

Guia para aumento do nível de proteção do AXIS OS

Portal AXIS OS | Notas da versão do AXIS OS | Base de conhecimento do AXIS OS | lista de reprodução do YouTube do AXIS OS | Avisos de segurança

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 de seus 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 manipulação. 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 da 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.

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](https://www.cisecurity.org).

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.

O diagrama da Arquitetura de segurança do AXIS OS descreve os recursos de segurança cibernética do AXIS OS em várias camadas. Ele fornece uma visão geral abrangente da base de segurança, da segurança assistida por silício, do sistema operacional AXIS OS e da camada de controle de acesso e aplicação.

Access control	Access control management Local user device management with password complexity indicator Federated user device management through OpenID Connect (RFC6749, 1.3.1 Authorization Code) providing ADFS-integration that unlocks features such as password complexity enforcement, rotation, automatic account lock-out Multi-factor authentication (MFA), Microsoft AD entitlement functionality		Privacy Use of diagnostics data Minimalistic approach to how much customer-specific data should be stored
	Application security TLS-based application security (MQTT, SFTP, NTS, HTTPS, WebRTC) Encrypted video streaming (RTSPS/SRTP, HTTPS), Secure remote syslog		
Operating system	Encryption and data protection OpenSSL 1.1.1 and 3.0 X.509 certificate PKI and cryptography Transport layer security (TLS 1.2/TLS 1.3) SD card encryption (AES-XTS-Plain64 256bit) Encrypted file system (AES-XTS-Plain64 256bit), Signed video	Default security HTTPS enabled by default Brute-Force Delay Protection Host-based Firewall Network time security (NTS) Insecure TLS versions disabled UART/Debug port disabled	Enterprise network security IEEE 802.1X (network access control) IEEE 802.1AR (secure device identity) IEEE 802.1AE (MAC security, MACsec)
AXIS OS Operating System Common Linux-based operating system with more than 95% industry-standard open-source software components such as OpenSSL, Apache, Curl and others. Active track for feature growth and 5-year long-term support tracks (LTS) for 3rd party integration and backwards-compatibility use cases.			
Silicon assisted security (chip)	Hardware root-of-trust ARM-based system-on-chip (SoC) security Trusted Execution Environment (TEE/OP-TEE) Trusted platform module (TPM 2.0), Secure element		Secure key storage Tamper-protected storage and operation of cryptographic keys such as customer uploaded private keys, video signing keys and the Axis Device ID.
Security foundation	Axis Security Development Model Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)	Compliance Common Criteria EAL FIPS 140 ETSI EN 303 645	Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed OS (code-signing) Axis Device ID (IEEE 802.1AR)

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

Autenticação

Desativado por padrão

CSC nº 4: Configuração segura de ativos corporativos e software

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

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.

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

Autenticação Digest

CSC nº 3: Proteção de dados

Os clientes que acessam o dispositivo autenticarão com uma senha que deve ser criptografada quando enviada pela rede. Recomendamos que você ative o HTTPS conforme descrito aqui. Se isso não for possível,

recomendamos que você use apenas a autenticação Digest, em vez da Basic, ou Basic e Digest em conjunto. 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 > Política de autenticação HTTP da rede)
≥ 10.9	System > Plain config > Network > Network HTTP Authentication policy (Sistema > Configuração simples > Rede > Política de autenticação HTTP da rede)

Proteção contra ataque de reprodução ONVIF

CSC nº 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 nº 4: Configuração segura de ativos corporativos e software

CSC nº 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 atrasos de força bruta é ativada por padrão a partir do AXIS OS 11.5. Para obter exemplos de configuração e recomendações detalhadas, 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)

Edge storage

CSC nº 4: Configuração segura de ativos corporativos e software

CSC nº 3: Proteção de dados

A partir do AXIS OS 12.0, a opção de montagem noexec foi adicionada como opção padrão para os compartilhamentos de rede montados. Isso desabilitará qualquer execução direta de binários do compartilhamento de rede montado. Cartões SD já tinham essa opção adicionada em versões anteriores do AXIS OS.

