Update your x509 certificate

Last Modified on 12/28/2022 12:25 pm EST

In July 2022, we rolled out a more secure version of our x509 certificate for SAML SSO.

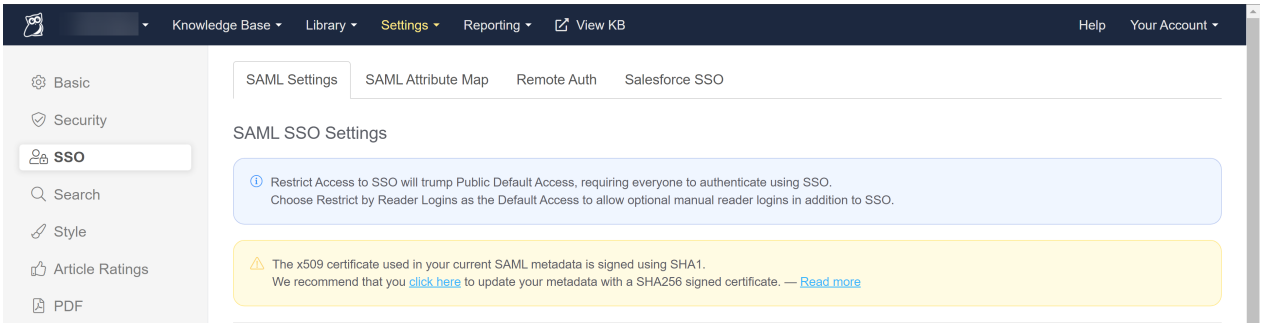
All SAML SSO integrations set up after this time automatically use the newer, more secure certificate.

For SAML SSO integrations enabled before 19 July 2022, you'll need to manually update to the new x509 certificate. See instructions below. This is especially important if you're using Azure AD.

Is my knowledge base affected?

To see if your knowledge base is affected by this change:

1. Go to **Settings > SSO**.
2. Be sure you're in the **SAML Settings** tab.
3. If you see a warning message near the top of the screen that says "The x509 certificate used in your current SAML metadata is signed using SHA1. We recommend that you click here to update your metadata with a SHA256 signed certificate", your knowledge base is using the older x509 certificate and needs to be updated. It should look something like this:



Update the certificate

The overall process for updating the certificate is:

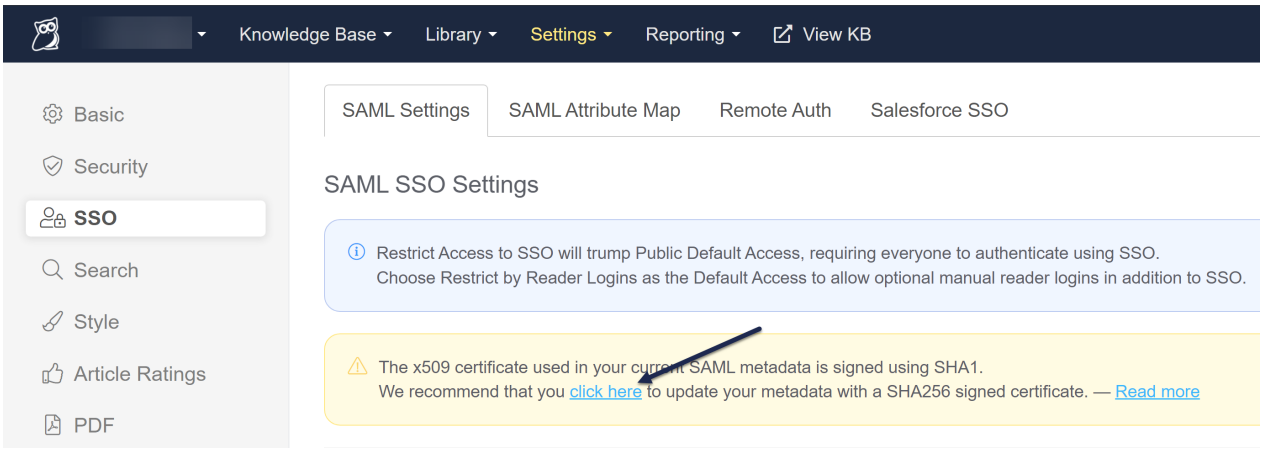
- In KnowledgeOwl, generate a new x509 certificate. Once generated, your existing SAML SSO integration will be broken.
- Copy the new KnowledgeOwl SP Metadata from KnowledgeOwl, paste it into a text editor, and save it in the format your IdP prefers for the certificate. (Common types include .crt, .cert, and .xml.)

