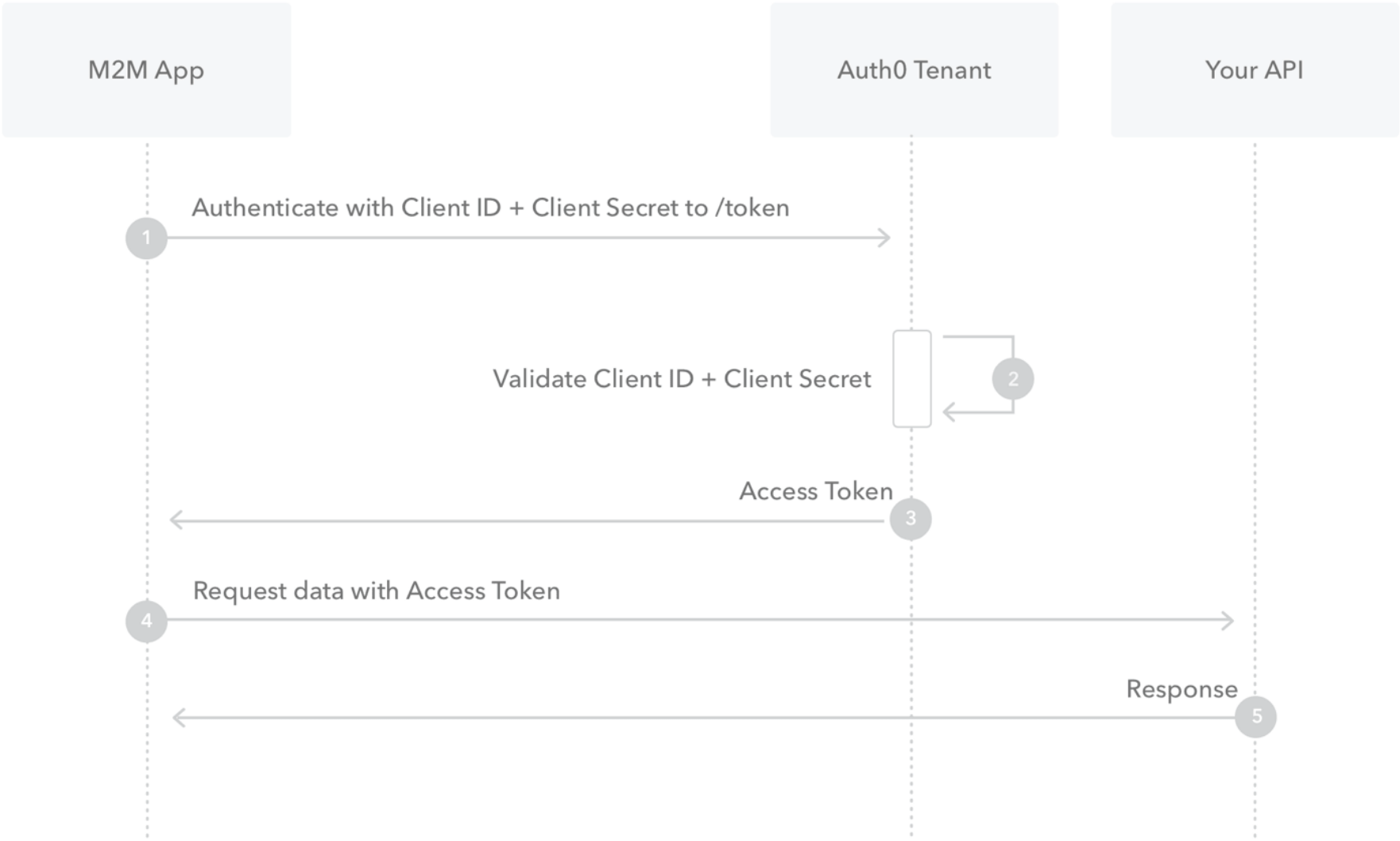
Client Credentials Flow

With machine-to-machine (M2M) applications, such as CLIs, daemons, or services running on your back-end, the system authenticates and authorizes the app rather than a user. For this scenario, typical authentication schemes like username + password or social logins don't make sense. Instead, M2M apps use the Client Credentials Flow (defined in OAuth 2.0 RFC 6749, section 4.4), in which they pass along their Client ID and Client Secret to authenticate themselves and get a token.

How it works



1. Your app authenticates with the Auth0 Authorization Server using its Client ID and Client Secret (`/oauth/token` endpoint).

2. Your Auth0 Authorization Server validates the Client ID and Client Secret.

3. Your Auth0 Authorization Server responds with an Access Token.

4. Your application can use the Access Token to call an API on behalf of itself.

5. The API responds with requested data.

How to implement it

The easiest way to implement the Client Credentials Flow is to follow our Backend Quickstarts.

You can also follow our tutorial to use our API endpoints to Call Your API Using the Client Credentials Flow.

Keep reading

- Auth0 Rules
- Auth0 Hooks
- Tokens
- Token Best Practices
- Which OAuth 2.0 Flow Should I Use?

PRODUCT

Pricing

Why Auth0

How It Works

Lock

COMPANY

About Us

Blog

Jobs

Press

LEARN

Availability & Trust

Security

White Hat

API Explorer

MORE

Help & Support

Professional Services

Documentation

Open Source

WordPress

CONTACT

10800 NE 8th Street
Suite 600
Bellevue, WA 98004

+1 (888) 235-2699
+1 (425) 312-6521
+44 (0) 33-3234-1966