

对 Cisco Secure ACS for Windows v3.2 配置 PEAP-MS-CHAPv2 机器身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景理论](#)

[规则](#)

[网络图](#)

[配置 Cisco Secure ACS for Windows v3.2](#)

[获取 ACS 服务器证书](#)

[配置 ACS 以使用存储中的证书](#)

[指定 ACS 应信任的其他证书颁发机构](#)

[重新启动服务并在 ACS 上配置 PEAP 设置](#)

[将接入点指定并配置为 AAA 客户端](#)

[配置外部用户数据库](#)

[重新启动服务](#)

[配置 Cisco 接入点](#)

[配置无线客户端](#)

[配置 MS 证书计算机自动注册](#)

[加入域](#)

[在 Windows 客户端上手动安装根证书](#)

[配置无线网络](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档演示如何使用针对 Windows 版本 3.2 的 Cisco Secure ACS 来配置受保护的可扩展的认证协议 (PEAP)。

有关如何使用无线局域网控制器、Microsoft Windows 2003软件和思科安全访问控制服务器 (ACS)4.0配置安全无线访问的详细信息，请参阅[带ACS 4.0和Windows 2003的统一无线网络下的PEAP](#)。

先决条件

[要求](#)

本文档没有任何特定的前提条件。

[使用的组件](#)

本文档中的信息基于以下软件和硬件版本。

- Cisco Secure ACS for Windows v3.2
- Microsoft 证书服务 (作为企业根证书颁发机构 [CA] 安装) **注意** : 有关详细信息 , [请参阅设置认证机构的分步指南](#) 。
- DNS 服务和 Windows 2000 Server (装有 Service Pack 3) **注** : 如果遇到CA服务器问题 , 请安装[修补程序323172](#) 。 Windows 2000 SP3客户端需要[修补程序](#) 313664来启用IEEE 802.1x身份验证。
- Cisco Aironet 1200 系列无线接入点 12.01T
- 运行 Windows XP Professional (装有 Service Pack 1) 的 IBM ThinkPad T30

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您是在真实网络上操作 , 请确保您在使用任何命令前已经了解其潜在影响。

[背景理论](#)

PEAP 和 EAP-TLS 构建并使用 TLS/安全套接字层 (SSL) 隧道。PEAP 仅使用服务器端身份验证 ; 只有服务器才具备证书 , 并向客户端证明其身份。EAP-TLS 在 ACS 服务器 (身份验证、授权和记帐 [AAA]) 和客户端都有证书的情况下使用相互认证 , 证明它们彼此的身份。

