NoPass

REGISTRO Y AUTENTICACIÓN SIN CONTRASEÑA PARA USUARIOS DE WINDOWS

Contáctenos
sales@identite.us
www.identite.us

Autenticación Full Duplex® segura y simple para aplicaciones de Microsoft

El repentino aumento del trabajo remoto en un mundo móvil y de aplicaciones en la nube ha desafiado a los profesionales de la seguridad de redes. El perímetro de seguridad, que ahora se extiende hasta el hogar de los trabajadores, aún debe brindar acceso seguro a una variedad de aplicaciones comerciales. Dado que los usuarios de hoy también requieren acceso a aplicaciones locales y aplicaciones en la nube, las organizaciones no pueden confiar en la arquitectura de seguridad perimetral tradicional para proteger el acceso a las aplicaciones. Los equipos de TI y ciberseguridad ahora se encargan de proporcionar acceso seguro a los recursos en un entorno híbrido de múltiples nubes. La mayor parte de la infraestructura de TI empresarial se basa en las plataformas Active Directory (local) y / o Azure (nube) de Microsoft. NoPass™ ofrece una variedad de funciones y soluciones que verifican la confianza de la fuerza laboral y cambian exitosamente hacia el trabajo remoto al implementar y hacer cumplir las prácticas de confianza cero de NoPass™.

NoPass™ es una solución de autenticación segura que le brinda las dos cosas que más necesita: el nivel más alto de seguridad de autenticación y la interfaz de usuario más simple. Ahora puede tener la confianza de no preocuparse nunca por comprometer sus credenciales en línea. La autenticación multi-factor sin contraseña de Windows NoPass™ garantiza que solo los usuarios autorizados tengan acceso a datos confidenciales en todos sus sistemas. Con NoPass™ es fácil para los usuarios autenticarse en las aplicaciones que necesitan sin comprometer la seguridad.

Integrar en AD con RADIUS

Los servicios de federación de Active Directory (ADFS) son el proveedor de identidad de facto en un entorno de Microsoft. Muchas organizaciones lo usarán para autenticar a los usuarios de Office 365 en un Active Directory local. El soporte entre los proveedores de servicios en la nube está creciendo, lo que le permite autenticar no solo a los usuarios de Office 365, sino también a los usuarios de una variedad de aplicaciones comerciales.

En determinadas circunstancias, es posible que desee solicitar la autenticación multifactor (MFA). De fábrica, ADFS solo brinda soporte para certificados X.509. Afortunadamente, existe el concepto de Adaptadores de autenticación, lo que le permite aumentar la seguridad y la simplicidad mediante un complemento MFA. En Identité™ hemos desarrollado un complemento RADIUS que le permite solicitar a los usuarios que ingresen su contraseña de AD, hacer que ejecuten dos o más factores adicionales de autenticación y enviar la respuesta al servidor NoPass™ que actúa como Cliente RADIUS, junto con las cuentas userPrincipalName, para validación y máxima seguridad de autenticación.

El proceso NoPass™, Full Duplex Authentication® sigue un modelo de autenticación descentralizado. Esta función detiene los ataques de suplantación de identidad y evita que los credenciales sean interceptados mediante un "ataque de intermediario" (MIM). NoPass™ tiene una arquitectura flexible para integrarse fácilmente con cualquier solución de autenticación de usuario.

Integración de SSO federado con Azure Directory y Office 365

Office 365 es un servicio de suscripción basado en la nube que reúne las mejores herramientas para la forma en que las personas trabajan hoy. Al combinar las mejores aplicaciones de su clase como Excel y Outlook con potentes servicios en la nube como OneDrive y Microsoft Teams, Office 365 permite que cualquier persona cree y comparta en cualquier lugar y en cualquier dispositivo.

NoPass™ proporciona un método simple y confiable para federar Active Directory local y Azure AD. La configuración de NoPass™ y Azure AD proporciona a los clientes un acceso seguro y sin problemas a Office 365.

NoPass™ brinda acceso seguro y sin problemas a sus aplicaciones móviles, en la nube y empresariales. La integración de Office 365 con NoPass™, que actúa como proveedor de identidad, se logra mediante los estándares abiertos SAML y OIDC, que admiten perfiles de usuario activos y pasivos..

MFA - más que un SMS OTP

Azure proporciona una solución SMS OTP como 2FA con el fin de aumentar la seguridad, pero con el aumento del phishing y otros ataques de identidad en nuestros días, la autenticación que requiere un nombre de usuario y contraseña (como RADIUS) puede estar potencialmente en riesgo. Los sofisticados esquemas de ingeniería social y las tácticas inteligentes pueden engañar incluso a los usuarios más expertos. Para combatir esto, NoPass™ ha presentado su solución MFA, que mejora significativamente la seguridad general y es compatible con los principales protocolos de autenticación que se encuentran en el mercado.

