Direito à AMP para endpoints

Contents

Introduction

Este documento descreve o processo para obter a licença de proteção avançada contra malware (AMP) e o acesso ao painel.

Contribuído por Uriel Islas, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento de:

- Licença da AMP para endpoints
- Conta de e-mail
- Computador

Componentes Utilizados

Este documento não está restrito a uma versão de software específica, no entanto, este documento com base neste software:

- Nuvem pública da 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. Se a sua rede estiver ativa, certifique-se de que você entende o impacto potencial de qualquer etapa.

Configurar

Para habilitar seu produto AMP para endpoints (AMP4E), consulte o eDelivery e-mail ou um e-mail de qualificação.

> **Note**: Se você não tiver acesso ao e-mail de eDelivery, poderá entrar em contato com: licensing@cisco.com ou visite o portal online em http://cisco.com/tac/caseopen. Depois de

selecionar a tecnologia e subtecnologia apropriadas, selecione **Licenciamento** listado em **Tipo de problema**.

Credenciais do AMP para endpoints

As credenciais do AMP4E pertencem ao domínio Cisco Security Account (CSA). Assim que as primeiras contas do Cisco Security forem configuradas, você poderá adicionar outros administradores de segurança na sua empresa. No momento em que você aplica sua licença para criar uma nova instância de nuvem, você cria um CSA ou pode inserir a licença usando suas credenciais CSA existentes. Depois de concluída, uma empresa deve estar vinculada à sua empresa.

