Derecho a AMP para terminales

Contenido

Introducción

Este documento describe el proceso para obtener la licencia de protección frente a malware avanzado (AMP) autorizada y el acceso al panel.

Colaborado por Uriel Islas, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de:

- Licencia de AMP para terminales
- Cuenta de correo electrónico
- Ordenador

Componentes Utilizados

Este documento no se limita a una versión de software específica, sin embargo, este documento se basa en este software:

- Nube pública AMP
- Outlook

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier paso.

Configurar

Para dar derecho al producto AMP para terminales (AMP4E), puede consultar el correo electrónico de entrega electrónica o un correo electrónico de autorización.

> **Nota:** Si no tiene acceso al correo electrónico de entrega electrónica, puede ponerse en contacto con: licensing@cisco.com o visite el portal en línea en

http://cisco.com/tac/caseopen. Después de seleccionar la tecnología y subtecnología apropiadas, seleccione **Licencias** enumeradas en **Tipo de problema**.

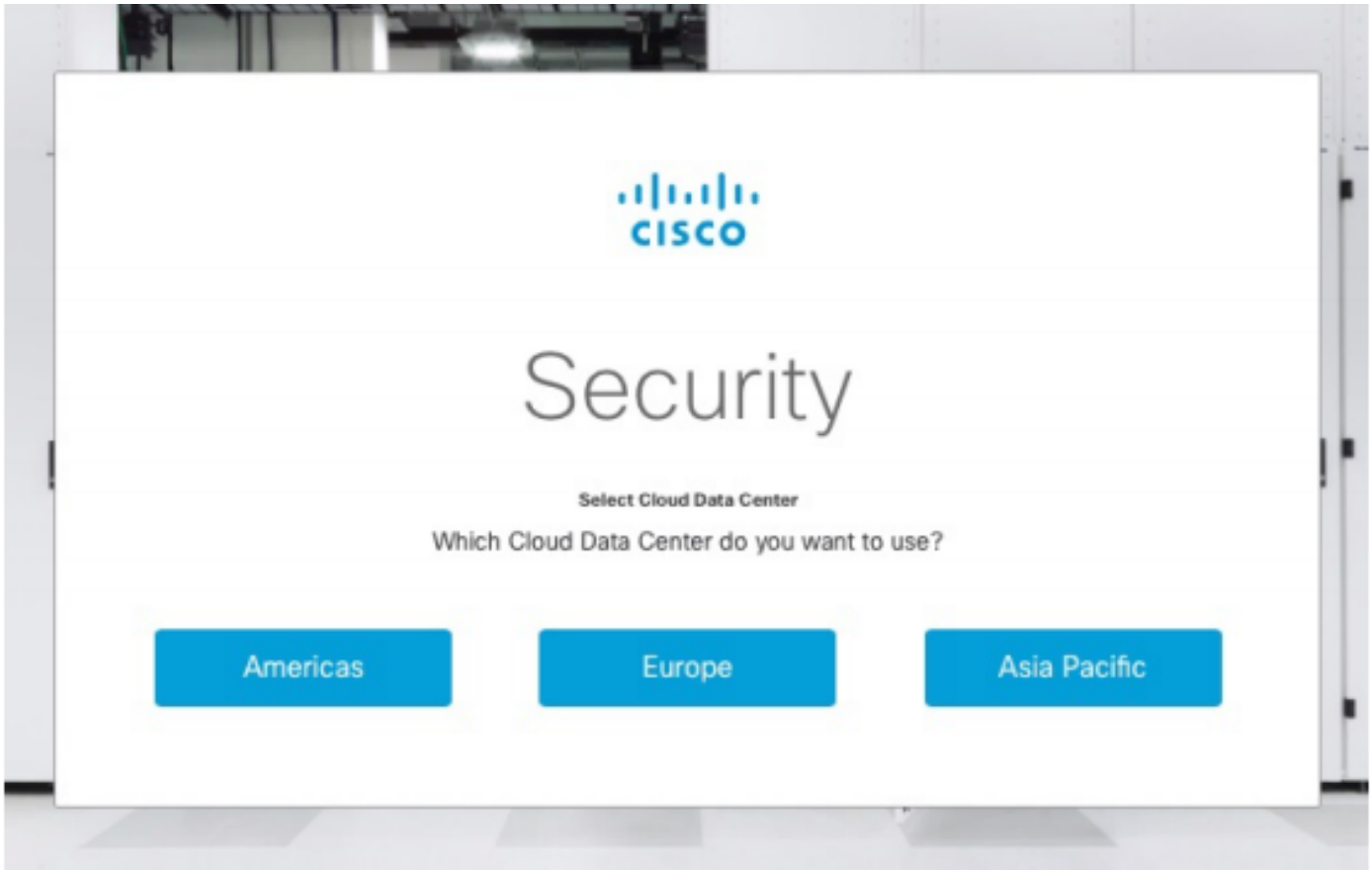
Credenciales de AMP para terminales

Las credenciales de AMP4E pertenecen al dominio Cisco Security Account (CSA). Tan pronto como se hayan configurado las primeras cuentas de seguridad de Cisco, podrá añadir más administradores de seguridad dentro de su organización. En el momento en que aplique su licencia para generar una nueva instancia de nube, cree una CSA o puede introducir la licencia mediante sus credenciales CSA existentes. Una vez hecho, una organización debe estar vinculada a su empresa.

