# Externe SAML SSO-verificatie configureren voor ESA- en SMA-beheer

## Inhoud



## Inleiding

In dit document wordt beschreven hoe SAML 2.0 SSO-externe verificatie voor ESA- en SMA-systeembeheer kan worden geconfigureerd.

### milieu

- Producten: Email Security Appliance (ESA), Security Management Appliance (SMA)
- Van toepassing op: ESA- en SMA-systeembeheer
- Clustergedrag: Serviceleverancier (SP)- en IdP-profielen worden geconfigureerd op machineniveau; externe verificatietoewijzing wordt geconfigureerd op clusterniveau.

## Voorwaarden

- Administratieve toegang tot de ESA/SMA-webinterface
- X.509-certificaat en privésleutel beschikbaar in PKCS # 12 (PFX) of PEM-formaat (zelf

ondertekend of CA-ondertekend)
- Toegang tot een Identity Provider (IdP)-toepassing van derden en de SAML-metagegevens/SSO-URL

### Controlelijst voor voorconfiguratie

- Controleer de hostnaam/FQDN van de beheerinterface die beheerders gebruiken om toegang te krijgen tot het toestel; bevestig dat de URL van de Assertion Consumer Service (ACS) overeenkomt met die hostnaam.
- Als het toestel zich in een cluster bevindt, moet u SAML voor elk lid op machineniveau configureren voordat u de externe verificatie van SAML inschakelt.
- Bepaal of de IdP een afzonderlijke toepassing of domein per toestel vereist.
- Bevestig dat de vereiste certificaten en sleutels beschikbaar zijn.
- Bevestig dat de IdP het attribuut groep of rol verzendt dat vereist is voor de toewijzing van ESA/SMA-rollen.

---

Let op: Dit document is niet van toepassing op de eindgebruikerquarantaine (EUQ) SAML SSO.

---

## Achtergrondinformatie

- Cisco TAC biedt geen technische ondersteuning voor IdP-configuraties van derden. Voorbeelden van configuratiereferenties worden verstrekt voor algemene IdP's.

SSO SAML-id's

- Duo Access Gateway (DAG) voegt tweefactorauthenticatie toe, compleet met populaire cloudservices met behulp van SAML 2.0-federatie.
- Active Directory Federation Services (ADFS) - getest met ADFS 2,3,4, Azure Active Directory (Azure AD), SecureAUTH en PingFederate
- Aanvullende tweefactorauthenticatie kan worden gebruikt als de IdP deze ondersteunt binnen het SAML 2.0 Single Sign-On-framework.
- Okta ondersteunt authenticatie met een IdP die de service ondersteunt.

### De ESA/SMA configureren als serviceprovider

Navigeer naar Systeembeheer > SAML > (Machineniveau) > Serviceverlener toevoegen.

---

Opmerking: ESA's in een cluster vereisen configuratie op machineniveau voor alle leden van het cluster voordat SAML kan worden ingeschakeld.

