在 Cisco Secure ACS 设备上为 PEAP 客户端安装证书

目录

简介
先决条件
要求
使用的组件
规则
Microsoft 证书服务安装
Cisco Secure ACS for Windows 证书设置
步骤 1：创建服务器证书
步骤 2： 批准来自 CA 的证书
步骤 3： 将服务器证书下载到 Cisco Secure ACS 服务器
步骤 4： 在 Cisco Secure ACS 服务器上安装 CA 证书
步骤 5：设置 Cisco Secure ACS 以使用服务器证书
Cisco Secure ACS 设备证书设置
步骤 1：创建证书签名请求
步骤 2： 使用您的 CSR 创建服务器证书
步骤 3： 将 CA 证书下载到您的 FTP 服务器
步骤 4： 在您的设备上安装 CA 证书
步骤 5：在您的设备上安装服务器证书
自签名证书设置（仅当您不使用外部 CA 时）
配置全局验证设置
在 Cisco Secure ACS 上设置 AP
配置 AP
安装 ACU 版本 6（仅当使用 Cisco Secure ACS 3.1 或需要 EAP-GTC 时）
为客户端安装根 CA 证书（仅适用于 EAP-MSCHAP-V2）
为 PEAP 设置客户端
计算机身份验证补充
设置 ACS 以允许计算机身份验证
设置客户端以用于计算机身份验证
WPA 密钥管理补充
配置 AP
为 PEAP 和 WPA 设置 Windows XP SP1（已安装 KB826942）或 SP2 客户端
验证
故障排除
问题 1
解决方案
问题 2

解决方案
问题 3
解决方案
问题 4
解决方案
相关信息

简介

此指南描述证书创建与Microsoft CA并且包含步骤为，当您使用一签署证书时，自思科安全访问控制服务器(ACS) 3.3支持。由于不需要外部 CA，因此使用自签名证书大大简化了初始受保护的可扩展的身份验证协议 (PEAP) 安装。但目前，自签名证书的默认有效期只有一年且不能更改。这是服务器证书的标准有效期。然而，因为自签名证书也作为根CA证书，这能每年含义新证书的安装在每个客户端的，当您使用Microsoft请求方时，除非不检查**验证服务器证书**选项。Cisco 建议您仅将自签名证书用作您可以使用传统 CA 之前的临时措施。如果希望使用自签名证书，请继续参阅自签名证书部分。

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：

- Cisco IOS接入点(AP) 12.02T1
- Cisco Secure ACS for Windows 3.1 及更高版本
- Cisco Secure ACS解决方案引擎(SE)。
- 安装有 ACU 版本 6 的 Microsoft Windows 2000（SP3 和 SP4）或 XP（如果使用 Cisco Secure ACS 3.2，则不需要 ACU）

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Microsoft 证书服务安装

完成这些步骤：

1. 选择**开始 > 设置 > 控制面板**。
2. 在控制面板中，打开**添加/删除程序**。
3. 在“添加/删除程序”中，选择**添加/删除 Windows 组件**。
4. 选中**证书服务**并单击“下一步”。对 IIS 消息单击**是**。

5. 选择一个独立（或企业）根 CA 并单击**下一步**。
6. 为该 CA 指定名称并单击**下一步**。所有其他框都是可选的。**注意：** 不要为 CA 指定与 Cisco Secure ACS 服务器一样的名称。这可能导致 PEAP 客户端身份验证失败，因为当找到与服务器证书同名的根 CA 证书时，这些客户端会分不清这二者。此问题并非 Cisco 客户端独有。
7. 单击 **Next**。
8. 单击 **完成**。**注意：** 在安装 CA 前，必须安装 IIS。

