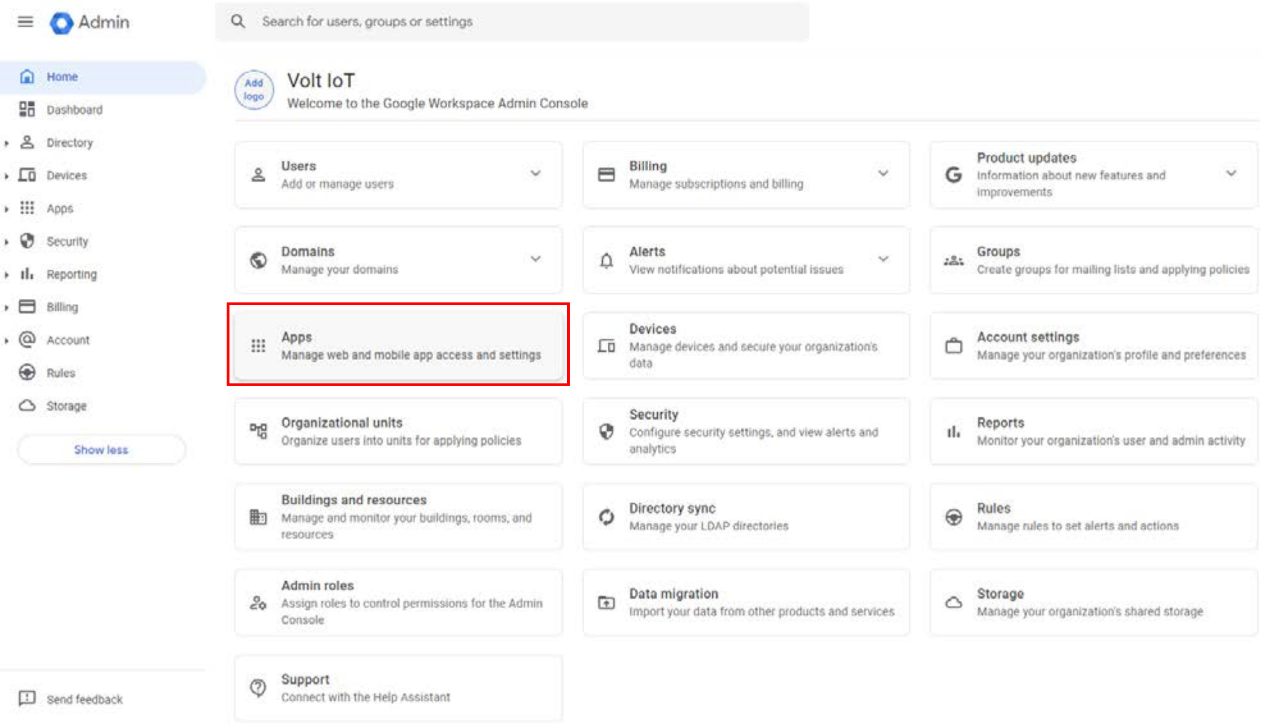
How to configure Single sign-on with Google Workspace to control access

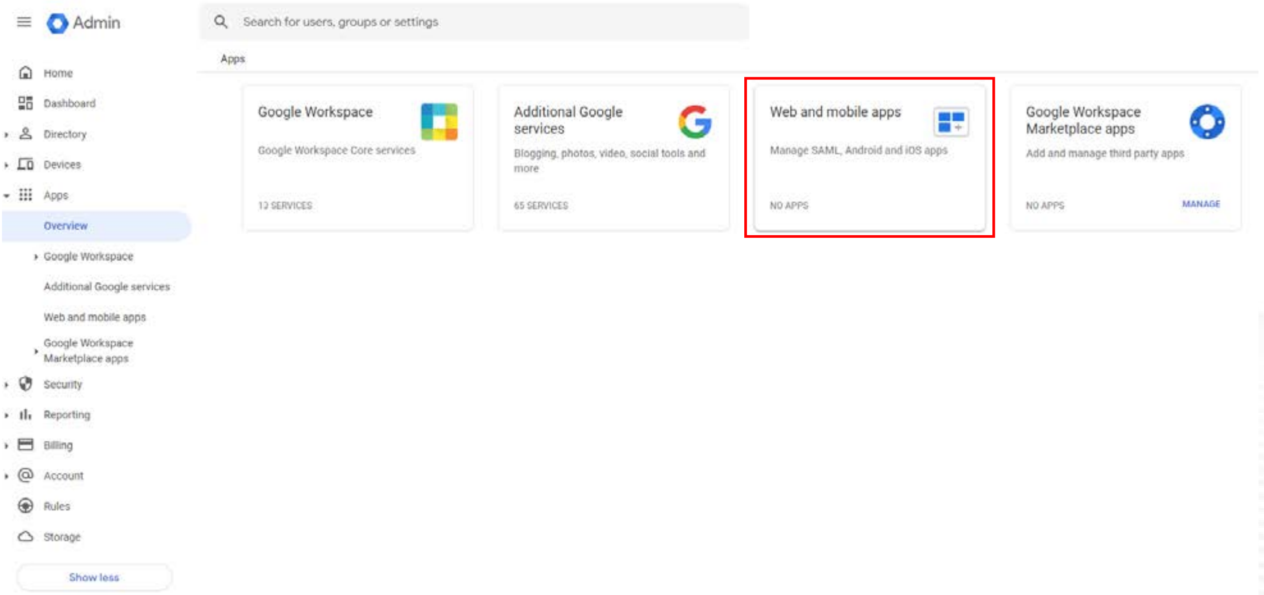
Google Workspace - Volt-IoT SAML 2.0

The objective of this article is to demonstrate the steps to be performed in Volt-IoT SAML 2.0 within Google Workspace to enable Single sign-on (SSO) in a centralized and secure way of controlling access to Volt-IoT Application

