



***Safenames Single Sign On
With OIDC***
Azure / Okta / OneLogin setup instructions

Document Classification:	Unclassified
Document Ref.	
Version:	0.6
Dated:	13 July 2023
Document Author:	Jon Stock
Document Owner:	Jon Stock

Revision History

Version	Date	Revision Author	Summary of Changes
0.1	23/02/2023	Jon Stock	First Draft
0.2	17/05/2023	Jon Stock	Added Azure SSO
0.3	26/06/2023	Jon Stock	Azure updates
0.4	26/06/2023	Jon Stock	Removed SWA Support
0.5	27/06/2023	Jon Stock	Added OneLogin Support

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Contents

1	OVERVIEW	4
2	OKTA	5
2.1	OKTA INTEGRATION OPTIONS.....	5
2.2	OKTA SWA.....	5
2.3	OKTA SSO	5
3	OKTA SSO WITH OIDC SETUP INSTRUCTIONS	6
3.1	PRE-CONFIGURATION	6
3.2	STEP 1 – CREATE THE APPLICATION IN YOUR OKTA TENANT	7
3.3	STEP 2 - SELECT APP INTEGRATION TYPE	8
3.4	STEP 3 – SELECT APPLICATION TYPE	9
3.5	STEP 4 - CONFIGURE THE APP INTEGRATION SETTINGS	10
3.6	STEP 5 - ENABLE PKCE	13
3.7	STEP 6 - SET LOGIN INITIATED BY.....	13
3.8	STEP 7 - SET LOGIN URI	14
3.9	LOGO (OPTIONAL)	14
3.10	POST CONFIGURATION	15
3.11	OKTA USER ACCOUNT SYNCHRONIZATION.....	17
4	AZURE	18
4.1	AZURE SSO APPLICATION SETUP	18
4.2	PRE-CONFIGURATION	18
4.3	STEP 1 – ACCESS AZURE ADMIN PORTAL	19
4.4	STEP 2 – ACCESS YOUR AZURE ACTIVE DIRECTORY.....	20
4.5	STEP 3 – SELECT ENTERPRISE APPLICATIONS	21
4.6	STEP 5 - CREATE NEW APPLICATION	22
4.7	STEP 6 – SELECT SINGLE TENANT.....	23
4.8	STEP 7 - CONFIGURE “SAFENAMES IDP” APPLICATION	24
4.9	STEP 8 – CONFIGURATION SETTINGS.....	25
4.10	STEP 9 – CREATE CLIENT SECRETS	26
4.11	STEP 10 - SET AUTHENTICATION URI	27
4.12	STEP 11 - USER PERMISSIONS.....	29
4.13	STEP 12 – POST CONFIGURATION	30
4.14	AZURE USER ACCOUNT SYNCHRONIZATION	30
5	ONELOGIN	31
5.1	PRE-CONFIGURATION	31
5.2	STEP 1 - CREATE CUSTOM CONNECTOR	32
5.3	STEP 2 - CREATE APPLICATION	36
5.4	STEP 3 - USERS PERMISSIONS.....	38
5.5	STEP 4 POST-CONFIGURATION	38
5.6	ONELOGIN USER ACCOUNT SYNCHRONIZATION	39
6	SSO DEVELOPMENT ROADMAP	40
6.1	OKTA	40
6.2	AZURE.....	40

1 Overview

Single Sign On technologies have been implemented into Safenames registrar portal (IDP)

We have enabled multiple methods and providers in order to provide clients with a solution that can be integrated into existing client frameworks to federate IDP access using your chosen Identity provider.

Safenames has elected to utilize OIDC (Open ID Connect) protocols.

OpenID Connect (OIDC) is an open authentication protocol that works on top of the OAuth 2.0 framework.

OIDC allows individuals to use single sign-on (SSO) to access relying party sites using OpenID Providers (OPs), to authenticate their identities.

Safenames has initially built support for Okta and Microsoft Azure with further Identity providers planned for the future.

2 Okta

Okta provides IDaaS (Identity-as-a-Service).

It provides Identity Access Management solutions for businesses, institutions, and individuals.

It allows seamless integration with over 5,000+ platforms and applications like Office 365, Facebook, PowerPoint, G Suite, and others used in day-to-day business.

2.1 Okta integration options

Okta can be used with the IDP by using Okta SWA or Okta SSO applications added to your existing Okta tenant.

2.2 Okta SWA

Is a custom application that provides a single login capability by securely storing your IDP password in your Okta tenant to offer a one-click login to Safenames IDP, this will require you to maintain the user accounts in 2 places, while this is not a true SSO application it can still be a simple way to maintain a single password less login for your IDP accounts.

NOTE: Okta is not accepting any more SWA applications into their app directory. SWA is considered a legacy method.

Any clients who currently utilize SWA should switch to OIDC.

We are no longer supporting SWA method with Safenames IDP.

2.3 Okta SSO

A true single sign on application using OIDC protocol.

To activate SSO you will add an OIDC application to your Okta tenant, then grant your users access to this application or not as required to control your IDP access.

When attempting to login to the IDP with Okta credentials we will use OIDC to obtain permission from your Okta tenant user directory to either grant or deny IDP access.

Currently the application must be added manually to your tenant, instructions on how to do this are in the next steps, in the future we will automate the creation of Okta application automatically.

3 Okta SSO with OIDC Setup Instructions

3.1 Pre-Configuration

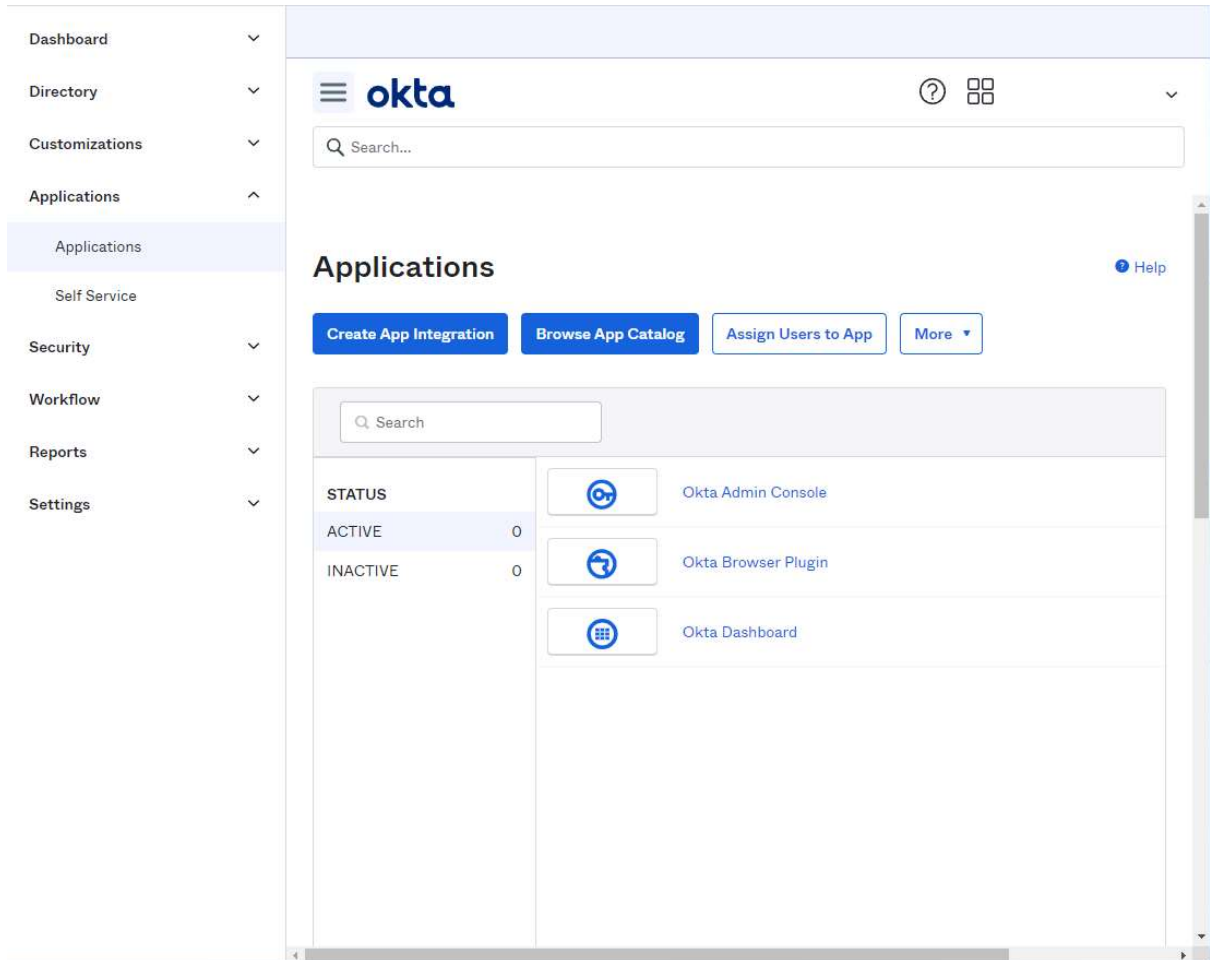
Before attempting to configure your Okta tenant for the Safenames IDP application we must assign you a unique client identifier that you will need to setup your tenant specific login and logout URI's

To obtain please contact your account manager who will open an onboarding request with tech support who will guide you through the setup and make the changes required to your IDP account to enable SSO access.

We will provide a 5-digit unique identifier, that you will need later in the setup section 4.5 to include in the sign-in / sign-out URL configuration.

3.2 Step 1 – Create the application in your Okta tenant

Login to your Okta tenant admin portal, select from the applications sub menu
Click the “Create App Integration” button



3.3 Step 2 - Select app integration type

Select the OIDC – OpenID Connect radio button, click Next

Create a new app integration x

Sign-in method

[Learn More](#) 

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

[Cancel](#)

[Next](#)

The IDP identity server is Open ID Connect only.

3.4 Step 3 – Select Application type

Select Web Application radio button and click Next

Create a new app integration X

Sign-in method

[Learn More](#) 

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

[Cancel](#)

[Next](#)

3.5 Step 4 - Configure the App Integration settings


The application must be configured to provide the correct data to our Identity server.

