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

V2.4
Tested for use on versions:
AppGate SDP v4.3 or newer
Last updated: March 2020

AppGate SDP – Azure AD: Integration Guide

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 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 Azure AD SSO authentication you will need to follow these steps:

1. Decide on your use case: Administrator and /or User authentication;
2. On your Azure AD console: create separate SAML Applications – one for each use case (Administrator Authentication and / or User Authentication);
3. In your AppGate SDP: create and configure a corresponding Azure IdP entity for each use case;
4. When configuring the two systems, use the appropriate ACS URL as the Reply 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). 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 Azure AD 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

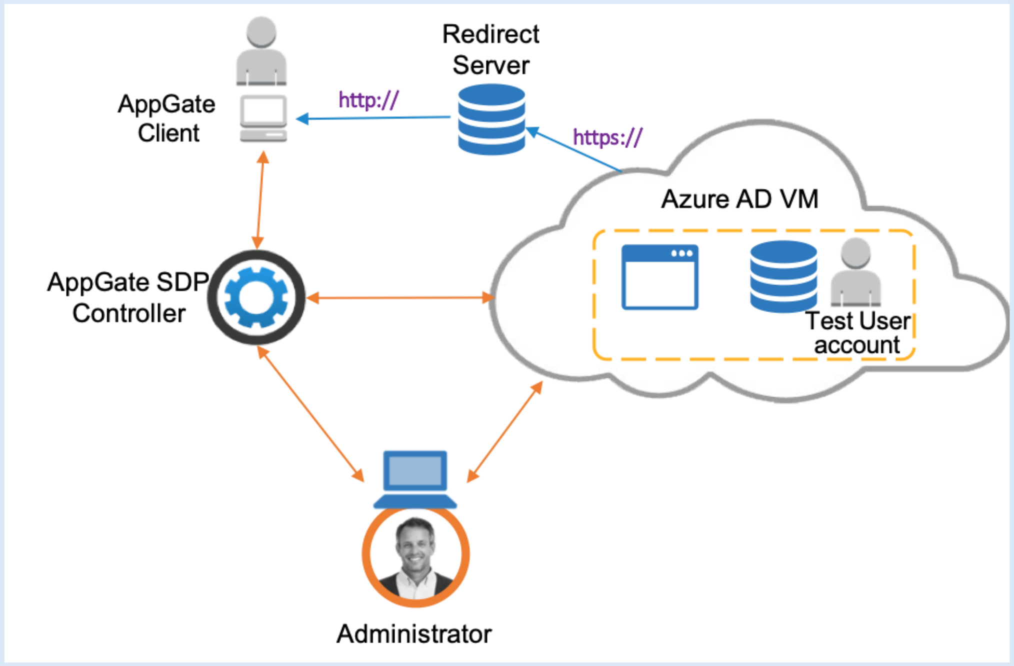


Figure 1: Azure AD integration test topology

This integration process requires the following:

- An Azure Active Directory (AD) instance on the Microsoft Azure public cloud that is accessible for users and AppGate SDP appliances
- An 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 on your Azure database, with at least one basic attribute field configured such as:
    1. *username* eg. “testuser”
    2. *first name eg.* “Joe”
    3. *last name* eg. “Smith”

Note that it may take some time to propagate these changes. For details about creating a user account refer to Microsoft support

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. AZURE AD SYSTEM CONFIGURATION: SET UP SINGLE SIGN-ON

Create a new application within Azure AD

- Sign in to the Azure portal using your Azure Active Directory administrator account.
- Browse to the Active Directory > Enterprise Applications > New application > Non-gallery application section
- Type in a name, eg:
  4. For Administrator Authentication: “AppGate Azure AD”
  5. For User Authentication: “AppGate Client Authentication”
- Click **<Add>**

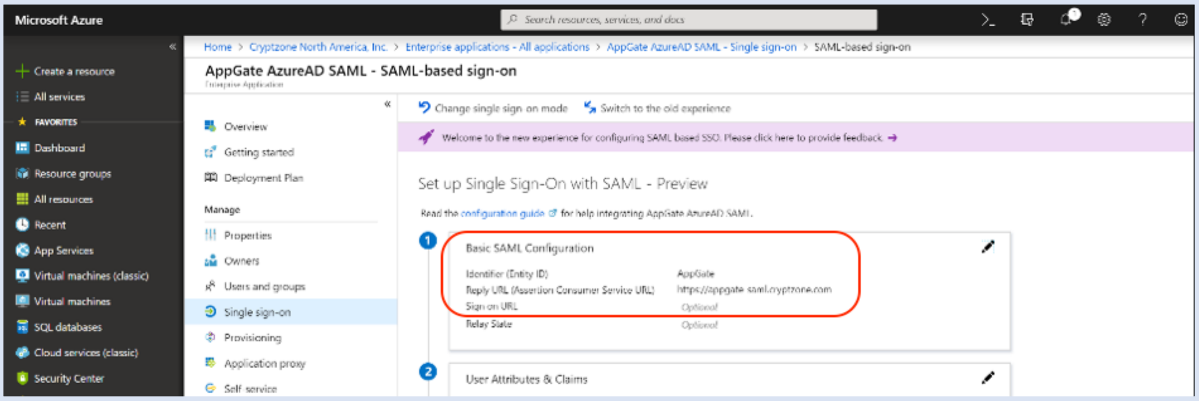
Enable Single Sign-On

- Browse to the Active Directory > Enterprise Applications section
- Search for and select the name of the app just created
- Select Configure Single Sign-On or click on Single sign-on from the application’s left-hand navigation menu
- Select SAML-based Sign-on from the menu

