# 在无线局域网控制器上使用 EAP-FAST 和 LDAP 服务器配置本地 EAP 认证的配置示例

目录

简介 先决条件 要求 使用的组件 规则 背景信息 配置 网络图 配置 在 WLC 上将 EAP-FAST 配置为本地 EAP 身份验证方法 为 WLC 生成设备证书 将设备证书下载到 WLC 上 将 PKI 的根证书安装到 WLC 中 为客户端生成设备证书 为客户端生成根 CA 证书 在 WLC 上配置本地 EAP 配置 LDAP 服务器 在域控制器上创建用户 为 LDAP 访问配置用户 使用 LDP 来标识用户属性 配置无线客户端 验证 故障排除 相关信息

# <u>简介</u>

本文档介绍如何在无线局域网控制器(WLC)上配置可扩展身份验证协议(EAP) — 通过安全隧道的灵 活身份验证(FAST)本地EAP身份验证。本文档还说明了如何将 Lightweight Directory Access Protocol (LDAP) 服务器配置为本地 EAP 的后端数据库,以便检索用户凭证并对用户进行身份验证

# <u>先决条件</u>

<u>要求</u>

0

本文档没有任何特定的要求。

## <u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

- 运行固件 4.2 的 Cisco 4400 系列 WLC
- Cisco Aironet 1232AG系列轻型接入点(LAP)
- 配置为域控制器、LDAP 服务器以及证书颁发机构服务器的 Microsoft Windows 2003 Server。
- 运行固件 4.2 版的 Cisco Aironet 802.11 a/b/g 客户端适配器
- •运行固件版本 4.2 的思科 Aironet 桌面实用程序 (ADU)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

#### <u>规则</u>

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

# <u>背景信息</u>

无线局域网控制器 4.1.171.0 版在无线局域网控制器上引入了本地 EAP 身份验证。

本地 EAP 是一种允许在控制器上对用户和无线客户端进行本地身份验证的身份验证方法。当后端系 统中断或外部身份验证服务器停机时,它用于要与无线客户端保持连接的远程办事处。当您启用本 地 EAP 时,控制器担当身份验证服务器和本地用户数据库,因此它无需依赖于外部身份验证服务器 。本地 EAP 从本地用户数据库或 LDAP 后端数据库检索用户凭证,以便对用户进行身份验证。本 地 EAP 在控制器与无线客户端之间支持 LEAP、EAP-FAST、EAP-TLS、P EAPv0/MSCHAPv2 和 PEAPv1/GTC 身份验证。

本地 EAP 可以将 LDAP 服务器用作其后端数据库,用来检索用户凭证。

LDAP 后端数据库允许控制器向 LDAP 服务器查询特定用户的凭证(用户名和密码)。然后使用这 些凭证对用户进行身份验证。

LDAP 后端数据库支持以下本地 EAP 方法:

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

**只有在 LDAP 服务器设置为返回明文密码时**,还支持 LEAP、EAPFAST/MSCHAPv2 和 PEAPv0/MSCHAPv2。例如,不支持 Microsoft Active Directory,因为它不返回明文密码。如果 LDAP 服务器不能配置为返回明文密码,则不支持 LEAP、EAPFAST/MSCHAPv2 和 PEAPv0/MSCHAPv2。

**注意:如**果在控制器上配置了任何RADIUS服务器,则控制器会首先尝试使用RADIUS服务器对无线 客户端进行身份验证。只有在因 RADIUS 服务器超时或未配置任何 RADIUS 服务器而找不到任何 RADIUS 服务器时才尝试本地 EAP。如果配置了四个 RADIUS 服务器,则控制器将尝试用第一个 RADIUS 服务器对客户端进行身份验证,然后尝试第二个 RADIUS 服务器,最后尝试本地 EAP。 如果随后客户端重新尝试手动进行身份验证,控制器将尝试第三个 RADIUS 服务器,然后尝试第四 个 RADIUS 服务器,最后尝试本地 EAP。 本示例在 WLC 上使用 EAP-FAST 作为本地 EAP 方法,该方法又配置为从 LDAP 后端数据库查询 无线客户端的用户凭证。

# 配置

本文档将 EAP-FAST 与客户端和服务器端上的证书配合使用。为此,安装程序使用Microsoft Certificate Authority(CA)服务器生成客户端和服务器证书。

用户凭证存储在 LDAP 服务器中,因此在成功验证证书后,控制器能够查询 LDAP 服务器,检索用 户凭证并对无线客户端进行身份验证。

本文档假设以下配置已经到位:

- •WLC 上已注册 LAP。有关注册过程的详细信息,请参阅<u>向无线局域网控制器(WLC)注册轻量</u> <u>AP(LAP)</u>。
- 已配置 DHCP 服务器,用于向无线客户端分配 IP 地址。
- Microsoft Windows 2003 Server 已配置为域控制器和 CA 服务器。本示例使用 wireless.com 作为域。有关将 Windows 2003 Server 配置为域控制器的详细信息,请参阅<u>将 Windows 2003 配置为域控制器。</u>要将Windows 2003 Server配置为企业CA服务器,请参阅<u>安装和配置Microsoft</u>Windows 2003 Server作为证书颁发机构(CA)服务器。

## <u>网络图</u>

本文档使用以下网络设置:





要实现此配置,请完成以下步骤:

- 在 WLC 上将 EAP-FAST 配置为本地 EAP 身份验证方法
- <u>配置 LDAP 服务器</u>
- 配置无线客户端

# 在 WLC 上将 EAP-FAST 配置为本地 EAP 身份验证方法

如前所述,本文档使用 EAP-FAST 作为本地 EAP 验证方法,与客户端和服务器端上的证书配合使用。第一步是将以下证书下载并安装到服务器(本示例中为 WLC)和客户端上。

WLC 和客户端均需要从 CA 服务器下载以下证书:

- 设备证书(一个用于 WLC,一个用于客户端)
- •WLC的公钥基础设施(PKI)的根证书,客户端的CA证书

## 为 WLC 生成设备证书

要从 CA 服务器为 WLC 生成设备证书,请执行以下步骤。此设备证书由 WLC 用于对客户端进行身 份验证。

 在与 CA 服务器相连的 PC 上,访问 http://<CA 服务器的 IP 地址>/certsrv。以CA服务器的管 理员身份登录。



2. 选择 Request a certificate。

Address 🕘 http://10.77.244.190/certary/	~
Mirmant Parificata Sanitan windons	н
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. B identity to people you communicate with over the Web, sign and encrypt messages, and, dependi perform other security tasks.	Ay using a certificate, you can verify your ing upon the type of certificate you request,
You can also use this Web site to download a certificate authority (CA) certificate, certificate chair view the status of a pending request.	in, or certificate revocation list (CRL), or to
For more information about Certificate Services, see <u>Certificate Services Documentation</u> .	
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
1	Internet
E"Request a Certificate"页中,单击 <b>advanced certificate requ</b>	uest。
E"Request a Certificate"页中,单击	iest。
E"Request a Certificate"页中,单击 advanced certificate requested to the services advanced certificate requested to the services advanced to the servi	iest。
E"Request a Certificate"页中,单击 advanced certificate requested to the second certificate requested to t	uest₀ □
E"Request a Certificate"页中,单击 advanced certificate requested for the services Microsoft Certificate Services Microsoft Internet Explorer  Content of the Services Tools Help  Attrace of Microsoft Certificate Services - Wireless	iest。 E •
E"Request a Certificate"页中,单击 advanced certificate request a Certificate request a Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - wireless Request a Certificate	uest。 □ ■
E"Request a Certificate"页中,单击 advanced certificate requests Alicrosoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Wireless Request a Certificate Select the certificate type:	uest。 [ ] Ha
E"Request a Certificate"页中,单击 advanced certificate request a Certificate services Microsoft Internet Explorer  Control Certificate Services - Microsoft Internet Explorer  Atternooft Certificate Services - Wireless  Request a Certificate  Select the certificate type: User Cartificate	iest。 C
E"Request a Certificate"页中,单击 advanced certificate request a Certificate services - Microsoft Internet Explorer  Microsoft Certificate Services - Microsoft Internet Explorer  Microsoft Certificate Services - Wireless  Request a Certificate Select the certificate type: User Codificate type: User Codificate Or Submit an advanced certificate request.	uest。 □ ■
王"Request a Certificate"页中,单击 advanced certificate request a Certificate services - Microsoft Internet Explorer Ne. Eds. Vew Revertes: Tools: Nep Kitcrosoft Certificate Services - wireless Request a Certificate Select the certificate type: User Cartificate Or submit an advanced certificate request.	uest。 □ ■ ■
王"Request a Certificate"页中,单击 advanced certificate request. Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Wireless Request a Certificate Select the certificate type: User Cartificate Or Submit an advanced certificate request.	iest。
E"Request a Certificate"页中,单击 advanced certificate request a Certificate Services - Microsoft Internet Explorer  Microsoft Certificate Services - Microsoft Internet Explorer  Microsoft Certificate Services - Wireless  Request a Certificate Select the certificate type: User Cartificate Or submit an advanced certificate request.	iest。
E"Request a Certificate"页中,单击 advanced certificate request a Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - wireless Request a Certificate Select the certificate type: User Contificate Type:	iest。
E"Request a Certificate"页中,单击 advanced certificate requests Microsoft Certificate Services - Microsoft Internet Explorer	iest。
E"Request a Certificate"页中,单击 advanced certificate requests Microsoft Certificate Services - Microsoft Internet Explorer	iest。
E"Request a Certificate "页中,单击 advanced certificate request Microsoft Internet Explorer  Microsoft Certificate Services - Microsoft Internet Explorer  Microsoft Certificate Services - Microsoft Internet Explorer  Microsoft Certificate Services - Wireless  Request a Certificate Select the certificate type: User CatHicette Or submit an advanced certificate request.	uest。
E"Request a Certificate Total Internet Explorer Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Wireless Microsoft Certificate Services - Wireless Request a Certificate type: User Cartificate Total Or submit an advanced certificate request.	uest。
E"Request a Certificate Services - Microsoft Internet Laplorer Microsoft Certificate Services - Microsoft Internet Laplorer Microsoft Certificate Services - Microsoft Internet Laplorer Microsoft Certificate Services - Wireless Request a Certificate Select the certificate type: User Cartificate Or submit an edwanced certificate request.	iest。
E"Request a Certificate Services Microsoft Internet Lxplorer Microsoft Certificate Services Microsoft Internet Lxplorer Microsoft Certificate Services Microsoft Internet Lxplorer Microsoft Certificate Services - Microsoft Request a Certificate Select the certificate type: User Cadificate Or submit an advanced certificate request.	uest。
生"Request a Certificate"页中,单击 advanced certificate requered internet implorer  Microsoft Certificate Services Microsoft Internet Implorer  Microsoft Certificate Services - wireless  Request a Certificate Select the certificate type: User Cathlecets  Or submit an advanced certificate request.	uest。
生"Request a Certificate"页中,单击 advanced certificate request interest intere	uest。
生"Request a Certificate"页中,单击 advanced certificate requered internet inplorer  Mitcrosoft Certificate Services - Mitcrosoft Internet Inplorer  Mitcrosoft Certificate Services - Wireless Request a Certificate Select the certificate type: User Cartificate Or submit an advanced certificate request.	uest。
生"Request a Certificate"页中,单击 advanced certificate requeed Microsoft Certificate Services - Microsoft Internet Lipplorer  Microsoft Certificate Services - Wireless Request a Certificate Select the certificate type: User Cartificate type: Or submit an advanced certificete request	uest。
在中国中的中国中国的中国中国的中国中国的中国中国的中国中国的中国中国的中国中国	uest。

