



Guardian Security Converged

Software for Physical
Identity and Access
Management (PIAM)



Guardian is the industry-leading Physical Identity and Access Management (PIAM) solution that integrates customers' Physical Access Control Systems (PACS), enterprise IT applications, HR, and LMS systems under one unified cyber-umbrella.

The Alert Enterprise solution addresses threats beyond IT, encompassing physical access and operational systems to ensure compliance with strict industry-specific and region-specific regulations and standards. Guardian software delivers comprehensive PIAM capabilities across diverse systems from multiple vendors. It provides a unified interface that ensures consistent policy enforcement across all facilities, sites, and locations, complemented by no-code, highly configurable workflows.

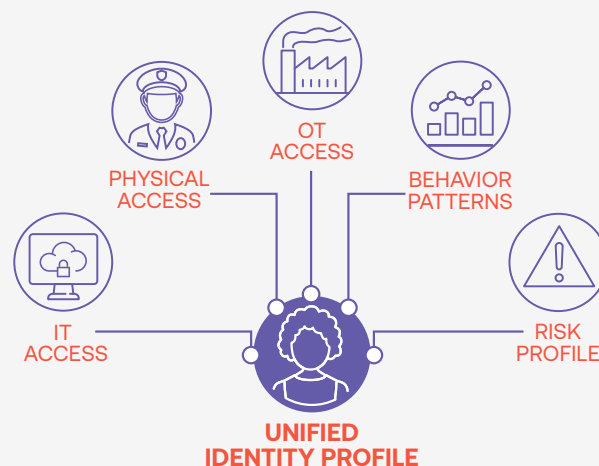
Automated PIAM from Hire to Retire.

Guardian simplifies user onboarding, offboarding, and termination processes by introducing a single interface for submitting access and review requests across multiple systems and asset types.

Extend Converged Digital Capabilities Across IT and Physical Environments.

Consolidated digital identities across physical, logical, and SCADA environments mitigate risks, close security gaps, and enforce customer policies. Guardian tracks multiple roles and identities, facilitating access to physical locations and virtual environments, as well as specific user rights within critical systems and applications.

A Unified Identity Profile Enables Intelligent Decision Making



Core Functions

Explore the core features and functions and see how Guardian solves challenges right out of the box.

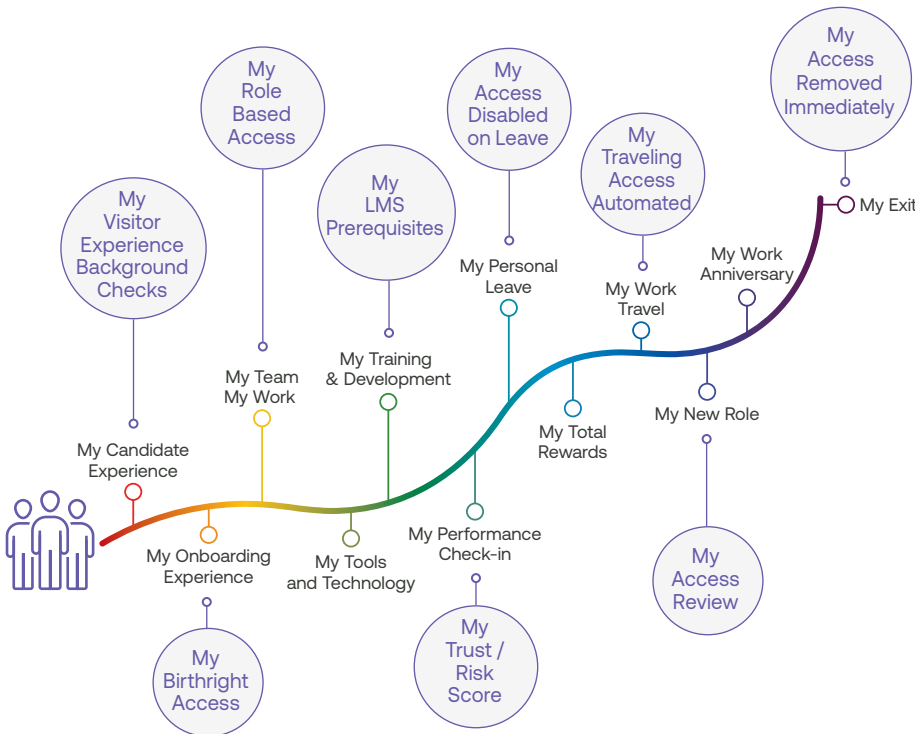
Access Management.

