

## AXIS D1110 Video Decoder 4K

4K video decoder with HDMI™ output

This 4K video decoder can be used to display live video in sequence view, and up to 16 video streams in multiview. It offers a cost-effective solution for video monitoring where live video can be displayed without the use of a PC. It can be used with monitors that support HDMI, plus, it can display advertisements or general information with or without audio. Furthermore, it supports both PoE and DC power for fast and easy installation.

- > **4K video with HDMI output**
- > **PoE or DC powered**
- > **Audio out**
- > **Seamless sequencing and multiview**
- > **Intuitive Axis interface**



# AXIS D1110 Video Decoder 4K

## System on chip (SoC)

### Model

i.MX8 QuadPlus

### Memory

2 GB RAM, 1 GB Flash

## Video

### Video compression

H.264/AVC (MPEG-4 Part 10/AVC Baseline, Main and High profile (B-frame and interlaced rendering are not supported))  
H.265/HEVC Main profile

### Frame rate

Up to 60 fps depending on resolution

### Video streaming

Up to 16 streams (eight using VPU, eight using CPU)

### Video output

All formats 16:9:

#### UHD

3840x2160 @25/30 fps (50/60 Hz)

#### FHD 1080p

1920x1080 @50/60 fps (50/60 Hz)

1920x1080 @25/30 fps (50/60 Hz)

#### HD 720p

1280x720 @50/60 fps (50/60 Hz)

#### SD

720x576 @50 fps (50 Hz)

720x480 @60 fps (60 Hz)

## Audio

### Output

Line output, HDMI (stereo)

## Network

### Network protocols

IPv4, IPv6 USGv6, ICMPv4/ICMPv6, HTTP, HTTPS<sup>1</sup>, HTTP/2, TLS<sup>1</sup>, CIFS/SMB, SMTP, mDNS (Bonjour), UPnP®, SNMP, v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, PTP, NTS, RTSP, RTP, RTSPS, TCP, UDP, IGMPv1/v2/v3, RTCP, DHCPv4/v6, SSH, LLDP, CDP, MQTT v3.1.1, Syslog, Link-Local address (ZeroConf), IEEE 802.1X (EAP-TLS), IEEE 802.1AR

## System integration

### Application Programming Interface

Open API for software integration, including VAPIX® and AXIS Camera Application Platform (ACAP); specifications at [axis.com/developer-community](https://axis.com/developer-community)  
One-click cloud connection

### Video management systems

Compatible with AXIS Camera Station Pro, AXIS Camera Station 5, and video management software from Axis' partners available at [axis.com/vms](https://axis.com/vms).

### Event conditions

IP address removed, live stream active, network lost, new IP address, system ready  
Edge storage: storage disruption, storage health issues detected  
I/O: manual trigger, virtual input  
MQTT: stateless  
Scheduled and recurring: schedule

### Event actions

MQTT: publish  
Notification: HTTP, HTTPS, TCP and email  
SNMP traps: send, send while the rule is active  
Status LED: flash, flash while the rule is active

## Approvals

### Product markings

UL/cUL, UKCA, CE, KC, VCCI, RCM

### Supply chain

TAA compliant

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. ([openssl.org](https://openssl.org)), and cryptographic software written by Eric Young ([eyay@cryptsoft.com](mailto:eyay@cryptsoft.com)).

## EMC

CISPR 35, CISPR 32 Class A, EN 55035,  
EN 55032 Class A, EN 61000-3-2, EN 61000-3-3,  
EN 61000-6-1, EN 61000-6-2  
**Australia/New Zealand:** RCM AS/NZS CISPR 32 Class A  
**Canada:** ICES-3(A)/NMB-3(A)  
**Japan:** VCCI Class A  
**Korea:** KS C 9835, KS C 9832 Class A  
**USA:** FCC Part 15 Subpart B Class A

## Safety

IEC/EN/UL 62368-1 ed. 3,  
CAN/CSA C22.2 No. 62368-1 ed. 3

## Environment

IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6,  
IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78,  
IEC/EN 60529 IP30

## Network

NIST SP500-267

## Cybersecurity

ETSI EN 303 645, BSI IT Security Label, FIPS-140

## Cybersecurity

### Edge security

**Software:** Signed OS, brute force delay protection, digest authentication and OAuth 2.0 RFC6749 Client Credential Flow/OpenID Authorization Code Flow for centralized ADFS account management, password protection, Axis Cryptographic Module (FIPS 140-2 level 1)

