onelogin

PRODUCT DATASHEET

OneLogin's Authentication

Strong and simple security for all your access needs

Today, the number of cybersecurity breaches continues to increase and attacks are increasingly sophisticated. Organizations must implement robust security solutions to protect company data, users, and integrity. When it comes to ensuring that the right people are accessing the right information, authentication is the critical first step, providing security and validating the process.

OneLogin's Authentication

OneLogin ensures secure authentication with a diverse multi-factor authentication (MFA) solution that allows organizations to implement policy-based access control for login and password resets. OneLogin authenticates people using a variety of factors depending on the user's context. For example, when users are signed into their Windows Domain on the corporate network, they're automatically signed into OneLogin using Integrated Windows Authentication (NTLM or Kerberos). When users sign in from outside the corporate network, they authenticate with a more traditional flow, requiring usernames and passwords.

In addition, OneLogin tracks user movement across locations and devices to leverage machine learning that detects anomalous login activity, such as logins from a new country, unlikely travel velocity, and known malicious IPs, which also can trigger stronger authentication. Using the same technology, OneLogin learns to trust locations of employees who consistently work from home so they don't have to use a second factor every time they sign in.

Secure Access to Critical Data

Protect organizational data against attacks with policy-based access control for login and password resets based on location, app, and user privilege level, to ensure only authorized users gain access to sensitive data. IT admins can implement demanding password policies such as required length, complexity, password reuse restrictions, session timeout, and a password reset self-service policy to heighten protection without impeding users.

Balancing Usability with Authentication

Depending on the security policy and context, OneLogin allows organizations to assign the appropriate authentication mechanism to users. With a diverse authentication solution that ranges from passwords, encryption keys, and certificates to stronger authentication factors such as one-time passwords, mobile push notifications, hardware tokens, PKI or a combination, OneLogin helps organizations to select the right authentication factor for their users.

TYPES OF AUTHENTICATION ONELOGIN SUPPORTS:

Authenticate into the Portal

OneLogin establishes a secure network connection (TLS using a digital certificate with 2048-bit RSA key) that transmits user passwords. The password is validated against a trusted user store like Active Directory or the OneLogin Cloud Directory. If the user store is OneLogin, the passwords are hashed using the bcrypt algorithm.

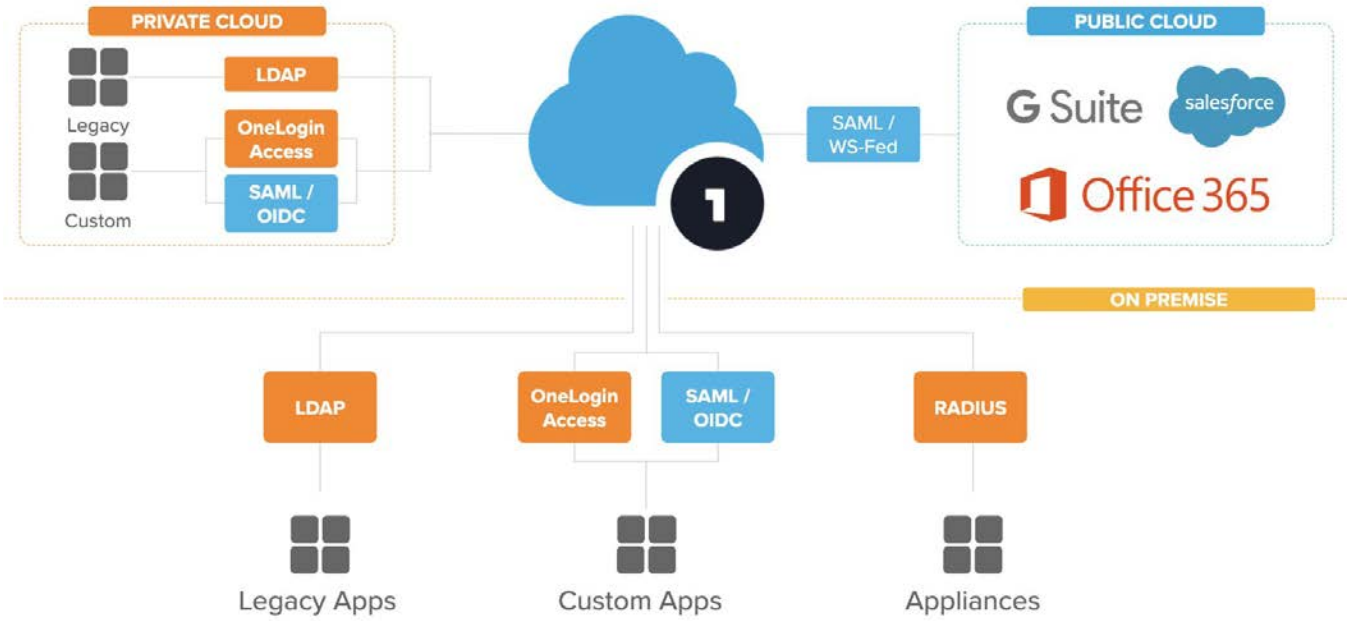
Authenticate into an App via SAML, OpenID Connect, WS-FED or API

When a user signs into an app that leverages SAML, OpenID Connect, WS-Feb or API, it authenticates the user based on a secure token from OneLogin. Currently, OneLogin has thousands of SAML and OpenID Connect-enabled applications in its app catalog including popular apps such as Office 365, G Suite (Google Apps), Salesforce, Concur, AWS, and Box.

Form-based Authentication

A web app presents a username and password web form for user credentials. OneLogin pushes the username and password values into the browser, using the browser extension to authenticate the user. OneLogin doesn't store passwords as a hash. Instead, OneLogin stores passwords encrypted using AES-256 in a Password Vault.

ONELOGIN AUTHENTICATION



AUTHENTICATION METHODS SUPPORTED BY ONELOGIN INCLUDE:

Passwords	Passwords are required for authenticating into OneLogin. OneLogin uses passwords as the primary authentication factor and complements passwords with a variety of multi-factor authentication (MFA) options.
Multi-Factor Authentication (MFA)	OneLogin Protect provides a seamless, integrated user experience for MFA. Instead of manually entering the time-based code, the user simply presses a button and gets signed in automatically. In addition, OneLogin also supports commonly-used MFA providers like DUO Security, RSA SecurID, Google Authenticator, etc.
Adaptive Authentication	Adaptive Authentication uses a machine learning algorithm that calculates risk to determine whether a login requires MFA. It uses a broad set of inputs, including networks, geography, devices, and time, to build a user profile to score the risk of new login attempts. Login attempts with elevated risk scores get prompted for multi-factor authentication, either from OneLogin OTP or a third-party authentication provider.
Password Vault	PKI Certificates prevent access to OneLogin accounts from unauthorized browsers. These can be downloaded and installed on the local machine by an authorized end user.
Security Questions	IT admins can determine the number of security questions required. End users can choose the questions they want to answer for account authentication, unlocking accounts, and resetting passwords.
Multi-MFA Configuration	Ability to define 'multiple' configurations of an authentication factor per tenant. For example, two configurations of OneLogin Protect for different user groups, one allowing backup/restore, and another one disallowing backup/restore.
WebAuthn	OneLogin supports WebAuthn as a second authentication factor. Customers may select authenticators such as YubiKey, NFC, Bluetooth and/or built-in platform biometric authenticators such as fingerprint sensor and face recognition.

To learn more about OneLogin's Authentication services, visit https://www.onelogin.com/product/multi-factor-authentication