- Guardian seamlessly integrates out-of-the box with the industry's leading enterprise-level access control applications
- Enables users and managers to easily view and submit access requests for themselves or others
- Audit granted access in line with industry-specific or company-specific standards
- Can be configured to deactivate badges after a specified period of inactivity - enhancing security and efficiency

Refine Search < System Create, View & Manage

Records Found : 10 Enter to Search

Type	Code	Type	Environment	Category
AMAG Con...	SYS-000009	AMAG Connector	QA	CIP
AMAG Sym...	SYS-000021	LenelS2 NetBox	PROD	CIP
Lenel	SYS-000025	Honeywell JACE Webstation	QA	CIP
SAP Field G...	SYS-000022	LenelS2 NetBox	PROD	CIP
SAP	SYS-000015	AMAG Connector	QA	CIP
SAP Succes...	AE-SYS-000011	AMAG Connector	QA	CIP
Active Direc...	SYS-000020	Lenel	PROD	Lenel
DMPConne...	SYS-000016	Lenel	PROD	CIP
LenelS2 Ne...	SYS-000041	CCURE 9000	DEV	CIP
TIA Portal	SYS-000046	CCURE 9000	DEV	CIP
SEL-GATEW...				
Rockwell Fa...				
Honeywell J...				
File Connec...				
IDO				
Oracle				
CyberArk				



Hire to Retire Automation.

Real-time integration with leading HR systems and data:

- Allows Supervisors, HR, and Security Administrators to initiate and manage identity onboarding and offboarding processes
- Provisioning and Deprovisioning of access levels based on various attributes like associated role, location, and company policies
- Facilitates automated removal of unused access rights to enhance company-wide security hygiene practices

Core Functions

Audit and Compliance.

- Guardian ensures availability of a detailed audit trail for every activity that takes place on the platform
- Facilitates compliance across diverse systems, through automation of security governance and policy enforcement
- Access requests and approvals are streamlined, with automatic policy and compliance documentation checks
- Supports comprehensive contractor and temporary employee management
- Unified interface delivers consistent policy enforcement - ensuring adherence to regulatory requirements



Anna Mordeno

Provisioning Invoked for : on Jul 26, 2024 2:34:32 pm by Anna Mordeno

Asset 1001154 deactivated successfully for user 12177663 [Alan Ward] in Lenel system.

Jul 26, 2024 02:34:32 PM



Anna Mordeno

Provisioning Invoked for : on Jul 26, 2024 2:34:32 pm by Anna Mordeno

Access 24x7 Clearance removal successful for user 1217763 [Alan Ward] in Lenel system with validity period 26-Jul-2024 13:32:22 UTC to 29-Jun-2025 18:30:00 UTC.

Jul 26, 2024 02:34:32 PM



Anna Mordeno

AccessRequest of type Emergency Termination created by Anna Mordeno (anna.mordeno) on Jul 26, 2024 2:34:31 pm

Asset: 1001154 added with action LOCK for Alan Ward with validity period 26-Jul-2024 13:31:37 UTC to 26-Jul-2025 13:31:37 UTC

System: Lenel added with action LOCK for Alan Ward with validity period 26-Jul-2024 13:31:37 UTC to 26-Jul-2025 13:31:37 UTC

Access: 24x7 Clearance added with action REMOVE for Alan Ward with validity period 26-Jul-2024 13:32:22 UTC to 29-Jun-2024 18:30:00 UTC

Access: 24x7 Clearance REMOVE (action) for Alan Ward

Jul 26, 2024 02:34:42 PM

Reports and Reviews.

