NoPass

PASSWORDLESS REGISTRATION AND AUTHENTICATION FOR WINDOWS USERS

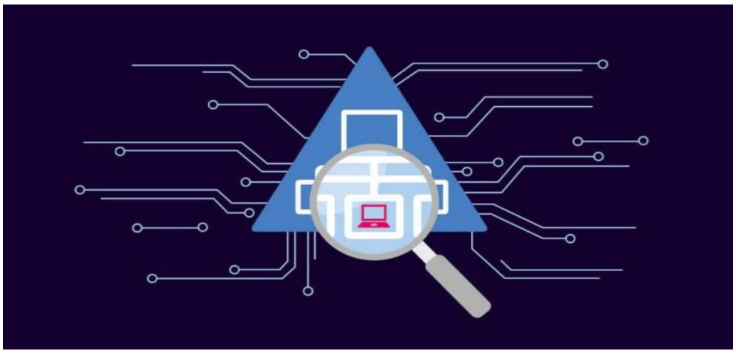
Contact us
sales@identite.us
www.identite.us

Secure, Simple, **Full Duplex Authentication®** for Microsoft Apps

The sudden surge in remote work in a cloud application and mobile world has challenged network security professionals. The security perimeter, which now extends to the workers home, must still provide secure access to a range of business applications. With today's users also requiring access to on-premises applications and cloud applications, organizations can't rely on traditional perimeter security architecture to secure access to applications. IT and cybersecurity teams are now charged with providing secure access to resources across a hybrid, multi-cloud environment. Most business IT infrastructure are founded on Microsoft's Active Directory (on-premise) and/or Azure (cloud) platforms. NoPass™ offers a variety of features and solutions that verify trust for the workforce and successfully shift towards remote work by implementing and enforcing NoPass™ zero-trust practices.

NoPass™ is a secure authentication solution 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™ Windows passwordless multi-factor authentication ensures that only authorized users get access to sensitive data across all your systems. With NoPass™ it's easy for users to authenticate to the applications they need without compromising security.

Integrate into AD with RADIUS



Active Directory Federation Services (ADFS), is the de facto identity provider in a Microsoft environment. Many organizations will be using it to authenticate Office 365 users to an on-premise Active Directory. Support amongst cloud service providers is growing, allowing you to authenticate not just Office 365 users but users of a variety of business applications.

In certain circumstances, you may want to require multi-factor authentication (MFA). Out the box, ADFS only provides support for X.509 certificates. Thankfully there's the concept of Authentication Adapters, allowing you to increase security and simplicity using an MFA plug-in. At Identité™ we've developed a RADIUS plugin that allows you to prompt users to enter their AD password, have them execute two or more additional factors of authentication and send the response to the NoPass™ server which acts as a RADIUS Client, along with the accounts userPrincipalName, for validation and maximum authentication security.

The NoPass™, Full Duplex Authentication® process follows a decentralized authentication model. This feature stops impersonation attacks and prevents credentials from being intercepted from a "Man In Middle attack" (MIM). NoPass™ has a flexible architecture to easily integrate with any User Authentication solution.

Federated SSO Integration with Azure Directory and Office 365

Office 365 is a cloud-based subscription service that brings together the best tools for the way people work today. By combining best-in-class apps like Excel and Outlook with powerful cloud services like OneDrive and Microsoft Teams, Office 365 lets anyone create and share anywhere on any device.

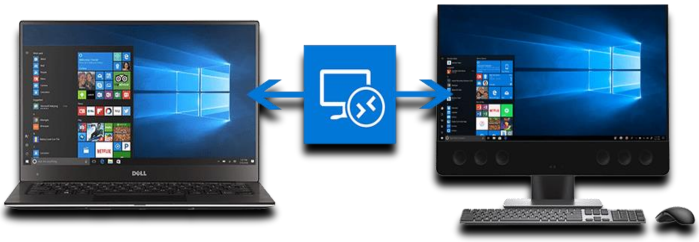
NoPass™ provides a simple and reliable method to federate on-premises Active Directory and Azure AD. The configuration of NoPass™ and Azure AD provides customers with a seamless and secure access to Office 365.

