

# Konfigurieren von Cisco Secure ACS für Windows 3.2 mit PEAP-MS-CHAPv2-Computerauthentifizierung

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundtheorie](#)

[Konventionen](#)

[Netzwerkdiagramm](#)

[Konfigurieren von Cisco Secure ACS für Windows 3.2](#)

[Zertifikat für den ACS-Server abrufen](#)

[Konfigurieren des ACS zur Verwendung eines Zertifikats aus dem Speicher](#)

[Angaben zusätzlicher Zertifizierungsstellen, denen der ACS vertrauen sollte](#)

[Starten Sie den Dienst neu, und konfigurieren Sie PEAP-Einstellungen auf dem ACS.](#)

[Angaben und Konfigurieren des Access Points als AAA-Client](#)

[Konfigurieren der externen Benutzerdatenbanken](#)

[Starten Sie den Dienst neu](#)

[Konfigurieren des Cisco Access Points](#)

[Konfigurieren des Wireless-Clients](#)

[Konfigurieren der automatischen Registrierung des MS-Zertifikats](#)

[Beitreten zur Domäne](#)

[Installieren Sie das Stammzertifikat manuell auf dem Windows-Client.](#)

[Konfigurieren der Wireless-Netzwerke](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## [Einführung](#)

Dieses Dokument veranschaulicht, wie das Protected Extensible Authentication Protocol (PEAP) mit Cisco Secure ACS für Windows 3.2 konfiguriert wird.

Weitere Informationen zur Konfiguration eines sicheren Wireless-Zugriffs mithilfe von Wireless LAN-Controllern, der Microsoft Windows 2003-Software und dem Cisco Secure Access Control Server (ACS) 4.0 finden Sie [unter Unified Wireless Networks with ACS 4.0 and Windows 2003 in PEAP](#).

# Voraussetzungen

## Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und Hardwareversionen.

- Cisco Secure ACS für Windows Version 3.2
- Microsoft Certificate Services (installiert als Enterprise Root Certificate Authority [CA])**Hinweis:** Weitere Informationen finden Sie im [schrittweisen Handbuch zum Einrichten einer Zertifizierungsstelle](#) .
- DNS-Dienst mit Windows 2000 Server mit Service Pack 3**Hinweis:** Wenn Probleme mit CA Server auftreten, installieren Sie [Hotfix 323172](#) . Der Windows 2000 SP3 Client benötigt [Hotfix 313664](#) , um die IEEE 802.1x-Authentifizierung zu aktivieren.
- Cisco Aironet 12.01T Wireless Access Point der Serie 1200
- IBM ThinkPad T30 mit Windows XP Professional und Service Pack 1

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

## Hintergrundtheorie

Sowohl PEAP als auch EAP-TLS erstellen und verwenden einen TLS/Secure Socket Layer (SSL)-Tunnel. PEAP verwendet nur serverseitige Authentifizierung. Nur der Server verfügt über ein Zertifikat und beweist seine Identität gegenüber dem Client. EAP-TLS verwendet jedoch die gegenseitige Authentifizierung, bei der sowohl der ACS-Server (Authentication, Authorization, Accounting [AAA]) als auch die Clients Zertifikate besitzen und ihre Identität gegenseitig nachweisen.