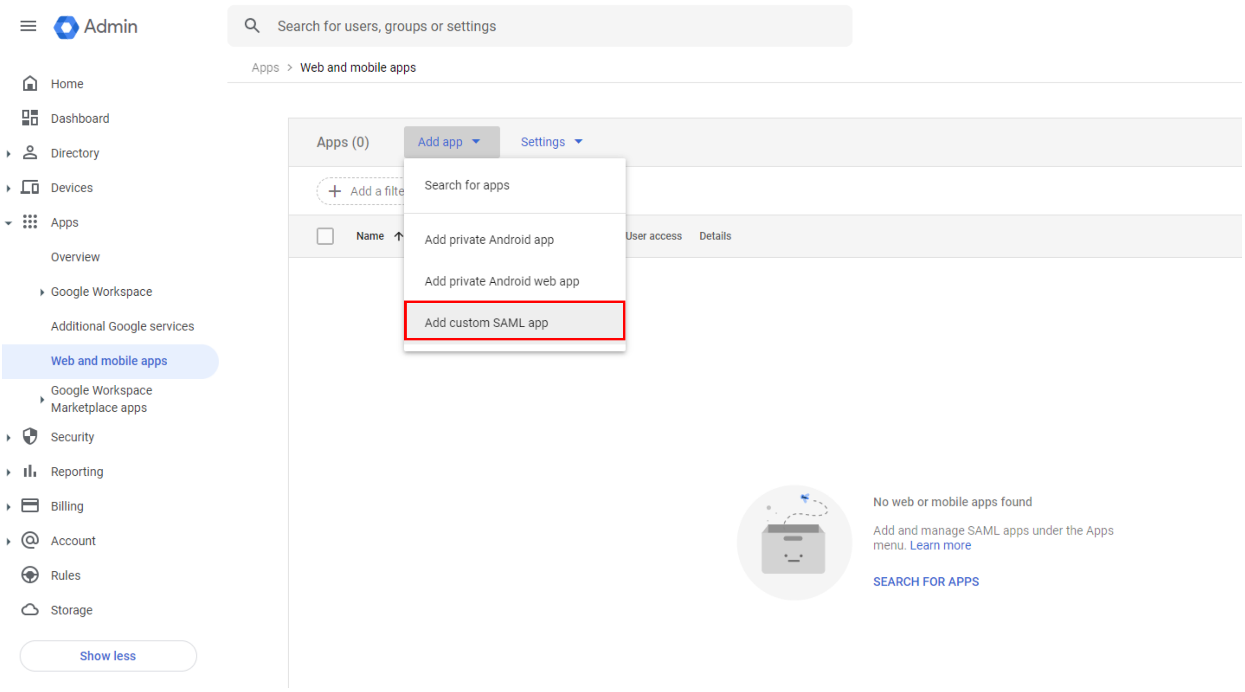
1. Login to your Google Workspace admin console and select **Apps.**


Admin
Search for users, groups or settings
Home
Dashboard
Directory
Devices
Apps
Security
Reporting
Billing
Account
Rules
Storage
Show less
Send feedback
Add logo
Volt IoT
Welcome to the Google Workspace Admin Console
Users
Add or manage users
Billing
Manage subscriptions and billing
Product updates
Information about new features and improvements
Domains
Manage your domains
Alerts
View notifications about potential issues
Groups
Create groups for mailing lists and applying policies
Apps
Manage web and mobile app access and settings
Devices
Manage devices and secure your organization's data
Account settings
Manage your organization's profile and preferences
Organizational units
Organize users into units for applying policies
Security
Configure security settings, and view alerts and analytics
Reports
Monitor your organization's user and admin activity
Buildings and resources
Manage and monitor your buildings, rooms, and resources
Directory sync
Manage your LDAP directories
Rules
Manage rules to set alerts and actions
Admin roles
Assign roles to control permissions for the Admin Console
Data migration
Import your data from other products and services
Storage
Manage your organization's shared storage
Support
Connect with the Help Assistant

2. Select **Web and mobile apps**.


Admin
Search for users, groups or settings
Home
Dashboard
Directory
Devices
Apps
Overview
Google Workspace
Additional Google services
Web and mobile apps
Google Workspace Marketplace apps
Security
Reporting
Billing
Account
Rules
Storage
Show less
Apps
Google Workspace
Google Workspace Core services
13 SERVICES
Additional Google services
Blogging, photos, video, social tools and more
65 SERVICES
Web and mobile apps
Manage SAML, Android and iOS apps
NO APPS
Google Workspace Marketplace apps
Add and manage third party apps
NO APPS
MANAGE

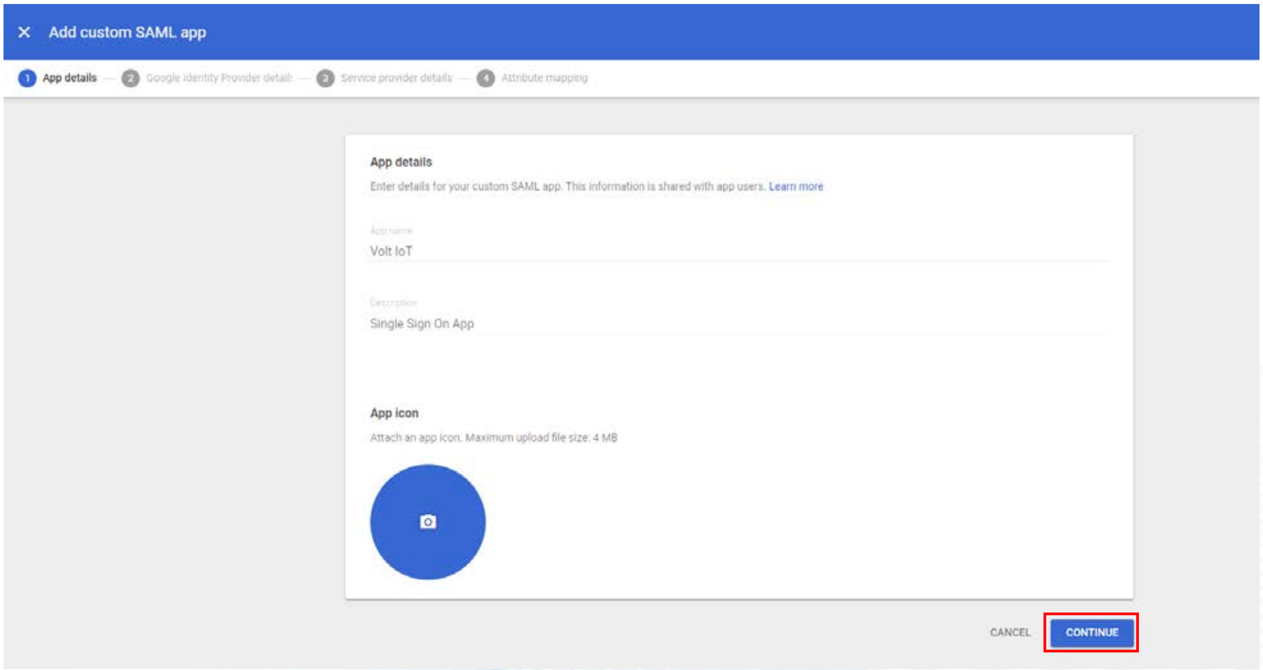
3. Go to **Add app** > **Add custom SAML app**.



