# RSA SECURID® ACCESS
# Implementation Guide

## OpenDataSoft

Gina Salvalzo, RSA Partner Engineering
Last Modified: September 05, 2017

## Solution Summary

OpenDataSoft is a private software company specialized in transforming structured data into API and visualizations. This integration supports both IdP and SP initiated authentication flows.

| RSA SecurID Access Features | |
|---|---|
| **OpenDataSoft** | |
| **On Premise Methods** | |
| RSA SecurID | ✓ |
| On Demand Authentication | ✓ |
| Risk-Based Authentication (AM) | - |
| **Cloud Authentication Service Methods** | |
| Authenticate App | ✓ |
| FIDO Token | ✓ |
| **SSO** | |
| SAML SSO | ✓ |
| HFED SSO | - |

| Identity Assurance | |
|---|---|
| Collect Device Assurance and User Behavior | ✓ |

## Configuration Summary

All of the supported use cases of RSA SecurID Access with OpenDataSoft require both server-side and client-side configuration changes.  This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

**RSA Cloud Authentication Service** – OpenDataSoft can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

**Cloud Authentication Service – Identity Router IdP Configuration**
**OpenDataSoft SAML Configuration**

# RSA SecurID Access Server Side Configuration

## *RSA Cloud Authentication Service Configuration*

### SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for OpenDataSoft in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

#### Configure RSA Identity Router SAML IdP

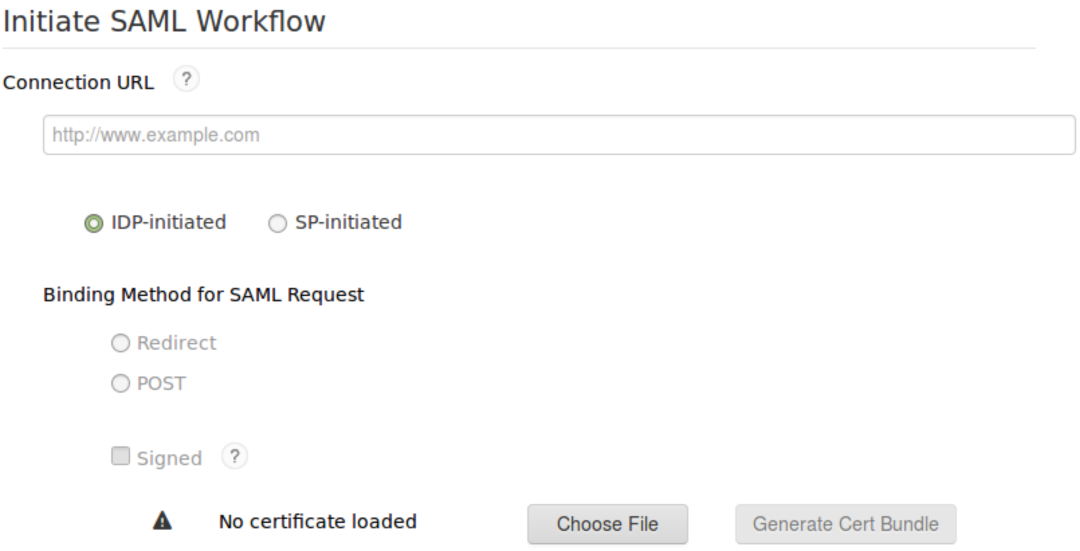
**Procedure**

1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for OpenDataSoft and click **+Add** to add the connector.

OpenDataSoft
SAML Direct

2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

> **Note:** The following IdP-initiated configuration works for SP-initiated OpenDataSoft connections as well.



