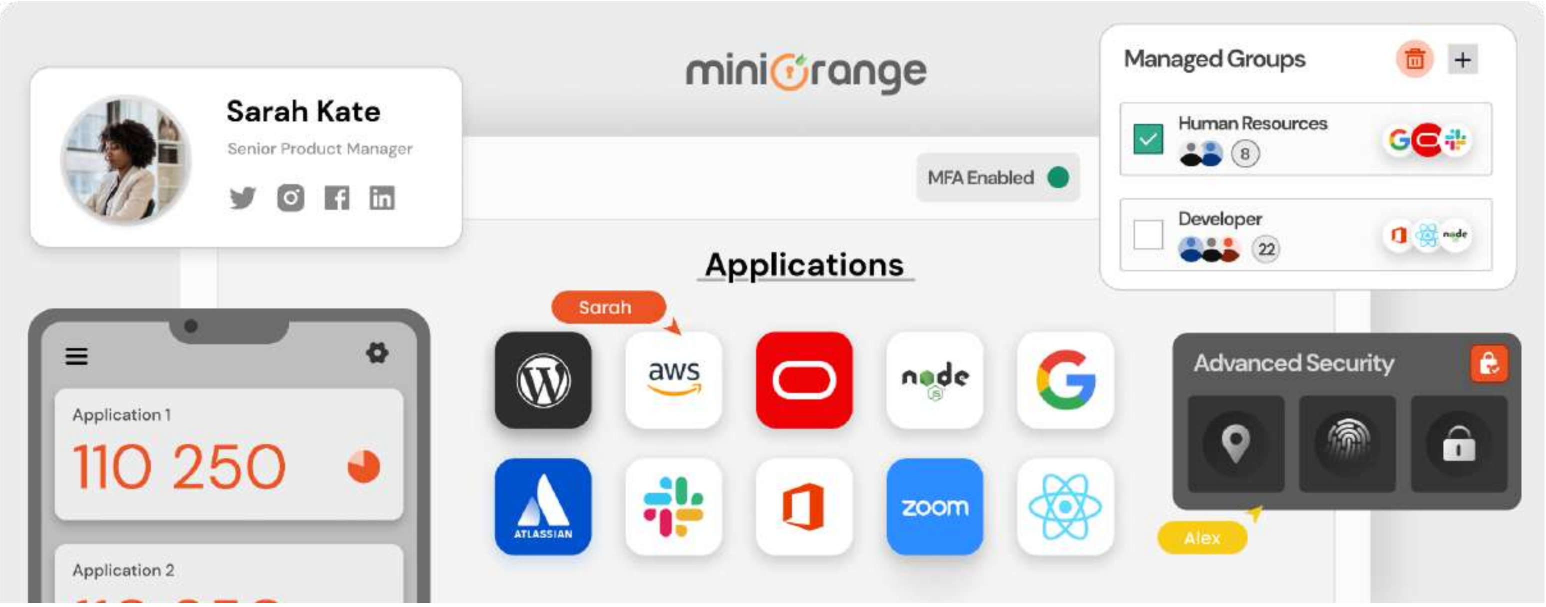
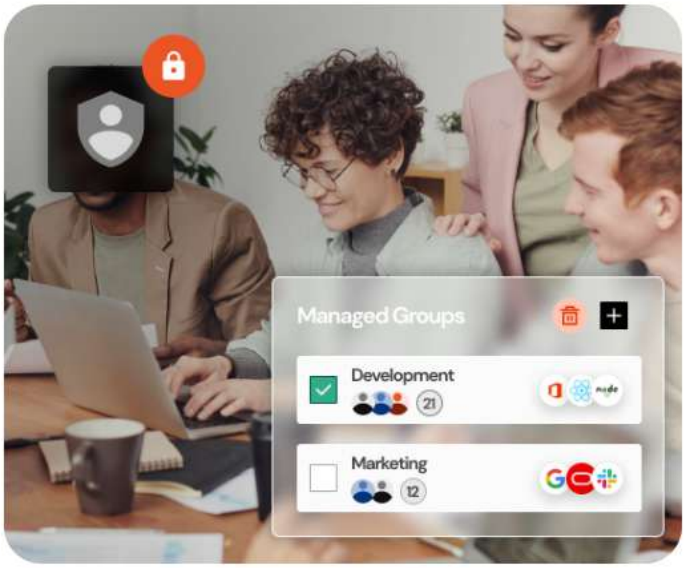
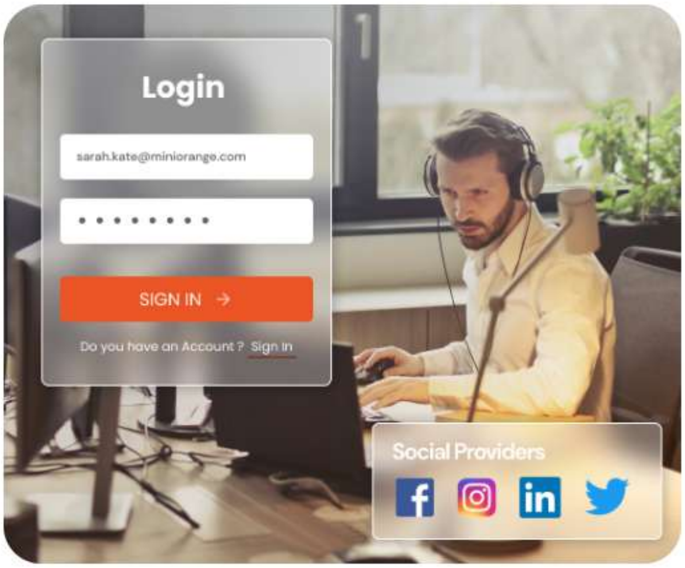
Title: miniOrange Identity & Access Management



