通過Umbrella API整合安全性和自動化工作流程

目錄

簡介

本文檔介紹Umbrella API平台的功能、配置選項和可用資源。

Umbrella API概述

Umbrella API平台為構建、擴展和與Umbrella整合提供了一個安全的環境。使用API建立跨平台工作流，將威脅情報與其他安全解決方案聚合在一起，以擴展實施、提高可視性並自動執行事件響應。

API終端和管理

- 所有Umbrella API終端均託管在api.umbrella.com。
- 端點按用例進行分組，每個使用特定路徑。
- 在Umbrella控制面板中的Admin > API keys下管理API金鑰，或使用KeyAdmin API以程式設計方式管理API金鑰。

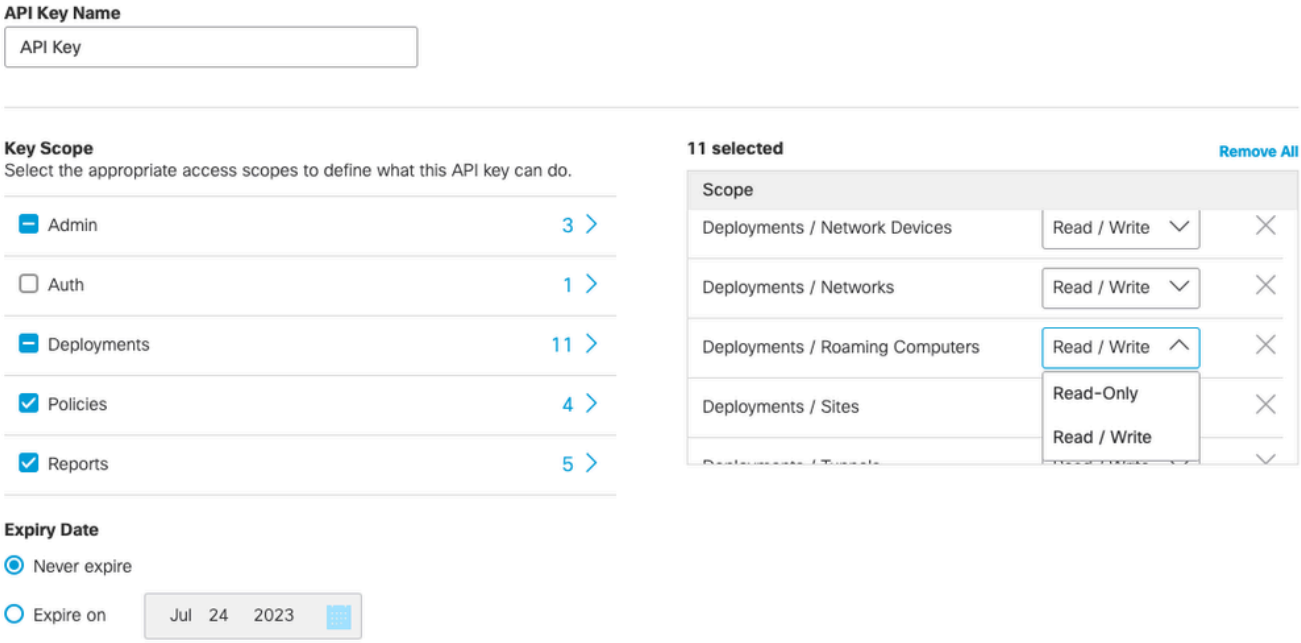
API使用案例和終端組

使用在以下主要使用案例下分組的粒度範圍配置每個API金鑰：

- 管理API終端:提供和管理API金鑰和使用者、檢視角色以及管理提供商和託管提供商的客戶。
- 驗證API端點:授權Umbrella和其他服務之間的整合。
- 部署API終端:調配、監控和管理網路和實體，通過在現有Umbrella策略中配置網路和實體來保護它們。
- 策略API終端:設定和管理目標清單和每個清單的目標。
- 調查API終端:研究Umbrella解析器觀察到的域、IP地址和URL。
- 報告API終端:讀取和稽核有關部署的即時安全資訊。App Discovery API提供對基於雲的應用的深入分析。

API金鑰訪問和過期

- 根據預期用途，將每個範圍的訪問級別設定為「讀/寫」或「只讀」。
- 根據需要將API金鑰配置為在預定義的日期過期。



15143392160916

身份驗證和令牌生命週期

- API憑證生成有效期為60分鐘的訪問令牌。
- 身份驗證過程使用OAuth 2.0客戶端憑證流。
- 在多組織或服務提供商環境中，父組織API憑證可以在授權期間為指定的子組織生成具有相同作用域的訪問標籤。

檔案和資源

- 訪問綜合說明和使用案例文檔。
- 每個API用例都記錄在API參考中。
- 所有端點和引數都列在OpenAPI規範中，並連結在每個使用案例概述的底部。
- 如果您使用舊版Umbrella API，請參閱API遷移指南。
- 使用Postman Collection for the Umbrella API進行初始測試。
- 在思科開發人員頁面的「雲安全」部分瞭解其他資源、學習實驗室和API測試沙盒。

支援

有關Umbrella API的問題或其他幫助，請與Umbrella支援部門聯絡。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。