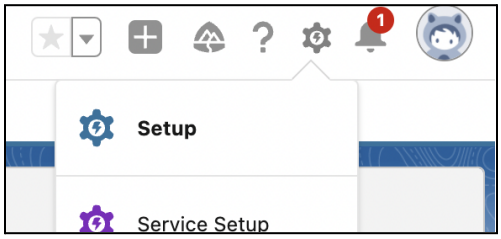
Astrix

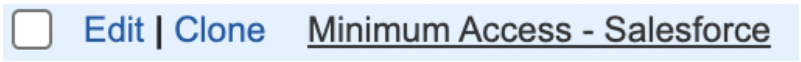
Integration Guide

Astrix Plugin for Salesforce

Stage 1 - Create a minimal access profile & user



1. Login to your **Salesforce admin account**.
2. In the top bar, go to **Setup**, as presented on the right:
3. Under the **Users** tab, go to **Profiles.**
4. Make a **clone** of the "Minimum Access - Salesforce" profile and name it **"Security Reviewer".**



5. Click the **Edit** button**,** and carefully add the following permissions to the profile:
    a. Under "General User Permissions":
        - Manage Connected Apps
    b. Under "Administrative Permissions":
        - API Enabled
        - Manage Users
        - Customize Application
        - View Real-Time Event Monitoring Data (Optional)
        - Lightning experience user
        - View event log files
6. Click **Save** at the bottom of the screen.
7. Create a user named Astrix Security and assign it the created profile.

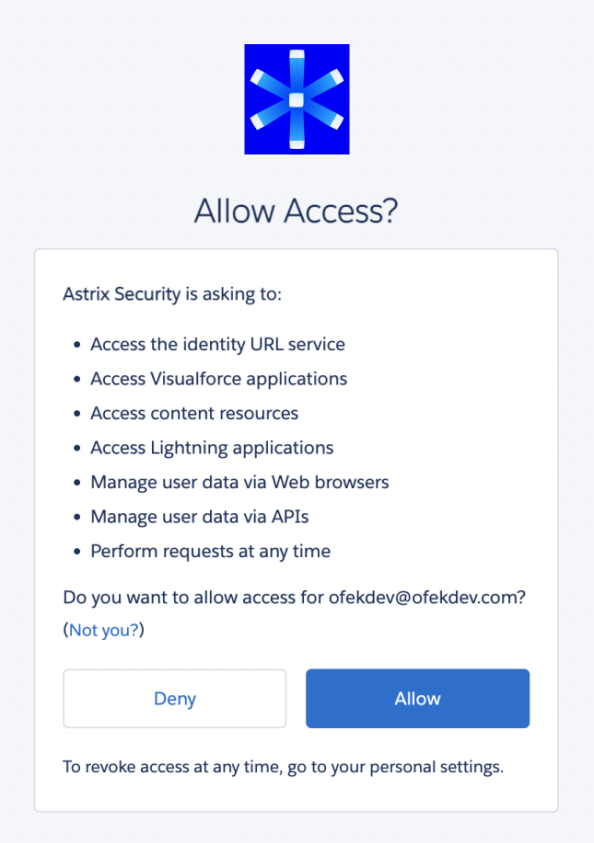
NOTICE

Astrix requires the listed permissions in order to properly function.

Read more about it in the appendix.

Stage 2 - Installing Astrix on the restricted user

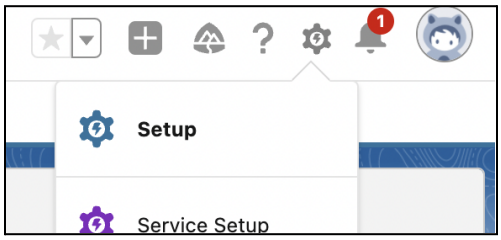
1. Browse to this URL (Use this URL if you are installing on a sandbox).
2. If not already logged in, login to the created user with Security Reviewer profile.
   In case SSO is enforced globally in your tenant, you'll need to create a new user in your Identity Provider and connect it to the Astrix Security user.
3. Expect the following screen:

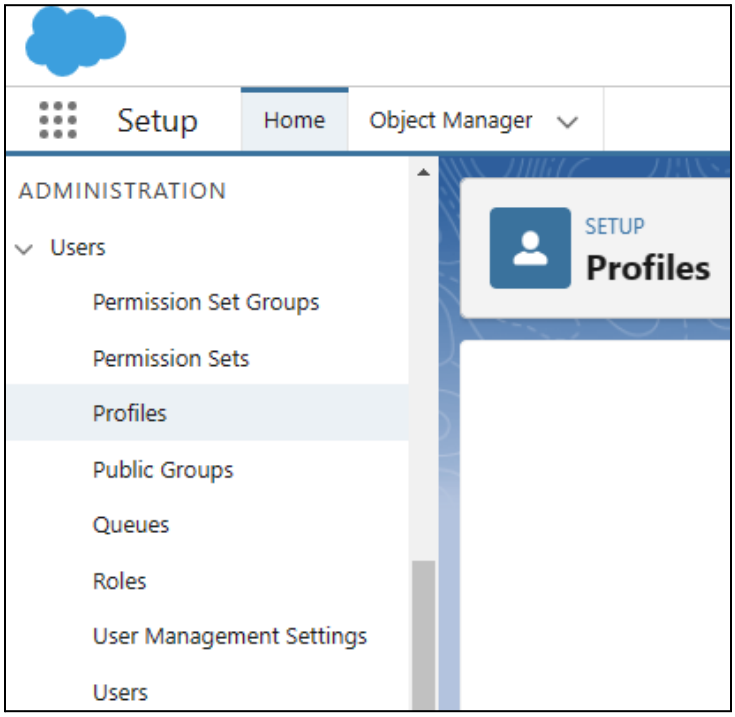


4. After clicking **Allow**, expect a simple confirmation screen that shows the text: **"Authorization Granted".**

Optional Stage - Restrict the user further using IP restriction feature

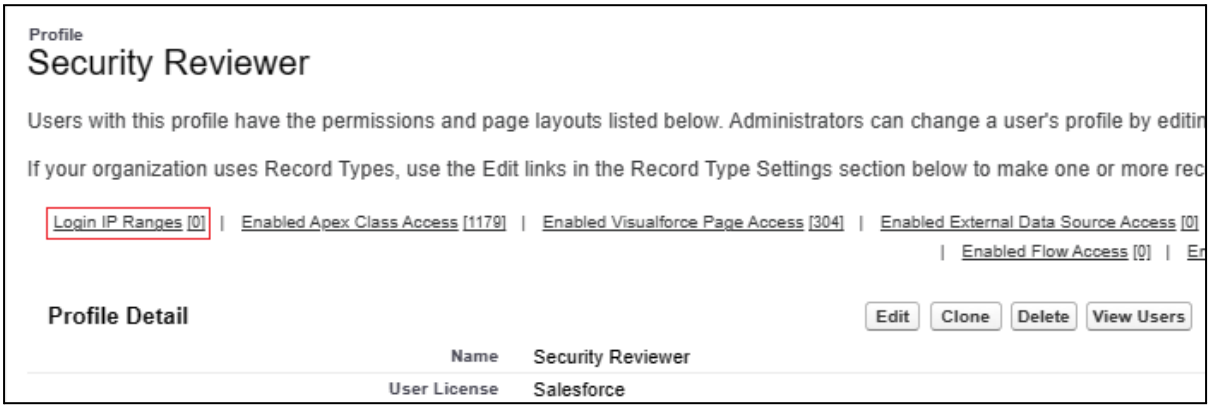
1. Login to your **Salesforce admin account**.
2. In the top bar, go to **Setup**, as presented on the right:
3. Under the **Users** tab, go to **Profiles.**





4. Click on the newly created **Security Reviewer** profile.

5. In the page that opens up, click on **Login IP ranges**.



6. Click **New**, add your own IP address and click **Save**, so that you can access the restricted user in the future.
7. Click **New** again, and add the Astrix IP address supplied to you by Astrix. This ensures that the user is only able to be used through Astrix's systems.

Appendix - Astrix Salesforce Integration - Required Permissions

- The restricted user has the following permissions:
    - Use api - access and usage of platform's API
    - Manage users and permissions - used to gather information about users, tokens and their permissions
    - Real time event monitoring - ability to gather real time events i.e. logins and api usage
    - Manage and customize applications - gather information about all applications installed
- All other permissions and their meaning can be found here:

Required scopes	Description	Why we need it
Manage user data via APIs	Provides access to the installing user's account using APIs	Allows Astrix to use Salesforce's APIs
Manage user data via Web browsers (web)	Allows use of the access_token on the web	Provide Astrix access to the web interface to extract additional information
Perform requests at any time	Allows a refresh token to be returned when the requesting client is eligible to receive one.	Astrix uses this scope to keep the permissions you granted Astrix when installing as long as you use our platform, so you won't have to re-grant them repeatedly
Access the identity URL service	Provides Astrix access to the Salesforce's identity URL service - allowing Astrix to get personal info, such as profile, email address, etc.	Astrix needs this in order to be able to seamlessly refer you to the relevant user, when an issue related to him arises
Access Lightning applications	Allows hybrid apps to directly obtain Lightning child sessions through the OAuth 2.0 hybrid app token flow and hybrid app refresh token flow	If your organization uses Salesforce Lightning, Astrix will use this scope to gather additional information
Access Visualforce applications	Allows access to customer-created Visualforce pages only. This scope doesn't allow access to standard Salesforce UIs	If your organization uses Salesforce Visualforce, Astrix will use this scope to gather additional information
Access content resources	Allows hybrid apps to directly obtain content child sessions through the OAuth 2.0 hybrid app token flow and hybrid app refresh token flow	Astrix will use this scope to look for issues related to content your organization has on Salesforce (such as documents upload and used within the platform)
Access custom permissions	Allows access to the custom permissions in an organization associated with the connected application	Allows Astrix to generate a list of Salesforce users and their permissions, so Astrix can spot anomalies
See more at https://help.salesforce.com/s/articleView?id=sf.connected_app_create_api_integration.htm&type=5		

Notes

- Astrix Security requires a minimal list of permissions in order to collect relevant information.

- Astrix Security only uses the minimal API calls needed to provide connectivity visibility and governance.
- Astrix Security doesn't access any content, intellectual property or customer data on the monitored platforms - only connectivity metadata.
- Plugin tokens are encrypted on an internal only facing storage and tokens are never stored in plain text and only decrypted in memory during usage.