Cisco Secure ACS アプライアンスへの PEAP クライアント用証明書のインストール

目次

概要

このガイドでは、Microsoft CA で作成した証明書について説明するほか、Cisco Secure Access Control Server（ACS）3.3 でサポートされる自己署名証明書を使用するための手順についても説明します。 自己署名証明書を使用すると、外部 CA が必要なくなるので、初回の Protected Extensible Authentication Protocol（PEAP）のインストールが大幅に簡略化されます。 ただし、現時点では、自己署名証明書のデフォルトの有効期限はわずか 1 年であり、これを変更することはできません。 サーバの証明書と言えば、これが標準です。 ただし、自己署名証明書がまたルートCA認証として機能するので、これは**検証サーバ証明** オプションをチェックしない場合を除いて Microsoft サプリカントを使用するとき各クライアントの新しい認証のインストールを毎年意味できます。 自己署名証明書は、従来の CA を使用できるようになるまでの一時的な手段としてのみ使用することを推奨します。 自己署名証明書を使用する場合は、「自己署名証明書」セクションに進んでください。

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 IOS® アクセス ポイント（AP）12.02T1
- Cisco Secure ACS for Windows 3.1 以降
- Cisco Secure ACS Solution Engine（SE）
- Microsoft Windows 2000（SP3 および SP4）または ACU バージョン 6 をインストール済みの XP（Cisco Secure ACS 3.2 を使用している場合、ACU は不要）

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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

Microsoft 証明書サービスのインストール

次の手順を実行します。

1. **[Start] > [Settings] > [Control Panel]**を選択します。
2. コントロールパネルで **[プログラムの追加と削除]** を開きます。
3. [Add/Remove Programs] で、[Add/Remove Windows Components] を選択します。
4. [Certificate Services] にチェックを入れ、[Next] をクリックします。 IIS のメッセージに対して **[Yes]** をクリックします。
5. スタンドアロン（またはエンタープライズ）ルート CA を選択し [Next] をクリックします。
6. CA の名前を決めて入力し、[Next] をクリックします。 他のボックスはすべてオプションです。**注:** CA には Cisco Secure ACS サーバと同じ名前を付けないでください。 同じ名前にすると、サーバ証明書と同じ名前のルート CA 証明書が検出された場合に PEAP クライアントが混乱し、認証が失敗します。 この問題は Cisco クライアントに固有のものではありません。
7. [Next] をクリックします。
8. **[Finish] をクリックします。注:** CA をインストールする前に、IIS をインストールする必要があります。

Cisco Secure ACS for Windows の証明書のセットアップ

ステップ 1： サーバ証明書の作成

サーバ証明書を作成するには、次の手順を実行します。

1. Cisco Secure ACS サーバから、CA（**http://IP_of_CA_server/certsrv/**）を表示します。
2. [Request a certificate] オプションを選択し、[Next] をクリックします。
3. [Advanced request] を選択して、[Next] をクリックします。
4. [Submit a certificate request to this CA using a form] を選択してから [Next] をクリックします。
5. 名前（CN）ボックスに任意の文字を入力します。
6. [Intended Purpose] に [Server Authentication Certificate] を選択します。**注:** エンタープライズ CA を使用している場合は、最初のドロップダウン ボックスで [Web Server] を選択します。**CSP** — Microsoft Base Cryptographic Provider v1.0**Key Size**：1024****注:** Windows 2003 エンタープライズ CA では、1024 より大きいサイズのキーを生成できます。 ただし、キーの使用は PEAP を主としてより 1024 使用しません。 認証は ACS で渡るようであるかもしれませんが認証を試みる間、クライアントはちょうどハングします。[Use Local Machine Store]（ソフトウェア ACS のみ）にチェックを入れます。他はすべてデフォルトのまま残し、[Submit] をクリックします。「Your certificate request has been received...」というメッセージが表示されます。**注:** 1024 より大きいキー サイズで作成した証明書は機能しません。

注 2

注: Microsoft では、Windows 2003 Enterprise CA のリリースに伴って、Web Server テンプレートを変更したため、キーがエクスポートできなくなり、このオプションはグレー表示されるようになりました。 証明書サービスでは、サーバ認証用の他の証明書テンプレート、およびドロップ

ダウンでキーをエクスポート可能としてマークできる他の証明書テンプレートは提供されていません。 したがって、その機能を実行できる新しいテンプレートを作成する必要があります。

