ARMATURA

ARMATURA ONE

Armatura One Security Platform

Web-Based Versatile Security Platform

AES 256 ENCRYPTION

TLS CERTIFIED

ASHRAE BACnet™

OPC®

Modbus
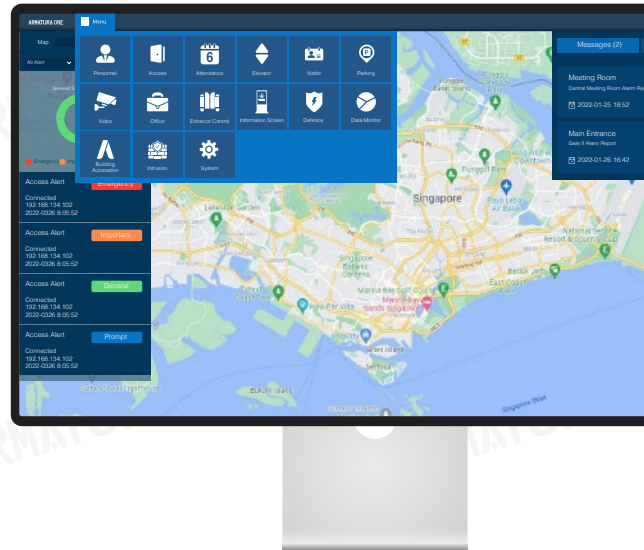
All-in-One Web-Based Integrated Security Platform

Armatura One is the ultimate "All-in-One" web-based security platform developed by Armatura. It contains multiple integrated modules: Personnel, Access Control, Time & Attendance, Elevator, Visitor, Parking Management, Video Management System, Office, Entrance Control, Information Screen, Defence, Data Monitor, Building Automation and Intrusion.

Personnel	Access	Attendance	Elevator	Visitor	Parking	Video

Office	Entrance Control	Information Screen	Defence	Data Monitor	Building Automation	Intrusion
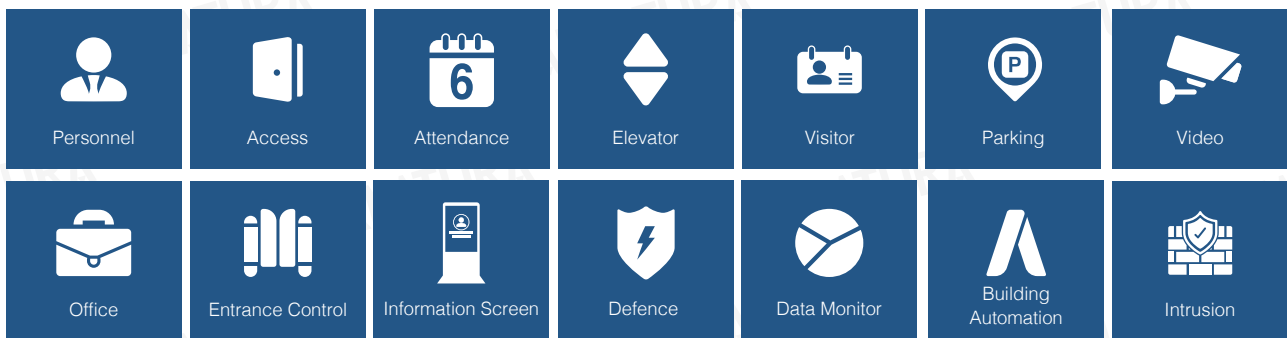
Overview

Armatura One is a web-based security platform developed & based on the ideas of being Openly Integrated, Highly Secure and User-friendly. Providing a comprehensive security solution including access control, elevator control, visitor management, parking management, time & attendance, building automation and intrusion alarm with the most advanced levels of security. To ease users' cyber security and privacy concerns, all the data within the system is encrypted with Advanced Encryption Standard (AES) and Transport Layer Security (TLS) cryptographic protocols and the whole system is certified with ISO27001, ISO27701 and ISO27017. In addition, it has a Restful API and SDK to integrate with almost all 3rd party systems. Moreover, with the help of the Armatura protocol gateway; Armatura One supports up to 260+ industrial-grade communication protocols including BACnet, OPC, and Modbus to flexibly integrate with 3rd party industrial-grade sensors and controllers with custom conditions and rules. At the same time, Armatura One supports various authentication credentials in line with advanced biometric technologies, mobile credentials, encrypted dynamic QR codes, and multi-tech RFID technologies to best suit all customer's needs.

