

PEAP-MS-CHAPv2 マシン認証が設定された Cisco Secure ACS for Windows v3.2

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景理論](#)

[表記法](#)

[ネットワーク図](#)

[設定 Cisco Secure ACS for Windows v3.2](#)

[ACS サーバ用の証明書を取得する](#)

[ストレージから証明書を使用するよう ACS を設定する](#)

[ACS が信頼する必要のある追加の認証局を指定する](#)

[サービスを再起動し、ACS での PEAP の設定を設定する](#)

[アクセス ポイントを AAA クライアントとして指定および設定する](#)

[外部ユーザ データベースを設定する](#)

[サービスを再起動する](#)

[Cisco アクセスポイントを設定して下さい](#)

[無線クライアントの設定](#)

[MS 認証 マシン autoenrollment を設定して下さい](#)

[ドメインに参加する](#)

[Windows クライアントでルート証明書を手動でインストールする](#)

[ワイヤレス ネットワーキングを設定する](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この文書では、Cisco Secure ACS for Windows バージョン 3.2 を使用して、Protected Extensible Authentication Protocol (PEAP) を設定する方法を説明します。

ワイヤレス LAN コントローラを使用してセキュア ワイヤレスアクセスを、Microsoft Windows 2003 ソフトウェア設定する方法に関する詳細についてはおおよび [Cisco Secure Access Control Server \(ACS \) 4.0 は ACS 4.0 および Windows 2003 が付いている Unified Wireless Network の下で、PEAP を示します。](#)

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Secure ACS for Windows バージョン 3.2
- Microsoft Certificate Services (エンタープライズのルート証明機関 [CA] としてインストールされている) 注: 詳細については、[認証局のセットアップに関する手順ガイド](#) を参照してください。
- Service Pack 3 をインストールした Windows 2000 Server を使った DNS サービス注: CA サーバの問題が発生した場合は、[ホットフィックス 323172](#) をインストールします。[Windows 2000 SP3 クライアントでは、ホットフィックス 313664](#) を適用しないと IEEE 802.1x 認証を有効にできません。
- Cisco Aironet 1200 シリーズ Wireless Access Point 12.01T
- Service Pack 1 を適用済みの Windows XP Professional を実行する IBM ThinkPad T30

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景理論

PEAP と EAP-TLS は両方とも TLS/Secure Socket Layer (SSL) トンネルを構築して、使用します。PEAP はサーバ側の認証だけ使用します; サーバだけが証明書を所有し、その ID をクライアントに証明します。しかし EAP-TLS では、ACS (Authentication, Authorization, and Accounting (AAA; 認証、認可、およびアカウントिंग)) サーバとクライアントの両方が証明書を用意し、相互に ID を証明する相互認証を使用します。

