Single Sign-On with ZoomInfo and Okta Integration Guide

For administrators setting up ZoomInfo Single Sign-On using Okta

This document describes how to configure Single Sign-On (SSO) using SAML 2.0 for ZoomInfo in Okta. Contact [ZoomInfo Support]() if you need additional assistance in setting up this configuration for your organization.

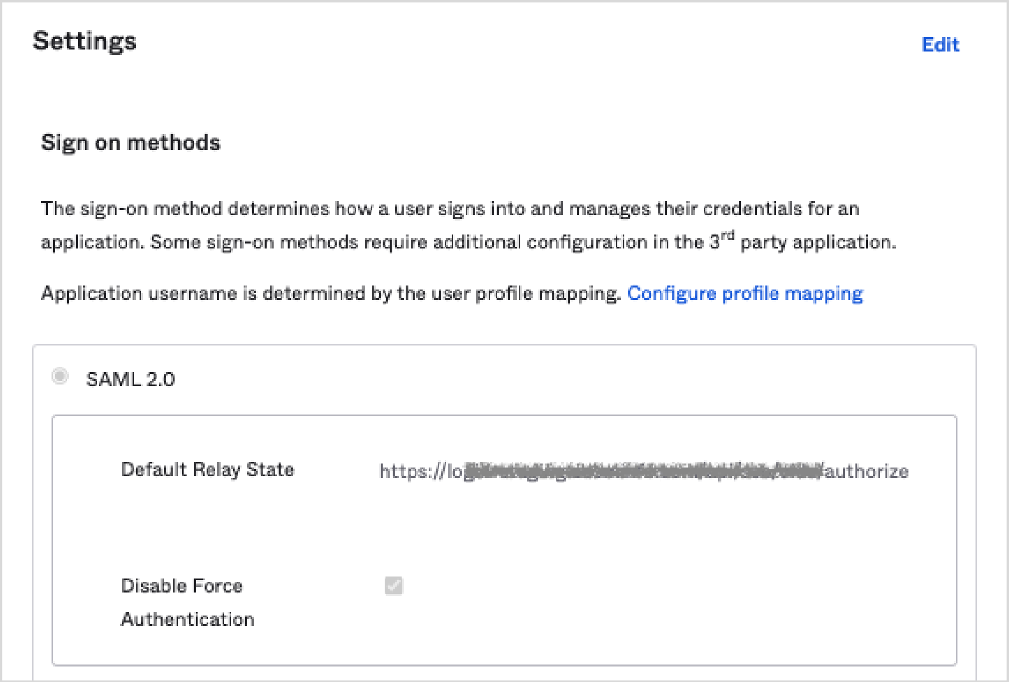
Add the ZoomInfo App to Okta

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.

Configure SAML 2.0 Single Sign On

1. In the Okta ZoomInfo app, complete the fields on the **General** page with your new **Application label** and click **Next**.
2. 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.

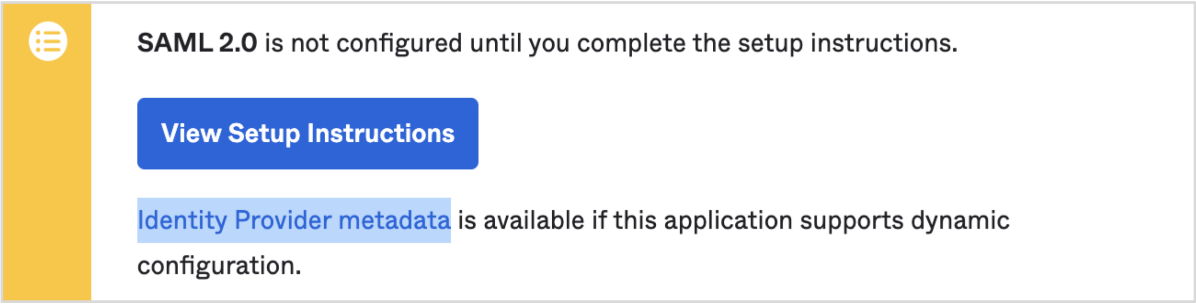
Application username is determined by the user profile mapping. Configure profile mapping

