

INTRODUCING...

Policy Based Access Control

For unique security, compliance and reporting requirements.



What is it?

Together, BioConnect and Alert Enterprise provide real-time policy-driven access control. A trusted security convergence platform that connects with existing access control systems and reader technologies to provide complete governance and intelligence for building access.

Who needs it?

Designed to meet the unique security, compliance and reporting requirements of highly regulated industries such as Critical Infrastructure (Energy, Transportation), Finance, Data Centers, Healthcare and others. Whether it is requiring biometric authentication to protect PII within a data center, dual authentication to authorize access within the electronic security perimeter of a hydro-electric facility or ensuring employees entering airside operations are current on their required training, Policy Based Access Control helps ensure compliance with a myriad of regulatory bodies.



The Need for Policy Based Access Control

As the threat landscape continues to evolve and grow, it is imperative for businesses to stay ahead with an adaptive and effective authentication mechanism and real-time policy interventions to protect their assets and people and (avoid fines for non-compliance). The requirements to comply with various privacy/regulatory standards and a hybrid workforce environment add a level of complexity. Additionally, disparate silos of identity sources lead to human errors, outdated information, and security vulnerabilities.



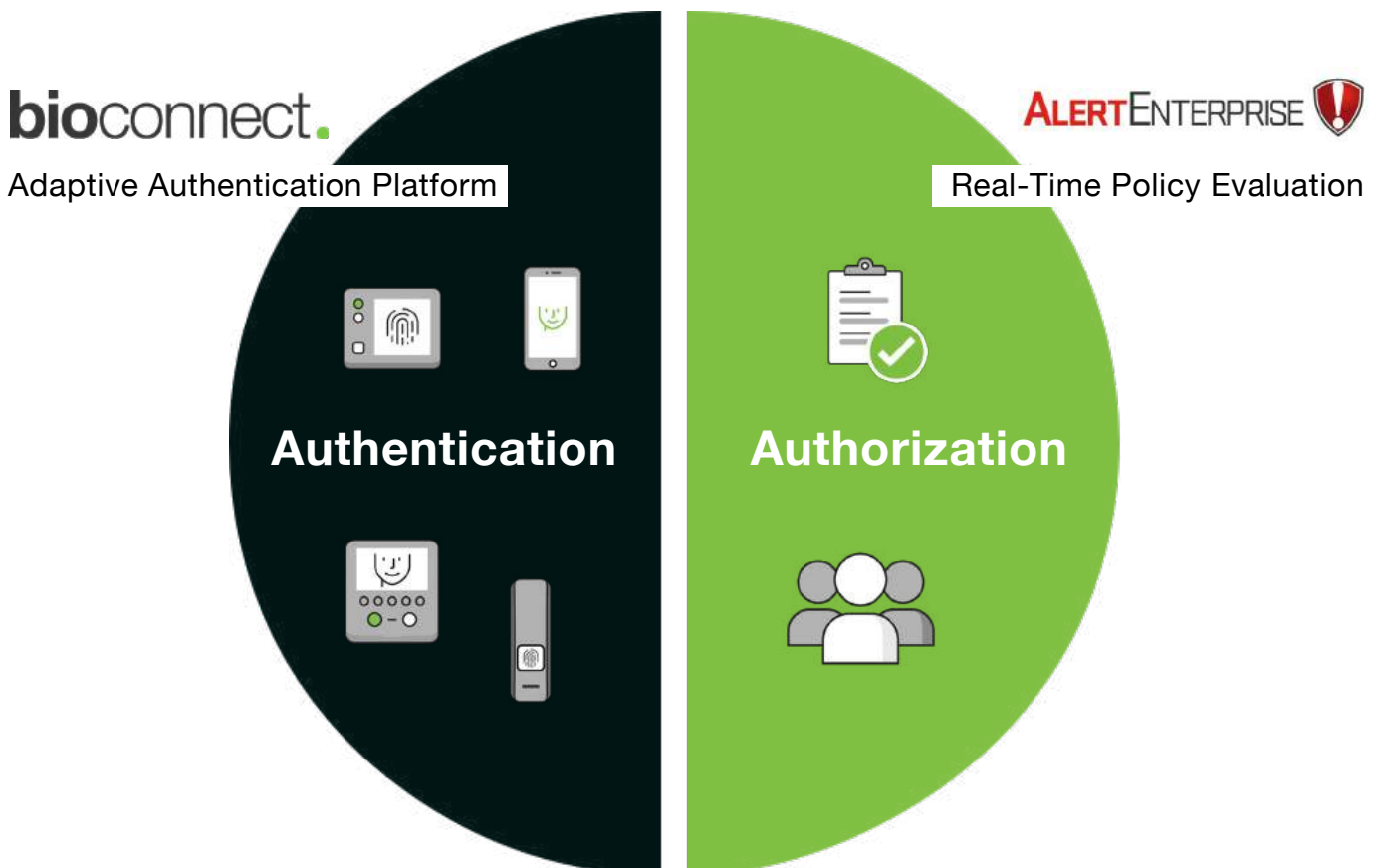
Our Solution

AlertEnterprise & BioConnect's Policy Based Access Control solves these problems at two levels:

1. By using a secure, adaptive authentication platform that reliably ensures and authenticates the identity of the person intending to enter
2. By using an effective authorization policy engine that ensures the individual seeking access has the right credentials and has fulfilled the requirements for gaining access

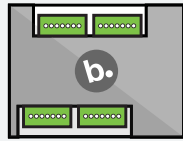
BioConnect's adaptive authentication Trust platform provides a sophisticated authentication layer that works in tandem with AlertEnterprise's governance policy engine. Together, the solution provides real-time policy enforcement by collating data from disparate identity sources such as Active Directory, HR and Training systems, at the point and time of badge swipe.

Holistic Security Approach



Solution Components

Policy Based Access Control is a simple, adaptive solution that works with your existing infrastructure to offer enhanced, enterprise grade security that is scalable, reliable, and cost-effective. To achieve this, it uses a combination of Hardware & Software components.



Link Device

An intelligent device designed to facilitate secure physical access



Link Console

Web console to manage users, rules, access events and to facilitate ACM sync.



Policy Engine

Policy based access control engine by Alert Enterprise

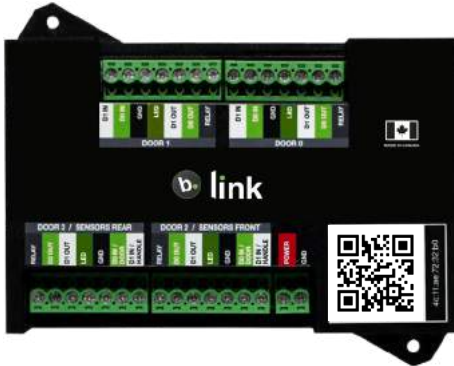


Mobile Authenticator

A mobile application to receive push notifications for user authentication.

Type	Component Name	Details
Hardware	BioConnect Link Mobile	A secure and intelligent device designed to assist in secure physical access. This IOT device supports both online as well as offline modes of operation and works with both Weigand and OSDP protocols.
Software	BioConnect Link Console	A centralized web interface to configure the solution, authentication modes, manage users, devices, scheduling, and other functionalities.
	AlertEnterprise Policy Engine	A configurable centralized Identity Store and policy engine that can be used to set up real-time policy requirements for granting access to physical spaces based on Cardholder and associated attributes, Training, Risk Profile, schedule, and Door/Building type
	Mobile Authenticator App	The BioConnect Mobile authenticator is a mobile application that manages the end-users biometric enrollment as well as authentication. It receives step-up notifications whenever it is triggered as part of an access event or policy evaluation. It supports other forms of authentication modes, including non-native biometrics, survey based authentication, mobile credential, as well as 3rd party MFA such as Duo, Okta, PingID.

