為CUCM建立Windows CA證書模板

目錄

簡介

本檔案介紹逐步程式，以便在符合X.509擴展要求(適用於各種型別的Cisco Unified Communications Manager(CUCM)憑證)的Windows伺服器型憑證授權單位(CA)上建立憑證模板。

必要條件

需求

思科建議您瞭解以下主題：

- CUCM 11.5(1)版或更高版本
- 建議同時具備有關Windows Server管理的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 本文檔中的資訊基於CUCM版本11.5(1)或更高版本。
- 安裝了CA服務的Microsoft Windows Server 2012 R2。

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

外部CA可以簽署五種型別的憑證：

憑證	使用	受影響的服務

Callmanager	在安全裝置註冊時提供，可以簽署證書信任清單(CTL)/內部信任清單(ITL)檔案，用於與其他伺服器(如安全會話發起協定(SIP)中繼)的安全互動。	·Cisco Call Manager ·Cisco CTI Manager ·Cisco TFTP
tomcat	針對安全超文本傳輸協定(HTTPS)互動提供。	·Cisco Tomcat ·單一登入(SSO) ·分機移動 ·公司目錄
ipsec	用於生成備份檔案，以及與媒體網關控制協定(MGCP)或H323網關的IP安全(IPsec)互動。	·Cisco DRF Master ·Cisco DRF Local
CAPF	用於生成電話的本地重要證書(LSC)。	·思科憑證授權單位代理功能
電視	用於在電話無法驗證未知證書時建立與信任驗證服務(TVS)的連線。	·思科信任驗證服務

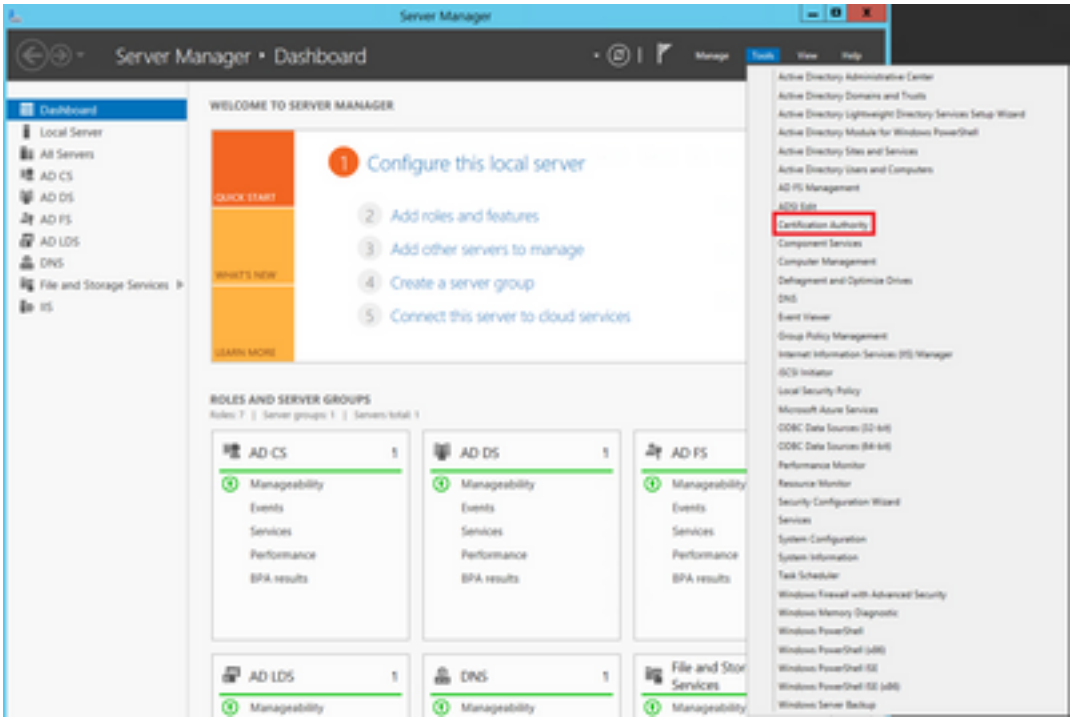
其中每個證書都有一些需要設定的X.509擴展要求，否則，您可能會在上述任何服務上遇到錯誤行為：

憑證	X.509金鑰用法	X.509擴充金鑰使用
Callmanager	·數位簽章 ·金鑰加密 ·資料加密	·Web伺服器身份驗證 ·Web客戶端身份驗證
tomcat	·數位簽章 ·金鑰加密 ·資料加密	·Web伺服器身份驗證 ·Web客戶端身份驗證
ipsec	·數位簽章 ·金鑰加密 ·資料加密	·Web伺服器身份驗證 ·Web客戶端身份驗證 ·IPsec終端系統
CAPF	·數位簽章 ·證書簽名 ·金鑰加密	·Web伺服器身份驗證 ·Web客戶端身份驗證
電視	·數位簽章 ·金鑰加密 ·資料加密	·Web伺服器身份驗證 ·Web客戶端身份驗證

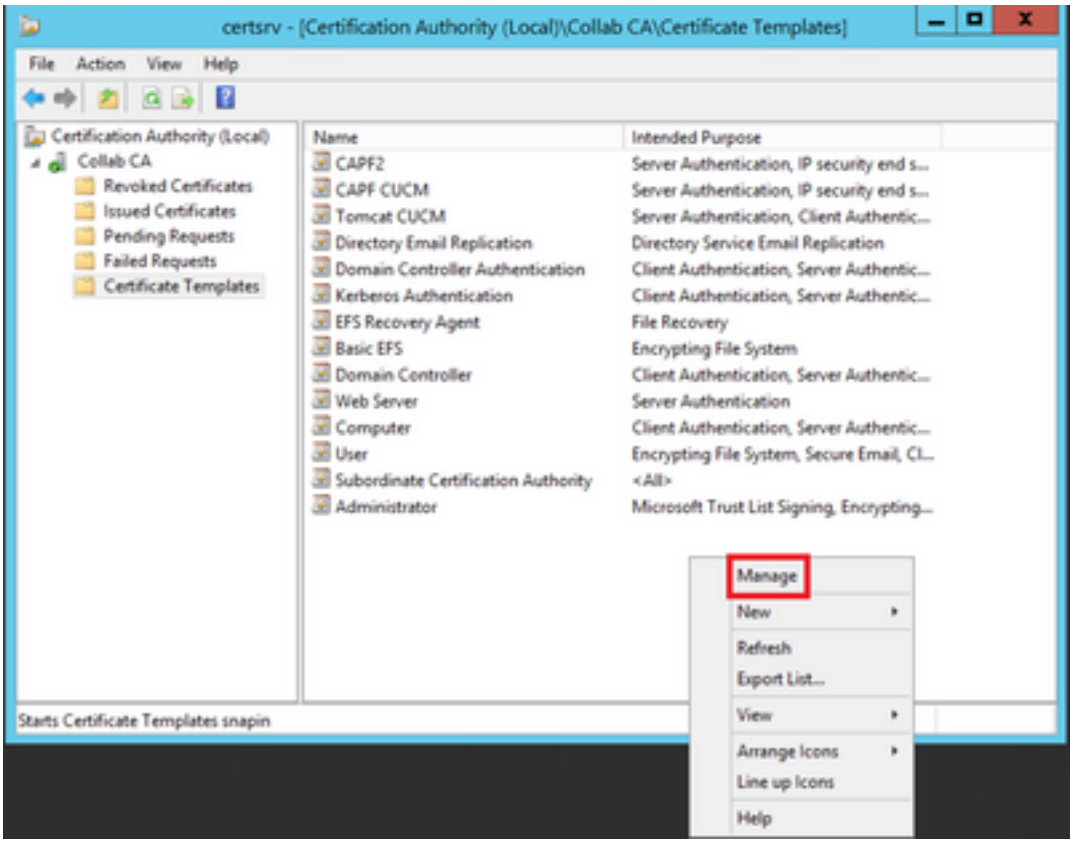
有關詳細資訊，請參閱Cisco Unified Communications Manager安全指南

設定

步驟1.在Windows Server上，導航到**Server Manager > Tools > Certification Authority**，如下圖所示。



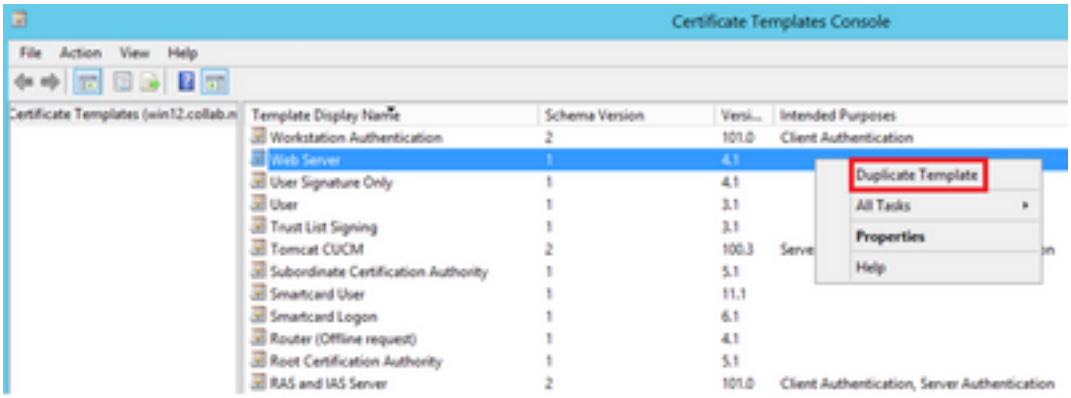
步驟2.選擇您的CA，然後導航到**Certificate Templates**，按一下右鍵清單並選擇**Manage**，如下圖所示。



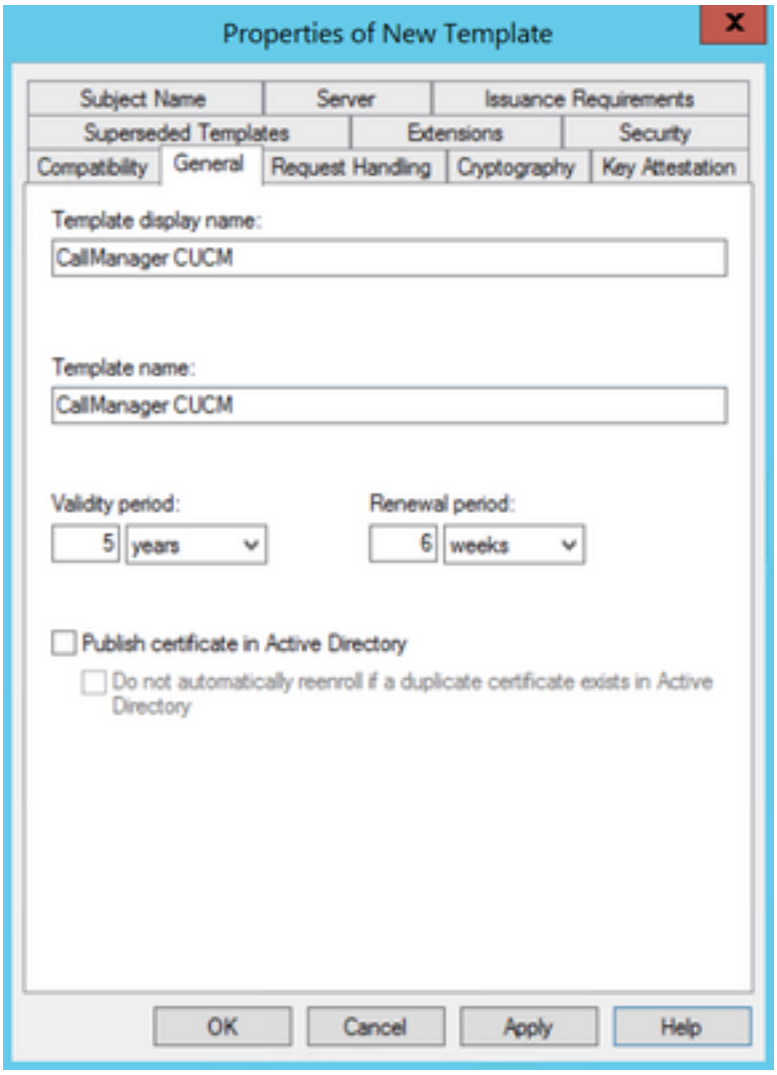
Callmanager/Tomcat/TVS模板

接下來的影象隻顯示CallManager模板的建立；但是可以按照相同的步驟為Tomcat和TVS服務建立證書模板。唯一的區別是確保分別的服務名稱用於步驟2中的每個新模板。

