

# Stealthwatch管理控制檯安全X功能區上出現授權錯誤

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[問題](#)

[解決方案](#)

## 簡介

本文檔描述StealthWatch Management Center Secure X功能區發生錯誤的原因以及如何解決此問題

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco Secure X
- 思科威脅回應(CTR)
- Cisco StealthWatch管理主控台(SMC)

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

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，請確保您瞭解任何指令可能造成的影響。

## 問題

儘管在Secure X設定（Secure X和SSE）下顯示了與Secure X的正確配置連線，但SMC在SMC功能區上顯示錯誤

## 解決方案

由於使用功能區需要其他許可權，因此必須重新生成API憑據，並且已選擇擴展作用域並將其應用於SMC。

步驟1. 導航至 <https://visibility.amp.cisco.com/settings/apiClients>

步驟2. 根據提示使用用於登入CTR/Secure X的憑據登入

步驟3. 按一下「**Generate API Client**」

步驟4. 在相應欄位中輸入所需資訊：

客戶端名稱：*任何描述性名稱*

範圍：*所有範圍均為必填項*

說明：*可選詳細資訊*

步驟5. 按一下「**Add New Client**」

步驟6. 將生成的客戶端API ID和金鑰輸入到「SMC Secure X設定」頁

*https://*

步驟7. 定位至SMC控制面板。Secure X Dashboard按預期運行。