# 為ISE SCEP整合配置HTTPS支援

# 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>設定</u> <u>NDES伺服器證書配置</u> <u>NDES伺服器IIS繫結配置</u> <u>ISE伺服器配置</u> <u>驗證</u> <u>疑難排解</u> <u>相關資訊</u>

# 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<u>KB</u>2483564<u>和KB</u>2633200<u>的修補程式</u>。
 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。

Teteraet Information Services (IIS) Manager	_	_	_	_	_	_	_	_	_			_	<b>a</b> = 31
Connections Q I : : : : : : : : : : : : : : : : : :	VII Piter: IIS ASP MPIC Types Hanageres Configuration	Authentication Authentication Hodules	DS6M Hon	ne Prev Al  0 Default Decument	ing by area Directory Browing Service Certificates	Error Pages Voyker Processes	Paled Reset	Handler Hanganga	HTTP Radvert	нтр Каро	ESAT and CGI Restrictors	Loging	Actuest Hasage Server C Rester E Dent E Dent Ver Acplacion Puolin Ver Stes Orline Help

- 0 >

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

Internet Information Consistan (IIC) Manager				
WIN-BGFEV17D56M				🖬 🖂 🏠 I 😣 •
Connections	<b>O</b>			Actions
Q	Server Certific	cates		Import
Start Page WIN-B6FEV37D56M (BN-LAB2\administrator)	Use this feature to request an	d manage certificates that the Web server	can use with Web sites	Create Certificate Request
Application Pools	Name +	Issued To	Issued By	Complete Certificate Request
🗈 😔 Default Web Site		WIN-86FEV37D56M.bn-lab.local bn-lab-WIN-86FEV37D56M-CA	bn-lab-WDV-86FEV37D56M-CA bn-lab-WDV-86FEV37D56M-CA	Create Self-Signed Certificate
1	IISCERT	WIN-86FEV37D56M.bn-lab.local	bn-lab-WIN-86PEV37D56M-CA	Vew
Reques	t Certificate		2 X	X Remove
	Distinguished Name Pr	roperties		W Help Online Help
	þ.			
Sped	fy the required information for the o	ertificate. State/province and City/locality	must be specified	
as of	fcial names and they cannot contain	abbreviations.		
Conv	non name: bn-lab-W	IN-B6FEV17D56M-CA		
Orga	nizational unit: Doclab	_	_	
Oty/	ocality Montreal			
State	/province: QC			
Coun	try/region: CA		-	
1			-	
11			-	
		Previous Next	Title Canad	
			Carde	
Request Certificate				<u>?</u> ×
Request Certificate				?×
Request Certificate				<u>?</u> ×
Request Certificate				2
Request Certificate				? ×
Request Certificate File Name Specify the file name for the certi authority for signing.	ficate request. This info	ormation can be sent to a c	ertification	? 🗙
Request Certificate         Image: Specify the file name for the certificate	ficate request. This info	ormation can be sent to a c	ertification	? 🗙
Request Certificate         File Name         Specify the file name for the certification         Specify the file name for the certification         Specify a file name for the certification	ficate request. This info ate request:	ormation can be sent to a c	ertification	
Request Certificate         Image: Specify the file name for the certific authority for signing.         Specify a file name for the certific newcert.cer	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Specify the file name for the certification authority for signing.         Specify a file name for the certification         Image: Specify a file name for the certification	ficate request. This info ate request:	ormation can be sent to a c	ertification	
Request Certificate         Image: Specify the file name for the certification         Specify the file name for the certification         Specify a file name for the certification         Image: Specify a file name for the certification <td>ficate request. This info ate request:</td> <td>ormation can be sent to a c</td> <td>ertification</td> <td></td>	ficate request. This info ate request:	ormation can be sent to a c	ertification	
Request Certificate         Image: Specify the file name for the certification of the certification	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Control of the certification         Specify the file name for the certification         Specify a file name for the certification         Image: Control of the certification         Image: Contrelet the certification <tr< th=""><td>ficate request. This info</td><td>ormation can be sent to a c</td><td>ertification</td><td></td></tr<>	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Constraint of the certification         Specify the file name for the certification         Specify a file name for the certification         Image: Constraint of the certification	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Constraint of the certification         Specify the file name for the certification         Specify a file name for the certification         Image: Constraint of the certification	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Constraint of the certification         Specify the file name for the certification         Specify a file name for the certification         Image: Constraint of the certification	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Specify the file name for the certification of the certification	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Control of the certification of the certifi	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Control of the certification         Specify the file name for the certification         Specify a file name for the certification         Image: Control of the certification         Image: Contrelet the certification <tr< th=""><td>ficate request. This info</td><td>ormation can be sent to a c</td><td>ertification</td><td></td></tr<>	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Control of the certification         Specify the file name for the certification         Specify a file name for the certification         Image: Control of the certification <t< th=""><th>ficate request. This info</th><th>ormation can be sent to a c</th><th>ertification</th><th></th></t<>	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Control of the certification of the certifi	ficate request. This info	ormation can be sent to a c	ertification	
Request Certificate         Image: Control of the certification of the certifi	ficate request. This info	ormation can be sent to a c	ertification	

