

# devfest

## Wifi:

Enterprise Workshops: <https://bit.ly/3udKRmJ>

Workshop Repo:

- start - <https://bit.ly/3uh8H0s>
- completed <https://bit.ly/47wBhJK>

Slides:



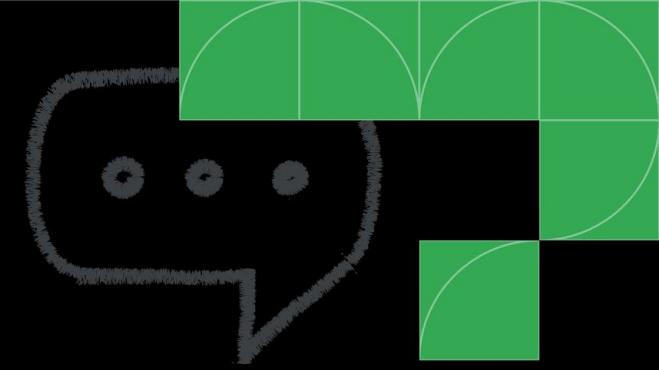
Google Developer Groups

Editable Location

## You will need:

- a laptop with admin access
- Node v18+
- terminal access
- an IDE that supports TypeScript, such as Visual Studio Code

devfest



Build a lasting relationship  
with your enterprise  
customers

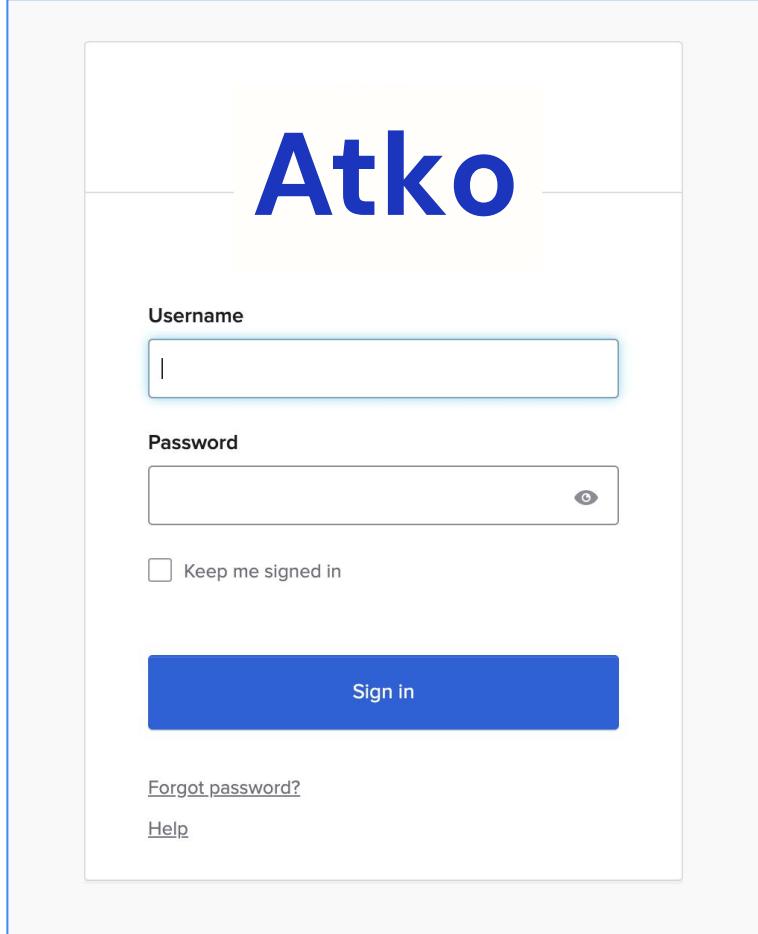


# Who am I?

```
{  
  "sub": "00upp1hf16Sn1H2fb0h7",  
  "name": "Semona Igama",  
  "email": "semona.igama@okta.com",  
  "ver": 1,  
  "iss": "https://semonav2.oktapreview.com",  
  "aud": "0oaqh3fceytYR7U1I0h7",  
  "iat": 1698872857,  
  "exp": 1698876457,  
  "jti": "ID.sGTbaSiUQUCa6SKbqZMDPfrJWjb5t-XoFzY66R0ERl4",  
  "amr": [  
    "pwd"  
,  
  ],  
  "role": "Developer Advocate at Okta",  
  "twitter_handle": "@sudomonas",  
  "fav_animal": "dolphin",  
  "sport": "ultimate",  
  "idp": "00opp1hezxr8yhXvQ0h7",  
  "nonce": "rhkhjm9oc",  
  "preferred_username": "semona.igama@okta.com",  
  "auth_time": 1698872820,  
  "at_hash": "acaWBJnAi1Y6ZNYLPRJteg",  
  "c_hash": "0fGTQcMQWaQtVl5keiE5sQ"  
}
```

# What's your login experience like?

- Follows standard security protocols
- Allows identity provider login options for Single Sign On (SSO)
- Allows



The image shows a clean, modern login interface for 'Atko'. At the top center is the 'Atko' logo in a large, bold, blue sans-serif font. Below it is a horizontal line. The main form area has a light gray background. It contains three input fields: a 'Username' field with a placeholder 'Username' and a small icon on the right; a 'Password' field with a placeholder 'Password' and a small eye icon on the right; and a 'Keep me signed in' checkbox. A large blue 'Sign in' button is centered below these fields. At the bottom of the form are two links: 'Forgot password?' and 'Help'.

Atko

Username

Password

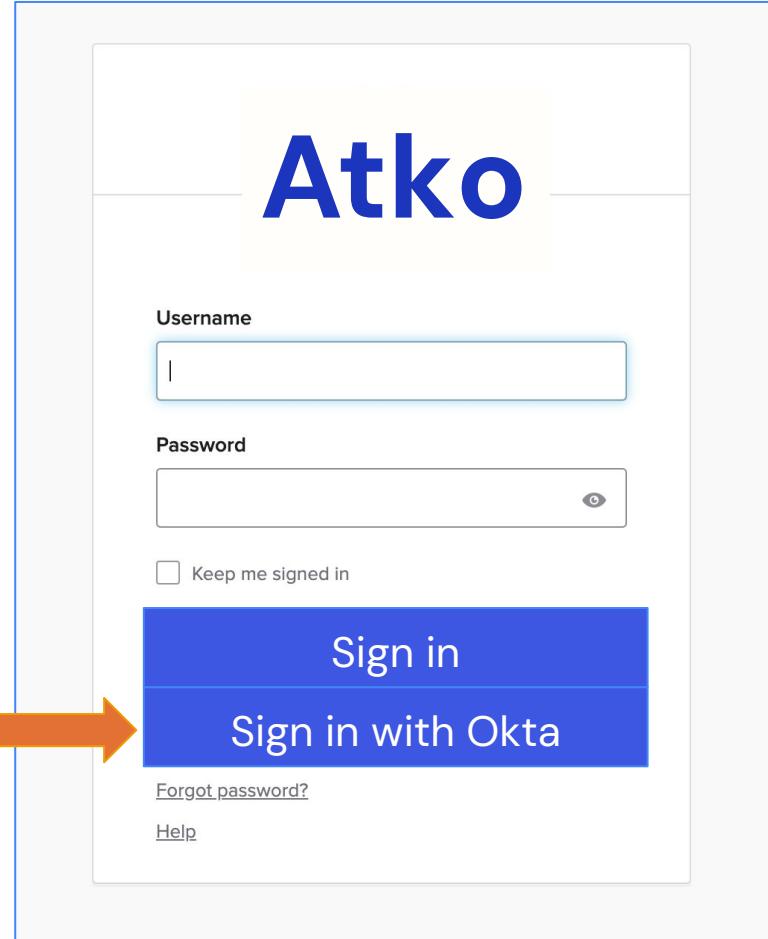
Keep me signed in

Sign in

[Forgot password?](#)

[Help](#)

Identity Provider  
(IdP e.g Okta, Auth0)  
OpenID Connect (OIDC)



The image shows a sign-in page for 'Atko'. At the top, the word 'Atko' is displayed in a large blue font. Below it is a form with fields for 'Username' and 'Password'. There is also a 'Keep me signed in' checkbox and two prominent blue buttons: 'Sign in' and 'Sign in with Okta'. At the bottom of the form are links for 'Forgot password?' and 'Help'.

