# Single Sign-On Setup Examples for Common Identity Providers

For administrators setting up Single Sign-On in the ZoomInfo platform with common identity providers

This document describes how to configure Single Sign-On (SSO) for ZoomInfo and provides examples of how to enable certificate management for common Identity Providers (IdPs).

ZoomInfo SSO can be configured with other IdPs not covered in this document. You can utilize this information to help understand similar configurations for these additional IdPs to complete your SSO configuration.

Contact ZoomInfo Support if you need additional assistance in setting up SSO for your organization.

# ZoomInfo Admin Portal Configuration

For each IdP described in this document, you will perform some configuration in the IdP application (e.g., Okta, OneLogin, and so on), and some configuration in the ZoomInfo Admin Portal. Ensure that you have appropriate access to both platforms.

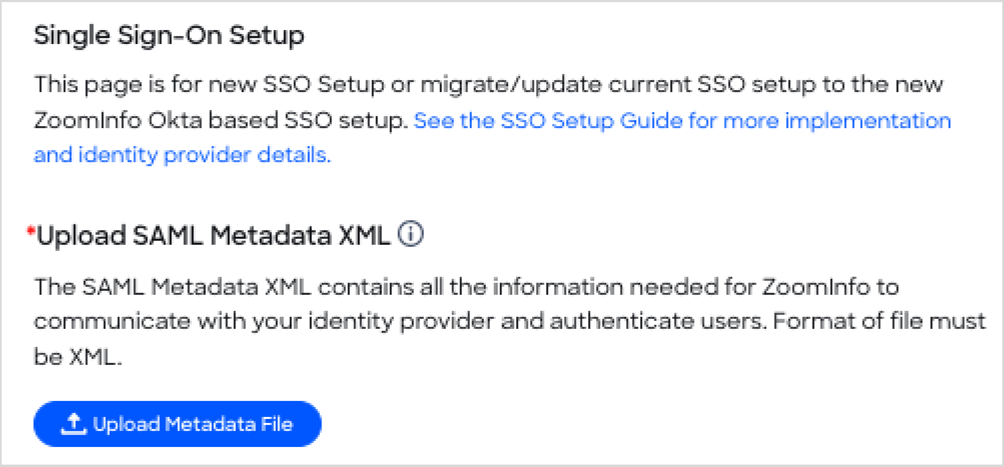
## SSO Configuration Page

To access the SSO configuration page in ZoomInfo:

1. Log in to ZoomInfo as an admin.
2. Go to the Zoominfo Admin Portal.
3. Click **Company Settings > Single Sign-On**.

## SAML Metadata XML

The ZoomInfo Single Sign-On Setup page displays. Here you will upload an XML metadata file that is created from your IdP configuration.



Single Sign-On Setup

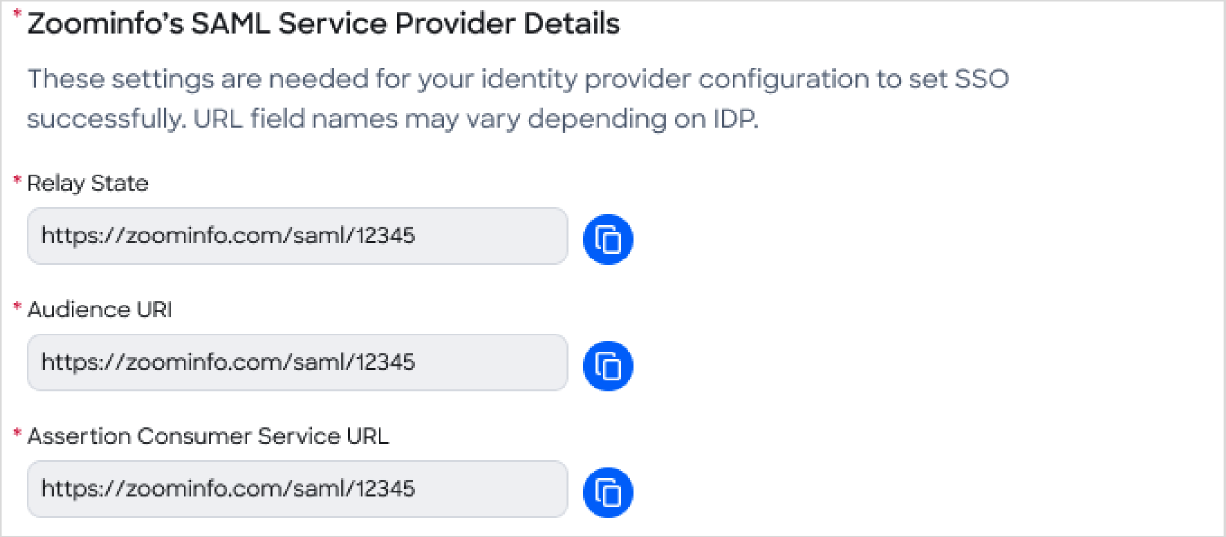
This page is for new SSO Setup or migrate/update current SSO setup to the new ZoomInfo Okta based SSO setup. See the SSO Setup Guide for more implementation and identity provider details.

*Upload SAML Metadata XML ⓘ

The SAML Metadata XML contains all the information needed for ZoomInfo to communicate with your identity provider and authenticate users. Format of file must be XML.

## Service Provider Details

In the **ZoomInfo's SAML Service Provider Details** section, you will copy some values back to your IdP.



* Zoominfo's SAML Service Provider Details

These settings are needed for your identity provider configuration to set SSO successfully. URL field names may vary depending on IDP.

* Relay State

https://zoominfo.com/saml/12345

* Audience URI

https://zoominfo.com/saml/12345

* Assertion Consumer Service URL

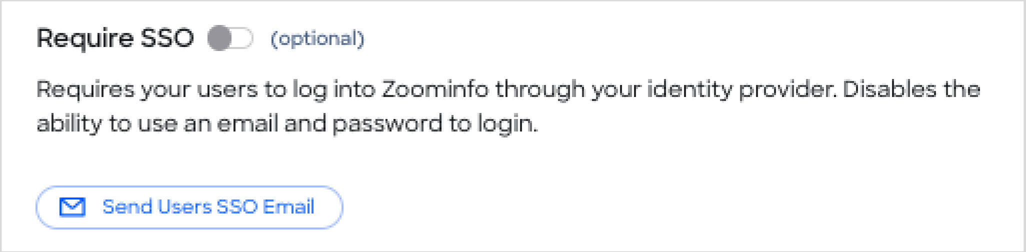
https://zoominfo.com/saml/12345

See the procedure for each IdP for details on completing this configuration.

## Require SSO and SSO Login Toggles

Once your configuration is complete, you can make some choices about requiring SSO and allowing or disabling social logins.

If you choose to only allow your users to log in using ZoomInfo through your SSO identity provider, enable the **Require SSO** toggle. Click **Send Users SSO Email** to generate an email for them to establish their SSO login.

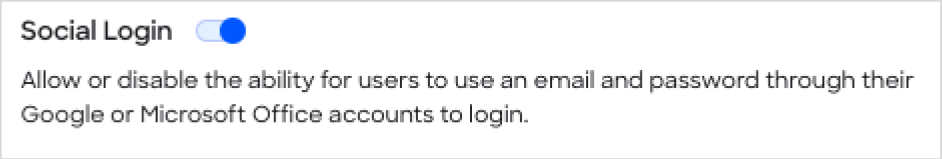


Require SSO (optional)

Requires your users to log into Zoominfo through your identity provider. Disables the ability to use an email and password to login.

Send Users SSO Email

You can also choose to allow or disable the ability for users to use an email and password through their Google or Microsoft Office accounts to log in.



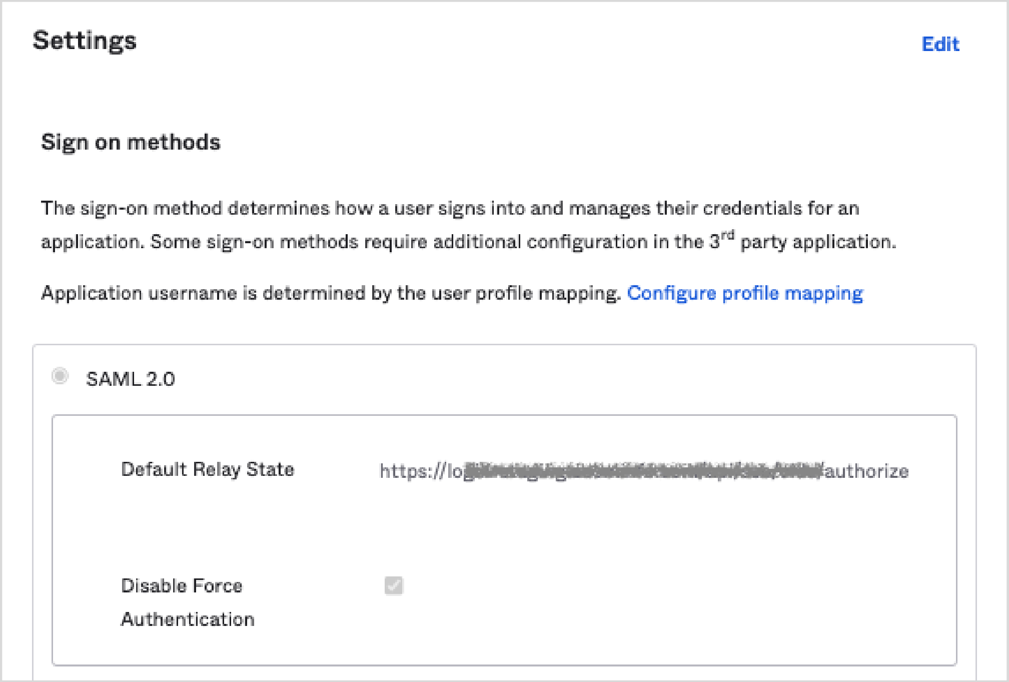
Social Login

Allow or disable the ability for users to use an email and password through their Google or Microsoft Office accounts to login.

