Developer guidelines

API rate limits

Rate limiting is applied to the Companies House API to ensure a high quality service is delivered for all users, and to protect client applications from unexpected loops.

You can make up to 600 requests within a 5 minute period. If you exceed this limit, you will receive a `429 Too Many Requests` HTTP status code for each request made within the rest of the 5 minute time frame. At the end of the period, your rate limit will reset back to 600 requests.

If you have an application that requires a higher rate limit than this default, contact us. (https://find-and-update.company-information.service.gov.uk/help/contact-us)

Enumerated types

A majority of the resources returned by the Companies House API contain members that reference enumeration types. This helps the resources to be self-documenting, and allows clients to interpret the meaning of a resource member without needing to parse a text description.

Enumeration types are used to supplement or replace a text description. This allows clients to display their own version of a description or provide descriptions in multiple languages.

The collection of enumeration types used by Companies House are available on GitHub (https://github.com/companieshouse/api-enumerations). These files provide mapping between enumeration type and text description, and are divided into sets or classes. Each API resource member will define which class of enumeration is being returned.

A planned enhancement to the enumeration scheme is the provision of API endpoints that will return the enumeration class catalogue. This avoids enumerations having to be hard-coded within a client, and by periodically checking for change through ETags, clients do not have to download the full catalogue.

Data resources

Data is mostly returned as JSON documents. Your application must be able to handle the order of document members changing over time and expect to receive members it has not seen before.

Application security

The API can only be accessed over Transport Layer Security (TLS). We recommend using TLS 1.2.

API key security

It is important to keep your API keys secure. This will prevent them from being discovered, your account from being compromised and your rate-limit quota from being exceeded.

Do not embed API keys in your code

Storing keys in your application code increases the risk that they will be discovered, particularly if any of your source code is made public or it can be viewed by people who should not have access to the key. Instead, you should consider storing them inside environment variables or configuration.

Do not store API keys in your source tree

If you store API keys in files, for example, configuration or environment files, do not store them inside the application source tree. If all or part of the source is made public, the key may be compromised.

Restrict API key use by IP address and domain

Limit the use of a key to a specific IP address or domain to reduce its usefulness if it becomes compromised.

Regenerate your API keys

Regenerate your API keys regularly, including with each application release, to reduce the chance that a key will be discovered.

Delete API keys when no longer required

Remove unused keys from your registered applications page to limit the number of entry points into your account.