리비치

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。

📕 newcert - Notepad	_ 🗆 🗵
File Edit Format View Help	
BEGIN NEW CERTIFICATE REQUEST MIIDazCCAtQCAQAwdTELMAkGA1UEBhMCQDExCZAJBGNVBAGMA1FDMREwDwYDVQQH DAhNb250cmVhbDEOMAwGA1UECgwFQ21zY28XDZANBGNVBASMBmJuLwXhYjE1MCMG A1UEAwwcV010LUI2RkVwSjdENTZNLmJuLwXhYi5Sb2NhbDCBnZANBgkqhkiG9w0B AQEFAAOBjQAwgYKCgYEAjyQYLLhwQH9V49+EHZtwa001mAQ63isaRG8hZn3iXnuI 9wGkHhUQBwPNhyCI510HYhSD8GZRIG5yLpp1Vq8CAhAIOnXhaZ9//kSgpFV8rN0s fd9fa7onoq0h+jHNxaYdLTjXMqTNDCOkok0vFLqZR9FXuGEeGCoz2LA3jF1OXXOC AwEAAaCCAbQwGgYKKWYBBAGCNw0CAZEMFg02LjEUNZYMM54yMFAGCSSGAQQBgjCV FDFDMEECAQUMHFdJTi1CNkZFVk03RDU2T55ibi1SYWIUbG9jYWMFUJOLUXBQJJC YWRtaWSpc3RyYXRvcgWTTU1DLkVYRTByBgorBgEEAYI3DQICMwQwYgIBARSAAE0A aQBjAHIAbwBZAG8AZgB0ACAAUgBTAEEAIABTAEMAAABhAG4AbgB1AGwAIABDAHIA eQBwAHQAbwBnAHIAYQBWAGGAaQBjACAAUABYAG8AdgBpAGQAZQBYAWEAMIHPBgkq hkiG9w0BCQ4xgcEwgb4wDgYDVR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCSGAQUF BwMBMHgGCSqGSIb3DQEJDWRrMGkwDgYIKOZIhvCNAWICAgCAMA4GCCqGSIb3DQME AqIAgDALBg]ghkgBZQMEASowCWYJYIZIAWUDBAEtMASGCwCGSAF1AwQBAjALBg]g hkgBZQMEAQUwBwYFKw4DAgcwCgYIKOZIhvCNAwCMHQYDVR00BBYEFLgkonC7Y+N9 dDrCREpo8/D/seatMA0GCSqGSIb3DQEBBQUAA4GBAHHCHBDd02+byxWFcm9sXUZY xpITWbkjxbmr0T+q3rcI0jLNQireDB57Has8wdgCoCrLJs8ncm40dzuzan1xYPPf +EthSI0YgtdL51gNJb35qAjLTCyDfNZEVP2PIFQNuM9DetkZkjuWLh8zqe0XJyxV +F80YWPo6CWPj3PWiz2y	
T I	
	- //

