JumpCloud SAML

1. Login to the Admin portal
2. Left-side menu under **User AUTHENTICATION** access **SSO Applications**
3. Within SSO Applications click on Add New Application
    a. Search for GitHub Enterprise Cloud and select the GitHub Enterprise Cloud Enterprise Account app.
    b. One done click Next at the bottom right corner.
    c. In the next panel click on advanced settings and add your Enterprise Managed User's enterprise name
    d. Click on Save Application.
    e. Finally proceed on clicking Configure Application.
4. Within the GitHub Enterprise Cloud Enterprise Account application within the SSO tab you will need to complete the following:
    a. **IDP Entity ID:** {This can be left with the default value or you can change it}
    b. **SP Entity ID**: https://github.com/enterprises/{EMU_SLUG}
    c. **ACS URLs**> Default ULR: https://github.com/enterprises/{EMU_SLUG}/saml/consume
    d. **Login URL**: https://github.com/enterprises/{EMU_SLUG}/sso
5. Click on **Save**

JumpCloud Granting Users Access

1. Access the left-side menu and under User Management access User Groups.
2. Access the group you want to grant access to the GitHub Enterprise Cloud Enterprise Account app.
3. Within the group settings access the Applications tab.
4. Select the GitHub Enterprise Cloud Enterprise Account app and click save group. Now if you access the Application, you should be able to see your group under User Groups.

GitHub SAML & Open SCIM Configuration

1. Login with you setup admin user.
2. With the admin user proceed on generating a personal access token GitHub Documentation – Creating SCIM scoped Token
3. Once done access the Identity Provider tab/section within you Enterprise settings
4. From the options Select SAML
5. Within SAML you will need to fill out the following values:
    a. Sign On URL = JumpCloud IDP URL
    b. **Issuer = JumpCloud IDP Entity ID** (this may or may not be a URL could be just the name you set)
    c. **Public Certificate: JumpCloud IDP Certificate Valid** (You will need to download the certificate)
6. Once you fill out the needed values proceed to Test SAML Configuration. You will be requested to authenticate against JumpCloud. Once succeeded you will see a message stating "Your SAML provider settings have been validated. Remember to save your changes."
7. Click on Save SAML Settings, you will be redirected to download/copy/print your recovery codes. Once you select the option of your choice, Procced on Enabling SAML.
8. Once done you will be redirected to the Single Sign-on configuration panel.
9. From the configuration panel Enable Open SCIM Configuration.

JumpCloud SCIM

1. Within the GitHub Enterprise Cloud Enterprise Account application within the Identity Management tab, within Configuration Settings you will need to complete the following:
    a. Select SCIM API
    b. SCIM Version: SCIM 2.0
    c. Base URL: https://api.github.com/scim/v2/enterprises/{EMU_SLUG}
    d. Token Key: GitHub Documentation – Creating SCIM scoped Token
    e. Test User Email: This can be left blank.
2. Group Management: ON
3. Within the Attribute Mapping section, you will need to map the following attributes:
    a. Password < > Password
    b. UserName < > Company Email
4. Click on Test Connection! If succeeded, Click on Activate
5. Save

IMPORTANT

- JumpCloud does not support provisioning individual users, hence all provisioning is done via Group provisioning.
- JumpCloud does not support creating custom attributes for identity management. Even if a custom attribute is created for a group this will not be passed on to the user upon provisioning when provisioning to GitHub Enterprise Cloud Enterprise Managed Users.

Note: Based on the above limitations from JumpCloud to complete your setup you will need to update the role of at least one of your users to Enterprise Owner, since the “Roles” attribute is not supported by JumpCloud nor can it be set in JumpCloud you will need to update the role for your user via our API. This is only needed for the Enterprise Owner, All other users are provisioned as Enterprise Members. For more details on the Roles for Enterprise Managed Users feel free to review our documentation:

- Roles in an enterprise - GitHub Enterprise Cloud Docs
- REST API endpoints for SCIM - GitHub Enterprise Cloud Docs

