

配置Cisco Secure ACS for Windows v3.2 (使用PEAP-MS-CHAPv2電腦身份驗證)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景理論](#)

[慣例](#)

[網路圖表](#)

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

[獲取ACS伺服器的證書](#)

[配置ACS以使用來自儲存的證書](#)

[指定ACS應信任的其他證書頒發機構](#)

[重新啟動服務並在ACS上配置PEAP設定](#)

[指定接入點並將其配置為AAA客戶端](#)

[配置外部使用者資料庫](#)

[重新啟動服務](#)

[配置思科接入點](#)

[配置無線客戶端](#)

[配置MS證書電腦自動註冊](#)

[加入域](#)

[在Windows客戶端上手動安裝根證書](#)

[配置無線網路](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文示範了如何使用Cisco Secure ACS for Windows 3.2版配置受保護的可擴展身份驗證協定 (PEAP)。

有關如何使用無線LAN控制器、Microsoft Windows 2003軟體和Cisco安全訪問控制伺服器 (ACS)4.0配置安全無線接入的詳細資訊，請參閱[ACS 4.0和Windows 2003的統一無線網路下的PEAP](#)。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本檔案中的資訊是根據以下軟體和硬體版本。

- 適用於Windows的Cisco安全ACS版本3.2
- Microsoft證書服務 (作為企業根證書頒發機構[CA]安裝) 注意：有關詳細資訊，請[參閱設定證書頒發機構的分步指南](#)。
- 帶有Service Pack 3的Windows 2000 Server的DNS服務注意：如果遇到CA伺服器問題，請安裝[修補程式323172](#)。Windows 2000 SP3客戶端需要[修補程式31364](#)，以啟用IEEE 802.1x身份驗證。
- Cisco Aironet 1200系列無線存取點12.01T
- 運行Windows XP Professional (帶Service Pack 1) 的IBM ThinkPad T30

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

背景理論

PEAP和EAP-TLS均構建並使用TLS/安全套接字層(SSL)隧道。PEAP僅使用伺服器端身份驗證；只有伺服器具有證書並向客戶端證明其身份。但是，EAP-TLS使用相互身份驗證，其中ACS (身份驗證、授權和記帳[AAA]) 伺服器和客戶端均具有證書並向彼此證明其身份。

