# AXIS Device Manager

## Manual do Usuário

## Índice

## Sobre o AXIS Device Manager

O AXIS Device Manager é um aplicativo de software para instalação e gerenciamento de produtos Axis. O software pode buscar dispositivos automaticamente na rede, atribuir endereços IP, configurar senhas, exibir status da conexão, gerenciar atualizações de firmware, certificados e configurar diversos dispositivos.

O AXIS Device Manager é composto por:

- AXIS Device Manager Service Control - o servidor que gerencia toda a comunicação com os produtos Axis
- AXIS Device Manager Client - a interface do usuário front-end que ativa o gerenciamento remoto pela Internet ou pela rede corporativa

Vários clientes podem estar conectados ao mesmo servidor. Um cliente pode estar conectado a vários servidores ao mesmo tempo.

O AXIS Device Manager também é muito útil para fortalecer seu sistema e aumentar a segurança. Para obter mais informações, consulte o *Guia de Segurança do AXIS Device Manager.*

# Visão geral da solução

## Pré-requisitos

**Sistemas operacionais compatíveis:**

Necessário: Sistema operacional de 64 bits Microsoft .NET versão 4.8

Sistema operacional compatível: Windows 10 Pro, Windows 11 Pro, Windows Server 2016, Windows Server 2019, Windows Server 2022

Recomendações: Service Packs mais recentes do sistema operacional.

**Recomendação de sistema mínima:**

- Mínimo (até 500 dispositivos): Intel core i5 ou equivalente, 4 GB de RAM, 100 Mbps em toda a infraestrutura de rede
- Recomendado (entre 500 a 2000 dispositivos): Intel core i7 ou equivalente, 8 GB de RAM, 1000 Mbps em toda a infraestrutura de rede
- Não é recomendável ter mais de 2000 dispositivos por servidor.
- Certifique-se de que os dispositivos Axis executem o sistema operacional AXIS mais recente disponível.

Observação

Sempre oferecemos suporte às duas versões anteriores da versão mais recente. Verifique as notas de versão mais recentes para saber quais versões específicas são compatíveis.

**Dispositivos com suporte:**

Produtos AXIS com versões do sistema operacional AXIS 4.40 ou superior. (Observe que a funcionalidade exata suportada varia de acordo com um modelo de produto e firmware específicos)

**Idiomas:**

Interface do usuário + arquivos de ajuda: Inglês, francês, alemão, italiano

Somente a interface do usuário: Árabe, tcheco, chinês (simplificado), chinês (tradicional), holandês, finlandês, japonês, coreano, persa, polonês, português (Brasil), russo, espanhol, sueco, tailandês, turco e vietnamita.

# Início

## Instalação do software

Para instalar o AXIS Device Manager 5, verifique se você tem direitos totais de administrador no computador em que está instalando e faça o seguinte:

1. *Vá para a página do produto em axis.com e baixe o aplicativo de desktop AXIS Device Manager*
2. Execute o instalador e siga as instruções na tela.

Observação

Se ainda não estiver instalado, o Microsoft .NET 4.8 framework será instalado (incluído no arquivo de instalação). Isso demorará alguns minutos. O Microsoft .NET 4.8 framework também pode ser instalado via Windows Update antes da instalação do AXIS Device Manager.

## Conectar a um servidor

Ao iniciar o AXIS Device Manager pela primeira vez, será solicitado que você se conecte a um servidor. O servidor pode ser executado no computador local ou em um servidor remoto.

**Para fazer login como um usuário local do Windows:**

1. Selecione **This computer** (Este computador).
2. Marque **Log on as current user** (Fazer login como usuário atual) para fazer login usando suas credenciais atuais.

Para fazer login como outro usuário no servidor ou no domínio:

- Selecione **Other user** (Outro usuário).
- Em **Other user** (Outro usuário), insira as credenciais dessa conta.
- Marque **Remember me** (Lembrar-me) para ignorar essa etapa na próxima vez que você executar o cliente.
- Clique em **Log on** (Fazer login).

Observação

Para limpar as credenciais salvas de todos os servidores, vá para a tela de login e selecione **Delete saved passwords** (Excluir senhas salvas).

**Para fazer login em um servidor remoto:**

1. Selecione **Remote server (Servidor remoto)**.
2. Selecione um servidor na lista suspensa ou insira o endereço IP ou DNS no campo.
3. Insira suas credenciais
4. Clique em **Log on** (Fazer login).