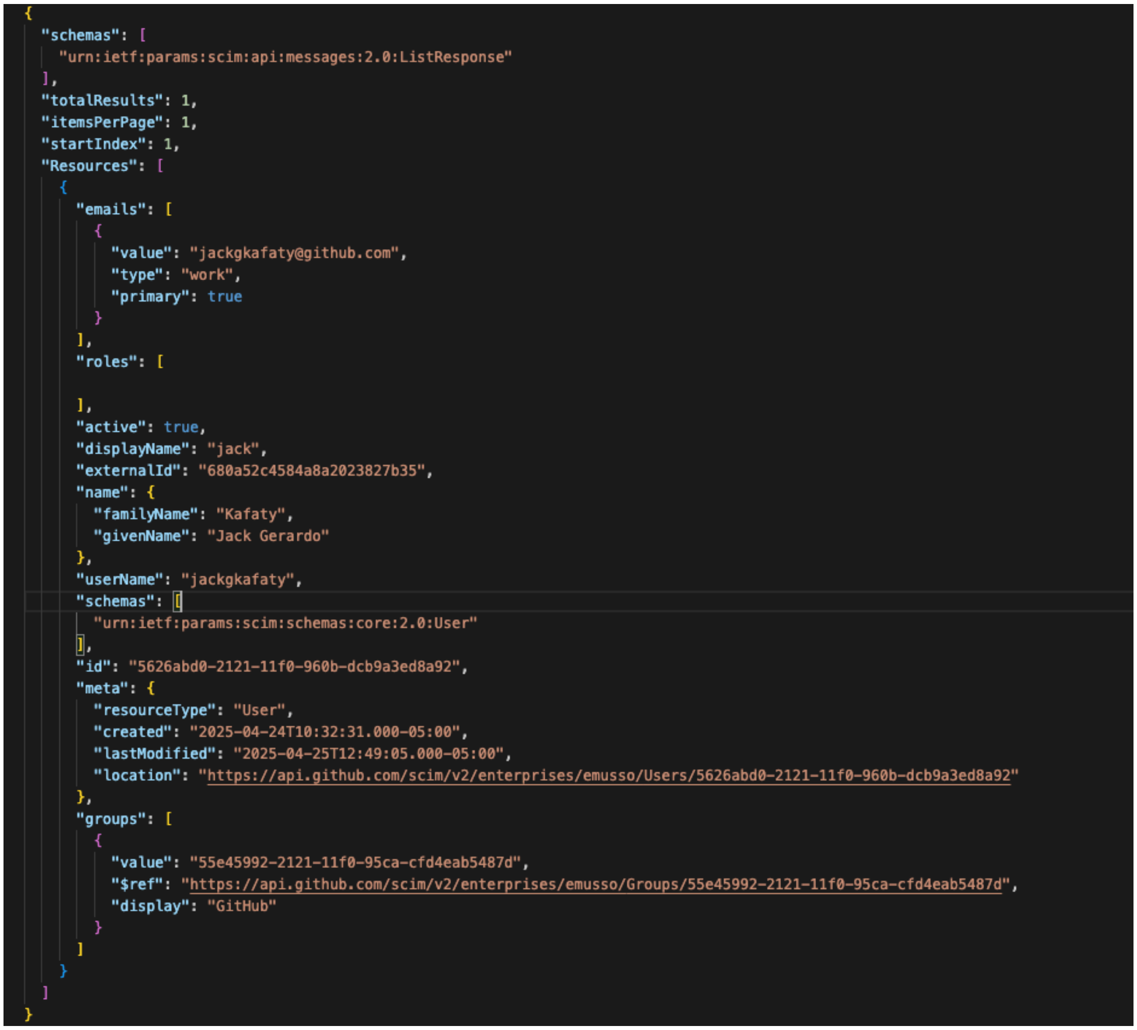
Assigning the Enterprise Owner Role

Before proceeding it's important that you complete all the steps mentioned above and can confirm that your users have been provisioned within your GitHub Enterprise tenant.

