**Autodesk on AWS: Getting HS & CC’s Set-up to Access Virtual Machines through Google**

Rev: 2020-09-22

# Setting up G Suite SAML 2.0 federation with Amazon AppStream 2.0

by Vinothkumar Narasimhan | on 29 MAY 2020 | in [Amazon AppStream 2.0](https://aws.amazon.com/blogs/desktop-and-application-streaming/category/desktop-app-streaming/amazon-appstream-2-0/),

<https://aws.amazon.com/blogs/desktop-and-application-streaming/setting-up-g-suite-saml-2-0-federation-with-amazon-appstream-2-0/>

<https://support.google.com/a/answer/6087519?hl=en>

This post walks through the following steps. Steps 2 & 3 are done by Mark Martin.

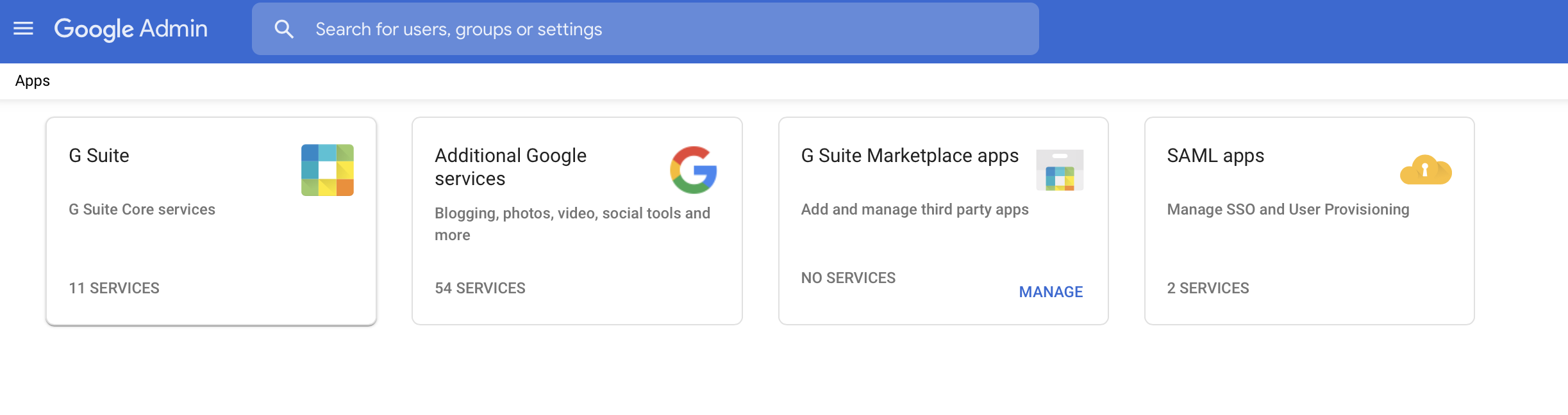
1. Create a SAML 2.0 application in the G Suite management console.
2. Create an AWS SAML IdP in IAM.
3. Create an IAM federation role.
4. Create a custom user attribute category in the G Suite admin console.
5. Add custom SAML attribute mappings.
6. Populate the values of the custom SAML attributes for a user.
7. Assign the SAML application to the user.

# ----

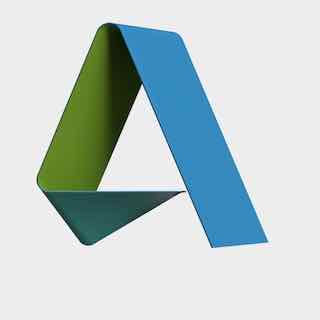
To complete this tutorial, you need the following:

* A G Suite subscription with an admin account

## **Step 1: Create a SAML 2.0 application in the G Suite management console**



1. Log in into your G Suite admin console using your admin account and choose **Apps, SAML Apps**.
2. Choose the plus icon (**+**) to create a new SAML application and choose **SETUP MY OWN CUSTOM APP**.
3. **Download the IdP metadata FILE and save it locally** 
   1. Append the name of your high school, or district at the end – depending who it will cover (e.g. GoogleIDPMetadata-SanLeandroUSD).
   2. Send this to Mark Martin as soon as you do it, [markmartin@peralta.edu](mailto:markmartin@peralta.edu)
4. Choose **Next**.
5. Provide a name for your SAML 2.0 application (ex. Autodesk CAD Software), description, and an optional logo (below) to easily identify the application in the user login portal. After entering the inputs, choose **Next**.



1. Provide the following input for various fields and then choose **Next**.

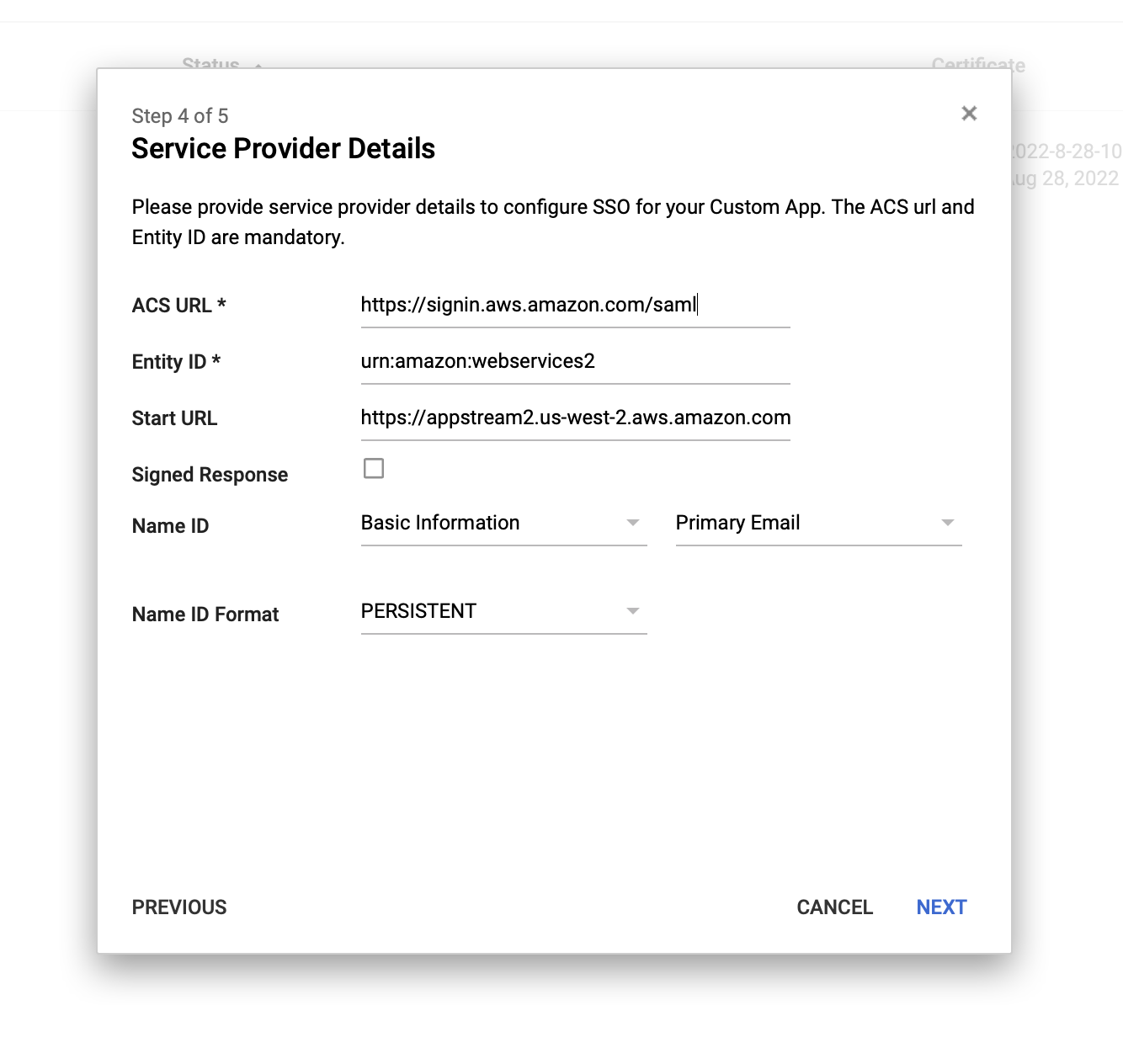
* **ACS URL** — https://signin.aws.amazon.com/saml
* **Entity ID** — urn:amazon:webservices

