



User Guide

Version 1.1.4

Contents

Copyright Notice	5
Document Revision History	6
Supported Authentication Providers	7
Admin Interface	8
Applications	9
Adapters	10
Add Adapter	11
Google Adapter	13
Microsoft Office Adapter	13
Active Directory Adapter	13
Gigya Adapter	13
Okta Adapter	13
SMS Adapter	13
Password Adapter	13
Remove Adapter	14
Edit Adapter	16
Microsoft Office	17
Preparations	17
Tenant ID	20
Create an Application	21
Permissions	27
Credentials	39
Google G Suite	43
Preparations	43
Create a Project	43
Configure Consent Screen	47
Create Service Account	48
Delegate Permissions	52
Create oAuth Client Account	55
Enable API Services	59
Credentials	67
Active Directory	72
Preparations	72
Configuration	72
LDAP URL	72
BaseDN	72
Credentials	73
Gigya	76

Preparations	77
Setup the site	77
Data Center	77
API Key	77
Setup OpenID Connect	79
Proxy Page URL	79
Issuer	79
Custom Claims	79
Scopes	79
Create Relay Party (RP) Client	81
Client ID	81
Client Secret	81
Description	81
Supported Response Type	81
Subject Identifier Type	81
Access Token Lifetime	81
Redirect URIs	81
Screen Set	84
Permission Groups	85
Application	88
Okta	93
Preparations	94
Configuration	94
Okta URL	94
Read-only Service Account	95
OpenID Connect Application	97
OpenID Connect Application for User Signin (Optional)	104
Assign users to Application	107
Credentials	109
Twilio SMS	113
Preparations	114
Configuration	114
Phone Number	115
Account SID	115
Auth Token	116
Credentials	117
Password	123
Configuration	123
Add Users	127
Reset User Password	131
Remove User	133
Clients	134

Add Client	135
Edit Client	137
Remove Client	139
Administrators	141
Users	143
Add User	143
Remove User	145
Groups	147
Add Group	148
Remove Group	150
Service Accounts	153
Add Service Accounts	153
Remove Service Accounts	157
Kerberos Integration	159
Whitelist Hostname	159
Service Principal Name (SPN)	159
Keytab	159

Copyright Notice

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without express written permission. Under the law, reproducing includes translating into another language or format.

The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g. a book or sound recording).

Document Revision History

April 26, 2018

- Initial release

June 28, 2019

- Additional adapters (Okta, Password, Username, Gigya)

November 7, 2019

- Kerberos Integration

Supported Authentication Providers

- Microsoft Office (Office 365)
- Google G Suite
- Active Directory (LDAP) (Azure Cloud / On-Premise)
- Gigya (OpenID Connect)
- Okta (OpenID Connect)
- Twilio SMS
- Password

Admin Interface

Applications are used by other services to integrate Bridge into themselves. Each application is unique within Bridge and includes Adapters, Clients, Service Accounts and Administrators.

Adapters are mechanism by which Bridge utilizes third-party services such as Microsoft Office, Google to authenticate users.

Clients are similar to OAuth Client that a third-party application uses to authenticate and communicate with Bridge.

Service Accounts are non-interactive credentials similar to User login without credentials. They are mostly used along with Clients by third-party applications to authenticate with Bridge.

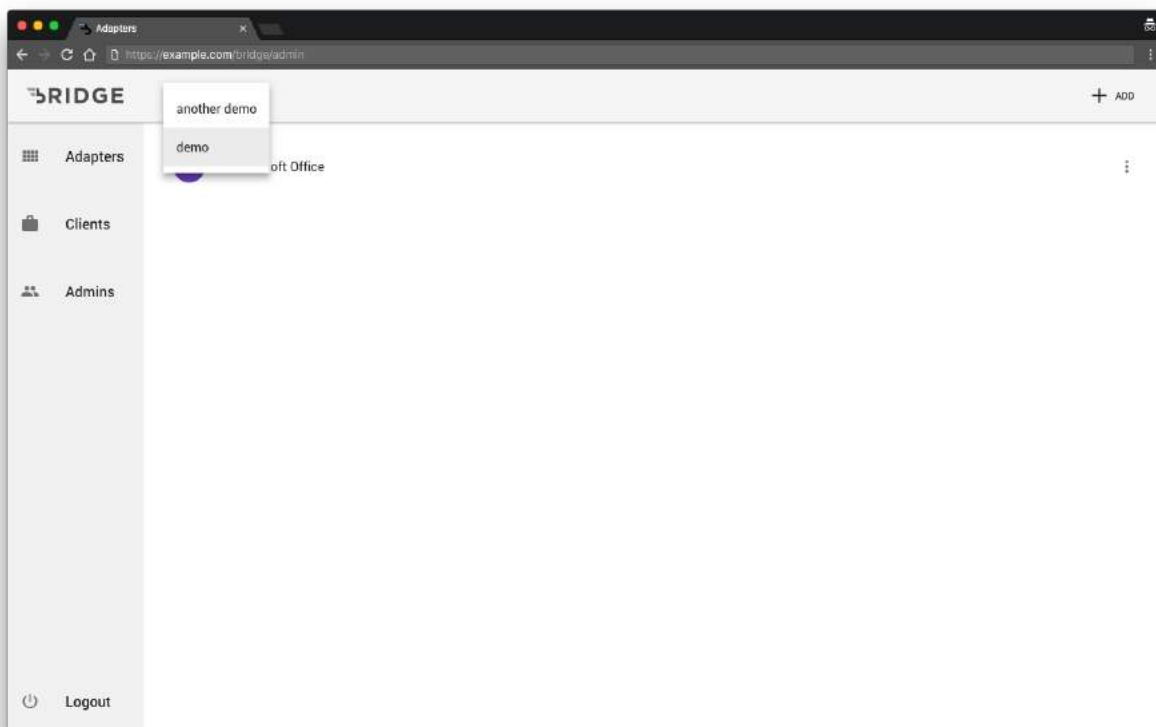
Administrators are list of users and groups with administrative access to Bridge. They can perform actions such as adding or removing users, groups, service accounts, clients and adapters.

Applications

Application is similar to an outer wrapper around a group of adapters. Bridge isolates these applications due to access control reasons.

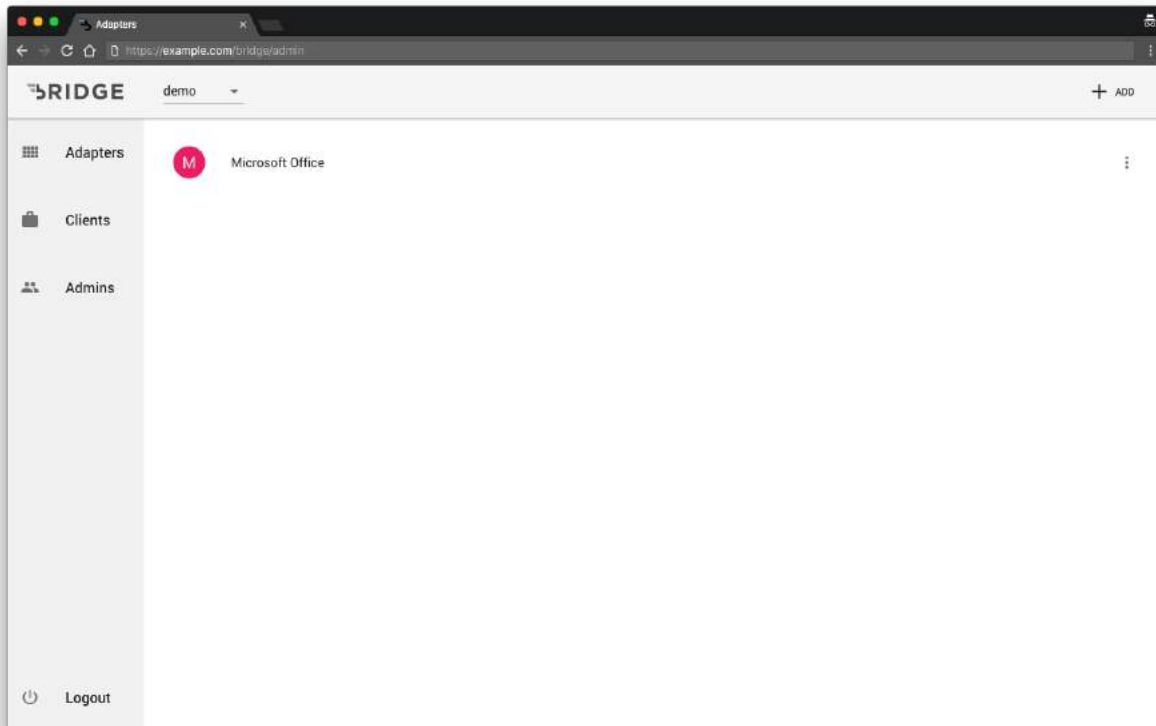
User can switch between the applications using the Application Switcher right next to the Bridge logo in the top left corner of the screen. In order to switch to a different application, click on the **Application Switcher** dropdown and select the application.

In this example below, the **demo** application is selected.



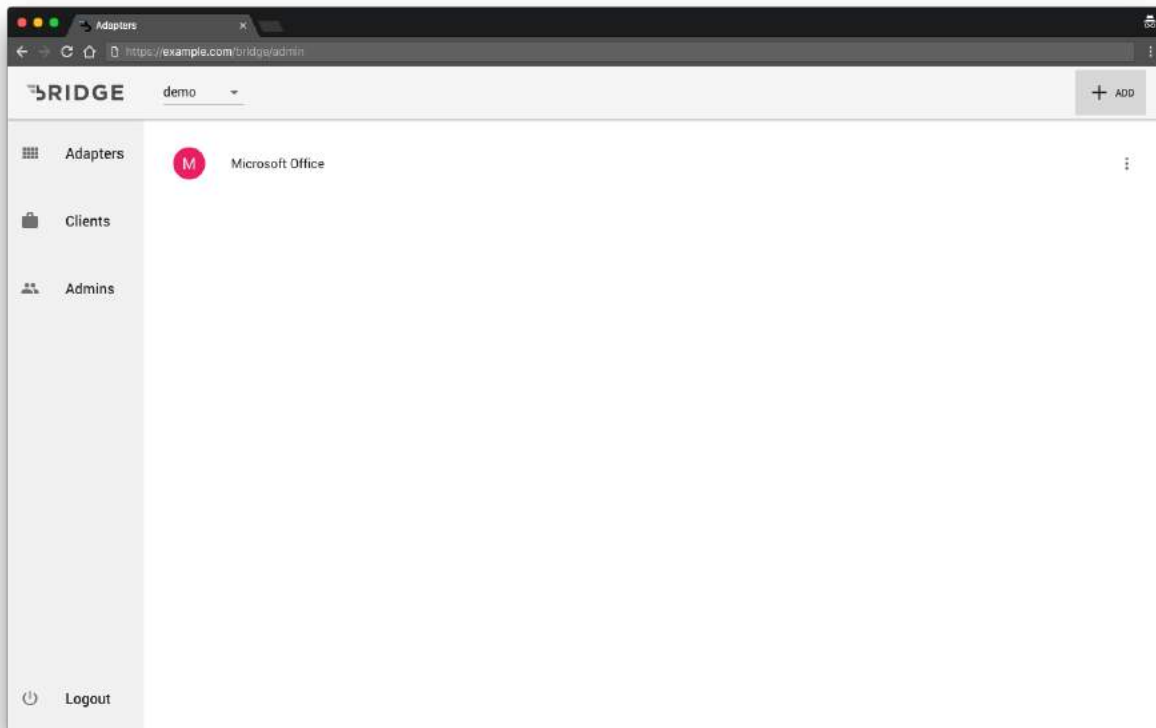
Adapters

The adapters page shows a list of adapters that are linked to the application.

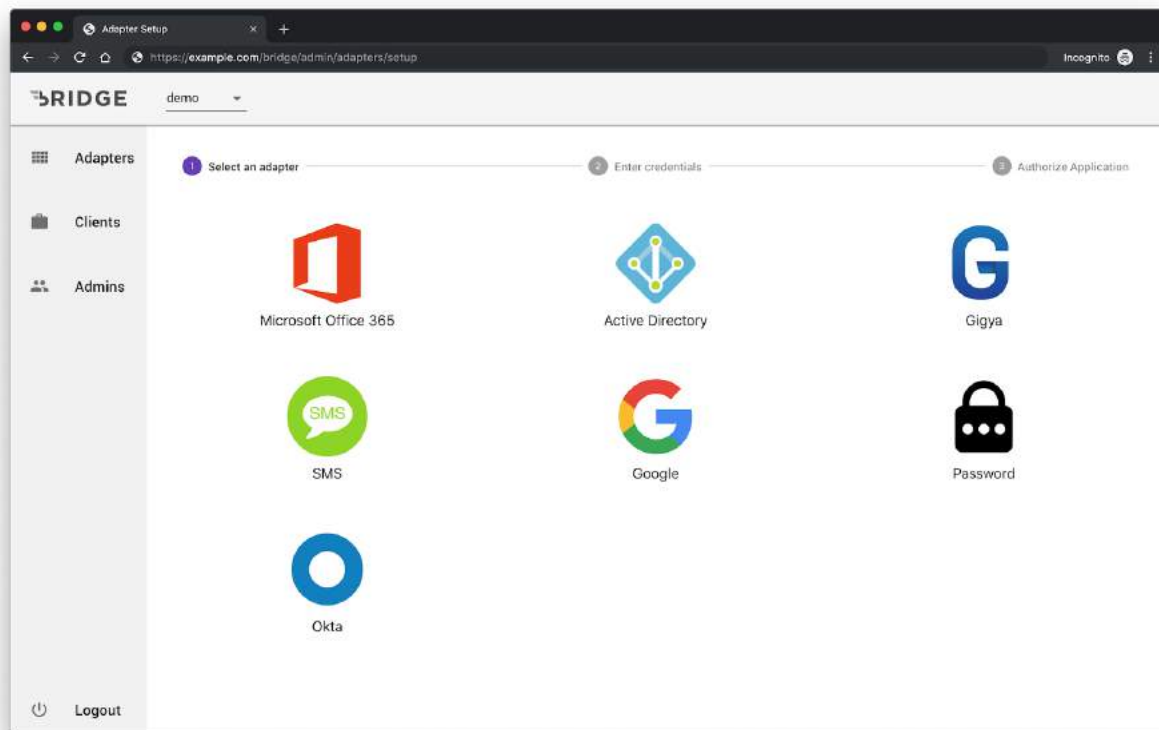


Add Adapter

Click on the + **ADD** button located at the top right corner of the header to add a new adapter.



Click on the relevant icon from the list of supported adapters.



Google Adapter

Instructions on setting up Google adapter are discussed under **Google G Suite** section.

Microsoft Office Adapter

Instructions on setting up Microsoft Office 365 adapter are discussed under **Microsoft Office** section.

Active Directory Adapter

Instructions on setting up Microsoft Office 365 adapter are discussed under **Active Directory** section.

Gigya Adapter

Instructions on setting up Gigya adapter are discussed under **Gigya** section.

Okta Adapter

Instructions on setting up Okta adapter are discussed under **Okta** section.

SMS Adapter

Instructions on setting up SMS adapter are discussed under **Twilio SMS** section.

Password Adapter

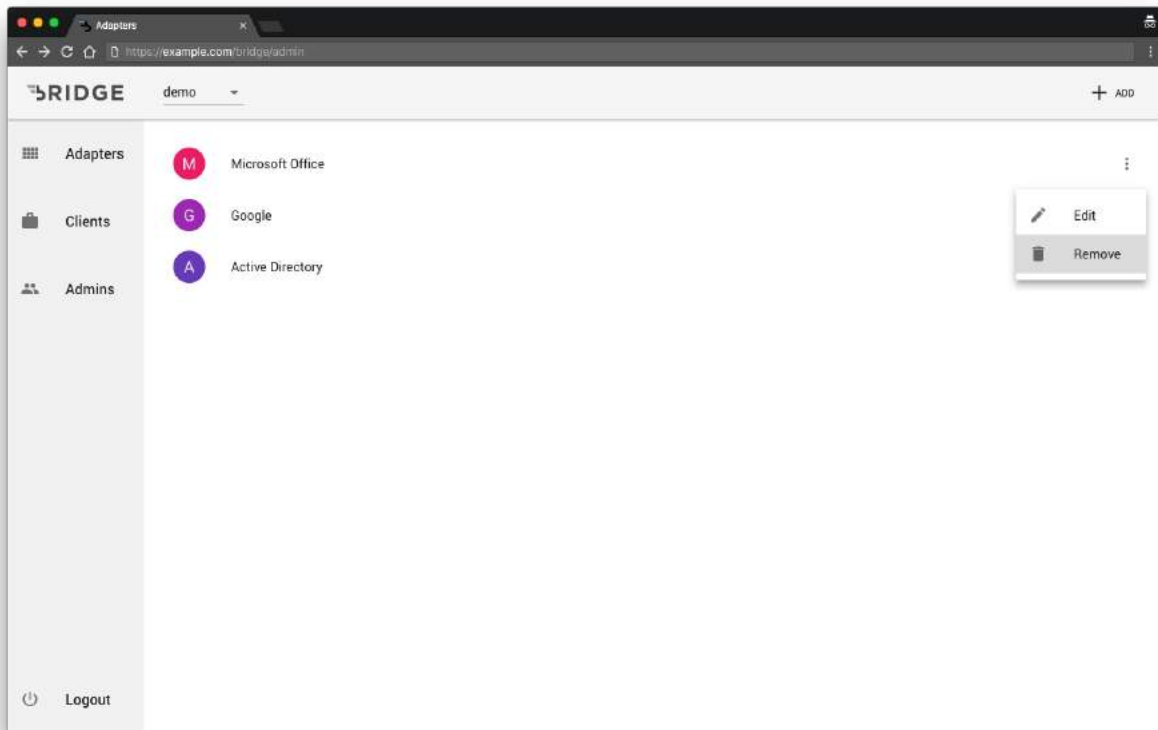
Instructions on setting up Password adapter are discussed under **Password** section.

Remove Adapter

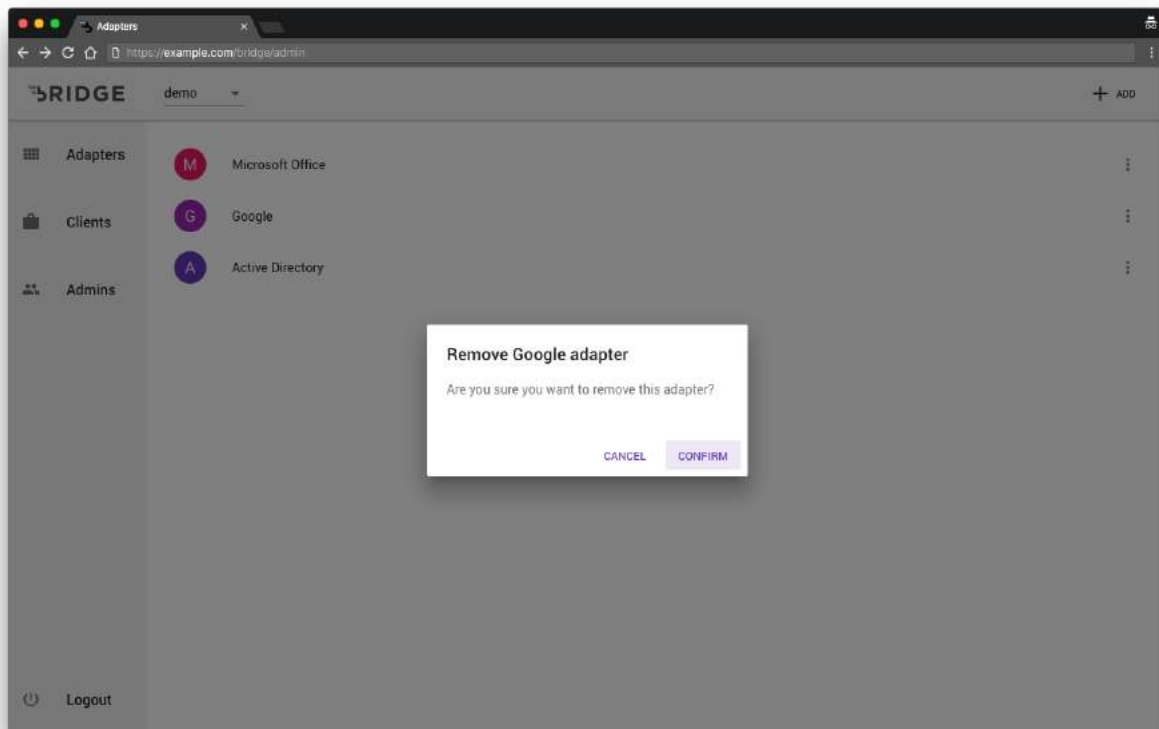
User can delete an Adapter by clicking on the **:** menu icon located towards the right side of the screen and click **Remove** from the popup menu.

WARNING


This action is not reversible.

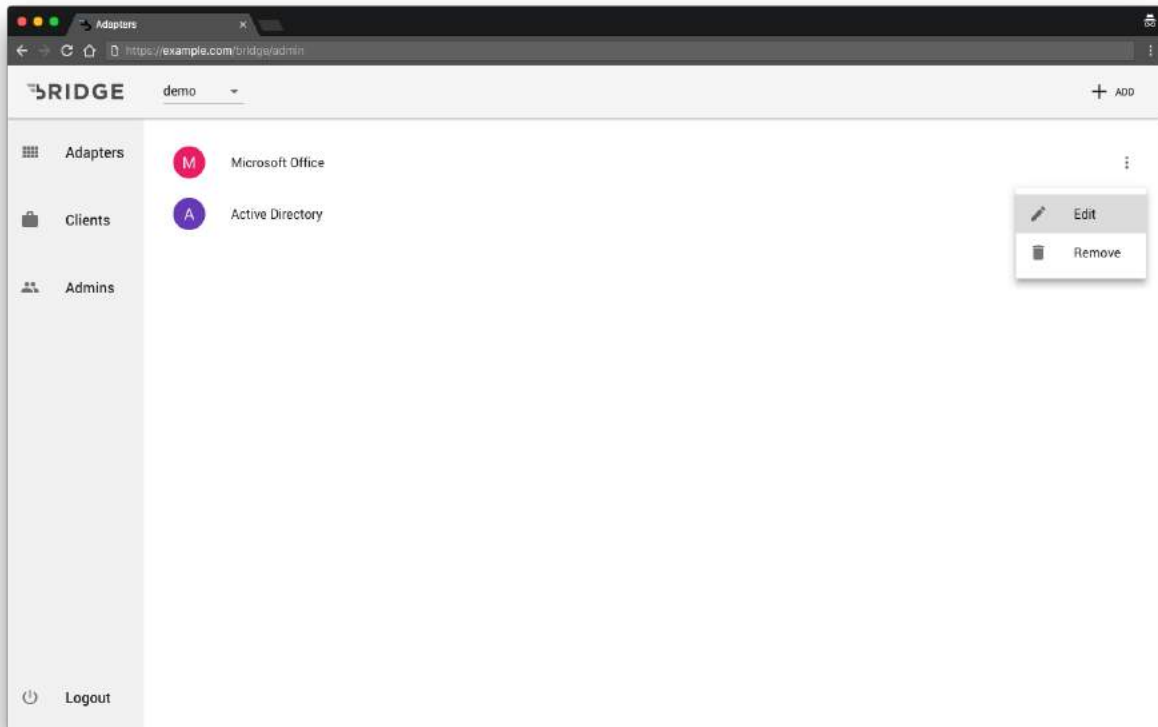


Click **CONFIRM** to remove the adapter permanently.



Edit Adapter

Click on the  menu icon located towards the right side of the screen then the **Edit** button from the popup menu.

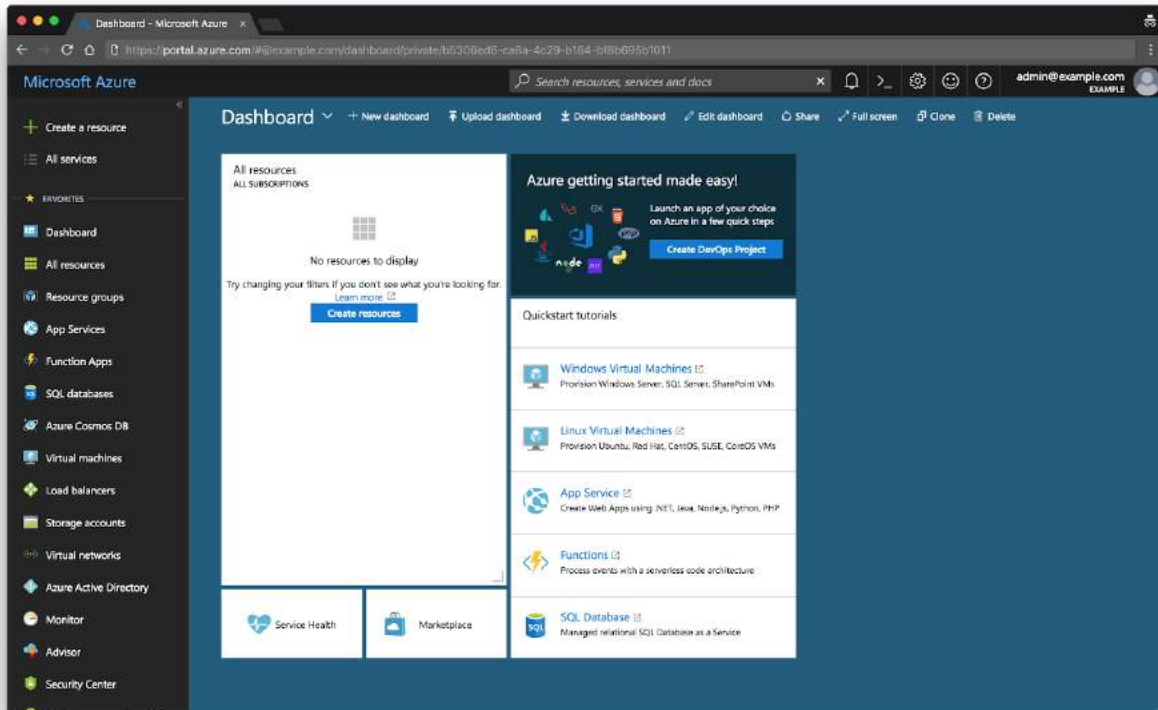


Microsoft Office

Preparations

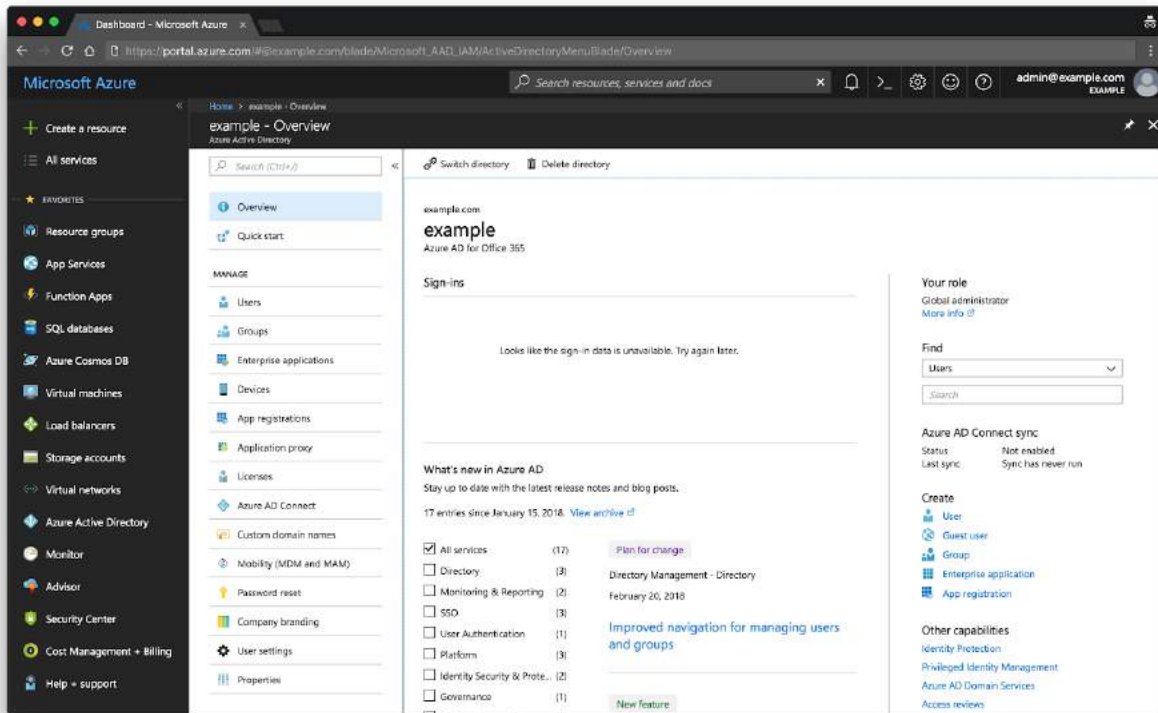
In order to use Microsoft adapter with Bridge, a Microsoft user account with domain administrative access is required.

Open [Azure Portal](https://portal.azure.com)¹ in web browser and login with the administrator account.

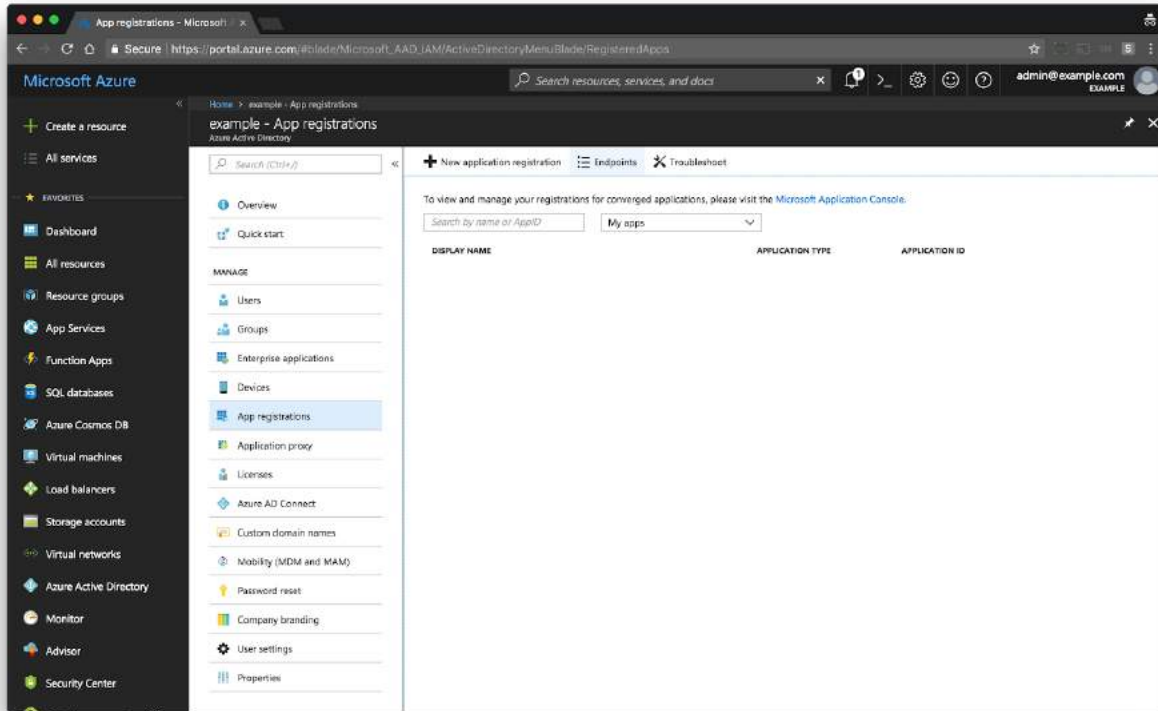


¹ Azure Portal <https://portal.azure.com>

Click on **Azure Active Directory** in the left sidebar to open Azure Active Directory dashboard.



Click on **App Registrations** in the inner left sidebar within the Azure Active Directory page. Click on the **Endpoints** button to access the **Tenant ID**.



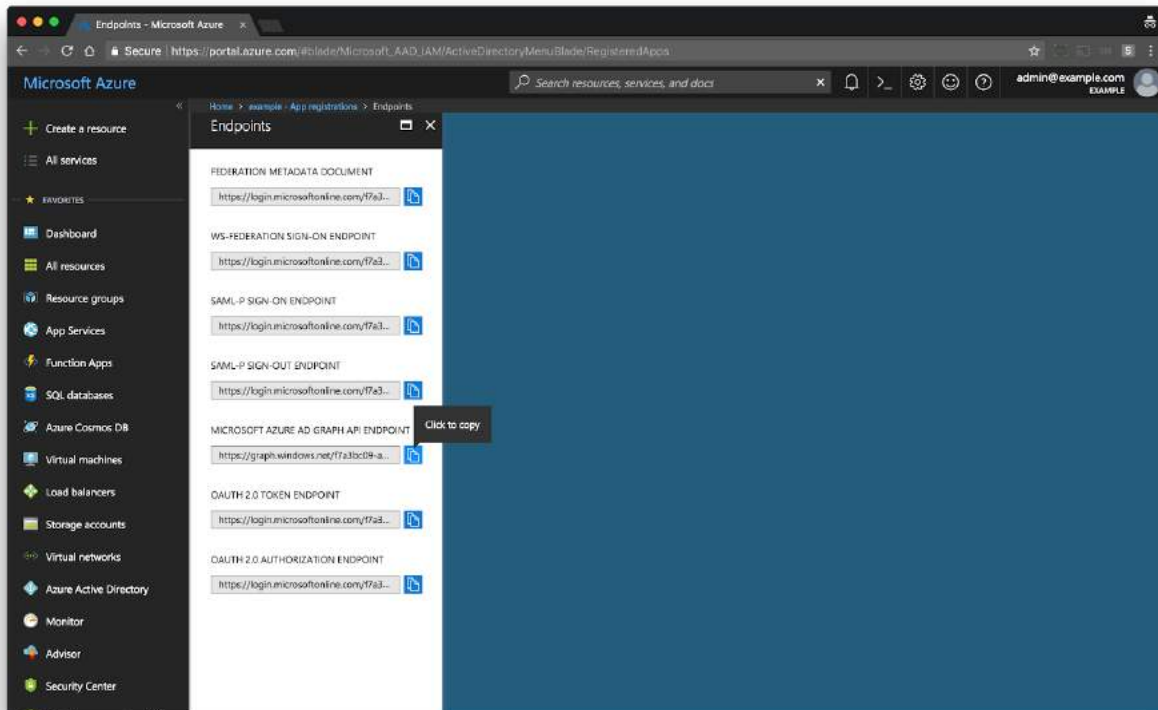
Tenant ID

Under the label **MICROSOFT AZURE AD GRAPH API ENDPOINT**, click the copy button next to the text field to copy the URL. To retrieve the [TENANT ID], paste the URL and pick out the following part:

`https://graph.windows.net/[TENANT ID]`

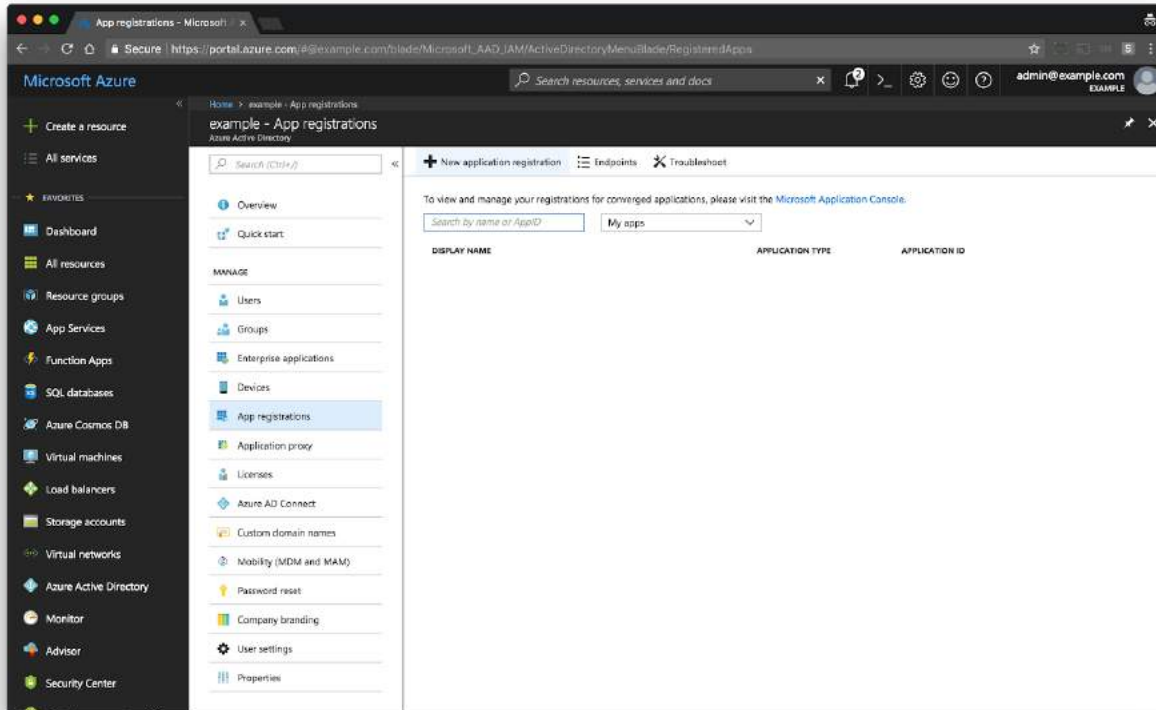
If the URL is `https://graph.windows.net/f7a3bc09-a37d-46de-8df1-a572825b6590`, the Tenant ID would be `f7a3bc09-a37d-46de-8df1-a572825b6590`.

Click on the **X** button to go back to the previous page.



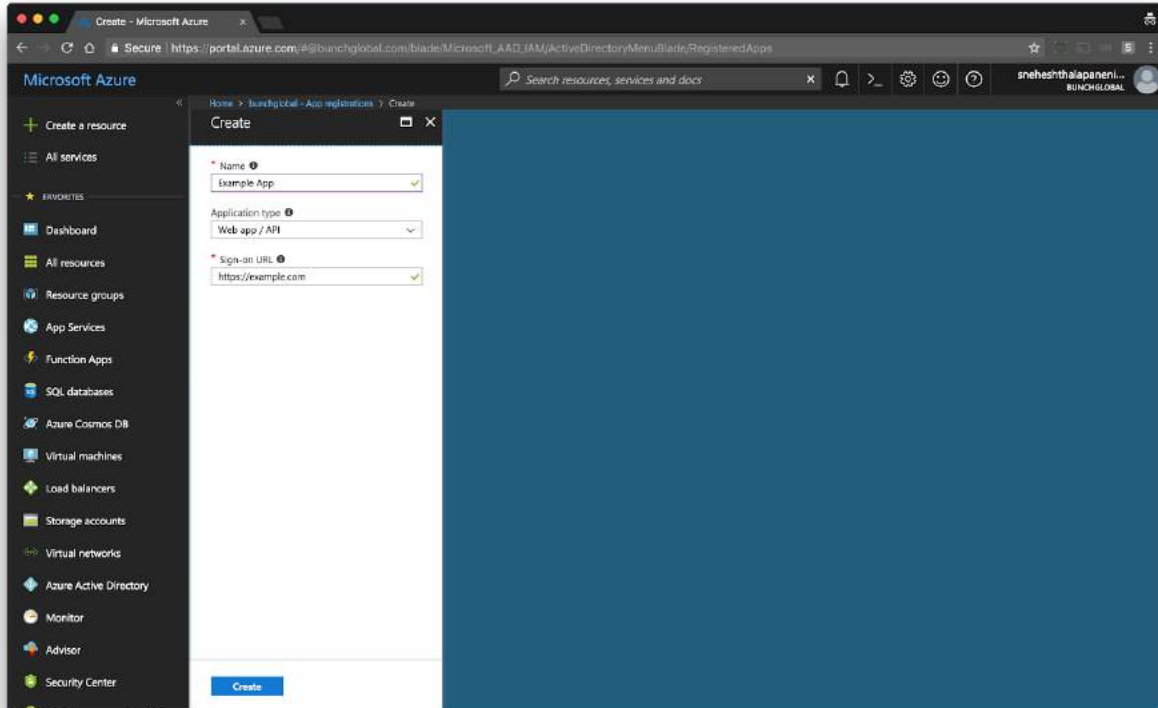
Create an Application

Click the **New application registration** button, highlighted in the image below.



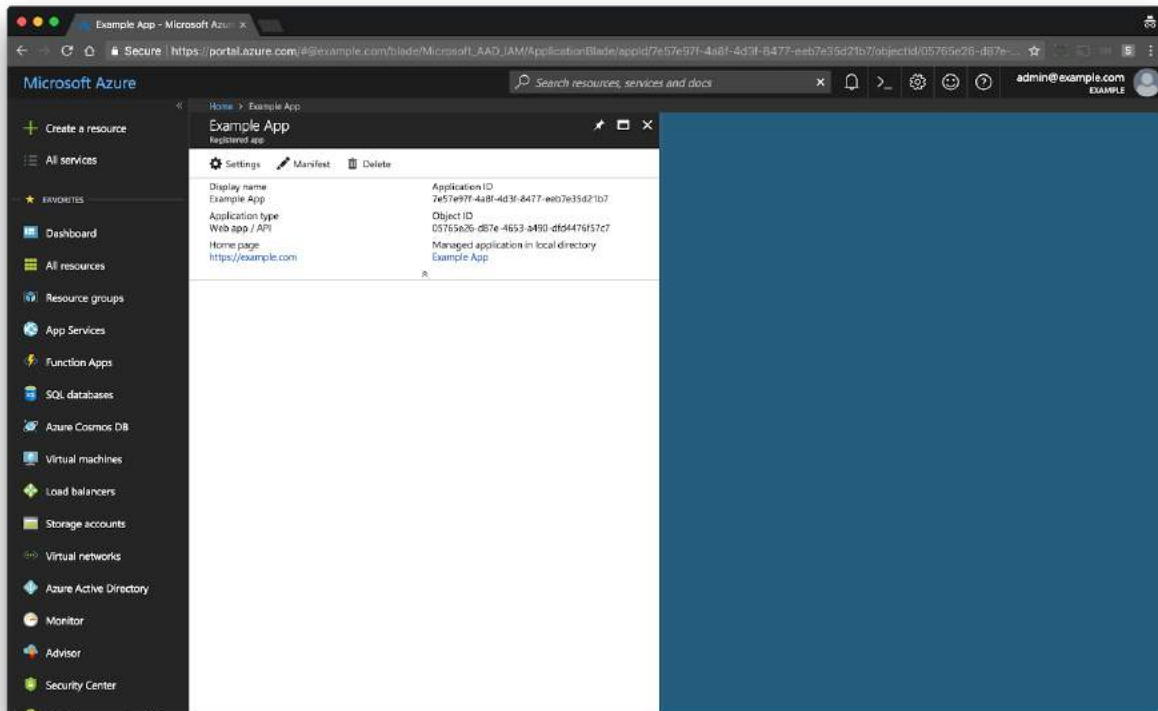
Enter your following details and click **Create**,

- **Name:** The name users will see when they sign in
- **Application type:** Select Web app/API
- **Sign-on URL:** Enter Bridge URL

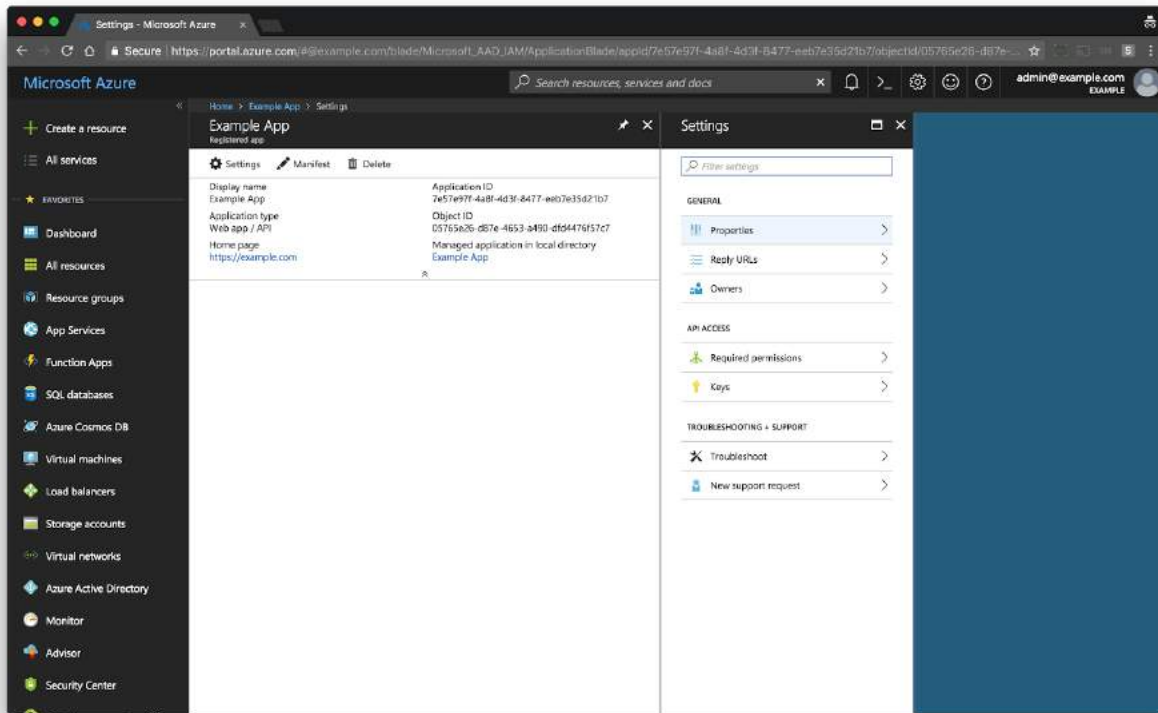


Once the application is created, save the **Application ID** as it will be required later.

The Application ID is unique to the application, In the image below, the **text under Application ID** is 7e57e97f-4a8f-4d3f-8477-eeb7e35d21b7, Hence the Application ID is 7e57e97f-4a8f-4d3f-8477-eeb7e35d21b7.

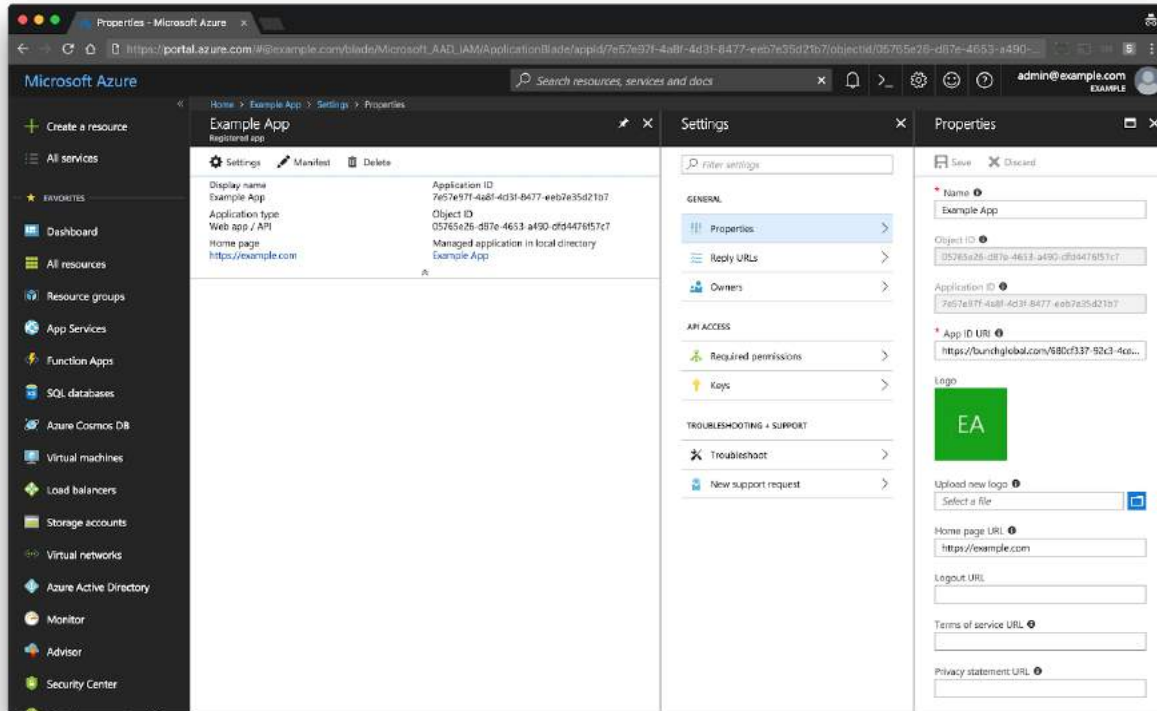


Click on **Settings** button within the application management page, and then click the **Properties** button highlighted in the screenshot below.