Além disso, os dispositivos Axis com AXIS OS 10.10 e versões posteriores 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

Segurança de rede

Protocolos de rede

CSC nº 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	Deteção automática	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

Protocolo	Deteção automática	Transporte	Comentários
			e ONVIF ou comunicação edge-to-edge.*
RTSP	554	TCP	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 deteção UPnP. NOTA: desativado por padrão no AXIS OS 12.0.
Bonjour	5353	UDP	Usado por aplicativos de terceiros para descobrir o dispositivo Axis via protocolo de deteção mDNS (Bonjour).
SSDP	1900	UDP	Usado por aplicativos de terceiros para descobrir o dispositivo Axis via SSDP (UPnP). NOTA: desativado por padrão no AXIS OS 12.0.
WS-Discovery***	3702	UDP	Usado por aplicativos de terceiros para descobrir o dispositivo Axis via protocolo de deteção WS-Discovery (ONVIF).

* Para obter mais informações sobre a tecnologia edge-to-edge, consulte o white paper *Edge-to-edge technology (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 na Wikipedia sobre *Ephemeral port (Porta efêmera)*.

*** O protocolo WebService Discovery (WS-Discovery) está desativado por padrão no AXIS OS 12.1 e posterior.

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 entrada/saída de áudio e a funcionalidade de microfone em produtos de videomonitoramento Axis, como câmeras em rede. Já nos intercomunicadores e alto-falantes em rede Axis, a entrada/saída de áudio e a funcionalidade de microfone são recursos básicos e, portanto, são ativados por padrão.

HTTPS ativado

CSC nº 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. No AXIS OS 10.10 e versões posteriores, o certificado autoassinado foi substituído pelo certificado de ID de dispositivo seguro IEEE 802.1AR.

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. No AXIS OS 9.80 e versões posteriores, você pode usar a API de cabeçalho HTTP personalizada VAPIX para configurar cabeçalhos de HTTP(S) 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.

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)

Controle de acesso à rede IEEE 802.1X

CSC nº 6: Gerenciamento de controle de acesso

CSC nº 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 nº 3: Proteção de dados

CSC nº 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 nº 1: Inventário e controle de ativos corporativos

CSC nº 13: Monitoramento e defesa da rede

Dispositivos Axis com o Axis Edge Vault são compatíveis com o padrão de rede IEEE 802.1AR, o que permite a integração automatizada e segura de dispositivos Axis em rede por meio do Axis Device ID, um certificado exclusivo instalado no dispositivo durante a produção. 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.

Interface UART/Debug

CSC nº 4: Configuração segura de ativos corporativos e software

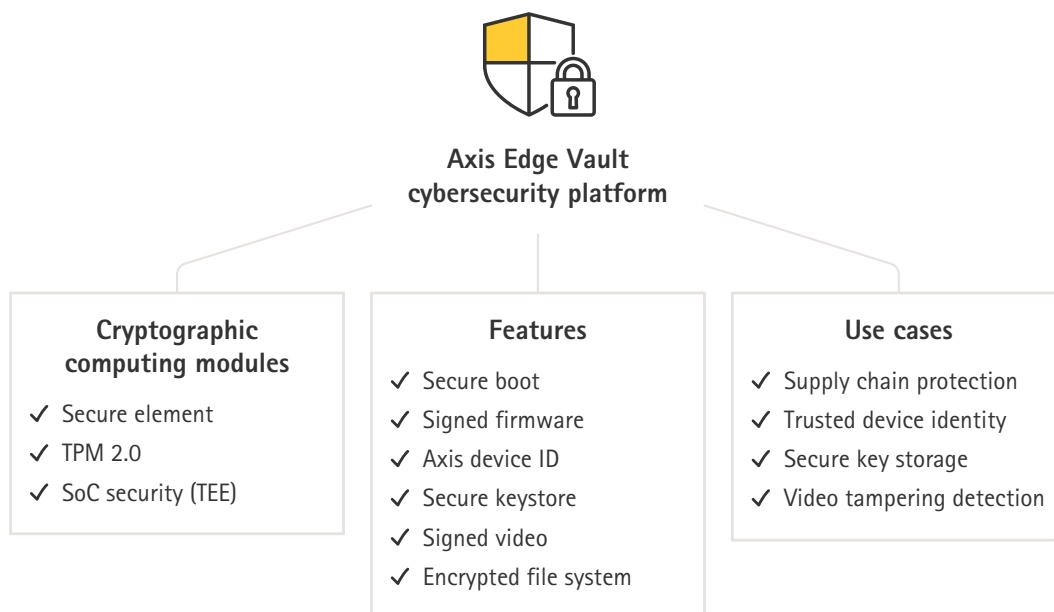
Todos os dispositivos Axis vêm com uma interface UART (Universal Asynchronous Receiver Transmitter) física, às vezes chamada de "porta de depuração" ou "console serial". A interface em si só pode ser acessada fisicamente por meio de extensa desmontagem do dispositivo Axis. A interface UART/debug é usada 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 depende de uma base sólida de módulos de computação criptográfica (elemento seguro e TPM) e segurança 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 permitem uma cadeia ininterrupta de software criptograficamente validado para a cadeia de confiança da qual dependem todas as operações seguras.