This is a parameter used by AWS (the service provider) to uniquely identify the SAML application. Every stack is configured as a SAML application in G Suite. You need to have a unique entity ID value for every AppStream 2.0 SAML application. If you have more than on Appstream SAML, just add a numerical counter as a suffix to this value. For example:

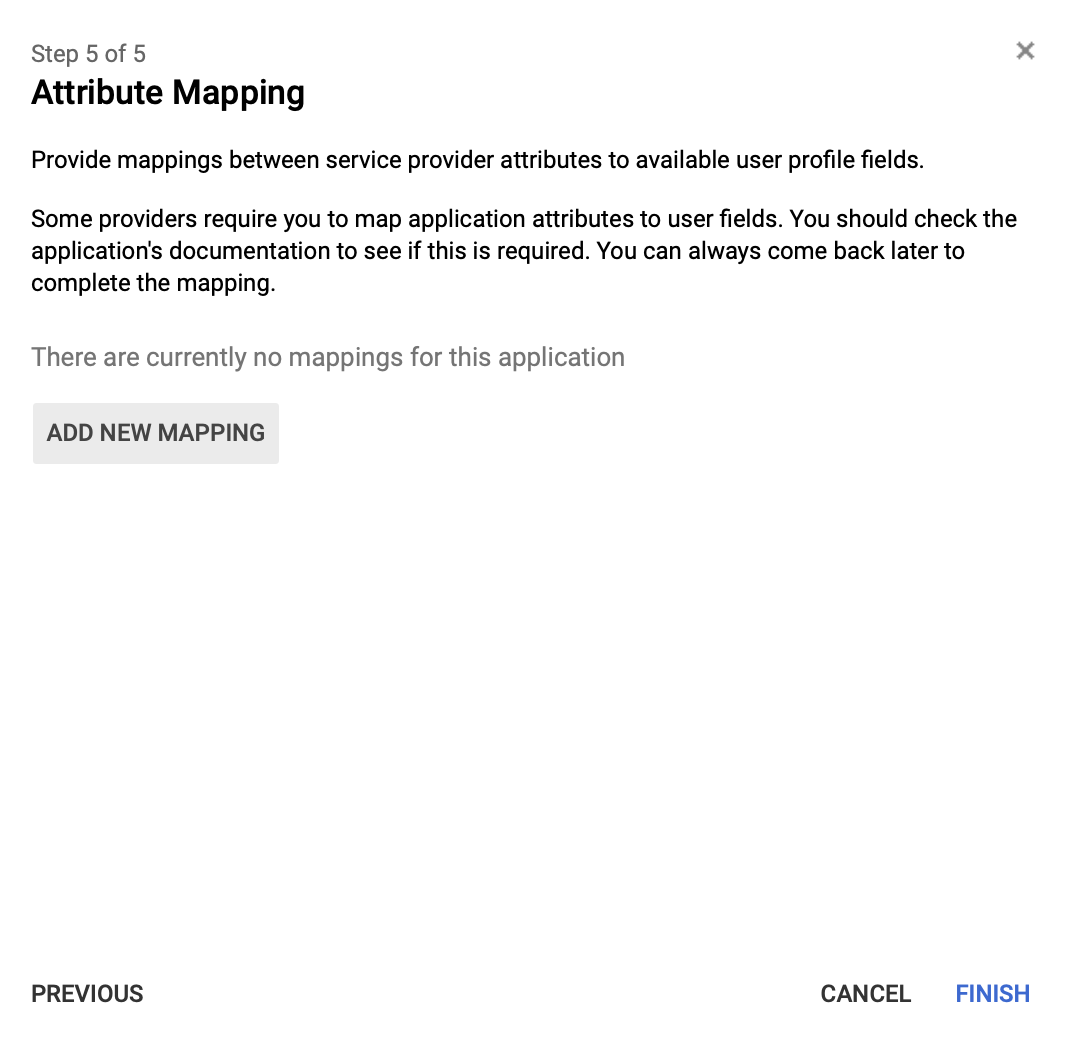
* + Stack2 app Entity ID – urn:amazon:webservices2
* **Start URL** — Relay state URL of your AppStream 2.0 stack. Use the following URL

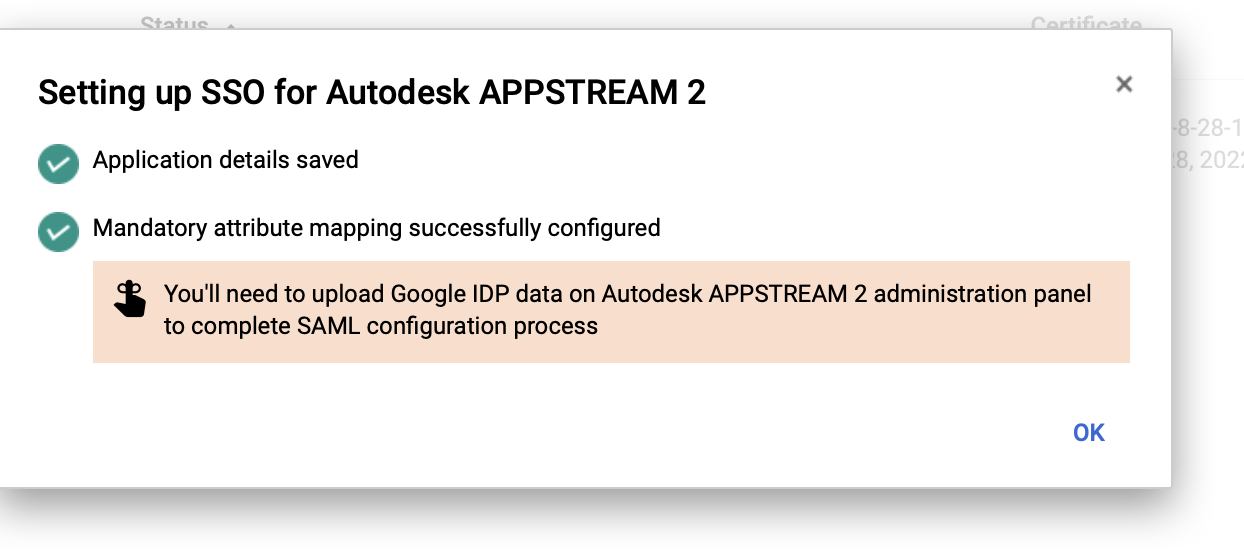
*https://*appstream2.us-west-2.aws.amazon.com/saml*?stack=*STACK\_AutodeskCADSoftware*&accountId=*550228651083*&app=*Desktop

* + For more information, see [Step 6: Configure the Relay State of Your Federation](https://docs.aws.amazon.com/appstream2/latest/developerguide/external-identity-providers-setting-up-saml.html#external-identity-providers-relay-state)
* **Signed Response** — Leave it unchecked
* **Name ID** — Choose: Basic Information, Primary Email
* **Name ID Format** — Choose: PERSISTENT