4. 在"Advanced Certificate Request"页中,单击 Create and submit a request to this CA。这将显示高级证书请求表。

Microsoft Certificate Services - Microsoft Internet Explorer		
e Edit View Favorites Tools Help		1
dress 🕘 http://10.77.244.198/certsrv/certropad.asp		👱 🔁 Go
Microwoff Certificate Services - wireless		Heme
dvanced Certificate Request		
he policy of the CA determines the types of certificates you can request. Click of	ne 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 PKCS #7 file.	file, or submit a renewal request by usin	ng a base-64-encoded
Request a certificate for a smart card on behalf of another user by using the s Note: You must have an enrollment agent certificate to submit a request on behalf of another	mart card certificate enrolment station, ruser.	
		Tobarnat

- 5. 在高级证书请求表中,选择 Web Server 作为证书模板。然后,指定此设备证书的名称。本示 例使用 ciscowlc123 作为证书名称。根据需要填写其他识别信息。
- 6. 在 Web Server 部分下,选择"Mark Keys as Exportable"选项。有时,如果您选择 Web 服务器 模板,此选项将变灰,并且不能启用或禁用。在这种情况下,从浏览器菜单中单击**返回返回一 页,再次回到此页。**此时"Mark Keys as Exportable"选项应该就可用了。

Microsoft Certi	ificate Services - Microsoft Internet Explorer	
File Edit View	Pavorites Tools Help	
G tack • 💭	- E C C - Search of Parenters @ 20 - 3 5 5 3	
ddress 🍇 http://14	0.77.244.198/certary/certrgna.asp	🛩 🛃 GO
Allower R. Court		
Macrosoft Certifi	Lais Sentes - midless	nome
Advanced Ce	ertificate Request	
Certificate Temp	plate:	
	Web Server	
Identifying Infor	rmation For Offline Template:	
Name:	eiscowlc123	
E-Mail		
Company:	cisco	
Department:		
City		
State		
Country/Region:		
Key Options:		
	Create new key set     Ouse existing key set	
CSP:	Microsoft RSA SChannel Cryptographic Previder	
Key Usage:	(*) Exchange	
Key Size:	1024 Max 10304 (common key sizer <u>512 1024 2048 4090 0192 10284</u> )	
	Automatic key container name     O User specified key container name	
	Mark keys as exportable	
	Export keys to file	
	Enable strong private Key protection     Stars cartificate is the level commuter cartificate store	
	Characteria and the focus computer centricate store	
Done		Internet

7. 配置其他所有必要字段,然后单击 Submit。

Microsoft Certil	ficate Services - Microsoft Internet Explorer	
File Edit View I	Pavorites Tools Help	<b>A</b>
G tak • 🕥	- 🖻 🗟 🐔 🔎 Search 👷 Pavortes 🥝 🔗 - 😓 🖼 🦓	
Address 者 http://10	0.77.294.198/certary/cerbrana.asp	💌 🔁 😡
	Create new key set	
CSP:	Microsoft RSA SChannel Cryptographic Previder 💌	
Key Usage:	Exchange	
Key Size:	1024 Min: 304 (common key sizes: 512, 5029 2048 4085 5192, 15384.)	
	Automatic key container name     O User specified 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 CA's certificate. You must be an administrator to generate or use a key in the local machine store.	
Additional Optio	105:	
Request Format:	OCMC OPKCS10	
Hash Algorithm:	SHA-1 Conty used to sign request.	
	Save request to a file	
Attributes:		
Friendly Name:		
	Submit >	
1.h		1.1.1.7

8. 在下一个窗口中单击 Yes,以便开始证书请求过程。

Potent	ial 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. 这将显示"Certificate Issued"窗口,表明证书请求过程已成功。下一步是将颁发的证书安装到此 PC 的证书存储中。单击 Install this certificate。

2011 Mtp://10.77.244.198/certsrv/cert/roh.asp	×
dicrosoft Certificate Services - wireless	He
ertificate Issued	
he certificate you requested was issued to you.	
( Install this certificate )	
	Triturnat
	🔮 Internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。	Internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Explorer Rev Eds. View Favorates_Tools_1940	🕒 internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Explorer The Eds Wew Favorase Tools Help	Internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Explorer Re Ed: West Pavortes_Tools_Help	internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Explorer Ne Ed: Wee Favorase Tools Help	internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Explorer Re Ex West Favorites_Tools_Help Address Microsoft Certificate Services - weekers Certificate Installed Your new certificate has been successfully installed.	Internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Explorer Re EX West Pavortes_Tools_Help Address Pavortes_Tools_Help Address Pavortes_Tools_Help Address Pavortes_Tools_Help Address Pavortes_Tools_Help Microsoft Certificate Services - wereless Certificate Installed Your new certificate has been successfully installed.	internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Explorer We Eds Wew Favoras Tools Help Address Phapel/10.77.244.198/bertsvy/certman.asp Microsoft Certificate Services - wireless Certificate Installed Your new certificate hes been successfully installed.	Internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Explorer Re Ex Wee Favores Toole_Hep Address Toole_Hep Microsoft Certificate Services - weekers Certificate Installed Your new certificate has been successfully installed.	Internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Explorer Refer Ca West Revolutes Tools _ Help Address Provement Certificate Services - wereless Certificate Installed Your new certificate has been successfully installed.	Internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Lxplorer Microsoft Certificate Services - Microsoft Internet Lxplorer Microsoft Certificate Services - Weekees Certificate Installed Your new certificate has been successfully installed.	Internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Lxplorer Re Ex Vee Favorites_Toole_Nep Address Travertes_Toole_Nep Address Travertes Services - weekers Certificate Installed Your new certificate has been successfully installed.	Internet
新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。 Microsoft Certificate Services - Microsoft Internet Lxplorer Microsoft Certificate Services - Microsoft Internet Lxplorer Microsoft Certificate Services - Weekes Certificate Installed Your new certificate has been successfully installed.	Internet
Microsoft Certificate Services _ Microsoft Internet Leptorer Ne Cit Wee Pavortee Toole Nep Addree ● Mapu/10.77.244.198/Unitervy/certrage.age Microsoft Certificate Services → Weekees Certificate Installed Your new certificate has been successfully installed.	. Internet 
Microsoft Certificate Services Microsoft Internet Lipitore Microsoft Certificate Services Microsoft Internet Lipitore Microsoft Certificate Services Tools Help Microsoft Certificate Services - Weekess Certificate Installed Your new certificate has been successfully installed.	Internet
Hitraedf Certificate Strates Microsoft Internet Explorer Microsoft Certificate Strates Nicrosoft Internet Explorer Certificate Installed Your new certificate has been successfully installed.	Internet
Hitrosoft Certificate Services - Microsoft Internet Explorer Microsoft Certificate Services - Microsoft Internet Explorer Certificate Installed Your new certificate has been successfully installed.	Internet
Microsoft Certificate Services - Microsoft Internet Laplorer Microsoft Certificate Services - Microsoft Internet Laplorer Microsoft Certificate Services - Wateves Certificate Installed Your new certificate has been successfully installed.	Internet
Microsofi Certificate Services _ Microsofi Internet Laplorer Microsofi Certificate Services _ Microsofi Internet Laplorer Microsofi Certificate Services _ Microsofi Internet Laplorer Microsofi Certificate Services _ Microsofi Certificate Installed Your new certificate has been successfully installed.	Internet
Wicrosoft Certificate Services - Wicrosoft Internet Laplorer Microsoft Certificate Services - Wicrosoft Internet Laplorer Microsoft Certificate Services - Wicrosoft Certificate Installed Your new certificate has been successfully installed.	Internet

11. 下一步是从证书存储中将此证书作为文件导出到硬盘上。此证书文件以后将用于将证书下载 到 WLC 上。为了从证书存储中导出证书,请打开 Internet Explorer 浏览器,然后单击**工具 >** Internet 选项。

about:blank - Microsoft Internet Explorer	
File Eds View Pavortes Tools Help	27
Address (a) about think, Mad and News *	💌 🛃 Go
Pop-up Blocker +	-
Manage Add-ons	
aprict/enter	
windows relationing	
an en en el polente : .	
	~
Dublics you to change settings.	

12. 单击内容 > 证书,以便访问用于安装证书的默认证书存储。

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. 设备证书通常安装在**个人证书列表下。**在此,您应该看到新安装的证书。选择该证书,然后 单击**导出**。

Certificate	25				?	×
Intended p	urpose:	<all></all>				~
Personal	Other Peop	le Intermediate Certification	Authorities Trusted Ro	ot Certification	<	>
Issued	То	Issued By	Expiratio Frien	dly Name		
🕮 cisco	owlc123	wireless	1/25/2010 <non< td=""><td>e&gt;</td><td></td><td></td></non<>	e>		
Import.		Remove		Advanc	ed.	
Certificate	e intended p	urposes				
Server Au	uthentication			View		)
				Clos	e	

14. 在接下来的窗口中单击**下一步。**在"证书导出向导"窗口中选择**是,导出私有密钥选项。**单击 Next。

Certificate Export Wizard	×
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.	
Do you want to export the private key with the certificate?	
Yes, export the private key	
No, do not export the private key	
< Back Next > Cancel	

15. 选择 .pfx 作为导出文件格式,并且选择"启用严格保护"选项。单击 Next。

Certificate Export Wizard	×
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	J
< Back Next >	Cancel
6. 在"密码"窗口中,输入密码。本示例使用 <b>cisco 作为密码。</b>	
Certificate Export Wizard	
Password	

To maintain security, you must protect the private key by using a password.

Passworu:	
*******	
Confirm password:	
*******	

17. 将证书文件(.PFX 文件)保存到硬盘上。单击下一步并成功完成导出过程。

Certificate Export Wizard	
File to Export Specify the name of the file	you want to export
File name:	
C: (OpenSSL2(bin)(ciscowic)	23.prx Browse
	< Back Next > Cancel
Certificate Export Wizard	×
	Completing the Certificate Export Wizard Vou have successfully completed the Certificate Export wizard. Vou have specified the following settings: File Name Export Keys Include all certificates in the certification path File Format
Certificate Export Wizard	
The export was successful.	< Back Finish Cancel

## 将设备证书下载到 WLC 上

现在 WLC 设备证书已经导出为 .PFX 文件,下一步是将该文件下载到控制器上。Cisco WLC 仅接 受 .PEM 格式的证书。因此,您首先要使用 openSSL 程序,将 .PFX 或 PKCS12 格式的文件转换 为 PEM 文件。

使用 openSSL 程序将证书从 PFX 格式转换为 PEM 格式

您可以将证书复制到任何已安装 openSSL 的 PC 上,以便将其转换为 PEM 格式。对 openSSL 程 序的 bin 文件夹中的 OpenssI.exe 文件,输入以下命令:

