# 使用EAP-FAST和LDAP伺服器配置的無線LAN控制器上的本地EAP身份驗證示例

目錄

簡介 必要條件 需求 採用元件 慣例 背景資訊 設定 網路圖表 組態 在WLC上將EAP-FAST配置為本地EAP身份驗證方法 產生WLC的裝置憑證 將裝置證書下載到WLC 將PKI的根證書安裝到WLC中 生成客戶端的裝置證書 生成客戶端的根CA證書 在WLC上配置本地EAP 配置LDAP伺服器 在域控制器上建立使用者 配置使用者的LDAP訪問 使用LDP標識使用者屬性 配置無線客戶端 驗證 疑難排解 相關資訊

# <u>簡介</u>

本檔案將說明如何在無線LAN控制器(WLC)上設定可擴充驗證通訊協定(EAP) — 透過安全通道進行 彈性驗證(FAST)本地EAP驗證。本文檔還說明了如何將輕量級目錄訪問協定(LDAP)伺服器配置為本 地EAP的後端資料庫,以檢索使用者憑據並對使用者進行身份驗證。

# <u>必要條件</u>



本文件沒有特定需求。

## <u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- 執行韌體4.2的Cisco 4400系列WLC
- Cisco Aironet 1232AG系列輕量型存取點(LAP)
- Microsoft Windows 2003伺服器配置為域控制器、LDAP伺服器以及證書頒發機構伺服器。
- 執行韌體版本4.2的Cisco Aironet 802.11 a/b/g使用者端配接器
- 運行韌體版本4.2的Cisco Aironet案頭實用程式(ADU)

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。

## <u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

# <u>背景資訊</u>

無線LAN控制器上的本地EAP身份驗證是隨無線LAN控制器4.1.171.0版引入的。

本地EAP是一種身份驗證方法,它允許使用者和無線客戶端在控制器上進行本地身份驗證。它適用 於想要在後端系統中斷或外部身份驗證伺服器關閉時保持與無線客戶端連線的遠端辦公室。啟用本 地EAP時,控制器用作身份驗證伺服器和本地使用者資料庫,因此它消除對外部身份驗證伺服器的 依賴。本地EAP從本地使用者資料庫或LDAP後端資料庫中檢索使用者憑證以驗證使用者。本地 EAP支援控制器與無線客戶端之間的LEAP、EAP-FAST、EAP-TLS、P EAPv0/MSCHAPv2和 PEAPv1/GTC身份驗證。

本地EAP可以使用LDAP伺服器作為其後端資料庫來檢索使用者憑據。

LDAP後端資料庫允許控制器向LDAP伺服器查詢特定使用者的憑證(使用者名稱和密碼)。然後使 用這些憑證對使用者進行身份驗證。

LDAP後端資料庫支援以下本地EAP方法:

- EAP-FAST/GTC
- EAP-TLS
- PEAPv1/GTC。

還支援LEAP、EAP-FAST/MSCHAPv2和PEAPv0/MSCHAPv2,但前提是將LDAP伺服器設定為返回明文密碼。例如,不支援Microsoft Active Directory,因為它不返回明文密碼。如果無法將 LDAP伺服器配置為返回明文密碼,則不支援LEAP、EAP-FAST/MSCHAPv2和 PEAPv0/MSCHAPv2。

**注意:**如果在控制器上配置了任何RADIUS伺服器,則控制器會先嘗試使用RADIUS伺服器對無線客 戶端進行身份驗證。僅當未找到RADIUS伺服器時嘗試本地EAP,原因可能是RADIUS伺服器超時或 未配置RADIUS伺服器。如果設定了四個RADIUS伺服器,則控制器會嘗試使用第一個RADIUS伺服 器、第二個RADIUS伺服器、以及本地EAP來驗證使用者端。如果使用者端嘗試然後手動重新驗證 ,則控制器會先嘗試第三個RADIUS伺服器,然後嘗試第四個RADIUS伺服器,最後嘗試本地EAP。

此示例使用EAP-FAST作為WLC上的本地EAP方法,WLC又配置為查詢LDAP後端資料庫以獲取無 線客戶端的使用者憑證。



本文檔使用客戶端和伺服器端證書的EAP-FAST。為此,安裝程式使用**Microsoft Certificate** Authority(CA)服務器生成客戶端和伺服器證書。

使用者憑證儲存在LDAP伺服器中,以便在證書驗證成功時,控制器將查詢LDAP伺服器以檢索使用 者憑證並對無線客戶端進行身份驗證。

本檔案假設以下設定已經就位:

- •LAP已註冊到WLC。有關註冊過程的詳細資訊,請參閱<u>向無線LAN控制器(WLC)註冊輕量</u> <u>AP(LAP)</u>。
- DHCP伺服器配置為向無線客戶端分配IP地址。
- Microsoft Windows 2003 server配置為域控制器以及CA伺服器。此範例使用wireless.com作為 網域。有關將Windows 2003伺服器配置為域控制器的詳細資訊,請參閱<u>將Windows 2003配置</u> 為域控制器。請參閱安裝並配置Microsoft Windows 2003 Server作為證書頒發機構(CA)伺服器 ,以便將Windows 2003 Server配置為企業CA伺服器。

#### 網路圖表

本檔案會使用以下網路設定:





完成以下步驟即可實作此組態:

- <u>在WLC上將EAP-FAST配置為本地EAP身份驗證方法</u>
- <u>配置LDAP伺服器</u>
- 配置無線客戶端

# <u>在WLC上將EAP-FAST配置為本地EAP身份驗證方法</u>

如前所述,本文檔使用客戶端和伺服器端證書的EAP-FAST作為本地EAP身份驗證方法。第一步是 下載下列憑證並將其安裝至伺服器(在此案例中為WLC)和使用者端。

WLC和使用者端都需要從CA伺服器下載這些憑證:

- 裝置憑證(一個用於WLC,一個用於使用者端)
- •WLC的公鑰基礎架構(PKI)的根憑證以及使用者端的CA憑證

## 產生WLC的裝置憑證

執行以下步驟,以便從CA伺服器為WLC生成裝置證書。WLC使用此裝置憑證對使用者端進行驗證 。

 從與CA伺服器具有網路連線的PC轉到http://<CA伺服器的IP地址>/certsrv。以CA伺服器管理 員身份登入。

Pile Edit Ver Piloritas Tober celp Address 4 Nater//10.77.244.198/certarv Connect to 10.77.244.198	یں م کا بر ۵
Address Mittgel/(10.77.244.198/certsrv	∞ <b>(3</b> ) ♥
Connecting to 10.77.244.198 User name:  administrator Password: Remember my password Cfc Cencel	
Opening page http://10.77.244.199/certarv	