Title: Securing user identities and their access





Workforce Identity

Protect and empower your employees, contractors and partners with simple and secure access to business resources.

Learn More

Customer Identity

Helps organizations to manage customer identities and data, as well as control customer access to applications and services.

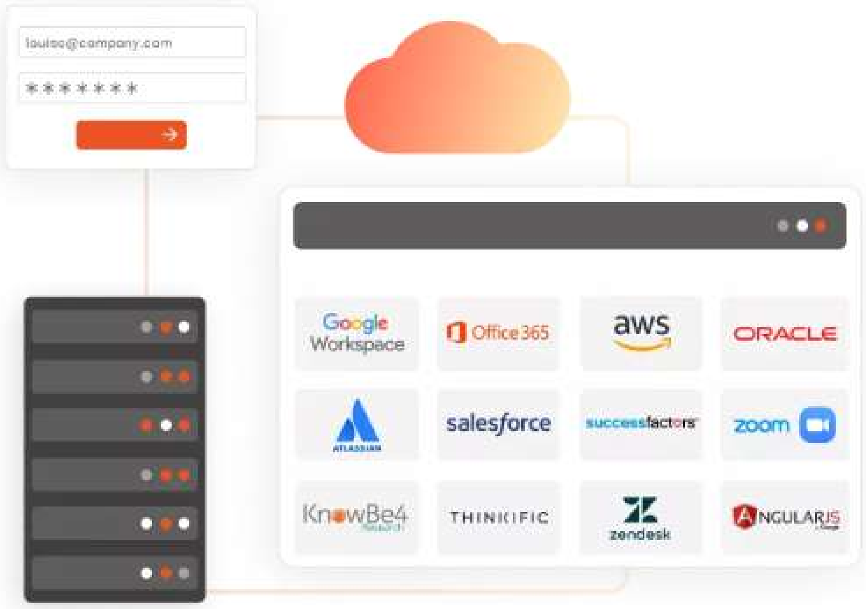
Learn More

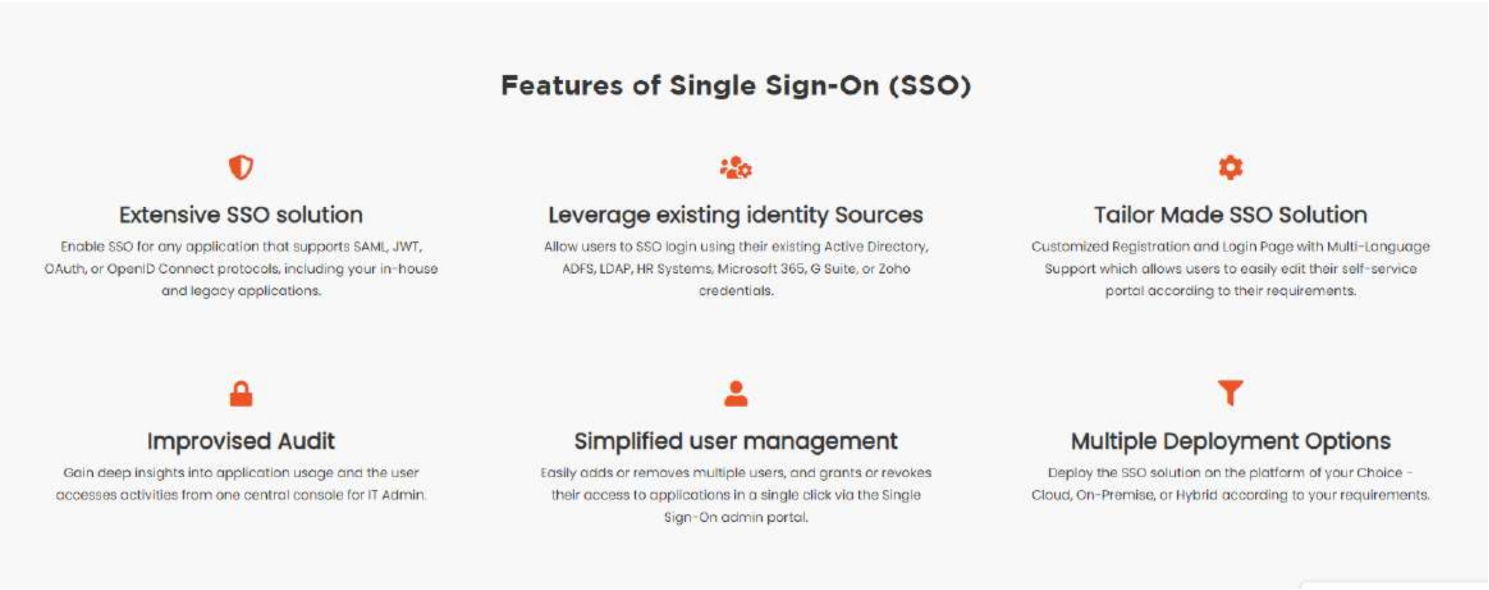
PRODUCTS

Single Sign-On (SSO)

A solution that allows users to get one-click secure access to multiple On-Premise, SAAS, and Cloud-based applications using a single username and password.

- A single dashboard to access enterprise applications
- Customize access policies per application
- Get deep insights into application usage and user access