Cómo configurar una nueva nube pública

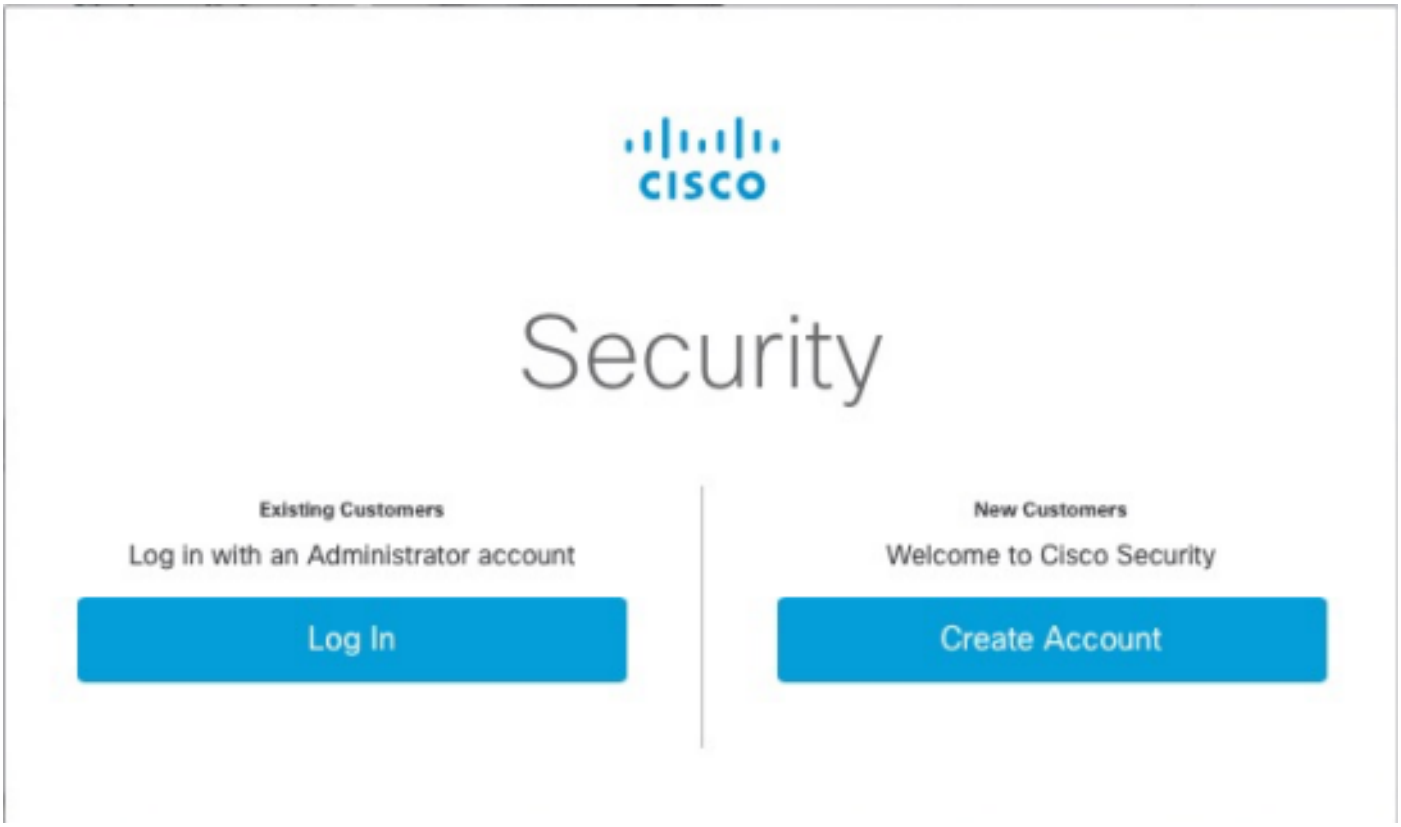
Paso 1. Desplácese bajo la URL proporcionada en el correo electrónico de entrega electrónica o el correo electrónico de derechos.

Paso 2. Seleccione el Data Center en la nube que prefiera.



Nota: La nube de América se puede utilizar en todos los países. No hay problemas relacionados con la latencia para los países que están lejos.