1. Skip the next page, Attribute Mapping, and choose **Finish**.



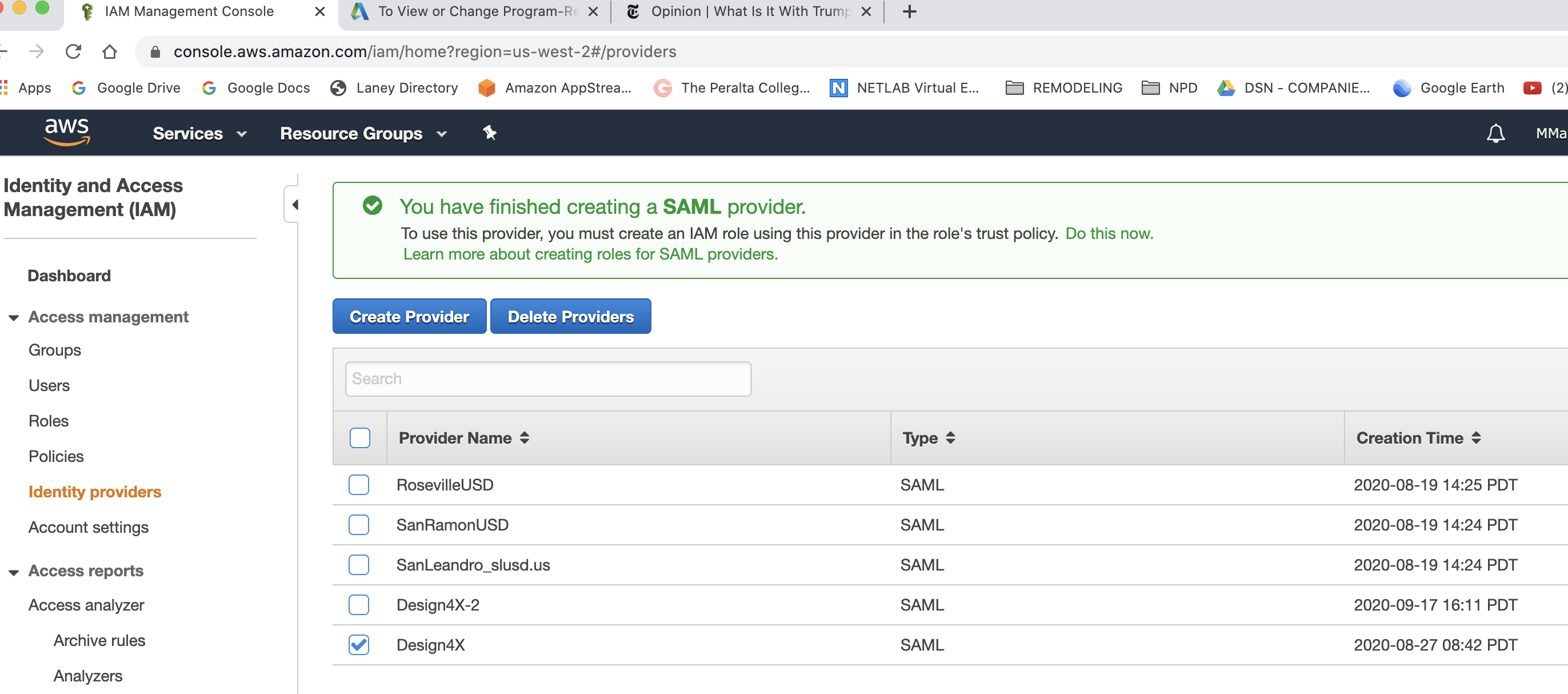


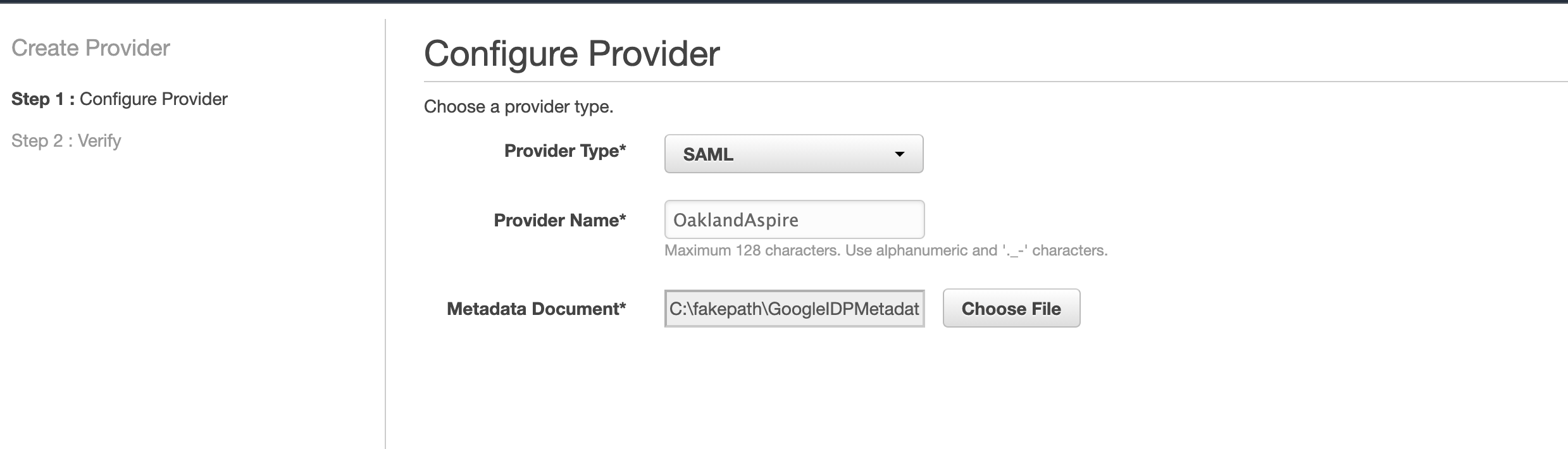
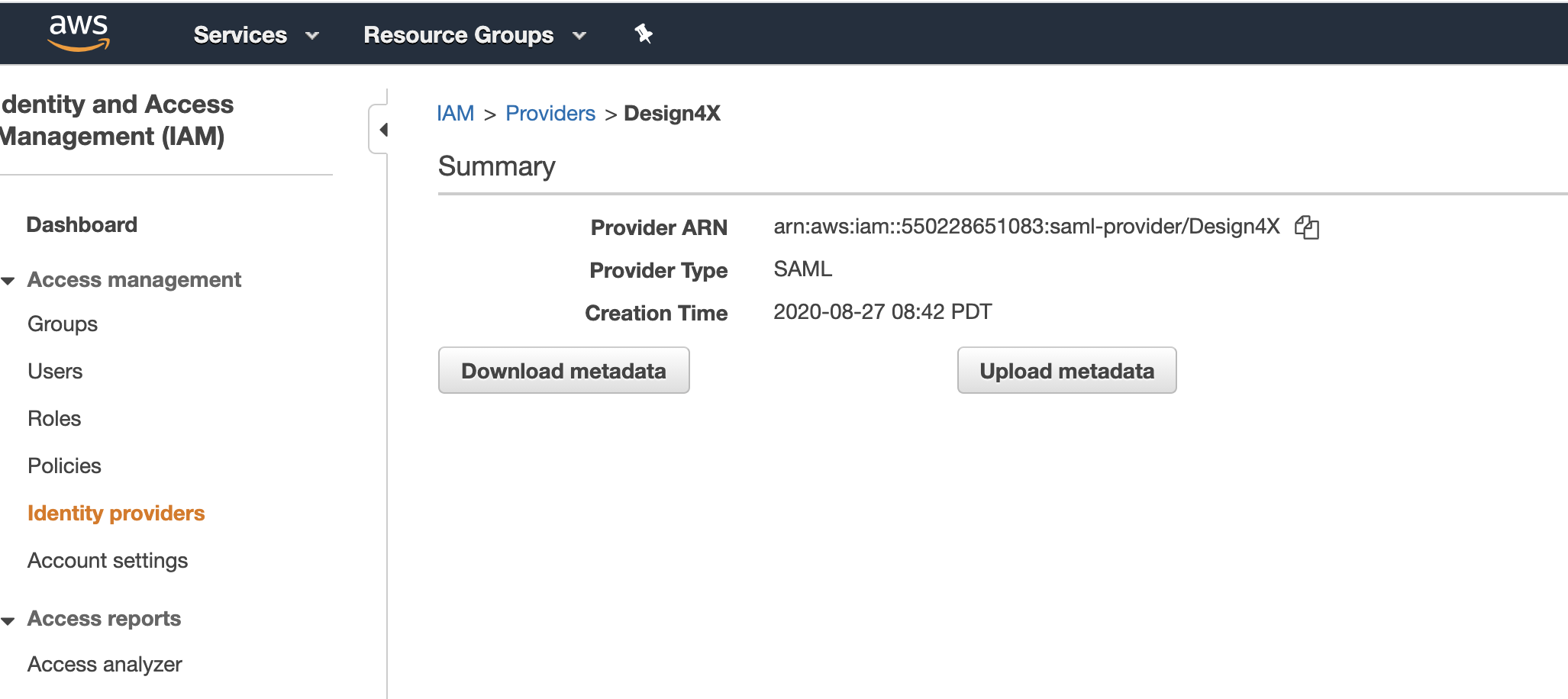
## **---------- Steps 2 & 3 will be done by Mark Martin ----------**

## **MM - Step 2: Create an AWS SAML IdP in IAM**

You need an IdP created in IAM. This IdP defines your organization’s IdP-to-AWS trust relationship using the metadata document generated by the IdP software in your organization. For more information and instructions, see [Creating and Managing a SAML Identity Provider (AWS Management Console)](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_create_saml.html#idp-manage-identityprovider-console).

