適用於終端的AMP的權利

目錄

簡介

本文檔介紹獲取高級惡意軟體防護(AMP)許可證並訪問控制面板的流程。

作者：Uriel Islas，思科TAC工程師。

必要條件

需求

思科建議您瞭解：

- AMP端點許可證
- 電子郵件帳戶
- 電腦

採用元件

- AMP公共雲
- Outlook

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何步驟可能造成的影響。

設定

若要授予您的終端進階惡意軟體防護(AMP4E)產品，您可以參閱eDelivery電子郵件或權利電子郵件。

> **附註**：如果您無權訪問eDelivery電子郵件，您可以聯絡：licensing@cisco.com或訪問線上門戶http://cisco.com/tac/caseopen。選擇適當的技術和子技術後，選擇**問題型別**下面列出的**許可**。

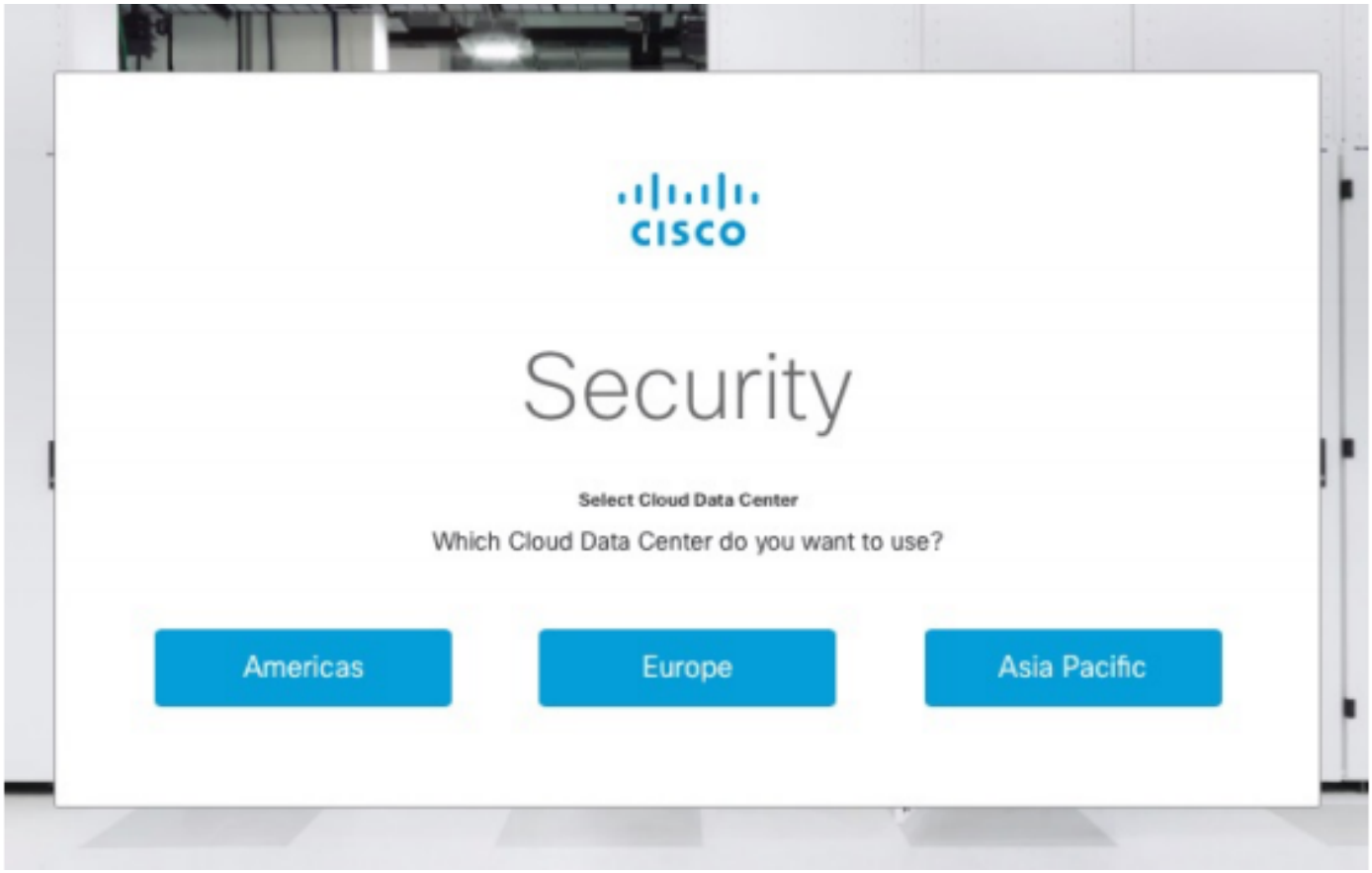
面向終端的AMP憑據

AMP4E憑證屬於思科安全帳戶(CSA)域。設定第一個思科安全帳戶後，您便可以在組織內新增更多安全管理員。在您申請許可證以生成新的雲例項時，您可以建立CSA，也可以使用現有CSA憑證輸入許可證。完成之後，您的企業就必須與組織保持聯絡。

