

為BYOD配置ISE SCEP支援

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[測試的CA/NDES部署方案](#)

[獨立部署](#)

[分散式部署](#)

[重要的Microsoft修補程式](#)

[重要的BYOD埠和協定](#)

[設定](#)

[禁用SCEP註冊質詢密碼要求](#)

[將SCEP註冊限制為已知ISE節點](#)

[擴展IIS中的URL長度](#)

[證書模板概述](#)

[證書模板配置](#)

[證書模板登錄檔配置](#)

[將ISE配置為SCEP代理](#)

[驗證](#)

[疑難排解](#)

[一般疑難排解說明](#)

[客戶端日誌記錄](#)

[ISE記錄](#)

[NDES日誌記錄和故障排除](#)

[相關資訊](#)

簡介

本文說明成功配置思科身份識別服務引擎(ISE)上自帶裝置(BYOD)的Microsoft網路裝置註冊服務(NDES)和簡單證書註冊協定(SCEP)的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- ISE版本1.1.1或更高版本
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012標準版

- 公開金鑰基礎架構(PKI)和憑證

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ISE版本1.1.1或更高版本
- 安裝了KB2483564和KB2633200修補程式的Windows Server 2008 R2 SP1
- Windows Server 2012標準版

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

與Microsoft證書服務相關的資訊是作為思科BYOD專用指南提供的。請參閱Microsoft TechNet作為Microsoft證書頒發機構、網路裝置註冊服務(NDES)和SCEP相關伺服器配置的最終資料來源。

背景資訊

思科支援ISE的自帶裝置實施的一個優勢是終端使用者能夠執行自助裝置註冊。這消除了IT分發身份驗證憑證和啟用網路上的裝置的管理負擔。BYOD解決方案的核心是網路請求方調配流程，該流程旨在將所需的證書分發給員工所有的裝置。為了滿足此要求，可以配置Microsoft證書頒發機構(CA)，以便使用SCEP自動完成證書註冊流程。

SCEP在虛擬專用網路(VPN)環境中已使用多年，目的是簡化證書註冊以及向遠端訪問客戶端和路由器的分發。在Windows 2008 R2伺服器上啟用SCEP功能需要安裝NDES。在NDES角色安裝期間，還將安裝Microsoft Internet Information Services(IIS)Web伺服器。IIS用於終止CA和ISE策略節點之間的HTTP或HTTPS SCEP註冊請求和響應。

NDES角色可以安裝在當前CA上，也可以安裝在成員伺服器上。在獨立部署中，NDES服務安裝在包含證書頒發機構服務和（可選）證書頒發機構Web註冊服務的現有CA上。在分散式部署中，NDES服務安裝在成員伺服器上。然後配置分散式NDES伺服器以便與上游根或子根CA通訊。在此案例中，本文檔中概述的登錄檔修改是使用自定義模板在NDES伺服器上進行的，其中證書位於上游CA上。

測試的CA/NDES部署方案

本節簡要概述在Cisco實驗室中測試的CA/NDES部署方案。請參閱Microsoft TechNet作為Microsoft CA、NDES和SCEP相關伺服器配置的最終資料來源。

獨立部署

在概念驗證(PoC)場景中使用ISE時，通常部署自包含Windows 2008或2012電腦，該電腦充當Active Directory(AD)域控制器、根CA和NDES伺服器：



- Domain Controller
- AD
- Root CA
- NDES

分散式部署

當ISE整合到當前的Microsoft AD/PKI生產環境時，更常見的是服務分佈在多個不同的Windows 2008或2012伺服器上。思科已測試兩種分散式部署方案。

此圖說明第一個經測試的分散式部署方案：



- Domain Controller
- AD
- Root CA



- Member Server
- Subordinate CA
- NDES

此圖說明了第二個分散式部署的測試場景：



- Domain Controller
- AD
- Root CA



- Member Server
- Subordinate CA



- Member Server
- NDES

重要的Microsoft修補程式

在為BYOD配置SCEP支援之前，請確保Windows 2008 R2 NDES伺服器已安裝以下Microsoft修補程式：

- [如果使用NDES管理證書，則Windows Server 2008 R2中SCEP證書的續訂請求失敗 — 出現此問題](#)，因為NDES不支援GetCACaps操作。
- [在Windows Server 2008 R2中重新啟動企業CA後，NDES不提交證書請求](#) — 此消息顯示在事件查看器中："網路裝置註冊服務無法提交證書請求(800706x.ba)。RPC伺服器不可用。"