# Okta Configuration

The ZoomInfo app is available as an application integration in Okta. This section describes how to add the app and configure it to support SAML 2.0 Single Sign On.

1. In the Okta Admin app, go to **Applications > Applications**.
2. Click **Browse App Catalog** and search for *ZoomInfo*.
3. Select **Add** to add the ZoomInfo app to Okta.
4. In the Okta ZoomInfo app, complete the fields on the **General** page with your new **Application label** and click **Next**.
5. In the **Settings** section of the **Sign On** tab, select **SAML 2.0** as your sign on method.



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

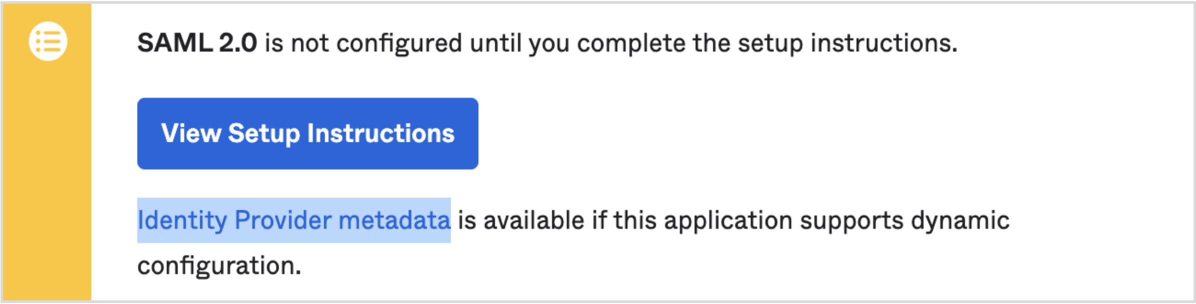
Application username is determined by the user profile mapping. Configure profile mapping

● SAML 2.0

Default Relay State https://lo[redacted]authorize

Disable Force Authentication ☑

6. Scroll down to this section.



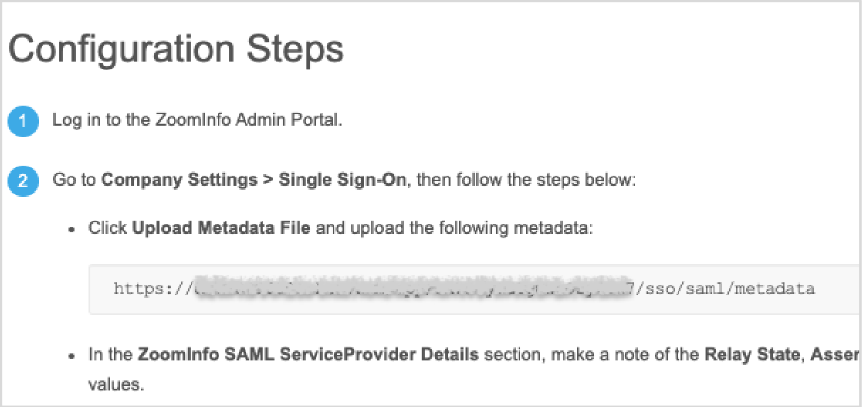
**SAML 2.0** is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

From here, you have two ways to obtain your IdP Metadata and save it to an XML file:

**Option 1: View Setup Instructions link**

Click **View Setup Instructions** and copy the link provided in the **Configuration Steps** section.



## Configuration Steps

1 Log in to the ZoomInfo Admin Portal.

2 Go to **Company Settings > Single Sign-On**, then follow the steps below:

- Click **Upload Metadata File** and upload the following metadata:

```
https://[redacted]7/sso/saml/metadata
```

- In the **ZoomInfo SAML ServiceProvider Details** section, make a note of the **Relay State**, **Asser** values.

Open a new tab in your browser, paste the link, and press **Enter**.

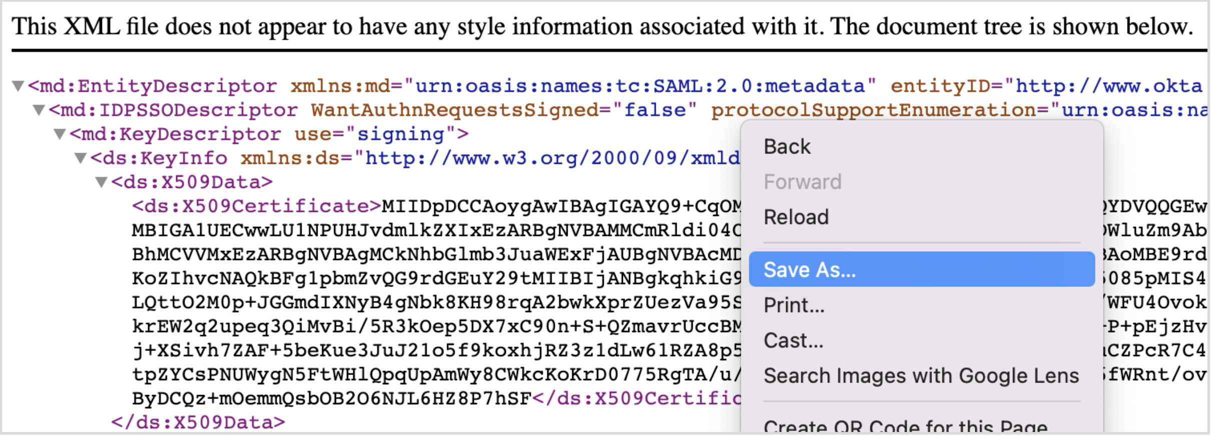
Go to step 7.

**Option 2: Identity Provider metadata link**

Click the **Identity Provider metadata** link to launch a new window that displays the XML.

Go to step 7.

