

## Controlador de accesos en red **AXIS A1210 Network Door Controller**

### Controlador de puerta compacto basado en el extremo

Este producto compacto con un precio competitivo, apto para instalarse en cualquier lugar, permite una instalación rápida y sencilla en paredes. Además, es apto para espacios de falsos techos. Incluye todo lo necesario para controlar una puerta, todo ello alimentado por un cable PoE. Gracias a la inteligencia en el extremo, puede gestionar internamente todas las tareas relacionadas con el acceso a las puertas, aunque la red esté caída. Este producto ampliable, completamente integrado dentro de las soluciones integrales de Axis, está optimizado para instalaciones tanto pequeñas como grandes y admite una autenticación flexible que utiliza distintos tipos de credenciales. Por otro lado, con funciones de ciberseguridad integradas, previene el acceso no autorizado y protege el sistema.

- > **Control completo de una puerta**
- > **Forma compacta**
- > **Inteligencia en el extremo**
- > **Características de ciberseguridad integradas**
- > **Completamente integrada dentro de las soluciones integrales de Axis**



# Controlador de accesos en red AXIS A1210 Network Door Controller

## Controlador de puerta

<b>Lectores</b>	Hasta 2 lectores OSDP (multiconexión) o 1 lector Wiegand por controlador Compatibilidad con el canal seguro OSDP OSDP Secure Profile verificado Integración con las tecnologías de cierre inalámbrico ASSA ABLOY Aperio®
<b>Puertas</b>	Hasta 16 puertas inalámbricas
<b>Credenciales</b>	Apto para un máximo de 250 000 credenciales almacenadas localmente
<b>Búfer de eventos</b>	Apto para un máximo de 250 000 eventos almacenados localmente

## Alimentación

Entrada de alimentación: 12 V CC, máx. 36 W, o alimentación a través de Ethernet (PoE) IEEE 802.3at, Tipo 2 Clase 4  
Relé: 1x relé NO/NC, máx. 2 A CC  
Bloqueo de salida de alimentación: 12/24 V, puente configurable  
Alimentado por PoE: máx. 900 mA a 12 V CC, máx. 450 mA a 24 V CC  
Alimentación CC: máx. 1600 mA a 12 V CC, máx. 800 mA a 24 V CC  
Lector de salida de alimentación: 12 V CC, máx. 500 mA  
Potencia disponible total para dispositivos periféricos (cerraduras, lectores, etc.): 2100 mA a 12 V con alimentación de CC, 1400 mA a 12 V con alimentación a través de PoE Clase 4

## Interfaz de E/S

<b>Lector</b>	Salida de CC: 12 V, máx 500 mA Datos: OSDP, Wiegand E/S: Tres salidas de colector abierto, máx. 30 V, 100 mA cada una Una entrada supervisada
<b>Door (Puerta)</b>	Salida de CC: 12/24 V, puente configurable Salida de alimentación: Consulte la sección Alimentación E/S: Entradas supervisadas de sensor de posición de puerta y REX Relés de salida: un relé, contactos con forma de C: 2 A a 30 V CC, resistente
<b>Auxiliar</b>	Salida de CC: 12 V, 50 mA E/S: Dos puertos, entradas o salidas configurables
<b>Externa</b>	Entrada supervisada de manipulación externa Entrada supervisada de alarma
<b>Entrada supervisada</b>	Entrada configurable para la interfaz del lector, entrada REX de puerta, entrada del sensor de posición de puerta y AUX Resistencias de final de línea programables, 1 K, 2,2 K, 4,7 K y 10 K, 1 %, estándar de 1/4 vatio Una entrada no supervisada, dedicada a la manipulación del armario

## Requisitos de cable

Tamaño del cable para los conectores: CSA: AWG 28–16, CUL/UL: AWG 30–14  
Alimentación CC y relé: AWG 18–16  
Ethernet y PoE: STP CAT 5e o superior  
Datos de lector (RS485): 1 par trenzado con blindaje, impedancia de 120 ohm, con capacidad para un máximo de 1000 m  
Datos del lector (Wiegand): Con capacidad para un máximo de 150 m  
Lector alimentado por controlador (RS485): AWG 20–16, con capacidad para un máximo de 200 m<sup>3</sup>  
Lector alimentado por controlador (Wiegand): AWG 20–16, con capacidad para un máximo de 150 m<sup>3</sup>  
E/S como entradas: Con capacidad para un máximo de 200 m

