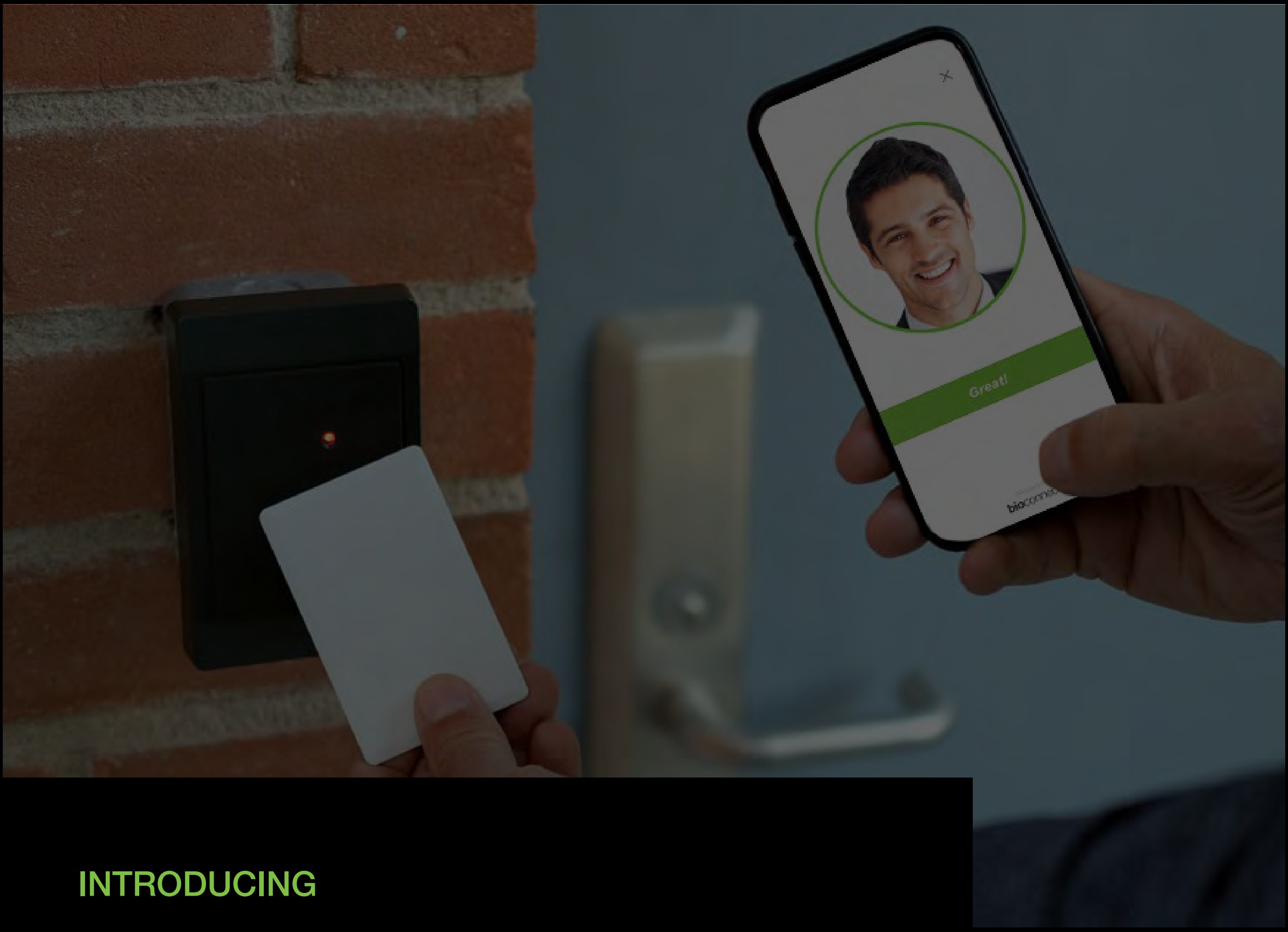


INTRODUCING

Multi-Factor Mobile Authentication for Physical Access

BioConnect Link Solution Overview

bioconnect.