如何設定新的公共雲

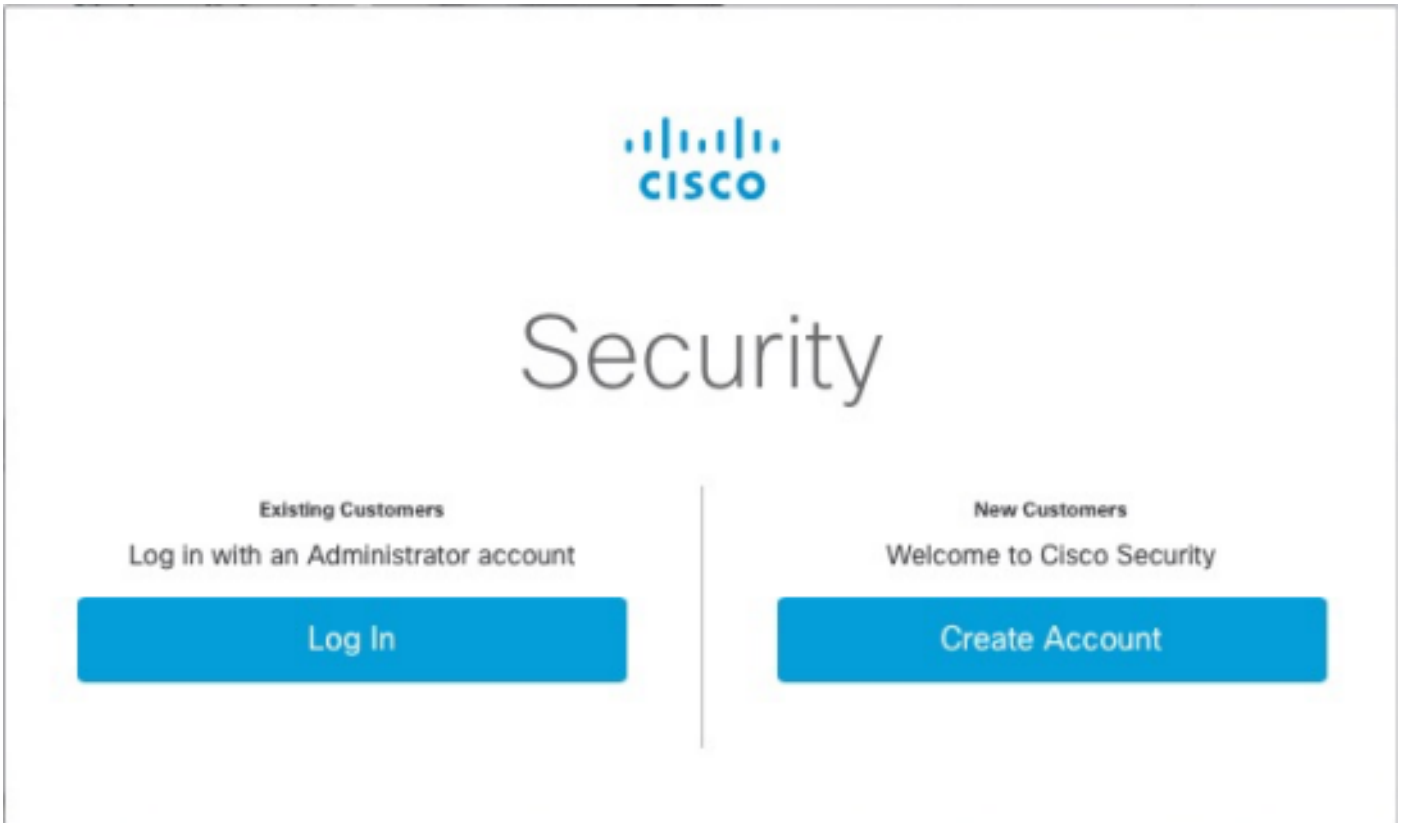
步驟1.在eDelivery電子郵件或權利電子郵件中提供的URL下導航。

步驟2.選擇您喜歡的雲資料中心。



附註：美洲雲可用於所有國家/地區。不存在與遙遠國家延遲相關的問題。

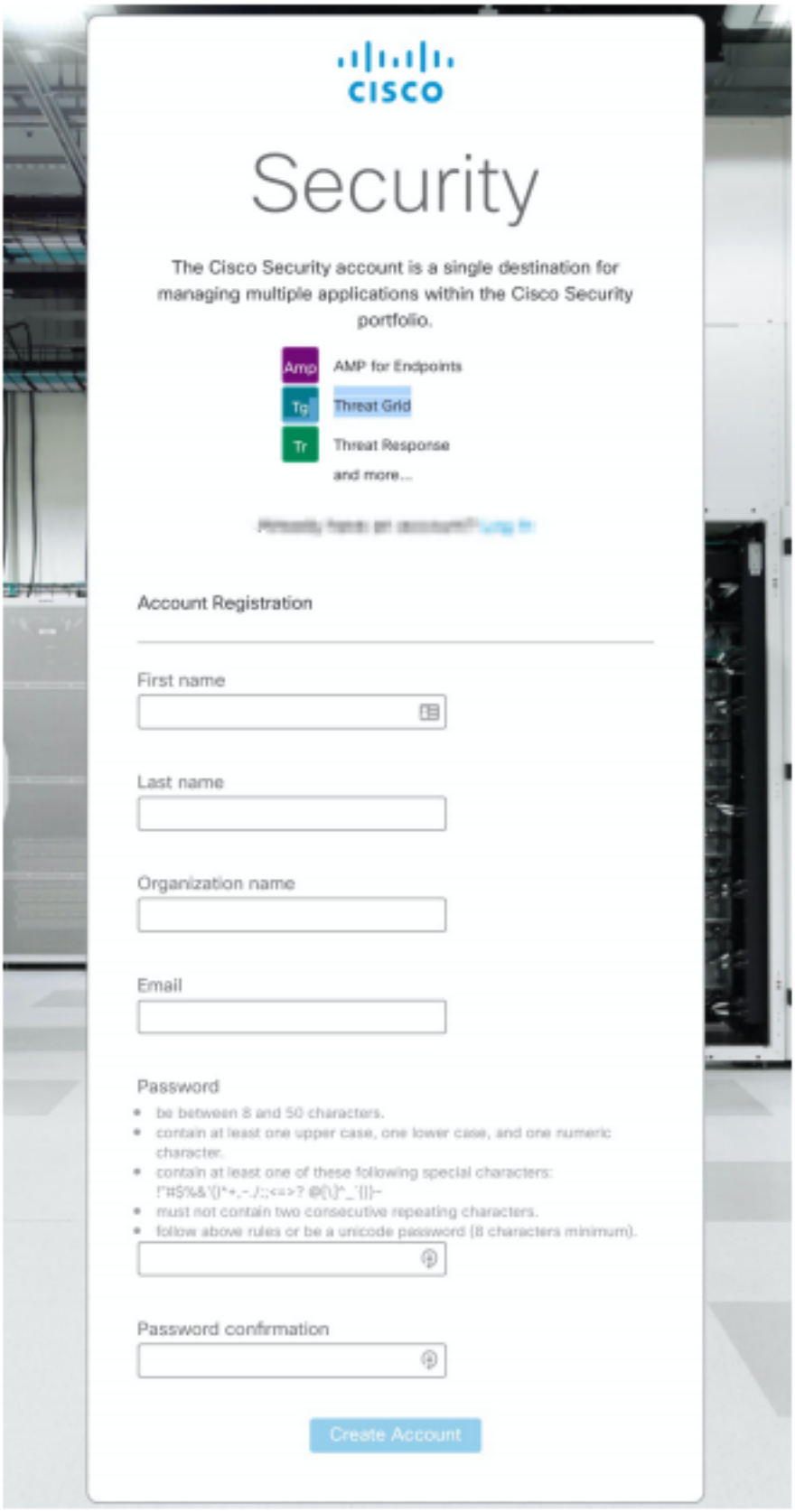
步驟3.將您的思科安全帳戶連結到AMP雲。



a)如果您已經擁有CSA的憑證，但沒有AMP4E，請按一下**Log in**。此選項必須將您的CSA連結到AMP雲。

b)如果您未設定AMP雲或思科安全組織，請點選**建立帳戶**為您的公司應用許可證。

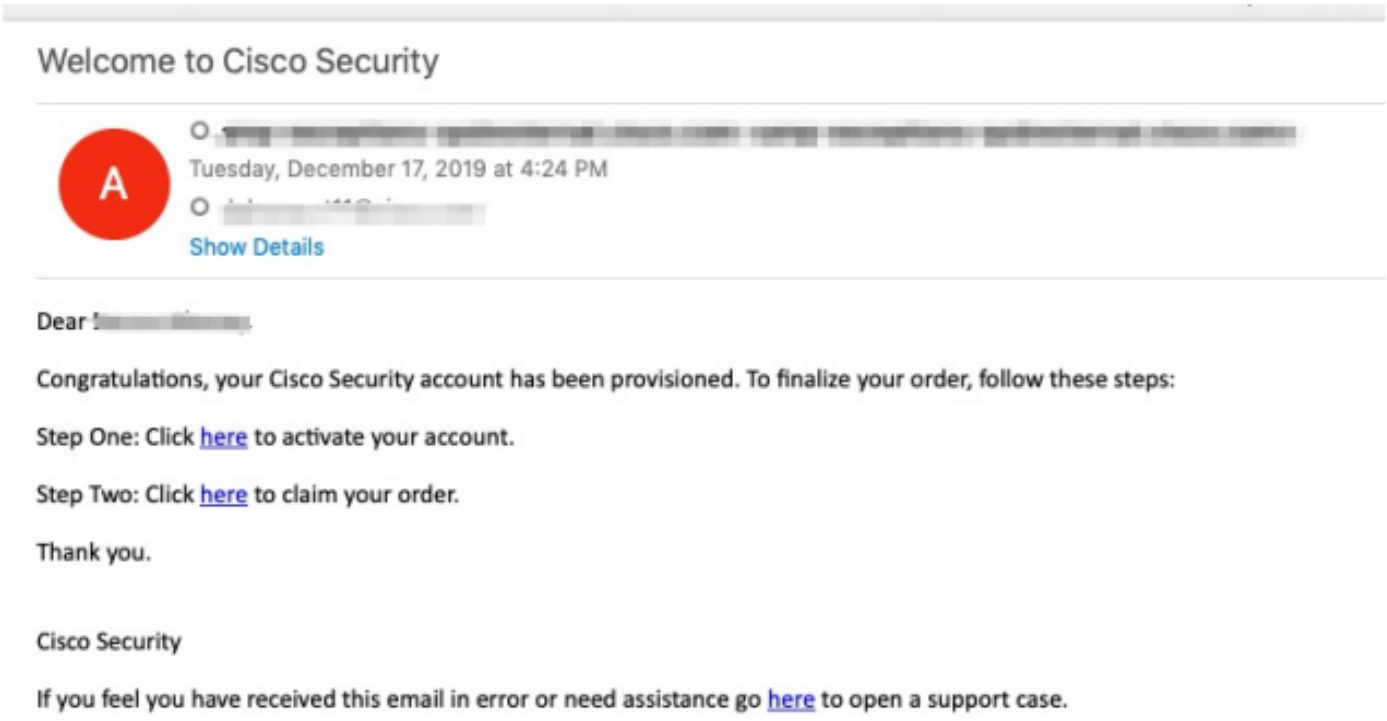
步驟4. 如果您的公司沒有CSA，則根據要求輸入所有欄位的值。



附註：如果某人在貴公司擁有CSA，則在castle網站下導航以驗證您的憑證。根據在2號上配置的雲選擇URL。 **美洲雲**:https://castle.amp.cisco.com **Europe Cloud**:https://castle.eu.amp.cisco.com **Asia Pacific Cloud**:https://castle.apjc.amp.cisco.com。

步驟5.建立CSA後，將顯示「帳戶註冊完成」頁。

步驟6.驗證來自no-reply@amp.cisco.com的新思科安全歡迎郵件。


Welcome to Cisco Security

A

Tuesday, December 17, 2019 at 4:24 PM

Show Details

Dear

Congratulations, your Cisco Security account has been provisioned. To finalize your order, follow these steps:

Step One: Click here to activate your account.

