

# 適用於Windows v3.2的安全ACS，採用EAP-TLS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EAP-TLS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MS證書電腦自動註冊](#)

[配置思科接入點](#)

[配置無線客戶端](#)

[加入域](#)

[為使用者獲取證書](#)

[配置無線網路](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本檔案介紹如何使用Windows 3.2版的Cisco安全存取控制系統(ACS)設定可擴充驗證通訊協定 — 傳輸層安全(EAP-TLS)。

**注意：**Novell Certificate Authority(CA)不支援電腦身份驗證。ACS可以使用EAP-TLS支援對Microsoft Windows Active Directory進行電腦身份驗證。終端使用者客戶端可能會將使用者身份驗證協定限制為與電腦身份驗證相同的協定。也就是說，對電腦身份驗證使用EAP-TLS可能需要對使用者身份驗證使用EAP-TLS。有關電腦身份驗證的詳細資訊，請參閱*Cisco安全訪問控制伺服器 4.1使用手冊*的[電腦身份驗證](#)部分。

**注意：**設定ACS以通過EAP-TLS對電腦進行身份驗證時，已將ACS設定為電腦身份驗證，必須將客

戶端配置為僅執行電腦身份驗證。有關詳細資訊，請參閱[如何在Windows Vista、Windows Server 2008和Windows XP Service Pack 3中為基於802.1X的網路啟用僅電腦身份驗證](#)。

## [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](#)。
- DNS服務(帶有Service Pack 3的Windows 2000 Server和修補程式[服務323172](#)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](#)

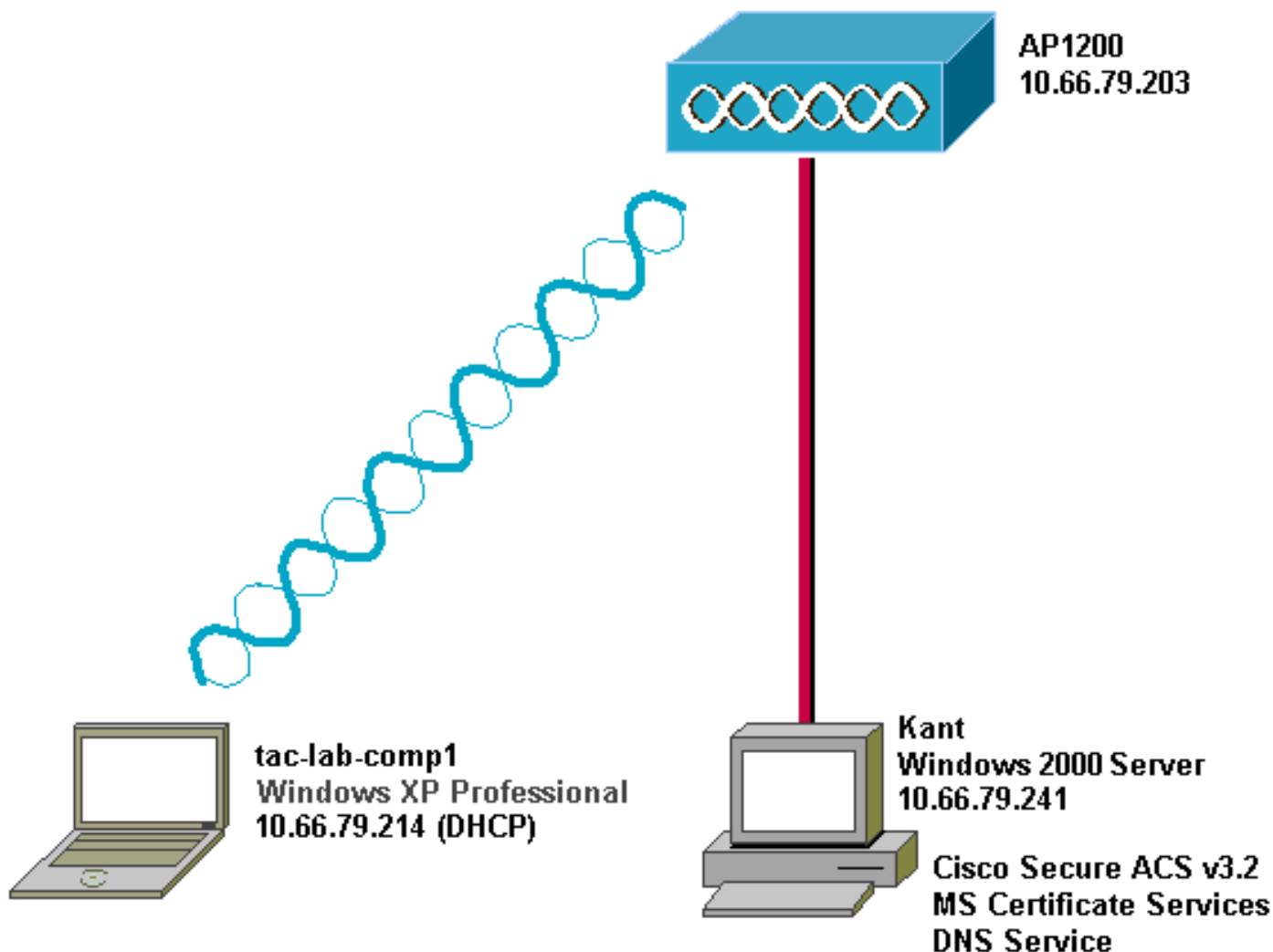
EAP-TLS和受保護的可擴展身份驗證協定(PEAP)都構建並使用TLS/安全套接字層(SSL)隧道。EAP-TLS使用相互身份驗證，其中ACS ( 身份驗證、授權和記帳[AAA] ) 伺服器和客戶端均具有證書並向彼此證明其身份。但是，PEAP僅使用伺服器端身份驗證；只有伺服器具有證書並向客戶端證明其身份。

