

## How does SSO work?

1. The authentication flow usually starts with the user clicking on a login button or accessing a part of the web application that is secured. Since the web application is configured for authentication with SAML, it creates a SAML message known as a SAML Authentication Request. As the name conveys, this message is a request to an Identity Provider to authenticate this user.
2. The Authentication Request message is compressed and Base64 encoded and the user’s browser is redirected to the Identity Provider with that message as an HTTP GET parameter.
3. Upon receiving the Authentication Request, the Identity Provider verifies that it comes from a Service Provider it trusts, and prompts the user to authenticate, most commonly using a login form.
4. The user authenticates with the Identity Provider using their existing credentials and if successful, the Identity Provider proceeds to create a SAML Response message that contains a SAML Assertion. In essence, by constructing the SAML Assertion, the Identity Provider asserts that this user has authenticated successfully and they are known to have certain characteristics that are released in the form of SAML Attributes and their values.
5. The Identity Provider, then, instructs the user’s browser to make an HTTP POST request to the URL where the Service Provider expects SAML Response messages, called the Assertion Consumer Service URL, with the SAML Response Base64 and URL encoded in the body of the request.
6. Finally, the Service Provider receives the SAML Response to the SAML Authentication Request it had originally created and after verifying its authenticity and integrity, “consumes” it in order to retrieve the fact that the user has been successfully authenticated and the information about that user’s identity in the form of attributes. It then passes this information to the web application for it to create a session for the user.

https://www.elastic.co/blog/how-to-enable-saml-authentication-in-kibana-and-elasticsearch