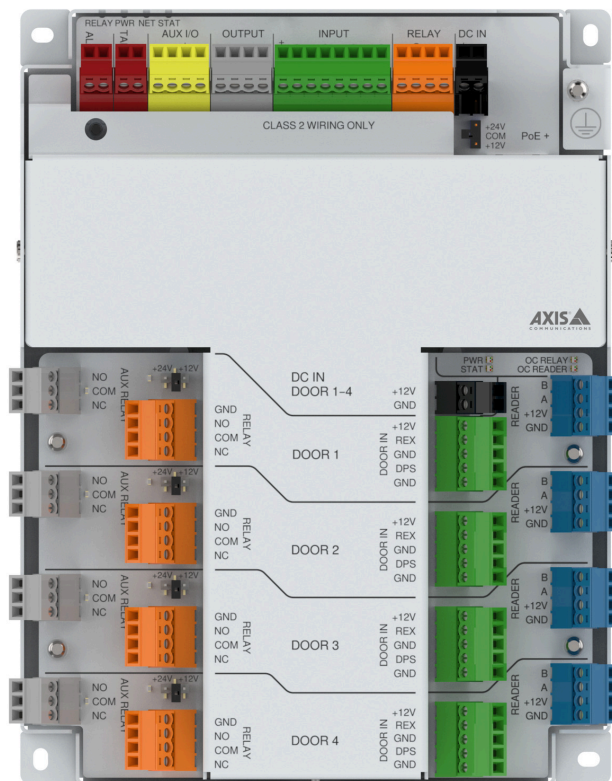


AXIS A1710-B Network Door Controller

Slogan

Ce contrôleur de portes multiples offre un contrôle complet pour un maximum de quatre portes, avec prise en charge de huit lecteurs OSDP et de huit verrous. Idéal pour les nouvelles installations centralisées et les adaptations d'installations avec des armoires Axis ou d'autres fournisseurs. Il occupe moins d'espace que la plupart des contrôleurs de porte du marché. La gestion intégrée de l'alimentation du verrou simplifie l'installation. Avec la prise en charge des lecteurs OSDP et un accessoire optionnel pour les lecteurs Wiegand, ce contrôleur de porte évolutif est optimisé pour les petites et grandes installations. Il peut être utilisé avec AXIS Camera Station Secure Entry ou des solutions partenaires pour fournir un système de gestion vidéo et de contrôle d'accès tout-en-un.

- > **Contrôle centralisé qui simplifie l'installation**
- > **Contrôle total jusqu'à quatre portes**
- > **Prise en charge intégrée de huit lecteurs OSDP et de huit verrous**
- > **Validé OSDP pour une communication sécurisée avec le lecteur**
- > **Fonctions de cybersécurité intégrées**



