
# AppGate SDP and Google ID SAML Single Sign-On Integration Guide

V2.0
Tested for use versions:
AppGate SDP v4.3 or newer
Last updated: March 2020

**TABLE OF CONTENTS**

# INTRODUCTION

AppGate SDP supports single sign-on authentication using SAML 2.0 identity providers (IdP) such as ADFS, OKTA, OneLogin and Ping. SAML can be used to authenticate users connecting through the Client, and also to authenticate administrators signing-in to the Controller's admin UI.
This Integration Guide is part of a suite of documents to help configure your AppGate SDP system to work with your third party systems; for information about other guides refer to the AppGate support pages.

## Using SAML authentication

AppGate SDP handles SAML response verification in different ways depending on use case - Administrators authenticating through the admin UI, or Users authenticating through the Client. The Assertion Consumer Service (ACS) that is used to verify the SAML response in single sign-on (SAML SSO) will be different for each use case. Therefore, to use Google SSO authentication you will need to follow these steps:

1. Decide on your use case: Administrator and /or User authentication;
2. On your Google admin console: create separate SAML apps – one for each use case (Administrator Authentication and User Authentication);
3. In your AppGate SDP: create and configure a corresponding Google IdP entity for each use case;
4. When configuring the two systems, use the appropriate Assertion Consumer Service (ACS) URL – refer to Table 1 below.

**Table 1: Assertion Consumer Service (ACS) Reply URL:**

| Administrator Authentication: | User Authentication: |
|---|---|
| In this use case, the Controller will be the Assertion Consumer Service (ACS).<br>To configure your IdP, you will need the Controller URL (using HTTPS) eg. `https://mycontroller.mycompany.com/admin/saml` | If your IdP requires secure TLS connection, then you will need to use a redirection server to act as the ACS. The redirection server needs a web server listener running on HTTPS to perform a redirect 307 for the SAML response to the Client.<br>In this situation, the ACS Reply URL will be the redirection server, eg. `https://redirectserver.mycompany.com/saml`<br>The redirect to will be to `http://127.0.0.1:29001/saml`<br>More information about the requirements for SAML response verification can be found at:<br>https://sdphelp.appgate.com/adminguide/saml-idp.html<br><br>If your IdP supports HTTP binding the AppGate SDP Client itself can be the ACS. In this case, the ACS Reply URL should be set to localhost, for example:<br>`http://127.0.0.1:29001/saml` |

## About this integration guide

This document provides a step-by-step guide to integrate Google SAML Single Sign-On and AppGate SDP.
The configuration process is similar for both use cases - Administrator Authentication to the admin UI and User Authentication through the Client. If you need to use your IdP for both of these use cases, you will need to repeat the process, ensuring that you have the appropriate test topology in place before you start, and that you enter the appropriate data in each case. The specific details of the data that needs to be entered in each case are provided in the tables as you go through the process.