● SAML 2.0

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

Disable Force Authentication ☑

3. Scroll down to this section.



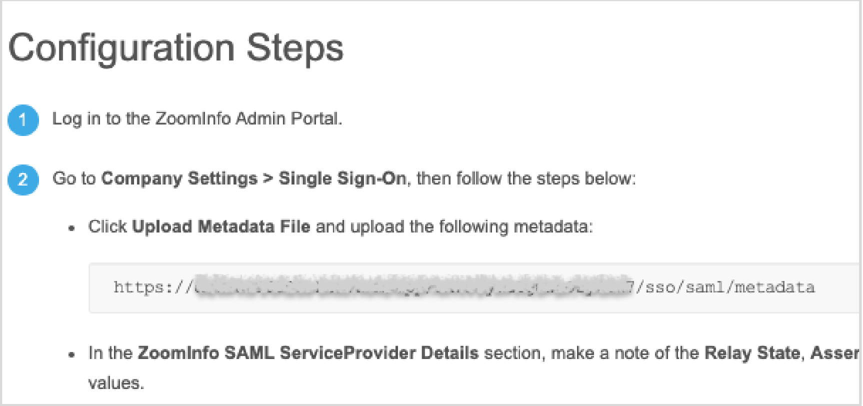
SAML 2.0 is not configured until you complete the setup instructions.

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**.

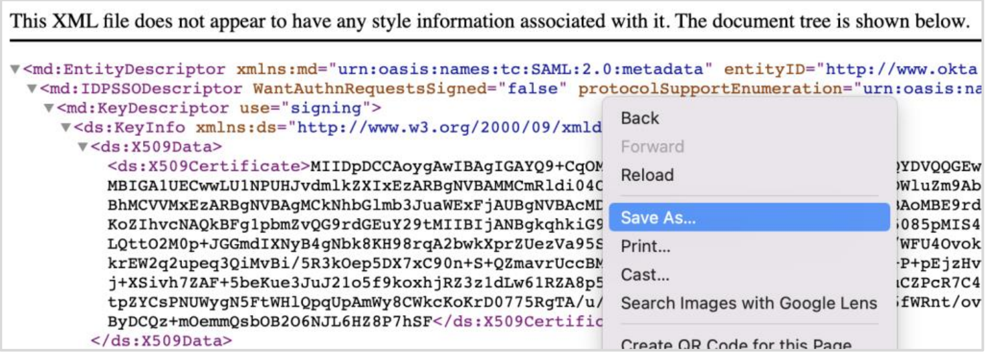
Go to step 4.

Option 2: Identity Provider metadata link

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

Go to step 4.

