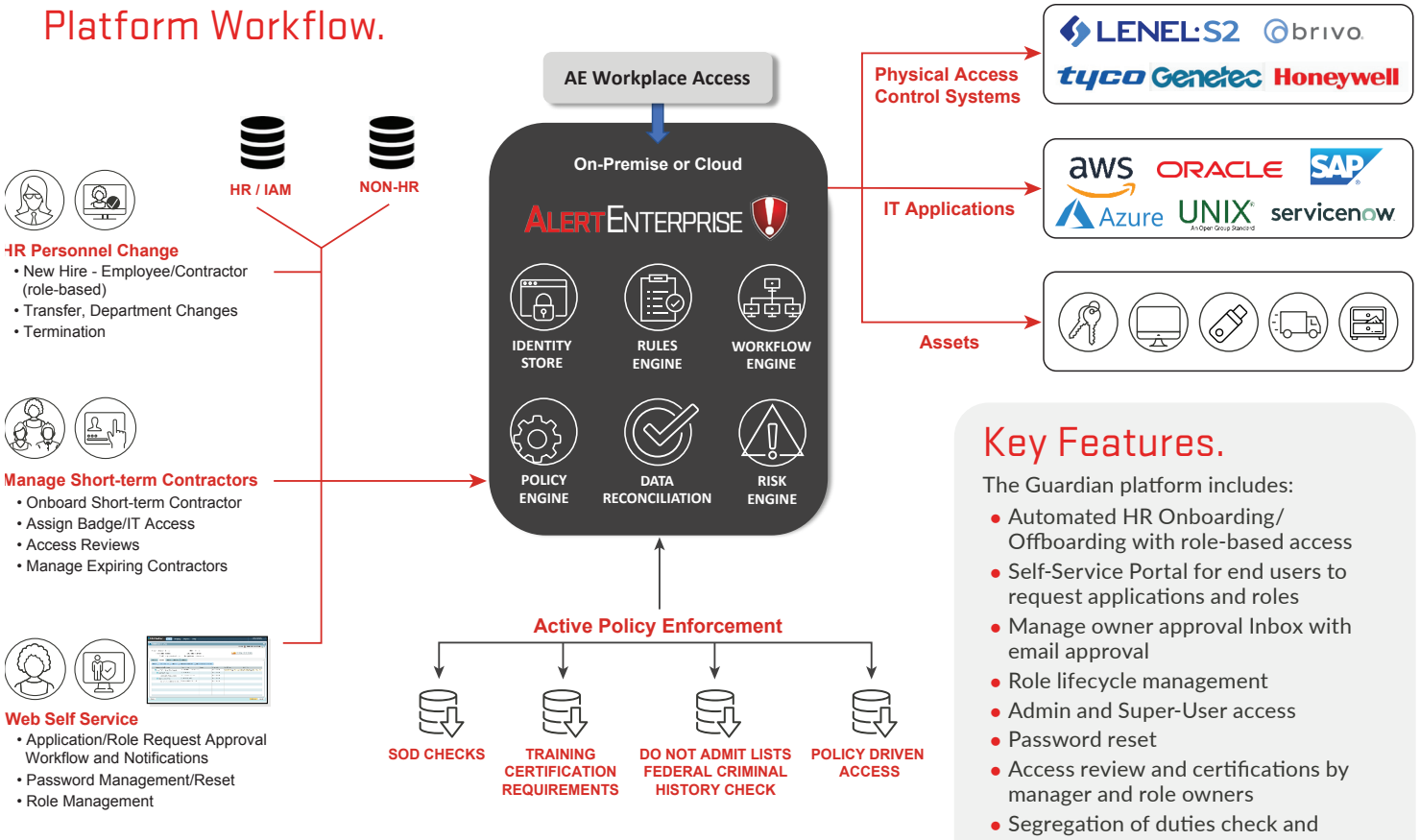
ALERTENTERPRISE | DATASHEET

Guardian IAM.

End-to-End Identity & Access Management Converged Across IT | Physical | OT

Guardian IAM is a highly configurable and scalable Identity and Access Governance platform, which spans across IT, Physical and Operational Technology systems. The platform provides a centralized, unique identity that can be mapped to any type of system, application or asset in an organization.

Platform Workflow.

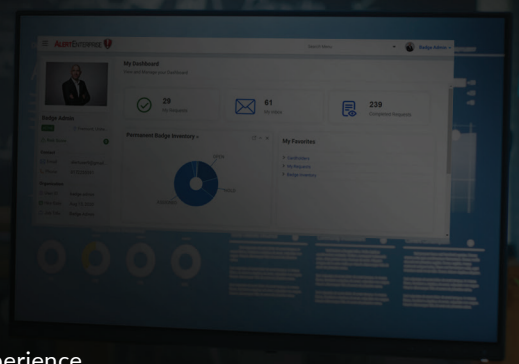


Key Features.

The Guardian platform includes:

- Automated HR Onboarding/ Offboarding with role-based access
- Self-Service Portal for end users to request applications and roles
- Manage owner approval Inbox with email approval
- Role lifecycle management
- Admin and Super-User access
- Password reset
- Access review and certifications by manager and role owners
- Segregation of duties check and mitigation control for conflicting access
- Highly configurable workflow and notification engine for individual applications
- Out-of-the-box connectivity with majority of IT applications vendors

Intuituve Interface.

