HTTP basic authentication to an API

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.

HTTP basic authentication is a standard part of HTTP, and it can be used for API endpoints or any HTTP URL. You send a username and password — encoded together in base64 — as part of your request to the API. The benefit of HTTP basic authentication is that it’s easy to implement and is typically included in standard frameworks. On the downside, HTTP basic authentication offers no advanced options and may be easily decoded.

Procedure

The most common and reliable way to set up a monitoring request with HTTP basic authentication is to encode that username:password value in base64 and send that value over in an authorization header.

While it’s easy to encode usernames and passwords into base64, it’s also very easy to reverse or decode so that a system can authenticate a request. You can try this yourself with an online base64 encoder/decoder. Because base64 is so accessible, it’s important to protect this type of direct authentication with SSL/TLS.

Next steps

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