No web or mobile apps found

Add and manage SAML apps under the Apps menu. Learn more

4. Fill the App detail, like App Name (e.g., Volt IoT) and click **Continue**.



App details

Enter details for your custom SAML app. This information is shared with app users. Learn more

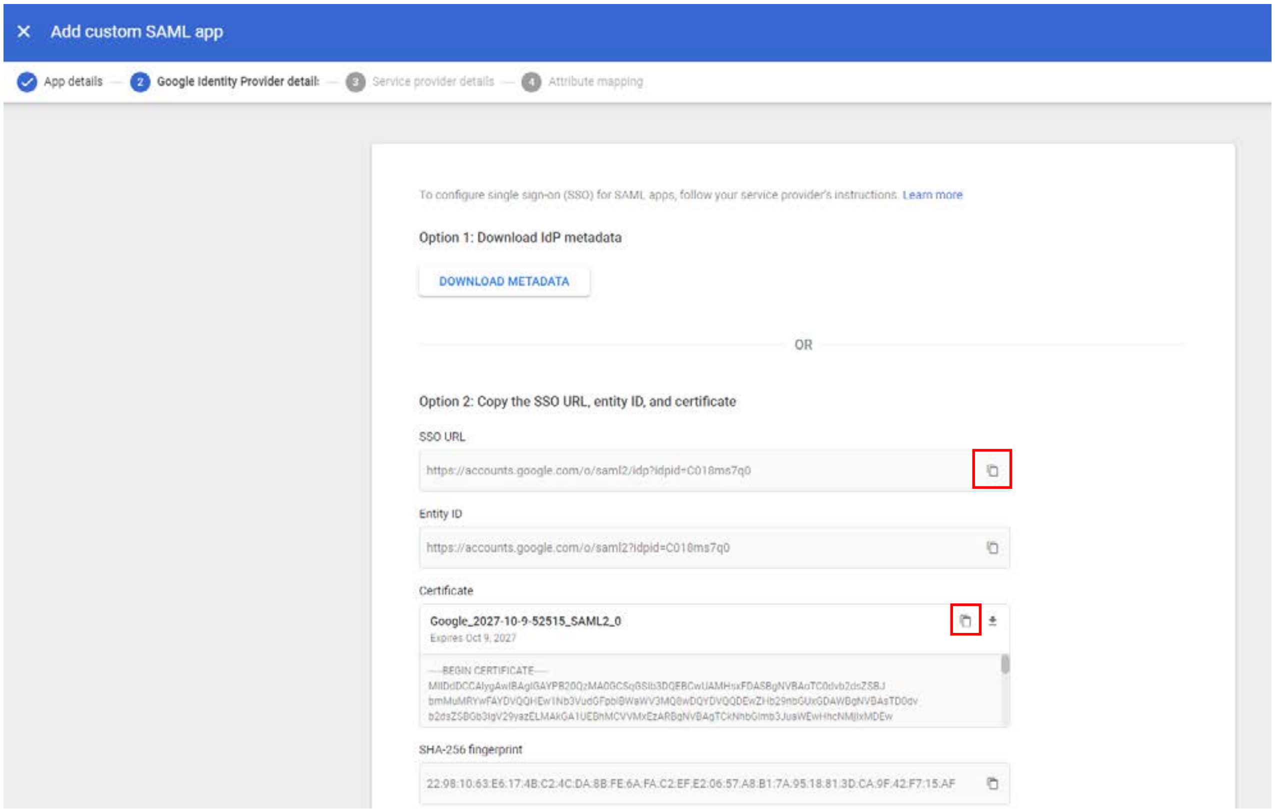
App name
Volt IoT

Description
Single Sign On App

App icon

Attach an app icon. Maximum upload file size: 4 MB

5. A screen will appear with the Google IdP information which is required to configure in Volt IoT.
   - Copy the **SSO URL**
   - Copy the **Certificate**



× Add custom SAML app
App details — 2 Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

