ONELOGIN WHITEPAPER

LDAP Integration

www.onelogin.com | **twitter.com/onelogin**

OneLogin, Inc. | 150 Spear Street, Suite 1400, San Francisco, CA 94015

855.426.7227

Even as enterprises continue to adopt more cloud applications, Active Directory and Lightweight Directory Access Protocol (LDAP) still play a critical role in how information security, personal computers and users are managed. This whitepaper describes how OneLogin securely connects your LDAP infrastructure to OneLogin and your cloud applications.

DIRECTORY INTEGRATION ADVANTAGES

There are several other advantages to directory integration besides enabling users to sign into applications with the existing network credentials:

- **Eliminate passwords** – The combination of SAML-based single sign-on and OneLogin's LDAP integration eliminates passwords for all the applications that support SAML. Fewer passwords mean reduced IT workload and increased security.
- **Unify multiple directories** – For organizations that have their user base spread over multiple directories, OneLogin can combine and present them as one, unified directory to other applications for federation via SAML.
- **Avoid point-to-point application integration** – Some applications can delegate authentication to a directory via LDAP; however, as the number of applications increases, the cost of maintaining the integrations increases, and your firewall ends up looking like Swiss cheese.
- **Centralized access control** – Instead of signing into applications directly, users must authenticate via the identity provider, subject to multiple authentication factors.
- **Centralized audit trail** – All sign-in activity is recorded in a centralized audit trail, which simplifies compliance and enables cross-application analysis.

The rest of this white paper goes into more detail about how OneLogin integrates with LDAP. (Note that a similar white paper exists about OneLogin's Active Directory integration.)

INSTALLATION

Integrating internal directories with cloud applications can be an expensive and cumbersome process that frustrates IT administrators and causes maintenance headaches for the entire organization. OneLogin's LDAP integration sets a new standard for ease-of-use with its no-touch installation process, which can be completed in as little as one minute.

One-minute Installation

The LDAP Connector is installed by downloading a Java ARchive (JAR) file that you can deploy in a Java container such as WebSphere, WebLogic and JBoss. Or you can simply run it from the shell using **java** or **jre**. You want to make sure that the Connector is running at all times so that OneLogin is always able to delegate authentication to the LDAP server.

OneLogin issues a unique 40-character security token for each directory connected with OneLogin, which must be entered during the connector installation process. OneLogin uses it to identify each directory.

As soon as the installation is complete, the LDAP Connector establishes a secure, outbound SSL connection to OneLogin that it will keep up at all times. You'll see in the OneLogin screen that the directory is connected, and you can browse a visual tree of all organizational units in the directory. Import one or more subtrees into OneLogin to begin user synchronization. From that point on, users in the selected subtrees will be automatically synchronized with OneLogin at configurable intervals.

No Firewall Changes Required

The LDAP Connector does not require any firewall changes to communicate with OneLogin, as all communication is performed over two separate, outbound SSL connections (see Figure 1).

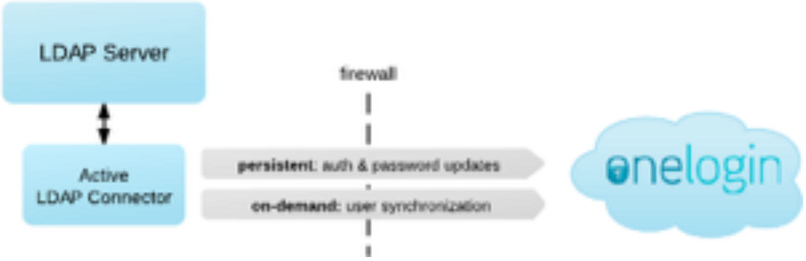

LDAP Server
firewall
Active
LDAP Connector
persistent: auth & password updates
on-demand: user synchronization
onelogin

Figure 1. Outbound SSL Connections to OneLogin

The connection for authentication and password updates is a persistent connection that the LDAP Connector keeps up at all times. If, for some reason, the connection fails, the LDAP Connector re-establishes it immediately. The Connector for user synchronization communicates with OneLogin's REST API and is only established when there are pending user updates.

HIGH-AVAILABILITY

The LDAP Connector also supports high-availability mode, in which there are multiple LDAP servers per domain (see Figure 2). You can install multiple LDAP Connectors per LDAP server, all of which will be connected to OneLogin simultaneously. One Connector is designated as the primary Connector. If OneLogin is unable to reach the primary Connector, one of the secondary Connectors is promoted to primary, automatically.