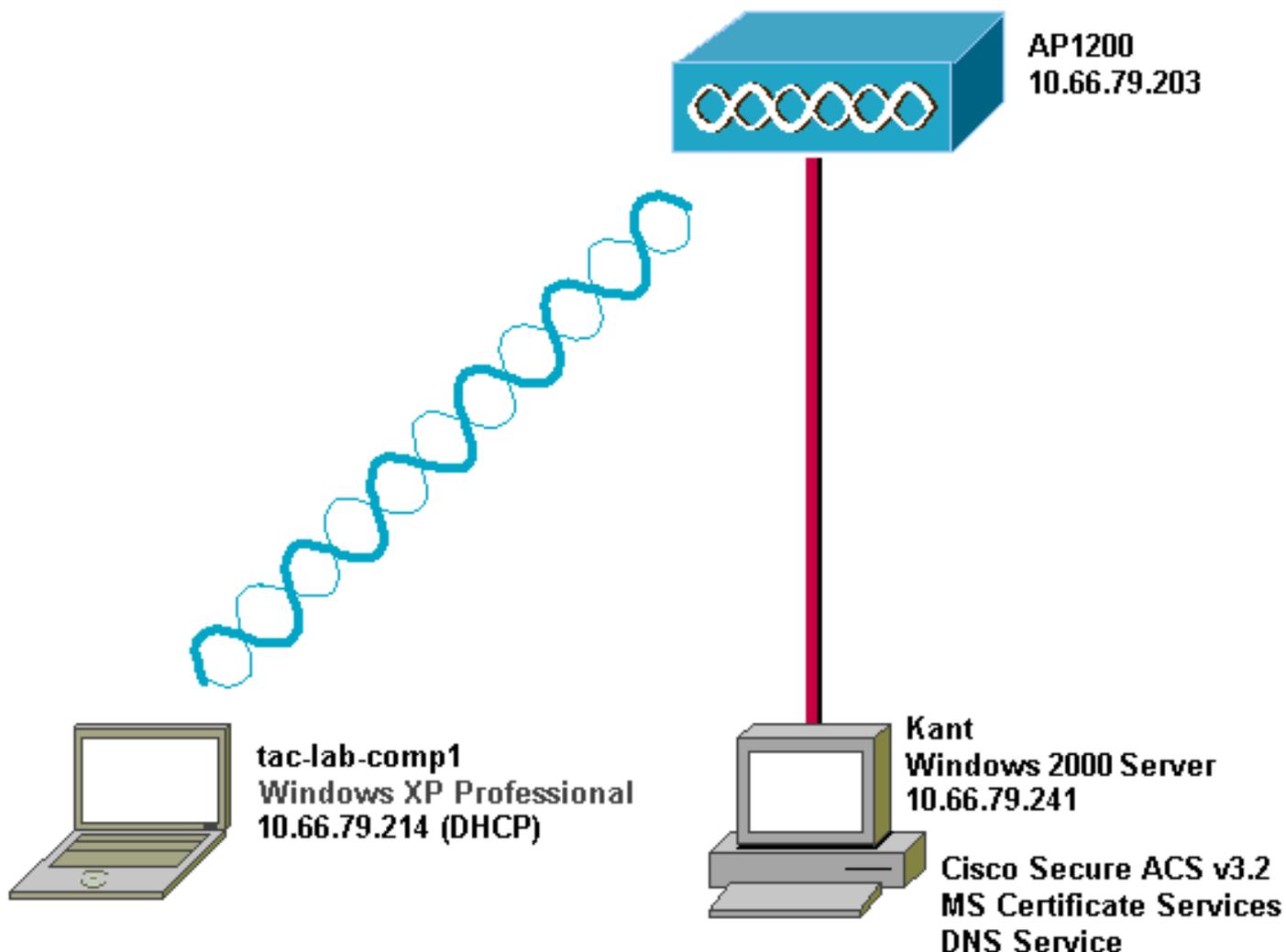
因为客户端不需要证书 , 因此 PEAP 非常方便。EAP-TLS 用于验证无外设设备 , 因为证书不需要任何用户交互。

[规则](#)

有关文档规则的详细信息 , 请参阅 [Cisco 技术提示规则](#)。

[网络图](#)

本文档使用下图所示的网络设置。



配置 Cisco Secure ACS for Windows v3.2

按照以下步骤配置 ACS 3.2。

1. [获取 ACS 服务器证书。](#)
2. [配置 ACS 以使用存储中的证书。](#)
3. [指定 ACS 应信任的其他证书颁发机构。](#)
4. [重新启动服务并在 ACS 上配置 PEAP 设置。](#)
5. [将接入点指定并配置为 AAA 客户端。](#)
6. [配置外部用户数据库。](#)
7. [重新启动服务。](#)

获取 ACS 服务器证书

按照以下步骤获取证书。

1. 在 ACS 服务器上打开 Web 浏览器，并在地址栏输入 `http://CA-ip-address/certsrv ip address/certsrv` 访问 CA 服务器。以管理员身份登录到域。

Enter Network Password [?] [X]

 Please type your user name and password.

Site: 10.66.79.241

User Name: Administrator

Password: *****

Domain: SEC-SYD

Save this password in your password list

OK Cancel

2. 选择 **Request a certificate** , 然后单击 Next。

Microsoft Certificate Services -- Our TAC CA [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

Next >

3. 选择 **Advanced request** , 然后单击 Next。

Choose Request Type

Please select the type of request you would like to make:

User certificate request:

A rectangular selection box with a blue header containing the text "User Certificate". The box is currently empty, indicating that this option is not selected.

Advanced request

Next >

4. 选择 **Submit a certificate request to this CA using a form** , 然后单击 Next。

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Next >

5. 配置证书选项。选择 **Web Server** 作为证书模板。输入 ACS 服务器的名称。

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OurACS

E-Mail:

Company:

Department:

City:

State:

Country/Region: US

将密钥大

小设置为 1024。选中 **Mark keys as exportable** 和 **Use local machine store** 选项。根据需要配置其他选项，然后单击 **Submit**。

Key Options:

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: Exchange Signature Both

Key Size: Min: 384 Max: 1024 (common key sizes: [512](#) [1024](#))

- Create new key set
 - Set the container name
- Use existing key set
- Enable strong private key protection
- Mark keys as exportable
 - Export keys to file
- Use local machine store

You must be an administrator to generate a key in the local machine store.

Additional Options:

Hash Algorithm:

Only used to sign request.

