

IP Authorization Overview

Last Modified on 01/23/2024 4:53 pm EST

Overview

IP Authorization gives an Administrator control over who can access an Org by validating a user's IP address with IP addresses on the Org's **IP Allow List**. Use the API (Swagger™) to configure the IP Authorization function with one of the following options:

- **Off:** Disables the IP Authorization control. User login attempts using SSO (Single Sign On), or username and password will not use the IP Authentication process.
- **On:** Enables the IP Authorization control. User login attempts using SSO, or username and password will use the IP Authentication process.



Note:

Enabling the IP Authorization control does not enable the Resolver API IP token validation function.

- **bypass_sso:** Enables the IP Authorization control for user login attempts using a username and password and bypasses SSO login attempts.

Users are not able to configure the IP Authorization control without assistance from the Resolver Support team. Please contact [Resolver Support](#) for assistance enabling or disabling the IP Authorization control.

Related Information/Setup

For more information on how to log into Resolver using IP Authorizations, please refer to the IP Authorizations Logins article.

- [IP Authorization Logins](#)

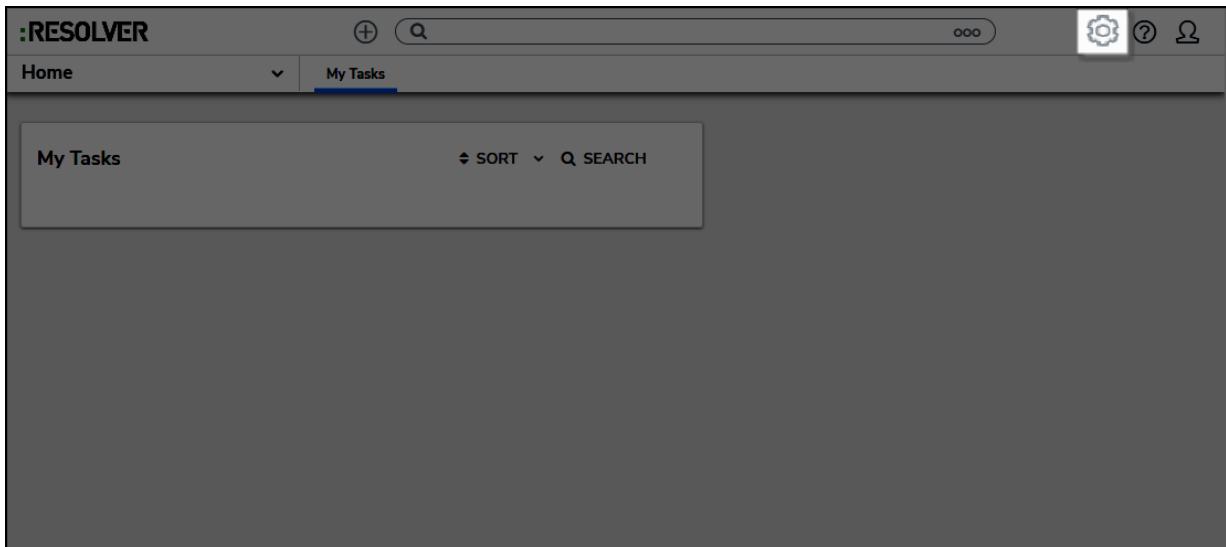
For more information on how to use the Token Validation process, please refer to the IP Token Validation article.

- [IP Token Validation](#)