# BEFORE YOU START

## Test topology

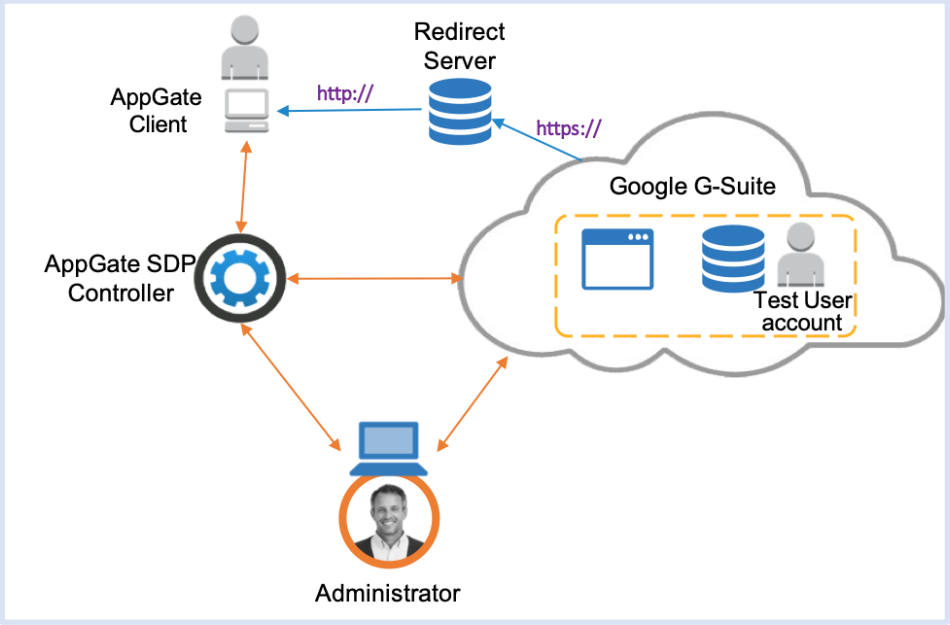



*Figure 1: Google IdP integration test topology*

To complete this integration, you must have:

- A Google G-Suite account with administrator permission to add new apps
- An AppGate SDP Controller installed and accessible on your network. Information for setting up your Controller can be found in the Admin UI: https://sdphelp.appgate.com/adminguide/index.html
- A test user account on your Google database. The user account must include first name, last name, email address and password. For details about creating a user account refer to Google Support: Add a user

# STEP BY STEP GUIDE TO INTEGRATION

You will need to complete this configuration process for each intended use case: Administrator Authentication to the admin UI and User Authentication through the Client.

## 1. GOOGLE CONFIGURATION: SETTING UP SINGLE SIGN-ON

**Create a new application**

- Log in to your Google account Admin console. Select SAML Apps>Add a service/App to your domain
- Click <+> ('Enable SSO for SAML Application') at the bottom of the page to add a new SAML IDP
- In the pop-up window select <SETUP MY OWN CUSTOM APP> at the bottom

**On the Google IdP information screen:**

- Either - Download the IDP metadata
- Or - Download the Certificate and note the information in the following fields:
  - *SSO URL*
  - *Entity ID*
- click <NEXT>


**On the Basic Information for your custom app screen:**

- *Application Name* – type in an application name eg "AppGate SDP" and add a description
- Click <NEXT>

**On the Service Provider Details screen:**

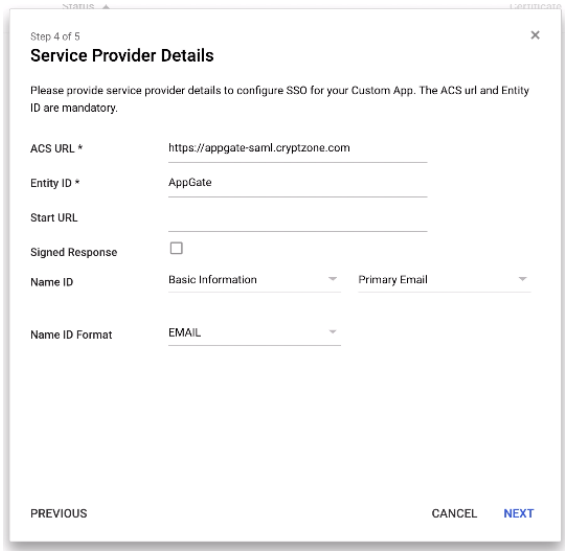
- *ACS URL* – type in the appropriate ACS URL depending on your use case – see the table below:

| Administrator Authentication: | User Authentication: |
|---|---|
| ACS URL = AppGate SDP Controller URL<br>`https://mycontroller.mycompany.com/admin/saml` | ACS URL = redirection server URL<br>`https://redirectserver.mycompany.com/saml` |

- *Entity ID* – This needs to be the same as the *Audience* field in the IdP form on your AppGate SDP console eg: "AppGate"
- *Name ID* – specify email to be used for the user name: select **Basic Information** <Primary Email>
- *Name ID Format* – select **EMAIL**

