

02_資訊服務申請 - 資訊 #1416

Forti防火牆無法以網域帳號登入

2026-03-16 14:16 - 駱正達

狀態:	In process-進行中	開始日期:	2026-03-16
優先權:	Normal	完成日期:	
被分派者:	駱正達	完成百分比:	80%
分類:		預估工時:	0:00 小時
版本:		耗用工時:	8:00 小時
需求人員:		聯絡人e-mail:	
需求部門單位:		希望完成日期:	
聯絡人分機/手機:		完成日期:	

概述

韌體升級(7.4.7)後，出現無法以網域帳號登入的狀況

歷史

#1 - 2026-03-16 16:40 - 駱正達

- 檔案 clipboard-202603161632-vatqn.jpg 已新增

- 狀態 從 New-新增 變更為 Resolved-解決

- 完成百分比 從 0 變更為 80

115.1月時發生無法以網域帳號登入的狀況

LDAP server設定後無法與AD建立連線

以網域帳號登入皆出現：驗證錯誤

3/13 聯繫防火牆維護商及代理商工程師。前來協助處理。

主要原因：(原廠訊息)

升級到FortiOS【7.4.4】後出現 LDAP 驗證失敗的情況主要原因是強制執行更嚴格的LDAPS (基於SSL的LDAP)憑證驗證,導致出現「未知CA」錯誤。若要解決此問題,請將簽署LDAP伺服器憑證的CA憑證匯入 FortiGate 的遠端CA儲存區。

根本原因和解決方案

· 強制執行LDAPS/STARTTLS 憑證檢查:FortiOS7.4及更高版本會嚴格驗證憑證鏈。如果LDAP 伺服器憑證不受信任,則驗證失敗。

。操作:前往「系統」>「憑證」,確保已將簽署 LDAP伺服器憑證的根/中間 CA憑證匯入並信任於「遠端CA」。

LDAP設定選項如下圖。CA_Cert_1, 需由AD Server產生。

clipboard-202603161632-vatqn.jpg

外點的防火牆, 由維護商【商丞】負責修正。

#2 - 2026-03-16 16:40 - 駱正達

- 狀態 從 Resolved-解決 變更為 In process-進行中

檔案

clipboard-202603161632-vatqn.jpg

99.8 KB

2026-03-16

駱正達