# EAP-TLS版本1.01配置指南

**文档ID**64064

已更新：2009年10月14日

 下载 pdf文档

 打印

Feedback

**相关产品**

- Cisco Aironet 1200接入点
- Cisco Aironet 350接入点
- **用于 Unix 的 Cisco 安全访问控制服务器**
- 用于 Windows 的 Cisco 安全访问控制服务器

## Contents

# Introduction

本文为可扩充验证传输层安全(EAP-TLS)版本1.01提供一配置示例。

**Note:** 本文假设，您使用微软认证授权(CA)。当您能使用自签证书时， Cisco高度劝阻此实践，并且本文不包括自署名的认证。自署名的认证的默认到期周期只是一年，并且您不能更改此设置。这为服务器证明是相当标准。然而，自签证书也作为根CA证书。所以，除非不检查" Validate server certificate "选项，您需要在每个客户端上每年安装新证书。实际CA一定取得到无论如何获得客户端证书，然后确实没有原因使用与EAP-TLS的自署名的认证。

# Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

本文档中的信息基于以下软件和硬件版本：

- 接入点(AP) 12.02T1
- 访问控制服务器(ACS) 3.1， 3.2和3.3
- Windows 2000和XP
- 企业根Certificate Authority (CA)

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is

live, make sure that you understand the potential impact of any command.

## Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# Configure

本部分提供有关如何配置本文档所述功能的信息。

**Note:** 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

## 安装 Microsoft 证书 (CA) 服务器

完成这些步骤：

1. 选择**开始 > 设置 > 控制面板**。
2. 点击**添加/去除**在控制面板的**程序**。
3. 选择**添加/去除Windows组件**。
4. 选择证书服务。
5. 单击 **Next**。
6. 对 IIS 消息单击**是**。
7. 选择一个独立(或企业)根CA。
8. 单击 **Next**。
9. 为该 CA 命名。**Note:** 所有其他机箱是可选的。**Note:** 因为这能造成PEAP客户端发生故障认证，请勿使用同一个名字CA象ACS服务器。与名字的一个根CA证书和服务器证明一样迷惑PEAP客户端。此问题对Cisco客户端不是唯一。当然，如果不计划使用PEAP，这不适用。
10. 单击 **Next**。数据库默认设置正确。
11. 单击 **Next**。在安装 CA 前，必须安装 IIS。

## 创建服务器证书

完成这些步骤：

1. 访问对CA (从您的ACS服务器的**http://IP_of_CA_server/certsrv/**)。
2. 选中 **Request a certificate** 框。
3. 单击 **Next**。
4. 选择**高级请求**。
5. 单击 **Next**。
6. **使用表，**选择**提交证书请求给此CA**。
7. 单击 **Next**。
8. 键入在命名(CN)机箱的一个名字。
9. 检查**服务器验证证书**机箱打算的目的。**Note:** 如果使用企业CA，请选择在第一张列表的**Web服务器**。
10. 选择这些选项在关键选项下创建一个新的模板：**CSP —微软Base Cryptographic供应者v1.0密钥大小— 1024Note:** 用密钥大小创建的证书极大比1024能工作为HTTPS，但是不为PEAP。**Note:** Windows 2003企业CA允许极大密钥大小比1024，但是关键大于1024不与

PEAP一起使用。认证在ACS能看上去通过，但是客户端暂停在认证尝试。检查**标记键作为可输出**选项**Note:** Microsoft 已在 Windows 2003 企业 CA 发行版中更改 Web 服务器模板。使用此模板更改，您能不再导出键，并且选项变灰。没有与是为服务器验证，或者产生能力标记键如可输出的证书服务一起提供的其他认证模板。要创建一个可实现此功能的新模板，请参阅创建新证书模板部分。检查**使用本地机器存储**选项**Note:** 保留所有其它选项的默认选择。

11. 单击 **submit**。您必须收到此消息：您的证书请求已收到。

## 创建新证书模板

完成这些步骤：

1. 选择**Start > Run**。
2. 键入**在**Run对话框的**certtmpl.msc**，并且按Enter。
3. 用鼠标右键单击**Web服务器模板**，并且选择**复制模板**。
4. 给出模板，例如， ACS。
5. 选择**处理请求**选项。
6. 检查**允许专用密钥是被导出的**选项。
7. 选择**CSPs**按钮。
8. 检查**微软Base Cryptographic供应者v1.0**选项。
9. 单击 **Ok**。**Note:** 保留所有其它选项的默认选择。
10. 单击 **Apply**。
11. 单击 **Ok**。
12. 打开卡扣式CA的MMC。
13. 用鼠标右键单击**认证模板**，并且选择**新>发出的认证模板**。
14. 选择您创建的新模板。
15. 单击 **Ok**。
16. 重新启动CA。新的模板在认证模板列表包括。

