

Kiuwan OAuth 2.0 and OIDC Integration

OAuth 2.0 is an authorization framework that allows software applications to access protected resources that belong to somebody or something. The software applications can obtain total or partial access to the protected resources, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service or by allowing the software applications to obtain access on their own behalf.

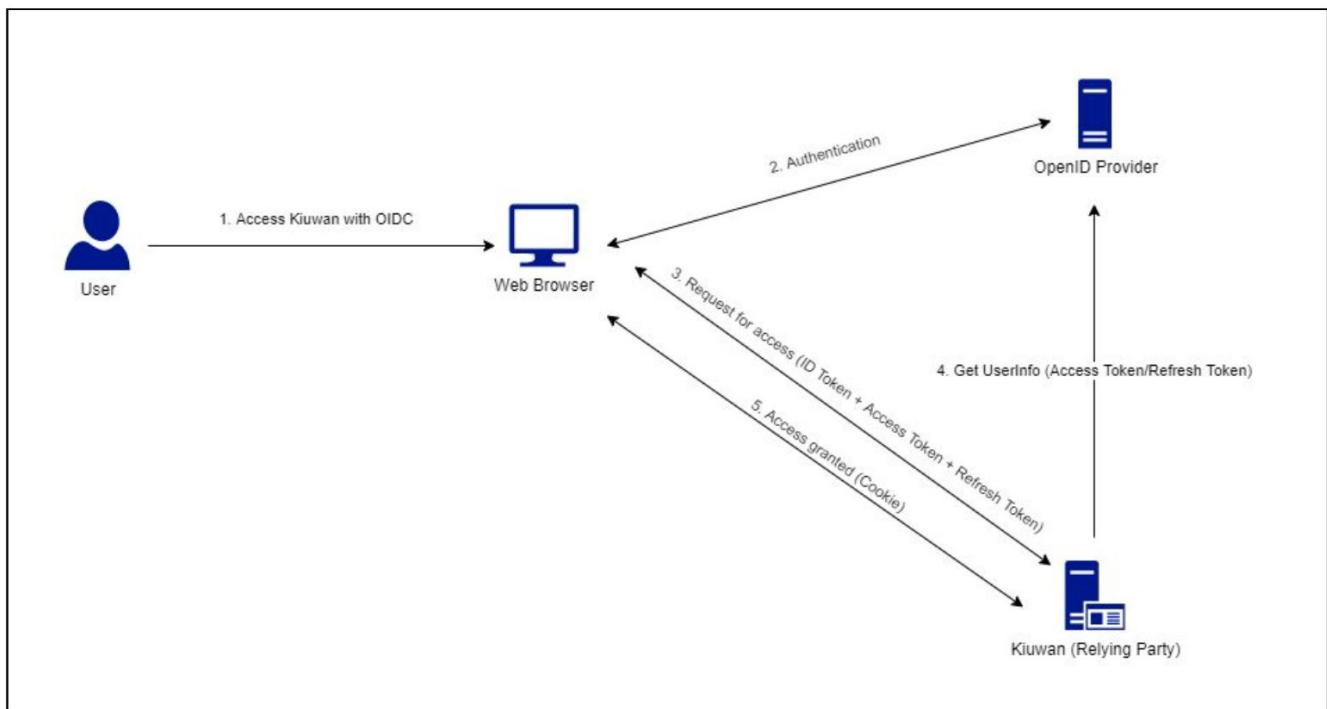
Additionally, OIDC adds a simple identity layer (adding end-users authentication-related data in the payload) on top of the OAuth 2.0, making simple integration with external systems that support some of the grant types defined in OAuth 2.0 specification ([OAuth 2.0 Authorization Framework](#)) i.e. most major online services nowadays.

Contents:

- [Web Browser Single Sign-On](#)
- [Configuring OpenID Provider](#)
 - [Registering Kiuwan as an Oauth/OIDC client in Azure AD](#)
 - [Registering Kiuwan as an OAuth/OIDC client in Windows ADFS 2016](#)
 - [Registering Kiuwan as an OAuth/OIDC client in OKTA](#)
- [Setting up Kiuwan SSO with OAuth/Open ID Connect](#)
- [Login to Kiuwan after OAuth SSO is activated](#)
 - [Login in with Kiuwan defined username and password](#)
- [Setup KLA to use OAuth2 SSO](#)
- [Login to KLA after OAuth SSO is activated](#)

Web Browser Single Sign-On

When configured, a Kiuwan user can authenticate against an OAuth/OIDC server, and access Kiuwan resources.



Before the user can start using Web Browser SSO flow, the administrator of the OpenID Provider in their organization must first have registered Kiuwan as a Relying Party, and subsequently, the account owner of the Kiuwan user account must have registered their OpenID Provider in Kiuwan.

Configuring OpenID Provider

The following describes how to setup Kiuwan as a registered application on Azure ADFS, any other OAuth2.0/Open ID Provider with a similar configuration.

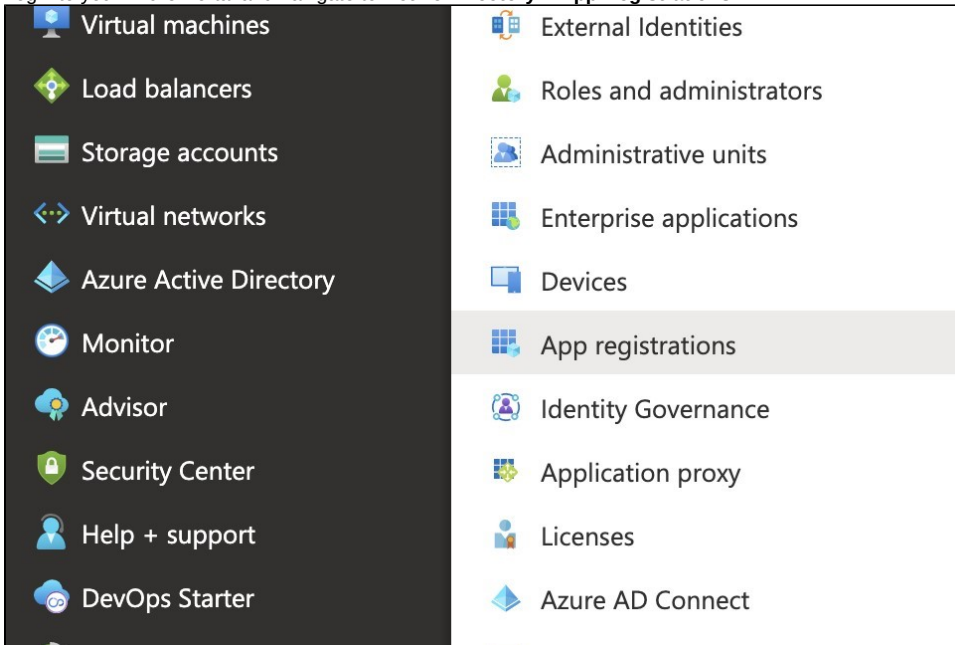
To enable the authentication through an OAuth/OIDC server when configuring Kiuwan as a client application is required to be obtained from OAuth Issuer the following:

1. **URL of the issuer:** The base URL provided by the OAuth provider that will be used for authentication and exchange of tokens.
2. **OIDC Metadata URL:** e.g. `.well-know/openid-configuration` URL while not mandatory by OpenID connect standard, the auto-configuration enables clients to derive all server configuration.