ARMATURA

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.

3rd Party Integration
Supports multiple forms of integration based on the Armatura One Restful Web API, Microsoft Active Dictatory, Microsoft Excel and CSV auto import.

Building Automation
With the help of the Armatura Protocol Gateway, it supports up to 268+ industrial-grade protocols including BACnet, OPC, Modbus, etc., which makes Armatura One easily integrable with Building Management Systems (BMS) or Property Management Systems (PMS).

Versatile Security Solutions
Armatura One is equipped with multiple application modules including access control and is fully integrated with different industry leaders' solutions to provide a well-rounded security solution. Integrating with BOSCH, Risco and Honeywell intrusion alarm systems; Schindler, Mitsubishi, Kone, Hitachi Elevator DCS & DOP systems; Milestone video management systems, Assa Abloy Aperio wireless lock systems and more for you to discover.

Advanced Multi-functional Linkages
Supports over 200 linkage conditions which cover most access control application scenarios. In addition, it supports high-level linkages with 3rd party industrial-grade devices via industrial-grade communication protocols. Users can flexibly set linkage conditions or attributes upon different device applications such as air quality sensors, air-conditioners, water leakage sensors & more.

SMS Notification System
Instead of providing just system prompts like other solutions, Armatura One pushes the limit further. Allowing administrators to have a faster and more direct way to receive notifications. Armatura One now supports various instant messenger applications including, WhatsApp, Line, Amazon SNS and SMS.

Powerful Digital Map
Seamlessly integrates with various powerful mapping tools including Google Maps, GIS Maps and SuperMap to best suit different clients' needs. From simple 2D floor plans to 3D multi-story building models or multi-location site management.

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

Advanced Access Control Functions
Supports advanced access control functions such as anti-passback, multi-level authentication, cross panel linkage (global linkage), elevator access control, visitor management, etc. Armatura One offers higher flexibility to the user supporting up to 256-bit card lengths that almost cover all needs and supports up to 15-time segments in a single time zone to offer flexible scheduling.

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 (touchless palm recognition and touchless face recognition).

Distributed Architecture (Coming Soon)
In a multi-server system, the system database server, application server, and Redis server are separated yet synchronized to enable multiple servers to work simultaneously to offload the workload from massive data processing in big projects. This eases the risk of facing server failures.

ARMATURA

General Information

Supported Products:

| AHSC-1000 Controller | AHDU Series Controller | AHEB Expansion Board | EP Series Reader | Omni Standalone Terminal Series | ACMS (Mobile credential cloud platform) |

Operating System

Server-Side	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 Browser for Client-Side	Chrome 33 or later, Safari 6.1.3 or later MS Edge 88 or later Firefox 64.0 or later
Database	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 Attendance Points	10,000
Maximum Visitors (Monthly)	1,000,000
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

Notification / Messages	Line / WhatsApp / Amazon SNS / SMS
Digital Map	Google Map / SuperMap/ GIS Map
Microsoft Active Directory	No Version restriction
Intrusion Alarm Integration	Bosch, RISCO, Honeywell (coming soon)
Elevator DCS	Kone, Mitsubishi, Schindler, Otis, Hitachi
Building Automation	BACnet, OPC, MQTT
Video Management System	Milestone, Arteco, Digifort, C2P
Smart Lock System	Aperio Wireless Lock System
OCR System	Desko, ZKTeco
High Availability System	Rose Data
Card Printer	HID Fargo, IDP
API	Restful API Supports： Person Interface of Attendance Area RESTful API Person Interface RESTful API Person Biometric Template Interface RESTful API Card Interface RESTful API Department Interface RESTful API Area Interface RESTful API Reader Interface RESTful API Media Interface RESTful API Door Interface RESTful API Floor Interface RESTful API Access Control Interface RESTful API Access Control Device Interface RESTful API Access Level RESTful API Access Control Transaction Interface RESTful API Attendance Transaction Interface RESTful API Attendance Device Interface RESTful API Elevator Control Level Interface RESTful API Elevator Device Interface RESTful API Elevator Transaction Interface RESTful API Vehicle Management Authorization Interface RESTful API Vehicle Management Transaction Interface RESTful API Visitor Reservation Interface RESTful API Visitor Level Interface RESTful API Visitor Registration Check Out Interface RESTful API
Database Mapping	Supports

