Rechten voor AMP voor endpoints

Inhoud

Inleiding

Dit document beschrijft het proces voor het verkrijgen van de Advanced Malware Protection (AMP)-licentie, inclusief de toegang tot het Dashboard.

Bijgedragen door Uriel Islas, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van:

- Advanced Malware Protection voor endpoints
- E-mailaccount
- Computer

Gebruikte componenten

Dit document is niet beperkt tot specifieke softwareversie. Dit document is echter gebaseerd op deze software:

- AMP openbare cloud
- Outlook

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van een stap begrijpt.

Configureren

U kunt uw AMP for Endpoints (AMP4E) product herkennen door naar de e-mail van levering of een e-mail met rechten te verwijzen.

> Opmerking: Als u geen toegang hebt tot het e-mailadres, kunt u contact opnemen met:

licensing@cisco.com of bezoek de onlineportal op http://cisco.com/tac/caseopen. Selecteer na het selecteren van de juiste technologie en subtechnologie de optie **Licentie** die wordt vermeld onder **Type of Probleem**.

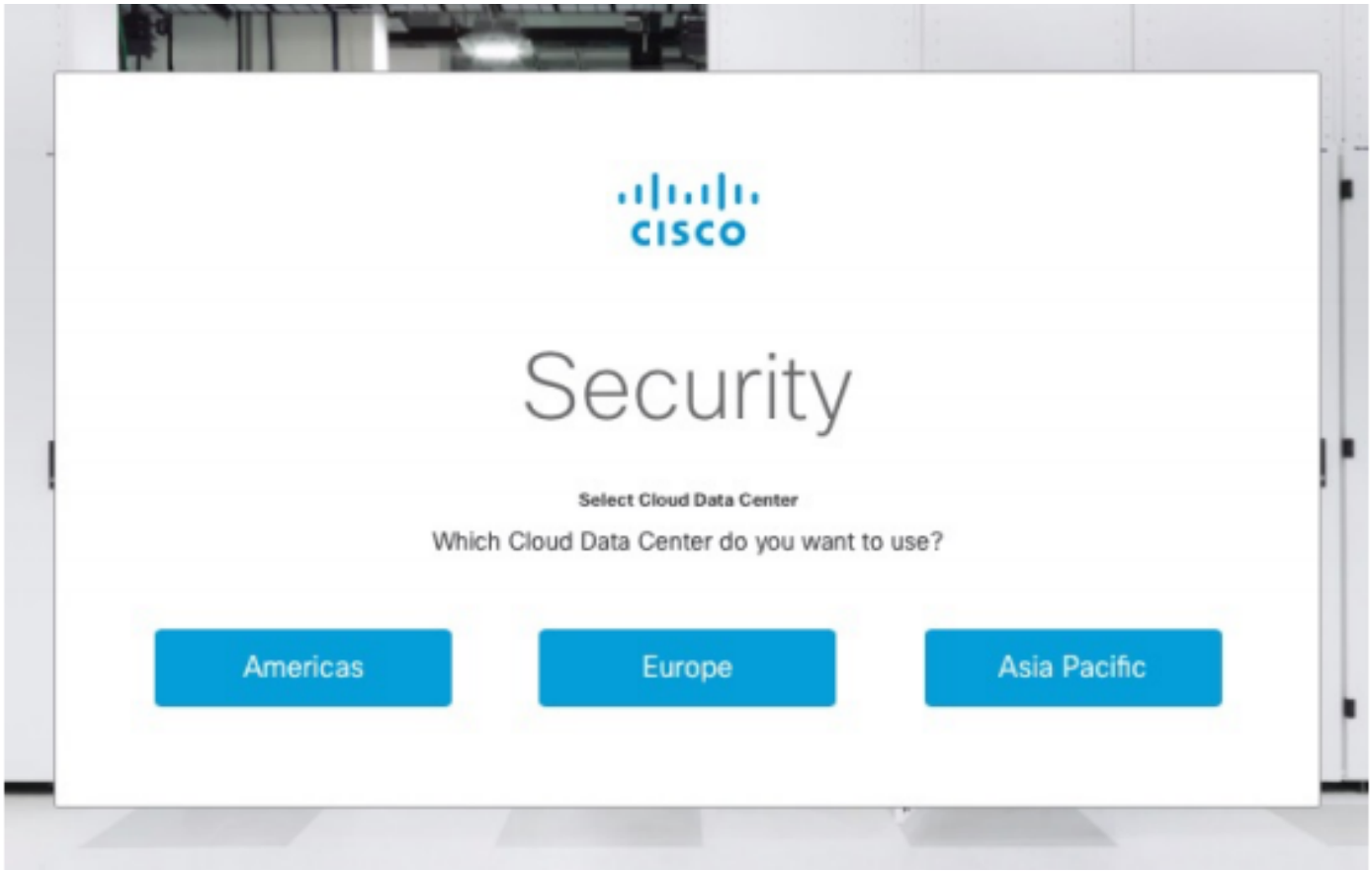
Advanced Malware Protection voor endpoints

AMP4E-aanmeldingsgegevens behoren tot het Cisco Security Account (CSA) domein. Zodra de eerste Cisco Security-rekeningen zijn ingesteld, kunt u verdere security beheerders binnen uw organisatie toevoegen. Op het moment dat u uw licentie toepast om een nieuw cloudexemplaar te hechten, maakt u een CSA of kunt u de licentie invoeren met uw bestaande CSA-referenties. Als het gedaan is, moet een organisatie gebonden zijn voor je bedrijf.

