onelogin

SOLUTION DATASHEET

Self-service password reset with OneLogin

RELIEVE THE HELPDESK, SECURE YOUR SCHOOL, AND SATISFY YOUR STUDENTS

Manual password resets: Unnecessary work, cost, and risk

It's getting harder and harder to manage the growing tech stack that keeps your institution competitive and secure. You have to protect student and school data, but you also have to give students the modern, simple user experience they expect.

More applications, more students, and more staff—growth is good but it also brings more password reset requests. If yours is like most IT departments, those requests are piling up and creating an endless barrage of helpdesk tickets, introducing security risks and negatively impacting students and staff—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.[1]
- Forrester found some large US-based organizations must allocate over $1 million annually for password-related support costs.[2]

Challenge: Risky password practices

- Helpdesks and users typically use predictable schemes for password (i.e., "MonthYear"). And these weak passwords often go unchanged for long periods.
- Cybercriminals spoof password reset requests to compromise accounts.

Challenge: Monetary impacts

- When students are locked out of systems, they can't register, apply for loans, or pay for classes. That loses you money and creates frustration.
- Staff are stopped dead in their tracks waiting on you to reset their password.
- Your school risks reputational and relationship damage from reset delays.

1,2 "Best Practices: Selecting, Deploying, and Managing Enterprise Password Managers", Merritt Maxim and Andras Cser, Forrester Research, January 8, 2018

Solution: Self-service password reset with OneLogin

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

- Eliminates up to 50 percent of helpdesk requests, cutting considerable cost and saving IT time.
- Enforces strong password and access policies.
- Ensures simple and secure access from any location and device for every student.
- Challenges the user to verify identity via an additional factor to prevent cyber criminals phishing via password requests.

Simple and secure access with Single Sign-On

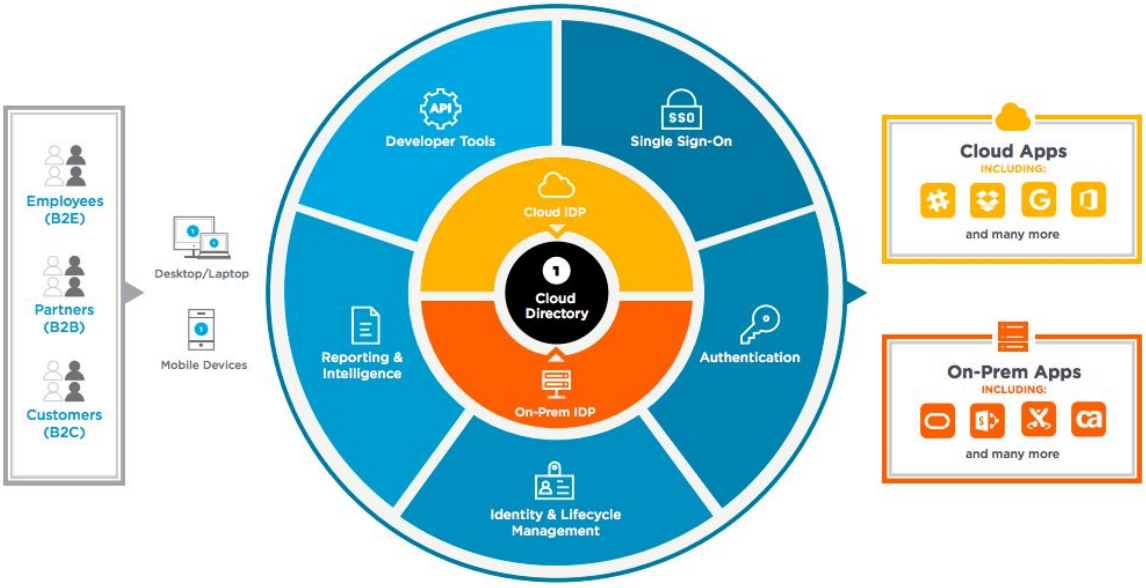
With the OneLogin Single Sign-On (SSO) portal, students and staff only have to enter one set of credentials to access their apps in the cloud and behind the firewall via laptops, smartphones, and tablets.

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

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.

"The product was very easy to install and integrate into our environment while proving a sophisticated secure solution with an easy to use interface. Our staff and students have adopted with little difficulty."
- Tony Casciotta, CIO and VP of IT, Broward College

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.

- Users sign into OneLogin with their AD password. When the AD password expires, the user is prompted to change it the next time they log into OneLogin.
- Students and staff can proactively change their AD password in the OneLogin Portal.
- When users change their password, they are synchronized to AD. Students can sign into OneLogin with the updated password and use OneLogin to access all their applications.

The OneLogin AD Connector only requires read access to a domain to authenticate users and gather user attributes for provisioning. But you can explicitly grant permission to allow it to change and synchronize user passwords.

When a user's password expires in AD and they attempt to login via OneLogin, OneLogin prompts the user to change their password. The user is presented with an easy to follow workflow and prompted to input their current password and new password.

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, like a student, decides they would like to change their password prior to the password ever expiring, they can change their password at anytime from their OneLogin portal, with full synchronization.

OneLogin lets you fully brand the OneLogin portal with your colors, logo, etc. Plus, it integrates with HR systems like Workday or BambooHR. So, if you use an HR system to manage staff, OneLogin synchronizes with it in real time just as with AD so that all your directories are up to date, all the time.