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

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。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

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。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

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。

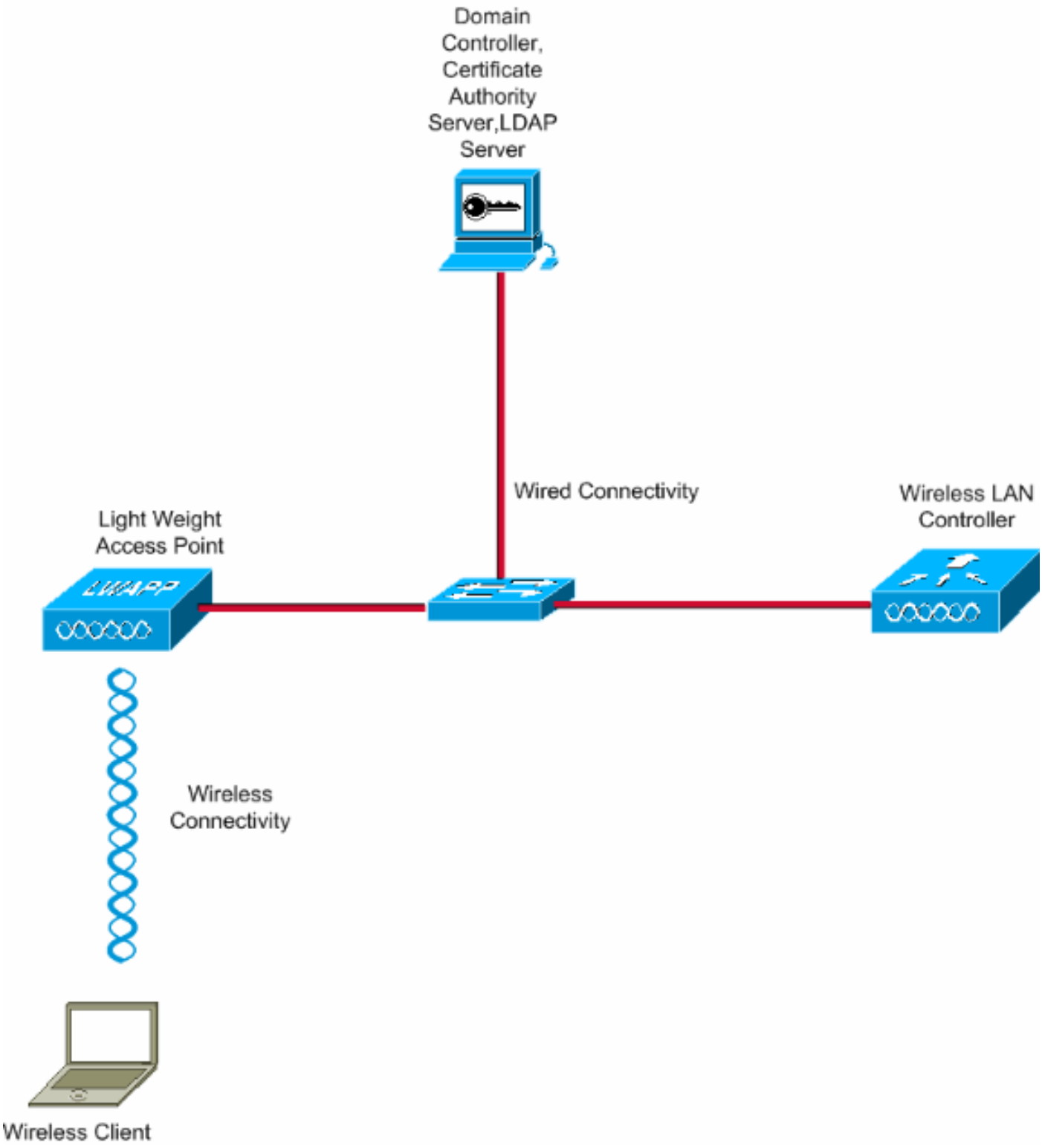
用户凭证存储在 LDAP 服务器中，因此在成功验证证书后，控制器能够查询 LDAP 服务器，检索用户凭证并对无线客户端进行身份验证。

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，请参阅向无线局域网控制器(WLC)注册轻量 AP(LAP)。
- 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，请参阅将 Windows 2003 配置为域控制器。要将Windows 2003 Server配置为企业CA服务器，请参阅安装和配置Microsoft Windows 2003 Server作为证书颁发机构(CA)服务器。

网络图

本文档使用以下网络设置：



配置

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
- 配置 LDAP 服务器
- 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。

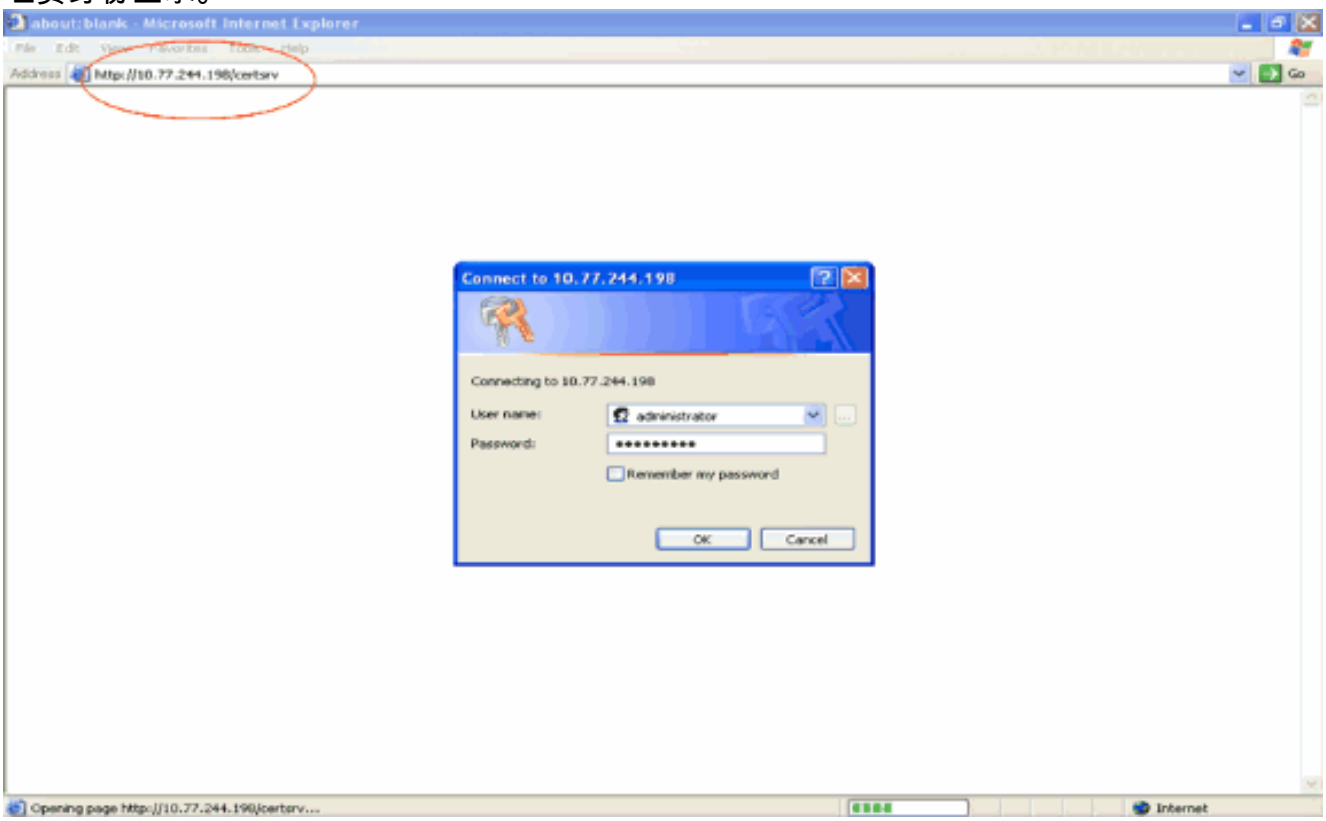
WLC 和客户端均需要从 CA 服务器下载以下证书：

- 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

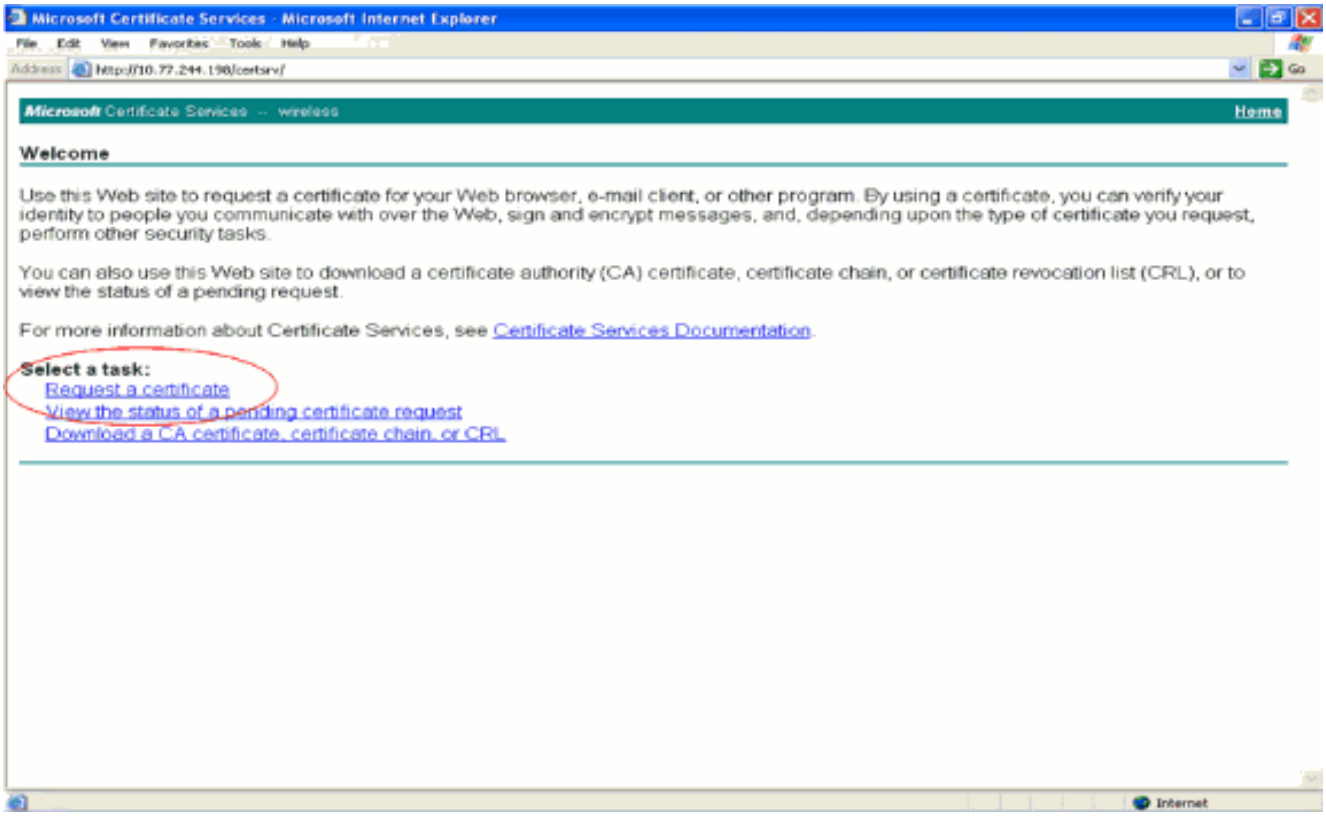
为 WLC 生成设备证书

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。

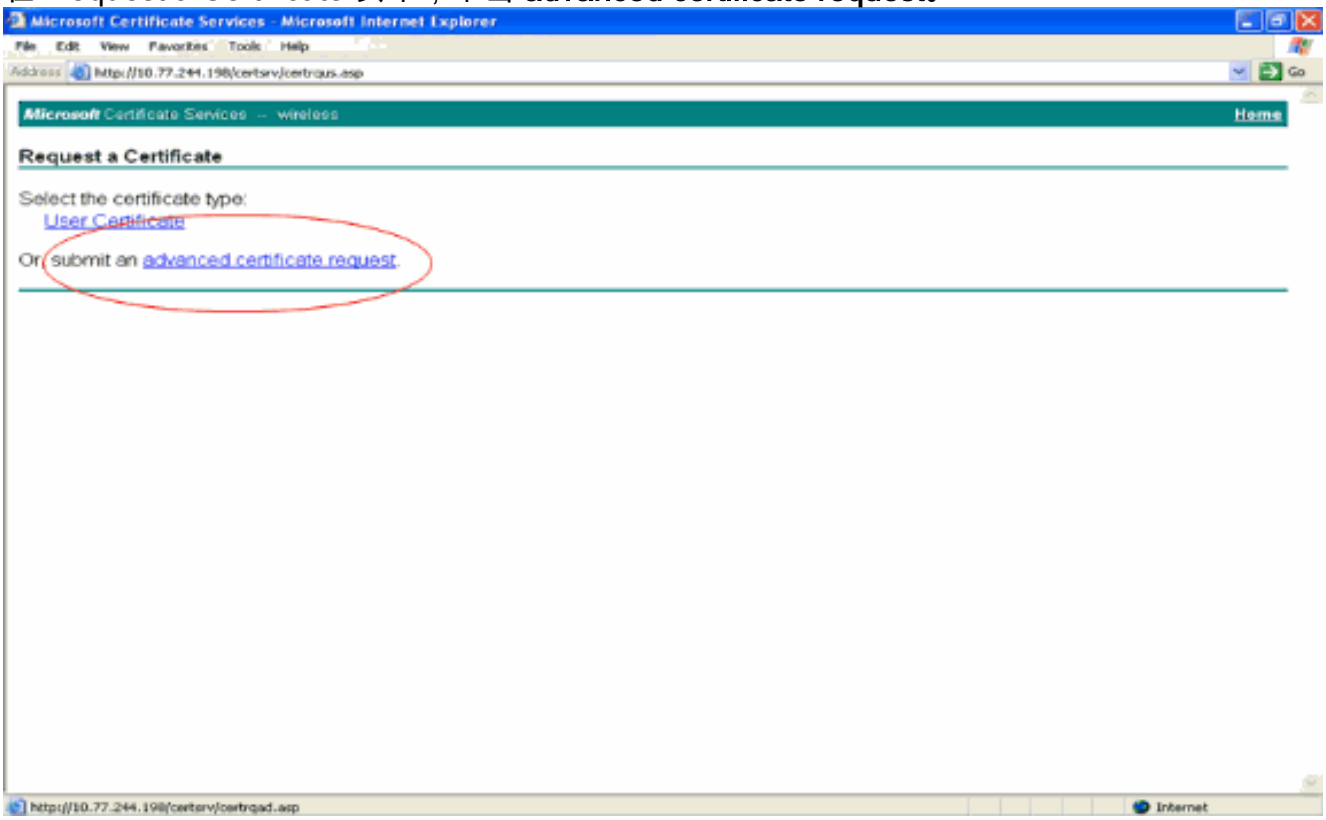
1. **在与 CA 服务器相连的 PC 上，访问 http://<CA 服务器的 IP 地址>/certsrv。**以CA服务器的管理员身份登录。



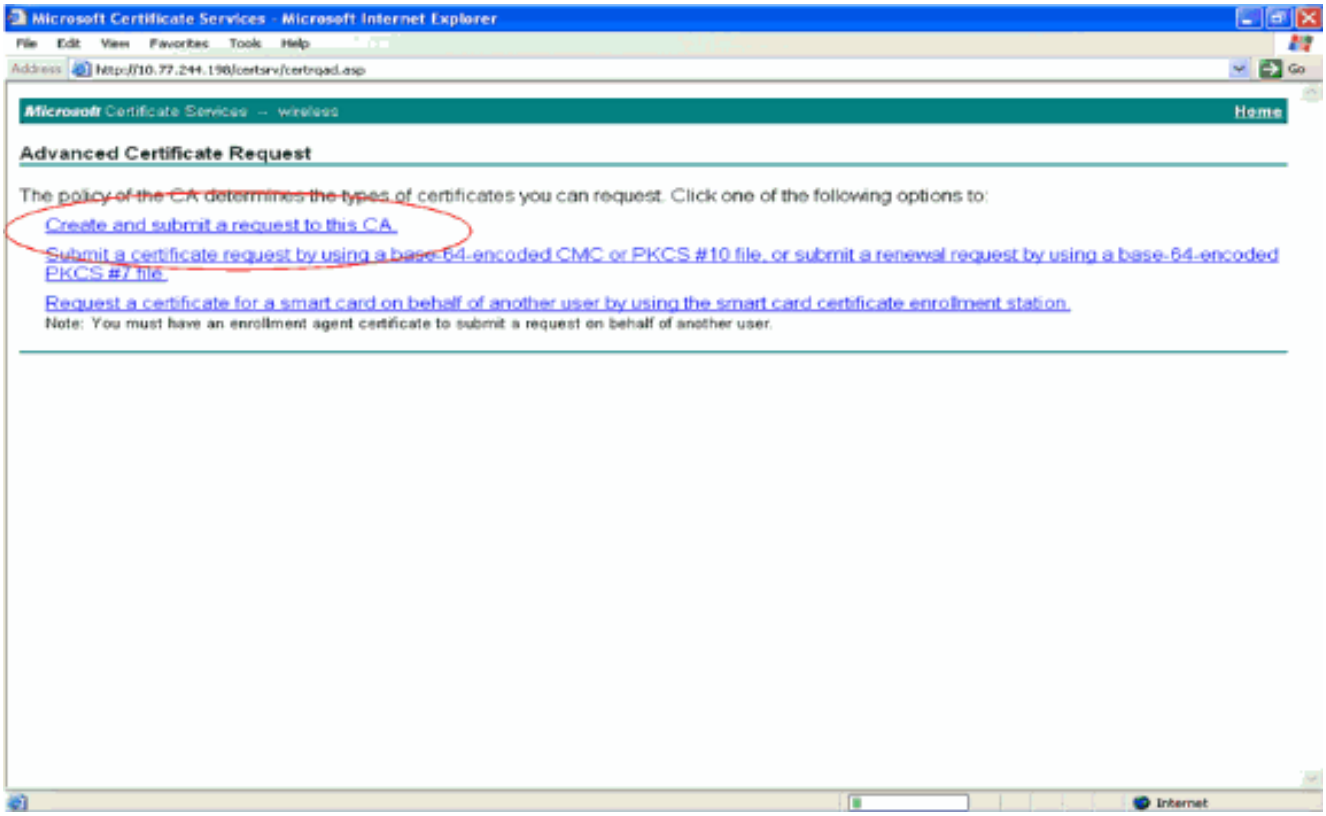
2. 选择 **Request a certificate。**



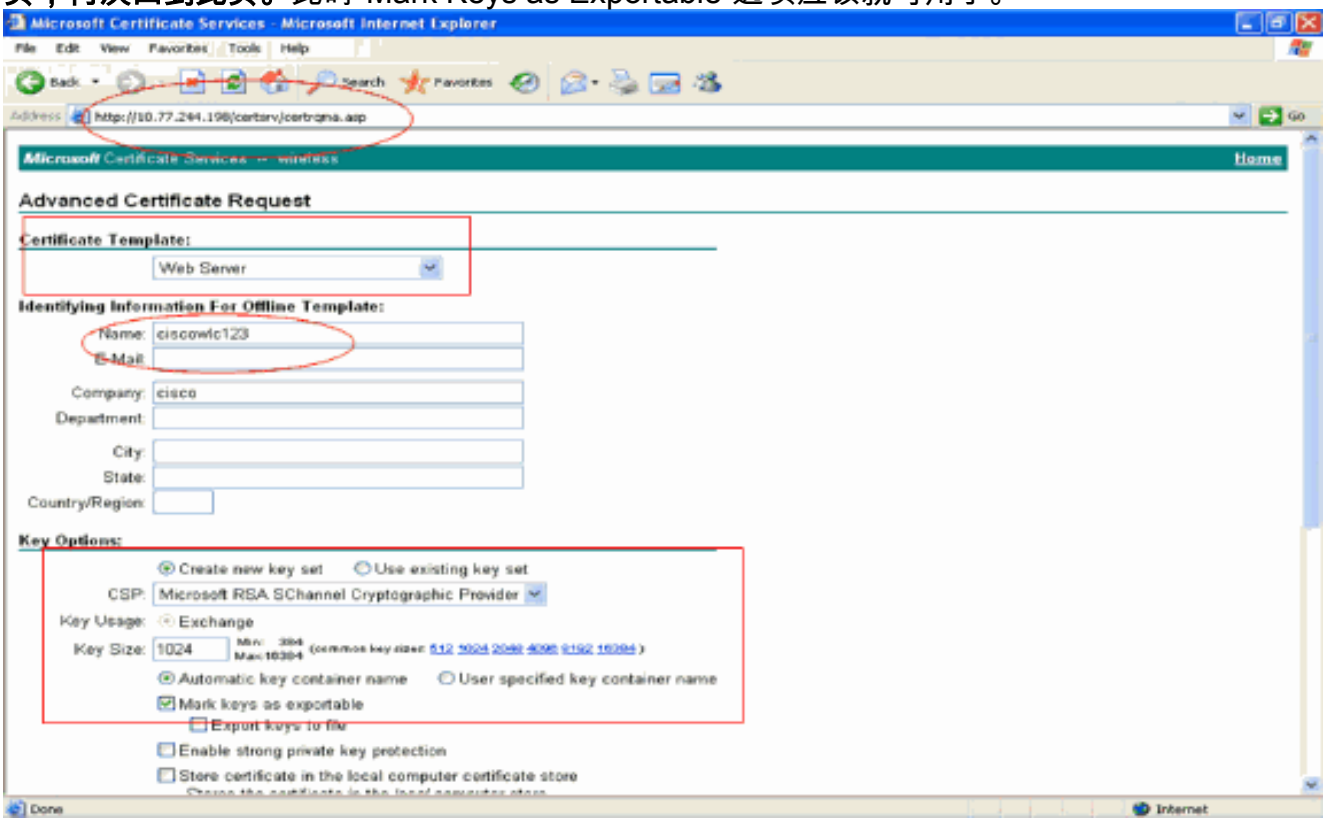
3. 在“Request a Certificate”页中，单击 **advanced certificate request**。



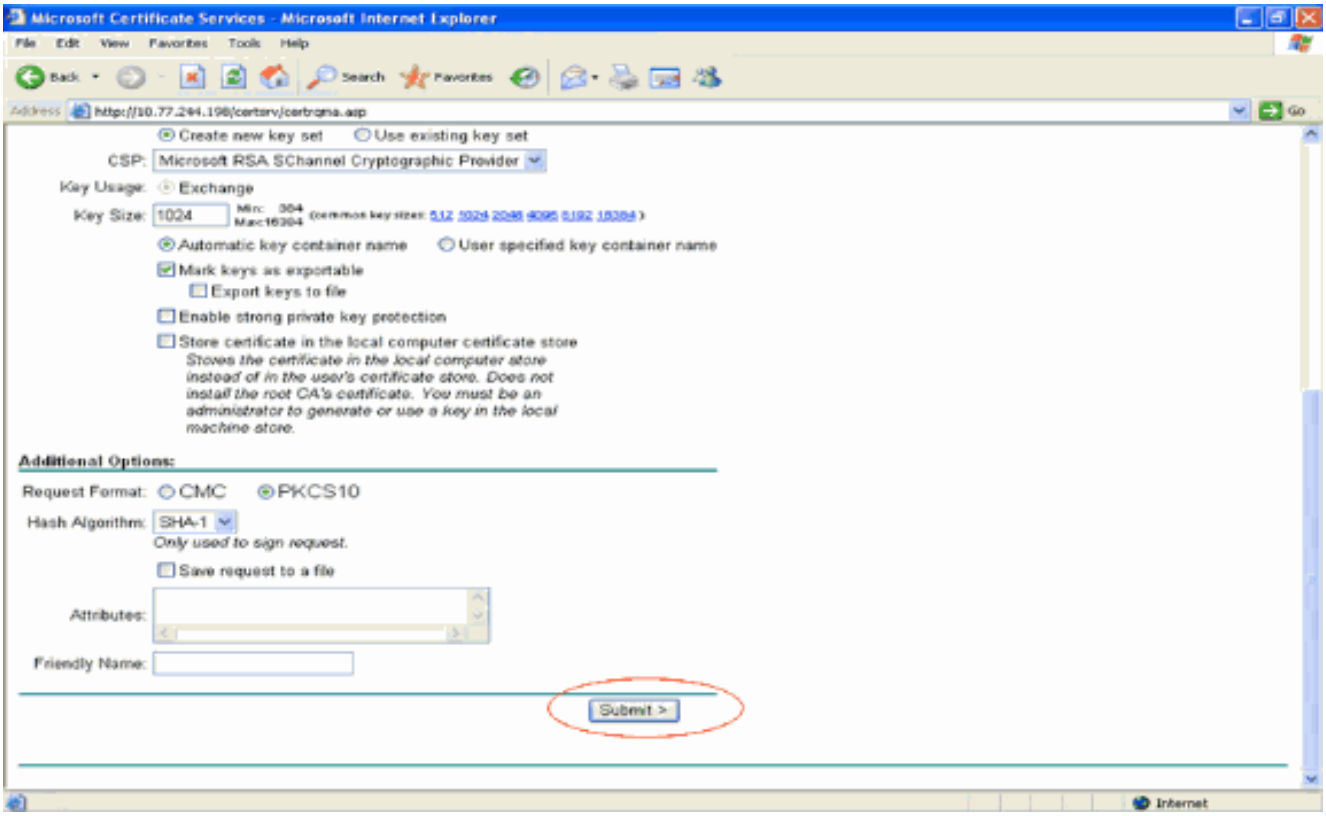
4. 在“Advanced Certificate Request”页中，单击 **Create and submit a request to this CA。**这将显示高级证书请求表。



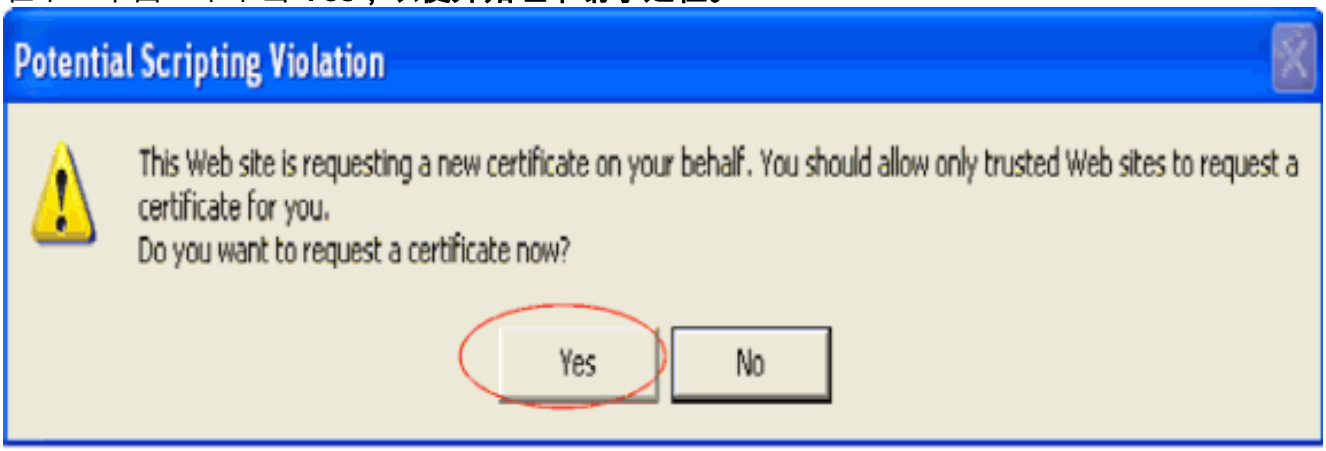
5. 在高级证书请求表中，选择 **Web Server 作为证书模板。**然后，指定此设备证书的名称。本示例使用 ciscowlc123 作为证书名称。根据需要填写其他识别信息。
6. 在 **Web Server 部分下，选择"Mark Keys as Exportable"选项。**有时，如果您选择 Web 服务器模板，此选项将变灰，并且不能启用或禁用。在这种情况下，从浏览器菜单中单击**返回返回一页，再次回到此页。**此时"Mark Keys as Exportable"选项应该就可用了。