AXIS A1710-B Network Door Controller

Contrôleur de porte		Système sur puce	
Lecteurs	Jusqu'à 8 lecteurs OSDP (multipoints) par contrôleur Canal sécurisé OSDP pris en charge	Flash	RAM de 512 Mo, mémoire flash de 2 Go
Portes	4 portes, deux relais prenant en charge les doubles verrouillages par porte Possibilité d'intégrer jusqu'à 16 serrures sans fil ASSA ABLOY Aperio ^{®f}	Réseau	Protocoles réseau IPv4, IPv6, HTTP, HTTP ^s , 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
Identifiants	Qualifié pour obtenir jusqu'à 250 000 accréditations stockées localement	Intégration système	
Tampon d'événements	Qualifié pour obtenir jusqu'à 250 000 événements stockés localement	Application Programming Interface (interface de programmation d'applications)	API ouverte pour l'intégration de logiciels, avec VAPIX [®] , métadonnées et AXIS Camera Application Platform (ACAP) ; caractéristiques disponibles sur axis.com/developer-community . ACAP inclut un SDK natif. Connexion au cloud en un clic
Alimentation		Détection de sabotage	Anti-détérioration du lecteur Inclinaison, vibration
Entrée	Power over Ethernet (PoE) IEEE 802.3at, Type 2 Classe 4 ou Entrée CC : 12 V CC, max. 36 W Entrée CC PORTE 1-4 : 12 V CC, max. 100 W (requis)	Agréments	
Interface E/S		Marquages de produit	CE, FCC, ICES, KC, RCM, UL/cUL, VCCI, DEEE
Lecteur	Sortie PORTE 1-4 ^a : 4 sorties 12 V CC, total combiné max. 2 A Données : 4x OSDP/RS485 half-duplex, multipoint Sortie PORTE 1-4 ^a : 4 sorties 12 V CC, total combiné max. 400 mA Entrée PORTE 1-4 : 4 capteurs REX (Request to Exit) et 4 capteurs de position de porte, entrée numérique 0 à max 30 V CC, possibilité de supervision entre 0-12 V CC (4 états)	Chaîne d'approvisionnement	
Relais	RELAIS : 1 relais type C, NO/NF Sec : max. 2 A à 30 V CC Humide : sortie CC ^a : 12/24 V CC, cavalier configurable Avec PoE : max. 150 mA à 12 V CC, max. 50 mA à 24 V CC, max. 1,8 W Avec PoE+ : max. 920 mA à 12 V CC, max. 420 mA à 24 V CC, max. 11,04 W Avec Entrée CC : max. 1900 mA à 12 V CC, max. 1000 mA à 24 V CC, max. 24 W RELAIS PORTE 1-4 : 4 de type C NO/NF Sec : max. 5 A à 30 V CC Humide : sortie CC ^a : 12/24 V CC, configurable par cavaliers, total combiné max. 3,8 A à 12 V CC ou max. 1,5 A à 24 V CC, max. 46 W AUX. PORTE 1-4 : 4 relais de type C, NO/NF Sec : max. 2 A à 30 V CC	Conforme aux exigences de la TAA	
E/S numérique	Connecteur d'entrée 3 entrées numériques, 0-30 V CC, possibilité de supervision entre 0-12 V CC (4 états) 1x sortie 12 V CC ^a , max 200 mA Connecteur de sortie 3 sorties numériques ^a , drain ouvert, 0-30 V CC, max. 100 mA Connecteur d'E/S AUX. 2 entrées ou sorties configurables Entrée : numérique, 0-30 V CC, possibilité de supervision entre 0-12 V CC (4 états) Sortie ^a : drain ouvert, 0-30 V CC, max. 100 mA 1x sortie 12 V CC ^a , max 250 mA	CEM	
Externe	1 entrée numérique pour détection de sabotage externe, 0-30 V CC, possibilité de supervision entre 0-12 V CC (4 états) 1 entrée numérique pour alarme, 0-30 V CC, possibilité de supervision entre 0-12 V CC (4 états)	CISPR 35, CISPR 32 Classe A, EN 55035, EN 55032 Classe A, EN 50130-4, EN 61000-6-1, EN 61000-6-2 Australie/Nouvelle-Zélande : RCM AS/NZS CISPR 32 Classe A Canada : ICES(A)/NMB(A) Japon : VCCI Classe A Corée : KS C 9835, KS C 9832 Classe A États-Unis : FCC partie 15 - sous-partie B, Classe A	
Entrée supervisée	Entrée configurable pour détection de sabotage, alarme, I1-I3, REX, DPS et AUX IO Résistances de fin de ligne programmables (connexion en série : 1 K, 2,2 K, 4,7 K et 10 K, connexion parallèle : 4,7 K et 22 K), 1 %, ¼ watt standard 1 entrée supervisée dédiée au sabotage de l'armoire	Environnement	
Exigences relatives aux câbles		IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-6, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-78	
Diamètre de conducteur pour les connecteurs : CUL/UL : AWG 30-14 Alimentation CC : AWG 16-14, qualifié jusqu'à 3 m (10 pi) Relais : AWG 16-14, qualifié jusqu'à 200 m (656 pi) Ethernet et PoE : STP CAT 5e ou une version supérieure Données du lecteur (RS485) : 1 paire torsadée, AWG 26-14, qualifié jusqu'à 1000 m Lecteur alimenté par contrôleur (RS485) : AWG 20-14, qualifié jusqu'à 200 m ^b E/S comme entrées : AWG 24-14, qualifié jusqu'à 200 m		Sécurité	
		CAN/CSA C22.2 No. 62368-1 éd. 3, IEC/EN/UL 62368-1 éd. 3, RCM AS/NZS 62368.1:2022, UL 2043	
		Cybersécurité	
		ETSI EN 303 645	
		Sécurité locale	
		Logiciel : firmware signé, protection contre les attaques par force brute, authentification Digest, protection par mot de passe Matériel : Plateforme de cybersécurité Axis Edge Vault Élément sécurisé (CC EAL 6+), keystore sécurisé, démarrage sécurisé	
		Sécurité réseau	
		IEEE 802.1X (EAP-TLS) ^c , IEEE 802.1AR, HTTPS/HSTS ^c , TLS v1.2/v1.3 ^c , sécurité de l'heure réseau (NTS), IGC de certification X.509, filtrage d'adresse IP	
		Documentation	
		<i>Guide de protection d'AXIS OS</i> <i>Politique de gestion des vulnérabilités d'Axis</i> <i>Modèle de développement de sécurité Axis</i> Nomenclature logicielle d'AXIS OS Pour télécharger des documents, rendez-vous sur axis.com/support/cybersecurity/resources Pour en savoir plus sur la prise en charge de la cybersécurité Axis, rendez-vous sur axis.com/cybersecurity	
		Général	
		Boîtier	
		Acier Couleur : blanc NCS S 1002-B	
		Fixation	
		Montage sur rail DIN, montage en armoire ^d	
		Connecteurs	
		Réseau : Câble RJ45 10BASE-T/100BASE-TX/1000BASE-T PoE blindé E/S : Blocs terminaux pour l'alimentation CC, entrées/sorties, RS485, relais. Connecteurs détachables et à codes couleurs pour une installation simple. Taille des fils pour les connecteurs : CUL/UL : AWG 30-14	
		Conditions de fonctionnement	
		-40 °C à 55 °C (-40 °F à 131 °F) Température maximale conditionnelle ^e : 70 °C (158 °F) UL 294 : 0 °C à 55 °C (32 °F à 131 °F) Humidité relative 10 % à 85 % (sans condensation)	
		Conditions de stockage	
		-40 °C à 70 °C (-40 °F à 158 °F) Humidité relative de 5 à 95 % (sans condensation)	