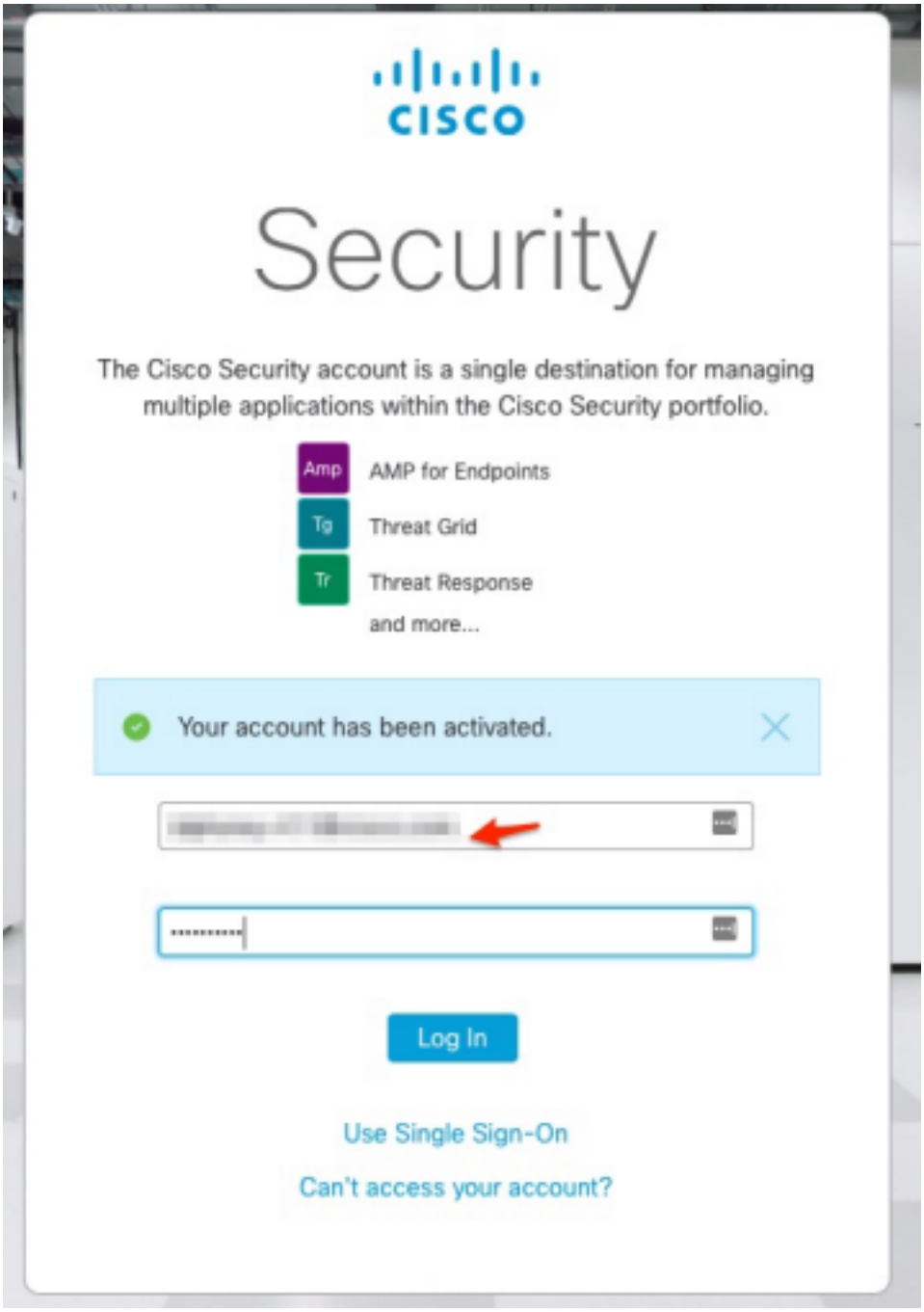
Step Two: Click here to claim your order.

Thank you.