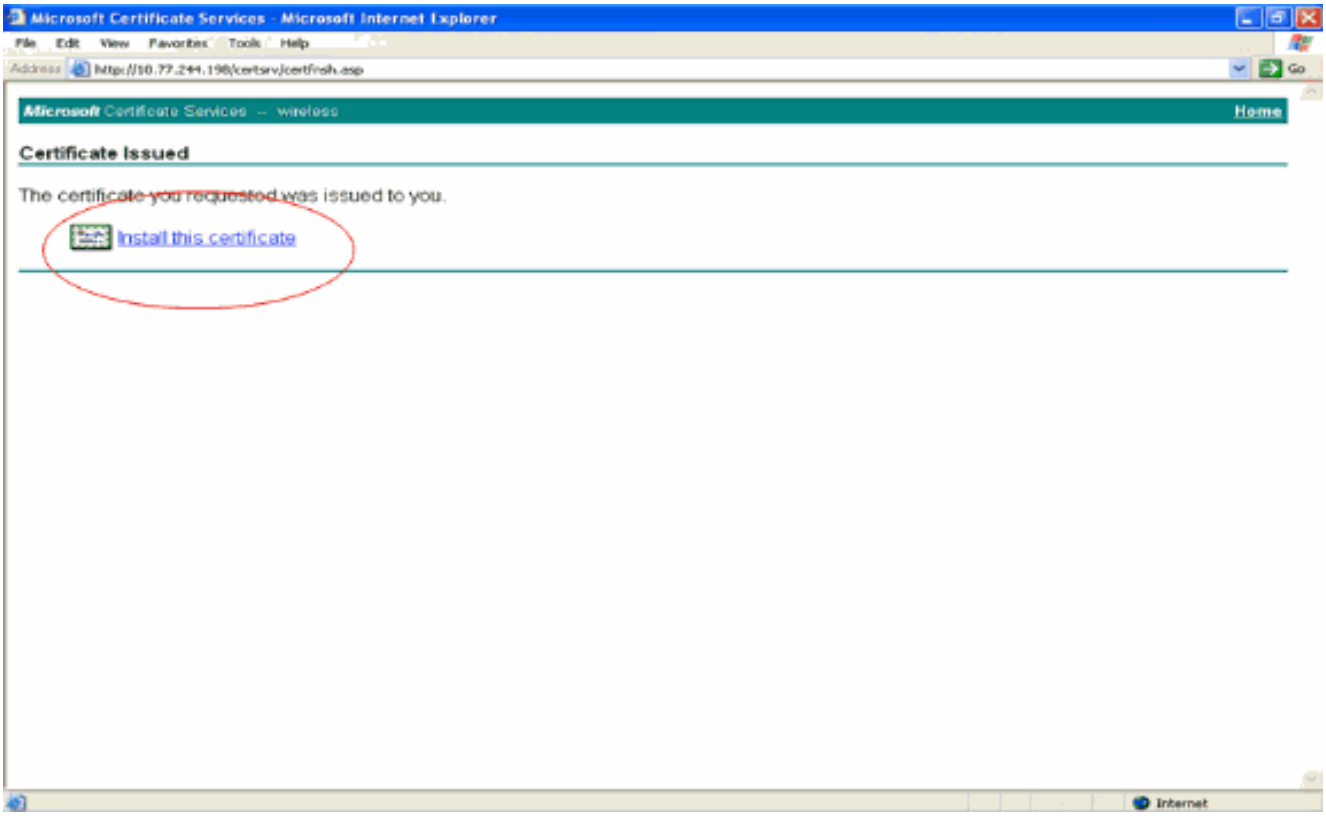
7. 配置其他所有必要字段，然后单击 **Submit。**



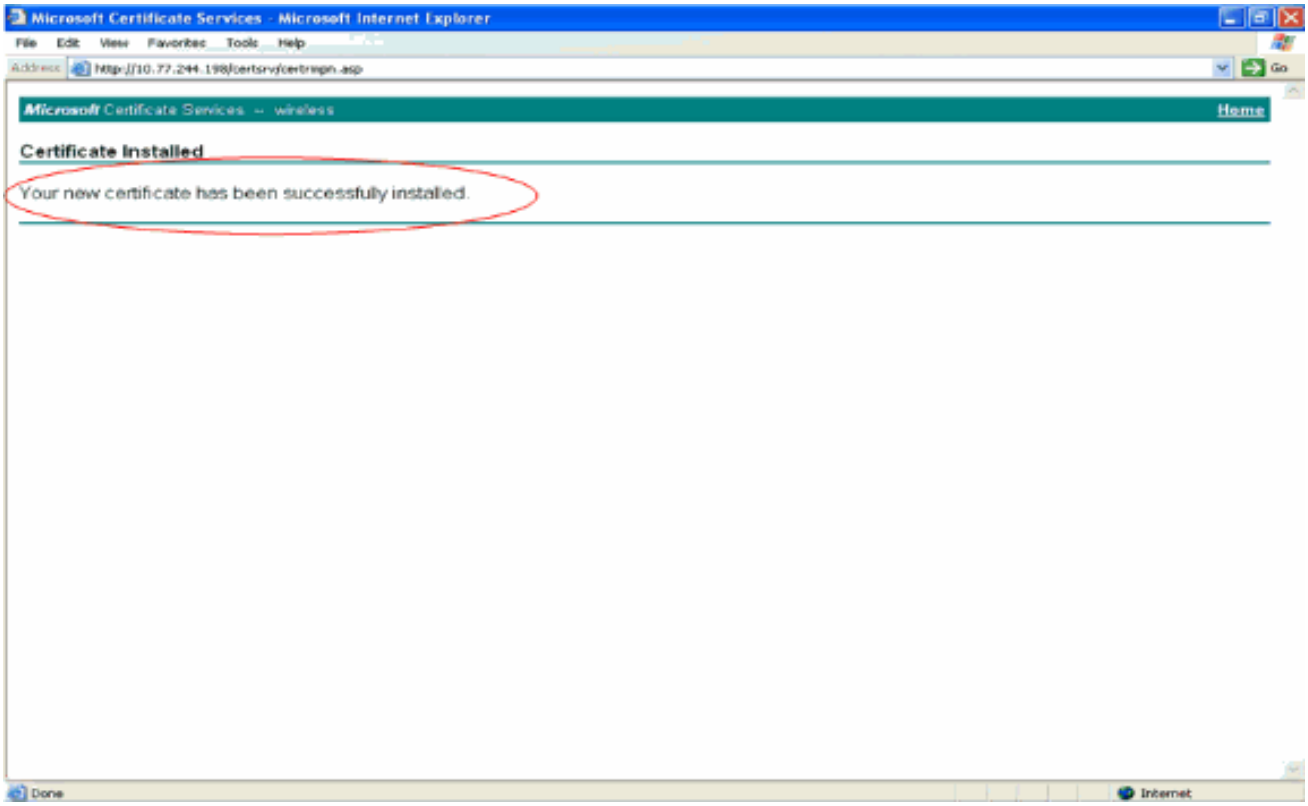
8. 在下一个窗口中单击 **Yes，以便开始证书请求过程。**



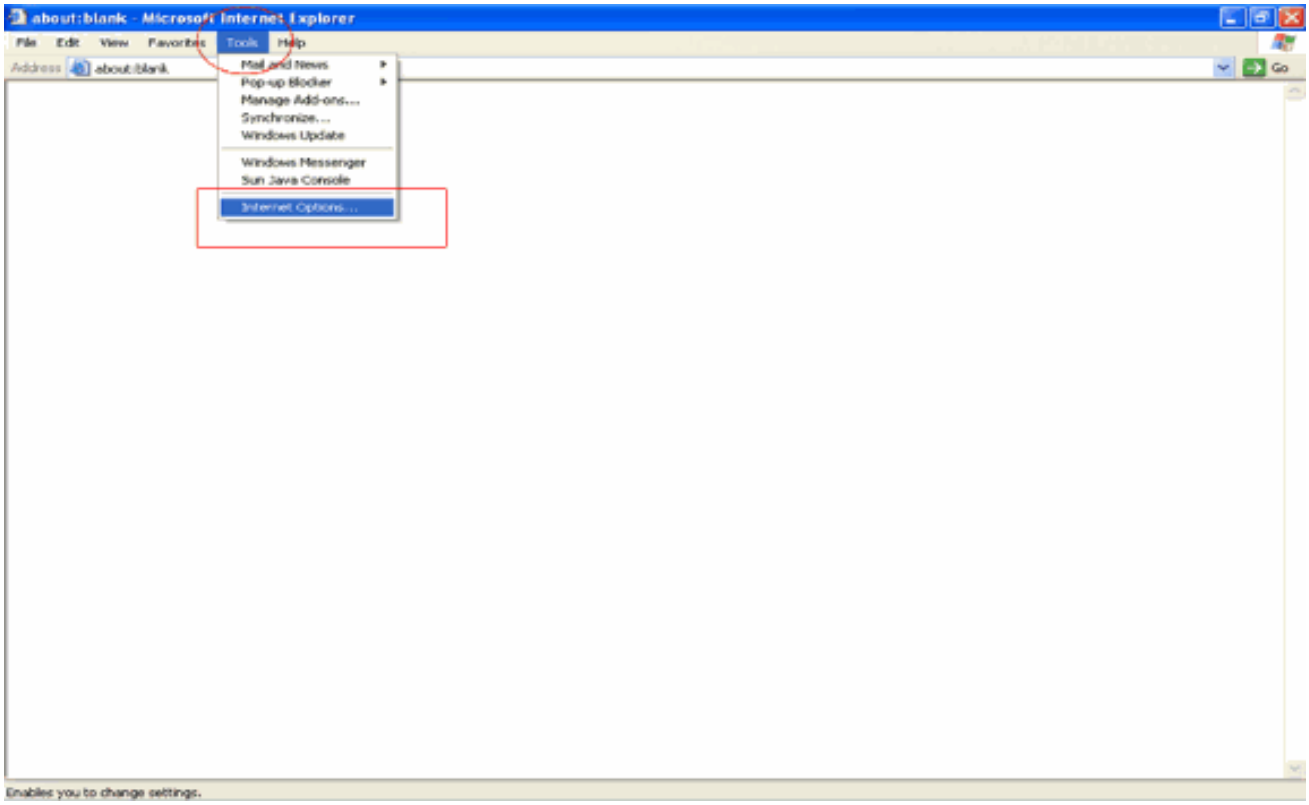
9. 这将显示“Certificate Issued”窗口，表明证书请求过程已成功。下一步是将颁发的证书安装到此 PC 的证书存储中。单击 **Install this certificate**。



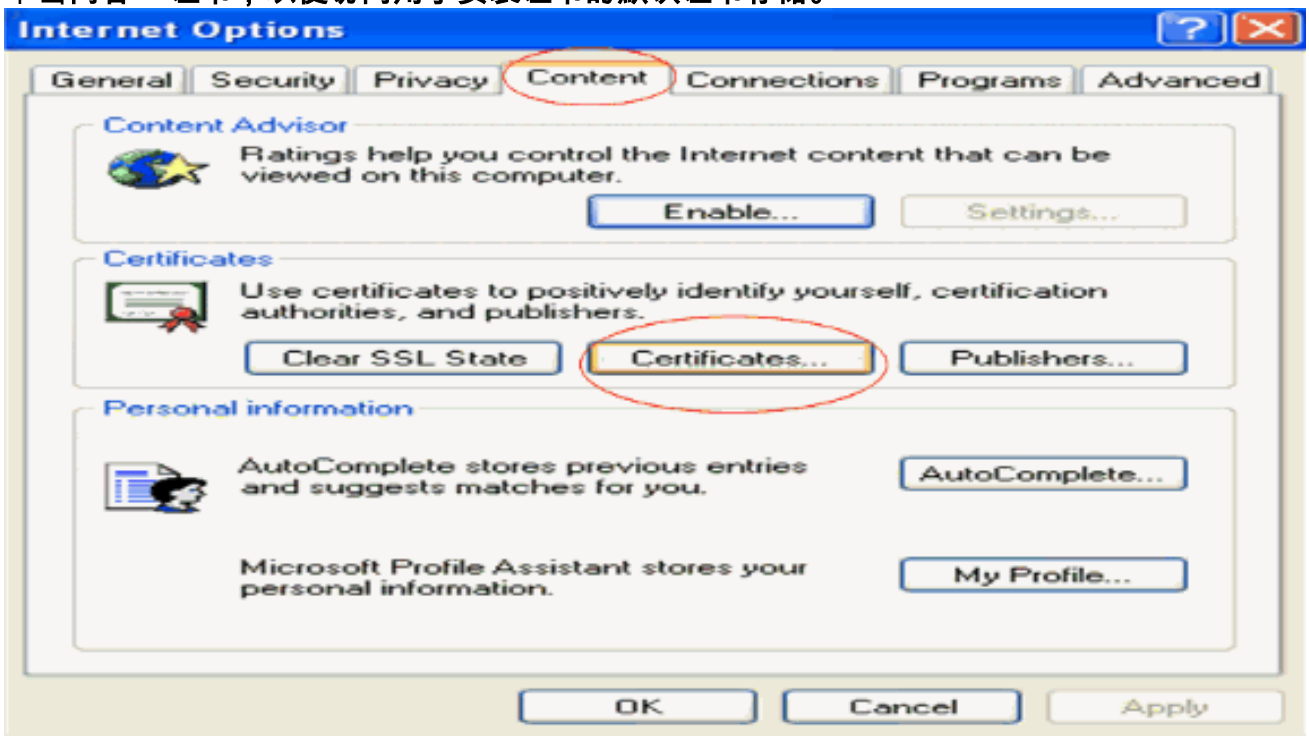
10. 新证书已经成功从向 CA 服务器生成请求的位置安装到 PC 上。



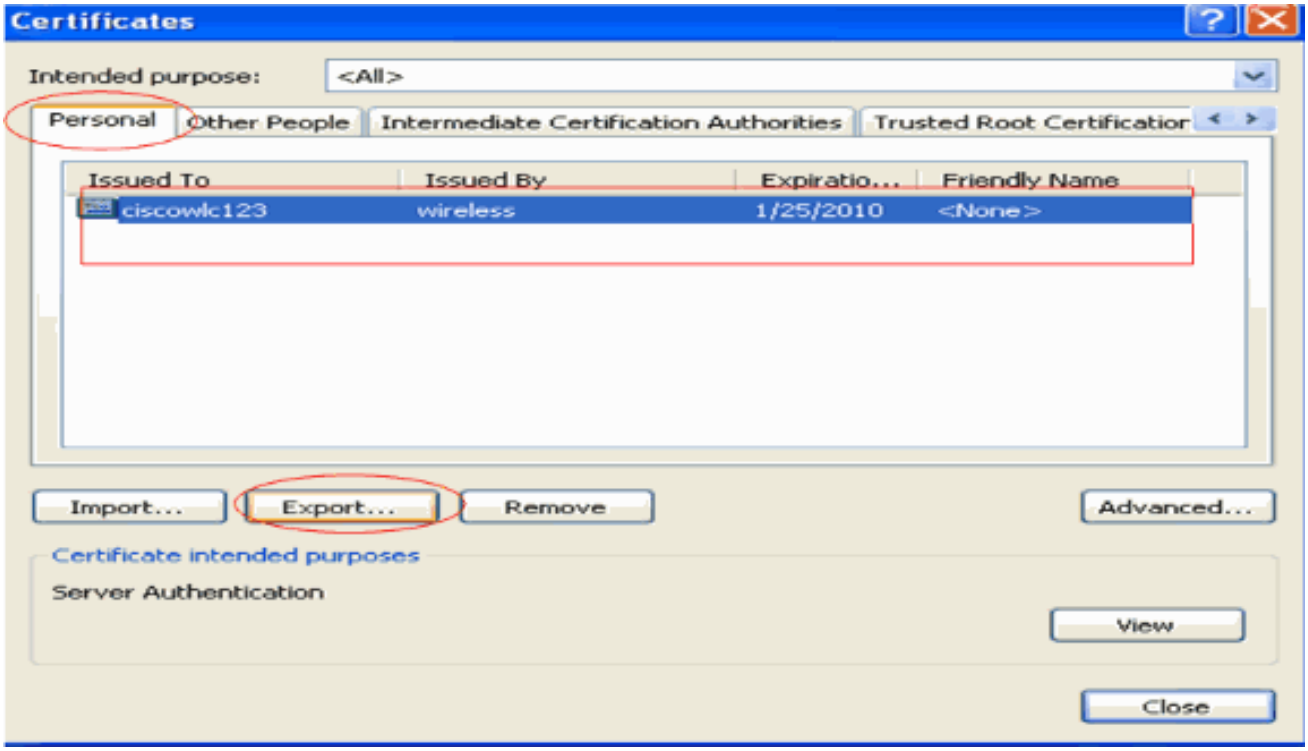
11. 下一步是从证书存储中将此证书作为文件导出到硬盘上。此证书文件以后将用于将证书下载到 WLC 上。为了从证书存储中导出证书，请打开 Internet Explorer 浏览器，然后单击**工具 > Internet 选项**。



12. 单击**内容 > 证书，以便访问用于安装证书的默认证书存储。**

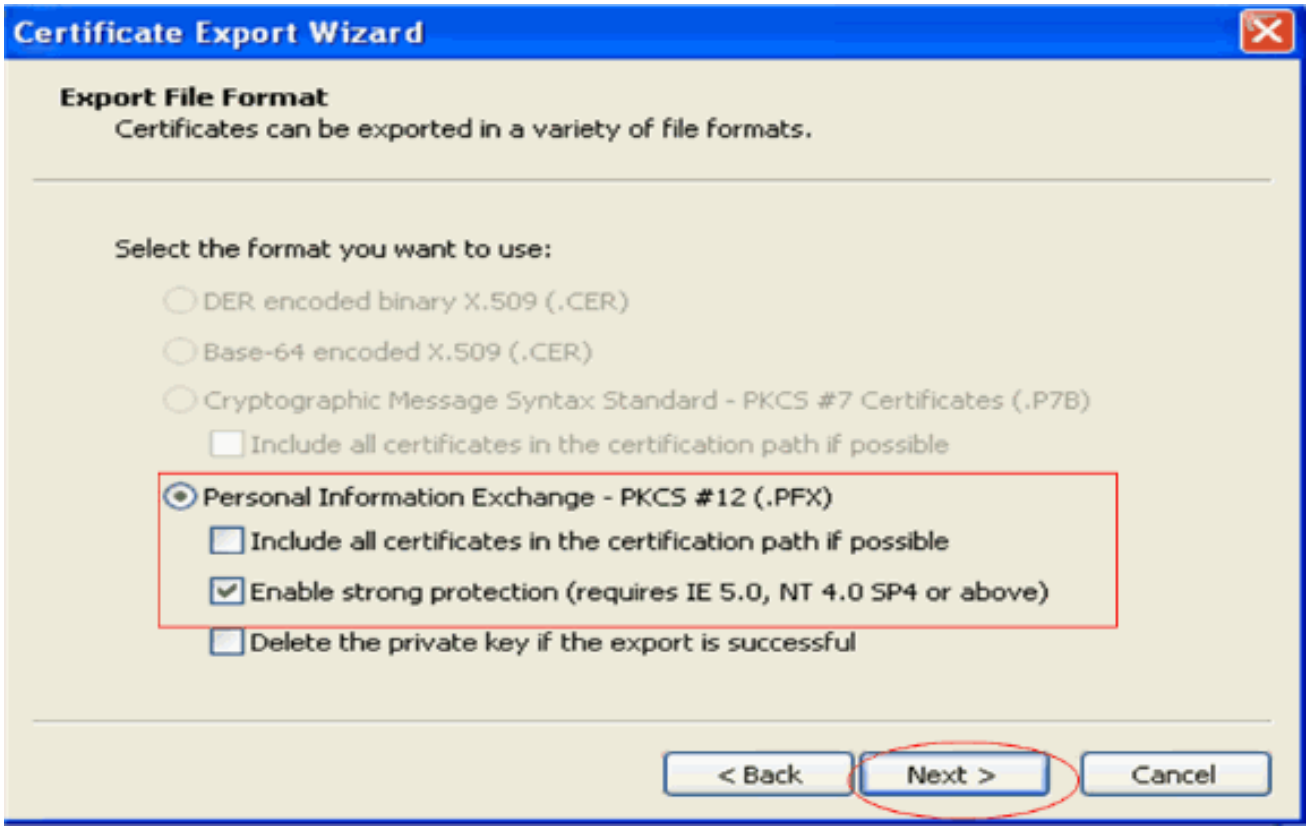


13. 设备证书通常安装在**个人证书列表下。**在此，您应该看到新安装的证书。选择该证书，然后单击**导出。**

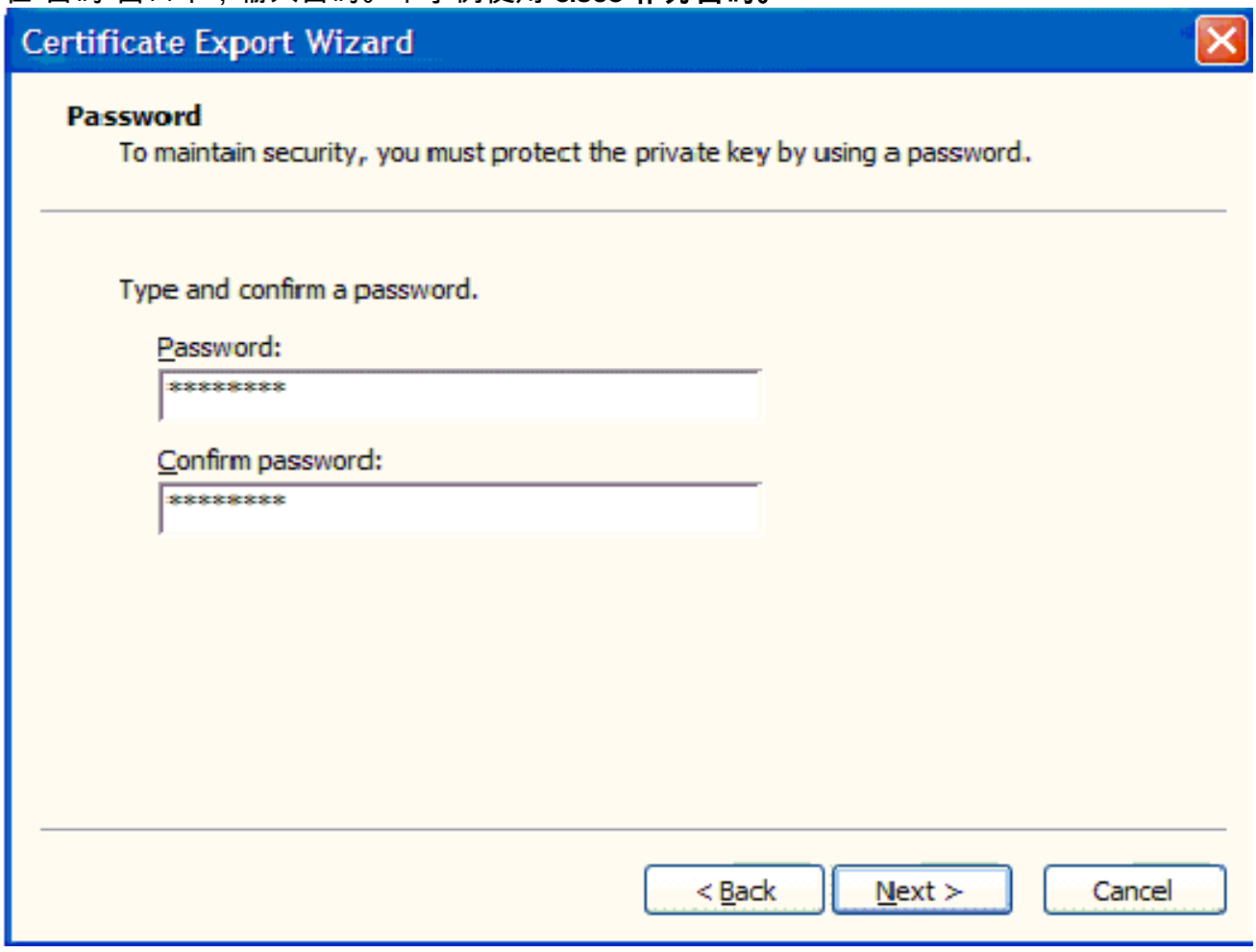


14. 在接下来的窗口中单击**下一步。**在“证书导出向导”窗口中选择**是，导出私有密钥选项。**单击**Next。**

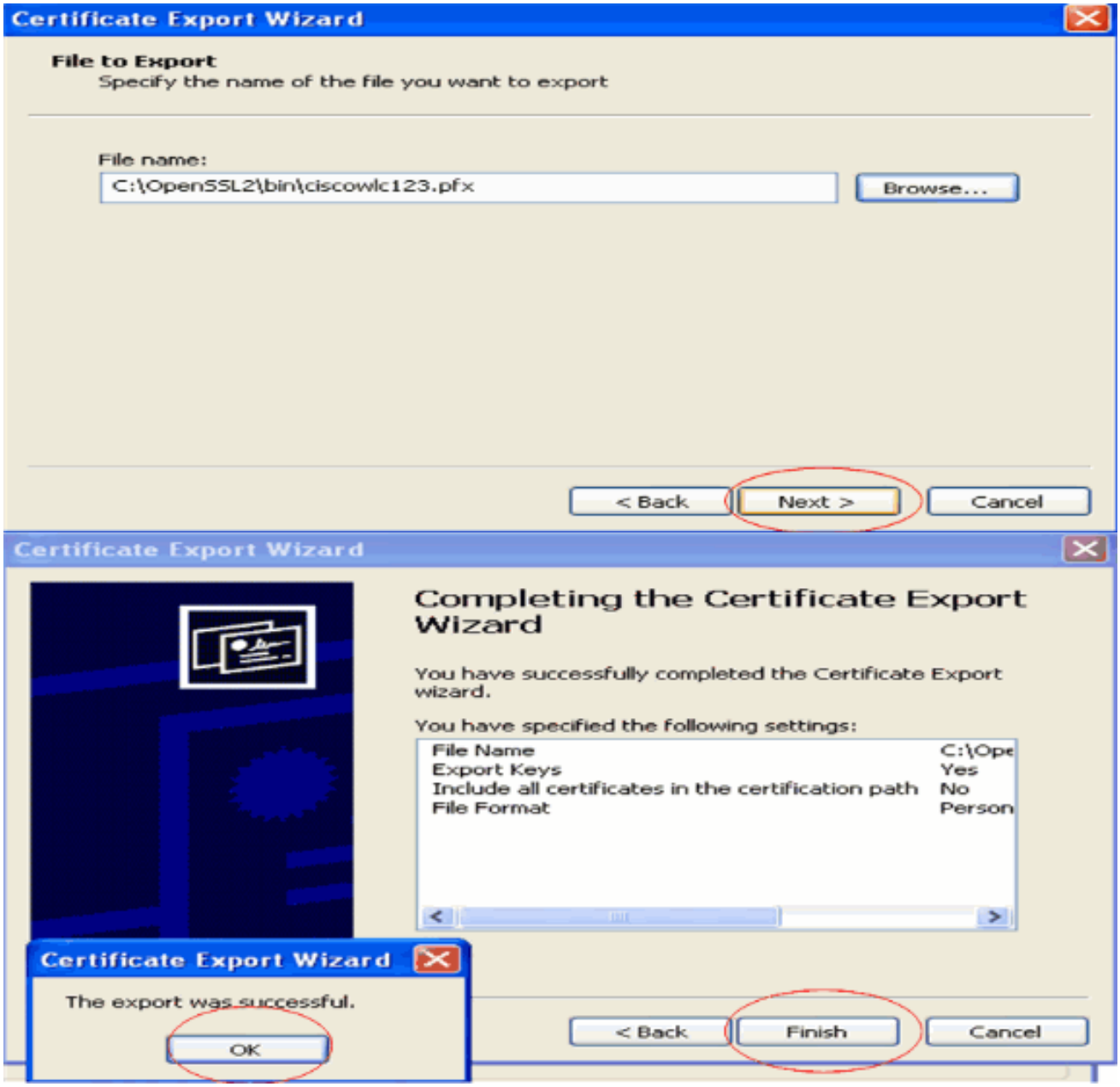
15. 选择 **.pfx 作为导出文件格式，并且选择“启用严格保护”选项。**单击 **Next。**



16. 在“密码”窗口中，输入密码。本示例使用 **cisco 作为密码。**



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。**



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 Openssl.exe 文件，输入以下命令：

注意：可以从OpenSSL网站下载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 地址。
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：

