AppGate SDP and AD FS SAML Single Sign-On Integration Guide

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

AppGate SDP – AD FS: Integration Guide

TABLE OF CONTENTS

INTRODUCTION

AppGate SDP supports single sign-on authentication using SAML 2.0 identity providers (IdP) such as PingOne, Okta, OneLogin and AD FS. SAML can be used to authenticate users connecting through the Client, and also to authenticate administrators logging into the Controller console.

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 Controller 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 AD FS SSO authentication you will need to follow these steps:

1. Decide on your use case: Administrator and /or User authentication;
2. On your AD FS console: create separate ***Relying Party Configurations*** – one for each use case (Administrator Authentication and / or User Authentication);
3. In your AppGate SDP: create and configure a corresponding AD FS 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. Note ACS URL is called “Service URL” in the AD FS configuration.

Table 1: Assertion Consumer Service (ACS) URL:

Administrator Authentication:	**User Authentication:**
In this use case, the Controller will be the Assertion Consumer Service (ACS). 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. In this situation, the ACS Reply URL will be the redirection server, eg. `https://redirectserver.mycompany.com/saml` The redirect to will be to `http://127.0.0.1:29001/saml` More information about the requirements for SAML response verification can be found at: https://sdphelp.appgate.com/adminguide/saml-idp.html 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: `http://127.0.0.1:29001/saml`

About this integration guide

This document provides a step-by-step guide to integrate AD FS SAML Single Sign-On and AppGate SDP.

The configuration process is the same for both use cases - Administrator Authentication through the Controller 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

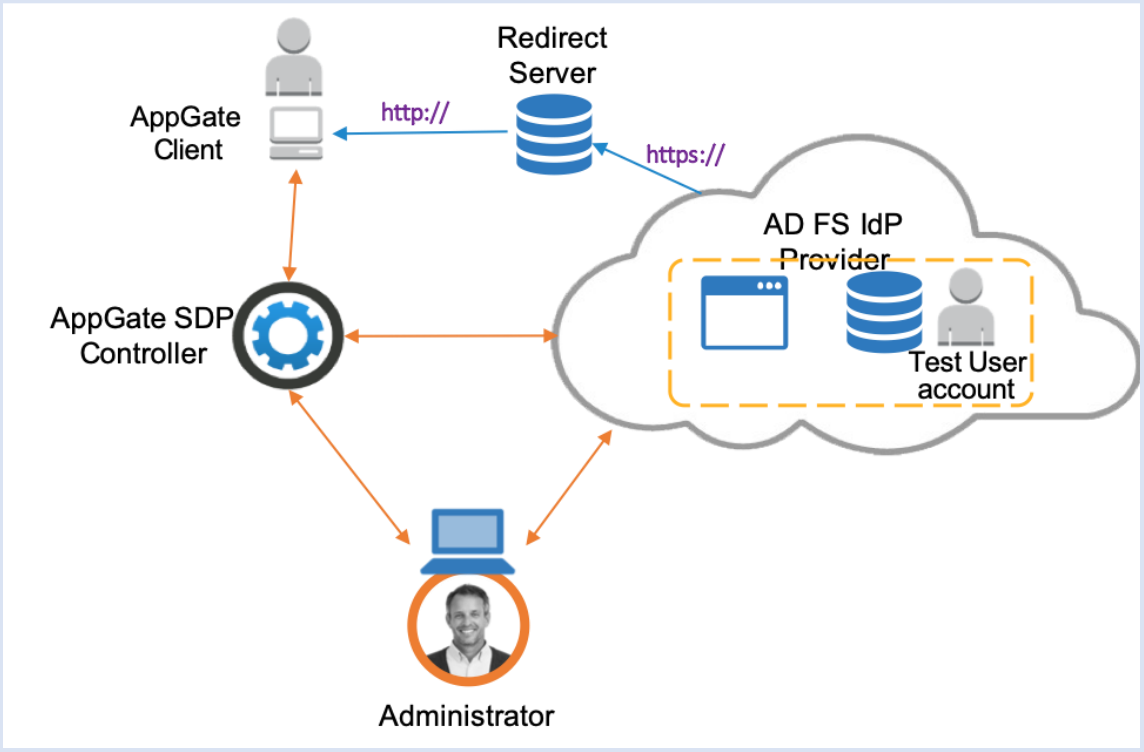


Figure 1: AD FS integration test topology

This integration process requires the following:

- AD FS IdP service account admin credentials
- AppGate SDP Controller installed and accessible. Information for setting up your Controller can be found in the Admin UI: https://sdphelp.appgate.com/adminguide/index.html
- A test user account in your AD FS directory, with at least one basic attribute field configured such as:
    - *username* eg. “testuser”
    - *firstName eg.* “Joe”
    - *lastName* eg. “Smith”

STEP BY STEP GUIDE TO INTEGRATION

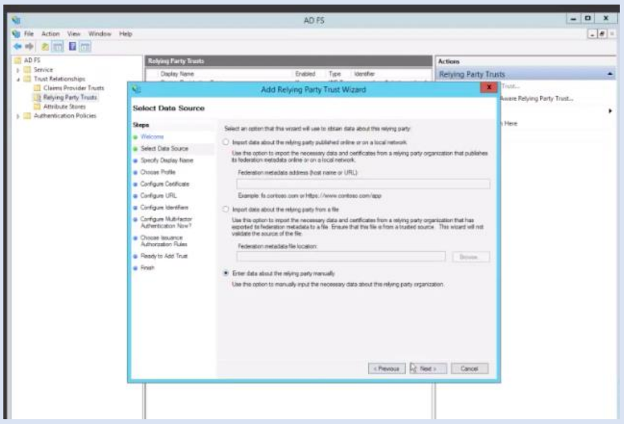
You will need to complete this configuration process for each intended use case: Administrator Authentication through the Controller and User Authentication through the Client.

1. AD FS CONFIGURATION: SET UP SINGLE SIGN-ON

Add a new Relying Party

- Log in to your AD FS administrator account and open the AD FS management console.
- Go to Relying Party Trusts, which opens the wizard for Add Relying Party Trust.
- Click <Start>

- Click <Enter data about the relying party manually>
- Click <Next>



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

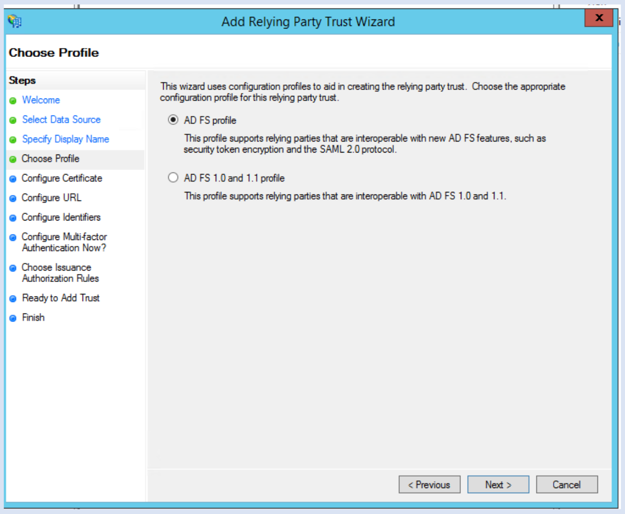
● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

- Type in a Display Name for your Relying party, eg:
  - For Administrator Authentication: “AppGate SDP”
  - For User Authentication: “AppGate SDP Client”
- Click <Next>

- Choose the option <AD FS profile> - this support SAML 2.0 protocol
- Click <Next>

