

Configure seu dispositivo

Esta seção aborda todas as configurações importantes que um instalador precisa fazer para colocar o produto em funcionamento após a conclusão da instalação do hardware.

Configuração de SIP direto (P2P)

VoIP (Voice over IP) é um grupo de tecnologias que permite a comunicação por voz e multimídia via redes IP. Para obter mais informações, consulte .

Neste dispositivo, o VoIP é habilitado pelo protocolo SIP. Para obter mais informações sobre SIP, consulte

Há dois tipos de configurações para SIPS: direta ou ponto a ponto (P2P) é uma delas. Use ponto a ponto quando a comunicação for feita entre alguns agentes de usuário na mesma rede IP e não houver necessidade de recursos adicionais que poderiam ser fornecidos por um servidor PBX. Para obter informações sobre como configurar esse tipo de comunicação, consulte .

1. Vá para **Communication > SIP > Settings** (Comunicação > SIP > Configurações de SIP) e selecione **Enable SIP** (Habilitar SIP).
2. Para permitir que o dispositivo receba chamadas, selecione **Allow incoming SIP calls** (Permitir recebimento de chamadas SIP).

OBSERVAÇÃO

Quando você permite o recebimento de chamadas, o dispositivo aceita chamadas de qualquer dispositivo conectado à rede. Se o dispositivo puder ser acessado de uma rede pública ou pela Internet, recomendamos não permitir o recebimento de chamadas.

3. Clique em **Call handling** (Tratamento de chamadas).
4. Em **Calling timeout** (Tempo limite de chamada), defina por quantos segundos a chamada irá durar se não houver resposta.
5. Se você tiver permitido o recebimento de chamadas defina o número de segundos antes da espera de chamadas de entrada no **Incoming call timeout** (Tempo limite de recebimento de chamadas).
6. Clique em **Ports** (Portas).
7. Insira o número da **SIP port** (Porta SIP) e o número da **TLS port** (Porta TLS).

Observação

- **SIP port (Porta SIP)** – Para sessões de SIP. O tráfego de sinalização por essa porta não é criptografado. O número da porta padrão é 5060.
 - **TLS port (Porta TLS)** – Para sessões de SIP protegidas por SIPS e TLS. O tráfego de sinalização por meio dessa porta é criptografado com o Transport Layer Security (TLS). O número da porta padrão é 5061.
 - **RTP start port (Porta de início de RTP)** – a porta usada para o primeiro stream de mídia RTP em uma chamada SIP. A porta de início padrão é 4000. Alguns firewalls podem bloquear o tráfego de RTP em determinados números de portas. O número da porta deve ser entre 1024 e 65535.
8. Clique em **NAT traversal**.
 9. Selecione os protocolos que deseja ativar para o NAT traversal.

Observação

Use o NAT traversal quando o dispositivo estiver conectado à rede por trás de um roteador NAT ou um firewall. Para obter mais informações consulte .

10. Clique em **Salvar**.

Configuração de SIP por meio de um servidor (PBX)

VoIP (Voice over IP) é um grupo de tecnologias que permite a comunicação por voz e multimídia via redes IP. Para obter mais informações, consulte .

Neste dispositivo, o VoIP é habilitado pelo protocolo SIP. Para obter mais informações sobre SIP, consulte

Há dois tipos de configurações para SIP: um servidor PBX é uma delas. Use um servidor PBX quando a comunicação precisar ser feita entre um número infinito de agentes de usuário dentro e fora da rede IP. Recursos adicionais podem ser adicionados à configuração dependendo do provedor de PBX. Para obter mais informações, consulte .

1. Solicite as seguintes informações do seu provedor de PBX:
 - ID de usuário
 - Domínio
 - Senha
 - ID de autenticação
 - ID do chamador
 - Registrador
 - Porta de início de RTP
2. Acesse **Communication > SIP > Accounts** (Comunicação > SIP > Contas) e clique em **+ Add account** (+ Adicionar conta).
3. Insira um **Name (Nome)** para a conta.
4. Selecione **Registered (Registrado)**.
5. Selecione um modo de transporte.
6. Adicione as informações da conta a partir do provedor de PBX.
7. Clique em **Salvar**.
8. Defina as configurações de SIP da mesma forma que para ponto a ponto, consulte . Use a porta de início de RTP do provedor de PBX.

Criar um contato

Este exemplo explica como criar um novo contato na lista de contatos. Antes de iniciar, ative o SIP em **Communication > SIP** (Comunicação > SIP).

Para criar um novo contato:

1. Vá para **Communication > Contact list** (Comunicação > Lista de contatos).
2. Clique em **+ Add contact** (+ Adicionar contato).
3. Insira o nome e o sobrenome do contato.
4. Insira o endereço SIP do contato.

Observação

Para obter informações sobre os endereços SIP, consulte .

5. Selecione a conta SIP da qual a chamada será efetuada.

Observação

As opções de disponibilidade são definidas em **System (Sistema) > Events (Eventos) > Schedules (Agendamentos)**.

6. Escolha a **Availability (Disponibilidade)** do contato. Se houver uma chamada quando o contato não estiver disponível, a chamada é cancelada, a menos que haja um contato de fallback.

Observação

Um fallback é um contato para quem a chamada é encaminhada se o contato original não responde ou fica indisponível.

7. Em **Fallback**, selecione **Nenhum**.
8. Clique em **Salvar**.

Adicionar um botão de chamada ao visor

Este exemplo explica como configurar o visor para mostrar um botão que os visitantes podem pressionar para chamar a recepção.

Antes de começar

- Crie o contato da recepção. Para obter instruções, consulte .
1. Vá para **Display > Pages (Visor > Páginas)**.
 2. Em **Default Homepage (Página inicial padrão)**, clique em  e selecione **Edit (Editar)**.
 3. Clique em **+** Adicionar.
 4. Na lista **Type (Tipo)**, selecione **Button (Botão)**.
 5. Na lista de contatos, selecione a recepção.
 6. Selecione um tamanho de botão.
 7. Para salvar o botão, clique em **Save (Salvar)**.
 8. Para salvar a página inicial padrão, clique em **Save (Salvar)**.

Configurar como leitor

É possível configurar seu comunicador interno como um leitor para permitir que os detentores de credencial abram a porta.

Ao usar a lista de entradas, a comunicação interna armazena as credenciais localmente e pode funcionar como um leitor independente para até cinquenta detentores de credencial.

Ao conectar o comunicador interno a um controlador de porta, o comunicador interno ainda pode armazenar até cinquenta credenciais e, se a credencial solicitada for encontrada na lista de entradas, o comunicador interno gerencia as permissões de acesso. Se uma credencial solicitada não for encontrada na lista de entradas e a opção **Usar controlador de porta conectado** estiver ativada, a solicitação será encaminhada para o controlador de porta, que então gerenciará as permissões de acesso.

Use a lista de entradas para permitir que os detentores de credencial abram a porta

Com a lista de entradas, você pode possibilitar que os detentores de credenciais usem sua credencial para acionar ações, como abrir uma porta. Este exemplo explica como adicionar um detentor de credencial que pode usar o cartão para abrir a porta dez vezes.

Pré-requisitos

- O tipo de chip correto deve estar ativo em **Reader > Chip types (Leitor > Tipos de chip)**.

Ative a lista de entradas e adicione um detentor de credencial:

1. Acesse **Reader > Entry list (Leitor > Lista de entrada)**.
2. Ative a opção **Use Entry list (Usar lista de entrada)**.
3. Clique em **+** Add credential holder (**+ Adicionar detentor de credencial**).
4. Digite o nome e o sobrenome do detentor da credencial. O nome deve ser único.
5. Selecione **Card (Cartão)**.
6. Passe o cartão do detentor de credencial no dispositivo e clique em **Get latest (Obter mais recente)**.
7. Mantenha a condição do evento como **Access granted (Acesso concedido)**.
8. Em **Valid to (Válido até)**, selecione **Number of times (Número de vezes)**.
9. Em **Number of times (Número de vezes)**, insira **10**.
10. Clique em **Salvar**.

Crie uma regra:

1. Acesse System > Events (Sistema > Eventos).
2. Em Rules (Regras), clique em +Add a rule (+ Adicionar regra).
3. Em Nome, digite Abrir porta.
4. Na lista de condições, selecione Entry list > Access granted (Lista de entrada > Acesso concedido).
5. Na lista de ações, selecione I/O > Toggle I/O once (E/S > Alternar E/S uma vez).
6. Na lista de portas, selecione Door (Porta).
7. Em State (Estado), selecione Active (Ativo).
8. Defina a duração para 00:00:07.
9. Clique em Salvar.

Configure como leitor de cartão usando um controlador de porta

Conexão de rede

Para usar o comunicador interno como um leitor de cartões, você deve conectá-lo a um controlador de porta. O controlador de porta armazena todas as credenciais e controla quem pode passar pela porta. Neste exemplo, conectamos os dispositivos pela rede. Também modificamos os tipos de cartões permitidos.

Importante

A conexão de rede funciona somente com controladores de porta Axis. Para conectar a um controlador de porta não Axis, você precisa conectar fisicamente os dispositivos com fios. Consulte .

Configurar o interfone como um leitor de cartões

1. Vá para Reader (Leitor) > Connection (Conexão).
2. Selecione o tipo de protocolo do VAPIX reader (Leitor de VAPIX).
3. Selecione o protocolo para comunicação com o controlador de porta.

Observação

Recomendamos ativar a opção Verify certificate (Verificar certificado) se estiver usando HTTPS.

4. Insira o endereço IP do controlador de porta.
5. Insira as credenciais do controlador de porta.
6. Clique em Conectar.
7. Selecione o leitor de entrada para a porta apropriada.
8. Clique em Salvar.

Conexão com fio

Para usar o porto eletrônico como um leitor de cartões, você deve conectá-lo a um controlador de porta. O controlador de porta armazena todas as credenciais e controla quem pode passar pela porta. Neste exemplo, conectamos os dispositivos com fios, usamos o protocolo Wiegand, ativamos o beeper e usamos uma porta de E/S para o LED. Também modificamos os tipos de cartão permitidos.

Importante

Use as portas de E/S que ainda não estão em uso. Se você usar portas de E/S já em uso, todos os eventos criados para essas portas deixarão de funcionar.

Antes de começar

- Conecte o interfone a um controlador de porta. Consulte os desenhos da fiação elétrica, que podem ser encontrados em .
- Configure o hardware do controlador de porta usando o protocolo Wiegand para o leitor. Consulte o manual do usuário do controlador de porta para obter instruções.

Configurar o interfone como um leitor de cartões

1. Vá para Reader (Leitor) > Connection (Conexão).
2. Selecione Wiegand como tipo de protocolo.
3. Ative o Beeper (Bipe).
4. Em Input for beeper (Entrada para bipe), selecione I3.
5. Em Input used for LED control (Entrada usada para controle de LED), selecione 1.
6. Em Entrada para LED1, selecione I1.
7. Selecione as cores a serem usadas para cada estado.
8. Em Keypress format (Formato do pressionamento de tecla), selecione FourBit.
9. Clique em Salvar.
10. Vá para Reader > Chip types (Leitor > Tipos de chip) e ative os tipos de chip que deseja usar.

Observação

Você pode manter o conjunto padrão de tipos de chip, mas recomenda-se modificar a lista de acordo com suas necessidades específicas.

11. Clique em Add data set (Adicionar conjunto de dados) para especificar os conjuntos de dados para os diferentes tipos de chips.
12. Clique em Save (Salvar).

Use dados protegidos em cartões para aumentar a segurança

Para aumentar a segurança em seu sistema de controle de acesso, você pode optar por usar dados de cartões seguros armazenados em alguns tipos de cartões. Os dados são protegidos por uma chave secreta. Para ler os dados do cartão, você precisa armazenar a chave secreta e outras informações sobre o cartão no dispositivo.

1. Vá para Reader > Chip types (Leitor > Tipos de chip).
2. Em Data sets (Conjuntos de dados), selecione o tipo de chip que deseja editar e clique em Add data set (Adicionar conjunto de dados).
3. Insira informações sobre os dados do cartão. As informações a serem inseridas dependerão do tipo de cartão e do modo como os cartões estão inscritos.
4. Se você usa os protocolos OSDP ou Wiegand, selecione Use as UID (Usar como UID) para enviar os dados seguros como UID/CSN em vez do UID/CSN normal.
5. Para permitir que somente cartões em conformidade com os dados do cartão especificado sejam enviados para o controlador de acesso, selecione Required data (Dados necessários). Os cartões que não são compatíveis são ignorados silenciosamente pelo leitor.
6. Clique em Salvar.

Usar DTMF para mostrar um mapa no visor

Quando um visitante faz uma chamada pelo intercomunicador e precisa de instruções, a pessoa que atende pode usar a sinalização DTMF (Dual-Tone Multi-Frequency) para mostrar um mapa no visor do intercomunicador.

Este exemplo explica como:

- Carregar uma imagem de mapa no intercomunicador.
- Criar uma página que contenha a imagem de mapa no intercomunicador.
- Definir a sequência DTMF no intercomunicador.
- Configurar o intercomunicador para mostrar a página do mapa por 30 segundos em resposta à sequência DTMF.

Antes de começar

- Permita chamadas SIP do dispositivo e crie uma conta SIP. Para obter instruções, consulte e .

Carregar imagem de mapa

1. Acesse **Media (Mídia)**.
2. Clique em **+** **Adicionar**.
3. Arraste e solte uma imagem que mostre um mapa do edifício. A resolução de imagem recomendada é de 480x800 pixels, e a resolução máxima é de 2048x2048 pixels.
4. Clique em **Salvar**.