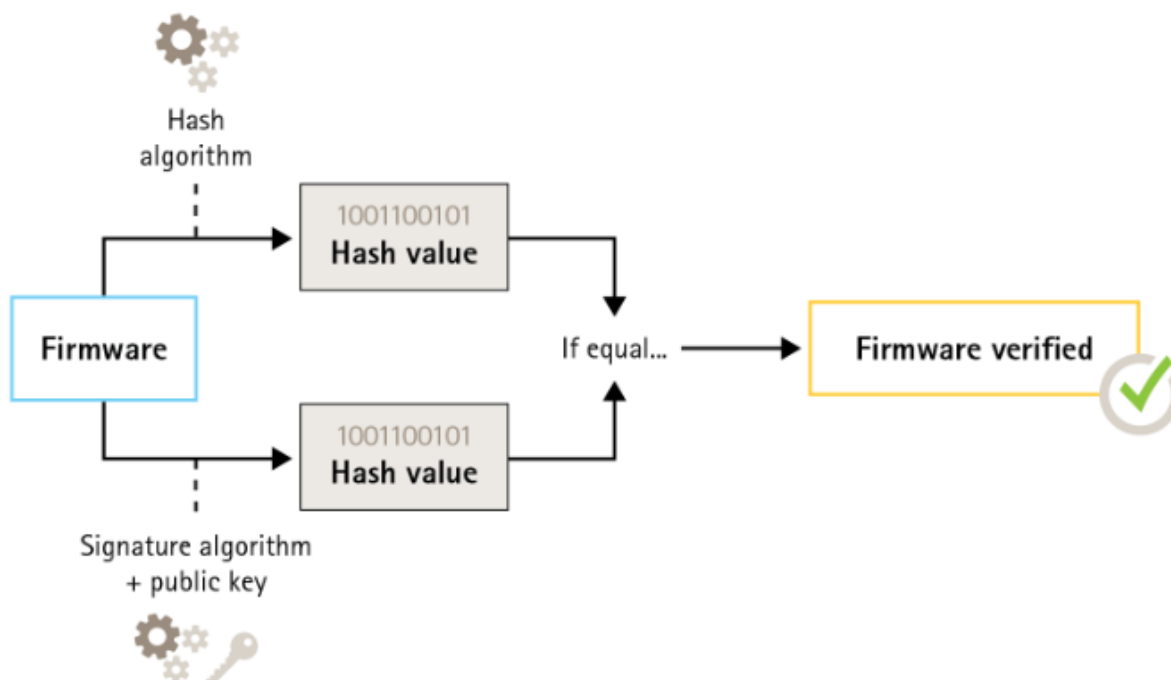
Os dispositivos Axis com o Axis Edge Vault minimizam a exposição do cliente a riscos de segurança cibernética, impedindo a espionagem e a extração maliciosa de informações confidenciais. O Axis Edge Vault também garante que o dispositivo Axis seja uma unidade confiável e confiável na rede do cliente.



Firmware assinado

CSC nº 2: Inventário e controle de ativos de software

O AXIS OS é assinado desde a 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 impedirá que invasores enganem os usuários para fazê-los instalar arquivos comprometidos.

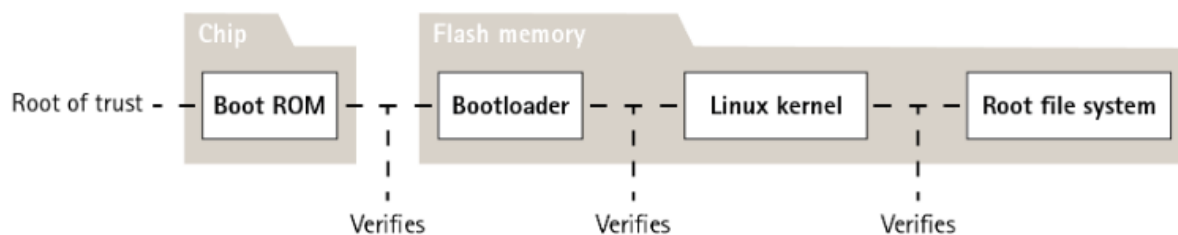


Para obter mais informações, consulte o white paper em *Axis Edge Vault*.

