



# NoPass

## REGISTRACIÓN Y AUTENTICACIÓN DE MULTI-FACTOR PARA EMPLEADOS

Contáctenos  
[sales@identite.us](mailto:sales@identite.us)  
[www.identite.us](http://www.identite.us)

### NoPass™ Tecnología de Autenticación

NoPass™ es un complemento de autenticación multifactor para usuarios remotos. Además del nombre y password del usuario, NoPass™ realiza dos factores adicionales de autenticación: algo que tiene y algo que es. Esto utiliza teléfonos inteligentes y no requiere la compra de dispositivos de autenticación de hardware adicionales para cada usuario. Tampoco utiliza SMS, que también puede ser costoso..

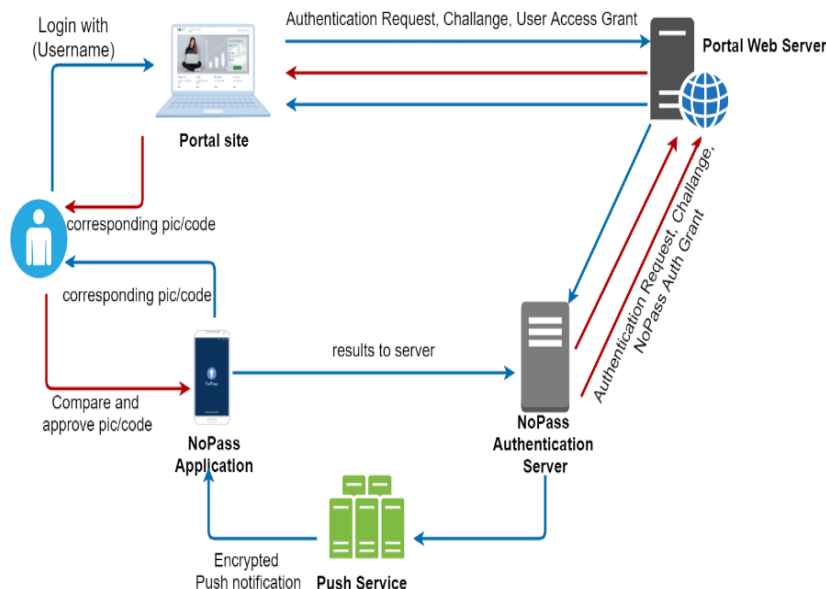


NoPass™ es una aplicación de autenticación segura que brinda las dos cosas que más se necesita: el nivel más alto de seguridad de autenticación y la interfaz de usuario más simple. Ahora puede tener la confianza de nunca preocuparse por el compromiso de sus credenciales en línea.

Junto con una seguridad muy fuerte, el usuario no necesita ingresar una contraseña. El servidor NoPass™ y la aplicación en el teléfono se encargan de todo el enlace bidireccional, y solo requieren que el usuario compare dos imágenes (un imagen y un número de 3 dígitos), luego toque el botón de aprobación, y están conectados.

Este método proporciona un millón de combinaciones encriptadas, y prácticamente no se puede comprometer por un hacker ya que los metadatos son válidos por solo unos segundos y después de eso son inútiles. Incluso si el usuario aprueba la transacción por error, podemos detectar la intrusión y bloquear la entrada al servidor.

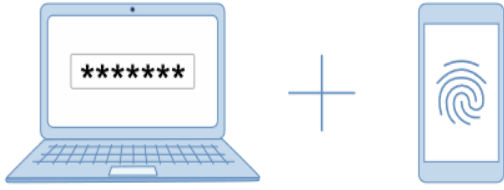
### TECNOLOGÍA AUTENTICACIÓN FULL DUPLEX™



El proceso NoPass™, Autenticación Full Duplex™ sigue un modelo de autenticación descentralizado. Esto nos permite trabajar con cualquier tipo de tecnología de autenticación de usuario tradicional, como PIN, OTP, PKI y biometría. NoPass™ tiene una arquitectura flexible para integrarse fácilmente con cualquier solución de autenticación de usuario.

