

AXIS S3008 Recorder

Sobre seu dispositivo

O AXIS S3008 Recorder é um gravador de vídeo em rede compacto com um switch PoE integrado para facilitar a instalação. O dispositivo possui uma unidade de disco rígido de categoria de monitoramento. Ela também inclui uma porta USB para facilitar a exportação de cenas de vídeo. O gravador é fornecido em três modelos – incluindo um disco rígido de 2 TB, 4 TB ou 8 TB.

Quantas câmeras posso conectar ao gravador?

Até oito dispositivos podem ser conectados ao switch PoE do gravador.

Quanta potência o gravador pode fornecer às câmeras?

Estas são as limitações do Power over Ethernet (PoE):

- O gravador pode alimentar até oito dispositivos com PoE.
- A potência total disponível é:
 - 2 TB e 4 TB: 65 W
 - 8 TB: 60 W
- Cada porta de rede pode fornecer até 15,4 W (PoE Classe 3) na porta PoE (PSE) e 12,95 W no lado da câmera (PD).
- O switch aloca a alimentação PoE com base na classe PoE do dispositivo conectado.

Suporte a navegadores

Windows®

- Chrome™ (recomendado)
- Firefox®
- Edge®

OS X®

- Chrome™ (recomendado)
- Safari®

Outros

- Chrome™
- Firefox®

Para saber mais sobre como usar o dispositivo, consulte o manual disponível em *Documentação | Axis Communications*.

Se desejar obter mais informações sobre navegadores recomendados, acesse *Suporte a navegadores do Axis OS | Axis Communications*.

Início

Observação

Acesso à Internet é necessário durante a configuração do sistema.

- 1.
- 2.
- 3.
- 4.
- 5.

Quando a instalação estiver concluída:

- Todos os dispositivos Axis no sistema têm o firmware mais recente.
- Todos os dispositivos têm uma senha.
- A gravação usando as configurações padrão está ativa.
- É possível usar o acesso remoto.

Registrar uma conta My Axis

Registre uma conta My Axis em 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.
2. Faça login com suas credenciais My Axis.
3. Acesse  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.

Instalação do hardware

1. Instale o hardware da câmera.
2. Conecte o gravador à rede via porta de LAN.
3. Conecte as câmeras ao switch PoE integrado do gravador ou a um switch PoE externo.
4. Conecte o computador à mesma rede que o gravador.
5. Conecte a fonte de alimentação ao gravador.

Importante

Primeiro, conecte o cabo de alimentação ao gravador e, em seguida, conecte o cabo de alimentação à tomada elétrica.

6. Aguarde alguns minutos para que o gravador e as câmeras sejam inicializados antes de prosseguir.

▲ CUIDADO

Mantenha o gravador em um ambiente bem ventilado e com bastante espaço vazio ao redor do gravador para evitar superaquecimento.

Instalação do aplicativo de desktop

1. Acesse axis.com/products/axis-camera-station-edge e clique em **Download (Baixar)** para baixar o AXIS S3008 Recorder para Windows.
2. Abra o arquivo de configuração e siga as instruções do assistente de configuração.
3. Faça login com sua *conta My Axis*.

Criar um local

Um site é um ponto de entrada único para uma solução de monitoramento, por exemplo, todas as câmeras em uma loja. Você pode manter o controle de vários sites por meio de uma única conta My Axis.

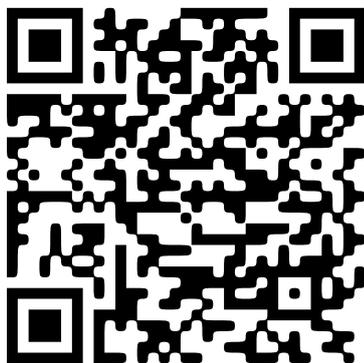
1. Inicie o aplicativo de desktop AXIS S3008 Recorder.
2. Faça login com sua *conta My Axis*.
3. Clique em **Create new site (Criar novo local)** e dê um nome ao local.
4. Clique em **Next (Próximo)**.
5. Selecione os dispositivos que deseja adicionar ao seu site.
6. Clique em **Next (Próximo)**.
7. Selecionar armazenamento.
8. Clique em **Next (Próximo)**.
9. Na página **Ready to install (Pronto para instalar)**, as opções **Offline mode (Modo offline)** e **Upgrade firmware (Atualizar firmware)** estão ativadas por padrão. Você poderá desativá-las se não quiser acessar o modo offline ou atualizar o firmware dos seus dispositivos para a versão mais recente.
10. Clique em **Install (Instalar)** e aguarde enquanto o AXIS S3008 Recorder configura os dispositivos. A configuração pode levar vários minutos.

Instalação do aplicativo para dispositivos móveis

Com o aplicativo para dispositivos móveis AXIS S3008 Recorder você pode acessar seus dispositivos e gravações de qualquer lugar. Você também pode obter notificações quando ocorrerem eventos ou quando alguém chamar de um intercomunicador.

