oneIdP
Zero Trust Access

Product of
Scalefusion

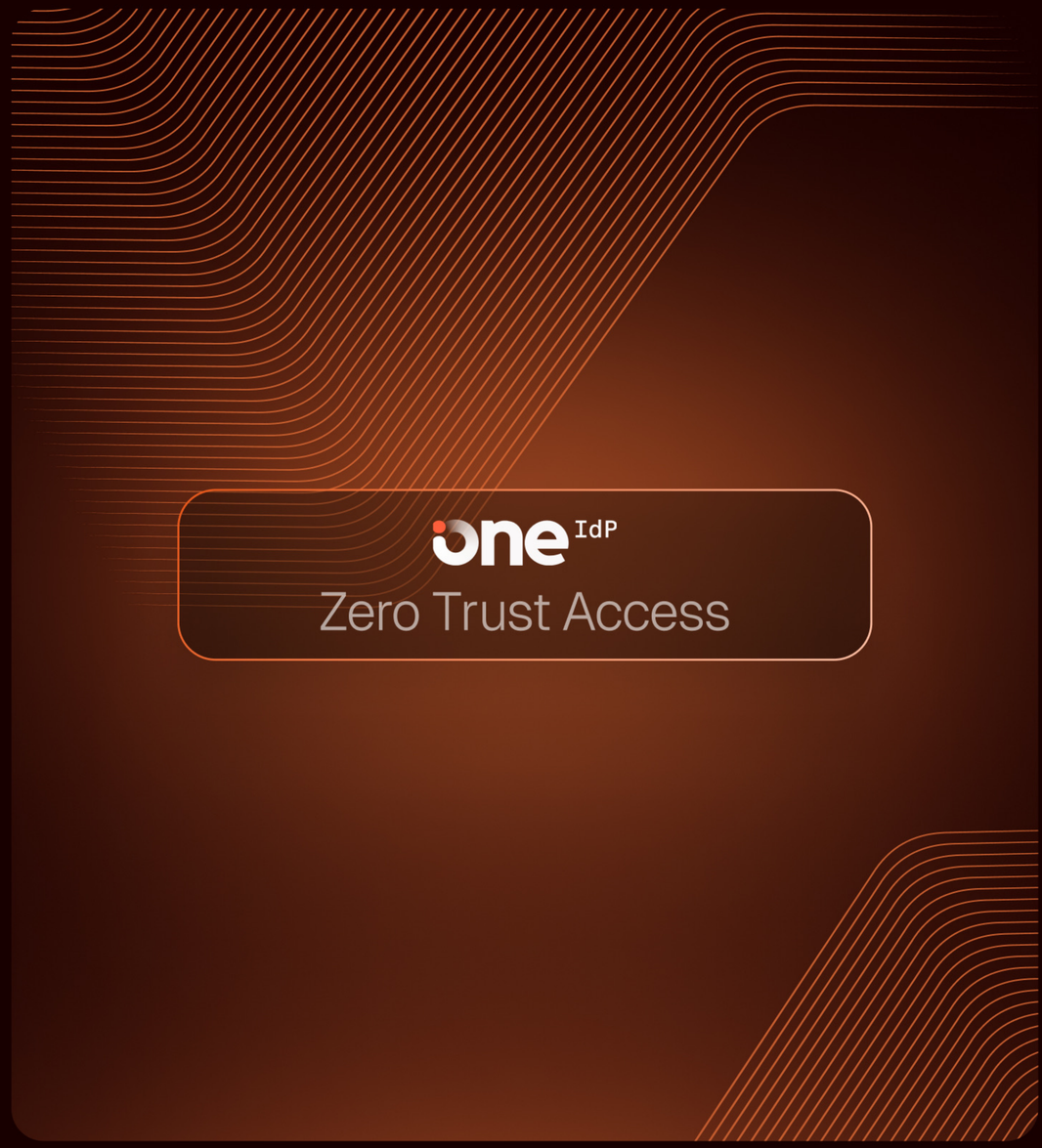
Enabling UEM-driven Zero Trust Access

Introduction

Most Zero Trust Access (ZTA) solutions are good at verifying user identity—but often completely overlook the device's security posture. This narrow approach creates a critical blind spot: even if the user is legitimate, the device might not be. And when unmanaged (Not managed by a Unified Endpoint Management) or non-compliant devices gain access to sensitive corporate data, the consequences can be severe.