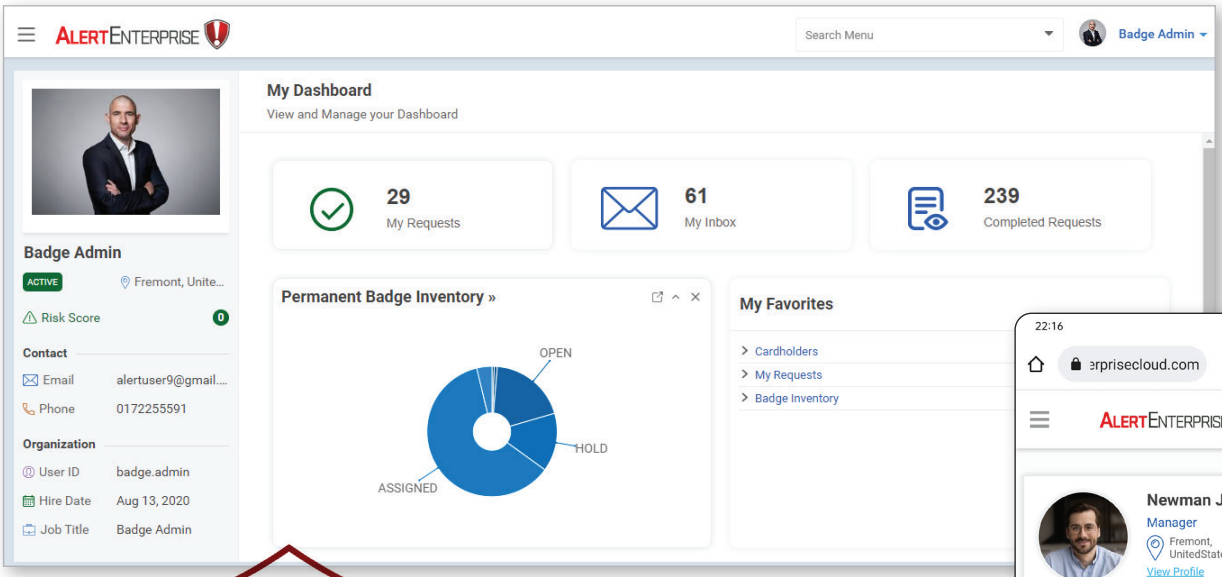


The Guardian solution provides a highly flexible and intuitive user experience, with minimum clicks to navigate and a customizable color scheme.

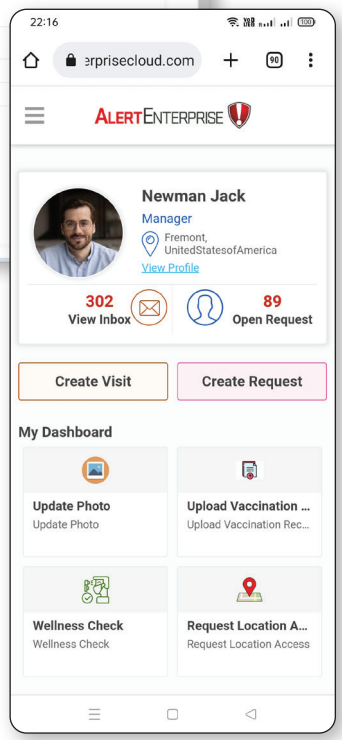
The interface is designed to be used with either a touch screen or standard data-entry, and includes a variety of functions available to the user, based on their individual personas and job duties.

Dashboard View.

When a user signs in, they are presented with a dashboard view that has been configured by your own administrative team, with only the elements and options they are authorized to view.