On the Properties page you can update the following,

- Application Name (optional)
- Logo (optional)
- Homepage URL (optional)
- Logout URL (optional)
- Terms of Service URL (optional)
- Privacy Statement URL (optional)

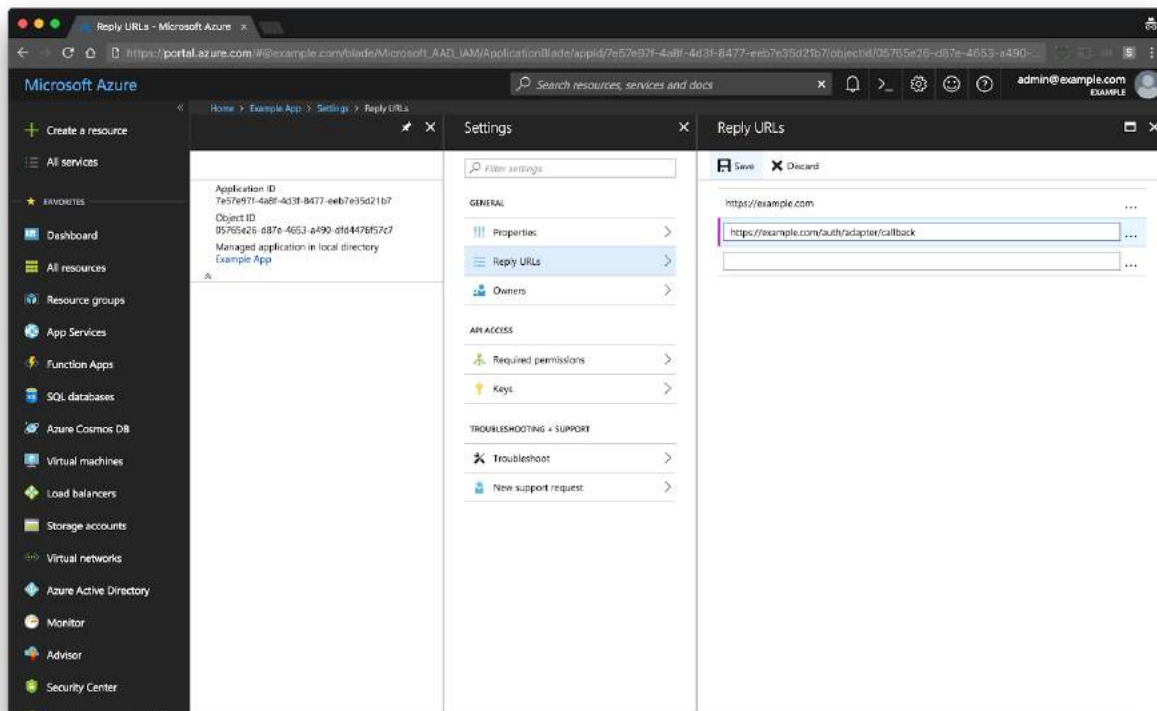


Click on the **Reply URLs** button on the settings page. Add a **Reply URL** and click on the **Save** button above the URL text field.

If the domain is **example.com**, then the reply URLs would be:

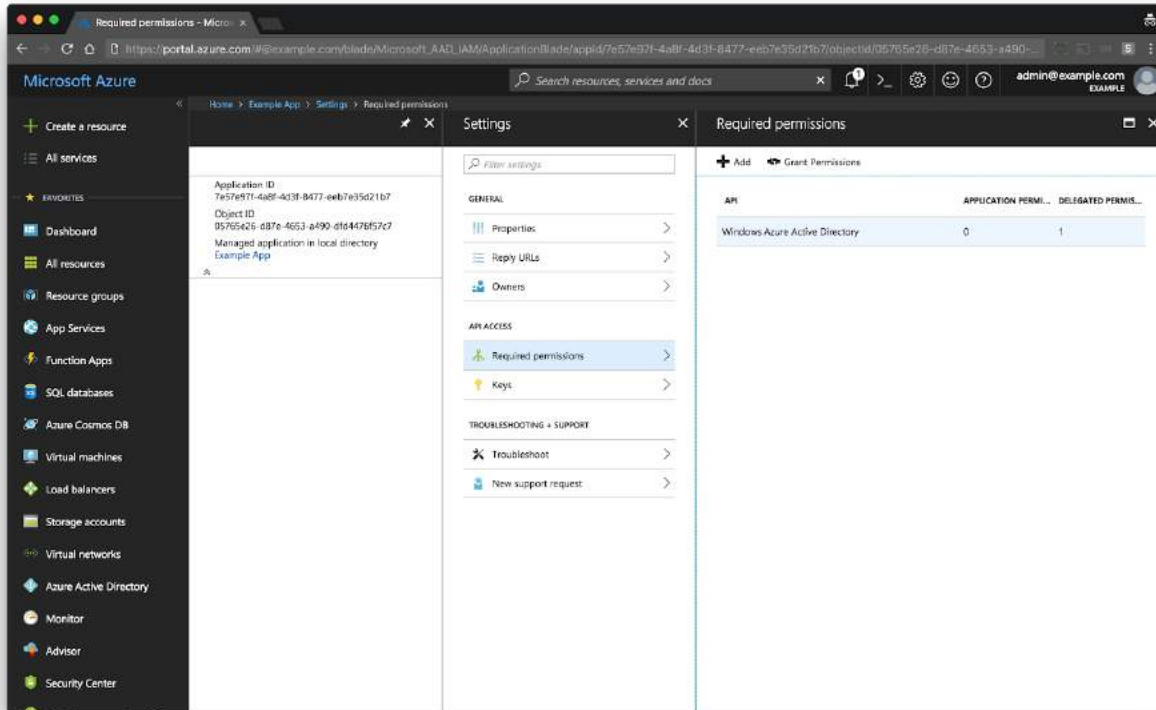
`https://example.com/auth/adapter/callback`

`https://example.com:443/auth/adapter/callback`



Permissions

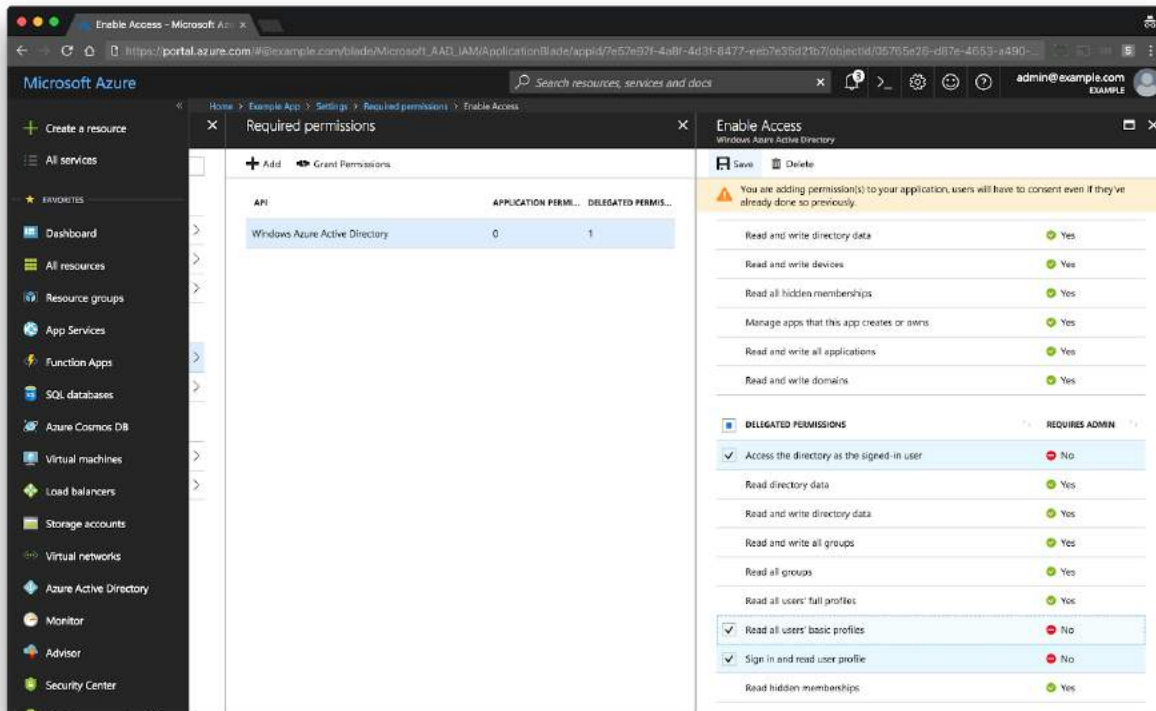
Click on **Required Permissions** on the Settings page under API Access section.



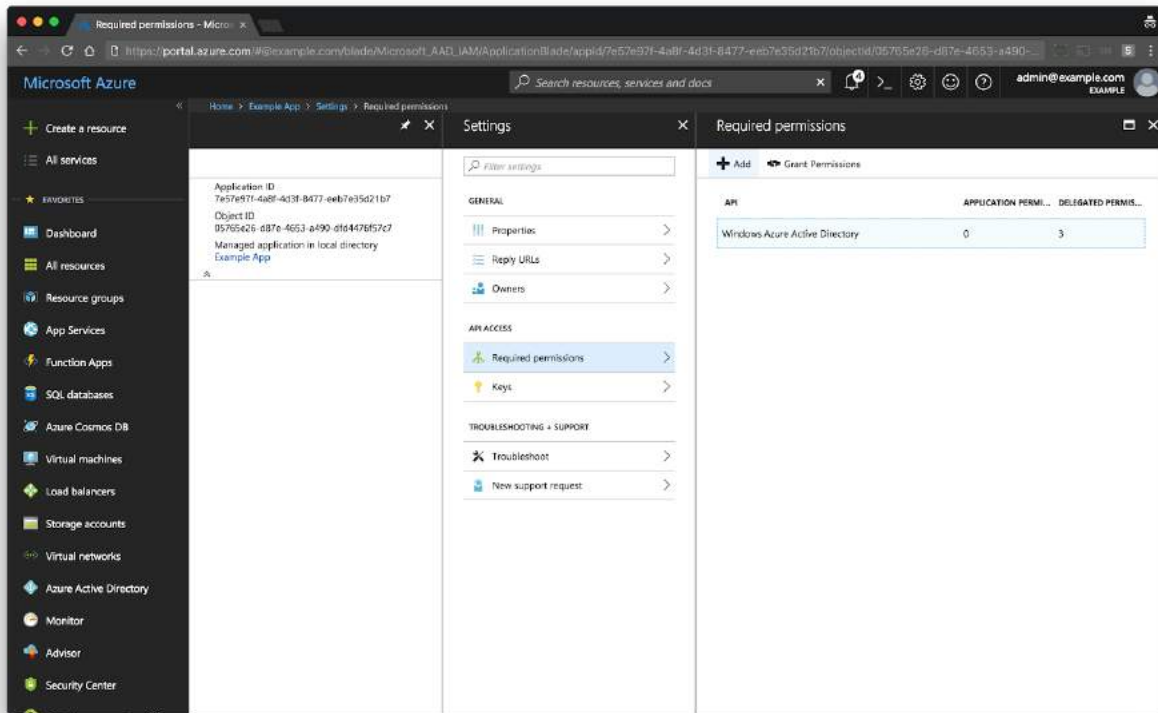
Click on **Windows Azure Active Directory** to open the **Enable Access** page and check the following boxes under **Delegated Permissions**:

- ✓ Access the directory as the signed-in user
- ✓ Read all users' basic profiles
- ✓ Sign in and read user profile

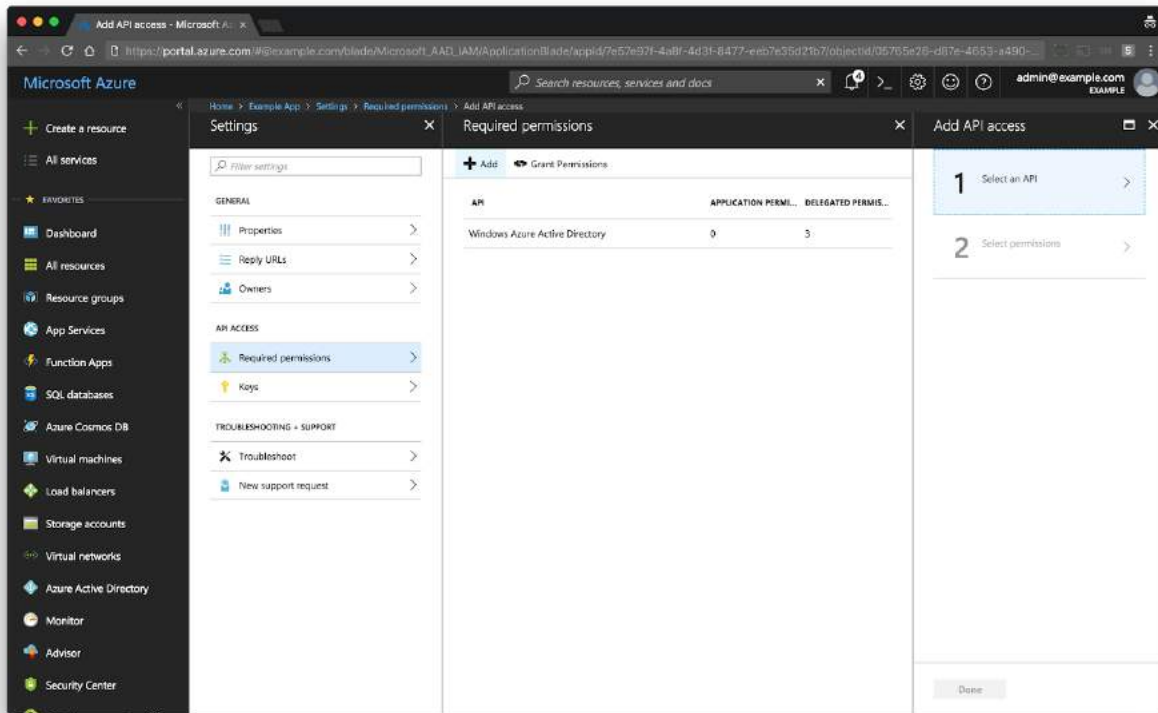
Click the **Save** button on **Enable Access** page.



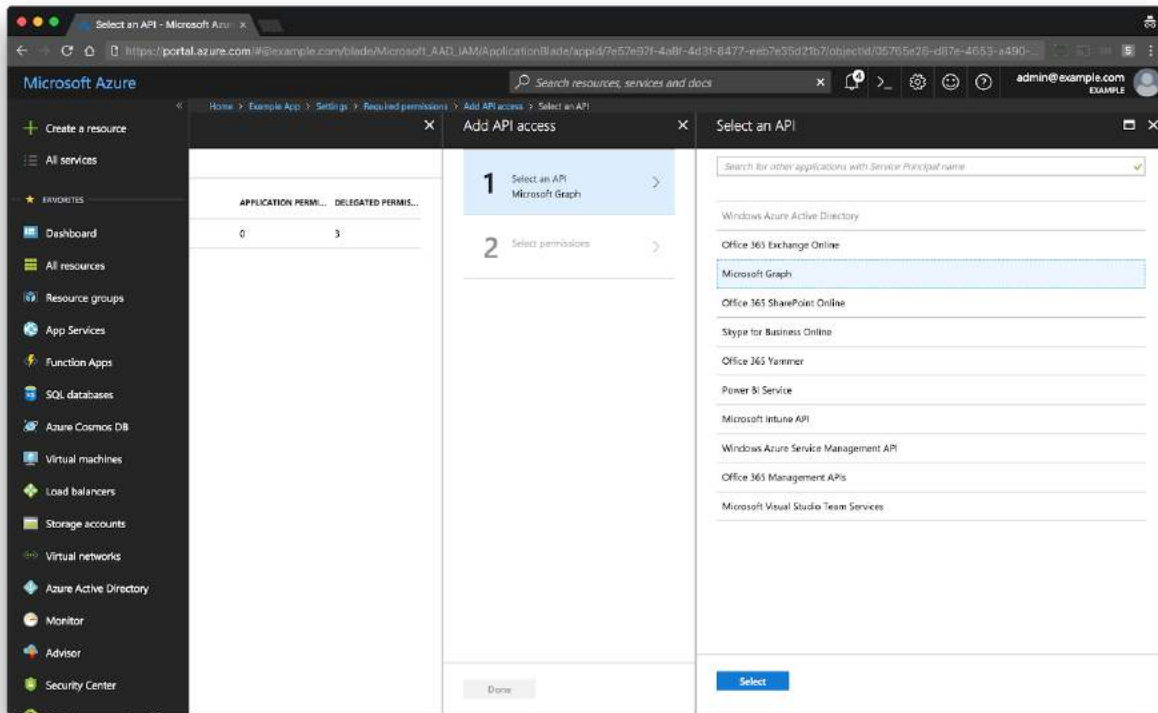
Click **Add** on the **Required Permissions** page to add Microsoft Graph API permissions.



Click on **Select an API** under Add API Access.



Click on **Microsoft Graph** under **Select an API** page and click the **Select** button at the bottom.

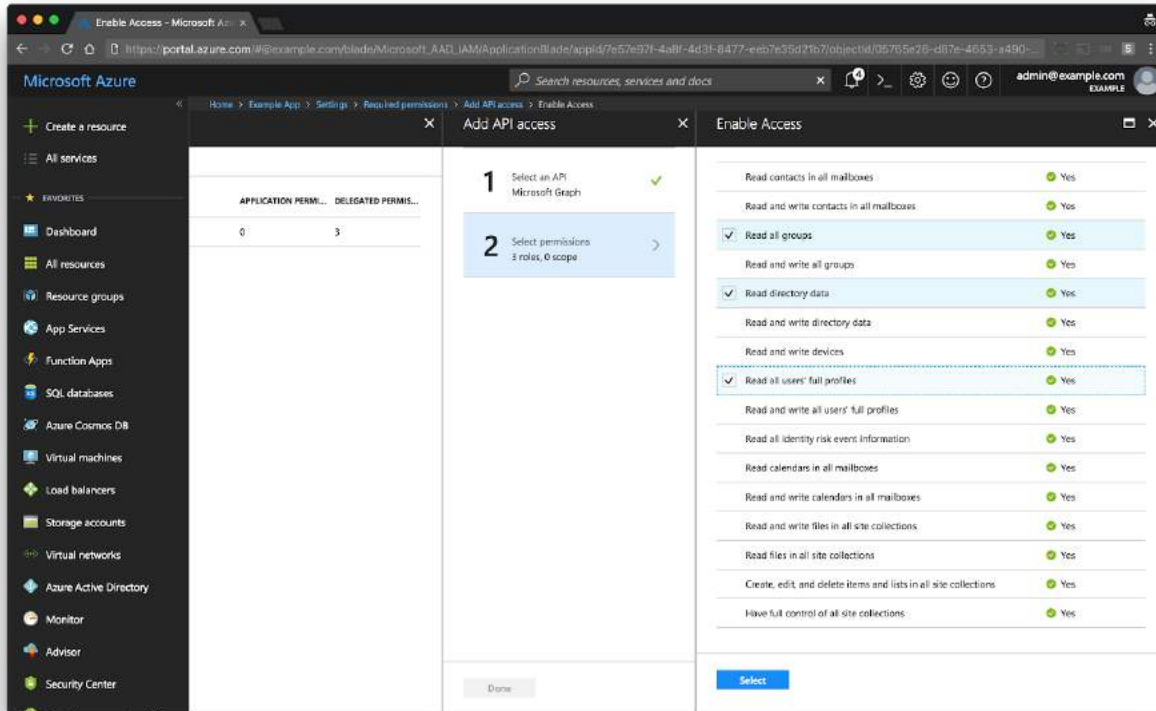


Click on **Select Permissions** on **Add API Access** page.

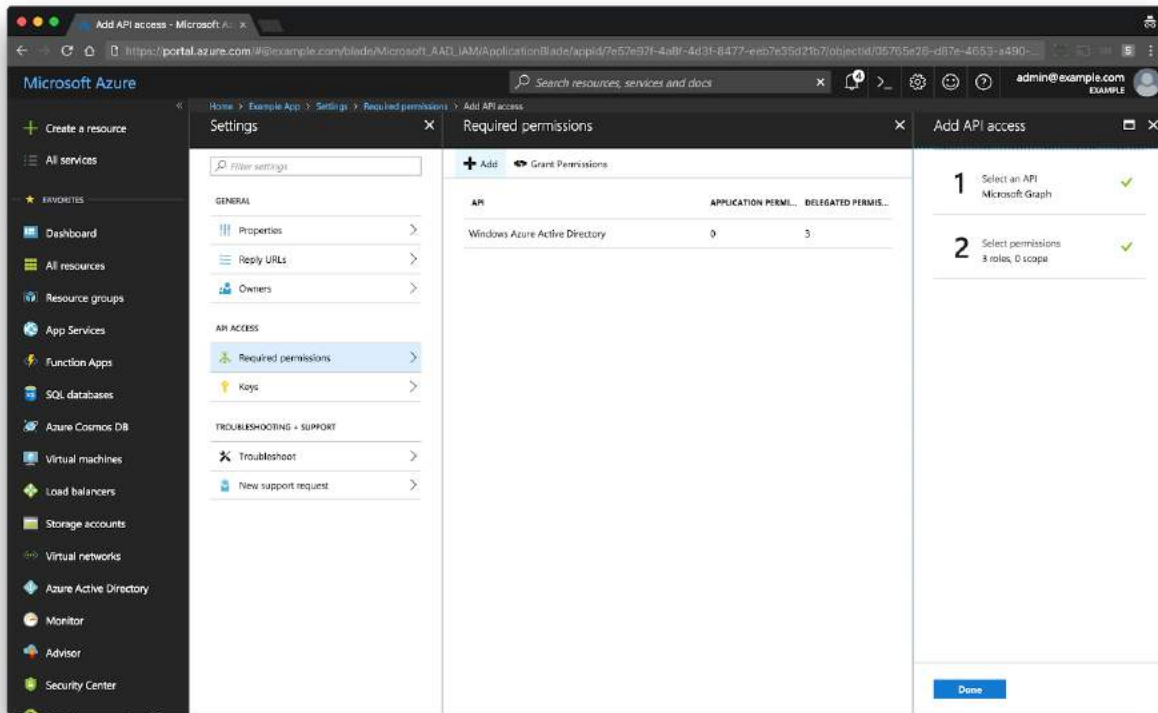
Select the following permissions under **Application Permissions** on **Enable Access** page under Application Permissions:

- ✓ Read all groups
- ✓ Read directory data
- ✓ Read all users' full profiles

Click the **Select** button at the bottom.

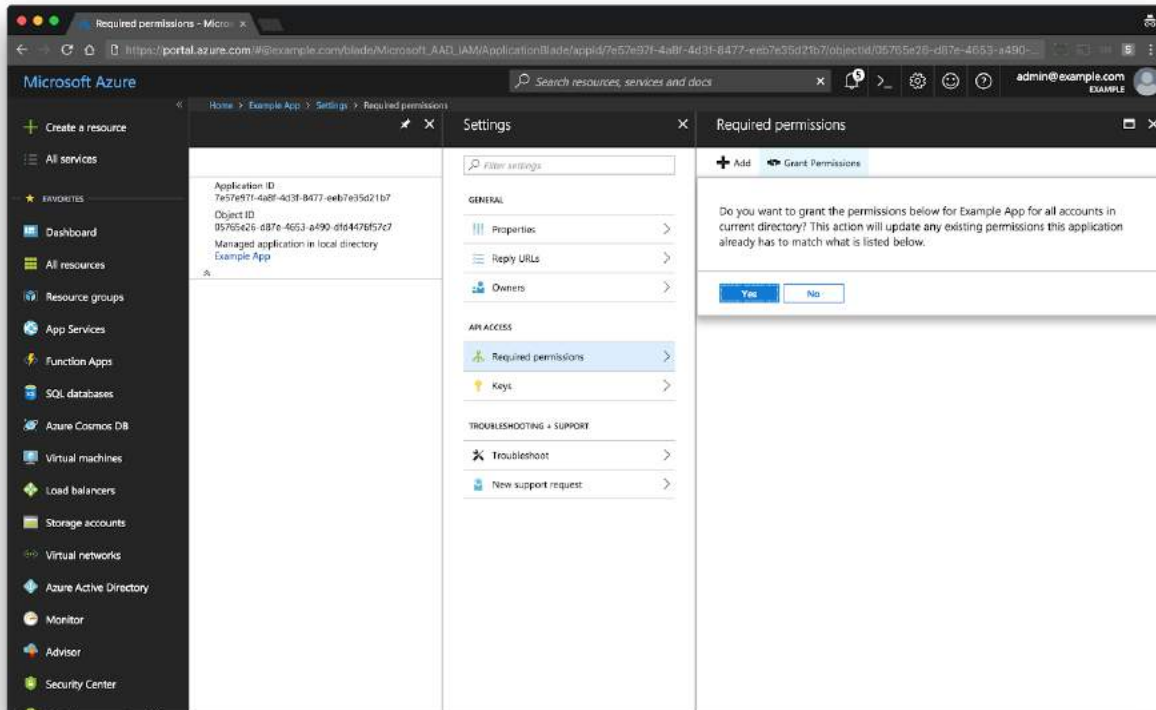


Click **Done** at the bottom of the **Add API Access** page.



Click on the **Grant Permissions** button highlighted in the image below, and click **Yes** to assign the required permissions to the application.

Please note, administrative access to the domain is required for this step.

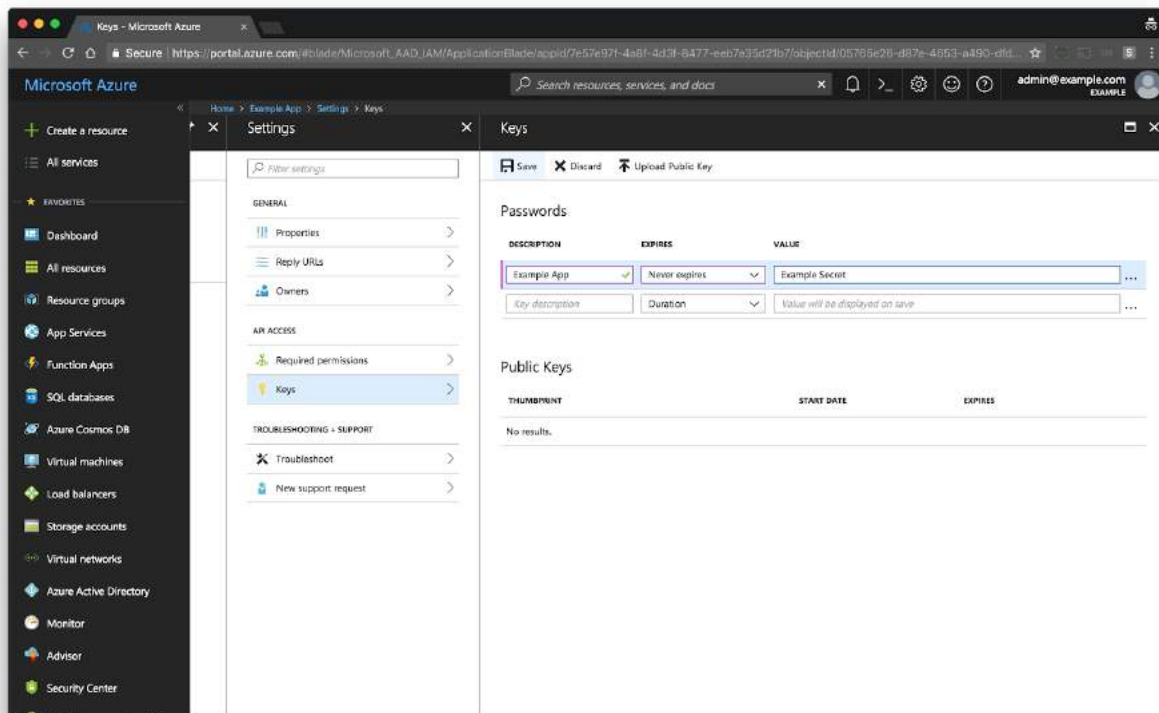


Click on **Keys** under **API Access** on the **Settings** page to generate an application secret.

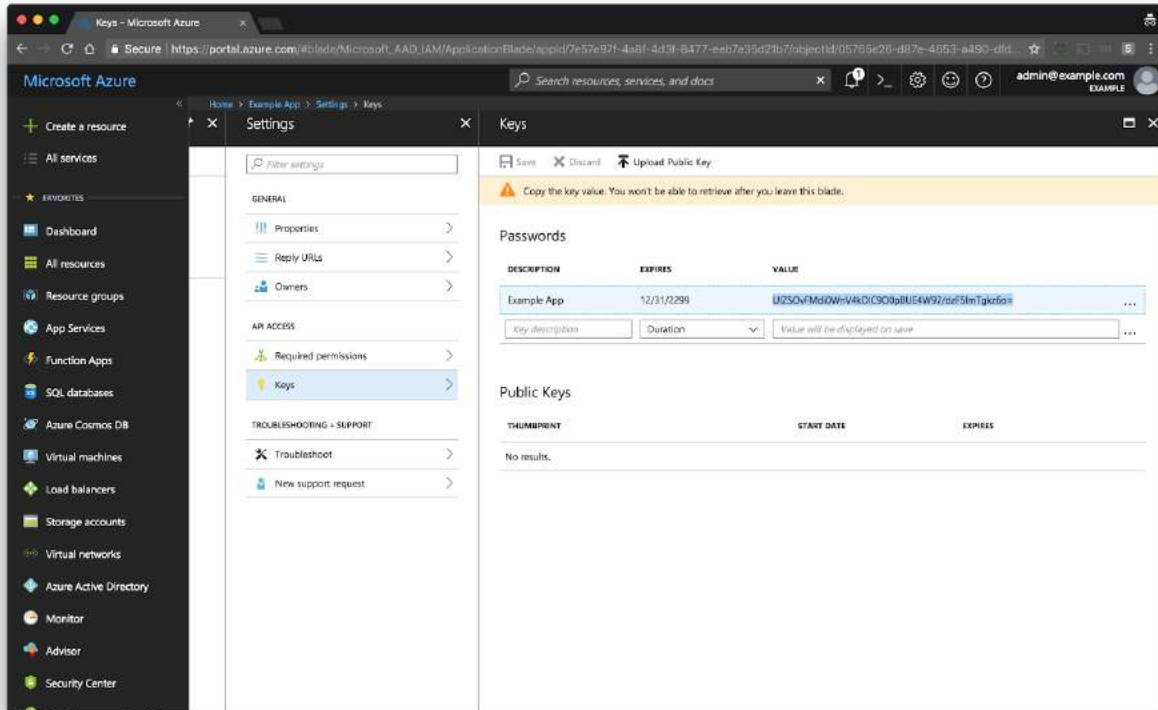
Enter the following details on the Password form:

- DESCRIPTION: Example App Name
- EXPIRES: Select **Never Expires** from the dropdown list
- VALUE: Any random words or characters. In the example below, the value is Example Secret

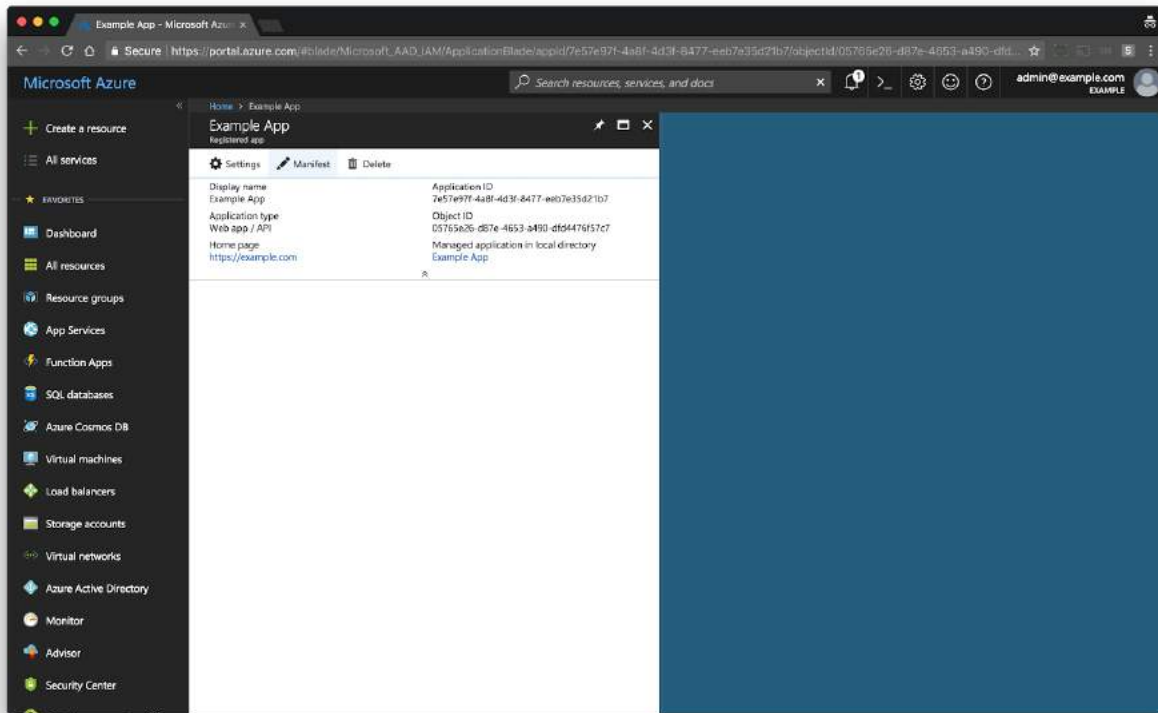
Click the **Save** button.



After clicking **Save**, the **VALUE** field will be updated. Copy the new value displayed on the screen, which is highlighted in the image below. Save this value, as it will be used as the **Application Secret** in later steps.



Click the **X** button to close the **Keys** page, then click the **X** button to close the **Settings** page.
Click on the **Manifest** button to open Application manifest.

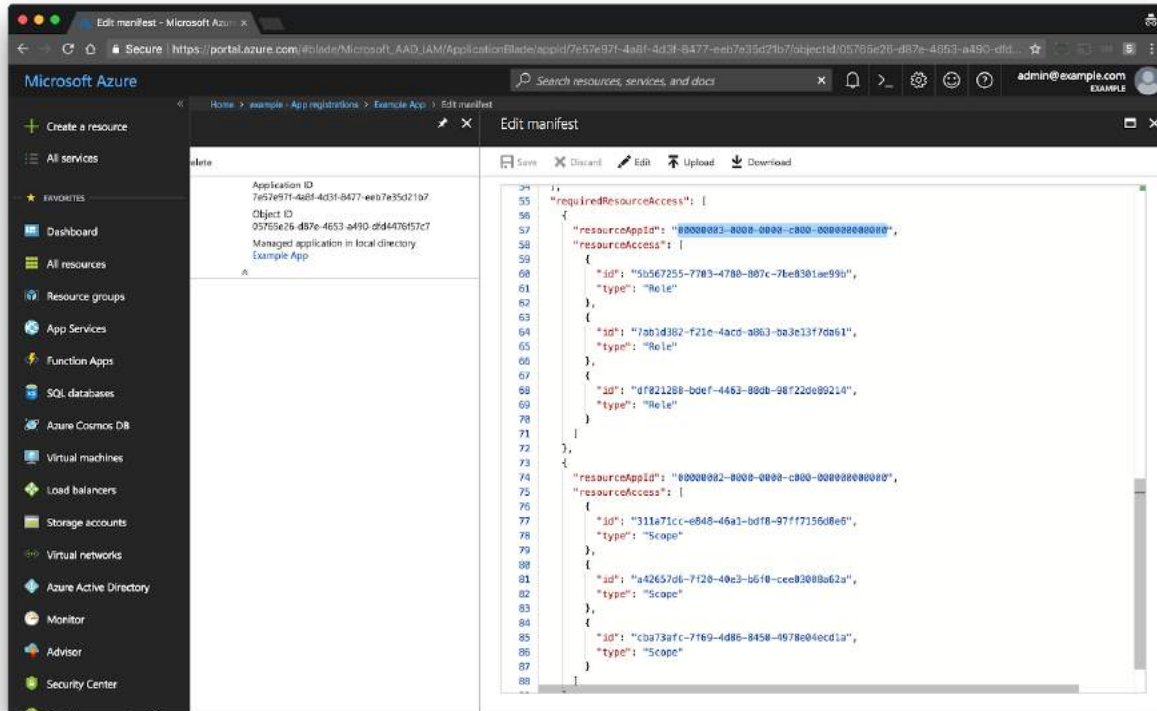


Scroll to the bottom of the Manifest file to the **requiredResourceAccess** section and copy the two **resourceAppId** fields.

In the example below, the **resourceAppId** fields are:

- Resource ID - **00000002-0000-0000-c000-000000000000**
- Admin Resource ID - **00000003-0000-0000-c000-000000000000**

If the resourceAppId are exactly similar to the above, then use the above results.



Credentials

From the previous steps, the following identifiers will be used when registering Microsoft Office Adapter on Bridge.

- Application ID
- Application Secret
- Tenant ID
- Resource ID
- Admin Resource ID

Click on Microsoft Office icon on **Add Adapter** page, Enter the credentials in the form and click **SIGN IN**.

The screenshot shows a web browser window titled 'Client Setup' with the URL 'https://example.com/bridge/admin/new?id=ce22519f-1271-4d3d-8e9e-ef5e5d05350'. The page is titled 'Setup a new adapter' and has three steps: 1. Select an adapter (completed), 2. Enter credentials (current step), and 3. Authorize Application.

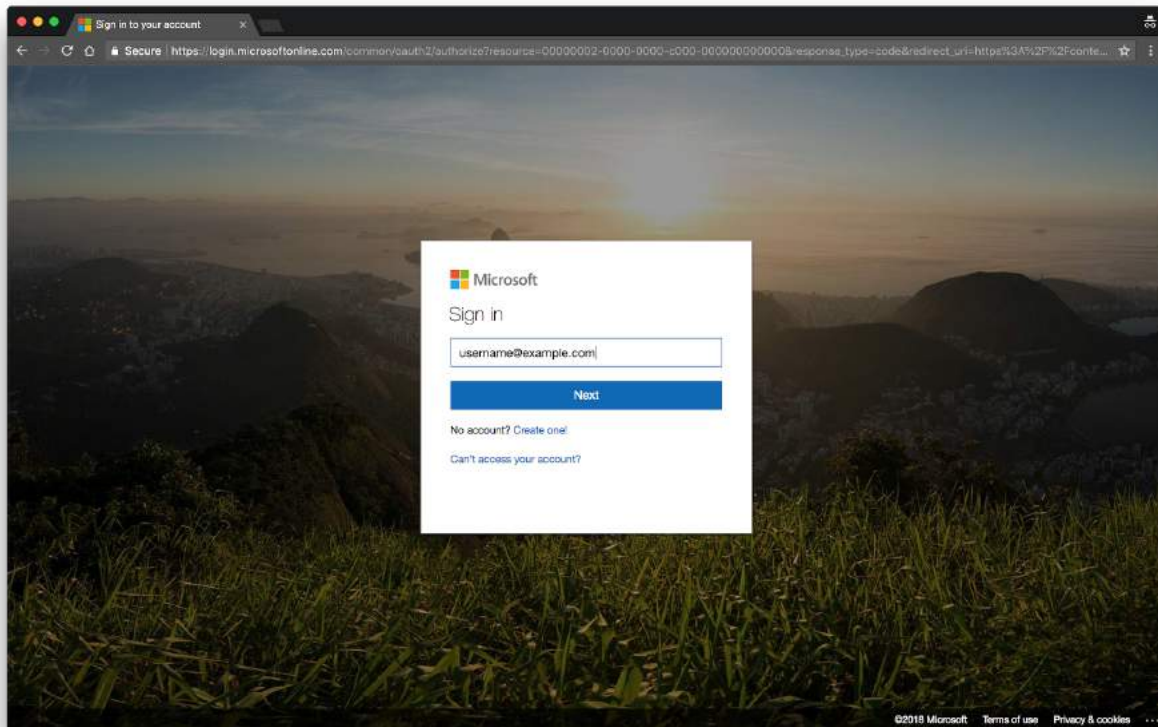
Under the 'Azure' section, there is a note: 'To retrieve the appropriate credentials, please login to your Microsoft Office 365 account and access your account settings.'

The form contains the following fields:

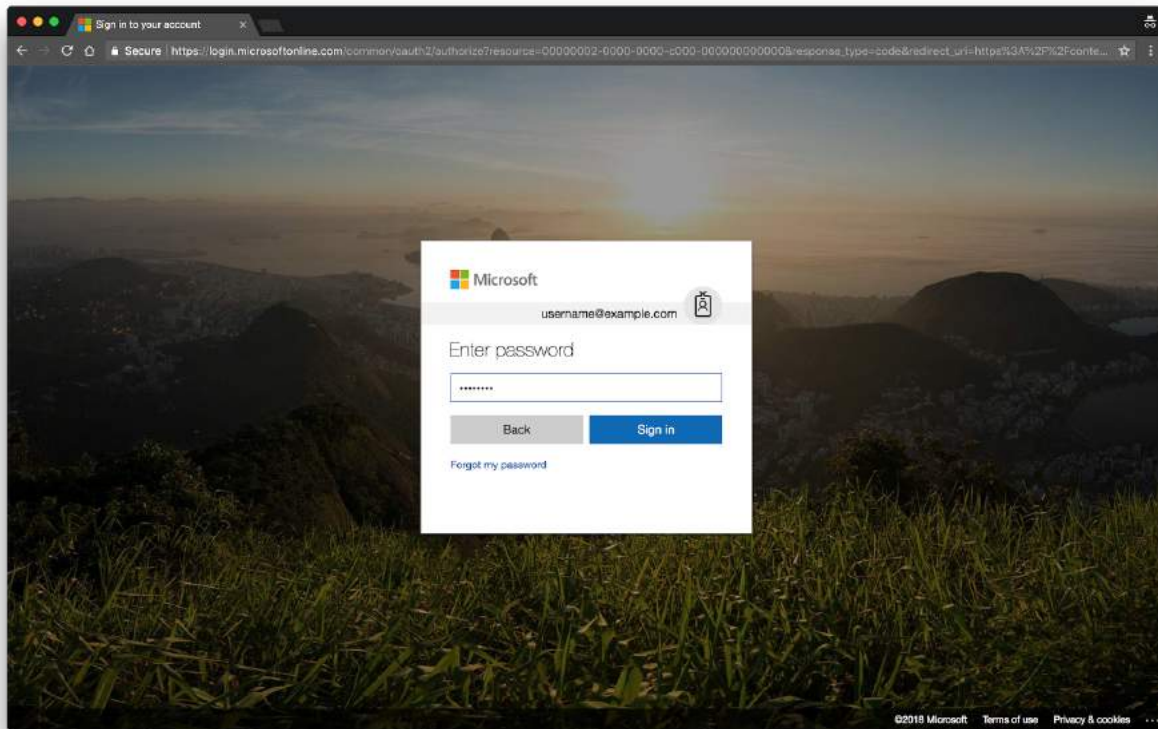
- Name: Microsoft Office
- Application ID: 7e57e97f-4a8f-4d3f-8477-eeb7e35d21b7
- Application Secret: 401jBIY5Bq5FXd5Kvm0aDHXoD3hYu+7C0YzS5Tl35A=
- Tenant ID: f7a3bc09-a37d-46de-8df1-a572825b6590
- Resource ID: 00000002-0000-0000-c000-000000000000
- Admin Resource ID: 00000003-0000-0000-c000-000000000000

At the bottom right, there are 'BACK' and 'SIGN IN' buttons.

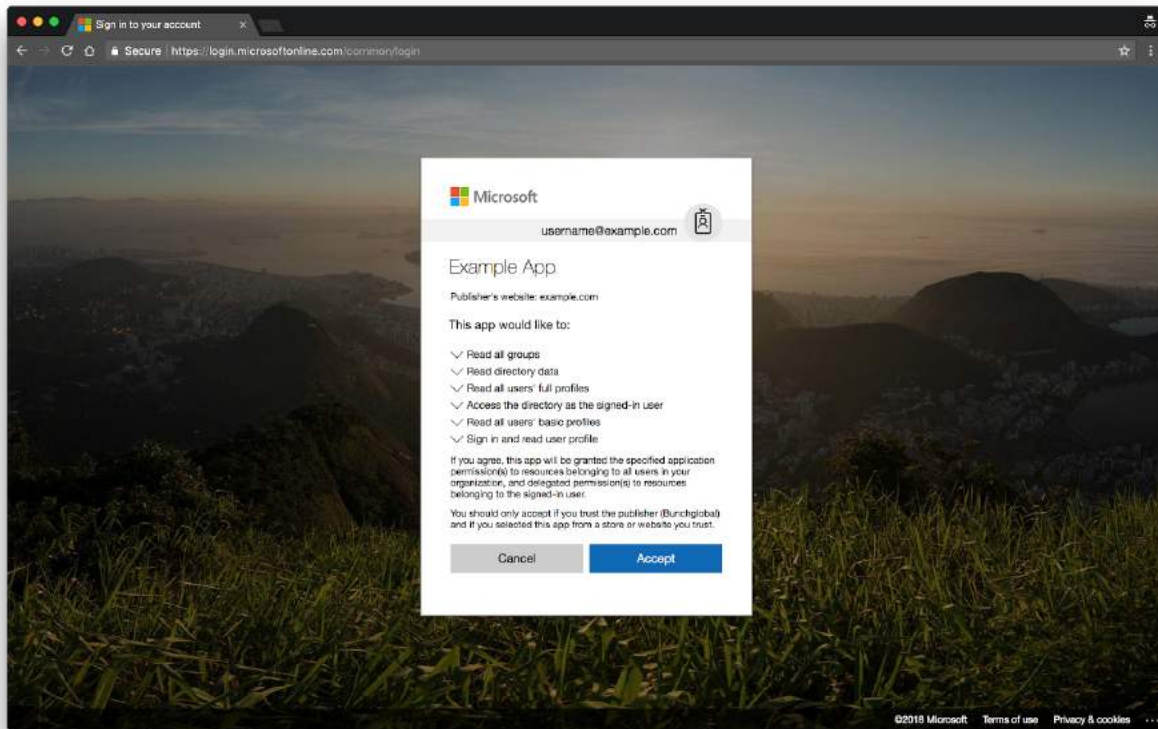
If the entered credentials are valid, the page is redirected to the Microsoft login page. Enter your email address and click on the **Next** button.



Enter the password and click **Sign In**.



Click **Accept** to authorize Bridge access to user information.



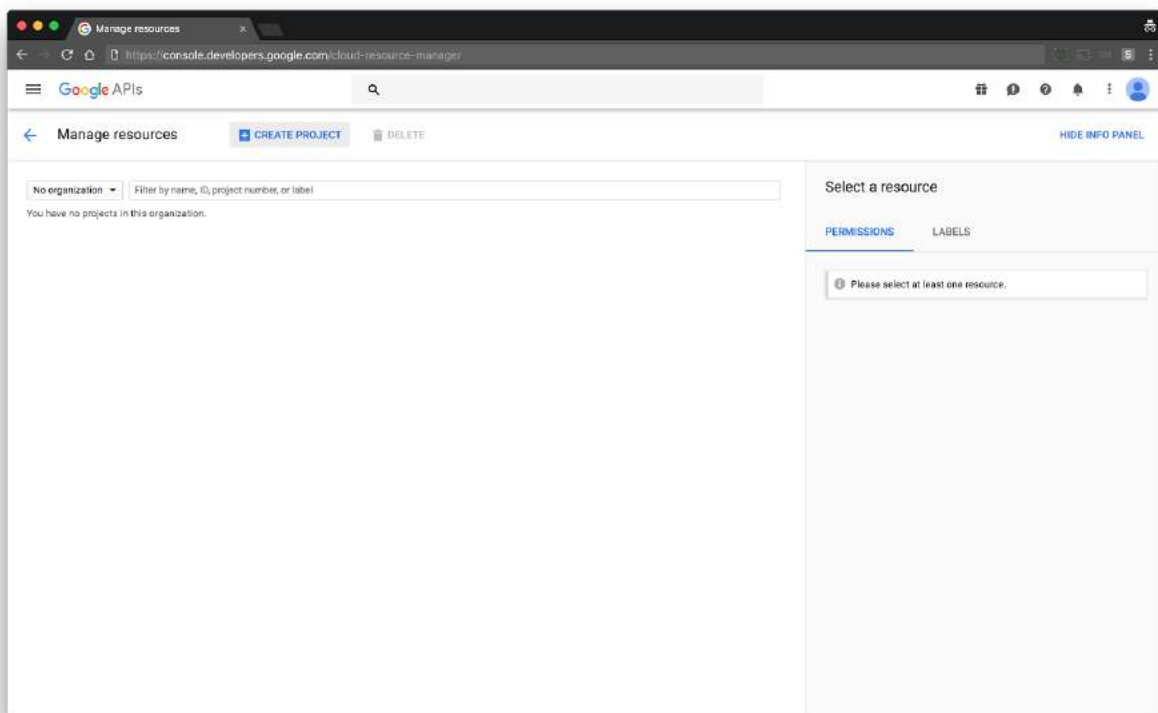
Google G Suite

Preparations

In order to setup a Google adapter with Bridge, a G Suite enabled Google account is required with G Suite administrative access.

Create a Project

Open on Cloud Resource Manager² on Google Developer Console³, Click on **No Organization** dropdown to select the organization and click on **Create Project**



² Cloud Resource Manager - <https://console.developers.google.com/cloud-resource-manager>

³ Google Developer Console - <https://console.developers.google.com>

Enter a project name and click **Create**.