The completed form should look like this:

- Click <**NEXT**>



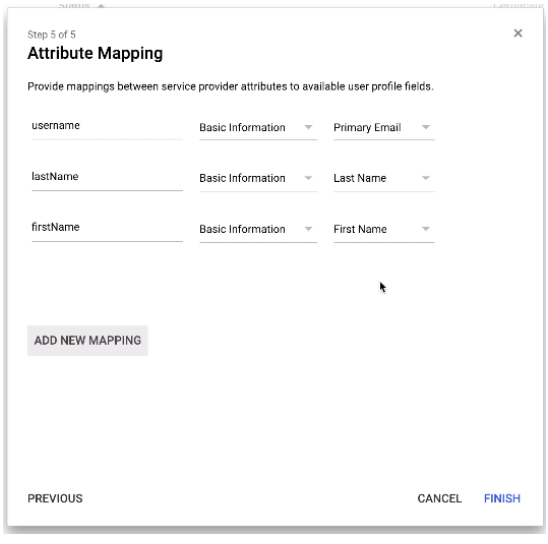

## Attribute Mapping

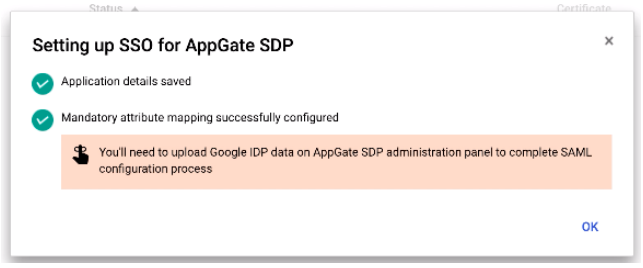
In the <**Attribute Mapping**> window specify the user attributes that need to be mapped to client token fields. Click <**ADD NEW MAPPING>** to add each new attribute mapping
AppGate SDP requires a minimum of three fields: *username*, *lastName, firstName*.

- Complete each new attribute field as follows (enter the field names precisely):
  - *Field name: "*username" - <Basic Information> <Primary Email>
  - *Field name:* "lastName" - <Basic Information> <Last Name>
  - *Field name:* "firstName" - <Basic Information> <First Name>

The completed form should look like this:

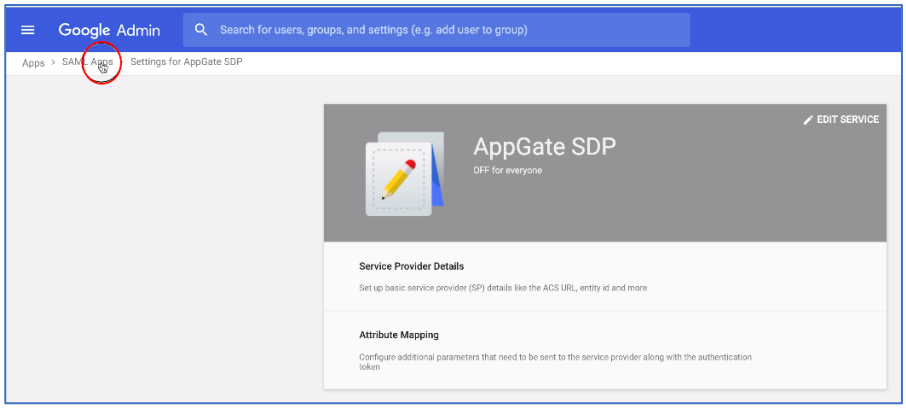
- Click <**FINISH**>
- Click <**OK**> to complete the application mapping and save the app details



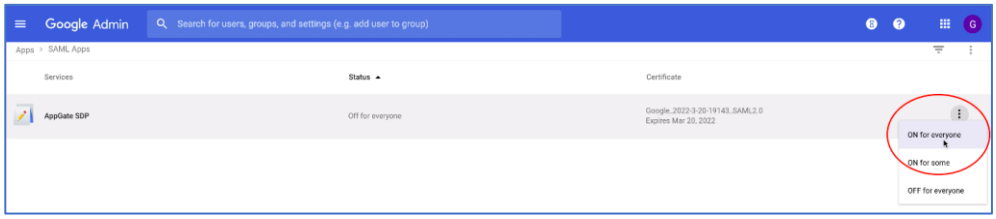
**Enable the application for users:**

Return to the <**SAML apps**> console (click on <**SAML Apps**> in the navigation at the top of the screen).