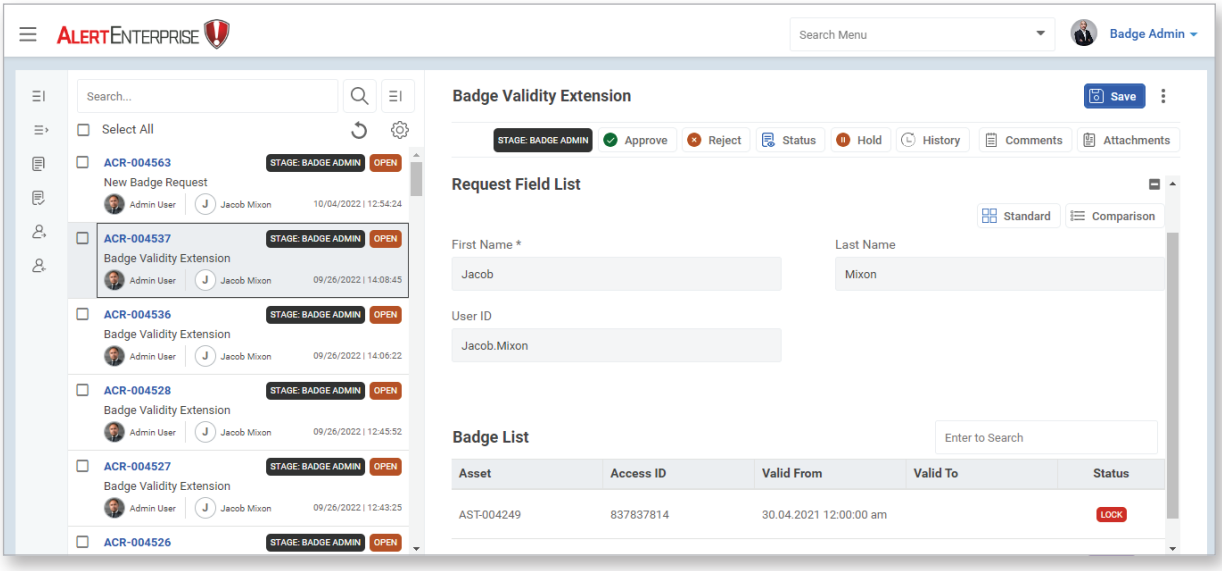


MOBILE >



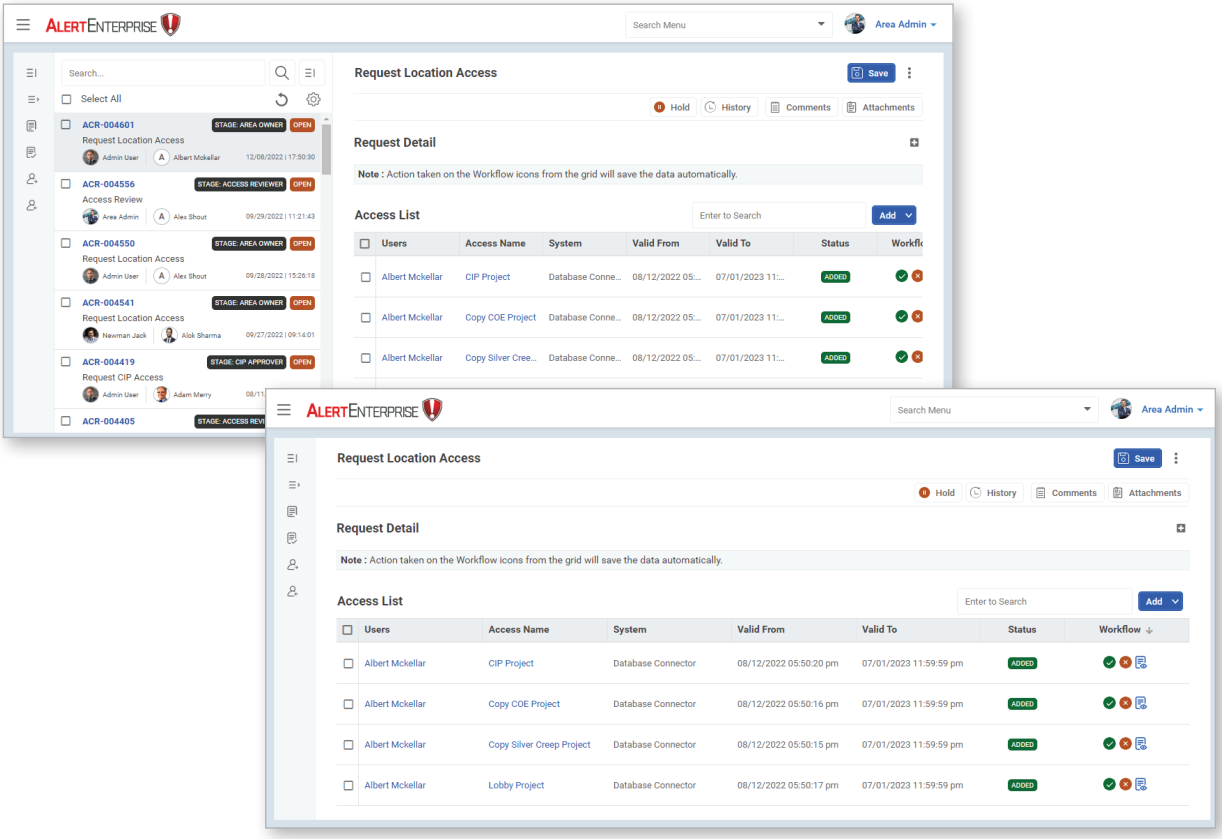
Approver Portal.

The approver portal view offers an easy and seamless way to navigate between new and completed access requests, easily recognize delegated requests, single or mass approval functionality, and single click printing if required.

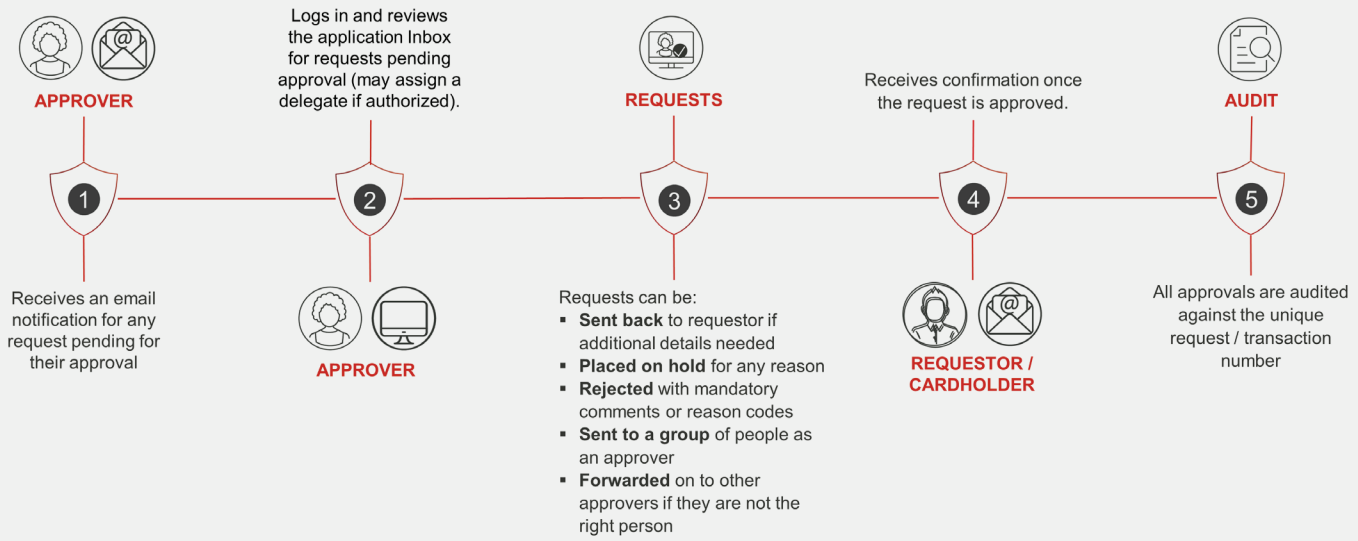


Approver Inbox.

The Guardian web-based inbox allows all approvers to review and approve/deny any request.



Approver Process Workflow.

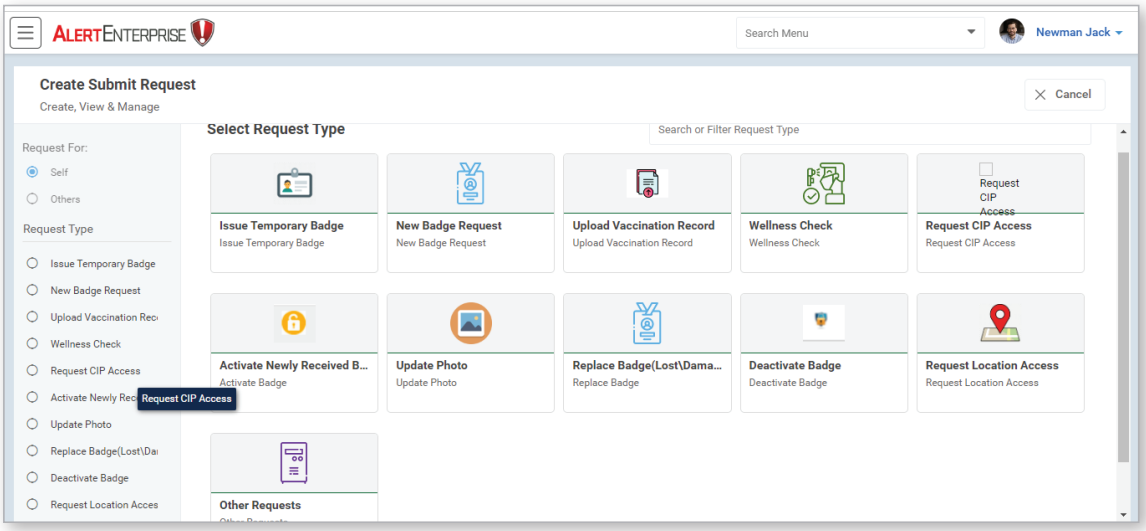


Automated Onboarding and Offboarding.