**Hardware:** Axis Edge Vault cybersecurity platform Secure element (CC EAL 6+), system-on-chip security (TEE), Axis device ID, secure keystore, secure boot, encrypted filesystem (AES-XTS-Plain 256bit)

### Network security

IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2)<sup>2</sup>,  
IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR,  
HTTPS/HSTS<sup>2</sup>, TLS v1.2/v1.3<sup>2</sup>, Network Time Security (NTS), X.509 Certificate PKI, host-based firewall

## Documentation

*AXIS OS Hardening Guide*

*Axis Vulnerability Management Policy*

*Axis Security Development Model*

To download documents, go to [axis.com/support/cybersecurity/resources](https://axis.com/support/cybersecurity/resources)

To read more about Axis cybersecurity support, go to [axis.com/cybersecurity](https://axis.com/cybersecurity)

## General

### Casing

IP30-rated  
Aluminum casing  
Color: NCS S 9000-N  
Security slot

### Mounting

AXIS T91A03 DIN Rail Clip A, mounting bracket, compatible with VESA mounting hole patterns

### Power

Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 2 Class 4  
10–28 V DC, max 17 W

### Connectors

Audio: 3.5 mm line out, stereo  
Data transfer: 2x USB Type A, supported USB class: HID, Mass Storage  
Network: RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE  
Power: DC input, terminal block  
SD-card slot (Highspeed/UHS-1)  
HDMI type A<sup>3</sup>, CEC supported

### Storage

Support for microSD/microSDHC/microSD UHS-1 card

### Operating conditions

0 °C to 40 °C (32 °F to 104 °F)  
Humidity 10–85% RH (non-condensing)

### Storage conditions

–20 °C to 65 °C (–4 °F to 149 °F)  
Humidity 5–95% RH (non-condensing)

### Dimensions

For the overall product dimensions, see the dimension drawing in this datasheet

### Weight

500 g (1.10 lb)

### Box content

Video decoder, installation guide, terminal block connector

2. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (openssl.org), and cryptographic software written by Eric Young (eay@cryptsoft.com).

3. ATC certified

### Optional accessories

AXIS TU9001 Control Board, AXIS Strain Relief TD3901, AXIS T91A03 DIN Rail Clip A, AXIS T8415 Wireless Installation Tool, AXIS Surveillance Cards  
For more accessories, go to [axis.com/products/axis-d1110#accessories](https://axis.com/products/axis-d1110#accessories)

---

### System tools

AXIS Site Designer, AXIS Device Manager, product selector, accessory selector  
Available at [axis.com](https://axis.com)

---

### Languages

English, German, French, Spanish, Italian, Russian, Simplified Chinese, Japanese, Korean, Portuguese, Polish, Traditional Chinese, Dutch, Czech, Swedish, Finnish, Turkish, Thai, Vietnamese

---

### Warranty

5-year warranty, see [axis.com/warranty](https://axis.com/warranty)

---

### Part numbers

Available at [axis.com/products/axis-d1110#part-numbers](https://axis.com/products/axis-d1110#part-numbers)

---

## Sustainability

### Substance control

RoHS in accordance with EU RoHS Directive 2011/65/EU/ and EN 63000:2018  
REACH in accordance with (EC) No 1907/2006. For SCIP UUID, see [echa.europa.eu](https://echa.europa.eu)