有时，当您尝试创建新证书时，“没‘CertificateAuthority.Request’”错误发生。

完成这些步骤为了更正此错误：

1. 选择**开始 > 管理工具 > IIS**。
2. 展开**网站 > 默认网站**。
3. 用鼠标右键单击**CertSrv**，并且选择**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. 选择选项按键。
6. 检查**Enable (event)会话状态**选项。**Note:** 保留所有其它选项的默认选择。
7. 单击**确定**两次。
8. 重新启动IIS。**Note:** 在模式未准备2003年与adprep/forestprep/domainprep的兼容性的2000年域的2003 CA不与EAP一起使用。如果您的浏览器锁定与“Activex”消息，您需要运行在此URL的修正：http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B330389 。**Note:** 如果CSP字段显示“….”请保证您没有在提交请求的机器的一软件防火墙。ZoneLabs' ZoneAlarm几乎每次导致此错误。某一其它软件能也导致此错误。

## 批准来自 CA 的证书

完成这些步骤：

1. 选择 **Start > Programs > Administrative Tools > Certificate Authority**。
2. 扩展在左窗格的认证。
3. 选择**等待请求**。
4. 右键单击该证书。
5. 选择所有任务。
6. 选择**问题**。

# 在Windows服务器上安装认证

## 将服务器证书下载到 ACS 服务器

完成这些步骤：

1. 访问对CA (从您的ACS服务器的**http://IP_of_CA_server/certsrv/**)。
2. 选择**在一个待定认证的检查**。
3. 单击 **Next**。
4. 选择证书。
5. 单击 **Next**。
6. 点击**安装**。

## 在 ACS 服务器上安装 CA 证书

**Note:** 这些步骤不是必要的ACS和CA是否在同一个服务器上安装。

1. 完成这些步骤：

2. 从 ACS 服务器浏览到 CA (http://IP_of_CA_server/certsrv/)。
3. 选择**检索CA证书或认证吊销列表**。
4. 单击 **Next**。
5. 选择**编码的Base64**。
6. 单击**下载 CA 证书**。
7. 点击**开放**。
8. 单击 **Install Certificate**。
9. 单击 **Next**。
10. **在以下存储**选择**地方所有证书**。
11. 点击**访问**。
12. 选中**显示物理存储区**框。
13. 扩展**可靠的根证书颁发机构**授权表。
14. 选择本地计算机。
15. 单击 **Ok**。
16. 单击 **Next**。
17. 单击 **完成**。消息框出现。
18. 单击 **Ok**。**Note:** 如果您的客户端证书通过CA被创建了与您的服务器证明不同，您必须重复在客户端证书创建和所有中间CAs的这些步骤涉及的根CA。

## 使用服务器证明的设置ACS

完成这些步骤：

1. 点击在ACS服务器的**系统配置**。
2. 选择**ACS认证设置**。
3. 选择**安装ACS认证**。
4. 选择 **Use certificate from storage**。
5. 输入CN名字(您输入创建第8步服务器证明部分)的同一个名字。
6. 单击 **submit**。
7. 点击在ACS服务器的**系统配置**。
8. 选择**ACS认证设置**。
9. 选择**编辑证书信任列表**。
10. 检查**CA**机箱。
11. 单击 **submit**。

## 创建证书签名请求

完成这些步骤：

1. 去**设置的系统配置> ACS认证>生成认证署名请求**。
2. 键入在证书主题字段的一个名字以`cn=name`格式。
3. 键入一个名字对于专用密钥文件。**Note:** 此字段缓存路径到专用密钥。所以，如果点击请**提交**第二次，在CSR被创建后，专用密钥重写和不会匹配原始CSR。当您尝试安装服务器证明时，这能导致“”错误。
4. 键入专用密钥密码。
5. 证实密码。
6. 选择 1024 的密钥长度。**Note:** ACS能生成极大密钥大小比1024。然而，关键大于1024不与EAP一起使用。认证在ACS能看上去通过，但是客户端暂停在认证尝试。
7. 单击 **submit**。
8. 复制在右边的CSR输出提交给CA。

