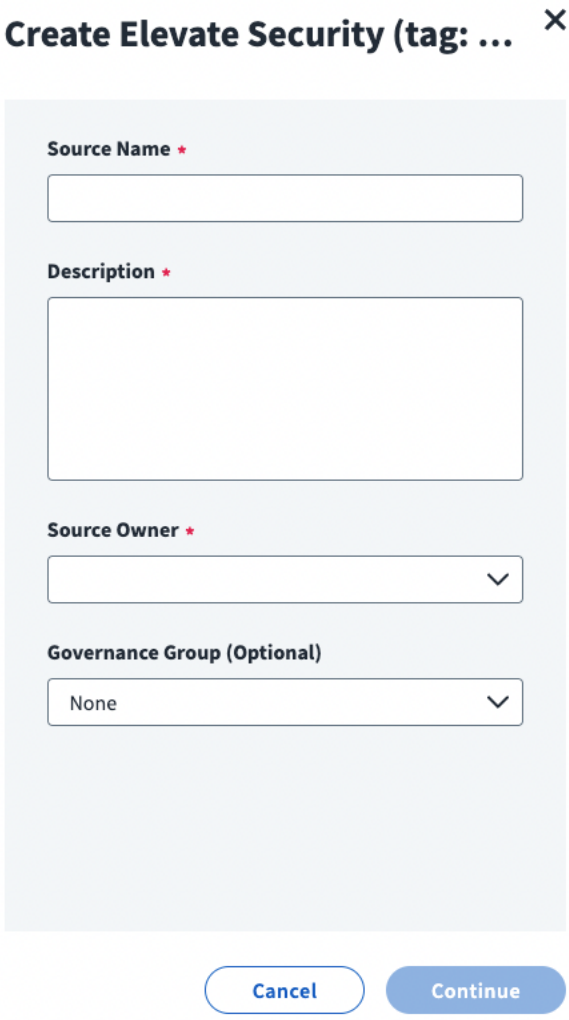
Elevate Security SaaS Connector User Guide

Overview

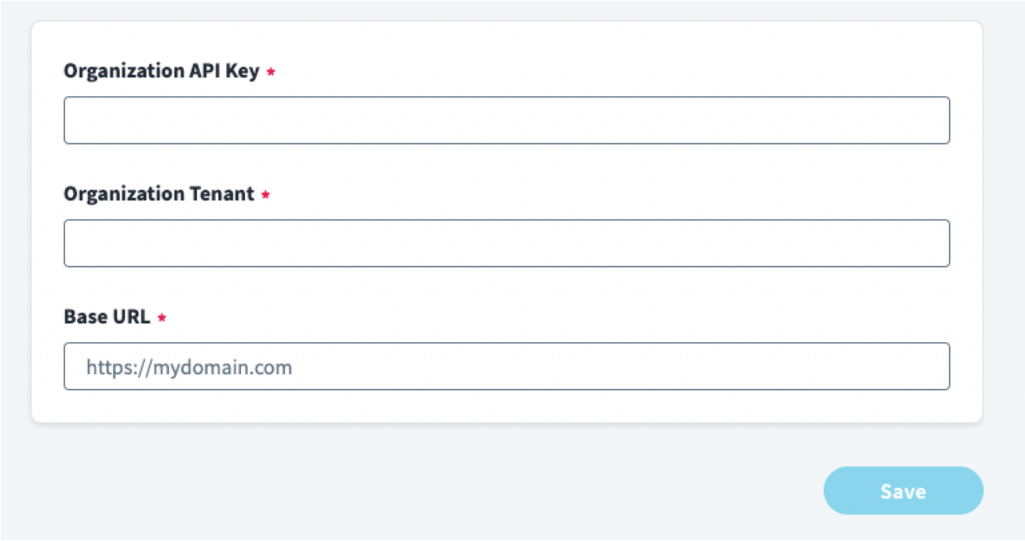
Elevate Security provides software as a service focused on addressing employee risk. Risk is evaluated according to proprietary methods of analyzing user behavioral data it collects from various sources. This SaaS Connector retrieves all employee users from the Elevate Security API for a given tenant along with all of the scores associated with each.

