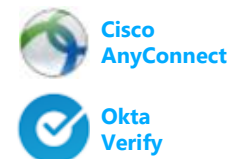


Beveiligde Toegang vanop Afstand op uw laptop

Gebruikershandleiding voor de vervanging van uw RSA token

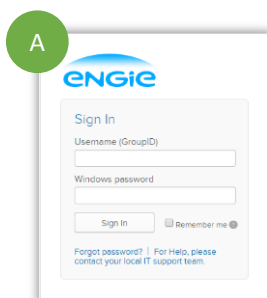
Dit document helpt je om:

- A. Je **smartphone** te registreren voor OKTA MFA om OKTA Verify te gebruiken – *sla deze stap over als je dit al hebt gedaan voor andere diensten (bv.: O365)*
- B. Je Okta account te configureren voor authenticatie via **SMS** op je **GSM** – *niet noodzakelijk als je de OKTA Verify app gebruikt, maar beide opties kunnen tegelijkertijd geactiveerd worden en naar keuze gebruikt*
- C. De dienst BTA te gebruiken met **Cisco AnyConnect** en **OKTA MFA** om je laptop met het ENGIE netwerk te verbinden.



A – Hoe je smartphone registreren voor Okta MFA

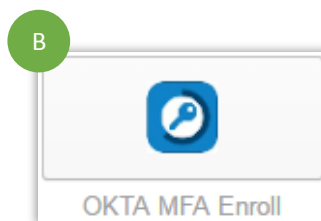
- 1 Op je smartphone : download de laatste versie van OKTA Verify via de gepaste app store (App Store, Play Store, Windows Store)
- 2 Op je laptop : volg volgende stappen om je smartphone te koppelen aan je OKTA account.



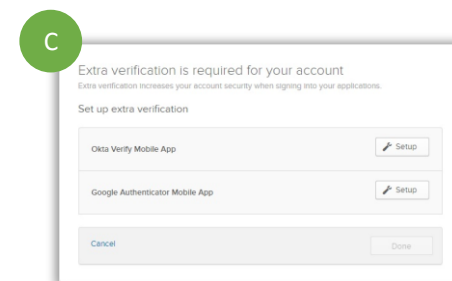
Ga naar <https://engie.okta-emea.com>

Vul in indien nodig:

- Gebruikersnaam: Group ID (in de vorm ABC123)
- Wachtwoord: Windows wachtwoord



Klik op "OKTA MFA Enroll"

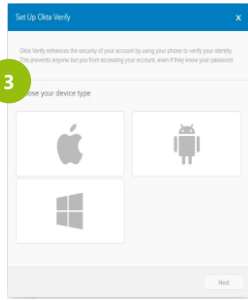


Selecteer de toepassing Okta Verify door te klikken op "Setup" en de instructies te volgen.

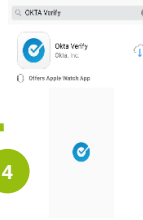
(kijk indien nodig op pagina 2)

A – Hoe je smartphone registreren voor Okta MFA

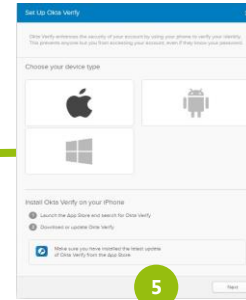
- 3 Kies het type toestel, klik op "volgende".**
Noot: Okta Verify is niet beschikbaar op Blackberry



- 4 Als je dit nog niet gedaan hebt, download of update de toepassing Okta Verify op je gsm.**

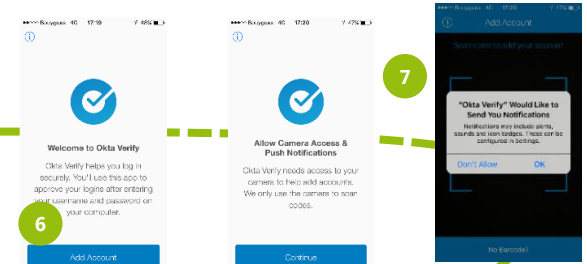


- 5 Klik op "volgende" op je computer wanneer de toepassing is geïnstalleerd op je gsm.**



- 6 Open Okta Verify op je gsm. Klik op "account toevoegen"**

- 7 Klik op "verdergaan" om "Camera Access & Push Notifications" toe te staan.**

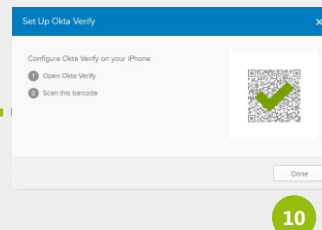


- 8 Volg stappen 9 tot 11, als je een pc of tablet met internetverbinding hebt tijdens de registratie. Is dit niet het geval, volg dan stappen 9' tot 14'**