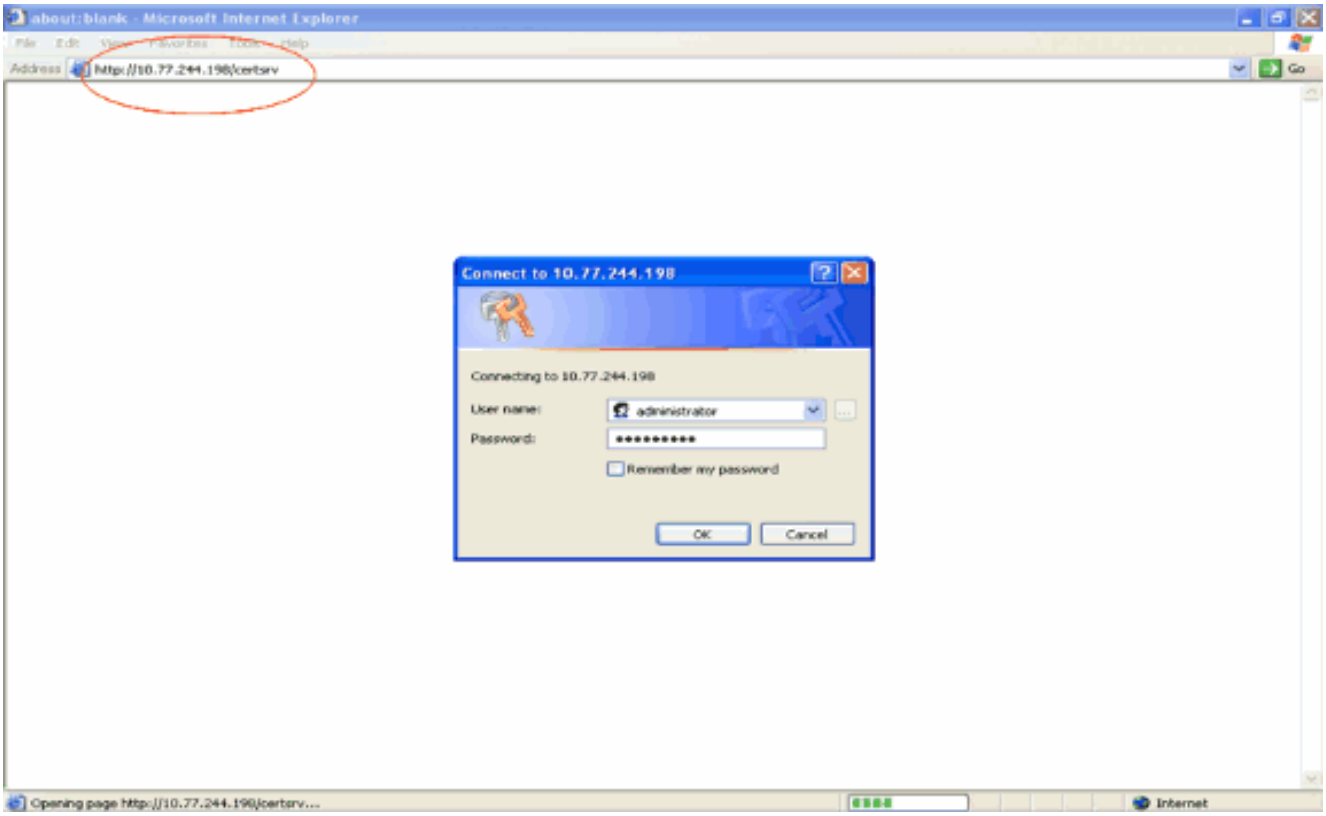
```
(Cisco Controller) >transfer download start

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

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

7. 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。

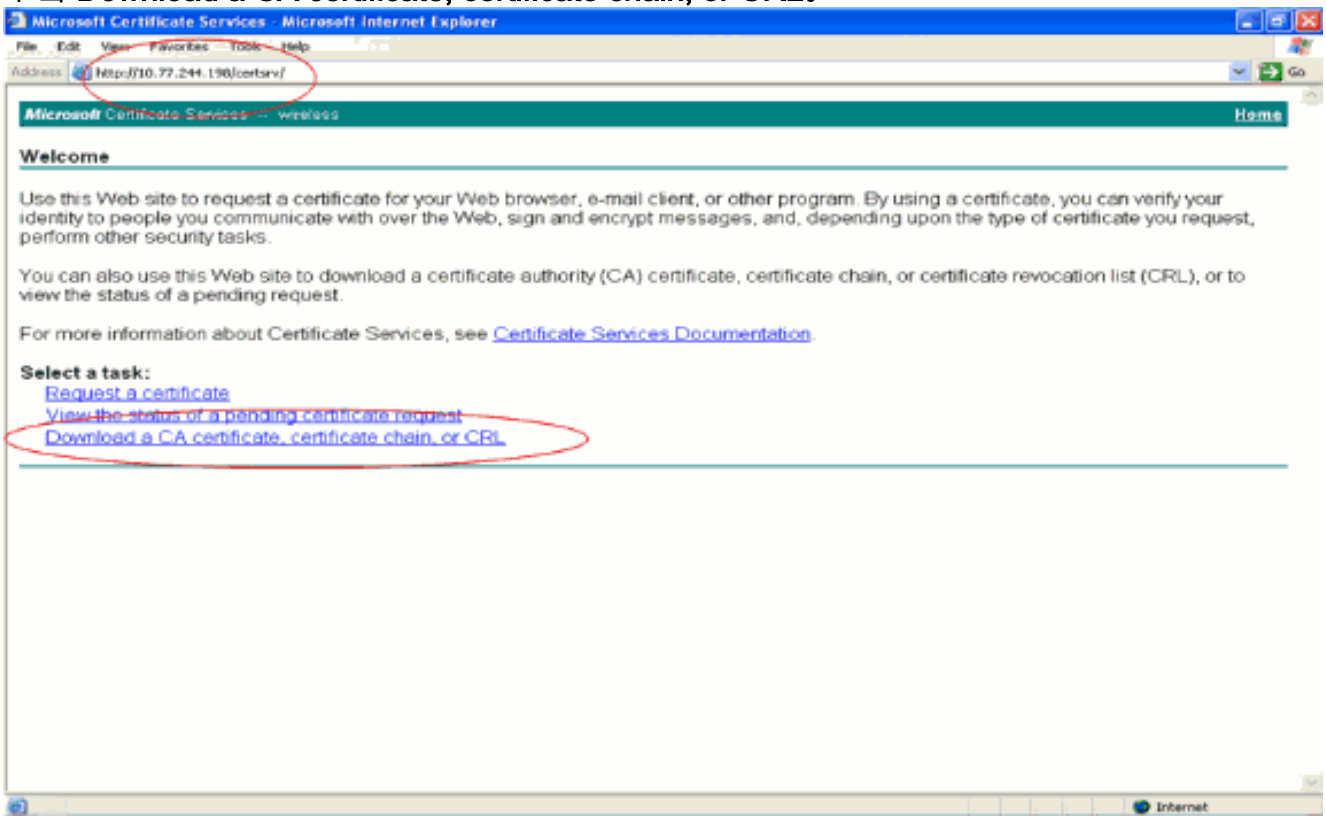
将 PKI 的根证书安装到 WLC 中

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：

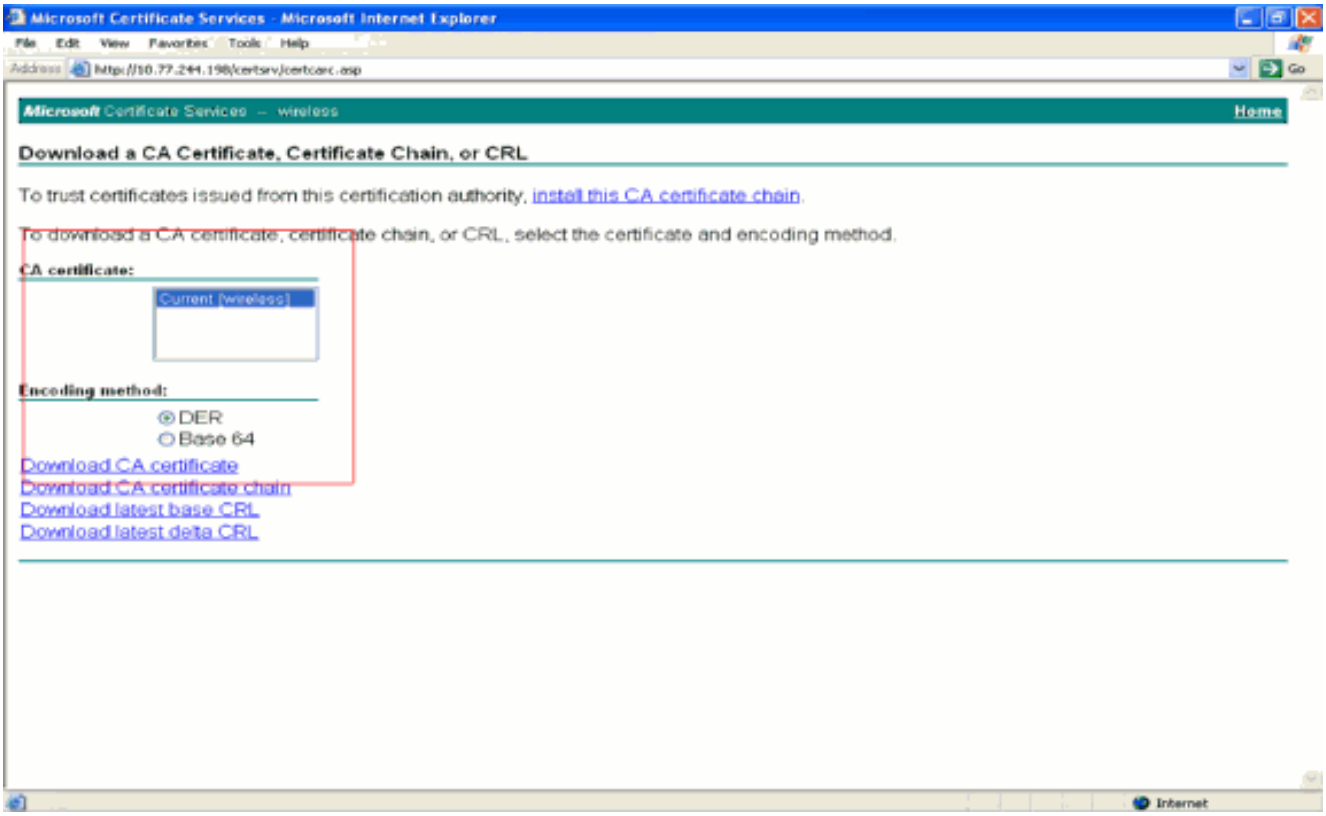
1. **在与 CA 服务器相连的 PC 上，访问 http://<CA 服务器的 IP 地址>/certsrv。**以 CA 服务器的管理员身份登录。



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



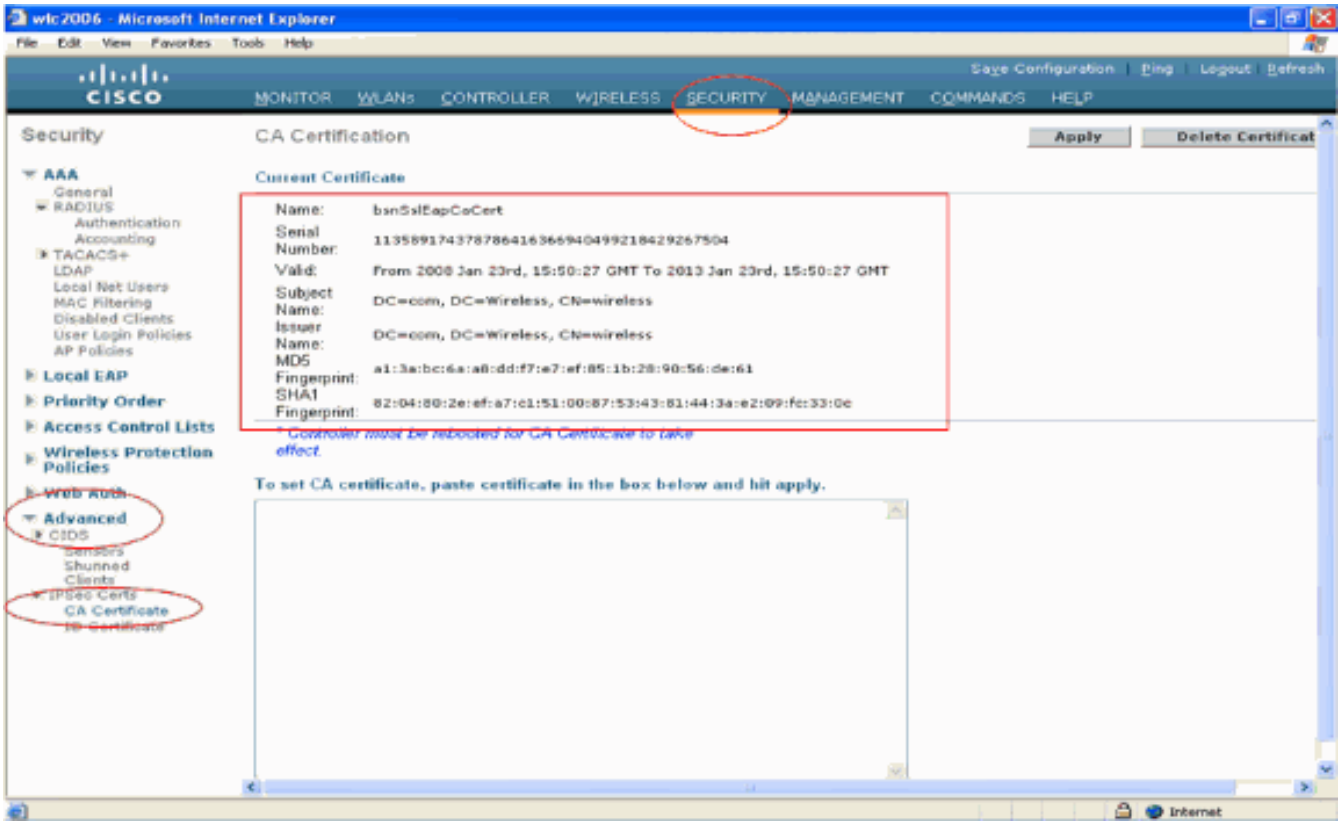
3. 在所显示的页中，您会在 CA certificate 框下看到 CA 服务器上当前可用的 CA 证书。选择 DER 作为编码方法，然后单击“Download CA certificate”。



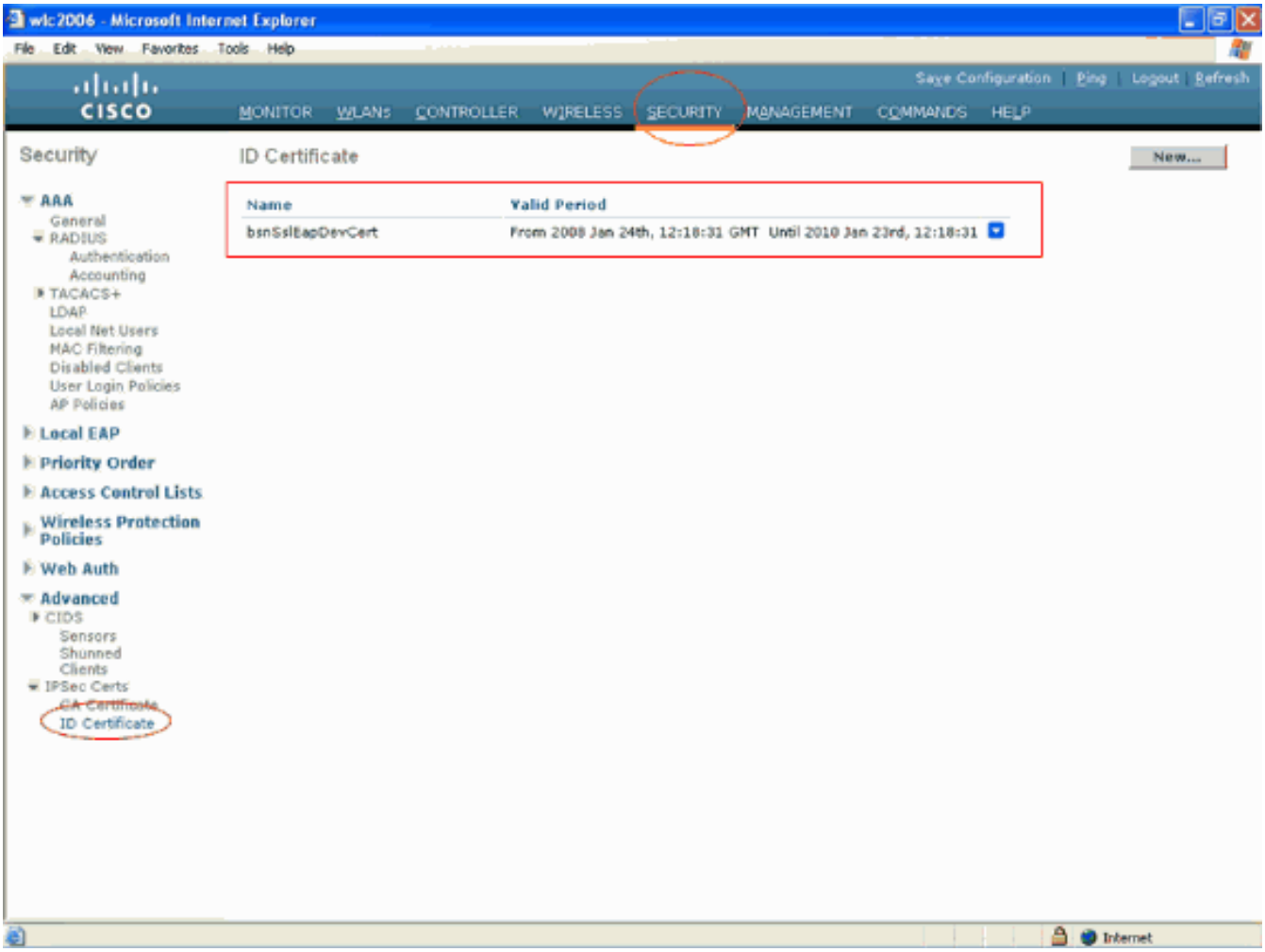
4. 将证书另存为 **.cer 文件。**本示例使用 **certnew.cer 作为文件名。**
5. 下一步是将 .cer 文件转换为 PEM 格式，并将其下载到控制器上。要执行这些步骤，请重复将设备证书下载到 WLC 上部分所述的过程，但有以下变化：openSSL 的 "-in" 和 "-out" 文件分别为 **certnew.cer 和 certnew.pem。**而且，此过程不需要 PEM 通行证短语或导入密码。而且，用于将 **.cer 文件转换为 .pem 文件的 openSSL 命令是：x509 -in *certnew.cer -inform DER -out certnew.pem -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
:

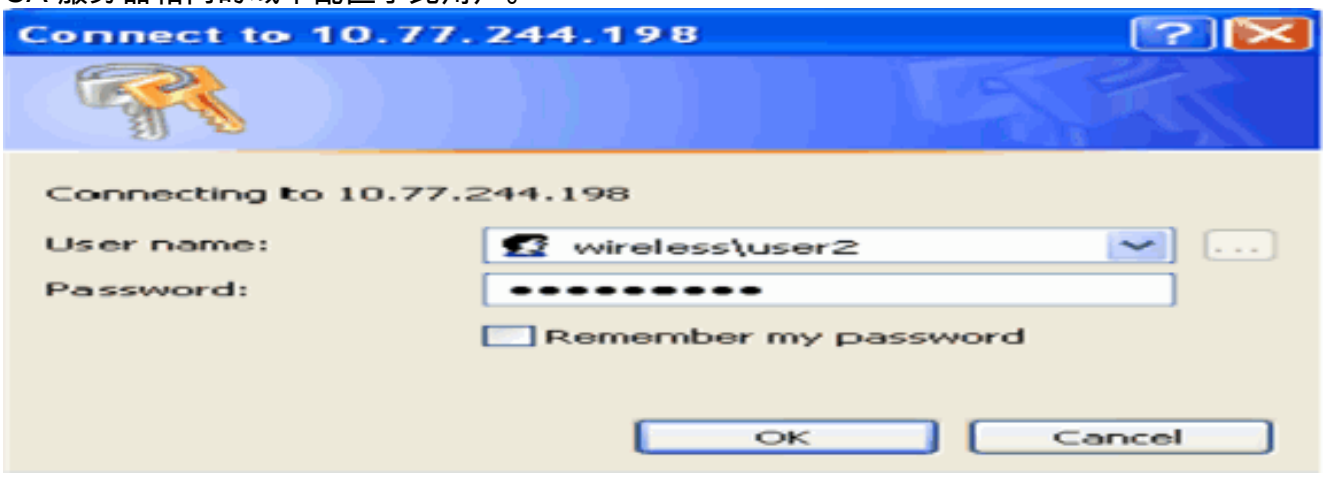


为客户端生成设备证书

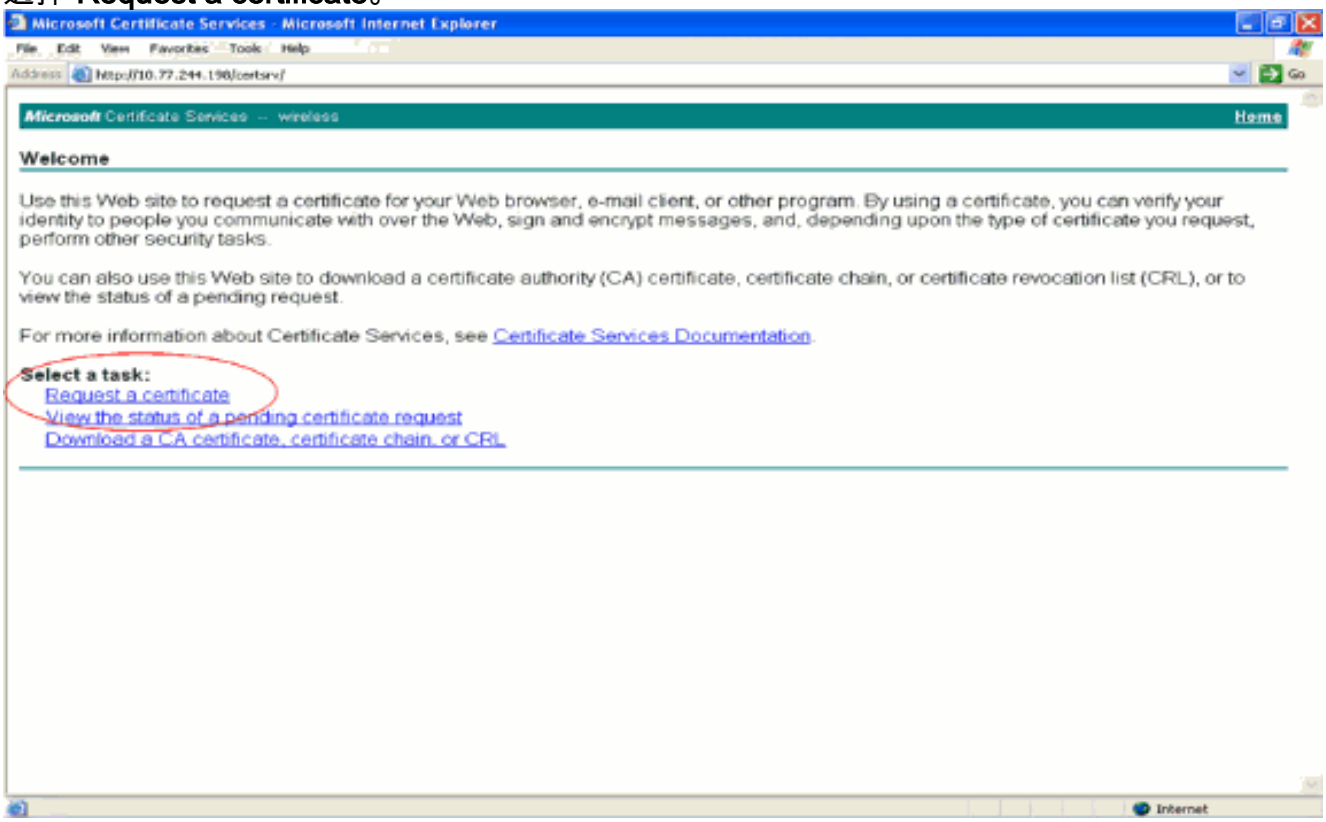
现在设备证书和 CA 证书均已安装到 WLC 上，下一步是为客户端生成这些证书。

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。

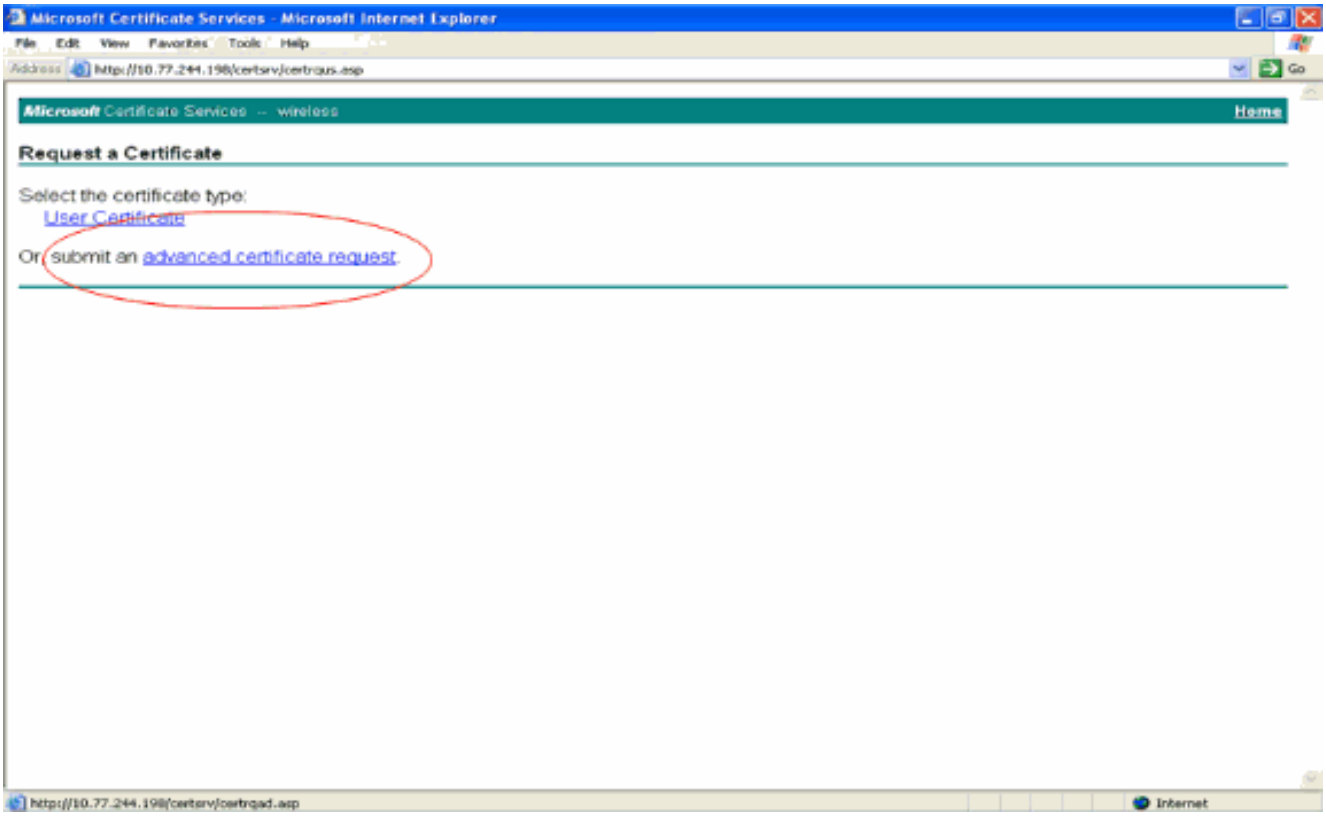
1. 从需要安装证书的客户端上，访问 **http://<CA 服务器的 IP 地址>/certsrv。**以域名\用户名的形式登录到 CA 服务器上。用户名应该是使用这台 XP 计算机的用户的名称，并且应该已经在与 CA 服务器相同的域中配置了此用户。



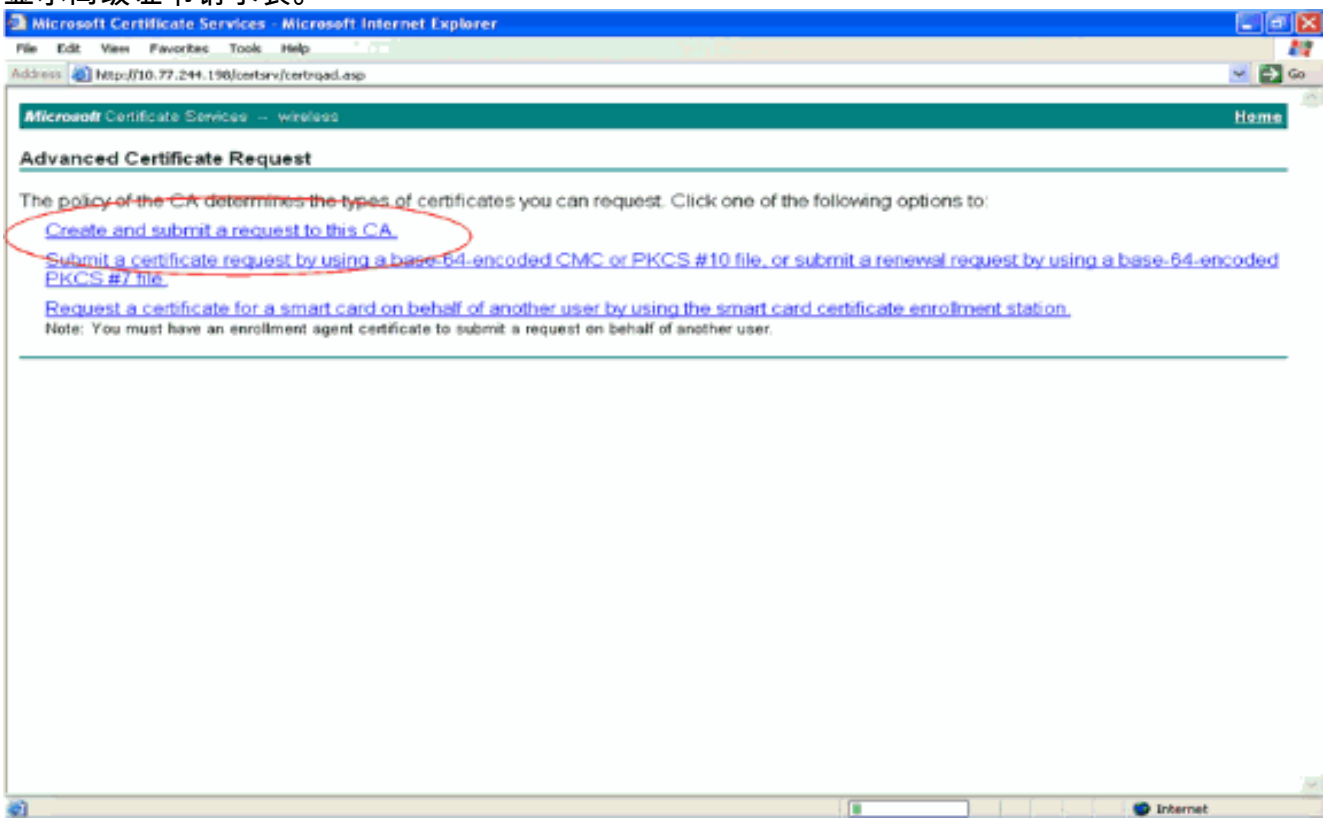
2. 选择 **Request a certificate。**



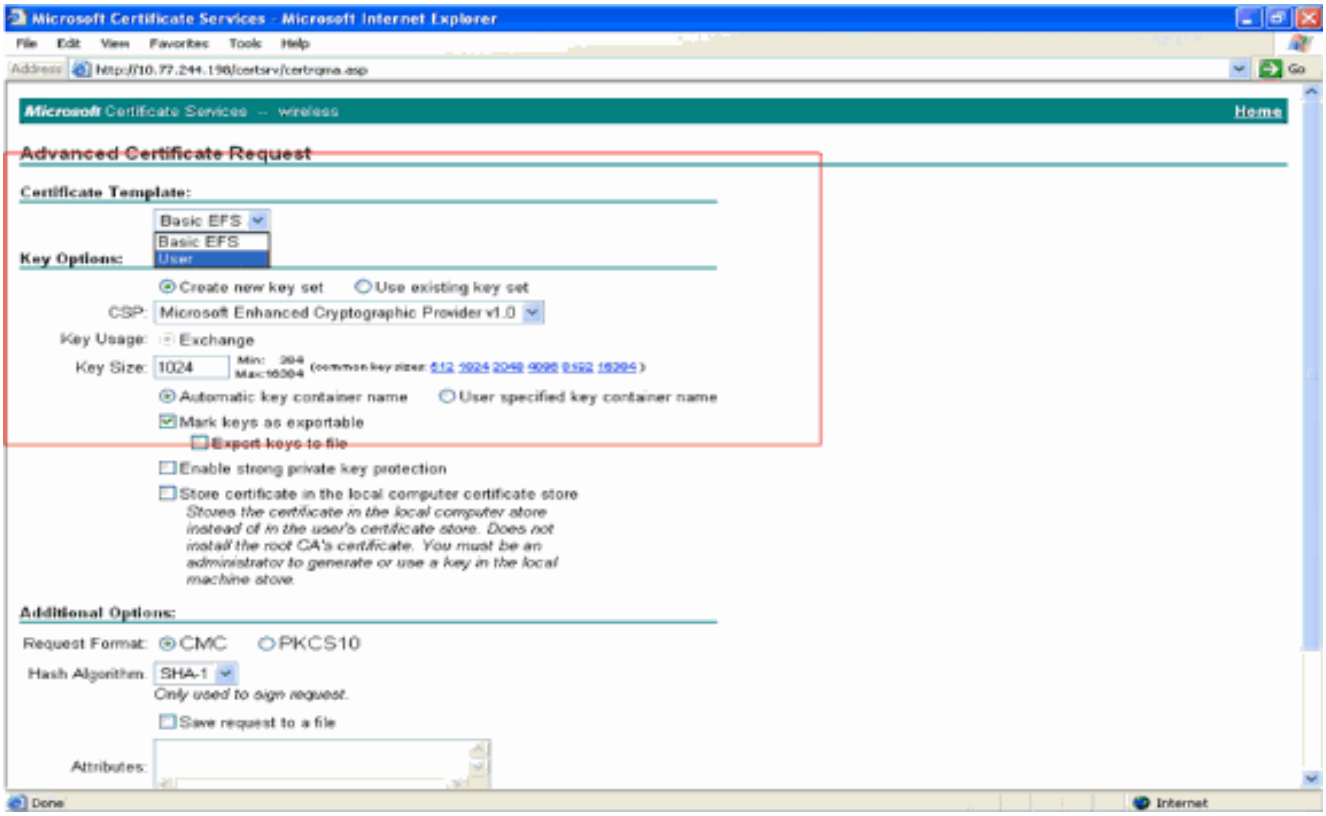
3. 在“Request a Certificate”页中，单击 **advanced certificate request。**



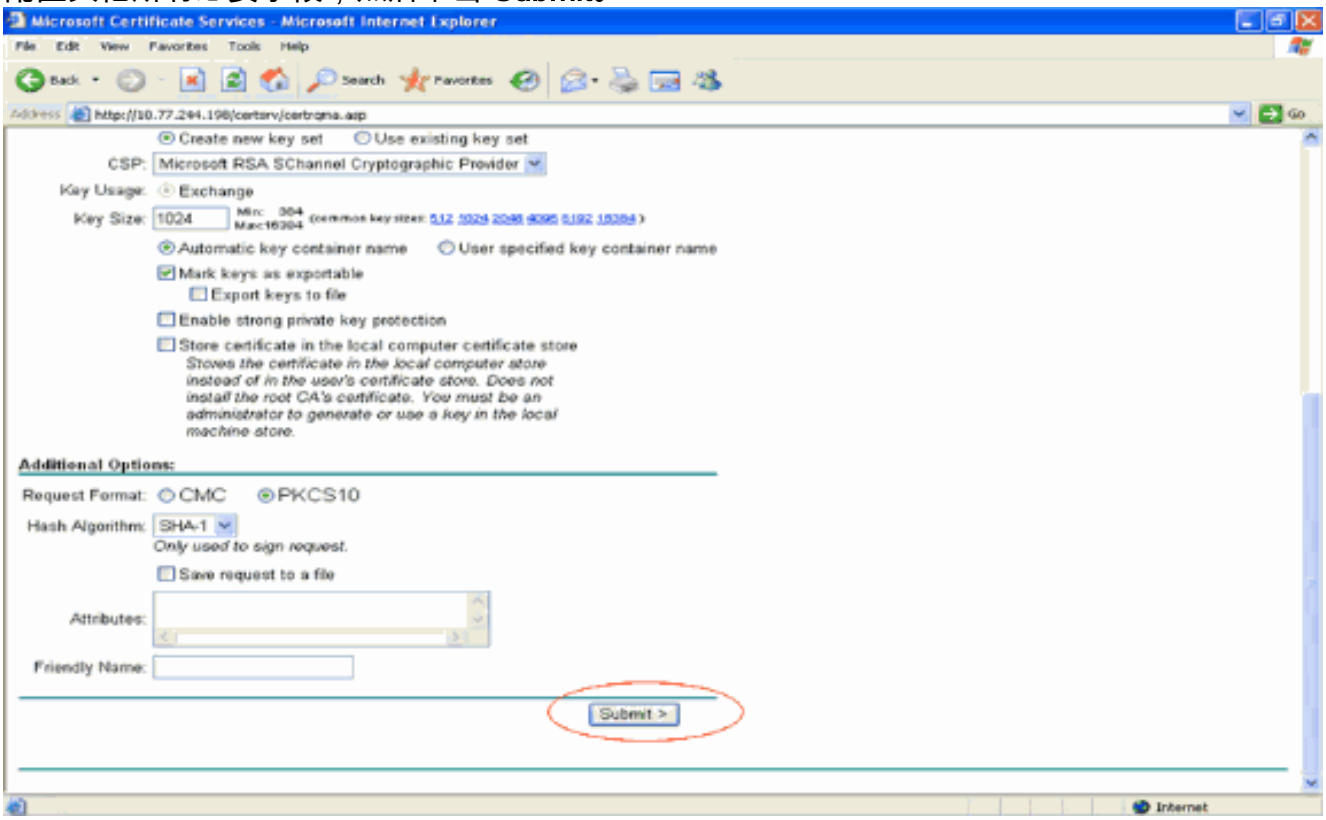
4. 在“Advanced Certificate Request”页中，单击 **Create and submit a request to this CA。**这将显示高级证书请求表。



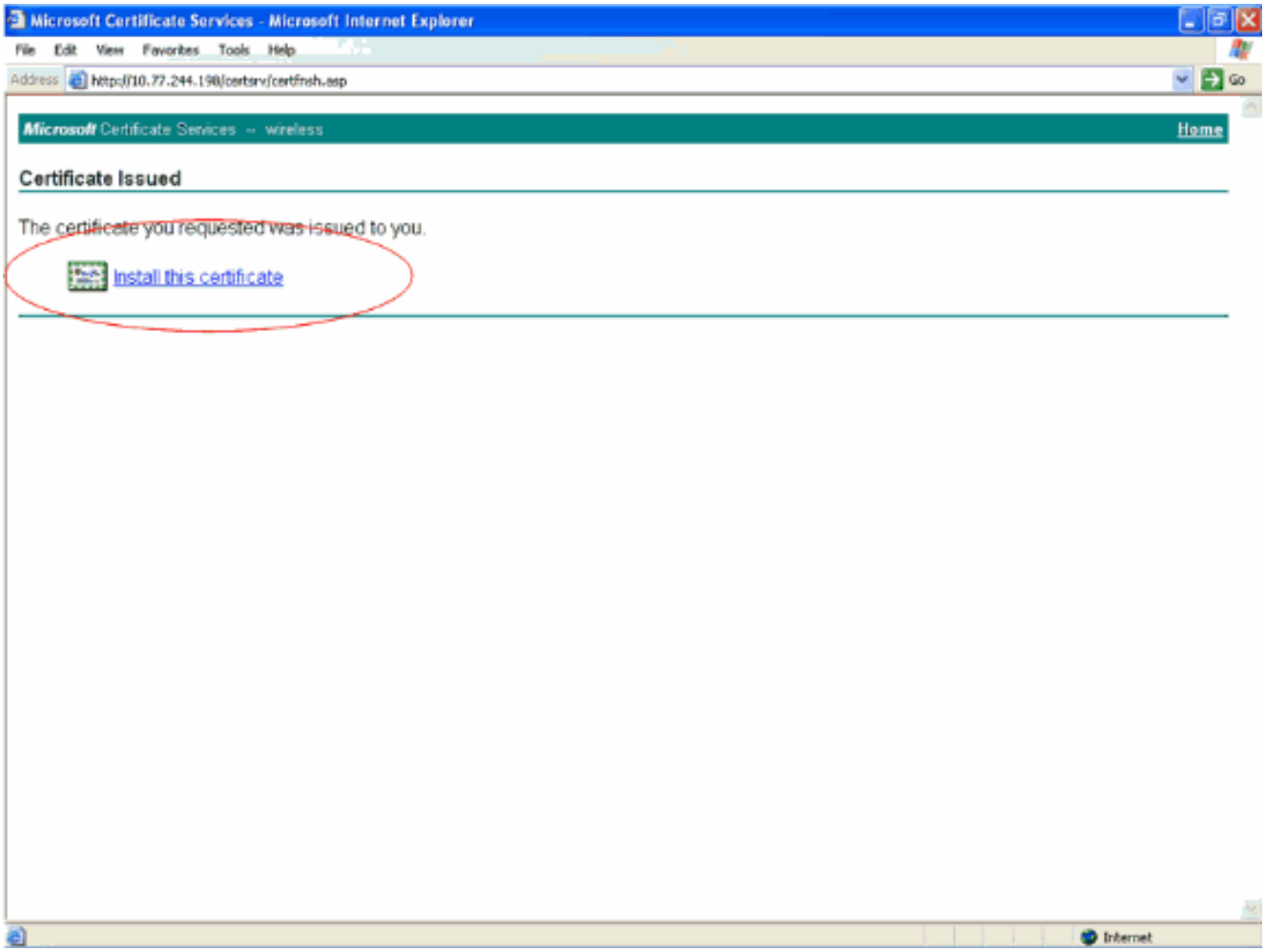
