為ISE SCEP整合配置HTTPS支援

目錄

簡介

本文檔介紹配置安全證書註冊協定(SCEP)與身份服務引擎(ISE)整合的超文本傳輸協定安全(HTTPS)支援所需的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Microsoft Internet Information Services(IIS)Web伺服器的基礎知識
- 在ISE上配置SCEP和證書的經驗

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.x
- 安裝了Windows Server 2008 R2企業版KB2483564和KB2633200的修補程式。

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專門為思科自帶裝置(BYOD)提供的指南。 請參閱Microsoft的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

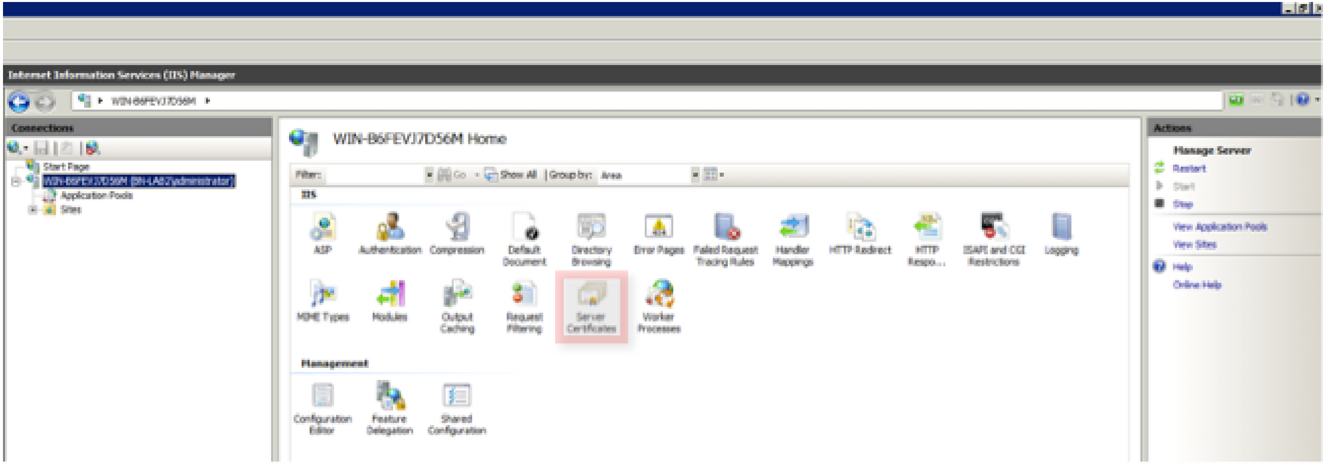
在BYOD部署中，核心元件之一是安裝了NDES角色的Microsoft 2008 R2 Enterprise伺服器。 此伺服器是Active Directory(AD)林的成員。 在NDES的初始安裝過程中，Microsoft的IIS Web伺服器會自動安裝並配置為支援SCEP的HTTP終止。 在一些BYOD部署中，客戶可能希望使用HTTPS進一步保護ISE和NDES之間的通訊。 此程式詳細介紹為SCEP網站請求和安裝安全套接字層(SSL)證書所需的步驟。