Cisco Secure ACS for Windows 证书设置

步骤 1：创建服务器证书

要创建服务器证书，请完成以下步骤。

1. 从您的 Cisco Secure ACS 服务器，浏览到 CA **http://IP_of_CA_server/certsrv/**。
2. 选择**请求证书**选项并单击“下一步”。
3. 选择**高级请求**并单击“下一步”。
4. 选择**使用表单向此 CA 提交证书请求**并单击“下一步”。
5. 在名称 (CN) 框中键入名称。
6. 选择**服务器身份验证证书**作为预期目的。**注意：** 如果使用企业 CA，请在第一个下拉框中选择 **Web 服务器**。**CSP** —微软Base Cryptographic供应者v1.0**密钥大小** - 1024**注意：** Windows 2003 企业 CA 允许大于 1024 的密钥大小。然而，使用关键大于1024不与PEAP一起使用。验证在ACS也许看上去通过，但是客户端暂停，当尝试验证时。选中**标记密钥为可导出**。选中**使用本地计算机存储**（仅软件 ACS）。保留所有其他项为默认值并单击**提交**。将显示一条消息，说明您的证书申请已经收到....**注意：** 使用大于 1024 的密钥大小创建的证书不会起作用。

注意 2

注意： Microsoft 已在 Windows 2003 企业 CA 发行版中更改 Web 服务器模板以使密钥不再可导出，该选项将变灰。没有随证书服务一起提供其他用于服务器身份验证并提供将密钥标记为“可导出”的功能（在下拉框中提供）的证书模板。因此，您需要创建一个新模板来实现此功能。

完成这些步骤：

1. 选择**开始 > 运行 > certtmpl.msc**。
2. 右键单击 **Web 服务器**模板并选择“复制模板”。
3. 使用容易识别的名称命名模板。
4. 转到“请求处理”选项卡，并选中**允许导出私钥**。
5. 单击 **CSP** 按钮并选中 Microsoft Base Cryptographic Provider v1.0。单击 **Ok**。
6. 所有其他选项都可以保留为默认值。
7. 单击**适用**并且**好**。
8. 打开 CA MMC 管理单元。
9. 右键单击**证书模板**并选择“新建”>“要颁发的证书模板”。
10. 选择您创建的新模板并单击**确定**。
11. 重新启动 CA。

当尝试创建新证书时，证书服务也可能出现 Failed to create 'CertificateAuthority.Request' object 错误。要更正此问题，请执行以下步骤：

1. 选择**开始 > 管理工具 > IIS**。

2. 展开**网站 > 默认网站**。
3. 右键单击 **CertSrv** 并选择“属性”。
4. 在“虚拟目录”选项卡的“应用程序设置”部分中单击**配置**按钮。
5. 转到“选项”选项卡并选中**启用会话状态**。
6. 保留所有其他项为默认值。
7. 单击**确定**两次。
8. 重新启动 IIS。如果您的浏览器锁定并显示消息 Downloading ActiveX Control，请运行 Microsoft 文档在您尝试使用证书服务器时，Internet Explorer 停止响应并显示“正在下载 ActiveX 控件”消息 中讨论的解决方法。 如果 CSP 字段只显示 Loading...，请确保不要在提交请求的计算机上运行软件防火墙。

步骤 2：批准来自 CA 的证书

完成这些步骤：

1. 打开 CA 并选择“开始”>“程序”>“管理工具”>“证书颁发机构”。
2. 在左侧展开证书，然后单击**待处理的请求**。
3. 右键单击证书，选择**所有任务**，并选择“颁发”。

步骤 3：将服务器证书下载到 Cisco Secure ACS 服务器

完成这些步骤：

1. 从您的 Cisco Secure ACS 服务器，浏览到 **CA -http://IP_of_CA_server/certsrv/** 目录。
2. 选择**检查挂起的证书**并单击“下一步”。
3. 选择证书并单击**下一步**。
4. 单击 **Install**。