警告：配置Microsoft CA時，必須瞭解ISE不支援RSASSA-PSS簽名演算法。思科建議您配置CA策略，以便改用sha1WithRSAEncryption或sha256WithRSAEncryption。

重要的BYOD埠和協定

以下是重要BYOD埠和協定的清單：

- TCP:8909調配：從思科ISE(Windows和Macintosh作業系統(OS))進行嚮導安裝
- TCP:443調配：從Google Play(Android)安裝嚮導
- TCP:8905調配：請求方調配流程
- TCP:80或TCP:443 SCEP代理到CA (基於SCEP RA URL配置)

附註：有關所需埠和協定的最新清單，請參閱ISE 1.2 [Hardware Installation Guide](#)。

設定

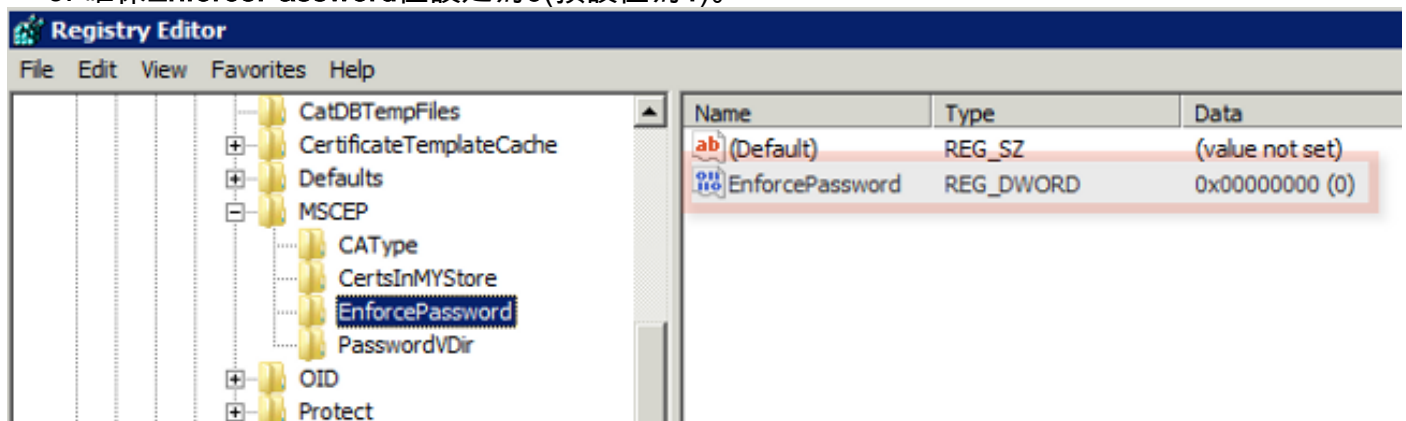
使用本節可配置對ISE上的BYOD的NDES和SCEP支援。

禁用SCEP註冊質詢密碼要求

預設情況下，Microsoft SCEP(MSCEP)實現使用動態質詢密碼，以便在證書註冊過程中對客戶端和終端進行身份驗證。有了此配置要求，您必須瀏覽到NDES伺服器上的MSCEP管理Web GUI，以便按需生成密碼。您必須將此密碼作為註冊請求的一部分。