Criar uma nova página de mapa para o visor

5. Vá para **Display > Pages (Visor > Páginas)**.
6. Clique em **+** **Adicionar**.
7. Digite um nome para a página, por exemplo, **Map page (Página de mapa)**.
8. Clique em **+** **Adicionar**.
9. Na lista de tipos, selecione **Image (Imagem)**.
10. Digite um nome para a imagem, por exemplo, **Map image (Imagen de mapa)**.
11. Na lista de imagens, selecione a imagem do mapa.
12. Clique em **Salvar**.
13. Clique novamente em **Save (Salvar)**.

Definir a sequência DTMF

14. Acesse **Communication > SIP > DTMF (Comunicação > SIP > DTMF)**.
15. Clique em **+** **Add sequence (+ Adicionar sequência)**.
16. Em **Sequence (Seqüência)**, insira **9**.
17. Em **Description (Descrição)**, insira **Show map (Mostrar mapa)**.
18. Selecione uma conta.
19. Clique em **Salvar**.

Criar uma regra

20. Acesse **System > Events > Rules (Sistema > Eventos > Regras)** e adicione uma regra:
21. Digite um nome para a regra, por exemplo, **Use DTMF to show map (Usar DTMF para mostrar mapa)**.
22. Na lista de condições, selecione **Call (Chamar) > DTMF**.
23. Na lista de IDs de eventos DTMF, selecione **Show map (Mostrar mapa)**.
24. Na lista de ações, selecione **Display > Show page (Visor > Mostrar página)**.
25. Na lista de páginas, selecione **Map page (Página de mapa)**.
26. Em **Duration (Duração)**, insira **00:00:30** para mostrar o mapa por 30 segundos.
27. Clique em **Salvar**.

A interface Web

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

Observação

O suporte aos recursos e às configurações descritas nesta seção variam para cada dispositivo. Este ícone



indica que o recurso ou configuração está disponível somente em alguns dispositivos.



Mostre ou oculte o menu principal.



Acesse as notas de versão.



Acesse a ajuda do produto.



Altere o idioma.



Defina o tema claro ou escuro.



 O menu de usuário contém:

- Informações sobre o usuário que está conectado.
-  Alterar conta: Saia da conta atual e faça login em uma nova conta.
-  Desconectar: Faça logout da conta atual.
- ⋮
- O menu de contexto contém:
 - Analytics data (Dados de analíticos): Aceite para compartilhar dados de navegador não pessoais.
 - Feedback (Comentários): Compartilhe qualquer feedback para nos ajudar a melhorar sua experiência de usuário.
 - Legal: veja informações sobre cookies e licenças.
 - About (Sobre): veja informações do dispositivo, incluindo versão e número de série do AXIS OS.

Status

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.

Status de sincronização de horário

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

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

Segurança

Mostra os tipos de acesso ao dispositivo que estão ativos, quais protocolos de criptografia estão em uso e se aplicativos não assinados são permitidos. Recomendações para as configurações são baseadas no Guia de Fortalecimento do AXIS OS.

Hardening guide (Guia de fortalecimento): Clique para ir para o *Guia de Fortalecimento do AXIS OS*, onde você poderá aprender mais sobre segurança cibernética em dispositivos Axis e práticas recomendadas.

Status de potência

Mostra as informações de status de potência, incluindo a potência atual, potência média e potência máxima.

Power settings (Configurações de energia): Exiba e atualize as configurações de alimentação elétrica do dispositivo. Encaminha você para a página de configurações de energia, onde é possível alterar essas configurações.

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

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.

Roll (Rolagem): Use o controle deslizante para ajustar o ângulo e tornar a imagem horizontal.

Imagen

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.
- **Placa de licença**  : Adequado para a captura de placas de licença.

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 sobreescrito 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 nuadas 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.

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 a transmissão de vídeo for girada em 90°, a zona superior se tornará a zona direita e a esquerda passará a ser a inferior na transmissão.

- **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 desfoco 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 desfoco por movimento em condições de pouca iluminação.

Blur-noise trade-off (Compromisso desfoco/ruído): use o controle deslizante para ajustar a prioridade entre desfoco por movimento e ruído. Se desejar priorizar a largura de banda reduzida e obter menos ruído às custas de detalhes em objetos móveis, move 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, move o controle deslizante para **Low motion blur (Desfoco 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 desfoco por movimento. Se aumentar o ganho, obterá mais ruído. Se você ajustar o **Blur-noise trade-off (Compromisso desfoco/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 (Desfoco 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, move 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, move 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.

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 monitoramento por vídeo que reduz a taxa de bits média em uma transmissão H.264, H.265 ou AV1 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 na transmissão 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).
 - Seleccione a posição da sobreposição na imagem ou clique e arraste a sobreposição para movê-la na visualização ao vivo.
- **Image (Imagem):** Seleccione para mostrar uma imagem estática sobre a transmissão de vídeo. Você pode usar arquivos .bmp, .png, .jpeg e .svg.
Para carregar uma imagem, clique em **Manage images (Gerenciar imagens)**. Antes de fazer upload de uma imagem, você pode escolher:
 - **Scale with resolution (Dimensionamento com resolução):** selecione para dimensionar automaticamente a imagem de sobreposição para adequá-la à resolução do vídeo.
 - **Use transparency (Usar transparência):** selecione e insira o valor hexadecimal RGB para a respectiva cor. Use o formato RRGGBB. Exemplos de valores hexadecimais são: FFFFFF para branco, 000000 para preto, FF0000 para vermelho, 6633FF para azul e 669900 para verde. Somente para imagens .bmp.
- **Anotação de cena** : Seleccione para mostrar uma sobreposição de texto na transmissão 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).
 - Seleccione a posição da sobreposição na imagem ou clique e arraste a sobreposição para movê-la na visualização ao vivo. A sobreposição é salva e permanece nas coordenadas de panorâmica e inclinação desta posição.
 - **Annotation between zoom levels (%) (Anotação entre níveis de zoom (%)):** Defina os níveis de zoom nos quais a sobreposição será mostrada.

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

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

Máscaras de privacidade



: Clique para criar uma máscara de privacidade.

Privacy masks x/32 (Máscaras de privacidade x/32) ou Privacy masks x/100 (Máscaras de privacidade X/100): Clique nesta barra de título para alterar a cor de todas as máscaras de privacidade ou para excluir todas as máscaras de privacidade permanentemente.



Cell size (Tamanho da célula): Se você escolher a cor do mosaico, as máscaras de privacidade aparecerão como padrões pixelados. Use o controle deslizante para alterar o tamanho dos pixels.



Mask x (Máscara x): Clique no nome/número de uma máscara individual para renomear, desativar ou excluir a máscara permanentemente.

Use zoom level (Usar nível de zoom): Ative para que a respectiva máscara de privacidade apareça apenas quando atingir o nível de zoom no qual foi criada. Ao diminuir o zoom na imagem, a máscara é ocultada novamente.

Comunicação

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.
- **Show video in call (Mostrar vídeo na chamada)**  : Mostra a transmissão de vídeo de entrada no visor do dispositivo.

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 fallback (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.

DTMF



Adicionar sequência: Clique para criar uma nova sequência de multifrequência de duplo tom (DTMF). Para criar uma regra ativada pelo tom de toque, vá para Events > Rules (Eventos > Regras).

Sequência: Insira os caracteres para ativar a regra. Caracteres permitidos: 0-9, A-D, # e *.

Description (Descrição): insira uma descrição da ação a ser acionada por sequência.

Contas: Selecione as contas que usarão a sequência DTMF. Se você escolher ponto a ponto, todas as contas ponto a ponto compartilharão a mesma sequência DTMF.

Protocolos

Selecione os protocolos a serem usados para cada conta. Todas as contas ponto a ponto compartilham as mesmas configurações de protocolo.

Use RTP (RFC2833) (Usar RTP (RFC2833)): Ative para permitir a sinalização DTMF (Dual-Tone Multifrequency), outros sinais de tom e eventos de telefonia em pacotes RTP.

Usar SIP INFO (RFC2976): Ative para incluir o método INFO no protocolo SIP. O método INFO adiciona informações opcionais da camada de aplicação, em geral relacionadas à sessão.

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.

Lista de acesso

Usar lista de acesso: Ative-se para restringir quem pode fazer chamadas para o dispositivo.

Policy (Política):

- **Permitir:** Selecione para permitir chamadas recebidas somente das fontes na lista de acesso.
- **Bloquear:** Selecione para bloquear chamadas recebidas somente das fontes na lista de acesso.



Adicionar origem: Clique em para criar uma nova entrada na lista de acessos.

SIP source (Origem SIP): Digite a ID do chamador ou o endereço do servidor SIP da fonte.

Chamadas no VMS

Chamadas no VMS

Permitir chamadas no software de gerenciamento de vídeo (VMS): selecione para permitir chamadas do dispositivo para o VMS. É possível fazer chamadas do VMS mesmo que o SIP esteja desativado.

Tempo limite da chamada: Defina a duração máxima de uma tentativa de chamada se ninguém atender.

Lista de contatos

Contatos



Clique para baixar a lista de contatos como um arquivo JSON.



Clique para importar uma lista de contatos (JSON).



Adicionar contato: Clique para adicionar um novo contato à lista de contatos.



Upload image (Carregar imagem) : clique para carregar uma imagem para representar o contato.

First name (Nome): Insira o nome do contato.

Last name (Sobrenome): Insira o sobrenome do contato.



Discagem rápida : Insira um número de discagem rápida disponível para o contato. Esse número é usado para chamar o contato no dispositivo.

Endereço SIP: Se você usa o SIP, insira o endereço IP ou o ramal do contato.

 : Clique para fazer uma chamada de teste. A chamada será encerrada automaticamente quando for respondida.

Conta SIP: Se você usa o SIP, selecione a conta SIP a ser usada para a chamada do dispositivo para o contato.

Disponibilidade: Selecione o cronograma de disponibilidade do contato. Você pode adicionar ou ajustar programações em **System > Events > Schedules (Sistema > Eventos > Programações)**. Se houver uma tentativa de chamada quando o contato não estiver disponível, a chamada será cancelada, a menos que haja um contato de contingência.

Fallback (Contingência): Se aplicável, selecione um contato de contingência na lista.

Observações: adicione informações opcionais sobre o contato.



O menu de contexto contém:

Edit contact (Editar contato): Edite as propriedades do contato.

Delete contact (Excluir contato): Exclua o contato.

Grupos



Clique para baixar a lista de contatos como um arquivo JSON.



Clique para importar uma lista de contatos (JSON).



Add group (Adicionar grupo): Clique para criar um novo grupo de contatos existentes.

Upload image (Carregar imagem) : Clique para carregar uma imagem para representar o grupo.

Nome: insira um nome para o grupo.

Usar somente para chamadas em grupo: Ative se deseja usar somente o grupo para chamadas em grupo. Desative se desejar adicionar contatos individuais em um grupo, mas não use o grupo para chamadas em grupo.

Speed dial (Discagem rápida): Insira um número de discagem rápida disponível para o grupo. Esse número é usado para chamar o grupo do dispositivo. Somente para grupos de chamadas em grupo.

Recipients (Destinatários): Selecione os contatos para incluir no grupo. As chamadas serão feitas para todos os destinatários ao mesmo tempo. O número máximo de destinatários é seis.

Fallback (Contingência): Se aplicável, selecione um contato de contingência na lista. Somente para grupos de chamadas em grupo.

Observações: adicione informações opcionais sobre o grupo.



O menu de contexto contém:

Edit group (Editar grupo): Edite as propriedades do grupo.

Delete group (Excluir grupo): Exclua o grupo.

Chamadas

Geral

Áudio

Observação

- O clipe de áudio selecionado é tocado somente quando uma chamada é feita.
- Se você alterar o clipe de áudio ou o ganho durante uma chamada em andamento, ele não entrará em vigor até a próxima chamada.

Ringtone (Toque): Selecione o clipe de áudio que será tocado quando alguém fizer uma chamada para o dispositivo. Use o controle deslizante para ajustar o ganho.

Ringback tone (Tom de retorno de chamada): Selecione o clipe de áudio que será tocado quando alguém fizer uma chamada do dispositivo. Use o controle deslizante para ajustar o ganho.

Visor

Páginas



Adicionar: Crie uma nova página para o visor.

Nome: Dê à página um nome para ajudar a identificá-la.

Background image (Imagem de plano de fundo): Selecione uma imagem na biblioteca de mídia para usar como plano de fundo. A resolução ideal da imagem é de 480x800 pixels. A resolução máxima de imagem permitida é de 2048x2048 pixels.



Adicionar: Adicione um widget, como um botão, texto ou imagem, à página. Um widget é um elemento gráfico.

Tipo: Selecione um tipo de widget.

- **Button (Botão) – Button type (Tipo de botão):** Selecione um tipo de botão.
 - **Contato**
 - **Contact (Contato):** Atribua um contato ao botão. Os visitantes pressionam o botão para fazer uma chamada para o contato.
 - **Tamanho:** Selecione o tamanho do botão de contato.
 - **Personalizado**
 - **Text (Texto):** Digite um texto a ser exibido no botão.
 - **Nome:** Dê um nome ao botão para ajudar a identificá-lo ao criar uma regra no sistema de eventos.
 - **Tamanho:** Selecione o tamanho do botão.
- **Imagen**
 - **Nome:** Atribua um nome à imagem.
 - **Dimensionamento de imagem**
 - **Auto:** Permita que o sistema otimize o dimensionamento da imagem.
 - **Fit (Ajustar):** Ajuste o dimensionamento para que a imagem caiba no visor.
 - **Fill (Preencher):** Ajuste o dimensionamento para que a imagem preencha o visor.
 - **Image (Imagem):** Selecione uma imagem na biblioteca de mídia. A resolução máxima de imagem permitida é de 2048x2048 pixels.
- **Texto**
 - **Text (Texto):** Digite um texto a ser exibido no visor.
 - **Styling (Estilo):** Escolha como formatar o texto.