**注意**:可以从OpenSSL网站下<u>载</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

证书文件就被转换为 PEM 格式。下一步是将 PEM 格式的设备证书下载到 WLC 上。

**注意:**在此之前,需要在要从中下载PEM文件的PC上安装TFTP服务器软件。此 PC 应该与 WLC 相连。TFTP 服务器应该将其当前目录和基准目录指定为存储 PEM 文件的位置。

将转换后的 PEM 格式的设备证书下载到 WLC 上

本示例通过 WLC 的 CLI 来解释下载过程。

- 1. 登录到控制器的 CLI。
- 2. 输入 transfer download datatype eapdevcert 命令。
- 3. 输入 transfer download serverip *10.77.244.196* 命令。10.77.244.196 是 TFTP 服务器的 IP 地 业。
- 4. 输入 **transfer download filename** *ciscowlc.pem* 命令。本示例中使用 ciscowlc123.pem 文件名。
- 5. 输入transfer download certpassword命令设置证书的密码。
- 6. 输入 transfer download start 命令,以便查看更新后的设置。然后,在显示提示时,回答 y,以便确认当前设置并开始下载过程。本示例显示了下载命令的输出: (Cisco Controller) >transfer download start

Mode.		TFTP
Data	Туре	Vendor Dev Cert
TFTP	Server IP	10.77.244.196
TFTP	Packet Timeout	б
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. 输入 reset system 命令,以便重新启动控制器。控制器现在已经加载了该设备证书。

#### <u>将 PKI 的根证书安装到 WLC 中</u>

现在设备证书就已经安装到 WLC 中,下一步是从 CA 服务器将 PKI 的根证书安装到 WLC 上。请 执行以下步骤:

 在与 CA 服务器相连的 PC 上,访问 http://<CA 服务器的 IP 地址>/certsrv。以 CA 服务器的管 理员身份登录。



2. 单击 Download a CA certificate, certificate chain, or CRL。

Alicrosoft Certificate Services - Microsoft Internet Explorer	- 2
Pile Ede Ven Pileotas Took Julo	- 21
iddinis @Http://10.77.244.190/cettary/	<del>)</del> 60
Memory On Sectors Sectors Weeklass	10
Welcome	_
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.	
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.	
For more information about Certificate Services, see Certificate Services Documentation.	
Select a task: Request a certificate	
View the status of a pending certificate request	
Download a CA certificate, certificate chain, or CRL	
	_
2 Internet	
午所显示的页中,您会在 CA certificate <b>框下看到 CA 服务器上当前可用的 CA 证书</b> 。选择	

3. 在所显示的页中,您会在 CA certificate 框下看到 CA 服务器上当前可用的 CA 证书。选择 DER 作为编码方法,然后单击"Download CA certificate"。

A Microsoft Certificate Services - Microsoft Internet Explorer	
Påe Edit View Pavorities Tools Help	1
Zdános 🕘 http://10.77.244.198/certsev/certcarc.asp	🛩 🔁 Go
Microsoff Certificate Services - wireless	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:	
DER     Dase 64	
Download CA certificate	
Download CA certificate chain	
Download latest deta CRL	
el	Internet

- 4. 将证书另存为.cer 文件。本示例使用 certnew.cer 作为文件名。
- 5. 下一步是将 .cer 文件转换为 PEM 格式,并将其下载到控制器上。要执行这些步骤,请重复将 设备证书下载到 WLC 上部分所述的过程,但有以下变化:openSSL 的 "-in" 和 "-out" 文件分 别为 certnew.cer 和 certnew.pem。而且,此过程不需要 PEM 通行证短语或导入密码。而且 ,用于将 .cer 文件转换为 .pem 文件的 openSSL 命令是:x509 -in certnew.cer -inform DER out certnew.pem -outform PEM在将转换后的 PEM 格式的设备证书下载到 WLC 上部分中的 第2步中,用于将证书下载到 WLC 上的命令是:(Cisco Controller)>transfer download datatype eapcacert要下载到 WLC 上的文件是 certnew.pem。

您可以按照以下方法,从控制器的 GUI 中验证证书是否已安装到 WLC 上:

• 从 WLC GUI 中,单击 Security。在"Security"页中,从左侧显示的任务中单击 Advanced > IPSec Certs。单击 CA Certificate,以便查看已安装的 CA 证书。如下面的示例所示 :



• 要验证设备证书是否已安装到 WLC 上,请从 WLC GUI 中单击 Security。在"Security"页中 ,从左侧显示的任务中单击 Advanced > IPSec Certs。单击 ID Certificate,以便查看已安装的 设备证书。如下面的示例所示

a wic2006 - Microsoft Inter	rnet Explorer									
File Edit View Favorites	Tools Help									
ahaha									<u>Ping</u> Log	out <u>R</u> efresh
cisco	MONITOR	WLANS	CONTROLLER	W1RELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Security	ID Certific	ate			$\smile$					New
▼ ARA General ▼ RADIUS Authentication Accounting IN TACACS+	Name bsnSslEapD	erCert		lid Period Im 2008 Jan 24	ቴት, 12:18:31 G	MT Until 2010 Jan	n 23rd, 12:18:31	•		
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies										
E Local EAP										
F Priority Order										
E Access Control Lists										
Wireless Protection     Policies										
N Web Auth										
<ul> <li>✓ Advanced</li> <li>▶ CIDS Sensors Shunned Clients</li> <li>▼ IPSec Certs</li> <li>Cartificate</li> <li>1D Certificate</li> </ul>										
<u>.</u>								1	) 🔵 Internet	

## <u>为客户端生成设备证书</u>

现在设备证书和 CA 证书均已安装到 WLC 上,下一步是为客户端生成这些证书。

要为客户端生成设备证书,请执行以下步骤。此证书将由客户端用来对 WLC 进行身份验证。本文 档解释在为 Windows XP Professional 客户端生成证书时所需的步骤。

 从需要安装证书的客户端上,访问 http://<CA 服务器的 IP 地址>/certsrv。以域名\用户名的形 式登录到 CA 服务器上。用户名应该是使用这台 XP 计算机的用户的名称,并且应该已经在与 CA 服务器相同的域中配置了此用户。

Connecting to 10.77.244.198 User name: Password: Remember my password Remember my password Remember my password Concel Remember my password Concel Remember my password Concel Remember my password Concel Remember my password Concel Remember my password Concel Remember my password Concel Co		
Connecting to 10.77.244.198 User name: Password: Password: Remember my password Concel Coc	<u>31</u> 30	
User name:       Image: wireless\user2         Password:       Image: wireless\user2         Remember my password         Image: wireless wireless         Image: wireless         Image: wireless         Image: wireless         Image: wireless         Image: wireless         Image: wirele	Connecting to 10.77.24	14.198
Password: Remember my password Concel Conce	Username:	🖸 wireless\user2 🛛 🔛
	Password:	
Concel	C	Remember my password
OK       Concel         Bit Proventies Contributes Services       Microsoft Internet Explorer         Fig. 58       View Proventies Toole Links         Microsoft Contificate Services       Microsoft Internet Explorer         Microsoft Contificate Services       Microsoft Contificate Services         Microsoft Contificate Services, see Centificate subnority (CA) centificate chain, or certificate revocation list (CRL), or to view the status of a pending request.         For more information about Certificate Services, see Centificate Services Documentation.         Setext a task:       Microsoft Contificate Contificate request         Microsoft Contificate Contificate chain, or CRL		
生 子 Request a certificate  Microsoft Certificate Services Microsoft Internet Explorer  Microsoft Certificate Services Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Certificate Services Microsoft Microsoft Certificate Services Microsoft Microsoft Certificate Services Microsoft Microsoft Certificate Services Microsoft Microsoft Microsoft Microsoft Certificate Services Microsoft		OK Cancel
Diff Request a certificate         Microsoft Certificate Services - Microsoft Internet Explorer         Ret Ven Provide: Took Help         Microsoft Certificate Services - Microsoft Internet Explorer         Microsoft Certificate Services - Wereless         Welcome         Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to be pople you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.         You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.         For more information about Certificate Services, see Certificate Services Documentation.         Select a task:         Request a certificate         View the status of a pending certificate request         Download a CA certificate chain, or CRL	S Deguaat a aartifiaata	
Text       Year       Pavertisis       Tools       Help       Help       Tools       Help       Help       Help       Tools       Help	F Request a certificate. crosoft Certificate Services - Microsoft Internet Explorer	
Addison @ Metpu/rt0.77.244.198/certarv/       Image: Comparison of Contificate Services - Weekees         Microsoft Contificate Services - Weekees       Herm         Welcome       Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.         You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.         For more information about Certificate Services, see Certificate Services Documentation.         Select a task:         Request a certificate, certificate request         Download a CA certificate, certificate chain, or CRL	Edt Ven Favorites Tools Help	
Microsoft Certificate Services wireless       Ham         Welcome       Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.         You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.         For more information about Certificate Services, see Certificate Services Documentation.         Select a task:         Request a certificate         View the status of a pending certificate request         Download a CA certificate, certificate chain, or CRL	A Mapel/10.77.244.198/certary/	× Þ
Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identify to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Certificate Services, see Certificate Services Documentation. Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	rosoft Certificate Services wireless	Home
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Certificate Services, see <u>Certificate Services Documentation</u> . Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	lcome	
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Certificate Services, see <u>Certificate Services Documentation</u> .	this Web site to request a certificate for your Web nity to people you communicate with over the Web, form other security tasks.	browser, e-mail client, or other program. By using a certificate, you can verify your sign and encrypt messages, and, depending upon the type of certificate you request,
For more information about Certificate Services, see <u>Certificate Services Documentation</u> .  Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	can also use this Web site to download a certificat v the status of a pending request.	e authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	more information about Certificate Services, see C	Certificate Services Documentation.
View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	ect a task:	
Download a CA certificate, certificate chain, or CRL	liew the status of a pending certificate request	
	Jownload a CA certificate, certificate chain, or CRL	•
		a Internat

3. 在"Request a Certificate"页中,单击 advanced certificate request。

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edt View Favorities Tools Help	
Address and http://10.77.244.198/certsrv/certraus.asp	💌 🔁 Go
All second de la calificación de la companya de la	
Alicrosoff Certificate Services wiretess	Home
Request a Certificate	
Select the certificate type:	
User Certificate	
Or submit an advanced certificate request.	
(i) http://10.77.244.198/centerv/centrgad.asp	Internet

4. 在"Advanced Certificate Request"页中,单击 **Create and submit a request to this CA。**这将显示高级证书请求表。

Microsoft Certificate Services - Microsoft Internet Explorer	
e Edit View Favorites Tools Help	1
ess al http://10.77.244.198/certsrv/certrgad.asp	🖂 🛃 G
Hannach Andlenia Randana - saladana	
Norowolf Certificate Services - wireless	Heme
dvanced Certificate Request	
te policy of the CA determines the types of certificates you can request. Click one of the following	options to:
Create and extent a request to this CA	opiona to:
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a re PKCS #7 file.	newal request by using a base-64-encoded
Request a certificate for a smart card on behalf of another user by using the smart card certificat	e enrolment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.	
	Internet
局级业书请求表中,从"Certificate Template"下拉菜单中选择	<b>User。</b> 在密钥选项部分下,

5. 在高级证书请求表中,从"Certificate Template"下拉菜单中选择 User。在密钥选项部分下,选择以下参数:在"Key Size"字段中输入密钥大小。本示例使用 1024。选中 Mark Keys as Exportable 选项。

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 keyo 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. 配置其他所有必要字段,然后单击 Submit。

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
🔾 Sadi + 🔘 - 📓 🐔 🔎 Search 👷 Pavortes  😥 🖓 🚃 🖄	
Sdiress 💨 https://10.77.244.198/certary/certrana.asp	🖌 🎦 😁
Create new key set Use existing key set	
CSP: Microsoft RSA SChannel Cryptographic Provider	
Kay Usage: 🛞 Exchange	
Key Size: 1024 Min: 004 (cemmon keysizes: 532 1025 2046 4085 5192 15355 )	
Automatic key container name O User specified key container name	
Mark keys as exportable	
Export keys to file	
Enable strong private key protection	
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: OCMC	
Hash Algorithm: SHA-1 V Only used to sign request.	
Save request to a file	
Attributes:	
Friendly Name:	
Submit >	