在BYOD部署中，要求使用質詢密碼會妨礙使用者自助服務解決方案的用途。若要移除此要求，您必須修改NDES伺服器上的此登錄檔項：

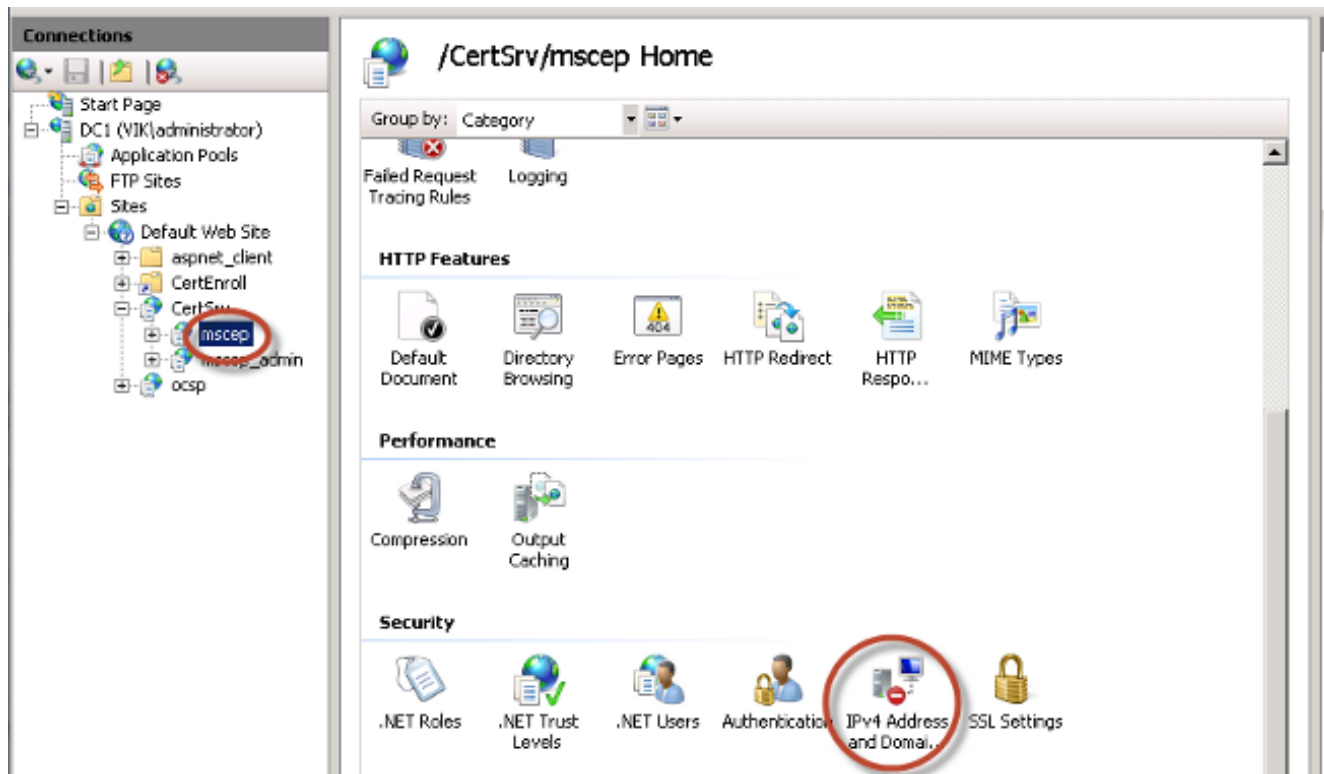
1. 按一下**Start**，然後在搜尋欄中輸入**regedit**。
2. 導航到Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword。
3. 確保EnforcePassword值設定為0(預設值為1)。