Save (Salvar): Salve a página para poder exibi-la no visor e criar regras para os widgets.



O menu de contexto contém:

Edit (Editar): Ajuste a página.

Reset (Redefinir): Desfaça alterações não salvas na página.

Duplicate (Duplicar): Crie uma cópia da página.

Set as default homepage (Definir como página inicial padrão): Faça com que esta página seja exibida quando nenhuma página programada estiver ativa. É necessário salvar uma página antes de poder defini-la como página inicial.

Schedule (Agendamento): Selecione para mostrar a página de acordo com uma das programações definidas em System > Events > Schedules (Sistema > Eventos > Programações).

Excluir: Exclua a página. Não é possível excluir a página definida como página inicial padrão.

Geral

Device language (Idioma do dispositivo): Selecione o idioma dos textos padrão no visor.

Show keypad on homepage (Mostrar teclado na página inicial): Ative para mostrar um botão de teclado na página inicial padrão. Os visitantes podem pressionar o botão para abrir um teclado e usar suas credenciais para destrancar a porta.

Protetor de tela



Adicionar: Clique para criar um novo protetor de tela.

Page (Página): Selecione uma página para mostrar quando o protetor de tela estiver ativo.

Duration (Duração): Selecione por quanto tempo o protetor de tela será exibido.

Edit (Editar): Selecione um protetor de tela na lista e clique para ajustá-lo.

Remover: Selecione um ou mais protetores de tela na lista e clique para excluí-los.

Settings (Configurações): Clique para ajustar as configurações gerais do protetor de tela.

Turn off display when inactive (Desligar visor quando inativo): Defina por quanto tempo o visor poderá ficar inativo antes de ser desligado.

Start screensaver when inactive (Iniciar protetor de tela quando inativo): Defina por quanto tempo o visor poderá ficar inativo antes que o protetor de tela seja ativado. Se você definir um tempo maior do que o tempo definido em Turn off display when inactive (Desligar visor quando inativo), o protetor de tela nunca será ativado.

Screensaver sequence (Sequência do protetor de tela): Selecione em que ordem mostrar os protetores de tela, se houver mais de um. Cada protetor de tela é exibido durante o tempo definido em Duration (Duração).

- **Listed (Listado):** Mostre os protetores de tela na ordem listada.
- **Random (Aleatório):** Mostre os protetores de tela em ordem aleatória.

Wake-up trigger (Acionador de ativação): Selecione como ativar o visor enquanto o protetor de tela estiver ativo ou quando o visor estiver desligado.

- **Touch (Toque):** Ative o visor quando alguém tocar nele.
- **Touch or presence detection (Toque ou detecção de presença):** Ative o visor quando alguém tocar nele ou quando o dispositivo detectar alguém em frente ao visor.

Analíticos

AXIS Object Analytics

Start (Iniciar): Clique para iniciar o AXIS Object Analytics. O aplicativo será executado em segundo plano e você poderá criar regras para eventos com base nas configurações atuais do aplicativo.

Open (Abrir): Clique para abrir o AXIS Object Analytics. O aplicativo abre em uma nova aba do navegador onde você pode configurar suas configurações.

- **Não instalado:** O AXIS Object Analytics não está instalado neste dispositivo. Atualize o AXIS OS para a versão mais recente para obter a versão mais recente do aplicativo.

Configuração de metadados

Produtores de metadados RTSP

Exiba e gerencie os canais de dados que transmitem metadados e dos canais que eles utilizam.

Observação

Essas configurações são destinadas a streams de metadados RTSP que usam ONVIF XML. As alterações feitas aqui não afetam a página de visualização de metadados.

Producer (Produtor): Um canal de dados que utiliza o Protocolo de Stream em Tempo Real (RTSP) para enviar metadados.

Canal: O canal utilizado para enviar metadados de um produtor. Ative para habilitar o stream de metadados. Desative por motivos de compatibilidade ou gerenciamento de recursos.

MQTT

Configure os produtores que geram e transmitem metadados por MQTT (Message Queuing Telemetry Transport).

-  **Crie:** Clique para criar um novo produtor MQTT.
 - **Key (Chave):** Selecione um identificador predefinido na lista suspensa para especificar a origem do stream de metadados.
 - **MQTT topic (Tópico MQTT):** Insira um nome para o tópico MQTT.
 - **QoS (Quality of Service) (Qualidade de Serviço):** Defina o nível de garantia de entrega de mensagens (0-2).

Retain messages (Reter mensagens): Escolha se deseja manter a última mensagem no tópico MQTT.

Use o prefixo do tópico do dispositivo cliente MQTT: Escolha se deseja adicionar um prefixo ao tópico MQTT para ajudar a identificar o dispositivo de origem.

- O menu de contexto contém:
 - **Update (Atualizar):** Modifique as configurações do produtor selecionado.
 - **Excluir:** Exclua o produtor selecionado.

Object snapshot (Instantâneo do objeto): Ative para incluir uma imagem recortada de cada objeto detectado.

Additional crop margin (Margem adicional de corte): Ative para adicionar margem extra ao redor das imagens recortadas dos objetos detectados.

PTZ

Posições predefinidas

Uma posição predefinida é uma posição de pan, tilt e zoom específica armazenada na memória da câmera. Você pode usar posições predefinidas para navegar rapidamente entre diferentes campos de exibição. Se seu dispositivo oferecer suporte a guard tours, você poderá usar posições predefinidas para criar guard tours automatizados.

Posições predefinidas

-  **Criar posição predefinida:** Crie uma nova posição predefinida com base na posição atual da câmera.
 - **Thumbnail (Miniatura):** Ative para adicionar uma imagem de miniatura para a posição predefinida.
 - **Nome:** Insira um nome para a posição de pré-ajuste.
 - **Home position (Posição inicial):** Ative para definir essa posição como o campo de visão padrão da câmera. A posição inicial é marcada com . A câmera sempre terá uma posição inicial.

Definições

- **Return to home position when inactive (Retornar para posição inicial quando inativo):** Ative-a para fazer a câmera retornar à posição inicial após um período especificado de inatividade.
- **Use thumbnails (Usar miniaturas):** Ative para adicionar automaticamente uma miniatura a qualquer posição predefinida que você criar.
- ⋮
- O menu de contexto contém:
 -  **Criar miniaturas**: Crie uma miniatura para todas as suas posições predefinidas.
 - **Refresh thumbnails (Atualizar miniaturas):** Substitua as miniaturas para suas posições predefinidas por miniaturas novas e atualizadas.
 - **Delete all preset positions (Excluir todas as posições predefinidas):** Remova todas as suas posições predefinidas. Isso também criará uma nova posição inicial automaticamente.

Modo de ronda



Guard tour: Crie um guard tour.

- **Posição predefinida:** Selecione para criar um guard tour com posições predefinidas.
- **Recorded (Gravado):** selecione para criar um guard tour gravado.

Posição predefinida

Um guard tour com posições predefinidas transmite continuamente imagens de uma seleção de posições predefinidas em uma sequência aleatória ou fixa. Você pode escolher por quanto tempo a câmera deve permanecer em cada posição predefinida antes de avançar para a próxima. O guard tour (modo de ronda) continuará a funcionar em um loop infinito até você interropê-lo, mesmo quando não houver clientes (navegadores da web) transmitindo as imagens.

Definições

- **Configurações gerais**
 - **Nome:** Insira um nome para o guard tour.
 - **Play guard tour in random order (Reproduzir guard tour em ordem aleatória):** Ative essa opção para fazer a câmera se mover de forma imprevisível entre as posições predefinidas durante o guard tour.
 - **Pause between runs (Pausa entre execuções):** Insira o intervalo de tempo desejado entre os guard tours. Você pode inserir qualquer intervalo de 0 minutos a 2 horas e 45 minutos.
- **Configurações de etapas**
 - **Duration (Duração):** Escolha quanto tempo deseja que a câmera permaneça em cada posição predefinida. O valor padrão é 10 segundos e o valor máximo permitido é de 60 minutos.
 - **Move speed (Velocidade de movimento):** Escolha a velocidade com que deseja que a câmera se move para a próxima posição predefinida. O valor padrão é 70, mas você pode selecionar qualquer valor entre 1 – 100.

Preset positions (Posições predefinidas): Para selecionar várias posições predefinidas, pressione SHIFT enquanto seleciona as posições predefinidas. Clique em  e arraste as posições predefinidas para a área **View order (Ordem de exibição)**.

View order (Ordem de exibição): Exibe as posições predefinidas incluídas no guard tour.

- **Import all preset positions (Importar todas as posições predefinidas):** Adicione todas as posições predefinidas na ordem em que foram criadas, começando pela mais antiga.
-  : Inicie o guard tour.

Gravado

Um tour gravado reproduz uma sequência gravada de movimentos de pan/tilt/zoom, incluindo suas velocidades e distâncias variáveis.

Configurações gerais

- **Nome:** Insira um nome para o guard tour.
- **Pause between runs (Pausa entre execuções):** Insira o intervalo de tempo desejado entre os guard tours. Você pode inserir qualquer intervalo de 0 minutos a 2 horas e 45 minutos.

Tour gravado

- **Start recording tour (Iniciar tour de gravação):** Comece a gravar os movimentos de pan/tilt/zoom que deseja que o guard tour reproduza.
- **Stop recording tour (Parar tour de gravação):** Pare de gravar os movimentos de pan/tilt/zoom que deseja que o guard tour reproduza.
- **Regravar:** Inicie uma nova gravação de movimentos de pan/tilt/zoom. Isso substituirá sua gravação mais recente.
-  Iniciar o tour gravado.
-  Pausar o tour gravado.
-  Parar o tour gravado.

Limites

Para restringir a área sob monitoramento, você pode limitar os movimentos de PTZ.

Salvar como pan 0°: Clique para definir a posição atual como ponto zero para coordenadas de pan.

Pan-tilt limits (Limites de pan-tilt): A câmera usa as coordenadas do centro da imagem quando você define limites de pan-tilt.

-  **Limite de pan esquerdo:** Clique para limitar os movimentos de pan da câmera para a esquerda. Clique novamente para remover o limite.
-  **Limite de pan direito:** Clique para limitar os movimentos de pan da câmera para a direita. Clique novamente para remover o limite.
-  **Limite de tilt superior:** Clique para limitar os movimentos de tilt da câmera para a parte superior. Clique novamente para remover o limite.
-  **Limite de tilt inferior:** Clique para limitar os movimentos de tilt da câmera para a parte inferior. Clique novamente para remover o limite.

Inversão automática  : Permite que a cabeça da câmera reverta 360° instantaneamente e continue a fazer pan além de seu limite mecânico.

E-flip  : Corrige automaticamente a exibição da câmera invertendo a imagem em 180° quando a câmera inclina além de -90°.

Flip Nadir  : Permite que a câmera faça pan de 180° ao inclinar além de -90° e, em seguida, continue para cima.

Limite do zoom: Selecione um valor para limitar o nível de zoom máximo da câmera. Óptica ou digital (por exemplo 480x D) valores podem ser selecionados. Quando um joystick é usado, somente níveis de zoom digitais podem ser aplicados para definir o limite de zoom.

Near focus limit (Limite de foco próximo): Selecione um valor para impedir que a câmera focalize automaticamente em objetos próximos a ela. Dessa forma, a câmera pode ignorar objetos como fios suspensos, postes de luz ou outros objetos próximos. Para fazer a câmera focalizar nas áreas de interesse, defina o limite de foco próximo para um valor que seja superior à distância na qual os objetos que não são de interesse tendem a aparecer.

Movimento

Velocidade proporcional  : Ative para definir a velocidade proporcional máxima.

- **Velocidade proporcional máxima**  : Defina um valor entre 1 e 1000 para limitar a velocidade de pan e tilt. A velocidade proporcional máxima é definida como um percentual, onde o valor 1000 equivale a 1000%.

Isso é útil quando o joystick é empurrado até o fim. Por exemplo, se a imagem possuir aproximadamente 44 graus de abertura com o zoom o mais afastado possível e a velocidade proporcional máxima for 100 (100%), a velocidade máxima será cerca de 44 graus/segundo. Se o zoom da imagem for modificado de 44 para 10 graus de abertura, a velocidade máxima atingirá cerca de 10 graus/segundo, o que provavelmente é muito rápido para uma exibição correta. Para limitar a velocidade, defina a velocidade proporcional máxima como 50 (50%). Dessa forma, a velocidade máxima atingirá somente 50% da máxima para o nível de zoom selecionado no momento. Isso significa que, quando a abertura da imagem é 44 graus, a maior velocidade possível é limitada a cerca de 22 graus/segundo e, quando a exibição é aproximada para 10 graus, a velocidade é limitada a cerca de 5 graus/segundo.

Adjustable zoom speed (Velocidade de zoom ajustável): Ative para usar velocidades variáveis ao controlar o zoom com um joystick ou a roda do mouse. A velocidade de zoom é definida automaticamente pelo comando `continuouszoommove` na interface de programação de aplicativos (API) VAPIX®. Desative para usar a velocidade de zoom mais alta, a qual é a mesma do deslocamento para posições predefinidas.