Inicialização segura

CSC nº 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 seguro de chaves

CSC nº 6: Gerenciamento de controle de acesso

O armazenamento seguro de chaves fornece armazenamento de informações criptográficas com base em hardware e protegido contra violação. 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 nº 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 manipulação da configuração em caso de roubo ou caso alguém obtenha acesso físico ao dispositivo. 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*.

Desativação

CSC nº 3: Proteção de dados

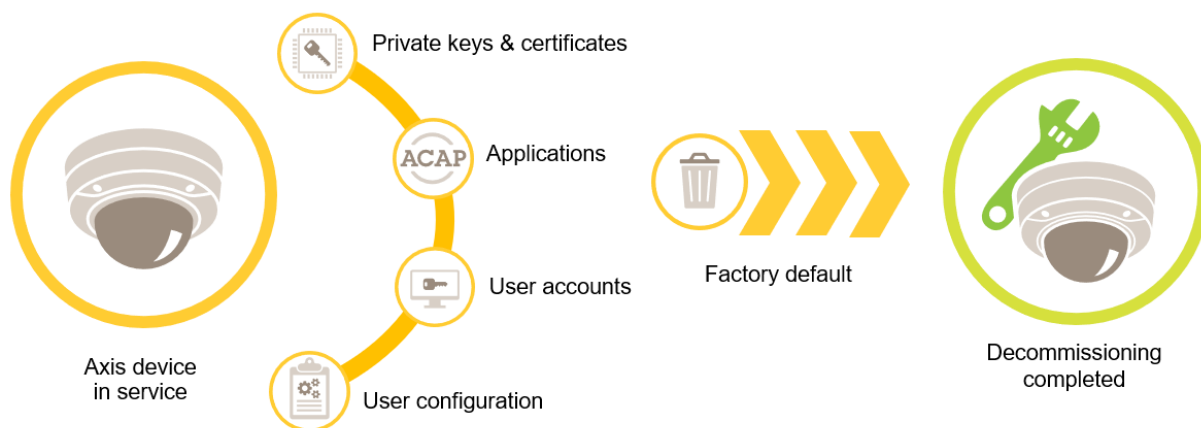
Os dispositivos Axis usam memória volátil e não volátil e, embora a memória volátil seja apagada sempre que o dispositivo é desligado da fonte de alimentação, as informações armazenadas na memória não volátil

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. Para memória flash NAND a função UBI Remove volume é usada. A função equivalente é usada para memória flash eMMC que sinaliza que os blocos de armazenamento não são mais usados. O controlador de armazenamento limpará então esses blocos de armazenamento de acordo.

Ao descomissionar um dispositivo Axis, recomendamos redefinir o dispositivo para as configurações padrão de fábrica, o que apagará todos os dados armazenados na memória não volátil do dispositivo.

Observe que a emissão de um comando padrão de fábrica não apagará imediatamente os dados; em vez disso, o dispositivo reiniciará e o apagamento dos dados ocorrerá durante a inicialização do sistema. Portanto, não basta apenas emitir o comando padrão de fábrica, é preciso também permitir que o dispositivo seja reinicializado e conclua sua inicialização antes de ser desligado para garantir a conclusão do apagamento dos dados.

Esse procedimento de apagar os dados do cliente segue a técnica de sanitização "Clear" descrita na NIST SP-800-88 Revisão 1.



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

* O processo de firmware assinado usa certificados personalizados que permitem que os usuários carreguem (entre outras coisas) o AXIS OS.

As gravações e imagens armazenadas no edge storage (cartão SD, compartilhamento de rede) devem ser excluídas pelo usuário separadamente. O apagamento dos dados do cliente no cartão SD é realizado de acordo com a NIST SP-800-88 Revisão 1, Cryptographic Erase (CE), e de acordo com a NIST SP-800-88 Revisão 1, Clear, para dados em HDDs (série S30-Recorder Series). Para obter mais informações, consulte a Base de conhecimento do AXIS OS.

*** Todas as configurações feitas pelo usuário, desde criação de contas até configurações de rede, O3C, eventos, imagens, PTZ e sistema.

**** O dispositivo mantém todos os aplicativos pré-instalados, mas exclui todas as configurações feitas pelo usuário referentes a eles.

***** Dados de produção (calibração, certificados de produção 802.1AR) e estatísticas de vida útil incluem informações não confidenciais e não relacionadas ao usuário.

