

## Instructions to Update a Certificate for a Custom Google SAML Application

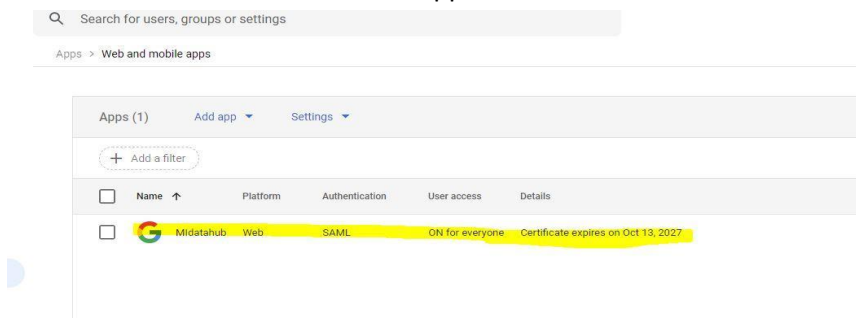
1. Login into the google domain as an admin
2. Select the Admin icon from the waffle



3. Use the top search bar, type web and mobile apps and select the web and mobile apps waffle.



4. Select the midatahub custom saml application\*:



\*The name may be different depending on how it was originally configured for your district.

5. Once the application is open select service provider details:



User access

To make the managed app available to select users, choose a group or organizational unit. [Learn more](#)

[View details](#)

ON for everyone

Service provider details

Certificate

Google\_2027-10-13-12214\_SAML2\_0  
(Expires Oct 13, 2027)

ACS URL

<https://adfs.midatahub.org/adfs/ls/>

Entity ID

<http://adfs.midatahub.org/adfs/services/trust>

SAML attribute mapping

Map Google directory user profile fields to SAML service provider attributes.

<http://schemas.xmlsoap.org/ws/2005/05/identity...>

Basic Information > Primary email

6. Select manage certificates:

Start URL

<https://milaunchpad.org>

☒ Signed response

**Certificate**

Select a certificate for this app

Certificate

Google\_2027-10-13-12214\_SAML2\_0 (Expires Oct 13, 2027)

[Manage certificates](#)

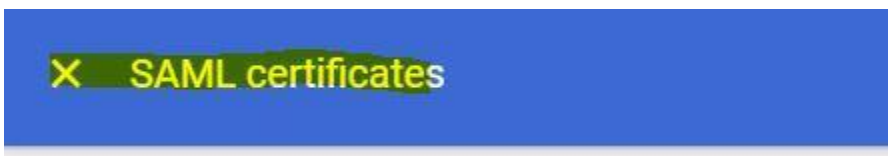
## 7. Select add certificate

SHA-256 fingerprint

DE:B5:30:95:A7:00:B3:5C:07:17:C0:17:85:B8:DC:A9:94:AC:BE:7B:9B:EB:C0:EE:91:FB:9A:12:85:36:D0:21

[ADD CERTIFICATE](#)

- Once the new cert is added close the SAML Certificates window:



9. Under service Provider details select the Certificate dropdown:

#### Certificate

Select a certificate for this app

Certificate

[Manage certificates](#)

10. Select the newly generated certificate (if the newly generated cert is not available refresh the page):

<https://milaunchpad.org>

☒ Signed response

#### Certificate

Select a certificate for this app

Google\_2027-10-24-114028\_SAML2\_0 (Expires Oct 24, 2027)

Choose certificate

[Manage certificates](#)

#### Name ID

11. Select Save at the bottom of the page

#### Certificate

Select a certificate for this app

Certificate

Google\_2027-10-24-114028\_SAML2\_0 (Expires Oct 24, 2027)

[Manage certificates](#)

#### Name ID

Defines the naming formats supported by the identity provider. [Learn more](#)

Name ID format

WIN\_DOMAIN\_QUALIFIED

Name ID

Basic Information > Primary email

CANCEL

SAVE

12. Select download metadata from the left navigation:

SAML

 Mldatahub

☒ TEST SAML LOGIN

 **DOWNLOAD METADATA**

 EDIT DETAILS

 DELETE APP



**MICHIGAN**  
**DataHub**

13. The following dialog is presented – select the download metadata button

## Download metadata

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. [Learn more](#)

**Option 1: Download IdP metadata**

DOWNLOAD METADATA

OR

**Option 2: Copy the SSO URL, entity ID, and certificate**

**SSO URL**

https://accounts.google.com/o/saml2/idp?idpid=C03mzadx1

**Entity ID**

https://accounts.google.com/o/saml2?idpid=C03mzadx1

**Certificate**

Google\_2027-10-24-114028\_SAML2\_0

Expires Oct 24, 2027

-----BEGIN CERTIFICATE-----  
MIIDdDCCAlYgAwIBAgIGAYQQcl//MA0GCSqGSIb3DQEBCwUAMHsxFD  
ASBqNVRBAoTCOdyb2dsZSRJ

14. Confirm the metadata has the new cert data by navigating to the downloaded metadata file and open it in a text or html browser window you should see the valid until tag reflects the new cert's expiration date:

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2027-10-24T18:40:28.000Z">  
    <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0<br/>-idp-metadata">  
        <md:keyDescriptor use="signing">  
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
                <ds:X509Data>  
                    <ds:X509Certificate>MIIDDCCAlYgAwIBAgIGAYQYQci//MAOGCSqGSIb3DQEBCwUAMHsxFDASBgNVBAoTC0dvb2dsZSBJbmMuMRYwFAYDVQQHEWlnb3VudGFpb2IwawVm3MQ8wDQYDVQQDEwZhbnBubGUxGDABGjNVAAsTD0dvb2dsZS5DbG9jaGVyY29ya2EMLAAKA1UEBHCVVMXzE=ARBGjNVAAGTCKnbhgblmb3JuaWwEWHwhcmlNMjIxMDI1MTk0NDt1LWU1dC01NTk0MTk0MDA1OTU0MTU1LnBvdy5EZA==-----BEGIN CERTIFICATE-----
```

15. Once confirmed that the new cert is contained in the file, please open a ticket to [miServiceDesk](#) requesting the federation be updated and attach the file.