Congelar imagem em PTZ

- **Off (Desativada)**: Nunca congelar a imagem.
- **All movements (Todos os movimentos)**: Congele a imagem enquanto a câmera está se movendo. Quando a câmera atingir sua nova posição, a exibição dessa posição será mostrada.
- **Preset positions (Posições predefinidas)**: Congele a imagem somente quando a câmera se mover entre posições predefinidas.

Pan-tilt speed (Velocidade de pan/tilt): Selecione a velocidade dos movimentos de pan e tilt da câmera.

Fila de controle

Usar fila de controle

- **PTZ control queue (Fila de controle de PTZ):** Ative para inserir solicitações de controle de PTZ em uma fila. Exibe o status e a posição dos usuários na fila. Para usar os controles de PTZ no AXIS Camera Station, desative essa configuração.
 - **Enter queue (Entrar na fila):** Clique para adicionar sua solicitação de controle de PTZ à fila.
 - **Release control (Liberar controle):** Clique para liberar o controle de PTZ.
- Os grupos de usuários são listados em uma ordem priorizada com a prioridade mais alta na parte superior. Para alterar a prioridade de um grupo de usuários, clique em **=** e arraste o grupo de usuários para cima ou para baixo.

Para cada grupo de usuários:

 - **Timeout duration (Duração do tempo limite):** Defina o tempo que deve ser aguardado antes do tempo limite se esgotar. O valor padrão é de 1 minuto, e os valores permitidos variam de 1 segundo a 60 minutos.
 - **Tipo de tempo limite**
 - **Timespan (Intervalo de tempo):** Tempo limite atingido após a duração definida.
 - **Atividade:** Tempo limite esgotado após atingir a duração definida desde a última atividade.
 - **Infinity (Infinito):** Nunca esgotar o tempo limite até que um usuário com prioridade mais alta assuma o controle.
 - **Use cookie (Usar cookie):** Selecione essa opção para permitir que a câmera reconheça e separe usuários dentro do mesmo grupo de usuários.

Definições

- **Limit number of users in queue (Número limite de usuários na fila):** Defina o número máximo de usuários permitidos em uma fila. O número padrão é 20, e os valores permitidos são 1 – 100.
- **Control queue poll time (Tempo de pesquisa na fila de controle):** Defina a frequência de sondar a câmera para atualizar o local dos usuários ou grupos de usuários na fila. O valor padrão é de 20 segundos, e os valores permitidos variam de 5 segundos a 60 minutos.

Definições

Use PTZ (Usar PTZ): ative para permitir a funcionalidade PTZ na exibição selecionada.

Leitor

Conexão

Leitor externo (Entrada)

Use external OSDP reader (Usar leitor OSDP externo): Ative-o para usar o dispositivo com um leitor externo. Conecte o leitor ao conector do leitor (IO1, IO2, 12V e GND).

Status:

- **Connected (Conectado):** O dispositivo está conectado ao leitor externo ativo.
- **Connecting (Conectando):** O dispositivo está tentando conectar ao leitor externo.
- **Não conectado:** o OSDP está desativado.

Protocolo do leitor

Reader protocol type (Tipo de protocolo do leitor): Selecione o protocolo que será usado para a funcionalidade de leitor.

- **VAPIX reader (Leitor VAPIX):** Pode ser usado somente com um controlador de porta Axis.
 - **Protocol (Protocolo):** Selecione **HTTPS** ou **HTTP**.
 - **Door controller address (Endereço do controlador de porta):** Insira o endereço IP do controlador de porta.
 - **User name (Nome de usuário):** Insira o nome de usuário do controlador de porta.
 - **Senha:** Insira a senha do controlador de porta.
 - **Connect (Conectar):** Clique para conectar ao controlador de portas.
 - **Select reader (Selecionar leitor):** Selecione o leitor de entrada para a porta apropriada.
- **OSDP:**
 - **OSDP address (Endereço OSDP):** Digite o endereço do leitor OSDP. 0 é o endereço padrão e mais comum para leitores únicos.
- **Wiegand** :
 - **Beeper (Sinal sonoro):** Ative para habilitar a entrada de sinal sonoro.
 - **Input for beeper (Entrada para sinal sonoro):** Selecione a porta de E/S usada para o sinal sonoro.
 - **Input used for LED control (Entrada usada para controle de LED):** Selecione quantas portas de E/S serão usadas para controlar o feedback dos LEDs no dispositivo.
 - **Entrada do LED1/LED2:** selecione as portas de E/S a serem usadas para a entrada de LED.
 - **Idle color (Cor de ociosidade):** Se nenhuma porta de E/S for usada para controlar o LED, você poderá selecionar uma cor estática para mostrar na faixa indicadora do leitor de cartões.
 - **Color for state low/high (Cor do estado baixo/alto):** se uma porta de E/S for usada para controle de LEDs, selecione a cor que será mostrada no estado baixo e a cor que será mostrada no estado alto.
 - **Idle color/LED1 color/LED2 color/LED1 + LED2 color (Cor de ociosidade/Cor do LED1/Cor do LED2/Cor do LED1 + LED2):** Se duas portas de E/S forem usadas para controle de LED, selecione as cores que serão mostradas para uso em ociosidade, LED1, LED2 e LED1 + LED2, respectivamente.
 - **Keypress format (Formato de pressionamento de tecla):** Selecione como formatar o PIN quando ele for enviado para a unidade de controle de acesso.
 - **FourBit:** o número de identificação pessoal 1234 é codificado e enviado como 0x1 0x2 0x3 0x4. Esse é o comportamento padrão e mais comum.
 - **EightBitZeroPadded:** o número de identificação pessoal 1234 é codificado e enviado como 0x01 0x02 0x03 0x04.
 - **EightBitInvertPadded:** o número de identificação pessoal 1234 é codificado e enviado como 0xE1 0xD2 0xC3 0xB4.
 - **Wiegand26:** o número de identificação pessoal é codificado no formato Wiegand26 com um código de recurso de 8 bits e um ID de 16 bits.
 - **Wiegand34:** o número de identificação pessoal é codificado no formato Wiegand34 com um código de recurso de 16 bits e um ID de 16 bits.
 - **Wiegand37:** o número de identificação pessoal é codificado em um formato Wiegand37 (H10302) com ID de 35 bits.
 - **Wiegand37FacilityCode:** o número de identificação pessoal é codificado no formato Wiegand37 (H10304) com um código de recurso de 16 bits e um ID de 19 bits.

- **Facility code (Código da instalação):** Insira o código da instalação a ser enviado. Essa opção está disponível somente para alguns formatos de pressionamento de tecla.

Formato da saída

Select data format (Selecionar formato de dados): Selecione em qual formato os dados de cartões serão enviados para a unidade de controle de acesso.

- **Raw (Bruto):** Transmite os dados do cartão da forma como estão.
- **Wiegand26:** codifica os dados do cartão no formato Wiegand26 com um código de recurso de 8 bits e um ID de 16 bits.
- **Wiegand34:** codifica os dados do cartão no formato Wiegand34 com um código de recurso de 16 bits e um ID de 16 bits.
- **Wiegand37:** codifica os dados do cartão no formato Wiegand37 (H10302) com ID de 35 bits.
- **Wiegand37FacilityCode:** codifica os dados do cartão no formato Wiegand37 (H10304) com um código de recurso de 16 bits e ID de 19 bits.
- **Custom (Personalizada):** Defina sua própria formatação.

Facility code override mode (Modo de substituição do código da instalação): Selecione uma opção para substituir o código da instalação.

- **Auto:** Não anula o código da instalação e cria um código de instalação a partir da detecção automática de dados de entrada. Usa o código da instalação original do cartão ou cria-o usando os bits excedentes de um número de cartão.
- **Optional (Opcional):** Usa o código de instalação dos dados de entrada ou substitui com um valor opcional configurado.
- **Override (Substituir):** Sempre substitui com um código de recurso instalação.

Tipos de chip

Tipos de chip

Activate chip type (Ativar tipo de chip): Selecione um tipo de chip na lista para ativá-lo.

Active chip types (Tipos de chip ativos) mostra uma lista de todos os tipos de chips ativos e se eles usam conjuntos de dados padrão ou personalizados.

- ⋮ O menu de contexto contém:
 - **Deactivate (Desativar):** Clique para remover o tipo de chip da lista de tipos de chips ativos.

Conjuntos de dados

Invert byte order for all chip types using the full card serial number (Inverter a ordem dos bytes para todos os tipos de chip usando o número de série completo do cartão (CSN)): ative para inverter a ordem dos bytes do número de série do cartão. O número de série do cartão são os dados padrão.

Invert byte order for all chip types using secure card data (Inverter a ordem dos bytes para todos os tipos de chip que usam dados de cartão seguros): Ative para reverter a ordem de byte dos dados de cartões seguros para os tipos de chips que usam um conjunto de dados personalizado.

Add data set (Adicionar conjunto de dados): Selecione um tipo de chip e clique para adicionar um conjunto de dados. Para dados personalizados.

- **Name of data set (Nome do conjunto de dados):** Renomeie o conjunto de dados para obter ajuda para identificar os dados. O nome deve ser único. Ele funciona como um ID na, por exemplo, API.
- **Enabled (Ativado):** Desative para parar de usar o conjunto de dados sem excluí-lo.
- **Required data (Dados necessários):** Se dados de cartões seguros por algum motivo não estiverem acessíveis, o dispositivo não enviará dados para o controlador de portas quando essa configuração estiver ativada. Desligue para enviar o CSN para o controlador de portas caso os dados seguros do cartão não possam ser acessados.
- **Use as authenticator (Usar como autenticador):** Desative se não desejar usar dados de cartões seguros para autenticação, mas enviá-los apenas como metadados válidos para o protocolo VAPIX.
- **Offset (bits) (Deslocamento (bits)):** insira a posição inicial dos dados. O significa que a posição inicial é o primeiro bit.
- **Length (bits) (Comprimento (bits)):** digite o comprimento dos dados. O significa que qualquer comprimento de dados será lido.
- **Use data on card (Usar dados no cartão):** Ative-o para usar dados de cartões seguros. Desligue para usar o CSN em vez de proteger os dados do cartão.

As demais configurações são específicas do tipo de chip e são usadas para definir como ler dados de cartões seguros.

PIN

As configurações de PIN devem coincidir com aquelas configuradas na unidade de controle de acesso.

Comprimento (0-32): insira o número de dígitos no número de identificação pessoal. Se os usuários não forem obrigados a usar um número de identificação pessoal ao usar o leitor, configure o comprimento como 0.

Tempo limite (segundos, 3-50): insira o número de segundos decorridos antes que o dispositivo retorne ao modo ocioso quando nenhum PIN for recebido.

Lista de entradas

Com a Lista de entradas, você pode configurar o dispositivo para permitir que os detentores de credenciais usem seus respectivos cartões, PINs ou um QR Code® para executar diferentes ações, como abrir uma porta. As credenciais são armazenadas localmente no dispositivo. Você também pode combinar essa funcionalidade com um controlador de porta externo.

QR Code é uma marca registrada da Denso Wave Incorporated no Japão e em outros países.

Detentores de credenciais

Use Entry list (Usar a lista de entradas): ative para usar a funcionalidade Lista de entradas.

Use connected door controller (Usar controlador de porta conectado): ative se o dispositivo já estiver conectado a um controlador de porta. Se alguém apresentar uma credencial que não existe na lista de entrada, enviaremos a solicitação para o controlador de porta conectado. Não enviamos as credenciais disponíveis na lista de entrada.

Add credential holder (Adicionar detentor de credencial): clique para adicionar um novo detentor de credencial.

First name (Nome): Insira um primeiro nome.

Last name (Sobrenome): insira um sobrenome.

Credential type (Tipo de credencial):

- **PIN:**
 - PIN: insira um número de identificação pessoal exclusivo ou clique em **Generate (Gerar)** para criar um automaticamente.
- **Card (Cartão):**
 - UID: insira o UID e o comprimento do bit do cartão ou clique em **Get latest (Obter o mais recente)** para buscar os dados da última passagem de cartão
- **QR Code®**

Event condition (Condição de evento): selecione uma ou mais condições para serem acionadas quando o detentor de credencial usar sua credencial. Para configurar a ação resultante, acesse **System > Events (Sistema > Eventos)** e crie uma regra usando a mesma condição selecionada aqui.

Valid from (Válido de): Selecione **Current device time (Hora atual do dispositivo)** para ativar a credencial imediatamente. Limpe para especificar quando ativar a credencial.

Valid to (Válido até):

- **No end date (Sem data de término):** a credencial é válida por tempo indeterminado.
- **End date (Data final):** especifique a data e a hora em que a credencial se tornará inválida.
- **Number of times (Número de vezes):** especifique quantas vezes o detentor da credencial pode usar a credencial. O valor no campo é reduzido à medida que a credencial é usada para exibir os usos restantes.

Observações: insira informações opcionais.

Suspend (Suspender): selecione para tornar a credencial temporariamente inválida.

Download QR Code when saving (Baixar QR Code ao salvar): Se você selecionou QR Code como tipo de credencial, marque essa caixa de seleção para fazer download do QR Code ao clicar em **Save (Salvar)**.

Registro de eventos

O registro de eventos mostra uma lista de eventos da lista de entradas. O tamanho máximo do arquivo de registro é de 2 MB, o que equivale a aproximadamente 6000 eventos.

