AXIS OS Hardening Guide

AXIS OS Hardening Guide

Introdução

Introdução

A Axis Communications se esforça para implementar as práticas recomendadas de segurança cibernética ao design, ao desenvolvimento e aos testes de nossos dispositivos a fim de minimizar o risco de falhas que possam ser exploradas por hackers em um ataque. No entanto, toda a cadeia de fornecedores e a organização de usuários finais devem estar envolvidas na proteção de uma rede, seus dispositivos e os serviços aos quais ela oferece suporte. Um ambiente seguro depende dos usuários, processos e tecnologia. A finalidade deste guia é ajudar você a manter sua rede e seus dispositivos e serviços protegidos.

As ameaças mais óbvias a um dispositivo Axis são sabotagem física, vandalismo e violações. Para proteger um produto contra essas ameaças, é importante selecionar um modelo ou caixa resistente a vandalismo, montá-lo da maneira recomendada e proteger os cabos.

Os dispositivos Axis são endpoints de rede, assim como computadores e telefones celulares. Muitos deles possuem uma interface Web que pode expor vulnerabilidades a sistemas conectados. Neste guia, explicamos como é possível reduzir esses riscos.

O guia fornece conselhos técnicos para todos os envolvidos na implantação de soluções Axis. Ele inclui uma configuração básica recomendada, bem como um guia de fortalecimento que considera o cenário de ameaças em evolução. Talvez seja necessário consultar o manual do usuário do produto para saber como ajustar configurações específicas. Observe que os dispositivos Axis receberam uma atualização da interface Web dos AXIS OS 7.10 e 10.9, o que alterou o caminho da configuração.

Configuração via interface Web
O guia se refere ao ajuste de configurações de dispositivos na interface Web do dispositivo Axis. O caminho de configuração difere de acordo com a versão do AXIS OS instalada no dispositivo:

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Security > IEEE 802.1X (Configurações > Opções do sistema > Segurança > IEEE 802.1X)
≥ 7.10	Settings > System > Security (Configurações > Sistema > Segurança)
≥ 10.9	System > Security (Sistema > Segurança)

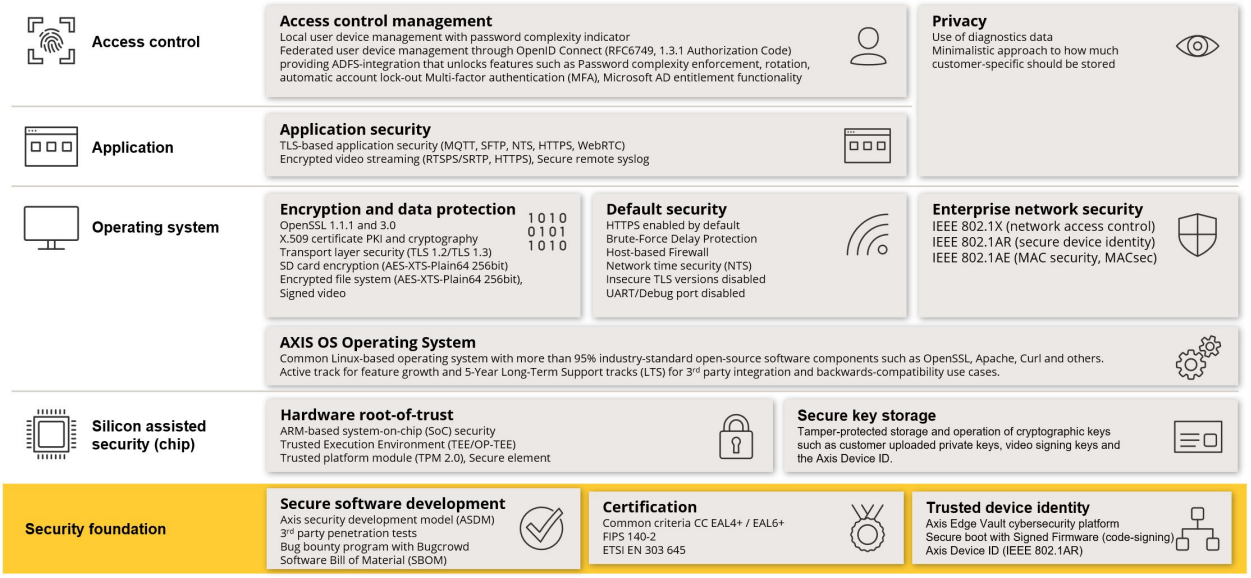
Escopo

Este guia se aplica a todos os produtos baseados em AXIS OS que executam o AXIS OS (LTS ou trilha ativa), bem como a produtos antigos que executam as versões 4.xx e 5.xx.

Introdução

Arquitetura de segurança do AXIS OS

O diagrama de Arquitetura de segurança do AXIS OS mostra os recursos de segurança cibernética do AXIS OS em várias camadas, oferecendo uma visão abrangente dos fundamentos de segurança, segurança assistida por hardware, sistema operacional AXIS OS e camadas de aplicativos e controle de acesso.



Clique com o botão direito e abra a imagem em uma nova guia para usufruir de uma experiência visual melhor.

Notificações de segurança

Recomendamos assinar o *serviço de notificação de segurança da Axis* para receber informações sobre vulnerabilidades recém-descobertas em produtos, soluções e serviços Axis e para obter informações sobre como manter seus dispositivos Axis seguros.

Níveis de proteção CIS

Seguimos os métodos descritos nos Controles do Center for Internet Safety (CIS) Versão 8 para estruturar nossas recomendações de estrutura de segurança cibernética. Os Controles CIS, anteriormente conhecidos como SANS Top 20 Critical Security Controls, fornecem 18 categorias de Controles de Segurança Críticos (CSC) focados no tratamento das categorias de risco de segurança cibernética mais comuns em uma organização.

Este guia se refere aos Controles de Segurança Críticos por meio da adição do número CSC (**CSC #**) para cada tópico de fortalecimento. Para obter mais informações sobre as categorias de CSC, consulte os *18 Controles de Segurança Críticos CIS* em cisecurity.org.

Proteção padrão

Proteção padrão

Os dispositivos Axis são fornecidos com configurações de proteção padrão. Há vários controles de segurança que não precisam ser configurados por você. Esses controles fornecem um nível básico de proteção de dispositivos e servem como base para um fortalecimento mais extenso.

Desativado por padrão

CSC #4: Configuração segura de ativos corporativos e software

O dispositivo Axis não funcionará até que a senha do administrador seja definida.

Para saber como configurar o acesso a dispositivos, consulte *Acesso de dispositivos* na Base de conhecimento do AXIS OS.

Acesso por meio de credencial

Após a configuração da senha de administrador, o acesso às funções de administrador e/ou streams de vídeo só é possível via autenticação de credenciais válidas de nome de usuário e senha. Não recomendamos usar recursos que permitam acesso não autorizado, como exibição anônima e modo sempre multicast.

Protocolos de rede

CSC #4: Configuração segura de ativos corporativos e software

Somente um número mínimo de protocolos e serviços de rede são ativados por padrão nos dispositivos Axis. Nesta tabela, é possível ver quais são eles.

Protocolo	Porta	Transporte	Comentários
HTTP	80	TCP	Tráfego HTTP geral, como acesso a interface Web, interface API VAPIX e ONVIF ou comunicação edge-to-edge*
HTTPS	443	TCP	Tráfego HTTPS geral, como acesso a interface Web, interface API VAPIX e ONVIF ou comunicação edge-to-edge*
RTSP	554	UDP	Usado pelo dispositivo Axis para streaming de vídeo/áudio
RTP	Faixa de portas efêmeras*	UDP	Usado pelo dispositivo Axis para streaming de vídeo/áudio
UPnP	49152	TCP	Usado por aplicativos de terceiros para descobrir o dispositivo Axis via protocolo de detecção UPnP
Bonjour	5353	UDP	Usado por aplicativos de terceiros para descobrir o dispositivo Axis via protocolo de detecção mDNS (Bonjour)

Proteção padrão

Protocolo	Porta	Transporte	Comentários
SSDP	1900	UDP	Usado por aplicativos de terceiros para descobrir o dispositivo Axis via SSDP (UPnP)
WS-Discovery	3702	UDP	Usado por aplicativos de terceiros para descobrir o dispositivo Axis via protocolo de detecção WS-Discovery (ONVIF)

** Para obter mais informações sobre edge-to-edge, consulte o white paper Tecnologia edge-to-edge.*

** *Alocado automaticamente dentro de uma faixa predefinida de números de porta de acordo com a RFC 6056. Para obter mais informações, consulte o artigo Porta efêmera* na Wikipedia.

Recomendamos desativar protocolos e serviços de rede não utilizados sempre que possível. Para obter uma lista completa dos serviços que são usados por padrão ou que podem ser ativados com base na configuração, consulte *Portas de rede comumente usadas* na Base de conhecimento do AXIS OS.

Por exemplo, é necessário ativar manualmente a funcionalidade de entrada/saída de áudio e microfone em produtos de videomonitoramento Axis, como câmeras de rede. Já nos intercomunicadores e alto-falantes de rede Axis, a entrada/saída de áudio e a funcionalidade de microfone são recursos principais e, portanto, são ativados por padrão.

Interface UART/Debug

CSC #4: Configuração segura de ativos corporativos e software

Cada dispositivo Axis é fornecido com uma interface UART (Universal Asynchronous Receiver Transmitter) física, algumas vezes conhecida como "porta de depuração" ou "console serial". A interface em si só pode ser acessada fisicamente por meio do desmonte extensivo do dispositivo Axis. A interface UART/debug é usada apenas para fins de desenvolvimento e depuração de produtos durante projetos internos de engenharia de P&D dentro da Axis.

