在ISE中安裝第三方CA簽名的證書

目錄

簡介

本檔案介紹如何在思科身分識別服務引擎(ISE)中安裝由第三方憑證授權單位(CA)簽署的憑證。

必要條件

需求

思科建議您瞭解基本公鑰基礎架構。

採用元件

本檔案中的資訊是根據思科身分識別服務引擎(ISE)版本3.0。相同組態適用於版本2.X

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。

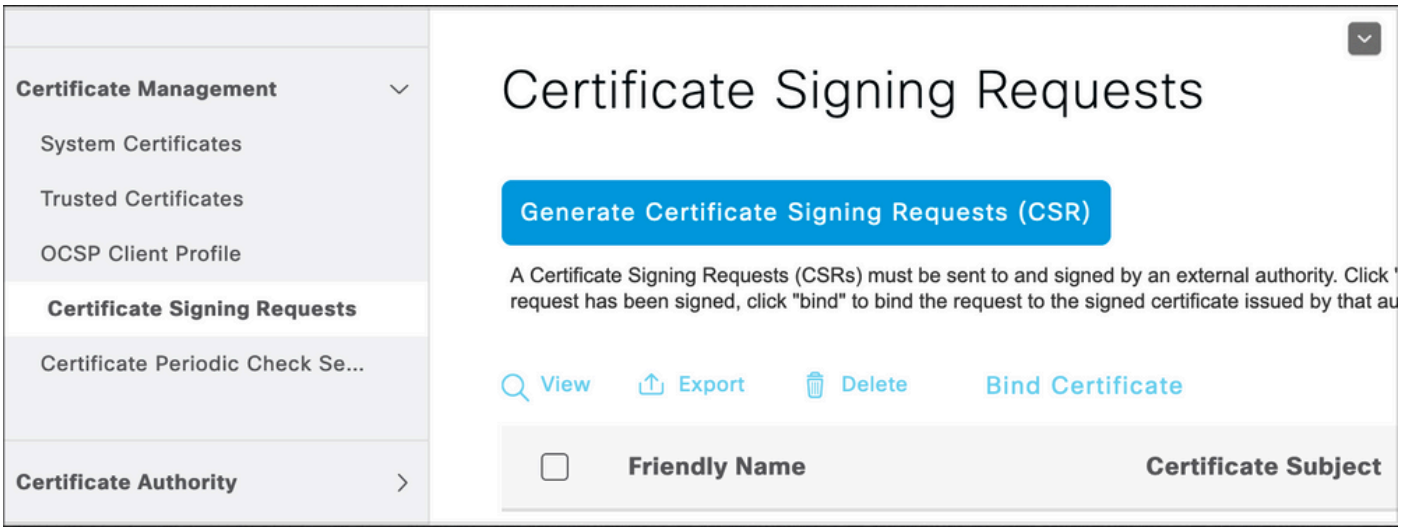
背景資訊

無論最終證書角色（EAP身份驗證、門戶、管理員和pxGrid）如何，此過程都是相同的。

設定

