onelogin

Active Directory Integration

www.onelogin.com | twitter.com/onelogin

OneLogin, Inc. | 50 Osgood Place, Suite 100, San Francisco, CA 94133

855.426.7227

Even as enterprises continue to adopt more cloud applications, Active Directory (AD) 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 Active Directory 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 AD 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 AD. (Note that a similar white paper exists about OneLogin's LDAP 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 AD 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 AD Connector is installed by downloading a Windows executable that deploys the Connector as a Windows service. Because the AD Connector runs as a Windows service, you don't have to worry about manually restarting it after a Windows reboot.

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 AD 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 in real time with OneLogin.

No Firewall Changes Required

The AD 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).

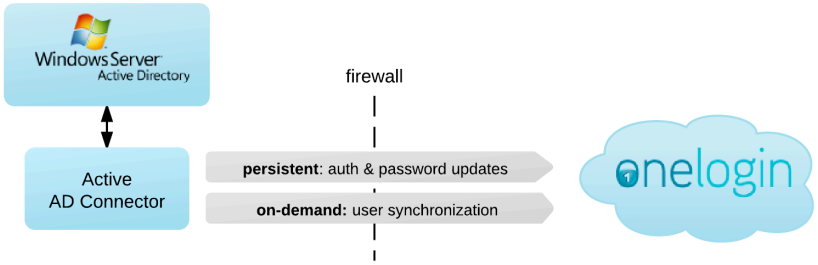

Figure 1. Outbound SSL Connections to OneLogin

The connection for authentication and password updates is a persistent connection that the AD Connector keeps up at all times. If, for some reason, the connection fails, the AD 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 AD Connector also supports high-availability mode, in which there are multiple domain controllers per domain (see Figure 2). You can install multiple AD Connectors per controller, 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.

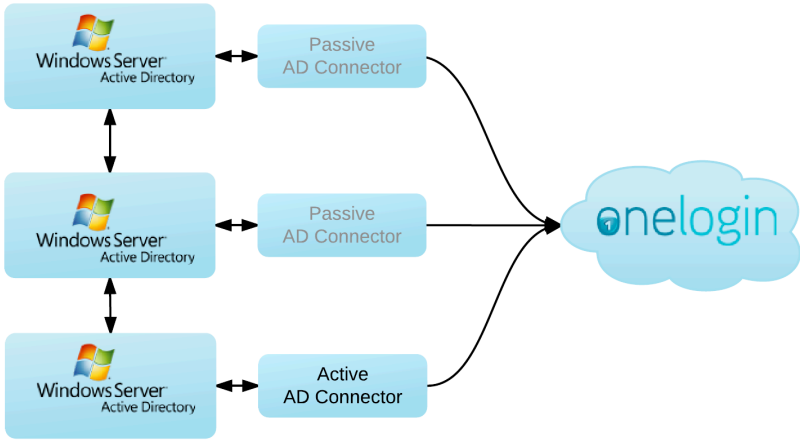

Figure 2. High-availability setup

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

BI-DIRECTIONAL USER SYNCHRONIZATION

Real-time User Synchronization

When users are created, updated or disabled in AD, the changes are pushed to OneLogin in real-time, which has several key benefits.

- New users don't have to wait until the next periodic sync before they can sign into OneLogin and start using their applications.
- When employees or contractors leave the company, the real-time user sync provides an instant kill switch that effectively locks users out of OneLogin, which reduces prevents unauthorized access and data loss.
- For applications that are being provisioned by OneLogin, the real-time aspect is twice as useful. For example, when a user is created in AD and mapped to the Sales security group, OneLogin provisions a user in the target application within seconds.

Full AD Attribute Mapping

As a minimum, OneLogin synchronizes email address, SAM Account, distinguishedName and memberOf, i.e. security 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 AD, unless the administrator explicitly enables this feature.

AD User Provisioning

If you are managing users in OneLogin or Workday, you can configure OneLogin to automatically push user updates to AD. For example, if Workday is the system of record for users, any new user in Workday is automatically created in OneLogin and in AD (see Figure 3).

Figure 3. AD User Provisioning

You can even use Workday provisioning groups to define the user's organizational unit and permission groups. For more information on how OneLogin integrates with Workday, read the OneLogin for Workday whitepaper.

AD Security Groups

OneLogin automatically imports user AD security 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 AD Connector enables OneLogin to validate user credentials against AD, without having to store any AD 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 AD Connector, which in turn validates the user's credentials against AD.

Delegated authentication ensures that your AD passwords are not stored anywhere outside the firewall.

AD 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 Active Directory 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 AD and LDAP directories, and presents them as a single directory to to other applications (see Figure 4).

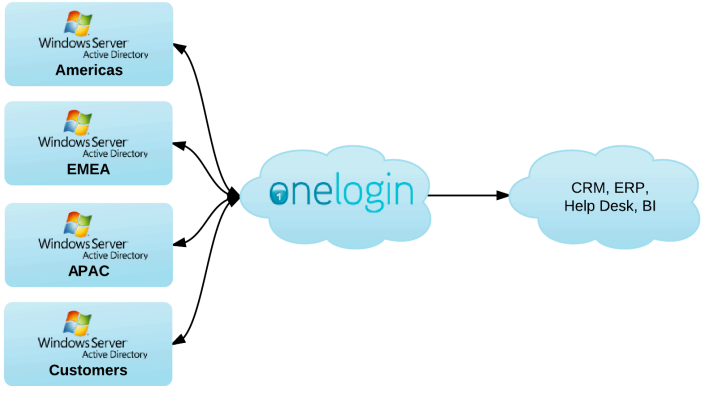

Figure 4. Unifying Multiple Directories

Most applications are only able to integrate with one directory per customer, but the combination of OneLogin's directory integration capabilities and SAML overcomes this limitation.

ACTIVE DIRECTORY FEDERATION SERVICES

OneLogin can co-exist and seamlessly integrate with your Active Directory Federation Services (AD-FS). Through OneLogin's catalog of thousands of pre-integrated applications, you can use AD-FS to sign users into OneLogin and directly into SAML-capable applications. Rather than investing time and energy learning how to integrate applications into AD-FS, you can simply leverage OneLogin's integration capabilities.

For more information about how OneLogin can integrate with AD-FS, please refer to the Trusted IdPs whitepaper.

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.