Fortalecimento básico

O fortalecimento básico é o nível mínimo de proteção recomendado para dispositivos Axis. Os tópicos de 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 do padrão de fábrica

CSC nº 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 .

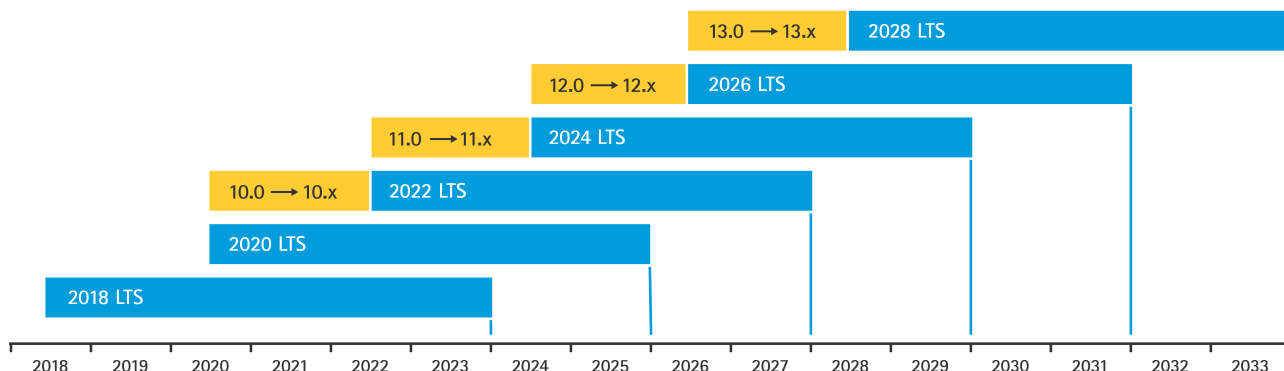
Versão do AXIS OS	Caminho de configuração da interface Web
< 7.10	Setup > System Options > Maintenance > Default (Configuração > Opções do sistema > Manutenção > Padrão).
7.10	Settings > System > Maintenance > Default (Configurações > Sistema > Manutenção > Padrão).
≥ 10.9	Maintenance > Default (Manutenção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

Atualizar para o AXIS OS mais recente

CSC nº 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 as trilhas 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.

AXIS OS 2018 LTS - Security Updates Timeline

2018 → 2019 → 2020 → 2021 → 2022

8.40.2 May ▪ OpenSSL	8.40.3.2 February ▪ Linux kernel ▪ CURL	8.40.4 July ▪ Apache ▪ CURL ▪ OpenSSL	8.40.4.2 April ▪ CURL ▪ OpenSSL	8.40.4.4 January ▪ Apache ▪ CURL ▪ OpenSSL
8.40.2.2 July ▪ OpenSSH ▪ OpenSSL ▪ TLSv1.3		8.40.4.1 November ▪ Apache	8.40.4.3 October ▪ Apache ▪ CURL ▪ OpenSSH ▪ OpenSSL	8.40.4.5 May ▪ Apache ▪ OpenSSL
8.40.3.1 Decem- ▪ Apache ▪ OpenSSL				8.40.4.6 July ▪ Apache ▪ CURL ▪ OpenSSL
				8.40.4.7 October ▪ CURL ▪ OpenSSL
				8.40.4.8 December ▪ CURL ▪ OpenSSL

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)

Criar contas dedicadas

CSC nº 4: Configuração segura de ativos corporativos e software

CSC nº 5: Gerenciamento de contas

Os dispositivos Axis podem ter dois tipos de contas: uma conta de administrador e uma de usuário cliente. A conta de administrador é a principal conta para o gerenciamento de seu dispositivo, e é essencial reservá-la apenas para tarefas administrativas. Ao configurar o dispositivo, você precisará criar um nome de usuário e uma senha para a conta de administrador.

Além da conta de administrador, crie uma conta de usuário cliente com privilégios limitados para operação diária. Isso permitirá gerenciar seu dispositivo com segurança, reduzindo o risco de comprometer a senha de administrador do dispositivo. A conta de usuário cliente deve ser usada para tarefas que não exijam privilégios totais de administrador.

Ao criar senhas para uma ou outra conta, recomendamos que você implemente diretrizes, por exemplo, as recomendações de senha do NIST ou do BSI, que exigem que as novas senhas sejam suficientemente longas e complexas. Os dispositivos Axis oferecem suporte a senhas com até 64 caracteres. Senhas com menos de 8

caracteres são consideradas fracas. Para obter mais informações, consulte *Gerenciamento de identidade e acesso* na Base de conhecimento do AXIS OS.

