

## Plataforma de seguridad Armatura One

Plataforma de seguridad iBMS versátil basada en web



Armatura One es la última plataforma de seguridad basada en web "Todo en Uno" desarrollada por Armatura. Contiene múltiples módulos integrados: Personal, Control de acceso, módulo de tiempo y asistencia, Ascensor, Gestión de Visitantes, Gestión de parqueadero, Sistema de gestión de vídeo, Programación de oficinas inteligentes, Alarma de incendios, Control de entrada peatonal, Gestión de kioscos, Detección de temperatura, Estados de alertas, Monitoreo de datos, Automatización de edificios e Intrusión.



### Descripción

Armatura One es una plataforma de seguridad basada en web desarrollada y basada en las ideas de integración abierta, alta seguridad y facilidad de uso. Para facilitar la ciberseguridad y la privacidad de los usuarios, todos los datos del sistema se cifran con los protocolos criptográficos Advanced Encryption Standard (AES) y Transport Layer Security (TLS), y todo el sistema cuenta con las certificaciones ISO27001, ISO27701 e ISO27017, estándar de alto nivel BS EN 60839-11-1:2013 Grado 3 y Grado. Además, cuenta con una API Restful y un SDK para integrarse con sistemas de terceros. Armatura One, admite hasta más de 260 protocolos de comunicación de grado industrial, incluidos BACnet, OPC, KNX y Modbus, para integrarse de forma flexible con sensores y controladores de grado industrial de terceros con condiciones y reglas personalizadas. Al mismo tiempo, Armatura One admite varias credenciales de autenticación en línea con tecnologías biométricas avanzadas, credenciales móviles, códigos QR dinámicos encriptados y tecnologías RFID multitecnología para adaptarse mejor a las necesidades de todos los clientes.

## Características



### Alta seguridad

Armatura One está diseñado para aplicaciones de alta seguridad. Todas las comunicaciones se cifran con protocolos criptográficos Advanced Encryption Standard y Transport Layer Security (TLS).



### Automatización de edificios

Con la ayuda de la pasarela de protocolos de Armatura, es compatible con más de 268 protocolos industriales, incluidos BACnet, OPC, KNX, Modbus, etc., lo que hace que Armatura One sea fácilmente integrable con sistemas de gestión de edificios (BMS) o sistemas de gestión de propiedades (PMS).



### Enlaces multifuncionales avanzados

Admite más de 200 condiciones de enlace que cubren la mayoría de los escenarios de aplicación de control de acceso. Además, admite enlaces de alto nivel con dispositivos industriales de terceros a través de protocolos de comunicación industriales. Los usuarios pueden configurar de forma flexible las condiciones de vinculación o los atributos en función de las diferentes aplicaciones de dispositivos, como sensores de calidad del aire acondicionado, sensores de fugas de agua, cableado estructurado, bombas hidráulicas, etc.



### Potente mapa digital

Se integra perfectamente con herramientas de mapeo, como Google Maps, GIS Maps y SuperMap, para adaptarse mejor a las necesidades de los distintos clientes. Desde simples planos 2D hasta modelos 3D de edificios de varias plantas o gestión de complejos urbanísticos e industriales.



### Funciones avanzadas de control de acceso

Admite funciones avanzadas de control de acceso como anti-passback, autenticación multiusuario, vinculación entre paneles (vinculación global), control de ascensores, gestión de visitantes, etc. Armatura One ofrece una mayor flexibilidad al usuario admitiendo longitudes de tarjeta de hasta 256 bits que cubren la mayoría de las necesidades y admite hasta 15 segmentos horarios en una única área para ofrecer una programación flexible.



### Arquitectura distribuida

En un sistema multiservicios, el servicio de base de datos del sistema, el servicio de aplicaciones y el servicio Redis. Están separados pero sincronizados para permitir que varios servicios trabajen simultáneamente para nivelar la carga de trabajo del procesamiento masivo de datos en grandes proyectos. Esto reduce el riesgo de que se produzcan fallos en el servidor.



### Integración de terceros

Soporta múltiples formas de integración basadas en Armatura One Restful Web API, Microsoft Active Directory, Microsoft Excel y auto importación CSV.