---

### Materials

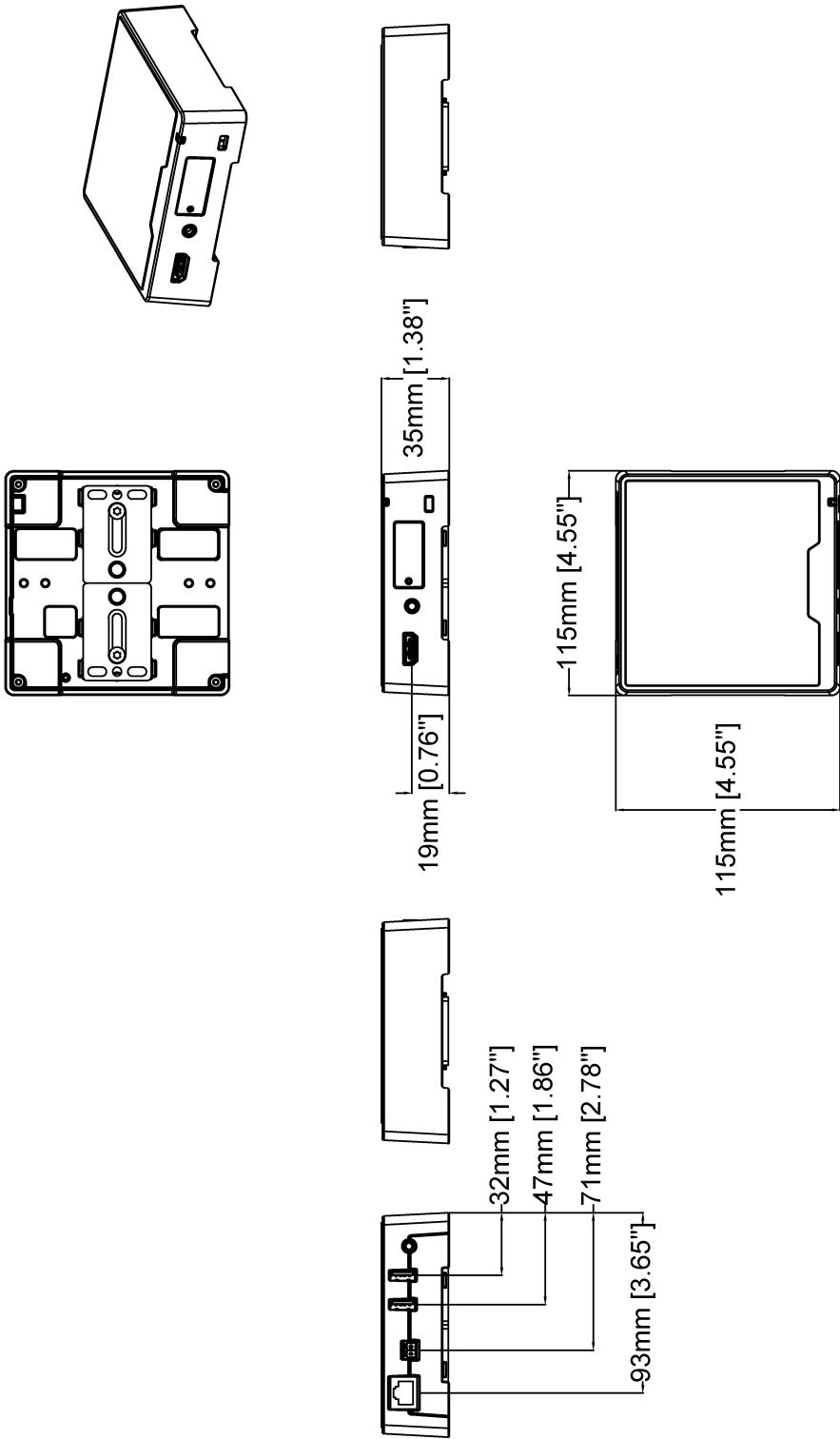
Screened for conflict minerals in accordance with OECD guidelines  
To read more about sustainability at Axis, go to [axis.com/about-axis/sustainability](https://axis.com/about-axis/sustainability)

---

### Environmental responsibility

[axis.com/environmental-responsibility](https://axis.com/environmental-responsibility)  
Axis Communications is a signatory of the UN Global Compact, read more at [unglobalcompact.org](https://unglobalcompact.org)

Dimension drawing



Revision	v.01	Revision date	2021-06-07
Paper size	A4	Release date	2021-06-07
Created by	JSK	Scale	1:3

© 2021 Axis Communications



AXIS D1110 Video Decoder 4K

## Highlighted capabilities

### Axis Edge Vault

Axis Edge Vault is the hardware-based cybersecurity platform that safeguards the Axis device. It forms the foundation that all secure operations depend on and offer features to protect the device's identity, safeguard its integrity and protect sensitive information from unauthorized access. For instance, **secure boot** ensures that a device can boot only with **signed OS**, which prevents physical supply chain tampering. With signed OS, the device is also able to validate new device software before accepting to install it. And the **secure keystore** is the critical building-block for protecting cryptographic information used for secure communication (IEEE 802.1X, HTTPS, Axis device ID, access control keys etc.) against malicious extraction in the event of a security breach. The secure keystore and secure connections are provided through a Common Criteria or FIPS 140 certified hardware-based cryptographic computing module.

To read more about Axis Edge Vault, go to [axis.com/solutions/edge-vault](https://axis.com/solutions/edge-vault).

For more information, see [axis.com/glossary](https://axis.com/glossary)