步骤 4：在 Cisco Secure ACS 服务器上安装 CA 证书

完成这些步骤：

注意： 如果将 Cisco Secure ACS 和 CA 安装在同一个服务器上，则不需要此步骤。

1. 从您的 Cisco Secure ACS 服务器，浏览到 **CA -http://IP_of_CA_server/certsrv/** 目录。
2. 选择**检索 CA 证书或证书吊销列表**并单击“下一步”。
3. 选择 **Base 64 编码**并单击“下载 CA 证书”。
4. 单击**打开**并选择“安装证书”。
5. 单击 **Next**。
6. 选择**将所有的证书放入下列存储**并单击“浏览”。
7. 选中**显示物理存储区**框。
8. 展开**受信任的根证书颁发机构**，选择“本地计算机”，并单击“确定”。
9. 依次单击**下一步**、“完成”，并在“导入成功”框中单击“确定”。

步骤 5：设置 Cisco Secure ACS 以使用服务器证书

完成这些步骤：

1. 在 Cisco Secure ACS 服务器上，单击 **System Configuration**。
2. 选择 **ACS Certificate Setup** 和 Install ACS certificate。
3. 选择 **Use certificate from storage**。
4. 键入 CN 名称并单击 **Submit**。
5. 在 Cisco Secure ACS 服务器上，单击 **System Configuration**。
6. 选择 **ACS Certificate Setup** 和 Edit Certificate Trust List。
7. 选中 CA 的框并单击 **Submit**。

Cisco Secure ACS 设备证书设置

步骤 1：创建证书签名请求

完成这些步骤：

1. 选择 **System Configuration > ACS Certificate Setup > Generate Certificate Signing Request**。
2. 在 Certificate subject 字段中以 cn=name 格式输入名称。
3. 输入私钥文件的名称。**注意：** 私钥的路径缓存在此字段中。如果在创建 CSR 后再按一次 **submit**，私钥将被重写，因而与原始 CSR 不匹配。当您尝试安装服务器证书时，这将导致出现 private key does not match 错误消息。
4. 输入私钥口令并确认它。
5. 选择 1024 的密钥长度。**注意：** 虽然 Cisco Secure ACS 可以生成大于 1024 的密钥大小，但使用大于 1024 的密钥不适用于 PEAP。身份验证看上去可能已在 Cisco Secure ACS 中通过，但当尝试身份验证时，客户端将挂起。
6. 单击 **Submit**
7. 复制右侧的 CSR 输出以提交到 CA。

步骤 2：使用您的 CSR 创建服务器证书

完成下面这些步骤。

1. 从您的 FTP 服务器，浏览到 **CA -http://IP_of_CA_server/certsrv/** 目录。
2. 选择**请求证书**选项并单击“下一步”。
3. 选择**高级请求**并且**其次**点击。
4. 选择**使用 base64 编码的 PKCS #10 文件提交一个证书请求，或使用 base64 编码的 PKCS #7 文件更新证书请求**。
5. 将证书签名请求的输出粘贴到“Base64 编码的证书请求”字段并单击**提交**。
6. 单击**下载 CA 证书**。
7. 单击**保存**，命名证书并将其保存到您的 FTP 目录中。

步骤 3：将 CA 证书下载到您的 FTP 服务器

完成这些步骤：

注意： 如果跳过这些步骤，将导致任何一方都无法启用 PEAP。您还会收到说明未安装服务器证书的错误（即使已安装服务器证书），或在您的尝试失败时收到 EAP type not configured 故障（即使已配置 EAP 类型）。

注意： 另请注意，如果使用中间 CA 创建服务器证书，您需要为根 CA 和服务器证书之间的链（其中包括根 CA 证书）中的每个 CA 重复这些步骤。

1. 从您的 FTP 服务器，浏览到 **CA -http://IP_of_CA_server/certsrv/** 目录。
2. 选择**检索 CA 证书或证书吊销列表**并单击“下一步”。
3. 选择 **Base 64 编码**并单击“下载 CA 证书”。
4. 单击**保存**并命名证书。将它保存到您的 FTP 目录。

步骤 4：在您的设备上安装 CA 证书

完成这些步骤：

注意： 如果跳过这些步骤，将导致任何一方都无法启用 PEAP。您还会收到说明未安装服务器证书的错误（即使已安装服务器证书），或在您的尝试失败时收到 EAP type not configured 故障（即使已配置 EAP 类型）。