次の手順を実行します。

1. [Start] > [Run] > [certtmpl.msc] の順に選択します。
2. [Web Server] テンプレートを右クリックして、[Duplicate Template] を選択します。
3. テンプレートにわかりやすい名前を付けます。
4. [Request Handling] タブに移動し、[**Allow private key to be exported**] にチェックを入れます。
5. [CSPs] ボタンをクリックし、[Microsoft Base Cryptographic Provider v1.0] にチェックを入れます。 [OK] をクリックします。
6. 他のすべてのオプションは、デフォルトのままにしておいてかまいません。
7. [Apply]、次に [OK] をクリックします。
8. CA MMC スナップインを開きます。
9. [Certificate Templates] を右クリックして、[New] > [Certificate Template to Issue] を選択します。
10. 作成した新しいテンプレートを選択して、[OK] をクリックします。
11. CA を再起動します。

新規証明書を作成しようとすると、証明書サービスにより「Failed to create 'CertificateAuthority.Request' object」というエラー メッセージが表示される場合あります。 この問題を解決するには、次の手順を実行します。

1. **[Start] > [Administrative Tools] > [IIS]**を選択します。
2. [Web Sites] > [Default Web Site] を展開します。
3. [CertSrv] を右クリックして、[Properties] を選択します。
4. [Virtual Directory] タブの [Application settings] セクションで [Configuration] ボタンをクリックします。
5. [Options] タブに移動し、[Enable session state] にチェックマークを付けます。
6. 他は、変更する必要はありません。
7. [OK] を 2 回クリックします。
8. IIS を再起動します。ブラウザが `ActiveX` とロックする場合、認証サーバを使用するために試みるとき応答する Microsoft 資料 Internet Explorer 停止で説明されている「ダウンロード ActiveX コントロール」メッセージで修正を実行して下さい 。 CSP フィールドが示せば …、要求を入れるマシンのソフトウェア ファイアウォールを実行しないことを確かめて下さい。

ステップ 2： CA からの証明書の承認

次の手順を実行します。

1. CA を開き、[Start] > [Programs] > [Administrative Tools] > [Certificate Authority] を選択します。
2. 左側にある証明書を展開し、[Pending Requests] をクリックします。
3. 証明書を右クリックし、[all tasks]、[Issue] の順にクリックします。

ステップ 3： Cisco Secure ACS サーバへのサーバ証明書のダウンロード

次の手順を実行します。

1. Cisco Secure ACS サーバから、CA（**http://IP_of_CA_server/certsrv/**）ディレクトリを表示します。
2. [Check on a Pending Certificate] を選択し、[Next] をクリックします。
3. 証明書を選択して [Next] をクリックします。
4. [Install] をクリックします。

ステップ 4： Cisco Secure ACS サーバへの CA 証明書のインストール

次の手順を実行します。

注: Cisco Secure ACS と CA を同じサーバにインストールした場合は、このセクションの手順は必要ありません。

1. Cisco Secure ACS サーバから、CA（**http://IP_of_CA_server/certsrv/**）ディレクトリを表示します。
2. [Retrieve the CA certificate or certificate revocation list] を選択し、[Next] をクリックします。
3. **Base 64 encodedand を**『Download CA certificate』 をクリック します選択して下さい。
4. [Open] をクリックし、[Install certificate] を選択します。
5. [Next] をクリックします。
6. [Place all certificates in the following store] を選択して、[Browse] をクリックします。
7. [Show physical stores] ボックスにチェックマークを付けます。
8. [Trusted root certification authorities] を展開し、[Local Computer] を選択して、[OK] をクリックします。
9. [Next]、[Finish] をクリックしてから [The import was successful] ボックスで [OK] をクリックします。

ステップ 5： サーバ証明書を使用するための Cisco Secure ACS のセットアップ

次の手順を実行します。

1. Cisco Secure ACS サーバで、[System Configuration] をクリックします。
2. [ACS Certificate Setup] および [Install ACS certificate] を選択します。
3. [Use certificate from storage] を選択します。
4. CN の名前を入力して、[Submit] をクリックします。
5. Cisco Secure ACS サーバで、[System Configuration] をクリックします。
6. [ACS Certificate Setup] および [Edit Certificate Trust List] をクリックします。
7. CA のボックスにチェック マークを付けて、[Submit] をクリックします。

Cisco Secure ACS アプライアンスの証明書のセットアップ

ステップ 1： 証明書署名要求の生成

次の手順を実行します。

1. [System Configuration] > [ACS Certificate Setup] > [Generate Certificate Signing Request] の

