

AppGate

SDP



AppGate SDP and Okta SAML Single Sign-On Integration Guide

V2.01

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

AppGate SDP – Okta: Integration Guide
Copyright © 2020 Cyxtera Cybersecurity, Inc. d/b/a AppGate

All rights reserved. AppGate is a trademark of Cyxtera Cybersecurity, Inc. d/b/a AppGate.
All other product names mentioned
herein are trademarks of their respective owners

TABLE OF CONTENTS

INTRODUCTION.....	3
BEFORE YOU START	4
STEP BY STEP GUIDE TO INTEGRATION	5
1. OKTA CONFIGURATION: SET UP SINGLE SIGN-ON	5
2. DOWNLOAD METADATA	8
3. APPGATE SDP CONFIGURATION: ADD A NEW IDENTITY PROVIDER	9
4. MAP ATTRIBUTES.....	11
5. TEST INTEGRATION	12
TROUBLESHOOTING.....	12
HELP AND SUPPORT.....	13
FEEDBACK	13

INTRODUCTION

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

1. Decide on your use case: **Administrator** and /or **User** authentication;
2. On your Okta 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 Okta 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 “Single sign-on URL” in the Okta configuration.

Table 1: Assertion Consumer Service (ACS) URL:

Administrator Authentication:	User Authentication:
<p>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. <code>https://mycontroller.mycompany.com:444/admin/saml</code></p>	<p>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. <code>https://redirectserver.mycompany.com/saml</code> The redirect to will be to <code>http://127.0.0.1:29001/saml</code> More information about the requirements for SAML response verification can be found at: https://sdphelp.appgate.com/adminguide/saml-idp.html</p> <p>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: <code>http://127.0.0.1:29001/saml</code></p>

About this integration guide

This document provides a step-by-step guide to integrate Okta 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

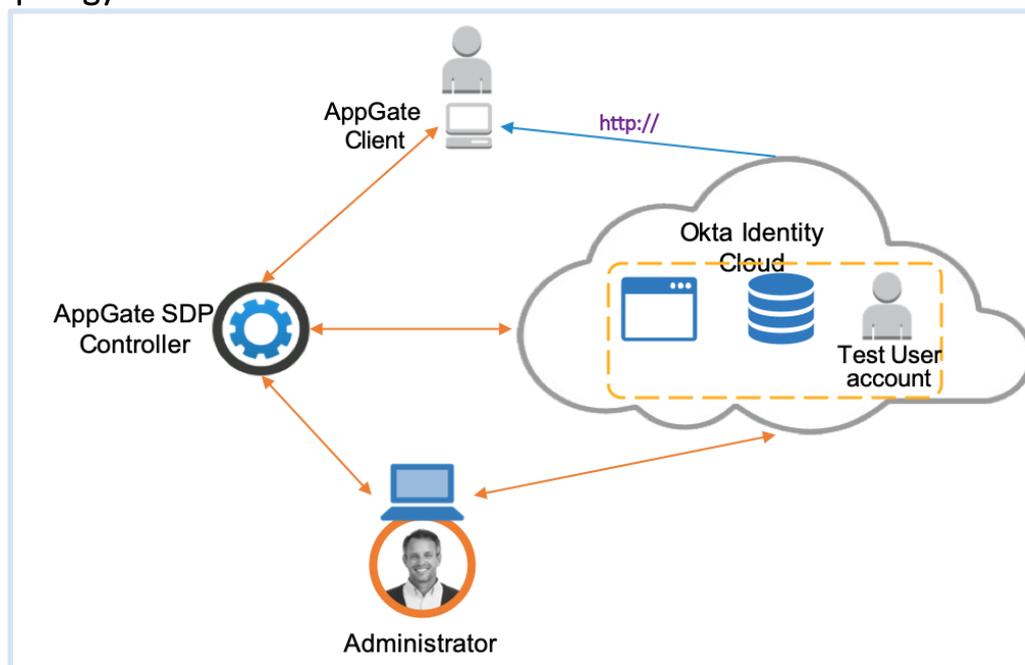


Figure 1: Okta integration test topology

This integration process requires the following:

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

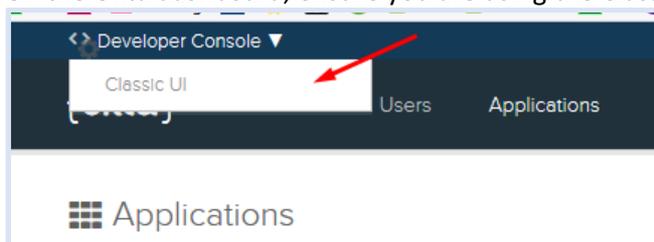
STEP BY STEP GUIDE TO INTEGRATION

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

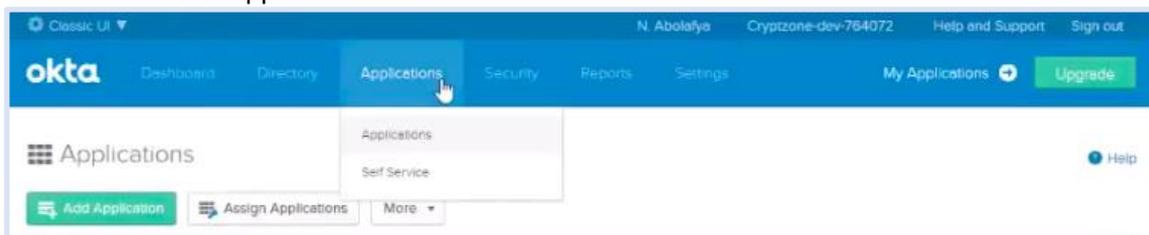
1. OKTA CONFIGURATION: SET UP SINGLE SIGN-ON

Add a new application

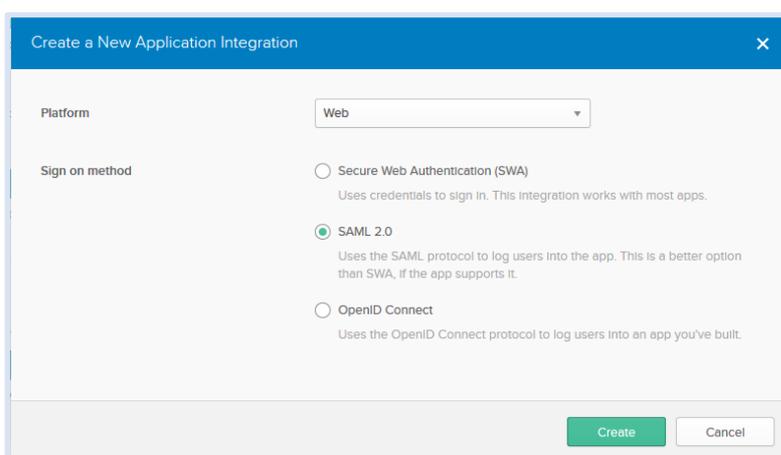
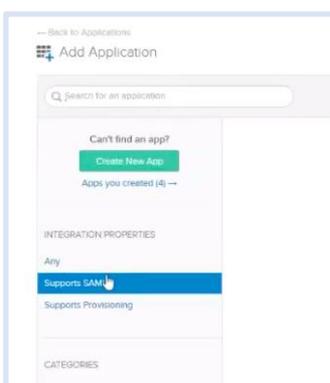
- Log in to your Okta administrator account.
- On the Okta dashboard, ensure you are using the Classic UI, not the Developer Console



- On the <Applications> screen click <Add Application>
- On the left hand menu: click INTEGRATION PROPERTIES -> Supports SAML
- Click <Create New App>



- On the Create a New Application console, click <SAML 2.0>
- Click <Create>



- On the *Create SAML Integration* console type in an app name, eg:
 - For **Administrator Authentication**: "AppGate SDP"
 - For **User Authentication**: "AppGate SDP Client App"
- Click <Next>

Application Configuration – GENERAL

- In the GENERAL section enter the basic *SAML Settings*:
 - *Single Sign-On URL*: – Type in the appropriate ACS URL, refer to the table below
 - *Audience URI* – Type in a unique name, make a note of this as it needs to match the *Audience* field when you configure AppGate SDP

Administrator Authentication:	User Authentication:
Single sign-on URL = ACS URL = AppGate SDP Controller URL https://mycontroller.mycompany.com:444/admin/saml	Single sign-on URL = ACS URL = localhost redirection server URL http://127.0.0.1:29001/saml

The GENERAL section should look something like this:

The screenshot shows the 'GENERAL' configuration page for an application. It includes the following fields and options:

- Single sign on URL**: Text input field containing 'http://127.0.0.1:29001/saml'. Below it are two checkboxes: 'Use this for Recipient URL and Destination URL' (checked) and 'Allow this app to request other SSO URLs' (unchecked).
- Audience URI (SP Entity ID)**: Text input field containing 'appgate-test'.
- Default RelayState**: Text input field (empty). Below it is a note: 'If no value is set, a blank RelayState is sent'.
- Name ID format**: Dropdown menu set to 'EmailAddress'.
- Application username**: Dropdown menu set to 'Okta username prefix'.
- Update application username on**: Dropdown menu set to 'Create and update'.

A 'Show Advanced Settings' link is located at the bottom right of the configuration area.

Attribute Mapping – ATTRIBUTE STATEMENTS

- 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. Attribute <Name> *username* is mapped to <Value> *user.login*
- Make a note of the Attribute names you have created, you will need them when configuring your AppGate SDP

The ATTRIBUTES section should look something like this:

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value	
username	Unspecified ▼	user.login ▼	
firstName	Unspecified ▼	user.firstName ▼	×
lastName	Unspecified ▼	user.lastName ▼	×
emails	Unspecified ▼	user.email ▼	×

[Add Another](#)

GROUP ATTRIBUTE STATEMENTS

- If your organization uses groups, use this option to return groups in the SAML assertion
- To filter all groups into a single SAML assertion:
- In the Filter field, select <Matches regex> and type in .*

The GROUP ATTRIBUTE STATEMENTS section should look exactly like this:

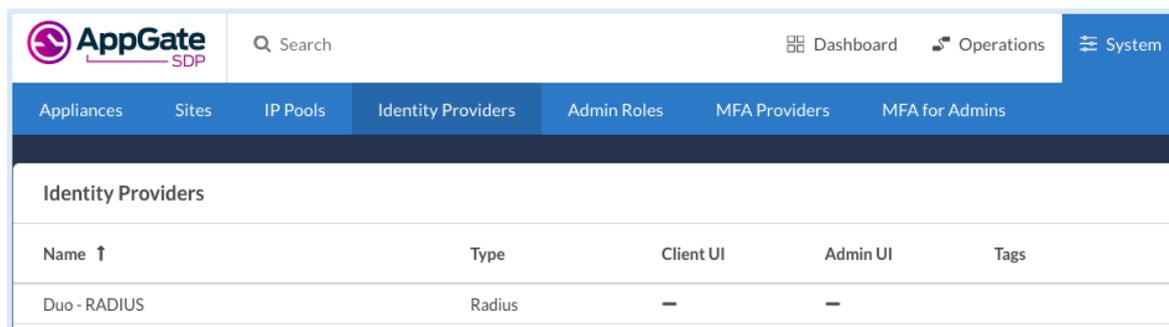
GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
groups	Unspecified ▼	Matches regex ▼ .*

[Add Another](#)

- Click <Next>
- Click <Finish>

3. 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:
<i>Name</i>	Enter a unique name eg: "Okta SAML Admin"	Enter a unique name eg: "Okta SAML User"
<i>IPv4Pool</i>	select default pool v4	select default pool v4
<i>Where to use</i>	tick "Use for Admin UI sign in"	(Will be specified in the profile link)
<i>Single Sign-on URL</i>	<i>See below</i>	
<i>Issuer</i>	<i>See below</i>	
<i>Audience</i>	type in the Audience URI you entered on the Okta configuration	
<i>Public Certificate</i>	<i>See below</i>	

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 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:

<i>Single Sign-on URL</i>	type in the Identity Provider Single Sign-ON URL
<i>Issuer</i>	type in the Identity Provider Issuer
<i>Public Certificate</i>	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 Okta:

Your Identity Provider form should look something like this:

Use XML Metadata file

okta-metadata.xml

Single Sign-On URL

 Will be automatically filled in by XML Metadata file above

Issuer

 Will be automatically filled in by XML Metadata file above

Audience

Public Certificate

-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAV250bv+MA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCMRldi03NjQwNzlxHDAaBgkqhkiG9w0BCQEWLWluZm9Ab2t0YS5jb20wHhcNMTCw