設定

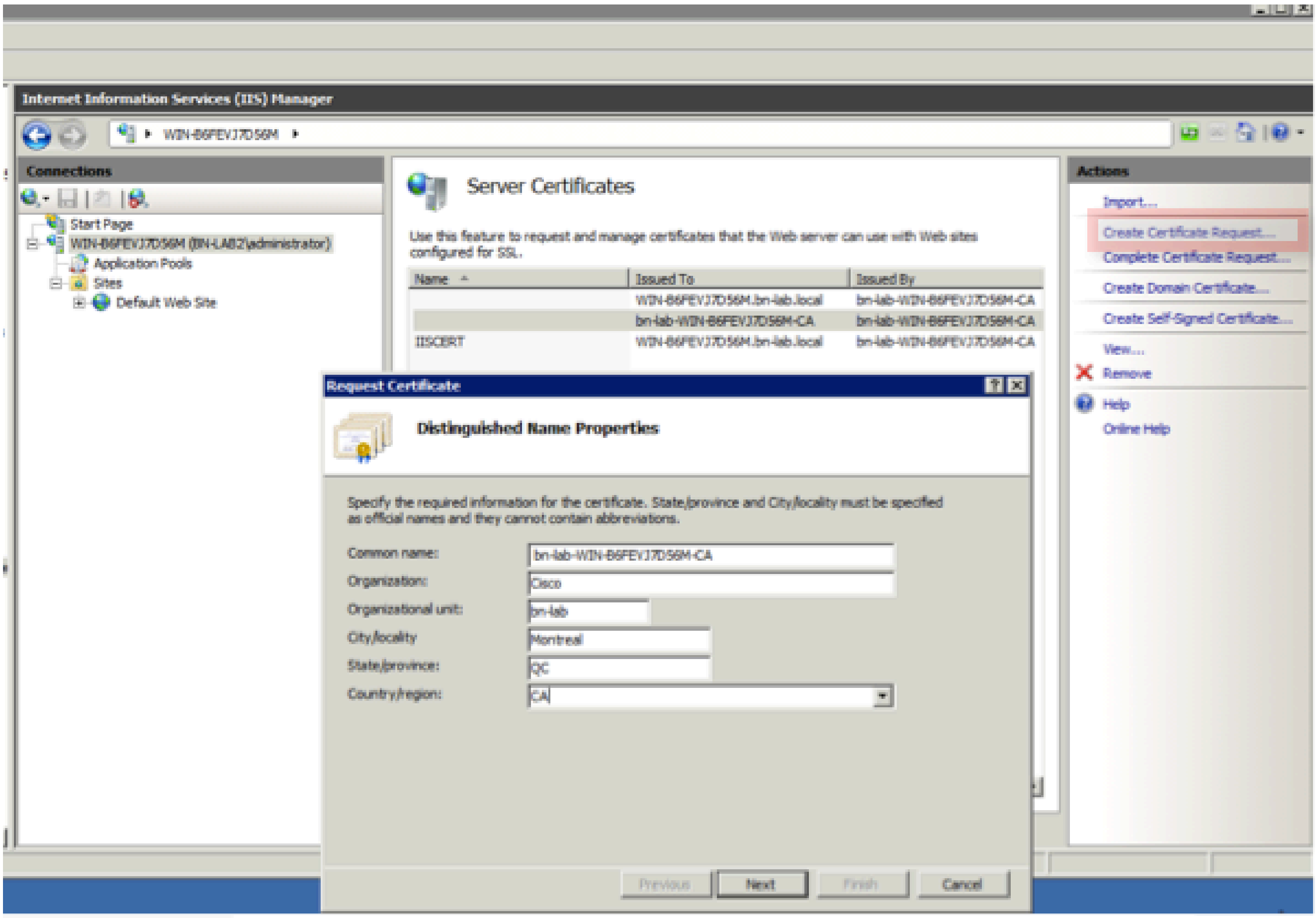
NDES伺服器證書配置

附註： 您必須為IIS配置新證書(僅當IIS與第三方PKI（如Verisign）整合時，或者當證書頒發機構(CA)和NDES伺服器角色分離到單獨的伺服器上時需要)。 在安裝中，如果NDES角色位於當前的Microsoft CA伺服器上，則IIS使用在CA設定期間建立的伺服器身份證書。 對於此類獨立配置，直接跳至本文檔中的**NDES Server IIS Binding Configuration**部分。

1. 通過控制檯或RDP連線到NDES伺服器。
2. 按一下**開始 — >管理工具 — > Internet資訊服務(IIS)管理器**。
3. 選中IIS伺服器名稱，然後按一下**Server Certificates**圖示。



4. 按一下**Create Certificate Request**，然後填寫欄位。



Internet Information Services (IIS) Manager

WIN-B6FEVJ7D56M ▸

Connections

- Start Page
- WIN-B6FEVJ7D56M (BN-LAB2\administrator)
  - Application Pools
  - Sites
    - Default Web Site

Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By
	WIN-B6FEVJ7D56M.bn-lab.local	bn-lab-WIN-B6FEVJ7D56M-CA
	bn-lab-WIN-B6FEVJ7D56M-CA	bn-lab-WIN-B6FEVJ7D56M-CA
IISCERT	WIN-B6FEVJ7D56M.bn-lab.local	bn-lab-WIN-B6FEVJ7D56M-CA

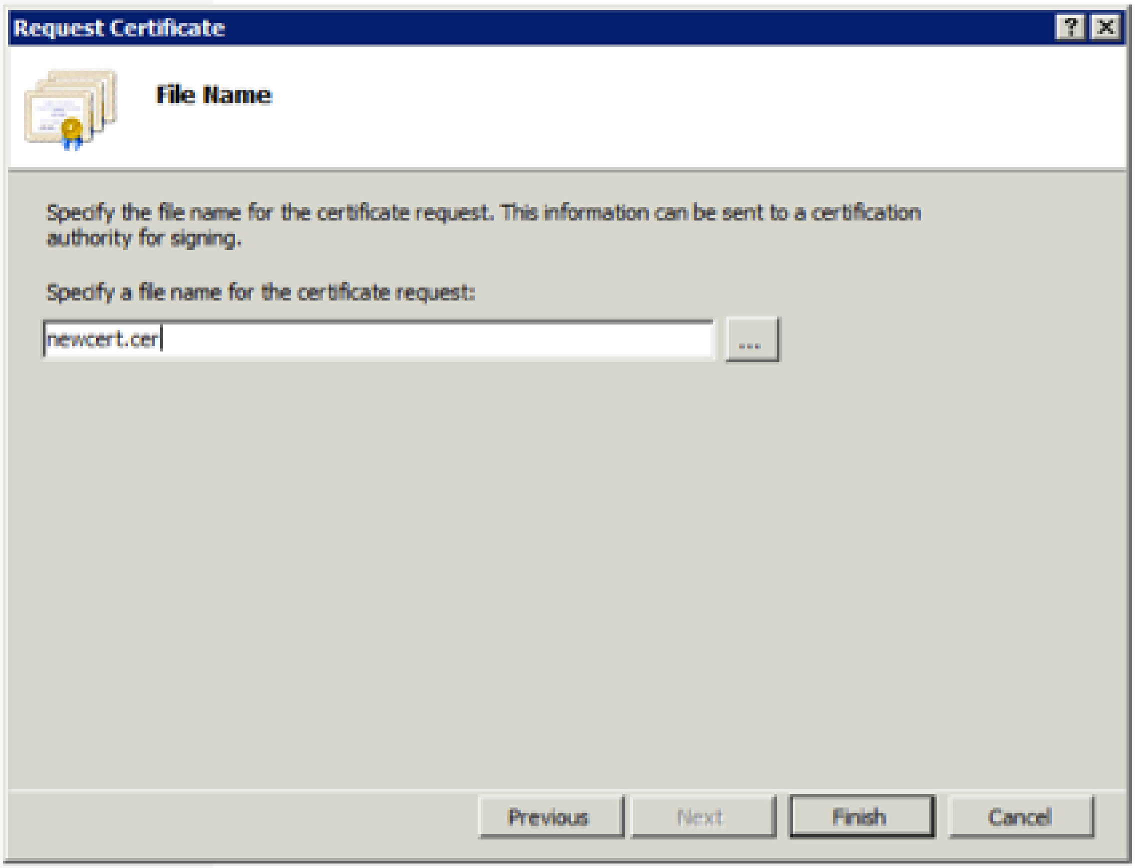
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Remove
Help
Online Help