Export all (Exportar todos): clique para exportar todos os eventos da lista. Para exportar apenas um subconjunto, selecione os eventos de seu interesse. Os eventos são exportados para um arquivo CSV.

Filtro: clique para mostrar os eventos que ocorreram em uma faixa de tempo específica.

 : digite para pesquisar todo o conteúdo correspondente na lista.

Áudio

Configurações do dispositivo

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

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.

Noise cancellation (Cancelamento de ruído): Ative para aprimorar a qualidade do áudio removendo ruídos de fundo.

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.

Controle automático de volume  : Ative para que o dispositivo ajuste o ganho de forma automática e dinâmica, com base no nível de ruído ambiente. O controle automático de volume afeta todas as saídas de áudio, incluindo linha e telebobina.

Stream

Codificação: Selecione a codificação que será usada para a transmissão 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

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

- Inicie uma gravação no dispositivo.
-  Escolha o dispositivo de armazenamento que será usado para salvar.
- Pare uma gravação no dispositivo.

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

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

-  Reproduza a gravação.
-  Pare a execução da gravação.
-  Mostre ou oculte informações sobre a gravação.

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

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

-  Clique para excluir uma gravação.

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



Clique para filtrar as gravações.

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

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

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

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

Armazenamento: mostra gravações com base no tipo de armazenamento.

Mídia

+ Add (Adicionar): Clique para adicionar um novo arquivo.

Storage location (Local de armazenamento): Escolha armazenar o arquivo na memória interna ou no armazenamento interno (cartão SD, se disponível).



O menu de contexto contém:

- **Information (Informações):** Exiba informações sobre o arquivo.
- **Copy link (Copiar link):** Copie o link do local do arquivo no dispositivo.
- **Excluir:** Exclua o arquivo do local de armazenamento.

Apps



Adicionar app: Instale um novo aplicativo.

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



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



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

Observação

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

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

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



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

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

Sistema

Hora e local

Data e hora

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

Observação

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

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

- **Data e hora automática (PTP):** Sincronize usando o protocolo de tempo de precisão.
- **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.
 - **Certificados NTS KE CA confiáveis:** Selecione os certificados CA confiáveis a serem usados para sincronização segura de hora NTS KE ou deixe como nenhum.
 - **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. O representa o norte.
- **Label (Rótulo):** Insira um nome descritivo para seu dispositivo.
- **Save (Salvar):** Clique em para salvar a localização do dispositivo.

Verificação de configuração

Imagen de dispositivo interativa: Clique nos botões na imagem para simular pressionamentos de teclas reais. Isso permite que você experimente configurações ou solucione problemas de hardware sem ter acesso físico ao dispositivo.

Credenciais mais recentes  : Mostra informações sobre as credenciais registradas pela última vez.

  Mostra os dados mais recentes das credenciais.

  O menu de contexto contém:

- **Inverter UID:** inverte a ordem de byte do UID.
- **Inverter UID:** inverte a ordem de byte do UID de volta para a ordem original.
- **Copiar para área de transferência:** Copie o UID.

Verificar credenciais  : Insira um UID ou um PIN e envie-o para verificar as credenciais. O sistema responderá da mesma forma que se você tivesse usado as credenciais no dispositivo. Se tanto o UID quanto o PIN forem necessários, insira o UID.

Rede

IPv4

Assign IPv4 automatically (Atribuir IPv4 automaticamente): Selecionar a opção de IP de IPv4 automático (DHCP) para permitir que a rede atribua seu endereço IP, máscara de sub-rede e roteador automaticamente, sem a necessidade de configuração manual. Recomendamos o uso da atribuição automática de IP (DHCP) para a maioria das redes.

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

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

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

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

Observação

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

IPv6

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

Nome de host

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

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

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

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

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

Servidores DNS

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

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

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

Observação

Se o DHCP estiver desativado, recursos que dependem da configuração automática de rede, como nome de host, servidores DNS, NTP e outros, podem parar de funcionar.

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 (ProxyHttps): 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 O3):

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

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

Host: Insira o endereço do servidor proxy.

Porta: Insira o número da porta usada para acesso.

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

Authentication method (Método de autenticação):

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

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

SNMP

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

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

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

Observação

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

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

Segurança

Certificados

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

- **Certificados cliente/servidor**

Um certificado cliente/servidor valida a identidade do produto e pode ser autoassinado ou emitido por uma autoridade de certificação (CA). Um certificado autoassinado oferece proteção limitada e pode ser usado antes que um certificado emitido por uma CA tenha sido obtido.

- **Certificados CA**

Você pode usar um certificado de CA para autenticar um certificado de par, por exemplo, para validar a identidade de um servidor de autenticação quando o dispositivo se conecta a uma rede protegida por IEEE 802.1X. O dispositivo possui vários certificados de CA pré-instalados.

Os seguintes formatos são aceitos:

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

Importante

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



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

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



O menu de contexto contém:

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

Secure keystore (Armazenamento de chaves seguro) :

- **Trusted Execution Environment (SoC TEE)**: Selecione para usar o SoC TEE para armazenamento de chaves seguro.
- **Secure element (CC EAL6+, FIPS 140-3 Level 3) (Elemento seguro [CC EAL6+, FIPS 140-3 Nível 3])** : Selecione para usar o elemento seguro no armazenamento de chaves seguro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Nível 2)** : Selecione para usar TPM 2.0 para armazenamento de chaves seguro.

Controle de acesso à rede e criptografia

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificados

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

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

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

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

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

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

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

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

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

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

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

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

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

Impedir ataques de força bruta

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

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

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

Firewall

Firewall: Ative para ativar o firewall.

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

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

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

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

Rule type (Tipo de regra):

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

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

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

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

Certificado do AXIS OS com assinatura personalizada

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

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

- ⋮
- O menu de contexto contém:
 - **Delete certificate (Excluir certificado):** Exclua o certificado.

Contas

Contas



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

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

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

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

Privileges (Privilégios):

- **Administrator (Administrador):** Tem acesso irrestrito a todas as configurações. Os administradores também podem adicionar, atualizar e remover outras contas.
 - **Operator (Operador):** Tem acesso a todas as configurações, exceto:
 - Todas as configurações do **System (Sistema)**.
 - **Viewer (Visualizador):** Tem acesso a:
 - Assistir e capturar instantâneos de uma transmissão 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.

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

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

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

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

Comentário: Insira um comentário (opcional).



⋮ O menu de contexto contém:

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

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

Virtual host (Host virtual)



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

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

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

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

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



• O menu de contexto contém:

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

Disabled (Desativado): o servidor está desativado.

Configuração de concessão de credenciais de cliente

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

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

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

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

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

Save (Salvar): Clique para salvar os valores.

Configuração de OpenID

Importante

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

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

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

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

URL do provedor: Insira o link Web para a autenticação do ponto de extremidade de API. O formato deve ser [https://\[inserir URL\]/.bem conhecido/openid-configuration](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 iniciaativamente as conexões de controle de FTP e dados para o servidor de destino. Isso é normalmente necessário quando há um firewall entre o dispositivo e o servidor FTP de destino.

- **HTTP**

- **URL:** Insira o endereço de rede do servidor HTTP e o script que cuidará da solicitação. Por exemplo, `http://192.168.254.10/cgi-bin/notify.cgi`.
- **Username (Nome de usuário):** insira o nome de usuário para o login.
- **Senha:** insira a senha para o login.
- **Proxy:** ative e insira as informações necessárias se houver a necessidade de passar por um servidor proxy para se conectar ao servidor HTTP.

- **HTTPS**

- **URL:** Insira o endereço de rede do servidor HTTPS e o script que cuidará da solicitação. Por exemplo, `https://192.168.254.10/cgi-bin/notify.cgi`.
- **Validate server certificate (Validar certificado do servidor):** marque para validar o certificado que foi criado pelo servidor HTTPS.
- **Username (Nome de usuário):** insira o nome de usuário para o login.
- **Senha:** insira a senha para o login.
- **Proxy:** ative e insira as informações necessárias se houver a necessidade de passar por um servidor proxy para se conectar ao servidor HTTPS.

- **Armazenamento de rede** 

Você pode adicionar armazenamento de rede, como um NAS (Network Attached Storage), e utilizá-lo como destinatário para armazenar arquivos. Os arquivos são armazenados no formato Matroska (MKV).

- **Host:** Insira o endereço IP ou o nome de host do armazenamento de rede.
- **Compartilhamento:** Insira o nome do compartilhamento no host.

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

- **SFTP**

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

- **SIP ou VMS** :

SIP: Selecione para fazer uma chamada SIP.

VMS: Selecione para fazer uma chamada VMS.

- **From SIP account (Da conta SIP):** selecione na lista.
- **To SIP address (Para endereço SIP):** Insira o endereço SIP.
- **Teste:** Clique para testar se suas configurações de chamada funcionam.

- **E-mail**

- **Enviar email para:** insira o endereço para enviar os emails. Para inserir vários emails, use vírgulas para separá-los.
- **Enviar email de:** insira o endereço de email do servidor de envio.
- **Username (Nome de usuário):** insira o nome de usuário para o servidor de email. Deixe esse campo em branco se o servidor de email não precisar de autenticação.

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

Observação

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

- **TCP**

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

Testar: clique para testar a configuração.



O menu de contexto contém:

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

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

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

Programações

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



Adicionar agendamento: clique para criar um cronograma ou pulso.

Acionadores manuais

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

MQTT

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

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

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

ALPN 

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

Cliente MQTT

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

Status: Mostra o status atual do cliente MQTT.

Broker

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

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

Porta: Insira o número da porta.

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

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

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

Senha: Insira uma senha para o nome de usuário.

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

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

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

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

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

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

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

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

Mensagem de conexão

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

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

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

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

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

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

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

Mensagem de Último desejo e testamento

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

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

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

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

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

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

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

Publicação MQTT

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

Incluir condição: selecione para incluir o tópico que descreve a condição no tópico MQTT.

Incluir espaços de nome: selecione para incluir espaços para nome de tópico ONVIF no tópico MQTT.

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



Adicionar condição: clique para adicionar uma condição.

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

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

QoS: selecione o nível desejado para a publicação MQTT.

Assinaturas MQTT

Adicionar assinatura: clique para adicionar uma nova assinatura MQTT.

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

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

Subscription type (Tipo de assinatura):

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

QoS: selecione o nível desejado para a assinatura MQTT.

Sobreposições MQTT

Observação

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



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

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

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

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

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

Armazenamento

Armazenamento de rede

Network storage (Armazenamento de rede): Ative para usar o armazenamento de rede.

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

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

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

Unbind (Desvincular): Clique para desvincular e desconectar o compartilhamento de rede.

Bind (Vincular): Clique para vincular e conectar o compartilhamento de rede.

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

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

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

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

Ferramentas

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

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

Armazenamento interno

Importante

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

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

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

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

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

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

Ferramentas

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

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

Wear trigger (Acionador de uso): Defina um valor para o nível de uso do cartão SD no qual você deseja acionar uma ação. O nível de desgaste varia de 0 a 200%. Um novo cartão SD que nunca foi usado tem um nível de desgaste de 0%. Um nível de desgaste de 100% indica que o cartão SD está próximo de seu tempo de vida esperado. Quando o nível de desgaste atinge 200%, há um alto risco de falha do cartão SD.

Recomendamos configurar o acionador de desgaste entre 80 – 90%. Isso permite baixar qualquer gravação, bem como substituir o cartão SD a tempo antes que ele possa se deteriorar. O acionador de desgaste permite a você configurar um evento e obter uma notificação quando o nível de desgaste atingir o valor definido.

Perfis de stream

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



Add stream profile (Adicionar perfil de transmissão): Clique para criar um novo perfil de transmissão.

Preview (Visualizar): Uma visualização da transmissão de vídeo com as configurações de perfil de transmissão 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.

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)**.
 - Adicionando aplicativos.
 - **Media account (Conta de mídia):** Permite acesso apenas à transmissão 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.

- **Selezione 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.

- **Selezione 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.

- **Selezione a configuração:** Selecione uma configuração definida pelo usuário da lista e ajuste as configurações de áudio. As configurações 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.

- **Selezione a configuração:** Selecione 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.

- **Selezione 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.

- **Selezione 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.

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



PTZ : Selecione as configurações PTZ para a sua configuração.

- **Selezione 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.

Detektoren

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): move 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.

Configurações de energia

Status de potência

Mostra as informações de status de potência. As informações variam de acordo com o produto.

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 consumo dinâmico)  : Ative-o para reduzir o consumo de energia quando o dispositivo estiver inativo.

Power warning overlay (Sobreposição de aviso de energia)  : Ative para exibir uma sobreposição de aviso de energia quando o dispositivo não tiver energia suficiente.

I/O port power (Alimentação da porta de E/S)  : Ative para fornecer alimentação de 12 V aos dispositivos externos conectados às portas de E/S. Deixe desativado para priorizar as funções internas, como IR, aquecimento e resfriamento. Resultado: os dispositivos e sensores que requerem alimentação de 12 V deixarão de funcionar corretamente.

Medidor de potência

Uso de energia

Mostra o uso de energia atual, o uso médio de energia, o uso máximo de energia e o consumo de energia ao longo do tempo.

- ⋮ O menu de contexto contém:
 - **Export (Exportar)**: Clique em para exportar os dados do gráfico.

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.

Usage (Uso): A opção padrão para a porta de relé é **Door (Porta)**. Para dispositivos com ícones indicadores,

 torna-se verde quando o estado muda e a porta é destrancada. Se você usa o relé para algo diferente de uma porta e não quer que o ícone acenda quando o estado mudar, selecione uma das outras opções para 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.

