

# Cisco Secure ACS voor Windows v3.2 configureren met PEAP-MS-CHAPv2-machineverificatie

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Conventies](#)

[Netwerkdigram](#)

[Cisco Secure ACS voor Windows v3.2 configureren](#)

[Een certificaat voor de ACS-server verkrijgen](#)

[ACS configureren voor gebruik van een opslagcertificaat](#)

[Specificeer aanvullende certificeringsinstanties die de ACS moeten vertrouwen](#)

[Start de service opnieuw en stel PEAP-instellingen in voor de ACS](#)

[Het access point als een AAA-client specificeren en configureren](#)

[De externe gebruikersdatabases configureren](#)

[Start de service opnieuw](#)

[Cisco access point configureren](#)

[De draadloze client configureren](#)

[Instellen van een MS-certificaatmachineverklaring](#)

[Join the Domain](#)

[Installeer het wortelcertificaat handmatig op de Windows-client](#)

[De draadloze netwerken configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document toont aan hoe u het Protected Extensible Authentication Protocol (PEAP) kunt configureren met Cisco Secure ACS voor Windows versie 3.2.

Voor meer informatie over het configureren van beveiligde draadloze toegang via draadloze LAN-controllers, verwijzen Microsoft Windows 2003-software en Cisco Secure Access Control Server (ACS) 4.0 naar [PEAP onder Unified Wireless Networks met ACS 4.0 en Windows 2003](#).

## Voorwaarden

### Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de onderstaande software- en hardwareversies.

- Cisco Secure ACS voor Windows versie 3.2
- Microsoft certificaatservices (geïnstalleerd als autoriteit voor Enterprise root [CA])**Opmerking:** Raadpleeg voor meer informatie [de stapsgewijze gids voor het instellen van een certificeringsinstantie](#) .
- DNS-service met Windows 2000-server met Service Pack 3**Opmerking:** Als u CA Server-problemen ondervindt, installeert u [hotfix 323172](#) . De Windows 2000 SP3-client vereist [hotfix 313664](#) om IEEE 802.1x-verificatie in te schakelen.
- Cisco Aironet 1200 Series draadloos access point 12.01T
- IBM ThinkPad T30 met Windows XP Professional met Service Pack 1

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

### Achtergrondinformatie

Zowel PEAP als EAP-TLS bouwen en gebruiken een TLS/Secure Socket Layer (SSL)-tunnel. PEAP gebruikt alleen verificatie aan serverzijde; alleen de server heeft een certificaat en bewijst zijn identiteit aan de cliënt . EAP-TLS gebruikt echter wederzijdse authenticatie waarbij zowel de ACS-server (authenticatie, autorisatie en accounting [AAA]) als de klanten certificaten hebben en hun identiteit aan elkaar bewijzen.

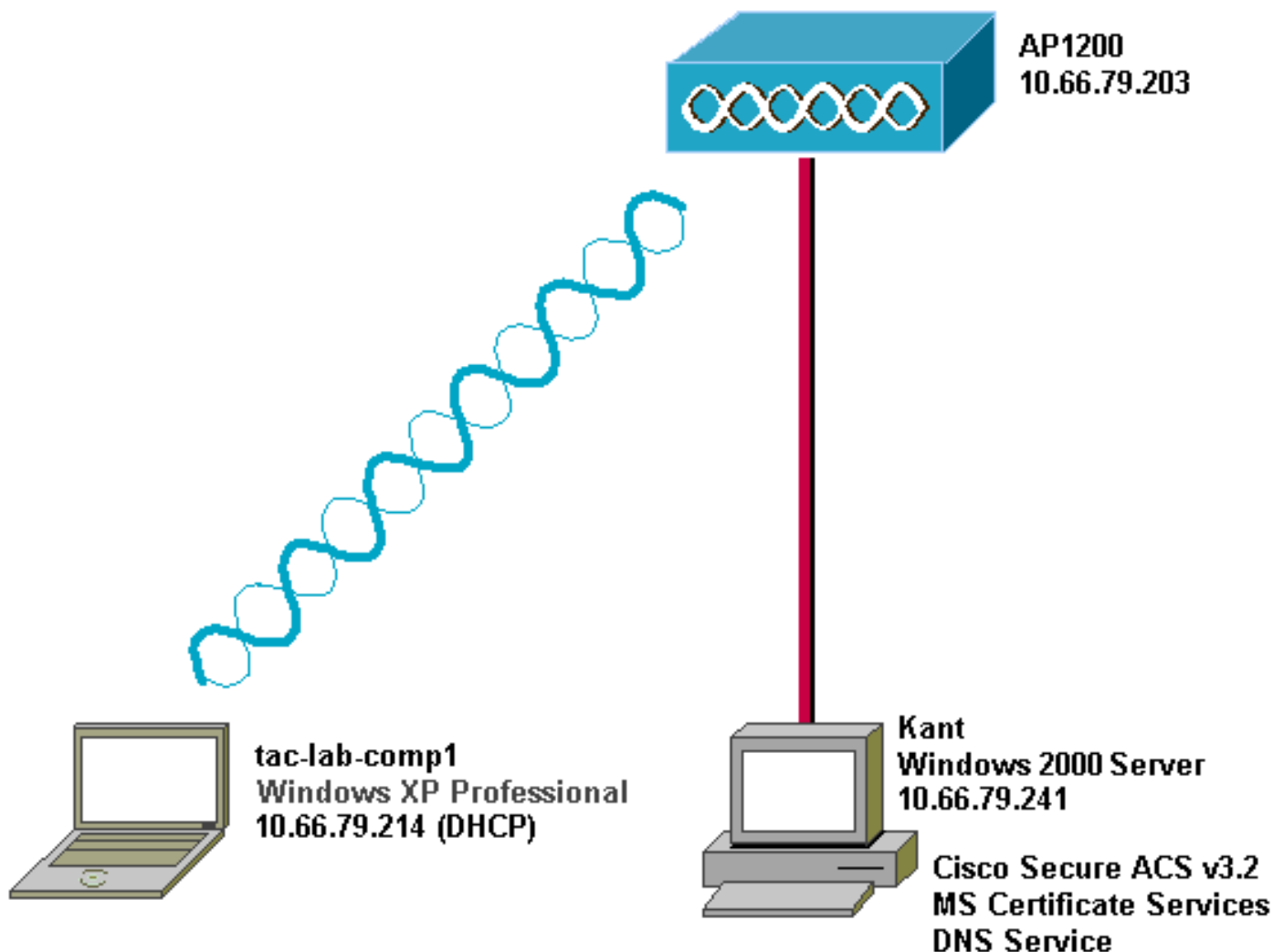
PEAP is handig omdat klanten geen certificaten nodig hebben. EAP-TLS is handig om koploze apparaten te authentifieren, omdat certificaten geen gebruikersinteractie vereisen.