步驟 1.生成證書簽名請求(CSR)。

若要產生CSR，請導覽至管理>憑證>憑證簽署請求，然後按一下Generate Certificate Signing Requests(CSR)。



1. 在「用法」部分下，從下拉選單中選擇要使用的角色。如果證書用於多個角色，則可以選擇「多用」。生成證書後，可以根據需要更改角色。

2. 選擇可為其生成證書的節點。

3. 根據需要填寫資訊（組織單位、組織、城市、州和國家）。

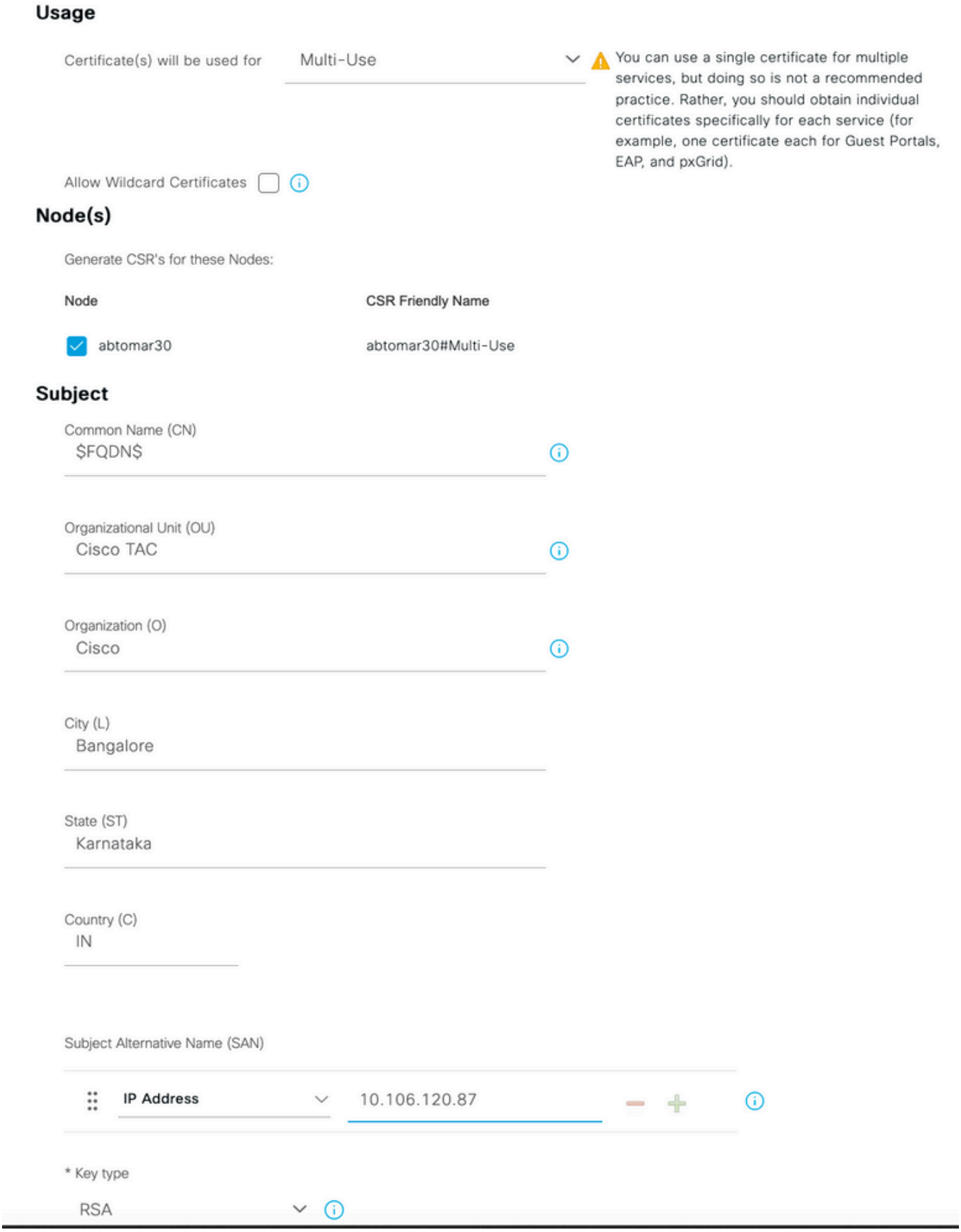
注意：在Common Name(CN)欄位下，ISE自動填充節點的完全限定域名(FQDN)。

