Frequently Asked Questions

In the following we want to answer frequently asked questions and provide a little more context on various topics. This is not a technical FAQ, but focuses on general, organizational and process-oriented questions. If in doubt or you have additional questions, please ask your sales or client success manager.

Table of Contents

Why are we modernizing Our Authentication System?

We're transitioning away from IP-based authentication to enhance your experience with our platform. While IP authentication has served us for years, it has become increasingly problematic—causing occasional system-wide outages, creating security vulnerabilities, and failing to meet modern compliance standards like GDPR and FERPA. Our new authentication approach offers significant benefits to both our platform and your institution: improved system stability with fewer disruptions to your work, simplified off-campus access for researchers and students, and better compliance with educational privacy regulations. Finally, and probably most importantly, we can now offer individualized access for each student. The individual users will be able to see their own bookmarks, their search history and benefit from the continuous personalization of our platform!

What are the most important arguments for transitioning away from IP Access?

Undetectable data usage risks: IP authentication cannot monitor unusual content access volumes, including potential AI training data harvesting. Enhanced authentication protects our shared resources and ensures responsible usage.

Personalization opportunities: IP-based login treats all users behind the same IP identically, preventing personalized features. Individual authentication enables customized content, recommendations, and analytics tailored to each user's specific needs.

System performance impact: Moving away from IP authentication allows us to significantly improve our database performance, shorten content loading times and make the overall experience smoother and more stable for our users.

What are the new access methods we are going to offer moving forward?

We are committed to providing our customers with the best possible data, while at the same time ensuring that our customers' personal data is secure. We want to offer the highest possible standard of stability and accessibility.

SAML

SAML (Security Assertion Markup Language) is a widely-used authentication protocol that enables secure, user-specific access to your platform. Technically, SAML works by exchanging authentication data between your Identity Provider (IdP, such as Google) and our platform (SP,

Service Provider). When a user logs in, the IdP verifies their credentials and sends a secure token (called an assertion) to our platform, granting access.

OpenAthens

OpenAthens is an identity provider (IdP) that uses a SAML proxy to facilitate federated authentication between libraries, publishers and service providers. It is fully compliant with SAML 2.0 and operates within or outside federations such as eduGAIN. OpenAthens functions as a gateway between your local directory or IdP and the external SAML-based resources you wish to connect with. OpenAthens can be used to connect to SAML-based services directly, including those that do not support federations.

Shibboleth

Shibboleth is a software based on the SAML protocol. It is used by universities to enable students to access university resources off-campus. It works by allowing users to sign in once, using their university account, granting access to various university-provided sources throughout their browsing session without needing to log in repeatedly. Shibboleth is open-source software that allows organizations to manage identity federations securely.

OpenID Connect

OpenID Connect is a modern authentication protocol built on OAuth 2.0, offering secure user-specific access. OpenID Connect requires an IdP compatible with OpenID standards (e.g., Google Workspace). OIDC extends OAuth 2.0 by introducing a standardized identity token (ID Token) and user information endpoint. It enables single sign-on (SSO) across different platforms while maintaining security and user privacy.

How will we ensure that the customers get the support they need?

We have decided to introduce a total of four levels, one contact and three support level. The first level is the pure contact level to your specific Sales or Customer Success Manager. They will be able to answer initial questions or process the facts by asking questions to be able to collect the appropriate solutions internally. The second support level is our designated Implementation Manager. This person has technical experience, is familiar with the topic and ensures that everything runs smoothly. The third support level is our Product Services team, which monitors and supports the technical setup of the respective access method. The fourth and final support level is our Platform Team, which oversees the technical infrastructure and can help if all other technical resources have been exhausted.

Does Statista has documentation and technical support on the beforementioned access methods?

Yes, Statista has documentations to the introduction and configuration of SAML, Shibboleth, OpenAthens and OpenID Connect. We are happy to help, just ask you point of contact at Statista.

Does Statista use the dynamic Metadata URL or manually imports (when the SSL Cert expires in 2 years)?

Metadata URL is manually imported each time a certificate is added/updated.

Does Statista need to make SSO changes or do you have an admin page that Legal Service Corporations can manage?

Changes are done on Statista's side. As of now, there is no admin page for users to manage their own SAML/SSO settings.

Does the vendor's application support Employee ID as the unique-identifier (not just email)?

The implementation of login via SAML/SSO, Shibboleth, OpenAthens and OpenID Connect only requires the attributes needed by the respective institution, like e.g. *first name*, *last name*, *email address*, or the *employee ID*. This is a matter for each institution to decide and assess what identifier to use.

When an employee/student becomes inactive, how will deprovisioning be handled? What does the vendor need from the institution?

The customer can periodically send over a list of inactive students/employees and their responsible CSM can do an account clean up on our end.

What is the retention time for data after the account is deprovisioned?

Customer data is retained after account deprovisioning in accordance with our internal data handling policies and our Privacy Policy. As outlined there, we store personal data only for as long as necessary to fulfill the original purpose for which it was collected, or to comply with legal

retention obligations - for example, under section 257 of the German Commercial Code (HGB), which requires certain records to be retained for a specific period.

For paid accounts, this may include documents such as invoices or other contractual records. For free accounts, data is retained only as long as necessary, and only where no legal or operational requirement applies. Retention periods vary depending on the type of account and the applicable legal or business requirements.

Are there any tiered level access rights? If so, what is needed from LSC OTS to assign privileges through SSO.

No tiered access for accounts with SAML/SSO, all created accounts will be connected to the Master account and have the same access rights.

How will the accounts get created (and/or updated within the application)?

If a SAML user does not have a Statista account yet, a new account will be created automatically once they log in via SAML for the first time. The user then gets immediate access to Statista via SAML without the need for additional registration steps.

Does the EZProxy mean anything for security or is it the same issues as IP authentication?

EZproxy is just a tool / provider through which we enable IP Authentication. Thus the same issues apply.

Sometimes EZProxy is said to have SAML authentication. Does EZProxy use SAML Authentication and if so, how does that work? Can we leverage this functionality?

EZproxy only supports SAML as a Service Provider (SP). It lets users authenticate using their institution's SAML IdP before gaining access to proxied resources. EZproxy does not support SAML in the opposite direction—it cannot act as a SAML IdP or a true proxy between an IdP and another SP. If you want to offer SAML-based access as a Resource Provider, you need your own application or service acting as a SAML SP, accepting SAML assertions directly from institutional IdPs. We are currently investigating a workaround with EZProxy. In more detail:

- **Support Direction**: EZproxy is designed to function as an SP in the SAML model—not as an IdP. This means:

    - EZproxy *receives* SAML assertions but does not itself issue SAML assertions to external Service Providers
- **Resource Provider Use-Case:** For resource providers (content sites), EZproxy is not intended to be placed between your resource server and the institution's IdP, issuing SAML tokens on your behalf. Instead, EZproxy acts as a consumer (SP)—not as a SAML identity provider (IdP) or SAML proxy
- **No SAML "Provider-Side" Mode:** While EZproxy enables SAML-based SSO for libraries and end-users (client-side), it cannot be used as a SAML IdP or as a true SAML-to-SAML proxy on the resource provider's side