Installation & Configuration

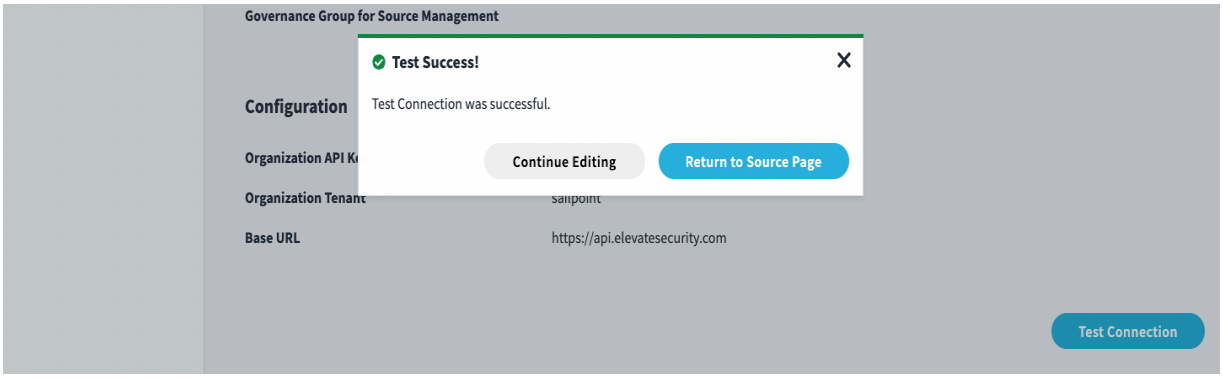
- You must have admin access to the tenant where the connector will be deployed.
- Upload the Elevate Security zip file as described in the SaaS Connectivity Test, Build, and Deploy guide
- In your IDN tenant (https://<tenant-name>.identitynow.com) navigate to **Admin**>**Connections**>**Sources**
- Click **Create New** and find the source by searching for the name you used to upload the zip file.
- Click **Configure**. Specify a Source Name, Description and Owner. Click **Continue**.



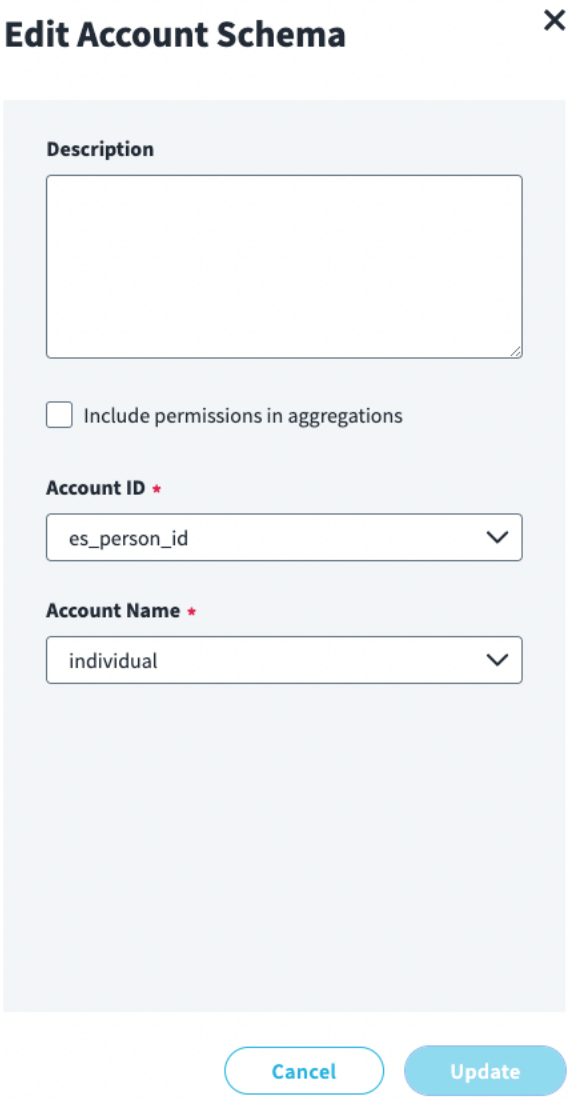
- Specify the API Key and Tenant Name from your Elevate Security tenant.