Initiate SAML Workflow

Connection URL: http://www.example.com

● IDP-initiated ○ SP-initiated

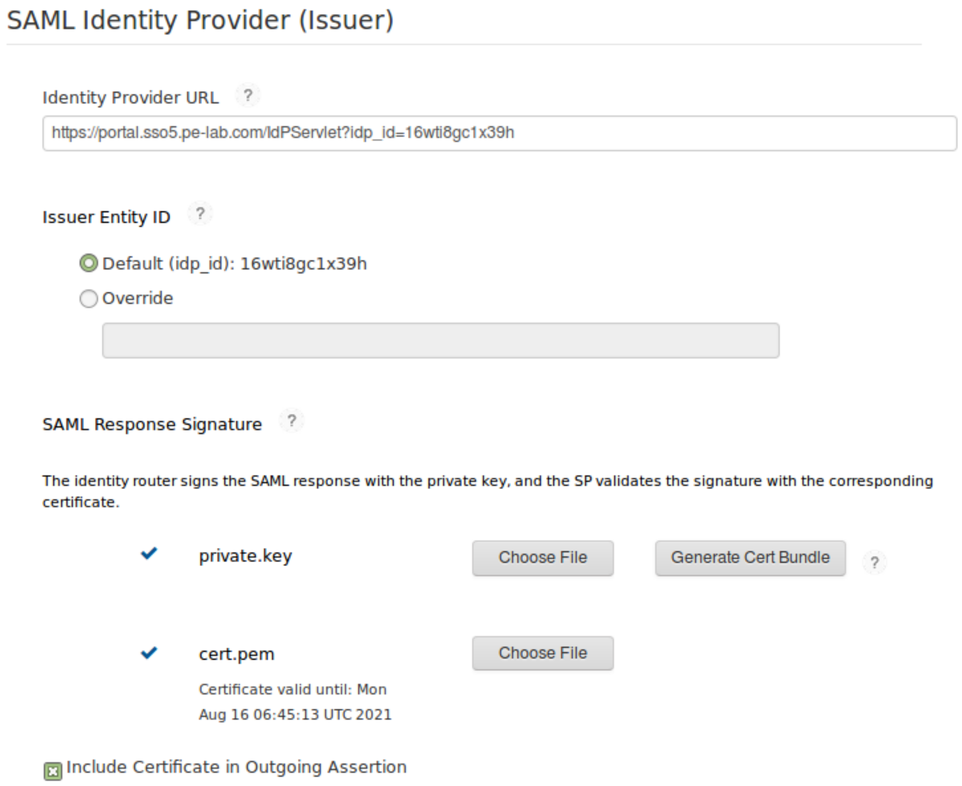
Binding Method for SAML Request

○ Redirect
○ POST

□ Signed

No certificate loaded

4. Scroll down to SAML Identity Provider (Issuer) section.



SAML Identity Provider (Issuer)

Identity Provider URL ?

https://portal.sso5.pe-lab.com/IdPServlet?idp_id=16wti8gc1x39h

Issuer Entity ID ?

