

EAP-TLS マシン認証を使用する Windows v3.2 の Secure ACS

目次

[はじめに](#)

[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](#)

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

[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 EAP-TLS 設定を構成する](#)

[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](#)

[MS 証明書のマシン自動登録の設定](#)

[シスコ アクセス ポイントの設定](#)

[ワイヤレス クライアントの設定](#)

[ドメインに参加する](#)

[ユーザ用の証明書を取得する](#)

[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](#)

はじめに

このドキュメントでは、Cisco Secure Access Control System (ACS) for Windows バージョン 3.2 を使用して、Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) を設定する方法を説明します。

注: Novell 認証局 (CA) によるマシン認証はサポートされません。ACS は、EAP-TLS を使用して、Microsoft Windows Active Directory に対するマシン認証をサポートすることができます。エンドユーザ クライアントは、ユーザ認証のプロトコルを、マシン認証に使用するプロトコルと同じものに制限する場合があります。その場合、マシン認証に EAP-TLS を使用するとしたら、ユーザ認証にも EAP-TLS を使用する必要があります。マシン認証に関する詳細については、『Cisco Secure Access Control Server 4.1 ユーザ ガイド』の「[マシン認証](#)」のセクションを参照し

てください。

注: EAP-TLS でマシンを認証するように ACS をセットアップする場合、その ACS がマシン認証用にセットアップされているとしたら、クライアントをマシン認証専用に変更する必要があります。詳細については、「[Windows Vista、Windows Server 2008、および Windows XP Service Pack 3 で、802.1X ベースのネットワーク用のコンピューターのための認証を有効にする方法](#)」を参照してください。

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 および[ホットフィックス 323172](#) を適用済みの Windows 2000 Server を使用した 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、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが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

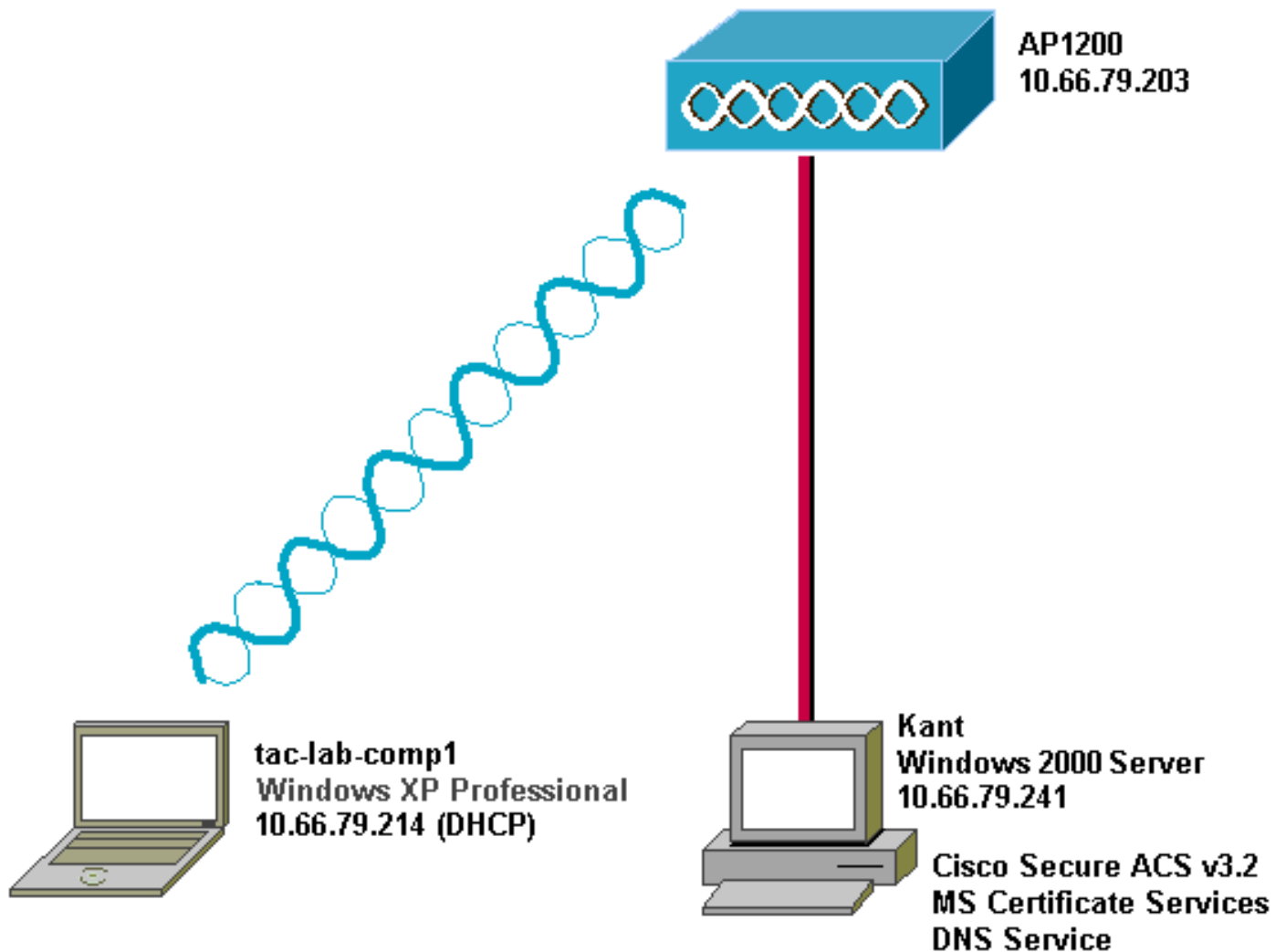
EAP-TLS と Protected Extensible Authentication Protocol (PEAP) は両方とも、TLS/Secure Socket Layer (SSL; セキュア ソケット レイヤ) トンネルを構築し、使用します。EAP-TLS では、ACS (Authentication, Authorization, and Accounting (AAA; 認証、認可、およびアカウントリング)) サーバとクライアントの両方が証明書を用意し、相互に ID を証明する相互認証を使用します。ただし、PEAP が使用するのはサーバ側の認証だけです。サーバだけが証明書を所有し、その ID をクライアントに証明します。