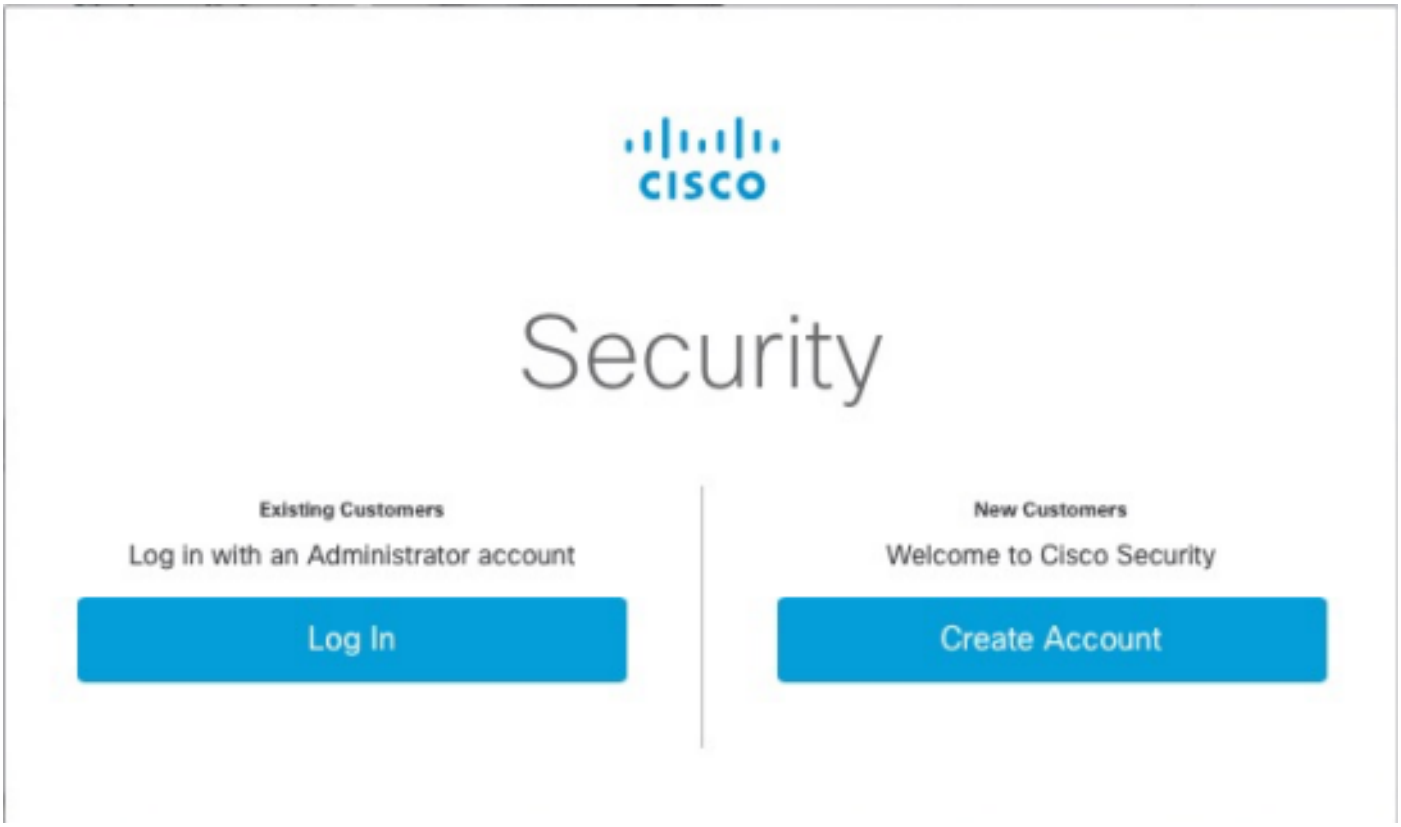
Como configurar uma nova nuvem pública

Etapa 1. Navegue pelo URL fornecido no e-mail de eDelivery ou e-mail de qualificação.

Etapa 2. Selecione seu data center de nuvem preferido.

Note: A nuvem das Américas pode ser usada para todos os países. Não há problemas relacionados à latência para países distantes.

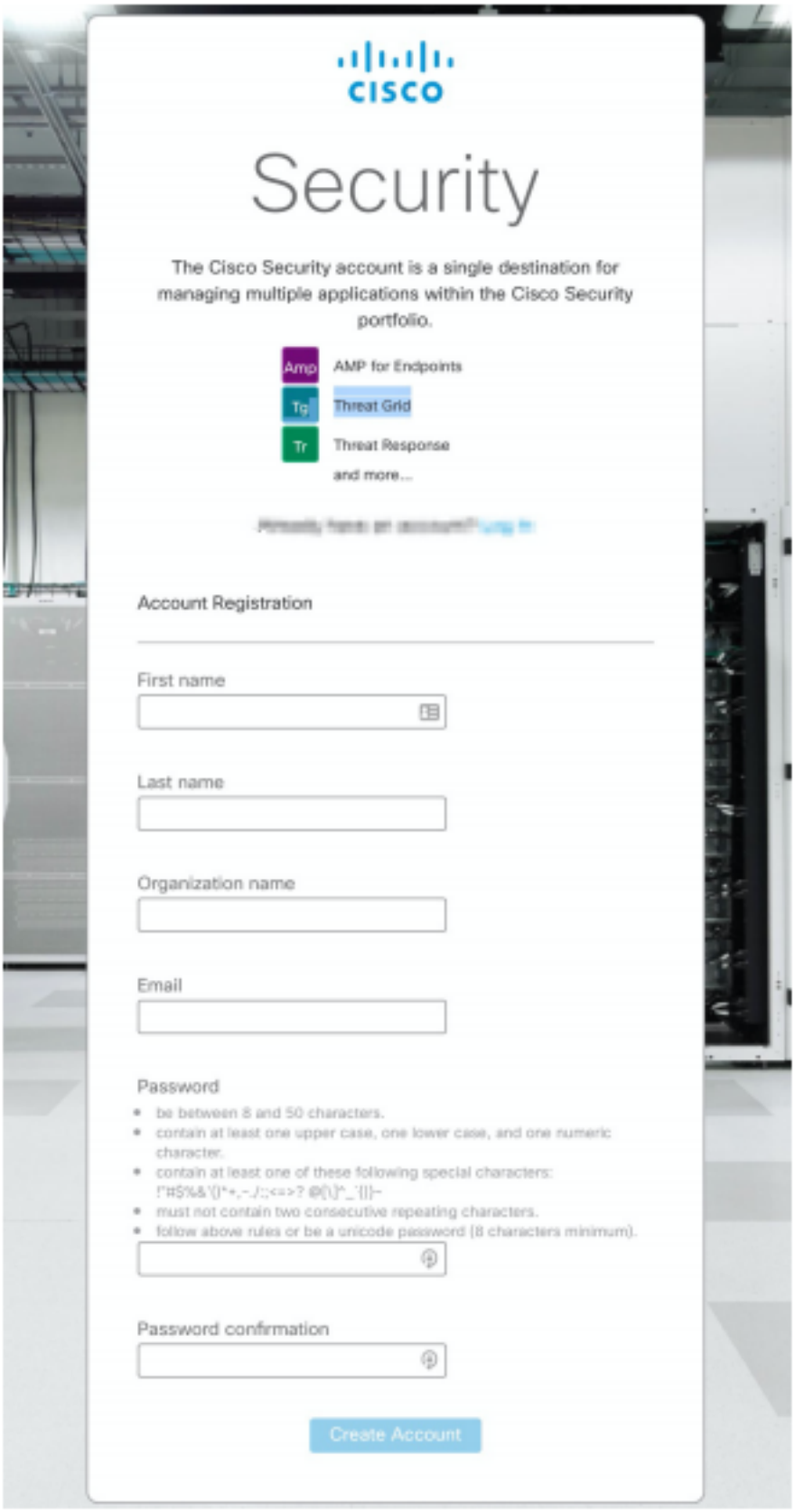
Etapa 3. Vincule sua conta de segurança da Cisco à nuvem da AMP.