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

Option 1: Download IdP metadata

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

SSO URL
https://accounts.google.com/o/saml2/idp?idpid=C018ms7q0

Entity ID
https://accounts.google.com/o/saml2?idpid=C018ms7q0

Certificate
Google_2027-10-9-52515_SAML2_0
Expires Oct 9, 2027

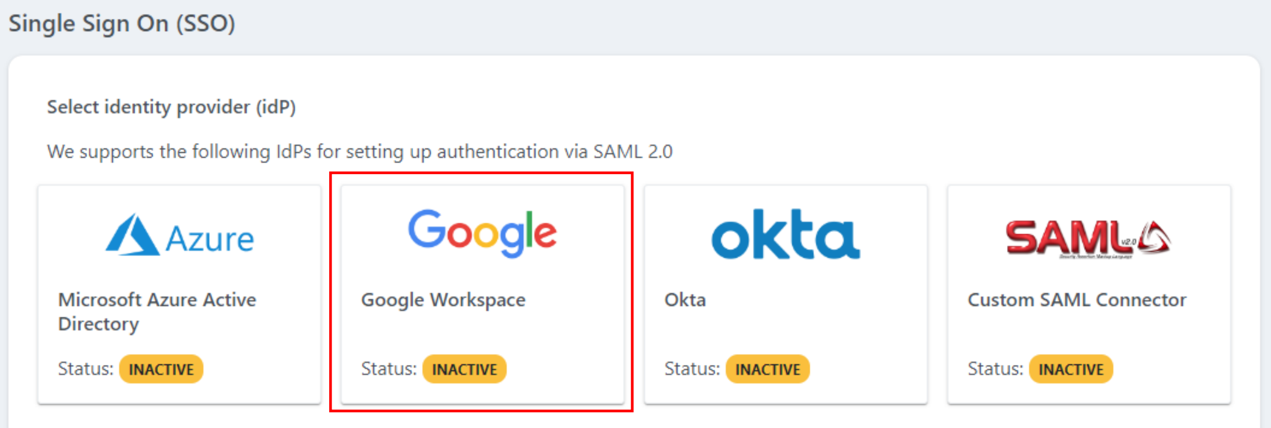
```
-----BEGIN CERTIFICATE-----
MIIDdDCCAlygAwIBAgIGAYPB20QzMA0GCSqGSIb3DQEBCwUAMHsxFDASBgNVBAoTC0dvb2dsZSBJ
bmMuMRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MQ8wDQYDVQQDEwZHb29nbGUxGDAWBgNVBAsTD0dv
b2dsZSBGb3IgV29yazELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEwHhcNMjIxMDEw
```

SHA-256 fingerprint
22:98:10:63:E6:17:4B:C2:4C:DA:8B:FE:6A:FA:C2:EF:E2:06:57:A8:B1:7A:95:18:81:3D:CA:9F:42:F7:15:AF

6. Login to your **Volt-IoT** super admin account access and select **Configuration** tab on the left-hand navigation bar.

7. Scroll down and go to the section of Single Sign-on (SSO) Configuration.

8. Select the Identity Provider **Google Workspace,** you will be directed to configuration settings which are required to setup **Volt-IoT** app on your IdP.



Single Sign On (SSO)

Select identity provider (idP)

We supports the following IdPs for setting up authentication via SAML 2.0

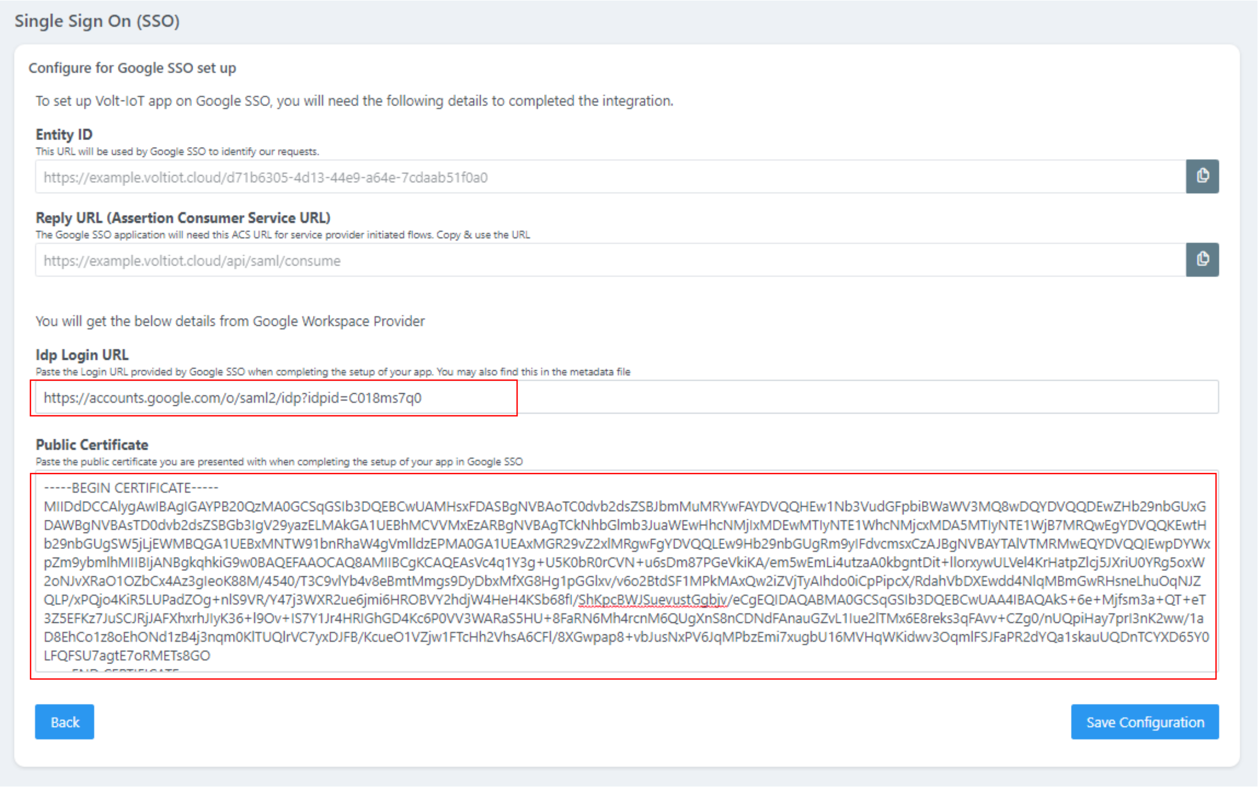
Microsoft Azure Active Directory
Status: INACTIVE

Google Workspace
Status: INACTIVE

Okta
Status: INACTIVE

Custom SAML Connector
Status: INACTIVE

9. Enter the following values.
    - **Login URL:** Paste SSO URL from the Google IdP configuration, which you copied in step 6
    - **Public Certificate:** Paste the certificate that you copied in step 6



Single Sign On (SSO)

Configure for Google SSO set up

To set up Volt-IoT app on Google SSO, you will need the following details to completed the integration.

