# Federated Authentication Overview

## What is federated authentication?

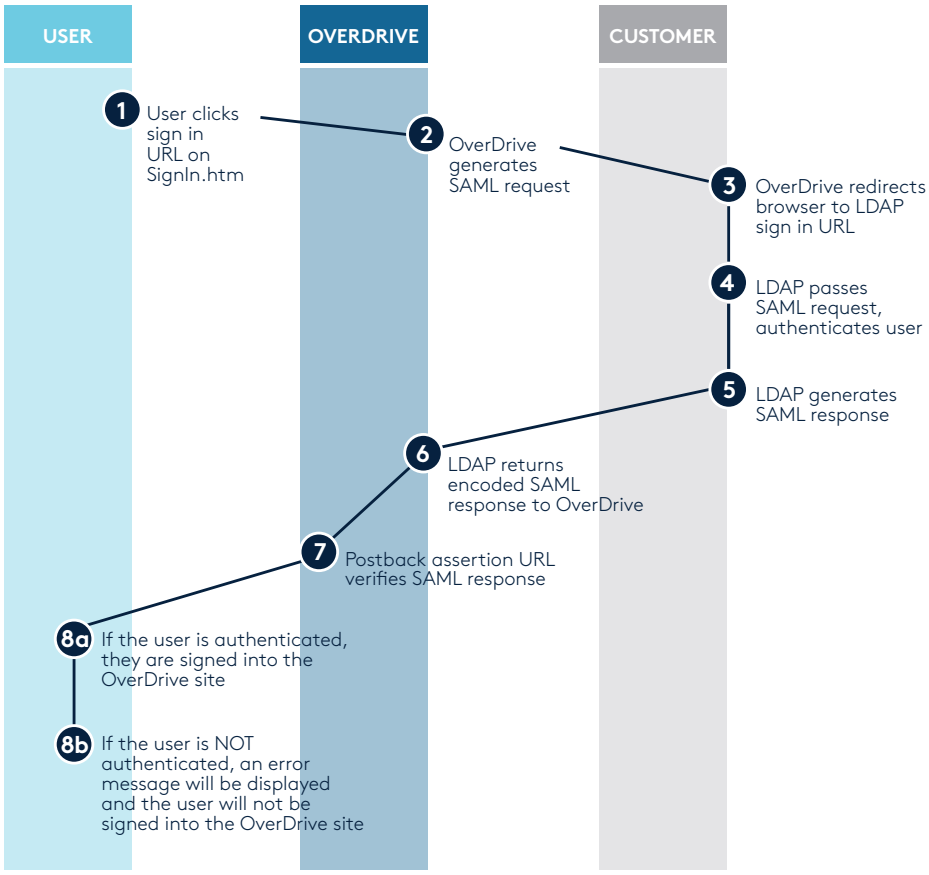
Federated authentication connects to your user directory system using SAML 2.0 protocols. Data is shared between both servers using a secure, encrypted connection. No user data is shared with OverDrive unless explicitly set up by your directory administrator. Examples of federated providers include Microsoft, Okta, Shibboleth, and Ping Identity.

## How does federated authentication work?

To check out or place a hold on a title, a user will be prompted to sign in to the OverDrive-powered website. OverDrive can authenticate users with a federated authentication server. Once the server is linked with the OverDrive website, the sign-in action will direct the user to the authentication server to enter his or her credentials. The authentication server will then pass back an encrypted response as to whether the user is authenticated on the network. The server only needs to pass OverDrive a value unique to the user, such as an email address.

## How can OverDrive implement federated authentication?

The below steps detail federated authentication implementation for your OverDrive service.




### Data protection

For solutions where OverDrive servers attempt to authenticate users by calling a webservice, the http communication will be made via SSL (https).



company.overdrive.com
sales@overdrive.com
+1 (216) 573-6886