

AXIS S2208 Mk II Standalone Appliance

Solução de gravação multifuncional com switch PoE integrado

Esse dispositivo autônomo multifuncional para até oito canais de vídeo é silencioso e não atrapalha as operações locais. Ele inclui oito licenças do AXIS Camera Station Pro, um switch PoE e armazenamento de 4 TB. É fácil expandir seu sistema usando a série AXIS S30 Recorder Series para ter mais canais, PoE e armazenamento. Fornecido com software e ferramentas pré-instalados que ajudam você a configurar e manter o seu sistema, como o AXIS Recorder Toolbox e seu respectivo assistente de instalação intuitivo, por exemplo. Além disso, o dispositivo oferece recursos e padrões de alta segurança, como o TPM com certificação FIPS 140-2 Nível 2.

- > **Solução tudo em um com switch PoE integrado**
- > **8 licenças do AXIS Camera Station Pro incluídas**
- > **Silencioso — não perturba as operações**
- > **Serviço de substituição avançada e garantia de hardware de 5 anos**
- > **Recursos e padrões de segurança cibernética de alto nível**



AXIS S2208 Mk II Standalone Appliance

Licenças

8 licenças do AXIS Camera Station Pro Core Device NVR e 10 licenças do AXIS Audio Manager Pro incluídas e vinculadas ao hardware. Podem ser atualizadas com licenças adicionais (vendidas separadamente).

Escalabilidade do sistema

Elegível para até 8 canais de vídeo e 16 portas simultaneamente, com uma taxa de gravação total de até 128 Mbps.
Possibilidade de expansão com dispositivos adicionais usando a série AXIS S30 Recorder Series.
Qualificado para 200 transmissões de áudio simultâneas utilizando o AXIS Audio Manager Pro.
Elegível para até 1.000 portas somente com controle de acesso.

Hardware

Processador

Intel® Core™ i3

Memória

16 GB DDR5 (2x 8 GB)

Armazenamento

Disco rígido para monitoramento
Total de slots para disco rígido: 2
Slot livre para disco rígido: 1
Armazenamento de fábrica: 4 TB (1 x 4 TB)

Switch

8 portas integradas, 135 W de capacidade total de potência
Power over Ethernet (PoE) IEEE 802.3at, Classe 4

Placa de vídeo

Placa gráfica Intel® UHD

Alimentação

Máx. 270 W, 135 W PoE dedicado
100 – 240 VCA, 3,5 A, 50/60 Hz
54 VCC, 5 A
Adaptador de energia externo

Consumo de energia

(Excluindo o consumo de energia dos dispositivos conectados)

Consumo de energia típico: 75 W

Consumo máximo de energia: 95 W

Conectores

Parte frontal:

2x USB 3.2

1x Conector de áudio universal

Switch, parte traseira:

8x PoE RJ45 1 Gbps

1x RJ45 1 Gbps

Servidor, parte traseira:

1x RJ45 1 Gbps

2x USB 2.0

2x HDMI 2.1

Vídeo

Streams de vídeo

Visualização ao vivo no cliente Windows:

1 stream x 4K a 30 FPS

4 divididas x 1080p a 30 FPS*

9 divididas x 720p a 30 FPS*

16 divisões x 360p a 15 FPS

25 divididas x 360p a 15 FPS

36 divisões x 360p a 15 FPS

Qualquer combinação dos itens acima para até dois monitores 4K, exceto para configurações marcadas com *, em que apenas um monitor pode exibir streams a 30 fps.

Compatível com um monitor 8K:

1 stream x 8K a 20 FPS

Atualmente, compatível apenas com 1 stream sem exibições divididas.

Visualização ao vivo no cliente Web (local ou remoto):

1 stream x 8K a 30 FPS

1 stream x 4K a 30 FPS

4 divididas x 1080p a 30 FPS

9 divididas x 720p a 30 FPS*

Qualquer combinação dos itens acima em um monitor 8K e um 4K, exceto para a configuração marcada com *, em que apenas um monitor pode exibir streams a 30 fps.

Divisões adicionais afetarão o desempenho da CPU do servidor. Máximo de 18 fluxos em todos os clientes Web, dependendo do perfil de fluxo.

Reprodução no cliente Windows:

Suporte aos mesmos cenários de divisão que a visualização ao vivo

Recomendado o uso de apenas um monitor, devido à carga do disco ao reproduzir vários streams de vídeo em alta resolução.