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

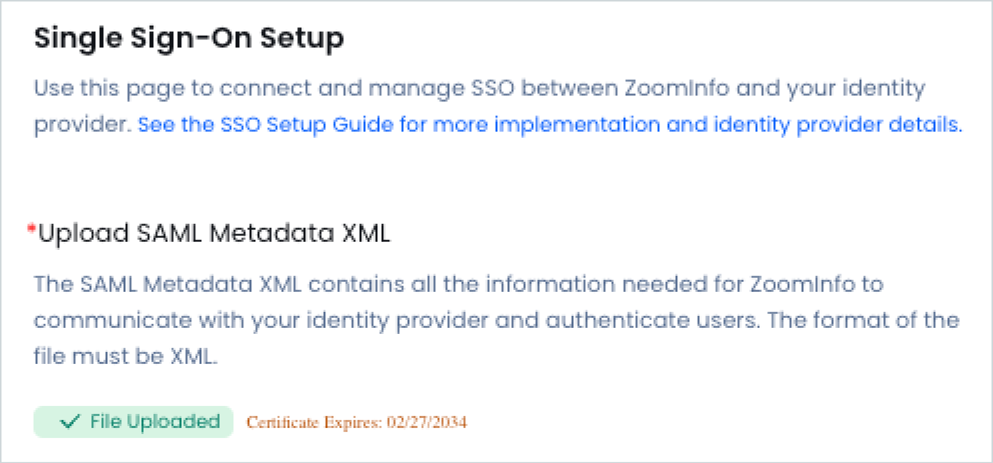


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<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                     YDVQQGEw
            MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCmRldi04C                     WluZm9Ab
            BhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMD                     AoMBE9rd
            KoZIhvcNAQkBFglpbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9                     085pMIS4
            LQttO2M0p+JGGmdIXNyB4gNbk8KH98rqA2bwkXprZUezVa95S                     WFU4Ovok
            krEW2q2upeq3QiMvBi/5R3kOep5DX7xC90n+S+QZmavrUccBM                     P+pEjzHv
            j+XSivh7ZAF+5beKue3JuJ21o5f9koxhjRZ3z1dLw61RZA8p5                     CZPcR7C4
            tpZYCsPNUWygN5FtWHlQpqUpAmWy8CWkcKoKrD0775RgTA/u/                     fWRnt/ov
            ByDCQz+mOemmQsbOB2O6NJL6HZ8P7hSF</ds:X509Certific
        </ds:X509Data>
```

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

