

[Documentation](#) → [Modules](#) → [Integrations](#) →

API Tokens



This article has been generated from the online version of the documentation and might be out of date. Please, make sure to always refer to the online version of the documentation for the up-to-date information.

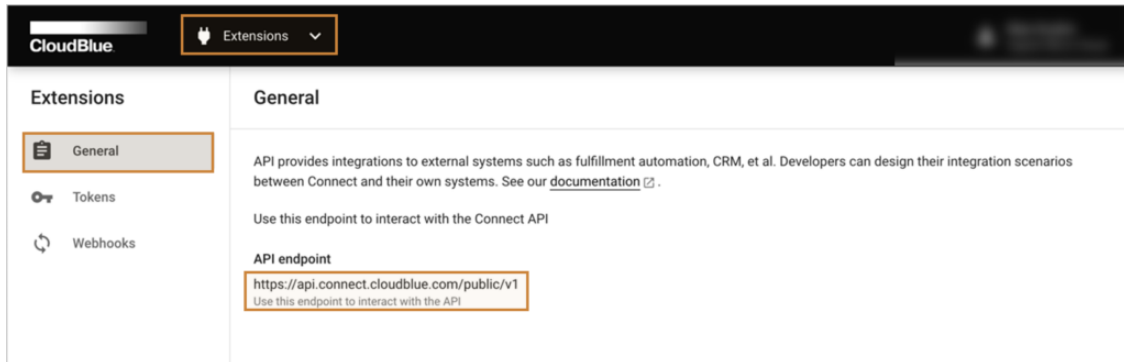
Auto-generated at January 16, 2021

CloudBlue

The Connect API requires API clients to authorize their HTTP requests through the **Authorization** header carrying a unique security token as the **ApiKey** argument. The Extensions module enables providers and vendors to generate such a token for every API client they want to use.

API Endpoint

On the **General** tab of the Extensions main page, you can find the Connect API endpoint URL:



This is the base URL to be used by all API clients interacting with Connect. Most examples in Connect documents omit this prefix for brevity. For example, to get a list of agreements, a sample request in documents looks as follows:

```
GET /agreements/
```

The above short call actually means:

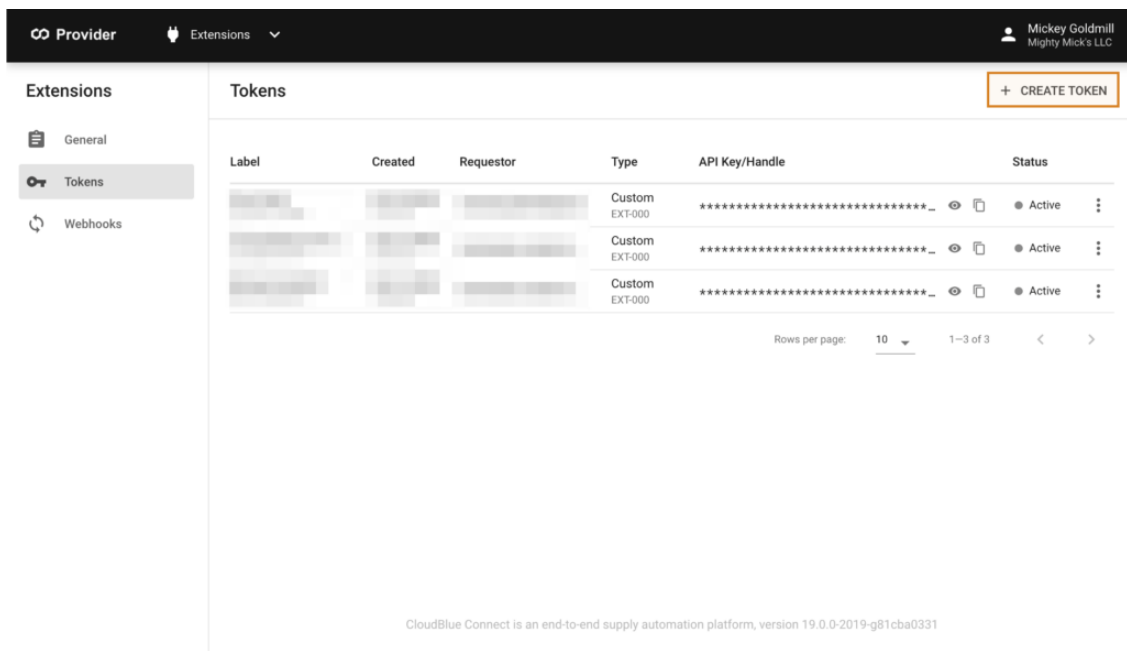
```
GET https://api.connect.cloudblue.com/public/v1/agreements/
```

Creating API Tokens

To create an API token in Connect, a provider or vendor must go through the following steps using the Extensions module.