Enter your App integration name – Safenames IDP

New Web App Integration

General Settings

App integration name

Logo (Optional) 

Grant type [Learn More](#)

Client acting on behalf of itself

- Client Credentials

Client acting on behalf of a user

- Authorization Code
- Refresh Token
- Implicit (hybrid)

Ensure the following check boxes are selected

Grant type – Select

- Client Credentials
- Authorization Code
- Implicit (hybrid)

Sign-in redirect URIs - Enter

- Production `https://identity.safenames.com/safenames/{provided by Safenames}/signin`
- Staging `https://st-identity.safenames.com/safenames/{provided by Safenames}/signin`

You will require a client specific ID to identify your tenant sign-in redirect URIs. This ID is used uniquely identify your sign in and sign out URIs.

Safenames will provide this during onboarding of your tenant and must be entered into your application setup.

Sign-in redirect URIs

Allow wildcard * in sign-in URI redirect.

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

[Learn More](#)

Configure your sign-out URI with your Safenames client ID we provided.

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

[Learn More](#)

Sign-out redirect URIs - Enter

- Production `https://identity.safenames.com/safenames/{provided by Safenames}/signout-callback`
- Staging `https://st-identity.safenames.com/safenames/{provided by Safenames}/signout-callback`

Assignments

This section controls which users have access to the application. In order to use the application, your Okta users should be granted access individually to use SSO.

Select Skip group assignment for now, and click Save.

Assignments


Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

- Allow everyone in your organization to access
- Limit access to selected groups
- Skip group assignment for now

[Save](#) [Cancel](#)

Once the application has been configured, you may enter the assignments section and enable access for your specific users according to your security policy.




Safenames IDP

[Active](#) [View Logs](#)

[General](#) [Sign On](#) [Assignments](#) [Okta API Scopes](#)

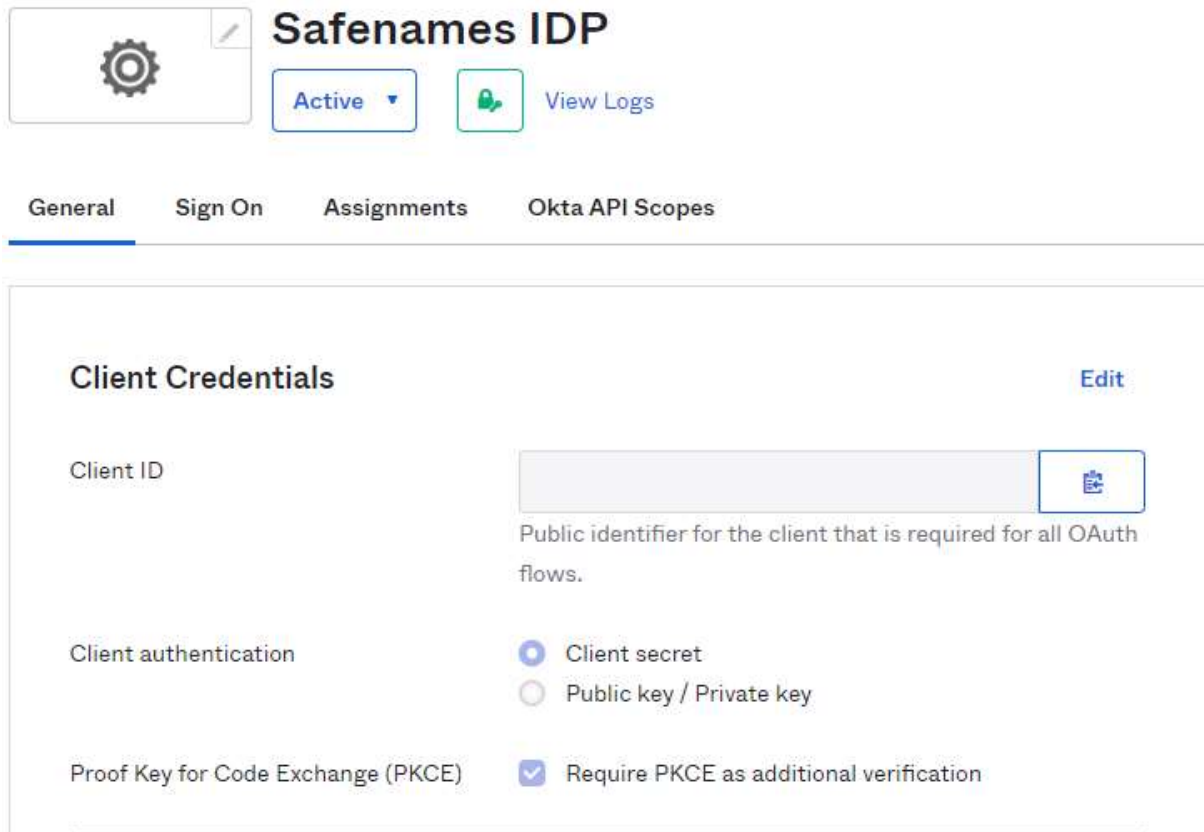
[Assign](#) [Convert assignments](#) [People](#)

Filters	Person	Type
People		Individual Edit Close
Groups		

3.6 Step 5 - Enable PKCE

IDP uses Proof Key for Code Exchange (PKCE) and must be enabled once your application has been configured.

Click the settings wheel of your application and tick the check box for PKCE.



The screenshot shows the configuration page for 'Safenames IDP'. At the top, there is a settings wheel icon, a status 'Active' dropdown, a 'View Logs' button, and tabs for 'General', 'Sign On', 'Assignments', and 'Okta API Scopes'. The 'General' tab is selected. Under the 'Client Credentials' section, there is an 'Edit' link. The 'Client ID' field is empty with a copy icon. Below it, the 'Client authentication' section has two radio buttons: 'Client secret' (selected) and 'Public key / Private key'. The 'Proof Key for Code Exchange (PKCE)' section has a checked checkbox for 'Require PKCE as additional verification'.

3.7 Step 6 - Set Login Initiated by

Click the settings wheel of your application and use the drop down to set the Login Initiated parameter to “Either Okta or App”

Login initiated by


3.8 Step 7 - Set Login URI

Set the Initiate Login URI

Initiate Login URI - Enter

- Production `https://idp.safenames.com?source={provided by safenames}`
- Staging `https://st-idp.safenames.com?source={provided by safenames}`

Click the settings wheel of your application and enter the URL

Initiate login URI 

`https://st-idp.safenames.com?source={provided by safen`

3.9 Logo (Optional)

We provide a logo that you can use on your application.

Download from here: -

[← Back to Applications](#)



Click the button on the application and upload our logo.

Safenames also provides a logo that you may upload if you wish, collect it at.

URL: <https://identity.safenames.com/images/safenames-logo-840-blue.png>

3.10 Post Configuration

To on-board your Okta tenant and custom application to IDP, Safenames will require the following information to be provided following the application configuration.

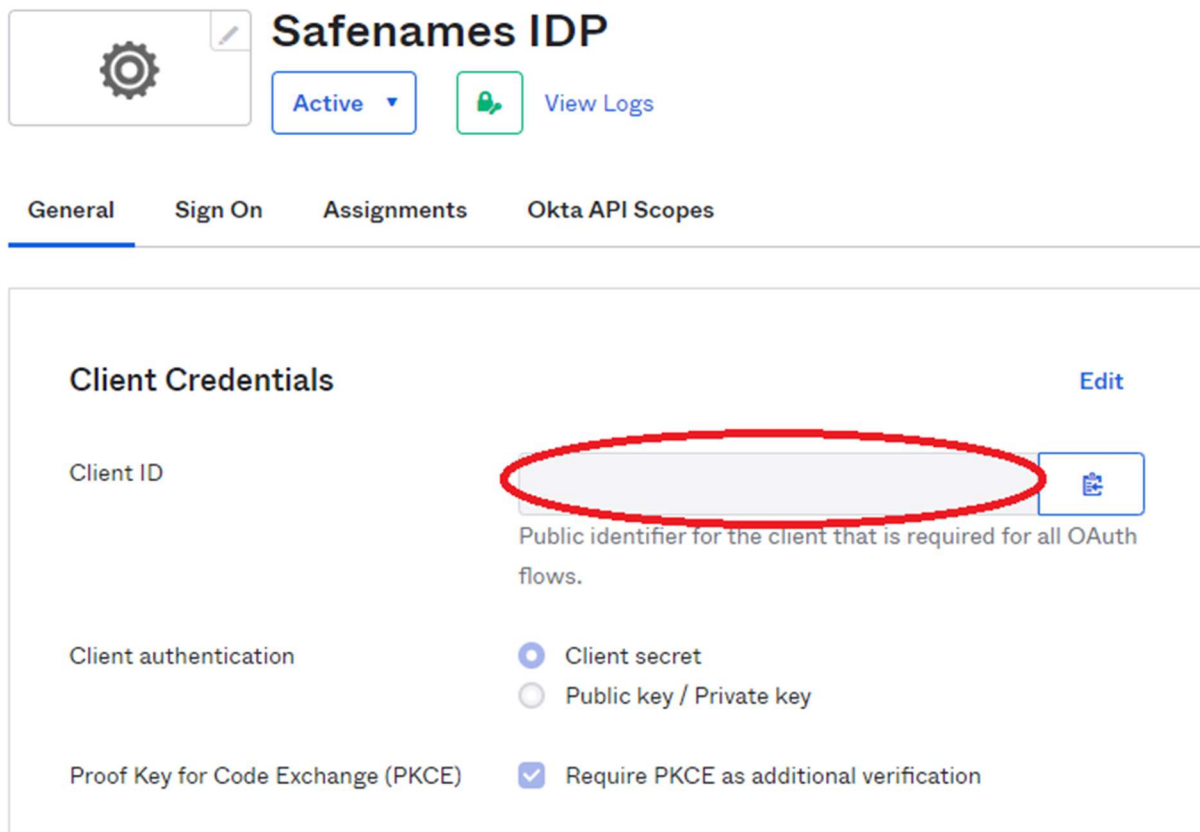
Once the application is created copy the following details and provide them to the Safenames tech support representative assigned to assist with your onboarding.