2. 選擇**請求證書**。

Microsoft Carifford's Concess — weekes  Provide a continue of the set of download a continue at each in the Velo, sign and encrypt messages, and, depending upon the type of certificate you required  of a pending request.  Provide a continue of a p	termi r, e-mail Clerit, or other program. By using a certificate, you can verify your d encrypt messages, and, depending upon the type of certificate you request, ity (CA) certificate, certificate chain, or certificate revocation list (CRL), or to a Services Documentation. Tadvanced certificate request. Warr Home	Workend Cardia de Services - wweeke     Worken     Workend	Image: Control of Co	
Macroame Sectors and Controlled's Service's — weekes Weicome Joe its Web site to request a certificate for your Web browner, e-mail clent, or other program. By using a cartificate you reque for the sector is used this web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or for once information about Certificate Service's, see Certificate Service's Documentation. For more information about Certificate Service's, see Certificate Service's Documentation. We we the setup of a Service's description of the service's description of the service's Documentation.	r, e-mail client, or other program. By using a certificate, you can verify your d encrypt messages, and, depending upon the type of certificate you request, ity (CA) certificate, certificate chain, or certificate revocation list (CRL), or to a Services Documentation. ■ Tradvanced certificate request. ■ Tradvanced certificate request. ■ Ham	Mercanic Currindus Exercise — weekes  Velocine  Velocine  Velocine  Velocine  Comparison	Microaed Cardiolas Cardona weeks  Weicome Weicome Weicome Use his Web site to request a certificate for your Web proveer, e-mail ciert, or other program. By using a certificate, you can verify your User his table to request a certificate of your Web, sign and encypt messages, and, depending upon the type of certificate you request perform dent source the Web, sign and encypt messages, and, depending upon the type of certificate you request perform dent source the source of the source o	
Wetcome           Use this Web site to request a conflicate for your Web browser, e-mail citert, or other program. By using a conflicate, you can werfly your define to be your center use werfly were defined by bus center used were set were set were set were set and were set to download a conflicate authority (CA) conflicate, centificate chain, or centificate revocation list (CRL), or for our all bus used to a pending request.           For our an about this Web site to download a conflicate authority (CA) conflicate, centificate chain, or centificate revocation list (CRL), or for our all bus used to a pending request.           For our an about Centificate Services, see Centificate Services Documentation.           Image: Documentation about Centificate request.           Image: Documentat	r, e-mail client, or other program. By using a certificate, you can verify your d encrypt messages, and, depending upon the type of certificate you request, ity (CA) certificate, certificate chain, or certificate revocation list (CRL), or to a Services Documentation. Internet - Tadvanced certificate request.	Velocities be this Yorks date to request a certificate for your Web browser, e-mail cleret, or other program. By using a certificate, you can verify you tright to predet a contribute with over the web, sign and encrypt messages, and, depending using the type of certificate you request, othern other soccarts tasks. Ou can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to wer the status of a pending request. Ou can also use and use of the todownload a certificate services Documentation  *** Tension a download a certificate Services, see <u>Certificate Services Documentation  *** User a status of a pending request. Download a certificate chain, or CFL  *** Tension a download a certificate chain, or CFL  ***  ***  ***  *** *** *** *** *** *</u>	Welcome Use this Web site to request a certificate for your Web browser, e-mail clert, or other program. By using a certificate, you can worthy cour request perform other security tasks. For more information about Certificate Services, see <u>Certificate Services</u> , certificate chain, or certificate revocation list (CRL), or to two the status of a pending request. For more information about Certificate Services, see <u>Certificate Services</u> , certificate chain, or certificate revocation list (CRL), or to two the status of a pending request. For more information about Certificate Services, see <u>Certificate Services</u> , certificate chain, or certificate revocation list (CRL), or to two the status of a pending request. For more information about Certificate Services, see <u>Certificate Services</u> , because the services of the servic	e.m
be the velocities to concluse the contribution for your Web browser, e-mail client, or other program. By using a certificate, you can verify your provide the value of the velocities of the velocities of a pending request. For one also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or intervent the states of a pending request. For once information about Certificate Services, see <u>Certificate Services Documentation</u> . ************************************	t, e-mail client, or other program. By using a cottificate, you can verify your d encrypt messages, and, depending upon the type of certificate you request, ity (CA) certificate, certificate chain, or certificate revocation list (CRL), or to e Services Documentation: ■ Tradvanced certificate request. ■ Tradvanced certificate request. ■ Tradvanced certificate request.	tex des values to be request a certificatio for your Web prevent , e-mail chert, or other program. By using a certificate you can will your endown other socurity tests. to use a also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to the status of a pendang request web rover the Web, sign and encrypt messages, and, depending upon the type of certificate you request, or more information about Certificate Services, see <u>Certificate Services Documentation</u> <b>The status of a certificate or counter</b> <b>The status of certificate or counte</b>	We there the to request a certificate for your Web browser, a-mail clert, or other program. By using a certificate, you can writely competed 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 write the site of a pending report.         You can also use this Web site to download a certificate sances: Documentation:         You can also use this Web site to download a certificate sances: Documentation:         You can also use this Web site to download a certificate sances: Documentation:         You can also use this Web site to download a certificate sances: Documentation:         You can also use this Web site to download a certificate sances: Documentation:         You can also use this Web site to download a certificate sances: Documentation:         You can also use this Web site to download a certificate request:         You can also use this Web site to download a certificate sances: Documentation:         You can also use this Web site to download a certificate sances: Documentation:         You can also use this Web site to download a certificate request:         Download a LA certificate prove and the sance of th	
ou can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or we the status. The rore information about Certificate Services, see <u>Certificate Services Documentation</u> <b>Second as CA</b> <b>Second as CA</b> <b>Certificate Certificate Certificate request</b> <b>Deveload a CA</b> <b>Certificate Service</b> <b>Second as CA</b> <b>Certificate Service</b> <b>Second Certificate</b> <b>Second Certificate</b> <b>Second Certificate</b> <b>Second Certificate</b> <b>Second Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b> <b>Second</b>	It (CA) certificate, certificate chain, or certificate revocation list (CRL), or to e Services Documentation ■ Internet ■ Tradvanced certificate request。 ■ Internet ■ Internet	au can also use this Web site to download a certificate subtrivity (CA) certificate, certificate chain, or certificate revocation list (CRL), or to wre information about Certificate Services, see Certificate Services Documentation Provide States Provide States Provide States Developed a CA certificate request Developed a CA certificate chain, or CRS Provide States Provide States Provi	You can also use this Web state to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to whe the states and certificate Services, see <u>Certificate Services Documentation</u> . <b>Server at sets:</b> Nature the attention of the services of the services of the services Documentation <b>Server at sets:</b> Nature the attention of the services of the services of the services Documentation <b>Server at sets:</b> Nature the attention of the services of the servic	t.,
The request a Certificate Service Service's Documentation	► Services Documentation	or more information about Certificate Services, see <u>Certificate Services Documentation</u> Request a certificate product of December of December Developed a CA certificate request Developed a CA certificate chain of CEL	For reversion about Certificate Services, see <u>Certificate Services Documentation</u> Financial Cartificate Deversion of a percent contractor request Deversion of a CA certificate request E F Request a Certificate j 頁面中,按一下advanced certificate requests Microsoft Certificate Services Microsoft Internet Legienze E Request a Certificate Microsoft Certificate Services - widelese Request a Certificate Select the certificate Services - widelese Request a Certificate Select the certificate Services - widelese Request a Certificate S	
Setera stask: Marging Standard and Analysing contificate request: Deverleded a CA contricate Contricate chain or CER. Image: Standard a CA contricate Contricate chain or CER. Image: Standard a CA contricate Contricate chain or CER. Image: Standard a CA contricate Contricate chain or CER. Image: Standard a CA contricate Contricate chain or CER. Image: Standard a CA contricate Contricate chain or CER. Image: Standard a CA contricate Contricate chain or CER. Image: Standard a CA contricate Contricate chain or CER. Image: Standard a Cantificate Internet Laplance Image: Standard Internet Laplance I	-⊤advanced certificate request。	Prevent task: Consult of 3 Deciminate Decimicate and the status of 3 Deciminate contribute request Decimicate a T_A certificate contribute request Decimicate a T_A certificate _ deciminate contribute request Contribute Status of 3 Deciminate request Deciminate Status of 3 Deciminate Status of 3 Decimination of 3 Deciminate Status of 3 Decimin	★ Int a task: May be according to a period of a period of a conduct of the request. Developed a CA conditions. Conditions request Developed a CA conditions. Conditions request E F Request a Certificate _ 頁面中,按一下advanced certificate request. Whereast Conditions The request Whereast Certificate Services Whereast Inspirest Whereast Certificate Services Whereast Inspirest May be were services a Certificate request. E Request a Certificate Services Whereast Inspirest E Conditions Services Whereast Intervent Inspirest May be were services a Certificate Services Whereast Intervent Inspirest E Conditions Services Intervent Inspirest E Services Inspirest E Services Intervent Inspirest E Services Intervent Inspirest E Services Intervent Inspirest E Services Intervent Inspirest E Services Inspirest E Services Intervent Inspirest E Services Intervent Inspirest E Services Inspirest E	
● Internet 「Request a Certificate」頁面中,按一下advanced certificate request。 Microsoft Certificate Services — Microsoft Internet Implement Sets Wer Provides Total Services — Wireless Wicrosoft Certificate Services — wireless Select the certificate type: User CattleCode Select the certificate request Wireless	- Tradvanced certificate request.	● Request a Certificate」頁面中,按一下advanced certificate request。 Microsoft Certificate Services - Microsoft Internet Logianer Col Wer Newton Took We	● Internet 王「Request a Certificate」頁面中,按一下advanced certificate request。 Microwoff Certificate Services - Microwoff View Hole Comparison - Worker Took Hole Comparison - Worker - Worker - Worker Microwoff Certificate Services - Workers Request a Certificate Select the certificate Spec Liser CodeRector Or submit an advanced certificate request	
● Internet 「Request a Certificate」頁面中,按一下advanced certificate request。 Microsoft Certificate Services Microsoft Internet Explorer © Wee Pavotes Took Hep © Wee Pavotes T	- 下advanced certificate request。	■ Internet	■ Internet E 「Request a Certificate」頁面中,按一下advanced certificate request. Microsoft Certificate Services Microsoft Internet Laplorer ● Microsoft Certificate Services - Wieless Microsoft Certificate Services - Wieless Request a Certificate type: User Catherents Or wurmit an advanced certificate request.	
Microsoft Certificate Services - Microsoft Internet Explorer  Microsoft Certificate Services - Microsoft Internet Explorer  Microsoft Certificate Services - Microsoft Internet Explorer  Microsoft Certificate Services - Wireless  Microsoft Certificate Services - Wireless  Microsoft Certificate type: User Codditions  If submit an advanced certificate request.		Microsoft Certificate Services - Microsoft Internet Explorer  Cot Were Preventes Tools - Microsoft Internet Explorer  Cot Very Preventes Tools - Microsoft Internet Explorer  Cot Services - Wroless  Here	Microsoft Certificate Services - Microsoft Internet Lxplorer           Microsoft Certificate Services - Microsoft Internet Lxplorer           L the Wew Favorate's Tools / Hep           Atternet for the favorate internet Lxplorer           Microsoft Certificate Services - Wireless           Microsoft Certificate type:           User Certificate type:           User Certificate type:           User Certificate type:           User Certificate request.	
In Edg. Wew Pavorkis' Took / Help	Herr	aces Yew Pewerkes Took Help Contract age I help Contract age I help (10.77.244.198/contract age I help (10.77.244.198/	Image: State         State         Yew         Perverties         Tooks         Height         Image: State         Height         Image: State         Height	5
Microsoft Certificate Services - Wireless Request a Certificate type: User Capilicate Or submit an advanced certificate request.	Herr	Microsoft Certificate Services wireless Here Request a Certificate relect the certificate type: User Cadificate relect the certificate request.	Microsoft Contificate Services - wireless         H           Microsoft Contificate Services - wireless         H           Request a Certificate         Select the contificate type:         User Contificate type:           User Contificate         Or submit an advanced certificate request.         H	
Microsoft Certificate Services wireless Request a Certificate Select the certificate type: User CodHicate Or submit an advanced certificate request.	Hem	Microsoft Cartificate Services – wireless Han tequest a Certificate islect the certificate type: User Cathlecate in submit an advanced certificate request.	Alicrosoft Contificate Services wireless     H       Request a Certificate     Select the certificate type:       User Contificate     User Contificate request.	
Request a Certificate Select the certificate type: User CadHicate Or submit an advanced certificate request.		Request a Certificate type: User CasHireate resubmit an advanced certificate request.	Request a Certificate type: User Cartificate Or submit an advanced certificate request	om
Select the certificate type: User CadHicate Or submit an advanced certificate request.		elect the certificate type: User Cathicette In submit an <u>advanced certificate request</u>	Select the certificate type: User Cashicate Or submit an advanced certificate request	
User Cadificate Or submit an advanced certificate request.		User Cadificate request.	User Castificate Or submit an advanced certificate request.	
Dr submit an <u>advanced certificate request</u>		r submit an advanced certificate request	Or submit an advanced certificate request	

 4. 在「高級證書請求」頁中,單擊「建立」並將請求提交到此CA。這會將您帶到「高級證書請 求」表單。

Internet

http://10.77.244.198/certsrv/certrgad.asp

Microsoft Certificate Services - Microsoft Internet Explorer		
e Edit View Pavorites Tools Help		1
2005 a) Http://10.77.244.196/certsrv/certrgad.asp		💌 🔁 G
<b>ficrosoft</b> Centificate Services - wireless		Home
dvanced Certificate Request		
he policy of the CA determines the types of certificates you can request. Click on	e 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 ft PKCS #7 file.	ile, or submit a renewal request by	using a base-64-encoded
Request a certificate for a smart card on behalf of another user by using the sm	art card certificate enrolment stati-	on.
Note: You must have an enrollment agent certificate to submit a request on behalf of another of	iser.	

- 5. 在「高級證書請求」表單中,選擇Web Server作為「證書模板」。然後,為此裝置證書指定 一個名稱。此範例將憑證名稱用作ciscowlc123。根據您的要求填寫其他標識資訊。
- 6. 在Key Options部分下,選擇Mark Keys as Exportable選項。有時,此特定選項會灰顯,如果 您選擇Web伺服器模板,則無法啟用或禁用。在這種情況下,從瀏覽器選單中按一下上一步 ,返回一頁,然後再次返回此頁。這一次,「將金鑰標籤為可匯出」(Mark Keys as Exportable)選項應可用。

Microsoft Certificate Services - Microsoft Internet Explorer	
e Edit View Pavorites Tools Help	4
State . On a Conference of Seventers of Several Second	
http://10.77.244.198/certsry/certrons.ap	v 📑 😡
Microsoff Certificate Services miteless	Home
dvanced Certificate Request	
ertificate Template:	
Web Server 🛛	
lentifying Information For Offline Template:	
Name: ciscowic123	
6-Mail	
Company: cisco	
Department:	
Čitv.	
State	
Country/Region	
ey Options:	
CRR Advancet DRA Schoool Contemptie Draide at	
Carr. Imcrosof Rox a Channel Cryptographic Provider	
New Wayses to Exchange	
Ney Size: 1024 Mac10304 (Within Rey sale) Did Sole 2011 Sole 1000 (	
Automatic key container name     O User specified key container name	
Emot keys as exportable	
Enable strong private key protection	
Store certificate in the local computer certificate store	
Charace the audition to the local associates stars	Tobury t

7. 配置所有其他必要的欄位,然後按一下Submit。

Microsoft Certificate Services - Microsoft Internet Explorer	
Fån Edit Væve Favoritæs Tools Help	4
🔇 Back + 💿 - 🖹 📓 🐔 🔎 Search 🦅 Pavortes 🤣 🎯 - چ 🖼 🦓	
43++si 🐌 http://10.77.244.198/certarv/certrgna.asp	🖂 🔁 G
Create new key set	
CSP: Microsoft RSA SChannel Cryptographic Previder 🛩	
Key Usager. () Exchange	
Key Size: 1024 Min: 064 (ceremon key size: 512 1024 2049 4088 5192 10084.)	
Automatic key container name	
Mark keys as exportable Export keys to file	
Enable strong private key protection	
Store the certificate in the local computer centricate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.	
Request Format: O CMC	
Hash Algorithm: SHA-1 M Only used to sign request.	
Save request to a file	
Attributes:	
Friendly Name:	
Submit >	

8. 在下一個視窗中按一下**Yes**以允許證書請求進程。

Potenti	al Scripting Violation
	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
	Yes No

9. 出現「Certificate Issued(已頒發的證書)」視窗,指示成功的證書請求過程。下一步是將頒 發的證書安裝到此PC的證書儲存區。按一下「Install this certificate」。

Microsoft Certificate Services - Microsoft Internet Explorer	
ddress 🕘 http://10.77.244.198/certSrv/certFrsh.esp	- E
Microsoft Certificate Services - wireless	Hem
Certificate Issued	
The certificate year representatives issued to you	
Intercenting of the participation of the state of the you.	
( ten install this certificate )	
· · · · · · · · · · · · · · · · · · ·	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。	- O Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer File Eds View Favorities Tools Help	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer Res Et View Pavortes Tools Nep Address @ http://10.77.244.198/JontSrv/GetFinge.agp Microsoft Certificate Services - wire/ess	internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services Microsoft Internet Explorer File Edit Wee Favorites Tools Help Favorites Attorneoft Certificate Services - wirefees Certificate Installed	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services Microsoft Internet Explorer No. Edit View Favorites Toole Help Address @ Migruff10.77.244 198/JostSry/certingen.asp Microsoft Certificate Services - wire/west	- Cinternet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services _ Microsoft Internet Explorer Pre_Edt_Vees _ Pavorites _ Tools _ Netp Address	internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services Microsoft Internet Explorer File Edit West Paverkes Tools Help TATA Active:      Http://10.77.244.199/Jeetsvy/certrepn.asp     Microsoft Certificate Services - westers     Certificate Installed     Your new certificate has been successfully installed.	i internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services Microsoft Internet Explorer Ne Ext Wee Favorites Tools Help 1999 Astronomic Certificate Services - Wireless Certificate Installed Your new certificate hes been successfully installed.	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer Not the Data New Favorities Toole New	internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer File EX Wee Favorites Tools Help Active: 副Http://10.77.244.199/JeetSrv/Getringb.asp Afformative Certificate Services - Weekess Certificate Installed Your new certificate has been successfully installed.	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer Rise Ext Veet Favories Tools 1980	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer File Edk Weie Favorites Toole Help Address Magniff Certificate Services - Weiers Afferend Certificate Installed Your new certificate has been successfully installed.	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer File Ext Vee Favories Tools Hep Address Map-UTID.77.244.198/Dentary/Dentar	Linternet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services Microsoft Internet Explorer Pre Ex View Favorites Tools Help for the Address Address Microsoft Certificate Services → Weekees Certificate Installed Your new certificate has been successfully installed.	Linternet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services Microsoft Internet Explorer Re Ex Wee Favories Tools Help	i i i internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Laplorer Net D2 Veer Favories Tools Teep Net D2 Veer Favories Tools Teep Net D2 Veer Favories Tools Teep Net D2 Veer Favories Tools Teep Certificate Installed Your new certificate has been successfully installed.	Linternet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer Ne E2 Wee Pavortes Tools Teep Active Pavortes Tools Teep Active Pavortes Tools Teep Active Certificate Services - Weekees Certificate Installed Your new certificate has been successfully installed.	i internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer Reference Tools _ Help Afficeated Certificate Services - wireless Certificate Installed Your new certificate has been successfully installed.	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer Refer @ Mapulato.77.244.1990erfory/certrage.app Microsoft Certificate Services - wireless Certificate Installed Your new certificate has been successfully installed.	Internet
新證書已成功安裝到從中生成請求到CA伺服器的PC。 Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Weekes Certificate Installed Your new certificate has been successfully installed.	i internet

11. 下一步是將此證書從證書儲存區作為檔案匯出到硬碟。此憑證檔案稍後會用於下載憑證到 WLC。若要從證書儲存匯出證書,請開啟Internet Explorer瀏覽器,然後按一下**工具>** Internet選項。

Internet

Done 🚳

about:blank - Microsoft Internet Explorer	
File Edit View Pavorities Tools Help	
Address about blank. Mail and News	a 🛃 😽
Pop-up Blocker  Manage Addi-ons	
Synchronize	
Windows Update	
Windows Messenger	
Sun Java Console	
Internet Options	
	×
Enables you to change settings.	