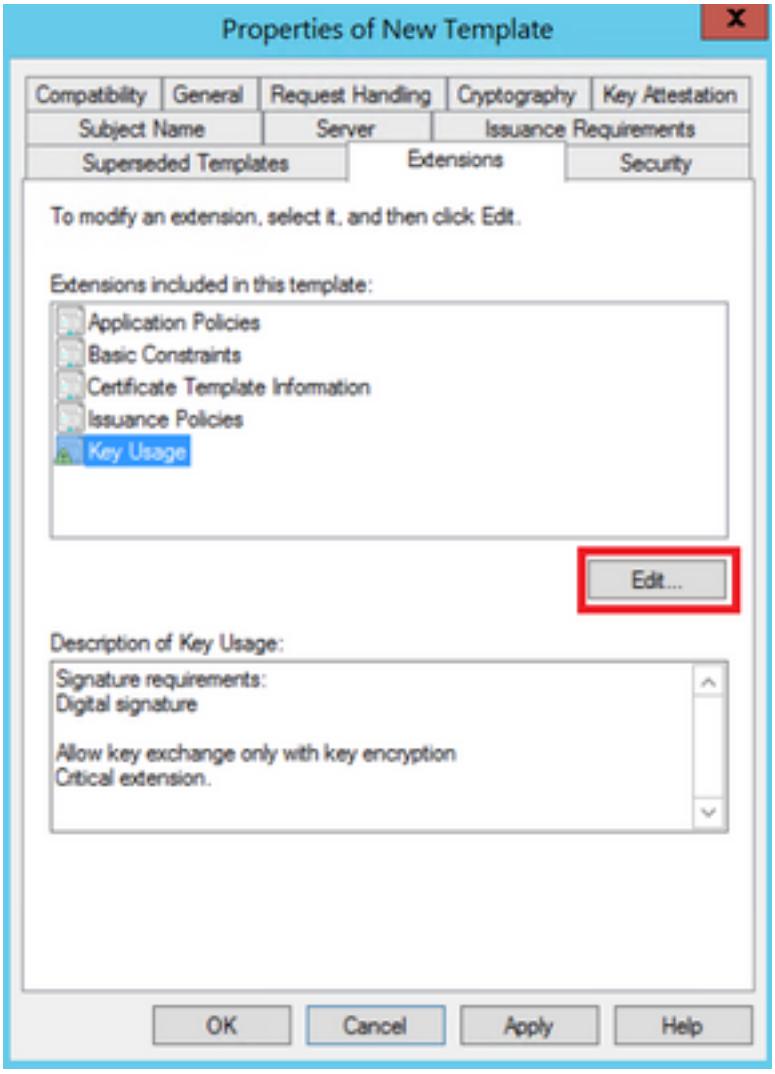
步驟1.找到**Web Server模板**，按一下右鍵該模板，然後選擇**Duplicate Template**，如下圖所示。



