API Keys

Get the API keys you need to authenticate client requests—and learn how to keep them safe.Suggest Edits

API keys are unique data strings used to authenticate a user and enable access to privileged operations on Circle APIs. All Circle APIs use API keys as the mechanism toauthenticate client requests. Your API key should be kept confidential and secure at all times.

- Authentication is required for all API requests; without it, the requests will fail.
- All API requests must be made over HTTPS.

Keep Your API Keys Safe

Because our API keys allow access to privileged operations on Circle APIs, you must keep them secure at all times.

- Ensure your API key is always stored securely.
- Never share it or record it in a publicly accessible medium (client-side code, public repositories, etc.).

Caution: If you lose secure control of your API keys, your entity may suffer financial loss.

Manage Your API keys

Use the Developer Dashboard to access and manage the API keys for your entity. Go to the Circle Mint developer dashboard and click on the API Keys tab to create, view, edit, and revoke API keys. You must be logged into the production or sandbox Developer Dashboard and be an Administrator to access the API keys page:

- Production:https://app.circle.com/developer
- Sandbox:https://app-sandbox.circle.com/developer

Note: By default, Circle disables all product APIs in Production. Please seeCircle APIs: Sandbox to Production Transition Guide for more instructions on how to enable access to product APIs.

Types of API keys

Circle API supports two types of API keys:

- Standard
- keys provide the permissions to use any of Circle APIs for which your entity has subscribed service.
- Restricted
- keys limit access to the product role you select during key generation.

It is possible to create restricted keys in the Developer Dashboard before you gain business access to the endpoints for that product. As such, you may have access to a valid key that is scoped to product APIs your entity is not authorized to use. Requests to API endpoints for which you are not enabled return a 401: Unauthorized HTTP status code. In that event, contact your Circle Support Engineer to verify product access for your entity.

Restricted key permissions cannot be viewed or edited in the developer dashboard. Also, they cannot be created in the developer dashboard. To learn more about editing or creating restricted keys, please reach out to your Circle representative or[email protected] .

All customers that were issued API keys prior to April 25th, 2023 were provided restricted API keys. To find out what permissions your key has, please contact your Circle representative or[email protected] .

Create an API key

Log into Circle Mint → Developers → API keys, then:

1. Select "create an API key"
2. Enter Name
3. Provide IP addresses for IP allowlist [OPTIONAL]
4. Select "create API key"
5. Copy API key
6. Select X

You can have a maximum of 10 API keys per environment.

View API Key Details

Log into Circle Mint → Developers → API keys, then:

1. Select the ellipses on the API key you want to view
2. Select view details

Edit an API key

Log into Circle Mint → Developers → API keys, then:

1. Select the ellipsis on the API key
2. Select edit
3. Change name
4. Change IP Allowlist IPs
5. Select save

Revoke an API key

Log into Circle Mint → Developers → API keys, then:

1. Select the ellipsis on the API key
2. Select delete
3. Type in DELETE
4. Select delete button Updated5 months ago

What's Next

- Authentication
- Sandbox & Production Environments
- Table of Contents
-