Atko

Username

Password

Keep me signed in

Sign in

Sign in with Okta

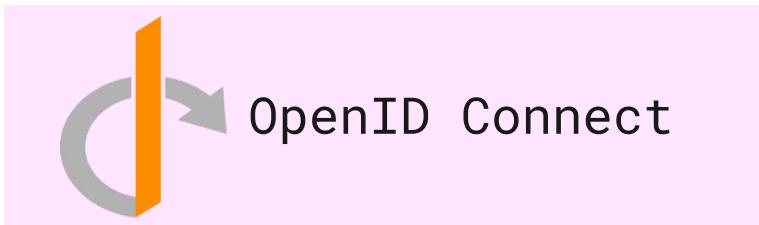
[Forgot password?](#)

[Help](#)



# What is OpenID Connect (OIDC) and why use it?

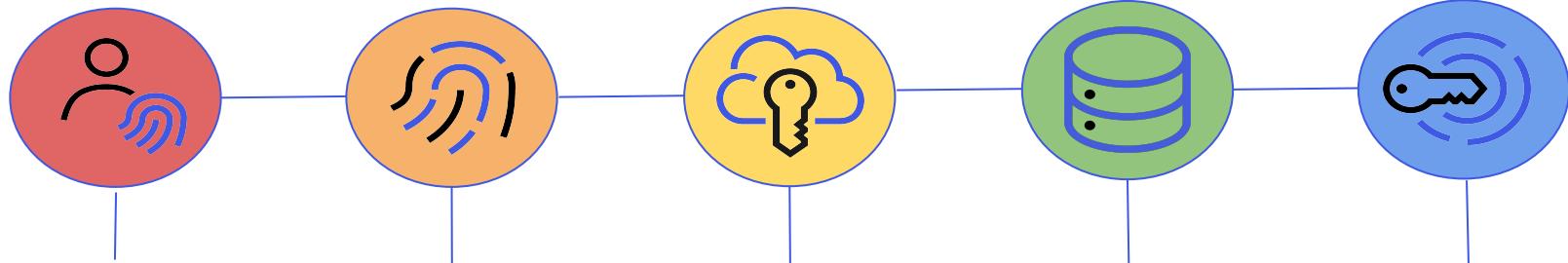
Authentication



Authorization







Standardizes  
scopes:  
openid,  
profile,  
email, and  
address

Standardizes  
claims  
for authn

Identity info  
stored in ID  
token to  
provide SSO  
to multiple  
apps

Standardize  
s endpoints  
i.e.  
/userinfo

Uses JWT  
(JSON Web  
Token) for  
the ID  
Token

# ID token

scopes



Authorize URI (required)  
<https://semonav2.oktapreview.com/oauth2/v1/authorize>

---

Redirect URI (required)  
<https://oidcdebugger.com/debug>

---

Client ID (required)  
0oaqh3fceytYR7U1l0h7

---

Scope (required)  
openid email profile

---

State  
aacq5u8l5bu

---

Nonce  
hxnkyllebb

---

Response type (required)

code       token       id\_token

# What is OpenID Connect (OIDC) and why use it?

ID token  
JWT

### Encoded

PASTE A TOKEN HERE

```
eyJraWQiOjIz0N1RjkyUDQtSzJQaHE3djhDa2x
Vb3VKWmJGdWwyZF9SR0FrWWZ00W5vIiwiYWxnIj
oiUlMyNTYifQ.eyJzdWIiOiIwMHVwcDFoZjE2U2
4xSDJmYjBoNyIsIm5hbWUiOjJzZW1vbmcuaWdhb
WFAb2t0YS5jb20iLCjsb2NhGUoIiJVUyIsImVt
YWlsIjoic2Vtb25hLmlnYW1hQGh1bnRvbmFrLmN
vbSIsInZlcii6MSwiaXNzIjoiaHR0cHM6Ly9zZW
1vbmr2Mi5va3RhchJ1dm1ldy5jb20iLCJhdWqiO
iIwb2FxaNdmY2V5dFlSN1UxSTBoNyIsImhdCI6
MTY50TQ4MTY5NSwiZXhwIjoxNjk5NDg1Mjk1LCJ
qdGkioiJJRC5GN24tdGVmWURSOftWnpWY01UE
FXZTJnYj1CRU1JRGx4cXEcYVTJqQVlviWY1yI
jpbInB3ZCJdLCJpZHAiOiIwMG9wcf0Zxp4cjh5
aFh2UTBoNyIsIm5vbniIjoiicHowd25iMXp4ZmY
iLCJwcmVmZJyjZWRfdXNlcm5hbWUiOjJzZW1vb
EuaWdhbWFAb2t0YS5jb20iLCJnaXZlb19uWY1I
joiU2Vtb25hIiwiZmFtaWx5X25hbWUiOjJJZ2Ft
YSISInpVbmPbmZvIjoiQW1lcm1jYS9Mb3nfQW5
nZWxlcyIsImVtYWlsX3ZlcmImaWVkJp0cnV1LC
JhdXRoX3RpBWi0jE20TkoDE20TQsInRlc3Qi0
iIiLCJmYXZvcm1oZUNvbG9yIjoiicWVkiwiChJ1
ZmVycmVkX2xhbmD1Ywd1IjoiIiwiZw1wbG95ZWV
0dw1iZXIi0iIyMzQ1Njc4In0.jU3o0GCLBzZ1u
Q51jyApwSkF4rmE36W5FIJUh3JoFPW9VuYmdaJ0
ectSqg9_zgtfrRbuQk35z2QSCw4eW189bNhpIrA
sgW4n8M0g4JcCFZOEKQIIYV13wfyG2ZrFgdP3Q9
n9n0672ikjwJMHLiEJGjrYt316Thof6W03kLItd
nEx4T70_W5gCE53Hr4xKrGcB6bNtYMGb9xG_QbF
H9yTMt1H2uMiY19fwSkK_Ruc4GGwQVNjiQVtDH
39KMKXqx6rluyuUWoJY1I7Y9WHFYg0WK3LEJW-
BQiIooONMjSsRVD0kw4ltoIfm9p0trYCFKML-
9Qna3S3uuukQ2-6pf3A
```

### Decoded

EDIT THE PAYLOAD AND SECRET

#### HEADER: ALGORITHM & TOKEN TYPE

```
{
  "kid": "bgCuF92P4-K2Phq7v8CklUouJZbFu12d_RGAkYfN9no",
  "alg": "RS256"
}
```

#### PAYOUT: DATA

```
{
  "sub": "00upp1hf16Sn1H2fb0h7",
  "name": "semona.igama@okta.com",
  "locale": "US",
  "email": "semona.igama@huntonak.com",
  "ver": 1,
  "iss": "https://semonav2.oktapreview.com",
  "aud": "0aqhq3fceytR7U1I0h7",
  "iat": 1699481695,
  "exp": 1699485295,
  "jti": "ID_F7n-
tefYDR8XmZvCISPAnWe2gb9BEMIDlxqq2U2jAYO",
  "amr": [
    "pwd"
  ],
  "idp": "00opp1hezxr8yhXvQ0h7",
  "nonce": "pz0wnb1zxff",
  "preferred_username": "semona.igama@okta.com",
  "given_name": "Semona",
  "family_name": "Igama",
  "zoneinfo": "America/Los_Angeles",
  "email_verified": true,
  "auth_time": 1699481694,
  "test": "",
  "favorite_color": "red",
  "preferred_language": "",
  "employeeNumber": "2345678"
}
```

#### VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  {
    "e": "AQAB"
}
```

claims

# Workshop goal

Support OIDC login in the Todo App:

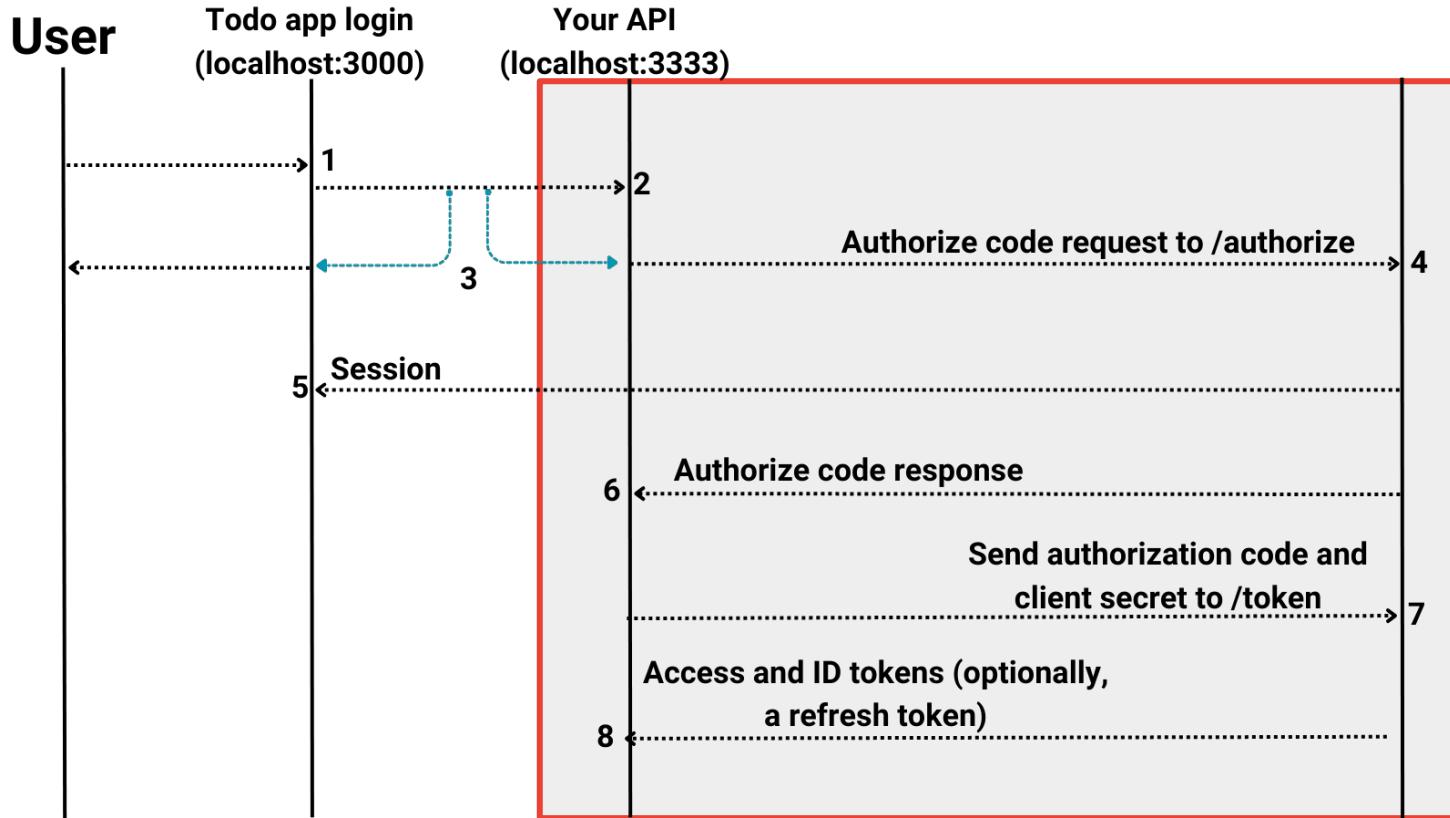
## 1. Frontend

- Login page to handle specific users with IdPs

## 2. Backend

- Enable OIDC flow

# IDP login via OIDC





SaaS

developer



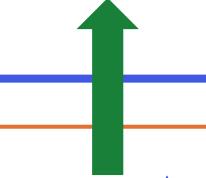
IdP (Okta) +  
login using  
via OIDC

Ready to take on the day?

You won't miss a task with this fantastic Todo app - sign in and get tasking!

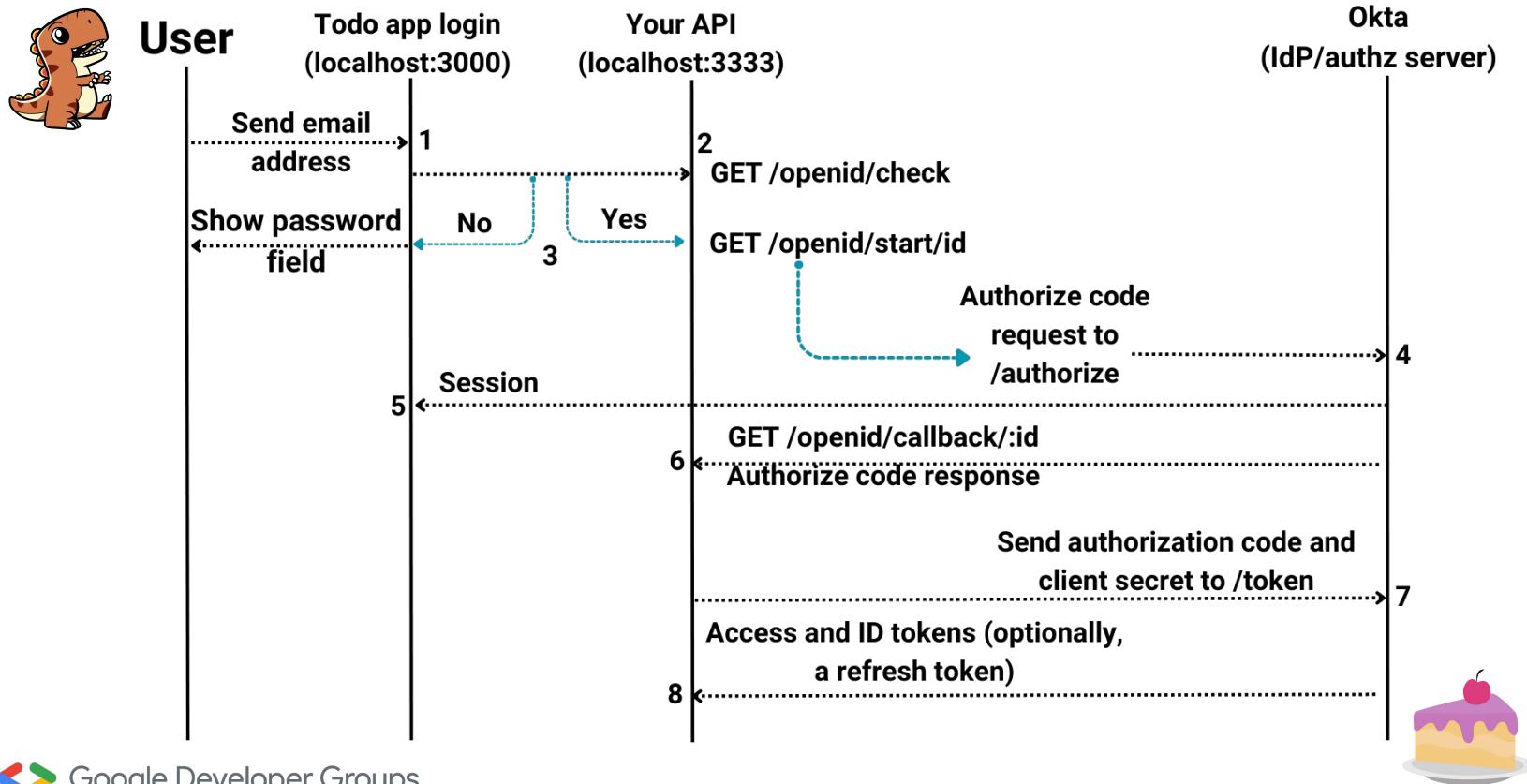
Email address

Sign in



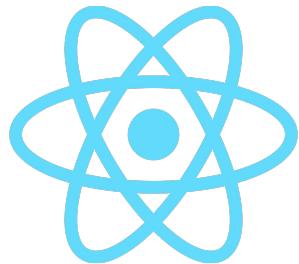
Enterprise  
customers' users

# How will we accomplish adding OIDC in our Todo App?



# Walk through adding OIDC to our Todo sample application

# Sample Todo App



Prisma

Express

# prisma/schema.prisma

```
model User {
    id      Int      @id @default(autoincrement())
    email   String
    password String?
    name    String
    Todo    Todo[]
    org     Org?     @relation(fields: [orgId], references: [id])
    orgId   Int?
    externalId String?
    @@unique([orgId, externalId])
}
```

# prisma/schema.prisma

```
model Org {
    id      Int      @id @default(autoincrement())
    domain String   @unique
    issuer           String @default("")
    authorization_endpoint String @default("")
    token_endpoint     String @default("")
    userinfo_endpoint String @default("")
    client_id         String @default("")
    client_secret      String @default("")
    apikey            String
    Todo      Todo []
    User      User []
}
```

# apps/api/src/main.ts

```
////////// OIDC helper functions
> async function orgFromId(id) { ...
}

> function getDomainFromEmail(email) { ...
}

> app.post('/api/openid/check', async (req, res, next) => { ...
});