a) Se você já tiver as credenciais para um CSA, mas não para o AMP4E, clique em **Fazer login**. Essa opção deve vincular seu CSA à nuvem da AMP.

b) Se você não tiver uma nuvem AMP ou uma Cisco Security Org configurada, clique em **Create Account (Criar conta)** para aplicar a licença para sua empresa.

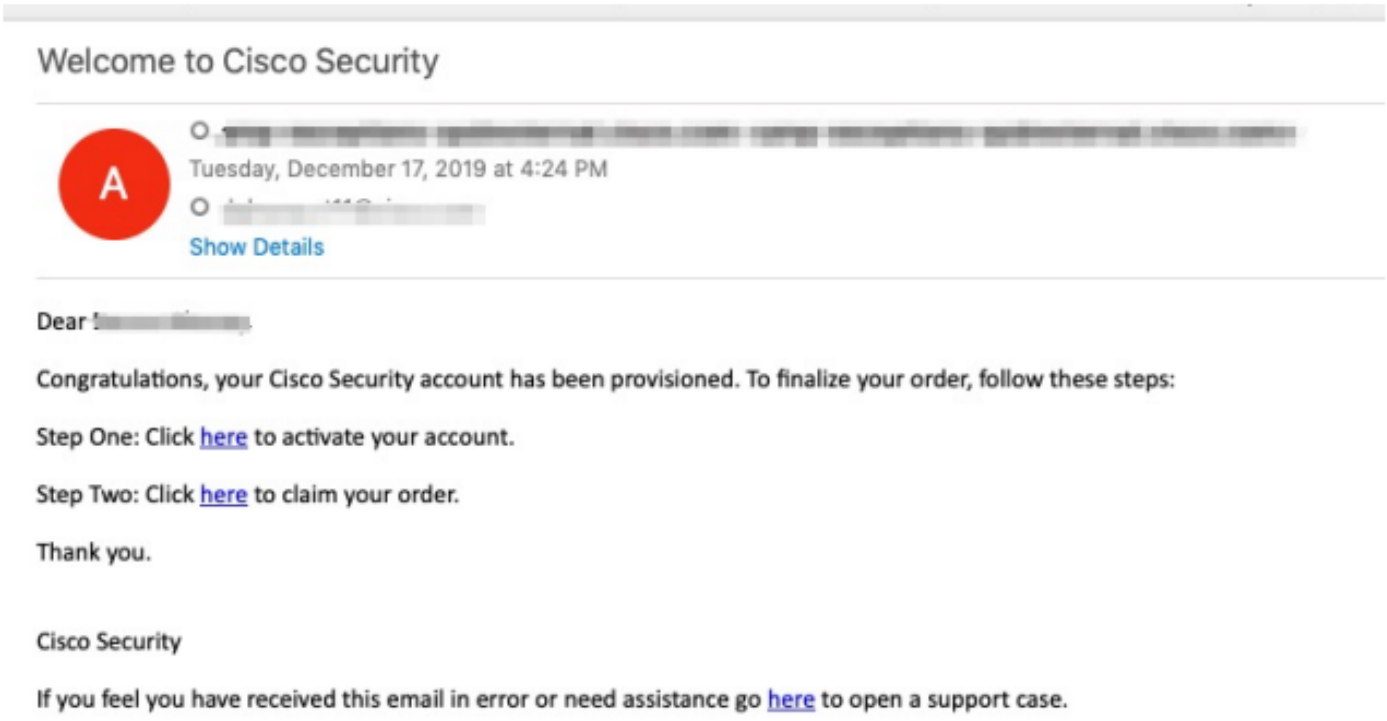
Etapa 4. Se sua empresa não tiver um CSA, insira os valores de todos os campos conforme solicitado para configuração.