萬用字元：

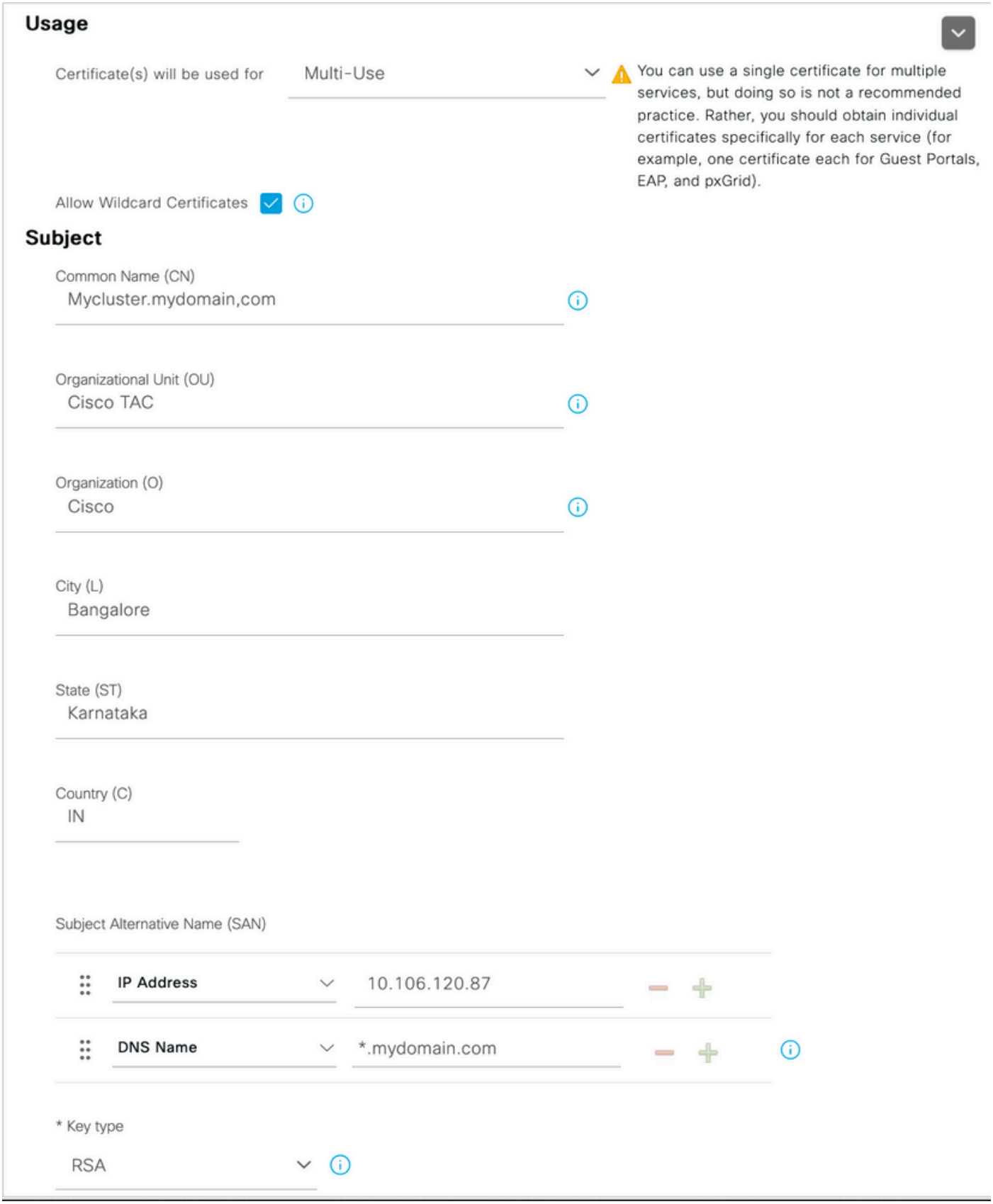
- 如果目標是生成萬用字元證書，請選中Allow Wildcard Certificates框。
- 如果證書用於EAP身份驗證，則*符號不能位於Subject CN欄位中，因為Windows請求方會拒絕伺服器證書。
- 即使Supplicant客戶端上禁用了Validate Server Identity，當*在CN欄位中時，SSL握手也可能失敗。
- 相反，可以在CN欄位中使用通用FQDN，然後 ***.domain.com** 可以在Subject Alternative Name(SAN)DNS Name欄位中使用。