This is where **UEM-driven Zero Trust Access** redefines the game. By tightly coupling user authentication with real-time device compliance, organizations can confidently differentiate between trusted and untrusted endpoints. It's not just about who is logging in, but also what they're logging in from.

Scalefusion OneIdP bridges this critical gap by deeply integrating with Unified Endpoint Management (UEM) to deliver context-aware, policy-driven access control. With every access attempt, OneIdP evaluates user identity, device status, location, network context, and more—ensuring that **only verified users on compliant, managed devices** can reach corporate email and apps. Read on to explore how OneIdP powers secure and efficient access management in real-world scenarios.



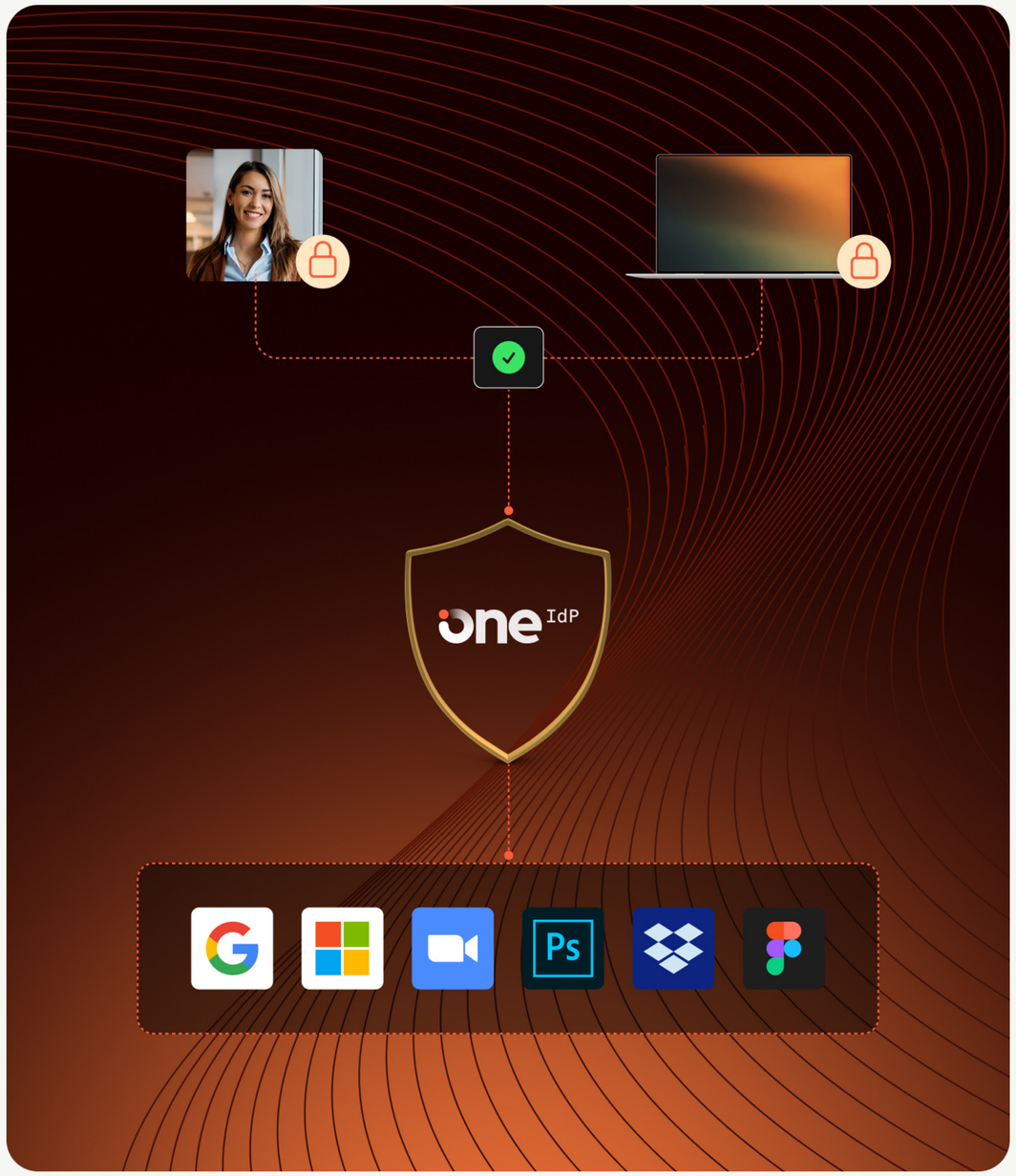
Single sign-on based on device and browser signals