THE SOLUTION

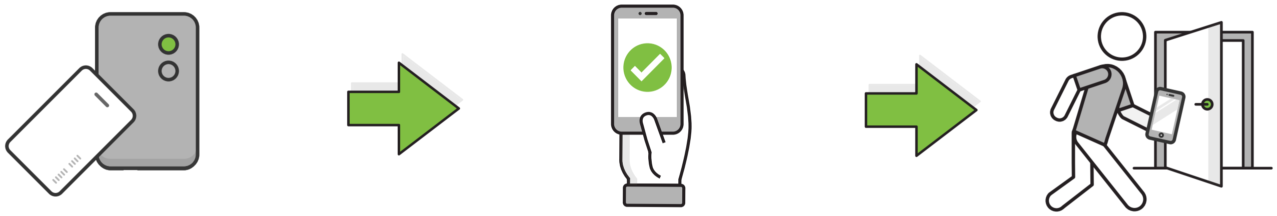
Reduce Risk at the Door with

Mobile Authentication for Physical Access

How it Works

Our Unified Mobile Access solution allows any organization to implement and ensure trusted access for all their digital applications and now their physical applications, as well.

It is retro-fit solution for doors, data centers, MDF & IDF closets and data rooms that leverages two-factor authentication (2FA) technology commonly used in digital security to confirm a digital identity.



Walk up to the door and tap your access card.

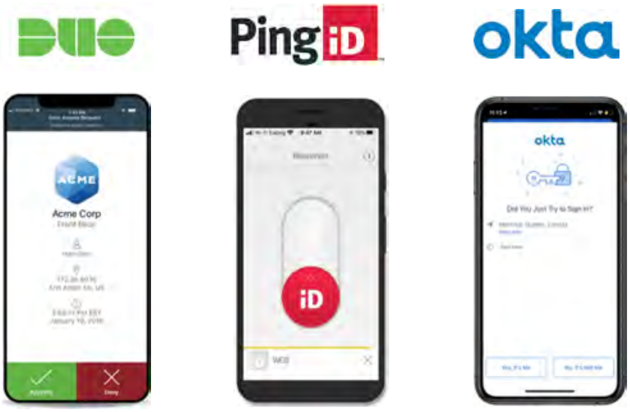
Receive and authenticate push notification on mobile device.

Access to door approved!

Pick and choose how you want to authenticate at the Door and Cabinet.

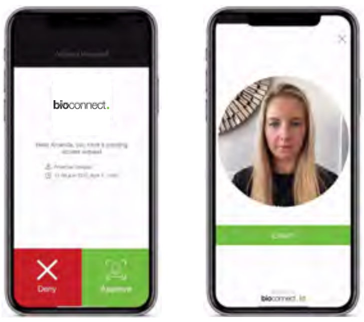
Utilize existing applications

The BioConnect Link Solution is integrated into the top mobile authenticators on the market and is continuously expanding its list of integrations. Some examples include DUO, Ping Identity and Okta.



Enable new authentication methods

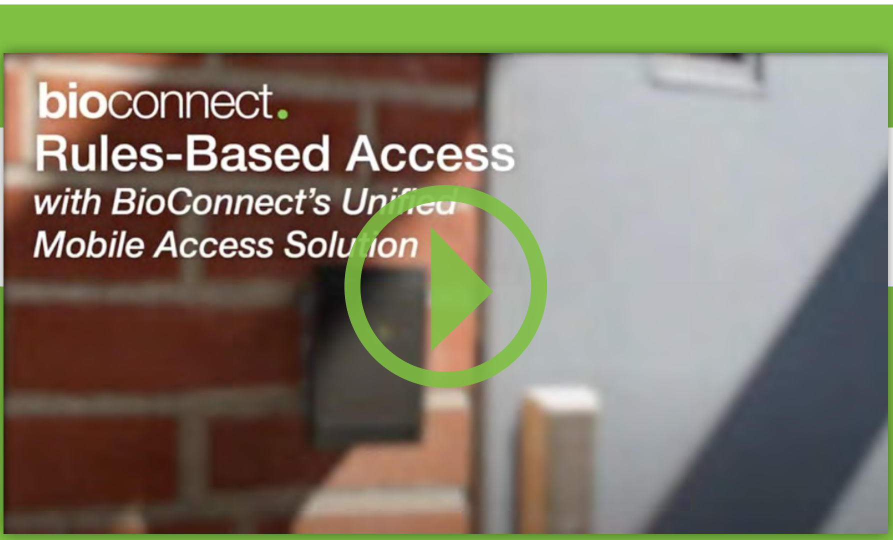
The BioConnect Link Solution includes the BC Mobile Authenticator, for customers that either do not have an existing mobile authenticator, or prefer the authentication methods available. Methods include Biometric Authentication, Simple Yes/No Approval and Wellness Declaration Authentication.