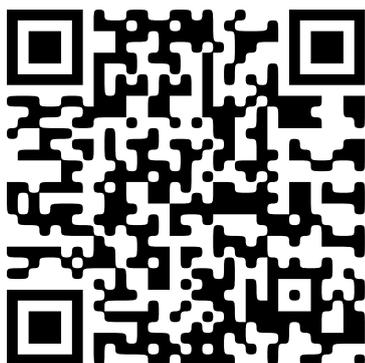
Para Android

Clique em *Download (Baixar)* ou leia o QR Code® a seguir.



Para iOS

Clique em *Download (Baixar)* ou leia o QR Code a seguir.



Abra o aplicativo AXIS S3008 Recorder para dispositivos móveis e faça login com suas credenciais da Axis.

Se você não tiver uma conta My Axis, acesse axis.com/my-axis para registrar uma nova conta.

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

A interface Web

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

-  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.

Cientes 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.

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.

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.

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

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

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

Observação

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

Local do dispositivo

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

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

Rede

IPv4

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

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

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

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

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

Observação

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

IPv6

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

Nome de host

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

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

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.

Protocolos de descoberta de rede

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

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

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

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

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

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

Proxies globais

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

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

Formatos permitidos para proxies http e https:

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

Observação

Reinicie o dispositivo para aplicar as configurações de proxy global.

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

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

Conexão com a nuvem com apenas um clique

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

Allow O3C (Permitir O3C):

- **One-click (Um clique):** Esta é a opção padrão. Para 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 a opção **Always (Sempre)** e permanecer conectado. Se o dispositivo não for registrado, ele será desconectado do O3C.
- **Sempre:** O dispositivo tenta continuamente estabelecer conexão com um serviço O3C pela Internet. Depois de registrar o dispositivo, ele permanecerá conectado. Use essa opção se o botão de controle estiver fora de alcance.
- **No (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 intercepções):** Ative para ativar o relatório de intercepções. O dispositivo usa intercepções para enviar mensagens sobre eventos importantes ou alterações de status para um sistema de gerenciamento. Na interface Web, você pode configurar intercepções para SNMP v1 e v2c. As intercepções serão desativadas automaticamente se você mudar para SNMP v3 ou desativar o SNMP. Se você usa SNMP v3, é possível configurar intercepções via aplicativo de gerenciamento do SNMP v3.
 - **Trap address (Endereço da intercepção):** Insira o endereço IP ou nome de host do servidor de gerenciamento.
 - **Trap community (Comunidade de intercepção):** Insira a comunidade que é usada quando o dispositivo envia uma mensagem de intercepção para o sistema de gerenciamento.
 - **Traps (Intercepções):**
 - **Cold start (Partida a frio):** Envia uma mensagem de intercepção quando o dispositivo é iniciado.
 - **Link up (Link ativo):** Envia uma mensagem de intercepção quando um link muda de inativo para ativo.
 - **Link down (Link inativo):** Envia uma mensagem de intercepção quando um link muda de ativo para inativo.
 - **Falha de autenticação:** Envia uma mensagem de intercepção quando uma tentativa de autenticação falha.

Observação

Todas as intercepções MIB de vídeo Axis são habilitados quando você ativa as intercepções 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 intercepções SNMP v1 e v2c não criptografadas. Se você usa SNMP v3, é possível configurar intercepções 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.

Power over Ethernet

Energia alocada: Número de Watts (W) que estão alocados no momento.

Total PoE consumption (Consumo total de PoE): Número de Watts (W) que são consumidos.

Keep PoE active during recorder restart (Manter PoE ativo durante reinício do gravador): Ative para fornecer energia para dispositivos conectados durante uma reinicialização do gravador.

Used space (Espaço usado): Percentual de espaço utilizado.

Free space (Espaço livre): Percentual de espaço disponível para gravações.

Free space (Espaço livre): Espaço em disco disponível exibido em megabytes (MB), gigabytes (GB) ou terabytes (TB).

Disk status (Status do disco): Status atual do disco.

Disk temperature (Temperatura do disco): Temperatura de operação no momento.

PoE: ative ou desative o PoE para cada porta. Quando um dispositivo for conectado, você verá as seguintes informações:

- **Nome amigável:** O nome amigável é definido nas **Configurações de rede**. O nome padrão é uma combinação do modelo e o endereço de controle de acesso à mídia (endereço MAC) do dispositivo conectado.
- **Consumo de energia:** Número de Watts (W) que são consumidos e estão alocados no momento.

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

Controle de acesso à rede e criptografia

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificados

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

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

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

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

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

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

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

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

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

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

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

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

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

Firewall: Ative para ativar o firewall.

Default Policy (Política padrão): Selecione como você 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 deseje permitir ou bloquear. Os números de portas devem estar entre 1 e 65535.
 - **Traffic type (Tipo de tráfego):** Selecione um 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 deseje 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 um 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 um stream de vídeo.
 - Assistir e exportar gravações.
 - Pan, tilt e zoom; com **acesso de conta usuário PTZ**.

⋮ O menu de contexto contém:

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

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

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

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

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

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

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

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

Segredo do cliente: Insira a senha OpenID novamente

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

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

Eventos

Regras

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

Observação

Você pode criar até 256 regras de ação.



