NoPass

PASSWORDLESS REGISTRATION AND AUTHENTICATION

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

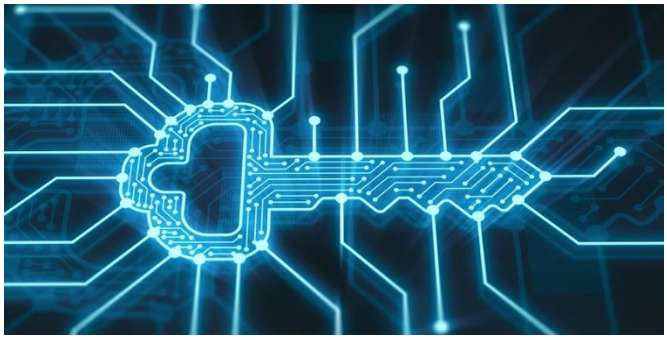
Single-Sign-On Technology

Today, organizations want to quickly and securely provide end-users with access to their corporate-approved apps. They want to ensure that the right people (i.e. employees, part-time employees, contractors, etc.) get access to the right company information. In fact, if there's an opportunity to reduce or eliminate password usage, both organizations and end-users will welcome that. When employee productivity and user experience are top priorities, single sign-on to corporate apps is key.

NoPass™ Employee SSO passwordless multi-factor authentication ensures that only authorized users get access to sensitive data across all your systems. With NoPass™ Employee SSO, you get all the features in the NoPass™ Employee MFA with additional features such as Federation/SAML/OIDC support and Identity Brokering.

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.

NoPass Single-Sign-On

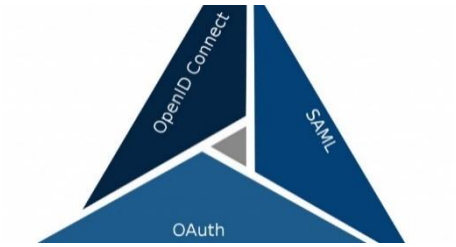


Increase productivity while keeping data secure. With NoPass™ Employee SSO users only have to authenticate once to access their web apps in the cloud. This foundational identity and access management (IAM) measure is a first step in building trusted experiences for your workforce, customers, and partners. NoPass™ Employee SSO password-less multi-factor authentication ensures that only authorized users get access to sensitive data. NoPass™ Employee SSO incorporates all the features that are offered in the NoPass™ Employee MFA with additional features for Single-Sign-on such as:

One-Time Login

With NoPass SSO, users only have to enter a username to securely access their web apps in the cloud and behind the firewall - via desktops, smartphones, and tablets. This greatly increases productivity while keeping data secure. NoPass SSO uses Integrated Windows Authentication (IWA) to sign users into NoPass automatically once they have signed into their Active Directory domain or their company portal.

Federation/SAML/OIDC Support



NoPass™ integrates with cloud and on-premise apps using SAML, WS-Federation, OpenID Connect, and web services to provide simple and fast single sign-on for any device, and serve as the identity provider to external service providers so that when the user logs into a service, instead of providing credentials to the service provider, the service provider trusts the identity provider to validate the credentials.
The NoPass™ authentication server has the capability to accept both SAML and OIDC authentication tokens and respond to each respectively.

Identity Brokering

NoPass™ Employee SSO can act as an intermediary service that connects multiple service providers with different identity providers. As an intermediary service, the NoPass™ Employee SSO is responsible for creating a trust relationship with an external identity provider in order to allow its identities access to internal services exposed by service providers. NoPass™ Employee SSO has the ability to add additional factors of authentication beyond the identity providers user authentication. Once an identity provider sends an authentication token via NoPass™, the user identity is registered on NoPass™. You can configure additional authentication factors for this user after NoPass receives a valid federation token.

Seamless User/Temporary-User Experience

With NoPass™ Employee SSO, you have the ability to add temporary users to your workforce and grant them the possibility to use the services your other employees are accessing. You can add restrictions such as the period they have access to resources, which resources are available and which are still restricted, and the time during the day when they can access these services. This option is very important for companies that have frequent guest visitors or outsource part of their services to third-party vendors. Enable your end-users to quickly access corporate approved apps in one click. Eliminate the inconvenience of managing, remembering, and resetting multiple passwords for end-users.

Infrastructure Requirements

On-premise

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

Cloud

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

Product Features

- Simple, Secure, and Convenient Full-Duplex Password-Less Authentication product
- The NoPass™, Full Duplex Authentication™ process follows a decentralized authentication model. Works together with any traditional user authentication technology, such as PIN, OTP, PKI, and Biometrics
- Completely Password-less SSO, Easy to install, meet the needs of any organization also gain
- Innovative picture and code OTP, user convenient and much higher brute force security
- Complete Administration Overview - Using the Admin Panel, set policies and restrictions such as device and geographical requirements
- Flexible architecture to easily Integration with any existing User Authentication

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 users from credential leaks and password phishing.