onelogin
by ONE IDENTITY

Active Roles and OneLogin Workforce Identity

Meeting Today's Active Directory and Access Management Needs

One Identity's Active Directory and Access Management solutions seamlessly integrate to **increase operational efficiency, user productivity and security.**

Protecting Users, Apps and Data

Workforce access management and rights provisioning – together or separately – can be a challenge if you don't have the appropriate tools and processes in place. One Identity Active Roles and OneLogin Workforce Identity solutions, two of the components of the One Identity Unified Identity Security platform, simplify your users' onboarding and application provisioning processes, secure your organization's data and accelerate user productivity. These solutions are a powerful combination.

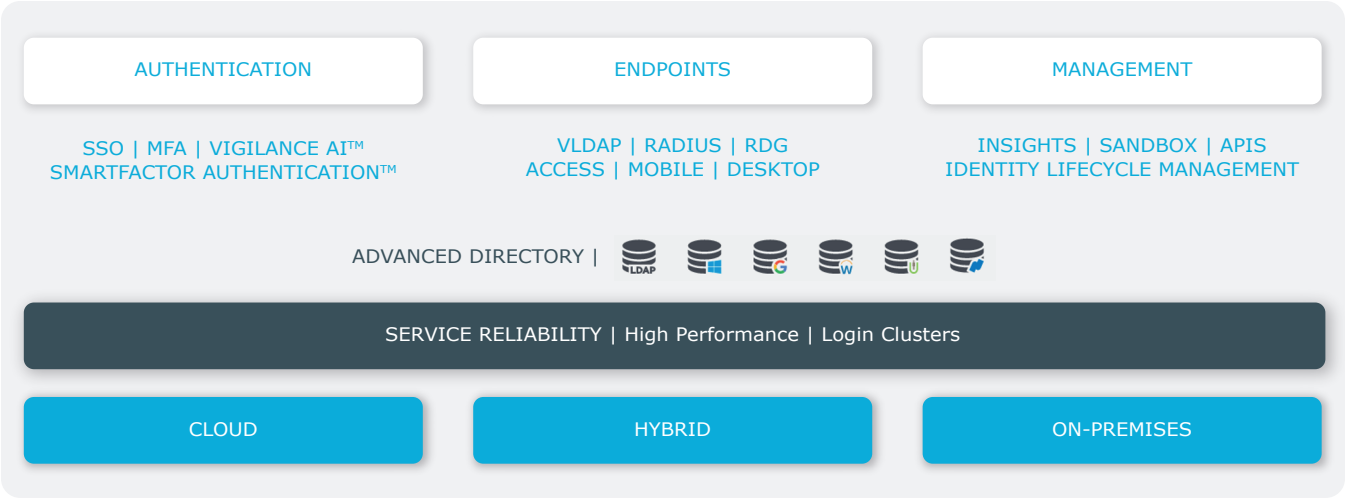
OneLogin's cloud-based access management and Multi-Factor Authentication (MFA) capabilities protect your users' access, as well as your data and applications, from breaches by threat actors. Once logged in, Active Roles' least-privilege access capabilities allow you to ensure that your employees only have the access to the resources they require do their job, nothing more, nothing less. Both solutions are easy to deploy and manage. So, your return on investment (ROI) is fast, the learning curve is short and your organization's security is strong, yet invisible while users execute daily tasks.

One Identity Active Roles

One Identity Active Roles makes user identity management easier for companies that use Microsoft Active Directory (AD) and Azure AD to manage their identities as it provides a "single pane of glass" for AD administration. The automation of account and group management processes and the security features offered by Active Roles reduce human errors due to manual input, increase efficiency and simplify the creation of access permissions for both cloud and legacy applications. Active Roles also helps ensure AD data integrity, while its audit capabilities can help you track all AD changes. Additionally, Active Roles provides manageability beyond Windows. When a user's access needs to be changed or removed, updates are made automatically across all relevant systems and applications in the hybrid AD environment, as well as AD-joined systems, including UNIX, Linux, Mac OS X and a growing collection of SaaS applications.

OneLogin Workforce Identity solutions

OneLogin's Workforce Identity solutions help users access the applications and resources they need to do their work. OneLogin's Single Sign-On (SSO), Multi-Factor Authentication (MFA) and SmartFactor Authentication offer users easy, yet secure, access to apps and other corporate assets, both on premises and in the cloud. No matter where users are logging in from, these solutions mitigate the risk of cyberattacks. OneLogin SSO provides role-based access controls along with ease of use resulting



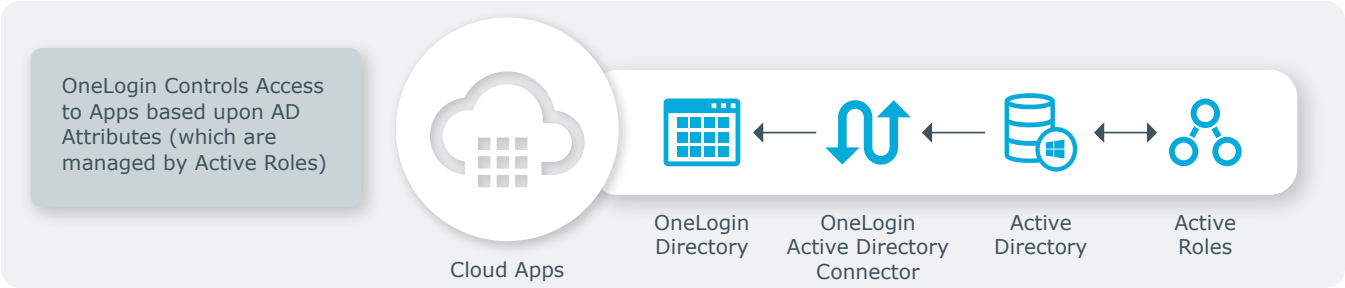
OneLogin Workforce Identity Solutions

from passwordless authentication. This dramatically improves user experience, helping to ensure they can authenticate without delay.

SmartFactor Authentication provides risk-based assessments that provide authentication of accounts by analyzing the context related to the user and their current situation (such as location, IP address, etc.) to identify risky login attempts. And, since remote employees need all the protection they can get, OneLogin Desktop and Desktop Pro offer them certificate-based trust. OneLogin HR-Driven Identity keeps employee PII and app access safe during their time with the company. And for easier user management, RADIUS streamlines both management and control with secure MFA for on-prem network appliances and apps, while Advanced Directory synchronizes users from multiple directories. Together, OneLogin Workforce Identity solutions make access management quick, easy and secure to ensure efficiency that doesn't compromise your organization's data.

Active Roles and OneLogin Workforce Identity Together

When you integrate Active Roles with OneLogin Workforce Identity solutions, you increase efficiency and consistency of user and group management, as well as help accelerate user productivity. OneLogin is designed to pull from a directory source. Active Directory and Azure AD, centrally managed by Active Roles, can serve as directory sources. Moreover, Active Roles provides the foundational identity management capabilities for Active Directory and Azure AD, enabling organizations to easily create the necessary permissions for cloud and legacy applications. In the end, users no longer need to worry about their workday and processes being disrupted by the organization's latest identity security enhancements. At the same time, your IT team will have fewer identity management concerns and, thanks to increased user onboarding and app provisioning automation, they will be able to focus on more strategic projects that drive the growth of your business. It's a win-win for everyone.



Active Roles changes affect OneLogin App assignments. *OneLogin can provision role-based access to applications based on real-time sync with AD, which are managed with Active Roles.*

onelogin by ONE IDENTITY