How to Configure SAML 2.0 for Obsidian Security

Contents

Summary

This document describes how Okta can be configured as an Identity Provider (IdP) for Obsidian Security.

If you need any additional assistance, please contact support@obsidiansecurity.com.

The fastest way to get help is to use the **Get help** chat button in the lower-left corner of your Obsidian admin console.

Supported Features

The Okta/Obsidian Security SAML integration currently supports the following features:

- IdP-initiated SSO
- SP-initiated SSO
- Just-in-time (JIT) provisioning
- NOT a big-bang SSO configuration

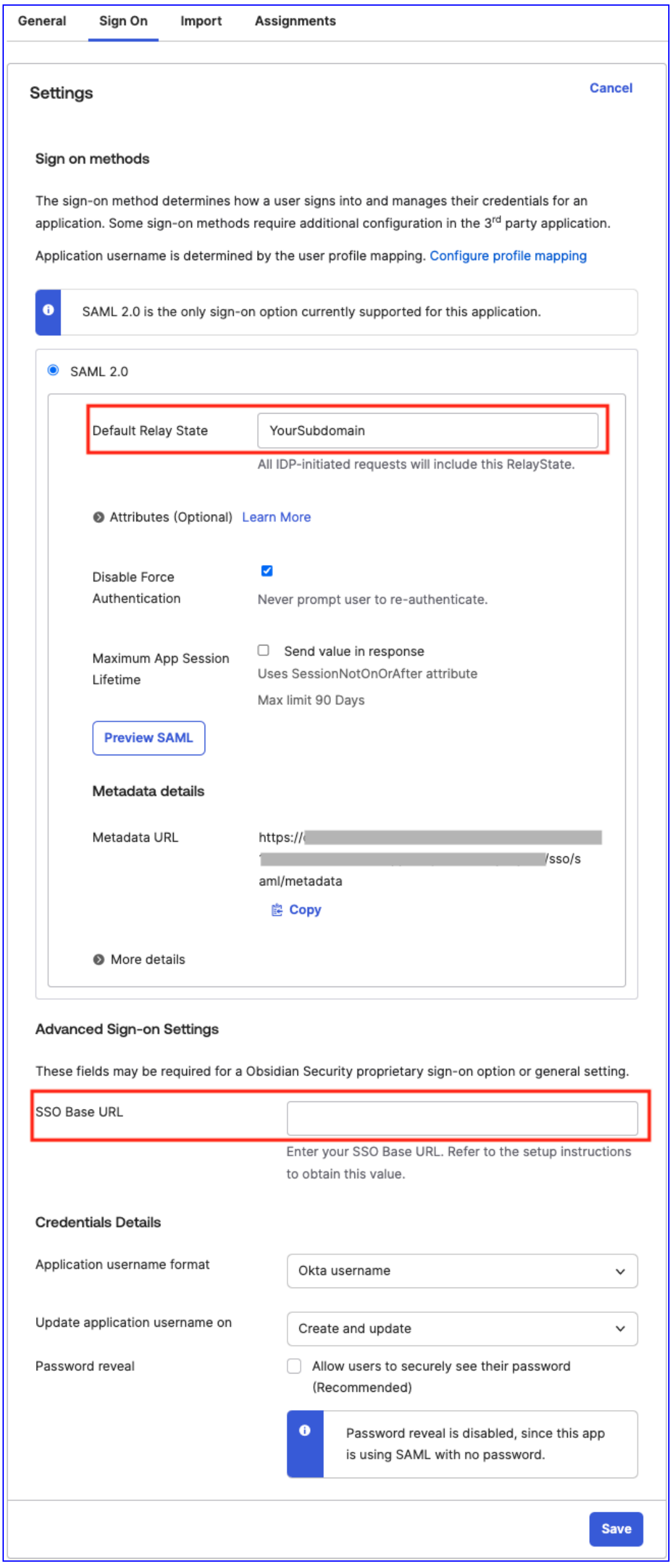
For more information on the listed features, visit the Okta Glossary.

Prerequisites

You must either be a Super Administrator, an Application Administrator, or have a delegated role with the ability to create and configure a new application in Okta and be able to assign users/groups to an application to complete this integration.

