AppGate SDP and PingOne®
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 – PingOne: Integration Guide

TABLE OF CONTENTS

INTRODUCTION

AppGate SDP supports single sign-on authentication using SAML 2.0 identity providers (IdP) such as ADFS, OKTA, OneLogin and PingOne. 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 PingOne SSO authentication you will need to follow these steps:

1. Decide on your use case: Administrator and /or User authentication;
2. On your PingOne 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 PingOne 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).
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 PingOne 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

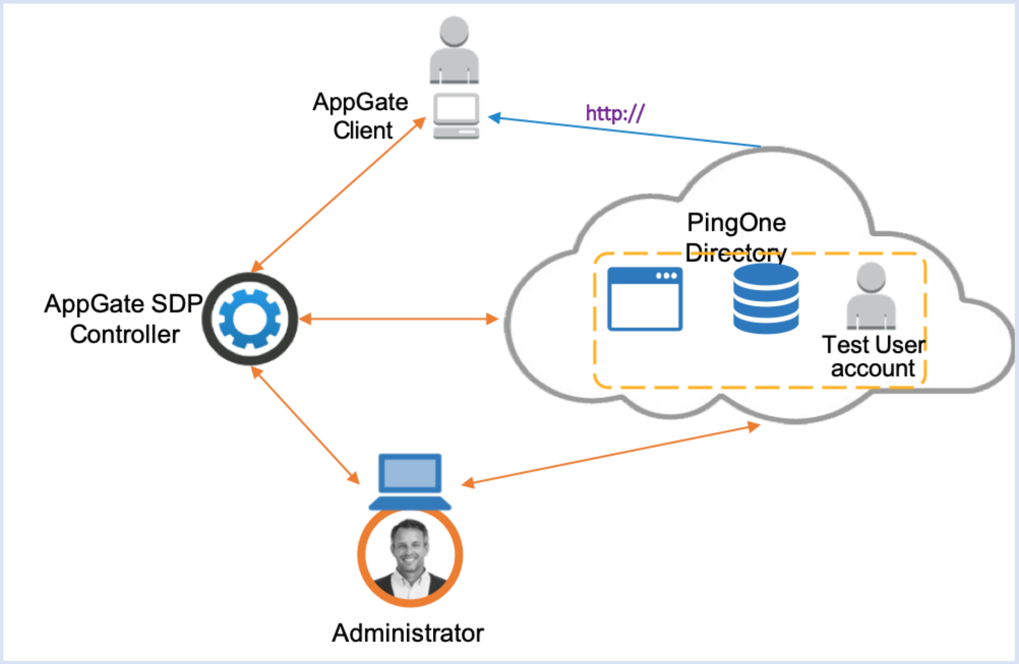


Figure 1: PingOne integration test topology

This integration process requires the following:

- PingOne 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 on your PingOne cloud directory, with at least one basic attribute field configured such as:
    - *username* eg. "testuser"
    - *firstName eg.* "Joe"
    - *lastName* eg. "Smith"

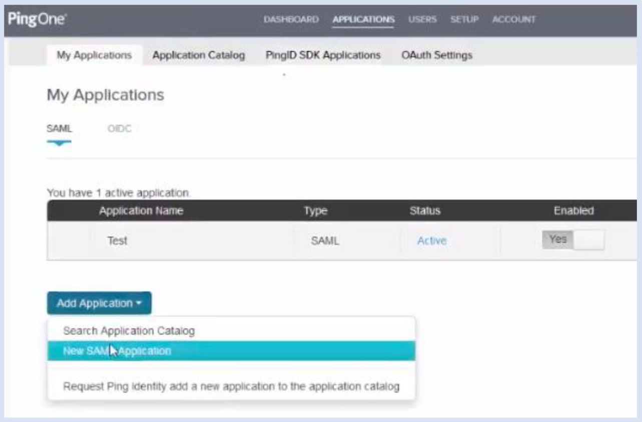
STEP BY STEP GUIDE TO INTEGRATION

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. PINGONE CONFIGURATION: SET UP SINGLE SIGN-ON

Screen 1. Add a new application

- Log in to your PingOne administrator account.
- In the <Applications> tab, click <Add Application> and choose <New SAML Application>
- Type in a name, eg:
  - For Administrator Authentication: “AppGate SDP”
  - For User Authentication: “AppGate SDP Client App”
- Click <Continue to Next Step>



My Applications

You have 1 active application.