Observação

Essa opção não pode ser usada para fazer login em um servidor remoto a partir de um computador que não faça parte de um domínio do Windows.

## Conexão a múltiplos servidores

Você pode se conectar a vários servidores com o AXIS Device Manager. Depois de fazer login com sucesso em um servidor, você poderá alternar entre os servidores no menu principal.

1. Vá para o menu principal > Servidores > Nova conexão
2. Escolha conectar-se ao seu computador ou a um servidor remoto, conforme descrito acima.

## Configuração inicial

Para começar, você precisa fazer o seguinte:

- Adicione dispositivos e crie contas de usuário, consulte:
- Forneça reforço de segurança cibernética ao seu sistema. Consulte

# Gerenciar dispositivos

## Adicionar dispositivos

O AXIS Device Manager procura automaticamente os dispositivos conectados na rede e tenta fazer login em todos eles. A lista de dispositivos encontrados mostra o endereço IP ou o nome do host, o número de série, o modelo e o status do dispositivo. O número de série (N/S) está impresso na etiqueta do produto.

Para adicionar dispositivos da lista:

1. Selecione os dispositivos para adicionar e clique em **Next** (Avançar).
2. Selecione **Use host name when possible** (Utilize o nome do host quando possível). Se um dispositivo é adicionado com seu nome de host, este será usado para todas as comunicações restantes com o dispositivo. Se um nome de host não está disponível, o endereço IP será usado.
3. Configure a senha para dispositivos sem senha. Se não for necessário configurar uma senha, selecione **Skip** (Pular).
4. Clique em **Next** (Próximo).

A página "Ready to add devices" (Pronto para adicionar dispositivos) mostra os dispositivos a serem adicionados.

5. Clique em **Finish** (Concluir) para adicionar os dispositivos.

## Remover dispositivos

Para remover dispositivos da lista:

1. Vá para **Gerenciamento de dispositivos**.
2. Selecione os dispositivos.
3. Clique com o botão direito do mouse e selecione **Remove** (Remover).
4. Clique em **Sim**.

## Substituir dispositivos

Para substituir um dispositivo no AXIS Device Manager, conecte um novo dispositivo e reutilize a configuração do dispositivo existente. O dispositivo substituído será excluído se a operação for bem-sucedida. Deve haver pelo menos um ponto de restauração disponível para esse dispositivo, consulte . Nenhum ponto de restauração será movido para o novo dispositivo.

1. Vá para **Gerenciamento de dispositivos**.
2. Vá para a barra de ferramentas e clique no ícone de substituição de dispositivo.
3. Selecione um dispositivo para substituir e clique em **OK**.
4. Selecione o dispositivo que deseja substituir e clique em **OK**.
5. Clique em **Next** (Avançar) para recuperar uma configuração de dispositivo do ponto de restauração mais recente.
6. Vá para **Parameters > Additional Settings** (Parâmetros > Configurações adicionais) e selecione os parâmetros e as configurações a serem aplicados.
7. Clique em **Next** (Próximo).
8. Clique em **Finish** (Concluir) para aplicar suas configurações.

## Recuperar dispositivos

É possível restaurar um ou vários dispositivos para pontos de restauração criados anteriormente. Para restaurar dispositivos, cada um deve ter pelo menos um ponto de restauração disponível. Por padrão, os pontos de restauração automática são criados e removidos continuamente todas as noites para todos os dispositivos no

servidor selecionado. Um número configurado dos últimos pontos de restauração automática é mantido para fins de restauração.

Restaurar dispositivos em um ponto de restauração anterior:

1. Acesse a área de trabalho **Device management** (Gerenciamento de dispositivos).
2. Selecione um ou vários dispositivos para restaurar.
3. Clique com o botão direito do mouse e selecione **Backup / Restore > Restore to a Previous Time** (Backup/Restauração > Restaurar para um momento anterior) no menu suspenso.
4. Selecione um ponto de restauração na lista dos pontos de restauração mais recentes disponíveis e clique em **Next** (Avançar).
5. Revise as configurações de cada dispositivo e clique em **Finish** (Concluir).

