Manage API keys

Every REST API request must include the following API keys:

1. The **Account key** identifies the account associated with the Redis Enterprise Cloud subscription.
2. The **User key** identifies the user and (optionally) the context of a request. Generated by account owners.

Use the **API Keys** tab of the **Access Management** screen to manage your keys:

1. Sign in to your Redis Cloud subscription as an account owner.
2. From the menu, choose **Access Management** and then select the **API Keys** tab.

If an **Enable API** button appears, select it to enable the REST API for your account.

**API account key**

The **API account key** is used as the value of the x-api-key HTTP header in order to authenticate a REST API request.

By default, the **API account key** is masked; that is, it is obscured for security reasons. You can use the **Show** button to display the key and the **Hide** button to mask it.

The **Copy** button copies the account key to the Clipboard.

**API user keys**

**API user keys** (also known as secret keys) are used as the value of the x-api-secret-key HTTP header used to authenticate a REST API request.

In this context, **user** refers to the account used to sign in to the admin console. Users must be account owners.

Users can have more than one user key; however, users should not share user keys.
Create a new user key

Use the Add button to create a new user key.

When you do this, you’re prompted for the **Key name** and the associated **User name**.

The key name:

- Must be between 10 and 50 characters long
- Can contain alphanumeric characters, hyphens, and underscores. Spaces are not allowed.

The user name must be an account owner.

Select **Create** to create the new key.

Create

When you do this, the **API user key** dialog appears.

API user key

*This is the only time that the API user key can be viewed or downloaded*

API user key for RedisLabsTeam-PM Account RedisLabs

```
............................
```

Finish

**Note**: use the account key together with your user key
Warning - This is the only time the value of the user key is available. Save it to a secure location before closing the dialog box.

If you lose the user key value, it cannot be retrieved. If this happens, create a new key to replace the lost one.

When you've saved the user key, use the Finish button to close the dialog box.

(The Finish button is disabled until you copy the key to the Clipboard.)

Delete a user key

To delete a user key:

1. Use the API Keys tab of the Access Management screen to locate the target key

2. Select the Delete button displayed to the right.

3. This displays the Delete API secret key dialog box.

Select the Delete button to confirm.

Manage CIDR allow list

By default, REST API requests are allowed from all IP addresses. To limit access to specific addresses, define a CIDR allow list for the user key.

To manage the CIDR allow list:

1. Use the API Keys tab of the Access Management screen to locate the target key
2. Select the **Manage** link in the **CIDR allow list** column; this displays the **Manage CIDR allow list** dialog box.

![Manage CIDR allow list dialog box](image)

3. Enter each allowed IP address in **CIDR format** (example: `127.0.0.0/24`) and then select the **Save** button.

![Save button](image)

Use the **Add CIDR rule** button to add additional addresses to the list.

![Add CIDR rule button](image)

Use the **Edit** button to change the address for a rule or the **Delete** button to remove a rule.

![Edit and Delete buttons](image)