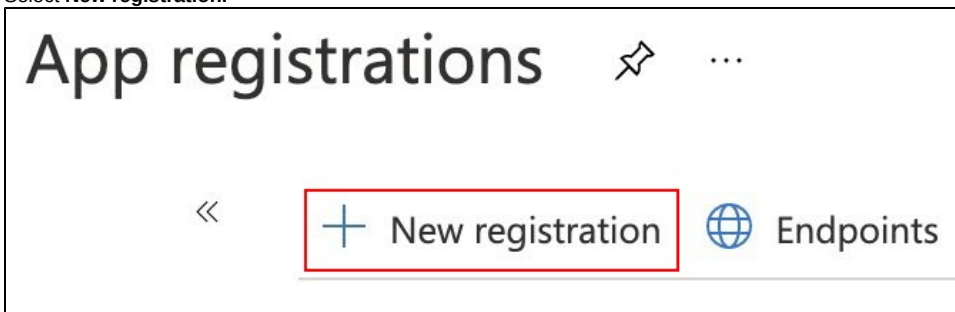
3. **Application ID:** The name of the Kiuwan application as registered in the Oauth2.0 / OIDC Server.
4. **Client Secret:** Kiuwan OIDC Client demands encrypted tokens, so a client secret, produced by the Oauth2.0/OIDC Server must be provided.
5. **The username mapping:** The name of the OAuth/OIDC token field that enables Kiuwan to obtain the corresponding user in Kiuwan. For instance, if a user email is used to define the Kiuwan username, then the user mapping could be "e-mail". Any other field described by the Oauth /OIDC server claims can be used, as long as the resulting value matches the Kiuwan user. It is common for the issuer server to include in the authentication token the field preferred_username, which usually maps to the username in the Identity Provider OAuth issuer.
In Azure AD, preferred_username matches the Unique Principal Name, e.g. the unique username of the identity within the AD definition.

Registering Kiuwan as an Oauth/OIDC client in Azure AD

1. Login to your Azure Portal and navigate to **Active Directory > App Registrations**.



2. Select **New registration**.



3. Fill in the required information

Register an application

*** Name**

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (DOMAIN only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

e.g. https://example.com/auth

4. Configure the Redirect URI as follows:

- Add the following URI as the redirect URI: <https://www.kiuwan.com/saas/oidc/auth>
- The endpoint OAuth2/OIDC server will redirect, within the Kiuwan server, after the successful authentication of a specific user.
- If you have a local installation of Kiuwan, instead of www.kiuwan.com enter the corresponding URL, or IP address, of the local Kiuwan server.
- After defining this Application Registration, the following is obtained:

foobar

Search (Cmd+J)

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Delete

Endpoints

Preview features

Essentials

Display name : foobar

Application (client) ID : ea6913b8-06d4-4176-b8e0-d253190e041f

Directory (tenant) ID : a661771f-a950-4156-b52b-ad98deec4638

Object ID : 86ce1fb8-bb63-482c-b883-26ea4e51e15d

Supported account types : My organization only

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in ... : foobar

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Call APIs

Documentation

Microsoft identity platform

Authentication scenarios

Authentication libraries

Code samples

Microsoft Graph

Glossary

Help and Support

5. Configure Client Secret.

- After creating the registration, select the **Certificates & Secrets** option, and **New Client Secret**.

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Thumbprint

Start date

Expires

ID

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description

Expires

Value

ID

No client secrets have been created for this application.

b. Enter the needed values and click **Add**.

Add a client secret

Description

Expires

☒ In 1 year

☐ In 2 years

☐ Never

Add

Cancel

c. A new secret for this Client Application ID is generated.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
foobar secret	3/16/2022	[REDACTED]	200a67d1-eb82-4565-8968-69554d0b94b5

Copy this value to a temporary location as it will be needed later and after the screen is closed the access to the secret value is lost. Ideally, paste it directly into the OAuth/OIDC configuration at Kiuwan described in the next chapter.

In the previous steps, you have created a new registry for Kiuwan to integrate with OAuth/OIDC server.

The following information was generated, that would be needed in configuring Kiuwan to use this registry:

Application ID:

Delete

Endpoints

Preview features

^ Essentials

Display name : foobar

Application (client) ID : ea6913b8-06d4-4176-b8e0-d253190e041f

Application Secret:

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
foobar secret	3/16/2022	[REDACTED]	200a67d1-eb82-4565-8968-69554d0b94b5

Additionally, you would also need to collect the following endpoints:

OpenID Connect metadata document

https://login.microsoftonline.com/[REDACTED]/v2.0/.well-known/openid-configuration

OAuth 2.0 authorization endpoint (v2)

https://login.microsoftonline.com/[REDACTED]/oauth2/v2.0/authorize

Registering Kiuwan as an OAuth/OIDC client in Windows ADFS 2016

Similar to Azure DevOps, as with any other OAuth/OIDC issuer or identity provider, the configuration of ADFS follows the specifics defined for that Idp. However, information needs to be collected during the setup of Kiuwan as a registered app, as detailed in section Summary:

- **Application ID:** As manually entered in ADFS
- **Application Secret:** Produced by ADFS during the setup.
- **ADFS issuer URL:** The base URL where Kiuwan is redirected to authenticate the user in ADFS.
(https://{YOUR_ADFS_HOSTNAME}/adfs)
- **ADFS Metadata URL:** The URL in ADFS providing the openid-configuration.
(https://{YOUR_ADFS_HOSTNAME}/adfs/.well-known/openid-configuration)

