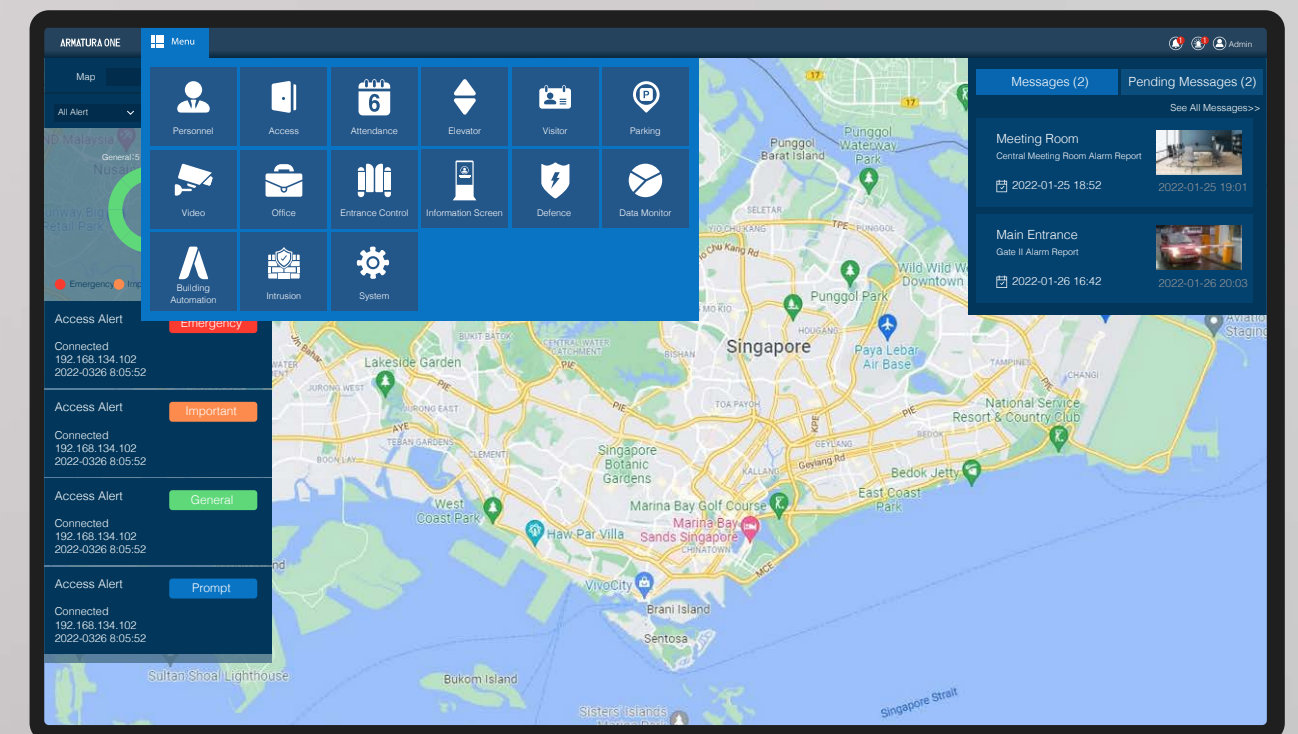


ARMATURA

ARMATURA ONE

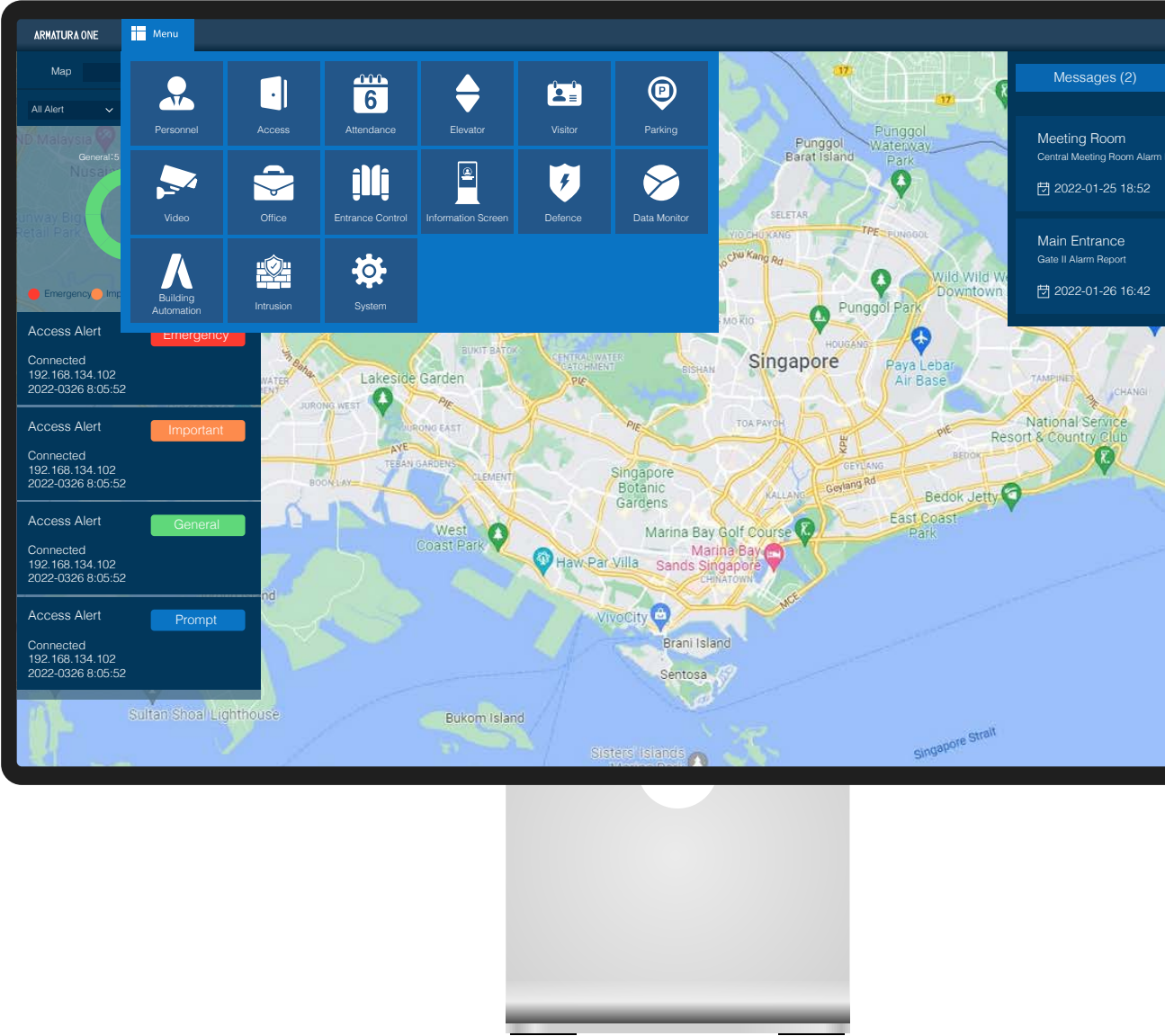
All-in-One Web-Based
Integrated Security Platform





Armatura One Security Platform

Web-Based Versatile Security Platform





Overview

Armatura One Security Platform is a web-based, cutting-edge security solution designed to cater to the diverse needs of businesses and organizations in terms of access control, elevator control, visitor management, parking management, time and attendance, building automation, and intrusion alarm. The platform has been developed with a strong emphasis on open integration, high security, and user-friendliness, ensuring that it can seamlessly adapt to different environments and cater to the specific requirements of each organization.

 Personnel	 Access	 Attendance	 Elevator	 Visitor	 Parking	 Video
 Office	 Entrance Control	 Information Screen	 Defence	 Data Monitor	 Building Automation	 Intrusion

Key Features of Armatura One Security Platform



Comprehensive Security Solutions

Armatura One is a web-based platform offering a complete security solution for access control, elevator control, visitor management, parking management, time and attendance, building automation, and intrusion alarms. The platform is designed to be highly secure, user-friendly, and openly integrated, ensuring compatibility with various third-party systems.



High Security and Privacy

Armatura One places the utmost importance on user privacy and security by encrypting all data using Advanced Encryption Standard (AES), Transport Layer Security (TLS), SSL and HTTPS cryptographic protocols. The system is certified with ISO27001, ISO27701, and ISO27017 to further ensure safety.



Grade 4 (EN-60839) International Standard

Armatura One is founded on Grade 4 (EN-60839) international standards for critical infrastructure. It is mandatory in European Union countries. The standard requires certification of Access Control Units (Controllers), readers (proximity, biometrics, etc.), and Access Control Software to enhance security in access control systems.



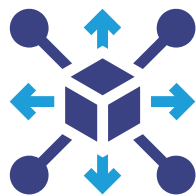
Flexible Integration Capabilities

The platform features a RESTful API and SDK, allowing seamless integration with a wide range of third-party systems. Armatura One also supports 260+ industrial-grade communication protocols, such as BACnet, OPC, and Modbus, through the Armatura protocol gateway, facilitating flexible integration with third-party industrial sensors and controllers.



Multiple Authentication Options

Armatura One offers various authentication options to suit different customer needs, including advanced biometric technologies, mobile credentials, encrypted dynamic QR codes, and multi-tech RFID technologies.



High Security and Compliance

Our system is designed to meet the most stringent access control standards in both Europe and the United States. It has been certified with UL294, a widely recognized standard for security equipment in the U.S., and BSEN 60839-11-1:2013 Level 4, the highest level of access control certification in Europe. These certifications ensure exceptional reliability, security, and compliance with international regulations.

Multi Server Architecture

Global Deployment · Instant Response · Security & Compliance

Core Value

- Global Architecture: Hybrid on-premises and cloud deployment for elastic expansion, cross-region redundancy, and disaster recovery
- Ultra-Low Latency: Local caching + event-driven sync for access decisions in under second
- High Availability & Clustering : Automatic failover with Load Balancing, Zero downtime

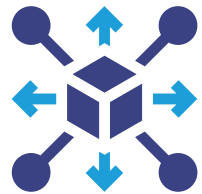


Market Challenges

- Single-point failure: One server cannot handle multiple branches and peak loads
- Sync delays: Permissions and logs not shared in real time, creating security and compliance risks
- Limited scalability: Upgrading hardware is complex, no cloud integration

Key Benefits:

- Elastic Scaling: Horizontal/Vertical/Cloud expansion supports 1 to 100+ sites
- Data Consistency: Delta replication + Automatic conflict resolution for uniform permissions and events
- Compliance Assured: Built-in GDPR/ISO27001 framework, encrypted transmission and audit logs



Building Automation and Advanced Linkages

The platform supports integration with Building Management Systems (BMS) or Property Management Systems (PMS) through the Armatura Protocol Gateway. It also provides advanced multi-functional linkages with over 200 conditions for flexible device applications and high-level linkages with third-party industrial-grade devices.



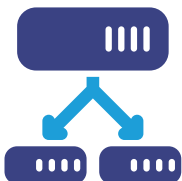
Powerful Digital Map

Armatura One seamlessly integrates with various mapping tools, including Google Maps, GIS Maps, and SuperMap, to suit different clients' needs, from simple 2D floor plans to 3D multi-story building models or multi-location site management.



Advanced Access Control Functions

The platform supports the advanced Wiegand 2.0 protocol, offering advanced access control functions such as anti-passback, multi-level authentication, cross-panel linkage (global linkage), elevator access control, and visitor management. It provides increased flexibility with card lengths of up to 256 bits and allows for up to 15 time segments within a single time zone, enabling flexible scheduling.



Distributed Architecture

The upcoming distributed architecture feature will enable multiple servers to work simultaneously to offload the workload from massive data processing in big projects, reducing the risk of server failures.

MQTT

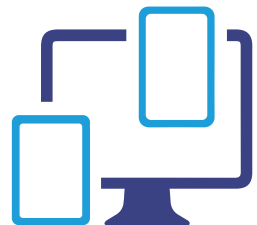


Scalability

The innovative MQTT-based communication protocol enables Armatura One to communicate with over 10,000 edge devices and manage over one million users under a simple network environment, making it highly scalable.

Various Credential Options

Armatura One supports numerous credential options, including RFID, mobile credentials, and biometric technology, such as touchless palm recognition and touchless face recognition.



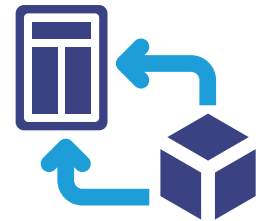
Responsive Design

Armatura One supports responsive design, which ensures optimal viewing and interaction across various devices and screen sizes. It involves adapting the layout, content, and functionality of a website or application to provide an optimal user experience on desktop computers, laptops, tablets, and mobile devices.



System-Wide Monitoring Capability:

The Armatura One platform incorporates a comprehensive monitoring system that allows users to receive real-time notifications from different modules throughout the application. These notifications include visitor scheduling and check-in updates, meeting-related alerts, and conference room equipment maintenance notifications. Simultaneously, users have access to all alarm events generated by the system, such as access control breaches, intrusion alarms, and other critical or urgent security-related incidents, enabling swift response and mitigation of potential issues.



Third-Party Integration

Armatura One supports multiple forms of integration based on its RESTful Web API, Microsoft Active Directory, Microsoft Excel, and CSV auto import. It integrates with industry-leading solutions such as BOSCH, Risco, and Honeywell intrusion alarm systems, as well as Hanwah and Artec video management systems, among others. Additionally, it supports the ONVIF, RTSP, and RTMP protocols.



Instant Message Platform

In addition to system prompts, Armatura One offers a more direct way to receive notifications through various instant messenger applications, such as Twilio, WhatsApp, Line, Amazon SNS, SMS, and Simple Mail Transfer Protocol (SMTP).

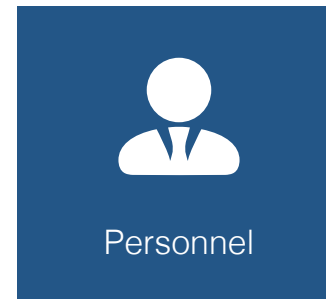
Flexible Installation Modes - Armatura One's Advanced and Easy Options

There are two separate modes available for installing the Armatura controller: Advanced Mode and Easy Mode.



In Advanced Mode, the installation process involves manual device registration and excludes any communication via HTTP before establishing MQTT communication. This approach enhances the security of data transmission. Additionally, the key import process is manual, reducing potential security vulnerabilities.

In Easy Mode, the installation process is user-friendly and simplified. It includes automated device registration, key transmission, and communication via both HTTP and MQTT. Easy Mode is ideal for users seeking a simplified configuration process.



Personnel Module

The Personnel Module in the Armatura One system is designed to provide comprehensive personnel management and support. It offers a wide range of features that cater to various organizational needs, streamlining processes and improving overall security.



Personnel Structure

The Armatura One Security Platform features a comprehensive Personnel Structure module, designed to effectively manage and organize a company's workforce. This module is divided into two main components: Department Management and Personnel Management. Each component serves a specific purpose in maintaining the company's organizational structure and personnel information.

Department Management

Department Management is focused on establishing and maintaining the company's organizational chart. It provides the necessary tools to create, modify, and manage departments and sub-departments within the organization (up to unlimited levels). This component ensures that the company's hierarchy is accurately represented and easily accessible in the platform, facilitating better communication and collaboration among teams.



Personnel Management

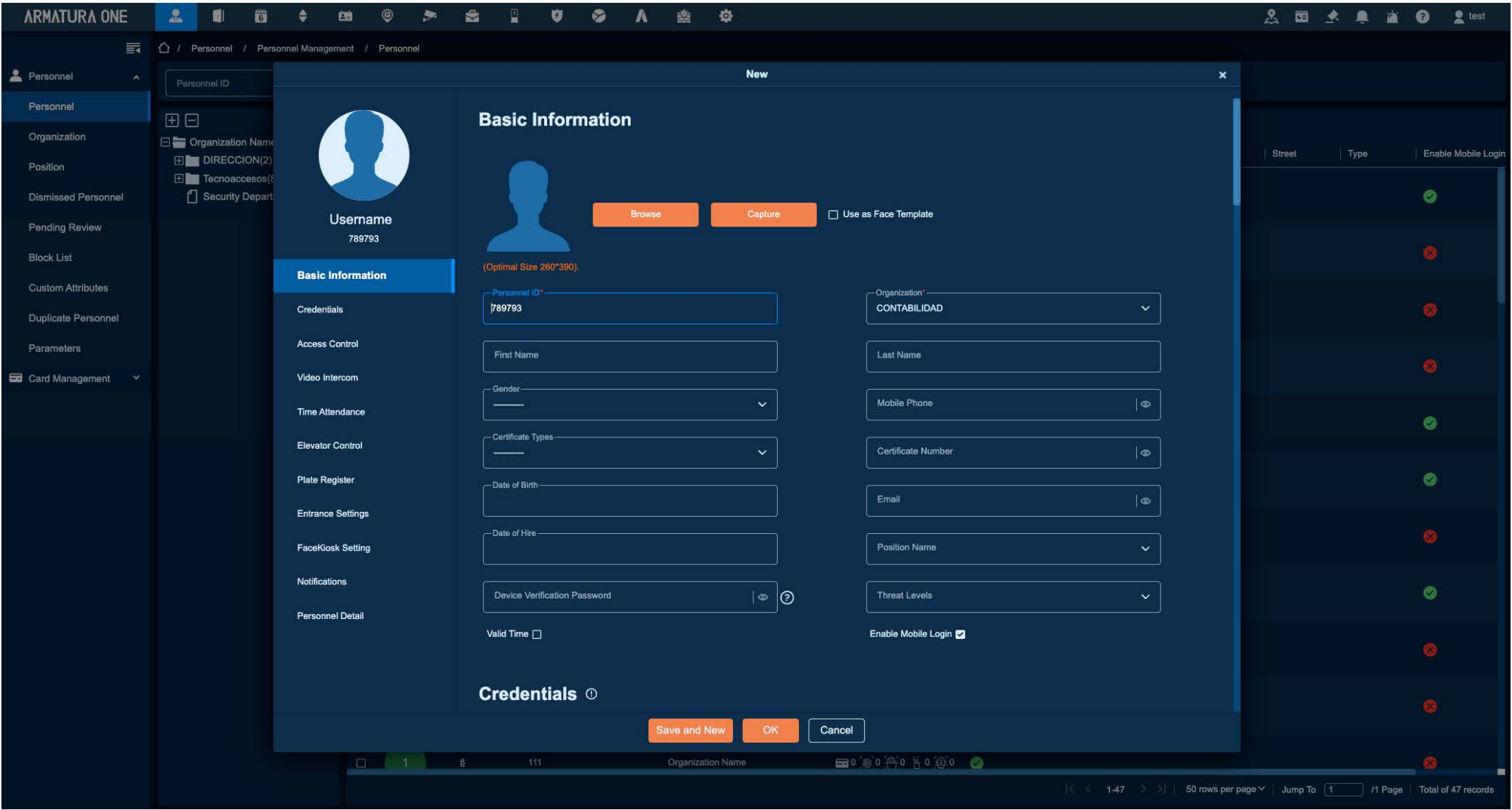
Personnel Management is responsible for handling personnel information and managing the associations between employees and their respective departments or sub-departments. This component allows users to store and manage crucial employee information, such as contact details, job titles, and access permissions. The Personnel Management component also enables the maintenance and management of personnel settings, ensuring that employee data remains accurate and up-to-date.





All-in-one Solution (Area/Department)

An intuitive personnel registration interface allows administrators to input employee details and staff enrollment data (e.g., Face, palm, RFID cards, mobile credential, dynamic QR code) and upload user photos on a single page.



Supports Various Card and Wiegand Formats and Card Stored Information

Armatura One is a versatile and adaptable access control system, designed to be compatible with a wide range of RFID card formats. With support for over 200+ different card formats, it offers seamless integration with various security protocols and technologies. Some of the notable card formats supported by Armatura One include:

- EM
- MIFARE
- DESFire
- Legic
- HID Proximity
- HID iClass
- Felica
- Type B



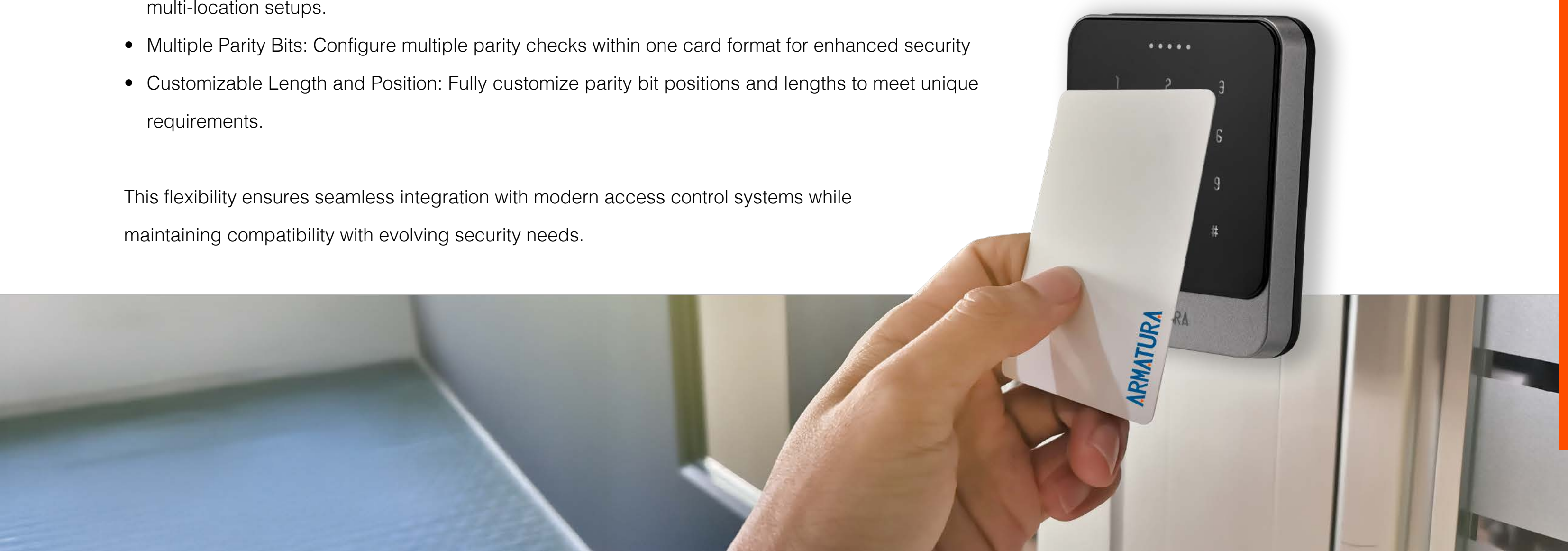


Advanced Wiegand Format Support

The advanced Wiegand format offers greater flexibility and functionality compared to traditional systems. Unlike older formats that support only a single site code and fixed parity bits, the advanced format allows:

- Multi-Site Code Support: Manage multiple site codes within a single system, ideal for complex, multi-location setups.
- Multiple Parity Bits: Configure multiple parity checks within one card format for enhanced security
- Customizable Length and Position: Fully customize parity bit positions and lengths to meet unique requirements.

This flexibility ensures seamless integration with modern access control systems while maintaining compatibility with evolving security needs.



Statistics

The system provides an overview of personnel count, fingerprint templates, facial templates, palm templates, card numbers, mobile credential data, gender, and other statistical information.

Statistics

	Statistical Type	Version	Current Total
Non-verification medium	Personnel		880
	Male		430
	Female		370
	Other		0
	Avatar		800
Verification medium	Fingerprint	V13.0	880
	Finger Vein		
	Palm Vein		880
	Visible palm		880
	Infra red Face		880
	Visible Face		880

Close

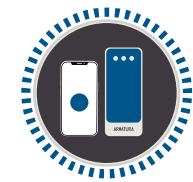
Supports Various Verification Methods

Multiple credential types are accepted, such as Biometric, Mobile Credential, Multi-tech RFID, and Passwords. It also offers three distinct mobile credential modes: card mode, remote mode, and QR-code mode (dynamic QR code encrypted with AES256 standard and TOTP method for enhanced security, regenerating every 2-3 seconds).



Card Mode

Present your smartphone to the reader like an access card



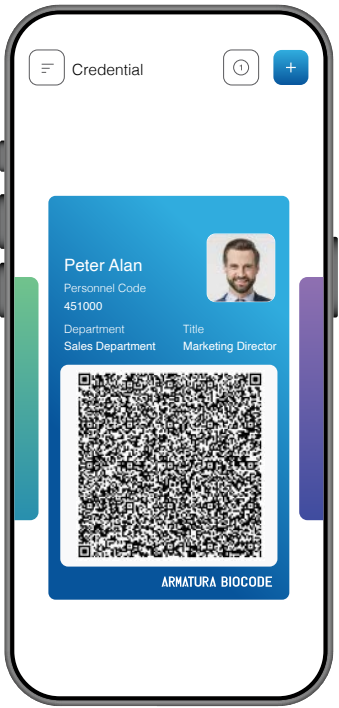
Remote Mode

Verify on the reader by clicking a button in the Armatura ID app



QR Code Mode

Present your QR Code and get access



Batch Import Photos for Facial Recognition Registration

The Armatura One Security Platform provides a Batch Import Photos feature that simplifies the process of managing photos for facial recognition registration. This function allows for the efficient importing of multiple photos at once (up to 3,000 JPG photos per upload), significantly reducing the time and effort required to register users for facial recognition. By enabling users to batch import photos for facial recognition registration, the system can automatically associate the imported images with the appropriate user profiles. This seamless integration leads to more efficient and organized management of user data within the platform, ensuring that the facial recognition system operates accurately and effectively.

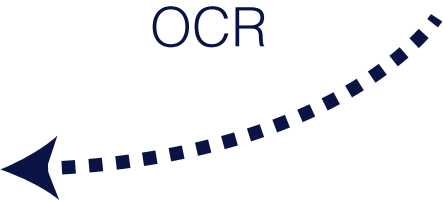
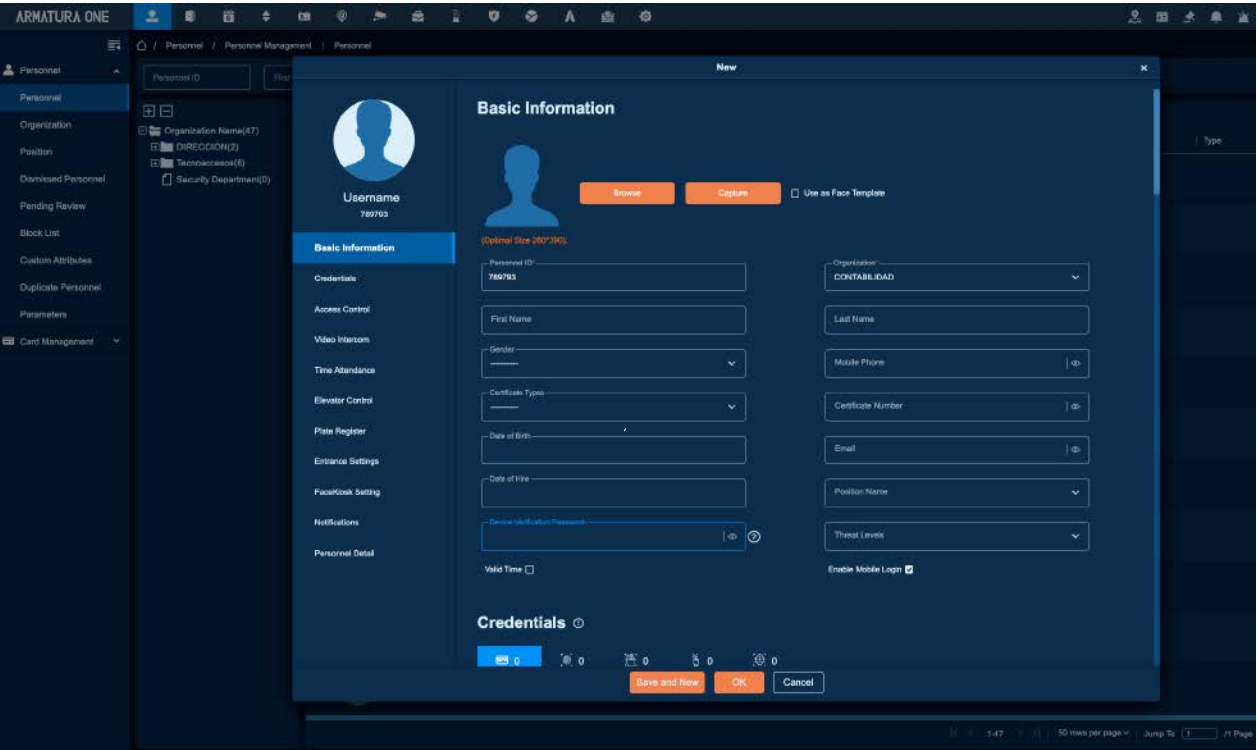


Integration with Desko and 3rd party OCR System

Fully integrated with the Desko and 3rd party OCR system for efficient visitor registration. Supports one-click capture of user images, passport photos, and automatic reading of identity documents (e.g., identity cards, passports) to enable rapid registration.

- Passport Photo + OCR Recognition
OCR function automatically reads identity document

- User's Portrait Capturing or Uploaded from the local PC
One-click capture of employees' portrait image



Active Directory and Database Field Mapping and Single Sign-On

Armatura One offers seamless integration with Active Directory (AD) servers for streamlined user management and authentication. With the ability to map fields from the AD server to corresponding database fields, users can maintain a consistent data structure across their organization.

Database Fields

Import AD fields

Personnel ID

First Name

Last Name

Organization Name

Mobile Phone

Email

Description

First Name

Last Name

Organization

Mobile

Email

Reset Configuration

User can call different fields from the AD Sever to map with the database fields, Armatura One almost opens all the field options that are available.

Last Name	Phone Number
Organization Name	Fax-Other
Personnel ID	Email
Mobile Phone	Direct Reports
First Name	Display Name
Email	Postal Code
Birth Date	Description
Country	Employee ID
Home Phone	Title
Home Address	Phone Number-other
Office Phone	Post Office Box
Office Address	Pager
Age Test	Pager-Other
Home Phone-Other	Mobile Phone-Other
IP Phone	Company
Office	Last Name
Creation Time	Organization
Manager-Name	User Login Name
User Login Name (Pre-Windows 2000)	Comment
English Abbreviation	Province

▲ User can choose different fields up to user’s decision



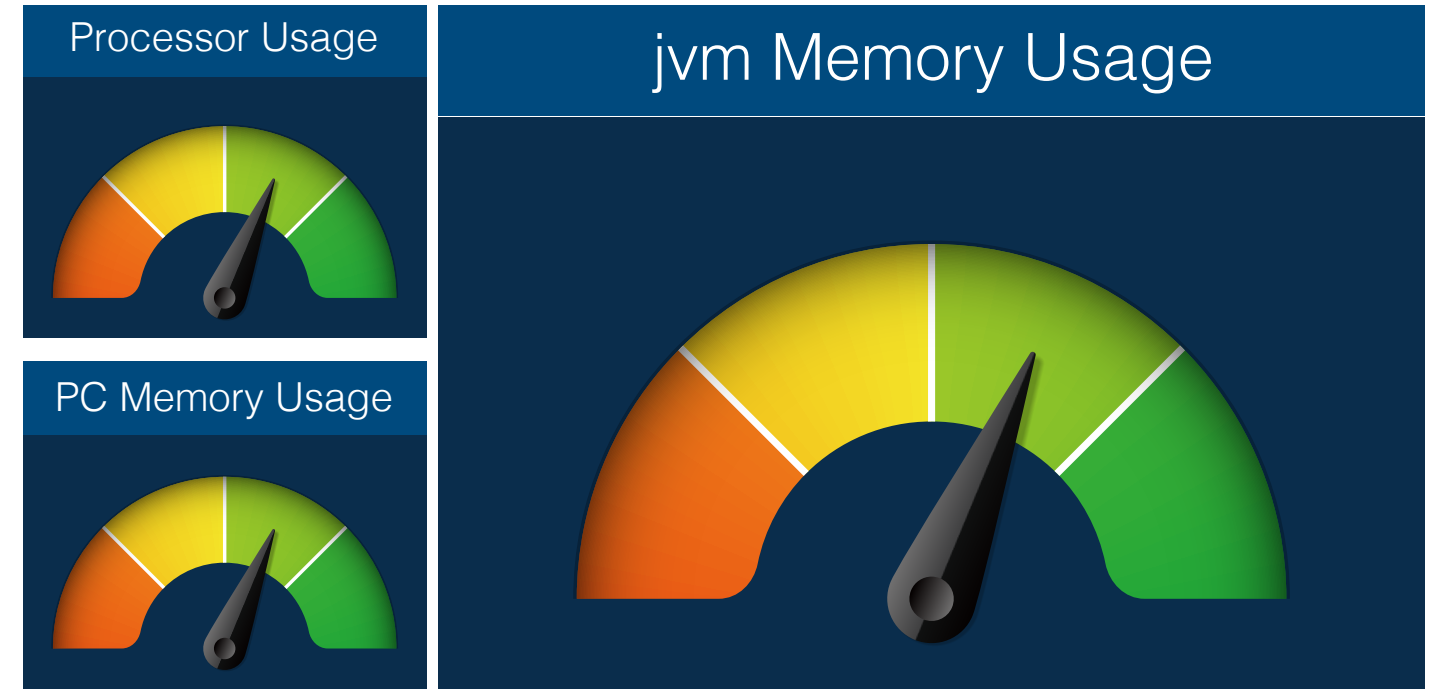
Client-Side Browser and Smartphone Fingerprint Login

Armatura One Security Platform offers a client-side browser fingerprint login feature that allows administrators to log in to the system using fingerprint verification for enhanced security and convenience. To utilize the fingerprint login feature, the administrator's login PC and smartphone must be equipped with an Armatura fingerprint sensor and have the fingerprint recognition function enabled.



System Monitoring

Displays server processor usage, host memory usage, processor information, memory information, and Java virtual machine memory usage to maintain optimal server and computer performance.





ACMS & Armatura One Seamless Integration

In Armatura One, you have the capability to efficiently manage the issuance of mobile credentials. With this powerful platform, users can conveniently input their card numbers, enabling employees to seamlessly utilize the Armatura ID Access Door. Armatura One streamlines the process of distributing mobile credentials, enhancing security and convenience for all parties involved. By centralizing the issuance workflow, Armatura One simplifies the management of mobile credentials, offering a seamless user experience and ensuring smooth access control operations.