Google Cloud Platform

Secure | <https://console.developers.google.com/project/create?previousPage=%2Fcloud-resource-manager%2Fauthuser%3D1&defaultProjectName=&authuser=1&project=1&id=der&organization=...>

Google APIs

New Project

You have 10 projects remaining in your quota. [Learn more.](#)

Project name ⓘ
Example Project

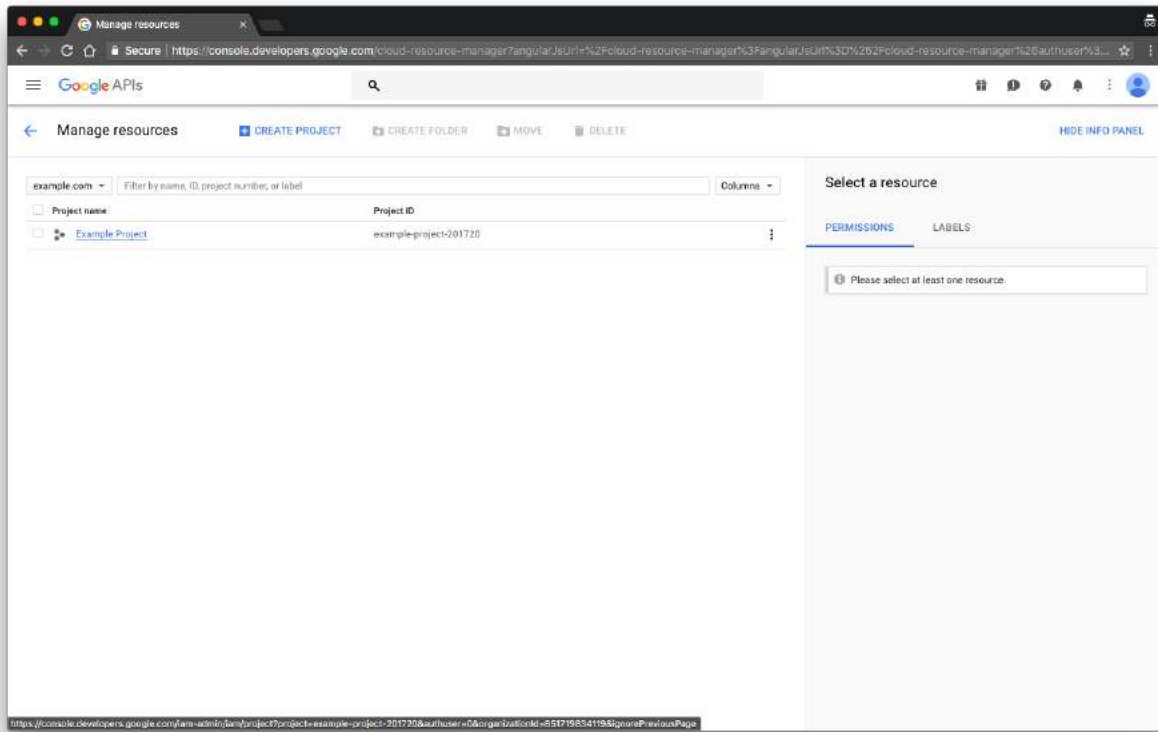
Your project ID will be example-project-201720 ⓘ [Edit](#)

Organization ⓘ
example.com

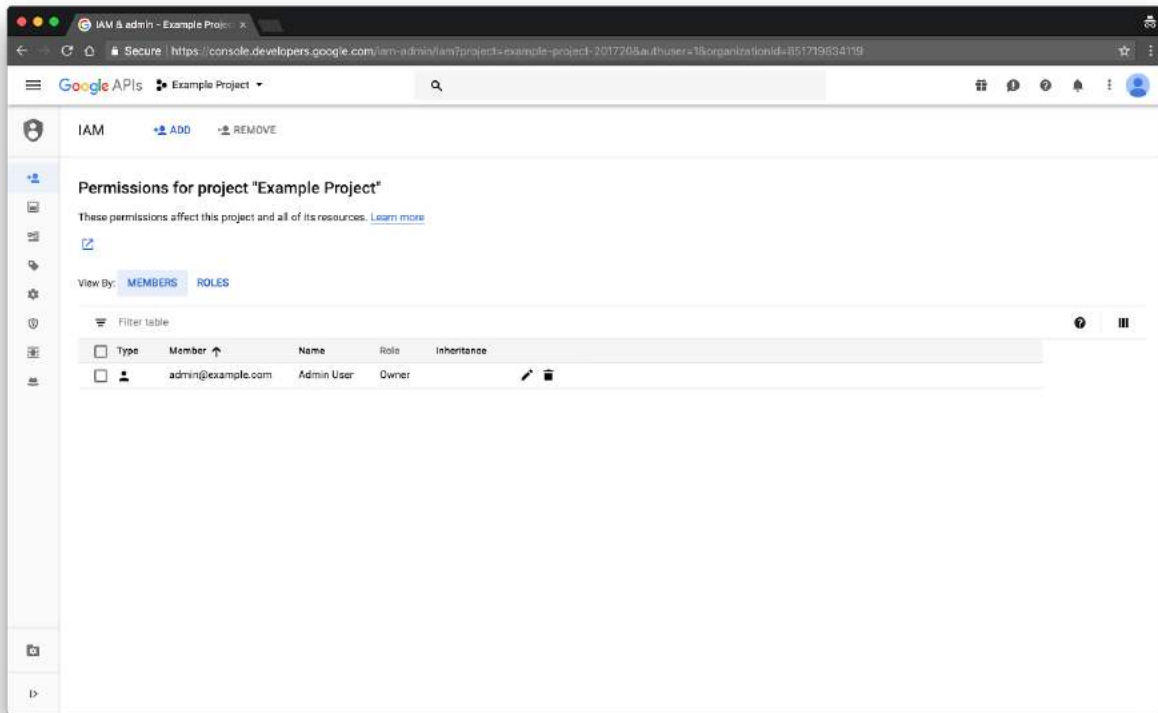
You have logged in under a managed account. Your domain administrator may be able to access, change or suspend any projects created using this account. If you do not want your domain administrator to access your projects, please log out and create a project under an unmanaged Google Account. For more information, please review [Google's Privacy Policy](#).

Create Cancel

Click on the project name entered in the previous step.



IAM page shows up with list of users that have access to the project.



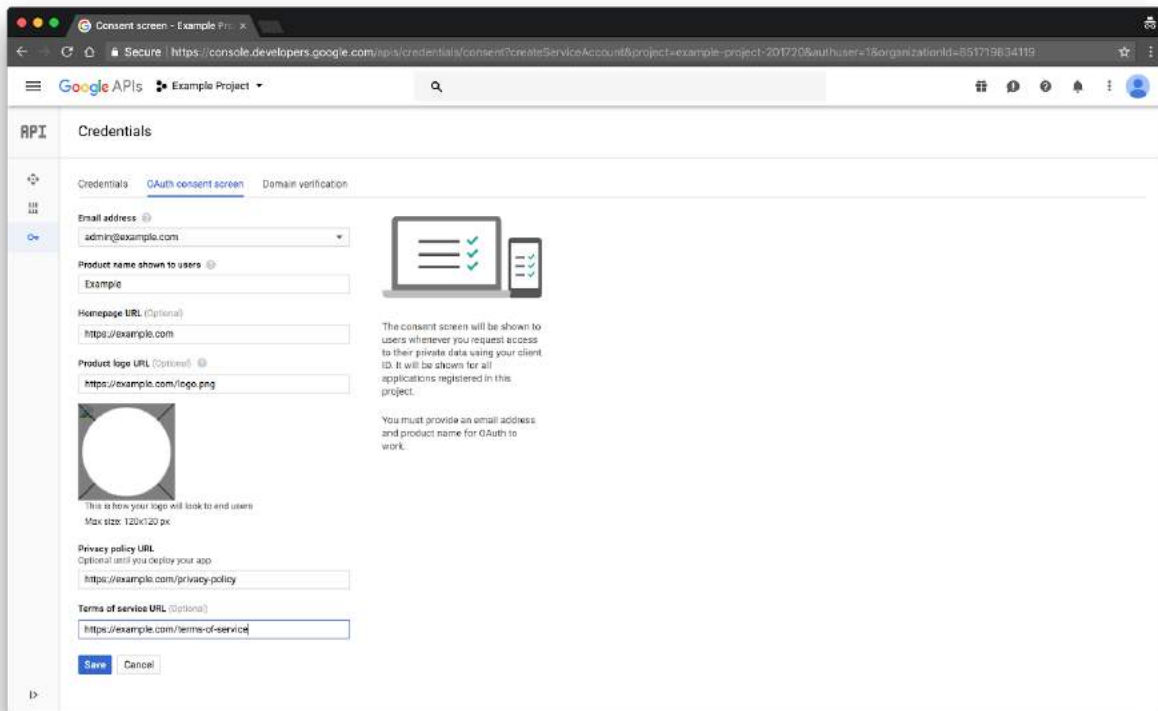
Configure Consent Screen

Open the [API dashboard](#)⁴ and click on **Credentials** (key icon) on the left side of the screen and select the **oAuth consent screen** tab.

Enter the following the details to configure the consent screen:

- Product Name shown to the users
- Homepage URL (optional)
- Product Logo (optional)
- Privacy Policy URL
- Terms of Service URL (optional)

Click **Save**.



The screenshot shows the 'oAuth consent screen' configuration page in the Google API console. The page is titled 'Credentials' and has three tabs: 'Credentials', 'oAuth consent screen' (selected), and 'Domain verification'. The 'oAuth consent screen' tab contains the following fields and instructions:

- Email address:** A dropdown menu with 'admin@example.com' selected.
- Product name shown to users:** A text input field with 'Example' entered.
- Homepage URL (Optional):** A text input field with 'https://example.com' entered.
- Product logo URL (Optional):** A text input field with 'https://example.com/logo.png' entered.
- Product logo:** A placeholder image with a circular logo and the text 'This is how your logo will look to end users. Max size: 120x120 px.'.
- Privacy policy URL:** A text input field with 'https://example.com/privacy-policy' entered.
- Terms of service URL (Optional):** A text input field with 'https://example.com/terms-of-service' entered.

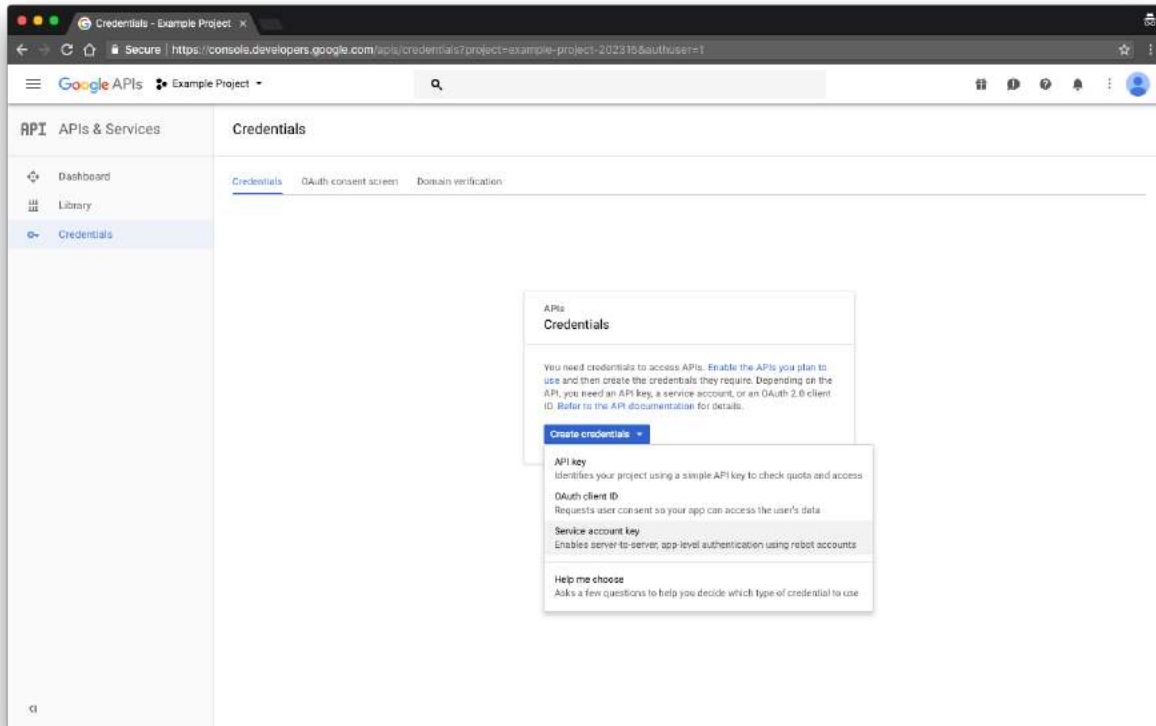
On the right side of the page, there is a diagram of a laptop and a smartphone displaying a consent screen. Below the diagram, there is a note: 'The consent screen will be shown to users whenever you request access to their private data using your client ID. It will be shown for all applications registered in this project.' Below this note, there is another note: 'You must provide an email address and product name for oAuth to work.'

At the bottom left, there are 'Save' and 'Cancel' buttons.

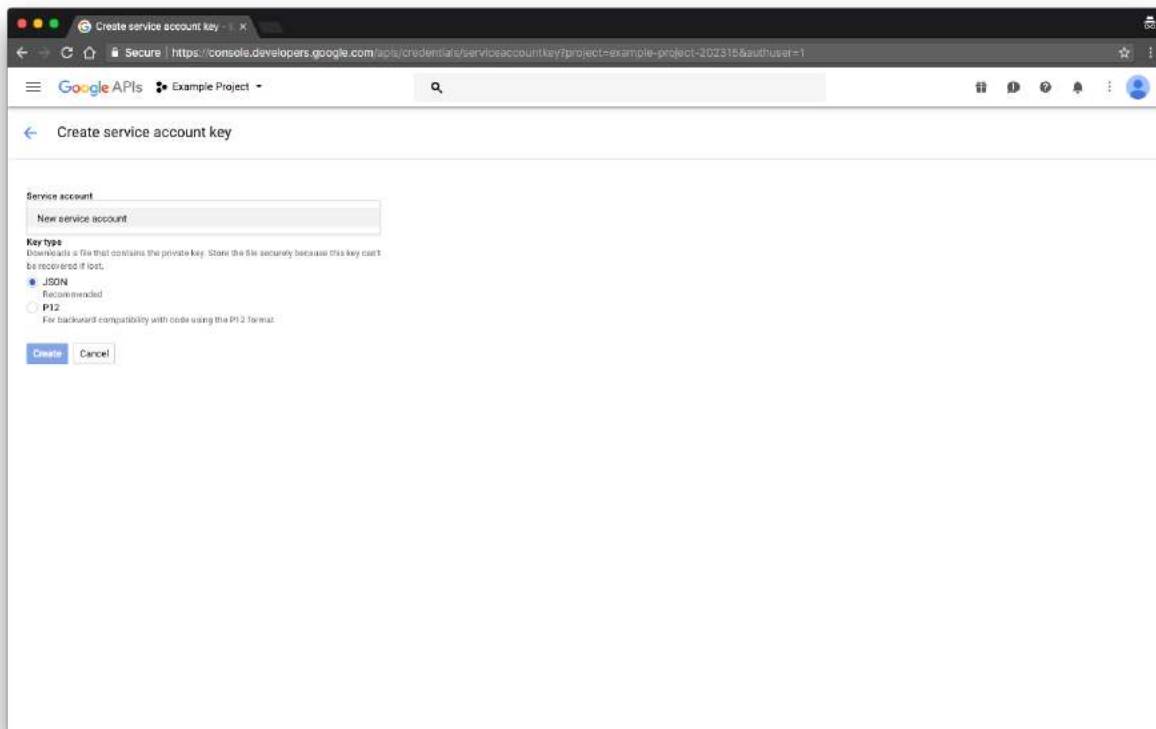
⁴ API Dashboard - <https://console.developers.google.com/apis/dashboard>

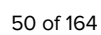
Create Service Account

Click **Create Credentials** and select **Service Account Key** from the dropdown.



Under the service account dropdown, select **New Service Account**.

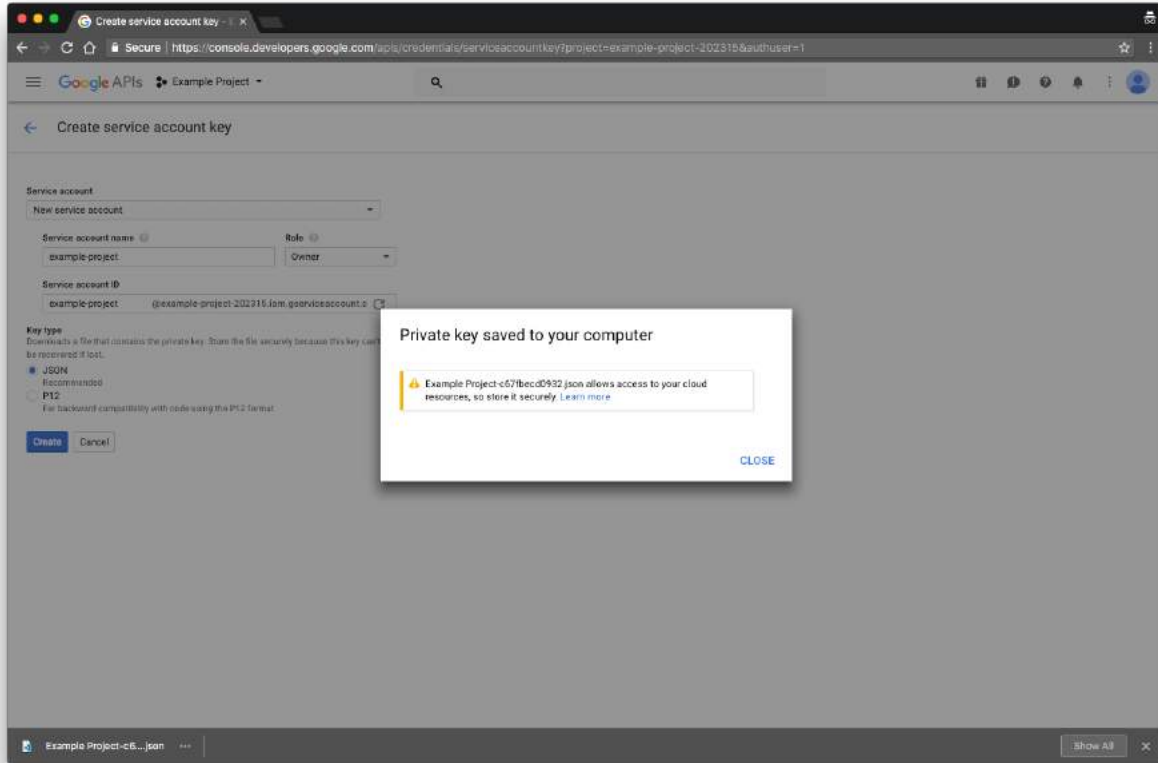




A JSON file is automatically downloaded onto your browser with the project name. Keep the JSON file in a safe place as it's not possible to redownload it.

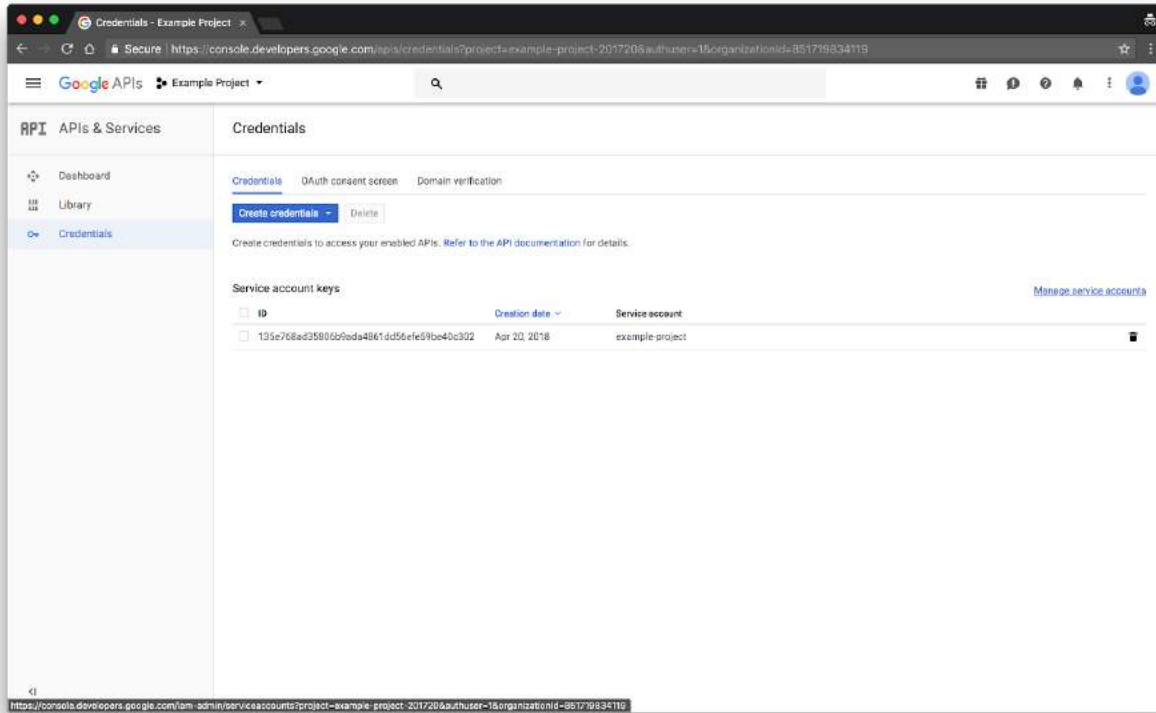
WARNING

Do not misplace the downloaded file.

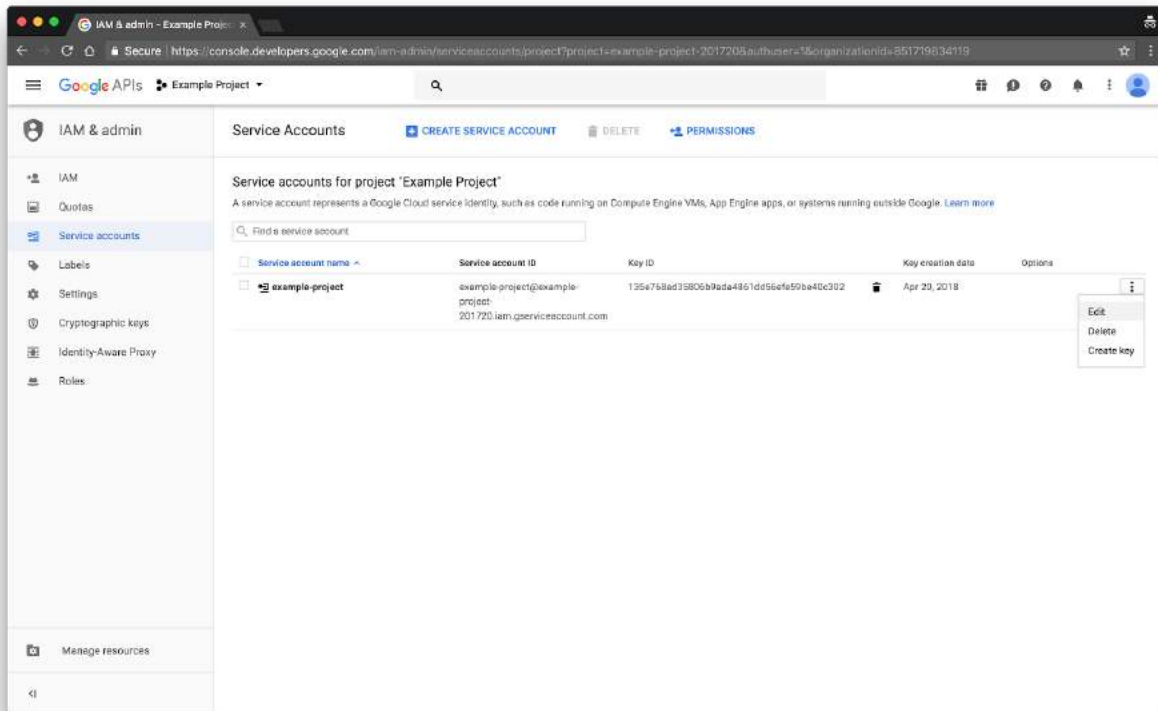


Delegate Permissions

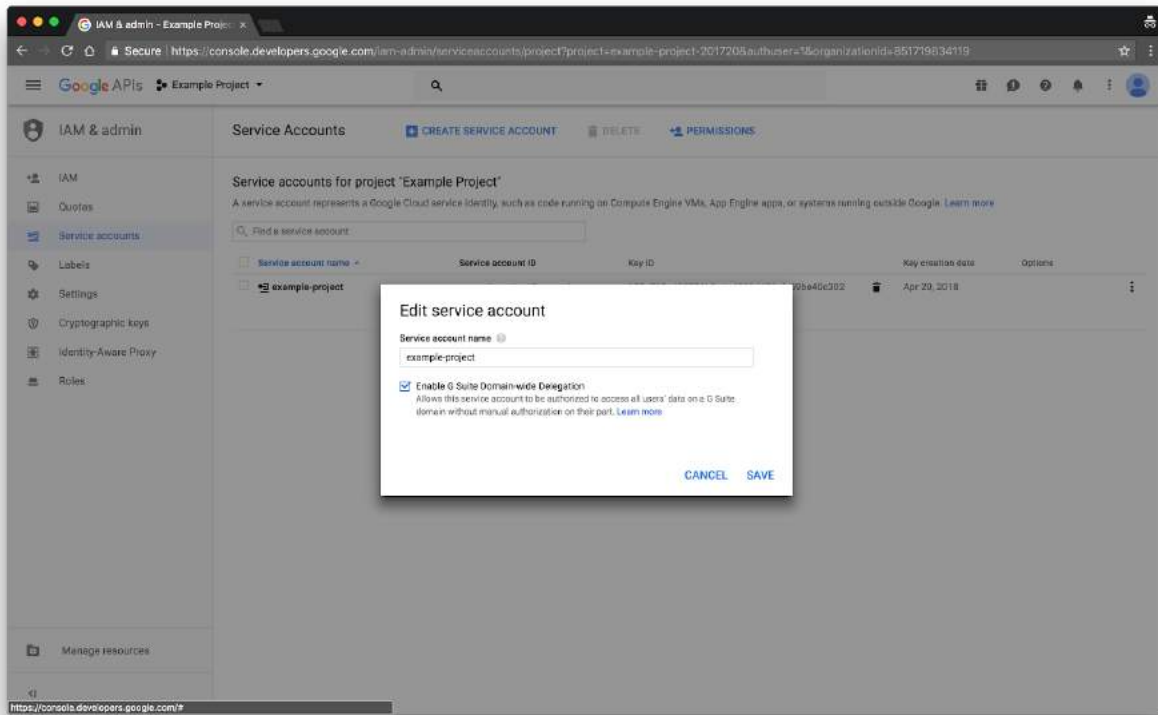
Ask your domain administrator to delegate admin permissions to the service account.
Click on the **Manage service accounts** link on right-side of the Service Account keys section



Select the **: More** button under options on the right side and click **Edit**.

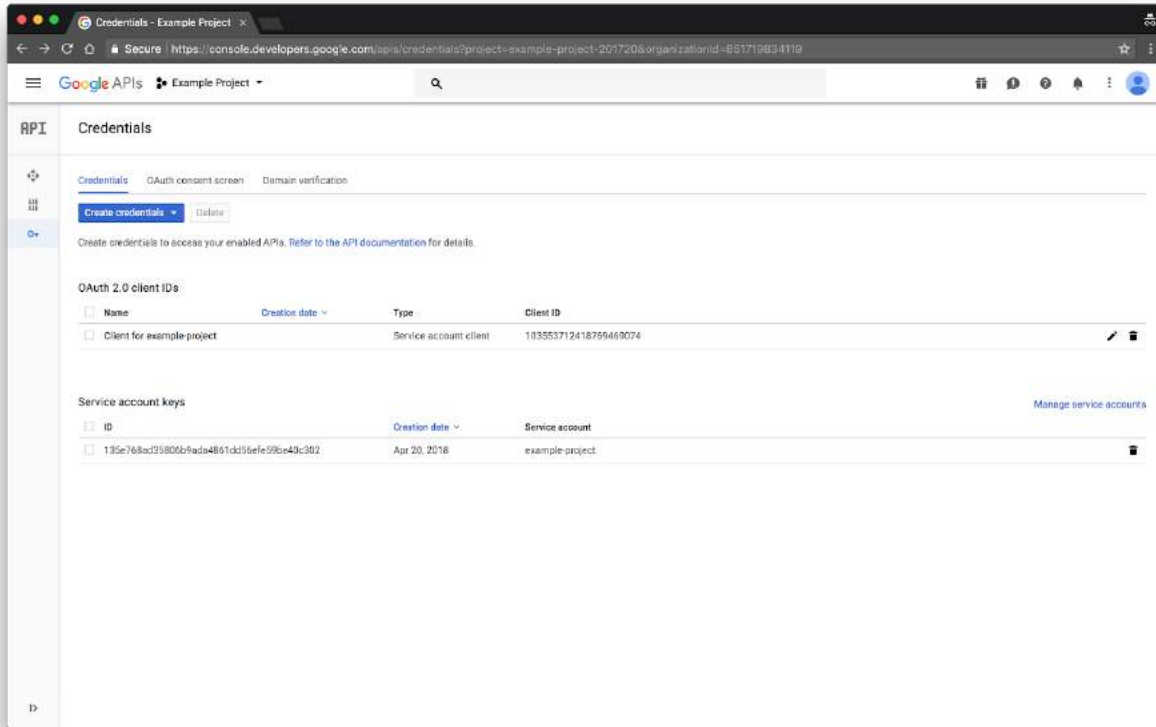


Check the **Enable G Suite Domain-wide Delegation** and click **Save**.



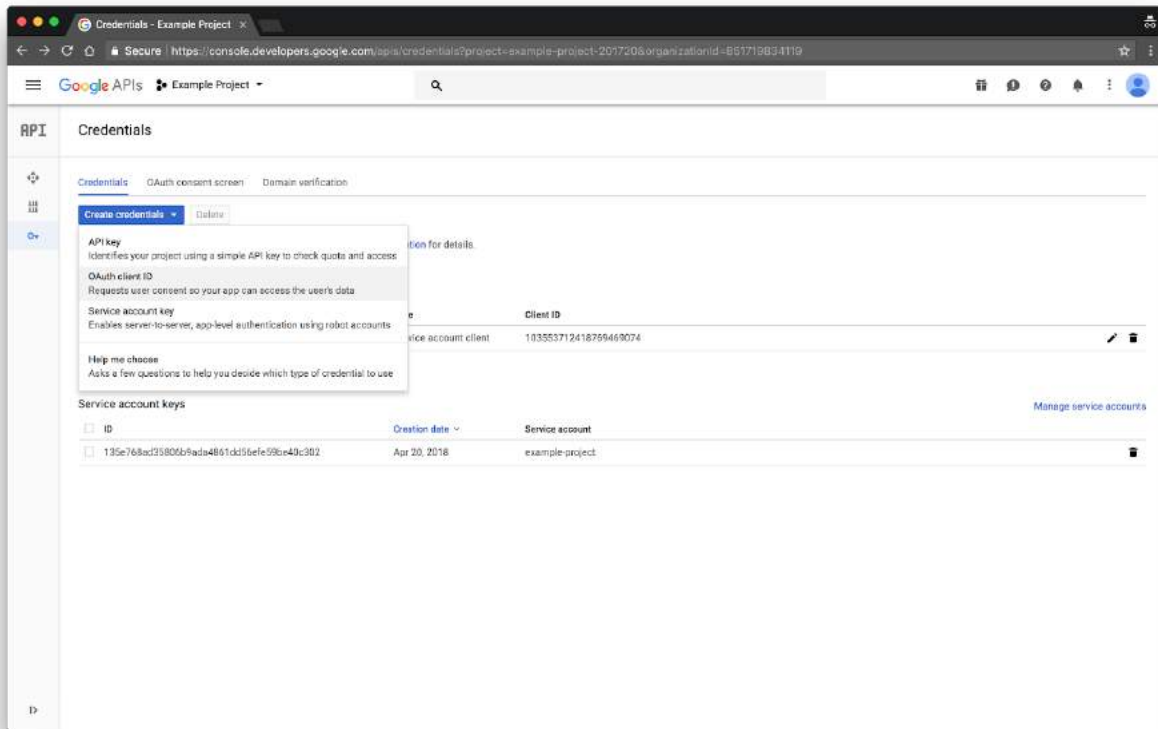
Create oAuth Client Account

Open [API Dashboard](https://console.developers.google.com/apis/credentials)⁵ and click on **Credentials** (key icon) in the left-side navigation bar and click on the **Credentials** tab



⁵ API Dashbaord - <https://console.developers.google.com/apis/credentials>

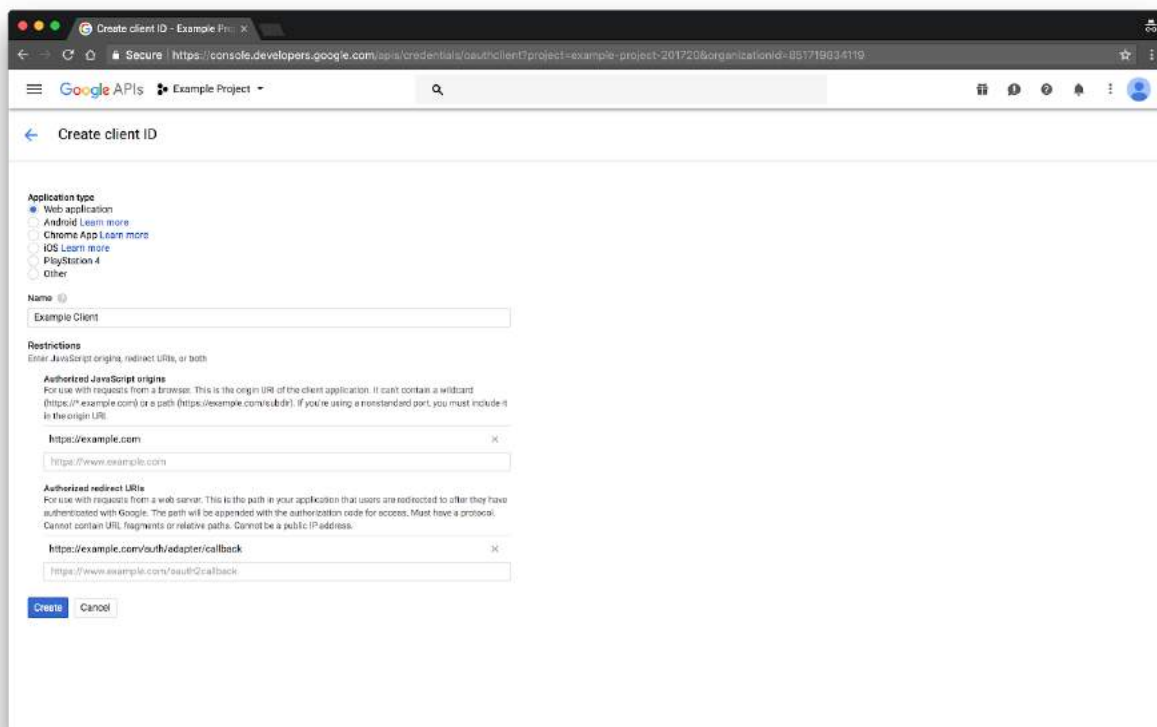
Click **Create Credentials** and click **OAuth Client ID** from the dropdown.



Set the application type to **Web Application**. Enter the following details to create the oAuth client:

- **Name:** Displayed to the user when they sign-in for the first time
- **Authorized Javascript Origins:** List of whitelisted domains that are authorized to use the oAuth client. If Bridge is deployed on example.com then the authorized javascript origins would be **https://example.com**
- **Authorized redirect URIs:** List of URLs the user could be redirected to after they login using their Google credentials. If Bridge is deployed on example.com then it would be **https://example.com/auth/adapter/callback**

Click **Create**.



The screenshot shows the 'Create client ID' page in the Google Cloud Console. The browser address bar shows the URL: `https://console.developers.google.com/apis/credentials/oauthclient?project=example-project-201720&organizationId=051719934119`. The page title is 'Create client ID'. Under 'Application type', 'Web application' is selected. The 'Name' field contains 'Example Client'. Under 'Restrictions', there are two sections: 'Authorized Javascript origins' and 'Authorized redirect URIs'. The 'Authorized Javascript origins' section has a text input field containing 'https://example.com'. The 'Authorized redirect URIs' section has a text input field containing 'https://example.com/auth/adapter/callback'. At the bottom, there are 'Create' and 'Cancel' buttons.

Create client ID - Example Project

Secure | `https://console.developers.google.com/apis/credentials/oauthclient?project=example-project-201720&organizationId=051719934119`

Google APIs | Example Project

Create client ID

Application type

- ☒ Web application
- ☐ Android [Learn more](#)
- ☐ Chrome App [Learn more](#)
- ☐ iOS [Learn more](#)
- ☐ PlayStation 4
- ☐ Other

Name

Example Client

Restrictions

Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (`https://*` example.com) or a path (`https://example.com/subdir`). If you're using a nonstandard port, you must include it in the origin URI.

`https://example.com`

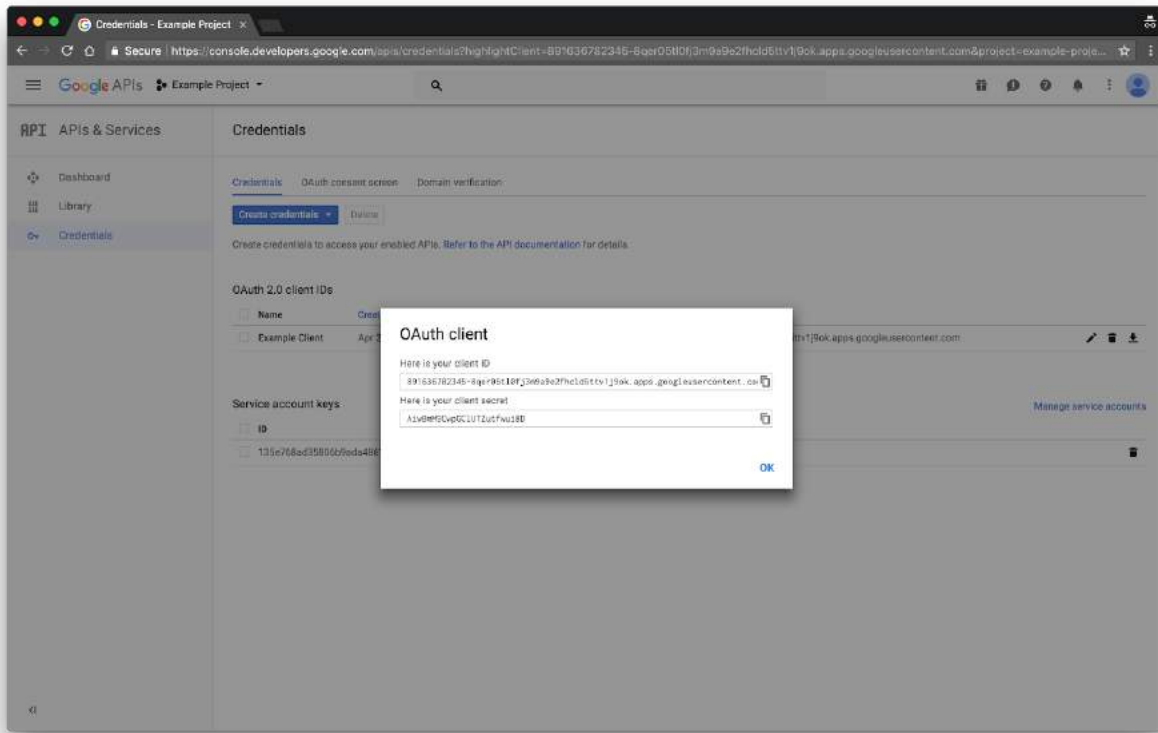
Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authorized with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

`https://example.com/auth/adapter/callback`

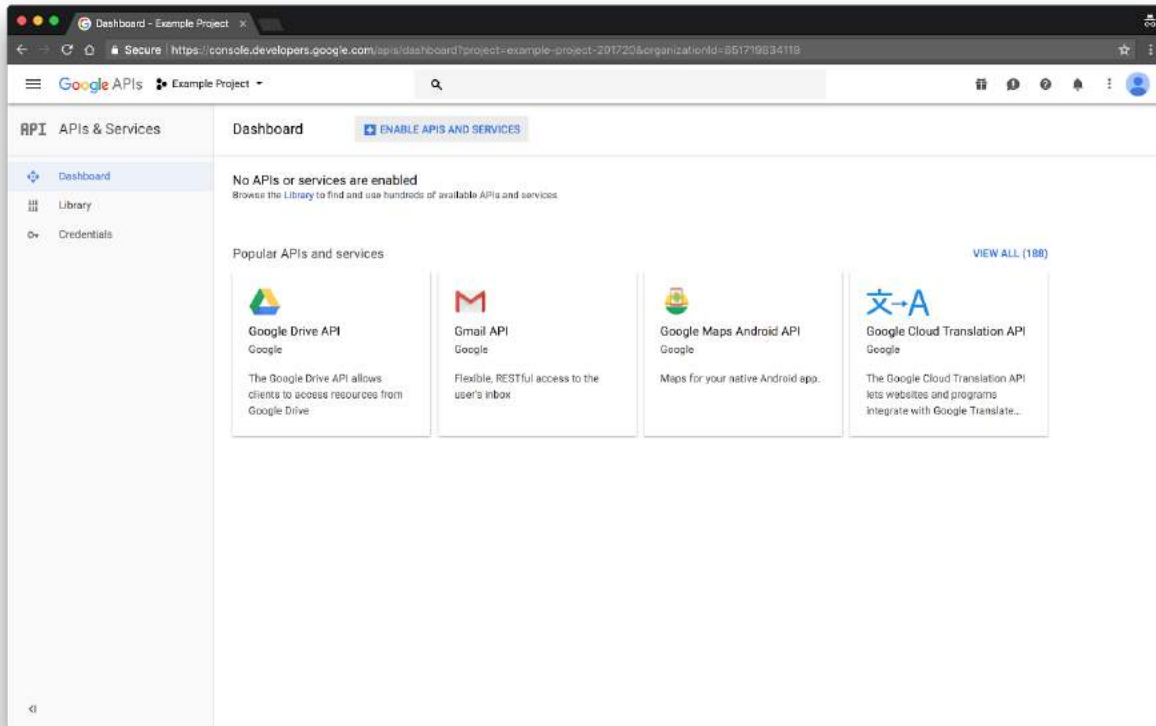
Create Cancel

After creating a new OAuth client, a modal will popup with **Client ID** and **Client Secret**. Please save these credentials as they are required later on in the setup process.



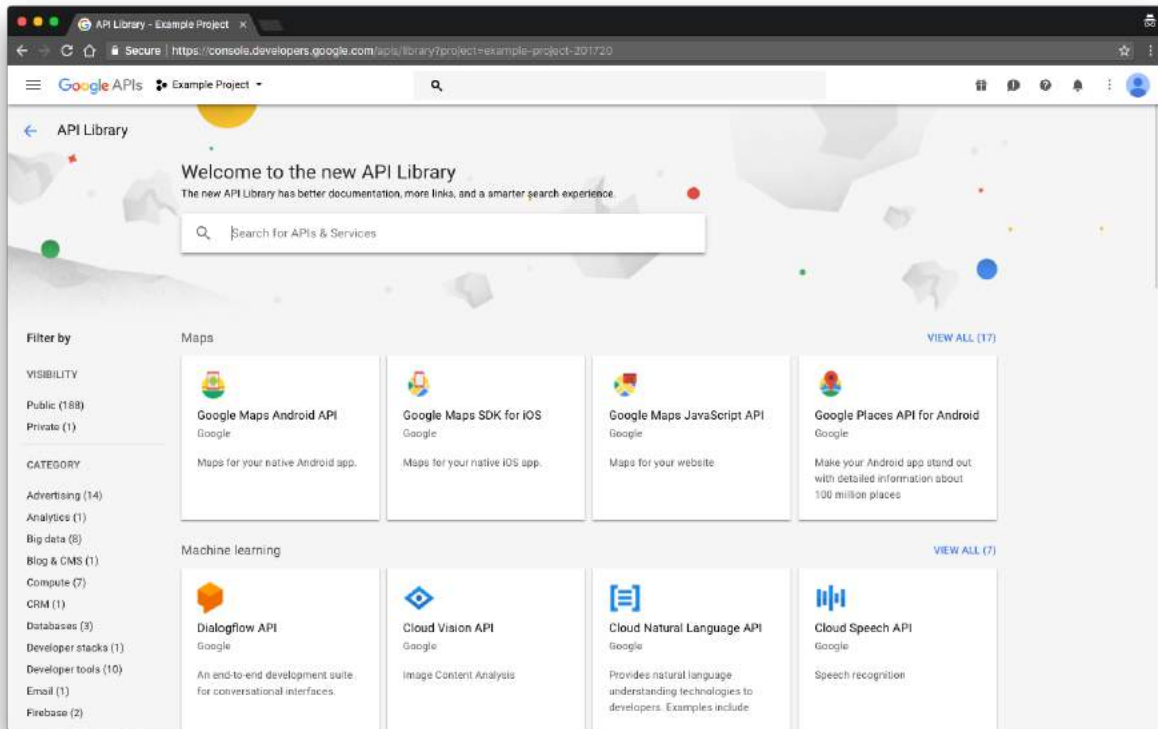
Enable API Services

Open [API Dashboard](#)⁶ and click **Enable API and Services** to open the API library.

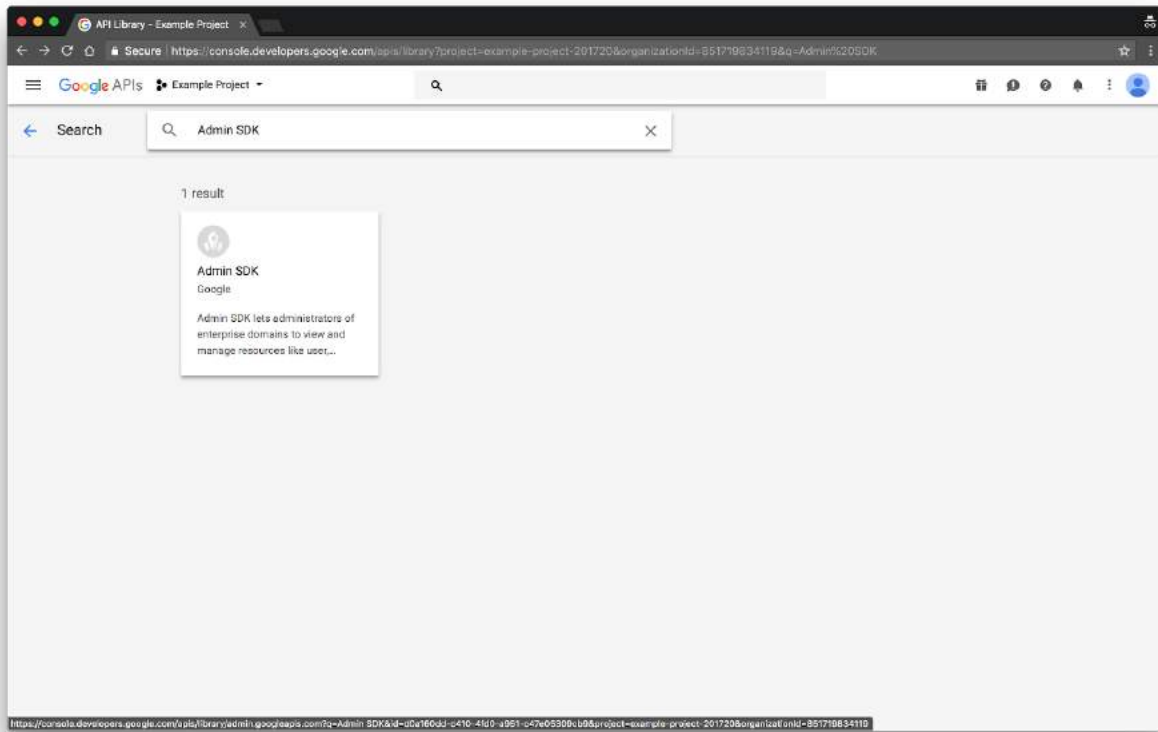


⁶ API Dashbaord - <https://console.developers.google.com/apis/credentials>

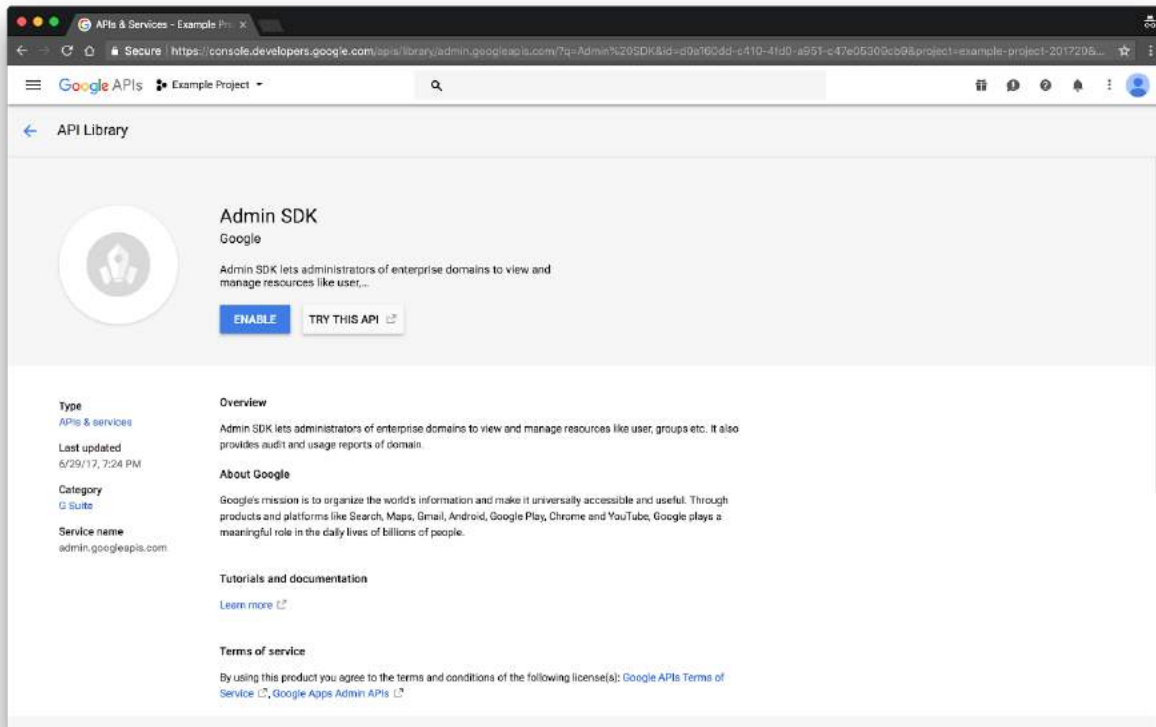
Click on the Search bar under Welcome to the new API Library.