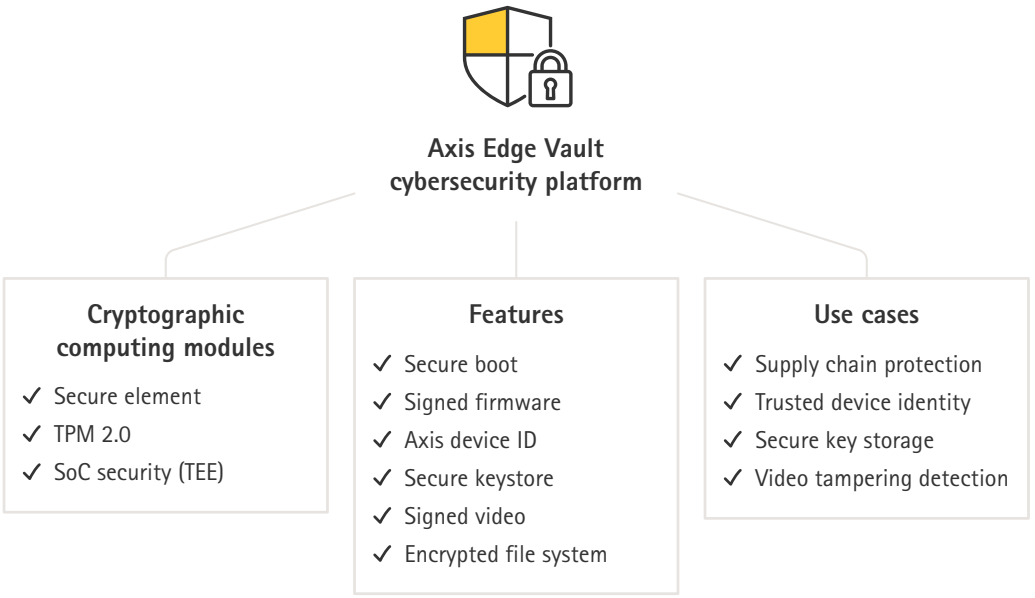
A interface UART/debug é ativada por padrão em dispositivos Axis com o AXIS OS 10.10 e versões anteriores, mas requer acesso autenticado e não expõe nenhuma informação sensível sem exigir autenticação. A partir do AXIS OS 10.11, a interface UART/depuração é desativada por padrão. A única forma de ativar a interface é destravando-a por meio de um certificado personalizado exclusivo do dispositivo fornecido pela Axis.

Axis Edge Vault

O AXIS Edge Vault oferece uma plataforma segurança cibernética baseada em hardware que protege os dispositivos Axis. Ele foi desenvolvido sobre uma base sólida de módulos de computação criptografados (elemento seguro e TPM) e na segurança de SoC (TEE e inicialização segura), combinada com a experiência em segurança de dispositivos de borda. O Axis Edge Vault baseia-se em uma raiz de confiança sólida estabelecida pela inicialização segura e pelo firmware assinado. Esses recursos criam uma cadeia inquebrável de software criptografado criptograficamente para a cadeia de confiança de que todas as operações seguras dependem.

Os dispositivos Axis com o Axis Edge Vault minimizam a exposição de clientes a riscos de segurança cibernética, evitando escutas e extração mal-intencionada de informações confidenciais. O Axis Edge Vault também garante que o dispositivo Axis seja uma unidade confiável e confiável na rede do cliente.

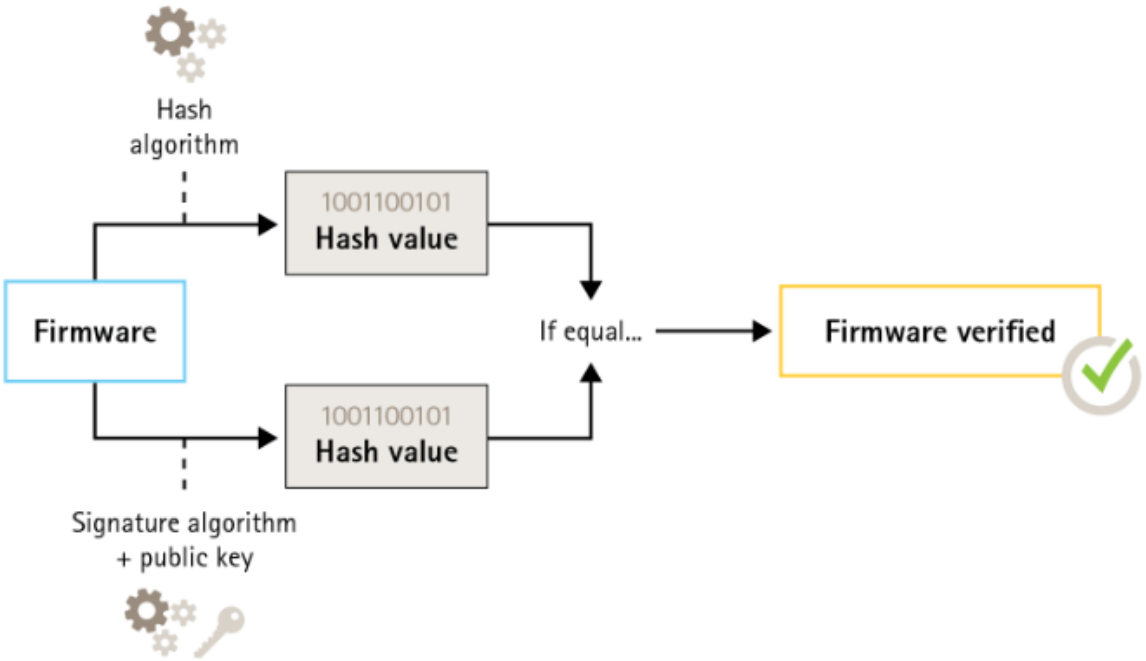
Proteção padrão



Firmware assinado

CSC #2: Inventário e controle de ativos de software

O AXIS OS é assinado a partir da versão 9.20.1. Sempre que você atualizar a versão do AXIS OS no dispositivo, o dispositivo verificará a integridade dos arquivos de atualização via verificação de assinaturas criptográficas e rejeitará qualquer arquivos adulterados. Isso impedira que invasores enganem os usuários para fazê-los instalar arquivos comprometidos.



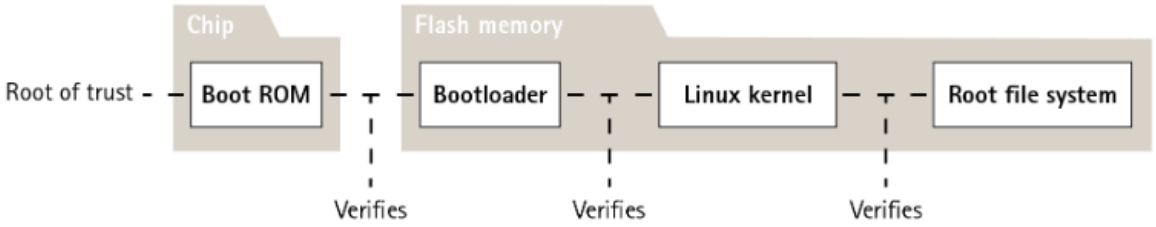
Proteção padrão

Para obter mais informações, consulte o white paper em *Axis Edge Vault*.

Inicialização segura

CSC #2: Inventário e controle de ativos de software

A maioria dos dispositivos Axis possui uma sequência de inicialização segura para proteger a integridade do dispositivo. A inicialização segura impede que você implante dispositivos Axis que foram adulterados.

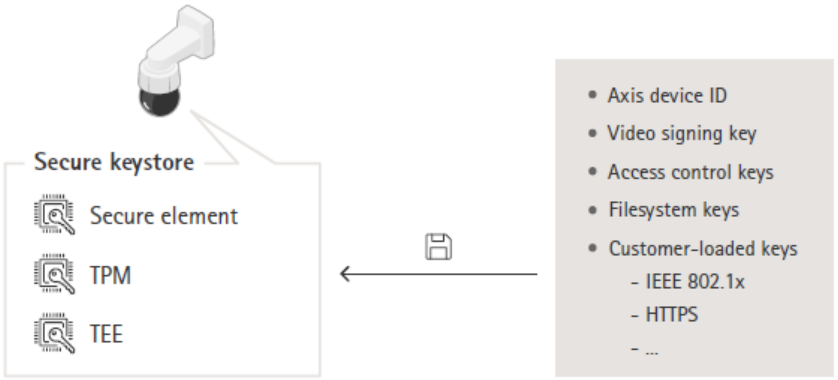


Para obter mais informações, consulte o white paper em *Axis Edge Vault*.

Armazenamento de chaves seguro

CSC #6: Gerenciamento de controle de acesso

O armazenamento de chaves seguro fornece armazenamento baseado em hardware protegido contra violações de informações criptográficas. Ele protege o ID de dispositivo Axis, bem como informações de criptografia carregadas pelo cliente, além de impedir acesso não autorizado e extração mal-intencionada em caso de violação de segurança. Dependendo dos requisitos de segurança, um dispositivo Axis pode ter um ou vários módulos, como um TPM 2,0 (Trusted Platform Module) ou um elemento seguro, e/ou um ambiente de execução confiável (TEE).



Para obter mais informações, consulte o white paper em *Axis Edge Vault*.

Sistema de arquivos criptografado

CSC #3: Proteção de dados

Um adversário mal-intencionado poderia tentar extrair informações do sistema de arquivos desmontando a memória flash e acessando-a através de um dispositivo de leitor de flash. No entanto, o dispositivo Axis pode proteger o sistema de arquivos contra exfiltração de dados mal-intencionada e violação de configuração em caso de alguém obter acesso físico ou roubá-lo. Quando o dispositivo Axis é desligado, as informações no sistema de arquivos são criptografadas em AES-XTS-Plain64 de 256 bits. Durante

o processo de inicialização segura, o sistema de arquivos de leitura/gravação é descriptografado e pode ser montado e usado pelo dispositivo Axis.

