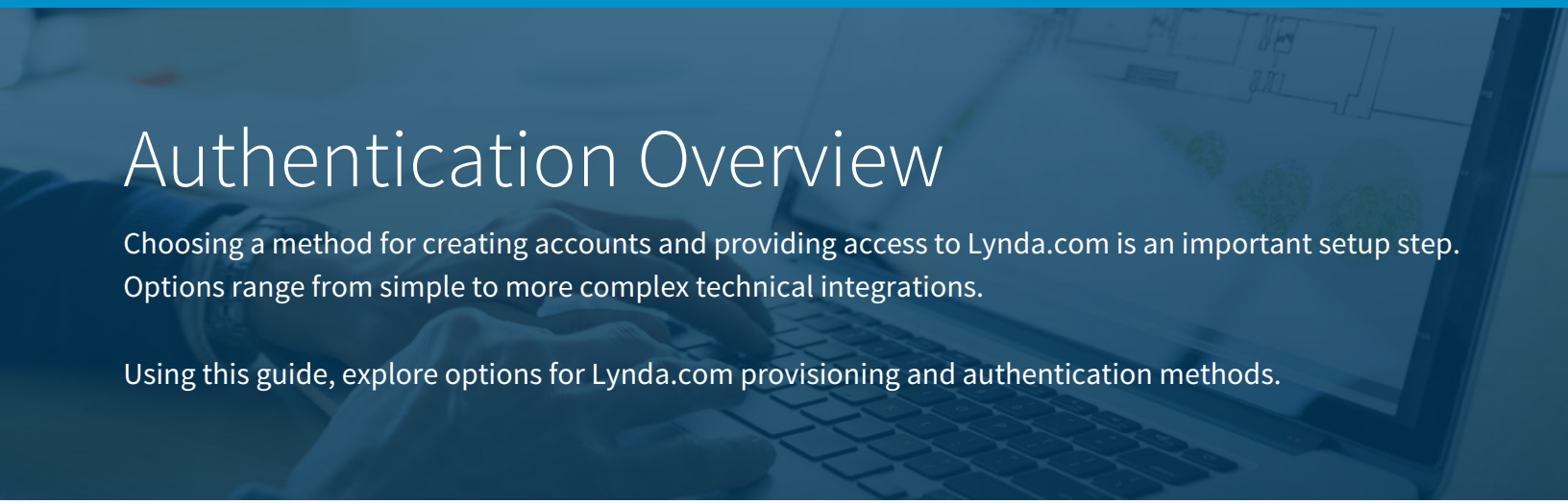

Authentication Overview

Choosing a method for creating accounts and providing access to Lynda.com is an important setup step. Options range from simple to more complex technical integrations.

Using this guide, explore options for Lynda.com provisioning and authentication methods.

Manual user upload

Manual upload is an easier method recommended for small organizations, or for those where the list of users doesn't change much. An account administrator manually adds new users one-by-one, or in bulk by uploading a CSV file. Once users are added, Lynda.com emails each with instructions for account activation.

This authentication method can be used on its own or in tandem with IP address verification or email verification.

If you choose to authenticate users only through bulk user upload, your users won't be able to add their own accounts, but they will be able to edit their user profiles after you've uploaded their names and email addresses. Your organization will be responsible for maintaining its user list as people join and leave the organization.

For more information, **review our Bulk User Upload guide.**

Email verification

Email verification is recommended for organizations that want users to create their own accounts, and when most of the people at the organization will access Lynda.com. This method allows users to complete initial account setup from anywhere with an internet connection.

Once you provide an email domain associated with your organization, users can begin creating accounts by visiting **http://www.lynda.com/email-signup** and entering an organization-provided email address. After Lynda.com verifies a user's email domain, that user will receive an email from Lynda.com prompting the user to create a profile.

The email verification profile creation method can be used on its own or in tandem with bulk user upload or IP address verification.

To implement email verification, contact your Lynda.com account representative or Customer Success Manager.

IP address authentication

IP address authentication is useful for organizations that want users to create their own accounts. This method works best when most users will first access Lynda.com from within the organization's network. IP address authentication allows users within your organization's defined range of IP addresses to access Lynda.com to create their accounts and set up their profiles. After initial account setup, those users can access Lynda.com offsite using an email address and password. Users who work remotely and aren't in the organization's network can be added using the bulk upload feature.

This authentication method can be used on its own or in tandem with email verification or bulk user upload.

For more information, **review our IP authentication guide.**

Single sign-on authentication

With SAML single sign-on (SSO) authentication, Lynda.com uses corporate credentials provided during the SSO authentication process to create a new user profile when a user accesses Lynda.com for the first time.

Setting up SSO is involved and requires technical resources from your organization. Its benefits include:

- Utilization of your existing authentication process.
- Improved security. Employees use your company's established password protocols instead of individual Lynda.com account logins.
- Easier user management when individuals join and leave your organization.

We support SSO using the following standards:

SAML (Security Assertion Markup Language) 2.0

Lynda.com is compatible with any SSO provider that is SAML compliant. Compliant enterprise SSO providers include:

- Shibboleth
- Active Directory Federation Services (ADFS) 2.0 provided as a part of Microsoft Server
- PingFederate
- OpenSSO
- OpenAM
- Oracle 9i
- Okta

Our SAML support is not necessarily limited to these identity providers.

Contact your IT team to determine whether your organization uses SAML, or if SSO is an option for your account. For more information on configuring SSO, **review our Single Sign-On Administrator guide.**

CAS (Central Authentication Service)

We support any version of the CAS protocol. CAS is a non-federated middleware application that provides a trusted connection between two or more service end points.

Google Apps

We support authentication through Google Apps Login. This allows for quick and easy configuration of SSO authentication for organizations that use Google Apps for Business or Google Apps for Education.

LMS authentication

LTI (Learning Tools Interoperability)

We support authentication through a learning management system (LMS) via the LTI standard. We support many popular LMS providers including Blackboard, Moodle, Desire2Learn, and Canvas.

Benefits of authentication through LMS integration include:

- Automatic user provisioning. Users don't have to manually register for Lynda.com or authenticate using a username and password.
- Tracking user course progress. Lynda.com communicates a user's percentage of course completion (0-100) back to the LMS.
- Content curation. The LMS administrator can link either to the Lynda.com homepage, or to a specific Lynda.com course page.

For more information on LTI, **review our LTI integration guide.**