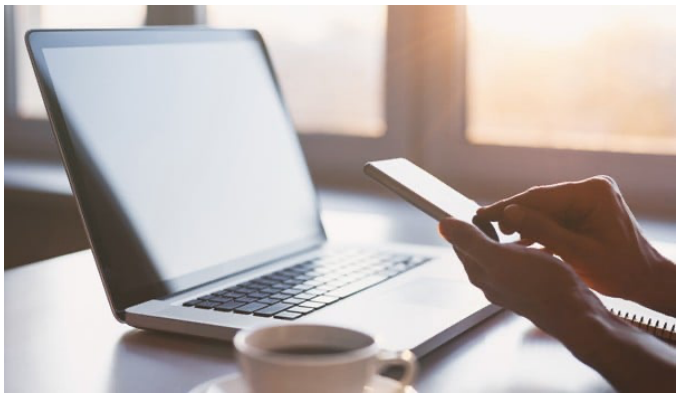
NoPass

NoPass™ MFA para el personal

Contáctanos
sales@identite.us
www.identite.us

NoPass™ MFA para el personal

NoPass™ conecta el acceso del personal con un dispositivo inscrito. Sus rutas documentadas incluyen federación SAML/OIDC, RADIUS y Desktop Unlock. Elige la integración y los factores de confirmación adecuados para tu entorno.

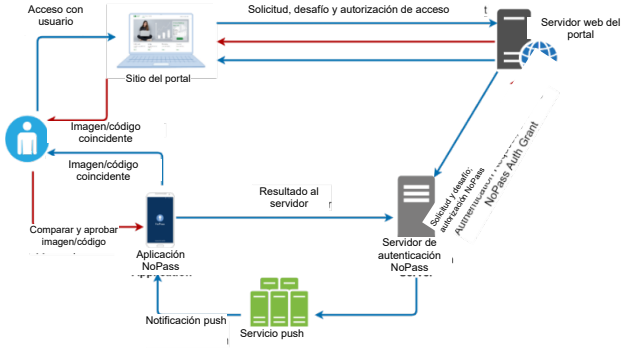


Una experiencia de acceso clara ayuda al personal a reconocer la solicitud y decidir. NoPass™ reúne el intercambio con el dispositivo inscrito y las herramientas administrativas para planificar el acceso y la recuperación.

En una integración configurada, la aplicación solicita autenticación y el servicio NoPass™ conecta la solicitud con el dispositivo inscrito. La persona compara la imagen y el número y confirma o rechaza según la configuración local. La aplicación recibe el resultado y conserva sus permisos y controles de ejecución. Define con el equipo responsable los factores, el vencimiento y la recuperación antes de ampliar el acceso.

Tecnología FULL DUPLEX AUTHENTICATION®

Full Duplex Authentication® incorpora la relación configurada entre la app inscrita y el servicio de autenticación. La persona participa en la decisión; la aplicación mantiene el control de permisos y ejecución. Evalúa la integración y su recuperación.





Conectar NoPass™ a tu empresa

Las rutas documentadas conectan NoPass™ con aplicaciones y puntos de acceso. Para una integración RADIUS, identifica el gateway, la configuración admitida y el equipo responsable de la política de acceso.

Para SSO, comienza con una federación SAML/OIDC concreta. La documentación muestra una ruta con Keycloak y NoPass™. Confirma las versiones, el mapeo de cuentas y la recuperación para la aplicación elegida.

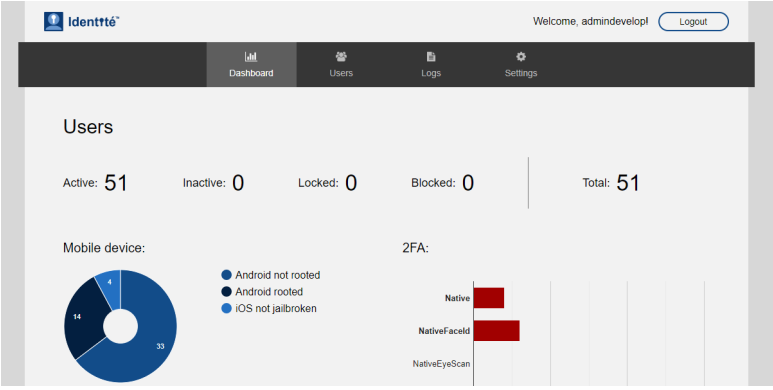
Planifica los dispositivos y la recuperación



Elige los dispositivos, factores y versiones admitidos para la integración. La ruta Desktop Unlock utiliza componentes de Windows y un dispositivo inscrito. Define quién autoriza la inscripción, revoca un equipo perdido y restablece el acceso. Comprueba cómo se gestionan las sesiones existentes, los cambios de dispositivo y la falta de conexión antes del despliegue.

Panel de administración NoPass™

Reúne usuarios, dispositivos y actividad de autenticación en la consola administrativa. Define responsables de inscripción, acceso y soporte para tu entorno.



Planifica la gestión de cuentas y dispositivos, los factores configurados y la recuperación. Asigna las acciones administrativas al equipo responsable.

Planificar el servicio

Servicio instalado

- Acordar disponibilidad y respaldo
- Confirmar el método de instalación
- Planificar red y acceso al servicio
- Probar respaldo y restauración

Entorno elegido

- Definir la ubicación del servicio
- Definir la recuperación del servicio
- Dimensionar la carga prevista
- Acordar ubicación y datos
- Asignar inscripción y soporte

Funciones del producto

Registro, autenticación y recuperación con una experiencia sencilla y clara.

- Define quién puede inscribirse y cómo se valida su cuenta.

• Dispositivo inscrito y factores configurados para el entorno.

- Full Duplex Authentication® incorpora una comprobación de la relación app/servicio y la decisión de la persona.
- Acordar los factores y la política para la integración elegida.
- Política de dispositivos.
- Elige una ruta de federación, RADIUS o Windows documentada y confirma su configuración.

- Define el respaldo y la recuperación de cuentas con el equipo responsable.

Beneficios de NoPass™
Seguridad

La app inscrita comprueba su relación configurada con el servicio de autenticación.

Comodidad

La confirmación local depende del dispositivo y de la configuración elegida.

Despliegue gradual
Evalúa una integración y amplía el acceso con evidencia.

Eficiencia de costos

Evalúa el esfuerzo de soporte.

Privacidad

Un acceso claro para la persona y control para tu aplicación.