

由於客戶端抑制和軟體缺陷，ISE 3.2 MDM合規性查詢失敗

目錄

問題

某些通過Cisco身份服務引擎(ISE)上的EAP-TLS進行身份驗證的終端間歇性地未從Microsoft Intune接收合規狀態，即使在Intune控制面板中顯示為合規狀態。因此，這些終端會遇到預設無線授權策略，而不是預期的終端安全評估合規策略或終端安全評估不合規策略。受影響的終端在ISE即時日誌或外部MDM報告中不顯示流動裝置管理(MDM)合規性屬性，並且該問題僅影響部署中的客戶端子集。

觀察到的具體症狀包括：

- 異常客戶端在外部流動裝置管理報告的ISE報告中沒有日誌。
- 異常客戶端在即時日誌詳細資訊中沒有諸如MDM相容狀態或裝置相容狀態之類的屬性。
- 非正常客戶端觸碰無線802.1x_EAP-TLS_toyotawifi授權策略，而不是狀態合規策略。
- 日誌中的錯誤消息顯示「無法連線到MDM伺服器：404 Not Found」。

環境

- Cisco ISE多節點群集版本3.2補丁6
- 集群中的8個ISE節點，全部顯示綠色狀態
- 11,000個與Microsoft Intune整合的無線/有線客戶端
- 客戶端使用EAP-TLS (電腦證書) 身份驗證
- ISE使用客戶端的MAC地址進行查詢以進行Intune
- 所有客戶端在Microsoft Intune儀表板上具有相容狀態

- 問題會影響某些客戶端，但不會影響所有客戶端

解析

通過上述步驟解決了此問題。

步驟 1: 確定根本原因

對ISE日誌的分析顯示，受影響的終端具有過時的MDM伺服器ID，從而無法執行MDM查詢。

日誌顯示：

```
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MDMUtil -:::- M
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MdmServersCache -
2026-06-15 13:35:14,344 ERROR [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.pip.MdmPartnerPIPHandl
```

此外，發現部署正在觸發Cisco錯誤ID CSCwv51917，這會在使用MAC地址時的MDM伺服器ID過時時影響MDM合規性查詢。

步驟 2: 臨時解決方法

作為臨時解決方法：

1. — 從情景可視性中刪除終結點並重新進行身份驗證。發現此問題是為了解決查詢MDM伺服器和獲取合規性狀態的問題。
2. — 導航至情景可視性。
3. — 選擇終端mac地址並將其刪除。
4. — 重新驗證端點。

步驟 3:永久解決方案 — 軟體升級

永久解決方案正在思科錯誤ID CSCwv51917下跟蹤。

原因

在身份驗證期間，ISE嘗試查詢過時的MDM伺服器引用，但對應的MDM伺服器對象不再存在或處於非活動狀態。因此，ISE不會從Intune檢索MDM合規性屬性。

相關內容

- [思科錯誤ID CSCwv519173134](#)
- [ISE 3.2版本說明 — 已解決的警告](#)
- [ISE 3.2生命週期終止通知](#)
- [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）。