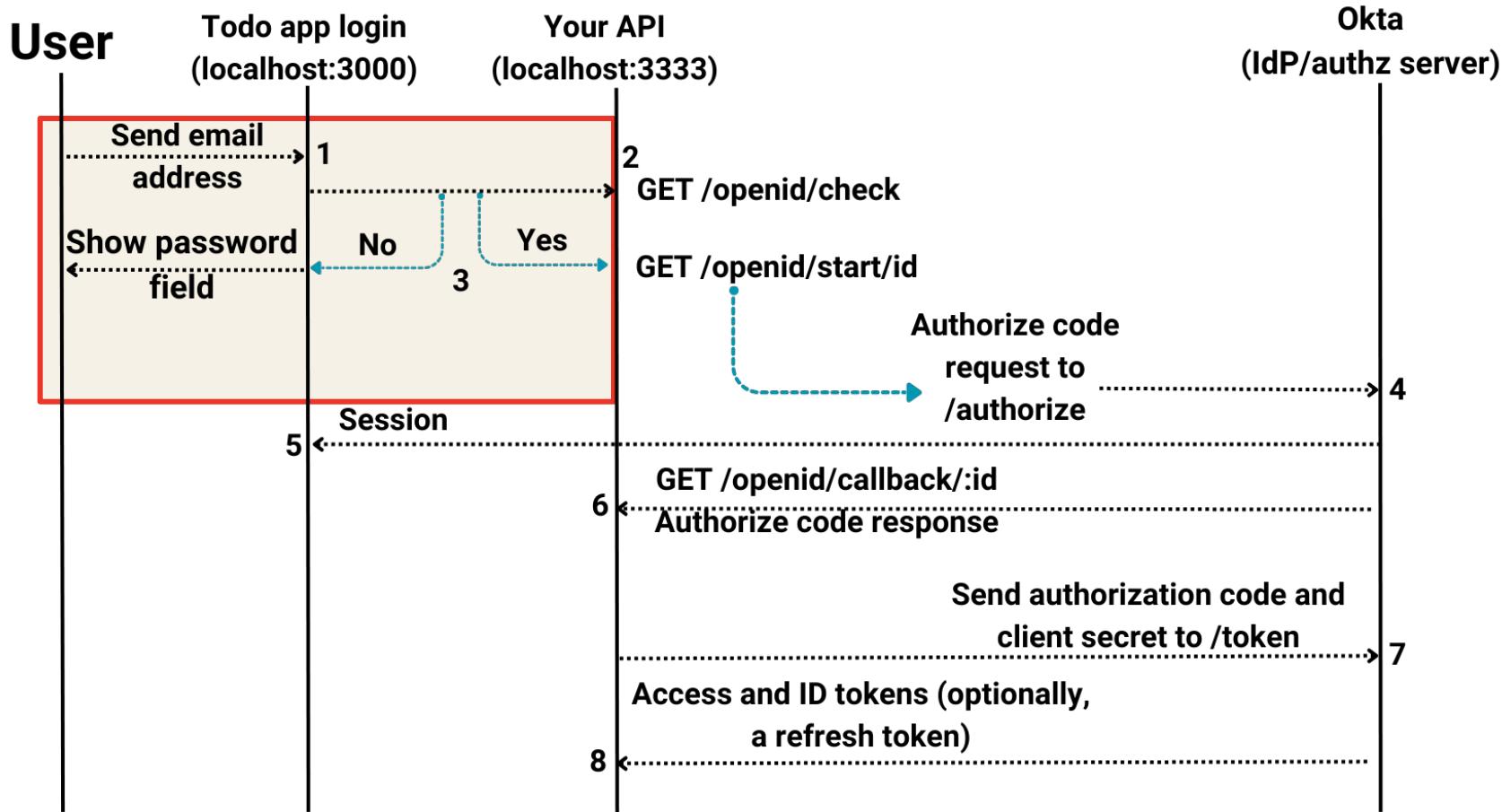
function createStrategy(org) {
>   return new OpenIDConnectStrategy({ ...
},  

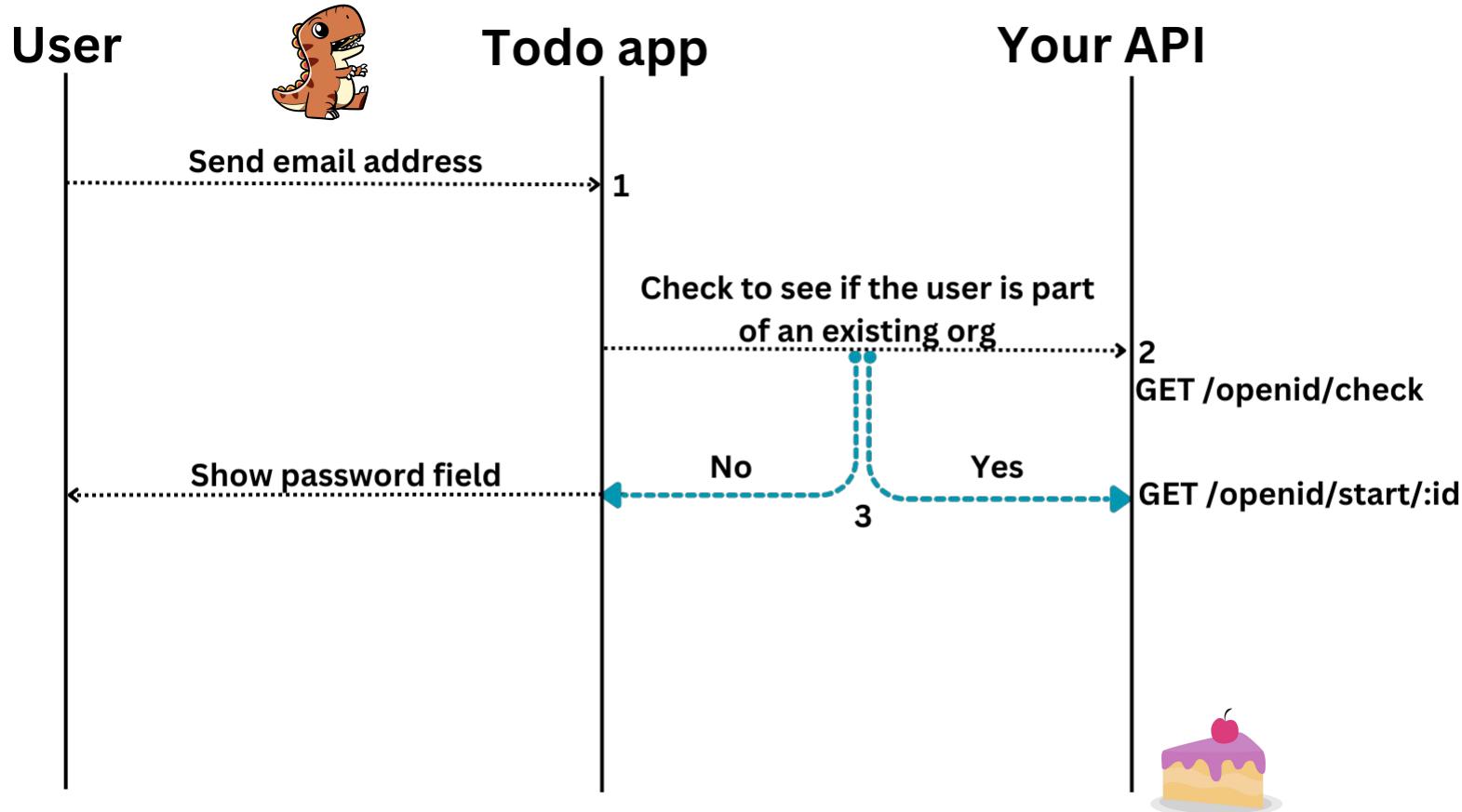
>   async function verify(issuer, profile, cb) { ...
  })
}

> // The frontend then redirects here to have the backend start the OIDC flow. ...
  // to avoid revealing how many enterprise customers you have.)
> app.get('/openid/start/:id', async (req, res, next) => { ...
});

> app.get('/openid/callback/:id', async (req, res, next) => { ...
});
```

# Frontend





## Steps:

1. Hide the password field in  
apps/todo-app/src/app/components/signin.tsx.  
Find the div containing the password, give it  
an identifier, and set it to be hidden by  
default:
2. Submit the email address to server
3. Confirm the user's organization

# Before

Ready to take on the day?

You won't miss a task with this fantastic Todo app - sign in and get tasking!

Email address

Password

[Sign in](#)



```
graph LR; A[Before] --> B[After]; B --> C[Redirect to IdP]
```

# After

Ready to take on the day?

You won't miss a task with this fantastic Todo app - sign in and get tasking!

Email address

[Sign in](#)



