

## **AXIS Device Manager Extend**

**Manual do Usuário**

# AXIS Device Manager Extend

## Índice

---

<b>Sobre</b> .....	3
<b>Sobre organizações</b> .....	4
<b>Visão geral da solução</b> .....	5
<b>Pré-requisitos</b> .....	10
<b>Início</b> .....	12
Registrar uma conta My Axis .....	12
Instale o cliente e ative sua conta .....	12
Criar organização .....	12
Instalar o host de borda .....	12
Reivindicar o host de borda .....	13
<b>Gerenciar dispositivos</b> .....	14
Adição de dispositivos descobertos ao seu host de borda .....	14
Remover dispositivos .....	15
Login nos seus dispositivos. ....	15
<b>Configuração</b> .....	16
Ativação do acesso remoto .....	16
Remoção de um local .....	16
Adição de novos usuários à sua organização .....	16
Sobre funções de usuário .....	17
Elevação de função de usuário .....	17
Remover usuários .....	17
<b>Gerenciamento do AXIS OS</b> .....	18
Gerenciar versões do AXIS OS com base no modelo .....	18
Gerenciar o AXIS OS em um host de borda. ....	18
Exibir atualizações em andamento e concluídas do AXIS OS .....	18
<b>Políticas</b> .....	19
Criar e aplicar uma política de segurança .....	19
Criar e aplicar uma política de aplicativo .....	19
Editar uma política .....	20
Excluir uma política .....	20
<b>Gerenciar licenças</b> .....	21
Licencie seu produto .....	21
<b>Solução de problemas</b> .....	22
Como configurar as opções de firewall .....	22

# AXIS Device Manager Extend

## Sobre

---

### Sobre

A solução AXIS Device Manager Extend oferece aos administradores de sistemas uma interface para descobrir, configurar e operar dispositivos Axis nas redes de suas organizações.

#### o aplicativo de desktop AXIS Device Manager Extend

O aplicativo de desktop é um programa utilitário de software que pode ser usado como uma interface do usuário sob demanda ou sempre disponível para gerenciar o sistema. Ele pode ser executado em um computador dedicado, juntamente com um host de borda instalado localmente, ou separado do host de borda em um laptop conectado remotamente. O cliente mostra ao usuário o status geral do sistema e as ações de gerenciamento prontamente disponíveis.

#### O host de borda

O componente de host de borda no AXIS Device Manager Extend é um serviço de gerenciamento local sempre disponível que é responsável por administrar dispositivos locais, como câmeras. O host de borda do AXIS Device Manager Extend também funciona como um link para o serviço de gerenciamento remoto da Axis, onde a mesma funcionalidade de API oferece suporte à administração remota de sites via Axis Service Platform.

# AXIS Device Manager Extend

## Sobre organizações

---

### Sobre organizações

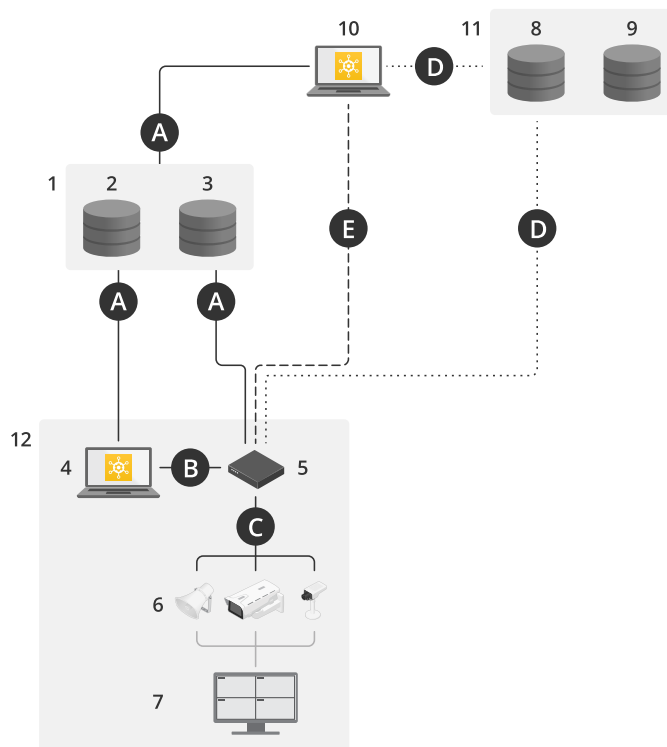
A organização é uma representação virtual de suas instalações de sistema Axis e é o centro dos seus serviços de nuvem. Uma organização hospeda todos os dispositivos e contas de usuário de uma empresa em uma hierarquia que regula o acesso e garante a máxima segurança. Ao mesmo tempo, possibilita o gerenciamento flexível de usuários e dispositivos para pequenas empresas e grandes corporações.