Adicionar uma regra: Crie uma regra.

Nome: Insira um nome para a regra.

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

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

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

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



Adicionar uma condição: clique para adicionar uma condição.

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

Destinatários

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

Observação

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

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

Observação

É possível criar até 20 destinatários.



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

Nome: insira um nome para o destinatário.

Tipo: selecione na lista:

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

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

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

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

- **SFTP** 

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

- **SIP ou VMS** 

SIP: Selecione para fazer uma chamada SIP.

VMS: Selecione para fazer uma chamada VMS.

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

- **E-mail**

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

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

Observação

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

- **TCP**

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

Testar: clique para testar a configuração.



O menu de contexto contém:

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

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

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

Programações

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



Adicionar agendamento: clique para criar um cronograma ou pulso.

Acionadores manuais

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

Armazenamento

Armazenamento interno

Disco rígido

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

Ferramentas

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

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

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

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

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.

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 o tipo 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.

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.
- **Autorollback (Reversão automática):** Atualize e confirme a atualização dentro do período definido. Se você não confirmar, o dispositivo reverterá para a versão anterior do AXIS OS.

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

solução de problemas

Reset PTR (Redefinir PTR)  : redefine 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)**.

Configure seu dispositivo

Allocated power (Potência alocada)

O gravador reserva uma certa quantidade de energia para cada porta. A potência reservada total não pode exceder o orçamento total de energia. Uma porta não será alimentada se o gravador tentar reservar mais energia do que o que está disponível. Isso garante que todos os dispositivos conectados tenham energia.

A potência PoE pode ser alocada para os dispositivos conectados das seguintes formas:

- **Classe de PoE** – Cada porta determina automaticamente a quantidade de energia que será reservada de acordo com a classe de PoE do dispositivo conectado.
- **LLDP** – Cada porta determina a quantidade de energia que será reservada por meio da troca de informações de PoE usando o protocolo LLDP.

Observação

A alocação de energia com LLDP funciona somente com dispositivos compatíveis com firmware 9.80 ou posterior e para o AXIS S3008 Recorder com firmware 10,2 ou posterior.

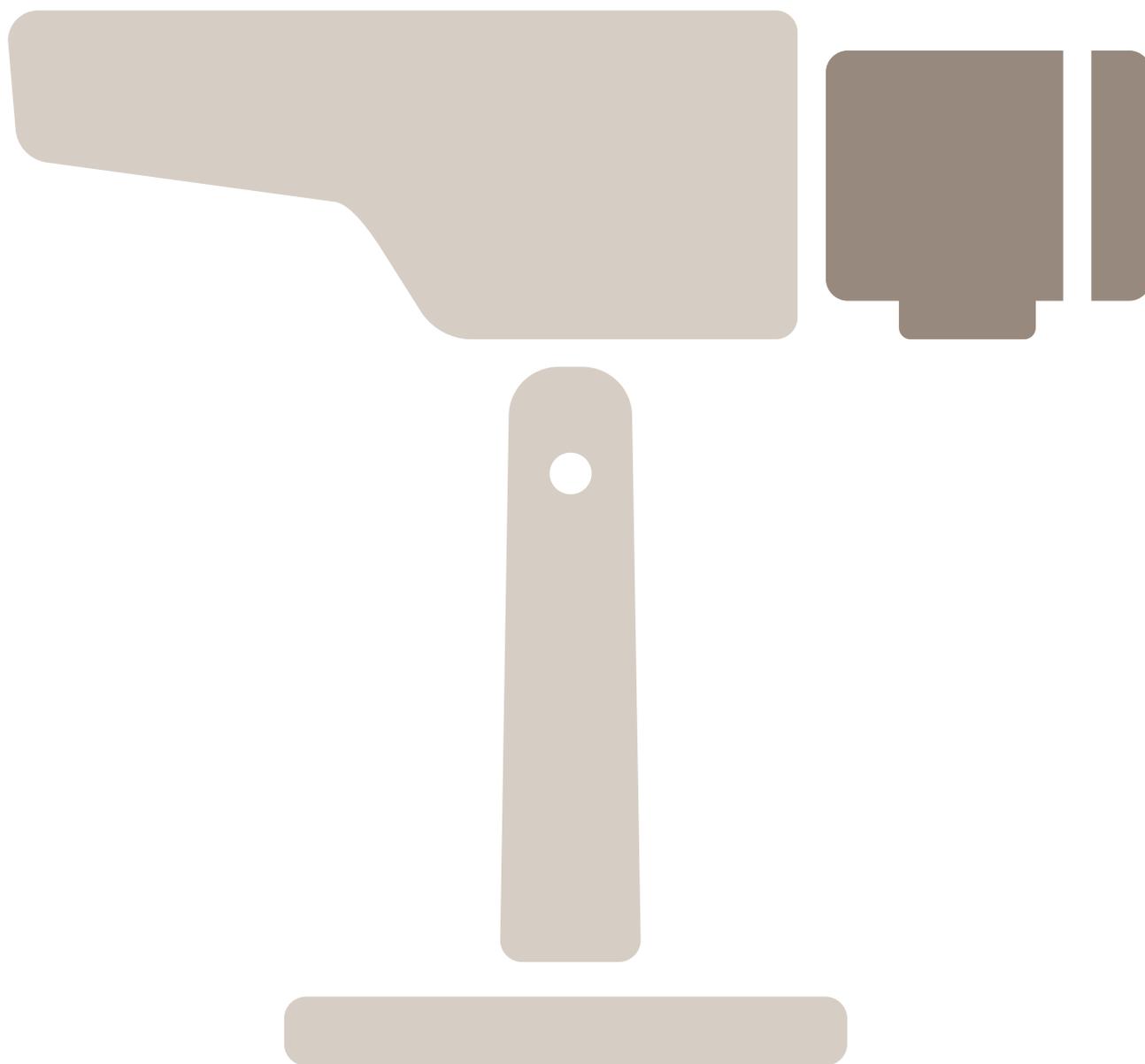
O LLDP está sempre ativo no AXIS S3008 Recorder, mas deve ser ativado no dispositivo conectado. Se o LLDP estiver desativado ou não houver suporte ao dispositivo conectado, a reserva de classe de PoE será usada em seu lugar.