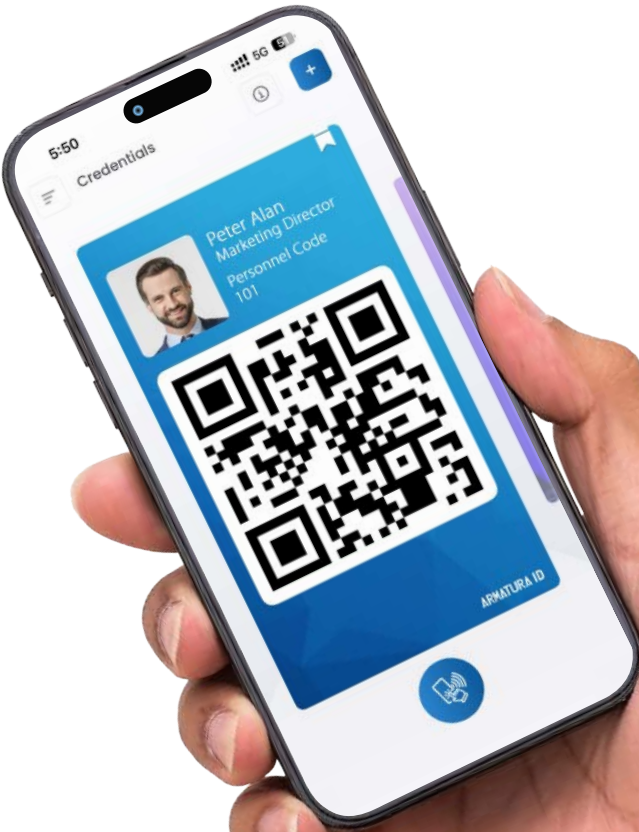
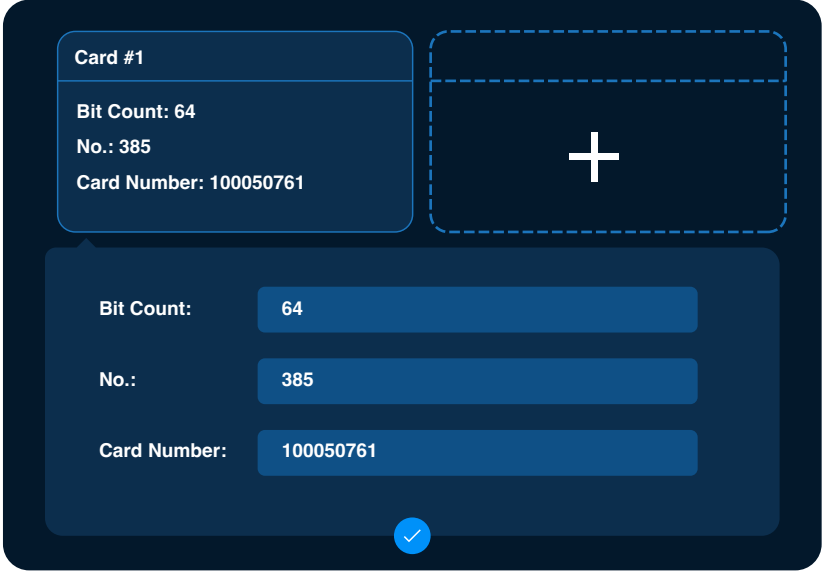
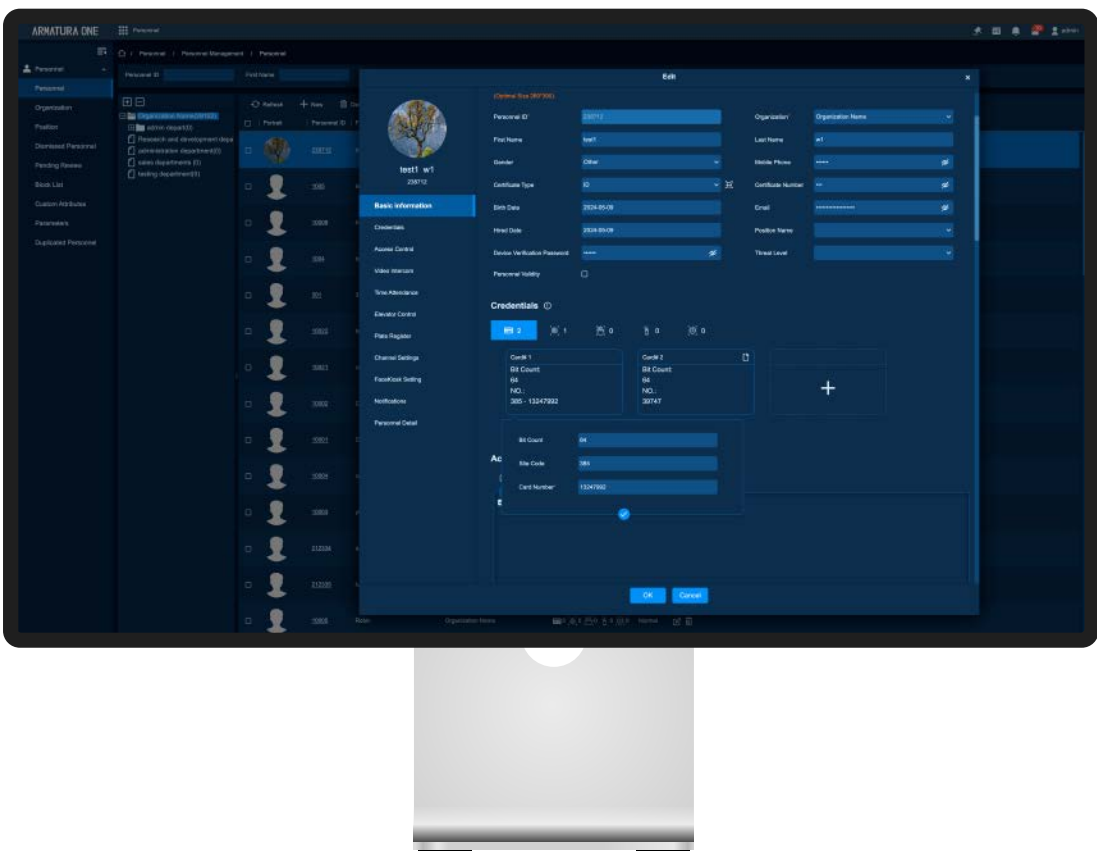




Photo Importing

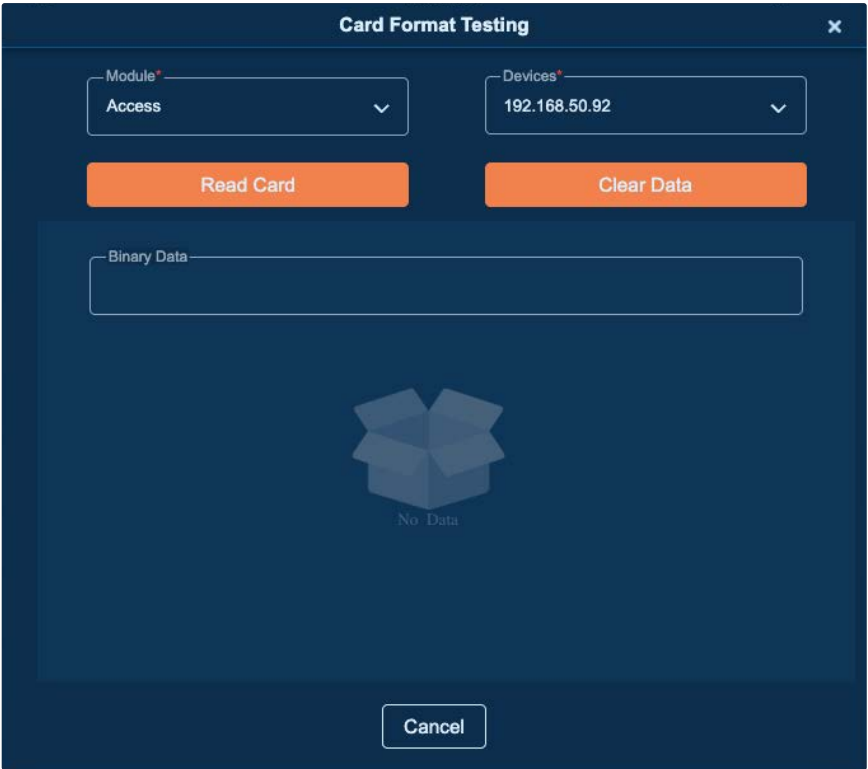
Supports single or compressed package uploading of user photos, with a maximum of 3,000 JPEG files per upload.



Maximum 3,000 JPEG Upload/ batch

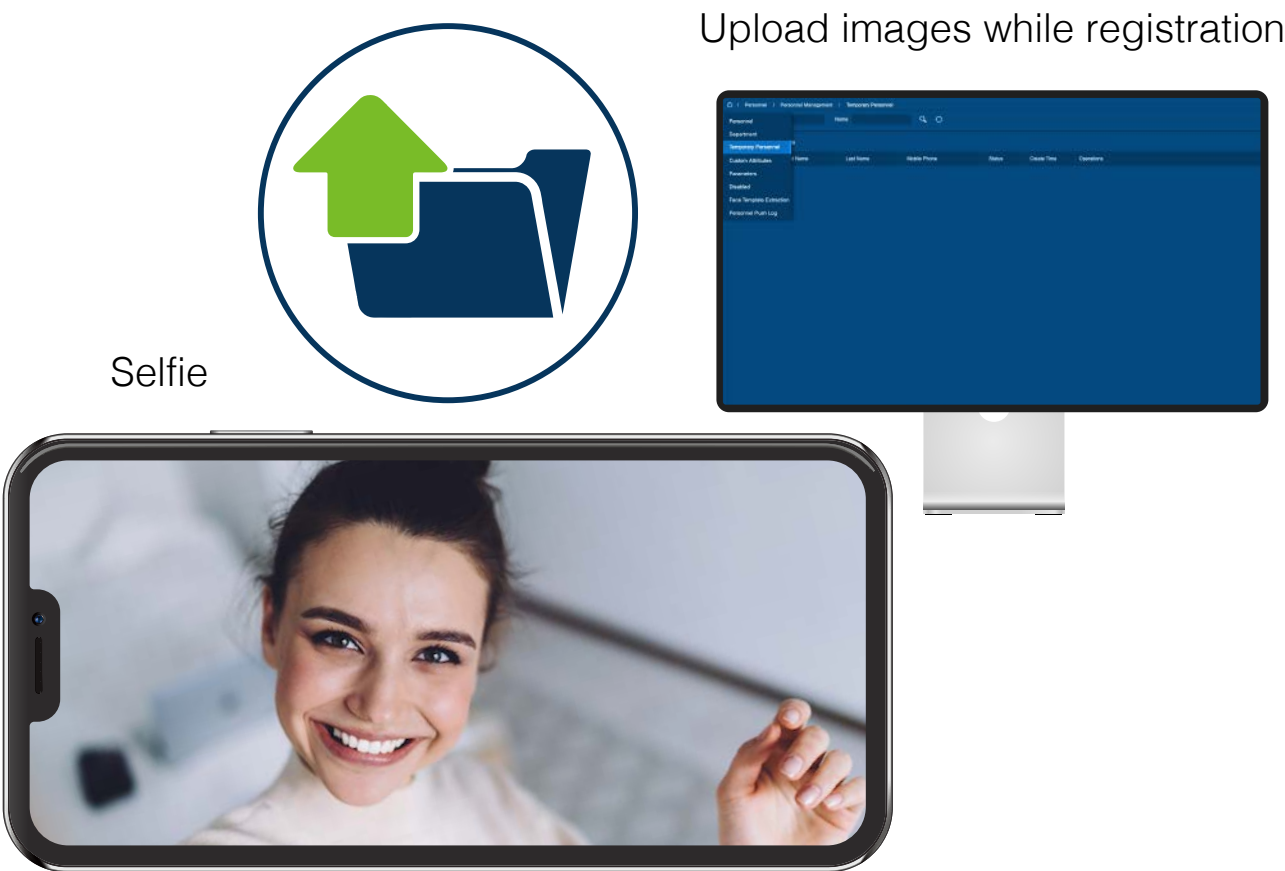
Access Card Format Testing

The Armatura One Security Platform features an Access Card Format Testing functionality that offers a simple and efficient way to verify access card formats and make necessary adjustments to Wiegand format when required. By providing a quick method to check access card formats, users can easily identify and resolve any discrepancies or inconsistencies, ensuring seamless integration between access cards and the security platform.



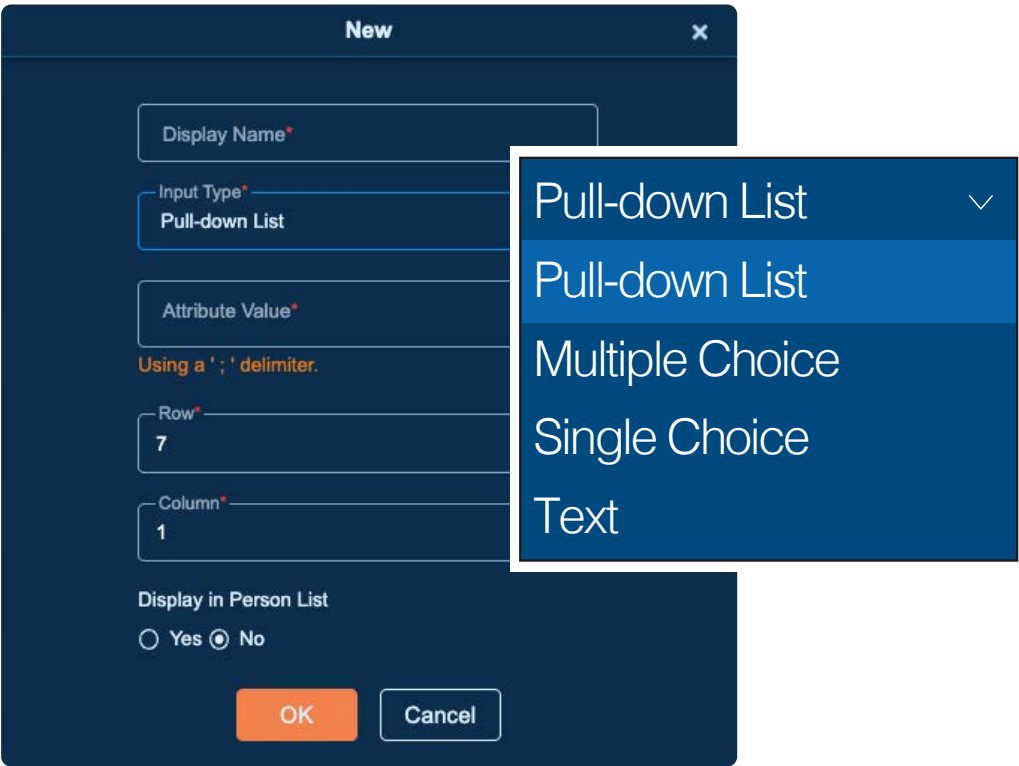
Personnel Photo for Facial Recognition Registration

The Armatura One Security Platform offers a convenient feature that utilizes profile pictures set within the system as facial recognition templates. This integration streamlines the registration process for facial recognition by automatically employing existing personnel photos for biometric authentication purposes.



Customized Attributes Support

The Armatura One Security Platform provides a flexible and user-friendly solution for managing personnel information through its Customized Attributes Support feature. Armatura One allows users to add customized attributes to the personnel page, ensuring that the platform can be tailored to suit each organization's unique requirements. This feature enables users to create and manage additional fields for storing and displaying information that is relevant to their specific needs.





Personnel Photo for Facial Recognition Registration

Selective Import/ Export:

Users can choose to import or export specific personnel records, giving them complete control over the data being transferred.

Export Personnel

Basic Information

☒ Check All

☒ Personnel ID

☒ Gender

☒ Email

☒ Position Name

☒ First Name

☒ Date of Birth

☒ Certificate Types

☒ SIP Account

☒ Last Name

☒ Mobile Phone

☒ Certificate Number

☒ Organization Number

☒ Card Number

☒ Date of Hire

☒ Organization Name

☒ License Plate

☒ Position Number

Custom Attributes

☐ Check All

☐ Employee Type

☐ Type

☐ Office Phone

☐ Hire Type

☐ Birth Place

☐ Office Address

☐ Job Title

☐ Country

☐ Floor Number

☐ Home Phone

☐ Street

☐ Home Address

Permission Group

☐ Check All

☐ Access Level

☐ Elevator Level

☐ Channel Level

File Format

File Format

EXCEL

OK

Cancel

Multi-Select:

If users need to import or export data for multiple individuals at once, the system enables them to select multiple records and perform the action in a single step.

Import Personnel Face Photos

Import mode

☒ Photo

☐ Compressed package

OK

Close

Export Personnel Photos

File Format

File Format

ZIP

OK

Cancel

Custom Field Options:

In addition to the standard fields, Armatura One provides the flexibility to include custom fields in the import/ export process. This ensures that all relevant information is captured and maintained within the system.

New

Display Name*

Input Type*

Pull-down List

Pull-down List

Multiple Choice

Single Choice

Text

Row*

7

Column*

1

Display in Person List

☐ Yes

☒ No

OK

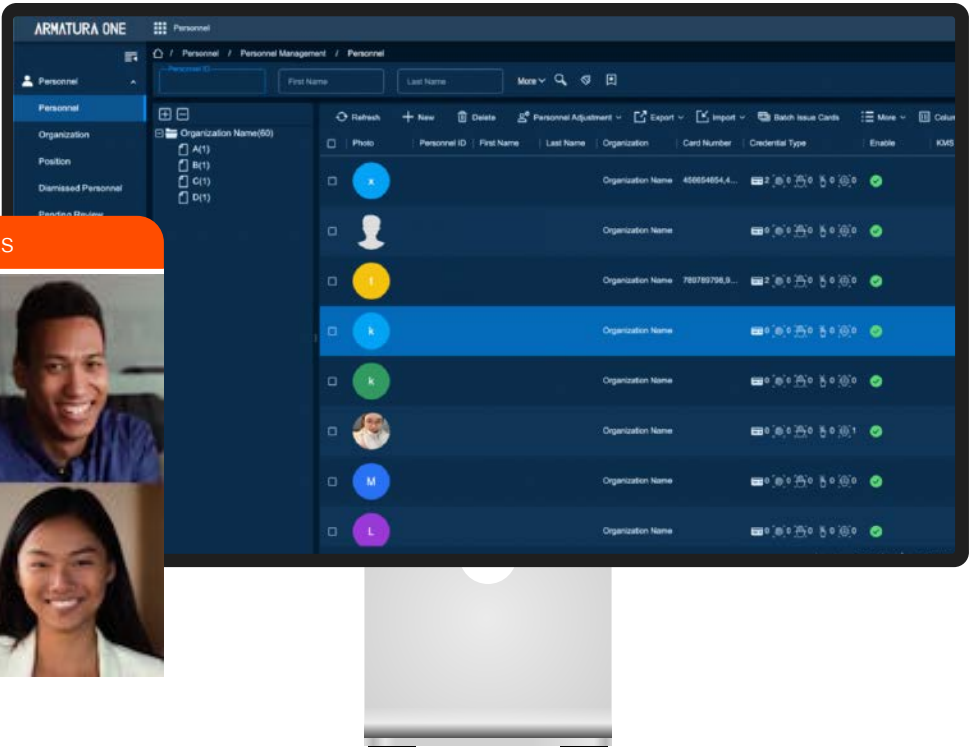
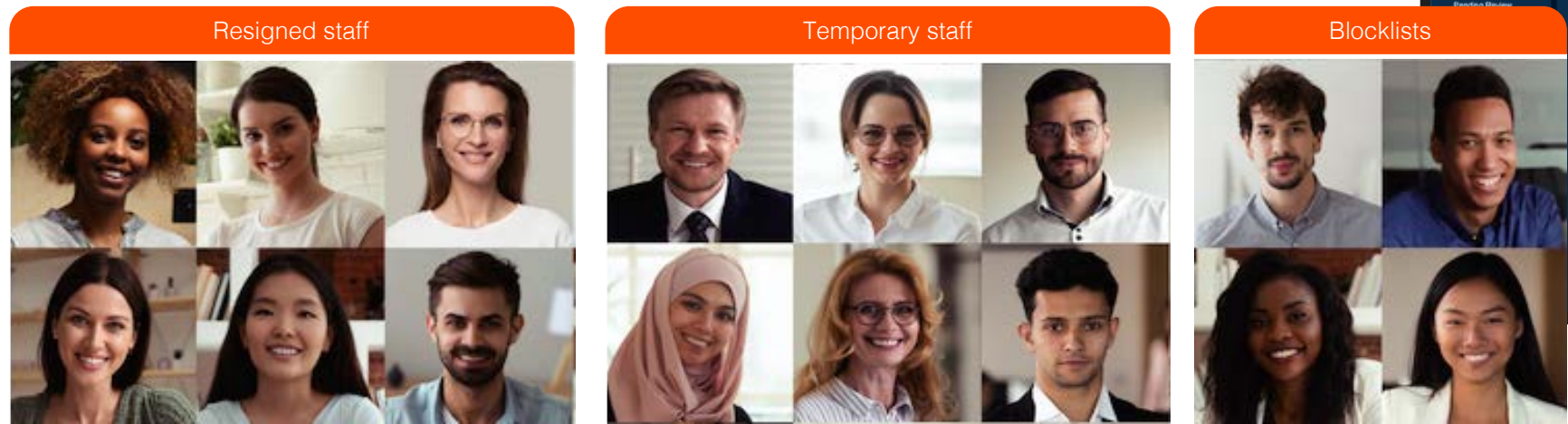
Cancel



Special Personnel Management

The Armatura One Security Platform offers a comprehensive Special Personnel Management feature that streamlines the handling of various personnel categories, such as resigned staff, temporary staff, blocklists, personnel tag libraries, and personnel tag library control. This functionality allows for efficient organization and management of personnel information, ensuring that access levels and attendance strategies can be tailored to suit the specific needs of each staff category.

- Resigned Staff Management
- Temporary Staff Management
- Blocklists
- Personnel Tag Libraries
- Personnel Tag Library Control

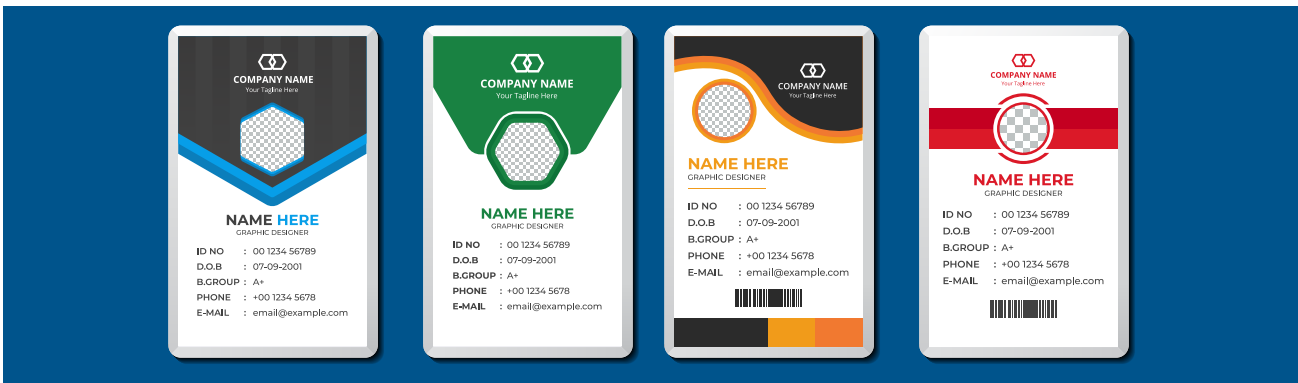


Supports Card Design and Card Printer

Armatura One offers a comprehensive card management solution by providing support for card design and integration with leading card printer brands. This feature enables users to create custom card designs and print them directly from the system, ensuring a seamless and efficient card issuance process.

Card Design:

The system allows users to design the appearance of their cards using a user-friendly interface. This includes adding company logos, user photos, custom text, and other design elements to create unique and professional-looking access cards.



Printer Integration:

Armatura One is fully integrated with popular card printer brands, such as Fargo and IDP. This compatibility ensures that users can easily print their custom-designed cards directly from the system without any additional software or configuration.

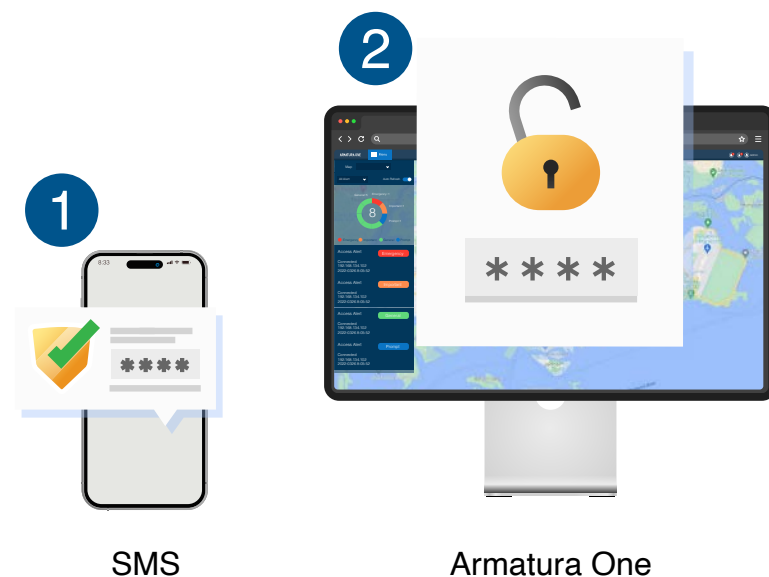


Supports 2FA User Login

Armatura One prioritizes security and user authentication by providing support for Two-Factor Authentication (2FA) during user login. This feature adds an extra layer of protection, ensuring that unauthorized individuals are unable to gain access to the system. The 2FA functionality in Armatura One includes the following options:

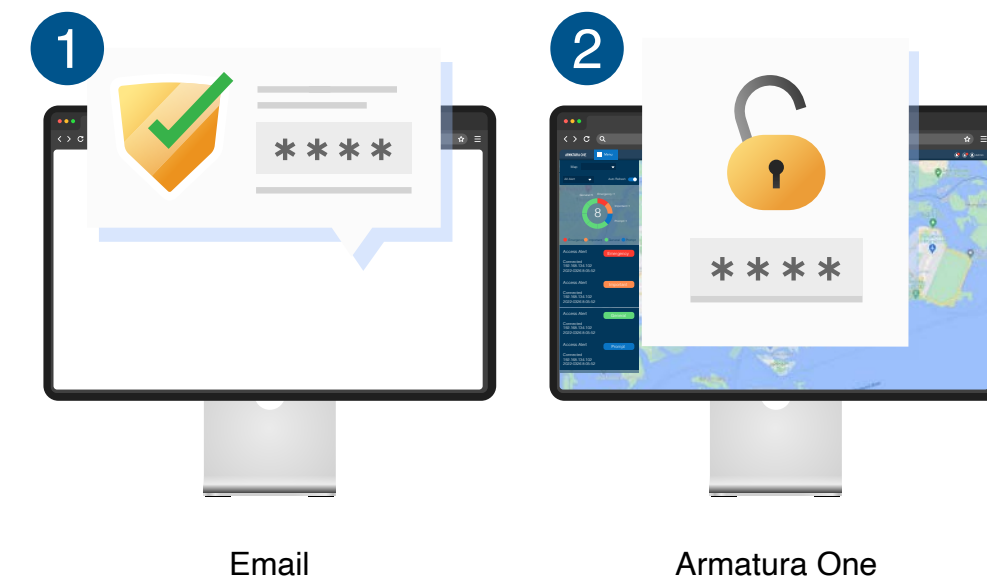
SMS:

Users can receive a One-Time Password (OTP) via SMS to their registered mobile number. After entering their username and password, users will be prompted to input the received OTP to complete the login process. This ensures that even if an attacker obtains a user's login credentials, they will not be able to access the system without the OTP sent to the user's mobile device.



Email:

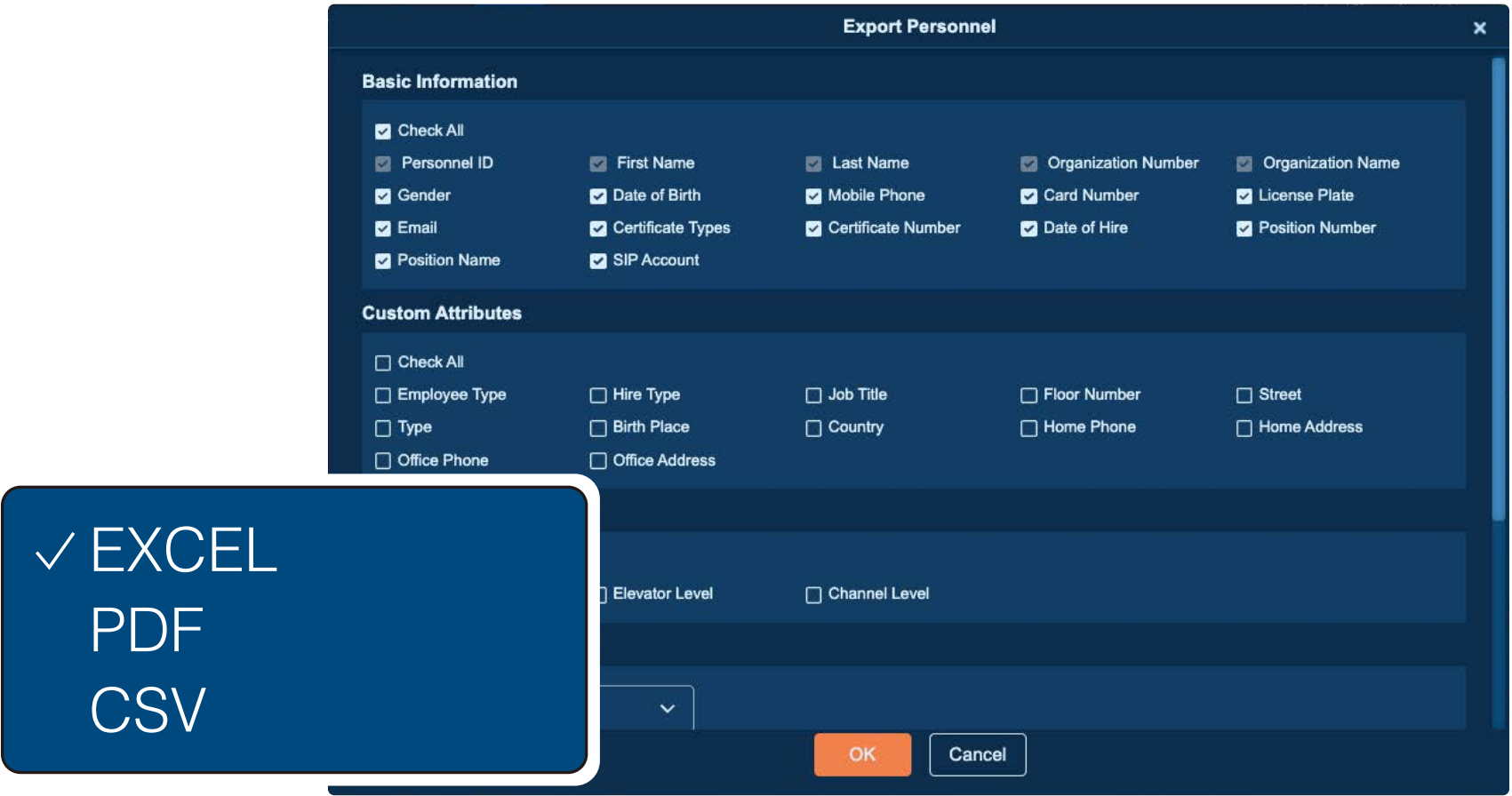
Similar to the SMS option, users can choose to receive the OTP via email. The OTP will be sent to the registered email address, and users will need to input it along with their username and password to successfully log in.



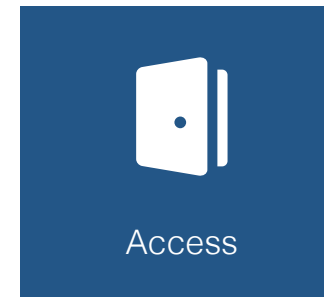


Export/ Import Personnel Information (CSV,PDF & Excel)

Armatura One offers a powerful and user-friendly feature for managing personnel information by allowing users to easily import and export personal details using CSV, PDF and Excel file formats. This functionality streamlines data management and ensures that the system remains up-to-date with the latest employee information.



Exported file could be either Excel, PDF and CSV format.



Access Module

The Access Control Module in the Armatura One system is an advanced, web-based management system designed to facilitate sophisticated access control functions, administration of networked access control panels via computer, and centralized personnel access management. It offers a wide range of features that cater to various organizational needs, improving overall security and access control.

BMS Integration

The integration with the Building Management System (BMS) supports transmitting Armatura ONE data to the BMS system using the OPC UA protocol, ensuring efficient data exchange. Additionally, our AHSC controller can be configured to enable Modbus RTU, allowing it to send data to gateways or DDCs within the BMS network. This provides flexible and seamless connectivity for enhanced system integration and operation.



Output Point

The Output Point allows configuration of linkages between multiple events, inputs/outputs, and events within the system. These linkages can be activated by events with different access levels, triggering correlated outputs and alarm outputs for a more integrated security response.



Common Instant Message Platform Integration

This feature enables automatic notifications to administrators through popular messaging platforms such as Twilio, Line, WhatsApp, Amazon SNS, and SMS when specific events occur. This ensures prompt communication and faster response times from security personnel.



Video Linkage

Video Linkage allows the system to send email and instant message notifications to administrators when specific events occur, providing visual evidence and details of the incident for a more informed response.



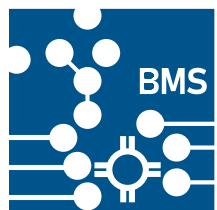
Email Notification:

The Email Notification feature automatically sends an email to notify administrators when specific events occur, ensuring that important security alerts are delivered in a timely manner.



BMS Devices:

The integration with Building Management System (BMS) devices allows configuration of linkages between multiple events and events within the system. These linkages can be activated by events with different access levels, triggering correlated BMS devices for a more holistic and coordinated security approach.



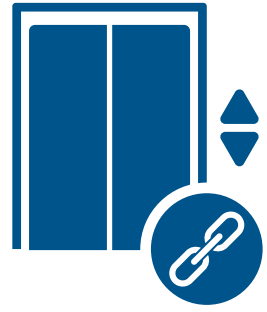
Extensive Linkage Options and Flexibility:

With over 200+ linkage options available in the Global Linkages, the system provides a high level of customization and adaptability. The BMS global linkage rules are extremely flexible, allowing users to set different rules based on system values, attributes, and prompts in the building automation module's rule engine. This ensures a tailored and comprehensive security solution that meets the unique needs of each facility.



Elevator Linkage

Elevator Linkage allows for seamless integration between the access control system and elevator Destination Control Systems (DCS). This feature ensures that access permissions are coordinated with elevator functions, restricting access to specific floors based on individual user permissions and enabling a more secure building environment.



DCS Linkage

Destination Control System (DCS) Linkage integrates the access control system with the building's elevator DCS, allowing for centralized monitoring and control of elevator access and functionality. This integration enables a coordinated response to security events, including automated actions such as initiating lockdown procedures, disabling elevator access to specific floors, or adjusting elevator priority.



Intrusion Alarm Linkage

Intrusion Alarm Linkage connects the access control system with intrusion detection systems, enabling a coordinated response to potential security breaches. When an intrusion alarm is triggered, the system can automatically take appropriate actions, such as activating video surveillance, sending notifications to security personnel, and logging the event for future reference.

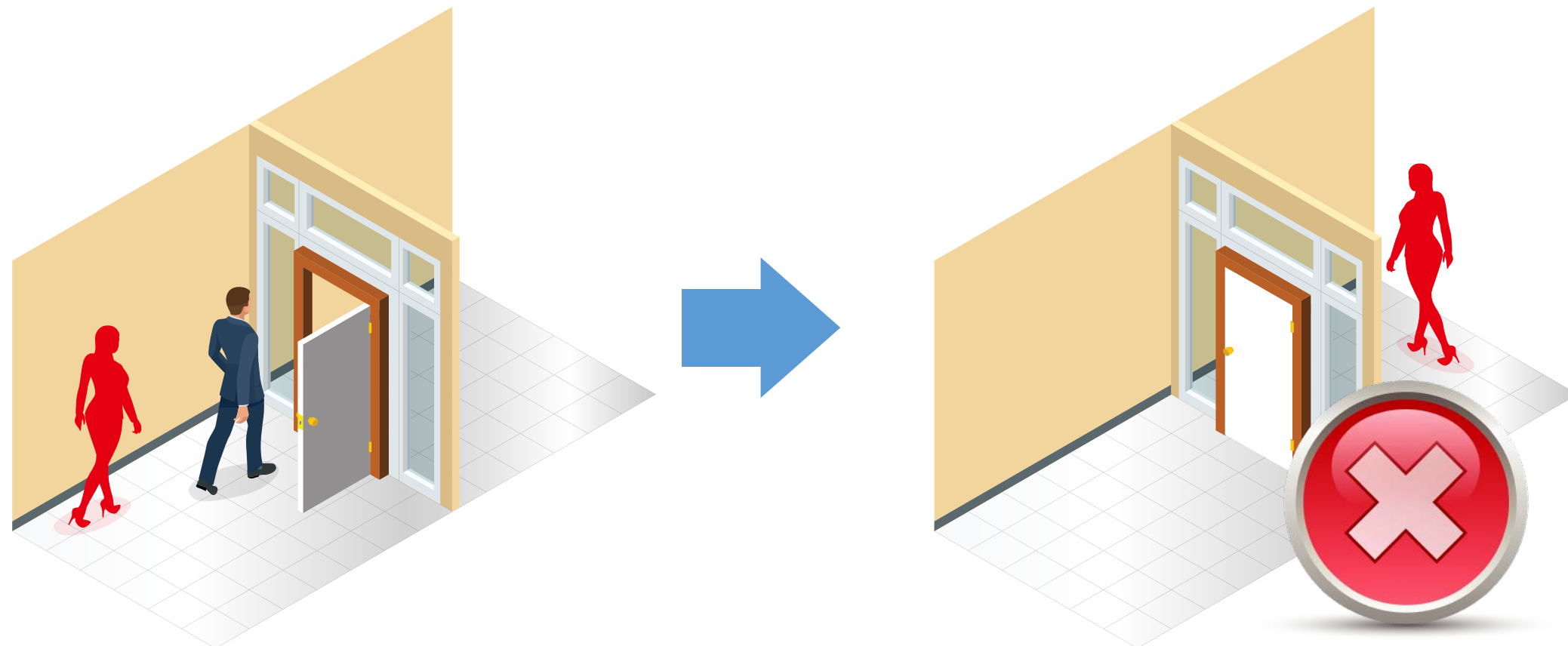


Fire Alarm Linkage

Fire Alarm Linkage integrates the access control system with fire detection and alarm systems, ensuring a rapid and coordinated response to fire incidents. When a fire alarm is triggered, the system can automatically unlock exit doors, send notifications to emergency responders, and initiate other procedures to ensure the safety of occupants.

Global Anti-Passback

Global Anti-Passback is an advanced security feature that enhances the traditional anti-passback function by allowing it to operate across multiple controllers. The core idea behind Global Anti-Passback is to prevent unauthorized personnel from entering or exiting an area without proper credentials, ensuring that the credentials such as access cards, mobile credential, or passwords cannot be shared and used by multiple individuals. By extending the anti-passback functionality across multiple controllers, the system can effectively monitor and regulate access to larger and more complex facilities, providing a comprehensive and adaptable security solution.