The Guardian application can be directly integrated with variety of HR systems to automate the onboarding and offboarding process. For onboarding, the application can create a new hire request and add the default position or employment-based roles/access to the request. Once the necessary approvals are completed, the user profile with necessary permissions is created in downstream connected systems, including AD, SAP, Windows, Oracle Apps and Unix, etc.

Guardian also has an ID generator capability designed to generate unique user IDs and passwords for different systems. The approval process can be defined based on the configured workflow for each request type, including:

- Automated New Hire Request
- Automated Termination Request – remove/deactivate access from downstream systems
- Automated Transfer Request - remove the system/roles per the old job position and suggest new roles per the new position



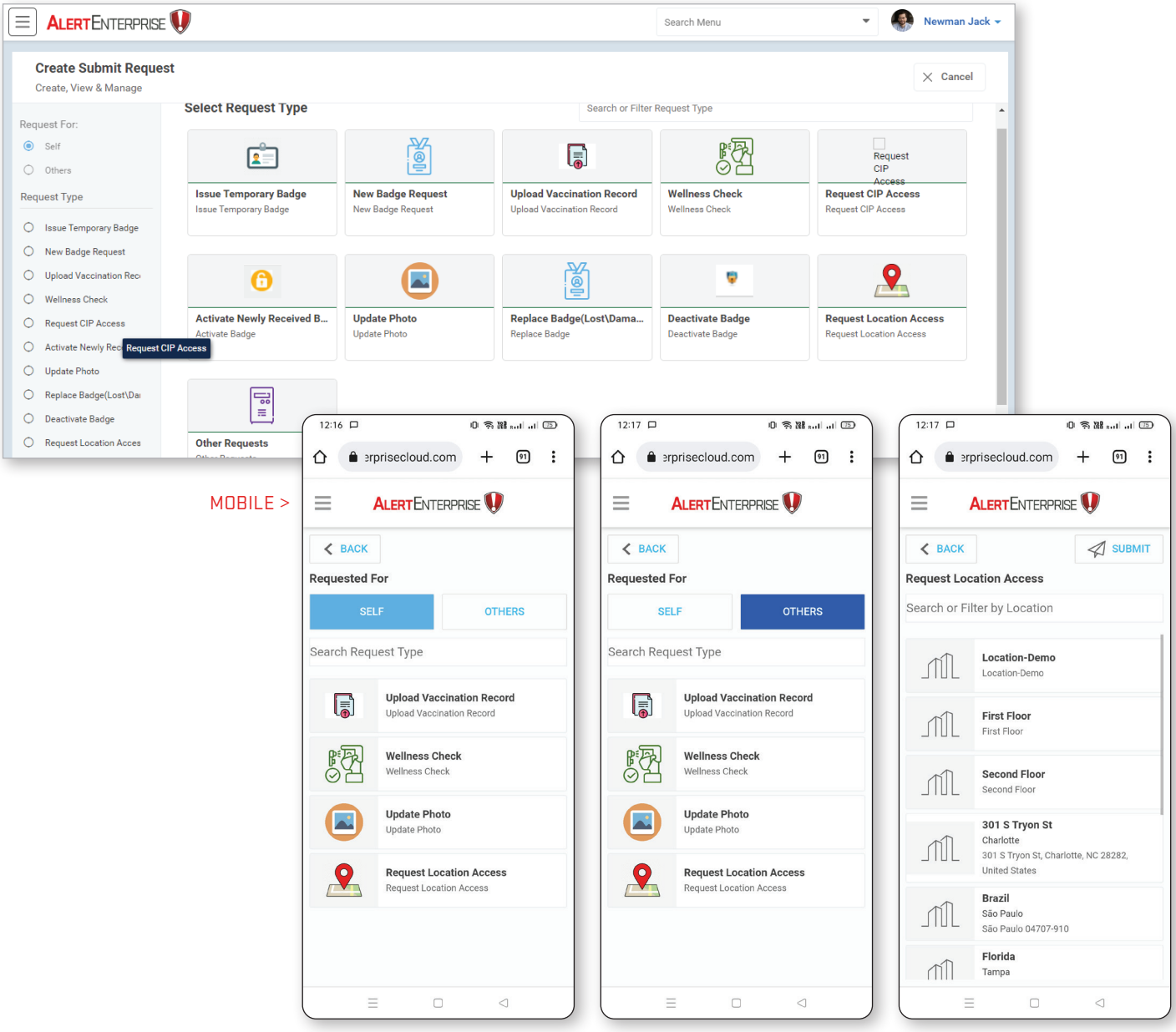
Self-Service Portal.

The self-service portal can be customized to specific processes and renders seamlessly on mobile devices.

Various types of self-service request categories such as “Request for Access” “Request to Change Access” and “Termination” are available for appropriate users, all backed by a configurable workflow approval process. An intelligent business layer enables self-service capabilities to automate access requests, enforce policies, ensure compliance, enable delegated administration, and generate roles-based dashboards and reports.

