INNOVOLTUS

New things under the sun


JULLIX

Brain of your energy management

# Tweestapsverificatie (2FA)

# Inhoudsopgave

# Tweestapsverificatie (2FA)

Om je account op het platform beter te beveiligen kan je een tweestapsverificatie of Two Factor Authenticatie inschakelen. Wanneer je dit inschakelt zal je naast je **gebruikersnaam** en je **wachtwoord** ook nog een 2de code moeten ingeven die gegenereert wordt door je **persoonlijk apparaat**.
*Heb je een installateur account dan is deze bijkomende beveiliging verplicht, dit wordt automatisch afgedwongen.*
De tweestapsverificatie in dit portaal is gebaseerd op de **TOTP-techniek** (Time-based One Time Passwords). Je persoonlijk apparaat met gratis app, wordt gekoppeld aan je account. Wanneer je wil inloggen geef je je gebruikersnaam en wachtwoord in en open je de app, de app zal een code laten zien die je moet ingeven in het login scherm. Deze code is maar 30 seconden geldig. *(Daarom is het belangrijk dat de klok van je persoonlijk apparaat juist staat.)*

## Inloggen met 2FA

Graag informeren wij u over een belangrijke extra stap in ons veiligheidsbeleid voor het energiemanagementsysteem (EMS) Jullix. Om de data van onze vele eindgebruikers van die Jullix te beschermen, activeren we tweefactorauthenticatie (2FA).

Installateurs die bij de klant een Jullix installeren, hebben toegang tot verschillende soorten gegevens van de klant. Die data vallen uiteraard onder de geldende privacywetgeving. Om eventuele datalekken te voorkomen, zetten we nu met 2FA een extra stap.

Wat is 2FA Inloggen met tweefactorauthenticatie verkleint de kans dat hackers toegang krijgen tot een account of data. 2FA gebruikt 2 verschillende middelen om in te loggen: je wachtwoord en een extra tweede stap zoals: Een tijdsgebonden code Bevestiging via sms-code Identificatie via een apparaatje Biometrische kenmerken zoals een vingerafdruk of gezichtsherkenning. Andere namen voor 2FA zijn tweestapsverificatie, tweetrapsauthenticatie of multifactorauthenticatie.

Waarom 2FA Dankzij 2FA vermijden we problemen wanneer een installateur een computer van een klant gebruikt voor de configuratie van een Jullix. Ongewild opgeslagen wachtwoorden vormen dan geen bedreiging. De klant kan het paswoord nadien niet gebruiken om in te loggen en toegang te krijgen tot data van andere klanten.

Hoe te werk gaan? 2FA wordt automatisch gestart voor de accounts van installateurs en kan niet omzeild worden. De installateur moet de 2FA beveiliging instellen en gebruiken. Daarbij maken we gebruik van de gratis apps zoals de Google-authenticator, de Microsoft Authenticator en Twilio Authy. Die zijn beschikbaar voor zowel Android als IOS. Twilio Authy kan ook gebruikt worden op Windows, macOS en Linux.

Bij het eerste gebruik maak je in de gekozen authenticator-app een account voor mijn.jullix.be aan. Je krijgt dan een QR-code die je kan scannen, of je geeft de beveiligingssleutel manueel in. Als je de volgende keer inlogt, geef je eerst je gebruikersnaam en wachtwoord in. Daarna voer je in ons portaal de cijfercode in die jouw authenticator app genereert. Het is dus belangrijk dat je voor installaties altijd het toestel meeneemt waarop je authenticator app staat. Anders kan je onmogelijk inloggen.