```
graph LR; A[Before] --> B[After]; B --> C[Redirect to IdP]
```

# Redirect to IdP

**okta**

Sign In

Username

Password

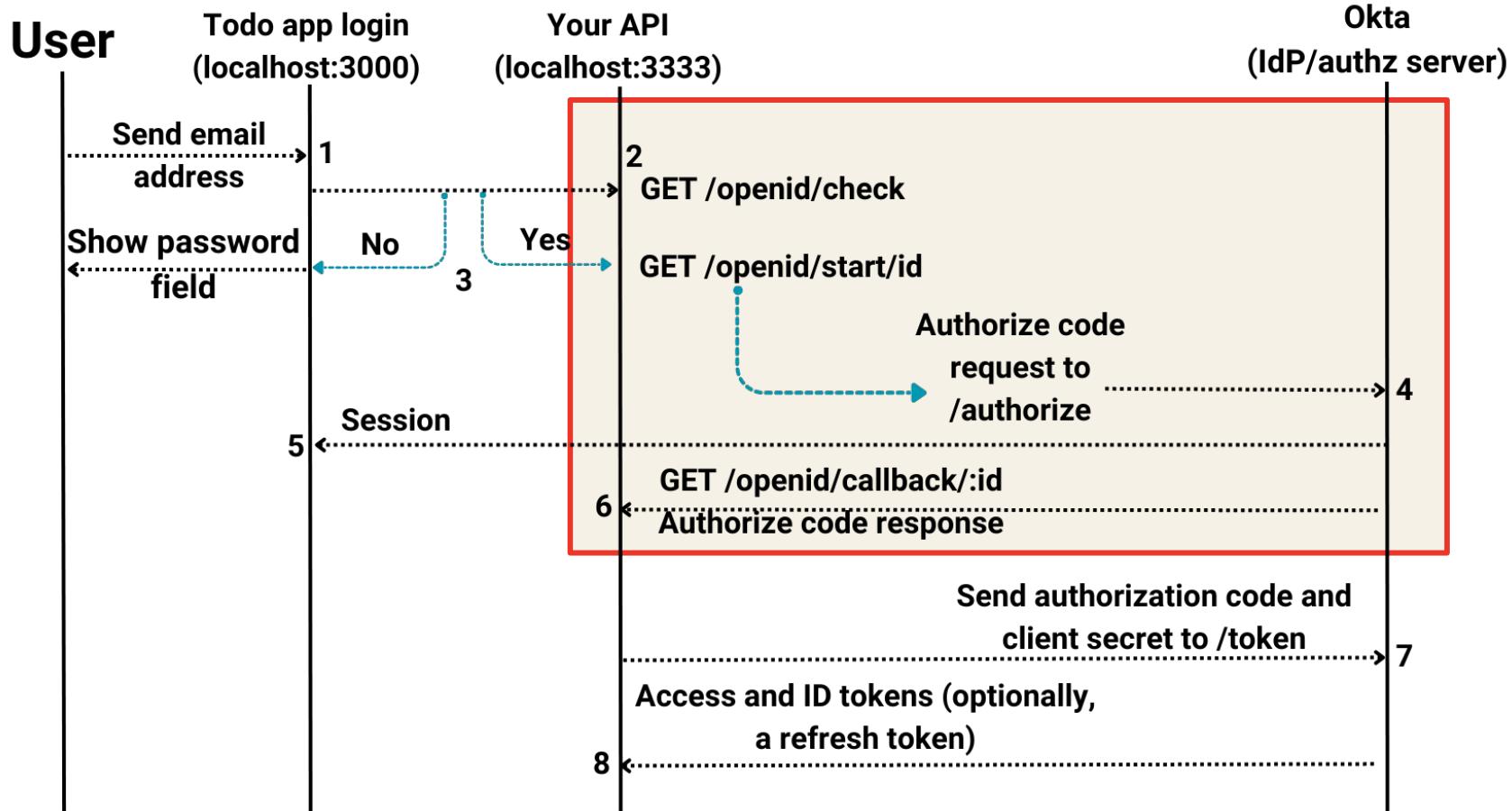
Keep me signed in

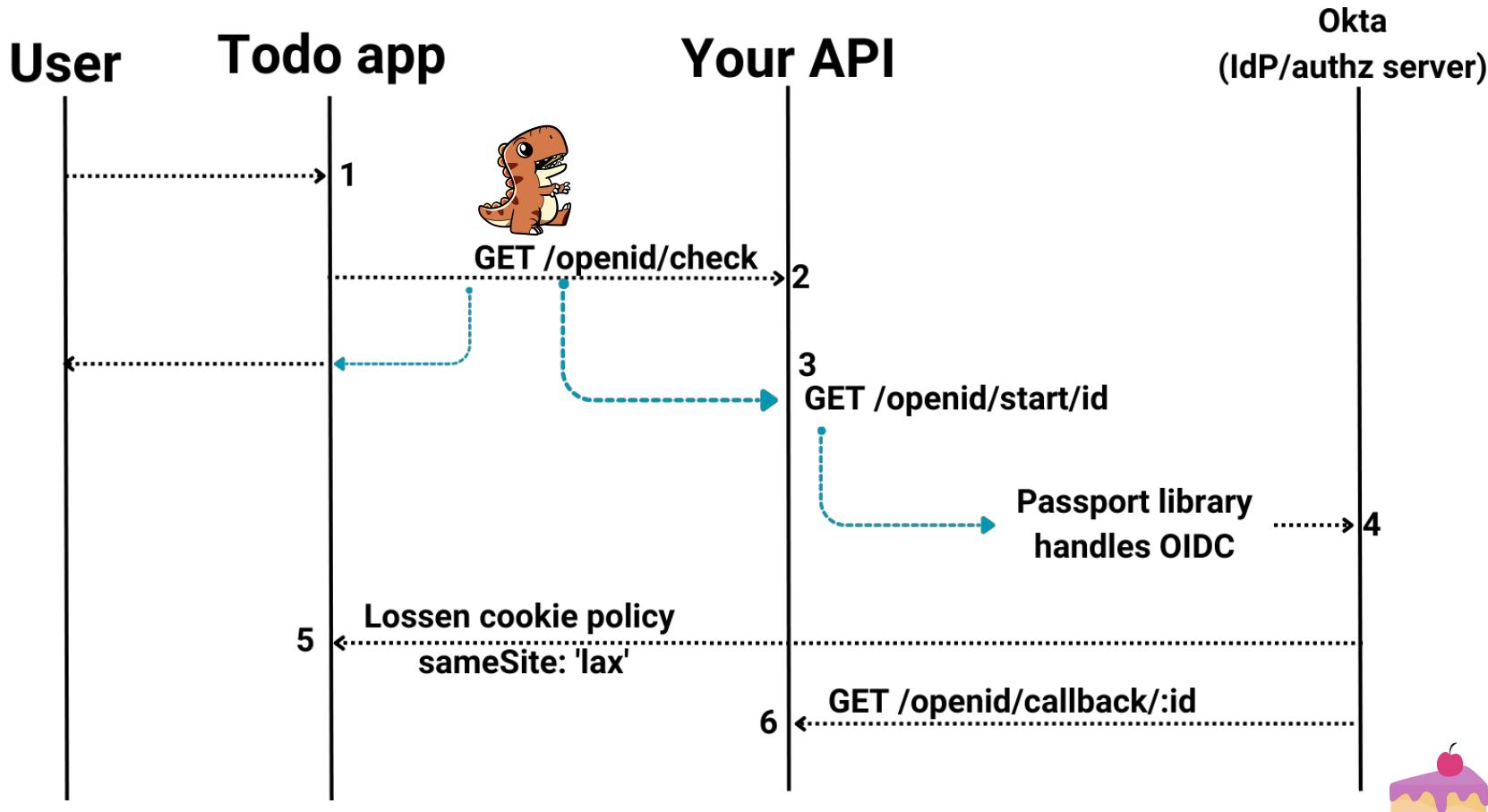
[Sign in](#)

[Forgot password?](#)

[Help](#)

# Backend





# Update the Express API to support OIDC

## Steps:

1. Install the Passport OIDC Library
2. Add helper functions `orgFromId` and `getDomainFromEmail`

# Add route to check the OpenID org

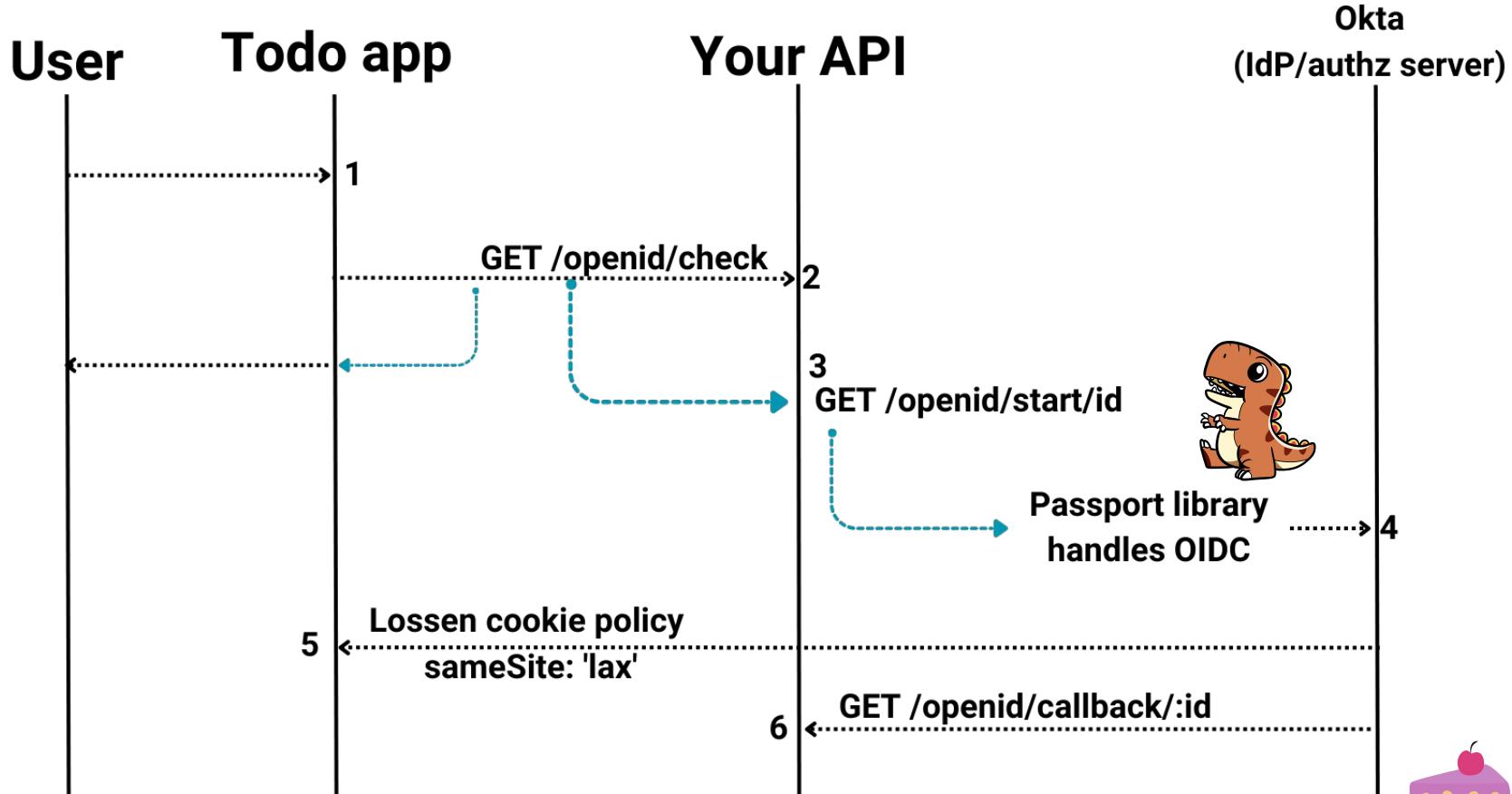
## Steps:

1. Modify `getDomainFromEmail` to include `/api/openid/check` endpoint which will return the numeric ID of the org that the user's email domain belongs to or otherwise return `null`

# Use the Passport OIDC library

## Steps:

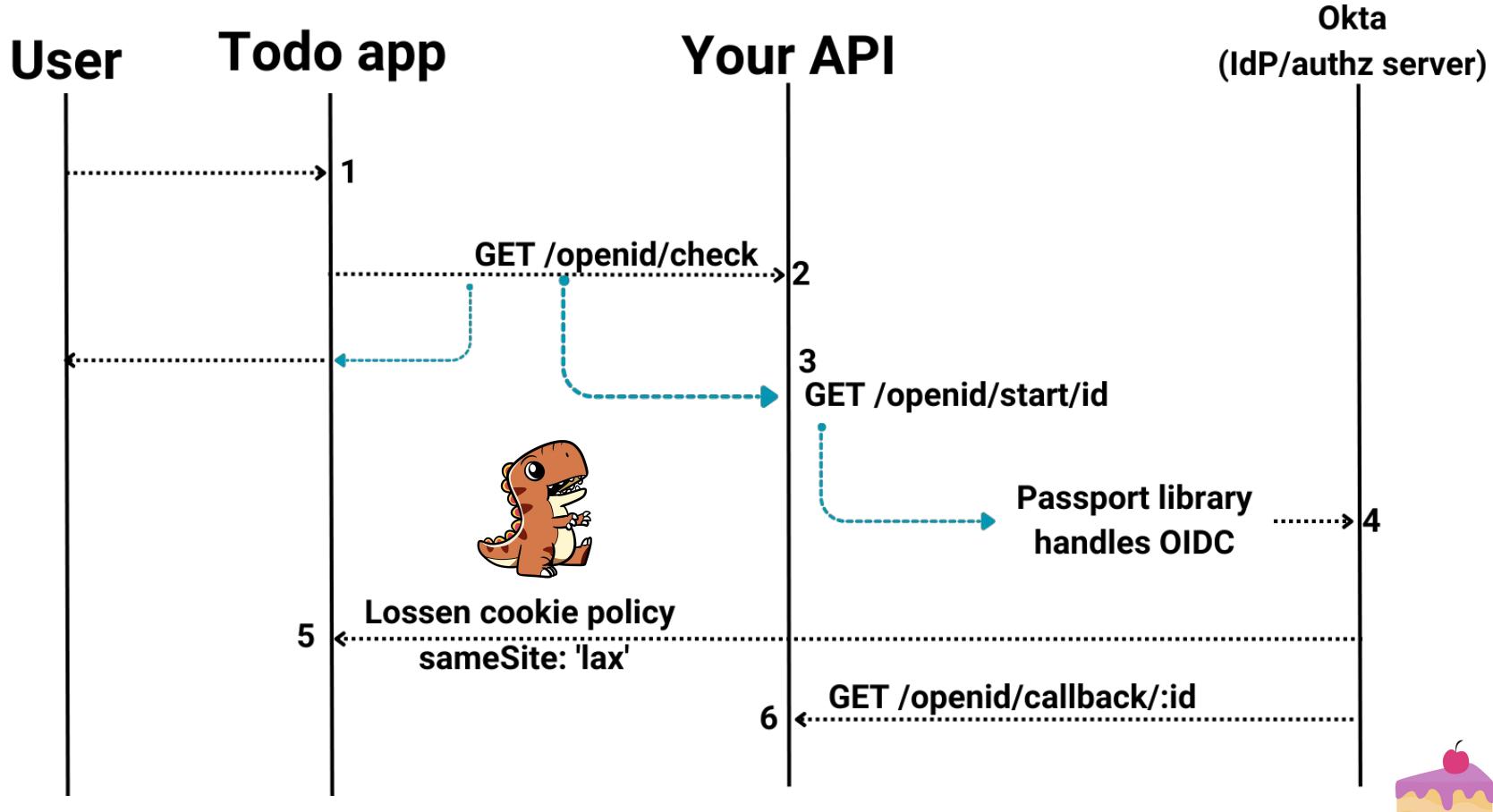
1. Add the import for the OIDC passport after the import for passport-local at the top of `apps/api/src/main.ts`  
→ `import passportOIDC from 'passport-openidconnect';`
2. Define a variable for the OIDC strategy so you can utilize it within the API  
→ `const OpenIDConnectStrategy = passportOIDC.Strategy;`
3. Create a strategy for each org



# **Loosen the cookie policy for the OIDC redirect authentication flow**

Steps:

1. In `apps/api/src/main.ts`, change the session cookie policy from `sameSite: 'strict'` to `sameSite: 'lax'`



# Enable the OpenID flow

## Steps:

1. The frontend will redirect the browser to the backend's `/openid/start/${org_id}` endpoint to initiate the OpenID login flow when a user belongs to an org.

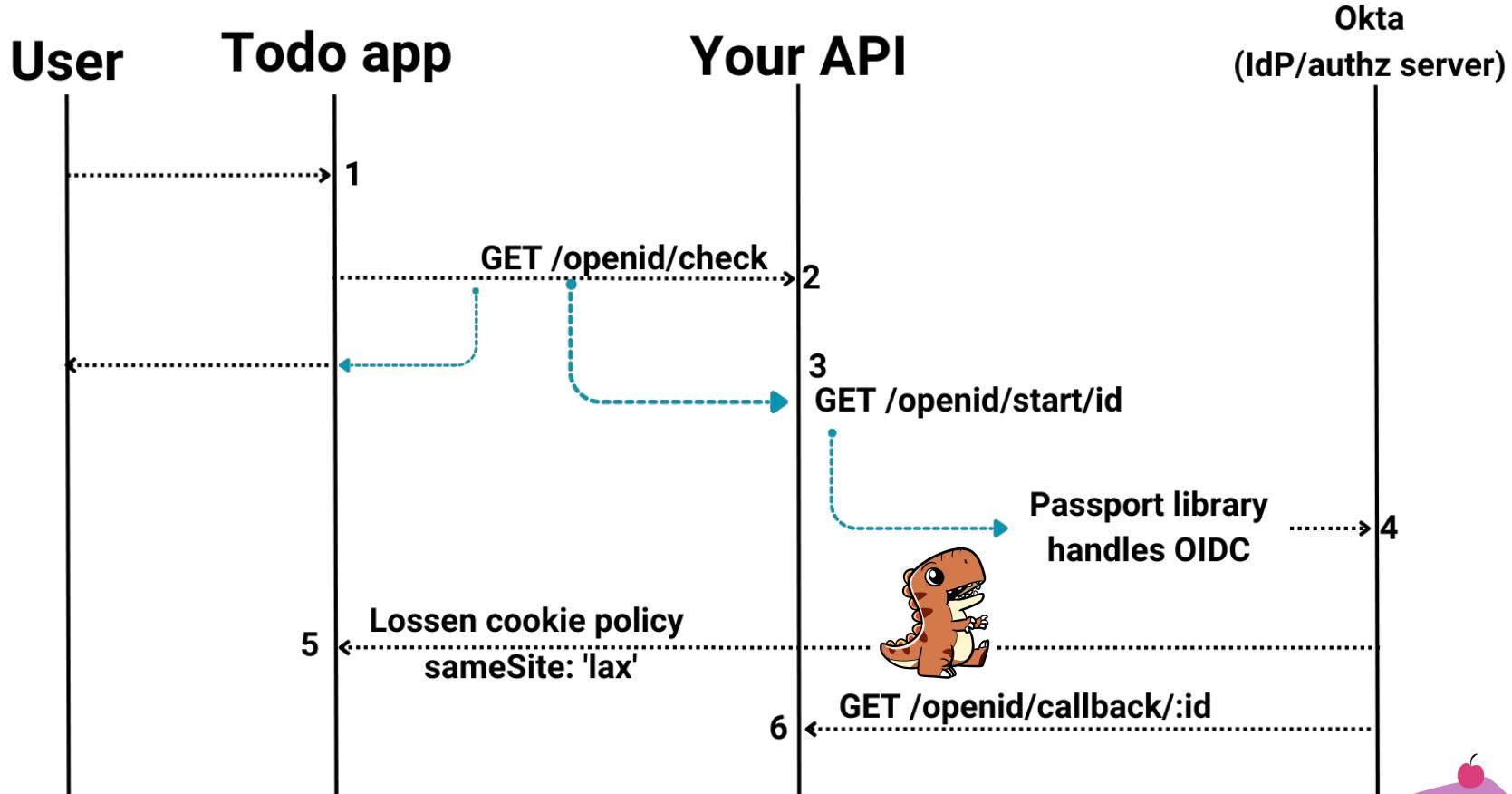
# Recap

To recap, redirecting the user to the backend's [`/openid/start/`](#) endpoint with an org's ID will use passport to redirect the user to their org's OpenID server. The user will prove their identity to their org's OpenID server, and that server will redirect the user to the app's backend, at which point Passport will start a session to the Todo app. Only the app's backend will see the information from the OIDC server, so frontend tampering cannot intercept the user's session.

# Receive callback after authentication

## Steps:

1. Build a callback route to the end of [`apps/api/src/main.ts`](#) in order to confirm that the ID of the request corresponds to an existing org in the database