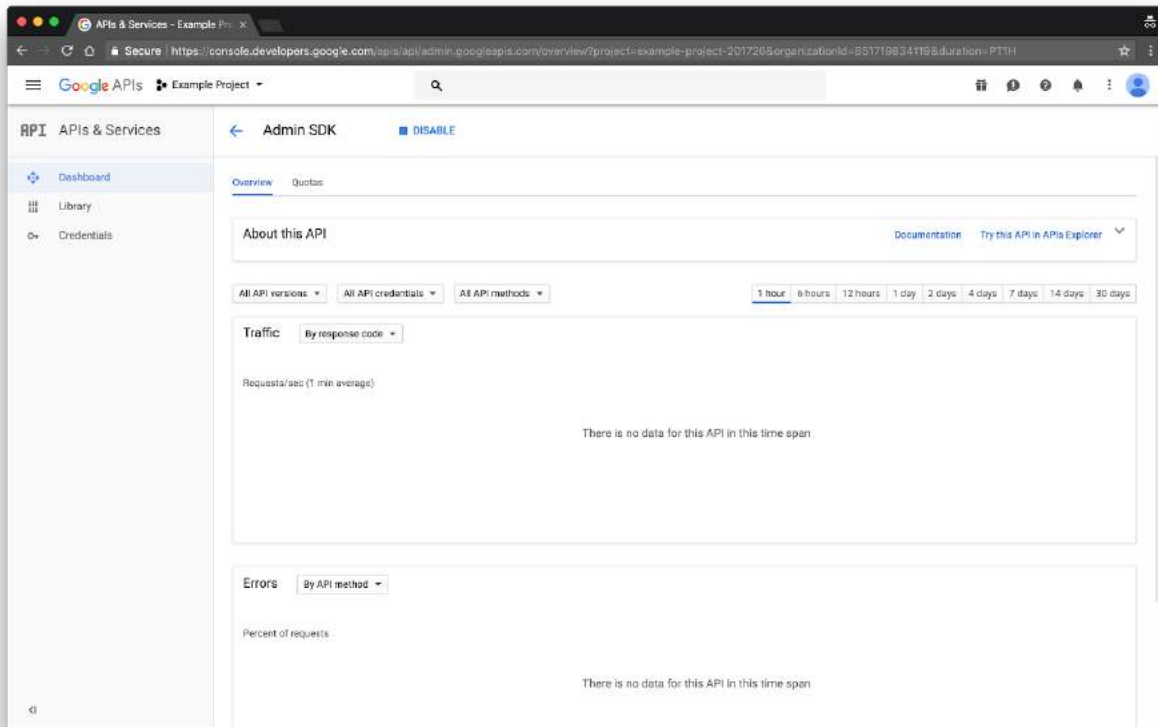
Search for “**Admin SDK**”. Click on the **Admin SDK** card.



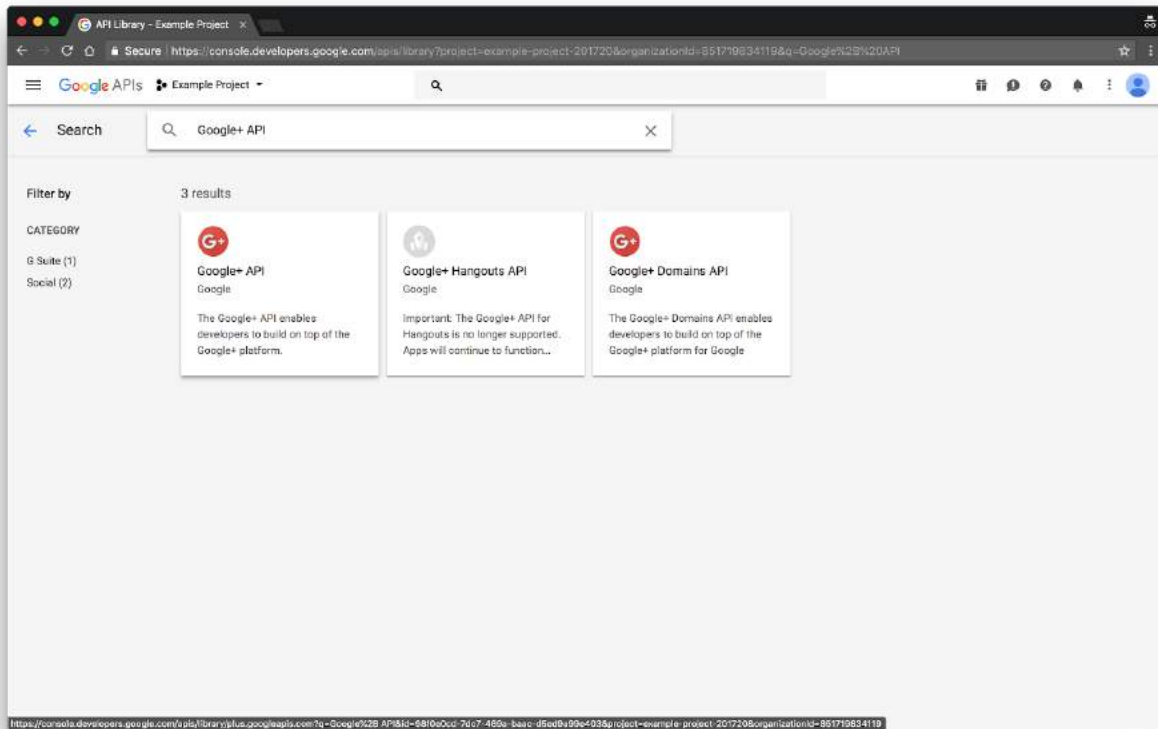
Click **Enable** on the **Admin SDK** page to enable the Admin SDK API.



After clicking the **Enable** button wait for few seconds until the page is updated and the Admin SDK API is enabled.

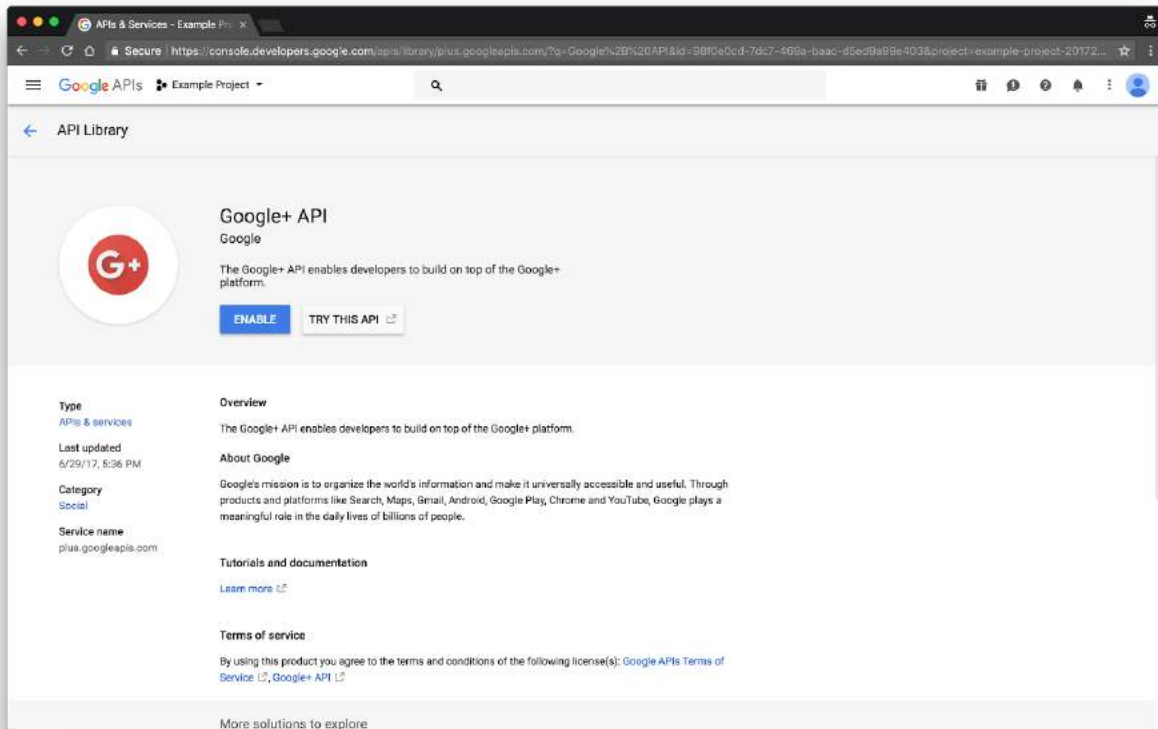


Go back to the [API Library](https://console.developers.google.com/apis/library)⁷ and search for “**Google+ API**” in the APIs and Services search bar. Click on the **Google+ API** card.

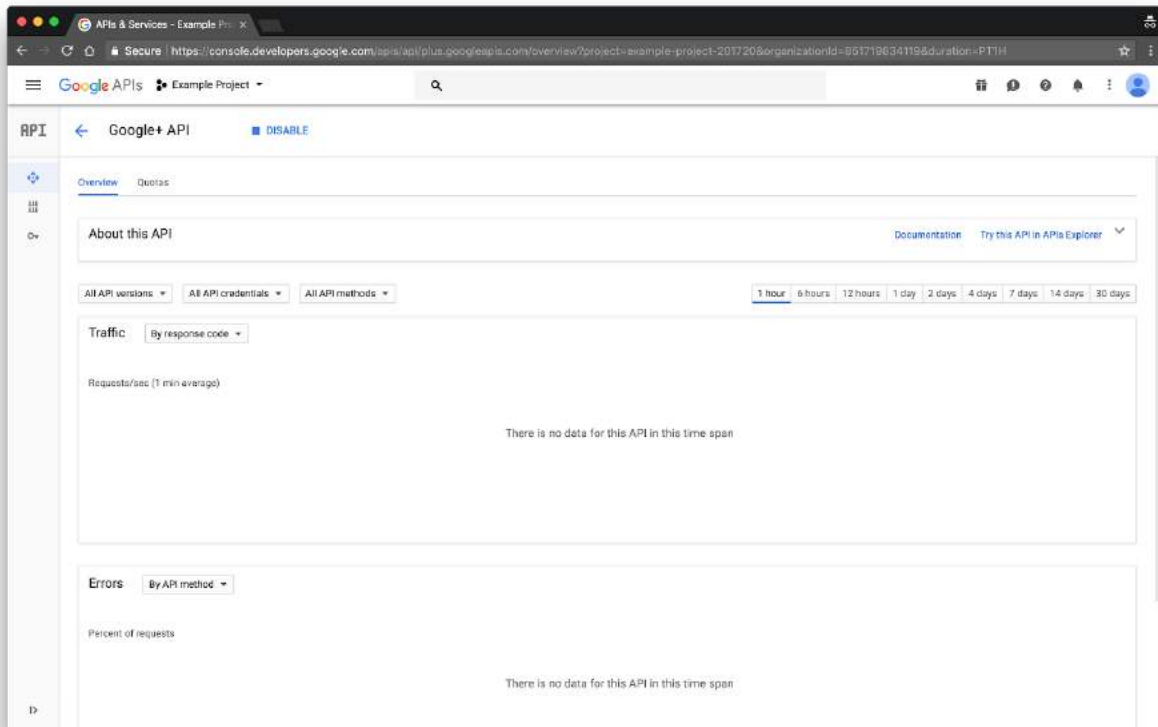


⁷ API Library - <https://console.developers.google.com/apis/library>

Click **Enable** on the Google+ API page.



After enabling the Google+ API, wait for a few seconds for the API to be enabled and the screen changes similar to the image below.



Credentials

From the previous steps, the following items are required to add the adapter to Bridge:

- Client ID
- Client Secret
- Service Account JSON file

You will also need the following:

- **Domain:** Google G Suite verified domain name used for issuing accounts. If your user's sign-in email address is represented as **username@exampledomain.com**, then the Domain is **exampledomain.com**
- **Domain Administrator Email:** Email of the user that has administrative access. If the user with email address as **administrator@exampledomain.com** has administrative access on **exampledomain.com**, then the Domain Administrator Email would be **administrator@exampledomain.com**

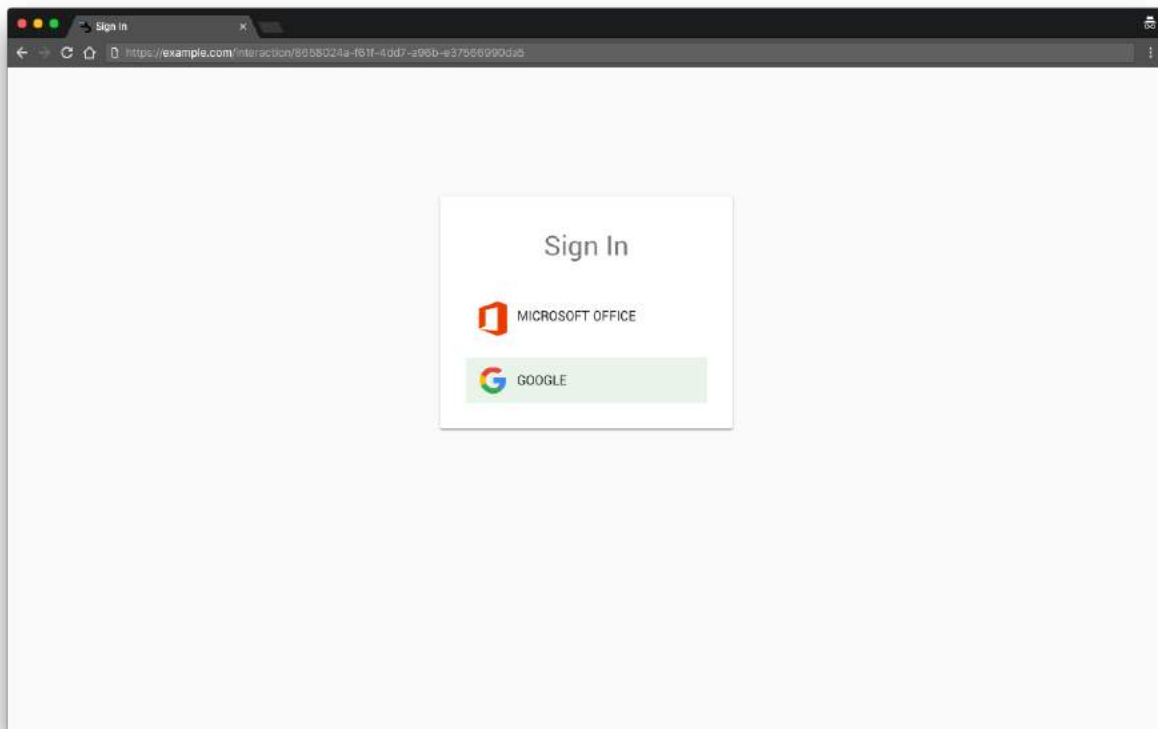
Click on Google icon on **Add Adapter** page, Enter the credentials and click on the **NEXT** button to authenticate with Google.

The screenshot shows the 'Adapter Setup' page in a web browser. The page has a sidebar with 'Adapters', 'Clients', and 'Admins' sections. The main content area is titled 'Google' and contains instructions for retrieving credentials from the Google Developer Console. It also includes a form to enter the following details:

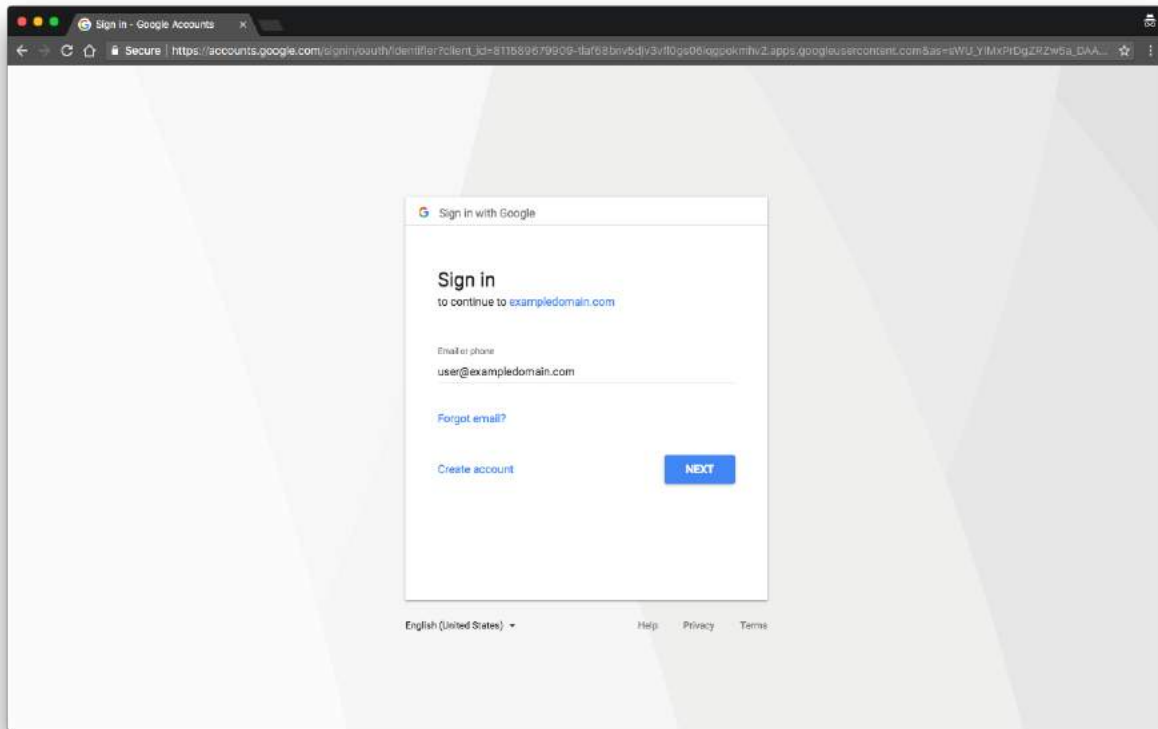
- Name: Google
- Client ID: 891638782345-8qer05tl0f3m9a9e2fhcd5tv1j9ok.apps.googleusercontent.com
- Client Secret: A/wBmM9CwpGCIUTZutfwui8D
- Domain: exampledomain.com
- Domain Admin Email: johndoe@exampledomain.com
- Service Account File: Example Project-135e768ad358.json

At the bottom right of the form, there are 'BACK' and 'NEXT' buttons. The 'NEXT' button is highlighted in blue. A 'Logout' button is located in the bottom left corner of the sidebar.

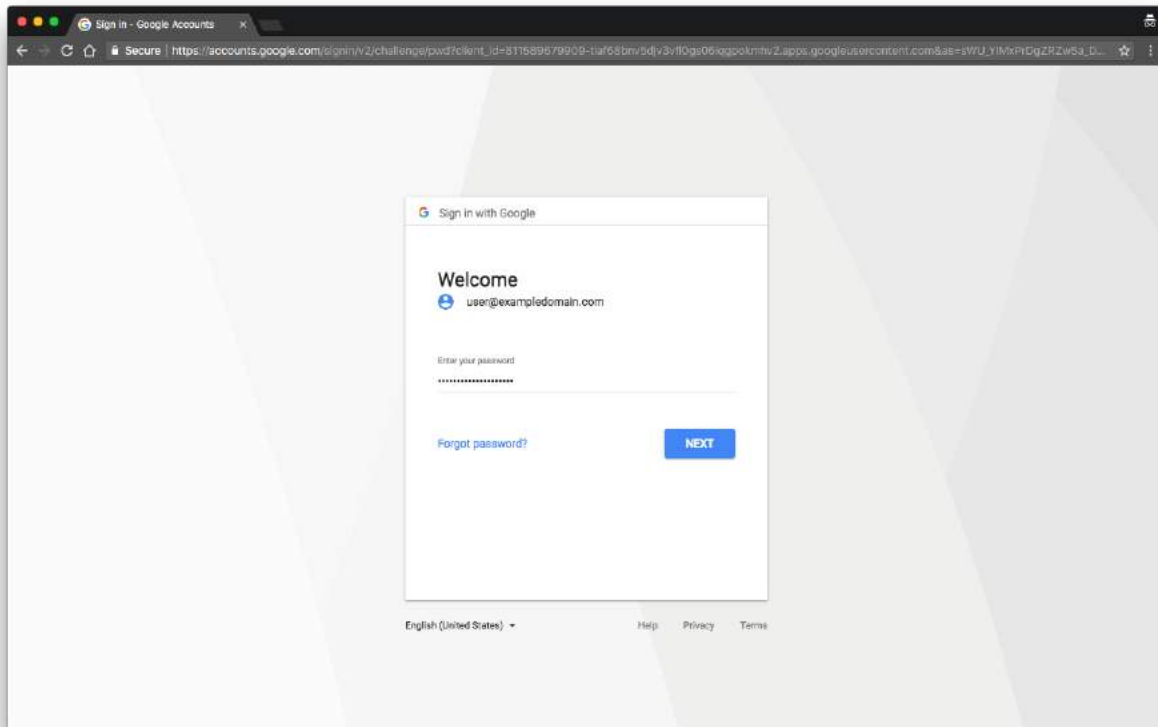
Click the **Adapter Name** entered in the previous step (in this example, **Google**) to authenticate with Google.



Enter the Google G Suite domain email address and click **Next** to login.



Enter the **Password** and click **Next** to login to Google. Press **Accept** to allow Bridge to access your profile information.



After successfully signing in with Google, the page is redirected to the Adapters page that now includes Google adapter that was just created.

Active Directory

Preparations

Setting up Active Directory adapter on Bridge requires an Active Directory account with administrative privileges.

Configuration

The following items are required to setup an Active Directory adapter on Bridge:

- LDAP URL
- BaseDN
- Username
- Password

LDAP URL

LDAP URL is the domain prefixed with **ldap://** that resolves to the Active Directory server.

For example, if **example.com** is set to resolve to Active Directory server then LDAP URL would be **ldap://example.com**

BaseDN

BaseDN can be obtained by running the following command on the Powershell within the Windows machine that is part of the Active Directory network,

Command

```
dsquery user -name $env:UserName
```

Result

```
CN=Username,CN=Users,DC=example,DC=com
```

The BaseDN can be extracted from the above result. From the previous result it would be **DC=example,DC=com**

Credentials

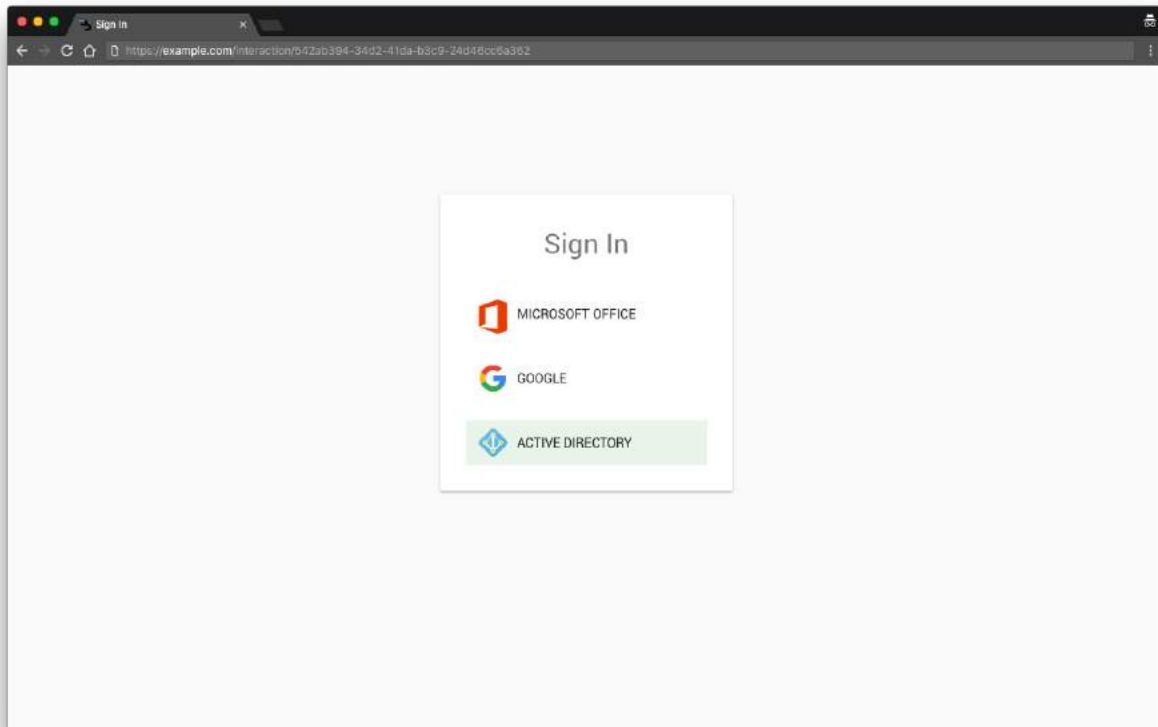
Active Directory adapter requires a user or system account with the following features:

- Non-rotating static password
- Permissions to access users and groups with in the Active Directory network
- Without any query or rate limitations

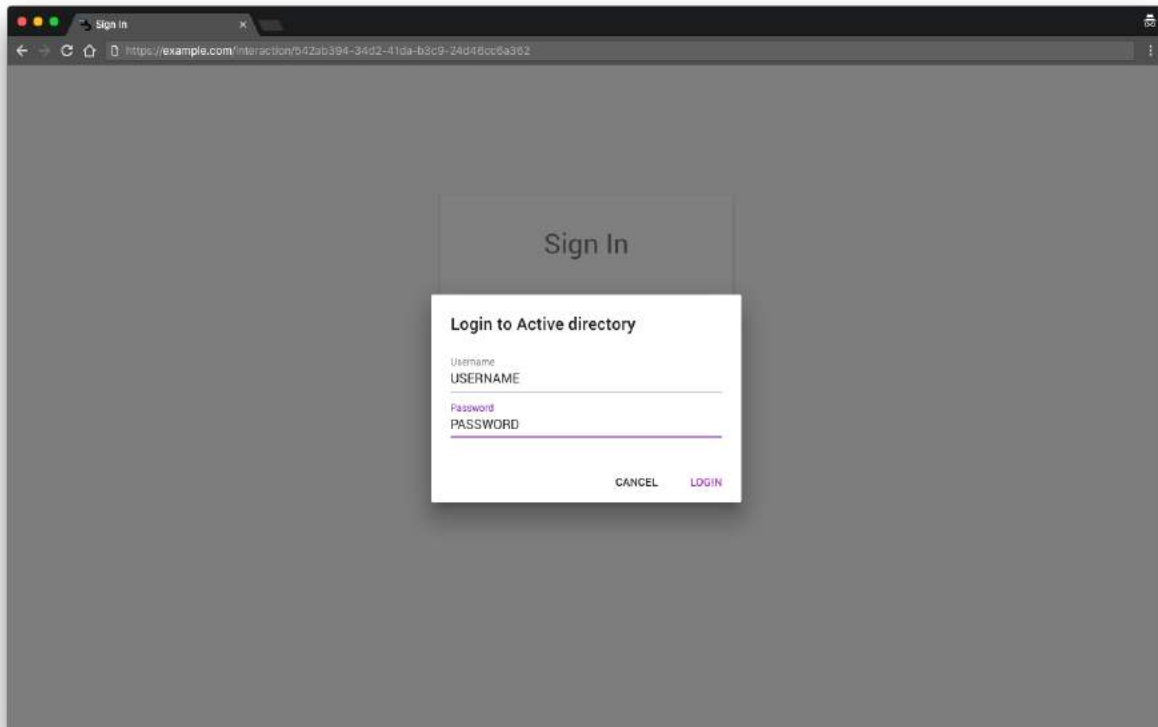
Click on Active Directory icon on **Add Adapter** page, Enter the credentials into the form and click **Next** to authenticate with Active Directory.

The screenshot shows the 'Adapter Setup' page in a web browser. The browser's address bar shows the URL 'https://example.com/bridge/admin/adapters/setup'. The page has a sidebar on the left with the 'BRIDGE' logo and a 'demo' dropdown menu. The sidebar contains three main sections: 'Adapters' (with a grid icon), 'Clients' (with a briefcase icon), and 'Admins' (with a group of people icon). At the bottom of the sidebar is a 'Logout' button with a power icon. The main content area is titled 'demo' and features a progress bar at the top with three steps: 'Select an adapter' (completed with a checkmark), 'Enter credentials' (active with a blue circle), and 'Authorize Application' (disabled with a grey circle). Below the progress bar, the 'Active Directory' adapter is selected. The configuration form includes the following fields: 'Name' (pre-filled with 'Active Directory'), 'URL' (pre-filled with 'ldap://example.com'), 'Base DN' (pre-filled with 'DC=example,DC=com'), 'Username' (pre-filled with 'USERNAME'), and 'Password' (pre-filled with 'PASSWORD'). At the bottom right of the form are 'BACK' and 'NEXT' buttons.

Click **Adapter Name** entered in the previous step (in this example, **Active Directory**) to authenticate with Active Directory.



Enter the **Username** and **Password** from the Active Directory adapter setup page and click **LOGIN** to login to the Active Directory server.



Gigya

Preparations

Setting up Gigya adapter on Bridge requires a Gigya account with administrative privileges.

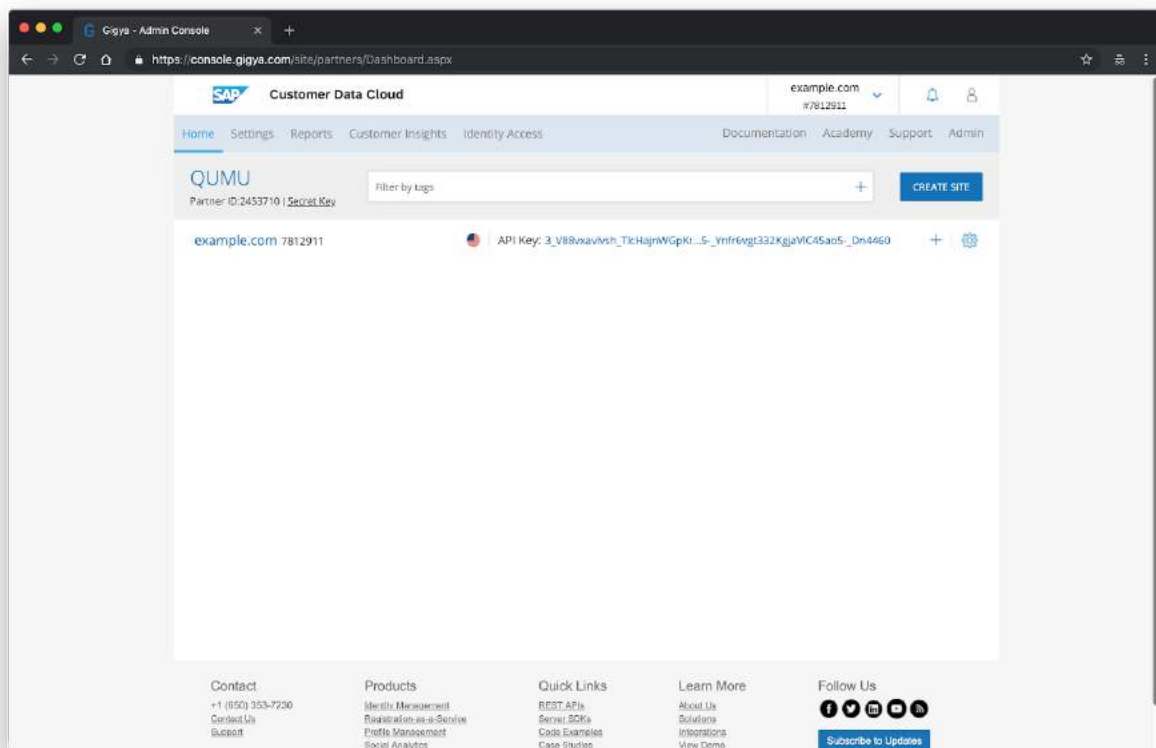
Setup the site

Data Center

Note the datacenter of the site based on the flag. See [Finding your Data Center](https://developers.gigya.com/display/GD/Finding+Your+Data+Center)⁸ for more information.

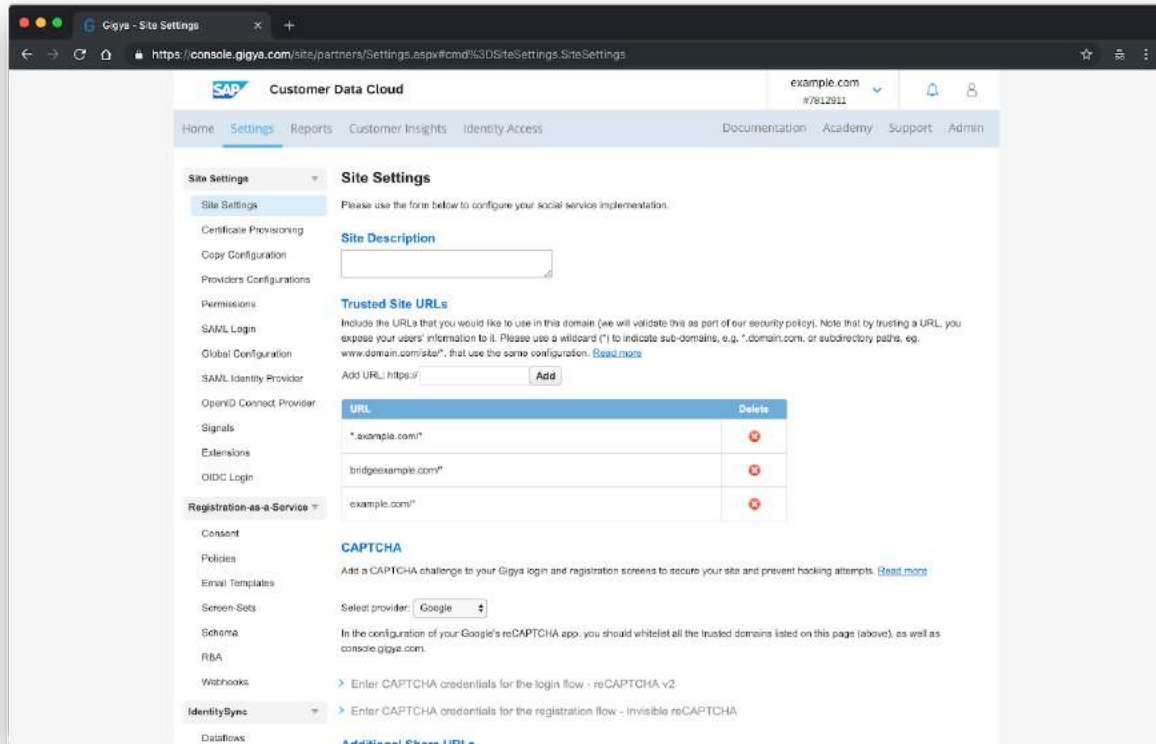
API Key

Make a note of the **API Key** since it's required to configure Gigya adapter on Bridge.



⁸ Finding your Data Center - <https://developers.gigya.com/display/GD/Finding+Your+Data+Center>

Open Site Settings page and add the Bridge domain name to the trusted site urls, this enables Gigya to share the user information with Bridge.



Setup OpenID Connect

Proxy Page URL

Open the OpenID Connect Provider on the settings page and setup the proxy page. If the proxy page is configured then proceed with the next step.

Bridge provides the proxy page functionality, in-order to use it configure the proxy page uri with the Bridge domain name followed by **/auth/adapter/gigya/proxy** path. For example, if the Bridge domain name is **bridge.example.com** the proxy page url would be

`https://bridge.example.com/auth/adapter/gigya/proxy`

Issuer

Issuer is the name of the site that issues the identity tokens to Bridge, configure the site name as the issuer. For example, If the site name is **example.com** then the issuer would be **https://example.com**.

Custom Claims

Custom claims map the user information properties to defined keys and are returned after the user is logged in. Configure the following custom claims to include profile and user Id during the initial sign in request.

- **UID**
Enter the claim name as **UID** and the mapped field as **UID**
- **profile**
Enter the claim name as **profile** and the mapped field as **profile**

Scopes

Scopes are utilized during the sign in request to include the user information along with the request. Configure the following scopes to allow Bridge to access user information such as User ID (uid) and profile.

- **UID**
Enter the scope name as **uid** and the mapped claim as **UID**
- **profile**
Enter the scope name as **profile** and the mapped claim as **profile**

Click **Save** to save the OpenID connect settings.

The screenshot shows the SAP Customer Data Cloud console interface. The browser address bar indicates the URL: `https://console.gigya.com/site/partners/Settings.aspx#/oidc-provider-app`. The page title is "Customer Data Cloud". The left sidebar contains a navigation menu with categories: "Site Settings", "Registration-as-a-Service", and "IdentitySync". The "OpenID Connect Provider" option is selected under "Site Settings".

The main content area is titled "OPENID CONNECT PROVIDER" and includes a "Developer's Guide" link. It is divided into three sections:

- Configure OP Settings**: Contains input fields for "Proxy Page URL" (with value `https://bridge.example.com/auth/adapter/gigya/proxy`) and "Issuer" (with value `https://bridge.example.com`).
- Custom Claims**: A table with columns "CLAIM NAME" and "MAPPED FIELD". It contains two rows:

CLAIM NAME	MAPPED FIELD
UID	UID
profile	profile
- Scopes**: A table with columns "SCOPE NAME" and "MAPPED CLAIMS". It contains two rows:

SCOPE NAME	MAPPED CLAIMS
uid	UID
profile	profile

At the bottom right of the main content area, there are "CANCEL" and "SAVE" buttons. The "SAVE" button is highlighted in blue.

Create Relay Party (RP) Client

Click on **Create RP** button on the OpenID Connect Provider page and enter the following information

Client ID

Client ID is auto-generated after saving the RP client. Make a note of it since it's required while setting up the adapter on Bridge.

Client Secret

Client Secret is auto-generated after saving the RP client. Make a note of it since it's required while setting up the adapter on Bridge.

Description

Enter the description of the client

Supported Response Type

Check the following boxes

1. **token**
2. **id_token**
3. **code**

Subject Identifier Type

Toggle **Auto-generated per RP (Pairwise)** option

Access Token Lifetime

Set the access token lifetime based on the organizational guidelines.

Redirect URIs

Setup the Bridge redirect uri's, for example, if the Bridge is setup on **bridge.example.com** then the redirect URIs would be the following

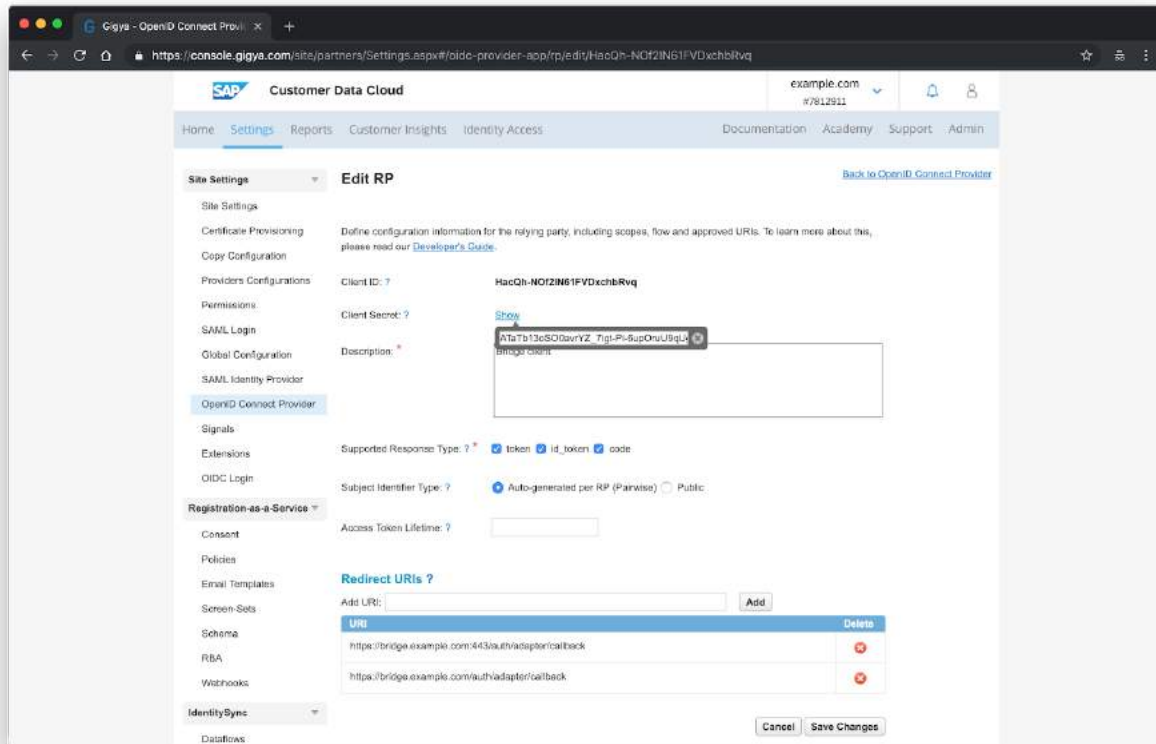
1. `https://bridge.example.com:443/auth/adapter/callback`
2. `https://bridge.example.com/auth/adapter/callback`

Click Create to create the RP Client.

The screenshot shows the SAP Customer Data Cloud console interface. The browser address bar indicates the URL: `https://console.gigya.com/site/partners/Settings.aspx#/oidc-provider-app/rp/create`. The page title is "Customer Data Cloud". The left sidebar contains a navigation menu with categories like "Site Settings", "Registration-as-a-Service", and "IdentitySync". The main content area is titled "Create RP" and includes a "Back to OpenID Connect Provider" link. The form contains several sections: "Site Settings" with a description and a "Developer's Guide" link; "Providers Configurations" with fields for "Client ID" and "Client Secret" (both auto-generated); a "Description" text area; "Supported Response Type" with checkboxes for "token", "id_token", and "code" (all checked); "Subject Identifier Type" with radio buttons for "Autogenerated per RP (Parwise)" (selected) and "Public"; "Access Token Lifetime" field; "Redirect URIs" section with an "Add URI" button and a table of existing URIs; and "Cancel" and "Create" buttons at the bottom right.

URI	Delete
<code>https://bridge.example.com/443/oauth2/implicit/callback</code>	
<code>https://bridge.example.com/oauth2/implicit/callback</code>	

After the successful creation of the RP client, the page is redirected to OpenID Connect Provider. Click on the newly created RP client that matches the description entered in the previous step.



Make a note of the **Client ID** and **Client Secret** since they are required during the adapter setup step.

Screen Set

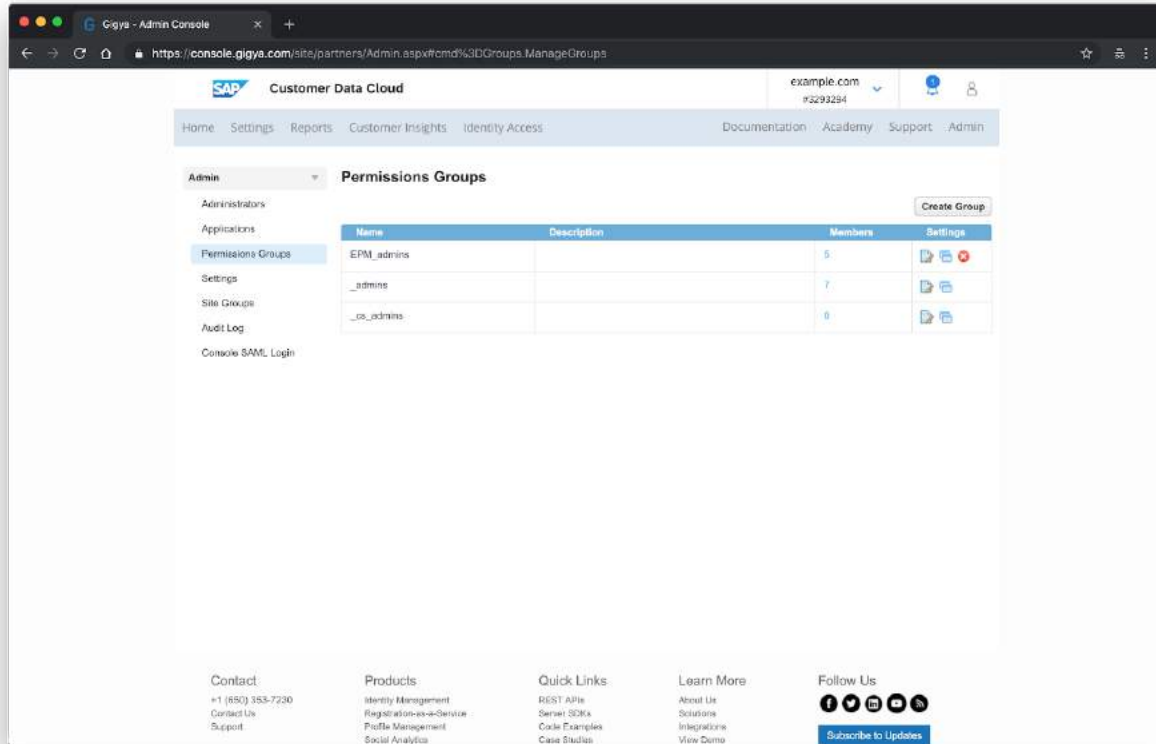
Open the Screen-Sets under Registration-as-a-Service section on the Settings page. Make a note of the **ID** of the screenset. It is required to setup the Gigya adapter on Bridge.

The screenshot shows the Gigya Customer Data Cloud console interface. The browser address bar displays `https://console.gigya.com/site/partners/Settings.aspx#/screen-sets-app/dashboard`. The page title is "Screen-Sets". On the right, a "Registration Conv. Rate" of 40% is shown. Below this, a text block explains that the default screen-set collection is provided out-of-the-box for various user flows like login/registration and user profile management, and offers a link to "Learn more here". A table lists the default screen-sets with columns for ID, Description, Last Modified, and Actions. The table contains five entries: DefaultLinkAccounts, DefaultLinkRegistration, DefaultProfileUpdate, DefaultReAuthentication, and DefaultRegistrationLogs. Each entry has a "U.S. Builder" button and icons for edit, delete, and share. On the left sidebar, the "Registration-as-a-Service" section is expanded, and "Screen-Sets" is selected. Other options in the sidebar include Site Settings, Certificate Provisioning, Copy Configuration, Providers Configurations, Permissions, SAML Login, Global Configuration, SAML Identity Provider, OpenID Connect Provider, Signals, Extensions, and OIDC Login. Under "Registration-as-a-Service", there are links for Consent, Policies, Email Templates, Screen-Sets (highlighted), Schema, RBA, Webhooks, and Identity Sync. At the bottom of the sidebar, there is a link for Dataflows.

