與技經評估組建立EAP連結

目錄

簡介

本文檔介紹如何使用基於隧道的可擴展身份驗證協定(TEAP)配置可擴展身份驗證協定(EAP)連結的ISE和Windows請求方。

必要條件

需求

思科建議您瞭解以下主題：

- ISE
- Windows請求方的配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本3.0
- Windows 10版本2004
- 技經評估組協定知識

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。

背景資訊

TEAP是一種基於隧道的可擴展身份驗證協定方法，它建立安全隧道並在該安全隧道的保護下執行其他EAP方法。

TEAP身份驗證在初始EAP身份請求/響應交換後分兩個階段進行。

在第一階段，技經評估組使用TLS握手來提供經驗證的金鑰交換，並建立受保護的隧道。隧道建立後，第二階段從對等體開始，伺服器進行進一步的對話以建立所需的身份驗證和授權策略。

Cisco ISE 2.7及更高版本支援TEAP協定。 型別長度值(TLV)對象在隧道內用於在EAP對等體和EAP伺服器之間傳輸身份驗證相關資料。

Microsoft在2020年5月發佈的Windows 10 2004版本中引入了對TEAP的支援。

EAP連結允許在一個EAP/Radius會話內進行使用者和電腦身份驗證，而不是兩個單獨的會話。

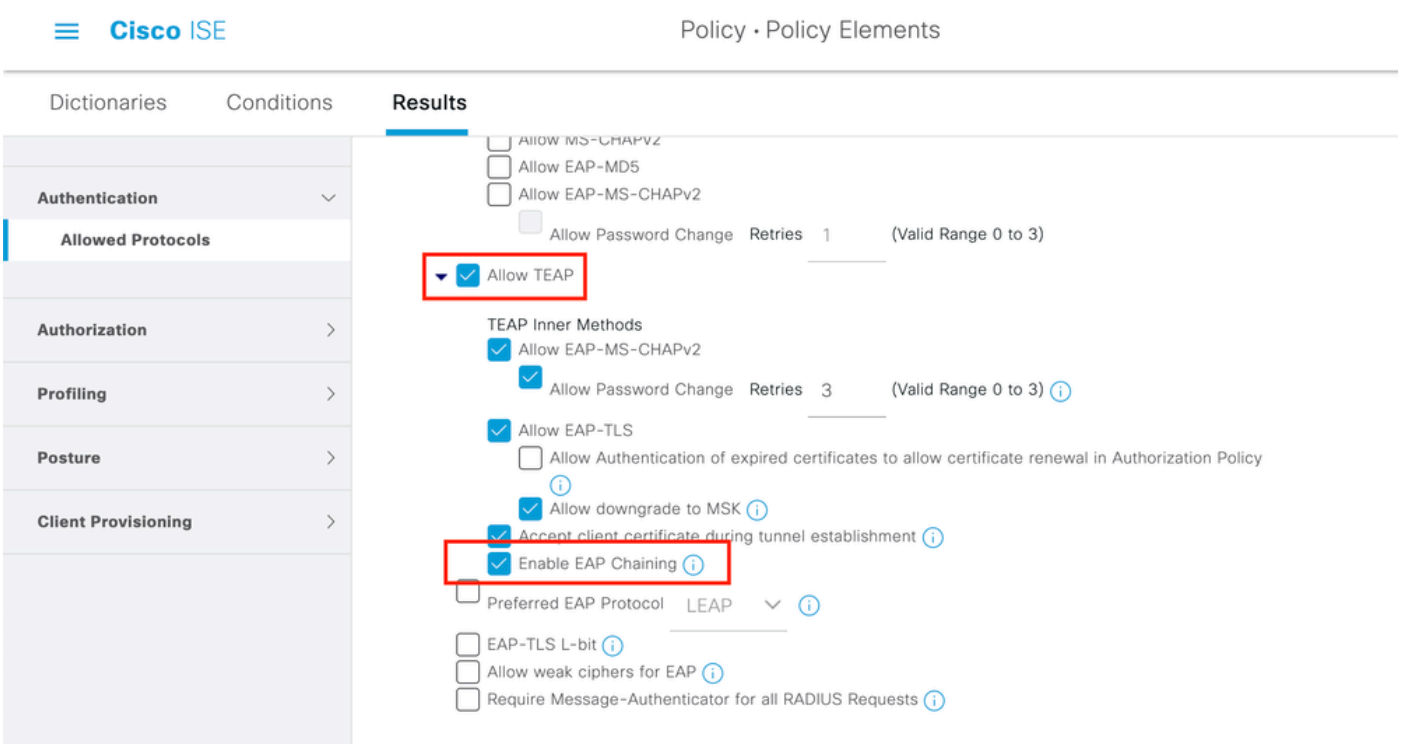
以前，要實現此目的，您需要使用Cisco AnyConnect NAM模組並在Windows請求方上使用EAP-FAST，因為本機Windows請求方不支援此功能。現在，您可以使用Windows原生Supplicant客戶端使用TEAP通過ISE 2.7執行EAP連結。