Employees use multiple applications throughout their workday—email, CRM, collaboration tools, and cloud storage. Remembering multiple passwords or repeatedly logging in disrupts workflow and increases security risks. OneIdP's Single Sign-On (SSO) uses device and user signals for advanced, context-aware access control to enable employees to access all corporate applications and emails with a single set of credentials.

- Enhanced security by reducing password-related risks
- Improved productivity with frictionless access to business tools.

Use case

An employee needs access to Google Workspace, Salesforce, and Slack throughout the day. Scalefusion UEM authenticates the device and enables conditional SSO based on device and browser signals. Instead of logging in separately to each app, OneIdP's SSO allows them to sign in once and instantly access all required platforms.



USE CASES

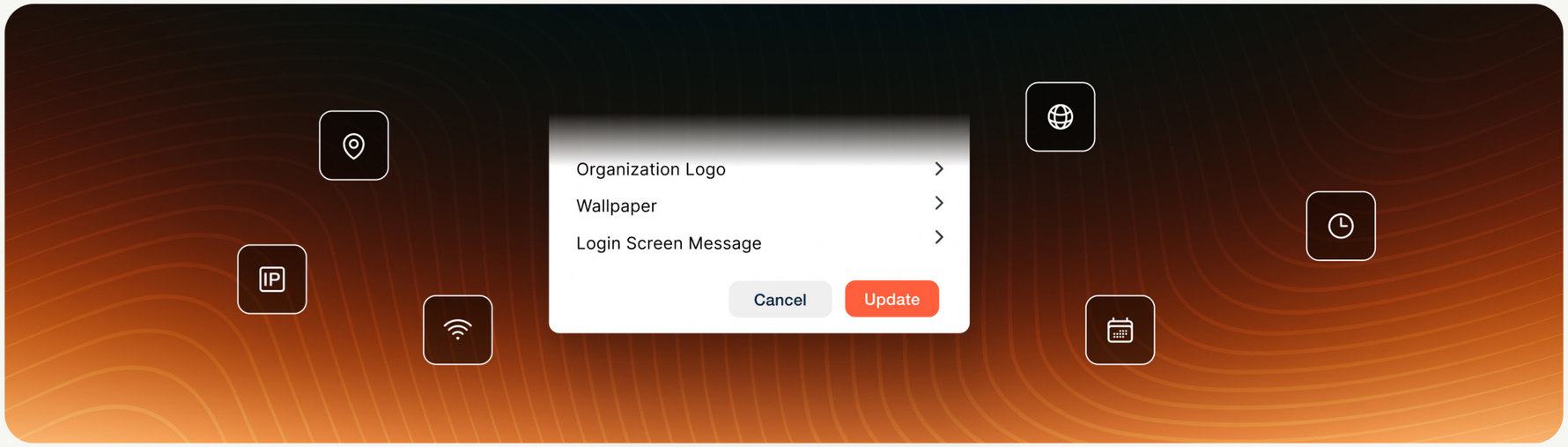
Seamless device authentication with *OneIdP*

OneIdP transforms how users login to their devices by eliminating local passwords and replacing them with seamless, policy-driven authentication using trusted Identity Provider (IdP) credentials—like Google Workspace, Microsoft Entra ID, AWS or Okta.