## Sistema en chip (SoC)

**Memoria** 512 MB de RAM, 2 GB de Flash

## Red

**Protocolos de red** IPv4, IPv6, HTTP, HTTPS, TLS, 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

## Integración del sistema

<b>Interfaz de programación de aplicaciones</b>	API abierta para la integración de software, incluidos VAPIX®, metadatos y AXIS Camera Application Platform (ACAP); las especificaciones están disponibles en <a href="http://axis.com/developer-community">axis.com/developer-community</a> . La ACAP incluye Native SDK. Conexión a la nube con un solo clic
<b>Sistemas de gestión de video</b>	Compatible con AXIS Camera Station y el software de gestión de video de socios desarrolladores de aplicaciones de Axis disponible en <a href="http://axis.com/vms">axis.com/vms</a> .
<b>Detección de manipulaciones</b>	Desmontaje de la cubierta de la unidad/manipulación de la parte frontal Manipulación del lector Movimiento vertical, vibración

## Homologaciones

<b>Marcas de productos</b>	UL/cUL, KC, EAC, VCCI
<b>Cadena de suministro</b>	Cumple los requisitos de TAA
<b>EMC</b>	EN 55035, EN 55032 Clase B, EN 61000-3-2, EN 61000-3-3 Corea: KC KN32 Clase B, KC KN35
<b>Seguridad</b>	IEC/EN/UL 62368-1, IEC/EN 60950-1, UL 2043, UL 294

## Ciberseguridad

<b>Seguridad perimetral</b>	<b>Software:</b> Firmware firmado, protección contra retrasos de fuerza bruta, autenticación Digest, protección con contraseña <b>Hardware:</b> Plataforma de ciberseguridad Axis Edge Vault Elemento seguro (CC EAL 6+), almacén de claves seguro, arranque seguro
<b>Seguridad de red</b>	IEEE 802.1X (EAP-TLS) <sup>c</sup> , IEEE 802.1AR, HTTPS/HSTS <sup>c</sup> , TLS v1.2/v1.3 <sup>c</sup> , Network Time Security (NTS), certificado PKI X.509 y filtrado de direcciones IP
<b>Documentación</b>	<i>Guía de seguridad de sistemas de AXIS OS</i> <i>Política de gestión de vulnerabilidades de Axis</i> <i>Modelo de desarrollo de la seguridad de Axis</i> Para descargar documentos, vaya a <a href="http://axis.com/support/cybersecurity/resources">axis.com/support/cybersecurity/resources</a> Para obtener más información sobre el servicio de asistencia para ciberseguridad de Axis, ir a <a href="http://axis.com/cybersecurity">axis.com/cybersecurity</a>