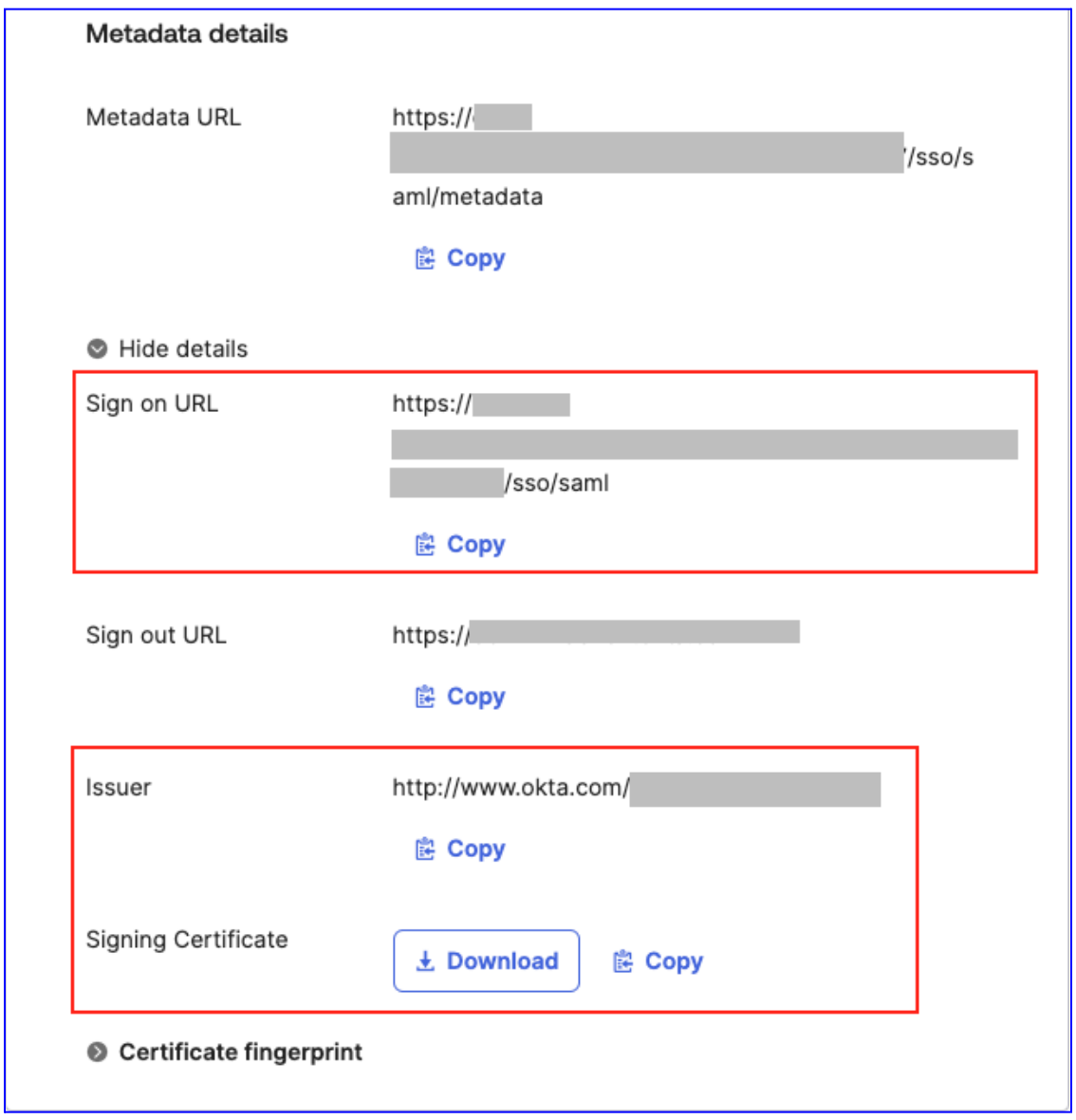
Configuration Steps

1. Click on the **Sign On** tab, as shown in the screenshot below.

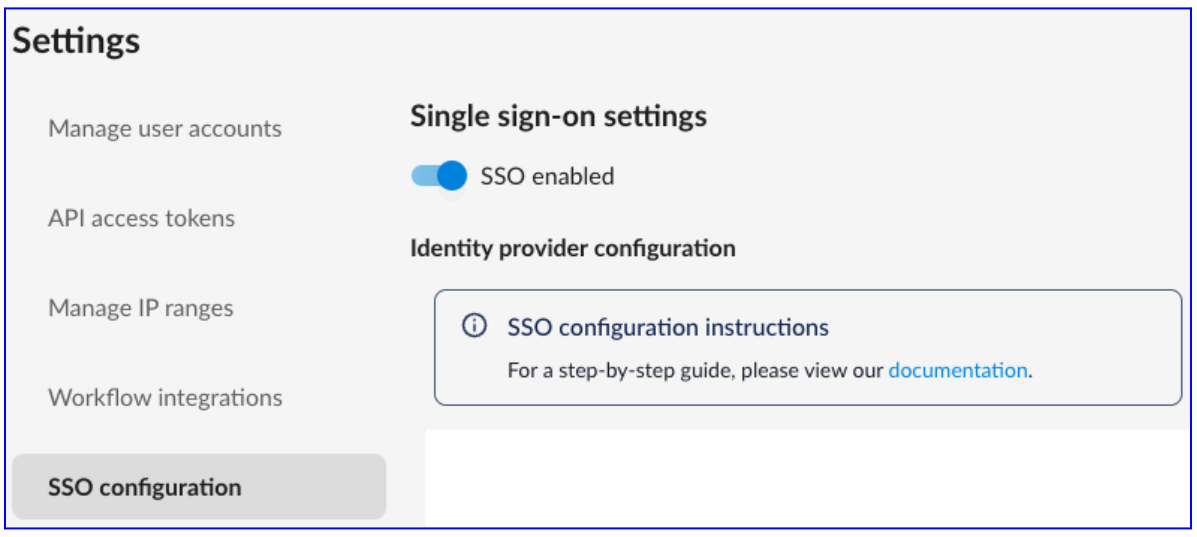


2. Click on **Edit**.
3. In the **Default Relay State** field - enter the ***YourSubdomain*** part of your Obsidian Security tenant. For example, if you access Obsidian with https://acme.obsec.io or https://acme.obsec.eu, *YourSubdomain* is the ***acme*** part of the URL.
4. Keep the **Disable Force Authentication** checkbox checked.
5. Keep the **Maximum App Session Lifetime** checkbox unchecked.
6. Enter your Obsidian Security tenant's **SSO Base URL**.
    a. If your Obsidian Security tenant is in the **United States (US) region**, enter *https://api.obsec.io*
    b. If your Obsidian Security tenant is in the **European Union (EU) region**, enter *https://api.obsec.eu*
    c. If your Obsidian Security tenant is in the **Australian (AU) region**, enter *https://api.sy.obsec.io*

7. Under the **Credentials Details**, select the following:
    a. Application username - Okta username
    b. Update application username on - Create and update
8. Click **Save.**
9. Under the **Assignments** tab, assign at least 1 user to the Obsidian Security application. You will log in with this user account to complete the integration described in **step #12**.
10. Once you've saved the application, on the **Sign On** tab and under the **Metadata details**, expand **More details**, as shown below. Copy the following values to a notepad/text editor of your choice. These values will be required to finish the SSO configuration in Obsidian Security's Admin Console described in **step #12**.
    a. **Sign On URL:** Copy the URL displayed for this field.
    b. **Issuer:** Copy the URL displayed for this field.
    c. **Signing Certificate:** Copy the X.509 certificate value.