7. 客户端的设备证书现在就已根据您的请求而生成。单击 Install the certificate,以便将证书安装 到证书存储中。

and shall be a second to the state	and manual adjusted		مت الت
File Edit View Payorites Tools Help		8°.	
Address 🕘 http://10.77.244.190/certsrv/cert/re	h,asp		<b>×</b> 🔁
Microsoff Certificate Services - wirele	15		<u>Home</u>
Certificate Issued			
The second			
The centricate you requested was	seved to you.		
Install this certificate			
e)			🐌 Internet
❶ 甬过客户端的 IF 浏览器	。 您应该能够在工 <b>具&gt;</b> Ir	nternet 选项 > 内容 >	↓ 证书下的个人证书列录
■ 通过客户端的 IE 浏览器 由找到已安装的客户端	器,您应该能够在 <b>工具&gt;lr</b> 设 <b>条证书</b> 。	iternet 选项 > 内容 >	● Internet 证书下的个人证书列录
通 通过客户端的 IE 浏览器 中找到已安装的客户端	器,您应该能够在 <b>工具 &gt; Ⅰr</b> <b>设备证书。</b>	iternet 选项 > 内容 >	♥ Internet 证书下的个人证书列表
通过客户端的 IE 浏览器 <b>中找到已安装的客户端</b> Certificates	器,您应该能够在 <b>工具&gt;Ⅰr 设备证书。</b>	iternet 选项 > 内容 >	♥ Internet 证书下的个人证书列表 [22] [
通过客户端的 IE 浏览器 中 <b>找到已安装的客户端</b> Certificates Intended purpose:	髻,您应该能够在 <b>工具&gt;Ir 设备证书。</b> _ <a⊪></a⊪>	iternet 选项 > 内容 >	● Internet 证书下的个人证书列表 [2][ [ ~
通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo	器,您应该能够在工 <b>具&gt; lr 设备证书。</b> 	nternet 选项 > 内容 >	♥ Internet 证书下的个人证书列表
自过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo	器,您应该能够在工 <b>具&gt;  r 设备证书。</b> 	nternet 选项 > 内容 > on Authorities Truster	♥ Internet 证书下的个人证书列表 ?? I Root Certification ◀ >
通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo	器,您应该能够在工具>Ir 设备证书。 <all> ple Intermediate Certificat</all>	iternet 选项 > 内容 > on Authorities Truster Expiratio F	● Internet 证书下的个人证书列表 2 d Root Certification
● 通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo ■ 1234	器,您应该能够在工具>Ir 设备证书。 <all> ple Intermediate Certificat Issued By wireless</all>	iternet 选项 > 内容 > on Authorities Truster Expiratio E 1/25/2009 <	● Internet 证书下的个人证书列表 d Root Certification riendly: Name None>
通过客户端的 IE 浏览器 P找到已安装的客户端 Certificates Intended purpose: Personal Other Peo	器,您应该能够在工 <b>具</b> >Ir 设备证书。 <all> ple Intermediate Certificat Issued By wireless</all>	iternet 选项 > 内容 > on Authorities Truster <u>Expiratio F</u> 1/25/2009 <	● Internet 证书下的个人证书列引 ?? I d Root Certification d Root Certification *
通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo	器,您应该能够在工具>Ir 设备证书。 <all> ple Intermediate Certificat Issued By wireless</all>	iternet 选项 > 内容 > on Authorities Truster Expiratio F 1/25/2009 <	♥ Internet 证书下的个人证书列ā ?? d Root Certification ◀ ♪ riendly Name None>
通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo	器,您应该能够在工具>Ir 设备证书。 <all> ple Intermediate Certificat Issued By wireless</all>	on Authorities Truster Expiratio F 1/25/2009 <	● Internet 证书下的个人证书列表 ? d Root Certification * iendly: Name None >
通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo	器,您应该能够在工 <b>具&gt;Ir 设备证书。</b> <all> ple Intermediate Certificat <u>Issued By</u> wireless</all>	iternet 选项 > 内容 > on Authorities Truster Expiratio E 1/25/2009 <	● Internet 证书下的个人证书列引 ?? I d Root Certification *riendly: Name None>
通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo	器,您应该能够在工具>Ir 设备证书。 <all> ple Intermediate Certificat Issued By wireless</all>	nternet 选项 > 内容 > on Authorities Truster Expiratio F 1/25/2009 <	♥Internet 证书下的个人证书列ā d Root Certification niendly Name None>
● 通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo Issued To ■ 1234	器,您应该能够在工具>Ir 设备证书。 <all> ple Intermediate Certificat <u>Issued By</u> wireless</all>	nternet 选项 > 内容 > ion Authorities Truster Expiratio F 1/25/2009 <	● Internet 证书下的个人证书列ā ? d Root Certificatior niendly Name None >
● 通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo Issued To ■ 1234	器,您应该能够在工具>Ir 设备证书。 <all> ple Intermediate Certificat Issued By wireless</all>	nternet 选项 > 内容 > on Authorities Truster Expiratio F 1/25/2009 <	w书下的个人证书列表 ② d Root Certification <del>viendly: Name</del> None>
通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo	main and a second sec	iternet 选项 > 内容 > on Authorities Truster Expiratio E 1/25/2009 <	■ Internet 证书下的个人证书列表 I Root Certification A Root Certification
Ma过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo 「Issued To 「第1234	a,您应该能够在工具>Ir 设备证书。 <all> ple Intermediate Certificat Issued By wireless</all>	iternet 选项 > 内容 > on Authorities Truster Expiratio F 1/25/2009 <	● Internet 证书下的个人证书列表 d Root Certification niendly Name None>
● 通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo Issued To ■ 1234 Import Ex	a , 您应该能够在工具 > Ir 设备证书。 <all> ple Intermediate Certificat Issued By wireless</all>	nternet 选项 > 内容 > on Authorities Truster Expiratio F 1/25/2009 <	■ Internet 证书下的个人证书列表 d Root Certification None> Advanced
自过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo 「Issued To 「三1234 Import Ex Certificate intended p	a , 您应该能够在工具 > In 设备证书。 <all> ple Intermediate Certificat Issued By wireless port Remove</all>	nternet 选项 > 内容 > on Authorities Truster Expiratio E 1/25/2009 <	● Internet 证书下的个人证书列表 d Root Certification riendly Name None> Advanced
■ 通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo 「Issued To ■ 1234 Import Ex Certificate intended p Encrypting File System	a, 您应该能够在工具 > In 设备证书。 ( <all> ple Intermediate Certificat Issued By wireless port Remove</all>	nternet 选项 > 内容 > on Authorities Truster Expiratio E 1/25/2009 <	Utternet 证书下的个人证书列表 Cont Certification Cont Certification Cont Certification Cont Certification Cont Certification Cont Certification
■ 通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo 「国1234 Import Ex Certificate intended p Encrypting File Syster	a,您应该能够在工具 > Ir 设备证书。 <all> ple Intermediate Certificat Issued By wireless port Remove</all>	nternet 选项 > 内容 > on Authorities Truster Expiratio F 1/25/2009 <	♥ Internet 证书下的个人证书列表 Carlendly Name None> Advanced
■ 通过客户端的 IE 浏览器 中找到已安装的客户端 Certificates Intended purpose: Personal Other Peo Issued To IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	a , 您应该能够在工具 > In 设备证书。 ( <all> ple Intermediate Certificat Issued By wireless port Remove</all>	nternet 选项 > 内容 > on Authorities Truster Expiratio F 1/25/2009 <	● Internet 证书下的个人证书列君 Carlendly Name None> Advanced

客户端的设备证书就已经安装到客户端上。

# 为客户端生成根 CA 证书

下一步是为客户端生成 CA 证书。请从客户端 PC 完成以下步骤:

 从需要安装证书的客户端上,访问 http://<CA 服务器的 IP 地址>/certsrv。以域名\用户名的形 式登录到 CA 服务器上。用户名应该是使用这台 XP 计算机的用户的名称,并且应该已经在与 CA 服务器相同的域中配置了此用户。

Connect to 10.77	.244.198	2 🔀
		1955 Fred
Connecting to 10.77	.244.198	
User name:	🛃 wireless\user2	<b>~</b>
Password:		
	Remember my pas	sword
	ОК	Cancel

2. 在所显示的页中,您会在 CA certificate 框下看到 CA 服务器上当前可用的 CA 证书。选择 Base 64 作为编码方法。然后,单击 Download CA certificate,并将文件作为.cer 文件保存到 客户端 PC 上。本示例使用 rootca.cer 作为文件名。

🔿 Microsoft Certificate Services - Microsoft Internet Explorer	🖬 🖬 🔣
File Edit Vers Factorities Tools Tellip	A
Address W Hetpol/10.77.244.198/certsrv/certcarc.asp	👻 🔁 😡
Microsoft Certificate Services without	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:	
Encoding method: O DER O Base 64	
Download CA certificate	
Download latest base CRL	
Download latest delta CRL	
	Internet

3. 下一步,将 .cer 格式的 CA 证书安装到客户端的证书存储中。双击 rootca.cer 文件,然后单击 **安装证书**。

Certifica	te	<b>?</b> ×
General	Details Certification Path	
	Certificate Information	
This	• certificate is intended for the following purpose(s): • All issuance policies • All application policies	
-	Issued to: wireless	-
	Issued by: wireless	
	Valid from 1/23/2008 to 1/23/2013	
	Install Certificate] Issuer Staten	nent
		OK ]

4. 单击下一步,以便将证书从客户端的硬盘导入到证书存储中。

Certificate Import Wizard	
	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. 选择根据证书类型,自动选择证书存储,然后单击"下一步"。

Certifi	cate Import Wizard	
Cert	t <b>ificate Store</b> 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	
	O Place all certificates in the following store	
	Certificate store:	
	Browse	
	< Back (Next > ) Cance	

6. 单击完成,以便	完成导入过程。			
Certificate In	nport Wizard			×
		Completing the C Wizard You have successfully complexizard. You have specified the follow	eted the Certificate Import	
		Certificate Store Selected Content	Automatically determined by t Certificate	
		< Back	Finish Cancel	

7. 默认情况下,CA 证书安装在客户端 IE 浏览器的工具 > Internet 选项 > 内容 > 证书下的"受信任的根证书颁发机构"列表下。如下面的示例所示

ntermediate Certifica	ation Authorities Trusted Root C	ertification Aut	norities DTrusted Pub	4
Issued To	Issued By	Expiratio	Friendly Name	~
VeriSign Trust N	letw VeriSign Trust Network	5/19/2018	VeriSign Class 3	
VeriSign Trust N	letw VeriSign Trust Network	8/2/2028	VeriSign Class 3	
VeriSign Trust N	Jetw VeriSign Trust Network	5/19/2018	VeriSign Class 4	
VeriSign Trust N	Jetw VeriSign Trust Network	8/2/2028	VeriSign Class 1	
VeriSign Trust N	letw VeriSign Trust Network	8/2/2028	VeriSign Class 4	
VeriSign Trust N	Jetw VeriSign Trust Network	5/19/2018	VeriSign Class 1	
EE wireless	wireless	1/23/2013	<none></none>	
Wireless-CA	Wireless-CA	12/18/2012	<none></none>	
Xcert EZ by DS	Xcert E2 by DST	7/11/2009	Xcert EZ by DST	~
Import Ex	port Remove		Advanc	ed
<all></all>				
				_