- Ao criar uma nova organização, você se torna seu proprietário. A organização conecta seu sistema aos usuários do serviço de nuvem Axis.
- Você pode convidar usuários para a organização. Consulte .
- Você pode atribuir funções diferentes aos usuários.
- A organização contém uma pasta padrão onde você pode começar a construir sua estrutura organizacional atendendo às suas necessidades. Você pode estruturar a organização em pastas e subpastas. Em geral, uma pasta representa um local físico ou localização de um sistema dentro de uma organização.
- Gerencie as licenças do seu sistema dentro de sua organização.
- Para criar uma organização, você precisa de uma conta My Axis.

# AXIS Device Manager Extend

## Visão geral da solução

### Visão geral da solução



AXIS Device Manager Extend com acesso local e remoto

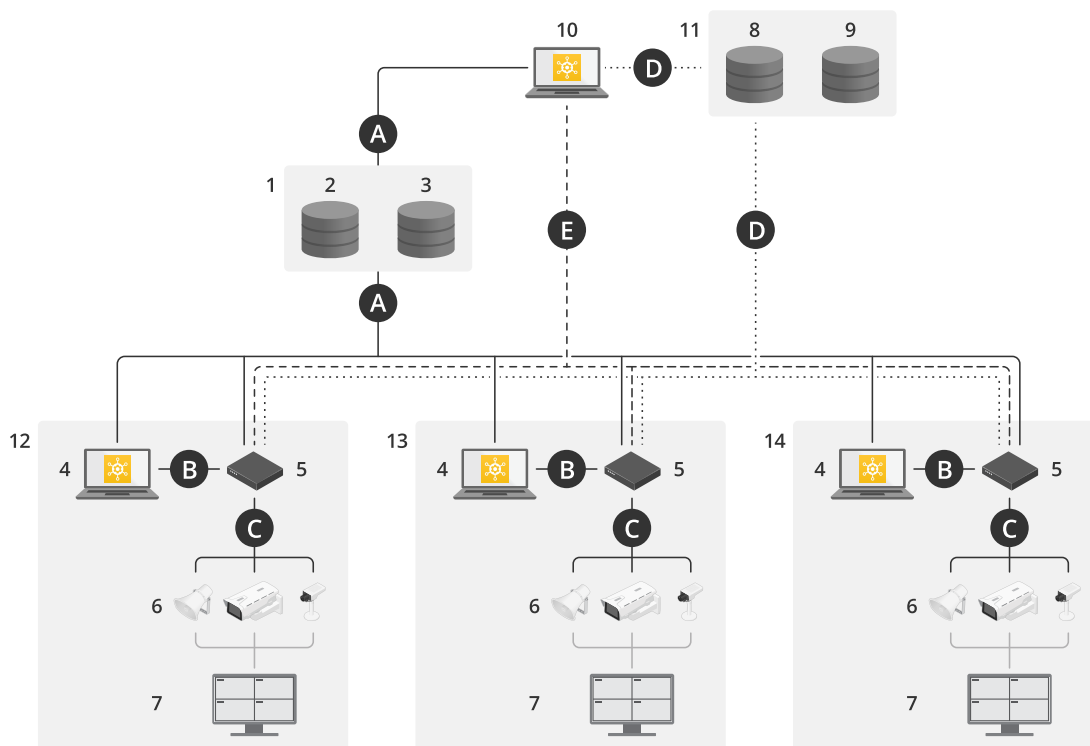
- 1 Axis
- 2 IAM (My Axis)
- 3 Dados da organização
- 4 Cliente local
- 5 Host de borda
- 6 Dispositivos
- 7 VMS
- 8 TURN
- 9 Sinalização
- 10 Cliente remoto
- 11 Servidores WebRTC de acesso remoto
- 12 Local 1

Conexão	URL e IP	Deteção automática	Protocolo	Comentários
A	prod.adm.connect.axis.com (52.224.128.152 ou 40.127.155.231)	443	HTTPS	Obrigatório

# AXIS Device Manager Extend

## Visão geral da solução

B	Descoberta de HTTP (do cliente para hosts de borda) Transferência de dados (entre o cliente e hosts de borda) Descoberta multicast (do cliente para hosts de borda) Descoberta multicast (de hosts de borda para o cliente)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Necessário para provisionar o local. Opcional após o provisionamento
C	Transferência de dados (entre o host de borda e os dispositivos) Descoberta de unicast Descoberta de multicast Descoberta de HTTP	80 / porta personalizada, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Obrigatório
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP e TCP)	Com base no padrão WebRTC Opcional e definido como desativado por padrão
E	Ponto a ponto (P2P)	49152-65535	DTLS (UDP e TCP)	