5. 在高级证书请求表中，从“Certificate Template”下拉菜单中选择 **User。**在密钥选项部分下，选择以下参数：在“Key Size”字段中输入密钥大小。本示例使用 **1024。**选中 **Mark Keys as Exportable 选项。**



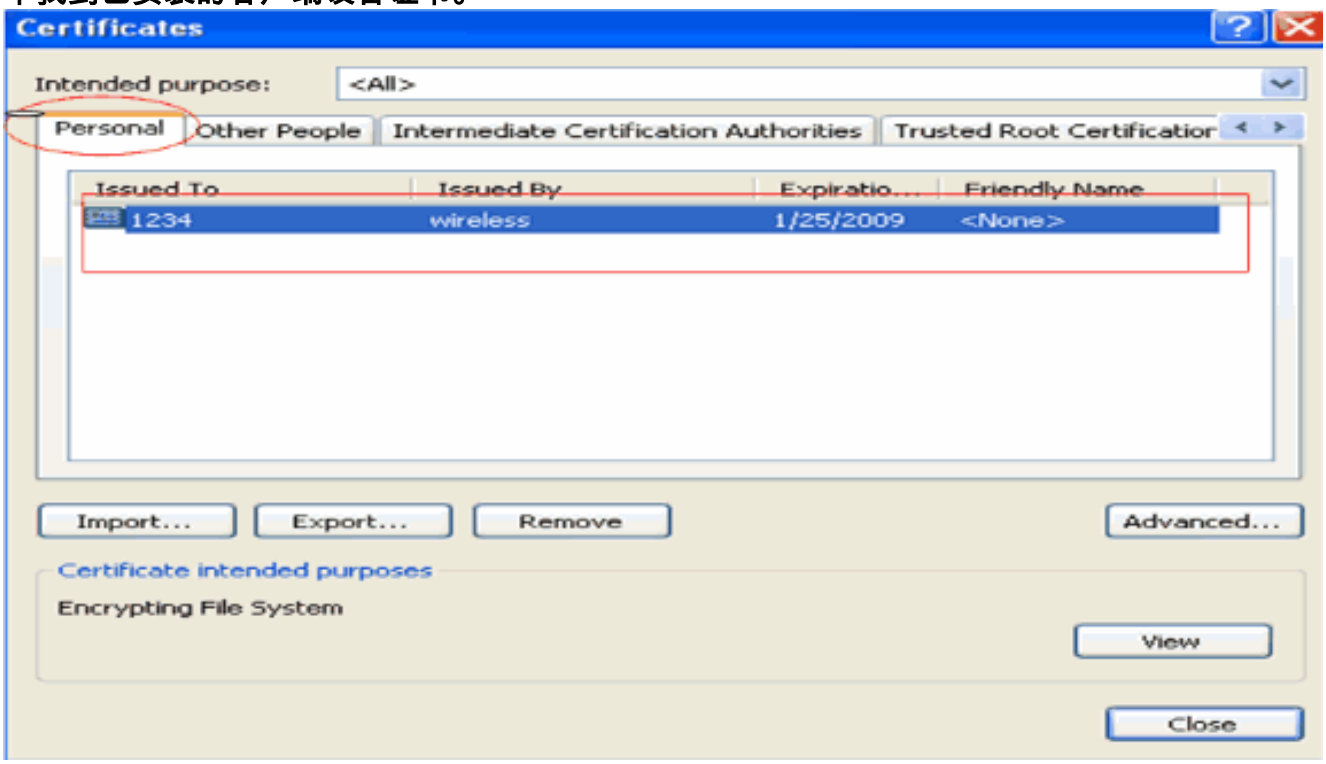
6. 配置其他所有必要字段，然后单击 **Submit**。



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。**



8. 通过客户端的 IE 浏览器，您应该能够在**工具 > Internet 选项 > 内容 > 证书下的个人证书列表中找到已安装的客户端设备证书。**

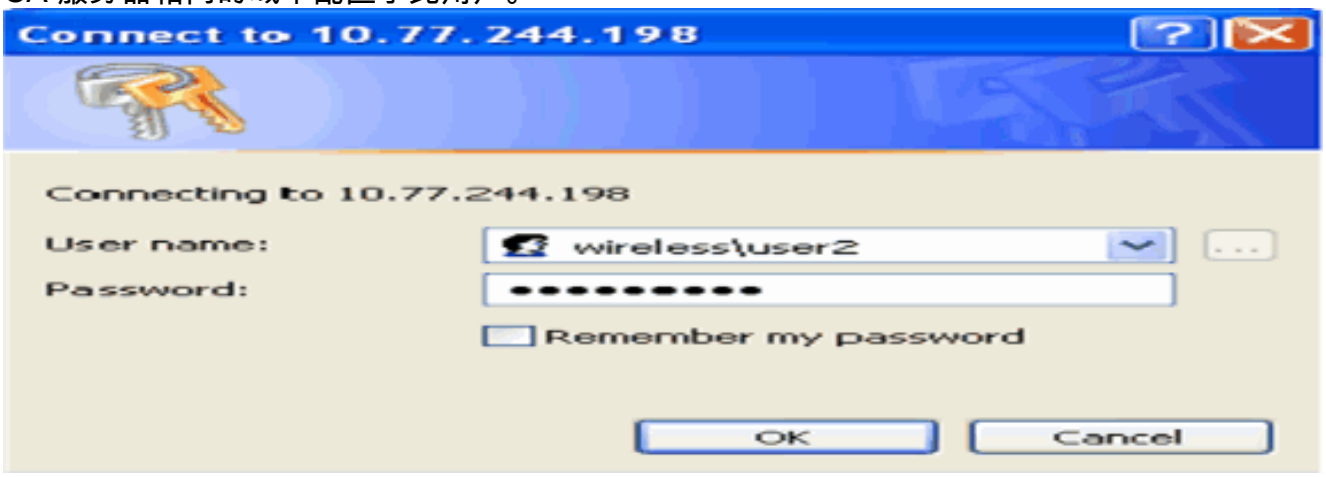


客户端的设备证书就已经安装到客户端上。

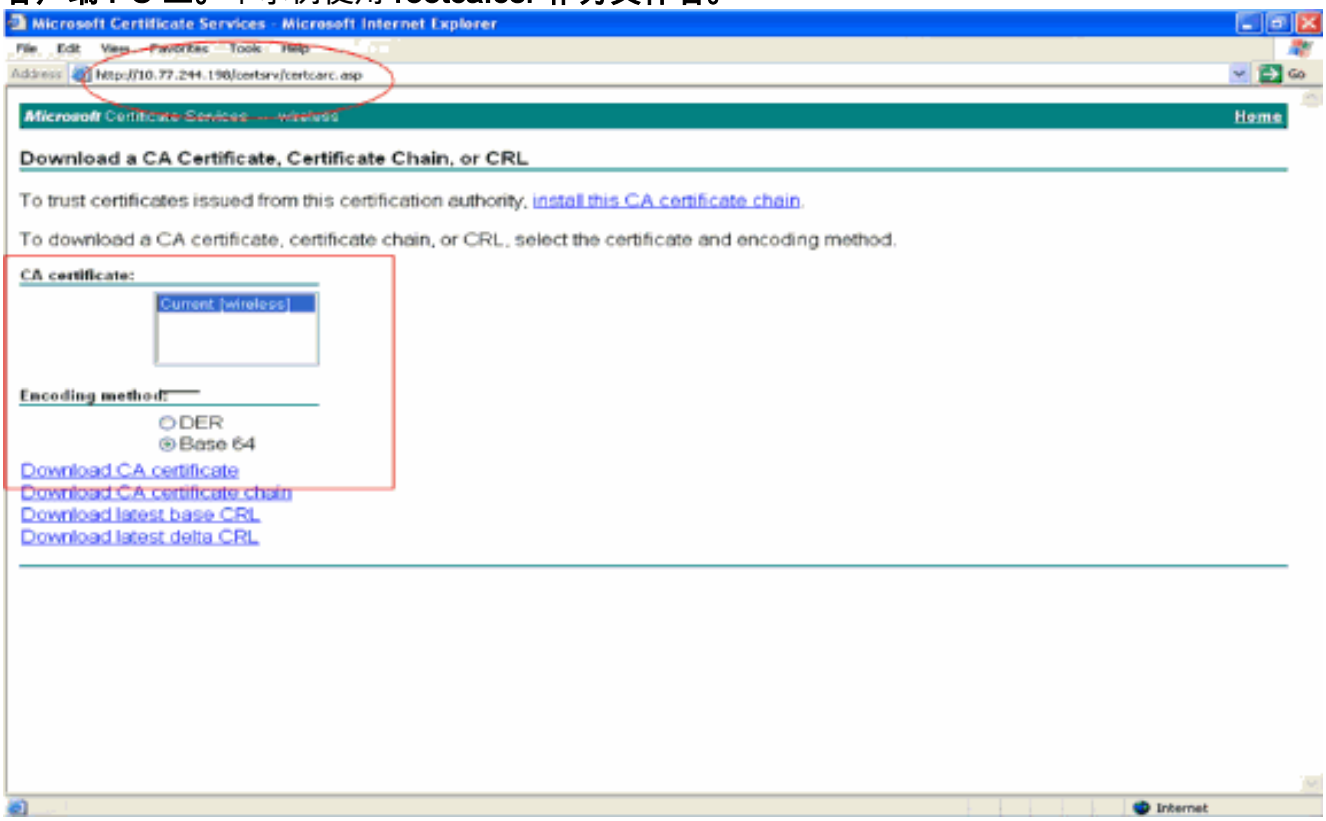
为客户端生成根 CA 证书

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：

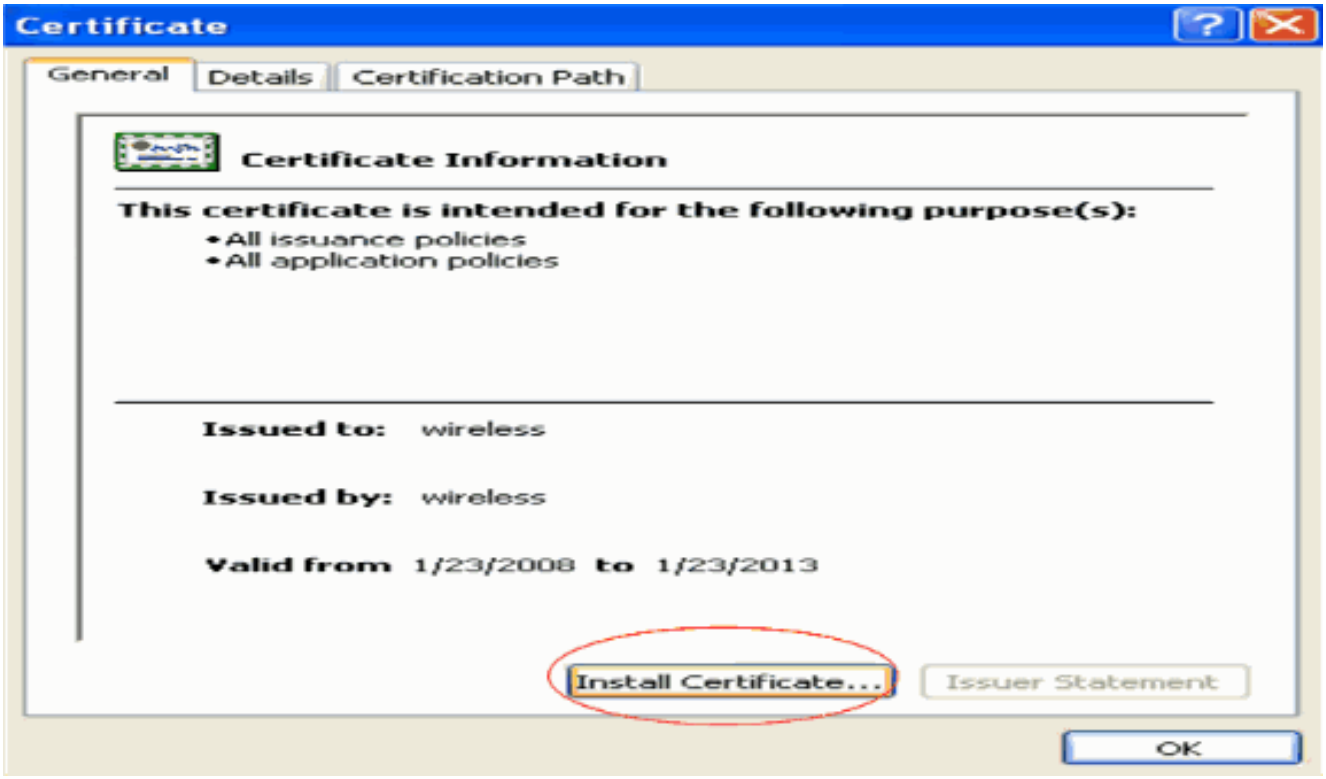
1. 从需要安装证书的客户端上，访问 **http://<CA 服务器的 IP 地址>/certsrv。**以域名\用户名的形式登录到 CA 服务器上。用户名应该是使用这台 XP 计算机的用户的名称，并且应该已经在与 CA 服务器相同的域中配置了此用户。



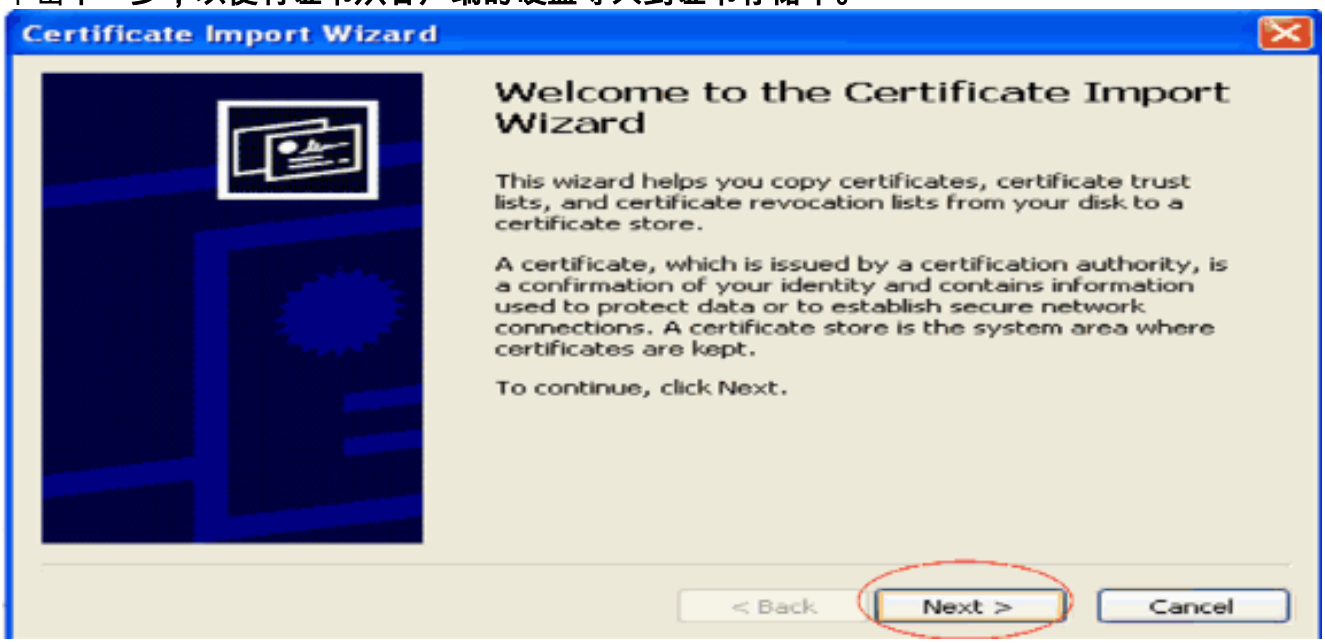
2. 在所显示的页中，您会在 **CA certificate 框下看到 CA 服务器上当前可用的 CA 证书。**选择 **Base 64 作为编码方法。**然后，单击 **Download CA certificate，并将文件作为 .cer 文件保存到客户端 PC 上。**本示例使用 **rootca.cer 作为文件名。**



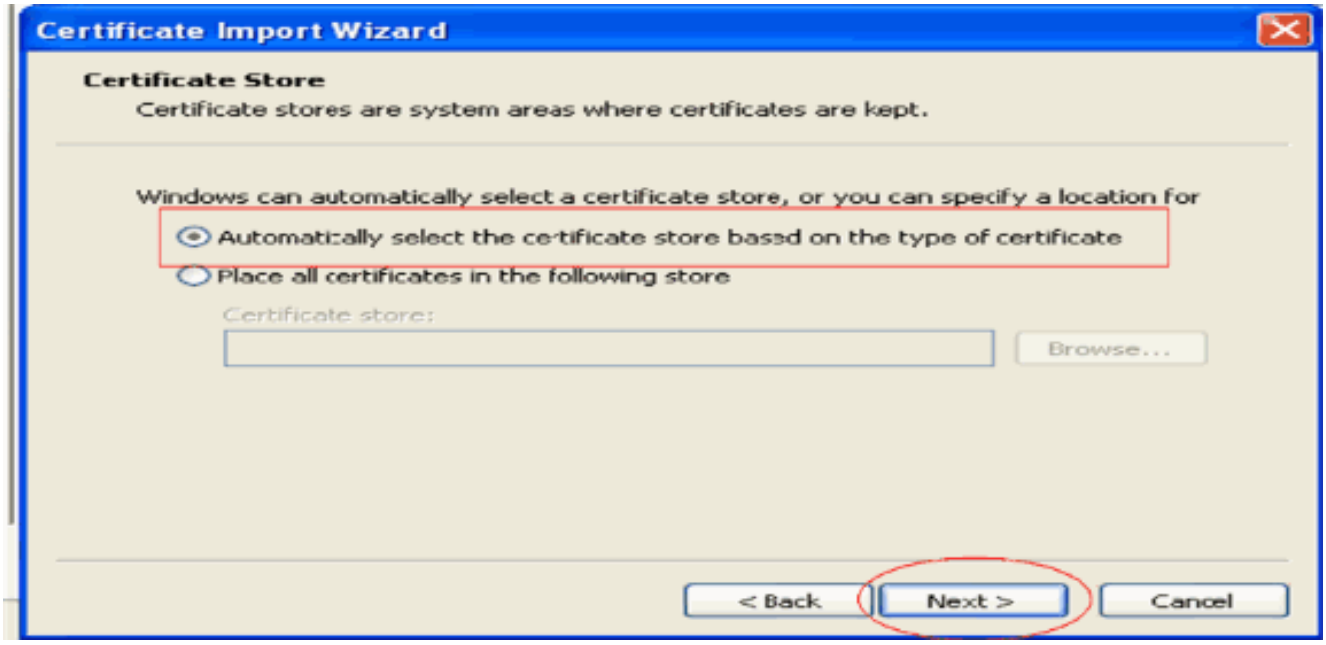
3. 下一步，将 .cer 格式的 CA 证书安装到客户端的证书存储中。双击 rootca.cer 文件，然后单击 **安装证书。**



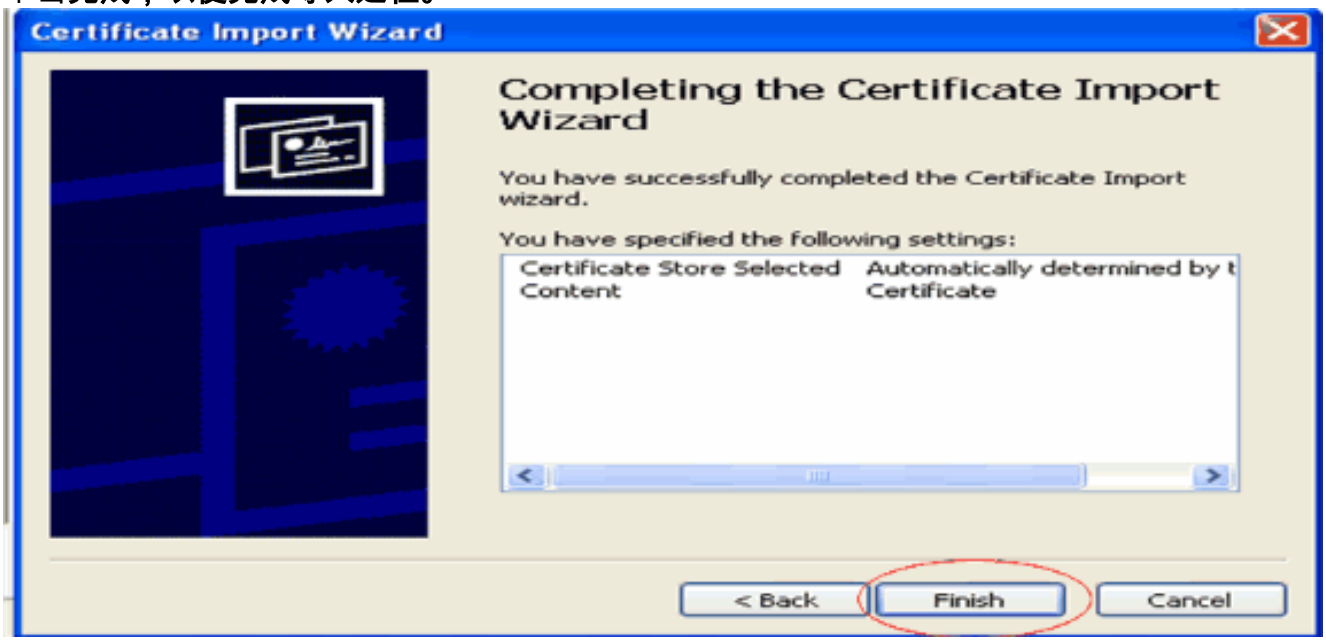
4. 单击**下一步，以便将证书从客户端的硬盘导入到证书存储中。**



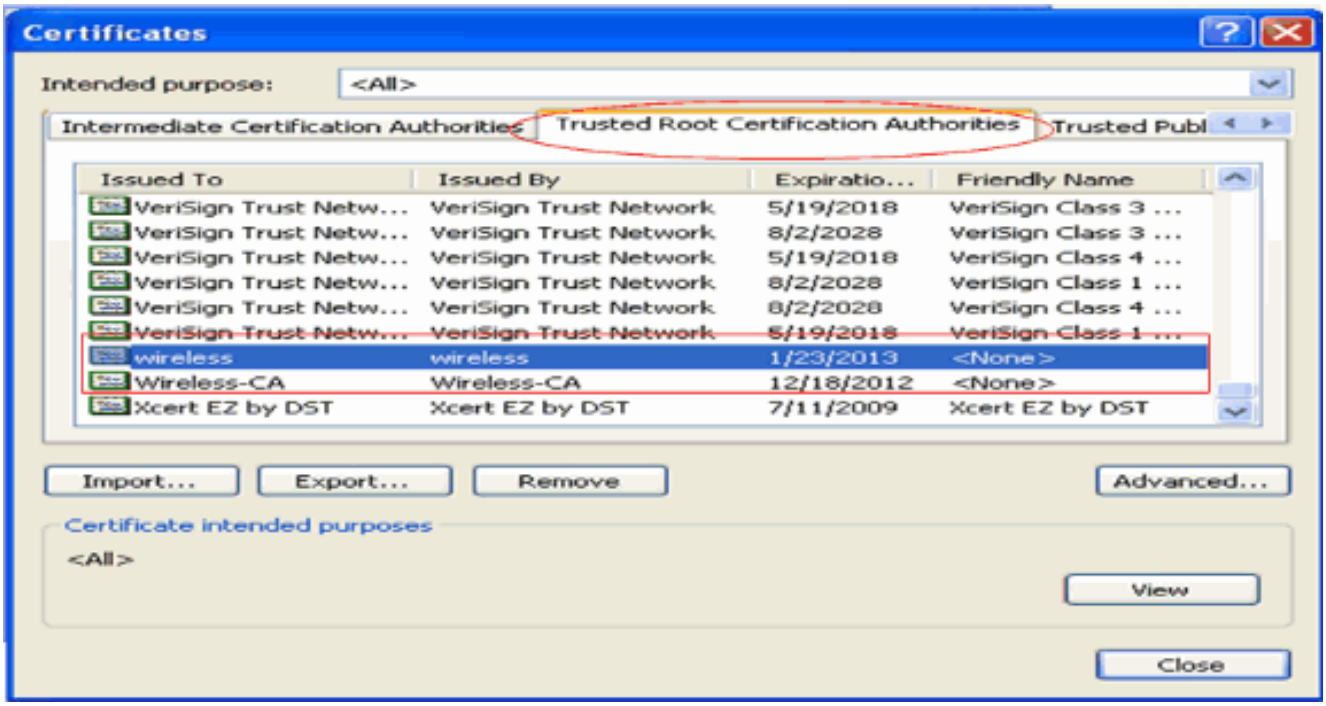
5. 选择**根据证书类型，自动选择证书存储，然后单击"下一步"。**



6. 单击**完成，以便完成导入过程。**



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：

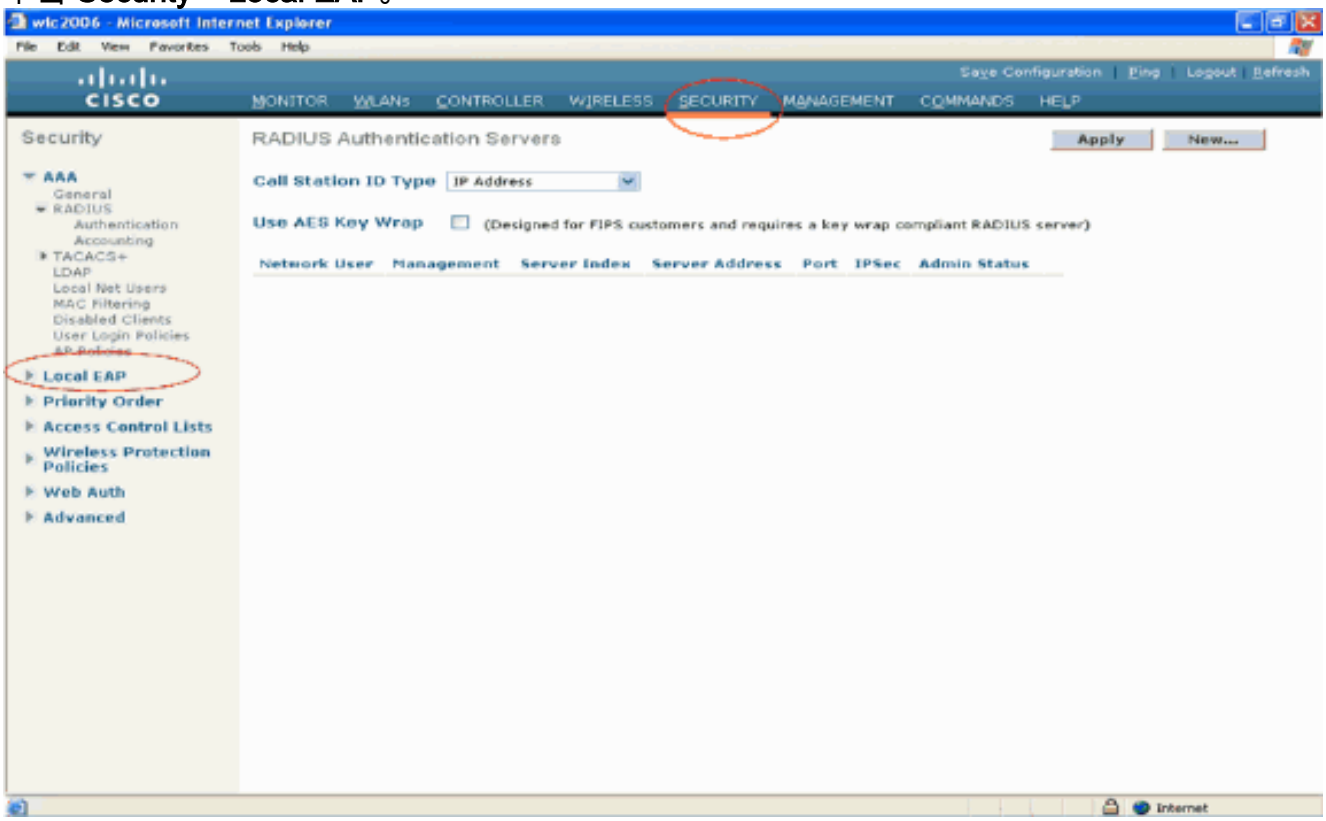


EAP-FAST 本地 EAP 身份验证所需的所有证书都已经安装在 WLC 和客户端上。下一步是为本地 EAP 身份验证配置 WLC。

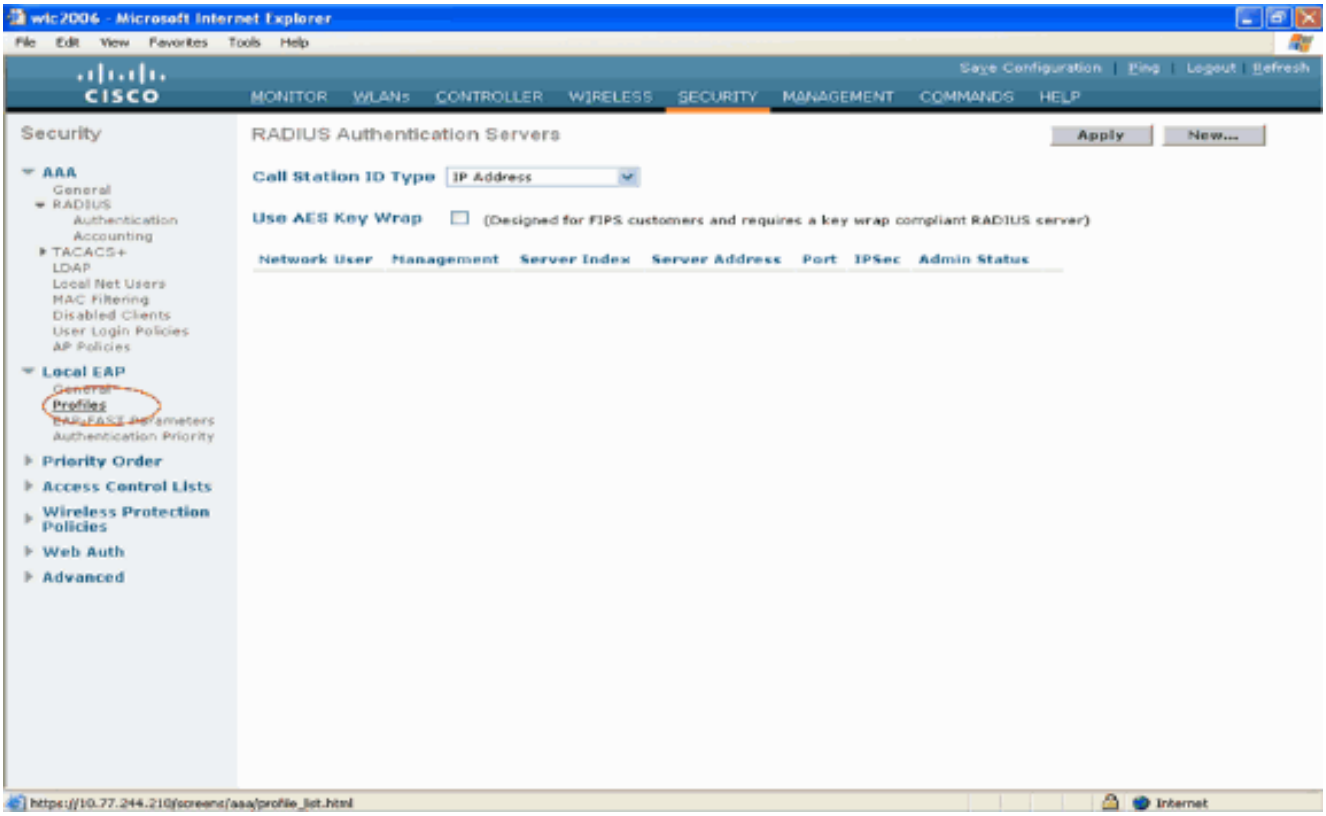
在 WLC 上配置本地 EAP

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：**

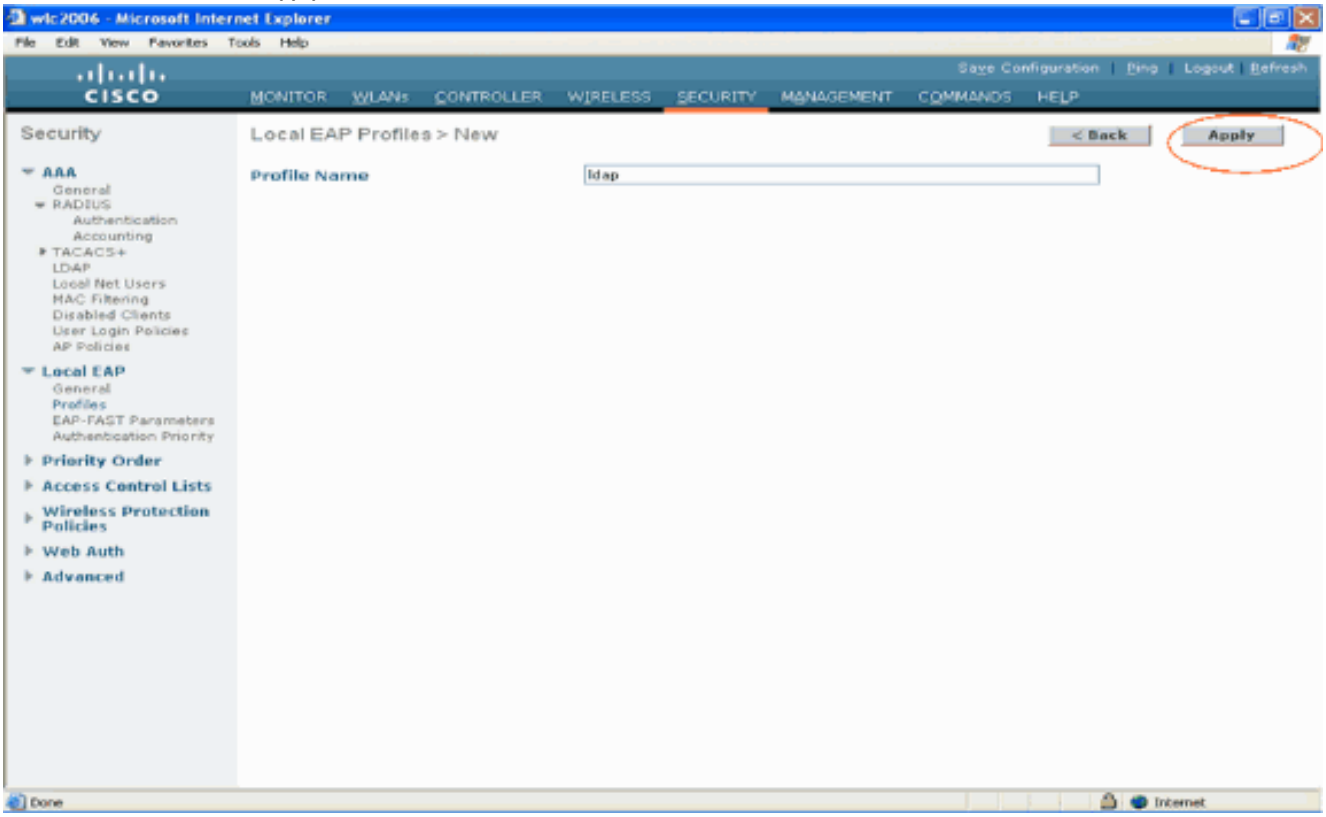
1. 单击 **Security > Local EAP。**



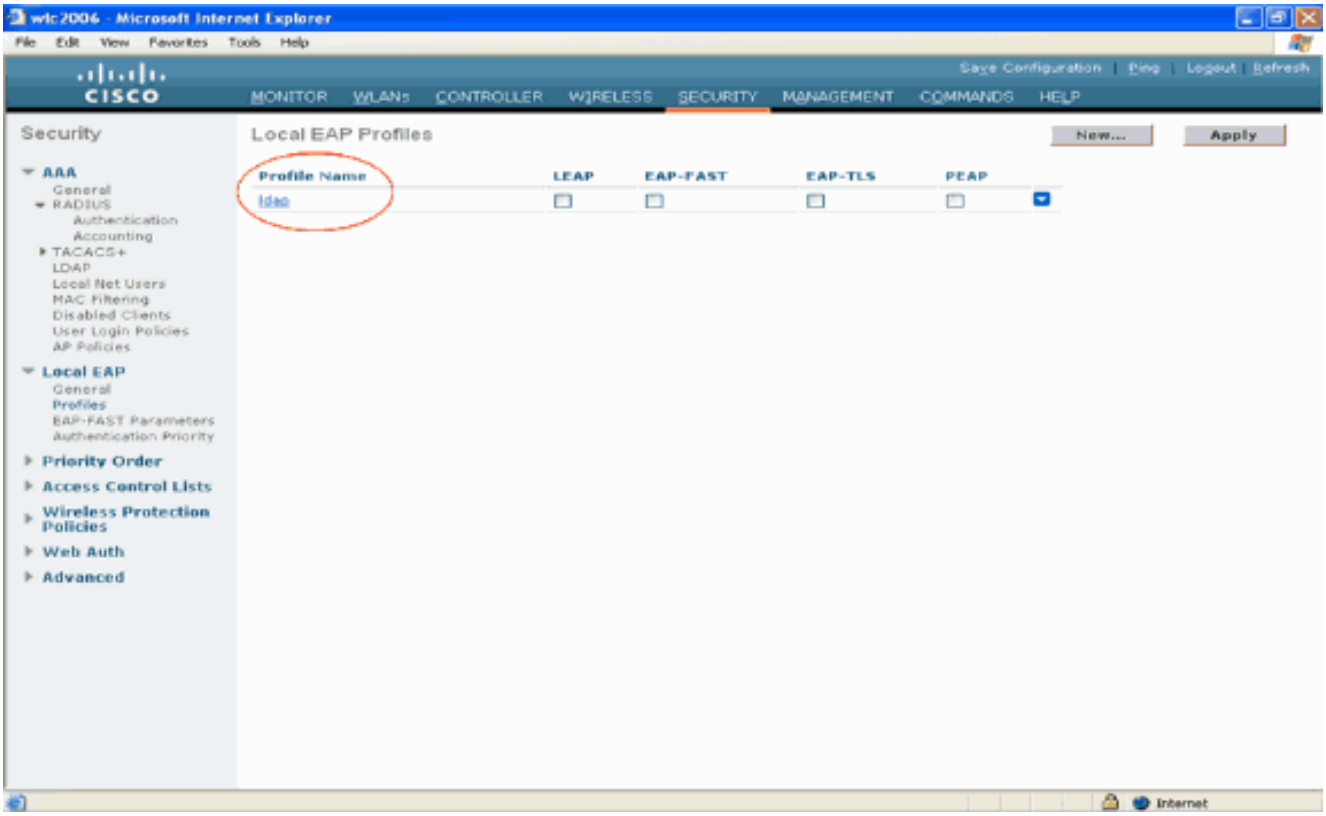
2. 在“Local EAP”下，单击 **Profiles，以便配置本地 EAP 配置文件。**



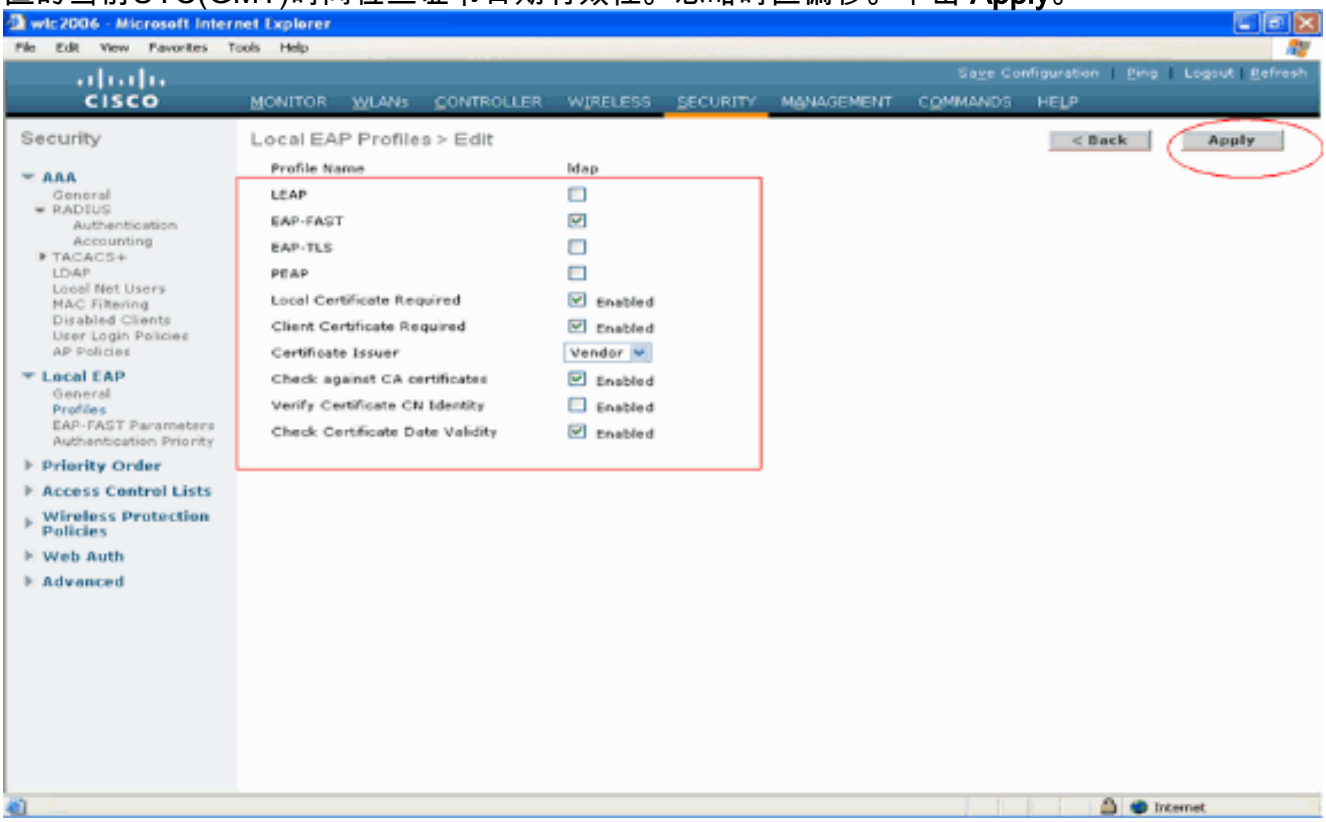
3. 单击 **New，以便创建新的本地 EAP 配置文件。**
4. 为此配置文件指定名称，然后单击 **Apply**。本示例中的配置文件名称为 **ldap**。这会显示 WLC 上创建的本地 EAP 配置文件。



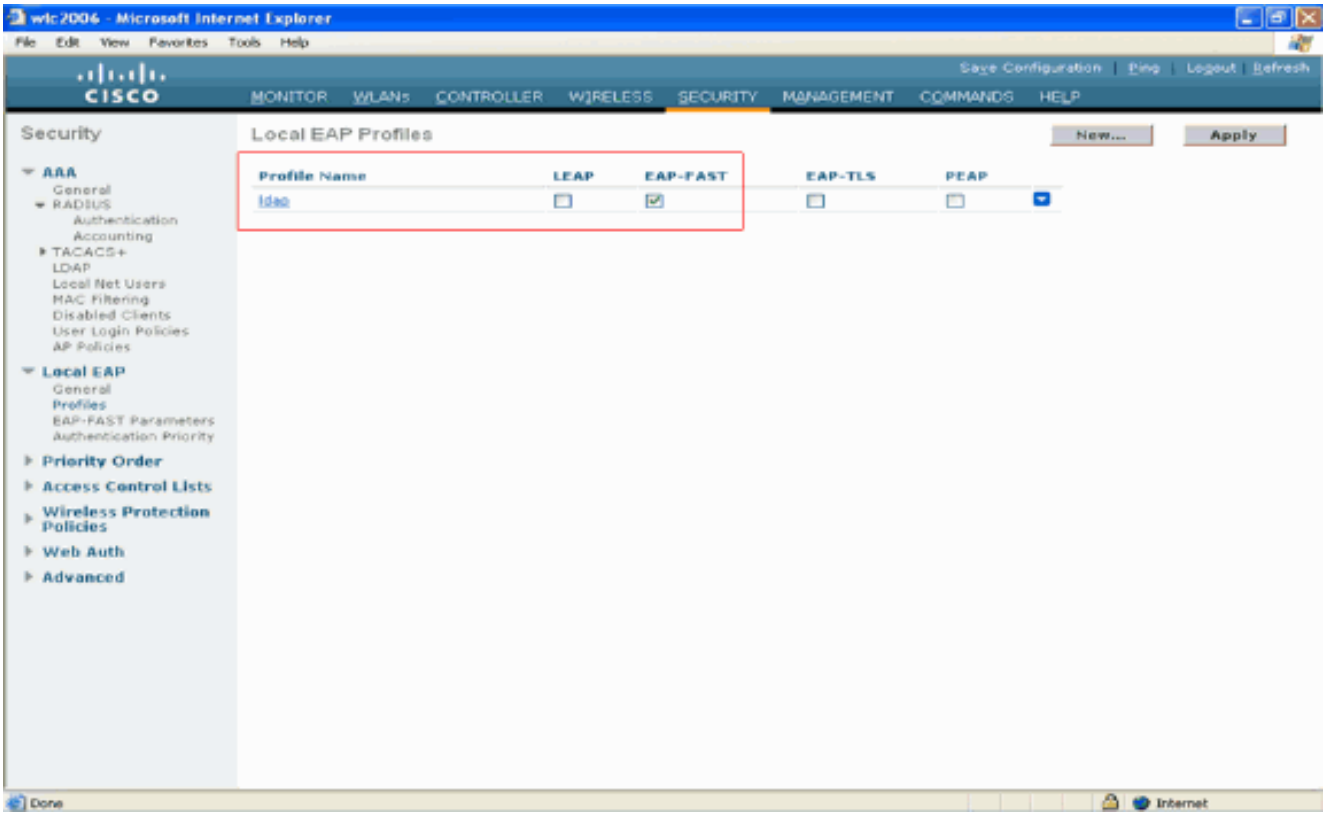
5. 单击刚刚创建的 **ldap 配置文件，该文件显示在“Local EAP Profiles”页的“Profile Name”字段下**。这会显示 **Local EAP Profiles > Edit 页。**