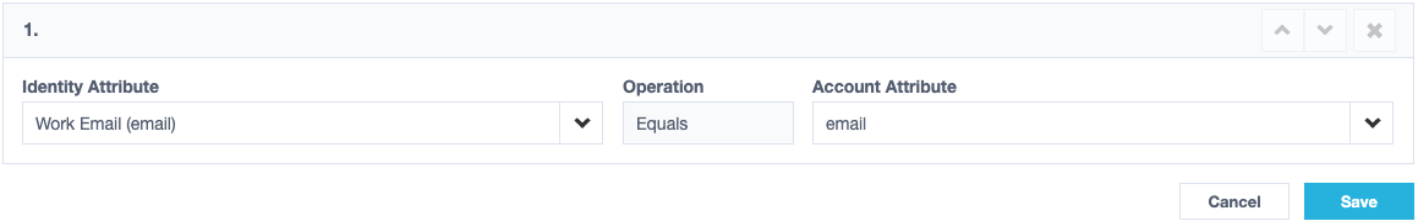
- Click Save, then click Review and Test. Click Test Connection to verify your connection parameters.



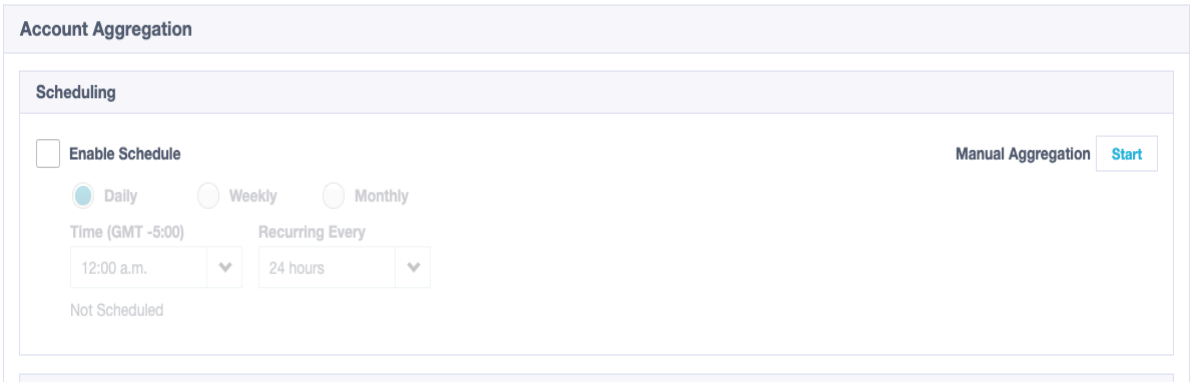
- Click the X in the upper right to return to the Source screen.
- Select Import Data > Account Schema
- Click Edit Schema
- Set Account ID to es_person_id and set Account Name to email, then click Update.



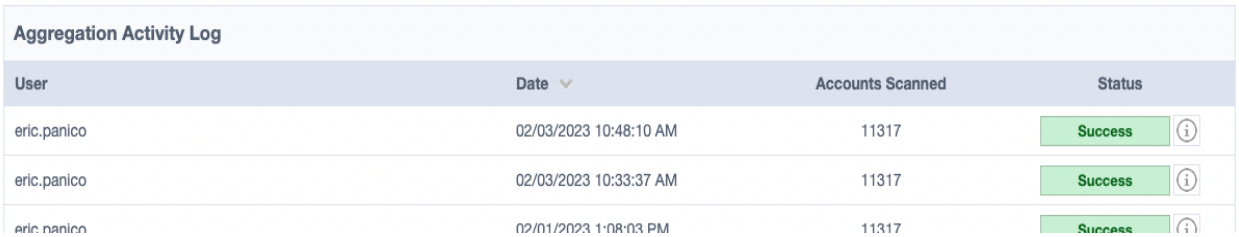
- Click Go Back, then select Correlation
- Identity Attribute, select Work Email (email), Operation Equals, Account Attribute email. Click Save.



- Click Import Data > Account Aggregation
- Click the Start button in the Account Aggregation section to begin a manual integration task.



- Scroll down to the Aggregation Activity Log section. Verify task is running. Wait until the status changes to Success.



Aggregation Activity Log

User	Date	Accounts Scanned	Status
eric.panico	02/03/2023 10:48:10 AM	11317	Success
eric.panico	02/03/2023 10:33:37 AM	11317	Success
eric.panico	02/01/2023 1:08:03 PM	11317	Success