Para obter mais informações, consulte o white paper em *Axis Edge Vault*.

HTTPS ativado

CSC #3: Proteção de dados

Começando no AXIS OS 7.20, o HTTPS foi ativado por padrão com um certificado autoassinado que permite configurar a senha do dispositivo de forma segura. A partir do AXIS OS 10.10, o certificado autoassinado foi substituído pelo certificado de ID de dispositivo seguro IEEE 802.1AR.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Security > HTTPS (Configuração > Opções do sistema > Segurança > HTTPS)
≥ 7.10	Settings > System > Security > HTTP and HTTPS (Configurações > Sistema > Segurança HTTP e HTTPS)
≥ 10.9	System > Network > HTTP and HTTPS (Sistema > Rede > HTTP e HTTPS)

Cabeçalhos de HTTP(S) padrão

O AXIS OS possui os cabeçalhos de HTTPs mais comuns relacionados à segurança ativados por padrão para melhorar o nível base de segurança cibernética no estado padrão de fábrica. A partir do AXIS OS 9.80, você pode usar a API de cabeçalho HTTP personalizada VAPIX para configurar cabeçalhos de HTTPs adicionais.

Para obter mais informações sobre a API VAPIX de cabeçalho HTTP, consulte a *Biblioteca VAPIX*.

Para ler mais sobre cabeçalhos HTTP(S) padrão, consulte *Cabeçalhos HTTP(S) padrão* na Base de conhecimento do AXIS OS.

Autenticação Digest

CSC #3: Proteção de dados

Os clientes que acessam o dispositivo autenticarão com uma senha que deve ser criptografada quando enviada pela rede. Por isso, recomendamos usar somente a autenticação Digest em vez de Básica ou Básica e Digest. Isso reduz o risco de sniffers de rede obterem a senha.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Advanced > Plain Config > Network > Network HTTP Authentication policy (Configuração > Opções do sistema > Avançado > Configuração simples > Rede > Política de autenticação HTTP da rede)
≥ 7.10	Settings > System > Plain config > Network > Network HTTP Authentication policy (Configurações > Sistema > Configuração simples > Rede > Politica de autenticação HTTP da rede)
≥ 10.9	System > Plain config > Network > Network HTTP Authentication policy (Sistema > Configuração simples > Rede > Politica de autenticação HTTP da rede)

Proteção padrão

Proteção contra ataque de reprodução ONVIF

CSC #3: Proteção de dados

A proteção contra ataque de reprodução é um recurso de segurança ativado por padrão em dispositivos Axis. Seu objetivo é proteger suficientemente a autenticação do usuário baseada em ONVIF com o acréscimo de um cabeçalho de segurança adicional que inclui token de nome de usuário, marca de data e hora válida, nonce e digest de senha. O digest da senha é calculado a partir da senha (que já está armazenada no sistema), nonce e marca de data e hora. A finalidade do digest da senha é validar o usuário e evitar ataques de reprodução. Por isso, os digests são armazenados em cache. Recomendamos manter essa configuração ativada.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Advanced > Plain Config > System > Enable Replay Attack Protection (Configuração > Opções do sistema > Avançado > Configuração simples > Sistema > Ativar proteção contra ataques de repetição)
≥ 7.10	Configurações > Sistema > Configuração simples > Serviço Web > Ativar proteção contra ataques de reprodução)
≥ 10.9	System > Plain config > WebService > Enable Replay Attack Protection (Sistema > Configuração simples > Serviço Web > Ativar proteção contra ataques de reprodução)

Impedir ataques de força bruta

CSC #4: Configuração segura de ativos e software corporativos
CSC #13: Monitoramento e defesa da rede

Os dispositivos Axis possuem um mecanismo de prevenção para identificar e bloquear ataques de força bruta provenientes da rede, por exemplo, ataques de adivinhação de senhas. O recurso, chamado de *proteção contra atrasos de força bruta*, está disponível no AXIS OS 7.30 e posterior.

A proteção contra atraso de força bruta é ativada por padrão a partir do AXIS OS 11.5. Para obter exemplos e recomendações detalhados de configuração, consulte *Proteção contra atrasos de força bruta* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > System > PreventDosAttack (Configurações > Sistema > Configuração simples > Sistema > Prevenir ataque de DoS
≥ 10.9	System > Security > Prevent brute-force attacks (Sistema > Segurança > Prevenir ataques de força bruta)

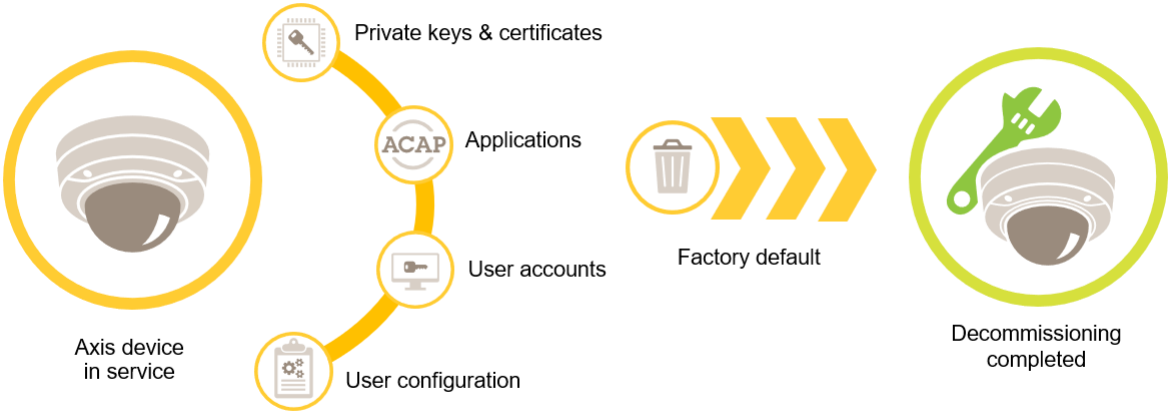
Descomissionamento

CSC #3: Proteção de dados

Ao descomissionar um dispositivo Axis, recomendamos redefinir o dispositivo para as configurações padrão de fábrica, o que apagará todos dados no dispositivo por meio de sobreposição/sanitização.

Os dispositivos Axis usam memória volátil e não volátil e, embora a memória volátil seja apagada sempre que o dispositivo é desligado da fonte de alimentação, as informações armazenadas na memória não volátil permanecem e são disponibilizadas novamente na inicialização. Evitamos a prática comumente adotada de simplesmente remover os ponteiros de dados para tornar os dados armazenados invisíveis ao sistema de arquivos. Por isso, uma redefinição de fábrica é necessária.

Proteção padrão



Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Maintenance > Default (Configuração > Opções do sistema > Manutenção > Padrão).
≥ 7.10	Settings > System > Maintenance > Default (Configurações > Sistema > Manutenção > Padrão).
≥ 10.9	Maintenance > Default (Manutenção > Padrão)

Esta tabela contém mais informações sobre dados armazenados na memória não volátil.

Informações e dados	**Apagados após redefinição para configurações padrão de fábrica**
Nomes de usuário e senhas VAPIX e ONVIF	Sim
Certificados e chaves privadas	Sim
Certificado autoassinado	Sim
Informações armazenadas no TPM e Axis Edge Vault	Sim
Configurações de WLAN e usuários/senhas	Sim
Certificados personalizados*	Não
Chave de criptografia de cartões SD	Sim
Dados de cartões SD**	Não
Configurações de compartilhamento de rede e usuários/senhas	Sim
Dados de compartilhamento de rede**	Não
Configuração do usuário***	Sim
Aplicativos carregados (ACAPs)****	Sim
Dados de produção e estatísticas de vida útil*****	Não
Gráficos e sobreposições carregados	Sim
Dados do relógio RTC	Sim

Proteção padrão

** O processo de firmware assinado usa certificados personalizados que permitem que os usuários carreguem (entre outras coisas) o AXIS OS.*
*** Gravações e imagens existentes no armazenamento de borda (cartão SD, compartilhamento de rede) devem ser excluídas pelo usuário separadamente. Para obter mais informações, consulte Formatação de cartões SD Axis* na Base de conhecimento do AXIS OS.
**** Todas as configurações feitas pelo usuário, da criação de contas à rede, O3C, eventos, imagem, PTZ e configurações do sistema.*
***** O dispositivo retém qualquer aplicativo pré-instalado, mas exclui todas as configurações feitas pelo usuário a eles*
****** Os dados de produção (calibração, certificados de produção 802.1AR) e as estatísticas de vida útil incluem informações não sensíveis e não relacionadas ao usuário.*

Fortalecimento básico

Fortalecimento básico

O fortalecimento básico é o nível mínimo de proteção recomendado para dispositivos Axis. Os tópicos do fortalecimento básico são "configuráveis na borda". Isso significa que eles podem ser configurados diretamente no dispositivo Axis sem dependências adicionais de infraestrutura de rede, vídeo ou sistemas de gerenciamento de evidências (VMS, EMS), equipamentos ou aplicações de terceiros.

Configurações padrão de fábrica

CSC #4: Configuração segura de ativos corporativos e software

Antes de configurar o dispositivo, certifique-se de que ele esteja em um estado padrão de fábrica. Também é importante redefinir o dispositivo para as configurações padrão de fábrica quando é necessário remover dados do usuário ou descomissioná-lo. Para obter mais informações, consulte *Descomissionamento na página 9*.