# Configuração

## Criar ponto de restauração

Para criar um ponto de restauração manual:

- Acesse a área de trabalho **Device management** (Gerenciamento de dispositivos).
- Selecione um ou vários dispositivos para restaurar.
- Clique com o botão direito do mouse e selecione **Backup / Restore > Create Restore Points** (Backup/ /Restauração > Criar pontos de restauração).
- Digite uma descrição que identifique o ponto de restauração.
- Clique em **OK**.

Observação

Os pontos de restauração criados manualmente não são removidos automaticamente.

### Criar pontos de restauração automática

Se você tiver mais de um servidor, selecione aquele a ser configurado na lista de servidores.

- Vá para **Options > Restore point settings** (Opções > Restaurar configurações de ponto).
- Selecione **Create restore points automatically** (Criar pontos de restauração automaticamente) para ativar a criação automática de pontos de restauração.
- Insira o número de pontos de restauração automática a serem salvos e clique em **OK**.

## Gerenciar várias credenciais

Essa funcionalidade fornece ao AXIS Device Manager credenciais para uma conta de administrador dos dispositivos.

**Digite as credenciais do dispositivo manualmente**

Se escolher inserir as credenciais do dispositivo manualmente, elas serão atualizadas no AXIS Device Manager para os dispositivos selecionados.

- Selecione um ou mais dispositivos
- Clique com o botão direito do mouse e selecione **Advanced -> Enter Device Credentials** (Avançado > Inserir credenciais do dispositivo) no menu suspenso.

Observação

As credenciais que não puderem ser verificadas como funcionando no dispositivo não serão atualizadas. A mesma senha e o mesmo nome de usuário devem ser usados em todos os dispositivos que participam dessa operação.

**Use um arquivo CSV para diferentes credenciais**

Ao usar um arquivo CSV, é possível usar senhas e nomes de usuário separados para cada dispositivo. O endereço MAC, o endereço IP ou o endereço do host é usado para mapear as linhas do arquivo CSV para os dispositivos correspondentes no banco de dados do Axis Device Manager.

Ao usar um arquivo CSV, a interface do usuário solicita que o usuário especifique como interpretar as colunas do arquivo CSV.

Observação

Como especificar a qual dispositivo pertence uma linha no arquivo CSV.

Uma coluna no arquivo CSV precisa conter endereços MAC, endereços IP ou endereços de host, portanto, especifique uma coluna no arquivo CSV para ser interpretada como endereço MAC ou como endereço IP ou endereço de host. Isso é necessário para especificar a qual dispositivo pertencem os dados em uma linha do arquivo CSV. Além disso, uma coluna pode ser especificada para ser interpretada como o nome do servidor. Dessa forma, é possível distinguir as linhas do arquivo CSV que têm como alvo dispositivos em diferentes

servidores do Axis Device Manager, mas com o mesmo endereço IP ou endereço de host. Se essa distinção não for necessária, não há utilidade em ter uma coluna para ser interpretada como nome do servidor. Em uma configuração em que um servidor usa o mesmo endereço IP ou endereço de host para vários dispositivos, mas usa portas para diferenciá-los uns dos outros, uma coluna pode ser especificada para ser interpretada como Porta. Se nenhuma distinção de porta for necessária, geralmente não há motivo para interpretar uma coluna como Porta. Uma opção para fornecer a porta em uma coluna dedicada é fornecer a porta junto com o endereço IP ou o endereço do host. O endereço IP ou o endereço do host deve ser seguido por dois pontos e o número da porta.

## Instale certificados

### Sobre certificados

O AXIS Device Manager fornece as configurações para o gerenciamento de certificados de servidor/cliente. Os certificados de cliente são usados para IEEE 802.1X e os certificados de servidor são usados para HTTPS. Para implementar quaisquer alterações, selecione os dispositivos apropriados no Gerenciamento de dispositivos e, em seguida, selecione Enable/update (Ativar/atualizar) no menu de contexto.

### Criar uma autoridade de certificação (CA)

Uma autoridade de certificação permitirá a você ativar HTTPS e IEEE 802.1 X em dispositivos sem qualquer certificados servidor/cliente em vigor. A CA instrui os dispositivos a criar certificados usando suas próprias chaves privadas, entrar com eles e instalá-las

Para criar uma autoridade de certificação:

- Vá para a guia **Configuration** (Configuração).
- Vá para **Security > Certificates** (Segurança > Certificados)
- Em **Certificate authority** (Autoridade de certificação), clique em **Generate...** (Gerar).
- Digite uma frase secreta e a confirme.
- Clique em **OK**.