1. For the IdP metadata, use the metadata file SENT BY EACH SCHOOL IT earlier from the G Suite console.
2. After you create the IdP, note the IdP ARN available from the details page. You need it later.



Example of IDP ARN - arn:aws:iam::550228651083:saml-provider/OaklandAspire

## **MM - Step 3: Create an IAM federation role**

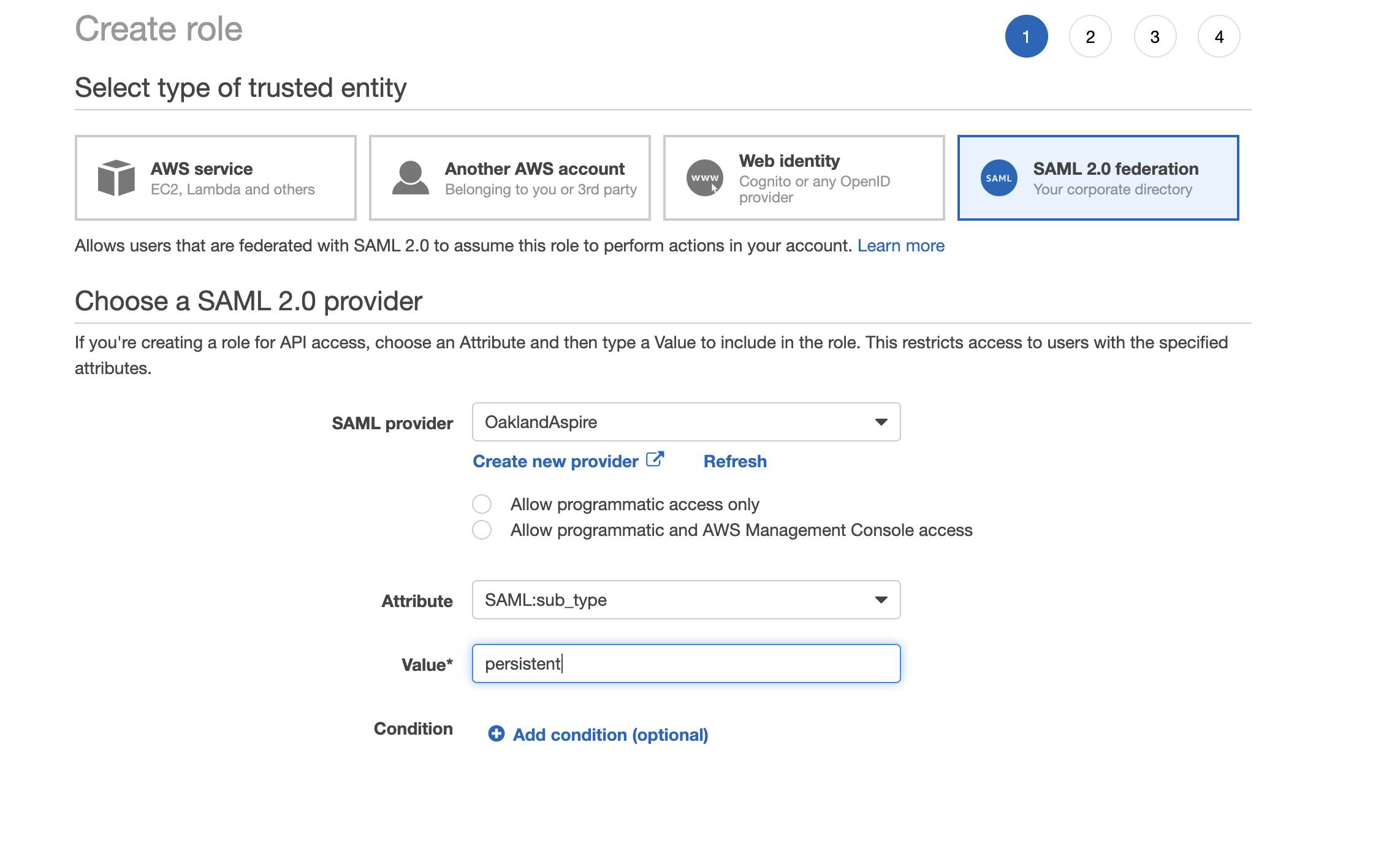
You need an IAM role to provide users with the permissions to access an AppStream 2.0 stack. The permissions defined in this IAM role dictate the stacks to which the federating users have access.

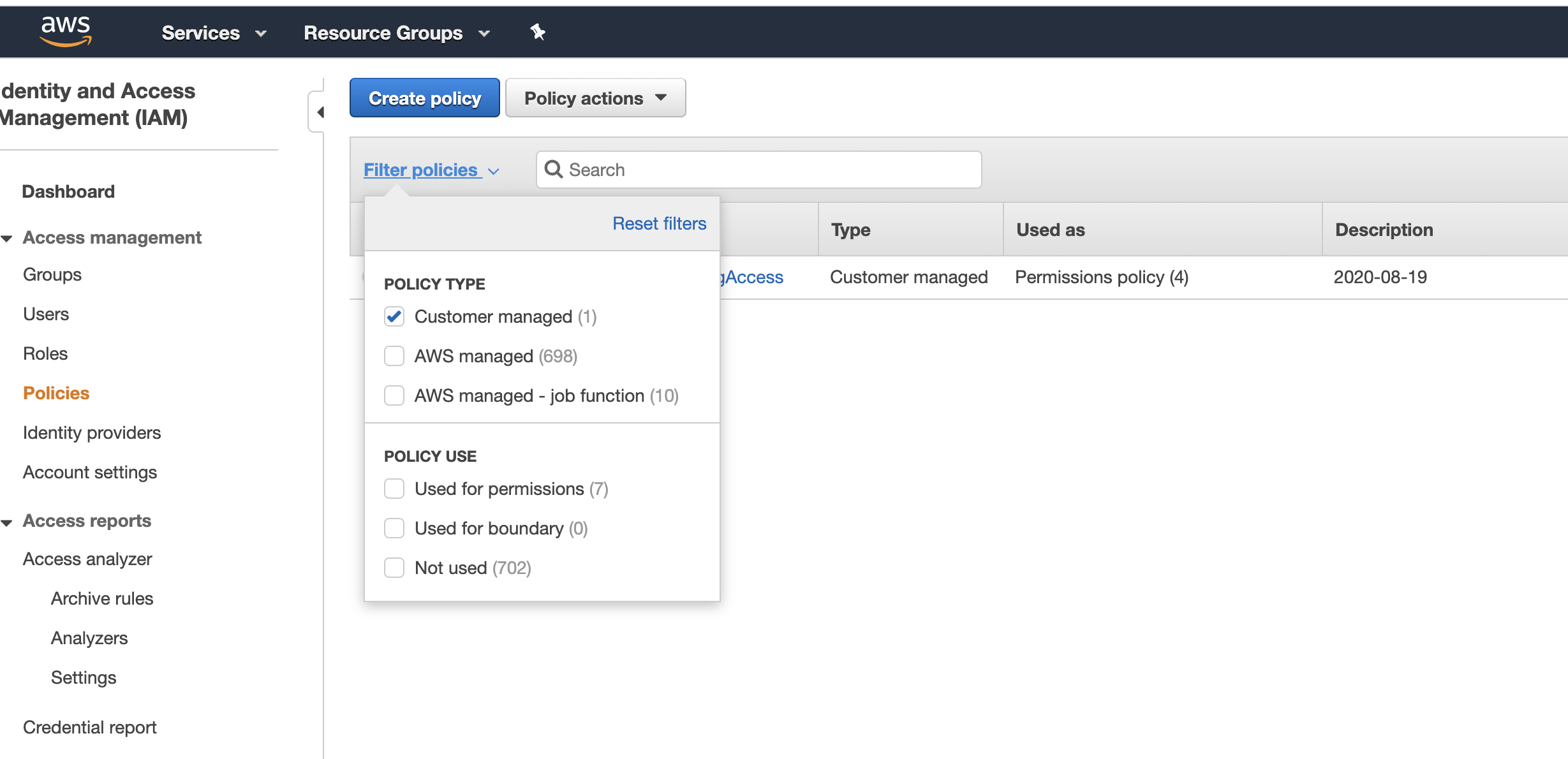
You can choose to provide permissions to all stacks in your AWS account or individually list the stacks that can be accessed by the user assuming this role on federation.  After you create the IAM role, note the role ARN available from the details page. You need it later.