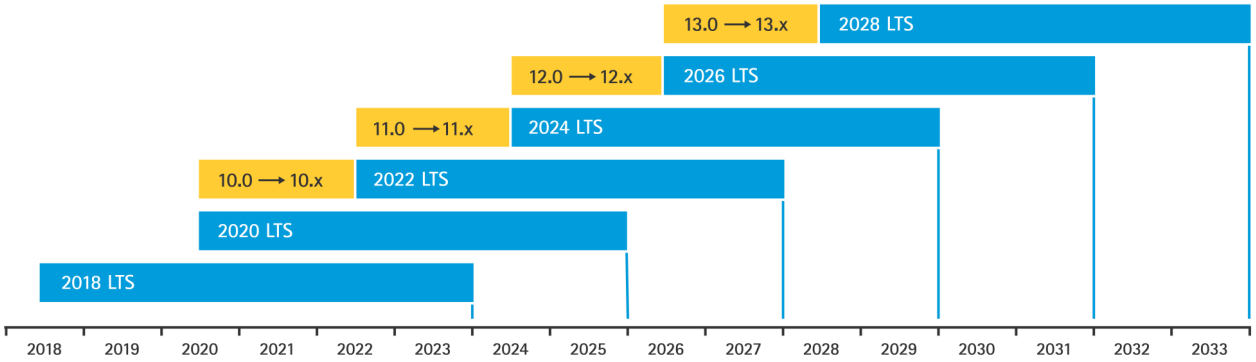
Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Maintenance > Default (Configuração > Opções do sistema > Manutenção > Padrão).
≥ 7.10	Settings > System > Maintenance > Default (Configurações > Sistema > Manutenção > Padrão).
≥ 10.9	Maintenance > Default (Manutenção > Padrão)

Atualizar para o AXIS OS mais recente

CSC #2: Inventário e controle de ativos de software

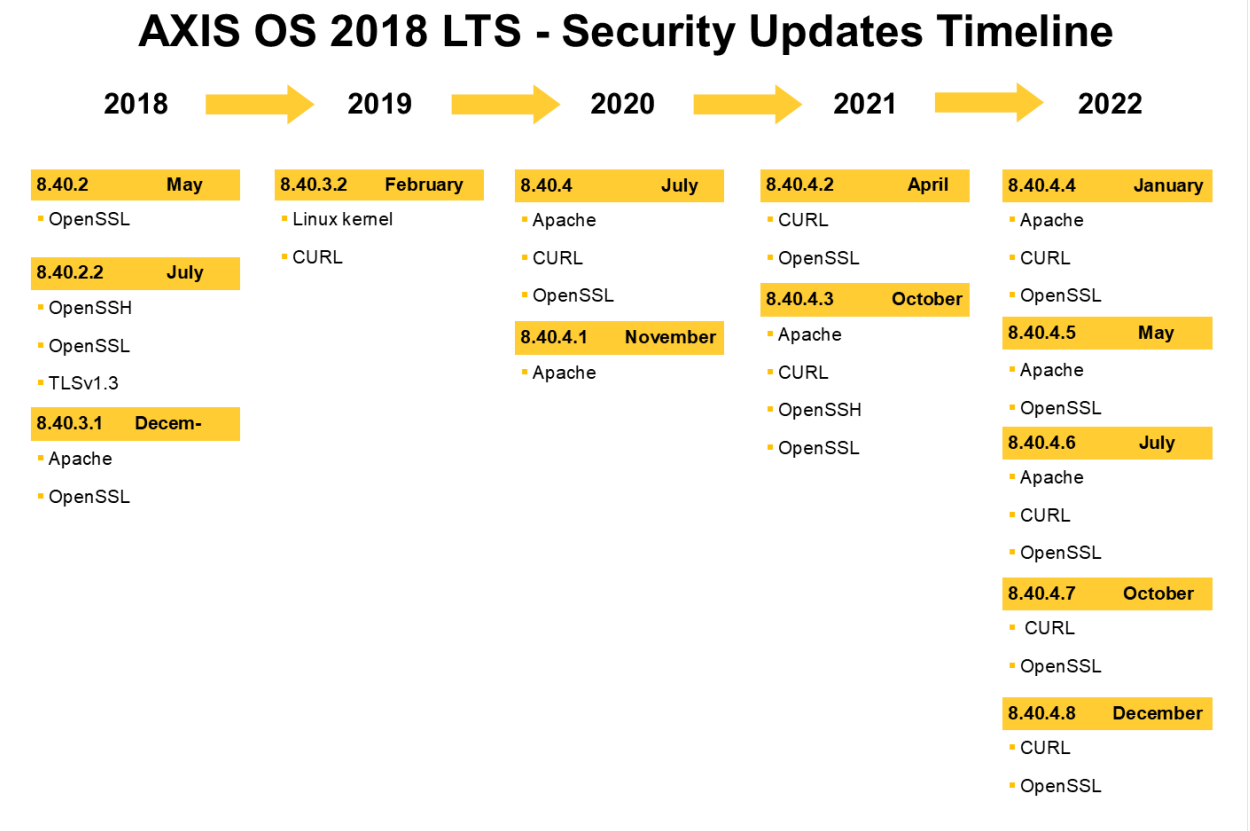
Aplicar patches em software é um aspecto importante da segurança cibernética. Os agressores muitas vezes tentarão explorar vulnerabilidades comumente conhecidas e poderão ter sucesso se obtiverem acesso de rede a um serviço sem patch. Certifique-se de usar sempre o AXIS OS mais recente, pois ele pode incluir patches de segurança para vulnerabilidades conhecidas. As notas de versão de uma versão específica podem mencionar explicitamente uma correção de segurança crítica, mas nem todas as correções gerais.

A Axis mantém dois tipos de trilhas do AXIS OS: A trilha ativa e a trilha de suporte de longo prazo (LTS). Embora ambos os tipos incluam os patches de vulnerabilidade críticos mais recentes, as trilhas LTS não incluem recursos novos, pois o objetivo é minimizar o risco de problemas de compatibilidade. Para obter mais informações, consulte *o ciclo de vida do AXIS OS* nas Informações do AXIS OS.



A Axis fornece uma previsão para as próximas versões com informações sobre novos recursos importantes, correções de bugs e patches de segurança. Para saber mais, consulte *Próximas versões* nas Informações do AXIS OS. Visite *Firmware* em axis.com para baixar o AXIS OS para seu dispositivo.

Este gráfico ilustra a importância de manter os dispositivos Axis atualizados.



Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Maintenance > Upgrade Server (Configuração > Opções do sistema > Manutenção > Atualização do servidor
≥ 7.10	Settings > System > Maintenance > Firmware upgrade (Configurações > Sistema > Manutenção > Atualização de firmware)
≥ 10.9	Maintenance > Firmware upgrade (Manutenção > Atualização de firmware)

Definir senha de root do dispositivo

CSC #4: Configuração segura de ativos e software corporativos
CSC #5: Gerenciamento de contas

A conta root do dispositivo é a principal conta de administração do dispositivo. Para usar a conta root, é necessário definir uma senha de dispositivo. Certifique-se de usar uma senha forte e limitar o uso da conta root somente a tarefas de administração. Não recomendamos usar a conta root na produção diária.

Ao operar dispositivos Axis, usar a mesma senha simplifica o gerenciamento, mas aumenta sua vulnerabilidade a violações e vazamentos de dados. Usar senhas exclusivas para cada dispositivo Axis proporciona alta segurança, mas torna o gerenciamento de dispositivos mais complexo. Recomendamos alterar regularmente a senha em seus dispositivos.

Fortalecimento básico

Recomendamos implementar diretrizes que exijam que as novas senhas sejam suficientemente longas e complexas, por exemplo, as *recomendações de senhas do NIST*. Os dispositivos Axis oferecem suporte a senhas com até 64 caracteres. Senhas com **menos de 8 caracteres** são consideradas fracas.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > Basic Setup > Users (Configuração > Configuração básica > Usuários)
≥ 7.10	Settings > System > Users (Configurações > Sistema > Usuários)
≥ 10.9	System > Users (Sistema > Usuários)
≥ 11.6	System > Accounts (Sistema > Contas)

Criar contas dedicadas

CSC #4: Configuração segura de ativos e software corporativos
CSC #5: Gerenciamento de contas

A conta root padrão possui todos os privilégios e deve ser reservada para tarefas administrativas. Recomendamos criar uma conta de usuário cliente com privilégios limitados para operação diária. Isso reduz o risco de comprometer a senha do administrador do dispositivo.

Para obter mais informações, consulte o white paper *Identidade e gerenciamento de acesso em sistemas de videomonitoramento*.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > Basic Setup > Users (Configuração > Configuração básica > Usuários)
≥ 7.10	Settings > System > Users (Configurações > Sistema > Usuários)
≥ 10.9	System > Users (Sistema > Usuários)
≥ 11.6	System > Accounts (Sistema > Contas)

Limitar o acesso à interface Web

CSC #5: Gerenciamento de contas

Os dispositivos Axis têm um servidor Web que permite que os usuários acessem o dispositivo por meio de um navegador da Web padrão. A interface Web destina-se a configuração, manutenção e solução de problemas. Ele não deve ser usada nas operações diárias, por exemplo, como um cliente para exibir vídeo.

Os únicos clientes que devem poder interagir com dispositivos Axis durante as operações diárias são sistemas de gerenciamento de vídeo (VMS) ou ferramentas de administração e gerenciamento de dispositivos, como o AXIS Device Manager. Os usuários do sistema nunca devem ter permissão para acessar os dispositivos Axis diretamente. Para obter mais informações, consulte *Desativar o acesso à interface Web na página 14*.