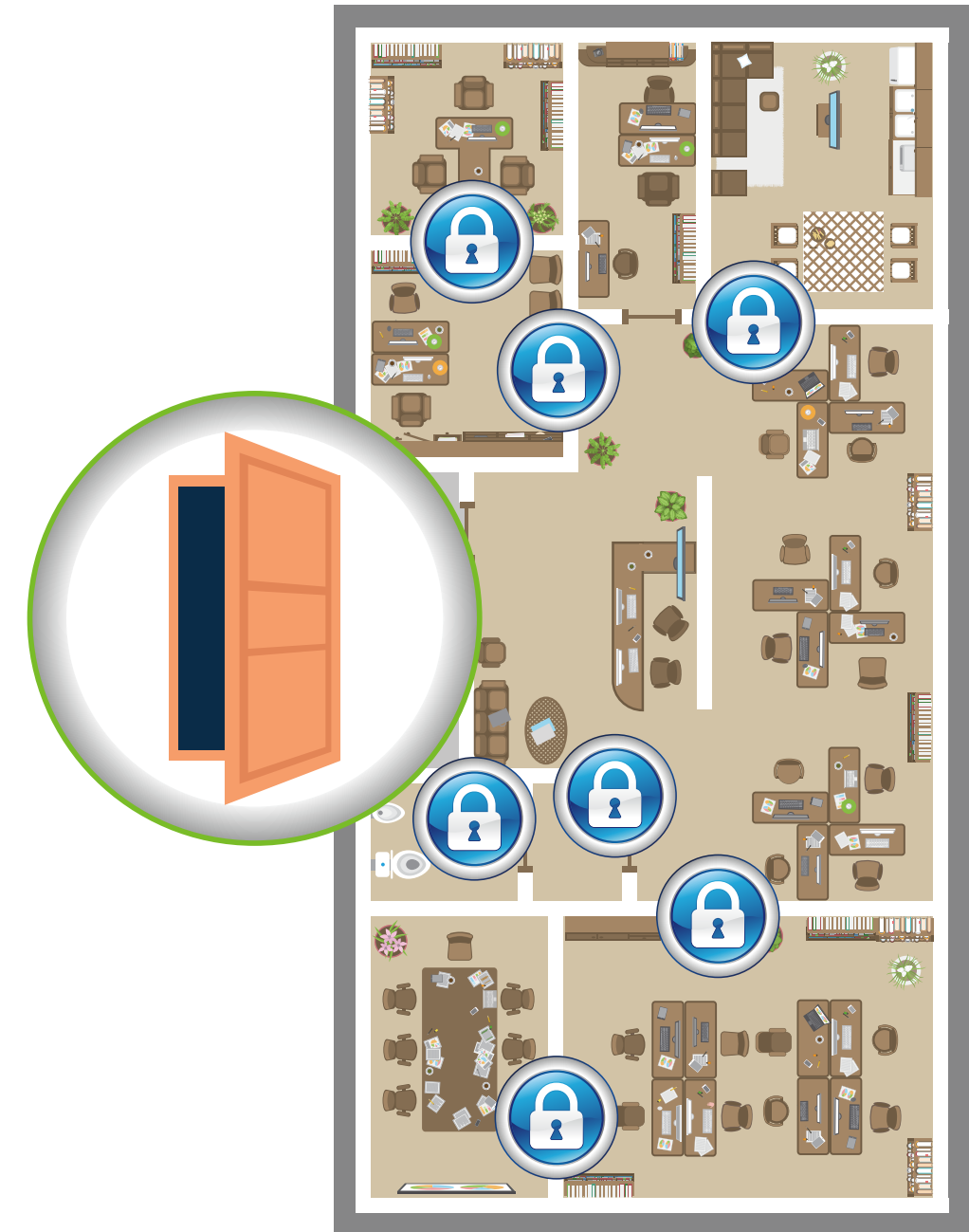


Global Interlock

Global Interlock is an advanced security feature that expands and enhances the traditional interlock function by allowing it to operate across multiple controllers.

The core principle of the Global Interlock feature is to interact with different security areas and prevent personnel or visitors from opening more than one door at a time. This function carefully assigns access authorization based on the status of correlated doors, ensuring that only authorized individuals can gain entry to sensitive areas. By extending the interlock functionality across multiple controllers, the Global Interlock feature provides a more comprehensive and adaptable security solution.

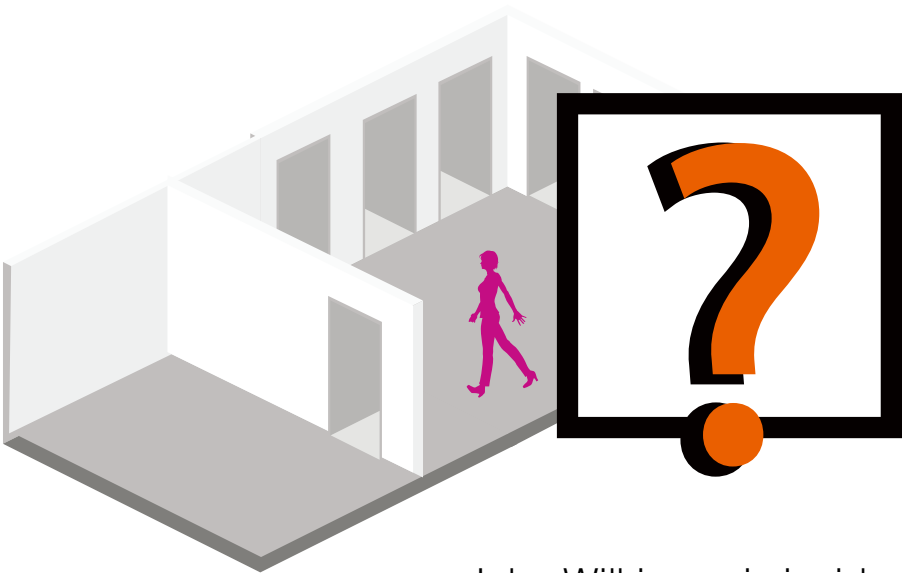
One of the highlights of the Armatura One Global Interlock feature is its ability to support up to 5 doors for global interlock settings as an interlock group. This capability offers users even greater flexibility in designing and implementing their security configurations, ensuring that a wide range of facility layouts and access control requirements can be accommodated.



One door is open, at the same time, the others cannot open

Who is Inside

The Armatura One Security Platform offers a valuable feature called "Who is Inside," which allows administrators to quickly and accurately determine the number of people remaining in a specific area or room at any given time. This function leverages the readers or standalone terminals installed both inside and outside the designated area, providing detailed personal information and access time for each individual.



John Wilkinson is inside the Area A

Zone	Personal ID	First Name	Last Name	Department	Card Number	Last Access Time
Area A	018964	John	Wilkinson	Account	015635	5:10pm
Area B	019156	May	Wilson	Sales	015450	4:10pm
Area C	025426	Walton	Burton	Admin	015628	3:20pm
Area D	032502	Eric	Harris	Sales	016365	2:08pm

Dual Occupancy / Multiple Occupancy Access Limitation

The Dual Occupancy / Multiple Occupancy Access Limitation feature in Armatura One Security Platform allows administrators to regulate the number of people in restricted spaces, ensuring compliance with room capacity limits and maintaining safety standards. This feature is particularly useful in high-security or sensitive areas where strict occupancy limits are required. Key aspects of Dual Occupancy / Multiple Occupancy Access Limitation include:



Occupancy Limits:

Administrators can set minimum and maximum occupancy limits for specific areas, ensuring that the number of people present in the restricted space remains within the defined range (e.g., a minimum of 2 people and a maximum of 5 people)



Real-time Monitoring:

The system constantly monitors the number of occupants in the restricted area, tracking entries and exits to maintain accurate occupancy data.

**EXCEED
LIMITS**



Notification and Alarms:

If the number of occupants in the area falls below or exceeds the defined limits, the system will trigger notifications and alarms to alert security personnel or other relevant parties.

**BELOW
LIMITS**



Access Control:

The system can automatically adjust access rights based on the current occupancy status. For instance, if the number of people in the area is below the minimum limit, the system can temporarily disable exit rights for those inside the room, ensuring compliance with the set occupancy requirements.

Various E-map Systems as Options

The Armatura One Security Platform offers integration with various E-map systems, each with its unique features and advantages. These multiple options ensure that organizations can choose the most suitable mapping system to meet their specific requirements and preferences.



Known for its high level of geographic accuracy, Google Map is an ideal choice for organizations seeking a reliable and user-friendly mapping solution. With its extensive database of global locations and streets, Google Map provides accurate and up-to-date geographical information, making it a popular choice for general navigation and location tracking.

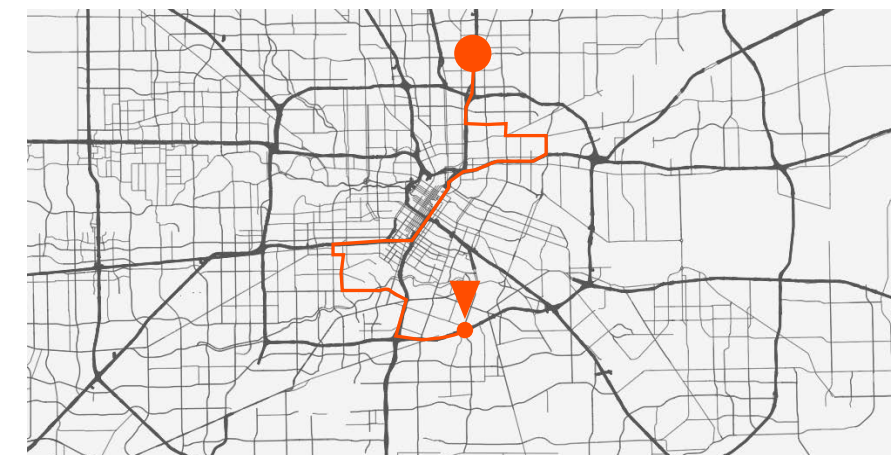


The Super Map system supports 3D multi-level maps, which allows users to visualize and navigate complex structures and spaces more effectively. This feature is particularly useful for organizations managing large or multi-story facilities, as it enables users to better understand the layout and relationships between different areas within the building or campus.



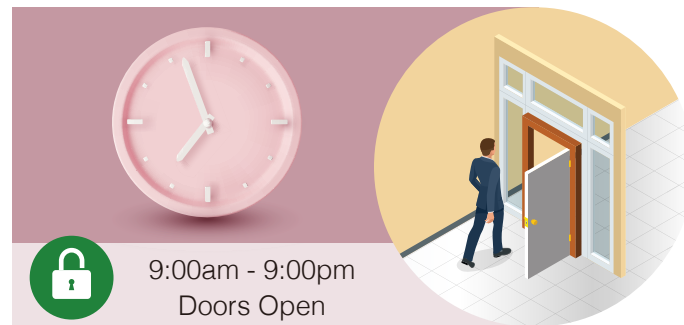
GIS Map

Equipped with personal trajectory functions, GIS Map allows users to track and analyze the movement of individuals within a specific area. This feature is valuable for organizations looking to monitor personnel movement patterns, optimize workspace utilization, or enhance security measures by identifying suspicious or unauthorized activities.



Access Control Time Zone

called Access Control Time Zone ensures that individuals are granted entry only during their authorized time frames and under the appropriate conditions. With the Access Control Time Zone feature, administrators can:



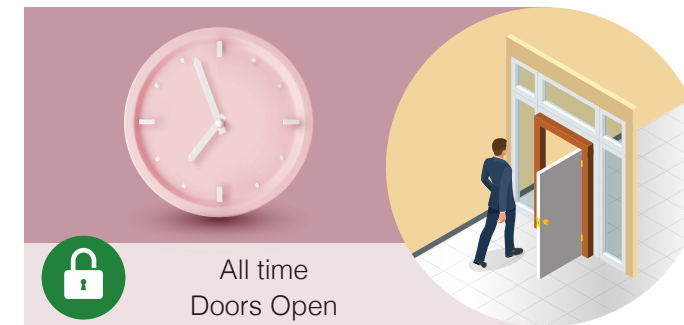
Different Accessibility

Define unique accessibility rules for different time zones, allowing users to access specific areas only during their designated times.



Customize Credential Requirements

Specify varying credential requirements for different time zones, such as using a password in Time Zone A and using biometric (palm / face / fingerprint), mobile credentials or 2-factor authentication in Time Zone B. This added layer of security helps prevent unauthorized access and enhances overall facility safety.



Unlimited Time Zones

Armatura One supports an unlimited number of time zones, providing administrators with the flexibility to create a highly customized access control system that caters to their unique needs.



Monitor and Adjust

Review access logs to analyze usage patterns and adjust time zones as needed to optimize security measures and resource allocation.



Programmable Supervised Input

The Armatura One Security Platform offers a robust feature called Programmable Supervised Input, which, along with Auxiliary Input, provides connections to various devices and alarm systems for enhanced security. This functionality enables the platform to monitor and manage a wide range of connected devices, ensuring a comprehensive and effective security solution. Armatura One supports four states of supervised inputs: Active, Inactive, Open, and Short, each representing a different status of the input. It also includes support for defining inputs as Normally Open (NO) or Normally Closed (NC), allowing the controller to recognize whether an Open or Close state should trigger an action, ensuring compatibility with diverse device operation requirements.

- 1. Active: The input circuit is active and functioning as intended.
- 2. Inactive: The input circuit is inactive and not currently engaged.
- 3. Open: The input circuit has been opened, which could indicate a potential issue or tampering.
- 4. Short: The input circuit has been shorted, suggesting a possible malfunction or security breach.

ARMATURA ONE Access

Home / Access / Reports / All Transactions

Time From 2023-06-06 11:31:26 To 2023-09-06 23:59:59 Personnel ID Device Name

Refresh

Export

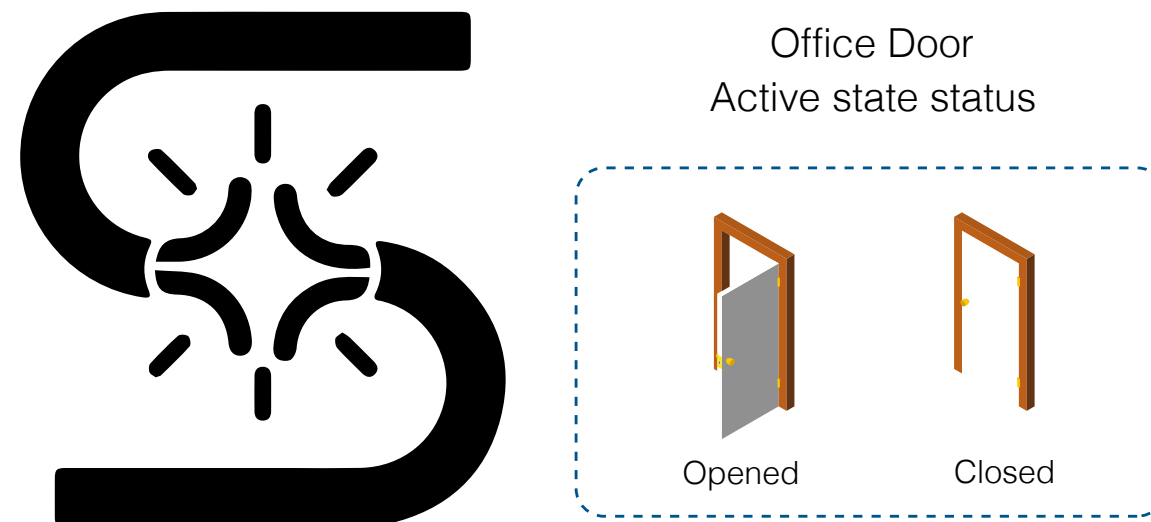
Export photos

Event ID	Time	Area Name	Device Name	Event Point	Event Description
5855	2023-09-06 11:30:01	Area Name	10.8.51.4	Auxiliary Input-1	In-Active (Auxiliary Input)
5854	2023-09-06 11:29:59	Area Name	10.8.51.4	Auxiliary Input-1	Active (Auxiliary Input)
5853	2023-09-06 10:54:...	Area Name	10.8.51.4	Auxiliary Input-1	Open (Auxiliary Input)
5852	2023-09-06 10:54:...	Area Name	10.8.51.4	Auxiliary Input-1	Shorted (Auxiliary Input)

Device Name	Serial Number	Area	Operation Status	Current Status	Commands List
10.8.51.249	TH40623060032	Area Name	Disconnected	Disconnected	535
10.8.51.233	CN30122200004	Area Name	Get real-time event	Normal	0
10.8.14.62	TH40623060075	Area Name	Connecting device	Disconnected	158
10.8.51.120	4366172000005	Area Name	Disconnected	Disconnected	485
10.8.51.223	CN30423150010	Area Name	Get real-time event	Normal	0
10.8.51.219	TH40523280059	Area Name	Disconnected	Disconnected	7
10.8.51.236	TH40623060067	Area Name	Get real-time event	Normal	0
10.8.51.210	CTKG232760001	Area Name	Get real-time event	Normal	0

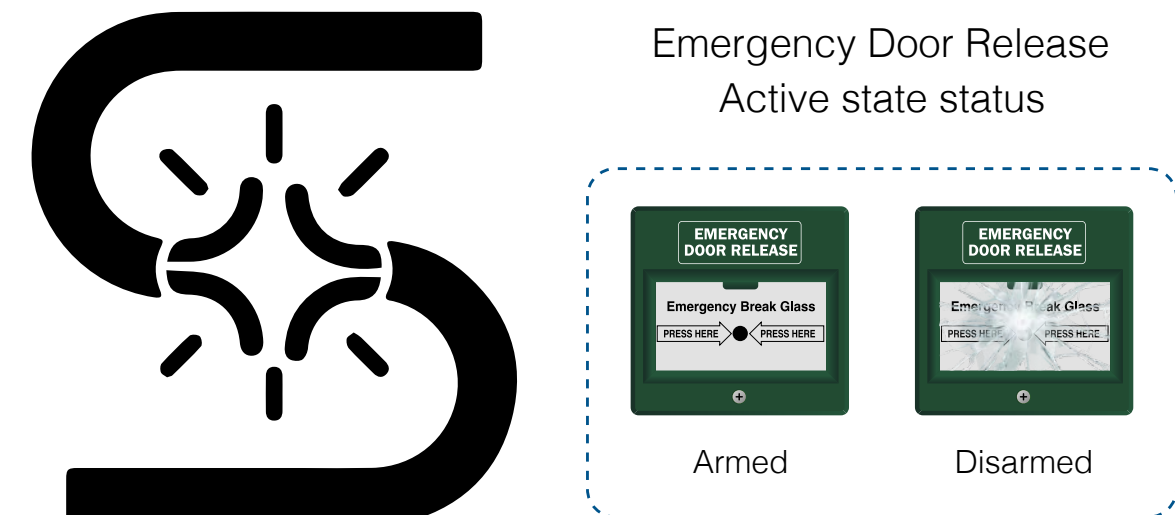
- Access Control System:

In this scenario, the can be connected to a door contact sensor. The Active state indicates that the door is closed and secured, while the Inactive state suggests that the door is open but still within normal operating parameters. The Open state may indicate that the door has been left open or forced open without proper access, while the Short state could signify a malfunction in the sensor or potential tampering with the system.



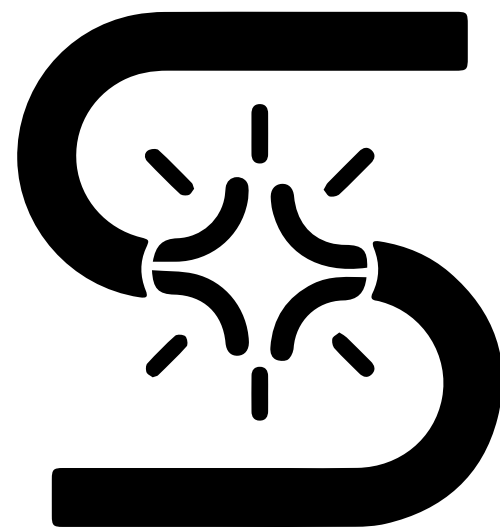
- Intrusion Detection:

The supervised input can connect to motion detectors or glass break sensors. When in the Active state, the sensor is actively monitoring for movement or glass break events. The Inactive state means the sensor is disarmed, possibly during business hours or when the area is occupied. An Open state could indicate a potential issue with the sensor's connection, while a Short state might suggest tampering or a malfunction.

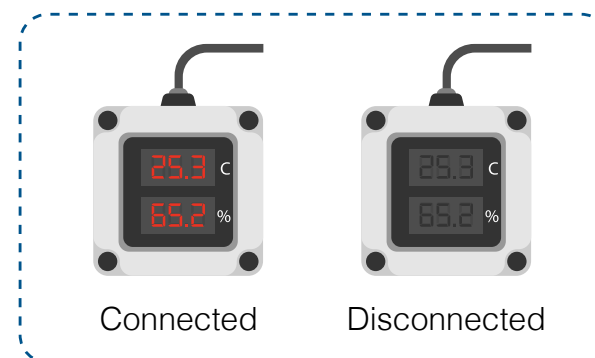


- Environmental Monitoring:

The supervised input can monitor temperature, humidity, or water leak sensors in critical areas such as server rooms or storage facilities. An Active state represents the environmental conditions being within acceptable parameters, while the Inactive state indicates that the monitoring is paused. An Open state could signify a disconnection of the sensor, and a Short state might indicate a malfunction or potential tampering with the sensor.

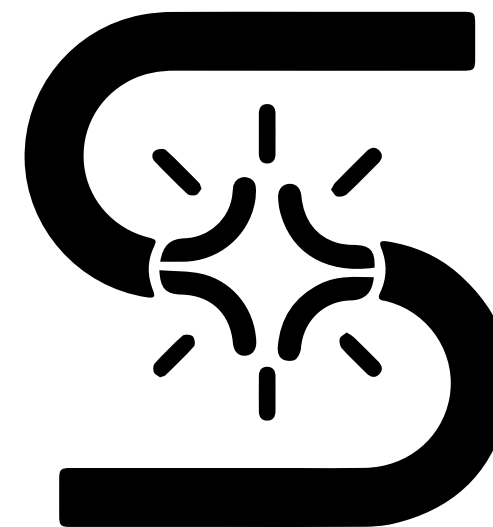


Temperature and Humidity Sensor
Active state status

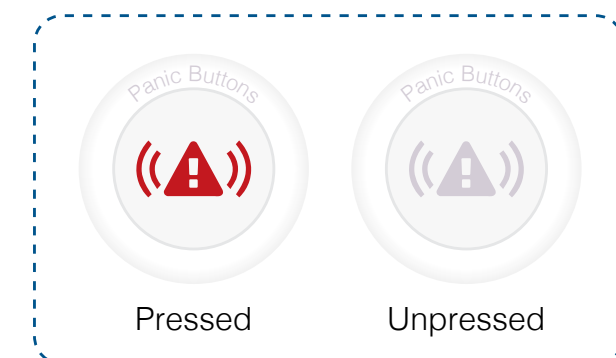


- Emergency Response Systems:

Supervised inputs can be connected to panic buttons or emergency call stations. The Active state indicates that the panic button has been pressed or the emergency call station is in use, signaling an emergency situation. The Inactive state signifies that the system is ready for use but not currently engaged. An Open state may indicate a potential issue with the wiring or connectivity, while a Short state might suggest tampering or a malfunction in the system.



Panic Buttons
Active state status





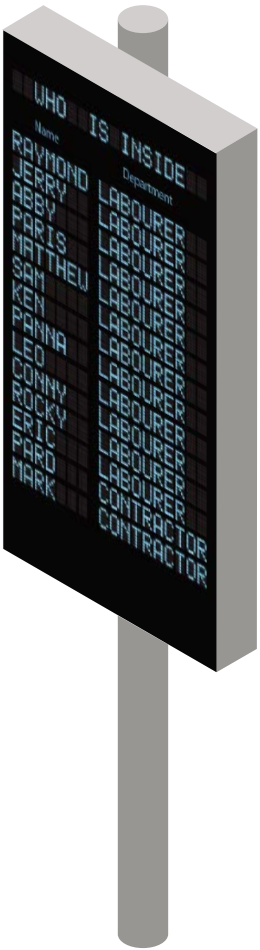
Flexible and Editable Text Function for LED/LCD Display Panel (Coming Soon)

The Armatura One Security Platform offers a unique feature that enhances user experience and communication by allowing administrators to customize the display text on LED/LCD panels for various events. This flexible and editable text function contributes to a more personalized and efficient security solution tailored to user requirements.

Key benefits of the flexible and editable text function include:

WHO IS INSIDE			
Name	Department	Name	Department
RAYMOND	LABOURER	PANNA	LABOURER
JERRY	LABOURER	LEO	LABOURER
ABBY	LABOURER	CONNY	LABOURER
PARIS	LABOURER	ROCKY	LABOURER
MATTHEW	LABOURER	ERIC	LABOURER
SAM	LABOURER	PARD	CONTRACTOR
KEN	LABOURER	MARK	CONTRACTOR

LED / LCD display
to show who is inside the specific area





Customized Messaging:

Administrators can create tailored messages for specific events, such as access granted, access denied, alarms, or system status updates. This ensures that users receive clear, relevant information on the display panel, improving overall communication.



Enhanced User Experience:

Customized display text allows users to quickly understand the system's response to their actions, reducing confusion and streamlining interactions with the security platform.



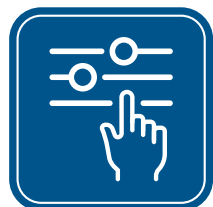
Multi-Language Support:

The editable text function can be used in conjunction with the platform's multi-language support to display messages in users' native languages. This further enhances accessibility and user experience for a diverse range of users.



Branding Opportunities:

Organizations can leverage this feature to reinforce their brand identity by displaying company-specific messages or logos on the LED/LCD panels.



Easy Configuration:

The Armatura One Security Platform provides an intuitive interface for administrators to easily edit and configure display text, allowing for quick updates and adjustments as needed.



Roll Call and Muster Reporting

Generate reports to account for all users present within a designated area. These reports serve the purpose of verifying the safe evacuation of all users in case of an emergency.



Multi-Language Support

Armatura One is designed with a user-friendly interface that supports multiple languages, ensuring that users from different regions can comfortably use the system.

With support for 19 languages, Armatura One caters to a diverse range of users and helps create a more inclusive and accessible security solution.

The languages supported by Armatura One include:



Comprehensive Reporting

Armatura One Security Platform offers a powerful reporting feature that enables users to generate customizable reports based on various criteria and statuses. This functionality allows for better analysis and understanding of security events and trends within the facility, assisting in data-driven decision-making and enhancing overall security management. Key aspects of the Comprehensive Reporting feature include:

- **Customizable Reports:**

Users can configure reports based on different criteria, such as Event ID, Time, Area Name, Device Name, Event Point, Event Description, Media File, Personnel ID, First Name, Last Name, Person Type, Card Number, Department Number, Department Name, Reader Name, Verification Mode, and Remarks.

- **Multiple Formats:**

Reports can be generated in various formats, including Excel, CSV, and PDF, ensuring compatibility with different software and platforms.

- **Scheduled Reports:**

Users can schedule reports for automatic generation at specified intervals, streamlining the reporting process and ensuring timely delivery of relevant data.

- **Multiple Delivery Options:**

Reports can be automatically sent to specified recipients via various channels, such as Email, WhatsApp, Line, SMS, and Amazon SNS, providing flexibility in communication and ensuring stakeholders stay informed.

- **Automatic Report Saving:**

The system can automatically save generated reports in dedicated locations and formats for easy integration with other systems or applications, simplifying data management and accessibility.



Backup and Restore

Includes a robust backup and restore function to ensure the integrity and availability of essential data, allowing administrators to schedule regular database backups and restore the system if necessary.



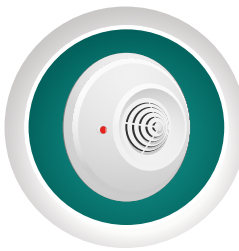
Backup and Restore

Integration with Third-Party Systems

Armatura One can be integrated with various third-party systems, such as video surveillance systems, fire alarms, and building management systems (BMS), providing seamless interoperability and enhancing overall security.



Alarm Siren



Smoke Detector



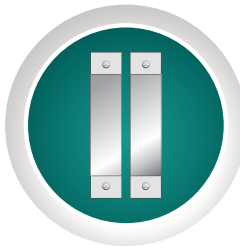
Motion Sensor



Glass Break Detector



Security Camera



Door Contact



Alarm System



Mobile App

Armatura One Security Platform offers seamless integration with its mobile applications, providing users with the convenience and flexibility to manage their security systems from their smartphones or tablets. These mobile apps include "Armatura ID" and "Armatura Connect," designed to enhance the user experience and provide additional features for mobile access and device configuration.

Armatura Apple and Google Wallet Powered By HID



Apple Wallet



Google Wallet

iOS & Android



 Bluetooth™

 NFC



Mobile Credential in Apple Wallet and Google Wallet

Armatura One Security Platform supports mobile credentials in Apple Wallet and Google Wallet, enabling users to securely store and use their access cards directly on their smartphones or smartwatches. With a simple tap of the device, doors can be unlocked quickly and conveniently—eliminating the need for physical cards. Mobile credentials are encrypted, easily managed remotely, and offer enhanced security with biometric authentication such as Face ID, Touch





Scalability

The Armatura One Security Platform is designed with scalability in mind, providing organizations with a flexible and adaptable solution that can grow with their needs. With sufficient resources, the system can support an extensive range of capabilities, ensuring that the platform remains a reliable security and access control solution for organizations of any size.

Key features of the Unlimited scalability include:

Unlimited Access Levels: The platform can support an unlimited number of access levels, providing organizations with the flexibility to define and manage various levels of access based on user roles and responsibilities.



Unlimited RFID
Cards



Unlimited
Personnel



Unlimited Access-Controlled
Doors and Attendance Points



Unlimited Monthly
Visitors



Unlimited
Surveillance Cameras



5,000+
simultaneous clients



Threat Level

Armatura One Security Platform's Threat Level feature empowers administrators to swiftly respond to diverse security situations by modifying user access rights and credential requirements. This flexible functionality enhances control over security measures, ensuring an agile and effective response to various scenarios.

Armatura One accommodates 5 threat levels, each featuring customizable settings for optimal customization.

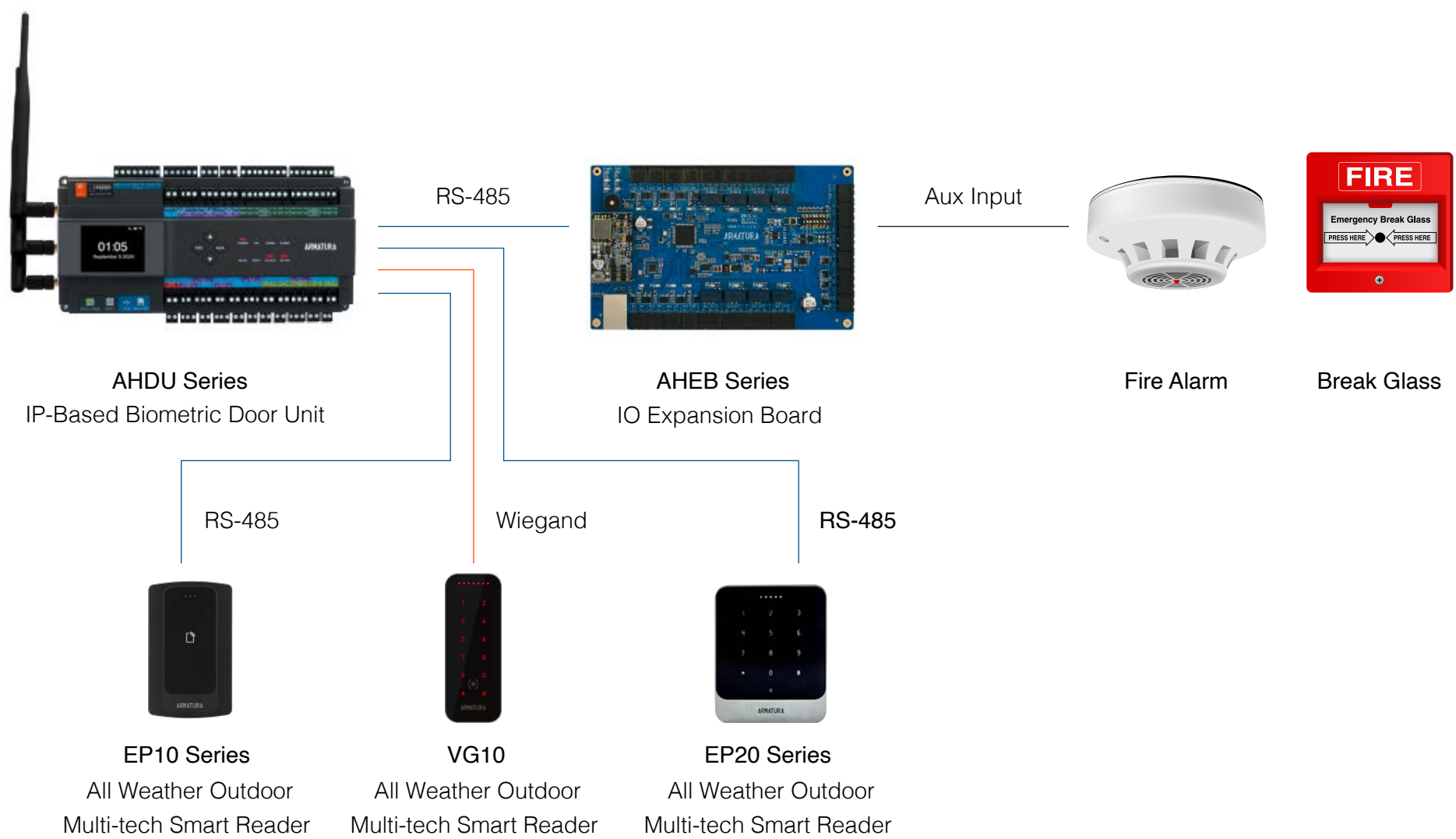
- Level 1:** Normal security situation, standard access rights and credential requirements.
- Level 2:** Increased threat level, stricter security measures, and potentially additional access restrictions or credential factors.
- Level 3:** Significant security concern, stringent access restrictions, and multi-factor authentication.
- Level 4:** Critical security situation, highest level of access control and verification measures.
- Level 5:** Emergency threat level, extreme situations, immediate and decisive action, potential restriction of access to essential personnel or temporary facility lockdown.

Name 🔍 OK Clear			
☐	Name	Threat Level	Remarks
☐	Low	1	
☐	Alert	2	
☐	Higher	3	



IO Board Management

For the management of I/O expansion boards, the system allows administrators to add or remove I/O boards as needed. Furthermore, it provides the ability to configure various communication protocol types. The system also enables the setting of RS-485 ports and RS485 addresses for seamless integration with other devices and systems.

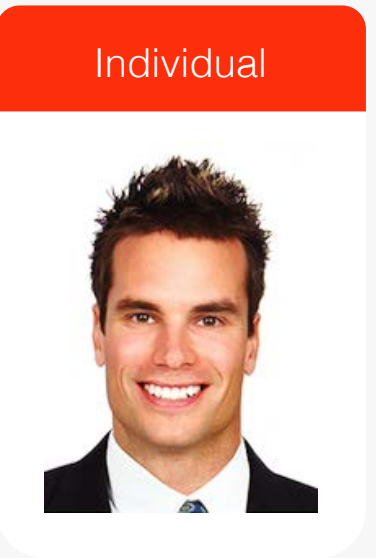


Multi-Person and Multi-Person Group Access Setting

Armatura One Security Platform offers advanced access control with the Multi-Person and Multi-Person Group Access Setting feature. This functionality ensures that specific doors can only be opened when multiple authorized persons access the door simultaneously or when one or more individuals from each designated person group are present. Key aspects of the Multi-Person and Multi-Person Group Access Setting feature include:

- **Multi-Person Access:**

The system supports up to 25 persons for multi-person access, requiring their simultaneous presence to open the door. This feature enhances security in high-risk or sensitive areas by ensuring that a single individual cannot access the area without the presence of other authorized personnel.



- **Multi-Person Group Access:**

The system allows users to create up to 5 person-groups, with each group supporting up to 5 persons. A door with this access setting can only be opened when one or more individuals from each group access the door at the same time. This feature ensures that access to specific areas is granted only when representatives from each designated group are present, promoting collaboration and oversight in critical situations.

