

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

<b>Document Classification:</b>	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	0	VERVIEW	.4
2	0	KTA	5
	2.1	OKTA INTEGRATION OPTIONS	5
	2.2	OKTA SWA	. 5
	2.3	OKTA SSO	. 5
3	0	KTA SSO WITH OIDC SETUP INSTRUCTIONS	6
	31	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	A	ZURE	18
	41	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	0	NELOGIN	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	SS	SO DEVELOPMENT ROADMAP	40
	6.1	ОКТА	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 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 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 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

Dashboard	~		
Directory	~	≡ okta ⑦ ⊞	×
Customizations	~	Q Search	
Applications	^		
Applications		Applications	P Help
Self Service			Theip
Security	~	Create App Integration Browse App Catalog Assign Users to App More *	
Workflow	~		
Reports	~	- Search	
Settings	~	STATUS Okta Admin Console	
		ACTIVE 0	
		INACTIVE 0 Okta Browser Plugin	
		Okta Dashboard	
			•

# 3.3 Step 2 - Select app integration type

# Select the OIDC - OpenID Connect radio button, click Next

#### Create a new app integration

×

# Sign-in method O OIDC - OpenID Connect Learn More C 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 Ne

The IDP identity server is Open ID Connect only.

#### Step 3 – Select Application type 3.4

Select Web Application radio button and click Next

#### × Create a new app integration OIDC - OpenID Connect Sign-in method Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API Learn More 🖸 endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget. O 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. O API Services Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication. Application type O Web Application Server-side applications where authentication and tokens are handled on the What kind of application are you trying to integrate server (for example, Go, Java, ASP.Net, Node.js, PHP) with Okta? Single-Page Application Specifying an application type customizes your Single-page web applications that run in the browser where the client receives experience and provides the best configuration, SDK, tokens (for example, Javascript, Angular, React, Vue) and sample recommendations. 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

App integration name	Safenames IDP	
Logo (Optional)		
	(Q)	
Grant type	Client acting on behalf of itself	
Learn More	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	https://st-identity.safenames.com/signin-oidc/{provided by safename	×
Learn More	+ Add URI	

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



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.



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

General	Sign On Assignments Okta AP	I Scopes	
Assign 🔻	Convert assignments 🔹	Q Search	People •
Filters	Person	Туре	
People Groups	1	Individual	/ ×

#### 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.

Safename Active	View Logs
neral Sign On Assignments	Okta API Scopes
Client Credentials	Edit
Client ID	Ē
	Public identifier for the client that is required for all OAuth flows.
Client authentication	<ul> <li>Client secret</li> <li>Public key / Private key</li> </ul>

# 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	Either Okta or App	•

#### 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: -



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 <a href="https://fcompany].okta.com">https://fcompany].okta.com</a>
- Client ID
- Client secrets

These secrets uniquely identify and secure your logon with us.

Client ID can be obtained here

Safename	SIDP View Logs
eneral Sign On Assignments	Okta API Scopes
Client Credentials	Edit
Client ID	Public identifier for the client that is required for all OAuth flows.
Client authentication	<ul> <li>Client secret</li> <li>Public key / Private key</li> </ul>
Proof Key for Code Exchange (PKCE)	Require PKCE as additional verification

Copy this value and provide to Safenames.

# Client secrets can be obtained from here

#### CLIENT SECRETS

		Ge	nerate r	new secret
Creation date	Secret			Status
Mar 6, 2023	*****	0	除	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.

+44 (0) 1908 200022 🚔 +1 703 574 5313   Contact Us
Safenames
Login
<ul> <li>Your user is associated with your organisation's single sign-on provider. You must sign on through your single sign-on portal.</li> </ul>
Username
Password
Forgot Password Forgot Username

# 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.

Microsoft	
Enter password	
Forgot my password	
	Sign in

# 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.

	Microsoft 365 admin center		ы 🕼 🎯 ? (рз)
≡		passwords	•
ඛ	Home	<ul> <li>Reduce support costs by turning on self-service password reset for all users</li> </ul>	
R	Users 🗸	in Azure Active Directory (Azure AD). Users will be prompted to provide alternate contact info so they can reset their own passwords.	
ጽ	Teams & groups 🛛 🗸 🗸	Turn this on in Azure AD	
ዲ	Roles 🗸 🗸		
퉉	Resources 🗸 🗸		
	Billing Y		
0	Support Y		
ŝ	Settings 🗸 🗸	User management	Microsoft 365 apps
Þ	Setup		
Ł	Reports 🗸 🗸	User management	2 of 2 licensed users have installed the apps
Ş	Health 🗸 🗸		
Adr	nin centers	Add, edit, and remove user accounts, and reset passwords.	
۲	Security		Installed Not Yet Installed
۲	Compliance		
۲	Azure Active Directo 🔗		
68	Exchange	Add user Edit a user 🗸	Email install link Install apps Q Help & support
¢	SharePoint		
<b>v</b> îî	Teams	Training, guides, & assistance	Give feedback
https:/	/entra.microsoft.com/#view/Microsoft_AAI	M/TenantOverview.ReactView?Microsoft_AAD_IAM_legacyAADRedirect=true	