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	bn-lab-WIN-B6FEVJ7D56M-CA
Organization:	Cisco
Organizational unit:	bn-lab
City/locality	Montreal
State/province:	QC
Country/region:	CA



Request Certificate

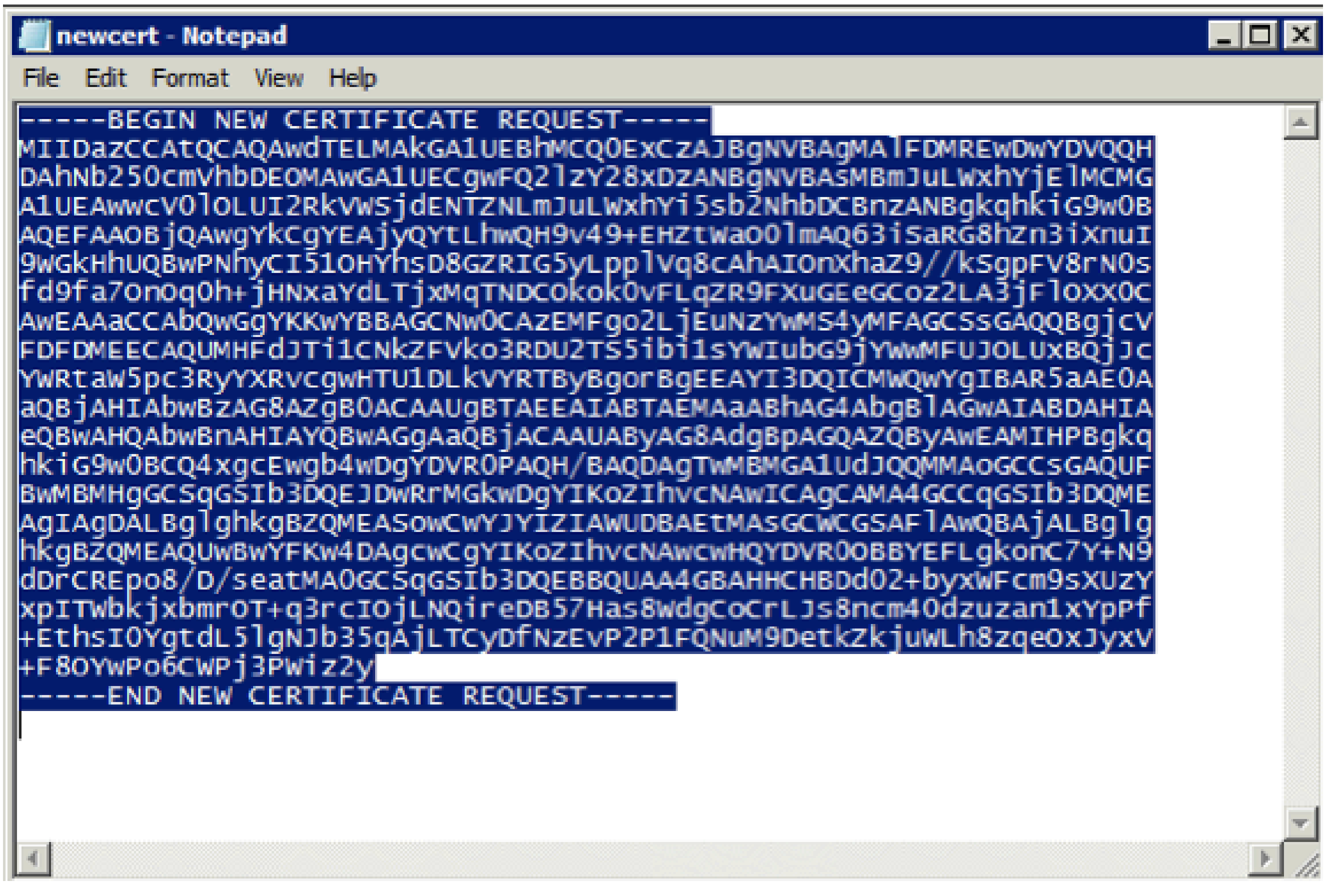
File Name

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

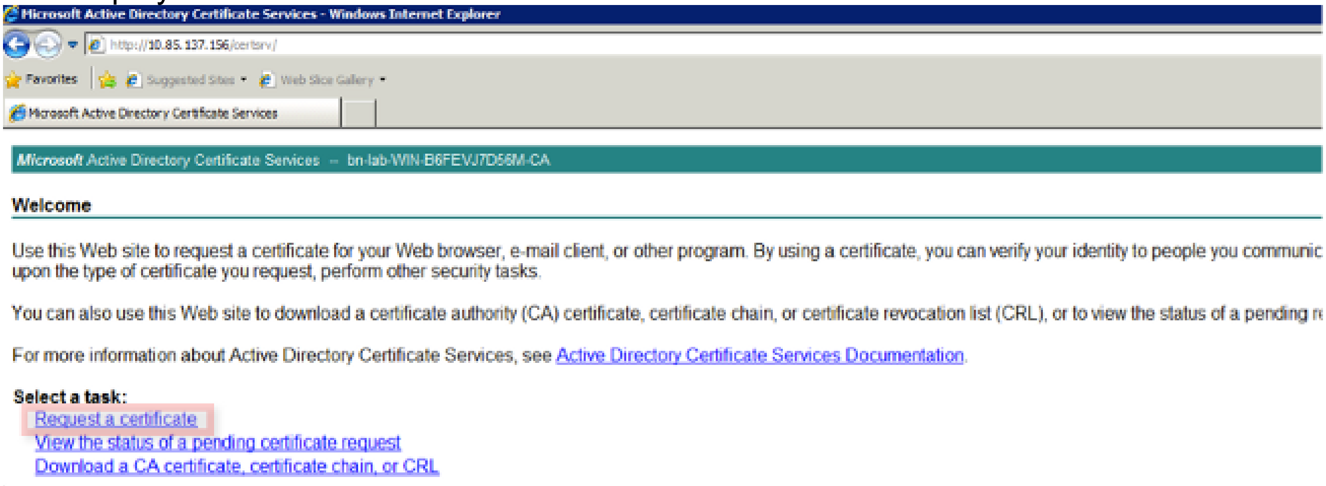
newcert.cer

5. 使用文本編輯器開啟上一步中建立的.cer檔案，並將內容複製到剪貼簿。



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDazCCAtQCAQAwdTELMAkGA1UEBhMCQ0ExCzAJBgNVBAgMAlFDMREwDwYDVQQH
DAhNb250cmVhbDEOMAwGA1UECgwFQ2lzY28xDzANBgNVBAsMBmJuLWxhYjElMCMG
A1UEAwwcV0lOLUI2RkVWSjdENTZNLmJuLWxhYi5sb2NhbDCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEAjyQYtLhwQH9v49+EHZtWaO0lmAQ63isaRG8hzn3ixnuI
9WGkHhUQBwPNhyCI51OHYhsD8GZRIG5yLpplVq8cAhAIOnXhaZ9//kSgpFV8rN0s
fd9fa7Onoq0h+jHNxaYdLTjxMqTNDCOkok0vFLqZR9FXuGEeGCoz2LA3jFloxx0C
AwEAAaCCAbQwGgYKKwYBBAGCNw0CAzEMFgo2LjEuNzYwMS4yMFAGCSsGAQQBgjcV
FDFDMEECAQUMHFdJTi1CNkZFVko3RDU2TS5ibi1sYWIubG9jYWwMFUJOLUxBQjJc
