AXIS TP3604-E Cellular Back Box

Manual do Usuário

Índice

Instalação 3
Introdução 4
Encontre o dispositivo na rede 4
Suporte a navegadores 4
Abra a interface web do dispositivo 4
Crie uma conta de administrador 4
Senhas seguras 4
Certifique-se de que o software do dispositivo não foi manipulado 5
Configure seu dispositivo 6
Gerenciamento de SIM 6
Configurar APN 6
Verificar a intensidade do sinal e o endereço IP 6
Testar a conectividade 6
Verificar portas de gerenciamento 6
Ative o encaminhamento para a câmera 7
Configurar a propriedade do endereço IP da câmera 7
Modo local 8
Modo Passthrough 8
Configuração de regras de eventos 9
Acionar uma ação 9
Acionar uma notificação quando a caixa de proteção for aberta 9
A interface Web 11
Especificações 12
Visão geral do produto 12
Indicadores de LED 12
Botões 13
Botão de controle 13
Conectores 13
Conector de entrada PoE (PoE de entrada) 13
Conector de rede (PoE de saída) 13
Conector de energia 13
Limpeza do dispositivo 14
Solução de problemas 15
Restauração das configurações padrão de fábrica 15
Opções do AXIS OS 15
Verificar a versão atual do AXIS OS 15
Atualizar o AXIS OS 16
Problemas técnicos e possíveis soluções 16
Entre em contato com o suporte 18
Cibersegurança 19
Gerenciamento de vulnerabilidades 19
Notificações de segurança 19
Ciclo de vida seguro do produto 19

Instalação



O vídeo mostra como realizar a instalação da AXIS TP3604-E Cellular Back Box com a AXIS P32 Dome Camera Series e a AXIS P14 Bullet Camera Series.

Para obter instruções que abrangem todos os cenários de instalação, bem como informações de segurança, consulte o guia de instalação.

Introdução

Encontre o dispositivo na rede

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	*	*	*	*

✓: Recomendada

*: Compatível com limitações

Abra a interface web do dispositivo

1. Digite o nome de usuário e a senha. Se você acessar o dispositivo pela primeira vez, você deverá criar uma conta de administrador. Consulte *Crie uma conta de administrador, on page 4*.

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

Crie uma conta de administrador

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

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

Senhas seguras

Importante

Use HTTPS (que vem ativado por padrão) para definir sua senha ou outras configurações confidenciais pela rede. 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 manipulado

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. Configure e instale o dispositivo.

Configure seu dispositivo

Para realizar a configuração de seu dispositivo, é necessário percorrer as etapas a seguir:

1. *Gerenciamento de SIM, on page 6*
2. Se a sua rede exigir um Nome de Access Point (APN) explícito, *Configurar APN, on page 6*
3. *Verificar a intensidade do sinal e o endereço IP, on page 6*
4. *Testar a conectividade, on page 6*
5. *Verificar portas de gerenciamento, on page 6*
6. *Ative o encaminhamento para a câmera, on page 7*

Gerenciamento de SIM

O gerenciamento do cartão SIM é obrigatório quando o PIN do SIM está ativado. Se o PIN do SIM estiver desativado, você pode pular esta etapa.

1. Insira o cartão SIM. Vá para **Modem > SIM management > SIM status (Modem > Gerenciamento do SIM > Estado do SIM)** para verificar a detecção do modem e do SIM.
2. Se o PIN do SIM estiver bloqueado, vá para **Modem > SIM management > SIM PIN > Unlock (Modem > Gerenciamento do SIM > PIN do SIM > Desbloquear)** para desbloqueá-lo com o PIN correto.

Configurar APN

Observação

Você só precisa realizar esta etapa se a sua rede exigir um APN (Nome do Access Point) explícito.

Para realizar a configuração do APN explícito, vá para **Modem > Cellular network > APN (Modem > Rede celular > APN)**.

Verificar a intensidade do sinal e o endereço IP

Observação

Esta etapa requer acesso à rede de celular.