步驟2.在**General**下，您可以更改證書模板的名稱、顯示名稱、有效性等。

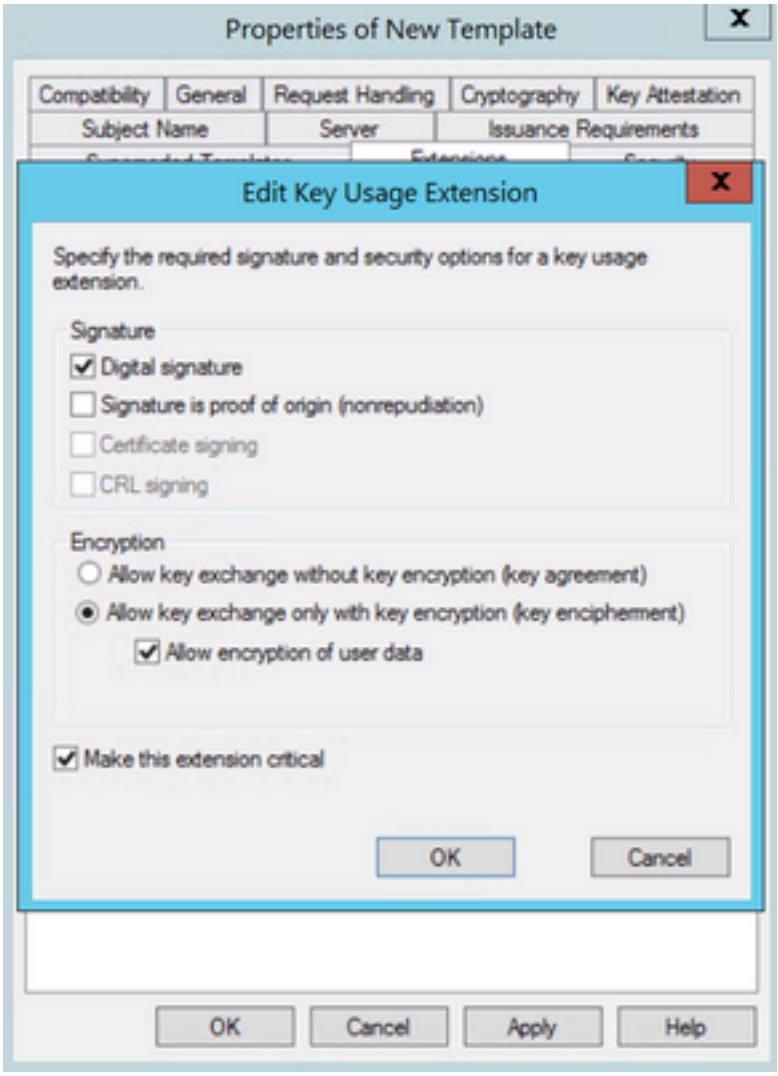


步驟3.導覽至**Extensions > Key Usage > Edit**，如下圖所示。

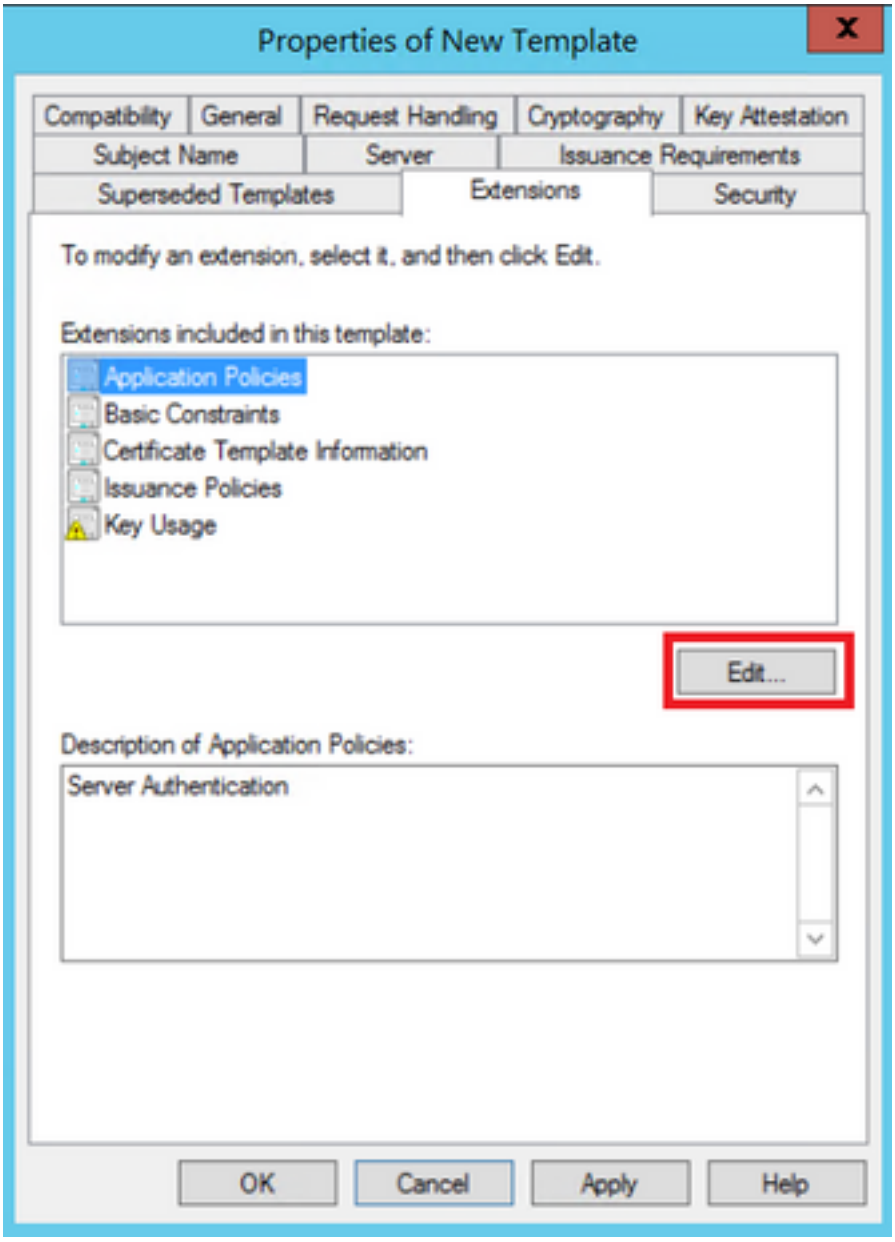


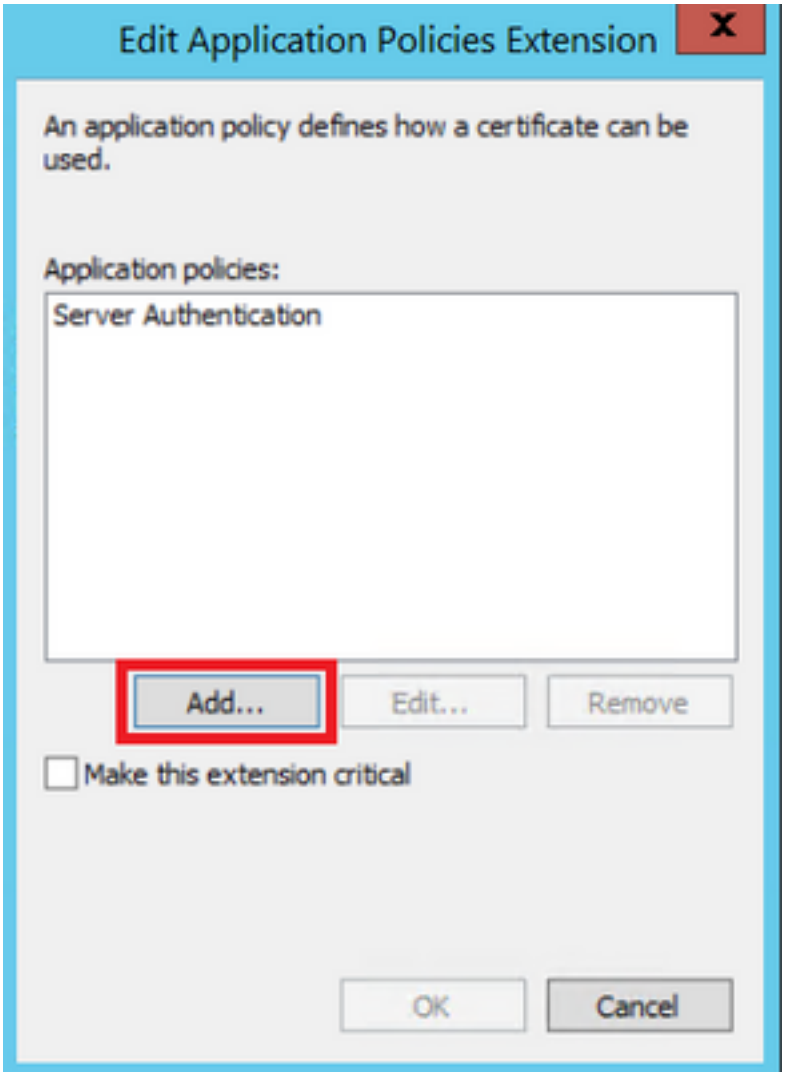
步驟4.選擇這些選項並選擇**確定**，如下圖所示。

- **數位簽章**
- **僅允許使用金鑰加密進行金鑰交換（金鑰加密）**
- **允許加密使用者資料**

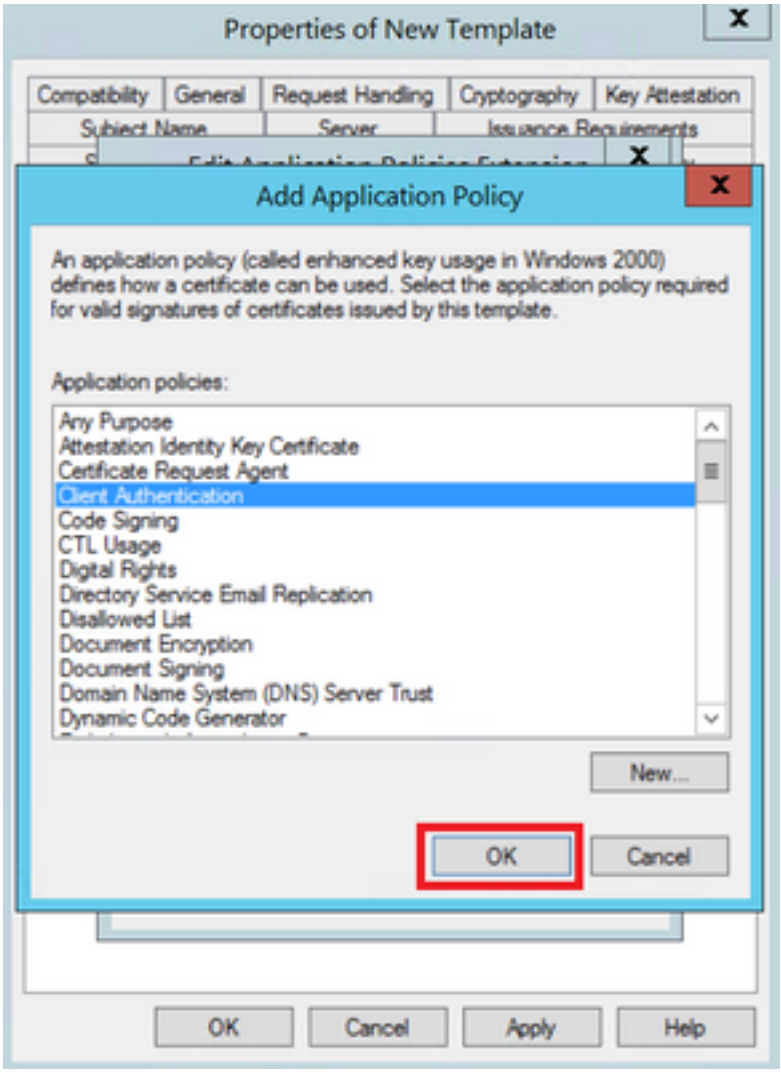


步驟5.導覽至**Extensions > Application Policies > Edit > Add**，如下圖所示。

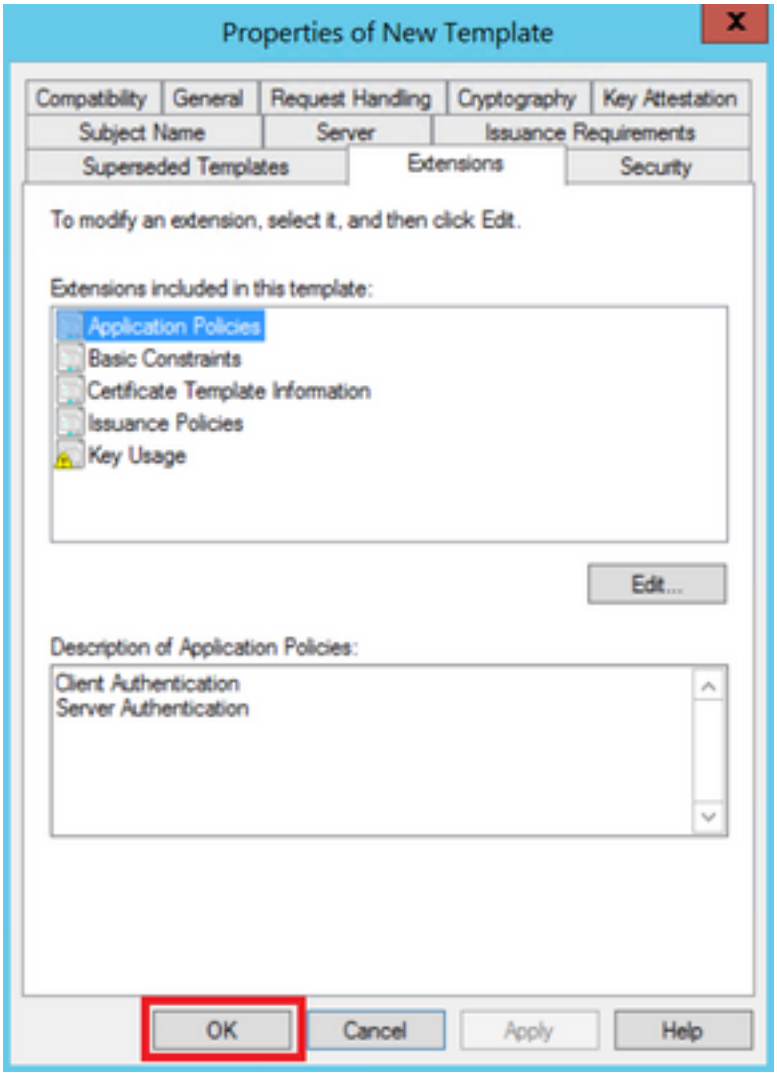

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Server Authentication
OK
Cancel
Apply
Help



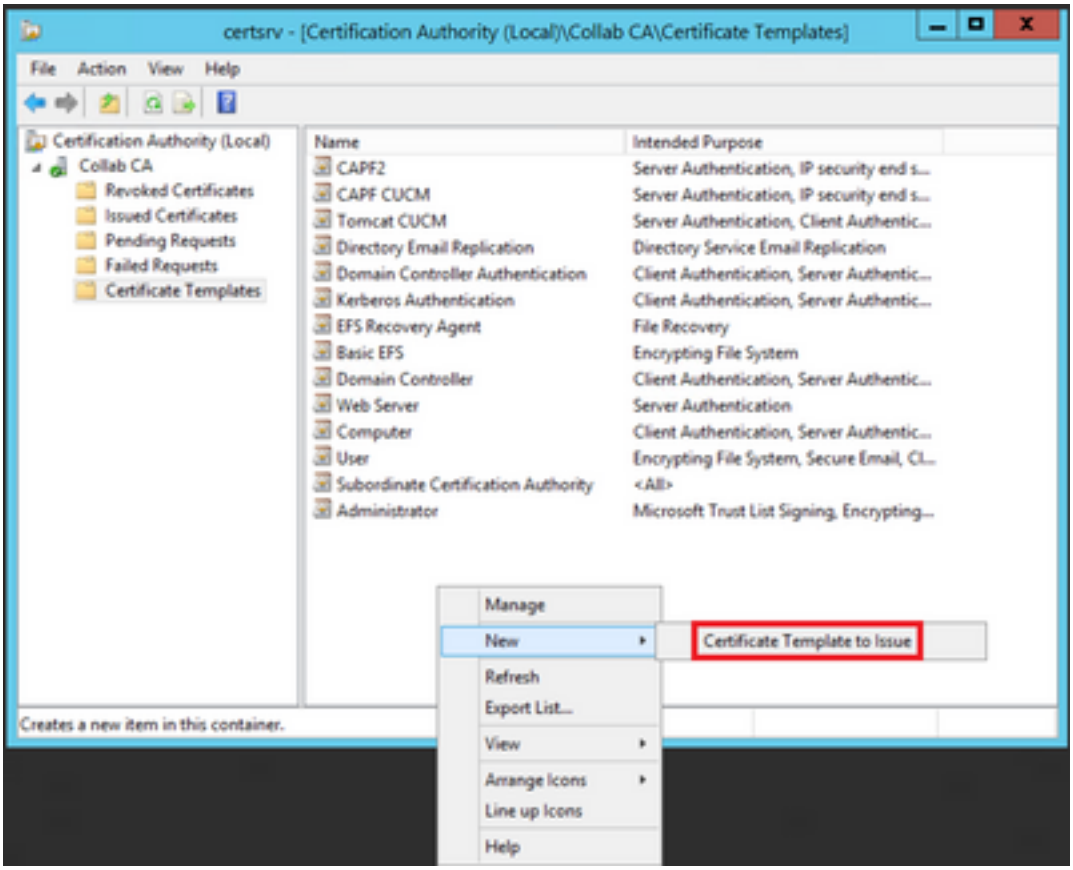
步驟6.搜尋Client Authentication，選擇該視窗，並在該視窗和上一個視窗上選擇OK，如下圖所示。



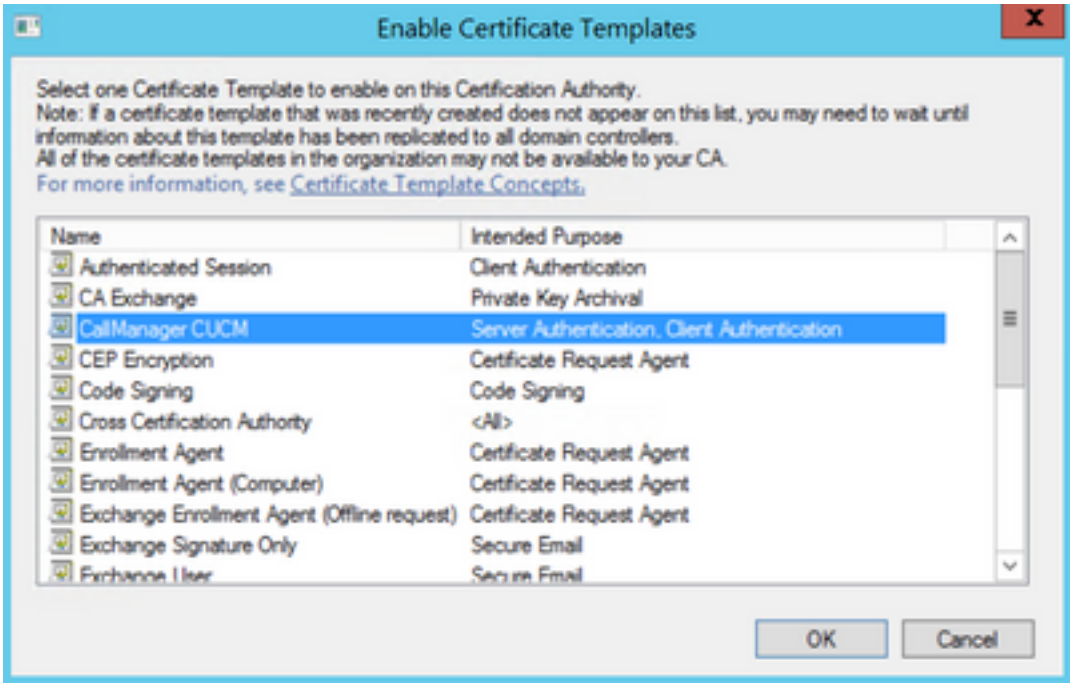
步驟7.回到模板上，選擇Apply，然後選擇OK。



步驟8.關閉「Certificate Template Console」視窗，然後在第一個視窗上導覽至New > Certificate Template to Issue，如下圖所示。



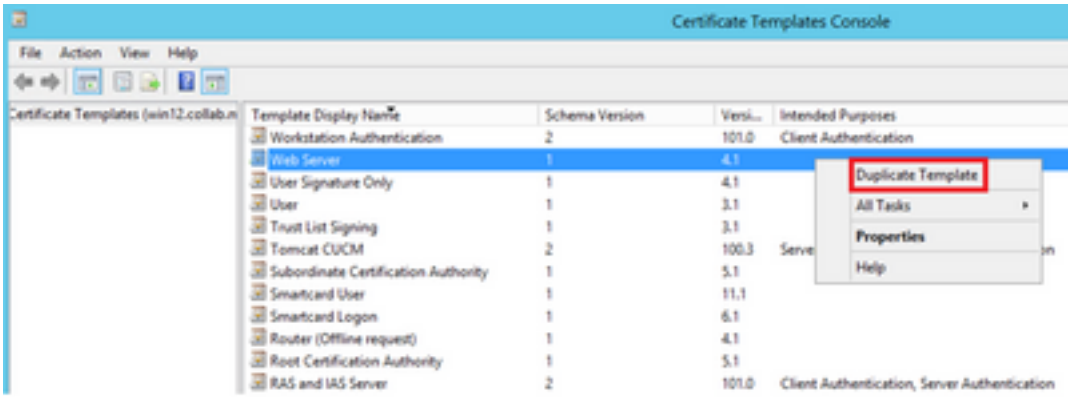
步驟9.選擇新的**CallManager CUCM模**板，然後選擇**OK**，如下圖所示。



