NoPass

PASSWORDLESS REGISTRATION AND AUTHENTICATION

Contact us
sales@identite.us
www.identite.us

NoPass™ Authentication Technology

NoPass™ is a multi-factor authentication add on for remote users. In addition to the username and password, NoPass™ performs two additional factors of authentication – something you have and something you are. This utilizes smartphones and does not require the purchase of additional hardware authentication devices for each user. It also does not use SMS, which can also be costly.

NoPass™ is a secure authentication app that brings you the two things you need most: the highest level of authentication security and the simplest user interface. Now you can have the confidence of never worrying about a compromise of your online credentials.

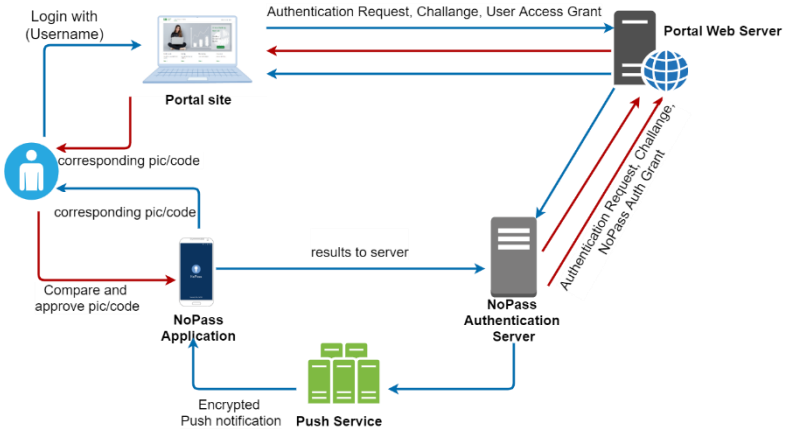
Along with very strong security, the user does not need to enter a password. The NoPass™ server and application in the phone takes care of all of the bi-directional handshaking, requiring only that the user compare two images (a picture and a 3-digit number), then swipe or touch the approve button, and they are connected.

This method provides a million encrypted combinations, and is virtually un-hackable since the metadata is valid for only a few seconds and is useless after that. Even if the user mistakenly approves the transaction, we are able to detect the intrusion and block the entry into the server.

FULL DUPLEX AUTHENTICATION™ Technology

The NoPass™, Full Duplex Authentication™ process follows a decentralized authentication model. This lets us work together with any kind of traditional user authentication technology, such as PIN, OTP, PKI, and Biometrics. NoPass™ has a flexible architecture to easily integrate with any User Authentication solution.

By combining public-key encryption with fast OTP authentication, NoPass™ Full Duplex Authentication™ MFA enables mobile-initiated login to workstations through your mobile device. It's fast and secure.



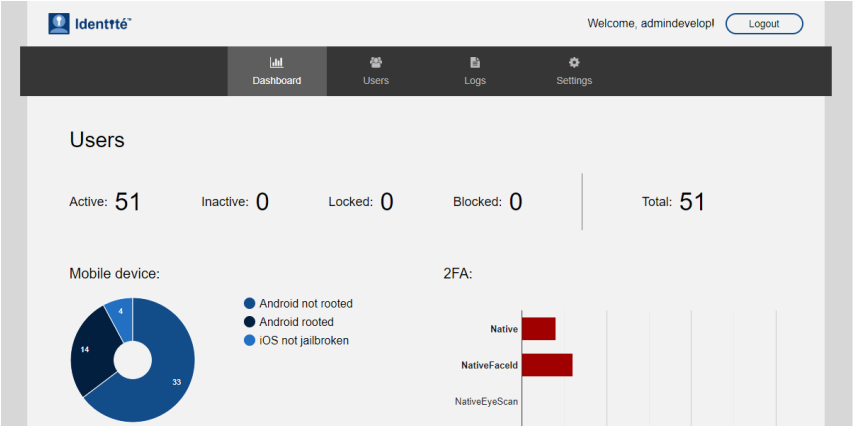
NoPass™ MFA

With the increase in phishing and other identity attacks in our day and age, authentication that requires a username and password (like RADIUS) can be potentially at risk. Sophisticated social engineering schemes and clever tactics can fool even the most savvy of users. In order to combat this, NoPass™ has introduced its MFA solution, a light feature that enhances the overall security and is adaptable with the leading authentication protocols that are in the market.

NoPass™ Admin Panel

Gain complete Administration Overview - Using the NoPass™ Admin Panel. Device Trust Ensure all devices meet security standards. Adaptive Access Policies Set policies to grant or block access attempts. Remote Access Secure access to all applications and servers.

Every aspect of your NoPass™ authentication system can be managed from the Admin Panel. This includes creating and managing applications, enrolling and activating users, managing mobile devices, fine-tuning the user experience of your NoPass™ installation, and more.



Infrastructure Requirements

On-premise

- Highly available deployment
- Docker & Kubernetes support
- Reverse proxy
- Clustering and HA

Cloud

- Private cloud deployable (ie. AWS, Azure, IBM)Highly available deployment
- High scalability
- Deploy in almost every country
- Support for self-sign up for trials and production

Product Features

- Simple & Clear User Experience for Registration, Authentication, and Restoration
- Innovative picture and code OTP, user convenient and much higher brute force security
- Easy to use Admin Panel to set policies and restrictions such as device and geographical requirements
- Controlling device hygiene and checking for rooted or jailbroken devices that may compromise security
- Flexible Integration with any existing User Authentication
- Encrypted secure cloud account backups accessible for both iOS and Android

Benefits of NoPass™

Security
Login credentials are unique across every website, never leave the user's device and are never stored on a server.

Convenience
Users unlock login credentials with simple built-in methods such as fingerprint readers or face scans.

Scalability
The wide use of smartphones and our cloud deployment make it super easy to scale any existing authentication.

Cost efficiency
Save millions in helpdesk and password support costs.

Privacy
Protect your users from credential leaks and password phishing