

Sicherer ACS für Windows v3.2 mit EAP-TLS- 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 die EAP-TLS-Einstellungen auf dem ACS.](#)

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

[Konfigurieren der externen Benutzerdatenbanken](#)

[Starten Sie den Dienst neu](#)

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

[Konfigurieren des Cisco Access Points](#)

[Konfigurieren des Wireless-Clients](#)

[Beitreten zur Domäne](#)

[Zertifikat für den Benutzer abrufen](#)

[Konfigurieren der Wireless-Netzwerke](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) mit dem Cisco Secure Access Control System (ACS) für Windows 3.2 konfigurieren.

Hinweis: Die Maschinenauthentifizierung wird von der Novell Certificate Authority (CA) nicht unterstützt. ACS kann EAP-TLS verwenden, um die Systemauthentifizierung für Microsoft Windows Active Directory zu unterstützen. Der Endbenutzer-Client kann das Protokoll für die Benutzerauthentifizierung auf dasselbe Protokoll beschränken, das für die Computerauthentifizierung verwendet wird. Das heißt, die Verwendung von EAP-TLS für die maschinelle Authentifizierung kann die Verwendung von EAP-TLS für die

Benutzerauthentifizierung erfordern. Weitere Informationen zur Computerauthentifizierung finden Sie im Abschnitt [Computerauthentifizierung](#) im *Benutzerhandbuch für Cisco Secure Access Control Server 4.1*.

Hinweis: Wenn der ACS für die Authentifizierung von Computern über EAP-TLS eingerichtet wurde und der ACS für die maschinelle Authentifizierung eingerichtet wurde, muss der Client so konfiguriert werden, dass er nur die maschinelle Authentifizierung durchführt. Weitere Informationen finden Sie unter [Aktivieren der Nur-Computer-Authentifizierung für ein 802.1X-basiertes Netzwerk in Windows Vista, Windows Server 2008 und Windows XP Service Pack 3](#).

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 und [Hotfix 323172](#)**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

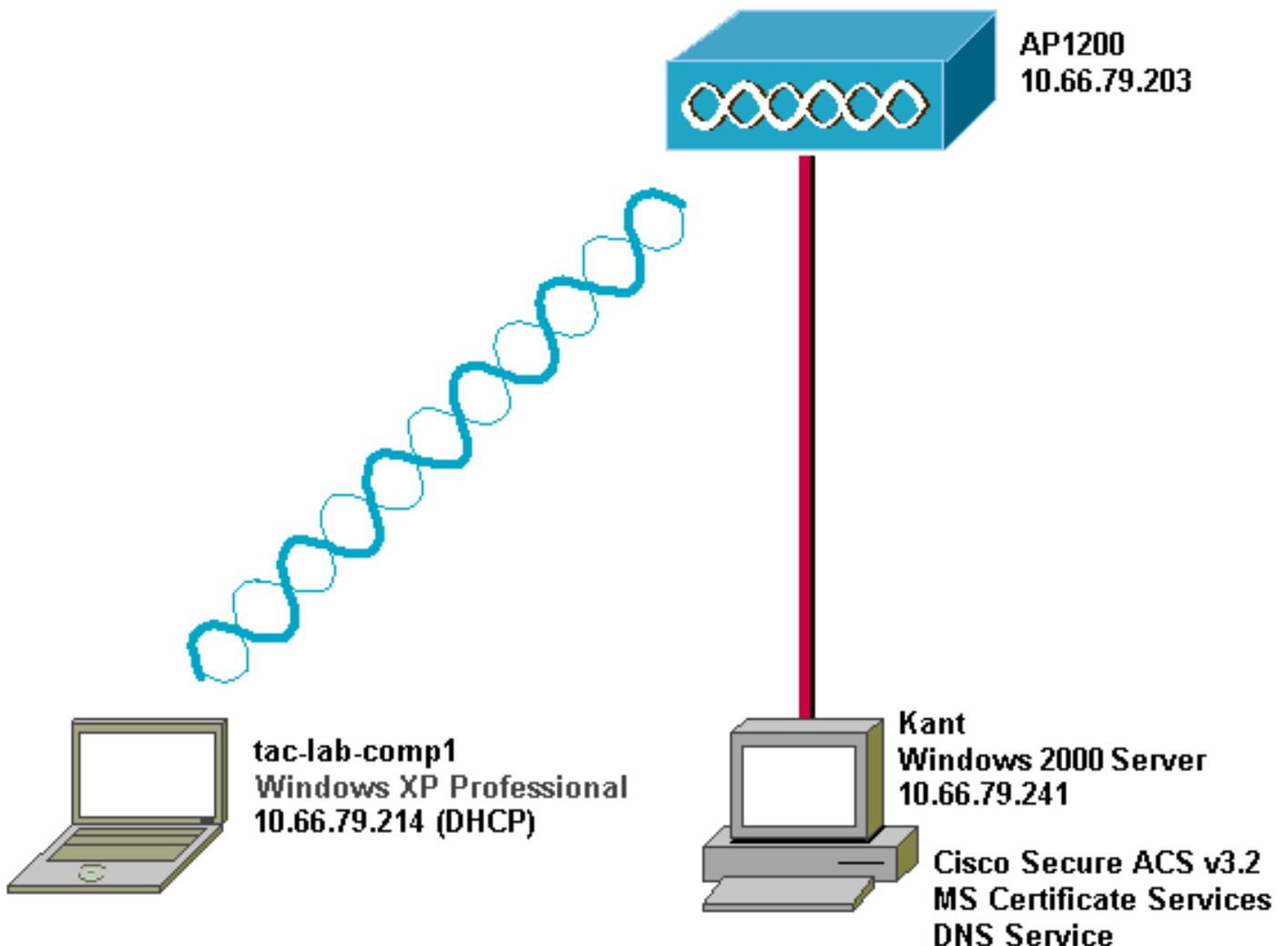
Sowohl EAP-TLS als auch Protected Extensible Authentication Protocol (PEAP) erstellen und verwenden einen TLS/Secure Socket Layer (SSL)-Tunnel. EAP-TLS verwendet gegenseitige Authentifizierung, bei der sowohl der ACS-Server (Authentication, Authorization, Accounting [AAA]) als auch die Clients Zertifikate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