For more information and instructions, see

[Step 2: Create a SAML 2.0 Federation IAM Role](https://docs.aws.amazon.com/appstream2/latest/developerguide/external-identity-providers-setting-up-saml.html#external-identity-providers-grantperms) and

[Step 3: Embed an Inline Policy for the IAM Role](https://docs.aws.amazon.com/appstream2/latest/developerguide/external-identity-providers-setting-up-saml.html#external-identity-providers-embed-inline-policy-for-IAM-role).

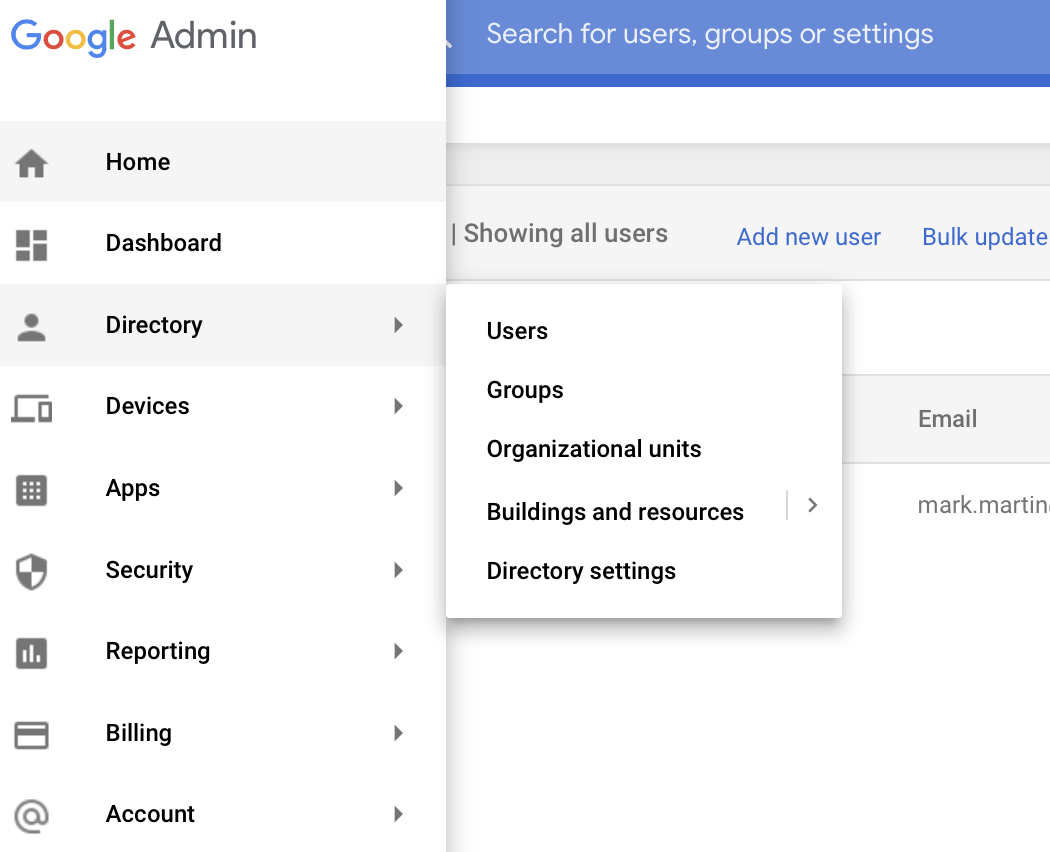




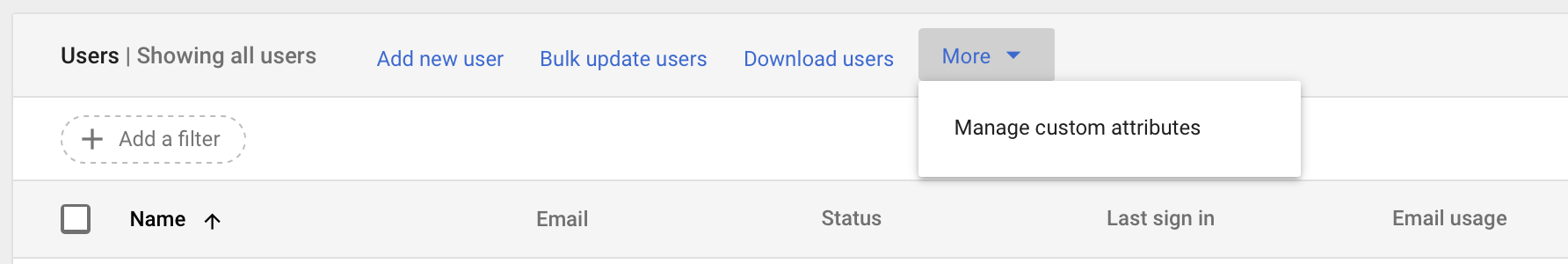
## **---------- Steps 2 & 3 complete ----------**

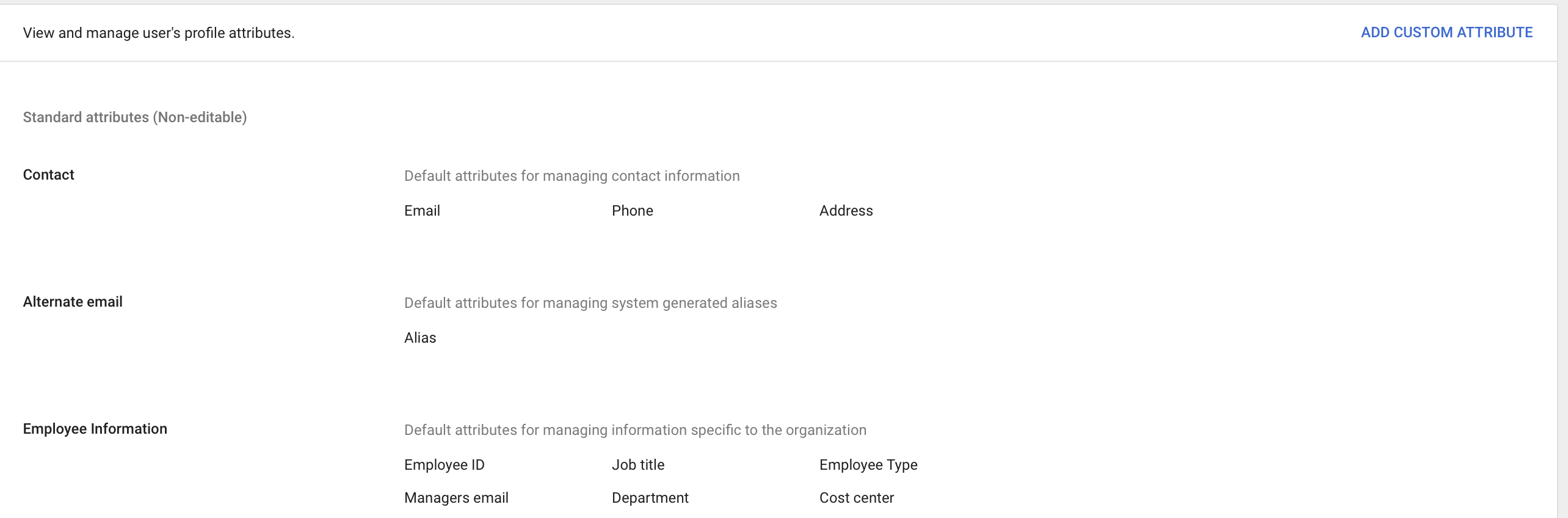
## **Step 4: Create a custom user attribute category in the G Suite admin console**