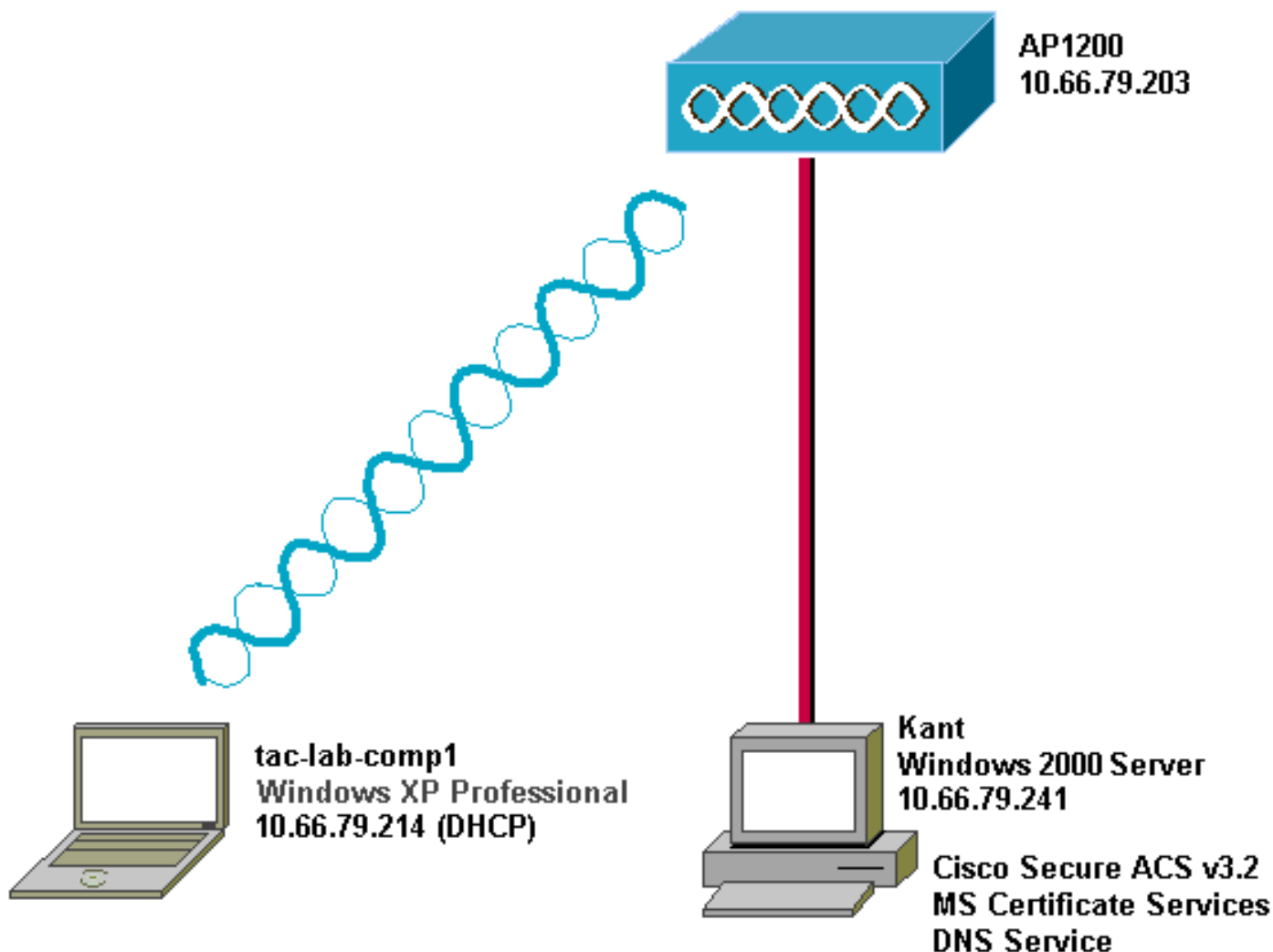
PEAP ist praktisch, da Clients keine Zertifikate benötigen. EAP-TLS eignet sich für die Authentifizierung von Headless-Geräten, da Zertifikate keine Benutzerinteraktion erfordern.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

## Netzwerkdigramm

In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



## Konfigurieren von Cisco Secure ACS für Windows 3.2

Führen Sie die folgenden Schritte aus, um ACS 3.2 zu konfigurieren.

1. [Erhalten Sie ein Zertifikat für den ACS-Server.](#)
2. [Konfigurieren des ACS zur Verwendung eines Zertifikats aus dem Speicher.](#)
3. [Geben Sie zusätzliche Zertifizierungsstellen an, denen der ACS vertrauen soll.](#)
4. [Starten Sie den Dienst neu, und konfigurieren Sie PEAP-Einstellungen auf dem ACS.](#)
5. [Angaben und Konfigurieren des Access Points als AAA-Client.](#)
6. [Konfigurieren Sie die externen Benutzerdatenbanken.](#)
7. [Starten Sie den Dienst neu.](#)

### Zertifikat für den ACS-Server abrufen

Befolgen Sie diese Schritte, um ein Zertifikat zu erhalten.

1. Öffnen Sie auf dem ACS-Server einen Webbrowser, und navigieren Sie zum CA-Server, indem Sie **http://CA-ip-address/certsrv** in die Adressleiste eingeben. Melden Sie sich als Administrator bei der Domäne

**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

an.

2. Wählen Sie **Zertifikat anfordern aus**, und klicken Sie dann auf

**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 >

Weiter.

3. Wählen Sie **Erweiterte Anforderung aus**, und klicken Sie dann auf

## Choose Request Type

---

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

User certificate request:

Advanced request

---

Next >

Weiter.

4. Wählen Sie eine Zertifikatsanforderung an diese Zertifizierungsstelle mithilfe eines Formulars **senden aus**, und klicken Sie dann auf

## 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 >

Weiter.