Para ativar o LLDP em seu dispositivo PoE:

1. Abra a página da Web do dispositivo.
2. Vá para **Settings (Configurações) > System (Sistema) > Plain config (Configuração simples) > Network (Rede)**.
3. Em **LLDP POE (LLDP PoE)**, selecione a caixa de seleção **LLDP Send Max PoE (LLDP Enviar máx. PoE)**.

Exemplo:

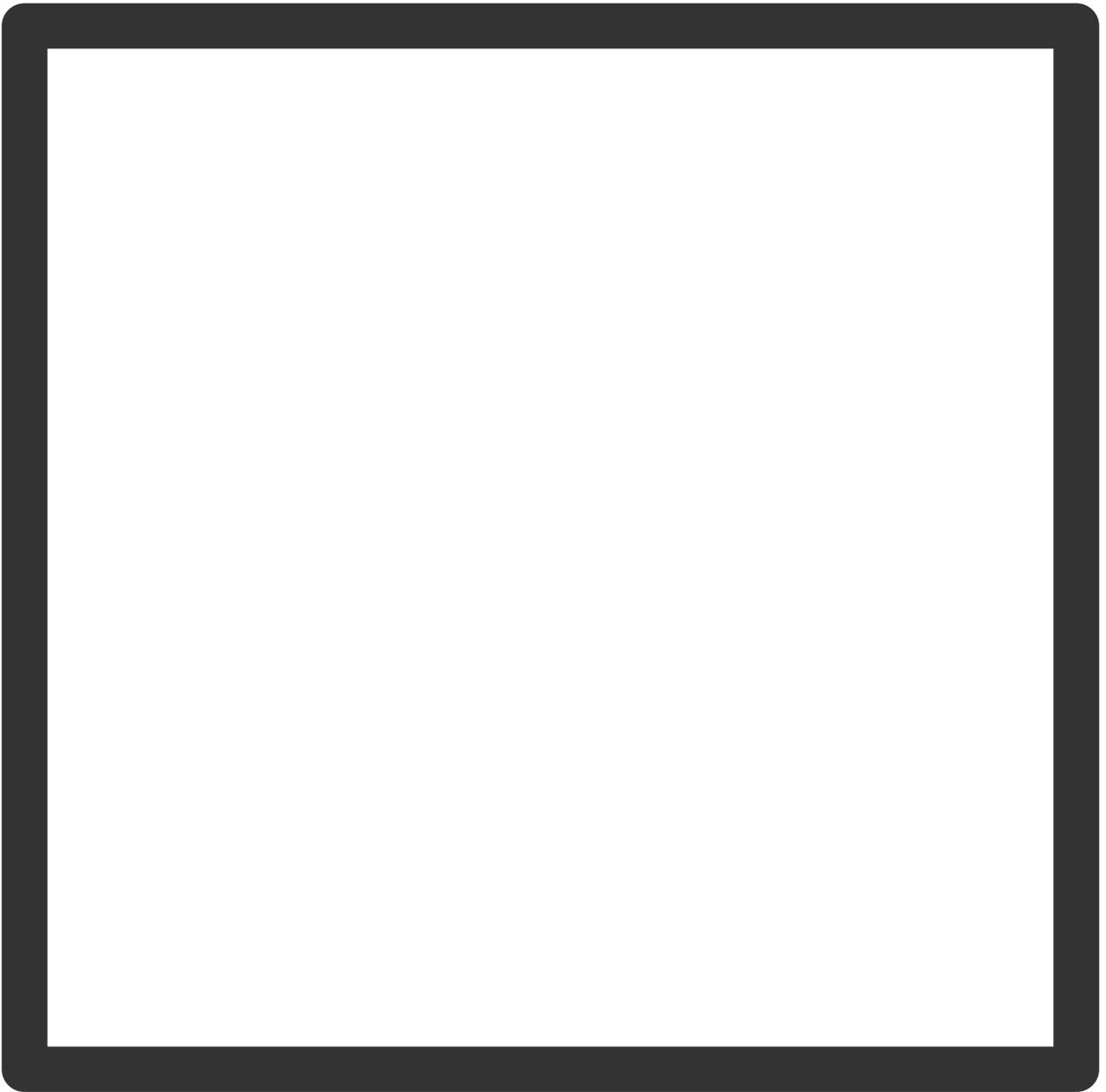
Neste exemplo, o AXIS S3008 Recorder tem um orçamento de potência total de 65 W.