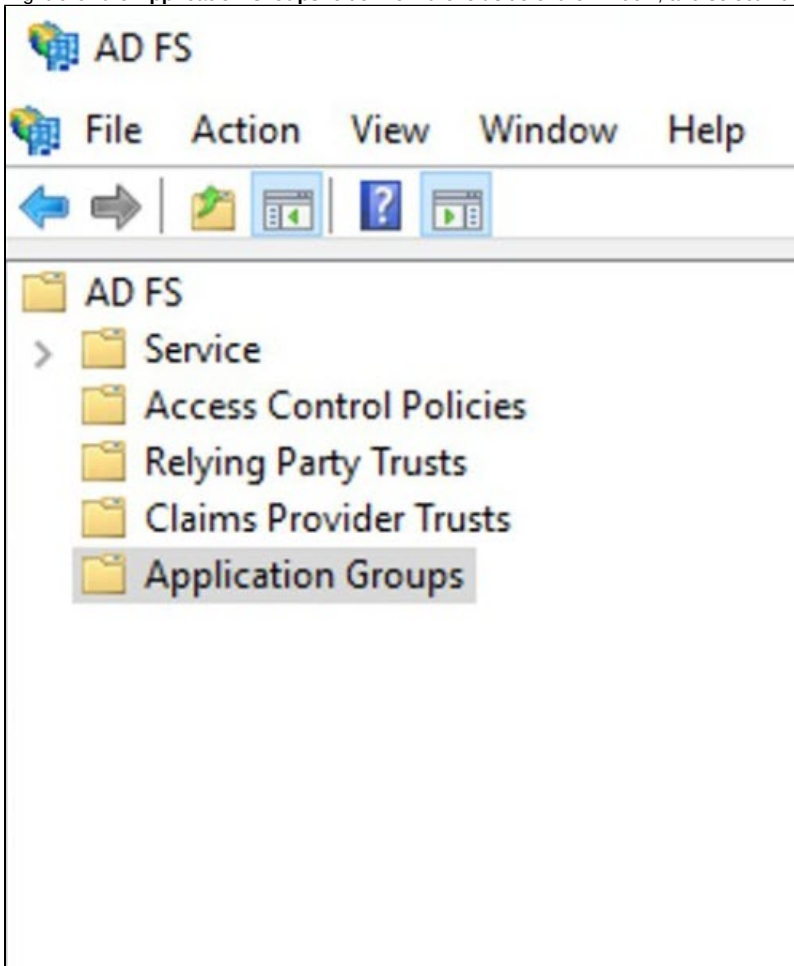
Endpoints		Enabled	Proxy Enabled	URL Path	Type
Metadata		Yes	Yes	/ads/services/trust/13/issuedtokenmixedsymmetricbasic...	WS-Trust 1.3
		Yes	Yes	/ads/services/trust/13/issuedtokenmixedsymmetricbasic...	WS-Trust 1.3
		No	No	/ads/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3
		Yes	Yes	/ads/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3
		No	No	/ads/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3
		No	No	/ads/services/trust/13/issuedtokensymmetricbasic256...	WS-Trust 1.3
		No	No	/ads/services/trust/13/issuedtokensymmetricbasic256sha...	WS-Trust 1.3
		No	No	/ads/services/trust/13/issuedtokensymmetrictripledes...	WS-Trust 1.3
		No	No	/ads/services/trust/13/issuedtokensymmetrictripledesha...	WS-Trust 1.3
		No	No	/ads/services/trust/13/issuedtokenmixedsymmetrictripledes...	WS-Trust 1.3
		No	No	/ads/services/trust/13/issuedtokenmixedsymmetrictripled...	WS-Trust 1.3
		No	No	/ads/services/trust/13/windows	WS-Trust 1.3
		No	No	/ads/services/trust/13/windowsmixed	WS-Trust 1.3
		No	No	/ads/services/trust/13/windowstransport	WS-Trust 1.3
		Yes	No	/ads/services/trustcp/windows	WS-Trust 2005
		No	No	/ads/services/trust/artifactresolution	SAML-ArtifactResolution
		Yes	Yes	/ads/oauth2/	OAuth
OpenID Connect		Yes	Yes	/ads/services/trust/mex	WS-MEX
		Yes	Yes	/Federation/Metadata/2007-06/FederationMetadata.xml	Federation Metadata
		Yes	No	/ads/fs/federationserver/service.asmx	ADFS 1.0 Metadata
Proxy		Yes	Yes	/ads/.well-known/openid-configuration	OpenID Connect Discovery
		Yes	Yes	/ads/discovery/keys	OpenID Connect JWKS
		Yes	Yes	/ads/userinfo	OpenID Connect UserInfo
		Yes	No	/ads/proxy/	Web Application Proxy
		Yes	No	/ads/proxy/EstablishTrust/	Web Application Proxy

The process of registering Kiuwan as an OAuth/OICD application is straightforward.

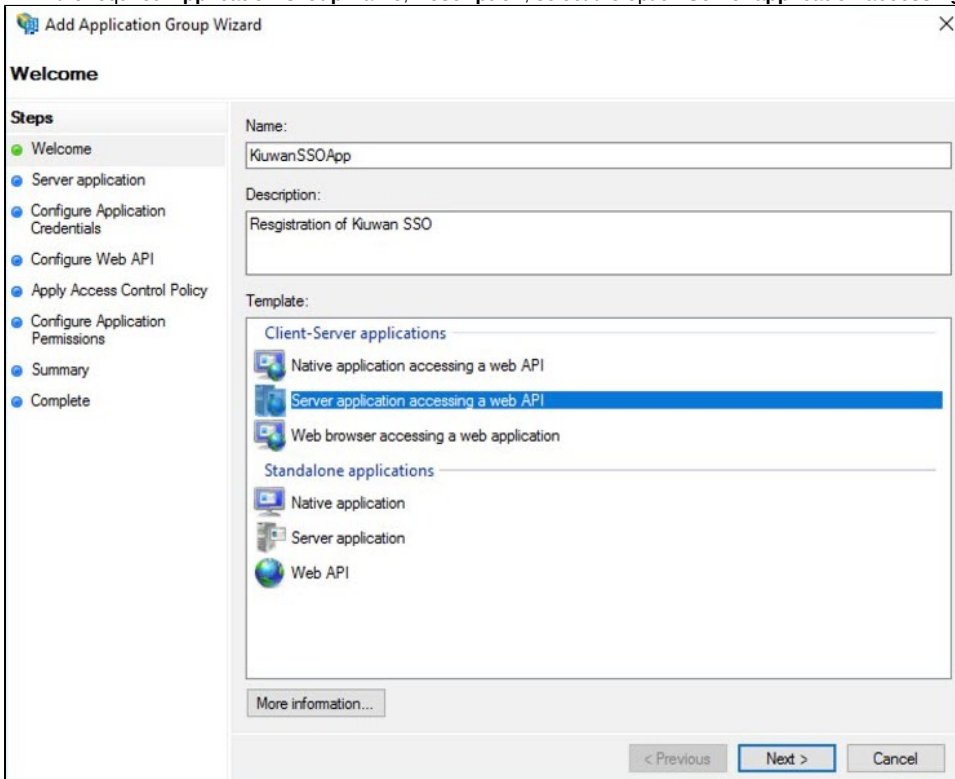
1. Start ADFS Management.

The screenshot shows the Azure portal interface for configuring AD FS. The left-hand navigation pane is open, showing the 'AD FS' section under the 'Service' category. The main content area is titled 'AD FS' and contains an 'Overview' section. This section explains that Active Directory Federation Services (AD FS) provides single-sign-on (SSO) access for client computers. It includes links to 'Learn More About AD FS' (What's new in AD FS?, AD FS Deployment Guide, AD FS Operations Guide, Integrate Azure Multi Factor Authentication with AD FS, Monitor AD FS Service using Azure Active Directory Connect Health) and 'Learn More About Azure Active Directory' (Azure Active Directory description, What is Azure Active Directory?, Extend your directory to Azure Active Directory Identity and Access Management). The right-hand pane shows the 'Actions' menu, which includes options like 'Add Relying Party Trust...', 'Add Claims Provider Trust...', 'Add Attribute Store...', 'Add Application Group...', 'Edit Federation Service Properties...', 'Edit Published Claims', 'Revoke All Proxies', 'View', 'New Window from Here', 'Refresh', and 'Help'.

2. Right-click the **Application Groups** folder from the left side of the window, and select **Add Application Group**.



3. Fill in the required **Application Group Name**, **Description**, select the option **Server application accessing web API**, and click **Next**.



4. Enter the **Name** of the Server Application and collect – and save in a temporary location the **Client Identifier** generated automatically. This information will be available for later consultation but can be copied now and pasted to the Kiuwan SSO configuration form as described in Click **Next**.

Add Application Group Wizard

Server application

Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name: KiuwanSSOApp - Server application

Client Identifier: 19a3b7b5-5aa3-495f-9e3a-42e16b4386f9

Redirect URI: Example: https://Contoso.com

Add Remove

Description:

< Previous Next > Cancel

5. Next, add the Kiuwan Login entry point URI as a valid URI for redirection, e.g. <https://www.kiuwan.com/saas/oidc/auth> or the corresponding if you are using Kiuwan On-Premises or a custom installation instead of the standard Kiuwan cloud setup. Click **Next**.

Add Application Group Wizard

Server application

Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name: KiuwanSSOApp - Server application

Client Identifier: 19a3b7b5-5aa3-495f-9e3a-42e16b4386f9

Redirect URI: Example: https://Contoso.com

Add Remove

Description: Redirect URI for Kiuwan SSO with oauth/oidc

< Previous Next > Cancel

6. On the **Configure Application Credentials** tab, check the option **Generate a shared secret**, this will create the corresponding secret to be copied into the Kiuwan OAuth configuration panel, as described in [Setting up Kiuwan SSO with OAuth/Open ID Connect](#). Click **Next**.

