Solarly for Agentforce Setup Guide

A concise install and post-install validation guide for admins and architects.

Purpose

This guide covers the minimum setup steps for Solarly for Agentforce. It is written for Salesforce admins, architects, and technical operators who are comfortable configuring a managed package and validating an external endpoint.

Important
Solarly for Agentforce is designed for organizations with in-house admin or architect capacity. It is not positioned as general Salesforce onboarding or implementation training.

Before You Begin

- Supported validation context: Salesforce Enterprise, Unlimited, and Developer editions.
- Lightning Experience should be enabled for the users who will access the application.
- An installed package version of Solarly for Agentforce must be available in the target org.
- You need permission to assign the packaged permission set and create or update Named Credentials.
- You need a reachable SolarlyEngine endpoint and any associated secrets or authentication material.

Required Configuration Steps

- Install the package in the target org and confirm the packaged components are visible after installation completes.
- Assign the Solarly for Agentforce admin permission set to the users who will run assessments.
- Create or update the SolarlyEngine Named Credential so it points to the correct reachable endpoint.
- Validate connectivity from Salesforce to the endpoint before relying on generated outputs.
- Open the Solarly application in Lightning Experience and confirm the assessment home screen loads as expected.

Post-Install Validation

- Create a test assessment and confirm the record persists successfully.
- Run the assessment workflow and confirm recommendation or summary data is returned.
- Review any audit or diagnostic details to confirm the endpoint configuration is working as intended.
- Verify that generated outputs can be reviewed by the intended admin or architect persona.

Support Boundary

Solarly support should focus on package issues, dependency configuration, and product behavior. Customers should maintain their own internal ownership for org administration, page layout decisions, security review, and downstream implementation work.