ARMATURA

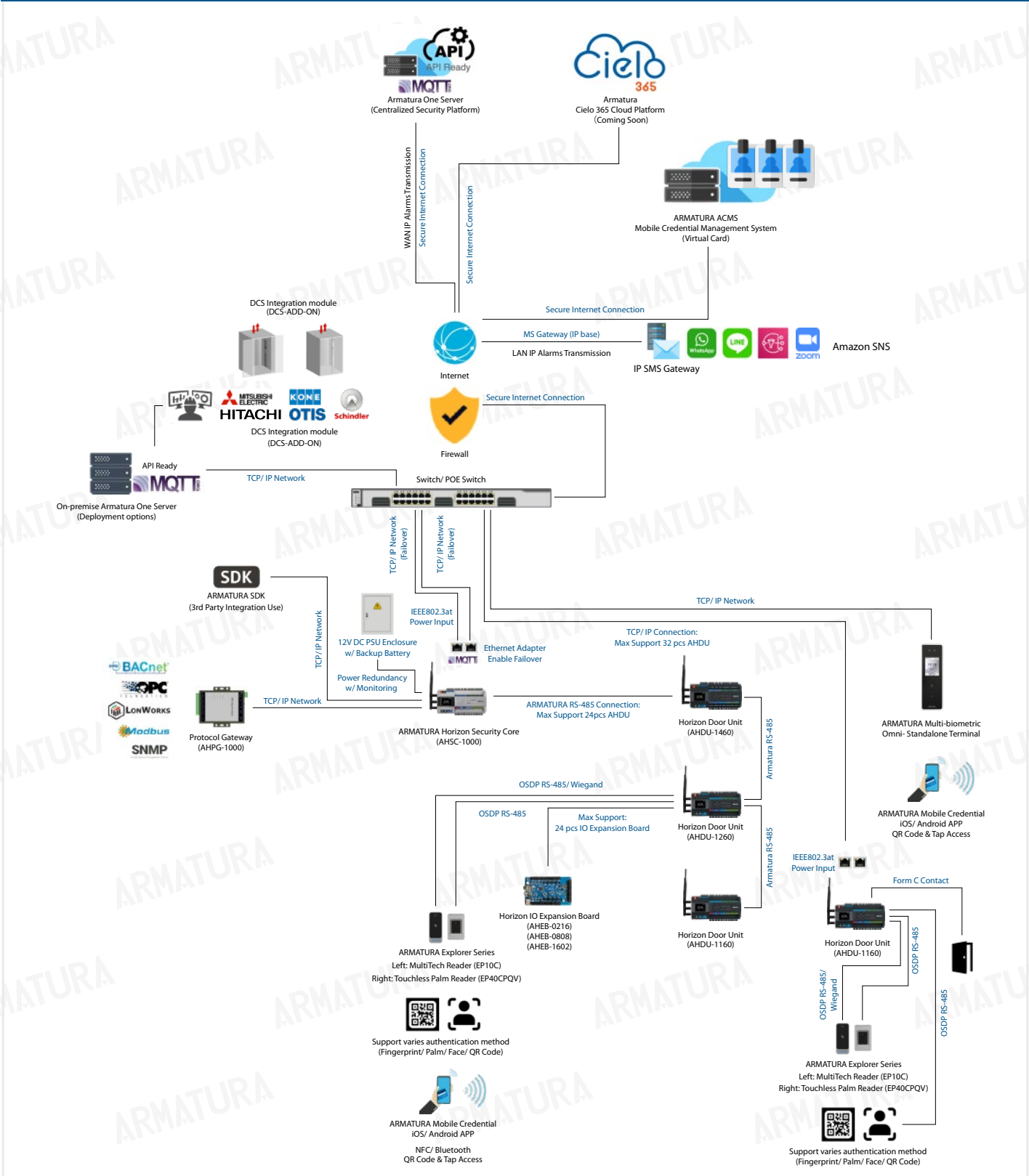## Data Protection

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	Lite Project	Professional Project	Enterprise Project
Server Quantity	Single Server	Single Server	Multi- Server
Usage	Within 200 Terminals	Within 1,000 Terminals	Within 2,000 Terminals
Recommended Database	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		
Screen Resolution	1920*1080 color display (recommended minimum screen size: .22")		
Ethernet	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

Armatura System Diagram

API Ready

MQTT

Armatura One Server
(Centralized Security Platform)

Cielo 365

Armatura
Cielo 365 Cloud Platform
(Coming Soon)

ARMATURA ACMS
Mobile Credential Management System
(Virtual Card)

WAN IP Alarms Transmission

Secure Internet Connection

Secure Internet Connection

DCS Integration module
(DCS-ADD-ON)

Secure Internet Connection

MS Gateway (IP base)

LAN IP Alarms Transmission

Internet

IP SMS Gateway

Amazon SNS

MITSUBISHI ELECTRIC
HITACHI
KONE
OTIS
Schindler

DCS Integration module
(DCS-ADD-ON)

Secure Internet Connection

API Ready

MQTT

Firewall

On-premise Armatura One Server
(Deployment options)

TCP/ IP Network

Switch/ POE Switch

TCP/ IP Network
(Failover)

TCP/ IP Network
(Failover)

TCP/ IP Network

SDK

ARMATURA SDK
(3rd Party Integration Use)