Users login via a custom-branded login screen and sign in using their trusted IdP credentials—instead of local passwords. This screen not only reinforces brand identity but also enforces Zero Trust by verifying context-aware signals—like device compliance, location, WiFi, IP, date, time and network —before granting access.

With OneIdP every login becomes an extension of your security posture:

- Passwords are replaced with secure IdP credentials
- Devices are authenticated based on Scalefusion UEM compliance
- Access is granted only under trusted conditions



Secure developer access with device authentication

The development team at BaseMobility works on high-priority projects using GitHub and Jira. To prevent unauthorized access to code repositories, the IT team wants to enforce IdP driven logins only from Scalefusion UEM managed devices to secure access on critical applications like GitHub and Jira.

Use case- *Unmanaged device access blocked*

A developer tries to log into GitHub from their personal laptop. Although they enter valid credentials, access is denied—because the device isn't managed by Scalefusion UEM. With OneIdP device authentication, login is allowed only from Scalefusion UEM-managed devices under specific conditions, ensuring that corporate apps are accessed securely.

Use case- *Access allowed for Scalefusion UEM-managed device*

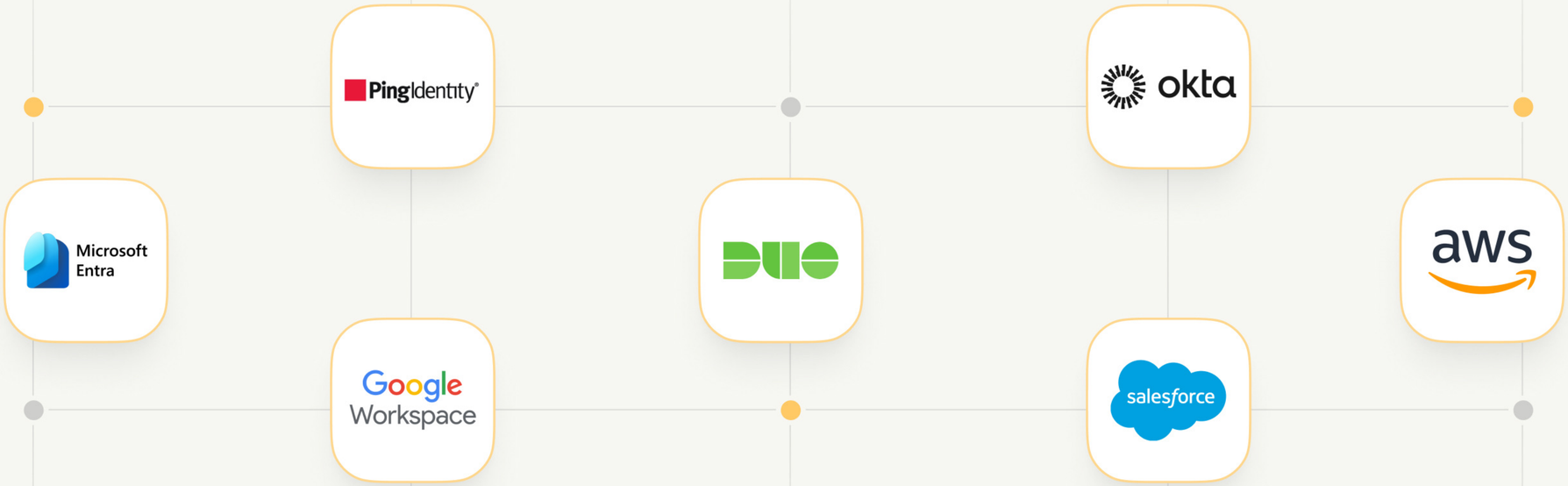
The same developer switches to their company-issued, Scalefusion UEM-managed laptop. This time, OneIdP validates the device, and the user is granted direct access using their IdP credentials—no local password required. The login screen is custom-branded, and the experience is seamless, secure, and policy-driven.