AXIS Device Manager Extend com a configuração de vários sites usando acesso local e remoto

- 1 Axis
- 2 IAM (My Axis)
- 3 Dados da organização
- 4 Cliente local
- 5 Host de borda
- 6 Dispositivos
- 7 VMS

# AXIS Device Manager Extend

## Visão geral da solução

---

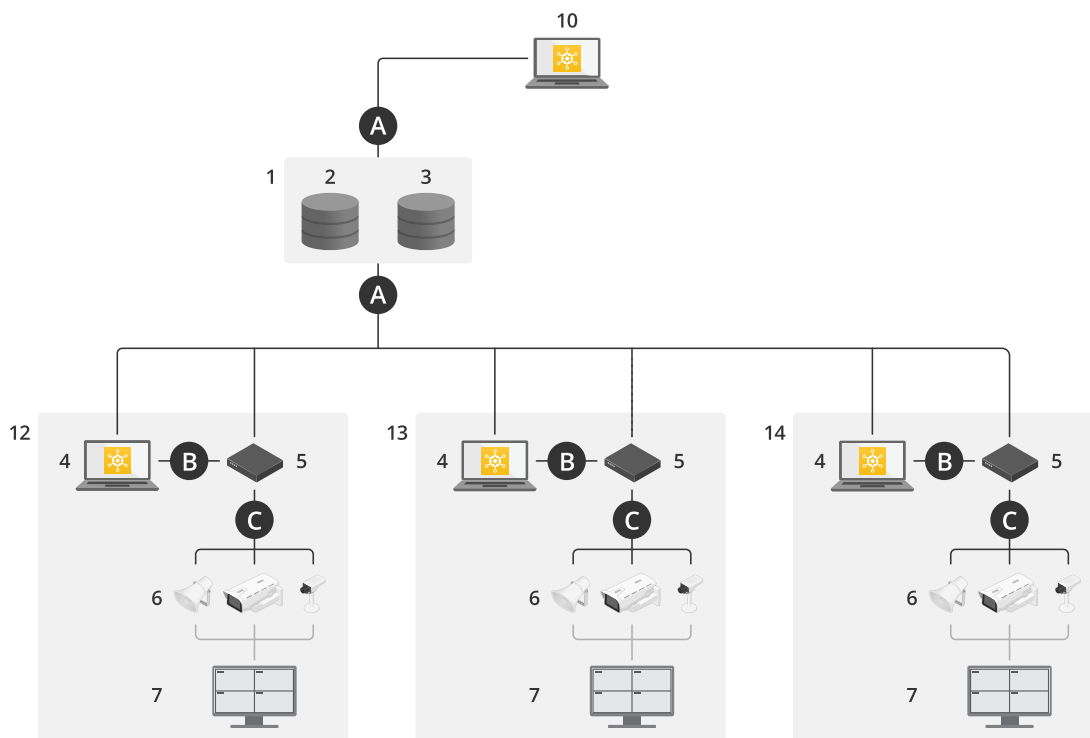
- 8 TURN
- 9 Sinalização
- 10 Cliente remoto
- 11 Servidores WebRTC de acesso remoto
- 12 Local 1
- 13 Local 2
- 14 Local 3

Conexão	URL e IP	Deteção automática	Protocolo	Comentários
A	prod.adm.connect.axis.com (52.224.128.152 ou 40.127.155.231)	443	HTTPS	Obrigatório
B	Descoberta de HTTP (do cliente para hosts de borda) Transferência de dados (entre o cliente e hosts de borda) Descoberta multicast (do cliente para hosts de borda) Descoberta multicast (de hosts de borda para o cliente)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Necessário para provisionar o local. Opcional após o provisionamento
C	Transferência de dados (entre o host de borda e os dispositivos) Descoberta de unicast Descoberta de multicast Descoberta de HTTP	80 / porta personalizada, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Obrigatório
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP e TCP)	Com base no padrão WebRTC Opcional e definido como desativado por padrão

# AXIS Device Manager Extend

## Visão geral da solução

E	Ponto a ponto (P2P)	49152-65535	DTLS (UDP e TCP)
---	---------------------	-------------	------------------



AXIS Device Manager Extend com acesso local e acesso remoto usando uma conexão VPN

- 1 Axis
- 2 IAM (My Axis)
- 3 Dados da organização
- 4 Cliente local
- 5 Host de borda
- 6 Dispositivos
- 7 VMS
- 8 TURN
- 9 Sinalização
- 10 Cliente remoto
- 11 Servidores WebRTC de acesso remoto
- 12 Local 1
- 13 Local 2
- 14 Local 3