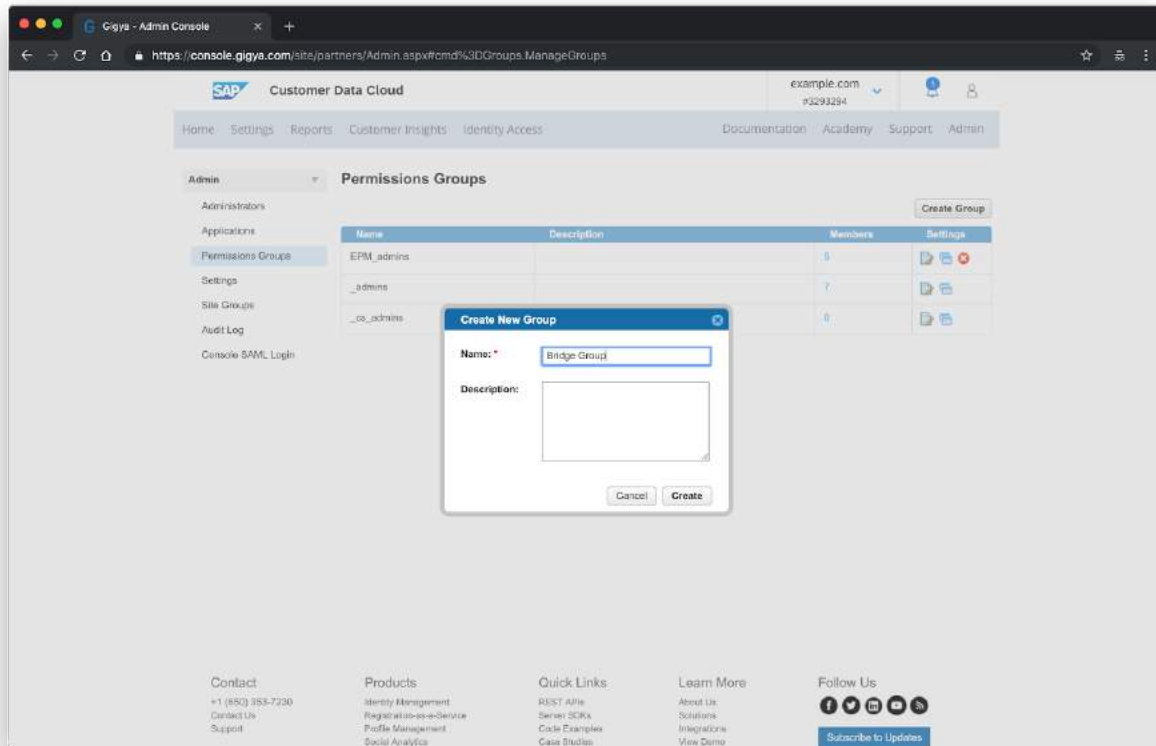
ID	Description	Last Modified	Actions
DefaultLinkAccounts		Nov 19, 2018, 11:31:16	U.S. Builder [Edit] [Delete] [Share]
DefaultLinkRegistration		Nov 19, 2018, 11:31:16	U.S. Builder [Edit] [Delete] [Share]
DefaultProfileUpdate		Nov 19, 2018, 11:31:17	U.S. Builder [Edit] [Delete] [Share]
DefaultReAuthentication		Nov 19, 2018, 11:31:16	U.S. Builder [Edit] [Delete] [Share]
DefaultRegistrationLogs		Nov 19, 2018, 11:31:16	U.S. Builder [Edit] [Delete] [Share]

Permission Groups

Open the Permission Groups page by clicking on the **Admin** and **Permission Groups** under Admin.

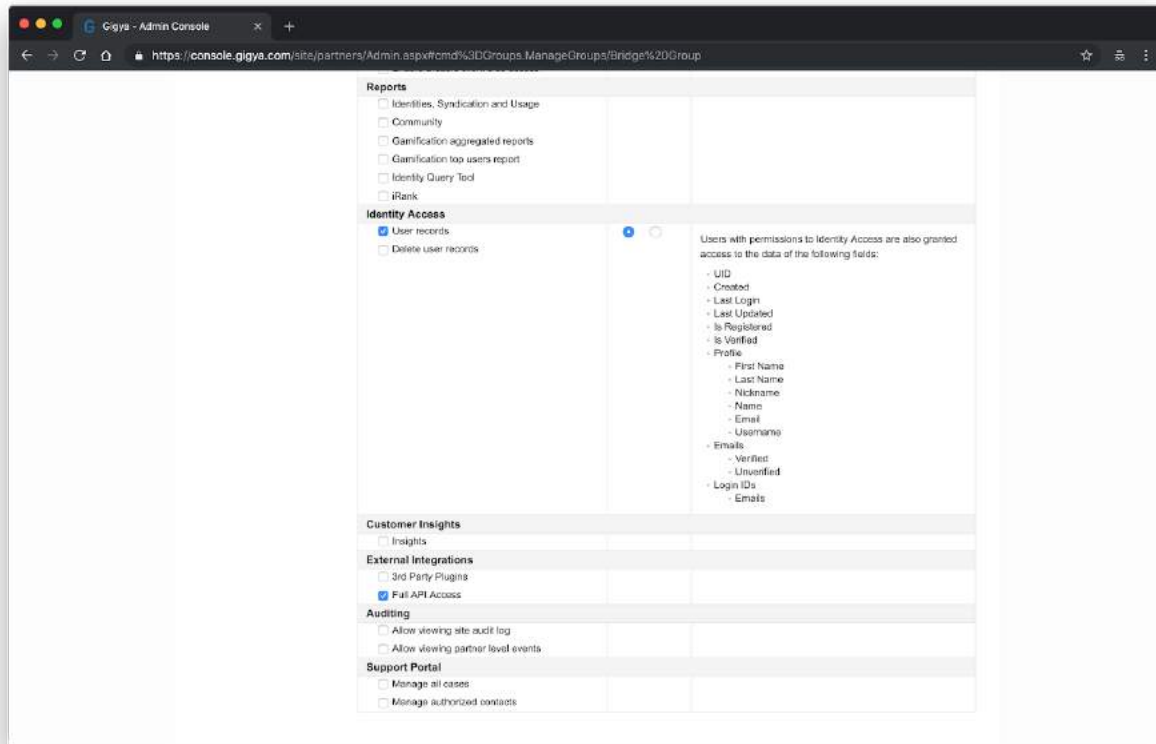


Click on **Create New Group** and click on **Create** after entering the name and description of the group.



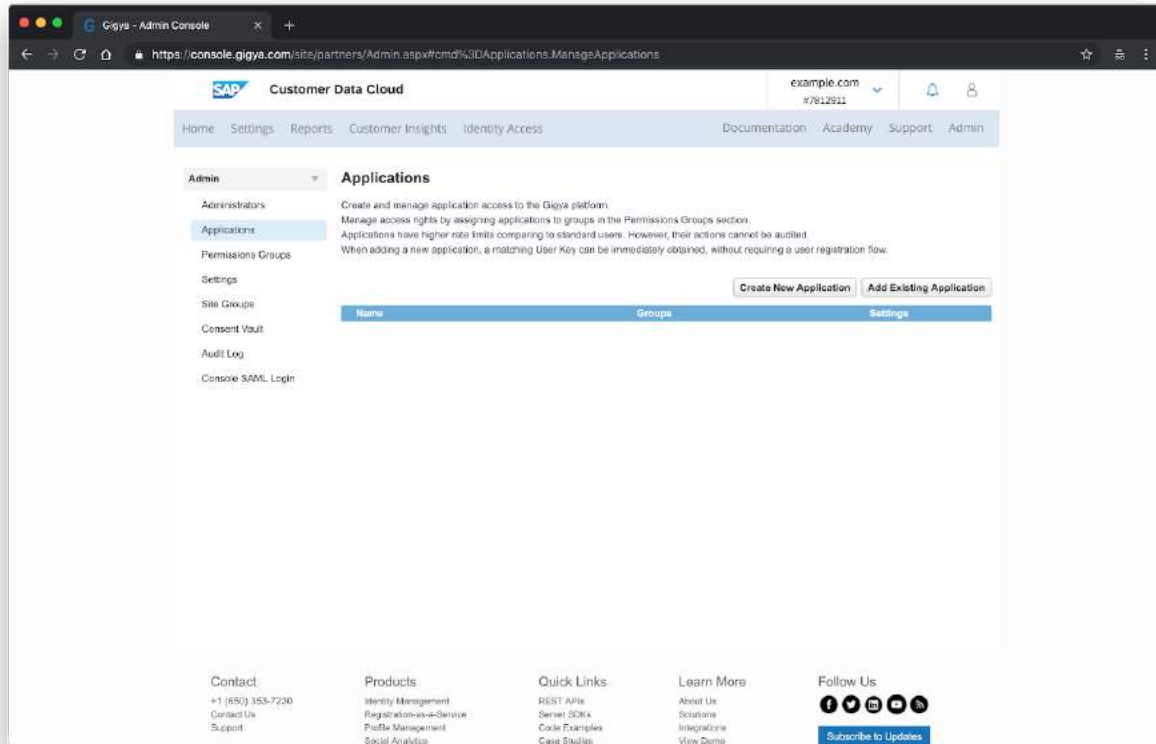
Click on the **edit** icon of the newly created permission group and enable the following on Privileges page.

- **Full API Access** under External Integrations
- **User Records** with **View** access under Identity Access

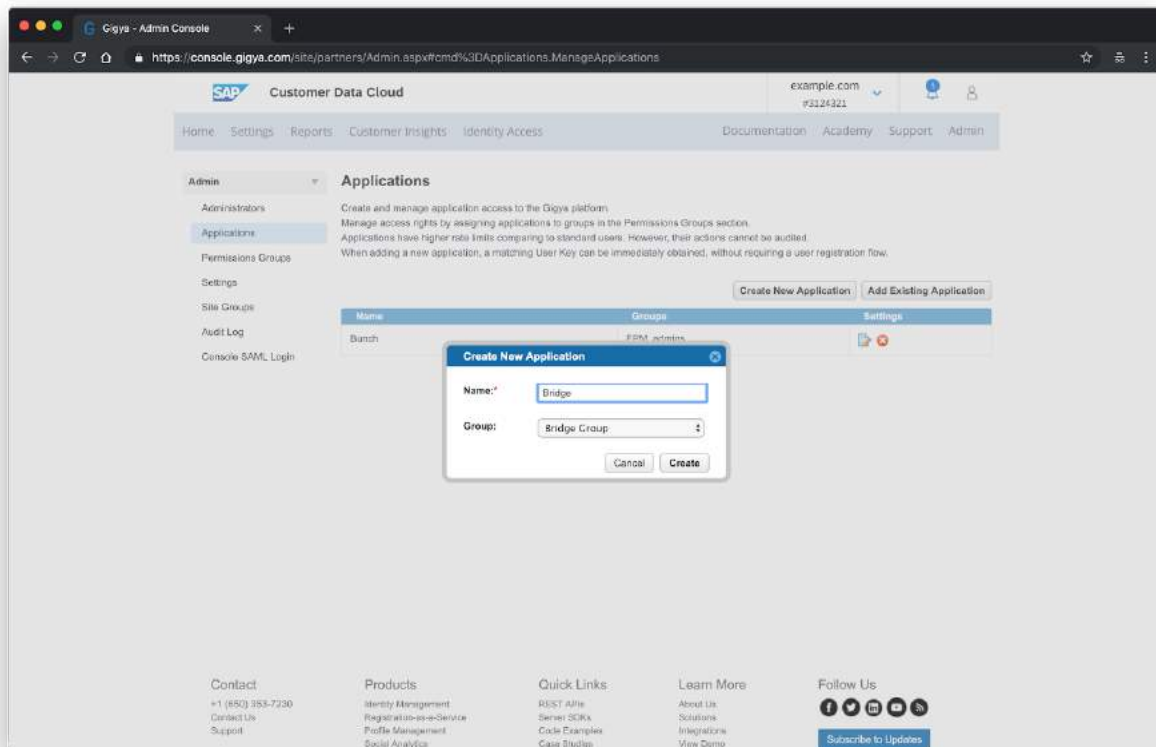


Application

Open the Applications page by clicking on the **Admin** and **Applications** under Admin.

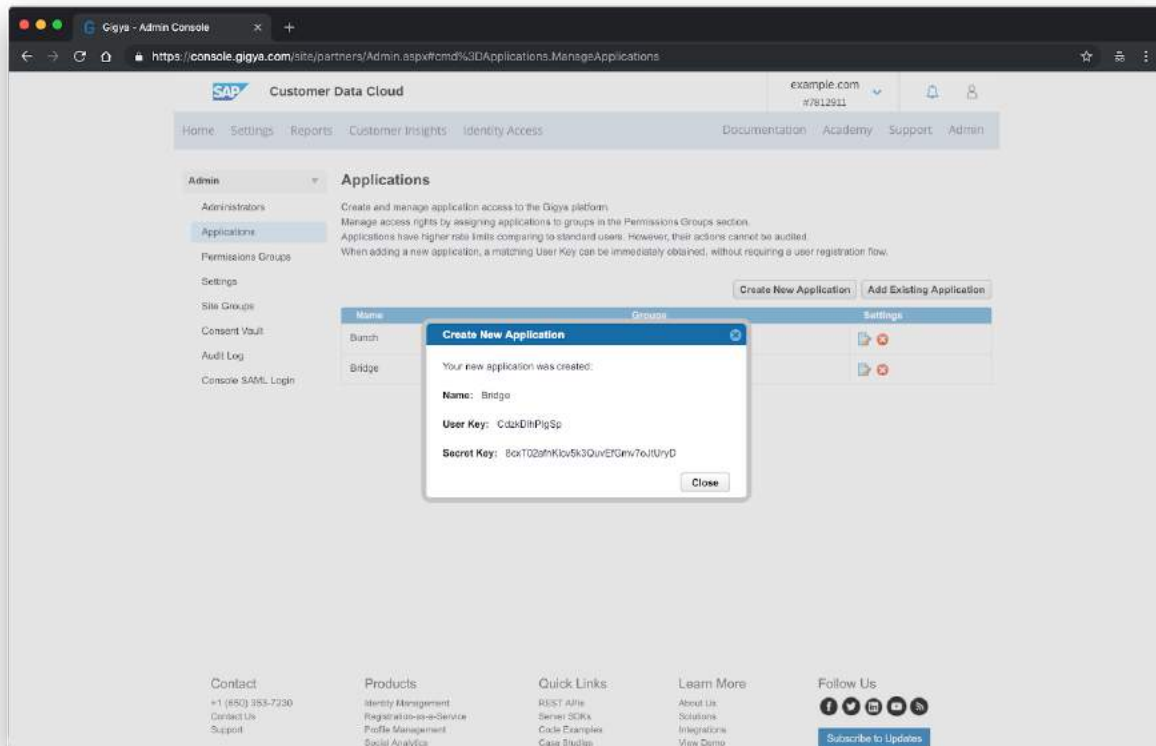


Click on **Create New Application**. Enter the name of the application and assign the group that was created in the previous step.



Copy the **User key** and **Secret key** from the dialog that appears after successful creation of the Application.

Make a note of the User key and Secret Key as they are required to add the Gigya adapter to Bridge.



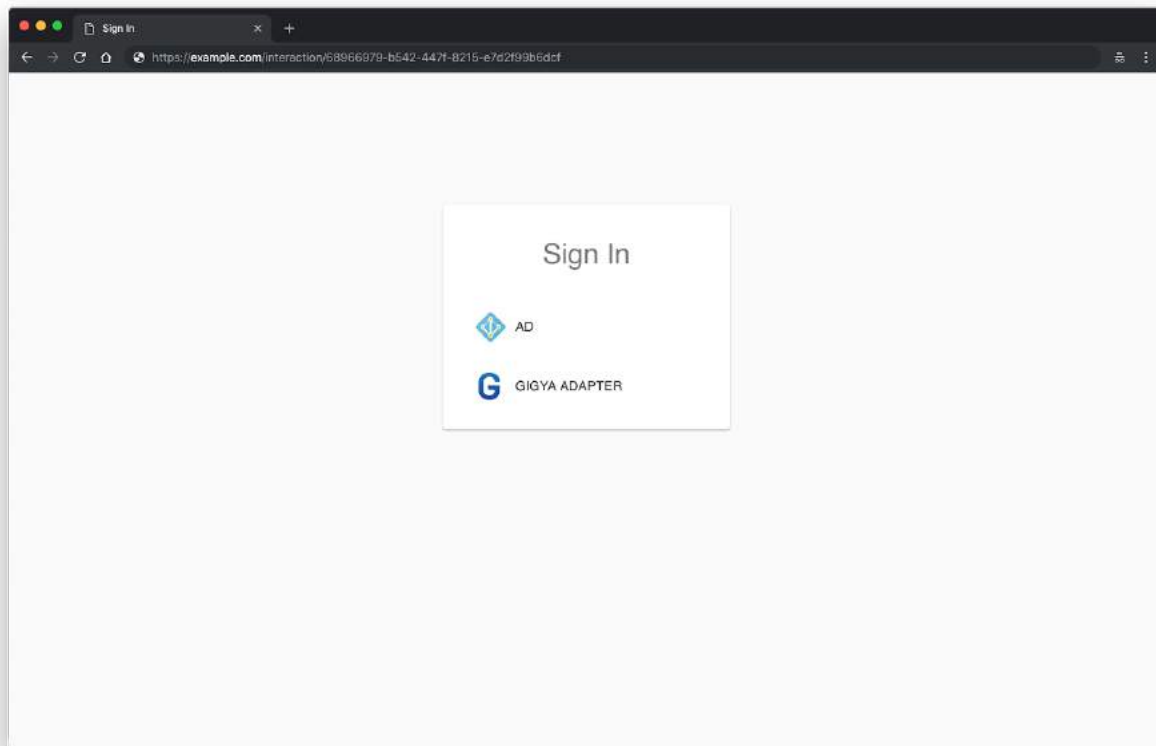
Click on Gigya icon on **Add Adapter** page, Enter the credentials into the Gigya adapter form and click **NEXT** to login to Gigya.

The screenshot shows the Bridge Admin interface for adding a new adapter. The browser address bar shows the URL `https://example.com/bridge/admin/adapters/setup`. The interface has a sidebar with 'Adapters', 'Clients', and 'Admins' sections. The main content area is titled 'Gigya' and includes instructions: 'To retrieve the appropriate credentials, login to Gigya and locate the following credentials.' The form contains the following fields:

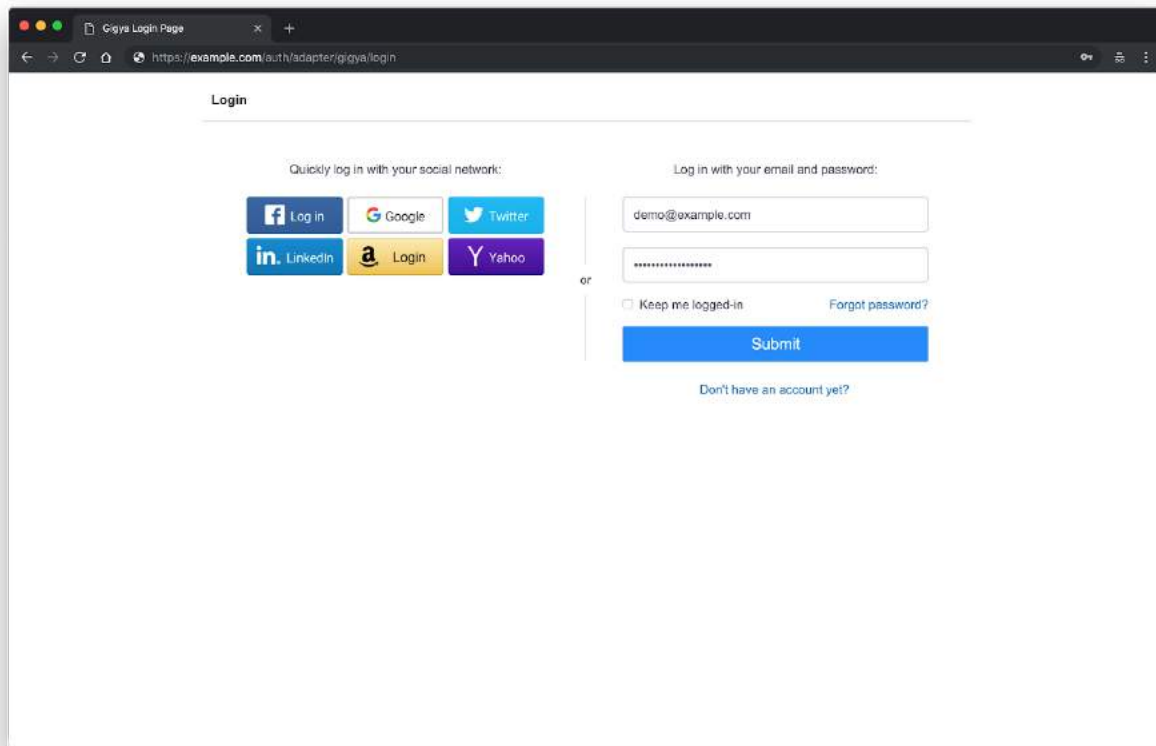
- Name: Gigya Adapter
- Gigya User Key: Example User key
- Gigya Secret Key: Example Secret Key
- Gigya API Key: Example API Key
- Datacenter: us1 (dropdown menu)
- Client ID: Example Client ID
- Client Secret: Example Client Secret
- Screen Set: Default-RegistrationLogin

At the bottom right of the form, there are 'BACK' and 'NEXT' buttons. The top of the form has three steps: 'Select an adapter' (completed), 'Enter credentials' (current step), and 'Authorize Application'.

Click on the adapter name entered in the previous step (**Gigya Adapter**) to proceed further with the login.



Enter the Gigya account credentials on the login page and click on **Submit** to login to Gigya.



The screenshot shows a web browser window titled "Gigya Login Page" with the URL "https://example.com/auth/adapter/gigya/login". The page has a "Login" header. Below the header, there are two main login sections separated by a vertical line and the word "or".

Left Section: Quickly log in with your social network:

- Buttons for: Facebook Log in, Google, Twitter, LinkedIn, Amazon Login, and Yahoo.

Right Section: Log in with your email and password:

- Email input field containing "demo@example.com".
- Password input field with masked characters "*****".
- Checkboxes for "Keep me logged-in" and a link for "Forgot password?".
- A blue "Submit" button.
- A link at the bottom: "Don't have an account yet?".

Okta

Preparations

Setting up an Okta adapter on Bridge requires an Okta account with administrative privilege and OAuth 2.0 for Okta APIs feature enabled.

To enable **OAuth 2.0 for Okta APIs**⁹ feature, submit a support ticket to Okta.

Configuration

The following items are required to setup an Okta adapter on Bridge:

- Okta Organization URL
- Service Account Username
- Service Account Password
- OpenID Connect Client Id
- OpenID Connect Client Secret

Okta URL

Okta domain can be viewed on Okta developer console, See [Find your Okta domain](#)¹⁰ page.

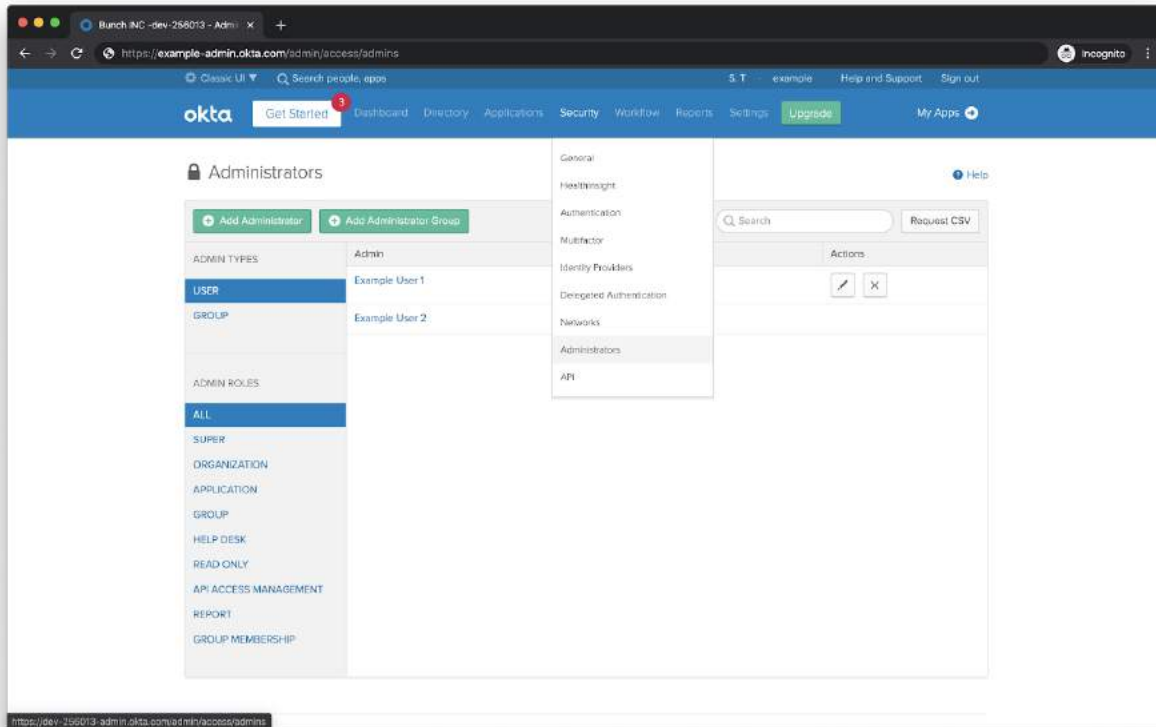
For example, if Okta domain is **example.okta.com** then the Okta URL would be **https://example.okta.com**.

⁹ <https://support.okta.com/help/s/productroadmap>

¹⁰ <https://developer.okta.com/docs/guides/find-your-domain/overview/>

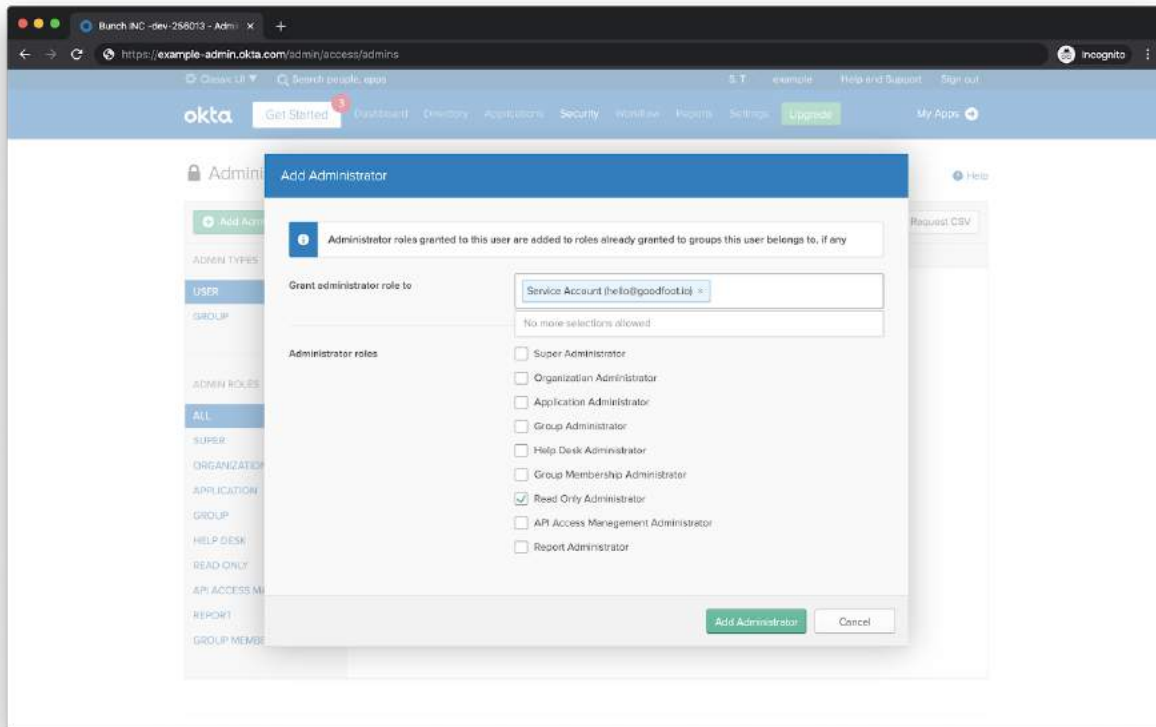
Read-only Service Account

Create a service account on Okta Developer console and assign Read Only Administrator role to it. Click on **Administrators** under **Security** in the navigational menu and click on the **Add Administrator** button.



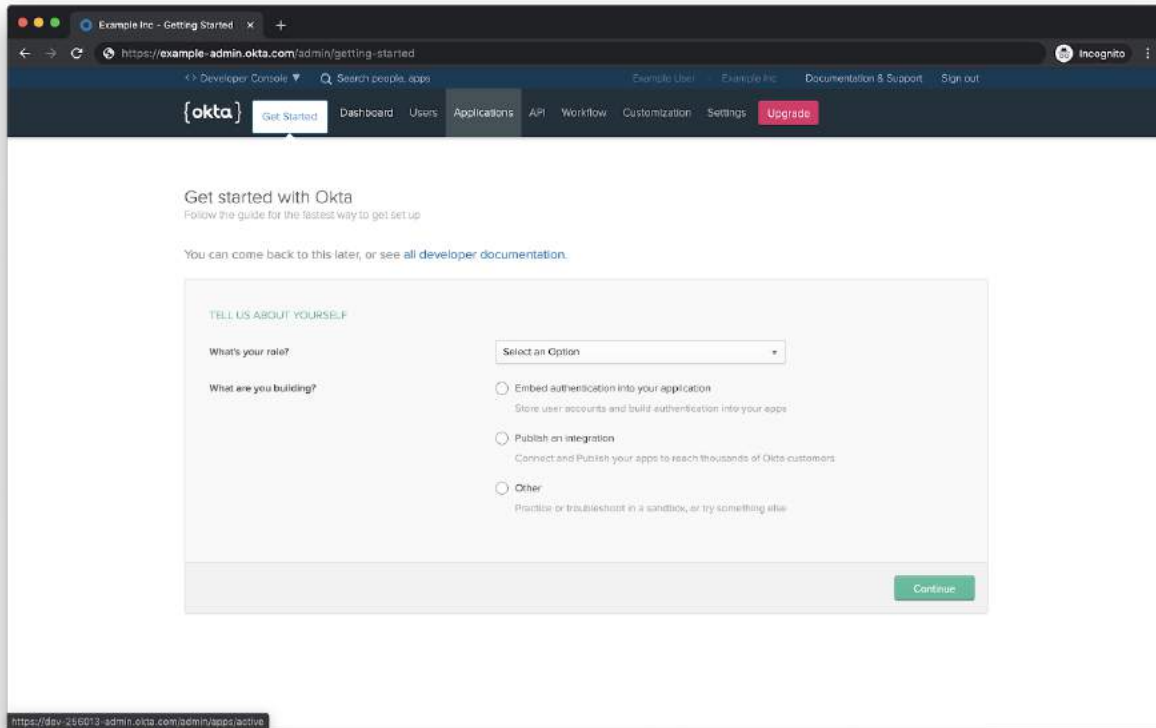
Type the Service Account name in the text area right of **Grant administrator role to** and select the account.

Click on the **Read Only Administrator** checkbox and click on the **Add Administrator** button to save the changes.

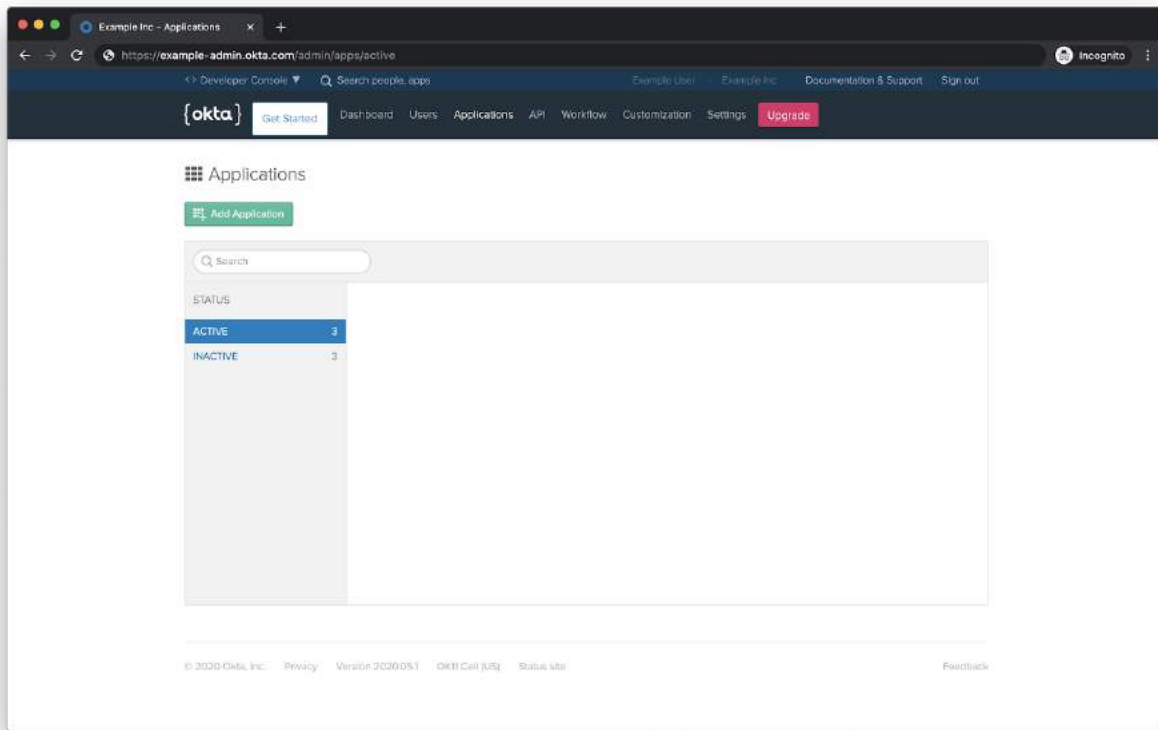


OpenID Connect Application

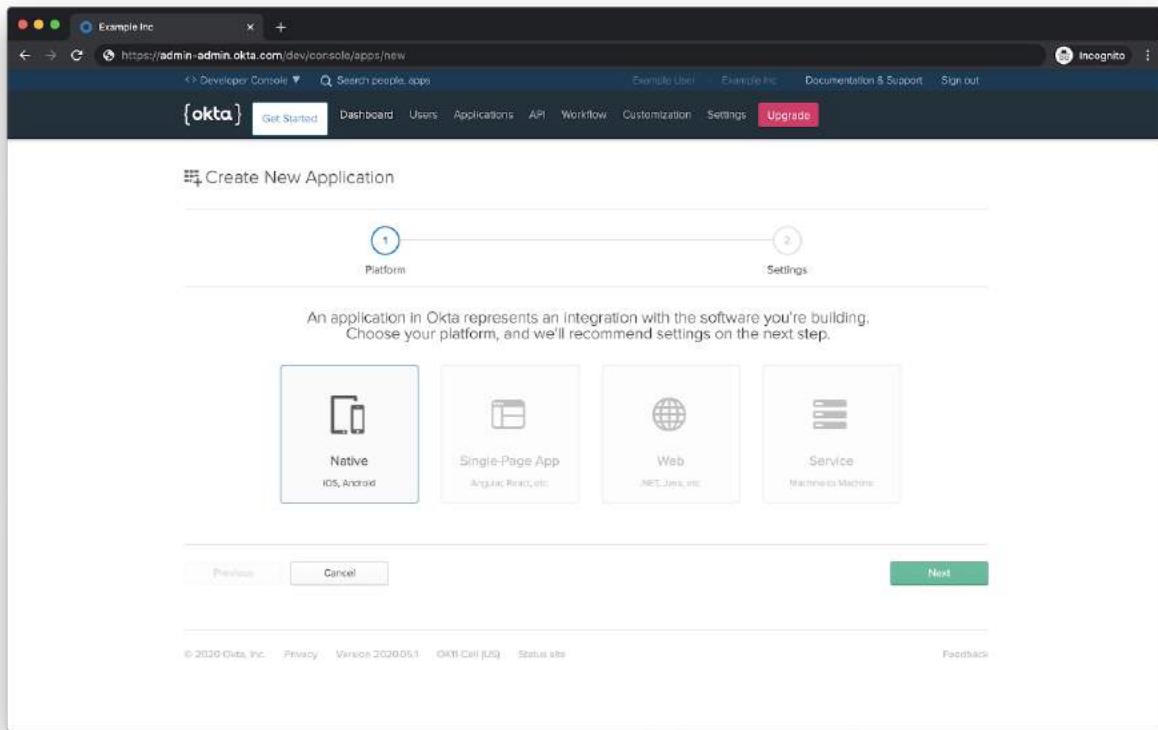
Create an OpenID Connect application on the Okta administrative console. Click on the **Applications** under **Applications** navigation menu.



Click on the **Add Application** button on the Applications page.



Select the **Native** option. Click on the **Next** button on the dialog.



Enter the following details and click on the **Done** button to create the application.

- **Application Name:** Displayed to the user when they sign-in for the first time
- **Login redirect URIs:** List of URLs the user could be redirected to after they login using their Okta credentials. If Bridge is deployed on **example.com**, then the redirect URIs would be,
 - <https://example.com/auth/adapter/callback>
 - <https://example.com:443/auth/adapter/callback>
- **Logout redirect URIs:** List of URLs the user is redirected to after logging out of the session. If Bridge is deployed on **example.com**, then the logout redirect uri would be **<https://example.com>**.
- **Group assignments:** List of Okta groups that are capable of logging in to Bridge using the OpenID connect client.
- **Grant type allowed:** Grant type used for the sign-in flow. Select the following grant types,
 - Authorization Code
 - Resource Owner Password

Click on the **Done** button to create the application.

The screenshot shows the 'New Application' form in the Okta Admin Console. The browser address bar shows 'https://admin-admin.okta.com/dev/console/apps/new'. The form fields are as follows:

- Name:** Example App
- Login redirect URIs:** Two entries: <https://band.example.com/auth/adapter/callback> and <https://band.example.com:443/auth/adapter/callback>. There is an '+ Add URI' button below.
- Logout redirect URIs:** One entry: <https://band.example.com>. There is an '+ Add URI' button below.
- Group assignments:** Optional. A dropdown menu is set to 'Everyone'.
- Grant type allowed:** Under the heading 'Client acting on behalf of a user', the following options are checked: ☒ Authorization Code, ☐ Refresh Token, ☒ Resource Owner Password, and ☐ Implicit (hybrid).

At the bottom of the form are three buttons: 'Previous', 'Cancel', and 'Done'.

Click on the **Edit** button next to General Settings and check **Resource Owner Password** under Allowed grant types and click on the **Save** button.

The screenshot shows the 'General Settings' form for an application in the Okta admin console. The form is divided into two main sections: 'APPLICATION' and 'LOGIN'.

APPLICATION Section:

- Application label:** Example Application
- Application type:** Native
- Allowed grant types:** Client acting on behalf of a user
 - ☒ Authorization Code
 - ☐ Refresh Token
 - ☒ Resource Owner Password
 - ☐ Implicit (Hybrid)

LOGIN Section:

- Login redirect URIs:** Two URIs are listed: `https://example.com/auth/adapter/callback` and `https://example.com/443/auth/adapter/callback`. There is an '+ Add URI' button.
- Logout redirect URIs:** One URI is listed: `https://example.com`. There is an '+ Add URI' button.
- Initiate login URI:** `https://example.com/auth/adapter/callback`

General Settings Summary (Right Side):

All fields are required unless marked optional. Some fields may no longer be editable.

Need provisioning for this app?

Okta doesn't provide user provisioning for this app yet, but it can be added with an on-premises provisioning. Contact your Okta sales representative to enable support. [Learn more](#)

Buttons: 'Cancel' (top right), 'Save' (bottom right), and 'Cancel' (bottom right).

Click on the **Edit** button next to **Client Credentials** and click the **Use Client Authentication** radio option and click on the **Save** button.

The screenshot shows a web browser window with the URL `https://example-admin.okta.com/admin/app/oidc_client/client/00e4xaq9xWuXgW1n4x6#tab-general`. The browser's address bar shows "Incognito". The page displays the "LOGIN" configuration for a client. The "Client Credentials" section is highlighted, showing the "Client ID" as `00e4xaq9xWuXgW1n4x6`. The "Client authentication" section has two radio buttons: "Use PKCE (for public clients)" and "Use Client Authentication". The "Use Client Authentication" option is selected. The "Save" button is highlighted in green.

LOGIN

Login redirect URIs `https://example.com/auth/adaptor/callback`
`https://example.com/443/auth/adaptor/callback`

Logout redirect URIs `https://example.com`

Initiate login URI `https://example.com/auth/adaptor/callback`

Client Credentials Cancel

Client ID `00e4xaq9xWuXgW1n4x6`
Public identifier for the client that is required for all OAuth flows.

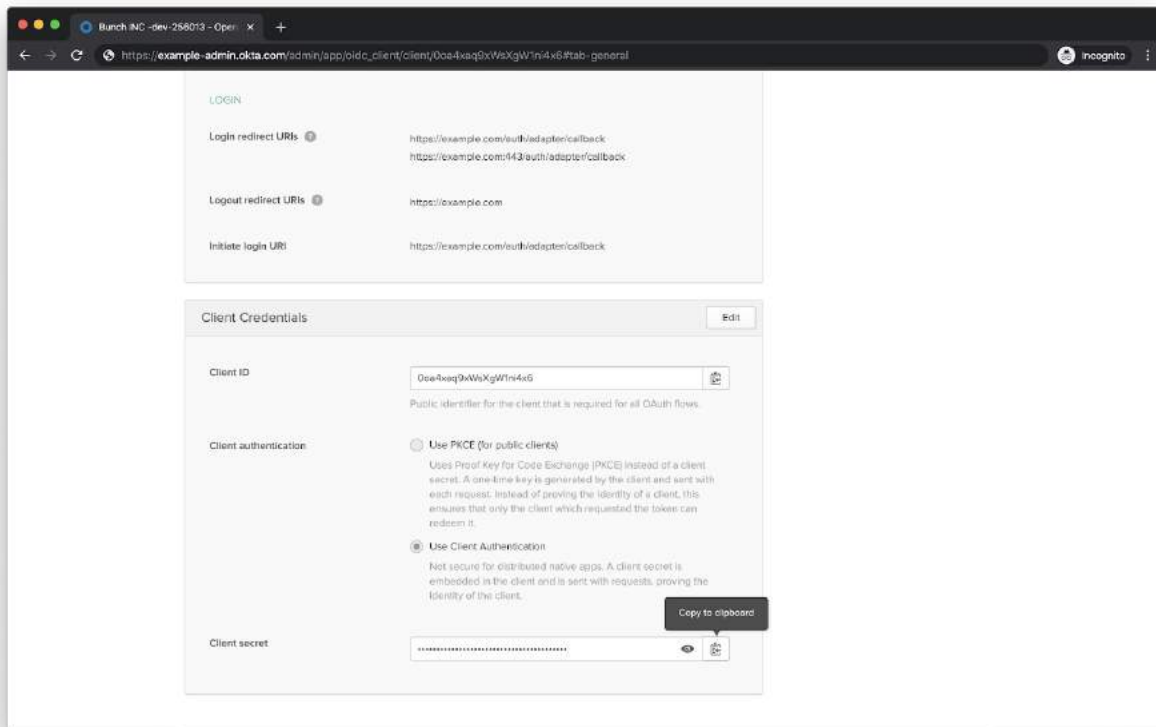
Client authentication

☐ Use PKCE (for public clients)
Uses Proof Key for Code Exchange (PKCE) instead of a client secret. A one-time key is generated by the client and sent with each request. Instead of proving the identity of a client, this ensures that only the client which requested the token can redeem it.

☒ Use Client Authentication
Not secure for distributed native apps. A client secret is embedded in the client and is sent with requests, proving the identity of the client.

Save Cancel

Make a note of the **Client Id** and **Client Secret** under **Client Credentials** at the bottom of the application page we created in the previous step.

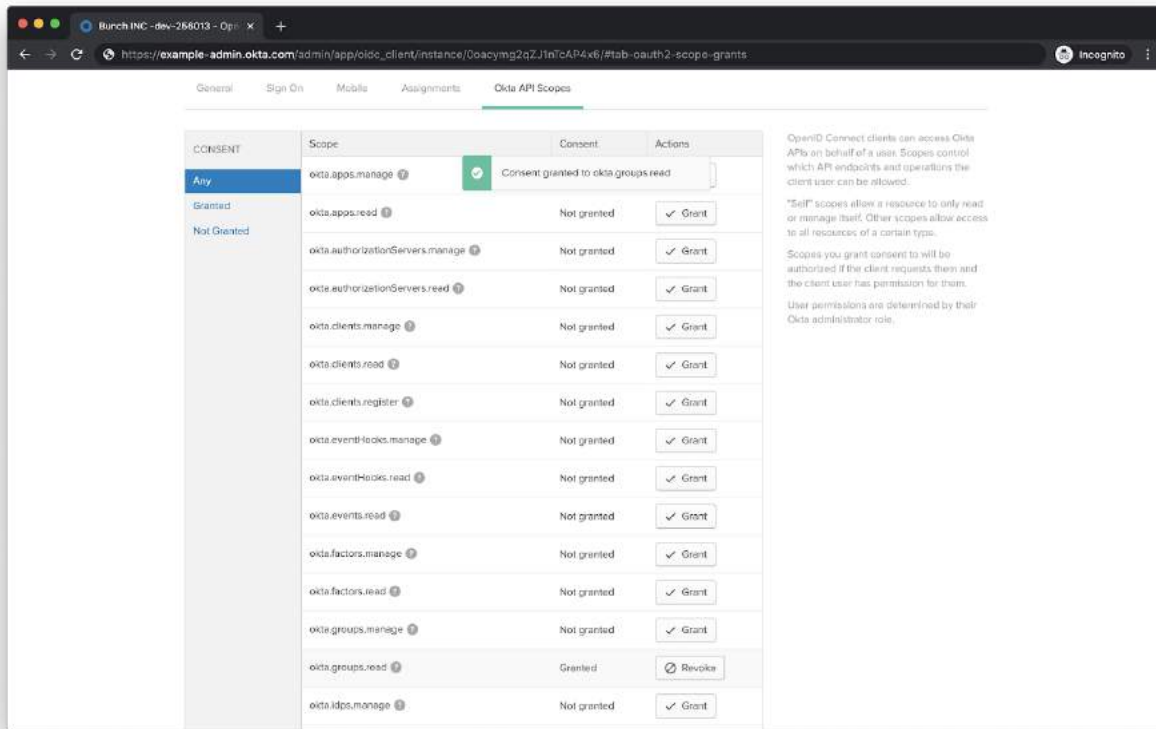


If the **OAuth 2.0 for Okta APIs** feature on the Okta domain is enabled, assign read permissions to users and groups.

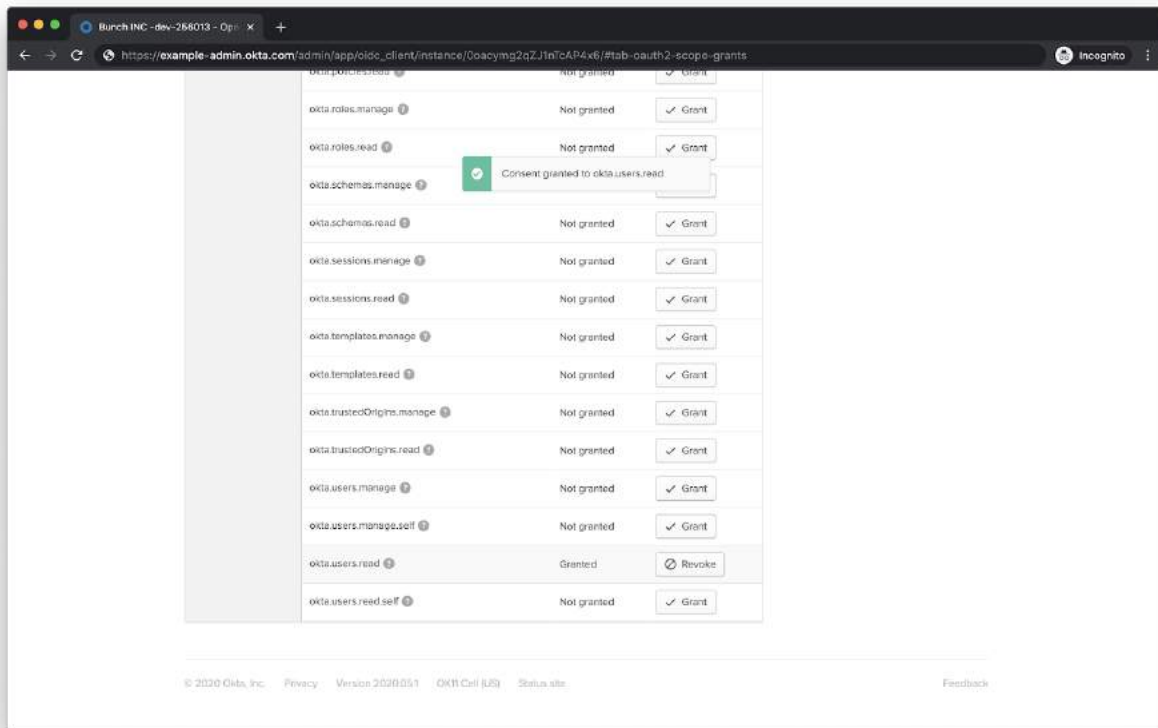
Click on the **Okta API Scopes** tab and grant the following permissions,

- `okta.groups.read`
- `okta.users.read`

Click on the **Grant** button next to `okta.groups.read`.