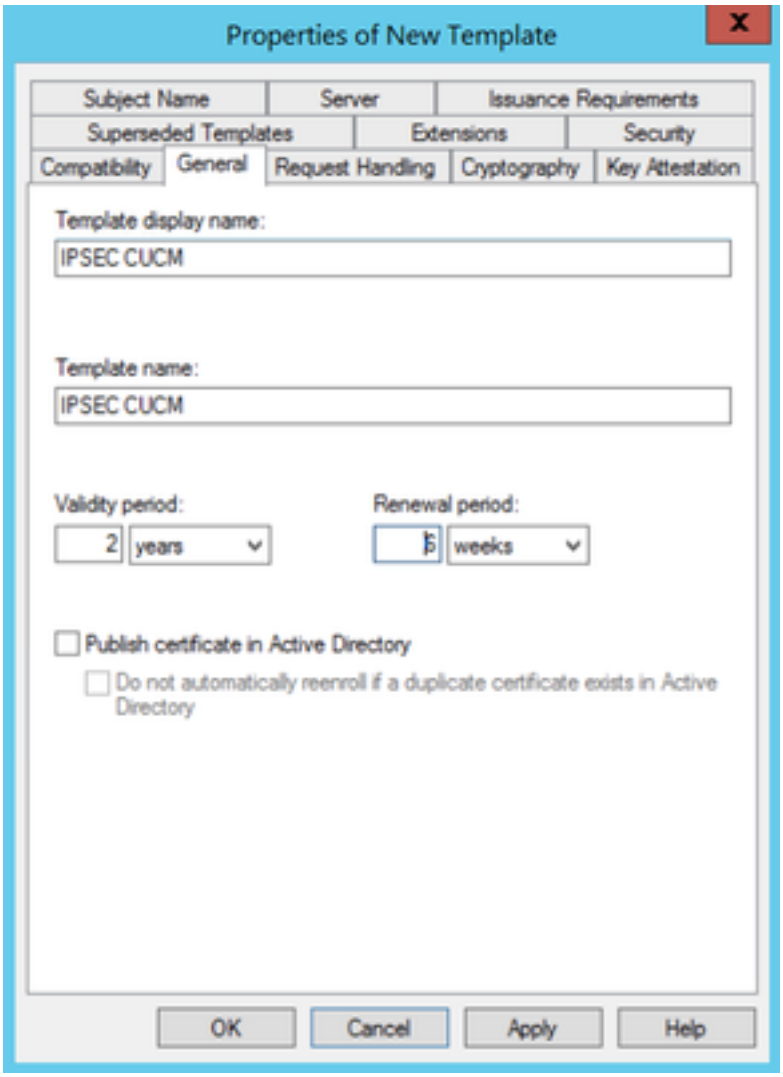
步驟10.根據需要重複前面的所有步驟，為Tomcat和TVS服務建立證書模板。

IPsec模板

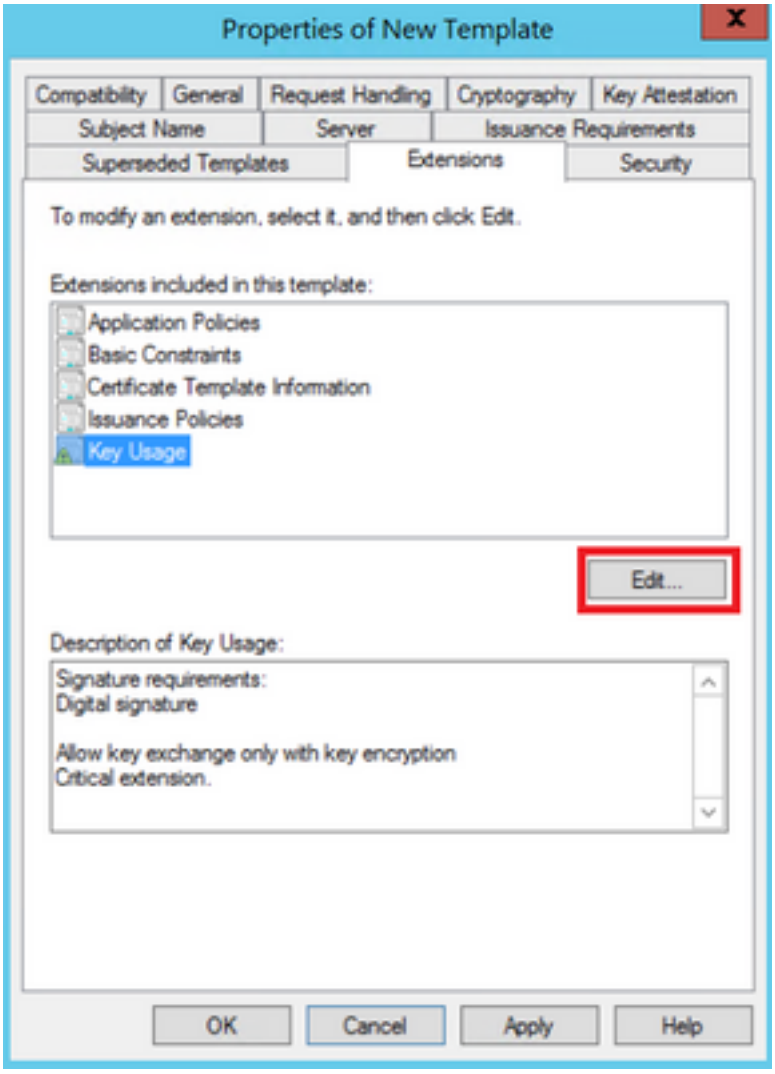
步驟1.找到**Web Server模板**，按一下右鍵該模板，然後選擇**複製模板**，如下圖所示。



