

AXIS S2224 Mk II Rack Appliance

Komplettaufzeichnungslösung mit integriertem PoE-Switch

Diese Rack-Komplettlösung ist ideal für größere Installationen und umfasst 24 AXIS Camera Station Pro-Lizenzen, einen integrierten PoE-Switch und 12 TB Speicher. Sie unterstützt KI-Anwendungen wie Smart Search 2. Außerdem können Sie Ihr System problemlos mit der Recorder-Serie AXIS S30 erweitern. Dieser Recorder ist mit Software und Tools ausgestattet, die Sie beim Einrichten und Warten Ihres Systems unterstützen. Zum Beispiel die AXIS Recorder Toolbox und ihr intuitiver Installationsassistent. Darüber hinaus bietet es Hochsicherheitsfunktionen und -standards wie ein nach FIPS 140-2 Level 2 zertifiziertes TPM.

- > **Komplettlösung mit integriertem PoE Switch**
- > **24 AXIS Camera Station Pro-Lizenzen im Lieferumfang enthalten.**
- > **Flexible Speicheroptionen einschließlich RAID**
- > **Vorgezogener Austauschservice und 5 Jahre Gewährleistung für die Hardware**
- > **Hohe Cybersicherheitsmerkmale und -standards**



AXIS S2224 Mk II Rack Appliance

Lizenzen

24 AXIS Camera Station Pro Core Device NVR-Lizenzen und 10 AXIS Audio Manager Pro-Lizenzen sind im Lieferumfang enthalten und an die Hardware gebunden. Upgrade mit zusätzlichen Lizenzen möglich (separat erhältlich).

Systemskalierbarkeit

Geeignet für bis zu 24 Videokanäle und 48 Zugänge gleichzeitig mit einer Gesamtaufzeichnungsrate von bis zu 384 Mbps.
Kann bei Verwendung der AXIS S30 Recorder-Serie mit weiteren Geräten skaliert werden.
Geeignet für 200 gleichzeitige Audio-Streams mit AXIS Audio Manager Pro.
Geeignet für bis zu 1.000 Zugänge nur mit Zutrittskontrolle.

Hardware

Prozessor

Intel® Core™ i3

Speicher

16 GB DDR5 (2x 8 GB)

Speicherun- g

RAID

RAID-Level ab Werk: Nicht konfiguriert
Unterstützte RAID-Level: 0, 1, 10

Switch

24 Ports integriert, 260 W Gesamtleistungsbudget
Power over Ethernet (PoE) IEEE 802.3at, Klasse 4

Grafikkarte

Intel® UHD Graphics

Stromversorgung

Max. 520 W, 260 W für den PoE vorgesehen
100 bis 240 V Wechselstrom, 6,5 bis 2,5 A, 50/60 Hz

Leistungsaufnahme

(außer Stromverbrauch von angeschlossenen Geräten)
Nennstromverbrauch: 110 W
Maximale Leistungsaufnahme: 130 W

Anschlüsse

Vorderseite:

2x USB 3.2
1x Audio-Universalbuchse
Switch auf der Rückseite:
24x PoE RJ45 1 GBit/s
1x SFP 1 GBit/s
1x RJ45 1 GBit/s

Server auf der Rückseite:

1x RJ45 1 GBit/s
2x USB 2.0
2 x HDMI 2.1

Video

Video-Streaming

Live-Ansicht im Windows-Client:

1 Stream x 4K bei 30 Bildern/s
4 Split x 1080p bei 30 Bildern/s*
9 Split x 720p bei 30 Bildern/s*
16 Split x 360p bei 15 Bildern/s
25 Split x 360p bei 15 Bildern/s
36 Split x 360p bei 15 Bildern/s
Jede beliebige Kombination der oben genannten Möglichkeiten für bis zu zwei 4K-Monitore, mit Ausnahme der mit * gekennzeichneten Konfigurationen, bei denen nur ein Monitor Videostreams mit 30 Bildern pro Sekunde anzeigen kann.

Unterstützt einen 8K-Monitor:

1 Stream x 8K bei 20 Bildern/s
Derzeit wird nur 1 Videostream ohne geteilte Ansichten unterstützt.

Live-Ansicht im Web-Client (lokal oder entfernt):

1 Stream x 8K bei 30 Bildern/s
1 Stream x 4K bei 30 Bildern/s
4 Split x 1080p bei 30 Bildern/s
9 Split x 720p bei 30 Bildern/s*
Jede beliebige Kombination der oben genannten Funktionen auf einem 8K- und einem 4K-Monitor, mit Ausnahme der mit * gekennzeichneten Konfiguration, bei der nur ein Monitor Videostreams mit 30 Bildern pro Sekunde anzeigen kann.

Größere Splits beeinträchtigen die CPU-Leistung des Servers. Maximal 18 Videostreams über alle Webclients hinweg, je nach Videostreamprofil.

Wiedergabe im Windows-Client:

Unterstützt die gleichen Split-Szenarien wie die Live-Ansicht
Bei der Wiedergabe mehrerer Videostreams mit hohen Videostreamprofilen wird aufgrund der Festplattenbelastung nur ein Monitor empfohlen.