7. Right click the XML text and save the content to an XML file.

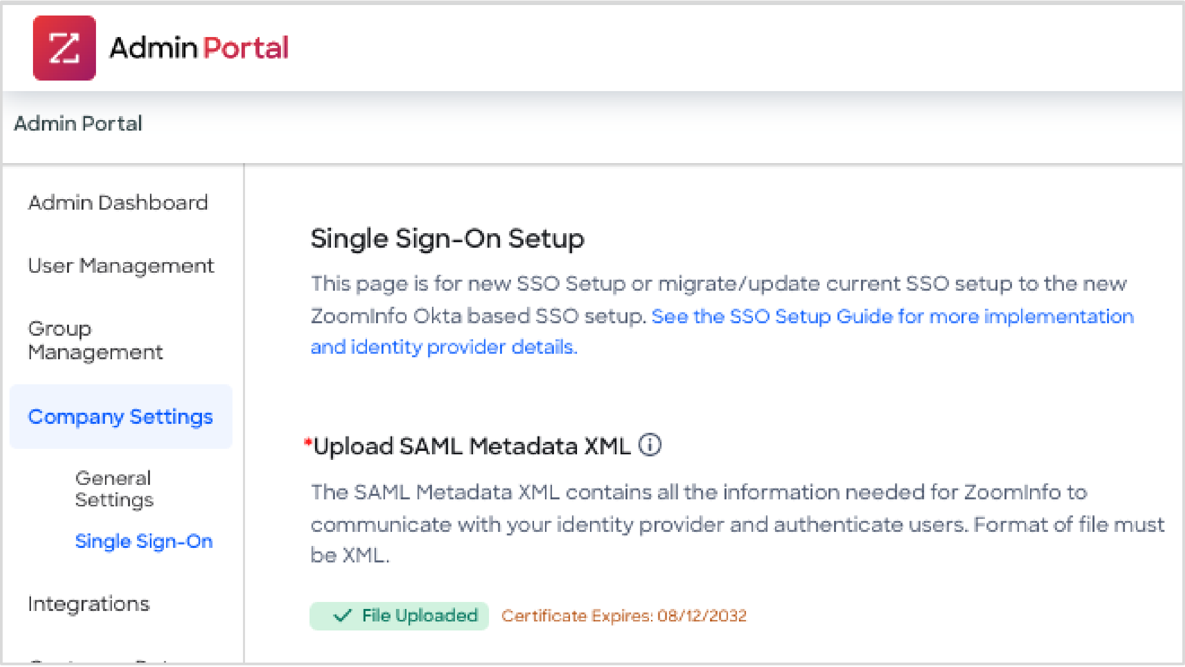


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://www.okta
  ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:na
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmld
        ▼<ds:X509Data>
            <ds:X509Certificate>MIIDpDCCAoygAwIBAgIGAYQ9+CqOM                    QYDVQQGEw
            MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCmRldi04C                    DWluZm9Ab
            BhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMD                    3AoMBE9rd
            KoZIhvcNAQkBFglpbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9                    5085pMIS4
            LQttO2M0p+JGGmdIXNyB4gNbk8KH98rqA2bwkXprZUezVa95S                    /WFU4Ovok
            krEW2q2upeq3QiMvBi/5R3kOep5DX7xC90n+S+QZmavrUccBM                    +P+pEjzHv
            j+XSivh7ZAF+5beKue3JuJ21o5f9koxhjRZ3z1dLw61RZA8p5                    aCZPcR7C4
            tpZYCsPNUWygN5FtWHlQpqUpAmWy8CWkcKoKrD0775RgTA/u/                    5fWRnt/ov
            ByDCQz+mOemmQsbOB2O6NJL6HZ8P7hSF</ds:X509Certific
        </ds:X509Data>
```

8. Return to the ZoomInfo Admin Portal and go to **Company Settings > Single Sign-On**.

9. Click **Upload Metadata File** and choose the XML file you saved from Okta.



Single Sign-On Setup

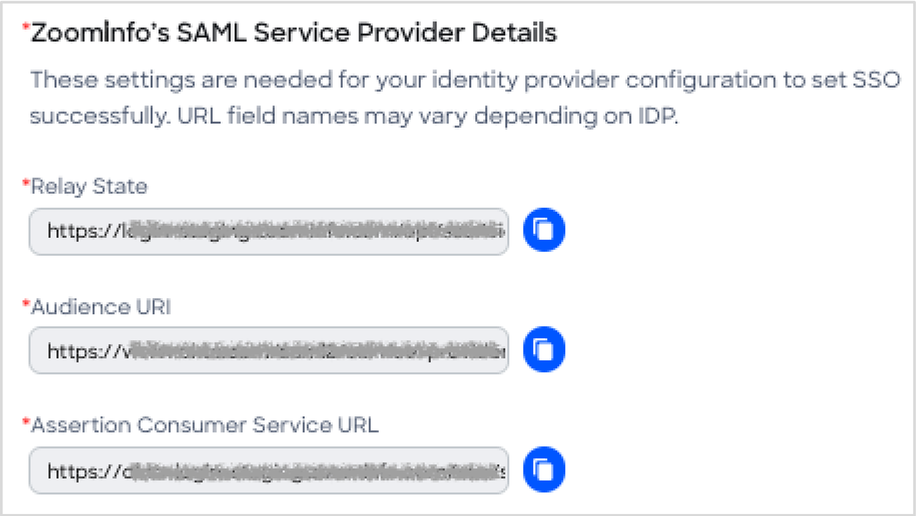
This page is for new SSO Setup or migrate/update current SSO setup to the new ZoomInfo Okta based SSO setup. See the SSO Setup Guide for more implementation and identity provider details.

*Upload SAML Metadata XML ⓘ

The SAML Metadata XML contains all the information needed for ZoomInfo to communicate with your identity provider and authenticate users. Format of file must be XML.

✓ File Uploaded Certificate Expires: 08/12/2032

Three URLs are displayed in the **ZoomInfo SAML Service Provider Details** section.



*ZoomInfo's SAML Service Provider Details

These settings are needed for your identity provider configuration to set SSO successfully. URL field names may vary depending on IDP.

*Relay State

https://l[redacted]

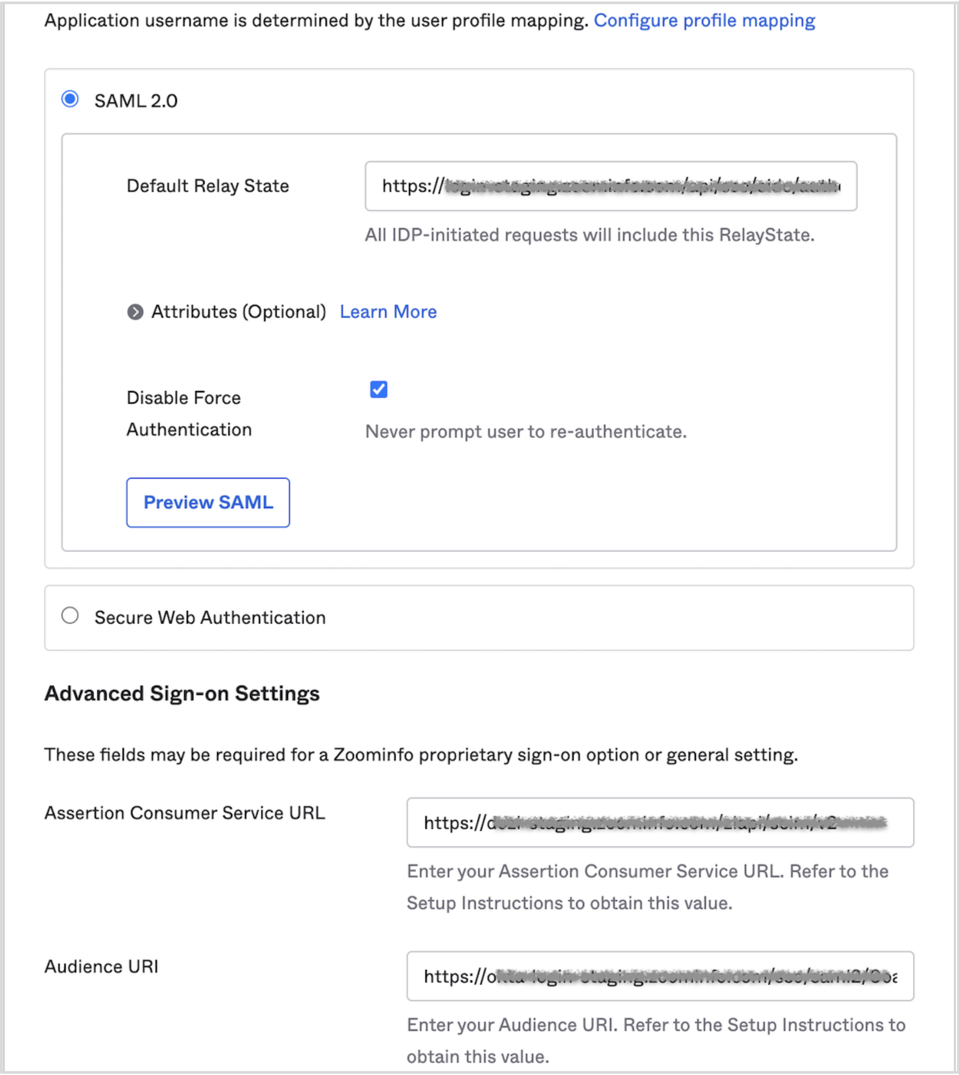
*Audience URI

https://v[redacted]

*Assertion Consumer Service URL

https://c[redacted]

10. Return to the Okta admin portal and on the **Sign On** tab, copy each URL from the ZoomInfo Admin Portal and paste it to the corresponding field.