Use biometric facial recognition or a simple ‘Approve’/’Deny’ to authenticate

SEE IT IN ACTION

Watch Video



Introducing...

Wellness Declaration

Designed to help companies prevent a second wave of COVID-19. Employees or visitors seeking to enter a building confirm their health status before being granted access to facilities.

WELLNESS-BASED ACCESS CONTROL

Enable survey authentication to protect your people and deny at-risk user access.

TOUCHLESS DOOR AUTHENTICATION

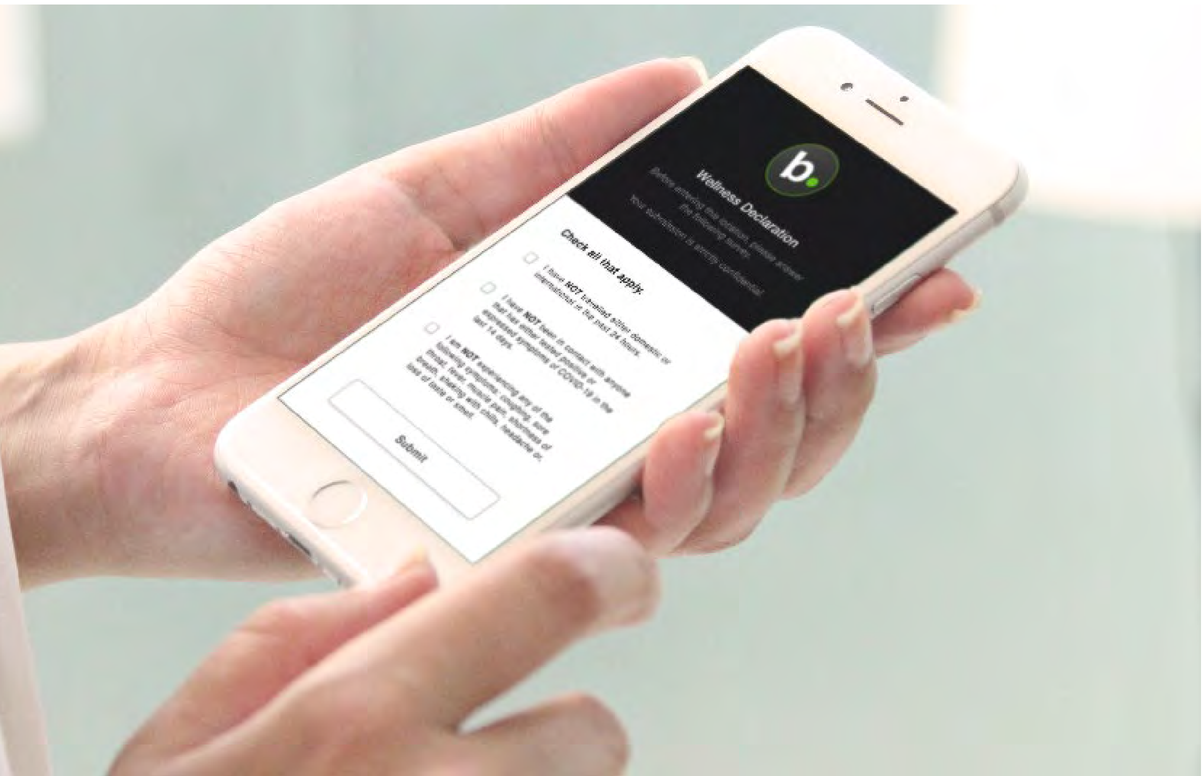
Minimize points using no-touch physical access with a mobile authentication solution.

ALERTS & VISIBILITY FOR MANAGEMENT & HR

Get alerted as-it-happens. Receive alerts through apps you use today (ex. Slack) if an individual is denied access.