YWRtaW5pc3RyYXRvcgwHTU1DLkVYRTByBgorBgEEAYI3DQICMWQwYgIBAR5aAE0A
aQBjAHIAbwBzAG8AZgB0ACAAUgBTAEEAIABTAEMAaABhAG4AbgBlAGwAIABDAHIA
eQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByAwEAMIHPBgkq
hkiG9w0BCQ4xgcEwgb4wDgYDVR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCsGAQUF
BwMBMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQME
AgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCGSAFlAwQBAjALBglg
hkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFLgkonC7Y+N9
dDrCREpo8/D/seatMA0GCSqGSIb3DQEBBQUAA4GBAHHCHBDd02+byxWFcm9sXUzY
xpITWbkjxbmrOT+q3rcIOjLNQireDB57Has8WdgCoCrLJs8ncm40dzuzan1xYpPf
+EthsI0YgtdL5lgNJb35qAjLTCyDfNzEvP2P1FQNuM9DetkZkjuWLh8zqeOxJyxV
+F8OYwPo6CWPj3PWiz2y
-----END NEW CERTIFICATE REQUEST-----
```

6. 訪問Microsoft CA Web Enrollment網站，然後按一下**Request a Certificate**。示例URL:http://yourCAIP/certsrv


Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://10.85.137.156/certsrv/
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services

Microsoft Active Directory Certificate Services -- bn-lab-WIN-B6FEVJ7D56M-CA