1. Navigate to the users dashboard by choosing **Directory, Users**.



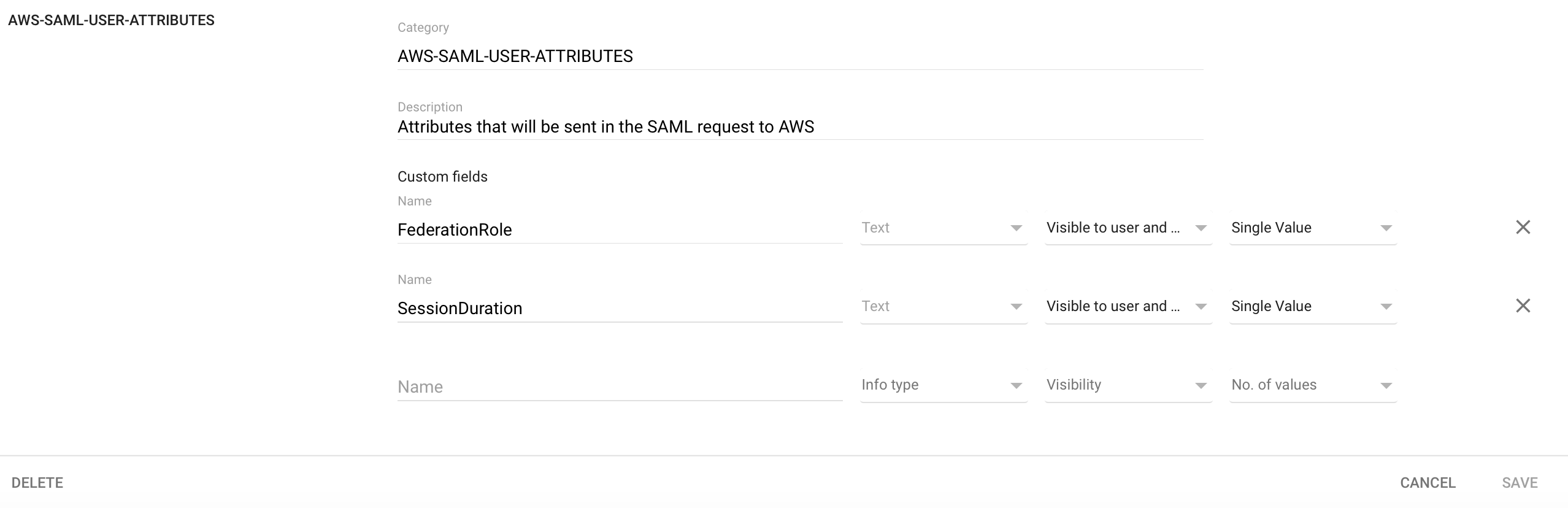
1. From the top right corner in the Users dashboard, choose **Manage Custom Attributes, choose ADD CUSTOM ATTRIBUTE**.





1. Provide a name for the category (ex: AWS-SAML-USER-ATTRIBUTES) and a description, add the SAML attributes as defined below, and then choose **Add**.

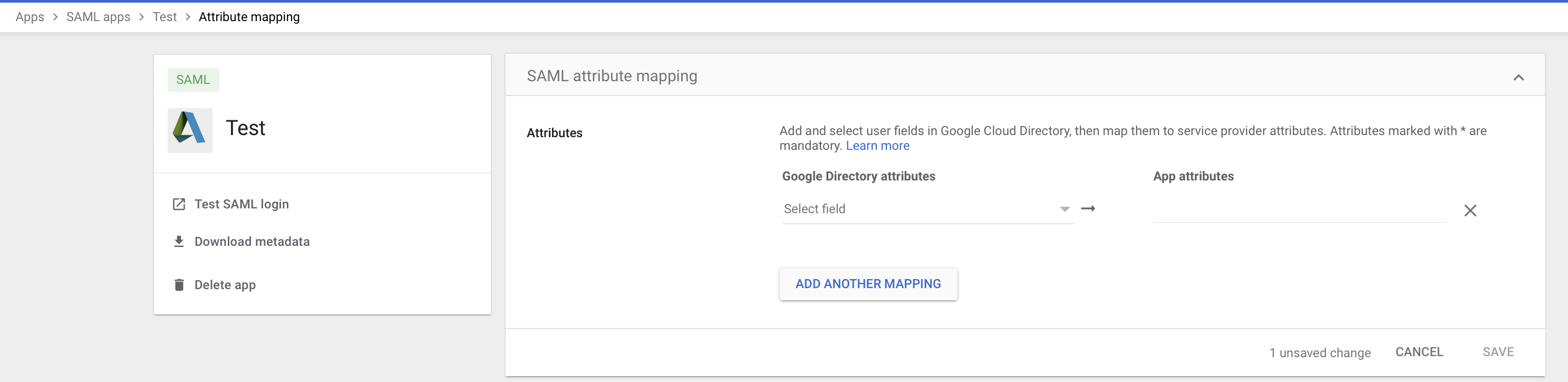
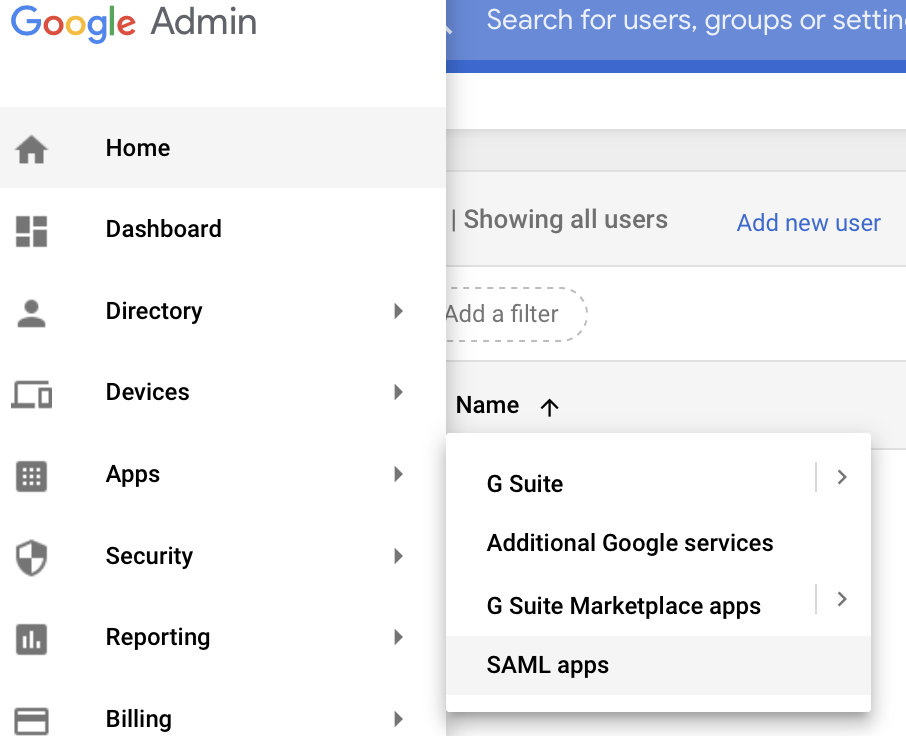
* **Attribute name** — FederationRole, Text, Visible to admin, Single Value
* **Attribute name** — SessionDuration, Text, Visible to admin, Single Value