Entity ID
This URL will be used by Google SSO to identify our requests.
https://example.voltiot.cloud/d71b6305-4d13-44e9-a64e-7cdaab51f0a0

Reply URL (Assertion Consumer Service URL)
The Google SSO application will need this ACS URL for service provider initiated flows. Copy & use the URL
https://example.voltiot.cloud/api/saml/consume

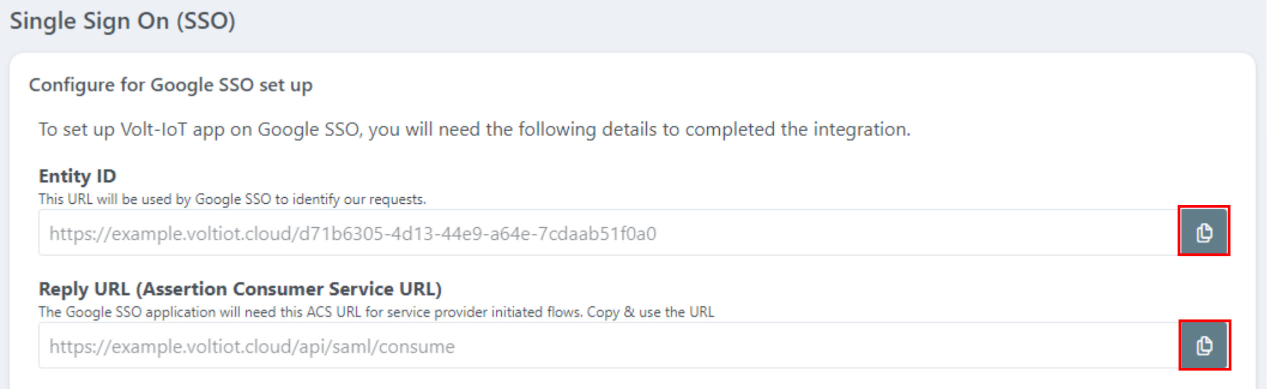
You will get the below details from Google Workspace Provider

Idp Login URL
Paste the Login URL provided by Google SSO when completing the setup of your app. You may also find this in the metadata file
https://accounts.google.com/o/saml2/idp?idpid=C018ms7q0

Public Certificate
Paste the public certificate you are presented with when completing the setup of your app in Google SSO

```
-----BEGIN CERTIFICATE-----
MIIDdDCCAlygAwIBAgIGAYPB20QzMA0GCSqGSIb3DQEBCwUAMHsxFDASBgNVBAoTC0dvb2dsZSBJbmMuMRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MQ8wDQYDVQQDEwZHb29nbGUxG
DAWBgNVBAsTD0dvb2dsZSBGb3IgV29yazELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEwHhcNMjIxMDEwMTIyNTE1WhcNMjcxMDA5MTIyNTE1WjB7MRQwEgYDVQQKEwtH
b29nbGUgSW5jLjEWMBQGA1UEBxMNTW91bnRhaW4gVmlldzEPMA0GA1UEAxMGR29vZ2xlMRgwFgYDVQQLEw9Hb29nbGUgRm9yIFdvcmsxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWx
pZm9ybmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsVc4q1Y3g+U5K0bR0rCVN+u6sDm87PGeVkiKA/em5wEmLi4utzaA0kbgntDit+llorxywULVel4KrHatpZlcj5JXriU0YRg5oxW
2oNJvXRaO1OZbCx4Az3gIeoK88M/4540/T3C9vlYb4v8eBmtMmgs9DyDbxMfXG8Hg1pGGlxv/v6o2BtdSF1MPkMAxQw2iZVjTyAIhdo0iCpPipcX/RdahVbDXEwdd4NlqMBmGwRHsneLhuOqNJZ
QLP/xPQjo4KiR5LUPadZOg+nlS9VR/Y47j3WXR2ue6jmi6HROBVY2hdjW4HeH4KSb68fl/ShKpcBWJSuevustGgbjv/eCgEQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAkS+6e+Mjfsm3a+QT+eT
3Z5EFKz7JuSCJRjJAFXhxrhJIyK36+l9Ov+IS7Y1Jr4HRIGhGD4Kc6P0VV3WARaS5HU+8FaRN6Mh4rcnM6QUgXnS8nCDNdFAnauGZvL1Iue2lTMx6E8reks3qFAvv+CZg0/nUQpiHay7prI3nK2ww/1a
D8EhCo1z8oEhONd1zB4j3nqm0KlTUQlrVC7yxDJFB/KcueO1VZjw1FTcHh2VhsA6CFl/8XGwpap8+vbJusNxPV6JqMPbzEmi7xugbU16MVHqWKidwv3OqmlFSJFaPR2dYQa1skauUQDnTCYXD65Y0
LFQFSU7agtE7oRMETs8GO
-----END CERTIFICATE-----
```

10. Copy the **Entity ID** and **Reply URL** (ACS URL) from configuration page.



Single Sign On (SSO)