## 请使用您的CSR创建服务器证明

完成这些步骤：

1. 访问对CA (从您的FTP服务器的**http://IP_of_CA_server/certsrv/**)。
2. 选择**请求身份验证选项**。
3. 单击 **Next**。
4. 选择**高级请求**。
5. 单击 **Next**。
6. **使用a base64 encoded PKCS -7 file**，选择**提交证书请求使用a base64 encoded PKCS -10 file或更新请求**。
7. 粘贴创建的第8步的输出认证署名请求部分到Base64编码的证书请求字段。
8. 单击 **submit**。
9. 单击**下载 CA 证书**。
10. 点击**“Save”**，键入一个名字对于认证，并且保存它对您的FTP目录。

# 在Windows工具上安装认证

## 将 CA 证书下载到您的 FTP 服务器

完成这些步骤：

1. 访问对CA (从您的FTP服务器的**http://IP_of_CA_server/certsrv/**)。
2. 选择**检索CA证书或认证吊销列表**。
3. 单击 **Next**。
4. 选择**编码的Base64**。
5. 单击**下载 CA 证书**。
6. 点击**"Save"**，键入一个名字对于认证，并且保存它对您的FTP目录。

## 在您的设备上安装 CA 证书

完成下面这些步骤。

1. 去**设置的系统配置> ACS认证> ACS认证机构设置**。
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. 键入Cisco Secure ACS能使用访问在洛金字段的FTP服务器的有效用户名。
5. 键入用户名的正确的密码在密码字段。
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。
10. 单击 **submit**。
11. 在 **System Configuration > Service Control** 中重新启动 ACS 服务。**Note:** 如果跳过在下载CA证书对您的FTP服务器和安装CA证书的步骤在您的这两个情况的工具第一部分能出现：您不能enable (event) EAP-TLS，并且错误信息看上去阐明，没有安装服务器证明，即使安装认证。或者，EAP故障在失败的尝试发生，即使配置EAP类型。**Note:** 并且请注意，如果使用中间CA创建您的服务器证明，您需要重复每个CA的这些步骤在根CA和服务器证明之间的一系列(包括根CA证书)。另外，如果通过CA创建了您的客户端证书与您的服务器证明不同，您必须重复在客户端证书创建和所有中间CAs的这些步骤涉及的根CA。

## 在您的工具上安装服务器证明

完成这些步骤：

1. 去**系统配置> ACS认证设置**。
2. 单击 **Install ACS Certificate**。
3. 选择读的认证从文件选项。
4. 点击**下载证书文件**链路。
5. 在 FTP Server 字段中键入 FTP 服务器的 IP 地址或主机名。
6. 键入Cisco Secure ACS能使用访问在洛金字段的FTP服务器的有效用户名。
7. 键入在密码字段的正确的密码。
8. 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。
9. 在 Remote FTP File Name 字段中键入服务器证书文件的名称。

10. 单击 **submit**。
11. 键入路径和密码专用密钥的。参考第3步和第4步创建认证署名请求部分。
12. 单击 **submit**。

# 其他任务

## 配置全局验证设置

完成这些步骤：

1. 点击在ACS服务器的**系统配置**。
2. 单击 **Global Authentication Setup**。
3. 检查**允许EAP-TLS**。
4. 选择一个或更多证书验证选项。如果选择所有方法， ACS依顺序尝试每个方法，直到成功验证发生或直到最后方法出故障。
5. 单击 **submit**。
6. 重新启动PC。

## 在 ACS 上设置 AP

要在 ACS 上设置 AP，请完成以下步骤：

1. 点击在ACS服务器的**网络配置**。
2. 单击 **Add Entry** 以添加 AAA 客户端。
3. 指定这些值在机箱：AAA客户端IP地址— IP_of_your_AP键—组成一关键(请确定键匹配AP被共享的密钥)验证使用— RADIUS (Cisco Aironet)
4. 单击 **submit**。
5. 重新启动PC。**Note:** 请勿更改其中任一个在AAA客户端设置的默认值。