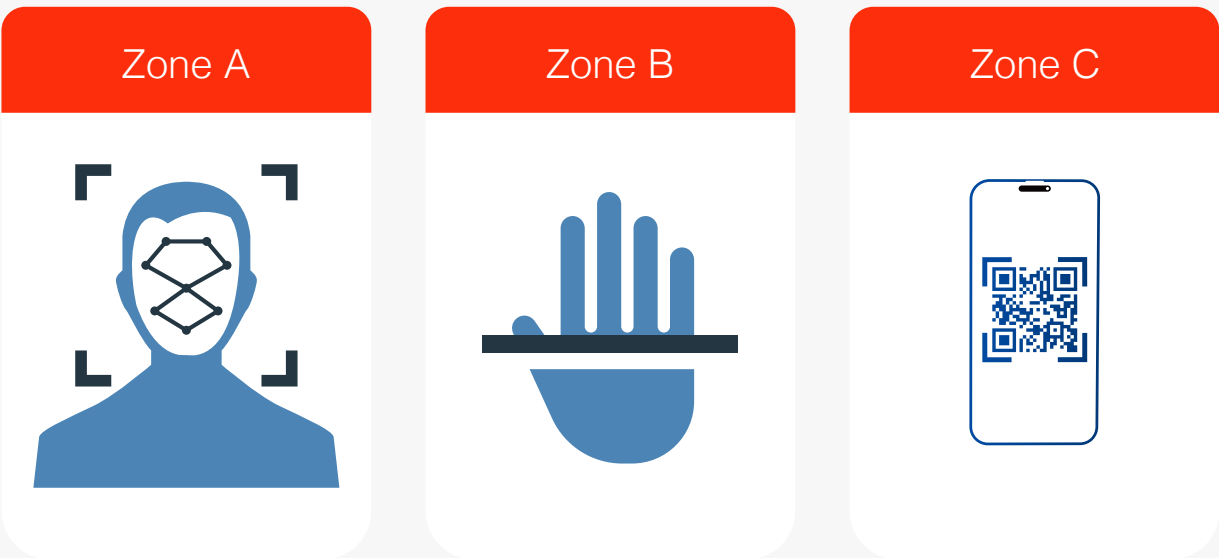


Verification Mode and Verification Mode Group Access Setting

Armatura One Security Platform offers advanced access control with the Verification Mode and Verification Mode Group Access Setting features. This functionality ensures that specific access points require different credential verification methods depending on the time zone, enhancing security and flexibility in access control management. Key aspects of the Verification Mode and Verification Mode Group Access Setting feature include:

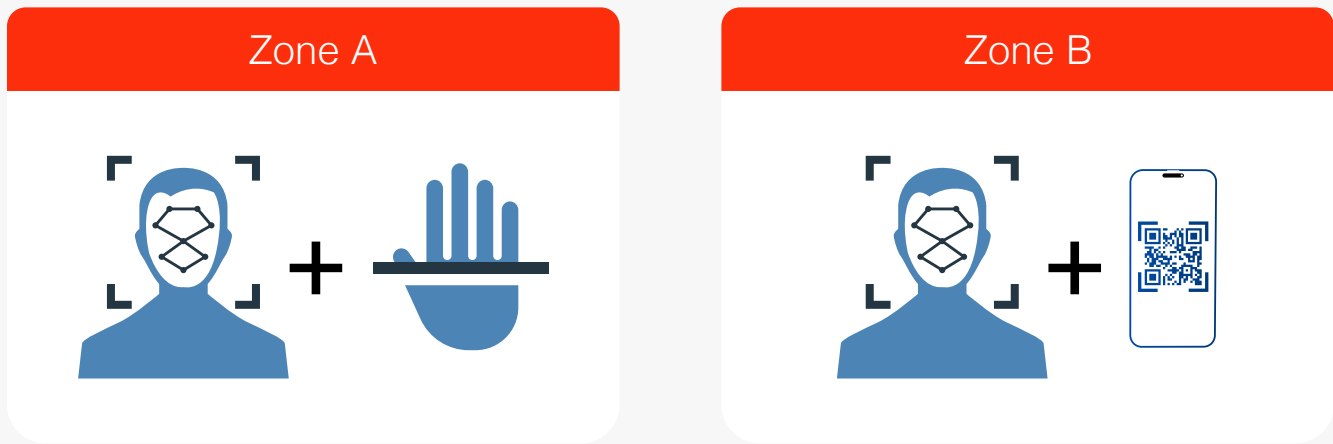
- **Verification Mode:**

The system supports changing credential verification requirements based on different time zones, with up to 15 time zones supported per day. For example, users may be required to use Face verification in Time Zone A and Palm verification in Time Zone B. This feature allows for dynamic access control that adapts to various security needs throughout the day.



- **Verification Mode Group:**

This setting allows the system to enforce different multi-factor verification combinations for users in different time zones. For instance, users might be required to use Password + Face verification in Time Zone A and Face + Palm + Mobile Credential verification in Time Zone B. The system supports an unlimited number of verification mode groups and can accommodate an unlimited number of persons in each group.



First-Person Normally Open

The Armatura One Software features a First-Person Normally Open function that enables the door to remain open for a specified interval after the first successful verification by a person with the First-Person Normally Open access level. Once the valid interval has expired, the door will automatically close and restore its previous access settings.

Administrators can configure the First-Person Normally Open settings for specific doors, including the door itself, the door opening time zone, and the personnel with the First-Person Normally Open access level. A single door can have multiple time zones set for the First-Person Normally Open function. The software interface for each door displays the number of existing First-Person Normally Open settings, allowing for easy monitoring and management.



Holiday Access Setting

To accommodate the varying access requirements during holidays or special events, Armatura One Software provides a holiday access setting feature with unlimited holiday support. Administrators can configure the system to allow or restrict access during specific dates or periods, ensuring that the security measures in place remain appropriate and effective, even during non-standard operating hours or events. This flexibility allows organizations to adapt to any number of holidays or special occasions without limitations.

Weekday



Monday - Friday
All Doors Open

Weekend



Saturday - Sunday
All Doors Closed

Holiday



Public Holiday
All Doors Closed

Limited Access

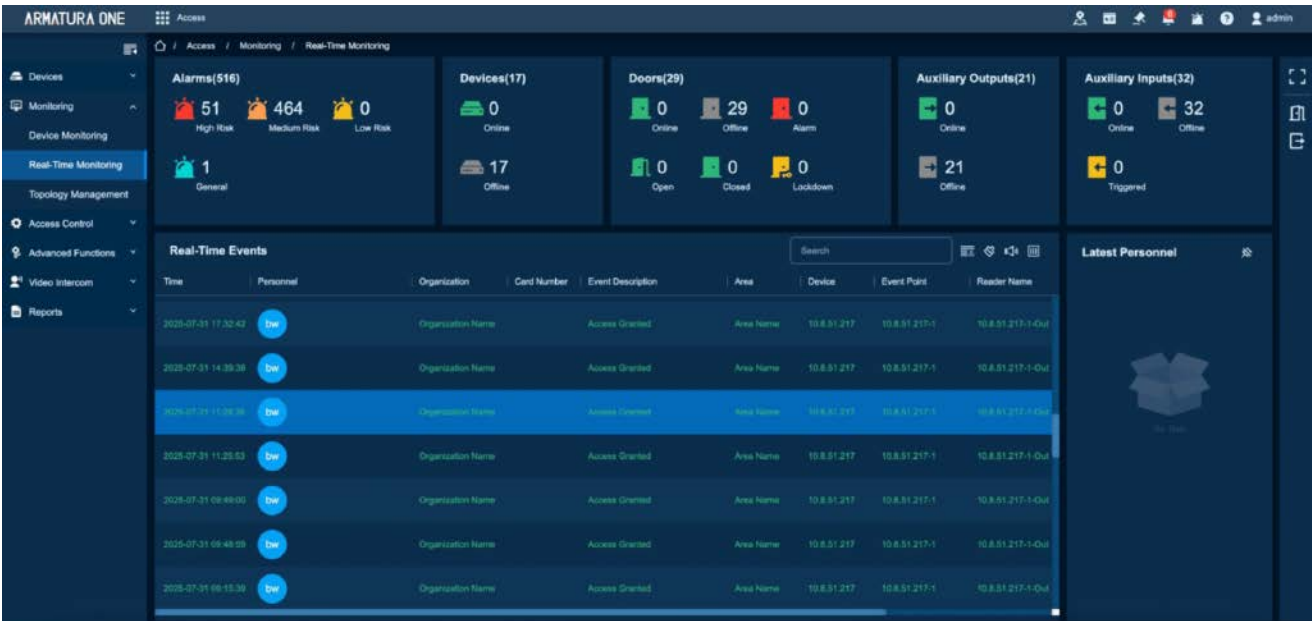


All Day
Specified Door(s) Unlocked



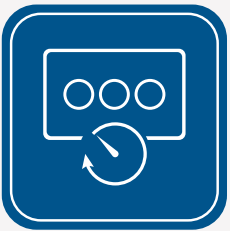
Edge Device Real-Time Monitoring

Armatura One Security Platform offers Edge Device Real-Time Monitoring, providing continuous supervision of various edge devices such as readers, standalone terminals, controllers, auxiliary input devices, auxiliary output devices, and sirens. This feature ensures that the devices' real-time statuses are monitored and displayed, allowing quick identification of issues and immediate response to potential security breaches.



- **Real-Time Status:**

The system continuously monitors and displays the real-time status of edge devices, such as whether they are online, offline, or experiencing a tamper alarm.



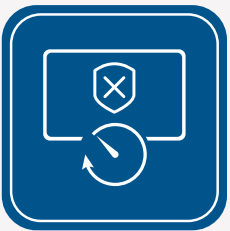
- **Device Health Monitoring:**

The feature keeps track of the devices' health, allowing administrators to identify potential issues or malfunctioning hardware that may require maintenance or replacement.



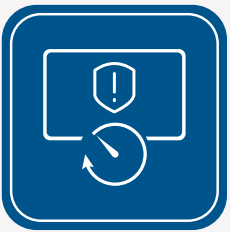
- **Tamper Detection:**

The monitoring system can detect tamper alarms, alerting security personnel to potential security breaches or attempts to manipulate the devices.



- **Disable Monitoring:**

The system displays the status of disabled devices, ensuring that security personnel are aware of any devices that are not currently operational.



Notification Status Filtering

Armatura One Security Platform offers advanced Notification Status Filtering within its real-time monitoring capabilities. This feature enables users to filter and prioritize notifications based on their status level, ensuring that relevant and critical alerts are brought to their attention promptly via their preferred communication channels, while less urgent notifications are sent to other destinations, such as email. Key aspects of the Notification Status Filtering feature include:



- Notification Status Levels:

Armatura One supports four notification status levels—Urgent, Important, General, and Notice—to categorize alerts based on their priority and importance.



- Customizable Filtering:

Users can configure their notification preferences to display only specific status levels and choose the delivery method for each level, allowing them to focus on alerts that require immediate attention through instant messaging apps like Line and WhatsApp, while keeping less critical notifications in their email or a general email account.

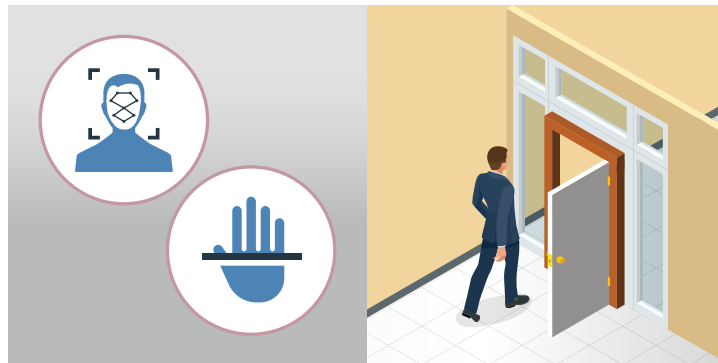


- Efficient Alert Management:

By filtering notifications based on their status and preferred delivery channel, users can manage alerts more effectively, ensuring that critical events are promptly addressed and reducing the risk of overlooking important notifications amidst a flood of less critical alerts.

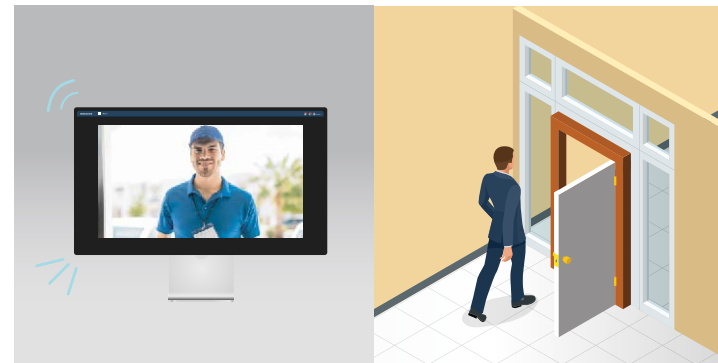
Onsite Verification (Two-Factor Verification)

Armatura One Security Platform offers the Onsite Verification feature, which implements a 2-Factor Verification process for enhanced security. When users are subject to Onsite Verification, they must pass through two separate verification stages. The first stage is a standard user verification, while the second stage involves remote verification by an administrator. Key aspects of the Onsite Verification (Two-Factor Verification) feature include:



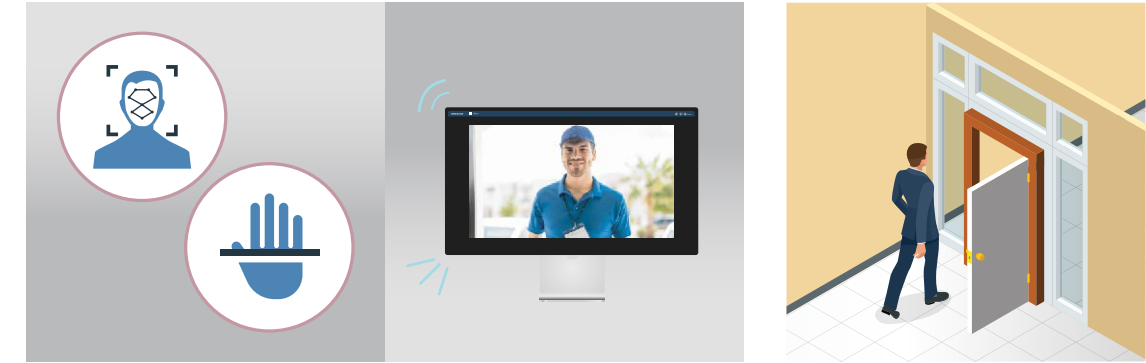
- **Two-Factor Verification:**

The user must first pass an initial verification stage, such as presenting an access card, entering a PIN, or using biometric authentication. Once the first verification is successful, the system prompts the administrator to initiate the second stage of verification.



- **Remote Administrator Verification:**

The administrator can remotely assess the situation through tools such as an intercom or live video feed from a camera. This allows them to verify the user's identity and the context of the access request before granting permission.



- **Enhanced Security:**

The Two-Factor Verification process adds an extra layer of security by requiring administrative approval for access. This helps prevent unauthorized access and ensures that only approved individuals can enter restricted areas.

Supports 3rd Party Network Time Service (NTP Server)

Armatura One Security Platform provides support for synchronizing time with 3rd party Network Time Services using the NTP (Network Time Protocol) to ensure all connected devices have the most accurate and consistent time information. Key aspects of the 3rd Party Network Time Service (NTP Server) support include:



- Time Synchronization:

The system synchronizes time across all connected devices, including access control devices and servers, ensuring that time-sensitive operations, logs, and events are accurately recorded and consistent throughout the entire system.



- NTP Protocol:

Armatura One utilizes the widely-adopted NTP protocol to sync time with 3rd party Network Time Services, ensuring compatibility with a broad range of external time sources.



- Reduced Time Drift:

By synchronizing with an external NTP server, the system minimizes time drift between devices, resulting in more accurate event and log timestamps, and preventing potential issues caused by time discrepancies.



- Enhanced Security:

Accurate timekeeping is essential for maintaining a secure environment, as it helps ensure that time-based access control policies are properly enforced and security events are correctly timestamped.

Duress Alert

Armatura One Security Platform offers a Duress Alert feature, which is a critical function of an electronic access control system designed to protect users from coercive situations. When a user is forced to grant unauthorized access to an intruder, the user can discreetly trigger a silent duress alert by entering a specific duress code, such as a password, fingerprint, or palm. Key aspects of the Duress Alert feature include:



Multiple Duress Code Options:

The system supports various types of duress codes, including password, fingerprint, and palm. This flexibility allows users to choose a method that is convenient and discreet for them in a coercive situation.



User Protection:

The Duress Alert feature is designed to protect users from potentially dangerous situations by providing a discreet way to signal for help without escalating the situation.



Silent Warning:

When a user is under duress and enters the designated duress code, the system sends a silent alert to administrators or security personnel without any audible or visible indications, preventing the intruder from becoming aware of the triggered alert.



Enhanced Security:

By offering the Duress Alert feature, Armatura One Security Platform helps maintain a secure environment and provides an additional layer of protection for users who may be subject to coercive activity.



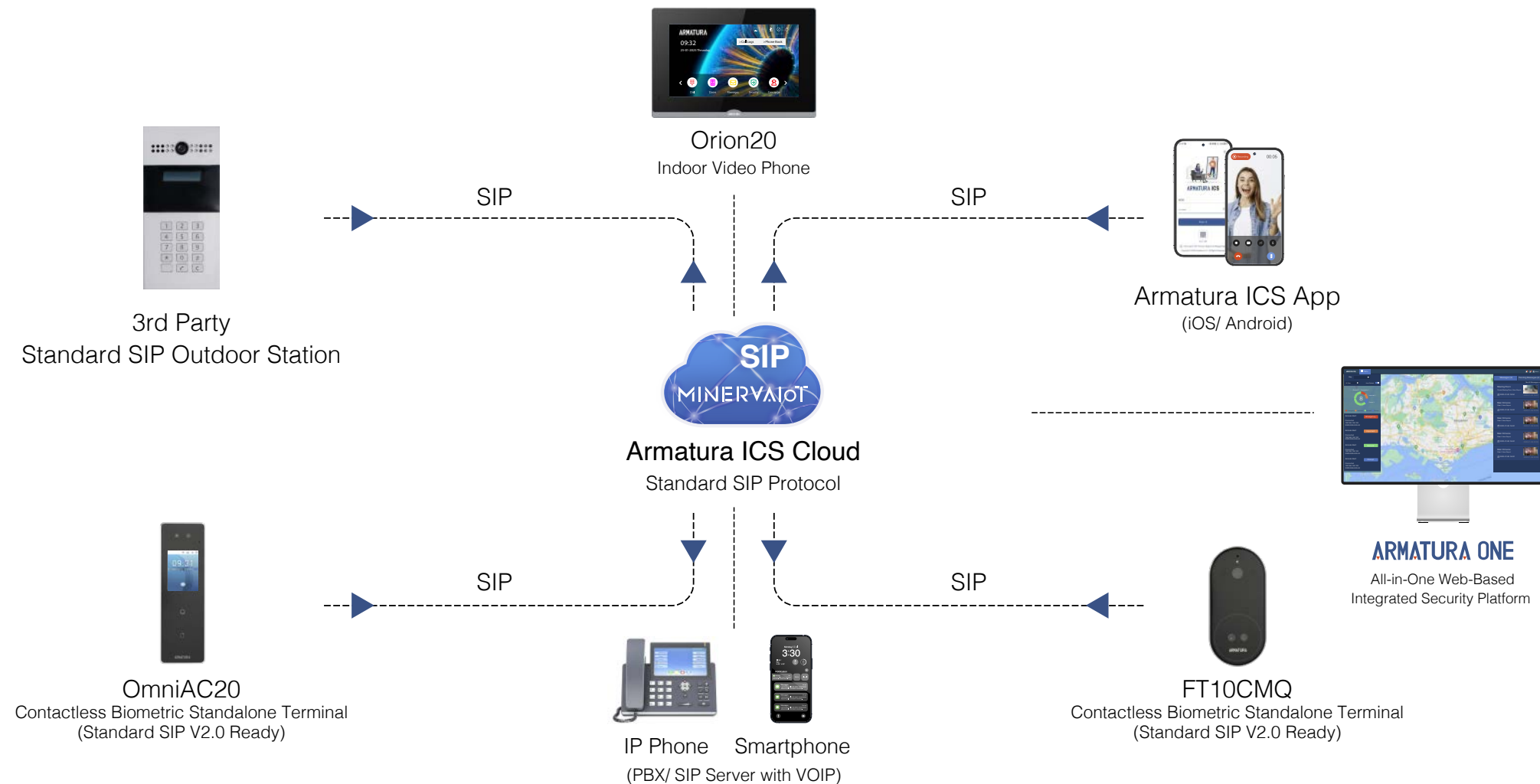
Immediate Response:

Upon receiving the duress alert, security personnel or administrators can respond quickly to the situation, coordinating with law enforcement or taking necessary actions to ensure the safety of the user.



Professional Video Intercom Functions Standard SIP Protocol with Armatura ICS Cloud

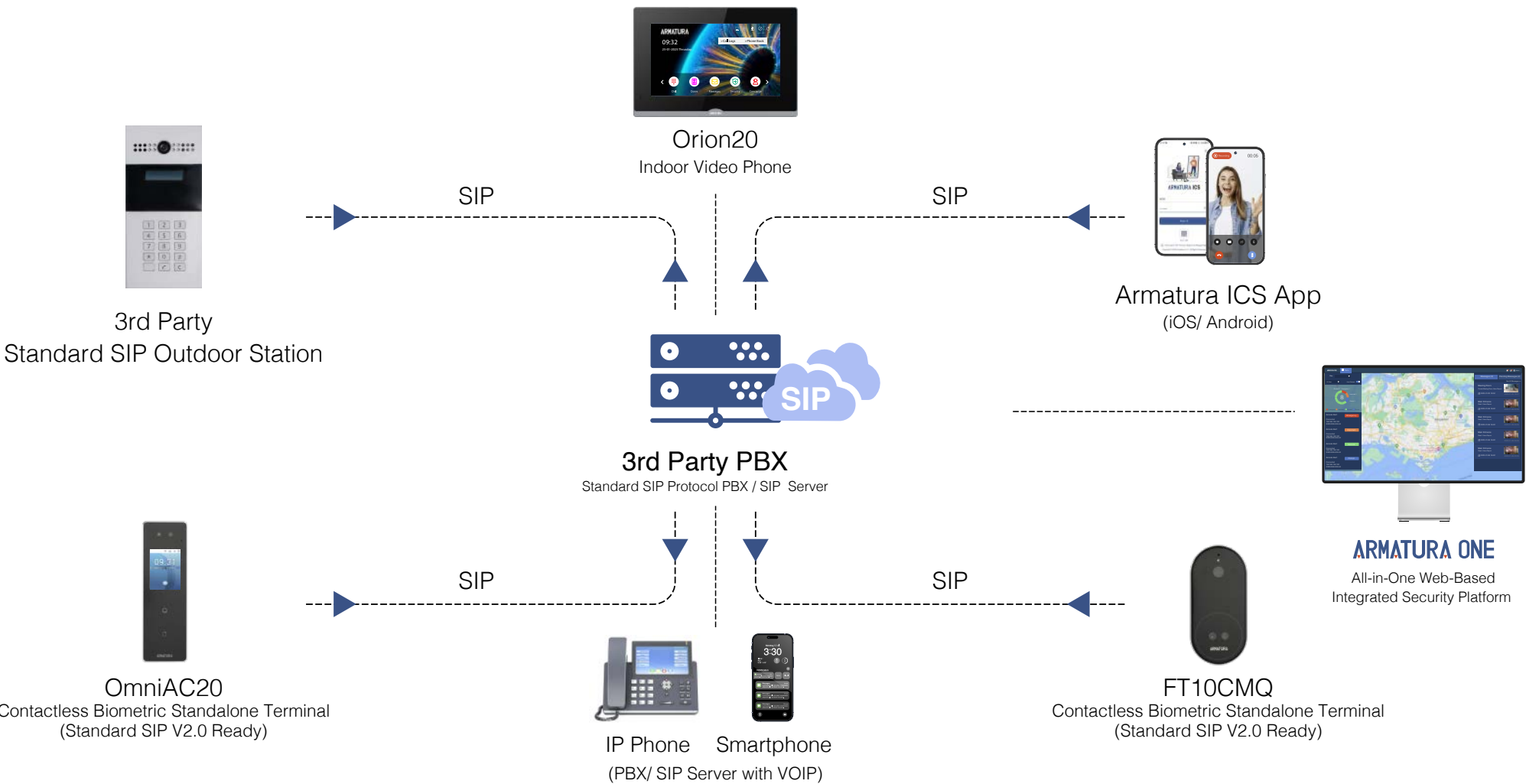
By combining Armatura One with the Armatura ICS smartphone app, the Access Control Terminal, and the ARMATURA ICS Cloud (a public cloud service), users can leverage Video Intercom products for efficient and convenient two-way audio and video verification during entry control. This integration utilizes the standard SIP protocol, enabling seamless communication between the Video Intercom system, Armatura's Access Control Terminal, and the user's smartphone. The Armatura ICS app allows users to easily receive and respond to video intercom calls, granting or denying access remotely through the cloud. This streamlined approach enhances security and provides a user-friendly entry control experience.





Professional Video Intercom Functions Standard SIP Protocoll with 3rd Party PBX

Armatura One supports Video Intercom functionality via the standard SIP protocol with third-party PBX systems. This integration enables secure two-way audio and video verification for entry control, ensuring smooth communication between Video Intercom devices, Armatura terminals, mobile apps, and PBX platforms. With the Armatura ICS app, users can conveniently answer intercom calls, grant or deny access, and manage entry points remotely—delivering a secure and user-friendly access control experience





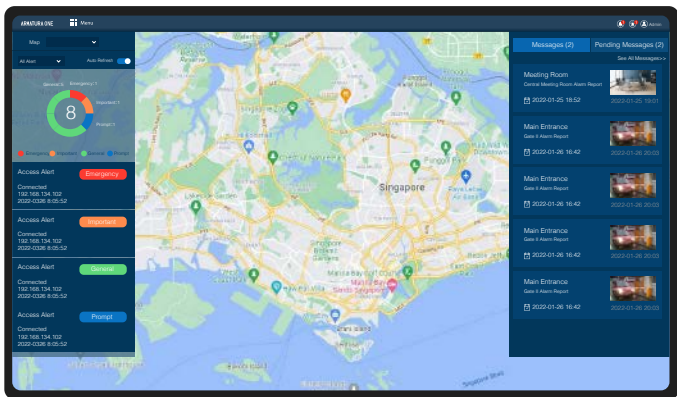
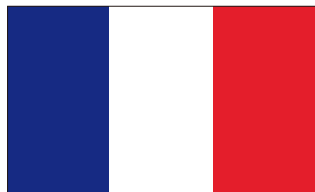
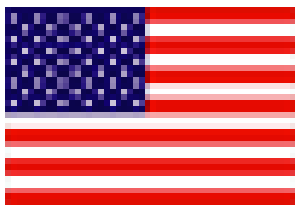
Time & Attendance Module

The Time and Attendance Module is a comprehensive, web-based management tool designed to handle complex time and attendance requirements across various industries. It offers a wide range of features, including flexible group scheduling, multi-location management, and integration with third-party HR management systems, ensuring efficient and accurate personnel management.

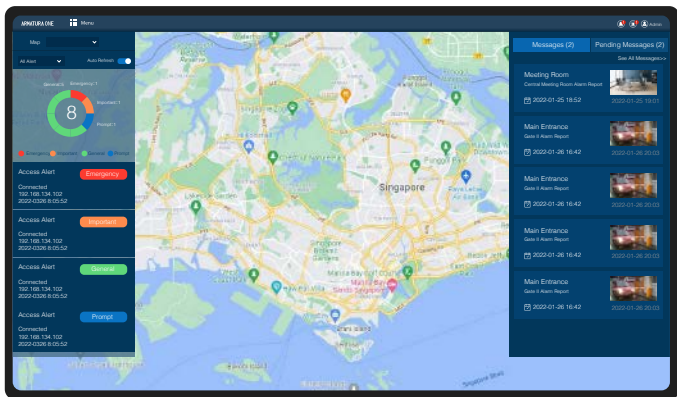


Professoinal Time & Attendance Module

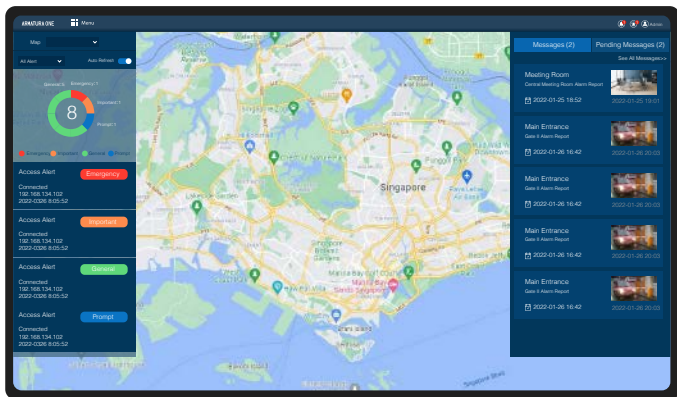
Armatura One's web-based time and attendance module allows administrators to manage the system from any location with internet access. It accommodates complex requirements such as flexible shifts, multi-level overtime, cross day shifts, and online leave applications with multi-level approval.



USA Office



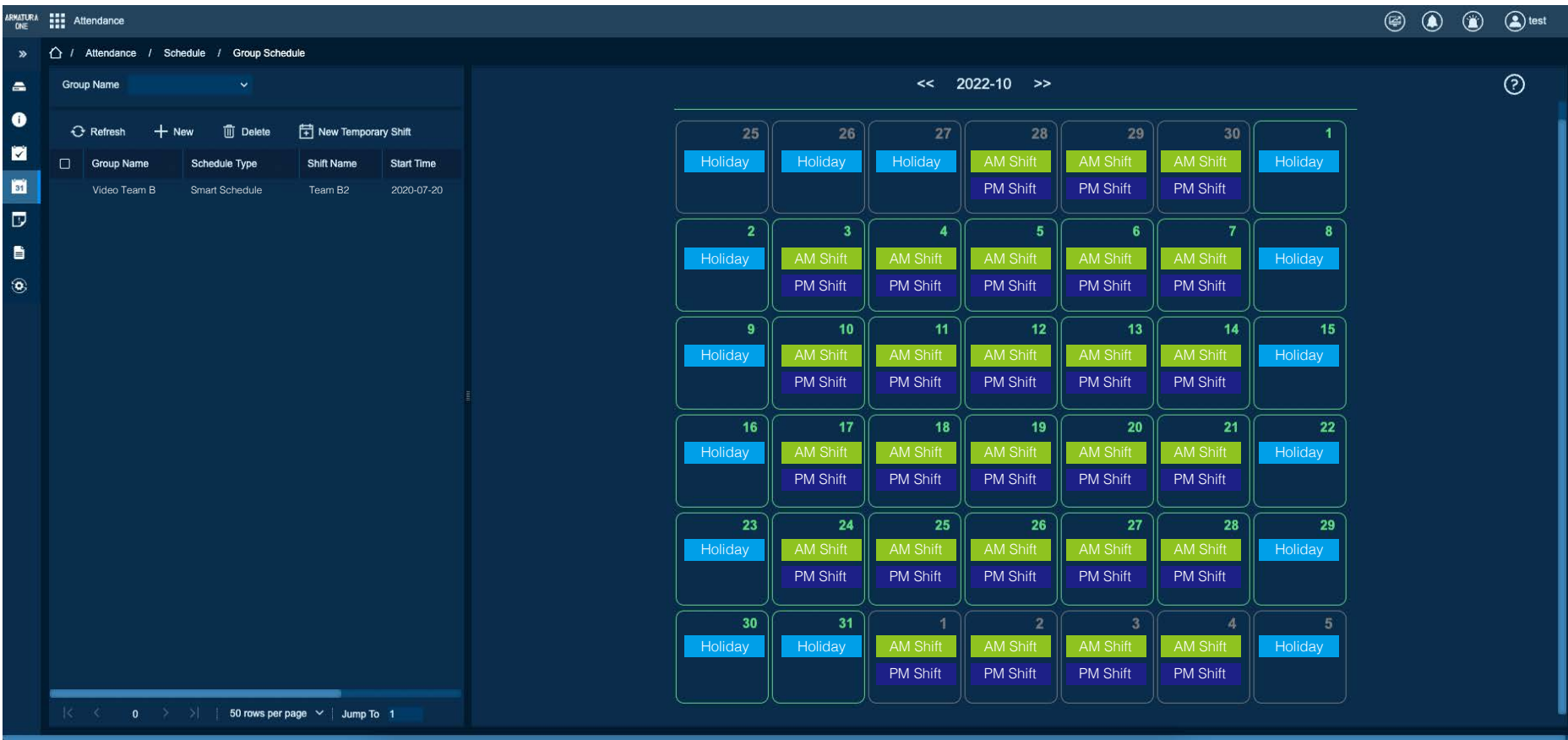
Australia Office



France Office

Flexible Group Scheduling

The Time & Attendance module supports flexible group scheduling, enabling users to create groups based on employees, the entire company, or individual departments with the same attendance rules. Attendance parameters, including check-in, check-out, and overtime rules, can be established.



Personnel Area Setting

The Personnel Area Setting function is divided into "Area" and "Person":

- Area:

Displays attendance information for all employees and staff within a specific division based on the area name.

- Person:

Displays attendance records based on employees' and staff members' IDs.

Multi-Level Approvals and Automatic Alerts

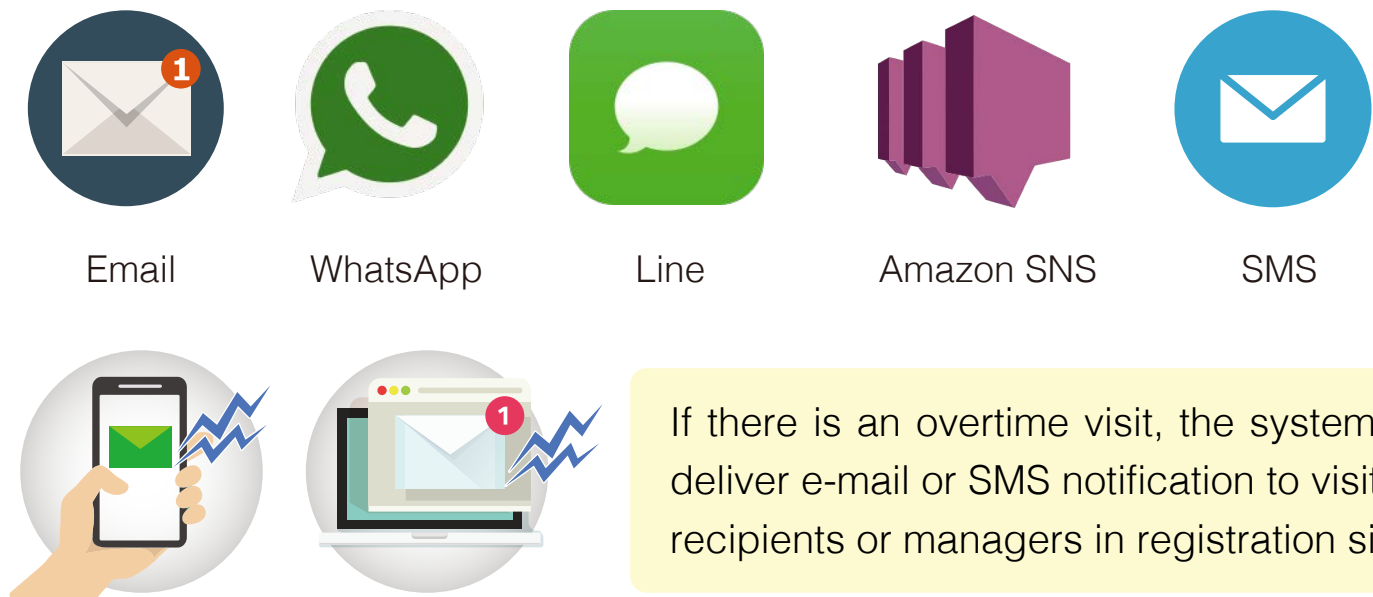
Administrators can design and configure their company's hierarchy, ensuring that approval processes align with the organization's structure. Example hierarchy levels include Boss > Manager > Assistant Manager > Officer.



Streamlined Approval Process:

Applications for leave, overtime, and other events are efficiently managed through the platform, enabling quick review and decision-making by the appropriate approvers.

Notifications can be sent out through various channels, such as WhatsApp, Line, SMS, Amazon SNS, and email, ensuring that approvers and employees stay informed about the status of their requests or actions.





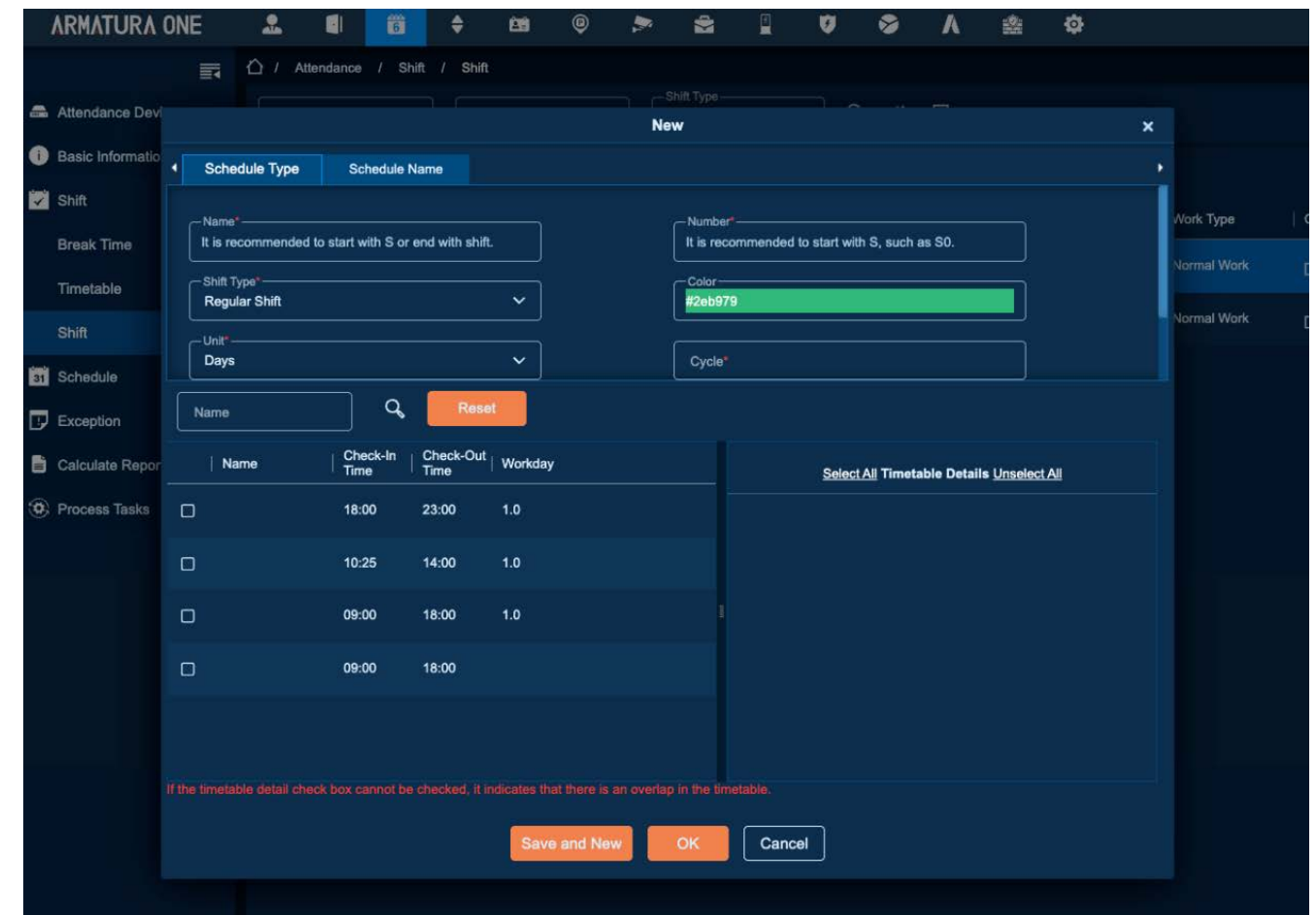
Employee Self Log-In

The Employee Self Log-In feature enables employees to access the server from any location at any time to perform job-related tasks. Employees can update personal information, apply for leave, submit exceptions (e.g., OT, manual punch-in, shift adjustment), and request self-report inquiries.