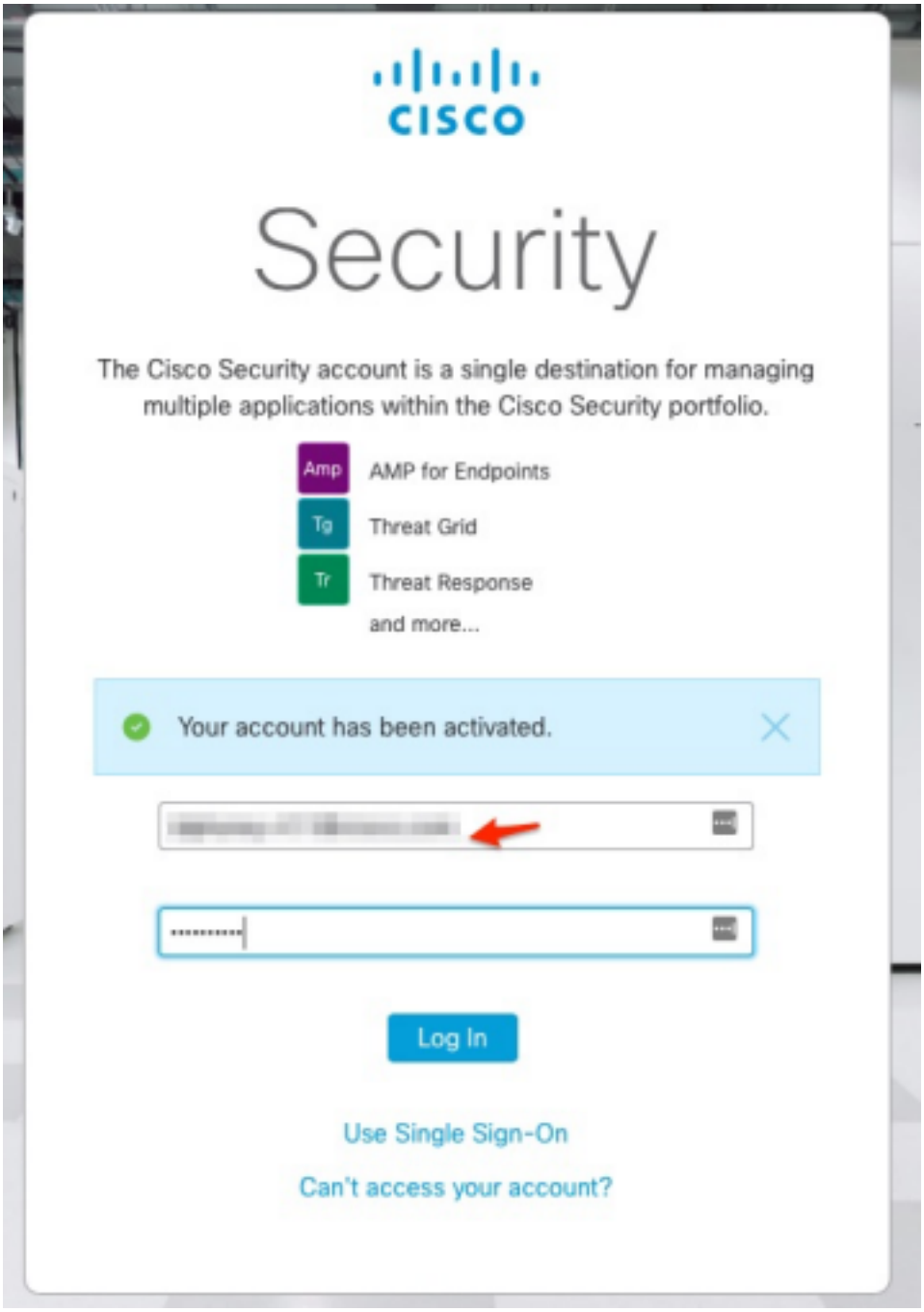
Note: Se alguém já tiver um CSA em sua empresa, navegue pelo site do Castle para autenticar suas credenciais. Selecione o URL com base na nuvem configurada no número 2. **Nuvem nas Américas**: https://castle.amp.cisco.com **Europe Cloud**: https://castle.eu.amp.cisco.com **Nuvem do Pacífico Asiático**: https://castle.apjc.amp.cisco.com.