設定

Cisco ISE配置

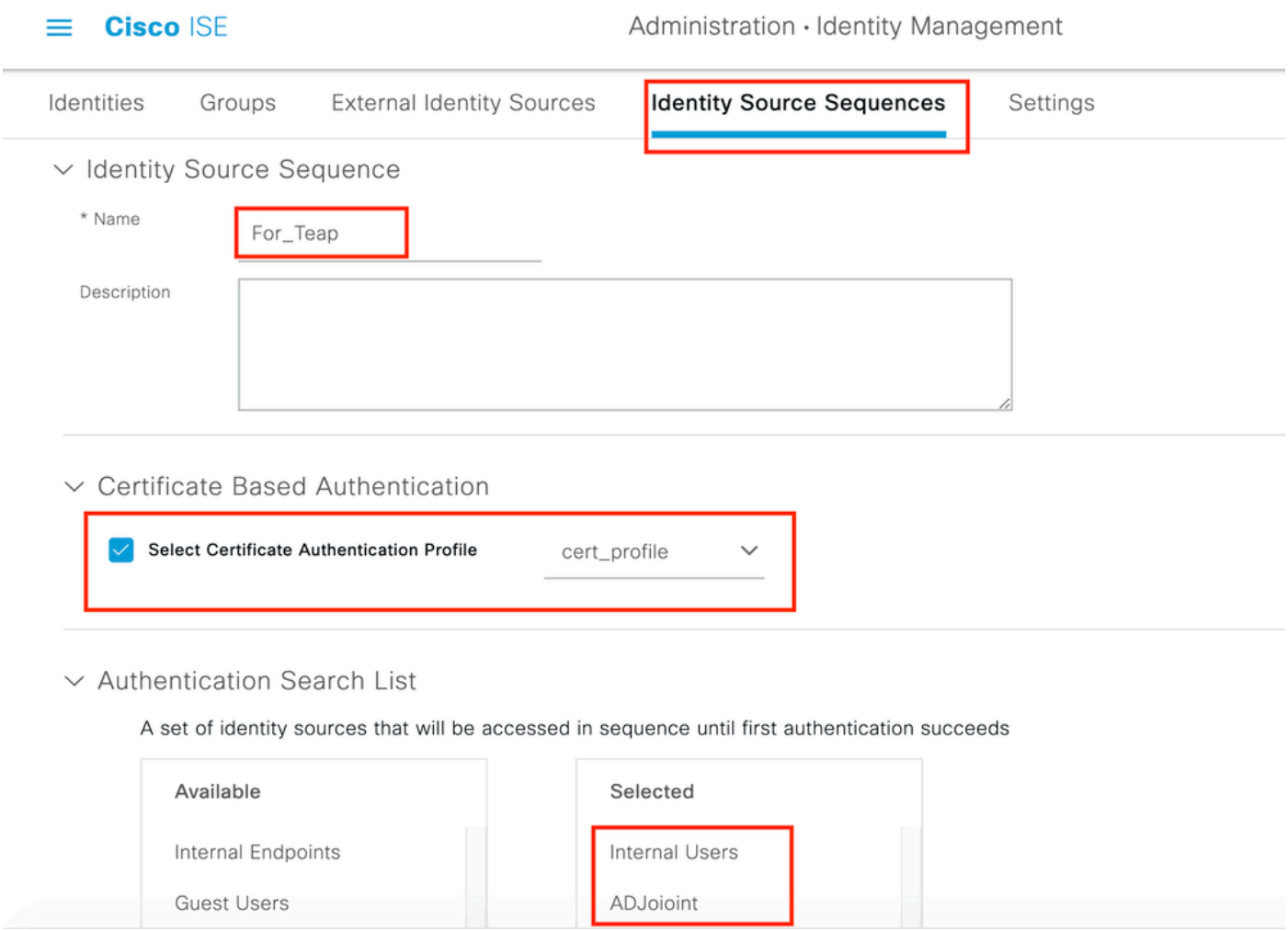
步驟1.您需要編輯「允許的協定」以啟用TEAP和EAP連結。

導航至 **ISE > Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add New** .選中TEAP和EAP連結覈取方塊。