Flexible Shift Scheduling

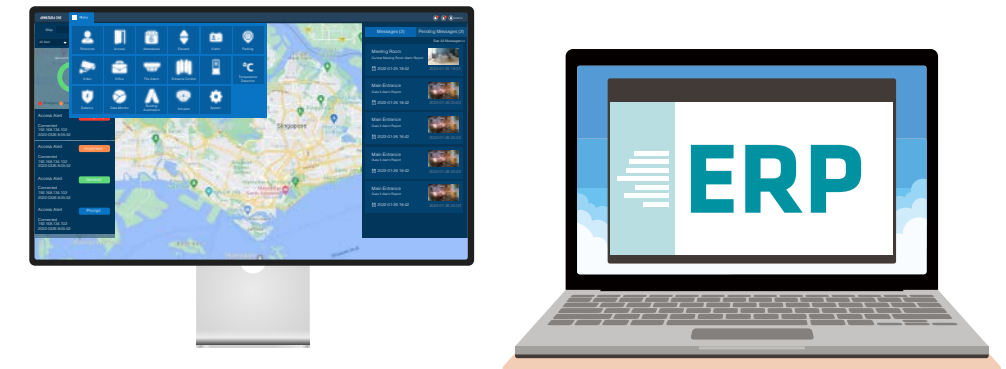
Industries with varying time and attendance shift requirements, such as retail, food and beverage, and patrol guards, benefit from Armatura One's flexible shift scheduling, which is essential for efficient operation management.



Integration with Third-Party HR Management Systems

Armatura One Security Platform is designed to be versatile and adaptable, allowing for seamless integration with a wide range of third-party ERP and HR systems. This integration capability extends the platform's functionality and ensures that organizations can efficiently manage their security and HR needs.

Armatura One offers various integration methods to suit different system requirements, including:



- **API:**

Armatura One provides a RESTful API to facilitate integration with third-party systems. This allows for easy communication and data exchange between Armatura One and other platforms, enabling seamless connectivity and streamlined processes.



- **Database Mapping:**

Armatura One supports integration with multiple databases, including PostgreSQL, MS SQL, and Oracle. This allows organizations to map their existing HR or ERP databases to the Armatura One platform, ensuring efficient data synchronization and management.



- **Automatic Report Generation:**

Armatura One enables the generation of custom reports with attributes such as staff name, department, area, staff ID, and more. These reports can be saved in designated locations using predefined names or custom naming logic. The platform supports CSV and Excel file formats, allowing organizations to choose the most suitable format for their needs.



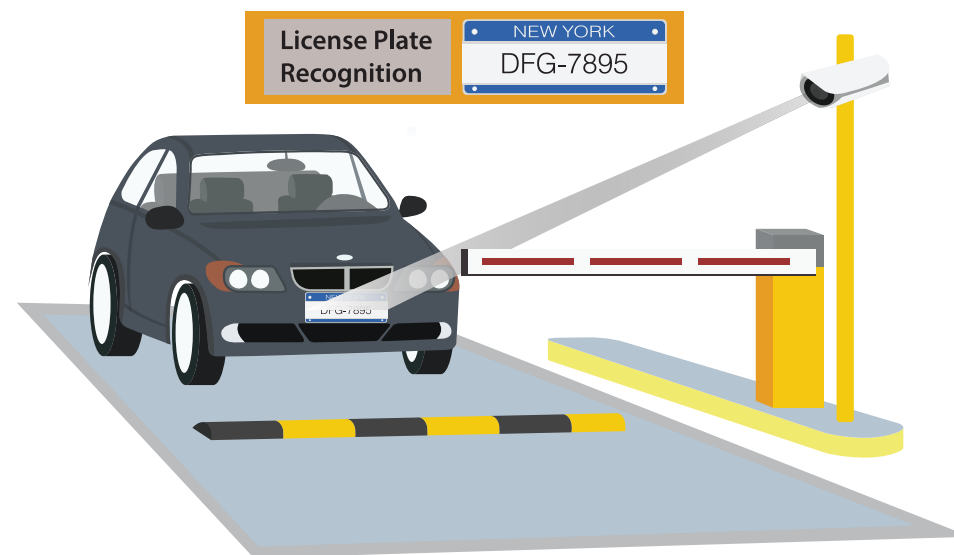
- **Active Directory Integration:**

Armatura One can integrate with Microsoft Active Directory, allowing organizations to leverage their existing user management infrastructure for authentication, authorization, and user data synchronization.

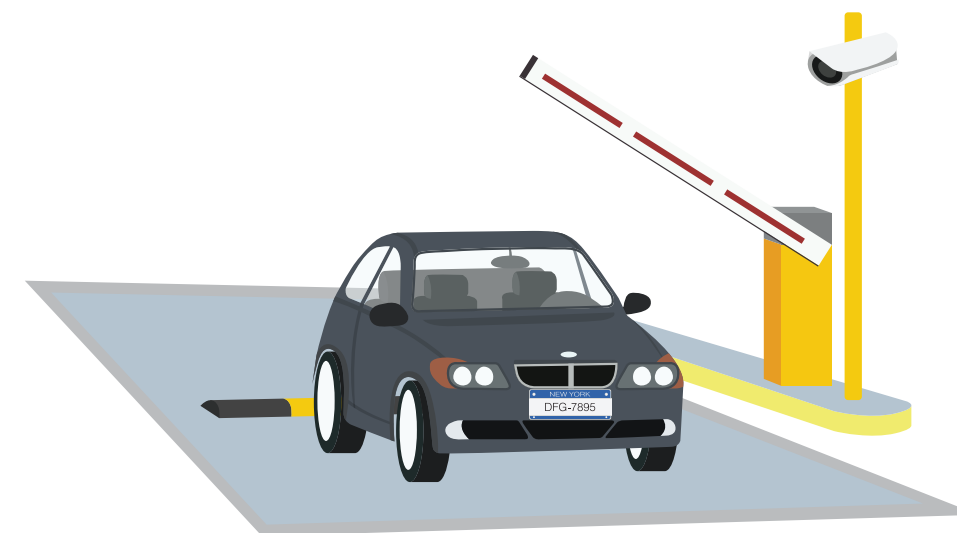
Access Control and LPR Attendance Tracking Integration

Armatura One can connect with access control terminals and panels linked to LPR (License Plate Reader) terminals, retrieving records for time and attendance calculations.

- LPR cameras scan license plate numbers as vehicles approach their reading range.
- Upon successful verification, the parking barrier is lifted, and attendance is recorded.



LPR Camera scan the number on the license plate when vehicle is approaching its reading range.



Parking barrier is lifted once the verification is confirmed. Attendance recorded.



Multi-Location Management

Users can access the centralized system remotely via their web browser to manage thousands of standalone terminals and controllers under a wide area network (WAN), enabling multi-location management.





Elevator Module

The Elevator Module in Armatura One A&E system provides a comprehensive and flexible solution for managing elevator access and control in various types of buildings. The module offers a wide range of features, including elevator access authentication control, elevator floor-level control, access control point identification, global linkage, building management support, and elevator operation limitation by timeslots.

Elevator Access Authentication Control

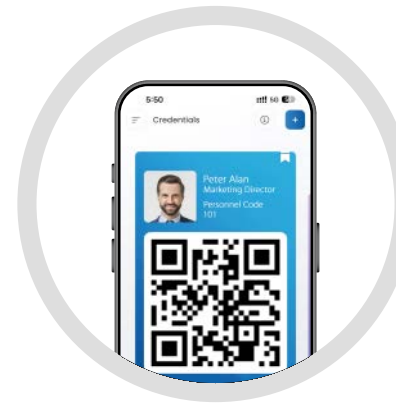
The Elevator Module manages personnel access rights using mobile credentials, RFID cards, and biometric technologies. It controls access to specific floors and supervises elevator events, allowing registered users' access rights to floors. The module integrates with access control modules for one-stop management and limits access to authorized users within specified time periods.



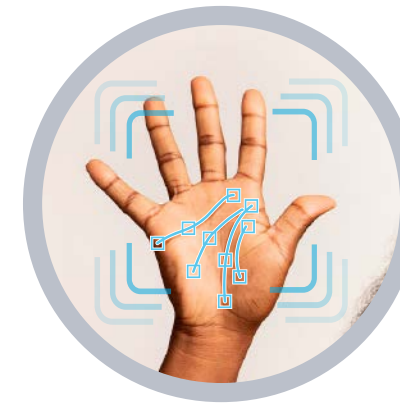
RFID



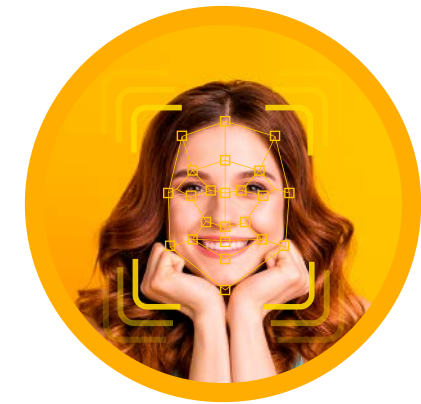
Mobile credential



Palm recognition



Facial recognition



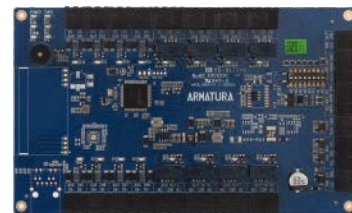


Elevator Floor-Level Control

Armatura One Security Platform's Elevator Module provides advanced floor-level control solutions to ensure secure and efficient elevator access. The platform offers two solutions for elevator floor-level control:



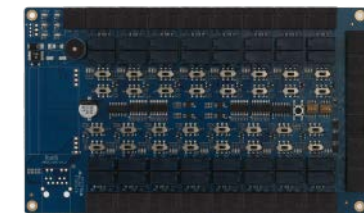
AHSC-1000
IP-Based Core Controller



AHEB-0808
IO Expansion Board



AHEB-1602
IO Expansion Board



AHEB-1616
IO Expansion Board

This solution utilizes the AHSC-1000 core controller and AHEB-1616 IO expansion board to provide a secure, scalable, versatile, and affordable access control solution for elevators. Key features of this solution include:

Elevator Control Mode

The AHEB series of expansion boards enhances building control systems with configurable relay ports that can be adapted as inputs or outputs to meet diverse operational needs. While all boards in the series ensure seamless and secure integration via OSDP over RS-485, the AHEB-1616 model distinctively supports advanced elevator control functions. This includes automatic floor selection and Floor Selection History Logging, capabilities exclusive to the AHEB-1616, making it ideal for complex, multi-story elevator management in larger buildings.

Floor-Level Control
& Floor Selection History Logging

Admin Dept.
3/F

Allow
Elevator Floor
Button Press

Floor Name	Event Description
B1	Button Pressed by Granted 2
B1,1,2,3,4,5,6,7,...	Access Granted 1

Automated Floor Access

Sales Dept.
18/F

Keyless Bypass
of Specific
Floor Buttons

DCS Integration (Supports KONE, Mitsubishi, Otis, Hitachi, Schindler Elevators)

This solution fully integrates with third-party elevator destination control systems (DCS) from leading manufacturers such as KONE, Mitsubishi, Otis, Hitachi, and Schindler.

Destination Control System (DCS) Integration

HITACHI
Inspire the Next

KONE

mitsubishi

Schindler



Present a card or a QR Code or verify the identify by facial recognition at the entrance control point. The screen will display the assigned elevator number and the destination floor.



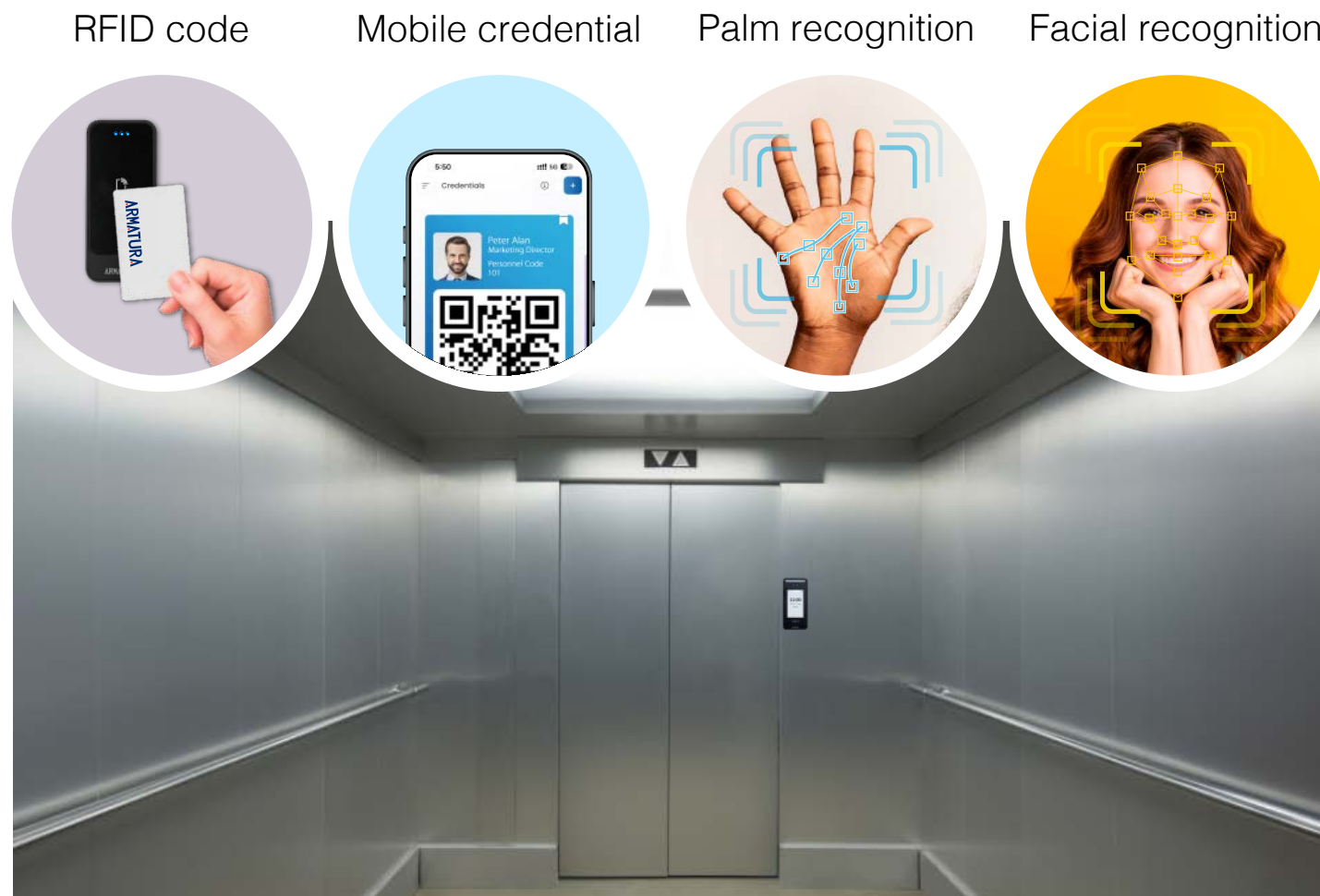
Enter the assigned elevator



The elevator will go to the destination floor

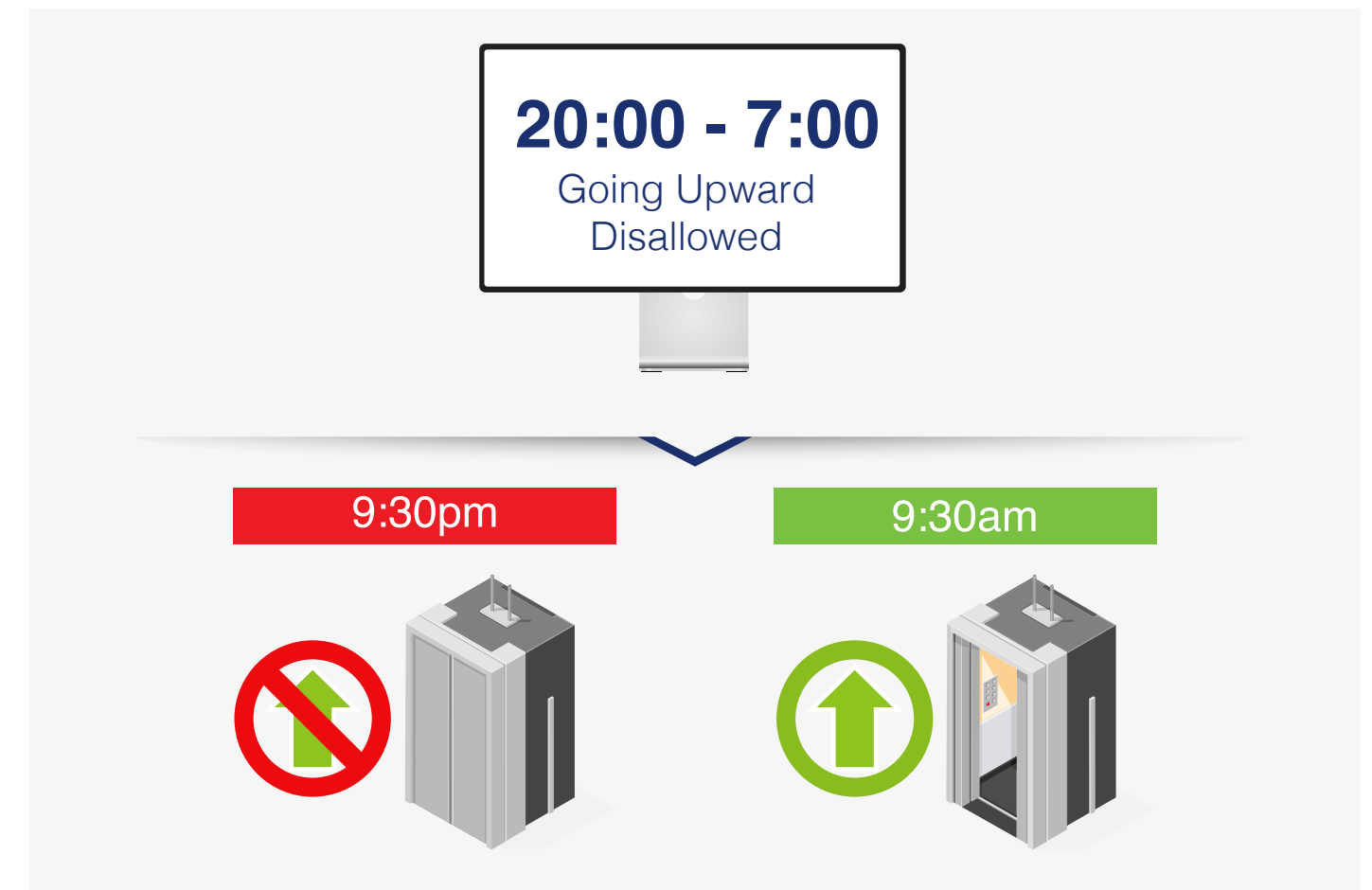
Access Control Point Identification

The Elevator Module allows presenting a card, mobile credential, Dynamic QR code, palm recognition or facial recognition for identity verification. It displays the assigned elevator number and destination floor on screen.



Elevator Operation Limitation by Timeslots

The module integrates with Armatura products to limit elevator operation during specific times. For example, unauthorized users can only go downward with floor access cards if elevator control is set to stop upward operation between 9:00 p.m. and 7:00 a.m.



Global Linkage for Elevator Control

The Global Linkage for Elevator Control module in Armatura One Security Platform is designed to enhance security within multi-level buildings by integrating access control systems with elevator Destination Control Systems (DCS). This feature ensures that access permissions are coordinated with elevator functions, restricting access to specific floors based on individual user permissions and providing a more secure building environment.

- **Triggering Events or Alarms:**

The module can trigger events or alarms based on various conditions, such as unregistered personnel, illegal time zone access, or duress verification, providing real-time alerts and ensuring prompt response to security issues.



- **Photo Capture and Video Recording:**

The system features photo capture and video recording capabilities, allowing for visual evidence and documentation of any access control events or security breaches.



- **Seamless Integration:**

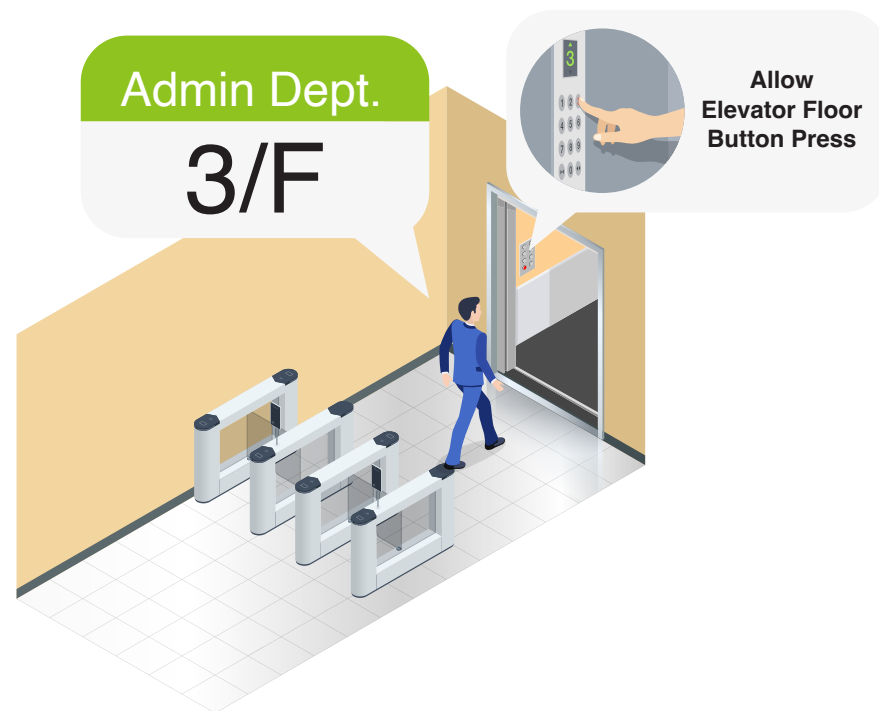
Elevator Linkage allows for seamless integration between access control systems and elevator DCS, ensuring a smooth flow of information and coordination of access permissions with elevator functions.

Facial recognition



- **Customized Access Permissions:**

The platform supports the creation of customized access permissions for users, restricting users from pressing specific floor buttons and accessing certain floors based on their roles, departments, or clearance levels.



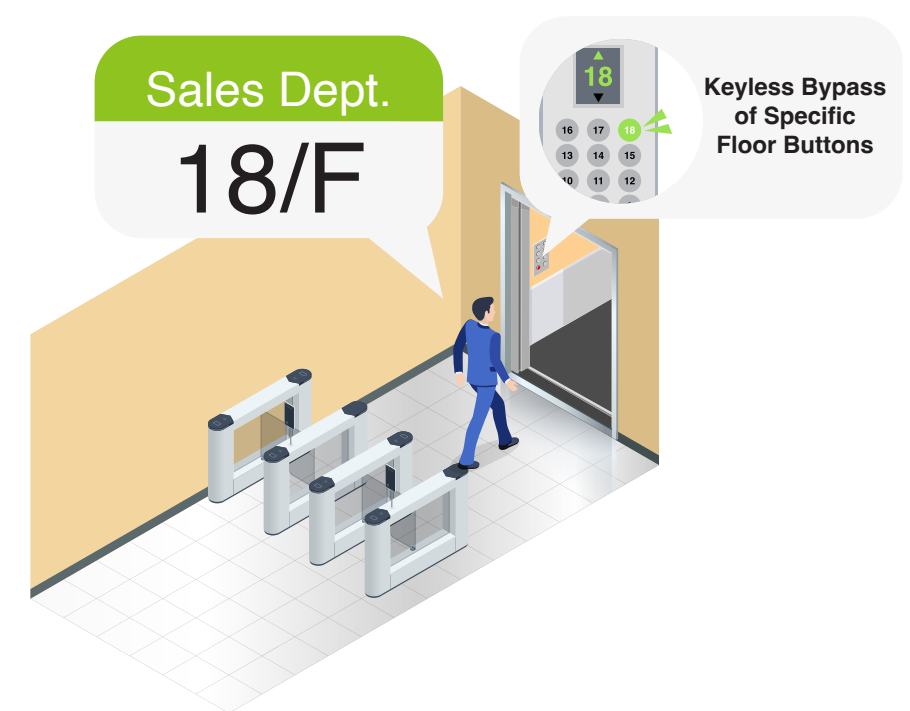
- **Photo Capture and Video Recording:**

The system features photo capture and video recording capabilities, allowing for visual evidence and documentation of any access control events or security breaches.



- **Automated Floor Access**

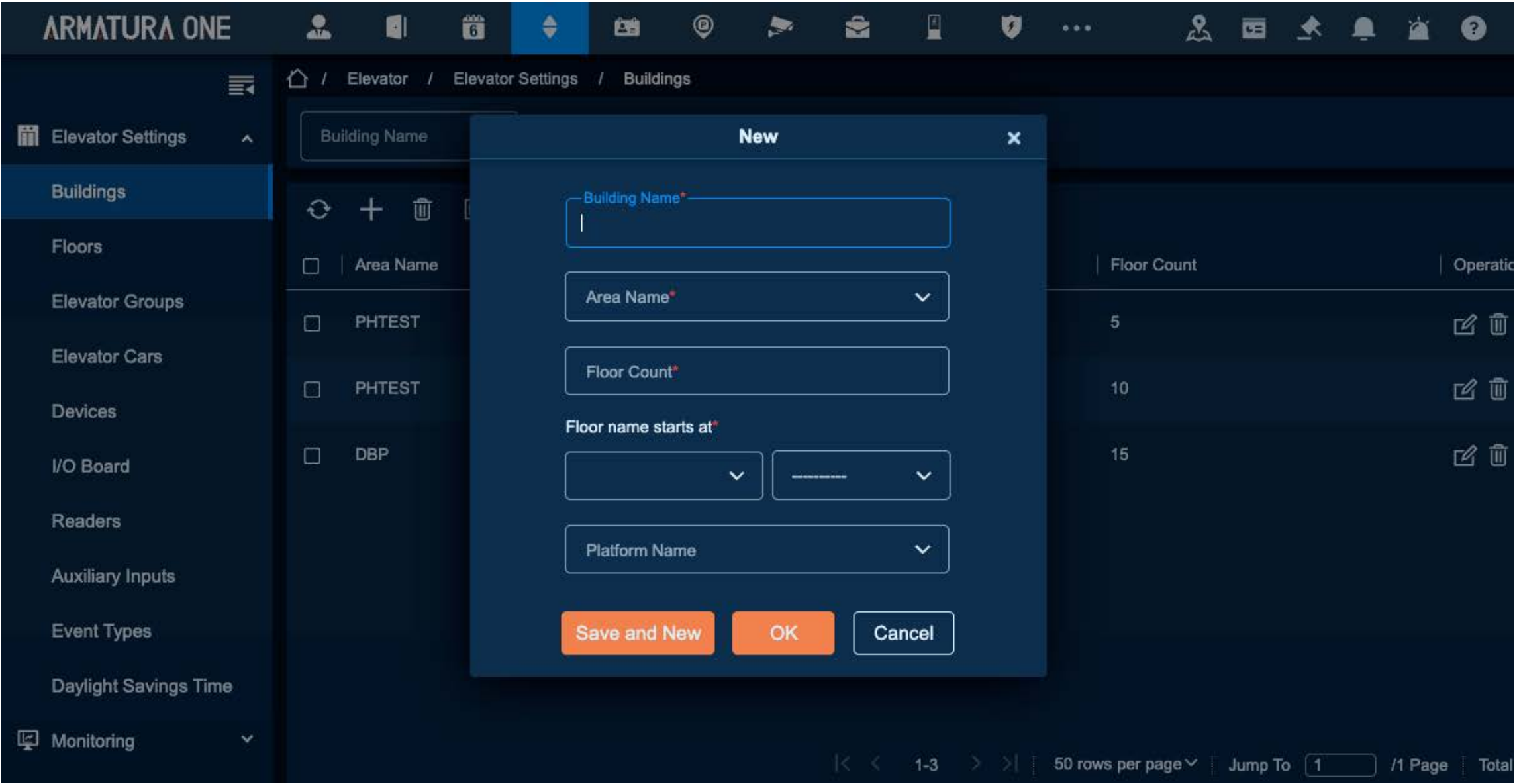
The platform supports the automatic key pressing to specific floors, allowing users to bypass the need for pressing specific floor buttons and accessing certain floors based on their roles, departments, or clearance levels.





Building Management Support

The Elevator Module customizes levels and starting level configurations, automatically adding floors based on building settings and corresponding floor information.





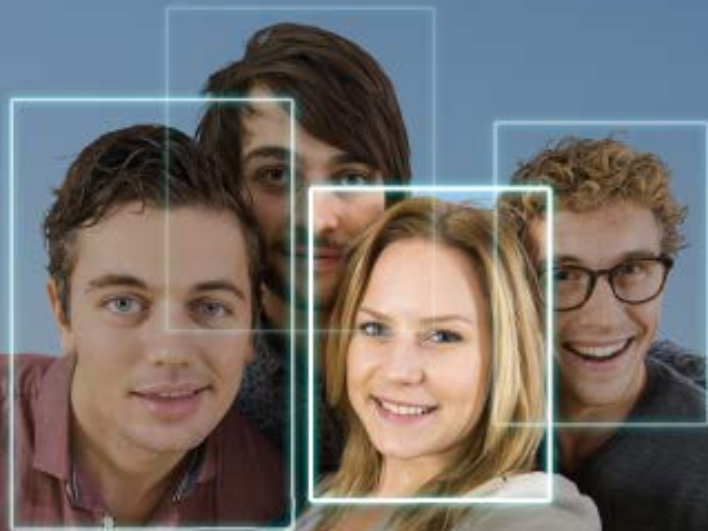
Visitor Module

The Visitor Module in the Armatura One system is a flexible and comprehensive solution for managing visitors within various facilities. It offers a wide range of features, including multiple credential options, dynamic QR code safe entry solutions, maximum visitor checks, integrated devices for visitor registration, visitor grouping, duplication of authorization information, the ability to add watch lists, visitor data privacy protection, and a responsive web design for visitor use.

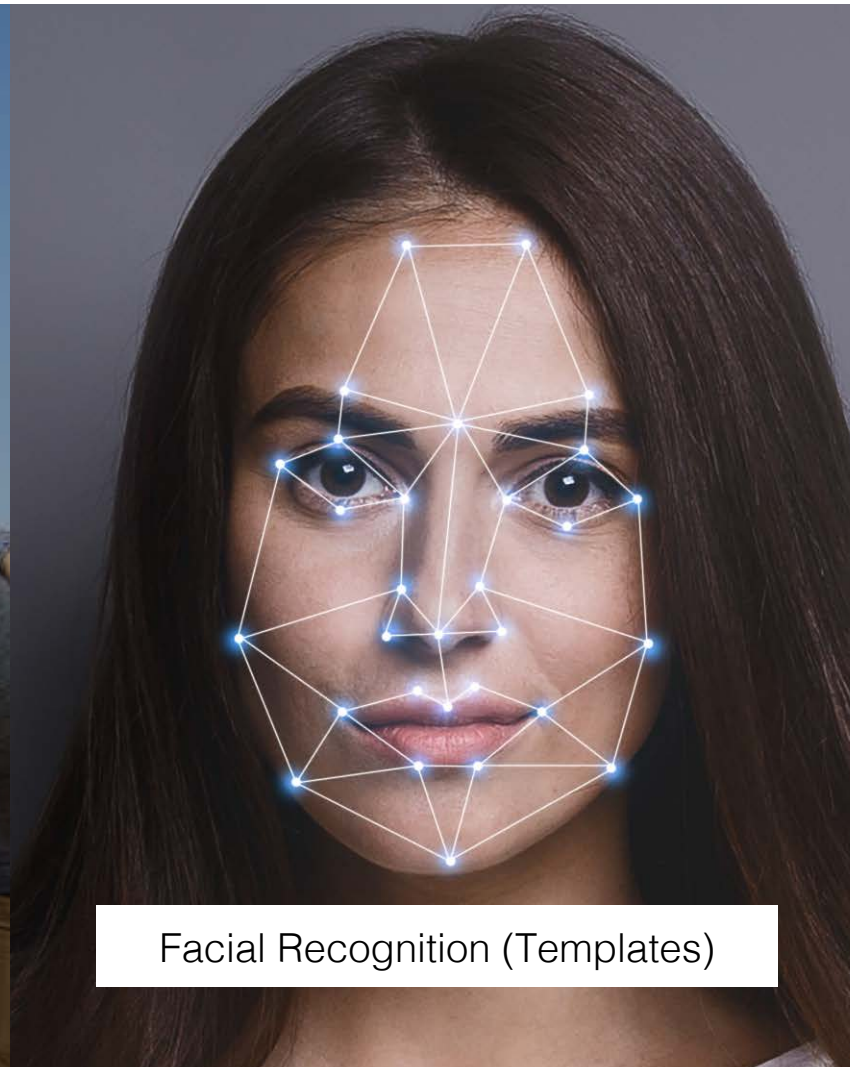
Visitor Module Credential Options

The Visitor Module supports the following credential options:

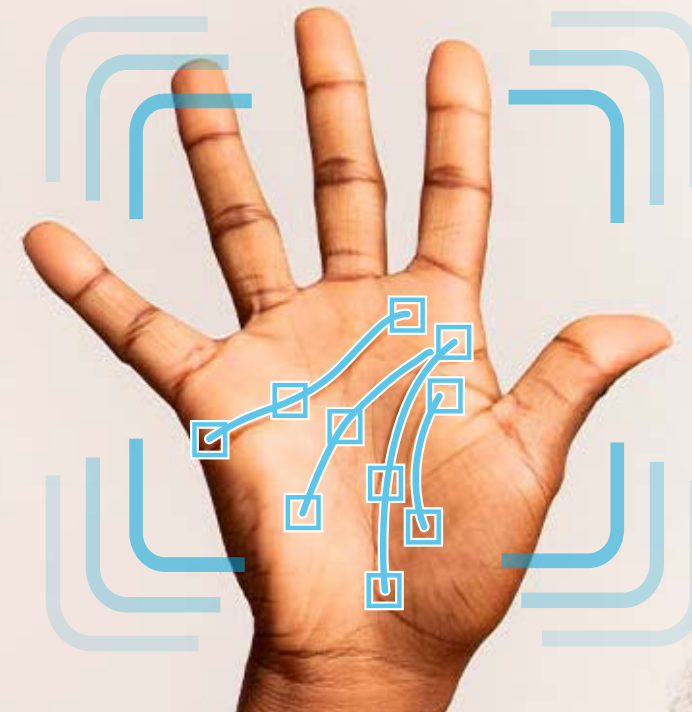
- Photo capture function for facial templates registration
- Sharing templates with all Facial Recognition Terminals
- Multiple credential options: RFID cards, mobile credentials, palm, fingerprint
- Online registration for mobile credentials, including dynamic QR codes as credentials



Facial Recognition (Photo)



Facial Recognition (Templates)



Palm Recongition



Mobile Credentials

Dynamic QR Code Safe Entry Solution for Staff and Visitors

The Armatura One Security Platform's Visitor Module offers a touchless check-in process through the use of dynamic QR codes, providing a seamless and safe entry experience for both staff and visitors. This innovative solution eliminates the need for physical contact, reducing the risk of spreading illnesses and enhancing overall safety. Visitors can use the dynamic QR code in two different ways:

1. Armatura ID Mobile App QR Code Mode

By utilizing the Armatura ID mobile app, visitors can access their unique QR code, which can be scanned at the entry point to verify their identity and grant access. This method provides a convenient and secure way for visitors to check in using their smartphones.