Etapa 5. Quando o CSA é criado, ele exibe uma página Registro de conta concluído.

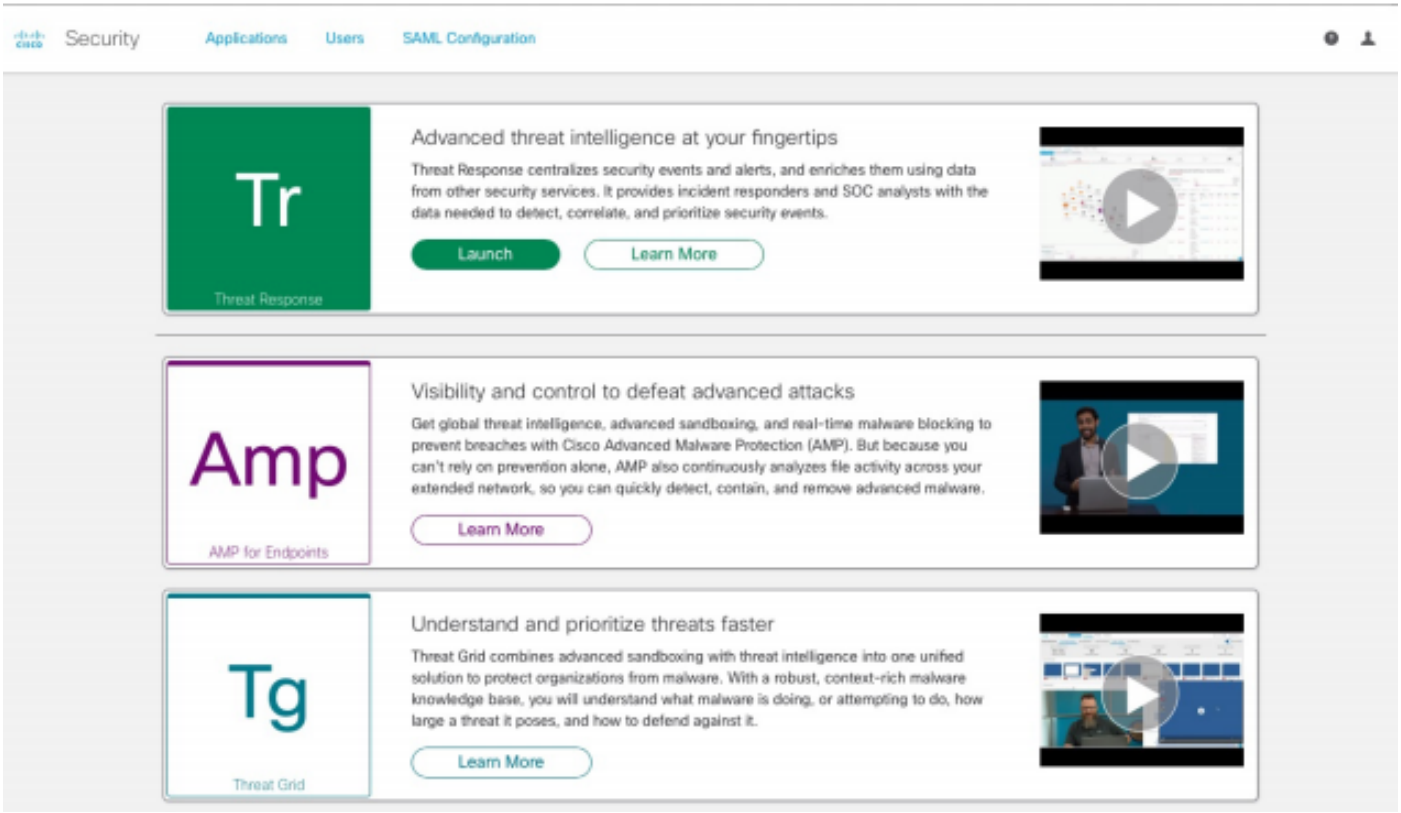
Etapa 6. Verifique um novo e-mail de boas-vindas ao Cisco Security em no-reply@amp.cisco.com.



Passo 7. Ative sua conta do e-mail de boas-vindas na etapa 1



Etapa 8. A autenticação no site do castelo depende da nuvem anterior configurada na sua empresa.