Welcome

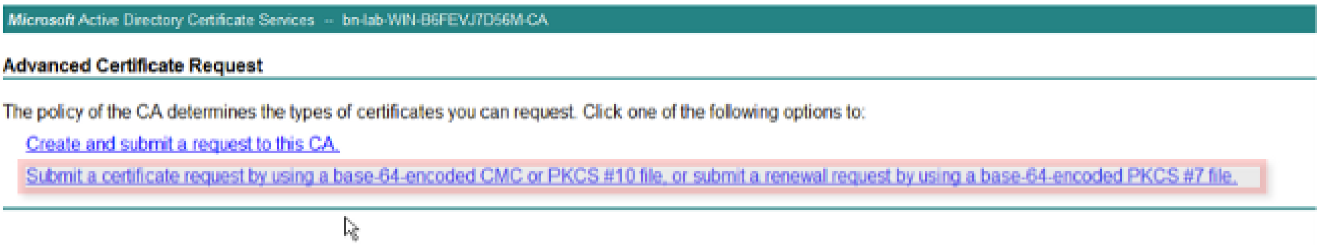
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communic upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending re

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

7. 按一下**Submit a certificate request by using....**從剪貼簿貼上證書內容，然後選擇**Web Server**模板。



Microsoft Active Directory Certificate Services -- bn-lab-WIN-B6FEVJ7D56M-CA

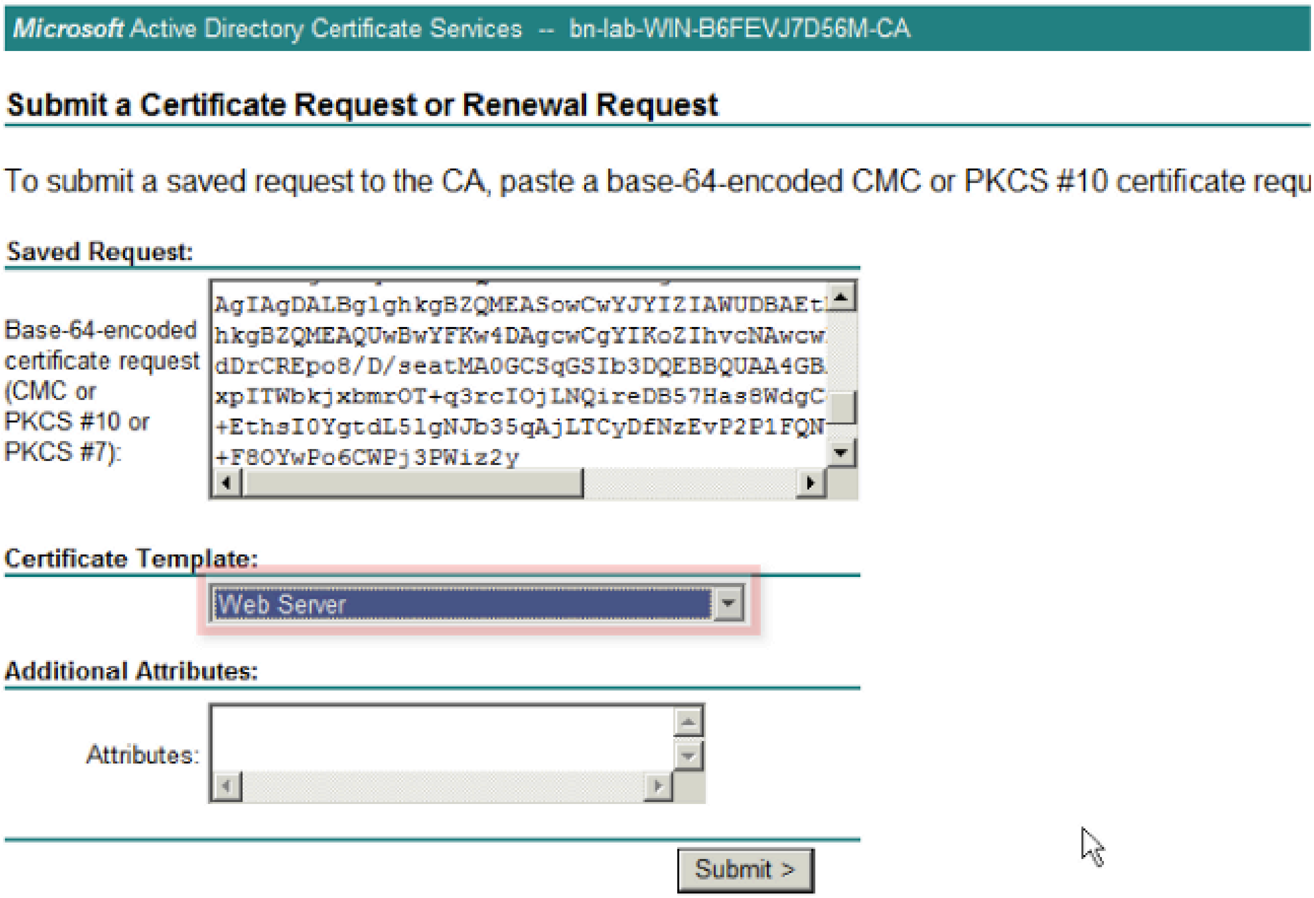
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

8. 按一下「**Submit**」，然後將憑證檔案儲存到案頭上。



Microsoft Active Directory Certificate Services -- bn-lab-WIN-B6FEVJ7D56M-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate requ

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
AgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEt
hkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcw
dDrCREpo8/D/seatMA0GCSqGSIb3DQEBBQUAA4GB
xpITWbkjxbmrOT+q3rcIOjLNQireDB57Has8WdgC
+EthsI0YgtdL51gNJb35qAjLTCyDfNzEvP2P1FQN
+F8OYwPo6CWPj3PWiz2y
```