1. We need to obtain the **externalID** and the **ID** from of the user we will be elevating their role from the default Enterprise Member to Enterprise Owner. You can accomplish this by modifying and executing the following call:

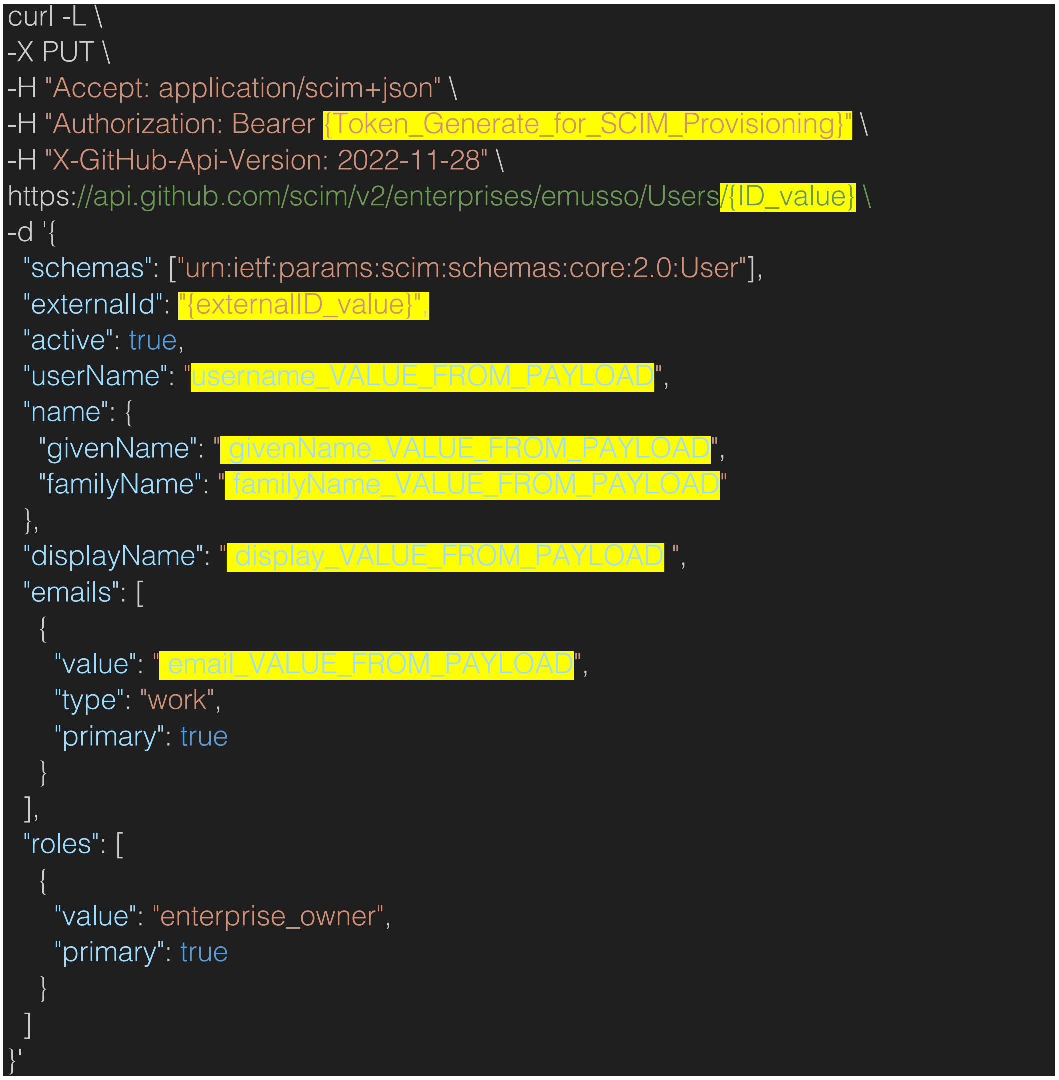
```
curl -L \
-H "Accept: application/scim+json" \
-H "Authorization: Bearer {Token_Generate_for_SCIM_Provisioning}" \
-H "X-GitHub-Api-Version: 2022-11-28" \
https://api.github.com/scim/v2/enterprises/{Your_Enterprise_Name}/Users
```

Your output should look like the following payload. From the payload you identify the user you would like to make an Enterprise Owner. From the payload for that user you will need the values for the **externalID** and the **ID.**