註：某些憑證授權單位(CA)可以自動將萬用字元(*)新增到憑證的CN中，即使該萬用字元不存在於CSR中。在這種情況下，需要發出特殊請求來阻止此操作。

單個伺服器證書CSR示例：

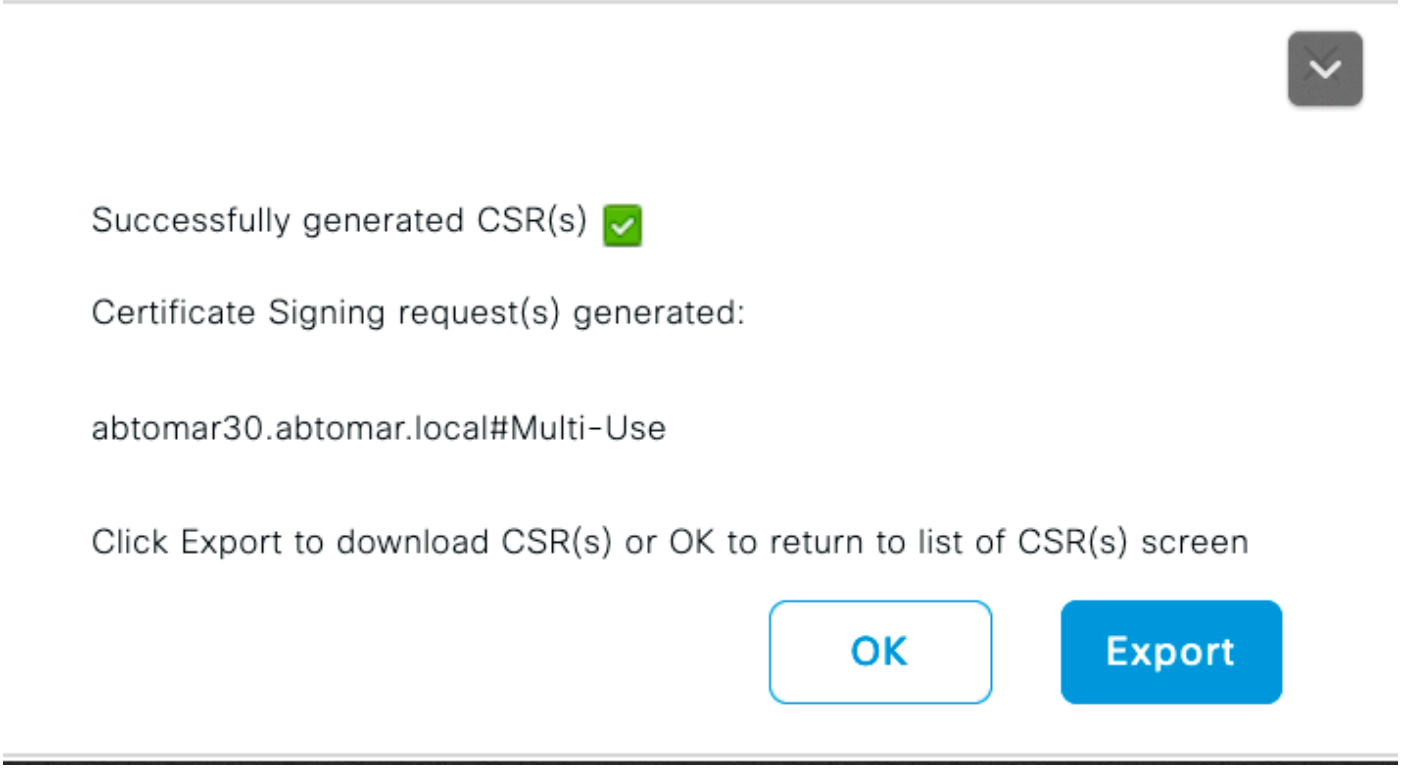

Usage
Certificate(s) will be used for
Multi-Use
You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).
Allow Wildcard Certificates
Node(s)
Generate CSR's for these Nodes:
Node
CSR Friendly Name
abtomar30
abtomar30#Multi-Use
Subject
Common Name (CN)
$FQDN$
Organizational Unit (OU)
Cisco TAC
Organization (O)
Cisco
City (L)
Bangalore
State (ST)
Karnataka
Country (C)
IN
Subject Alternative Name (SAN)
IP Address
10.106.120.87
* Key type
RSA