## 配置 AP

**Note:** 网络EAP是必要的是否要安装ACU。

如果使用广播密钥交替，您不需要设置键，当必须已经设置键。如果没有设置键，请去**设置> Radio预付款**和设置广播密钥交替的值。您很可能不需要设置此任何更低的然后5分钟(300秒)。在您设置值后，请点击OK键，并且回到无线数据加密页。

### VxWorks

完成这些步骤：

1. 打开AP。
2. 选择**Setup > Security >认证服务器**。
3. 输入ACS IP地址。
4. 输入共有的秘密。此值必须匹配ACS键。
5. 检查**EAP验证**机箱。
6. 单击 **Ok**。

7. 选择 **Setup > Security > Radio Data Encryption**。
8. 检查**开放**机箱。
9. 如果不使用广播密钥交替，请选择**WEP密钥1**和**128**。
10. 请由位置更改Use of Data Encryption到**完全加密**(如果不能更改此，点击首先**适用**)。
11. 单击 **Ok**。

### IOS AP Web接口

完成这些步骤：

1. 选择**安全>Server管理器**。
2. 从当前服务器列表选择RADIUS。
3. 键入ACS IP地址。
4. 键入共有的秘密。此值必须匹配在ACS的键。
5. 检查**EAP验证**机箱。
6. 从EAP验证列表，请选择RADIUS服务器的IP地址。
7. 点击OK键在警告对话框的。
8. 单击 **Apply**。

### SSID管理器(仅WEP加密)

只完成WEP加密的这些步骤：

1. 从当前SSID列表选择SSID或者指定一新的SSID在SSID字段。
2. 检查**开放式验证**机箱。
3. 选择**与EAP**从列表。
4. 检查**网络EAP**机箱。
5. 单击 **Apply**。

### 加密管理器(仅WEP加密)

只完成WEP加密的这些步骤：

1. 选择 **Security > Encryption Manager**。
2. 点击**WEP加密**单选按钮。
3. 从列表选择必须。
4. 点击**加密密钥1**单选按钮。
5. 指定键。
6. 从密钥大小列表选择**128**。
7. 单击 **Apply**。**Note:** 如果使用 WPA，则配置将有所不同。请参阅WPA密钥管理补充在本文结束时关于详细资料。

## 下载并且安装客户端的根CA证书

此步骤对于EAP-TLS的*每个*客户端*是必需的*能在该客户端工作。完成这些步骤：

1. 访问对CA (从客户端PC机的**http://IP_of_CA_server/certsrv/**)。
2. 选择**检索CA证书**。

3. 单击 **Next**。
4. 选择**编码的Base64**。
5. 单击**下载 CA 证书**。
6. 点击**开放**。
7. 单击 **Install Certificate**。
8. 单击 **Next**。
9. **在以下存储**选择**地方所有证书**。
10. 点击**访问**。
11. 选中**显示物理存储区**框。
12. 扩展**可靠的根证书颁发机构**，并且选择**本地计算机**。
13. 单击 **Ok**。
14. 单击 **Next**。
15. 单击 **完成**。
16. 点击OK键在消息框的用消息。

## 创建客户端证书

### 企业CA

完成这些步骤：

1. 访问对CA (从客户端的用户帐户的**http://IP_of_CA_server/certsrv/**)。
2. 选择**请求身份验证选项**。
3. 单击 **Next**。
4. 选择**高级请求**。
5. 单击 **Next**。
6. **使用表，**选择**提交证书请求给此CA**。
7. 单击 **Next**。
8. 选择认证模板列表的**用户**。
9. 设置这些值在关键选项下：CSP —微软Base Cryptographic供应者v1.0密钥大小— 1024所有其它选项—保留默认值
10. 单击 **submit**。消息框显现…消息。

### 独立CA

完成这些步骤：

1. 访问对CA (从客户端的用户帐户的**http://IP_of_CA_server/certsrv/**)。
2. 选择**请求身份验证选项**。
3. 单击 **Next**。
4. 选择**高级请求**。
5. 单击 **Next**。
6. **使用表，**选择**提交证书请求给此CA**。
7. 单击 **Next**。
8. 键入在CN字段的用户名。此值必须匹配在认证数据库的用户名。
9. 为打算的目的选择客户端身份验证证书。
10. 设置这些值在关键选项下：CSP —微软Base Cryptographic供应者v1.0密钥大小— 1024所有

