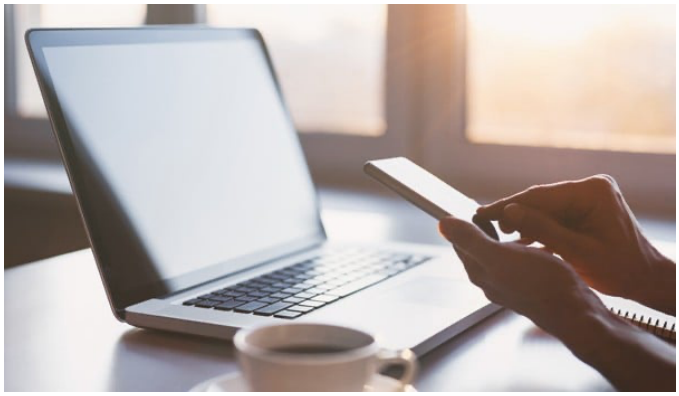
NoPass

NoPass™ Employee MFA

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

NoPass™ Passwordless MFA Technology



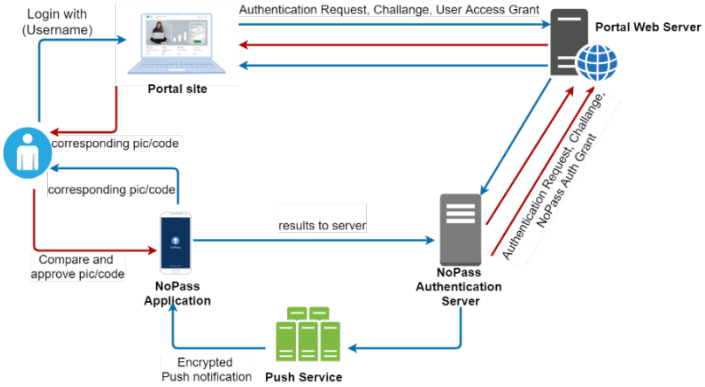
NoPass™ is a passwordless multi-factor authentication solution built for the workforce. NoPass™ takes a user through all three types of authentication – something you know, something you have and something you are. This utilizes existing trusted devices such as a smartphone and/or the PC or Mac. Passwords and SMS OTP are **not** supported as these methods are not secure.

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.

The passwordless MFA experience for the worker begins at the desktop. Along with very strong security, the user does not need to enter a password. The NoPass™ server and application in the trusted device takes care of all the bi-directional handshaking. The user simply compares two images (a picture and a 3-digit number), then taps or clicks the approve button to complete the authentication request. 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. Additional factors are supported such as a biometric from the trusted device as well as HW tokens like a Yubikey device.

FULL DUPLEX AUTHENTICATION® Technology

The NoPass™ Full Duplex Authentication® process is patented technology that follows a decentralized authentication model and enforces two-way authentication between a user and the NoPass™ Server. This prevents phishing and replay attacks. This is also compliant with NIST 800-63-B AAL3, which is the highest level defined.





Connecting NoPass™ to your Enterprise

In addition to the desktop unlock, NoPass™ can be integrated into other systems and applications in your enterprise. There are two main methods used to connect NoPass to your enterprise. The first uses the RADIUS protocol. The NoPass™ server becomes a RADIUS client and will perform all the factors of authentication for which the security policy has been configured.

The second method uses SSO Federation. The NoPass™ server can be configured as the "Identity Provider" to services in your enterprise such as Active Directory/Azure, SSO server (Okta, Ping, ForgeRock, etc.) or any service that supports SSO protocols SAML and OpenID.

NoPass™ Authenticator Device Support

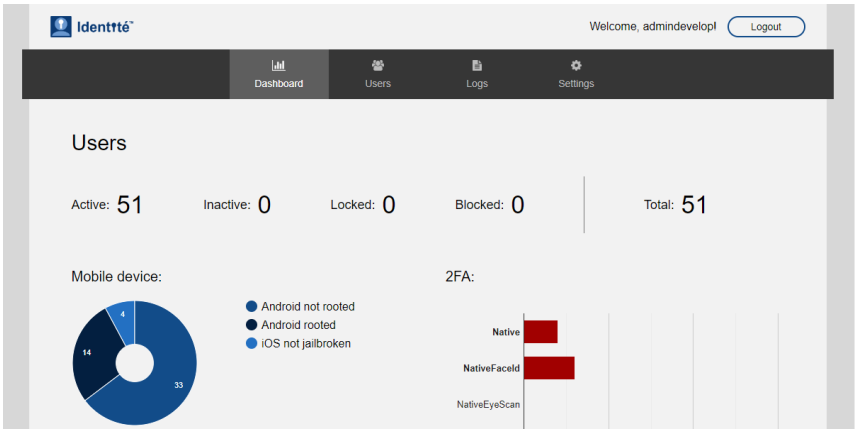


NoPass™ technology turns a user's trusted device into a secure HW token. A variety of devices are supported that include Windows, MacOS, iOS and Android. By utilizing a user's favorite personal device, NoPass™ can incorporate additional native authentication factors such as a biometric and/or a HW token device such as a Yubikey. Security policies can be set in the NoPass™ server that define the required factors. Users can easily pair additional devices after the first device is registered. Having more than one device configured for authentication resolves issues with lost or stolen devices and devices can easily be deauthorized by a user's other device or by the admin using the NoPass admin portal.

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
- Support for self-registration within the enterprise or externally via email invitation
- Multiple devices supported as well as other factors such as biometric and HW Tokens
- Patented Full Duplex Authentication® using picture and code OTP – impervious to phishing and replay attacks
- Set policies such as required and optional authentication factors
- Checks for rooted or jailbroken devices
- Flexible Integration with any existing User Authentication system in your enterprise including the Windows desktop
- Encrypted secure cloud account backups accessible for both iOS and Android

Benefits of NoPass™

Security

Login credentials are unique across every service, 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.