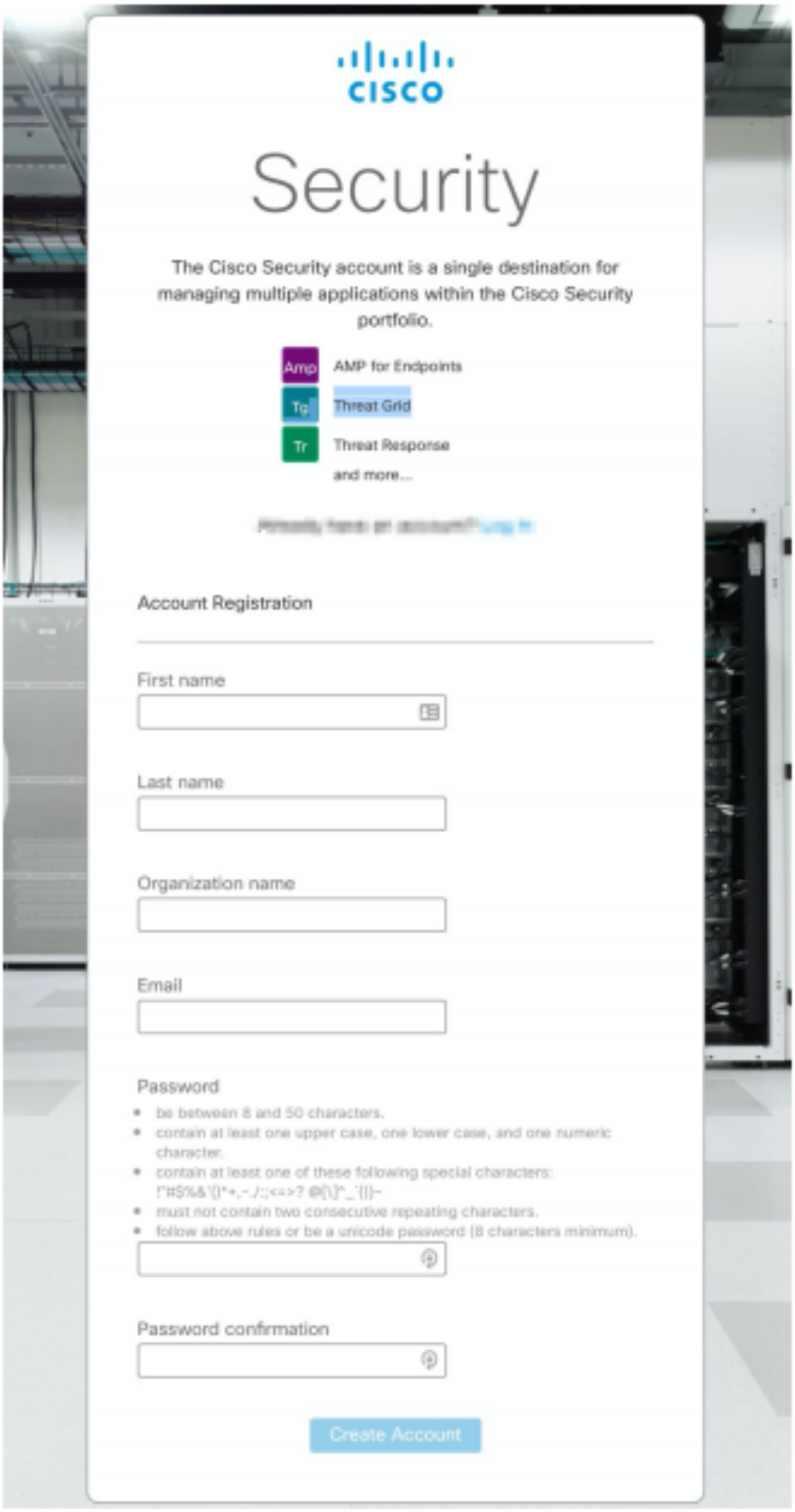
Paso 3. Conecte su cuenta de seguridad de Cisco a la nube de AMP.



a) Si ya tiene las credenciales para un CSA, pero no para AMP4E, haga clic en **Iniciar sesión**. Esta opción debe vincular su CSA a la nube de AMP.

b) si no tiene una nube de AMP o una organización de seguridad de Cisco configurada, haga clic en **Crear cuenta** para aplicar la licencia a su empresa.

