Update Your SAML Certificate

Document generated 12/05/2024

PDF VERSION

Tags | **Authentication** | **SAML** | **Certificates** |

ADMIN PRIVILEGES REQUIRED

Applies to: Free **Basic** **Business** Enterprise

Enterprise users can access their documentation here. Find your plan.

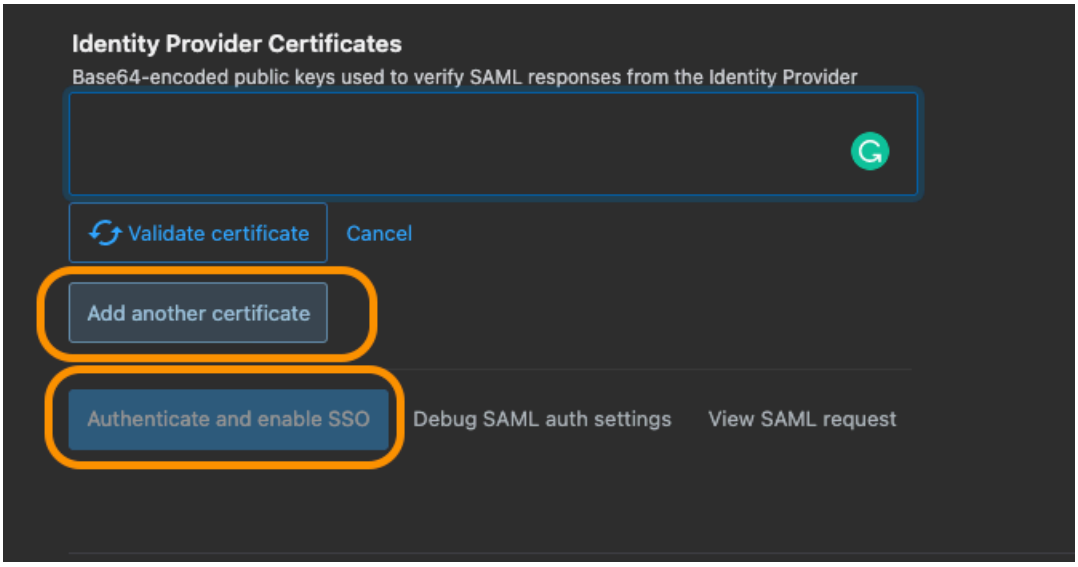
When you set up Single Sign-On (SSO) for your Team, one of the steps requires you to set up SAML certificates generated by your identity provider (IdP). SAML certificates are only valid for a certain time period. We can only use valid, non-expired certificates to verify that authentication requests from your IdP are legitimate and trustworthy.

30 days before your SAML certificates will expire, we will send you an automated warning about the upcoming expiration. As a Teams admin, you will see a warning at the top of your page saying "*Your SAML identity provider's certificates will expire soon. Add a new certificate to avoid losing access to this Team*".

We recommend that you act soon and add new certificates to your authentication settings. If your current certificates expire and you did not upload new certificates before that happens, your entire team will be locked out with an "X509 Credential Invalid" error. If that happens, contact our Support team here.

1. Upload New Identity Provider Certificate Certificate

To upload a new certificate, go to your Team's Settings - Authentication section. At the bottom, you will see a button to Add another certificate.



Click the *Add another certificate* button and paste the Base64-encoded public key that you got from your Identity Provider. Click *Validate Certificate* to verify the metadata for the public key. Looking at the metadata, make sure that the new certificate is valid and will be valid in the next weeks and months to come.

Once everything looks good, click on *Authenticate and enable*, to save the new certificate.

Need help? Submit an issue or question through our support portal.