

Single sign-on for Dialog

Online platform

# Introduction

Dialog supports single sign-on (SSO) based on OAuth 2.0 and OpenID connect 1.0. In order to set this up for your organization, you must take a number of actions yourself. In addition, we need certain information to properly set up the SSO on our side.

In this document you will find all the information necessary to use the SSO. We also share a number of frequently asked questions about the SSO and the corresponding answers. If you have any other questions, please do not hesitate to send an email to support@dialog.nl.

# Actions

Perform the following actions in your identity provider.

1. Check if your SSO provider supports the 'Authorization Code flow'
2. Check if the following scopes are allowed: 'openid', 'email', 'profile'
3. Allow the following redirect url:
	* <https://api.dialog.nl/api/sso/openidconnectcallback>
	* [https://acceptance-api.dialog.nl/api/sso/openidconnectcallback](https://api.dialog.nl/api/sso/openidconnectcallback)
4. If possible, set the homepage for the SSO as: https://app.dialog.nl
5. Set the following icon as the icon for the link:

# Claims

Dialog follows the OpenID Connect 1.0 standard and expects the following claims to be sent along in the Identity Token (<https://openid.net/specs/openid-connect-core-1_0.html#Claims>):

* email
* given\_name
* middle\_name
* family\_name
* name
* picture (optional)
* gender (optional)

The exact naming, as indicated above, is essential for parsing the token. Some identity providers must explicitly state that the claims are also placed in the identity token.

In addition to the above actions, the following is important to check:

* Make sure that in your Identity Provider users have entered both the first name and last name (claims: 'given\_name', 'middle\_name', 'family\_name'). This is taken over by Dialog. If these fields are empty, the full name (the 'name' claim) will be transferred.
* Make sure that users in Dialog are invited with their original email address. Alias ​​email addresses cause problems logging into Dialog if the Dialog email address is different from the user's original email address.

# Required information

After performing the above actions, you will see information that we need to properly configure the SSO. Enter the answers in the column 'Answer'.

|  |  |  |
| --- | --- | --- |
| Category | Example | Answer |
| Discovery url | https://login.microsoftonline.com/{Directory/tenantID}/v2.0/.well-known/openid-configuration |  |
| Client ID |  |  |
| Client secret |  |  |
| Issuer ID  | https://login.microsoftonline.com/{Directory/tenant ID}/v2.0 |  |
| Domain | dialog.nl |  |

# Frequently asked questions

## What changes in the login flow when SSO is enabled in Dialog?

When the SSO is setup, the default login flow is replaced by an SSO login flow. Users then log in with their organization account, such as an Office 365 or Google account. They will continue to do this from https://app.dialog.nl/account/login, but will be forwarded to the SSO login after filling in the email address field. After successful login in the SSO environment, the user is redirected back to Dialog.

## Do I still need to invite new users to Dialog?

You will still need to create new users in Dialog. The date you provide with the invitation is the date on which the account becomes active and can therefore be used. The user will then receive an invitation email to start using Dialog. This new user does not have to register, but enters the login screen of Dialog. The user logs in with his SSO account and then ends up in Dialog.

##  Is two factor authentication possible when we use SSO?

You can set up two-factor authentication in your identity provider. This is not something that needs to be arranged in or by Dialog.

## Can a user change his name, email address or password in Dialog after logging in with SSO?

No. When the user logs into Dialog with his SSO / company account for the first time, the fields for name, email and password are locked in Dialog. Users can therefore no longer adjust these fields. The name of the user is retrieved from your identity provider. The password reset flow also goes through your identity provider.