Os dispositivos Axis que executam o AXIS OS 11.6 ou superior oferecem suporte ao OAuth 2.0, que permite o gerenciamento de identidade e acesso (IAM) centralizado e identidades federadas para autenticação no dispositivo. Isso elimina a necessidade de gerenciamento local dos usuários do dispositivo. Para obter mais informações, consulte .

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)

Desativar o acesso à interface Web

CSC nº 4: Configuração segura de ativos corporativos e software

CSC nº 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.

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 opções de rede, data e hora

CSC nº 4: CSC nº 8: Gerenciamento de registros de auditoria

CSC nº 12: Gerenciamento da infraestrutura de rede

É importante configurar corretamente as definições de rede, data e hora do dispositivo para manter seu dispositivo Axis funcional e seguro. Essas configurações afetam vários aspectos do comportamento do dispositivo, incluindo comunicação em rede, registro em log e validação de certificados.

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. Revise a topologia de sua rede sempre que adicionar novos componentes. Recomendamos usar a configuração de endereço IP estático para garantir a acessibilidade da rede e minimizar as dependências de servidores de rede que possam ser vulneráveis a ataques, como servidores DHCP.

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)

A cronometragem precisa é essencial para manter logs do sistema, validar certificados digitais e ativar serviços como HTTPS, IEEE e 802.1x. Recomendamos sincronizar o relógio do dispositivo com servidores NTP (Network Time Protocol) ou NTS (Network Time Security). O Network Time Security (NTS), uma variante criptografada e segura do Network Time Protocol (NTP), foi adicionado ao AXIS OS 11.1. Recomendamos a configuração de vários servidores de horário para obter mais precisão e para considerar possíveis falhas. Se não for possível hospedar servidores de horário locais, considere o uso de servidores NTP ou NTS públicos. 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)

Criptografia de armazenamento na borda

CSC nº 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)

Aplicativos (ACAPs)

CSC nº 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 *Analíticos* 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 nº 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 descoberta de rede

Os protocolos de detecção, como Bonjour, UPnP, ZeroConf e WS-Discovery e LLDP/CDP, 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
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)

Versão do AXIS OS	Caminho de configuração da interface Web
	System > Plain config > WebService > DiscoveryMode > Enable WS-Discovery discoverable mode (Sistema > Configuração simples > Serviço Web > Modo de detecção > Ativar modo de descoberta WS-Discovery)
≥ 11.11	System > Network > Network discovery protocols > LLDP and CDP** (Sistema > Rede > Protocolos de descoberta de rede > LLDP e CDP)

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

** Desativar as configurações LLDP e o CDP poderia afetar a negociação de energia PoE.

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.

As versões desatualizadas do TLS foram removidas do AXIS OS 12.0 e não estão disponíveis em versões posteriores.

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 para videomonitoramento Axis, como câmeras em rede, a entrada/saída de áudio e a funcionalidade de microfone são desativadas 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 não seguro usado apenas para fins de solução de problemas e depuração. O acesso FTP foi removido do AXIS OS 11.1 e não está disponível em 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 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 é compatível com dispositivos Axis com versões anteriores ao AXIS OS 5.50. Recomendamos desativar o acesso Telnet.

Versão do AXIS OS	Caminho de configuração da interface Web
< 5.50	Para obter instruções, consulte <i>Acesso a dispositivos</i> 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

USB

A partir do AXIS OS 12.1, o AXIS D1110 vem com a opção de desativar a porta USB. Deixar portas USB 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
≥ 12.1	System > > Accessories > USB Configuration (Sistema > Acessórios > Configuração USB)

Firewall baseado em host

CSC nº 1: Inventário e controle de ativos corporativos

CSC nº 4: Configuração segura de ativos corporativos e software

CSC nº 13: Monitoramento e defesa da rede

Introduzido no AXIS OS 11.9, o firewall baseado em host é um recurso de segurança que permite criar regras que regulam o tráfego de entrada por endereço IP e/ou números de porta TCP/UDP. Isso ajuda a impedir o acesso não autorizado ao dispositivo ou a seus serviços.

Se você definir a política padrão como "Negar", certifique-se de adicionar todos os clientes autorizados (VMS e clientes administrativos) e/ou portas à sua lista.