步驟2.在General下，您可以更改證書模板的名稱、顯示名稱、有效性等。

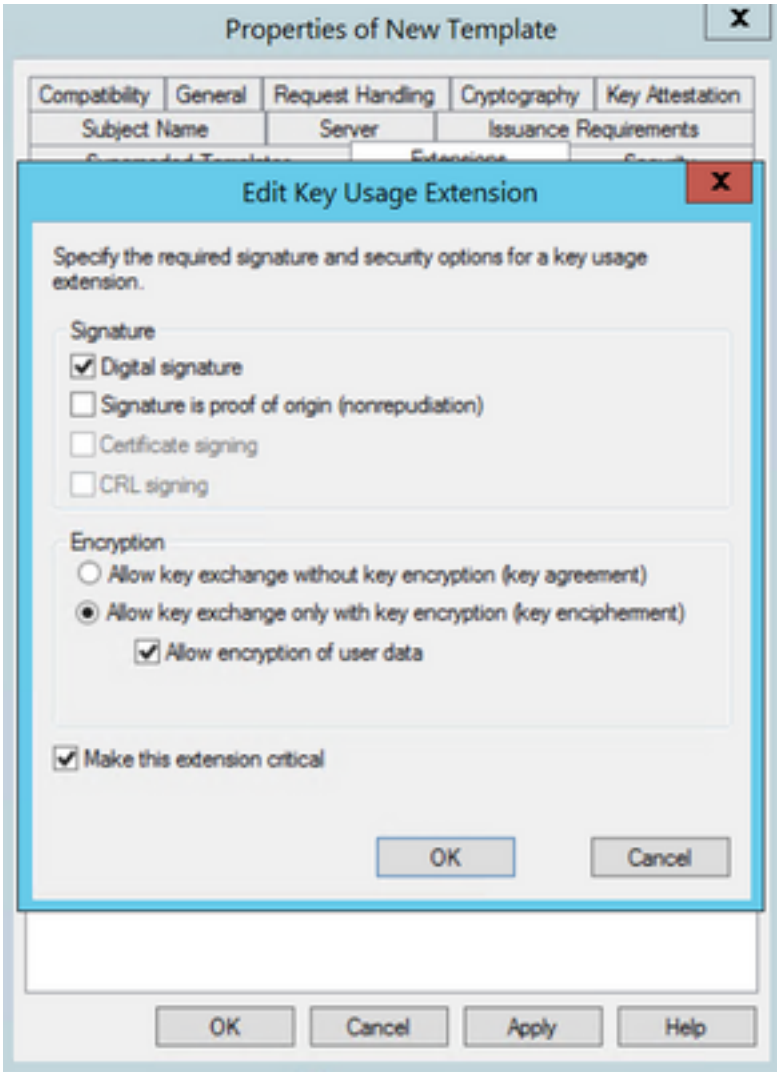


步驟3.導覽至Extensions > Key Usage > Edit，如下圖所示。

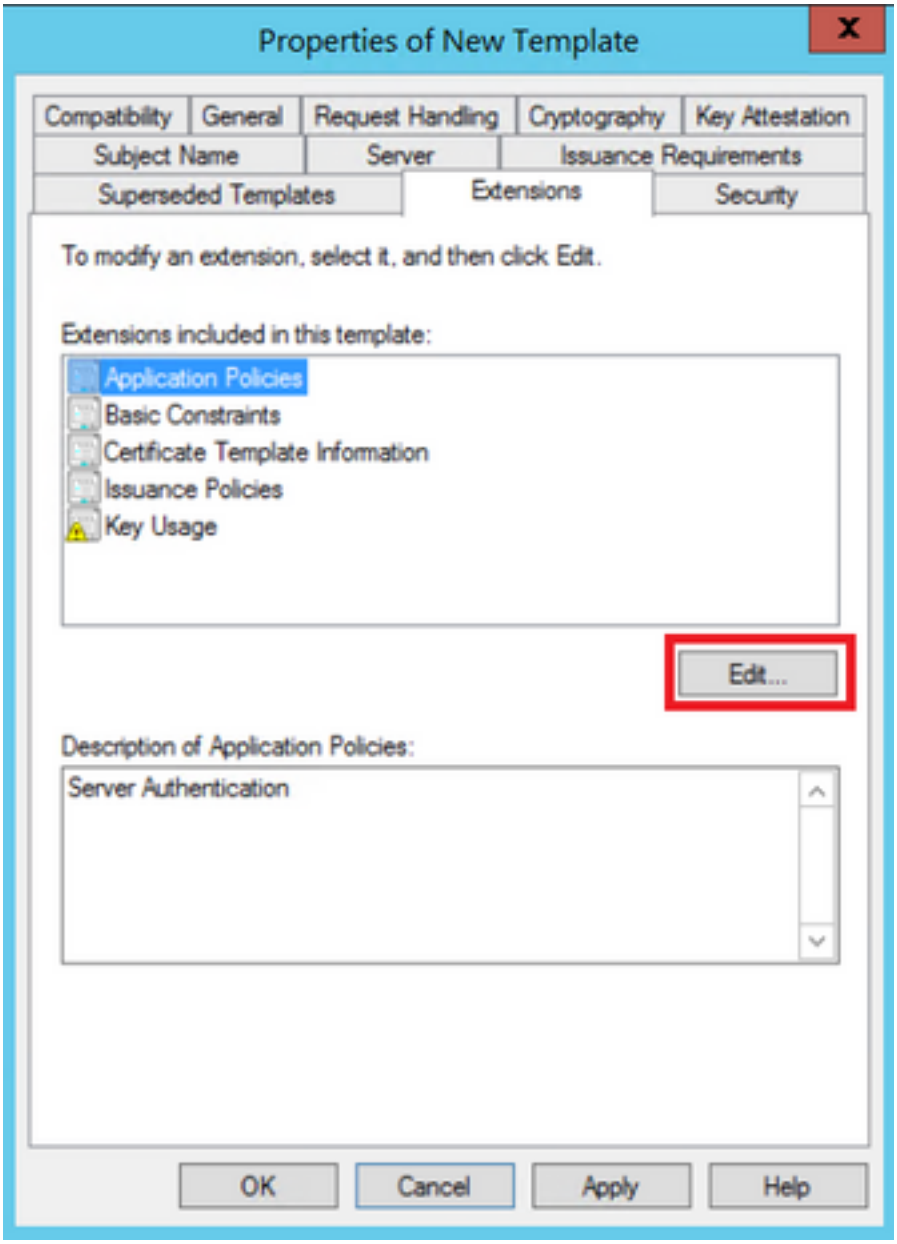


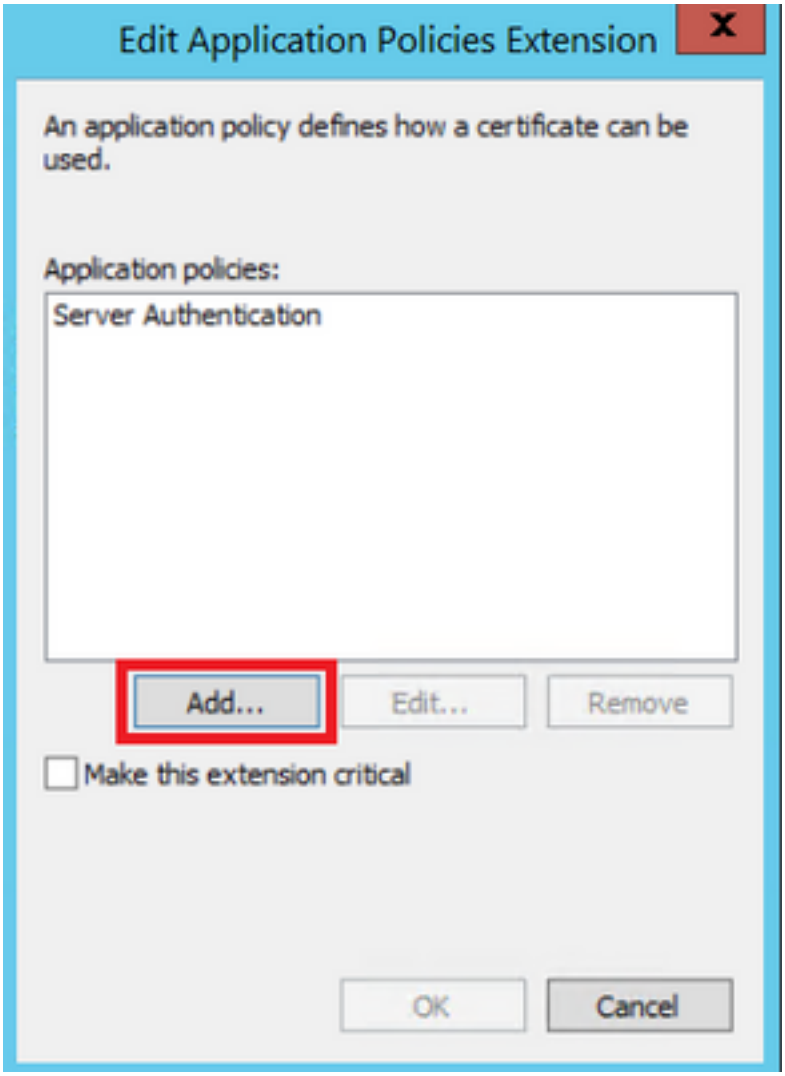
步驟4.選擇這些選項並選擇**確定**，如下圖所示。

- **數位簽章**
- **僅允許使用金鑰加密進行金鑰交換（金鑰加密）**
- **允許加密使用者資料**

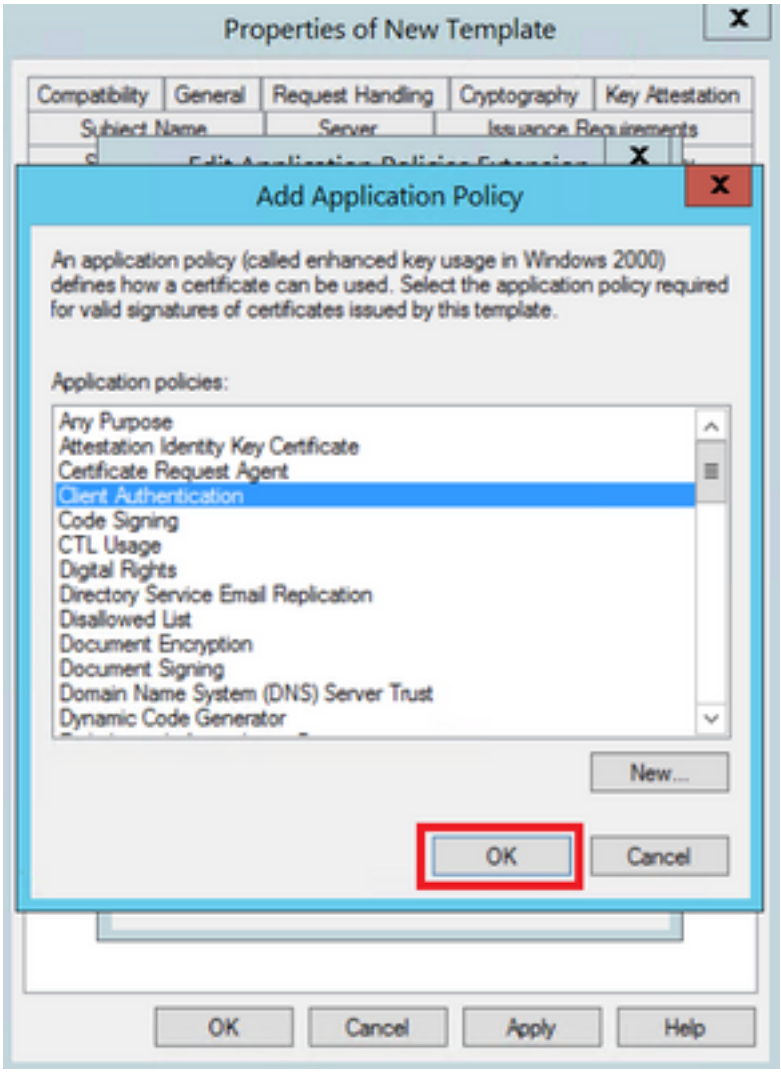


步驟5.導覽至**Extensions > Application Policies > Edit > Add**，如下圖所示。

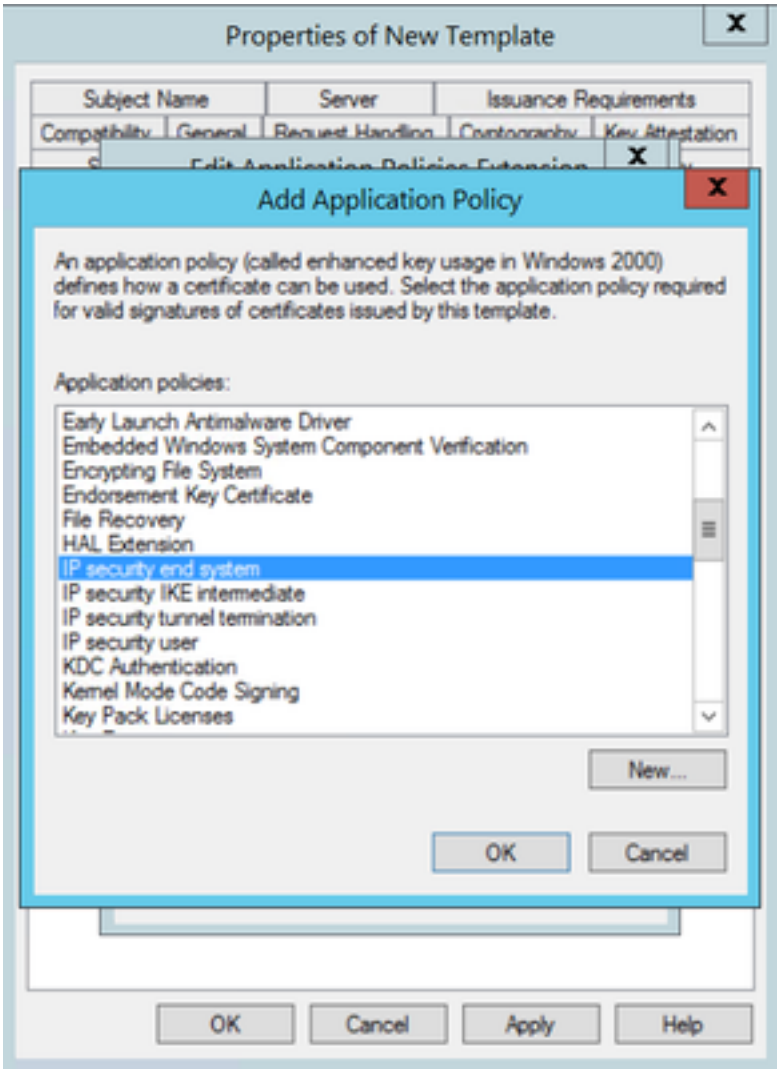

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Server Authentication
OK
Cancel
Apply
Help



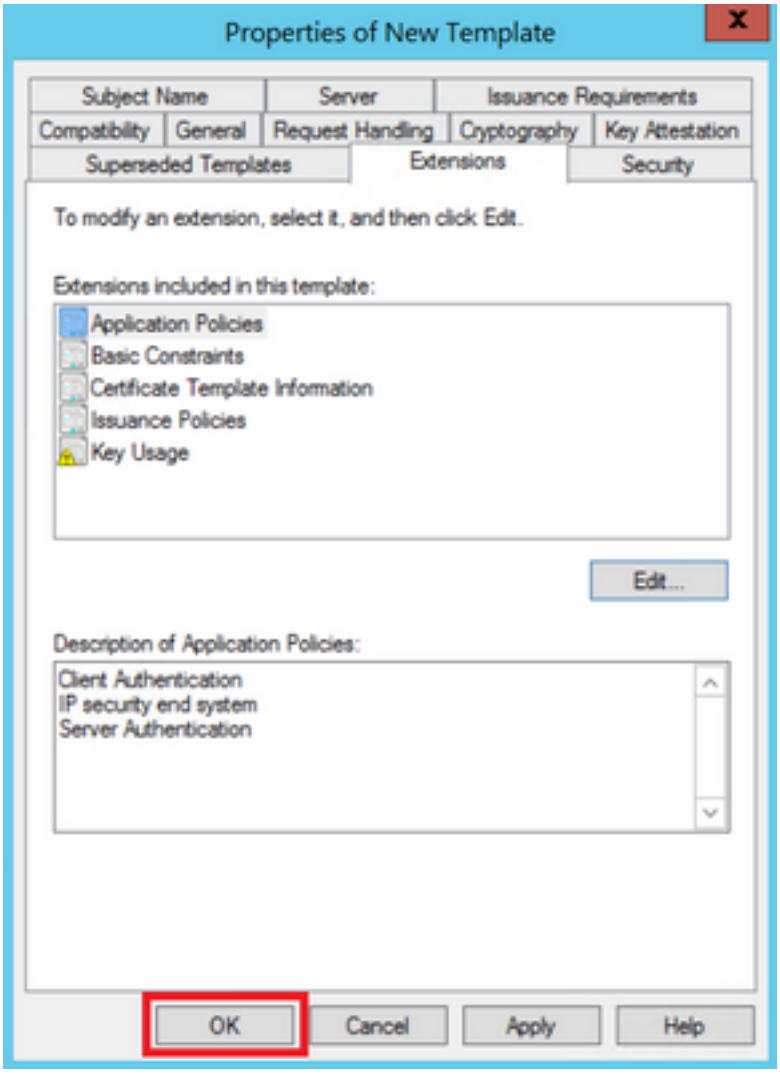
步驟6.搜尋Client Authentication，選擇它，然後OK，如下圖所示。



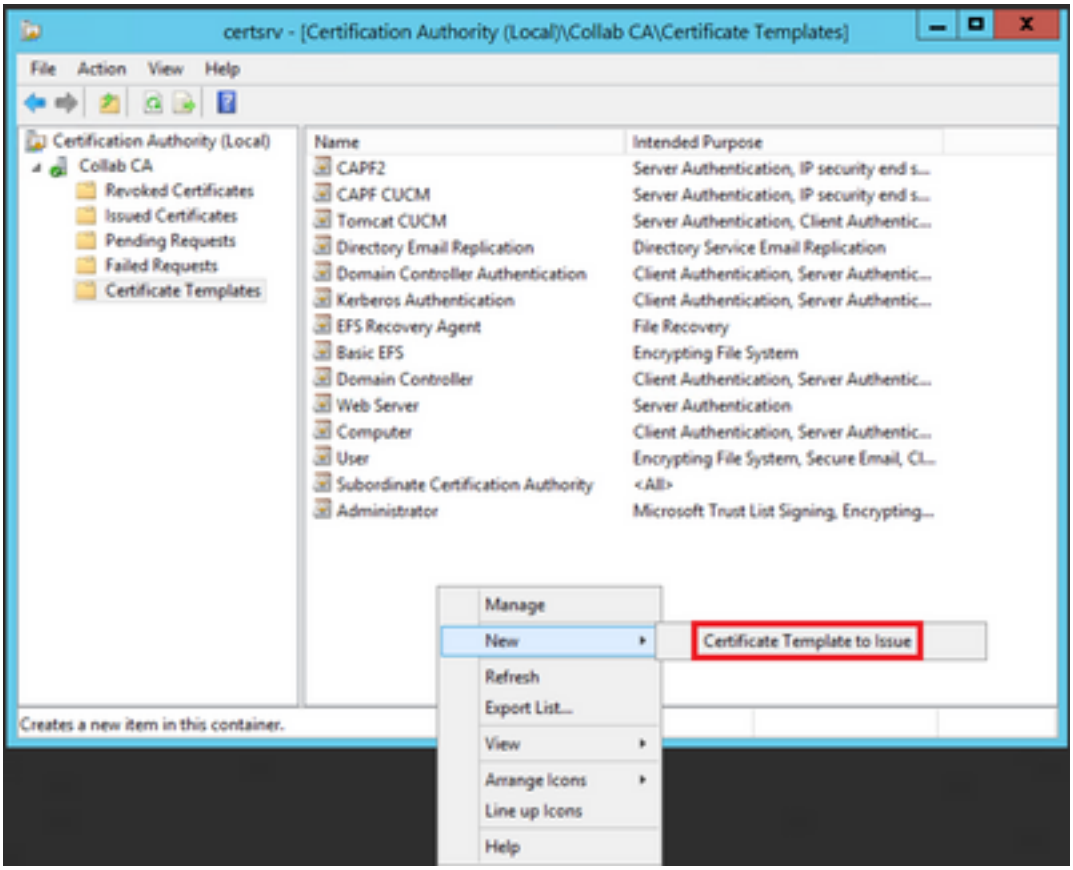
步驟7.再次選擇**Add**，搜尋**IP安全終端系統**，選擇它，然後在此視窗和上一個視窗中選擇**OK**。



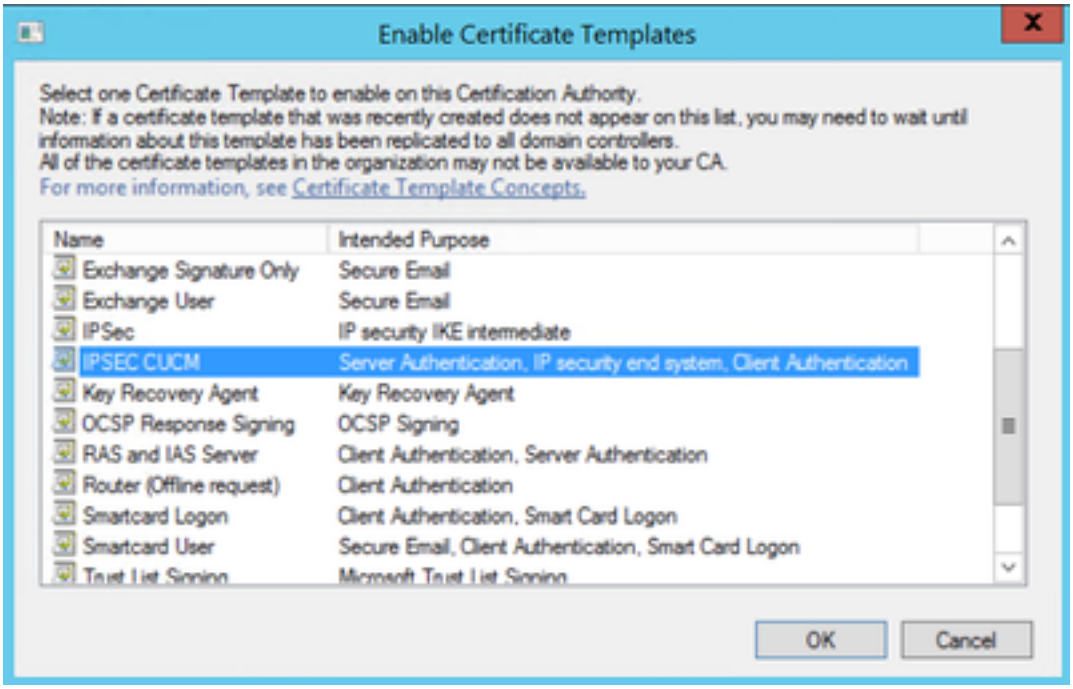
步驟8.回到模板上，選擇**Apply**，然後選擇**OK**，如下圖所示。



步驟9.關閉「Certificate Templates Console」視窗，然後在第一個視窗上導覽至New > Certificate Template to Issue，如下圖所示。