## General

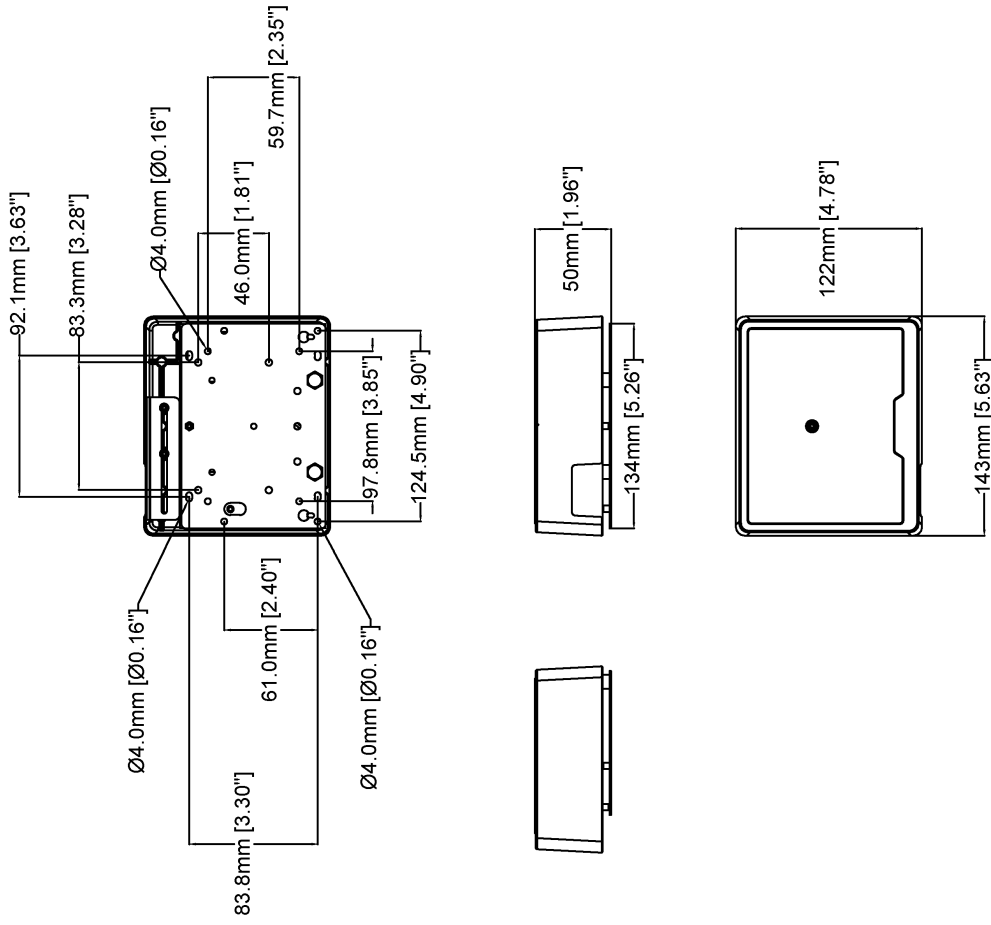
<b>Carcasa</b>	Aluminio color: Blanco NCS S 1002-B
<b>Montaje</b>	Montaje en pared Montaje en carril DIN
<b>Conectores</b>	Red: PoE apantallado RJ45 10BASE-T/100BASE-TX/1000BASE-T E/S: Bloques de terminales para alimentación CC, entradas/salidas, RS485/Wiegand, relé. Conectores desmontables con códigos de color para una instalación sencilla. Tamaño del cable para los conectores: CSA: AWG 28–16, CUL/UL: AWG 30–14
<b>Condiciones de funcionamiento</b>	0 °C a 70 °C (32 °F a 158 °F) Humedad relativa del 20 al 85 % (sin condensación)
<b>Condiciones de almacenamiento</b>	De -40 °C a 70 °C
<b>Dimensiones</b>	Para obtener información sobre las dimensiones generales del producto, consulte el dibujo de dimensiones de la hoja de datos.
<b>Peso</b>	645 g
<b>Contenido de la caja</b>	controlador de puerta, guía de instalación, kit de conectores (instalados), kit de conexión a tierra, abrazaderas para cables

<b>Accesorios opcionales</b>	<p>AXIS TA4701 Access Card          AXIS TA4702 Key Fob          AXIS TA1801 Top Cover          AXIS TA1901 DIN Rail Clip          Kit de conector de control de acceso AXIS TA1902<sup>d</sup>          AXIS TQ1808-VE Surveillance Cabinet<sup>d</sup>          AXIS 30 W Midspan<sup>d</sup>          AXIS 30 W Midspan AC/DC<sup>d</sup>          AXIS T8006 PS12<sup>d</sup>          Para obtener más información sobre accesorios, vaya a <a href="http://axis.com/products/axis-a1210">axis.com/products/axis-a1210</a>.</p>
<b>Herramientas de sistema</b>	<p>AXIS Site Designer, AXIS Device Manager, selector de productos, selector de accesorios          Disponibles en <a href="http://axis.com">axis.com</a></p>
<b>Idiomas</b>	<p>Inglés, alemán, francés, español, italiano, ruso, chino simplificado, japonés, coreano, portugués, polaco, chino tradicional</p>
<b>Garantía</b>	<p>Garantía de 5 años; consulte <a href="http://axis.com/warranty">axis.com/warranty</a></p>
<b>Referencias</b>	<p>Disponible en <a href="http://axis.com/products/axis-a1210#part-numbers">axis.com/products/axis-a1210#part-numbers</a></p>

