SSO Advanced options

Last Modified on 12/23/2024 1:45 pm EST

If you can't quite get the SAML SSO behavior you want, one or more of the **Advanced options** may help fix your issue.

To access these options:

1. Go to **Security and access > Single sign-on**.

2. Be sure you're on the **SAML settings** tab.

3. Look for the **Advanced options** section in the **SAML settings** section.

Available advanced options

- **Use a unique SP entity ID for this knowledge base:** Use this option if you're setting up multiple knowledge bases to connect to the same IdP. With this option selected, Entity ID and metadata will be updated upon saving and you'll need to update your IdP with the new info.
- **Issue a remote logout request using the IdP logout URL when a reader logs out:** With this option selected, when a reader logs out of KnowledgeOwl, it will also send a logout request to to the IdP. Use this option if you want to ensure someone gets logged out fully from your IdP when they log out of KnowledgeOwl.
- **On IdP initiated SSO, send readers to the RelayState specified landing page:** Check this box if people are opening links to specific articles, authenticating, and then getting kicked back to the homepage rather than redirected to the link they originally opened. (The default behavior is to send readers to the homepage. Using this option will send readers to the RelayState specified landing page a.k.a. the page they were originally trying to access!)
- **Sign all messages coming from this SP**
- **Sign metadata coming from this SP**
- **Sign all logout requests coming from this SP**
- **Require all IdP assertions to be signed**
- **Require all IdP messages to be signed**
- **Require all IdP assertions to be encrypted:** The assertions will be encrypted using the RSA-SHA256 algorithm. You'll need the **SP public key** found in the **SP metadata XML** in the **Service provider metadata** section.
- **Reader login on SSO ID match only:** The default behavior for ID matching is to login with a matching SSO ID. If no matching SSO ID is found, we then fall back to match on username / email. With this option selected, username / email will be ignored and only the SSO ID match is used for logins.