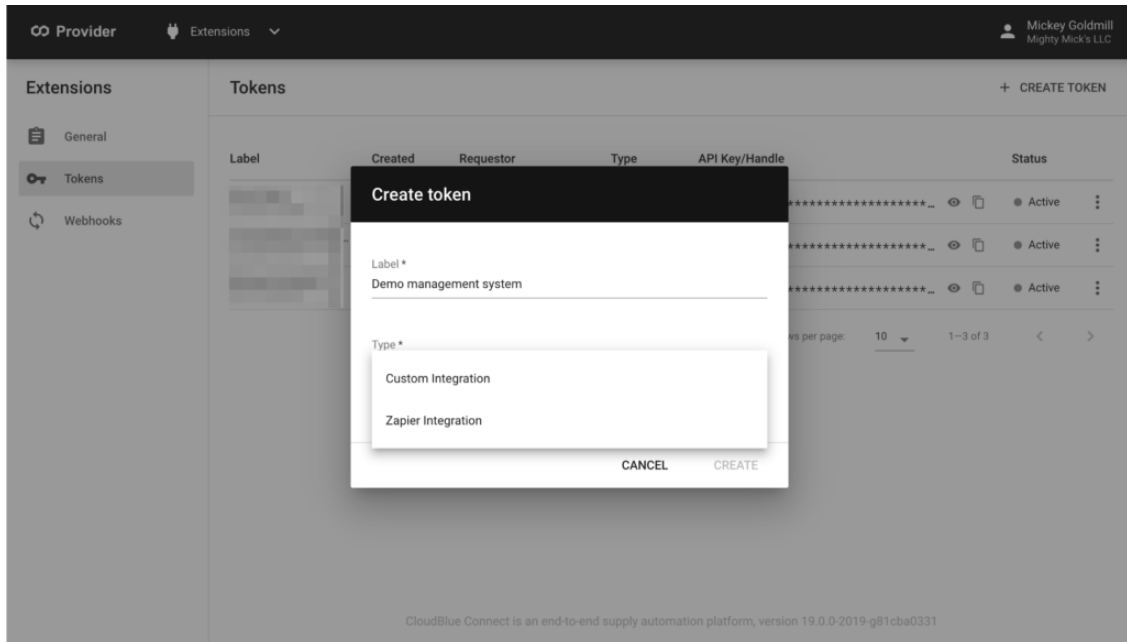
1. Start creating a token

On the Extensions main page, navigate to the **Tokens** tab and click the **Create Token** button on the top-right corner:



2. Specify the token properties

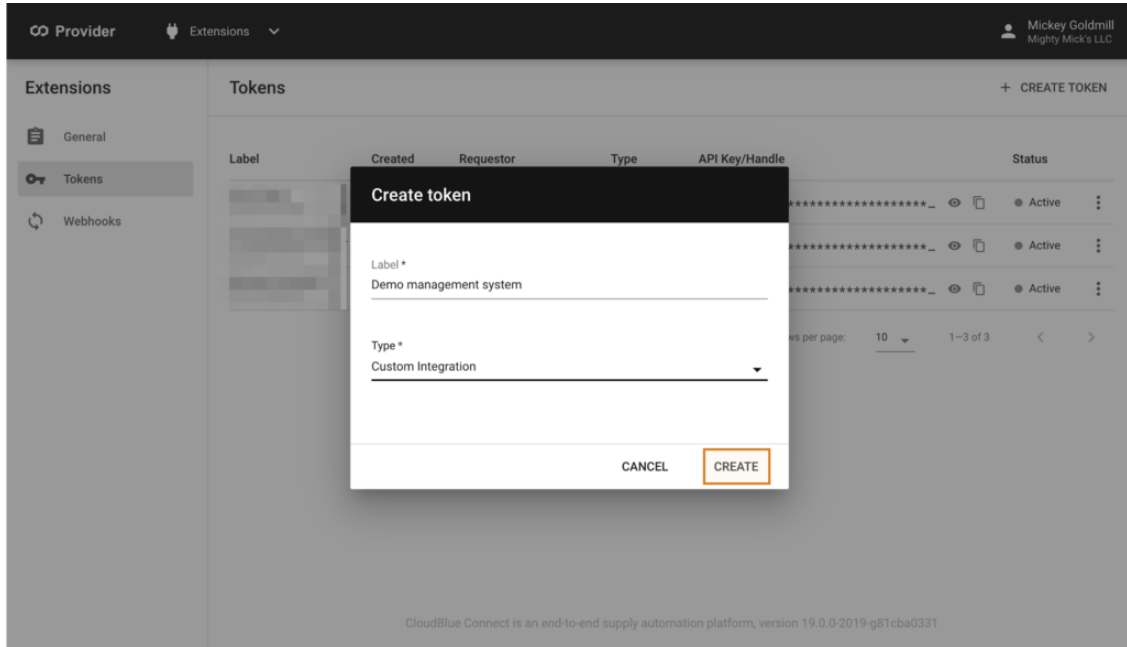
On the pop-up screen, specify the token properties:



- **Label:** enter a short descriptive name to distinguish this token from others.
- **Type:** from the drop-down box, select one on the following:
 - **Custom integration:** select this if you will use your token for an API client other than Zapier.
 - **Zapier:** select this if you will use this token to integrate Zapier with Connect.

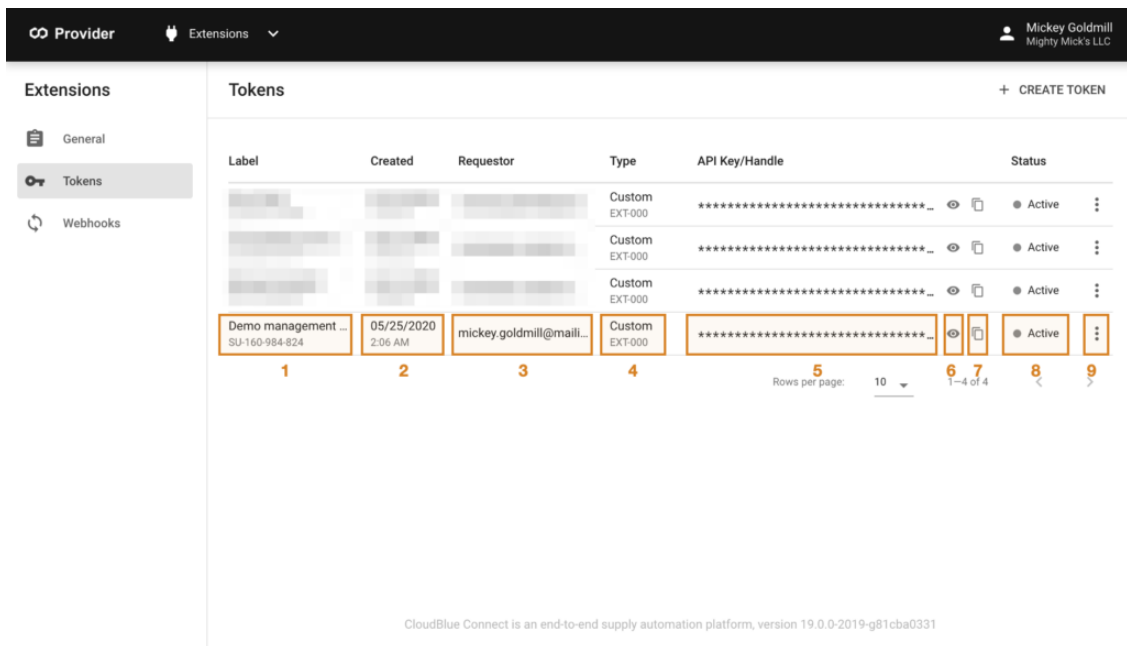
3. Complete token creation

Click **Create** to complete creation of the API token:



Token Management

In the list of API tokens, a token owner can watch and manage their API tokens.



The numbered parts of an API token the above image are used for the following purposes:

1. **Label** displays the API token label and internal ID.
2. **Created** displays the date and time when the token was created.
3. **Requestor** displays the email of the Connect user who created the token.
4. **Type** specifies whether the token is custom or created for Zapier.
5. **API Key/Handle** is the value to be used in the **Authorization** header of requests that the corresponding API client will be sending to Connect.
6. The **Eye** icon is used to show or hide the **API Key/Handle** value.
7. The **Copy** icon is used to copy the **API Key/Handle** value to the clipboard.
8. **Status** indicates the current status of the token.
9. The **"..." (vertical ellipsis) menu** provides the option to **delete** the token. The deletion needs to be confirmed in an additional popup.

Using API Tokens

To use a particular API token for Connect API authentication, copy the **API Key/Handle** value from the corresponding API token and use it in the HTTP **Authorization** header of API requests as in the following example (the **ApiKey** value is cut for brevity):

```
GET /agreements/  
Authorization: ApiKey SU-160-984-824:8c8e87f858cb70370
```



Note

An API token does not expire until you delete it.

For more details about the Connect API, refer to REST API.