AlertEnterprise!

Enterprise Guardian™

Converged Enterprise Identity Governance and Management Suite
Single Solution for IT, Physical Security and Operational Systems

What is the Enterprise Guardian™ Suite and What Are the Benefits to You?

Identity Governance and Management

- Upfront Analysis for Risk and Training prior to Onboarding, Offboarding
- Access Certification and Role Lifecycle Management
- Provisioning to On-Premise, Cloud Applications and Badging Systems

Physical Identity Management

- Common Digital Identity for Logical and Physical Identities with Active Directory Integration
- Single interface to provision across multiple badging systems
- Support for high security standards like PIV-I, PIV-C, FICAM etc.

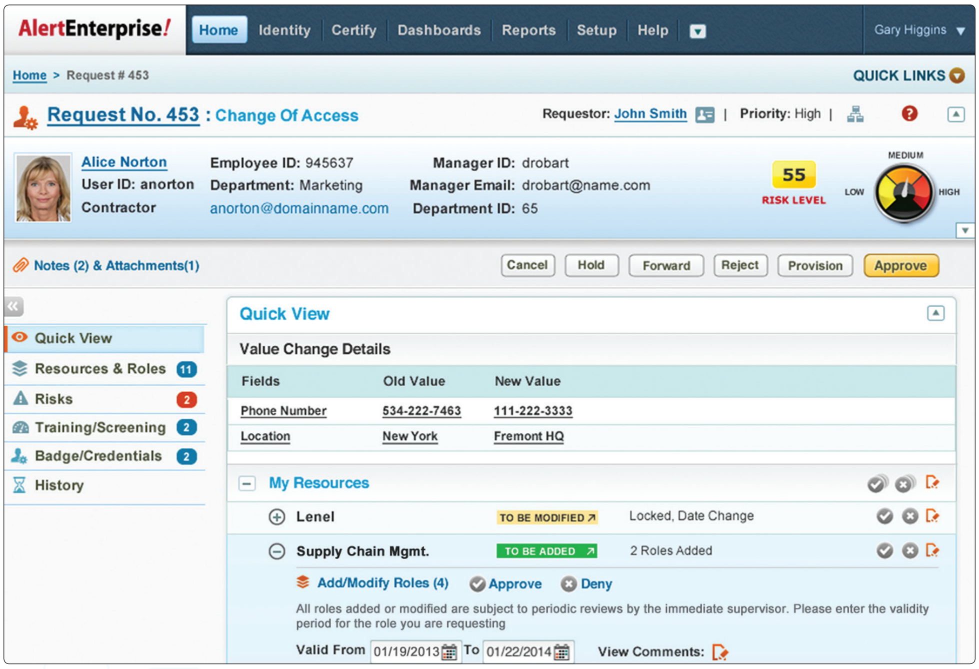
Manage Access to Operating Assets / SCADA Assets

- Monitor and restrict access to key roles for critical plant operating assets
- Integrate events and alerts from SCADA, DCS and Plant Applications into security and operational dashboards

The current approach to handling enterprise security in silos is not working. AlertEnterprise has developed a solution to bridge the security gaps across these silos with a Converged Identity Governance and Management solution that extends beyond IT and enables you to manage and control user access risks across the entire enterprise.

AlertEnterprise delivers a next-generation Identity and Access Management solution that addresses one of the most frequently cited issues with traditional IAM – technical complexity. Traditional IAM was developed a decade ago. Now is the time to consider innovations that are going to last you the next ten years.

Cloud delivery and mobile support enhance Identity and Risk Analytics, Delegated Administration, Self-Service capabilities, Role Lifecycle Management and Access Certification. AlertEnterprise provides an intelligent business layer managing end-to-end identity lifecycles while hiding the complexity of integration across multiple enterprise applications, legacy systems, badge access control systems and access to operational systems like SCADA Industrial Control for plant operations.



Home > Request # 453

Request No. 453 : Change Of Access

Requestor: John Smith | Priority: High |

Alice Norton
User ID: anorton
Contractor

Employee ID: 945637
Department: Marketing
anorton@domainname.com

Manager ID: drobart
Manager Email: drobart@name.com
Department ID: 65

55
RISK LEVEL

Notes (2) & Attachments(1)

Quick View

Value Change Details

Fields	Old Value	New Value
Phone Number	534-222-7463	111-222-3333
Location	New York	Fremont HQ

My Resources

Lenel	TO BE MODIFIED	Locked, Date Change
Supply Chain Mgmt.	TO BE ADDED	2 Roles Added