2. Responsive Design

Armatura One supports responsive design for the visitor module, ensuring that visitors can have an optimal viewing and interaction experience across various devices and screen sizes, including desktop computers, laptops, tablets, and mobile devices. This involves adapting the layout, content, and functionality of a website or application to provide the best user experience on different devices



ARMATURA ID

Dynamic QR Code Safe Entry Solution for Staff and Visitors

The module implements dynamic QR codes to prevent unauthorized access. It allows users to adjust the QR code image refresh rate (default: 1 seconds) for added security.



Maximum Visitor Check

The Visitor Module monitors visitor count and sets an upper limit for secure visitor management. Administrators are notified when the limit is reached, ensuring proper control of visitor flow.



Maximum visitor check

- ☒ Open single-day maximum visitor visits monitoring
Maximum number of visits
- ☒ Open single-day single-person maximum visitor visits monitoring
Maximum number of visits

Integrated Devices to Improve Visitor Registration Speed

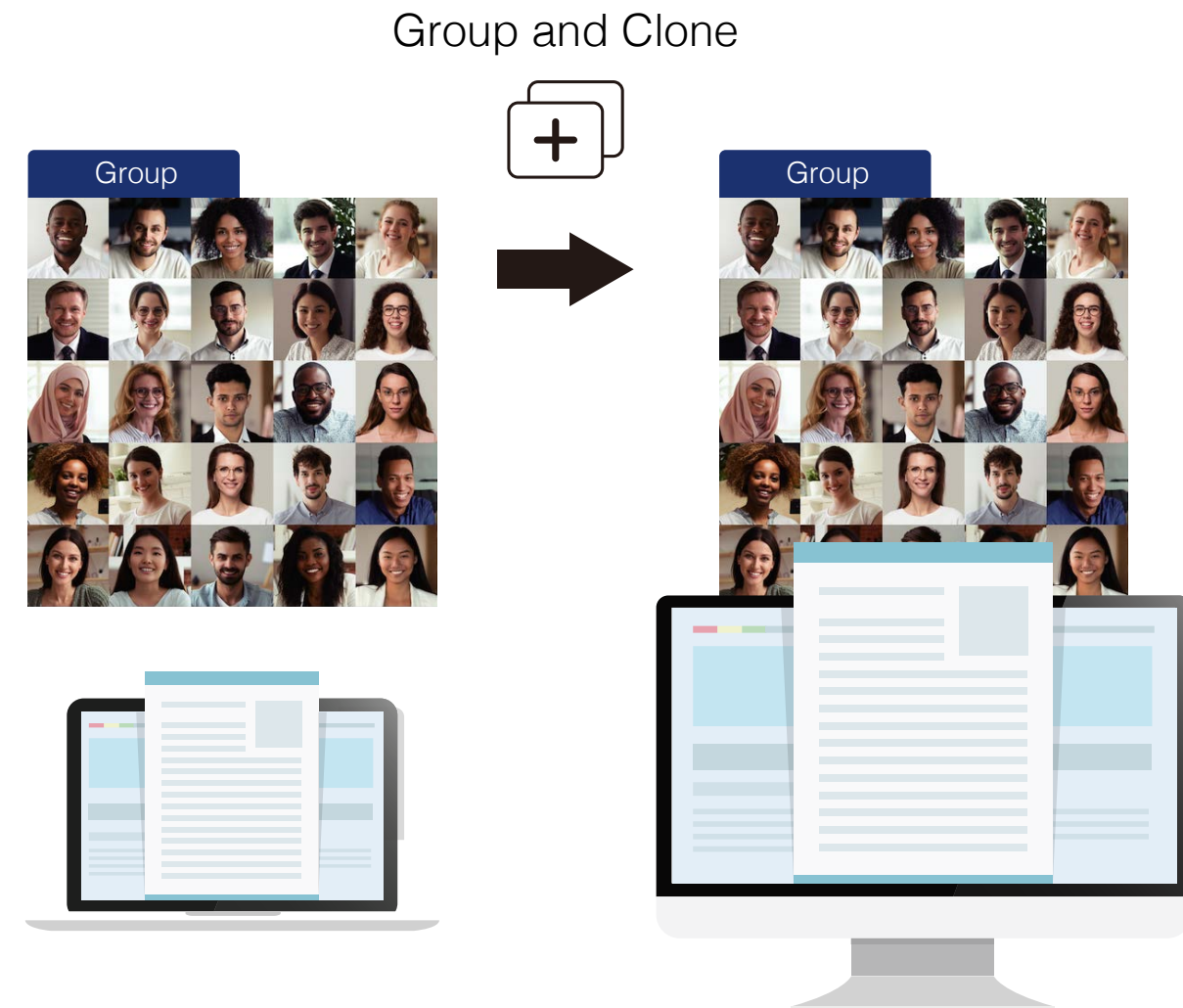
The module incorporates various devices to enhance visitor registration efficiency:

- OCR devices recognize passports and identity documents from over 190 countries
- ID readers support partial countries' identity documents
- Printers produce customizable visitor tags
- USB cameras and fingerprint readers register visitors' fingerprints and faces



Visitor Grouping and Authorization Information Duplication

The Visitor Module supports batch pre-registration, attendance, and sign-out of visitors through document import. It also allows duplication of visitor authorization groups, time, and persons visited for re-visit registration efficiency.



Adding Watch List

The module enables marking special visitors (e.g. VIP, block list users) and automatically prompts visitor information and visit history during registration.



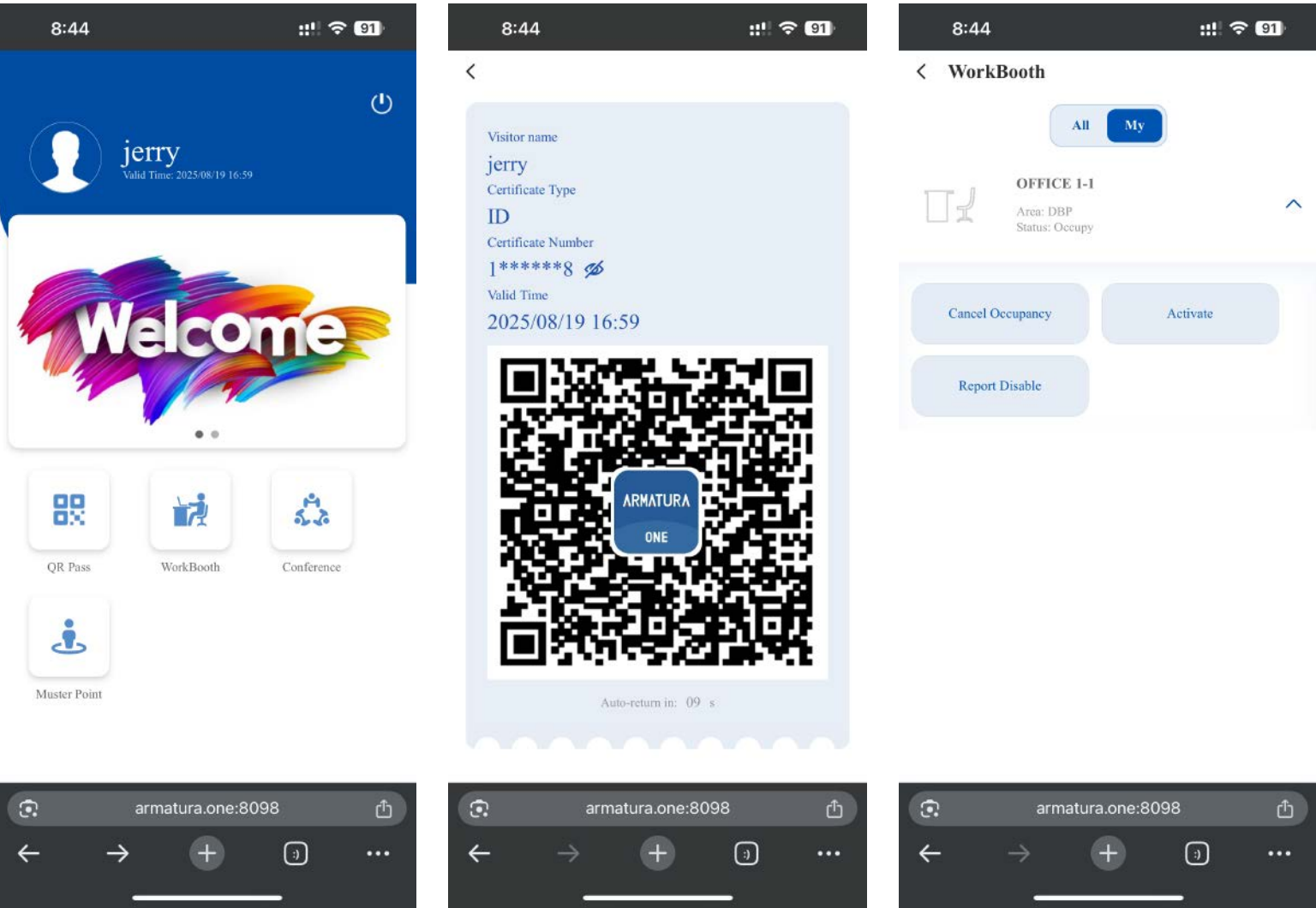
Visitor Data Privacy Protection

The Visitor Module allows customization of visitor privacy agreements and notifications during registration, ensuring compliance with data privacy regulations, such as GDPR Compliance.



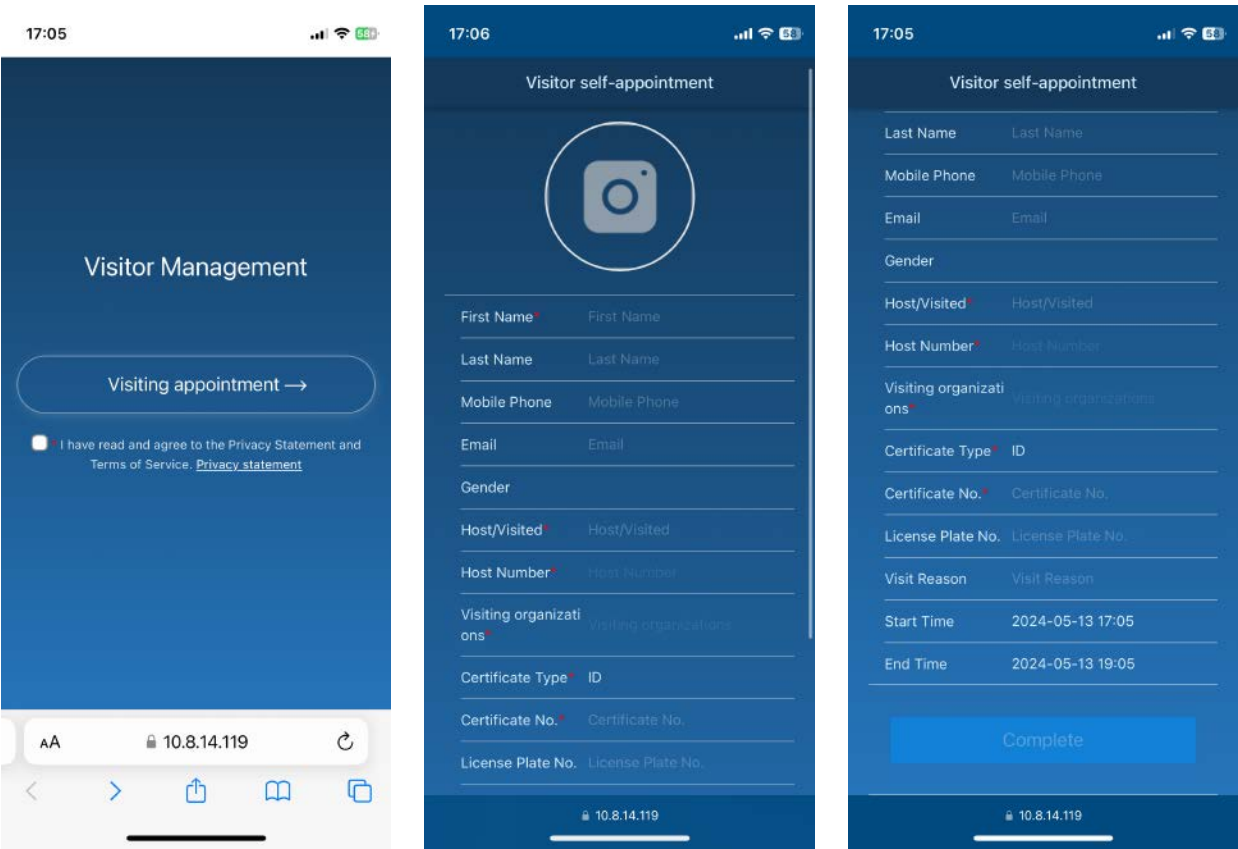
HTML5 Web Application for Visitor Use

The module provides a dedicated mobile HTML5 page for shared workspace and conference room viewing and reservation applications, making it easy for visitors to access relevant information and services.



Visitor Self-Registration Page

For invited visitors, they can click the hyperlink sent via email or SMS to proceed with self-registration. After registration, visitors' access rights will be delivered to their devices. Users can then access authorized areas, such as access control devices, elevator controls, and meeting rooms, upon successful verification.



Online Registration

Administrators can provide an HTML5 link for visitors to register online. The system is capable of automatically sending the registration link to designated users via email, WhatsApp, Line, SMS, or Amazon SNS. Users can then fill in the required information and upload personal photos for facial recognition registration or opt for using a dynamic QR Code. Upon completion of registration, the administrator will receive a notification within the system and can initiate the approval process. Once the registration is approved, the user will receive a confirmation via email, WhatsApp, Line, SMS, or Amazon SNS. If the user has chosen to use a dynamic QR code, then the confirmation will include a link for dynamic QR code usage.



Email



WhatsApp



Line



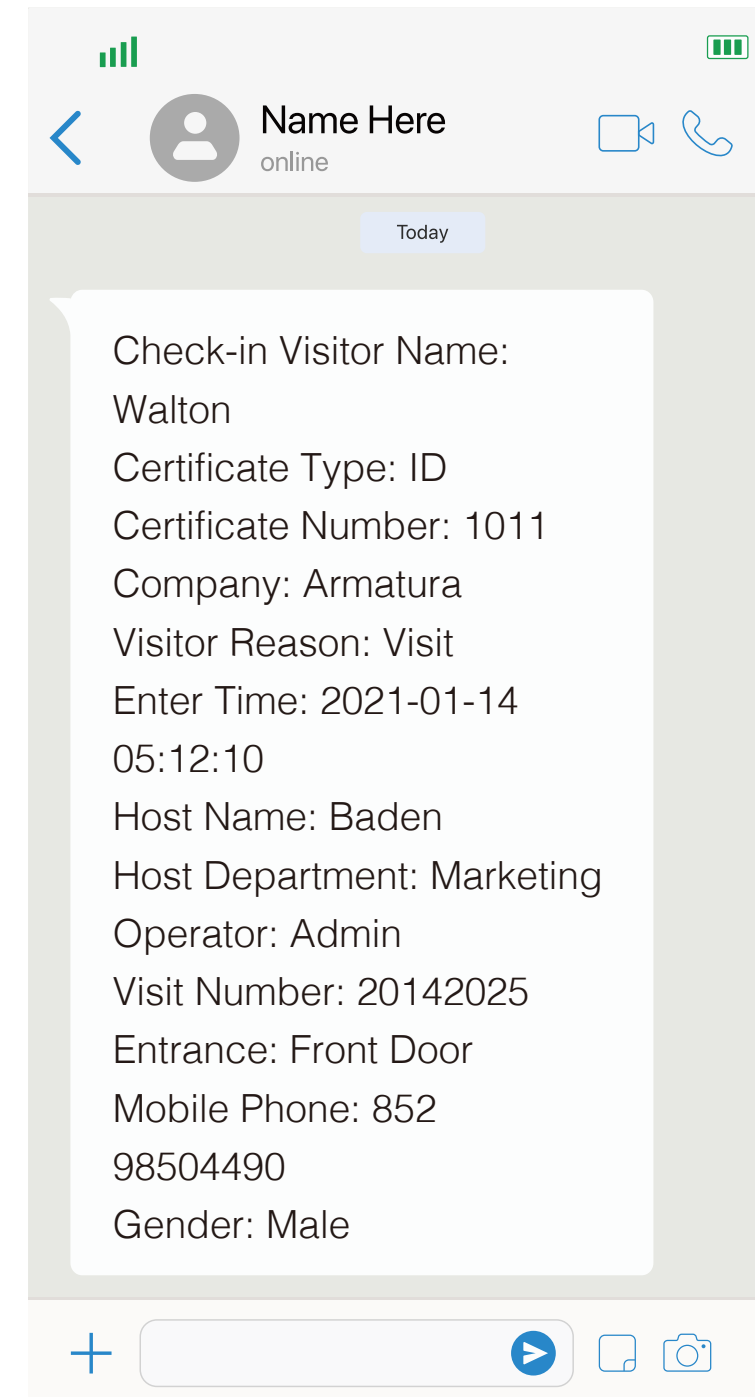
Amazon SNS



SMS



If there is an overtime visit, the system will deliver e-mail or SMS notification to visitors, recipients or managers in registration sites.



Self-registration

Armatura One incorporates a convenient self-registration feature, utilizing facial recognition smart kiosk. This functionality allows visitors to complete on-site self-reservation, check-in, and check-out processes directly on the kiosk, streamlining and simplifying the visitor management experience. By leveraging facial recognition, the system ensures a seamless and secure check-in process, enhancing overall security and reducing the need for manual intervention.

In addition to facial recognition, the Android Smart Kiosk also has the capability to print out QR tickets for visitor access. These QR tickets can be scanned at designated access points, allowing visitors a quick and efficient entry process while maintaining a secure and controlled environment. This feature further enhances the user experience by providing a convenient and contactless method for granting temporary access to facilities.





Parking Management Module

Automatic and intelligent vehicle management effectively and accurately monitors and manages vehicles at all exits and entrances.



Enhancing Car Park Efficiency and Security with Armatura One's License Plate Recognition Technology

The Armatura One Parking Management Module includes a Car ID LPR camera with embedded License Plate Recognition software. This camera can identify license plates from over 80 countries, ensuring secure and efficient car park operations.



One Vehicle can bond with multiple person

The Parking module allows one vehicle to be registered with multiple individuals, facilitating efficient management and accurate tracking of vehicle ownership and usage. This feature is especially beneficial when a vehicle is shared among a group, such as coworkers in the same department. By enabling the association of multiple people with a single registered car, the Parking module streamlines administration and ensures precise monitoring of vehicle-related activities.



Two-Factor Authentication of Face/ Palm/ RFID with Number Plate Registration

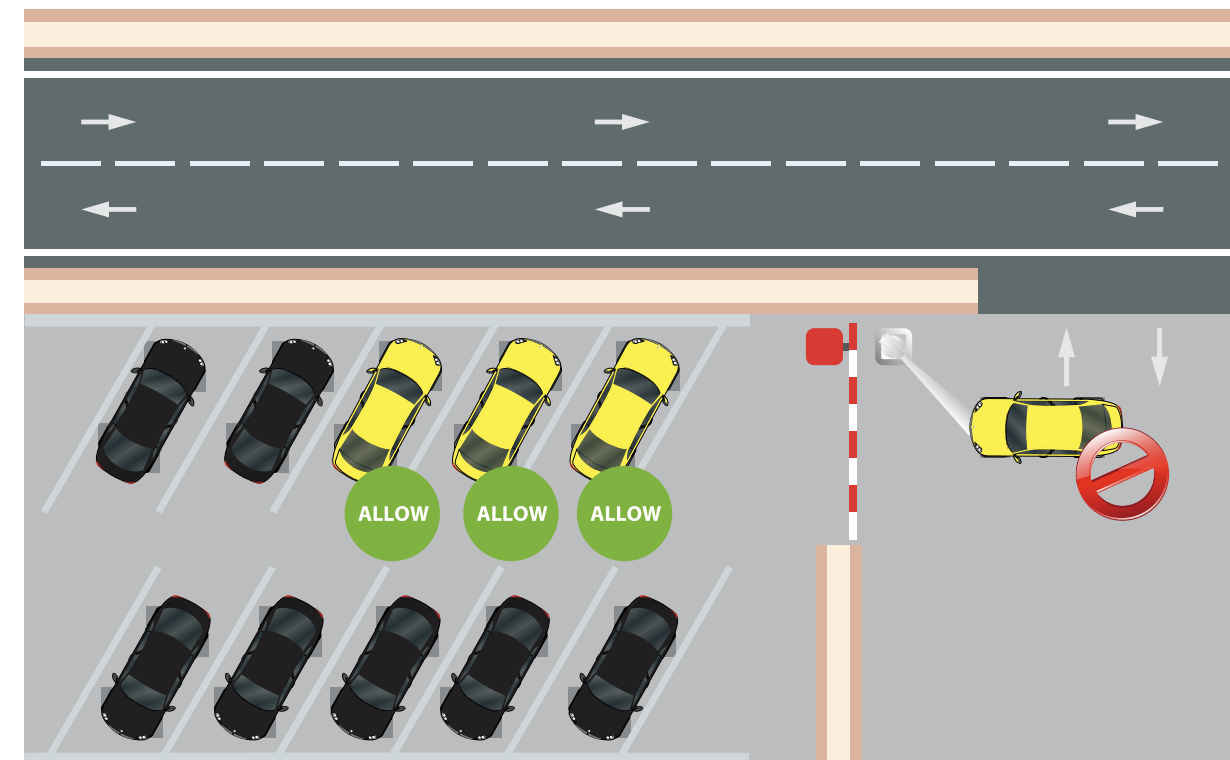
Two-factor authentication utilizing facial and license plate recognition enhances security. The LPR camera scans and verifies license plates as vehicles enter. The system matches the driver's registered face image in the database. If both the license plate and facial recognition are successful, the car park barrier lifts for access; otherwise, it remains closed.

Additionally, users can also employ palm and RFID authentication with the LPR camera. If the palm and RFID credentials match the database, along with the license plate number, the car park barrier also opens for vehicle access.



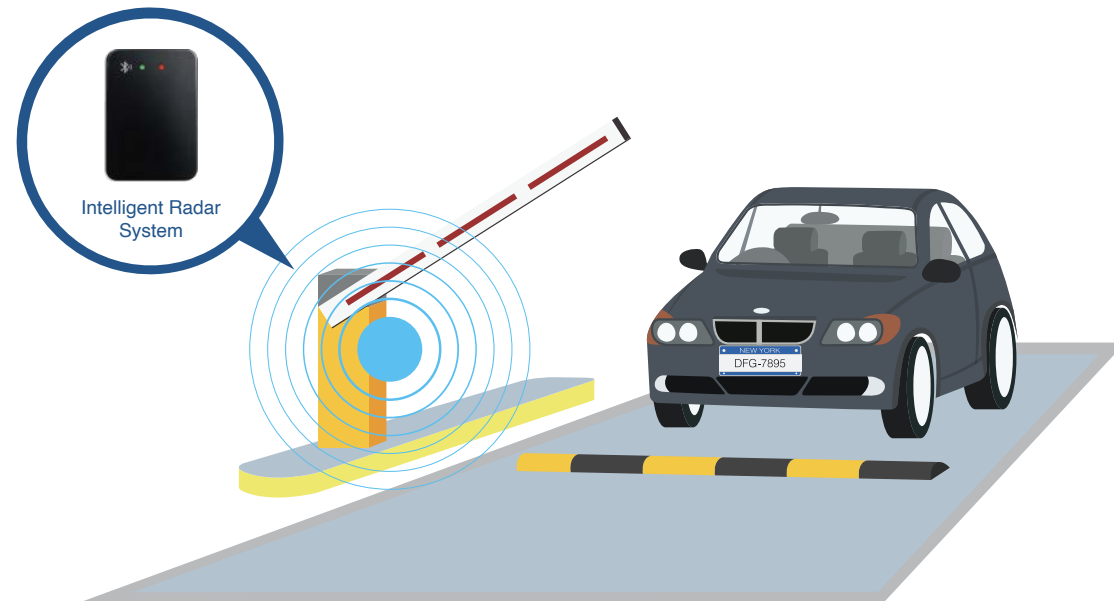
Multi-Car Parking Management: Efficient Allocation and Limitations

It allows multiple cars to be associated with multiple car park lots. For example, if a company has 10 cars but only three parking lots available, the fourth car or any additional cars beyond the limit of 3 will be denied entry to the car park.



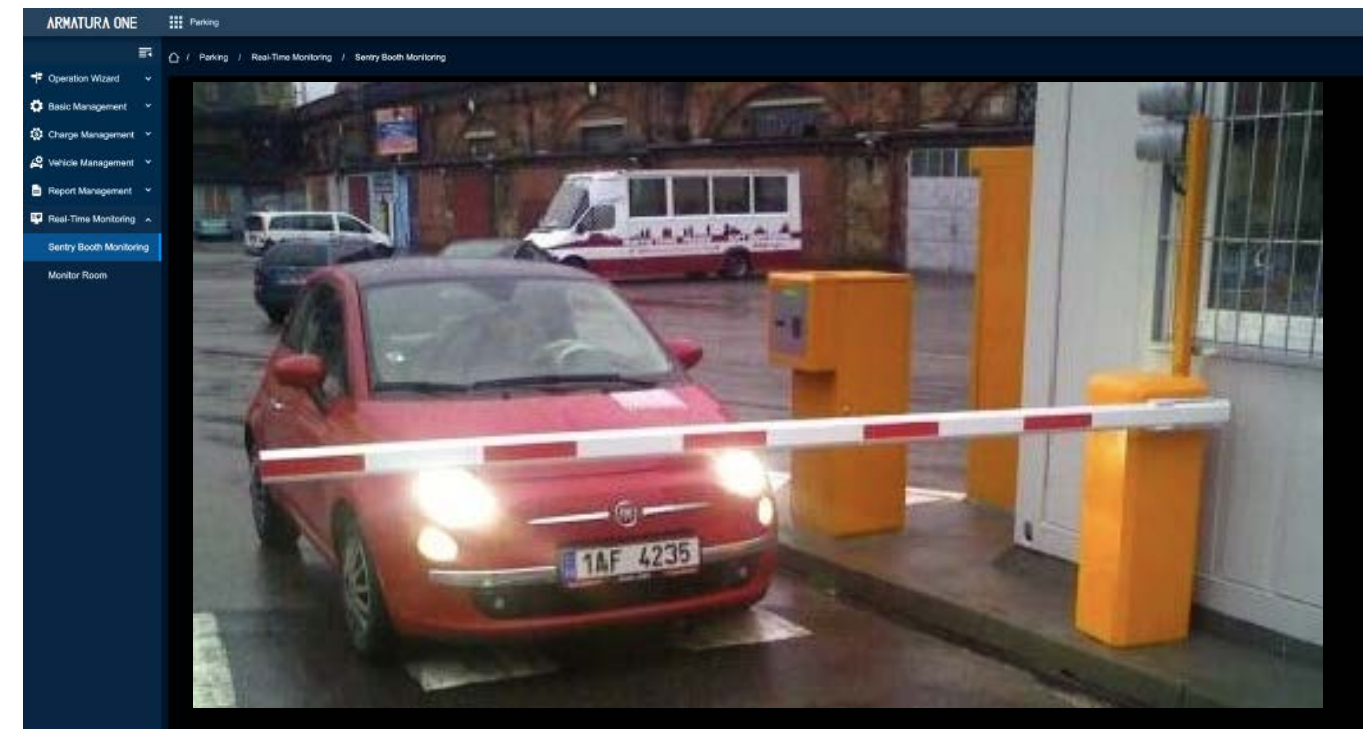
Support Intelligent Radar for car park gate

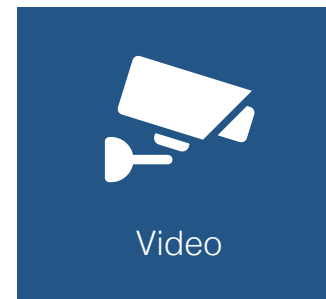
Armatura One supports an intelligent radar system for car park gates. It can precisely control the rising and falling of the barrier arm and detect targets, such as vehicles, pedestrians, and other objects, effectively and sensitively within the arm's range.



LPR / Gate & Camera Linkage

The Parking Management Module supports video and camera linkage through Armatura One. By utilizing Vehicle Recognition technology, it automatically and rapidly identifies vehicle license numbers. Furthermore, prior to the vehicle reaching the gate, it possesses the capability to connect with multiple camera channels for capturing photos and recording videos.





Video Module

The Video Module in Armatura One is a robust solution for video surveillance and management in different facilities. It includes various features such as Video Management System (VMS) integration, high-capacity camera support using compression, PTZ operation support, ONVIF compatibility, and video patrol. Additionally, Armatura One enables video linkage with access control, elevator, intrusion, and visitor modules. Notifications are triggered when abnormal activity events are detected. Moreover, Armatura One seamlessly integrates with License Plate Recognition (LPR) systems, enabling gates to open automatically when the license plate number is matched.

Flexible Integration with VMS Platforms Supporting ONVIF and RTSP Protocols

Armatura One integrates with leading VMS platforms such as Linkingvision, Hanwha Wisenet, Milestone, and Digifort, which support ONVIF and RTSP protocols.

These platforms enable compatibility with a wide range of third-party cameras and NVRs.

This architecture ensures that Armatura One can be seamlessly incorporated into existing video surveillance infrastructures by leveraging the proven integration capabilities of these VMS platforms.



This approach allows Armatura One to work seamlessly with brands like Bosch, Axis, Hanwha, and Pelco through the VMS layer, without directly connecting to the devices.



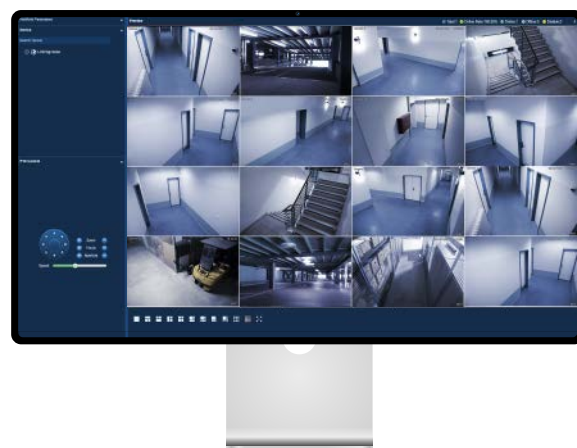


Supports up to 1,024+ Cameras with H.265+ High compression format

Armatura One supports up to 1024+ cameras and allows for 16 simultaneous camera playback. It utilizes H.265/H.264 high-profile compression formats, enabling high-quality video playback at lower bit rates.

Supports 16 Real-time Video Channel in Single Monitor

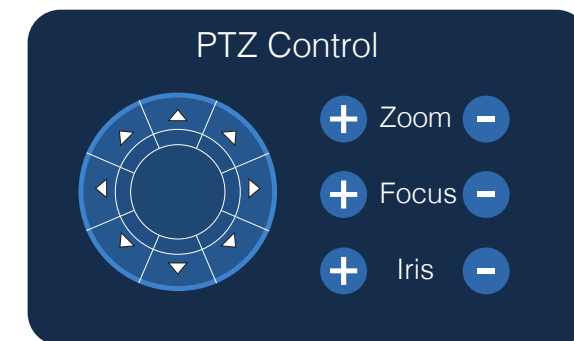
Armatura One's Video Module empowers organizations, users, and individuals with the ability to seamlessly monitor up to 16 video surveillance feeds simultaneously, spread across 16 diverse locations all in real-time. This comprehensive solution ensures that users can effortlessly keep a watchful eye on their premises, no matter where they are located.



Supports
1024+

PTZ Operation Support

The software enables pan-tilt-zoom (PTZ) control of IP cameras, allowing remote directional and zoom control, as well as fine adjustment of the camera's center position. Zoom control, iris level adjustment, and PTZ movement speed adjustment enhance both security and convenience.



Video Management System Integration

The VMS of the Video Module is fully integrated with Armatura One and compatible with third-party video surveillance systems such as Digifort, Hanwaht and Artec. It offers support for intelligent video functions, including object detection, area detection, and line crossing alerts, which can be seamlessly applied to access control systems.



Video Linkage & Photo Capture Linkage with Access Control, Elevator Control, Intrusion, Visitor Module

Armatura One is a system that automatically delivers an email to notify administrators when particular events occur in access control, elevator control, intrusion and visitor module. It enables users to monitor the entire system in real-time by showing the detailed status, including any abnormal situation at a door, with support for video linkage and photo capture pop-up when an abnormal security event occurs

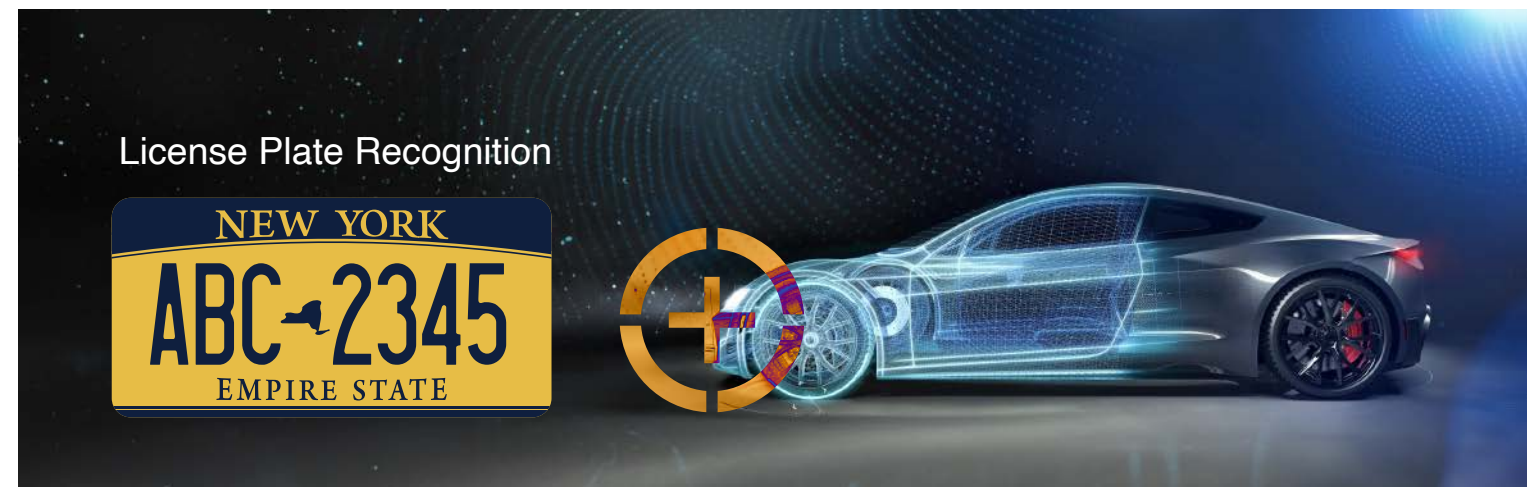




Support 3rd Party LPR systems and open for integration

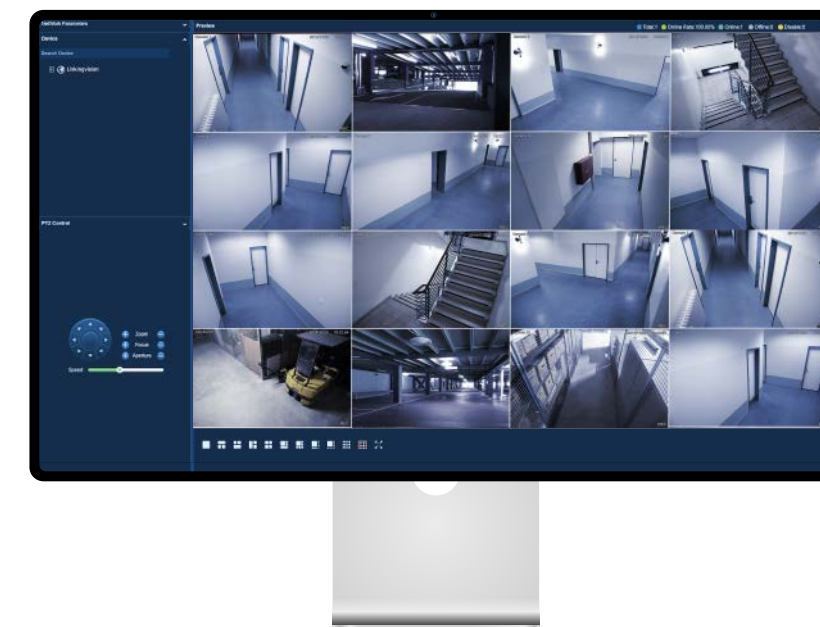
Armatura One provides robust support for third-party License Plate Recognition (LPR) systems, facilitating seamless car authentication. By integrating with these systems, Armatura One enables license plates to serve as credentials. Once the license number is matched, it will automatically control gates and barriers for convenient access to parking lots.

Furthermore, Armatura One offers the capability to record LPR data and export comprehensive reports, allowing for further analysis and documentation, this includes essential information such as car entry time, date, and the corresponding region or country.