Een nieuwe openbare cloud instellen

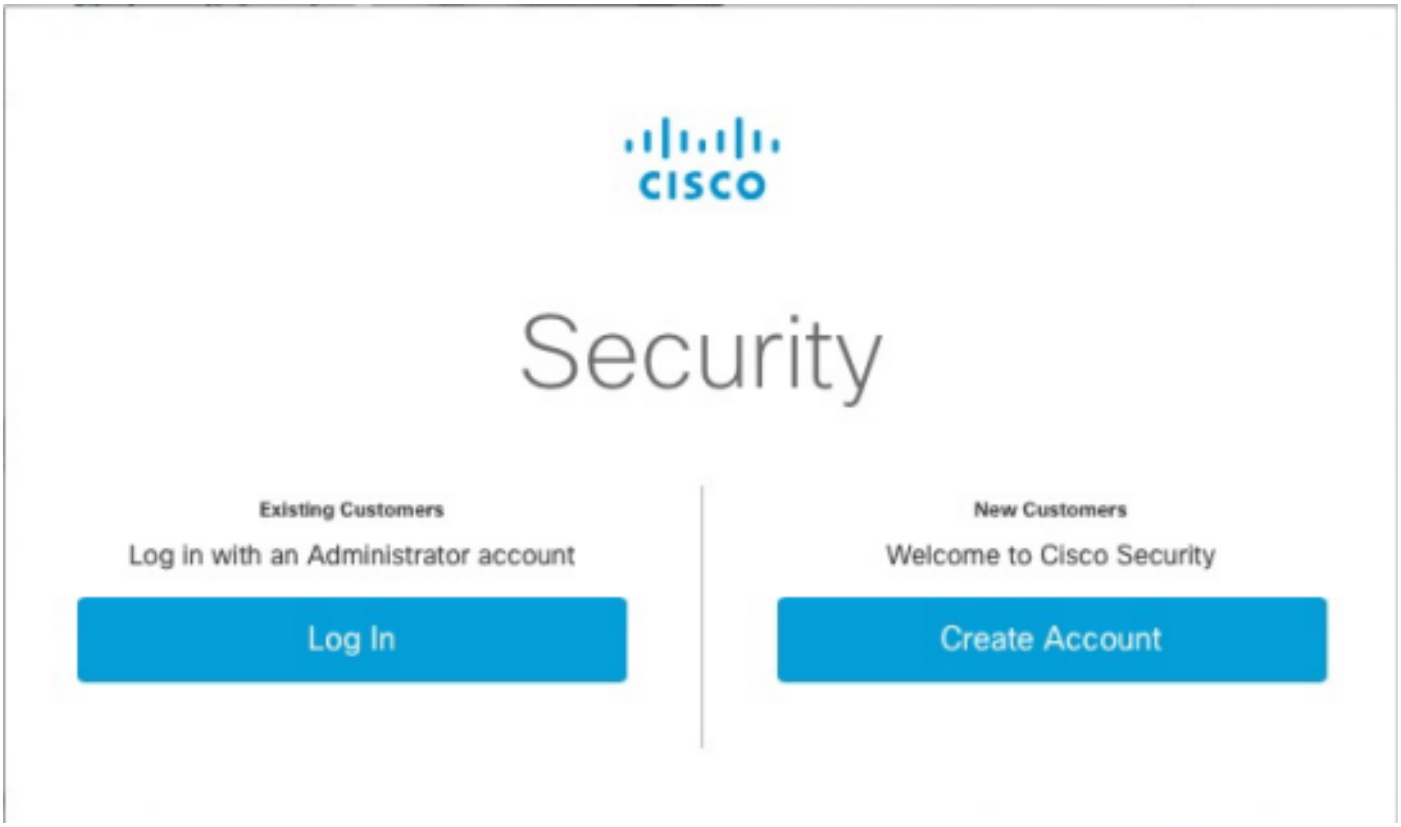
Stap 1. Navigeer onder de URL die in de e-mail van levering of in de e-mail van rechten is voorzien.

Stap 2. Selecteer uw gewenste Cloud Data Center.



Opmerking: De Amerikaanse cloud kan voor alle landen worden gebruikt. Er zijn geen kwesties die te maken hebben met latentie voor landen die ver weg zijn.