Wiedergabe mit hoher Geschwindigkeit kann die Videoleistung beeinträchtigen.
Wiedergabe im Web-Client (lokal oder entfernt):
1 Videostream bis zu 8K bei 30 Bildern pro Sekunde

Zulassungen

Produktkennzeichnungen

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

Lieferkette

Entspricht TAA

EMV

EN 55035, EN 55032 Class A

EN 61000-3-2, EN 61000-3-3

Australien/Neuseeland: RCM AS/NZS CISPR 32 Klasse A

Kanada: ICES(A)/NMB(A)

Japan: VCCI Klasse A

Korea: KS C 9835, KS C 9832 Class A

USA: FCC Teil 15 Abschnitt B Klasse A

Taiwan: CNS 15936

Sicherheit

CAN/CSA C22.2 Nr. 62368-1 Ausg. 3,

IEC/EN/UL 62368-1 ed. 3, RCM AS/NZS 62368. 1:2018,
IS 13252

Cybersicherheit

Schutz vor Bedrohungen

FIPS 140-2 Level 2 zertifiziertes Trusted Platform
Module (TPM 2.0), das ein verschlüsseltes
Betriebssystem- und Aufzeichnungslaufwerk
unterstützt.

Sicheres Booten, signierte Switch-Firmware

Allgemeines

Betriebssystem

Microsoft® Windows® 11 IoT Enterprise LTSC 2024

Wiederherstellung des Betriebssystems: ja

Laufwerk des Betriebssystems: 256 GB SSD

Betriebsbedingungen

0 °C bis +40 °C (32 °F bis 104 °F)

Relative Luftfeuchtigkeit: 10 bis 90 % (nicht
kondensierend)

Lagerbedingungen

-40 °C bis +65 °C (-40 °F bis +149 °F)

Relative Luftfeuchtigkeit: 10 bis 90 % (nicht
kondensierend)

Abmessungen

476 x 440 x 45 mm, Gehäuse 1U

Gewicht

11 kg

Im Lieferumfang enthaltenes Zubehör

Rackschienen, Netzkabel

Optionales Zubehör

Überwachungs-Festplatte 6 TB erhältlich bei Axis

Überwachungs-Festplatte 4 TB erhältlich bei Axis

Axis Deskopterminals

Axis Ethernet Surge Protector

Weiteres Zubehör finden Sie auf axis.com

Gewährleistung

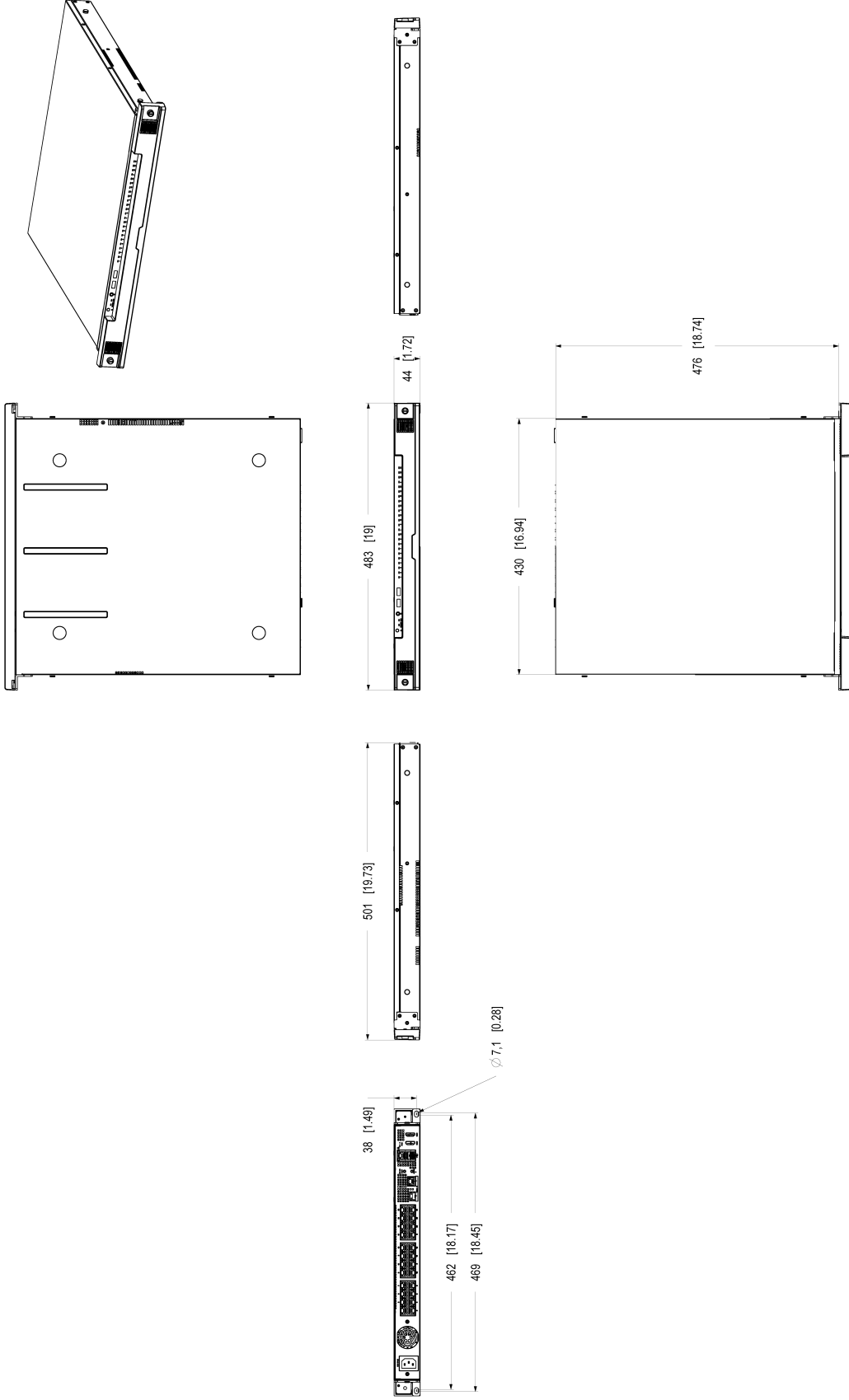
Recorder und Festplatte: 5 Jahre Gewährleistung, siehe
axis.com/warranty

