

Setup of the OKTA OIDC platform on Landslide for User Authentication.

See Admin -> Server Settings (User Authentication)

#1. Create a new application with OIDC and native application type:

## Create a new app integration

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](#)

In this example, MyApplication is used as the application name to store the Client ID and Client Secrets :

Select **Client secret** for Client authentication :

[← Back to Applications](#)



## MyApplication

Active ▾



View Logs

General

Sign On

Assignments

Okta API Scopes

### Client Credentials

[Edit](#)

Client ID

Ooa6ozis1ljGy6S4w5d7



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

Client authentication

- None
- Client secret
- Public key / Private key

Proof Key for Code Exchange (PKCE)

- Require PKCE as additional verification

### CLIENT SECRETS

[Generate new secret](#)

Creation date	Secret	Status
Sep 30, 2022	.....	Active ▾

Select **Resource Owner Password** for Grant Type :

## General Settings

[Edit](#)

### APPLICATION

- App integration name MyApplication
- Application type Native
- Grant type Client acting on behalf of a user
- Authorization Code
  - Interaction Code
  - Refresh Token
  - Resource Owner Password
  - SAML 2.0 Assertion
  - Device Authorization
  - Token Exchange
  - Implicit (hybrid)
- 

### Refresh Token

- Refresh token behavior
- Rotate token after every use
  - Use persistent token
- 

### USER CONSENT

- User consent ?  Require consent
- Terms of Service URI ?
- Policy URI ?

## #2 Create the following groups in the OKTA platform

The screenshot displays the Okta Groups management interface. The left sidebar contains a navigation menu with the following items: Dashboard, Directory, People, Groups (highlighted with a red arrow), Devices, Profile Editor, Directory Integrations, Profile Sources, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'Groups' and features a search bar, an 'Advanced search' dropdown, and a 'Group source type' dropdown set to 'All'. Below this is a table listing groups with columns for 'Group name', 'People', and 'Applicat'. Three groups are highlighted with red arrows: 'landslide-Test-Operator', 'landslide-Test-Administrator', and 'landslide-system-administrator'.

Group name	People	Applicat
landslide-Test-Operator No description	0	0
landslide-Test-Administrator No description	0	1
Everyone All users in your organization	2	0
landslide-system-administrator No description	1	1

And assign users to the corresponding groups.

For instance, admin user is assigned to the landslide-system- administrator :

**admin user**  
barneyliu@hotmail.com

Reset or Remove password More Actions

User Active View Logs

Applications **Groups** Profile Devices Admin roles

### Groups

Group

Group	
Everyone All users in your organization	X
landslide-system-administrator	X

**Groups**  
Groups allow you to manage app assignments and user profile attributes more efficiently.

**Converting Assignments**  
Application access and user profile attributes can be converted from be individually-managed to group-managed. You can convert assignments from an app's Group tab.

Add MyApplication to the Added group.

Enter Security/API to create a new Authorization Servers. You can use the default one as shown below:

okta Search...

YuoLiu@github.okta-dev-36144762

**API** Help

Authorization Servers Tokens Trusted Origins

Add Authorization Server Search...

Name	Audience	Issuer URI	
default	api://default	https://dev-36144762.okta.com/oauth2/default	Active /
demo	api://demo	https://dev-36144762.okta.com/oauth2/ausGozj5b85WAGVlu5d7	Active /

Show More

© 2022 Okta, Inc. Privacy Version 2022.09.3 E OK12 Cell (US) Status site Download Okta Plugin Feedback

Enter the new added auth server, add a new claim to allow Landslide to retrieve the information of user group :

## Edit Claim

Name

Include in token type

Value type

Filter ? Only include groups that meet the following condition.

Disable claim  Disable claim

Include in  Any scope  The following scopes:

Validation:

After the above configuration is done, you can use the following postman collection to validate the configuration :

```
{
  "info": {
    "_postman_id": "6005697d-bc93-4c56-9934-9eb92f47ba70",
    "name": "okta",
    "schema": "https://schema.getpostman.com/json/collection/v2.1.0/collection.json"
  },
  "item": [
    {
      "name": "okta-resource-owner-password",
      "request": {
        "auth": {
          "type": "basic",
          "basic": [
            {
              "key": "password",
              "value":
"tgp5a7ybAvduO69whB5rsUsoy6YVrNZRWYA20ZDY",
              "type": "string"
            },
            {
              "key": "username",
```

```
        "value": "0oa6ozis1ljGy6S4w5d7",
        "type": "string"
    }
]
},
"method": "POST",
"header": [],
"body": {
    "mode": "urlencoded",
    "urlencoded": [
        {
            "key": "grant_type",
            "value": "password",
            "type": "default"
        },
        {
            "key": "username",
            "value": "barneyliu@hotmail.com",
            "type": "default"
        },
        {
            "key": "password",
            "value": "1234567890qwE",
```



```
        "type": "default"
    },
    {
        "key": "scope",
        "value": "openid group",
        "type": "default"
    }
]
},
"url": {
    "raw": "https://dev-
36144762.okta.com/oauth2/aus6ozj5b85WAQVIu5d7/v1/token",
    "protocol": "https",
    "host": [
        "dev-36144762",
        "okta",
        "com"
    ],
    "path": [
        "oauth2",
        "aus6ozj5b85WAQVIu5d7",
        "v1",
        "token"
    ]
}
```

```
}  
  
},  
  
"response": []  
  
}  
  
]  
  
}
```

okta / okta-resource-owner-password replace with Your authorization server url

POST https://dev-36144762.okta.com/oauth2/aus6ozj5b85WAQVlu5d7/v1/token

Params Authorization Headers (10) Body Pre-request Script Tests Settings

Type Basic Auth

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)

Username 0oa6ozis1jGy6S4w5d7 Client ID

Password ..... Client Secret

Show Password

POST https://dev-36144762.okta.com/oauth2/aus6ozj5b85WAQVlu5d7/v1/token

Params Authorization Headers (10) Body Pre-request Script Tests Settings

none  form-data  x-www-form-urlencoded  raw  binary  GraphQL

KEY	VALUE
<input checked="" type="checkbox"/> grant_type	password
<input checked="" type="checkbox"/> username	barneyliu@hotmail.com
<input checked="" type="checkbox"/> password	1234567890qwE
<input checked="" type="checkbox"/> scope	openid <span style="border: 1px solid red; padding: 2px;">group</span>
Key	Value

Scope associated with claim

## Result:

```
Body Cookies (2) Headers (24) Test Results Status: 200 OK Time: 1542 ms Size: 6.28 KB Save Response
Pretty Raw Preview Visualize JSON
1
2 "token_type": "Bearer",
3 "expires_in": 3600,
4 "access_token": "eyJ3aWQ1OjB1L2YktTendyR3FwYV90c3BEZFPpN0FEZiDfBkZPZ3U0ZV8fc2lXV11jIiwiaWxkIjo1LmYnNTYifQ.",
5 "id_token": "eyJ3aWQ1OjB1L2YktTendyR3FwYV90c3BEZFPpN0FEZiDfBkZPZ3U0ZV8fc2lXV11jIiwiaWxkIjo1LmYnNTYifQ.",
6 "scope": "openid group",
7 "user-group": "landslide-system-administrator"
```

In this example, we put the claim in the ID\_TOKEN, if we decode the ID\_TOKEN, we get the user-group claim information.

```
PAYLOAD: DATA
{
  "sub": "00u6ozm1rojL1RW1L5d7",
  "ver": 1,
  "iss": "https://dev-36144762.okta.com/oauth2/aus6ozj5b85WAQVIu5d7",
  "aud": "00a6ozis1ljGy6S4w5d7",
  "iat": 1665384033,
  "exp": 1665387633,
  "jti": "ID.eakhtnX17L9z1l1tep6a0BL7sx0Art0_EuH80s7Yge-M",
  "amr": [
    "pwd"
  ],
  "idp": "00o61jzz0dEDQscF5d7",
  "auth_time": 1665384033,
  "at_hash": "68ZEaB5HCWt0W15qqPmTSw",
  "user-group": [
    "landslide-system-administrator"
  ]
}
```

VERIFY SIGNATURE

Another way to configure the OKTA Authentication server is to return the user group for landslide application.

Okta allows several ways to define a claim, we recommend using regex.

Example: define the claim by using regex

**Edit Claim**

Name: user-group

Include in token type: ID Token, Always

Value type: Groups

Filter: Only include groups that meet the following condition.  
Matches regex: .\*

Disable claim:  Disable claim

Include in:  Any scope,  The following scopes:

Save Cancel

*OKTA group*

the response will return the user-group

```
as {  
  "al_nashn": "x0j000054MjBIM30V/RU1g",  
  "user-group": [  
    "Everyone",  
    "landslide-system-administrator"  
  ]  
}
```