- Save request to a PKCS #10 file

Attributes:

Submit >

注：如果您看到一个警告窗口，指代脚本违规（取决于浏览器的安全/隐私设置），请单击“是”继续。



6. 单击 **Install this certificate**。

Microsoft Certificate Services -- Our TAC CA [Home](#)

Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

注：如果您看到一个警告窗口，指代脚本违规（取决于浏览器的安全/隐私设置），请单击“是”继续。

Potential Scripting Violation ✕

 This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

7. 如果安装成功，您将看到一条确认消息。

Microsoft Certificate Services -- Our TAC CA [Home](#)

Certificate Installed

Your new certificate has been successfully installed.

[配置 ACS 以使用存储中的证书](#)

按照以下步骤将 ACS 配置为使用存储中的证书。

1. 打开 Web 浏览器，并通过在地址栏中输入 **http://ACS-ip-address:2002/** 浏览到 ACS 服务器。单击 **System Configuration**，然后单击 ACS Certificate Setup。
2. 单击 **Install ACS Certificate**。
3. 选择 **Use certificate from storage**。在 Certificate CN 字段中，输入您在[获取 ACS 服务器证书](#)部分的步骤 5a 中指定的证书名称。单击“Submit”。在高级的证书请求期间，此条目必须与您输入名称字段的名称匹配。该名称是服务器证书的 subject 字段中的 CN 名称；可以对服务器证书进行编辑，以查看此名称。在本示例中，该名称为“OurACS”。请勿输入颁发者的 CN 名

CISCO SYSTEMS

System Configuration

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration**
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

Install ACS Certificate

Install new certificate ?

Read certificate from file

Certificate file

Use certificate from storage

Certificate CN

Private key file

Private key password

Back to Help ?

称。

4. 当配置完成时，您将看到一条确认消息，指示 ACS 服务器的配置已被更改。注意：此时您无需重新启动ACS。

CISCO SYSTEMS

System Configuration

Edit

Install ACS Certificate

Installed Certificate Information ?

Issued to: OurACS
Issued by: Our TAC CA
Valid from: June 23 2003 at 02:19:56
Valid to: June 18 2005 at 00:52:30
Validity: OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Install New Certificate Cancel

Navigation Menu:

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

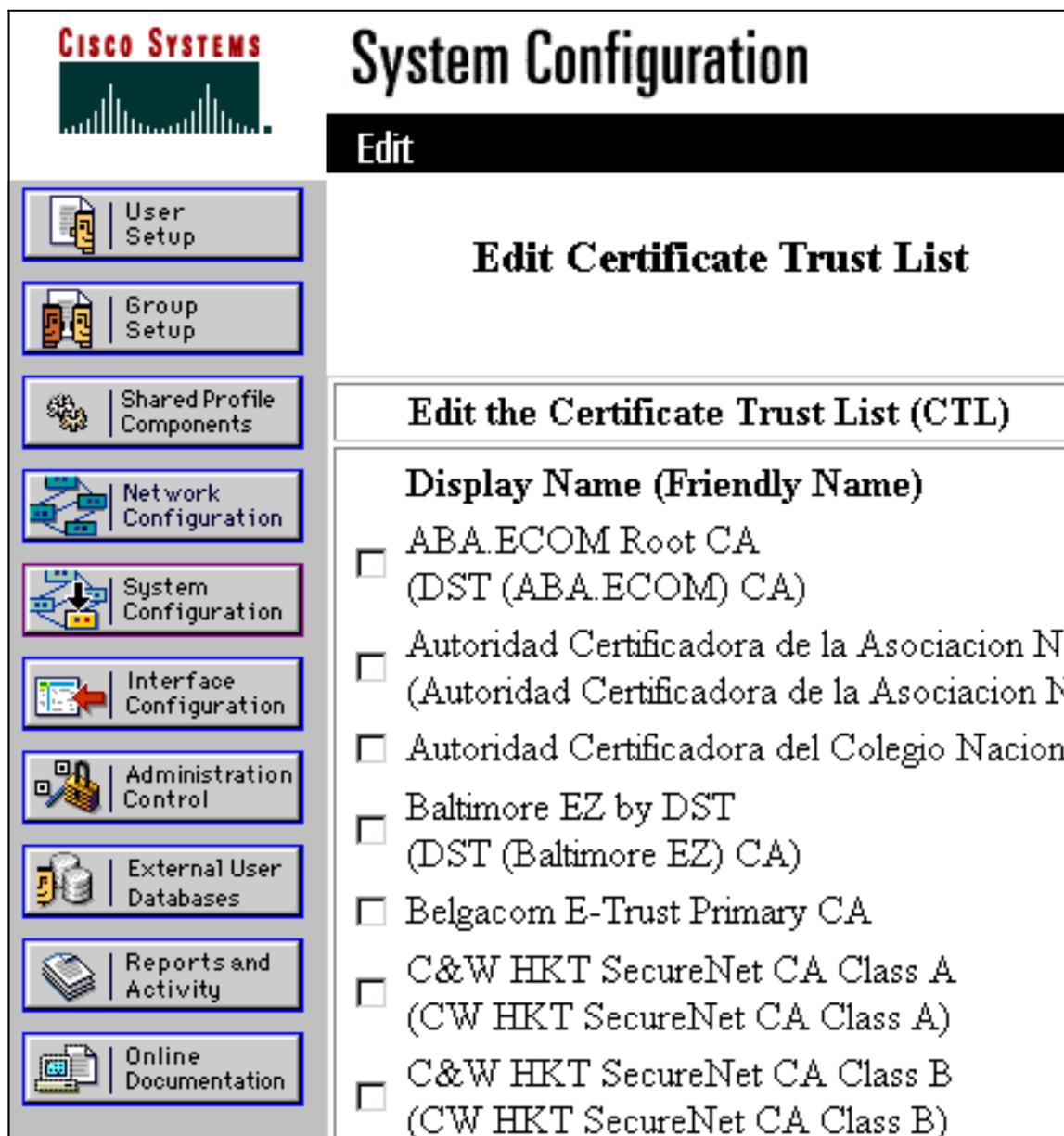
[指定 ACS 应信任的其他证书颁发机构](#)