Desativar o acesso à interface Web

CSC #4: Configuração segura de ativos corporativos e software

A partir do AXIS OS 9.50, é possível desativar a interface Web de um dispositivo Axis. Após implantar um dispositivo Axis em um sistema (ou adicioná-lo ao AXIS Device Manager), recomendamos remover a opção que permite que pessoas da organização acessem o dispositivo via navegador da Web. Isso cria uma camada adicional de segurança se a senha da conta do dispositivo for compartilhada dentro da organização. A opção mais segura é configurar o acesso a dispositivos Axis para ser feito exclusivamente por meio de aplicativos dedicados que oferecem arquitetura avançada de gerenciamento de acesso a identidade (IAM), mais rastreabilidade e proteções para evitar vazamentos de contas.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > System > Web Interface Disabled (Configurações > Sistema > Configuração simples > Sistema > Interface Web desativada)
≥ 10.9	System > Plain config > System > Web Interface Disabled (Sistema > Configuração simples > Sistema > Interface Web desativada)

Configurar as opções de rede

CSC #12: Gerenciamento da infraestrutura de rede

A configuração de IP do dispositivo depende da configuração de rede, como IPv4/IPv6, endereço de rede estático ou dinâmico (DHCP), máscara de sub-rede e roteador padrão. Recomendamos revisar sua topologia de rede sempre que adicionar novos tipos de componentes.

Recomendamos também usar a configuração de endereços IP estáticos em seus dispositivos Axis para garantir a comunicação da rede e desembaraçar a dependência de servidores na rede (como servidores DHCP) que podem ser alvos de ataques.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > Basic Setup > TCP/IP (Configuração > Configuração básica > TCP/IP)
≥ 7.10	Settings > System > TCP/IP (Configurações > Sistema > TCP/IP)
≥ 10.9	System > Network (Sistema > Rede)

Configurar as opções de data e hora

CSC #8: Gerenciamento de logs de auditoria

Do ponto de vista da segurança, é importante definir a data e a hora corretas. Isso garante, por exemplo, que os logs do sistema sejam marcados corretamente e que os certificados digitais possam ser validados e usados em tempo de execução. Sem a sincronização adequada da hora, os serviços que dependem de certificados digitais, como HTTPS, IEEE e 802.1x, podem não funcionar corretamente.

Recomendamos manter o relógio do dispositivo Axis sincronizado com servidores de Network Time Protocol (NTP, não criptografado) ou, preferencialmente, servidores de Network Time Security (NTS, criptografado). O Network Time Security (NTS), uma versão criptografada e segura do Network Time Protocol (NTP), foi adicionada ao AXIS OS 11.1. Recomendamos configurar vários servidores de hora para garantir uma maior precisão de sincronização, mas também para criar um cenário de failover em que um dos servidores de hora configurados pode não estar disponível.

Usar servidores NTP ou NTS públicos pode ser uma alternativa para indivíduos e pequenas organizações que não podem disponibilizar instâncias locais do servidor de hora por conta própria. Para obter mais informações sobre NTP/NTS em dispositivos Axis, consulte *NTP e NTS* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > Basic Setup > Date & Time (Configuração > Configuração básica > Data e hora)
≥ 7.10	Settings > System > Date and time (Configurações > Sistema > Data e hora)
≥ 10.9	Settings > Date and time (Configurações > Data e hora)
≥ 11.6	System > Time and location (Sistema > Hora e localização)

Fortalecimento básico

Criptografia de armazenamento na borda

CSC #3: Proteção de dados

Cartão SD
Se o dispositivo Axis oferecer suporte e usar cartões Secure Digital (SD) para armazenar gravações de vídeo, recomendamos aplicar criptografia. Isso impedirá que indivíduos não autorizados possam reproduzir o vídeo armazenado de um cartão SD removido.

Para saber mais sobre criptografia de cartão SD nos dispositivos Axis, consulte *Suporte a cartões SD* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Storage (Configuração > Opções do sistema > Armazenamento)
≥ 7.10	Settings > System > Storage (Configurações > Sistema > Armazenamento)
≥ 10.9	System > Storage (Sistema > Armazenamento)

Compartilhamento de rede (NAS)
Se você usa um armazenamento de rede (NAS) como dispositivo de gravação, recomendamos mantê-lo em uma área bloqueada com acesso limitado e ativar a criptografia de disco rígido. Os dispositivos Axis utilizam o SMB como protocolo de rede para conectar a um NAS para armazenar gravações de vídeo. Embora versões anteriores de SMB (1.0 e 2.0) não forneçam segurança ou criptografia, versões posteriores (2.1 e posterior) o fazem. Por isso, recomendamos usar versões posteriores durante a produção.

Para saber mais sobre configurações SMB adequadas ao conectar um dispositivo Axis a um compartilhamento de rede, consulte *Compartilhamento de rede* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Storage (Configuração > Opções do sistema > Armazenamento)
≥ 7.10	Settings > System > Storage (Configurações > Sistema > Armazenamento)
≥ 10.9	System > Storage (Sistema > Armazenamento)

Exportar criptografia de gravação

CSC #3: Proteção de dados

A partir do AXIS OS 10.10, os dispositivos Axis oferecem suporte à exportação criptografada de gravações na borda. Recomendamos usar esse recurso, pois ele impede que indivíduos não autorizados possam reproduzir material de vídeo exportado.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	N/A
≥ 7.10	N/A
≥ 10.9	Gravações

Aplicativos (ACAPs)

CSC #4: Configuração segura de ativos corporativos e software

Você pode carregar aplicativos no dispositivo Axis para estender sua funcionalidade. Muitos deles oferecem sua própria interface do usuário para interagir com determinado recurso. Os aplicativos podem usar a funcionalidade de segurança fornecida pelo AXIS OS.

Os dispositivos Axis são pré-carregados com vários aplicativos desenvolvidos pela Axis de acordo com o *modelo de desenvolvimento de segurança da Axis (ASDM)*. Para obter mais informações sobre aplicativos Axis, consulte *Análise* em axis.com.

Para aplicativos de terceiros, recomendamos entrar em contato com o fornecedor para obter pontos de prova sobre a segurança do aplicativo em termos de operação e teste e se ele foi desenvolvido de acordo com modelos de desenvolvimento de segurança de práticas recomendadas comuns. As vulnerabilidades encontradas em aplicativos de terceiros devem ser relatadas diretamente ao fornecedor terceirizado.

Recomendamos executar somente aplicativos confiáveis e remover dos dispositivos Axis quaisquer aplicativos não utilizados.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > Applications (Configuração > Aplicativos)
≥ 7.10	Settings > Apps (Configurações > Aplicativos)
≥ 10.9	Apps

Desativar serviços/funções não utilizados

CSC #4: Configuração segura de ativos corporativos e software

Embora serviços e funções não usados não sejam uma ameaça imediata à segurança, é uma boa prática desativar serviços e funções não utilizados para reduzir riscos desnecessários. Continue lendo para saber mais sobre serviços e funções que você poderá desativar se eles não estiverem sendo usados.

Portas de rede físicas não utilizadas

A partir do AXIS OS 11.2, dispositivos com várias portas de rede, como o AXIS S3008, têm a opção de desativar o tráfego de rede e PoE de suas portas de rede. Deixar portas de rede não utilizadas sem supervisão e ativas representa um grave risco à segurança.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	N/A
≥ 7.10	N/A
≥ 11.2	System > Power over Ethernet (Sistema > Power over Ethernet)

Protocolos de detecção de rede

Os protocolos de detecção, como Bonjour, UPnP, ZeroConf e WS-Discovery, são serviços de suporte que facilitam encontrar o dispositivo Axis e seus serviços na rede. Depois de implantar o dispositivo e adicioná-lo ao VMS, recomendamos desativar o protocolo de detecção para impedir que o dispositivo Axis anuncie sua presença na rede.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Advanced > Plain Config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled* (Configuração > Opções do sistema > Avançado > Configuração simples > Rede > Bonjour de rede ativado, UPnP de rede ativado, Configuração zero de rede ativada, NAT Traversal UPnP de rede ativada)
	N/A

Versão do AXIS OS	Caminho de configuração da interface Web
≥ 7.10	Settings > System > Plain Config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled* (Configurações > Sistema > Configuração simples > Rede > Bonjour de rede ativado, UPnP de rede ativado, Configuração zero de rede ativada, NAT Traversal UPnP de rede ativada)
	Settings > System > Plain config > WebService > Discovery Mode (Configurações > Sistema > Configuração plana > Serviço Web > Modo de detecção)
≥ 10.9	Settings > Plain config > Network > Bonjour Enabled, UPnP Enabled, ZeroConf Enabled (Configurações > Configuração simples > Rede > Bonjour ativado, UPnP ativado, Configuração zero ativada)
	System > Plain config > WebService > DiscoveryMode > Enable WS-Discovery discoverable mode (Sistema > Configuração simples > Serviço Web > Modo de detecção > Ativar modo de descoberta WS-Discovery)

** A funcionalidade foi removida no AXIS OS 10.12 e não está disponível nas versões posteriores.*

Versões de TLS desatualizadas

Recomendamos desativar versões de TLS antigas, desatualizadas e inseguras antes de colocar seu dispositivo Axis em produção. As versões de TLS desatualizadas normalmente são desativadas por padrão, mas é possível habilitá-las em dispositivos Axis para oferecer compatibilidade reversa com aplicativos de terceiros que ainda não implementaram TLS 1.2 e TLS 1.3.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Advanced > Plain Config > HTTPS > Allow TLSv1.0 *e/ou* Allow TLSv1.1 (Configuração > Opções do sistema > Avançado > Configuração simples > HTTPS > Permitir TLSv1.0 e/ou Allow TLSv1.1)
≥ 7.10	Settings > System > Plain config > HTTPS > Allow TLSv1.0 *e/ou* Allow TLSv1.1 (Configurações > Sistema > Configuração simples > HTTPS > Permitir TLSv1.0 e/ou Permitir TLSv1.1)
≥ 10.9	System > Plain config > HTTPS > Allow TLSv1.0 *e/ou* Allow TLSv1.1 Sistema > Configuração simples > HTTPS > Permitir TLSv1.0 e/ou Permitir TLSv1.1)

Ambiente do editor de scripts

Recomendamos desativar o acesso ao ambiente do editor de scripts. O editor de scripts é usado somente para fins de solução de problemas e depuração.