### Soluciones de seguridad versátiles

Armatura One está equipado con múltiples módulos de aplicación, incluido el control de acceso, y está totalmente integrado con las soluciones de diferentes líderes del sector para proporcionar una solución de seguridad completa. Se integra con los sistemas de alarma de intrusión de BOSCH, Risco y Honeywell; los sistemas DCS/DOP de Schindler, Mitsubishi, Kone, Hitachi Elevator; los sistemas de gestión de vídeo Milestone, los sistemas de cerraduras inalámbricas Assa Abloy Aperio y muchos más para la gestión de los propios.



### Sistema de notificación por SMS

En lugar de proporcionar sólo avisos del sistema como otras soluciones, Armatura One va más allá. Permitiendo a los administradores tener una forma más rápida y directa de recibir notificaciones. Armatura One ahora es compatible con varias aplicaciones de mensajería instantánea, incluyendo, WhatsApp, Line, Amazon SNS y SMS.



### Escalable

Innovador protocolo de comunicación basado en MQTT, como protocolo de comunicación ligero utilizado generalmente por dispositivos IoT. Sus características lo convierten en una solución óptima para sistemas de seguridad inteligentes que permiten a Armatura One comunicarse con más de 10.000 dispositivos en borde (controladores, unidad de puerta, lectores, sensores, etc.) y gestionar más de un millón de usuarios en un entorno de red.



### Varias opciones de autenticación

Admite varias opciones de credenciales, como RFID (más de 200 tipos de tarjetas y multi-tecnología RFID), credenciales móviles (NFC y Bluetooth y código QR dinámico) y tecnología biométrica (huella, reconocimiento de la palma de la mano sin contacto y reconocimiento facial sin contacto).

## Información general

### Dispositivos compatibles



Controladora  
AHSC-1000



Controladora  
AHDU Series



Tarjeta de expansión  
AHEB



Lectores  
Series EP



Serie de terminales  
Omni



ACMS  
(Plataforma móvil de  
credenciales en la nube)

## Sistemas operativos recomendados

Servidor	Microsoft Windows Server 2012(64-bit) Microsoft Windows Server 2016(64-bit) Microsoft Windows Server 2019(64-bit) Microsoft Windows 10 20H2 or later(64-bit) Microsoft Windows 11(64-bit)
Navegador sugerido	Chrome 33 o superior Safari 6.1.3 o superior MS Edge 88 o superior Firefox 64.0 o superior
Base de datos	PostgreSQL ver.9.6 (por defecto), MS SQL 2005/2008/2012/2019 (Compatible), Oracle 11g/12c (Compatible)
Número máximo de clientes admitidos (simultáneamente)	5,000
Personal o usuarios máximos	Hasta 1,000,000
Tarjetas RFID máximas	Hasta 1,000,000
Contraseñas máximas	Hasta 1,000,000
Huellas dactilares máximas	Hasta 1,000,000
Biometría de reconocimiento facial	Hasta 1,000,000
Biometría de palma	Hasta 1,000,000
Puertas con control de acceso máximo	10,000
Niveles máximos de control de acceso	Sin límite (depende del servidor y la red)
Puntos máximos de asistencia	10,000
Visitantes máximos (mensuales)	Hasta 1,000,000
Máximas cámaras de vigilancia	Hasta 5,000
Servidores de vídeo inteligentes	50
Salidas máximas controladas	Sin límite (depende del servidor y la red)
Entradas máximas	Sin límite (depende del servidor y la red)