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



Single Sign-On Setup

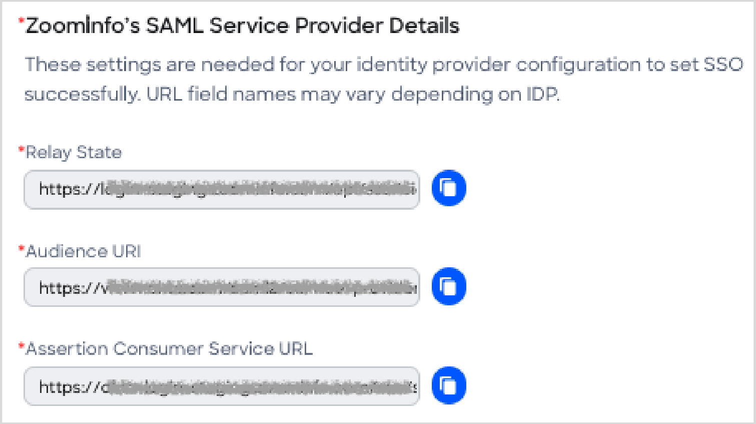
Use this page to connect and manage SSO between ZoomInfo and your identity provider. See the SSO Setup Guide for more implementation and identity provider details.

*Upload SAML Metadata XML

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

✓ File Uploaded Certificate Expires: 02/27/2034

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]

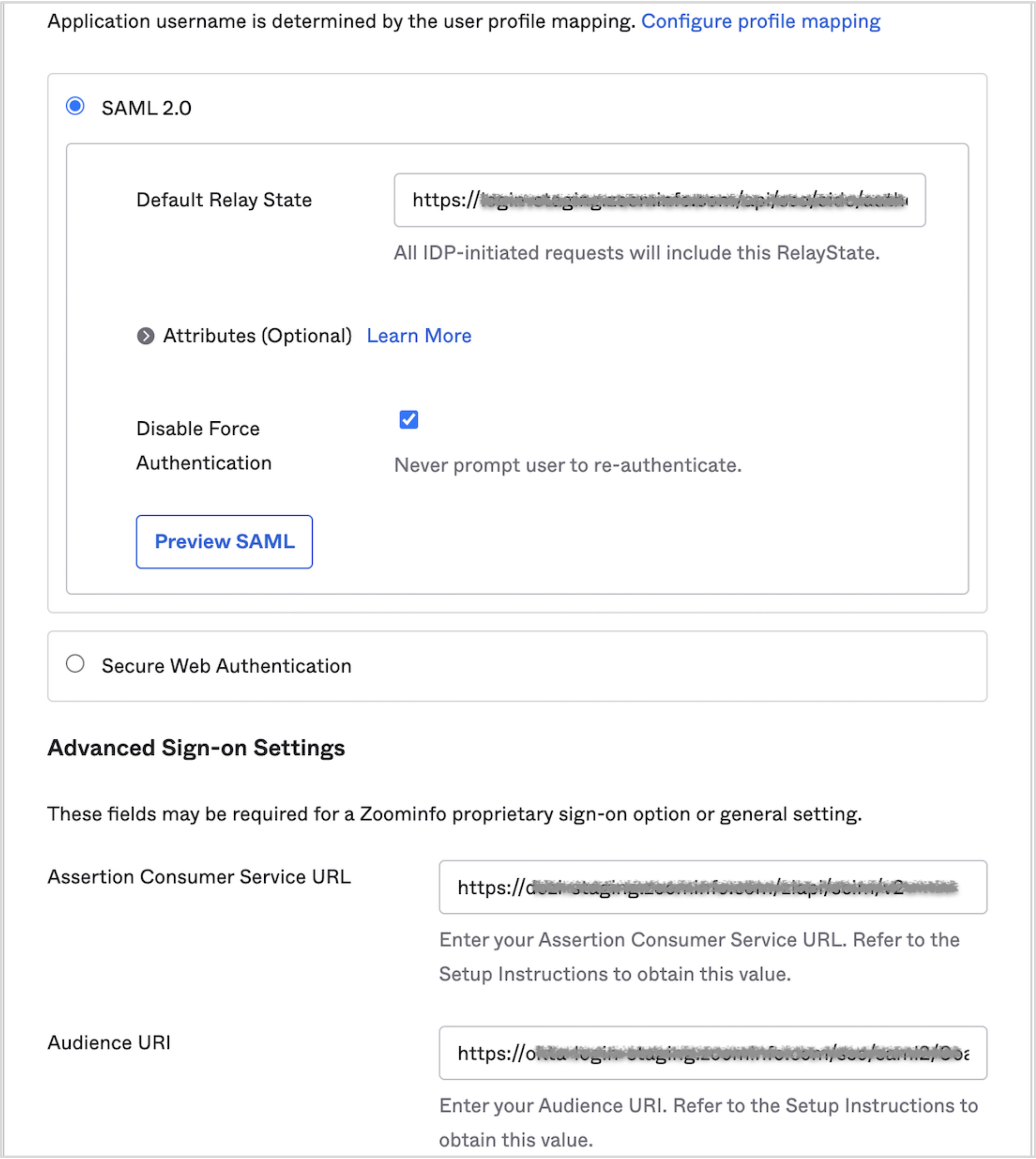
*Audience URI

https://v[redacted]

*Assertion Consumer Service URL

https://d[redacted]

7. 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://d[redacted]

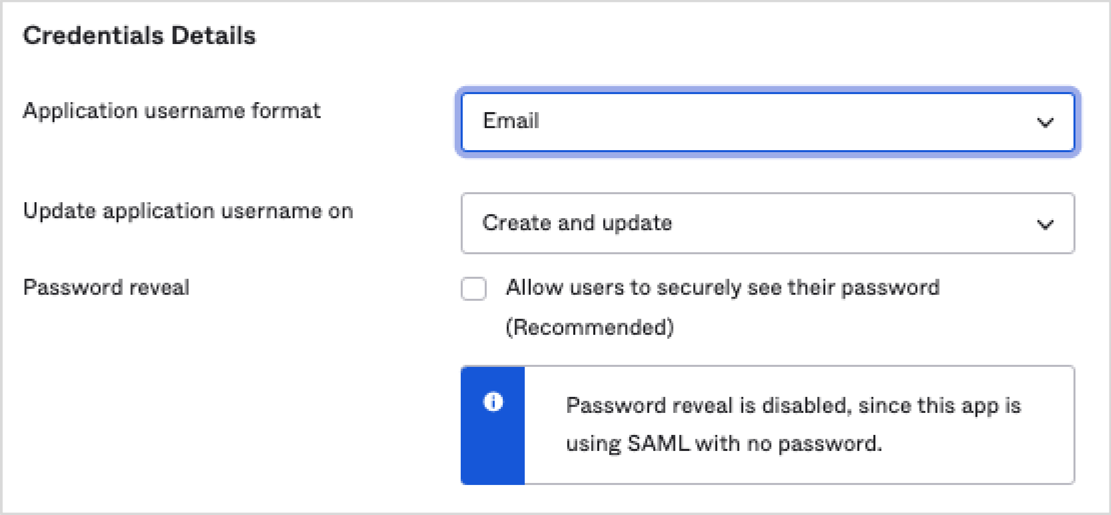
Enter your Assertion Consumer Service URL. Refer to the Setup Instructions to obtain this value.

Audience URI: https://o[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

8. 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.

9. Click **Done**. Your SAML 2.0 configuration is complete.