Enter basic SAML configuration in Box 1:

- *Identifier (Entity ID)* – Type in a unique name, see the table below
- *Reply URL* – type in the URL of the ACS verifying the SAML response, refer to the table below

Administrator Authentication:	**User Authentication:**
Identifier (Entity ID) = “AppGate” Reply URL = AppGate SDP Controller URL `https://mycontroller.mycompany.com/admin/saml`	Identifier (Entity ID) = “AppGate Client” Reply URL = redirection server URL `https://redirectserver.mycompany.com/saml`



AppGate AzureAD SAML - SAML-based sign-on

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →

Set up Single Sign-On with SAML - Preview

Read the configuration guide for help integrating AppGate AzureAD SAML.

Basic SAML Configuration

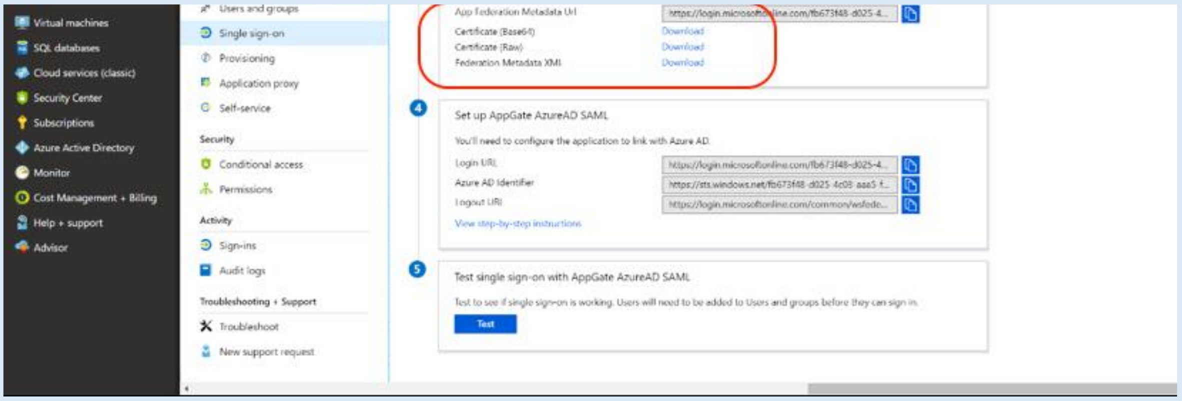
Identifier (Entity ID) AppGate
Reply URL (Assertion Consumer Service URL) https://appgate-saml.cryptzone.com
Sign on URL Optional
Relay State Optional

User Attributes & Claims

Figure 2: Box 1 SAML Configuration

Download the Certificate (Base64) in Box 3 -

- Choose the Base64 certificate and click **<Download>**



App Federation Metadata Url https://login.microsoftonline.com/fb673f48-d025-4...
Certificate (Base64) Download
Certificate (Raw) Download
Federation Metadata XML Download

Set up AppGate AzureAD SAML

You'll need to configure the application to link with Azure AD.

Login URL https://login.microsoftonline.com/fb673f48-d025-4...
Azure AD Identifier https://sts.windows.net/fb673f48-d025-4c03-aaa5-f...
Logout URL https://login.microsoftonline.com/common/wsfede...

View step-by-step instructions

Test single sign-on with AppGate AzureAD SAML

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

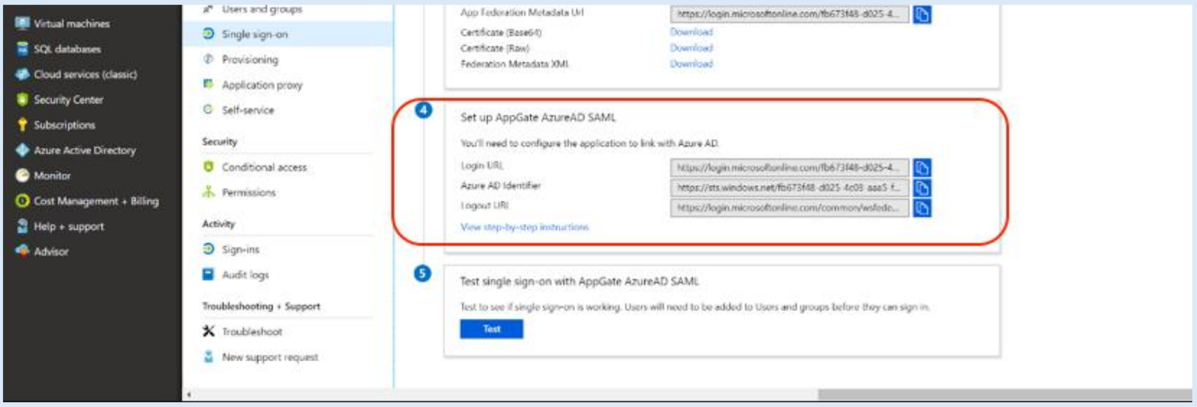
Figure 3: Box 3 Base64 Certificate Download

Download the XML metadata file in box 3:

- click on the metadata Download button

Make a note of the additional information you will need to configure your AppGate SDP:

Information needed for configuring AppGate SDP	
Box 1	• *Identifier (Entity ID)* • *Reply URL*
Box 4	• *Login URL:* the URL for your Azure AD app • *Azure AD Identifier:* your Azure AD app identifier



App Federation Metadata Url https://login.microsoftonline.com/fb673f48-d025-4...
Certificate (Base64) Download
Certificate (Raw) Download
Federation Metadata XML Download

Set up AppGate AzureAD SAML

You'll need to configure the application to link with Azure AD.

