bioconnect.id

Mobile Biometric Authentication for the Enterprise

No Matter the Biometric Type, Application or Device

BioConnect is leading the world's Quest for Rightful Identity. Trust and security is eroding in the digital world with escalating cybercrime and weak passwords. BioConnect is emerging as a leader to strengthen trust and security for the Enterprise.

BioConnect realizes that not all transactions or access attempts require the same level of security, or trust, to confirm the identity of the user.

BioConnect ID provides a platform of best-in-class biometric authentication technologies to protect all internal and external facing enterprise cloud applications.

Our biometric security platform eliminates the cost and complexity of implementing current and future biometric technology. We design, build and test our technology to enhance the trust between an enterprise, its customers, employees and partners.

Benefits of BioConnect ID Mobile Authentication Platform

Scalable and Reliable

Continually grow your user base without worrying about issues or downtime. BioConnect ID delivers a level of reliability to enable growth.

Best-in-Class Biometrics

Future proof your authentication strategy, we do the work so a single integration gives access to all current and future biometric modalities.

Not Just Touch ID

Integrate with biometric modalities that are stronger than a 4-digit PIN. Plus, offer users authentication with multiple modalities in a single event.

Enhance the User Experience

Eliminate inconvenient methods of user authentication caused by passwords, pins and PVQs. Provide secure and convenient omni-channel authentication.

Identity Assurance

Confidently manage identities and establish trust across all your applications and users with single or multi-modal biometrics for stronger identity assurance.

Reduced Costs & Complexity

Deploy without worrying about costs. BioConnect ID in the cloud follows a simple SaaS pricing model where you only pay for what you need.

bioconnect.id

Use Cases and Authentication Types

There are many use cases for the different authentication types that are offered by BioConnect ID. Below is an overview of ideas, further use cases can be discussed.

Use Cases

A Passwordless Experience

Convenient and Secure Solution for Users

Using biometrics removes the need for passwords and provides the highest standards of security and customer convenience. Remove the need for passwords as users' unique physiological characteristics become the authenticator. So long to password reset requests or password policies and complexity.

Transaction

Real-time Security for High Value Transactions

Add increased security to high value transactions. Match authentication security with the risk profile of transaction events. Tailor authentication methods and policies depending on the identity context and confidence of a users' identity.

Multi-Factor Authentication

Step Up Customer Security

Add additional security with multi-factor authentication. Multi-factor authentication incorporates at least two of three authentication methods; something you have (device), something you know (password), something you are (biometric) providing a layered defense against unauthorized access.

How Can BioConnect ID be Consumed?

Biometric, OTP, Mobile, Push Notification

BioConnect ID allows for convenient and secure biometric authentication in methods your customers are familiar with. Leverage biometric technology with push notifications or OTP for a consistent customer authentication experience across iOS & Android.

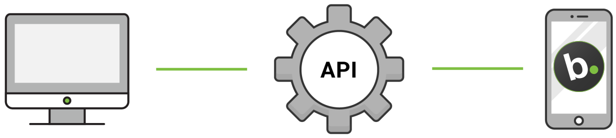
View more use cases at
bioconnectid.com/use-cases

bioconnect.id

Deployment Options and Compatibility

The BioConnect ID technology consists of a platform with API integrations, an AdminConsole for user, device and modality management and reporting and audit logging, as well as the iOS and Android mobile authenticator applications.

Deployment Options

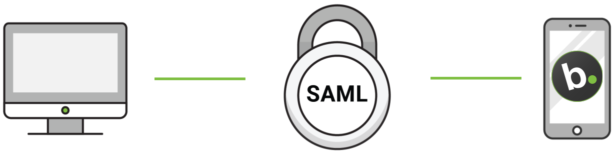


Direct API Integration

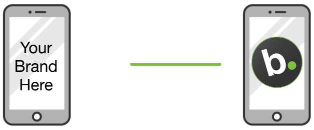
Connect your Web Service to our API and Authenticate with the BioConnect ID Mobile Authenticator.

SAML Integration

Configured to provide authentication for any SAML 2.0-enabled application or website, preconfigured with out-of-the-box gateways for a variety of popular web applications, including Salesforce, Dropbox, Office 365, Google Apps, and GoToMeeting.



Have a mobile deployment of over 100,000 users? Let us know. We have an SDK just for you.



Universal Linking

Connect your mobile app to the BioConnect ID Mobile Authenticator with Universal Linking technology.

Application Compatibility

BioConnect ID Mobile Authenticator Application

The BioConnect ID mobile authenticator app is available for download from both the Google Play and Apple App stores. The app is compatible with the following device and OS versions:

- Apple iPhone 5S and above, iOS 9.0.X and above
- Android 6 and above, API level 23 and above

BioConnect ID AdminConsole

The AdminConsole is a web application that is compatible with all mainstream browsers including Chrome, FireFox and Internet Explorer 11 and above.

bioconnect.id

Platform Feature List

Have a question about one of the below features? Or which features are included in the different pricing tiers? Reach out to us at sales@bioconnect.com. We also offer optional activation services (not included in monthly subscription, quoted separately) upon request.

Trust AI (Risk Based Authentication)

Multi Factor Authentication (ID, Password + OTP)
Multimodal Biometrics (Face, Voice, Finger)
Local Matching & Liveness Detection
Behavioral
Contextual
Device Fingerprinting
Fraud IP Detection
Trust Score

Mobile Authenticator (iOS & Android)

Cross Platform Support & Backwards Compatibility
Location Services
Authentication History
Environmental Optimization during Authentication
Push Notification Support
Device Life Cycle Management

Risk Based MFA Step-Up / Push Notification

Step Up Authentication Context for Authorization Services
Dynamic Push Notification Services
Selective Modalities
Out of Band Authentication
Off Line Authentication

Standards Based

Google Authenticator (TOTP / RFC 6238) Support
SAML 2 Identity & Service Provider Support
OATH 2.0 Support
IBM ISAM Integration

Administration Console

Dashboard (System, User Reporting & Audit Logs)
Modality & User Verification Performance Results
Group & User Geo Verification Tagging
Authentication Reporting
Privileged Administrator User Access
Event Logging & Auditing
Life Cycle User Management
User On-Boarding Options (QR Code, Universal Link)
User Self On-Boarding

Platform Security

Secure Platform
Encrypted Data (At Rest & In-Transit)
High Reliability, Availibility, Scalability
Encryption Key Life Cycle Management (KMS)

Data Privacy

GDPR Compliant
FIDO Standard Compliant

Integration Made Simple (Open API)

Stateless API
API Application Plug Ins
BioConnect Certified API Plug Ins

Support

Online Documentation,
Community & Chat
Email & Telephone Support (830am-830pm EST, M-F)
Premium Support (24/7)