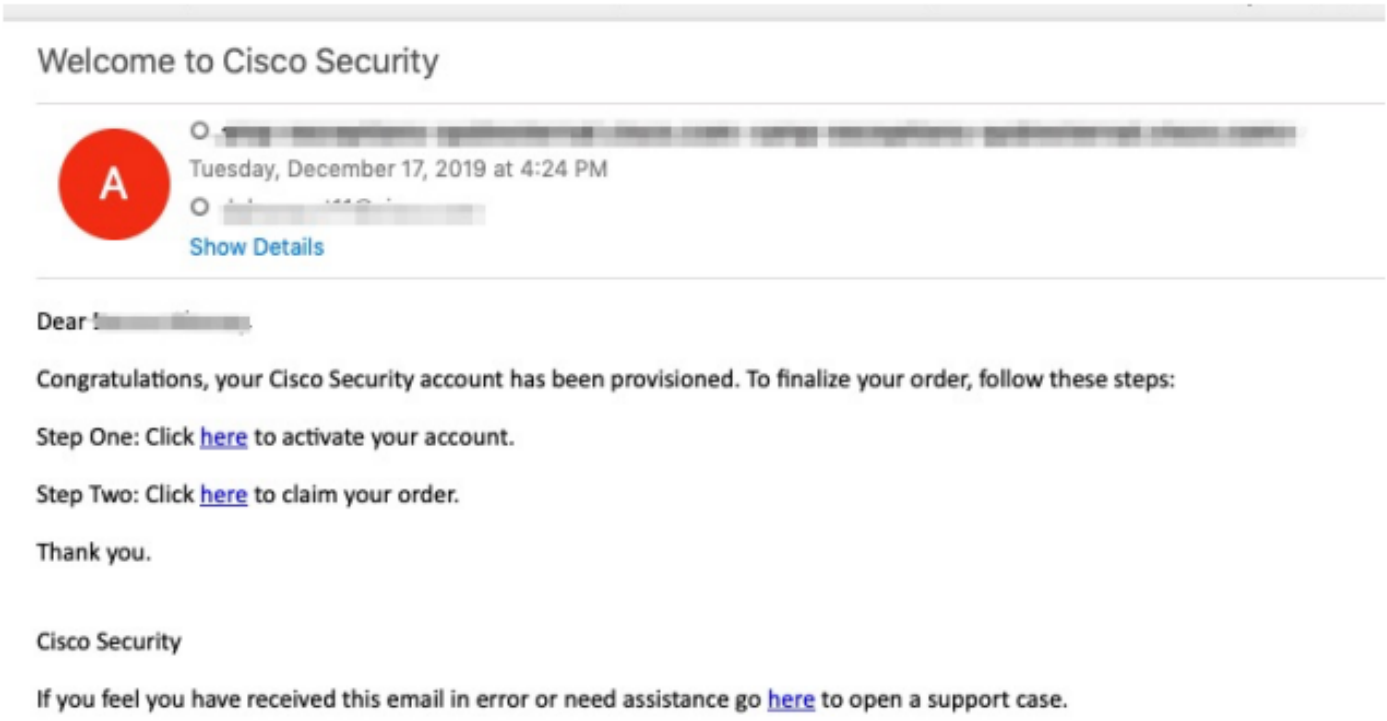
Paso 4. Si su empresa no dispone de una CSA, introduzca los valores de todos los campos según se le solicite.



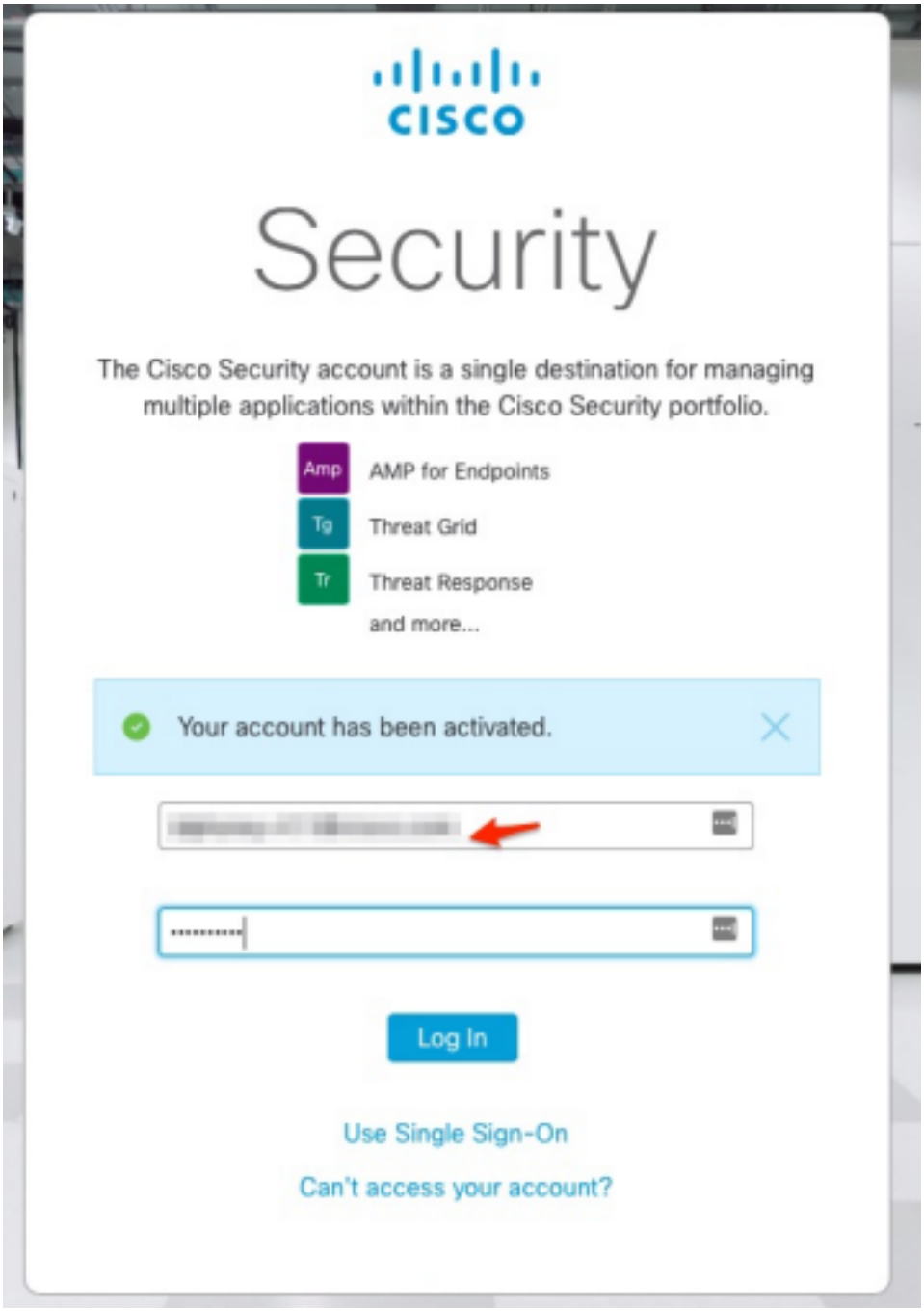
Nota: Si alguien ya tiene una CSA en su empresa, navegue por el sitio web del castillo para autenticar sus credenciales. Seleccione la URL basada en la nube que se configuró en el número 2. **Nube de América**: https://castle.amp.cisco.com **Europa Cloud**: https://castle.eu.amp.cisco.com **Nube Asia-Pacífico**: https://castle.apjc.amp.cisco.com.