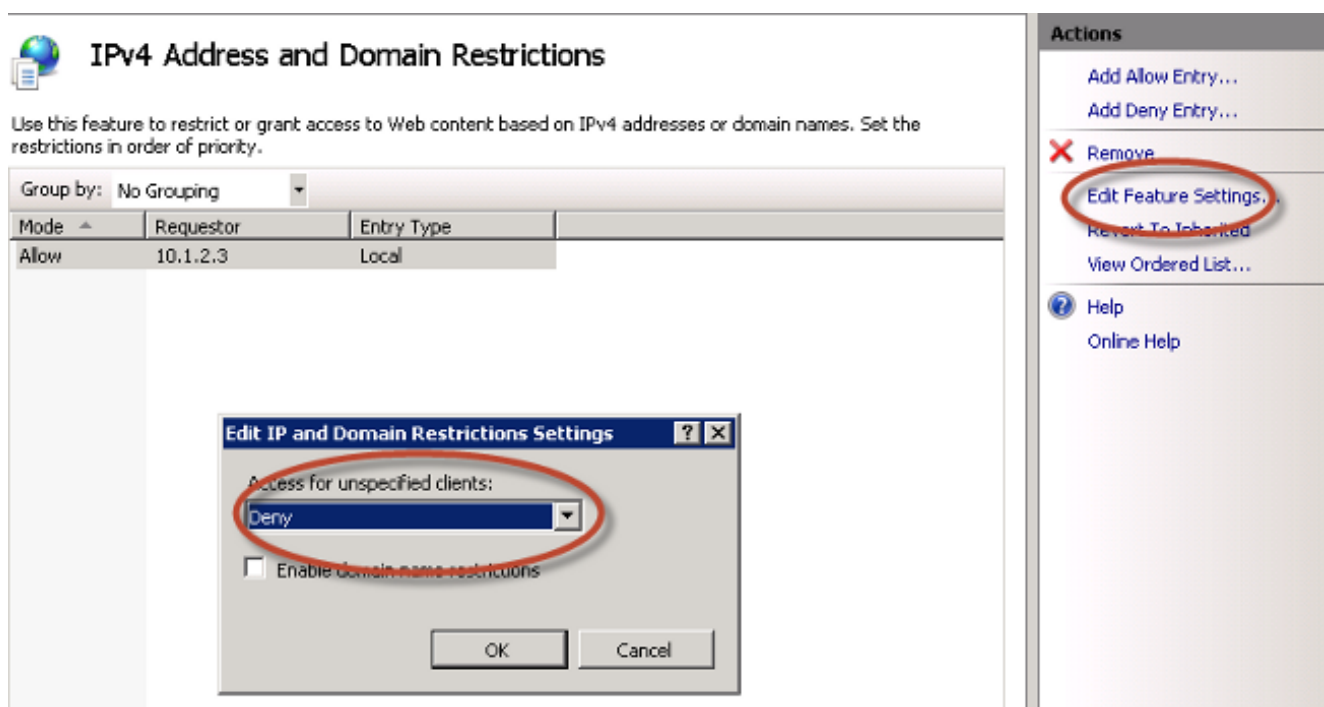
將SCEP註冊限制為已知ISE節點

在某些部署方案中，最好將SCEP通訊限制在已知ISE節點的選定清單中。這可以通過IIS中的IPv4地址和域限制功能來實現：

1. 開啟IIS並導航到/CertSrv/mscep網站。



- 按兩下 **Security > IPv4地址和域限制**。使用 **Add Allow Entry** 和 **Add Deny Entry** 操作可根據 ISE 節點 IPv4 地址或域名允許或限制對 Web 內容的訪問。使用 **Edit Feature Settings** 操作可為未指定的客戶端定義預設訪問規則。

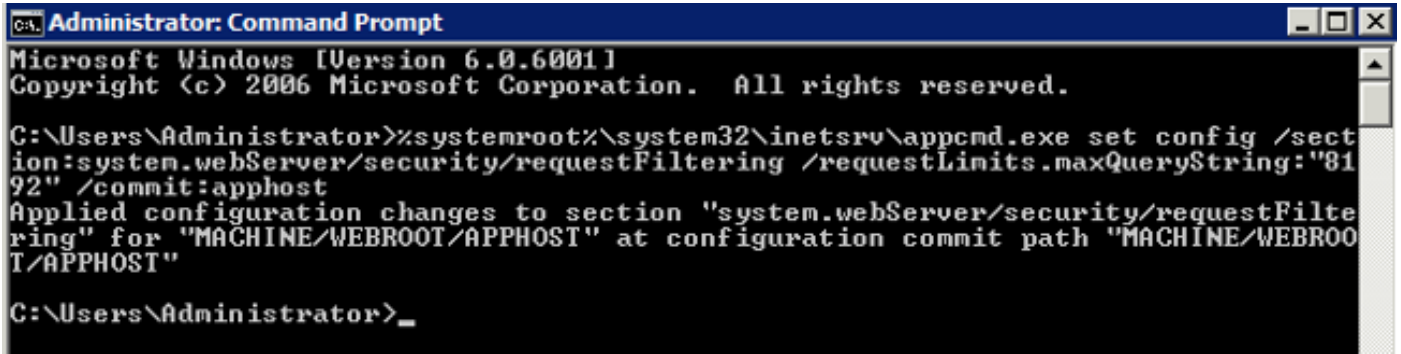


擴展 IIS 中的 URL 長度

ISE 可能會生成對 IIS Web 伺服器來說太長的 URL。為了避免此問題，可以修改預設 IIS 配置以允許使用更長的 URL。從 NDES 伺服器 CLI 輸入以下命令：

```
%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/
security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost
```