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.
- **View the audit log (Exibir o log de auditoria):** Clique para exibir informações sobre as atividades do usuário e do sistema, por exemplo, autenticações e configurações bem-sucedidas ou com falha.

Acesse o sistema remotamente

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



Servidor: Clique para adicionar um novo servidor.

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

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

- Axis
- RFC 3164
- RFC 5424

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

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

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

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

Tipo: Selecione os tipos de registros que deseja enviar.

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

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

Configuração simples

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

Manutenção

Manutenção

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

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

Importante

As únicas configurações que permanecem salvas após a restauração são:

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

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

Observação

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

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

Ao atualizar, é possível escolher entre três opções:

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

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

solução de problemas

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

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

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

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

Rastreamento de rede

Importante

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

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

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

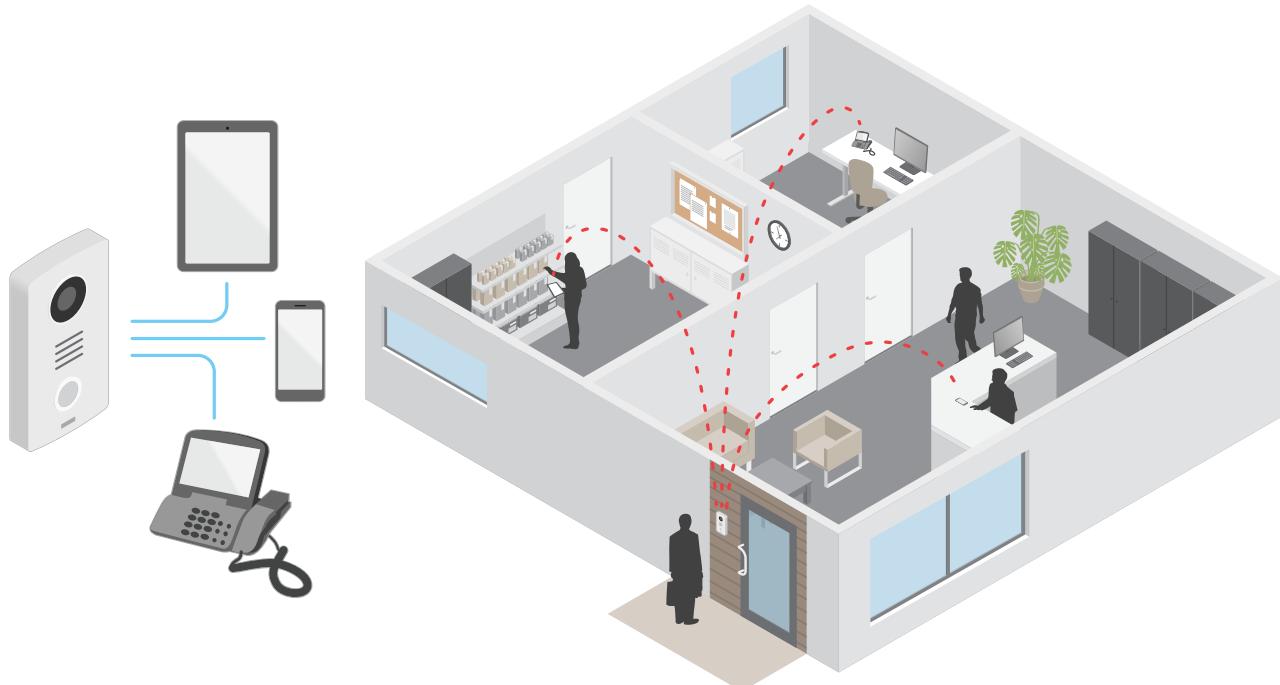
Saiba mais

Voice over IP (VoIP)

Voice over IP (VoIP) é um grupo de tecnologias que permite a comunicação por voz e sessões multimídia via redes IP, como a Internet. Em chamadas telefônicas tradicionais, os sinais analógicos são enviados através de transmissões de circuito através da rede de telefonia comutada pública (PSTN). Em uma chamada VoIP, os sinais analógicos são convertidos em sinais digitais para possibilitar o envio de pacotes de dados via redes IP locais ou pela Internet.

No produto Axis, o VoIP é possibilitado pelo Session Initiation Protocol (SIP) e a sinalização Dual-Tone multi-Frequency (DTMF).

Exemplo:



Quando você pressiona o botão de chamada em um intercomunicador Axis, uma chamada é iniciada para um ou mais destinatários predefinidos. Quando um destinatário responde, uma chamada é estabelecida. A voz e o vídeo são transmitidos por meio de tecnologias VoIP.

Session Initiation Protocol (SIP)

O Session Initiation Protocol (SIP) é usado para configurar, manter e encerrar chamadas de VoIP. Você pode fazer chamadas entre duas ou mais partes, chamadas de agentes de usuário SIP. Para fazer uma chamada SIP, você pode usar, por exemplo, telefones SIP, softphones ou dispositivos Axis compatíveis com SIP.

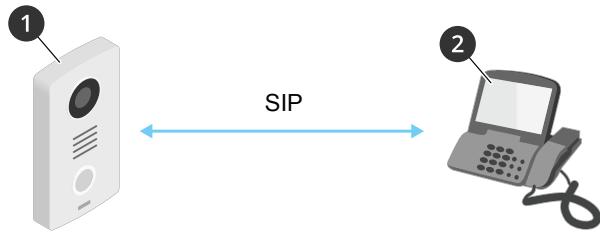
O áudio ou vídeo efetivos são trocados entre os agentes de usuário SIP com um protocolo de transporte, por exemplo, RTP (Real-Time Transport Protocol).

Você pode fazer chamadas em redes locais usando uma configuração ponto a ponto ou através de redes que usam um PBX.

SIP ponto a ponto (P2PSIP)

O tipo mais básico de comunicação SIP ocorre diretamente entre dois ou mais agentes de usuário SIP. Isso é chamado de SIP ponto a ponto (P2PSIP). Se ele ocorre em uma rede local, tudo o que é necessário são os endereços SIP dos agentes de usuário. Um endereço SIP típico, nesse caso, seria `sip:<local-ip>`.

Exemplo:



- 1 Agente de usuário A – intercomunicador. Endereço SIP: `sip:192.168.1.101`
 2 Agente de usuário B – telefone compatível com SIP. Endereço SIP: `sip:192.168.1.100`

Você pode configurar o intercomunicador Axis para chamar, por exemplo, um telefone compatível com SIP na mesma rede usando uma configuração de SIP ponto a ponto.

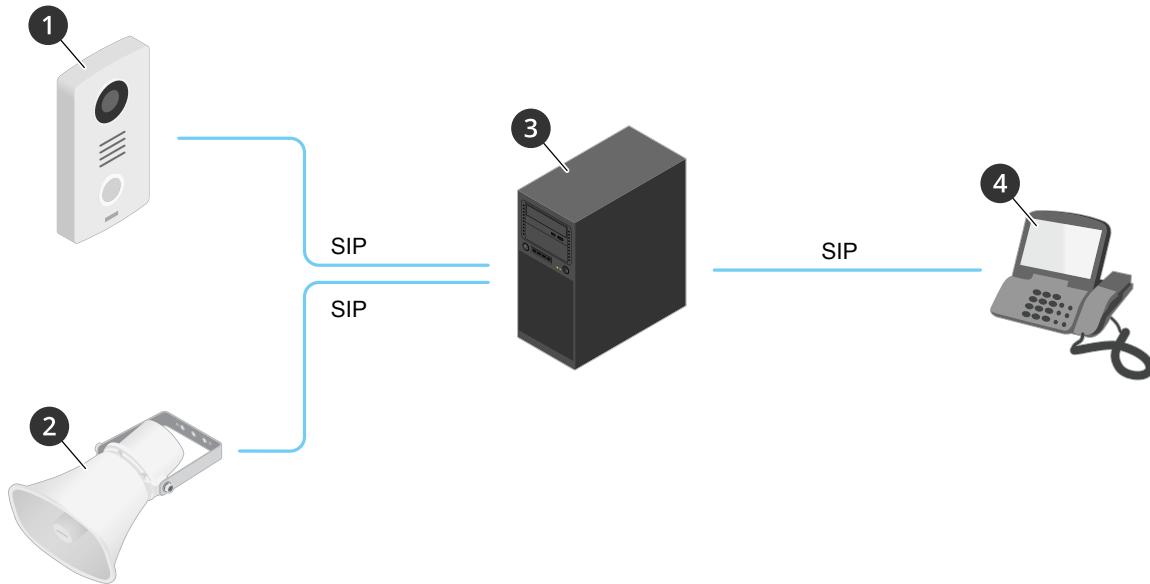
Private Branch Exchange (PBX)

Quando você faz chamadas SIP fora da sua rede IP local, um PBX (Private Branch Exchange) pode atuar como hub central. O componente principal de um PBX é um servidor SIP, o qual também é conhecido como proxy SIP ou registrador. Um PBX funciona como uma mesa telefônica tradicional, mostrando o status atual do cliente e permitindo transferências de chamadas, correio de voz e redirecionamentos.

O servidor SIP de PBX pode ser configurado como uma entidade local ou externa. Ele pode ser hospedado em uma intranet ou por um provedor terceirizado. Quando você faz chamadas SIP entre redes, as chamadas são roteadas através de um conjunto de PBXs, que consultam o local do endereço SIP a ser acessado.

Cada agente de usuário SIP registra-se no PBX e pode, em seguida, alcançar os outros discando o ramal correto. Um endereço SIP típico, nesse caso, seria `sip:<user>@<domain>` ou `sip:<user>@<registrar-ip>`. O endereço SIP é independente de seu endereço IP e o PBX torna o dispositivo acessível, desde que esteja registrado no PBX.

Exemplo:



- 1 `sip:minhporto@empresa.com`
 2 `sip:meualtofalante@empresa.com`
 3 **PBX** `sip.empresa.com`
 4 `sip:escritorio@empresa.com`

Quando você pressiona o botão de chamada em um intercomunicador Axis, a chamada é encaminhada através de um ou mais PBXs para um endereço SIP na rede IP local ou via Internet.

NAT traversal

Use o NAT (Network Address Translation) traversal quando o dispositivo Axis estiver localizado em uma rede privada (LAN) e você deseja acessá-lo de fora dessa rede.

Observação

O roteador deve ser compatível com o NAT traversal e 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 Axis 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 do servidor TURN e as informações de login.

Configuração de regras de eventos

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

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

Aplicativos

Usando aplicativos, você pode obter mais do seu dispositivo Axis. A AXIS Camera Application Platform (ACAP) é uma plataforma aberta que permite que qualquer pessoa desenvolva aplicativos de análise e outros aplicativos para dispositivos Axis. Os aplicativos podem ser pré-instalados no dispositivo, disponibilizados para download gratuitamente ou mediante uma tarifa de licença.

Para encontrar manuais de usuário para aplicativos da Axis, vá para help.axis.com.

Cibersegurança

Para obter informações específicas do produto sobre segurança cibernética, consulte a folha de dados do produto em axis.com.

Para obter informações detalhadas sobre segurança cibernética no AXIS OS, leia o *guia para aumento do nível de proteção do AXIS OS*.

Serviço de notificação de segurança Axis

A Axis fornece um serviço de notificação com informações sobre vulnerabilidades e outras questões relacionadas à segurança para os dispositivos Axis. Para receber notificações, inscreva-se em axis.com/security-notification-service.

Gerenciamento de vulnerabilidades

Para minimizar o risco de exposição dos clientes, a Axis, na condição de Autoridade de Numeração (CNA) de Vulnerabilidades e Exposições Comuns (CVE), segue os padrões do setor para gerenciar e responder a vulnerabilidades descobertas em nossos dispositivos, software e serviços. Para obter mais informações sobre a

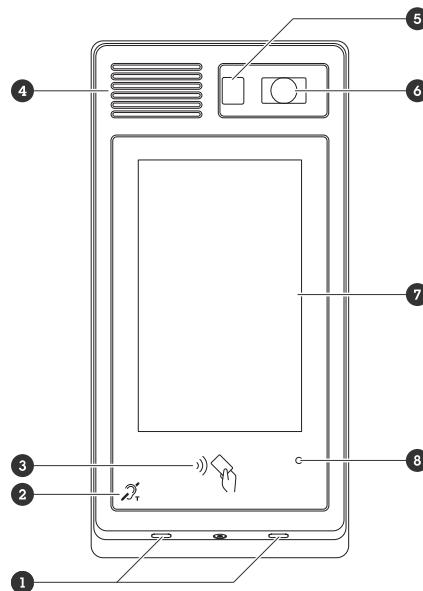
política de gerenciamento de vulnerabilidades da Axis, como relatar vulnerabilidades, vulnerabilidades já conhecidas e as respectivas orientações de segurança, consulte axis.com/vulnerability-management.