# Connect to the Identity Provider

# developer.okta.com

The screenshot shows the top navigation bar of the developer.okta.com website. It includes links for 'Community', 'Blog', 'Pricing', 'Okta.com', 'Log in', and a prominent 'Sign up' button. An orange arrow points from the text 'Choose what works best. Sign up is free.' to the 'Sign up' button.

okta Developer

Community ▾ Blog Pricing

Okta.com Log in Sign up

Guides Concepts References Languages & SDKs Release Notes

## Okta Developer

Our developer portal enables you to deploy auth that protects your users, apps, APIs, and infrastructure.

Get your app [enterprise-ready](#) with [free virtual workshops!](#)

### Start your Workforce Identity journey

Welcome! Start with **Learn** if you're new to Workforce Identity Cloud, or find the step in your journey and follow the links to browse docs.

#### Learn



#### Understand the basics of identity

Learn the key concepts you need for creating identity and access management (IAM) solutions for WIC.

[Understand IAM](#)

[How WIC works](#)

[Choose an authentication protocol](#)

[Get a developer org](#)

Choose what works best. **Sign up is free.**

#### Customer Identity Cloud

powered by auth0

**FREE**

For the first tier

**BEST FOR DEVELOPERS**

#### Secure my customers or SaaS applications

Build intuitive, secure user experiences in customer-facing applications.

[Try Customer Identity Cloud →](#)

#### Workforce Identity Cloud

**FREE TRIAL**

Get access for 30 days

**BEST FOR IT ADMINS**

#### Secure my employees, contractors, & partners

Manage secure, frictionless access to the tools and data your teams need, on demand.

[Try Workforce Identity Cloud →](#)

**FREE**

Test, explore, and manage integrations

**BEST FOR DEVELOPERS**

#### Access the Okta Developer Edition Service

Test your code and apps, as well as manage and automate Okta for employees and partners.

[Sign up free for Developer Edition](#)

# Okta CLI - cli.okta.com

## Okta CLI (beta) Documentation

The Okta CLI is the easiest way to get started with Okta!  
Get started today by installing on your platform.