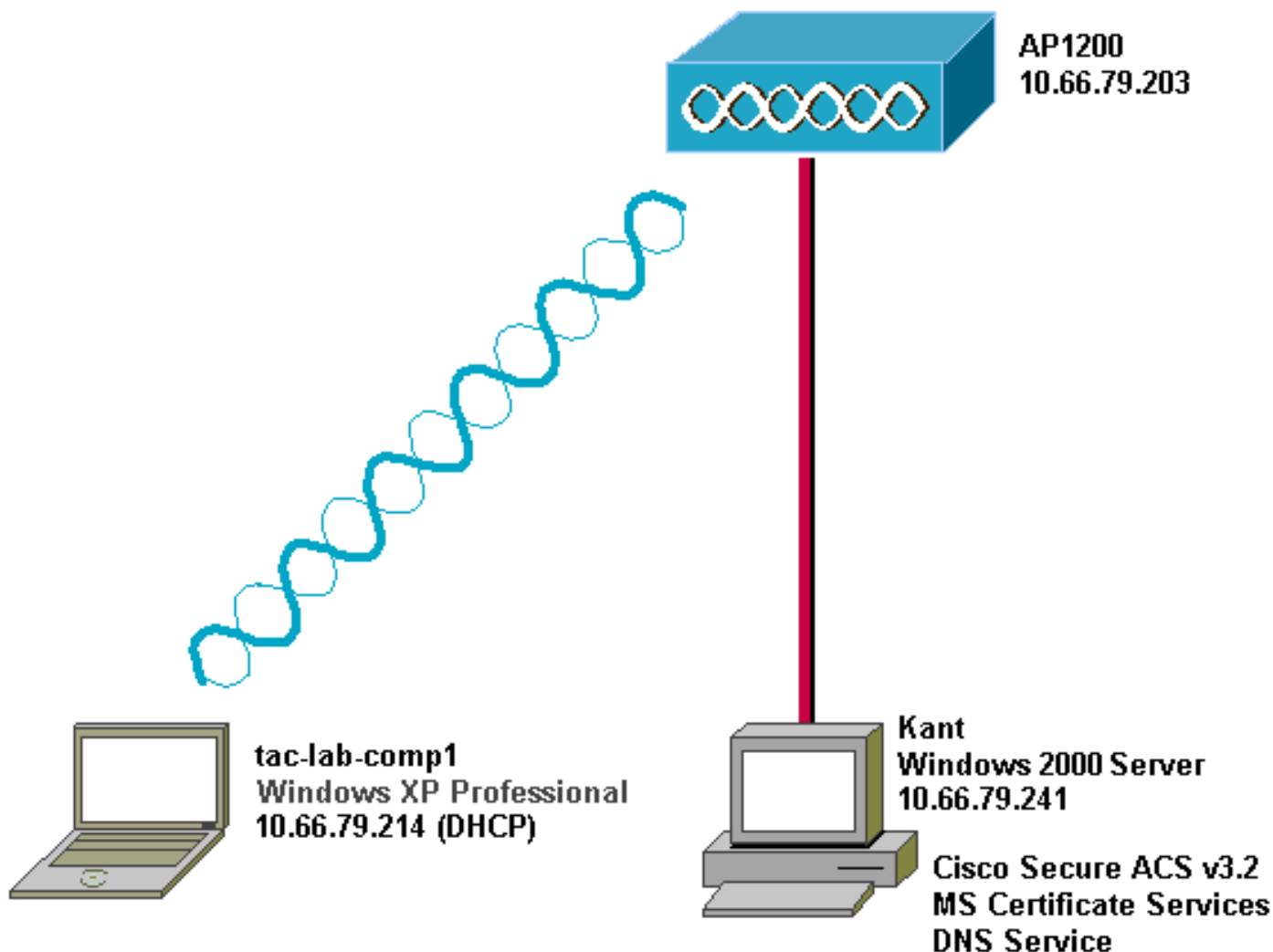
クライアントが証明書を必要としないため、PEAP は便利です。EAP-TLS は、証明書がユーザからのインタラクションを必要とないため、認証を行うヘッドレス デバイスでは有用です。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

ネットワーク図

このドキュメントでは次の図に示すネットワーク



設定 Cisco Secure ACS for Windows v3.2

ACS 3.2 を設定するために次の手順に従って下さい。


1. [ACS サーバ用の証明書を取得する。](#)
2. [ストレージから証明書を使用するよう ACS を設定する。](#)
3. [ACS が信頼する必要のある追加の認証局を指定する。](#)
4. [サービスを再起動し、ACS での EAP-TLS 設定を構成する。](#)
5. [アクセスポイントを AAA クライアントとして指定および設定する。](#)
6. [外部ユーザ データベースを設定する。](#)
7. [サービスを再起動する。](#)

ACS サーバ用の証明書を取得する

証明書を取得するには、次のステップに従います。

1. ACS サーバで Web ブラウザを開き、アドレスバーに `http://CA-ip-address/certsrv` と入力して CA サーバを表示します。Administrator としてドメインにログインします。

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

2. [Request a certificate] を選択してから [Next] をクリックします。

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. [Advanced request] を選択してから [Next] をクリックします。

Choose Request Type

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

User certificate request:

Advanced request

Next >

4. [Submit a certificate request to this CA using a form] を選択してから [Next] をクリックしま

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 >

す。

5. 証明書のオプションを設定します。証明書のテンプレートとして Web Server を選択します。ACS サーバの名前を入力します。

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OurACS

E-Mail:

Company:

Department:

City:

State:

Country/Region: US

鍵のサイ

ズを 1024 に設定します。 Mark keys as exportable と Use local machine store のオプションを選択します。 必要に応じてその他のオプションを設定し、[Submit] をクリックします。

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:

注: (ブラウザのセキュリティ/プライバシー設定に応じて) スクリプト違反を通知する警告ウィンドウが表示された場合は、Yes をクリックして続きます。




6. [Install this certificate] をクリックします。

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

Certificate Issued


The certificate you requested was issued to you.