Add Application Group Wizard

Configure Application Credentials

Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.

☐ Register a key used to sign JSON Web Tokens for authentication

☐ Windows Integrated Authentication

Select the AD Account:

Example: CONTOSO\expensevc

☒ Generate a shared secret

Secret:

4vJaYrfvmBt5yo-_hGmVzjr1hxfUhEGkLdSDMexb

Copy to clipboard

i Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.

< Previous Next > Cancel



Copy the generated the shared secret for a temporary location as it will not be available again, and if needed it will need to be regenerated.

7. Configure the **Web API for ADFS** by entering the name of the API and a description for the identifier of this Web API in ADFS. Click **Next**.

Add Application Group Wizard

Configure Web API

Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name:

KiuwanSSOApp - Web API

Identifier:

Kiuwan wbe app registration

Add

Remove

Description:

< Previous Next > Cancel

Add Application Group Wizard

Configure Web API

Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name: KiuwanSSOApp - Web API

Identifier: Example: https://Contoso.com Add

Kiuwan wbe app registration Remove

Description:

< Previous Next > Cancel

8. Select the **Permit Everyone** option as a policy for Access Control and click **Next**.

Add Application Group Wizard

Choose Access Control Policy

Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFAf...
Permit everyone and require MFA for specific group	Grant access to everyone and require MFAf...
Permit everyone and require MFA from extranet access	Grant access to the intranet users and requir...
Permit everyone and require MFA from unauthenticated ...	Grant access to everyone and require MFAf...
Permit everyone and require MFA, allow automatic devi...	Grant access to everyone and require MFAf...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more specifi...

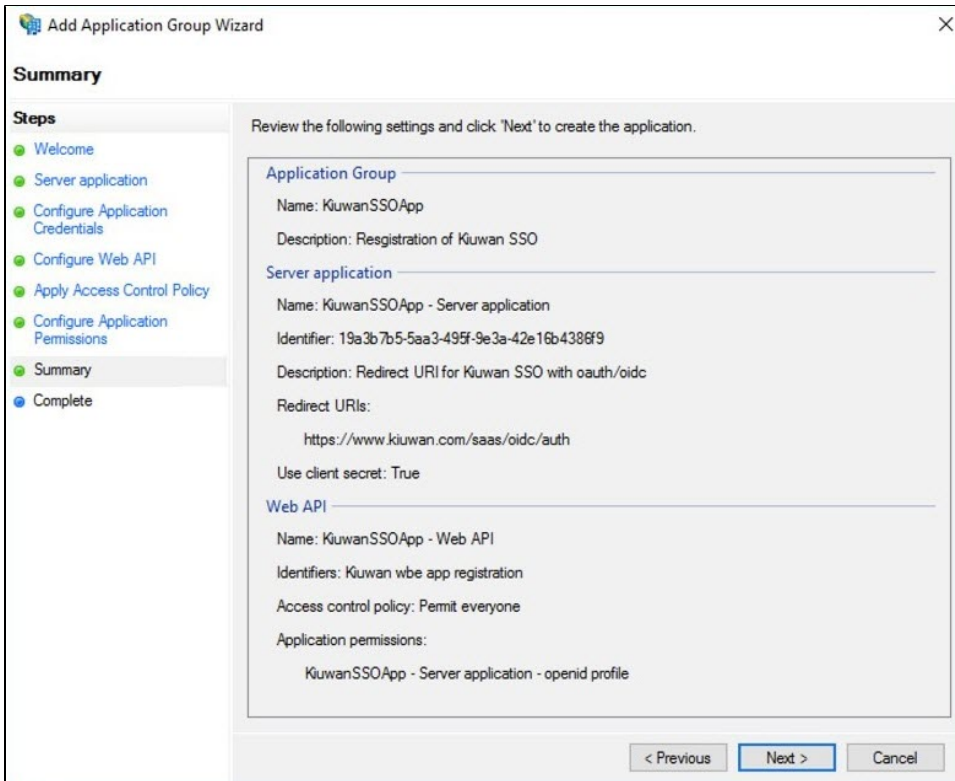
Policy

Permit everyone

☐ I do not want to configure the access control policy at this time. No users will be permitted access for this application.

< Previous Next > Cancel

9. Configure Application Permissions, select **OpenID** and **Profile** as Permitted scopes. If needed or desired additional scopes can be added to the list, this configures the available information about the authenticated user to be passed to Kiuwan. If more information is required in Kiuwan to match the ADFS user with the Kiuwan user, it is allowed to select or even define new scopes. As minimal both OpenID (default) and profile scopes are needed by Kiuwan. Click **next**, to confirm the summary information.



Add Application Group Wizard

Summary

Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Review the following settings and click 'Next' to create the application.

Application Group

Name: KiuwanSSOApp
Description: Resgistration of Kiuwan SSO

Server application

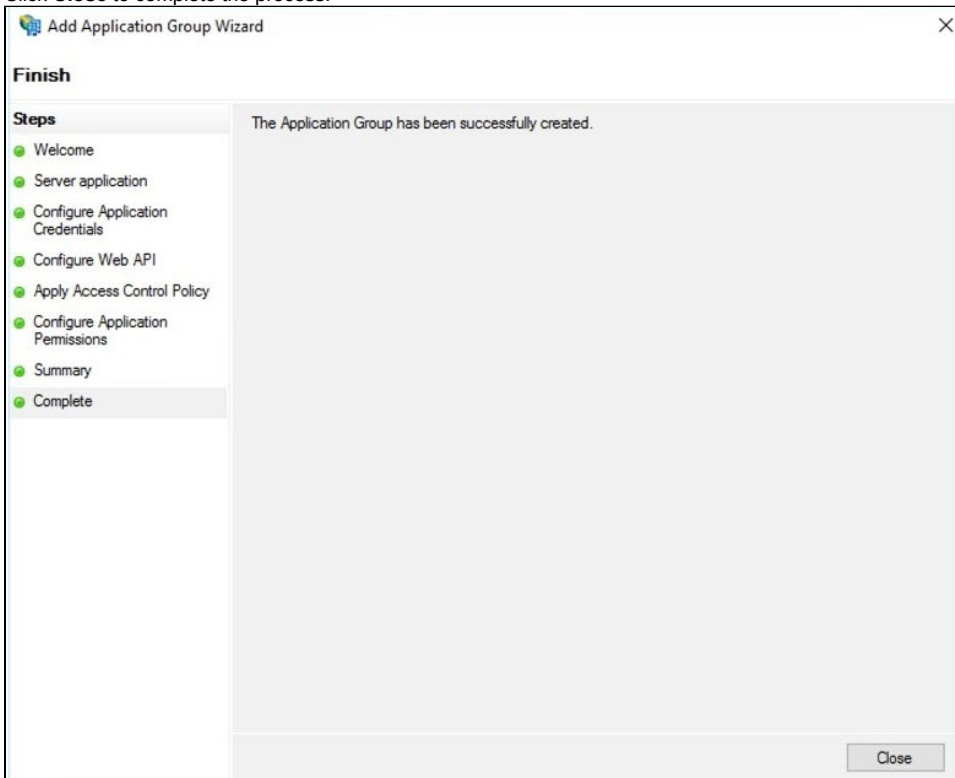
Name: KiuwanSSOApp - Server application
Identifier: 19a3b7b5-5aa3-495f-9e3a-42e16b4386f9
Description: Redirect URI for Kiuwan SSO with oauth/oidc
Redirect URIs:
https://www.kiuwan.com/saas/oidc/auth
Use client secret: True

Web API

Name: KiuwanSSOApp - Web API
Identifiers: Kiuwan wbe app registration
Access control policy: Permit everyone
Application permissions:
KiuwanSSOApp - Server application - openid profile

< Previous Next > Cancel

10. Click **Close** to complete the process.



Add Application Group Wizard

Finish

Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

The Application Group has been successfully created.