● Default (idp_id): 16wti8gc1x39h

○ Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

✓ private.key

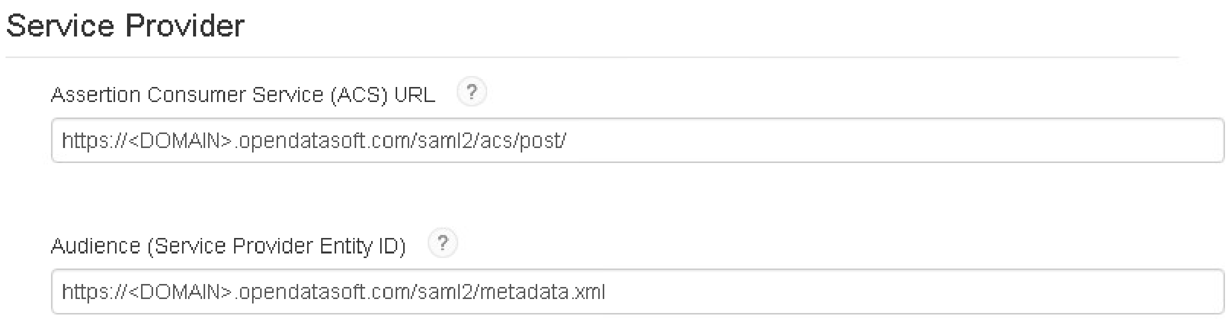
✓ cert.pem

Certificate valid until: Mon Aug 16 06:45:13 UTC 2021

☒ Include Certificate in Outgoing Assertion

a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

5. Scroll down to the **Service Provider** section.



Service Provider

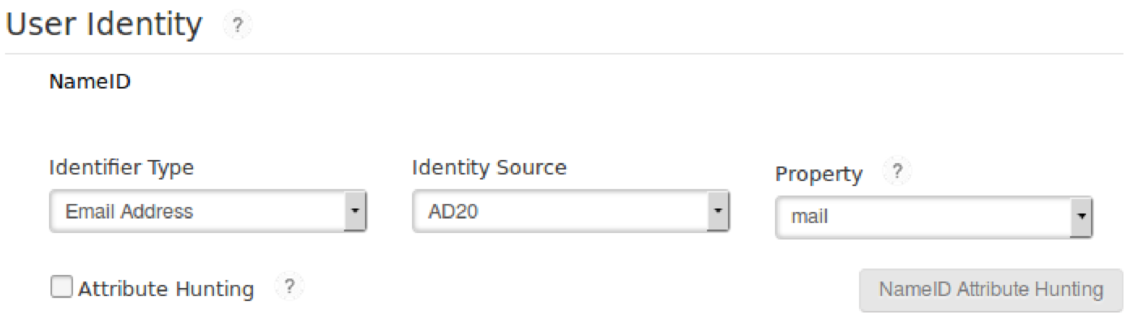
Assertion Consumer Service (ACS) URL ?

https://<DOMAIN>.opendatasoft.com/saml2/acs/post/

Audience (Service Provider Entity ID) ?

https://<DOMAIN>.opendatasoft.com/saml2/metadata.xml

6. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your account specific domain.
7. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> with your account specific domain.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



User Identity ?

NameID

Identifier Type: Email Address

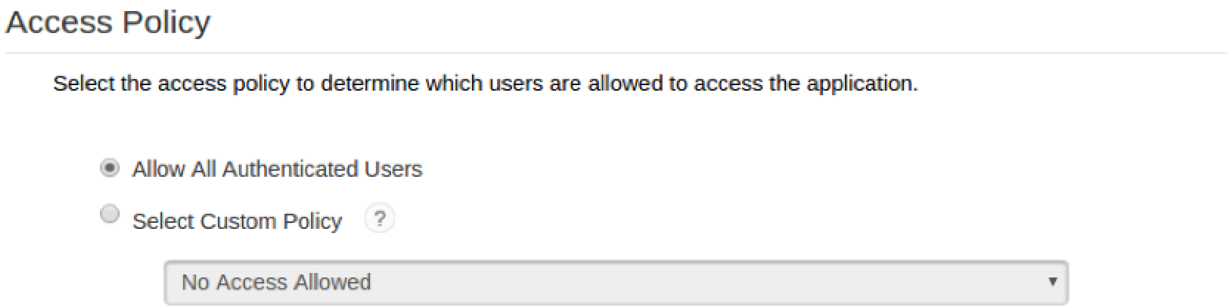
Identity Source: AD20

Property ?: mail

□ Attribute Hunting ?

9. Click **Next Step**.

10. On the User Access page, select **Allow All Authenticated Users** user policy from the available options.



Access Policy

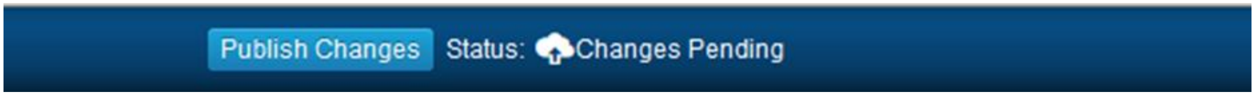
Select the access policy to determine which users are allowed to access the application.