1. Verifique a intensidade do sinal em **System > Modem > Cellular network > Radio parameters > Signal strength index (Sistema > Modem > Rede celular > Parâmetros de rádio > Índice de intensidade do sinal)**. Três a quatro barras indicam uma boa qualidade de sinal.
2. Em **System > Modem > Cellular network > User equipment IP address (Sistema > Modem > Rede celular > Endereço IP do equipamento do usuário)**, verifique se um endereço IP da rede celular foi recebido.

Testar a conectividade

Observação

Esta etapa requer acesso à rede de celular.

1. Vá para **System > Modem > Cellular network > Test cellular connection (Sistema > Modem > Rede celular > Testar conexão celular)**. Insira um nome de host ou um endereço IP.
2. Verifique se o teste de conexão foi bem-sucedido.

Verificar portas de gerenciamento

Antes de ativar o modo de roteamento final, verifique as portas de gerenciamento da back box.

1. Vá para **Cellular routing > Back box management ports (Roteamento celular > Portas de gerenciamento da back box)**.

2. Altere as portas, caso os valores padrões não sejam compatíveis com a rede.

Ative o encaminhamento para a câmera

A etapa final é ativar o encaminhamento para a câmera.

1. Vá para **Cellular routing > Main mode (Roteamento celular > Modo principal)** e clique em **Enable forwarding to connected device (Ativar encaminhamento para o dispositivo conectado)**.

Assim que o encaminhamento for ativado, as portas de serviço normais serão encaminhadas para a câmera, e o gerenciamento da back box continuará disponível por meio das portas de gerenciamento reservadas.

2. Teste o acesso à câmera: em um navegador da web, insira o endereço IP do celular seguido do número da porta 80, `http://<cellular-ip-address>:80`.
3. Teste o acesso à caixa traseira: em um navegador da web, insira o endereço IP do celular seguido do número da porta 11080 (a porta padrão de gerenciamento da back box para HTTP), `http://<cellular-ip-address>:11080`.

Configurar a propriedade do endereço IP da câmera

Observação

Esta etapa é opcional e só é necessária caso você precise alterar o comportamento padrão da sub-rede ou ajustá-lo.

Uma rede celular atribui apenas um único endereço IP, e esse endereço está vinculado à identidade do cartão SIM. Uma instalação padrão envolve uma back box e uma câmera conectada a ela. O modo DHCP determina qual IP a câmera "receberá". Essa é a decisão fundamental por trás da escolha do modo de operação de um servidor DHCP.

Por padrão (modo local), o endereço IP do celular permanece na back box, e à câmera é atribuído um endereço IP privado da rede local da back box. A câmera permanece totalmente acessível pela rede de celular. Na maioria das implantações, isso é tudo o que é necessário e mantém a câmera isolada com segurança em uma rede privada.

A diferença fica evidente quando uma ferramenta analisa o endereço IP da perspectiva da própria câmera. Se um VMS ler o endereço IP informado pela câmera, ou se a câmera estiver configurada para exibir seu endereço IP em uma sobreposição de vídeo, esse IP será o endereço IP privado da câmera na LAN, e não o endereço IP público da rede celular que o mundo externo usa para acessá-la. Os dois endereços não coincidem, pois o IP do celular pertence à identidade do cartão SIM armazenada no dispositivo traseiro, e não à câmera.

O modo Passthrough resolve isso ao pegar o único endereço IP que a rede celular atribui ao roteador e encaminhá-lo para a câmera. Com Passthrough ativado, a câmera possui exatamente o mesmo endereço IP da rede celular; portanto, o endereço que a câmera informa (e exibe em uma sobreposição no vídeo) é o mesmo endereço usado para acessá-la remotamente. Como a câmera agora possui a identidade celular, essa escolha também altera a forma como a câmera pode se comunicar com outros equipamentos de usuário (UEs) na rede celular.

O restante desta seção descreve cada modo em detalhes.

É possível acessar a câmera conectada à back box por meio do IP de celular nas portas padrão (`80/443/554/22`) e também é possível acessar a back box pelas portas de gerenciamento reservadas (por exemplo,`11080/11443/11554/11022`).

A diferença entre os modos Local e Passthrough:

Modo local

- À câmera é atribuída uma sub-rede local privada.
- O endereço IP interno da câmera é diferente do endereço IP acessível pela rede celular.
- Se tiver dúvidas, use o modo DHCP local.