Application Name	Type	Status	Enabled
Test	SAML	Active	Yes

Screen 2. Application Configuration

- Fill in the configuration form:
  - *Protocol Version* - set to <SAML 2.0>
  - *Assertion Consumer Service (ACS)* – Type in the appropriate ACS URL, refer to the table below
  - *Entity ID* – Type in a unique name, make a note of this as you will need it to configure AppGate SDP

Administrator Authentication:	**User Authentication:**

ACS = AppGate SDP Controller URL
`https://mycontroller.mycompany.com/admin/saml`
	ACS = localhost redirection server URL
	`http://127.0.0.1:29001/saml`

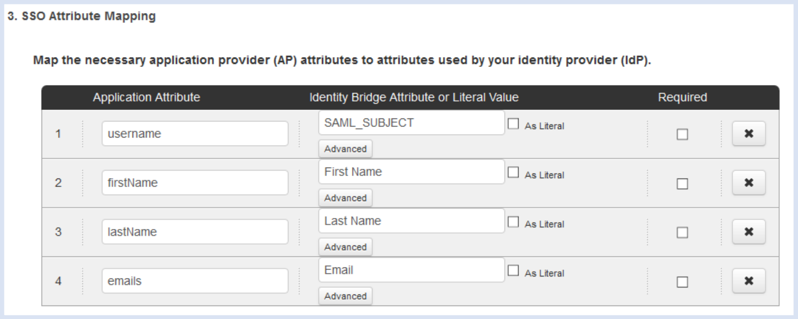
- Click <Continue to Next Step>

Screen 3. SSO Attribute Mapping

- Create application attributes and specify which SAML attributes should be mapped to in the ID token. Use the attributes that have been configured for the test user account
  eg.
  - Application attribute *username* - Identity bridge attribute *SAML_SUBJECT*
  - Application attribute *firstName* - Identity bridge attribute *FirstName*
  - Application attribute *lastName* - Identity bridge attribute *LastName*

- Make a note of the Application Attribute names you have created, you will need them when configuring your AppGate SDP

- Click <Continue to Next Step>



3. SSO Attribute Mapping

Map the necessary application provider (AP) attributes to attributes used by your identity provider (IdP).

	Application Attribute	Identity Bridge Attribute or Literal Value		Required	
1	username	SAML_SUBJECT	□ As Literal	□	✖
2	firstName	First Name	□ As Literal	□	✖
3	lastName	Last Name	□ As Literal	□	✖
4	emails	Email	□ As Literal	□	✖