Scroll down to the bottom of the page and click on the **Grant** button next to **okta.users.read**.

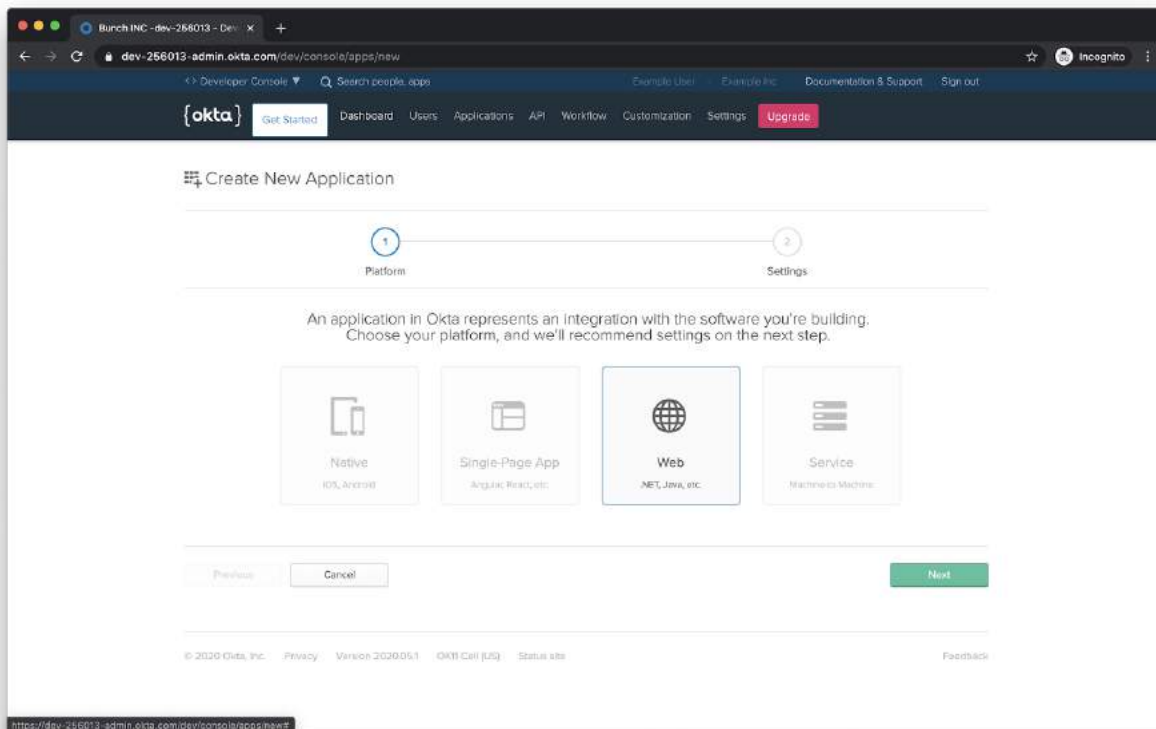


OpenID Connect Application for User Signin (Optional)

Create an additional OpenID Connect application on the Okta administrative console to use for user sign-in. Click on the **Applications** under **Applications** navigation menu.

This application is specifically used for signing in users whereas the other OpenID Connect application is used for user and group search.

Click on the **Add Application** button on the Applications page. Select the **Web** and click on the **Next** button.



Enter the following details,

- **Application Name:** Displayed to the user when they sign-in for the first time
- **Base URIs** (optional): List of URLs that are trusted by okta. For example, if Bridge is deployed on example.com, then the Base URIs would be,
 - https://example.com
- **Login redirect URIs:** List of URLs the user could be redirected to after they login using their Okta credentials. If Bridge is deployed on **example.com**, then the redirect URIs would be,
 - https://**example.com**/auth/adapters/callback
 - https://**example.com**:443/auth/adapters/callback
- **Logout redirect URIs:** List of URLs the user is redirected to after logging out of the session. If Bridge is deployed on **example.com**, then the logout redirect uri would be **https://example.com**.
- **Group assignments:** List of Okta groups that are capable of logging in to Bridge using the OpenID connect client.
- **Grant type allowed:** Grant type used for the sign-in flow. Check on **Authorization Code** grant type.

Click on the **Done** button to create the OpenID Connect client for User sign-in.

Developer Console
Search people, apps
Example User
Example Inc.
Documentation & Support
Sign out

[okta]
Get Started
Dashboard
Users
Applications
API
Workflow
Customization
Settings
Upgrade

Create New Application

Platform
Settings

We use these default values for our web app samples. Edit them to fit your needs. All these settings can be changed at any time.

APPLICATION SETTINGS

Name
Bridge User Sign-in Client

Base URIs
Optional
https://band.example.com
+ Add URI

The domains where your application runs. Trusted Origins are created for these URIs and are the only domains that Okta accepts API calls from. [Docs](#)

Login redirect URIs
https://band.example.com/auth/adapter/callback
https://band.example.com:443/auth/adapter/callback
+ Add URI

Okta sends an OAuth authorization response to these URIs. Add your application's callback endpoint. [Docs](#)

Logout redirect URIs
https://band.example.com
+ Add URI

When a user signs out, your application can specify a URI where the browser is redirected. Okta only allows redirects for URIs that are listed here. [Docs](#)

Group assignments
Optional
Everyone

Users can only sign in to apps that they are assigned to. Group assignments are easier to manage than individual users.

Grant type allowed

Client acting on behalf of itself
☐ Client Credentials

Client acting on behalf of a user
☒ Authorization Code
☐ Refresh Token
☐ Implicit (Hybrid)

Okta can authorize your native app's requests with these OAuth 2.0 grant types. Limit the allowed grant types to minimize security risks. [Docs](#)

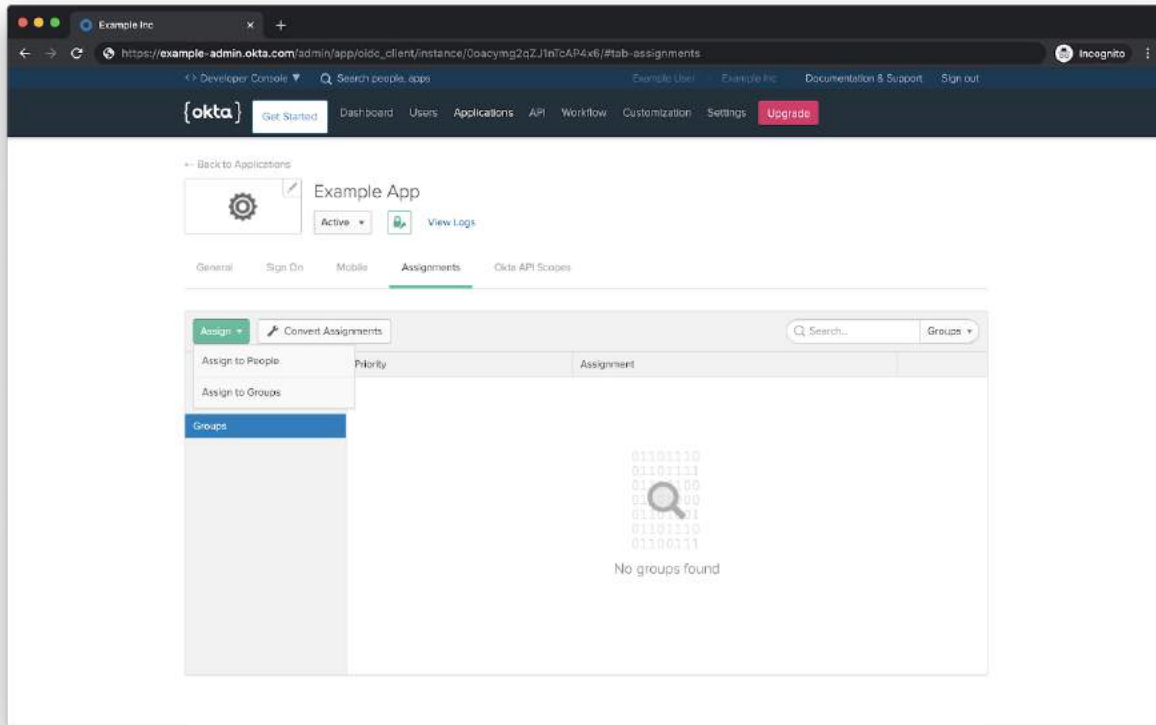
Quick Start Guides
Node.js
Java
.NET
.NET

Previous
Cancel
Done

© 2020 Okta, Inc.
Privacy
Version 2020.051
OKTA Call (US)
Status site
Feedback

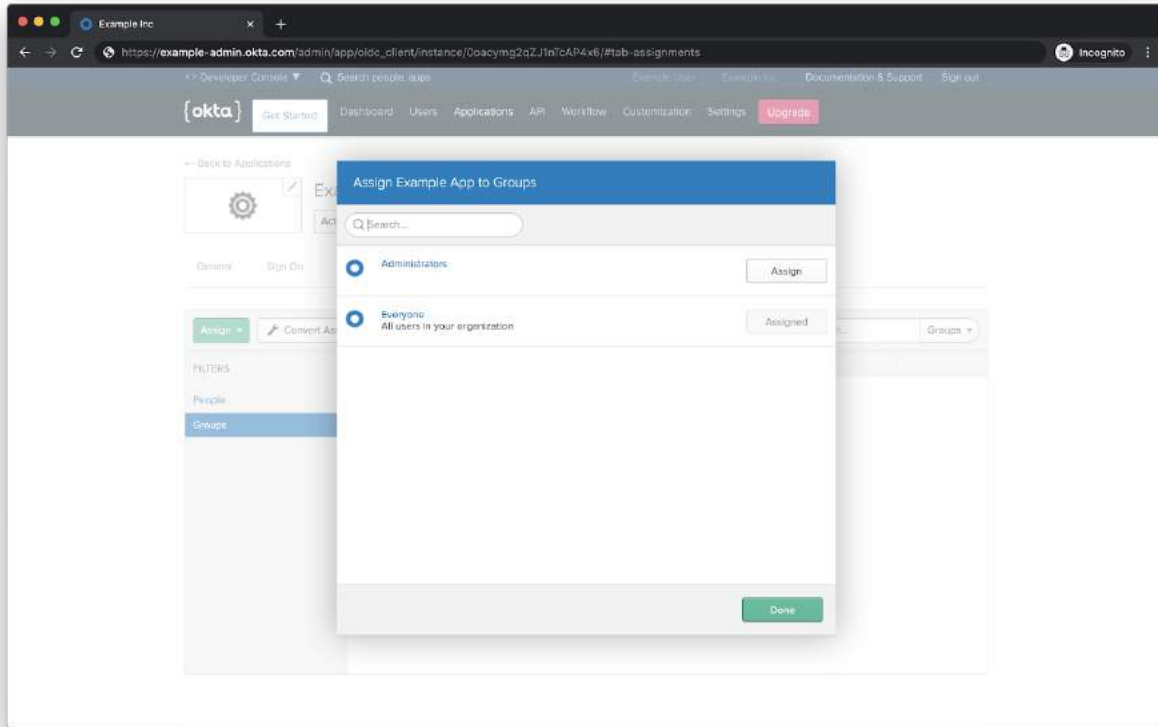
Assign users to Application

Navigate to **Assignments** tab on the application page. Click on the **Assign** button and select **Assign to Groups** on the drop down.

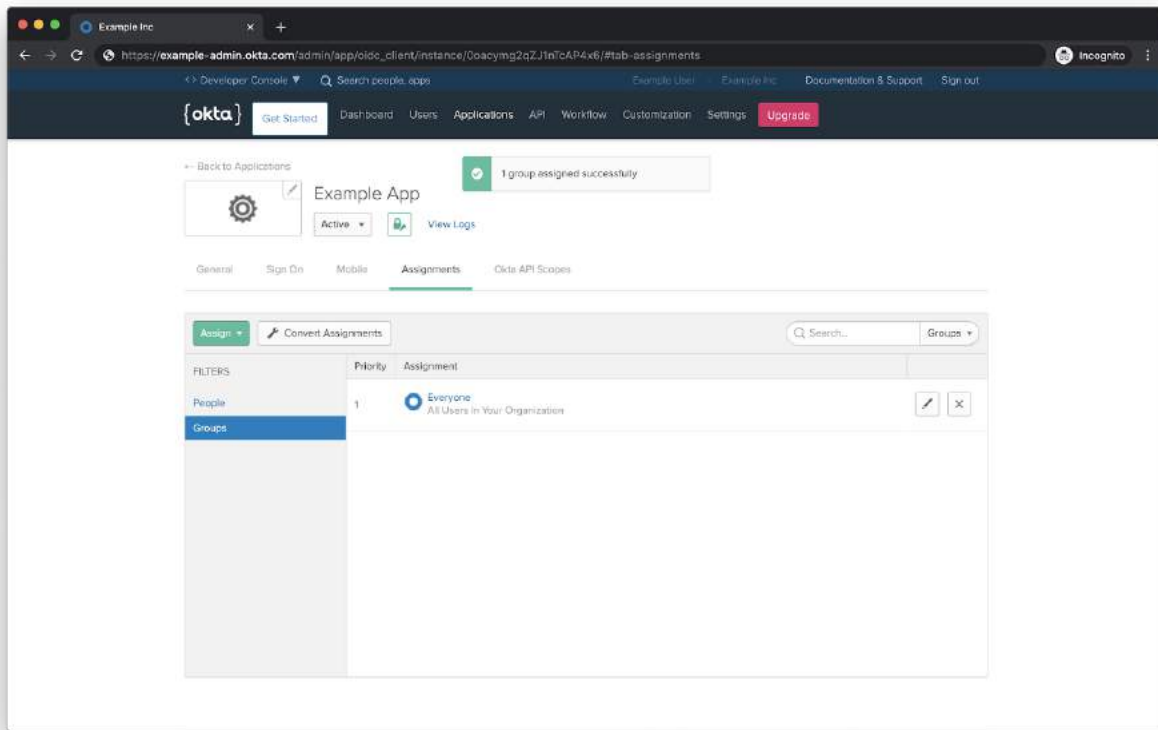


Select the group that needs to be assigned to the application and click on the **Assign** button on the right side of the selected group.

For example, Select **Everyone** group to allow all the users under the organization access the applications through Bridge.



Click on the **Done** button at the bottom right hand corner of the dialog.



Credentials

From the previous steps, the following items are required to add the Okta adapter to Bridge:

- Okta Organization URL
- Client ID
- Client Secret
- Service Account Username
- Service Account Password
- User Sign-in Client Id (optional)
- User Sign-in Client Secret (optional)

Click on the Okta icon on **Add Adapter** page, Enter the credentials in the Okta adapter form and click on the **NEXT** button.

The screenshot shows a web browser window titled 'Adapter Setup' with the URL 'https://example.com/bridge/admin/adapters/setup'. The page is part of the 'BRIDGE' application, with a 'demo' dropdown menu. On the left sidebar, there are three main sections: 'Adapters' (selected), 'Clients', and 'Admins'. The 'Adapters' section has a progress bar with three steps: 'Select an adapter' (completed), 'Enter credentials' (current step), and 'Authorize Application'. The 'Okta' adapter is selected. The form fields are as follows:

- Name: Okta
- Org Url: https://example.okta.com
- Client Id: Example Client ID
- Client Secret: Example Client Secret
- Username: service_account
- Password: (masked with dots)
- User sign-in workflow (Optional):
 - ☐ Use another OpenID Connect client for user sign-in
- User Signin Client Id: (empty field)
- User Signin Client Secret: (empty field)

At the bottom right, there are 'BACK' and 'NEXT' buttons. At the bottom left, there is a 'Logout' button with a power icon.

If an OpenID Connect application is created for User sign-in flow, click on the toggle switch to enable User Sign-in Client form.

Enter the User Sign-in Client Id and Client Secret and click on the **Next** button.

The screenshot shows the Bridge Admin interface for setting up an adapter. The sidebar on the left contains 'Adapters', 'Clients', and 'Admins'. The main area is titled 'demo' and shows a progress bar with three steps: 'Select an adapter' (checked), 'Enter credentials' (active), and 'Authorize Application'. The 'Enter credentials' step is for the 'Okta' adapter. It includes the following fields:

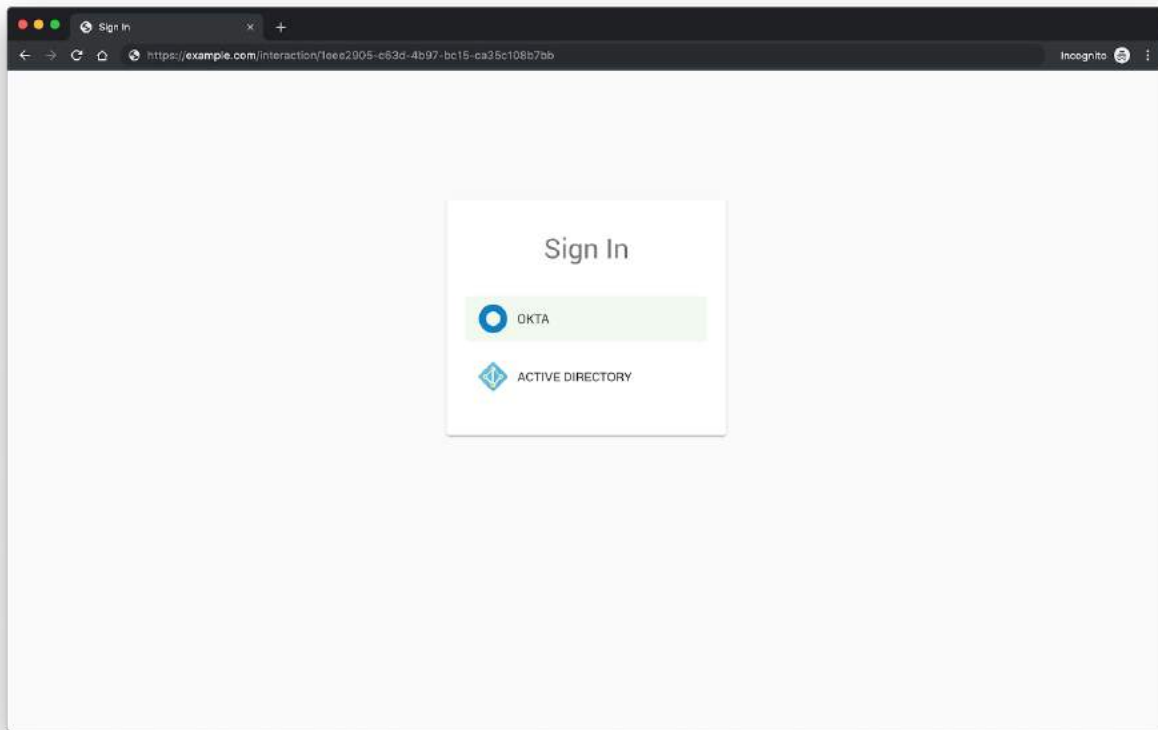
- Name: Okta
- Org Url: https://example.okta.com
- Client Id: Example Client ID
- Client Secret: Example Client Secret
- Username: service_account
- Password: (masked with dots)

Below these fields is a section for 'User sign-in workflow (Optional)' with a toggle switch set to 'Use another OpenID Connect client for user sign-in'. This section includes the following fields:

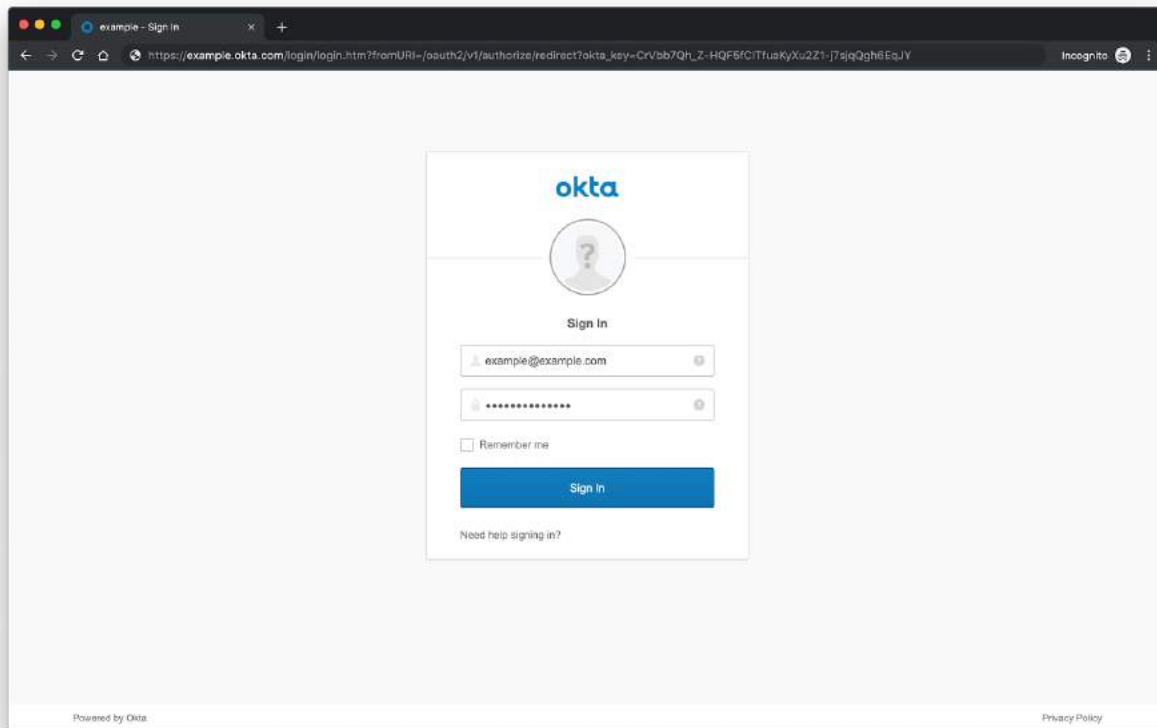
- User Sign-in Client Id
- User Sign-in Client Secret
- User Sign-in Client Secret

At the bottom right of the form are 'BACK' and 'NEXT' buttons. A 'Logout' button is located in the bottom left corner of the sidebar.

Click on the adapter name (**Okta**) entered in the previous step to proceed with the sign in.



Enter the **Okta** user account credentials on the okta login page and click on the **Sign In** button.



Twilio SMS

Preparations

Setting up SMS adapter on Bridge requires a Twilio account with a phone number.

Configuration

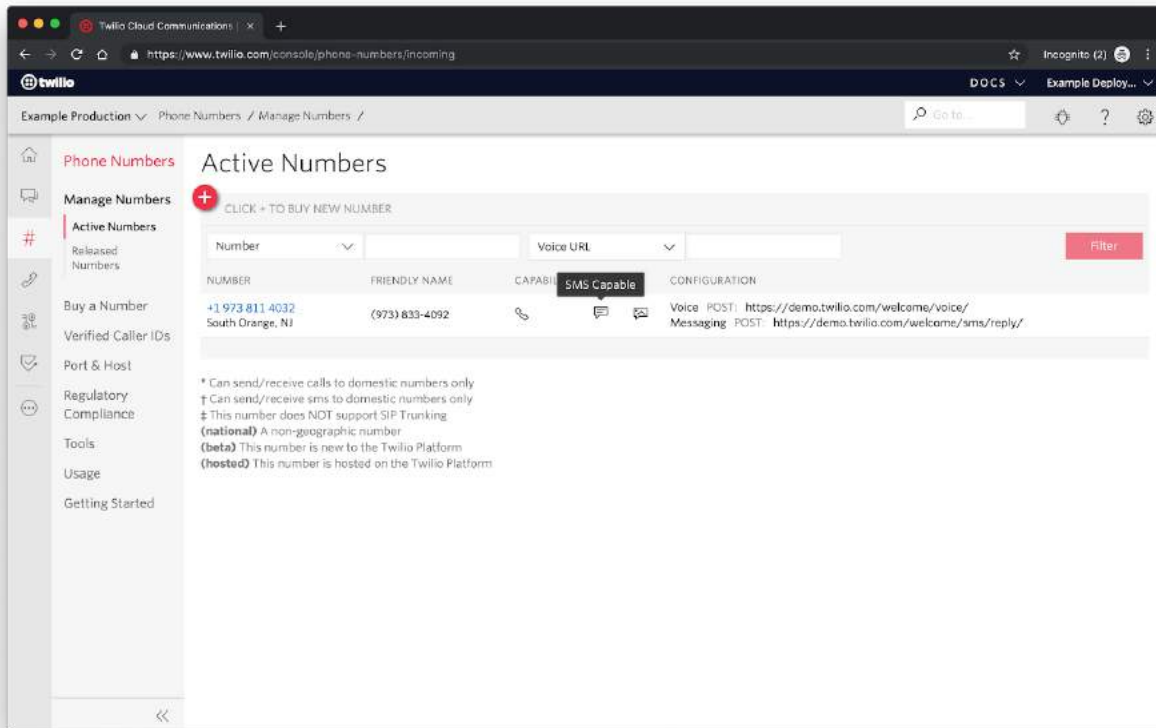
The following items from twilio are required to setup an SMS adapter on Bridge:

- Account SID
- Auth Token
- Number

Phone Number

Twilio phone number can be purchased on [Buy a Number](https://www.twilio.com/console/phone-numbers/search)¹¹ page on Twilio dashboard, Alternatively an existing number in service can be ported to twilio.

The phone number must be **SMS capable** in order to work with Bridge.

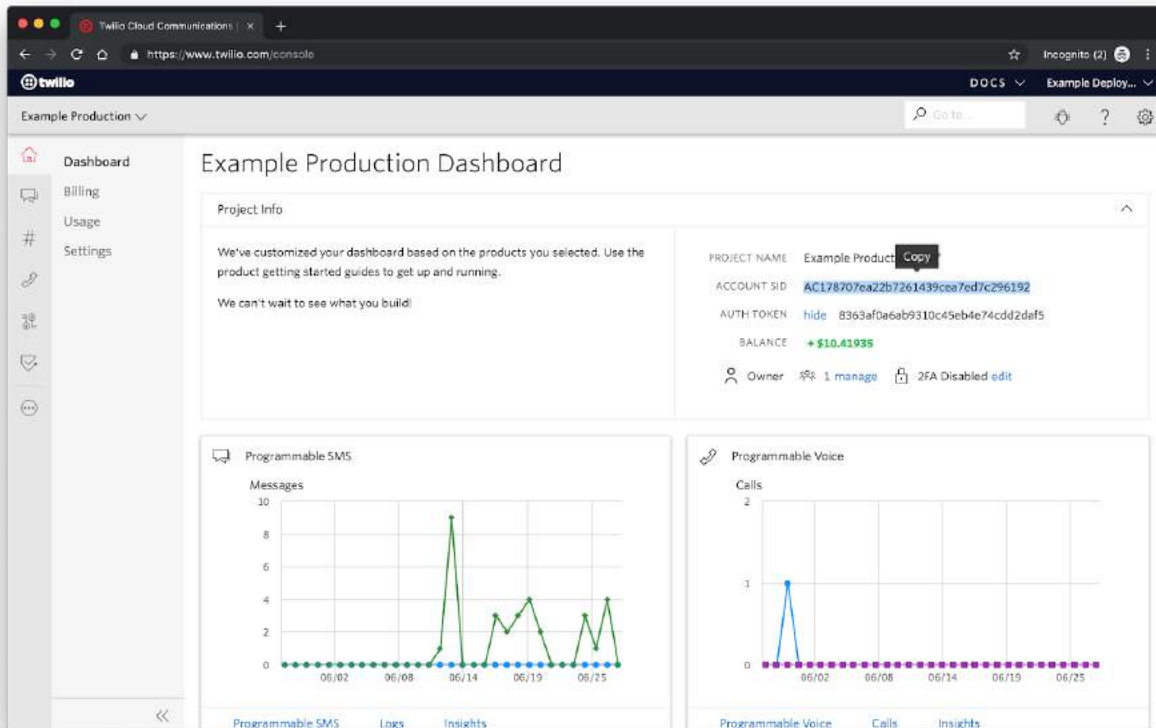


¹¹ <https://www.twilio.com/console/phone-numbers/search>

Account SID

Navigate to the [Twilio dashboard](https://www.twilio.com/console)¹² and make a note of the **ACCOUNT SID** located on the right hand side of the page.

See the highlighted text in the following picture.

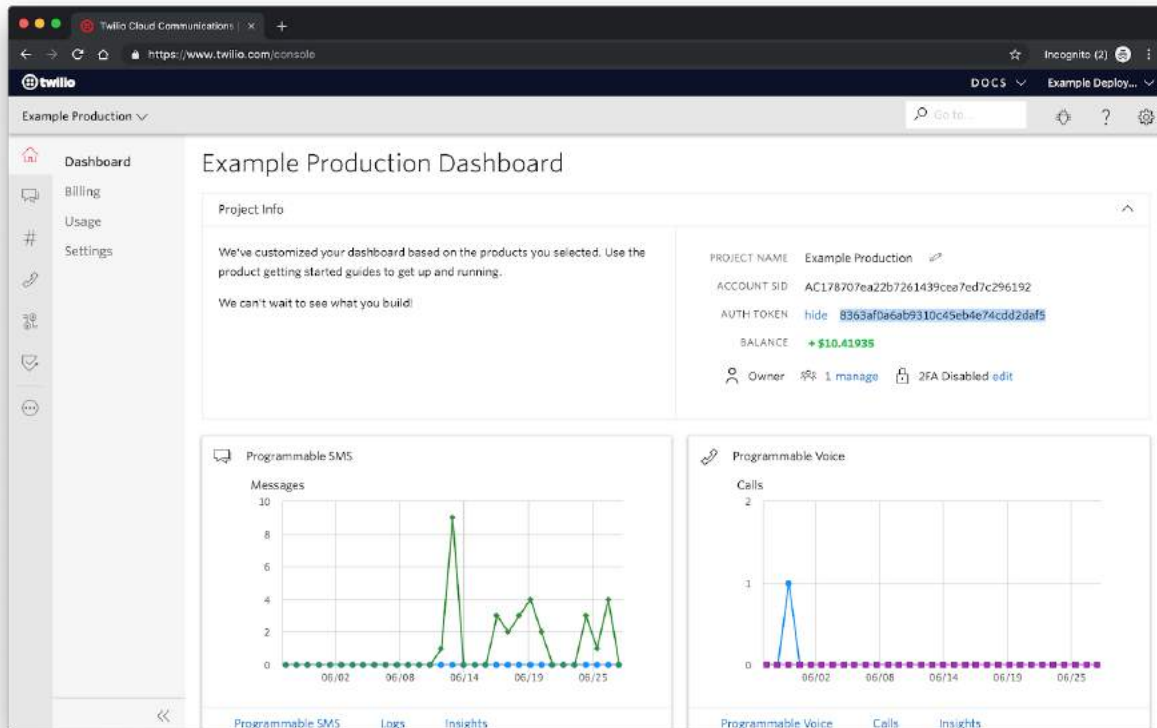


¹² <https://www.twilio.com/console>

Auth Token

Navigate to the [Twilio dashboard](https://www.twilio.com/console)¹³ and make a note of the **AUTH TOKEN** located on the right hand side of the page.

See the highlighted text in the following picture.



¹³ <https://www.twilio.com/console>

Credentials

From the previous steps, the following items are required to add the SMS adapter to Bridge:

- Account SID
- Auth Token
- Phone Number

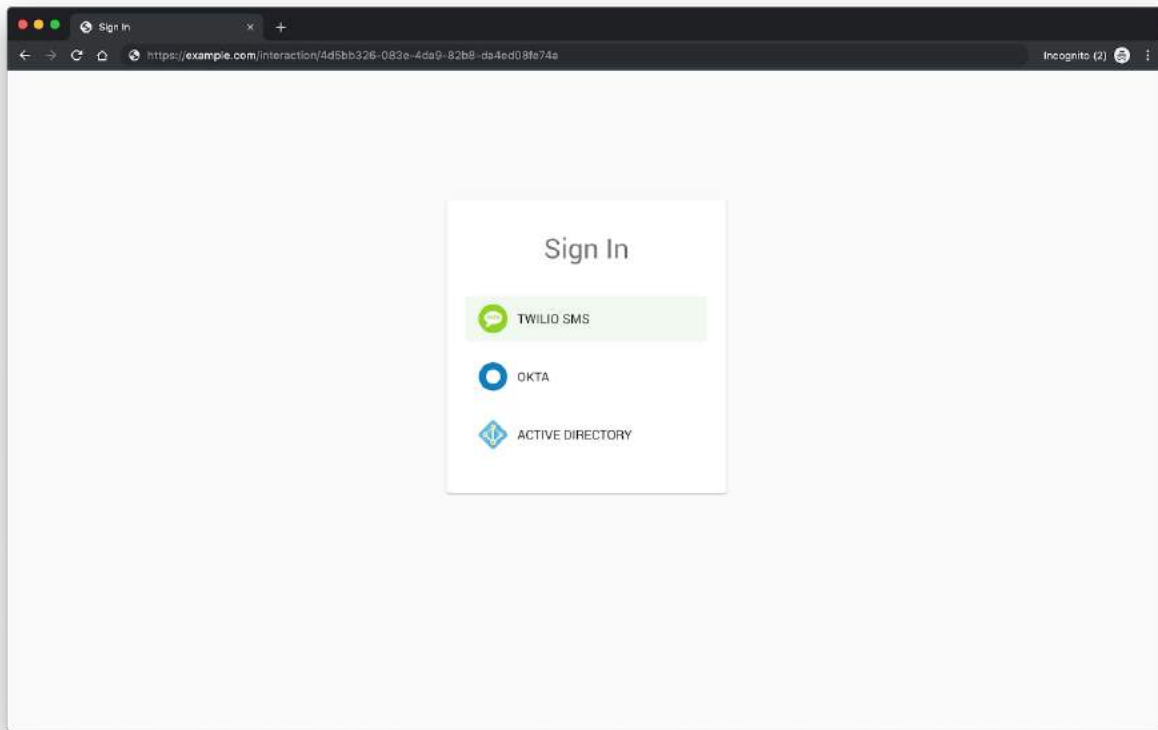
Click on SMS icon on **Add Adapter** page, Enter the credentials in the SMS adapter form and click on the **NEXT** button.

The screenshot shows a web browser window with the URL `https://example.com/bridge/admin/adapters/setup`. The page is titled "BRIDGE" and has a "demo" dropdown menu. On the left, there is a sidebar with "Adapters", "Clients", and "Admins" sections. The "Adapters" section is active, showing a progress bar with three steps: "Select an adapter" (completed), "Enter credentials" (current step), and "Authorize Application". The "SMS" adapter is selected. The form contains the following fields:

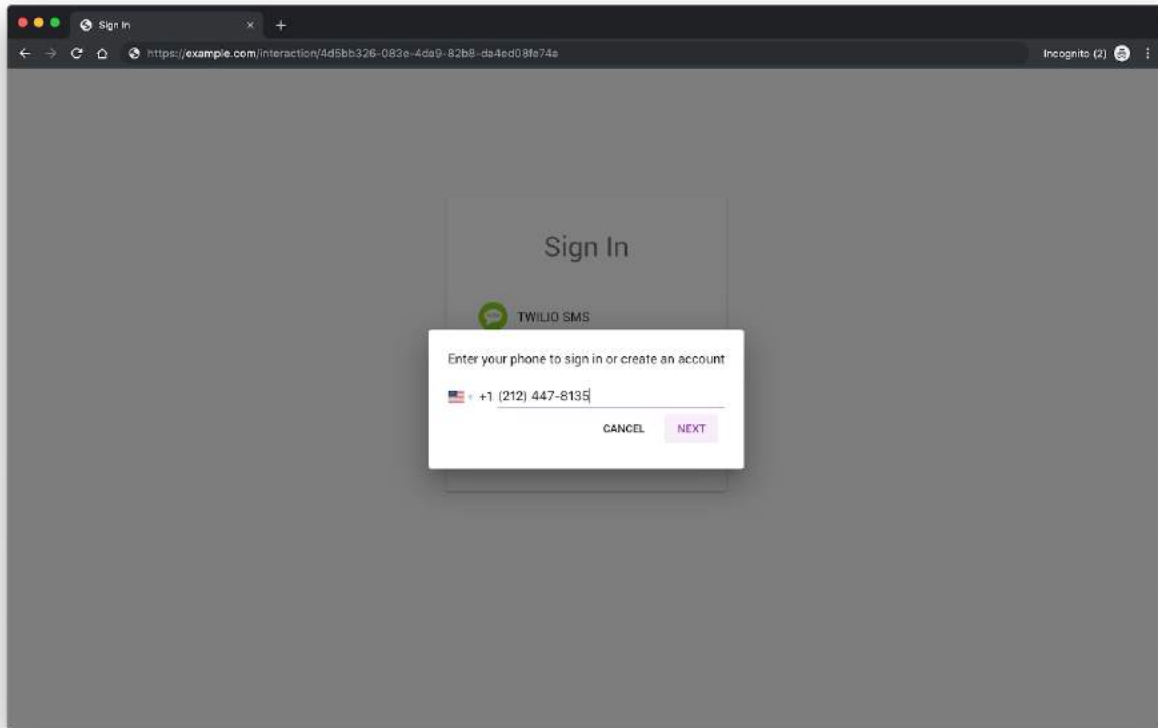
- Name: Twilio SMS
- Twilio Account SID: AC178707ea22b7261053cea76d79296a92
- Twilio Authentication Token: 8363af0a6ab9310c45eb4e74cdd2daf5
- Twilio "From" Phone Number: +19738114032

Below the fields, a note states: "Format should be country code and phone number. Eg: +12223334444". At the bottom right, there are "BACK" and "NEXT" buttons. A "Logout" button is located in the bottom left corner of the sidebar.

Click on the adapter name (**Twilio SMS**) entered in the previous step.

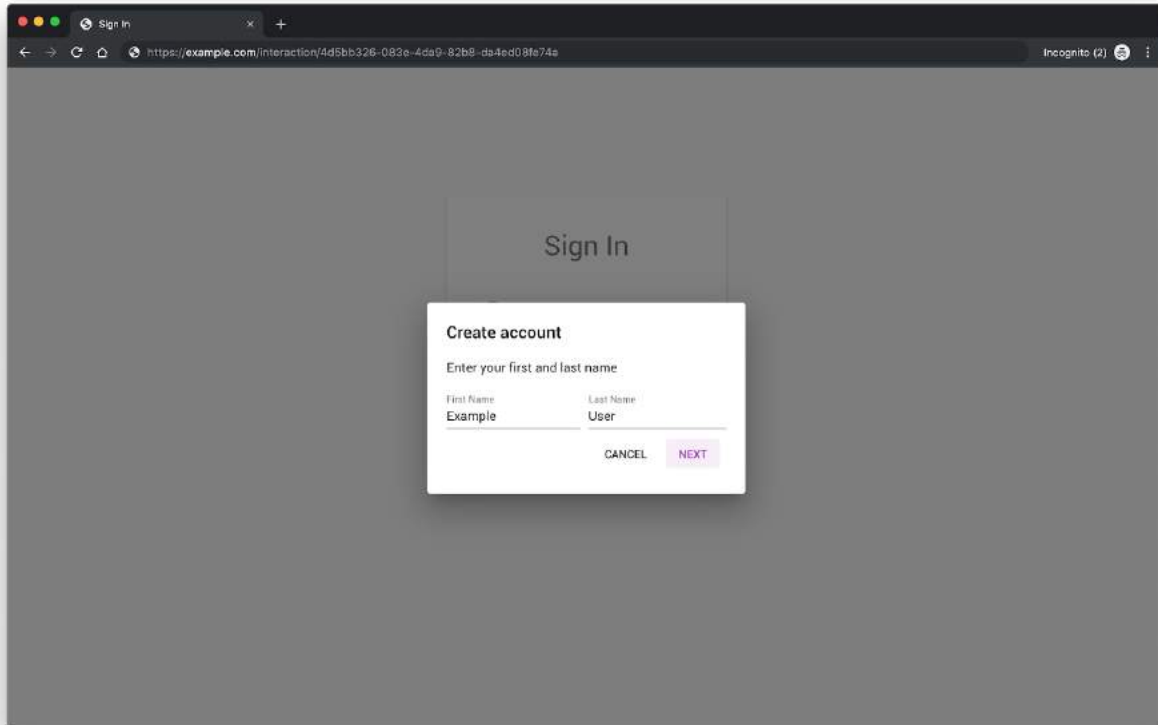


Enter the phone number of the user and click on the **NEXT** button. Shortly after Bridge will send the number an sms message with a 5 digit authentication code from twilio phone number.



If an account with the phone number entered in the previous doesn't exist in Bridge, it will request the user details such as first name, last name to create an account on Bridge.

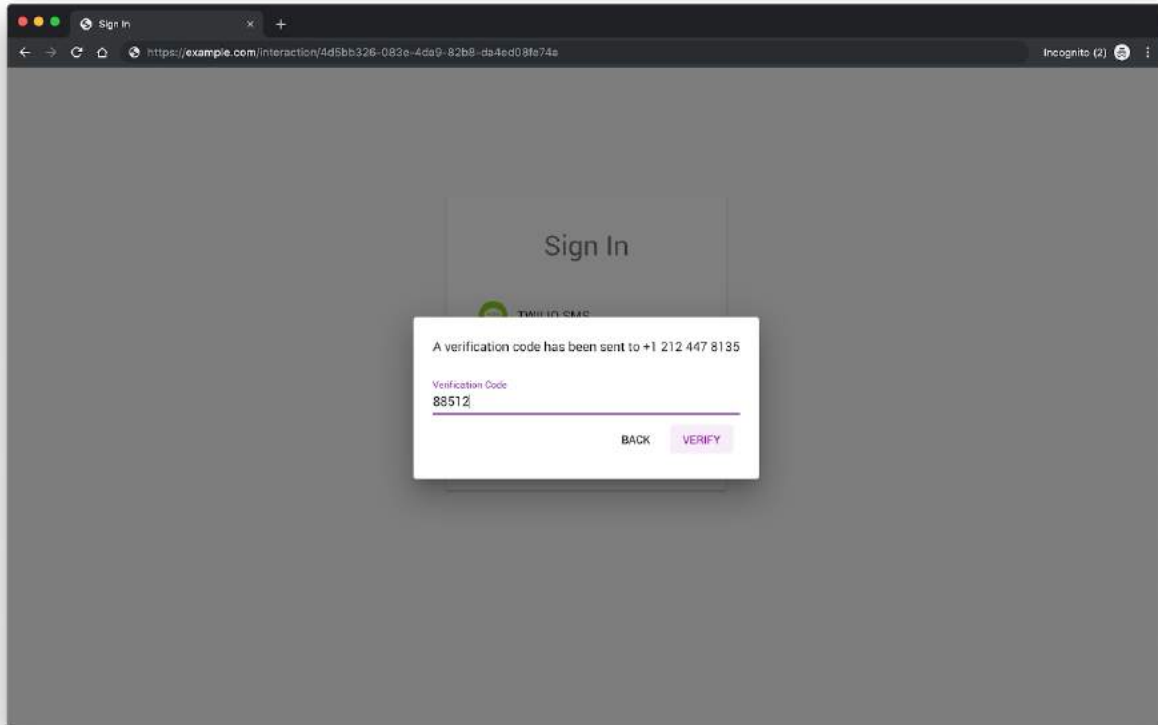
Enter the first name, last name and click on the **NEXT** button to proceed to create an account.



The screenshot shows a web browser window with a dark theme. The address bar displays a URL starting with 'https://example.com/'. The main content area is a dark gray rectangle. In the center, there is a light gray box labeled 'Sign In'. Overlaid on this is a white modal form titled 'Create account'. The form contains the instruction 'Enter your first and last name' and two input fields: 'First Name' with the text 'Example' and 'Last Name' with the text 'User'. At the bottom of the form are two buttons: 'CANCEL' and 'NEXT'.

Enter the 5 digit verification code sent to the number entered in the previous step from the phone number configured during the adapter setup.

Click on **VERIFY** button to sign in.

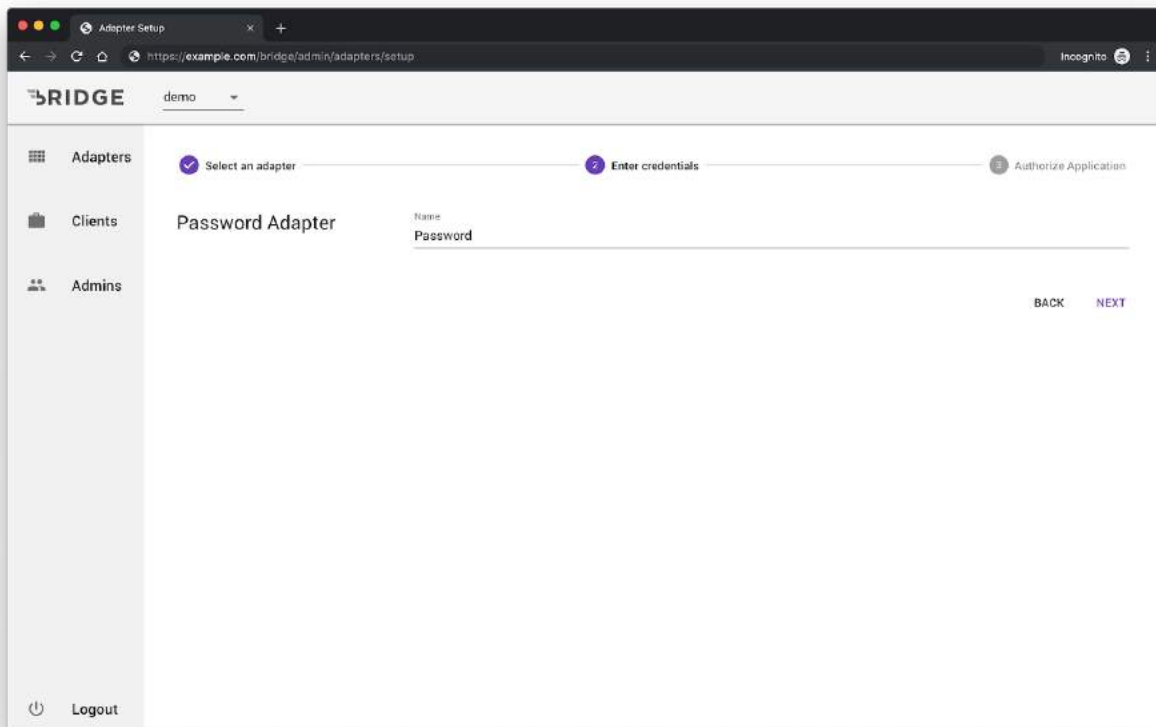


Password

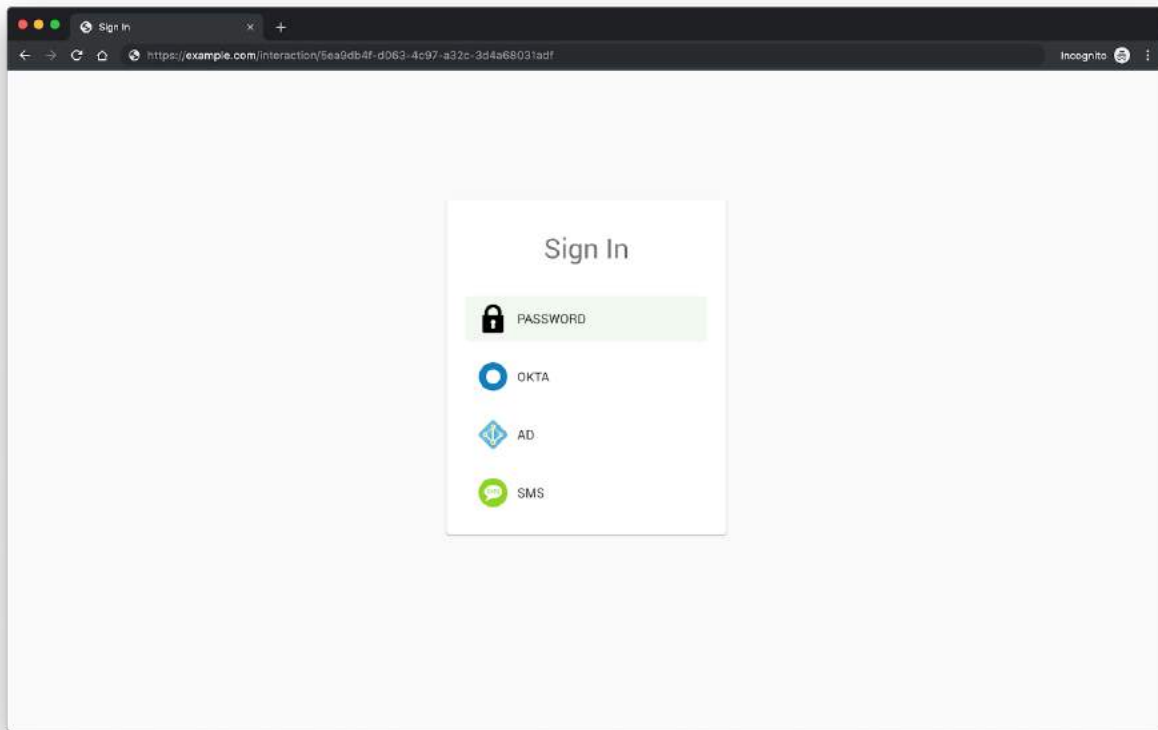
Configuration

Setting up Password adapter on Bridge stores the user information on Bridge database, so there are no 3rd party dependencies.