Safenames requires

- Your tenant ID usually in the form of [https://\[company\].okta.com](https://[company].okta.com)
- Client ID
- Client secrets

These secrets uniquely identify and secure your logon with us.

Client ID can be obtained here



Copy this value and provide to Safenames.

Client secrets can be obtained from here

CLIENT SECRETS

		Generate new secret	
Creation date	Secret		Status
Mar 6, 2023	 	Active ▾

If at any time you regenerate your secret keys, you will need to provide these to Safenames.

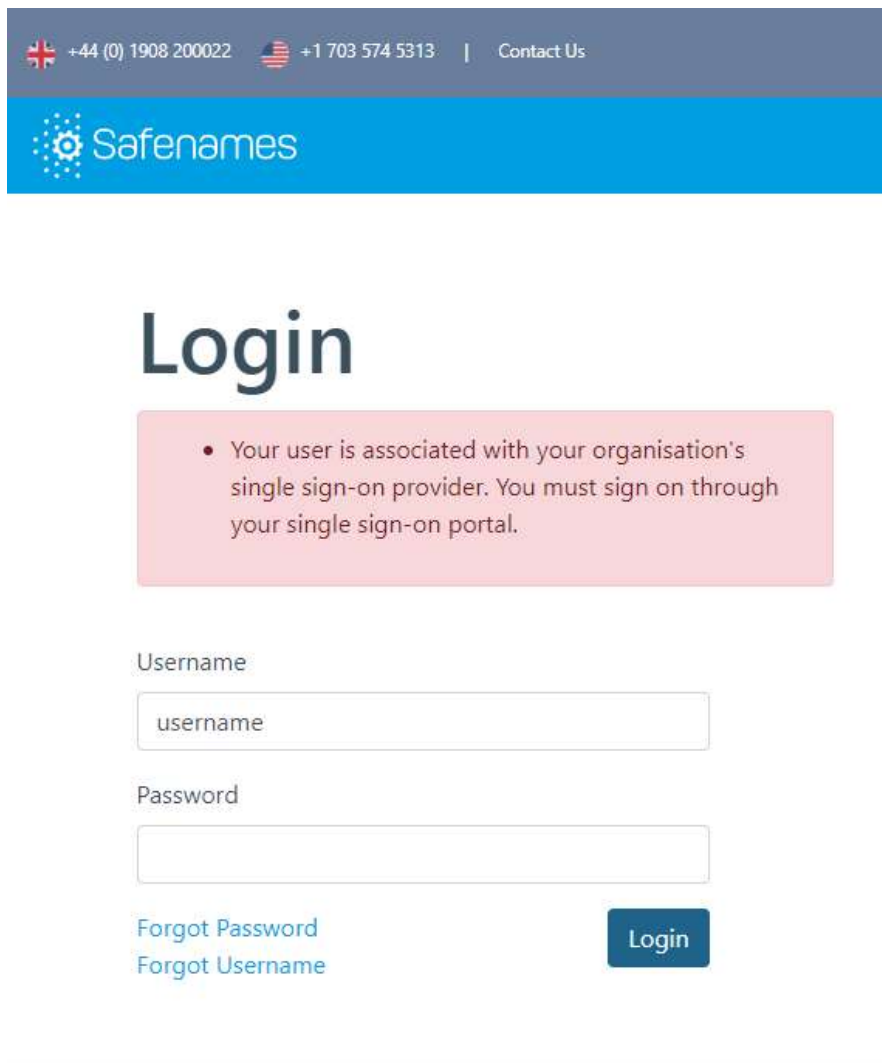
Copy this value and provide to Safenames.

3.11 Okta User account synchronization

Okta user accounts are usually identified by an email address and IDP accounts are usually identify by a username, therefore we need to map them together in the IDP.

Please provide Safenames with a list of your Okta user email address and the IDP accounts they should be mapped to so that they can be enabled for SSO.

Once users are enabled for IDP access through SSO they will no longer be able to access IDP using the old credentials. If you attempt to login directly to IDP you will receive the following error message.



4 Azure

Azure Active Directory (Azure AD), part of Microsoft, is an enterprise identity service that provides single sign-on, multifactor authentication, and conditional access to thousands of applications.

4.1 Azure SSO application setup

To enable Single Sign-on(SSO) for Azure a single tenant application should be created and users from that tenant granted permission to use.

Once the application has been configured Safenames requires the following information from your tenant to be provided to us, so that we can connect your IDP account to your Azure tenant.

- Tenant ID – the unique ID that identifies your account on Azure
- Application ID – the unique ID of the created IDP application
- Client secret key value – the unique secret key

When these 3 values are combined they ensure that only your Azure tenant and its users are able to access your Safenames IDP account.

The following steps will guide you through adding an application to your tenant and the configuration steps needed to ensure it will be compatible with Safenames Identity server.

4.2 Pre-configuration

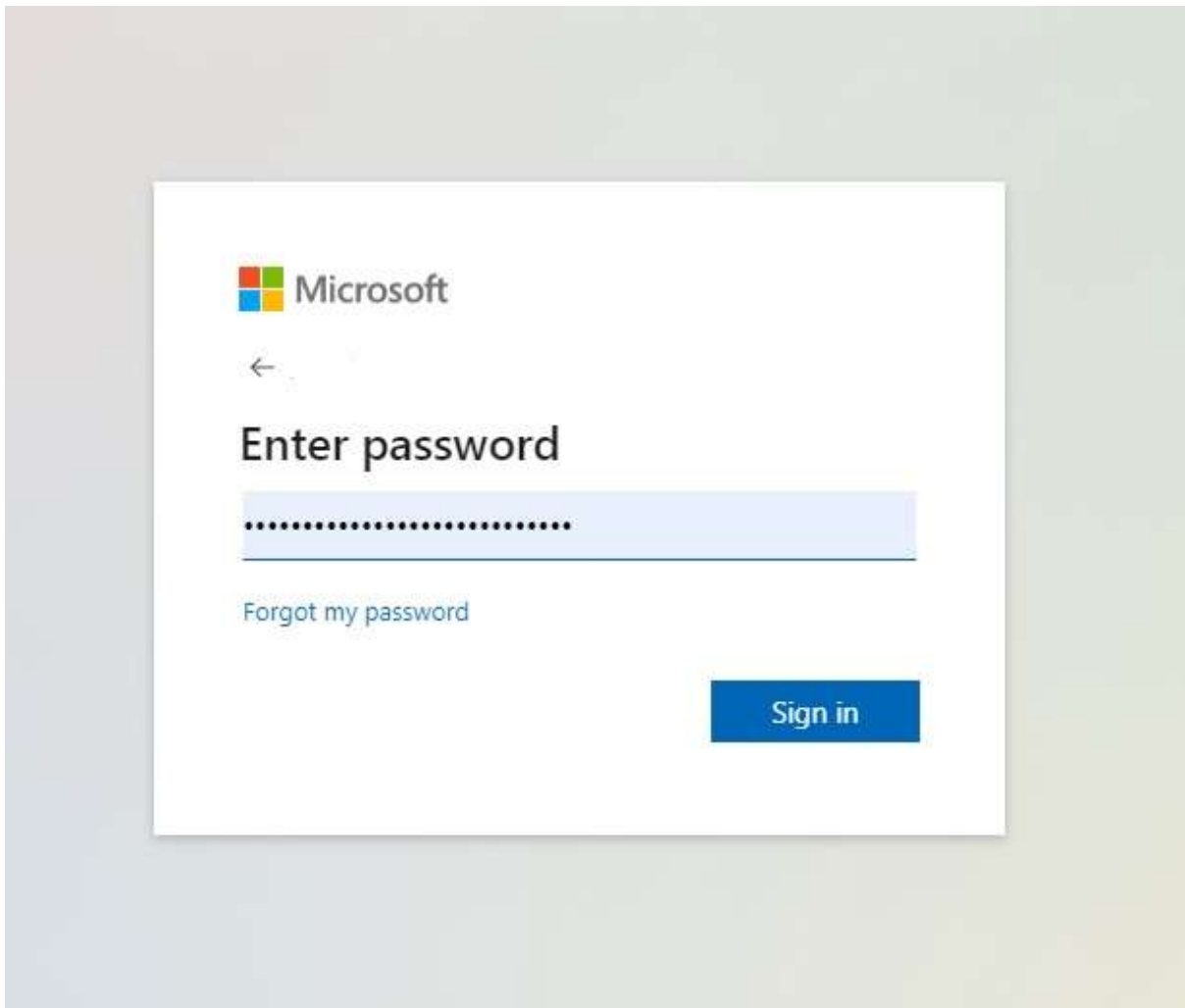
Before attempting to configure your Azure tenant for the Safenames IDP application we must assign you a unique client identifier that you will need to use on your tenant specific login and logout URI's

To obtain please contact your account manager who will open an onboarding request with tech support who will guide you through the setup and make the changes required to your IDP account to enable SSO access.

We will provide a 5-digit unique identifier, that you will need later in the setup section 4.9 to include in the sign-in / sign-out URL configuration.