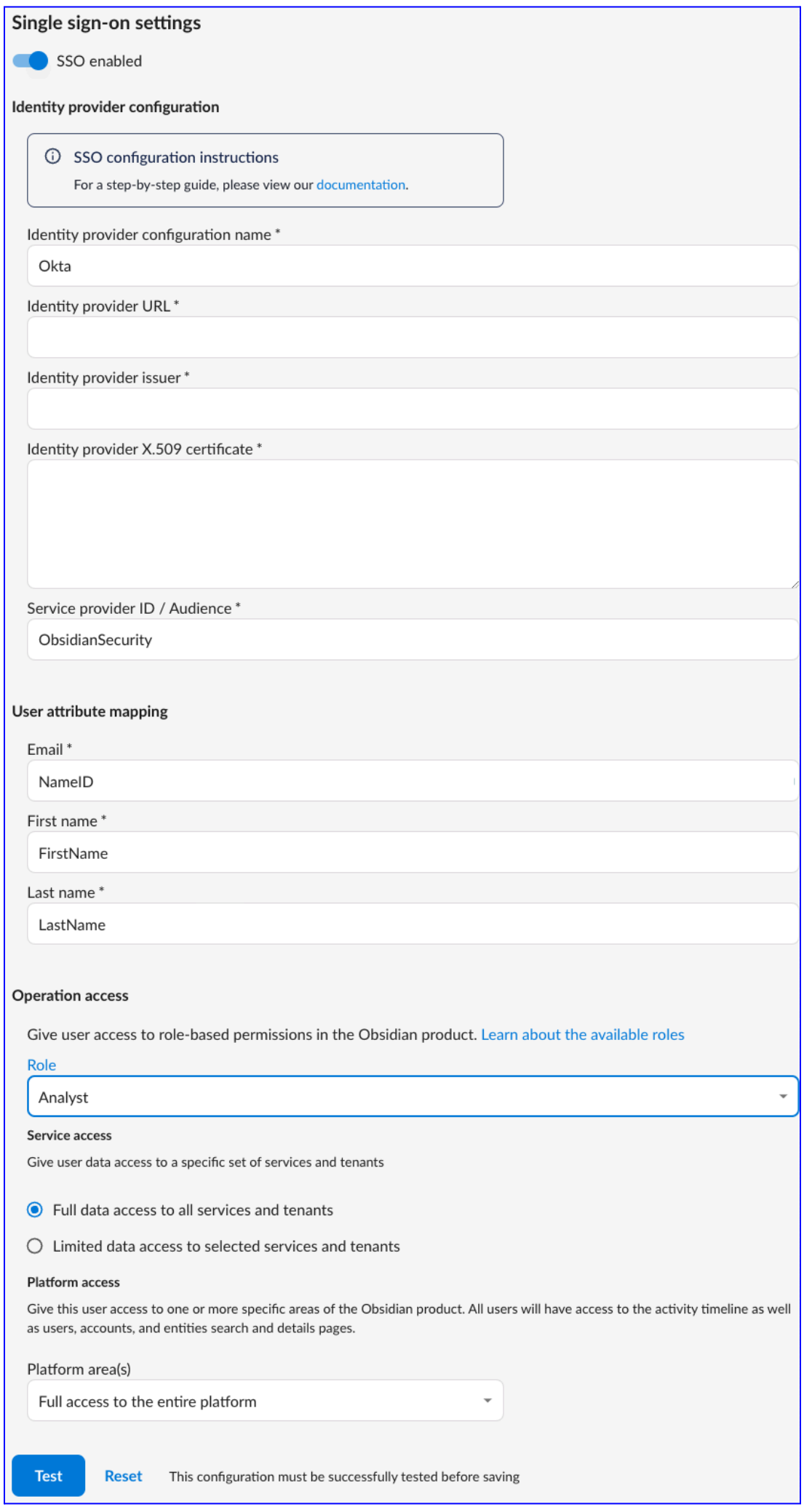
11. Log in to your **Obsidian Security** tenant as an Administrator.
12. On the bottom left corner of the admin console, click on the ⚙️ icon, then navigate to **SSO configuration**.



13. On the **Identity provider configuration** page, enter the following values, as shown in the screenshot below:
    a. **Identity provider configuration name** - *A friendly name. E.g. Okta.*
    b. **Identity provider URL (Sign on URL)** - *Value copied from **step #10(a)**.*
    c. **Identity provider issuer (Issuer)** - *Value copied from **step #10(b)**.*
    d. **Identity provider X.509 certificate (Signing Certificate)** - *Value copied from **step #10(c)**.*
    e. **Service provider ID / Audience** - *ObsidianSecurity*
    f. User attribute mapping