Click on Password icon on **Add Adapter** page, Enter the name of the password adapter and click on the **NEXT** button.

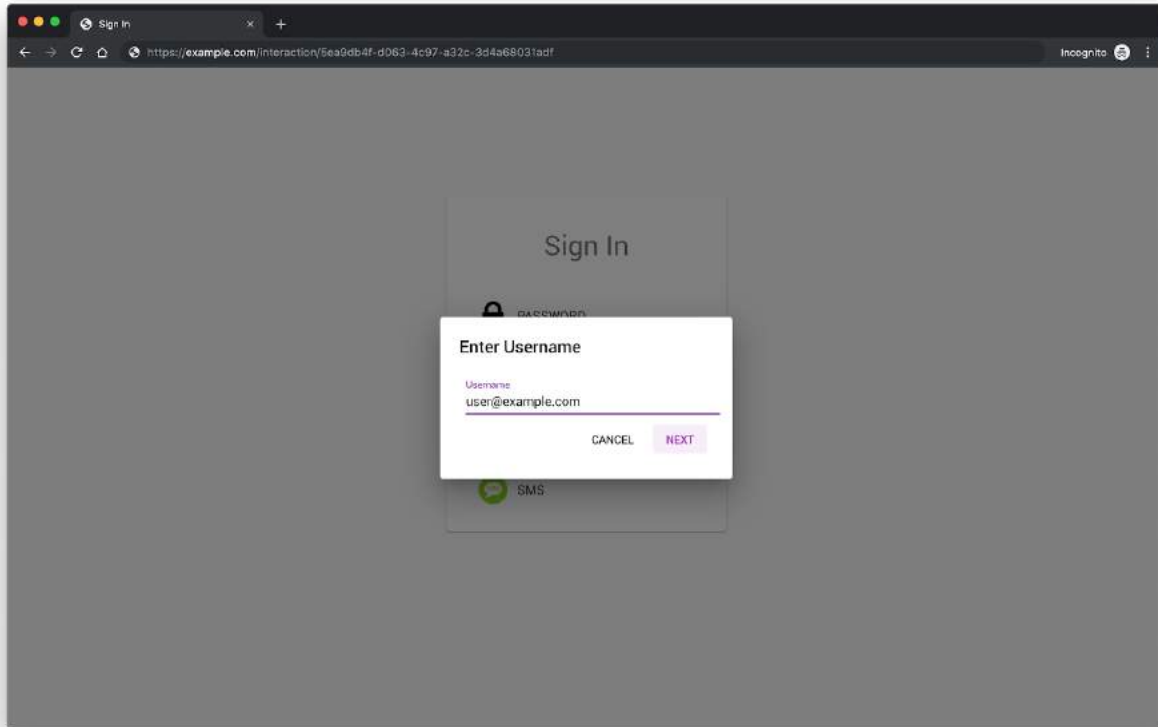


Click on the adapter name entered in the previous step (**Password**).



Enter the email address of the user to create an account. This email address can be used later to login to the password adapter.

Click on the **NEXT** button to proceed to the next step.

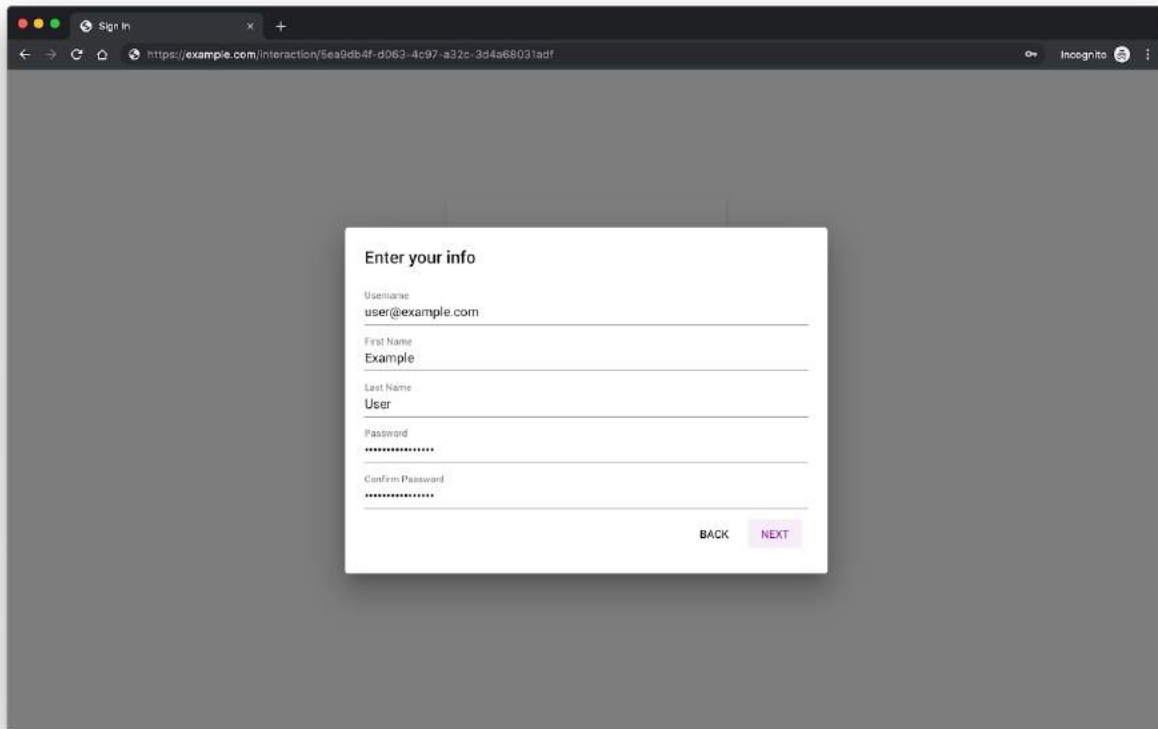


If the user with the email address entered in the previous step does not exist in Bridge, It will create a new account. Enter the user first name, last name and password to create an account in Bridge.

Click on the **NEXT** button to proceed to the next step.

WARNING

Make a note of the email address and password as they are required to login to bridge.

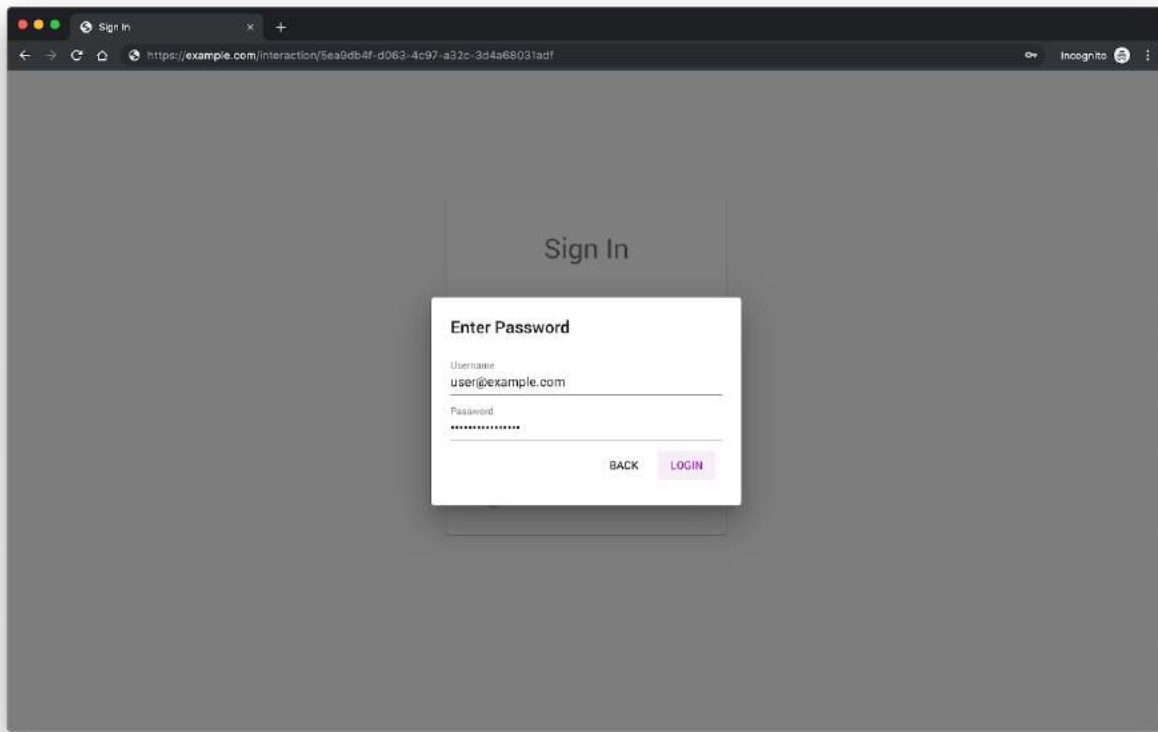


The screenshot shows a web browser window with a dark theme. The address bar displays a URL starting with 'https://example.com/'. The page title is 'Sign in'. A white modal form titled 'Enter your info' is centered on the screen. The form contains the following fields and values:


- Username:** user@example.com
- First Name:** Example
- Last Name:** User
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)

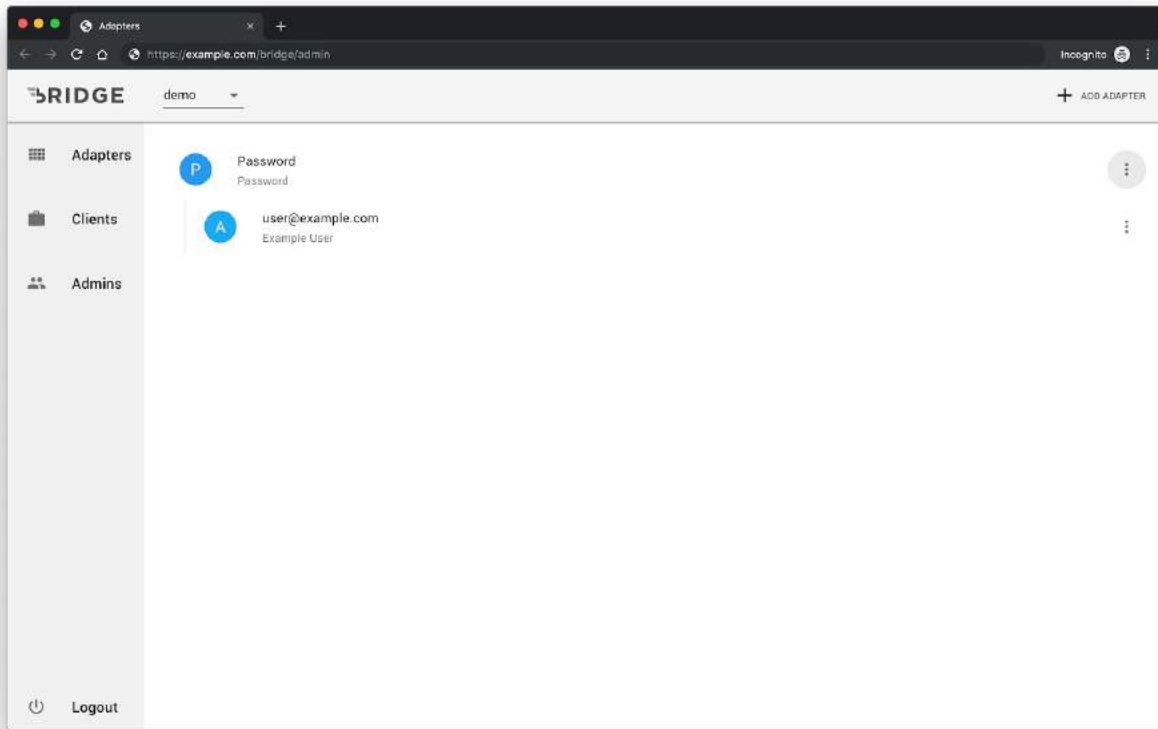
At the bottom right of the form, there are two buttons: 'BACK' and 'NEXT'.

Enter the username and password of the account created in the previous step. Click on **LOGIN** to proceed to login to bridge with the user email, password.



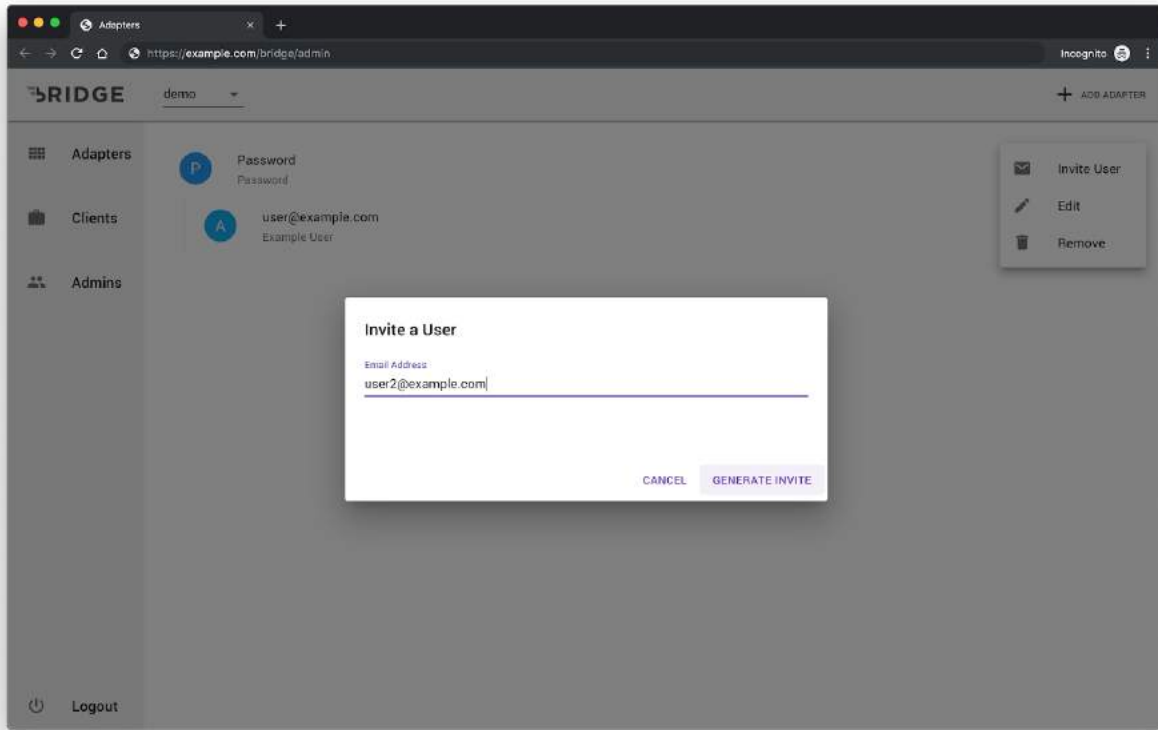
Add Users

Click on the  menu icon located on the right hand side of the password adapter.

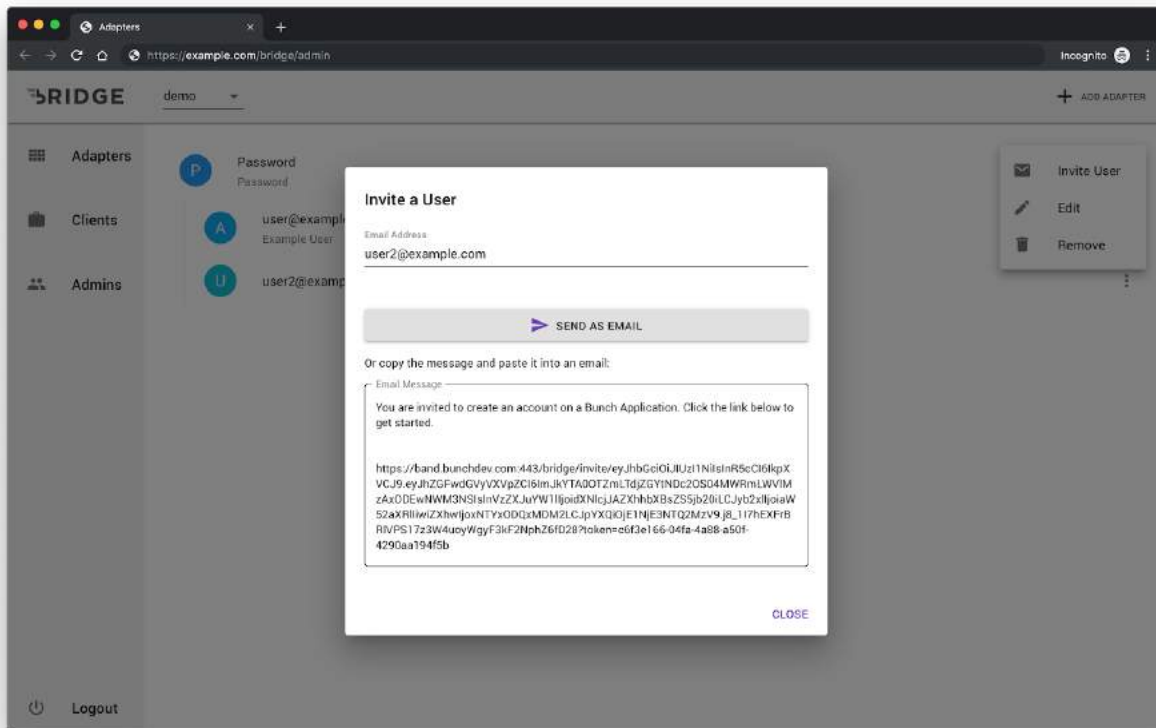


Click on **Invite User** on the pop up menu.

Enter the email address of the user and click on the **GENERATE INVITE** button.

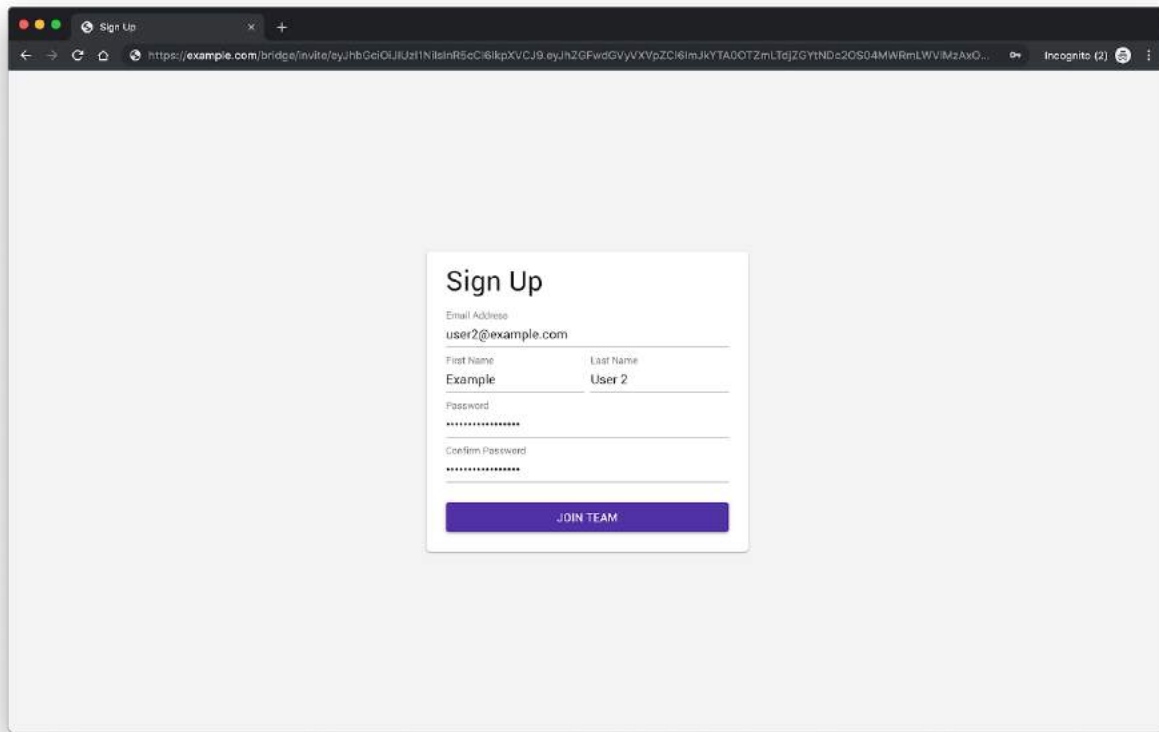


Send the **Email message** to the invited user.



The Invitation URL can be used by the invited user to create an account on Bridge.

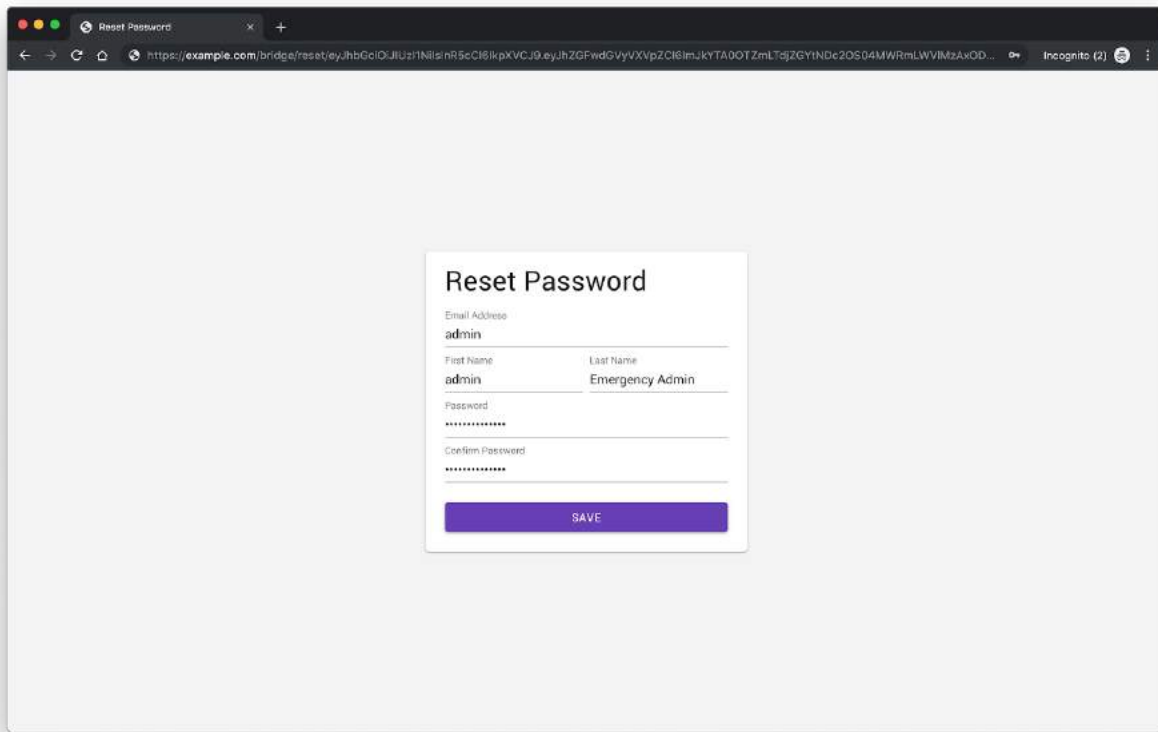
Click on **JOIN TEAM** button to create an account and join the team.



The screenshot shows a web browser window with a single tab titled "Sign Up". The address bar displays a long, complex URL starting with "https://example.com/bridge/invite/". The main content area is a light gray, and centered within it is a white "Sign Up" form. The form has the title "Sign Up" at the top. Below the title are five input fields: "Email Address" with the value "user2@example.com", "First Name" with the value "Example", "Last Name" with the value "User 2", "Password", and "Confirm Password". The password fields are masked with dots. At the bottom of the form is a purple button with the text "JOIN TEAM" in white capital letters.

The **Password Reset URL** can be used to reset the current password of the Bridge account.

Click on the **SAVE** button after updating the password.




The screenshot shows a web browser window with the title 'Reset Password'. The address bar displays a URL starting with 'https://example.com/bridge/reset/'. The main content area features a white form with the title 'Reset Password'. The form contains the following fields:

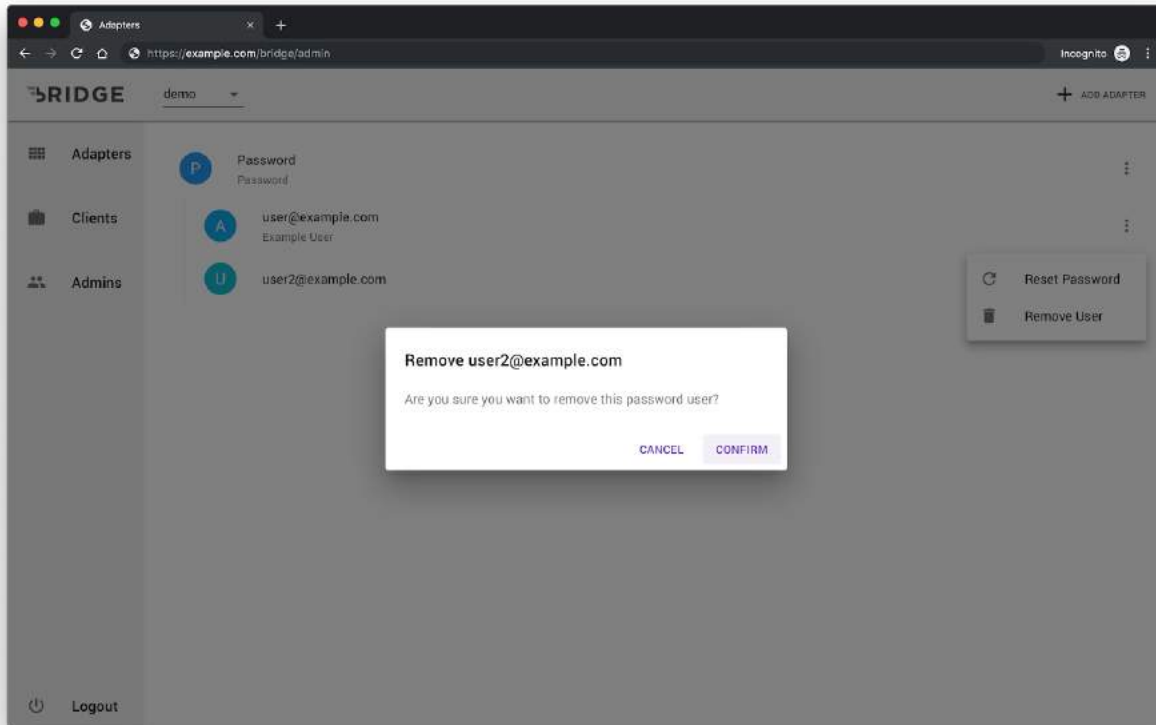
- Email Address:** A text input field containing the value 'admin'.
- First Name:** A text input field containing the value 'admin'.
- Last Name:** A text input field containing the value 'Emergency Admin'.
- Password:** A password input field with masked characters (dots).
- Confirm Password:** A password input field with masked characters (dots).

At the bottom of the form is a purple button labeled 'SAVE'.

Remove User

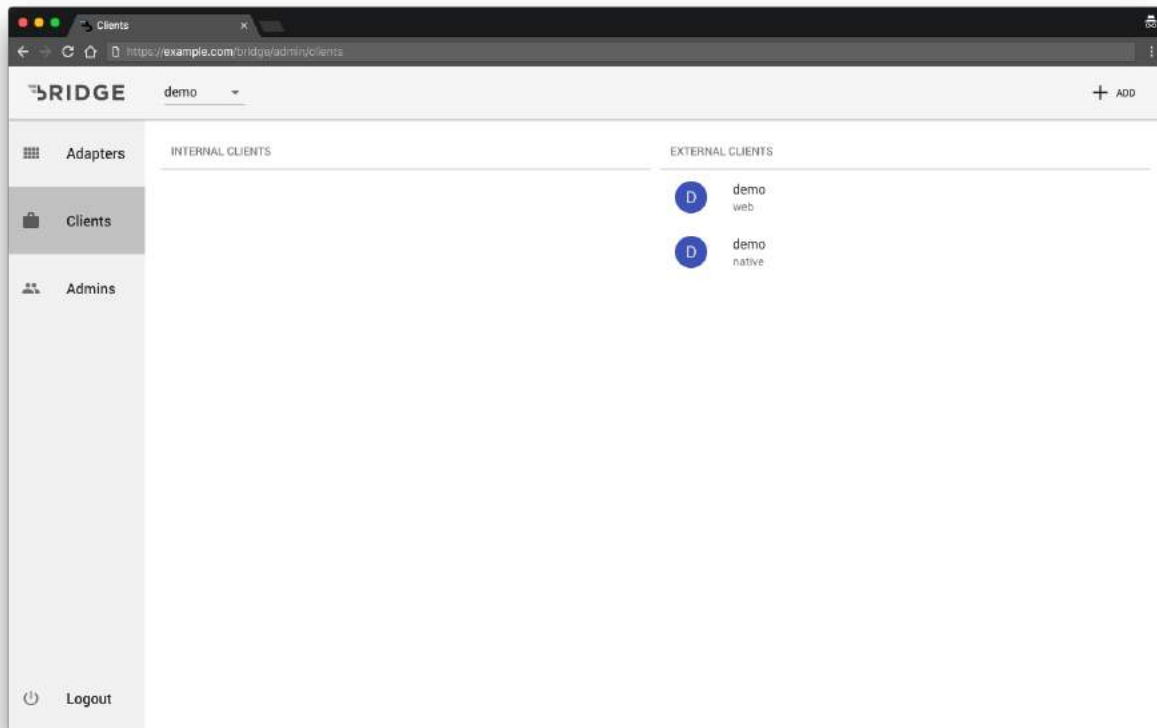
Click on the  menu icon located on the right hand side of the user under the password adapter. Select **Reset User** on the popup menu.

Click on the **CONFIRM** button to remove the user.



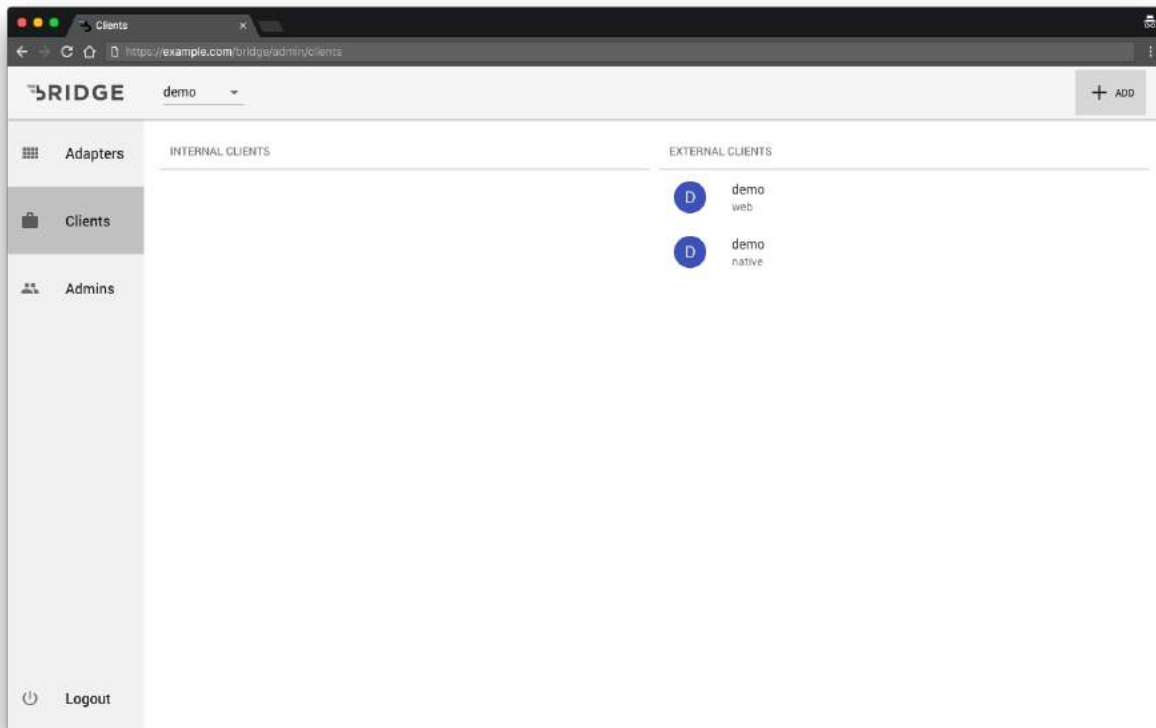
Clients

Clients are used by third-party applications authenticate with Bridge. Click on **Clients** on the left side navigation bar.



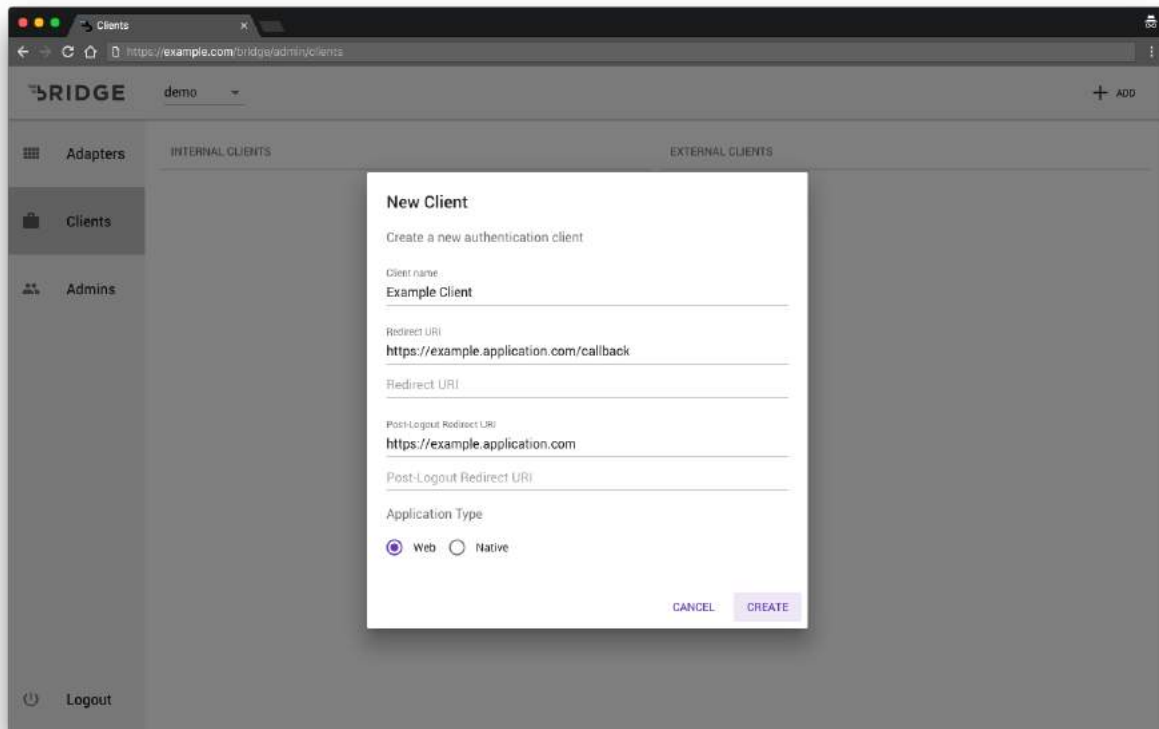
Add Client

Click on the + **ADD** button on the top right corner of the screen.



Enter the following details to add a new client:

- **Client Name:** Name of the Client
- **Redirect URI:** URL to redirect users after authenticating them with Bridge along with their access token
- **Post Logout Redirect URI:** URL to redirect users after logging out of Bridge
- **Application Type:** Select Native only when the client is used by a mobile application, Otherwise select **Web**



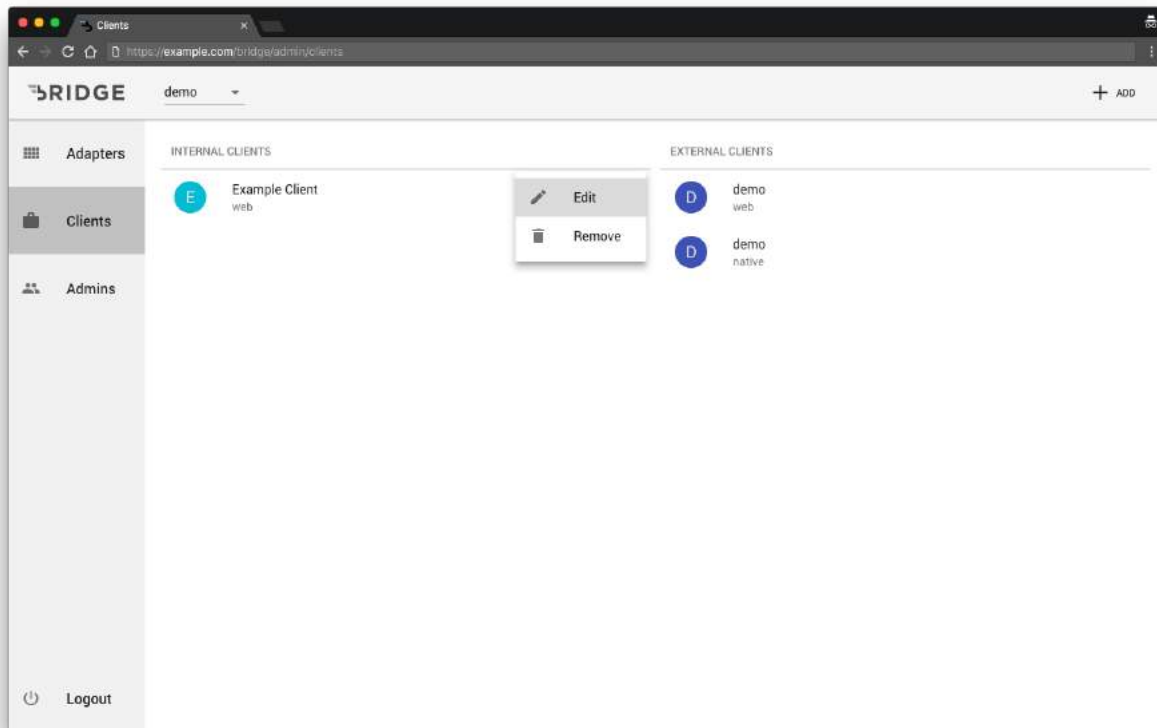
The screenshot shows the Bridge Admin interface in a web browser. The main menu on the left includes 'Adapters', 'Clients', and 'Admins'. The 'Clients' section is active, showing 'INTERNAL CLIENTS' and 'EXTERNAL CLIENTS' tabs. A 'New Client' modal is open, prompting the user to 'Create a new authentication client'. The form contains the following fields:

- Client name:** Example Client
- Redirect URI:** https://example.application.com/callback
- Post-Logout Redirect URI:** https://example.application.com
- Application Type:** Web (selected), Native

At the bottom of the modal are 'CANCEL' and 'CREATE' buttons. The background interface shows a 'demo' dropdown and an '+ ADD' button in the top right corner.

Edit Client

Click on the  menu icon then the **Edit** option from the popup menu.




Add or edit the fields then click **Save** to apply the changes.

The screenshot shows a web browser window with the URL `https://example.com/bridge/admin/clients/97c90819-807c-4cca-8008-2ec34e32d78f`. The page title is "BRIDGE" and the user is logged in as "demo". The sidebar on the left has three main sections: "Adapters" (with a grid icon), "Clients" (with a briefcase icon and highlighted), and "Admins" (with a group of people icon). At the bottom of the sidebar is a "Logout" button with a power icon. The main content area is titled "EXAMPLE CLIENT" and contains the following fields:

- Client Name:** Example Client
- Redirect URI:** https://example.application.com/callback
- Post-Logout Redirect URI:** https://example.application.com

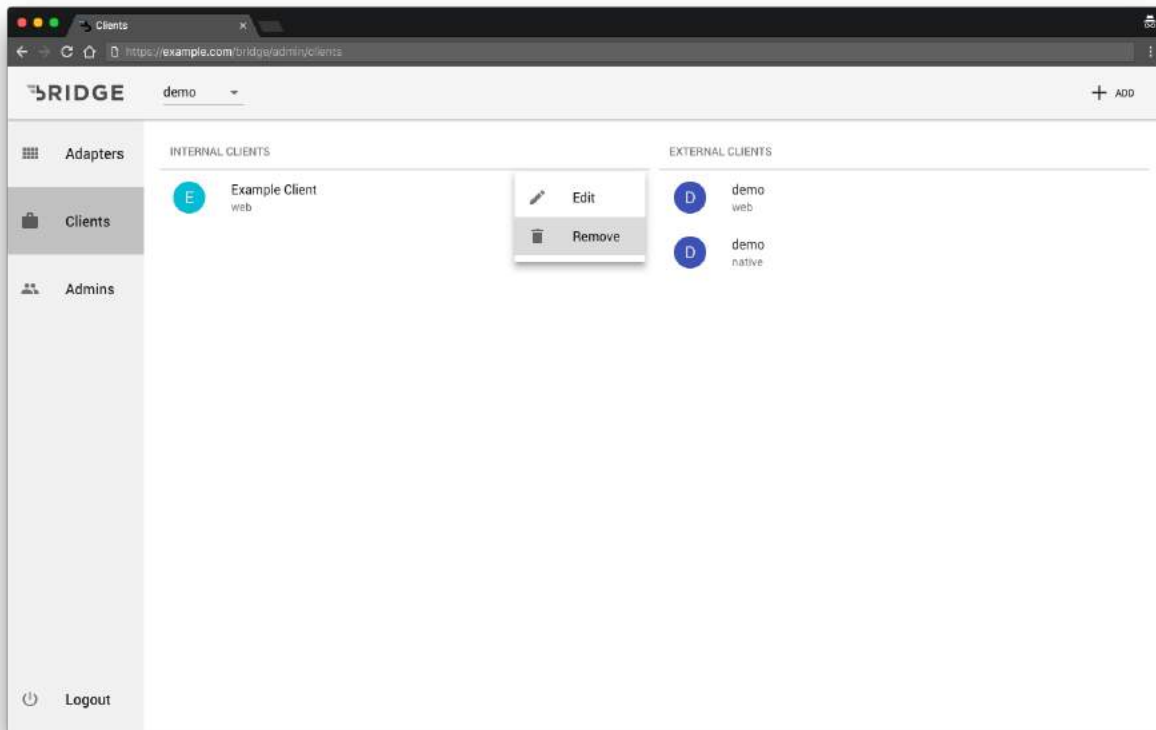
At the bottom of the form is a purple "SAVE" button.

Remove Client

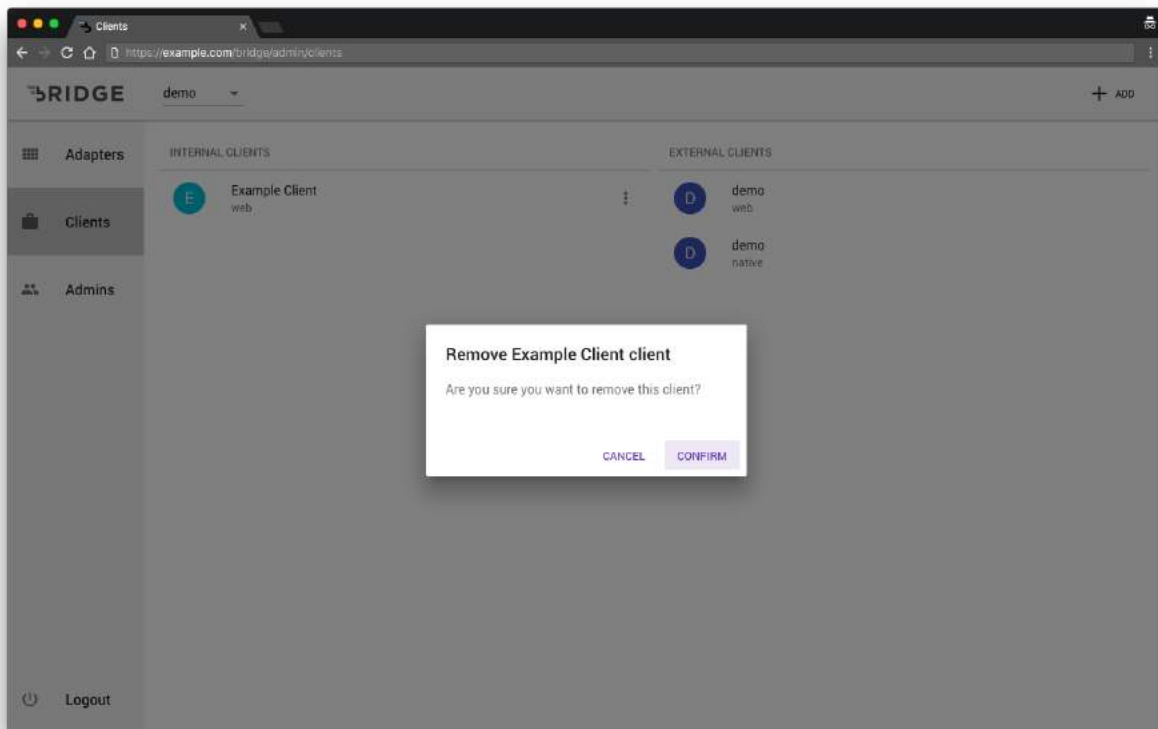
Click on the  menu icon then click on the **Remove** option in the popup menu.

WARNING

This action is not reversible.



Click **CONFIRM** in the confirmation dialog to remove the client.

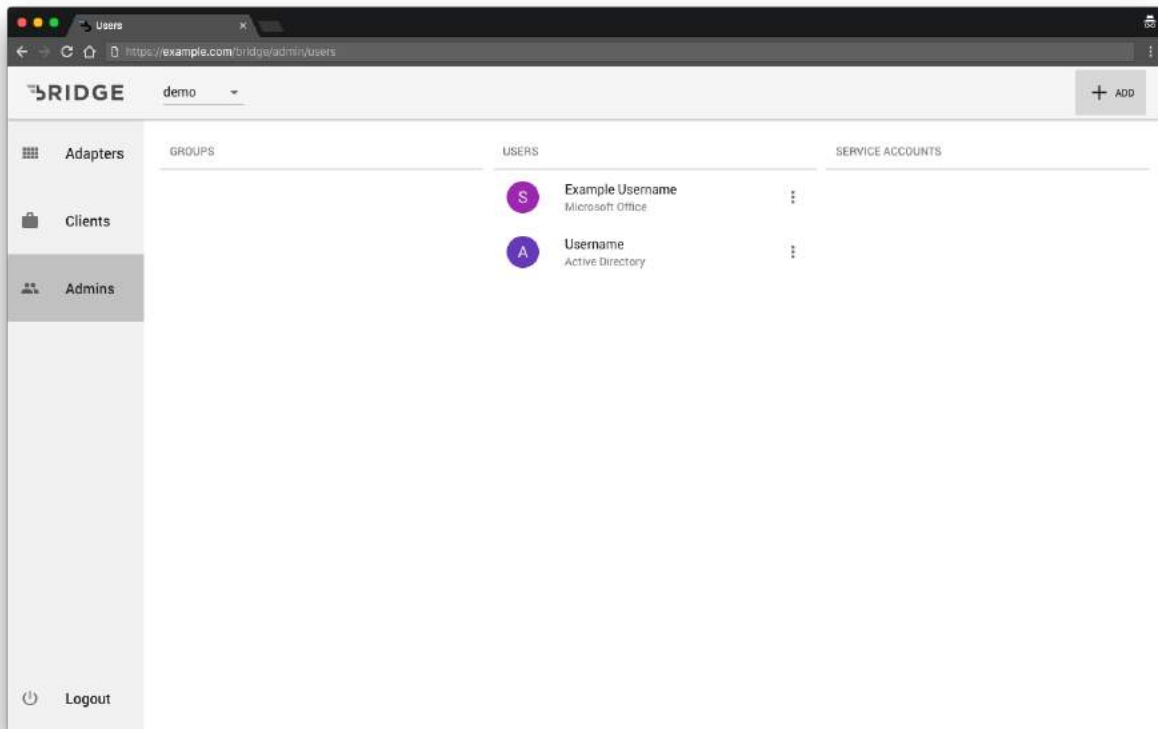


Administrators

Users or groups can be added as Bridge administrators.

Bridge administrator can add, edit and remove adapters, clients, service accounts and other administrators.