4.3 Step 1 – Access Azure Admin Portal

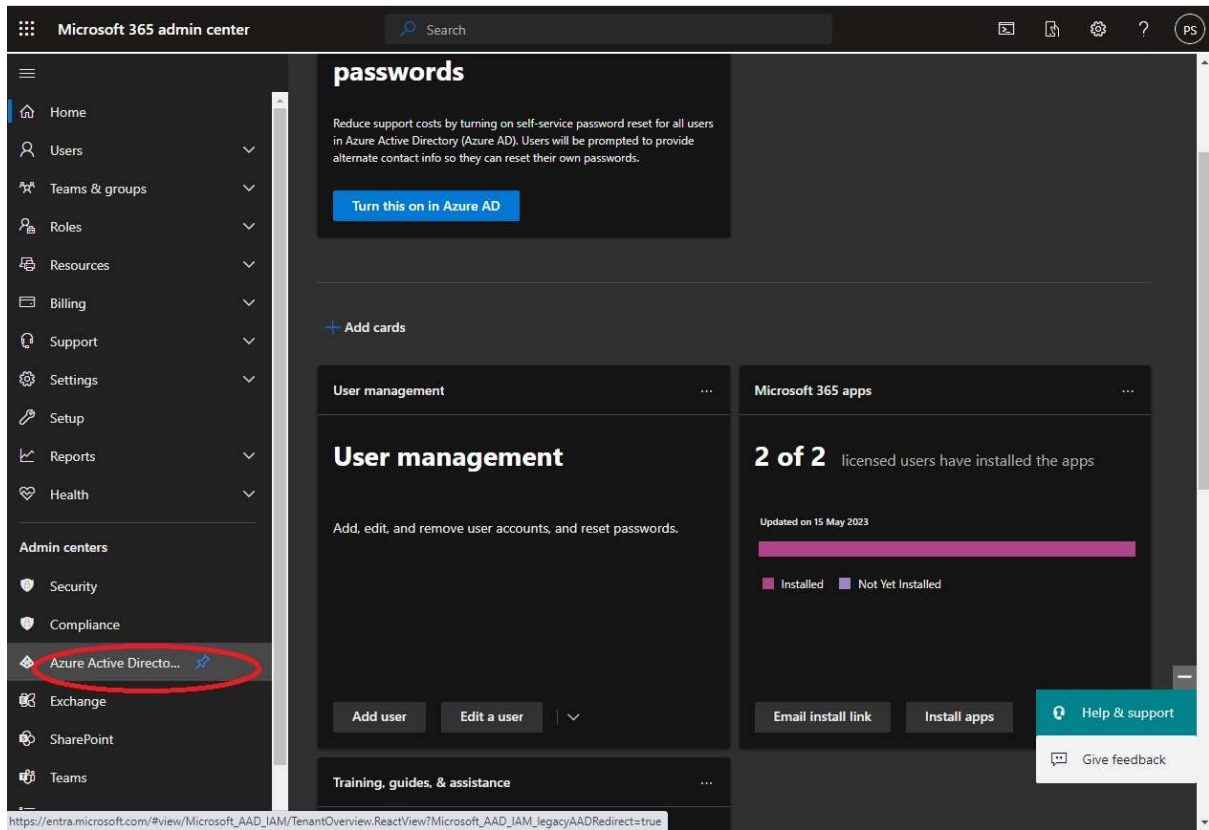
Access your Microsoft Azure Tennant admin portal
Usually this can be found at admin.microsoft.com login with your administrator credentials.



4.4 Step 2 – Access your Azure Active Directory

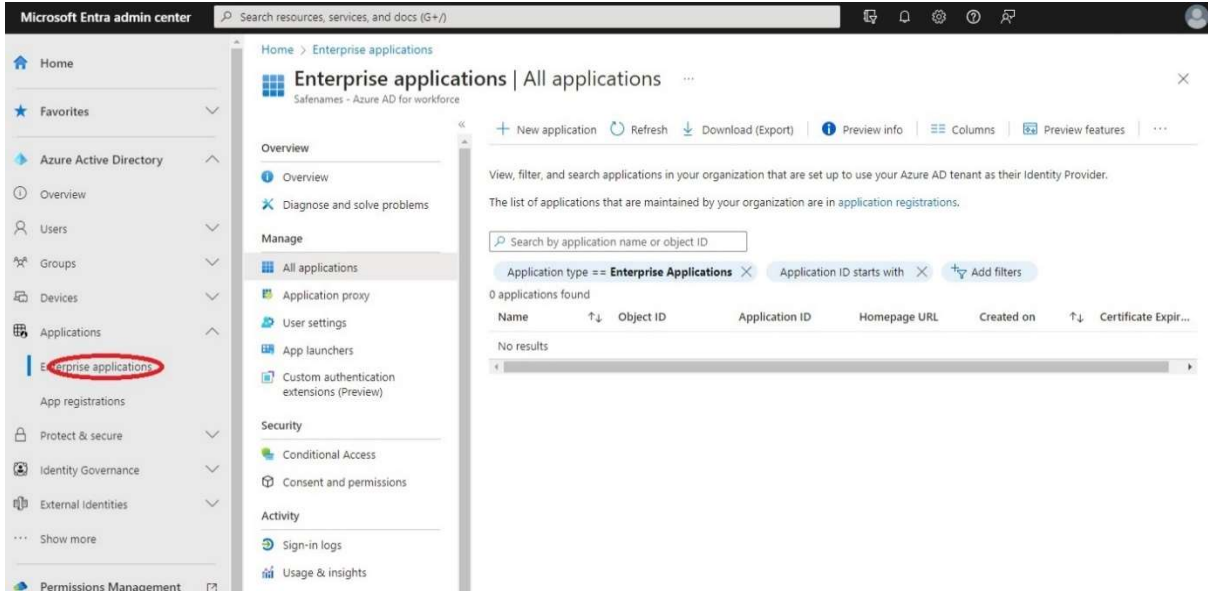
After logging into your Azure admin portal, you should have the following screen.

Select Azure Active Directory to manage your applications and users.
This will open up the Azure Active directory management portal in a new window.



4.5 Step 3 – Select Enterprise Applications

From the left hand nav menu;
Select Enterprise Applications to display your existing applications.



Existing applications will be displayed in the right hand pane.

4.6 Step 5 - Create new Application

Select “New Application” from the top nav to enter the new application wizard.

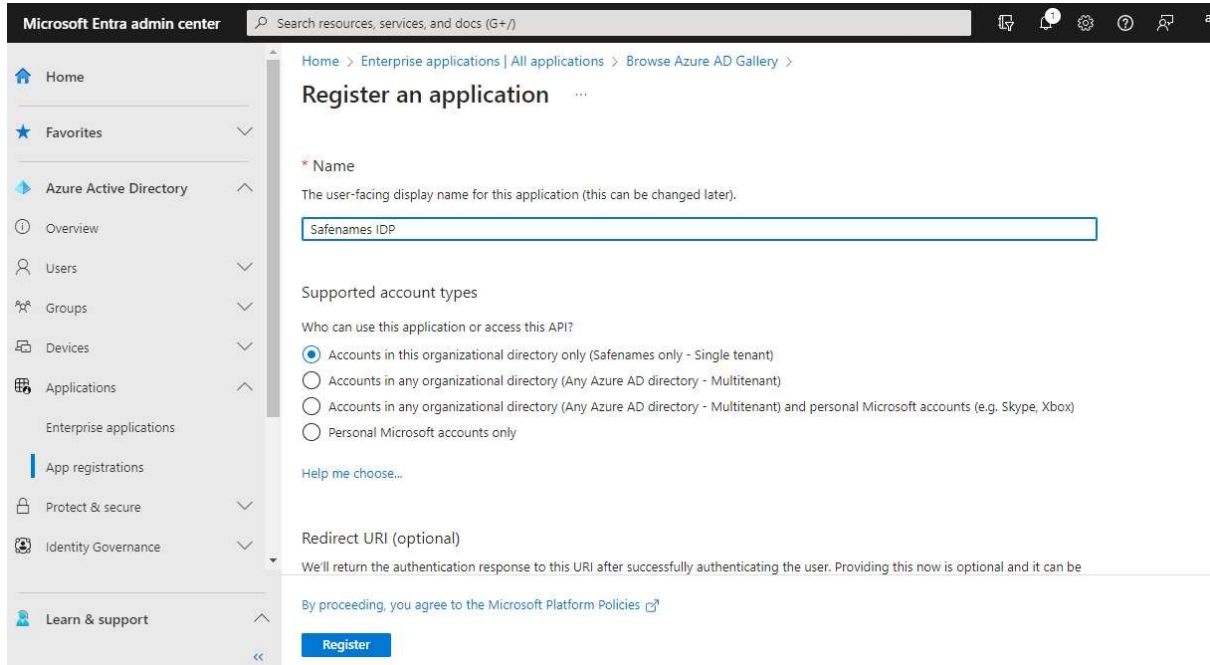
The screenshot shows a dialog box titled "Create your own application" with a close button (X) in the top right corner. Below the title is a link "Got feedback?". The main text reads: "If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here." Below this is the question "What's the name of your app?" followed by a text input field containing "Safenames IDP" and a checkmark icon. Underneath is the question "What are you looking to do with your application?" followed by three radio button options: "Configure Application Proxy for secure remote access to an on-premises application", "Register an application to integrate with Azure AD (App you're developing)" (which is selected), and "Integrate any other application you don't find in the gallery (Non-gallery)". At the bottom left of the dialog is a blue "Create" button.

Name your application “Safenames IDP”, and select the radio button “Register an application to integrate with Azure AD (App you're developing)”

4.7 Step 6 – Select Single Tenant

Select Accounts in this organizational directory only.

This will limit the application only to your tenant users.



Click the register button to create your custom application.

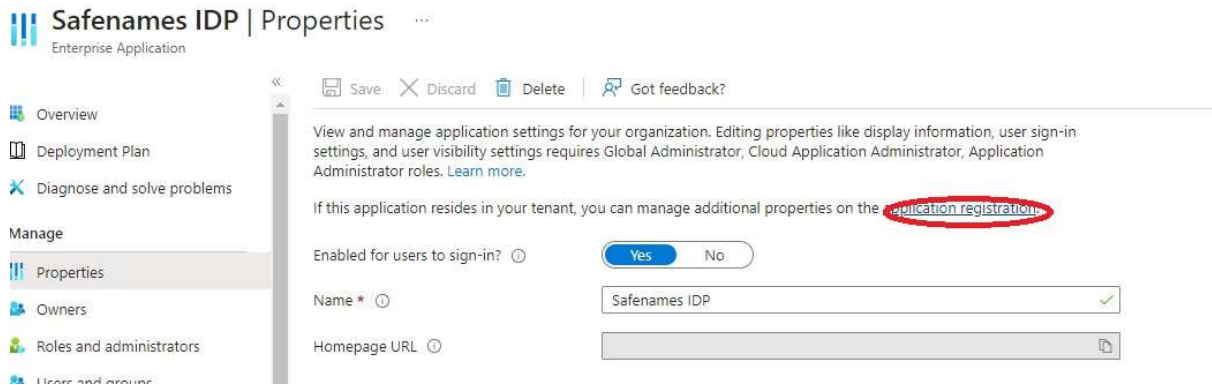
In the next steps the application will be configure to be compatible with the IDP.