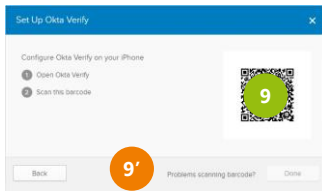
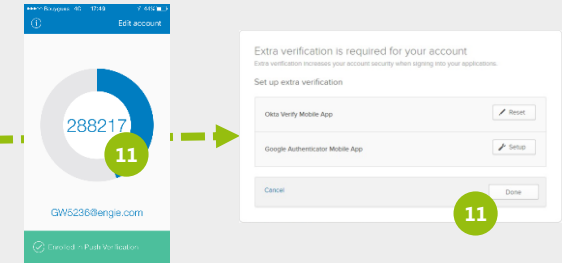
- 9 Scan de QR-code op je pc met je smartphone**



- 10 De camera herkent de QR-code. Klik op "klaar"**

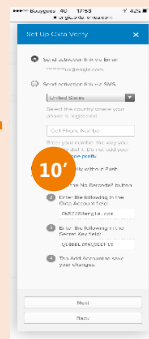


- 11 Je gsm is nu geconfigureerd voor OKTA MFA. Klik op "klaar" op je pc**



- 9' Klik op "Problemen om barcode te scannen?"**

- 10' Klik op "handmatig instellen zonder push notificatie" en kopieer de velden Okta Account en Secret Key**



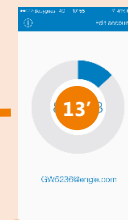
- 11' Ga naar de toepassing Okta Verify en klik op "No Barcode?"**



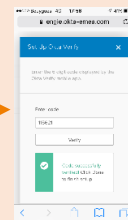
- 12' Plak de velden Okta Account en Secret Key**



- 13' Kopieer de Okta-code**



- 14' Ga naar de browser en klik op "Next". Plak de Okta-code en klik op "Verify". Je smartphone is nu geconfigureerd voor MFA**



B – Instellen van je Okta account om SMS als tweede authenticatiefactor te gebruiken

Volg volgende stappen op je pc om je **GSM** te registreren :

1

Surf naar <https://engie.okta-emea.com>

Geef indien nodig volgende gegevens in :

- Username: GroupID (vb. ABC123)
- Password: Windows Password

2

Klik op het kleine pijltje naast je naam en kies 'Instellingen'.

3

Kies 'Profiel bewerken'.
Als deze knop niet verschijnt,
ga door naar stap 5

4

Geef je windows wachtwoord in en klik op 'Verifiëren'.

5

In het blok 'Extra verificatie',
Klik 'instellen' bij verificatie via tekstbericht.

6

Kies het land (Belgium) en geef je mobiele nummer in. Klik op 'Verstuur code', je zal nu een verificatiecode via SMS ontvangen.

7

Vul de verificatiecode in en klik op 'Verifiëren', vervolgens op 'Klaar'. Je Okta account is nu ingesteld om gebruik te maken van verificatie via SMS.

B – Gebruik de BTA van Cisco AnyConnect met Okta MFA

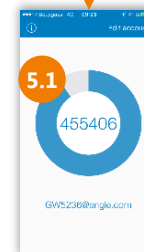
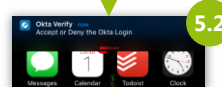
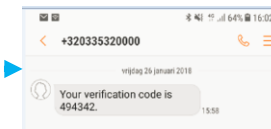
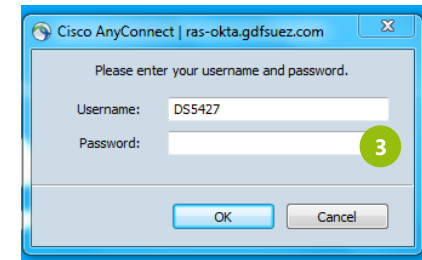
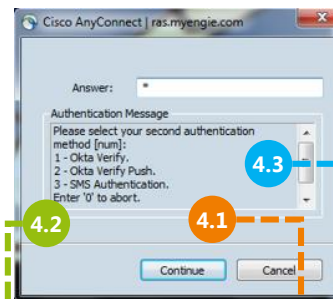
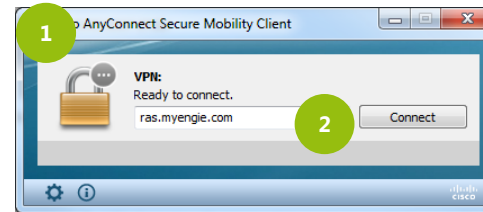
- 1 Open de toepassing **Cisco AnyConnect** op je computer
Via het menu « Start » of het Windows Notification Center