# 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.



Name your application "Safenames IDP", and select the radio button "Register an application to integrate with Azure AD (App your 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"

Safenames IDP   Pr Enterprise Application	roperties …		
Overview     Deployment Plan     Diagnose and solve problems	Save X Discard Delete View and manage application settings f settings, and user visibility settings requ Administrator roles. Learn more. If this application resides in your tenan	Got feedback? for your organization. Editing properties like display inform uires Global Administrator, Cloud Application Administrator t, you can manage additional properties on the <u>capication</u>	nation, user sign-in or, Application n registration.
Properties	Enabled for users to sign-in? ①	Yes No	
🔒 Owners	Name * 🕜	Safenames IDP	*
🝰 Roles and administrators	Homepage URL ①		D
R Users and esource			

# 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 <u>https://idp.safenames.com</u>/?source={provided by safenames}

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

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

Microsoft Entra admin center		𝒫 Search resources, services	tes, and docs (G+/)
1 Home	Home > Enterprise applications   All app	lications > Safenames IDP nding & proper	Properties > Safenames IDP ties ≉ …
★ Favorites	✓	Sot feedback?	
Azure Active Directory     Overview	<ul> <li>Overview</li> <li>Quickstart</li> </ul>		: @ Satenames
A Users	Integration assistant	Upload new logo 🕥	"safenames-logo-840-blue.png"
්ස් Groups	Manage     Reanding & properties	Home page URL 🛈	https://st-identity.safenames.com
起 Devices	Authentication	Terms of service URL ①	https://www.safenames.net/resources/terms-conditions
Applications	Certificates & secrets	Privacy statement URL ①	https://www.safenames.net/resources/privacy-policy
Enterprise applications	Token configuration     API permissions	Service management reference 🕕	
App registrations	i Expose an API	Internal notes 🛈	Add information relevant to the management of this application.
A Protect & secure	App roles		
Identity Governance	V A Owners		
External Identities	Manifest	Dublisher demain	lindate domain
Show more	Support + Troubleshooting	Publisher domain ()	This domain will appear on the application's consent screen.
Permissions Management	Troubleshooting	Publisher verification	
Verified ID	New support request	Associate a verified Microsc various places, including the	oft Partner Center (MPN) account with your application. A verified badge will appear in e application consent screen. Learn more 🗗
		MPN ID	Add MPN ID to verify publisher
		Publisher display name	Not provided
Learn & support	~		
	**	Save Discard	

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 readd it.

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

Inner ) Seferenze IDO I Presentia	<ul> <li>Sofewares IDB</li> </ul>			
Conferences IDP   Propertie	Cartification Drawston A	Add a client secret		)
P Safenames IDP	Certificates & secrets 🖉 ····	Description	100	
₽ Search	≪ Å <sup>2</sup> Got feedback?	Description	Curtom	
Cherrien -		Expires	Recommended: 180 days (6 months)	
Ouickstart	Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens	Start	90 days (3 months)	
Integration assistant	scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.	End	365 days (12 months)	
megionoriosistem			545 days (12 months)	
Manage	Application registration certificates, secrets and federated credentials can be found in the tabs below.		740 days (14 months)	
Branding & properties			Custom	
Authentication	Certificates (0) Client secrets (0) Federated credentials (0)		Custom	
Certificates & secrets	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as appl			
Token configuration				
API permissions	+ New client secret			
Expose an API	Description Expires Value 🛈			
App roles	No client secrets have been created for this application.			
Owners	The start starter that went exercises and approximately			
Roles and administrators				
Manifest				
upport + Troubleshooting		Add Cancel		

