Managing Keys

From the Settings > Keys tab, you can view a zone’s agent access key and all associated API keys.

Prerequisites: You must be a Global or Zone Administrator to manage API keys for the zone that you manage.

Viewing Keys

Select the Settings > Keys tab to view the agent access key and the API keys.

Account ID

This is the UUID for the account. (Only global or zone administrators can see this ID)

- To copy the agent access key, click the Copy button (clipboard) to the right of the field.

Agent Access Key

The agent access key is used to add devices to your Automox account.

- To copy the agent access key, click the Copy button (clipboard) to the right of the field.

API Key
The API key is used to access the Automox API.

**Note:** API keys are not automatically generated for new users or new zones. See Adding API Keys.

- To view an API key, click the **Show** button to the right of the hidden characters. The key will automatically hide again after 10 seconds.

- To copy the API key, click the **Copy** button (clipboard) to the right of the field. It is automatically decrypted.

![API Key Preview](image)

**Note:** When you use API keys, take care to keep them secure. Follow best practices such as these:

- Do not embed API keys directly in code.
- Do not store API keys in files inside your application’s source tree.

### Managing API Keys

Your user account role determines what API key management functionality is available to your account. There are four types of user roles:

- **Zone administrators** can view and manage all organizational API keys for the zone that they have permissions to.

- **Zone operators** (formerly patch administrators) can only view and manage API keys created with their user account.

- **Billing administrators** can only view and manage API keys created with their user account.

- **Read Only** users can only view and manage API keys created with their user account.

(See **User Accounts** for more information about role-based account controls.)

### Global and Zone Administrator privileges

- View all of the zone’s API keys on the **Settings > Keys** page of the console.

- Disable and delete all of the zone’s API keys on the **Settings > Keys** page of the console.
- Disable and delete all of the zone's API keys through the API.

**All other administrator and user privileges**

Zone operators, billing administrators and read-only users have the following permissions:

- They can view only the API keys that were created by their user login on the Settings page of the console.
- They can disable and delete the API keys that were created by their user login on the Settings page of the console.
- They can disable and delete the API keys that were created by their user login through the API.

**All users**

- Users can sort on the user column.
- Users can only add keys for their own account.

**Adding API Keys**

You can add up to 10 unique API keys to a user account.

- From the **Settings > Keys** page, click **Add**.
- Enter the unique name of the API key. You will see an error message if you enter a name that already exists.
- (Optionally) You can select an expiration date for the API key.
- Click **Create**.

**Disabling API Keys**
You can disable API keys that are from your own account. Only Global and Zone Administrators can disable API keys for all users.

- Select the Settings > Keys tab to view the list of API keys.

- To find the API key that you want to disable, sort by the Name or User column. Show or hide the API key, as needed. If you don’t see the API key you want, select from the next page at the bottom.

- To disable the API key, turn off the toggle switch under Enabled.

![Image of API key management interface]

**Note:** When an API key is disabled, the key is rejected and returns an error. It is possible to re-enable an API key.

### Deleting API Keys

You can delete API keys that are from your own account. Only Global and Zone Administrators can delete API keys for all users.

- Select the Settings > Keys tab to view the list of API keys.

- You can sort by the Name or User column to find the API key that you want to delete. Show or hide the API key, as needed. If you don’t see the API key you want, select from the next page at the bottom.

- To delete the API key, click **Delete** in the manage column.

**Note:** When an API key is deleted, the key is rejected and returns an error.

### Managing Columns

Use the Column drop-down menu to select which table columns you want to include or exclude from view.

- Select or clear any checkboxes to control the API Keys page view.

- You can change the order of the columns by dragging the = next to the column names to the desired position.
<table>
<thead>
<tr>
<th>Column</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
</tr>
<tr>
<td>Created</td>
<td></td>
</tr>
<tr>
<td>Expires</td>
<td></td>
</tr>
<tr>
<td>API Key</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Manage</td>
<td></td>
</tr>
</tbody>
</table>