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



Cisco Secure ACS for Windows v3.2 の設定

ACS 3.2 を設定するには、次のステップに従います。


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 が信頼する必要が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、CA サーバにアクセスするためにアドレスバーに `http://CA-ip-address/certsrv` と入力します。
2. 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

3. [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

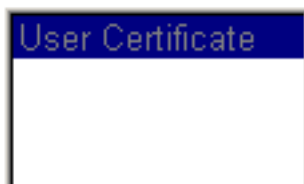
Next >

4. [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:

A rectangular selection box with a blue header containing the text "User Certificate". The main body of the box is empty.

Advanced request

Next >

5. [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。

6. 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、ACS サーバの名前を入力します。

Advanced Certificate Request

Certificate Template:

Identifying Information For Offline Template:

[Key Size]

フィールドに **1024** と入力し、[Mark keys as exportable] および [Use local machine store] チェックボックスをオンにします。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: 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:

Submit >

注

: [Potential Scripting Violation] ダイアログボックスが表示されたら、[Yes] をクリックして続




行します。

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

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

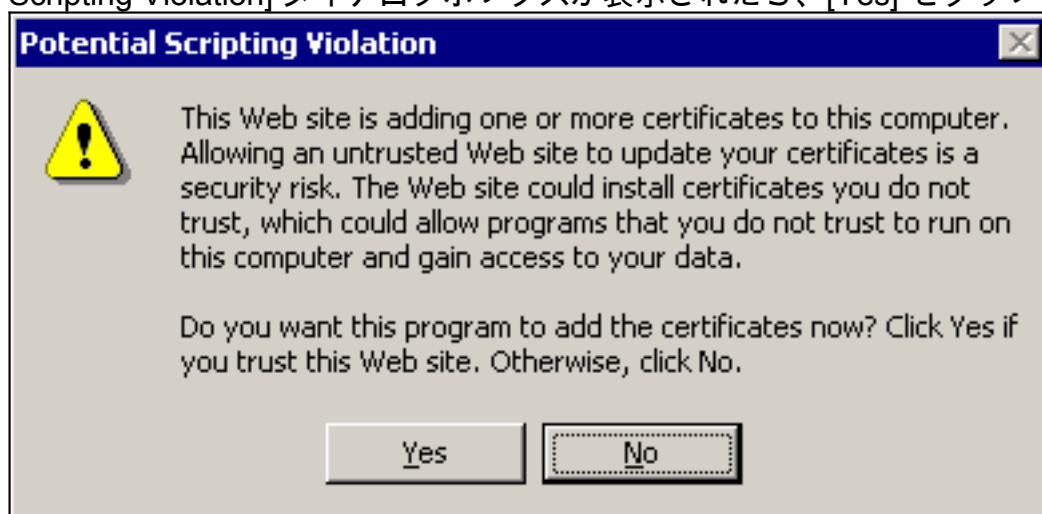
Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

注

: [Potential Scripting Violation] ダイアログボックスが表示されたら、[Yes] をクリックして続



行します。

8. インストールが正常に完了すると、[Certificate Installed] 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、ACS サーバにアクセスするためにアドレス バーに `http://ACS-ip-address:2002/` と入力します。
2. [System Configuration] をクリックし、[ACS Certificate Setup] をクリックします。
3. [Install ACS Certificate] をクリックします。
4. [Use certificate from storage] オプション ボタンをクリックします。
5. [Certificate CN] フィールドに、このドキュメントの「[ACS サーバ用の証明書を取得する](#)」セクションのステップ 5a で割り当てた証明書の名前を入力します。

6. [Submit] をクリックします。

The screenshot shows the Cisco System Configuration web interface. The left sidebar contains navigation menus: 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 current page is "Install ACS Certificate". Under the heading "Install new certificate", 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, the "Certificate CN" field is filled with "OurACS" and is also circled in red. There are empty 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, there are "Submit" and "Cancel" buttons.