其它选项—保留默认值

11. 单击 **submit**。消息框显现…消息。

## 审批从CA的客户端证书

完成这些步骤：

1. 选择打开CA的**Start > Programs > Administrative Tools >认证机关**。
2. 扩展在左边的认证。
3. 点击**等待请求**。
4. 用鼠标右键单击在认证并且选择所有任务。
5. 选择**问题**。

## 在客户端PC机上安装客户端证书

完成这些步骤：

1. 访问对CA (从客户端的用户帐户的**http://IP_of_CA_server/certsrv/**)。
2. 选择**在一个待定认证的检查**。
3. 单击 **Next**。
4. 选择证书。
5. 单击 **Next**。
6. 点击**安装**。**Note:** 为了验证认证安装，请去微软互联网探索者微软因特网资源管理器，并且选择**工具> Internet选项>内容>证书**。与记录在用户ID或用户名的名字的一个认证一定存在。

## 委托在ACS的客户端证书

只有当客户端证书和服务器证明通过不同的CAs，被创建了您需要执行这些步骤。

1. 保证根CA证书和半成品CA证书根据步骤安装了在安装上CA证书在ACS服务器上并且在您的工具部分上安装CA证书。
2. 去在ACS **> ACS认证设置的系统配置**。
3. 单击 **Edit Certificate Trust List**。
4. 在创建客户端证书的根CA旁边检查机箱。
5. 单击 **submit**。

## 设置EAP-TLS的客户端

完成这些步骤：

1. 选择**开始 > 控制面板 > 网络连接**。
2. 用鼠标右键单击无线网络，并且选择**属性**。
3. 点击**无线网络**选项。
4. 保证**配置使用的窗口…**被检查。
5. 如果看到在列表的SSID请点击**配置**。否则，单击**添加**。
6. 放置在SSID。
7. 检查**WEP**和**键为我自动地提供**复选框。
8. 选择**Authentication选项**。**Note:** 如果看不到Authentication选项， 802.1X服务在一个禁用状态

上安装。为了解决此问题，您必须enable (event)在服务列表的无线配置服务。完成这些步骤：用鼠标右键单击**我的计算机**，并且选择**管理**。单击 **Services and Applications**。单击 **Services**。将服务的启动值设置为 Automatic。启动服务。**Note:** 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。请参见使用在运行Windows 2000的客户端计算机的802.1x认证 。

9. 保证**enable (event)访问控制使用…**被检查。
10. 为EAP类型选择**智能卡或其他认证**，并且点击**属性**。
11. 选择**在此计算机**选项的**使用身份验证**。
12. 检查**使用简单的认证选择**复选框。
13. 选中“受信任的根证书”下 **CA** 的框。
14. 点击OK键三倍。

# 计算机身份验证补充

EAP-TLS机器认证*要求*激活目录，并且企业根CA.为了获取EAP-TLS机器认证的一个认证，计算机必须有连接到企业CA通过有线连接或通过同802.1x安全停用的无线连接。这是获得有效机器认证的*唯一方法*(与“机器”在“认证模板”领域)。当完成，机器认证在**证书(本地计算机)上**在卡扣式证书(本地计算机)的MMC安装**>私有>证书**文件夹，当查看。认证在主题和SAN字段包含完全合格的AD机器名字。具有计算机的名字，但是的认证未被创建正如此部分所描述不是真的机器认证(用“机器”在认证模板领域)。这样认证没有使用机器认证，但是OS相当看到这样认证作为普通用户认证。

## 允许机器认证的设置ACS

完成这些步骤：

1. 去**外部用户数据库>数据库配置**。
2. 单击 **Windows Database**。
3. 单击 **Configure**。
4. 检查**Enable (event) EAP-TLS机器认证**复选框。
5. 单击 **submit**。

## 配置认证自动注册的域

完成这些步骤：

1. 打开用户和计算机MMC卡扣式在域控制器。
2. 用鼠标右键单击域条目并且选择**属性**。
3. 去**Group Policy选项**。
4. 选择**默认域策略**。
5. 点击**编辑**。
6. 去**Computer Configuration > Windows Settings > Security Settings >公共密钥策略**。
7. 用鼠标右键单击**自动证书请求设置**。
8. 选择**新>自动证书请求**。
9. 单击 **Next**。
10. 突出显示**计算机**。
11. 单击 **Next**。
12. 检查企业CA。
13. 单击 **Next**。

