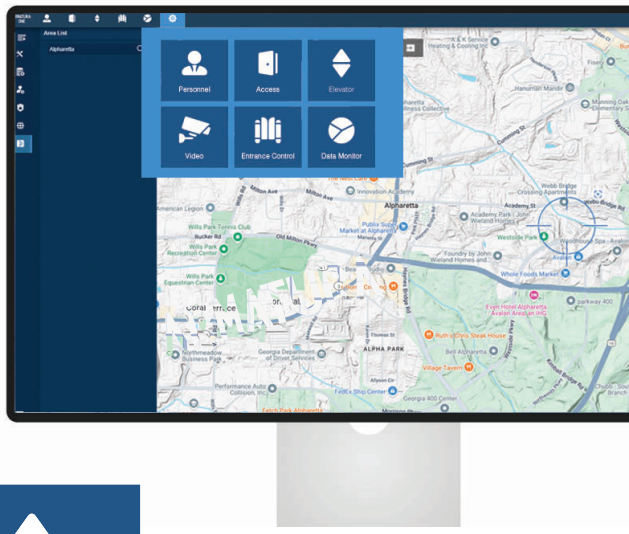
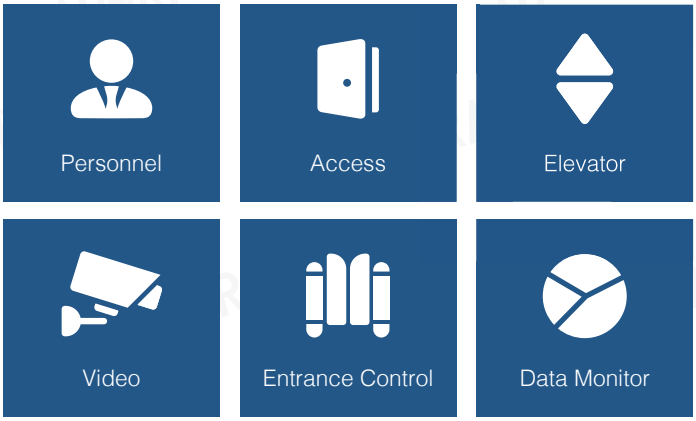
ARMATURA ONE

Web-Based Security Platform



All-in-One Web-Based Integrated Security Platform

Armatura One is the ultimate "All-in-One" web-based security platform developed by Armatura. It features multiple integrated modules, including Personnel, Access Control, Elevator Control, Video Surveillance, Entrance Control, Data Monitoring, and more.



Overview

Armatura One is a web-based security platform developed for open integration, high security, and user-friendly operation. It provides a comprehensive security solution, including access control, elevator control, video surveillance, and more, all with the most advanced levels of security.

All data within the system is encrypted using Advanced Encryption Standard (AES) and Transport Layer Security (TLS) cryptographic protocols. The entire system is certified with ISO 27001, ISO 27701, and ISO 27017 standards. Additionally, Armatura One features a RESTful API and SDK, allowing integration with nearly all third-party systems.

Moreover, the Armatura protocol gateway enables Armatura One to support over 260 industrial-grade communication protocols, including BACnet, OPC, and Modbus. This allows for flexible integration with third-party industrial-grade sensors and controllers, accommodating custom conditions and rules.

Armatura One also supports various authentication credentials, including advanced biometric technologies, mobile credentials, encrypted dynamic QR codes, and multi-tech RFID technologies, to meet all customer needs.

Features

High Security

Armatura One is designed for high-security applications. All communications are encrypted with Advanced Encryption Standard and Transport Layer Security (TLS) cryptographic protocols.

Advanced Multi-functional Linkages

Supports over 200 linkage conditions, covering most access control application scenarios. Additionally, it supports high-level linkages with third-party industrial-grade devices via industrial-grade communication protocols. Users can flexibly set linkage conditions or attributes for various device applications, such as air quality sensors, air conditioners, water leakage sensors, and more.

Powerful Digital Map

Armatura One works with powerful digital map feature that provide real-time visualization of security systems. This allows for intuitive monitoring and management of all connected devices and their statuses, enhancing situational awareness and response times.

Advanced Access Control Functions

Supports advanced access control functions such as anti-passback, multi-level authentication, cross-panel linkage (global linkage), elevator access control, and visitor management. It offers higher flexibility by supporting card lengths up to 256 bits, accommodating nearly all needs, and supports up to 15 time segments in a single time zone for flexible scheduling.

