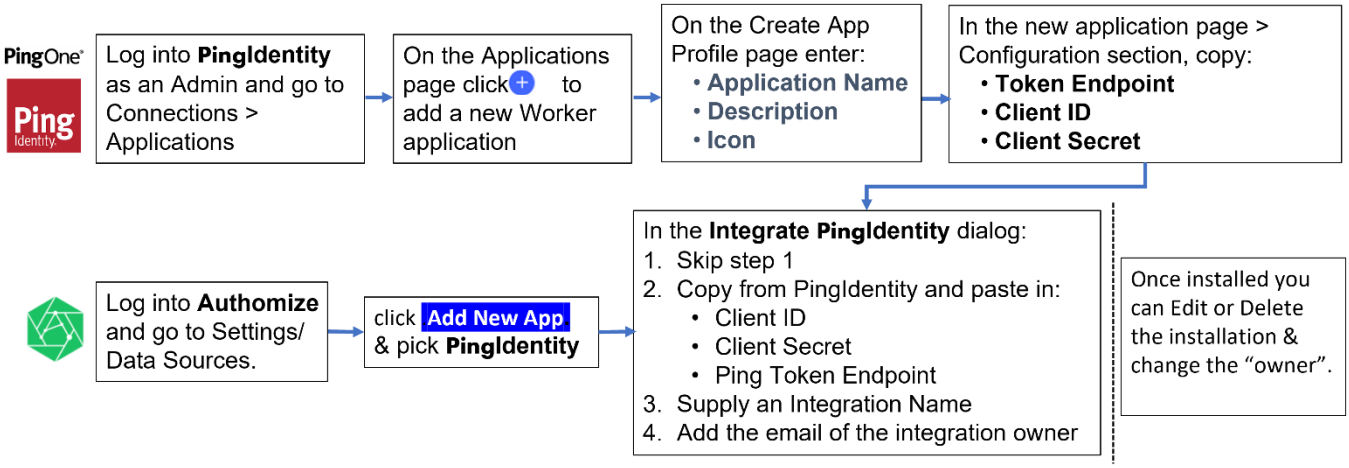
Integrating PingOne with Authomize

Integration with **PingOne** provides visibility about your **PingOne** users, groups, roles and the applications they can access. After integration, Authomize provides visibility into **PingOne** and the applications (in **PingOne** or other IDPs) that **PingOne** supports as an Identity Provider, enabling improved identity security and automated access reviews.

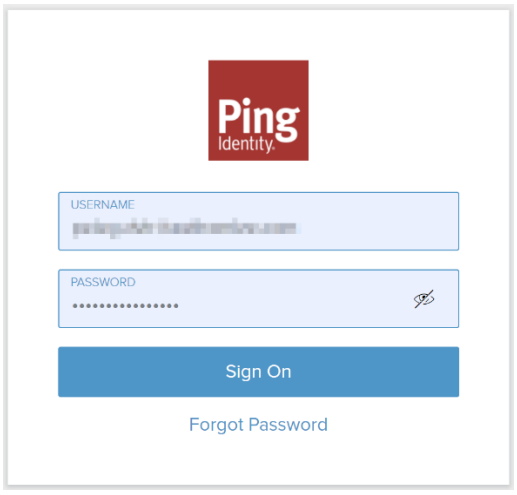
Note: PingOne is PingIdentity's Identity-as-a-Service single sign-on product. "PingOne" and "PingIdentity" are used interchangeably since PingOne is, basically, PingIdentity's only product.