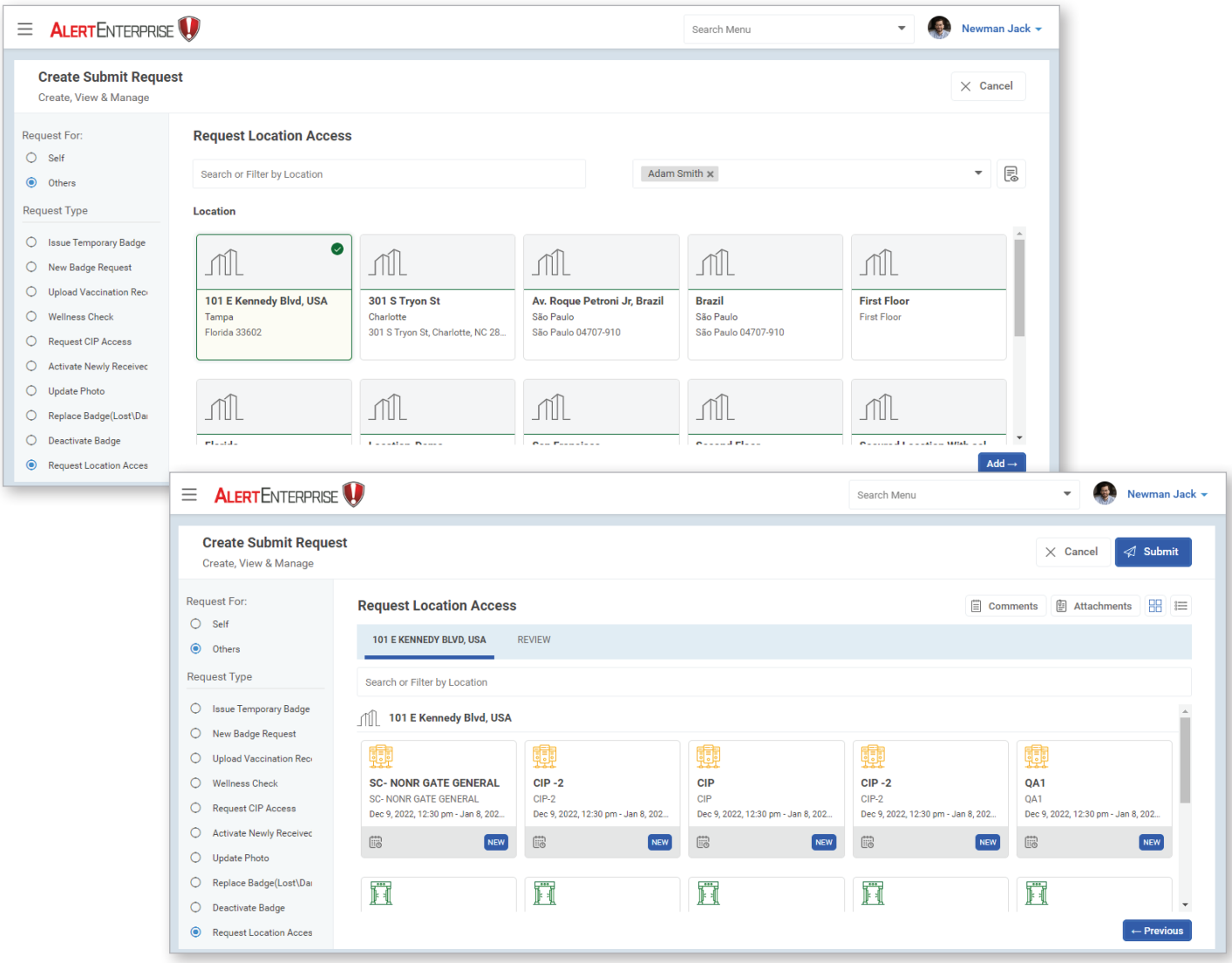
The permission-controlled end-user interface includes seamless integrations with industry-standard SSO and authentication applications. It provides the workforce with the flexibility and control to request additional or special access for themselves, for specific periods of time, by clearly stating the business reasons for needing the access.

The portal also provides the ability for end users to check the status of their individual requests, review their personal information and customize their inbox per their personal preferences and ease of use. The widget-based elements, shortcuts and favorites are configurable by end users to offer a highly personalized experience.



Requesting Access.

In addition to the birthright and role-based access, users can login into the self-service portal and request additional access. Once the access is requested, it goes to an approval process. After the approval is done, the system access and roles would be automatically provisioned to the downstream system.



Birthright Permissions.

Guardian IAM enables organizations to implement role-based and attribute-based access controls that automatically add and remove access rights according to a user's specific attributes or roles. By providing a database of roles determined by location, manager, department, or other variables, IT administrators can easily assign users the proper permissions without any guesswork or room for error.

Provisioning and Deprovisioning.

Guardian provides automated provisioning to downstream systems supplemented by an auto-retry in case of connectivity loss. Once the system access or role is provisioned, necessary notifications are sent as part of request workflow.

Attribute Mapping.

The provisioning engine also comes with configurable attribute mapping which can be used to define which attributes in the downstream systems need to be populated as part of provisioning. This process can be updated anytime as necessary.

Access Review and Certification.

