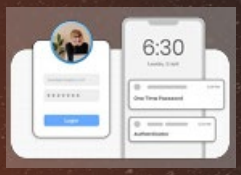
Ficha de Producto

AUTENTICADOR MULTIFACTOR



Validar la identidad del usuario a través de una experiencia personalizada.

Ofrecemos una solución altamente personalizable basada en tus necesidades. Puedes ahorrar hasta 5 veces en comparación con otros proveedores de servicios, con facilidades adicionales como más de 15 métodos de autenticación que son fáciles de configurar y gestionar. Nuestra propuesta de valor es nuestro soporte al cliente de clase mundial 24/7 proporcionado por nuestro equipo de expertos.

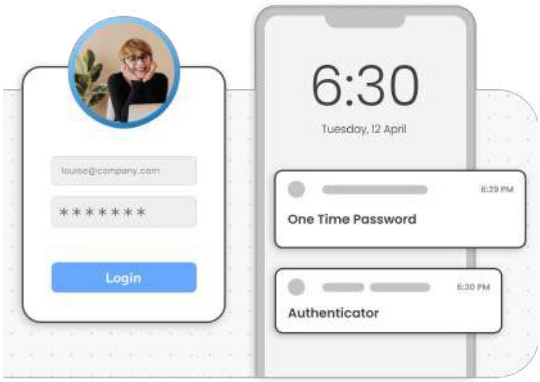
miniOrange

OTP por Email/SMS

SMS / Email con Enlace

Notificaciones Push via mO app

Preguntas de Seguridad



Hardware Token Yubikey

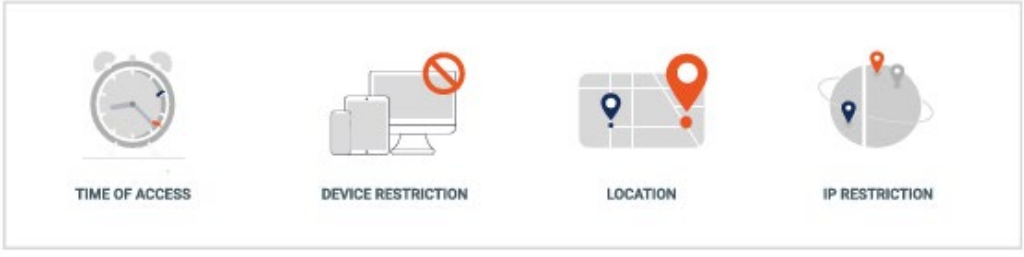
Autenticador Google

Autenticador miniOrange

Autenticador Microsoft

Autenticador Adaptativo

El administrador tiene privilegios para restringir los métodos de 2FA (autenticación de dos factores) para los usuarios finales, de modo que los usuarios solo puedan utilizar métodos de 2FA específicos. El administrador puede establecer el método de 2FA predeterminado para los usuarios, evitando el paso adicional donde cada usuario configura su propio método. Los usuarios solo podrán ver los métodos de 2FA permitidos en su perfil de usuario.



Restringir Métodos de 2FA para Usuarios Finales

El administrador tiene privilegios para restringir los métodos de autenticación de dos factores (2FA) para los usuarios finales, de modo que los usuarios solo puedan utilizar métodos específicos de 2FA. El administrador puede establecer un método de 2FA predeterminado para los usuarios, evitando el paso adicional de que cada usuario configure su propio método. Los usuarios solo podrán ver los métodos de 2FA permitidos en su perfil de usuario.

Métodos Alternativos de Inicio de Sesión con 2FA

Habilita la opción de "olvidó el teléfono" con preguntas de seguridad y OTP (contraseña de un solo uso) a través de un correo electrónico alternativo. Esta opción puede ser utilizada cuando los usuarios no tienen acceso a los dispositivos principales donde se configuró el 2FA. Los usuarios pueden usar el método alternativo que hayan configurado, como preguntas de seguridad o OTP enviado a un correo electrónico alternativo.

2FA Basado en Roles

La autenticación basada en roles o 2FA basado en roles es un enfoque para restringir el acceso al sistema a usuarios autorizados. Ofrecemos la opción de gestionar usuarios según sus roles y proporcionarles el acceso necesario. El administrador puede habilitar o deshabilitar el 2FA para un rol en particular y para cualquier aplicación.

Casos de Uso

MFA para Autenticación VPN-RADIUS

miniOrange proporciona autenticación de dos factores sobre la autenticación VPN actuando como un servidor RADIUS. Podemos configurar nuestro producto de autenticación de tres formas posibles con su servidor RADIUS:

I. Lado a Lado
2. Incluir y Extender
3. RADIUS Personalizado

MFA para Inicio de Sesión en Windows y Acceso RDP

El 2FA en Windows siempre verifica las identidades antes de permitir el acceso, dificultando que usuarios no autorizados accedan a tu cuenta de Microsoft Windows. El Proveedor de Credenciales de miniOrange puede instalarse en los sistemas operativos de cliente y servidor de Microsoft Windows para habilitar la autenticación de dos factores en el Escritorio Remoto (RDP) y en el inicio de sesión local de Windows.

MFA para Inicio de Sesión en Linux y Acceso SSH

El Módulo de Autenticación de Dos Factores (2FA) de miniOrange para SSH proporciona una manera segura de iniciar sesión en servidores Linux que mejora la seguridad y hace que los ataques de fuerza bruta sean más difíciles. La autenticación de dos factores sobre el acceso SSH agrega una capa extra de seguridad para aumentar la certeza de la identidad y reducir riesgos y exposiciones.

MFA para Infraestructura de Escritorio Virtual (VDI)

La Infraestructura de Escritorio Virtual ofrece una solución completa para gestionar y proporcionar acceso a entornos de escritorio virtualizados alojados en el centro de datos. El MFA para Infraestructura de Escritorio Virtual permite a las organizaciones simplificar la administración de forma segura, reducir los costos operativos, aumentar la utilización de los activos de TI existentes y mejorar la seguridad, pasando de un entorno de escritorio tradicional vulnerable a uno habilitado con MFA en VDI.