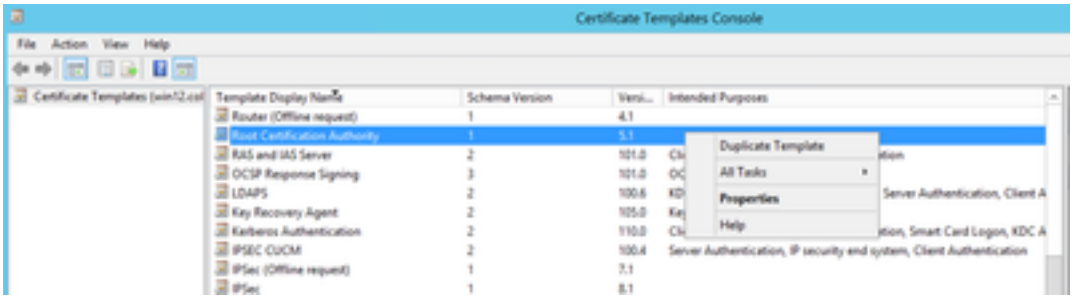


步驟10.選擇新的**IPSEC CUCM模**板，然後選擇**OK**，如下圖所示。



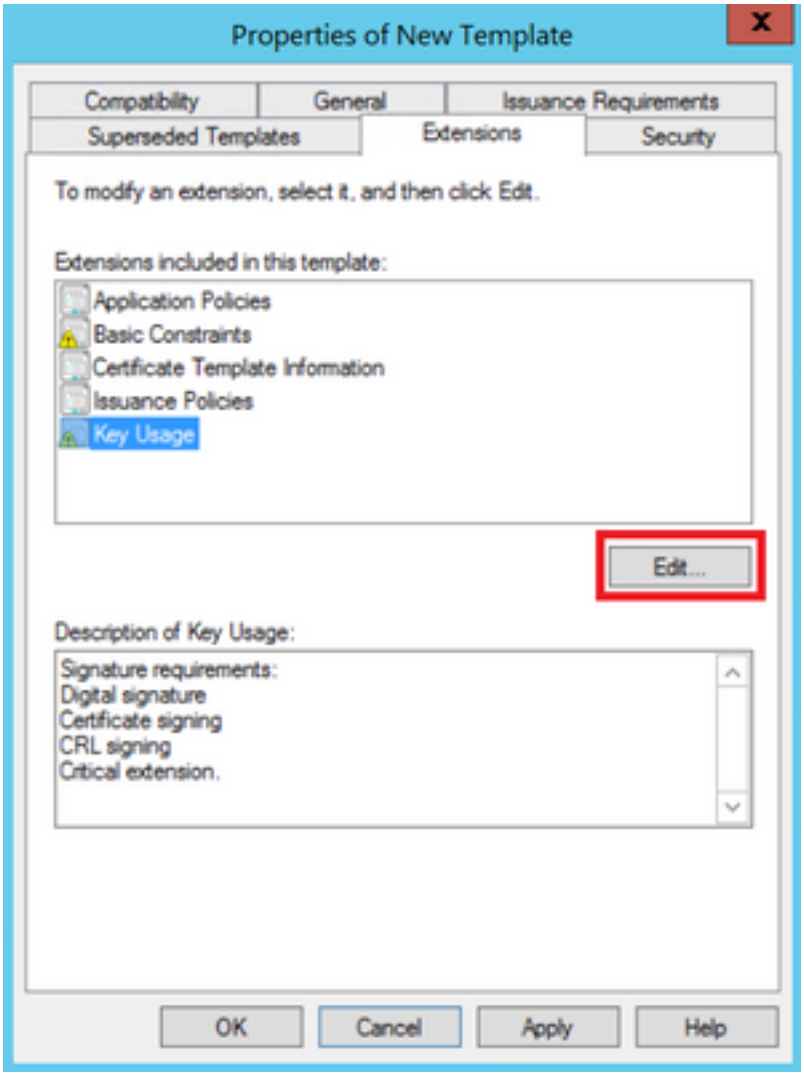
CAPF模板

步驟1.找到**根CA**模板，然後按一下右鍵該模板。然後選擇**Duplicate Template**，如下圖所示。



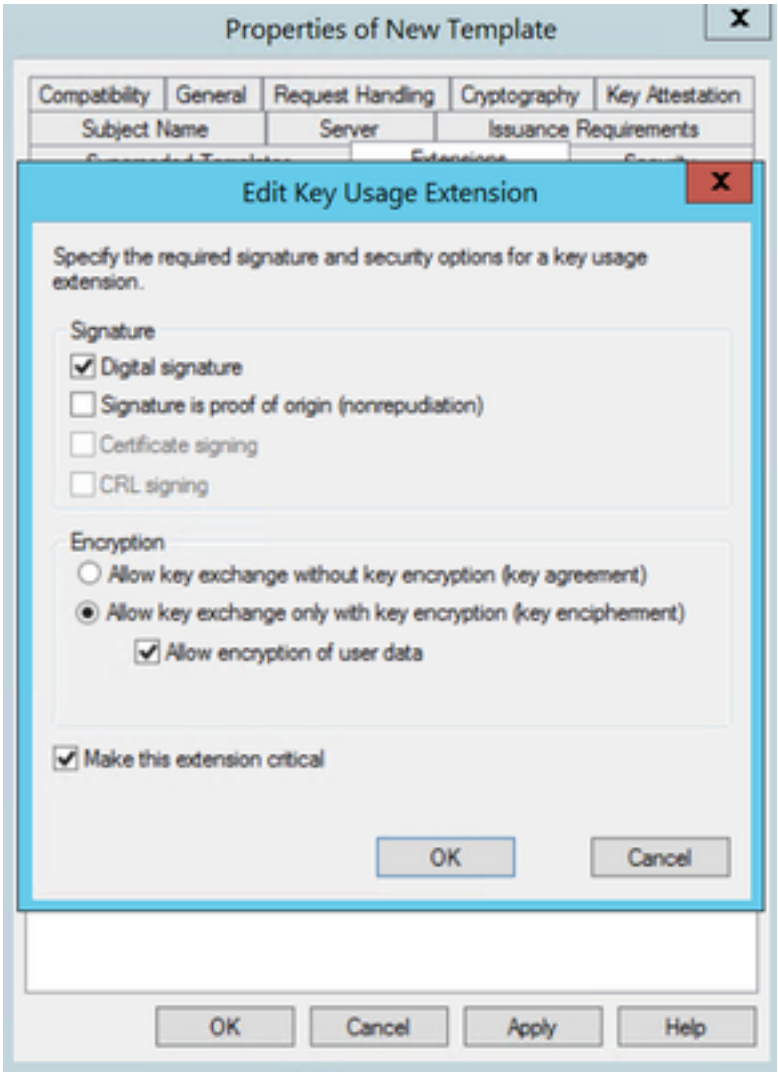
步驟2.在**General**下，您可以更改證書模板的名稱、顯示名稱、有效性等。