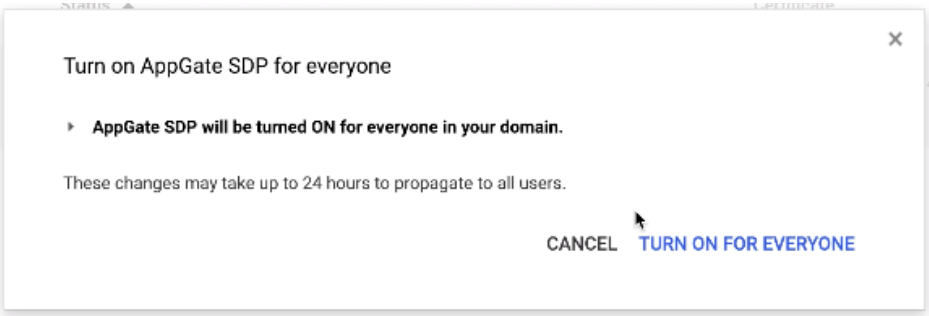



Your new SAML app named “AppGate SDP” should be listed on the console.

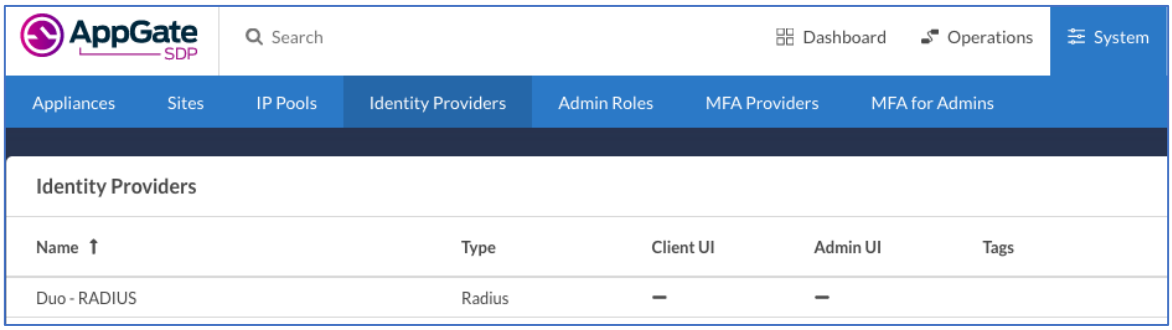
- Click the option button on the right-hand side and select <**ON for everyone**>




- Click <**TURN ON FOR EVERYONE**> on the confirmation window



## 2. APPGATE SDP CONFIGURATION: ADD A NEW IDENTITY PROVIDER




**In your AppGate SDP console:**

- select **System > Identity Providers**
- create a new Identity Provider
- choose the type SAML
- start configuring your identity provider following the details in the tables below.

| | **Administrator Authentication:** | **User Authentication:** |
|---|---|---|
| *Name* | Enter a unique name eg: "Google SAML Admin" | Enter a unique name eg: "Google SAML User" |
| *IPv4Pool* | select **default pool v4** | select **default pool v4** |
| *Where to use* | tick "Admin UI" | (will become available for a Profile link) |
| *Single Sign-on URL* | *See below* | |
| *Issuer* | *See below* | |
| *Audience* | type in the **Entity ID** you entered on the Google Service Provider Details screen | |
| *Public Certificate* | *See below* | |