附註：查詢字串大小可能取決於ISE和終端配置。從具有管理許可權的NDES伺服器CLI輸入此命令。



```
C:\Users\Administrator>%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost
Applied configuration changes to section "system.webServer/security/requestFiltering" for "MACHINE/WEBROOT/APPHOST" at configuration commit path "MACHINE/WEBROOT/APPHOST"
C:\Users\Administrator>_
```

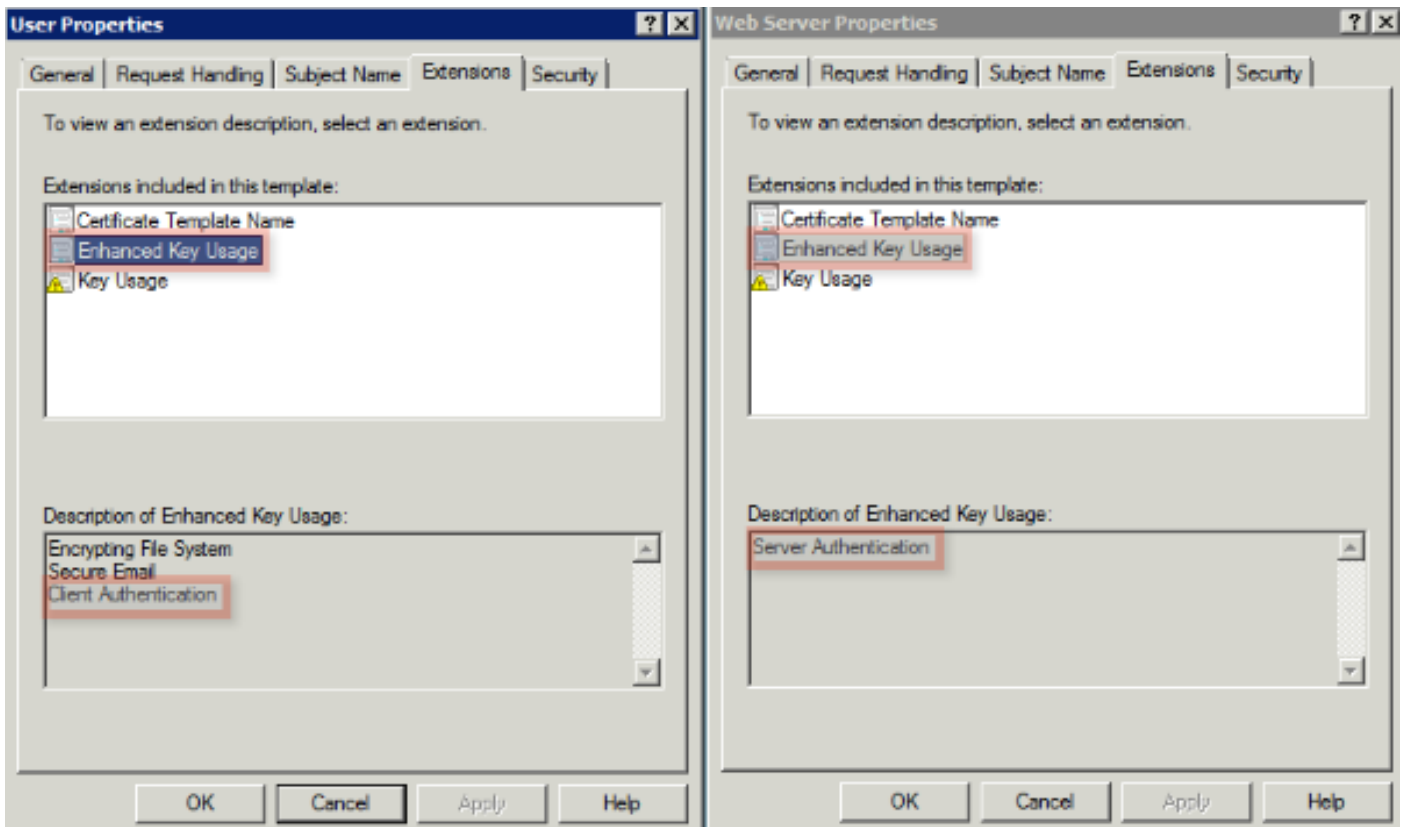
證書模板概述

Microsoft CA的管理員可以配置一個或多個模板，這些模板用於將應用程式策略應用於一組通用的證書。這些策略有助於確定使用證書和相關金鑰的功能。應用策略值包含在證書的Extended Key Usage(EKU)欄位中。驗證器解析EKU欄位中的值，以確保客戶端提供的證書可用於預期功能。一些更常見的使用包括伺服器身份驗證、客戶端身份驗證、IPSec VPN和電子郵件。在ISE方面，更常用的EKU值包括伺服器和/或客戶端身份驗證。

