Je eigen AI-assistent koppelen

Aan de slag · https://autorespond.nl/docs/je-eigen-ai-assistent-koppelen/

Je platform heeft een MCP-endpoint, waarmee een AI-assistent kan werken met je CRM, je projectborden, je helpdesk en je kennisbank. Deze pagina beschrijft hoe je dat instelt en hoe je het verstandig houdt.

Wat je nodig hebt

- Een client die MCP ondersteunt. Claude, Claude Code, Cursor en Codex werken allemaal.
- Een zakelijk abonnement bij je AI-leverancier, geen gratis of consumentenabonnement. Dat is van belang voor de verwerkersovereenkomst.
- Vijf minuten.

Stap 1: maak een gebruiker voor de assistent

Koppel niet als jezelf. Maak een aparte gebruiker aan in je platform en geef die de smalste rol die nog doet wat je wilt. De koppeling erft exact de rechten van die gebruiker, dus de rol is je controle.

Ons advies voor de eerste weken: een rol die wel mag lezen en niet mag schrijven. De meeste waarde zit in lezen.

Stap 2: genereer een applicatiewachtwoord

Genereer in het profiel van die gebruiker een applicatiewachtwoord. Kopieer het meteen, want het wordt daarna niet opnieuw getoond. Dit is een sleutel die je op elk moment kunt intrekken zonder iemands inlogwachtwoord te wijzigen.

Stap 3: kopieer de configuratie

Het instellingenscherm genereert een kant-en-klaar configuratieblok voor Claude Desktop, Claude Code, Cursor en Codex. Plak het in de configuratie van je client en start de client opnieuw.

Stap 4: controleer wat de assistent kan zien

Vraag eerst iets wat alleen leest. "Hoeveel contacten hebben we, en hoeveel zijn er in de laatste dertig dagen bijgekomen?" Komen de getallen overeen met wat je in je eigen dashboard ziet, dan klopt de koppeling.

Verstandig houden

Keur alles goed wat onomkeerbaar is. Laat de assistent opstellen en voorstellen. Jij keurt goed wat verstuurt, afschrijft of verwijdert. Niet omdat de assistent onzorgvuldig is, maar omdat instructies meerduidig zijn en gevolgen dat niet zijn.

Verruim de toegang langzaam. Als je tien keer hebt gezien dat iets goed gaat, geef de assistent dan toestemming om dat te doen. Niet eerder.

Let op instructies in de inhoud. Je assistent leest tekst die anderen hebben geschreven: tickets, formulierinzendingen, reviews. Zet iemand instructies in die tekst, dan komen ze in dezelfde context terecht als die van jou. Alleen-lezen-toegang haalt het grootste deel van dit risico weg, en goedkeuring door een mens de rest.

De AVG-kant

Zodra persoonsgegevens bij je AI-leverancier terechtkomen, wordt die leverancier verwerker voor jou, niet voor ons. Dus: een zakelijk abonnement met een verwerkersovereenkomst, training op jouw gegevens uitgezet, de leverancier opgenomen in je verwerkingsregister en een vermelding in je eigen privacyverklaring.

Wij helpen met de technische kant. Het papierwerk is van jou, en het valt mee.

Toegang intrekken

Verwijder het applicatiewachtwoord in het profiel van de gebruiker. De koppeling stopt direct. Verder verandert er niets.