Application username is determined by the user profile mapping. Configure profile mapping

● SAML 2.0

Default Relay State: https://[redacted]

All IDP-initiated requests will include this RelayState.

Disable Force Authentication: ☑

Never prompt user to re-authenticate.

○ Secure Web Authentication

**Advanced Sign-on Settings**

These fields may be required for a Zoominfo proprietary sign-on option or general setting.

Assertion Consumer Service URL: https://[redacted]

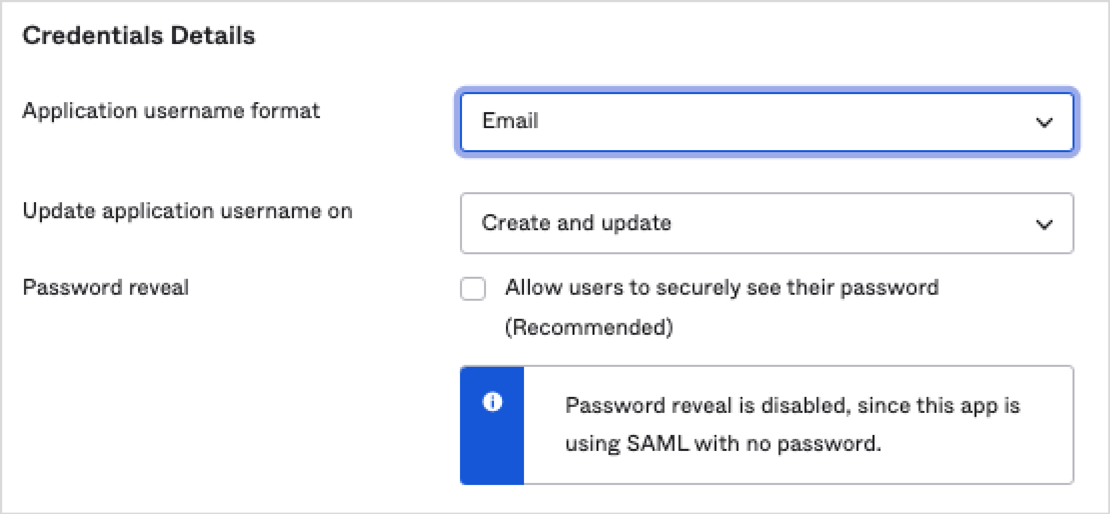
Enter your Assertion Consumer Service URL. Refer to the Setup Instructions to obtain this value.

Audience URI: https://[redacted]

Enter your Audience URI. Refer to the Setup Instructions to obtain this value.

| Copy from ZoomInfo Admin Portal | Paste in Okta |
|---|---|
| Relay State | Default Relay State |
| Assertion Consumer Service URL | Assertion Consumer Service URL |
| Audience URI | Audience URI |

11. In the **Credentials Details** section, select **Email** for the **Application username format**.



Credentials Details

Application username format: Email

Update application username on: Create and update

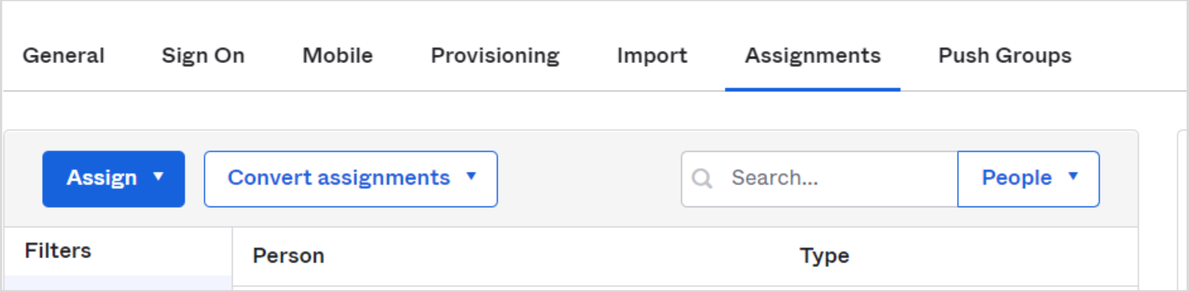
Password reveal: □ Allow users to securely see their password (Recommended)

Password reveal is disabled, since this app is using SAML with no password.

12. Click **Done**.

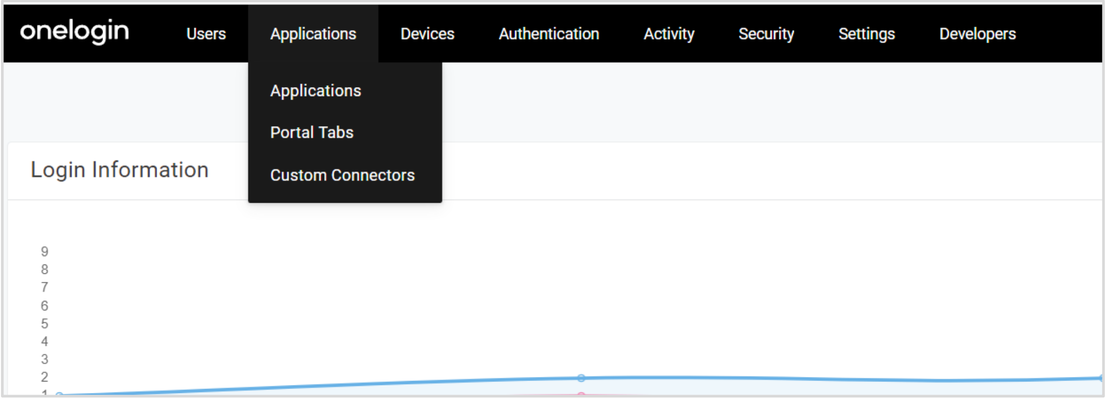
13. Go to the **Assignments** tab In the application you just created in Okta.

14. Assign a group or users that you want to use SSO.



# OneLogin Configuration

1. Log into your OneLogin Admin Portal.
2. Go to **Applications**.



3. Click **Add App**.

1. Select the SAML 2.0 app you want to use to add SAML. For example, SAML Custom Connector (Advanced).
2. Go to the **SSO** tab and ensure that your **SAML Signature Algorithm** is SHA-256.
3. Copy the **Issuer URL** to a different tab and download the metadata XML file.
4. In ZoomInfo, go to **Admin Portal** > **Company Settings** > **Single Sign-On**, click **Upload Metadata File** and choose the XML file you saved from OneLogin.
5. From the ZoomInfo Admin Portal **Single Sign-On Setup** page:
    a. Copy the **Relay State** URL from the Zoominfo Admin Portal to **RelayState** in the OneLogin Admin Portal **Configuration** tab.

    b. Copy the **Audience** URI from the ZoomInfo Admin Portal to **Audience (EntityID)** in OneLogin.