Login URL https://login.microsoftonline.com/fb673f48-d025-4...
Azure AD Identifier https://sts.windows.net/fb673f48-d025-4c03-aaa5-f...
Logout URL https://login.microsoftonline.com/common/wsfede...

View step-by-step instructions

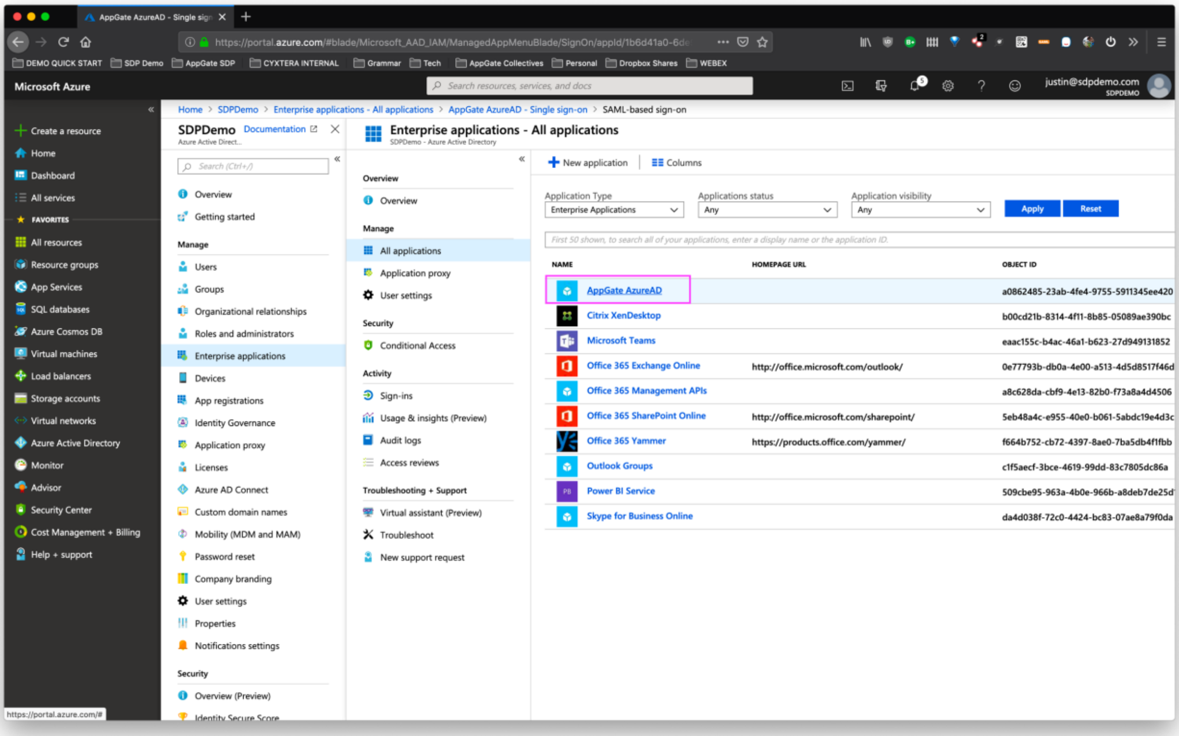
Test single sign-on with AppGate AzureAD SAML

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Figure 4: Box 4 Azure AD app identifier and login details

Attribute mapping – USING GROUP MEMBERSHIP

- In AD it is very common to want to map Group membership and use this to make Policy assignment decisions later on. In your Azure portal, navigate to **Azure Active Directory** > **Enterprise Applications** and then click on the SAML app you created for AppGate.