Paso 5. Una vez creado el CSA, muestra una página Account Registration Complete (Registro de cuenta finalizado).

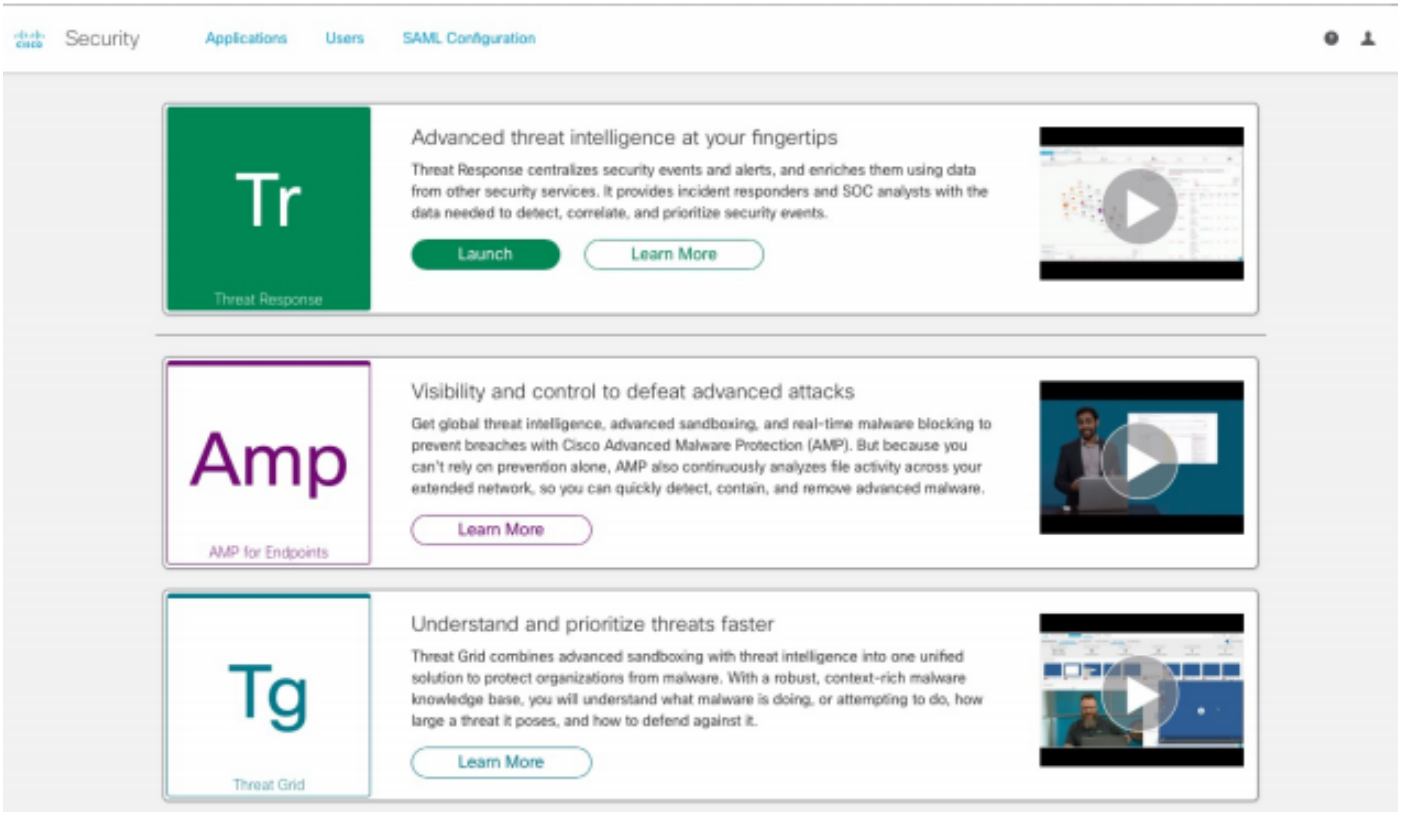
Paso 6. Verifique un nuevo mensaje de correo electrónico de bienvenida a Cisco Security desde no-reply@amp.cisco.com.