- On the next screen do not set an encryption token.
- Click <Next>



Choose Profile

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

● AD FS profile

This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

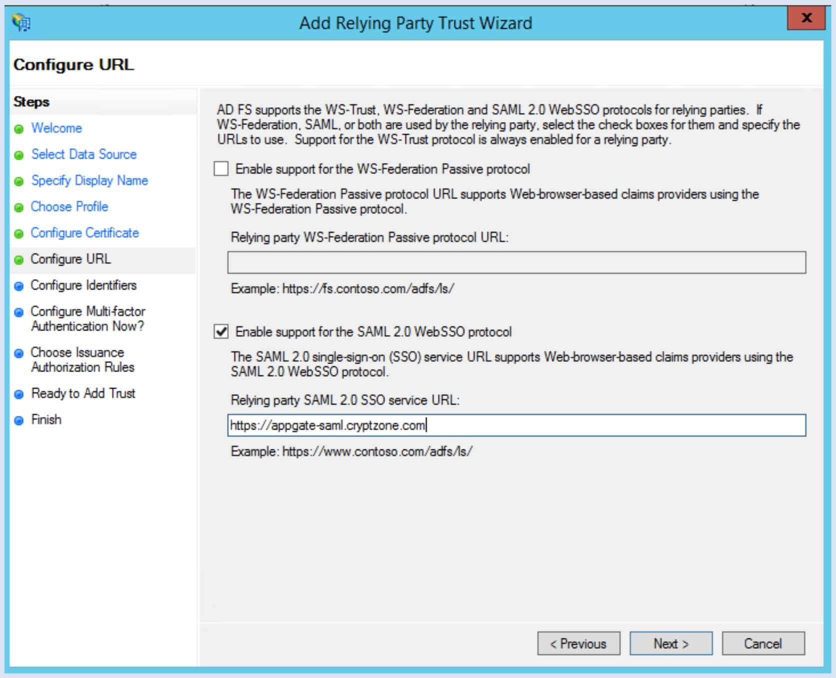
This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

On the next screen you need to define the Assertion Consumer Service (ACS) URL which is referred to as *Relying Party service URL*:

- Choose the option <Enable support for the SAML 2.0 Web SSO protocol>
- Complete the field as follows:
  - *Relying Party SAML 2.0 SSO service URL:*- type in the appropriate ACS URL depending on your use case – see the table below:

Administrator Authentication:	**User Authentication:**
Relying Party Service URL = AppGate SDP Controller URL `https://mycontroller.mycompany.com/admin/saml`	Relying Party Service URL = redirection server URL `https://redirectserver.mycompany.com/saml`

- Your configuration form should look something like this. (Note that the URL for the Relying Party Service is an example redirection server URL only.)



AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

https://appgate-saml.cryptzone.com

Example: https://www.contoso.com/adfs/ls/

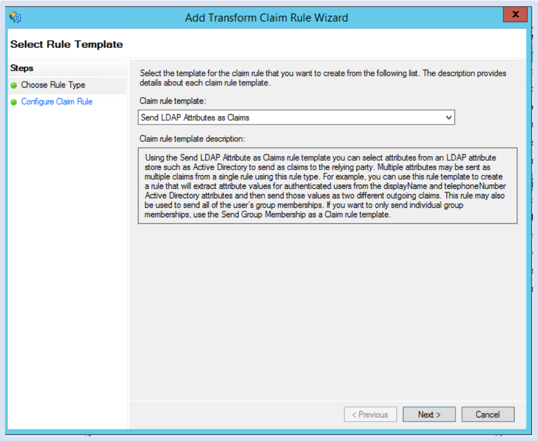
- Click <Next>

- On the next screen, complete the following field:
    - *Relying Party Trust Identifier:-* Type in a unique name eg. *AppGate SDP*, make a note of this as it needs to match the *Audience* field when you configure AppGate SDP
- Click <Add>
- Click <Next>

- On the next screen choose the option not to configure multi-factor authentication. This can be configured if required after successful completion of the system Integration process.
- Click <Next>

- On the next screen choose the option to <Permit all users to access this relying party>.
- Click Next.