12. <u>按一下「**Content > Certificates**」,以前往預設會安裝憑證的憑證儲存區。</u>

Internet Options
General Security Privacy Content Connections Programs Advanced
Content Advisor
Ratings help you control the Internet content that can be viewed on this computer.
Enable Settings
Certificates
Use certificates to positively identify yourself, certification authorities, and publishers.
Clear SSL State Certificates Publishers
Personal information
AutoComplete stores previous entries and suggests matches for you. AutoComplete
Microsoft Profile Assistant stores your My Profile
OK Cancel Apply

13. 裝置證書通常安裝在Personal證書清單下。在此,您應該看到新安裝的證書。選擇憑證並按 一下Export。

	5				?
Intended pur	pose:	All>			~
Personal	other People	Intermediate Certification	Authorities Trust	ed Root Certification	< >
Issued 1	0	Issued By	Expiratio	Friendly Name	
2 ciscov	wlc123	wireless	1/25/2010	<none></none>	
Import	Expo	rt Remove		Advance	ed
Import		Remove		Advance	ed
Import Certificate Server Auto	Expo intended pur hentication	rt Remove		Advance	ed
Import Certificate Server Aut	Expo intended pur hentication	rt Remove		Advance	ed
Import Certificate Server Aut	Expo intended pur hentication	rt Remove		Advance	ed

14. 在以下視窗中按一下Next。在「Certificate Export Wizard」視窗中選擇Yes, export the private key選項。按「Next」(下一步)。

Certificate Export Wizard	$\mathbf{\times}$
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
O you want to export the private key with the certificate?	
No, do not export the private key	
< Back Next > Cancel	

15. 選擇匯出檔案格式為.PFX,然後選擇Enable strong protection選項。按「Next」(下一步)。

Certificate Export Wizard	$\mathbf{X}$
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
Include all certificates in the certification path if possible	
<ul> <li>Personal Information Exchange - PKCS #12 (.PFX)</li> <li>Include all certificates in the certification path if possible</li> <li>Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)</li> </ul>	
Delete the private key if the export is successful    	Cancel
I6. 在「密碼」視窗中,輸入密碼。此範例使用 <b>cisco</b> 作為密碼。	
Certificate Export Wizard	×

Trans and an and a second seco		
Type and confirm a password.		
Password:	 r	
Confirm password:	 -	
*******		

17. 將證書檔案(.PFX檔案)儲存到硬碟。按一下「**Next**」,然後成功完成匯出程式。

la de la companya de
you want to export
123.pfx Browse
< Back Next > Cancel
Completing the Certificate Export         Wizard         You have successfully completed the Certificate Export         You have specified the following settings:         File Name       C:\Ope         Export Keys       C:\Ope         Include all certificates in the certification path       No         File Format       Person

## <u>將裝置證書下載到WLC</u>

現在,WLC裝置證書可以作為.PFX檔案使用,下一步是將該檔案下載到控制器。Cisco WLC僅接受 .PEM格式的證書。因此,您需要首先使用openSSL程式將.PFX或PKCS12格式檔案轉換為PEM檔 案。

#### 使用openSSL程式將PFX格式證書轉換為PEM格式

您可以將憑證複製到任何安裝了openSSL的PC,以將其轉換為PEM格式。在openSSL程式的bin資 料夾中的OpenssI.exe檔案上輸入以下命令:

**注意**:您可以從OpenSSL網站<u>下載</u>openSSL。

openssl>**pkcs12 -in** *ciscowlc123.pfx* -**out** *ciscowlc123.pem* !--- *ciscowlc123 is* the name used in this example for the exported file. !--- You can specify *any* name to your certificate file. Enter Import Password : **cisco** !--- This is the same password that is mentioned in step 16 of the previous section. MAC verified Ok Enter PEM Pass phrase : **cisco**  !--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco

證書檔案將轉換為PEM格式。下一步是將PEM格式裝置憑證下載到WLC。

**注意:**在此之前,您需要在要從中下載PEM檔案的PC上安裝TFTP伺服器軟體。這台電腦應該能連 線到WLC。TFTP伺服器的當前目錄和基目錄應指定PEM檔案的儲存位置。

<u>將轉換後的PEM格式裝置證書下載到WLC</u>

此範例說明透過WLC的CLI下載程式。

- 1. 登入控制器CLI。
- 2. 輸入transfer download datatype eapdevcert命令。
- 3. 輸入**transfer download serverip** *10.77.244.196* 命令。10.77.244.196是TFTP伺服器的IP地址。
- 4. 輸入**transfer download filename** *ciscowlc.pem* 指令。ciscowlc123.pem是本範例中使用的檔案 名稱。
- 5. 輸入transfer download certpassword命令以設定憑證的密碼。
- 6. 輸入transfer download start命令檢視更新的設定。然後,當系統提示確認當前設定並開始下載 過程時,請回答y。此範例顯示download指令輸出: (Cisco Controller) >transfer download start

Mode		TFTP
Data	Туре	Vendor Dev Cert
TFTP	Server IP	10.77.244.196
TFTP	Packet Timeout	6
TFTP	Max Retries	10
TFTP	Path	
TFTP	Filename	ciscowlc.pem

This may take some time. Are you sure you want to start? (y/N) y TFTP EAP CA cert transfer starting. Certificate installed. Reboot the switch to use the new certificate. Enter the reset system command to reboot the controller. The controller is now loaded with the device certificate.

7. 輸入reset system指令以重新啟動控制器。控制器現在載入了裝置證書。

#### 將PKI的根證書安裝到WLC中

現在裝置證書安裝在WLC中,下一步是將PKI的根證書從CA伺服器安裝到WLC。執行以下步驟:

1. 從與CA伺服器具有網路連線的PC轉到http://<CA伺服器的IP地址>/certsrv。以CA伺服器管理 員身份登入。



2. 按一下「Download a CA certificate, certificate chain, or CRL」。

Microsoft Certificate Services - Microsoft Internet Explorer	
in Edt Ven Favortes Took telp	A1
62xxxx au http://10.77.244.196/certsrv/	🗹 🎦 Go
Microsoft Centificate Strates	Home
Nelcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certif dentity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the ty perform other security tasks.	ficate, you can verify your pe of certificate you request,
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate view the status of a pending request.	e revocation list (CRL), or to
For more information about Certificate Services, see Certificate Services Documentation.	
Select a task: Request a certificate View the stews of a pending certificate request Download a CA certificate, certificate chain, or CRL	
	1
	Internet
E結果頁面中,您可以在 <b>CA證書</b> 框下看到CA伺服器上可用的當前CA證 <sup>:</sup>	書。選擇DER作為

 在結果頁面中,您可以在CA證書框下看到CA伺服器上可用的當前CA證書。選擇DER作為 Encoding方法,然後按一下Download CA certificate。

Microsoft Certificate Services - Microsoft Internet Explorer	
Får Edt Verv Pavertis Tools Help	4
Addimen 🕘 http://10.77.244.198/certsev/certcarc.asp	🛁 🔁 Go
Microsoft Certificate Services - wireless	Home
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Current (wireless)	
Encoding method:	
OER	
O Base 64 Download CA certificate	
Download CA certificate chain	
Download latest base CRL	
Downoad latest detta CRC	
	Internet

- 4. 將憑證另存為.cer檔案。此示例使用certnew.cer作為檔名。
- 5. 下一步是將.cer檔案轉換為PEM格式並下載到控制器。若要執行這些步驟,請重複在<u>將裝置憑證下載到WLC</u>一節中說明的相同程式,並執行以下變更:openSSL "-in"和"-out"檔案是certnew.cer和certnew.pem。此外,此過程不需要PEM密碼或匯入密碼。此外,用於將.cer檔案轉換為.pem檔案的openSSL命令為:x509 -in certnew.cer -inform DER -out certnew.pem outform PEM在將轉換的PEM格式裝置憑證下載到WLC</u>一節的步驟2中,將憑證下載到WLC的命令如下:(思科控制器)>transfer download datatype eapcacert要下載到WLC的檔案為certnew.pem。

您可以透過控制器GUI驗證憑證是否安裝在WLC上,如下所示:

 在WLC GUI上,按一下「Security」。在Security頁面中,從左側顯示的任務中按一下 Advanced > IPSec Certs。按一下「CA Certificate」以檢視已安裝的CA證書。以下是範例
 :



・若要確認裝置憑證是否安裝在WLC上,請在WLC GUI上按一下「Security」。在Security頁面中,從左側顯示的任務中按一下Advanced > IPSec Certs。按一下ID Certificate以檢視安裝的裝置證書。以下是範例

🗿 wic2006 - Microsoft Inter	net Explorer									×
File Edit View Favorites	Tools Help									<b>R</b>
ababa								guration	Ping Logout Refr	resh
cisco	MONITOR	WLANS		W]RELESS	SECURITY	MANAGEMENT	COMMANDS	неце		
Security	ID Certific	ate:			$\smile$				New	1
T AAA	Name		Ya	ilid Period						
General RADIUS Authentication	bsnSslEapD	)evCert	Fin	om 2008 Jan 24	æh, 12:18:31 G	MT Until 2010 Jar	n 23nd, 12:18:31	3		
Accounting TACACS+ LDAP										
Local Net-Users MAC Filtering Disabled Clients										
User Login Policies AP Policies										
E Local EAP										
Priority Order										
E Access Control Lists										
Vireless Protection Policies										
F Web Auth										
Advanced     FCIDS     Sensors     Shunned     Clients      ElSes Centre										
ID Certificate										
ē)								6	🔵 Internet	

## 生成客戶端的裝置證書

由於裝置憑證和CA憑證已安裝在WLC上,下一步是產生使用者端的這些憑證。

執行這些步驟,以便為客戶端生成裝置證書。使用者端會使用此憑證對WLC進行驗證。本文檔介紹 為Windows XP專業版客戶端生成證書所涉及的步驟。

 從需要安裝證書的客戶端轉到http://<CA伺服器的IP地址>/certsrv。以域名\使用者名稱登入到 CA伺服器。使用者名稱應該是使用此XP電腦的使用者的名稱,該使用者應該已經配置為CA伺 服器所在域的一部分。

Connect to 10.	77.244.198	<b>?</b> 🔀
		AN AN
Connecting to 10.	.77.244.198	
User name:	🖸 wireless\user2	<b>~</b>
Password:		
	Remember my passwo	rd
	ОК	Cancel
ち倖 <b>请水<b>应音</b>。 Microsoft Certificate Services - Microsoft Inte</b>	rnet Explorer	
File Edit View Pavorites Tools Help		
lddress 🕘 http://10.77.244.198/certsrv/		<u> </u>
Microsoft Certificate Services wireless		Heme
Welcome		
Use this Web site to request a certificate fidentity to people you communicate with or perform other security tasks. You can also use this Web site to download view the status of a pending request. For more information about Certificate Security Certificate Certificate Security Certificate Security Certificate Certif	or your Web browser, e-mail client, or other program. By using a ce ver the Web, sign and encrypt messages, and, depending upon the of a certificate authority (CA) certificate, certificate chain, or certific rvices, see <u>Certificate Services Documentation</u> .	artificate, you can verify your ⊧ type of certificate you request, ate revocation list (CRL), or to
a		Internet

3. 在「Request a Certificate」頁面中,按一下advanced certificate request。

Microsoft Certificate Services - Microsoft Internet Explorer	E 🖬 🔀
Fée, Edit: View Favorities' Tools Help	
753/coss a) http://10.77.244.198/certsrv/certrups.asp	🛁 🛃 Go
	<u></u>
Microsoff Certificate Services wireless	Home
Request a Certificate	
Select the certificate type:	
User Cartificate	
On submit an advanced certificate request.	
	····
C http://10.77-244.198/cettprv/cettglad.asp	Internet

4. 在「高級證書請求」頁中,單**擊「建立」並將請求提交到此CA**。這會將您帶到「高級證書」 申請表。

H		
Mi	At Certificate Services - Microsoft Internet Explorer	
	Vern Pavorites Tools Help	
	Mtp://10.77.244.190/cettsrv/certrqad.asp	Sec.
	r Centricate Services - Winness	Home
1	ed Certificate Request	
ĺ	· · ·	
	cy of the CA determines the types of certificates you can request. Click one of the following options to:	
(	te and submit a request to this CA.	
ŝ	nit 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
	<u>S#7hie</u>	
ł	lest a certificate for a smart card on behalf of another user by using the smart card certificate enrolment station.	
	You must have an enrollment agent certificate to submit a request on behalf of another user.	
		ernet
	dveneed Cartificate request,丰富中,然「Cartificate Templete,下拉潔買中	い現世