Conexão	URL e IP	Deteção automática	Protocolo	Comentários
A	prod.adm.connect.axis.com (52.224.128.152 ou 40.127.155.231)	443	HTTPS	Obrigatório



# AXIS Device Manager Extend

## Visão geral da solução

---

B	Descoberta de HTTP (do cliente para hosts de borda) Transferência de dados (entre o cliente e hosts de borda) Descoberta multicast (do cliente para hosts de borda) Descoberta multicast (de hosts de borda para o cliente)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Necessário para provisionar o local. Opcional após o provisionamento
C	Transferência de dados (entre o host de borda e os dispositivos) Descoberta de unicast Descoberta de multicast Descoberta de HTTP	80 / porta personalizada, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Obrigatório
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP e TCP)	Com base no padrão WebRTC Opcional e definido como desativado por padrão
E	Ponto a ponto (P2P)	49152-65535	DTLS (UDP e TCP)	

- Um requisito adicional é um DNS público como o Google DNS: 8.8.8.8 / 8.8.4.4 ou Cloudflare DNS: 1.1.1.1
- Ambas as conexões A e C são necessárias para oferecer suporte à funcionalidade plena do sistema AXIS Device Manager Extend.
- Estamos trabalhando continuamente no desenvolvimento do aplicativo. Por isso, recomendamos permitir acesso no firewall a conexões de rede de saída do aplicativo de desktop AXIS Device Manager Extend e qualquer host de borda.

# AXIS Device Manager Extend

## Pré-requisitos

---

### Pré-requisitos

#### Sistemas operacionais compatíveis:

- Windows 10 Pro e Enterprise
- Windows 11 Pro e Enterprise
- Windows Server 2016, 2019 e 2022 (sistema baseado em x64)
- Privilégios de administrador do sistema necessário para instalação e alterações na configuração.

#### Recomendação de sistema mínima:

- CPU: Intel Core i5
- RAM: 4 GB
- Rede: 100 Mbps

#### Conectividade à Internet

##### Observação

O aplicativo AXIS Device Manager Extend exige que a conexão com a Internet seja configurada com certificados que a identifiquem como pertencente à organização criada e associada à conta My Axis usada na instalação. No entanto, para se beneficiar de determinados recursos, como informações de garantia e suporte multissite, uma conexão com a Internet é necessária. Além disso, o cliente e/ou o host de borda só se atualizam automaticamente no modo online.

#### Data e hora sincronizadas

##### Observação

Certifique-se de que todos os componentes do sistema estejam sincronizados. Caso contrário, a autenticação de certificado entre o host de borda e o cliente ou backend poderá falhar. Recomenda-se que todas as máquinas host sejam sincronizadas com um Network Time Server comum para evitar possíveis problemas.

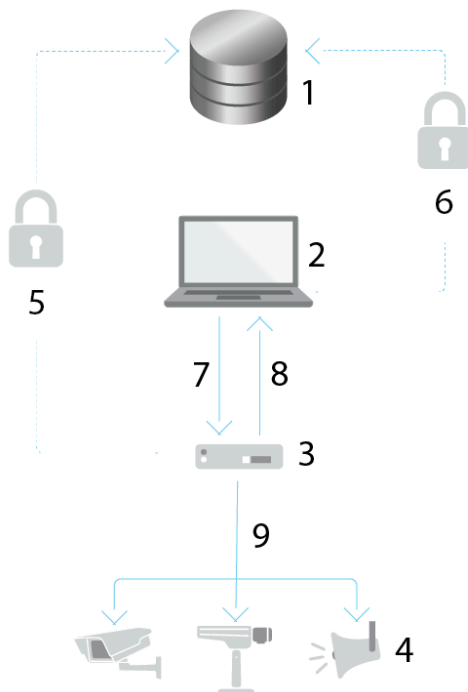
#### Portas de rede abertas:

Para conexões seguras do aplicativo de desktop AXIS Device Manager Extend ao host de borda, descoberta de host de borda e AXIS Remote Service.

# AXIS Device Manager Extend

## Pré-requisitos

---



- 1 Plataforma de serviços Axis
- 2 Aplicativo de desktop AXIS Device Manager Extend
- 3 Host de borda
- 4 Dispositivos
- 5 HTTPS (porta 443)
- 6 HTTPS (porta 443)
- 7 HTTPS (porta 37443), descoberta UDP Multicast (porta 6801), descoberta HTTP (porta 37080)
- 8 Descoberta UDP Multicast (porta 6801)
- 9 HTTPS e HTTP (portas 443 e 80), descoberta Multicast – SSDP (porta 1900) – Bonjour (porta 5353), descoberta Unicast (porta 1900), descoberta HTTP (portas 80 e 443)

### Acesso de rede de saída

Estamos trabalhando continuamente no desenvolvimento do aplicativo. Por isso, recomendamos permitir acesso no firewall a conexões de rede de saída do aplicativo de desktop AXIS Device Manager Extend e qualquer host de borda.