- Guardian integrates with IT, HR, cybersecurity, learning management, and ticketing systems
- Goes beyond simple data reconciliation - generates detailed reports with predefined frequency or as needed
- Both physical and logical access to be reviewed on a regular basis – adhering to compliance standards
- Reports can be used to review identities that are active, inactive, and pending for approval or certification

Identity Tracking

Identity Tracking

Records Found: 32

User ID	First Name	Last Name	Last Badge Swipe	Badge Type	Badge ID	DR Down
11045	Brock	Vogel	12/09/2022 09:47:00 pm	permanent_badge	3069403470683607	+
add.robart	Addi	Robert	12/09/2022 09:47:00 pm	temporary_badge	304994658068314	+
AnthonySmith85	Anthony	Smith	06/06/2022 09:47:00 pm	permanent_badge	3541454861245786	+
bern.stokes	Benn	Stokes	12/09/2022 09:47:00 pm	permanent_badge	3062482915040595	+
Charles.rob	Charles	Rob	12/09/2022 09:47:00 pm	permanent_badge	3056899251658014	+
Charles.rob	Charles	Rob	06/09/2022 09:47:00 pm	temporary_badge	3110691268253120	+
chris.woakes	Chris	Woakes	12/09/2022 09:47:00 pm	permanent_badge	3062482915069782	+
chris.woakes	Chris	Woakes	12/09/2022 09:47:00 pm	permanent_badge	3062745247944318	+
FredTyson35	Fred	Tyson	23/08/2021 09:58:00 pm	Door_reader	3305652115184921	+
FredTyson35	Fred	Tyson	05/04/2024 11:58:00 am	permanent_badge	4546242521196448	+
gary.khen	Gary	Khan	12/09/2022 09:47:00 pm	permanent_badge	3061256220201051	+
JackPaul18	Jack	Paul	12/09/2022 09:47:00 pm	permanent_badge	3059845323082098	+

Core Functions

Dashboards.

- The solution features intuitive, interactive dashboards designed for ease of use and flexibility
- Users can drill down into specific sites and areas for detailed insights, and configure business intelligence views to meet their specific needs
- Optional integrations with news feeds and popular messaging apps are available upon request

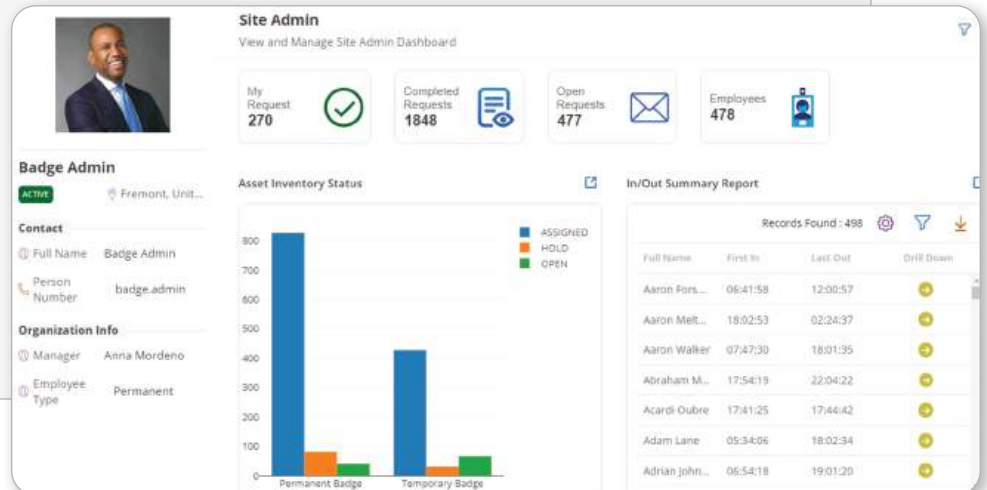
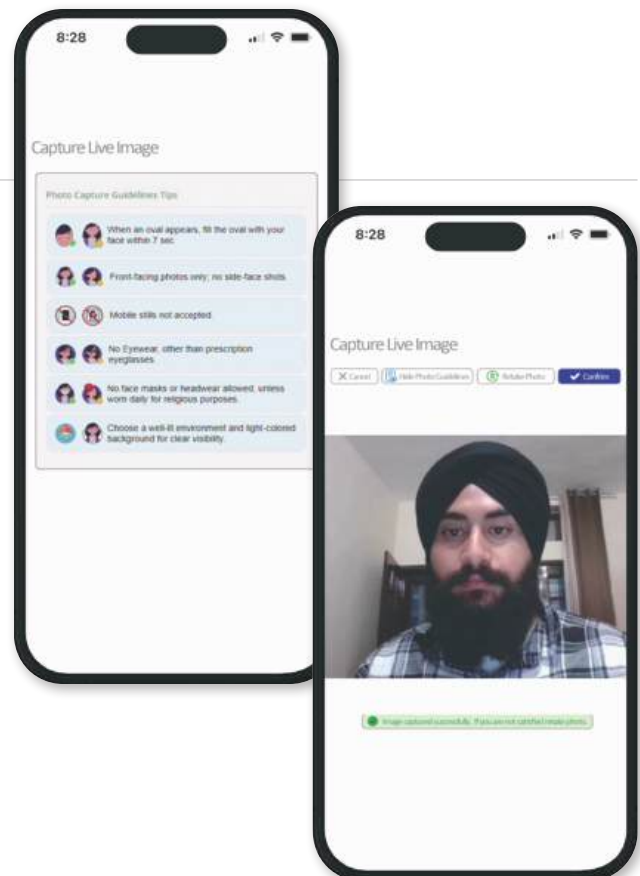