5. 在「Advanced Certificate request」表單中,從「Certificate Template」下拉選單中選擇 User。在Key options部分下,選擇以下引數:在Key Size欄位中輸入金鑰大小。本示例使用 1024。選中Mark Keys as Exportable選項。

Microsoft Conti	ficate Services - Microsoft Internet Explorer	
Pile Edit View	Pavorites Took Help	
iddresis 🔕 http://10	. 77.244.190/certsrv/certrgna.asp	- E) a
Microsoff Certific	tate Services whereas	Home
Advanced Ce	rtificate Request	1
Certificate Temp	slate:	
	Basic EFS 💌	
	Basic EFS	
Key Options:	User	
000	Create new key set	
Key Heare	Exchange Cryptographic Provider VI.0	
Vey Size:	1004 Min: 294 (common burging \$12,4024,2048,0008,0422,18204.3	
Key alze.	0.24 Max 10004 (Weining and 214 Jose 1000 Line and 10000 /	
	Automatic key container name     Over specified key container name	
	Export keys to file	
	Enable strong private key protection	
	Store certificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not instead the root GA's certificate. You must be an administrator to generate or use a key in the local machine store.	
Additional Optic	05:	
Request Format:	CMC OPKCS10	
Hash Algorithm	SHA-1 v Cnly used to sign request.	
	Save request to a file	
Attributes:		
Done	Den Carra	Internet

6. 配置所有其他必要的欄位,然後按一下Submit。

a sectored estimate setties - sectored internet experies	
File Edit View Pavorites Tools Help	
🔾 Sad. • 🜍 - 📧 🗟 🐔 🔎 Search 🤺 Pavorites  🚱 🖓 🚃 🖄	
/di/ress @ http://10.77.244.198/certary/cerbrgna.asp	💙 🔂 GO
Create new key set Use existing key set	
CSP: Microsoft RSA SChannel Cryptographic Previder 🌱	
Kay Usage: 🛞 Exchange	
Key Size: 1024 Min: 004 (common key size: 512 2029 2088 6192 10086 5192 10089 3	
Automatic key container name	
Mark keys as exportable	
Export keys to file	
Enable strong private key protection	
Store certificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root GA's certificate. You must be an administrator to generate or use a key in the local reactions store.	
Additional Options:	
Request Format: O CMC	
Hash Algorithm: SHA-1 Conly used to sign request.	
Hash Algorithm: SHA-1 Conly used to sign request.	
Hash Algorithm: SHA-1 Confy used to sign request.	
Hash Algorithm: SHA-1 Only used to sign request. Save request to a file Attributes:	
Hash Algorithm: SHA-1 Conly used to sign request.	
Hash Algorithm: SHA-1 Only used to sign request. Save request to a file Attributes: Friendly Name: Submit >	
Hash Algorithm: SHA-1 Only used to sign request. Save request to a file Attributes:	

7. 現在將根據請求生成客戶端的裝置證書。按一下「Install the certificate」,將憑證安裝到憑證 庫中。

Microsoft Certificate Services - Microso	ft Internet Explorer	-		
File Edit View Favorites Tools Help				A¥
Address all http://10.77.244.190/certary/certfinah.	sp			💌 🔁 😡
Microsoff Certificate Services - wireless				Home
Certificate Issued				
The certificate you requested was is	ued to you.			
ITEM INCOMENTATION				
issue install this certificate				
				<u>M</u>
			Inter	net
您應該能夠找到客戶端的	IE瀏覽器上Tools >	Internet Options >	Content > Certificate	s下的
Personal certificate清單	中安裝的客戶端裝置	證書。		
Certificates				? X
Intended purpose:	<all></all>			~
Personal Other Peopl	e Intermediate Certi	fication Authorities	Trusted Root Certificat	ior < >
_Issued_To	Issued By	Expirati	o Friendly Name	_

	<b>200</b> 1234	wireless	1/25/2009	<none></none>		
	·					
_						-
	Import	Export Remove			Advanced	٦
						-
	Certificate inter	nded purposes				
	in an unbin of File (	Tuckers				
6	incrypting rile :	System		_		
					View	
						_
					Close	J

客戶端的裝置證書已安裝在客戶端上。

生成客戶端的根CA證書

下一步是產生使用者端的CA憑證。從客戶端PC完成以下步驟:

 從需要安裝證書的客戶端轉到http://<CA伺服器的IP地址>/certsrv。以域名\使用者名稱登入到 CA伺服器。使用者名稱應該是使用此XP電腦的使用者的名稱,該使用者應該已經配置為CA伺 服器所在域的一部分。

Connect to 10.77	. 244.198 🔹 💽 🔀
Connecting to 10.77	.244.198
User name:	🛃 wireless\user2
Password:	
	Remember my password
	OK Cancel

2. 在結果頁面中,您可以在**CA證書**框下看到CA伺服器上可用的當前CA證書。選擇**Base 64**作為 Encoding方法。然後,按一下**Download CA certificate**,將該檔案另存為.cer檔案到客戶**端的** PC。此示例使用**rootca.cer**作為檔名。

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Pavorites Tools Help	
Address Mtpp://10.77.244.198/certsrv/certcarc.asp	🛩 🔁 Go
	10
Alteroyoff Certificate Services Vereines	Heme
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Current (wireless)	
Encoding method	
ODER	
Base 64	
Download CA certificate	
Download CA certificate chain	
Download latest base CRL	
Download latest delta CRL	
	Internet
位于中,收入了,收入保存的人就会中并对它后带的就会做方面。	

3. 接下來,將以.cer格式儲存的CA證書安裝到客戶端的證書儲存中。按兩下rootca.cer檔案,然 後按一下Install Certificate。

General Details Certification Path									
Certificate Information									
<ul> <li>This certificate is intended for the following purpose(s):</li> <li>All issuance policies</li> <li>All application policies</li> </ul>									
Issued to: wireless									
Issued by: wireless									
Valid from 1/23/2008 to 1/23/2013									
Install Certificate Issuer Statement									

4. 按一下「Next」將憑證從使用者端的硬碟匯入憑證儲存區。

Certificate Import Wizard		$\times$
	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next.	
	< Back Next > Cancel	

5. 選擇Automatically select the certificate store based on the type of certificate,然後按一下 Next。

Certificate stores are system areas where certificates are kept.   Windows can automatically select a certificate store, or you can specify a location for   Automatically select the certificate store based on the type of certificate   Place all certificates in the following store   Certificate store:     Prowse      Cancel   Rest   Mext >     Certificate Import Mizerd   Sompleting the Certificate Import Curve successfully completed the Certificate Import Content Certificate Store Selected Automatically determined by [Certificate Content Certificate Certificate Import Content Certificate Certificate Import Content Certificate Certificate Content Certificate Certificate Certificate Content Certificate Certifica	Certificate Import Wizard	
Windows can automatically select the certificate store based on the type of certificate         Dec all certificates in the following store         Certificate store:         Provese             Cancel             Sec T Finish URER [Import] RETS             Certificate Import Wizard             Sec Support             Certificate Store:             Certificate Import Wizard             Support             Certificate Store:             Certificate Store:             Support             Support             Support             Certificate Import Wizard             Support             Certificate Store:             Certificate Store:             Certificate             Certificate             Certificate:             Certificate:             Certificate:	Certificate Store Certificate stores are system	m areas where certificates are kept.
を下「Finish」以完成「Import」程式。 Certificate Import Wizard Completing the Certificate Import Mizard Completing the Certificate Import Mizard Counce Study completed the Certificate Import Mizard. Sou have successfully completed the Certificate Import Mizard.	Windows can automatically select t  Automatically select t  Place all certificates in Certificate store:	select a certificate store, or you can specify a location for the certificate store based on the type of certificate in the following store Browse
<image/>	了一下「Finish」以完成「Import」 Certificate Import Wizard	<pre>&lt; Back Next &gt; Cancel </pre>
		Completing the Certificate Import Wizard You have successfully completed the Certificate Import wizard. You have specified the following settings: Certificate Store Selected Automatically determined by t Content Certificate

7. 預設情況下,CA證書安裝在客戶端IE瀏覽器中工具> Internet選項>內容>證書下的「受信任的 根證書頒發機構」清單下。以下是範例 :

1

rtificates				?
tended purpose: </th <th><b>₩</b>&gt;</th> <th></th> <th></th> <th></th>	<b>₩</b> >			
Intermediate Certification	Authorities Trusted Root C	Certification Aut	horities Trusted Put	× 1
Issued To	Issued By	Expiratio	Friendly Name	-
VeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 3	
🔤 VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 3	
WeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 4	
VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 1	
VeriSign Trust Netw	VeriSign Trust Network	8/2/2028	VeriSign Class 4	
VeriSign Trust Netw	VeriSign Trust Network	5/19/2018	VeriSign Class 1	-
🕮 wireless	wireless	1/23/2013	<none></none>	
Wireless-CA	Wireless-CA	12/18/2012	<none></none>	
Xcert EZ by DST	Xcert EZ by DST	7/11/2009	Xcert EZ by DST	~
Import Export	Remove		Advan	ced.
<pre>Certificate intended purp <all></all></pre>	oses		View	_
				se

WLC和客戶端上都安裝了所需的所有證書,以進行EAP-FAST本地EAP身份驗證。下一步是將WLC配置為本地EAP身份驗證。

## 在WLC上配置本地EAP

在WLC GUI模式中完成以下步驟,以便在WLC上設定本地EAP驗證:

1. 按一下Security > Local EAP。



2. 在Local EAP下,按一下Profiles以配置本地EAP配置檔案。



- 3. 按一下New以建立新的本地EAP配置檔案。
- 4. 為此配置檔案配置名稱,然後按一下**Apply**。在此示例中,配置檔名稱為**Idap**。這會將您引導 到WLC上建立的本地EAP配置檔案。

Wic2006 - Microsoft Inter	net Explorer								
File Edit View Pavorites 1	fools Help								an a
ahaha								nfiguration	Ping   Logout Befresh
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EA	P Profile	s > New					< Da	ck Apply
AAA     General     PADIUS     Authentication     Accounting     TACACS+     LDAP     Local Net Users     MAC Fittering     Disabled Clients     User Login Policies     AP Folicies	Profile Na	me		ld ap					
<ul> <li>Local EAP General Profiles EAP-FAST Parameters Authentication Priority</li> </ul>									
▶ Priority Order									
▶ Access Control Lists									
Wireless Protection Policies									
▶ Web Auth									
▶ Advanced									
() Done							I.I.	1 1 16	) 🕥 Internet
		- 1512							

5. 按一下剛建立的Idap配置檔案,該配置檔案顯示在「本地EAP配置檔案」頁的「配置檔名稱」 欄位下。這會將您帶到本地EAP配置檔案>編輯頁面。

Net 2006 - Microsoft Internet Explorer												
ahaha							Saye Co	nfiguration _ ting	Logout Befresh			
CISCO	MONITOR	WLANS	CONTROLLER	W]RELES	S SECURITY	MANAGEMENT	COMMANDS	HELP				
Security	Local EAF	Profile:	0					New	Apply			
- AAA	Profile Nat	me		LEAP	EAP-PAST	EAP-TLS	PEAP					
General # RADIUS Authentication Accounting # TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Ideo											
<ul> <li>Local EAP General Profiles EAP-FAST Parameters Authentication Priority</li> </ul>												
▶ Priority Order												
▶ Access Control Lists												
Wireless Protection Policies												
▶ Web Auth												
▶ Advanced												
(4)								🛆 🙂 🛛	ternet			

6. 在Local EAP Profiles > Edit頁面上配置特定於此配置檔案的引數。選擇EAP-FAST作為本地 EAP身份驗證方法。啟用Local Certificate Required和Client Certificate Required旁邊的覈取方 塊。選擇Vendor作為證書頒發者,因為本文檔使用第三方CA伺服器。啟用檢查CA憑證旁邊的 覈取方塊,以允許根據控制器上的CA憑證驗證來自使用者端的傳入憑證。如果要對照控制器 上的CA憑證的CN來驗證傳入憑證中的公用名稱(CN),請選中Verify Certificate CN Identity覈 取方塊。預設設定已禁用。若要允許控制器驗證傳入的裝置證書是否仍然有效且尚未過期,請 選中Check Certificate Date Validity覈取方塊。注意:根據控制器上配置的當前UTC(GMT)時 間檢查證書日期有效性。忽略時區偏移。按一下「Apply」。

