Four 51 API Documentation

Environments

- Staging (Sandbox)
  - API URL - https://stage-four51-api.waxingthecity.com/
  - API Documentation - https://stage-four51-api.waxingthecity.com/api-docs/index.html
  - OIDC Discovery URL - https://stage-identity.waxingthecity.com/.well-known/openid-configuration
  - Token URL - https://stage-identity.waxingthecity.com/connect/token
  - Authorize URL - https://stage-identity.waxingthecity.com/connect/authorize
- Production
  - URL - https://four51-api.waxingthecity.com/api-docs/index.html
  - API Documentation - https://four51-api.waxingthecity.com/api-docs/index.html
  - OIDC Discovery URL - https://identity.waxingthecity.com/.well-known/openid-configuration
  - Token URL – https://identity.waxingthecity.com/connect/token
  - Authorize URL – https://identity.waxingthecity.com/connect/authorize

Our Identity server (IdP) is OIDC spec compliant so that any OIDC reference material or SDK can be used to perform the auth steps described below. It has been configured with a redirect URL to allow testing auth flows and API calls with Postman. The api-docs site also has 'try-it' functionality for making test API calls.

Four51 Client Information

1) Machine-to-machine client

client_id(s):

- Staging - Four51-M2M-CONFIDENTIAL.hr6dncmb44f4
- Production - Four51-M2M-CONFIDENTIAL.wt896vzfe2rc

client_secret(s): Will be sent in a separate communication

- SEB recommends securely storing this secret value in some form of Key management system. Azure Keyvault would be a good option.
- This secret will be valid for up to one year. When nearing the expiration date, SEB will be in touch to provide a new secret.

Grant Types Allowed

- client_credentials
  - This should be used to perform the batch data syncs between the Four51 API and your system. This *should not* be used for the SSO/interactive use case

Scopes Allowed (brand is required. Consult the api-docs for per-endpoint scope requirements)

- https://identity.sebrands.com/scopes/brand.waxingthecity

- https://identity.sebrands.com/scopes/locations.readonly
- https://identity.sebrands.com/scopes/staff.readonly

Workflow

Four51 will be able to request an access token via client credentials from a token endpoint. The access (bearer) token returned from this request should then be appended to all subsequent requests with a "Authorization: Bearer <token>" header value. Also, a "ClientID: {EnvClientID}" header value is required as well.

We will be asking for Four51 to perform nightly full data syncs of all Location and Staff data as needed to meet their requirements. We currently do not support the ability to filter any data by the updated date, which is what makes the full data sync necessary.

2) Interactive Client

Note: we will require your Redirect URL and CORS Origin information in advance to put into our system in order to allow you to test/use this grant type.

client_id(s):

- Staging - Four51-USER-CONFIDENTIAL.9tyg7t7v8hmc
- Production - Four51-USER-CONFIDENTIAL.y57b49wygnhx

client_secret(s): Will be sent in a separate communication

Grant Types Allowed

- authorization_code
  - PKCE with code_challenge_method of S256

Commented [GU1]: Should probably be PKCE

Commented [GB2R1]: Nice catch Updated.

Scopes Allowed (brand is required. Consult the api-docs for per-endpoint scope requirements. The /staff/{id} endpoint used during the SSO process will require the staff.readonly scope)

- https://identity.sebrands.com/scopes/brand.waxingthecity
- https://identity.sebrands.com/scopes/staff.readonly
- openid (to receive an id token with the user's id in the 'sub' claim)
- profile (no additional claims are returned at this time. Future enhancement)
- offline_access (to receive a refresh token)

Workflow

This will be the OIDC flow that will allow Four51 to authorize a user into their system, using SEB as the identity provider. The OIDC authorization_code with PCKE standard can be followed to authenticate the client, as well as authorize the user. After the access and identity tokens are retrieved, the "subject" of the identity token will contain the ID of the authorized user. The access (bearer) token should then be appended to all subsequent requests with a "Authorization: Bearer <token>" header value. Also, a "ClientID: {EnvClientID}" header value is required as well.

The access token can then be used to lookup the staff member by the ID returned in the 'sub' claim of the identity token, via the /api/v1/staff/{id} endpoint. Note that authorization rules will prevent the user-specific access token from being used to access data for other staff members. In the future, the fields returned by that endpoint will be available in the id token when requesting the 'profile' scope in order to remove the need for making the /staff/{id} API call.

Token Lifetimes

Access Token Lifetime – 3600 seconds

Identity Token Lifetime – 300 seconds

Authorization Code Lifetime – 300 seconds

Refresh Token Lifetime – 30 days (one-time use tokens)

Special Considerations

SEB will be actively working with Four51 on any potential additional needs and will attempt to accommodate where possible. That said, SEB will also be working on improvements to the Four51 API and may request future changes from Four51.

Question – does Four51 want the user's name to be returned in the ID Token in order to display in the UI immediately upon completing the SSO?