onelogin

PRODUCT DATASHEET

# External Users and OneLogin Provide Security and Identity Management

Companies are moving increasingly more sales and service functions online in order to leverage the efficiencies of the web. As the number of applications required to support a company's online presence grows, so do the challenges related to managing identities for customers, suppliers and other partners.

**Identity Challenges in the Online Channel**
Customers, suppliers and partners should never experience unnecessary friction while registering, signing in, or accessing online services. These services typically provide critical business functions such as trouble ticketing, online chat, billing,order management, community engagement as well as custom functionality built for a company's unique business requirements.

When external users are unable to service themselves online, it has a negative impact on customer satisfaction and revenues. Just compare booking an airline ticket online versus doing it at an airport ticketing counter. Successful online experiences reduce costs and lead to happier customers and repeat business.

Managing external user identities across multiple applications poses several challenges:

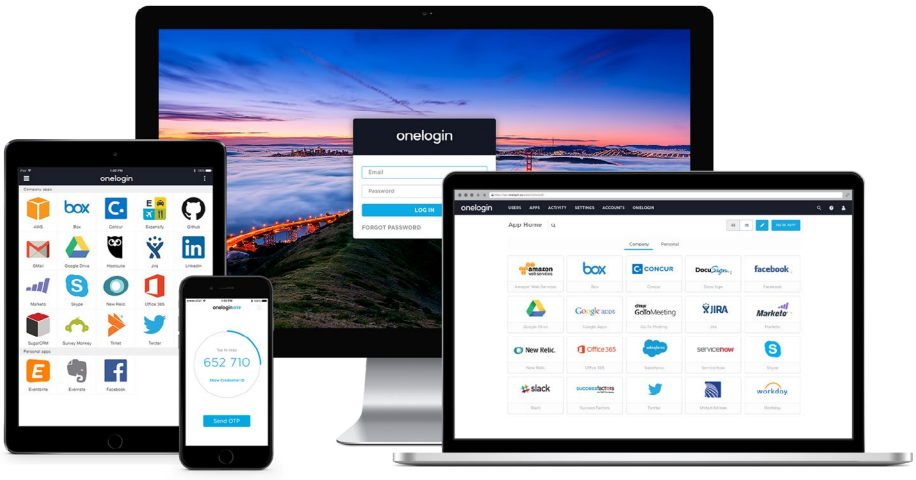
- Synchronizing user identities from a central repository to target applications
- Seamlessly signing users in when they switch between applications
- Automating password resets
- Streamlining user registration

Most companies keep the system of record for external users behind the firewall,usually in an LDAP-based directory or relational database. Connecting on-premise directories with cloud-based applications has its own set of challenges, including high availability, firewall traversal, user management, directory-to-application connectivity and total cost of ownership.

**Why OneLogin?**
When your customer-facing applications are located in the cloud, it makes sense to also place identity management for these users in the cloud. OneLogin provides a cloud-based, turn-key solution for managing external user identities, including user store, self-registration and single sign-on.

OneLogin provides the following benefits for managing external user identities:

- **Cost efficiency** OneLogin's total cost of ownership cannot be matched by an in-house solution, which requires hardware and engineering resources to develop and maintain.
- **Scalability** OneLogin scales automatically with your growing user base and easily supports millions of users.
- **Standards-based SSO** By leveraging standards for single sign-on, new applications can easily be integrated and you can leverage OneLogin's vast catalog of pre-integrated applications.
- **Comprehensive functionality** OneLogin provides rich functionality for user management, authentication, single sign-on, directory integration and user provisioning.




### Directory Integration

Many organizations house their external users in an internal user directory, either LDAP-based or a relational database. OneLogin enables extensive functionality for integrating with Active Directory and LDAP servers simply by deploying OneLogin's Directory Connector behind the firewall. The connector communicates with OneLogin using an outbound, persistent SSL connection, which means no firewall changes are required. The persistent connection enables OneLogin to delegate authentication to the local directory and user changes are synchronized to OneLogin in real-time.

