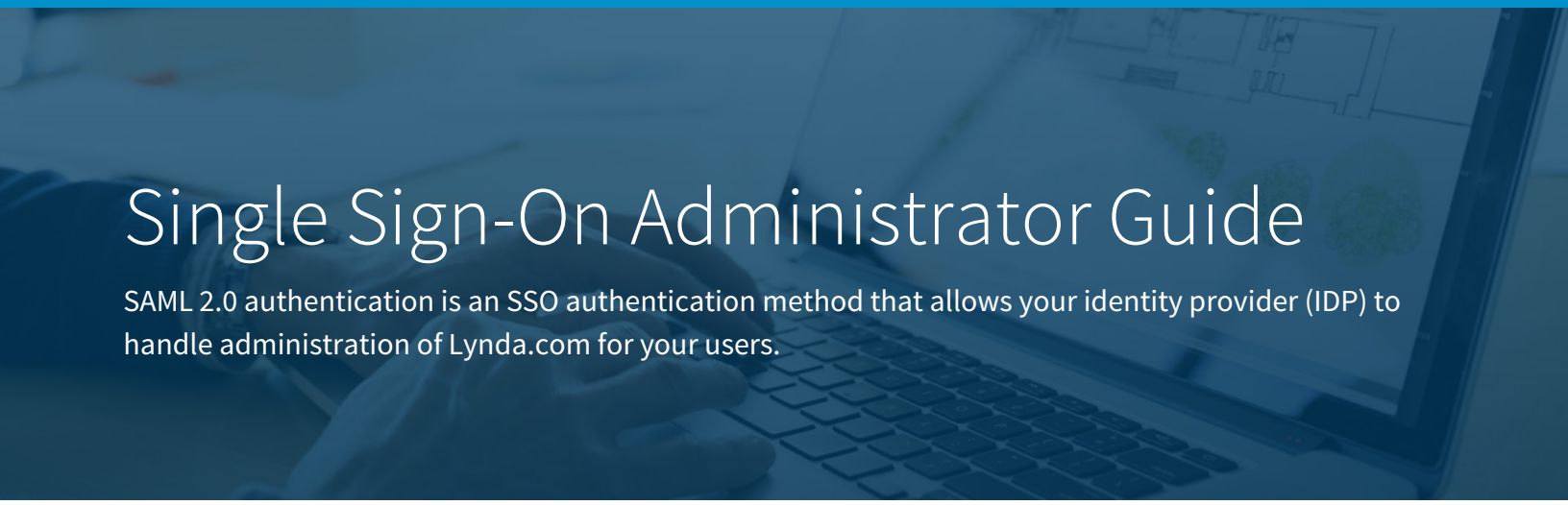

Single Sign-On Administrator Guide

SAML 2.0 authentication is an SSO authentication method that allows your identity provider (IDP) to handle administration of Lynda.com for your users.

How SAML 2.0 authentication works

SAML 2.0 is a web-based single sign-on (SSO) method of authenticating users between domains. It is based on the XML standard of exchanging data about an end user between an IDP (the organization requesting a resource) and a service provider (an organization providing the resource). When working with Lynda.com, your organization is the identity provider and we are the service provider (SP).

We support IDP-initiated SSO and SP-initiated SSO. In the former (IDP initiated), the user requests access to our service and your IDP generates a SAML assertion, including attribute information about the user, and then redirects the user to our service. In the latter (SP initiated), the user requests access to a resource using a link on our domain. We then send a SAML request to your IDP inquiring if the requesting user is authenticated with your organization.

If the user has a session with your IDP, your IDP will generate a SAML assertion, including attribute information about the user, and then redirects the user to our service. If the user is not authenticated, the user will be challenged by your IDP to provide domain credentials. Upon successful authentication, your IDP will generate a SAML assertion, including attribute information about the user, and then redirect the user to our service.

All web traffic is sent as a hidden POST form using HTTPS and is invisible to the user. In this way, SAML 2.0 provides a secure and seamless user experience as it connects your existing identity management infrastructure to Lynda.com.

How to Implement SAML 2.0 authentication

To implement SAML 2.0 authentication, you will need to work with a Lynda.com Technical Consultant. Please contact your account representative or Customer Success Manager to get a Lynda Technical Consultant involved.

To learn more about what information will be required by the Technical Consultant, please continue reading.

Technical Requirements

Federations

Lynda.com is a member of several well-known public federations, including:

- InCommon Federation
- UK Access Management Federation
- Canadian Access Federation
- Belnet R&E Federation
- Australian Access Federation
- Tuakiri, New Zealand Access Federation

If you are not a member of a public federation, you can still take advantage of the benefits of SAML 2.0 authentication with Lynda.com by setting up a private federation between your organization and Lynda.com.

Lynda.com supports Mesh as well as Hub and Spoke federations. If you are a member of a Hub and Spoke federation, you will need to send us an attribute that uniquely identifies your organization within that federation.

SAML 2.0 Metadata

If you are connecting with Lynda.com through a public federation such as InCommon, you will need to provide us with your entity ID. We will use your entity ID to look up your organization's SAML metadata. You will need to know our entity ID to retrieve our metadata and set up Lynda.com as a service provider. See the Entity ID section below for more information.

If you are connecting with Lynda.com using a private federation, we must exchange metadata. You can provide Lynda.com with your IDP metadata as a file or a URL.

Entity ID

Your IDP must have an entity ID as a globally unique identifier that we use to identify SAML 2.0 assertions from your organization. The entity ID is found in your IDP metadata. Refer to your vendor's IDP documentation if you are unable to locate your entity ID.