O editor de scripts foi removido do AXIS OS 10.11 e não está disponível nas versões posteriores.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > System > Enable the script editor (editcgi) (Configurações > Sistema > Configuração simples > Sistema > Ativar o editor de scripts (editcgi))
≥ 10.9	System > Plain config > System > Enable the script editor (editcgi) (Sistema > Configuração simples > Sistema > Ativar o editor de scripts (editcgi))

Cabeçalhos do servidor HTTP(S)

Por padrão, os dispositivos Axis anunciam suas versões de Apache e OpenSSL atuais durante as conexões HTTP(S) com clientes na rede. Essas informações são úteis quando você usa scanners de segurança de rede regularmente, pois fornece um relatório mais detalhado de vulnerabilidades pendentes em uma versão específica do AXIS OS.

É possível desativar os cabeçalhos do servidor HTTP(S) para reduzir a exposição de informações durante conexões HTTPs. No entanto, recomendamos desativar os cabeçalhos somente se você operar seu dispositivo de acordo com nossas recomendações e mantê-lo sempre atualizado.

A opção de desativar os cabeçalhos de servidor HTTP(S) está disponível a partir do AXIS OS 10.6.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > System > HTTP Server Header Comments (Configurações > Sistema > Configuração simples > Sistema > Comentários do cabeçalho do servidor HTTP)
≥ 10.9	System > Plain config > System > HTTP Server Header Comments (Sistema > Configuração simples > Sistema > Comentários do cabeçalho do servidor HTTP)

Áudio

Em produtos orientados para vigilância por vídeo Axis, como câmeras de rede, a funcionalidade de entrada/saída de áudio e microfone é desativada por padrão. Se você necessitar de recursos de áudio, ative-os antes de usá-los. Em produtos Axis em que a funcionalidade de entrada/saída de áudio e microfone são recursos importantes, como interfones e alto-falantes de rede Axis, os recursos de áudio são ativados por padrão.

Recomendamos desativar os recursos de áudio se você não usá-los.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Advanced > Plain Config > Audio > Audio A* > Enabled (Configuração > Opções do sistema > Avançado > Configuração simples > Áudio > Audio A* > Ativado
≥ 7.10	Settings > Audio > Allow audio (Configurações > Áudio > Permitir áudio)
≥ 10.9	Audio > Device settings (Áudio > Configurações do dispositivo).

Entradas para cartão SD

Os dispositivos Axis normalmente oferecem suporte a pelo menos um cartão SD para permitir o armazenamento de borda local das gravações de vídeo. Recomendamos desativar totalmente a entrada para cartões SD caso não utilize cartões SD. A opção de desativar a entrada para cartão SD está disponível no AXIS OS 9.80.

Para obter mais informações, consulte *Desativando o cartão SD* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	N/A
≥ 7.10	Settings > System > Plain config > Storage > SD Disk Enabled (Configurações > Sistema > Configuração simples > Armazenamento > Disco SD ativado)
≥ 10.9	System > Plain config > Storage > SD Disk Enabled (Sistema > Configuração simples > Armazenamento > Disco SD ativado)

Acesso via FTP

O FTP é um protocolo de comunicação inseguro usado somente para fins de solução de problemas e depuração. O acesso via FTP foi removido do AXIS OS 11.1 e não está disponível nas versões posteriores. Recomendamos desativar o acesso via FTP e usar acesso SSH seguro para fins de solução de problemas.

Para obter mais informações sobre o SSH, consulte *Acesso via SSH* no Portal do Axis OS. Para obter informações sobre opções de depuração usando FTP, consulte *Acesso via FTP* no Portal do Axis OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Plain Config > Network > FTP Enabled (Configuração > Opções do sistema > Configuração simples > Rede > FTP ativado)
≥ 7.10	Settings > System > Plain config > Network > FTP Enabled (Configurações > Sistema > Configuração simples > Rede > FTP ativado)
≥ 10.9	System > Plain config > Network > FTP Enabled (Sistema > Configuração simples > Rede > FTP ativado)

Acesso via SSH

O SSH é um protocolo de comunicação seguro usado somente para fins de solução de problemas e depuração. Ele é compatível com dispositivos Axis a partir do AXIS OS 5.50. Recomendamos desativar o acesso via SSH.

Para obter mais informações sobre opções de depuração usando SSH, consulte *Acesso via SSH* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Plain Config > Network > SSH Enabled (Configuração > Opções do sistema > Configuração simples > Rede > SSH ativado)
≥ 7.10	Settings > System > Plain config > Network > SSH Enabled (Configurações > Sistema > Configuração simples > Rede > SSH ativado)
≥ 10.9	System > Plain config > Network > SSH Enabled (Sistema > Configuração simples > Rede > SSH ativado)

Acesso via Telnet

O Telnet é um protocolo de comunicação inseguro usado somente para fins de solução de problemas e depuração. Ele pode ser usado com dispositivos Axis com versões anteriores ao AXIS OS 5.50. Recomendamos desativar o acesso via Telnet.

Versão do AXIS OS	Caminho de configuração da interface Web
< 5.50	Para obter instruções, consulte *Acesso a dispositivos* na Base de conhecimento do AXIS OS.
< 7.10	N/A
≥ 7.10	N/A
≥ 10.9	N/A

ARP/Ping

ARP/Ping era um método usado para configurar o endereço IP do dispositivo Axis usando ferramentas como o AXIS IP Utility. A funcionalidade foi removida no AXIS OS 7.10 e não está disponível nas versões posteriores. Recomendamos desativar o recurso em dispositivos Axis com o AXIS OS 7.10 ou versões anteriores.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Advanced > Plain Config > Network > ARP/Ping (Configuração > Opções do sistema > Avançado > Configuração simples > Rede > ARP/Ping)
≥ 7.10	N/A
≥ 10.9	N/A

Filtro de endereços IP

CSC #1: Inventário e controle de ativos corporativos
CSC #4: Configuração segura de ativos e software corporativos
CSC #13: Monitoramento e defesa da rede

A filtragem de endereços IP impede que clientes não autorizados acessem o dispositivo Axis. Recomendamos configurar seu dispositivo para permitir os endereços IP dos hosts de rede autorizados ou negar os endereços IP dos hosts de rede não autorizados.

Se você optar por permitir endereços IP, certifique-se de adicionar todos os clientes autorizados (servidor VMS e clientes administrativos) à lista.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Security > IP Address Filter (Configuração > Opções do sistema > Segurança > Filtro de endereços IP)
≥ 7.10	Settings > System > TCP/IP > IP address filter (Configurações > Sistema > TCP/IP > Filtro de endereços IP)
≥ 10.9	Settings > Security > IP address filter (Configurações > Segurança > Filtro de endereços IP)

HTTPS

CSC #3: Proteção de dados

Os protocolos HTTP e HTTPS são ativados por padrão em dispositivos Axis a partir do AXIS OS 7.20. Embora o acesso HTTP seja inseguro, o HTTPS criptografa o tráfego entre o cliente e o dispositivo Axis. Recomendamos usar HTTPS para todas as tarefas administrativas no dispositivo Axis.

Para obter instruções de configuração, consulte *Somente HTTPS na página 22* e *Codificadores HTTPS na página 22*.

Fortalecimento básico

Somente HTTPS

Recomendamos configurar seu dispositivo Axis para usar somente HTTPS (sem acesso HTTP possível). Isso ativará automaticamente o HSTS (HTTP Strict Transport Security), o que aprimorará ainda mais a segurança do dispositivo.

A partir do AXIS OS 7.20, os dispositivos Axis são fornecidos com um certificado autoassinado. Embora um certificado autoassinado não seja confiável pelo design, ele é adequado para acessar com segurança o dispositivo Axis durante a configuração inicial e quando não há infraestrutura de chave pública (PKI) disponível. Se disponível, o certificado autoassinado deverá ser removido e substituído por certificados de clientes assinados corretamente emitidos pela autoridade PKI prefererida. A partir do AXIS OS 10.10, o certificado autoassinado foi substituído pelo certificado de ID de dispositivo seguro IEEE 802.1AR.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Security > HTTPS (Configuração > Opções do sistema > Segurança > HTTPS)
≥ 7.10	Settings > System > Security > HTTP and HTTPS (Configurações > Sistema > Segurança HTTP e HTTPS)
≥ 10.9	System > Network > HTTP and HTTPS (Sistema > Rede > HTTP e HTTPS)

Codificadores HTTPS

Os dispositivos Axis são compatíveis e usam pacotes codificadores TLS 1.2 e TLS 1.3 para criptografar com segurança conexões HTTPS. A versão de TLS específica e o conjunto de codificadores usados dependem do cliente conectado ao dispositivo Axis e será negociado de acordo. Após redefinir o dispositivo Axis para as configurações padrão de fábrica, é possível que a lista de codificadores possa ser atualizada automaticamente de acordo com a configuração de melhores práticas mais recente disponível fornecida pela Axis.

Para referência e transparência, use os pacotes de codificação seguros e fortes listados em *TLS 1.2 e inferiores na página 22* e *TLS 1.3 na página 22*.