COMPLY WITH SAFETY REQUIREMENTS

Safety rules and regulations for returning to offices require certain protocols to ensure the health and wellness of your employees and visitors.



Wellness Declaration

Before entering this location, please answer the following survey.

Your submission is strictly confidential.

Check all that apply.

□ I have **NOT** travelled either domestic or international in the past 24 hours.

□ I have **NOT** been in contact with anyone that has either tested positive or expressed symptoms of COVID-19 in the last 14 days.

□ I am **NOT** experiencing any of the following symptoms: coughing, sore throat, fever, muscle pain, shortness of breath, shaking with chills, headache or, loss of taste or smell.

Submit

Wellness Declaration

Key Features

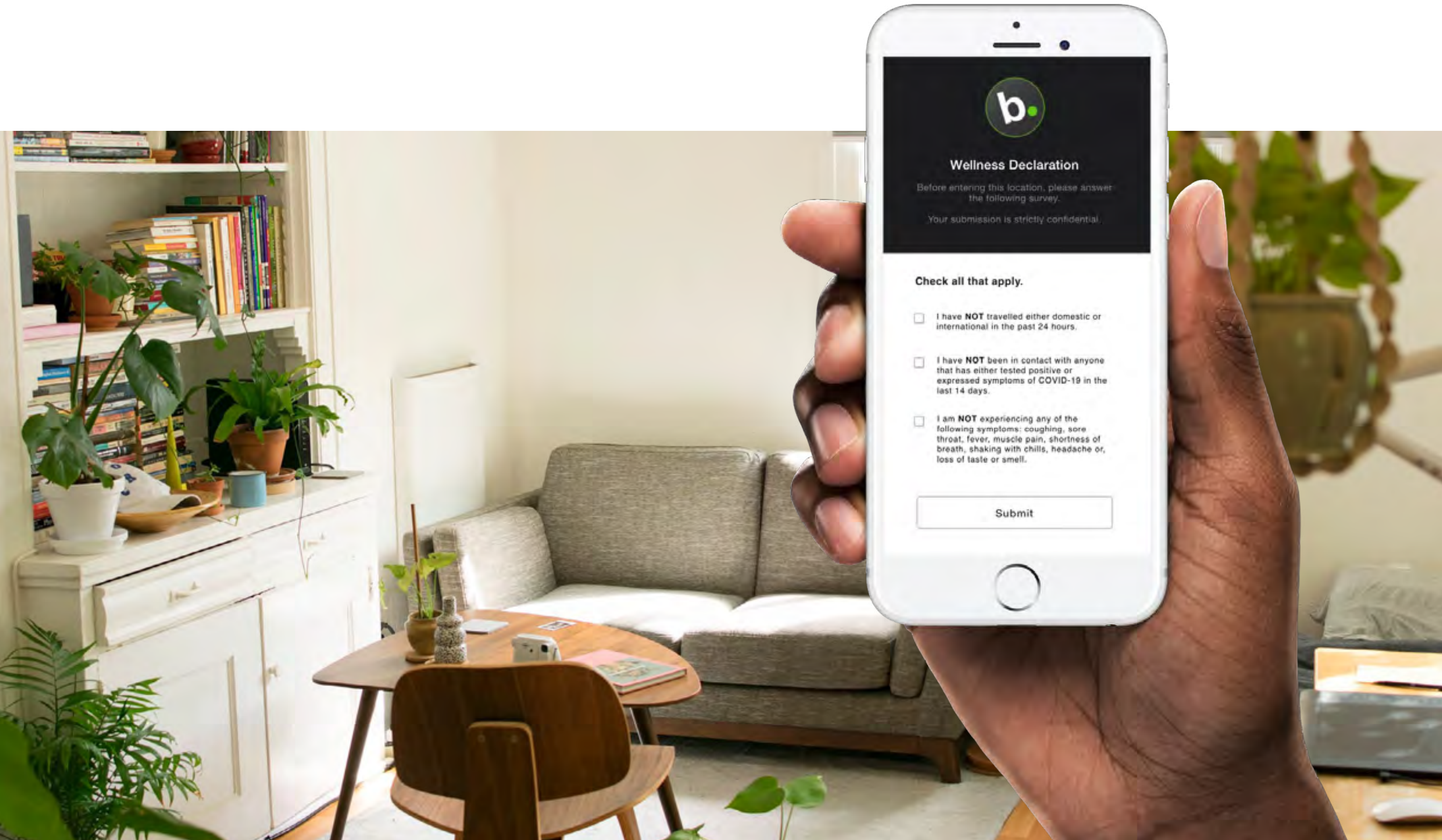
FLEXIBLE AND CONVENIENT

Enroll Users Remotely

The BioConnect Link Solution was designed to be implemented as seamlessly as possible. Get up and running in no time with the ability to enroll and invite users to the solution completely remotely.

