Common Questions Answers

Q: For some reason when I get my invite email to my application, it redirects me to “localhost:3000” - but I didn’t set this. How can I change it?

Solution:

1. Go to **Configurations → Applications**
2. Update the App URL in your application settings to match your actual domain

Q: Why don’t I see the ‘Users’ page on my admin portal (in the app settings button)?

Solution: User management features need to be explicitly enabled in your Frontegg configuration.

1. Go to **Frontegg Dashboard → Builder → Admin Portal**
2. Enable the **"Users"** feature
3. Save changes and refresh your application

Bonus:

1. Check **Roles & Permissions** settings
2. Ensure your user role has **"Write Users"** permission enabled

Q: For some reason I don’t have the google login - why is that?

Solution: In your **Login Box Builder** you should Activate “**Google**” under **Social logins**

Q: Explain what refresh tokens are and why we need them?

Solution: Refresh tokens are long-lived credentials used to obtain new access tokens without requiring the user to re-authenticate.

We need them because access tokens typically have short lifespans (minutes to hours) for security reasons. When an access token expires, rather than forcing the user to log in again, the application can use a refresh token to get a new access token automatically.

Bonus: The 401 error is your app trying to re-authenticate using an expired access token
Bonus: JWT tokens are often used as access tokens - they're self-contained with encoded user info and permissions, typically short-lived (15-60 minutes), and sent with every API request for authorization. Refresh tokens are separate credentials with longer lifespans that exist solely to obtain new JWT access tokens when they expire. When your JWT expires and returns a 401, the app automatically sends the refresh token to the auth server, which validates it and issues a new JWT, allowing seamless re-authentication without user login.

Q: Can you please point out which API I can use to change the user's active tenant? How should one use it?
Solution:
`PUT /identity/resources/applications/user-tenants/active/v1`
Usage:

```
await
fetch('https://api.frontegg.com/identity/resources/applications/user-tenants/active/v1', {
  method: 'PUT',
  headers: {
    'Content-Type': 'application/json',
    'frontegg-user-id': 'user-123',
    'Authorization': 'Bearer your-jwt-token'
  },
  body: JSON.stringify({
    activeApplicationTenants: [{
      applicationId: 'your-app-id',
      tenantId: 'new-tenant-id'
    }]
  })
});
```

This switches the user's active tenant for your application. The user will need to refresh their session to see the change take effect.

Bonus:

Using the SDK

```
  switchTenant(tenant: any) {
   this.fronteggAuthService.switchTenant({
     tenantId: tenant.tenantId,
   });
 }
```

Q: Is there a way to block users with a certain email from signing up to a tenant? If yes, how?

Solution: Yes

1. Navigate to **Management** → **Accounts**
2. Select your target tenant
3. Click the **Security** tab
4. Go to **Restrictions** section
5. Under **Domain restrictions**, select **"Deny only"**
6. Add the domains you want to block