步驟3.導覽至**Extensions > Key Usage > Edit**，如下圖所示。

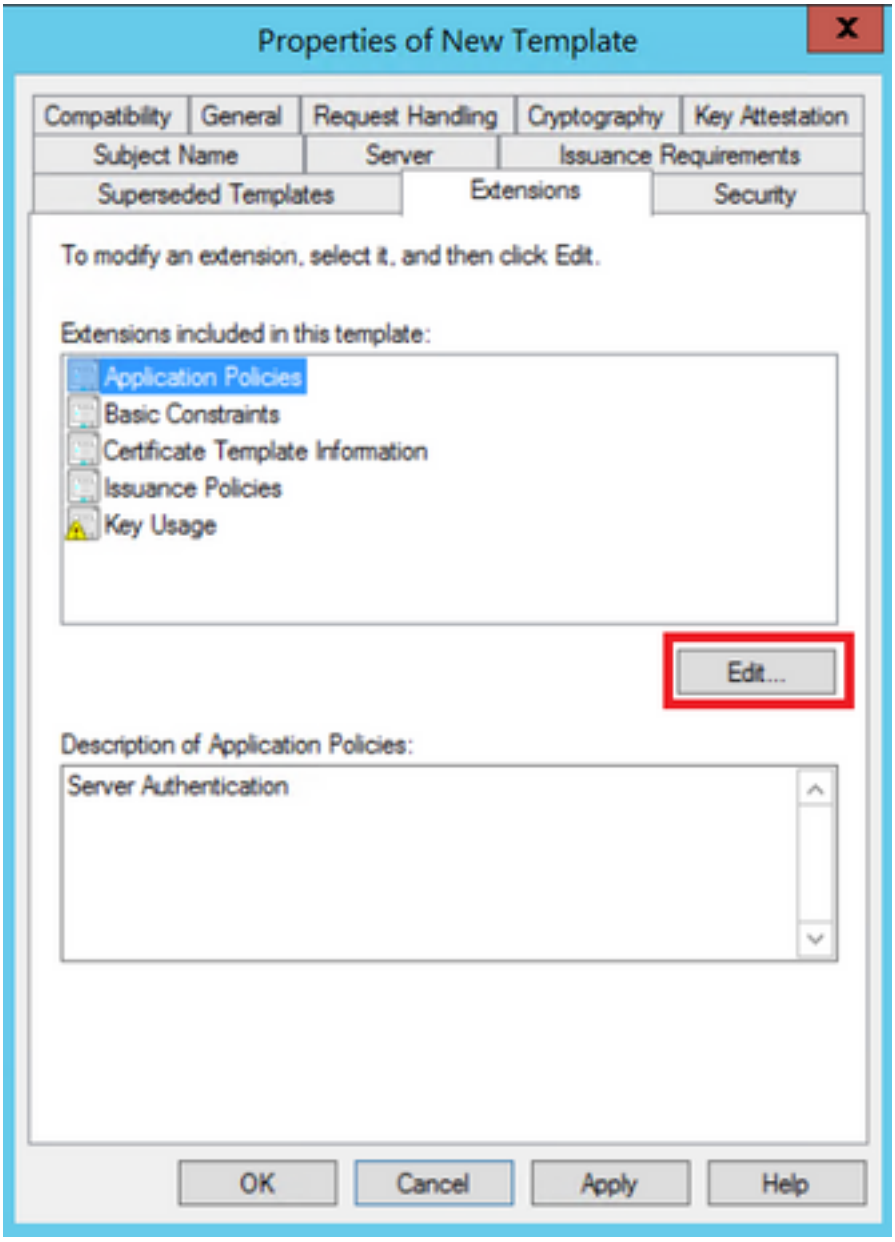


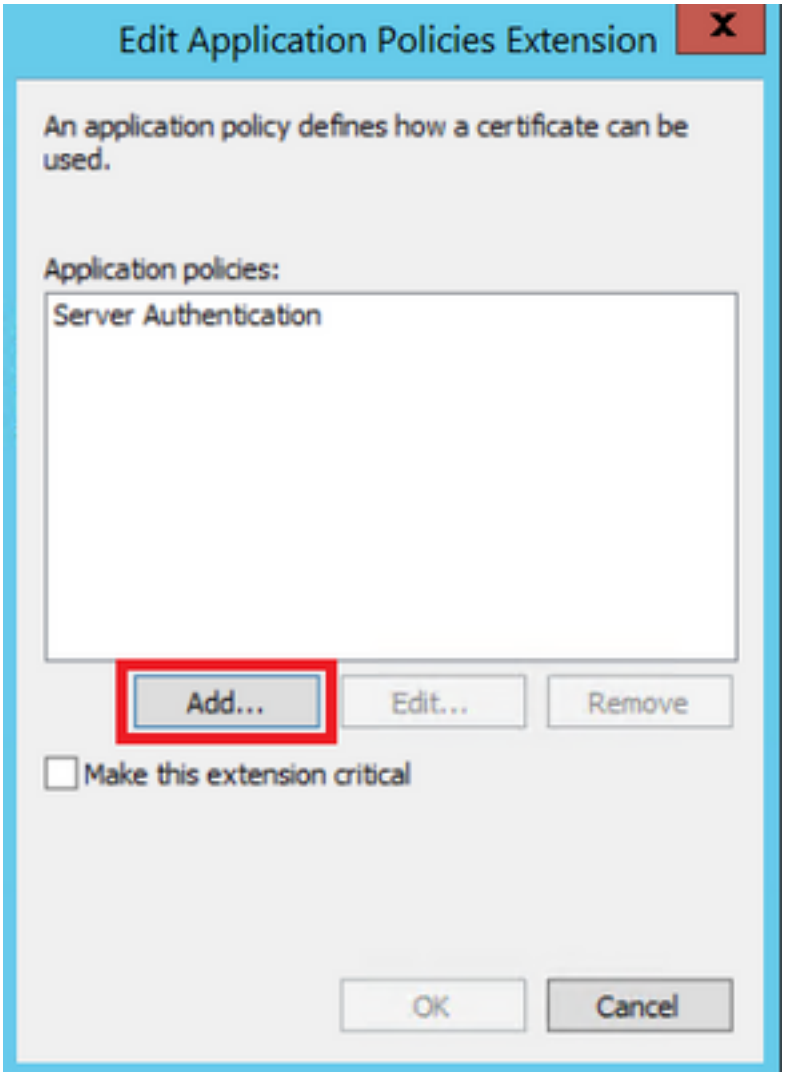
步驟4.選擇這些選項並選擇**確定**，如下圖所示。

- **數位簽章**
- **證書簽名**
- **CRL簽名**

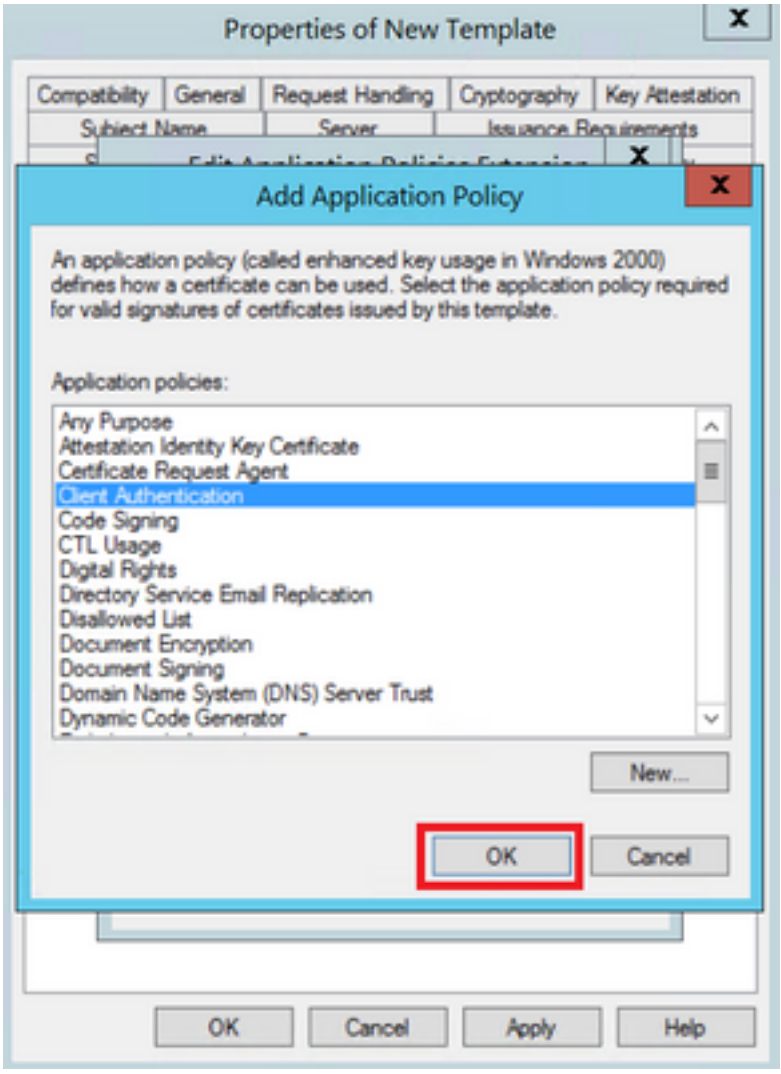


步驟5.導覽至**Extensions > Application Policies > Edit > Add**，如下圖所示。

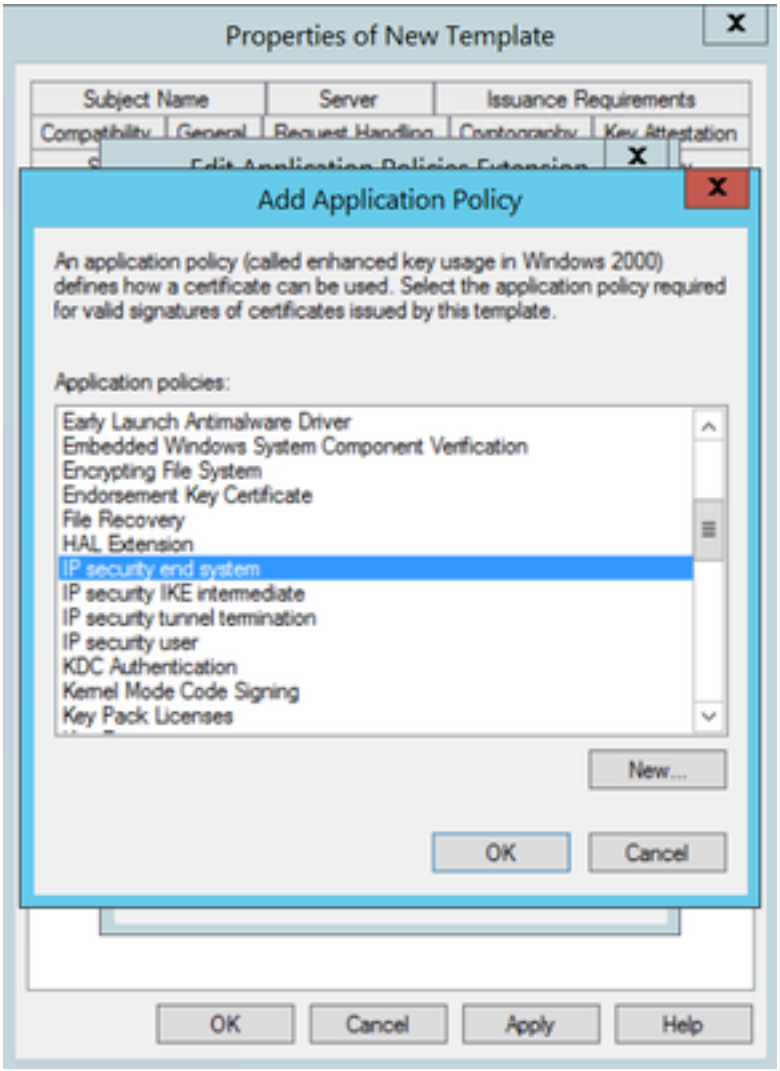

Properties of New Template
Compatibility
General
Request Handling
Cryptography
Key Attestation
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Server Authentication
OK
Cancel
Apply
Help



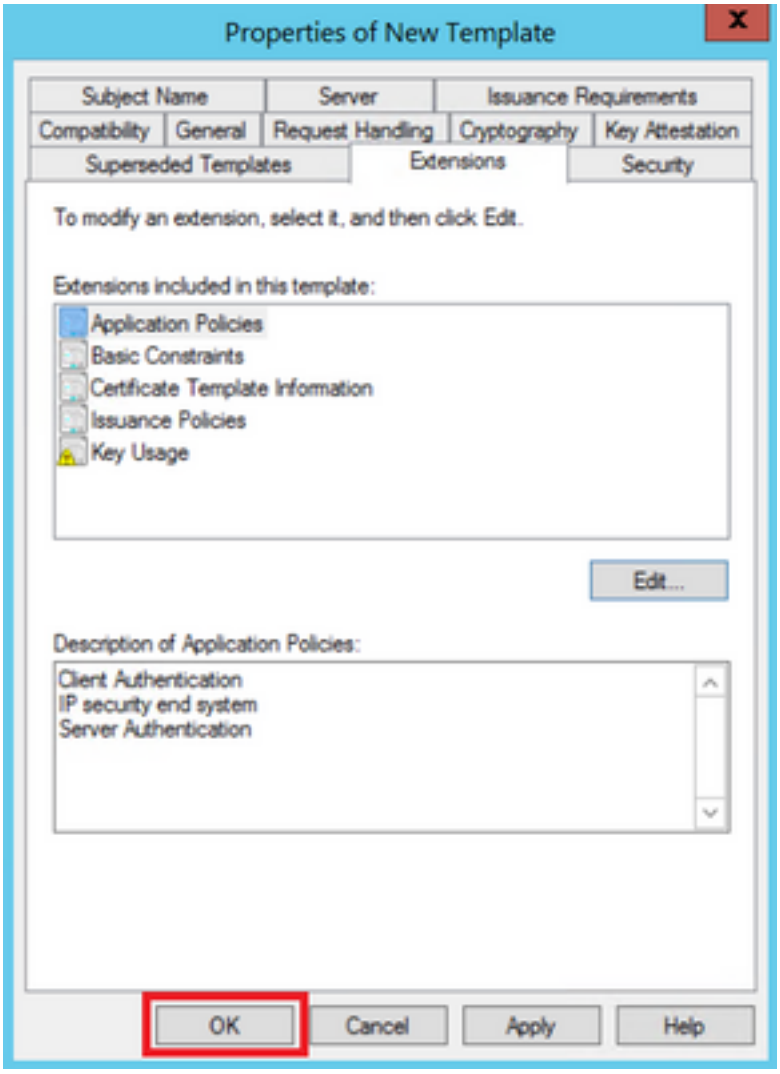
步驟6.搜尋Client Authentication，選擇它，然後選擇OK，如下圖所示。



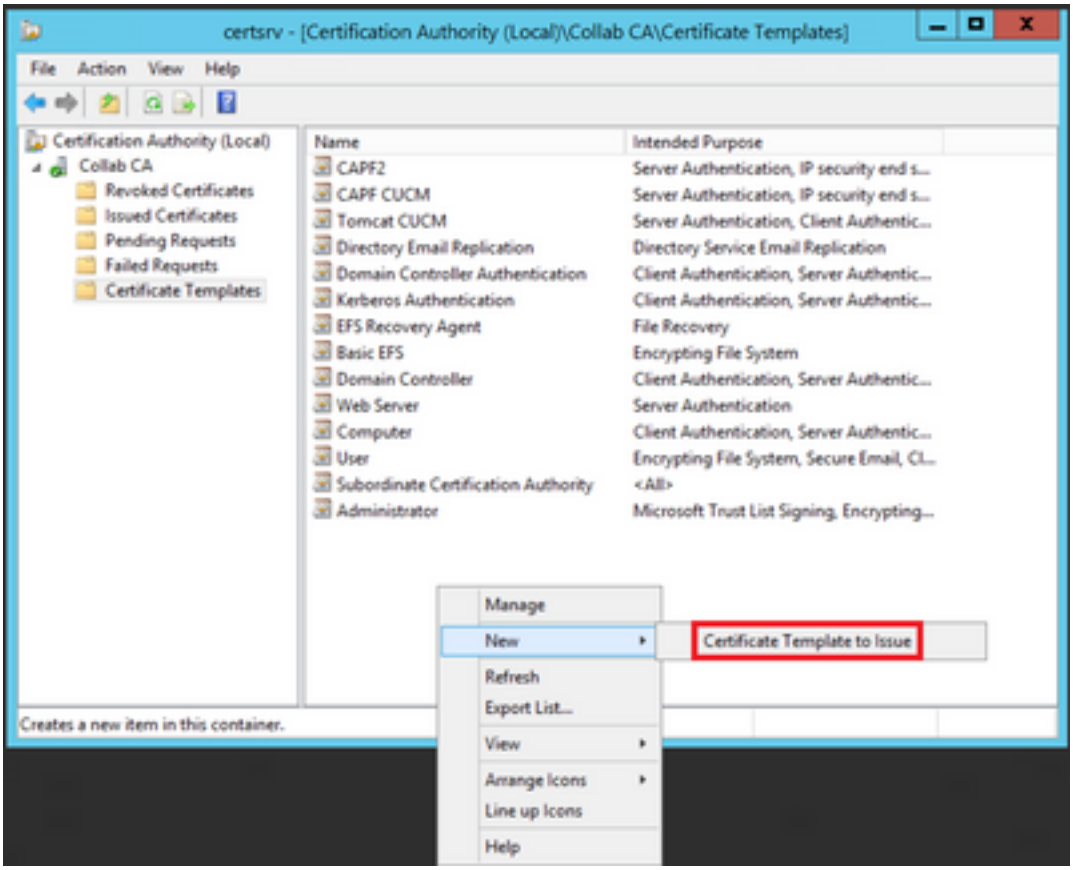
步驟7.再次選擇**Add**，搜尋**IP安全終端系統**，選擇它，然後在上面和本視窗中選擇OK，如下圖所示。



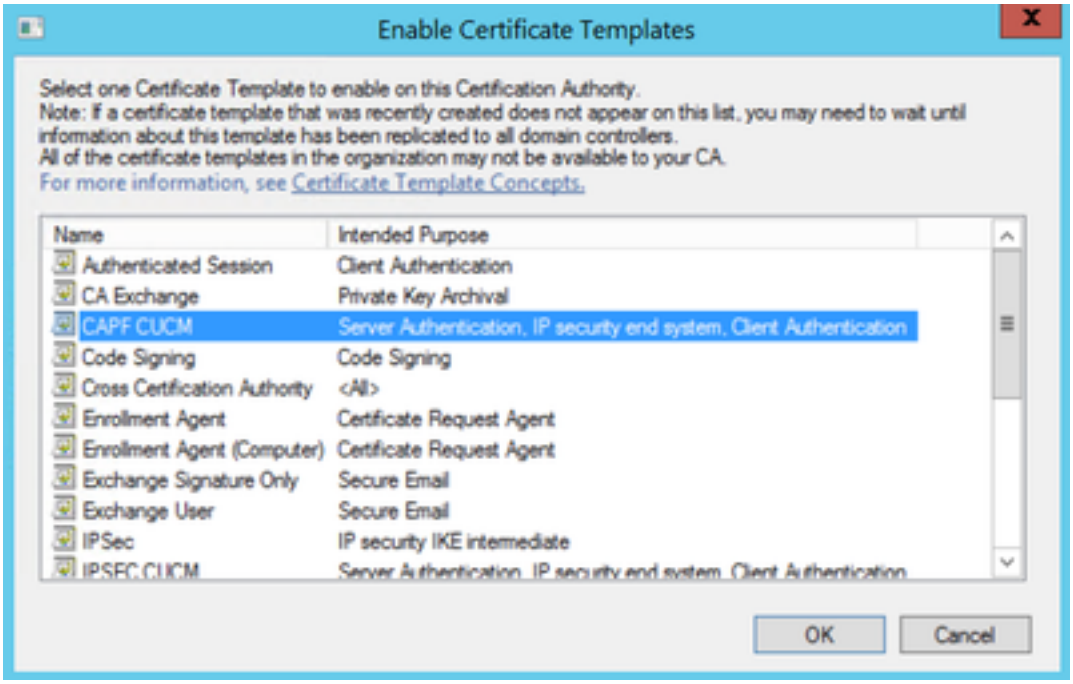
步驟8.回到模板上，選擇**Apply**，然後選擇**OK**，如下圖所示。



步驟9.關閉「Certificate Templates Console」視窗，然後在第一個視窗上導覽至New > Certificate Template to Issue，如下圖所示。