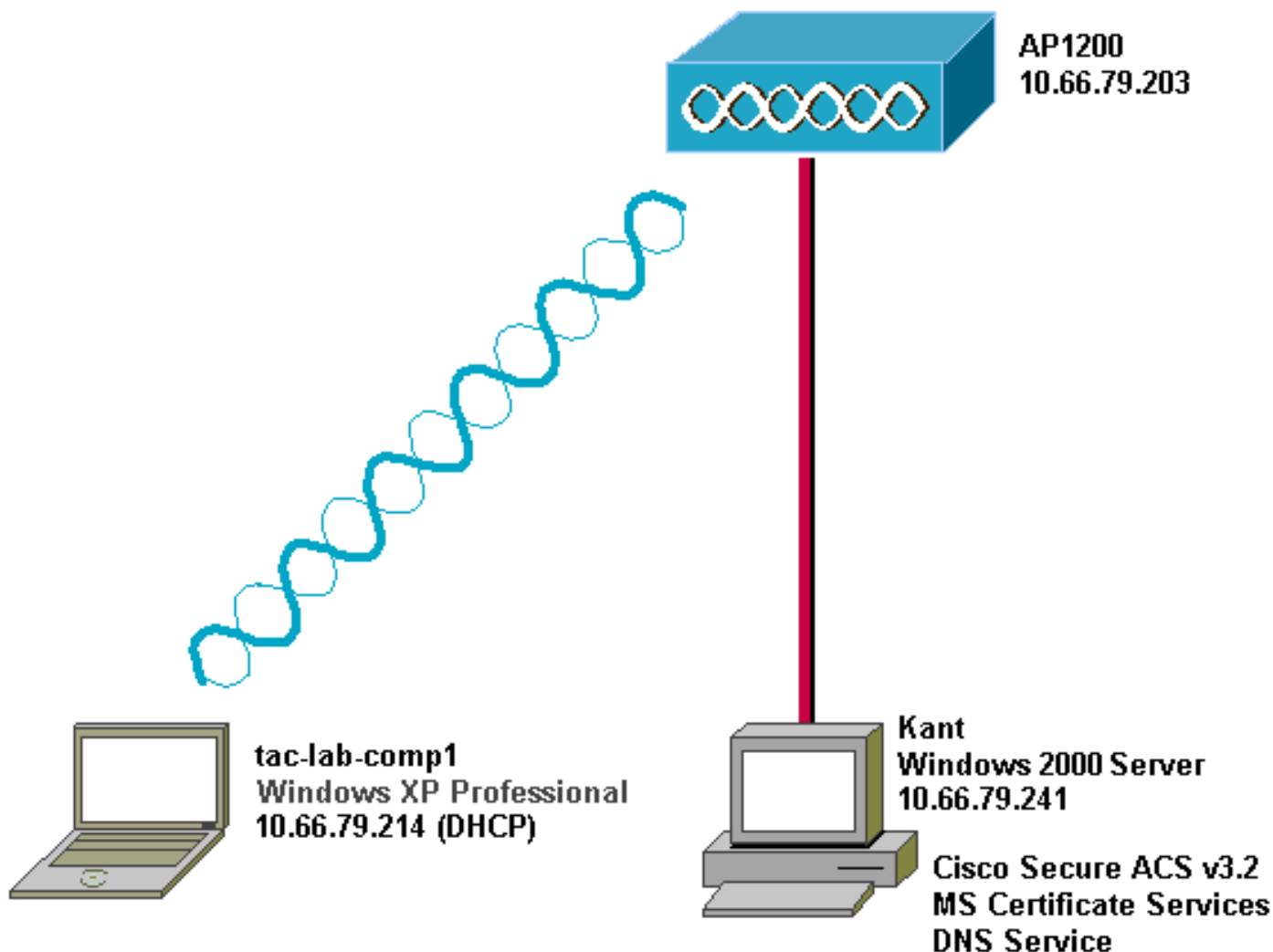
PEAP非常方便，因為客戶端不需要證書。EAP-TLS對驗證無頭裝置非常有用，因為證書不需要使用者互動。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

網路圖表

本文檔使用下圖所示的網路設定。



配置Cisco Secure ACS for Windows v3.2

按照以下步驟配置ACS 3.2。


1. [獲取ACS伺服器的證書。](#)
2. [配置ACS以使用來自儲存的證書。](#)
3. [指定ACS應信任的其他證書頒發機構。](#)
4. [重新啟動服務並在ACS上配置PEAP設定。](#)
5. [指定接入點並將其配置為AAA客戶端。](#)
6. [配置外部使用者資料庫。](#)
7. [重新啟動服務。](#)

獲取ACS伺服器的證書

請依照以下步驟操作，取得憑證。

1. 在ACS伺服器上，開啟Web瀏覽器，在位址列中輸入<http://CA-ip-address/certsrv>以瀏覽到CA伺服器。以管理員身份登入域。

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. 選擇 **Request a certificate** , 然後按一下 **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. 選擇 **Advanced request** , 然後按一下 **Next**。

Choose Request Type

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

User certificate request:

Advanced request

Next >

4. 選擇Submit a certificate request to this CA using a form，然後按一下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. 設定憑證選項。選擇**Web Server**作為證書模板。輸入ACS伺服器的名稱。

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OurACS

E-Mail:

Company:

Department:

City:

State:

Country/Region: US

將金鑰大

小設定為1024。選擇Mark keys as exportable和Use local machine store的選項。根據需要配置其他選項，然後按一下Submit。

Key Options:

CSP:

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:

注意：如果您看到一個警告視窗，該視窗涉及指令碼衝突（取決於瀏覽器的安全/隱私設定），請按一




下「是」繼續。

6. 按一下「Install this certificate」。

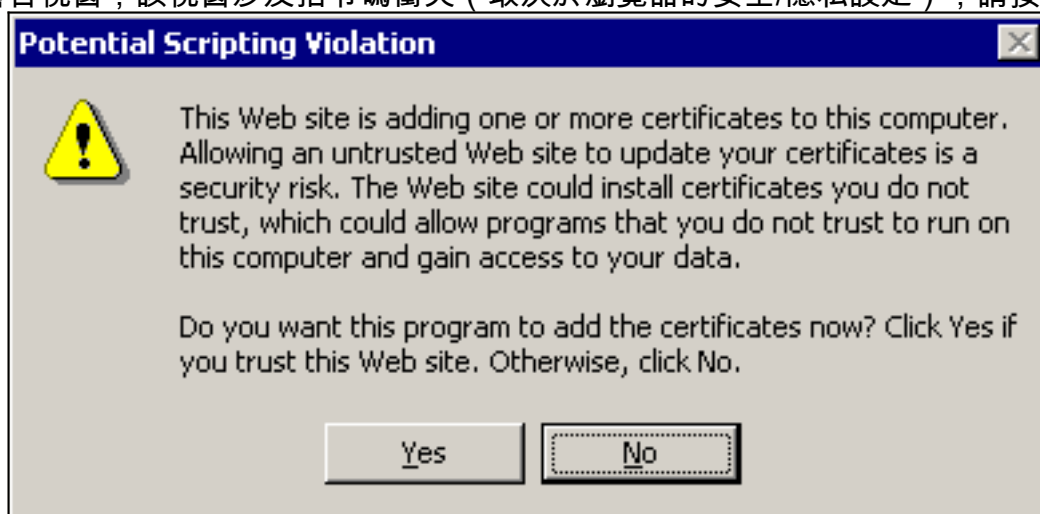
Microsoft Certificate Services -- Our TAC CA [Home](#)

Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

注意：如果您看到一個警告視窗，該視窗涉及指令碼衝突（取決於瀏覽器的安全/隱私設定），請按一



下「是」繼續。

7. 如果安裝成功，您將看到一條確認消息。

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

Certificate Installed

Your new certificate has been successfully installed.

[配置ACS以使用來自儲存的證書](#)

按照以下步驟配置ACS以使用儲存中的證書。

1. 開啟Web瀏覽器，在位址列中輸入<http://ACS-ip-address:2002/>以瀏覽到ACS伺服器。按一下 **System Configuration**，然後按一下 **ACS Certificate Setup**。
2. 按一下 **安裝ACS證書**。
3. 選擇 **Use certificate from storage**。在「Certificate CN」欄位中，輸入在[Obtain a Certificate for the ACS Server](#)一節的步驟5a中指派的憑證的名稱。按一下「**Submit**」。此條目必須與您在高級證書請求期間在「名稱」欄位中鍵入的名稱相匹配。是伺服器憑證主體欄位中的CN名稱；可以編輯伺服器證書以檢查此名稱。在本範例中，名稱是「OurACS」。不要輸入頒發者

的CN名稱。

The screenshot shows the Cisco System Configuration web interface. The left sidebar contains navigation menus: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "System Configuration" and "Edit". The current page is "Install ACS Certificate".

Install ACS Certificate

Install new certificate [?]

Read certificate from file

Certificate file []

Use certificate from storage

Certificate CN [OurACS]

Private key file []

Private key password []

[?] Back to Help

[Submit] [Cancel]

4. 配置完成後，您將看到一條確認消息，指示ACS伺服器的配置已更改。注意：此時不需要重新

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

Left sidebar menu items:
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation

啟動ACS。

[指定ACS應信任的其他證書頒發機構](#)

ACS將自動信任頒發其證書的CA。如果使用者端憑證是由額外的CA核發，則需要完成以下步驟。


1. 按一下**System Configuration**，然後按一下**ACS Certificate Setup**。
2. 按一下**ACS Certificate Authority Setup**，將CA新增到受信任證書清單中。在CA證書檔案的欄位中，輸入證書的位置，然後按一下**提交**。