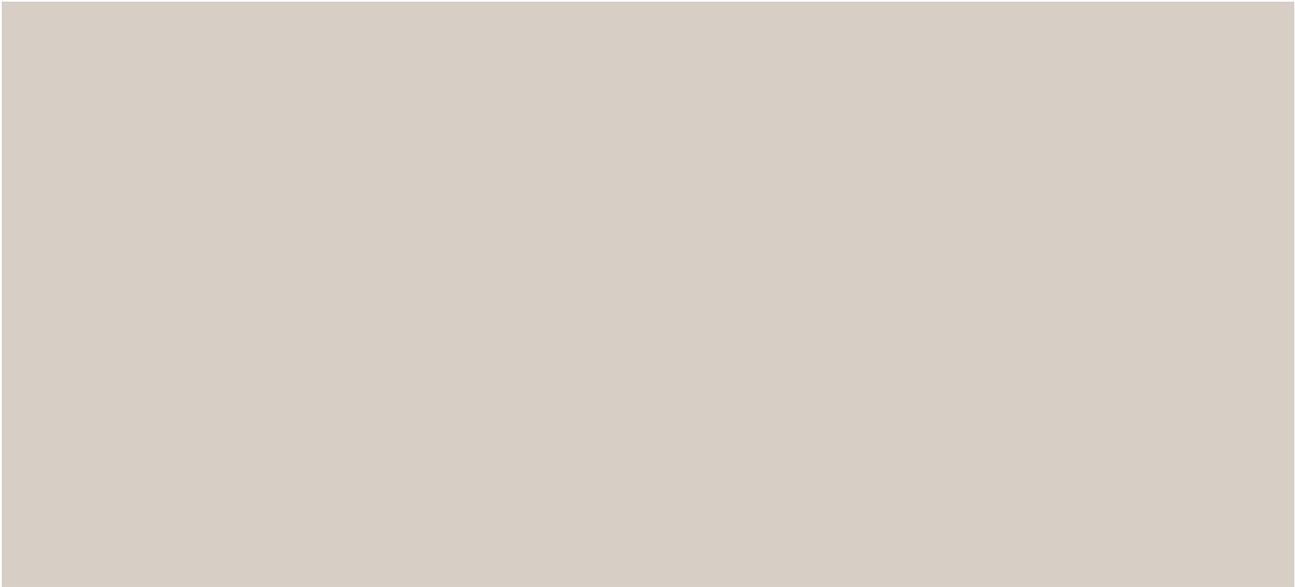
Dispositivo PoE Classe 2. Requer alimentação de 7 W, mas consome 5 W.



Dispositivo PoE Classe 3. Requer alimentação de 15,5 W, mas consome 7,5 W.



Potência reservada.