EAP-FAST 本地 EAP 身份验证所需的所有证书都已经安装在 WLC 和客户端上。下一步是为本地 EAP 身份验证配置 WLC。

## 在 WLC 上配置本地 EAP

要在 WLC 上配置本地 EAP 身份验证,请从 WLC GUI 模式完成以下步骤:

1. 单击 Security > Local EAP。

The Lett War Parents tools Help       Sage Configuration [Ping] Logart Lettersh         Security       Call Station ID Type [Pinddress]         * AAA       Call Station ID Type [Pinddress]         * AAA       Call Station ID Type [Pinddress]         * Windexating       Use ACS Koy Wrap         * TACACS+       Use ACS Koy Wrap         * Call Station ID Type [Pinddress]         * Windexating         * Call Station ID Type [Pinddress]         * Local IAP         * Nurdess Portection         * Mindess Portection         * Windess	wic2006 - Microsoft Inter	rnet Explorer	
Image: Circle Control Lists       Montrol WAANS CONTROLLER WIRELESS ECURITY MANAGEMENT COMMANDS HELP         Security       RADIUS Authentication Servers       Apply         * AAA       Coll Station JD Type       IP Address       Image: Control Lists         * ArcAcC4       LDAP       Use AEB Key Wrop       (Decigned for FIPS customers and requires a key wrap compliant RADIUS server)         * ACACC5       LDAP       Network User Nanagement Server Index Server Address Port IPSec Admin Status         * Drivity Order       * Advanced	File Edit View Povorites 1	Tools Help	
CISCO       MORNTOR       WLANS       CONTROLLER       WIPLELESS       SPOURTY       MANAGEMENT       COMMANDS       HELP         Security       RADIUS       Authentication       Servers       Apply       New         * AAA       Consrat       IP Address       IP       IP Address       IP         * AAA       Coll Station ID Type       IP Address       IP       IP       IP         * Athentication       Accounting       IP Address       IP	alada		figuration Ping Logout Befresh
Security       RADIUS Authentication Servers       Apply       New         Cali Station ID Type       P Address       Image: Cali Station ID Type       P Address         Cali Station ID Type       P Address       Image: Cali Station ID Type       Image: Cali Station ID Type <t< th=""><th>CISCO</th><th>MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS</th><th>HELP</th></t<>	CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	HELP
<ul> <li>AAA</li> <li>Gall Station 1D Type P Address</li> <li>Sabitis Accounting Accounting Accounting TraCAC3+ LOAP Load INST Users Not Ritering Disable Clears User User Nanagement Server Index Server Address Port 1PSec Admin Status</li> <li>Network User Nanagement Server Index Server Address Port 1PSec Admin Status</li> <li>Network User Nanagement Server Index Server Address Port 1PSec Admin Status</li> <li>Network User Nanagement Server Index Server Address Port 1PSec Admin Status</li> </ul>	Security	RADIUS Authentication Servers	Apply New
<ul> <li>RADUUS Accusation Accusatio</li></ul>	General	Call Station ID Type IP Address	
TACACS+       LOAP         Local Net Users       Network User Management Server Index Server Address Port IPSec Admin Status         Disabled Clines       Local EAP         Priority Order       Access Control Lists         Wireless Protection       Policies         Work Auth       Advanced	RADIUS     Authentication     Accounting	Use AES Key Wrop 🛛 (Designed for FIPS customers and requires a key wrap compliant RADIUS	server)
MAC Hitering Disabled Clients User Login Policies I Local EAP > Access Control Lists > Wroless Protection Policies > Wob Auth > Advanced	* TACACS+ LDAP	Network User Management Server Index Server Address Port IPSec Admin Status	
User Login Policies P Local EAP P Priority Order A Access Control Lists Wiebess Protection Policies E Web Auth E Advanced E Advanced E Internet	MAC Filtering Disabled Clients		
	User Login Policies		
Access Control Lists  Vireless Protection Policies  Web Auth Advanced  Itemst	Priority Order		
Wireless Protection Policies Web Auth Advanced	► Access Control Lists		
Web Auth Advanced  It is a state of the st	Wireless Protection Policies		
Advanced  Itemet	Web Auth		
Internet	▶ Advanced		
2 Internet			
2			
a 🖉 🖉 Internet			
a 🖉 🖉 Internet			
a			
a 🕒 🕲 Internet			
	<b>1</b>		🚔 🔵 Internet

2. 在"Local EAP"下,单击 Profiles,以便配置本地 EAP 配置文件。



- 3. 单击 New,以便创建新的本地 EAP 配置文件。
- 4. 为此配置文件指定名称,然后单击 Apply。本示例中的配置文件名称为 Idap。这会显示 WLC 上创建的本地 EAP 配置文件。

wic2006 - Microsoft Inter	net Explorer								
File Edit View Pavorites 1	fools Help								
ahaha							Save Co	nfiguration   <u>P</u>	ing   Logout   Befresh
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MONAGEMENT	COMMANDS	HELP	
Security	Local EA	P Profile	s > New					< Back	Apply
ARA General ADJUS Authentication Accounting TACACS+ LOAP Local Net Users MAC Fittering Disabled Clients User Login Policies AP Policies Cocal EAP General Profiles EAP-PAST Parameters	Profile No	ime		Idap					
Priority Order									
▶ Access Control Lists									
Wireless Protection     Policies									
▶ Web Auth									
▶ Advanced									
a) Done								A 4	Internet

- 5. 单击刚刚创建的 Idap 配置文件,该文件显示在"Local EAP Profiles"页的"Profile Name"字段下
  - 。这会显示 Local EAP Profiles > Edit 页。

wic2006 - Microsoft Inter	net Explorer tools Help							
						Saye Co	nfiguration Ping	Logout Befresh
CISCO	MONITOR WLA		WIRELES	SS SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EAP Pro	files					New	Apply
- AAA	Profile Name		LEAP	EAP-PAST	EAP-TLS	PEAP		
General * RADBUS Autheotication Accounting * TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Idea							
<ul> <li>Local EAP General Profiles EAP-FAST Parameters Authentication Priority</li> </ul>								
▶ Priority Order								
▶ Access Control Lists								
Wireless Protection Policies								
Web Auth								
Advanced								sternet

6. 在 Local EAP Profiles > Edit 页上配置此配置文件的特定参数。选择 EAP-FAST 作为本地 EAP 身份验证方法。启用 Local Certificate Required 和"Client Certificate Required"旁边的复选框。选择 Vendor 作为证书颁发者,因为此文档使用第三方 CA 服务器。启用 Check against CA certificates 旁边的复选框,以便从客户端传入的证书针对控制器上的 CA 证书进行 验证。如果希望根据控制器上的CA证书的CN验证传入证书中的公用名(CN),请选中Verify Certificate CN Identity复选框。默认设置为已禁用。为了使控制器能够验证传入的设备证书仍 然有效且尚未过期,请选中 Check Certificate Date Validity check 框。注意:根据控制器上配 置的当前UTC(GMT)时间检查证书日期有效性。忽略时区偏移。单击 Apply。

Ic2006 - Microsoft Inter	net Explorer								
Edit View Favorites T	ools Help								
ahaha								nfiguration <u>P</u>	ing Logout Bef
cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
curity	Local EA	P Profile	s ≻ Edit					< Dack	Apply
	Profile Na	me		Idap					
General	LEAP								
RADIUS	EAP-FAST	г		2					
Accounting	EAP-TLS								
TACACS+	PEAP								
Local Net Users	Local Cer	tificate Rec	wired	E Enabled					
Disabled Clients	Client Ce	rtificate Re	quired	E Enabled					
User Login Policies AP Policies	Certificat	e Issuer		Vendor M					
Local EAP	Charle an	ains CA es	etificates						
General	Verify Ce	utificate Ct	Manthy	Cashled					
Profiles EAP-FAST Parameters	Charle Co	and the first of t	the Market	Enabled					
Authentication Priority	Check Cr	ertinicate Dia	te validity	Enabled					
Priority Order									
Access Control Lists									
Wireless Protection Policies									
Web Auth									
Advanced									
covanceo									

7. 现在已经在 WLC 上创建了用于 EAP-FAST 身份验证的本地 EAP 配置文件。

🗿 wic2006 - Microsoft Inter	net Explorer							
File Edit View Pevorites 1	tools Help							
ahaha							infiguration Ping	Logout Refresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	S SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Local EAP Profile	0					New	Apply
- AAA	Profile Name		LEAP	EAP-PAST	EAP-TLS	PEAP		
General * RADIUS Authentication Accounting > TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies * Local EAP General Profiles EAP-FAST Parameters Authentication Priority > Priority Order > Access Control Lists > Wireless Protection Policies > Web Auth > Advanced	Idea							
10 -							0.7	
E Done							🗀 🔵 In	ternet

8. 下一步是在 WLC 上配置 EAP-FAST 的特定参数。在"WLC Security"页中,单击 Local EAP > EAP-FAST Parameters,以便转到"EAP-FAST Method Parameters"页。取消选中 Anonymous Provision 复选框,因为本示例解释的是使用证书的 EAP-FAST。使其他所有参数 保留默认值。单击 Apply。

Wic2006 - Microsoft Intern	et Explorer				لقاركا
Pile Edit View Pavorites To	xols Help				
ahaha					nfiguration   Ping   Logout Befre
CISCO	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS	HELP
Security	EAP-FAST Method P	arameters	$\bigcirc$		Apply
Constal	Server Key (in hex)		••••		
	Confirm Server Key		••••		
IF TACACS+ LDAP	Time to live for the PA	c	10 doys		
MAC Filtering Disabled Clients	Authority ID (in hex)		436973636f		
User Login Policies AP Policies	Authority ID Informati	on	Cisco A-ID		
T Local EAP Gopand Profiles EAP-FAST Parameters References	Anonymous Provision		Enabled		
E Priority Order					
► Access Control Lists					
Wireless Protection     Policies					
Web Auth					
E Advanced					
40 -					A a thread
				. I.	Unkernet

#### 用 LDAP 服务器的详细信息配置 WLC

现在已经用本地 EAP 配置文件和相关信息对 WLC 进行了配置,下一步是用 LDAP 服务器的详细信 息来配置 WLC。在 WLC 上完成以下步骤: 1. 在 WLC 的 Security 页中,从左侧的任务窗格中选择"AAA">"LDAP",以便转到"LDAP server configuration"页。要添加 LDAP 服务器,请单击 New。这会显示 LDAP Servers > New 页。

wic2006 - Microsoft Inter	net Explorer	
File Edit View Favorites T	ools Help	
սիսիս		Sage Configuration   Ping   Logout   Refresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COM	MMANDS HELP
Security	RADIUS Authentication Servers	Apply New
▼ AAA General ▼ RADIUS Authentication	Call Station ID Type IP Address	int RADIUS server)
Accounting TACACS+ LDAP Local Net Users	Network User Management Server Index Server Address Port IPSec Adm	nin Status
MAC Filtering Disabled Clients User Login Policies AP Policies		
Elocal EAP		
▶ Priority Order		
▶ Access Control Lists		
Wireless Protection     Policies		
E Web Auth		
▶ Advanced		
<u>8</u>		🚔 🔵 Internet