## **Step 5: Add custom SAML attribute mappings**

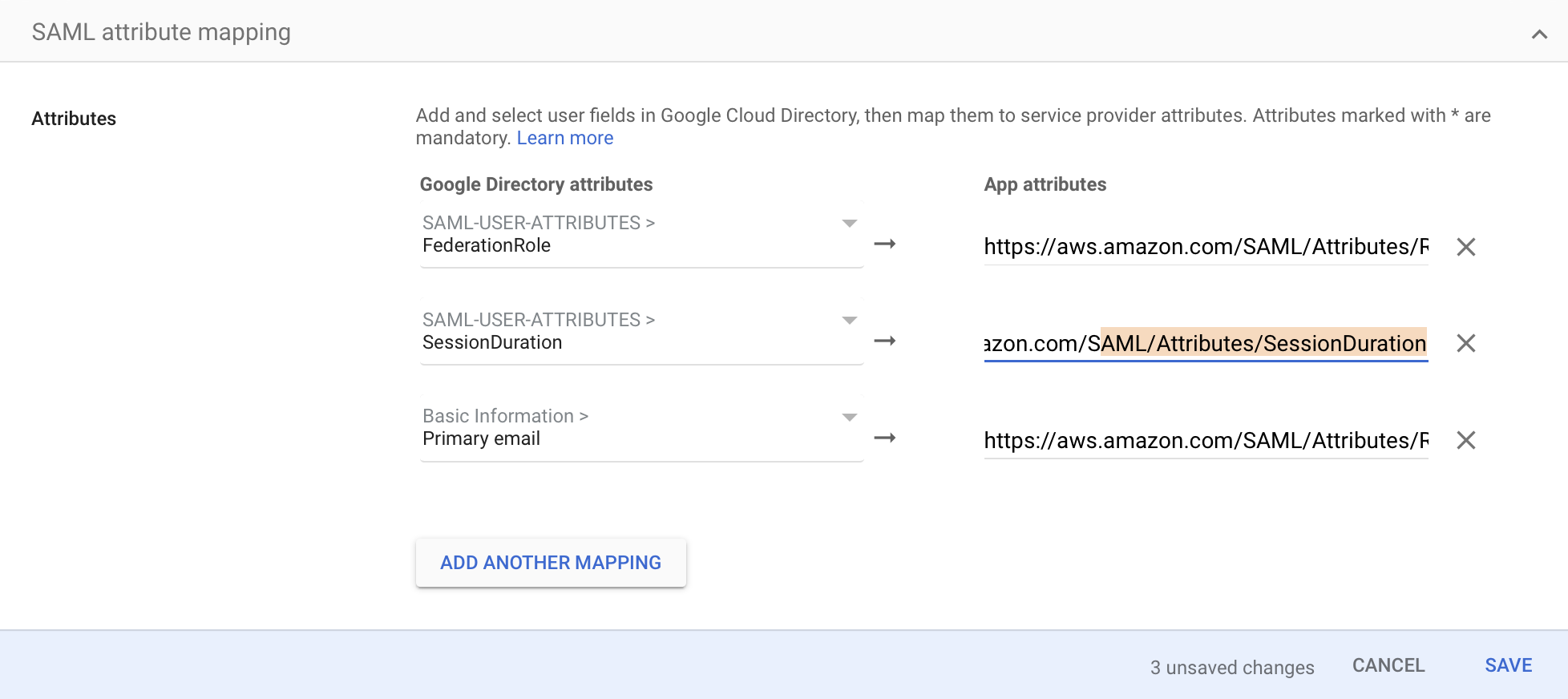
Navigate to the newly created SAML app.

1. Choose**Main menu, Apps, SAML Apps** and select the newly created application**.**



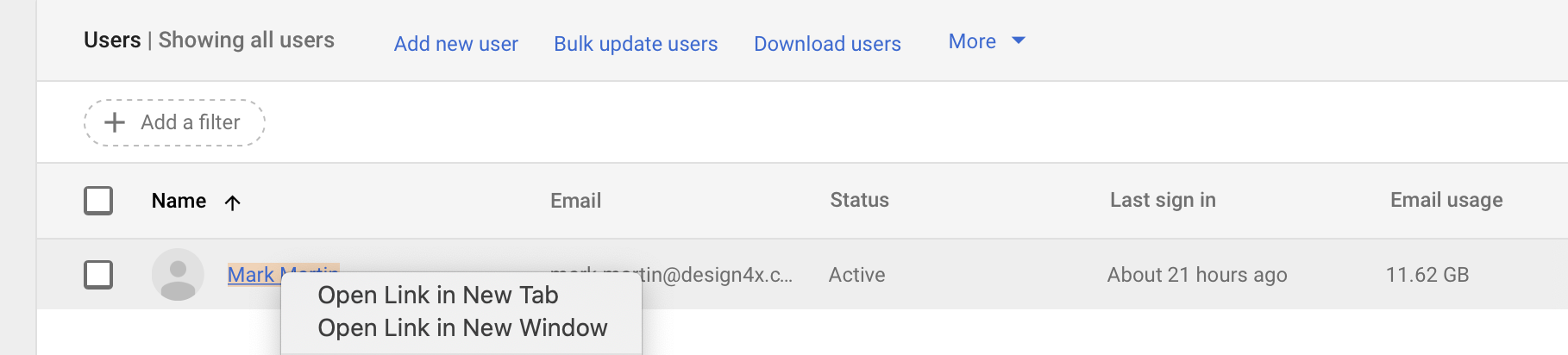
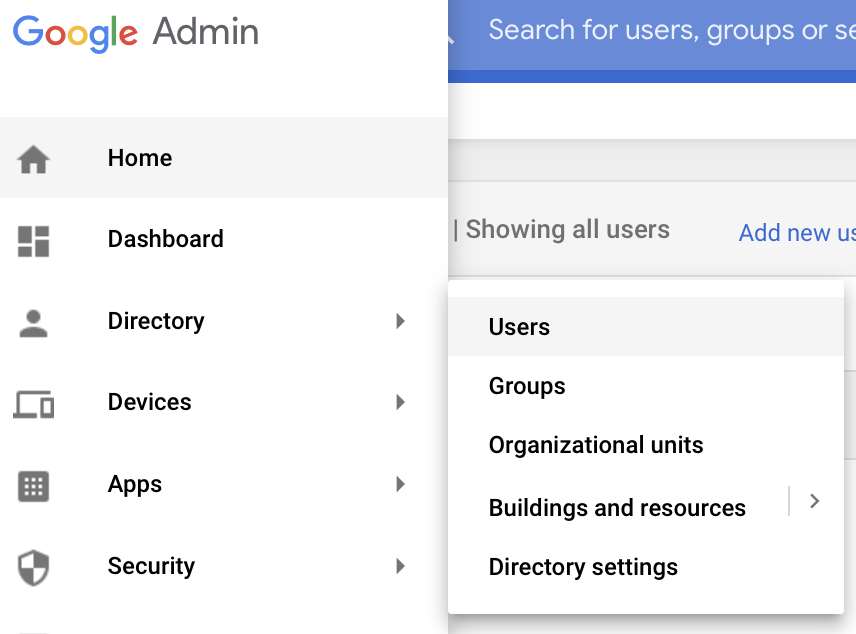
1. Choose **Attribute Mapping**, **Add New Mapping**, add three mappings as defined below, and then choose **Save**.

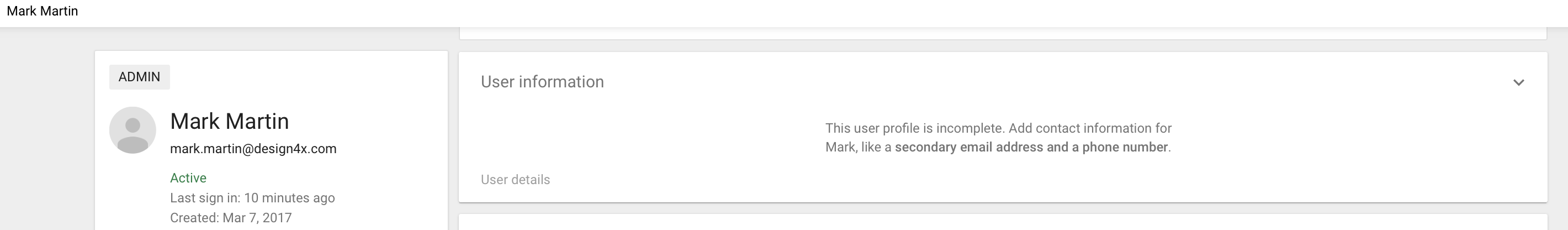
* **Application attribute (**AWS-SAML-ATTRIBUTES, FederationRole) — https://aws.amazon.com/SAML/Attributes/Role
* **Application attribute (**AWS-SAML-ATTRIBUTES, SessionDuration) — https://aws.amazon.com/SAML/Attributes/SessionDuration
* **Application attribute (**Basic Information, Primary Email) —https://aws.amazon.com/SAML/Attributes/RoleSessionName



## **Step 6: Populate the values of the custom SAML attributes for a user**

1. Select a user whose custom attribute values have to be updated from the **Users** dashboard. In the **User details** page, choose **User Information**.