PRÉALABLE Fiche technique

Dimensions	Pour obtenir les dimensions du produit dans son ensemble, voir le plan coté dans cette fiche technique.
Poids	880 g (1,9 lb)
Contenu de la boîte	contrôleur de porte, guide d'installation, kit de connexion (monté), kit de mise à la terre, connecteurs pour épissures
Accessoires en option	AXIS TA4711 Access Card AXIS TA4712 Key Fob AXIS TA1901 DIN Rail Clip AXIS TA1902 Access Control Connector Kit ^f AXIS 30 W Midspan AXIS 30 W Midspan AC/DC ^f AXIS T8006 PS12 ^f Pour en savoir plus sur les accessoires, rendez-vous sur axis.com/products/axis-a1710-b
Outils système	AXIS Site Designer, AXIS Device Manager, sélecteur de produits, sélecteur d'accessoires Disponible sur axis.com
Langues	Anglais, Allemand, Français, Espagnol, Italien, Russe, Chinois simplifié, Japonais, Coréen, Portugais, Polonais, Chinois traditionnel
Garantie	Garantie de 5 ans, voir axis.com/warranty
Références	Disponible sur axis.com/products/axis-a1710-b#part-numbers

Écoresponsabilité

Contrôle des substances	Sans PVC RoHS conformément à la directive de l'UE RoHS 2011/65/EU/ et EN 63000:2018 REACH conformément à la directive (CE) n° 1907/2006. Pour l'UUID SCIP, voir echa.europa.eu .
Matériaux	Vérification conformément aux lignes directrices de l'OCDE concernant le devoir de diligence pour les chaînes d'approvisionnement en minerais provenant de zones de conflit Pour en savoir plus sur le développement durable chez Axis, rendez-vous sur axis.com/about-axis/sustainability
Responsabilité environnementale	axis.com/environmental-responsibility Axis Communications est signataire du Pacte mondial des Nations unies ; pour en savoir plus, accédez à unglobalcompact.org

a. *Toutes les sorties sont dotées de circuits de protection contre les surintensités avec réessai automatique.*

b. *En fonction de la plage d'entrée de tension et de courant du lecteur. Évalué avec A4020-E et A4120-E.*