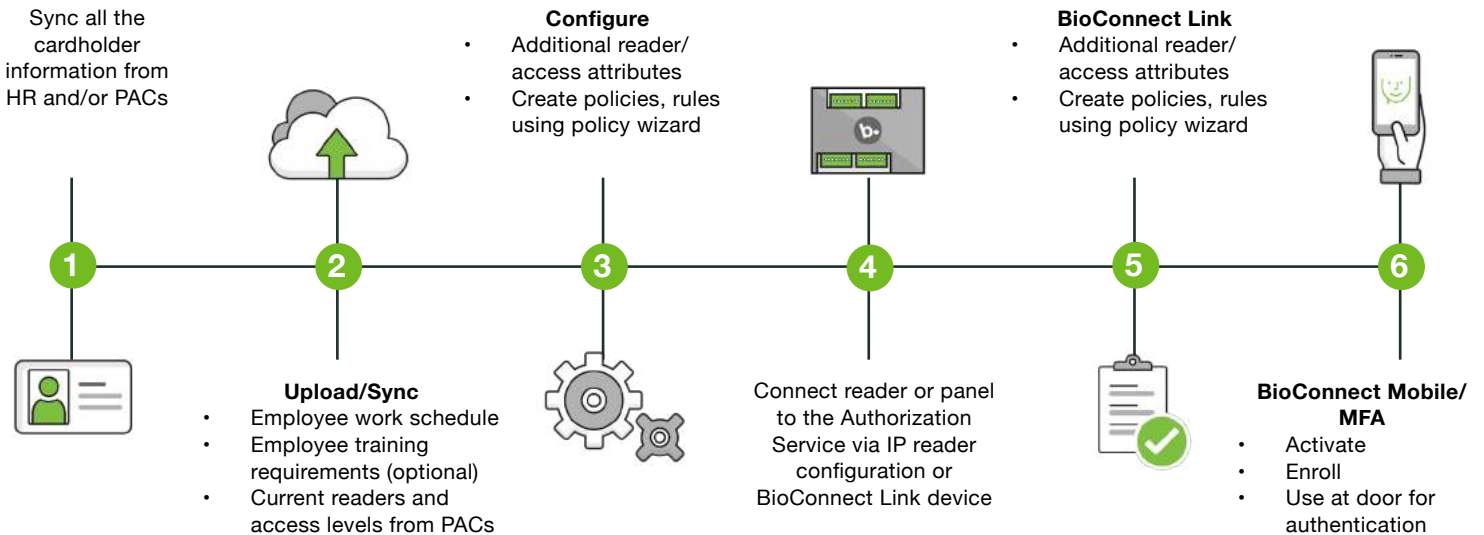
Link Device



Processor	Xtensa LX6 dual-core 240MHz with Secure Boot ATmega168 16MHz
Dynamic Memory	500KB SRAM
Long-Term Storage	4MB hardware-encrypted flash storage (FIPS-197 compliant)
Network Connectivity	10Base-T / 100Base-TX 802.11B/G/N, WPA/WPA2 Secure 2.4GHz Wireless Mesh (optional) Bluetooth 4.2 BR/EDR/BLE
Input Voltage	+12 V DC / PoE (+44VDC)
Wiegand Interface	4 pairs: Wiegand In/Out + LED control
Relays	4 pairs: 12-30VDC (dry), 2.5A inductive, 5A resistive
Operating Temperature	-40°C (-40°F) to +125°C (+257°F)
Dimensions	86.4mm X 132.9mm X 24.7 mm































Policy Based Access Control Workflow


The Below diagram represents the simple 6 steps process to enable policies/rules, that can be set up in a matter of a few weeks.





Out Of The Box Policy Rules


Below are the list of out of the box policies available to use. Any policy rule can be changed enabled/disabled as required. Additional rules can be created based on the customer requirements.

Overriding Door Authorization Policy	Employee	Contractor	Vendor/Temp
Unapproved Cardholder Rule			
Critical Doors Access Rule	 	 	 
General Doors Access Rule		 	 
Expired/Un-Vaccinated All Doors Rule			
Expired Training at Critical Doors Rule			
High Risk Cardholder at Critical Doors Rule			
High Risk Cardholder at General Door Rule			
Temp Badge Issued More Than 24 Hours at Critical Door Rule			
Critical Door Used by Conflicting Business Unit's Identity Rule			