順に選択します。
2. [Certificate subject] フィールドに「cn=name」形式で名前を入力します。
3. 秘密鍵ファイルの名前を入力します。**注:** このフィールドの秘密キーへのパスはキャッシュされます。 CSR 作成後にもう一度 [Submit] をクリックした場合、秘密鍵が上書きされてしまうため、最初に作成した CSR と一致しなくなります。 その結果、サーバ証明書をインストールしようとすると、「private key does not match」というエラー メッセージが表示されます。
4. 秘密キーのパスワードを入力して確認します。
5. キー長に 1024 を選択します。**注:** Cisco Secure ACS は 1024 より大きいサイズのキーを生成できますが、PEAP では 1024 より大きいキーは機能しません。 Cisco Secure ACS での認証は通過するように見えますが、クライアントでは認証を試みるとハングします。
6. [Submit] をクリックします。
7. CA への送信用に、出力された CSR を右側にコピーします。

ステップ 2： CSR を使用したサーバ証明書の作成

次の手順を実行します。

1. FTP サーバから、CA（**http://IP_of_CA_server/certsrv/**）ディレクトリを表示します。
2. [Request a certificate] オプションを選択し、[Next] をクリックします。
3. [Advanced Request] を選択して、[Next] をクリックします。
4. [Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file] を選択します。
5. 証明書署名要求の出力を、[Base64 Encoded Certificate Request] フィールドに貼り付け、[Submit] をクリックします。
6. [Download CA Certificate] をクリックします。
7. [Save] をクリックし、証明書に名前を付けて FTP ディレクトリに保存します。

ステップ 3： FTP サーバへの CA 証明書のダウンロード

次の手順を実行します。

注: このステップを省略すると、PEAP をイネーブルにできなくなります。 また、サーバ証明書がインストールされているにもかかわらず、インストールされていないというエラーを受信したり、EAP タイプが設定されているにもかかわらず、設定が失敗して「EAP type not configured」というエラーを受信します。

注: サーバ証明書の作成に中間 CA を使用している場合には、ルート CA からサーバ証明書までのチェーンを構成するすべての CA（ルート CA 証明書を含む）について、これらの手順を繰り返す必要がある点にも注意してください。

1. FTP サーバから、CA（**http://IP_of_CA_server/certsrv/**）ディレクトリを表示します。
2. [Retrieve the CA certificate or certificate revocation list] を選択し、[Next] をクリックします。
3. [Base 64 encoded] を選択し、[Download CA certificate] をクリックします。
4. [Save] をクリックし、証明書に名前を付けます。 証明書の名前を FTP ディレクトリに保存します。

ステップ 4： アプライアンスでの CA 証明書のインストール

次の手順を実行します。

注: このステップを省略すると、PEAP をイネーブルにできなくなります。 また、サーバ証明書がインストールされているにもかかわらず、インストールされていないという エラーを受信したり、EAP タイプが設定されているにもかかわらず、設定が失敗して「EAP type not configured」というエラーを受信します。

注: サーバ証明書の作成に中間 CA を使用している場合には、ルート CA からサーバ証明書までのチェーンを構成するすべての CA (ルート CA 証明書を含む) について、これらの手順を繰り返す必要がある点にも注意してください。

1. [System Configuration] > [ACS Certificate Setup] > [ACS Certification Authority Setup] を開きます。
2. [Download CA certificate file] をクリックします。
3. [FTP Server] フィールドに FTP サーバの IP アドレスまたはホスト名を入力します。
4. Cisco Secure ACS が FTP サーバへのアクセスに使用できる有効なユーザ名を [Login] フィールドに入力します。
5. そのユーザのパスワードを [Password] フィールドに入力します。
6. FTP サーバのルート ディレクトリから CA 証明書ファイルが保存されたディレクトリまでの相対パスを [Remote FTP Directory] フィールドに入力します。
7. CA 証明書ファイルの名前を [Remote FTP File Name] フィールドに入力します。
8. [Submit] をクリックします。
9. フィールドのファイル名を確認し、[Submit] をクリックします。
10. [System Configuration] > [Service Control] で ACS サービスを再起動します。