注意： 另请注意，如果使用中间 CA 创建服务器证书，您需要为根 CA 和服务器证书之间的链（其中包括根 CA 证书）中的每个 CA 重复这些步骤。

1. 选择 **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**。
2. 单击 **Download CA certificate file**。
3. 在 FTP Server 字段中键入 FTP 服务器的 IP 地址或主机名。
4. 在 Login 字段中键入 Cisco Secure ACS 可用来访问 FTP 服务器的有效用户名。
5. 在 Password 字段中键入用户的口令。
6. 在 Remote FTP Directory 字段中键入从 FTP 服务器根目录到包含 CA 证书文件的目录的相对路径。
7. 在 Remote FTP File Name 字段中键入 CA 证书文件的名称。
8. 单击 **submit**。
9. 验证字段中的文件名并单击 **Submit**。
10. 在 **System Configuration > Service Control** 中重新启动 ACS 服务。

步骤 5：在您的设备上安装服务器证书

完成这些步骤：

1. 选择 **System Configuration > ACS Certificate Setup**。
2. 单击 **Install ACS Certificate**。
3. 选择 **Read certificate from file** 选项，然后单击 Download certificate file 链接。
4. 在 FTP Server 字段中键入 FTP 服务器的 IP 地址或主机名。
5. 在 Login 字段中键入 Cisco Secure ACS 可用来访问 FTP 服务器的有效用户名。
6. 在 Password 字段中键入用户的口令。
7. 在 Remote FTP Directory 字段中键入从 FTP 服务器根目录到包含服务器证书文件的目录的相对路径。
8. 在 Remote FTP File Name 字段中键入服务器证书文件的名称。
9. 单击 **submit**。
10. 输入私钥的路径。
11. 输入私钥的口令。
12. 单击 **submit**。

自签名证书设置（仅当您不使用外部 CA 时）

注意： 当您在实验室中使用自签名证书进行测试时，客户端第一次使用 Microsoft 请求方进行身份验证可能需要较长的身份验证时间。所有后续身份验证都很正常。

完成这些步骤：

1. 在 Cisco Secure ACS 服务器上，单击 **System Configuration**。
2. 单击 **ACS Certificate Setup**。
3. 单击 **Generate Self-signed Certificate**。
4. 在 Certificate subject 字段中键入以 **cn=** 开头的主题，例如，cn=ACS33。
5. 键入要创建的证书的完整路径和名称，例如，c:\acscert \acs33.cer。
6. 键入要创建的私钥文件的完整路径和名称，例如 c:\acscert \acs33.pvk。
7. 输入私钥口令并确认它。
8. 从密钥长度下拉菜单中选择 **1024**。**注意：** 虽然 Cisco Secure ACS 可以生成大于 1024 的密钥大小，但使用大于 1024 的密钥不适用于 PEAP。身份验证看上去可能已在 ACS 中通过，但当尝试身份验证时，客户端将挂起。
9. 选中 **Install generated certificate**。
10. 单击 **submit**。

配置全局验证设置

完成下面这些步骤。

1. 在 Cisco Secure ACS 服务器上，单击 **System Configuration**。
2. 单击 **Global Authentication Setup**。**对于 Cisco Secure ACS 3.2 版及更高版本**如果使用 Microsoft PEAP，则选中 **Allow EAP-MSCHAPv2**。如果使用 Cisco PEAP，则选中 **Allow EAP-GTC** 。选中 **Allow MS-CHAP Version 1 Authentication**。选中 **Allow MS-CHAP Version 2 Authentication**。单击 **Submit** 并重新启动。**对于 Cisco Secure ACS 3.1 版**选中 **Allow PEAP**。选中 **Allow MS-CHAP Version 1 Authentication**。选中 **Allow MS-CHAP Version 2 Authentication**。单击 **Submit** 并重新启动。

