Authlogics Multi-Factor Authentication

Quick deployment, multiple token types, no password required.

Authlogics Multi-Factor Authentication is a secure login and password replacement solution that can be deployed in record time. It offers multiple token and tokenless options to suit any scenario while ensuring a simple user experience.

For years the password has been the foundation upon which user access has been built. But passwords are very risky as they rely on humans for creation, recall, and protection. Complex password policies just add complexity and frustration, which is why many companies turn to Multi-Factor Authentication to address the weaknesses of passwords alone.

Many organisations would like to do away with passwords eventually; however, many MFA solutions simply add a factor on top of the existing password. An MFA solution that uses the password as dependency does not pave the way for a password-less future.

Authlogics are dedicated to helping IT managers improve security while making it easier for users to access their information. We focus on helping organisations to transition away from passwords with MFA that does not require them. This not only improves security, but it also provides a simpler user experience.

Engineered from the ground up with the modern IT manager and user in mind, Authlogics' solutions are feature-rich and simple to deploy.

Authentication Factors

Moving from a single "knowledge-based" factor like a password to adding an additional factor can seem like a big step. Not only are there multiple factors to deal with, but also multiple types of each factor to deal with. Choosing the best combination of the number and types of factors, to best suit your use cases, users and applications is critical.

Authlogics provides many options to choose from, including alternative "knowledge-based" factors to passwords paving the way for their replacement.

Our pioneering Deviceless OTP opens up new use case scenarios by providing the benefits of a traditional Once Time Code logon but without the overhead of managing physical devices.

Authlogics MFA includes support for up to 10 devices per user at no extra cost. Choose from:

- The Authlogics Authenticator soft token
- SMS & email tokens (pre or post-send)
- YubiKey hardware tokens

Furthermore, the SC Magazine award-winning PINgrid and PINpass technologies include transaction signing functionality to deliver the most secure solution available in the industry without requiring dedicated hardware.

Application support

Supporting multiple applications, both on-premises and in the Cloud, is critical. Authlogics MFA includes support for industry-standard protocols such as SAML 2.0 for SSO and Cloud access, and RADIUS for VPN and network devices. Multiple agents are included to integrate directly with common applications such as Windows Desktops and Citrix gateways.

A Web API is also available for custom integrations, IFTTT automation, scripting and orchestration.

Features and highlights

- Fast deployment and bulk user enrolment
- Deviceless OTP, 2 and 3 factor risk-appropriate security
- Flexible token type choices on a per-user basis
- On-premises and Cloud
- User self-service provisioning and AD password reset
- Up to 10 tokens per user
- Easy Side-by-side migration from other vendors
- IFTTT Automation and orchestration via Web API
- Secure Password Vault for password-less logins
- Multiple agents for 3rd party integrations
- SIEM compatible logging

Authlogics

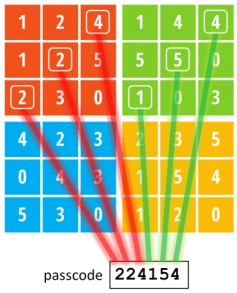
Authlogics Multi-Factor Authentication

Authenticate on the Phone, Web or in App... without a password

Rewrite the rule book for authentication solutions – and make it simple

Authentication Technologies

With Authlogics, you're spoiled for choice when it comes to authentication types:



PINgrid: This pattern-based logon technology requires no static PIN or password. All you need to remember is a pattern which, unlike a password, is never given away during a logon; keeping the knowledge in your head a secret.

PINphrase: Random letters from an answer to a question act as a One-Time Passcode. The user does not need to remember anything new and no password is required; the secret is again kept safe.

PINpass: A widely used 6-8-digit random One-Time Code solution which is OATH (Open Authentication) compliant (RFC 4226 and 6238) which can be used with PINs, passwords or Biometrics.

YubiKey: A highly secure USB hardware token with no batteries required.

Empower your users

Empowered users are happier and more productive people. Authlogics allows users to perform common management tasks themselves via a simple responsive web interface, including:

- Enrolling new token devices
- Updating mobile phone numbers
- Resetting Active Directory passwords

Password reset requests alone are estimated to account for approximately 40% of all help desk calls. This is a costly exercise in terms of both support staff and lost staff productivity, which could be mostly eliminated.

When paired with the Authlogics Password Security Management (PSM) solution, users have an intuitive interface to help them choose a non-breached compliant password, with helpful "traffic light" guidance as to why their password may or may not meet the password policy requirements.

Simplified Management

The administration is performed either via our rich Management Console or easily accessible Web Management Portal - perfect for helpdesk tasks such as enabling Emergency Override Access. Role-based access means you get to choose who is authorised to perform which tasks, while extensive logging tracks all activity for auditing requirements and is compatible with common SIEM solutions.

Need to provision 10,000 users in 15 minutes? No problem. With a toolset ranging from wizards to customisable scripts, you can perform seemingly impossible tasks in no time.

Native Active Directory Integration

Because nobody wants yet another directory database, Authlogics MFA was designed to integrate directly with AD, without extending the schema. This brings many advantages and also avoids common directory synchronisation problems.

Our Password Vault keeps track of all your users' AD passwords allowing for a password-less login experience to Windows desktops. The vault is AES256 asymmetric encrypted with HSM support to keep the data secure.

About Authlogics

Award-winning authentication experts Authlogics are committed to assisting IT managers with improving security while making it easier for users to access their information. Authlogics focuses on helping your business transition away from password-driven environments while increasing your security posture and compliance with policy and regulatory controls.

Authlogics Authentication Server is one of the core components of the Authlogics product suite, an enterprise-ready authentication and password management platform designed to fit seamlessly into existing Active Directory environments, or as a standalone solution.

Authlogics has been designed to integrate with most systems from remote access solutions to application-specific requirements via standard interfaces such as RADIUS and Web Services. It is quick to deploy, easy to maintain and manage with tools such as web-based user self-service and helpdesk operation portals. Authlogics also includes Windows Desktop Logon functionality to allow for online and offline access to Windows PCs.

Available on the App Store | GET IT ON Google Play | Available at amazon | Get it from Microsoft

Authlogics

www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866