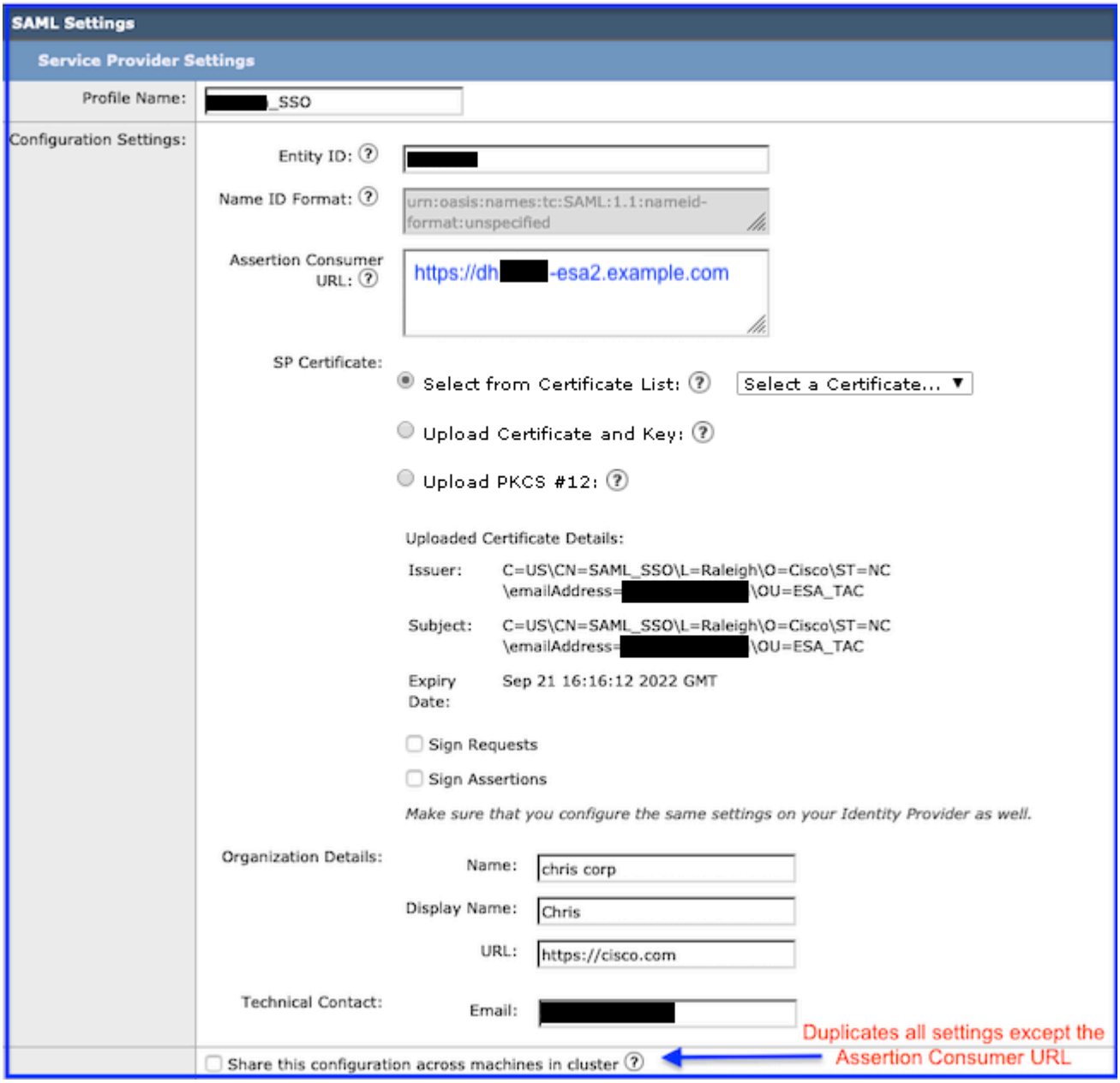
---

- Als de optie onder aan de pagina, Deze configuratie delen op systemen in het cluster, is geselecteerd, zijn de volgende voorwaarden van toepassing:
    - Alle velden worden gerepliceerd naar de clusterleden, behalve de URL Assertion Consumer.
    - De Assertion Consumer URL vult automatisch de hostnaam van de beheerinterface in als de ACS.
    - Omgevingen die een alternatieve hostnaam gebruiken om toegang te krijgen tot de host, vereisen handmatige configuratie voor elke host, bijvoorbeeld CES-gehoste apparaten.
    - Profielnaam: naam die wordt gebruikt om de SP-instantie in de ESA- of SMA-interface te labelen.
    - Entiteit-ID: naam die wordt gebruikt voor de SP-instantie zoals de IdP deze ziet. Deze naam is het label dat door de IdP wordt gebruikt om de SP te vertegenwoordigen. Dit kan elke naam zijn, bijvoorbeeld ESA_SP of ESA_SSO.
    - Naam-ID-indeling: niet-configureerbaar veld.
    - Bewering Consument URL of Bewering Consumentenservice (ACS): URL die door de IdP wordt gebruikt om te communiceren met deze ESA / SMA-host.
    - SP-certificaat:
        - Formaat: X.509 publiek/private certificaten in PFX/PKCS12 of PEM formaat.
        - Optie 1: Maak een keuze uit de certificatenlijst: selecteer een van de certificaten die al in het ESR zijn gemaakt in Netwerk > Certificaten.
        - Optie 2: certificaat en sleutel uploaden: een certificaat en sleutel met PEM-indeling uploaden.
        - Optie 3: Upload PKCS #12: Upload een PKCS #12 bestand.
        - Optioneel: maak een zelf ondertekend certificaat op de ESA/SMA voor SAML Single Sign-On.
        - Bescherm de persoonlijke sleutel indien nodig met een wachtwoord.

