Industry Standard 2 Factor Authentication

Turn any mobile device into a soft token

PIN PASS

What if you could incorporate some of the strongest logon security available, while cutting costs and reuse existing investments that work for you? Put PINpass to work for you.

Given the growing sophistication of security threats worldwide, strengthening logon security has become a critical component of any security system. IT managers are fending off increasingly more advanced attacks with limited spend, while ensuring users have access to the resources they need when they need them. It's perhaps one of the most delicate balances to maintain in the business landscape.

PINpass provides a simple-to-use, cost effective 2 Factor Authentication solution for organisations looking for a standards-based approach to logon security.

How it works

PINpass uses two unique and separate factors:

- 'Something you have': a standards-compliant (RFC 4226 and 6238) random One Time Pin (OTP) is generated by a soft token device, a YubiKey, or sent to the user via SMS or email.
- 'Something you know': a user-selected static PIN number, or an existing Active Directory password.

The Authenticator app or YubiKey generates an OTP, or Authlogics Server generates 6 - to 8 - digit OTPs which are delivered to users in either real-time or pre-send configurations.

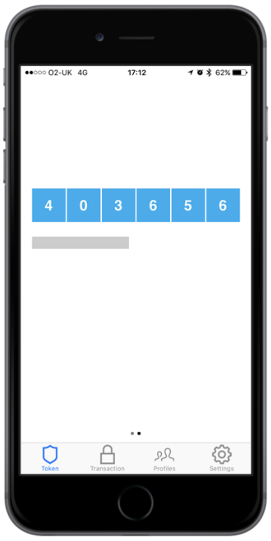
Real-time OTPs are sent one at a time and only when the user needs to logon. Pre-send OTPs are sent when the user is first enabled for PINpass, and subsequently after the last pre-send OTP has been used.

A login process can then compare the OTP entered to verify that only that user could have created or received that OTP.

Remote access on your terms, even offline

PINpass enables Bring Your Own Device (BYOD) initiatives with minimal effort and without compromising security. In fact, the use of pre-send OTPs helps overcome SMS or email delivery limitations associated with inadequate mobile coverage or data connectivity.

Administrators can configure up to 10 pre-send tokens to be delivered in a single message. This reduces delivery costs and ensures the user has enough tokens on hand before requiring connectivity again. The life span of pre-send OTPs can also be configured on a per-user basis to better balance corporate security with the need for mobile enablement.



Features and highlights

- Support Authlogics Authenticator soft-token or YubiKey hardware-based token
- Securely logon on to Windows Desktops from any location
- Cost effective - especially compared to hardware solutions
- Emergency Override Access
- Secure access to internal and cloud-based applications
- Rapid user provisioning (thousands in minutes)
- Self Service AD password reset
- Web-based Operator portal for day-to-day IT helpdesk operations
- Real-time or pre-send token delivery via SMS or email

Authlogics

Industry Standard 2 Factor Authentication

PIN
PASS

A simple and feature rich OATH soft token

PINpass is just one way in which Authlogics supports OATH's drive to use open standards to lower cost of ownership and reduce complexity.

Less complex. More secure

Simple deployments are better for everyone. They also reduce the costs associated with user training, which are often overlooked. PINpass enables administrators to allow users to use their Active Directory password instead of a PIN. Security levels are maintained by entering this Password or PIN before or after the OTP. The PIN can even be entered in the middle of the OTP, making it even more difficult for potential hackers to differentiate between the static PIN and OTP.

Topping up your bottom line

Security comes at a cost. Companies are frugal. IT Managers manage this gap daily as the lion's share of the budget gets siphoned off by infrastructure. With Authlogics, you can spend less and get more.

•PINpass delivers industry-standard OATH technology in a highly cost-effective package by doing away with plastic key fobs and the hidden logistics costs - which can be greater than the initial purchase price.

•Batching one-time codes reduces the number of SMS messages sent, slashing ongoing SMS delivery costs up to 90%.

•Leveraging existing AD infrastructure and mobile devices requires no additional management overhead.

•Utilising Blackberry or ActiveSync infrastructure to deliver OTPs reduces the cost of delivery to zero, while the security of sending an OTP is maintained, even over email.

World-class, integrated deployment that suits and simplifies your environment

• It has been designed to use an existing Active Directory as the accounts database without extending the AD schema. There are no extra databases to backup and manage, and it's by nature highly available.

• SQL Server may be used as a repository instead

• Authlogics includes a full RADIUS server for authentication and accounting to easily integrate with any RADIUS aware 3rd party system.

• RADIUS proxy is also supported for coexistence or migration scenarios and RADIUS extensions can provide extra information about users to the authenticating device.

• If RADIUS isn't enough, an XML Web Services interface is also available for seamless integration into any application.

• SMS-based OTPs are delivered via a choice of built in international SMS gateways (with sign-up assistance) while email based OTPs are sent via SMTP with optional Auth and TLS encryption.

- SMS flash and message overwrite functionality
- Active Directory or SQL Server database storage (no schema extensions)
- RADIUS and Web Services interface for universal integration
- Leverage existing Active Directory password or use a static PIN
- OATH , HOTP and TOTP (RFC 4226 and 6238) compliant
- FIPS 198 & 180-3 compliant

About Authlogics

Award-winning authentication experts Authlogics are committed to assisting IT managers improve 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 to policy.

PINpass is one of the core components of the Authlogics product suite, an enterprise-ready multi-factor authentication and 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 PCs.

Authlogics