API Interface Guide

IDEA 3.0 incorporates OAuth 2.0 for all API access. The process of issuing access, refresh and idTokens is delegated to AWS Cognito.

For IDEA hosted applications, the OAuth 2.0 flow is simplified using IDEA Cluster Manager, which interacts directly with Cognito User Pool admin APIs and returns the authorization result, without having to go through the OAuth 2.0 authorization code flow.

Cluster Admins can add additional OAuth 2.0 Clients to the Cognito User Pool for external API integrations, which can implement Authorization Code grant or Client Credentials grant.

User Authorization

API Authorization is available in 4 categories:

- **Public** - As long as client has network access to the endpoint.
- **Authenticated User** - The calling user must send a valid JWT token issued by the cluster's Cognito User Pool
- **Manager** - The user must be part of the **managers** Cognito User Group. **(Functionality not exposed yet)**
- **Administrator** - The user must be part of the **administrators** Cognito User Group, in addition to the Sudoers LDAP Group.

JWT Access Token Claims

Authenticated End User

```
{
  "origin_jti": "383f4b23-1e9b-48d0-98d0-5a4c3a5e4ff9",
  "sub": "cc5782b1-06aa-48ba-9e92-12725dd3def3",
  "event_id": "44934cfe-ee89-4c71-a718-32a9b3cec7c9",
  "token_use": "access",
  "scope": "aws.cognito.signin.user.admin",
  "auth_time": 1645637942,
  "iss": "https://cognito-idp.us-west-2.amazonaws.com/us-west-2_K9GpSFhXa",
  "exp": 1645641542,
  "iat": 1645637942,
  "jti": "583d2a71-f651-41cf-b3ec-75f35c09b66b",
  "client_id": "dqsbnuebm3an8toaghc96sos9",
  "username": "kulkary"
}
```

Authenticated Admin User

```
{
  "sub": "29d071f7-e632-42e6-a0e3-61d1b9392efa",
  "cognito:groups": [
    "administrators"
  ],
  "iss": "https://cognito-idp.us-west-2.amazonaws.com/us-west-2_K9GpSFhXa",
  "client_id": "dqsbnuebm3an8toaghc96sos9",
  "origin_jti": "1f5d7e2b-fee4-4224-89ff-83b3e868d87c",
  "event_id": "f6e67d7e-cdb4-49d3-834b-c441e311fd68",
  "token_use": "access",
  "scope": "aws.cognito.signin.user.admin",
  "auth_time": 1645636855,
  "exp": 1645640675,
  "iat": 1645637075,
  "jti": "3156ff84-68af-49b8-ab50-13a097744776",
  "username": "socaadmin"
}
```

API Samples

Auth.InitiateAuth (Using Username/Password)

InitiateAuth is a public API, that is used to authenticate the cluster user. The API may return the authentication result or challenges such as FORCE_RESET_PASSWORD, MFA challenge based configuration.

```
POST <CLUSTER_ALB_ENDPOINT>/cluster-manager/api/v1 HTTP/1.1
Content-Type: application/json
```

Username/Password Auth: Request Payload

```
{
    "header": {
        "namespace": "Auth.InitiateAuth",
        "request_id": "defc4408-922a-401c-a004-6be6f00718ee"
    },
    "payload": {
        "auth_flow": "USER_PASSWORD_AUTH",
        "username": "<username>",
        "password": "<password>"
    }
}
```

Username/Password Auth: Response Payload

```
{
    "header": {
        "namespace": "Auth.InitiateAuth",
        "request_id": "defc4408-922a-401c-a004-6be6f00718ee"
    },
    "success": true,
    "payload": {
        "auth": {
            "access_token": "eyJra.eyJzd...",
            "id_token": "eyJraWQiOi....",
            "refresh_token": "eyJ...",
            "expires_in": 3600,
            "token_type": "Bearer"
        }
    }
}
```

RefreshToken Auth: Request Payload

```
{
    "header": {
        "namespace": "Auth.InitiateAuth",
        "request_id": "defc4408-922a-401c-a004-6be6f00718ee"
    },
    "payload": {
        "auth_flow": "REFRESH_TOKEN_AUTH",
        "username": "<username>",
        "refresh_token": "<refresh_token>"
    }
}
```

Username/Password Auth: Response Payload

```
{
    "header": {
        "namespace": "Auth.InitiateAuth",
        "request_id": "defc4408-922a-401c-a004-6be6f00718ee"
    },
    "success": true,
    "payload": {
        "auth": {
            "access_token": "eyJra.eyJzd...",
            "id_token": "eyJraWQiOi....",
            "expires_in": 3600,
            "token_type": "Bearer"
        }
    }
}
```


Authenticated API Invocations

To invoke authenticated APIs, set the Authorization HTTP Header with: Bearer <access_token> and invoke applicable APIs.