Close

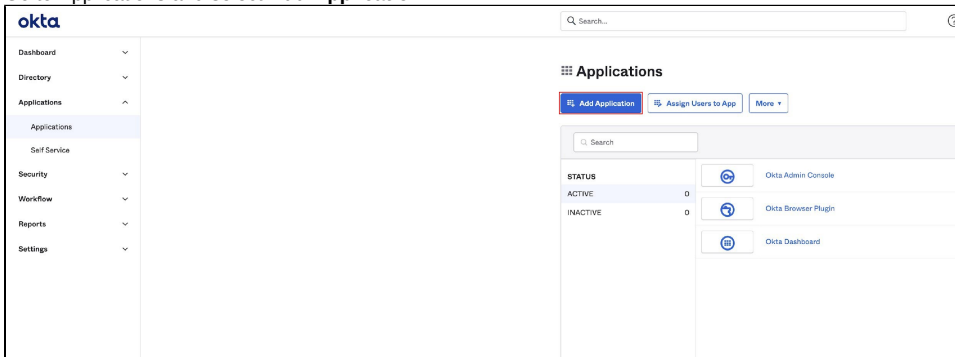
As stated, the application group and corresponding client are now configured.

Registering Kiuwan as an OAuth/OIDC client in OKTA

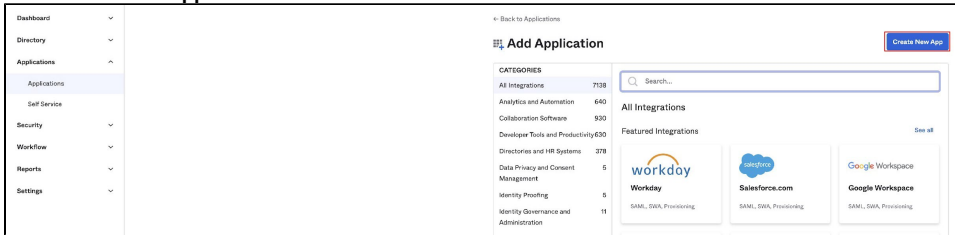
To use OKTA as an OAuth SSO identity provider, it is required to register Kiuwan in OKTA.

Follow these instructions to register Kiuwan in OKTA:

1. Go to Applications and select **Add Application**.



2. Click **Create New App**.



3. On the **Create a New Application Integration** window, select **Web** as Platform entry and select **OpenID Connect** as a Sign on method. Click **Create**.

Create a New Application Integration

Platform

Web

Sign on method

☐ Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.

☐ SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

☒ OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

Create

Cancel

4. In the following screen fill in the required information, adding <https://www.kiuwan.com/saas/oidc/auth> as a Redirect URI. Click **Save**.

Create OpenID Connect App Integration

General Settings

Application name

Kiuwan SSO Web App

Application logo (Optional) ?

Browse files...

Requirements

- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with

- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

Configure OpenID Connect

Login redirect URIs

https://www.kiuwan.com/saas/oidc/auth

×

+ Add URI

After Okta authenticates a user's sign-in request, Okta redirects the user to one of these URIs

Logout redirect URIs (Optional)

+ Add URI

After your application contacts Okta to end the session, Okta then redirects the user to one of these URIs

Save

Cancel

5. Collect the needed information to configure Kiuwan, the application ID, and client secret. Note that the latest will not be available anymore after passing the following screen:

Client Credentials

Edit

Client ID

OoasumtxmQ7dx5Zt25d6



Public identifier for the client that is required for all OAuth flows.

Client secret

.....



Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

General Settings

Edit

Okta domain

shiftleft-kiuwan-sso.okta.com



APPLICATION

Application name

Kiuwan SSO Web App

Application type

Web

Allowed grant types

Client acting on behalf of itself

☐ Client Credentials

Client acting on behalf of a user

☒ Authorization Code

☐ Refresh Token

☐ Implicit (Hybrid)

6. On the tab collect the issuer URI needed for configuring Kiuwan.

General

Sign On

Assignments

Okta API Scopes

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](#)

☒ OpenID Connect

Token Credentials

Edit

Signing credential rotation ⓘ Automatic

OpenID Connect ID Token

Edit

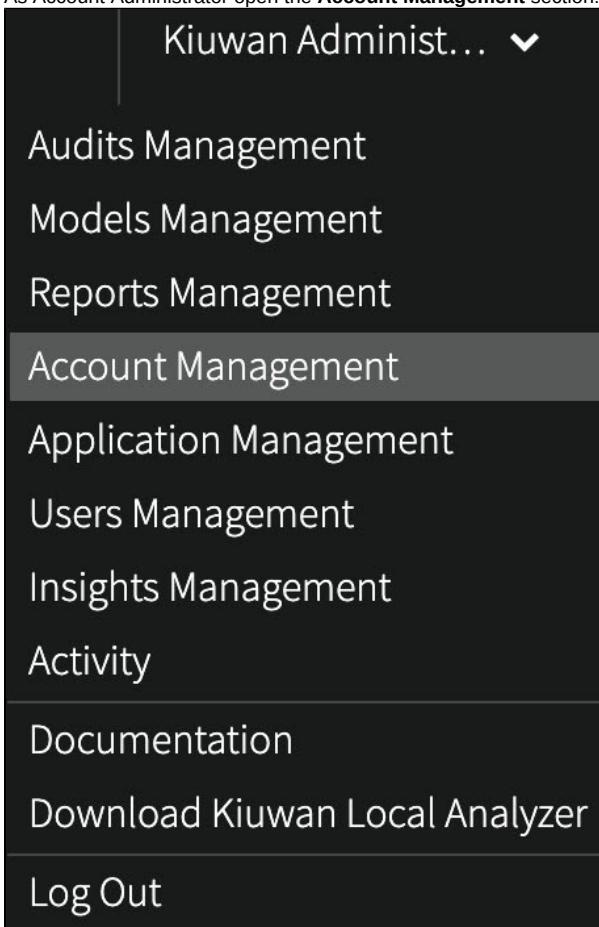
Issuer	https://shiftleft-kiuwan-sso.okta.com
Audience	OoasumtxmQ7dx5Zt25d6
Claims	Claims for this token include all user attributes on the app profile.
Groups claim type	Filter
Groups claim filter ⓘ	None Using Groups Claim

OKTA allows for additional configuration and provides extensive support, make sure you tailor the configuration to your needs.