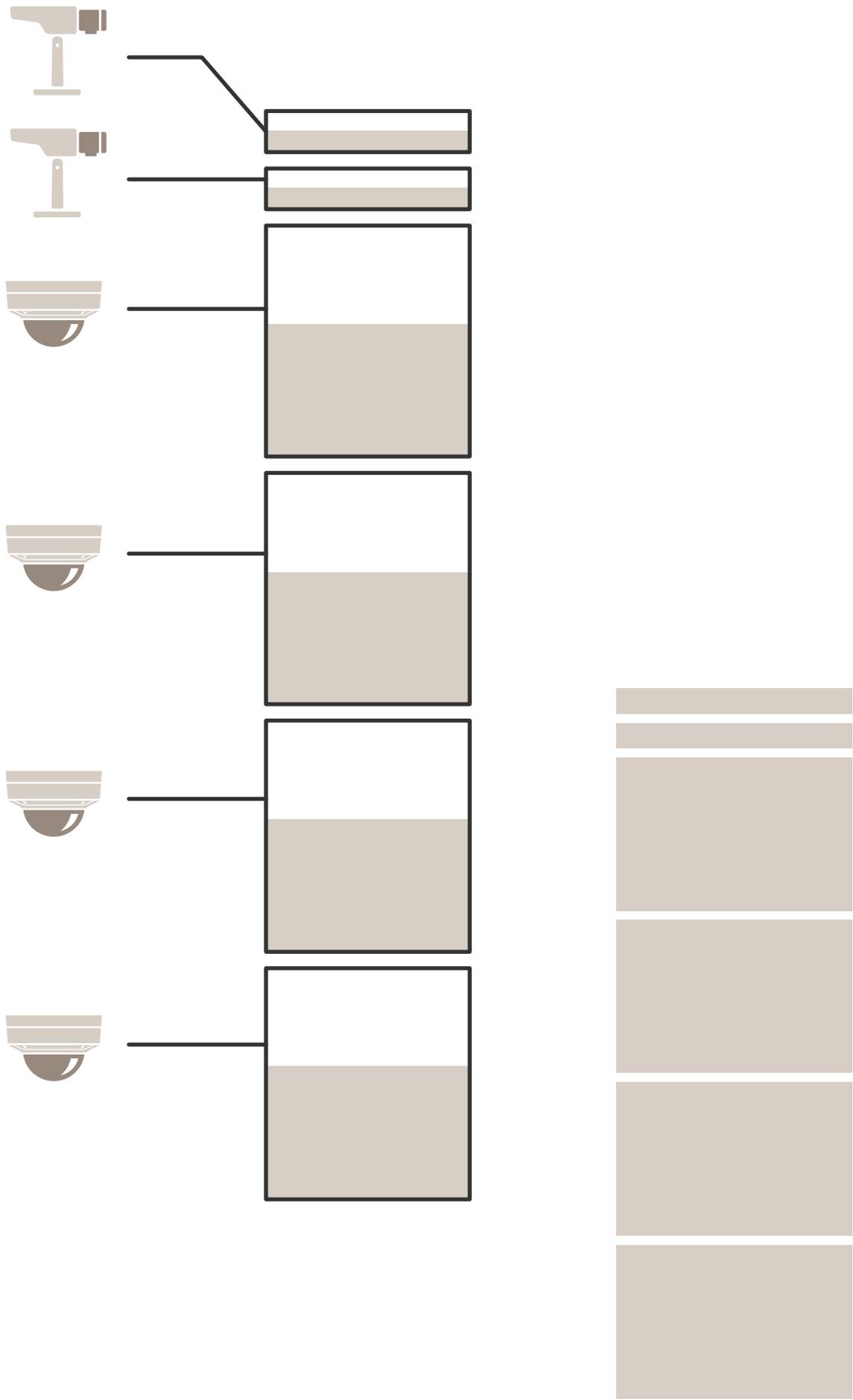


Consumo real de energia.

Alocação de potência por classe de PoE

Potência reservada

Consumo real de energia



- Cada porta reserva a quantidade de energia de acordo com a classe PoE do dispositivo.
- O gravador pode alimentar 2 dispositivos PoE Classe 3 e 4 dispositivos PoE Classe 2.
- A potência total reservada é $(2 \times 15,5) + (4 \times 7) = 59 \text{ W}$.
- A potência real consumida é $(2 \times 7,5) + (4 \times 5) = 35 \text{ W}$.