例如，當您瀏覽到安全的銀行網站時，處理請求的Web伺服器會使用具有伺服器身份驗證的應用策略的證書進行配置。當伺服器收到HTTPS要求時，會傳送伺服器驗證憑證到連線的Web瀏覽器以進行驗證。這裡的重要一點是，這是從伺服器到客戶端的單向交換。與ISE相關，伺服器身份驗證證書的一個常見用途是管理員GUI訪問。ISE將已配置的證書傳送到連線的瀏覽器，並不期望從客戶端收到證書。

對於使用EAP-TLS的BYOD等服務，首選相互身份驗證。要啟用此雙向證書交換，用於生成ISE身份證書的模板必須擁有最低的應用策略伺服器身份驗證。Web伺服器證書模板滿足此要求。生成終端證書的證書模板必須包含客戶端身份驗證的最低應用策略。使用者證書模板滿足此要求。如果為Inline Policy Enforcement Point(iPEP)等服務配置ISE，則用於生成ISE伺服器身份證書的模板應包含客戶端和伺服器身份驗證屬性（如果使用ISE版本1.1.x或更低版本）。這允許管理員節點和內聯節點相互進行身份驗證。ISE版本1.2刪除了針對iPEP的EKU驗證，使得此要求變得無關緊要。

您可以重複使用預設的Microsoft CA Web Server和使用者模板，也可以使用本文檔中概述的流程克隆並建立新模板。根據這些證書要求，應仔細規劃CA配置以及產生的ISE和終端證書，以便在安裝到生產環境中時將任何不需要的配置更改降至最低。



證書模板配置

如簡介中所述，SCEP在IPSec VPN環境中得到了廣泛的應用。因此，安裝NDES角色會自動配置伺服器以使用SCEP的IPSec(離線請求)模板。因此，為BYOD準備Microsoft CA的第一步之一是使用正確的應用程式策略構建新模板。在獨立部署中，證書頒發機構和NDES服務配置在同一伺服器上，並且模板和所需的登錄檔修改包含在同一伺服器上。在分散式NDES部署中，在NDES伺服器上進行登錄檔修改；但是，實際模板是在NDES服務安裝中指定的根或子根CA伺服器上定義的。

完成以下步驟以設定憑證模板：

1. 以admin身份登入CA伺服器。
2. 按一下**開始 > 管理工具 > 證書頒發機構**。
3. 展開CA伺服器詳細資訊並選擇**Certificate Templates**資料夾。此資料夾包含當前啟用的模板清單。
4. 要管理證書模板，請按一下右鍵**Certificate Templates**資料夾並選擇**Manage**。
5. 在**Certificate Templates Console**中，會顯示許多非活動模板。
6. 要配置用於SCEP的新模板，請按一下右鍵已經存在的模板(例如User)，然後選擇**Duplicate Template**。
7. 選擇**Windows 2003**或**Windows 2008**，具體取決於環境中的最低CA作業系統。
8. 在**General**頁籤上，新增顯示名稱(例如ISE-BYOD)和有效期；取消選中所有其他選項。
附註：模板有效期必須小於或等於CA根證書和中間證書的有效期。

