

Hoe wijzig ik mijn e-mailwachtwoord via Roundcube?

Kies een nieuw e-mailwachtwoord. Raadpleeg ook de 'Algemene wachtwoordtips' op blz. 2.

Heb je een nieuw wachtwoord gekozen? Volg dan de stappen hieronder hoe je in Roundcube het wachtwoord aanpast.

Stap 1

Type voor een beveiligde verbinding met Roundcube: <https://jouwdomein.nl/roundcube>

Vul bij 'jouwdomein.nl' de door jou gebruikte domeinnaam in. De door jou gebruikte domeinnaam staat **achter** het @-teken van je e-mailadres.

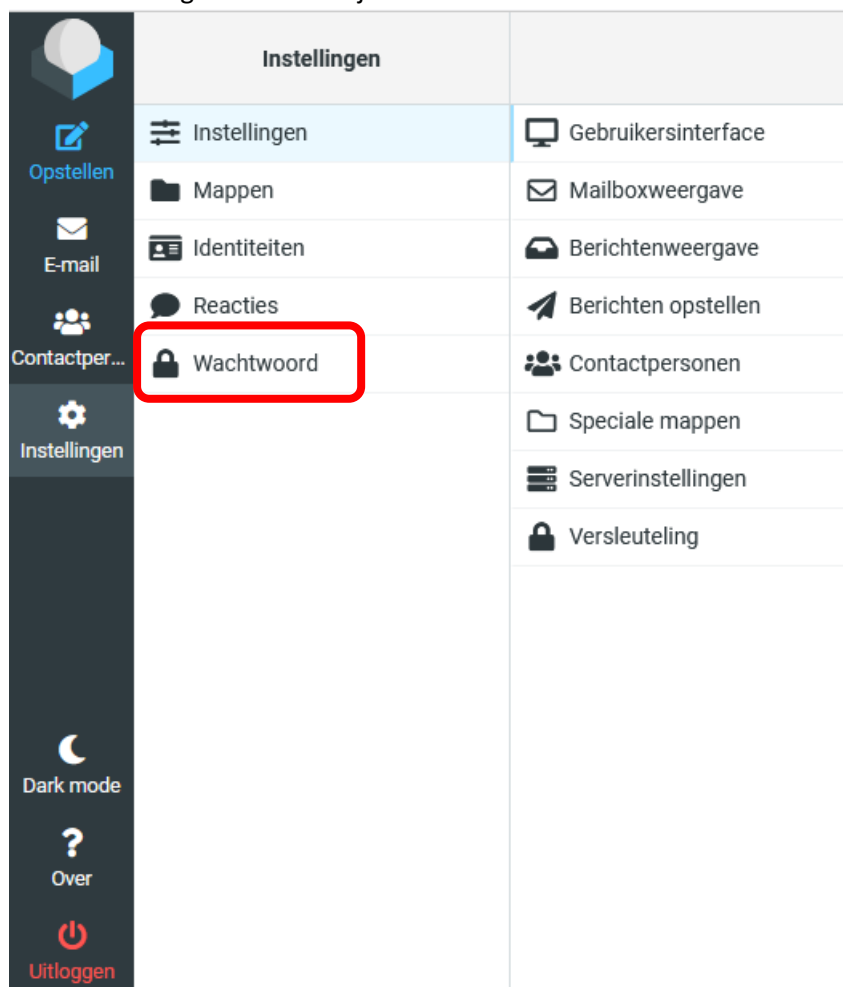
Stap 2

Login met je e-mailadres en wachtwoord.

Zodra je ingelogd bent in Roundcube, ga je naar '**Instellingen**'.

Stap 3

In het Instellingen scherm zie je links onderaan het menu '**Wachtwoord**'. Klik hierop.



Stap 4

Zodra je daarop geklikt hebt, krijg je een nieuw overzicht te zien. Hier vul je het oude wachtwoord in en daaronder het gekozen nieuwe wachtwoord.

Huidig wachtwoord:

Nieuw wachtwoord:

Bevestig nieuw wachtwoord:

Het wachtwoord moet minimaal 8 tekens lang zijn.

Na het invoeren en bevestigen van het nieuwe wachtwoord klik je op de knop '**Opslaan**'. Zodra je dit hebt opgeslagen, kun je direct gebruikmaken van je nieuwe wachtwoord!

LET OP!

Als je ook andere e-mailprogramma's gebruikt, zoals bijv. Outlook of Gmail, vergeet dan niet om in de instellingen daarvan het wachtwoord ook aan te passen met je nieuw aangemaakte wachtwoord.

Doe dit op alle apparaten die je gebruikt om je e-mail mee op te halen en te verzenden.

UITZONDERING: gebruik je om e-mail te **verzenden (smtp)** een andere server dan die van je inkomende e-mail, bijvoorbeeld de **smtp**-server van je Internetprovider, verander **dat** wachtwoord dan niet.

Algemene wachtwoordtips

Een wachtwoord moet lang en uniek zijn om geautomatiseerde aanvallen van criminelen af te weren. Met moderne technieken kunnen ze soms miljarden wachtwoorden per seconde proberen. De volgende tips maken je wachtwoorden moeilijker te kraken:

- **Hoe meer tekens, des te veiliger.** Acht tekens is aan de korte kant. Het is verstandiger een lengte van minimaal 12 tekens aan te houden. Dat maakt het wachtwoord tot 80 miljoen keer zo sterk. Maar meer tekens is nog beter.
- **Cijfers, hoofdletters en speciale tekens** (&, ?, #, !, %, enz.) versterken het wachtwoord.
- Het wachtwoord mag geen gemakkelijk te raden **persoonlijke informatie** bevatten, zoals een naam, geboortedatum of adres.
- Gebruik **verschillende wachtwoorden** voor elke website en dienst.

Een sterk wachtwoord kun je ook online laten aanmaken met een passwordgenerator.