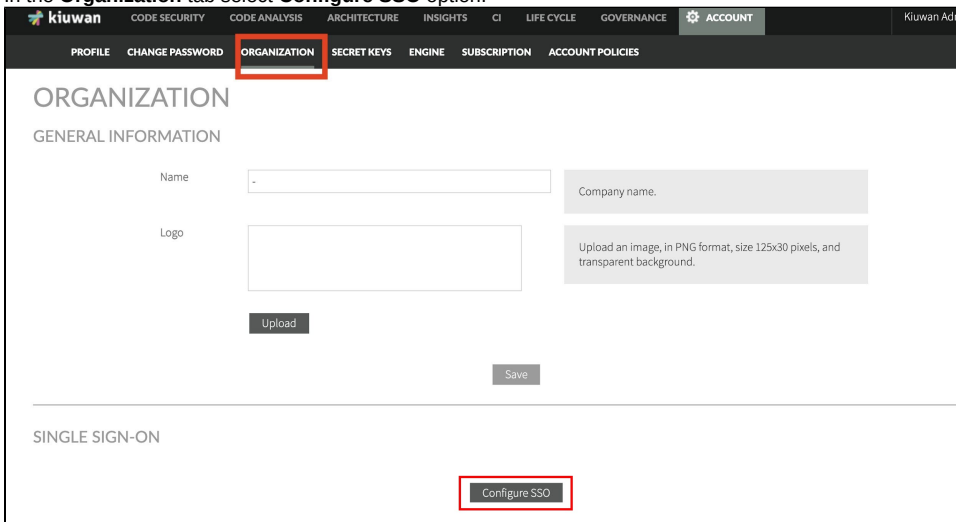
Setting up Kiuwan SSO with OAuth/Open ID Connect

To set up Kiuwan SSO with OAuth/OpenID connect follow these instructions:

1. As Account Administrator open the **Account Management** section:



2. In the **Organization** tab select **Configure SSO** option.



3. Select **OAuth2/OpenID Connect** option and confirm.

SSO TYPE

SELECT A SSO TYPE TO CONFIGURE FOR YOUR ORGANIZATION

☐ SAML

☒ OAuth2/OpenID Connect

Select SSO Type

4. Read the following text explaining the implications when activating SSO, click **Continue** to proceed to the OAuth2/OpenID Connect setup.

SSO CONFIGURATION

This page allows you to activate the access by SSO to the users of your organization. Nevertheless, before you start with the activation process, you should keep in mind the following:

- By activating the SSO in your account, all users of your account will be automatically migrated to your own domain to avoid conflict with other usernames in other Kiuwan accounts.
- After this migration, all users of your account must use a new URL for the Login, leaving the login URL that you have been using until now. This new URL will be communicated to you in the next steps of this page.
- In order to continue using the Kiuwan Local Analyzer, API REST, Kiuwan for Developers, or any other plugin that needs to request for some data to Kiuwan, you must change the configuration and indicate the DOMAIN ID in their respective configuration screens. This DOMAIN ID will be provided when you activate the SSO.
- Once activated the SSO, you must communicate to all your users the new login URL and your DOMAIN ID.
- Once SSO is activated, it is NOT possible to disable it or re-migrate users to the previous Kiuwan domain.
- Event though the activation process is completed, you will need to register Kiuwan as SP in your IdP. Till then, you can not use SSO.

To continue with the activation process, click on 'Continue'.

Continue

5. Fill in the information, as gathered during Configuring OpenID Provider, and confirm entered data by selecting **Enable new IdP**.

SSO CONFIGURATION

Enable new IdP

After confirming the SSO data, a new email is sent with the activation confirmation code, alongside the instructions explaining how to log in to

To continue with SSO activation process, please enter the following activation code in the screen:

Activation Code:

Remember that after SSO activation, you have to use the following link to log into Kiuwan using your username and password:

Login URL: <http://localhost:8080/saas/web/login.html?domain=93a8096f169c96794d6922ea25d7678ee98a41c1f5026f865568f5724165768ff1fdbb80392ad983fc5487a55fcaadd5d51f9971a69887503e6d476b48df2f29>

And this is your DOMAIN ID, necessary to use the Kiuwan Local Analyzer, Kiuwan REST API, and Kiuwan plugins:

DOMAIN ID:
93a8096f169c96794d6922ea25d7678ee98a41c1f5026f865568f5724165768ff1fdbb80392ad983fc5487a55fcaadd5d51f9971a69887503e6d476b48df2f29

Thanks for using Kiuwan. Have fun analyzing!
The Kiuwan Team

Kiuwan after the SSO is activated.

6. Copy the confirmation code and enter it in the confirmation form.

SSO CONFIGURATION

☐ Disable login with password for all my users.

DOMAIN ID

Login URL

Enter activation code :

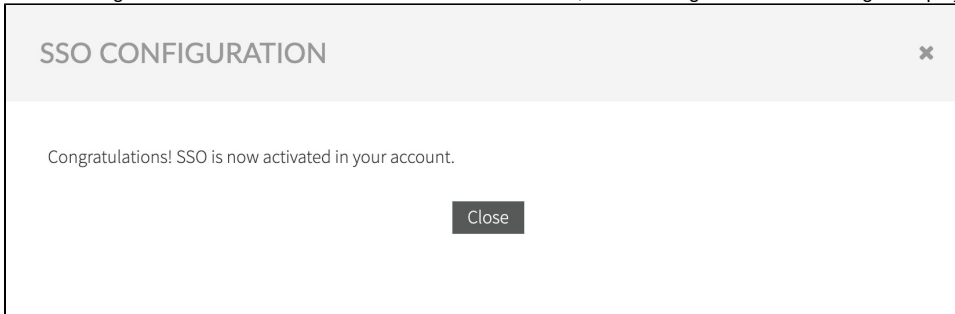
Activate SSO



When the option **Disable Login with password for all my users** is checked, it prevents any user registered in your account, with the exception of Account Owner user, to be able to login using Kiuwan managed identity username/password.

Users will be able to log in only through defined OAuth/OIDC server authentication.