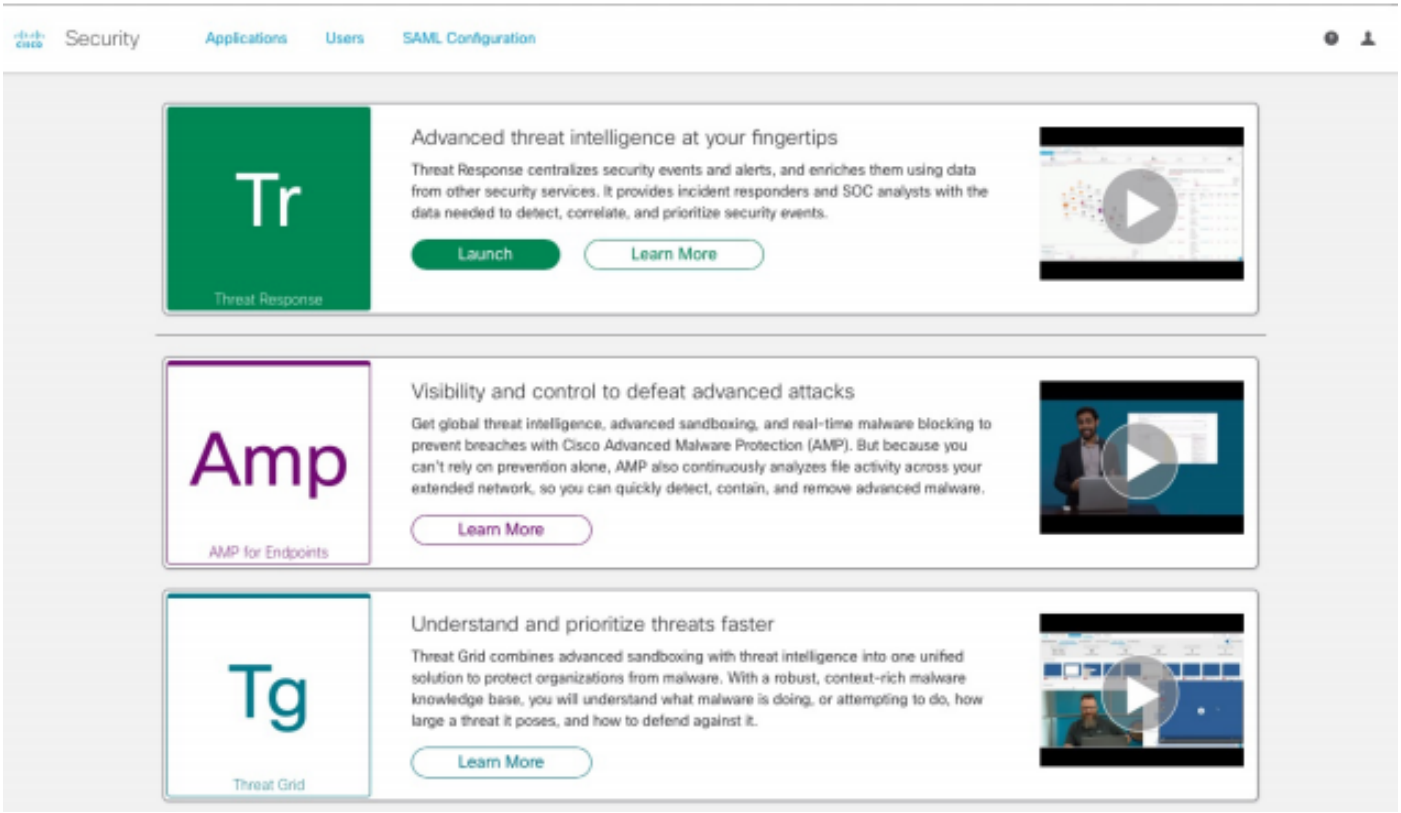
Cisco Security

If you feel you have received this email in error or need assistance go here to open a support case.