Paso 7. Active su cuenta desde el correo electrónico de bienvenida en el paso 1



Paso 8. La autenticación en el sitio web del castillo depende de la nube anterior configurada en su empresa.

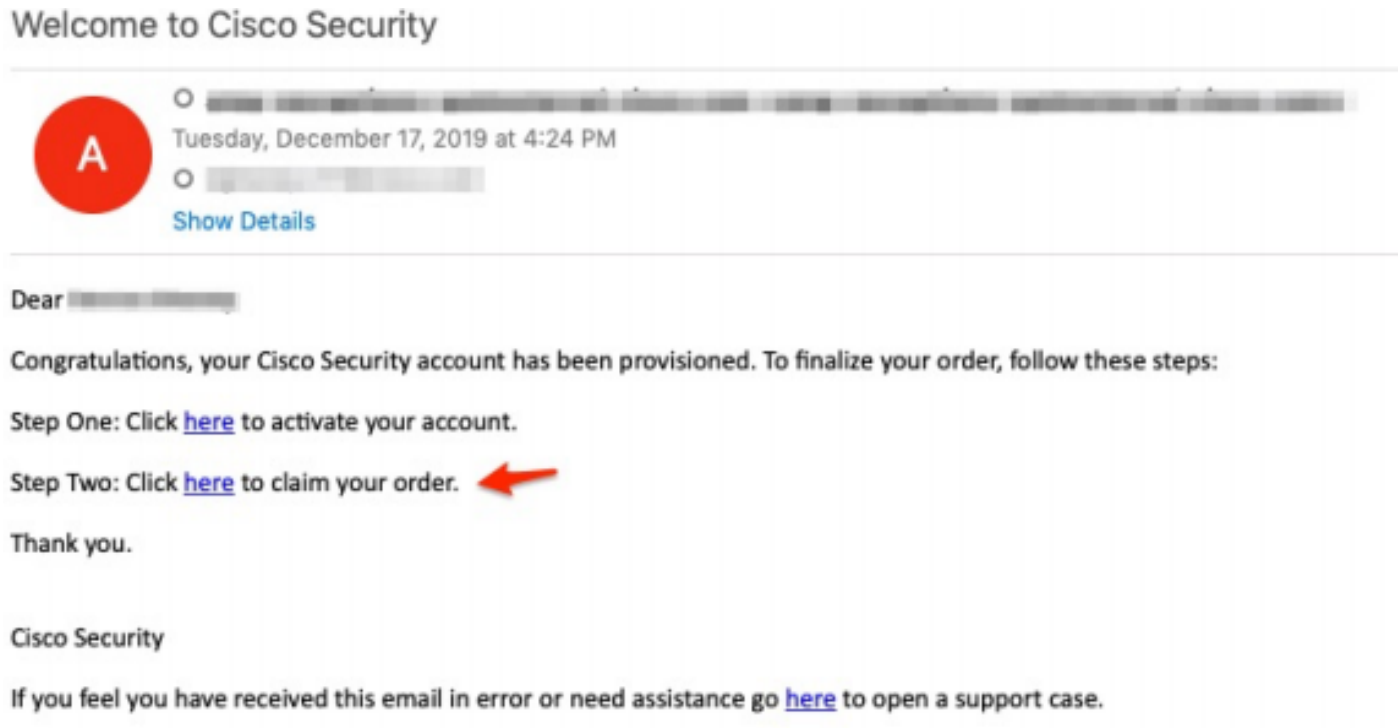


