

# OneLogin Desktop

Move toward a passwordless work environment and optimize your IT cloud infrastructure

Active Directory (AD) worked well in the past, when everyone used their personal workstations in the office and behind the firewall. IT could configure password policies in AD and have them enforced across an entire fleet of PCs. But that scenario has changed.

Today's modern organizations increasingly consist of employees, contractors, and remote workers with a variety of devices in many locations. A more distributed workforce means reduced reliance on the corporate network. As a result, a large portion of worker laptops never join an AD Domain. And, often, companies born in the cloud don't even have AD. Either scenario can mean stale or weak passwords for devices. In fact, More than 80 percent of breaches within hacking involve brute force or the use of lost or stolen credentials.<sup>1</sup> IT teams, therefore, must find ways to eliminate the risks that come with unmanaged laptops and unsecured passwords.

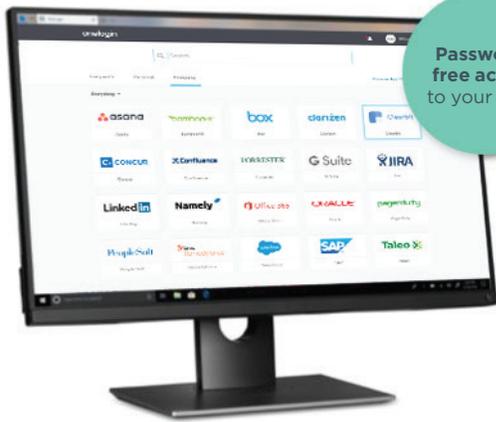
## The One Identity OneLogin Desktop

OneLogin Desktop enables organizations to seamlessly move towards a passwordless environment and provide simple and secure single sign-on to applications accessed through the OneLogin portal on both PCs and Macs. It binds PCs and Macs to the cloud directory, ensuring users always authenticate against a live directory, no matter where they are located.

### Key Benefits

- **A cloud directory for all apps** – Companies that operate in the cloud have AD on the wrong side of the firewall. OneLogin Desktop authenticates laptops against the unified cloud directory using modern APIs.
- **Improved SSO experience** – Once a user signs into their laptop, they are automatically signed into OneLogin. No need to sign in twice. And fewer passwords to remember means fewer (or no) mistakes.
- **Reduced TCO** – With OneLogin Desktop, you don't need to purchase AD licenses for every device. Save money on AD licenses so you can spend it on other priorities.
- **Limit access to untrusted devices** – Using PKI certificates, access to the portal is restricted to only devices that have OneLogin Desktop installed and are sanctioned by the IT department.
- **Greater visibility, control and management** – Easily run the reports you need on device inventory and OneLogin Desktop events to fulfill security compliance and auditing requirements.
- **Enhanced multi-user experience** – For locations where multiple workers share the same machine, OneLogin Desktop can operate as a kiosk that allows different users to securely sign into their OneLogin portal from the same device.

## What is OneLogin Desktop?



### OneLogin Desktop

Login to your OneLogin portal without entering your credentials



### OneLogin Desktop Pro

Adds login to your Mac or Windows computer using your OneLogin credentials

KEY CAPABILITIES	OneLogin Desktop	OneLogin Desktop Pro
<p><b>Strong authentication with OneLogin Desktop Certificate</b></p> <p>OneLogin Desktop issues a unique certificate to each PC or Mac for strong authentication, which can be revoked by admins in case of a lost device.</p>	✓	✓
<p><b>MDM deployment support</b></p> <p>Admins can securely deploy OneLogin Desktop to groups of PCs and Macs with 3rd party solutions, such as Airwatch, JAMF, Meraki, etc.</p>	✓	✓
<p><b>Simple for IT to manage</b></p> <p>Easy device and security policy management, all in one place. Users receive automated password expiration notices, enabling self-service password reset.</p>	✓	✓
<p><b>Shared workstation / kiosk mode</b></p> <p>Support multiple users for one machine to eliminate password sharing. When a user signs in to the Tray App, it binds the profile to that user with a specific certificate.</p>	✓	✓
<p><b>Device authentication</b></p> <p>To reduce security fatigue, users can sign into their PC or Mac with their OneLogin password at boot time and on the lock screen.</p>	✗	✓

Over 2,500 enterprise customers globally secure their applications with OneLogin



AIRBUS

pandora

Steelcase

STITCH FIX