A CA agora será gerada e estará pronta para uso.

Observação

Seu certificado autoassinado root e sua chave privada, protegidos por uma frase secreta de sua escolha. Um certificado gerado pelo AXIS Device Manager durará 3 anos. Se quiser que o AXIS Device Manager renova os certificados de servidor/cliente de forma automática, você deverá marcar a caixa intitulada **Remember passphrase** (Lembrar frase secreta). Se uma CA não estiver configurada, será necessário criar certificados de servidor/cliente fora do AXIS Device Manager. Assim, você perderá as vantagens do gerenciamento automático de certificados.

**Import** (Importar) - Usando o recurso Import, você pode importar uma CA existente que consiste em um certificado público e uma chave privada. Você terá que fornecer uma senha.

**Save to file** (Salvar em arquivo) - Salve o certificado público da CA nos formatos .cer ou .crt. O arquivo não conterá a chave privada e, portanto, não será criptografado.

**Backup** - Recomenda-se fazer um backup de uma CA caso ocorra uma falha de hardware. Se selecionado, será feito um backup do certificado CA e da chave privada da CA usada pelo Axis Device Manager. Os dados do backup serão protegidos pela frase secreta usada para gerar a CA.

Aviso de expiração de certificado Uma notificação do sistema será criada se um certificado estiver expirado ou prestes a expirar. Isso se aplica a todos os certificados instalados em dispositivos conectados, exceto CAs instaladas fora do AXIS Device Manager. O aviso aparecerá como um alarme do sistema, na coluna de status no gerenciamento de dispositivos, como ícones na caixa de diálogo "View installed certificates" (Exibir certificados instalados) e no espaço de trabalho de configuração.

Especifique o quanto cedo deseja que o AXIS Device Manager notifique você quando os certificados estiverem se aproximando da data de validade. Por padrão, os certificados de servidor e cliente gerados pelo AXIS Device Manager serão renovados automaticamente sete dias antes do aviso de expiração ser configurado para aparecer.

Para receber notificações quando a CA estiver configurada para expirar, é necessário marcar a opção "remember passphrase" (lembrar senha).

## Ativar o HTTPS.

Para ativar o HTTPS, um certificado de servidor deve estar presente em cada dispositivo. O AXIS Device Manager pode usar uma Autoridade de Certificação (CA) para se conectar e instalar certificados de servidor para dispositivos.

Você também pode fazer isso manualmente:

1. Vá para a guia **Device manager** (Gerenciamento de dispositivos)
2. Clique com o botão direito do mouse nos dispositivos e escolha **Install server certificates** (Instalar certificados de servidor) para cada dispositivo no menu de contexto.

Só pode haver um certificado de servidor presente em cada dispositivo antes de ativar o HTTPS. Os certificados em excesso podem ser excluídos do menu de contexto.

3. Depois de instalar os certificados, você pode ativar o HTTPS no menu de contexto.

Observação

Uma conexão pode ser feita usando HTTP se uma conexão segura (HTTPS) não estiver disponível. Isso é feito para que seja possível configurar dispositivos que ainda não são seguros.

**Ignorar validação do certificado**

O AXIS Device Manager não se conectará a um dispositivo se seu certificado não for validado. O certificado do servidor deve ser assinado pela CA ativa no AXIS Device Manager ou validado por meio do Repositório de Certificados do Windows. Ao selecionar Ignore certificate validation (Ignorar validação de certificado), o AXIS Device Manager não validará se o certificado enviado pelo dispositivo é confiável ou não.

Para fazer com que o AXIS Device Manager ignore a validação de certificado.

- Vá para a guia **Configuration** (Configuração).
- Em **HTTPS**, ative **Ignore certificate validation** (Ignorar validação de certificado).

## Ativar 802.1X

Para ativar o IEEE 802.1X, um certificado de cliente deve estar presente em cada dispositivo. O AXIS Device Manager pode usar uma Autoridade de Certificação (CA) para se conectar e instalar certificados de cliente para dispositivos.