Modo Passthrough

- O endereço IP do celular é atribuído à câmera.

Modo local

Ativar modo Local

1. Em **Cellular routing > Advanced DHCP configuration > DHCP server mode (Roteamento celular > Configuração avançada de DHCP > Modo do servidor DHCP)**, selecione **Local**.
2. Verifique se o endereço IP local da câmera não está em conflito com nenhum outro endereço IP acessível na rede: **Cellular routing > Advanced DHCP configuration > Local private network configuration (Roteamento celular > Configuração avançada de DHCP > Configuração da rede privada local)**
3. Se necessário, altere o endereço IP em **Cellular routing > Advanced DHCP configuration > Local private network configuration (Roteamento celular > Configuração avançada de DHCP > Configuração da rede privada local)**. Use o mesmo valor para **Starting IP address (Endereço IP inicial)** e **Ending IP address (Endereço IP final)**.
4. Clique em **Save (Salvar)**.

Modo Passthrough

Se os UEs (Equipamentos do Usuário, ou seja, câmeras) não se comunicarem entre si e o tráfego sempre vier de outra LAN do VMS em direção aos UEs, não haverá caminho de UE para UE para o IP shadowing. Nesse caso, o Passthrough é considerado seguro do ponto de vista do IP shadowing.

Em termos gerais, isso significa que a rede celular é estendida em direção à câmera. Isso é útil quando a câmera deve aparecer diretamente no endereço IP voltado para o celular.

Risco importante: Mapeamento de IP no Passthrough

Esta descrição de risco se aplica a configurações com uma única câmera. Mesmo com apenas uma câmera, o Passthrough ainda precisa de dois endereços IP na sub-rede do lado da LAN:

- Um endereço IP para a câmera.
- Um IP para o servidor DHCP da back box no lado da Ethernet.

Cenário 1: sub-rede mínima por UE `(/30)`

Nesse modelo, cada UE possui uma pequena sub-rede independente.

- Um `(/30)` fornece dois endereços IP de host utilizáveis.
- A câmera utiliza um endereço IP.

O IP disponível é utilizado internamente pelo servidor DHCP da back box.

Recomendação para o cenário 1:

- Mantenha cada sub-rede de UE separada.
- Certifique-se de que todas as sub-redes UE sejam únicas. Não permita que as sub-redes se sobreponham entre os UEs.

Cenário 2: sub-rede maior compartilhada, com muitos UEs

Algumas implantações utilizam uma sub-rede maior, compartilhada por vários UEs. O risco de shadowing surge se a câmera tentar se conectar a outro UE que utilize o mesmo IP do servidor DHCP da back box. Nesse caso, o tráfego pode ser direcionado para o endereço local do back box, em vez de para o UE remoto pretendido.

Recomendação para o Cenário 2:

- Verifique o endereço IP do servidor DHCP do roteador nas configurações de passthrough.
- Certifique-se de que esse endereço IP não esteja atribuído a nenhum outro UE.
- Certifique-se de que esse endereço IP não esteja atribuído a nenhum SIM no portal de serviços da rede.

Ativar modo Passthrough

Observação

É necessário ter acesso a uma rede de celular.

1. Em **Cellular routing > Advanced DHCP configuration > DHCP server mode (Roteamento celular > Configuração avançada de DHCP > Modo do servidor DHCP)**, selecione **Passthrough**.
2. Em **Cellular routing > Advanced DHCP configuration > Local private network configuration > Server IP and prefix length (Roteamento celular > Configuração avançada de DHCP > Configuração da rede privada local > IP do servidor e comprimento do prefixo)**, verifique se o IP do servidor e o comprimento do prefixo de sub-rede selecionados automaticamente não estão em conflito com outros endereços IP acessíveis.
3. Clique em **Save (Salvar)**.