Identity Federation with leading providers

Enterprises use multiple Identity Providers (IdPs) like Microsoft Entra ID (Azure AD), Okta, and Google Workspace to authenticate users. OneIdP integrates with these providers, offering a unified identity framework across different authentication sources—ensuring seamless, federated access to corporate applications.

Use case

An enterprise using Microsoft Entra ID (Azure AD) for workforce authentication integrates OneIdP, allowing employees to access both cloud and on-prem applications with a unified identity across platforms.



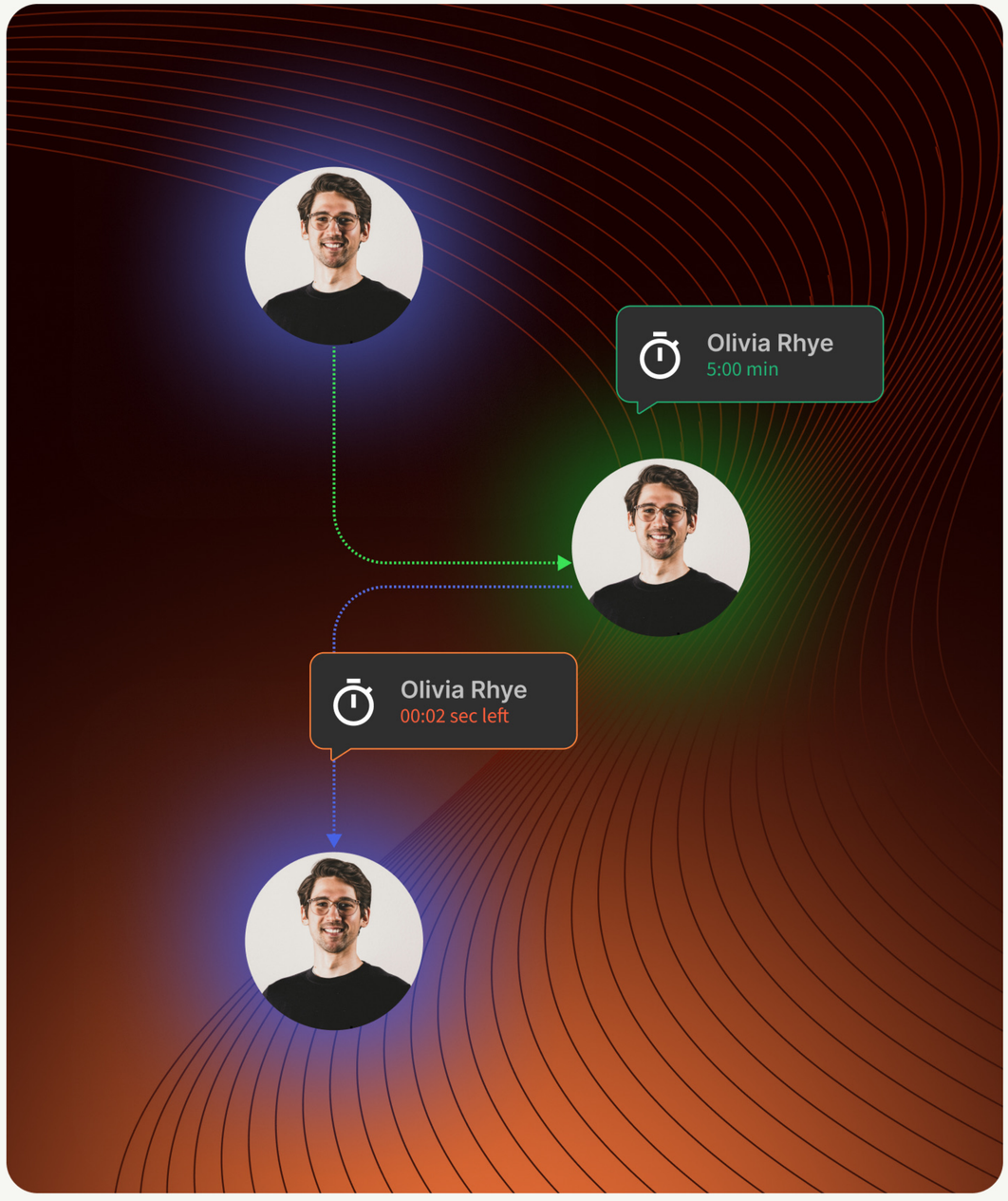
Elevate standard employee privileges with *Just-In-Time Admin* access