<b>Sostenibilidad</b>	
<b>Control de sustancias</b>	<p>Sin PVC, sin BFR/CFR de conformidad con la norma JEDEC/ECA, JS709          RoHS de conformidad con la directiva europea RoHS 2011/65/UE y EN 63000:2018          REACH de conformidad con (CE) no 1907/2006. Para SCIP UUID, consulte <a href="http://echa.europa.eu">echa.europa.eu</a></p>
<b>Materiales</b>	<p>Se ha evaluado para encontrar minerales en conflicto de acuerdo con las guías de la OCDE          Para obtener más información sobre la sostenibilidad en Axis, vaya a <a href="http://axis.com/about-axis/sustainability">axis.com/about-axis/sustainability</a></p>
<b>Responsabilidad medioambiental</b>	<p><a href="http://axis.com/environmental-responsibility">axis.com/environmental-responsibility</a>          Axis Communications es firmante del Acuerdo Mundial de las Naciones Unidas, lea más en <a href="http://unglobalcompact.org">unglobalcompact.org</a></p>

a. Según el rango de entrada de corriente y tensión del lector. Evaluado con A4020-E y A4120-E.  
b. Según el rango de entrada de corriente y tensión del lector.  
c. Este producto incluye software desarrollado por OpenSSL Project para su uso en el kit de herramientas OpenSSL. ([openssl.org](http://openssl.org)) y software criptográfico escrito por Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).  
d. No indicado para UL 294

# Esquemas de dimensiones



Revision	v.01	Revision date	2022-11-16
Paper size	A4	Release date	2022-11-16
Created by	MF	Scale	1:4

## Funciones destacadas

### Axis Edge Vault

Axis Edge Vault es la plataforma de ciberseguridad basada en hardware que protege el dispositivo Axis. Constituye la base de la que dependen todas las operaciones seguras y ofrece características para proteger la identidad del dispositivo, proteger su integridad de fábrica y proteger la información confidencial frente a accesos no autorizados.

La base de la confianza comienza en el proceso de arranque del dispositivo. En los dispositivos Axis, el mecanismo de **arranque seguro** basado en hardware verifica el sistema operativo (AXIS OS) desde el que se está iniciando el dispositivo. El SO de AXIS, a su vez, tiene firma criptográfica (**firmware firmado**) durante el proceso de compilación. El arranque seguro y el firmware firmado están vinculados entre sí; se aseguran de que no se haya manipulado el firmware durante el ciclo de vida del dispositivo y que el dispositivo solo arranque con firmware autorizado. De este modo se crea una cadena de software validado criptográficamente para la cadena de confianza de la que dependen todas las operaciones seguras.

Desde un aspecto de seguridad, la **pulsación de tecla segura** es la pieza clave para proteger la información criptográfica que se utiliza para una comunicación segura (IEEE 802.1X, HTTPS, ID de dispositivo Axis, claves de control de acceso, etc.) contra la extracción maliciosa en caso de una infracción de la seguridad. La pulsación de tecla segura se proporciona a través de un módulo de cálculo criptográfico basado en hardware certificado por FIPS 140 o criterios comunes. En función de los requisitos de seguridad, un dispositivo Axis puede tener uno o varios de estos módulos, como un TPM 2.0 (Módulo de plataforma de confianza) o un elemento seguro, o un entorno de ejecución de confianza (TEE) integrado en el sistema en un chip (SoC).

Para obtener más información sobre Axis Edge Vault, vaya a [axis.com/solutions/edge-vault](https://axis.com/solutions/edge-vault).

Para obtener más información, consulte [axis.com/glossary](https://axis.com/glossary)