---

Opmerking: als u certificaten met PEM-indeling gebruikt, bewaart u elk certificaat en elke privésleutel in afzonderlijke bestanden.

---




Pagina Installatie van serviceprovider

Pagina Installatie van serviceprovider

- Verzoeken ondertekenen: optie om ESA/SMA SAML-communicatie te ondertekenen die naar de IdP wordt verzonden.
- Beweringen ondertekenen: Optie om de IdP te verplichten beweringen te ondertekenen die naar de ESA/SMA zijn verzonden.
- Organisatiegegevens: kan worden ingevuld met de juiste bedrijfsgegevens.
- Wijzigingen indienen en vastleggen om de instellingen te behouden.
- Download de SP-metagegevens van de SAML-configuratiepagina.

## De Identity Provider (IdP) configureren voor gebruik met de ESA/SMA-toestellen

Opmerking: voor sommige IdP's zijn afzonderlijke toepassingen of realms vereist voor elke ESA. (voorbeeld: DUO)

Deze koppelingen bieden voorbeeldconfiguraties voor meerdere IdP's op het moment van publicatie.
Cisco TAC biedt geen technische ondersteuning voor producten van derden. Deze voorbeelden worden gegeven als referenties.

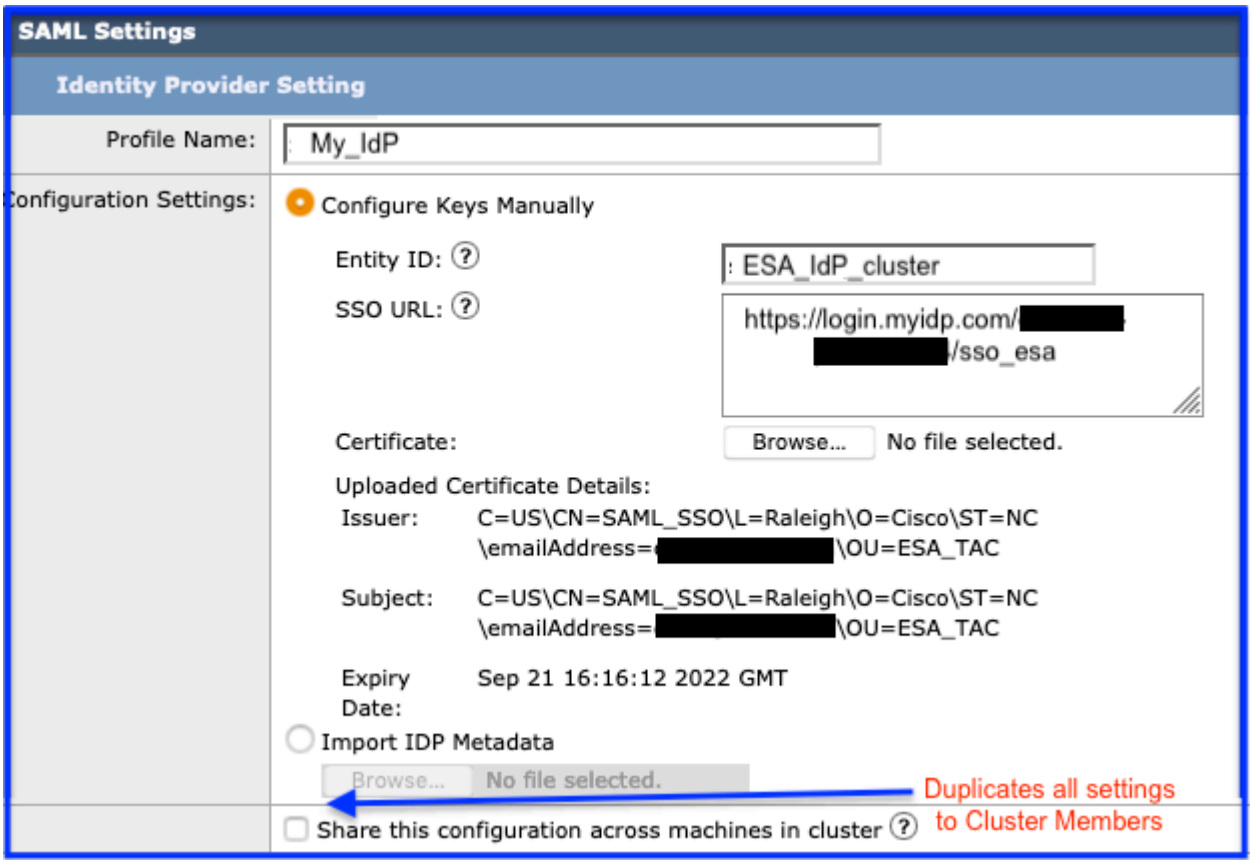
## IDP-instellingen configureren op de ESA/SMA