Photo Capturing.

- Live Photo Capturing feature provides facial detection, recognition, and comparison for identity verification against documents or database photos
- Integrated “Liveness” detection ensures that captured individuals are in front of the camera rather than photos or videos
- Ideal for contractor onboarding, automated badge printing, and security screening to prevent imposter fraud and face spoofing

See Our Photo Capture Feature in Action



Guardian Software Engines

Rules Engine.

- Designed to automate and enforce access control policies by applying predefined rules
- Allows organizations to define and manage rules based on specific conditions and attributes, such as user roles, access levels, and time-based restrictions
- Organizations can ensure consistent application of security policies, streamline access requests/approvals, and reduce the risk of human error

Name ↑	Type	Condition	Status
<input type="checkbox"/> Assign / copy Asset in new badge Request	General Rule	iff(AccessRequestRule.requ...	ACTIVE
<input type="checkbox"/> Copy photo for new badge request	General Rule	log_info(" Check in --- "); if(A...	ACTIVE
<input type="checkbox"/> Filter Rule for search only permanent badg...	Filter Rules	SearchCriteria searchCriter...	ACTIVE
<input type="checkbox"/> New Badge	General Rule	{AccessRequestRule.reque...	ACTIVE
<input type="checkbox"/> New Badge Request	General Rule	{AccessRequestRule.reque...	ACTIVE
<input type="checkbox"/> New Badge Request Rule for Active Inactive...	Validation	log_info("AR-613 validation ...	ACTIVE
<input type="checkbox"/> New Badge Request Rule for Active Inactive...	Validation	log_info("AR-613 validation ...	ACTIVE

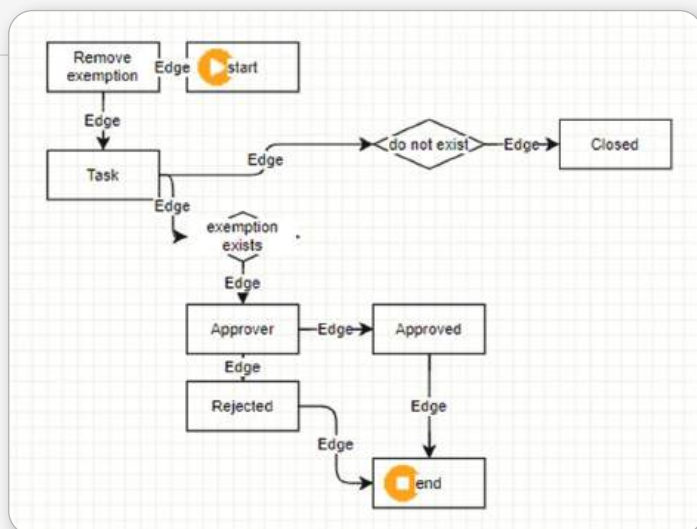
Code	Type	Name	Description	Policy Group	Rule Sets	Status
<input type="checkbox"/> POL-000022	Validation	Preventive ...	Preventive Risk for IT Access	RiskPolicyGrp	Preventive ...	ACTIVE
<input type="checkbox"/> POL-000021	Validation	IT Access S...	IT Access SOD Check	RiskPolicyGrp	IT Access S...	ACTIVE
<input type="checkbox"/> POL-000019	Validation	High Risk Ac...	High Risk Access Level SOD	RiskPolicyGrp	High Risk Ac...	ACTIVE
<input type="checkbox"/> POL-000018	Validation	kiosk badge...	kiosk badge template policy	kiosk_Badg...	VIM_BadgeT...	ACTIVE
<input type="checkbox"/> POL-000017	Validation	Suggest Def...	Suggest Default Policy Group	Suggest Def...	Non-Employ...	ACTIVE
<input type="checkbox"/> POL-000013	Validation	Assign and ...	Assign and Return temp Badge	Suggest Def...	Trigger rule ...	ACTIVE
<input type="checkbox"/> POL-000013	Validation	Compliance ...	Compliance Rules Auto Exem...	Compliance ...	Compliance ...	ACTIVE