## Integración de terceros

Notificación / Mensajes	Line / WhatsApp / Amazon SNS / SMS
Gestión de mapeo	Google Map / SuperMap/ GIS Map
Directorio Activo de Microsoft	Cualquier versión
Integración de alarmas de intrusión	Bosch, RISCO, Ajax, Honeywell (Próximamente)
Sistema DCS de ascensores	Kone, Mitsubishi, Schindler, Otis, Hitachi
Automatización de edificios	BACnet, OPC, KNX, MQTT
Sistema de gestión de vídeo	Milestone, Artec, Digifort, ZKTeco, C2P
Sistema Smart Lock	Aperio Wireless Lock System
Sistema OCR	Desko, ZKTeco
Sistema de alta disponibilidad	Rose Data
Impresora de tarjetas	HID Fargo, IDP
API	<p>Soportes Restful API :</p> <ul style="list-style-type: none"> <li>Interfaz de persona de la API RESTful del Área de Asistencia</li> <li>Interfaz Persona API RESTful</li> <li>Interfaz de plantillas biométricas de persona API RESTful</li> <li>Interfaz de tarjeta API RESTful</li> <li>Interfaz de departamento API RESTful</li> <li>Interfaz de área API RESTful</li> <li>Interfaz de lector API RESTful</li> <li>Interfaz de medios API RESTful</li> <li>Interfaz de puerta API RESTful</li> <li>Interfaz de suelo API RESTful</li> <li>Interfaz de control de acceso API RESTful</li> <li>Interfaz de dispositivos de control de acceso API RESTful</li> <li>Nivel de acceso API RESTful</li> <li>Interfaz de transacciones de control de acceso API RESTful</li> <li>Interfaz de transacciones de asistencia API RESTful</li> <li>Interfaz de dispositivos de asistencia API RESTful</li> <li>Interfaz de nivel de control de ascensores API RESTful</li> <li>Interfaz de dispositivos de ascensores API RESTful</li> <li>Interfaz de transacciones de ascensores API RESTful</li> <li>Interfaz de autorización de gestión de vehículos API RESTful</li> <li>Gestión de vehículos Interfaz de transacciones API RESTful</li> <li>Interfaz de reserva de visitantes API RESTful</li> <li>Interfaz a nivel de visitante API RESTful</li> <li>Registro de visitantes Interfaz de salida API RESTful</li> </ul>
Mapeo de bases de datos	Compatible con MySQL, Oracle 11g/12c, SQLServer 2005/2008/2012, SQLEXPRESS

## Protección de datos

Protección de datos

Certificado ISO 27701, Certificado ISO27017, Certificado ISO27001, protección de datos GDPR, encriptación HTTPS, RSA (criptosistema), SSL (Secure Sockets Layer), TLS (Transport Layer Security), AES (Advanced Encryption Standard), OTP

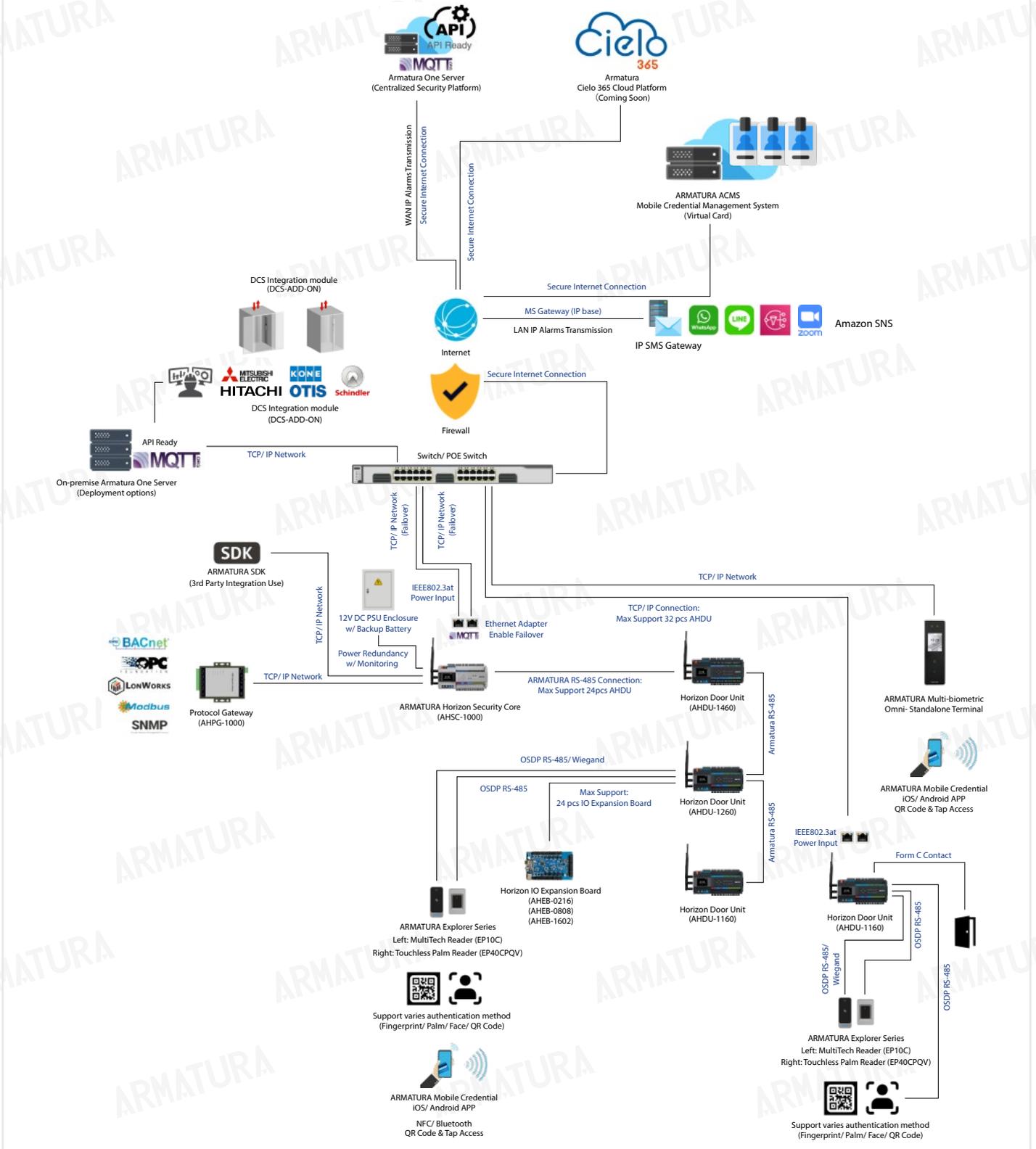
(One-time Password), TOTP (Time-based One Time Password), 2FA (2-factor Authentication), HMAC (Hash-based Message Authentication), HOTP y SHA (Algoritmo de Hash Seguro).