Features of Single Sign-On (SSO)

Extensive SSO solution

Enable SSO for any application that supports SAML, JWT, OAuth, or OpenID Connect protocols, including your in-house and legacy applications.

Leverage existing identity Sources

Allow users to SSO login using their existing Active Directory, ADFS, LDAP, HR Systems, Microsoft 365, G Suite, or Zoho credentials.

Tailor Made SSO Solution

Customized Registration and Login Page with Multi-Language Support which allows users to easily edit their self-service portal according to their requirements.

Improvised Audit

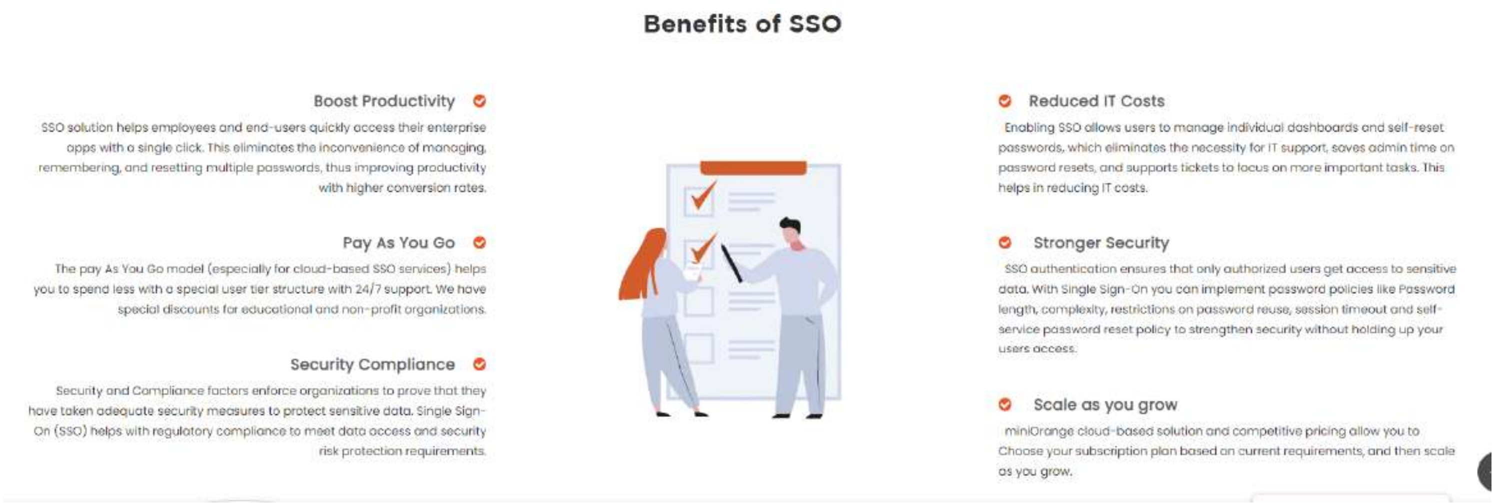
Gain deep insights into application usage and the user accesses activities from one central console for IT Admin.