Navigation

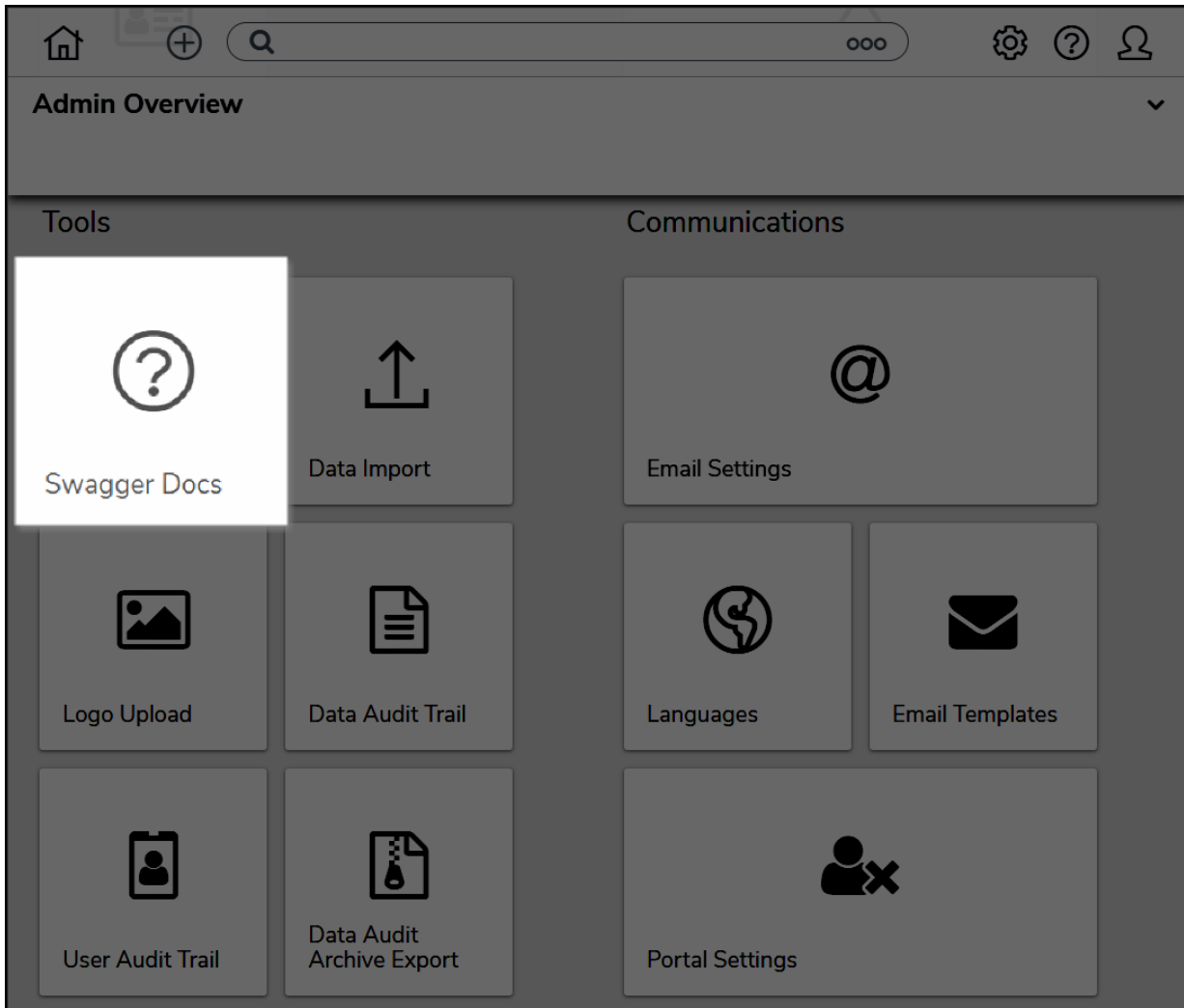
The **Core API** can be accessed from the **Admin Overview** screen by clicking the **Swagger Docs Tile** on the **Tools** section and selecting the **ipAllowList** endpoint. Any changes made to the **IP Allow List** are captured in the **User Audit Trail**.

1. Using your username and password or the Single Sign-On (SSO) function, log into Resolver.
2. From the **Home** screen, select the **System** icon.



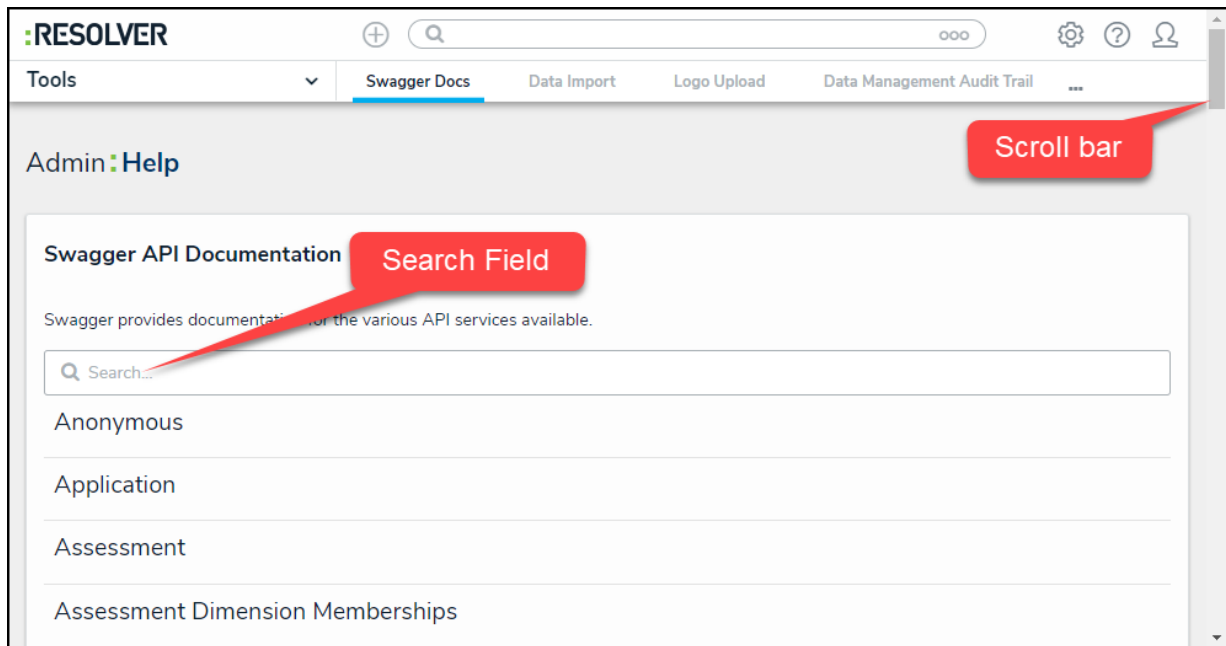
Select the Gear Icon

3. From the **Admin Overview** screen, navigate to the **Tools** section and select the **Swagger Docs Tile**.



Select the Swagger Docs Tile

4. From the **Swagger API Documentation** screen, use the **Search** field or **Scroll bar** to navigate to the **ipAllowList** endpoint.

