

Secure ACS voor Windows v3.2 met EAP-TLS-machiniverificatie

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 de EAP-TLS-instellingen in op de ACS](#)

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

[De externe gebruikersdatabases configureren](#)

[Start de service opnieuw](#)

[De automatische inschrijving van de MS-certificaatmachine configureren](#)

[Het Cisco access point configureren](#)

[De draadloze client configureren](#)

[Join the Domain](#)

[Een certificaat voor de gebruiker verkrijgen](#)

[De draadloze netwerken configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft hoe u de EXTRA COMPUTER-beveiliging (EAP-TLS) voor verificatie kunt configureren met Cisco Secure Access Control System (ACS) voor Windows versie 3.2.

Opmerking: Machineechtheidscontrole wordt niet ondersteund door de autoriteit voor het Novell-certificaat (CA). ACS kan EAP-TLS gebruiken om machine-verificatie te ondersteunen in Microsoft Windows Active Directory. De eindgebruiker client kan het protocol voor gebruikersverificatie beperken tot hetzelfde protocol dat wordt gebruikt voor de verificatie van machines. Voor het gebruik van EAP-TLS voor de authenticatie van de machine zou het gebruik van EAP-TLS's voor gebruikersauthenticatie nodig kunnen zijn. Raadpleeg het gedeelte [Machineverificatie](#) van de *Gebruikershandleiding voor Cisco Secure Access Control Server 4.1* voor meer informatie over

machineverantwoording.

Opmerking: Bij het opzetten van ACS om machines via EAP-TLS te authenticeren en het ACS is ingesteld voor Machineverificatie, moet de klant zodanig zijn ingericht dat hij alleen machineverantwoording doet. Raadpleeg voor meer informatie [Hoe u alleen-computerverificatie kunt inschakelen voor een op 802.1X gebaseerd netwerk in Windows Vista, in Windows Server 2008 en in Windows XP Service Pack 3.](#)

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 servicepack 3 en [hotfix 323172](#)**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

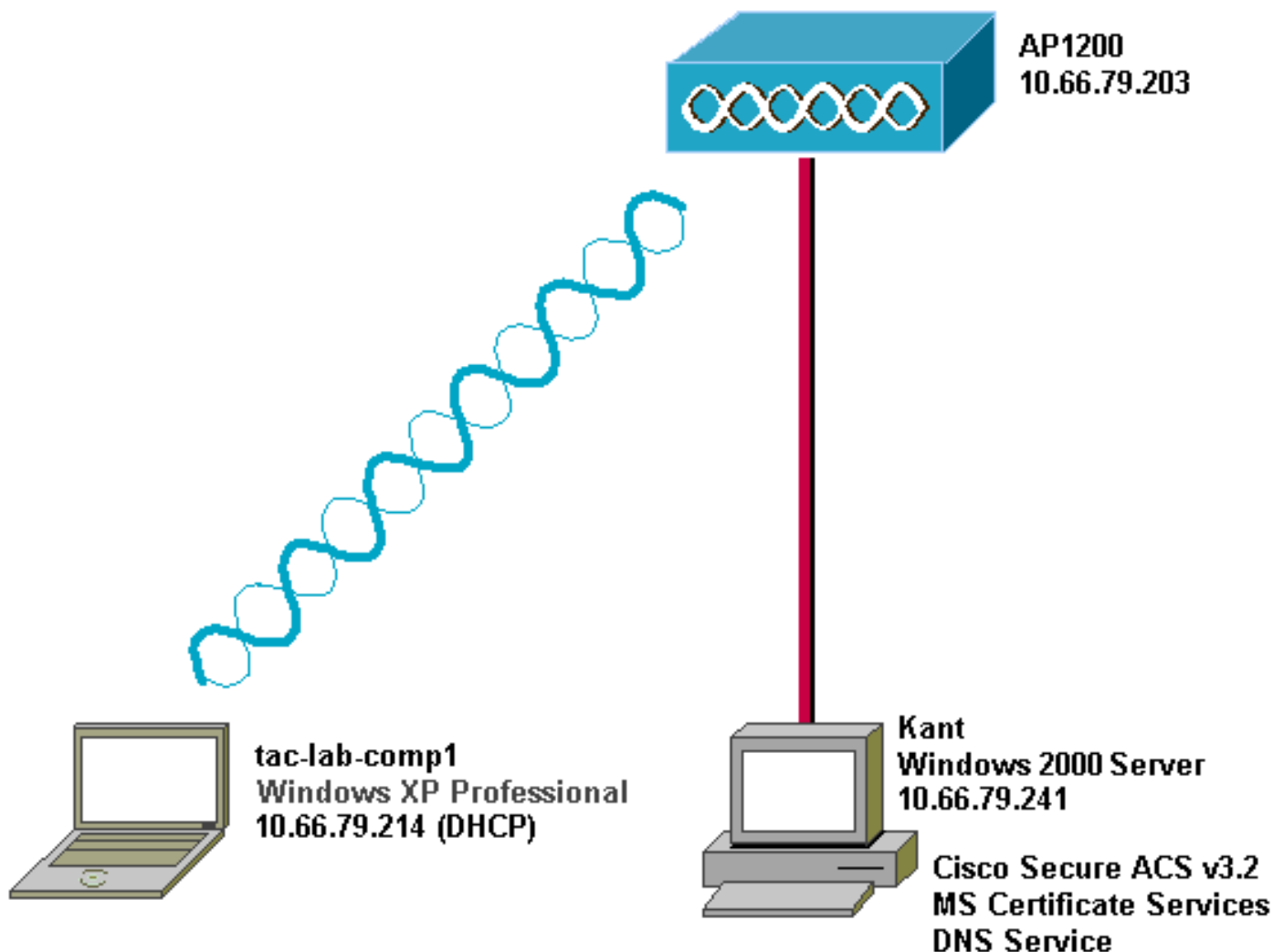
Zowel EAP-TLS als Protected Extensible Authentication Protocol (PEAP) bouwen en gebruiken een TLS/Secure Socket Layer (SSL)-tunnel. EAP-TLS maakt gebruik van wederzijdse authenticatie waarbij zowel de ACS-server (authenticatie, autorisatie en accounting [AAA]) als de klanten over certificaten beschikken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

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 de onderstaande 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 voer **http:// CA-ip-adres/certsrv** in om toegang te krijgen tot de CA-server.
2. 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.