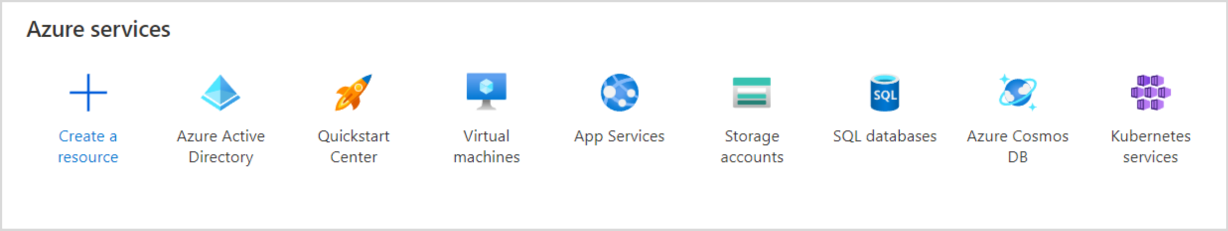
    c. Copy **Assertion Consumer Service URL** from the ZoomInfo Admin Portal to **ACS (Consumer) URL** and **Recipient** in OneLogin.

    d. Copy the following to **ACS (Consumer) URL Validator** in OneLogin:

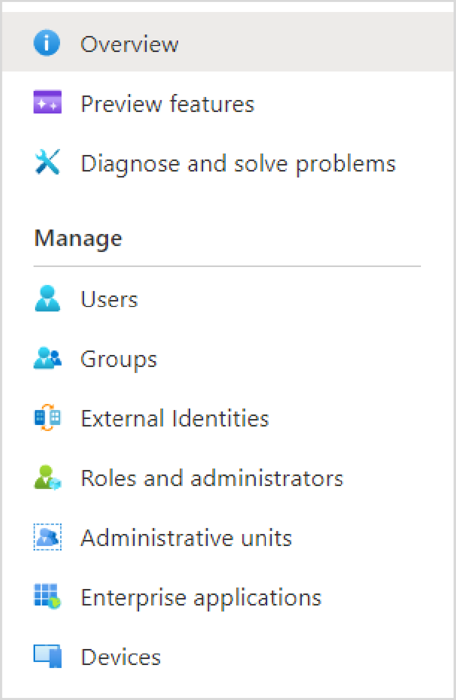
    ```
    [-a-zA-Z0-9@:%._\+~#=]{2,256}\.[a-z]{2,6}\b([-a-zA-Z0-9@:%_\+.~#?&//=]*)
    ```
6. Assign users that you want to use SAML.

# Microsoft Azure Configuration

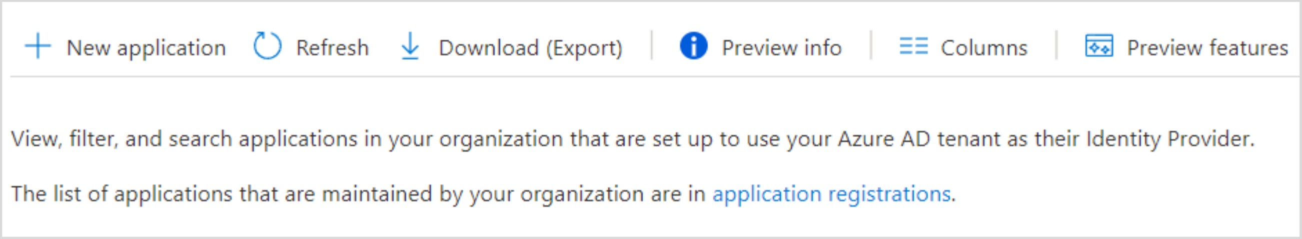
1. Go to Azure admin portal and select **Azure Active Directory**.



2. Click **Enterprise Applications** in the left panel



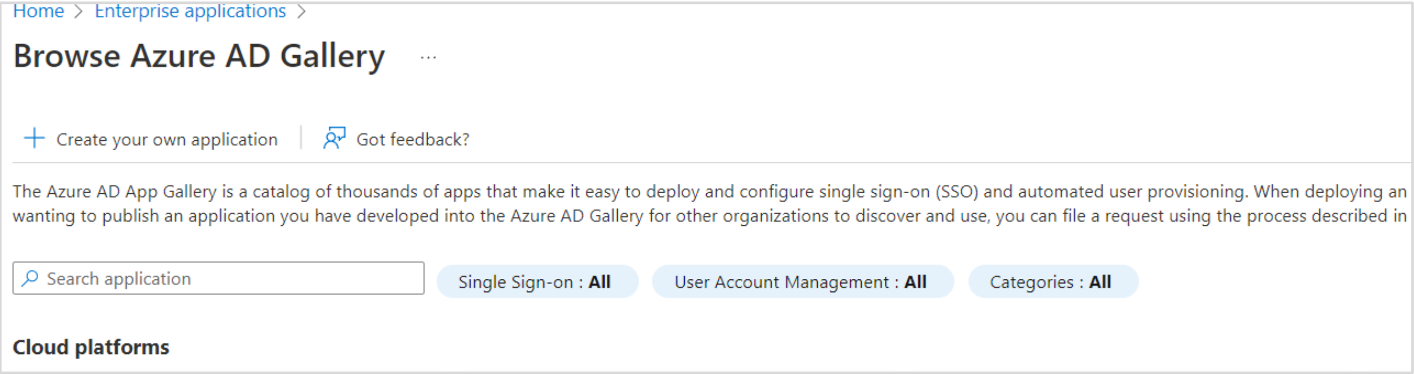
3. Click **New application**.



View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

4. Click **Create your own application**.


Home > Enterprise applications >
+ Create your own application
Got feedback?
Search application
Single Sign-on : All
User Account Management : All
Categories : All

Browse Azure AD Gallery ...

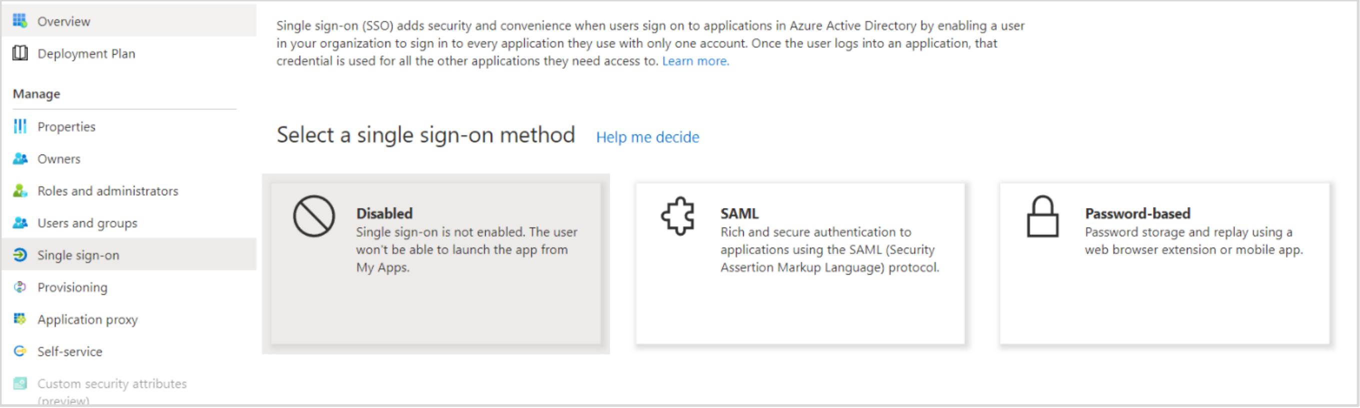
The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an wanting to publish an application you have developed into the Azure AD Gallery for other organizations to discover and use, you can file a request using the process described in

Cloud platforms

5. Leave the option as default, and provide an application name.

6. Click **Create**.

7. Click **Single sign-on** and select **SAML** as your single sign on method



Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

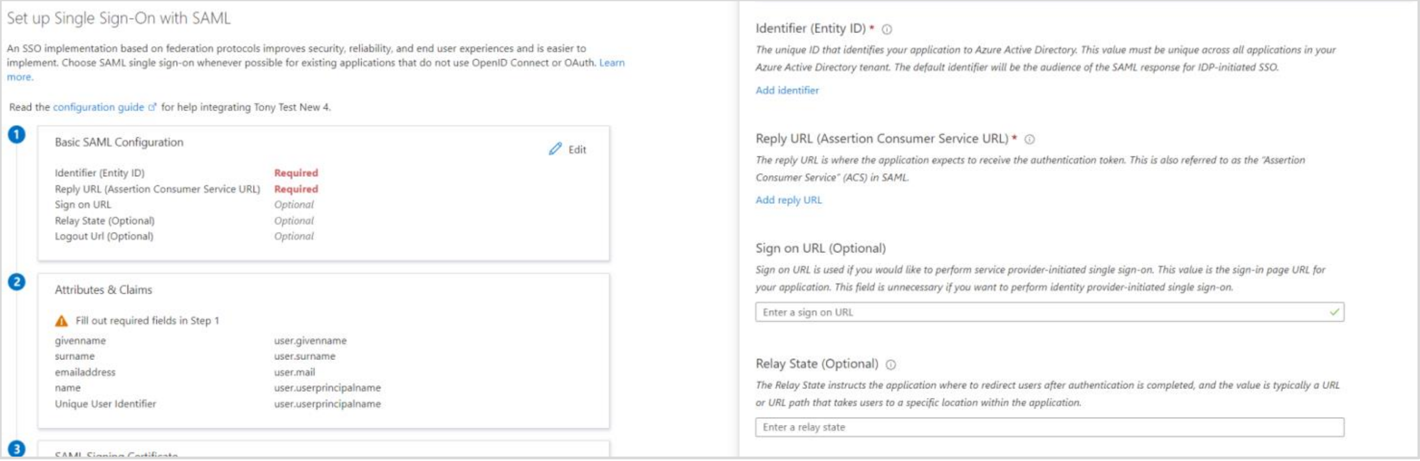
Select a single sign-on method

**Disabled** Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

**SAML** Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

**Password-based** Password storage and replay using a web browser extension or mobile app.

8. Edit the basic configuration.



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating Tony Test New 4.

Basic SAML Configuration

| | |
|---|---|
| Identifier (Entity ID) | Required |
| Reply URL (Assertion Consumer Service URL) | Required |
| Sign on URL | Optional |
| Relay State (Optional) | Optional |
| Logout Url (Optional) | Optional |

Attributes & Claims

⚠ Fill out required fields in Step 1

| | |
|---|---|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |

Identifier (Entity ID) *

*The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.*