Operação segura de dispositivos Axis

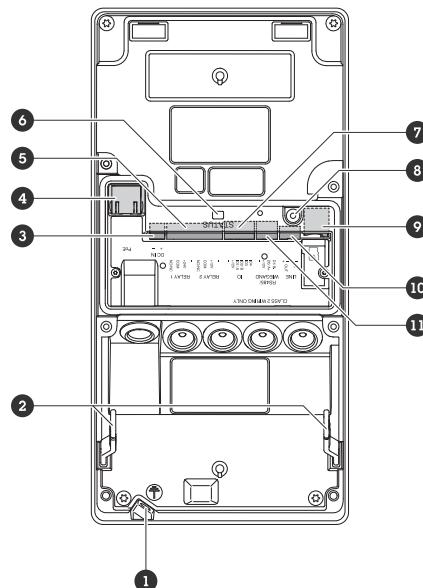
Os dispositivos Axis com configurações padrão de fábrica são pré-configurados com mecanismos de proteção padrão seguros. Recomendamos usar mais configuração de segurança ao instalar o dispositivo. Para saber mais sobre a abordagem da Axis em relação à segurança cibernética, incluindo práticas recomendadas, recursos e diretrizes para proteger seus dispositivos, acesse <https://www.axis.com/about-axis/cybersecurity>.

Especificações

Visão geral do produto



- 1 Microfone (x2)
- 2 Bobina T
- 3 Leitor RFID
- 4 Alto-falante
- 5 Sensor PIR
- 6 Câmera
- 7 Visor
- 8 Sensor de luminosidade



- 1 Parafuso de aterramento
- 2 Dobradiças de instalação
- 3 Conector de energia
- 4 Conector de rede
- 5 Conector do relé (x2)
- 6 LED de estado
- 7
- 8
- 9
- 10
- 11

- 7 Conector de E/S
- 8 Botão de controle
- 9 Entrada para cartão SD (microSD)
- 10 Conector de áudio
- 11 Conector do leitor

Indicadores de LED

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

Slot de cartão SD

OBSERVAÇÃO

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

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

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

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

Botões

Botão de controle

O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte [Restaurar para configurações padrão](#).

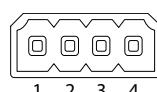
Conectores

Conector de rede

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

Conector de áudio

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

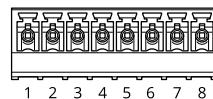


Função	Pino	Observações
Entrada de linha	1	Entrada de áudio (mono)
GND	2	Aterramento de áudio
Saída de linha	3	Saída de linha
GND	4	Aterramento de áudio

Conektor do relé

Bloco de terminais com 8 pinos para relés de estado sólido que podem ser usados das seguintes formas:

- Como um relé padrão que abre e fecha circuitos auxiliares.
- Para controlar diretamente uma trava.
- Para controlar uma trava através de um relé de segurança. Usar um relé de segurança no lado seguro da porta evita hotwiring.



Função	Pino	Observações	Especificações
NO/NC	1	Normalmente aberto/Normalmente fechado Para conectar dispositivos de relé. Os dois pinos de relé estão galvanicamente separados do resto do circuito.	Corrente máxima 1 A Tensão máxima 30 V CC
COM	2	Comum	
24 VCC	3	Para equipamento auxiliar de alimentação. Observação: esse pino pode ser usado somente como saída de energia.	Tensão de saída 24 VCC Corrente máxima 50 mA ¹ Corrente máxima 300 mA ²
Terra CC	4		0 VCC
NO/NC	5	Normalmente aberto/Normalmente fechado Para conectar dispositivos de relé. Os dois pinos de relé estão galvanicamente separados do resto do circuito.	Corrente máxima 1 A Tensão máxima 30 V CC
COM	6	Comum	
12 V CC	7	Para equipamento auxiliar de alimentação. Observação: esse pino pode ser usado somente como saída de energia.	Tensão de saída 12 VCC Corrente máxima 100 mA ¹ Corrente máxima 600 mA ²
Terra CC	8		0 VCC

Conektor do leitor

Bloco de terminais com 4 pinos para conectar leitor externo.

Função	Pino	Observações	Especificações
Terra CC	1		0 VCC
12 V CC	2	Para equipamento auxiliar de alimentação. Observação: esse pino pode ser usado somente como saída de energia.	Tensão de saída 12 VCC

1. Quando alimentado por Power over Ethernet IEEE 802.3af/802.3at Tipo 1 Classe 3.

2. Quando alimentado por Power over Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Classe 4 ou entrada de alimentação CC.

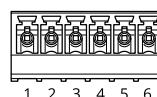
D0/A+	3	Wiegand: saída DATA0 RS485: A+	
D1/B-	4	Wiegand: saída DATA1 RS485: B-	

Conector de E/S

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

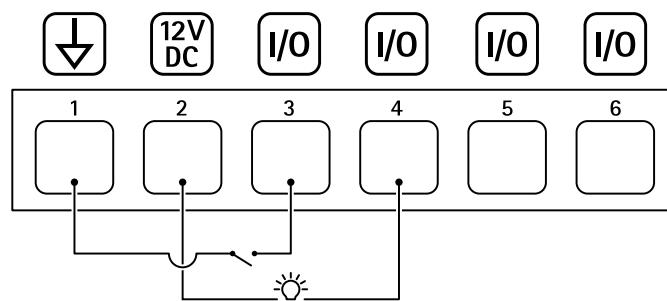
Entrada digital – Para conectar dispositivos que podem alternar entre um circuito aberto ou fechado, por exemplo, sensores PIR, contatos de portas/janelas e detectores de quebra de vidros.

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.



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

Exemplo:

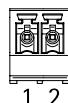


- 1 Terra CC
- 2 Saída CC 12 V, máx. 50 mA
- 3 E/S configurada como entrada
- 4 E/S configurada como saída
- 5 E/S configurável

6 E/S configurável

Conector de energia

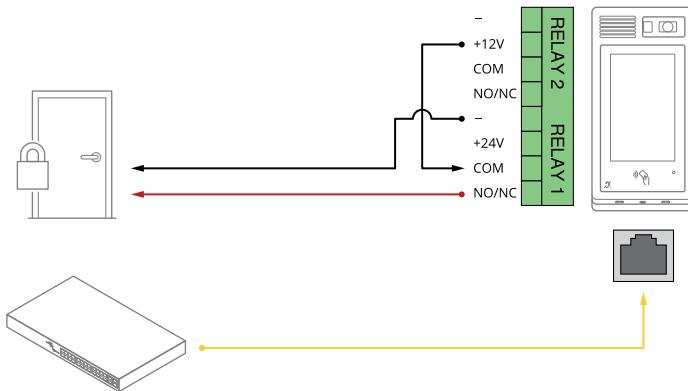
Bloco de terminais com 2 pinos para entrada de energia CC Use uma fonte de energia com limitação (LPS) compatível com os requisitos de voltagem de segurança extra baixa (SELV) e com potência de saída nominal restrita a ≤ 100 W ou corrente de saída nominal limitada a ≤ 5 A.



Função	Pino	Observações	Especificações
Terra CC	1		0 VCC
Entrada CC	2	Para controlador de alimentação sem usar Power over Ethernet. Observação: esse pino pode ser usado somente como entrada de energia.	18 – 28 VCC, máx. 22 W Carga máx. em saídas 9 W

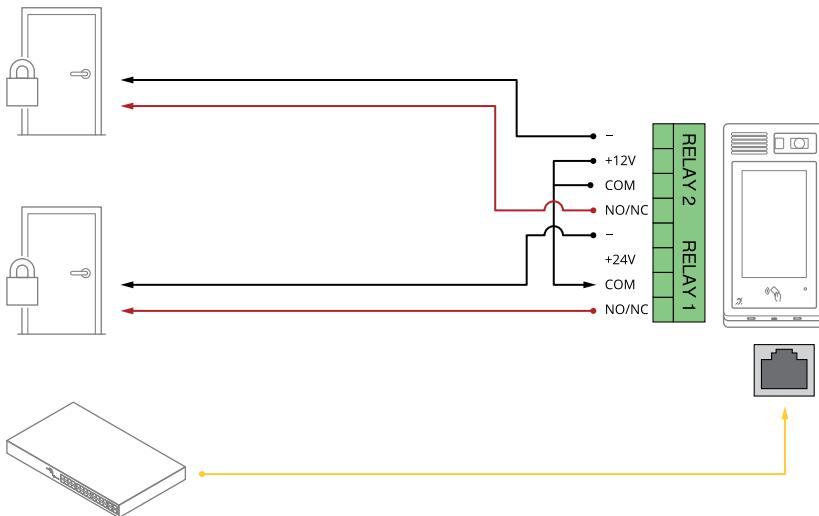
Coneção de equipamentos

Um relé alimentado por PoE (12 V)



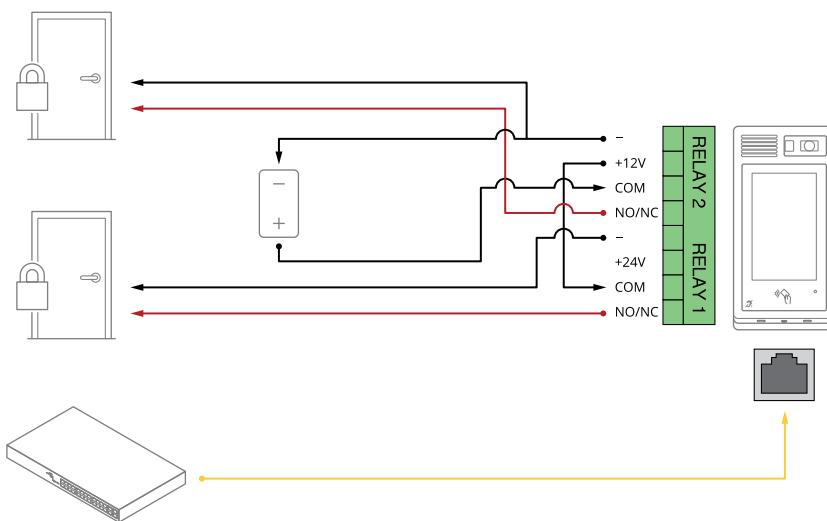
1. Para verificar o estado do relé, vá para **System > Accessories** (Sistema > Acessórios) e encontre a porta do relé.
2. Defina **Normal state** (Estado normal) como:
 - para uma fechadura protegida contra falhas.
 - para uma fechadura protegida contra falhas.

Dois relés alimentados por PoE (12 V)



1. Para verificar o estado do relé, vá para **System > Accessories** (Sistema > Acessórios) e encontre a porta do relé.
2. Defina **Normal state** (Estado normal) como:
 - para uma fechadura protegida contra falhas.
 - para uma fechadura protegida contra falhas.

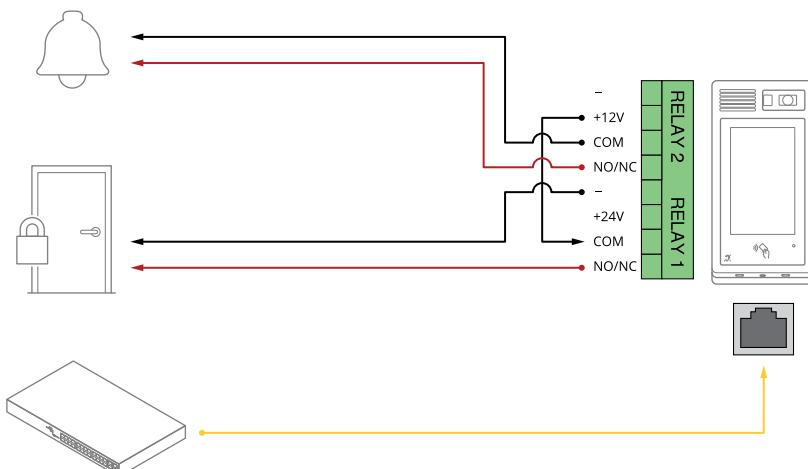
Um relé alimentado por PoE (12 V) + um relé alimentado por fonte de alimentação externa



1. Para verificar o estado do relé, vá para **System > Accessories** (Sistema > Acessórios) e encontre a porta do relé.
2. Defina **Normal state (Estado normal)** como:
 - para uma fechadura protegida contra falhas.
 - para uma fechadura protegida contra falhas.

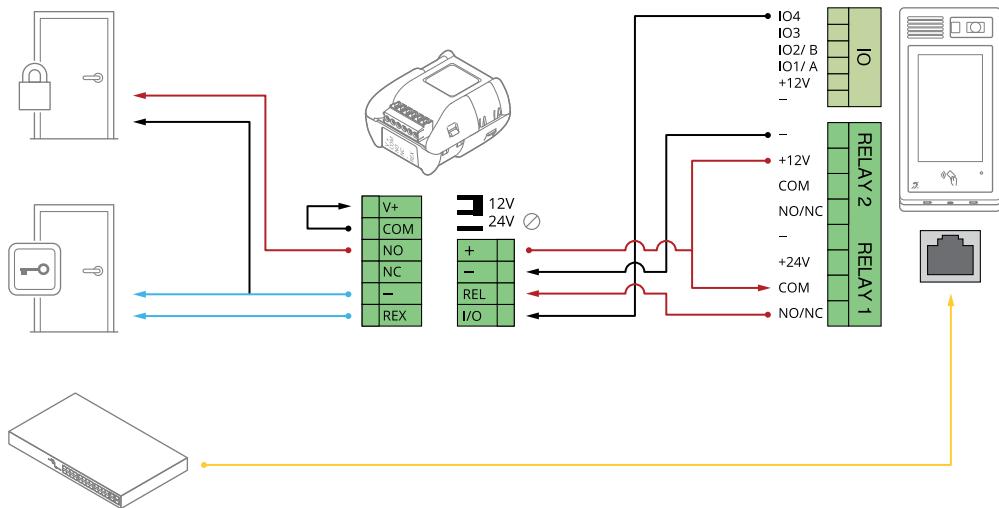
Um relé alimentado por PoE (12 V) + um relé de contato livre de potencial

O contato livre de potencial pode ser, por exemplo, uma campainha de porta.