2. 在"LDAP Servers Edit"页中,指定 LDAP 服务器的详细信息,例如 LDAP 服务器的 IP 地址、 端口号、启用服务器状态等。从 Server Index (Priority) 下拉框中选择一个数字,以便指定此 **服务器相对于其他任何已配置的 LDAP 服务器的优先顺序。**最多可以配置 17 个服务器。如果 控制器不能到达第一个服务器,则尝试列表中的第二个服务器,依此类推。在 Server IP Address 字段中输入 LDAP 服务器的 IP 地址。在 Port Number 字段中输入 LDAP 服务器的 TCP 端口号。有效范围是 1 到 65535,默认值是 389。在"User Base DN"字段中,请输入包 含所有用户列表的 LDAP 服务器中的子树的可分辨名称 (DN)。例如,ou=组织单位,.ou=下一 个组织单位,o=corporation.com。如果包含用户的树是基准 DN,请输入 "o=corporation.com"或"dc=corporation, dc=com"。在本示例中,用户位于组织单位 (OU)Idapuser下,该用户又创建为Wireless.com域的一部分。用户基准 DN 应该指定用户信息 (对于 EAP-FAST 身份验证方法,是用户凭证)所在的完整路径。在本示例中,用户位于基 准 DN"OU=Idapuser, DC=Wireless, DC=com"下。有关 OU 以及用户配置的详细信息,请参 阅本文档的在域控制器上创建用户部分中的解释。在 User Attribute 字段中,输入包含用户名 的用户记录中的属性名称。在 User Object Type 字段中,输入将记录标识为用户的 LDAP objectType 属性的值。通常,用户记录具有多个 objectType 属性值,其中有些对用户是唯一 的,而另一些则与其他对象类型共享。注意:您可以使用LDAP浏览器实用程序(作为 Windows 2003支持工具的一部分)从目录服务器获取这两个字段的值。此 Microsoft LDAP 浏 **览器工具称为 LDP。**在此工具的帮助下,您可以了解此用户的用户基准 DN、用户属性和用户 对象类型字段。有关如何使用 LDP 来了解这些用户特定属性的详细信息,请参阅本文档的使 <u>用 LDP 来识别用户属性部分中的讨论。</u>如果您希望所有 LDAP 事务都使用安全 TLS 隧道,请 从"Server Mode"下拉框中选择 Secure。否则,请选择 None(这是默认设置)。在 Server Timeout 字段中, 输入重新传输之间相隔的秒数。 有效范围是 2 到 30 秒, 默认值是 2 秒。选 中 Enable Server Status 复选框以启用此 LDAP 服务器,或者取消选中以禁用它。默认值是禁 用。单击**适用做您的更改。**下面是已经配置了此信息的示例

Clark and the result of t	wic2006 - Microsoft Inter	rnet Explorer							
CISCO       MONITOR       VLANE       CONTROLLER       VJRELESS       SECURTY       MANAGEMENT       COMMANDE       HELP         Security       IDAP       Server Address       10.77.244.158       Formal       Address       Formal	ababa						Saye Co	nfiguration   Eing	Logout   Befresh
Security  AAA General FADIS Authentication Accounting TrACACC+ LOAP Load Hitting Dividual Clanst User Address AP Policies AP Policies Forer Timeout Ensable Server Status Ensable Server Server Server Status Ensable Server Server Status Ensable Server Server Server	CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
🖹 Done 🗎 🔮 🐲 Internet	CISCO Security CAAA General Cancel Counting TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies E Local EAP Priority Order Access Control Lists Wireless Protection Policies Web Auth Advanced	MONITOR WLANS LDAP Servers > Server Index Server Address Port Number User Base DN User Attribute User Object Type Server Mode Server Timeout Enable Server Statu	CONTROLLER Edit 10.7 389 OU- sAM Pers Non 30 ss	VUIRELESS 77.244.198 eldapuser,DC=w AccountName e seconds	SECURITY	MANAGEMENT		KELP < Back	Apply
								A	to and
	E Done					·			Nernet.

现在已经在 WLC 上配直了与 LDAP 服务器相关的详细信息,下一步是将 LDAP 配直为优先的 后端数据库,使 WLC 先从 LDAP 数据库中查找用户凭证,而不是从其他任何数据库中进行查 找。

#### 将 LDAP 配置为优先的后端数据库

要将 LDAP 配置为优先的后端数据库,请在 WLC 上完成以下步骤:

 在"Security"页中,单击 Local EAP > Authentication Priority。在"Priority Order > Local-Auth"页中,您可以找到两个能用来存储用户凭证的数据库(本地和 LDAP)。要将 LDAP 设 置为优先数据库,请从左侧的用户凭证框中选择 LDAP,然后单击">"按钮,以便将 LDAP 移 到右侧的优先顺序框中。

Security MANAGEMENT COMMANDS HELP Security Priority Order > Local-Auth Apply Ana General Professiona Accounting Control Less Contr	Wic2006 - Microsoft Intern File Edit Vew Pavortes To	et Explorer ols Help							
CISCO     MONITOR     WIANA     CONTROLLER     WIRELESS     BECURITY     MAAAddement     Control Les       Security     Priority Order > Local-Auth     Image: Control Less     Image: Control Less     Image: Control Less     Image: Control Less       Ceneral     Image: Control Less     Image: Control Less     Image: Control Less     Image: Control Less       Machine     Image: Control Less     Image: Control Less     Image: Control Less     Image: Control Less       Marcel     Image: Control Less     Image: Control Less     Image: Control Less     Image: Control Less       Marcel     Image: Control Less     Image: Control Less     Image: Control Less       Marcel     Image: Control Less     Image: Control Less     Image: Control Less	alado				~	<b>.</b>	Saye Co	nfiguration	Ping   Logout   Befresh
Security Priority Order > Local-Auth     Conset     Security	CISCO	MONITOR WU	ANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
AAA General Presentation Accounting Development Accounting Development Deve	Security	Priority Order	> Local-Auth						Apply
General Profiles Authentication Priority Profiles Control Lists. Policies Policies Policies Policies Policies	AAA     General     RADUUS     Autheotication     Accounting     XACACS+     LoAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies     PLocal EAP	LOCAL		-qL nwc					
	General Profiles Profiles Authentication Priority E Priority Order E Access Control Lists E Wireless Protection Policies E Web Auth E Advanced								

 本示例清晰地演示了在左侧框中选择 LDAP 并选择 > 按钮。结果, LDAP 被移到用来决定优先 级的右侧框中。LDAP 数据库被选为身份验证的优先数据库。单击 Apply。

wic2006 - Microsoft Inter	net Explorer								
File Edit View Favorites	Tools Help								27
ahaha								nfiguration	Ping   Logout Befresh
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Priority 0	rder > L	ocal-Auth						Apply
<ul> <li>♥ AAA</li> <li>General</li> <li>♥ RADIUS: Authentication Accounting</li> <li>№ TaCACS*</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> </ul>	LOCAL	lentials		P MD					
Teneral General Profiles EAP-FAST Parameters Authentication Priority									
E Priority Order									
E Access Control Lists									
Wireless Protection     Policies									
E Web Auth									
F Advanced									
<b>a</b>								1 1 14	🗿 🐵 Internet
		х л. <u>±</u> ∠7		64 65 L L			ㅋㅋㅋ		ь т т <del>д</del> ☆ӣ

**注意:如果**LDAP和LOCAL都显示在正确的User Credentials框中,其中LDAP位于顶部 ,LOCAL位于底部,则Local EAP尝试使用LDAP后端数据库对客户端进行身份验证,并且如 果LDAP服务器不可访问,则故障切换到本地用户数据库。如果未找到用户,则身份验证尝试 被拒绝。如果 LOCAL 显示在上,则本地 EAP 仅尝试使用本地用户数据库进行身份验证。它 不会故障转移到 LDAP 后端数据库。

在 WLC 上将 WLAN 配置为使用本地 EAP 身份验证

WLC 中的最后一步是将 WLAN 配置为使用本地 EAP 作为其身份验证方法并使用 LDAP 作为其后端数据库。请执行以下步骤:

- 从控制器的主菜单中,单击 WLANs,以便转到 WLAN 配置页。在 WLAN 页中,单击 New,以便创建新的 WLAN。本示例将创建新的 WLAN Idap。单击 Apply。下一步是在 "WLANs">"Edit"页中配置 WLAN 参数。
- 2. 在 WLAN 编辑页中,启用此 WLAN 的状态。配置其他所有必要的参数。

File Edit View Favorites. T	tools Help							
cisco			WIRELESS	SECURITY	MANAGEMENT	Saye Co COMMANDS	nfiguration   Eing HELP	Logout   <u>R</u> efresh
WLANS WLANS WLANS	WLANS > Edit General Secur Profile Name Type SSID Status Security Policies Radio Policy Interface Broadcest SSID	ity QoS Idapuser WEAN Idap V Enable (Modification All manager V Enable V Enable in a not support in a not sup	Advanced	)] r security tab	will appear after of hendication hendication	aplying the chan	< Back pes.)	Apply
61						ſ.ſ	A 🐠 1	nternet

- 3. 单击 Security,以便为此 WLAN 配置与安全性相关的参数。本示例使用带有 104 位动态 WEP 的 802.1x 作为第 2 层安全性。注意:本文档使用带有动态WEP的802.1x作为示例。建议使用 更加安全的身份验证方法,例如 WPA/WPA2。
- 4. 在"WLAN Security configuration"页中,单击 AAA servers 选项卡。在"AAA servers"页中,启 用本地 EAP 身份验证方法,并从对应于"EAP Profile Name"参数的下拉框中选择 **Idap。**这是 本示例中创建的本地 EAP 配置文件。

D wic2006 - Microsoft Internet Explorer	
Pile Edit View Pervertes Tools Help 	Sage Configuration   Pine   Logout   Befresh MANAGEMENT COMMANDS HELP
WLANS         * WLANS         * Advanced         * Advanced         Select AAA servers below to override use of default server         Radius Servers         Select AAA servers below to override use of default server         Radius Servers         Server 1         None *         Server 2         None *         <	C Back Apply

5. 从下拉框中选择 LDAP 服务器(以前在 WLC 上配置的)。确保能够从 WLC 到达此 LDAP 服务器。单击 Apply。

The bit were Poortes took Help       Sage Configuration IP poort logand. [Befrech ICLESCO         Monitore VLANS       MONITOR VLANS CONTROLLER VIPELESS SECURITY MANAGEMENT COMMANCE HELP         WLANS       WLANS > Edit       Rank       Apply         WLANS       WLANS > Edit       Rank       Apply         Select AAA servers below to override use of default servers on this WLAN       Select AAA servers below to override use of default servers on this WLAN         VILANS       WLANS Servers       Logar Servers       Logar Servers       Logar Servers         Select AAA servers below to override use of default servers on this WLAN       Server 1 None W       None W       Server 1       Server 2       Server 1       Server 1       Server 1       Server	a wic2006 - Microsoft Inte	rnet Explorer 📰 🗐 🗐
Searce Configuration       Degret       Legent       Legent <thlegent< th=""> <thlegent< th="">       Legent       <thle< th=""><th>File Edit View Favorites</th><th>Tools Help</th></thle<></thlegent<></thlegent<>	File Edit View Favorites	Tools Help
WLANS       WLANS belt       Cence       Apply         * WLANS       * Advanced </th <th>cisco</th> <th>Sage Configuration   Bing   Logout   Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP</th>	cisco	Sage Configuration   Bing   Logout   Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
	WLANS WLANS MLANS Advanced	<form>         WLNs &gt; Edit       @ Back pp y         General       Security       QS       Advanced         Layer 2       Layer 3       Advanced       Image: Control of Security       <td< th=""></td<></form>
		🛆 🧐 Internet