Add identifier

Reply URL (Assertion Consumer Service URL) *

*The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.*

Add reply URL

Sign on URL (Optional)

*Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.*

Enter a sign on URL

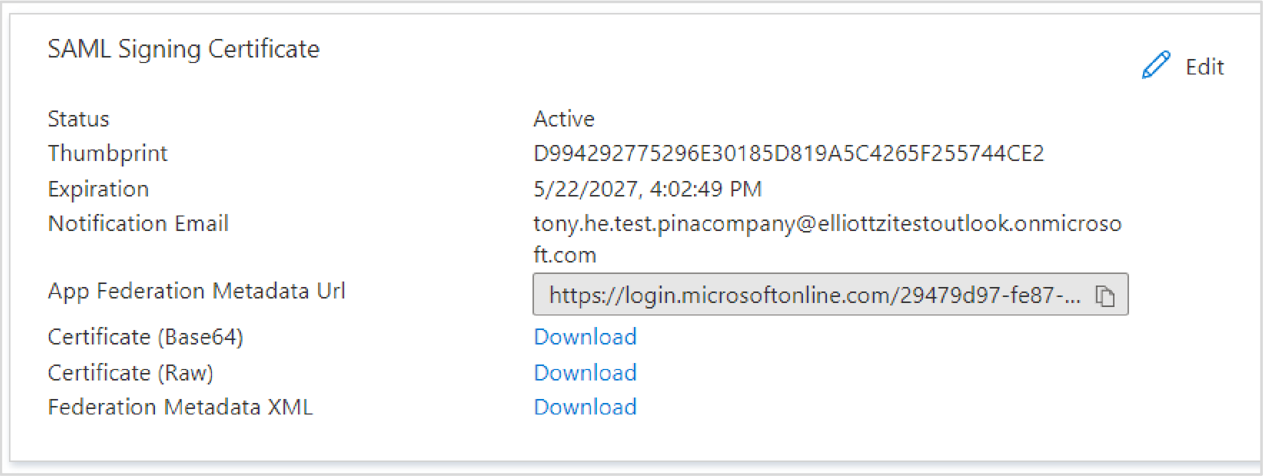
Relay State (Optional)

*The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.*

Enter a relay state

1. Add `https://zoominfo.com` to both **Identifier** and **Reply URL** and click **Save**.

2. Download Federation Metadata XML.



SAML Signing Certificate

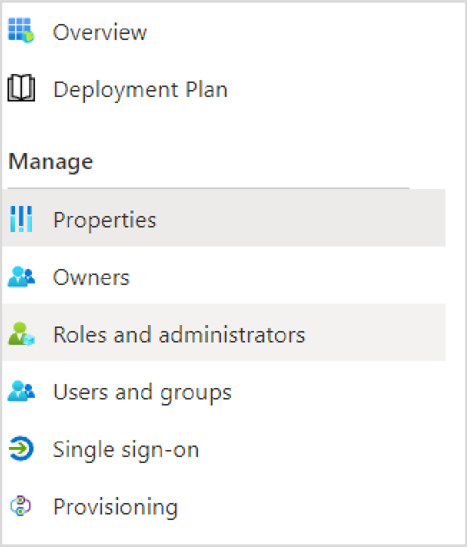
| | |
|---|---|
| Status | Active |
| Thumbprint | D994292775296E30185D819A5C4265F255744CE2 |
| Expiration | 5/22/2027, 4:02:49 PM |
| Notification Email | tony.he.test.pinacompany@elliottzitestoutlook.onmicrosoft.com |
| App Federation Metadata Url | https://login.microsoftonline.com/29479d97-fe87-... |
| Certificate (Base64) | Download |
| Certificate (Raw) | Download |
| Federation Metadata XML | Download |

3. In ZoomInfo, go to **Admin Portal > Company Settings > Single Sign-On**, click **Upload Metadata File** and choose the XML file you saved from Azure.
4. From the ZoomInfo Admin Portal **Single Sign-On Setup** page:
    a. Copy the **Relay State** URL from the Zoominfo Admin Portal to **Relay State** in the Azure Admin Portal **Single Sign-On** tab.

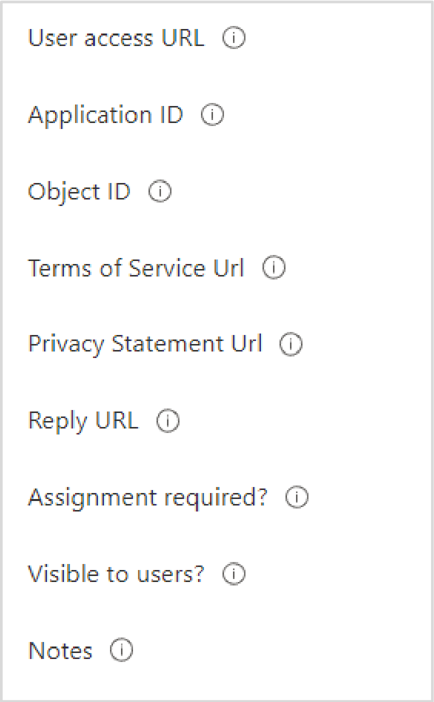
    b. Copy the **Audience** URI  from the Zoominfo Admin Portal to **Identifier** (override `https://zoominfo.com`) in Azure.

    c. Copy the **Assertion Consumer Service URL**  from the Zoominfo Admin Portal to **Reply URL** (override `https://zoominfo.com`) in Azure.

    d. Click **Save**.
5. Wait a few minutes for the configuration to take effect.
6. Assign users that you want to use the SAML settings to the app.
7. Go to the **Properties** tab.



8. Use the **User access URL** (shown below) provided by Azure to sign in. Do not use login.zoominfo.com for Azure SSO.



User access URL ⓘ

Application ID ⓘ

Object ID ⓘ

Terms of Service Url ⓘ

Privacy Statement Url ⓘ

Reply URL ⓘ

Assignment required? ⓘ

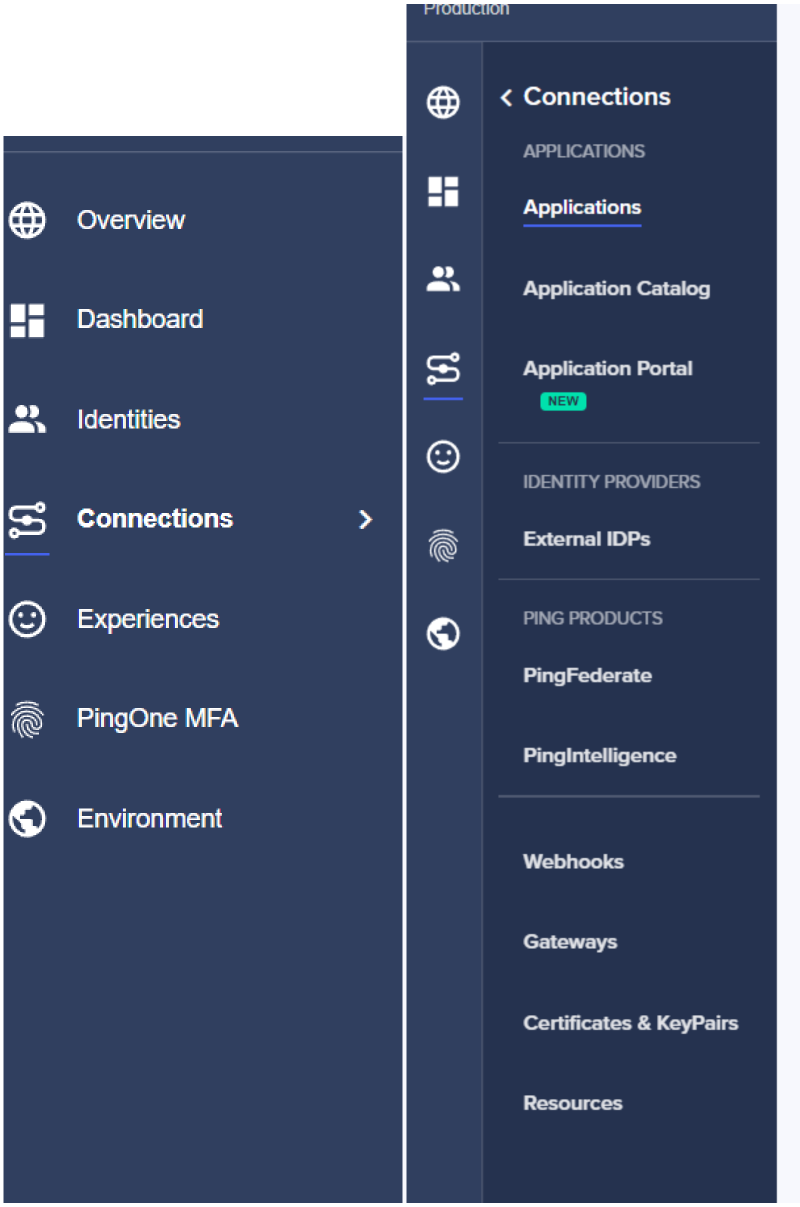
Visible to users? ⓘ

Notes ⓘ

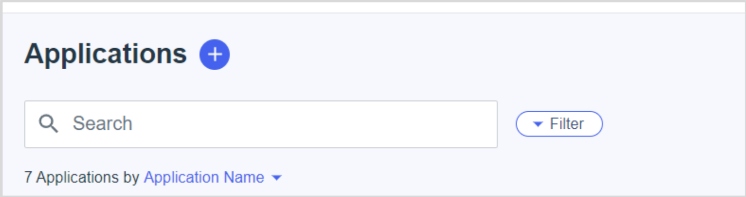
**Note**: For issues related to Unique User Identifier in Attributes & Claims, see Troubleshooting.

# PingOne Configuration

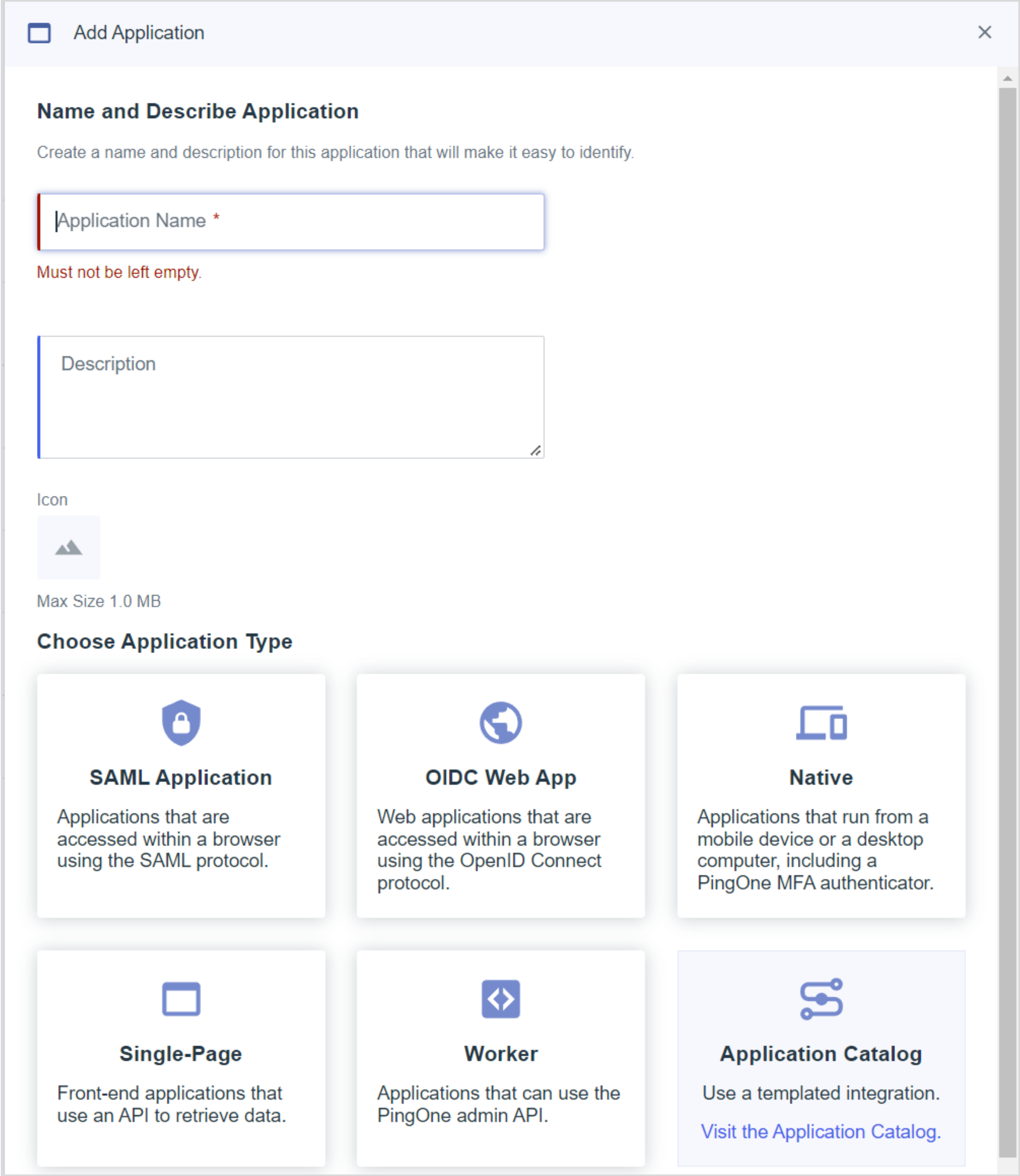