步驟10.選擇新的**CAPF CUCM模**板，然後選擇**OK**，如下圖所示。



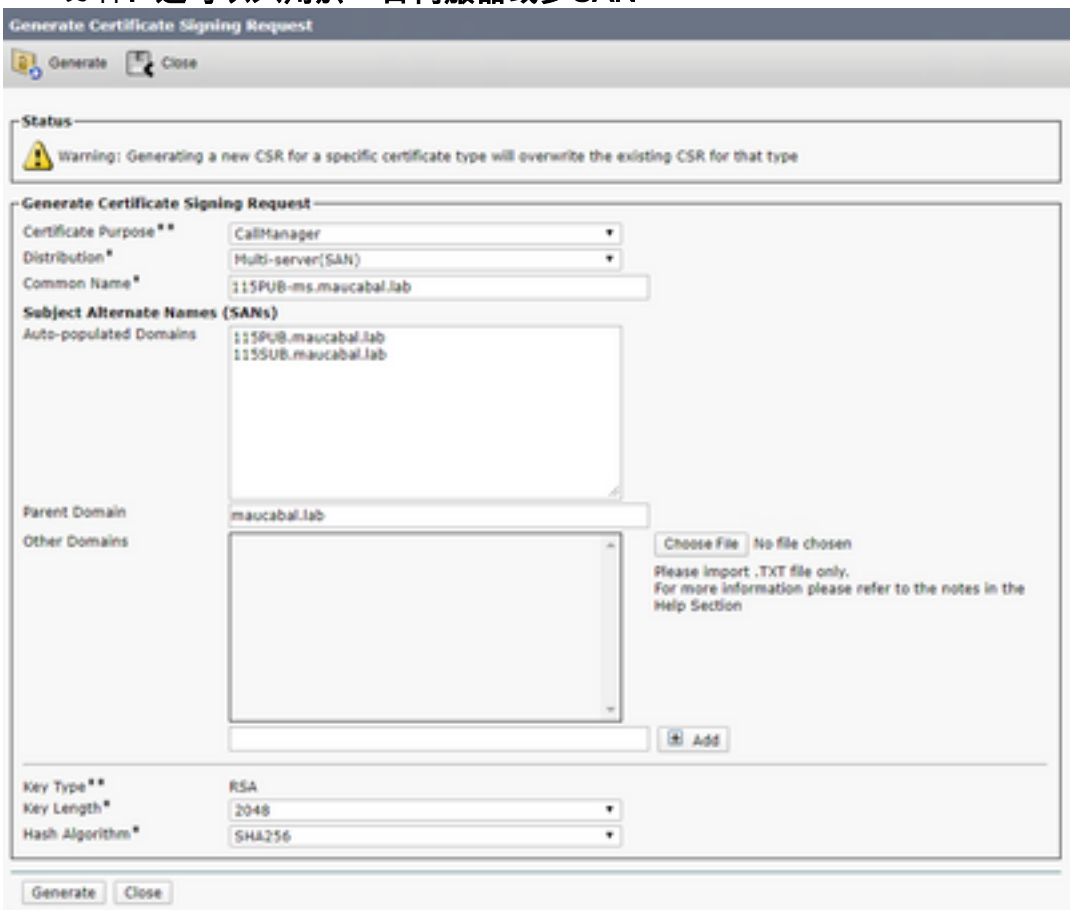
生成證書簽名請求

使用此示例可使用新建立的模板生成CallManager證書。相同的過程可用於任何證書型別，您只需要相應地選擇證書和模板型別：

步驟1.在CUCM上，導航到**OS Administration > Security > Certificate Management > Generate CSR**。

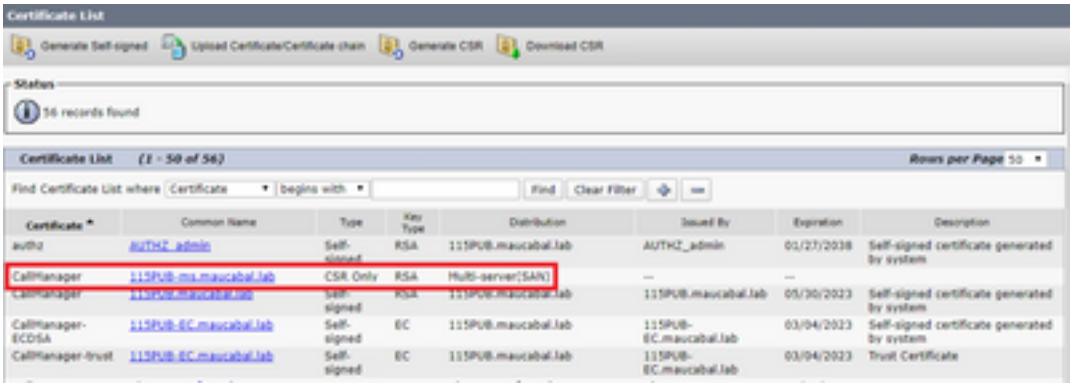
步驟2.選擇這些選項，然後選擇**Generate**，如下圖所示。

- 證書用途：CallManager
- 分佈:<這可以只用於一台伺服器或多SAN>

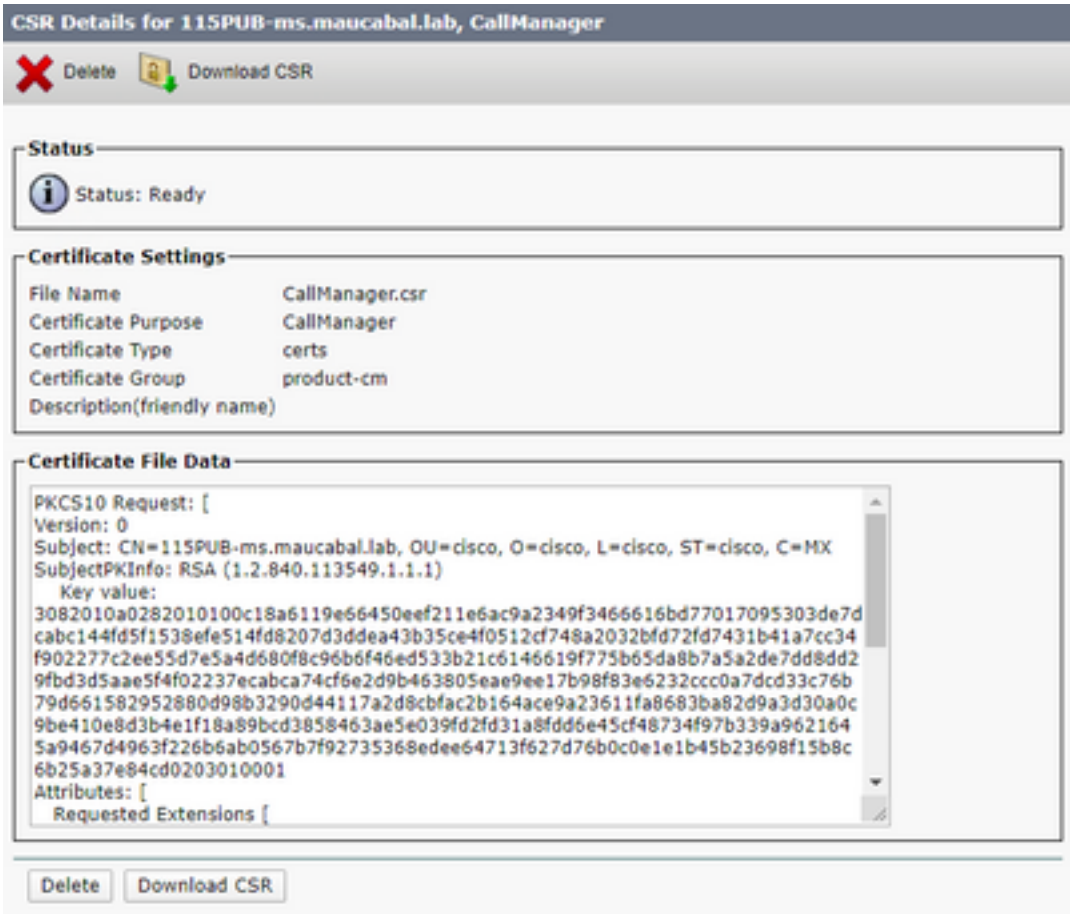


步驟3.系統生成確認消息，如下圖所示。

步驟4.在憑證清單上，尋找型別為CSR Only的專案，然後選擇它，如下圖所示。

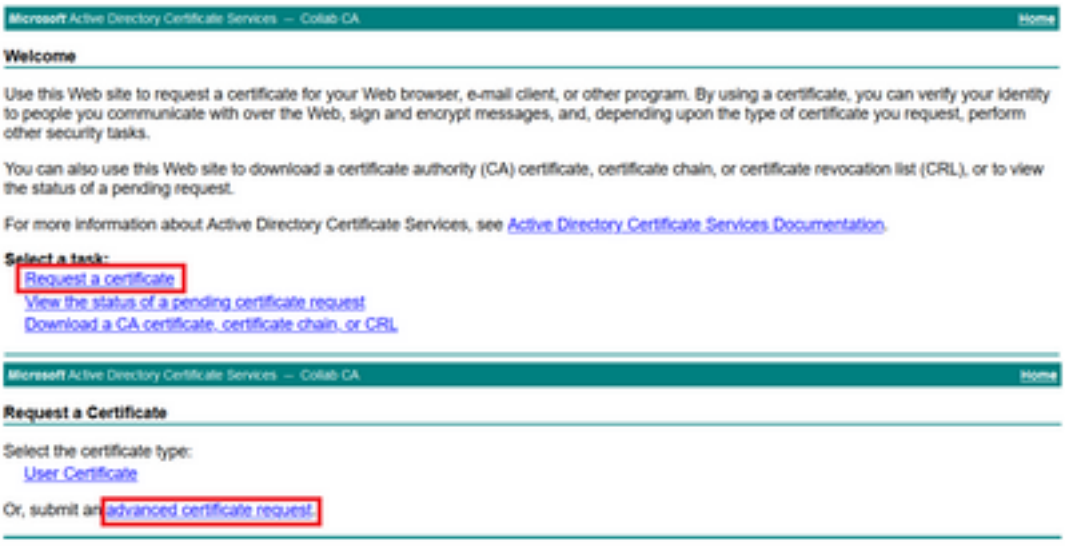


步驟5.在彈出視窗中，選擇Download CSR，然後將檔案儲存到您的電腦上。

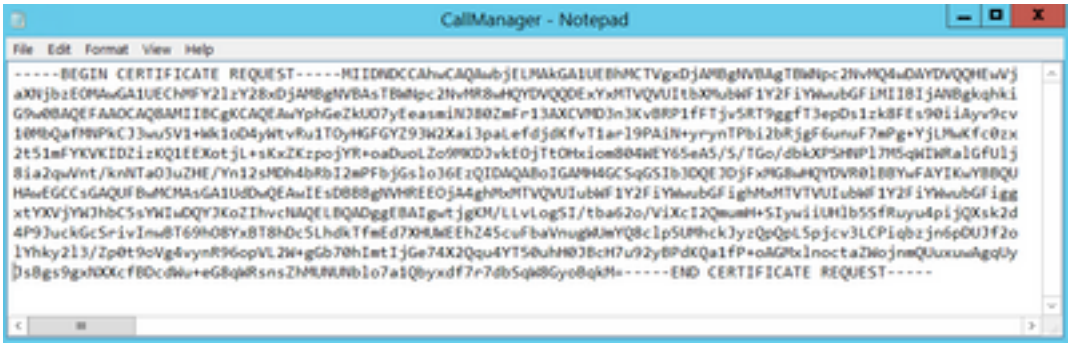


步驟6.在瀏覽器上，導航到此URL，然後輸入域控制器管理員憑據：**https://<yourWindowsServerIP>/certsrv/**。

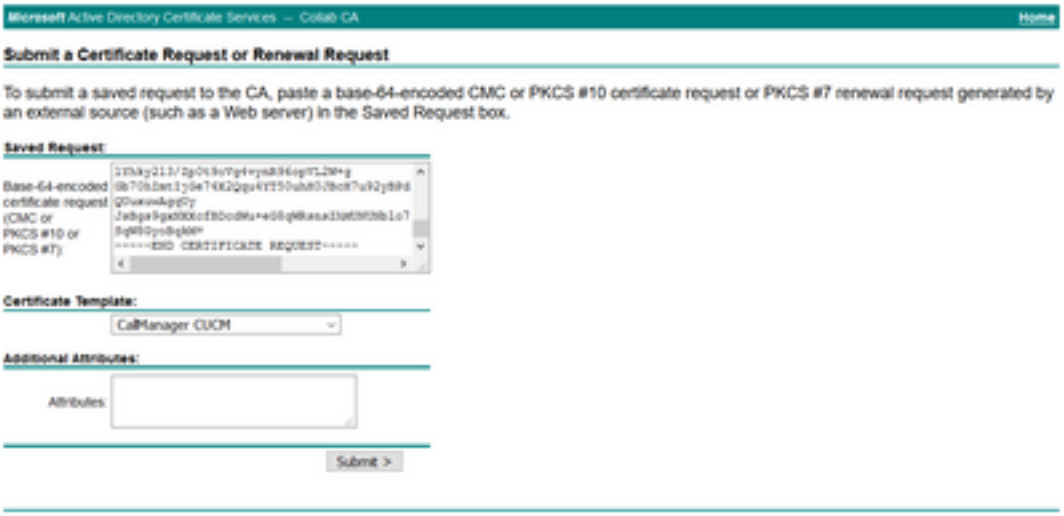
步驟7.導覽至**Request a certificate > advanced certificate request**，如下圖所示。



步驟8.開啟CSR檔案並複製其所有內容：



步驟9.將CSR貼上到**Base-64-encoded certificate request欄位**中。在**Certificate Template**下，選擇正確的模板，然後選擇**Submit**，如下圖所示。



步驟10.最後，選擇**Base 64 encoded**和**Download certificate chain**，現在可以將生成的檔案上傳到CUCM。

驗證

驗證過程實際上是配置過程的一部分。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

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）。