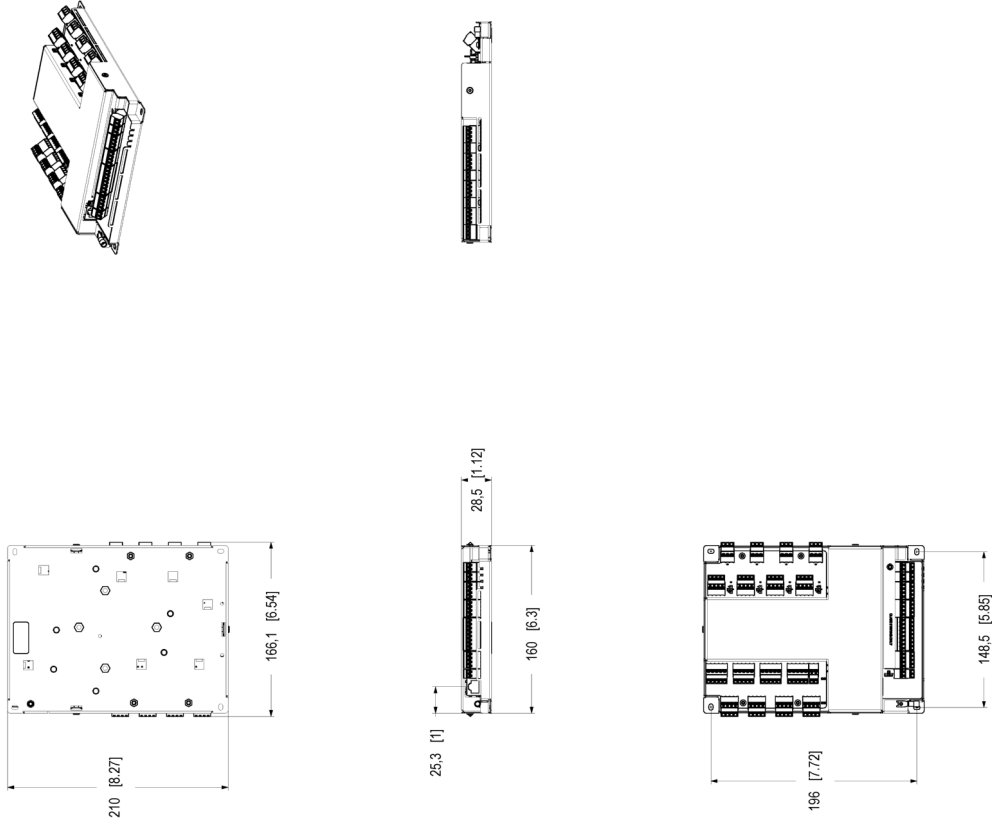
c. *Ce produit comprend des logiciels développés par le projet OpenSSL pour une utilisation dans la boîte à outils OpenSSL (openssl.org), ainsi qu'un logiciel de cryptographie développé par Eric Young (eyay@cryptsoft.com).*

d. *Doit être monté dans un boîtier UL 294 avec interrupteur antisabotage.*

e. *Entrée CC uniquement comme source d'alimentation. Le ou les verrous doivent être alimentés de manière externe. Contact sec uniquement.*

f. *Non prévu pour UL 294*

Plan coté



Dimensions in mm [inches]
2024 Nov 05
11/18/2025

AXIS A1710-B Network Door Controller

Fonctionnalités en surbrillance

Axis Edge Vault

Axis Edge Vault est la plate-forme de cybersécurité matérielle qui protège les périphériques Axis. Elle constitue la base sur qui reposent toutes les opérations sécurisées et offre des fonctions qui protègent l'identité de l'appareil, préservent son intégrité et protègent les informations sensibles contre tout accès non autorisé. Par exemple, le **démarrage sécurisé** garantit qu'un appareil ne peut démarrer qu'avec un **SE signé**, ce qui empêche toute manipulation physique de la chaîne d'approvisionnement. Avec le système d'exploitation signé, le périphérique est aussi capable de valider un nouveau logiciel de dispositif avant d'accepter son installation. Et le **keystore sécurisé** est un élément clé

de la protection des informations cryptographiques utilisées dans le cadre des communications sécurisées (IEEE 802.1X, HTTPS, identifiant de périphérique Axis, clés de contrôle d'accès, etc.) contre toute extraction malveillante en cas de faille. Le keystore sécurisé et des connexions sécurisées sont mis en œuvre via un module de calcul cryptographique basé sur du matériel certifié FIPS 140 et conforme aux critères courants.

Pour en savoir plus sur Axis Edge Vault, rendez-vous sur axis.com/solutions/edge-vault.

Pour en savoir plus, voir axis.com/glossary