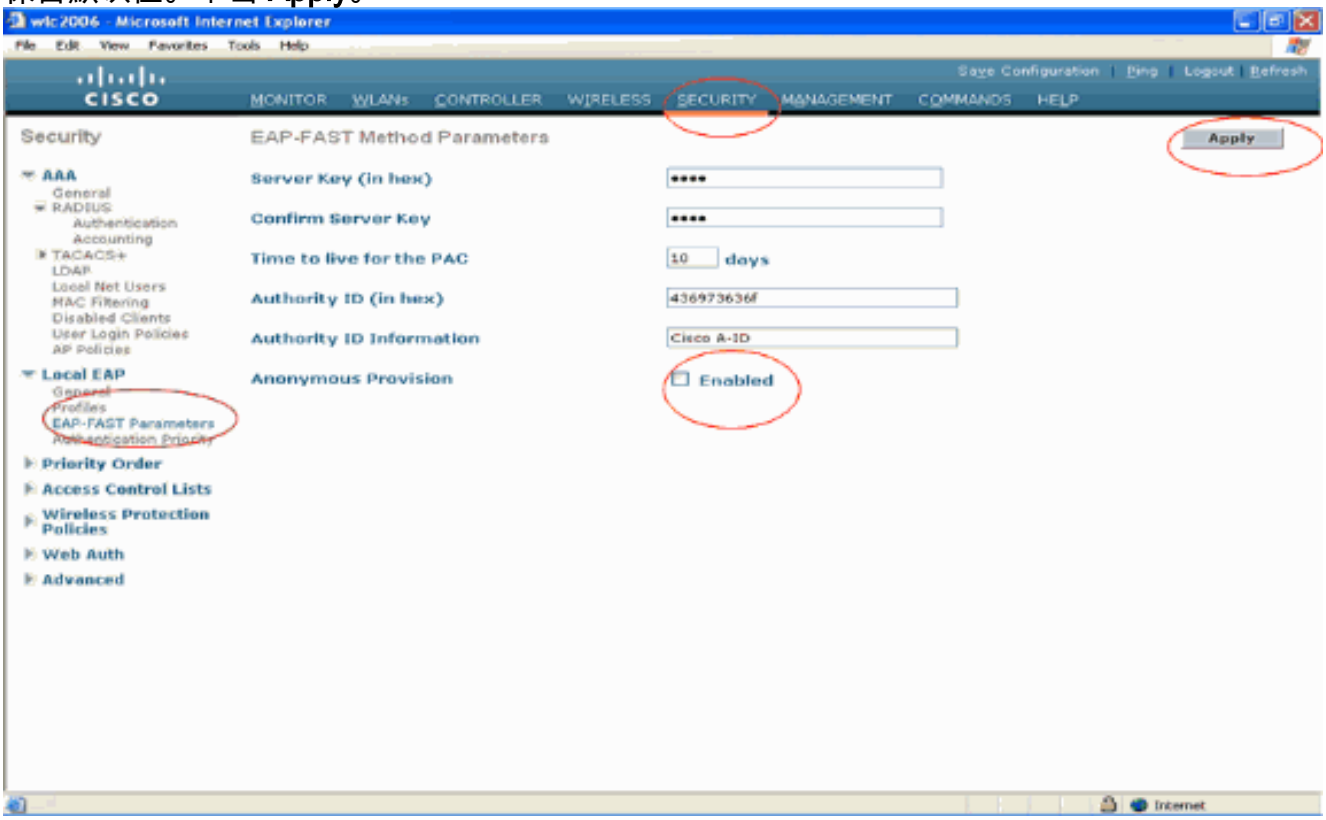
6. 在 **Local EAP Profiles > Edit 页上配置此配置文件的特定参数。**选择 **EAP-FAST 作为本地 EAP 身份验证方法。**启用 **Local Certificate Required 和"Client Certificate Required"旁边的复选框。**选择 **Vendor 作为证书颁发者，因为此文档使用第三方 CA 服务器。**启用 **Check against CA certificates 旁边的复选框，以便从客户端传入的证书针对控制器上的 CA 证书进行验证。**如果希望根据控制器上的CA证书的CN验证传入证书中的公用名(CN)，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**。



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。



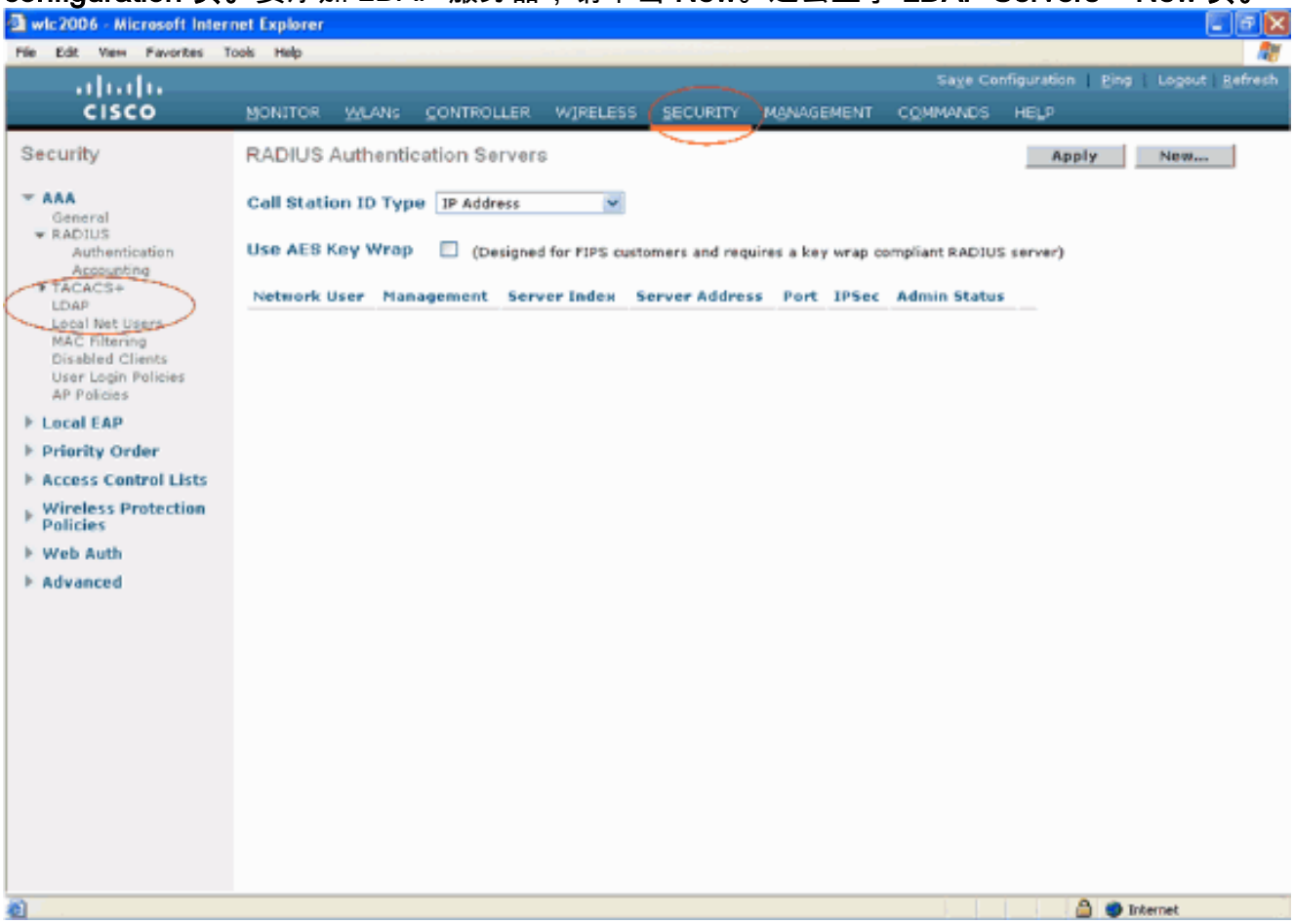
8. 下一步是在 WLC 上配置 EAP-FAST 的特定参数。在“WLC Security”页中，单击 **Local EAP > EAP-FAST Parameters，以便转到“EAP-FAST Method Parameters”页。**取消选中 **Anonymous Provision 复选框，因为本示例解释的是使用证书的 EAP-FAST。**使其他所有参数保留默认值。单击 **Apply**。



用 LDAP 服务器的详细信息配置 WLC

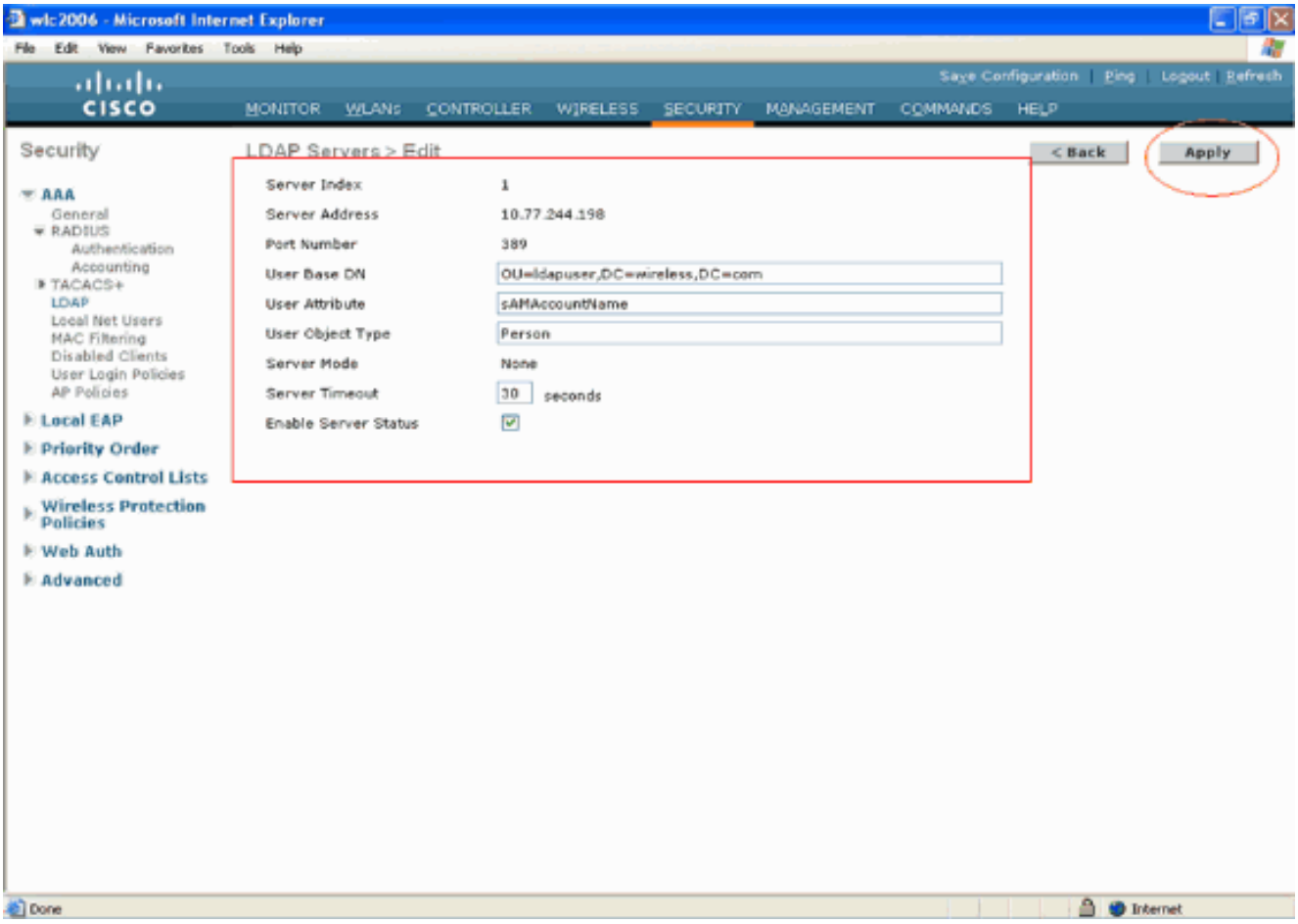
现在已经用本地 EAP 配置文件和相关信息对 WLC 进行了配置，下一步是用 LDAP 服务器的详细信息来配置 WLC。在 WLC 上完成以下步骤：

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。



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)**ldapuser**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=ldapuser, 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，请参阅本文档的使用 LDP 来识别用户属性部分中的讨论。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

：

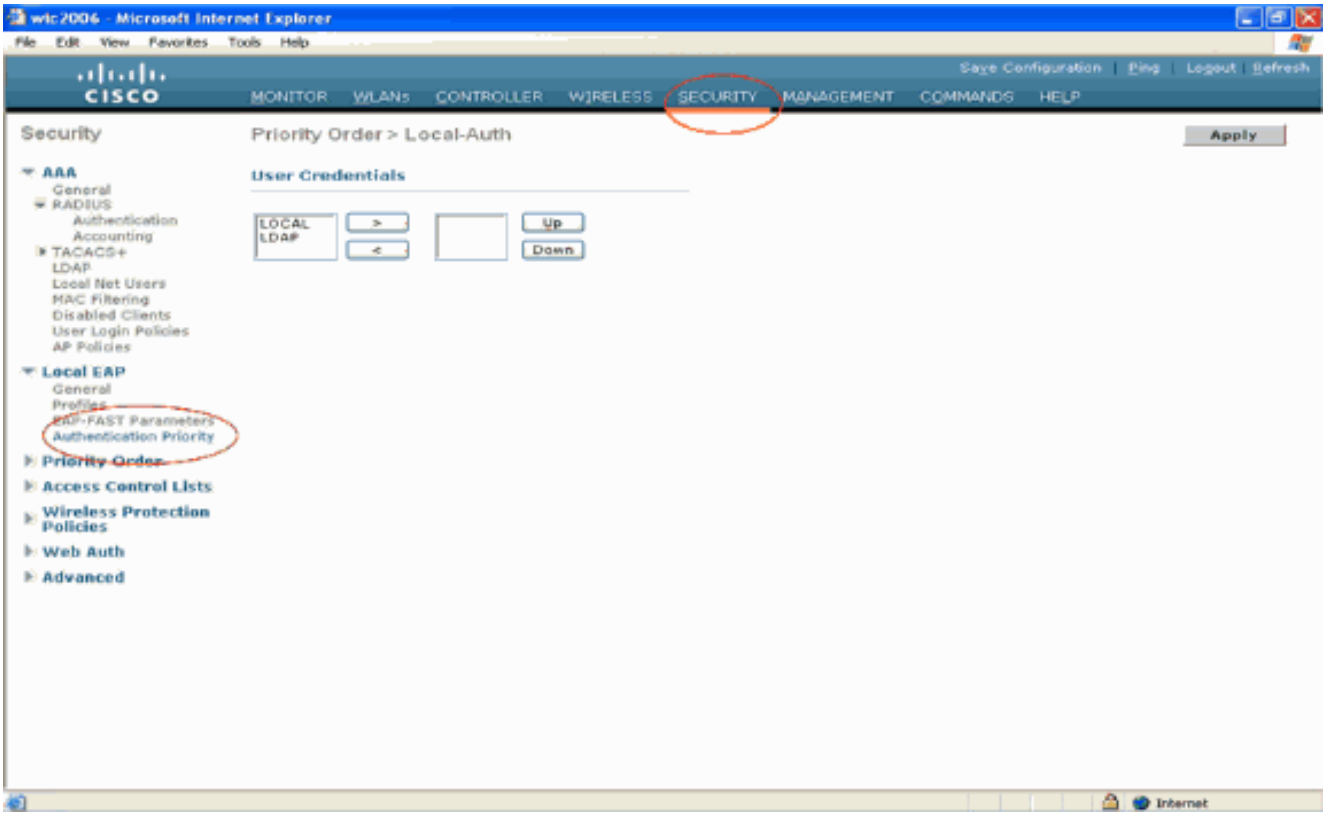


现在已经在 WLC 上配置了与 LDAP 服务器相关的详细信息，下一步是将 LDAP 配置为优先的后端数据库，使 WLC 先从 LDAP 数据库中查找用户凭证，而不是从其他任何数据库中进行查找。

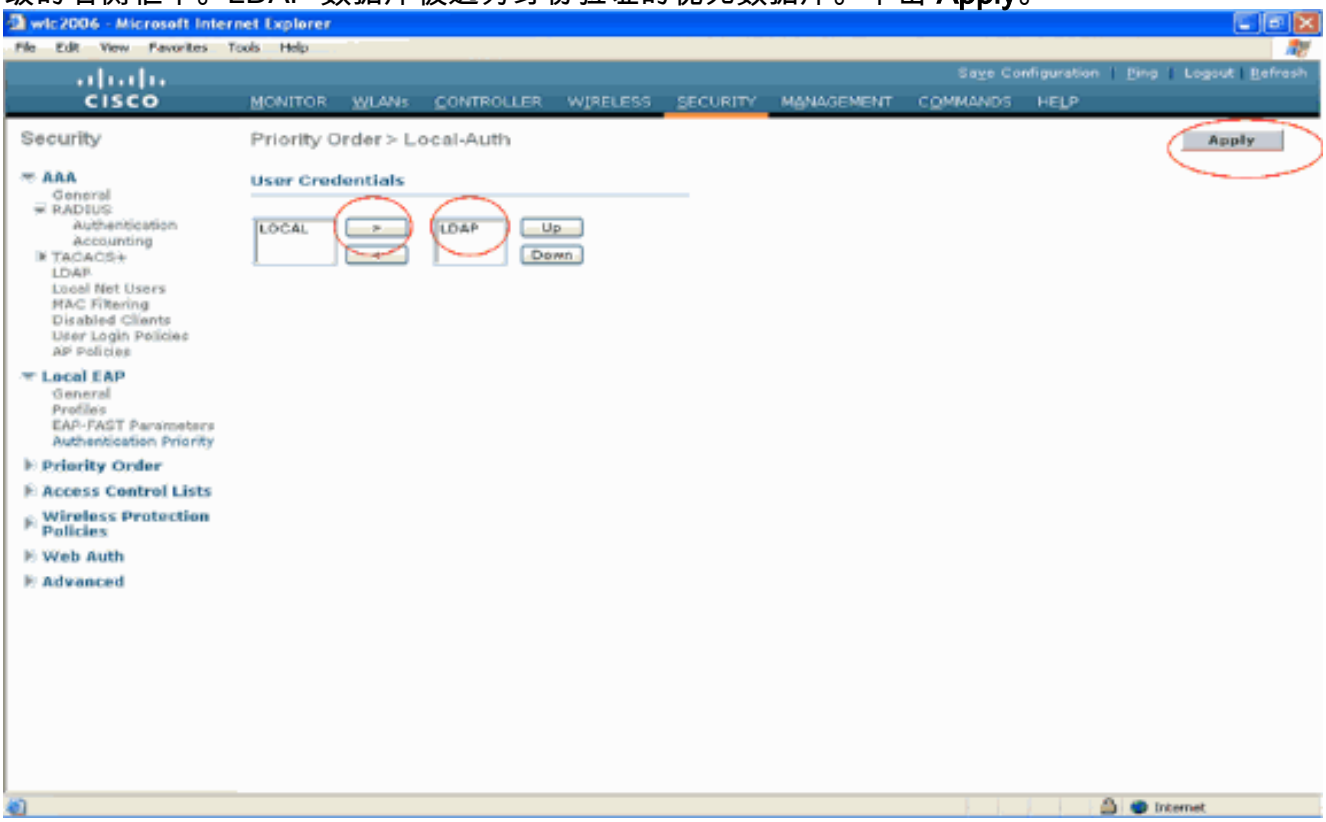
将 LDAP 配置为优先的后端数据库

要将 LDAP 配置为优先的后端数据库，请在 WLC 上完成以下步骤：

1. 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。**



2. 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**。

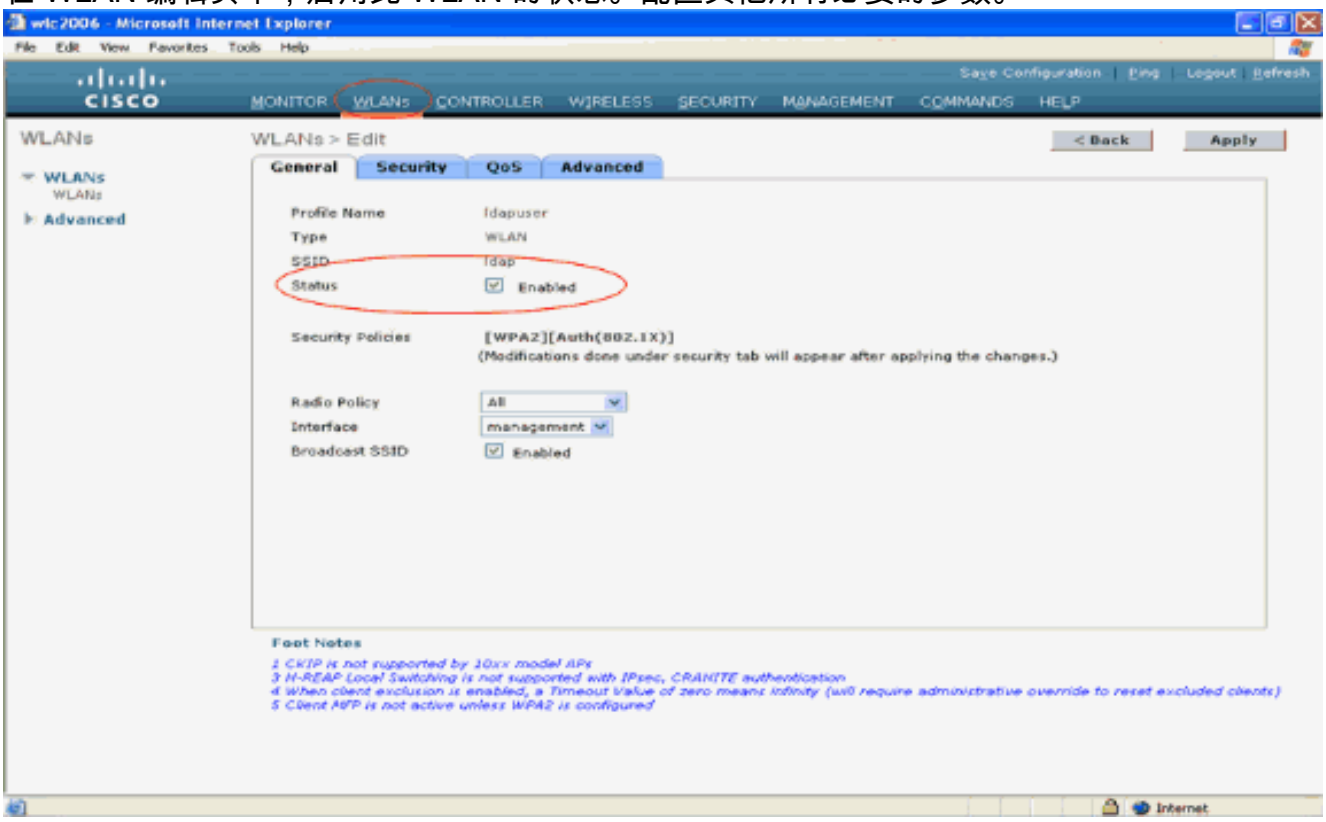


注意：如果LDAP和LOCAL都显示在正确的User Credentials框中，其中LDAP位于顶部，LOCAL位于底部，则Local EAP尝试使用LDAP后端数据库对客户端进行身份验证，并且如果LDAP服务器不可访问，则故障切换到本地用户数据库。如果未找到用户，则身份验证尝试被拒绝。如果 LOCAL 显示在上，则本地 EAP 仅尝试使用本地用户数据库进行身份验证。它不会故障转移到 LDAP 后端数据库。

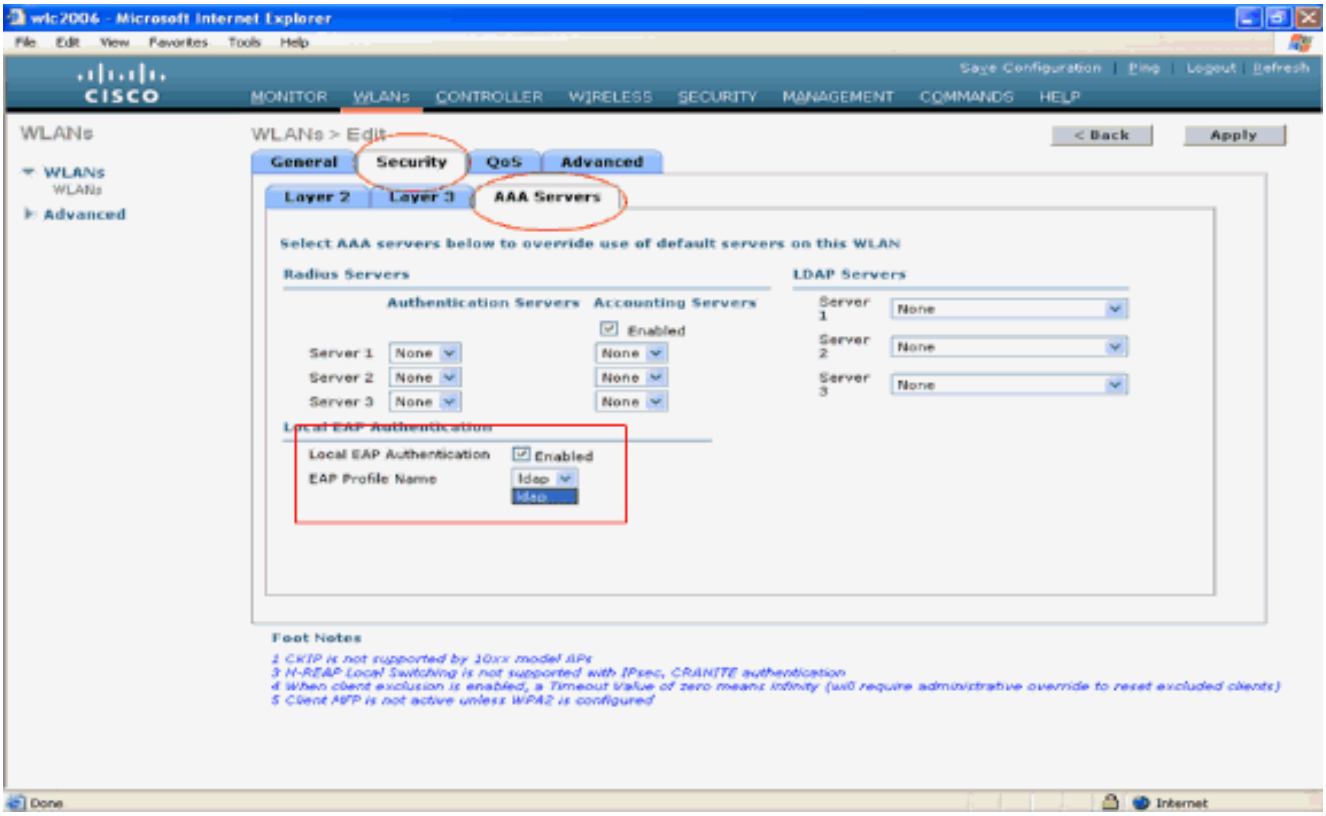