### Conventies

Zie de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

### Netwerkdigram

Dit document gebruikt de netwerkinstellingen die in het onderstaande schema zijn weergegeven.



## Cisco Secure ACS voor Windows v3.2 configureren

Volg deze stappen om ACS 3.2 te configureren.

1. [Verkrijg een certificaat voor de ACS server.](#)
2. [ACS configureren om een opslagcertificaat te gebruiken.](#)
3. [Specificeer aanvullende certificeringsinstanties die de ACS moeten vertrouwen.](#)
4. [Start de service opnieuw en stel PEAP-instellingen in op de ACS.](#)
5. [Specificeer en configureren het access point als een AAA-client.](#)
6. [Het configureren van de externe gebruikersdatabases.](#)
7. [Start de service opnieuw.](#)

### Een certificaat voor de ACS-server verkrijgen

Volg deze stappen om een certificaat te verkrijgen.

1. Open op de ACS-server een webbrowser en blader naar de CA-server door **http:// CA-ip-adres/certsrv** in de adresbalk in te voeren. Meld u aan bij het domein als

**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

beheerder.

2. Selecteer **Een certificaat aanvragen** en klik vervolgens op **Volgende**.

**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. Selecteer **Geavanceerd verzoek** en klik vervolgens op

## Choose Request Type

---

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

User certificate request:

Advanced request

---

Next >

Volgende.

4. Selecteer een certificaataanvraag bij deze CA indienen met behulp van een formulier en klik vervolgens op

## 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 >

**Volgende.**

5. Configuratie van de certificeringsopties. Selecteer **Web Server** als de certificaatsjabloon. Voer de naam van de ACS-server

## Advanced Certificate Request

### Certificate Template:

Web Server

### Identifying Information For Offline Template:

Name: OurACS

E-Mail:

Company:

Department:

City:

State:

Country/Region: US

in.

Stel de

sluutelgrootte in op 1024. Selecteer de opties voor **Toetsen als exporteerbaar** en **gebruik de lokale machinewinkel**. Configureer de gewenste opties en klik vervolgens op

**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:

Indienen.

**Opmerking:** Als u een waarschuwingsvenster ziet dat verwijst naar een schending van het schrift (afhankelijk van de beveiligingsinstellingen/de privacy van uw browser), klikt u op **Ja**



om door te gaan.

6. Klik op **Installeer dit**




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

---

## Certificate Issued

---

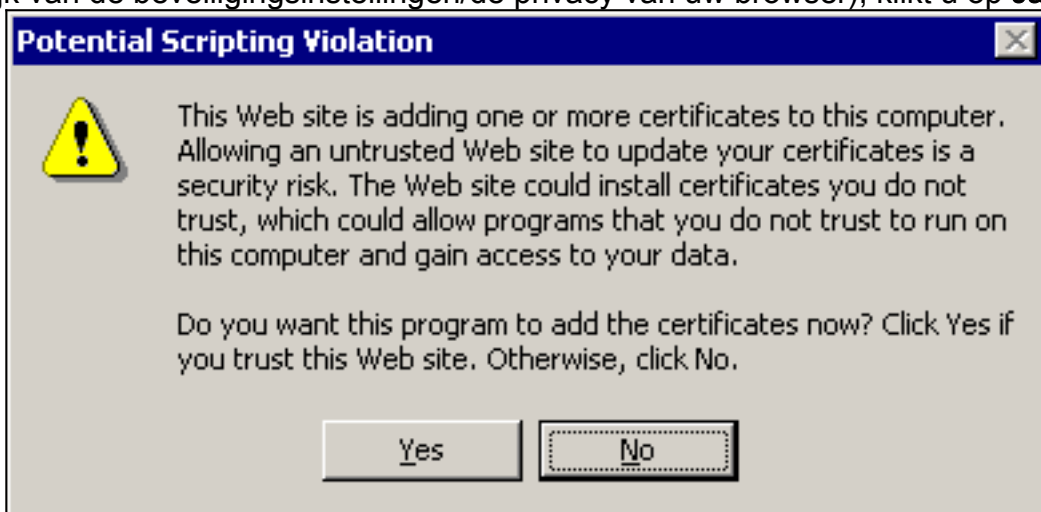
The certificate you requested was issued to you.

