SAML SSO setup overview

Last Modified on 12/23/2024 1:18 pm EST

While specific individual steps vary based on your flavor of SAML Single Sign-On (SSO), at a high level, the overall process includes these steps:

1. Add the KnowledgeOwl SP info to your SAML SSO provider, found in **Security and access > Single sign-on** in the **Service provider metadata** section.
2. Add your IdP info to KnowledgeOwl in **Security and access > Single sign-on** in the **Identity provider metadata** section.
3. Upload the IdP certificate from your SAML SSO provider to KnowledgeOwl in **Security and access > Single sign-on** in the **Identity provider metadata** section.
4. Select **Enable SAML SSO** =in KnowledgeOwl in **Security and access > Single sign-on** in the **SAML settings** section, **SAML SSO behavior** subsection.
5. Add the KnowledgeOwl x509 certificate to your IdP (found in **Security and access > Single sign-on** in the **Service provider metadata** section, **SP metadata XML**).
6. Map SAML Attributes to fields in KnowledgeOwl to properly create reader accounts (SSO ID is required--you'll receive an error if you skip this step. Refer to Missing SSO ID mapping warning for more details)
    - For existing attributes that directly map to KnowledgeOwl fields, use the SAML attribute map.
    - To transform attribute values coming from your SSO provider (such as setting all readers to automatically be a member of one group in KnowledgeOwl), use Custom attribute map rules.
7. To help with troubleshooting or to see the attribute values being passed, select **Enable debug mode to troubleshoot issues** in **Security and access > Single sign-on** in the **SAML settings** section. Then try logging in with an account through your SAML SSO provider--instead of logging in to the knowledge base, it will display the information that's being passed over from SSO to KnowledgeOwl, so you can ensure a) Info is being passed over, and b) That you have chosen the correct attributes for your mappings.
8. *Optional:* To make it so that SAML SSO is the **only** access method for your knowledge base, select **Require all readers to log in via SAML SSO** in **Security and access > Single sign-on** in the **SAML settings** section.
9. *Optional:* If you're using SAML SSO as your only or primary reader authentication mechanism, set the **Unauthenticated access behavior** in **Security and access > Security settings** to **Redirect them to your SAML Login URL.**

For more detailed, step-by-step instructions, see:

- Configure SAML SSO (generic instructions)
- Configure SSO using Active Directory Federation Services (ADFS)
- Configure SSO using Azure Active Directory (Azure AD)
- Configure SSO using G Suite (formerly Google Apps)
- Configure SSO using Salesforce (this uses very different steps)