6. WLC 上已经配置了新的 WLAN Idap。此 WLAN 用本地 EAP 身份验证(本示例中为 EAP-FAST)对客户端进行身份验证,并查询 LDAP 后端数据库以进行客户端凭证验证。

Wic2006 - Microsoft Inter File Edit View Fevorites T	net Explorer ools Help					
alada cisco	MONITOR WLANS	CONTROLLER WI	RELESS SECURITY	MANAGEMENT COM	Sage Configuration   Eing   MANDS   HELP	Logout   <u>B</u> efresh
WLANs	WLANs					New
- WLANs WLANs	Profile Name	Туре	WLAN SSID	Admin Status	Security Policies	
► Advanced	Tawee Ideouser	WLAN	TSWED Idap	Enabled	[WFA2][Auth(002.1X)] 002.1X	
Cone					🛆 🕥 Inter	net

# 配置 LDAP 服务器

现在 WLC 上已经配置了本地 EAP,下一步是配置 LDAP 服务器,使其担当后端数据库,在证书验 证成功时对无线客户端进行身份验证。

配置 LDAP 服务器时的第一步是在 LDAP 服务器上创建用户数据库,使得 WLC 能够查询此数据库 ,对用户进行身份验证。

#### 在域控制器上创建用户

在本示例中,将创建一个新的 OU **Idapuser,并在此 OU 下创建用户 user2。**通过配置此用户进行 LDAP 访问,WLC 可以查询此 LDAP 数据库以便进行用户身份验证。

本示例中使用的域是 wireless.com。

#### 在 OU 下创建用户数据库

本部分解释如何在域中创建新的 OU 以及在此 OU 上创建新用户。

- 1. 在域控制器中,单击**开始 > 程序 > 管理工具 > Active Directory 用户和计算机,以便启动** "Active Directory 用户和计算机"管理控制台。
- 右键单击您的域名(本示例中为 wireless.com),然后从上下文菜单中选择新建 > 组织单位以 便创建新的 OU。

A File Action View Window Help	t m t m t m t
A De Dener Test Weissen Teb	- 티 즈
Active Directory Users and CompL Wireless.com 12 objects	
Saved Queres     Name     Type     Description	
Bulkin Delegate Control     DultinDomain     Container Default container for upgr	
Comput Pind     Connect to Domain     Organizational Default container for dom	
Foreign: Connect to Domain Controller     Container Default container for secu	
Comparison of the second	
Gostaiper     Default location for storag	
Computer Itin system settings	
Group Fault container for upgr	
Adn New Window from Here InetOrgPerson	
Cer MSMQ Queue Allas     MSMQ CER Refrech     Organizational Unit	
DHK Export List Printer	
OHK     User     User	
Shared Folder	
Don. Gep	
Computers     Domain Computers	
Domain Guests	
Company Users     Enterprise Admins	
3. 为此 OU 指定名称,然后单击 <b>确定</b> 。	
New Object - Organizational Unit	X
Create in: Wireless.com/	
Name:	
lidapusen	
	ncel 1

现在已经在 LDAP 服务器上创建了新的 OU **Idapuser,下一步是在此 OU 下创建用户 user2。**为此 ,请完成以下步骤: 1. 右键单击新创建的 OU。从所显示的上下文菜单中选择新建 > 用户,以便创建新用户。



在"用户设置"页中,填写必要的字段,如本示例所示。本示例使用 user2 作为用户的登录名。
 这是在 LDAP 数据库中对客户端进行身份验证时所验证的用户名。本示例使用 abcd 作为名字
 和姓氏。单击 Next。

	New Object - User	$\mathbf{x}$
	Create in: Wireless.com/Idapuser	
	Eirst name: abcd Initials:	
	Last name:	
	Full ngme: abcd	
	Eser logon name:	
	user2	
	User logon name (pre- <u>W</u> indows 2000):	
	WIRELESS\ user2	
		_
	< Back Next > Cancel	
3.	输入密码并确认此密码。选中 <b>密码永不过期选项,然后单击"下一步"。</b>	
	New Object - User	×

Password:	Wireless.com/Idapuser
Confirm password:	•••••
User <u>m</u> ust change (     User cannot change     Password never ex     Account is disabled	password at next logon ge password pires d

4. 单击 完成。OU ldapuser 下就创建了新用户 **user2。**用户凭证是:用户名**:user2**密码 :**Laptop123** 

v Object	- User				
<b>S</b>	Create in:	Wireless.co	om/Idapuser		
When yo	u click Finish,	he following	g object will b	e created:	
Full nam	e: abcd				_
User log	on name: user/	@Wireless	.com		
The pas	sword never ex	pires.			
					-
			< Back	Finish	Cancel

现在已经在 OU 下创建了用户,下一步是配置此用户进行 LDAP 访问。

## <u>为 LDAP 访问配置用户</u>

要配置用户进行 LDAP 访问,请执行本部分中的步骤:

在 Windows 2003 Server 上启用匿名绑定功能

为了使所有第三方应用程序都能够访问 LDAP 上的 Windows 2003 AD,应该在 Windows 2003 上 启用匿名绑定功能。默认情况下,Windows 2003 域控制器上不允许执行匿名 LDAP 操作。

要启用匿名绑定功能,请执行以下步骤:

- 1. 从位置**开始>运行>类型:ADSI Edit.msc**启动ADSI Edit。此工具是 Windows 2003 支持工具的 一部分。
- 在ADSI Edit窗口中,展开Root domain(Configuration [tsweb-lapt.Wireless.com])。展开 CN=服务 > CN=Windows NT > CN=目录服务。右键单击 CN=目录服务容器,然后从上下文 菜单中选择操作。

🐗 ADSI Edit				
Ile Action Yew Win	dow <u>H</u> elp			_8×
⇔ ⇒ 🖻 📧 🗙 😭	o 🗈 😰 💷			
🚳 ADSI Edt		 Name	Class	Distinguished
Domain [tsweb-lapt. Wire Configuration [tsweb-lap CN=Configuration,D CN=DisplaySpec CN=Extended-R CN=ForestUpda CN=ForestUpda CN=NTDS Quote CN=Partitions CN=Physical Loc CN=Partitions CN=Physical Loc CN=Services CN=Vervic	kess.com] k.Wireless,com] C=Wireless,DC=com fiers ights tes ndConfig is ations rvices ices ey Services s NT Move New ⊆onnection from Here New ⊆onnection from Here Qew key Move New ∭indow from Here Qelete Rename	CN=Query-Policies	container	CN=Query-P
Opens the properties dialog box	Refresh	 		
	Export List			
	Ptoperties			

3. 在 CN=目录服务属性窗口中,单击"属性"字段下的"dsHeuristics"属性,然后选择"编辑"。在此属性的字符串属性编辑器窗口中,输入值 0000002,然后单击"应用"和"确定"。Windows 2003 Server 上就启用了匿名绑定功能。注意:最后(第七)个字符是控制可绑定到LDAP服务的方式的字符。"0"或无第七个字符表示禁用匿名 LDAP 操作。将第七个字符设置为"2",即可启用 医名绑定功能

ᆸᆸᇭᇨᇧᇏ					
N=Directory Service Pr	operties		? X		
Attribute Editor Security			. E	Class	Disting
Show mandatory attri	butes			container	CN=Q4
Show optional attribut	tes				
Show only attributes	that have values				
Attributes:	_				
Attribute	Suntax	Value	<u> </u>		
directReports	String Attribut	e Editor			×
displayName displayNamePrintable	Attribute: dSHe	euristics			
distinguishedName	Value				
dSCorePropagationD					_
dSHeuristics					
extensionName flags	<u>C</u> lear		(	ок 丿 с	ancel
fromEntry					
frsComputerReferenc	Distinguished	<not set=""></not>			
fSM0RoleOwner	Distinguished	(Not Set)	-		
•					
5.0					
	OK	[ Cancel ]	Applu		
		Cancer	2000		

**注意:**如果此属性已经包含值,请确保仅更改左侧的第七个字符。这是在启用匿名捆绑时唯一 需要更改的字符。例如,如果当前值是"0010000",则您需要将其改为"0010002"。如果当前值

少于7个字符,则需要在未使用的位置置零:"001"将变为"0010002"。

#### 向用户"user2"授予"匿名登录"访问权限

下一步是向用户 user2 授予**匿名登录访问权限。**为此,请完成以下步骤:

- 1. 打开 Active Directory 用户和计算机。
- 2. 确保选中查看高级功能。
- 3. 导航到用户 user2, 然后右键单击。从上下文菜单中选择属性。此用户的名字为"abcd"。



4. 在"abcd 属性"窗口中转到**安全性。** 

Published Certificate:	s Member Of Dial	in   Object   Sec	urite
nvironment Session	ns   Remote control   Terr	ninal Services Profile	ON.
General   Address	Account   Profile	Telephones   Urganiza	atio
🕵 abod			
Eirst name:	abcd	Initials:	_
Last name:	[		
Display name:	abcd		
Description:			
Office:			
<u>T</u> elephone number:		Other	
E-mail:			
Web page:		Other	
	OK	Cancel 1 Apr	1.

5. 在所显示的窗口中单击**添加。** 

E"输入要选择的对象名称"框下输入 <b>匿名登录,然后确认此对话</b> #	王。
Select Users, Computers, or Groups	<u>? ×</u>
Colort this object type:	
Select this object type.	
Users, Groups, or Built-in security principals	Object Types
From this location:	
Wireless.com	Locations

Enter the object names to select (examples):	
ANONYMOUS LOGON	Check Names
Advanced	OK Cancel

7. 在 ACL 中,您将看到**匿名登录可以访问用户的一些属性集。**Click **OK**.已经向此用户授予"匿名 登录"访问权限。

ocd Properties		2 2
Environment   Sessions   Remote control   Te General   Address   Account   Profile   Published Certificates   Member Of   Di	erminal Service Telephones ial-in 0bje	es Profile   COM+   Organization ect Security
<u>G</u> roup or user names:		
Account Operators (WIRELESS Account Administrators (WIRELESS Administrators (WIRELESS Administrators)	nt Operators) ors)	-
ANONYMOUS LOGON		
Authenticated Users		
Cert Publishers (WIRELESS\Cert Publishers (WIRELESS\Cert Publishers )	hers)	-
	Add	<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.	gs, _	Advanced
ок	Cancel	Apply

## 在 OU 上授予"列出内容"权限

下一步是向用户所在的 OU 上的"匿名登录"至少授予**列出内容权限。**在本示例中,"user2"位于 OU"Idapuser"上。为此,请完成以下步骤:

1. 在 Active Directory 用户和计算机中,右键单击 OU Idapuser 并选择"属性"。



2. 单击安全性,然后单击"高级"。

puser Properties			? 🗡
General   Managed By   Object   Security	COM+ Group	Policy	
Group or user pames:			
Account Operators (W/IBELESS)Acco	unt Operators)	-	аΙ
Administrators [WIBELESS \Administra	tors)		1
Authenticated Users			
Domain Admins (WIRELESS\Domain	Admins)		
Enterprise Admins (WIRELESS\Enterp	orise Admins)		
	-DC		-
	A <u>d</u> d	<u>R</u> emove	
Permissions for Account Operators	Allow	Depu	
	~1077	00.0	
Full Control			- I
Full Control Read			1
Full Control Read Write			
Full Control Read Write Create All Child Objects			
Full Control Read Write Create All Child Objects Delete All Child Objects			
Full Control Read Write Create All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging			
Full Control Read Write Create All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging For special permissions or for advanced sett click Advanced.	a)	Advanced	
Full Control Read Write Create All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging For special permissions or for advanced sett click Advanced.	a)	Advanced	

