Working with 2tCloud APIs

Setting up an API Key

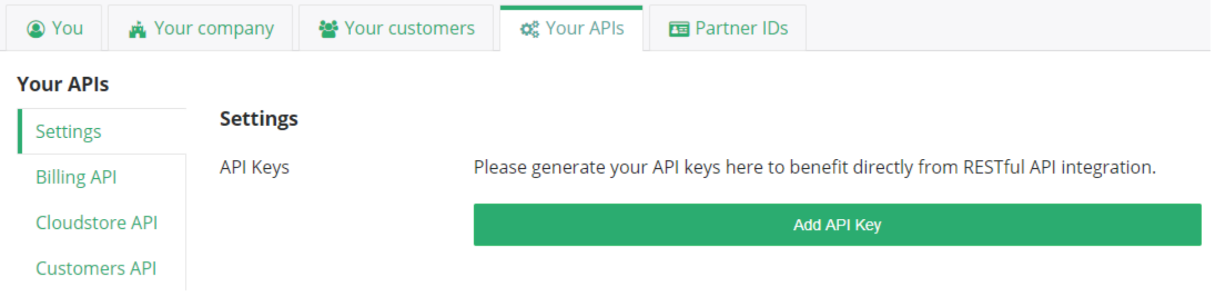
Once you have decided to start using a 2tCloud API the first step is to create an API key.

Creating an API key is a self-service service that can be used by any user that has the administrator role or API administrator permission attached to his account on the 2tCloud support center portal (https://2tcloud.supportcenter.services).

In order to request an API key log in to 2tCloud support center with your platform account. Navigate to the profile section and click the "Your APIs" tab. The "Settings" tab should now open and if you have sufficient permissions it will give you an "Add API Key" button as shown in the screenshot below.

If your account does not have sufficient permissions and you are not sure who the administrator is within your company, please log in to 2tCloud support center and visit the "Your company" → "Users" tab in the profile section. The admin users will be listed on top of the users table and will show "Admin" in the "User Type" column.

If you prefer you can also request the admin(s) of your company to change your account to admin or just assign the "API administrator" role to your account. Once that is done you will be able to create an API key by yourself.



Please generate your API keys here to benefit directly from RESTful API integration.

Assuming you do see the "Add API Key" button and you clicked it, you will now get a dialog that allows you to select the following options:

- API Name : The name of the API that you want to generate a key for
- Key Type : The type of key you want to generate
- Key Label : An optional label for your key
- IP Address : The (external) IP address of the server that will call the API with this key

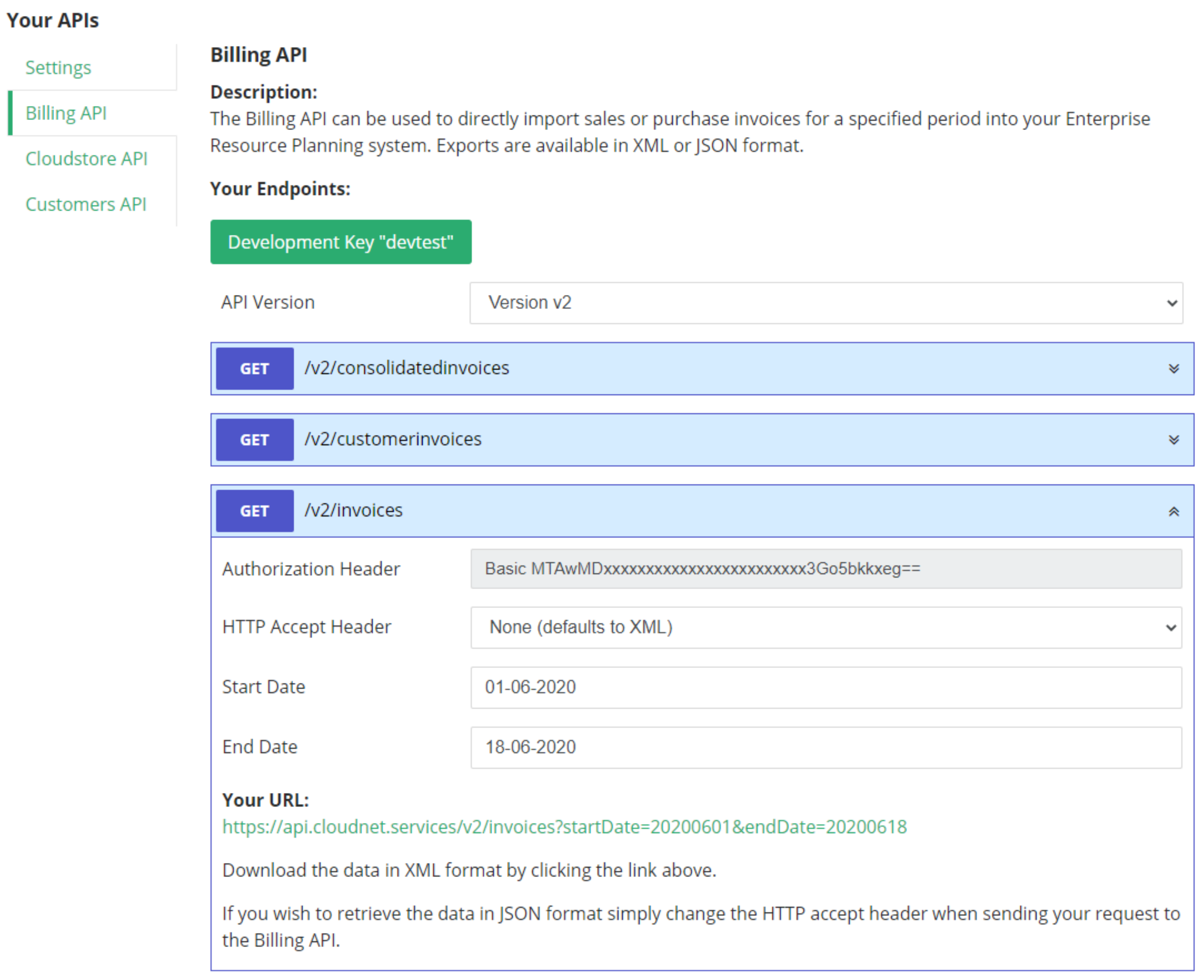
Once you have selected the right options and provided an IP address, you can click "Generate Key". Please note that the IP address you provide is the only one that is allowed to call endpoints with this API key. If your IP address changes you can log in to the support center portal and update it as a self-service once again.