Certificate Template:

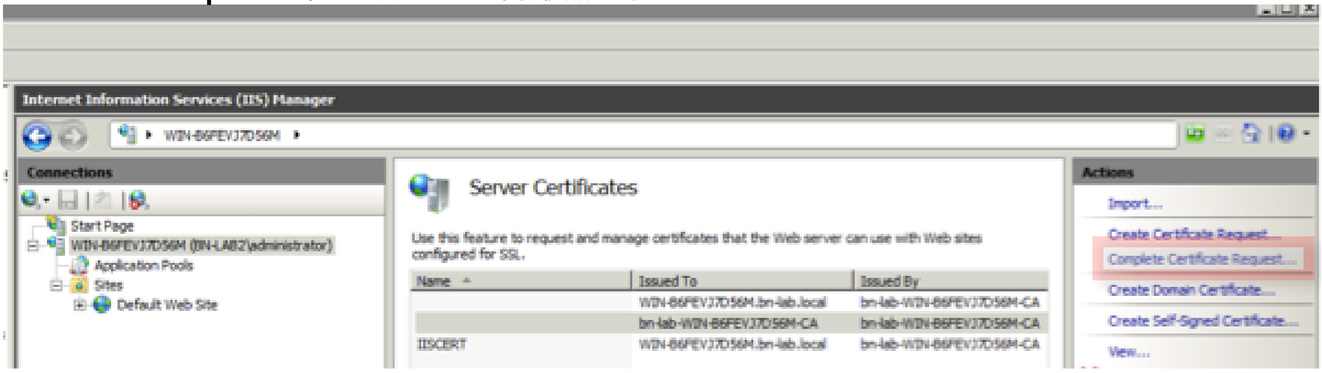
Web Server

Additional Attributes:

Attributes:

Submit >

9. 返回NDES伺服器並開啟IIS管理器實用程式。按一下伺服器名稱，然後按一下**Complete Certificate Request**以匯入新建立的伺服器證書。



Internet Information Services (IIS) Manager

WIN-B6FEVJ7D56M ▸

Connections

- Start Page
- WIN-B6FEVJ7D56M (BN-LAB2\administrator)
  - Application Pools
  - Sites
    - Default Web Site

Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

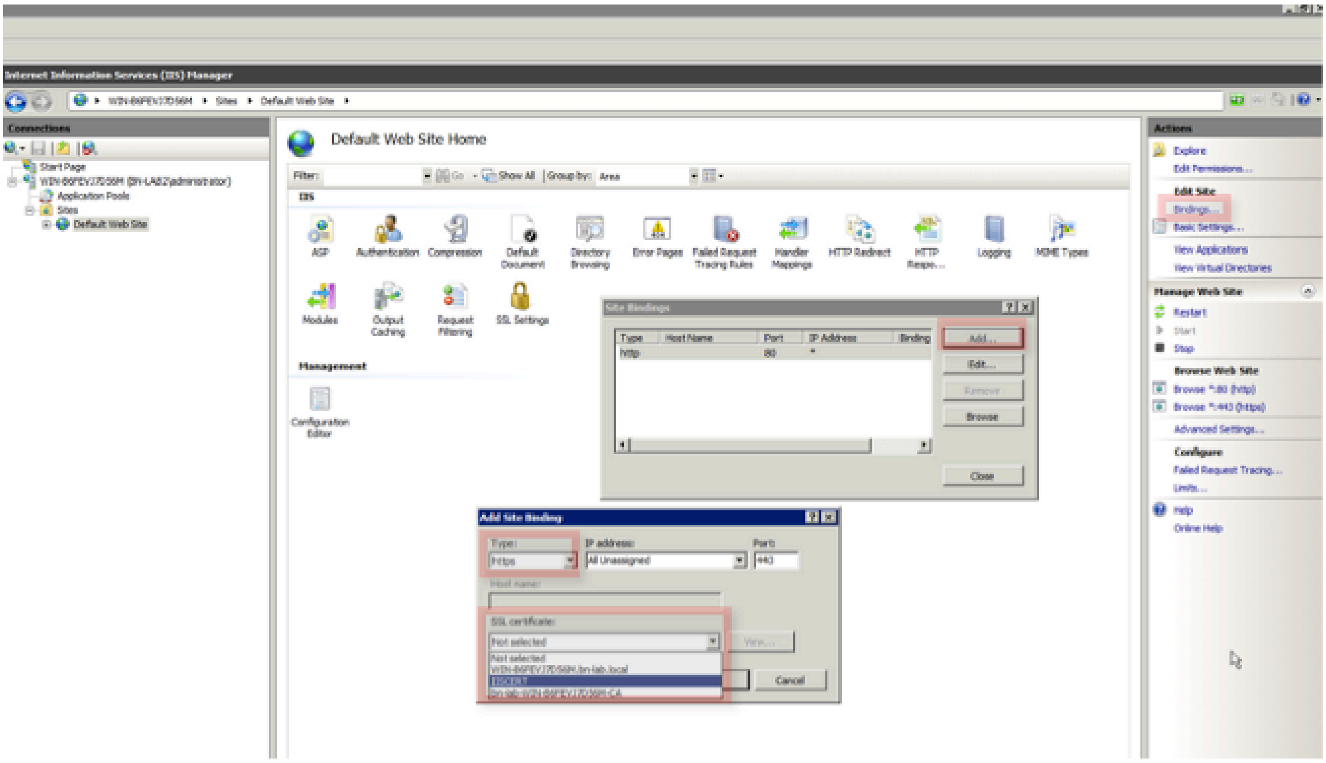
Name	Issued To	Issued By
	WIN-B6FEVJ7D56M.bn-lab.local	bn-lab-WIN-B6FEVJ7D56M-CA
	bn-lab-WIN-B6FEVJ7D56M-CA	bn-lab-WIN-B6FEVJ7D56M-CA
IISCERT	WIN-B6FEVJ7D56M.bn-lab.local	bn-lab-WIN-B6FEVJ7D56M-CA

