

AXIS A1210 Network Door Controller

Compact edge-based one door controller

Suitable for installation anywhere, this compact, competitively priced product offers fast and easy installation on walls. Plus, it's suitable for plenum spaces. It includes everything needed to control one door all powered by one PoE cable. With intelligence on the edge, it can internally handle all tasks related to door access—even if the network is down. Fully integrated within Axis end-to-end solutions, this scalable product is optimized for both small and large installations and supports flexible authentication using different types of credentials. Furthermore, with built-in cybersecurity features, it prevents unauthorized access and safeguards your system.

- > **Complete control for one door**
- > **Compact form factor**
- > **Intelligence on the edge**
- > **Built-in cybersecurity features**
- > **Fully integrated within Axis end-to-end solutions**



AXIS A1210 Network Door Controller

Door controller

Readers	Up to 2 OSDP readers (multi-drop) or 1 Wiegand reader per controller OSDP Secure Channel supported OSDP Secure Profile verified Integration with ASSA ABLOY Aperio® wireless lock technologies
Doors	Up to 16 wireless doors
Credentials	Qualified for up to 250 000 credentials stored locally
Event buffer	Qualified for up to 250 000 events stored locally

Power

Power in: 12 V DC, max 36 W, or
Power over Ethernet (PoE) IEEE 802.3at, Type 2 Class 4
Relay: 1x relay NO/NC, max 2 A DC
Power out lock: 12/24 V, jumper configurable
Powered by PoE: max 900 mA at 12 V DC, max 450 mA at 24 V DC
Powered by DC: max 1600 mA at 12 V DC, max 800 mA at 24 V DC
Power out reader: 12 V DC, max 500 mA
Total power budget for peripheral devices (locks, readers etc.):
2100 mA at 12 V if powered by DC, 1400 mA at 12 V if powered by PoE Class 4

I/O interface

Reader	DC output: 12 V, max 500 mA Data: OSDP, Wiegand I/O: Three open drain outputs, max 30 V, 100 mA each One supervised input
Door	DC output: 12/24 V, jumper configurable Power output: See the Power section I/O: REX and door position sensor supervised inputs Output relays: one relay, Form-C contacts: 2 A at 30 V DC, resistive
Auxiliary	DC output: 12 V, 50 mA I/O: Two ports, configurable inputs or outputs
External	External tamper supervised input Alarm supervised input
Supervised input	Configurable input for reader interface, door REX input, door position sensor input, and AUX Programmable end-of-line resistors, 1 K, 2.2 K, 4.7 K and 10 K, 1 %, ¼ watt standard One unsupervised input dedicated for cabinet tamper

Cable requirements

Wire size for connectors: CSA: AWG 28–16, CUL/UL: AWG 30–14
DC power and relay: AWG 18–16
Ethernet and PoE: STP CAT 5e or higher
Reader data (RS485): 1 twisted pair with shield, 120 ohm impedance, qualified for up to 1000 m (3281 ft)
Reader data (Wiegand): Qualified for up to 150 m (500 ft)
Reader powered by controller (RS485): AWG 20–16, qualified for up to 200 m (656 ft)^a
Reader powered by controller (Wiegand): AWG 20–16, qualified for up to 150 m (500 ft)^b
I/Os as inputs: Qualified for up to 200 m (656 ft)

System on chip (SoC)

Memory 512 MB RAM, 2 GB Flash

Network

Network protocols IPv4, IPv6, HTTP, HTTPS^c, TLS^c, QoS Layer 3 DiffServ, SMTP, mDNS (Bonjour), UPnP[®], SNMP v1/v2c/v3 (MIB-II), DNS/DNSv6, DDNS, NTP, RTSP, RTCP, RTP, TCP, UDP, IGMPv1/v2/v3, DHCPv4/v6, SOCKS, SSH, MQTT v3.1.1, Syslog

System integration

Application Programming Interface	Open API for software integration, including VAPIX®, metadata and AXIS Camera Application Platform (ACAP); specifications at axis.com/developer-community . ACAP includes Native SDK. One-click cloud connection
Video management systems	Compatible with AXIS Camera Station, video management software from Axis' Application Development Partners available at axis.com/vms
Tamper detection	Removal of unit cover/tamper front Reader tamper