● Allow All Authenticated Users

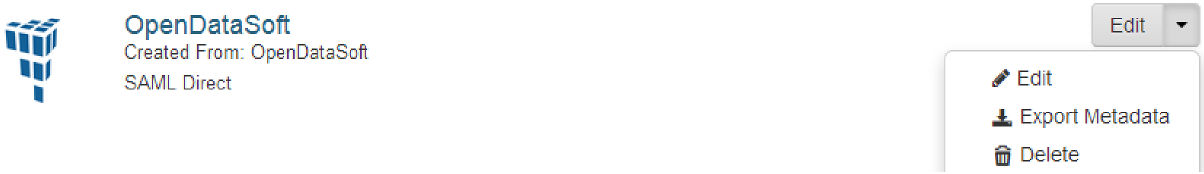
○ Select Custom Policy ?

No Access Allowed ▾

11. Click **Next Step**.
12. On the **Portal Display** page, select **Display in Portal**.
13. Click **Save and Finish**.
14. Click **Publish Changes**. Your application is now enabled for SSO.



15. Navigate to **Applications** > **My Applications**.
16. Locate **OpenDataSoft** in the list and from the **Edit** option, select **Export Metadata**.



OpenDataSoft
Created From: OpenDataSoft
SAML Direct

# Partner Product Configuration

## *Before You Begin*

This section provides instructions for configuring the OpenDataSoft with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

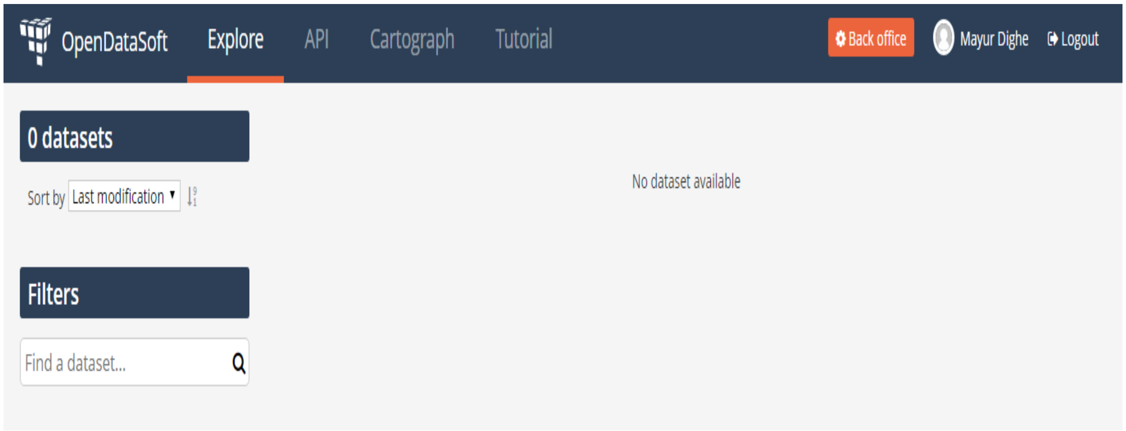
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All OpenDataSoft components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

