配置安全訪問安全配置檔案API高級

目錄

問題

嘗試通過公共API配置思科安全訪問安全配置檔案時，使用者會遇到一些限制，即只能使用預設設定建立基本配置檔案。API不公開高級安全功能的精細配置選項，包括：

- TLS解密設定
- 威脅類別實施控制
- 檔案型別阻止和檢查
- 惡意軟體檢測設定

使用者報告在嘗試通過標準API呼叫配置解密設定時收到「403 Forbidden」錯誤。記錄的公共API端點似乎缺少可通過GUI介面提供的詳細的安全配置檔案配置引數，從而限制了程式管理功能。

環境

- 思科安全存取平台
- 安全配置檔案API實施
- 所有受影響的軟體版本
- 公共API文檔終端

解析

高級安全配置檔案配置功能可通過Cisco Secure Access API獲得，但需要特定的實施方法和欄位命名約定，這些方法與記錄的公共API示例不同。這些解決步驟針對每個配置區域：

基本安全性配置檔案建立工作流

使用高級設定建立安全配置檔案的正確工作流程遵循兩個步驟：

步驟 1:使用POST建立基本安全配置檔案。

```
POST /api/v1/security-profiles
{
  "name": "profile_name",
  "description": "profile_description"
}
```

步驟 2:使用具有配置檔案ID的PUT配置高級選項。

```
PUT /api/v1/security-profiles/{profile_id}
{
  "advanced_settings": {
    "decryption_settings": {...},
    "file_settings": {...},
    "threat_settings": {...}
  }
}
```

檔案檢測和檔案型別阻止配置

可以在PUT請求中使用以下API欄位名稱來配置檔案檢查和檔案型別阻止：

- fileEngine — 控制檔案檢查功能。
- fileTypeControlStatus -啟用或禁用檔案型別阻止。

檔案設定的配置示例：

```
{
  "fileEngines": "enabled",
  "fileTypeControlStatus": "active",
  "blockedFileTypes": ["exe", "zip", "rar"]
}
```

TLS解密配置

TLS解密配置要求引用「不解密」清單ID，而不是使用專用的POST終結點。通過以下方法通過PUT API請求實現配置：

步驟 1:從現有配置中識別不解密清單ID。

步驟 2:引用PUT API請求中的清單ID。

```
{
  "seetingGroupBypassInspectionGroupID": "do_not_decrypt_list_id",
  "decryptionEnabled": true
}
```

這解決了嘗試通過其他API方法配置解密時發生的「403 Forbidden」錯誤。

威脅類別配置

威脅類別配置可通過未記錄的API終結點獲得，該終結點在成功解密配置後變為可訪問狀態。端點允許精細的威脅類別控制，但要求首先使用解密設定正確配置安全配置檔案。

API欄位名稱參考

此表將常用安全配置檔案功能對映到其對應的API欄位名稱：

功能	API欄位名稱	說明
TLS解密	設定GroupBypassInspectionGroupID	引用不解密清單ID
檔案檢查	檔案引擎	控制檔案檢查功能
檔案型別阻止	fileTypeControlStatus	啟用檔案型別限制

原因

限制的主要原因是API文檔不完整以及欄位命名規則不直觀，而不是實際的功能限制。高級安全配置檔案配置功能存在於API中，但通過以下方式實施：

- 與GUI術語不同的非明顯欄位名稱
- 兩步工作流程（POST用於建立，PUT用於高級配置）
- 依賴現有配置對象（如「不解密」清單）
- 針對某些功能的未記錄的API端點

公用API文檔沒有明確顯示這些實施細節，因此當通過替代方法實際提供這些功能時，會感覺到API的侷限性。

相關內容

- 思科安全存取安全設定檔API檔案
- 思科技術支援與下載

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）。