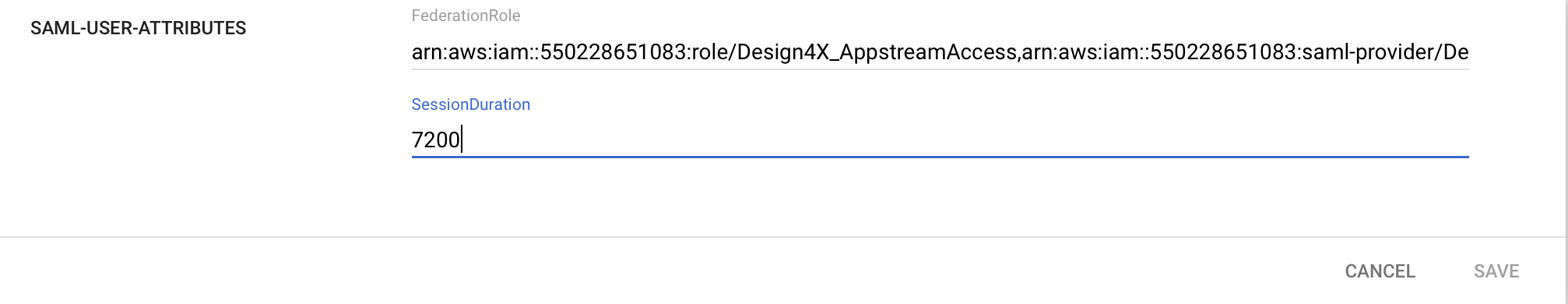
1. Edit the values for AWS-SAML-USER-ATTRIBUTES (or whatever name you previously gave this attribute), the custom attribute category, as defined below, and choose **Save**.

* **Federation Role** — Comma-separated string of the IAM federation role ARN and IdP ARN in the following format: <Role-ARN>,<IDP-ARN>

arn:aws:iam::550228651083:role/*<SchoolDescrip>*,arn:aws:iam::550228651083:saml-provider/*<SchoolName>*

***<SchoolDescrip> & <SchoolName>*** *will be sent to you after receiving the Metadata file from Step 1 (give me a day or two)*

* **SessionDuration** — **7200** The maximum duration of the AppStream 2.0 session in seconds (so 2 hours).

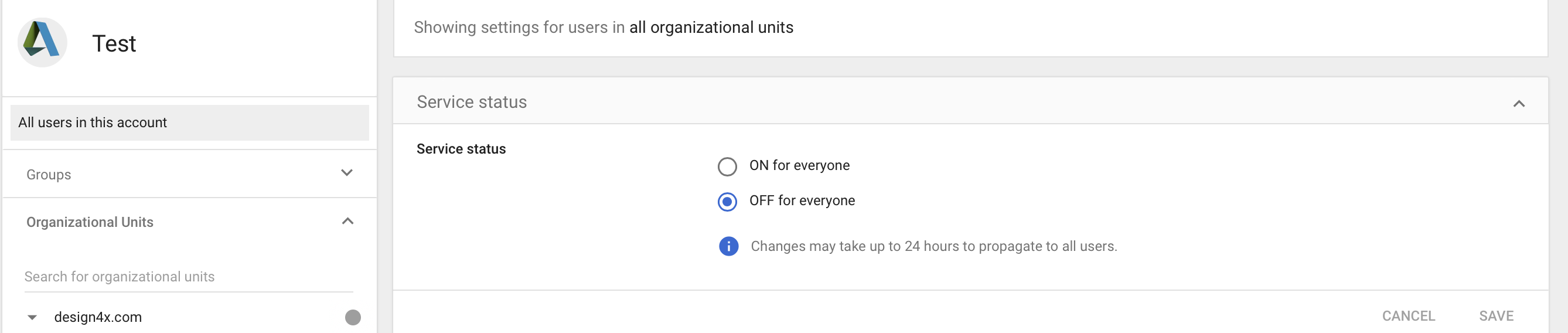


1. Repeat the steps for other users to whom to assign this SAML application. To avoid editing the SAML attribute values manually for every user, follow the steps at the end of this guide to programmatically update the custom user attribute values using a Python script.

## **Step 7: Assign the SAML application to the user**

Choose the SAML application from the **Apps** dashboard.  
From the details page, you can choose to do one of the following:

* Turn on the app for every user in your G Suite account.
* Turn on the app for a selective organization under your G Suite account.



Test the federation by choosing the SAML apps from the Google Apps menu. You may have to choose **More** to see the SAML app.

# Update custom SAML user attribute values programmatically for multiple values

G Suite does not allow you the option to bulk edit users and update their SAML attribute values.  To do that, you have to use the G Suite admin SDK to programmatically update the details of multiple users.

The G Suite Admin SDK offers support for multiple programming languages like Python and Java. In this post, you use Python.

Before using this script, you need to install Python, PIP, and a few Google Python libraries on your machine from which you will be executing this script::

* For more information about installing Python, see [Python For Beginners](https://www.python.org/about/gettingstarted/).
* For more information about installing PIP, see [Installation](https://pip.pypa.io/en/stable/installing/) in the pip 10.0.1 documentation.
* To install the required Google Python Libraries, after you install PIP, launch a terminal window and run the following command: pip install –upgrade google-api-python-client google-auth-httplib2 google-auth-oauthlib

Follow the Google Directory API Python QuickStart to enable the Directory API, configure your OAuth client for Desktop app, and download your credentials.json file. This file will need to saved in the same path as the script, below.

The following Python script extracts all the users in your G Suite domain and updates the FederationRole and SessionDuration values of the custom user category SAML-USER-ATTRIBUTES. You can apply the settings for all users in your G Suite domain or use the search filters of the users.list API to apply the changes to only a selected set of users. For more information, see [Users: list](https://developers.google.com/admin-sdk/directory/v1/reference/users/list) in the G Suite Admin SDK documentation.

When you execute the script, a Google form pops up. Sign in using your admin credentials, consent to the script accessing the Directory API, and choose **Submit**.

[Python Script found here](https://aws.amazon.com/blogs/desktop-and-application-streaming/setting-up-g-suite-saml-2-0-federation-with-amazon-appstream-2-0/)

# Conclusion

This completes the walkthrough for configuring G Suite SSO for SAML 2.0 federation to AppStream 2.0. For every AppStream 2.0 stack, you have to create a separate SAML application. To learn more, see [Single Sign-on Access to AppStream 2.0 Using SAML 2.0](https://docs.aws.amazon.com/appstream2/latest/developerguide/external-identity-providers.html).

To learn more about AppStream 2.0, see the following:

* [Amazon AppStream 2.0 product page](http://aws.amazon.com/appstream2)
* [Amazon AppStream 2.0 documentation](http://aws.amazon.com/documentation/appstream2)
* [AppStream 2.0 Pricing](http://aws.amazon.com/appstream2/pricing)

----------------

**Bandwidth recommended for students to use AWS**

<https://docs.aws.amazon.com/appstream2/latest/developerguide/bandwidth-recommendations-user-connections.html>

The following table provides guidance on the recommended network bandwidth and latency for AppStream 2.0 streaming sessions based on common workloads.

For each workload, the bandwidth recommendation is based on what an individual user might require at a specific point in time. The recommendation does not reflect the bandwidth required for sustained throughput. When only a few pixels change on the screen during a streaming session, the sustained throughput is much lower. Although users who have less bandwidth available can still stream their applications, the frame rate or image quality may not be optimal.

| **Workload** | **Description** | **Bandwidth recommended per user** | **Recommended maximum roundtrip latency** |
| --- | --- | --- | --- |
| Line of business applications | Document writing applications, database analysis utilities | 2 Mbps | < 150 ms |
| Graphics applications | Computer-aided design and modeling applications, photo and video editing | 5 Mbps | < 100 ms |
| High fidelity | High-fidelity datasets or maps across multiple monitors | 10 Mbps | < 50 ms |