在 Cisco Secure ACS 上设置 AP

完成这些步骤：

1. 在 Cisco Secure ACS 服务器上，单击 **Network Configuration**。
2. 单击 **Add Entry** 以添加 AAA 客户端。
3. 填写以下框：AAA客户端IP地址- IP_of_your_AP**Key** - 构造密钥，并确保该密钥与 AP 共享密钥匹配。认证使用- RADIUS (Cisco Aironet)
4. 单击 **Submit** 并重新启动。**注意：** 未更改 AAA 客户端设置的任何默认值。

配置 AP

使用 VxWorks

完成这些步骤：

1. 打开 AP 并选择 **Setup > Security > Authentication Server**。输入 Cisco Secure ACS IP 地址。输入共享密钥，该密钥必须与 Cisco Secure ACS 中的密钥匹配。选中 **EAP Authentication**。单击 **Ok**。
2. 选择 **Setup > Security > Radio Data Encryption**。为 Accept Authentication Type 选中 **Open** 和 Network-EAP。为 Require EAP 选中 **Open**。如果不使用广播密钥轮换，请设置 **WEP key 1** 并选择 128 位。将 Use of Data Encryption by Stations 更改为 **full Encryption**。如果不能更改数据加密的用法，请首先单击 **Apply**。单击 **Ok**。

使用 Cisco IOS AP Web 接口

完成这些步骤：

1. 打开 AP 并选择 **Security > Server Manager**。从 Current Server 下拉列表中选择 **RADIUS**。输入 Cisco Secure ACS IP 地址。输入共享密钥，该密钥必须与 Cisco Secure ACS 中的“密钥”匹配。选中 **EAP Authentication**。在警告对话框上单击 **OK**，然后单击 Apply。
2. 选择 **Security > SSID Manager**。**注意：** 如果使用 WPA，则配置将有所不同。有关详细信息，请参阅本文档末尾的 WPA 密钥管理补充。从 Current SSID 列表中选择 SSID 或在 SSID 字段中输入新 SSID。选中 **Open Authentication** 并从下拉菜单中选择 EAP。选中 **Network EAP**。保留所有其他值为其默认值并单击 **Apply**。
3. 选择 **Security > Encryption Manager**。**注意：** 如果使用 WPA，则配置将有所不同。有关详细信息，请参阅本文档末尾的 WPA 密钥管理补充。单击 **WEP Encryption** 单选按钮并从下拉菜单中选择 Mandatory。单击 **Encryption Key 1** 单选按钮并在字段中输入密钥。从 Key Size 下拉菜单中选择 **128 bit**。单击 **Apply**。

注意： 如果安装 ACU，则需要网络 EAP。

注意： 如果使用广播密钥轮换，则不需要设置密钥，因为应已设置了密钥。如果未设置密钥，请选择 **Setup > Radio Advance** 并设置广播密钥轮换值。不需要将该值设置为任何低于五分钟（300 秒）的值。设置值后，单击 **OK** 并返回到 Radio Data Encryption 页。

安装 ACU 版本 6（仅当使用 Cisco Secure ACS 3.1 或需要 EAP-GTC 时）

由于快速安装不安装 Cisco PEAP 请求方，因此需要选择自定义安装。当您在网络连接属性的“身份验证”选项卡中查看 EAP 类型时，您可以看出是否安装了 Cisco 请求方。如果它显示 PEAP，则这是 Microsoft PEAP 请求方。如果它只显示 PEAP，则使用 Cisco PEAP 请求方。

为客户端安装根 CA 证书（仅适用于 EAP-MSCHAP-V2）

如果使用来自 Microsoft CA 的证书

完成这些步骤：

1. 从客户端 PC 中，浏览到 CA -**http://IP_of_CA_server/certsrv/**。
2. 选择**检索 CA 证书**并单击“下一步”。
3. 选择 **Base64 编码**和“下载 CA 证书”。
4. 单击**打开**并选择“安装证书”。
5. 单击 **Next**。
6. 选择**将所有的证书放入下列存储**，然后单击“浏览”。
7. 选中**显示物理存储区**框。

