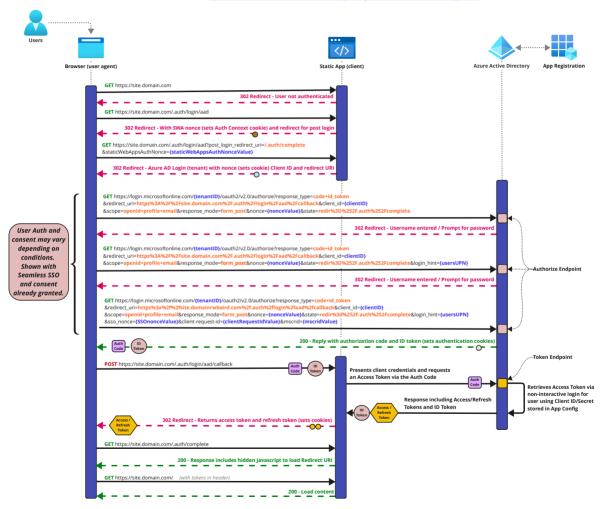# Azure Static Web App

- **configured with custom AAD auth to lock down to single tenant**
  - **https://learn.microsoft.com/en-us/azure/static-web-apps/authentication-custom?tabs=aad%2Cinvitations**
- **entire site wrapped with auth**
  - **https://learn.microsoft.com/en-us/azure/static-web-apps/configuration#restrict-access-to-entire-application**

Users

Browser (user agent)

Static App (client)

Azure Active Directory

App Registration

GET https://site.domain.com

302 Redirect - User not authenticated

GET https://site.domain.com/.auth/login/aad

302 Redirect - With SWA nonce (sets Auth Context cookie) and redirect for post login

GET https://site.domain.com/.auth/login/aad?post_login_redirect_uri=**/.auth/complete**
&staticWebAppsAuthNonce=**{staticWebAppsAuthNonceValue}**

302 Redirect - Azure AD Login (tenant) with nonce (sets cookie) Client ID and redirect URI

GET https://login.microsoftonline.com/**{tenantID}**/oauth2/v2.0/authorize?response_type=**code+id_token**
&redirect_uri=**https%3A%2F%2Fsite.domain.com%2F.auth%2Flogin%2Faad%2Fcallback**&client_id=**{clientID}**
&scope=**openid+profile+email**&response_mode=**form_post**&nonce=**{nonceValue}**&state=**redir%3D%252F.auth%252Fcomplete**

302 Redirect - Username entered / Prompt for password

GET https://login.microsoftonline.com/**{tenantID}**/oauth2/v2.0/authorize?response_type=**code+id_token**
&redirect_uri=**https%3A%2F%2Fsite.domain.com%2F.auth%2Flogin%2Faad%2Fcallback**&client_id=**{clientID}**
&scope=**openid+profile+email**&response_mode=**form_post**&nonce=**{nonceValue}**&state=**redir%3D%252F.auth%252Fcomplete**&login_hint=**{usersUPN}**

302 Redirect - Username entered / Prompt for password

GET https://login.microsoftonline.com/**{tenantID}**/oauth2/v2.0/authorize?response_type=**code+id_token**
&redirect_uri=**https%3a%2f%2fsite.domainrwbaird.com%2f.auth%2flogin%2faad%2fcallback**&client_id=**{clientID}**
&scope=**openid+profile+email**&response_mode=**form_post**&nonce=**{nonceValue}**&state=**redir%3d%252f.auth%252fcomplete**&login_hint=**{usersUPN}**
&sso_nonce=**{SSOnonceValue}**&client-request-id=**{clientRequestIdValue}**&mscrid=**{mscridValue}**

Authorize Endpoint

User Auth and consent may vary depending on conditions. Shown with Seamless SSO and consent already granted.

200 - Reply with authorization code and ID token (sets authentication cookies)

Auth Code   ID Token

POST https://site.domain.com/.auth/login/aad/callback

Auth Code   ID Token

Presents client credentials and requests an Access Token via the Auth Code

Auth Code

Token Endpoint

Retrieves Access Token via non-interactive login for user using Client ID/Secret stored in App Config

Response including Access/Refresh Tokens and ID Token

ID Token   Access / Refresh Token

Access / Refresh Token

302 Redirect - Returns access token and refresh token (sets cookies)

GET https://site.domain.com/.auth/complete

200 - Response includes hidden Javascript to load Redirect URI

GET https://site.domain.com/ *(with tokens in header)*

200 - Load content

Hybrid Flow
https://learn.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow#request-an-id-token-as-well-or-hybrid-flow