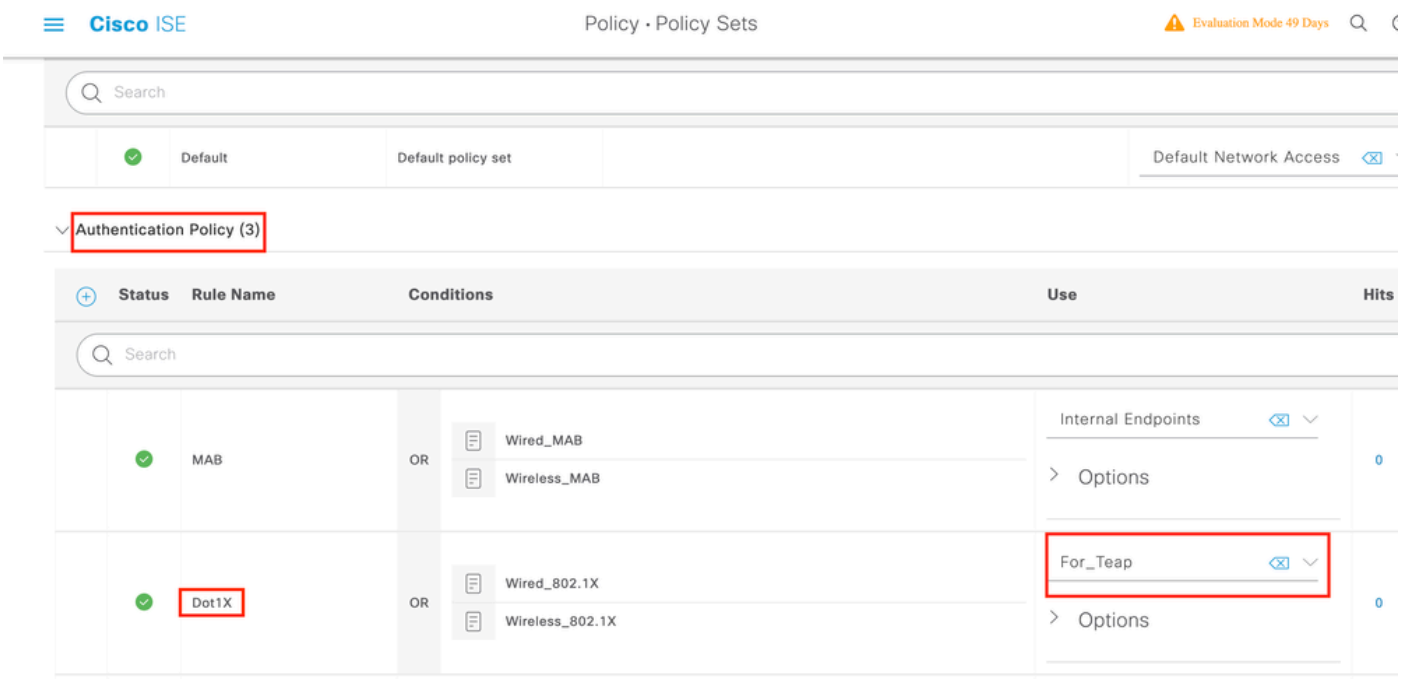
步驟2.建立證書配置檔案並將其新增到身份源序列。

導航至 **ISE > Administration > Identities > identity Source Sequence** 並選擇證書配置檔案。



步驟3.您需要在身份驗證策略中呼叫此序列。

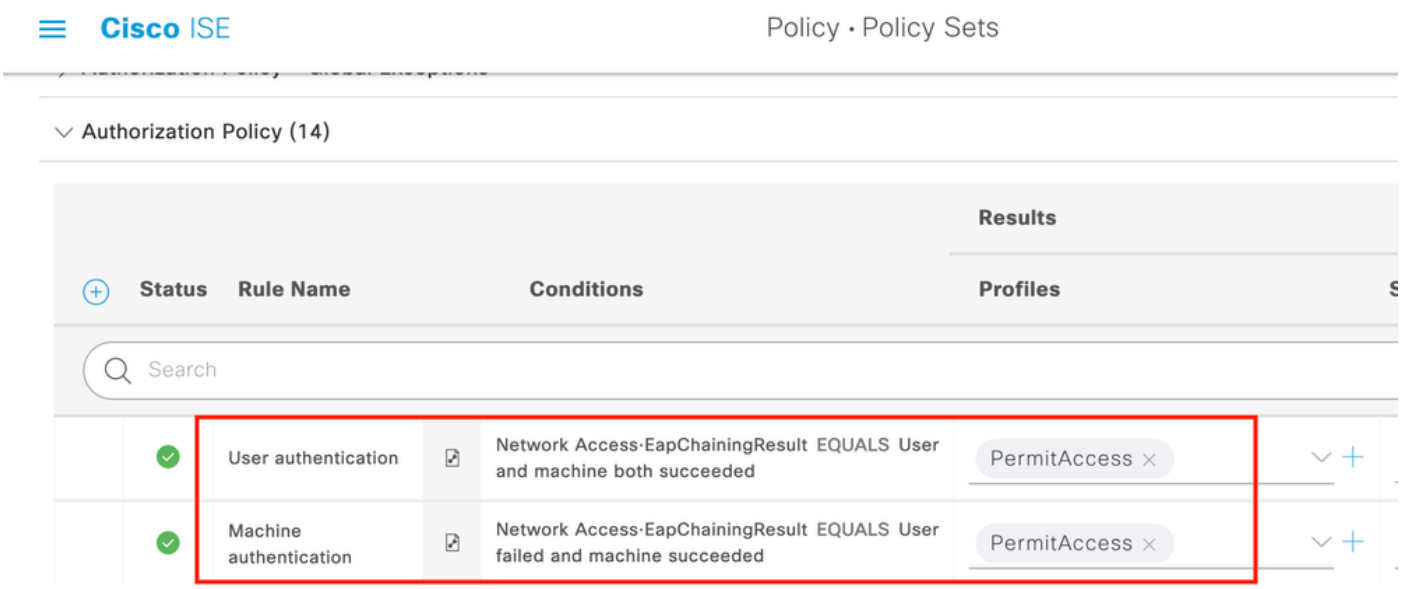
導航至 ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy 並選擇在步驟2中建立的Identity源序列。



步驟4.現在，您需要修改Dot1x Policy Set下的授權策略。

導航至 **ISE > Policy > Policy Sets . Choose the Policy Set for Dot1x > Authentication Policy .**