步驟7.在第1步從歡迎電子郵件啟用您的帳戶



步驟8.通過身份驗證進入Castle網站，具體取決於您的企業上配置的上一個雲。

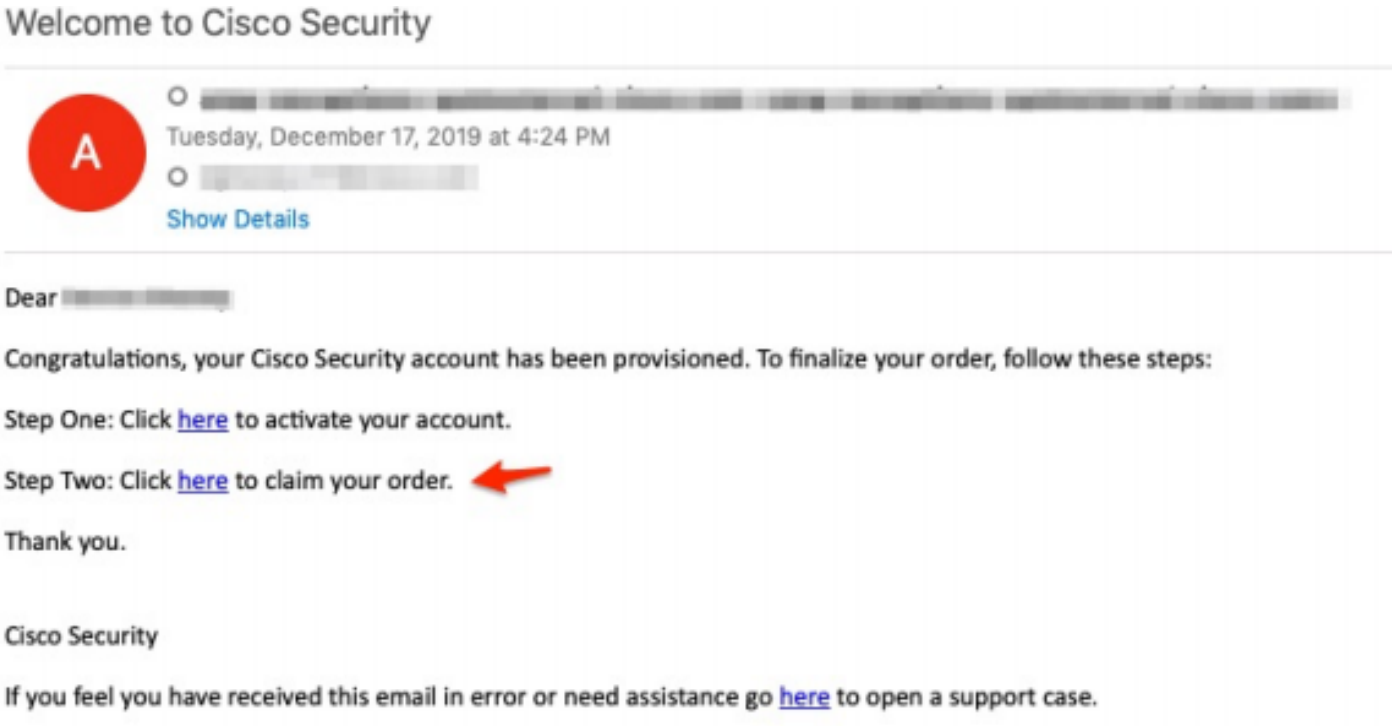


美洲雲 — https://castle.amp.cisco.com

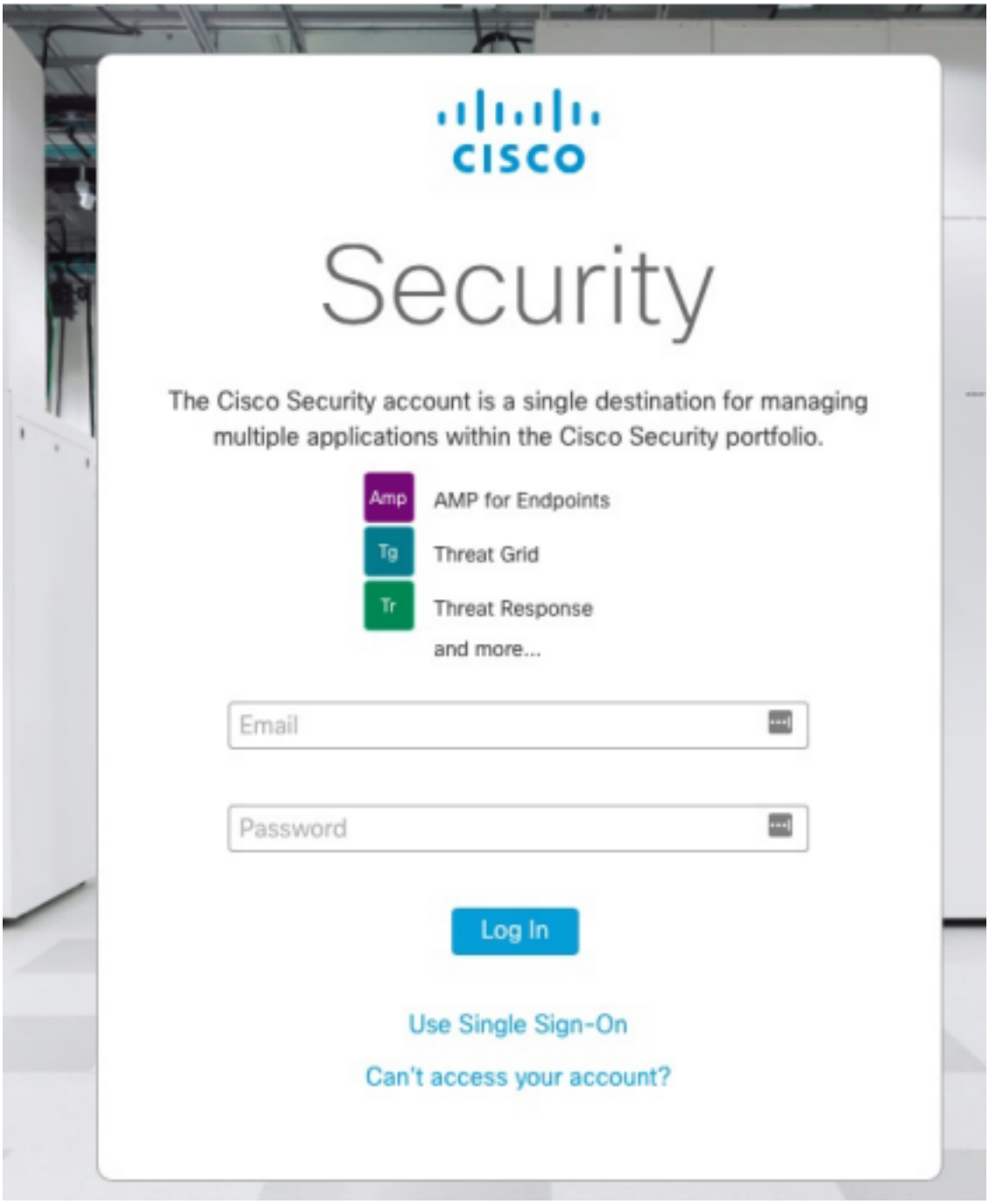