3. 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 >

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

Choose Request Type

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

User certificate request:

A rectangular button with a blue header containing the text "User Certificate" and a white body area below it.

Advanced request

Next >

Volgende.

5. 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.

6. Configuratie van de certificeringsopties: Selecteer **Webserver** als de certificaatsjabloon en 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.

Typ

1024 in het veld Key Size en controleer de **Mark-toetsen als exportbaar** en **gebruik de vinkjes van de lokale machinewinkel**. Configureer de gewenste opties en klik vervolgens op

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:

Indienen.

N.B.: Als het dialoogvenster Potentiële Schending van de Schrift verschijnt, klikt u op **Ja** om




door te gaan.

7. Klik op **Installeer dit**

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

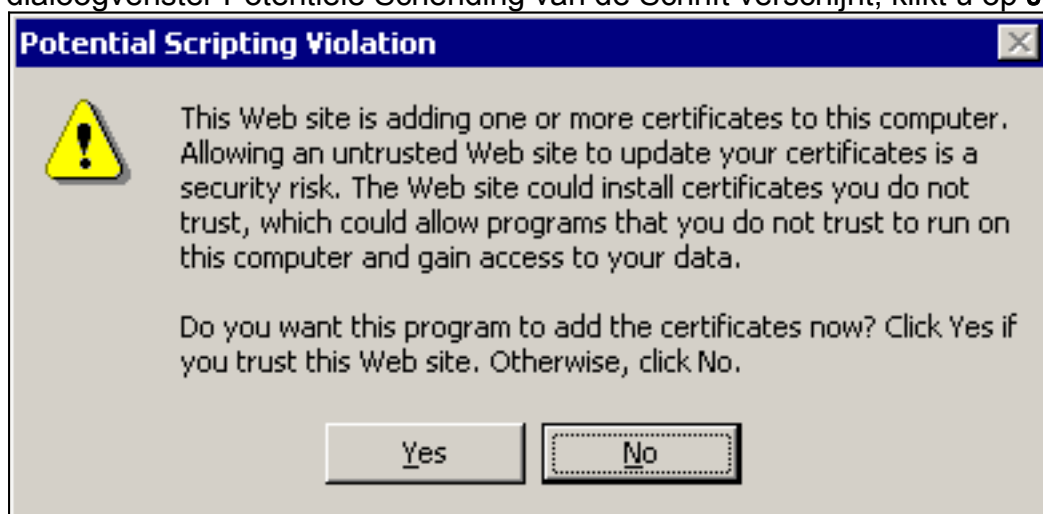
Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

certificaat.

N.B.: Als het dialoogvenster Potentiële Schending van de Schrift verschijnt, klikt u op Ja om



door te gaan.

8. Als de installatie geslaagd is, verschijnt het geïnstalleerde bericht van het Certificaat.

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

Certificate Installed

Your new certificate has been successfully installed.

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

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

1. Open een webbrowser en voer **http:// ACS-ip-adres in:2002/**om toegang te krijgen tot de ACS-server.
2. Klik op **System Configuration** en vervolgens op **ACS-certificaatinstelling**.
3. Klik op **ACS-certificaat installeren**.
4. Klik vanuit het keuzerondje **Storage op het certificaat**.
5. Voer in het veld certificaatGN de naam in van het certificaat dat u in stap 5a van het [vak](#)

[Certificaat verkrijgen van de ACS-server](#) van dit document hebt toegewezen.

6. Klik op

The screenshot shows the Cisco System Configuration web interface. On the left is a navigation menu with the following items: 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. There are two radio button options: 'Read certificate from file' and 'Use certificate from storage'. The 'Use certificate from storage' option is selected and circled in red. Below it, a text box labeled 'Certificate CN' contains the text 'OurACS' and is also circled in red. Further down are text boxes for 'Private key file' and 'Private key password'. At the bottom of the form are 'Submit' and 'Cancel' buttons. A yellow 'Back to Help' button with a question mark icon is located above the 'Submit' and 'Cancel' buttons.

Inzenden.

odra de configuratie is voltooid, verschijnt er 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 vertrouwt automatisch op de CA die haar eigen certificaat heeft afgegeven. Als de client-certificaten zijn afgegeven door extra CA's, moet u deze stappen voltooien:


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.
3. 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.

4. Klik op **certificaatlijst bewerken**.
5. Controleer alle CA's die de ACS moeten vertrouwen en verwijder alle CA's die de ACS niet moeten vertrouwen.
6. 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 de EAP-TLS-instellingen in op de ACS](#)

Voltooi deze stappen om de service te hervatten en stel de instellingen van EAP-TLS in:

1. Klik op **System Configuration** en vervolgens op **Service Control**.
2. Klik op **Start** opnieuw om de service te hervatten.
3. Klik om de instellingen van EAP-TLS te configureren op **System Configuration** en klik vervolgens op **Global Authentication Setup**.
4. Controleer **MAP-TLS toestaan** en controleer vervolgens een of meer van de certificaatvergelijkingen.
5. Klik op