1. Ga naar Systeembeheer > SAML.

2. Selecteer Identiteitsprovider toevoegen.

- Er zijn twee opties beschikbaar:
- IdP-metagegevens importeren
- Toetsen handmatig configureren:
    - Entiteit-ID: kan elke waarde zijn die wordt gebruikt om de IdP te identificeren
    - SSO-URL: URL waarnaar de SP SAML-verificatieverzoeken stuurt
    - Upload de privésleutel en het openbare certificaat in afzonderlijke bestanden

3. Deel deze configuratie met alle machines in het cluster om de configuratie met alle ESA's in het cluster te repliceren:

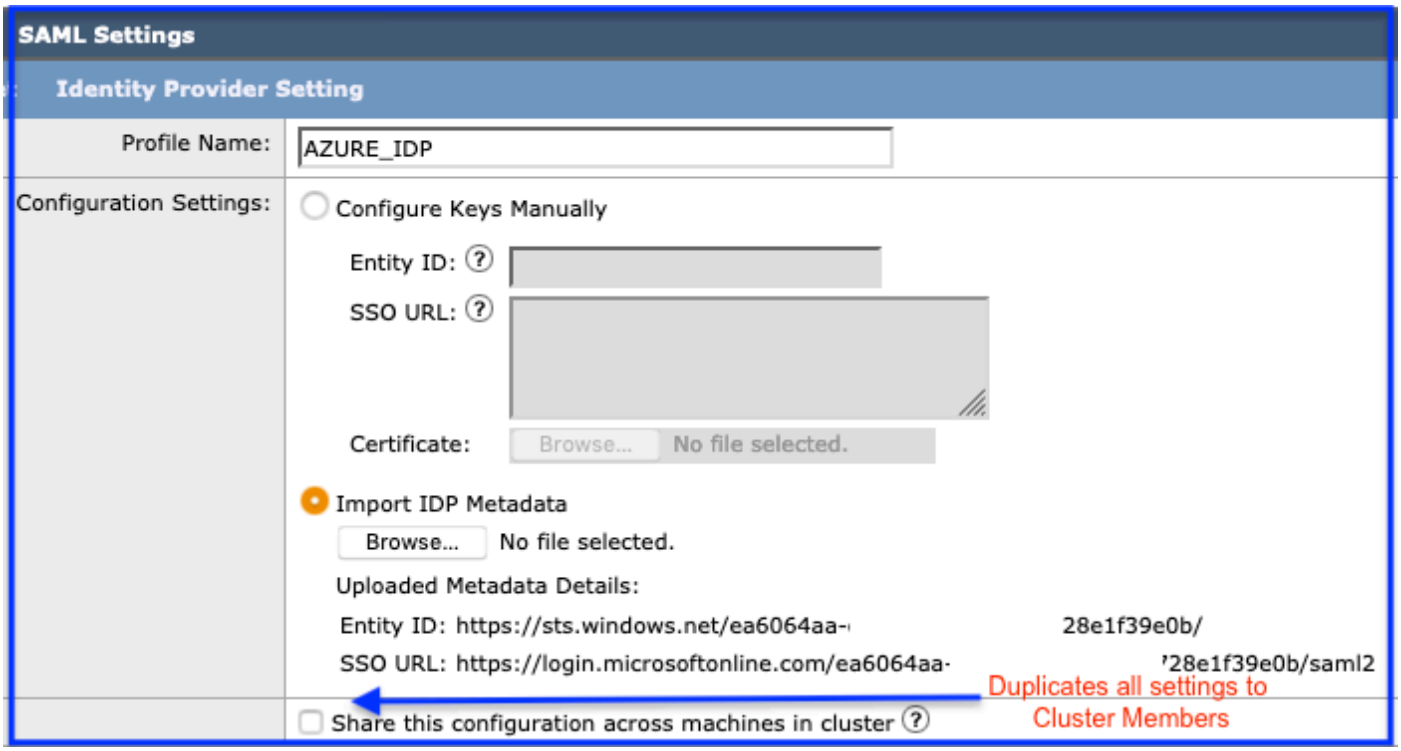



Handmatig IDp-inhoud invoeren

Handmatig IDp-inhoud invoeren

4. Metagegevens uploaden vanaf IdP

- Selecteer IdP-metagegevens importeren.
- Blader naar het metagegevensbestand dat is opgeslagen in de IdP en sla de configuratie op.
- De optie om deze configuratie te delen over systemen in een cluster is beschikbaar als deze van toepassing is op de implementatie.




Metagegevens uploaden van IDP

Metagegevens uploaden van IDP

## Externe verificatie inschakelen met SAML op de ESA/SMA

Net als bij externe LDAP-verificatie, vereist SAML Single Sign-On mapping om groepen toe te wijzen aan beheerdersrollen.

1. Navigeer naar Systeembeheer > Gebruikers (clusterniveau) > Externe verificatie > Inschakelen.

2. Selecteer Verificatietype: SAML.

3. Attribuutnaam voor overeenkomende naamtoewijzing (optioneel): Voer de naam van het kenmerk in om te zoeken in de groepstoewijzing.

