# 為Web策略管理配置基於規則的策略中的規則操 作

目錄			

### 簡介

本文檔介紹如何在基於規則的策略中為Web策略管理配置規則操作。

### 概觀

基於規則的策略使用基於身份匹配的規則集。每個規則集包含規則,每個規則根據身份、目標和計畫進行匹配。系統以自上而下的優先順序順序應用規則集和規則。標識與第一個適用的規則集匹配,然後應用與標識、目標和計畫匹配的第一個規則。

基於規則的策略中的一項新功能允許管理員將允許、警告、阻止或隔離操作分配給特定目標和應用程式的規則標識。

有關如何配置規則集和規則的說明,請參閱管理Web策略文檔。

# 動作:允許、允許(安全)、警告、阻止和隔離

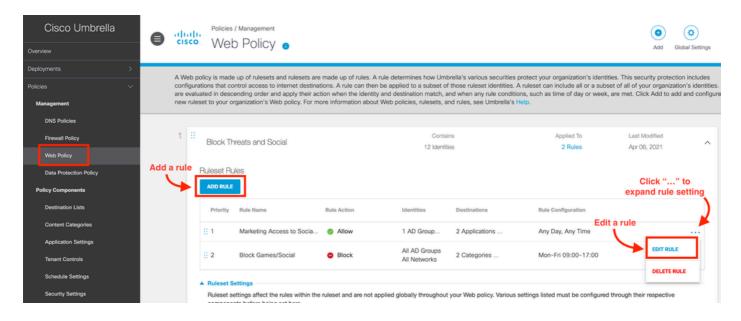
可以將以下操作之一分配給規則集中的單個規則:

IAIIOW ( ## # )	允許訪問目標或應用程式,除非檢測到安全問題。檔案檢查和安全類別仍然適用。 除非選擇安全覆蓋,否則這是「允許」的預設操作。	
允許	允許在沒有安全保護的情況下訪問目標或應用程式。無法覆蓋整個內容類別的安全設定。	
<u>警</u> 告	使用警告頁面和繼續選項來顯示規則身份,而不是阻止訪問。	
封鎖	拒絕訪問目標。規則標識無法覆蓋或繼續超過阻止頁。	
隔離	基於雲的瀏覽器不是阻止來自目標端點的標識,而是託管該目標的瀏覽會話。	

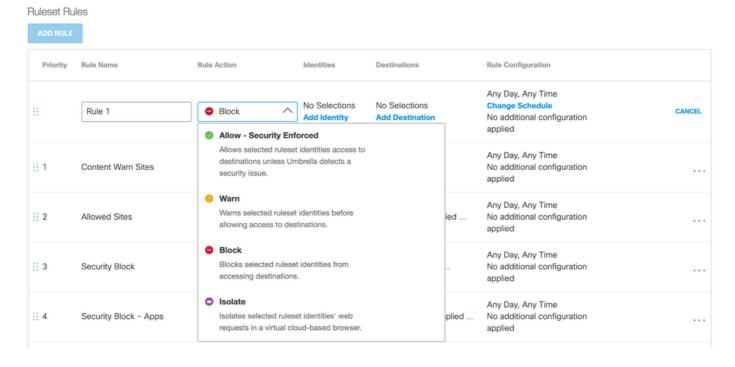
## 設定規則操作

建立或編輯規則時選擇規則操作。

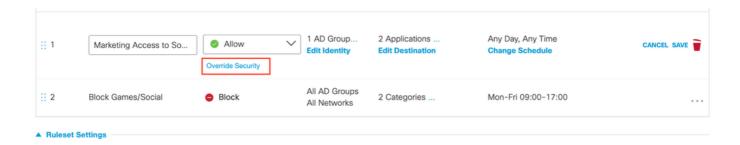
- 1. 轉至Web策略> [選擇適當的規則集]。
- 2. 按一下新增規則或編輯規則。



3. 在下拉選單中,為目標選擇Allow、Warn、Block或Isolatefor。



- 「allow」的預設設定應用安全性,並在檢測到威脅時阻止目標。
- 要允許無安全保護的訪問,請選擇「覆蓋安全」選項。



有關詳細資訊,<u>請訪問Umbrella Learning Hub獲取有關基於規則的策略的影片</u>。

#### 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)。