3rd Party Integration

Supports multiple forms of integration, via the Armatura One RESTful Web API, Microsoft Active Directory, Microsoft Excel, and CSV auto import.

SMS Notification System

Instead of providing just system prompts like other solutions, Armatura One pushes the limits further by allowing administrators to receive notifications faster and more directly. Armatura One now supports various instant messaging applications, including WhatsApp, Line, Amazon SNS, and SMS.

Scalable

The innovative MQTT-based communication protocol is generally used by IoT devices and is a lightweight communication protocol. Its features make it an optimal solution for intelligent security systems, enabling Armatura One to communicate with over 10,000 edge devices (controllers, door units, readers, sensors, etc.) and manage over one million users in a simple network environment.

Various Credential Options

Supports various credential options including RFID (200+ card types & multi-tech RFID technology), mobile credentials (NFC & Bluetooth & dynamic QR code) and biometric technology (touch-less palm authentication and touch-less face authentication).

ARMATURA

General Information

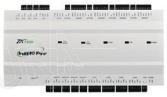
Supported Products:

AHEB
Expansion Board

EP Series
Reader

ACMS
(Mobile credential cloud platform)

Legacy Products:



inbio460 Pro

US-C3-400 Pro

SF1008-WP

SF1005

Omni Standalone
Reader Controller

Operating System

Supported Systems	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) * Mac Boot Camp is not supported
Suggested Browsers	Chrome 33 or later, Safari 6.1.3 or later MS Edge 88 or later Firefox 64.0 or later
Supported Databases	PostgreSQL ver.9.6 (built-in), MS SQL 2005/2008/2012/2019 (Supported), Oracle 11g/12c (Supported)
Maximum Supported Clients (Simultaneously)	5,000
Maximum Supported Personnel	1,000,000
Maximum RFID Cards	1,000,000
Maximum Passwords	1,000,000
Maximum Fingerprints	1,000,000
Maximum Faces	10,000
Maximum Access Controlled Doors	10,000
Maximum Access Control Levels	Unlimited (Upon server and network performance)
Maximum Surveillance Cameras	5,000
Maximum Intelligent Video Servers	50
Maximum Controlled Outputs	Unlimited (Upon server and network performance)
Maximum Inputs	Unlimited (Upon server and network performance)