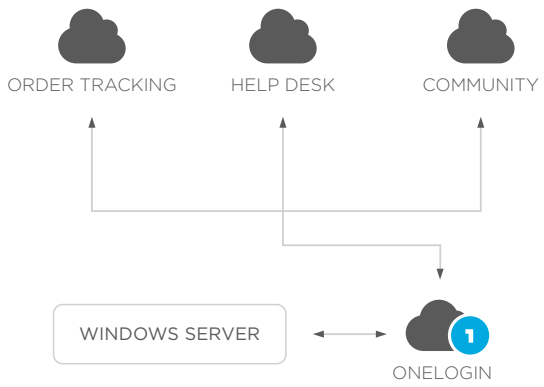



Figure 1. Cloud Integration via OneLogin

OneLogin also provides an easy-to-use REST API for managing users, which can be used to integrate with custom user stores, such as relational databases.

### OneLogin Cloud Directory

Although OneLogin provides very robust functionality for integrating with Active Directory and LDAP, you can benefit tremendously from using OneLogin as a cloud-based directory for your external users. By having user identities stored closer to the related cloud applications, your infrastructure becomes more homogenous and you can leverage other functionality provided by OneLogin.

Some of the functionality OneLogin provides out-of-the-box includes:

- Integrated password reset function
- Self-registration
- REST API for easy user management

OneLogin's solution briefs on Active Directory and LDAP integrationdescribe these capabilities in greater detail.

### Standards-Based Single Sign-On

Security Assertion Markup Language (SAML) is the industry standard for browser-based single sign-on and is supported by an increasing number of commercial cloud applications. One of the main benefits of SAML is that it allows an identity provider to sign a user into an application without a password, which means that there is only one password per user.

### SAML Toolkits

In addition to being pre-integrated with over 2,500 commercial applications,OneLogin also provides SAML toolkits that enable you to easily SAML-enable internally built applications written in Java, .NET, PHP, Python and Ruby.

### Deep Linking

Another benefit of SAML is that single sign-on can be triggered by both the identity provider and other applications. For example, when a user signs into their customer portal and selects "My open tickets", the identity provider signs the user into the help desk application using SSO. But what happens when a user clicks on a link in an email from the help desk application and is sent directly to the help desk application?

If the help desk application is able to detect the user's identity from the link, it can initiate single sign-on and send the user to the identity provider. If the user does not currently have a browser session with the identity provider, the user will be authenticated and then sent to the link they originally requested. This deep linking capability is unique to SAML and ensures that customers always get signed in and land on the intended content

### Password Resets

Forgotten passwords are the enemy of online services. When users forget their password, they often postpone their business and may not even come around again. Or, it may result in a costly call to your customer support center. OneLogin streamlines and automates passwords resets so users can always get access to their account.

### Multi-factor Authentication

If your are hosting sensitive data or have particularly security-conscious customers,OneLogin can provide extra protection using multi-factor authentication. Additional authentication factors prevent unauthorized access from individuals who guess or steal a user's credentials.

Besides being pre-integrated with strong authentication solutions from RSA, Symantec, VASCO and Yubico, OneLogin also provides its own Mobile One-Time Password solution that sends the one-time password out-of-band with the click of a button.

### Self-Registration Profiles

Customer on-boarding can be tricky to implement, especially if you are dealing with different sets of users, approval policies and applications. For example, customers may be allowed to complete self-registration without approval and get access to:

- Whether registration requests must be manually approved
- Blacklisted email domains
- Apps to be automatically assigned to users after sign-up

An organization can define any number of self-registration profiles and thereby providing custom workflows for different sets of users.

### User Administration

OneLogin's browser-based user interface makes it easy to manage users.Administrators can quickly find users, create new or update existing users, manage access to applications, reset passwords, and inspect audit trails. Administrators can even impersonate a user, which can be a tremendous help when providing technical support.

### Case Study Steelcase 20,000 users

Steelcase is the global leader in the office furniture industry with $2.75 billion in revenue and over 10,000 employees around the world.

Steelcase uses OneLogin for identity & access management for its employees, customers and partners. The users are stored in four Active Directory instances that are kept synchronized with OneLogin in real-time. The four directories contain US employees, EMEA employees, APAC employees and external users. The external users sign into a Steelcase-branded login page and get access to a multiple applications that make up Steelcase's online presence. Using OneLogin for all types of users makes it easier for Steelcase to control access to cloud applications and to allow users with different roles to access the same accounts.