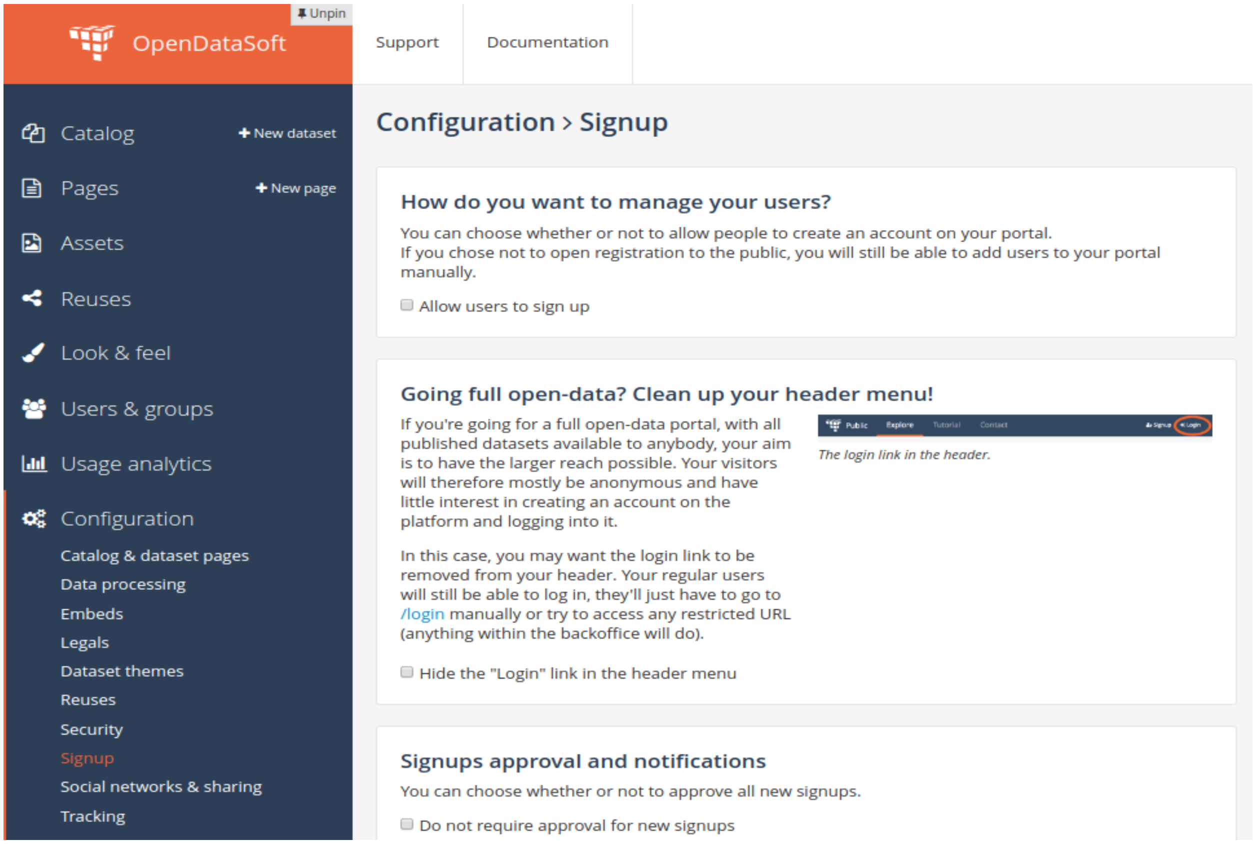
### OpenDataSoft SAML Configuration

**Procedure**

1. Login to your OpenDataSoft application web account.
   https://<your_domain>.opendatasoft.com/login/
2. An Admin user can configure it to authenticate team members using company's SAML server. To enable SAML authentication click **Back Office** tab.



3. Navigate to the **Signup** page in the domain Configuration interface.



Configuration > Signup

**How do you want to manage your users?**

You can choose whether or not to allow people to create an account on your portal.
If you chose not to open registration to the public, you will still be able to add users to your portal manually.

□ Allow users to sign up

**Going full open-data? Clean up your header menu!**

If you're going for a full open-data portal, with all published datasets available to anybody, your aim is to have the larger reach possible. Your visitors will therefore mostly be anonymous and have little interest in creating an account on the platform and logging into it.

In this case, you may want the login link to be removed from your header. Your regular users will still be able to log in, they'll just have to go to /login manually or try to access any restricted URL (anything within the backoffice will do).