I wic2006 - Microsoft Inter	net Explorer								
le Edit View Favorites T	ools Help			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1					4
ahaha								nfiguration   ]	2ing   Logout   <u>R</u> efres
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EA	P Profile	s > Edit					< Back	Apply
AAA	Profile Na	ime		ldap					
# RADIUS	LEAP								
Authentication	EAP-FAST	Т		<b>Y</b>					
▶ TACACS+	EAP-TLS								
LDAP.	PEAP								
MAC Filtering	Local Cer	tificate Rec	puired	🗹 Enabled					
Disabled Clients User Login Policies	Client Ce	rtificate Re	quired	C Enabled					
AP Policies	Certificat	e Issuer		Vendor 🐱					
Local EAP	Check ag	painst CA o	rtificates	🗹 Enabled					
Profiles	Verify Ce	stificate CN	Identity	Enabled					
EAP-FAST Parameters Authentication Priority	Check Ce	ertificate De	ite Validity	🗹 Enabled					
Priority Order									
Access Control Lists									
Wireless Protection									
Web Auth									
Advanced									
Advanced									
							1		Totainat

7. 現在,在WLC上建立了採用EAP-FAST身份驗證的本地EAP配置檔案。

Wic2006 - Microsoft Inter	net Explorer Jools Help							
						Sage Co	nfiguration Ping	Logout Befresh
CISCO	MONITOR WLANS	CONTROLLER	W1RELES		MANAGEMENT	COMMANDS	HELP	
Security	Local EAP Profile:	9					New	Apply
- AAA	Profile Name		LEAP	EAP-PAST	EAP-TLS	PEAP		
General     ADIUS     Authentication     Accounting	Idag						•	
TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies								
<ul> <li>Local EAP General Profiles EAP-FAST Parameters Authentication Priority</li> </ul>								
▶ Priority Order								
▶ Access Control Lists								
<ul> <li>Wireless Protection Policies</li> </ul>								
Web Auth								
▶ Advanced								
-							0 -	
Cone Done							🗀 🙂 Ir	ternet

8. 下一步是在WLC上設定EAP-FAST特定引數。在WLC Security頁面中,按一下Local EAP > EAP-FAST Parameters以轉到EAP-FAST Method Parameters頁面。取消選中Anonymous Provision覈取方塊,因為此示例說明了使用證書的EAP-FAST。將所有其他引數保留為預設值。按一下「Apply」。

🕲 wic2006 - Microsoft Intern	et Explorer								
File EdR View Pavorites To	ols Help								
սիսիս									Eing Logout Befresh
CISCO	MONITOR	<u>WLANs</u>	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	EAP-FAS	T Metho	d Parameters		$\overline{}$				Apply
Concrol	Server Ke	y (in hex	)		••••				
	Confirm S	erver Ke	v		••••				
IN TACAOS+	Time to liv	e for the	PAC		10 days	•			
MAC Filtering Disabled Clients	Authority	ID (in he	×)		436973636f				
User Login Policies AP Policies	Authority	ID Inform	nation		Citico A-ID				
T Local EAP Gaparet Profiles EAP-FAST Parameters Reliantication Priority	Anonymo	is Provis	ion		Enable				
E Priority Order									
Access Control Lists     Wireless Protection									
Policies									
E Advanced									
<b>4</b> 1								111	🗳 🖤 Internet

#### 使用LDAP伺服器的詳細資訊配置WLC

現在已使用本地EAP配置檔案和相關資訊配置WLC,下一步是使用LDAP伺服器的詳細資訊配置WLC。在WLC上完成以下步驟:

 在WLC的Security頁面中,從左側任務窗格中選擇AAA > LDAP,以轉到LDAP伺服器配置頁面 。要新增LDAP伺服器,請按一下New。系統將顯示LDAP Servers > New頁面。

💁 wic2006 - Microsoft Inter	net Explorer								
File Edit View Favorites T	Tools Help								AU
abab								nfiguration <u>P</u> in	g   Logout   <u>R</u> efresh
cisco	MONITOR	<u>WL</u> ANS	CONTROLLER	W]RELESS	SECURITY	MANAGEMENT	COMMANDS	не⊾р	
Security	RADIUS	Authentic	ation Server	8	$\smile$			Apply	New
T AAA General T RADIUS	Call Static	on ID Type	9 IP Address	¥					
Authentication	Use AES K	ley Wrap	(Designe)	d for FIPS cust	tomers and req	uires a key wrap	compliant RADIU:	S server)	
TACACS+ LDAP	Network U	lser Man	agement Ser	ver Index	server Addre	ss Port IPSec	Admin Statu:		
Local Net Users MAC Filtering Disabled Clients User Login Policies									
Local EAP									
▶ Priority Order									
▶ Access Control Lists									
Wireless Protection Policies									
Web Auth									
Advanced									
<b></b> 創								i i i i i i i i i i i i i i i i i i i	Internet

2. 在「LDAP伺服器編輯」頁中,指定LDAP伺服器的詳細資訊,例如LDAP伺服器的IP地址、埠 號、啟用伺服器狀態等。從Server Index(Priority)下拉框中選擇一個數字,以指定此伺服器相 對於任何其他已配置的LDAP伺服器的優先順序順序。最多可以配置17台伺服器。如果控制器 無法連線到第一個伺服器,便會嘗試清單中的第二個伺服器,以此類推。在Server IP Address欄位中輸入LDAP伺服器的IP地址。在Port Number欄位中輸入LDAP伺服器的TCP埠 號。有效範圍為1至65535,預設值為389。在User Base DN欄位中,輸入包含所有使用者清 單的LDAP伺服器子樹的可分辨名稱(DN)。例如,ou=組織單位、 ou=next organizational unit和o=corporation.com。如果包含使用者的樹是基本DN,請輸入o=corporation.com或 dc=corporation, dc=com。在本示例中,使用者位於Organizational Unit(OU)Idapuser下,該 使用者又建立為Wireless.com域的一部分。使用者基礎DN應指向使用者資訊(根據EAP-FAST身份驗證方法的使用者憑證)所在的完整路徑。在本示例中,使用者位於基本DN OU=Idapuser、DC=Wireless、DC=com下。有關OU及使用者配置的更多詳細資訊,請參閱本 文檔的在域控制器上建立使用者部分。在「User Attribute」欄位中,輸入包含使用者名稱的使 用者記錄中的屬性名稱。在User Object Type欄位中,輸入將記錄標識為使用者的LDAP objectType屬性的值。通常,使用者記錄有若干objectType屬性值,其中某些值對於使用者是 唯一的,而某些值則與其他對象型別共用。注意:您可以使用LDAP瀏覽器實用程式(作為 Windows 2003支援工具的一部分)從目錄伺服器獲取這兩個欄位的值。此Microsoft LDAP瀏 **覽器工具稱為LDP。**藉助此工具,您可以瞭解此特定使用者的「使用者基礎DN」、「使用者 屬性」和「使用者對象型別」欄位。有關使用LDP瞭解這些使用者特定屬性的詳細資訊,請參 閱本文檔的<u>使用LDP識別使用者屬性</u>部分。如果希望所有LDAP事務使用安全TLS隧道,請從 「伺服器模式」下拉框中選擇**安全**。否則,請選擇None,這是預設設定。在Server Timeout欄 位中,輸入重新傳輸之間的秒數。有效範圍為2到30秒,預設值為2秒。選中Enable Server Status覈取方塊以啟用此LDAP伺服器,或取消選中以禁用。預設值已停用。按一下Apply提交 更改。以下是已使用以下資訊設定的範例

wic2006 - Microsoft Inter	met Explorer							
ahaha	The The					Sage Co	nfiguration   Eing	Logout   Befresh
CISCO	MONITOR WLAM		R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
CISCO Security AAA General RADSUS Authentication Accounting TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP Policies Policies Wireless Protection Policies Web Auth R Advanced	MONITOR WLAN LDAP Servers: Server Index Server Address Port Number User Base DN User Attribute User Object Type Server Mode Server Timeout Enable Server St	Eclit	R WIRELESS	SECURITY	MANAGEMENT		HELP < Back	Apply
2 Done							A 🔿 1	nternet
ᄪᅭᆋᆇᇄᇉᅌᅣ	<b>記器右関I</b> Γ	∧D 伺 服 哭	副的鲜细落	र प≣ ३			署为佴生峒	ī 它 么 ሥ 盗

現在已在WLC上配置有關LDAP伺服器的詳細資訊,下一步是將LDAP配置為優先順序後端資 料庫,以便WLC首先檢視LDAP資料庫以獲取使用者憑據,而不是任何其他資料庫。

#### 將LDAP配置為優先順序後端資料庫

在WLC上完成以下步驟,以便將LDAP配置為優先順序後端資料庫:

 在Security頁面中,按一下Local EAP > Authentication Priority。在Priority Order > Local-Auth頁面中,您可以找到兩個可以儲存使用者憑據的資料庫(Local和LDAP)。要將LDAP作 為優先順序資料庫,請從左側使用者憑據框中選擇LDAP,然後按一下 >按鈕將LDAP移動到右 側優先順序順序框中。

🗃 wic2006 - Microsoft Intern	et Explorer								
He Edit New Pavorites To	xis Help						Saye Co	ofiguration	Ping Logout Befresh
cisco	MONITOR	WLAN5		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Priority O	rder > Lo	ocal-Auth		$\smile$				Apply
General	User Cred	entials							
Authentication Accounting IF TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	LOCAL LDA#	*		ip Imn					
Cocal EAP General Profiles Physics Authentication Priority									
E Priority Order									
E Access Control Lists									
Policies									
E Web Auth									
P: Advanced									
<b>4</b> 0									Internet

2. 此示例清楚地說明在左側框中選擇了LDAP,並且選中了>按鈕。因此,LDAP移到決定優先順 序的右側的框中。選擇LDAP資料庫作為Authentication-priority資料庫。按一下「Apply」。

wic2006 - Microsoft Inte	ernet Explorer								
File Edit View Favorites	Tools Help								<b></b>
ահահո							Save Co	nfiguration	Ping   Logout   Befresh
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Priority 0	rder > Lo	ocal-Auth						Apply
≪ AAA     General     General     RADBUS     Authenicication     Accounting     NTACACS+     LOAP     Load Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies	LOCAL	entials		P WD					
T Local EAP General Profiles EAP-FAST Parameters Authentication Priority									
E Priority Order									
⊨ Access Control Lists									
F: Wireless Protection Policies									
E Web Auth									
F Advanced									
<b>(1)</b>								1	Internet
注音・加里口へ			顕示左右	间的「相	田老白	<b>份</b> 諮田,才	短山 甘	шлл	D位体面如

**注意:如果**LDAP和LOCAL都顯示在右側的「使用者身份證明」框中,其中LDAP位於頂部 ,LOCAL位於底部,則Local EAP會嘗試使用LDAP後端資料庫對客戶端進行身份驗證,並且 如果LDAP伺服器無法訪問,則故障轉移到本地使用者資料庫。如果找不到該使用者,則會拒 絕身份驗證嘗試。如果LOCAL位於頂部,Local EAP將嘗試僅使用本地使用者資料庫進行身份 驗證。它不會故障切換到LDAP後端資料庫。 WLC的最後一步是配置一個WLAN,該WLAN使用Local EAP作為其身份驗證方法,LDAP作為其後 端資料庫。執行以下步驟:

- 1. 在「Controller Main(控制器主選單)」中,按一下「**WLANs**」以進入WLANs配置頁面。在 WLANs頁面中,按一下**New**以建立一個新的WLAN。本示例建立一個新的WLAN **Idap**。按一 下「**Apply**」。下一步是在「WLANs」>「Edit」頁面中設定WLAN引數。
- 2. 在WLAN edit頁面中,啟用此WLAN的狀態。配置所有其他必要的引數。

cisco		CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Collock i Ro
LANS WLANS MUANS Advanced	WLANS > Edit General Securit Profile Name Type SSID Status Security Policies Radio Policy Interface Broadcast SSID	Idapuser WEAN Idap V Enabi (Medification All Managem V Enable	Advanced	] security tab	will appear after of	oplying the chan	< Back	Apply
	Feet Notes 1 CKIP is not supporte 3 H-REAF Local Switch 4 When cleart exclusio 5 Cleant APP is not act	id by 10xx mode ing is not suppor n is enabled, a T ive unless WP42	l dPy ted with IPsec, Imeout Value o Is configured	CRANITE aut d zero means	hendiaation Infinity (will requir	e administrative	override to reset e	cluded clients

- 按一下「Security」以設定此WLAN的安全相關引數。此示例將第2層安全用作802.1x和104位 動態WEP。注意:本文檔使用帶動態WEP的802.1x作為示例。建議使用更安全的身份驗證方 法,例如WPA/WPA2。
- 4. 在WLAN Security配置頁面中,按一下**AAA servers選項**卡。在AAA servers頁面中,啟用 Local EAP Authentication方法,並從與EAP配置檔名稱引數對應的下拉框中選擇**Idap**。這是在 本示例中建立的本地EAP配置檔案。

