Get started with the REST API

To use the Redis Enterprise Cloud REST API, you need to:

- Enable the API
- Create an account key
- Create a user key
- Collect endpoint details

**Note:** The Redis Cloud REST API is available only with Flexible or Annual subscriptions. It is not supported for Fixed or Free subscriptions.

To use the keys to authenticate and authorize your request, include the keys with the request headers:

<table>
<thead>
<tr>
<th>Key name</th>
<th>HTTP header name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account key</td>
<td>x-api-key</td>
<td>Account-level key assigned to all users of an account</td>
</tr>
<tr>
<td>User key</td>
<td>x-api-secret-key</td>
<td>Personal key associated with a specific user and possibly limited to certain IP ranges</td>
</tr>
</tbody>
</table>

Enable the API

The API is disabled on all accounts by default. You must **enable the API** before you can use it.

Account key

The account key identifies your specific account when you perform an API request. This is the account responsible for your subscription.

**Note:** An account key is an account-level secret. Do not share this key with anyone not authorized to use the account.

You create the account key once when enabling API access.

If you need to change or delete your account key, please contact support.

User key

The user key is a personal key that belongs to a specific user having the **owner** role. User keys are assigned owners when they're created. Keys cannot be assigned to users that aren't owners. Keys can belong to only one owner; however, an owner may have multiple keys.

You can view keys or copy their values only during the creation process.

**Note:** User keys are personal secrets. Do not share them.

Individual owners can generate multiple user keys for themselves, for separate apps, or for other owners within the same account.

Use key names to uniquely associate specific API requests to individual users or apps.
Doing so lets you audit API requests using the system log, which tracks the key used to authenticate each request.

**Authentication using API keys**

Every API request must use the **account key** and a **user key** to authenticate.

The keys are provided as **HTTP request headers**, shown earlier.

**Authenticate a request**

An API request successfully authenticates when:

1. The account and user keys are valid and properly defined in the HTTP request headers.
2. The user key is associated with the same account as the account key.
3. The request originates from a valid source IP address, as defined in a **CIDR allow list** associated with the user key.

   This requirement applies when you’ve defined a **CIDR allow list** for the secret key.

**More info**

To learn more, see:

- Manage API keys
- Use the API

**Updated:** October 31, 2021