# AXIS Device Manager Extend

## Início

---


### Início

#### Registrar uma conta My Axis

Registre uma conta My Axis em [axis.com/my-axis/login](https://axis.com/my-axis/login).

Para tornar sua conta My Axis mais segura, ative a autenticação multifator (MFA). A MFA é um sistema de segurança que adiciona outra camada de verificação para garantir a identidade do usuário.

Para ativar a MFA:

1. Acesse [axis.com/my-axis/login](https://axis.com/my-axis/login).
2. Faça login com suas credenciais My Axis.
3. Vá para  e selecione **Account settings (Configurações da conta)**.
4. Clique em **Security settings (Configurações de segurança)**
5. Clique em **Handle your 2-factor authentication (Lidar com sua autenticação de 2 fatores)**.
6. Insira suas credenciais de My Axis.
7. Escolha um dos métodos de autenticação **Authenticator App (TOTP) (App autenticador (TOTP))** ou **Email** e siga as instruções na tela.

#### Instale o cliente e ative sua conta

Vá para a página do produto em [axis.com](https://axis.com) e baixe o instalador do aplicativo de desktop **AXIS Device Manager Extend**

1. Vá para o local em que o aplicativo foi baixado e clique em para instalá-lo.
2. **Select client (cliente)** e clique em **Install (Instalar)**.
3. Entre em sua conta My Axis.
4. Confirme seu endereço de email para concluir a ativação.
5. Crie ou ingresse em uma organização existente.

#### Criar organização

Para adicionar dispositivos ao seu sistema, você precisa fazer parte de uma organização. É assim que você mantém e protege seus dispositivos de forma segura em um ou mais locais. Se ainda não for membro de uma organização, um assistente de configuração aparecerá e o guiará pelo processo.

Para criar uma organização:

1. Entre no Axis Device Manager Extend usando sua conta My Axis.
2. Siga as instruções do assistente de configuração

Para criar organizações adicionais:

- Vá para o menu suspenso com o nome de sua organização.
- Selecione **+ Criar nova organização**
- Siga as instruções do assistente de configuração.

# AXIS Device Manager Extend

## Início

---

### Instalar o host de borda

O host de borda e o cliente de área de trabalho estão incluídos no instalador do AXIS Device Manager Extend. Recomendamos instalar o host de borda em um servidor o mais próximo possível dos seus dispositivos.

1. Escolha um servidor no qual deseja instalar o host de borda.
2. Execute o instalador no servidor e selecione somente para instalar o host de borda.

### Reivindicar o host de borda

Para criar uma conexão segura com seus dispositivos no aplicativo de desktop AXIS Device Manager Extend, primeiro é necessário reivindicar um host de borda para sua organização.

1. Clique em um host de borda com o status **Unclaimed (Não reivindicado)**
  - 1.1 Clique em **Add new edge host (Adicionar novo host de borda)** se não houver host de borda na lista
  - 1.2 Digite o endereço IP do local em que o host de borda está localizado
2. Digite o nome do host de borda
3. Adicione uma descrição opcional (recomendado)
4. Clique em **Claim edge host (Reivindicar host de borda)**

# AXIS Device Manager Extend

## Gerenciar dispositivos

---

### Gerenciar dispositivos

#### Adição de dispositivos descobertos ao seu host de borda

1. Vá para Edge hosts (Hosts de borda).
2. Selecione um host de borda reivindicado na lista à qual deseja adicionar dispositivos.
3. Vá para Devices > Discovered (Dispositivos > Descobertos).
4. Selecione os dispositivos que gostaria de adicionar ou selecione todos os dispositivos marcando a caixa na parte superior da coluna de seleção.
5. Clique em Add devices to edge host (Adicionar dispositivos a host de borda) .

Os dispositivos agora são listados na guia Managed (Gerenciados) e seus status podem ser revisados na Edge host overview (Visão geral do host de borda).

#### Adicionar dispositivos a partir de endereços IP

Adicione dispositivos que não são detectados automaticamente de sub-redes, endereços IP individuais ou um intervalo IP.

#### Adicione dispositivos a partir da faixa IP

1. Vá para um host de borda reivindicado por sua organização.
2. Vá para Settings > Device discovery (Configurações > Descoberta de dispositivos).
3. Clique em Add by IP (Adicionar por IP)
4. Selecione Manual entry (Entrada manual)
5. Digite a faixa de IPs
6. Clique em Add IP addresses (Adicionar endereços IP)
7. Vá para Devices > Discovered (Dispositivos > Descobertos)
8. Selecione os dispositivos que gostaria de adicionar ou selecione todos os dispositivos marcando a caixa na parte superior da coluna de seleção.
9. Clique em Add devices (Adicionar dispositivos).