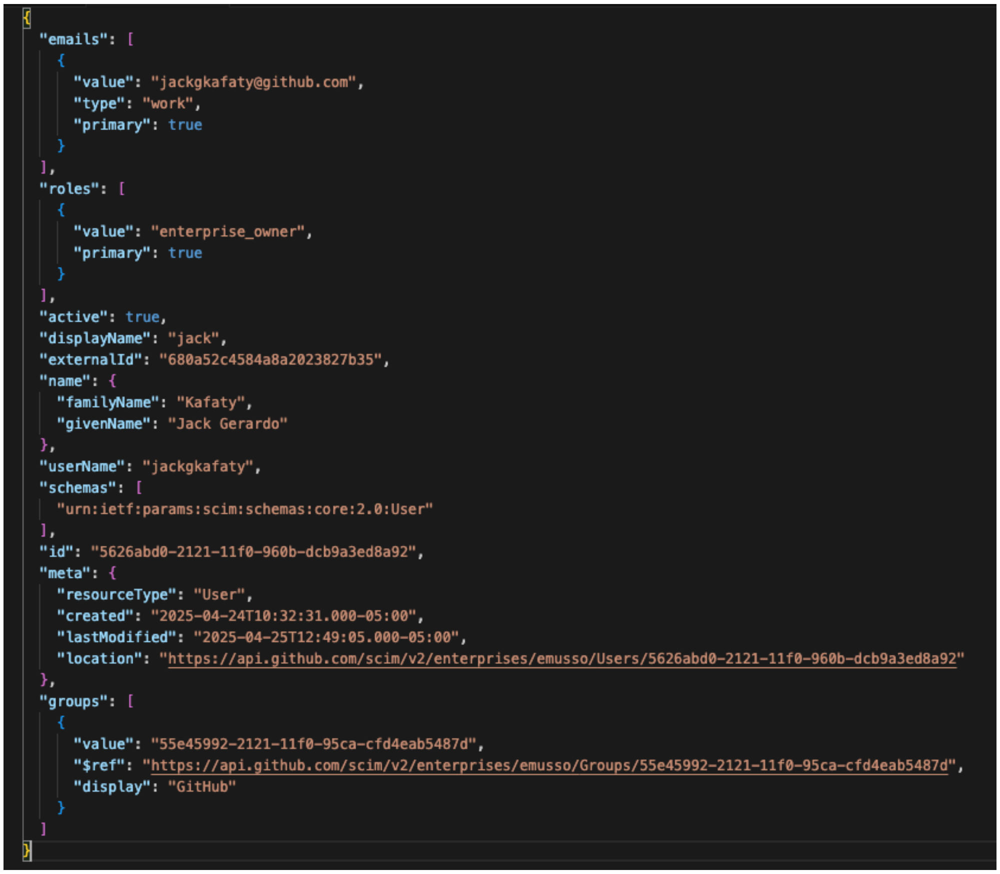
```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"
  ],
  "totalResults": 1,
  "itemsPerPage": 1,
  "startIndex": 1,
  "Resources": [
    {
      "emails": [
        {
          "value": "jackgkafaty@github.com",
          "type": "work",
          "primary": true
        }
      ],
      "roles": [

      ],
      "active": true,
      "displayName": "jack",
      "externalId": "680a52c4584a8a2023827b35",
      "name": {
        "familyName": "Kafaty",
        "givenName": "Jack Gerardo"
      },
      "userName": "jackgkafaty",
      "schemas": [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "id": "5626abd0-2121-11f0-960b-dcb9a3ed8a92",
      "meta": {
        "resourceType": "User",
        "created": "2025-04-24T10:32:31.000-05:00",
        "lastModified": "2025-04-25T12:49:05.000-05:00",
        "location": "https://api.github.com/scim/v2/enterprises/emusso/Users/5626abd0-2121-11f0-960b-dcb9a3ed8a92"
      },
      "groups": [
        {
          "value": "55e45992-2121-11f0-95ca-cfd4eab5487d",
          "$ref": "https://api.github.com/scim/v2/enterprises/emusso/Groups/55e45992-2121-11f0-95ca-cfd4eab5487d",
          "display": "GitHub"
        }
      ]
    }
  ]
}
```