*The login link in the header.*

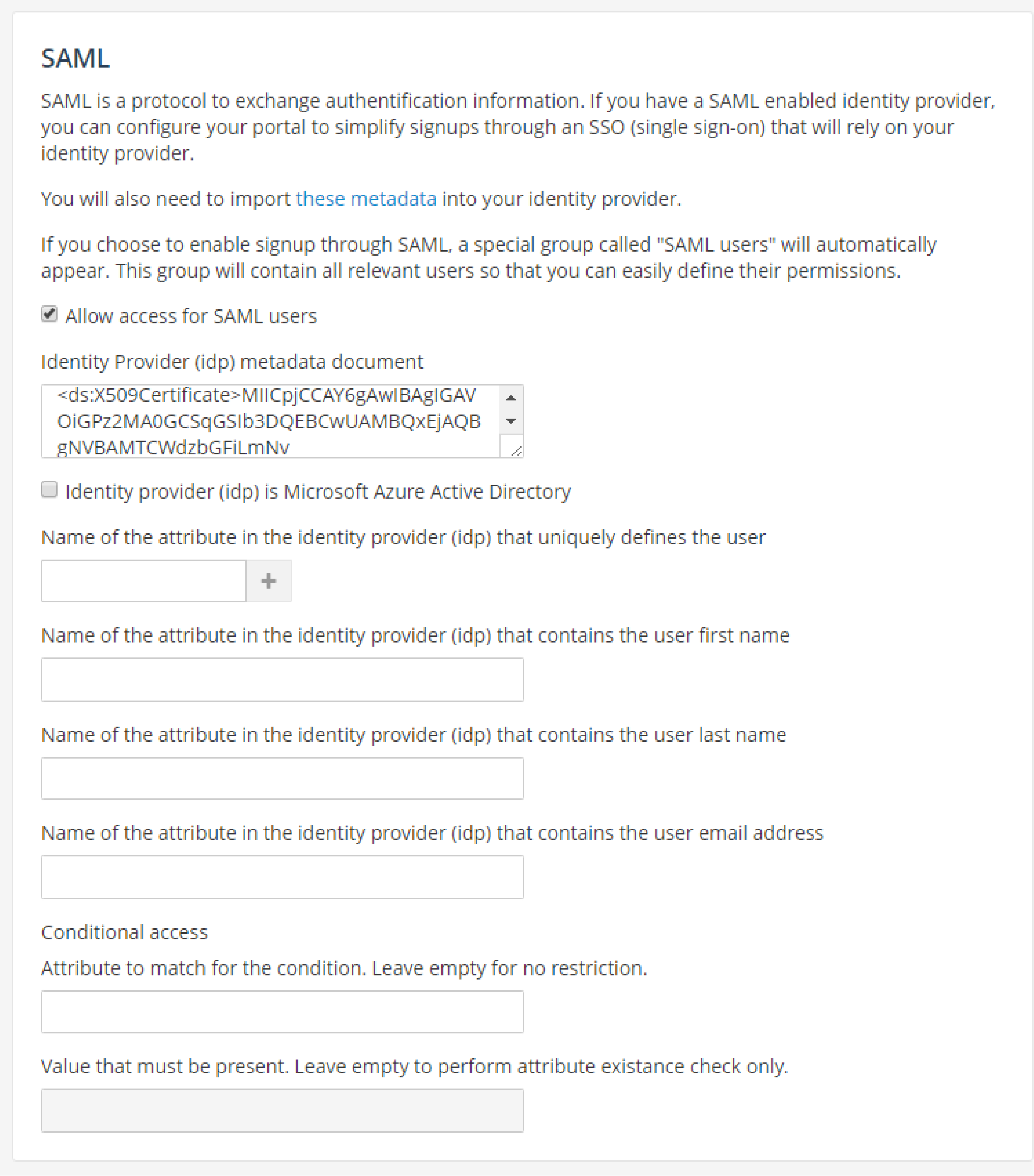
□ Hide the "Login" link in the header menu

**Signups approval and notifications**

You can choose whether or not to approve all new signups.

□ Do not require approval for new signups

4. Following UI will be displayed. Check **Allow access for SAML users**.
5. Paste your **metadata document** in the "IDP metadata document" field which you copied earlier.
6. Keep all other fields empty as they are.
7. Click on **Save** in the upper right corner.



SAML

SAML is a protocol to exchange authentification information. If you have a SAML enabled identity provider, you can configure your portal to simplify signups through an SSO (single sign-on) that will rely on your identity provider.

You will also need to import these metadata into your identity provider.

If you choose to enable signup through SAML, a special group called "SAML users" will automatically appear. This group will contain all relevant users so that you can easily define their permissions.