TLS 1.2 e inferiores

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
```

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Advanced > Plain Config > HTTPS > Ciphers (Configuração > Opções do sistema > Avançado > Configuração simples > HTTPS > Codificadores)
≥ 7.10	Settings > System > Plain config > HTTPS > Ciphers (Configurações > Sistema > Configuração simples > HTTPS > Codificadores)
≥ 10.9	System > Plain config > HTTPS > Ciphers (Sistema > Configuração simples > HTTPS > Codificadores)

TLS 1.3

Por padrão, somente pacotes de codificação fortes de acordo com as especificações de TLS 1.3 estão disponíveis:

```
TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_SHA384
```

Esses pacotes não podem ser configurados pelo usuário.

Fortalecimento básico

Log de acesso

CSC #1: Inventário e controle de ativos corporativos
CSC #8: Gerenciamento de logs de auditoria

O log de acesso fornece logs detalhados de usuários que acessam o dispositivo Axis, o que facilita tanto as auditorias quanto o gerenciamento de controle de acesso. Recomendamos ativar esse recurso e combiná-lo com um servidor de syslog remoto para que o dispositivo Axis possa enviar seus logs para um ambiente de log central. Isso simplifica o armazenamento de mensagens de log e seu tempo de retenção.

Para obter mais informações, consulte *Log de acesso de dispositivos* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Advanced > Plain Config > System > Access log (Configuração > Opções do sistema > Avançado > Configuração simples > Sistema > Log de acesso)
≥ 7.10	Settings > System > Plain config > System > Access log (Configurações > Sistema > Configuração simples > Sistema > Log de acesso)
≥ 10.9	System > Plain config > System > Access log (Sistema > Configuração simples > Sistema > Log de acesso)

Acessórios antiviolação física

CSC #1: Inventário e controle de ativos corporativos
CSC #12: Gerenciamento da infraestrutura de rede

A Axis oferece chaves de invasão e/ou violação física como acessórios opcionais para aprimorar a proteção física de dispositivos Axis. Essas chaves podem acionar um alarme que permite que os dispositivos Axis enviem uma notificação ou um alarme para clientes selecionados.

Para obter mais informações sobre os acessórios antiviolação disponíveis, consulte:

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *AXIS Door Switch A*

Fortalecimento estendido

As instruções de fortalecimento estendido baseiam-se nos tópicos de fortalecimento descritos em *Proteção padrão na página 4* and *Fortalecimento básico na página 12*. No entanto, embora você possa aplicar as instruções de fortalecimento padrão e básicas diretamente ao seu dispositivo Axis, o fortalecimento estendido requer a participação ativa de toda a cadeia de suprimentos do fornecedor, da organização do usuário final e da infraestrutura de TI e/ou rede subjacente.

Limite a exposição à Internet

CSC #12: Gerenciamento da infraestrutura de rede

Não recomendamos expor o dispositivo Axis como servidor Web público ou, de alguma outra forma, permitir o acesso via rede de clientes desconhecidos ao dispositivo. Para pequenas organizações e indivíduos que não operam um VMS ou precisam acessar vídeo de locais remotos, recomendamos usar o AXIS Companion.

O AXIS Companion emprega o software cliente Windows/iOS/Android, é gratuito e oferece uma maneira fácil de acessar vídeo de forma segura sem expor o dispositivo Axis à Internet. Para obter mais informações sobre o AXIS Companion, consulte *axis.com/companion*.

Observação

Todas as organizações que usam um VMS devem consultar o fornecedor de VMS para se informar as melhores práticas sobre acesso remoto a vídeo.

Limite a exposição à rede

CSC #12: Gerenciamento da infraestrutura de rede

Uma forma comum de reduzir os riscos de exposição à rede é isolar fisicamente e virtualmente dispositivos de rede e infraestruturas e aplicativos relacionados. Exemplos de infraestrutura e aplicativos são software de gerenciamento de vídeo (VMS), gravadores de vídeo em rede (NVR) e outros tipos de equipamentos de monitoramento.

Recomendamos isolar seus dispositivos Axis e infraestruturas e aplicativos relacionados em uma rede local que não esteja conectada à sua rede de produção e negócios.

Para aplicar fortalecimento básico, proteja a rede local e sua infraestrutura (roteador, switches) contra acesso não autorizado adicionando uma várias camadas de mecanismos de segurança de rede. Exemplos desses mecanismos são segmentação de VLAN, recursos de roteamento limitados, rede privada virtual (VPN) para acesso site-site ou WAN, firewall da camada de rede 2/3 e listas de controle de acesso (ACL).

Para estender o fortalecimento básico, recomendamos aplicar técnicas de inspeção de rede mais avançadas, como inspeção de pacotes profunda e detecção de invasões. Isso adicionará proteção de ameaça consistente e abrangente dentro da rede. O fortalecimento estendido da rede requer software e/ou dispositivos de hardware dedicados.

Varredura de vulnerabilidades de rede

CSC #1: Inventário e controle de ativos corporativos
CSC #12: Gerenciamento da infraestrutura de rede

Você pode usar scanners de segurança de rede para realizar avaliações de vulnerabilidade dos seus dispositivos de rede. A finalidade de uma avaliação de vulnerabilidade é proporcionar uma revisão sistemática de potenciais vulnerabilidades de segurança e configurações incorretas.

Recomendamos realizar avaliações regulares de vulnerabilidade dos seus dispositivos Axis e de sua infraestrutura relacionada. Antes de iniciar a varredura, certifique-se de que seus dispositivos Axis tenham sido atualizados para a versão mais recente do AXIS OS disponível, seja no LTS ou na trilha ativa.

Também recomendamos revisar o relatório de varredura e filtrar falsos positivos conhecidos para separá-los dos dispositivos Axis, os quais você pode encontrar no *Guia de Varredura de Vulnerabilidades do AXIS OS*. Envie o relatório e quaisquer observações adicionais em um tíquete de suporte técnico para o *Suporte da Axis* em axis.com.

Infraestrutura de chave pública (PKI) confiável

CSC #3: Proteção de dados
CSC #12: Gerenciamento da infraestrutura de rede

Recomendamos implantar certificados de cliente e servidor Web em seus dispositivos Axis confiáveis e assinados por autoridades de certificados públicas ou privadas (CA). Um certificado assinado por CA com uma cadeia de confiança validada ajuda a remover avisos de certificados do navegador quando você conecta via HTTPS. Um certificado assinado por CA também garante a autenticidade do dispositivo Axis ao implantar uma solução de controle de acesso à rede (NAC). Isso atenua o risco de ataques por meio de um computador personificando um dispositivo Axis.

Você pode usar o AXIS Device Manager, fornecido com um serviço de CA integrado, para emitir certificados assinados para dispositivos Axis.

Controle de acesso à rede IEEE 802.1X

CSC #6: Gerenciamento de controle de acesso
CSC #13: Monitoramento e defesa da rede

Os dispositivos Axis oferecem suporte a controle de acesso à rede baseado em porta IEEE 802.1X por meio do método EAP-TLS. Para obter a proteção ideal, recomendamos usar certificados de clientes assinados por uma autoridade de certificação (CA) confiável ao autenticar seu dispositivo Axis.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Security > IEEE 802.1X (Configurações > Opções do sistema > Segurança > IEEE 802.1X)
≥ 7.10	Settings > System > Security > IEEE 802.1X (Configurações > Sistema > Segurança > IEEE 802.1X)
≥ 10.9	System > Security > IEEE 802.1X (Sistema > Segurança > IEEE 802.1X)

IEEE 802.1AE MACsec

CSC #3: Proteção de dados
CSC #6: Gerenciamento de controle de acesso

Os dispositivos Axis oferecem suporte ao 802.1AE MACsec, que é um protocolo de rede bem definido que protege criptograficamente os links Ethernet ponto a ponto na camada 2 da rede, garantindo a confidencialidade e a integridade das transmissões de dados entre dois hosts. Como o MACsec opera na camada 2 baixa da pilha de rede, ele acrescenta uma camada adicional de segurança aos protocolos de rede que não oferecem recursos de criptografia nativos (ARP, NTP, DHCP, LLDP, CDP...) e também aos que oferecem (HTTPS, TLS).

O padrão IEEE 802.1AE MACsec descreve dois modos de operação, um modo PSK (chave pré-compartilhada)/CAK estático configurável manualmente e um modo de sessão mestre/CAK dinâmico automático usando sessões IEEE 802.1X EAP-TLS. O dispositivo Axis é compatível com os dois modos.

Para obter mais informações sobre o 802.1AE MACsec e como configurá-lo nos dispositivos AXIS OS, consulte *IEEE 802.1AE* na base de conhecimento do AXIS OS.

Identidade de dispositivo segura IEEE 802.1AR

CSC #1: Inventário e controle de ativos corporativos
CSC #13: Monitoramento e defesa da rede

Os dispositivos Axis com Axis Edge Vault são compatíveis com o padrão de rede IEEE 802.1AR. Isso permite a conexão automatizada e segura de dispositivos Axis na rede por meio do ID de dispositivo Axis, um certificado exclusivo

instalado no dispositivo durante a fabricação. Para obter um exemplo de integração segura de dispositivo, leia mais em *Integração segura de dispositivos Axis em redes Aruba*.

Para obter mais informações, consulte o white paper em *Axis Edge Vault*. Para baixar a cadeia de certificados de IDs de dispositivos Axis, usada para validar a identidade dos dispositivos Axis, consulte o *Repositório de infraestrutura de chaves públicas* em axis.com.

Monitoramento de SNMP

CSC #8: Gerenciamento de logs de auditoria

Os dispositivos Axis oferecem suporte aos seguintes protocolos SNMP:

- **SNMP v1**: suporte oferecido somente por questões de compatibilidade com versões anteriores, não utilize.
- **SNMP v2c**: pode ser usado em um segmento de rede protegido.
- **SNMP v3**: recomendado para fins de monitoramento.

Os dispositivos Axis também oferecem suporte ao monitoramento de MIB-II e AXIS Video MIB. Para baixar o AXIS Video MIB, consulte *AXIS Video MIB* na Base de conhecimento do AXIS OS.

Para saber mais sobre como configurar o SNMP no AXIS OS, consulte *SNMP (Simple Network Management Protocol)* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Network > SNMP (Configuração > Opções do sistema > Rede > SNMP
≥ 7.10	Settings > System > SNMP (Configurações > Sistema > SNMP)
≥ 10.9	System > Network > SNMP (Sistema > Rede > SNMP)

Syslog remoto

CSC #8: Gerenciamento de logs de auditoria

É possível configurar um dispositivo Axis para enviar todas as suas mensagens de log criptografadas para um servidor de syslog central. Isso facilita as auditorias e impede que as mensagens de log sejam excluídas no dispositivo Axis, seja intencional, maliciosa ou acidentalmente. Dependendo das políticas da empresa, também é possível aumentar o tempo de retenção dos logs dos dispositivos.