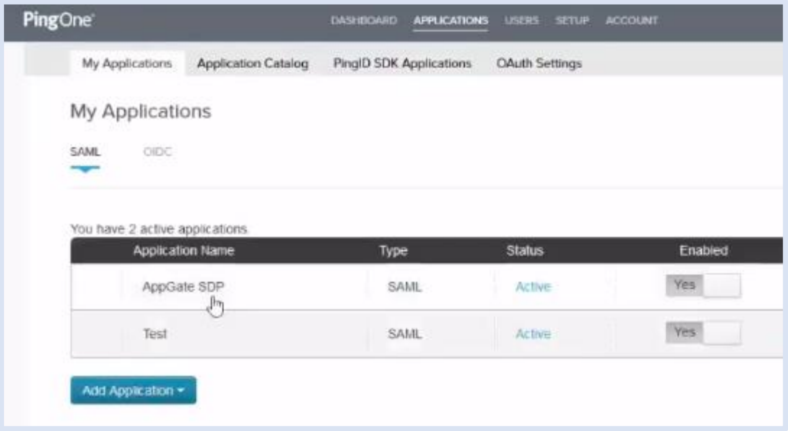
Screen 4. Group Access

- This is optional
- Click <Continue to Next Step>

Screen 5. Review Setup

- Click <Finish>

On your PingOne console your new application should be active



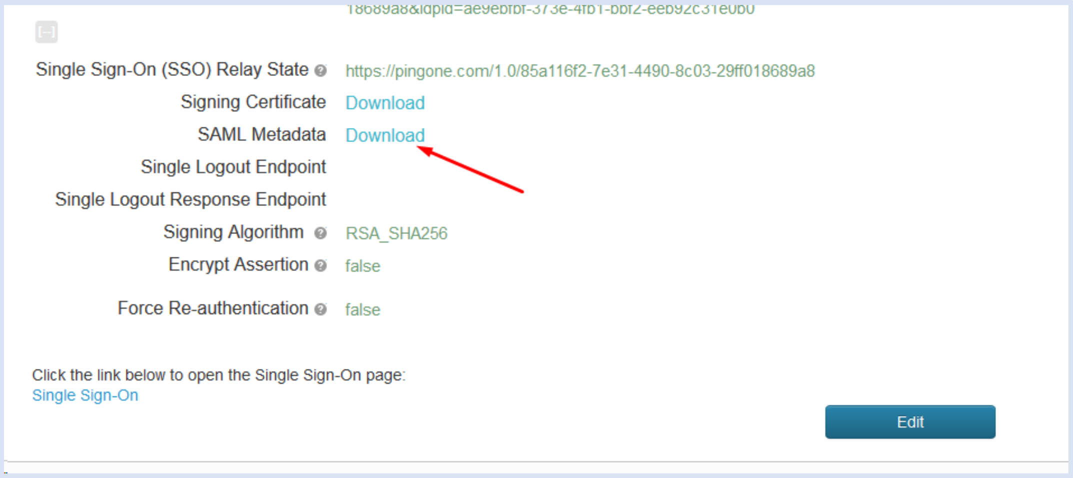
My Applications

You have 2 active applications

Application Name	Type	Status	Enabled
AppGate SDP	SAML	Active	Yes
Test	SAML	Active	Yes

2. DOWNLOAD METADATA

- On your PingOne console click on the *AppGate SDP* application you have just created
- Download SAML Metadata
- If you are running AppGate SDP v4.2 or earlier, you will also need to download the Signing Certificate

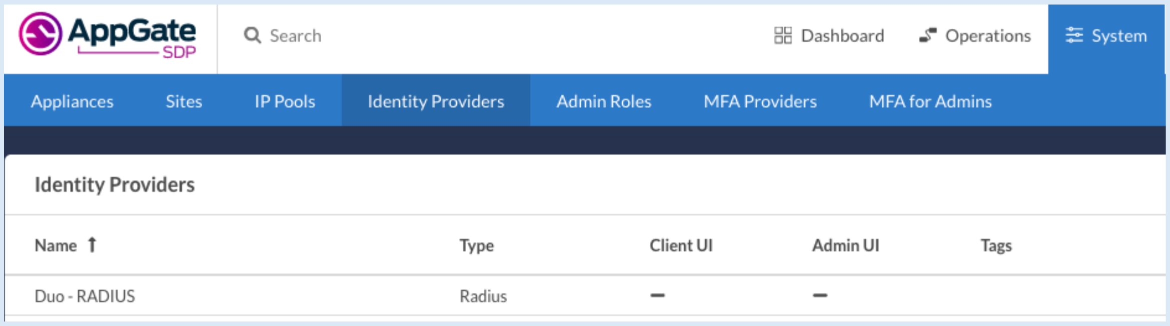


18689a8&idpid=ae9ebfbf-373e-4fb1-bbf2-eeb92c31e0b0

Single Sign-On (SSO) Relay State	https://pingone.com/1.0/85a116f2-7e31-4490-8c03-29ff018689a8
Signing Certificate	Download
SAML Metadata	Download
Single Logout Endpoint	
Single Logout Response Endpoint	
Signing Algorithm	RSA_SHA256
Encrypt Assertion	false
Force Re-authentication	false

Click the link below to open the Single Sign-On page:
Single Sign-On

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.