Add/Modify Roles (4) Approve Deny

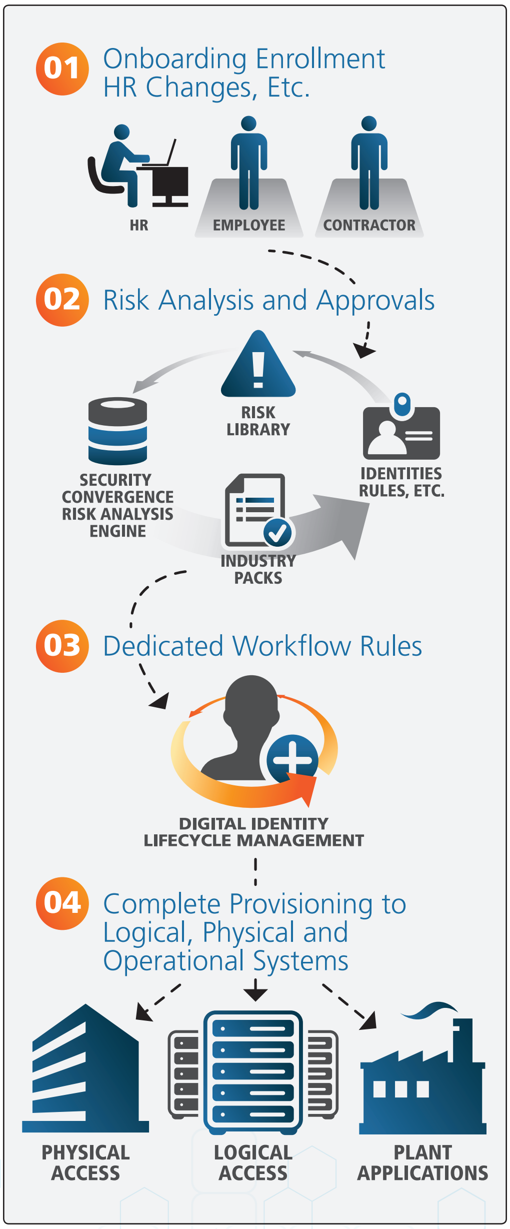
All roles added or modified are subject to periodic reviews by the immediate supervisor. Please enter the validity period for the role you are requesting

Valid From 01/19/2013 To 01/22/2014 View Comments:

Enterprise Guardian™ from AlertEnterprise® automates the upfront risk analysis allowing business managers to gauge risk and make decisions about how much access to grant certain individuals based on their roles. Active Policy Enforcement makes sure that adequate controls are in place prior to granting access across IT applications, physical facility access as well as access to operational plant systems

Enterprise Guardian

- Unified Access Request process across IT, Physical and Operational Systems (e.g. Plant, SCADA)
- Automated Access Certification and Validation
- Role Lifecycle Management
- Federation, Single Sign-On and Password Management
- Converged Identity Warehouse
- Built-in Risk Management and Policy Enforcement
- Role-specific Dashboards and Reporting


01 Onboarding Enrollment HR Changes, Etc.
HR
EMPLOYEE
CONTRACTOR
02 Risk Analysis and Approvals
RISK LIBRARY
SECURITY CONVERGENCE RISK ANALYSIS ENGINE
IDENTITIES RULES, ETC.
INDUSTRY PACKS
03 Dedicated Workflow Rules
DIGITAL IDENTITY LIFECYCLE MANAGEMENT
04 Complete Provisioning to Logical, Physical and Operational Systems
PHYSICAL ACCESS
LOGICAL ACCESS
PLANT APPLICATIONS

Identity Management Challenges

Companies are faced with the daunting task of how to effectively and efficiently manage user identities, roles, and access across their extended enterprise. To accomplish this, an identity and access management strategy needs to be aligned across multiple disparate systems and functions, and deliver automated capabilities for user enrollment, provisioning, and complete life-cycle management.

Companies continue to struggle with implementing a single identity and access management solution across their entire enterprise. Each user within an organization has multiple roles and identities, including identities to access physical locations, logical systems, and even specific roles to access individual functions within key systems and applications. Companies have not had a way to effectively govern and manage identity and access risk across these disparate systems, and have been forced to implement multiple point solutions that are ineffective, inefficient, and costly.

IT Is A Good Place To Start

Using a monolithic approach for Identity and Access Management to automate everything in its path has led to many solutions that are not well-suited to the enterprise. Identity and Access Intelligence capabilities enable a Business Layer that hides the complexity of integrating across multiple enterprise applications and delivers enhanced Business and IT alignment. Onboarding - Offboarding processes are simplified when access requests for multiple systems as well as IT and non-IT assets can be compared in single view.