在 WLC 上将 WLAN 配置为使用本地 EAP 身份验证

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：

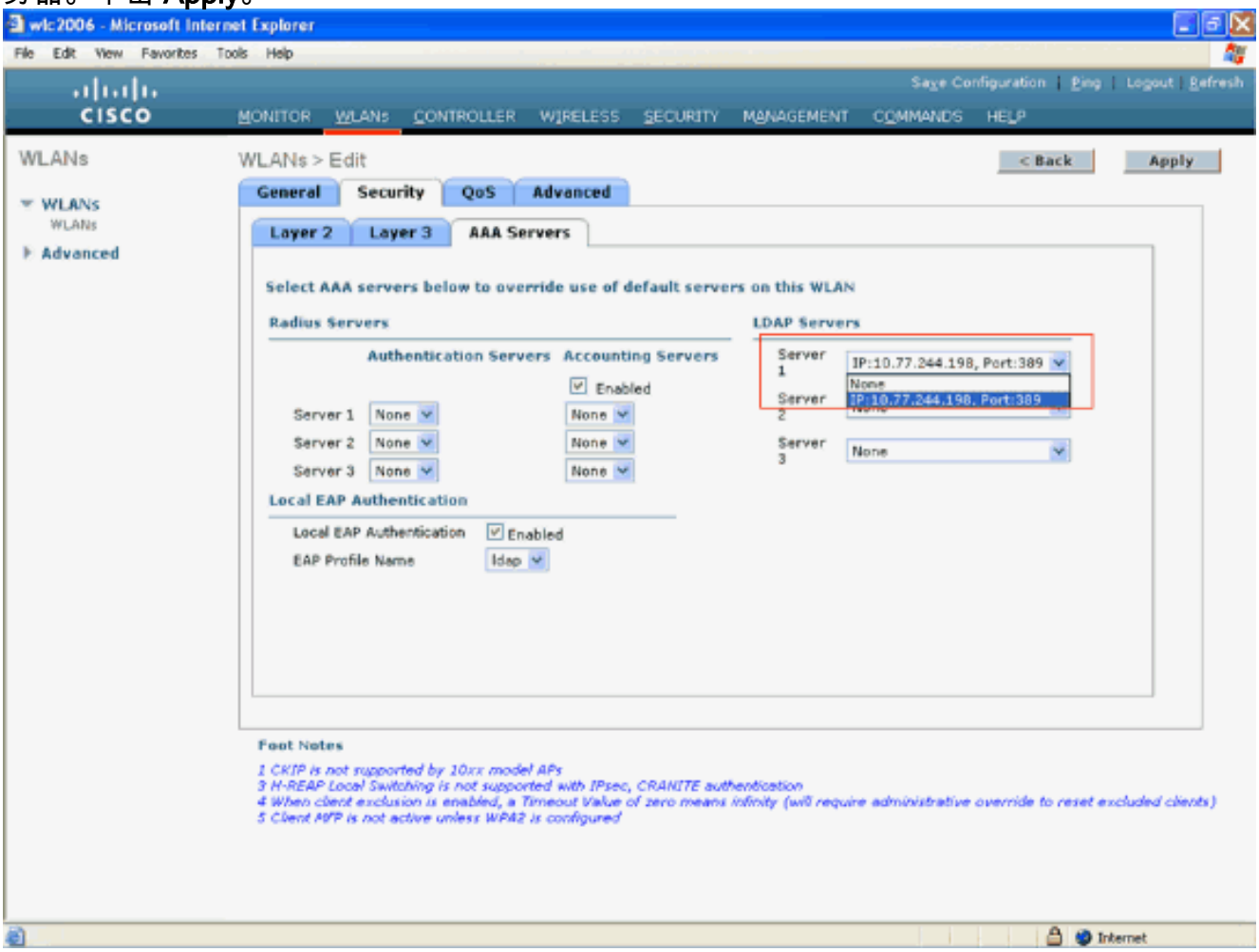
1. 从控制器的主菜单中，单击 **WLANs，以便转到 WLAN 配置页。**在 WLAN 页中，单击 **New，以便创建新的 WLAN。**本示例将创建新的 WLAN **ldap**。单击 **Apply。下一步是在“WLANs”>“Edit”页中配置 WLAN 参数。**
2. 在 WLAN 编辑页中，启用此 WLAN 的状态。配置其他所有必要的参数。



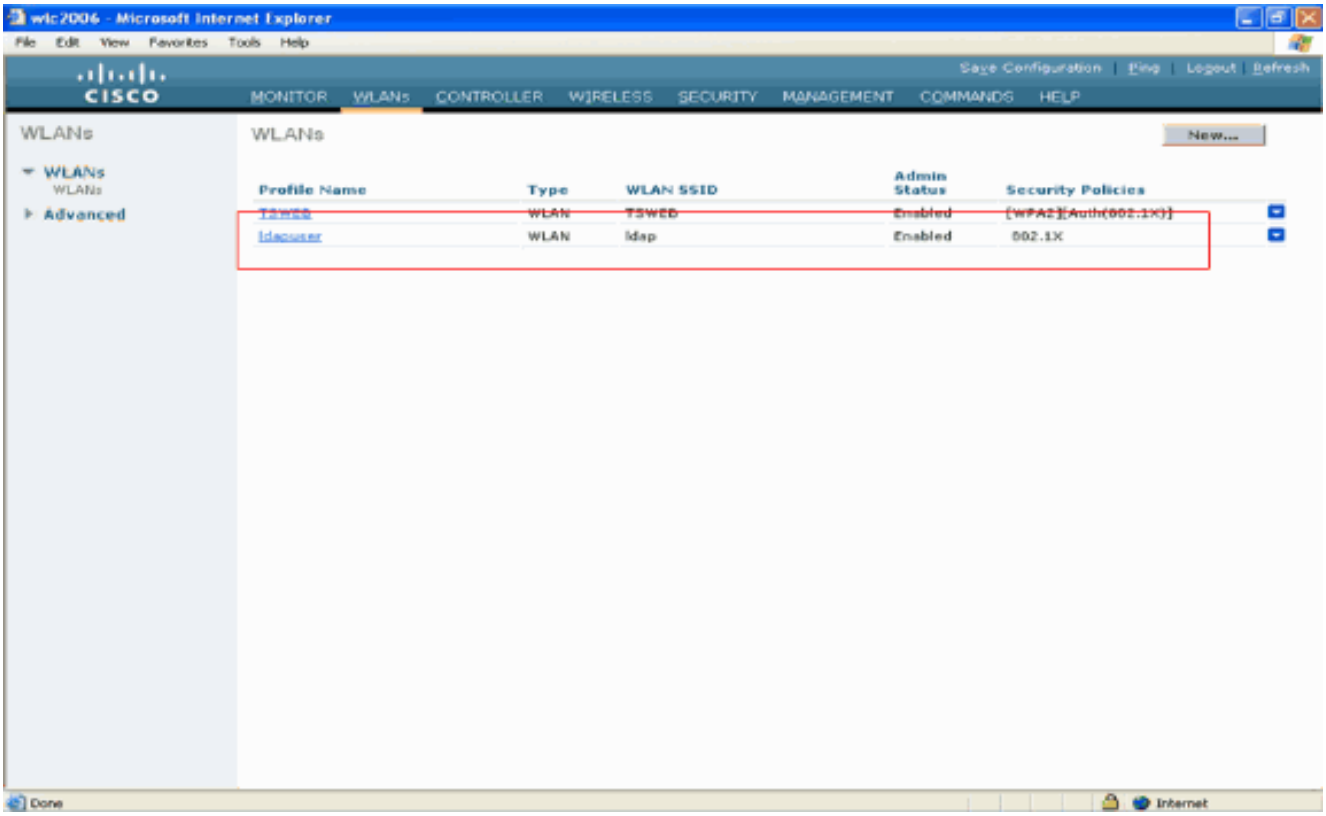
3. 单击 **Security，以便为此 WLAN 配置与安全性相关的参数。**本示例使用带有 104 位动态 WEP 的 802.1x 作为第 2 层安全性。**注意：**本文档使用带有动态WEP的802.1x作为示例。建议使用更加安全的身份验证方法，例如 WPA/WPA2。
4. 在“WLAN Security configuration”页中，单击 AAA servers 选项卡。在“AAA servers”页中，启用本地 EAP 身份验证方法，并从对应于“EAP Profile Name”参数的下拉框中选择 **ldap。**这是本示例中创建的本地 EAP 配置文件。



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**。



6. WLC 上已经配置了新的 WLAN **ldap**。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。



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

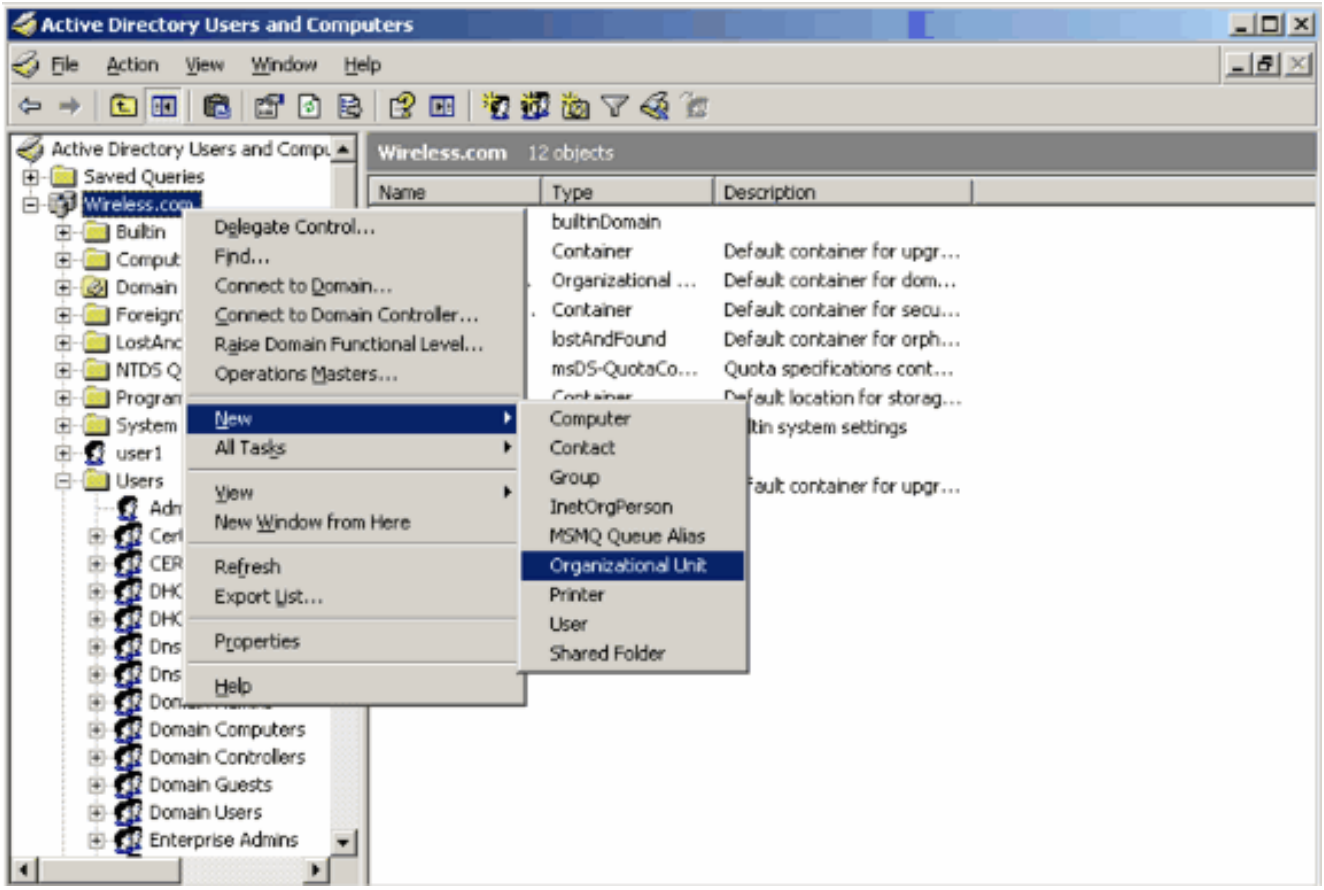
在本示例中，将创建一个新的 OU **ldapuser，并在此 OU 下创建用户 user2。**通过配置此用户进行 LDAP 访问，WLC 可以查询此 LDAP 数据库以便进行用户身份验证。

本示例中使用的域是 **wireless.com**。

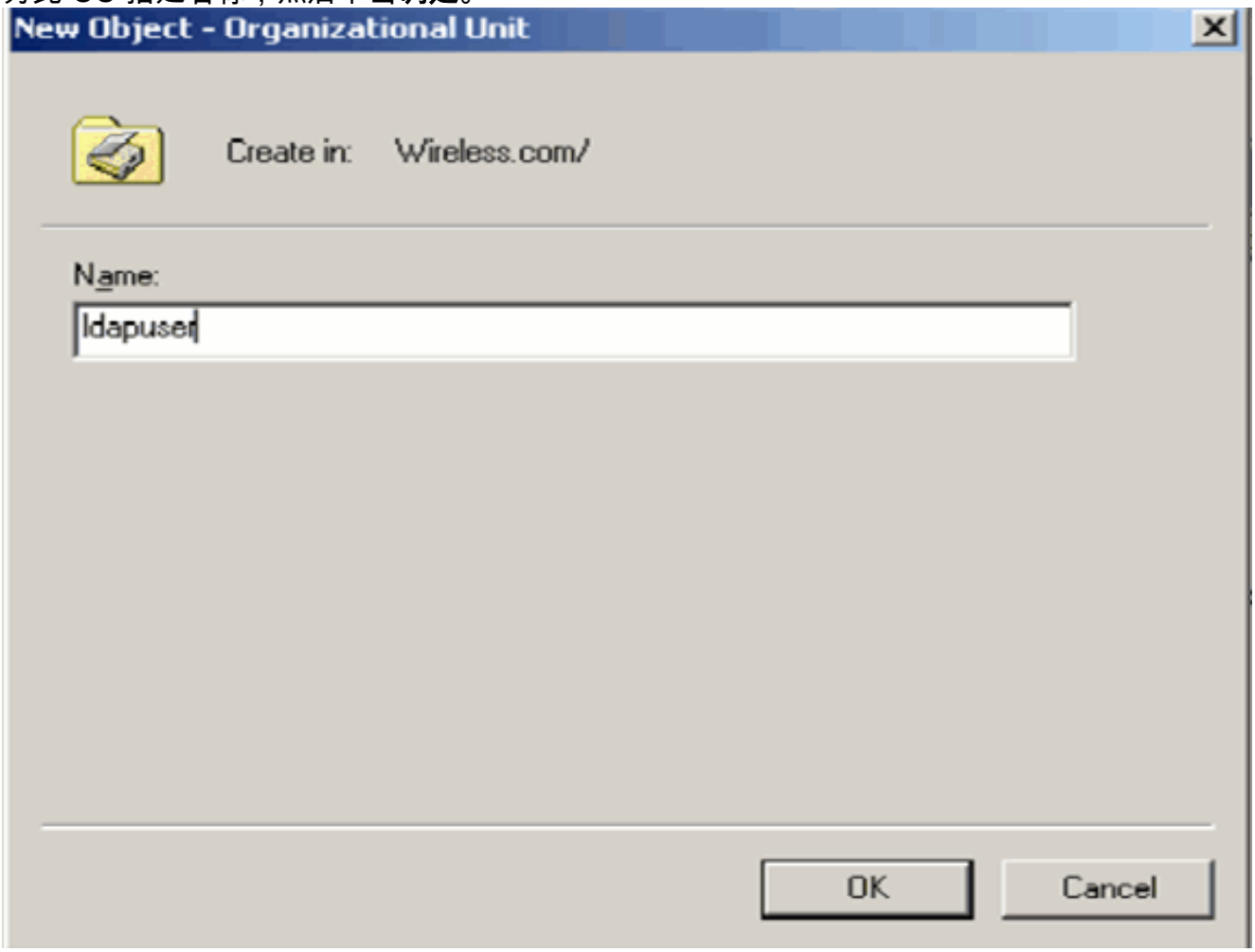
在 OU 下创建用户数据库

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。**
2. 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。**

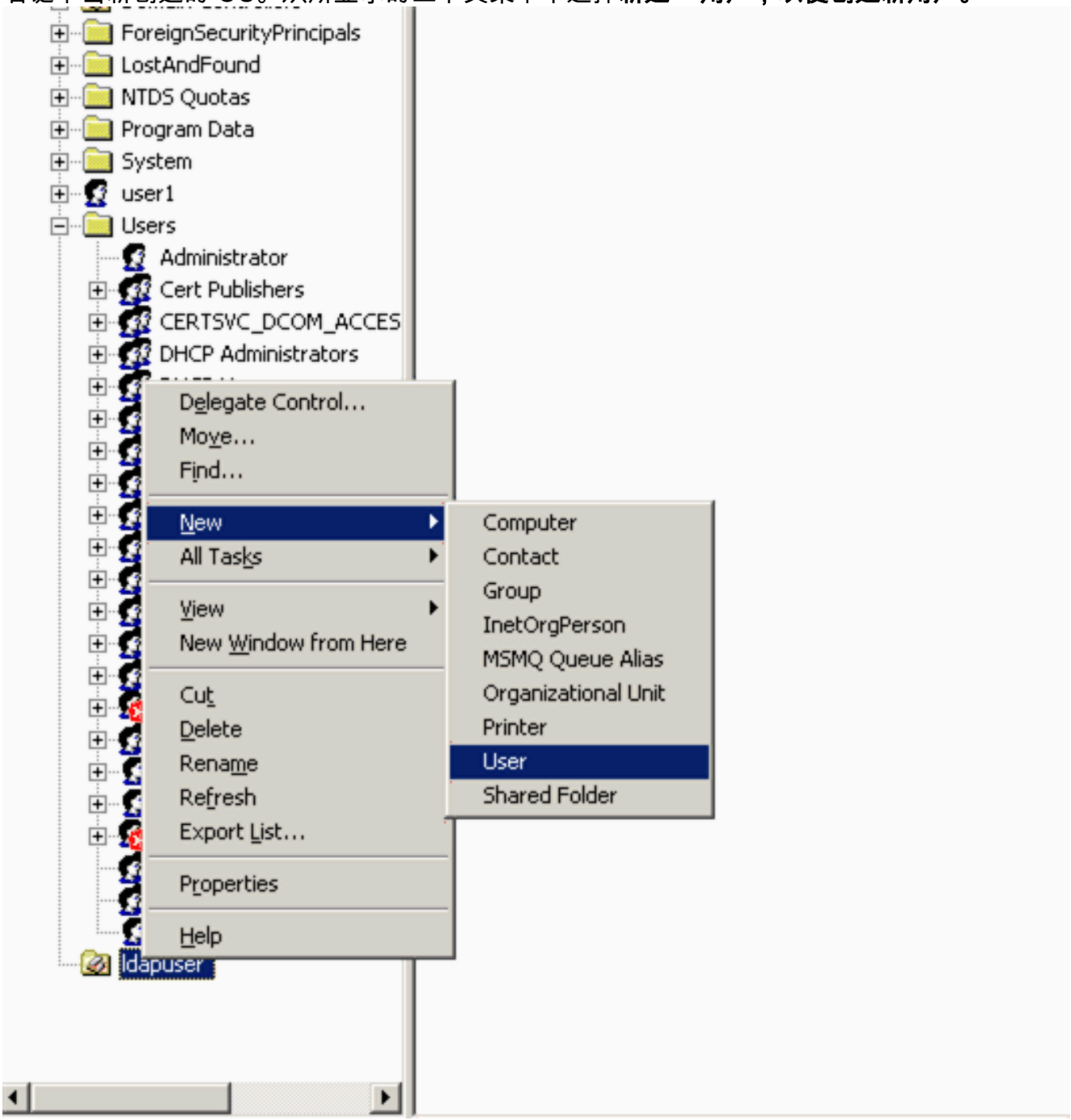


3. 为此 OU 指定名称，然后单击**确定**。

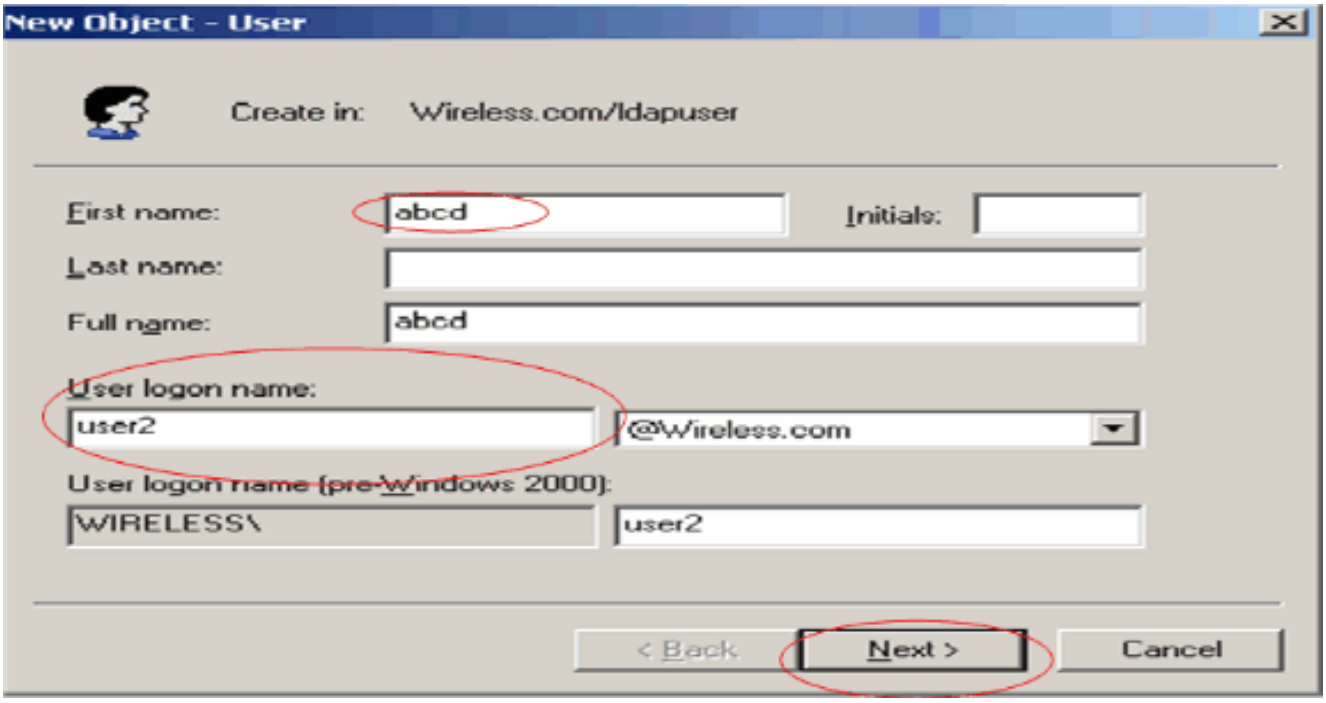


现在已经在 LDAP 服务器上创建了新的 OU **ldapuser，下一步是在此 OU 下创建用户 user2。**为此，请完成以下步骤：

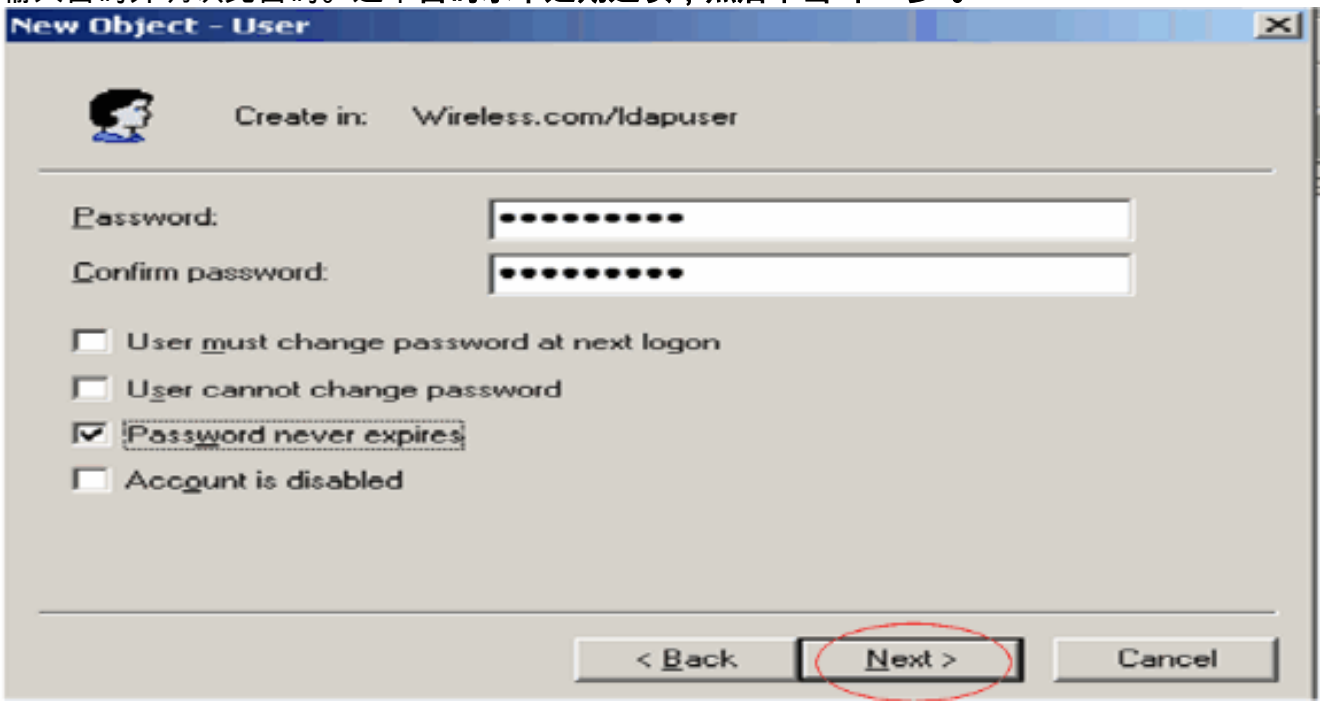
1. 右键单击新创建的 OU。从所显示的上下文菜单中选择**新建 > 用户，以便创建新用户。**



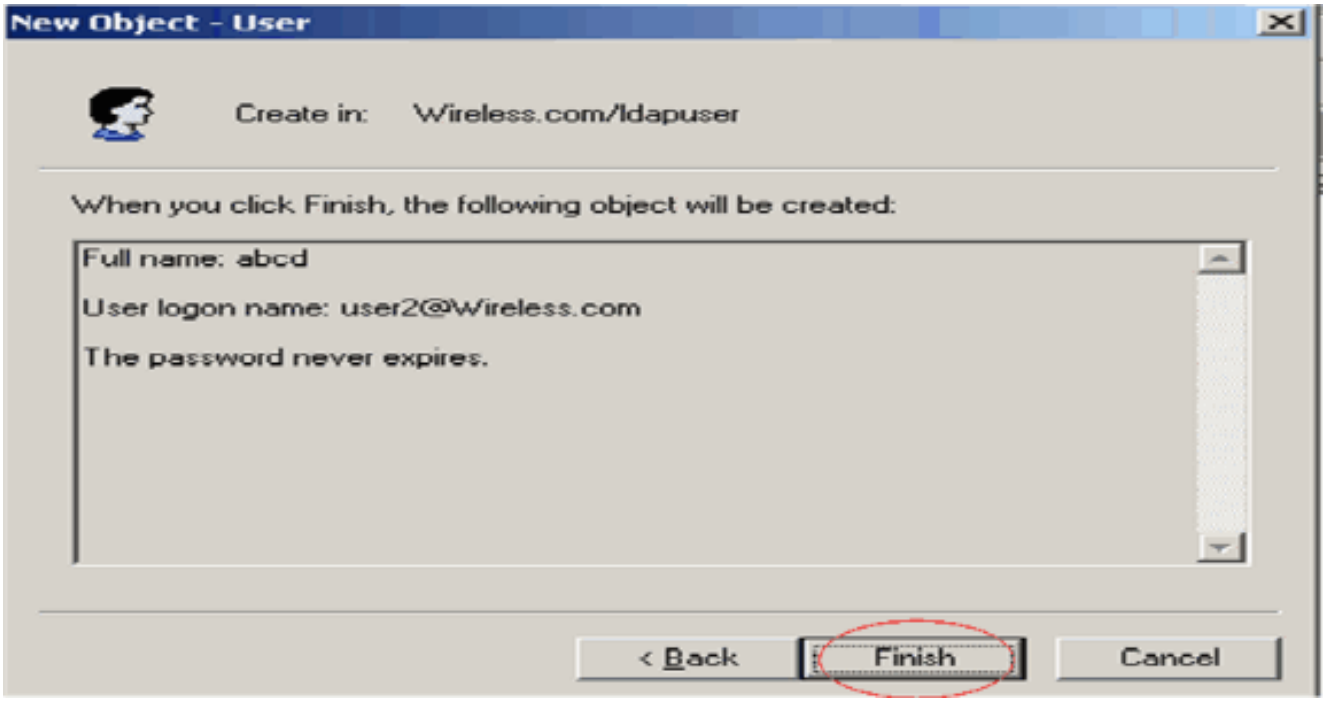
2. 在“用户设置”页中，填写必要的字段，如本示例所示。本示例使用 **user2 作为用户的登录名。**这是在 LDAP 数据库中对客户端进行身份验证时所验证的用户名。本示例使用 **abcd 作为名字和姓氏。**单击 **Next**。



3. 输入密码并确认此密码。选中**密码永不过期选项，然后单击"下一步"。**



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**



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。

为 LDAP 访问配置用户

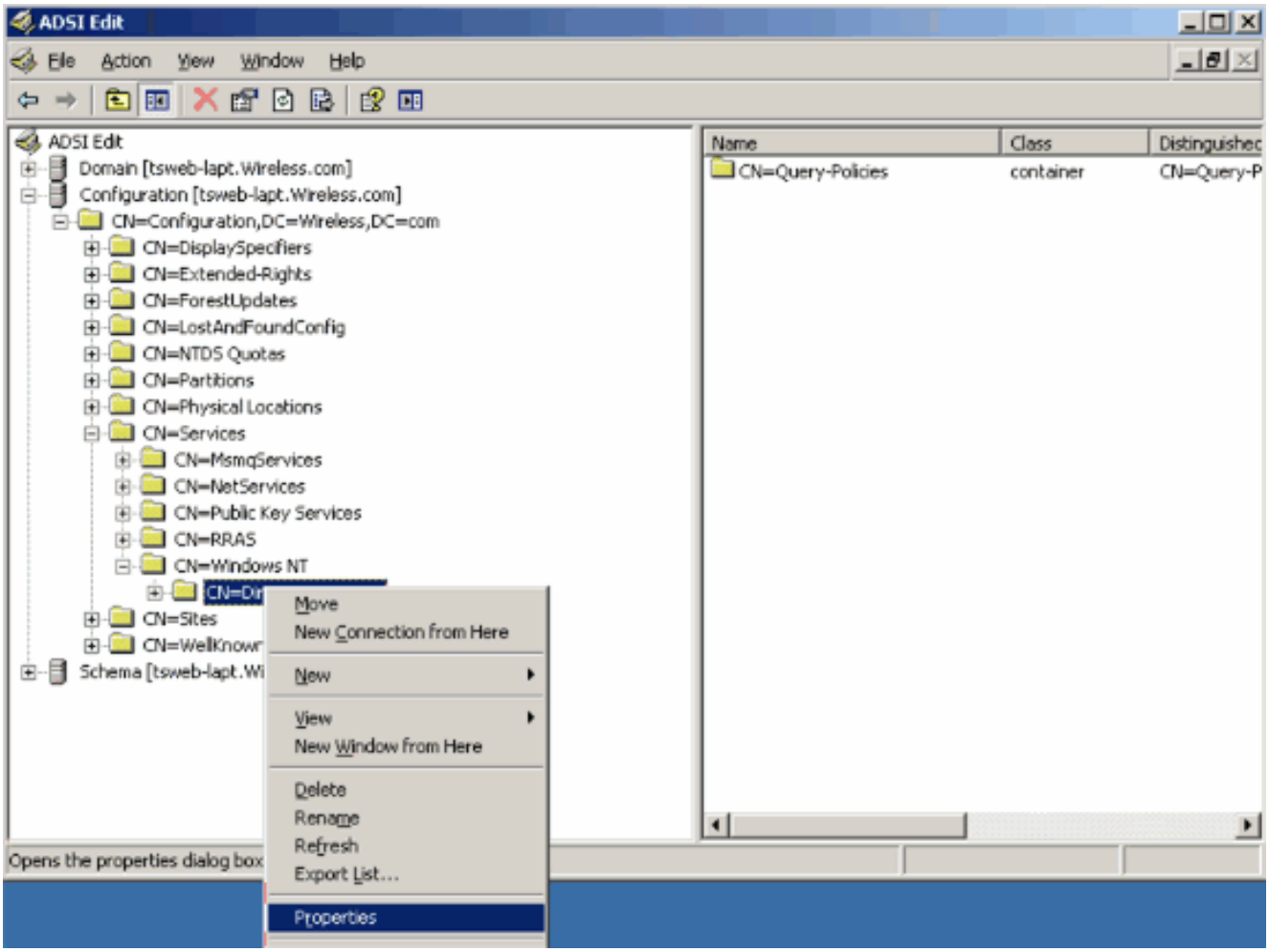
要配置用户进行 LDAP 访问，请执行本部分中的步骤：