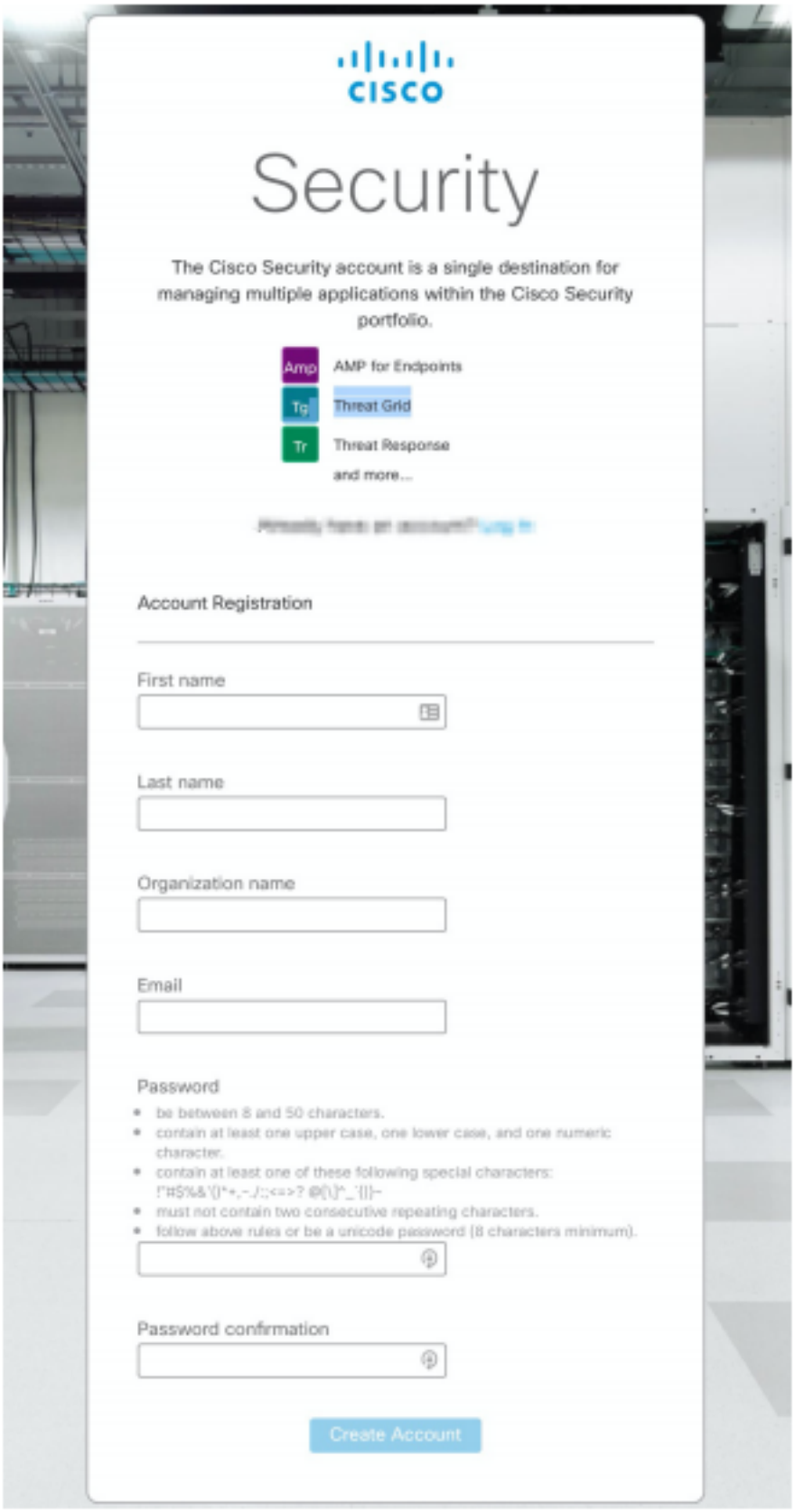
Stap 3. Koppel uw Cisco-beveiligingsaccount aan de AMP-cloud.



a) Als u al de aanmeldingsgegevens voor een CSA hebt, maar niet voor AMP4E, klik dan op **Inloggen**. Deze optie moet uw CSA aan de AMP wolk verbinden.

b) Als u geen AMP-wolk hebt of Cisco Security Org hebt ingesteld, klik op **Create Account** om de licentie voor uw bedrijf toe te passen.