Complete Survey Anywhere, Anytime.

Users can complete the survey from anywhere at any point in time. If a user has not completed the survey that day, prior to arriving at your location, they will be prompted to complete the survey upon tapping their card at the door.



Wellness Declaration

Before entering this location, please answer the following survey.

Your submission is strictly confidential.

Check all that apply.

□ I have **NOT** travelled either domestic or international in the past 24 hours.

□ I have **NOT** been in contact with anyone that has either tested positive or expressed symptoms of COVID-19 in the last 14 days.

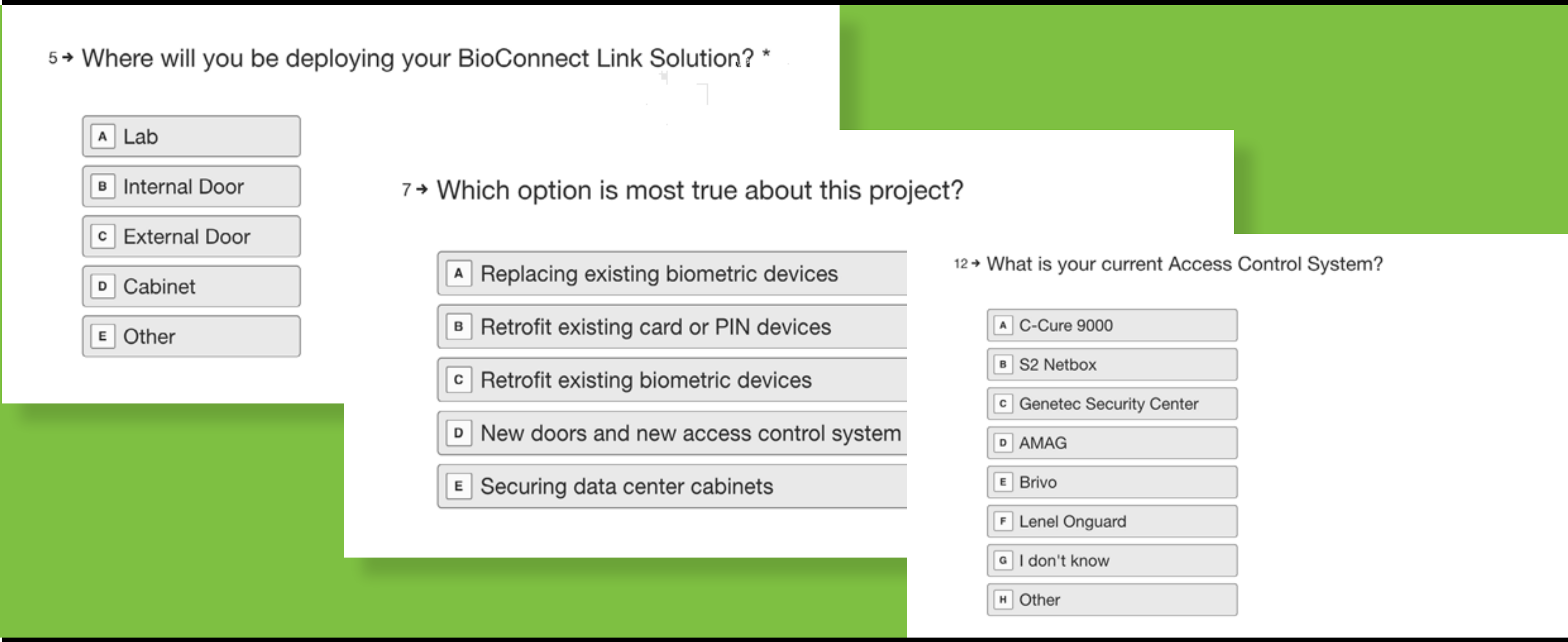
□ I am **NOT** experiencing any of the following symptoms: coughing, sore throat, fever, muscle pain, shortness of breath, shaking with chills, headache or, loss of taste or smell.