8. 展开**受信任的根证书颁发机构**，选择“本地计算机”，并单击“确定”。
9. 依次单击**下一步**、“完成”，并在“导入成功”框中单击“确定”。

如果使用来自 Cisco Secure ACS 的自签名证书

完成这些步骤：

1. 将证书从其位置复制到客户端。
2. 右键单击 **.cer** 文件并单击“安装证书”。
3. 单击 **Next**。
4. 选择**将所有的证书放入下列存储**并单击“浏览”。
5. 选中**显示物理存储**。
6. 展开**受信任的根证书颁发机构**，选择“本地计算机”，并单击“确定”。
7. 依次单击**下一步**、“完成”和“确定”。**注意：** 如果使用 EAP-MSCHAP-V 并在 Windows 的 PEAP 属性中选中**验证服务器证书**框，则必须为每个客户端设置 Cisco Secure ACS 的 AP。

为 PEAP 设置客户端

为 PEAP 设置 Windows XP SP1 或 SP

完成这些步骤：

注意： 如果使用 WPA，则此配置将有所不同。有关详细信息，请参阅本文档的 WPA 密钥管理部分。

注意： Windows XP SP2 当前对除 IAS 以外的 RADIUS 服务器进行 PEAP 身份验证时会出现问题。这记录在 KB885453 中，Microsoft 有一个按要求提供的补丁程序。

1. 在控制面板上打开“网络连接”并选择**开始 > 控制面板**。
2. 右键单击“无线网络”并选择**属性**。
3. 在“无线网络”选项卡上，请确保已选中**使用 Windows 配置...**。
4. 如果在列表中看到 SSID，请单击**配置**。否则，单击**添加**。
5. 输入 SSID 并选中 **WEP**，系统将自动提供密钥。
6. 选择“身份验证”选项卡并确保已选中**启用使用...的网络访问控制**。
7. 选择**受保护的 EAP** 并单击该 EAP 类型的“属性”。
8. 选中“受信任的根证书”下 **CA** 的框。
9. 单击 **OK** 三次。

为证书设置 Windows XP（不带 SP1）

完成这些步骤：

1. 在控制面板上打开“网络连接”并选择**开始 > 控制面板**。
2. 右键单击“无线网络”并选择**属性**。
3. 在“无线网络”选项卡上，请确保已选中**使用 Windows 配置...**。
4. 选择“身份验证”选项卡并确保已选中**启用使用...的网络访问控制**。
5. 选择 **PEAP** 并单击该 EAP 类型的“属性”。
6. 选中“受信任的根证书”下 **CA** 的框。

7. 单击 **OK** 三次。

为 PEAP 设置 Windows 2000

完成这些步骤：

1. 如果运行 SP3，请从 Microsoft 下载并安装 802.1x 修补程序 。 这对于 SP4 没有必要。
2. 选择**开始 > 控制面板 > 网络和拨号连接**。
3. 右键单击您的无线连接并选择**属性**。
4. 单击“身份验证”选项卡。**注意：** 如果没有“身份验证”选项卡，则表示 802.1X 服务在禁用状态下安装。要解决此问题，必须启用服务列表中的**无线配置服务**：右键单击**我的电脑**并单击“管理”。选择**服务 > 应用程序**并单击“服务”。将服务的“启动类型”值设置为**自动**，然后启动服务。**注意：** 如果“身份验证”选项卡存在但不可用，这表明网络适配器驱动程序无法正确支持 802.1x。检查 802.1x 修补程序 页底部的列表或供应商网站以查找支持的驱动程序。
5. 选中**启用使用 IEEE 802.1x 的网络访问控制**。
6. 从“EAP 类型”下拉菜单中选择 **PEAP** 并单击“确定”。