歐洲雲 — https://castle.eu.amp.cisco.com

亞太地區雲 — https://castle.apjc.amp.cisco.com

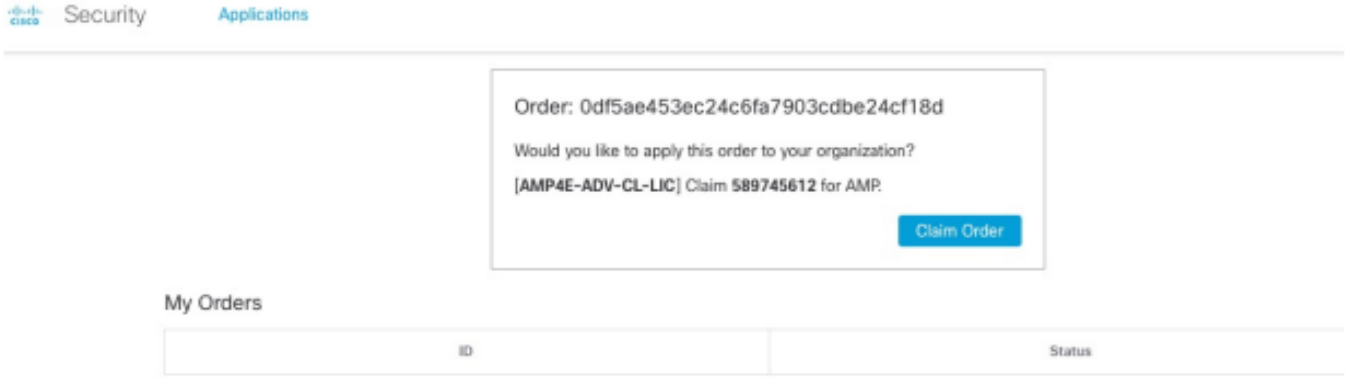
步驟9. 在第2步應用許可證。