2. Now that you have the needed values you can proceed on setting the role for the user executing the following call after you update the values:



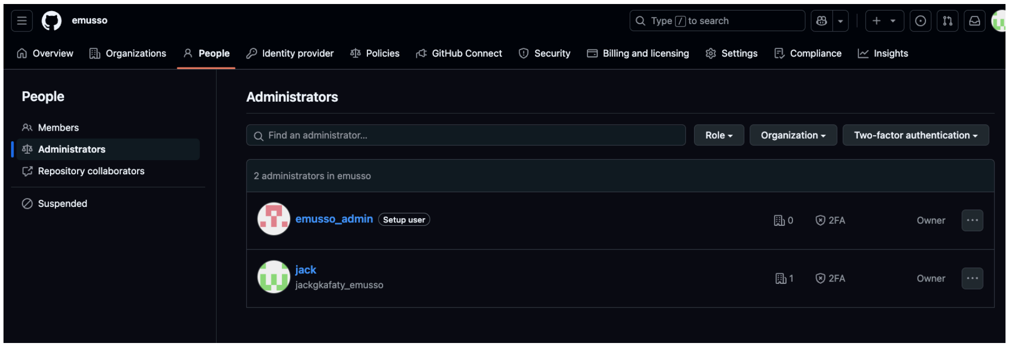
```
curl -L \
-X PUT \
-H "Accept: application/scim+json" \
-H "Authorization: Bearer {Token_Generate_for_SCIM_Provisioning}" \
-H "X-GitHub-Api-Version: 2022-11-28" \
https://api.github.com/scim/v2/enterprises/emusso/Users/{ID_value} \
-d '{
  "schemas": ["urn:ietf:params:scim:schemas:core:2.0:User"],
  "externalId": "{externalID_value}",
  "active": true,
  "userName": "username_VALUE_FROM_PAYLOAD",
  "name": {
    "givenName": " givenName_VALUE_FROM_PAYLOAD",
    "familyName": " familyName_VALUE_FROM_PAYLOAD"
  },
  "displayName": " display_VALUE_FROM_PAYLOAD ",
  "emails": [
    {
      "value": " email_VALUE_FROM_PAYLOAD",
      "type": "work",
      "primary": true
    }
  ],
  "roles": [
    {
      "value": "enterprise_owner",
      "primary": true
    }
  ]
}'
```

Once executed you should see the output and confirm the user role has been added.



```
{
  "emails": [
    {
      "value": "jackgkafaty@github.com",
      "type": "work",
      "primary": true
    }
  ],
  "roles": [
    {
      "value": "enterprise_owner",
      "primary": true
    }
  ],
  "active": true,
  "displayName": "jack",
  "externalId": "680a52c4584a8a2023827b35",
  "name": {
    "familyName": "Kafaty",
    "givenName": "Jack Gerardo"
  },
  "userName": "jackgkafaty",
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "id": "5626abd0-2121-11f0-960b-dcb9a3ed8a92",
  "meta": {
    "resourceType": "User",
    "created": "2025-04-24T10:32:31.000-05:00",
    "lastModified": "2025-04-25T12:49:05.000-05:00",
    "location": "https://api.github.com/scim/v2/enterprises/emusso/Users/5626abd0-2121-11f0-960b-dcb9a3ed8a92"
  },
  "groups": [
    {
      "value": "55e45992-2121-11f0-95ca-cfd4eab5487d",
      "$ref": "https://api.github.com/scim/v2/enterprises/emusso/Groups/55e45992-2121-11f0-95ca-cfd4eab5487d",
      "display": "GitHub"
    }
  ]
}
```

3. Finally, in GitHub, refresh your Enterprise Admin portal and under **People Tab**, **Administrators** you should see your users being displayed there.



Administrators

2 administrators in emusso

emusso_admin Setup user 0 2FA Owner

jack jackgkafaty_emusso 1 2FA Owner

4. Now! Logout from the Setup Admin user and login with your user account. As an enterprise Owner you will be able to create Organizations and complete your setup.