 Access Denied

 Enable 2FA

 Shift Hours

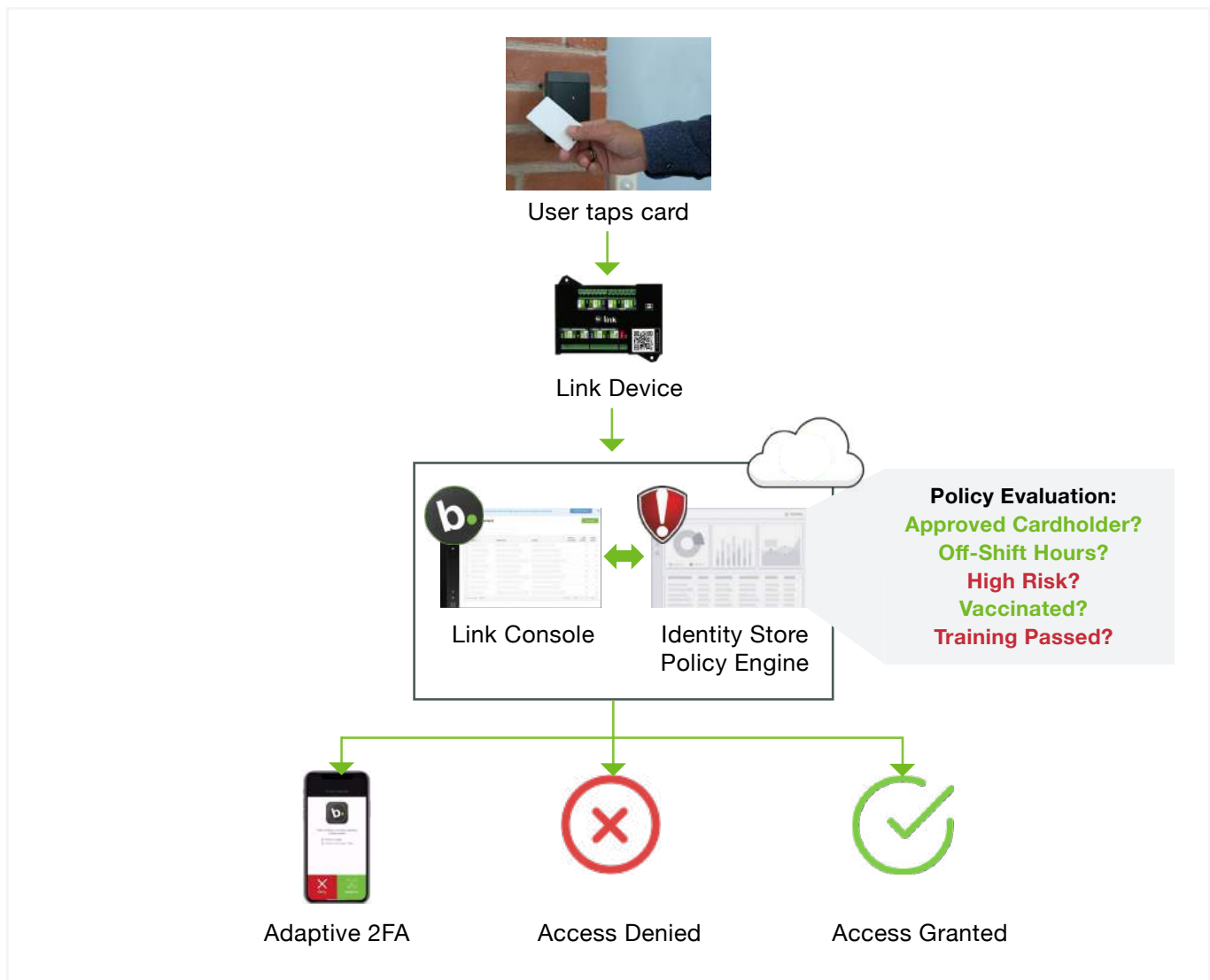
 Off-Shift Hours

Example: Vendor/Temp Worker experience as per above defined policies: The access is denied under the following policies:

1. When they are not in approved identity list managed by the Policy Engine (Someone directly added a Cardholder in PACS system)
2. When accessing critical door during off-shift hours, enable MFA during shift hours
3. Enable MFA when accessing general door after shift hours
4. When the records indicate that they have not been vaccinated or display any infectious symptoms
5. When the records indicate that they have not completed requisite training, or their training has expired
6. When they are deemed as high-risk such as someone on a notice period or terminated or found on a watchlist. [The Definition of 'High Risk' is variable and can be dependent on various configurable factors like - how the Access is being used, Too Many failed attempts, Off-shift hours access, Termination is due in the next 2 weeks, Person found in Federal criminal history, etc.]
7. When their assigned temporary badge is active beyond an allowed business policy limit
8. When the door they are trying to access is marked for a specific business unit and identity (Cardholder) belongs to a conflicting business unit. (Segregation of Duties check)

Example of a User Workflow with Policy Based Access Control

1. When they are not in approved identity list managed by the Policy Engine (Someone directly added a Cardholder in PACS system)
2. When accessing critical door during off-shift hours, enable MFA during shift hours
3. Enable MFA when accessing general door after shift hours
4. When the records indicate that they have not been vaccinated or display any infectious symptoms
5. When the records indicate that they have not completed requisite training, or their training has expired
6. When they are deemed as high-risk such as someone on a notice period or terminated or found on a watchlist. [The Definition of 'High Risk' is variable and can be dependent on various configurable factors like - how the Access is being used, Too Many failed attempts, Off-shift hours access, Termination is due in the next 2 weeks, Person found in Federal criminal history, etc.]
7. When their assigned temporary badge is active beyond an allowed business policy limit
8. When the door they are trying to access is marked for a specific business unit and identity (Cardholder) belongs to a conflicting business unit.(Segregation of Duties check)



Key Advantages

Policy Based Access Control is the perfect solution because:



It helps meet the enterprise grade security, compliance and auditing requirements of highly regulated industries such as critical infrastructure, data centers, finance and healthcare



It helps protect data and identity without compromising security or user convenience



It can be retrofit into the existing physical access infrastructure and enhance it with adaptive authentication



It supports a wide range of authentication mechanisms from traditional biometric readers to modern mobile based authentication techniques and touchless solutions



It provides coverage for privacy and user-consent requirements as part of BIPA, CCPA, GDPR and other upcoming regulations



It provides real-time policy check at the point of entry during badge-swipe by integrating identity information from multiple sources.



For more information, contact us at:

sales@bioconnect.com or sales@alertenterprise.com