ServiceTitan®

Manage client ID & secret

Client ID & Secret key management

To access ServiceTitan APIs, your App must supply a Client ID & Secret key pair. As an App developer you can produce these or have your Tenant admin produce and configure. Note: Each Tenant ID requires its own unique Client ID and Client Secret key pair. Additionally, the Client ID, Client Secret, and Access Token are specific to their respective environments.

If you are an app developer (including a third-party organization), you must generate the Client ID and Secret Key directly from the developer portal after the tenant (admin) enables your app. Follow the steps below:

New Applications

1. Login to the Developer Portal

2. Select "My Apps" at the top of the page

3. Select "+ New App"

4. Fill all the required fields and scopes

5. Under "Client Credentials Management", select "I, the app developer, will configure the credentials on behalf of each tenant"

6. Click "Create App"

Existing Applications

1. Login to the Developer Portal

2. Select "My Apps" at the top of the page

3. Click "Edit" on your application

4. Under "Client Credentials Management", select "I, the app developer, will configure the credentials on behalf of each tenant"

5. Click Save

<u>Generating a Client Secret</u>

If you haven't done so already, please add the client's Tenant ID to your application. Once the Tenant Admin has allowed access and connected to your application through their "API Application Access" settings, you can begin the process of obtaining the tenant's client ID and client secret in your developer portal:

1. Login to the Developer Portal

2. Select "My Apps" at the top of the page

3. Click "View Connections" for your app

4. Click "Generate" under Client Secret to create a new Client Secret

5. Reference the tenant's Client ID on this page as well

Note: Until the Application is Allowed by the Tenant admin, you will continue to see the status as 'Not Connected Yet' as the status. Please contact your Tenant Admin if you see this message and ask that they connect to your app.

If you are a tenant admin and want to generate Client ID & Secret key (for Zapier)

1. As a ServiceTitan admin, log into the ServiceTitan either in the integration or production environment.

   Note: Client ID & Secret Key are specific to the environment in which they are generated and should be used accordingly.

2. On the side menu, click Integrations>API Application Access.
   The Manage API Application Access page opens.

3. Click Connect New App. Existing apps, if any, are listed here.

   Note: If you don't see the app you want to connect to ask the developer of the app to add your tenant ID through the developer portal.

4. Choose the app to which you would like to connect.

5. The API scopes open (how the app wants to interact with your resources and data). You can choose to Allow or Decline access.

6. If you allow access, your Client ID & Secret Key are generated. Share the Client ID & Secret Key along with your Tenant ID to the app developer in a secure way. App developers will embed the Client ID & Secret Key into the app.

   Note: Enabling a Client ID and Secret Key and sharing it with an app developer means, you, as the admin (resource owner), are granting access to the app to operate on your resources (data).

Note: If you have multiple tenants, say X number of tenants, then you need to obtain X tenant specific Client ID & Secret pairs.

ServiceTitan Developer: If you are a ServiceTitan developer, you will only have access to a Client ID and Secret Key for the integration environment. You can use the Integration environment to test your app. If you are marketing your app to a ServiceTitan customer, you should obtain the Client ID and Secret Key from the customer who wants to use your app.

Upgrade an existing App version

1. Sometimes developers add or remove API scopes. Adding new API scopes means access to more data for an app developer.

    1. On the side menu, click Integrations>API Application Access. The Manage API Application Access page opens.

    2. Look for the New Version Available tag and the Upgrade to New Version button.

    3. Click Upgrade to New Version.

    4. The API scopes opens. This is how the app wants to interact with your resources and data. You may choose to Allow or Decline access.

        1. Newly added versions are highlighted in green. Removed versions are struck out.

    Click Allow to accept the API scope changes. You will see an upgrade success message. Click Decline if you do not accept the API scope changes.

    Note:You need not generate a new Client ID & Secret key after upgrading to a new version.

Disabling Client ID & Secret

If you have previously enabled a Client ID & Secret Key and for some reason you want to disable it, you can. By disabling, you are pausing the previously granted access to the developer. In this state, the app cannot access your resources. You will still have the ability to restore access.

To Disable the Client ID & Secret Key

1. From Manage API Application Access, select the app from the list of apps that you want to disable.

2. Click Disable>Confirm and Continue.