Simplified user management

Easily adds or removes multiple users, and grants or revokes their access to applications in a single click via the Single Sign-On admin portal.

Multiple Deployment Options

Deploy the SSO solution on the platform of your Choice - Cloud, On-Premise, or Hybrid according to your requirements.



Benefits of SSO

Boost Productivity

SSO solution helps employees and end-users quickly access their enterprise apps with a single click. This eliminates the inconvenience of managing, remembering, and resetting multiple passwords, thus improving productivity with higher conversion rates.

Pay As You Go

The pay As You Go model (especially for cloud-based SSO services) helps you to spend less with a special user tier structure with 24/7 support. We have special discounts for educational and non-profit organizations.

Security Compliance

Security and Compliance factors enforce organizations to prove that they have taken adequate security measures to protect sensitive data. Single Sign-On (SSO) helps with regulatory compliance to meet data access and security risk protection requirements.

Reduced IT Costs

Enabling SSO allows users to manage individual dashboards and self-reset passwords, which eliminates the necessity for IT support, saves admin time on password resets, and supports tickets to locus on more important tasks. This helps in reducing IT costs.

Stronger Security

SSO authentication ensures that only authorized users get access to sensitive data. With Single Sign-On you can implement password policies like Password length, complexity, restrictions on password reuse, session timeout and self-service password reset policy to strengthen security without holding up your users access.