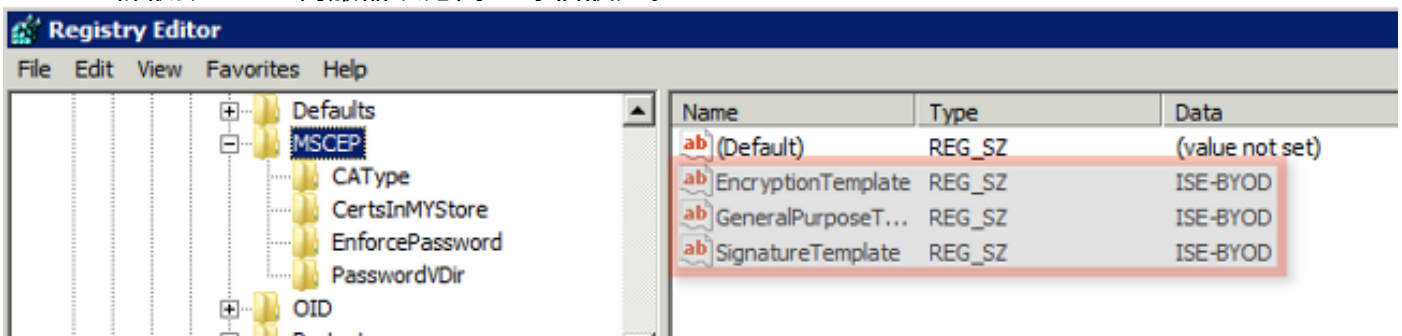
9. 按一下**Subject Name**頁籤，並確認已選擇請求中的Supply。
10. 點選**Issuance Requirements**選項卡。在典型的分層CA環境中，思科建議您將**Issuance**策略留空。
11. 按一下**Extensions**頁籤、**Application Policies**和**Edit**。
12. 按一下**Add**，確保**Client Authentication**已新增為應用程式策略。按一下「OK」（確定）。
13. 按一下**Security**頁籤，然後按一下**Add...**確保NDES服務安裝中定義的SCEP服務帳戶完全控制模板，然後按一下**確定**。
14. 返回到證書頒發機構GUI介面。
15. 按一下右鍵**Certificate Templates**目錄。導覽至**New > Certificate Template**以核發。
16. 選擇**先前配置**的ISE-BYOD模板，然後按一下**OK**。

附註：或者，您可以使用**certutil -SetCAtemplates + ISE-BYOD**命令通過CLI啟用模板。ISE-BYOD模板現在應列在啟用的證書模板清單中。

證書模板登錄檔配置

完成以下步驟以配置證書模板登錄檔項：

1. 連線到NDES伺服器。
2. 按一下**Start**，然後在搜尋欄中輸入**regedit**。
3. 導航到**Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**。
4. 將**EncryptionTemplate**、**GeneralPurposeTemplate**和**SignatureTemplate**金鑰從**IPSec(Offline Request)**更改為先前建立的ISE-BYOD模板。
5. 重新啟動NDES伺服器以應用登錄檔設定。



將ISE配置為SCEP代理

在BYOD部署中，端點不直接與後端NDES伺服器通訊。相反，ISE策略節點配置為SCEP代理並代

表終端與NDES伺服器通訊。終端直接與ISE通訊。可以配置NDES伺服器上的IIS例項以支援SCEP虛擬目錄的HTTP和/或HTTPS繫結。

完成以下步驟，將ISE配置為SCEP代理：

1. 使用**管理憑證**登入ISE GUI。
2. 按一下**Administration**、**Certificates**，然後按一下**SCEP CA Profiles**。
3. 按一下「**Add**」。
4. 輸入伺服器名稱和說明。
5. 輸入具有IP或完全限定域名(FQDN)的SCEP伺服器的URL(例如 <http://10.10.10.10/certsrv/mscep/>)。
6. 按一下「**Test Connectivity**」。成功的連線會產生成功的伺服器響應彈出消息。
7. 按一下**Save**以應用設定。
8. 若要驗證，請按一下**Administration**、**Certificates**、**Certificate Store**，並確認SCEP NDES伺服器RA證書已自動下載到ISE節點。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

使用本節內容，對組態進行疑難排解。

一般疑難排解說明

以下是可用於對組態進行疑難排解的重要說明清單：

- 將BYOD網路拓撲分解為邏輯路徑點，以幫助識別沿ISE、NDES和CA端點之間路徑的調試和捕獲點。
- 確保ISE節點和CA共用公共網路時間協定(NTP)時間源。
- 終端應該能夠使用從DHCP獲取的NTP和時區選項自動設定時間。
- 客戶端的DNS伺服器必須能夠解析ISE節點的FQDN。
- 確保ISE和NDES伺服器之間雙向允許TCP 80和/或TCP 443。
- 由於改進了客戶端日誌記錄，因此使用Windows電腦進行測試。或者，將Apple iDevice與