5. Konfigurieren Sie die Zertifikatoptionen. Wählen Sie **Webserver** als Zertifikatsvorlage aus. Geben Sie den Namen des ACS-Servers

## Advanced Certificate Request

### Certificate Template:

### Identifying Information For Offline Template:

ein.

Legen

Sie die Schlüssellänge auf **1024 fest**. Wählen Sie die Optionen für **Schlüssel als exportierbar markieren** und **Lokalen Maschinenspeicher verwenden aus**. Konfigurieren Sie nach Bedarf weitere Optionen, und klicken Sie dann auf

**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:**

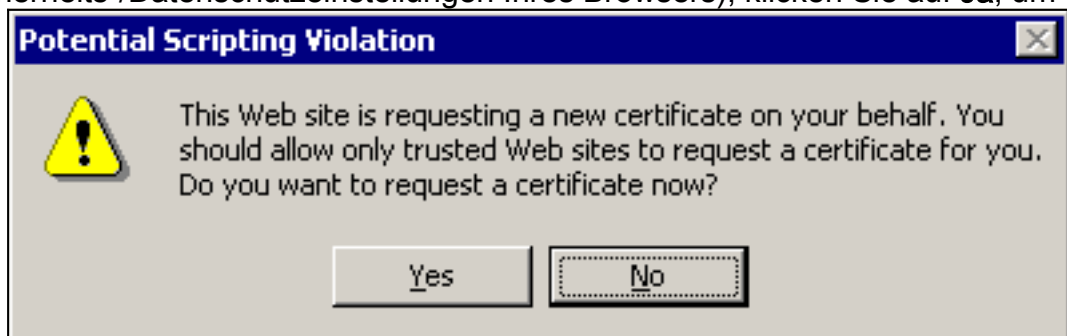
Hash Algorithm:  Only used to sign request.

Save request to a PKCS #10 file

Attributes:

Senden.

**inweis:** Wenn Sie ein Warnfenster sehen, das auf eine Skriptverletzung verweist (abhängig von den Sicherheits-/Datenschutzeinstellungen Ihres Browsers), klicken Sie auf **Ja**, um



fortzufahren.

6. Klicken Sie auf **Zertifikat installieren**.




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

---

## Certificate Issued

---

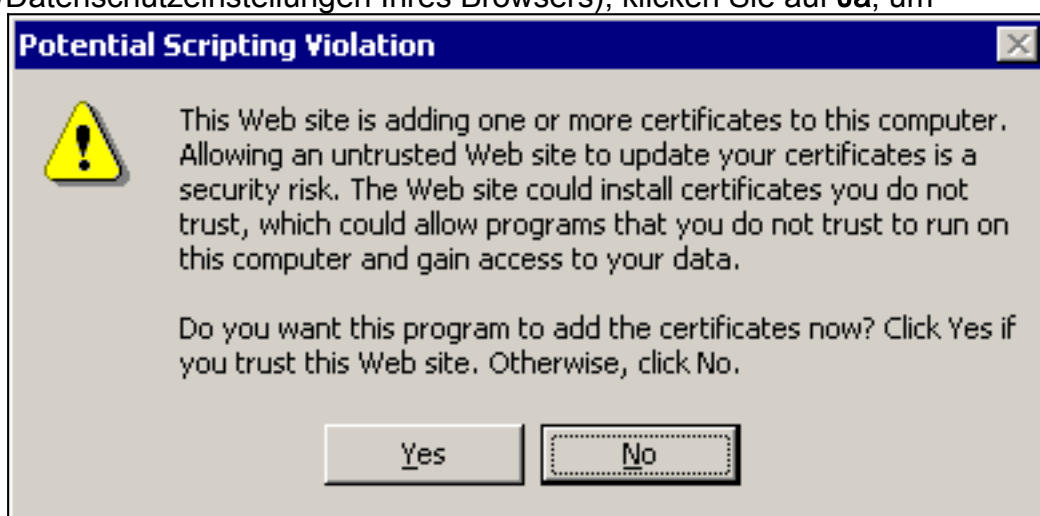
The certificate you requested was issued to you.

 [Install this certificate](#)

---

Hinweis:

Wenn Sie ein Warnfenster sehen, das auf eine Skriptverletzung verweist (abhängig von den Sicherheits-/Datenschutzeinstellungen Ihres Browsers), klicken Sie auf **Ja**, um



fortzufahren.

7. Wenn die Installation erfolgreich war, wird eine Bestätigungsmeldung angezeigt.

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

---

## Certificate Installed

---

Your new certificate has been successfully installed.

---

### [Konfigurieren des ACS zur Verwendung eines Zertifikats aus dem Speicher](#)

Befolgen Sie diese Schritte, um ACS für die Verwendung des Zertifikats im Speicher zu konfigurieren.