 [Install this certificate](#)

---

certificaat.

**Opmerking:** Als u een waarschuwingsvenster ziet dat verwijst naar een schending van het schrift (afhankelijk van de beveiligingsinstellingen/de privacy van uw browser), klikt u op **Ja**



om door te gaan.

7. Als de installatie is geslaagd, ontvangt u een bevestigingsbericht.

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

---

## Certificate Installed

---

Your new certificate has been successfully installed.

---

### [ACS configureren voor gebruik van een opslagcertificaat](#)

Volg deze stappen om ACS te configureren om het opgeslagen certificaat te gebruiken.

1. Open een webbrowser en blader naar de ACS-server door **http:// ACS-ip-adres** in te voeren:**2002/** in de adresbalk. Klik op **System Configuration** en vervolgens op **ACS-certificaatinstelling**.
2. Klik op **ACS-certificaat installeren**.
3. Selecteer **FineReader-certificaat gebruiken tijdens opslag**. Voer in het veld certificaatGN in

de naam van het certificaat dat u in stap 5a van de sectie hebt toegewezen, [een certificaat voor de ACS-server in](#). Klik op **Inzenden**. Deze ingang moet de naam overeenkomen die u in het veld Naam hebt getypt tijdens de geavanceerde certificaataanvraag. Het is de GN-naam in het onderwerpveld van het servercertificaat; U kunt het servercertificaat bewerken om deze naam te controleren. In dit voorbeeld is de naam "OurACS". Voer *geen* GN-naam van de uitgevende instelling

The screenshot shows the Cisco System Configuration web interface. On the left is a navigation menu with icons and labels for: 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". Below this is the "Install ACS Certificate" section. It contains a sub-section "Install new certificate" with a help icon. Two radio buttons are present: "Read certificate from file" (unselected) and "Use certificate from storage" (selected). Below the second radio button is a text input field labeled "Certificate CN" containing the text "OurACS". Below this are two more text input fields: "Private key file" and "Private key password", both currently empty. At the bottom of the form area is a yellow button with a question mark icon and the text "Back to Help". At the very bottom of the page are two buttons: "Submit" and "Cancel".

in.

4. Wanneer de configuratie is voltooid, ziet u een bevestigingsbericht dat aangeeft dat de configuratie van de ACS-server is gewijzigd. **Opmerking:** U hoeft het ACS-systeem op dit moment niet opnieuw te

**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

**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

starten.

### [Specificeer aanvullende certificeringsinstanties die de ACS moeten vertrouwen](#)

ACS zal automatisch vertrouwen hebben in de CA die haar eigen certificaat heeft afgegeven. Als de client-certificaten zijn afgegeven door extra CA's moet u de volgende stappen uitvoeren.


1. Klik op **System Configuration** en vervolgens op **ACS-certificaatinstelling**.
2. Klik op **ACS certificaatinstelling** om CA's aan de lijst van vertrouwde certificaten toe te voegen. Typ in het veld voor CA-certificaatbestand de locatie van het certificaat en klik vervolgens op

**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**

Inzenden.

3. Klik op **certificaatlijst bewerken**. Controleer alle CA's die de ACS moeten vertrouwen en verwijder alle CA's die de ACS niet moeten vertrouwen. Klik op

**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)

Inzenden.

## [Start de service opnieuw en stel PEAP-instellingen in voor de ACS](#)

Volg deze stappen om de service opnieuw te starten en de PEAP-instellingen te configureren.

1. Klik op **System Configuration** en vervolgens op **Service Control**.
2. Klik op **Start** opnieuw om de service te hervatten.
3. Als u PEAP-instellingen wilt configureren klikt u op **System Configuration** en vervolgens klikt u op **Global Authentication Setup**.
4. Controleer de twee onderstaande instellingen en laat alle andere instellingen standaard staan. Als u wilt, kunt u extra instellingen instellen, zoals Snel opnieuw aansluiten inschakelen. Klik op **Inzenden** als u klaar bent. **Toestaan van EAP-MSCHAPv2Laat MS-CHAP versie 2 verificatie toe**. **N.B.:** Raadpleeg voor meer informatie over Fast Connect "Verificatieopties" in [systeemconfiguratie: Verificatie en certificaten](#).