Deployment Requirements

In order to ensure a simple and frictionless onboarding experience for the Link Solution, it is important to understand the project requirements. To make this easy, we've created a customer deployment questionnaire to identify enviroment requirements, such as, the number of devices a customer will require for their access points.

1. Complete the Link Checklist
2. Upon completion, the customer will receive an email outlining the details of the questionnaire.

Complete Checklist



5→ Where will you be deploying your BioConnect Link Solution? *

A Lab
B Internal Door
C External Door
D Cabinet
E Other

7→ Which option is most true about this project?

A Replacing existing biometric devices
B Retrofit existing card or PIN devices
C Retrofit existing biometric devices
D New doors and new access control system
E Securing data center cabinets

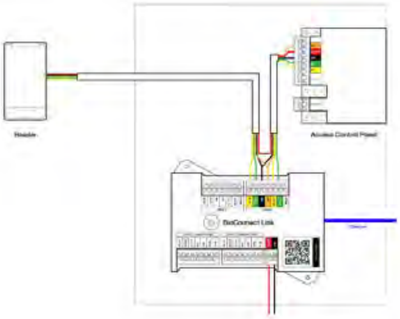
12→ What is your current Access Control System?

A C-Cure 9000
B S2 Netbox
C Genetec Security Center
D AMAG
E Brivo
F Lenel Onguard
G I don't know
H Other

Installation & Activation

Get up and running in less than **30** minutes....

1. Wire the Device(s)



2. Activate Device(s)

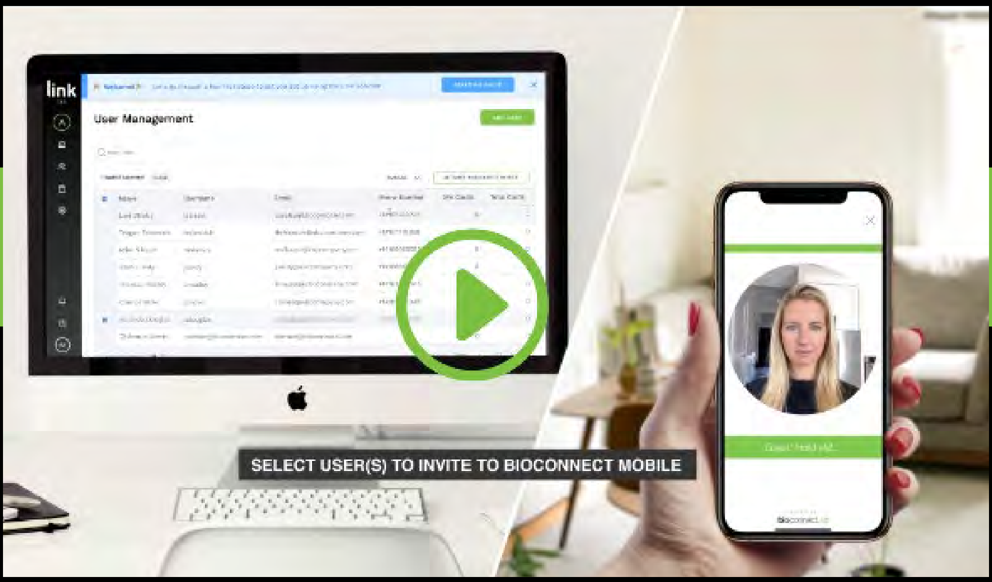
3. Configure 2FA Settings

See Installation Guide

Enroll Users Remotely

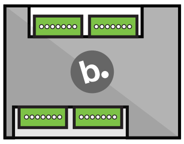
SEE IT IN ACTION

Watch Video



Product Specifications

Solution Components



+

+

Link Device

An intelligent device designed to facilitate the unification of physical security with mobile authentication applications. Easy installation, less than 30 minutes.

Link Admin Console

A web platform to manage users, devices, rules, system configuration and two-factor authentication scheduling. Syncs users via the solutions ACM sync feature.