Policy Engine..

- Provides a framework for defining, managing, and enforcing security policies across the enterprise
- Enables organizations to establish comprehensive access policies based on user attributes, organizational roles, and regulatory requirements
- Ensures that access decisions are aligned with organizational standards and compliance mandates

Workflow Engine.

- Orchestrates complex workflows for tasks such as access requests, approvals, provisioning, and de-provisioning - ensuring these processes are handled efficiently and in accordance with established policies
- Workflow Designer:
 - User-friendly interface that allows administrators to design and configure workflows with ease
 - Provides a drag-and-drop functionality, enabling users to create, modify, and visualize workflows without the need for extensive programming knowledge





Guardian Personas and Out-of-the-Box Use Cases



Managers.

Role: Managers oversee access permissions and security within their teams, departments, or other areas of responsibility. They use Guardian to monitor and manage access rights and responding promptly to access-related issues.



Visitors.

Role: Visitors require temporary access to facilities for meetings or events. The system facilitates visitor management by issuing temporary access credentials, tracking visitor movements, enhancing security, and ensuring a smooth visitor experience.



Employees.

Role: Employees use the system to request access to physical facilities and IT resources via a Self-Service portal, based on their job roles and responsibilities.



Sponsors.

Role: Sponsors are responsible for endorsing access requests and ensuring they align with business needs and security requirements.



Administrators.

Role: Administrators have overall responsibility for configuring and managing the Guardian system, including setting policies, integration with other systems, defining workflows, and generating reports.



Contractors.

Role: Contractors utilize the system to obtain temporary access to facilities or specific areas within an organization to perform contracted work.



Notifications.

Alert Enterprise VIM automates communications by sending SMS, email, or automated phone calls for visitor and employee check-ins/outs. Upon visitor check-in, their host is instantly notified with the visitor's details through email, SMS, or phone call. Additionally, it can send emergency notifications to specific individuals or to all visitors.

 Google Chat

 Outlook

 slack



Guest Wi-Fi.

Automatically issue WiFi credentials to:

- Visitors
- Intercompany travelers
- Hybrid employees visiting a workspace

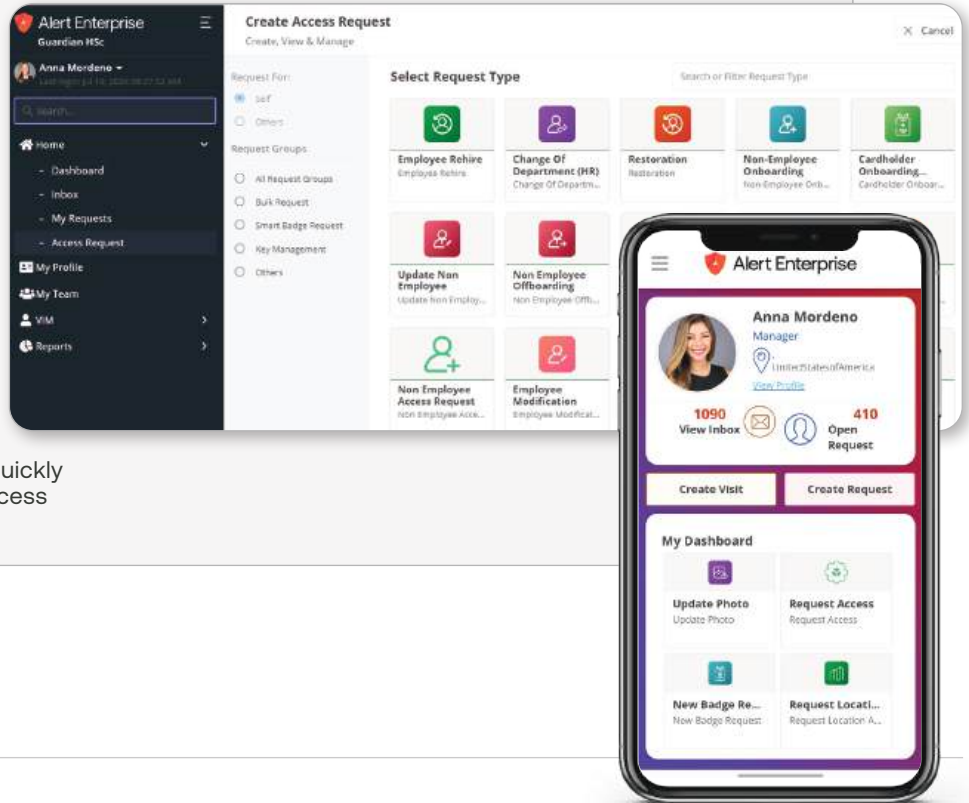
 CISCO

 aruba
NETWORKS

Exceptional Experience. Simplified Administration.

Self-Service Portal.

- Allows users, managers, and area owners to handle their own access needs, reducing the workload on support staff
- Employees have the ability to report lost or stolen badges, reset passwords or PINs, and request access to specific areas
- Area owners or building administrators can manage access to their buildings and conduct access review re-certifications
- System administrators can quickly disable badges or remove access during emergencies



Device Agnostic.

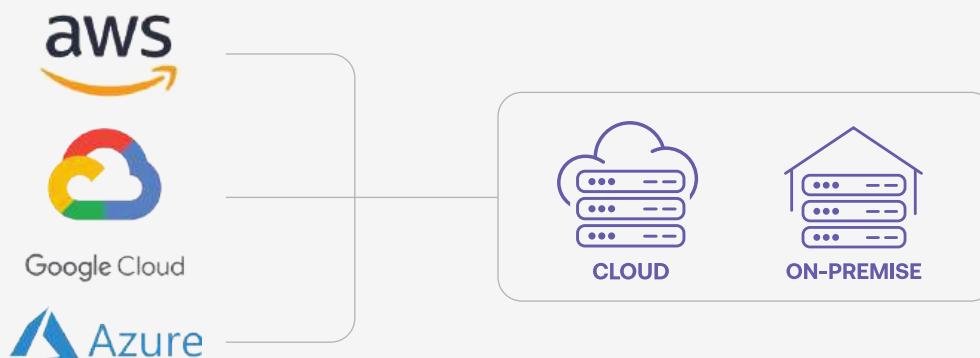
The Guardian solution is designed to be fully device-agnostic, offering seamless functionality across any operating system or hardware without requiring dedicated applications. It operates efficiently within any web browser, leveraging the power of HTML5 and the EXTJS library to deliver a responsive and intuitive user interface. Its mobile-friendly design ensures that users have a smooth and accessible experience on both desktop and mobile devices.



Deployment & Integrations

Cloud Hosting Options

No two customers are the same, our platform hosting is agnostic. You can leverage native SaaS with a global SLA 24/7 hosted in the US or the EU, or self-host in your own cloud with all the leading providers or on-premise. Deploy according to your needs and controls.



SaaS or not, we've got you covered with a global services team for end-to-end delivery from discovery to GoLive - along with a world class support team that provides a 24/7, 365 SLA globally.

Physical Access Control Integrations.

The Guardian PIAM solution integrates with leading Physical Access Control Systems (PACS), offering such capabilities as credential management, access level management, user management, and flexible reconciliation of system-specific attributes.

[See the Full List of Our Integrations](#)



Additional Features

Multilingual.

Front desk or back office, the entire application is multilingual for your workforce and all guest-facing components to cater to even the largest enterprise. All while providing a friendly local experience that reflects your brand.



Custom Messaging & Branding.

We've got all the tools you need to ensure your guests arrive safely, have an exceptional experience and see the extension of your brand reach right on their mobile phone!



Safety, Security and Compliance.

- ID verification
- Enforced escort check-in policies
- NDA management
- Training validation
- Configurable branding and corporate messaging
- Health & Safety policies
- Local watchlist, federal criminal history checks and workflow approvals



[CONTACT US](#) | [LEARN MORE](#)