AlertEnterprise delivers a complete Identity and Access Management Suite that extends beyond IT to include Physical Access in a layered approach that features core operational IAM, Governance and Compliance, and an easy to use self-service Business Layer with performance and risk analytics.

Benefits

- Business, IT and Operations alignment
- Standardization across geographically dispersed systems
- Active Policy Enforcement for corporate and regulatory compliance

ACTIVE POLICY ENFORCEMENT IN ACTION

Tom, an Operator works in the Transmission Control Room for a regulated Utility company we call Utilco. Tom must complete certain on-going training requirements to maintain his license to operate. Utilco has a Learning Management System (LMS) in place that is linked to the company HR system.

AlertEnterprise is integrated with the HR systems, the Identity Management as well as the Badge Access system. During the onboarding process, AlertEnterprise automates the background check process prescribed by Utilco and proceeds to make sure that all the certification requirements are met. If the requisite Continuing Education is not completed, the application reminds Tom that he has two more weeks to complete it. Tom may want to access the computer-based training in the evenings to make up for lost time.

If additional reminders don't have the desired effect, finally on the last day, when Tom uses his electronic access badge to get into the control room, it will automatically lock him out, enforcing the company policy and avoiding the possibility of costly compliance violations.

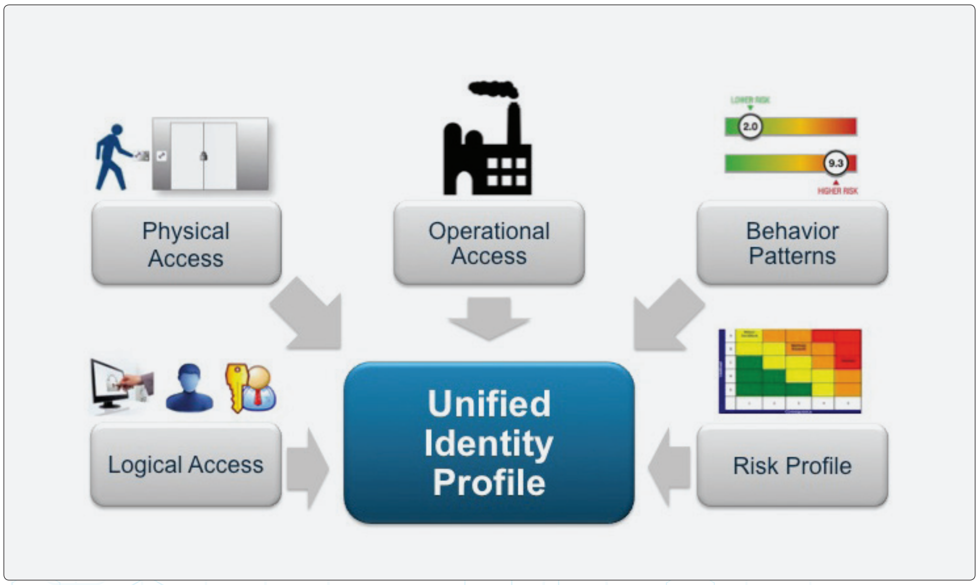
Physical Identity Management

Companies are faced with the daunting task of reconciling employee, contractor and visitor lists against HR Management Systems, Manual Contractor acquisition processes and the list of electronic access cards that are actually active. Add to that the complexity of monitoring the system access that they have in enterprise and legacy applications.

Organizations are living with the risk that terminated employees or contractors still have physical access to facilities. As companies grow and acquire other facilities and merge with other companies, Access Control systems from multiple vendors need to be accounted for. A single command and control console that can consolidate identities and access rules across multi-vendor badging systems can eliminate the overlap, cost burden and manual processes needed to centrally manage physical access across all these systems without resorting to cost prohibitive replacement of systems that are working fine.

Enterprise Guardian Physical

- Manage a Common Digital Identity for employees, contractors, visitors etc.
- Actively enforce termination and transfers
- Built in badging solution with provisioning across leading Access Control vendors
- Single interface to create identity and badge for multiple Access Control Systems
- Enhanced risk analysis and Training validation with Active Policy Enforcement
- Powerful, easy to use reporting across physical access vendors consolidating access and usage
- Available support for PIV-I and PIV-C for Government and High Security Applications including FICAM, HSPD-12 and OMB M-11-11 support

