API key authentication

Authentication for an API defines who has permission to access secure data or endpoints. This is especially important for APIs sharing sensitive information, APIs that allow end users to make changes, or for companies that charge some cost for accessing data via API.

API keys are just a long string of hexadecimal digits, i.e. 34d83d84f28d146aeae0e32f7803c88d, that can be sent instead of a username or password to authenticate access to an API endpoint. API keys are essentially the same as a set of username and password credentials, but they provide a layer of abstraction that is useful. For example, multiple end users could share a single API key.

Procedure

To replicate the process of hitting an endpoint with an API key in the URL or with request headers, supply the key and remember that if it ever changes you'll need to update your monitoring test's configuration as well. Different systems may accept API keys in different ways — for example, as part of the POST data instead of as a request header — so check with the API you are monitoring to understand how to properly transmit the API Key.

When using any type of direct authentication, it’s important that you also use SSL/TLS or https:// at the start of the API endpoint URL. Using SSL/TLS ensures that the HTTP basic authentication credentials or API keys aren’t exposed in the URL.

Next steps

You might be interested in other processes associated with the Monitoring API transactions use case.