NoPass

REGISTRACIÓN Y AUTENTICACIÓN SIN PASSWORD

Contáctenos
sales@identite.us
www.identite.us

Carga de Passwords

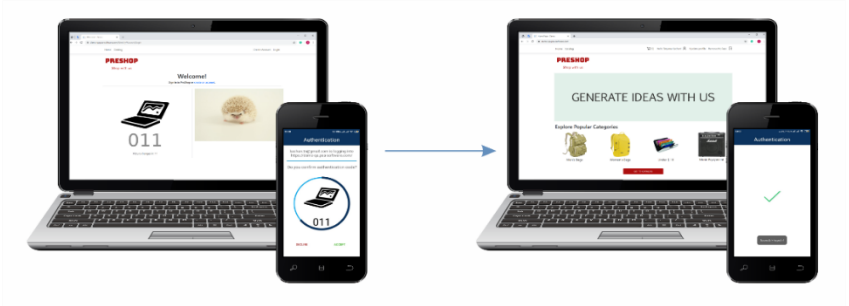
Las contraseñas son la forma más utilizada de autenticación de sitios web. La autenticación con contraseña requiere que los usuarios creen una clave que solo ellos (y el sitio web) conozcan como una forma de acceder a sus cuentas en línea.

La seguridad basada en contraseña se ha vuelto menos segura en los últimos tiempos debido a los ataques de phishing, cada día más sofisticados y los desafíos que enfrentan los usuarios para crear y administrar numerosas contraseñas. Además, el almacenamiento centralizado de millones de credenciales de usuario (incluyendo las contraseñas) en la nube o un servidor de sitio web puede proporcionar un único punto de destino para los piratas informáticos, lo que puede aumentar en gran medida el costo de una sola violación de seguridad. Los ataques en línea como Man-in-the-Middle (MitM) y Man-in-the-Browser (MitB) pueden representar una amenaza sustancial para la autenticación en línea al modificar ocultamente la comunicación entre el usuario y el servidor.

NoPass™ - Autenticación Sin Password

NoPass™ es una herramienta de registración y autenticación sin contraseña para autenticar a los usuarios que ingresan a un cliente o portal constituyente. Con teclar poco o acciones mínimas por parte de un usuario, pueden registrarse y autenticarse rápidamente con 3 factores: algo que usted sabe, algo que tiene y algo que usted es.

Sencillo y seguro

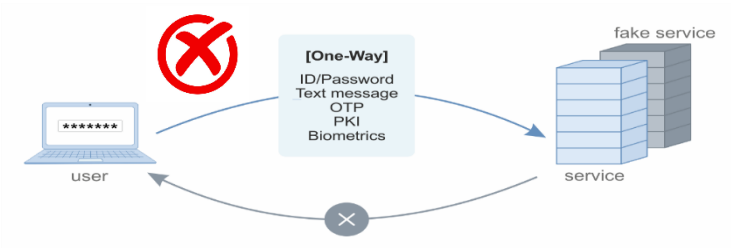


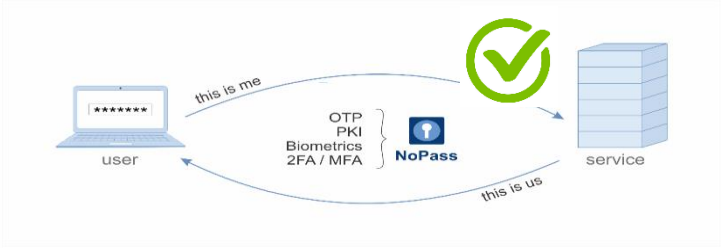
NoPass™ es una aplicación de autenticación segura que brinda las dos cosas que más necesitas: el nivel más alto de seguridad de autenticación y la experiencia de usuario más simple. Ahora puede tener la confianza de nunca preocuparse por el compromiso de sus credenciales en línea. Junto con una seguridad muy fuerte, el usuario no necesita ingresar una contraseña. El servidor NoPass™ y la aplicación en del smartphone 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 con solo tocar el botón de aprobación, están conectado.

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 junto 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.

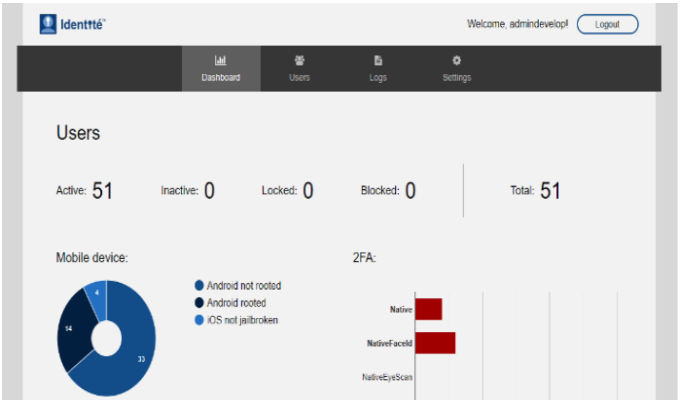




NoPass™ Panel de Administración

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 Infrastructura

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
- Inscripción progresiva con mecanografía o acciones mínimas por parte del usuario
- 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

Beneficios de **NoPass™**

✓ **Aumento de ingresos**

La experiencia de usuario mejorada ayudará a adquirir nuevos clientes y retener a los antiguos.

✓ **Seguridad**

Los credenciales de inicio de sesión son únicos en todos los sitios web, nunca salen del dispositivo del usuario y nunca se almacenan en un servidor. Prevenga el robo de identidad al eliminar los ataques internos de los credenciales comprometidos de los empleados.

✓ **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.

✓ **Privacidad**

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