# Update your x509 certificate

Last modified on 11/07/2026 12:01 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.



**Older x509 certificates**
For SAML SSO integrations enabled before 19 July 2022, please manually update to the new x509 certificate using the instructions below. This is especially important if you're using Microsoft Entra ID (formerly Azure AD).

## Is my knowledge base affected?

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

1. Go to **Security and access > Access & SSO**.
2. In the **Login methods** section, look at the **SAML** row. If it shows the warning "Uses an older SHA1 certificate", your knowledge base is using the older x509 certificate and needs to be updated.
3. To see the full message, select **Manage** next to **SAML** and open step 1, **Give these details to your identity provider**. Affected knowledge bases show: "Your metadata uses an older SHA1 certificate. Generate a SHA256 certificate, then give the updated metadata to your IdP."

## Update the certificate

The overall process for updating the certificate is:

- In KnowledgeOwl, generate a new x509 certificate. Once you generate the new certificate, your existing SAML SSO integration won't work!
- Download or copy the new KnowledgeOwl SP metadata from KnowledgeOwl 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.

To begin updating the certificate, in KnowledgeOwl:

1. Go to **Security and access > Access & SSO**.
2. In the **Login methods** section, select **Manage** next to **SAML**.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

3. Open step 1, **Give these details to your identity provider.**




4. In the SHA1 warning, select **Generate SHA256 certificate.**



**Don't break your SSO**
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.

5. Your browser asks you to confirm: "Generate a new SHA256 certificate? You will need to give the updated metadata to your identity provider." When you're ready, select **OK.** The certificate is generated right away, and a confirmation message appears: "New certificate generated. Give the updated metadata to your identity provider."

6. Still in step 1, get your updated metadata:
   - Select **Download metadata** to save it as `knowledgeowl-sp-metadata.xml`.
   - Or select **View metadata** to open the **KnowledgeOwl metadata** modal, then select **Copy to clipboard**, paste the text into a text editor of your choice, and save it using the file extension your IdP expects.

7. From here, you'll need to update the x509 certificate with your IdP. These steps vary by provider:
   - For Active Directory Federation Services, refer to 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, refer to Configure SSO using Azure Active Directory (Azure AD).
   - For G Suite, refer to Configure SSO using G Suite (formerly Google Apps).
   - For all other SSO providers, refer to Configure SAML SSO (generic instructions) and your provider's documentation.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.