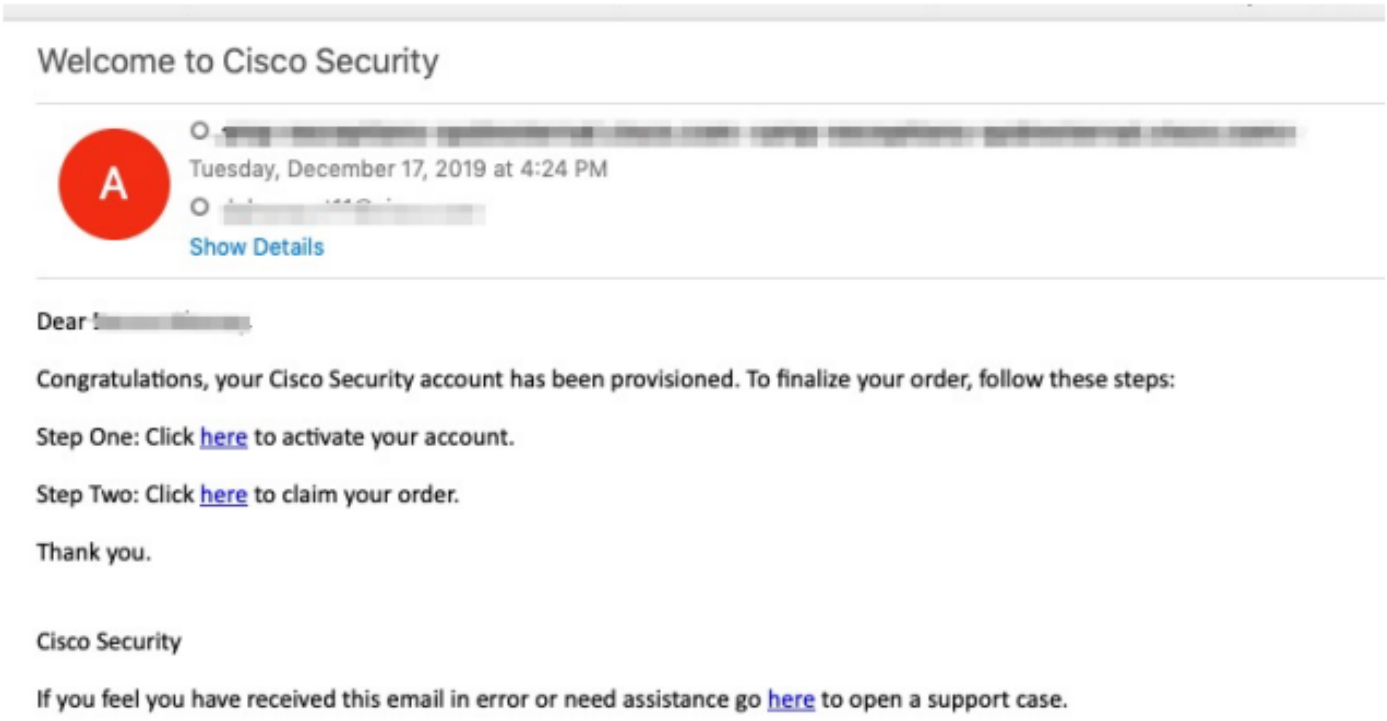
Stap 4. Als uw bedrijf geen CSA heeft, voer dan de waarden voor alle velden in zoals gevraagd om op te zetten.



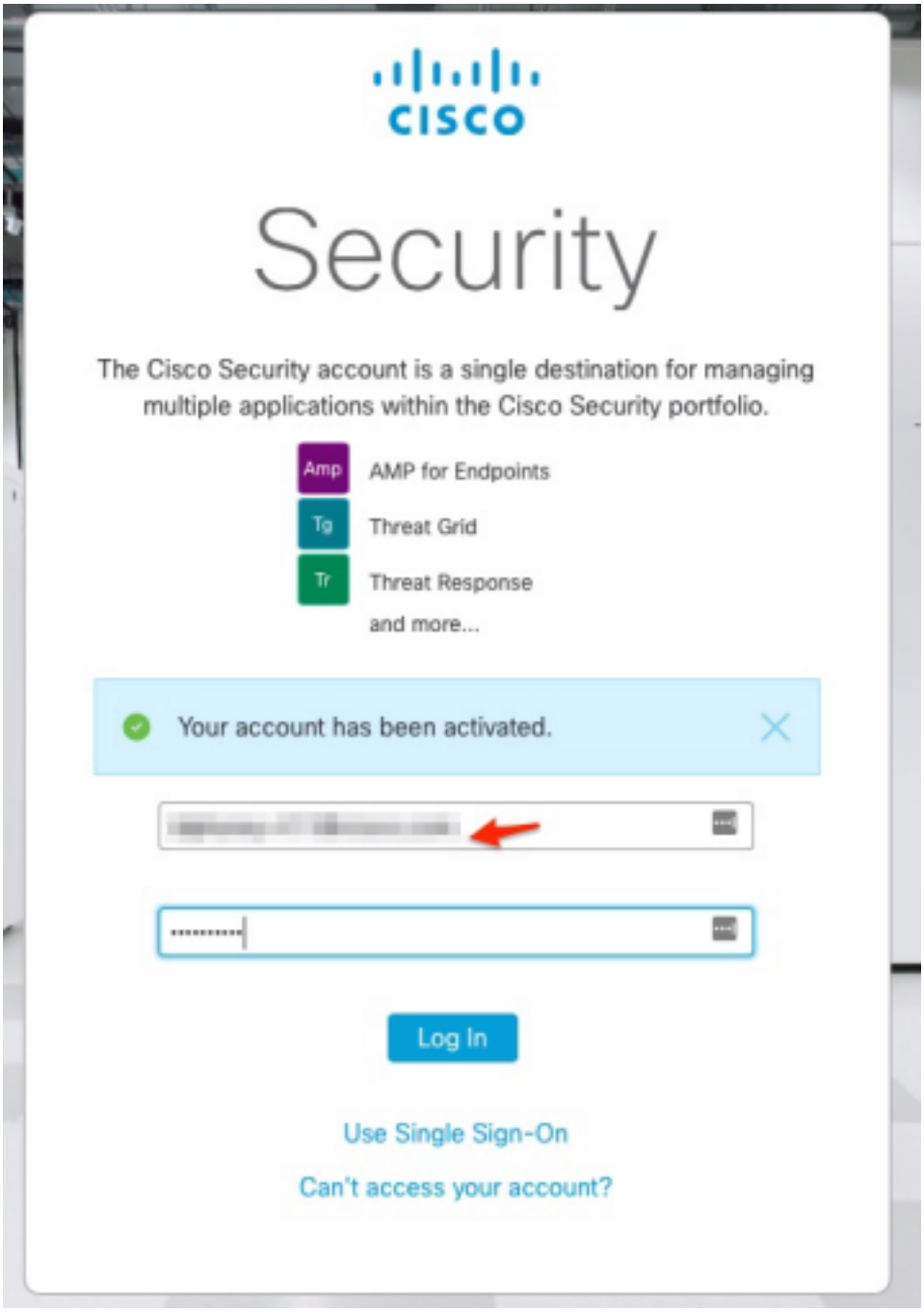
Opmerking: Als iemand al een CSA op je bedrijf heeft, dan navigeer onder kasteel website om je geloofsbrieven te controleren. Selecteer de URL op basis van de cloud die is ingesteld op nummer 2. **De Amerikaanse cloud**: https://castle.amp.cisco.com **Europe Cloud**: https://castle.eu.amp.cisco.com **Asia Pacific Cloud**: https://castle.apjc.amp.cisco.com.