Apple iPhone配置實用程式配合使用，以監控客戶端控制檯日誌。

- 監視CA和NDES伺服器應用程式日誌中的註冊錯誤，並使用Google或TechNet研究這些錯誤。
- 在整個測試階段，使用HTTP for SCEP來簡化ISE、NDES和CA之間的資料包捕獲。
- 使用ISE策略服務節點(PSN)上的TCP轉儲實用程式，監控進出該NDES伺服器的流量。位於 **Operations > Diagnostic Tools > General Tools** 下。
- 在CA和NDES伺服器上安裝Wireshark，或在中間交換機上使用SPAN，以便捕獲來往於ISE PSN的SCEP流量。
- 確保在ISE策略節點上安裝適當的CA證書鏈以對客戶端證書進行身份驗證。
- 確保在登入期間將適當的CA證書鏈自動安裝到客戶端上。
- 預覽ISE和終端身份證書並確認存在正確的EKU屬性。
- 監控ISE GUI中的即時身份驗證日誌，瞭解身份驗證和授權失敗。
附註： 如果存在錯誤的EKU (例如具有伺服器身份驗證的EKU的客戶端證書)，則某些請求方不會初始化客戶端證書交換。因此，ISE日誌中可能並不總是存在身份驗證失敗。
- 在分散式部署中安裝NDES時，遠端根或子根CA將在服務安裝中由CA名稱或電腦名稱指定。NDES伺服器向此目標CA伺服器傳送證書註冊請求。如果終端證書註冊過程失敗，資料包捕獲(PCAP)可能會顯示NDES伺服器向ISE節點返回**404 Not Found**錯誤。要解決此問題，請重新安裝NDES服務並選擇Computer Name (電腦名稱) 選項，而不是CA Name (CA名稱)。
- 在裝置加入後，避免對SCEP CA鏈進行更改。終端OS (如Apple iOS) 不會自動更新以前安裝的BYOD配置檔案。在此iOS示例中，必須從終端中刪除當前配置檔案，並將終端從ISE資料庫中刪除，以便可以再次執行入網。
- 您可以配置Microsoft證書伺服器以連線到Internet並自動從Microsoft根證書程式更新證書。如果在具有受限Internet策略的環境中配置此網路檢索選項，則無法連線到Internet的CA/NDES伺服器預設情況下可能需要15秒超時。這會對來自SCEP代理 (例如ISE) 的SCEP請求的處理增加15秒延遲。ISE被程式設計，以便如果未收到響應，則在12秒後超時SCEP請求。為了解決此問題，請允許CA/NDES伺服器訪問Internet，或者修改Microsoft CA/NDES伺服器的本地安全策略中的網路檢索超時設定。要在Microsoft伺服器上找到此配置，請導航到**開始>管理工具>本地安全策略>公鑰策略>證書路徑驗證設定>網路檢索**。

客戶端日誌記錄

以下是用於對客戶端日誌記錄問題進行故障排除的有用技術清單：

- 輸入日誌%temp%\spwProfileLog.txt。命令檢視Microsoft Windows應用程式的客戶端日誌。
附註： WinHTTP用於Microsoft Windows終端和ISE之間的連線。有關錯誤代碼清單，請參閱Microsoft Windows錯誤消息文章。
- 輸入/sdcards/downloads/spw.log命令以檢視Android應用程式的客戶端日誌。
- 對於MAC OSX，請使用Console應用程式，並查詢SPW進程。

- 對於Apple iOS，請使用[Apple Configurator 2.0](#)來檢視消息。

ISE記錄

完成以下步驟以檢視ISE日誌：

1. 導航到Administration > Logging > Debug Log Configuration，然後選擇適當的ISE策略節點。
2. 根據需要將client和provisioning日誌設定為調試或跟蹤。
3. 重現問題並記錄相關的種子資訊，以便於搜尋，例如MAC、IP和使用者。
4. 導航到操作 > 下載日誌，然後選擇適當的ISE節點。
5. 在Debug Logs頁籤上，將名為ise-psc.log的日誌下載到案頭。
6. 使用智慧編輯器(例如[記事本++](#))來分析日誌檔案。
7. 當問題被隔離後，將日誌級別恢復為預設級別。

NDES日誌記錄和故障排除

有關詳細資訊，請參閱[AD CS:疑難解答網路裝置註冊服務Windows Server](#)文章。

相關資訊

- [BYOD解決方案指南 — 證書頒發機構伺服器配置](#)
- [Windows 2008 R2中的NDES概述](#)
- [MSCEP白皮書](#)
- [配置NDES伺服器以支援SSL](#)
- [使用EAP-TLS或具有EAP-TLS的PEAP時的證書要求](#)
- [技術支援與檔案](#)