1. Öffnen Sie einen Webbrowser, und navigieren Sie zum ACS-Server, indem Sie **http://ACS-ip-address:2002/** in die Adressleiste eingeben. Klicken Sie auf **Systemkonfiguration** und dann auf **ACS Certificate Setup**.
2. Klicken Sie auf **ACS-Zertifikat installieren**.

3. Wählen Sie **Zertifikat aus Speicher verwenden aus**. Geben Sie im Feld Certificate CN den Namen des Zertifikats ein, das Sie in Schritt 5a des Abschnitts [Obtain a Certificate for the ACS Server](#) zugewiesen haben. Klicken Sie auf **Senden**. Dieser Eintrag muss mit dem Namen übereinstimmen, den Sie bei der erweiterten Zertifikatsanforderung im Feld Name eingegeben haben. Es ist der CN-Name im Betrefffeld des Serverzertifikats. Sie können das Serverzertifikat bearbeiten, um nach diesem Namen zu suchen. In diesem Beispiel lautet der Name "OurACS". Geben Sie *nicht* den KN-Namen des Emittenten

The screenshot shows the Cisco Systems System Configuration interface. The left sidebar contains navigation options: 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 primary heading is "Install ACS Certificate". Below this is a section titled "Install new certificate" with a help icon. Two radio buttons are present: "Read certificate from file" (unselected) and "Use certificate from storage" (selected). The "Use certificate from storage" option is circled in red. Below it, the "Certificate CN" field is also circled in red and contains the text "OurACS". Further down are fields for "Private key file" and "Private key password". At the bottom of the form area is a yellow "Back to Help" button. At the very bottom of the page are "Submit" and "Cancel" buttons.

ein.

4. Wenn die Konfiguration abgeschlossen ist, wird eine Bestätigungsmeldung angezeigt, dass die Konfiguration des ACS-Servers geändert wurde. **Hinweis:** Sie müssen den ACS derzeit nicht neu

**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.**

starten.

### Angeben zusätzlicher Zertifizierungsstellen, denen der ACS vertrauen sollte

Der ACS vertraut automatisch der Zertifizierungsstelle, die ein eigenes Zertifikat ausgestellt hat. Wenn die Client-Zertifikate von zusätzlichen Zertifizierungsstellen ausgestellt werden, müssen Sie die folgenden Schritte ausführen.

1. Klicken Sie auf **Systemkonfiguration** und dann auf **ACS Certificate Setup**.
2. Klicken Sie auf **ACS Certificate Authority Setup**, um der Liste der vertrauenswürdigen Zertifikate CAs hinzuzufügen. Geben Sie im Feld für Zertifizierungsstellenzertifikatdatei den Speicherort des Zertifikats ein, und klicken Sie dann auf

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. On the left side, there is a vertical navigation menu with the following items: "User Setup", "Group Setup", "Shared Profile Components", "Network Configuration", "System Configuration" (highlighted with a red border), "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". At the bottom of the main content area is a yellow button with a question mark icon and the text "Back to Help".

Senden.

3. Klicken Sie auf **Liste der Zertifikatsvertrauenslisten bearbeiten**. Überprüfen Sie alle CAs, denen der ACS vertrauen soll, und deaktivieren Sie alle CAs, denen der ACS nicht vertrauen darf. Klicken Sie auf

**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)

Senden.

[Starten Sie den Dienst neu, und konfigurieren Sie PEAP-Einstellungen auf dem ACS.](#)

Befolgen Sie diese Schritte, um den Dienst neu zu starten und PEAP-Einstellungen zu konfigurieren.

1. Klicken Sie auf **Systemkonfiguration** und dann auf **Dienststeuerung**.
2. Klicken Sie auf **Neu starten**, um den Dienst neu zu starten.
3. Um PEAP-Einstellungen zu konfigurieren, klicken Sie auf **Systemkonfiguration** und dann auf **Globales Authentifizierungs-Setup**.
4. Aktivieren Sie die beiden unten angezeigten Einstellungen, und belassen Sie alle anderen Einstellungen als Standard. Auf Wunsch können Sie zusätzliche Einstellungen festlegen, z. B. Fast Reconnect aktivieren. Wenn Sie fertig sind, klicken Sie auf **Senden.EAP-MSCHAPv2 zulassenMS-CHAP-Authentifizierung Version 2 zulassenHinweis: Weitere Informationen zu Fast Connect finden Sie unter "Authentication Configuration Options" (Authentifizierungskonfigurationsoptionen) in der [Systemkonfiguration: Authentifizierung und Zertifikate](#).**