No. Dec. Note:       Dec. Contraction (Dec. Logical, Legistration)         CLSCO       MONITOR       WEAKS       CONTROLLER       VURLESS       SECURITY       MANAGEMENT       COMMANCE       HEAR         WLANS       WLANS       WLANS > Edit       Clack       Apply         WLANS       WLANS       Control uservice use of default servers on this WLAN       Commander       Apply         WLANS       Select AAA servers       Select AAA servers       Loade and servers       Loade AAA         Select AAA servers       Select AAA servers       Control uservice use of default servers on this WLAN       Commander         Select AAA servers       Select AAA servers       Control uservice use of default servers on this WLAN       Control uservice	🗿 wic2006 - Microsoft Ini	nternet Explorer	
WLANS       WLANS       WLANS       Cancel       Apply         WLANS       Advanced       Cancel       <	He Edit New Pavorites	Tools Help Sage Configuration   Eing   Logout MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	: L <u>B</u> efresi
	WLANS WLANS WLANS MAdvanced	WLANS > Edit       C Back       App         General       Security       QoS       Advanced         Layer 2       Layer 3       AAA Servers       LDAF Servers         Setect AAA servers below to override use of default servers on this WLAN       Radius Servers       LDAF Servers         Setver 1       None ¥       Enabled       Server 1       None ¥         Server 2       None ¥       Enabled       Server 1       None ¥         Local EAP Authentication       Enabled       Server 7       None ¥       Server 7         Local EAP Authentication       Enabled       Server 7       None ¥       Server 7       None ¥         Local EAP Authentication       Enabled       Server 7       None ¥       Server 7       None ¥         Local EAP Authentication       Enabled       Server 7       None ¥       Server 7       None ¥         Local EAP Authentication       Enabled       Server 7       None ¥       Server 7       Se	pily objects)

5. 從下拉框中選擇LDAP伺服器(之前在WLC上配置)。確保可以從WLC訪問LDAP伺服器。按 一下「Apply」。

File         Edit         View         Favorites         Tools         Help           IIIIII         Sage Configuration         Bing         Legout         Befre           CISCO         MONITOR         CONTROLLER         WIRELESS         SECURITY         MANAGEMENT         COMMANDS         HELP
Sage Configuration   Bing   Logout   Befre CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs     WLANs > Edit        WLANs     General     Security     QoS     Advanced
WLANS         > Advanced         > Advanced         Select AAA servers below to override use of default servers on this WLAN         Radius Servers         Authentication Servers Accounting Servers         Server 1         None W         Server 2         Server 3         None W         Local EAP Authentication         Local EAP Authentication </td
a Internet

6. 已在WLC上配置新的WLAN Idaphas。此WLAN使用本地EAP身份驗證(本例中為EAP-FAST)對客戶端進行身份驗證,並查詢LDAP後端資料庫以進行客戶端憑據驗證。

Wic2006 - Microsoft Inter File Edit View Favorites T	net Explorer ools Help					
uludu cisco	MONITOR WLANS	CONTROLLER WI	RELESS SECURITY	Sa MANAGEMENT COMMA	iye Configuration   Eing   Le NDS HELP	gout   <u>B</u> efresh
WLANs	WLANs				N	ew
- WLANS WLANS	Profile Name	Туре	WLAN SSID	Admin Status	Security Policies	
▶ Advanced	Ideouser	WLAN	Idap	Enabled	[WPA2][Auth(002.1×)] 002.1×	
						J
and Done					A 🔿 Interna	it.

# 配置LDAP伺服器

現在,在WLC上配置了本地EAP,下一步是配置LDAP伺服器,該伺服器用作後端資料庫,以便在 證書驗證成功時驗證無線客戶端。

配置LDAP伺服器的第一步是在LDAP伺服器上建立使用者資料庫,以便WLC可以查詢此資料庫以驗 證使用者。

#### <u>在域控制器上建立使用者</u>

在本示例中,將建立新的OU **Idapuser**,並在此OU下建立使用者**user2**。通過配置此使用者以進行 LDAP訪問,WLC可以查詢此LDAP資料庫以進行使用者身份驗證。

本示例中使用的域是wireless.com。

#### 在OU下建立使用者資料庫

本節介紹如何在您的域中建立新的OU並在此OU上建立新使用者。

- 1. 在域控制器中,按一下**開始>程式>管理工具> Active Directory使用者和電腦**,以啟動Active Directory使用者和電腦管理控制檯。
- 2. 按一下右鍵您的域名(本例中為wireless.com),然後從上下文選單中選擇**New > Organizational Unit**以建立新的OU。

	4 N	ctive Director	y Users and Com	puters			
	4 E	jie <u>A</u> ction	⊻iew <u>W</u> indow <u>b</u>	<u>i</u> elp			_ <b>5</b> ×
	¢	ə 🗈 🖬	🛍 🖆 🖥	3 🕄 🖪 🦉	💆 🖄 🖓 🍕 🖆		
	3	Active Directory	Users and Compl 🔺	Wireless.com	12 objects		
		Saved Queri	es	Name	Туре	Description	
		🗄 - 🦲 Builtin	Delegate Contro	l	builtinDomain	Default container for uppr	
		E-Comput	Find	ND	. Organizational	Default container for dom	
		E- Correign	Connect to Dom	ain Controller	. Container	Default container for secu	
		E- CostAnc	Raise Domain Fu	nctional Level	lostAndFound	Default container for orph	
			Operations Mast	ers	Container	fault location for storag	
		🗄 🧰 System	<u>N</u> ew	,	Computer	tin system settings	
		E-12 user1	All Tasijs		Group	Fault container for unor	
	l '	🖸 Adn	View Window fro	m Here	InetOrgPerson	aux concerner ror upgr	
		Cerl	Defect		MSMQ Queue Alias	_	
		DHK	Export List		Printer		
		DHK	Properties		User		
		<ul> <li>Uns</li> <li>Dns</li> </ul>	Hab		Shared Folder		
		Don.	Geb	1			
		E − 12 Dom E − 12 Dom	ain Computers ain Controllers				
		🗈 🚮 Dom	ain Guests				
		E C Ente	ain Users rorise Admins 🛛 👻				
	•			1			
3.	為該	፩OU分配╡	名稱,然後打	安一下 <b>OK</b> 。			
	Ne	w Objec	t - Organi	zational U	Init		X
			Create i	n: Wirele	ss.com/		
	-						
		Name					
		Tigine.	-				
		Idapuse	er				
	-						
						ПК	Cancel

現在,在LDAP伺服器上建立了新的OU **Idapuser**,下一步是在此OU下建立**user**2。為了達成此目的 ,請完成以下步驟: 1. 按一下右鍵建立的新OU。從生成的上下文選單中選擇**新建>使用者**,以建立新使用者。



2. 在「使用者設定」頁面中,填寫所需欄位,如本例所示。此示例將user2用作使用者登入名。
 這是將在LDAP資料庫中驗證用於驗證客戶端的使用者名稱。本示例使用abcd作為名字和姓氏。按「Next」(下一步)。

v Object - U	lser	
5 °	reate in: Wireless.com/Idapuser	
<u>F</u> irst name:	abcd Initials:	
Last name:		
Full n <u>a</u> me:	abcd	
User logon n	iame:	
user2	@Wireless.com	
User logon n	rame (pre- <u>W</u> indows 2000):	
WIRELESS	\user2	
	< Back Next > Cance	el l

3. 輸入密碼並確認密碼。選擇Password never expires選項,然後按一下Next。 New Object - User

🛃 Create in: W	/ireless.com/Idapuser
Password:	•••••
User <u>m</u> ust change pas User cannot change p Ressword never expire	asword at next logon bassword
Account is disabled	
	< Back Next > Cancel

×

- 4. 按一下「Finish」(結束)。在OU **Idapuser**下**建立**新的使用者**user2**。使用者憑據為:使用者 名稱:**user2**密碼
  - : Laptop123



現在建立了OU下的使用者,下一步是配置此使用者以進行LDAP訪問。

## <u>配置使用者的LDAP訪問</u>

執行本節中的步驟,配置使用者進行LDAP訪問。

在Windows 2003 Server上啟用匿名繫結功能

對於要在LDAP上訪問Windows 2003 AD的任何第三方應用程式,應在Windows 2003上啟用匿名繫 結功能。預設情況下,在Windows 2003域控制器上不允許匿名LDAP操作。

執行以下步驟以啟用匿名繫結功能:

- 1. 從位置**開始>運行>型別:ADSI Edit.msc**啟動ADSI Edit工具。此工具是Windows 2003支援工具的一部分。
- 在ADSI Edit視窗中,展開Root domain(Configuration [tsweb-lapt.Wireless.com])。展開 CN=Services > CN=Windows NT > CN=Directory Service。按一下右鍵CN=Directory Service容器,然後從上下文選單中選擇properties。

🐗 ADSI Edit					
Ile Action Yew Wind	dow <u>H</u> elp				_8×
⇔ ⇒ 🖻 📧 🗙 😭	o 🗈 😰 💷				
ADSI Edit			Name	Class	Distinguished
Domain [tsweb-lapt. Wire Configuration [tsweb-lap CN=Configuration,D CN=DisplaySpec CN=Extended-R CN=ForestUpdal CN=ForestUpdal CN=CN=NTDS Quota CN=Partitions CN=Physical Loc CN=Physical Loc CN=Services CN=MsmqSe CN=VetServices CN=VetServices CN=VetServices CN=VetServices CN=VetServices CN=VetServices CN=VetServices CN=VetServices CN=VetServices CN=VetServices CN=VetServices CN=Stress CN=Stress CN=Stress CN=Welknowr CN=Stress CN=Welknowr CN=Welknowr	eless.com] xt.Wireless,com] C=Wireless,DC=com fiers ights tes indConfig ss ations xvices rvices is NT Move New ⊆onnection from Here New ≦indow from Here Qelete Rename		CN=Query-Policies	container	CN=Query-P
Opens the properties dialog box	Refresh				
opens the properties daug box	Export List				
	Ptoperties	]			

3. 在CN=Directory Service Properties視窗中,按一下Attribute欄位下的dsHeuristics屬性,然後 選擇Edit。在此屬性的字串屬性編輯器視窗中,輸入值0000002,然後按一下Apply和OK。在 Windows 2003 Server上啟用了匿名繫結功能。注意:最後一個字元(第七)是控制繫結到 LDAP服務的方式的字元。「0」或無第七個字元表示已禁用匿名LDAP操作。將第七個字元設 定為"2"將啟用匿名繫結功能。

CN=Directory Service Properties     ? ×       Attribute Editor     Security       Image: Show mandatory attributes     Image: Show estional attributes	Class container	Disting
Attribute Editor   Security	Class container	Disting
Show mandatory attributes	container	CNI
Show optional attributes		C14=Q
Te show optional attributes		
Show only attributes that have values		
Attributes:		
Attribute Syntax Value		
directReports String Attribute Editor		×
displayName displayNamePrintable Attributer dCHermistics		
distinguishedName		
dSASignature Value:		
dSHeuristics	_	
extensionName Clear OK		Cancel
frags		
frsComputerReferenc Distinguished <not set=""></not>		
fRSMemberReferenc Distinguished <not seb<="" td=""><td></td><td></td></not>		
Edit		
OK Cancel Apply		

**注意:**如果此屬性已經包含值,請確保僅更改左側的第七個字元。這是唯一需要更改的字元 ,以便啟用匿名繫結。例如,如果當前值為「0010000」,則需要將其更改為「0010002」。 如果當前值少於7個字元,則需要在未使用的位置中置零:「001」將變為「001002」。

向使用者「user2」授予ANONYMOUS LOGON訪問許可權

下一步是向使用者user2授予ANONYMOUS LOGON訪問許可權。完成以下步驟即可完成以下操作 :

- 1. 開啟Active Directory使用者和電腦。
- 2. 確保選中View Advanced Features。
- 3. 導航到使用者user2, 然後按一下右鍵該使用者。從上下文選單中選擇**屬性**。此使用者使用名 字「abcd」標識。



4. 在「shu xing屬性」視窗中,轉到**安全**。

ocd Properties	
Published Certificates	s Member Of Dial-in Object Security
Environment Session	ns   Remote control   Terminal Services Profile. COM
General Address	Account   Profile   Telephones   Organization
C abod	
<u>z</u> .	
First parae:	Initials
<u>r</u> ast name.	Initials.
Last name:	
Digplay name:	abcd
Description:	
Officer	
onge.	1
Talaakana muulaan	
Lelephone number:	
E-mail:	
Web page:	Other
	OK Cancel Apply

- 5. 在生成的視窗中按一下Add。
- 6. 在Enter the object names to select框下輸入ANONYMOUS LOGON並確認對話方塊。 Select Users, Computers, or Groups

Select this object type:	
Users, Groups, or Built-in security principals	<u>O</u> bject Types
From this location:	
Wireless.com	Locations
Enter the object names to select (examples):	
ANONYMOUS LOGON	<u>C</u> heck Names
Advanced	OK Cancel

7. 在ACL中,您會注意到ANONYMOUS LOGON有權訪問使用者的一些屬性集。按一下「OK」 (確定)。已授予此使用者的ANONYMOUS登入訪問許可權。

ocd Properties		?>
Environment   Sessions   Remote control   T General   Address   Account   Profile Published Certificates   Member Of   D	erminal Servic   Telephones ial-in   Obje	es Profile   COM+   Organization ect Security
<u>G</u> roup or user names:		
Account Operators (WIRELESS Accou Administrators (WIRELESS Administrators	int Operators) ors)	-
ANONYMOUS LOGON		
Authenticated Users		
Cert Publishers (WIRELESS\Cert Publis	hers)	-
	A <u>d</u> d	<u>R</u> emove
Permissions for ANONYMOUS LOGON	Allow	Deny
Full Control		
Read	$\checkmark$	
Write		
Create All Child Objects		
Delete All Child Objects		
Allowed to Authenticate		
For special permissions or for advanced settin click Advanced.	ngs,	Adyanced
ОК	Cancel	Apply