 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

Attribute Claim name Array Encrypted ✓ ✕ + Add new

- Map the *Attributes* that were created in the Okta configuration to AppGate SDP User Claims.
- The Okta *Attribute Names* 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.
- If you use Groups, Map the *Group Attribute Name* to <**Claim name**> *Groups* and tick the *array* box
- Click <**Save**>

Map Attributes to User Claims

Attribute Claim name

ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)
username	Unspecified
firstName	Unspecified
lastName	Unspecified
emails	Unspecified

Your completed attribute list should look something like this:

Map Attributes to User Claims

+ Add new

- groups mapped to claim groups (array)
- 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:
<p>On your AppGate SDP admin UI:</p> <ul style="list-style-type: none"> • Sign out of the admin UI • Log in using the following information: <i>Identity Provider</i> – 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: <i>“You don’t have any administration rights”</i> – this confirms that the test user credentials have been successfully authenticated by your Identity Provider. 	<p>On the AppGate SDP Client:</p> <ul style="list-style-type: none"> • 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.

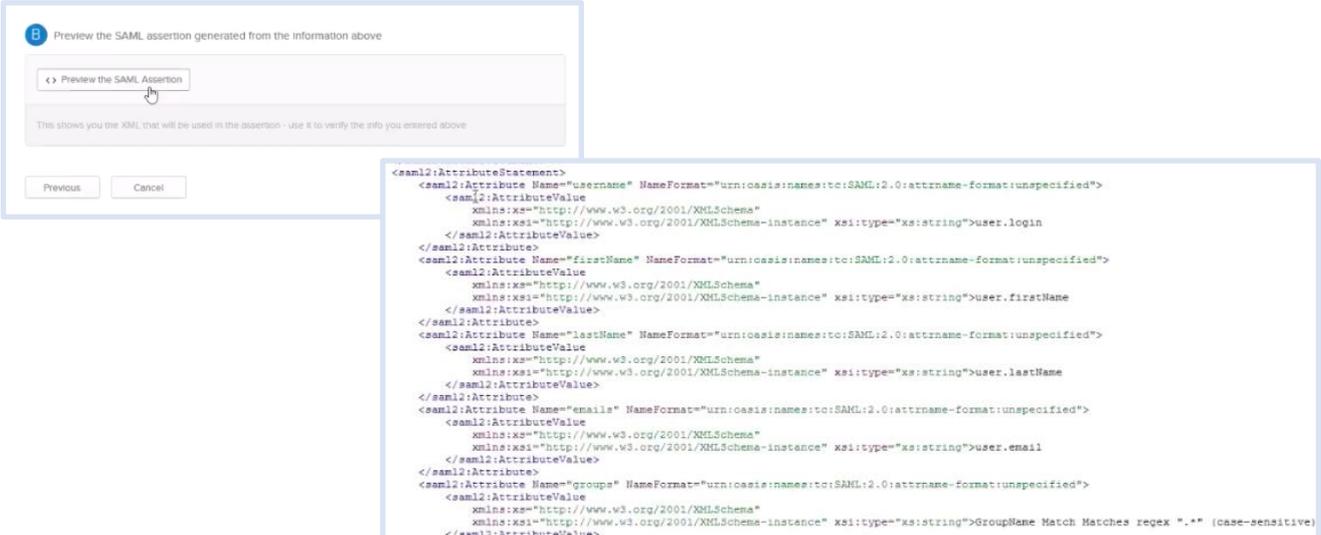
TROUBLESHOOTING

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 Okta configuration.

You can use the *Preview* function in your Okta configuration to check the SAML XML that your IdP will be generating:

- On your Okta console: open the *GENERAL SETTINGS* form for your AppGate SDP application
- Below the *Attributes* section, click on the <Preview SAML Assertion> button to view the XML



Preview the SAML assertion generated from the information above

<> Preview the SAML Assertion

This shows you the XML that will be used in the assertion – use it to verify the info you entered above

Previous Cancel

```

<saml2:AttributeStatement>
  <saml2:Attribute Name="username" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue>
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns: xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">user.login
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="firstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue>
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns: xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">user.firstName
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="lastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue>
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns: xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">user.lastName
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="emails" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue>
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns: xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">user.email
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="groups" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue>
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns: xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">GroupName Match Matches regex *.* (case-sensitive)
    </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>

```

Alternatively, on your AppGate SDP LogServer, 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](#).