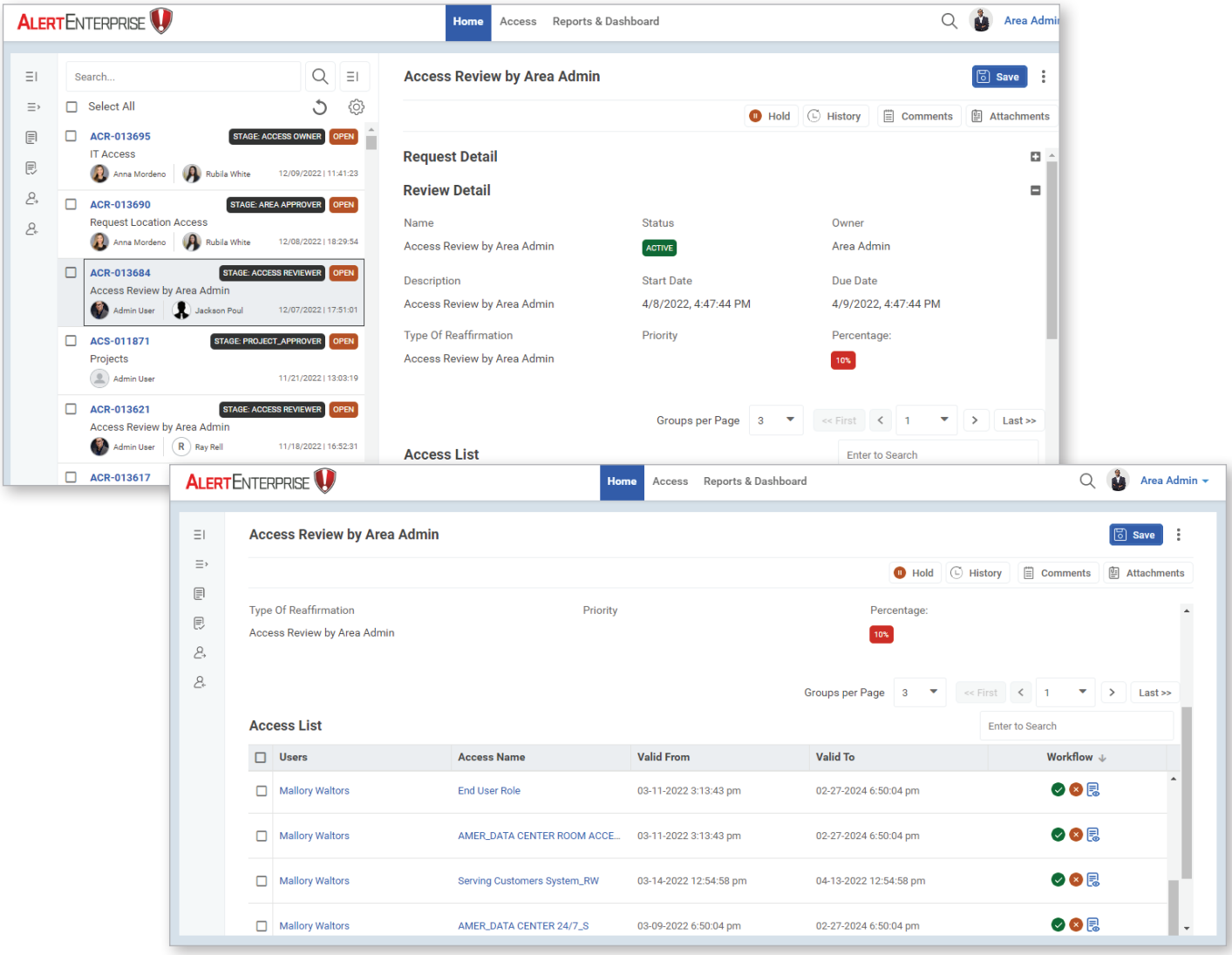
This function is an important Identity and Access Management control activity required for internal and external audits. It helps provide assurance that the appropriate users have access to appropriate systems, and includes:

- Control validations
- Developing and sustaining strategies
- Education and awareness
- Escalation management
- Exception oversight
- Conduct briefings

Guardian provides an IT System Role and Badge Access Review module. The review process can be configured to run automatically after certain intervals for different systems or different types of employees.

Once the review process is set up, role owners or managers will receive a System Role review request in their inbox for the approval. The reviewer must complete the process in a configured period of time. The reminders and escalations can be set as needed.

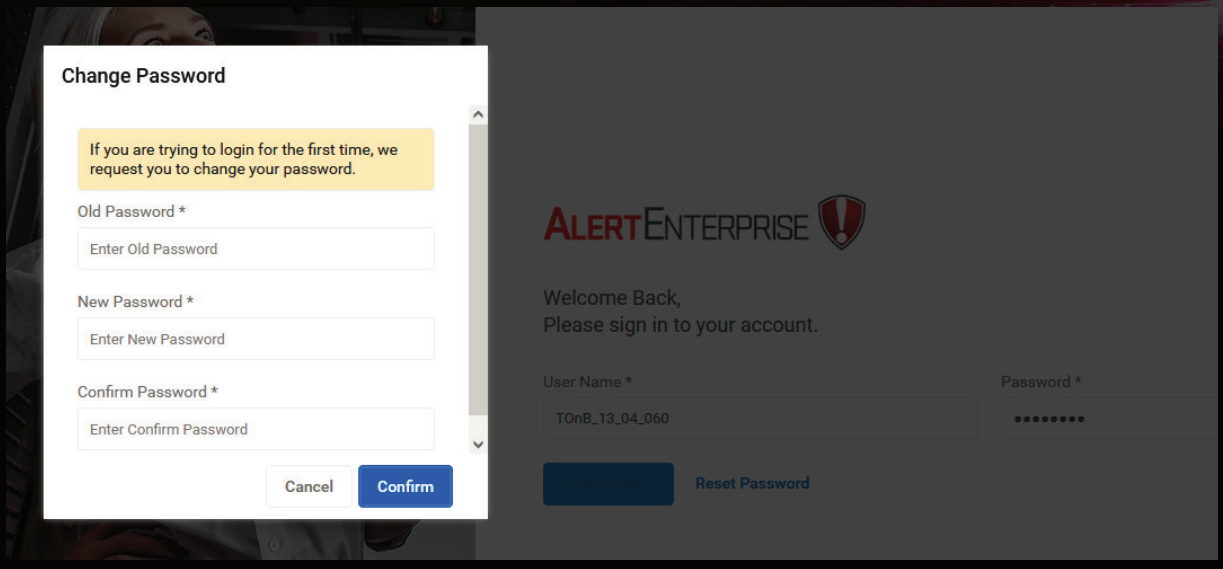
If a role is rejected, Guardian will automatically de-provision the role from the user in any connected systems. All the actions are recorded against the unique transaction number.