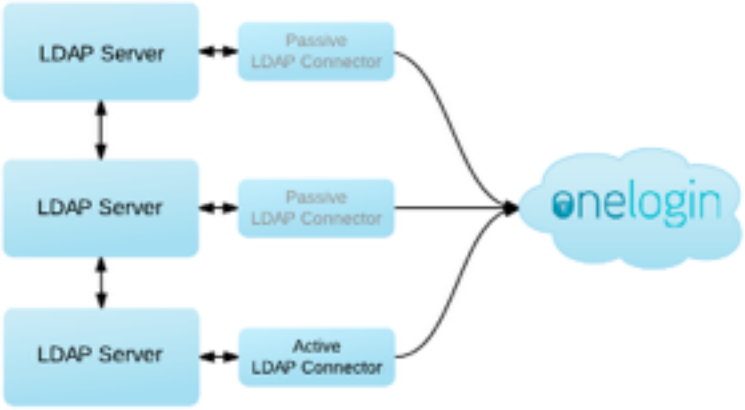


Figure 2. High-availability setup

Figure 2 shows how multiple connectors can run in parallel. You can even install multiple connectors per LDAP instance. Administrators can also manually promote LDAP Connectors or bring them online or offline in OneLogin.

USER SYNCHRONIZATION

Automatic User Synchronization

When users are created, updated or disabled in LDAP, the changes are pushed to OneLogin within minutes, which has several key benefits.

- New users can sign into OneLogin and start using their applications immediately.
- When employees or contractors leave the company, the automatic sync provides a kill switch that effectively locks users out of OneLogin, which prevents unauthorized access and data loss.
- For applications that are being provisioned by OneLogin, the automatic sync is twice as useful. For example, when a user is created in LDAP and mapped to the Sales security group, OneLogin provisions the user in the target application within minutes.

By default, the LDAP directory is scanned for changes every 5 minutes, but this interval is configurable as a command line option.

Full LDAP Attribute Mapping

As a minimum, OneLogin synchronizes email address, user name and group memberships. You can also configure OneLogin to synchronize additional fields and map them to custom fields. Note that OneLogin does not synchronize passwords from LDAP, unless the administrator explicitly enables this feature.

LDAP Groups

OneLogin automatically imports user group memberships, which can be used to automate the assignment of applications to users. This is done via powerful rule-based mappings that make it possible to express rules such as the following:

> For all users where OU contains “Sales” and OU does not contain “USA”
>
> Assign the roles **Employee** and **European Sales**

Roles are the mechanism within OneLogin that assigns applications to users. A user can have multiple roles, and one application can belong to multiple roles. For example:

> **Employee role**: Box, Google Apps, Workday, Yammer
>
> **Marketing role**: Marketo, Salesforce, WordPress
>
> **Sales role**: Salesforce, Zendesk

Even though both the marketing and sales roles contain Salesforce, assigning both roles to a user will only give the user one Salesforce login.

DELEGATED AUTHENTICATION

The outbound, persistent connection from the LDAP Connector enables OneLogin to validate user credentials against an LDAP server, without having to store any LDAP passwords in OneLogin. When a user tries to sign into OneLogin by entering the username and password, OneLogin sends a delegated authentication request to the LDAP Connector, which in turn validates the user's credentials against LDAP. Delegated authentication ensures that your LDAP passwords are not stored anywhere outside the firewall.

LDAP Password Updates

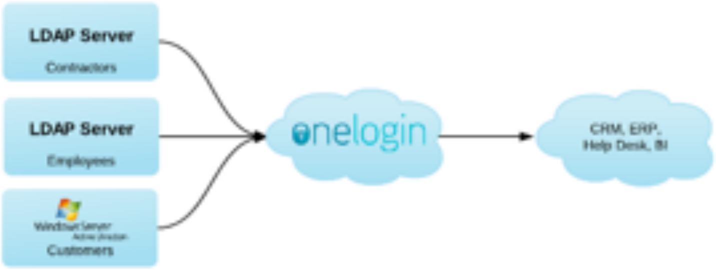
When a user with an expired password tries to sign into OneLogin, they are prompted to enter the existing password and select a new password that complies with password requirements as defined by the user's security policy in OneLogin. Security policies define password minimum length, whether the password must contain digits or special characters, how often the password expires and how long to prevent reuse of old passwords.

Once the user enters a valid new password, OneLogin updates the user's password in LDAP and the user is signed into OneLogin. It is possible to disable this password update feature in OneLogin.

COMPLEX DIRECTORY INFRASTRUCTURES

For organizations with multiple directories, OneLogin is a real life saver, because it allows for the integration of any number of Active Directory and LDAP directories, and presents them as a single directory to to other applications (see Figure 4).

Figure 4. Multiple



Unifying Directories

Most applications
integrate with one
customer, but the
OneLogin's

are only able to
directory per
combination of
directory

integration capabilities and SAML overcomes this limitation.

CONCLUSION

OneLogin's turnkey solutions makes it easy to connect your directory infrastructure to applications in the cloud and behind the firewall, without compromising security.