1. In the PingOne Admin Portal, click **Connections > Applications**.



2. Select the **+** button.



3. Provide an application name and select **SAML Application**.



Add Application

**Name and Describe Application**

Create a name and description for this application that will make it easy to identify.

Application Name *

Must not be left empty.

Description

Icon

Max Size 1.0 MB

**Choose Application Type**

**SAML Application**

Applications that are accessed within a browser using the SAML protocol.

**OIDC Web App**

Web applications that are accessed within a browser using the OpenID Connect protocol.

**Native**

Applications that run from a mobile device or a desktop computer, including a PingOne MFA authenticator.

**Single-Page**

Front-end applications that use an API to retrieve data.

**Worker**

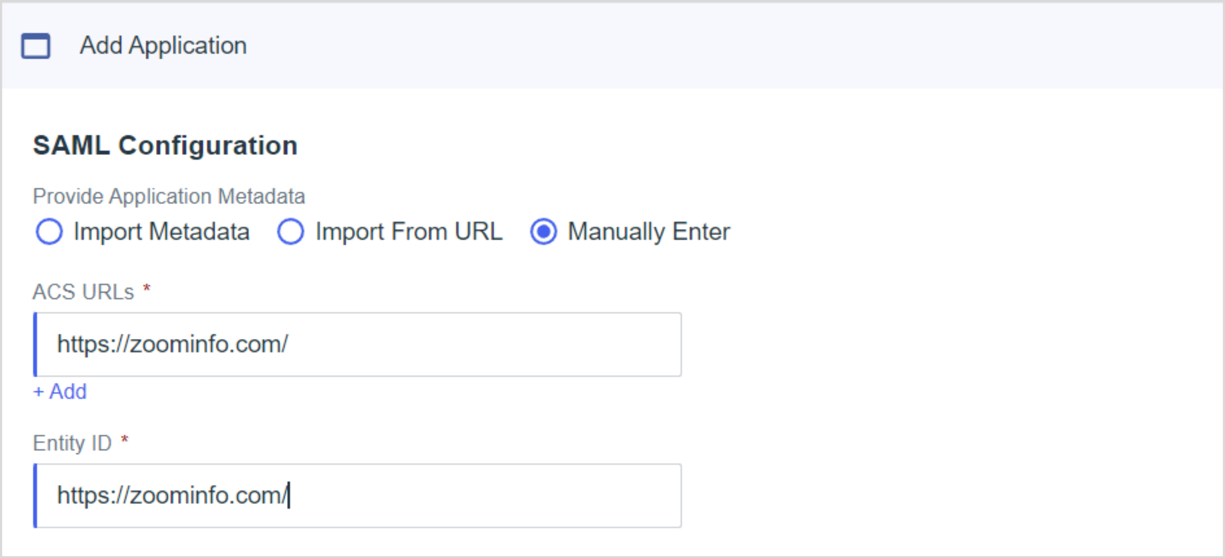
Applications that can use the PingOne admin API.

**Application Catalog**

Use a templated integration.

Visit the Application Catalog.

4. Click **Configure** at the bottom.
5. Type `https://zoominfo.com` in the **ACS URLs** and **Entity ID** fields.


Add Application

SAML Configuration

Provide Application Metadata

○ Import Metadata ○ Import From URL ● Manually Enter

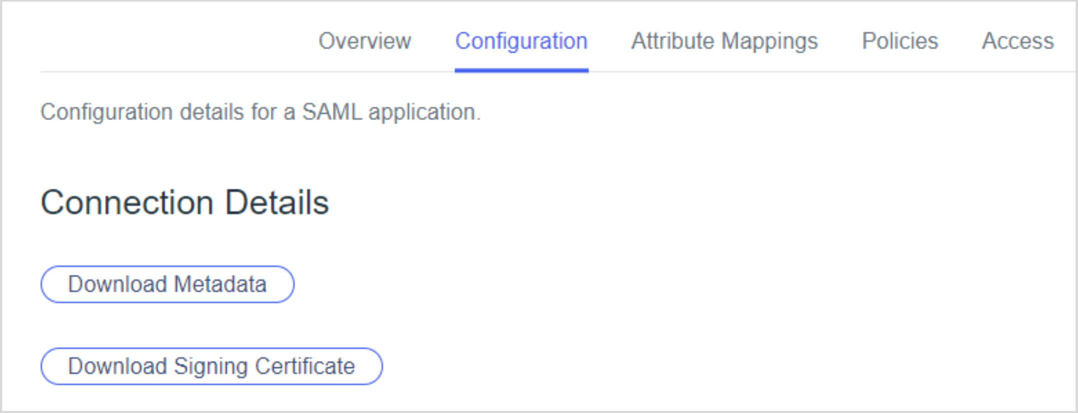
ACS URLs *

https://zoominfo.com/

Entity ID *

https://zoominfo.com/

6. Go to the **Configuration** tab and click **Download Metadata**.



Configuration details for a SAML application.

Connection Details

7. In ZoomInfo, go to **Admin Portal > Company Settings > Single Sign-On**, click **Upload Metadata File** and choose the XML file you saved from PingOne.

8. From the ZoomInfo Admin Portal **Single Sign-On Setup** page:

   a. Copy the **Relay State** URL from the Zoominfo Admin Portal to **Target Application URL** in PingOne.

   b. Copy the **Audience** URI to **Entity Id** in PingOne.

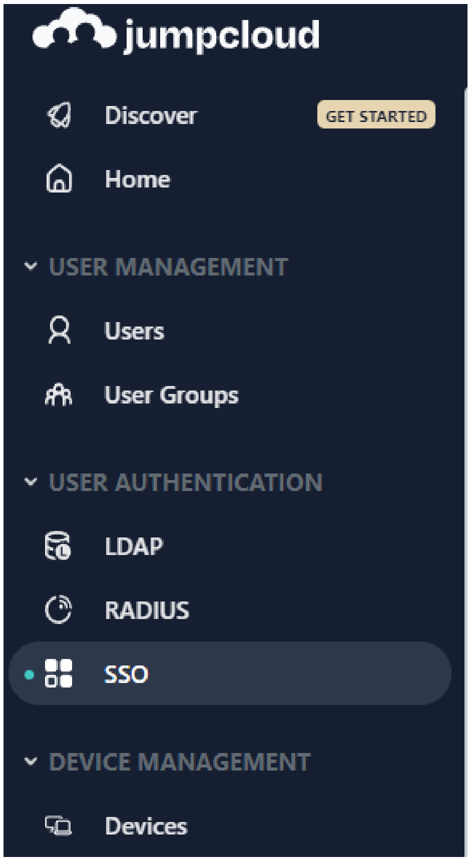
   c. Copy the **Assertion Consumer Service** URL to **ACS URLs** in PingOne

   d. Select urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress for the **Subject Nameid Format** in PingOne.

9. Use **Initiate Single Sign-On URL** to log in.

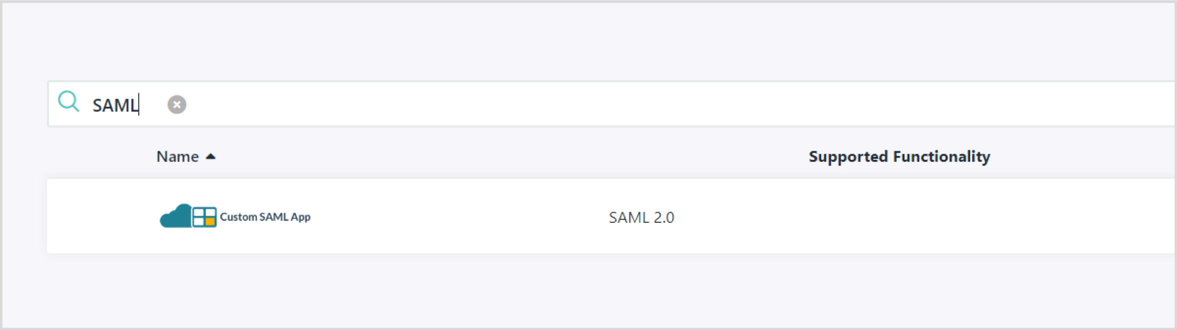
# JumpCloud Configuration

1. Go to the JumpCloud Admin Portal and click **SSO**.



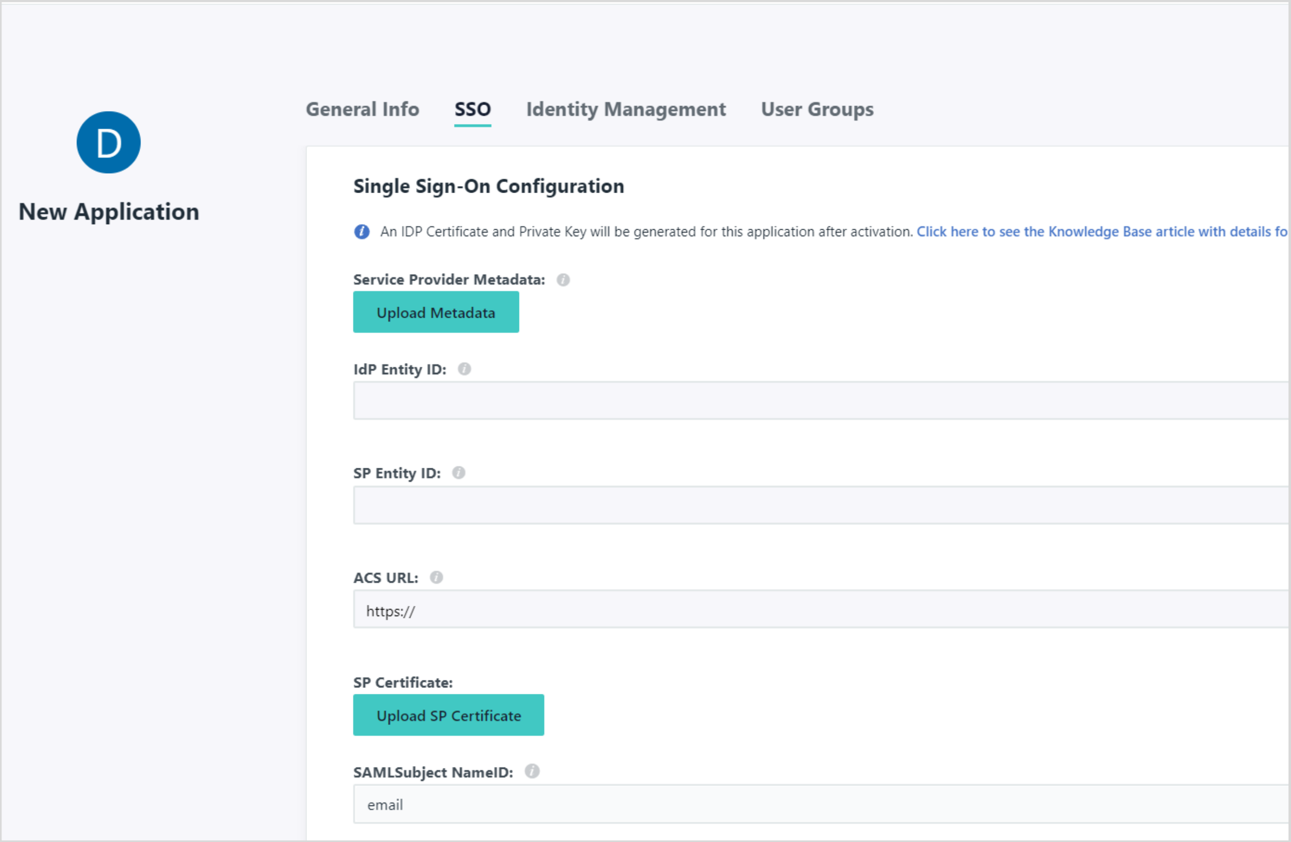
2. Create a new app.

3. Search for the SAML app.


SAML