Exportbeschränkungen

Dieses Produkt unterliegt Exportkontrollbestimmungen.
Achten Sie daher bitte stets auf die Einhaltung aller
geltenden nationalen und internationalen Export- bzw.
Re-Exportkontrollbestimmungen.

AXIS Camera Station Pro

Weitere Informationen zu Merkmalen und Funktionen von AXIS Camera Station Pro finden Sie im entsprechenden Datenblatt unter www.axis.com



Hervorgehobene Funktionen

Sicheres Hochfahren

Sicheres Booten ist ein Sicherheitssystem, das gewährleistet, dass nur zugelassene Software (Betriebssystem und ggf. integrierte Switch-Firmware) beim Start auf einem Axis Gerät ausgeführt wird. Es verwendet einen Boot-Prozess, der aus einer ununterbrochenen Kette von kryptografisch validierter Software besteht, die im unveränderlichen Speicher (Boot-ROM) beginnt, um die Authentifizierung der Software zu überprüfen. Durch den Aufbau der Vertrauenskette garantiert Secure Boot, dass das Gerät nur Software mit einer gültigen digitalen Signatur ausführt. Dadurch wird verhindert, dass bösartiger Code auf dem Gerät ausgeführt wird, und es wird sichergestellt, dass das Gerät nur mit einer signierten Software startet.

Signierte Firmware

Die integrierte Firmware des Switches wird mit digitalen Zertifikaten unter Verwendung eines geheimen, privaten Schlüssels signiert, um ihre Authentizität und Integrität zu gewährleisten. Dabei wird das Firmware-Image des Geräts mit einer digitalen Signatur versehen, die dann vom Gerät vor der Annahme und Installation überprüft wird. Der Verifizierungsprozess prüft, ob die Integrität der Software beeinträchtigt ist, und weist sie bei Manipulationen zurück. Auf der Grundlage des in der Industrie anerkannten elliptischen Kurven-Signaturschemas Ed25519 bestätigt der Verifizierungsprozess mit Hilfe des digitalen Zertifikats, dass die Firmware unverändert und authentisch ist, so dass jede Manipulation zur Manipulationserfassung während der Übertragung vor der Installation detektiert wird.

SBOM (Software Bill of Materials)

SBOM ist eine detaillierte Liste aller Software-Komponenten, die in einem Axis Produkt enthalten sind, einschließlich Bibliotheken von Drittanbietern und Lizenzinformationen. Diese Liste gibt den Kunden einen Einblick in die Zusammensetzung der Software des Produkts, was die Verwaltung der Softwaresicherheit und die Erfüllung der Transparenzanforderungen erleichtert.

TPM (Trusted Platform Module)

TPM ist ein in Axis Geräte integrierter Sicherheitschip, der eine sichere Umgebung für die Speicherung und Verarbeitung sensibler Daten bietet. Als Komponente, die eine Reihe von kryptografischen Funktionen bietet, schützt das TPM Informationen vor unbefugtem Zugriff. Insbesondere speichert es den privaten Schlüssel sicher, der das TPM nie verlässt, und verarbeitet alle damit verbundenen kryptografischen Betriebe innerhalb des Moduls selbst. Dadurch wird sichergestellt, dass der geheime Teil des Zertifikats auch im Falle einer

Sicherheitsverletzung sicher bleibt. Indem es Funktionen wie Verschlüsselung, Authentifizierung und Plattformintegrität aktiviert, trägt das TPM dazu bei, das Gerät vor unbefugtem Zugriff und Manipulation zu schützen.

Weitere Informationen finden Sie auf [axis.com/glossary](https://www.axis.com/glossary)