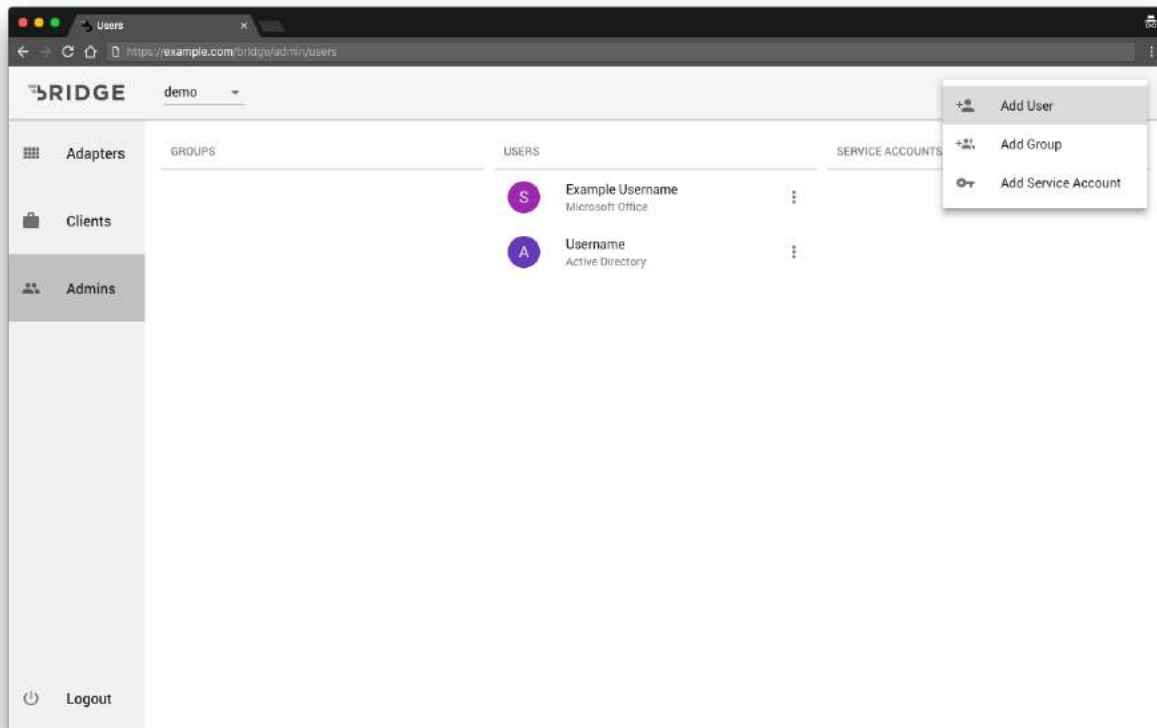
Click on the + **ADD** button in the top right hand corner of the screen.



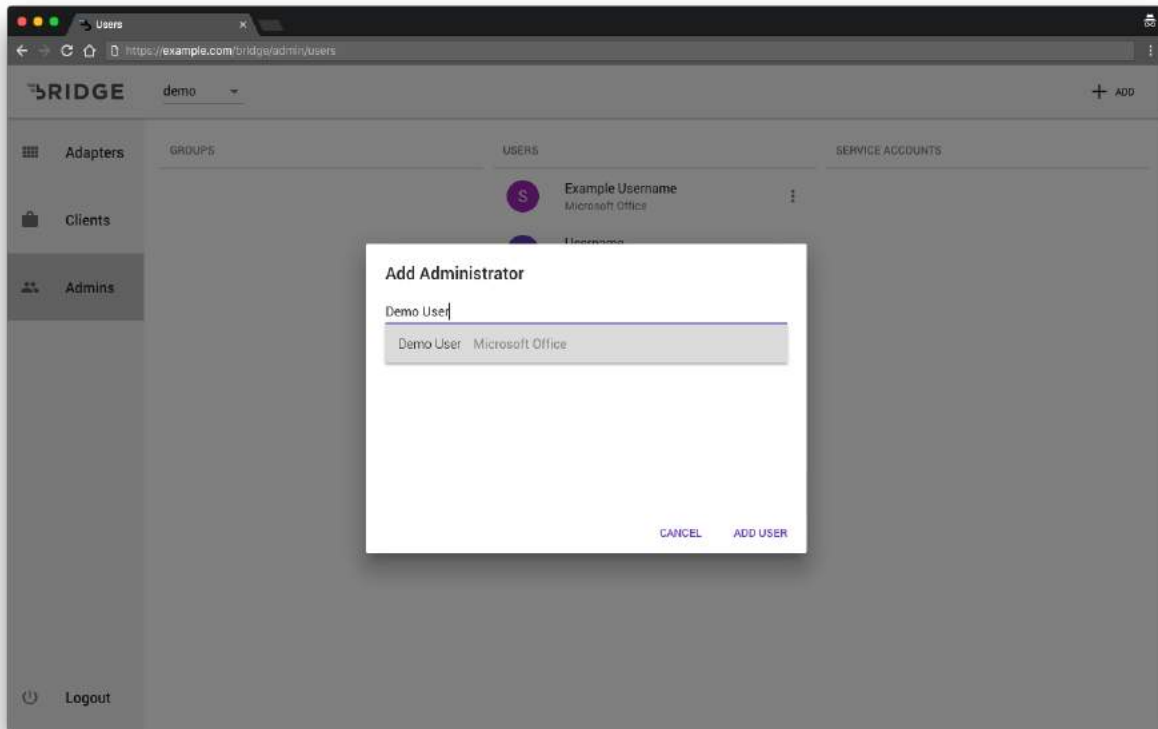
Users

Add User

Click on the + **ADD** button and clicking on the **Add User** option from the popup menu.

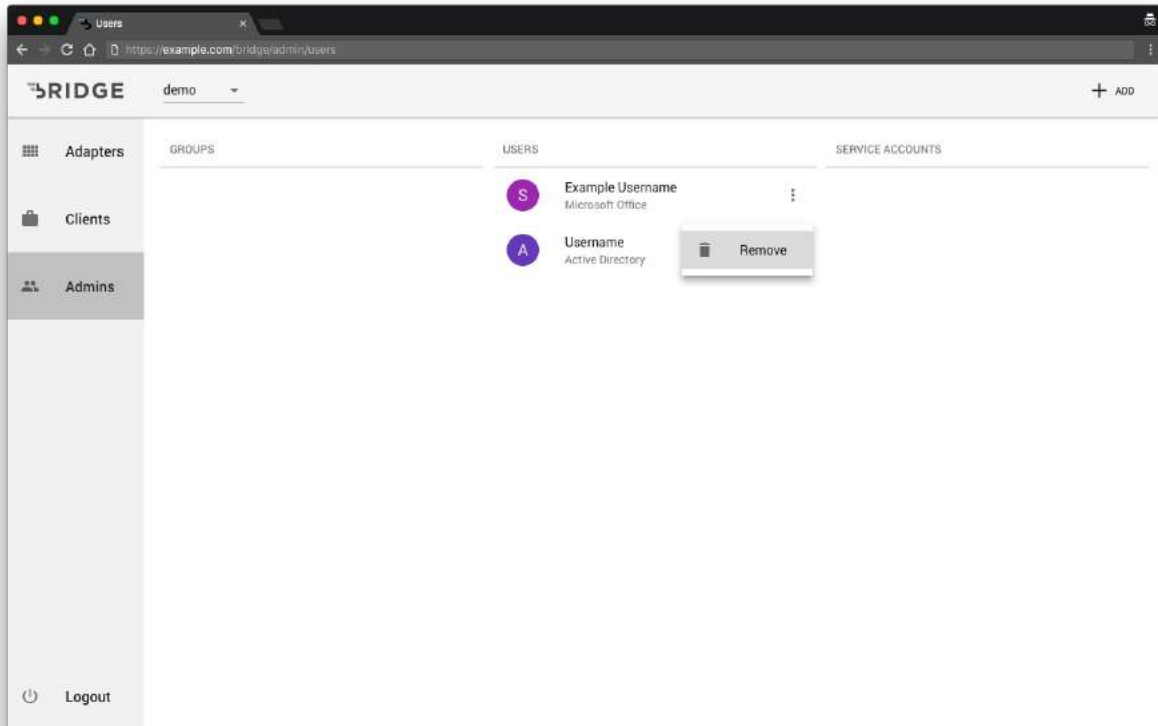


Search for user by name or email address and select one from the dropdown list. Click **ADD USER** to add the user to the application as an administrator.

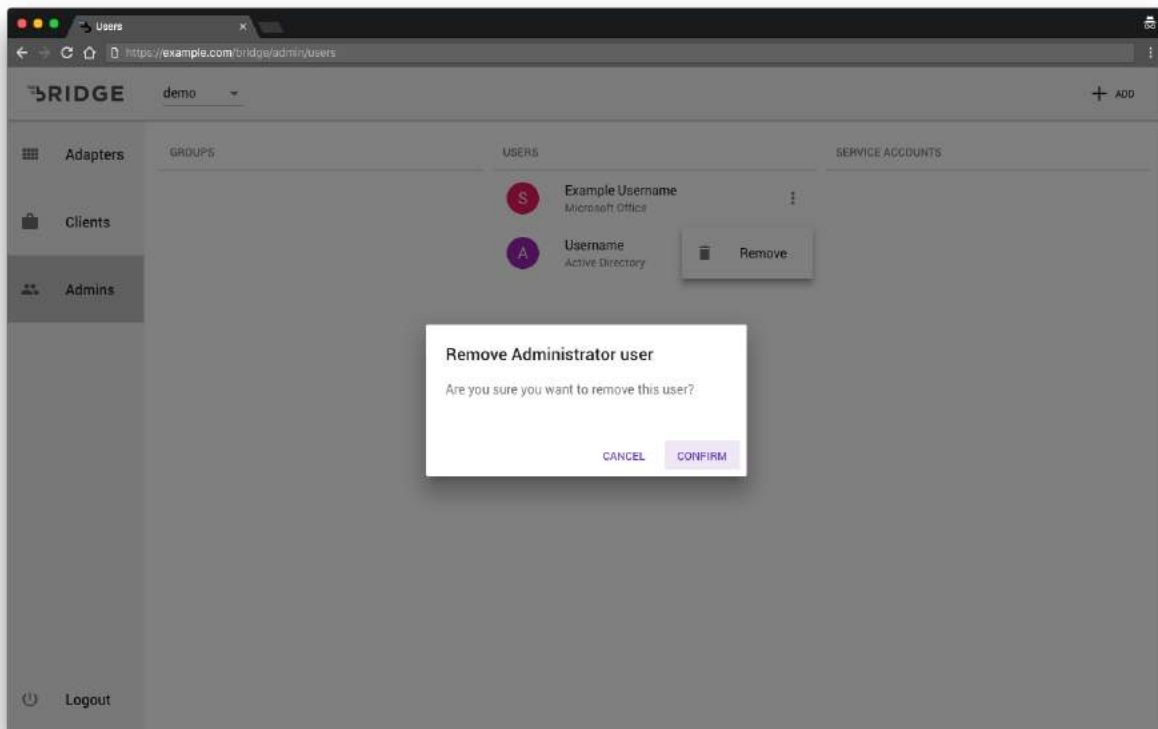


Remove User

Click on the **:** menu icon adjacent to the user then click the **Remove** option from the popup menu.



Click **CONFIRM** on the confirmation dialog to remove the user.

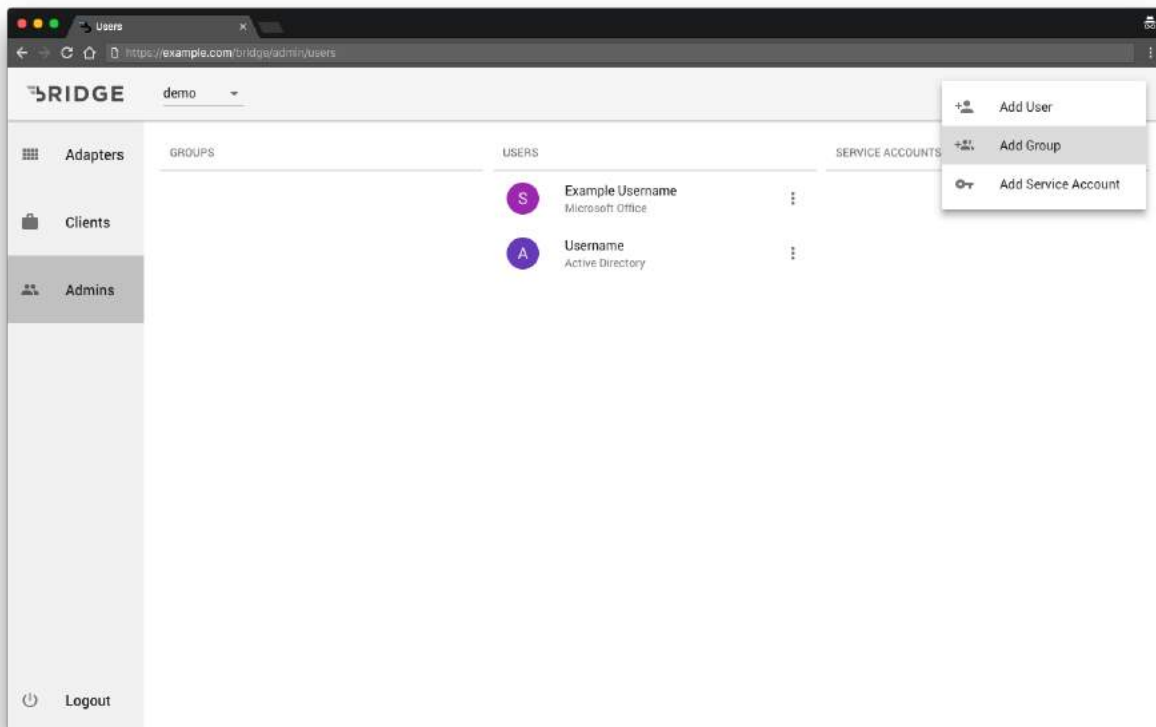


Groups

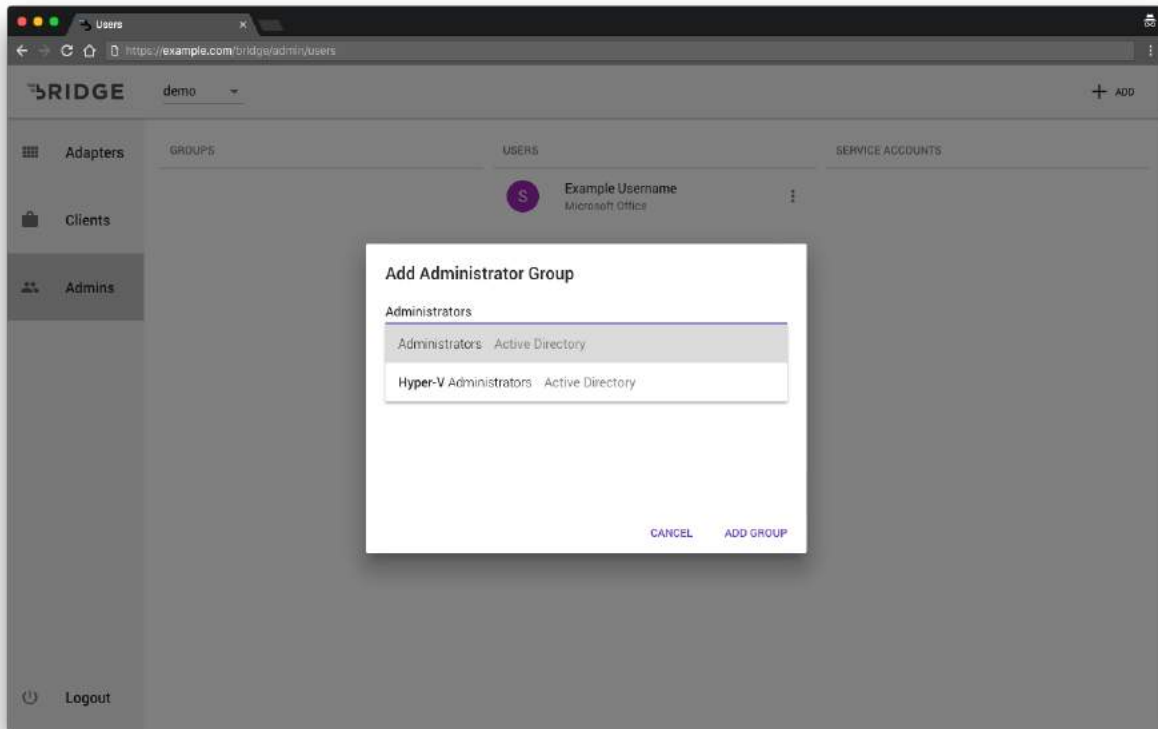
Add Group

Adding a group as an administrator to the Bridge application will give all the users that are part of the group administrative access to Bridge.

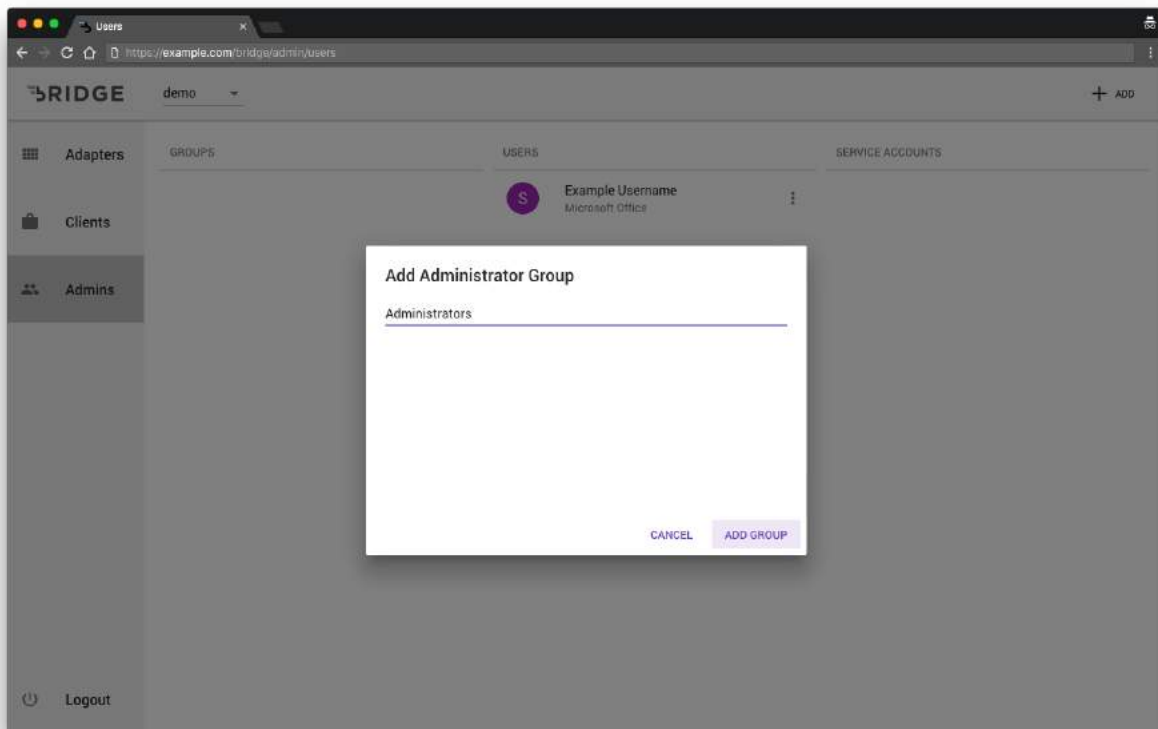
Click on the + **ADD** button in the top right corner of the screen and click **Add Group**.



Search by group name and select one of the group from the dropdown list.

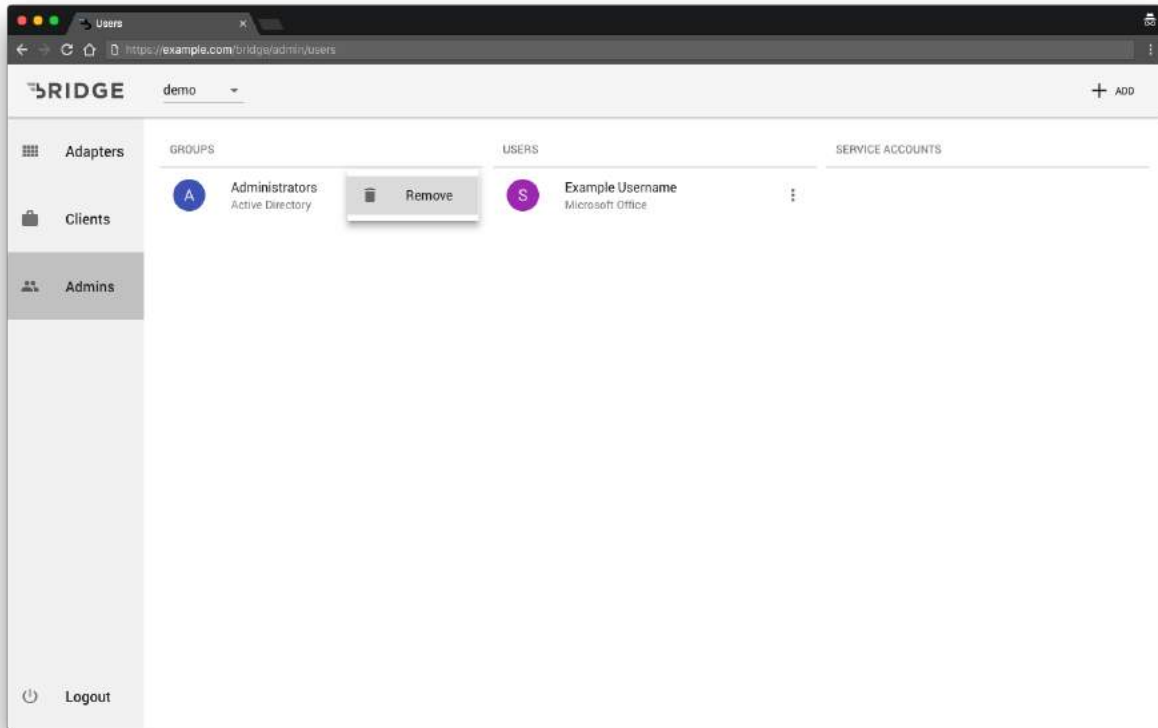


Click **ADD GROUP** to add the group to the application as an administrator.

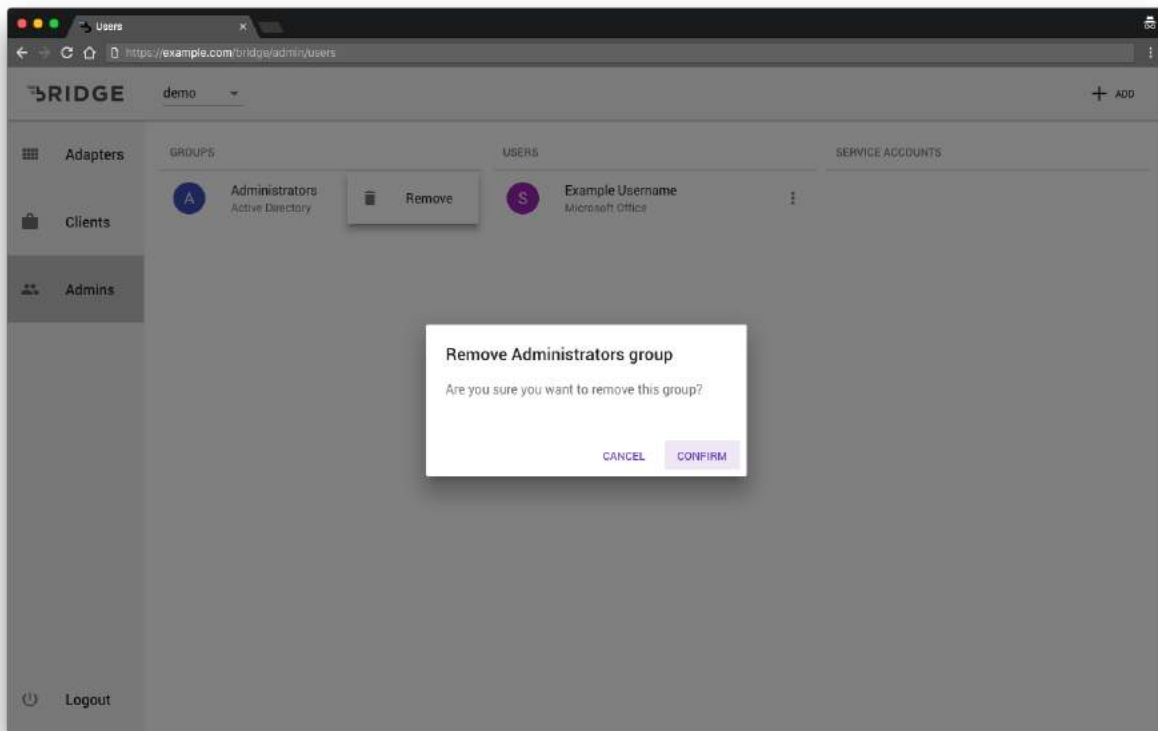


Remove Group

Click on the **:** menu icon adjacent to the group and click the **Remove** option from the popup menu.



Click **CONFIRM** on the confirmation dialog to remove the group.

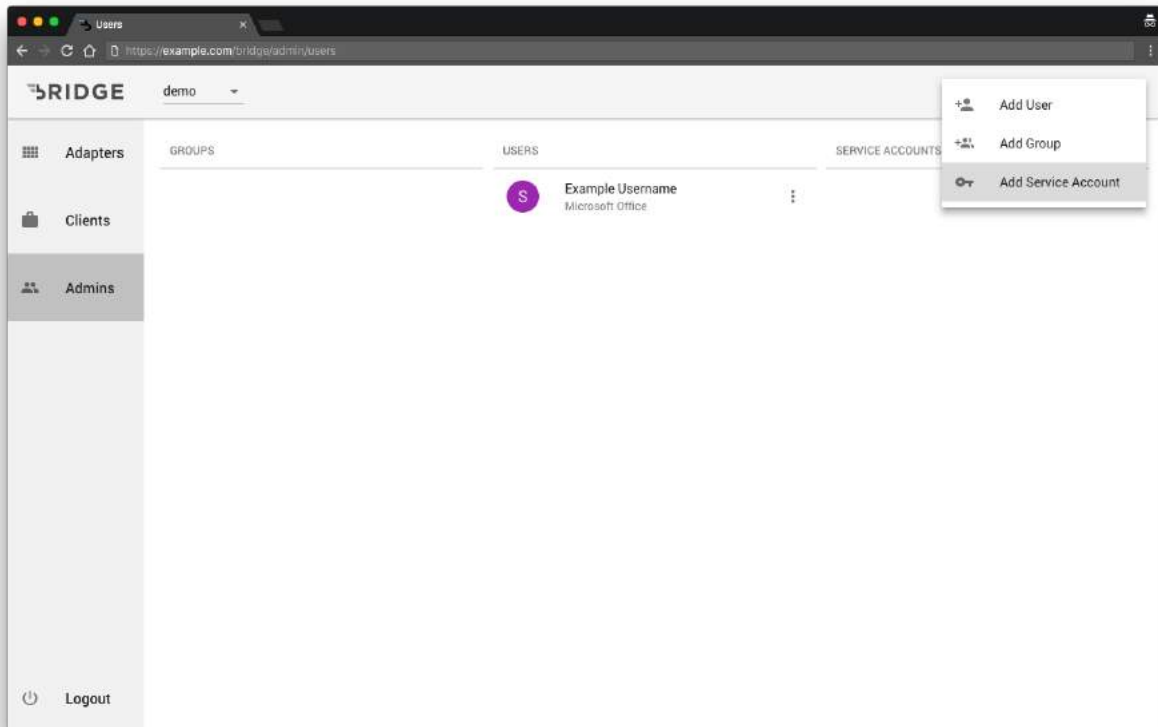


Service Accounts

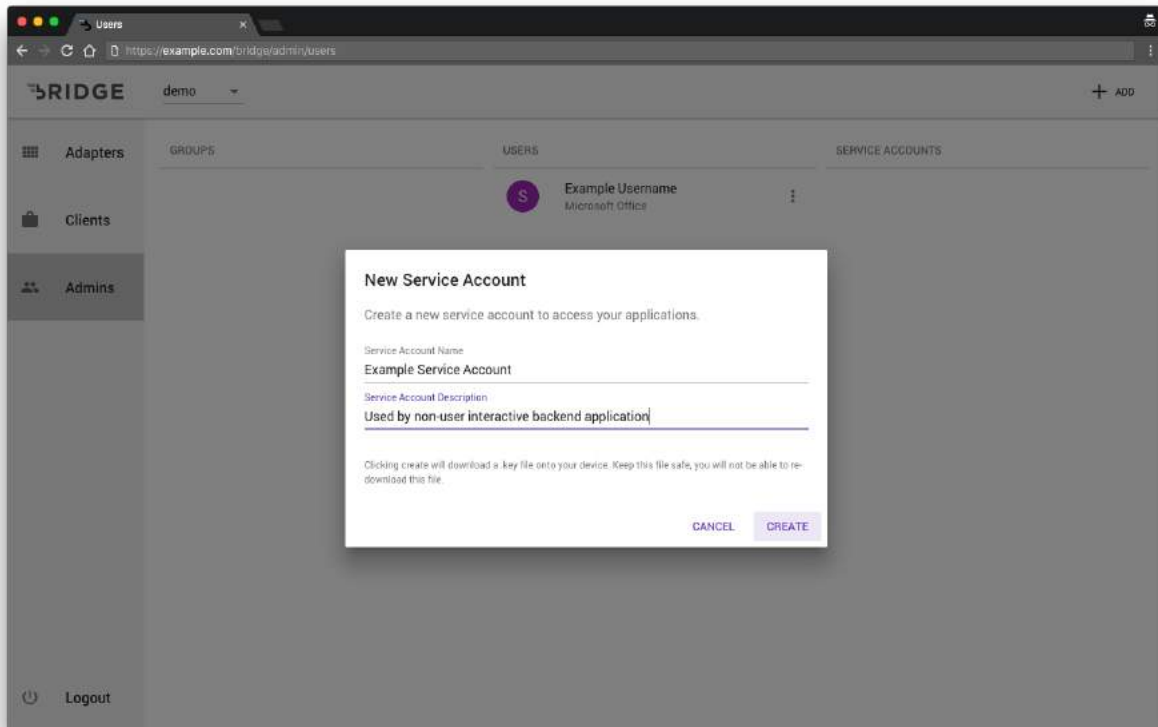
Service Account can be used by a third-party application to authenticate with Bridge application.

Add Service Accounts

Click on the + **ADD** button on the top right corner of the screen and click **Add Service Account**.



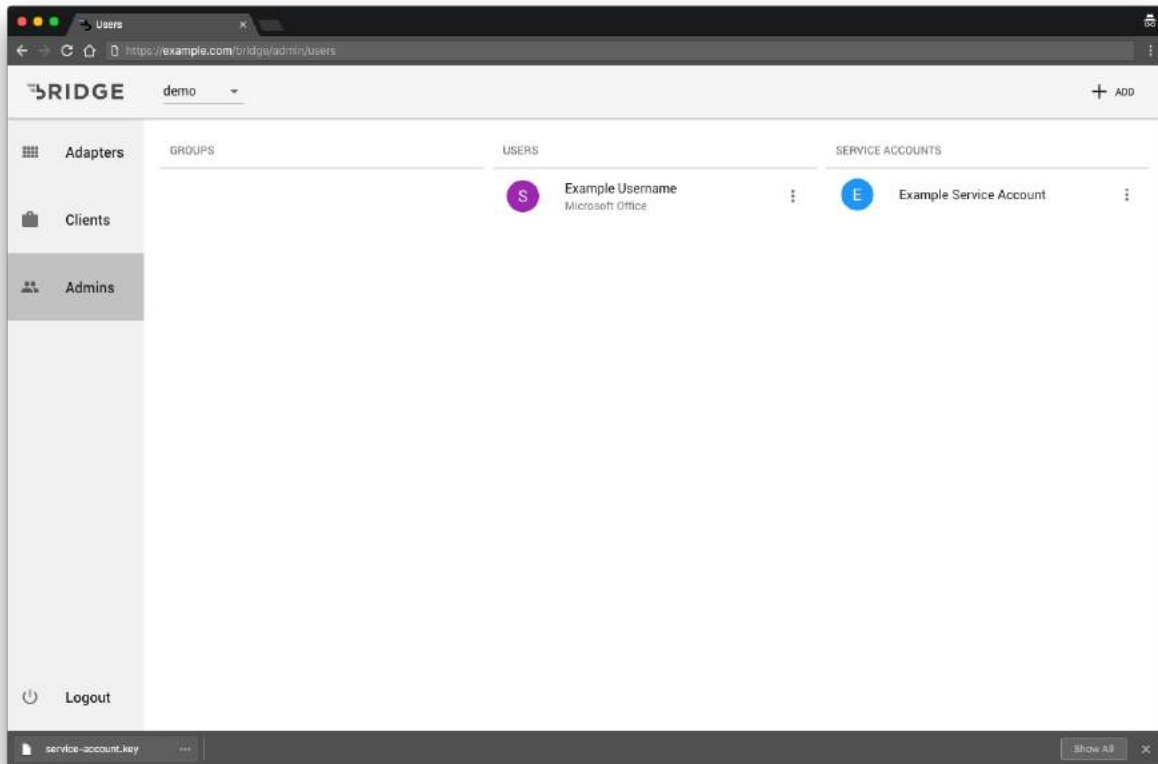
Enter a **Name** and **Description** and click **CREATE** to add the new service account to the application.



After creating the Service Account, a file called **service-account.key** is automatically downloaded onto your computer. This file is used by other applications to authenticate with Bridge.


WARNING

Do not misplace the **service-account.key** file. It cannot be recovered under any circumstances.



The **service-account.key** file if opened in a text editor should be in JSON format with the following keys,

- uuid
- name
- privateKey
- applicationUuid
- clientId
- url



```
{ "uuid": "9e2768ea-0f81-4a45-afbb-d51ea3842c26", "name": "Example Service Account", "privateKey": "-----BEGIN RSA PRIVATE KEY-----\nMIIBOQIBAAJBAK3ADmU9l6sEWqATwNnq6YWF7UWM17hxHiYYun4yFocAMQ2Isjg\nUqs052jxC5c0KEIjgwZkdAZSh3UhbGMnHuscAwEAAQJALjyNmCNr2Pavpymai\nGMB\nnAY0x1N6zj0xHfFARANJR3qh/A78W07Linfb2QQ4K60gZxn2U2T/J5xCQ77Vf6iB1\nnAQIhAPe/rqwsGcLTKCIZsnKJyM/\neyK+VsxLawtbkFvTc3Y6nAiEAs4l1d6DeiuYu\nnz9so0JPzfcB8tuvtdUSJs2GBJDEHGh0CIGFt61ZgPX1FpxnJ+0hZ8TP2S/vpJjQ6\n/baemnyPQZ4vAiAcZFSLQolu9c/ZVxMxSPRsopAWbWDz9o7AK1881f0FkQIgXWtf\nnNGuZEO+mR4Mjzq50HVogRi46PCFtnXXs7I/LXM=\n-----END RSA PRIVATE\nKEY-----", "applicationId": "61ac0f25-b6f0-460d-b646-7234794b3396", "clientId": "9c373062-aae9-489e-8648-\ne4c1e799ca07", "url": "https://example.com" }
```

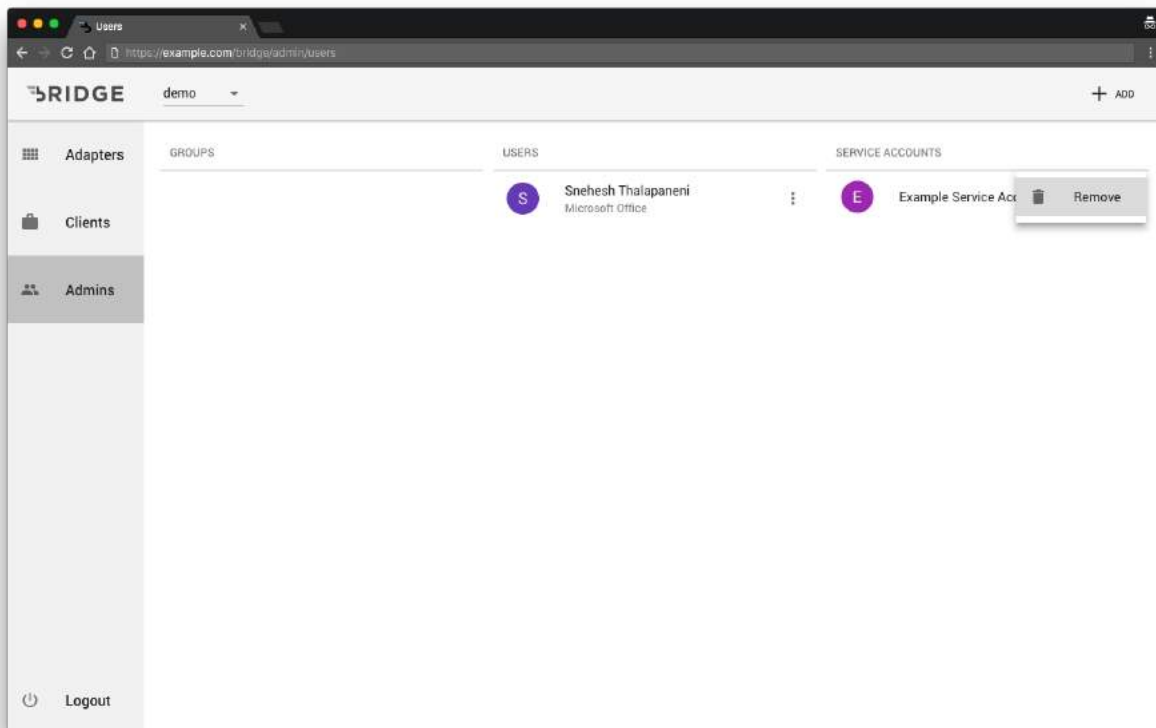
Remove Service Accounts

Click on the **:** menu icon adjacent to the Service Account and click the **Remove** option from the popup menu.

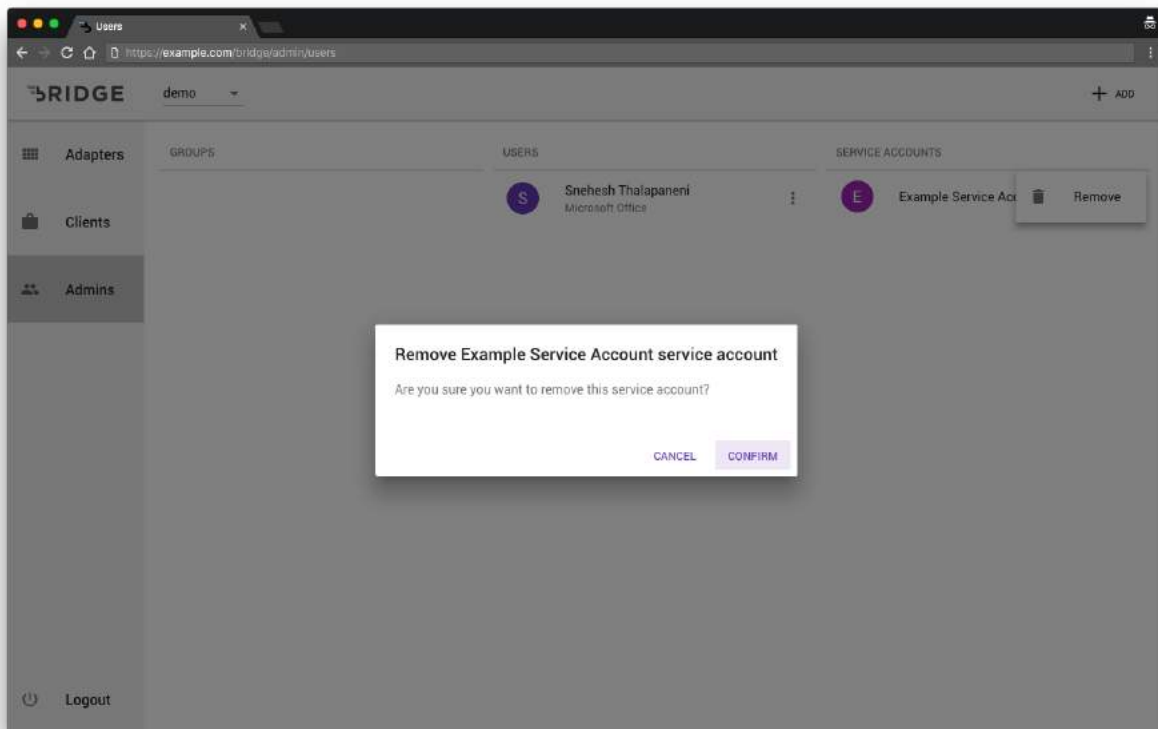
Removing the Service Account will result in deauthorizing all the applications that rely on the Service Account to communicate with Bridge.

WARNING

This action is not reversible.



Click **CONFIRM** on the confirmation dialog to remove the Service Account.



Kerberos Integration

Whitelist Hostname

Add Server Hostname to the Site to Zone Assignment List in Group Policy to ensure hostname is trusted to allow kerberos authentication.

Service Principal Name (SPN)

Service Principal Name (SPN) is a unique name used by the clients to identify themselves when connecting to the Key Distribution Center (KDC) in a Windows domain.

SPN has to be constructed based on the protocol, server hostname, Active directory domain. For web servers, SPN has to be in the following format,

HTTP/<Server Hostname>@<Active Directory Domain>

For example, If the hostname of the web server is **band.example.com** and Active Directory domain is **Example.com** then the SPN should be,

HTTP/band.example.com@EXAMPLE.COM

Keytab

A Keytab file contains Service principal name and encryption keys necessary for decrypt Kerberos tickets.

Keytab is used by Bridge to authenticate users with the Active Directory server. Generate a keytab requires the following information,

- User Account with non-renewable passwords
- Bridge Hostname
- An Active directory administrative account to generate the keytab

Launch a PowerShell in the Active Directory server as an administrator and run the following command.

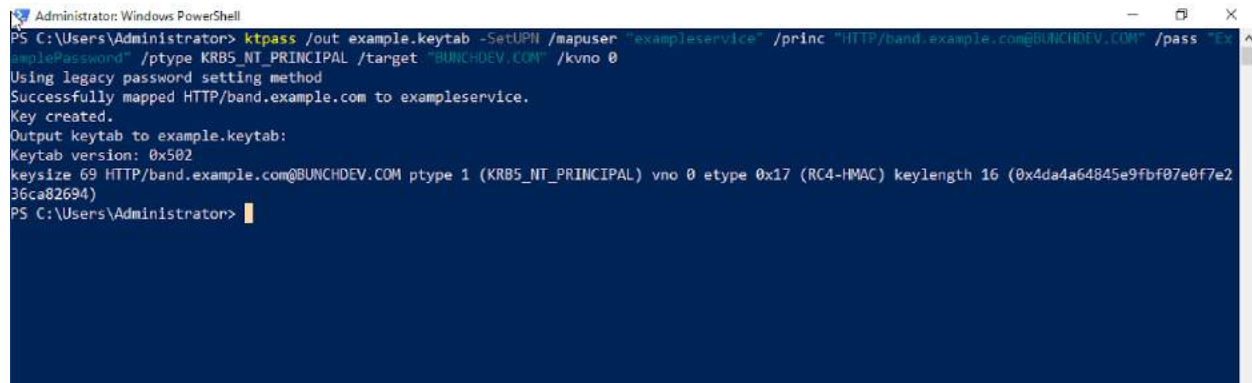
```
ktpass /out example.keytab -SetUPN /mapuser "exampleservice" /princ  
"HTTP/band.example.com@AD.EXAMPLE.COM" /pass "ExamplePassword" /ptype  
KRB5_NT_PRINCIPAL /target "AD.EXAMPLE.COM" /kvno 0
```

/out	- Output path of the keytab file
-SetUPN	- Set attribute userPrincipalName.
/mapuser	- Name of the Active Directory account.
/princ	- Service Principal name
/pass	- Password for the Active Directory account
/ptype	- Service Principal type
/target	- Active Directory Domain
/kvno	- Key version number

Backup the **example.keytab** file generated after the command runs successfully.

For example, If the Active Directory server is **BUNCHDEV.COM**, Command for generating a keytab for the service with hostname **band.example.com** and **exampleservice** Active Directory account would be,

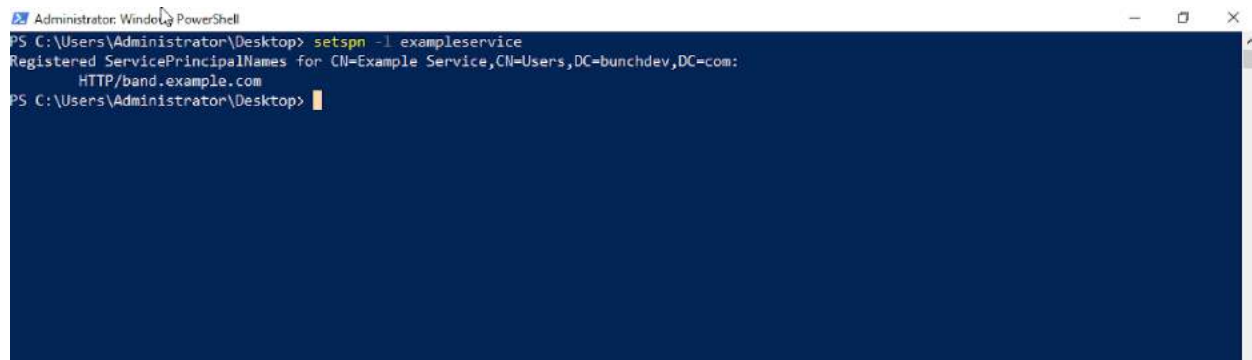
```
ktpass /out example.keytab -SetUPN /mapuser "exampleservice" /princ "HTTP/band.example.com@BUNCHDEV.COM" /pass "ExamplePassword" /ptype KRB5_NT_PRINCIPAL /target "BUNCHDEV.COM" /kvno 0
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ktpass /out example.keytab -SetUPN /mapuser "exampleservice" /princ "HTTP/band.example.com@BUNCHDEV.COM" /pass "ExamplePassword" /ptype KRB5_NT_PRINCIPAL /target "BUNCHDEV.COM" /kvno 0
Using legacy password setting method
Successfully mapped HTTP/band.example.com to exampleservice.
Key created.
Output keytab to example.keytab:
Keytab version: 0x502
keysize 69 HTTP/band.example.com@BUNCHDEV.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x17 (RC4-HMAC) keylength 16 (0x4da4a64845e9fbf07e0f7e236ca82694)
PS C:\Users\Administrator>
```

Verify SPN is mapped to the Active Directory account **exampleservice** with the following command,

```
setspn -L exampleservice
```



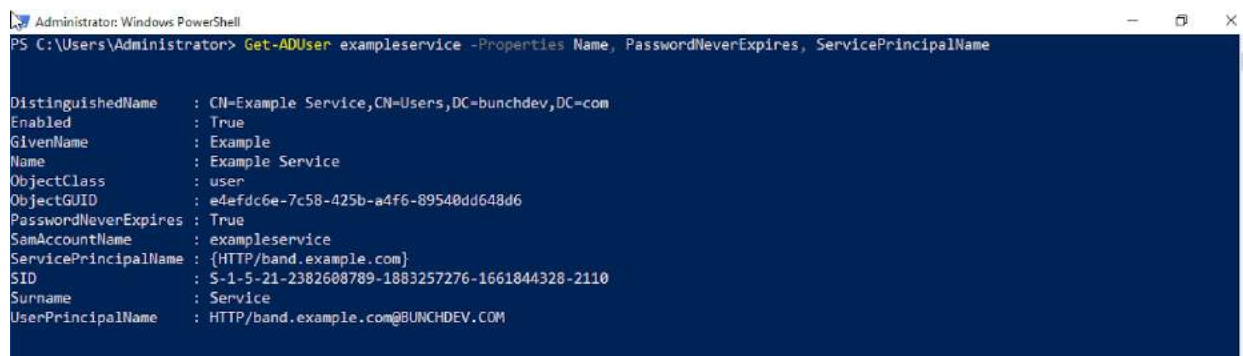
```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop> setspn -L exampleservice
Registered ServicePrincipalNames for CN=Example Service,CN=Users,DC=bunchdev,DC=com:
HTTP/band.example.com
PS C:\Users\Administrator\Desktop>
```

Verify Password expiration, Service Principal Name of the Active Directory account by running the following command,

```
Get-ADUser <Active Directory account> -Properties Name,  
PasswordNeverExpires, ServicePrincipalName
```

For example, If Active Directory account name is **exampleservice** and Service Principal Name is **HTTP/band.example.com@BUNCHDEV.COM**,

```
Get-ADUser exampleservice -Properties Name, PasswordNeverExpires,  
ServicePrincipalName
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADUser exampleservice -Properties Name, PasswordNeverExpires, ServicePrincipalName

DistinguishedName : CN=Example Service,CN=Users,DC=bunchdev,DC=com
Enabled           : True
GivenName        : Example
Name             : Example Service
ObjectClass      : user
ObjectGUID       : e4efdc6e-7c58-425b-a4f6-89540dd648d6
PasswordNeverExpires : True
SamAccountName   : exampleservice
ServicePrincipalName : {HTTP/band.example.com}
SID              : S-1-5-21-2382608789-1883257276-1661844328-2110
Surname          : Service
UserPrincipalName : HTTP/band.example.com@BUNCHDEV.COM
```