Actions

Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...

NDES伺服器IIS繫結配置

1. 展開**伺服器名稱**，展開**Sites**，然後按一下**Default Web Site**。
2. 按一下右上角的**Bindings**。
3. 按一下**Add**，將Typeto HTTPS變更為，然後從下拉式清單中選擇憑證。
4. 按一下「**OK**」（**確定**）。



Site Bindings

Type	Host Name	Port	IP Address	Binding
http		80	*	

Type: https

IP address: All Unassigned

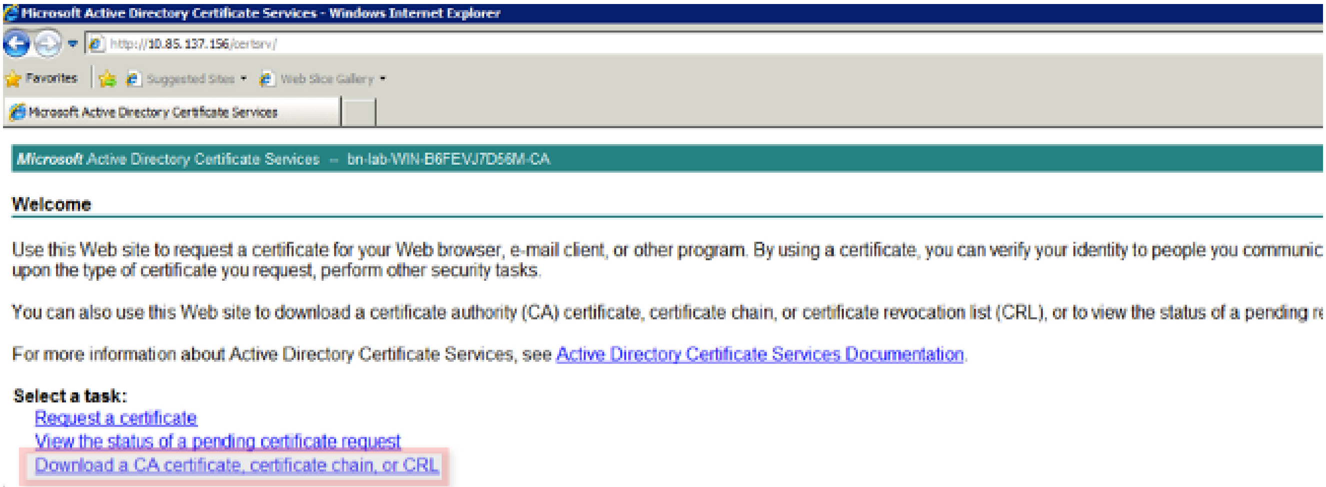
Port: 443

SSL certificate: Not selected

- Not selected
- WIN-B6FEVJ7D56M.bn-lab.local
- ISSCERT
- bn-lab-WIN-B6FEVJ7D56M-CA

ISE伺服器配置

1. 連線到CA伺服器的Web註冊介面並下載CA證書鏈。



Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://10.85.137.156/certsrv/
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services

Microsoft Active Directory Certificate Services -- bn-lab-WIN-B6FEVJ7D56M-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communic
upon the type of certificate you request, perform other security tasks.