Asegurar el acceso a VPN y RDP Gateway para los trabajadores en casa

Ya sea que esté ejecutando sus aplicaciones de escritorio alojadas de forma local o si planea mover esas cargas de trabajo a la nube, necesita una conexión de red segura a la oficina para los trabajadores domésticos. NoPass ™ se integra con los sistemas operativos de servidor y cliente de Microsoft Windows para agregar autenticación de múltiples factores a los inicios de sesión con una solución que equilibra la seguridad y la usabilidad. Las políticas de acceso se pueden configurar para bloquear el acceso a estaciones de trabajo remotas sensibles desde dispositivos que están desactualizados o no cumplen con sus requisitos de seguridad.

NoPass™ para Windows Logon agrega la autenticación multifactor NoPass™ a los inicios de sesión del servidor y del escritorio de Windows, tanto en la consola local como en las conexiones entrantes de escritorio remoto (RDP) y VPN. Un factor será algo que tenga el usuario, un token seguro. Esto está protegido por la patente pendiente Full Duplex Authentication® de Identité que es impermeable a la suplantación de identidad. Otro factor que podría ser un usuario podría ser un token de hardware como un Yubikey. Si el dispositivo admite datos biométricos, entonces algo que sea un usuario podría ser otro factor.

Cliente nativo de Windows

El cliente de autenticación NoPass ™ para Windows proporciona el mismo multifactor que la aplicación móvil. Además, los tokens de hardware nativos

como Yubikey y otros dispositivos de terceros son compatibles con el cliente de Windows, NoPass ™ es una solución de autenticación de dos factores fácil de usar que se adapta perfectamente a los flujos de trabajo diarios de sus usuarios.

Algunos sitios web y servicios en línea permiten a los usuarios proteger sus cuentas con un código de acceso generado por dispositivos móviles que se debe ingresar manualmente y solo funciona durante un cierto período de tiempo, generalmente de 30 a 60 segundos. Tanto el cliente de autenticación Windows como Mobile NoPass ™ pueden proteger todos los sitios con credenciales únicas protegidas por Full Duplex Authentication®. Todos los usuarios mantienen todas sus cuentas y credenciales en una billetera digital virtual.

Integración de Windows Login (GINA) que incluye desbloqueo sin contraseña con teléfonos inteligentes habilitados para Bluetooth

NoPass ™ permite que los dispositivos inalámbricos equipados con Bluetooth se utilicen para la seguridad informática (inicio de sesión, autenticación, bloqueo / desbloqueo). Su teléfono móvil juega el papel de su clave de acceso desde su PC:

- Inicio de sesión automático de Windows cuando un usuario se acerca a la computadora (con el teléfono móvil).
- La computadora estará protegida con una contraseña, pero no es necesario que la ingrese manualmente.

NoPass™ es una solución de autenticación genuina con reemplazo completo de contraseña, y no solo un casillero de PC primitivo como muchos otros programas donde debe ingresar una contraseña manualmente de todos modos para iniciar sesión.

Opciones de Implementación

En Sitio

- Implementación de alta disponibilidad
- Compatibilidad con Docker y Kubernetes
- Proxy inverso
- Agrupación en clústeres y alta disponibilidad

Nube

- Implementación de nube privada (es decir, AWS, Azure, IBM)
- Alta escalabilidad
- Implementar en casi todos los países
- Soporte para autoinscripción para pruebas y producción

Características del producto

- Producto de autenticación sin contraseña simple y seguro
- El proceso NoPass ™, Full Duplex Authentication® sigue un modelo de autenticación descentralizado. Funciona junto con cualquier tecnología de autenticación de usuario tradicional, como PIN, OTP, PKI y biometría
- SSO completamente sin contraseña, fácil de instalar, satisface las necesidades de cualquier organización también gana
- Imagen innovadora y código OTP, conveniente para el usuario y seguridad de fuerza bruta mucho mayor
- Descripción general completa de la administración: mediante el panel de administración, establezca políticas y restricciones como requisitos geográficos y de dispositivo
- Arquitectura flexible para integrarse fácilmente con cualquier autenticación de usuario existente

Beneficios de **NoPass™**

Seguridad

Los credenciales de inicio de sesión son únicos en cada sitio web, nunca abandonan el dispositivo del usuario y nunca se almacenan en un servidor

Conveniencia

Los usuarios desbloquean las 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 soporte técnico y de apoyo técnico para el password

Privacidad

Proteja los usuarios de fugas de credenciales y phishing de contraseñas