# 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

C All platforms	Quickstart Docs
* Redirect URIs	
The URIs we will accept as destinations when returning a after successfully authenticating or signing out users. Th request to the login server should match one listed here more about Redirect URIs and their restrictions	authentication responses (tokens) e redirect URI you send in the . Also referred to as reply URLs. Lea
https://st-identity.safenames.com/signin-oidc/azure	à
Front-channel logout URL This is where we send a request to have the application required for single sign-out to work correctly.	clear the user's session data. This is
Front-channel logout URL This is where we send a request to have the application required for single sign-out to work correctly. e.g. https://example.com/logout	clear the user's session data. This is
Front-channel logout URL This is where we send a request to have the application required for single sign-out to work correctly. e.g. https://example.com/logout Implicit grant and hybrid flows	clear the user's session data. This is
Front-channel logout URL This is where we send a request to have the application required for single sign-out to work correctly. e.g. https://example.com/logout Implicit grant and hybrid flows Request a token directly from the authorization endpoir architecture (SPA) and doesn't use the authorization cod JavaScript, select both access tokens and ID tokens. For web apps that use hybrid authentication, select only ID	clear the user's session data. This is it. If the application has a single-pa le flow, or if it invokes a web API vi ASP.NET Core web apps and other tokens. Learn more about tokens.
Front-channel logout URL This is where we send a request to have the application required for single sign-out to work correctly. e.g. https://example.com/logout Implicit grant and hybrid flows Request a token directly from the authorization endpoir architecture (SPA) and doesn't use the authorization coording JavaScript, select both access tokens and ID tokens. For web apps that use hybrid authentication, select only ID Select the tokens you would like to be issued by the authored the second	clear the user's session data. This is t. If the application has a single-pa le flow, or if it invokes a web API via ASP.NET Core web apps and other tokens. Learn more about tokens. horization endpoint:
Front-channel logout URL This is where we send a request to have the application required for single sign-out to work correctly. e.g. https://example.com/logout Implicit grant and hybrid flows Request a token directly from the authorization endpoir architecture (SPA) and doesn't use the authorization cod JavaScript, select both access tokens and ID tokens. For web apps that use hybrid authentication, select only ID Select the tokens you would like to be issued by the aut Access tokens (used for implicit flows)	clear the user's session data. This is it. If the application has a single-pa le flow, or if it invokes a web API vi ASP.NET Core web apps and other tokens. Learn more about tokens. horization endpoint:

Enter the URIs and Press "configure" to save

#### 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.

	${\cal P}$ Search resources, services, and docs (G+/)		G 🖓 🕸 O
Home > Safenames IDP			
Safenames IDP	Users and groups		
	<ul> <li>Add user/group</li> <li>Edit assignment</li> <li>Ren</li> </ul>	nove	
Overview     Overview     Deployment Plan	The application will appear for assigned users within M	y Apps. Set 'visible to users?' to no in properties to prevent this. $\rightarrow$	
X Diagnose and solve problems	Assign users and groups to app-roles for your application	here. To create new app-roles for this application, use the application registration.	
	P First 200 shown, to search all users & gro		
Owners	Display Name	Object Type	Role assigned
& Roles and administrators	No application assignments found		
Users and groups	1		
Single sign-on	1		
Provisioning			
Application proxy			
Self-service			
<ul> <li>Custom security attributes (preview)</li> </ul>			
Security			
Conditional Access			
👫 Permissions			
Token encryption			

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

+44 (0) 1908 200022 🚔 +1 703 574 5313   Contact Us
o Safenames
Login
<ul> <li>Your user is associated with your organisation's single sign-on provider. You must sign on through your single sign-on portal.</li> </ul>
Username
username
Password
Forgot Password Login

# 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

onelogin	Users	Applications	Devices	Authenticatior
		Applications Portal Tabs		
Login Informa	ation	Custom Conne	ctors	
No Login Data availa	able		27	
Reports				Cert
Assumed user acti	vity last 3 m	onths		Low S
New users				Stand
Privileged users				

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

Connectors / Untitled		
Basic Configuration	Icon Rectangular Icon	Square Icon

# Sign on Method – Select OpenID Connect

# Connectors / Untitled Basic Configuration Sign on method Form-based auth Basic 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	OpenID Connect
	Redirect URI
	https://identity.safenames.com/signin-oidc/{cus
	Post Logout Redirect URI
	https://identity.safenames.com/signout-oidc/{cu
	Signing Algorithm
	RS256 -
	Login URL
	Login url
	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 lcon.

App Listing / Add Safenames IDP		Canc	el Save
Configuration	Portal Display Name Safenames IDP Visible in portal	Square Icon	
	Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG	Upload a square icon at least 512x512px as either a transparent .PNG or .SVG	

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.

Applications / Safenames IDP		
Info	Enable OpenID Connect	
Parameters	Client ID	
Rules		6
sso	Client Secret	
Access	Hide client secret Regenerate client secret	E.
Users		
Privileges	Issuer UKL https://safenames-dev.onelogin.com/oidc/2 Well-known Configuration	

Set "Application Type" from the dropdown to "Web"

Set "Token Endpoint" from the dropdown to "POST"

nfo	Application Type	
Parameters	Application Type	
Pulse	Web	•
Rules		
SSO		
Access	Token Endpoint	
Users	Authentication Method	
Privileges	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 Jo	onathan Stock	
Allow the user to sign in		
Hide this app in Portal		
Reset login ( What's this? )		
	Cancel	

# 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.

+44 (0) 1908 200022 🚔 +1 703 574 5313   Contact Us	
Safenames	
• Your user is associated with your organisation's	
single sign-on provider. You must sign on through your single sign-on portal.	
Username	
Password	
Forgot Password Login	

# 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