#### Adicionar dispositivos de um arquivo

1. Vá para um host de borda reivindicado por sua organização.
2. Vá para Settings > Device discovery (Configurações > Descoberta de dispositivos).
3. Clique em Add by IP (Adicionar por IP)
4. Selecione Import from file (Importar de arquivo).
5. Selecione o arquivo separado por vírgulas (. CSV) com os endereços IP
6. Clique em Import (Importar)
7. Vá para Devices > Discovered devices (Dispositivos > Dispositivos descobertos).
8. Selecione os dispositivos que gostaria de adicionar ou selecione todos os dispositivos marcando a caixa na parte superior da coluna de seleção.

# AXIS Device Manager Extend

## Gerenciar dispositivos

---

9. Clique em **Add devices** (Adicionar dispositivos).

### Observação

O arquivo deve ter:  
Um cabeçalho para a coluna de endereços IP.  
Uma única coluna.  
No máximo 25.600 endereços IP.

## Remover dispositivos



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

[help.axis.com/?&piald=63389&tsection=remove-devices](http://help.axis.com/?&piald=63389&tsection=remove-devices)

*Remover dispositivos de um host de borda*

1. Clique em **Edge host (Host de borda)**
2. Selecione um host de borda.
3. Vá para **Devices (Dispositivos)**
4. Selecione os dispositivos que gostaria de remover ou selecione todos os dispositivos marcando a caixa na parte superior da coluna de seleção.
5. Clique no ícone **Remover dispositivos do host de borda** no menu de ação.
6. Clique em **Remove (Remover)**.

Os dispositivos removidos podem ser encontrados em **Devices > Discovered (Dispositivos > Descobertos)**.

## Login nos seus dispositivos.

1. Clique em **Edge hosts (Hosts de borda)**
2. Selecione um host de borda.
3. Vá para **Devices > Managed (Dispositivos > Gerenciados)**.
4. Selecione os dispositivos que deseja acessar ou selecione todos os dispositivos marcando a caixa na parte superior da coluna de seleção.
5. Clique em **Log in (Fazer login)** para fazer login automaticamente em vários dispositivos.
6. Digite o nome de usuário e a senha.
7. Clique em **Fazer login**

### Observação

Se o nome de usuário e a senha estiverem corretos, **Status** mostrará **Reachable (Alcançável)**

# AXIS Device Manager Extend

## Configuração

---

### Configuração

#### Ativação do acesso remoto

Se suas configurações de firewall bloquearem conexões de saída, talvez seja necessário fornecer uma conexão de proxy para acessar o site remotamente.

1. Selecione o host de borda para o qual deseja ativar o acesso remoto.
2. Vá para **Settings > Edge hosts connections (Configurações > Conexões de hosts de borda)**.
3. Ative **Allow remote access to edge host (Permitir acesso remoto ao host de borda)**.
4. Se você precisar inserir um endereço de proxy para acessar a Internet, digite-o em **Proxy address (Endereço proxy)**.

Você será notificado assim que a conexão estiver ativa.

#### Observação

Para oferecer suporte à conexão com hosts de borda em outras redes, talvez seja necessário adicionar a seguinte configuração à "lista de permissões" do firewall da rede corporativa: Endpoint Porta Protocolo signaling.prod.webrtc.connect.axis.com 443 HTTPS \*.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (Turn e P2P) 5349, 49152 - 65535 DTLS (UDP e TCP)

#### Remoção de um local

Antes de remover um host de borda da sua organização, você precisará pertencentes ao host de borda. Os dispositivos podem ser encontrados em **Devices > Discovered (Dispositivos > Descobertos)**.

1. Clique em **Edge hosts (Hosts de borda)**.
2. Selecione o host de borda com as teclas de seta ou mova o cursor do mouse sobre ele com o ponteiro.
3. Clique em ... e selecione **Remove edge host (Remover host de borda)** do menu suspenso.
4. Marque a opção **I'm aware of the risks. (Estou ciente dos riscos.)**
5. Clique em **Remove (Remover)**.

#### Adição de novos usuários à sua organização

1. Selecione a organização em que deseja definir as configurações de usuário.
2. Vá para o painel **My Systems (Meus sistemas)**.
3. Vá para **Organization > Users (Organização > Usuários)**.
4. Clique em **Invite users (Convidar usuários)**.
5. Digite o endereço de email do usuário que deseja convidar para sua organização.
6. Selecione a função a ser atribuída aos usuários. Observe que, se quiser outra função para alguns usuários, será necessário convidá-los em um convite separado.
7. Se tiver selecionado **Operator (Operador)** ou **Viewer (Visualizador)**, selecione as pastas às quais os usuários terão acesso. Observe que as funções **Admin** têm acesso a todas as pastas da organização.
8. Clique em **Invite user (Convidar usuário)**.