在 Windows 2003 Server 上启用匿名绑定功能

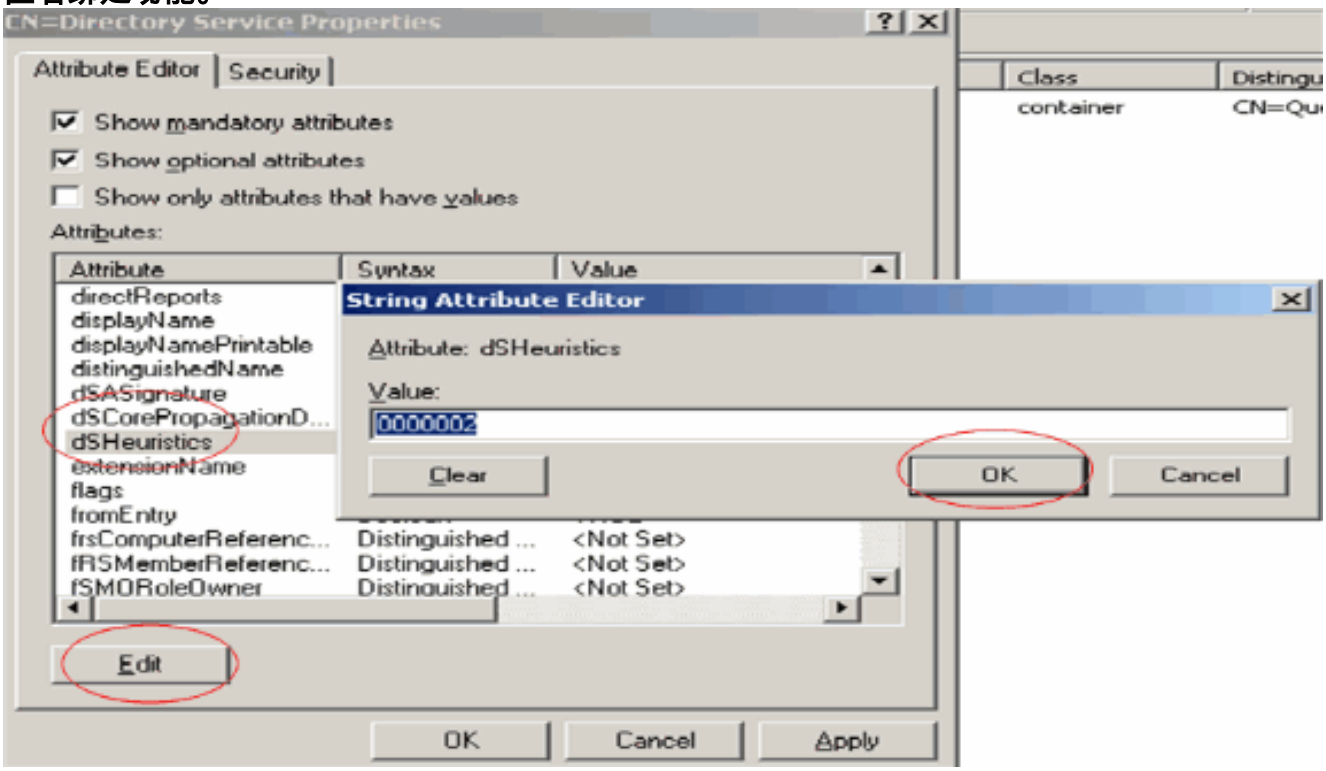
为了使所有第三方应用程序都能够访问 LDAP 上的 Windows 2003 AD，应该在 Windows 2003 上启用匿名绑定功能。默认情况下，Windows 2003 域控制器上不允许执行匿名 LDAP 操作。

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。
2. 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。**



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”，即可启用匿名绑定功能。**



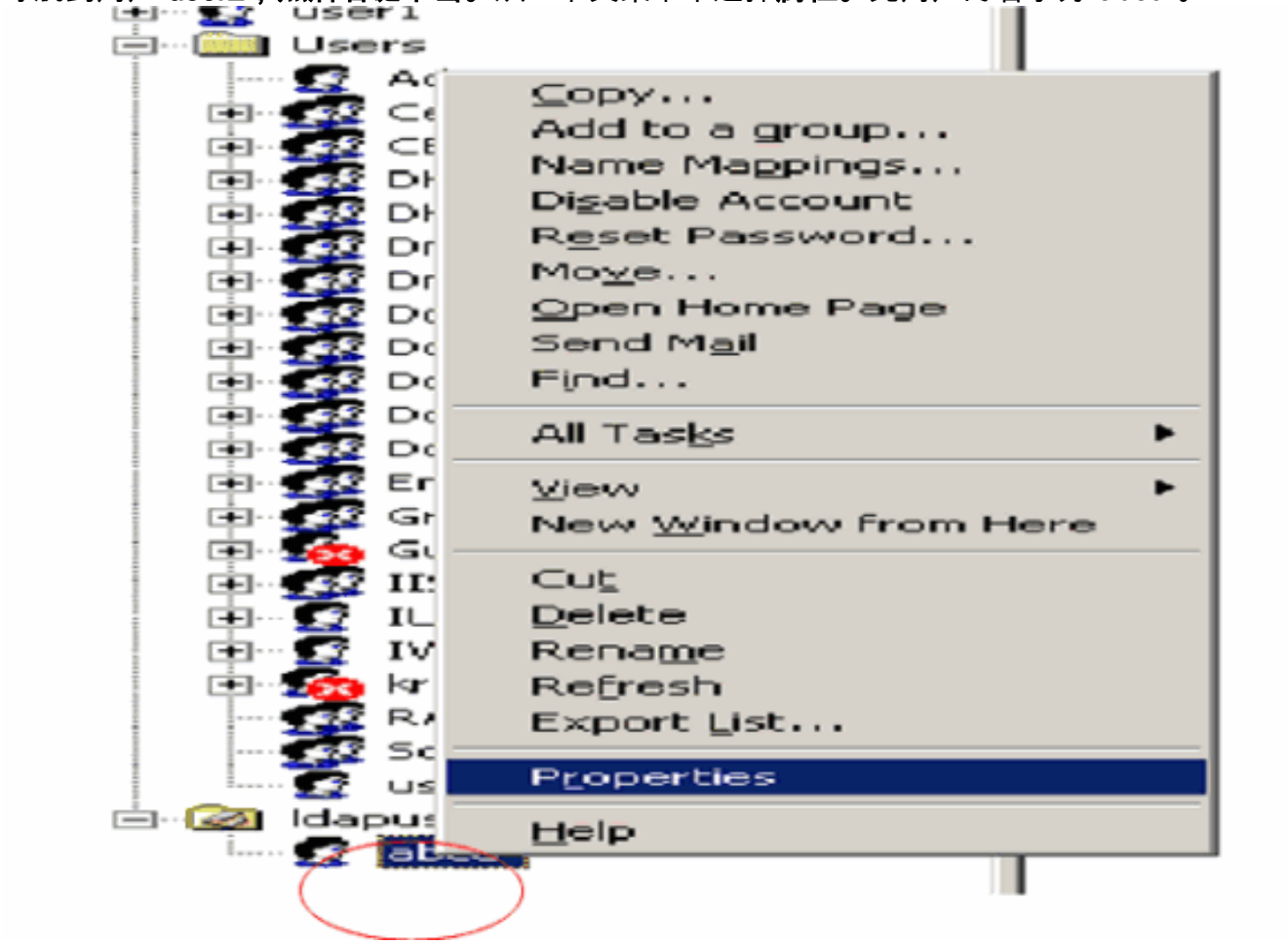
注意：如果此属性已经包含值，请确保仅更改左侧的第七个字符。这是在启用匿名捆绑时唯一需要更改的字符。例如，如果当前值是“0010000”，则您需要将其改为“0010002”。如果当前值

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

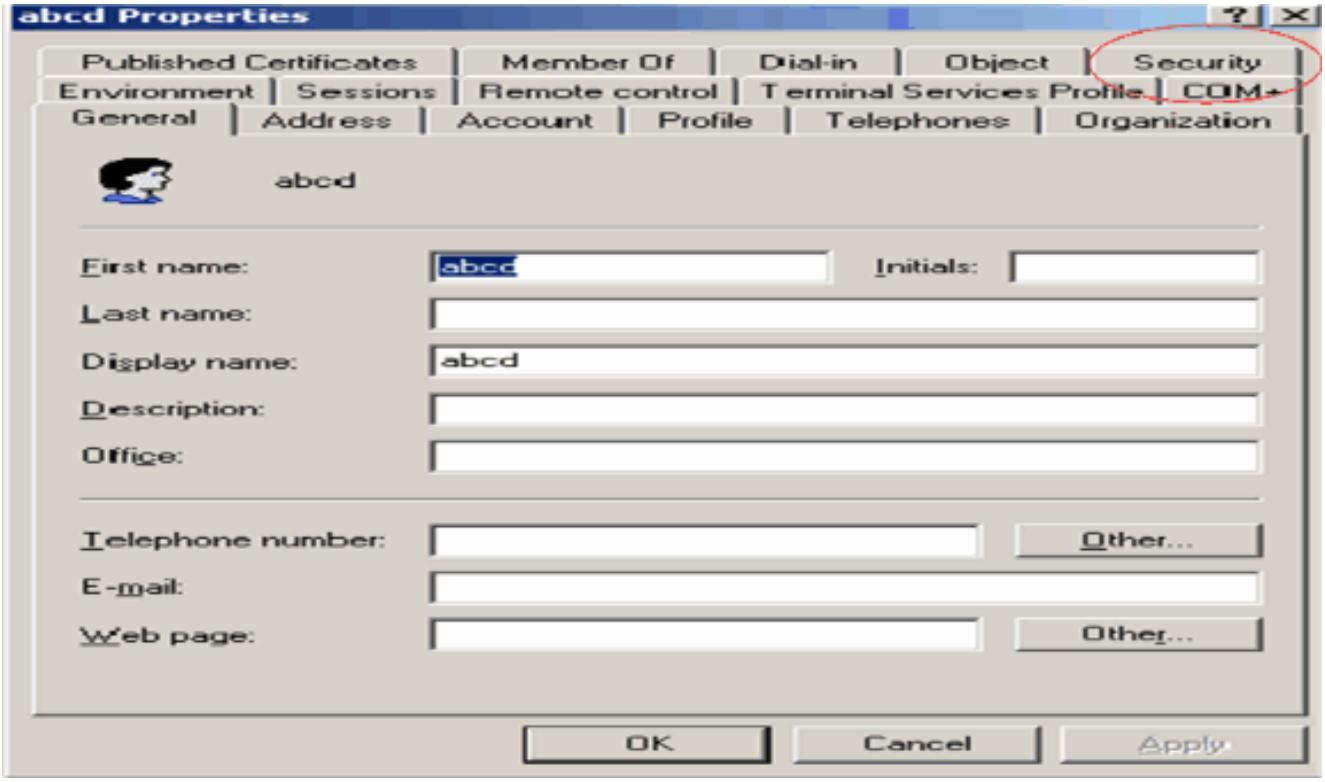
向用户“user2”授予“匿名登录”访问权限

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：

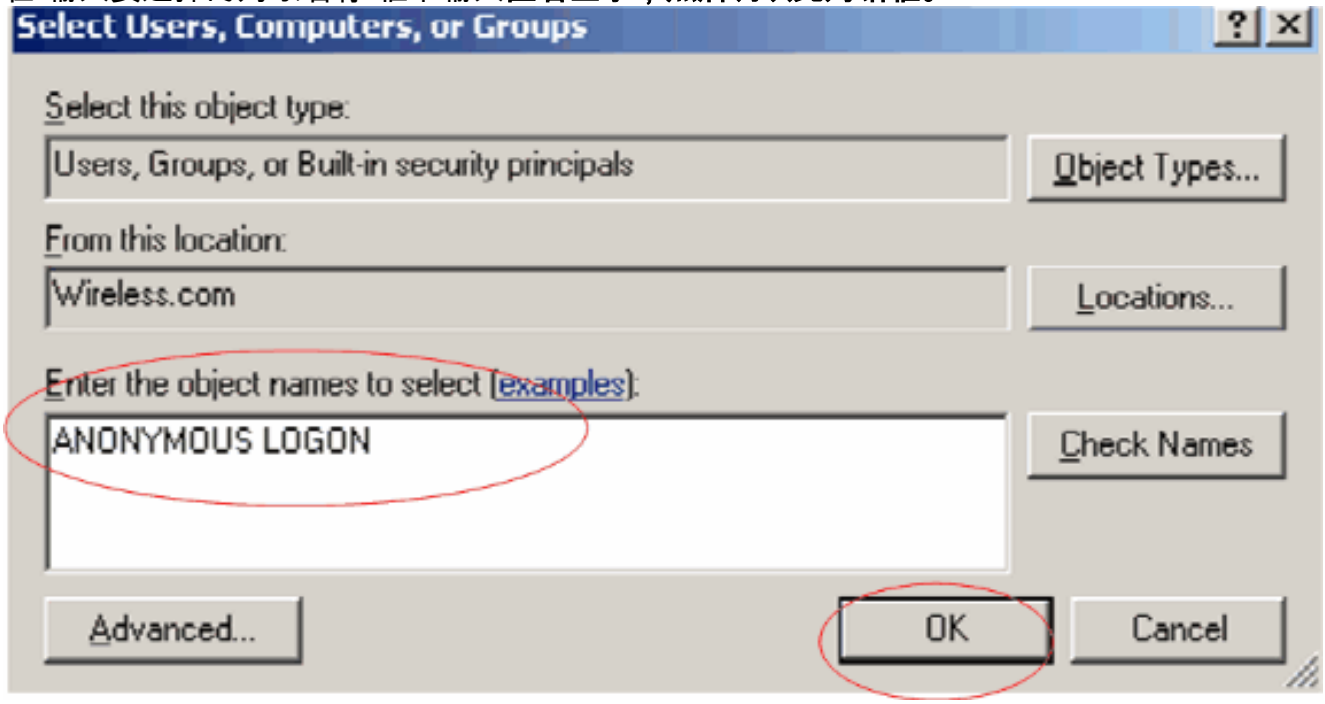
1. 打开 **Active Directory 用户和计算机。**
2. 确保选中**查看高级功能。**
3. 导航到用户 **user2，然后右键单击。**从上下文菜单中选择**属性。**此用户的名字为“abcd”。



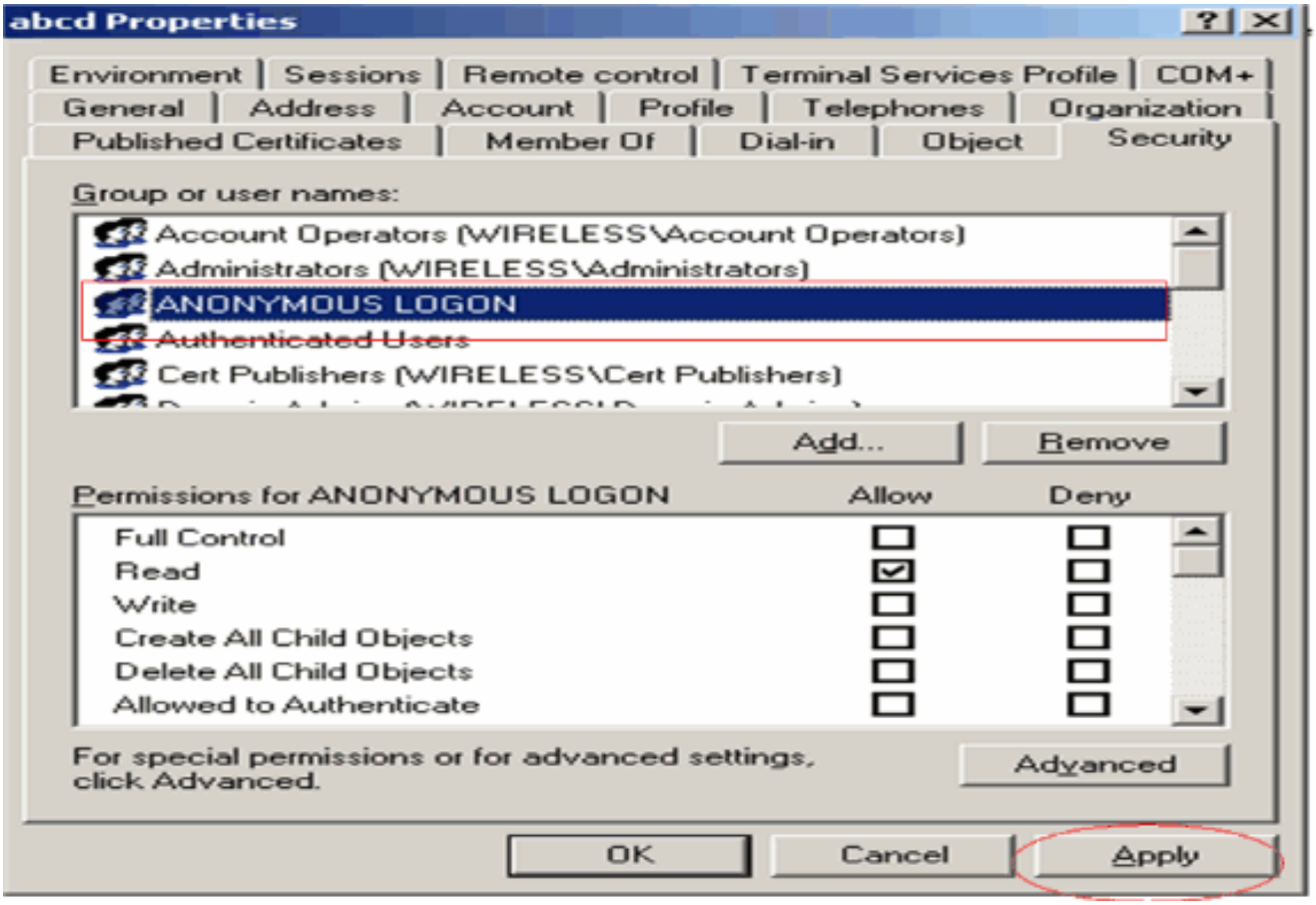
4. 在“abcd 属性”窗口中转到**安全性。**



5. 在所显示的窗口中单击**添加。**
6. 在“输入要选择的对象名称”框下输入**匿名登录，然后确认此对话框。**



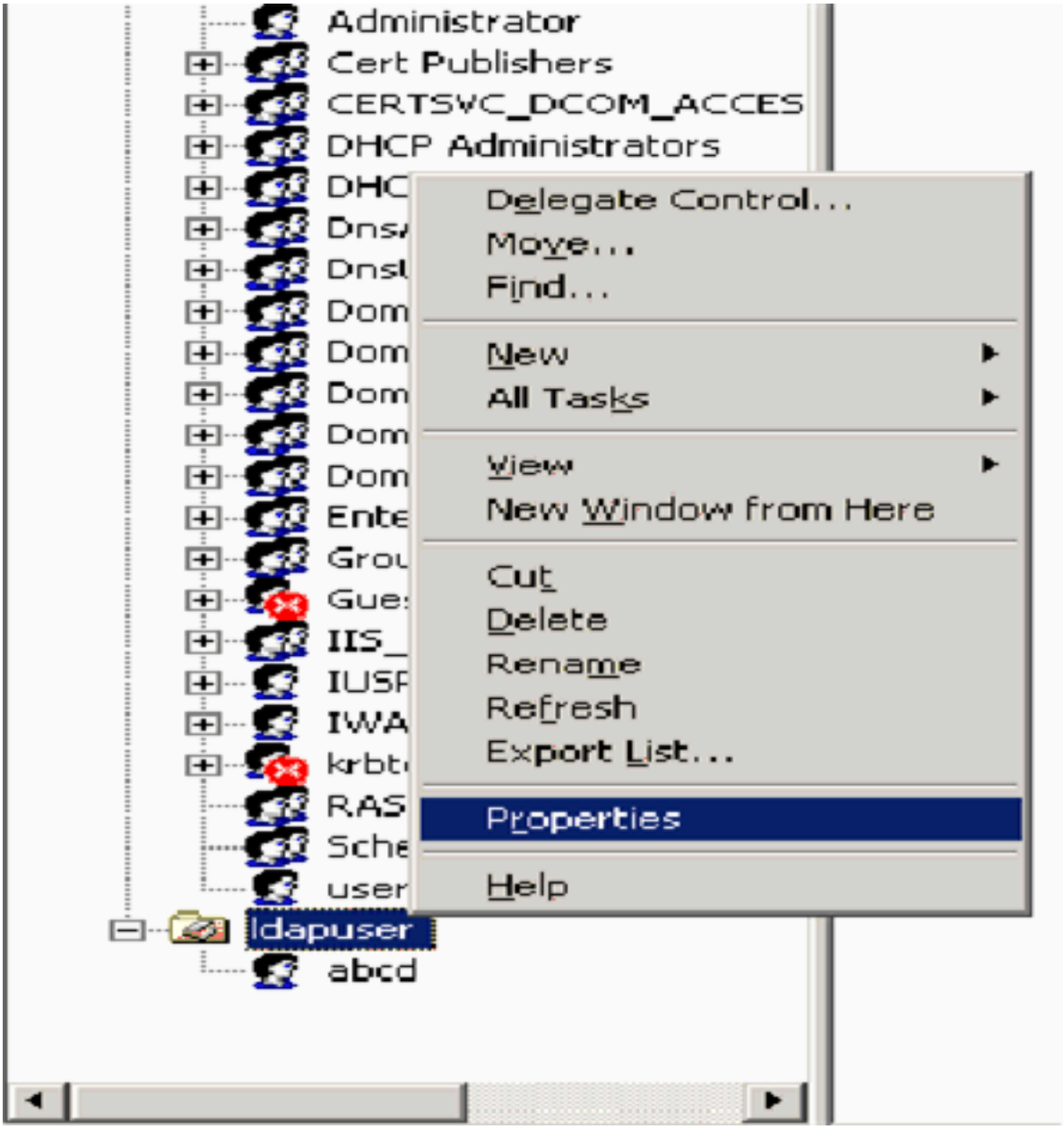
7. 在 ACL 中，您将看到**匿名登录可以访问用户的一些属性集。**Click **OK**.已经向此用户授予“匿名登录”访问权限。



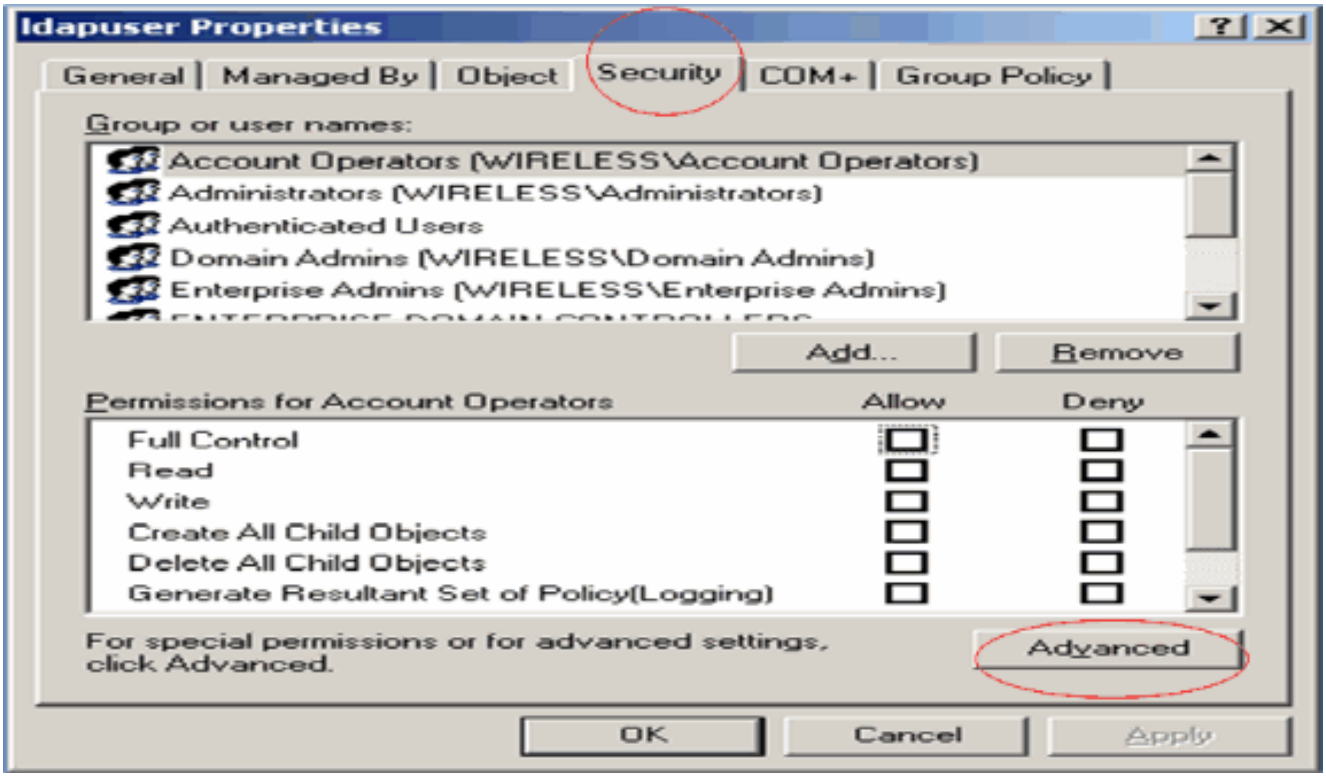
在 OU 上授予“列出内容”权限

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“ldapuser”上。为此，请完成以下步骤：

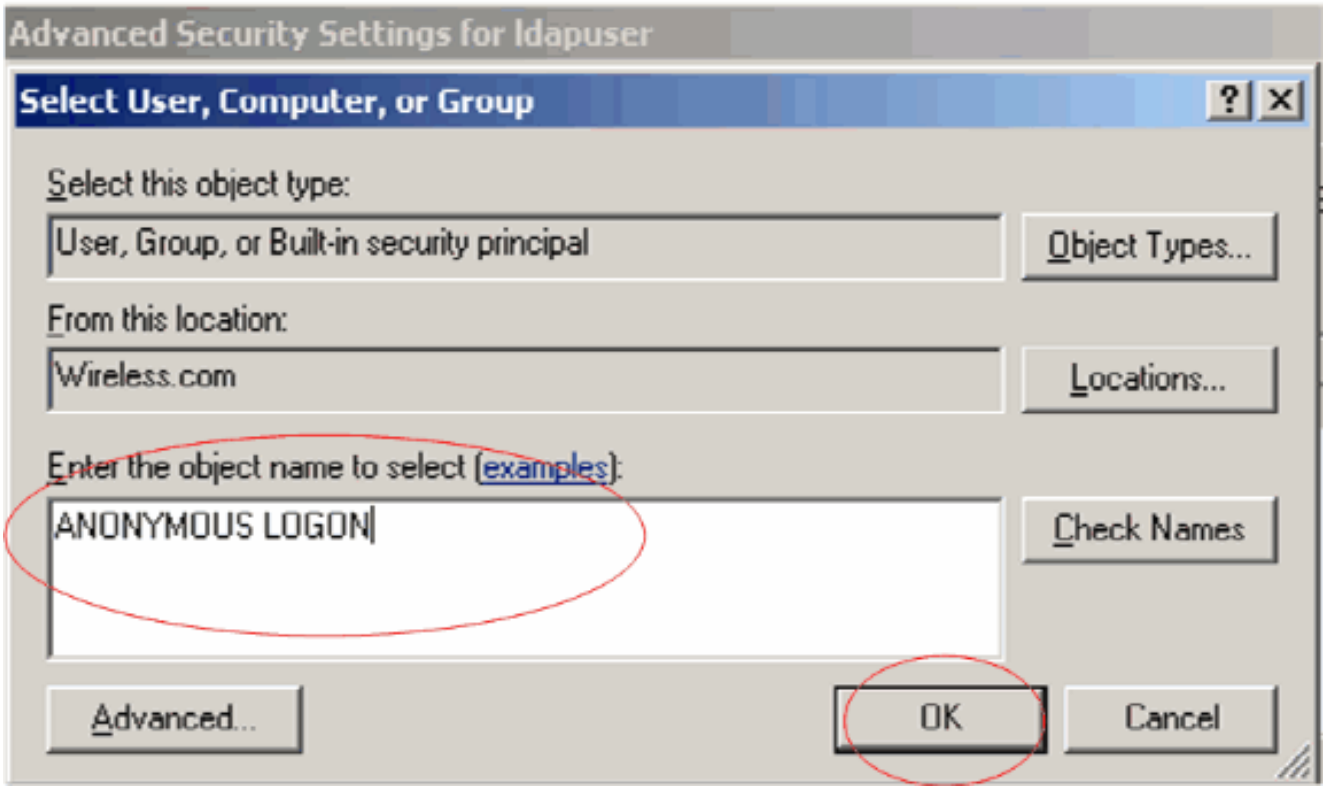
1. 在 Active Directory 用户和计算机中，右键单击 OU **ldapuser 并选择“属性”。**



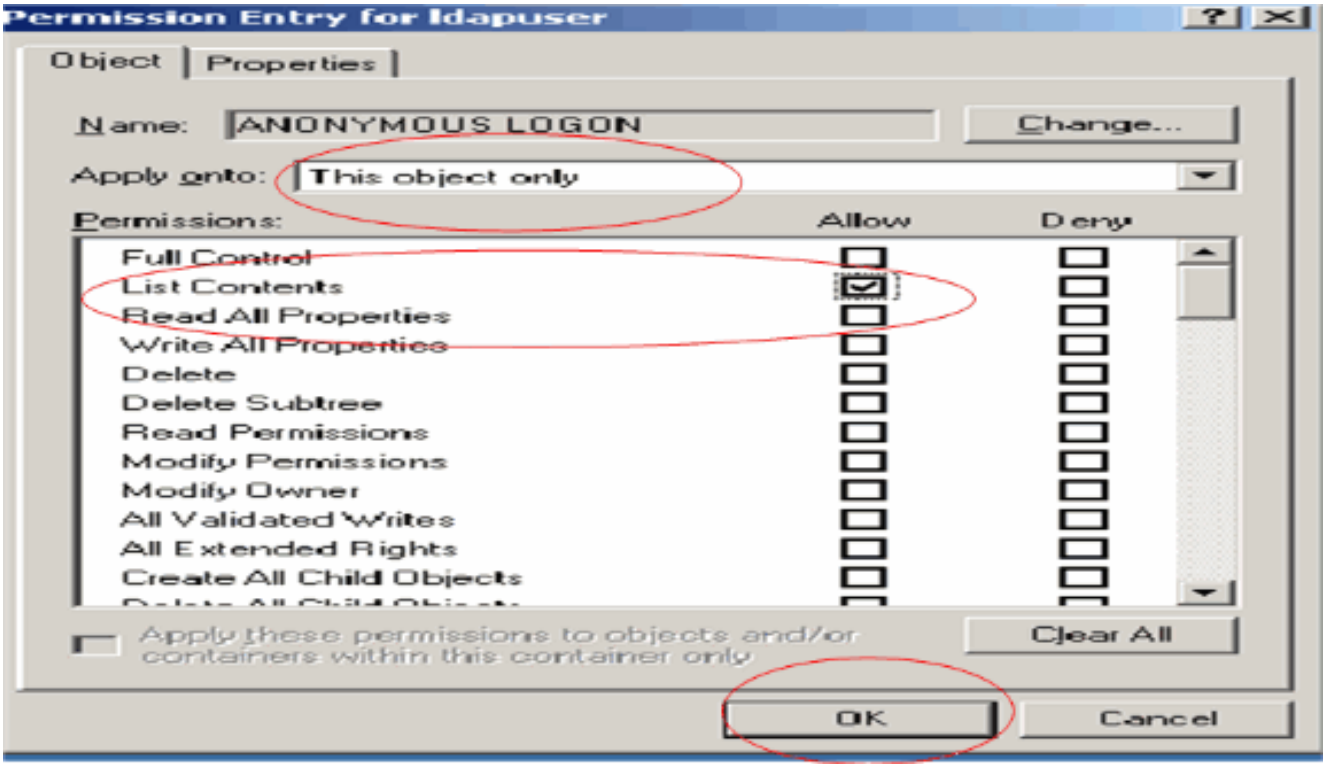
2. 单击**安全性，然后单击“高级”。**



3. 单击 Add。在打开的对话框中，输入**匿名登录**。



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。**

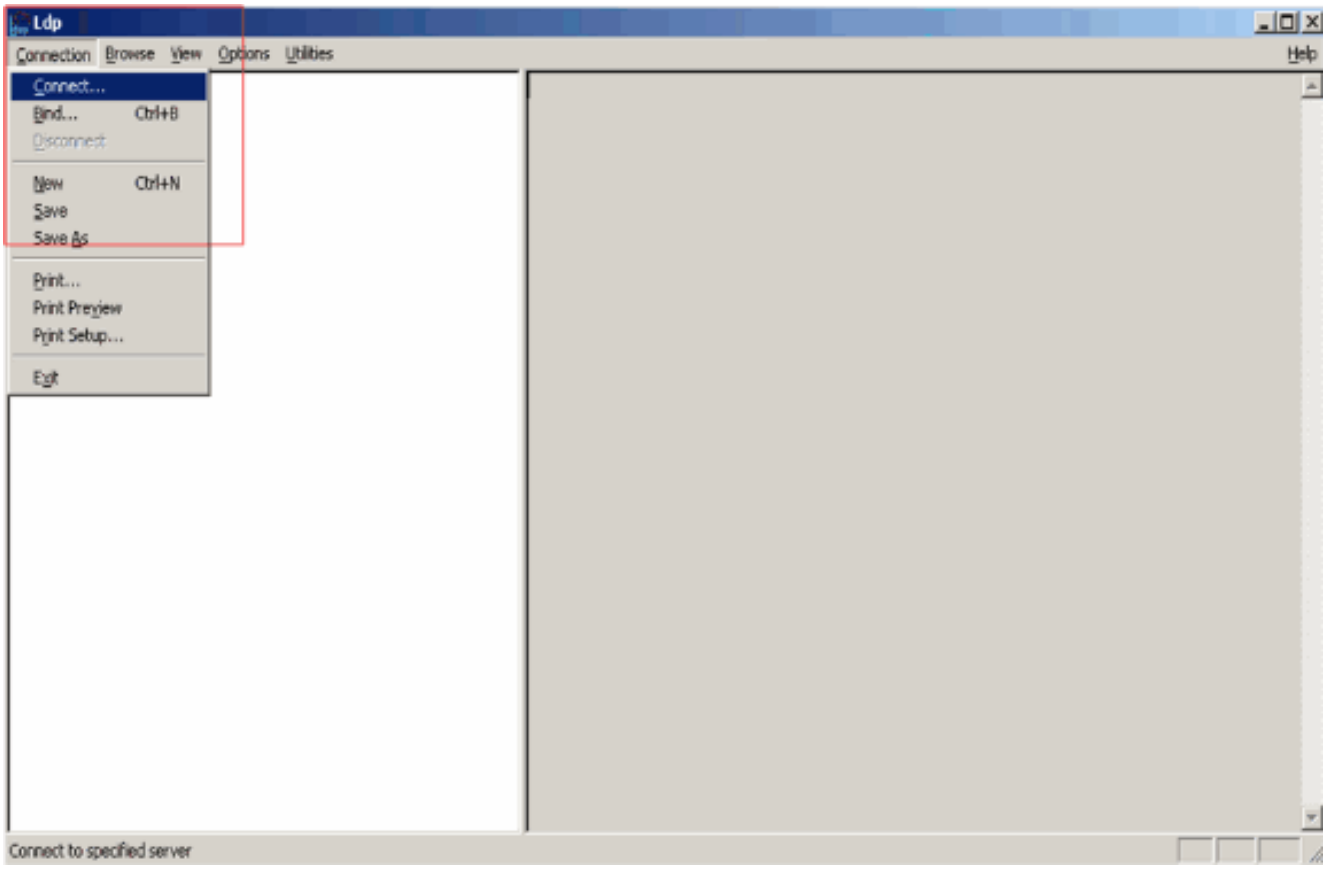


使用 LDP 来标识用户属性

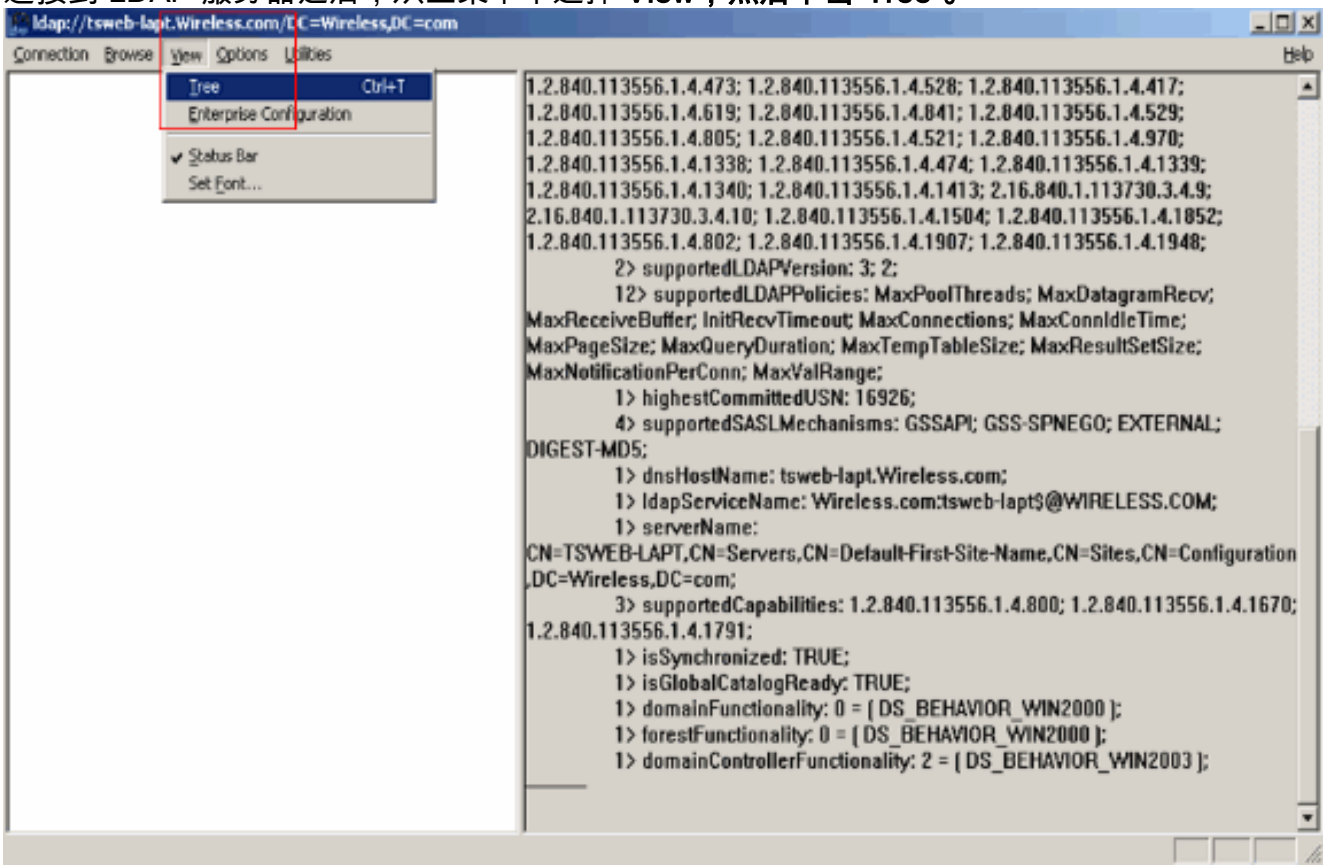
此 GUI 工具是一个 LDAP 客户端，它允许用户对任何 LDAP 兼容目录（例如 Active Directory）执行操作（例如连接、绑定、搜索、修改、添加、删除）。LDP 用于查看 Active Directory 中存储的对象及其元数据，例如安全描述符和复制元数据。

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。

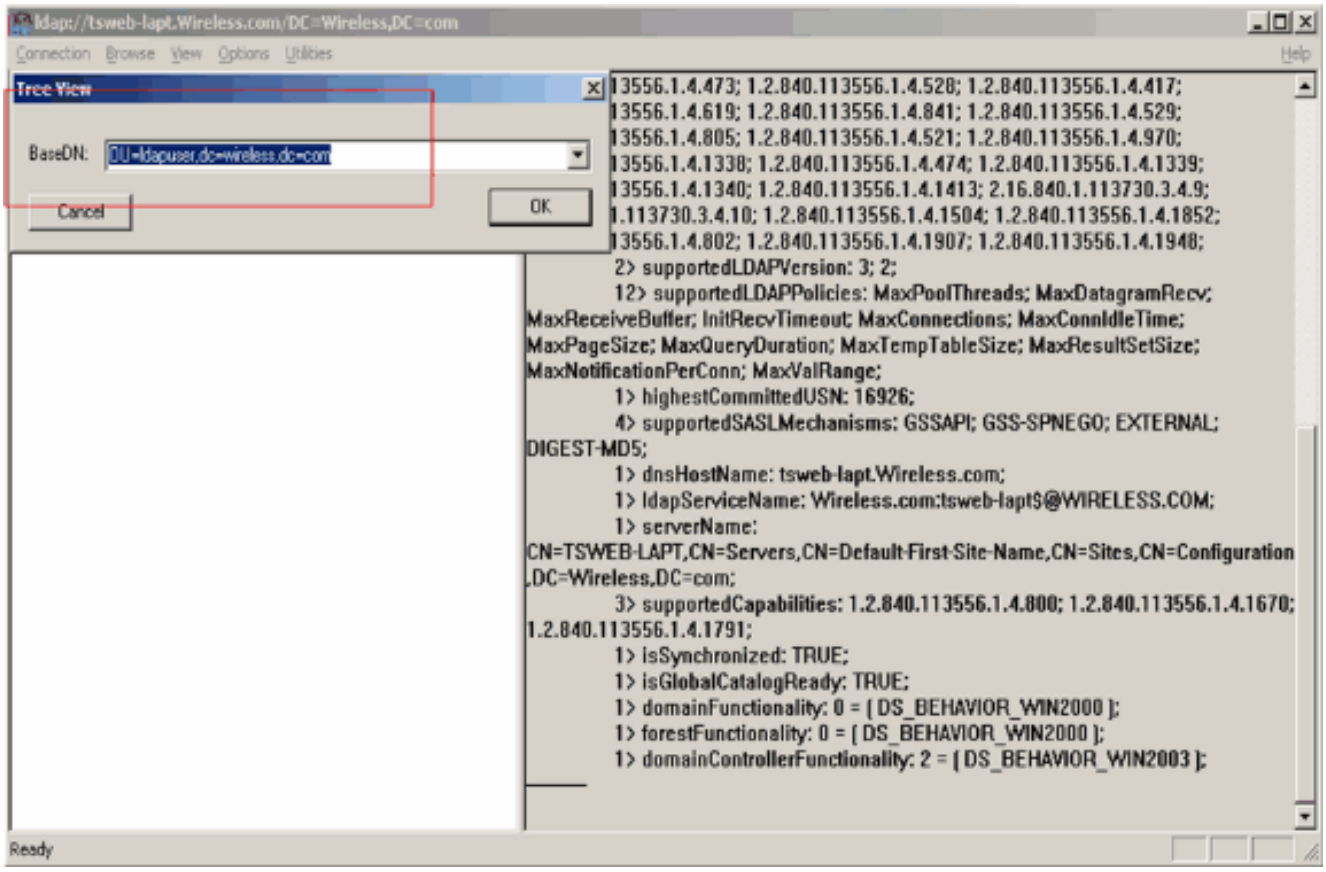
1. 在 Windows 2003 Server 上（即使在相同的 LDAP 服务器上），单击**开始 > 运行，然后输入 LDP 以便访问 LDP 浏览器。**