4.8 Step 7 - Configure “Safenames IDP” Application

To configure the application

From the "Manage" left hand menu categories select "Properties"

Then select “application registration”



4.9 Step 8 – Configuration Settings

Enter the following values in the fields

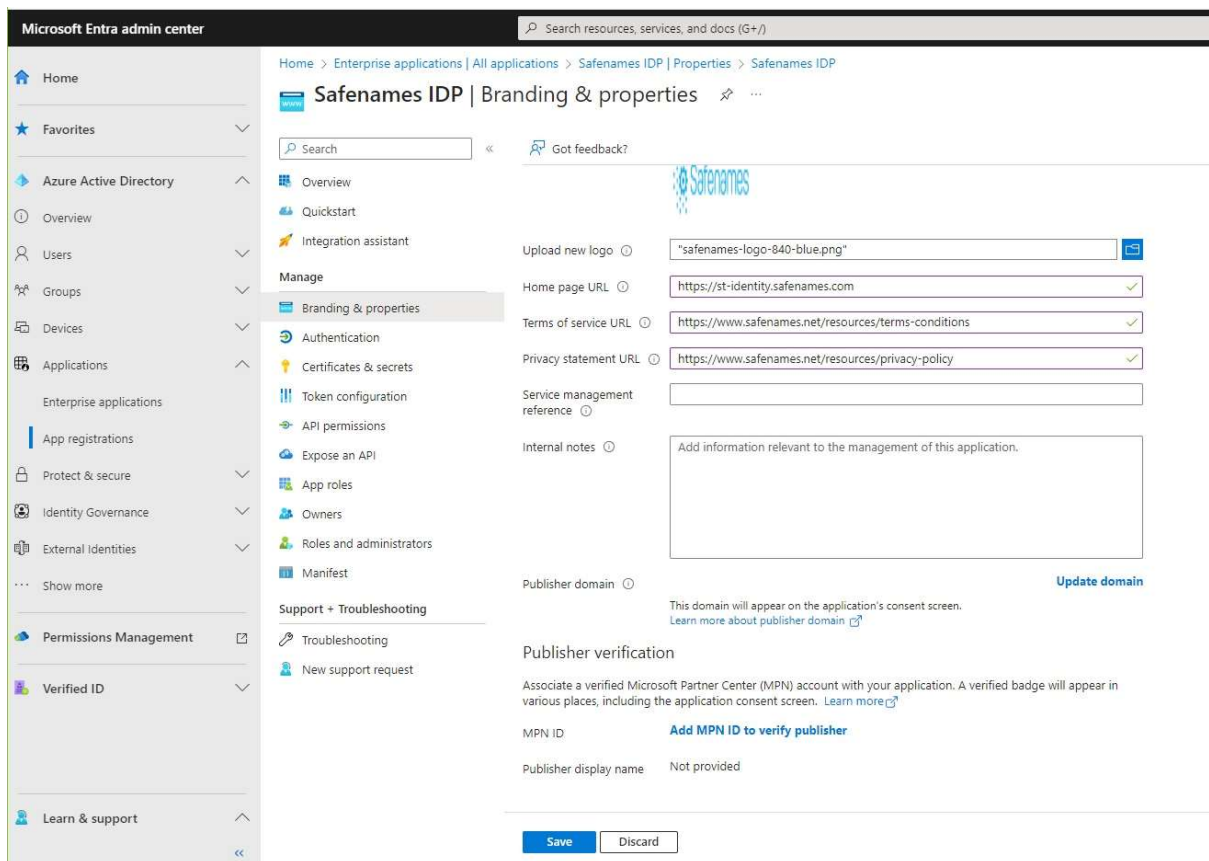
Safenames provides a production and staging environment for prior testing.

Homepage URL:

- Staging - <https://st-idp.safenames.com/?source={provided by safenames}>
- Production - <https://idp.safenames.com/?source={provided by safenames}>

Terms of service URL: <https://www.safenames.net/resources/terms-conditions>

Privacy statement URL: <https://www.safenames.net/resources/privacy-policy>



Safenames also provides a logo that you may upload if you wish, collect it at.

URL: <https://identity.safenames.com/images/safenames-logo-840-blue.png>

4.10 Step 9 – Create Client Secrets

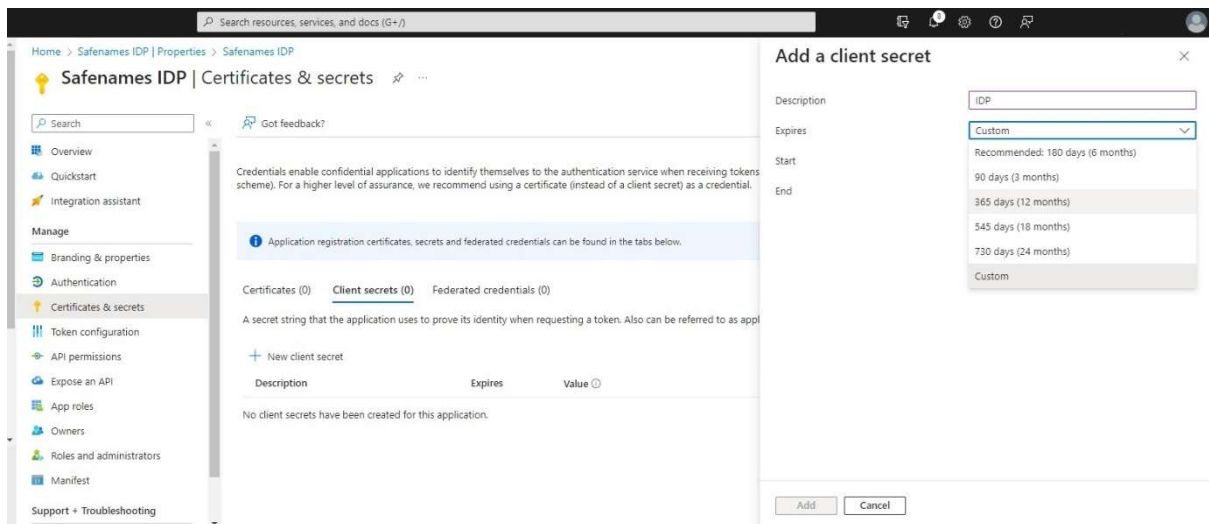
To secure your application a client secret must be created and shared with Safenames.

The client secret ensures that only your application and users have access to your IDP account.

Safenames recommends setting the lifetime to 12 months. When keys rollover they will need to be provided, in order to maintain IDP access.

The secret is only available at the time of creation, so ensure to save it as you cannot view it later. If you don't save, its fine to just delete the client secret and re-add it.

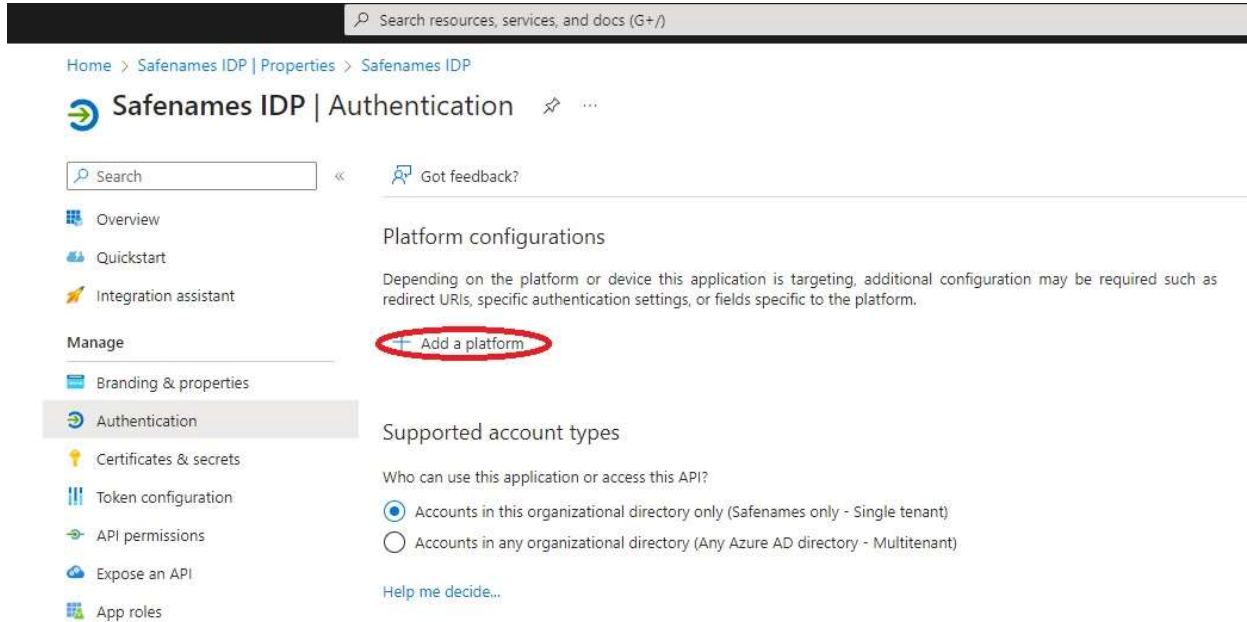
Please provide the value of your client secret to Safenames once created.



4.11 Step 10 - Set Authentication URI

Next set the authentication platform URL to Safenames identity servers.

From the Manage menu, select authentication / Add a platform



Leave supported account types set to single tenant mode.

From the Web Platform types offered, select "Web" and add the Redirect URIs for either our staging environment or production. Ensure you add your unique identifier provided by Safenames.