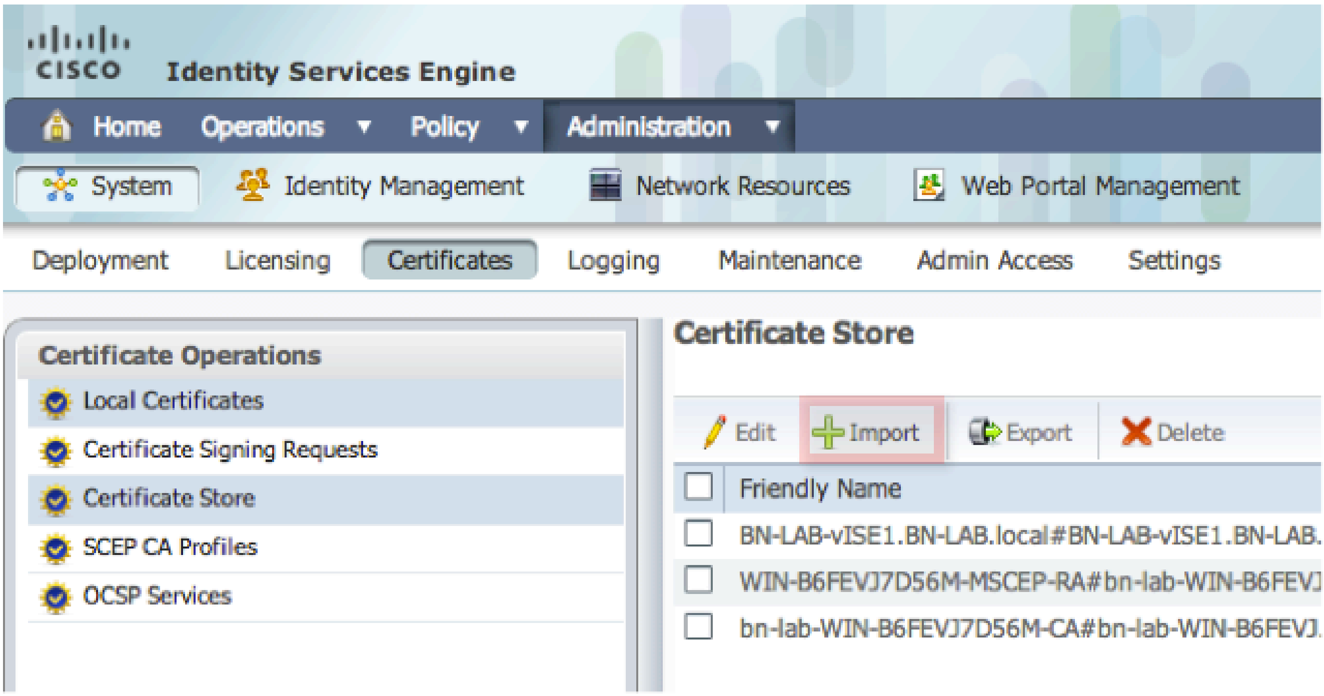
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending re

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

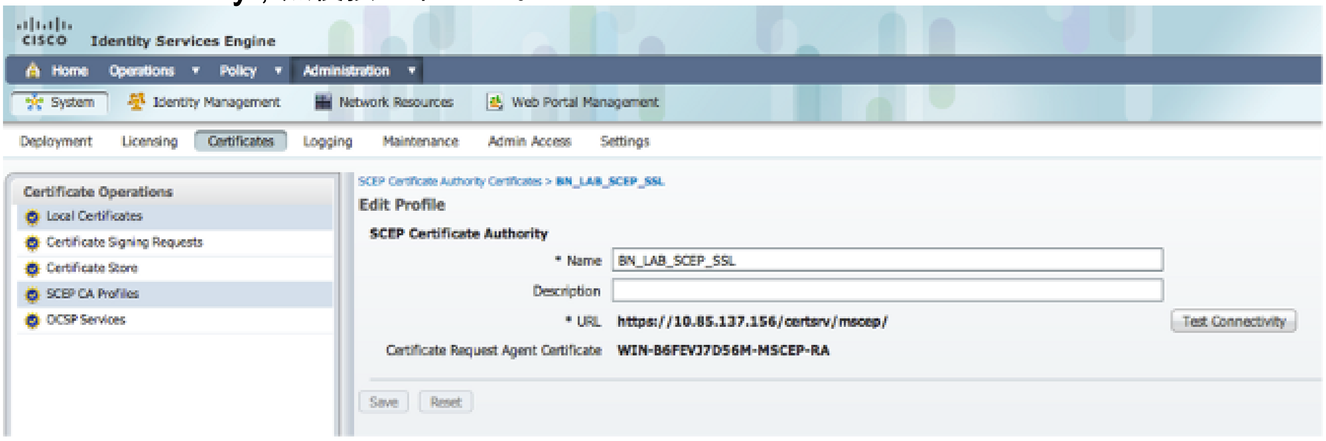
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

2. 從ISE GUI導航到**管理 — >證書 — >證書儲存**，然後將CA證書鏈匯入ISE儲存。



□	Friendly Name
□	BN-LAB-vISE1.BN-LAB.local#BN-LAB-vISE1.BN-LAB.
□	WIN-B6FEVJ7D56M-MSCEP-RA#bn-lab-WIN-B6FEVJ
□	bn-lab-WIN-B6FEVJ7D56M-CA#bn-lab-WIN-B6FEVJ.

3. 導覽至**Administration -> Certificates -> SCEP CA Profiles**，然後為HTTPS設定URL。按一下**Test Connectivity**，然後按一下**Save**。



Edit Profile

SCEP Certificate Authority

* Name: BN_LAB_SCEP_SSL

Description:

* URL: https://10.85.137.156/certsrv/mscep/

Certificate Request Agent Certificate: WIN-B6FEVJ7D56M-MSCEP-RA

驗證

使用本節內容，確認您的組態是否正常運作。

- 導覽至**Administration -> Certificates -> Certificate** Store，然後確認CA憑證鏈結和NDES伺服器註冊授權單位(RA)憑證是否存在。
- 使用Wireshark或TCP轉儲來監控ISE管理節點和NDES伺服器之間的初始SSL交換。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 將BYOD網路拓撲分解為邏輯路徑點，以幫助識別這些終端之間的路徑上的調試和捕獲點 — ISE、NDES和CA。
- 確保ISE和NDES伺服器之間雙向允許TCP 443。

- 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。
- 使用ISE 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。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

相關資訊

- **為BYOD配置SCEP支援**
- **技術支援與文件 - Cisco Systems**