onelogin

SOLUTION DATASHEET

Self-service password reset with OneLogin

RELIEVE THE HELPDESK, SECURE YOUR BUSINESS, AND EMPOWER EMPLOYEES

Manual password resets: Unnecessary work, cost, and risk

Today's business environment just keeps growing in complexity. In fact, 94 percent of Chief Information Officers believe the tech stack will be more complex in the future, with more apps, data, devices, and transactions. And 93 percent of CIOs anticipate the pace of business will increase, with 59 percent predicting it will more than double by 2025.[1]

More applications, more users, and more types of users (full-time employees, contractors, partners, even customers), means more password reset requests. If yours is like most IT departments, the requests are probably already piling up creating an endless barrage of helpdesk tickets, introducing security risks, and negatively impacting employee productivity—and the reputation of the IT team.

Challenge: Endless helpdesk tickets

- Per Gartner, up to 50 percent of helpdesk inquiries are password reset requests.
- Forrester Research found the average helpdesk labor cost for a single password reset is $70.[2]
- Forrester found some large US-based organizations must allocate over $1 million annually for password-related support costs.[3]

Challenge: Risky password practices

- Helpdesks typically use predictable schemes for temporary password (i.e., "MonthYear"). These weak passwords often go unchanged by users.
- Cybercriminals spoof password reset requests to compromise accounts.

Challenge: Productivity impacts

- When users are locked out of systems, they aren't productive. But they are frustrated.
- Second and third shift employees, night owls, and weekend warriors face extreme wait times.
- Work slows down, and when it's customer-facing, you risk reputational and relationship damage. Or even violating Service Level Agreements (SLAs).

Solution: Self-service password reset with OneLogin

OneLogin enables employees to reset their own passwords while enforcing secure password practices. OneLogin:

- Eliminates up to 50 percent of helpdesk requests, cutting considerable cost and saving staff time.
- Enforces strong password and access policies.
- Ensures simple and secure access from any location and device for every employee.

Simple and secure access with Single Sign-On

With the OneLogin Single Sign-On (SSO) portal, users only have to enter one set of credentials to access their apps in the cloud and behind the firewall via desktops, smartphones, and tablets. That means greater productivity and security.

OneLogin's policy-driven password security and multi-factor authentication (MFA) ensure that only authorized users gain access to sensitive data.

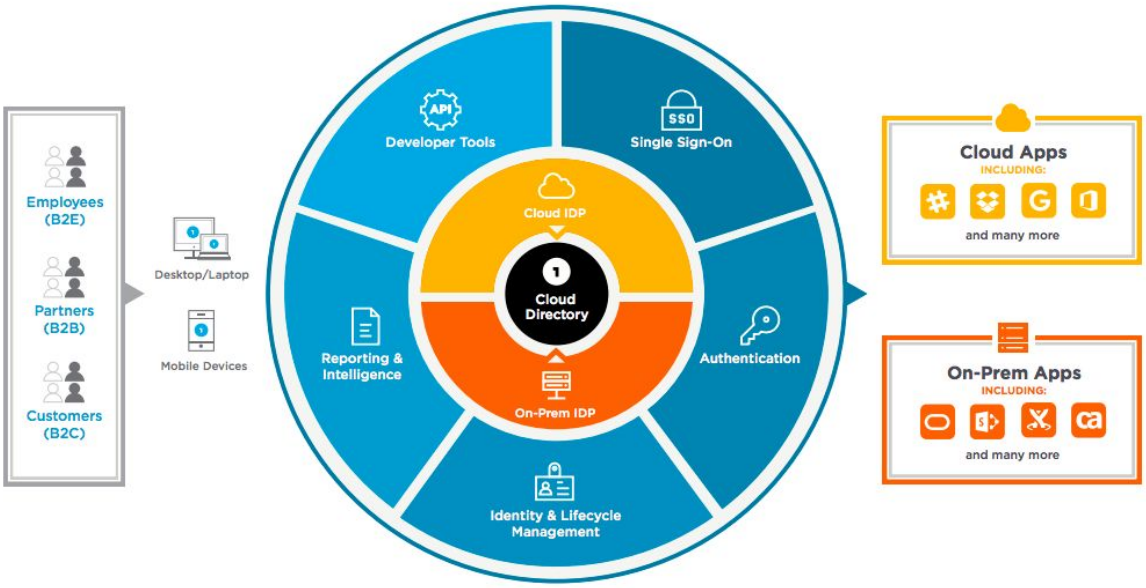
Implement more secure password policies including required length, complexity, and password-reuse restrictions. Add session timeouts and self-service password reset to heighten protection without impeding users.

1 "The Future of Identity and Access Management: A CIO Survey", Pulse Q&A, January 2019
2,3 "Best Practices: Selecting, Deploying, and Managing Enterprise Password Managers", Merritt Maxim and Andras Cser, Forrester Research, January 8, 2018

"We have implemented the password reset feature, reducing calls to our support team by approximately 45% - a percentage we expect to continue to rise."
- Ben Mollett, Application Delivery Engineer, Acuris

"We've seen a substantial reduction in the number of password reset requests flowing through the help desk. When you're accessing through OneLogin, you never have to do anything with your password - it's a huge time saver."
- Brim Bason, IT Solutions Architect, Susan G. Komen

The OneLogin Unified Access Management Platform



Self-service password reset: How it works

OneLogin is a frictionless way to synchronize password changes across Active Directory (AD), the OneLogin portal, and the web apps secured with OneLogin.

- When a user's password expires in AD, they're prompted to change the password the next time they log into OneLogin.
- Users can proactively change their AD password through OneLogin in the OneLogin Portal.
- When a user changes their password via OneLogin, it keeps the password synchronized with AD and any cloud applications where password provisioning is active.

By default, the OneLogin AD Connector only requires read access to a corporate domain for authenticating users and gathering user attributes for provisioning. But you can explicitly grant it permission to allow the changing and synchronization of user passwords.

When a user's password expires in Active Directory, the real-time connection to OneLogin reflects this immediately and will prompt the user to change their password from the OneLogin sign-in page.

The user is presented with an easy to follow workflow and prompted to input their current password and new password twice (similar to what a user experiences on their desktop when changing their domain credentials).

Once the new password is confirmed, OneLogin changes the user's password in Active Directory to match, and also provisions it out to any applications that are configured with password provisioning in OneLogin.

Additionally, if a user decides they would like to change their password prior to the password ever expiring, they may sign into OneLogin and change their password at anytime from their OneLogin portal, with full synchronization.