CISCO SYSTEMS

System Configuration


Edit

ACS Certification Authority Setup

CA Operations 

Add new CA certificate to local certificate storage

CA certificate file

 **Back to Help**

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

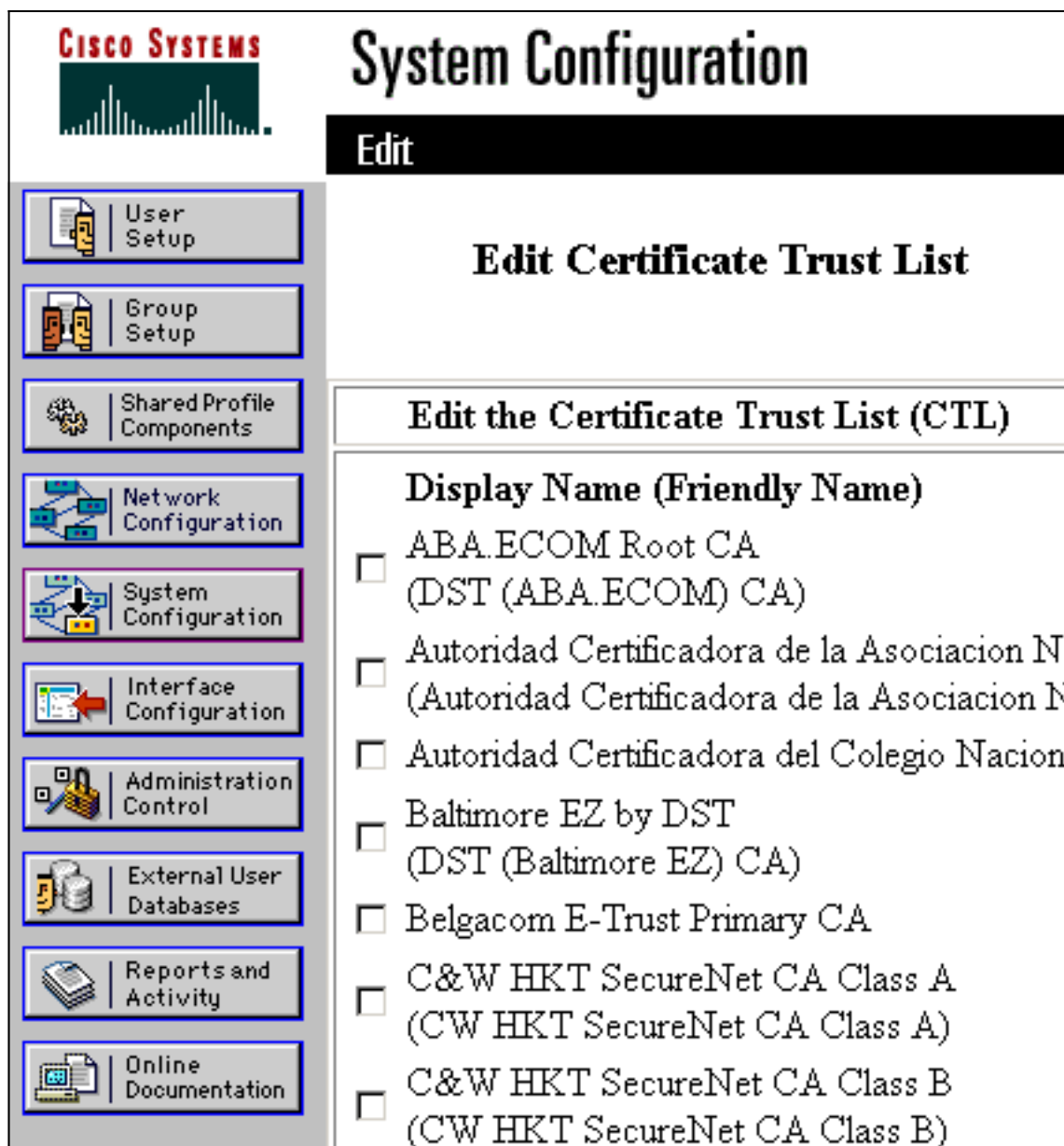
Administration Control

External User Databases

Reports and Activity

Online Documentation

3. 按一下「**Edit Certificate Trust List**」。檢查ACS應信任的所有CA，並取消檢查ACS不應信任的所有CA。按一下「**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)

[重新啟動服務並在ACS上配置PEAP設定](#)

按照以下步驟重新啟動服務並配置PEAP設定。

1. 按一下**System Configuration**，然後按一下**Service Control**。
2. 按一下**Restart**以重新啟動服務。
3. 要配置PEAP設定，請按一下**System Configuration**，然後按一下**Global Authentication Setup**。
4. 檢查下面顯示的兩個設定，並將所有其他設定保留為預設值。如果需要，可以指定其他設定，例如「啟用快速重新連線」。完成後，按一下**Submit**。**允許EAP-MSCHAPv2允許MS-CHAP版本2身份驗證註：有關快速連線的詳細資訊，請參閱系統配置中的「身份驗證配置選項」：[驗證與憑證](#)。**