3. 单击 Add。在打开的对话框中,输入**匿名登录**。

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. 确认对话框。这会打开一个新的对话框窗口。

5. 在应用到下拉框中选择"仅此对象",然后启用"允许列出内容"复选框。

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 Bead All Properties Write All Properties Delete Delete Subtree Read Permissions Modify Permissions Modify Owner All Validated Writes All Extended Rights Create All Child Objects Delete All Child Objects Delete All Child Objects	and/or		
	ок	Cancel	

# 使用 LDP 来标识用户属性

此 GUI 工具是一个 LDAP 客户端,它允许用户对任何 LDAP 兼容目录(例如 Active Directory)执 行操作(例如连接、绑定、搜索、修改、添加、删除)。LDP 用于查看 Active Directory 中存储的 对象及其元数据,例如安全描述符和复制元数据。

当您从产品 CD 安装 Windows Server 2003 支持工具时,即已包含 LDP GUI 工具。本部分解释如 何使用 LDP 实用程序来标识与用户 **user2** 相关联的特定属性。其中有些属性用于填充 WLC 上的 LDAP 服务器配置参数,例如"用户属性"类型和"用户对象"类型。

- 1. 在 Windows 2003 Server 上(即使在相同的 LDAP 服务器上),单击**开始 > 运行,然后输入** LDP 以便访问 LDP 浏览器。
- 2. 在 LDP 主窗口中,单击 Connection > Connect,然后通过输入 LDAP 服务器的 IP 地址连接 到该 LDAP 服务器。

je Ldp	
Connection Browse View Options Utilities	Pitter State
Connect         Operation           Bind         Cbrl+B           Disconnect         Operation           New         Cbrl+N           Save         Operation	
Save &s	
Print Print Preyjew Print Setup Egit	
Connect to specified server	

## 3. 连接到 LDAP 服务器之后,从主菜单中选择 View,然后单击"Tree"。

anapa/ csweb rapid wireless control = wireless, oc = com	
Connection Browse View Options Utilities	Be
Iree     Ctrl+T       Enterprise 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; 1.2.840.113556.1.4.618; 1.2.840.113556.1.4.528; 1.2.840.113556.1.4.529; 1.2.840.113556.1.4.805; 1.2.840.113556.1.4.521; 1.2.840.113556.1.4.970; 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; 1.2.840.113556.1.4.1907; 1.2.840.113556.1.4.1948; 2.&gt; supportedLDAPVersion: 3; 2; 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; 1.2.&gt; supportedLDAPVersion: 3; 2; 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; supportedCapabilities: 1.2.840.113556.1.4.800; 1.2.840.113556.1.4.1670; 1.2.840.113556.1.4.1791; 1.&gt; isGlobalCatalogReady: TRUE; 1.&gt; isGlobalCatalogReady: TRUE; 1.&gt; isGlobalCatalogReady: TRUE; 1.&gt; domainFunctionality: 0 = [DS_BEHAVIOR_WIN2000]; 1.&gt; domainControllerFunctionality: 2 = [DS_BEHAVIOR_WIN2003];</pre>

4. 在所显示的树视图窗口中,输入用户的 BaseDN。在本示例中,user2 位于 OU "Idapuser" 下 ,而后者又位于域 Wireless.com 下。因此,用户 user2 的 BaseDN 是"OU=Idapuser, dc=wireless, dc=com"。Click OK.

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 浏览器的左侧显示指定 BaseDN (**OU=Idapuser, dc=wireless, dc=com**) 下的完整的树。 展开此树以查找用户 **user2**。此用户可以用代表用户名字的 CN 值表示。在本示例中,它是 **CN=abcd**。双击 **CN=abcd**。在 LDP 浏览器的右侧面板中,**LDP 将显示与 user2 相关联的所 有属性**。本示例解释了此步骤

Idap://tsweb-lapt.Wireless.com/DC=Wireless,DC=com	
Connection Browse View Options Utilities	Reb
OU=Idapuser, dc=wireless, dc=com OU=Idapuser, dc=wireless, dc=com No children	<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; codePage: 0; 1&gt; badPasswordTime: 0; 1&gt; lastLogori 0; 1&gt; badPasswordTime: 0; 1&gt; lastLogori 0; 1&gt; pwdLastSet </pre>
Ready	

在本示例中,请观察右侧被圈出的字段。

- 6. 按照本文档的<u>用 LDAP 服务器的详细信息来配置 WLC 部分中所述,在</u> User Attribute 字段中,输入用户记录中包含用户名的属性的名称。从此 LDP 输出中,您可以看到 sAMAccountName 是包含用户名"user2"的一个属性。因此,请输入与 WLC 上的"用户属性"字 段相对应的 sAMAccountName 属性。
- 7. 在 User Object Type 字段中,输入将记录标识为用户的 LDAP objectType 属性的值。通常 ,用户记录具有多个 objectType 属性值,其中有些对用户是唯一的,而另一些则与其他对象 类型共享。在 LDP 输出中, CN=Person 是将记录识别为用户的一个值。所以,请指定 Person 作为 WLC 上的"用户对象类型"属性。

# <u>配置无线客户端</u>

最后一步是配置无线客户端,使其使用客户端和服务器证书进行 EAP-FAST 身份验证。为此,请完成以下步骤:

 1. 启动Cisco Aironet Desktop Utility(ADU)。在 ADU 主窗口中,单击 Profile Management > New,以便创建新的无线客户端配置文件。

🛜 Cisco Aironet Desktop Ul	ility - Current Profile: sdreteretet	? 🔀
Action Options Help		
Current Status Profile Manager	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

 指定配置文件名称,并向此配置文件分配一个 SSID 名称。此 SSID 名称应该与 WLC 上配置 的相同。在本示例中,SSID 名称是 Idap。

General Security Advanced  Profile Settings Profile Name: Idapuser Client Name: CLIENT1  Network Names SSIDT Idap SSID2: SSID3:	Security Advanced Settings Profile Name: Idapuser Client Name: CLIENT1 CNames SSIDT: Idap SSID2: SSID3:	ofile Management		2
Profile Settings         Profile Name:       Idapuser         Client Name:       CLIENT1         Network:       Names         SSID1:       Idap         SSID2:       SSID3:	Profile Name: Idapuser   Client Name: CLIENT1     c Names SSID1   SSID2: SSID3:	General Security Advance	d	
Network Names SSID1 Idap SSID2 SSID3:	SSID1: Idap SSID2: SSID3:	Profile Settings Profile Name: Client Name;	Idapuser CLIENT1	
SSID3:	SSID3:	Network Names SSID SSID2:	kdap	
		SSID3:		

- 3. 单击 Security 选项卡,然后选择 802.1x/EAP 作为第 2 层安全性。选择 EAP-FAST 作为 EAP 方法,然后单击"Configure"。
- 4. 在 EAP-FAST 配置页中,从"EAP-FAST Authentication Method"下拉框中选择 **TLS Client Certificate,然后单击"Configure"。**

EAP-FAST Authentication Method MSCHAPv2 User Name and Password GTC Token/Password MSCHAPv2 User Name and Password TLS Client Certificate Select One or More PAC Authorities	
MSCHAPv2 User Name and Password GTC Token/Password MSCHAPv2 User Name and Password TLS Client Certificate Select One or More PAC Authorities	
GTC Token/Password MSCHAPv2 User Name and Password TLS Client Certificate Select One or More PAC Authorities	2
Select One-or-More PAC Authorities	
Manage	
Use Any PAC Belonging to the Same Group	
Allow Automatic PAC Provisioning	
Use Machine Information for Domain Logon	
✓ No Network Connection Unless User Is Logged In	
OK Cancel	

5. 在"TLS Client Certificate Configuration"窗口中: 启用 Validate Server Identity 复选框,并选择 客户端上安装的 CA 证书(如本文档的为客户端生成根 CA 证书部分中所述)作为受信任的根 证书颁发机构。选择客户端上安装的设备证书(如本文档的<u>为客户端生成设备证书部分所述</u>)作为客户端证书。Click OK.本示例解释了此步骤

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

这就创建了无线客户端配置文件。

# <u>验证</u>

要验证您的配置是否能正确使用,请执行以下步骤。

- 1. 在 ADU 上激活 Idap SSID。
- 根据需要,在接下来的窗口中单击 Yes 或"OK"。您应该能够在 ADU 上看到所有客户端身份验 证和关联步骤都成功完成。

使用本部分可确认配置能否正常运行。使用 WLC CLI 模式。

• 要验证 WLC 是否能与 LDAP 服务器通信并找到用户,请从 WLC CLI 指定 debug aaa Idap enable 命令。本示例解释了一个成功的通信 LDAP 进程:注意:出于空间考虑,本节中的某些 输出已移至第二行。(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

从此调试输出中突出显示的信息来看,很明显 WLC 通过其上指定的用户属性来查询 LDAP 服

务器,并且 LDAP 进程成功完成。

• 要验证本地 EAP 身份验证是否成功,请从 WLC CLI 指定 debug aaa local-auth eap method events enable 命令。示例如下: (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。示例如下:(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 • 要查看 WLC 中安装的用于本地身份验证的证书,请从 WLC CLI 发出 show local-auth certificates 命令。示例如下: (Cisco Controller) > 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.

## • 要从 CLI 模式查看 WLC 上的本地身份验证配置,请发出 **show local-auth config 命令。**示例如 下:(Cisco Controller) >show local-auth config

User credentials database search order:

Primary ..... LDAP

Timer:

Active timeout	•••		• •		•••	•••	••	• •	• •				•		•		• •	300
----------------	-----	--	-----	--	-----	-----	----	-----	-----	--	--	--	---	--	---	--	-----	-----

Configured EAP profiles:

N	Jame	ldapuser
	Certificate issuer	vendor
	Peer verification options:	
	Check against CA certificates	Enabled
	Verify certificate CN identity	Disabled
	Check certificate date validity	Disabled
	EAP-FAST configuration:	
	Local certificate required	Yes
	Client certificate required	Yes
	Enabled methods	fast
	Configured 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>故障排除</u>

您可以使用以下命令来排除配置问题:

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

# 相关信息

- 包含无线局域网控制器和外部 RADIUS 服务器的 EAP-FAST 身份验证配置示例
- 统一无线网络先的PEAP与Microsoft互联网认证服务(IAS)
- 使用 WLC 基于 ACS 对 Active Directory 组映射执行动态 VLAN 分配配置示例
- Cisco 无线局域网控制器配置指南 配置安全解决方案
- Cisco 无线局域网控制器配置指南 管理控制器软件和配置
- WLAN 控制器 (WLC) 中 EAP 身份验证的配置示例
- •无线局域网控制器(WLC)设计和功能常见问题
- 使用 EAP-FAST 身份验证的 Cisco 安全服务客户端
- 无线局域网控制器(WLC)常见问题
- 控制器无线局域网控制器(WLC)错误和系统消息常见问题
- <u>技术支持和文档 Cisco Systems</u>

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。