NoPass™ provides secured seamless access to their mobile, cloud and enterprise applications. Integrating Office 365 with NoPass™ acting as the identity provider is accomplished through the open standards SAML and OIDC, which support both active and passive user profiles.

MFA – more than just an SMS OTP

Azure provides a SMS OTP solution as a 2FA for the sake of increasing security but 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 savviest of users. In order to combat this, NoPass™ has introduced its MFA solution, that significantly enhances overall security and is compatible with the leading authentication protocols that are in the market.

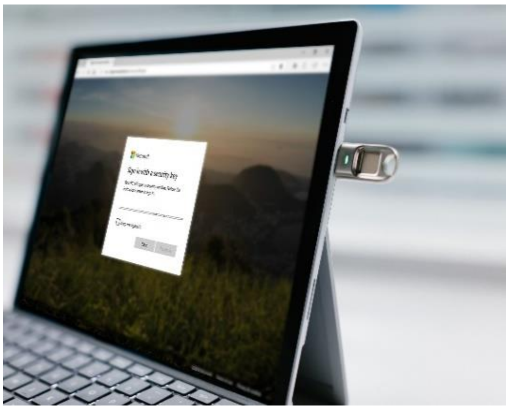
Securing VPN and RDP Gateway access for workers at home



Whether you're already running your hosted desktop applications as on-premises or planning to move those workloads to the cloud, you need a secure network connection to the office for home workers. NoPass™ integrates with Microsoft Windows client and server operating systems to add multi-factor authentication to logins with a solution that balances security and usability. Access policies can be configured to block access to sensitive remote workstations from devices that are out of date or non-compliant with your security requirements.

NoPass™ for Windows Logon adds NoPass™ multi-factor authentication to Windows desktop and server logins, both at the local console and incoming Remote Desktop (RDP) and VPN connections. One factor will be something a user has, a secure token. This is protected by Identité's patent pending Full Duplex Authentication® which is impervious to impersonation. Another factor a user as could be a hardware token like a Yubikey. If the device supports a biometric, then something a user is could be yet another factor.

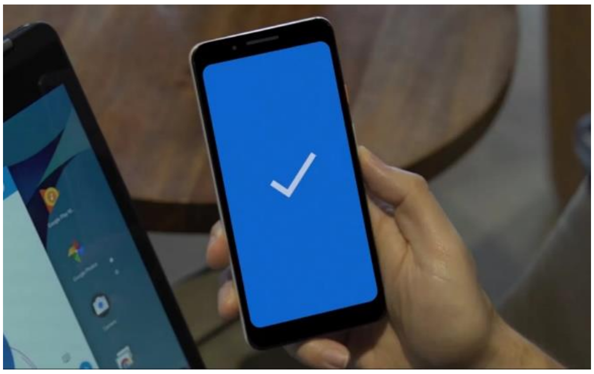
Native Windows Client



The NoPass™ Authentication client for Windows provides the same multi-factor as the mobile application. In addition, native hardware tokens such as Yubikey, and other third-party devices are supported by the windows client, NoPass™ is an easy-to-use two-factor authentication solution that fits seamlessly in your users' daily workflows.

Some websites and online services let users protect their accounts with a mobile-generated passcode that must be manually entered and only works for a certain amount of time — typically 30-60 seconds. Both the Windows and Mobile NoPass™ authentication client can protect all sites with unique credentials protected by Full Duplex Authentication®. All users keep all their accounts and credentials in a virtual digital wallet.

Windows Login (GINA) integration including passwordless unlock with Bluetooth enabled smartphones



NoPass™ enables wireless devices equipped with Bluetooth to be used for computer security (login, authentication, lock/unlock). Your mobile phone plays the role of your access key from your PC:

- Automatic Windows logon when a user approaches the computer (with the mobile phone).
- Computer will be protected with a password, but you don't have to enter it manually.

NoPass™ is a genuine authentication solution with complete password replacement, and not just a primitive PC locker like many other programs where you must enter a password manually anyway for logon.

Deployment Options

On-premise

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

Cloud

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

Product Features

- Simple and Secure passwordless 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 passwordless 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 facial 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