Versão do AXIS OS	Caminho de configuração da interface Web
≥ 11.9	Setup > Security > Firewall (Configuração > Segurança > Firewall)

Filtro de endereços IP

Dispositivos com o AXIS OS 11.8 e versões anteriores usam filtragem de endereço IP para impedir o acesso de clientes não autorizados. Recomendamos configurar seu dispositivo para permitir endereços IP de hosts de rede autorizados ou negar os não autorizados.

Se você optar por permitir endereços IP, certifique-se de adicionar todos os clientes autorizados, incluindo 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 – 11.8	Settings > Security > IP address filter (Configurações > Segurança > Filtro de endereços IP)

Observação

É possível ativar logs mais detalhados de tentativas de acesso à rede para ajudar você a identificar tentativas de acesso indesejadas de outros hosts da rede. Para isso, acesse **System > Plain config > Network** (Sistema > Configuração simples > Rede) e o Registro de filtro de rede.

HTTPS

CSC nº 3: Proteção de dados

O HTTP e o HTTPS são ativados por padrão nos dispositivos Axis a partir do AXIS OS 7.20. Enquanto o acesso HTTP é não seguro sem nenhuma criptografia, 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 e .

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 preferida. 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. Durante as atualizações regulares do AXIS OS, a lista de cifras disponíveis do dispositivo Axis pode receber atualizações sem que a configuração real do codificador alterada. A alteração das configurações do codificador deve ser iniciada pelo usuário, seja por meio da execução de um padrão de fábrica do dispositivo Axis ou por meio da configuração manual do usuário. A partir do AXIS OS 10.8 e posterior, a lista de codificadores é atualizada automaticamente quando o usuário realiza uma atualização do AXIS OS.

TLS 1.2 e inferiores

Ao usar o TLS 1.2 ou inferior, você pode especificar os codificadores HTTPS a serem usados pelo dispositivo Axis quando ele for reiniciado. Não há restrições aos codificadores que você pode escolher, mas recomendamos que você selecione qualquer um dos seguintes codificadores fortes:

ECDHE-ECDHE-AES128-GCM-SHA256 : ECDHE-RSA-AES128-GCM-SHA256 : ECDHE-ECDHE-AES256-GCM-SHA384 : ECDHE-RSA-AES256-GCM-SHA384 : ECDHE-ECDHE-CHACHA20-POLY1305 : ECDHE-RSA-CHACHA20-POLY1305

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.

Registro de acesso

CSC nº 1: Inventário e controle de ativos corporativos

CSC nº 8: Gerenciamento de registros 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 contra manipulação física

CSC nº 1: Inventário e controle de ativos corporativos

CSC nº 12: Gerenciamento da infraestrutura de rede

A Axis oferece chaves contra invasão e/ou manipulação física como acessórios opcionais para aprimorar a proteção física dos 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 contra manipulação disponíveis, consulte:

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *Chave de porta AXIS A*

Aumento do nível de proteção estendido

As instruções de fortalecimento estendido baseiam-se nos tópicos de fortalecimento descritos em and . 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.

Limitar a exposição na internet e na rede

CSC nº 12: Gerenciamento da infraestrutura de rede

Recomendamos evitar expor qualquer dispositivo Axis como um servidor da Web público ou, de qualquer outra forma, permitir o acesso de clientes desconhecidos à rede do dispositivo. Para pequenas organizações e indivíduos que não usam software de gerenciamento de vídeo (VMS) ou que precisam acessar vídeo de locais remotos, o AXIS Camera Station Edge é uma boa opção.

O AXIS Camera Station Edge está disponível para Windows, iOS e Android, gratuitamente, e oferece uma maneira fácil de acessar vídeos com segurança sem expor seu dispositivo na internet. Para obter mais informações, consulte axis.com/products/axis-camera-station-edge.

Observação

Se a sua organização usa um VMS, consulte o fornecedor do VMS para obter as melhores práticas de acesso remoto a vídeo.

O isolamento dos dispositivos de rede, da infraestrutura e dos aplicativos relacionados reduz o risco de exposição da rede.

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

Para aplicar fortalecimento básico, proteja a rede local e sua infraestrutura (roteador, switches) contra acesso não autorizado usando várias camadas de mecanismos de segurança de rede. Entre eles, segmentação de VLAN, recursos limitados de roteamento, VPN para acesso de local a local ou WAN, firewall de camada de rede 2/3 e listas de controle de acesso (ACL).