Alocação de potência por LLDP

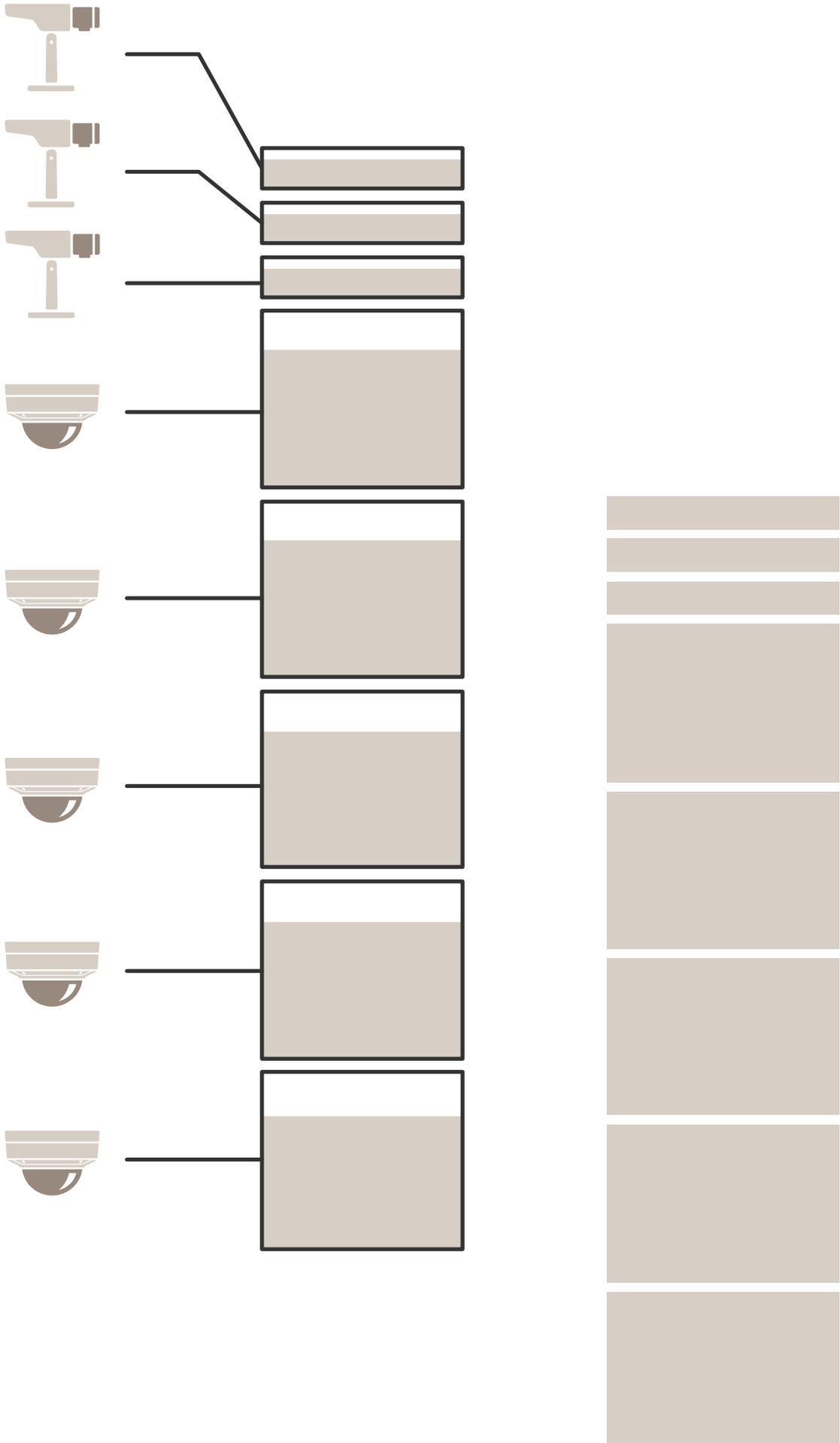
Observação

A alocação de potência via LLDP levará em conta a perda de potência que ocorrerá ao longo do cabo de rede.

Classe de PoE	1	2	3
Potência máxima da câmera	3.84	6.49	12.95
Perda de potência no cabo no pior caso	0,14	0.41	1.92
Potência necessária no gravador	3.98	6.90	14.87
Potência máxima para classe	4.00	7.00	15.40
Potência reservada no gravador	4 W	7 W	15,5 W

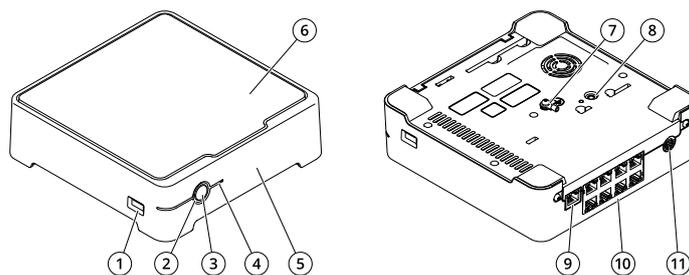
Potência reservada

Consumo real de energia



- Potência máxima determinada pelo dispositivo conectado.
- Cada porta reserva a quantidade de potência de acordo com o consumo máximo de potência PoE do dispositivo.
- O gravador poderá alimentar até 8 dispositivos se seus requisitos de potência máximos permanecerem dentro dos limites.
- A potência total reservada por 8 dispositivos PoE Classe 3 com LLDP é $(8 \times 7,5) = 60 \text{ W}$.
- A potência real consumida por 8 dispositivos PoE Classe 3 com LLDP é $(8 \times 7) = 56 \text{ W}$.
- Dessa forma, uma alocação de capacidade de PoE maior permite conectar mais dispositivos.

Visão geral do produto



- 1 Porta USB
- 2 LED de estado
- 3 Botão liga/desliga
- 4 LED do disco rígido
- 5 Sinal do alarme
- 6 Disco rígido
- 7 Aterramento
- 8 Botão de controle
- 9 Porta LAN
- 10 Porta PoE (8x)
- 11 Potência de entrada

Botão liga/desliga

- Para desligar o gravador, pressione o botão liga/desliga até que o alarme sonoro toque brevemente.
- Para parar o alarme sonoro, pressione brevemente o botão liga/desliga.

Botão de controle

O botão de controle é usado para:

- Restaurar o produto para as configurações padrão de fábrica. Consulte .
- Conexão a um serviço de conexão em nuvem com um clique (O3C) via Internet. Para conectar, mantenha o botão pressionado por aproximadamente 3 segundos até o LED de status piscar em verde.

Solução de problemas

O LED de status fornece as seguintes informações:

LED de estado	Indicação
Verde	O gravador está ligado e o status está ok
Laranja	O gravador está inicializando ou o firmware está sendo atualizado. Espere até o LED ficar verde.
Vermelho	Isso pode significar que a capacidade de PoE foi excedida. Se você acabou de conectar um dispositivo ao gravador, tente removê-lo novamente. Para obter mais informações sobre as limitações de PoE, consulte .

O LED do disco rígido fornece as seguintes informações:

LED do disco rígido	Indicação
Verde	O LED pisca em verde quando os dados são gravados na unidade de disco rígido.
Vermelho	Uma interrupção de gravação ocorreu. Vá para System (Sistema) > Storage (Armazenamento) para obter mais informações.