Stap 5 **.** Zodra het CSA is gemaakt, wordt er een volledige pagina voor de registratie van rekeningen weergegeven.

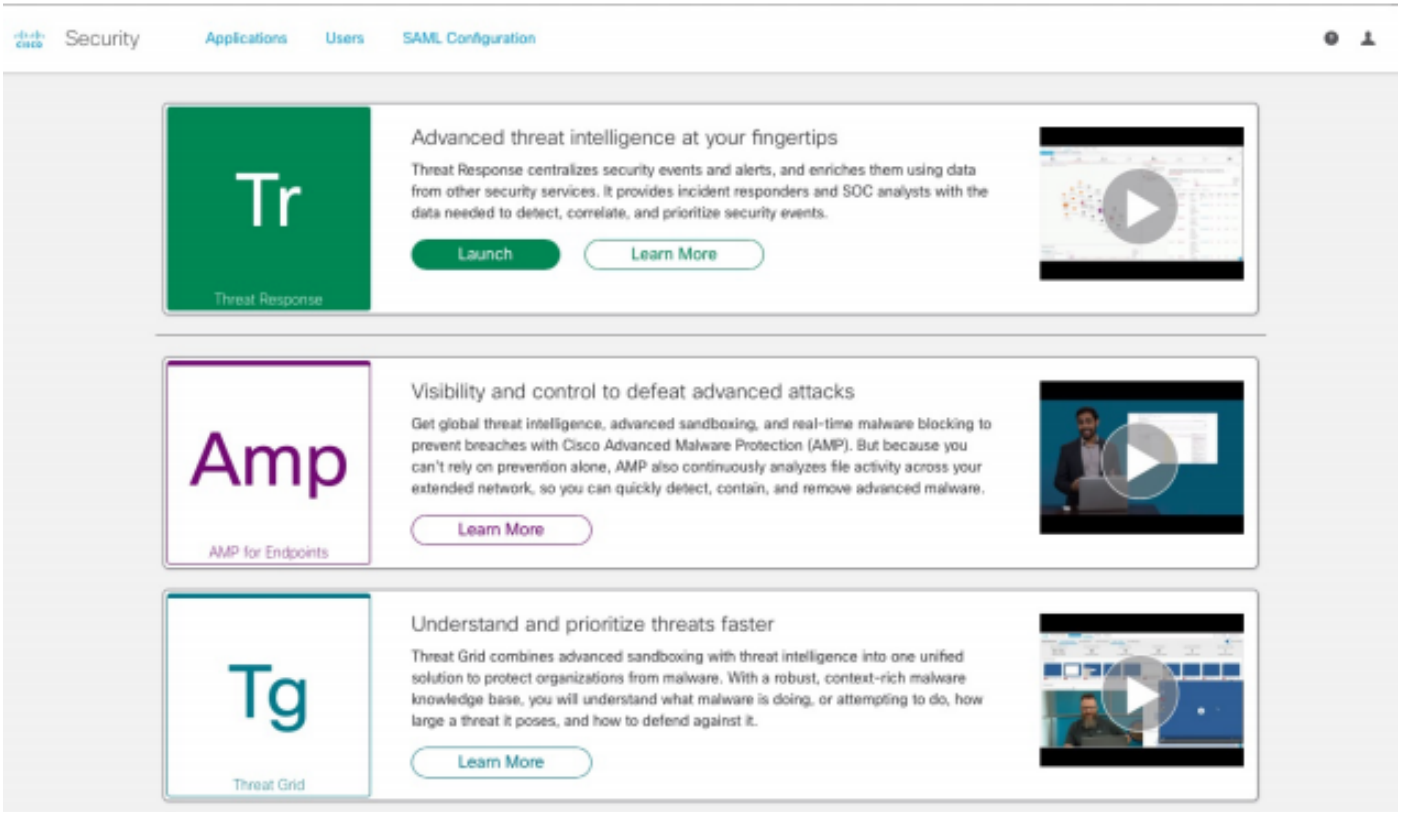
Stap 6. Controleer een nieuw Welkom in Cisco Security-e-mail vanaf no-reply@amp.cisco.com.