Nube de América - https://castle.amp.cisco.com

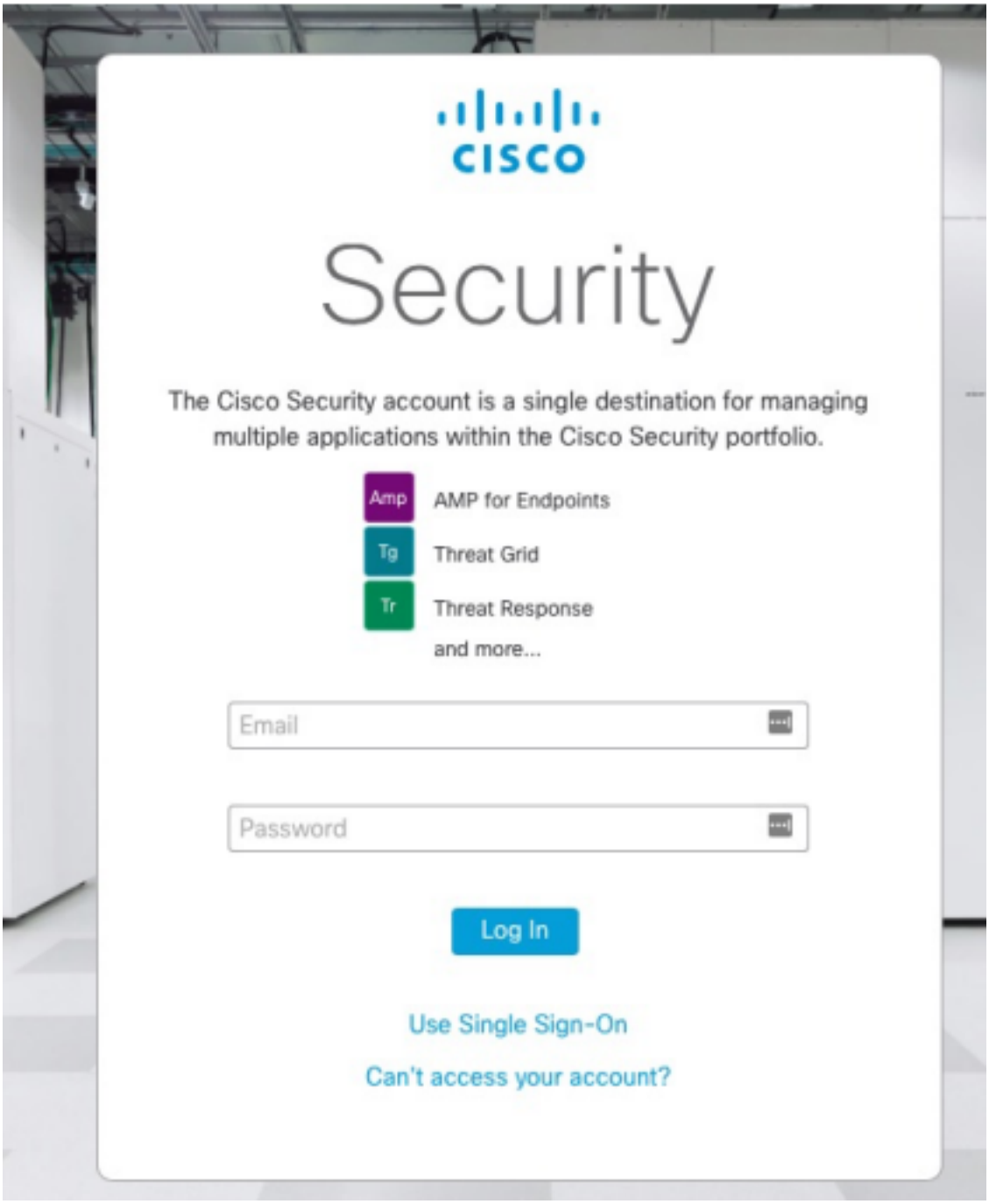
Nube europea - https://castle.eu.amp.cisco.com

Nube Asia-Pacífico - https://castle.apjc.amp.cisco.com

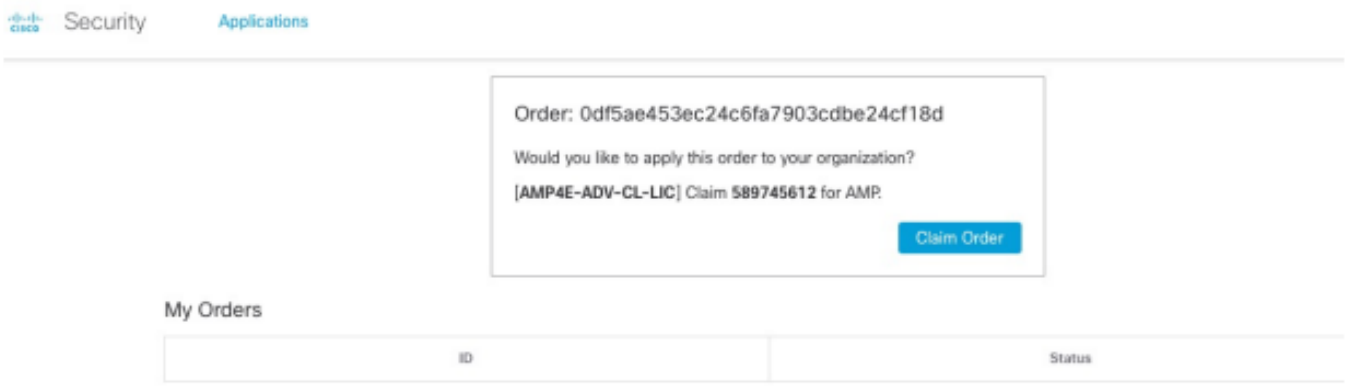
Paso 9. Aplique su licencia en el paso 2.