### [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，輸入<http://CA-ip-address/certsrv>以訪問CA伺服器。
2. 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

3. 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 >


4. 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:

A rectangular selection box with a blue header containing the text "User Certificate". The main body of the box is empty.

Advanced request

---

Next >

5. 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 >

6. 設定憑證選項：選擇**Web Server**作為證書模板，然後輸入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

在Key

Size欄位中輸入1024，並選中Mark keys as exportable和Use local machine store覈取方塊。  
根據需要配置其他選項，然後按一下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 >

注意：如

果出現「潛在的指令碼衝突」對話方塊，請按一下「是」以繼續。



7. 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

果出現「潛在的指令碼衝突」對話方塊，請按一下「是」以繼續。

**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.

8. 如果安裝成功，則會顯示「證書已安裝」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](#)

完成這些步驟，配置ACS使用儲存中的證書。

1. 開啟Web瀏覽器，輸入<http://ACS-ip-address:2002/>以訪問ACS伺服器。
2. 按一下**System Configuration**，然後按一下**ACS Certificate Setup**。
3. 按一下**安裝ACS證書**。
4. 按一下**Use certificate from storage**單選按鈕。
5. 在「Certificate CN」欄位中，輸入您在本檔案[從ACS伺服器獲取證書](#)一節的步驟5a中指派的證書的名稱。
6. 按一下「**Submit**」。



# 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

Submit

Cancel

配置完成後，將出現一條確認消息，指示ACS伺服器的配置已更改。注意：此時不需要重新啟動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應信任的其他證書頒發機構](#)

ACS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，您必須完成以下步驟：


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。
3. 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**

4. 按一下「**Edit Certificate Trust List**」。
5. 檢查ACS應信任的所有CA，並取消檢查ACS不應信任的所有CA。
6. 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EAP-TLS設定](#)

完成以下步驟以重新啟動服務和配置EAP-TLS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EAP-TLS設定，請按一下**System Configuration**，然後按一下**Global Authentication Setup**。
4. 選中**Allow EAP-TLS**，然後選中一個或多個證書比較。
5. 按一下「**Submit**」。