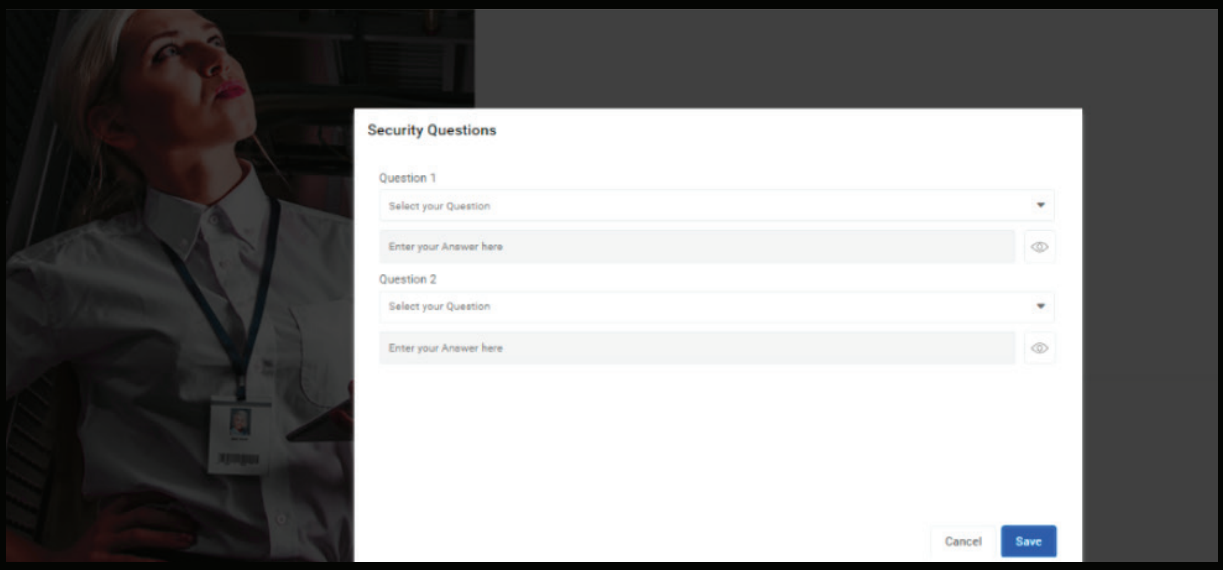


Password Reset Portal.

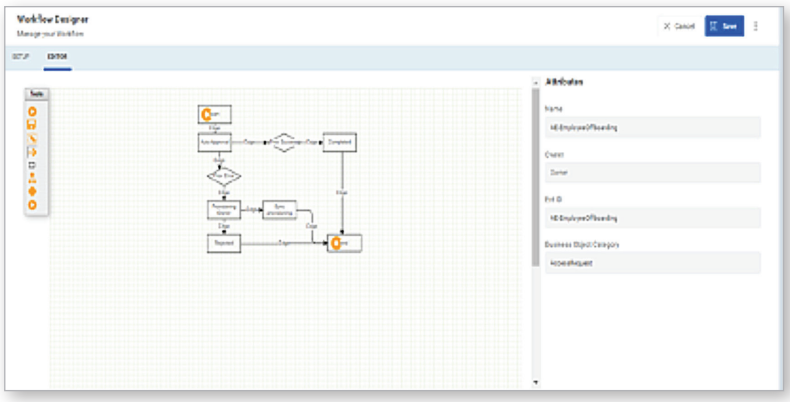
The password management function provides the capabilities to reset cardholder passwords in IT and other systems if they are locked out. The key features include:

- Supports management of passwords, and provides the ability to reset passwords, generate passwords, and set complex password requirements, as well as a Password Help Desk
- New users can:
  - Sign into the system from the login prompt using a “password reset” UI element
  - Enter their identifier and answer a series of personal questions
  - Walk through the enrollment process:
    - Complete a profile of security questions for future use
    - Select an initial password for the user’s AD and any other accounts
    - Sign in with their AD login ID and newly chosen password
- Each password change is audited, and a confirmation is sent to the end users when successful





Dynamic Process Workflow Tool.



The Guardian platform provides an easy-to-use, easily configurable, drag-and-drop workflow generator tool. It enables system administrators to easily define workflows, that emulate corporate processes, without any technical knowledge.

The workflow editor has the ability to incorporate multi-stage approvals, set up email notifications facilitating continuous reminders and escalations, as well as active policy enforcements for vetting services and prerequisite checks.

The Workflow Engine allows for request work items to be configured for sequential or parallel approvals, and includes the following key features:

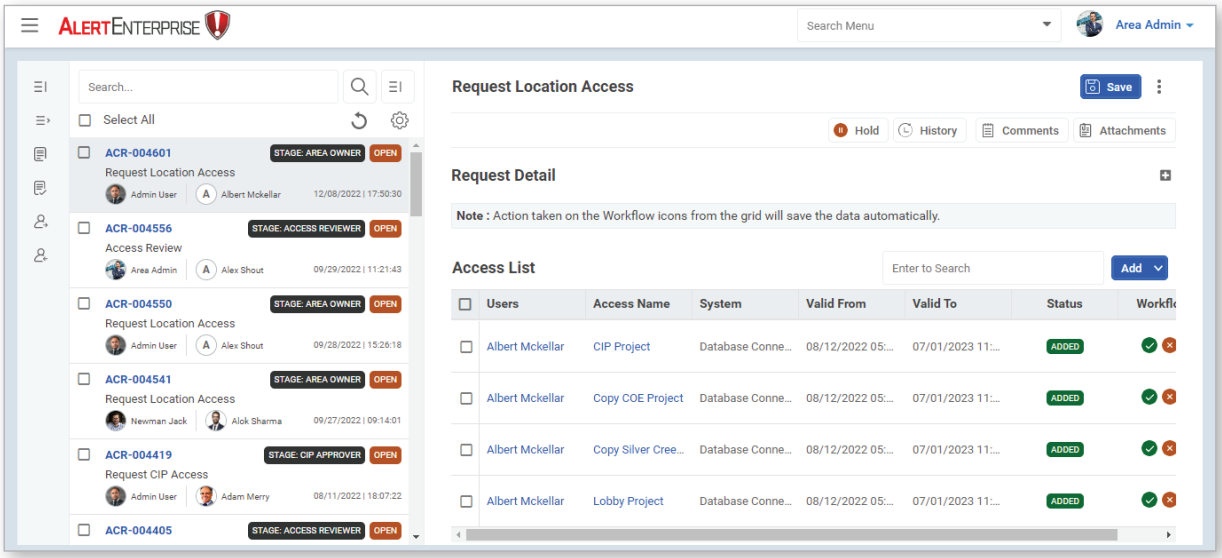
- Drag-and-drop web-based UI Workflow Designer
- Multi-stage approval with sequential or parallel approval
- Attribute-based decision making and approval paths
- Configurable reminders, escalation frequencies and actions
- Escalated requests sent to approver's manager, administrator or other Identities
- Notifications associated with any request submission, approval, reminders, escalation or closure for workflow stage
- Configurable approvers or approver groups based on cardholder attributes and automatic assignment
- Configurable approver UI screen with control over sections/attributes visibility and edit capabilities
- Different workflow can be triggered based on policy rules
- All modifications to the workflow are audited and available in report
- For workflows: setup the workflow priority, copy existing workflows and create new ones, enable/disable workflows
- The application comes with capabilities for single or bulk approvals, along with ability to approve via email

Notifications and Escalation.