萬用字元CSR示例：



注意：每個部署節點的IP地址都可以新增到SAN欄位，以避免通過IP地址訪問伺服器時出現證書警告。

建立CSR後，ISE將顯示一個彈出視窗，其中包含匯出該視窗的選項。 匯出後，此檔案必須傳送到CA進行簽名。



步驟 2.匯入新的證書鏈。

證書頒發機構返回已簽名的伺服器證書以及完整的證書鏈（根/中間）。收到證書後，請執行以下步驟將證書匯入ISE伺服器：

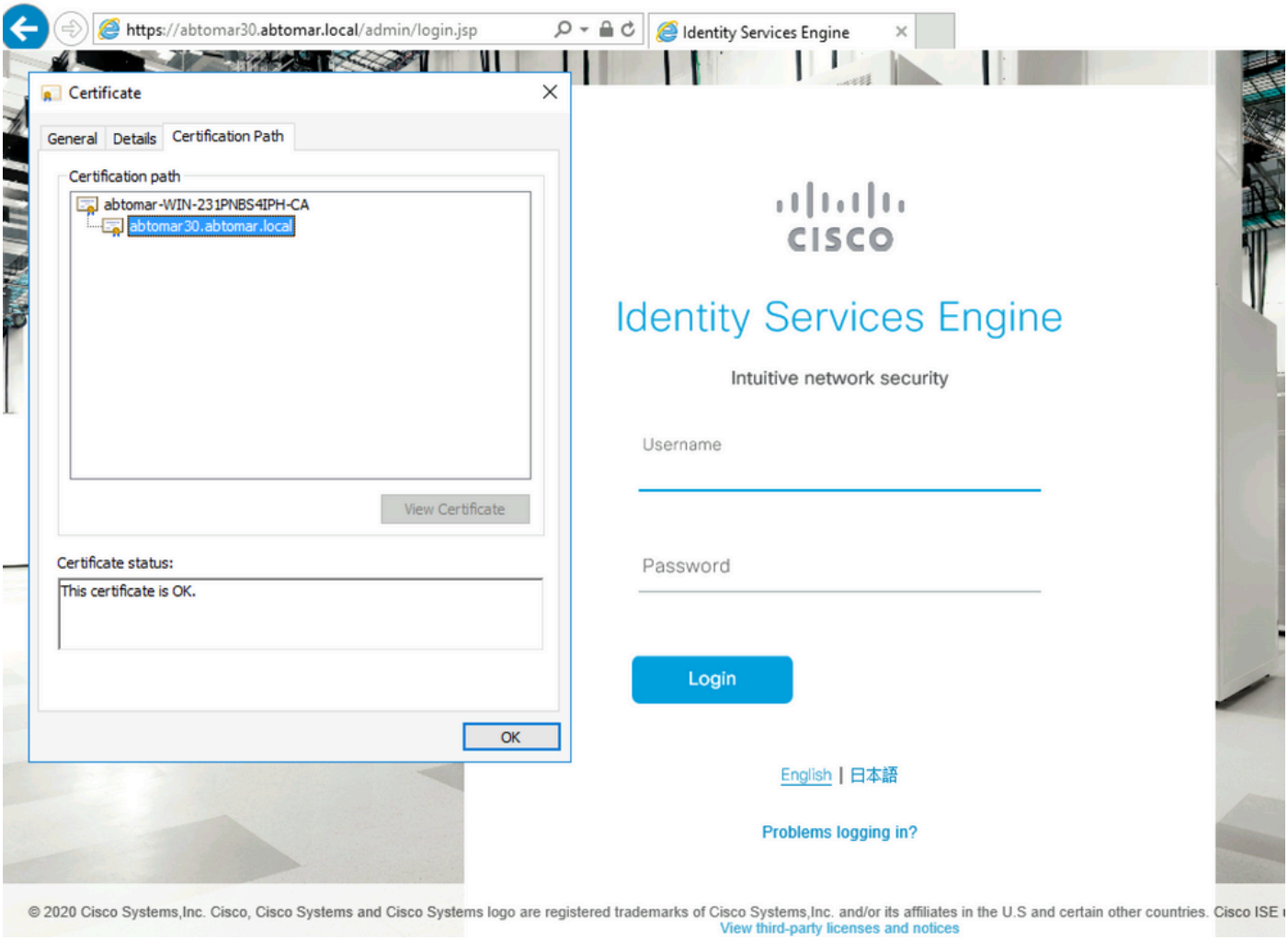
1. 要匯入CA提供的任何根和（或）中間證書，請導航到管理>證書>受信任證書。
2. 按一下Import，然後選擇Root和/或Intermediate證書，並在申請提交時選擇相關覈取方塊。
3. 若要匯入伺服器證書，請導航到管理>證書>證書簽名請求。
4. 選擇先前建立的CSR，然後按一下「Bind Certificate」。
5. 選擇新的證書位置，ISE將證書繫結到資料庫中建立和儲存的私鑰。

注意：如果已為此證書選擇管理員角色，則特定ISE伺服器服務將重新啟動。

注意：如果匯入的證書用於部署的主管理節點，並且選擇了管理員角色，則所有節點上的服務將依次重新啟動。這是預期情況，建議執行此活動時停機。

驗證

如果在證書匯入期間選擇了管理員角色，則可以通過在瀏覽器中載入admin頁來驗證新證書是否就位。只要鏈結構建正確，且憑證鏈結受瀏覽器信任，瀏覽器就必須信任新的管理員憑證。



對於其他驗證，請在瀏覽器中選擇鎖符號，並在證書路徑下驗證整個鏈是否存在，以及電腦是否信任該鏈。這不是伺服器正確向下傳遞了完整鏈的直接指示器，而是瀏覽器能夠基於其本地信任儲存信任伺服器證書的指示器。

疑難排解

在dot1x身份驗證期間，請求方不信任ISE本地伺服器證書

驗證ISE是否在SSL握手過程中通過完整證書鏈。

當使用需要伺服器證書（即PEAP）的EAP方法並且選擇了Validate Server Identity時，在身份驗證過程中，請求方使用其本地信任儲存中的證書來驗證證書鏈。作為SSL握手流程的一部分，ISE會呈現其證書以及其鏈中存在的任何根證書和（或）中間證書。如果鏈不完整，請求方將無法驗證伺服器身份。若要驗證憑證鏈結是否傳遞回使用者端，可以執行以下步驟：