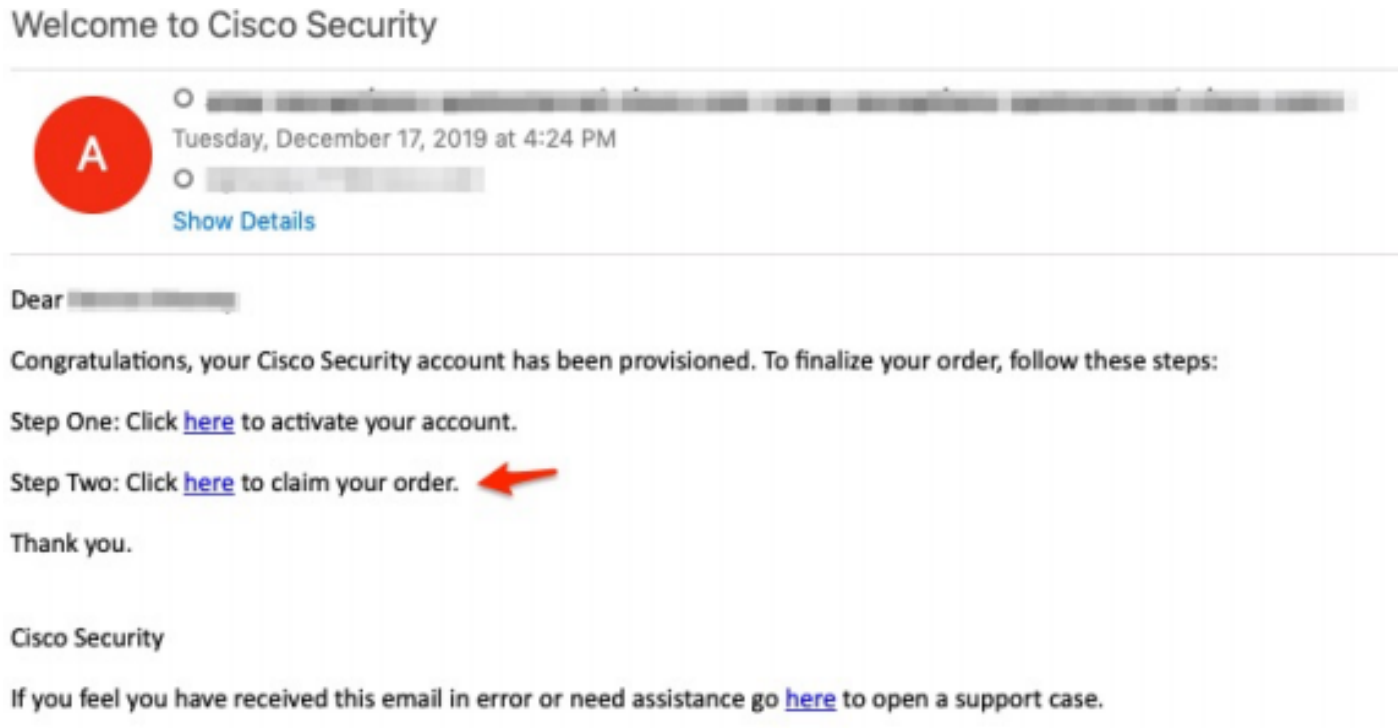


Nuvem das Américas - https://castle.amp.cisco.com

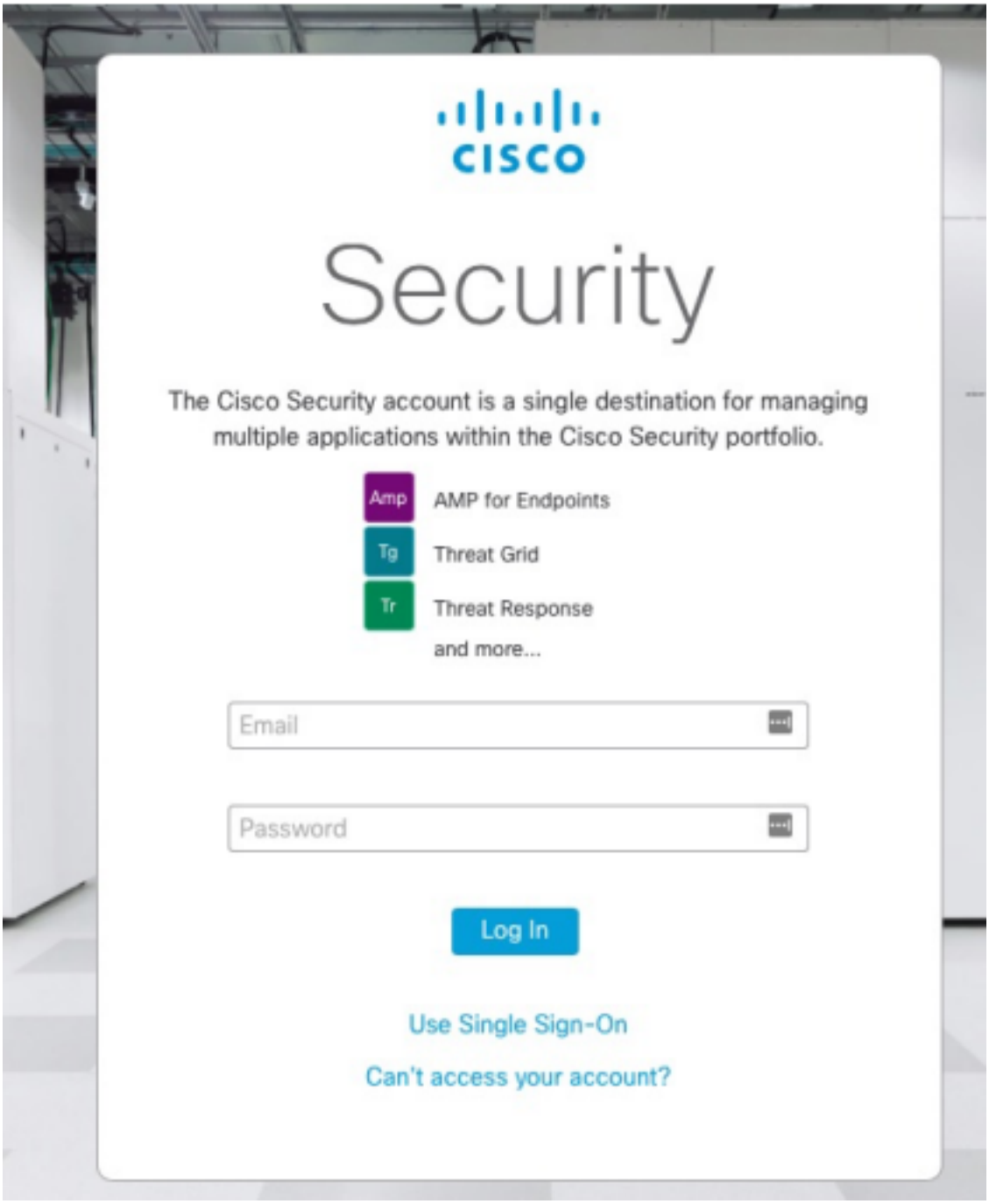
Europa em nuvem - https://castle.eu.amp.cisco.com