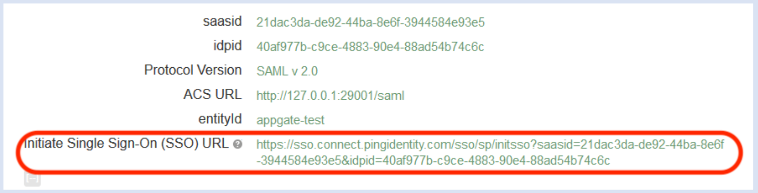
	Administrator Authentication:	**User Authentication:**
Name	Enter a unique name eg: “PingOne SAML Admin”	Enter a unique name eg: “PingOne SAML User”
IPv4Pool	select **default pool v4**	select **default pool v4**
Where to use	tick “Admin UI”	(will become available for a Profile link)
Single Sign-on URL	*See below*	
Issuer	*See below*	
Audience	type in the **Entity ID** you entered on the PingOne configuration	
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:
  1. *Single Sign-On URL:* copy & paste the Single Sign-On (SSO) URL from your PingOne Application form
  2. *Public Certificate:* upload the certificate you have already downloaded
  3. *Issuer:* This is the URL for your SAML provider. Reference the PingOne metadata file.

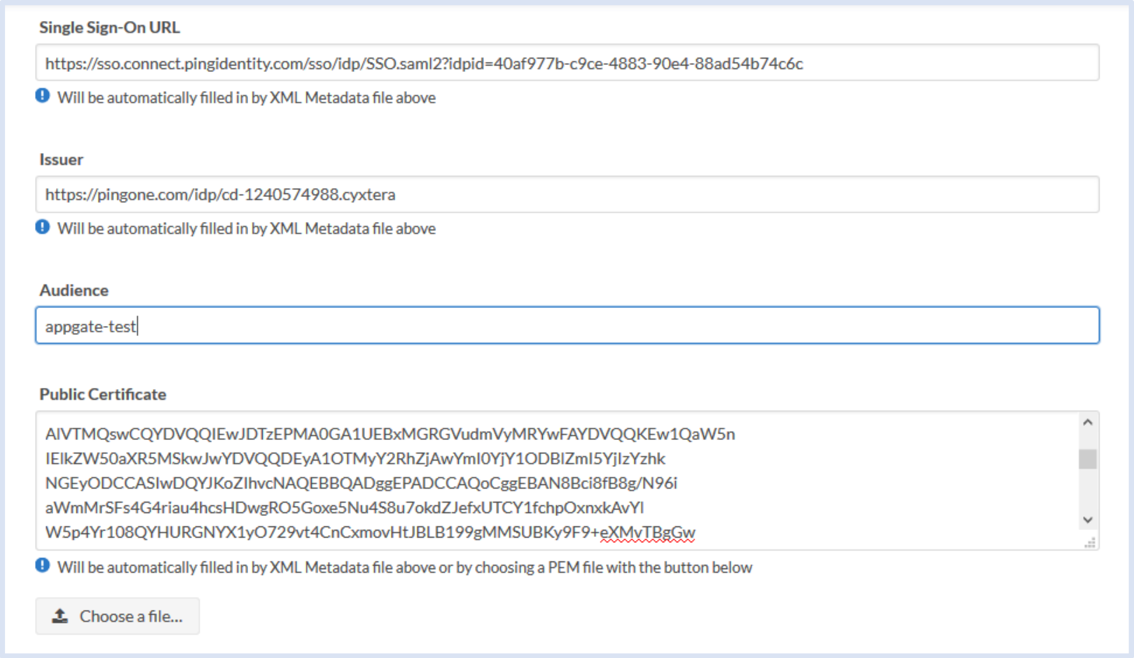


saasid	21dac3da-de92-44ba-8e6f-3944584e93e5
idpid	40af977b-c9ce-4883-90e4-88ad54b74c6c
Protocol Version	SAML v 2.0
ACS URL	http://127.0.0.1:29001/saml
entityId	appgate-test
Initiate Single Sign-On (SSO) URL	https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=21dac3da-de92-44ba-8e6f-3944584e93e5&idpid=40af977b-c9ce-4883-90e4-88ad54b74c6c