Stap 7. activeer uw account vanaf de welkome e e-mail op stap 1



Stap 8. Verificatie in kasteel website is afhankelijk van de vorige wolk die op uw bedrijf is ingesteld.

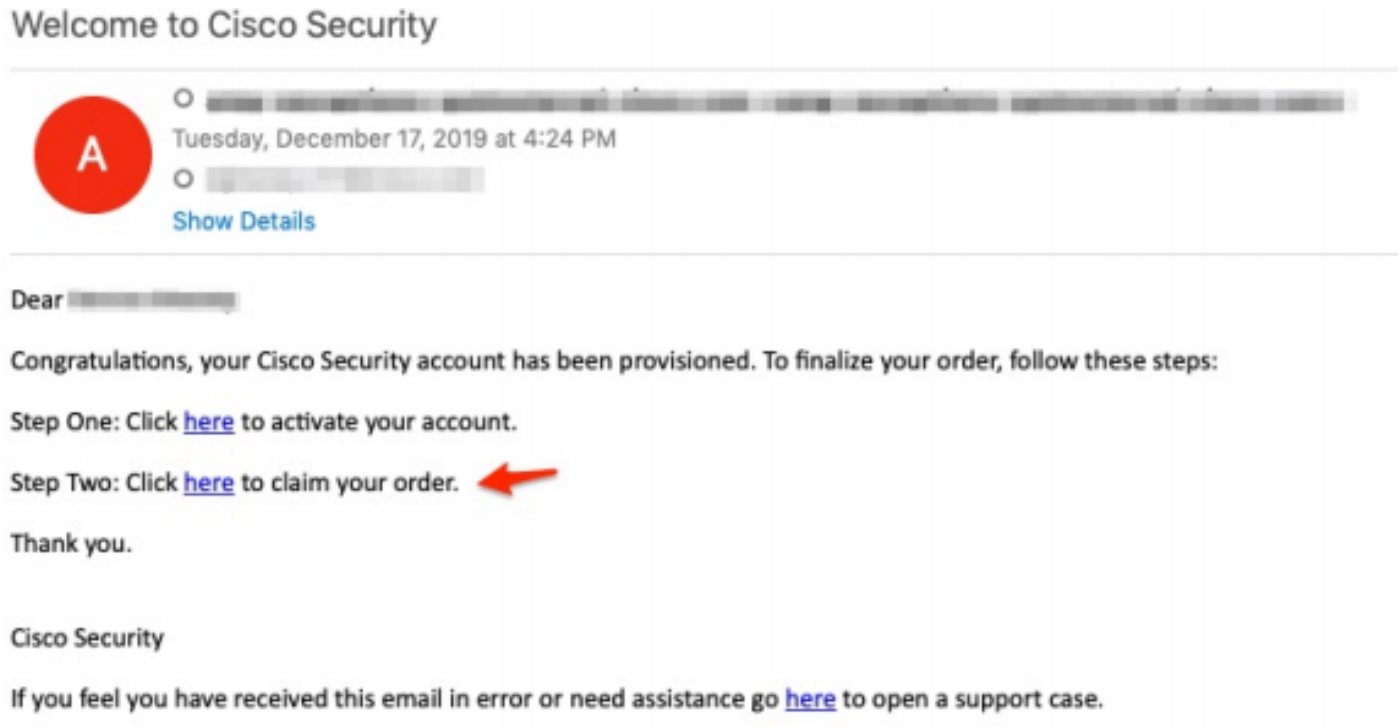


De Amerikaanse cloud - https://castle.amp.cisco.com