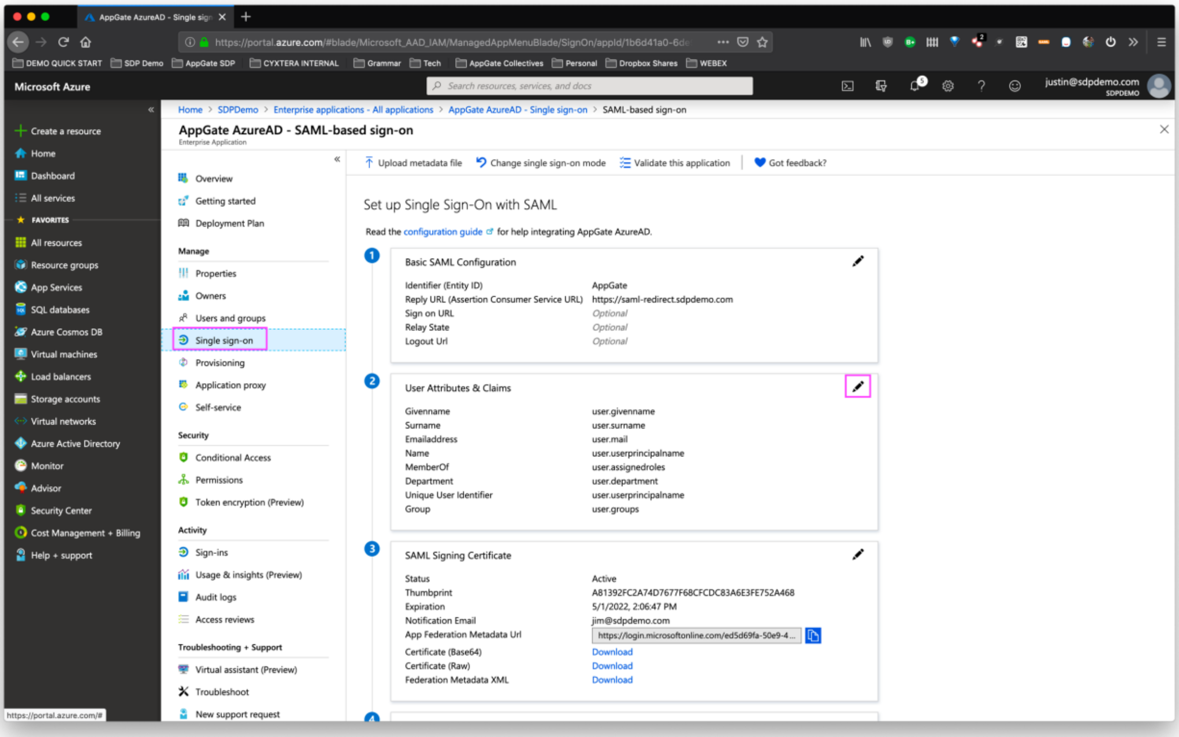
Enterprise applications - All applications

Application Type: Enterprise Applications
Applications status: Any
Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

NAME	HOMEPAGE URL	OBJECT ID
AppGate AzureAD		a0862485-23ab-4fe4-9755-5911345ee420
Citrix XenDesktop		b00cd21b-8314-4f11-8b85-05089ae390bc
Microsoft Teams		eaac155c-b4ac-46a1-b623-27d949131852
Office 365 Exchange Online	http://office.microsoft.com/outlook/	0e77793b-db0a-4e00-a513-4d5d8517f46d
Office 365 Management APIs		a8c628da-cbf9-4e13-82b0-f73a8a4d4506
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	5eb48a4c-e955-40e0-b061-5abdc19e4d3c
Office 365 Yammer	https://products.office.com/yammer/	f664b752-cb72-4397-8ae0-7ba5db4f1fbb
Outlook Groups		c1f5aecf-3bce-4619-99dd-83c7805dc86a
Power BI Service		509cbe95-963a-4b0e-966b-a8deb7de25d
Skype for Business Online		da4d038f-72c0-4424-bc83-07ae8a79f0da

- Open the **Single Sign-On** pane and click the edit (pencil) icon to the right of **User Attributes & Claims**.


Microsoft Azure
Home > SDPDemo > Enterprise applications - All applications > AppGate AzureAD - Single sign-on > SAML-based sign-on
AppGate AzureAD - SAML-based sign-on
Enterprise Application
Single sign-on
Upload metadata file
Change single sign-on mode
Validate this application
Got feedback?

Set up Single Sign-On with SAML

Read the configuration guide for help integrating AppGate AzureAD.

1 Basic SAML Configuration

Identifier (Entity ID)	AppGate
Reply URL (Assertion Consumer Service URL)	https://saml-redirect.sdpdemo.com
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

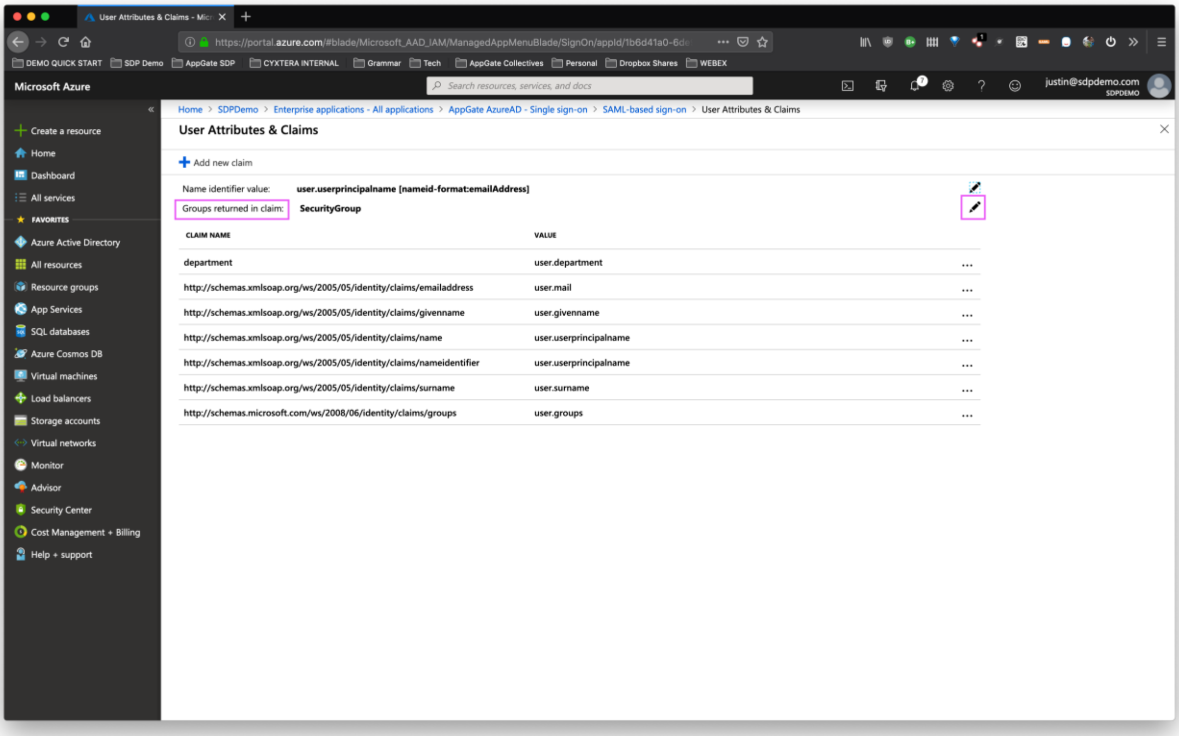
2 User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
MemberOf	user.assignedroles
Department	user.department
Unique User Identifier	user.userprincipalname
Group	user.groups