**If you are running AppGate SDP v4.3 or later:**

- Use XML Metadata file to autocomplete *Single Sign-On, Issuer* and *Public Certificate* fields
- Click <**Choose a file**> and select the downloaded metadata file, which will autocomplete the relevant fields

**If you are running AppGate SDP v4.2 or earlier:**

- You will need to manually complete the following fields (from your Google IdP Information screen):
  - *Single Sign-On URL:* copy & paste the Single Sign-On (SSO) URL
  - *Public Certificate:* upload the certificate you have already downloaded
  - *Issuer:* copy and paste the Entity ID URL.
- If you need more information about how to manually complete the IdP configuration, please contact the Help Center

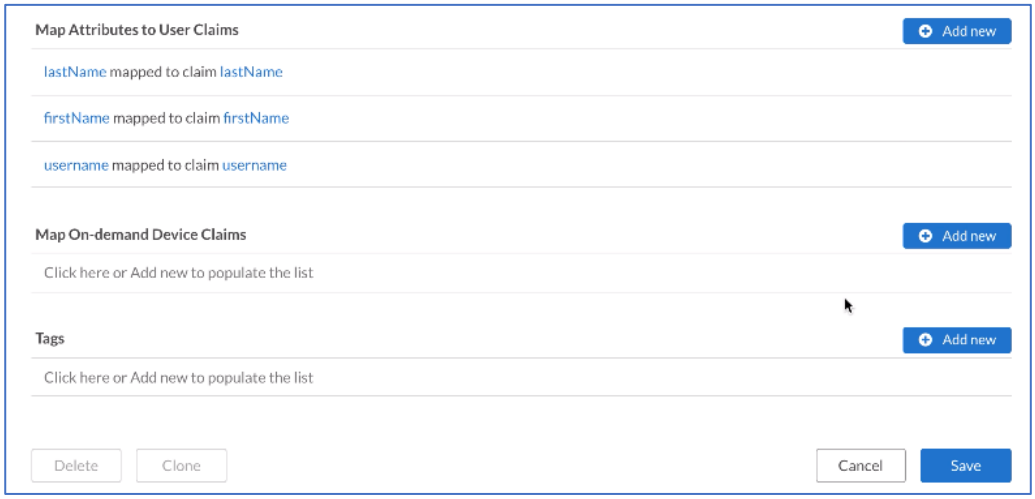
- Click **<SAVE>** to save your configuration

## 3. MAPPING ATTRIBUTES

In your AppGate SDP console, finish configuring the identity provider form by mapping attributes.
In the <**Map Attributes to User Claims**> field:

- click <+ **ADD NEW>** to add each attribute mapping
- Complete each new attribute field as follows (enter the field names precisely):
- *attribute: "*username" – *claim name "*username"
- *attribute:* "lastName" – *claim name "*lastName"
- *attribute:* "firstName" – *claim name "*firstName"

The completed form should look like this:




## 4. TESTING INTEGRATION

After completing the Identity Provider form on the AppGate SDP console, save the configuration form.
To test that integration has been completed successfully you need to sign in as the Test User either through the Client or through the AppGate SDP Controller admin UI, as follows:

| **Administrator Authentication:** | **User Authentication:** |
|---|---|
| **On your AppGate SDP admin UI:**<br>• Sign out of the admin UI<br>• Log in using the following information: *Identity Provider* – choose this new IdP from the drop down list<br>• Click <Sign in with browser> to connect to your authenticator<br>• You may see the following message: *"You don't have any administration rights"* – this confirms that the test user credentials have been successfully authenticated by your Identity Provider. | **On the AppGate SDP Client:**<br>• Quit if you are already connected<br>• Get a new profile link from the Controller that includes this new IdP.<br>• Add a new profile in the Client<br>• Click <Sign in with provider><br>• Sign in using the browser to connect.<br>• You should see the Client sign-in. |

# TROUBLESHOOTING

Common errors to check for when integrating a SAML IdP are missing fields or a mismatch in the names between the SAML app and AppGate SDP configuration, for example:

1. **Audience doesn't match:** the *Entity ID* field on the Google SAML app configuration does not match the *Audience* field on the AppGate SDP configuration form.
2. **Missing Attributes:** the three attribute names entered on the SAML app do not match the attribute names on the AppGate SDP configuration - *username*, *lastName, firstName*

Use the *controllerd* log to find the source of the error.