 [Install this certificate](#)

注: (ブラ

ウザのセキュリティ/プライバシー設定に応じて) スクリプト違反を通知する警告ウィンドウが表示された場合は、Yes をクリックして継続します。

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.

7. インストールに成功した場合は、確認メッセージが表示されます。

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

Certificate Installed

Your new certificate has been successfully installed.

[ストレージから証明書を使用するよう ACS を設定する](#)

ストレージにある証明書を使用するよう ACS を設定するには、次のステップに従います。

1. Web ブラウザを開き、アドレス バーに `http://ACS-ip-address:2002/` と入力して ACS サーバを表示します。 [System Configuration] をクリックし、 [ACS Certificate Setup] をクリックします。
2. [Install ACS Certificate] をクリックします。
3. Use certificate from storage を選択します。 Certificate CN フィールドでは、セクションのステップ 5a で [得る ACS サーバのための認証](#) を割り当てた認証の名前を入力して下さい。

[Submit] をクリックします。ここで入力する情報は、高度な証明書の要求時に Name フィールドにタイプした名前と同じである必要があります。それはサーバ証明の Subject フィールドの CN 名前です; この名前があるように確認するためにサーバ証明を編集できます。この例では、この名前は「OurACS」です。発行者の CN 名は入力しないでください。

The screenshot shows the Cisco Systems System Configuration interface. The main title is "System Configuration" with a "Cisco SYSTEMS" logo. Below the title is a black bar with the word "Edit" in white. A vertical sidebar on the left contains several menu items: "User Setup", "Group Setup", "Shared Profile Components", "Network Configuration", "System Configuration" (highlighted with a blue border), "Interface Configuration", "Administration Control", "External User Databases", "Reports and Activity", and "Online Documentation". The main content area is titled "Install ACS Certificate" and contains a form for "Install new certificate". The form has two radio buttons: "Read certificate from file" (unselected) and "Use certificate from storage" (selected). Below the selected option is a text input field for "Certificate CN" with the value "OurACS". There are also input fields for "Certificate file", "Private key file", and "Private key password". A yellow "Back to Help" button is located below the form. At the bottom of the page are "Submit" and "Cancel" buttons.

4. 設定が完了すると、ACS サーバの設定が変更されたことを示す確認メッセージが表示されます。注: この時点では ACS を再起動する必要はありません。

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

ACS が信頼する必要のある追加の認証局を指定する

ACS は、独自の証明書を発行した CA を自動的に信頼します。クライアントの証明書が追加の CA により発行された場合は、次のステップを完了する必要があります。

1. [System Configuration] をクリックし、[ACS Certificate Setup] をクリックします。
2. ACS Certificate Authority Setup をクリックして、信頼された証明書のリストに CA を追加します。CA 証明書ファイル用のフィールドに証明書の場所を入力し、[Submit] をクリックし

The screenshot shows the Cisco System Configuration web 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. The left sidebar contains a vertical menu of configuration options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted in purple), 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 "Add new CA certificate to local certificate storage" is displayed. Below the text is a text input field labeled "CA certificate file". At the bottom of the main content area is a yellow button with a help icon and the text "Back to Help".

ます。

3. Edit Certificate Trust List をクリックします。ACS が信頼するすべての CA にチェックマークを付け、ACS が信頼しないすべての CA のチェックマークを外します。[Submit] をクリックします。

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)

サービスを再起動し、ACS での PEAP の設定を設定する

サービスを再開し、PEAP 設定を行うために次の手順に従って下さい。

1. [System Configuration] をクリックし、[Service Control] をクリックします。
2. Restart をクリックしてサービスを再起動します。
3. PEAP の設定を設定するには、System Configuration をクリックしてから Global Authentication Setup をクリックします。
4. 次に示す 2 つの設定をチェックし、その他の設定をデフォルトのままにします。必要に応じて、Enable Fast Reconnect などの追加設定を設定できます。設定を終えたら [Submit] をクリックします。Allow EAP-MSCHAPv2 Allow MS-CHAP Version 2 Authentication 注: [Fast Connect](#) の詳細については、『システム設定：認証と証明書』の「認証設定オプション」を参照してください。