☑ Allow access for SAML users

Identity Provider (idp) metadata document

```
<ds:X509Certificate>MIICpjCCAY6gAwIBAgIGAV
OiGPz2MA0GCSqGSIb3DQEBCwUAMBQxEjAQB
gNVBAMTCWdzbGFiLmNv
```

☐ Identity provider (idp) is Microsoft Azure Active Directory

Name of the attribute in the identity provider (idp) that uniquely defines the user

Name of the attribute in the identity provider (idp) that contains the user first name

Name of the attribute in the identity provider (idp) that contains the user last name

Name of the attribute in the identity provider (idp) that contains the user email address

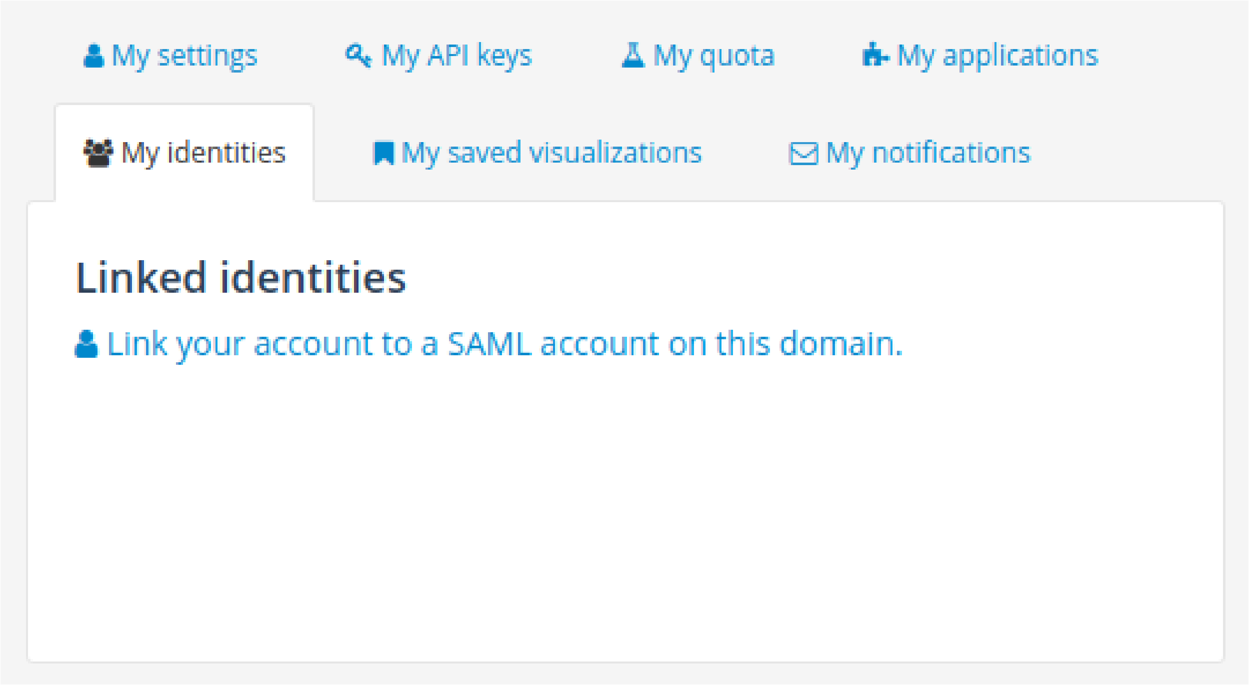
Conditional access

Attribute to match for the condition. Leave empty for no restriction.

Value that must be present. Leave empty to perform attribute existance check only.

**Linked mode**

a. After completing above steps navigate to **Account** section, click **My identities**.
b. Users have to do this step manually after Admin sets company's SAML server.
c. In the linked mode, users that have an OpenDataSoft user account can link this account to particular values of the set of parameters defined in the account mapper setting. After the link has been established, users who log in through SAML will be logged to their OpenDataSoft user account.



Linked identities

Link your account to a SAML account on this domain.