Você também pode fazer isso manualmente no gerenciamento de dispositivos se clicar com o botão direito do mouse nos dispositivos e escolher instalar certificados de cliente para cada dispositivo no menu de contexto. Só pode haver um certificado de cliente presente em cada dispositivo antes de ativar o IEEE 802.1X. Os certificados em excesso podem ser excluídos do menu de contexto. Depois de instalar os certificados, você pode ativar o IEEE 802.1X no menu de contexto.

Você também precisa de um certificado CA de autenticação IEEE 802.1X para usar o protocolo IEEE 802.1X.

EAPOL Version (Versão EAPOL) - Selecione a versão do Extensible Authentication Protocol (EAP) que deseja usar.

EAP Identity (Identidade EAP) - Insira o endereço MAC e o nome do host do dispositivo ou um texto personalizado.

Custom (Personalizado) - Insira qualquer texto que funcionará como a identidade EAP.

IEEE 802.1X authentication CA certificate (Certificado CA de autenticação IEEE 802.1X) - Além do certificado de cliente, um certificado CA de autenticação IEEE 802.1 deve ser instalado. Para ativar o IEEE 802.1X, é necessário apenas o certificado público e não a chave privada, portanto, não há necessidade de nenhuma frase secreta. O certificado CA de autenticação IEEE 802.1 X será instalado para permitir ou atualizar o IEEE 802.1 X..

**Import** (Importar) - Selecione um certificado CA que será instalado nos dispositivos e usado para validar o servidor de autenticação. O certificado CA pode ser criado pela CA no AXIS Device Manager ou vir de uma fonte externa.

**View** (Exibição) - Detalhes do certificado CA usado durante o processo de autenticação IEEE 802.1X.

**Common name (Nome comum)** - Selecione a identidade EAP do dispositivo ou o endereço IP do dispositivo. Se o campo personalizado for deixado em branco, o nome do host será selecionado. Se houver um problema com o nome do host, o endereço IP será usado como o nome comum.

## Gerencie contas SIP

# Gerenciar software do dispositivo

## Atualizações do AXIS OS

As novas versões do sistema operacional AXIS podem ser obtidas de duas maneiras:

- Baixar usando o AXIS Device Manager (requer acesso à internet)
- Importar de um arquivo (por exemplo, em um disco rígido ou cartão de memória).

Observação

Recomendamos que você siga o caminho de atualização do AXIS OS recomendado. Leia mais sobre isso aqui: *https://help.axis.com/axis-os#upgrade-path*

**Atualização manual do sistema operacional AXIS**

1. Selecione os dispositivos que deseja atualizar com uma nova versão do AXIS OS, clique com o botão direito do mouse e selecione **Upgrade firmware (Atualizar firmware)**.
2. Após ser informado de que os dispositivos ficarão inacessíveis durante a atualização, clique em **Yes (Sim)**.
3. Para atualizar a lista de versões de firmware disponíveis para download, na caixa de diálogo **Upgrade firmware (Atualizar firmware)**, clique em **Check for Updates (Verificar se há atualizações)**.
4. Para procurar um ou mais arquivos de versão do sistema operacional AXIS armazenados no cliente local, clique no botão **Browse** (Procurar).
5. Selecione os dispositivos e as versões do AXIS OS que você deseja atualizar.
6. Para definir o padrão de fábrica dos dispositivos selecionados durante a atualização do sistema operacional AXIS, clique na caixa de seleção **Factory default** (Padrão de fábrica). Esse é um requisito para o downgrade de algumas versões do sistema operacional AXIS.
7. Clique em **OK** para iniciar a atualização dos dispositivos selecionados na lista.

Observação

Por padrão, as atualizações do AXIS OS são implementadas em todos os dispositivos selecionados ao mesmo tempo. A ordem de atualização pode ser alterada em **Configuration > Connected Services > Firmware upgrade settings (Configuração > Serviços conectados > Configurações de atualização de firmware)**.

**Atualizações automáticas**

A configuração padrão do AXIS Device Manager 5 é não verificar se há atualizações de firmware, mas ele pode ser configurado para verificar automaticamente se há atualizações do AXIS OS disponíveis no servidor ou no site axis.com.

Para verificar manualmente se há atualizações do AXIS OS, pressione o botão **Check now (Verificar agora)** no menu de ação.