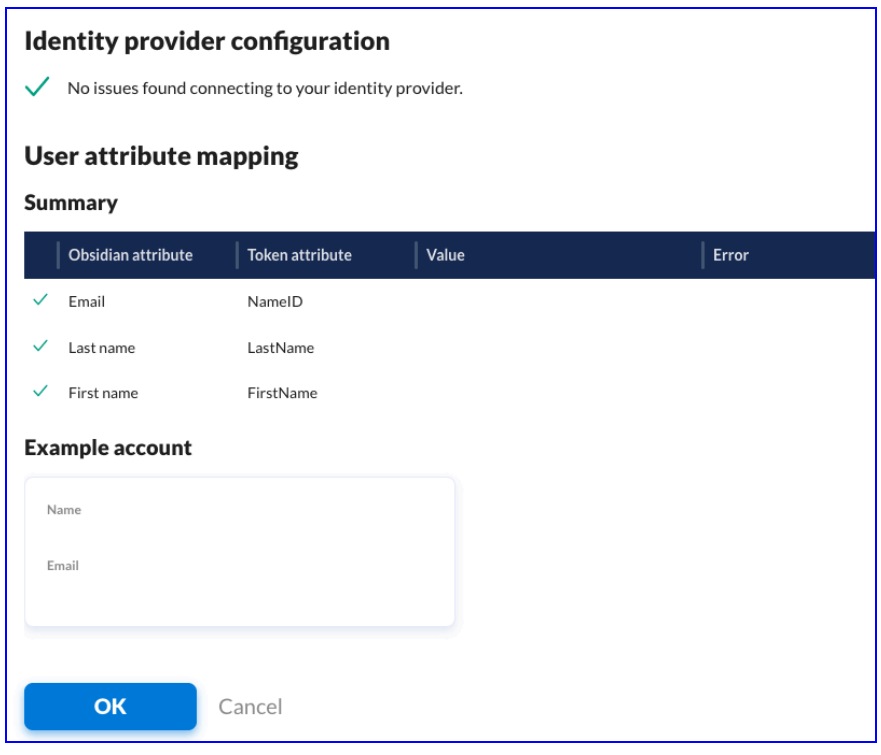
i. **Email** - *NameID*
ii. **FirstName** - *FirstName*
iii. **LastName** - *LastName*

g. **Default role mapping** - Select ***Analyst*** for the default role. This will ensure that all users assigned to the Obsidian Security application from Okta will have the same role when they SSO from Okta to Obsidian Security. Once the user does a successful SSO and the user is provisioned from Okta to Obsidian Security through SAML Just-In-Time (JIT) provisioning, you can change the role assignment for individual users by logging in to the Obsidian Security Admin Console as an Administrator.



Test SAML Authentication

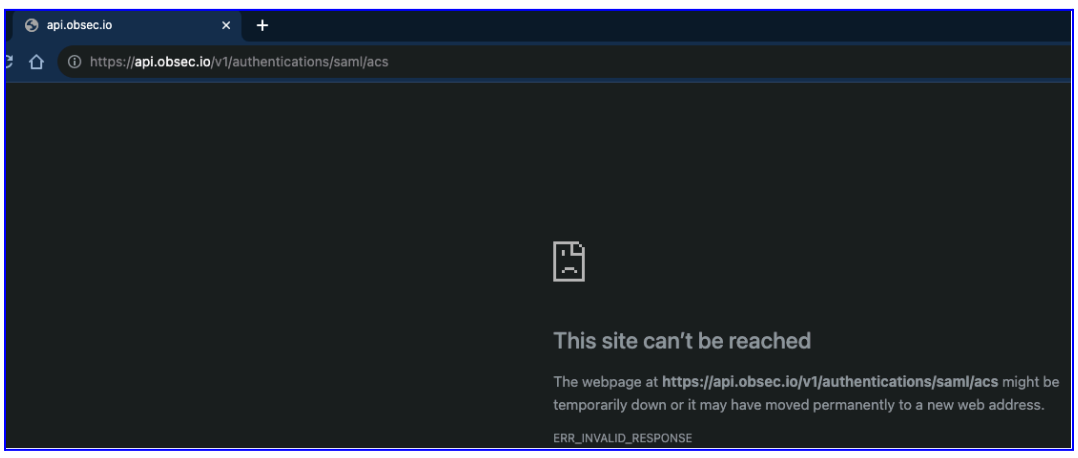
14. Once you have completed all the steps, click the **Test** button. This will require you to log in to your Okta tenant. Log in with the user you assigned to the Obsidian Security application in **step #9**.
15. A successful test should look as shown below:



16. If the test passes successfully, click on **OK**.
17. Click **Save** on the main page.
18. **Congratulations!** SSO is now configured.

Notes And Troubleshooting

- If you get the following error message when you try to SSO from the Okta end-user dashboard



  Go to **step # 3** of the Configuration Steps section in this document and ensure that you entered the correct value in the **Default Relay State** field under the Sign On tab. Leaving it blank or using an incorrect value will prevent you from doing a successful SSO from the Okta end-user dashboard to Obsidian Security.
- The following SAML attributes are supported:

Name	Value
NameID	user.email
FirstName	user.firstName
LastName	user.lastName

SP-initiated SSO

1. Go to: https://[YourSubdomain].obsec.io/ or https://[YourSubdomain].obsec.eu or https://[YourSubdomain].sy.obsec.io/
2. Click Continue with SSO

[1]

[1] Version 4.0 - Updated on 28 Aug 2024.