ACS 将自动信任颁发其自己的证书的 CA。如果另外的 CA 发行客户端证书，则您需要完成以下步骤。

1. 单击 **System Configuration**，然后单击 **ACS Certificate Setup**。
2. 单击 **ACS Certificate Authority Setup** 以向受信任的证书列表添加 CA。在 CA 证书文件的字段中，输入证书的位置，然后单击 **Submit**。

The screenshot shows the Cisco System Configuration interface. At the top left is the Cisco Systems logo. The main title is "System Configuration". Below the title is a black bar with the word "Edit" in white. The left sidebar contains several menu items: "User Setup", "Group Setup", "Shared Profile Components", "Network Configuration", "System Configuration" (highlighted in purple), "Interface Configuration", "Administration Control", "External User Databases", "Reports and Activity", and "Online Documentation". The main content area is titled "ACS Certification Authority Setup". Below this title is a section titled "CA Operations" with a help icon. The text below reads "Add new CA certificate to local certificate storage". There is a text input field labeled "CA certificate file" with a red border. Below the input field is a yellow button with a question mark icon and the text "Back to Help".

3. 单击 **Edit Certificate Trust List**。选中 ACS 应该信任的所有 CA，不要选择 ACS 不应信任的所有 CA。单击“Submit”。



CISCO SYSTEMS

System Configuration

Edit

Edit Certificate Trust List

Edit the Certificate Trust List (CTL)

Display Name (Friendly Name)

- ABA.ECOM Root CA
(DST (ABA.ECOM) CA)
- Autoridad Certificadora de la Asociacion Na
(Autoridad Certificadora de la Asociacion N)
- Autoridad Certificadora del Colegio Naciona
- Baltimore EZ by DST
(DST (Baltimore EZ) CA)
- Belgacom E-Trust Primary CA
- C&W HKT SecureNet CA Class A
(CW HKT SecureNet CA Class A)
- C&W HKT SecureNet CA Class B
(CW HKT SecureNet CA Class B)

[重新启动服务并在 ACS 上配置 PEAP 设置](#)

按照以下步骤重新启动服务和配置 PEAP 设置。

1. 单击 **System Configuration**，然后单击 **Service Control**。
2. 单击 **Restart** 以重新启动服务。
3. 要配置 PEAP 设置，请单击 **System Configuration**，然后单击 **Global Authentication Setup**。
4. 选中如下所示的两个设置，并将所有其他设置保留为默认值。如果您愿意，您可以指定其他设置，例如，**Enable Fast Reconnect**。请在完成后单击 **Submit**。 **Allow EAP-MSCHAPv2 Allow MS-CHAP Version 2 Authentication**注：有关快速连接的详细信息，请参阅系统配置中的“身份验证配置选项”：身份验证和证书中的“身份验证配置选项”。