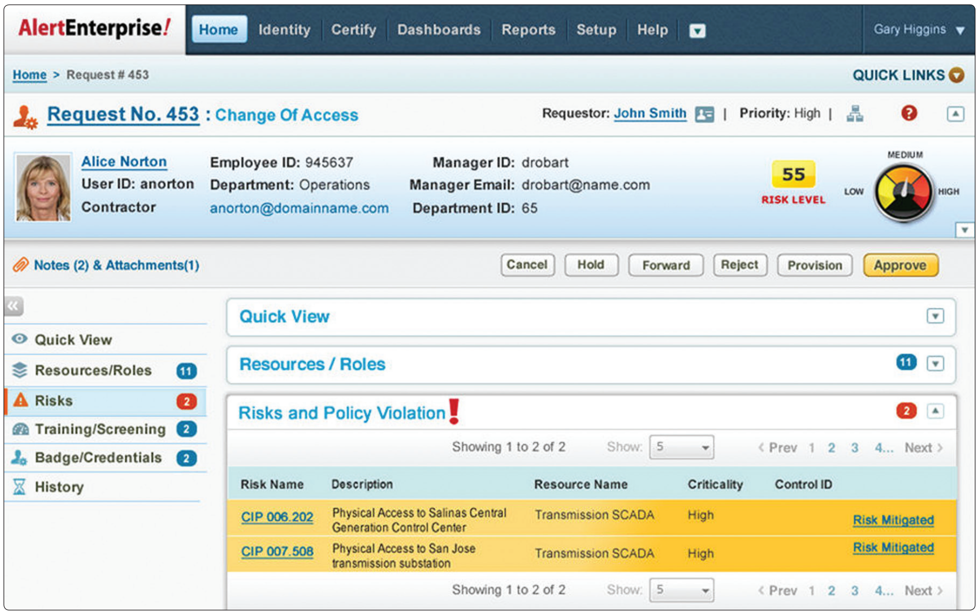


A Unified Identity Profile maps attributes related to roles, identities, logical access, physical access, access to operational systems and maintains a real-time risk profile that includes behavior patterns. Enterprise Guardian delivers a powerful business layer with Identity and Risk Analytics across multiple IT enterprise applications and extends the onboarding / offboarding capabilities to include physical access to facilities and critical assets.

Access to Operational Systems and Critical Assets

Companies that own or operate critical infrastructure need to comply with standards and regulations like NERC CIP, CFATS, PHMSA, MTSA, NEI 08-09, 10CFR 73.54 (for Nuclear). There are various requirements to monitor and report on individuals who have access to IT Systems, Physical Facilities, and where appropriate, the Critical Operating Assets and associated industrial control systems (e.g. SCADA, HMI, DCS etc.).

To get the most comprehensive and informed view of risk in these environments it is important to monitor the situational context in which events and activities are taking place. AlertEnterprise can monitor and control who is accessing what information, zone and equipment, with what authorization and privileges, under what circumstances and with what impact on systems and end-points in real-time is fundamental to securing the organization and the reliability of its operations.



Home > Request # 453

Request No. 453 : Change Of Access

Requestor: John Smith | Priority: High |

Alice Norton
User ID: anorton
Contractor

Employee ID: 945637
Department: Operations
anorton@domainname.com

Manager ID: drobart
Manager Email: drobart@name.com
Department ID: 65

55 RISK LEVEL

Notes (2) & Attachments(1)

Quick View

Resources / Roles 11

Risks and Policy Violation! 2

Showing 1 to 2 of 2 Show: 5 ‹ Prev 1 2 3 4... Next ›

Risk Name	Description	Resource Name	Criticality	Control ID
CIP 006.202	Physical Access to Salinas Central Generation Control Center	Transmission SCADA	High	Risk Mitigated
CIP 007.508	Physical Access to San Jose transmission substation	Transmission SCADA	High	Risk Mitigated

Showing 1 to 2 of 2 Show: 5 ‹ Prev 1 2 3 4... Next ›

Enterprise Guardian delivers the most unique and comprehensive identity management platform that evaluates risk to the organization based on the type of access granted and the potential impact it could have. In the example above the employee continues to have access to both Generation and Transmission Management Systems following a transfer – a policy violation.

About AlertEnterprise

AlertEnterprise delivers Security Convergence solutions for corporate and critical infrastructure protection. AlertEnterprise software enables rules-based correlation of complex threats across the domains of IT Security, Physical Security and Industrial Control Systems for contextual understanding of security events and timely, informed action. AlertEnterprise consolidates Identity and Access Management functions for true prevention of theft, fraud, sabotage and acts of terrorism.

AWARDS/RECOGNITION

SAP Pinnacle Awards 2013 Winner

Security Products' GOVIES 2013 Government Security Awards

ASIS 12 accolades Security's Best Winner

Security Products Magazine 2012 New Product of the Year

2012 Winner GSN: Government Security News Homeland Security Awards www.alertenterprise.com

AlertEnterprise!
4350 Starboard Drive,
Fremont, CA 94538
P: 510.440.0840
F: 510.440.0841
info@alertenterprise.com