IP Authorization Overview

Last Modified on 09/07/2021 9:41 am MDT

IP authorization allows admins to control who can access an org by validating users' IP addresses against entries in an IP allow list. This list is enabled and managed in the Core API (Swagger) and can be configured with one of the following options:

- **off:** No IP authorization control is performed for any authentication requests.
- **on:** IP authorization control is performed for all SSO and basic access authentication (i.e., username and password) requests.

  IP token validation must be enabled separately from IP authorization.

- **bypass_sso:** IP authorization control is performed only for basic access authentication requests and is not performed for SSO.

See the IP Authorization Logins and IP Token Validation articles for login functionality details when this feature is enabled.

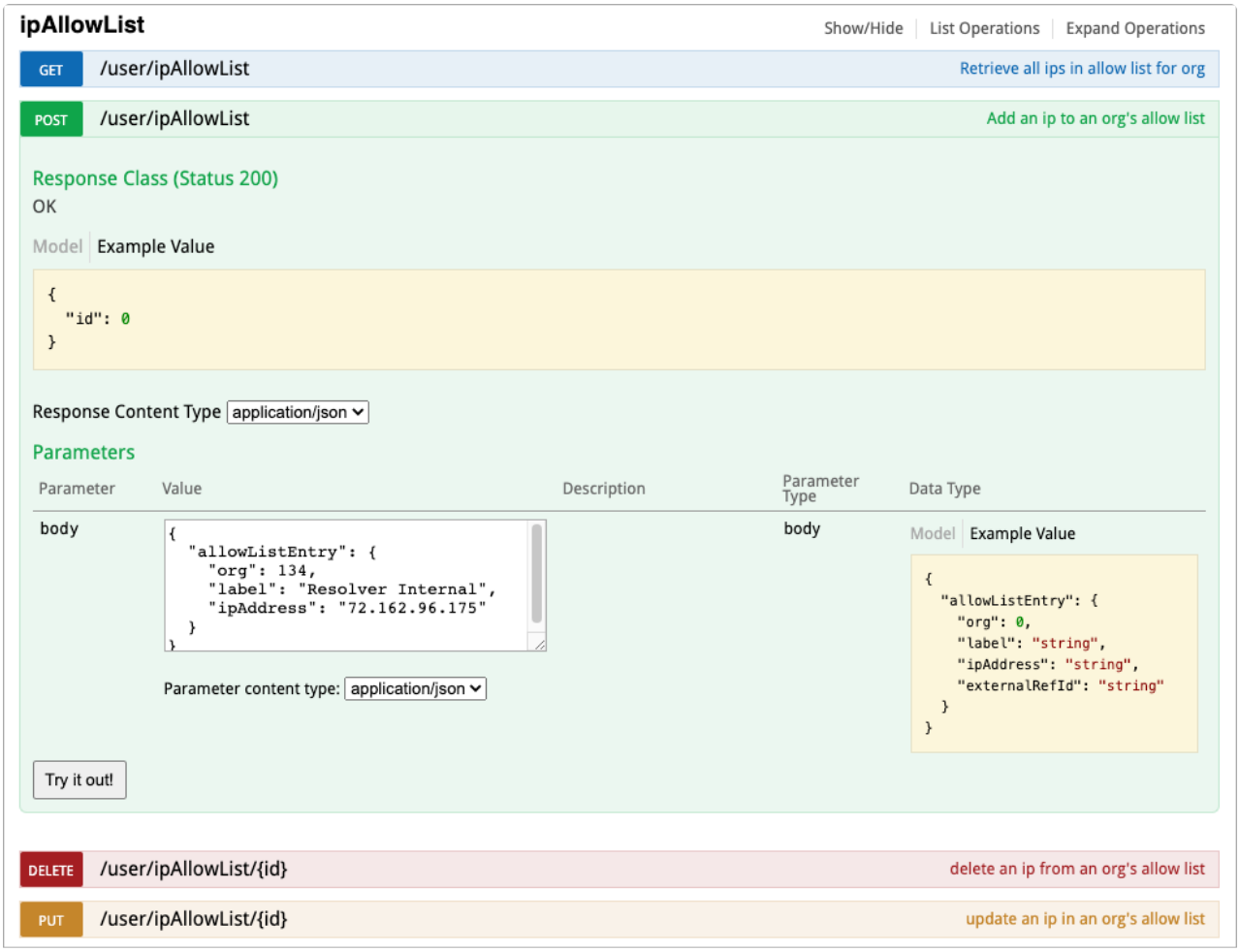
IP authorization control must be enabled or disabled by Resolver Support.

ipAllowList Endpoint

The IP allow list is managed through the **ipAllowList** endpoint in **Swagger**, where admins can add, update, or delete entries through the following calls:

- **POST /user/ipAllowList:** Add an IP to an org's allow list.
- **PUT /user/ipAllowList/{id}:** Update an IP in an org's allow list.
- **DELETE /user/ipAllowList/{id}:** Delete an IP from an org's allow list.
- **GET /user/ipAllowList:** Retrieve all IPs in an org's allow list.

The API can be accessed from the **Admin** settings, then clicking **Swagger Docs** in the **Tools** section. Any changes made to the IP allow list is captured in the User Audit Trail.



The IpAllowList endpoint in the Core API.

Important Notes

- This feature is available to all customers; however, it must be enabled or disabled by Resolver Support.
- IP authorization is an org-wide setting that can only be enabled and managed in the API. It cannot be modified through org import.
- The IP allow list supports CIDR notation for IP ranges; however private IP addresses cannot be added to the list. Specifically:
    - 10.0.0.0 - 10.255.255.255 (CIDR notation: 10.0.0.0/8)
    - 172.16.0.0 - 172.31.255.255 (CIDR notation: 172.16.0.0/12)
    - 192.168.0.0 - 192.168.255.255 (CIDR notation: 192.168.0.0/16)
- If IP authorization is set to **on** or **bypass_sso**, the last entry in the IP allow list cannot be deleted.
- The **ipAuthorize** flag cannot be set to **on** or **by_pass SSO** until at least one IP address has been added to the allow list.

- Admins can enforce IP authorization control on individual anonymous logins from the Anonymous Login settings; however, until IP authorization control is enabled for the org, this option will be greyed out.
- If a previously authorized user's network changes during an active session, they'll be logged out and need to log in again.
- All updates to the IP allow list are captured in the User Audit Trail below the **IP Authorization** subject type.
- An IP allow list is deleted when its associated org is deleted.
- Members of the Resolver Support team (i.e., users with the domain @resolver.com) will automatically bypass any IP authorization control. This allows Resolver Support to access an org and provide assistance when needed without IP validation.