- Staging – <https://st-identity.safenames.com/safenames/{provided by Safenames}/signin>
- Production - <https://identity.safenames.com/safenames/{provided by Safenames}/signin>

Configure your Front-Channel logout URL

- Staging – <https://st-identity.safenames.com/safenames/{provided by Safenames}/signout-callback>
- Production - <https://identity.safenames.com/safenames/{provided by Safenames}/signout-callback>

Enter the URIs and Press "configure" to save

Configure Web ✕

[← All platforms](#) [Quickstart](#) [Docs](#)

*** Redirect URIs**

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

 ✓

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

Access tokens (used for implicit flows)

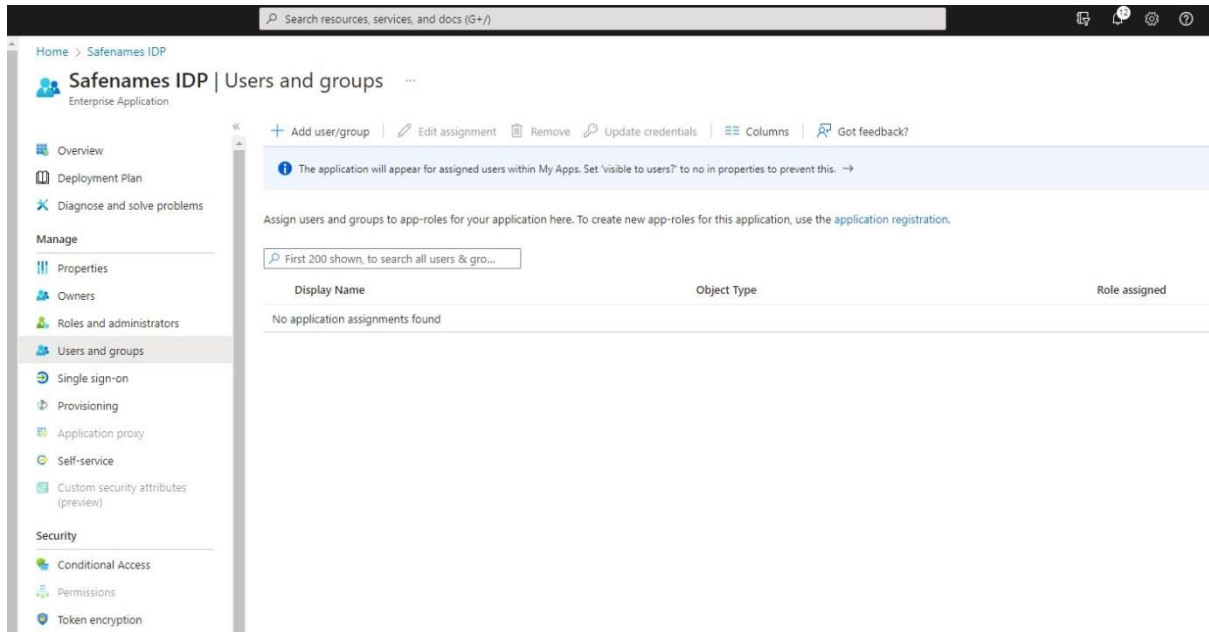
ID tokens (used for implicit and hybrid flows)

4.12 Step 11 - User Permissions

Once the application is created and configured for use, the final step is to grant your users access.

Select “Users and Groups” from left hand menu.

Click “+ Add user/group” and grant your users access to use the application.



Safenames will require your list of user names only, to join them to your IDP account users.

Safenames IDP has 5 roles 1 through 5 that grant access to certain functionality

- Level 1 Administrator
- Level 2 Registration
- Level 3 Billing
- Level 4 Technical
- Level 5 View Only

Users need assigned to a role on the Safenames side to enable functionality.

Please provide to your account manager, your usernames with email address and requested IDP security level.

4.13 Step 12 – Post Configuration

To complete the setup please provide Safenames with the following information.

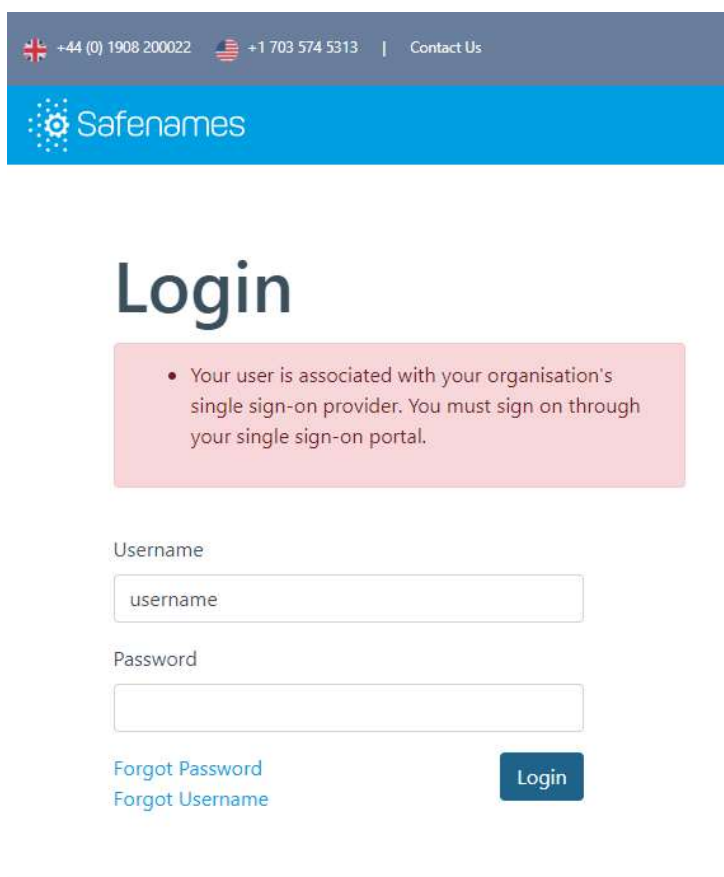
- Tenant ID – the unique ID that identifies your account on Azure
- Application ID – the unique ID of the created IDP application
- Client secret key value – the unique secret key
- List of your Azure tenant users and permission level 1-5

Azure user accounts are usually identified by an email address and IDP accounts are usually identify by a username, therefore we need to map them together in the IDP.

Please provide Safenames with a list of your Azure user email address and the IDP accounts they should be mapped to so that they can be enabled for SSO.

Once users are enabled for IDP access through SSO they will no longer be able to access IDP using the old credentials. If you attempt to login directly to IDP you will receive the following error message.

4.14 Azure User account synchronization



5 Onelogin

OneLogin simplifies identity management with secure, one-click access, for employees, customers and partners, through all device types, to all enterprise cloud and on-premises applications.

OneLogin enables IT identity policy enforcement and instantly disables app access for employees who leave or change roles in real-time by removing them from Active Directory. Take control over application access, quickly on- and off-board team members, and provide end-users with easy access to all their applications on every device. Extend your on-premises security model to the cloud in minutes.

5.1 Pre-Configuration

Before attempting to configure your Onelogin tenant for the Safenames IDP application we must assign you a unique client identifier that you will need to use on your tenant specific login and logout URI's

To obtain please contact your account manager who will open an onboarding request with tech support who will guide you through the setup and make the changes required to your IDP account to enable SSO access.

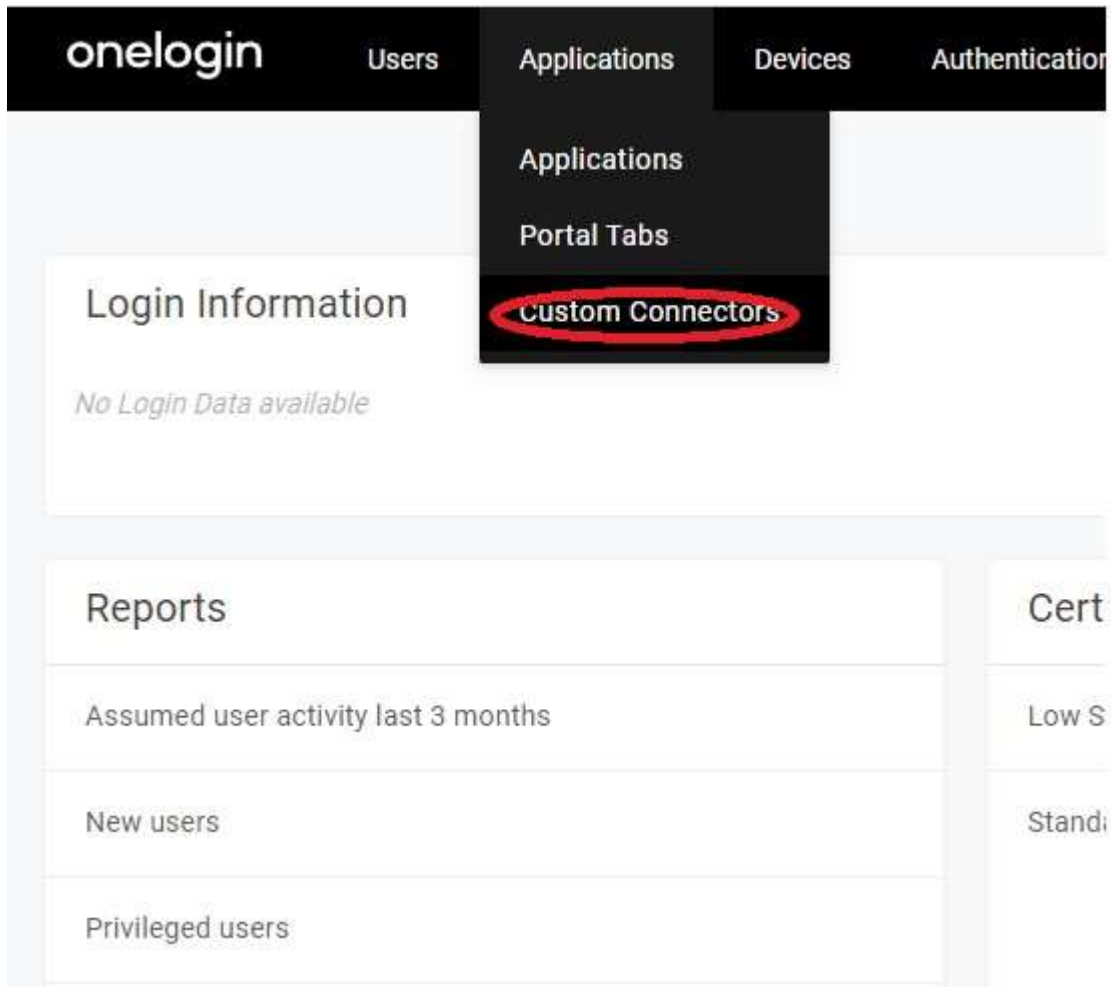
We will provide a 5-digit unique identifier, that you will need later in the setup section include in the sign-in / sign-out URL configuration.