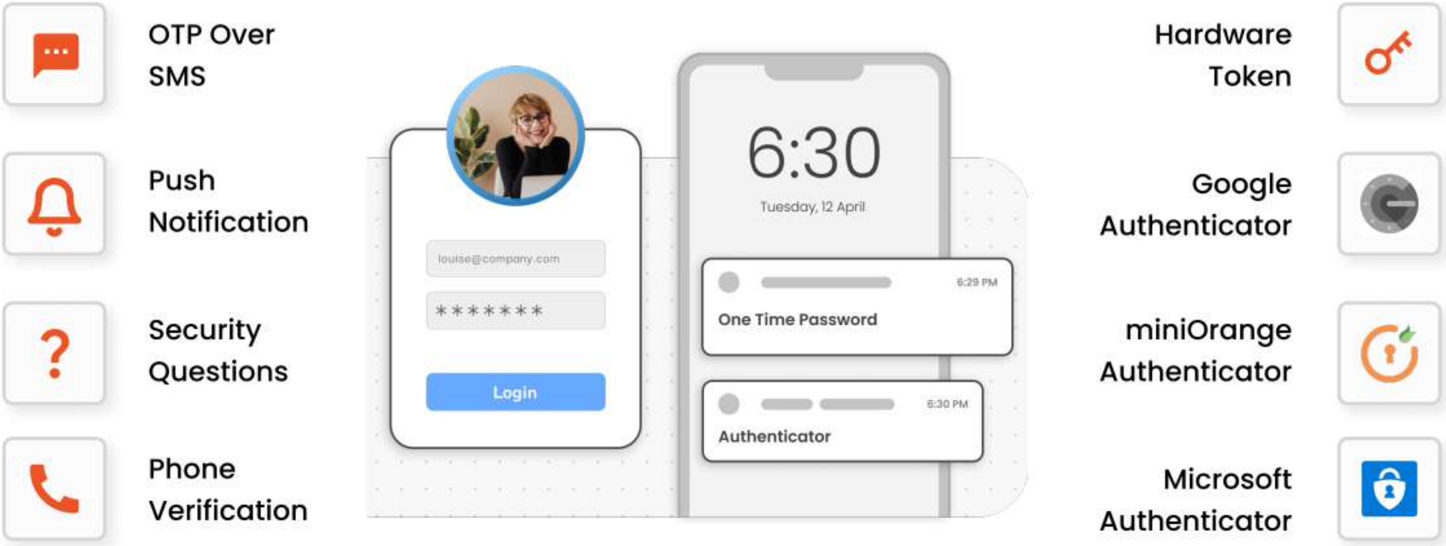
Scale as you grow

miniOrange cloud-based solution and competitive pricing allow you to Choose your subscription plan based on current requirements, and then scale as you grow.

Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is an advanced level of authentication with two or more levels of security factors. Ensuring the correct identity has access to your sensitive information.

- For web apps, VPNs, VDIs, Network Devices, and Windows/Linux
- 15+ authentication methods



Benefits of Multi-Factor Authentication (MFA)

Enhanced security

Multi-Factor Authentication (MFA) adds an extra layer of security, reducing the chances of an attacker gaining access to the system.

Increased productivity and flexibility

Employees may securely access business apps and resources from practically any device and location, without jeopardising the company's network.

Fraud Prevention

Multi-Factor Authentication (MFA) adds an additional degree of protection by ensuring that everyone is who they say they are, preventing unwanted access.

Improved user trust

When employing Multi Factor Authentication (MFA), users may secure the protection of their personal information without exerting additional effort.

Reduced management cost

You'll observe less suspicious behaviour on client accounts if you use **Multi-Factor Authentication** (MFA), and you'll spend less money on security management as a result.

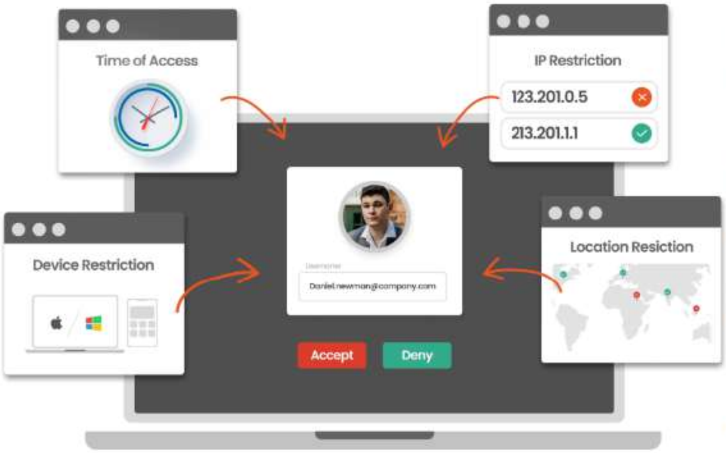
Adaptability for different use cases

Additional security is required when processing high-value transactions or accessing sensitive information from unknown networks and devices, such as geolocation, IP address, and time since the last login.

The Future of Workplace Security - Adaptive / Risk-based Authentication

Adaptive Authentication provides an extra edge to MFA security based on risk and access provided by the security admin to control user access.

Adaptive Authentication (also known as **Risk-based Authentication**) detects fraudulent attempts based on predetermined risk criteria and prompts customers to complete an additional authentication step to confirm their identities.