| Name ▲ | Supported Functionality |
|---|---|
| Custom SAML App | SAML 2.0 |

4. Provide an application name and click the **SSO** tab



New Application

Single Sign-On Configuration

An IDP Certificate and Private Key will be generated for this application after activation. Click here to see the Knowledge Base article with details fo

Service Provider Metadata:

IdP Entity ID:

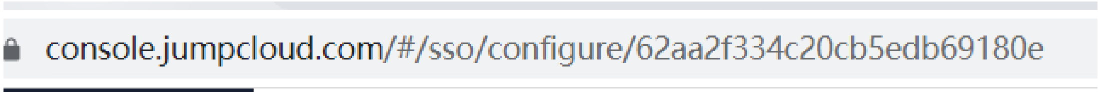
SP Entity ID:

ACS URL: https://

SP Certificate:

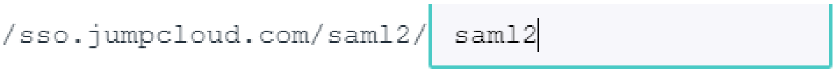
SAMLSubject NameID: email

5. Type your application id as **IdP Entity ID**:



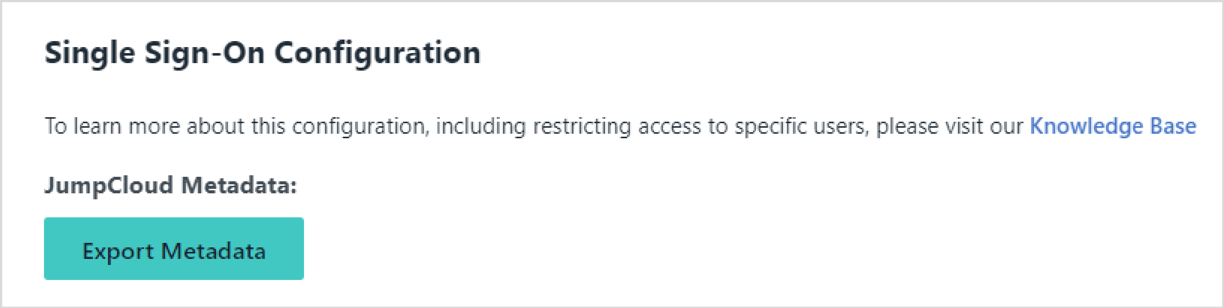
console.jumpcloud.com/#/sso/configure/62aa2f334c20cb5edb69180e

6. Type `https://zoominfo.com` as your **SP Entity ID** and **ACS URL**.
7. Change the **SAMLSubject NameID** format to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
8. Update the **IdP URL** to a desired value. For example:



/sso.jumpcloud.com/saml2/ saml2

9. Click the **Activate** button on the bottom right.
10. Return to the **Application > SSO** tab
11. Click **Export Metadata**.



**Single Sign-On Configuration**

To learn more about this configuration, including restricting access to specific users, please visit our Knowledge Base

**JumpCloud Metadata:**

12. In ZoomInfo, go to **Admin Portal > Company Settings > Single Sign-On**, click **Upload Metadata File** and choose the XML file you saved from JumpCloud.
13. From the ZoomInfo Admin Portal **Single Sign-On Setup** page:
    a. Copy the **Relay State** URL from Zoominfo Admin Portal to **Default RelayState** in JumpCloud.
    b. Copy the **Audience** URI to **SP Entity ID** in JumpCloud
    c. Copy the **Assertion Consumer Service URL** to **ACS URL** in JumpCloud
14. Assign the users that you want to use this SAML application.
15. Use your IdP URL to log in to ZoomInfo.

## Troubleshooting

If XML upload fails, please check if your XML is in the right format.

- You should save the XML directly from the website.
- Use Ctrl + S to save the file if it does not save automatically
- Do not copy the XML file into a Word document.

If you have already uploaded a file, you must press RESET ALL to upload a new file.

For Microsoft Azure, ensure that your username is set as your Unique User Identifier. The default value for Unique User Identifier in Attributes & Claim is username (e.g. user.userprincipalname or user.mail)