---

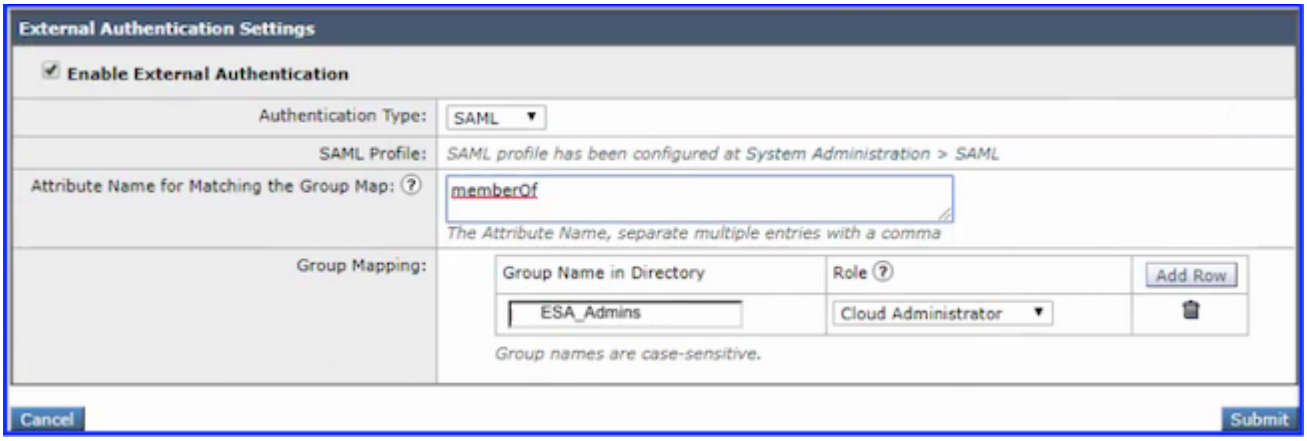
Opmerking: De naam van het kenmerk is afhankelijk van de kenmerken die zijn geconfigureerd voor de Identity Provider om door te geven in de SAML-reactie. Het toestel zoekt naar overeenkomende items van de opgegeven attribuutnaam in het SAML-antwoord tegen de attributen die zijn geconfigureerd in het veld Groepstoewijzing. Als dit veld niet is geconfigureerd, zoekt het toestel alle attributen die aanwezig zijn in de SAML-respons tegen het geconfigureerde veld Groepstoewijzing.

---

4. Voer het attribuut groepsnaam in zoals gedefinieerd in de SAML-directory op basis van de

vooraf gedefinieerde of aangepaste gebruikersrol.

- Het veld Groepstoewijzing moet een groepskenmerk bevatten. Het kenmerk Niet-gespecificeerde groepen kan worden toegevoegd om SAML-beweringen of -antwoorden te verifiëren.




Instellingen voor externe verificatie

Instellingen voor externe verificatie

5. Wijzigingen indienen en vastleggen.

Nadat de configuratie is voltooid, wordt een nieuwe koppeling weergegeven onder aan de aanmeldingspagina. Op de aanmeldingspagina van ESA/SMA wordt een koppeling Eenmalige aanmelding gebruiken weergegeven waarmee beheerders worden doorverwezen naar de bedrijfsidentiteitsprovider (IdP).

Als deze optie is geselecteerd, wordt de beheerder doorgestuurd naar de SAML-aanmeldingspagina van het bedrijf.

# Problemen oplossen

Gebruik deze indicatoren om vast te stellen of het probleem verband houdt met de toestelconfiguratie of de IdP-configuratie.

## SSO Redirect Link verschijnt niet op de aanmeldingspagina ("Single Sign-On gebruiken")

Controleer of Systeembeheer > Gebruikers > Externe verificatie > SAML is geconfigureerd.

## Omleiden Keert terug naar de ESA/SMA-aanmeldingspagina met "Single Sign-On Authentication Failed! Neem dan contact op met uw beheerder."

Fout: "Verificatie bij eenmalige aanmelding mislukt! Neem dan contact op met uw beheerder."

- Verificatie mislukt bij de IdP.
    - Dit geeft aan dat de configuratie werkt totdat de verificatiepagina voor eenmalige aanmelding is bereikt en referenties zijn ingediend.
    - Deze fout is vaak te wijten aan de IdP-configuratie en vereist aanvullende verificatie van IdP-instellingen.

## Omleiden Retourneert naar ESA/SMA-aanmeldingspagina met "Autorisatie mislukt! Neem dan contact op met uw beheerder."

Fout: "Fout bij autorisatie! Neem dan contact op met uw beheerder."

- De authenticatie is geslaagd, maar de autorisatie is mislukt bij de ESA/SMA.
    - Focus op de instellingen in Gebruikers > Externe verificatie > SAML.
        - Attribuutnaam, groepsnaam en groepstoewijzing.

## Gerelateerde informatie

- Cisco Email Security Appliance - Gebruikershandleidingen
- Cisco Content Security Management Appliance - Gebruikershandleidingen
- Cisco Web Security - Gebruikershandleidingen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.