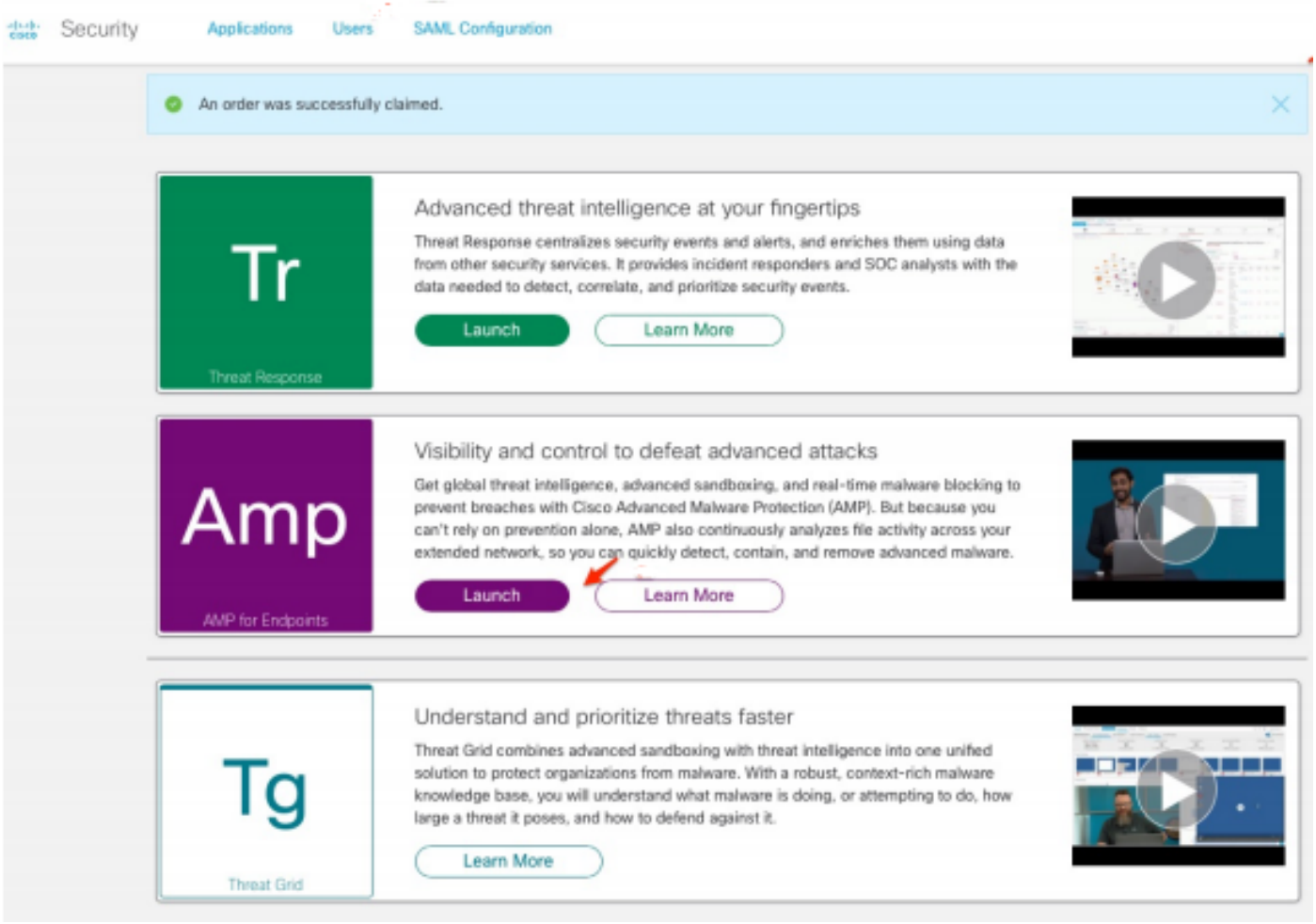
步驟10.使用您的思科安全帳戶登入。



步驟11。進入後，點選**申領訂單。**



步驟12。現在，您的訂單已成功申請，您可以啟動AMP4E控制檯。


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