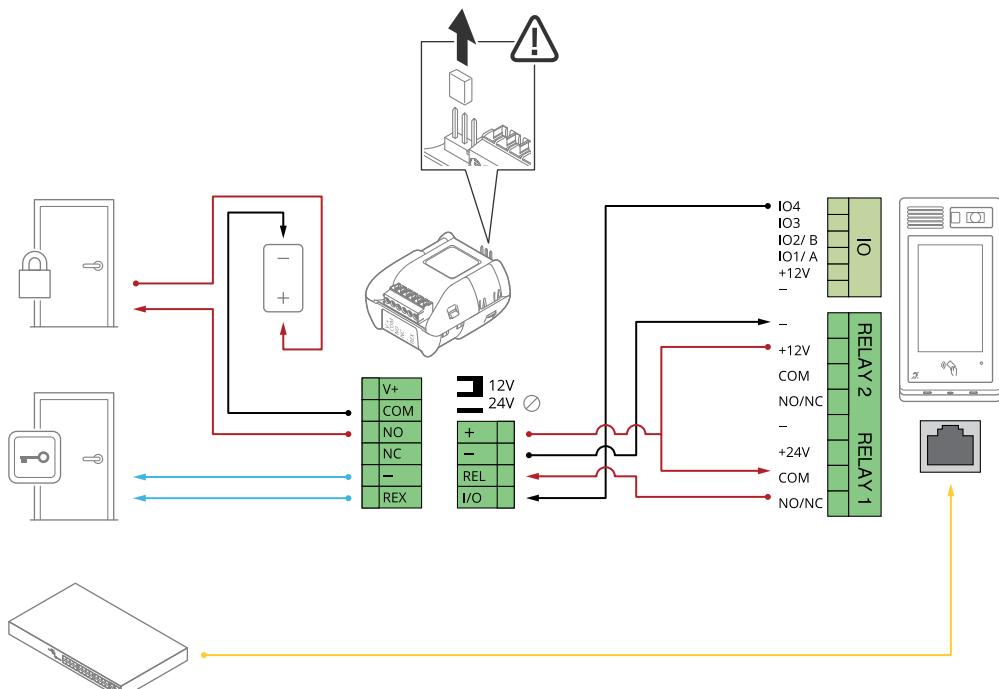
1. Para verificar o estado do relé, vá para **System > Accessories** (Sistema > Acessórios) e encontre a porta do relé.
2. Defina **Normal state (Estado normal)** como:
 - para uma fechadura protegida contra falhas.
 - para uma fechadura protegida contra falhas.

Fechadura de 12 V protegida contra falhas alimentada por PoE+ pelo intercomunicador



1. Para verificar o estado do relé, vá para **System > Accessories** (Sistema > Acessórios) e encontre a porta do relé.
2. Defina **Normal state (Estado normal)** como:
 -  para uma fechadura protegida contra falhas.
 -  para uma fechadura protegida contra falhas.

Fechadura protegida contra falhas alimentada por fonte externa

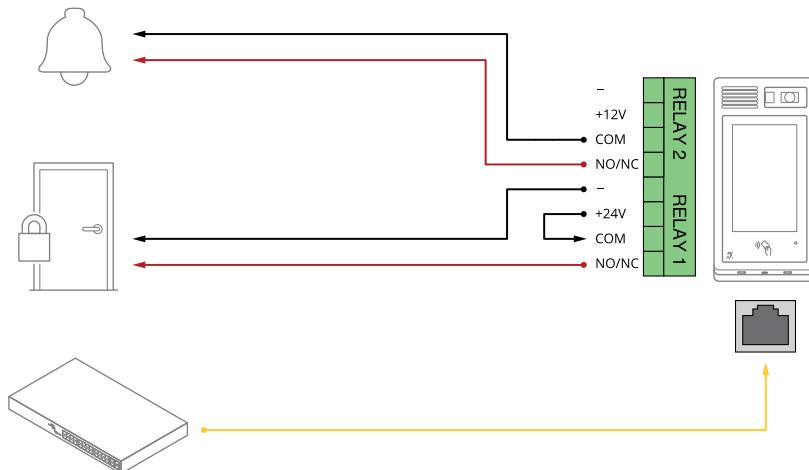


1. Para verificar o estado do relé, vá para **System > Accessories** (Sistema > Acessórios) e encontre a porta do relé.
2. Defina **Normal state (Estado normal)** como:
 -  para uma fechadura protegida contra falhas.

-  para uma fechadura protegida contra falhas.

Um relé alimentado por PoE (24 V) + um relé de contato livre de potencial

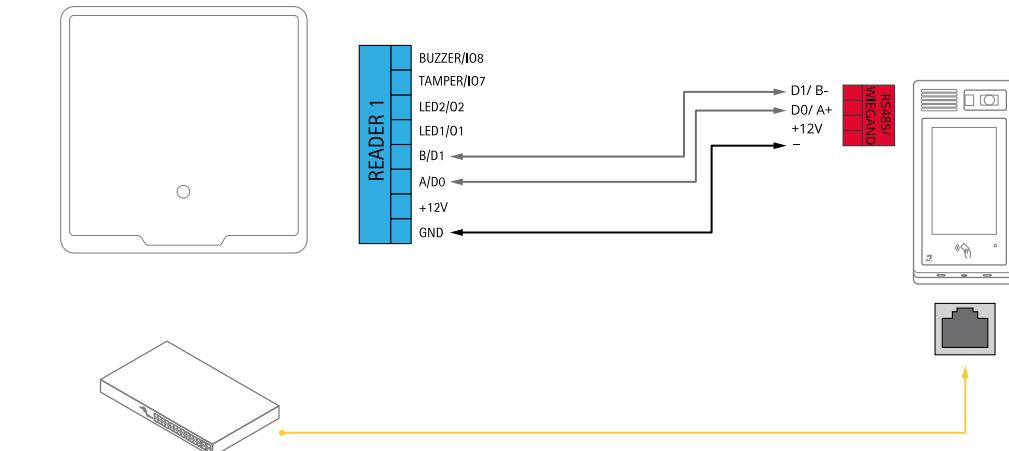
O contato livre de potencial pode ser, por exemplo, uma campainha de porta.



1. Para verificar o estado do relé, vá para **System > Accessories** (Sistema > Acessórios) e encontre a porta do relé.
2. Defina **Normal state** (Estado normal) como:

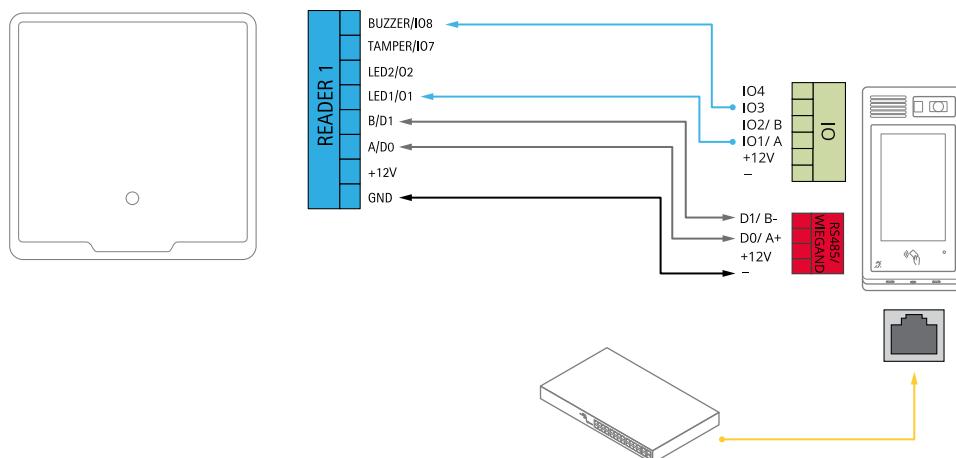
-  para uma fechadura protegida contra falhas.
-  para uma fechadura protegida contra falhas.

Leitor conectado ao controlador de porta usando OSDP



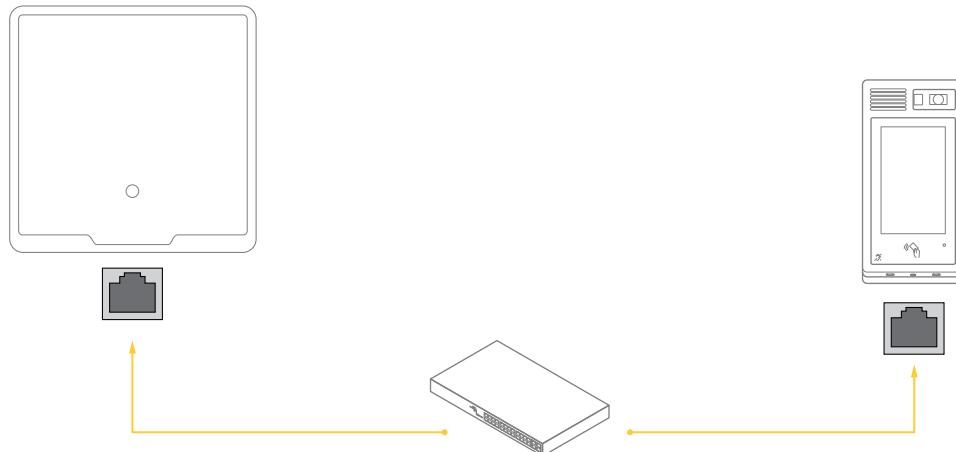
1. Vá para **Reader > Connection > Reader protocol** (Leitor > Conexão > Protocolo do leitor).
2. Defina **Reader protocol type** (Tipo de protocolo do leitor) como **OSDP** e clique em **Save** (Salvar).

Leitor conectado ao controlador de porta usando Wiegand



1. Vá para Reader > Connection > Reader protocol (Leitor > Conexão > Protocolo do leitor).
2. Defina Reader protocol type (Tipo de protocolo do leitor) como Wiegand.
3. Ative o Beeper (Bipe).
4. Em Input for beeper (Entrada para bipe), selecione I3.
5. Em Input used for LED control (Entrada usada para controle de LED), selecione 1.
6. Em Input for LED1 (Entrada para LED1), selecione I1.
7. Ajuste as outras configurações e clique em Save (Salvar).

Leitor conectado ao controlador de porta Axis usando leitor VAPIX



1. Vá para Reader > Connection > Reader protocol (Leitor > Conexão > Protocolo do leitor).
2. Defina Reader protocol type (Tipo de protocolo do leitor) como VAPIX reader (Leitor VAPIX).
3. Conecte a um controlador de porta Axis.

Solução de problemas

Redefinição para as configurações padrão de fábrica

Importante

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

Para redefinir o produto para as configurações padrão de fábrica:

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

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

Opções do AXIS OS

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

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

Verificar a versão atual do AXIS OS

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

Para verificar a versão atual do AXIS OS:

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

Atualizar o AXIS OS

Importante

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

Observação

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

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

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

Problemas técnicos, dicas e soluções

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

Problemas ao atualizar o AXIS OS

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

Problemas na configuração do endereço IP

O dispositivo está localizado em uma sub-rede diferente	Se o endereço IP destinado ao dispositivo e o endereço IP do computador usado para acessar o dispositivo estiverem localizados em sub-redes diferentes, você não poderá definir o endereço IP. Entre em contato com o administrador da rede para obter um endereço IP.
---	--

O endereço IP está sendo usado por outro dispositivo

Desconecte o dispositivo Axis da rede. Execute o comando ping (em uma janela de comando/DOS, digite ping e o endereço IP do dispositivo):

- Se você receber: Reply from <IP address>: bytes=32; time= 10 . . . , 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 você receber: Request timed out, significa que o endereço IP está disponível para uso com o dispositivo Axis. Verifique todo o cabeamento e reinstale o dispositivo.

Possível conflito de endereço IP com outro dispositivo na mesma sub-rede

O endereço IP estático no dispositivo Axis é usado antes que o DHCP defina um endereço dinâmico. Isso significa que, se o mesmo endereço IP estático padrão também for usado por outro dispositivo, poderá haver problemas para acessar o dispositivo.

O dispositivo não pode ser acessado por um navegador

Não é possível fazer login

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

Se a senha da conta root for perdida, o dispositivo deverá ser restaurado para as configurações padrão de fábrica. Consulte .

O endereço IP foi alterado pelo DHCP

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

Se necessário, um endereço IP estático poderá ser atribuído manualmente. Para obter instruções, vá para axis.com/support.

Erro de certificado ao usar IEEE 802.1X

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

O dispositivo está acessível local, mas não externamente

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

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

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

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

O firewall bloqueia o tráfego usando a porta 8883, pois é considerada insegura.

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

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

Considerações sobre desempenho

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

Entre em contato com o suporte

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

Informações sobre segurança

Níveis de perigo

▲ PERIGO

Indica uma situação perigosa que, se não evitada, irá resultar em morte ou lesões graves.

▲ AVISO

Indica uma situação perigosa que, se não evitada, poderá resultar em morte ou lesões graves.

▲ CUIDADO

Indica uma situação perigosa que, se não evitada, poderá resultar em lesões leves ou moderadas.

OBSERVAÇÃO

Indica uma situação perigosa que, se não evitada, poderá resultar em danos à propriedade.

Outros níveis de mensagens

Importante

Indica informações significativas que são essenciais para o produto funcionar corretamente.

Observação

Indica informações úteis que ajudam a obter o máximo do produto.

T10213214_pt

2025-11 (M6.2)

© 2025 Axis Communications AB