Configuração de regras de eventos

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

Acionar uma ação

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

Acionar uma notificação quando a caixa de proteção for aberta

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

Adicionar um destinatário de email:

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

Crie uma regra:

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

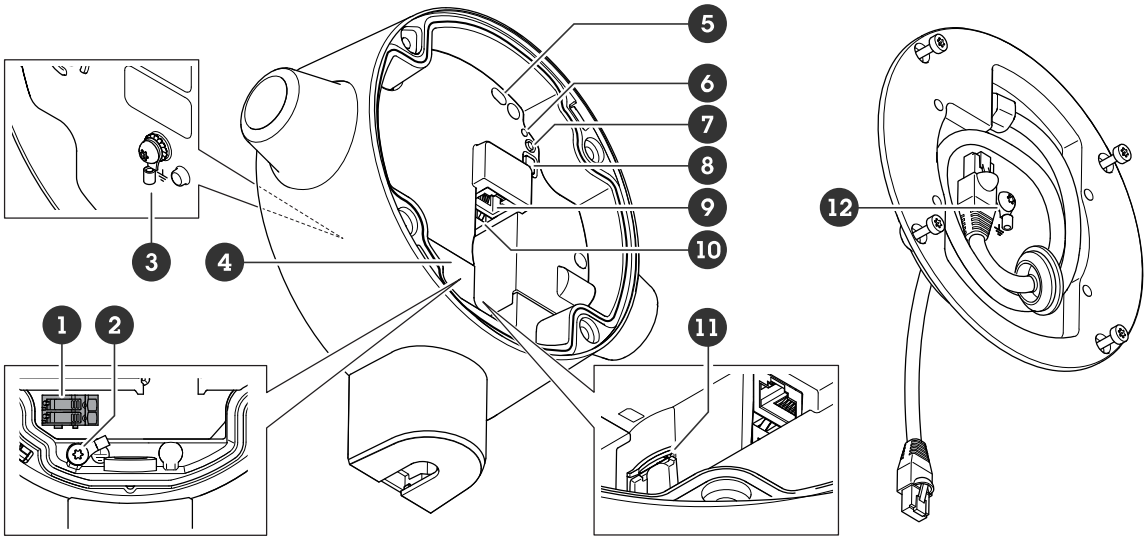
15. Clique em **Save (Salvar)**.

A interface Web

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

Especificações

Visão geral do produto



1 *Conector CA*
2 *Aterramento de proteção*
3 *Parafuso de aterramento*
4 *Capa protetora (CA)*
5 *Detector de abertura da caixa*
6 *Botão Reiniciar*
7 *LED de estado*
8 *Botão de controle*
9 *PoE de saída (dados)*
10 *Entrada PoE*
11 *Slot para cartão SIM*
12 *Parafuso do terra (câmera)*

Indicadores de LED

LED de status no modo de configuração

LED de estado	Indicação
Apagado	O sensor de IR de detecção de caixa de proteção é coberto.
Verde	Operação normal: a interface Ethernet está pronta.
Âmbar	Aceso durante a inicialização. Pisca durante uma atualização do software do dispositivo ou redefinição para o padrão de fábrica.
Âmbar/ /Vermelho	Não há conexão de Ethernet e o modem é configurado durante a inicialização.
Vermelho	Falha na atualização do software de dispositivo.

LED de status no modo conectado

LED de estado	Indicação
Apagado	O sensor de IR de detecção de caixa de proteção é coberto.
Verde	O modem não está conectado à rede.

Âmbar	Aceso durante a inicialização. Pisca durante uma atualização do software do dispositivo ou redefinição para o padrão de fábrica.
Âmbar/ /Vermelho	O modem é configurado durante a inicialização.
Vermelho	Falha na atualização do software de dispositivo.

Botões

Botão de controle

O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte *Restauração das configurações padrão de fábrica, on page 15*.
- Conexão a um serviço de conexão em nuvem com um clique (O3C) via Internet. Para conectar, pressione e solte o botão e aguarde até que o LED de status pisque em verde três vezes.

Conectores

Conector de entrada PoE (PoE de entrada)

Conector de Ethernet RJ45 com Power over Ethernet (PoE) IEEE 802.3af/802.3at/802.3bt Tipo 3 Classe 5.

Observação

Este conector é usado apenas para entrada de energia; não há conexão da rede disponível.

Observação

- É necessária uma entrada CA para a saída PoE IEEE 802.3at tipo 2 Classe 4.
- Para uma saída PoE IEEE 802.3af Tipo 1 Classe 3, é necessário o padrão IEEE 802.3at Tipo 2 Classe 4 ou superior.
- Para entrada PoE IEEE 802.3af Tipo 1 Classe 3, o dispositivo está operacional, mas não tem saída de energia.

