SAML SSO customers: Update your SAML signing x509 cert

Last Modified on 12/28/2022 12:24 pm EST

We've released an important security update affecting our SAML SSO customers:

We've updated the SAML signing cert we use from SHA1 to SHA256, a more secure certificate.

What this means

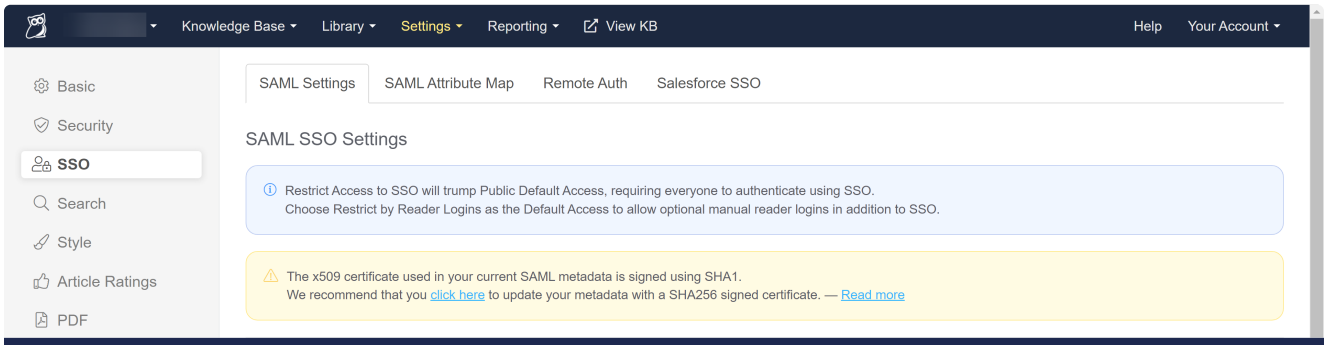
- All SAML SSO integrations set up from 19 July forward will automatically use the new certificate.
- For customers who have existing SAML SSO integrations, your existing cert will continue to work.

We **strongly recommend** you schedule time to upgrade your SAML SSO to use the newer, more secure x509 certificate. This is especially true for Azure AD SAML SSO customers, as Azure AD is phasing out support for SHA1 certificates.

Is my knowledge base impacted?

If you are using SAML SSO for authentication to your knowledge base and you set up that configuration at any point prior to today (19 July 2022), you need to upgrade.

If your SAML SSO integration is using the older certificate, you'll see a yellow warning message encouraging you to upgrade at the top of **Settings > SSO**:



Sample warning message in **Settings > SSO** indicating you need to update to the new certificate

How do I upgrade?

To generate the new certificate, click the "click here" link in that yellow warning message on **Settings > SSO**. Once the new certificate is generated, you'll need to update your SAML IdP with that new certificate.

See Update your x509 certificate for more detailed instructions. (These instructions will also open in the widget when you click the "Read more" link in that message. 😉)

Once you generate the new certificate, your existing SAML SSO integration **WILL NOT WORK** until it's fully updated with the new certificate, so we suggest you plan to do this during a downtime/maintenance window for your knowledge base.