

Update AWS Secrets Manager

AWS Secrets Manager is used to store the SAML Identity Provider (IdP) certificate securely. The SandboxStudio-API stack creates a secret for this purpose. You must update it with the correct certificate from your Identity Center application.

If the certificate is missing or incorrect, Sandbox Studio will not be able to validate SAML assertions, and user login will fail.

1. Get the secret ARN

- Check the outputs of the **SandboxStudio-API** CloudFormation stack.
- Look for the output key **IdpCertArn**.

2. Retrieve the IdP certificate

- Open the **IAM Identity Center application** you created for Sandbox Studio.
- Download the **SAML metadata XML** or copy the signing certificate directly.
- Ensure it is in **PEM format** (starts with `-----BEGIN CERTIFICATE-----`).

3. Update the secret

- In the **Hub account**, open **AWS Secrets Manager**.
- Find the secret with the ARN from step 1.
- Edit the secret value.
- Paste in the IdP certificate.

4. Save and test

- Save the new secret value.
- Restart the login flow in Sandbox Studio to confirm that SAML authentication works.

Revision #4

Created 2025-07-18 10:46:24 UTC by Winston

Updated 2025-08-27 09:30:44 UTC by Andy