PingOne integration workflow

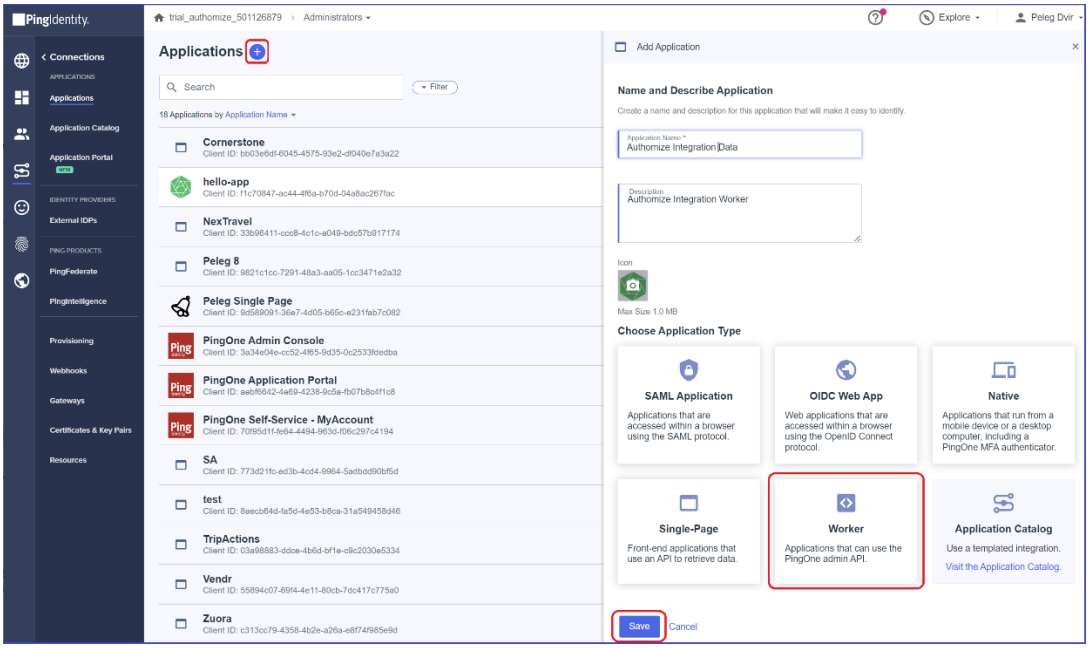


Setting Up PingOne

1. Log into PingIdentity as an admin.

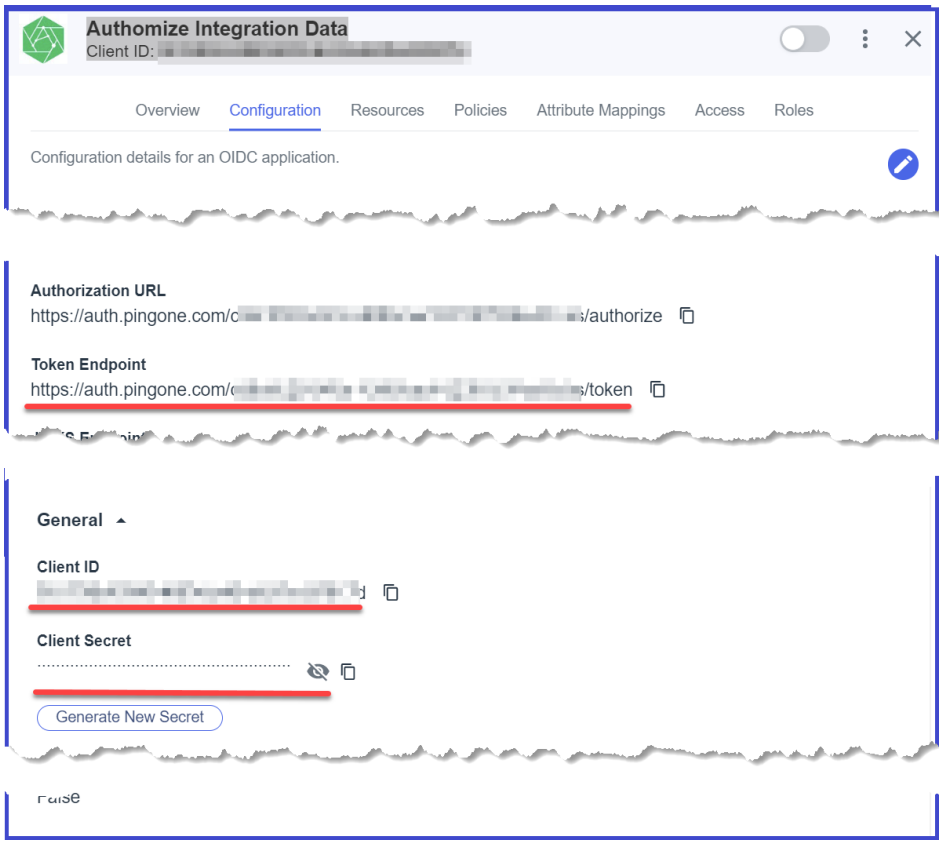


2. Go to Connections > Applications, click  , and enter:
    - **Application Name**
    - **Description**
    - **Icon**



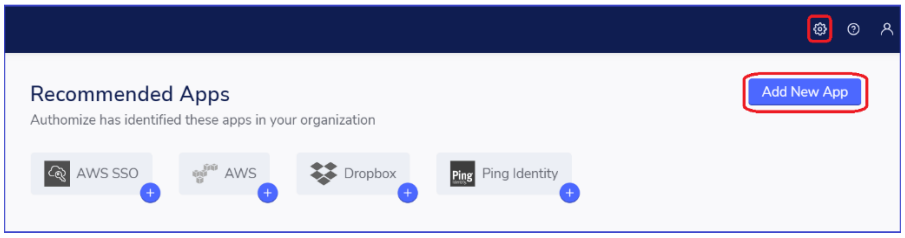
3. Pick **Worker** application type and then click **Save**.