- 2 Selecteer de url **ras.myengie.com**
Opgelet: gebruik niet ras.gdfsuez.com

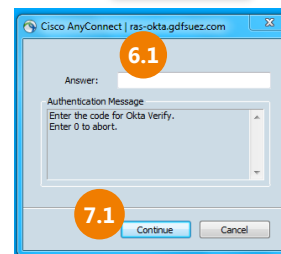
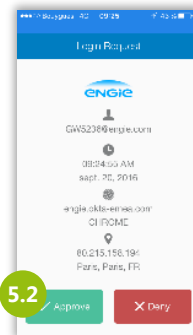
- 3 Vul de volgende gegevens in:
- Gebruikersnaam: **UserID** (bv.: ABC123)
 - Wachtwoord: **Windows**-wachtwoord

- 4 Drie opties worden voorgesteld
- 1 – **Okta Verify** (je moet een code kopiëren)
 - 2 – **Okta Verify Push** (je moet een melding accepteren)
 - 3 – **SMS Authentication** (je krijgt een code per SMS)

- 5.2 Afhankelijk van je type gsm (iOS, Android) moet je:
- (indien voorgesteld) Klikken op de melding
 - Snel** de vraag accepteren
- Antwoord je buiten de tijd, dan begin je opnieuw met stap 4*

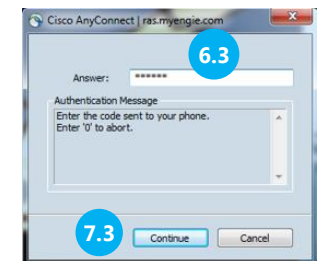


Open Okta Verify op je GSM



Vul op de authenticatiepagina de code in, die je verkreeg via de toepassing Okta Verify.

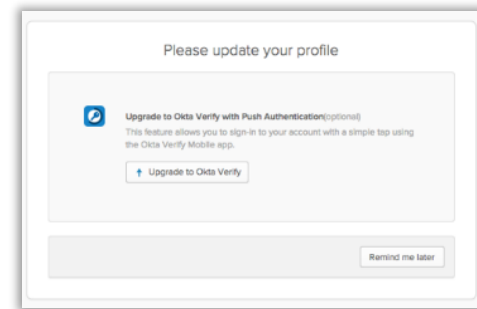
Klik on "Continue"



Vul op de authenticatiepagina de code in, die je verkreeg via SMS.

Klik on "Continue"

- **Ik heb me meer dan 5 keer vergist tijdens de aanmeldingsprocedure**
 - Het Okta-account blokkeert automatisch na vijf foutieve pogingen. Wacht 10 minuten voor je opnieuw probeert. Contacteer je lokale Service Desk als het probleem aanhoudt.
- **Ik krijg geen melding van Okta Verify Push als ik via wifi geconnecteerd ben**
 - Sommige wifi-netwerken (vooral publieke) kunnen Okta Verify Push blokkeren. Probeer opnieuw via het 4G-netwerk.
 - Kan je geen verbinding maken met 4G, kies dan voor Okta Verify met code.
- **De optie Okta Verify Push werkt niet (login failed)**
 - Het functioneren van deze optie hangt af van de kwaliteit van je mobiele netwerk (4G). Als de dekking van het netwerk niet volstaat, probeer dan opnieuw met de optie Okta Verify met code.
- **Ik heb een andere gsm. Hoe beëindig ik de registratie van mijn oude gsm?**
 - Ga naar <https://engie.okta-emea.com>
 - Rechts bovenaan de pagina, klik je op "Settings" en dan op "Edit Profile"
 - In het tabblad "Extra Verification", klik je op "Reset" voor de mobiele toepassing Okta Verify
 - Als je oude toestel is uitgeschreven, kan je het nieuwe registreren.
- **Mijn smartphone is geregistreerd, maar ik kan geen push meldingen versturen**
 - Gebruik je je gsm voor MFA maar kan je geen meldingen versturen, dan moet je gaan naar <https://engie.okta-emea.com>
 - Vul je logingegevens in. De pagina hiernaast verschijnt een keer per dag
 - Volg de instructies



- **Ik ben mijn smartphone kwijt of ik heb de toepassing verwijderd zonder eerst uit te schrijven**
 - Contacteer je lokale Service Desk met vermelding van je UserID.
- **Maar... wat is multifactor-authenticatie (MFA) ?**
 - Door authenticatie zijn we zeker dat een gebruiker is wie hij of zij zegt te zijn. Hoe meer factoren we gebruiken, hoe meer zekerheid we hebben. Multifactor-authenticatie (MFA) kan door een combinatie van de volgende factoren: kennis (een wachtwoord), bezit (een token) en een persoonlijke eigenschap (een digitale vingerafdruk).

Vragen of hulp nodig,
gelieve dan je lokale IT Service Desk te
contacteren