**Ordem de atualização do sistema operacional AXIS**

As atualizações do AXIS OS podem ser implementadas em todos os dispositivos ao mesmo tempo ou em um dispositivo após o outro.

- Para atualizar todos os dispositivos de uma só vez, selecione a ordem de atualização **Parallel (Paralelo)**
- Para atualizar os dispositivos um após o outro, selecione **Sequential** (Sequencial). Essa opção demora mais, mas os dispositivos não permanecerão off-line ao mesmo tempo. Também é possível parar uma atualização sequencial se um problema for encontrado ao marcar a caixa **Cancel all remaining upgrades if one device fails** (Cancelar atualizações restantes se um dispositivo falhar).

# Solução de problemas

## Entre em contato com o suporte

Ao entrar em contato com o suporte, primeiro crie um tíquete e inclua um arquivo de relatório do sistema para facilitar a solução de problemas específicos:

1. Vá para o menu principal.
2. Vá para **Help > System Report...** (Ajuda > Relatório do sistema...)
3. Salve o arquivo de relatório em uma pasta escolhida.
4. Vá para *axis.com/support*.
5. Crie um tíquete de suporte.
6. Anexe o arquivo ao seu ticket de suporte.

Observação

Para criar um relatório do sistema a partir de um sistema que não responde:

1. Vá para `C:\ProgramData\Axis Communications\`
2. Arquive o conteúdo da pasta em um arquivo .zip e anexe-o ao tíquete de suporte.

## Processo de encaminhamento

Caso enfrente problemas que não podem ser resolvidos com a ajuda deste guia, encaminhe-os para o Suporte técnico online da Axis. Consulte *Suporte técnico online da Axis*. Para que nossa equipe de suporte entenda seu problema e consiga solucioná-lo, é necessário incluir as seguintes informações:

- Uma descrição clara sobre como reproduzir o problema ou em que circunstâncias ele ocorre.
- A hora e o nome ou endereço IP do dispositivo em questão em que o problema ocorre.
- AXIS Device Manager gerado diretamente após o problema ocorrer. O relatório do sistema deve ser gerado no cliente ou servidor em que o problema foi reproduzido.
- Capturas de tela ou gravações opcionais que mostrem o problema.
- Se necessário, inclui os arquivos do banco de dados. Exclua-os para fazer o upload ir mais rápido.

Alguns problemas exigem informações adicionais solicitadas pela equipe de suporte, se necessário.

Observação

Se o arquivo tiver mais de 100 MB, por exemplo, um rastreamento de rede ou arquivo de banco de dados, use um serviço de compartilhamento de arquivos seguro e confiável.

| Informações adicionais | |
|---|---|
| **Logs de nível de depuração** | Às vezes, precisamos usar o log em nível de depuração para coletar mais informações. Isso só é feito por solicitação de um engenheiro de suporte da Axis. Você pode encontrar instruções no *suporte técnico online da Axis*. |
| **Rastreamento de rede** | Se solicitado pelo engenheiro de suporte, gere traços de rede ao criar o relatório do sistema. Obtenha os traços de rede durante o tempo em que o problema ocorre, se forem reproduzíveis. Os recursos incluem:<br>• Um trace de rede de 60 segundos obtido na câmera (aplicável apenas ao firmware 5.20 e superior)<br>Use o seguinte comando VAPIX para alterar o login, o endereço IP e a duração (em segundos) se necessário:<br>`http://root:pass@192.168.0.90/axis-cgi/ /debug/debug.tgz?cmd=pcapdump&duration=60`<br>• Um trace de rede de 10 a 30 segundos feito no servidor que mostra a comunicação entre o servidor e a câmera. |

| Informações adicionais | |
|---|---|
| **Arquivos de banco de dados** | Nos casos em que precisamos examinar ou reparar manualmente o banco de dados. Selecione **Include database in the report (Incluir banco de dados no relatório)** antes de gerar o relatório do sistema. |
| **Capturas de tela** | Use capturas de tela quando se tratar de um problema de visualização ao vivo, relacionado à interface do usuário. Por exemplo, quando quiser mostrar uma linha do tempo para gravações ou quando for difícil de descrever. |
| **Gravações de tela** | Use gravações de tela quando é difícil descrever o problema em palavras, por exemplo, quando há muitas interações com a interface do usuário envolvidas para reproduzir o problema. |

T10211981_pt

2025-09 (M3.2)