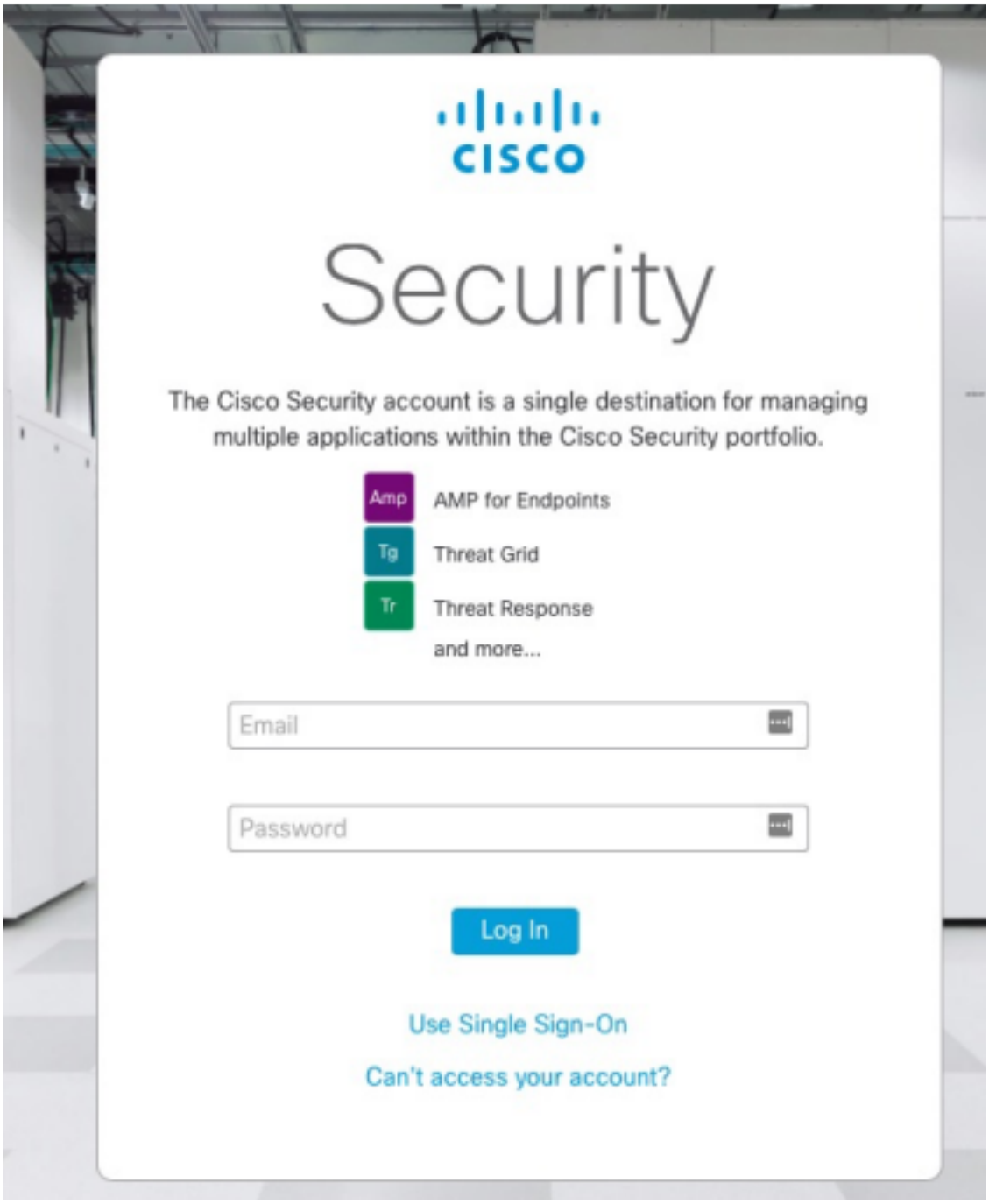
Europa Cloud - https://castle.eu.amp.cisco.com

Zuidoost-Azië - https://castle.apjc.amp.cisco.com

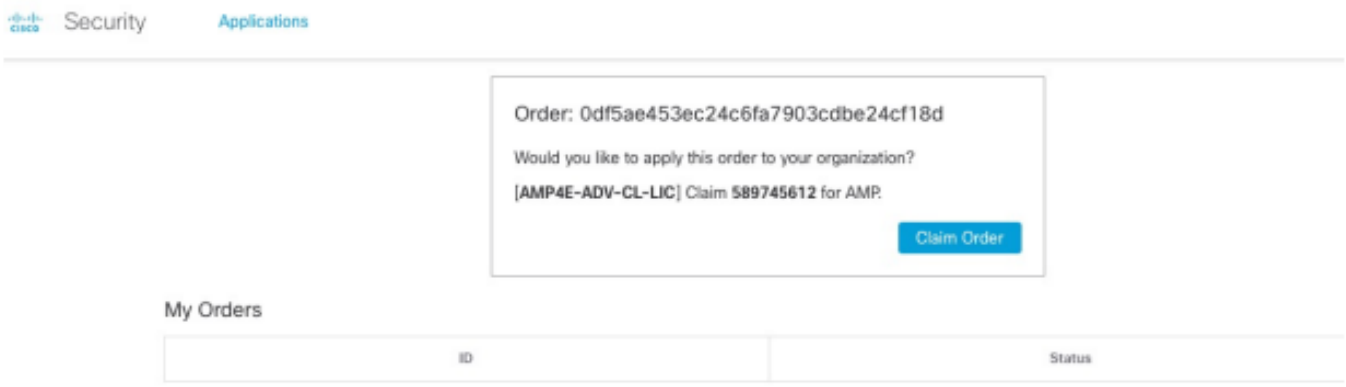
Stap 9. Pas uw licentie toe op stap 2.