設定が完了

すると、ACS サーバの設定が変更されたことを通知する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

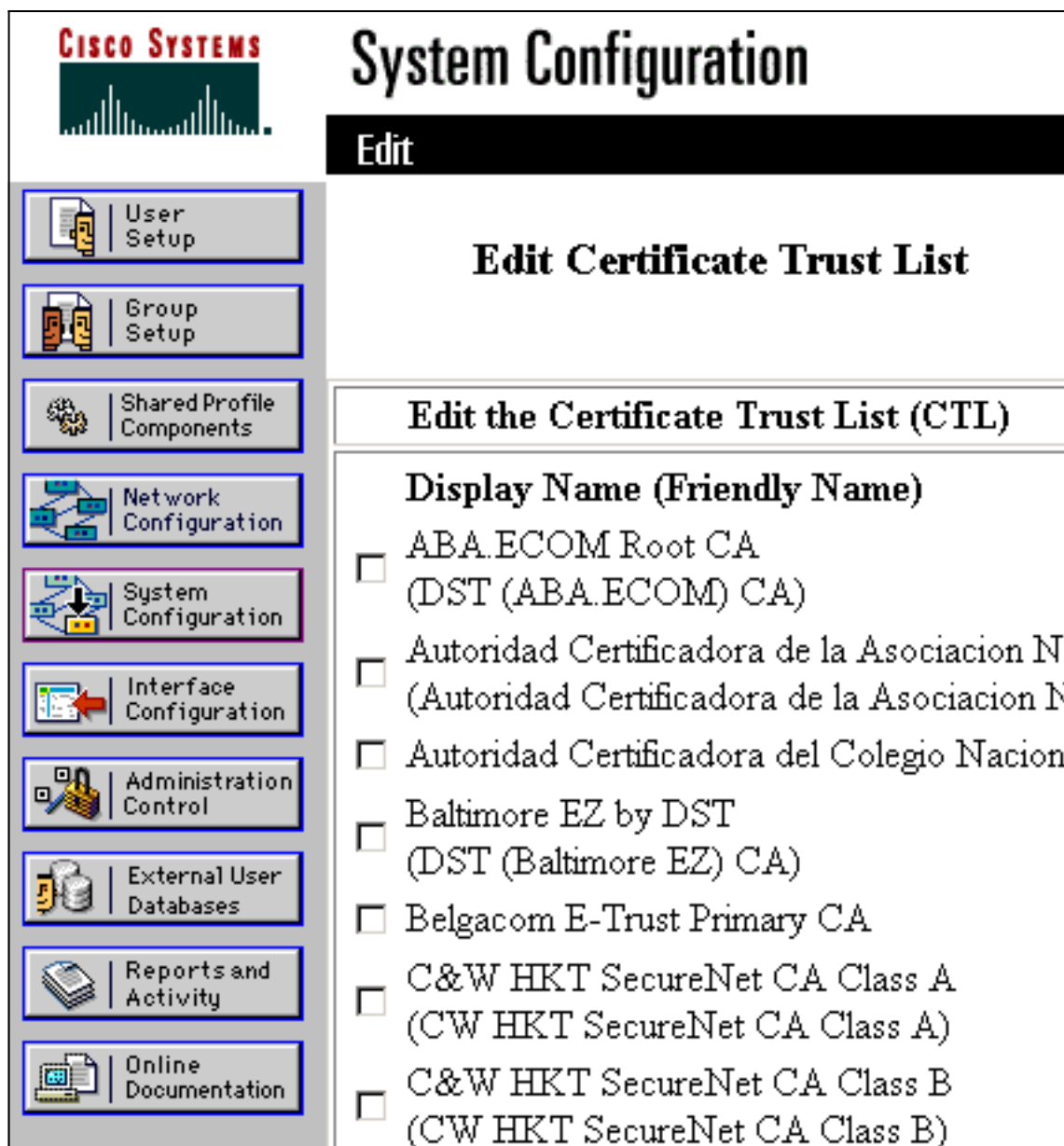
ACS が信頼する必要のある追加の認証局を指定する

ACS は、自身の証明書を発行した CA を自動的に信頼します。クライアント証明書が別の 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。
3. 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] をクリックします。

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 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 below reads "Add new CA certificate to local certificate storage". There is a text input field labeled "CA certificate file" with a red border. Below the input field is a yellow button with a question mark icon and the text "Back to Help".

4. [Edit Certificate Trust List] をクリックします。
5. 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。
6. [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 EAP-TLS 設定を構成する](#)

サービスを再起動して EAP-TLS 設定を構成するには、次のステップに従います。

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. EAP-TLS 設定を構成するために、[System Configuration] をクリックし、[Global Authentication Setup] をクリックします。
4. [Allow EAP-TLS] チェックボックスをオンにしてから、1 つ以上の証明書比較にチェックマークを付けます。
5. [Submit] をクリックします。