After pressing "Generate Key" a message will appear to confirm that your key was generated successfully.

For most APIs (except the Cloudstore API) your API key becomes active immediately.

Working with the endpoints

Once you have an active API key and visit the tab for the corresponding API, that tab will show all endpoints that are available to you. You can toggle the endpoint URL to get more details about that endpoint and in some cases even actually call that endpoint to check the response you can expect.



Billing API

Description:
The Billing API can be used to directly import sales or purchase invoices for a specified period into your Enterprise Resource Planning system. Exports are available in XML or JSON format.

Your Endpoints:

API Version: Version v2

GET /v2/consolidatedinvoices

GET /v2/customerinvoices

GET /v2/invoices

Authorization Header: Basic MTAwMDxxxxxxxxxxxxxxxxxxxxxxxxx3Go5bkkxeg==

HTTP Accept Header: None (defaults to XML)

Start Date: 01-06-2020

End Date: 18-06-2020

Your URL:
https://api.cloudnet.services/v2/invoices?startDate=20200601&endDate=20200618

Download the data in XML format by clicking the link above.

If you wish to retrieve the data in JSON format simply change the HTTP accept header when sending your request to the Billing API.

The expanded section will show the value of your HTTP Authorization header and the supported values for the HTTP Accept header. When you hover over the "Authorization Header" value with your mouse you will see the decoded base64 value that was used to create it. The next paragraph "creating the authorization header" will explain how the value for this header is created in more detail.

In some cases (e.g. billing API and customers API) you will be able to actually call the endpoint by clicking on the URL it creates for you. For some other APIs (e.g. cloudstore API) only a sample of the request body will be shown, but no actual request can be fired from within the support center portal.

It is important to note that the endpoints that are part of any given API (e.g. Customers, Billing, Cloudstore) always act as a single, versioned, collection. You can choose the version to use by changing the {version} part of the endpoint URL to your desired version (e.g. V1, V2, …).

By default the endpoints that are shown on the API tabs in the "Your APIs" section default to the latest version, but you can use the "API Version" dropdown in this screen to see which other versions are available or select "no version selected" to see where the {version} is substituted into the endpoint URL.

Just make sure that at any given time you are using the same version for all endpoints belonging to a single API.

Mixing versions of endpoints is not supported by 2tCloud and may lead to unexpected behavior. It is however ok to user different versions between different APIs, e.g. using version v1 for the Cloudstore API while using version v2 for the Billing API is perfectly fine.

Creating the authorization header

With every request you need to send an HTTP Basic Authentication header. For your convenience you can find the actual base-64 encoded value for this header in the expanded view of any endpoint within the 2tCloud support center portal (see previous paragraph).

Should you wish to generate this header by yourself, consider the following;

The value for this header consists of a base64 encoded string holding a username and a password. The "username" is your Account ID and the "password" is one of the active API keys for the API you want to call.

You need to create a string in this format: {accountID}:{ApiKey} (substitute {…} with the actual value) and encode that in base-64 format, then put the word "Basic " (notice the trailing space) in front of it. You can find your Account ID in the profile section under the "Your company" → "Information" tab and your API key can be found on the "Your APIs" → "Settings" tab.

To authorize your request you need to make sure that you send the request from the IP number that is linked to the API Key that you are using in the Authorization header. If the IP number a request is coming from is not linked to the API key contained in the Authorization header your request will not be authorized and a HTTP status code 403 (Forbidden) will be returned.

Calling an endpoint

All endpoints are available on the https://api.cloudnet.services domain.

When calling an endpoint you need to consider the following:

- Use the right HTTP verb, currently all API endpoints use either GET or POST.
- All POST endpoints expect a request in JSON format only.
- Sending an "Accept" HTTP header is optional:
    - Customer and Billing API endpoints support both XML and JSON responses. When no "Accept" header is provided it will default to XML, but if you provide an "Accept" header with value "application/json" you will receive the response in JSON format.
    - Cloudstore API endpoints currently only support JSON, providing an "Accept" header is not useful as all Cloudstore API endpoints default to JSON.
- You need to send an HTTP Basic Authentication header to authenticate your request.
- Make sure the request is sent from the IP address that is attached to your API key. You can always update this IP address in the 2tCloud support center portal.
- Use the API key that belongs to the same API as the endpoint you are calling (e.g. when calling an endpoint that belongs to the Billing API, make sure you use one of your Billing API keys).
- Make sure you are using an "active" API key.

When you get a 403 (Forbidden) response it means that either you are not sending a valid HTTP Basic Authentication header or you are sending the request from a different IP address than the one that is attached to the API key you used in the header you are sending.

Both of these values can be verified from the applicable API tab in the "Your APIs" section of your profile on the 2tCloud support center portal.