3 SAML Signing Certificate

Status	Active
Thumbprint	A81392FC2A74D7677F68CFCDC83A6E3FE752A468
Expiration	5/1/2022, 2:06:47 PM
Notification Email	jim@sdpdemo.com
App Federation Metadata Url	https://login.microsoftonline.com/ed5d69fa-50e9-4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

- Click the edit (pencil) icon to the right of **Groups returned in claim**.



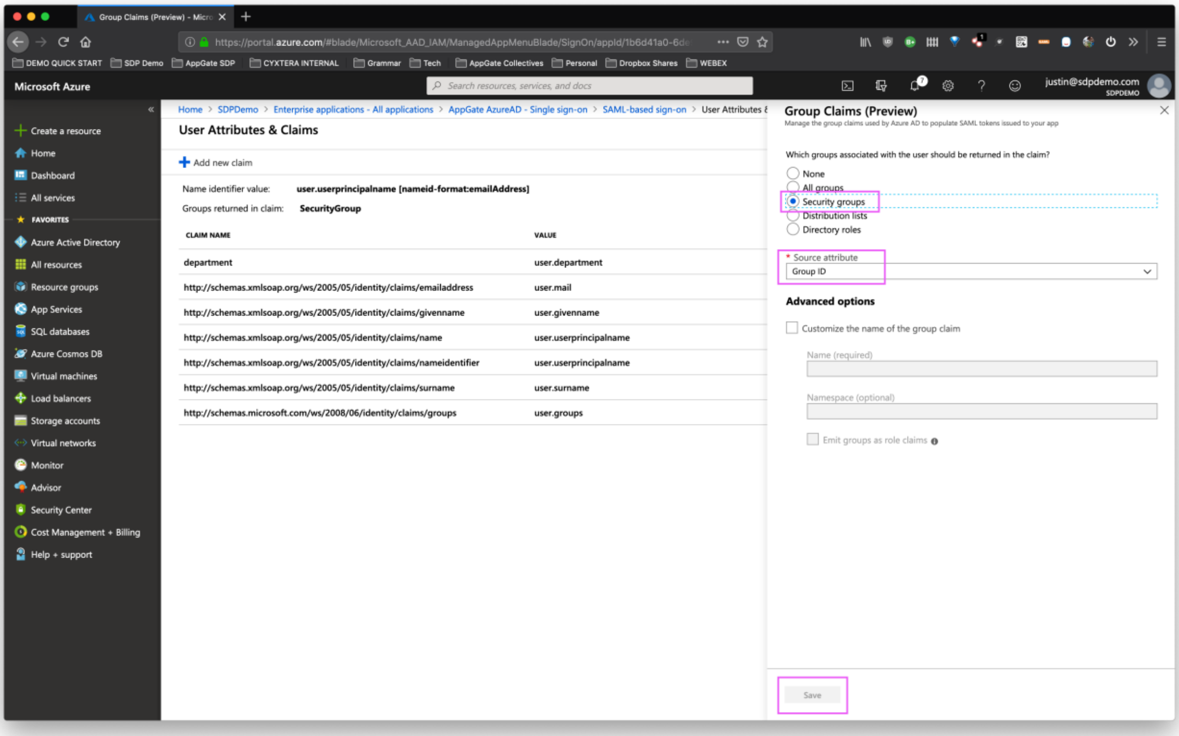
User Attributes & Claims

Name identifier value: **user.userprincipalname [nameid-format:emailAddress]**

Groups returned in claim: **SecurityGroup**

CLAIM NAME	VALUE
department	user.department
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups

- Apply settings as shown below, then press **Save**.



User Attributes & Claims

Name identifier value: **user.userprincipalname [nameid-format:emailAddress]**

Groups returned in claim: **SecurityGroup**

CLAIM NAME	VALUE
department	user.department
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups

Group Claims (Preview)

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
○ All groups
● Security groups
○ Distribution lists
○ Directory roles