The Lynda.com entity ID is **https://shib.Lynda.com/shibboleth-sp.**

Signed AuthN Requests

Your organization may require Lynda.com to cryptographically sign SSO AuthN requests to your IDP when a user requests access. If you require signed requests, communicate this to your Technical Consultant so that a Lynda.com engineer can set a relying party rule to enable signing.

There is no security protection to be gained by requiring signed AuthN requests and several drawbacks associated with it. Tampering with the AuthN request will either have no practical effect or cause the IDP to refuse to issue a response entirely. The IDP will also refuse to send assertions intended for endpoints that are not valid for an SP.

Exposing an endpoint that issues signed AuthN requests can also make you a target for Direct Denial of Service (DDoS) attacks because of the highly asymmetric nature of the exchange (one unauthenticated, re-playable request from the attacker versus an expensive service-sider cryptographic operation at the Service Provider).

Testing credentials

We'll need a valid user name and password to test the connection to your SAML 2.0 IDP. These test credentials must be able to authenticate using your IDP and access the Lynda.com service, but they do not need authorization to other internal systems on your network.

Your IT department can disable these credentials after we have completed testing and configuration. If you are unable to give out testing credentials, you will need to test the integration and provide feedback to Lynda.com if there are any problems.

Account Settings

Customizing profile attributes

Attributes are pieces of information about users stored in your directory. Attributes can be a name, email address, department, location, district, job title, language, or other information. If you provide more than the required attributes, we will include them in reports and profiles and use them to create and filter groups. We will display these attributes in reports without trimming blank spaces or changing the capitalization of the values.

Lynda.com uses Shibboleth Service Provider (http://shibboleth.net/products/service-provider.html) to receive SAML 2.0 assertions. Shibboleth SP uses the OASIS standard names in the OID format (urn:oid: urn:oid:2.5.4.4) and requires the attribute name format as urn:oasis:names:tc:SAML:2.0:attrname-format:uri. The AttributeStatement below contains an excerpt of a valid SAML 2.0 assertion where the user's email address is passed to Lynda.com with the expected attribute conventions.

```
AttributeStatement>
<Attribute FriendlyName="mail”
Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<AttributeValue FriendlyName="mail"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">username@example.com</AttributeValue>
</Attribute>
</AttributeStatement>
```

The actual data format and content should comply with standards for attribute usage and not violate XML schema. For example, scoped attributes (e.g., eduPersonPrincipalName) must contain a scope and be encoded for scoped usage.

Attributes transmitted to Lynda.com through the SAML assertion must conform to the EduPerson schema or LDAP standard schema. To provide an attribute that does not conform to either standard, please contact your dedicated Customer Success Manager or your Training Solutions Advisor.

The SAML assertion sends attributes that we store in our database and use to create profiles. We can store up to 30 attributes for each user with the SAML assertion. There are three types of informational attributes that can be stored for each user:

- User ID (required)
- User profile attributes
- Custom profile attributes

A user ID is required for authentication with Lynda.com. It must be unique and immutable for each user. The user ID can be an email address, employee number, hash value, or a GUID. You can use any supported attribute to send this value.

In addition to the user ID, you can add attributes to the SAML assertion to transmit additional information about a user. These can take the form of user profile attributes or custom profile attributes.

User profile attributes include the first and last names and an email address. These are visible to users as part of their Lynda.com profiles. Sending this information for each user helps personalize the user experience at Lynda.com. In addition, it will allow you to easily identify users in usage reports. To transmit user profile attributes through the SAML assertion, identify the attribute names for your Technical Consultant.

Custom profile attributes will be included in usage reports and can be used to filter users and create groups. For example, when a user authenticates, your organization's IDP could send an attribute for the user's department and the master administrator account could filter your user list based on the departments with which your users associate. To transmit custom profile attributes through the SAML assertion, talk to your Technical Consultant.

Authorization attribute

We can use a SAML 2.0 attribute to authorize access for a subset of your organization's users. For example, a corporation may choose to grant access to specific departments only. We can authorize access based on the following:

- The presence of an attribute. For example, if a user is authenticated and the user has the specified attribute, the user is authorized to access Lynda.com.
- Custom criteria matching the value of an attribute. For example, if a user is authenticated and the user has a value of "marketing" for the required attribute "department," the user is authorized to access Lynda.com.

If the users are not authorized to access Lynda.com based on the attribute or criteria you identified, they will be redirected to a custom URL you specify. Communicate the URL you would like us to redirect users as the "failed login URL" to your Technical Consultant.

Organization keyword

Your organization's domain is used as a keyword to redirect users from the Lynda.com login form to your SSO initiator link. The keyword is also used to authenticate users into the Lynda.com iOS or Android app, share content internally, and integrate with Learning Management Systems.

Logout URL

The Lynda.com logout link can be configured to redirect to your IDP's logout path. If you provide Lynda.com with a logout URL once a user selects the Lynda.com logout link the user will be redirected to the logout path where their SAML session will terminate. This is an optional setting that does not apply to all IDPs.

Optional Lynda.com profile page

If you don't transmit attributes for the name and email address, we can ask your users to add this information to their profile to personalize their Lynda.com experience, account information, and your reports. Users will set this information from a customized landing page the first time they log in. This landing page will not appear for subsequent logins.

You decide whether this page is required, optional, or not offered. For example, if you're concerned about protecting your users' privacy, you might choose to not offer this page. If your users provide their name and email address, that information will be stored in our databases and included in Lynda.com usage reports to help you sort and filter users.

Customizing the profile page

If you choose to make the Lynda.com profile page required or optional, your users will see this page when they log in to Lynda.com the first time. This can include a customized greeting to the user at the top of every Lynda.com page when they are logged in. Your Technical Consultant can help you make these customizations.