Konventionen

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

Netzwerkdiagramm

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



Konfigurieren von Cisco Secure ACS für Windows 3.2

Folgen Sie den Schritten unten, 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 geben Sie **<http://CA-ip-address/certsrv>** ein, um auf den CA-Server zuzugreifen.

2. Melden Sie sich als Administrator bei der Domäne



Enter Network Password

Please type your user name and password.

Site: 10.66.79.241

User Name Administrator

Password xxxxxx

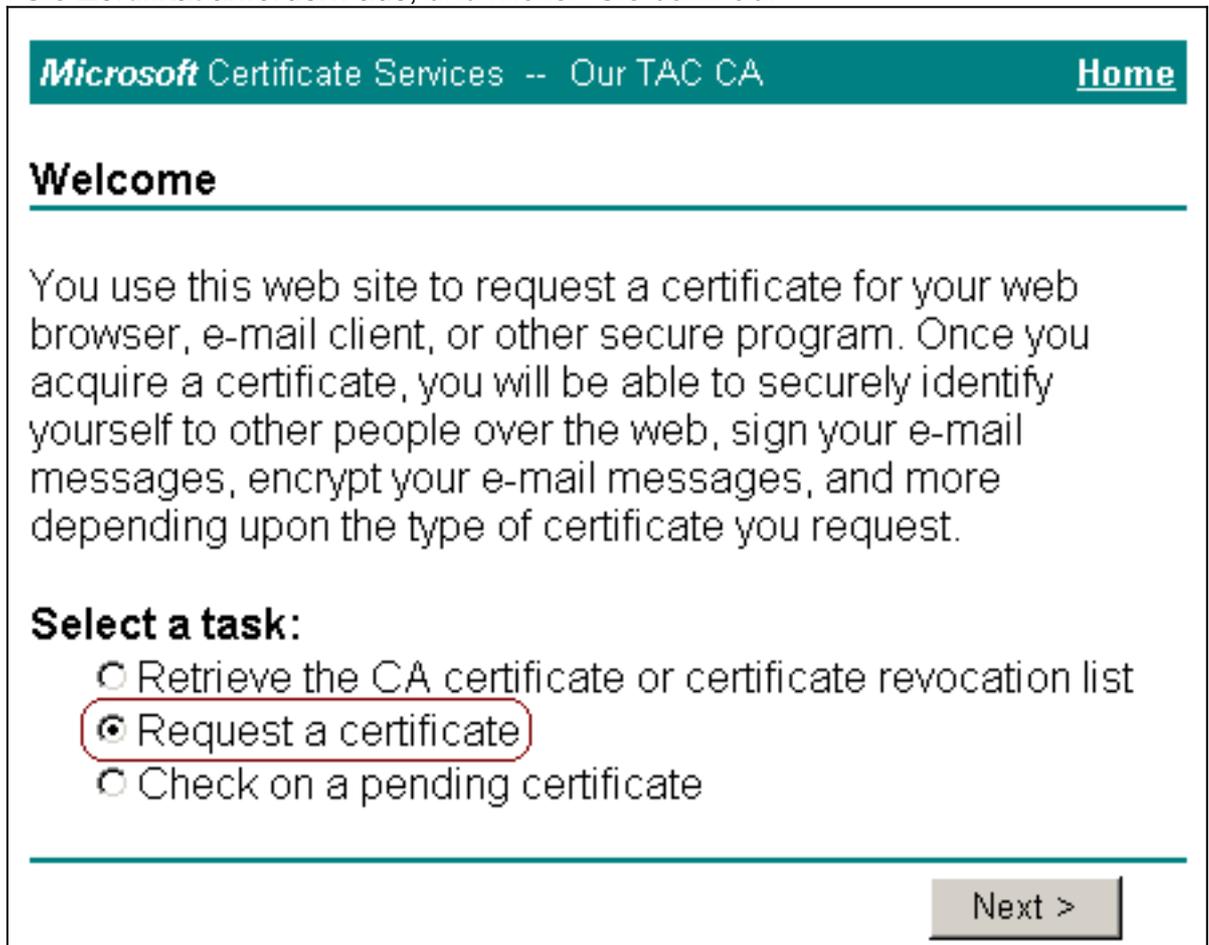
Domain SEC-SYD

Save this password in your password list

OK Cancel

an.

3. 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.

4. 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.

5. 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.

6. Konfigurieren Sie die Zertifikatoptionen: Wählen Sie **Webserver** als Zertifikatsvorlage aus, und geben Sie den Namen des ACS-Servers

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OurACS

E-Mail:

Company:

Department:

City:

State:

Country/Region: US

ein.

Gebe

n Sie **1024** im Feld Schlüsselgröße ein, und aktivieren Sie die Kontrollkästchen **Schlüssel als exportierbar markieren** und **Lokalen Maschinenspeicher verwenden**. 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 das Dialogfeld "Potenzielle Skriptverstöße" angezeigt wird, klicken Sie zum



Fortfahren auf Ja.

7. 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 das Dialogfeld "Potenzielle Skriptverstöße" angezeigt wird, klicken Sie zum Fortfahren



auf Ja.

8. Wenn die Installation erfolgreich war, wird die Meldung Certificate Installed (Zertifikat installiert) 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](#)

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

1. Öffnen Sie einen Webbrowser, und geben Sie **http://ACS-ip-address:2002/** ein, um auf den ACS-Server zuzugreifen.