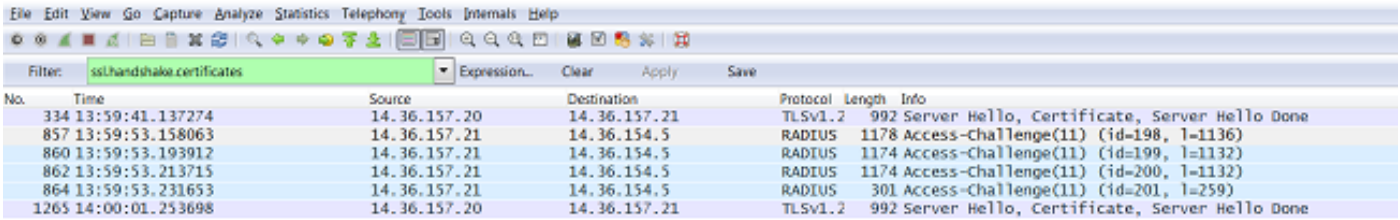
1. 要在身份驗證期間從ISE(TCPDump)獲取捕獲，請導航到操作>診斷工具>常規工具> TCP轉儲。

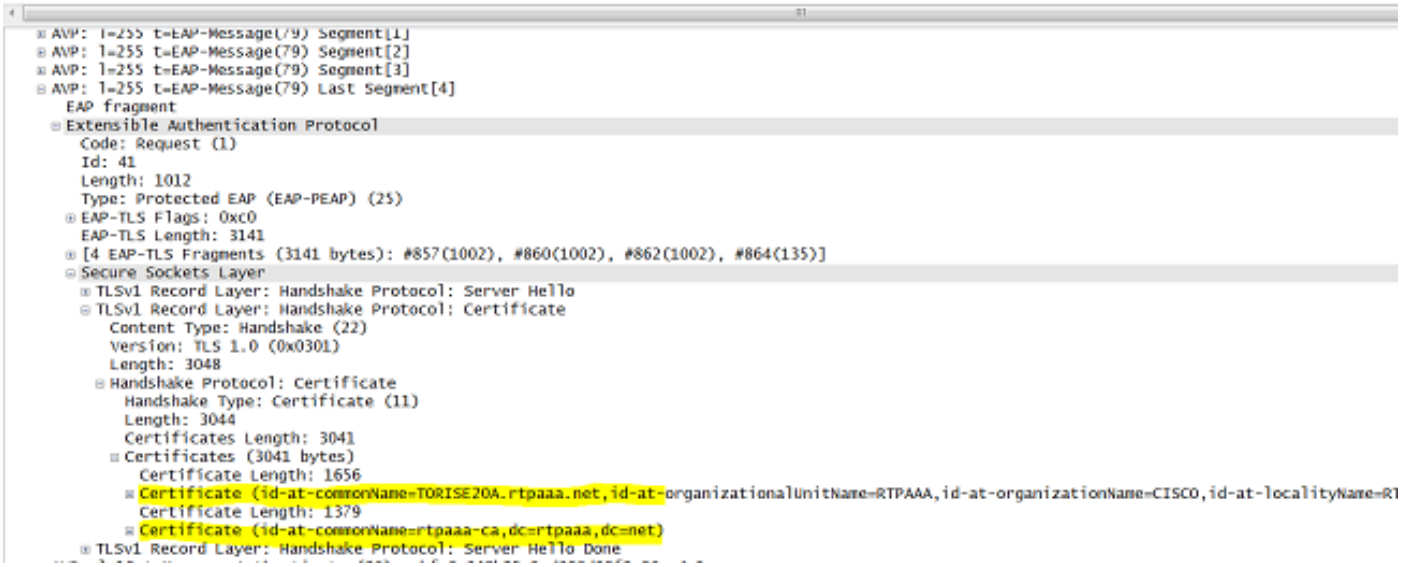
2. 下載/開啟捕獲並應用Wireshark中的過濾器ssl.handshake.certificates，然後查詢訪問質詢。