* Source attribute: Group ID

Advanced options

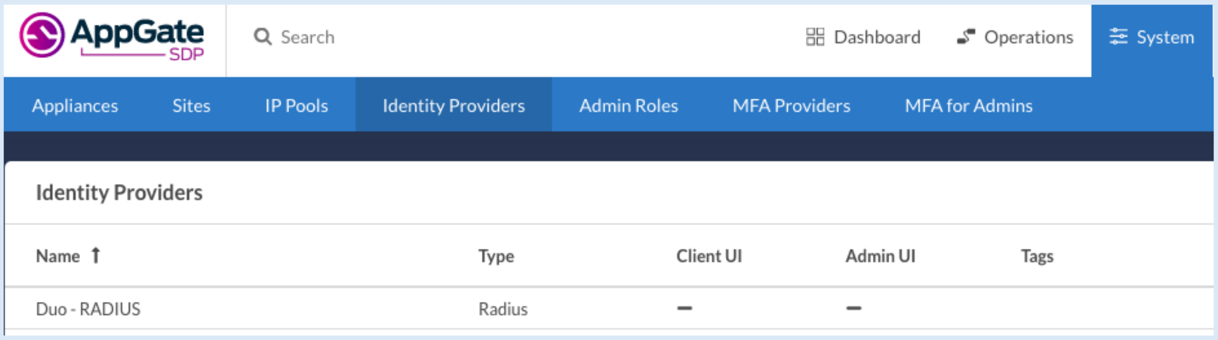
□ Customize the name of the group claim

Name (required)

Namespace (optional)

□ Emit groups as role claims

2. 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: “Azure SAML Admin”	Enter a unique name eg: “Azure 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 **Identifier (Entity ID)** from the Azure AD basic configuration (Box 1)	
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:

- You will need to manually complete the following fields with the data noted in section 1 above:

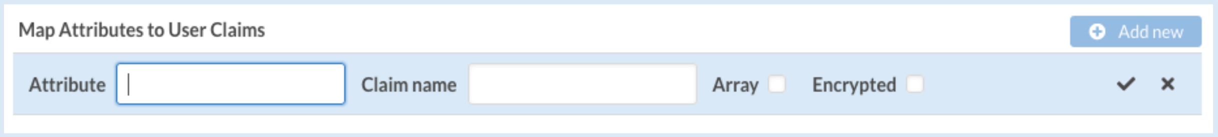
Single Sign-on URL	type in the ***Login URL*** from the Azure AD configuration (Box 4)
Issuer	type in the ***Azure AD Identifier*** from the Azure AD configuration (Box 4)
Public Certificate	click <**Choose a File**> and upload the Certificate that you downloaded (Box 3)

3. MAP ATTRIBUTES

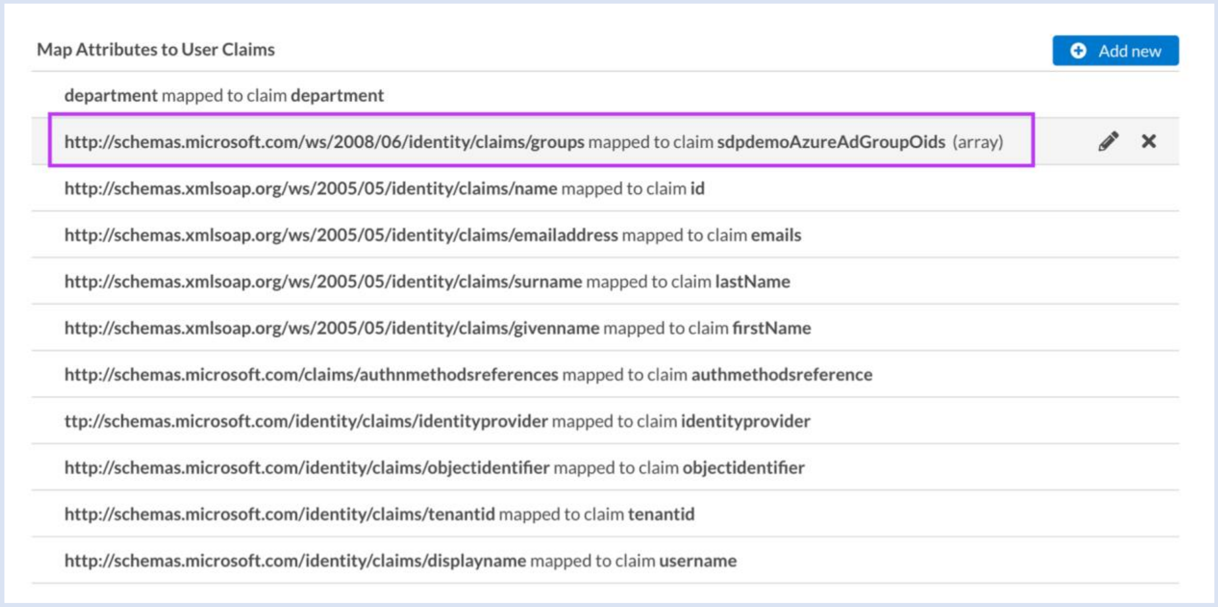
In the configuration form that you have created for your IdP:

- On the **System > Identity Providers** UI, open the Identity Provider form for your Azure AD authentication. In the <**Attribute Mapping**> section at the bottom of the form specify the Azure AD attribute fields that need to be mapped to AppGate SDP.
- User Claims: click <**ADD NEW MAPPING>** to add each new attribute mapping such as when mapping group membership (Array):

  To use the Group membership attribute set up earlier add a new claim as follows:
  Attribute: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
  Claim name: AzureGroups
  NOTE: you can name this anything that makes sense to you



Your completed form should look something like this:



department mapped to claim **department**

http://schemas.microsoft.com/ws/2008/06/identity/claims/groups mapped to claim **sdpdemoAzureAdGroupOids** (array)

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name mapped to claim **id**

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress mapped to claim **emails**