Empowering Global Surveillance with Real-Time Video Monitoring

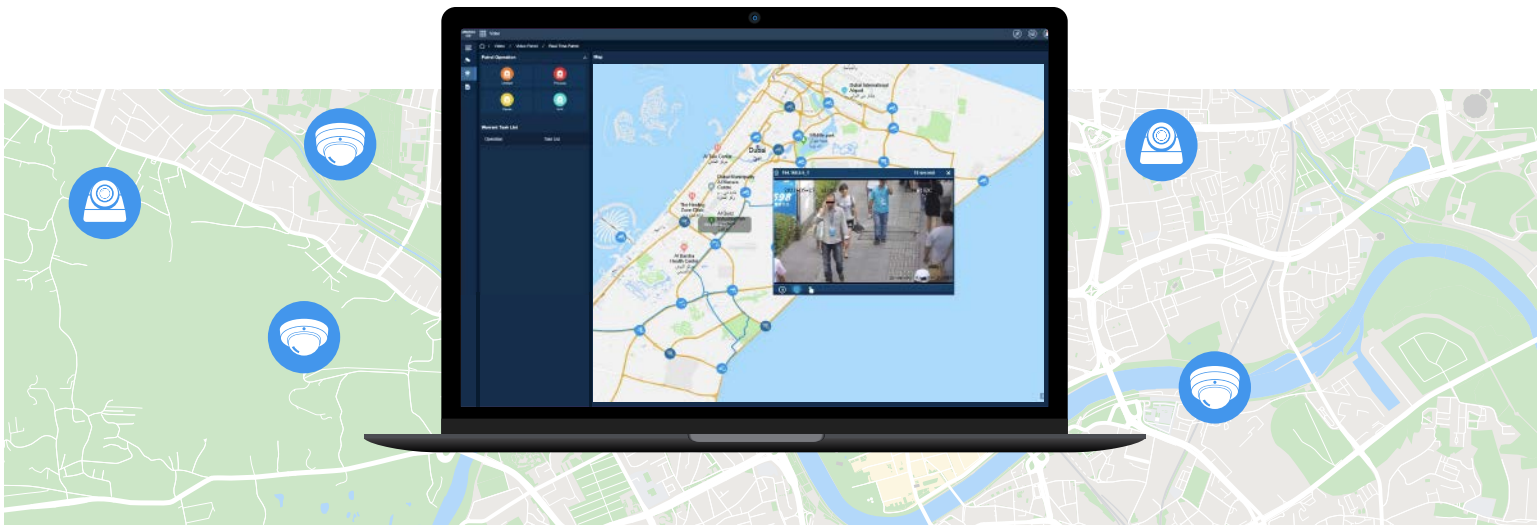
Armatura One is a web-based security software that offers a complete suite of features. One of its notable capabilities is the video module, which enables individuals, users, and organizations to conveniently view their video surveillance feeds in real-time, regardless of their location worldwide. This means that Armatura One users can effortlessly monitor their video surveillance systems from anywhere across the globe, ensuring enhanced security and peace of mind.





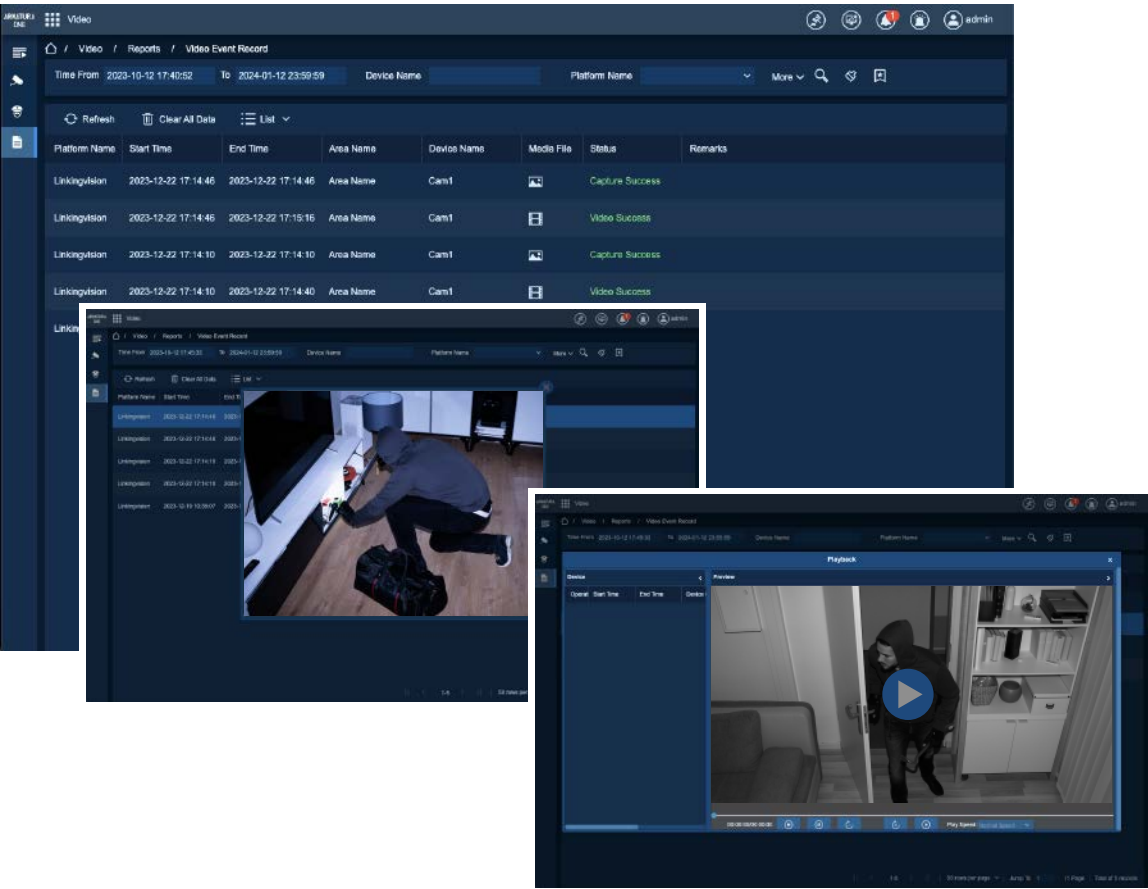
Enhancing Surveillance with Real-Time Camera Views and Efficient Patrol Management

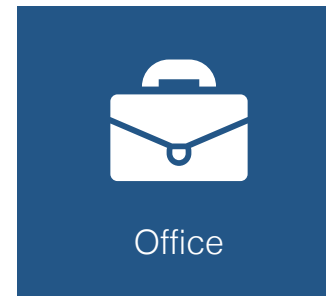
Video Patrol provides real-time camera views for surveillance patrol. Administrators can create patrol groups for specific staff, patrol timeslots, devices, and plans. Patrol staff can log in to the system, preview their patrol via real-time video surveillance, and report abnormal events for manual alarm and patrol. The system generates automatic patrol reports for management review.



Camera Alarm Monitoring and Processing in the System

The system supports delivery of various alarms of the cameras to the system, thus enabling real-time monitoring of events in the alarm centre, with only a single click, security staffs may view the locations of the events of abnormality. The system also support preview of real-time video and playback of the video records of the events, and add records of the processing of the alarm events.





Office Module

The Armatura Office Module integrates modern Meeting Room and Shared Work Booth reservation systems for efficient reservation management. This module enables users to generate QR codes and share them with guests for streamlined access control. It also offers full integration with popular video conferencing tools like Zoom.

Meeting Room Reservation

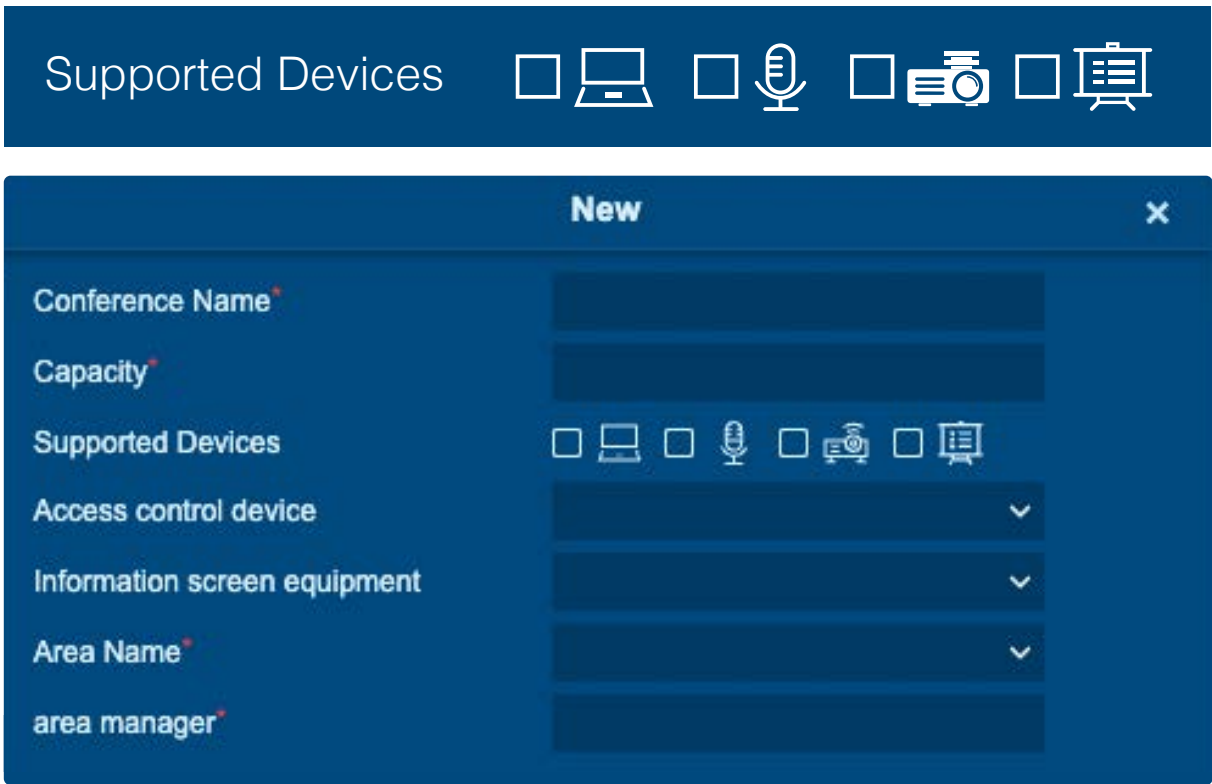
The meeting room reservation function allows users to book meeting rooms via the reservation section display. Users can select from available rooms in the facility management, specifying start and end times for their reservations through a web browser.



Room Devices Overview

Administrators can display the devices available within a specific meeting room, providing users with an overview of equipment such as:

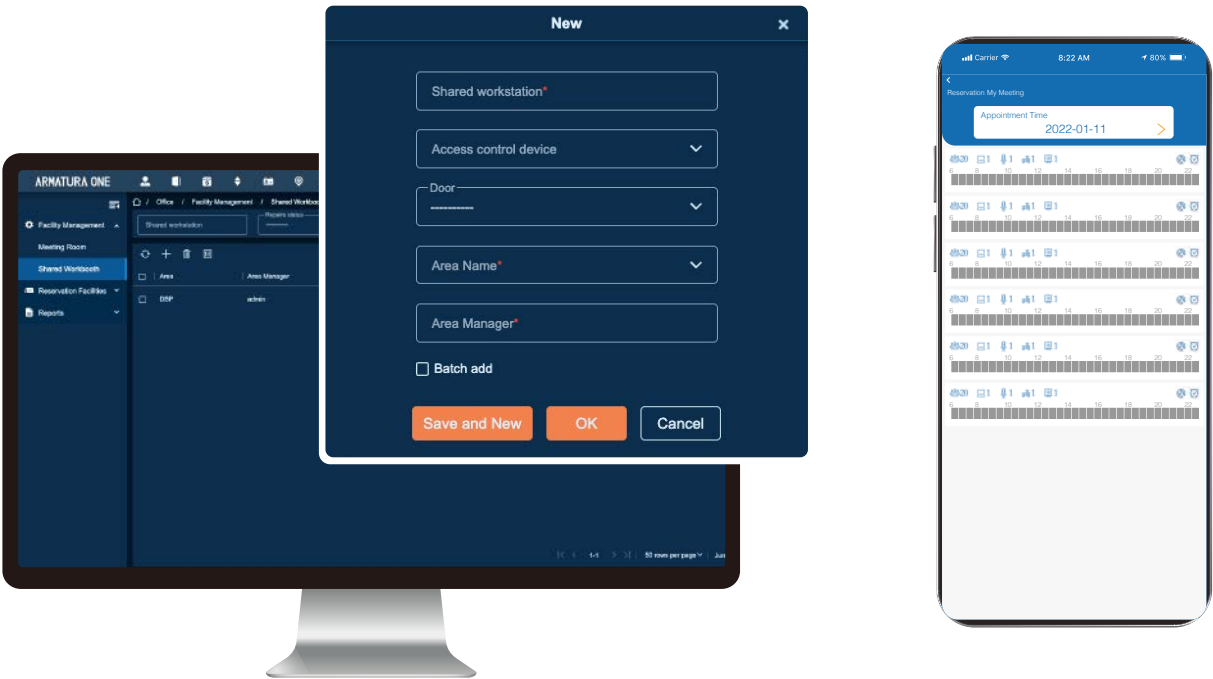
- 1) Computers
- 2) Microphones
- 3) Projectors
- 4) Interactive Whiteboards





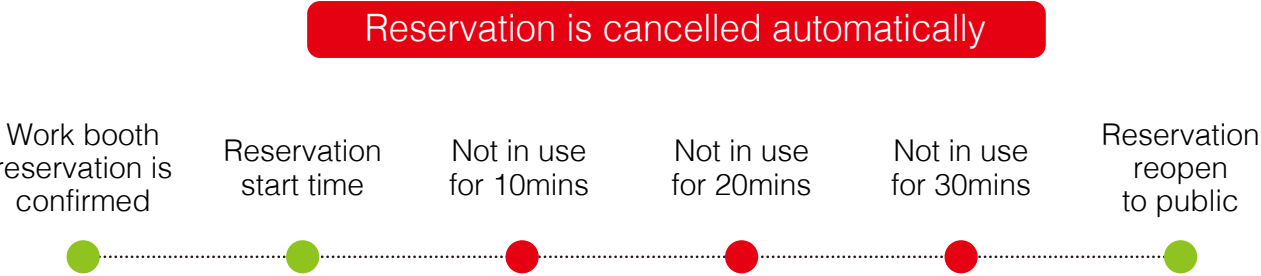
Shared Work Booth Reservation

Users can easily reserve shared work booths online by selecting available booths and specifying start and end times for booking sessions through a web browser.



Auto-Cancellation of Reservation

The auto-cancellation function, when activated, will automatically cancel and release reservations if a desk remains unused for 30 minutes past the scheduled reservation time.



Integration of Dynamic QR Code in Booking System

Armatura One combines room management and Dynamic QR code functionality to offer users a straightforward method for granting access to guests and visitors. The system generates accounts and Dynamic QR codes for access to specific areas through the following process:

- 1) Reserve a room or shared work booth for a person on a specific date and time
- 2) Enter the participant's personal information
- 3) Reservation details and meeting schedule are emailed to the participant
- 4) The participant logs into the portal using the email
- 5) The participant scans the provided QR Code for access to the meeting room or work booth



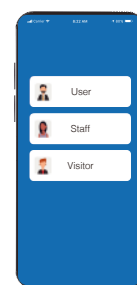
Reserves a room or a shared work booth for a person on a destined date and time



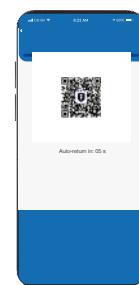
Fill in the select participants' personal information



The relevant reservation details and meeting schedule will be delivered to the person via email



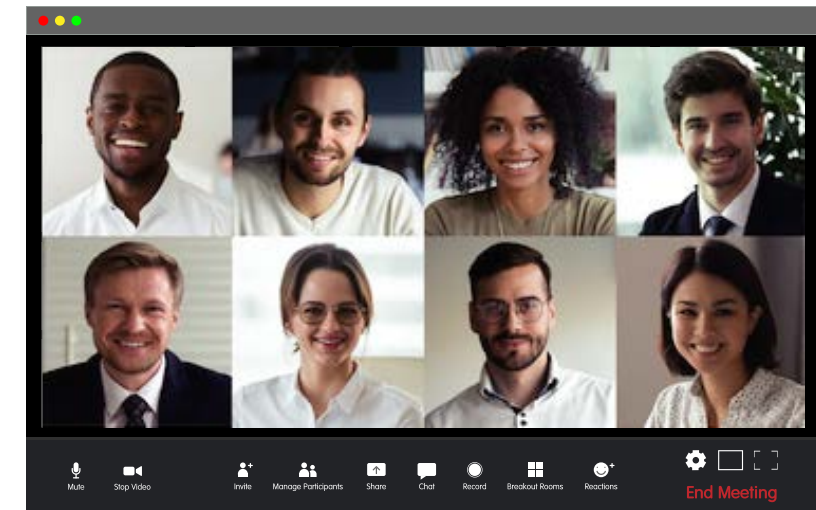
With the email, the person may log into the portal



The person only needs to scan the given QR Code to enter the meeting room or work booth accordingly

Full Integration with Zoom

After linking Armatura One with a user's Zoom account, the system assists users in reserving, creating, scheduling, and sending notification emails for virtual meeting rooms while simultaneously reserving a physical meeting room within Armatura One.





Entrance Control Module

The Entrance Control Module connects to gate control boards via channel devices and directly controls gate parameters through software, enabling comprehensive entrance/exit control and automatic gate management. It offers key features such as device online upgrading, entrance control access rules, and real-time monitoring.

Device Online Upgrade

The Armatura One Security Platform is designed to provide a seamless user experience by offering online upgrades for entrance control panels. This feature ensures that organizations can keep their security systems up to date with the latest features and improvements. In addition to online upgrades, the platform also supports online device parameter configuration, device capacity management, and parameter acquisition.

Key benefits of the Device Online Upgrade feature include:



- **Easy Upgrades:**

Online upgrades simplify the update process for entrance control panels, allowing organizations to quickly access new features, bug fixes, and performance improvements without the need for onsite visits or manual intervention.

Entrance Control Access Rules

Users can set gate barrier access rules, distribute personnel access rights, configure anti-passback rules, remotely configure barrier opening/closing speed, and closing barrier delay time.

ARMATURA ONE

Entrance

Channel Device

Monitoring

Entrance Control

Barrier Gate Permission...

Set Access By Levels

Anti-Passback

Linkages

Parameters

Passage Settings

Channel Reports

Entrance / Entrance Control / Parameters

Transaction Retrieval Settings

Periodically

Interval

1 hour(s)

Transaction Retrieval Times

Select All

Cancel

☒ 0:00

☐ 1:00

☐ 2:00

☐ 3:00

☐ 4:00

☐ 5:00

☐ 6:00

☐ 7:00

☐ 8:00

☐ 9:00

☐ 10:00

☐ 11:00

☐ 12:00

☐ 13:00

☐ 14:00

☐ 15:00

☐ 16:00

☐ 17:00

☐ 18:00

☐ 19:00

☐ 20:00

☐ 21:00

☐ 22:00

☐ 23:00

Getting transactions and synchronization time will be done at the same time.

Real Time Monitoring

Photo Pop-Up Size in Real-Time Monitoring

Max Height

140 px(80 - 500)

Refresh the real-time monitoring page after setting Height.

Alarm Monitoring Recipient's Mailbox

Example:123@xxx.com;456@xxx.com

Send to multiple email addresses by using a comma (,) or a semicolon (;)

Real-Time Monitoring

Dynamic image display of barrier status is enabled, with support for remote barrier opening, remote activation of always-open timeslots, remote alarm cancellation, and quick view of recent barrier events.

Remote opening (In)

Remote opening (Out)

Cancel alarm

Remote lock

Remote unlock

Remote normally open

ARMATURA ONE

Entrance Control

Entrance Control / Channel device / Real-Time Monitoring

Area

Status

Device Name

More

Barrier Gate

Auxiliary Input

All Gates

Remote Opening (In)

Remote Opening (Out)

Cancel alarm

Remote lock

Remote unlock

Remote Normally Open

More

Current Total:0

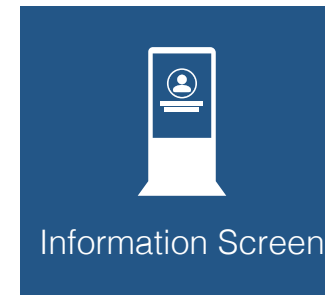
Online:0

Disable:0

Offline:0

Unknown:0

Barrier Gate Name



Information Screen Module

The Information Screen Module in Armatura One supports third-party kiosk devices, offering a convenient face recognition solution for various applications managing time & attendance. The module allows user-friendly attendance detail displays and advertisement displays, enhancing cost-effectiveness and precision for time & attendance management.



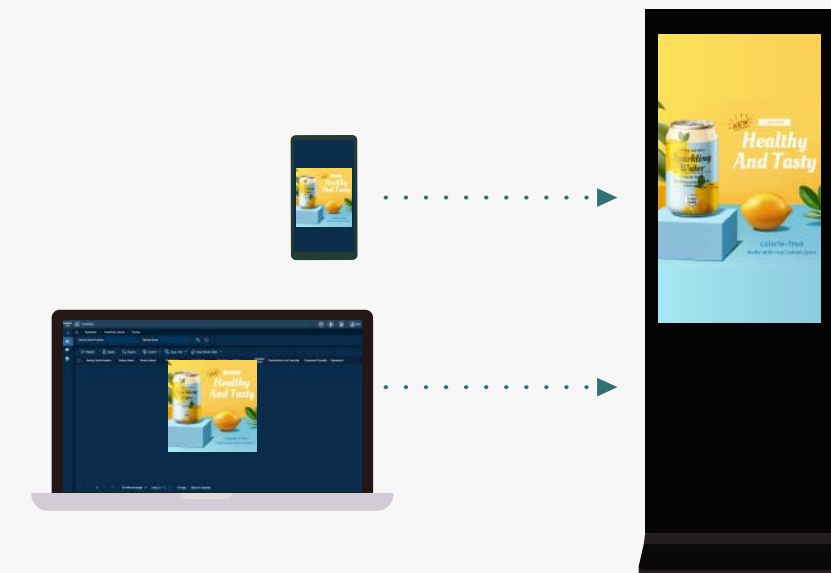
Managing Third-Party Kiosk Devices

Armatura One manages third-party kiosk devices for face recognition applications across a wide range of scenarios, efficiently managing time & attendance and kiosk advertisement functions.



Kiosk Advertisement Management

Third-party kiosks can be used effectively for marketing, with Armatura One enabling the uploading and management of advertisement images and videos via internet access.



Attendance Details Display by Area or by Person

- Area: Displays staff attendance information according to areas.
- Person: Displays specific staff identities and their attendance records.

Time and Attendance Management with Kiosk Devices

Armatura One supports visible light face recognition devices, accurately recording staff attendance when facing kiosk devices for monitoring and management of employee attendance, including working hours, late arrivals, early punch-outs, break hours, and absences.





Defence Module

The Defence Module is a scenario-based defence mechanism offering capacity control and access control with high security and convenience. It detects human faces, counts entrance and exit numbers, verifies and tracks people for optimal access control solutions with ultimate efficiency and safety.

Global Target Control

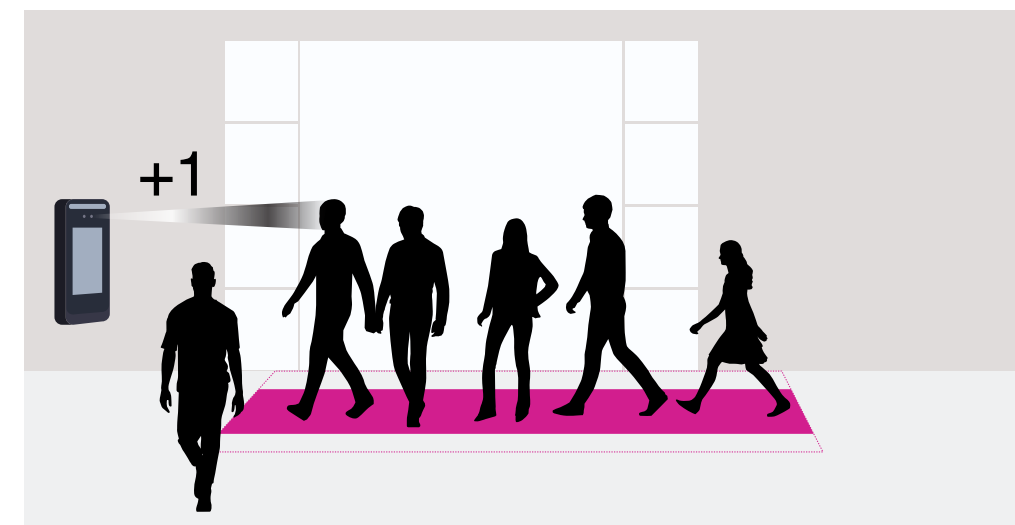
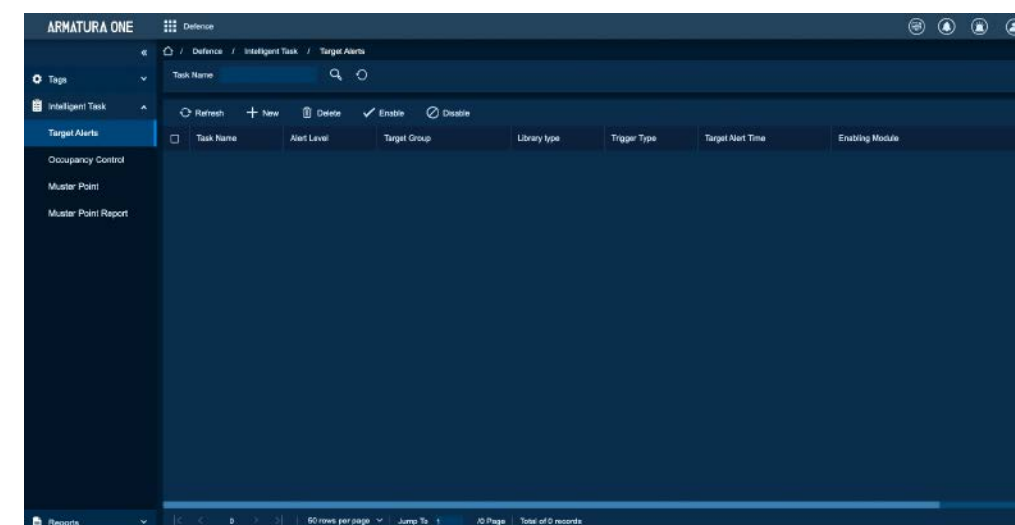
This function extends people control from video surveillance devices for facial recognition to full-module devices, enabling access control, time & attendance, elevator control, and parking management system target control. It provides new alarm sources while maintaining existing device functionality across various modules.

Features:

1. Inter-module actualisation includes access control, time & attendance, elevator control, parking management, visitor management, and information display devices
2. Supports hit alarm and missed alarm
3. Supports customisations of 4 event types: Emergency, Important, General, and Prompt
4. All control alarm records are displayed in the alarm center and can be processed and handled smoothly

People Counting

The system combines facial recognition and people counting functions for access control and capacity control. It detects human faces in specific areas, automatically counts the total number of people in those areas, and displays the figures in Armatura One live view.





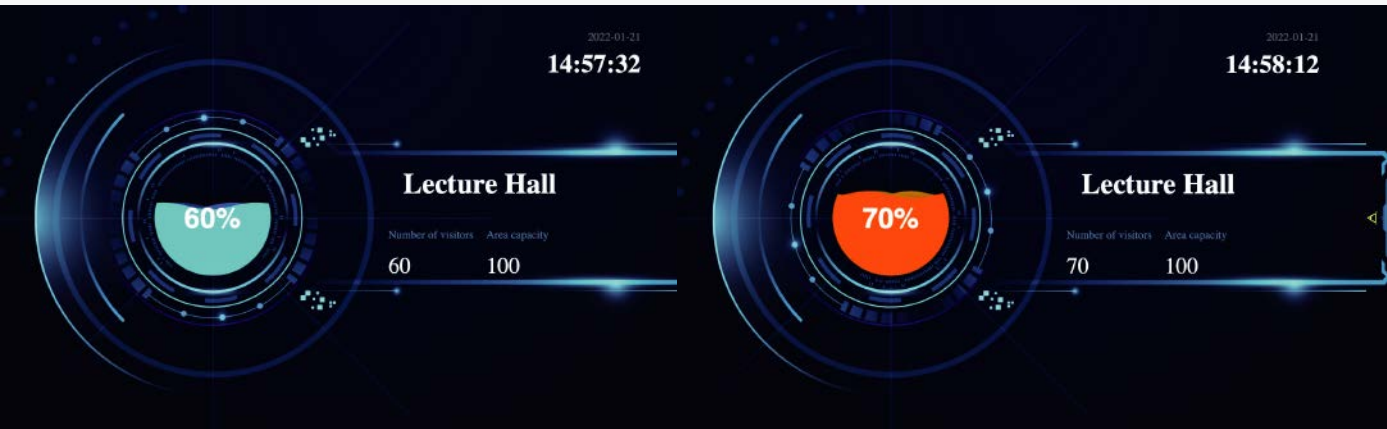
Occupancy Management

Armatura One helps control visitor flow with a pre-set maximum capacity, tracking the number of people entering and exiting venues and sharing real-time occupancy data.



Below Limitation (Access Allowed)

The system shows the occupancy rate of people in percentages and colors, with blue representing 0% to 69%, orange representing 70% to 89%, and red representing 90% to 100%.



Exceeding Limitation (Access Disallowed)

When red is displayed, it indicates that occupancy is near the capacity limit. Once the occupancy rate reaches 100%, people will not be allowed to access specific areas.





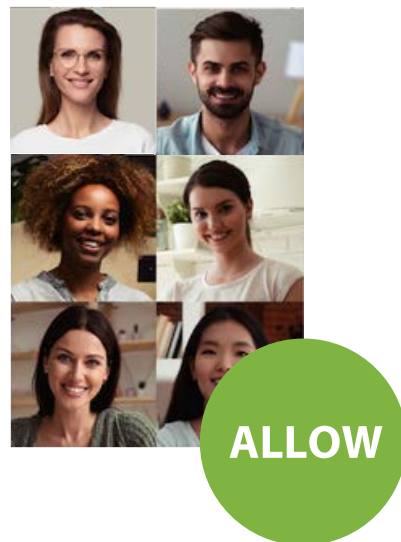
Real-Time Tracking Access Control Solution

Armatura One combines cutting-edge technologies, including facial recognition access control, time attendance, video surveillance, and LPR, to provide precise positioning information to track people in real-time. The system automatically tracks visitors and obtains their entire routes upon entering specific areas.



Allow List, Block List, and Visitor List Management

Armatura One supports the management of Allow Lists, Block Lists, and Visitor Lists to facilitate secure and efficient access control.



Allow List Management

The Allow List includes authorized personnel who are granted access to specific areas or facilities. Armatura One allows you to easily manage and assign access rights to individuals or groups, ensuring only authorized personnel can enter restricted areas.



Block List Management

The Block List includes unauthorized personnel or persons of interest who are denied access to specific areas or facilities. Armatura One enables you to manage the Block List, ensuring that unauthorized individuals are restricted from entering secured areas.



Visitor List Management

The Visitor List includes temporary visitors who are granted limited-time access to specific areas or facilities. Armatura One allows you to manage Visitor Lists, ensuring a smooth and secure visitor experience.

Muster Point

Armatura One Security Platform supports the implementation of a Muster Point feature to ensure the safety and accountability of users during urgent situations, such as fires, natural disasters, or other emergencies. By directing users to gather at designated muster points and utilizing installed terminals or readers for people counting, the system helps provide life savers with critical information about the number of people still trapped inside the facility.



Designated Gathering Areas

Muster points are strategically placed in safe and accessible locations within or outside the facility to ensure users can quickly gather during an emergency.



People Counting

Installed terminals or readers at muster points are used to check in users as they arrive, providing a real-time count of the number of people who have reached safety.



Critical Information for Life Savers

The people counting data collected at muster points can be shared with emergency responders or life savers, helping them determine the number of individuals still trapped inside the facility and prioritize rescue efforts accordingly.



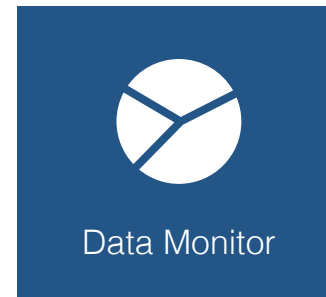
Enhanced Safety and Accountability

The Muster Point feature helps improve overall safety and accountability during emergencies by providing an organized and efficient method for managing evacuations and ensuring users are accounted for.



Roll Call and Muster Reporting

Generate reports to account for all users present within a designated area. These reports serve the purpose of verifying the safe evacuation of all users in case of an emergency.



Data Monitor Module

The Data Monitor Module is designed to provide real-time summaries and insights into module data across Access Control, Visitor, Office, Personnel, Video, and System domains. This platform facilitates a clear and comprehensive understanding of trends and patterns in data that accurately represent the current state of operations.



Access Control Data Monitor

- Device Type Statistics, Regional Equipment Statistics, Module in Use, and Door Event Statistics Overview
- Normal and abnormal event Access Charts



Visitor Data Monitor

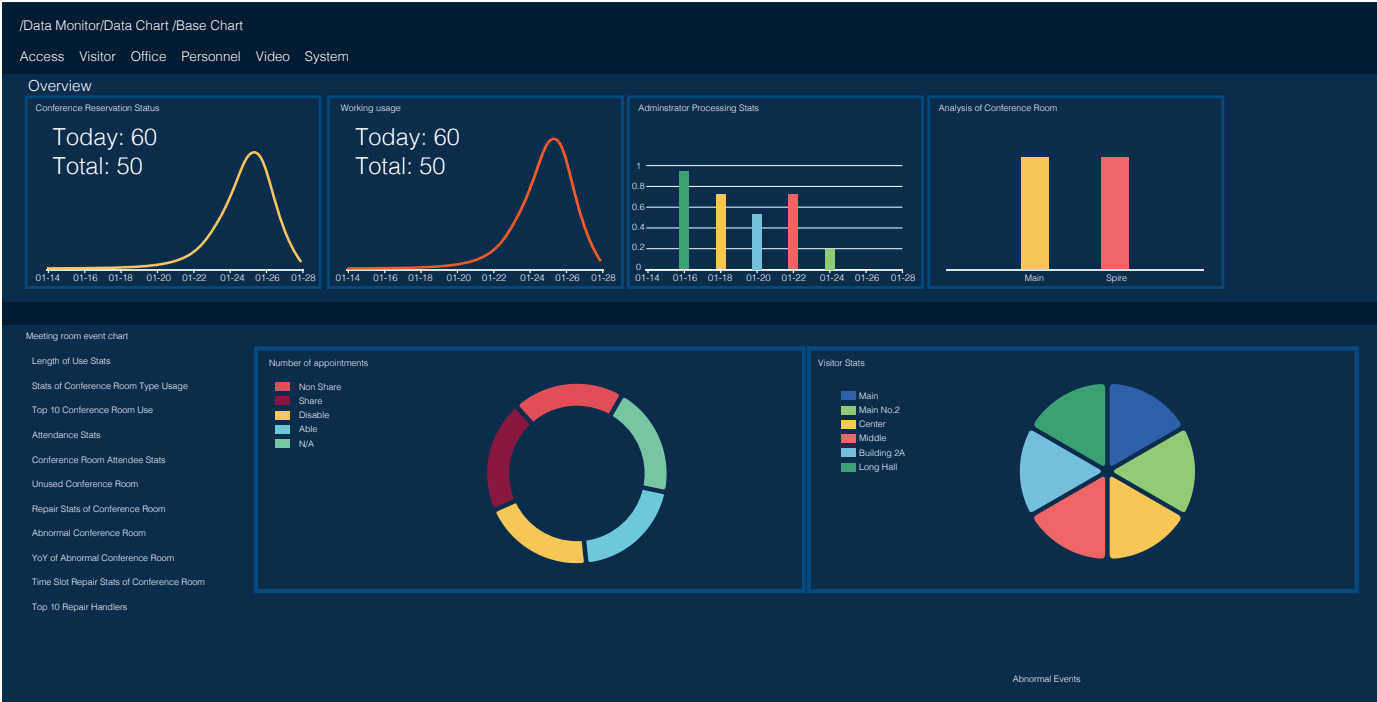
- Reservation Statistics, Visitor Statistics, and Check-out Statistics Overview
- Number of Appointments and Visitor Statistics charts





Office Data Monitor

- Conference Reservation Statistics, Workstation Usage, and Admin Processing Statistics Overview
- Conference Room Use Rate and Conference Room Reservation Statistics in Workstation Event Chart



Personnel Data Monitor

- Employee Statistics, Department and Personnel Statistics, and Number of Personnel in Control overview
- Expiring Personnel and Position Statistics charts





Video Data Monitor

- Regional Device Statistics and Patrol Times Statistics Overview
- Personnel Hit Alert Statistics and Personnel Non-Hit Alert Statistics charts



System Data Monitor

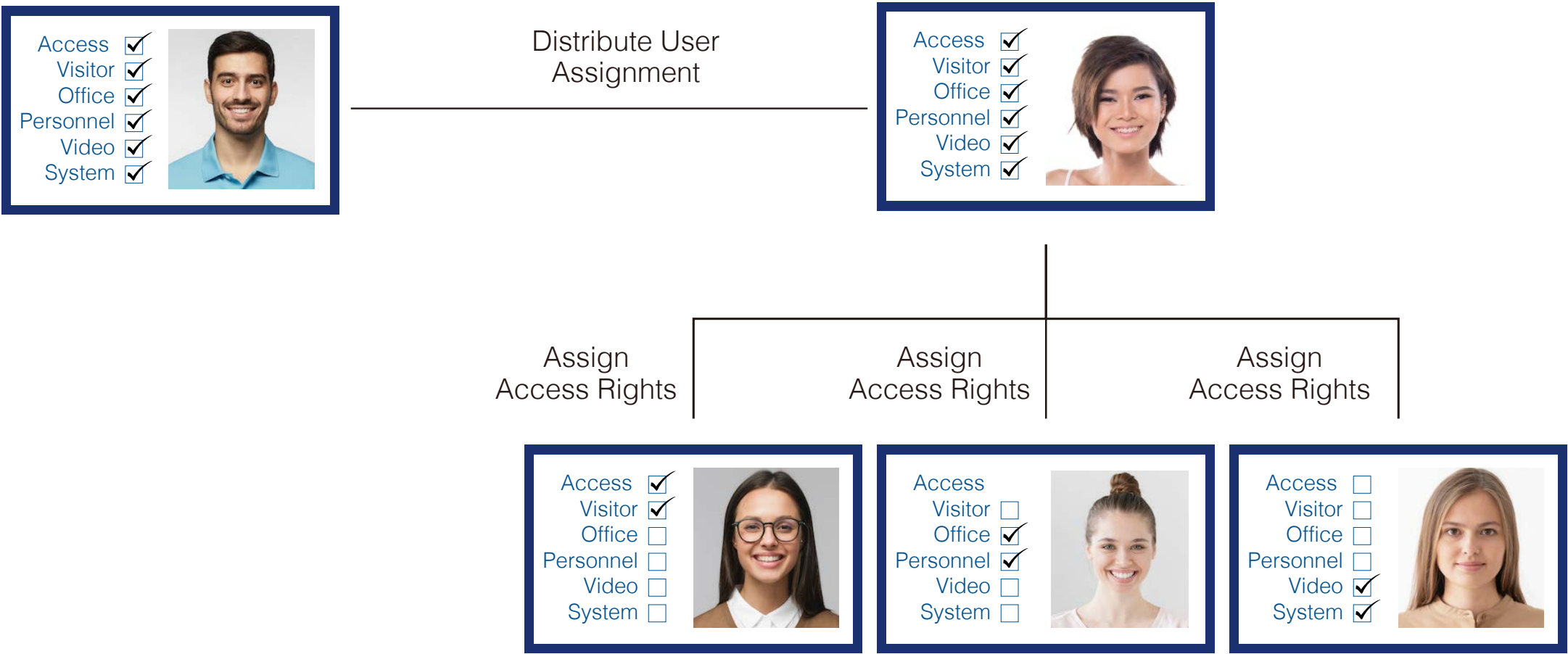
- Area Statistics, Role Statistics, and User Statistics Overview
- Mail Delivery Status and Top 5 Mail Subjects in System Charts

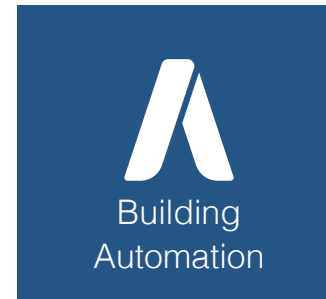




Role-Based Dashboard Access

Administrators have the ability to assign specific roles to team members with varying levels of access to different dashboard features. This enables efficient task completion by granting team members the appropriate level of access required for their assigned tasks while maintaining overall security and access control.