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



#### 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。

### 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:	Saved	Req	uest:
----------------	-------	-----	-------

	· · · · · · · · · · · · · · · · · · ·	
	AgIAgDALBglghkgBZQMEASow	Cwyjyiziawudbaet
Base-64-encoded	hkgBZQMEAQUwBwYFKw4DAgcw(	CgYIKoZIhvcNAwcw
certificate request	dDrCREpo8/D/seatMA0GCSqG	SIb3DQEBBQUAA4GB
(CMC or	xpITWbkjxbmrOT+q3rcIOjLN	lireDB57Has8WdgC
PKCS #10 or	+EthsI0YgtdL51gNJb35gAjL	CyDfNzEvP2P1FQN-
PKCS #7):	+F80YwPo6CWPj3PWiz2y	-
	4	Þ

Certificate Tem	plate:	
	Web Server	
Additional Attri	butes:	
Attributes		
	Submit >	R

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							
(3) (3) ► WIN-66FEV17D56M ►							
Connections	Server Certificates Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.			Actions Import Create Certificate Request Complete Certificate Request			
⊖ Stes	Name +	Issued To WIN-86FEV37D56M.bn-lab.local bn-lab-WIN-86FEV37D56M-CA WIN-86FEV37D56M-CA	Issued By bn-lab-WDN-86PEV37D56M-CA bn-lab-WDN-86PEV37D56M-CA bn-lab-WDN-86PEV37D56M-CA	Create Domain Certificate Create Self-Signed Certificate			
I I	HOUDK!	11214-00FE1272/230FL0148020C8	DIHED-HUN-DOPEN/J/J/JOPH-CA	Vew			

## 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)。



## 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。

G Hicrosoft Active Directory Certificate Services - Windows Internet Explorer
👷 Favorites 🛛 🎪 😰 Suggested Sites 🔹 🌮 Web Site Galery 🔹
6 Microsoft Active Directory Certificate Services
Microsoft Active Directory Cartificate Senices
Microsoft Active Directory Centrolate Centrols - Enhantime Dol Elforobolin 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.



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

CISCO Identity Services Engine	
💧 Home Operations 🔻 Policy 🔻	Administration 🔻
🔆 System 🔮 Identity Management	Network Resources 🛃 Web Portal Management
Deployment Licensing Certificates	Logging Maintenance Admin Access Settings
Certificate Operations	Certificate Store
<ul> <li>Certificate Store</li> <li>SCEP CA Profiles</li> <li>OCSP Services</li> </ul>	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。

CISCO Identity Services Engine			
🛕 Home Operations * Policy * Admin	istration 🔻		
🔆 System 📲 Identity Management 📲 I	Network Resources 🛛 🛃 Web Portal Mana	agement	
Deployment Licensing Certificates Loggin	ng Maintenance Admin Access S	ettings	
Certificate Operations	SCEP Certificate Authority Certificates > BN_LAB_	SCEP_SSL	
Local Certificates	Edit Profile		
Certificate Signing Requests	SCEP Certificate Authority		
Certificate Store	* Name	BN_LAB_SCEP_SSL	
SCEP CA Profiles	Description		
OCSP Services	* URL	https://10.85.137.156/certsrv/mscep/	Test Connectivity
	Certificate Request Agent Certificate	WIN-B6FEVJ7D56M-MSCEP-RA	
	Save Reset		

# 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。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>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。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>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<u>有關 Debug 指令的重要資訊</u>。

# 相關資訊

- <u>為BYOD配置SCEP支援</u>
- 技術支援與文件 Cisco Systems