To enable Onelogin the steps required are to first create a custom connector then an OIDC application.

5.2 Step 1 - Create Custom Connector

Login to your tenant OneLogin administrator panel.

From the application menu select customer connector

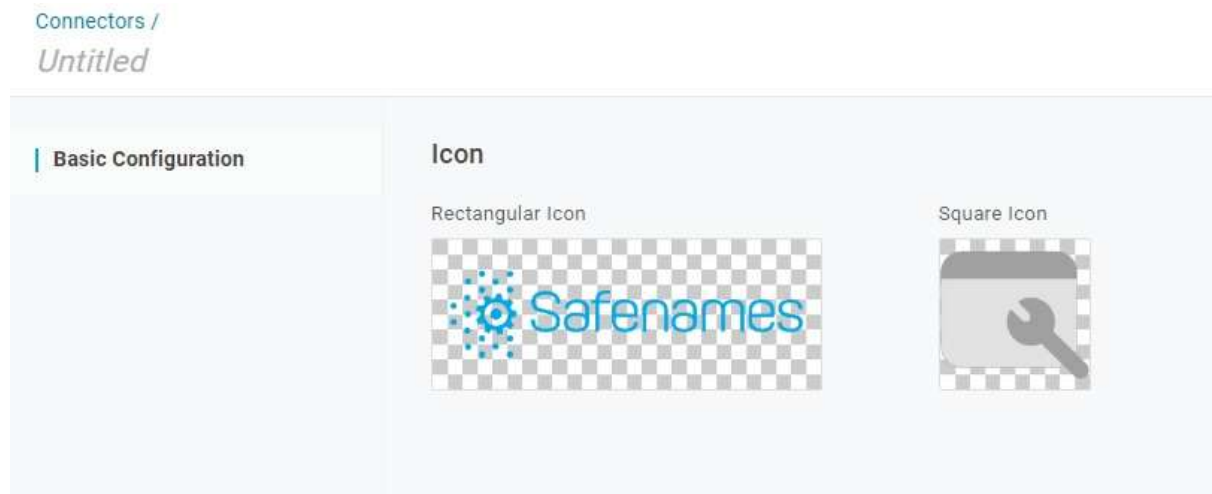


To configure the connector, add the following settings

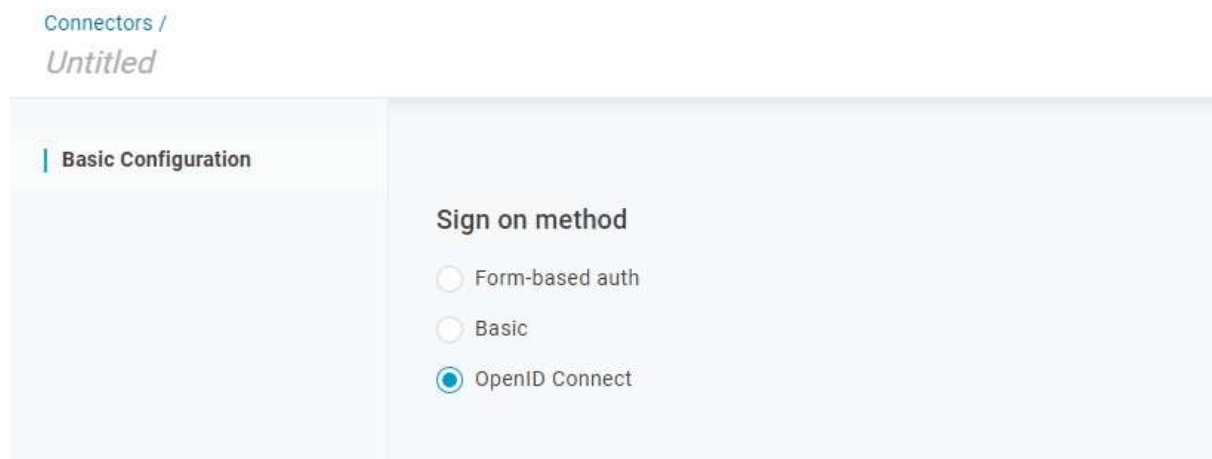
Icon – Select Rectangular Icon

Safenames provides a logo that you may upload if you wish, collect it at.

URL: <https://identity.safenames.com/images/safenames-logo-840-blue.png>



Sign on Method – Select OpenID Connect



Configure URI's

Safenames uses customer specific ID's, to identity tenants.
Please obtain from Safenames before starting configuration

Redirect URL –

- Production - <https://identity.safenames.com/safenames/{provided by Safenames}/signin>
- Staging - <https://st-identity.safenames.com/safenames/{provided by Safenames}/signin>

Post Logout Redirect URL

- Production - <https://identity.safenames.com/safenames/{provided by Safenames}/signout-callback>
- Staging - <https://st-identity.safenames.com/safenames/{provided by Safenames}/signout-callback>

Signing Algorithm

Should be RS256

Login URL

Production - <https://idp.safenames.com/?source={custom id}>
Staging - <https://idp.safenames.com/?source={custom id}>

Connectors /
Untitled

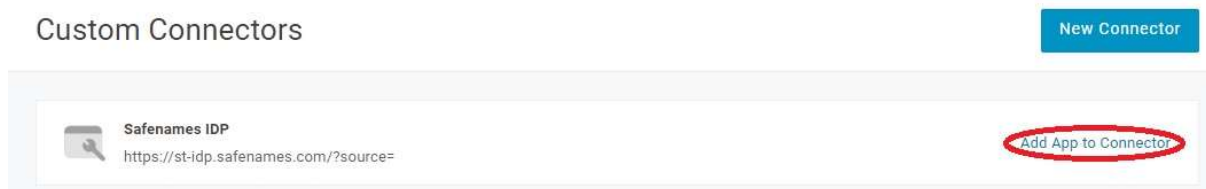
Basic Configuration	<h3>OpenID Connect</h3> <p>Redirect URI</p> <input type="text" value="https://identity.safenames.com/signin-oidc/{cus"/> <p>Post Logout Redirect URI</p> <input type="text" value="https://identity.safenames.com/signout-oidc/{cu"/> <p>Signing Algorithm</p> <input type="text" value="RS256"/> <h3>Login URL</h3> <p>Login url</p> <input type="text" value="https://idp.safenames.com/?source={custom id}"/>
----------------------------	---

Click Save to add your connector.

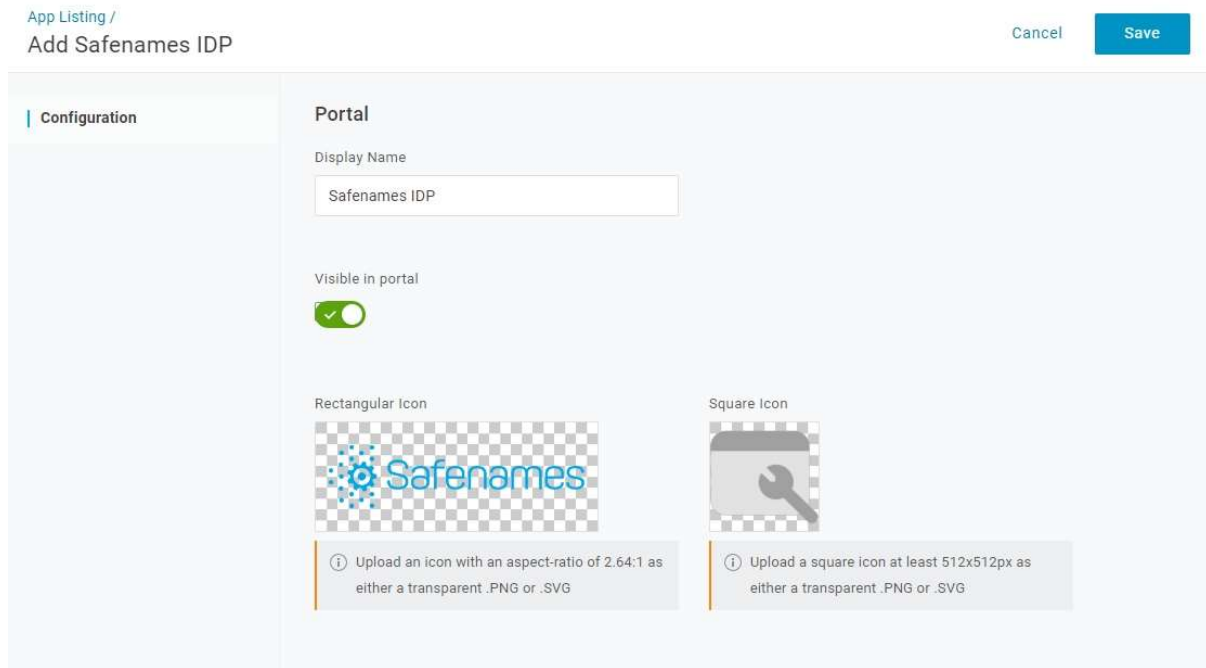
5.3 Step 2 - Create Application

Once you customer connector has been created.

Click “Add App to Connector”



Call the application Safenames IDP, ensure visible in portal is selected and upload our Icon.