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname mapped to claim **lastName**

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname mapped to claim **firstName**

http://schemas.microsoft.com/claims/authnmethodsreferences mapped to claim **authmethodsreference**

ttp://schemas.microsoft.com/identity/claims/identityprovider mapped to claim **identityprovider**

http://schemas.microsoft.com/identity/claims/objectidentifier mapped to claim **objectidentifier**

http://schemas.microsoft.com/identity/claims/tenantid mapped to claim **tenantid**

http://schemas.microsoft.com/identity/claims/displayname mapped to claim **username**

4. 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:

On your AppGate SDP Controller console:

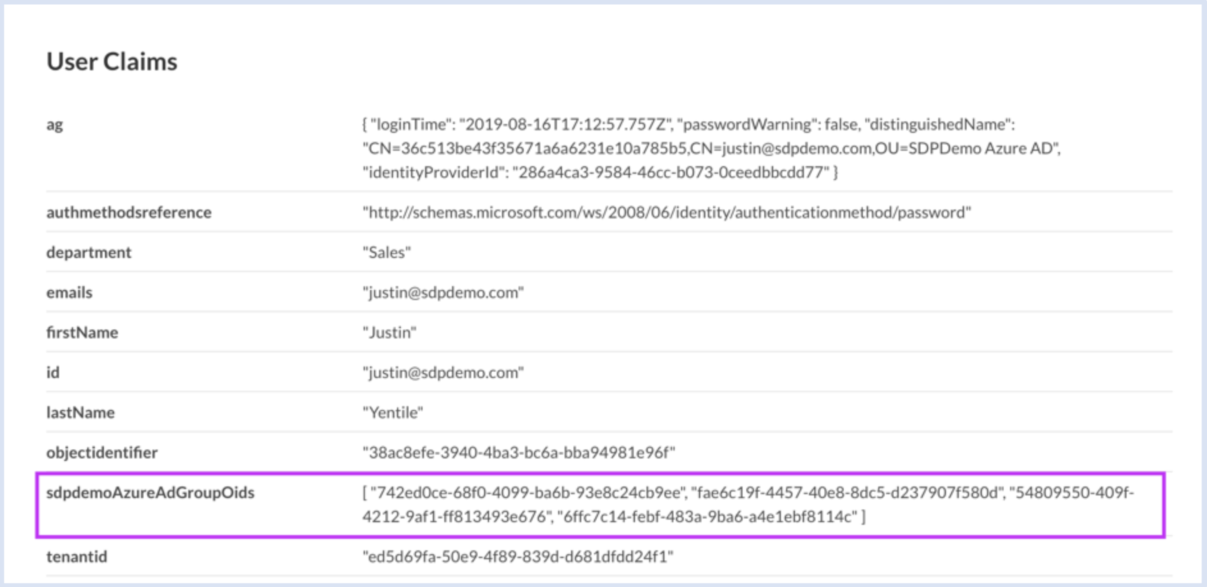
- Log out of the admin UI
- Log in using the following information:
- *Identity Provider* – choose your Azure IdP from the drop down list
- Click <Sign in with browser> to connect to your authenticator
- You may see the following message:
  "You don't have any administration rights" – this confirms that the test user credentials have been successfully authenticated by your Identity Provider.

User Authentication:

On the AppGate SDP Client:

- Quit if you are already connected
- Select your Azure IdP from the Identity Provider drop down list
- Click <NEXT>
- Click <OPEN> to open a browser to connect to your authenticator
- You should see a message from your client confirming successful authentication

- In the AppGate admin console, navigate to **Dashboard** > **Active Sessions** > **[your session]**. In the **User Claims** section, you'll now see the OIDs of the Security Groups to which you're a member listed in the claim you defined in the previous step.