14. 单击 **完成**。

## 设置机器认证的客户端

### 加入域

如果客户端加入了域，在您配置了自动注册前，必须发行认证到机器，当下次您重新启动计算机，在自动注册被配置，不用需要答辩计算机对域以后。

完成这些步骤加入域：

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**Computer Name选项**。
4. 点击**更改**。
5. 键入在Computer Name字段的主机名。
6. 选择**域**。
7. 键入域的名字。
8. 单击 **Ok**。登录对话框出现。
9. 登陆与有权限加入域帐户的证件。计算机加入域。
10. 重新启动计算机。计算机当前是域的成员，并且有CA的一个认证和安装的机器认证。

### 设置机器认证的EAP-TLS请求方

完成这些步骤：

1. 选择**开始 > 控制面板 > 网络连接**。
2. 用鼠标右键单击网络连接并且选择**属性**。
3. 选择**Authentication选项**。
4. 检查**验证作为计算机**。

# WPA 密钥管理补充

此部分是可适用的对Cisco IOS AP 12.02(13)JA1、与WPA ICM Hotfixes的ACS 3.2和XP SP1。根据在此部分的文档， Windows 2000客户端不本地支持WPA密钥管理，并且您必须使用供应商的客户端软件为了获得此技术支持。参考在Windows XP的WPA无线安全更新概述 。

Cisco ACU当前不支持招待基础的EAP的WPA密钥管理(EAP-TLS和PEAP)。您必须安装一个第三方客户端，例如， Funk冒险旅行客户端或者Meetinghouse支持客户端。欲知关于思科产品的WPA技术支持的详情参考Windows的无线LAN适配器文件。此信息是可适用的对Windows莫比尔也2003个(口袋PC)客户端。

WPA密钥管理基本上是相同的，但是有所不同在这两个程序：

1. 配置AP。
2. 设置EAP-TLS和WPA的XP客户端。

## 配置 AP

完成这些步骤：

1. 去**安全>加密管理器**。
2. 点击**WEP密码**选项。
3. 选择**TKIP**。
4. 单击 **Apply**。
5. 去**安全> SSID管理器**。
6. 从当前SSID列表选择SSID。或者，您在SSID字段能指定一新的SSID。
7. 检查**开放式验证**。
8. 选择**与EAP**从列表。
9. 选中 **Network EAP**。
10. 选择**必须**从列表在验证密钥管理下。
11. 点击**WPA**。
12. 单击 **Apply**。

### 设置EAP-TLS和WPA的XP客户端

完成这些步骤：

1. 选择**开始 > 控制面板 > 网络连接**。
2. 用鼠标右键单击无线网络，并且选择**属性**。
3. 选择**无线网络**选项。
4. 保证**配置使用的窗口**选项被检查。
5. 如果看到在列表的SSID请点击**配置**。否则，单击**添加**。
6. 放置在SSID。
7. 选择网络验证的**WPA**。
8. 选择数据加密的**TKIP**。
9. 选择**Authentication选项**。
10. 保证**enable (event)访问控制使用**被检查。
11. 为EAP类型选择**智能卡或其他认证**。
12. 单击 **Properties**。
13. 选择**在此计算机**选项的**使用身份验证**。
14. 检查**使用简单的认证选择**复选框。
15. 选中“受信任的根证书”下 **CA** 的框。
16. 点击OK键三倍。

## Verify

当前没有可用于此配置的验证过程。

## Troubleshoot

### Error:认证的问题，当连接到WLAN时

此错误出现在无线客户端。

“<Authentication server>”“<CA name>”“<CA name>”

## 解决方案

为了解决此问题，您能导出发行认证到认证服务器对文件CA的根证明。复制文件到无线客户端从一高的Prompt命令然后运行此命令。

```
certutil -- addstore NTAuth CA_CertFilename.cer
```

当连接到在一台工作组机器的一个无线网络欲知更多信息时， 请参考Windows安全警报出现。

# Related Information

- Windows支持页面的Cisco Secure ACS
- UNIX支持页面的Cisco Secure ACS
- Technical Support & Documentation - Cisco Systems

本文档是否是有用？有 没有

感谢您的反馈。

打开支持案例（需要思科服务合同。）

## 相关的思科支持社区讨论

思科支持社区是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 Cisco Technical Tips Conventions 。

已更新：2009年10月14日
**文档ID**64064