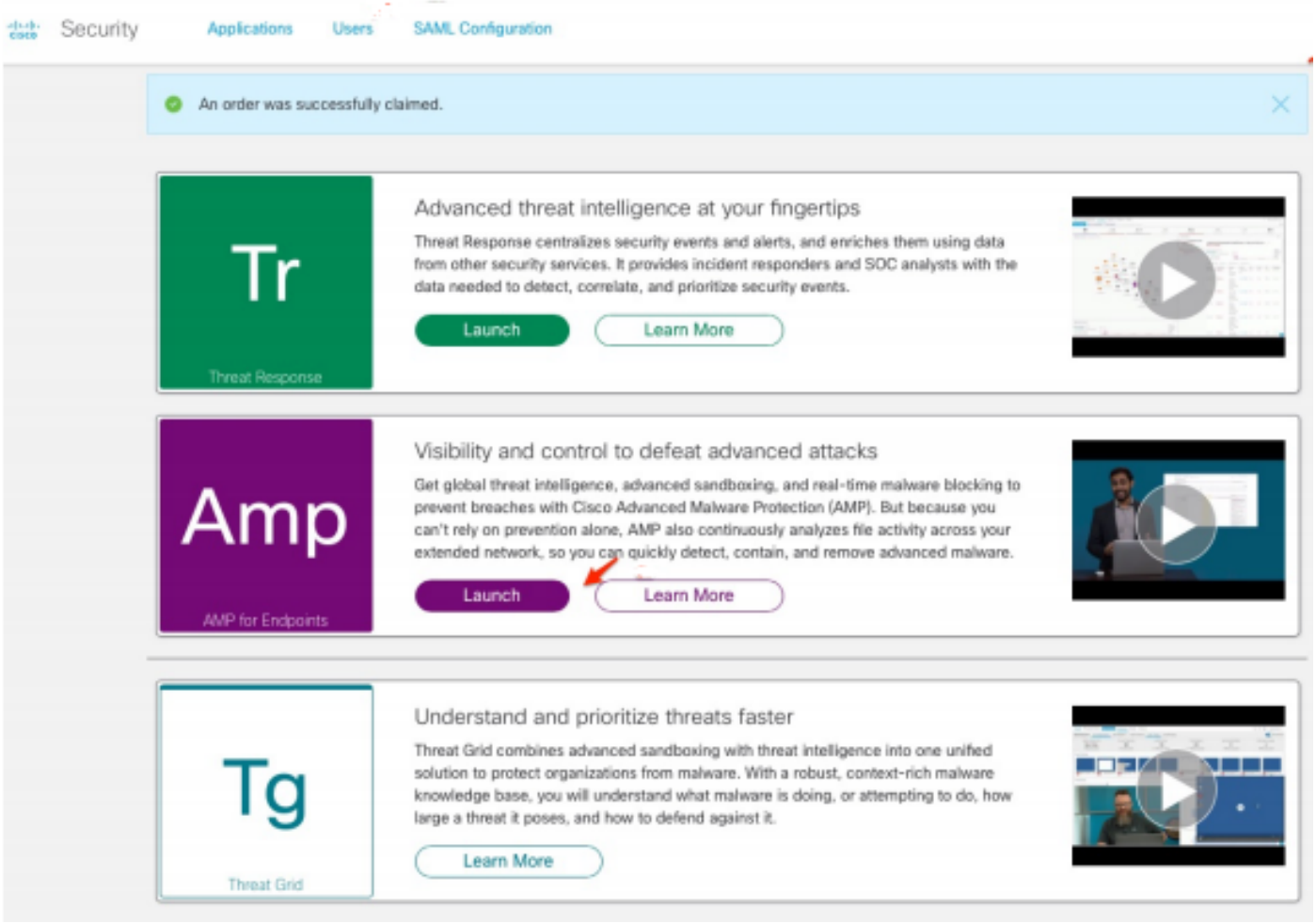
Paso 10. Inicie sesión con su cuenta de seguridad de Cisco.



Paso 11. Una vez que entre, haga clic en **Reclamar pedido.**



Paso 12. Ahora su pedido se ha realizado correctamente y podría iniciar la consola de AMP4E.


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