Fischer Authenticator™

Multifactor Authentication and Passwordless Login

Passwords alone cannot provide adequate protection from unauthorized access, especially for high-value targets – including your IGA solution.

Deploying multifactor authentication (MFA) will ensure that all users accessing your Fischer ecosystem will be secured with up to five factors of additional authentication.

STRONG SECURITY THAT DOESN'T GET IN THE USER'S WAY

FISCHER™ INTERNATIONAL

Pattern Codes

Use either a simple "thumb slide," "circle code," or a virtual, interactive combination lock.

PIN Codes

End users create a 4-digit PIN code known only to them. PIN reset frequency is controlled by your Fischer access policies.

Bluetooth Proximity

Insure that the user's registered Bluetooth® device is within close proximity when they try to authenticate.

Fingerprint Scan

Leverage biometrics to validate the user's identity on sensor-equipped mobile devices.

Geofencing

Use the user's location as part of the login evaluation. Deny access or increase factors depending on where the login occurs.

MFA: THE TIME IS NOW!

Given the scope of Identity Governance & Administration, it is now more important than ever that organizations provide multifactor authentication. With hackers charging forward, taking advantage of even the lowest profile of user to gain an edge on you, securing your high-profile users as well as your end users has become a fundamental pillar and necessary investment to more fully secure your operating environment.

Intelligent, Contextual Access Control. Secure More Risk.

Effective identity assurance requires more than establishing trust in "who" is logging in. Authenticator™ provides you with a richer picture of the risk each login event presents. The user's current accounts, entitlements and location can all be used to dynamically determine the number and type of factors to enforce. Align authentication requirements with perceived risk.

Strong Authentication with Extreme User Experience

Authenticator™ supports the three primary factors of authentication (knowledge, possession and inherence) in addition to location (geofencing), yet all factors are quick and easy to use. Users respond to authentication requests by simply opening the Fischer Authenticator™ mobile app and authenticating using the number and type of factors requested.

Users are "Security Partners"

While securing your environment is best left to your security experts, Fischer believes that a collaborative approach provides the strongest authentication model possible.

- You control the number and type of factors required to access your Fischer environment, but can allow end users to select which factors they want to use
- End users apply their own secrets that are never stored in your environment

Go Passwordless, with Fischer!

You can only enforce password entropy to a level acceptable to end users without burdening your help desk, and force users to change their passwords so many times or in so many ways before the user experience begins to degrade. Want to empower your users with a consumer-grade user experience? With Fischer, you can. Remove the burden of managing passwords.

Extend the Power and Value of Your Fischer Investment

Adding MFA to your Fischer ecosystem is simple and leverages your identity and governance infrastructure already in place.

- Benefit from existing Fischer processes and controls: access policies to determine the number of factors to present, provision / deprovision MFA entitlements, approvals, user interfaces and more
- Provide users with consistent processes and UX. Users visit Fischer Self-Service to request temporary access if their mobile device is unavailable or lost
- Eliminate duplicate MFA license, cost and administration

There's No Comparison

Fischer Authenticator™ is the most advanced and effective solution available for strong identity assurance. There's no comparison with 2-factor or other MFA products.

	Typical 2-Factor Auth	Fischer Authenticator™
iOS	✓	✓
Android	✓	✓
Push Notification	✓	✓
Remote Logout	not supported	✓
Remote Device Unpair	not supported	✓
OTP Generator	✓	no thanks
Total # Auth Methods	not supported	✓
Fingerprint Scan	not supported	✓
Pattern Code	not supported	✓
PIN Code	not supported	✓
Bluetooth Proximity	not supported	✓
Geofencing	not supported	✓