7. After entering the activation code a confirm the activation of SSO, the following confirmation dialogue displays:

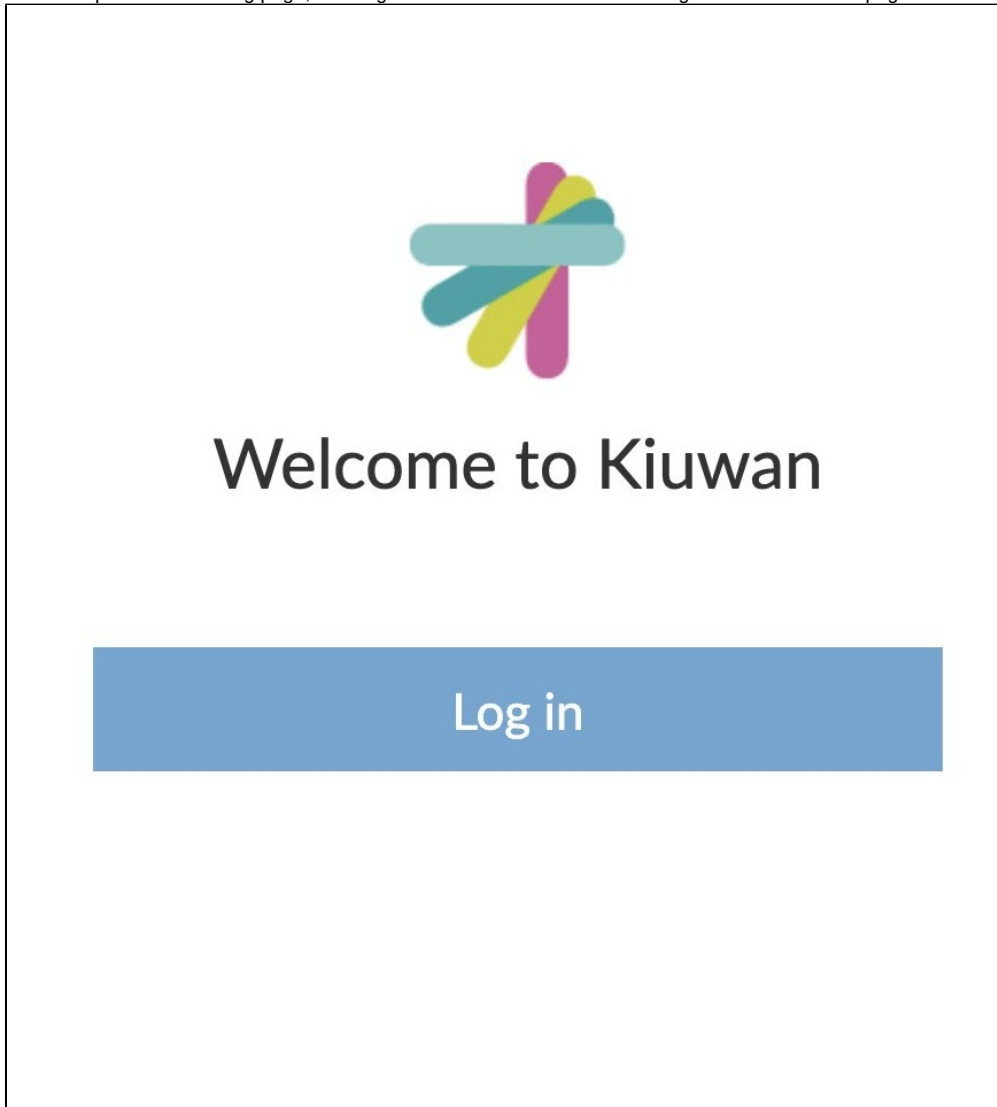


Login to Kiuwan after OAuth SSO is activated

As explained in the confirmation email received during the configuration process, and as shown, after SSO setup in the Organization tab in the Account Management section, after SSO is completed the login must comply with the following URL:

<https://<kiuwan.server.url>/saas/login?domain=<the.created.domain>&sso=on>

This link opens the following page, click login to redirect the user to the configured authentication page at the OAuth/OIDC identity management system.



Successful authentication will enable access to Kiuwan, with the corresponding authorization configured for the logged-in user.

Login in with Kiuwan defined username and password

When the user is configured to login with Username and Password in Kiuwan, as shown below:

NEW USER

Username

Email

Name

Lastname

Enabled

☐

Generate password

☐

Enable Login with password

☒

It is possible to login into Kiuwan bypassing the SSO, this is particularly useful for accessing Kiuwan through the provided REST API, or when SSO is unavailable. To do so, use the following construct to access the Kiuwan console application:

<https://<kiuwan.server.url>/saas/login?domain=<the.created.domain>&sso=off>

It opens the standard Kiuwan Login screen:



Welcome to Kiuwan

Log in

[Forgot your password?](#)

In either case, after setting up SSO, the domain must always be set during the authentication process, otherwise, Kiuwan will not be able to identify the corresponding user.

Setup KLA to use Oauth2 SSO

After an account is configured to use SSO through OAuth2, this configuration becomes also available to KLA.

To enable KLA to use OAuth2/OIDC in the login form follow these steps:

1. Select the **Advanced** option.

Kiuwan Local Analyzer - Login

 **kiuwan**
Local Analyzer

Username

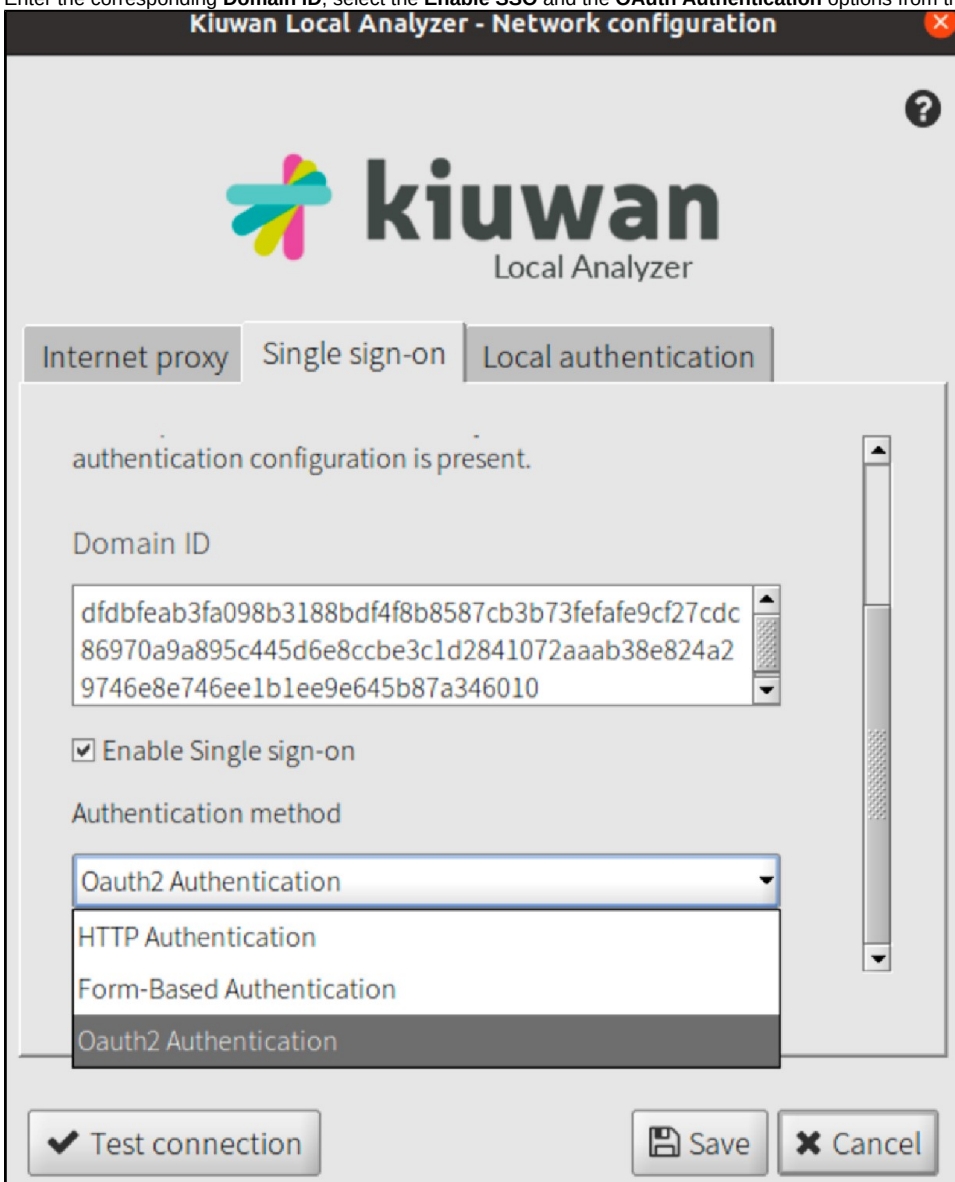
Password

 **Advanced**

 **Login**

 **Exit**

2. Enter the corresponding **Domain ID**, select the **Enable SSO** and the **OAuth Authentication** options from the pull-down list.



The image shows a screenshot of the 'Kiuwan Local Analyzer - Network configuration' dialog box. The title bar is dark with the text 'Kiuwan Local Analyzer - Network configuration' and a red close button. The main area has a light gray background with the Kiuwan logo (a colorful star-like shape) and the text 'kiuwan Local Analyzer'. Below the logo are three tabs: 'Internet proxy', 'Single sign-on', and 'Local authentication'. The 'Single sign-on' tab is selected. The text 'authentication configuration is present.' is displayed. Below this is the 'Domain ID' label and a text box containing a long alphanumeric string: 'dfdbfeab3fa098b3188bdf4f8b8587cb3b73fefafe9cf27cdc86970a9a895c445d6e8ccbe3c1d2841072aaab38e824a29746e8e746ee1b1ee9e645b87a346010'. Below the text box is a checked checkbox labeled 'Enable Single sign-on'. Below that is the 'Authentication method' label and a pull-down menu showing 'OAuth2 Authentication' selected. The menu also lists 'HTTP Authentication', 'Form-Based Authentication', and 'OAuth2 Authentication' (highlighted). At the bottom are three buttons: 'Test connection' (with a checkmark icon), 'Save' (with a floppy disk icon), and 'Cancel' (with an 'X' icon).