如果使用 ACU

完成这些步骤：

1. 打开 ACU。
2. 选择**管理配置文件**并创建配置文件或编辑配置文件。
3. 输入 AP 的客户端名称和 SSID。
4. 选择“网络安全”选项卡。
5. 为 Network Security Type 选择 **Host-based EAP**。
6. 为 WEP 选择 **Use Dynamic WEP Keys**。
7. 单击**确定**两次。
8. 选择您创建的配置文件。**注意：** 如果使用 Cisco 请求方，则“身份验证”选项卡上只有 PEAP。如果使用 Microsoft 请求方，则显示 Protected EAP (PEAP)。**注意：** 在客户端尝试关联到 AP 之前有很长的延迟（大约一分钟），使用 Microsoft 的用于 Windows XP 的无线更新总成包现已面世 修补程序，可以部分减少延迟。 此修补程序可能会重新安装阻止 EAP-GTC 兼容数据库类型正常运行的 EAP-MSCHAPv2 请求方。**注意：** 如果未关联成功，请尝试禁用然后重新启用卡。

为 PEAP 设置 Windows 2003 Mobile

完成这些步骤：

1. 安装最新版本的 Cisco ACU for Windows CE 并确保在此安装期间安装 PEAP 请求方。
2. 打开 ACU 并从 Active Profile 下拉菜单中选择 **<External Settings>**。
3. 插入您的 Cisco 网卡，单击任务栏上的网络图标，并选择 **Settings > Advanced > Network Card**。
4. 单击您的 SSID（如果有）或 **Add New Settings**。
5. 验证 Network Name 字段中的 SSID 和要连接的网络。
6. 单击“身份验证”选项卡。
7. 选中**数据加密 (WEP)** 和“为我提供此密钥...”””
8. 选中**启用使用 802.1x 的网络访问控制**并选择 Cisco PEAP。

9. 单击**属性**并选中“验证服务器证书”（可选）。**注意：** 如果选中此选项，则需要在 PocketPC 上安装根 CA 证书。Windows Mobile 不包括可用于导入/管理证书的好方法。有一些可用的实用程序 。 Cisco 不支持这些实用程序。使用 ACU 时，不需要手动导入根 CA，因为 Cisco PEAP 请求方会为您导入它。目前，所有版本的 PocketPC 操作系统都不支持自签名证书，因此您不能将自签名证书导入到 PocketPC 中进行验证。如果取消选中 **Validate server certificate** 选项，则仍可以使用自签名证书。
10. 单击 **OK**，直到返回 Configure Wireless Networks 屏幕。
11. 单击 **Connect**。

计算机身份验证补充

计算机身份验证的目的是允许在用户身份验证前建立 EAP 身份验证和网络连接，以便登录脚本可以运行并且用户可以登录到域。要建立计算机凭据并进行身份验证，必须具有域成员资格。

设置 ACS 以允许计算机身份验证

完成这些步骤：

1. 选择 **External User Databases > Database Configuration**。
2. 单击 **Windows Database** 并选择 Configure。
3. 选中 **Enable PEAP machine authentication**。
4. 单击 **submit**。

设置客户端以用于计算机身份验证

加入域（如果尚不是域的成员）

完成这些步骤：

1. 使用具有管理员权限的帐户登录到 Windows。
2. 右键单击**我的电脑**并选择“属性”。
3. 选择“计算机名”选项卡并单击**更改**。
4. 在“计算机名”字段中输入主机名。
5. 选择**域**，输入域名，然后单击“确定”。
6. 为了加入域，将显示一个登录对话框。使用有权加入域的帐户登录。
7. 计算机成功加入域后，重新启动该计算机。计算机已是域的成员，并具有只有操作系统知道的与域协商的身份验证凭据。在 Cisco Secure ACS 中，用户名显示为主机/主机名。

设置 PEAP 请求方以用于计算机身份验证

完成这些步骤：

1. 选择**开始 > 控制面板**以在控制面板上打开“网络连接”。
2. 右键单击网络连接并选择**属性**。
3. 选择“身份验证”选项卡，并选中**验证为计算机**。

WPA 密钥管理补充

为 Cisco IOS AP 12.02(13)JA1、Cisco Secure ACS 3.2 和具有 WPA 修补程序的 Windows XP SP1 编写。