- The next screen provides an overview of the configuration
- Click Next and Close. This should exit the wizard.



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Attribute Mapping

- On your AD FS console you should see your new Relying Party listed.
- Right-click on the relying party and select <Edit Claim Rules>.
- In the <Issuance transform rules> tab, click <Add Rule>.
- Select *Claim Rule Template* type - <Send LDAP attributes as claims>
- Click <Next>

- Configure the claim rule as follows:
  - *Claim Rule Name* – type in a name eg. AppGate SDP Claims
  - *Attribute Store* – choose Active Directory
  - *Mapping of LDAP attributes:* specify which SAML attributes should be mapped to in the ID token.
    The left-hand column is the *LDAP attribute name*
    The righthand column *Outgoing Claim Type* is the Attribute Name that will be received in the SAML response.

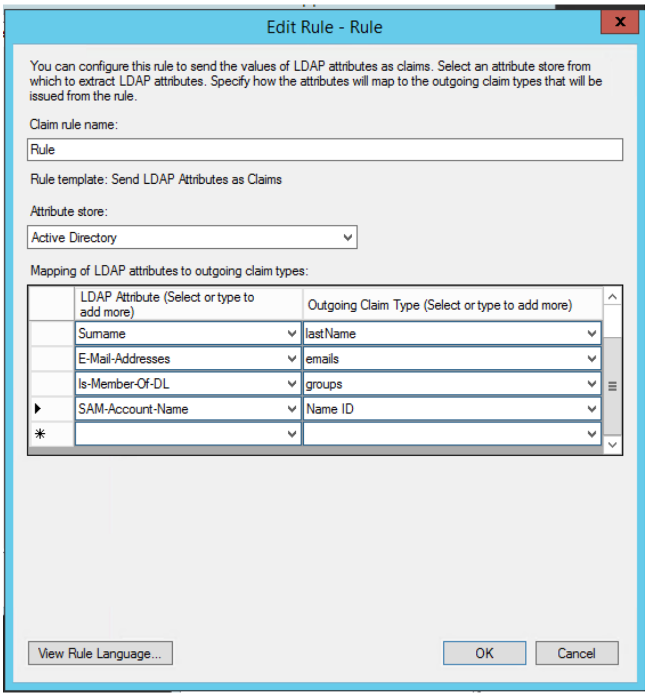
    Start with the following mapping which is required to format the SAML assertion:
    "SAM-Account-Name" -> "Name ID"

- Then create additional mappings to return claims in the ID token. Use the attributes configured for your test user

  Eg:
  "SAM-Account-Name" -> "username"
  "Given-Name" -> "firstName"
  "Surname" -> "lastName"
  "E-Mail-Addresses" -> "emails"
  "Is-Member-Of-DL" -> "groups"

- Click <**Finish>,** and then click <OK>

Your attribute rule should look something like this:



Edit Rule - Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Rule

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	Surname	lastName
	E-Mail-Addresses	emails
	Is-Member-Of-DL	groups
▶	SAM-Account-Name	Name ID
*		

2. DOWNLOAD METADATA

If you are running AppGate v4.3 or later:

- Locate the metadata file as follows:
  - Use a browser to navigate to the metadata export URL on the AD FS server and download the file. The export URL will be https://*localhost*/FederationMetadata/2007-06/FederationMetadata.xml where *localhost* is the URL for your AD FS server. So the URL will look something like this:

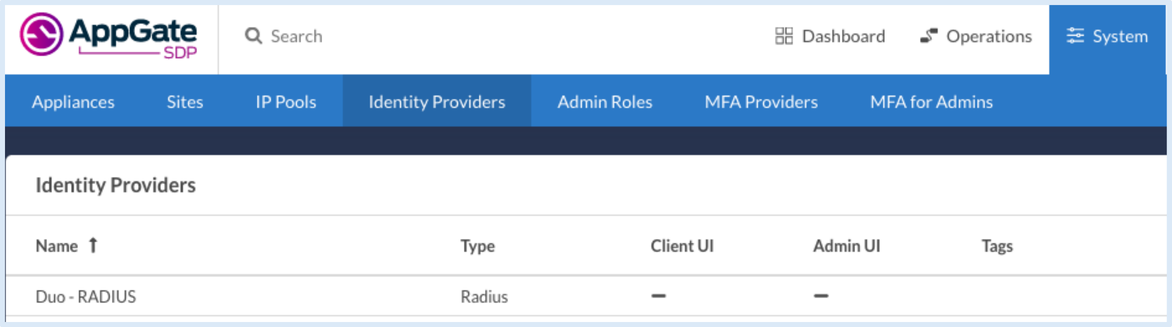
    ```
    https://AD FS.ad.mycompany.com/FederationMetadata/2007-
    06/FederationMetadata.xml
    ```

- Save the metadata file

If you are running AppGate v4.2 or earlier:

- Download the Public Certificate:
  - From the AD FS console navigate to Service > Endpoints
  - Click the Token-signing certificate.
  - In the Actions section, click View Certificate.
  - Click the Details tab, click Copy to File, and then click Next.
  - Select Base-64 encoded X.509 (.CER), and click Next.
  - Click Browse, select a location, enter a file name, and then click Save.
- Locate the following information – SSO (Single Sign-On) service URL and Entity URL:
  - From the AD FS console navigate to Service > Certificates
  - Search for SSO service endpoint and the entity URL.
    The SSO service URL will look like: `https://”yourdomain”/AD FS/ls/`
    The entity URL ends in “`AD FS/services/trust`”.

3. APPGATE SDP CONFIGURATION: ADD A NEW IDENTITY PROVIDER



Identity Providers

Name ↑	Type	Client UI	Admin UI	Tags
Duo - RADIUS	Radius	–	–	

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: "AD FS SAML Admin"	Enter a unique name eg: "AD FS SAML User"
IPv4Pool	select **default pool v4**	select **default pool v4**
Where to use	tick "Use for Admin UI sign in"	(Will be specified in the profile link)
Single Sign-on URL	*See below*	
Issuer	*See below*	
Audience	type in the ***Relying Party Trust Identifier*** you entered on the AD FS configuration	
Public Certificate	*See below*	

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

- Upload the XML Metadata file to autocomplete *Single Sign-On, Issuer* and *Public Certificate* fields
- Click <Choose a file> and select the metadata file that you created previously - this will autocomplete the relevant fields