Mobile Authenticator

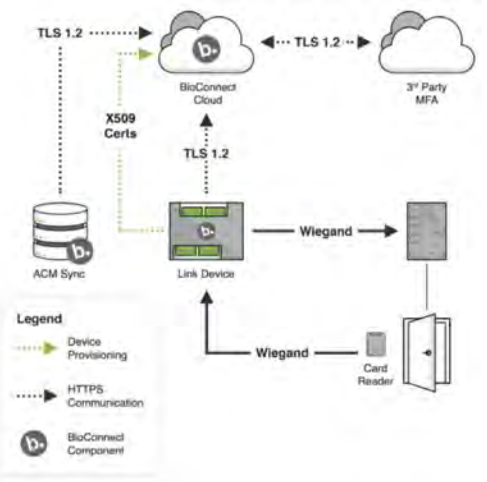
The second factor of authentication to the presented card. This can be BioConnect's provided mobile authentication app (using biometrics or a simple yes/no approval), or a supported 3rd Party Authenticator.

Product Specifications

	Product Code	Name	Class	Description
Door Controller	**BC-Doorlink**	BioConnect Link MFA Module for Doors	Reader - Type 3	BioConnect B Link for Doors
	BC-Cablink	BioConnect Link MFA Module for Cabinets	Reader - Type 3	BioConnect B Link for Cabinets
	BC-KitLink	BioConnect Link MFA Kit for Cabinets	Reader - Tyoe 3	BioConnect B Link Kit for Cabinets (2xK-Lock, 1xHarness, 2xMag Switch, 2xPlastic Lock Core, 1xPoE, 1xB-Link)
Software	**BC-Blink-D**	BioConnect Link for Doors - 1 Year Subscription (1 Door)	Software	BioConnect B Link for Doors - 1 Year Subscription (1 Door)
	BC-Blink-C	BioConnect Link for Cabinets - 1 Year Subscription (1 Cabinet)	Software	BioConnect B Link for Cabinets - 1 Year Subscription (1 Cabinet)

Hardware Specifications

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



Security & Privacy

Hardware: BioConnect Link Device

The communication between the Link hardware and the BioConnect cloud service is protected using mutually authenticated TLS 1.2 certificates on a secure MQTT protocol. Our hardware has multiple layers of redundancy to ensure your access events go through, even in the event of one or more of power, hardware or software failure.

1. Mechanical bypass to ACM in loss of power to the hardware device.

2. Device bypass to ACM if hardware device loses internet connection or cannot connect to the BioConnect cloud service.

3. Hardware equipped with partition to load an older OTA config/
Firmware.

4. Cloud redundancy for each service for BioConnect Link hardware device.

5. Link has a dedicated hardware watchdog and software watchdog; either of these will completely reboot and reinitialize the Wiegand circuitry within 250ms of detecting a hardware or software error.

Software: BioConnect Link Admin Console

Operates behind HTTPS, using TLS 1.2 and provides a standard web application to administer the solution, for example, adding users, schedules, devices, and cards. Our software uses a micro-service infrastructure to follow modular software design principles, allowing for higher manageability and scalability. Our cloud service has been designed to scale horizontally, and vertically as required. This is to ensure that access requests are processed regardless of failures and seamlessly handles peak traffic loads.

Privacy and Data Storage

1. **Data in Transit:** Each device is securely provisioned with a X509 certificate, and BioConnect does not have access to the device's locally generated private key. For a device, certificate-based authentication is the sole method of logging into the BioConnect cloud exchange; there are no generic usernames or pre-shared passwords that could be obtained by a third-party and then used to forge a connection to your cloud service. In addition to the encrypted transport layer, all user physical access data is separately protected, using either strong symmetric encryption or anonymized using one-way secure hashing. (HMAC-AES256) before it leaves the device.

2. **Data at Rest:** All local flash memory is protected by hardware encryption (AES-256), using a random key that is generated locally on each device and securely stored in a dedicated hardware enclave. Over-The-Air configuration upgrades support full, automatic rollback in the event of configuration errors.

bioconnect.

THANK YOU

For more information, please visit www.bioconnect.com

ISG
Identification Systems Group

www.IdentificationSystemsGroup.com
Info@IdentificationSystemsGroup.com
888-964-6482