2. Klicken Sie auf **Systemkonfiguration** und dann auf **ACS Certificate Setup**.
3. Klicken Sie auf **ACS-Zertifikat installieren**.

4. Klicken Sie auf das Optionsfeld **Zertifikat vom Speicher verwenden**.
5. Geben Sie im Feld Certificate CN (CN-Zertifikat) den Namen des Zertifikats ein, das Sie in Schritt 5a des Abschnitts [Obtain a Certificate From the ACS Server](#) (Zertifikat vom ACS-Server [beziehen](#)) dieses Dokuments zugewiesen haben.
6. Klicken Sie auf

CISCO SYSTEMS

System Configuration

Edit

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

Senden.

Nach Abschluss der Konfiguration wird eine Bestätigungsmeldung angezeigt, die anzeigt, dass die Konfiguration des ACS-Servers geändert wurde. **Hinweis:** Sie müssen den ACS derzeit nicht neu

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.

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.
3. Geben Sie im Feld für Zertifizierungsstellenzertifikatdatei den Speicherort des Zertifikats ein, und klicken Sie dann auf

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

Senden.

4. Klicken Sie auf **Liste der Zertifikatsvertrauenslisten bearbeiten**.
5. Überprüfen Sie alle CAs, denen der ACS vertrauen soll, und deaktivieren Sie alle CAs, denen der ACS nicht vertrauen darf.
6. 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 Nacional
- 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 die EAP-TLS-Einstellungen auf dem ACS.](#)

Gehen Sie wie folgt vor, um den Service neu zu starten und die EAP-TLS-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 EAP-TLS-Einstellungen zu konfigurieren, klicken Sie auf **Systemkonfiguration** und dann auf **Globales Authentifizierungs-Setup**.
4. Aktivieren Sie **EAP-TLS zulassen**, und überprüfen Sie dann einen oder mehrere Zertifikatvergleiche.
5. Klicken Sie auf