TCP/ IP Network

IEEE802.3at
Power Input

12V DC PSU Enclosure
w/ Backup Battery

TCP/ IP Connection:
Max Support 32 pcs AHDU

ARMATURA Multi-biometric
Omni- Standalone Terminal

Power Redundancy
w/ Monitoring

Ethernet Adapter
Enable Failover

MQTT

BACnet
OPC
LonWorks
Modbus
SNMP

TCP/ IP Network

Protocol Gateway
(AHPG-1000)

ARMATURA RS-485 Connection:
Max Support 24pcs AHDU

ARMATURA Horizon Security Core
(AHSC-1000)

Horizon Door Unit
(AHDU-1460)

Armatura RS-485

ARMATURA Mobile Credential
iOS/ Android APP
QR Code & Tap Access

OSDP RS-485/ Wiegand

OSDP RS-485

Max Support:
24 pcs IO Expansion Board

Horizon Door Unit
(AHDU-1260)

Armatura RS-485

IEEE802.3at
Power Input

Form C Contact

Horizon IO Expansion Board
(AHEB-0216)
(AHEB-0808)
(AHEB-1602)

Horizon Door Unit
(AHDU-1160)

Horizon Door Unit
(AHDU-1160)

OSDP RS-485

ARMATURA Explorer Series
Left: MultiTech Reader (EP10C)
Right: Touchless Palm Reader (EP40CPQV)

OSDP RS-485/
Wiegand

OSDP RS-485

Support varies authentication method
(Fingerprint/ Palm/ Face/ QR Code)

ARMATURA Explorer Series
Left: MultiTech Reader (EP10C)
Right: Touchless Palm Reader (EP40CPQV)

ARMATURA Mobile Credential
iOS/ Android APP

NFC/ Bluetooth
QR Code & Tap Access

Support varies authentication method
(Fingerprint/ Palm/ Face/ QR Code)

ARMATURA

ArmaSec-06132024