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

IdP Configuration for PingOne:

Your Identity Provider form should look something like this:



Single Sign-On URL

https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=40af977b-c9ce-4883-90e4-88ad54b74c6c

Will be automatically filled in by XML Metadata file above

Issuer

https://pingone.com/idp/cd-1240574988.cyxtera

Will be automatically filled in by XML Metadata file above

Audience

appgate-test

Public Certificate

AIVTMQswCQYDVQQIEwJDTzEPMA0GA1UEBxMGRGVudmVyMRYwFAYDVQQKEw1QaW5n
IElkZW50aXR5MSkwJwYDVQQDEyA1OTMyY2RhZjAwYmI0YjY1ODBlZmI5YjIzYzhk
NGEyODCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN8Bci8fB8g/N96i
aWmMrSFs4G4riau4hcsHDwgRO5Goxe5Nu4S8u7okdZJefxUTCY1fchpOxnxkAvYl
W5p4Yr108QYHURGNYX1yO729vt4CnCxmovHtJBLB199gMMSUBKy9F9+eXMvTBgGw

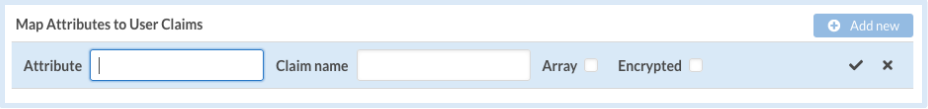
Will be automatically filled in by XML Metadata file above or by choosing a PEM file with the button below

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

4. MAP ATTRIBUTES

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

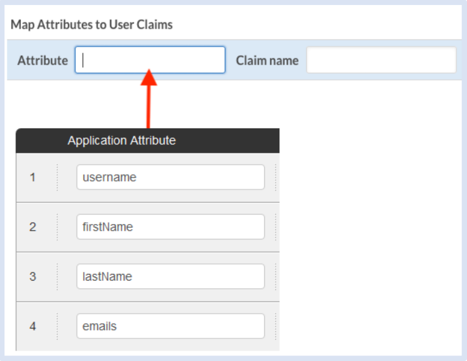
- Fill in the <**Attribute Mapping**> section at the bottom of the form
- Click <**ADD NEW MAPPING>** to add each new attribute mapping



Map Attributes to User Claims

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

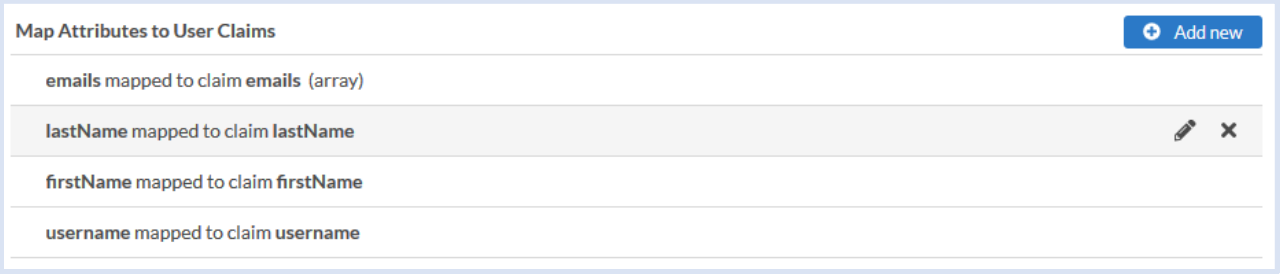
- Click <**Save>**



Map Attributes to User Claims

Application Attribute	
1	username
2	firstName
3	lastName
4	emails

Your completed attribute list should look something like this:



Map Attributes to User Claims

emails mapped to claim **emails** (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 *Entity ID* field on the SAML app 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 *Application Attributes* on your PingOne 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 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.