#### 對OU授予清單內容許可權

下一步是至少向使用者所在的OU上的ANONYMOUS LOGON授予List Contents許可權。在本示例中,「user2」位於OU "Idapuser"上。完成以下步驟即可完成以下操作:

1. 在Active Directory使用者和電腦中,按一下右鍵OU Idapuser並選擇屬性。



2. 按一下「Security」,然後「Advanced」。

apuser Properties		?	L ×
General Managed By Object Security	COM+ Group	Policy	
Group or user pames:			- 1
Account Operators M/IBELESS\Acco	unt Operators)	<b>^</b>	1 I
Administrators [WIBELESS Administra	ntors)		1
Authenticated Users			
Domain Admins (WIRELESS\Domain	Admins)		
Enterprise Admins (WIRELESS\Enter	prise Admins)	_	
		-	
	A <u>d</u> d	<u>R</u> emove	
Permissions for Account Operators	Allow	Deny	
Full Control			1 1
Bead			
Write			
Write Create All Child Objects			
Write Create All Child Objects Delete All Child Objects			]
Write Create All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging			
Write Create All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging For special permissions or for advanced set click Advanced.	o)	Advanced	

3. 按一下「Add」。在開啟的對話方塊中,輸入ANONYMOUS LOGON。

Advanced Security Settings for Idapuser	
Select User, Computer, or Group	? ×
Select this object type:	
User, Group, or Built-in security principal	Object Types
From this location:	
Wireless.com	Locations
Enter the object name to select (examples):	
ANONYMOUS LOGON	<u>C</u> heck Names
Advanced OK	Cancel

- 4. 確認對話方塊。這將開啟一個新的對話方塊視窗。
- 5. 在Apply to下拉框中,選擇This object only,並啟用List Contents Allow覈取方塊。

Permission Entry for Idapuser		?	×
Object Properties			
Name: ANONYMOUS LOGON		<u>C</u> hange	
Apply onto: This object only		-	
Permissions:	Allow	Deny	
Full Control List Contents Read All Properties Write All Properties Delete Delete Subtree Read Permissions Modify Permissions Modify Owner All Validated Writes All Extended Rights Create All Child Objects Create All Child Objects	ts and/or		
	ок	Cancel	

# 使用LDP標識使用者屬性

此GUI工具是一個LDAP客戶端,允許使用者針對任何與LDAP相容的目錄(如Active Directory)執 行操作(如連線、繫結、搜尋、修改、新增、刪除)。LDP用於檢視Active Directory中儲存的對象 及其後設資料,如安全描述符和複製後設資料。

從產品CD安裝Windows Server 2003支援工具時,會包括LDP GUI工具。本節介紹使用LDP實用程 式標識與使用者**user**2關聯的特定**屬性**。其中有些屬性用於填寫WLC上的LDAP伺服器配置引數,例 如「使用者屬性」型別和「使用者對象」型別。

- 1. 在Windows 2003伺服器上(即使在同一個LDAP伺服器上),按一下**Start > Run**並輸入**LDP**以 訪問LDP瀏覽器。
- 2. 在LDP主視窗中,按一下**Connection > Connect**,然後通過輸入LDAP伺服器的IP地址連線到 LDAP伺服器。

p Ldp	
Connection Browse View Options Utilities	μe
Bind     Connect       Bind     Connect       Bind     Corl+B       Osconnest     Disconnest       New     Corl+N       Save     Save       Save     Bs       Print     Print Pregiew       Print Sebup     Egit	AULA del A
	×
Connect to specified server	

## 3. <u>連線到LDAP伺服器後,從主選單中選擇View,然後按一下Tree</u>。

Connection         Browse         Users         Users <thusers< th="">         Users         <thusers< th=""></thusers<></thusers<>	and the second requirements are an interesting a con-		ن تكتار
Itee         C0HT           Enterptive Configuration         1.2.840.113556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.528;           * Set Eont         1.2.840.113556.1.4.613; 1.2.240.113556.1.4.641; 1.2.840.113556.1.4.528;           * Set Eont         1.2.840.113556.1.4.613; 1.2.840.113556.1.4.641; 1.2.840.113556.1.4.528;           * Set Eont         1.2.840.113556.1.4.613; 1.2.840.113556.1.4.613; 1.2.840.113556.1.4.1355.1.4.13556.1.4.13556.1.4.13556.1.4.13556.1.4.1333;           * Set Eont         1.2.840.113556.1.4.1338; 1.2.840.113556.1.4.13556.1.4.13556.1.4.1333;           * Set Eont         1.2.840.113556.1.4.1338;           * Set Eont         1.2.840.113556.1.4.1340;           * Set Eont         1.2.840.113556.1.4.1338;           * Set Eont         1.2.840.113556.1.4.1378;           * Set Eont         1.2.840.113556.1.4.1378;           * Set Eont         1.3.8561.4.1378;           * Set Eont	onnection Browse Yew Options Usilities		Hel
	If the Configuration If the Configuration ✓ Status Bar Set Font	<pre>1.2.840.113556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 1.2.840.113556.1.4.619; 1.2.840.113556.1.4.841; 1.2.840.113556.1.4.529; 1.2.840.113556.1.4.805; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 1.2.840.113556.1.4.1338; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 1.2.840.113556.1.4.1340; 1.2.840.113556.1.4.1413; 2.16.840.1.113730.3.4.9; 2.16.840.1.113730.3.4.10; 1.2.840.113556.1.4.1504; 1.2.840.113556.1.4.1982; 1.2.840.113556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2.&gt; supportedLDAPVersion; 3; 2; 12&gt; supportedLDAPVersion; 3; 2; 12&gt; supportedLDAPVersion; MaxPoolThreads; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections; MaxConnIdleTime; MaxPageSize; MaxQueryDuration; MaxTempTableSize; MaxResultSetSize; MaxNotificationPerConn; MaxVaIRange; 1.&gt; highestCommittedUSN: 16926; 4.&gt; supportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1.&gt; dnsHostName: tsweb-lapt.Wireless.com; 1.&gt; ldapServiceName: Wireless.com; 1.&gt; ldapServiceName: Wireless.com; 3.&gt; serverName: CN=TSWEB-LAPT,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configur; DC=Wireless,DC=com; 3.&gt; supportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4.1 1.2.840.113556.1.4.1791; 1.&gt; isSynchronized: TRUE; 1.&gt; isGlobalCatalogReady: TRUE; 1.&gt; domainFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1.&gt; torestFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1.&gt; domainControllerFunctionality: 2 = [DS_BEHAVIOR_WIN2003];</pre>	stion 670;

4. 在生成的「樹檢視」視窗中,輸入使用者的BaseDN。在本示例中**,user2位於域** Wireless.com下的OU "Idapuser"下。因此,使用者user2的BaseDN為OU=Idapuser, dc=wireless, dc=com。按一下「OK」(確定)。

Onnecton         Deve         Set         Help           rece Yicm         XI         33556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 13556.1.4.619; 1.2.840.113556.1.4.529; 13556.1.4.619; 1.2.840.113556.1.4.619; 1.2.840.113556.1.4.470; 13556.1.4.1339; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1397; 13556.1.4.1339; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1393; 13556.1.4.10; 1.2.840.113556.1.4.1317, 2.1.840.113556.1.4.1982; 13556.1.4.805; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1982; 13556.1.4.80; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1984; 2> supportedLDAPVersion; 3; 2; 12> supportedLDAPVersion; 3; 2; 12> supportedLDAPVersion; 3; 2; 12> supportedLDAPVersion; 3; 2; 13> supportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 13 dnsHostName: tsweb-laptWireless.com; 15 IdapServiceName: Wreless.com; 15 IdapServiceName: Wreless.com; 15 IdapServiceName: CN=TSWEB-LAPT,CN=Servers,CN=Default First-Site-Name,CN=Sites,CN=Configuration ,DC=Wireless,DC=com; 35 supportedCapabilities; 1.2.840.113556.1.4.800; 1.2.840.113556.1.4.1670; 1.2.840.113556.1.4.1791; 15 IsSynchronized: TRUE; 15 IsSynchronized: TRUE; 15 IsSynchronized: TRUE; 15 IsSynchronized: TRUE; 15 IsSynchronized: TRUE; 15 IsSynchronized: TRUE; 15 IsSbarchalageRay: TRUE; 15 IsSbarchalageRay: TRUE; 15 IsGlobalCatalogReady: TRUE;	Mildap://tsweb-lapt.Wireless.com/DC=Wireless,DC=com		IJ×
rec View       XI         3556.1.4.473; 1.2.040.113556.1.4.528; 1.2.840.113556.1.4.417;	Connection Browse View Options Utilities		Help
	Tree Yiew BaseDN: DU-Maguser,do-wireless.do-com Cancel	X   3556.1.4.473; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.417; 13556.1.4.619; 1.2.840.113556.1.4.841; 1.2.840.113556.1.4.529; 13556.1.4.805; 1.2.840.113556.1.4.841; 1.2.840.113556.1.4.1339; 13556.1.4.1338; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 13556.1.4.1340; 1.2.840.113556.1.4.474; 1.2.840.113556.1.4.1339; 13556.1.4.1340; 1.2.840.113556.1.4.1413; 2.16.840.1.113730.3.4.9; 1.113730.3.4.10; 1.2.840.113556.1.4.1504; 1.2.840.113556.1.4.1852; 13556.1.4.802; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: 3; 2; 12> supportedLDAPVersion: MaxConnections; MaxConnIdleTime; MaxPageSize; MaxQueryDuration; MaxTempTableSize; MaxResultSetSize; MaxNotificationPerConn; MaxValRange; 1> highestCommittedUSN: 16926; 4> supportedSASLMechanisms: GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5; 1> dnsHostName: tsweb-lapt.Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 1> ldapServiceName: Wireless.com; 3> supportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4.167 1.2.840.113556.1.4.1791; 1> isSynchronized: TRUE; 1> isSynchronized: TRUE; 1> isSynchronized: TRUE; 1> isSynchronized: TRUE; 1> domainFunctionality: 0 = { DS_BEHAVIOR_WIN2000 }; 1> domainControllerFunctionality: 2 = { DS_BEHAVIOR_WIN2003 };	• • •
sady //	Ready		1.

5. LDP瀏覽器的左側顯示出現在指定BaseDN(**OU=Idapuser, dc=wireless, dc=com)下的整個** 樹。展開樹以找到使用者user2。此使用者可以使用代表該使用者名稱字的CN值進行標識。在 本例中,它是**CN=abcd**。按兩下**CN=abcd**。在LDP瀏覽器的右側窗格中,LDP**將顯示與** user2**關聯的所有屬性**。以下範例將說明此步驟

🚰 ldap://tsweb-lapt.Wireless.com/DC=Wireless,DC=com	
Connection Browse View Options Utilities	Heb
OU=ldapuser, dc=wireless, dc=com OU=ldapuser, dc=wireless, dc=wire	<pre>1&gt; whenCreated: 1/27/2008 21:56:30 India Standard Time India Standard Time; 1&gt; whenChanged: 1/27/2008 22:2:15 India Standard Time India Standard Time; 1&gt; displayName: abcd; 1&gt; uSNCreated: 16917; 1&gt; uSNChanged: 16923; 1&gt; name: abcd; 1&gt; objectGUID: db0ad755-2e36-493d-9325-3429aa907626; 1&gt; userAccountControl: 0x10200 = ( UF_NORMAL_ACCOUNT   UF_DONT_EXPIRE_PASSWD ); 1&gt; badPwdCount: 0; 1&gt; codePage: 0; 1&gt; countryCode: 0; 1&gt; badPwdCount: 0; 1&gt; badPasswordTime: 0; 1&gt; lastLogoff: 0; 1&gt; lastLogoff: 0; 1&gt; lastLogoff: 0; 1&gt; pwdLastSet: </pre>
Ready	

在此示例中,請觀察右側的環繞欄位。

- 6. 如本文檔的使用LDAP伺服器的詳細資訊配置WLC部分中所述,在User Attribute欄位中,在包含使用者名稱的使用者記錄中輸入屬性的名稱。從此LDP輸出中,可以看到 sAMAccountName是包含使用者名稱「user2」的一個屬性。因此,請輸入與WLC上的User Attribute欄位對應的sAMAccountName屬性。
- 7. 在User Object Type欄位中,輸入將記錄標識為使用者的LDAP objectType屬性的值。通常 ,使用者記錄有若干objectType屬性值,其中某些值對於使用者是唯一的,而某些值則與其他 對象型別共用。在LDP輸出中, CN=Person是將記錄標識為使用者的值。因此,在WLC上指 定Person作為User Object Type屬性。

# 配置無線客戶端

最後一步是配置無線客戶端,使其使用客戶端和伺服器證書進行EAP-FAST身份驗證。完成以下步 驟即可完成以下操作:

 1. 啟動Cisco Aironet Desktop Utility(ADU)。在ADU主視窗中,按一下Profile Management > New以建立新的無線客戶端配置檔案。