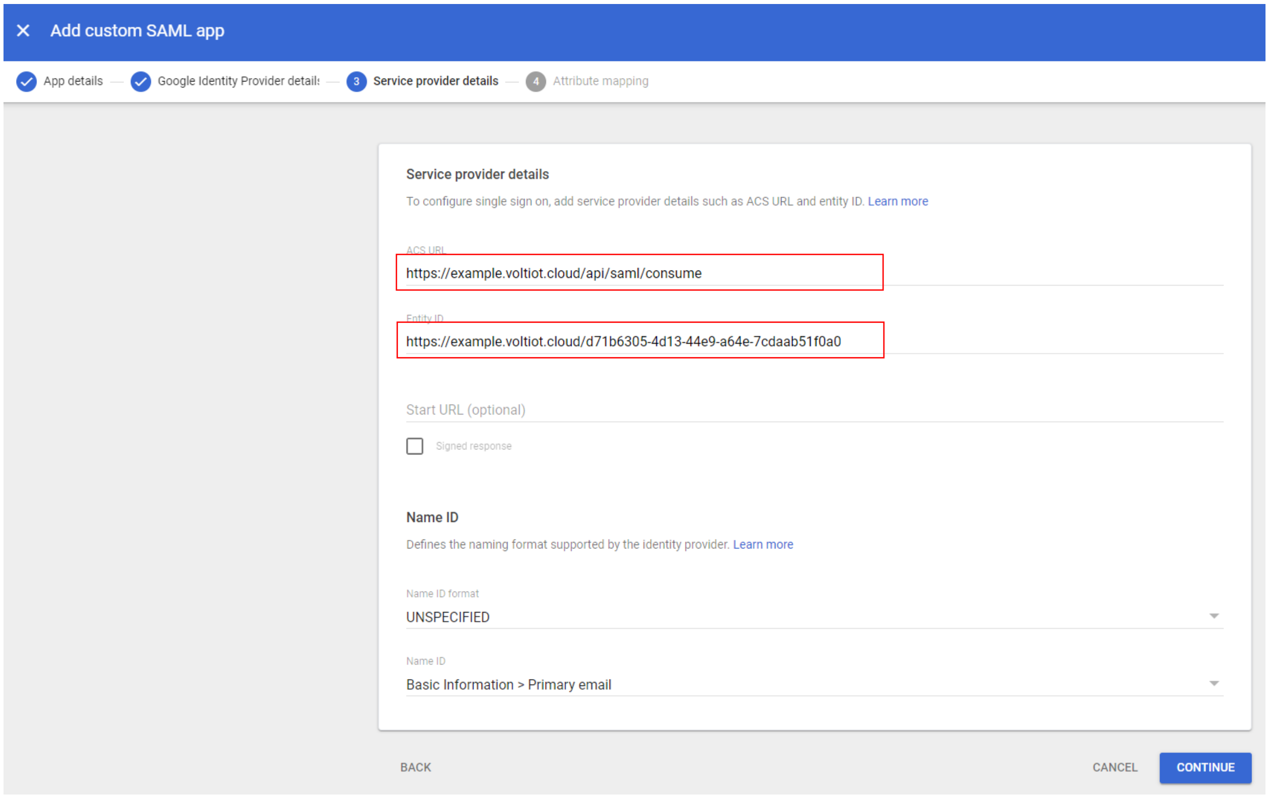
Configure for Google SSO set up

To set up Volt-IoT app on Google SSO, you will need the following details to completed the integration.

Entity ID
This URL will be used by Google SSO to identify our requests.
https://example.voltiot.cloud/d71b6305-4d13-44e9-a64e-7cdaab51f0a0

Reply URL (Assertion Consumer Service URL)
The Google SSO application will need this ACS URL for service provider initiated flows. Copy & use the URL
https://example.voltiot.cloud/api/saml/consume

11. Navigate back to **Google Workspace** Custom SAML app configuration and paste the **Entity ID** and **ACS URL** which you copied in step 10.



Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. Learn more

ACS URL
https://example.voltiot.cloud/api/saml/consume

Entity ID
https://example.voltiot.cloud/d71b6305-4d13-44e9-a64e-7cdaab51f0a0

Start URL (optional)

□ Signed response

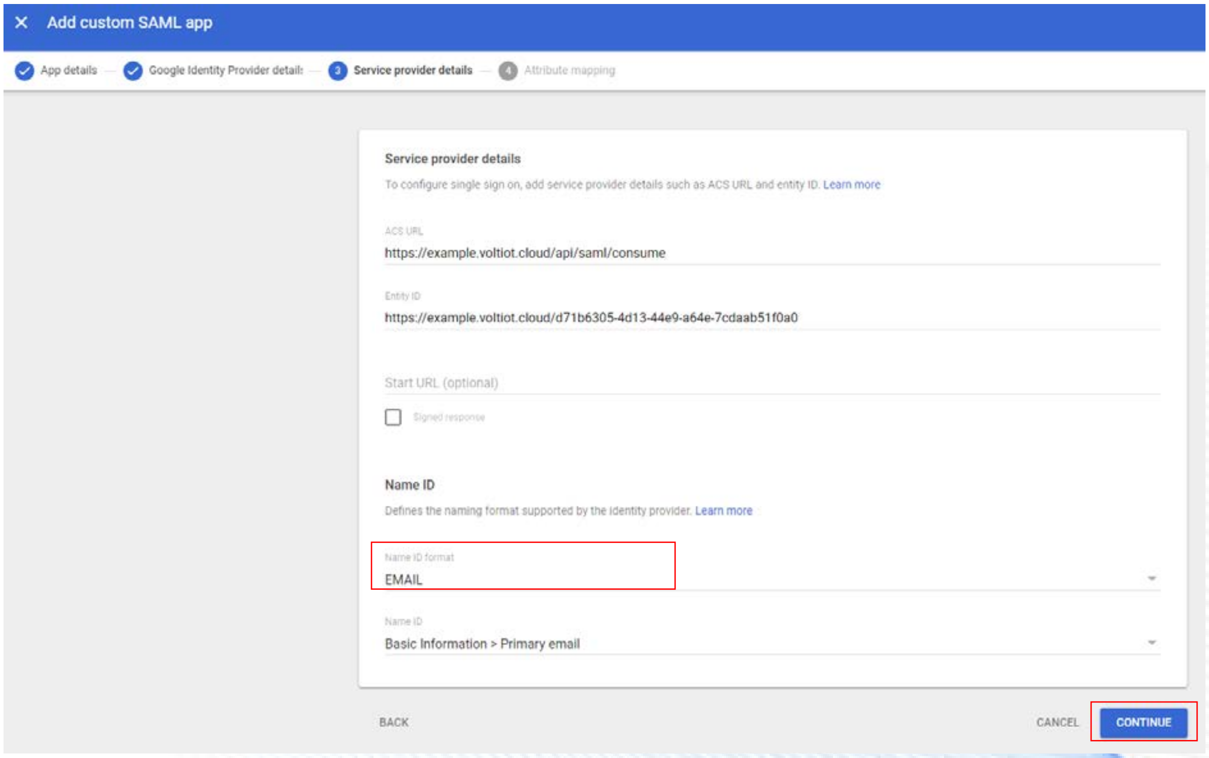
Name ID

Defines the naming format supported by the identity provider. Learn more

Name ID format
UNSPECIFIED

Name ID
Basic Information > Primary email

12. Select **Name ID format** is **Email** and keep **Name ID Basic Information > Primary Email** and click **Continue.**



Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. Learn more

ACS URL
https://example.voltiot.cloud/api/saml/consume

Entity ID
https://example.voltiot.cloud/d71b6305-4d13-44e9-a64e-7cdaab51f0a0

Start URL (optional)

□ Signed response

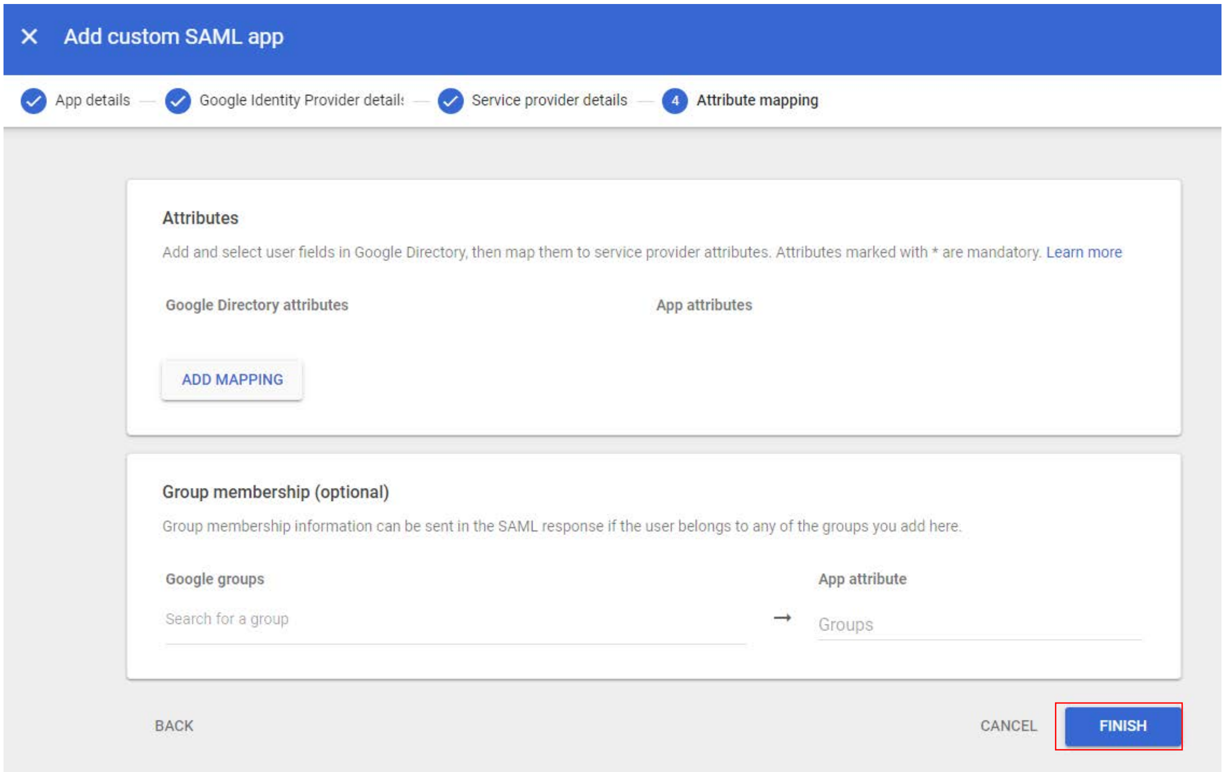
Name ID

Defines the naming format supported by the identity provider. Learn more

Name ID format
EMAIL

Name ID
Basic Information > Primary email

13. The SAML application for **Volt IoT** has been configured. Click **Finish** to continue



Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. Learn more

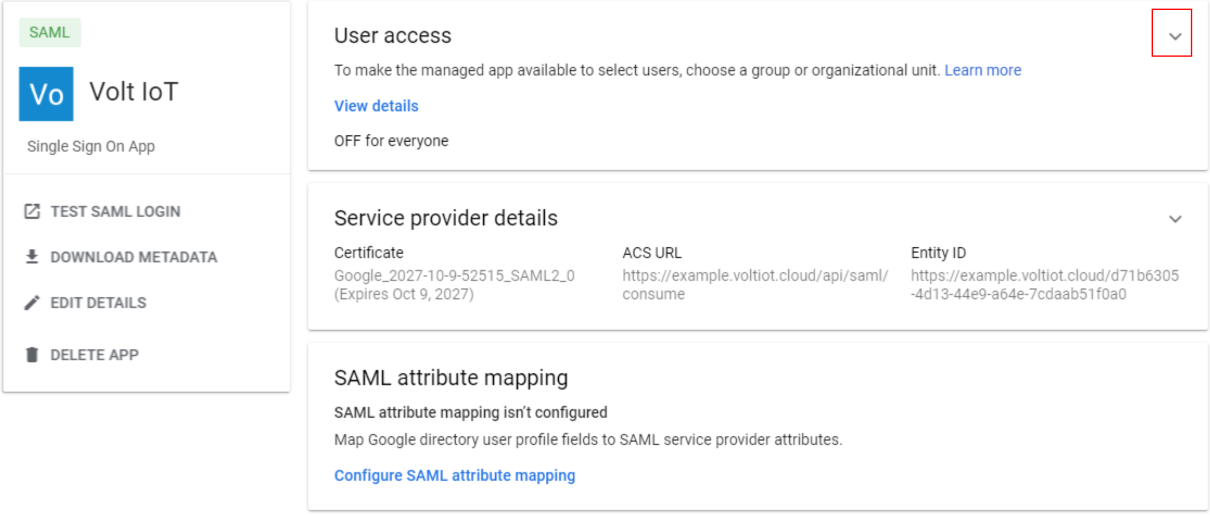
Google Directory attributes	App attributes

Group membership (optional)

Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

Google groups		App attribute
Search for a group	→	Groups

14. Expand the **User Access** pane.



User access

To make the managed app available to select users, choose a group or organizational unit. Learn more