Observação

O comprimento máximo do cabo Ethernet é de 20 m.

Conector de rede (PoE de saída)

Conector Ethernet RJ45.

Observação

- É necessária uma entrada CA para a saída PoE IEEE 802.3at tipo 2 Classe 4.
- Para uma saída PoE IEEE 802.3af Tipo 1 Classe 3, é necessário o padrão IEEE 802.3at Tipo 2 Classe 4 ou superior.
- Para entrada PoE IEEE 802.3af Tipo 1 Classe 3, o dispositivo está operacional, mas não tem saída de energia.

Observação

O comprimento máximo do cabo Ethernet é de 20 m.

Conector de energia

Bloco de terminais para conexão de energia CA.

Observação

É necessária uma entrada CA para a saída PoE IEEE 802.3at tipo 2 Classe 4.

Limpeza do dispositivo

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

OBSERVAÇÃO

- Produtos químicos abrasivos podem danificar o dispositivo. Não use produtos químicos como limpa-vidros ou acetona para limpar o dispositivo.
- Evite limpar o dispositivo sob luz solar direta ou em temperaturas elevadas, visto que isso pode causar manchas.

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

Para obter mais informações sobre a limpeza de dispositivos Axis, consulte o white paper *Resistência química a agentes de limpeza comuns*.

Solução de problemas

Restauração das configurações padrão de fábrica

Importante

A restauração para as 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 *Visão geral do produto, on page 12*.
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 será padrão para um dos seguintes:
   - **Dispositivos com AXIS OS 12.0 e versões posteriores:** Obtidos da sub-rede de endereço local do link (169.254.0.0/16)
   - **Dispositivos com AXIS SO 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 recomendados se você usa integrações de outros fabricantes, as quais podem não ser continuamente validadas com a trilha ativa mais recente. Com o LTS, os produtos podem manter a segurança cibernética sem apresentar quaisquer alterações funcionais significativas nem afetar quaisquer integrações existentes. Para obter informações mais detalhadas sobre a estratégia de software de dispositivos Axis, acesse *axis.com/support/device-software*.

Verificar a versão atual do AXIS OS

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

Para verificar a versão atual do AXIS OS:

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

Atualizar o AXIS OS

Importante

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

Observação

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

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

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

Problemas técnicos e possíveis soluções

Problemas ao atualizar o AXIS OS

A atualização do AXIS OS falhou

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

Problemas após a atualização do AXIS OS

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

Problemas na configuração do endereço IP

Não é possível definir o endereço IP

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

Problemas com o acesso ao dispositivo

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

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

Caso tenha perdido a senha da conta root, será necessário redefinir o dispositivo para as configurações padrão de fábrica. Para obter instruções, consulte *Restauração das configurações padrão de fábrica, on page 15*.

O endereço IP foi alterado pelo DHCP

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

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

Erro de certificado ao usar IEEE 802.1X

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

O navegador não é compatível

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

Não é possível acessar o dispositivo externamente

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

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

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

Problemas com MQTT

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

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

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

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

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

Entre em contato com o suporte

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

Cibersegurança

A segurança cibernética oferece suporte a um ciclo de vida de produto bem-sucedido com riscos minimizados. Você pode encontrar informações detalhadas e documentação sobre nossa abordagem à segurança cibernética em *axis.com/about-axis/cybersecurity*. Siga as diretrizes de segurança cibernética abaixo para receber notificações de segurança da Axis sobre o produto e para realizar a configuração do produto, de modo a garantir um ciclo de vida e um descomissionamento seguros.

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

Gerenciamento de vulnerabilidades

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

Notificações de segurança

Inscreva-se para receber emails de notificação de segurança da Axis em *axis.com/security-notification-service*. Enviaremos a você informações sobre vulnerabilidades, alertas de segurança correspondentes e outros assuntos relacionados à segurança do seu produto Axis.

Ciclo de vida seguro do produto

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

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

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

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

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

T10233346_pt

2026-10 (M2.2)

© 2026 Axis Communications AB