

Norton Antivirus解除安裝後，Windows Defender簽名資料庫為空，導致ISE狀態失敗

目錄

問題

通過VPN連線的Windows 11 25H2終端無法通過ISE狀態檢查並標籤為不合規的，從而阻止身份驗證和訪問網路資源。終端符合ISE規則要求，但在VPN連線後仍報告「使用者不符合要求」。

Windows Defender防病毒定義版本驗證安全狀態檢查特別失敗，出現以下錯誤：

```
[csc_iseposture]Function: CheckOpswat::CheckOpswatProd Thread Id: 0x277C File: CheckOpswat.cpp Line: 27
```

狀態代理報告Windows Defender的定義版本和定義日期為空0，導致AUC_WIN11_IT要求失敗。

環境

- 身分識別服務引擎(ISE)3.3
- Windows 11 25H2終端
- 帶ISE終端安全評估模組的思科安全客戶端
- ISECcompliance模組版本4.3.5626.8192
- Windows Defender版本4.18.25080.5
- 以前安裝並解除安裝了Norton 360防病毒軟體
- 啟用ISE終端安全評估實施的VPN連線

解析

解決方法涉及解除安裝Norton，然後手動更新Windows Defender簽名並瞭解第三方防病毒軟體和Windows Defender之間的共存行為。

步驟 1:更新Windows Defender簽名

1. — 導航到Windows安全設定並手動更新簽名資料庫：
2. — 轉到設定→隱私和安全→ Windows安全→病毒和威脅防護→病毒和威脅防護更新→檢查更新。
3. — 請等待Security intelligence version顯示非空值和當前時間戳，然後繼續狀態驗證。

步驟 3:驗證狀態合規性

更新簽名後，重新連線到VPN並驗證狀態檢查是否通過。安全情報版本現在必須顯示有效值，而不是為空。

第三方防病毒的重要注意事項

安裝任何第三方防病毒軟體並正確註冊到Windows安全中心後，Microsoft Windows會故意將Windows Defender置於被動模式以避免衝突。在被動模式下，Defender不會通過OPSWAT讀取的Windows安全中心/WMI API發佈其簽名新鮮度資料，導致狀態檢查失敗。

為防止出現此問題，請解除安裝windows進入「活動」模式的第三方應用程式。如果需要重新安裝Norton或其他第三方防病毒軟體，請注意這會導致終端再次變得不合規了。

原因

根本原因在於，當第三方防病毒軟體(Norton)是主要防病毒軟體時，Windows Defender簽名資料庫會變得陳舊。安裝Norton時，Windows故意使Defender定義儲存保持陳舊，因為被動模式防病毒軟體不會接收計畫的更新。在解除安裝Norton之後，Windows Defender成為主要防病毒軟體，但其簽名資料庫保持為空，因為第一個簽名提取在Windows Update後排隊，並且僅在下一個計畫觸發時或在使用者手動強制時自動運行。

當Defender本地定義儲存為空時，OPSWAT v4 SDK方法1001(GetDefinitionState)返回空負載，導致ISE狀態代理向ISE傳輸空定義版本。然後，ISE將此空值與策略閾值進行比較，並將端點標籤為不合規的。

相關內容

- [思科安全客戶端管理員指南 — 第三方軟體注意事項](#)
- [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）。