Permanent admin privileges increase security risks. OneIdP's Just-In-Time Admin Access (JIT) ensures that elevated access is granted only when needed and for a limited time—reducing the chances of privilege misuse or insider threats.

- Elevate standard users to temporary admins
- Automatic revocation of elevated access rights once task is completed
- Adopt a zero-trust security model
- Track all activities performed during elevated access sessions

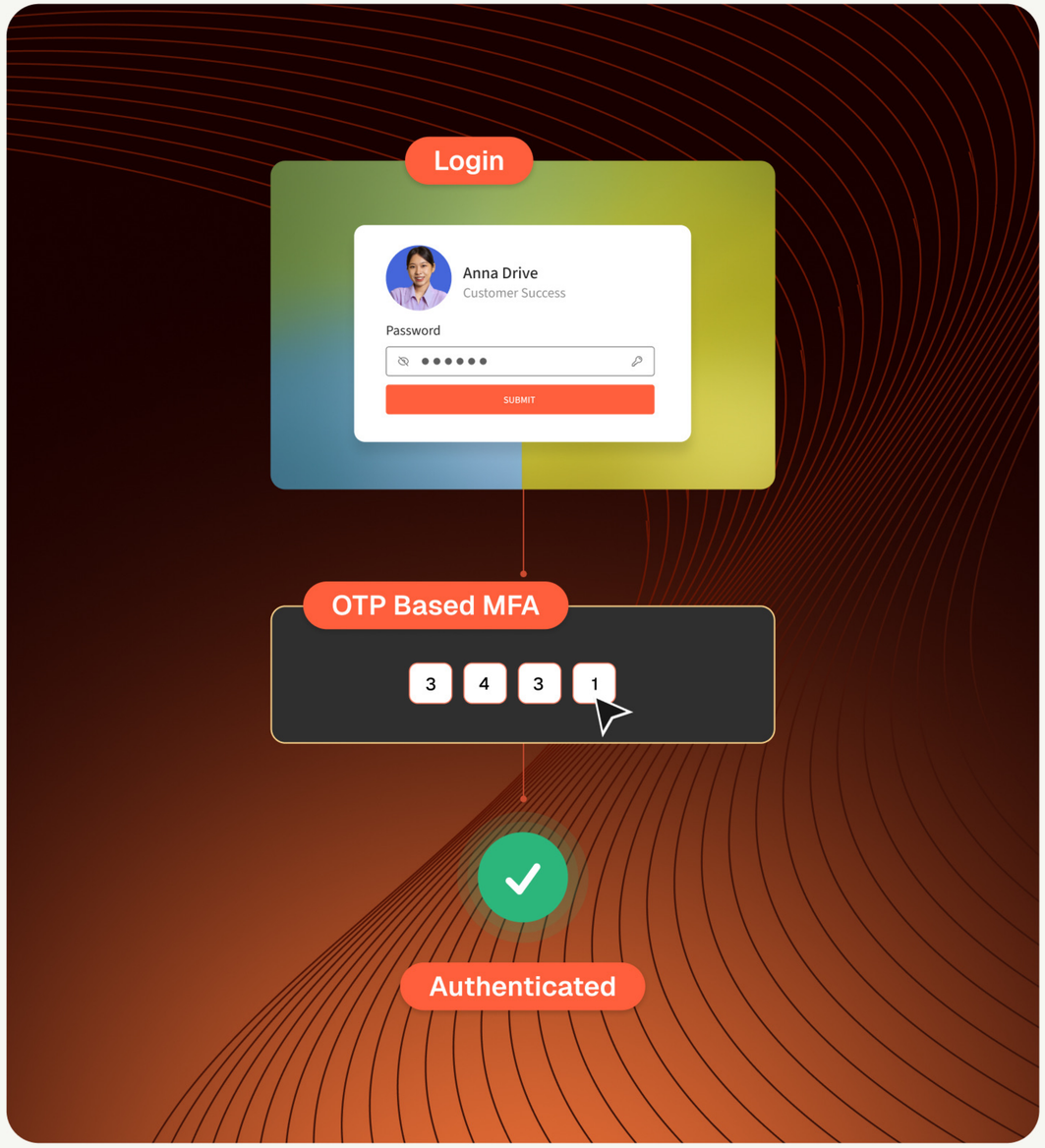
Use case

A system administrator needs temporary elevated access to troubleshoot a critical server issue. Instead of assigning permanent admin rights, OneIdP grants JIT access for a specific duration, preventing the risk of unauthorized actions and privilege misuse.



Add extra layer of authentication with *MFA enforcement*

Enhance security with an extra layer of authentication before granting access. OneIdP enforces Multi-Factor Authentication (MFA), requiring users to verify their identity via a second factor (OTP from a managed devices or from any third-party authenticator app) before granting access.



Use case

An analyst tries to log in from a new location. OneIdP enforces Multi-Factor Authentication (MFA), requiring an additional one-time passcode before granting access, enhancing security.

Restricting work email access to Scalefusion UEM-*managed devices*

Enterprises handling sensitive corporate emails need strict policies on which devices can access them. OneIdP ensures that work email accounts are accessible only from Scalefusion UEM-managed devices, preventing unauthorized access from unsecured endpoints. This guarantees email security and regulatory compliance.

Use case

An Acme Corporation employee tries to access his corporate email from a public PC while traveling. Since the device is not managed by Scalefusion UEM, OneIdP blocks access, ensuring compliance with Acme Corp's strict security policies.

Secure email access from *unmanaged devices* with enhanced authentication

Some employees may need to access corporate emails from unmanaged devices. OneIdP ensures secure access by enforcing strong authentication methods such as OTP-based verification from a managed device or any third-party authenticator app. This balances security with flexibility for remote employees.

Use case

An employee needs to check his work email from a public PC. OneIdP prompts an OTP verification sent to his Scalefusion-managed device or a verified authenticator app, ensuring secure email access without compromising security.

