onelogin

SAML Service Provider Interface

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

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

855.426.7227

OneLogin's SAML Service Provider feature enables it to act as a SAML service provider, which means that it can integrate with third party identity providers, such as Active Directory Federation Services, Shibboleth, CA SiteMinder and PingFederate.

The service provider interface allows other identity providers to using SAML to:

- sign users into OneLogin
- sign users into applications that are already federated with OneLogin using SAML

The ability to integrate with other identity providers is key in projects where the existing identity provider infrastructure is being phased out or enhanced to work with cloud-based applications.

ESTABLISHING TRUST BETWEEN ONELOGIN AND ANOTHER IDENTITY PROVIDER

Other identity providers federate with OneLogin the same way they would any cloud application; by uploading their X.509 certificate to OneLogin. This enables OneLogin to verify that SAML assertions come from a trusted party.

SIGNING USERS INTO ONELOGIN USING SAML

The most basic way of using OneLogin as a SAML service provider is let users get signed into OneLogin by another identity provider. For example, users could be signed into OneLogin by AD-FS when they click on a link in a SharePoint site or some other application that federates with AD-SF.

The identity provider simply posts a SAML response to the URL below with the user's user name or email address in the NameID attribute.

```
https://app.onelogin.com/session/saml
```

This method requires the user to already exist in OneLogin.

SAML Chaining

A more advanced way of using OneLogin's as a SAML service provider is treating OneLogin as a proxy. This

is also sometimes called SAML chaining and can in principle be any number of times.

Figure 1. SAML chaining or proxying

In contrast to the first scenario, chaining does not require the users to exist in OneLogin, rather OneLogin can be used merely as a proxy that re-issues a SAML assertion to the target application based on a certificate that the target application trusts.

OneLogin will trust that the originating identity provider to determine whether a user has access to a particular application. OneLogin allows SAML chaining on a per app basis and issues a SAML consumer URL for each with the following format.

```
https://app.onelogin.com/saml/proxy/9381415
```

OneLogin will pass on the NameID and AttributeStatement structures from the original SAML response, but will rebuild recipient, audience and signature based on the target application.

CASE STUDY

OneLogin recently worked with a client where the SAML Service Provider feature solved a critical problem. The company has 4,000 employees and was being split into two separate divisions, but were still sharing the same applications. This posed a problem because the company was already using an on-premise solution for single sign-on. Most cloud applications only allows customers to federate with one identity provider at a time, but the company now each half of its employees managed by two different identity providers.

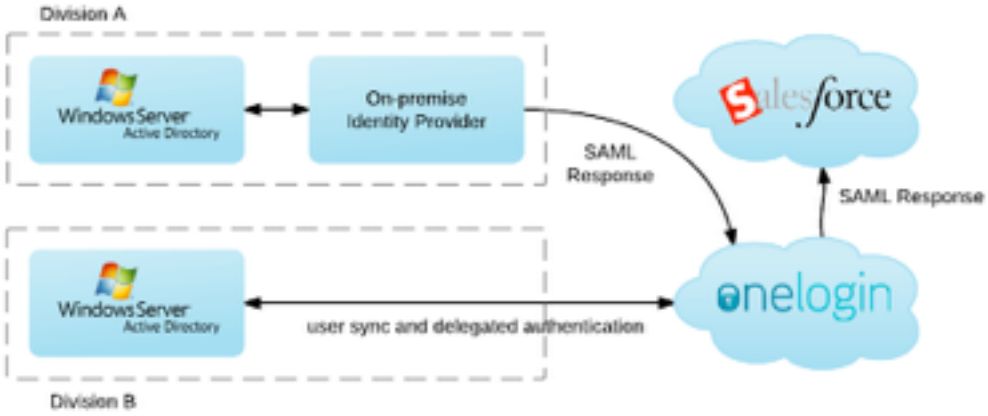

Figure 2. Co-existing with on-premise identity provider

The simple solution was to leverage OneLogin's ability to act as SAML service provider. The X.509 certificate issued by OneLogin was uploaded to Salesforce and the on-premise identity provider was configured to sign users into OneLogin instead of directly into Salesforce.

This capability in OneLogin allowed the client to transfer control of federation to OneLogin without interrupting single sign-on for those employees who were using the incumbent identity provider.