After the Organization is mapped, a rule-based engine enables the system administrator to establish a notification and escalation policy, so that if an action is not acted upon, an escalation workflow will be initiated and the action item will be forwarded to the next approver in the workflow.

Workflow notifications are an integral part of workflow design. Approval stages and email notifications can be added as required, through the intuitive and easy to use, GUI based workflow designer tool.

The AlertEnterprise application can generate email, as well as text-based notifications that can be integrated to all the identity and access lifecycle processes (like onboarding, offboarding, additional access requests, revoke requests, termination requests and more) as required.



Additional Guardian IAM Platform Features.

Active Policy Enforcement.

Guardian provides additional configurable capabilities to enforce policies and provide automated controls which helps deliver optimal access governance.

- Segregation of Duties (SOD) controls with validation checks and risk mitigation
- For training and background checks, the system features include:
  - Associating roles with training and background check prerequisites
  - Automated checks at the time of approval if someone's training is expired (if so, stop the request from approval)
  - Automated check with internal/external background check system before critical access assignment
  - Notify users in advance if their training and/or background check is expiring
  - Remove critical access if any of the prerequisite background checks or training are expired
- Managers notification to renew their contractors' badges
- Enforcement of access review and certification by role owners and managers at regular intervals
- Automated escalations to managers if access reviews or approval requests are not being completed on time

Authentication and Authorization.

Guardian provides the capability to connect with the customer's Single Sign On (SSO) server for authentication and authorizations. The key features include:

- Ability to integrate with SSO server using SAML or SAML2 technologies and provide MFA
- Out-of-the-box integration with SSO service providers (Ping, Siteminder, Okta, OAuth, etc.)
- Assignment of user roles/permissions based on the SAML authentication response
- Creation of local user accounts for authentication and authorizations
- Direct integration with active directory/ADFS for authentication and authorization
- Active Directory groups can help directly assign the role/permissions

Reports and Dashboards.

Guardian features a comprehensive report designer to allow the creation of new and customized reports and dashboards. The designer tool is a drag-and-drop type, wizard-based interface that supports the following functionality:

- Drag and Drop based UI to create new reports or charts
- Add multiple reports and charts to a dashboard
- Add static content and external reports or URLs to the reports
- Connectivity to any database in the network to create advanced reports
- Provide single web page for commutative reports listing
- Assign roles/permissions to the reports and dashboard
- Group reports and dashboard in configurable reports categories
- Report data in tabular or chart formats
- Ability to toggle between design and display mode
- Import/Export features to move reports between the environments
- Custom reports that are not impacted with new upgrades

Systems Framework.

The Guardian application includes a highly configurable and scalable system framework.

The solution provides out-of-the-box system connectors that aggregate data and provision to and from over 200+ existing connectors. It connects with a wide variety of systems, including ERP solutions, databases, SCADA systems, IT applications, physical access control systems and others. Key features include:

- UI-based connector configuration and easy maintenance
- Configurable UI based on attribute mapping for each connector system
- Built-in Policy Engine to validate each attribute before processing the cardholder record
- Two-way connection to push or pull data to/from external systems
- Process to define system owners for approval process
- Testing connection functionality to check the connectivity
- Automated reporting once the connectivity is lost with external system
- Out-of-the-box connectivity with all databases and file systems
- Out-of-the box connectors for:
  - All major PACS systems
  - IT systems like AD SAP, Oracle, UNIX, Linux, etc.
  - OT Systems like Siemens, Rockwell, etc.
- JAVA-based APIs available for customers and partners to create their own connectors
- Seamless connectivity once the software is upgraded

Data Reconciliation Engine.

Integration with Enterprise HR systems/Authoritative data sources like Oracle/SAP/AD/LDAP to retrieve and synchronize employee/identity data, to create a consolidated identity store and drive onboarding / offboarding and access management processes is a simple and easy-to-use process using the web based reconciliation engine. The tool helps provide business logic before consuming the received data for identity and access management lifecycle events. Key features include:

- Configurable attribute mapping for each data source/connector
- Workflow based on data processing logic
- Ability to add attributes received from different data sources to an identity profile
- Automatically map master Identity Profile (HR ID), with system specific user ID like PACS UUID
- Provide single-identity view with mapped systems IDs
- Validation checks on received attributes and associated actions
- Auto-populating dependent attributes based on received attributes
- Ability to flag and send notifications for orphan cardholder accounts
- Trigger different workflow requests based on data received and notifications of poor data quality
- Complete audit history for processed and unprocessed records

UI Form and Attributes Designer.

While Guardian comes with more than 200 attributes and UI forms, additional forms and attributes can be easily created.

- Create new attributes (text, label, date, dropdown, multiselect, checkbox, etc.)
- Provide labels and dropdown values with multi-language support
- Map values from the external source
- Regular expression support for attribute-value validation
- Control the visibility and edit capabilities of the attributes
- Create UI forms with configurable layout designer
- Create multiple sections and their sequence on the layout
- Add/remove attributes on layout sections with tab and visibility sequence control
- Control single and multi-attribute column views
- Provide default values to the attributes
- Add HTML text on the UI forms and their layouts
- Map layouts with the request types and approver views

ALERTENTERPRISE

Cyber-physical identity access management for the cloud enterprise.

INFO@ALERTENTERPRISE.COM | ALERTENTERPRISE.COM