View details

OFF for everyone

Service provider details

Certificate	ACS URL	Entity ID
Google_2027-10-9-52515_SAML2_0 (Expires Oct 9, 2027)	https://example.voltiot.cloud/api/saml/consume	https://example.voltiot.cloud/d71b6305-4d13-44e9-a64e-7cdaab51f0a0

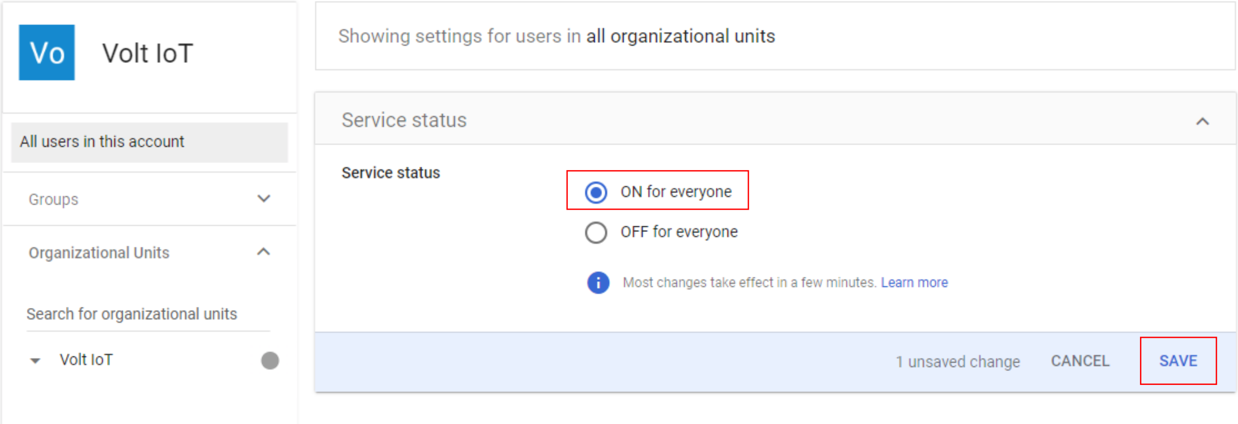
SAML attribute mapping

SAML attribute mapping isn't configured

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

Configure SAML attribute mapping

15. Select **On for everyone** and click **Save.**



Vo Volt IoT

All users in this account

Groups

Organizational Units

Search for organizational units

Volt IoT

Showing settings for users in all organizational units

Service status

Service status

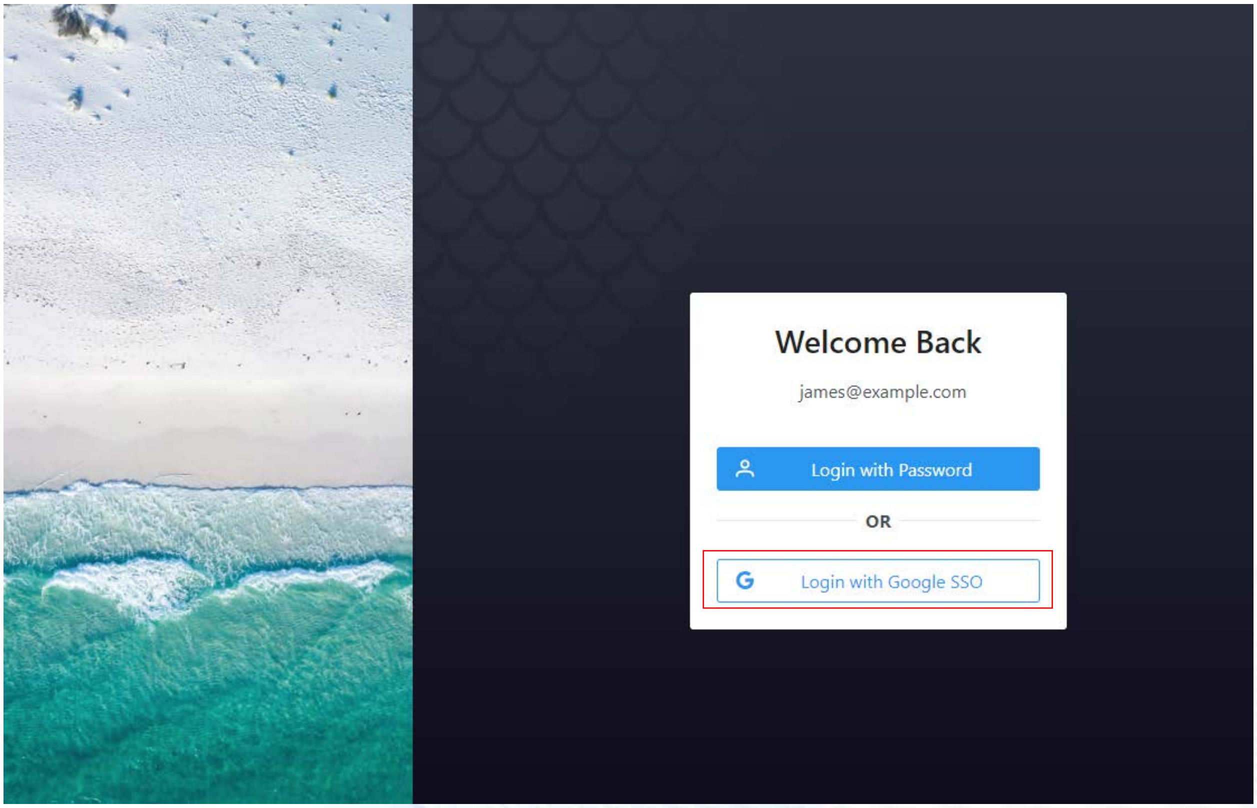
● ON for everyone

○ OFF for everyone

Most changes take effect in a few minutes. Learn more

1 unsaved change CANCEL SAVE

16. The configuration is finished. It can now be tested. Go to your **Volt IoT** application and log in with the **Google SSO**. The login will be routed to Google



Welcome Back

james@example.com

Login with Password

OR

Login with Google SSO

17. Once authenticated through Google, the user will be logged into Volt IoT with their Google account.