Nuvem do Pacífico Asiático - https://castle.apjc.amp.cisco.com

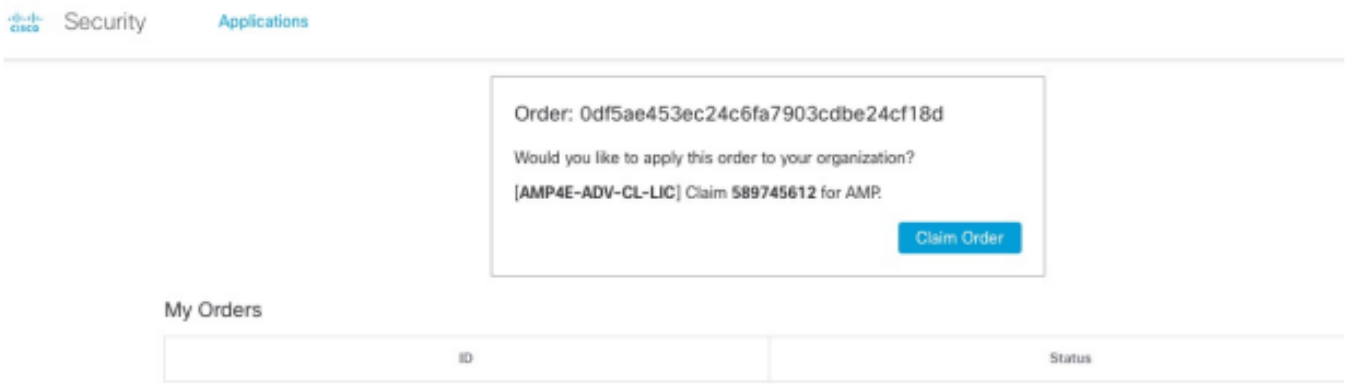
Etapa 9. Aplique sua licença na etapa 2.