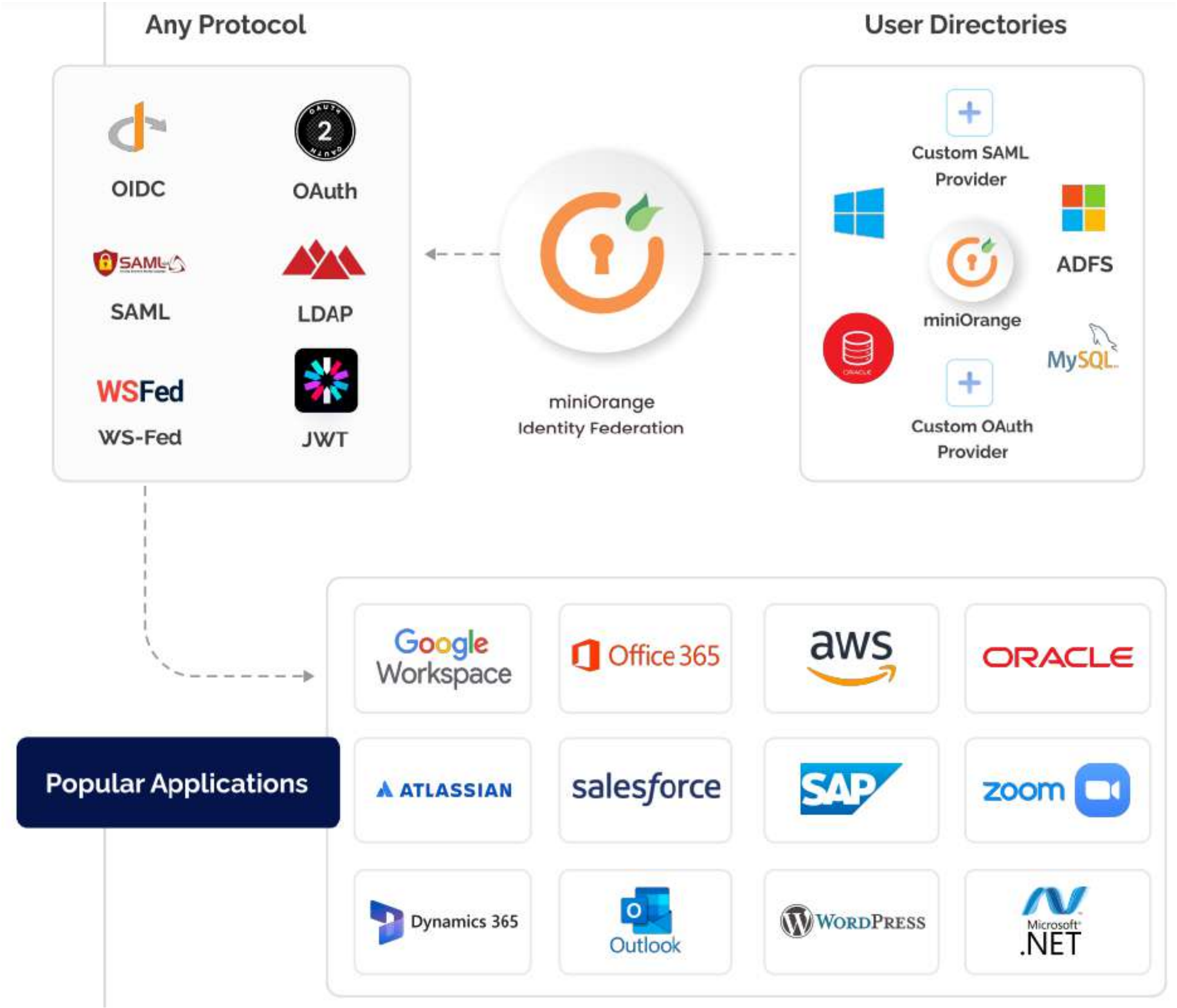
Adaptive / Risk-based authentication takes advantage of real-time analytics to get a complete picture of the circumstances surrounding each login.

When a user tries to sign in, a **adaptive authentication** system looks at things like:

- **Device** - Is the employee using their personal laptop instead of using a company-issued laptop?
- **Location** - Is the employee trying to access a system using a public network rather than the company's network? Or is the employee in another time zone?
- **IP Address** - Is the employee connecting from a known IP? Or Is it info from another country?
- **Sensitivity** - Is the requested file critical to the company's operations? Is it a little bit of knowledge, or is it significant?