2. 在 LDP 主窗口中，单击 **Connection > Connect，然后通过输入 LDAP 服务器的 IP 地址连接到该 LDAP 服务器。**



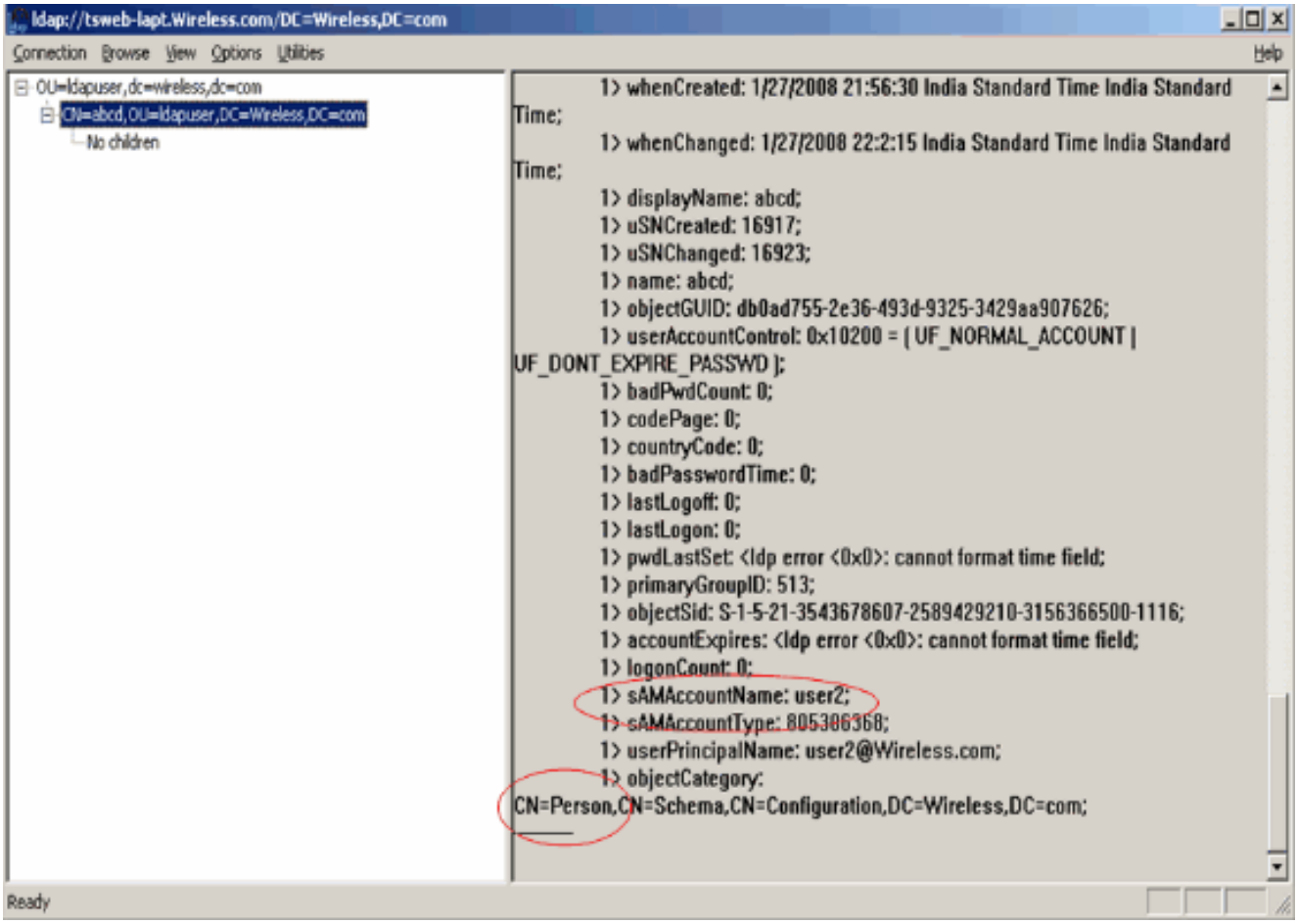
3. 连接到 LDAP 服务器之后，从主菜单中选择 **View，然后单击“Tree”。**



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 "ldapuser" 下，而后者又位于域 Wireless.com 下。**因此，用户 **user2 的 BaseDN 是“OU=ldapuser, dc=wireless, dc=com”。**Click **OK**.



5. LDP 浏览器的左侧显示指定 BaseDN (**OU=ldapuser, 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
：



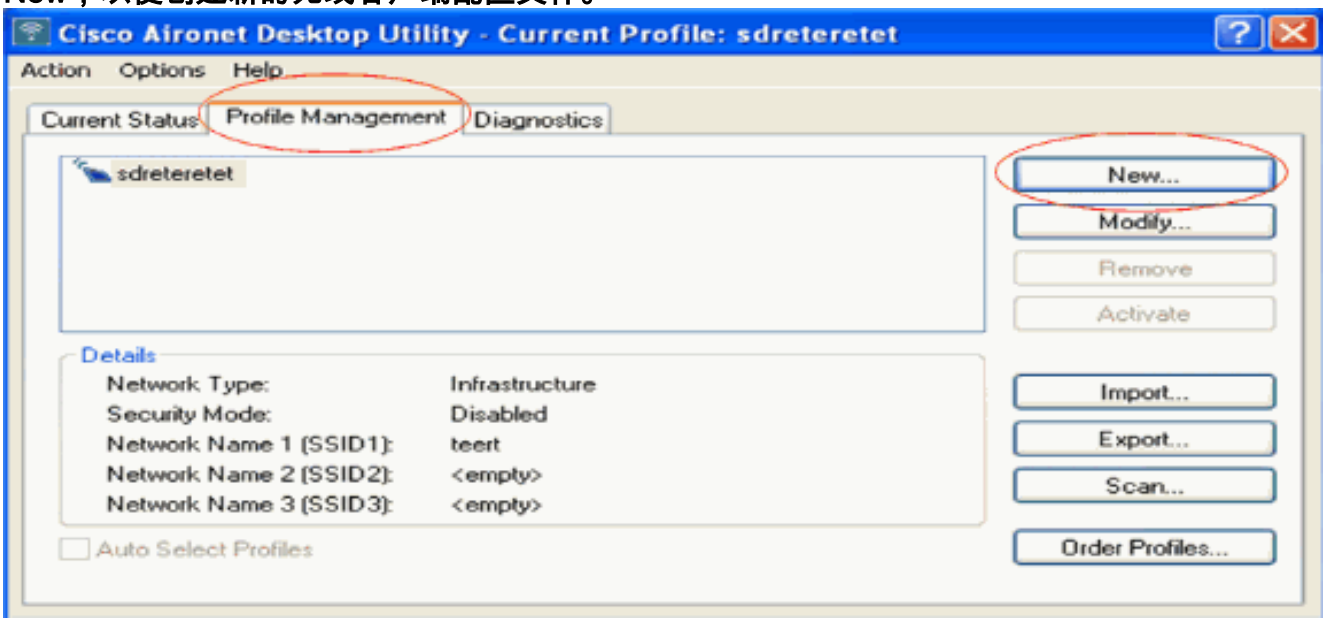
在本示例中，请观察右侧被圈出的字段。

6. 按照本文档的用 LDAP 服务器的详细信息来配置 WLC 部分中所述，在 **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。**

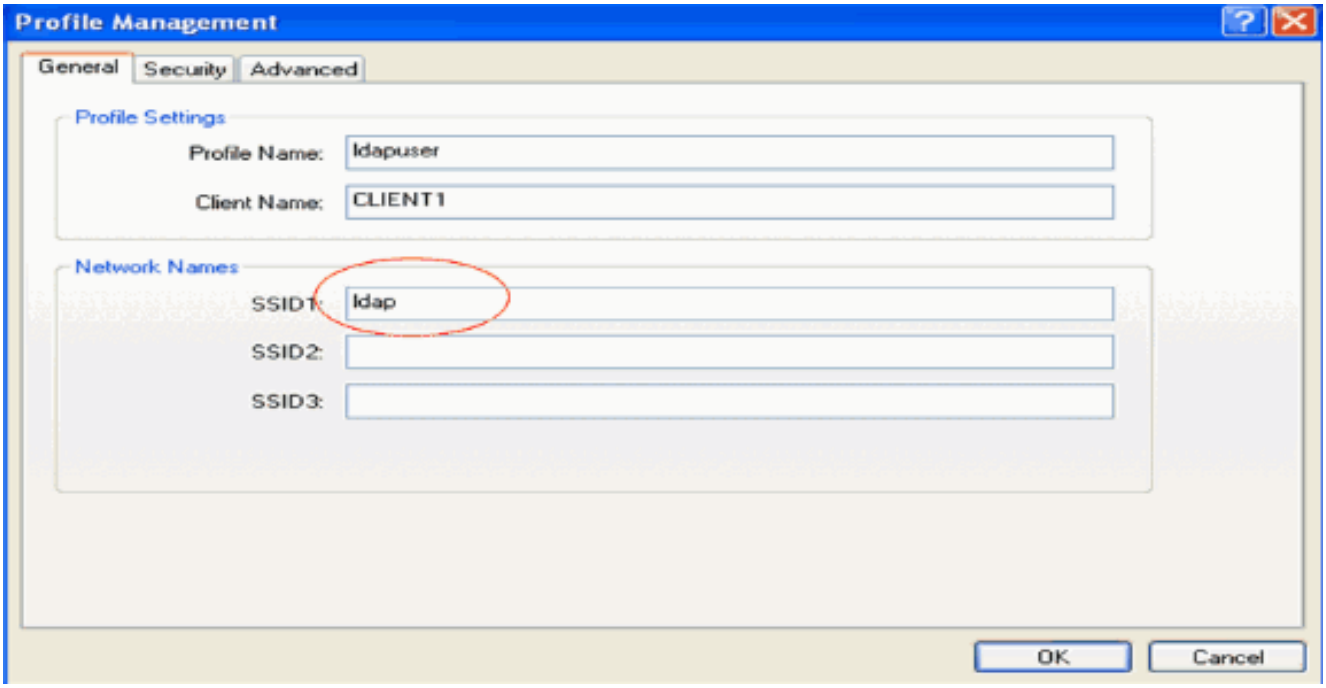
配置无线客户端

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：

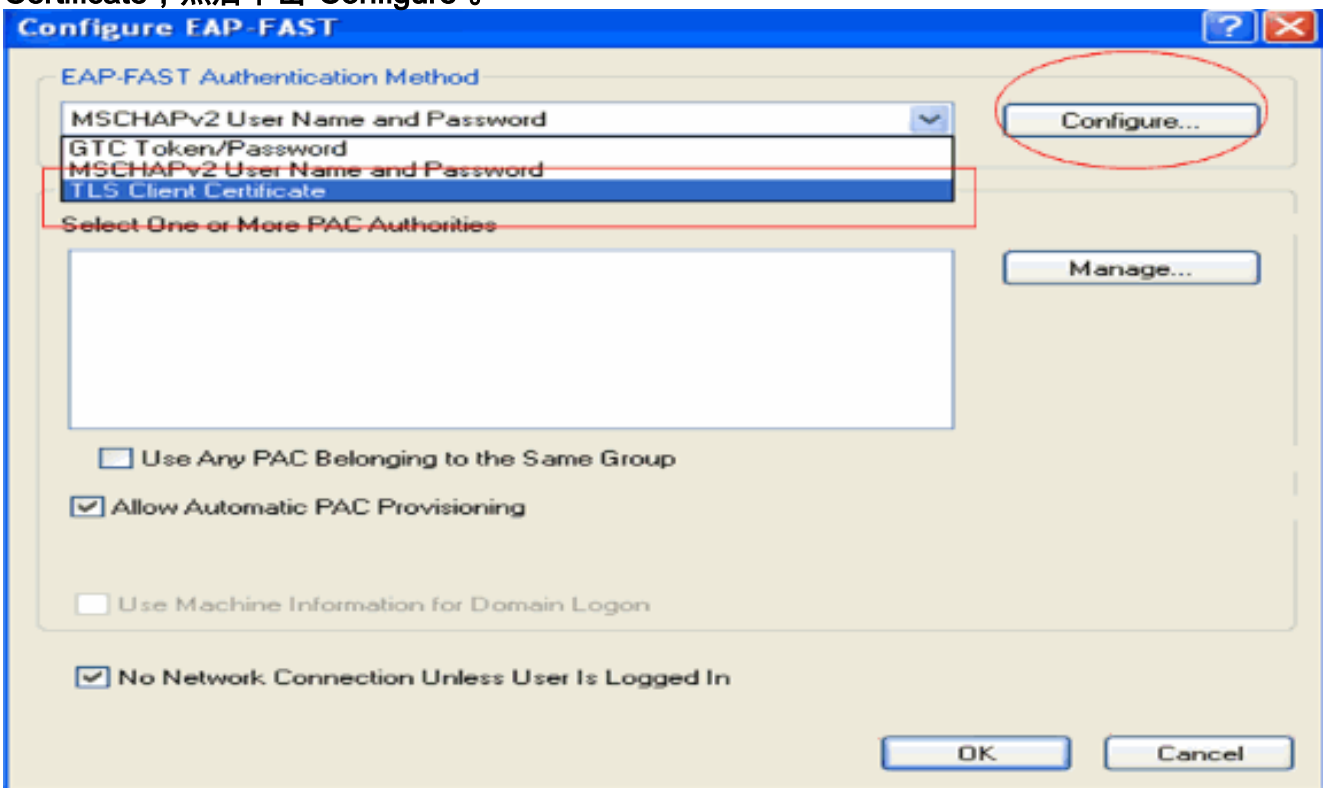
1. 启动**Cisco Aironet Desktop Utility**(ADU)。在 ADU 主窗口中，单击 **Profile Management > New，以便创建新的无线客户端配置文件。**



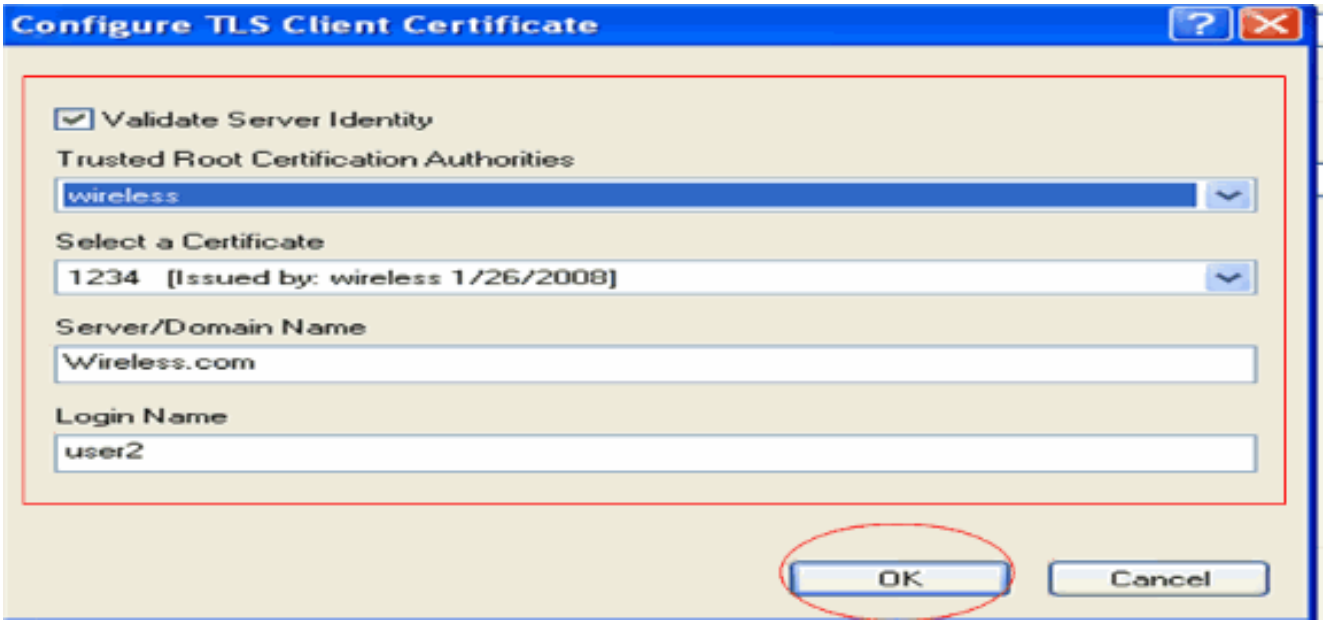
2. 指定配置文件名称，并向此配置文件分配一个 SSID 名称。此 SSID 名称应该与 WLC 上配置的相同。在本示例中，SSID 名称是 **ldap**。



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”。**



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（如本文档的为客户端生成设备证书部分所述）作为客户端证书。Click **OK**.本示例解释了此步骤
：



这就创建了无线客户端配置文件。

验证

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 **ldap SSID。**
2. 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 ldap 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 ldap 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
(436973636f000000000000000000000000)

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: Creating new context
```

```
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:

    Name ........................................ 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
```

故障排除

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
- 技术支持和文档 - Cisco Systems

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）。