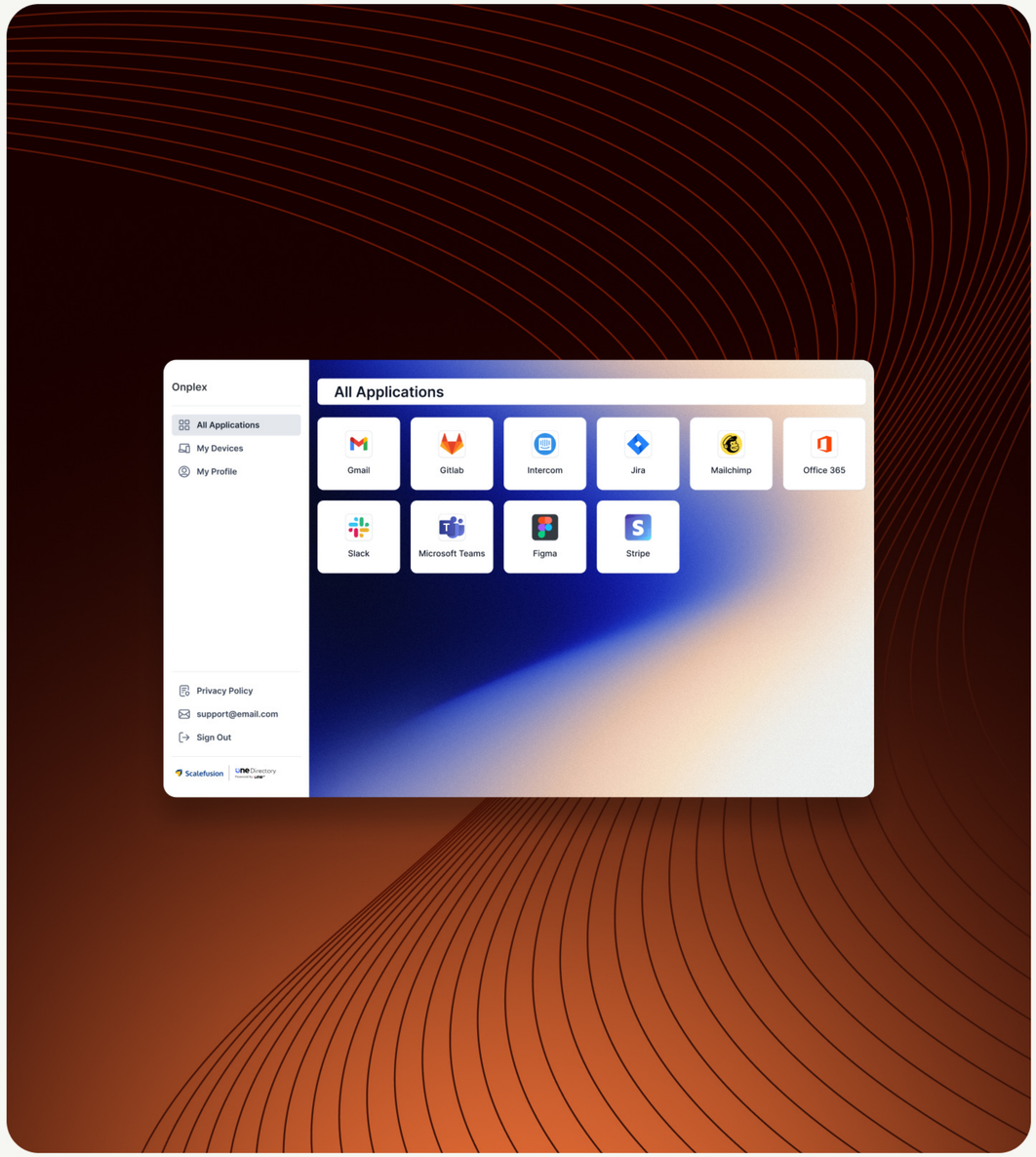
Company *User Portal* for Single Sign-On

A centralized platform designed to simplify application access, enhance security, and boost productivity across organizations. The User Portal transforms how users interact with work applications.

- Single Sign-On (SSO) integration
- Customizable application visibility
- Enhanced access controls
- Centralized application access

Use case

A new marketing team member joins the organization and needs access to tools like the design suite, campaign manager, and content calendar. Instead of IT sending links and credentials manually, the User Portal presents a pre-configured dashboard with everything they need. With secure, SSO-enabled access, the employee is productive from day one.



Your next step toward Zero Trust

Scalefusion OneIdP bridges the critical gap between identity and device security. The use cases explored in this document highlight how real-world organizations can protect corporate resources without adding friction to end users. Whether it's restricting email access to managed devices, enabling secure login from unmanaged PCs with additional verification, or enforcing time-bound admin rights—OneIdP turns access policies into dynamic, enforceable controls.

As your organization looks ahead, OneIdP becomes more than a solution—it becomes the foundation for secure, seamless, and scalable access, powered by deep UEM integration that ensures every device, user, and login aligns with your Zero Trust strategy.

Enable secure access with *UEM-driven Zero Trust.*

Book a demo

Sign up for free