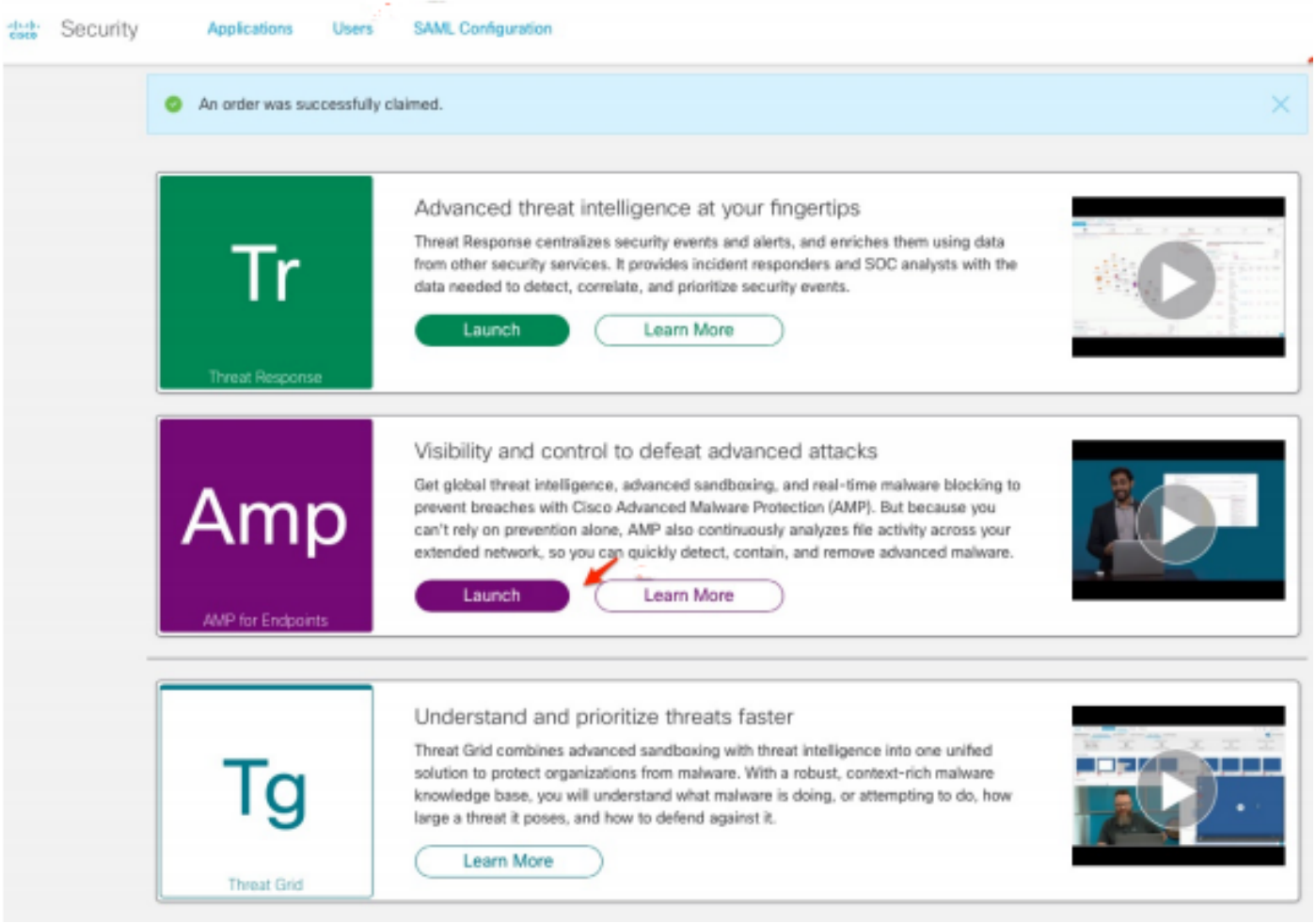
Etapa 10. Faça login com sua conta de segurança da Cisco.



Etapa 11. Depois de entrar, clique em **Pedido de Reivindicação.**



Etapa 12. Agora seu pedido foi reivindicado com êxito e você poderá iniciar o console do 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