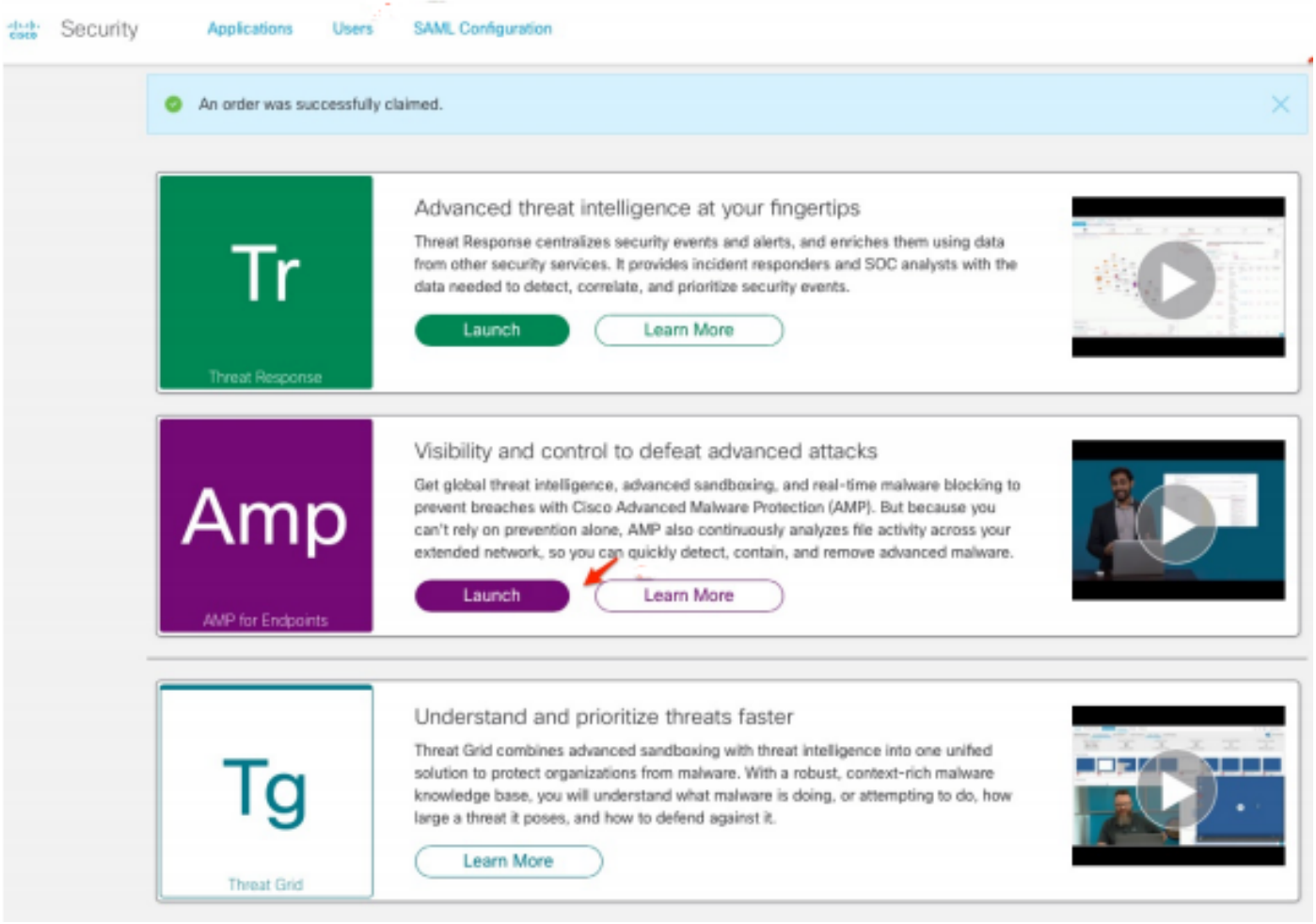
Stap 10. Meld u aan bij uw Cisco-beveiligingsaccount.



Stap 11. Klik op **Opdrachtvolgorde** zodra u binnenkomt.



Stap 12. Nu kan uw opdracht met succes worden uitgevoerd en kunt u de AMP4E-console starten.


Security
Applications
Users
SAML Configuration
An order was successfully claimed.
Tr
Threat Response
Advanced threat intelligence at your fingertips
Threat Response centralizes security events and alerts, and enriches them using data from other security services. It provides incident responders and SOC analysts with the data needed to detect, correlate, and prioritize security events.
Launch
Learn More
Amp
AMP for Endpoints
Visibility and control to defeat advanced attacks
Get global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches with Cisco Advanced Malware Protection (AMP). But because you can't rely on prevention alone, AMP also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.
Launch
Learn More
Tg
Threat Grid
Understand and prioritize threats faster
Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.
Learn More