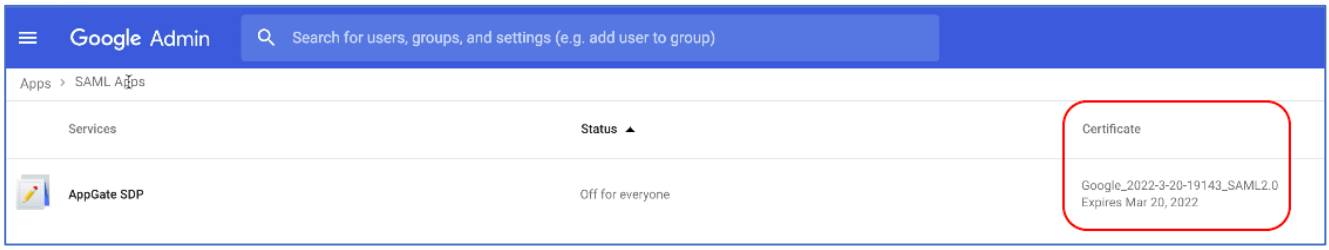
- Launch the terminal window and enter the command: *journalctl -u cz-controllerd -f*
- Try to login to the Controller Admin UI using your SAML IdP and watch the *controllerd* log
- You may see something like this:
  *Dec 20 12:59:31 Ctrl.example.co cz-controllerd[1320]: WARN [SamlConnector] Audience is either empty or doesn't match this provider. Value: AppGate*

# MAINTENANCE

Some changes to your IdP provider or your AppGate SDP configuration may require updating and retesting system integration:

**X.509 certificate rotation:**
X.509 certificates have a five-year lifetime. When the X.509 certificate associated with an application expires, your users won't be able to log in to their AppGate SDP client using Google ID.

On your Google Admin>SAML apps console, you can see when the certificate for your AppGate SDP app is about to expire:




You will need to create a new X.509 certificate before your active SAML certificate is due to expire. Assign this new certificate to your SAML app and update the Google IdP configuration on your AppGate SDP Controller.

1. **Create a new certificate (certificate rotation):**
   You will need to delete and then replace any expiring or compromised certificate for your "AppGate SDP" SAML app. Follow the instructions from your IdP provider: Google Support: Maintain SAML certificates
   Note that while the old certificate is being deleted and updated, the SAML app will not be available for users to log in to the AppGate SDP Client
- When a new certificate has been assigned to your SAML app, open the Google IDP Information window and download a copy of the new certificate

2. **Update your AppGate SDP configuration:**
- On your AppGate SDP admin UI, open the **System>Identity Provider** configuration form for Google IdP. In the *Public Certificate* field, click the <**Choose a File**> button and upload the Certificate that you downloaded and Save the changes.

3. Test the system integration: repeat the "Testing Integration" steps above.

# HELP AND SUPPORT

For more information about the next steps in setting up your AppGate SDP system , refer to the Admin Guide
Please visit the Help Center to browse the knowledge base or log a support ticket for all Cyxtera products. Learn more about the Help Center below.

**Self-service help**
Self-service help can be browsed or searched for technical solutions. Browse FAQs, known issues, best practices, service examples, guides and manuals.
**Customer support requests**
Customers can submit support requests in accordance with their Support and Maintenance contracts. We recommend that you sign in to the support portal and submit from your own support account. If you do not have access, please fill in the “request a login” form available on the Help Centre.

# FEEDBACK

If there is any information in this Integration Guide that needs to be updated, or instructions that need further clarification, please let us know. Contact send your feedback to Send your feedback to the Help Center.