4. In the configuration section on the new application page, copy:
    - **Client ID**
    - **Token Endpoint**
    - **Client Secret**

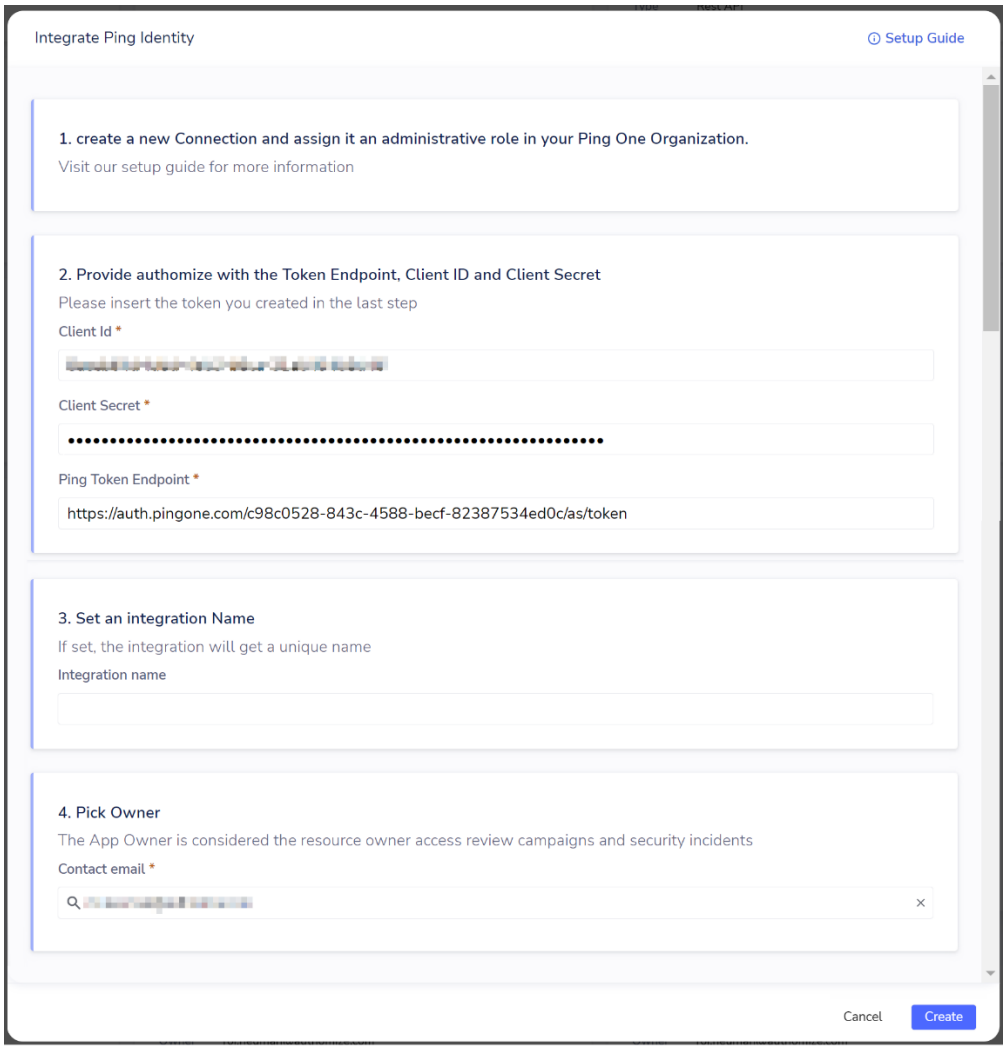


Integration with Authomize

1. Log into **Authomize**
2. Go to the **Settings/Data Sources** page.
3. Click **Add New App** and pick **PingIdentity**.

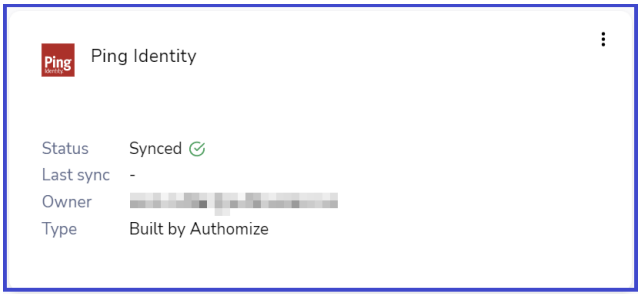


4. In the **Integrate PingIdentity** dialog:
   - Step 1. Skip step 1
   - Step 2. Copy from PingOne and paste in:
     - Client ID
     - Client Secret
     - Ping Token Endpoint
   - Step 3. Supply an Integration Name
   - Step 4. Add the email of the integration owner



5. Click Create

When the connector is successfully added you will see a PingIdentity entry in the connectors list.



What data is collected

Azure Active Directory

- **Users**
- **Groups and Roles**
- **Applications**
- **Service Accounts**