A reprodução em alta velocidade pode afetar o desempenho de vídeos.
Reprodução no cliente Web (local ou remoto):
1 stream de até 8K a 30 fps

Aprovações

Marcações de produtos

UL/cUL, BIS, CE, KC, VCCI, RCM, BSMI, FCC, NOM

Cadeia de suprimentos

Compatível com TAA

EMC

EN 55035, EN 55032 Class A
EN 61000-3-2, EN 61000-3-3
Austrália/Nova Zelândia:
RCM AS/NZS CISPR 32 Classe A
Canadá: ICES(A)/NMB(A)
Japão: VCCI Classe A
Coreia: KS C 9835, KS C 9832 Classe A
EUA: FCC Parte 15 Subparte B Classe A
Taiwan: CNS 15936

Proteção

CAN/CSA-C22.2 No. 62368-1 ed. 3,
IEC/EN/UL 62368-1 ed. 3, RCM AS/NZS 62368. 1:2018,
IS 13252

Segurança cibernética

Segurança

Trusted Platform Module (TPM 2.0) com certificação
FIPS 140-2 nível 2, compatível com unidade de sistema
operacional e unidade de gravação criptografadas.
Inicialização segura, firmware de switch assinado

Geral

Sistema operacional

Microsoft® Windows® 11 IoT Enterprise LTSC 2024
Recuperação do sistema operacional: sim
Unidade do sistema operacional: SSD de 256 GB

Condições operacionais

De 0 °C a 40 °C (32 °F a 104 °F)
Umidade: 10 – 90% de umidade relativa (sem
condensação)

Condições de armazenamento

De -40 °C a 65 °C (-40 °F a 149 °F)
Umidade: 10 – 90% de umidade relativa (sem
condensação)

Dimensões

330 x 230 x 78 mm (13 x 9,1 x 3,1 pol.)

Peso

5,8 kg (12,8 lb)

Acessórios incluídos

Abas de rack, adaptador de energia

Acessórios opcionais

Surveillance Hard Drive 6 TB disponível da Axis
Surveillance Hard Drive 4 TB disponível da Axis
AXIS TS2901 Appliance Stand
Terminais desktop Axis

Protetor contra surtos Ethernet Axis
Para obter informações adicionais sobre acessórios,
consulte axis.com

Garantia:

Gravador e disco rígido: garantia de 5 anos, consulte
axis.com/warranty

Controle de exportação

Este produto está sujeito a regulamentações de controle
de exportação e você deve sempre obedecer a todas as
regulamentações nacionais e internacionais aplicáveis
de exportação ou reexportação.

AXIS Camera Station Pro

Para obter detalhes sobre os recursos e funções do AXIS
Camera Station Pro, consulte a folha de dados do AXIS
Camera Station Pro em axis.com

Recursos em destaque

Inicialização segura

A Inicialização segura é um sistema de segurança que garante que somente software aprovado (sistema operacional e firmware incorporado ao switch, quando aplicável) seja executado em um dispositivo Axis na inicialização. Ela usa um processo de inicialização que consiste em uma cadeia ininterrupta de software validado criptograficamente, começando na memória imutável (ROM de inicialização), para verificar a autenticidade do software. Ao estabelecer a cadeia de confiança, a Inicialização segura garante que o dispositivo execute apenas software com uma assinatura digital válida, impedindo a execução de código malicioso no dispositivo e assegurando que o dispositivo seja inicializado apenas com um software assinado.

contribui para proteger o dispositivo contra acesso não autorizado e manipulação.

Para obter mais informações, consulte axis.com/glossary

Firmware assinado

O firmware incorporado ao switch é assinado com certificados digitais, usando uma chave secreta e privada para garantir sua autenticidade e integridade. Isso envolve acrescentar uma assinatura digital à imagem do firmware do dispositivo, que é, então, verificada pelo dispositivo antes da aceitação e da instalação. O processo de verificação confirma se a integridade do software foi comprometida, rejeitando-o em caso de violação. Com base no esquema de assinatura de curva elíptica Ed25519 reconhecido pelo setor, o processo de verificação usa o certificado digital para confirmar se o firmware permanece inalterado e autêntico, garantindo que qualquer manipulação ou violação durante a transmissão seja detectada antes da instalação.

SBOM (Lista de materiais de software)

SBOM é uma lista detalhada de todos os componentes de software incluídos em um produto Axis, inclusive bibliotecas de outros fornecedores e informações de licença. Essa lista fornece aos clientes informações sobre a composição do software do produto, o que facilita o gerenciamento da segurança do software e atende aos requisitos de transparência.

TPM (Trusted Platform Module)

O TPM é um chip de segurança integrado aos dispositivos Axis para fornecer um ambiente seguro para o armazenamento e o processamento de dados confidenciais. Como um componente que fornece um conjunto de recursos criptográficos, o TPM protege as informações contra acesso não autorizado. Especificamente, ele armazena com segurança a chave privada, que nunca deixa o TPM, e processa todas as operações criptográficas relacionadas dentro do próprio módulo. Isso garante que a parte secreta do certificado permaneça segura, mesmo em caso de violação de segurança. Ao operar recursos como criptografia, autenticação e integridade da plataforma, o TPM