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

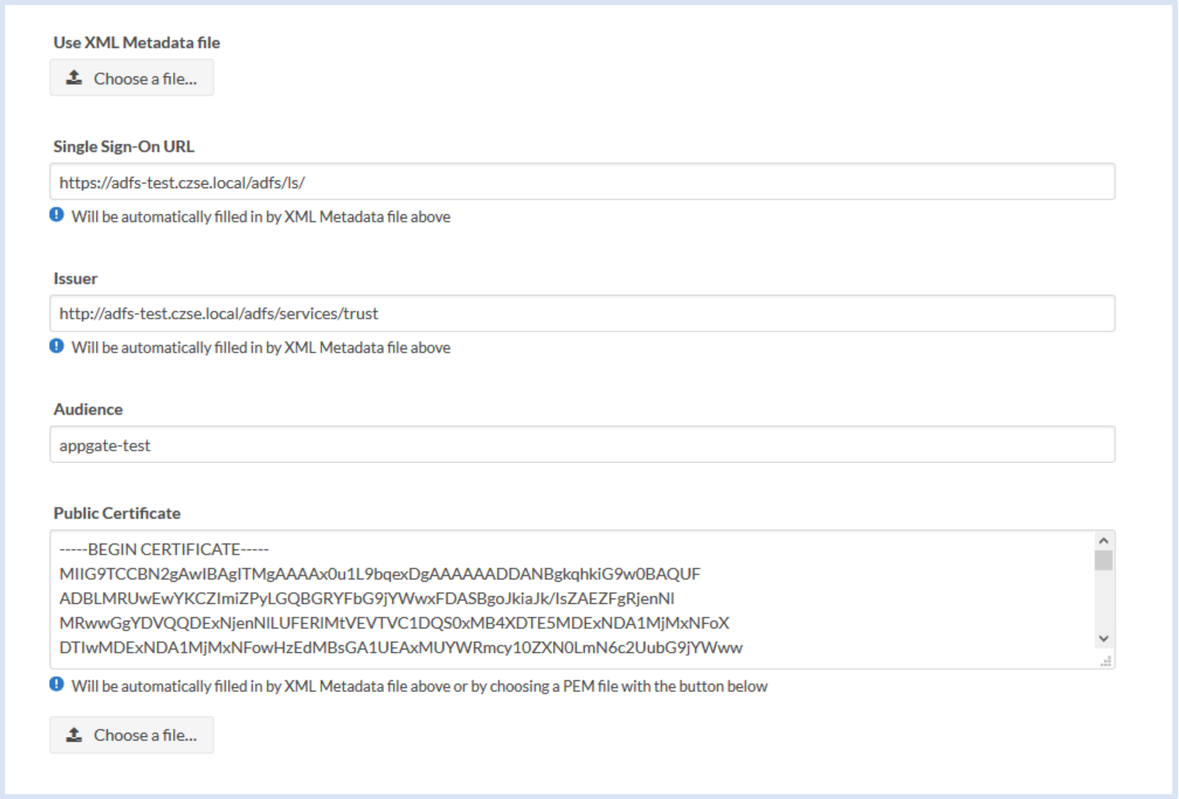
- You will need to manually complete the following fields with the data noted in section 2 above:

Single Sign-on URL	type in the ***SSO (Single Sign-On) service URL***
Issuer	type in the ***Entity URL***
Public Certificate	click <**Choose a File**> and upload the Certificate that you downloaded

If you need more information about how to manually complete the IdP configuration, please contact the Help Center

IdP Configuration for AD FS:

Your Identity Provider form should look something like this:



Use XML Metadata file

Single Sign-On URL

https://adfs-test.czse.local/adfs/ls/

Will be automatically filled in by XML Metadata file above

Issuer

http://adfs-test.czse.local/adfs/services/trust

Will be automatically filled in by XML Metadata file above

Audience

appgate-test

Public Certificate

```
-----BEGIN CERTIFICATE-----
MIIG9TCCBN2gAwIBAgITMgAAAAx0u1L9bqexDgAAAAAADDANBgkqhkiG9w0BAQUF
ADBLMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRjenNI
MRwwGgYDVQQDExNjenNILUFERlMtVEVTVC1DQS0xMB4XDTE5MDExNDA1MjMxNFoX
DTIwMDExNDA1MjMxNFowHzEdMBsGA1UEAxMUYWRmcy10ZXN0LmN6c2UubG9jYWww
```

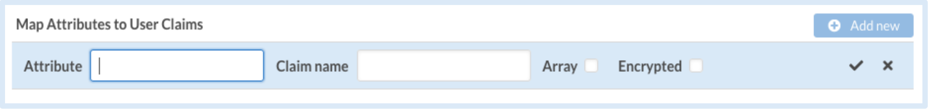
Will be automatically filled in by XML Metadata file above or by choosing a PEM file with the button below

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

4. MAP ATTRIBUTES

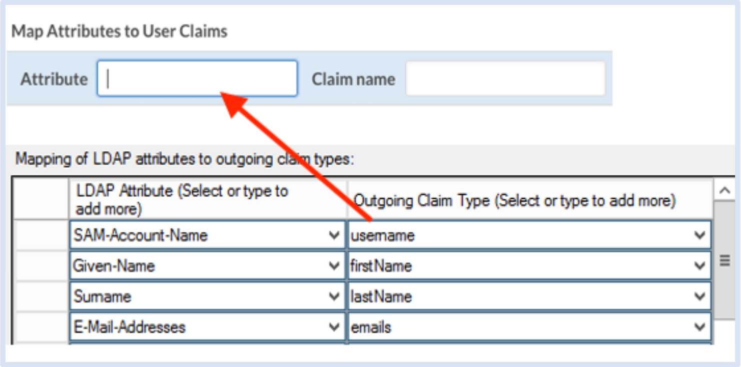
In the configuration form that you have created for your IdP:

- Fill in the <Attribute Mapping> section at the bottom of the form
- Click <ADD NEW MAPPING> to add each new attribute mapping



Map Attributes to User Claims

- Map the *LDAP Attributes* that were mapped in the AD FS configuration to AppGate SDP User Claims.
- The *Outgoing Claim Type* names that you created in AD FS need to be copied exactly into the AppGate SDP <Attribute> field.
- Pick an existing User Claim name to map to, or create new claim names.



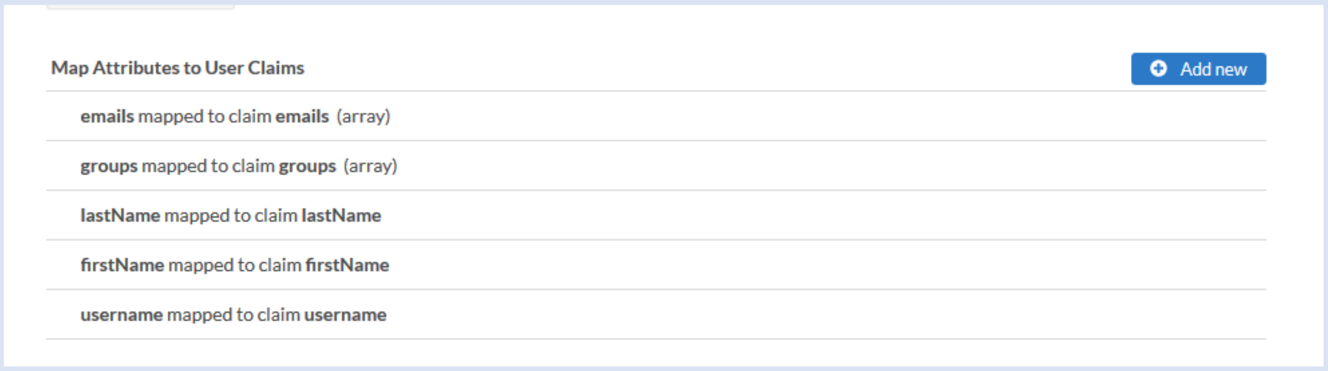
Map Attributes to User Claims

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
SAM-Account-Name	username
Given-Name	firstName
Sumame	lastName
E-Mail-Addresses	emails

- If you use Groups, Map the *Group Attribute Name* to <Claim name> *Groups* and tick the *array* box
- Click <Save>

Your completed attribute list should look something like this:



Map Attributes to User Claims

emails mapped to claim **emails** (array)

groups mapped to claim **groups** (array)

lastName mapped to claim **lastName**

firstName mapped to claim **firstName**

username mapped to claim **username**

5. TEST INTEGRATION

To test that integration has been completed successfully you need to log 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: • Sign out of the admin UI • Log in using the following information: *Identity Provider* – choose this new IdP from the drop down list • Click <Sign in with browser> to connect to your authenticator • 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:** • Quit if you are already connected • Get a new profile link from the Controller that includes this new IdP. • Add a new profile in the Client • Click <Sign in with provider> • Sign in using the browser to connect. • 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 ***Relying Party Trust Identifier*** on the AD FS configuration does not match the *Audience* field on the AppGate SDP configuration form.
2. **Attribute mapping:** the *Attributes* on the AppGate SDP configuration do not match the *Claim Types* on your AD FS configuration.

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
```

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 AppGate 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. Send your feedback to the Help Center.