Identity Brokering Service

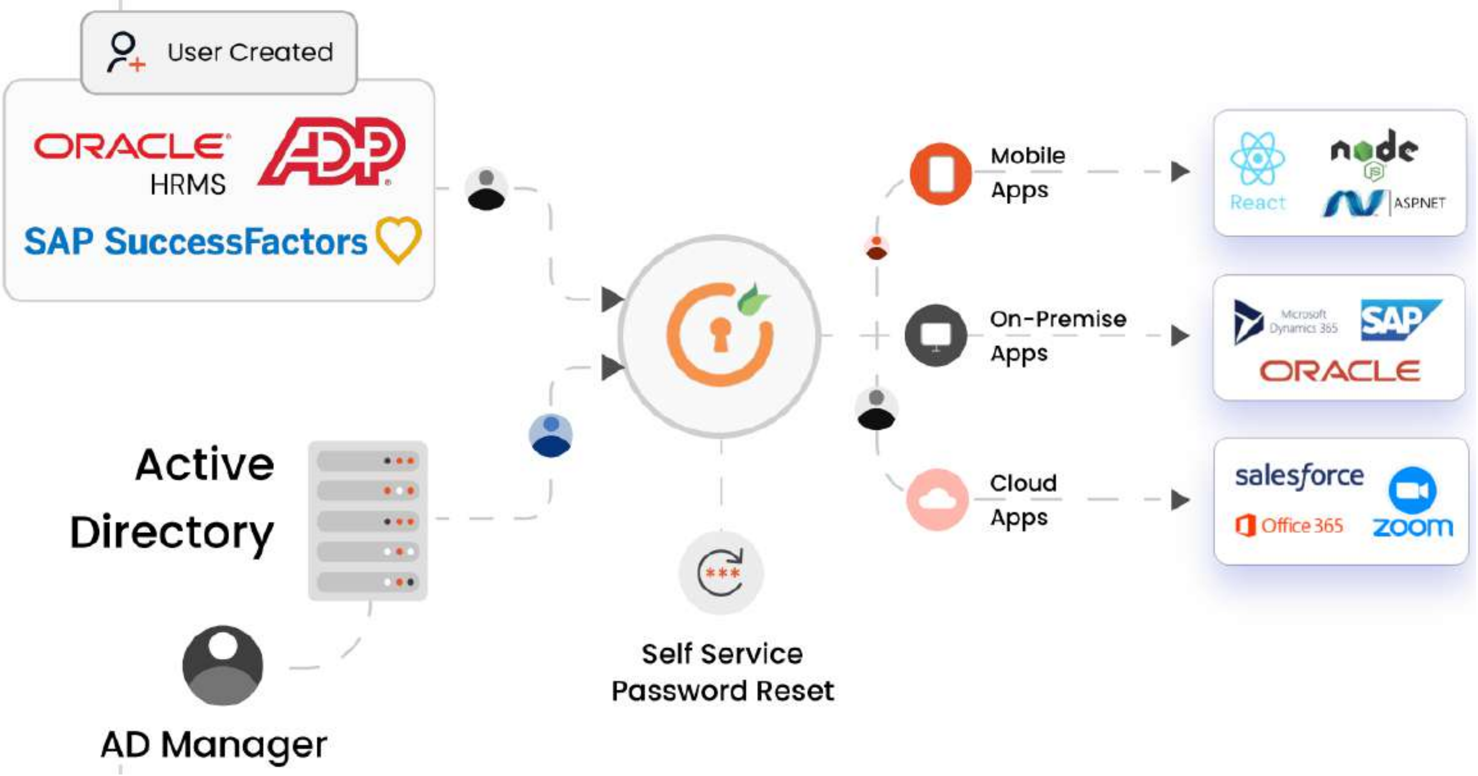
To establish trust between parties that want to use online identities of one another. Identity Broker is a service that connects multiple Service Providers(SPs) with different Identity Providers(IdPs).



User Lifecycle Management

miniOrange automates the process of creating, deleting, and managing user accounts across multiple applications and services, simplifying user management and sync across platforms and reducing the risk of errors or security vulnerabilities to your organization.

- Built in standardized support for SCIM, API, Webhooks and JIT for all your user lifecycle management needs across AD/LDAP, HR system, and any IdP
- Keep user data sync across all your platforms with timely bidirectional automated sync feature
- Quickly add, modify, or delete users with bulk upload and customizable attribute mapping options


User Created
ORACLE HRMS
ADP
SAP SuccessFactors
Active Directory
AD Manager
Self Service Password Reset
Mobile Apps
On-Premise Apps
Cloud Apps
React
node
ASP.NET
Microsoft Dynamics 365
SAP
ORACLE
salesforce
Office 365
zoom