注意： Windows 2000 客户端不会对 WPA 密钥管理提供本地支持 。 您必须使用供应商的客户端软件才能获得此支持：

注意： 目前，Cisco ACU 不支持基于主机的 EAP（EAP-TLS 和 PEAP）的 WPA 密钥管理。您必须安装第三方客户端，如 Funk Odyssey 客户端或 Meetinghouse AEGIS 客户端。有关 Cisco 产品的 WPA 支持的详细信息，请参阅 WPA 支持。

注意： 另请注意，目前，由 Pocket PC 版本的 ACU 为 Cisco 卡安装的驱动程序不支持 WPA。WPA 不为 PocketPC 上的 Cisco 客户端工作，即使安装了第三方请求方也是如此。

配置 AP

完成这些步骤：

1. 选择 **Security > Encryption Manager**。选择 WEP **Cipher** 并从下列菜单中选择 TKIP。单击 **Apply**。
2. 选择 **Security > SSID Manager**。从 Current SSID 列表中选择 SSID 或在 SSID 字段中输入新 SSID。选中 **Open Authentication** 并从下拉菜单中选择 EAP。选中 **Network EAP**。在 Authenticated Key Management 下，从下拉菜单中选择 **Mandatory** 并单击 WPA。单击 **Apply**。

为 PEAP 和 WPA 设置 Windows XP SP1（已安装 KB826942）或 SP2 客户端

完成这些步骤：

1. 选择**开始 > 控制面板**以在控制面板上打开“网络连接”。
2. 右键单击“无线网络”并选择**属性**。
3. 在“无线网络”选项卡上，请确保已选中**使用 Windows 配置...**。
4. 如果在列表中看到 SSID，请单击**配置**。否则，单击**添加**。
5. 输入 SSID 并为“网络身份验证”选择 **WPA**，为“数据加密”选择 TKIP。
6. 选择“身份验证”选项卡并确保已选中**启用使用...的网络访问控制**。
7. 选择**受保护的 EAP** 并单击该 EAP 类型的“属性”。
8. 选中“受信任的根证书”下 **CA** 的框。
9. 单击 **OK** 三次。

验证

当前没有可用于此配置的验证过程。

故障排除

问题 1

在使用 ACS 进行证书安装/身份验证期间将出现此错误。

```
Unsupported private key file format
Failed to initialize PEAP or EAP-TLS authentication protocol because ACS certificate is
not installed
```

解决方案

之所以出现此错误，是因为没有正确安装 peap 证书。删除证书并安装新的自签名证书可解决此问题。

问题 2

在使用 ACS 进行证书安装/身份验证期间将出现此错误。

```
Failed to initialize PEAP or EAP-TLS authentication protocol because CA certificate is
 not installed.
```

解决方案

要解决此错误，请使用 ACS 证书颁发机构安装程序安装 CA 证书。如果未使用自签名证书，则此错误是由于 CA 证书不正确导致的。

问题 3

当 ACS 升级完成时，将出现此错误。

```
A required certificate is not within its validity period when verifying
against the current system clock or the timestamp in the signed file.
(800B0101)
```

解决方案

当 ACS 软件升级完成时，如果不升级管理软件，将出现此错误。执行管理软件升级然后执行 ACS 软件升级，可以解决此问题。有关如何升级 ACS 的详细信息，请参阅管理 Cisco Secure ACS 设备的升级设备部分。

问题 4

此错误在有ACS的认证安装时出现。

```
Private key you've selected doesn't fit to this certificate
```

解决方案

此的多数常见原因偶然地覆盖专用密钥由生成新的CSR。

验证此信息：

1. 您装载正确证书作为ACS证书。
2. RSA客栈密钥长度是1024个位在请求的创建时。
3. 当您生成CSR时，您使用完整CN=string。

相关信息

- Cisco Secure ACS for UNIX 支持页
- 安全产品 Field Notices（包括 CiscoSecure UNIX）
- 用于 Unix 的 Cisco 安全访问控制服务器文档
- Cisco Secure ACS for Windows 支持页
- Cisco Secure ACS for Windows 文档
- 技术支持和文档 - Cisco Systems