ステップ 5： アプライアンスでのサーバ証明書のインストール

次の手順を実行します。

1. [System Configuration] > [ACS Certificate Setup] を選択します。
2. [Install ACS Certificate] をクリックします。
3. オプションから [Read certificate] を選択し、[Download certificate file] リンクをクリックします。
4. [FTP Server] フィールドに FTP サーバの IP アドレスまたはホスト名を入力します。
5. Cisco Secure ACS が FTP サーバへのアクセスに使用できる有効なユーザ名を [Login] フィールドに入力します。
6. そのユーザのパスワードを [Password] フィールドに入力します。
7. FTP サーバのルート ディレクトリからサーバ証明書ファイルが保存されたディレクトリまでの相対パスを [Remote FTP Directory] フィールドに入力します。
8. サーバ証明書ファイルの名前を [Remote FTP File Name] フィールドに入力します。
9. [Submit] をクリックします。
10. 秘密キーへのパスを入力します。
11. 秘密キーのパスワードを入力します。
12. [Submit] をクリックします。

自己署名証明書のセットアップ (外部 CA を使用しない場合のみ)

注: ラボで自己署名証明書を使用してテストを行うと、クライアントが初めて Microsoft のサプリカントで認証する場合に認証時間が長くかかります。 2 回目以降の認証は問題なく実行されます。

次の手順を実行します。

1. Cisco Secure ACS サーバで、[System Configuration] をクリックします。
2. [ACS Certificate Setup] をクリックします。
3. [Generate Self-signed Certificate] をクリックします。
4. [Certificate subject] フィールドに「**cn=**」で始まる任意の文字列を入力します（例：cn=ACS33）。
5. 作成する証明書のフル パスと名前を入力します（例：c:\acscert \acs33.cer）。
6. 作成する秘密キーのフル パスと名前を入力します（例：c:\acscert \acs33.pvk）。
7. 秘密キーのパスワードを入力して確認します。
8. キー長のドロップダウン メニューから、**1024** を選択します。**注:** Cisco Secure ACS は 1024 より大きいサイズのキーを生成できますが、PEAP では 1024 より大きいキーは機能しません。 ACS での認証は通過するように見えますが、クライアントでは認証を試みるとハングします。
9. [Install generated certificate] にチェックマークを付けます。
10. [Submit] をクリックします。

グローバル認証の設定

次の手順を実行します。

1. Cisco Secure ACS サーバで、[System Configuration] をクリックします。
2. [Global Authentication Setup] をクリックします。**Cisco Secure ACS バージョン 3.2 以降** Microsoft PEAP を使用している場合は、[Allow EAP-MSCHAPv2] にチェックマークを付けます。Cisco PEAP を使用している場合は、[Allow EAP-GTC] にチェックマークを付けます。[Allow MS-CHAP Version 1 Authentication] にチェックマークを付けます。[Allow MS-CHAP Version 2 Authentication] にチェックマークを付けます。[Submit]、[Restart] の順にクリックします。**Cisco Secure ACS バージョン 3.1**[Allow PEAP] にチェックマークを付けます。[Allow MS-CHAP Version 1 Authentication] にチェックマークを付けます。[Allow MS-CHAP Version 2 Authentication] にチェックマークを付けます。[Submit]、[Restart] の順にクリックします。

Cisco Secure ACS での AP の設定

次の手順を実行します。

1. Cisco Secure ACS サーバで、[Network Configuration] をクリックします。
2. [Add Entry] をクリックして、AAA クライアントを追加します。
3. 次のボックスに入力します。**AAA Client IP Address**：AP の IP アドレス**Key**：キーを作成し、キーが AP 共有秘密と一致することを確認**Authenticate Using**：RADIUS（Cisco Aironet）
4. [Submit]、[Restart] の順にクリックします。**注:** AAA クライアントのセットアップでは、デフォルトから何も変更されません。

AP の設定

VxWorks を使用

次の手順を実行します。

1. AP を開き、[Setup] > [Security] > [Authentication Server] を選択します。Cisco Secure ACS の IP アドレスを入力します。共有秘密を入力します（Cisco Secure ACS 内のキーと一致する必要があります）。[EAP Authentication] にチェックマークを付けます。[OK] をクリックします。
2. [Setup] > [Security] > [Radio Data Encryption] を選択します。[Accept Authentication Type] の [Open] および [Network-EAP] にチェックマークを付けます。[Require EAP] の [Open] にチェックマークを付けます。[WEP key 1] を設定し、ブロードキャスト キー ローテーションを使用していない場合は、[128 bit] を選択します。[Use of Data Encryption by Stations] を [full Encryption] に変更します。 [Use of Data Encryption] を変更できない場合は、[Apply] を先にクリックします。[OK] をクリックします。