Building Automation Module

The Building Automation Module employs a computerized centralized control system to enable centralized management of decentralized control processes. The decentralized controllers typically utilize Direct Digital Controllers (DDC) for computer-based monitoring and management. The Building Automation System comprises several subsystems, including Air Conditioning, Heating, Ventilation, and Air Conditioning (HVAC) monitoring, Water supply and drainage monitoring, Lighting monitoring, Power supply monitoring, Structured integrated wiring system, and Dynamic environmental monitoring.



Monitoring and Management: Quick Response and Problem Handling

The Building Management System is a comprehensive, multi-dimensional management solution specifically designed for various scenarios, including buildings, factories, and parks. The system is compatible with Armatura Gateway and facilitates seamless integration with standard building management system protocols, such as BACnet, Modbus, KNX, and OPC. This integration enables effective monitoring and management of diverse subsystems, including HVAC, lighting, electricity supply, water supply and drainage, and environmental monitoring. By concentrating on monitoring subsystems, maps, and device attributes, the system is capable of providing multi-dimensional, rapid responses to issues and ensuring efficient problem handling.

AHPG-1000 Gateway (which supports BACnet, Modbus, KNX, OPC, and more) has been developed to work seamlessly with third-party building management terminals to enhance the system's capabilities. This compatibility extends to industry-leading brands, such as Honeywell, Johnson Controls, Siemens, and Bosch. By incorporating Armatura-OPC Gateway into the Building Management System, users benefit from a robust solution that offers increased flexibility, interoperability, and overall system efficiency. This collaboration enables better management, monitoring, and control of various building subsystems, fostering quick response times and effective problem resolution.

Building Automation / Device / Terminal

Terminal management

Terminal nameTerminal code

RefreshDelete

Terminal name	Terminal code	Gateway name	Subsystem
Office	24416	Office	HVAC
Front Door	25747	Front Door	HVAC
Back Door	35141	Back Door	HVAC
Meeting Room	87651	Meeting Room	HVAC

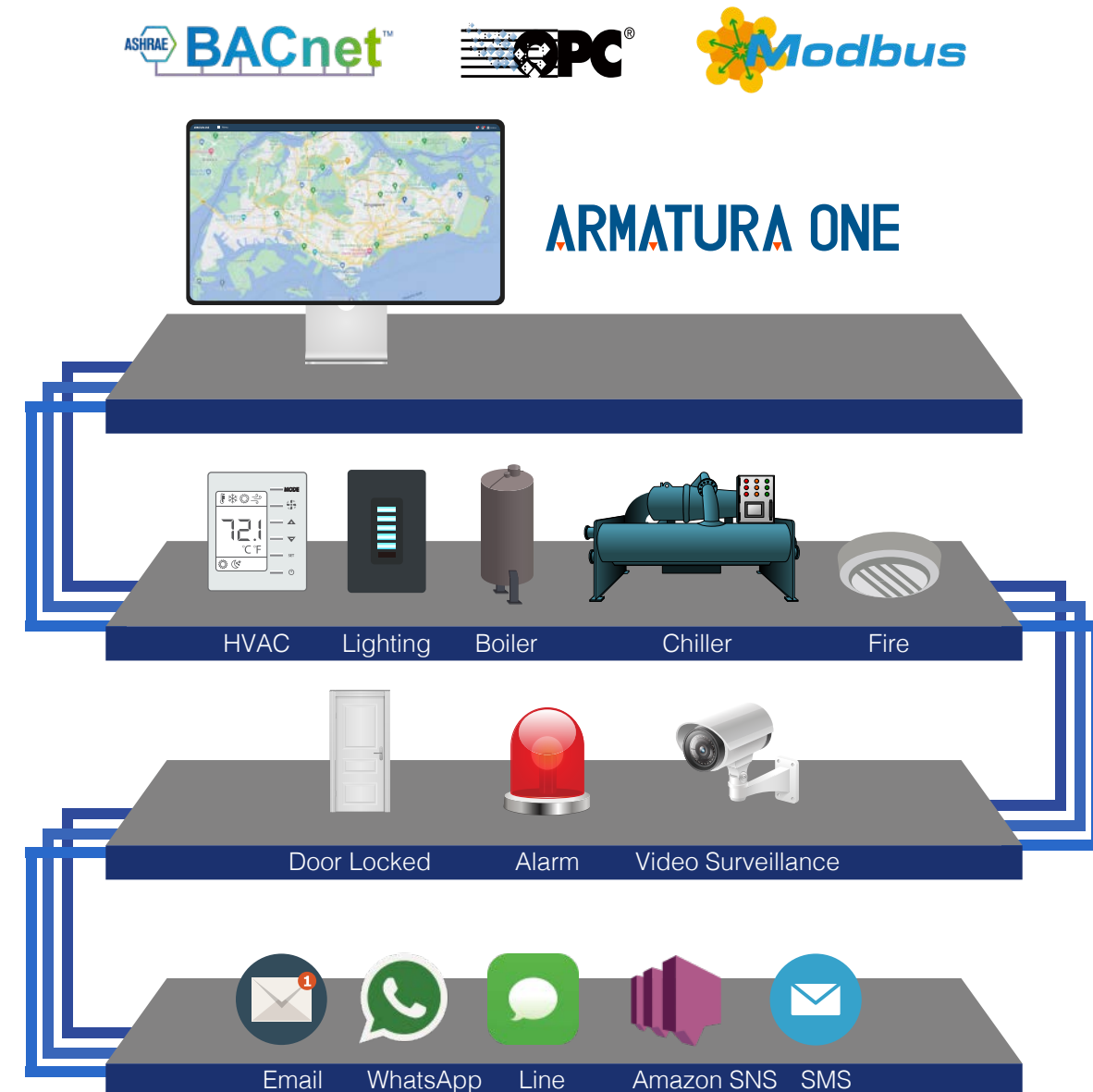
Attribute NameAttribute Code

Refresh

Attribute Name	Attribute Code	Data Type	Writable	Current Value
CLG_ONLY	CLG_ONLY	Boolean	✖	false
EFF_ZNT	EFF_ZNT	Float	✖	27.642
ERROR	ERROR	Integer	✖	1
FAN_S	FAN_S	Integer	✖	3
LC_PWR_PRI	LC_PWR_PRI	Integer	✖	1
OCC_S	OCC_S	Integer	✖	2
OPR_MODE	OPR_MODE	Integer	✖	3
POWER	POWER	Boolean	✖	true
ZN_SP	ZN_SP	Float	✖	28.0

Rules Center

The rules engine is designed to interact with different Armatura One connected devices for various linkage actions. Users can set multiple rules to communicate with different devices and systems, along with various attributes, system values, prompts, etc. This enhances cross-system interaction and provides advanced automation to end-users.





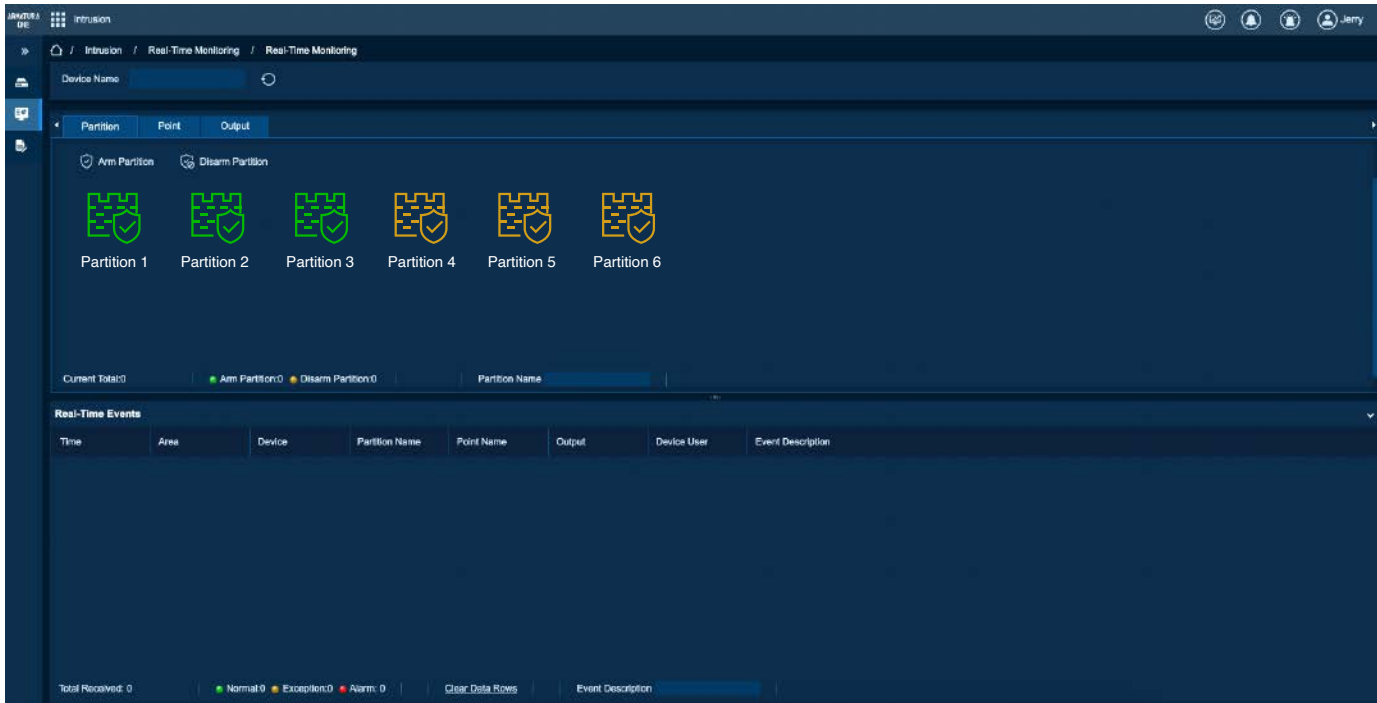
Intrusion Module

The Intrusion Alarm Module employs sensor technology and electronic information technology to detect, indicate, and process unauthorized entries or attempted unauthorized entries into a secured area. It also provides the ability for users to intentionally trigger emergency alarms in critical situations such as hijackings, robberies, or other emergencies.



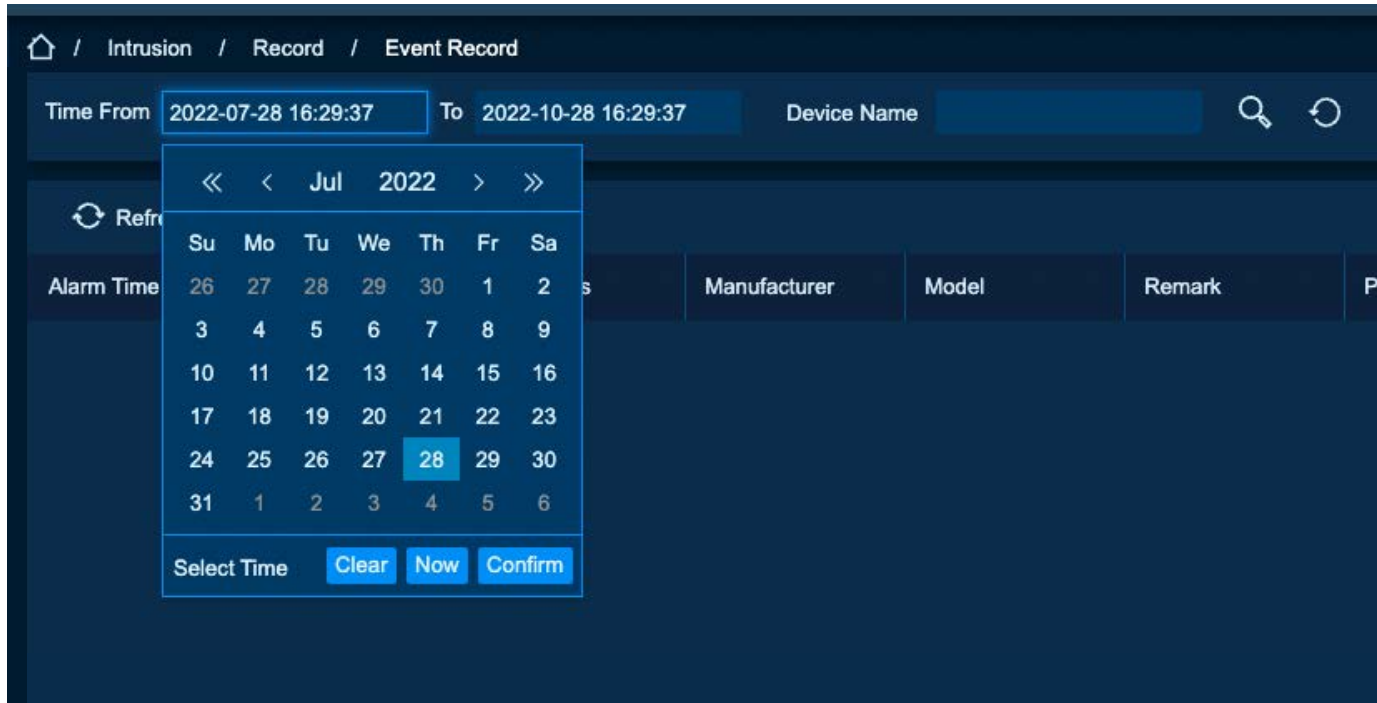
Real-Time Monitoring

This feature enables dynamic image display of alarm statuses (Online/Offline) and supports alarm operations, remote activation of always-open time slots, remote cancellation of alarms, and quick viewing of recent alarm events.



Event Record

The system automatically records triggered alarms and can display records for specific periods. For example, suppose the record of triggered alarms is required from July 28th to 30th, 2022. In that case, the system automatically collects, sorts, and displays the records for the selected time period, facilitating convenient inspection of the records.



ARMATURA

Report Templates

Personnel Management Summary Report @Personnel Module

Person													
Personnel ID	First Name	Last Name	Department Number	Department Name	Gender	Birthday	Password	Certificate Type	Certificate Number	Card Number	Email	Reservation Code	Mobile Phone
1	Jerry	Williams	1	General	Male	1980-04-23	1	1	TP443566	4461253	abwe@qwe.com	123456	59496464
2	Lucky	Williams	3	Development Department	Female	1992-12-08	2	3	784515	6155266	778@abc.com	123456	4425521
2940	Sherry	Brown	hotel	Hotel	Female	1997-12-01	2940	1	741741	1411237	555@qq.com	123456	145145145
3	Leo	Davis	4	Financial Department	Male	1998-12-22	3	1	23687	13271770	3232@qq.com	123456	34342543
4	Berry	Miller	1	General	Female	2007-12-05	4	4	745688QQWA	13592341	QWA@zzz.com	123456	74755466
5	Necol	Smith	2	Marketing Department	Male	2017-01-10	5	1	32242311	13260079	3322@qq.com	123456	6645454
6	Amber	Wilkinson	4	Financial Department	Female	2017-07-04	6	1	784525004	4628036	787878@eru.com	123456	44620545
7	Jacky	Williams	1	General		2016-01-05	7	8	ees1213232	6323994	434@qq.com	123456	54243231
8	Glori	Smith	2	Marketing Department	Female	1995-12-05	8	1	433114354	6189166	987@abcd.com	123456	77545353
9	Lilian	Miller	3	Development Department	Female	1992-12-23	9	1	XS22030	9505930	8989@pp.com	123456	221112121

Access Report @Access Module

Total People 10						
Personnel ID	First Name	Last Name	Department	Card Number	Last Access Time	Last Access Reader
1	Jerry	Williams	General	4461253	2017-12-18 09:29:31	192.168.218.60-2-In
2	Lucky	Williams	Development Department	6155266	2017-12-18 09:27:12	192.168.218.60-1-In
2940	Sherry	Brown	Hotel	1411237	2017-12-18 09:55:52	192.168.218.60-1-In
3	Leo	Davis	Financial Department	13271770	2017-12-18 09:34:57	192.168.218.60-2-In
4	Berry	Miller	General	13592341	2017-12-18 09:55:58	192.168.218.60-1-In
5	Necol	Smith	Marketing Department	13260079	2017-12-18 09:34:18	192.168.218.60-1-In
6	Amber	Wilkinson	Financial Department	4628036	2017-12-18 09:25:29	192.168.218.60-1-In
7	Jacky	Williams	General	6323994	2017-12-18 09:27:18	192.168.218.60-2-In
8	Glori	Smith	Marketing Department	6189166	2017-12-18 09:34:20	192.168.218.60-2-In
9	Lilian	Miller	Development Department	9505930	2017-12-18 09:27:22	192.168.218.60-1-In

All Access Transactions @Access Module

All Transactions

Time: 2017-09-15 00 : 00 : 00 - 2017-12-15 23 : 59 : 59

Time	Device Name	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department Name	Reader Name	Verification Mode	Area Name	Remark
2017-12-15 18:29:02	192.168.218.60	192.168.218.60-2	Background Verify Success	6	Amber	Wilkinson	4628036	Financial Department	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:59	192.168.218.60	192.168.218.60-1	Background Verify Success	6	Amber	Wilkinson	4628036	Financial Department	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:45	192.168.218.60	192.168.218.60-2	Background Verify Success	5	Necol	Smith	13260079	Marketing Department	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:41	192.168.218.60	192.168.218.60-1	Background Verify Success	5	Necol	Smith	13260079	Marketing Department	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:38	192.168.218.60	192.168.218.60-2	Background Verify Success	1	Jerry	Williams	4461253	General	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:35	192.168.218.60	192.168.218.60-1	Background Verify Success	1	Jerry	Williams	4461253	General	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:23	192.168.218.60	192.168.218.60-2	Background Verify Success	2940	Sherry	Brown	1411237	Hotel	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:20	192.168.218.60	192.168.218.60-1	Background Verify Success	2940	Sherry	Brown	1411237	Hotel	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:17	192.168.218.60	192.168.218.60-2	Background Verify Success	9	Lilian	Miller	9505930	Development Department	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:13	192.168.218.60	192.168.218.60-1	Background Verify Success	9	Lilian	Miller	9505930	Development Department	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:08	192.168.218.60	192.168.218.60-2	Background Verify Success	3	Leo	Davis	13271770	Financial Department	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:01	192.168.218.60	192.168.218.60-1	Background Verify Success	3	Leo	Davis	13271770	Financial Department	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:25:18	192.168.218.60	192.168.218.60-1	Remote Opening						Other	Other	Area Name	
2017-12-15 18:25:04	192.168.218.60	192.168.218.60-1	Remote Opening						Other	Other	Area Name	
2017-12-15 18:23:52	192.168.218.60	192.168.218.60-2	Background Verify Success	1	Jerry	Williams	4461253	General	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:40	192.168.218.60	192.168.218.60-1	Remote Opening						Other	Other	Area Name	
2017-12-15 18:23:26	192.168.218.60	192.168.218.60-1	Remote Opening						Other	Other	Area Name	
2017-12-15 18:23:	192.168.218.60	192.168.218.60-2	Background Verify	1	Jerry	Williams	4461253	General	192.168.218.60-2-	Only Card	Area Name	

Business Trip Report @Attendance Module

Business Trip

Personnel ID	First Name	Last Name	Department Number	Department Name	Start Time	End Time	Remark	Operation Time
4	Berry	Miller	1	General	2017-12-15 16:37:27	2017-12-15 16:37:27		2017-12-15 16:37:31
5	Necol	Smith	2	Marketing Department	2017-12-18 11:42:28	2017-12-18 11:42:28	Go to Shenzhen	2017-12-18 11:42:51
8	Glori	Smith	2	Marketing Department	2017-12-18 11:42:55	2017-12-18 11:42:55	Go to Thailand	2017-12-18 11:43:08

Overtime Report @Attendance Module

Overtime

Personnel ID	First Name	Last Name	Department Number	Department Name	OT Type	Start Time	End Time	Remark	Operation Time
3	Leo	Davis	4	Financial Department	Normal OT	2017-12-15 16:37:34	2017-12-15 16:37:34		2017-12-15 16:37:37
5	Necol	Smith	2	Marketing Department	Normal OT	2017-12-18 11:44:03	2017-12-18 11:44:03	Finish Project	2017-12-18 11:44:28

Daily Attendance Report @Attendance Module

Daily Attendance									
Personnel ID	First Name	Last Name	Department Number	Department Name	Record Date	Record Times	Earliest Time	Latest Time	Punch Time
1	Jerry	Williams	1	General	2017-12-15	35	16:33:27	18:28:38	16:33:27;16:33:29; 16:33:34;16:34:03; 16:34:04;16:34:05; 16:34:08;16:35:02; 16:35:03;17:35:25; 17:35:26;17:42:50; 17:42:51;17:42:52; 17:58:49;17:58:50; 18:04:44;18:04:45; 18:22:20;18:22:21; 18:23:12;18:23:18; 18:23:18;18:23:19; 18:23:38;18:23:37; 18:23:52;18:24:59; 18:25:00;18:25:13; 18:25:14;18:28:34; 18:28:35;18:28:37; 18:28:38;
2	Lucky	Williams	3	Development Department	2017-12-15	28	16:33:42	18:28:56	16:33:42;16:33:43; 16:33:51;16:33:59; 16:34:00;16:35:05; 16:35:06;17:35:32; 17:42:47;17:42:48; 17:58:03;17:58:04; 17:59:38;17:59:39; 18:04:59;18:05:00; 18:05:07;18:05:08; 18:09:35;18:09:38; 18:23:00;18:23:01; 18:23:02;18:28:53; 18:28:55;18:28:56;
2940	Sherry	Brown	hotel	Hotel	2017-12-15	17	16:33:16	18:28:23	16:33:16;16:34:08; 16:34:10;16:35:08; 16:35:09;17:35:19; 17:43:01;17:43:02;

Leave Summary Report @Attendance Module

Leave Summary					
Personnel ID	First Name	Last Name	Department Number	Department Name	Leave Type Statistics
1	Jerry	Williams	1	General	Casual Leave(1) Marriage Leave(0) Maternity Leave(0) Sick Leave(0) Annual Leave(0) Bereavement Leave(0) Breastfeeding Leave(0) Custom (0)
5	Necol	Smith	2	Marketing Department	Casual Leave(0) Marriage Leave(0) Maternity Leave(0) Sick Leave(0) Annual Leave(1) Bereavement Leave(0) Breastfeeding Leave(0) Custom (0)
9	Lillian	Miller	3	Development Department	Casual Leave(0) Marriage Leave(0) Maternity Leave(0) Sick Leave(0) Annual Leave(0) Bereavement Leave(0) Breastfeeding Leave(1) Custom (0)
3	Leo	Davis	4	Financial Department	Casual Leave(0) Marriage Leave(1) Maternity Leave(0) Sick Leave(0) Annual Leave(0)

Leave Report @Attendance Module

Leave									
Personnel ID	First Name	Last Name	Department Number	Department Name	Leave Type	Start Time	End Time	Remark	Operation Time
1	Jerry	Williams	1	General	Casual Leave	2017-12-15 16:36:07	2017-12-15 16:36:07		2017-12-15 16:36:17
3	Leo	Davis	4	Financial Department	Marriage Leave	2017-12-15 18:38:48	2017-12-15 18:38:48		2017-12-15 18:38:53
5	Necol	Smith	2	Marketing Department	Annual Leave	2017-12-15 16:36:19	2017-12-15 16:36:19		2017-12-15 16:36:27
6	Amber	Wilkinson	4	Financial Department	Sick Leave	2017-12-15 18:38:54	2017-12-15 18:38:54		2017-12-15 18:39:00
9	Lilian	Miller	3	Development Department	Breastfeeding Leave	2017-12-15 18:39:02	2017-12-15 18:39:02		2017-12-15 18:39:10

Time Shift Report @Attendance Module

Shift						
Name	Number	Schedule Type	Unit	Cycle	Start Date	Cycle Shift in one Month
Day Shift	1	Regular Shift	Day	10	2017-12-15	Yes
Night	2	Regular Shift	Day	10	2017-12-18	Yes
Flexible	3	Flexible Shift	Day	10	2017-12-18	Yes

Time Zone @Attendance Module

Time Zone						
Name	Number	Timetable Type	Check-in Start Time	Check-in Time	Check-out Time	Check-out End Time
Normal Time	1	Normal Time Zone	08:00	09:00	18:00	19:00
Flexible Timetable	2	Flexible Timetable	09:00			18:00
Day Time	3	Normal Time Zone	08:00	08:30	18:00	19:00
Test	T4	Normal Time Zone	20:00	20:30	23:30	23:59

Elevator control report @Elevator Module

All Transactions												
Time: 2017-09-18 00 : 00 : 00 - 2017-12-18 23 : 59 : 59												
Time	Device	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department	Reader Name	Verification Mode	Area	Remark
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-8	Normal Punch Open	3	Leo	Davis	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-5	Normal Punch Open	3	Leo	Davis	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-9	Normal Punch Open	3	Leo	Davis	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-1	Normal Punch Open	1	Jerry	Williams	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-4	Normal Punch Open	1	Jerry	Williams	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-3	Normal Punch Open	1	Jerry	Williams	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-2	Normal Punch Open	1	Jerry	Williams	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:38	192.168.218.65	192.168.218.65-8	Normal Punch Open	2	Lucky	Miller	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:38	192.168.218.65	192.168.218.65-10	Normal Punch Open	2	Lucky	Miller	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:38	192.168.218.65	192.168.218.65-9	Normal Punch Open	2	Lucky	Miller	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:38	192.168.218.65	192.168.218.65-7	Normal Punch Open	2	Lucky	Miller	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-6	Normal Punch Open	2940	Sherry	Davis	4481253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Davis	4481253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-7	Normal Punch Open	2940	Sherry	Davis	4481253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Davis	4481253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:51	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Davis	4481253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:51	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Davis	4481253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:	192.168.218.65	192.168.218.65-6	Normal Punch	2940	Sherry	Davis	4481253	General	192.168.218.65-	Card or Fingerprint	Area Name	

Guest Check-in Report @Hotel Module

Guest Checkin Report									
First Name	Last Name	Document Type	Document No.	Card Number	Check-In Time	Check-Out Time	Checkin Type	Room Name	Room Type
Maryan	Brown	ID	44443333	4117849102	2017-12-15 14:42:09	2017-12-15 15:18:49	Daily Rate Room	A1101	A
Carian	Miller	Passport	332454	4117858142	2017-12-15 14:51:15	2017-12-15 15:14:20	Daily Rate Room	B1103	A
Lucy	Smith	Passport	232145523	301973533	2017-12-15 14:43:39	2017-12-15 15:13:52	Daily Rate Room	A1102	A
Lucy	Smith	Passport	232145523	301973533	2017-12-15 15:13:52	2017-12-15 15:19:06	Daily Rate Room	B1105	A
Hook	Brown	ID	5577556	4117882494	2017-12-15 14:45:37	2017-12-15 14:50:09	Daily Rate Room	B1102	A
Maryan	Davis	ID	44443333	4117849102	2017-12-15 14:42:09	2017-12-15 15:18:49	Daily Rate Room	A1101	A
Bruno	Williams	Driver License	22322123	4117882494	2017-12-15 14:51:15	2017-12-15 15:14:20	Daily Rate Room	B1103	A

Visitor History Record @Visitor Module

Visitor History Record															
Visitor Code	First Name	Last Name	Company	Visit Reason	Host Number	Host First Name	Host Last Name	Visit Status	Card Number	Enter Time	Entrance	Exit Time	Exit Place	Carrying Goods In	Carrying Goods Out
800000011	Morry	Wilkinson	Google	Visit	7	Jacky	Smith	Check-Out	6189166	2017-12-15 11:44:57	server	2017-12-15 11:45:20	server	Camera Device	Camera Device
800000010	Tommy	Anderson	ZKTeco-Th	Visit	6	Amber	Wilkinson	Check-Out	6323994	2017-12-15 11:42:38	server	2017-12-15 11:45:26	server	Camera Card	Camera Card
800000009	Elian	Taylor	ZKTeco-Eu	Visit	5	Necol	Williams	Check-Out	13562341	2017-12-15 11:41:01	server	2017-12-15 11:45:51	server	Book Bottle	Book Bottle
800000008	Goura	Thomas	Essl	Visit	4	Berry	Miller	Check-Out	1411237	2017-12-15 11:39:14	server	2017-12-15 11:46:00	server	Kindle	Kindle
800000007	Monic	Miller	ZKTECO	Visit	1	Jerry	Williams	Check-Out	4628036	2017-12-15 11:21:06	server	2017-12-15 11:23:10	server	PC	PC
800000006	Bella	Jackson		Visit	2940	Sherry	Davis	Check-Out	4461253	2017-12-15 11:05:28	server	2017-12-15 11:22:00	server		Video
800000005	Bill	White		Visit	3	Leo	Davis	Check-Out	9605630	2017-12-15 11:02:36	server	2017-12-15 11:21:43	server		PC
800000004	Tom	Harris		Visit	2	Lucky	Taylor	Check-Out	13260079	2017-12-15 10:59:56	server	2017-12-15 11:21:31	server		IPAD
800000003	Stephn	Martin		Visit	3	Leo	Davis	Check-Out	13260079	2017-12-15 10:47:43	server	2017-12-15 10:56:57	server		
800000002	Joey	Leung		Visit	2	Lucky	Tan	Check-Out	9605630	2017-12-15 10:46:06	server	2017-12-15 10:57:05	server		
800000001	Mary	Huang		Visit	2940	Sherry	Davis	Check-Out	4461253	2017-12-15 10:43:43	server	2017-12-15 10:57:27	server		

Patrol Guard Transaction Record @Patrol Module

All Transactions											
Time: 2017-09-15 00 : 00 : 00 - 2017-12-15 23 : 59 : 59											
Time	Device Name	Personnel ID	First Name	Last Name	Card Number	Device Module	Route Name	Checkpoint	Verification Mode	Area Name	Remark
2017-12-15 13:53:51	192.168.218.60	8	Glori	Taylor	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53:51	192.168.218.60	8	Glori	Taylor	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:49	192.168.218.60	8	Glori	Taylor	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:48	192.168.218.60	8	Glori	Taylor	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53:46	192.168.218.60	7	Jacky	Miller	6323994	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:46	192.168.218.60	7	Jacky	Miller	6323994	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:18	192.168.218.60	8	Glori	Taylor	6189166	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:17	192.168.218.60	8	Glori	Taylor	6189166	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54:15	192.168.218.60	7	Jacky	Miller	6323994	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54:14	192.168.218.60	7	Jacky	Miller	6323994	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:10	192.168.218.60	5	Necol	White	13260079	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54:10	192.168.218.60	5	Necol	White	13260079	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:08	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:07	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53:48	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53:47	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53:44	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53:	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint2	Only Card	Area Name	

Patrol Record by Day @Patrol Module

Patrol Records Today											
Time	Device Name	Personnel ID	First Name	Last Name	Card Number	Device Module	Route Name	Checkpoint	Verification Mode	Area Name	Remark
2017-12-15 13:53:51	192.168.218.60	8	Glori	Taylor	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53:51	192.168.218.60	8	Glori	Taylor	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:49	192.168.218.60	8	Glori	Taylor	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:48	192.168.218.60	8	Glori	Taylor	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53:46	192.168.218.60	7	Jacky	Anderson	6323994	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53:46	192.168.218.60	7	Jacky	Anderson	6323994	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:18	192.168.218.60	8	Glori	Taylor	6189166	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:17	192.168.218.60	8	Glori	Taylor	6189166	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54:15	192.168.218.60	7	Jacky	Anderson	6323994	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54:14	192.168.218.60	7	Jacky	Anderson	6323994	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:10	192.168.218.60	5	Necol	Thomas	13260079	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54:10	192.168.218.60	5	Necol	Thomas	13260079	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:08	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54:07	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53:48	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53:47	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53:44	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53:43	192.168.218.60	2	Lucky	Wilkinson	6155266	Access	route1	checkpoint2	Only Card	Area Name	

Operation Log Record @System Module

Operation Log							
Operation User	Operation Time	Operation IP	Module	Operating Object	Operation Type	Operation Content	Result
admin	2017-12-18 15:06:35	127.0.0.1	Visitor	Visitor	Export	Export	Succeed
admin	2017-12-18 15:03:40	127.0.0.1	Elevator	Access Rights By Personnel	Export	Export	Succeed
admin	2017-12-18 15:03:17	127.0.0.1	Elevator	Access Rights By Floor	Export	Export	Succeed
admin	2017-12-18 15:02:59	127.0.0.1	Elevator	All Exception Events	Export	Export	Succeed
admin	2017-12-18 15:01:27	127.0.0.1	Elevator	All Transactions	Export	Export	Succeed
admin	2017-12-18 14:25:34	127.0.0.1	Attendance	Appended Receipt	Export	Export	Succeed
admin	2017-12-18 14:24:41	127.0.0.1	Attendance	Leave	Export	Export	Succeed
admin	2017-12-18 14:24:05	127.0.0.1	Attendance	Leave	Export	Export	Succeed
admin	2017-12-18 14:23:45	127.0.0.1	Attendance	Business Trip	Export	Export	Succeed
admin	2017-12-18 14:23:25	127.0.0.1	Attendance	Go Out	Export	Export	Succeed
admin	2017-12-18 14:22:26	127.0.0.1	Attendance	Overtime	Export	Export	Succeed
admin	2017-12-18 14:13:29	127.0.0.1	Attendance	Overtime	Export	Export	Succeed
admin	2017-12-18 14:08:58	127.0.0.1	Attendance	Adjust and Append	Export	Export	Succeed
admin	2017-12-18 14:04:21	127.0.0.1	Attendance	Adjust Shift	Export	Export	Succeed
admin	2017-12-18 14:02:21	127.0.0.1	Attendance	Adjust Shift	New	5	Succeed
admin	2017-12-18 14:00:27	127.0.0.1	Attendance	Adjust Shift	New	4;3	Succeed
admin	2017-12-18 13:58:27	127.0.0.1	Attendance	Adjust Shift	New	3	Succeed
admin	2017-12-18 13:55:40	127.0.0.1	Attendance	Adjust and Append	New	3;;3	Succeed

ARMATURA



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005

Phone: +1-650-4556863

Email: sales@armatura.us

Website: www.armatura.us

Copyright © 2025 Armatura LLC @ ARMATURA, the ARMATURA logo, are trademarks of Armatura