# AXIS Device Manager Extend

## Configuração

---

### Observação

O usuário receberá um email de convite que ele poderá usar para entrar em My Systems (Meus sistemas). Se o usuário não tiver uma conta My Axis, deverá usar esse email para se inscrever para acessar a organização. Os convites podem ser revogados enquanto a aceitação está pendente.

## Sobre funções de usuário

As funções de usuário determinam quanto acesso um usuário tem aos sistemas de sua organização. Os recursos disponíveis variam em função da função do usuário.

### Administrador

Os administradores têm acesso a todo o sistema. Isso inclui o gerenciamento de usuários, dispositivos, licenças, vídeos e outros conteúdos.

Eles também podem integrar dispositivos usando o AXIS Camera Station Pro e o AXIS Installer. Os administradores podem gerenciar o monitoramento do servidor do AXIS Camera Station Pro em My Systems (Meus sistemas).

### Operador

Os operadores podem monitorar feeds de vídeo ao vivo, controlar dispositivos e acessar gravações para reprodução. Eles obtêm uma visão geral dos usuários da organização e suas respectivas funções. Os operadores também podem gerenciar o monitoramento do servidor do AXIS Camera Station Pro em My Systems (Meus sistemas).

### Visualizador

Os visualizadores podem monitorar feeds de vídeo ao vivo, mas não podem controlar dispositivos nem acessar gravações. Eles obtêm uma visão geral dos usuários da organização e suas respectivas funções.

## Elevação de função de usuário

1. Selecione a organização em que deseja definir as configurações de usuário.
2. Vá para **Users (Usuários)**.
3. Vá para a **Role (Função)** do usuário que deseja elevar
4. Clique no menu suspenso para selecionar a nova função

### Observação

A função muda imediatamente uma vez selecionada. Por motivos de segurança, os convites são limitados à função de visualizador.

## Remover usuários

1. Selecione a organização em que deseja definir as configurações de usuário.
2. Vá para **Users (Usuários)**.
3. Mova o ponteiro do mouse sobre o usuário que gostaria de remover para mostrar um novo menu de opções: ...
4. Clique em ... e selecione **Remove user (Remover usuário)** no menu suspenso.

# AXIS Device Manager Extend

## Gerenciamento do AXIS OS

---

### Gerenciamento do AXIS OS

Com o AXIS Device Manager Extend é possível gerenciar o sistema operacional de vários dispositivos em cada organização.

Para obter uma lista de atualizações do AXIS OS disponíveis para cada dispositivo em sua organização, agrupada por modelo, vá para **Home > AXIS OS inventory (Início > Inventário do AXIS OS)**. Para obter uma lista de atualizações do AXIS OS que estão disponíveis em um host de borda específico, selecione o host de borda e vá para **AXIS OS inventory (Inventário do AXIS OS)**.

### Gerenciar versões do AXIS OS com base no modelo

Para gerenciar o AXIS OS por modelo em sua organização:

1. Vá para **Home > AXIS OS versions (Início > Versões do AXIS OS)**
2. Clique no link da versão recomendada do AXIS OS. Isso abrirá as opções de atualização do AXIS OS.
3. Clique no menu suspenso **Upgrade to (Atualizar para)** para ver as opções disponíveis. A versão mais recente do AXIS OS será pré-selecionada.
4. Clique em **Upgrade (Atualizar)**.

### Gerenciar o AXIS OS em um host de borda.

Para gerenciar o AXIS OS em alguns ou todos os dispositivos adicionados a um host de borda:

1. Vá para **Edge hosts (Hosts de borda)**.
2. Clique no host de borda que deseja acessar.
3. Vá para **Devices (Dispositivos)**
4. Selecione todos ou apenas os dispositivos que deseja gerenciar.
5. Clique no ícone **AXIS OS** no menu de ações
6. Verifique todos ou alguns dos modelos na lista.
7. Se desejar alterar a versão do AXIS OS, clique na versão sugerida para ver o que está disponível para cada dispositivo. A versão mais recente do AXIS OS será pré-selecionada.
8. Clique em **Atualizar**.

### Exibir atualizações em andamento e concluídas do AXIS OS

Para exibir atualizações de software em andamento dos dispositivos conectados a um host de borda específico:

1. Clique em **Edge hosts (Hosts de borda)**
2. Clique no host de borda que deseja acessar.
3. Vá para **Log**

Para ver as atualizações de software em andamento:

4. Vá para **Log > Ongoing tasks (Log > Tarefas em andamento)**

### Políticas

As políticas gerenciam seus dispositivos automaticamente. Crie políticas para manter a segurança cibernética em seu site. Você também pode definir uma política para instalar e atualizar aplicativos automaticamente em seus dispositivos.