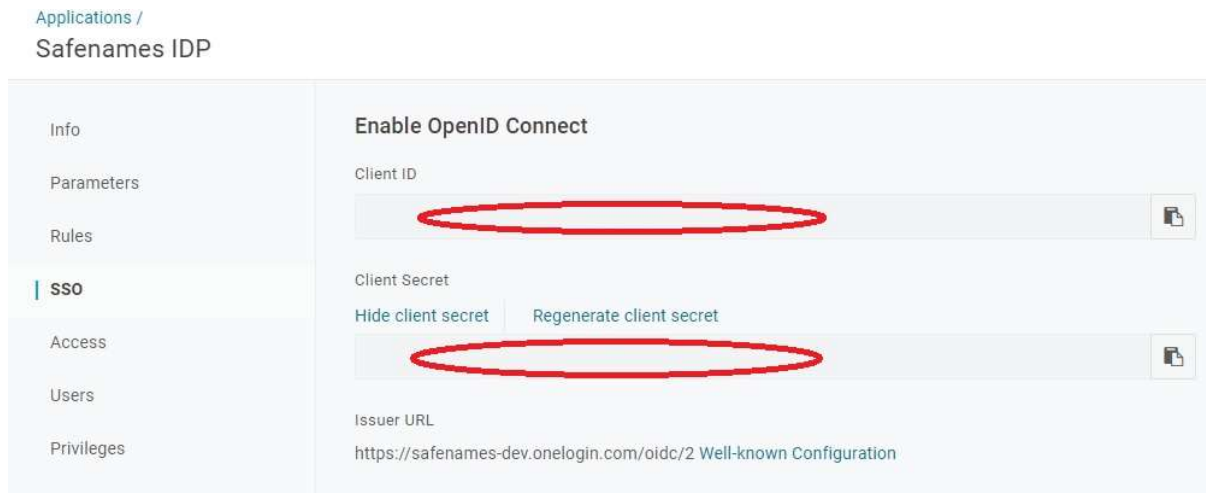
Click Save to continue to the application configuration section.

Additional settings need to be made on the application.

Select SSO Menu Option

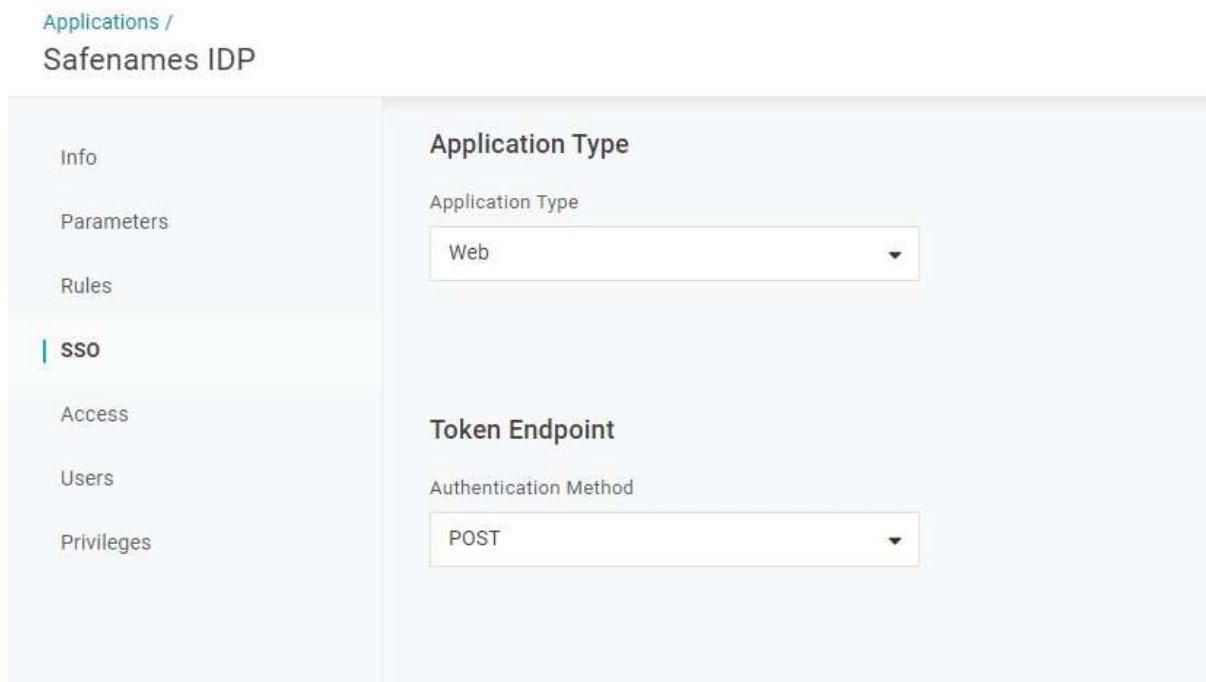
Record the **Client ID** and provide it to Safenames during onboarding call

Click the **“Show client secret”** and Record the key, provide it to Safenames during the onboarding call.



Set **“Application Type”** from the dropdown to **“Web”**

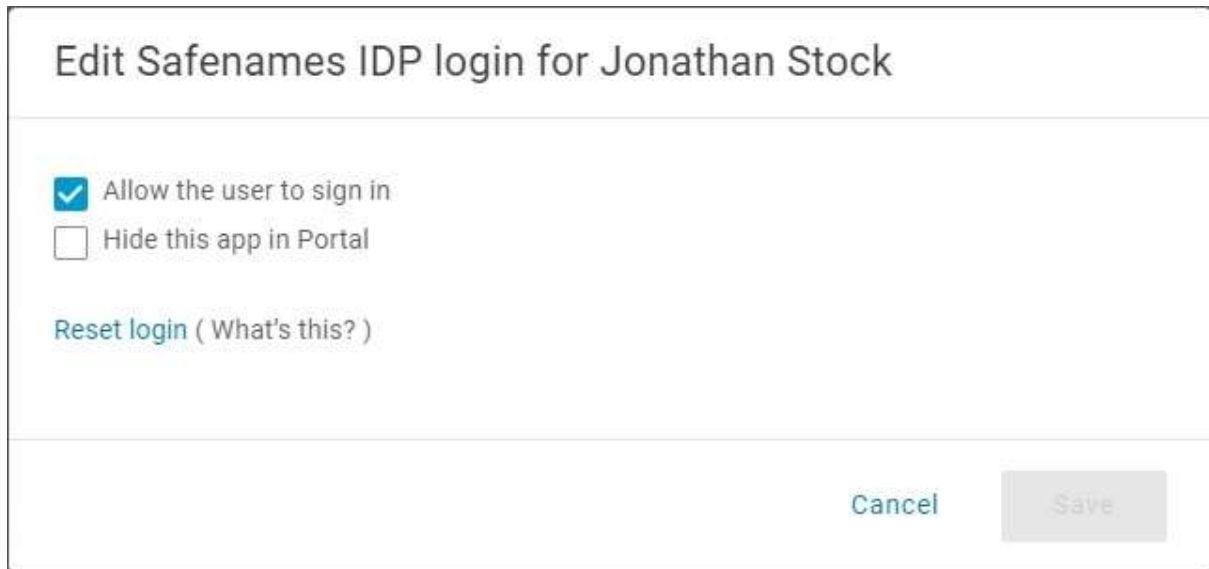
Set **“Token Endpoint”** from the dropdown to **“POST”**



5.4 Step 3 - Users Permissions

Before a user may use the newly create application they must be granted access to use it.

From the Users menu option select your users and grant access to the application



Edit Safenames IDP login for Jonathan Stock

Allow the user to sign in

Hide this app in Portal

[Reset login \(What's this? \)](#)

Cancel Save

5.5 Step 4 Post-Configuration

Book an onboarding call through your account manager.

Safenames will require the following information to onboard your tenant, available from the SSO menu option

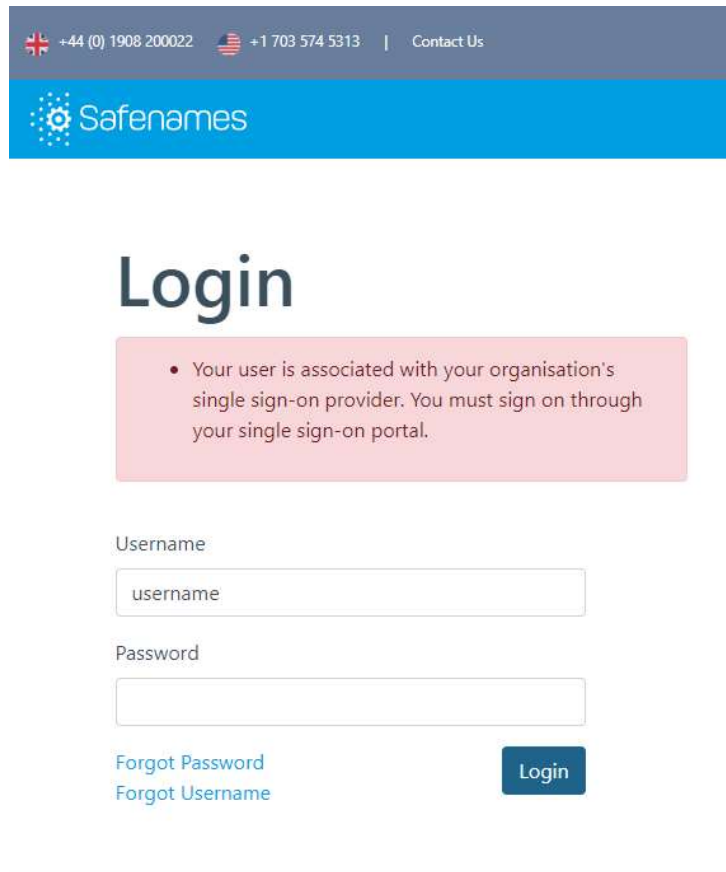
- Client ID
- Client Secret
- Issuer URL

5.6 OneLogin User account synchronization

OneLogin user accounts are usually identified by an email address and IDP accounts are usually identify by a username, therefore we need to map them together in the IDP.

Please provide Safenames with a list of your OneLogin user email address and the IDP accounts they should be mapped to so that they can be enabled for SSO.

Once users are enabled for IDP access through SSO they will no longer be able to access IDP using the old credentials. If you attempt to login directly to IDP you will receive the following error message.



6 SSO development Roadmap

6.1 Okta

This represents the first release of our SSO integration with Okta, work is continuing to provide enhanced functionality

Safenames development roadmap for Okta SSO functionality.

- Application to be included in Okta OIN (Okta Integration Network)
- Automated setup of the application in Okta tenant
- IDP control panel to sync users and enable / disable SSO
- Deeper permissions control of IDP functionality

6.2 Azure

This represents the first release of our SSO integration with Microsoft Azure, work is continuing to provide enhanced functionality

Safenames development roadmap for Azure SSO functionality.

- Application to be included in Azure AD App Gallery
- Automated setup of the application in Azure tenant
- IDP control panel to sync users and enable / disable SSO
- Deeper permissions control of IDP functionality through Azure roles and groups