Para ampliar o fortalecimento básico, aplique técnicas avançadas de inspeção de rede, como inspeção profunda de pacotes e detecção de intrusão. Isso aumenta a proteção contra ameaças dentro da rede. Observe que fortalecimento de rede estendido normalmente requer software e/ou hardware especializados.

Varredura de vulnerabilidades de rede

CSC nº 1: Inventário e controle de ativos corporativos

CSC nº 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 nº 3: Proteção de dados

CSC nº 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 pela CA com uma cadeia de confiança válida ajuda a remover os avisos de certificado do navegador quando você se conecta via HTTPS. Um certificado assinado pela CA também garante a autenticidade do dispositivo Axis quando você implanta 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.

Syslog remoto

CSC nº 8: Gerenciamento de registros 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 <i>Syslog</i> 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 nº 3: Proteção de dados

A partir do AXIS OS 7.40, os dispositivos Axis são compatíveis com streaming de vídeo seguro por RTP, também chamado de SRTP/RTSPS, usa um método de transporte criptografado seguro de ponta a ponta para garantir que somente clientes autorizados recebam o streaming 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 nº 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)

OAuth 2.0

CSC nº 4: Configuração segura de ativos corporativos e software

CSC nº 5: Gerenciamento de contas

Com o OAuth 2.0, é possível integrar dispositivos AXIS OS que executam o AXIS OS 11.6 ou superior a uma infraestrutura de TI com um serviço centralizado de gerenciamento de identidade e acesso (IAM). Isso permite o uso de identidades federadas para autenticação no dispositivo Axis, eliminando a necessidade de gerenciamento local dos usuários do dispositivo.

Dependendo dos recursos do provedor de serviços, você pode usar os seguintes mecanismos de segurança para autenticação aprimorada baseada em identidade no dispositivo Axis:

- Autenticação multifator (MFA)
- Aplicação de complexidade de senha
- Rotatividade de senha
- Tempo limite de autenticação
- Gerenciamento centralizado de identidade (conta de usuário/serviço)

Para obter mais informações sobre como ativar e configurar o OAuth 2.0 em dispositivos AXIS OS, consulte *OAuth 2.0 OpenID Connect* 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
≥ 11.6	System > Accounts > OpenID Configuration (Sistema > Contas > Configuração do OpenID)

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 . No entanto, ele não aborda os tópicos em, 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

Observação

Os erros comuns de configuração listados abaixo aumentam potencialmente a superfície de ataque do dispositivo Axis e reduzem suas camadas de defesa de segurança cibernética, resultando em um risco maior de exploração, uso indevido ou operação insegura do dispositivo.

Dispositivos expostos 'à Internet

CSC nº 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 .

Senha comum

CSC nº 4: Configuração segura de ativos corporativos e software

CSC nº 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 *Gerenciamento de identidade e acesso* na Base de conhecimento do AXIS OS e .

Acesso anônimo

CSC nº 4: Configuração segura de ativos corporativos e software

CSC nº 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 .

Comunicação segura desativada

CSC nº 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 . Para obter recomendações de configuração, consulte .

Versão do AXIS OS desatualizada

CSC nº 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 .

Fortalecimento básico via API VAPIX

Você pode usar a API VAPIX para fortalecer seus dispositivos Axis com base nos tópicos abordados em . 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.

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

Finalidade	Chamada à API VAPIX
<i>Configuração do codificador seguro TLS 1.2</i>	<code>https://ip-address/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</code>
<i>Ativar proteção contra ataques de força bruta***</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1</code>
<i>Desativar ambiente do editor de scripts</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no</code>
<i>Ativar log de acesso de usuários aprimorado</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On</code>
<i>Ativar proteção contra ataques de reprodução ONVIF</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes</code>
<i>Desativar acesso à interface Web do dispositivo</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes</code>
<i>Desativar cabeçalho do servidor HTTP/OpenSSL</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no</code>
<i>Desativar visualizador anônimo e acesso a PTZ</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password</code>

Finalidade	Chamada à API VAPIX
<i>Impedir a instalação do privilégio root que requer aplicativos ACAP</i>	<code>http://ip-address/axis-cgi/ /applications/config.cgi?action= set&name=AllowRoot&value=false</code>
<i>Impedir a instalação de aplicativos ACAP não assinados</i>	<code>http://ip-address/axis-cgi/ /applications/config.cgi?action= set&name=AllowUnsigned&value=false</code>

* 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 é 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 . Use este *arquivo de configuração*, o qual consiste nas mesmas configurações de configuração listadas em .

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.

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.