🛜 Cisco Aironet Desktop Uti	lity - Current Profile: sdreteretet	? 🔀
Action Options Help		
Current Status Profile Manageme	ent Diagnostics	
Sdreteretet		New
		Modify
		Remove
		Activate
⊂ Details		
Network Type:	Infrastructure	Import
Security Mode:	Disabled	
Network Name 1 (SSID1):	teert	Export
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	
Auto Select Profiles		Order Profiles

 指定配置檔名稱,並為該配置檔案分配SSID名稱。此SSID名稱應該與WLC上配置的相同。在 本示例中,SSID名稱為Idap。

Profile Settings	ced	]
Client Name	CLIENT1	
Network Names SSID SSID2 SSID3		

- 3. 按一下Security頁籤,然後選擇802.1x/EAP作為第2層安全。選擇EAP-FAST作為EAP方法 ,然後按一下Configure。
- 4. 在EAP-FAST配置頁面中,從EAP-FAST身份驗證方法(EAP-FAST Authentication Method)下 拉框中選擇**TLS客戶端證書(TLS Client Certificate**),然後按一下**配置(Configure**)。

Configure EAP-FAST	
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
GTC Token/Password	
MSCHAPv2 User Name and Password	
Select One or More PAC Authorities	-
	Manage
Use Any PAC Belonging to the Same Group	_
Allow Automatic PAC Provisioning	
Milow Automatic PAC Provisioning	
Lise Machine Information for Domain Logon	
No Network Connection Unless User Is Logged In	
	OK Cancel

5. 在「TLS客戶端證書配置」視窗中:啟用Validate Server Identity覈取方塊,並選擇客戶端上安裝的CA證書(請參閱本文檔的<u>為客戶端生成根CA證書</u>部分)作為受信任的根證書頒發機構。選擇安裝在客戶端上的裝置證書(本文檔的<u>為客戶端生成裝置證書</u>一節中有說明)作為客戶端證書。按一下「OK」(確定)。以下範例將說明此步驟

✓ Validate Server Identity	
Trusted Root Certification Authorities	
wireless	~
Select a Certificate	
1234 [Issued by: wireless 1/26/2008]	~
Server/Domain Name	
Wireless.com	
Login Name	
user2	

無線客戶端配置檔案已建立。

<u>驗證</u>

執行以下步驟以驗證您的配置是否正常工作。

- 1. 啟用ADU上的Idap SSID。
- 2. 根據需要在下一視窗中按一下Yes或OK。您應該能夠在ADU上看到客戶端身份驗證和關聯的 所有步驟,這樣才能成功。

使用本節內容,確認您的組態是否正常運作。使用WLC CLI模式。

• 為了驗證WLC是否能夠與LDAP伺服器通訊並找到使用者,請從WLC CLI指定debug aaa Idap enable命令。此示例說明了一個成功的通訊LDAP過程:注意:由於空間方面的考慮,本節中的 某些輸出已移至第二行。(Cisco Controller)>debug aaa Idap enable Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514 Sun Jan 27 09:23:46 2008: Callback.....0x8 344900 Sun Jan 27 09:23:46 2008: protocolType.....0x0 0100002 Sun Jan 27 09:23:46 2008: proxyState.....00: 40:96:AC:E6:57-00:00 Sun Jan 27 09:23:46 2008: Packet contains 2 AVPs (not shown) Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1) Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi\_init (rc = 0 - Success) Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi\_bind (rc = 0 - Success) Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED Sun Jan 27 09:23:46 2008: LDAP server 1 now active Sun Jan 27 09:23:46 2008: LDAP\_CLIENT: UID Search (base=OU=ldapuser, DC=wireless, DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2))) Sun Jan 27 09:23:46 2008: LDAP CLIENT: Returned msg type 0x64 Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi\_query base="OU=ldapus er, DC=wireless, DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0 - Success) Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com (size 38) Sun Jan 27 09:23:46 2008: Handling LDAP response Success

從此調試輸出中突出顯示的資訊可以清楚地看到,WLC會使用在WLC上指定的使用者屬性來查

詢LDAP伺服器,並且LDAP進程成功。

## • 若要驗證本地EAP身份驗證是否成功,請從WLC CLI指定debug aaa local-auth eap method events enable命令。以下是範例:(Cisco Controller)>debug aaa local-auth eap method events enable Sun Jan 27 09:38:28 2008: eap\_fast.c-EVENT: New context (EAP handle = 0x1B000009)Sun Jan 27 09:38:28 2008: eap\_fast.c-EVENT: Allocated new EAP-FAST context (handle = 0x22000009)Sun Jan 27 09:38:28 2008: eap\_fast\_auth.c-AUTH-EVENT: Process Response (EAP handle = 0x1B000009)Sun Jan 27 09:38:28 2008: eap\_fast\_auth.c-AUTH-EVENT: Received Identity Sun Jan 27 09:38:28 2008: eap\_fast\_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV (436973636f0000000000000000000000) Sun Jan 27 09:38:28 2008: eap\_fast\_auth.c-AUTH-EVENT: Sending Start Sun Jan 27 09:38:29 2008: eap\_fast.c-AUTH-EVENT: Process Response, type: 0x2b Sun Jan 27 09:38:29 2008: eap\_fast\_auth.c-AUTH-EVENT: Process Response (EAP handle = 0x1B000009)Sun Jan 27 09:38:29 2008: eap\_fast\_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Start Sun Jan 27 09:38:29 2008: eap\_fast\_auth.c-AUTH-EVENT: Local certificate found Sun Jan 27 09:38:29 2008: eap\_fast\_auth.c-AUTH-EVENT: Reading Client Hello handshake Sun Jan 27 09:38:29 2008: eap\_fast\_auth.c-AUTH-EVENT: TLS\_DHE\_RSA\_AES\_128\_CBC\_SHA proposed... Sun Jan 27 09:38:29 2008: eap\_fast.c-EVENT: Proposed ciphersuite(s): Sun Jan 27 09:38:29 2008: eap\_fast.c-EVENT: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA Sun Jan 27 09:38:29 2008: eap\_fast.c-EVENT: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA Sun Jan 27 09:38:29 2008: eap\_fast.c-EVENT: TLS\_RSA\_WITH\_RC4\_128\_SHA Sun Jan 27 09:38:29 2008: eap\_fast.c-EVENT: Selected ciphersuite: Sun Jan 27 09:38:29 2008: eap\_fast.c-EVENT: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA Sun Jan 27 09:38:29 2008: eap\_fast\_auth.c-AUTH-EVENT: Building Provisioning Server Hello Sun Jan 27 09:38:29 2008: eap\_fast\_crypto.c-EVENT: Starting Diffie Hellman phase 1 ... Sun Jan 27 09:38:30 2008: eap\_fast\_crypto.c-EVENT: Diffie Hellman phase 1 complete Sun Jan 27 09:38:30 2008: eap\_fast\_auth.c-AUTH-EVENT: DH signature length = 128 Sun Jan 27 09:38:30 2008: eap\_fast\_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello Sun Jan 27 09:38:30 2008: eap\_fast.c-EVENT: Tx packet fragmentation required

Sun Jan 27 09:38:30 2008: eap\_fast.c-AUTH-EVENT: eap\_fast\_rx\_packet():

EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap\_fast.c-AUTH-EVENT: eap\_fast\_rx\_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap\_fast.c-AUTH-EVENT: eap\_fast\_rx\_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:32 2008: eap\_fast.c-AUTH-EVENT: Process Response, type: 0x2b Sun Jan 27 09:38:32 2008: eap\_fast.c-EVENT: Reassembling TLS record Sun Jan 27 09:38:32 2008: eap\_fast.c-EVENT: Sending EAP-FAST Ack Sun Jan 27 09:38:32 2008: eap\_fast\_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Sent provisioning Server Hello Sun Jan 27 09:38:32 2008: eap\_fast\_auth.c-AUTH-EVENT: Reading Client Certificate handshake Sun Jan 27 09:38:32 2008: eap fast.c-EVENT: Added certificate 1 to chain Sun Jan 27 09:38:32 2008: eap\_fast.c-EVENT: Added certificate 2 to chain Sun Jan 27 09:38:32 2008: eap\_fast.c-EVENT: Successfully validated received certificate Sun Jan 27 09:38:32 2008: eap\_fast\_auth.c-AUTH-EVENT: Rx'd I-ID: "EAP-FAST I-ID" from Peer Cert Sun Jan 27 09:38:32 2008: eap\_fast\_auth.c-AUTH-EVENT: Reading Client Key Exchange handshake Sun Jan 27 09:38:32 2008: eap\_fast\_crypto.c-EVENT: Starting Diffie Hellman phase 2 ... Sun Jan 27 09:38:32 2008: eap\_fast\_crypto.c-EVENT: Diffie Hellman phase 2 complete. Sun Jan 27 09:38:32 2008: eap\_fast\_auth.c-AUTH-EVENT: Reading Client Certificate Verify handshake Sun Jan 27 09:38:32 2008: eap\_fast\_crypto.c-EVENT: Sign certificate verify succeeded (compare) ..... • debug aaa local-auth db enable命令也非常有用。以下是範例:(Cisco Controller)>debug aaa local-auth db enable

Sun Jan 27 09:35:32 2008: LOCAL\_AUTH: EAP: Received an auth request

Sun Jan 27 09:35:32 2008: LOCAL\_AUTH: Local auth profile name for context 'ldapuser' Sun Jan 27 09:35:32 2008: LOCAL\_AUTH: Created new context eap session handle fb000007 Sun Jan 27 09:35:32 2008: LOCAL\_AUTH: (EAP:8) Sending the Rxd EAP packet (id 2) to EAP subsys Sun Jan 27 09:35:32 2008: LOCAL AUTH: Found matching context for id - 8 Sun Jan 27 09:35:32 2008: LOCAL\_AUTH: (EAP) Sending user credential request username 'user2' to LDAP Sun Jan 27 09:35:32 2008: LOCAL\_AUTH: Found context matching MAC address - 8 Sun Jan 27 09:35:36 2008: LOCAL\_AUTH: (EAP:8) Sending the Rxd EAP packet (id 12) to EAP subsys Sun Jan 27 09:35:36 2008: LOCAL\_AUTH: Found matching context for id - 8 Sun Jan 27 09:35:36 2008: LOCAL\_AUTH: (EAP:8) ---> [KEY AVAIL] send\_len 64, recv\_len 0 Sun Jan 27 09:35:36 2008: LOCAL\_AUTH: (EAP:8) received keys waiting for success Sun Jan 27 09:35:36 2008: LOCAL\_AUTH: Found matching context for id - 8 Sun Jan 27 09:35:36 2008: LOCAL AUTH: (EAP:8) Received success event Sun Jan 27 09:35:36 2008: LOCAL\_AUTH: (EAP:8) Processing keys success 若要檢視WLC中安裝用於本機驗證之憑證,請從WLC CLI發出show local-auth certificates命令 。以下是範例:(思科控制器)>show local-auth certificates Certificates available for Local EAP authentication: Certificate issuer ..... vendor CA certificate: Subject: DC=com, DC=Wireless, CN=wireless Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

Device certificate:

Subject: O=cisco, CN=ciscowlc123

Issuer: DC=com, DC=Wireless, CN=wireless

Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT

Certificate issuer ..... cisco

CA certificate:

Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

Device certificate:

Not installed.

#### • 若要從CLI模式檢視WLC上的本機驗證組態,請發出show local-auth config指令。以下是範例 :(思科控制器)>show local-auth config

User credentials database search order:

Primary ..... LDAP

Timer:

Active timeout ...... 300

Configured EAP profiles:

Name	•••••••••••••••••••••••••••••••••••••••	ldapuser
Certifi	icate issuer	vendor
Peer ve	erification options:	
Check	against CA certificates	Enabled
Verif	Ey certificate CN identity	Disabled
Check	c certificate date validity	Disabled
EAP-FAS	ST configuration:	
Local	l certificate required	Yes
Clier	nt certificate required	Yes
Enabled	d methods	fast
Configu	ared on WLANs	2

EAP Method configuration:

EAP-FAST:

--More-- or (q)uit

Server key ..... <hidden>

TTL for the PAC 10
Anonymous provision allowed No
Authority Information Cisco A-ID

# <u>疑難排解</u>

您可以使用以下命令對組態進行疑難排解:

- · debug aaa local-auth eap method events enable
- debug aaa all enable
- debug dot1x packet enable

# 相關資訊

- 使用無線LAN控制器和外部RADIUS伺服器的EAP-FAST身份驗證配置示例
- 採用Microsoft Internet身份驗證服務(IAS)的統一無線網路下的PEAP
- 使用基於ACS的WLC進行動態VLAN分配到Active Directory組對映配置示例
- 思科無線LAN控制器組態設定指南 設定安全解決方案
- Cisco無線LAN控制器組態設定指南 管理控制器軟體和組態
- 使用WLAN控制器(WLC)的EAP驗證組態範例
- •無線區域網路控制器(WLC)設計和功能常見問題
- <u>採用EAP-FAST驗證的思科安全服務使用者端</u>
- 無線 LAN 控制器 (WLC) 常見問題
- 控制器無線LAN控制器(WLC)錯誤和系統消息常見問題
- 技術支援與文件 Cisco Systems

#### 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)。