Al combinar el cifrado de clave pública con la autenticación OTP rápida, NoPass™ Autenticación Full Duplex™ MFA permite el login de sesión iniciado en dispositivos móviles directo a las estaciones de trabajo a través de su dispositivo móvil. Es rápido y seguro.

## NoPass™ 2FA

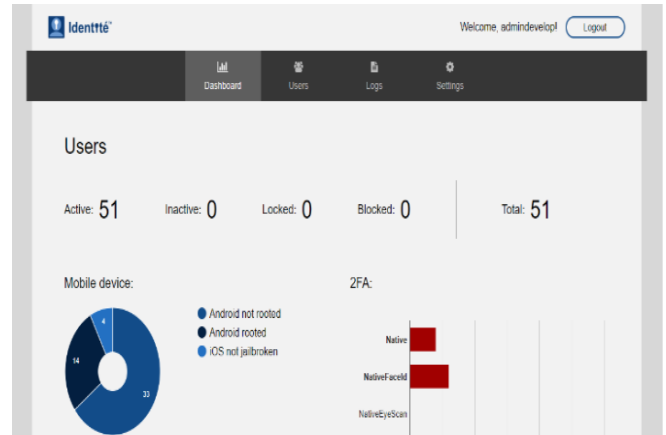


Con el aumento de phishing y otros ataques de identidad en estos tiempos, la autenticación que requiere un nombre de usuario y contraseña (como RADIUS) puede estar en riesgo. Los sofisticados esquemas de ingeniería social y las tácticas inteligentes pueden engañar incluso a los usuarios más inteligentes. Para combatir esto, NoPass™ ha presentado su solución doble factor, una característica liviana que mejora la seguridad general y se puede adaptar a los protocolos de autenticación líderes en el mercado.

## NoPass™ Panel de Administrador

Obtenga una descripción general completa de administración: uso del panel de administración de NoPass™. Device Trust Ensure - asegúrese que todos los dispositivos cumplan con los estándares de seguridad. Políticas de acceso adaptativo establezca políticas para otorgar o bloquear intentos de acceso. Acceso remoto, Acceso seguro a todas las aplicaciones y servidores.

Todos los aspectos de su sistema de autenticación NoPass™ se puede administrar desde el Panel de administración de NoPass™. Esto incluye crear y administrar aplicaciones, inscribir y activar usuarios, administrar dispositivos móviles, ajustar la experiencia del usuario de su instalación NoPass™ y más.



## Requerimientos de Infraestructura

### Interno (servidor de la empresa)

- Despliegue altamente disponible
- Soporte de Docker y Kubernetes
- Proxy inverso
- Agrupación y HA

### Nube

- Implementación en la nube privada (es decir, AWS, Azure, IBM) Implementación de alta disponibilidad
- Alta escalabilidad
- Implementar en casi todos los países
- Soporte para el auto-registro para pruebas y producción

## Características del producto

- Experiencia de usuario simple y clara para registro, autenticación y restauración
- Innovador imagen y código OTP, conveniencia del usuario y seguridad contra fuerza bruta mucho más alta
- Panel de administración fácil de usar para establecer políticas y restricciones
- Controlar la higiene del dispositivo y verificar si hay dispositivos rooteados o liberados que puedan comprometer la seguridad
- Integración flexible con cualquier autenticación de usuario existente
- Compatible con Android e iOS
- Copias de seguridad encriptadas de cuentas en la nube accesibles tanto para iOS como para Android

## Beneficiosa de NoPass™

### Seguridad

Los credenciales de inicio de sesión son únicos en todos los sitios web, nunca abandonan el dispositivo del usuario y nunca se almacenan en un servidor.

### Conveniencia

Los usuarios desbloquean los credenciales de inicio de sesión con métodos simples integrados, como lectores de huellas digitales o escaneos faciales.

### Escalabilidad

El amplio uso de teléfonos inteligentes y nuestra implementación en la nube hacen que sea muy fácil escalar cualquier autenticación existente.

### Eficiencia de Costo

Ahorre millones en costos de asistencia técnica y soporte de contraseña.

### Privacidad

Proteja a sus usuarios de fugas de credenciales y phishing de contraseña