Para obter mais informações sobre como ativar o servidor de syslog remoto em diferentes versões do AXIS OS, consulte *Syslog* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Para obter instruções, consulte *Syslog* no Portal do AXIS OS
≥ 7.10	Settings > System > TCP/IP (Configurações > Sistema > TCP/IP)
≥ 10.9	System > Logs (Sistema > Logs)

Streaming de vídeo seguro (SRTP/RTSPS)

CSC #3: Proteção de dados

A partir do AXIS OS 7.40, os dispositivos Axis oferecem suporte a streaming de vídeo seguro via RTP, também conhecidos como SRTP/RTSPS. O SRTP/RTSPS usa um método seguro de transporte criptografado ponta a ponta para garantir que somente clientes autorizados recebam o stream de vídeo do dispositivo Axis. Recomendamos ativar o SRTP/RTSPS se o seu sistema de gerenciamento de vídeo (VMS) for compatível. Se disponível, use SRTP em vez de streaming de vídeo RTP não criptografado.

Observação

O SRTP/RTSPS criptografa somente os dados do stream de vídeo. Para tarefas de configuração administrativa, recomendamos ativar o HTTPS somente para criptografar esse tipo de comunicação.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Advanced > Plain Config > Network > RTSPS (Configuração > Opções do sistema > Avançado > Configuração simples > Rede > RTSPS)
≥ 7.10	Settings > System > Plain config > Network > RTSPS (Configuração > Sistema > Configuração simples > Rede > RTSPS)
≥ 10.9	System > Plain config > Network > RTSPS (Sistema > Configuração plana > Rede > RTSPS)

Vídeo assinado

CSC #3: Proteção de dados

A partir do AXIS OS 10.11, os dispositivos Axis compatíveis com o Axis Edge Vault oferecem suporte a vídeos assinados. Com o vídeo assinado, os dispositivos Axis podem adicionar uma assinatura ao seu stream de vídeo para garantir que o vídeo esteja intacto e verificar sua origem ao rastreá-lo de volta ao dispositivo que o gerou. O sistema de gerenciamento de vídeo (VMS) ou sistema de gerenciamento de evidências (EMS) também pode verificar a autenticidade do vídeo fornecido por um dispositivo Axis.

Para obter mais informações, consulte o white paper em *Axis Edge Vault*. Para encontrar os certificados root da Axis usados para validar a autenticidade do vídeo assinado, consulte *Acesso a dispositivos* na Base de conhecimento do AXIS OS.

Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	N/A
≥ 7.10	N/A
≥ 10.9	System > Plain config > Image > SignedVideo (Sistema > Configuração simples > Imagem > Vídeo assinado)

Guia de início rápido

O guia de início rápido fornece uma breve visão geral das configurações que você deve configurar quando dispositivos Axis são fortalecidos com o AXIS OS 5.51 e versões posteriores. Ele aborda os tópicos de fortalecimento sobre os quais você pode ler em *Fortalecimento básico na página 12*. No entanto, ele não aborda os tópicos em, *Fortalecimento estendido na página 24* pois eles necessitam de configurações abrangentes e específicas do cliente caso a caso.

Recomendamos usar o AXIS Device Manager para fortalecer vários dispositivos Axis de forma rápida e econômica. Se você precisar usar outro aplicativo para configuração de dispositivos ou apenas para fortalecer alguns dispositivos Axis, recomendamos usar a API VAPIX.

Erros de configuração comuns

Dispositivos expostosà Internet
CSC #12: Gerenciamento da infraestrutura de rede

Não recomendamos expor o dispositivo Axis como servidor Web público ou, de alguma outra forma, permitir o acesso via rede de clientes desconhecidos ao dispositivo. Para obter mais informações, consulte *Limite a exposição à Internet na página 24*.

Senha comum
CSC #4: Configuração segura de ativos e software corporativos
CSC #5: Gerenciamento de contas

Recomendamos enfaticamente que você use uma senha exclusiva para cada dispositivo em vez de uma senha genérica para todos os dispositivos. Para obter instruções, consulte *Definir senha de root do dispositivo na página 13* e *Criar contas dedicadas na página 14*.

Acessoanônimo
CSC nº 4: Configuração segura de ativos e software corporativos
CSC #5: Gerenciamento de contas.

Não recomendamos permitir que usuários anônimos acessem as configurações de vídeo e configuração no dispositivo sem precisar fornecer credenciais de login. Para obter mais informações, consulte *Acesso por meio de credencial na página 4*.

Comunicação segura desativada
CSC #3: Proteção de dados

Não recomendamos operar o dispositivo usando métodos de comunicação e acesso inseguros, como HTTP ou autenticação básica para onde senhas são transferidas sem criptografia. Para obter mais informações, consulte *HTTPS ativado na página 8*. Para obter recomendações de configuração, consulte *Autenticação Digest na página 8*.

Versão do AXIS OS desatualizada
CSC #2: Inventário e controle de ativos de software

Recomenda-se operar o dispositivo Axis usando a versão mais recente do AXIS OS disponível, seja no LTS ou na trilha ativa. Ambas as trilhas oferecem os patches de segurança e correções de bug mais recentes. Para obter mais informações, consulte *Atualizar para o AXIS OS mais recente na página 12*.

Fortalecimento básico via API VAPIX

Você pode usar a API VAPIX para fortalecer seus dispositivos Axis com base nos tópicos abordados em *Fortalecimento básico na página 12*. Nesta tabela, você pode encontrar todas as configurações básicas de configuração de fortalecimento, independentemente da versão do AXIS OS de seu dispositivo Axis.

É possível que algumas configurações não estejam mais disponíveis na versão AXIS OS do seu dispositivo, pois algumas funcionalidades foram removidas ao longo do tempo para aumentar a segurança. Se você receber um erro ao emitir a chamada VAPIX, isso poderá ser uma indicação de que a funcionalidade não está mais disponível na versão do AXIS OS.

Guia de início rápido

Finalidade	Chamada à API VAPIX
*Desativar PoE em portas de rede não utilizadas**	`http://endereço-ip/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no`
*Desativar o tráfego de rede em portas de rede não utilizadas***	`http://endereço-ip/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }`
Desativar o protocolo de detecção Bonjour	`https://endereço-ip/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no`
Desativar o protocolo de detecção UPnP	`https://endereço-ip/axis-cgi/param.cgi?action=update&Network.UPnP.Enabled=no https://endereço-ip/axis-cgi/param.cgi?action=update&Network.UPnP.NATTraversal.Enabled=no`
Desativar o protocolo de detecção WebService	`https://endereço-ip/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no`
Desativar o One-click-cloud connection (O3C)	`https://endereço-ip/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no`
Desativar acesso à manutenção do dispositivo via SSH	`https://endereço-ip/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`
Desativar acesso à manutenção do dispositivo via FTP	`https://endereço-ip/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`
Desativar configuração de endereços IP ARP-Ping	`https://endereço-ip/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no`
Desativar a configuração de endereços IP com configuração zero	`http://endereço-ip/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no`
Ativar somente HTTPS	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https https://endereço-ip/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https https://endereço-ip/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https`
Ativar somente TLS 1.2 e TLS 1.3	`https://endereço-ip/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no`

Guia de início rápido

Finalidade	Chamada à API VAPIX
Configuração do codificador seguro TLS 1.2	`https://endereço-ip/axis-cgi/param.cgi?action=update&HTTPS.Ciphers=ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384`

*Ativar proteção contra ataques de força bruta****	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on`
	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10`
	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20`
	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1`
	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20`
	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1`

Desativar ambiente do editor de scripts	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.EditCgi=no`
Ativar log de acesso de usuários aprimorado	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.AccessLog=On`
Ativar proteção contra ataques de reprodução ONVIF	`https://endereço-ip/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes`
Desativar acesso à interface Web do dispositivo	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes`
Desativar cabeçalho do servidor HTTP/OpenSSL	`https://endereço-ip/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no`

Desativar visualizador anônimo e acesso a PTZ	`https://endereço-ip/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password`
	`https://endereço-ip/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password`
	`https://endereço-ip/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password`

** Substitua "X" pelo número da porta real em "port=X". Exemplos: "port=1" desativará a porta 1 e "port=2" desativará a porta 2.*
*** Substitua "1" pelo número da porta real em "eth1.1". Exemplos: "eth1.1" desativará a porta 1 e "eth1.2" desativará a porta 2.*

**** Após 20 tentativas de login com falha em um segundo, o endereço IP do cliente será bloqueado por 10 segundos. Cada solicitação com falha a seguir no intervalo de 30 segundos fará com que o período de bloqueio de DoS seja estendido por mais 10 segundos.*

Fortalecimento básico via AXIS Device Manager (Extend)

Você pode usar o AXIS Device Manager e o AXIS Device Manager Extend para fortalecer seus dispositivos Axis com base nos tópicos abordados em *Fortalecimento básico na página 12*. Use este *arquivo de configuração*, o qual consiste nas mesmas configurações de configuração listadas em *Fortalecimento básico via API VAPIX na página 28*.

É possível que algumas configurações não estejam mais disponíveis na versão AXIS OS do seu dispositivo, pois algumas funcionalidades foram removidas ao longo do tempo para aumentar a segurança. O AXIS Device Manager e o AXIS Device Manager Extend removerão automaticamente essas configurações da configuração de fortalecimento.

Observação

Após você carregar o arquivo de configuração, o dispositivo Axis será configurado somente para HTTPS e a interface da Web será desativada. Você pode modificar o arquivo de configuração de acordo com suas necessidades, por exemplo, removendo ou adicionando parâmetros.

AXIS OS Hardening Guide
Ver. M43.2
Data: Setembro 2023
Nº da peça