O alerta sonoro soa por este motivo:

- O orçamento do PoE está excedido. Se você acabou de conectar um dispositivo ao gravador, tente removê-lo novamente. Para obter mais informações sobre as limitações de PoE, consulte .

Observação

Você pode parar o alerta sonoro com uma pressionamento curto do botão liga/desliga.

O gravador desliga:

- O gravador está extremamente superaquecido.

Problemas técnicos, dicas e soluções

Emissão	Solução
Minhas gravações não estão disponíveis.	Vá para .
Não consigo conectar às minhas câmeras.	Vá para .
Recebo uma notificação de erro: "No contact" ("Sem contato").	Vá para .
Os meus sites não aparecem no meu aplicativo móvel.	Certifique-se de ter a versão 4 do app AXIS Companion para dispositivos móveis.

Corrigir problemas comuns

Antes de reiniciar, configurar ou redefinir seus dispositivos, recomendamos que salvar um relatório do sistema.

Consulte .

1. Verifique se suas câmeras e o gravador têm energia.
2. Verifique a conexão com a internet.
3. Verifique se a rede está funcionando.
4. Verifique se as câmeras estão conectadas à mesma rede que o computador, a menos que você esteja acessando remotamente.

Ainda não está funcionando?

5. Certifique-se de que as câmeras, o gravador e o aplicativo de desktop AXIS Companion possuam o firmware e as atualizações de software mais recentes.
Consulte .
6. Reinicie o aplicativo de desktop AXIS Companion.
7. Reinicie suas câmeras e o gravador.

Ainda não está funcionando?

8. Faça uma reinicialização forçada nas câmeras e no gravador, para colocá-los completamente nas configurações padrão de fábrica.
Consulte .
9. Adicione as câmeras redefinidas novamente ao site.

Ainda não está funcionando?

10. Atualize sua placa gráfica com os drivers mais recentes.

Ainda não está funcionando?

11. Salve um relatório do sistema e entre em contato com o *suporte técnico da Axis*.
Consulte .

Atualizar o firmware

As novas atualizações de firmware trazem para você o mais recente e avançado conjunto de recursos, funções e aperfeiçoamentos de segurança.

1. Vá para a interface Web do dispositivo líder.
2. Vá para **Maintenance (Manutenção) > Firmware upgrade (Atualização de firmware)** e clique em **Upgrade (Atualizar)**.
3. Siga as instruções na tela.

Reiniciar um gravador forçadamente

Importante

Mova o gravador cuidadosamente enquanto ele estiver ligado. Movimentos repentinos ou choques podem danificar o disco rígido.

Observação

- Uma redefinição forçada redefinirá todas as configurações, incluindo o endereço IP.
 - Uma redefinição forçada não removerá suas gravações.
1. Desligue o gravador:
Pressione o botão liga/desliga na parte frontal do gravador por 4 – 5 segundos até ouvir um bipe.
 2. Aguarde até que o gravador seja desligado e, em seguida, ligue-o para acessar o botão de controle.
 3. Pressione e segure o botão de controle. Pressione e solte o botão liga/desliga para iniciar o gravador. Solte o botão de controle após 15 – 30 segundos quando o LED indicador piscar em âmbar.
 4. Coloque cuidadosamente o gravador de volta no lugar.
 5. O processo estará concluído quando o indicador do LED de estado ficar verde. O produto foi então redefinido para as configurações padrão de fábrica. 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
6. Redefina seus dispositivos conectados ao gravador.
 7. Se o disco rígido estiver criptografado, ele deverá ser montado manualmente após a redefinição do gravador:
 - 7.1. Vá para a interface Web do dispositivo.
 - 7.2. Vá para **System (Sistema) > Storage (Armazenamento)** e clique em **Mount (Montar)**.
 - 7.3. Insira a senha de criptografia usada ao criptografar a unidade de disco rígido.

Não consigo fazer login na interface Web do produto.

Se você definir uma senha para o produto durante a configuração e posteriormente adicioná-lo a um site, não será mais possível fazer login na interface Web do produto com essa senha que você definiu. Isso ocorre porque o software AXIS Companion altera as senhas de todos os dispositivos no site.

Para fazer login em um dispositivo em seu site, digite o nome de usuário **root** e a senha do seu site.

Como apagar todas as gravações

1. Na interface Web do dispositivo, vá para **System (Sistema) > Storage (Armazenamento)**.
2. Selecione **Format (Formatar)** e clique em **Use tool (Usar ferramenta)**.

Observação

Este procedimento apaga todas as gravações da unidade de disco rígido, mas a configuração do gravador e do site não muda.

Salvar um relatório do sistema

1. Em AXIS S3008 Recorder, acesse  > **Save system report (Salvar relatório do sistema)**.
2. Quando você registrar um novo caso em Axis Helpdesk, anexe o relatório do sistema.

Precisa de mais ajuda?

Links úteis

- *Manual do usuário AXIS Companion*

Entre em contato com o suporte

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

T10152902_pt

2025-06 (M32.2)

© 2020 – 2025 Axis Communications AB