Tilting, vibration

Approvals

Product markings UL/cUL, KC, EAC, VCCI

Supply chain TAA compliant

EMC EN 55035, EN 55032 Class B, EN 61000-3-2, EN 61000-3-3
Korea: KC KN32 Class B, KC KN35

Safety IEC/EN/UL 62368-1, IEC/EN 60950-1, UL 2043, UL 294

Cybersecurity

Edge security Software: Signed firmware, brute force delay protection, digest authentication, password protection
Hardware: Axis Edge Vault cybersecurity platform
Secure element (CC EAL 6+), secure keystore, secure boot

Network security IEEE 802.1X (EAP-TLS)^c, IEEE 802.1AR, HTTPS/HSTS^c, TLS v1.2/v1.3^c, Network Time Security (NTS), X.509 Certificate PKI, IP address filtering

Documentation *AXIS OS Hardening Guide*
Axis Vulnerability Management Policy
Axis Security Development Model
To download documents, go to axis.com/support/cybersecurity/resources
To read more about Axis cybersecurity support, go to axis.com/cybersecurity

General

Casing Aluminum
Color: white NCS S 1002-B

Mounting Wall mount
DIN rail mount

Connectors Network: Shielded RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE
I/O: Terminal blocks for DC power, inputs/outputs, RS485/Wiegand, relay. Detachable and color coded connectors for ease of installation.
Wire size for connectors: CSA: AWG 28–16, CUL/UL: AWG 30–14

Operating conditions 0 °C to 70 °C (32 °F to 158 °F)
Humidity 20–85% RH (non-condensing)

Storage conditions -40 °C to 70 °C (-40 °F to 158 °F)

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

Weight 645 g (1.4 lb)

Box content door controller, installation guide, connector kit (mounted), grounding kit, cable ties

Optional accessories AXIS TA4701 Access Card
AXIS TA4702 Key Fob
AXIS TA1801 Top Cover
AXIS TA1901 DIN Rail Clip
AXIS TA1902 Access Control Connector Kit^d
AXIS TQ1808-VE Surveillance Cabinet^d
AXIS 30 W Midspan^d
AXIS 30 W Midspan AC/DC^d
AXIS T8006 PS12^d
For more accessories, go to axis.com/products/axis-a1210

System tools AXIS Site Designer, AXIS Device Manager, product selector, accessory selector
Available at axis.com

Languages English, German, French, Spanish, Italian, Russian, Simplified Chinese, Japanese, Korean, Portuguese, Polish, Traditional Chinese

Warranty 5-year warranty, see axis.com/warranty

Part numbers Available at axis.com/products/axis-a1210#part-numbers

Sustainability

Substance control PVC free, BFR/CFR free in accordance with JEDEC/ECA Standard J5709
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

Materials Screened for conflict minerals in accordance with OECD guidelines

To read more about sustainability at Axis, go to axis.com/about-axis/sustainability

**Environmental
responsibility**

axis.com/environmental-responsibility
Axis Communications is a signatory of the UN Global Compact, read more at unglobalcompact.org

- a. *Depending on the reader's voltage and current input range. Evaluated with A4020-E and A4120-E.*
- b. *Depending on the reader's voltage and current input range.*
- c. *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).*
- d. *Not intended for UL 294*

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 offers features to protect the device's identity, safeguard its integrity from factory and protect sensitive information from unauthorized access.

Establishing the root of trust starts at the device's boot process. In Axis devices, the hardware-based mechanism **secure boot** verifies the operating system (AXIS OS) that the device is booting from. AXIS OS, in turn, is cryptographically signed (**signed firmware**) during the build process. Secure boot and signed firmware tie into each other and ensure that the firmware has not been tampered with during the lifecycle of the device and that the device only boots from authorized firmware. This creates an unbroken chain of cryptographically validated software for the chain of trust that all secure operations depend on.

From a security aspect, 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 is provided through a Common Criteria and/or FIPS 140 certified hardware-based cryptographic computing module. Depending on security requirements, an Axis device can have either one or multiple such modules, like a TPM 2.0 (Trusted Platform Module) or a secure element, and/or a system-on-chip (SoC) embedded Trusted Execution Environment (TEE).

To read more about Axis Edge Vault, go to axis.com/solutions/edge-vault.

For more information, see axis.com/glossary