## Requisitos mínimos de hardware del servidor

Escenarios de aplicación	Proyecto pequeño	Proyecto profesional	Proyecto empresarial
Cantidad de servidores	Servidor único	Servidor único	Multi-servidor
Uso	Dentro de 200 terminales	Dentro de 1.000 terminales	Dentro de 2.000 terminales
Base de datos recomendada	1. PostgreSQL (incorporado) 2. MS SQL or Oracle (proporcionado por clientes) 3. Se recomienda utilizar base de datos MS SQL u Oracle en aplicaciones multiservidor		
Sistema operativo del servidor	Windows 10 /11 Windows Server 2016 / 2019		
Resolución de pantalla	Pantalla en color de 1920*1080 (tamaño mínimo de pantalla recomendado: 0,22")		
Ethernet	NIC (tarjeta de interfaz de red) 1000 Mbps o Gigabit Ethernet o especificaciones superiores		
RAM	8GB DDR4	32GB DDR4	64GB DDR4
CPU	Intel(R) Core(TM) i5 Procesador de 6 núcleos de la serie 11 Gen o superior con una velocidad de 2,7 GHz o superior	Intel(R) Core(TM) i7 Procesador de 8 núcleos de la serie 11 Gen o superior con una velocidad de 3,0 GHz o superior	Intel(R) Core(TM) i9 Procesador de 8 núcleos de la serie 11 Gen o superior con una velocidad de 3,5 GHz o superior
ROM	500 GB de espacio libre o más (se recomienda utilizar una unidad de estado sólido) 32 GB DDR4		
Tarjeta gráfica (opcional)	Gráficos Intel IrisX (integrados) o tarjeta gráfica discreta Recomendado: Nvidia GeForce RTX 3050 8GB de memoria		

Esta guía de requisitos mínimos de hardware del servidor es sólo para aplicaciones generales.

## Diagrama del sistema Armatura



# ARMATURA

## Plataforma de Mensajería



### Otros



### Sistema de Mapas



### Automatización de Edificios



### Alarma de Intrusión



### Alarma contra Incendios



## Credenciales Móviles

# ARMATURA

CREDENTIAL MANAGEMENT



### Ascensores Sistemas + DSC



### Sistemas de Video



### Oficinas Automatizadas



# ARMATURA ONE