- Update the x509 certificate with your IdP using that file.

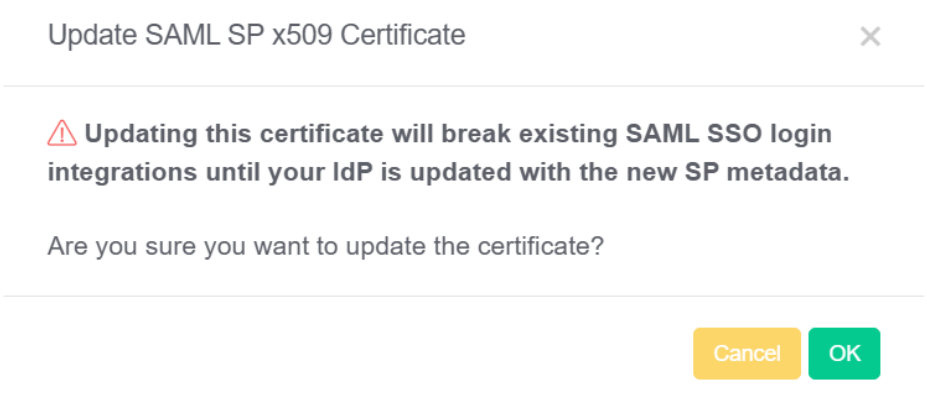
Once you generate a new x509 certificate, your existing SSO integration WILL NOT WORK. We recommend checking your IdP's process and file format for updating the SP x509 certificate before you begin this process, so you can update it as quickly as possible once you begin.

To begin updating the certificate, in KnowledgeOwl:

1. Go to **Settings > SSO**.
2. Be sure you're in the **SAML SSO Settings** tab.
3. In the warning message that appears near the top, click the **click here** link to begin generating the new x509 certificate:



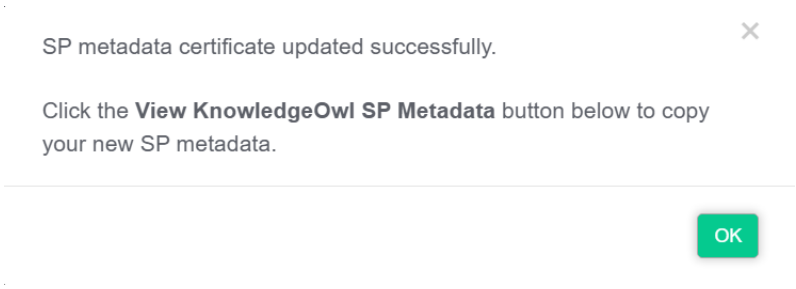
4. This will open a pop-up asking if you are sure you want to proceed. **Once you click OK in this pop-up, your existing SAML SSO login integrations will be broken until you finish updating the x509 certificate with your IdP.**



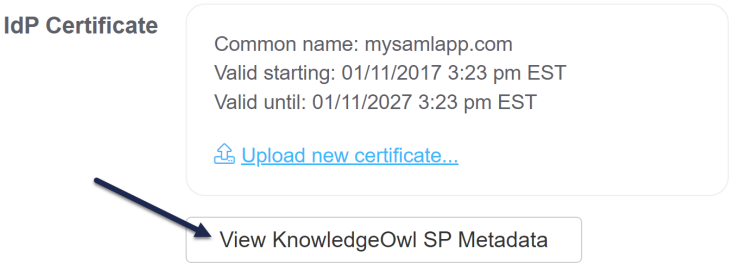
Certificate regeneration confirmation message; only click OK when you're ready to update your IdP certificate!

5. When you're ready, click **OK** to update the certificate.

6. **You'll get a confirmation message that the certificate has been updated:**



7. **You can now click the View KnowledgeOwl SP Metadata button in the IdP Certificate section to copy the updated certificate's XML:**



8. **From here, you'll need to update the x509 certificate with your IdP. These steps vary by provider:**
   - **For Active Directory Federation Services, see Configure SSO using Active Directory Federation Services (AD FS), Step 4: Add the KnowledgeOwl SP info to your IdP, steps 1-10.**
   - **For Azure Active Directory, see Configure SSO using Azure Active Directory (Azure AD).**
   - **For G Suite, see Configure SSO using G Suite (formerly Google Apps).**
   - **For all other SSO providers, see Configure SAML SSO (generic instructions) and your provider's documentation.**