您需要建立兩個規則。第一條 規則檢查電腦是否已驗證，但使用者未驗證。第二規則驗證使用者和機器都經過身份驗證。



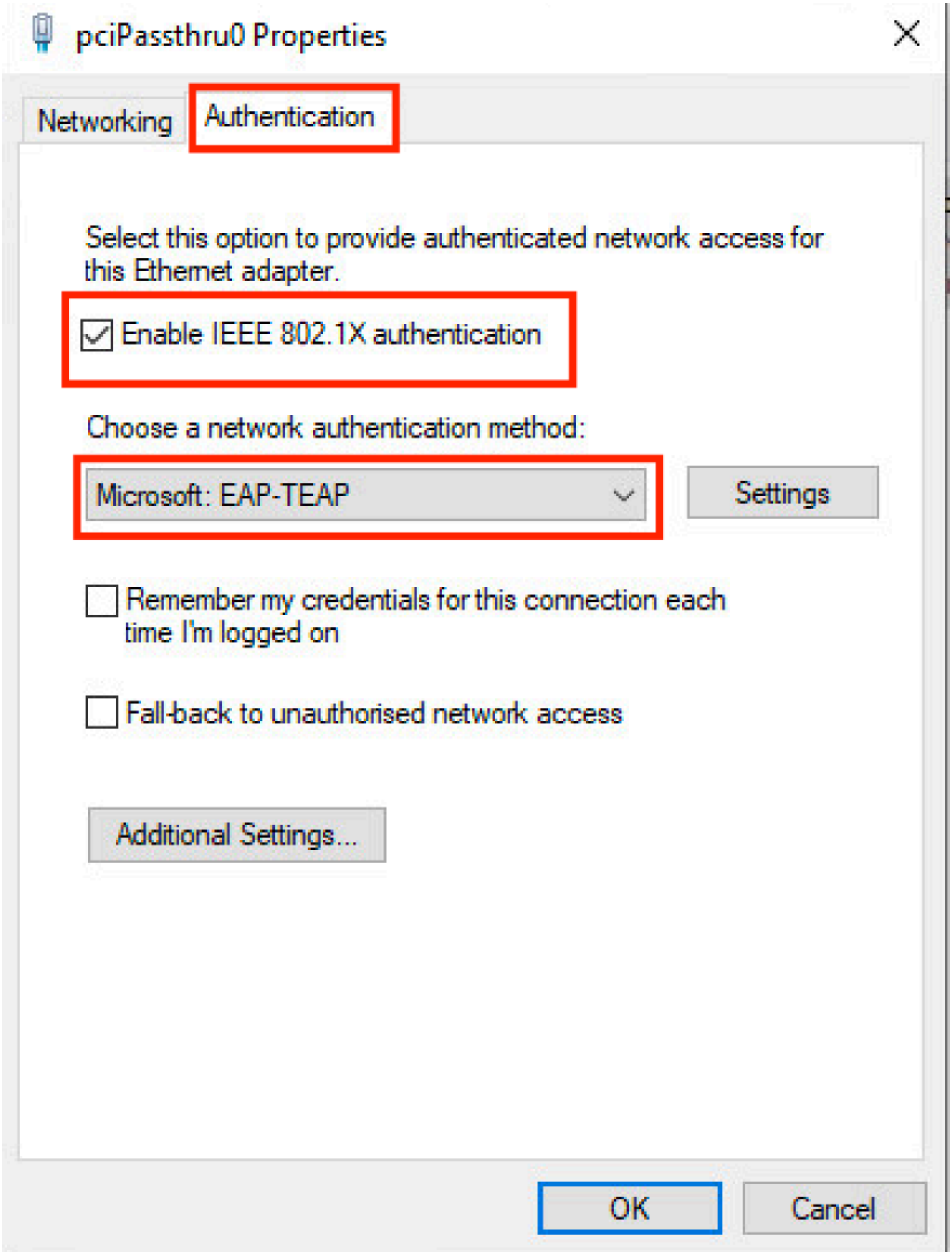
從ISE伺服器端完成配置。

Windows原生Supplicant客戶端配置

配置本文檔中的有線身份驗證設定。

導航至 Control Panel > Network and Sharing Center > Change Adapter Settings 並按一下右鍵 **LAN Connection > Properties.**按一下 **Authentication** 頁籤。

步驟1.按一下 Authentication 下拉選單並選擇 Microsoft EAP-TEAP.



步驟2. 按一下 **Settings** 按鈕。

1. 保留 Enable Identity Privacy 啟用了 anonymous 作為身份。
2. 在用於在ISE PSN上簽署EAP身份驗證證書的受信任的根證書頒發機構下的根CA伺服器旁邊放置一個複選標籤。

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）。