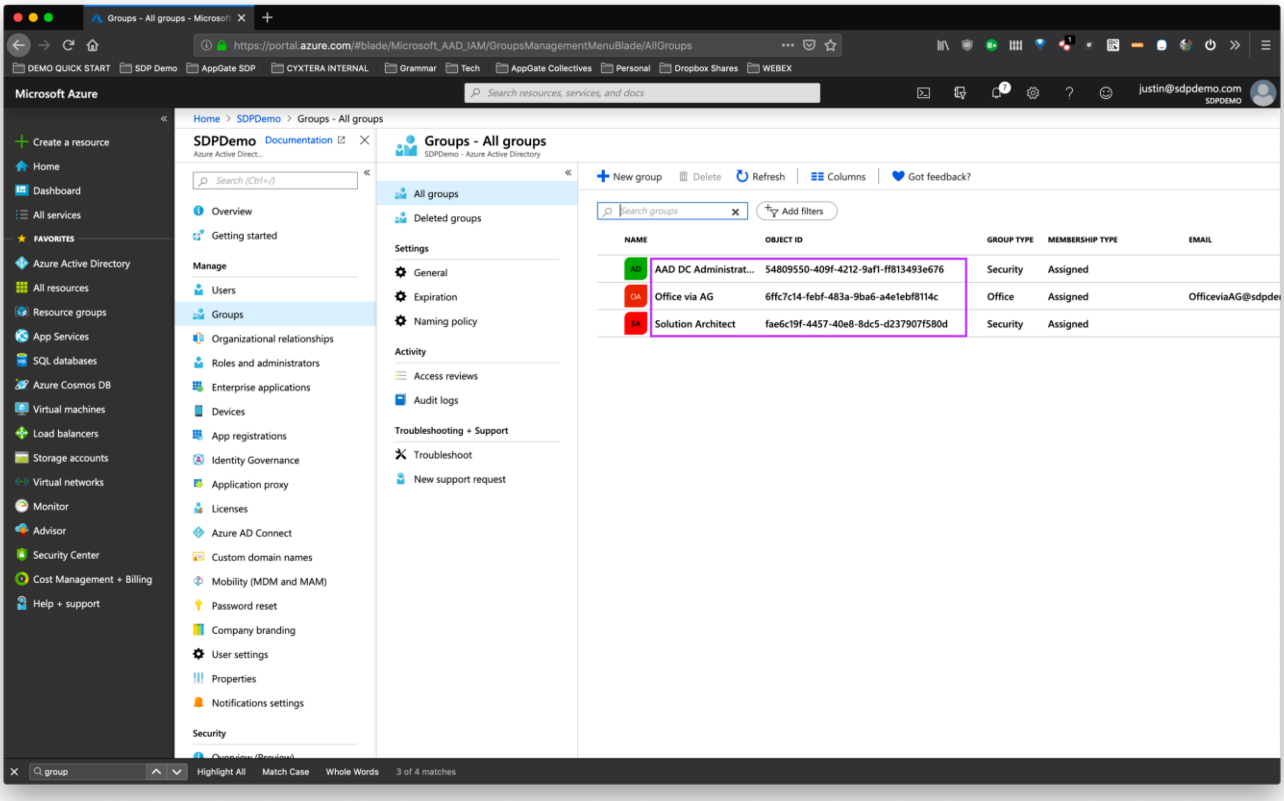
User Claims

ag	{ "loginTime": "2019-08-16T17:12:57.757Z", "passwordWarning": false, "distinguishedName": "CN=36c513be43f35671a6a6231e10a785b5,CN=justin@sdpdemo.com,OU=SDPDemo Azure AD", "identityProviderId": "286a4ca3-9584-46cc-b073-0ceedbbcdd77" }
authmethodsreference	"http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password"
department	"Sales"
emails	"justin@sdpdemo.com"
firstName	"Justin"
id	"justin@sdpdemo.com"
lastName	"Yentile"
objectidentifier	"38ac8efe-3940-4ba3-bc6a-bba94981e96f"
sdpdemoAzureAdGroupOids	["742ed0ce-68f0-4099-ba6b-93e8c24cb9ee", "fae6c19f-4457-40e8-8dc5-d237907f580d", "54809550-409f-4212-9af1-ff813493e676", "6ffc7c14-febf-483a-9ba6-a4e1ebf8114c"]
tenantid	"ed5d69fa-50e9-4f89-839d-d681dfdd24f1"

5. POLICY ASSIGNMENT - to an authenticated member of that group:

In your AppGate SDP admin UI:

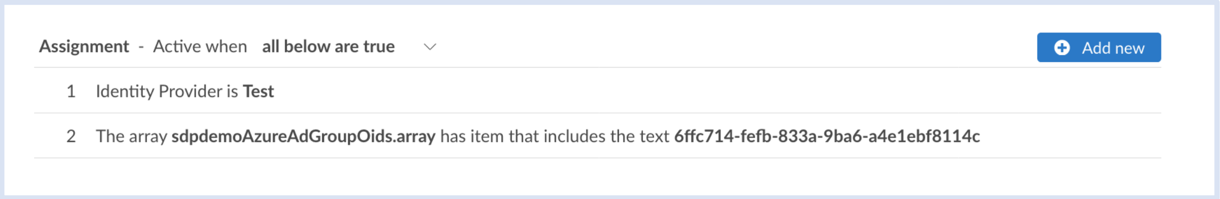
- Use the Operations > Policies UI to create a new Policy
- Use these OIDs as access criteria in your Policies.
  In order to correlate group OID to group name you should go back to **Azure Active Directory** > **Groups** where the Names and Object IDs are shown:



Groups - All groups - Microsoft
https://portal.azure.com/#blade/Microsoft_AAD_IAM/GroupsManagementMenuBlade/AllGroups
Microsoft Azure
Home > SDPDemo > Groups - All groups
SDPDemo
Groups - All groups
SDPDemo - Azure Active Directory
All groups
Deleted groups
New group
Delete
Refresh
Columns
Got feedback?
Search groups
Add filters

NAME	OBJECT ID	GROUP TYPE	MEMBERSHIP TYPE	EMAIL
AD AAD DC Administrat...	54809550-409f-4212-9af1-ff813493e676	Security	Assigned	
OA Office via AG	6ffc7c14-febf-483a-9ba6-a4e1ebf8114c	Office	Assigned	OfficeviaAG@sdpde
SA Solution Architect	fae6c19f-4457-40e8-8dc5-d237907f580d	Security	Assigned	

- In the Assignment section, ad a new Policy assignment criteria that uses the group array that was mapped earlier. For example, your Policy assignment might look like this:



Assignment - Active when **all below are true**

1 Identity Provider is **Test**

2 The array **sdpdemoAzureAdGroupOids.array** has item that includes the text **6ffc714-fefb-833a-9ba6-a4e1ebf8114c**

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 SAML app configuration does not match the *Audience* field on the AppGate SDP configuration form.
2. **Attribute mapping:** there is an error in the Groups array configuration on AppGate SDP

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 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. Send your feedback to the Help Center.