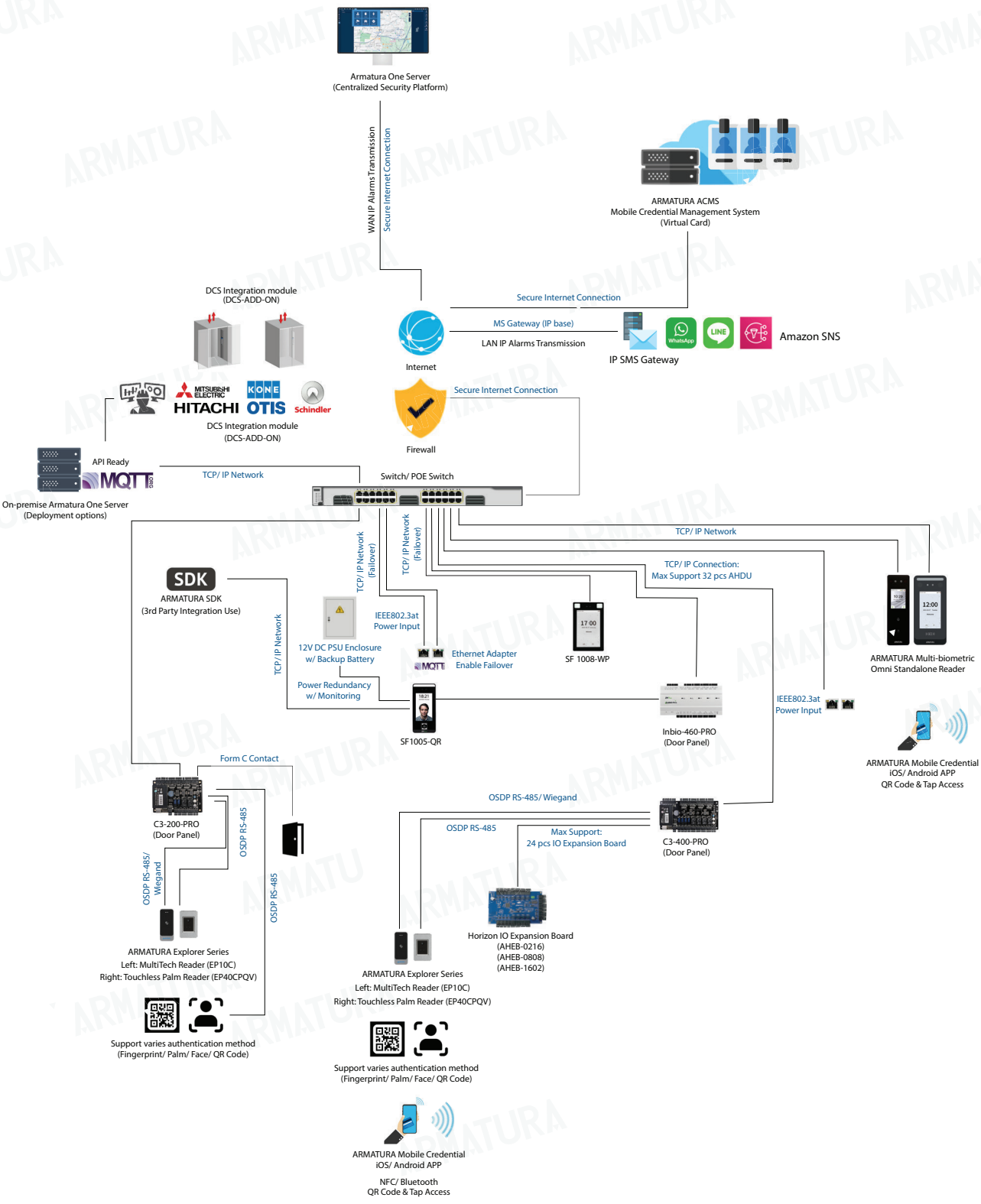
3rd-Party Integration	
Notifications/ Messaging	Line / WhatsApp / Amazon SNS / SMS
Digital Maps	Google Map / SuperMap/ GIS Map
Microsoft Active Directory	No Version restriction
Instrusion Systems	Bosch, RISCO, Honeywell (coming soon)
Elevator Desination Control Systems Building	Kone, Mitsubishi, Schindler, Otis, Hitachi
Automation	BACnet, OPC, MQTT
Video Management Systems Smart Lock	Milestone, Arteco, Digifort, C2P
Smart Locks	Aperio Wireless Lock System
OCR Systems	Desko, ZKTeco
High Availability Systems	Rose Data
Card Printers	HID Fargo, IDP
API	**The Armatura One RESTful API supports calls for:** • Personnel • Personnel Biometric Templates • Cards • Departments • Areas • Readers • Media Files • Doors • Floors • Access Control • Access Control Devices • Access Levels • Access Control Events • Elevator Levels • Elevator Devices • Elevator Events
Database Mapping	Supports

Data Protection	
Data Protection	ISO 27701 Certified, ISO27017 Certified, ISO27001 Certified, GDPR Complaint, Communication protected by HTTPS, RSA (cryptosystem), 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), HAMC (Hash-based Message Authentication), HOTP and SHA (Secure Hash Algorithm).

Minimum Server Hardware Requirements			
Application Scenarios	Small Projects	Mid-level Projects	Enterprise Projects
Server Quantity	Single Server	Single Server	Multi-Server
Usage	Within 200 Terminals	Within 1,000 Terminals	Within 2,000 Terminals
Recommended Databases	1. PostgreSQL (built-in) 2. MS SQL or Oracle (provided by clients) 3. Recommended to use MS SQL or Oracle database on multi-server application		
Server OS	Windows 10 /11 Windows Server 2016/2019/2022		
Network	NIC (Network Interface Card) 1000Mbps or Gigabit Ethernet or higher spec		
RAM	8GB DDR4	32GB DDR4	32GB DDR4
CPU	Intel(R) Core(TM) i5 11th Gen series or above 6 Core processor with speed of 2.7GHz or above	Intel(R) Core(TM) i7 11th Gen series or above 8 Core processor with speed of 2.5 GHz or above	Intel(R) Core(TM) i7 11th Gen series or above 8 Core processor with speed of 2.5 GHz or above
ROM	500GB free space or larger (recommend using solid-state drive) 32GB DDR4		
Graphics Card (Optional)	Intel IrisX Graphics (Integrated) or Discrete Graphics Card Recommend: Nvidia GeForce RTX 3050 8GB memory		

This minimum server hardware requirements guideline is for general applications only.

Armatura System Diagram



Address:190 Bluegrass Valley Parkway, Alpharetta, GA 30005
Phone: + 1 (470) 816-1970
Email: sales@armatura.us
Website: www.armatura.id