### Criar e aplicar uma política de segurança

Neste caso de uso de exemplo, criamos e aplicamos uma política de segurança básica a um número seletivo de dispositivos conectados a um host de borda.

Crie uma política de segurança básica:

1. Vá para **Edge hosts (Hosts de borda)**.
2. Clique no host de borda que deseja acessar.
3. Vá para **Devices (Dispositivos)**
4. Clique no ícone + próximo a **Policies (Políticas)**
5. Selecione **Basic security (Segurança básica)** e clique em **Continue (Continuar)**
6. Nomear sua política
7. Selecione as configurações que atendem às suas necessidades de segurança. Para o nível de segurança recomendado, mantenha as configurações padrão.
  - Para alterar a senha de root dos dispositivos selecionados, clique em **Device root password (Senha de root do dispositivo)** e digite a nova senha de root.
8. Clique em **Create (Criar)**.

Aplique a política:

1. Selecione os dispositivos aos quais deseja que a política seja aplicada.
2. Clique no ícone **Policy options (Opções da política)** no menu de ações.
3. Selecione a política de segurança e clique em **Save (Salvar)**.

### Criar e aplicar uma política de aplicativo

Neste caso de uso de exemplo, criamos e aplicamos uma política de aplicativo a um número seletivo de dispositivos conectados a um host de borda.

1. Vá para **Edge hosts (Hosts de borda)**.
2. Clique no host de borda que deseja acessar.
3. Vá para **Devices (Dispositivos)**
4. Clique no ícone + próximo a **Policies (Políticas)**
5. Selecione **Apps (Aplicativos)** e clique em **Continue (Continuar)**
6. Nomear sua política
7. Selecione os aplicativos que deseja instalar e atualizar em seus dispositivos.
8. Selecione a janela de atualização no menu suspenso.

# AXIS Device Manager Extend

## Políticas

---

9. Clique em **Create (Criar)**.

Aplique a política:

1. Selecione os dispositivos aos quais deseja que a política seja aplicada.
2. Clique no ícone **Policy options (Opções da política)** no menu de ações.
3. Selecione a política de aplicativos que deseja aplicar.
4. Clique em **Salvar**.

### Observação

Os aplicativos selecionados serão reinstalados automaticamente se forem removidos.

## Editar uma política

Para editar uma política existente:

1. Vá para **Edge hosts (Hosts de borda)**.
2. Clique no host de borda que deseja acessar.
3. Vá para **Devices (Dispositivos)**.
4. Clique em ... próximo à política que deseja editar e selecione **Edit policy (Editar política)** no menu suspenso.
5. Edite as configurações da política para atender às suas necessidades.
6. Clique em **Save (Salvar)**.

## Excluir uma política

Para excluir uma política existente:

- Vá para **Edge hosts (Hosts de borda)**.
- Clique no host de borda que deseja acessar.
- Vá para **Devices (Dispositivos)**.
- Clique em ... próximo à política que deseja editar e selecione **Delete policy (Excluir política)** no menu suspenso.
- Clique em **Delete (Excluir)**.

### Observação

Todos os dispositivos com essa diretiva aplicada serão mantidos com as configurações de política, mas as configurações não serão mais persistentes.

# AXIS Device Manager Extend

## Gerenciar licenças

---

### Gerenciar licenças

#### Licencie seu produto

Para licenciar seu produto, vá para *My Systems > Licenses (Licenças)*. Para saber mais sobre licenças para produtos e serviços Axis, consulte o *Manual do usuário do My Systems*.

# AXIS Device Manager Extend

## Solução de problemas

---

### Solução de problemas

#### Como configurar as opções de firewall

O cliente do AXIS Device Manager Extend requer acesso ao domínio axis.com e qualquer subdomínio.

Para que o host de borda do AXIS Device Manager Extend se comunique com o serviço Axis, os seguintes endereços IP e portas devem ser adicionados à lista de permissões no firewall da organização:

- 40.127.155.231 (UE), porta 443
- 52.224.128.152 e 40.127.155.231 (EUA), porta 443
- Um IP público de servidor DNS, porta 53

Como alternativa, o domínio prod.adm.connect.axis.com (que é um registro DNS A apontando para os endereços IP acima) poderia ser usado nas configurações do firewall.

O host de borda do AXIS Device Manager Extend usa o nome de domínio prod.adm.connect.axis.com para todas as solicitações de saída.

Para que isso funcione, a rede precisará usar um servidor DNS público e permitir o tráfego para o endereço IP do servidor DNS (e a porta padrão 53).