Kiuwan Local Analyzer - Network configuration

authentication configuration is present.

Domain ID

dfdbfeab3fa098b3188bdf4f8b8587cb3b73fefafe9cf27cdc
86970a9a895c445d6e8ccbe3c1d2841072aaab38e824a2
9746e8e746ee1b1ee9e645b87a346010

☒ Enable Single sign-on

Authentication method

OAuth2 Authentication

HTTP Authentication

Form-Based Authentication

OAuth2 Authentication

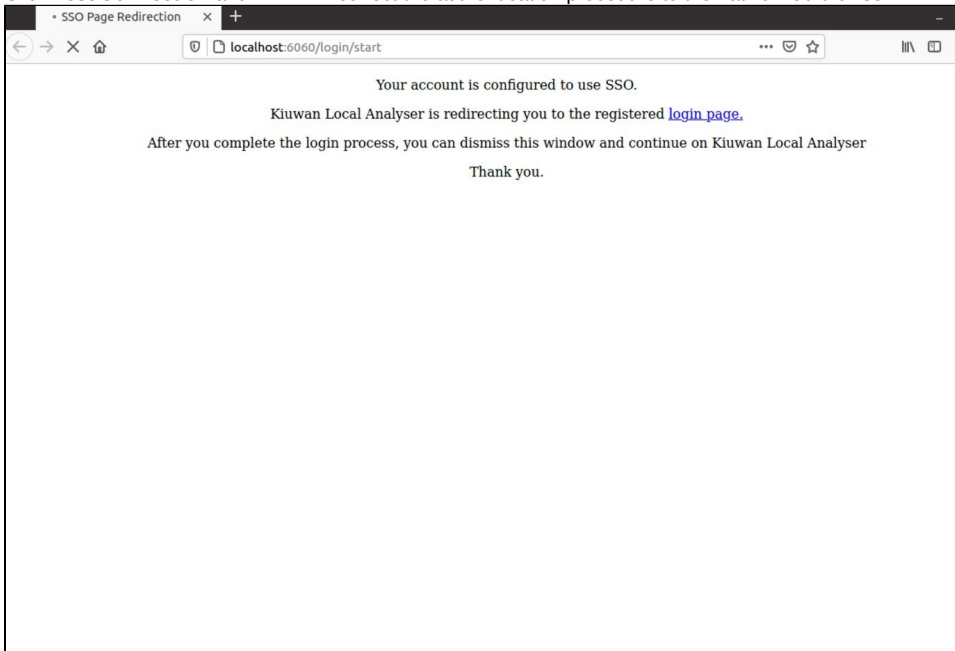
✓ Test connection

Save

Cancel

KLA is now configured to use the OAuth authentication as configured for that Kiuwan Account.

3. Click **Test Connection** and KLA will redirect the authentication procedure to the native web browser:



The above page is temporarily presented informing the user that the login process is underway, and finally the regular authentication process for the configured Identity provided is initiated.

After the authentication process is completed, the browser window can be discarded as KLA has collected the needed information to proceed.

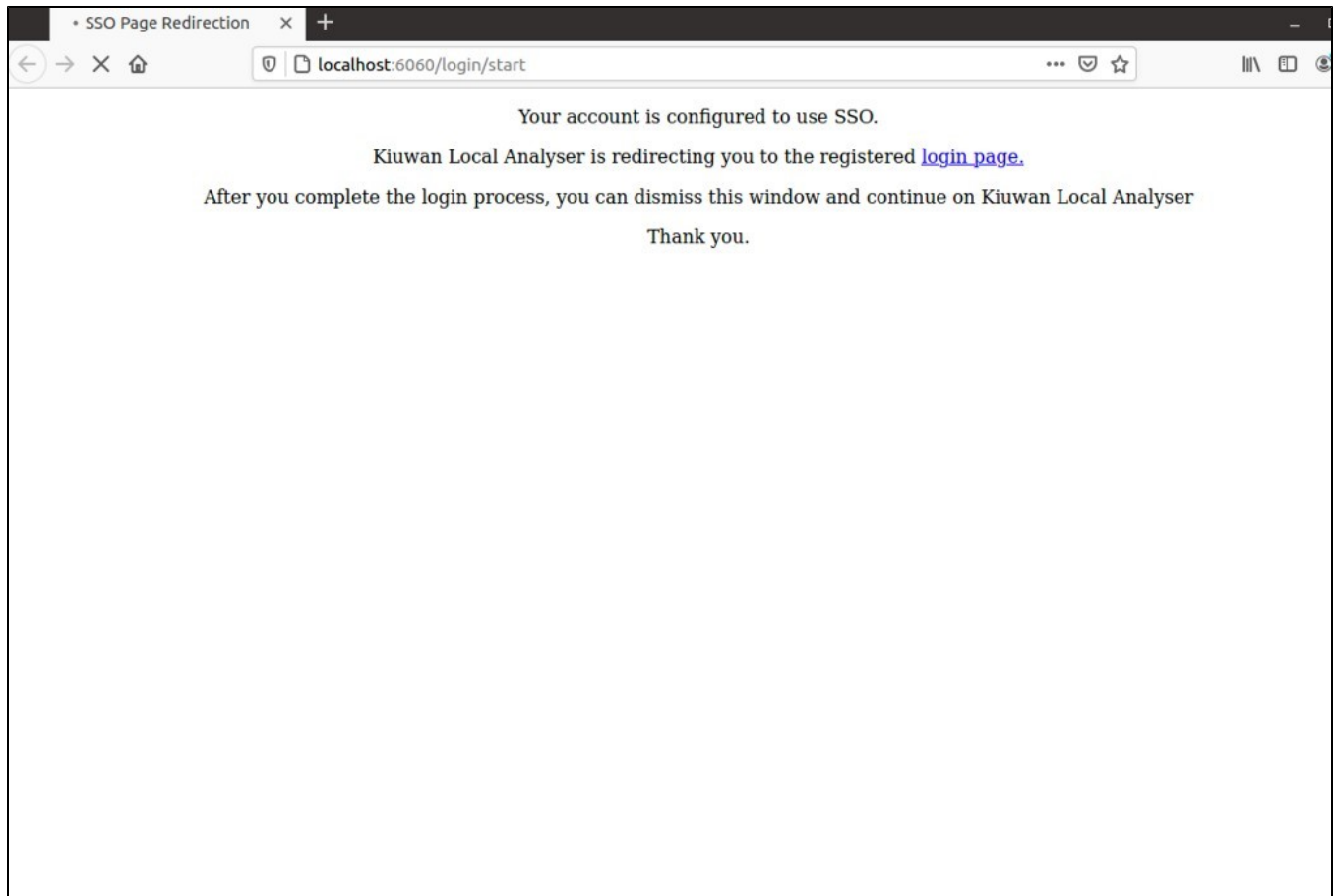
Login to KLA after OAuth SSO is activated

When KLA is configured to use SSO with OAuth, the Login form will show an indication that SSO is activated.



By selecting **Login** in the login form, KLA starts a new browser window to initiate the login flow.

Initially, the browser displays the following information:



Eventually, it would be redirected to the regular Authentication page of the configured Identity provider for the selected account.

Upon successful completion of the authentication process, the browser window can be dismissed, and KLA will be available to be used according to the user's corresponding capabilities.