3. 選中後，導航至展開Radius協定>屬性值對> EAP — 消息最後段>可擴展身份驗證協定>安全

套接字層>證書>證書。

捕獲中的證書鏈。

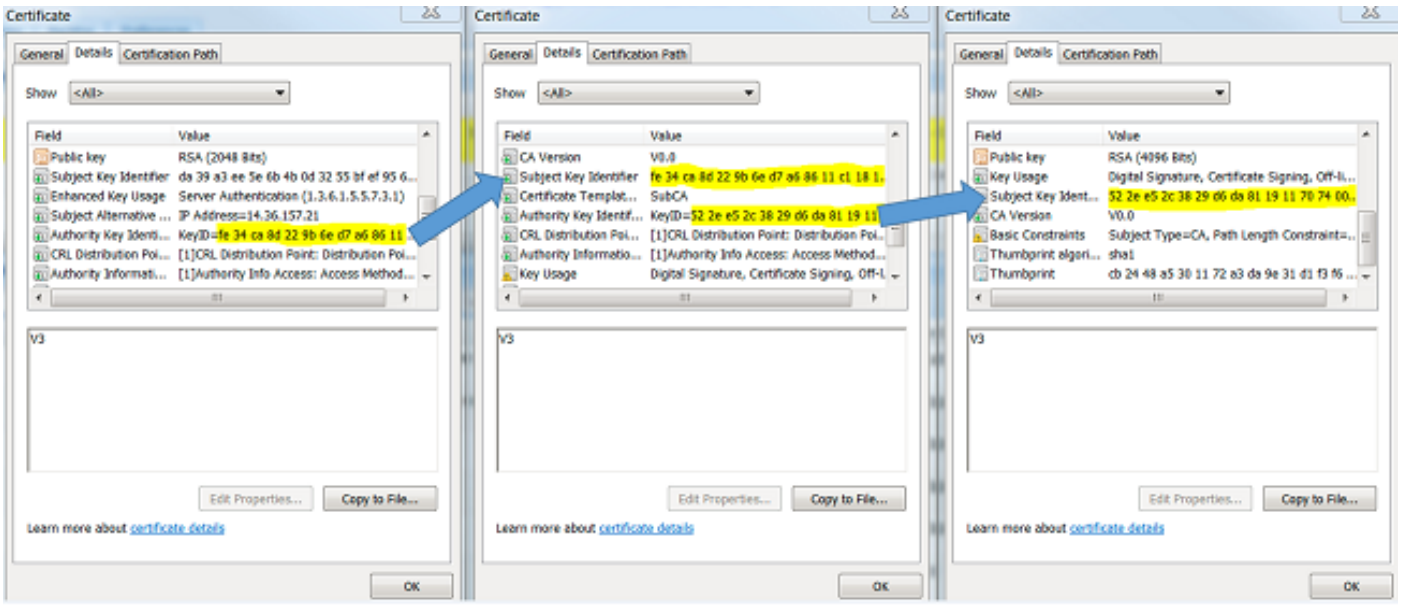




如果鏈不完整，請導航到ISE管理>證書>受信任證書，並驗證根和（或）中間證書是否存在。如果證書鏈成功通過，則必須使用此處概述的方法來驗證證書鏈本身是否有效。

開啟每個證書（伺服器、中間和根），通過將每個證書的主題金鑰識別符號(SKI)與鏈中下一個證書的頒發機構金鑰識別符號(AKI)匹配來驗證信任鏈。

憑證鏈結範例。

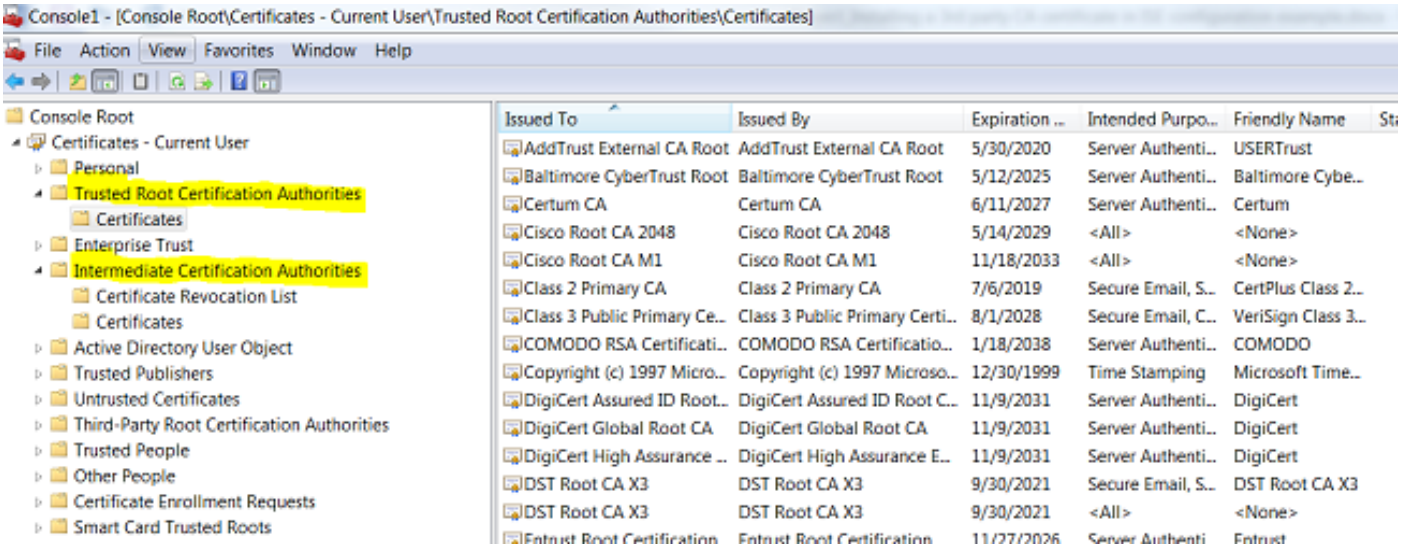


ISE證書鏈正確，但終端在身份驗證期間拒絕ISE伺服器證書

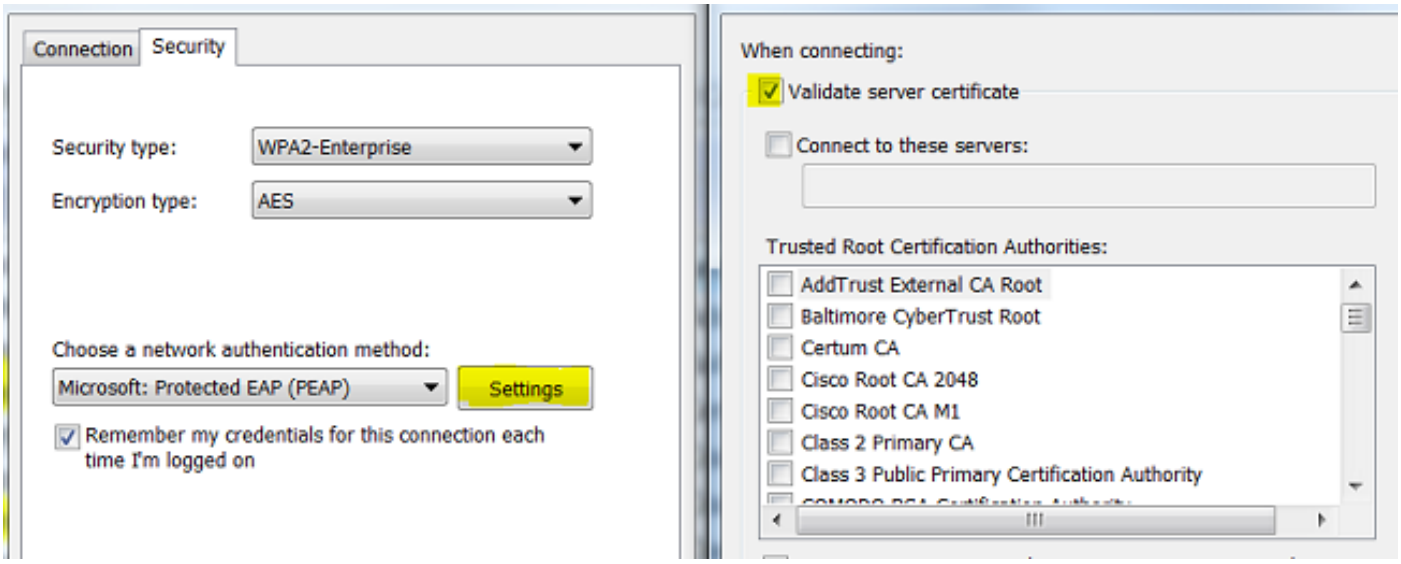
如果ISE在SSL握手期間呈現其完整證書鏈，而請求方仍拒絕證書鏈；下一步是驗證根證書和（或）中間證書是否在客戶端本地信任儲存中。

若要從Windows裝置驗證這一點，請導航到mmc.exe 檔案>新增 — 刪除管理單元。從「可用管理單元」列中選擇「證書」，然後按一下「新增」。根據使用的身份驗證型別（使用者或電腦）選擇我的使用者帳戶或電腦帳戶，然後按一下確定。

在控制檯檢視下，選擇Trusted Root Certification Authorities和Intermediate Certification Authorities以驗證本地信任儲存中是否存在根證書和中間證書。



驗證這是一個伺服器身份檢查問題的簡單方法，取消選中Supplicant客戶端配置檔案配置下的Validate Server Certificate，然後再次對其進行測試。



相關資訊

- 思科身份服務引擎管理員指南3.0版
- 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）。