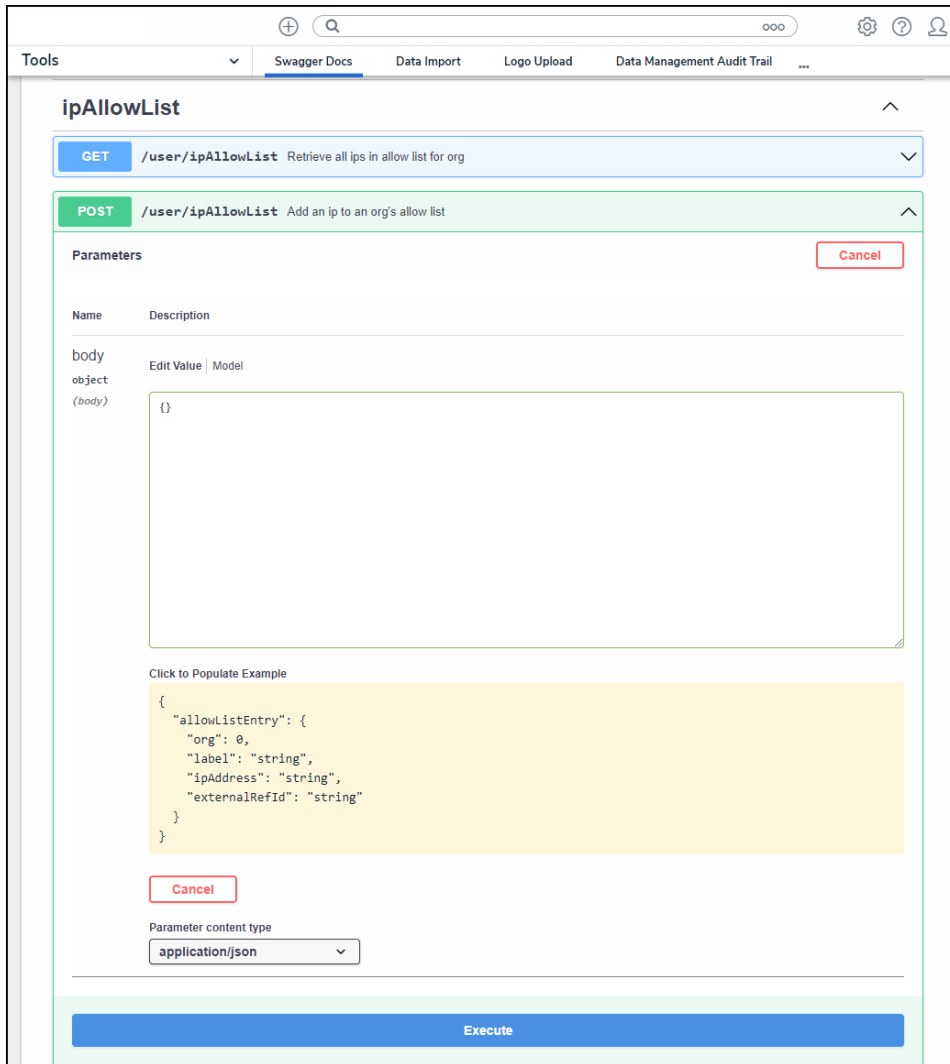


Navigation Options

ipAllowList Endpoint

The **ipAllowList** endpoint in Core API in Swagger allows you to configure/manage the **IP Allow List**. Administrators can add, update, or delete entries using the following calls:

- **GET /user/ipAllowList:** This call will retrieve a list of all IP address on an Org's **IP Allow List**.
- **POST /user/ipAllowList:** This call allows an Administrator to add an IP address to an Org's **IP Allow List**.
- **DELETE /user/ipAllowList/{id}:** This call will delete an IP address from an Org's **IP Allow List**.
- **PUT /user/ipAllowList/{id}:** This call will edit/update an IP address on an Org's **IP Allow List**.



IpAllowList endpoint in the API

Important Information

- The IP Authorization feature is available to all customers; however, it must be enabled or disabled by a [Resolver Support](#) team member. Members of the Resolver Support team will automatically bypass IP Authorization allowing them to access an Org and provide assistance when needed without IP validation.
- IP Authorization is an Org-wide setting that is enabled and managed in the API.
- IP Authorization cannot be modified through [org import](#).
- The IP allow list supports CIDR notation for IP ranges. You cannot add private IP addresses 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)
- You cannot delete the last entry in the IP allow list if the IP Authorization is **on** or

bypass_sso.

- You must add at least one IP Address to the allow list to use **on** or **by_pass SSO** option on the **ipAuthorize** flag.
- Admins can enforce IP Authorization control on individual confidential logins from the [Confidential Login](#) settings; however, this option will be greyed out until IP Authorization control is enabled for the org.
- 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.