```
brew install --cask oktadeveloper/tap/okta
```

[macOS Install](#)

[View installation instructions for all platforms →](#)  
[View all Okta CLI commands →](#)

## Getting Started

```
$ okta start spring-boot
Registering for a new Okta account, if you would like to use an existing account, use 'okta login' instead.

First name: Jamie
Last name: Example
Email address: jamie@example.com
Company: Okta Test Company
Creating new Okta Organization, this may take a minute:
OrgUrl: https://dev-123456.okta.com
An email has been sent to you with a verification code.
```

# Create an OIDC Application in Okta

Steps:

1. In the Okta Admin Console, navigate to Applications under the “Applications” heading in the left sidebar.
2. Click the Create App Integration button
3. In the “Create a new app integration” dialog box, select the OIDC - OpenID Connect sign-in method, specify that the application is a “Web Application” in the “Application Type” options that appear, and use the “Next” button to continue.
4. Give this app integration a useful name like “Todo app”, and make sure that Authorization Code box is selected under “Client acting on behalf of a user” in the Grant type field.
5. Find the ID used for this customer in your app by checking the database. For this workshop, the first customer has ID 1, so the sign-in redirect URI is  
<http://localhost:3333/openid/callback/1>
6. under Assignments, select “Allow everyone in your organization to access”. Saving these changes using the Save button at the bottom of the page will take you to the app’s General settings tab, which provides a Client ID and Client Secret.



Search for people, apps and groups

?

semona.igama+de...  
okta-dev-77700421

Dashboard

Directory

Customizations

Applications

Applications

Self Service

API Integrations

Security

Workflow

Reports

Settings

## Applications

Help

Developer Edition provides a limited number of apps.

Deactivate unused apps or check out our [plans page](#). Contact us to find a plan that is right for your organization.

Create App Integration

Browse App Catalog

Assign Users to App

More ▾

Search

STATUS

ACTIVE

INACTIVE



Okta Admin Console



Okta Browser Plugin



Okta Dashboard

## Create a new app integration

### Sign-in method

[Learn More !\[\]\(d022703cf7c7a09c8fdc4d0a5796b273\_img.jpg\)](#)

**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  
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

## New Web App Integration

### General Settings

App integration name

Todo App

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

Client-initiated backchannel authentication flow (CIBA)

Implicit (hybrid)

Sign-in redirect URIs

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

[Learn More](#)

Allow wildcard \* in sign-in URI redirect.

http://localhost:8080/authorization-code/callback



http://localhost:3333/openid/callback/1



[+ Add URI](#)

## Assignments

### Controlled access

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

### Enable immediate access (Recommended)

Recommended if you want to grant access to everyone without pre-assigning your app to users and use Okta only for authentication.

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

#### Enable immediate access with **Federation Broker Mode**



To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. Learn more about [Federation Broker Mode](#).

Save

Cancel

# Add org configuration to the database

## Steps:

1. Edit the database and add a new org using Prisma Studio.  
→ `npx prisma studio`
2. Domain - Enter the domain name of this organization i.e. `whiterabbit.fake`
3. Fill out the `client_id` and `client_secret` for the org with ID 1, using the values from Okta.
4. Issuer - In the “Security” section of the sidebar in the Okta Admin Console, navigate to API. This page lists the Issuer URI for the Okta organization, which goes into the app's database for that org as its `issuer`.
5. Authorization endpoint and Token endpoint - On the same page in the Okta Admin console as the issuer, click the name of the default authorization server, find the Metadata URI. This URI will be of the form `your-dev-account-id.okta.com/oauth2/default/.well-known/oauth-authorization-server`. Click on the URI to open it in the browser where you will see data in JSON format. From this authorization server metadata, copy the `authorization_endpoint` to the `authorization_endpoint` field in your app's database. Copy the `token_endpoint` to the corresponding field in the database as well.
6. Userinfo endpoint - To find the `userinfo_endpoint`, replace the string `oauth-authorization-server` in the metadata URL with `openid-configuration`, and copy the `userinfo_endpoint` from the resulting page to the database.
7. Save changes!!

Dashboard

Directory

Customizations

Applications

Applications

Self Service

API Service Integrations

Security

Workflow

Reports

Settings

## Todo App

Active



View Logs

General

Sign On

Assignments

Okta API Scopes

Application Rate Limits



### Client Credentials

[Edit](#)

Client ID

0oaczcp47jVYyB9w15d7  
[Edit](#)

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

### Client authentication

 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
Oct 27, 2023	*****	<a href="#">Edit</a>



General

HealthInsight

Authenticators

Authentication Policies

Global Session Policy

Profile Enrollment

Identity Providers

Delegated Authentication

Networks

Behavior Detection

Device Assurance Policies

Device Integrations

Administrators

API

Workflow

[← Back to Authorization Servers](#)

## default

[Help](#)[Active ▾](#)

Default

[Settings](#)[Scopes](#)[Claims](#)[Access Policies](#)[Token Preview](#)

### Settings

[Edit](#)

Name

default

Audience

api://default

Description

Default Authorization Server for your Applications

Issuer

Okta URL (<https://dev-77700421.okta.com/oauth2/default>)

Metadata URI

<https://dev-77700421.okta.com/oauth2/default/.well-known/oauth-authorization-server>Signing Key Rotation [?](#)

Automatic

Last Rotation

Oct 27, 2023

### Authorization Servers

An authorization server defines your security boundary, and is used to mint access and identity tokens for use with OIDC clients and OAuth 2.0 service accounts when accessing your resources via API. Within each authorization server you can define your own OAuth scopes, claims, and access policies. Read more at [help](#)

[FAQ](#)

