

AXIS S2216 Mk II Rack Appliance

Solução de gravação multifuncional com switch PoE integrado

Ideal para instalações de porte maior, esse dispositivo multifuncional para rack inclui 16 licenças do AXIS Camera Station Pro, um switch PoE integrado e armazenamento de 8 TB. Ele é compatível com aplicativos de IA, como a Pesquisa Inteligente 2, e também oferece opções flexíveis de armazenamento e compatibilidade com diversas configurações de RAID (níveis 0/1/5/10). E você pode expandir facilmente o seu sistema usando a série AXIS S30 Recorder Series. Esse gravador é 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**
- > **16 licenças do AXIS Camera Station Pro incluídas**
- > **Opções de armazenamento flexíveis, incluindo RAID**
- > **Serviço de substituição avançada e garantia de hardware de 5 anos**
- > **Recursos e padrões de segurança cibernética de alto nível**

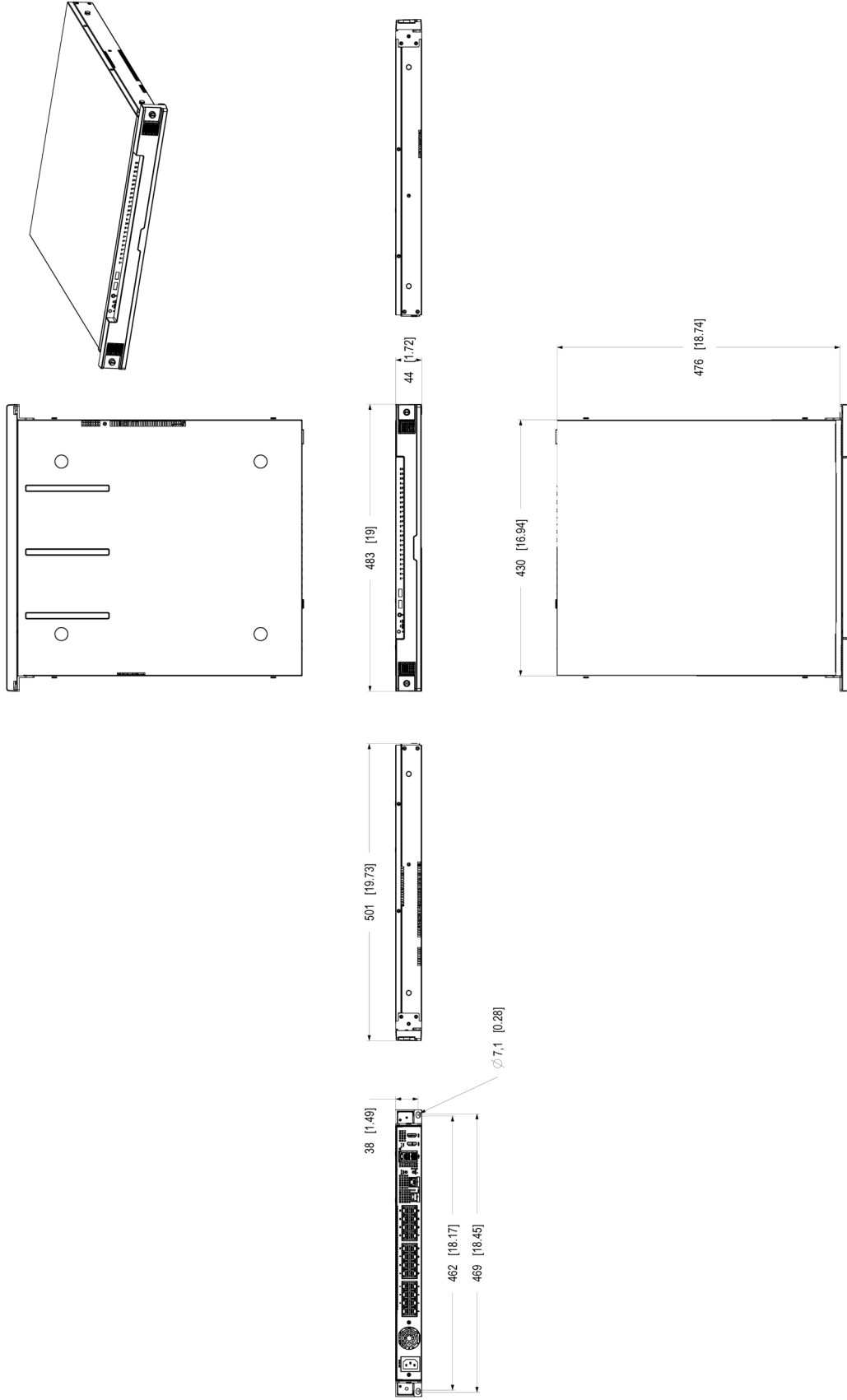


AXIS S2216 Mk II Rack Appliance

Licenças	16 licenças do AXIS Camera Station Pro Core Device NVR incluídas e vinculadas ao hardware. Podem ser atualizadas com licenças adicionais (vendidas separadamente).
Escalabilidade do sistema	Elegível para até 16 canais de vídeo e 32 portas simultaneamente, com uma taxa de gravação total de até 256 Mbps. Possibilidade de expansão com dispositivos adicionais usando a série AXIS S30 Recorder Series. Elegível para até 1.000 portas somente com controle de acesso. Testado com: 10 clientes Windows de visualização ao vivo 2 clientes executando operações pesadas de scrubbing ou reprodução
Hardware	
Processador	Intel® Core™ i3
Memória	16 GB DDR5 (2x 8 GB)
Armazenamento	Disco rígido de categoria de vigilância Total de slots para disco rígido: 4 Slot livre para disco rígido: 2 Armazenamento de fábrica: 8 TB (2 x 4 TB)
RAID	Nível de RAID de fábrica: Não configurado Níveis de RAID suportados: 0, 1, 10
Switch	16 portas integradas, 260 W de capacidade total de potência Power over Ethernet (PoE) IEEE 802.3at, Classe 4
Placa de vídeo	Placa gráfica Intel® UHD
Alimentação elétrica	Máx. 520 W, 260 W PoE dedicado 100 – 240 VCA, 6,5 – 2,5 A, 50/60 Hz
Conectores	Parte frontal: 2x USB 3.2 1x Conector de áudio universal Switch, parte traseira: 16x PoE RJ45 1 Gbps 1x SFP 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 streams em todos os clientes Web, dependendo do perfil de stream. 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
Segurança	CAN/CSA-C22.2 No. 62368-1 ed. 3, IEC/EN/UL 62368-1 ed. 3, RCM AS/NZS 62368.1:2018, IS 13252
Cibersegurança	
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	476 x 440 x 45 mm (18,7 x 17,3 x 1,8 pol.), chassi 1U
Peso	11 kg (24,3 lb)
Acessórios incluídos	Trilhos de rack, cabo de alimentação
Acessórios opcionais	Surveillance Hard Drive 6 TB disponível da Axis Surveillance Hard Drive 4 TB disponível da Axis 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



Dimensions in mm (inch)	
2024 Max-S	W1 L3
2024 Max-S	W1 L3
2024 Max-S	A1 U1

AXIS S2216 / S2224 MKII

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.

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

Para obter mais informações, consulte [axis.com/glossary](https://www.axis.com/glossary)