```
object {26}
  issuer : "https://dev-77700421.okta.com/oauth2/default"
  authorization_endpoint : "https://dev-77700421.okta.com/oauth2/default/v1/authorize"
  token_endpoint : "https://dev-77700421.okta.com/oauth2/default/v1/token"
  userinfo_endpoint : "https://dev-77700421.okta.com/oauth2/default/v1/userinfo"
  registration_endpoint : "https://dev-77700421.okta.com/oauth2/v1/clients"
  jwks_uri : "https://dev-77700421.okta.com/oauth2/default/v1/keys"
  response_types_supported [6]
    0 : "code"
    1 : "id_token"
    2 : "code id_token"
    3 : "code token"
    4 : "id_token token"
    5 : "code id_token token"
  response_modes_supported [4]
    0 : "query"
    1 : "fragment"
    2 : "form_post"
    3 : "okta_post_message"
  grant_types_supported [6]
    0 : "authorization_code"
    1 : "implicit"
    2 : "refresh_token"
    3 : "password"
    4 : "urn:ietf:params:oauth:grant-type:device_code"
    5 : "urn:openid:params:grant-type:ciba"
```

← → ⌂ ⓘ localhost:5555

User Org + ⚙️

Filters None Fields All Showing 1 of 1 Add record

	id #	domain	issuer	authorization_endpoint	token_endpoint	userinfo_endpoint	client_id	client_secret	apikey	Todo [ ]
	1	whiterabbit.fake	https://dev-77700421...	https://dev-77700421...	https://dev-77700421...	https://dev-77700421...	0oaczcp47jVyyB9w15d7	G_Y2K69PM2r9rK46uSBY4...		0 Todo

# **Use OIDC authentication in the application**

## Steps:

1. Create some user accounts in your Okta Admin Console, and try logging into the Todo app as those users! Use Prisma (`npx prisma studio`) to see how each user's database record is created the first time they log in.

Dashboard

Directory

People

Groups

Devices

Profile Editor

Directory Integrations

Profile Sources

Customizations

Applications

## People

Add person

More actions ▾

Search for users by first name, primary email or username



Advanced search ▾

Status

All

Showing

Person &amp; username

Primary email

semona igama

semona.igama+devtest@okta.com

semona.igama+devtest@okta.com

## Add Person

User type 

User

First name

Test

Last name

User

Username

test.user@whiterabbit.fake

Primary email

test.user@whiterabbit.fake

Groups (optional)

You haven't added any [groups](#)

Activation

Activate now

I will set password

••••••••••

To create new users with password, enrollment policy  
must set password as required

User must change password on first login

Do not send unsolicited or unauthorized activation emails. [Read more](#)

Save

Save and Add Another

Cancel

Connecting to 

Sign in with your account to access Todo App



# Ready to take on the day?

You won't miss a task with this fantastic Todo app - sign in and get tasking!

Email address

test.user@whiterabbit.fake

Sign in

# okta

Sign In

Username

test.user@whiterabbit.fake

Password



Keep me signed in

Sign in

[Forgot password?](#)

[Help](#)



Welcome, Test User! [Profile](#) [Sign out](#)

# Ready to take on the day?

You won't miss a task with this fantastic Todo app - sign in and get tasking!

[Where's my todos?](#)

localhost:5555

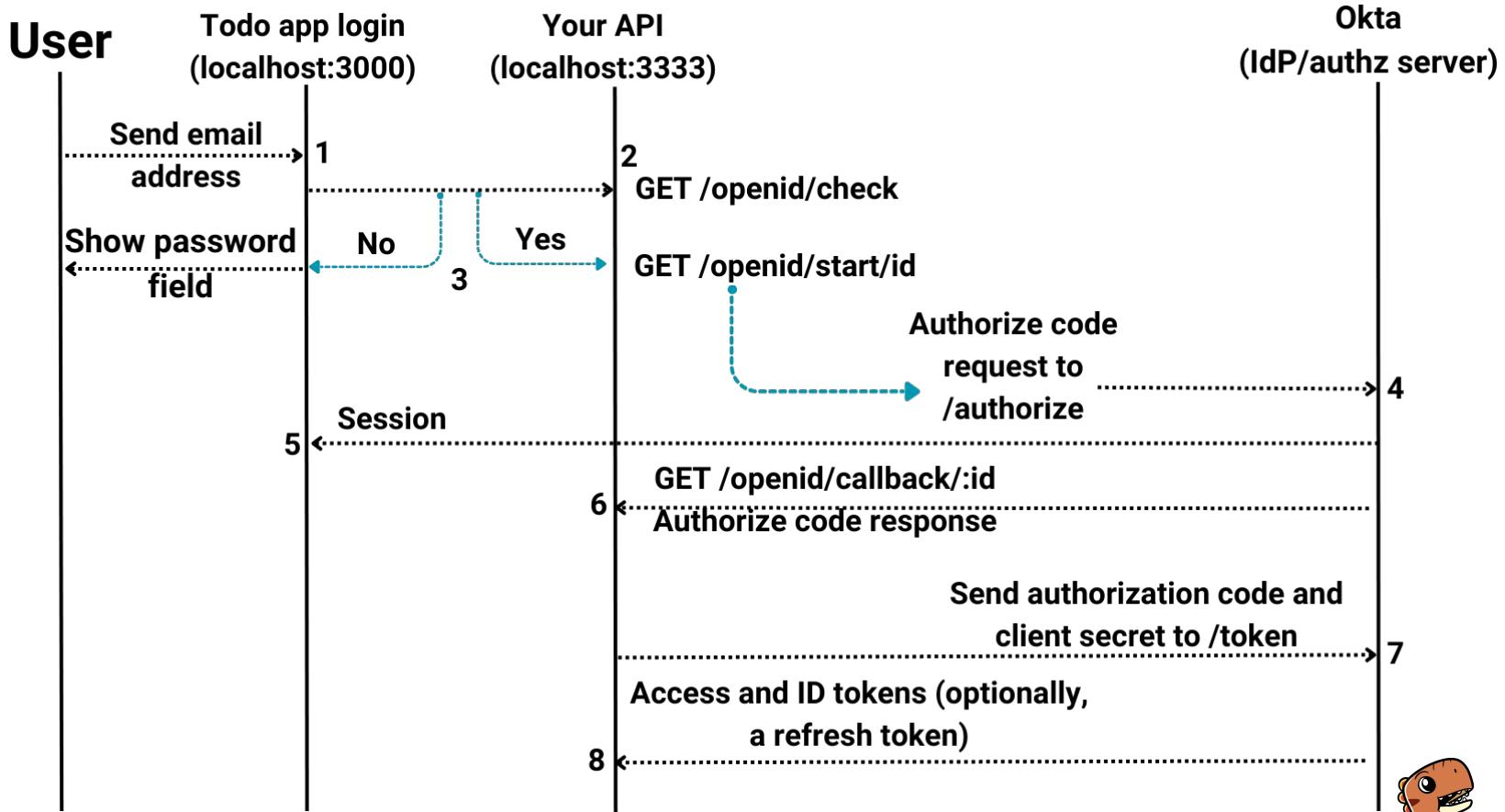
User Org +

Filters None Fields All Showing 2 of 2 Add record

	id #	email A?	password A?	name A?	Todo []	org ()?	orgId #?	externalId A?
	1	semona.igama+devtest@...	null	semona igama	0 Todo	Org	1	00ucz8s1y4qGmS6F25d7
	2	test.user@whiterabbit...	null	Test User	0 Todo	Org	1	00ud0i9yglooMcfNY5d7

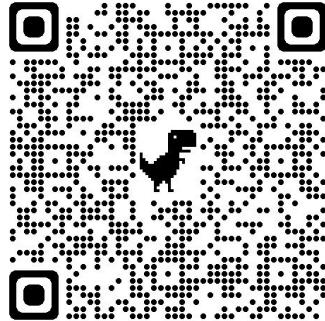
# Recap

1. From Aaron's video



# Friends don't let friends build auth. Stay in touch!

Survey



@sudomonas  
@0ktaDev on YouTube, X  
[developer.okta.com](https://developer.okta.com)  
[devforum.okta.com](https://devforum.okta.com)  
**#i<30IDC**

# Resources

- <https://auth0.com/intro-to-iam/what-is-openid-connect-oidc>
- [https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html)
- <https://www.okta.com/openid-connect/>
- <https://jwt.io/>
- <https://jwt.io/introduction>
- Tenor GIF -  
<https://tenor.com/view/mando-way-this-is-the-way-mandalorian-star-wars-gif-18467370>
-