Cisco IOS AP Web インターフェイスを使用

次の手順を実行します。

1. AP を開き、[Security] > [Server Manager] の順に選択します。[Current Server List] ドロップダウンから [RADIUS] を選択します。Cisco Secure ACS の IP アドレスを入力します。共有秘密を入力します（Cisco Secure ACS 内の「キー」と一致する必要があります）。[EAP Authentication] にチェックマークを付けます。警告ダイアログの [OK] をクリックし、次に [Apply] をクリックします。
2. [Security] > [SSID Manager] を選択します。**注:** WPA を使用する場合は、設定が異なります。 詳細は、このドキュメントの最後の WPA キー管理に関する補足説明を参照してください。[Current SSID List] から [SSID] を選択します。または [SSID] フィールドに新しい SSID を入力します。[Open Authentication] にチェック マークを付け、ドロップダウン メニューから [with EAP] を選択します。[Network EAP] にチェックマークを入れます。他の値はすべてデフォルトのままにして、[Apply] をクリックします。
3. [Security] > [Encryption Manager]を選択します。**注:** WPA を使用する場合は、設定が異なります。 詳細は、このドキュメントの最後の WPA キー管理に関する補足説明を参照してください。[WEP Encryption] オプション ボタンをクリックし、ドロップダウンから [Mandatory] を選択します。[Encryption Key 1] オプション ボタンをクリックし、フィールドにキーを入力します。[Key Size] ドロップダウンから、[128 bit] を選択します。[Apply] をクリックします。

注: ACU をインストールする場合は、Network-EAP が必要です。

注: ブロードキャスト キー ローテーションを使用している場合は、鍵はすでに設定されているはずなので、鍵を設定する必要はありません。 鍵が設定されていrない場合は、[Setup] > [Radio Advance] を選択して、ブロードキャスト キー ローテーションの値を設定します。 5 分（300 秒）より低い値を設定する必要はありません。 値が設定されたら、[OK] をクリックして [Radio Data Encryption] ページに戻ります。

ACU バージョン 6 のインストール（Cisco Secure ACS 3.1 を使用している場合、または EAP-GTC が必要な場合のみ）

エクスプレス セットアップでは、Cisco PEAP サプリカントはインストールされないため、カス

タム インストールを選択する必要があります。 Cisco のサプリカントがインストールされているかどうかは、ネットワーク接続プロパティの [Authentication] タブで EAP タイプを見るとわかります。 PEAP と表示されていれば、Microsoft PEAP サプリカントです。 ただ PEAP とだけ表示されている場合は、Cisco PEAP サプリカントを使用します。

クライアント用ルート CA 証明書のインストール（EAP-MSCHAP-V2 用のみ）

Microsoft CA からの証明書を使用する場合

次の手順を実行します。

1. PC から、CA（**http://IP_of_CA_server/certsrv/**）を表示します。
2. [Retrieve a CA certificate] を選択し、[Next] をクリックします。
3. [Base64 Encoding] および [Download CA certificate] を選択します。
4. [Open] をクリックし、[Install Certificate] を選択します。
5. [Next] をクリックします。
6. [Place all certificates in the following store] を選択し、[Browse] をクリックします。
7. [Show physical stores] ボックスにチェックマークを付けます。
8. [Trusted root certification authorities] を展開して、[Local Computer] を選択してから [OK] をクリックします。
9. [Next]、[Finish] をクリックしてから [The import was successful] ボックスで [OK] をクリックします。

Cisco Secure ACS からの自己署名証明書を使用している場合

次の手順を実行します。

1. 証明書を元の場所からクライアントにコピーします。
2. .cer ファイルを右クリックして、[install certificate] をクリックします。
3. [Next] をクリックします。
4. [Place all certificates in the following store] を選択して、[Browse] をクリックします。
5. [show physical stores] にチェックマークを付けます。
6. [Trusted Root Certification Authorities] を展開して、[Local Computer] を選択してから [OK] をクリックします。
7. [Next]、[Finish]、[OK] をクリックします。**注:** EAP-MSCHAP-V を保持していて、Windows の PEAP プロパティで [Validate server certificate] ボックスにチェック マークを付けた場合は、Cisco Secure ACS での AP の設定が必要です。

PEAP のクライアントの設定

Windows XP SP1 または SP の PEAP の設定

次の手順を実行します。

注: WPA を使用する場合は、設定が異なります。 詳細は、このドキュメントの「WPA キー管理」セクションを参照してください。

注: 現時点で、Windows XP SP2 は IAS 以外の RADIUS サーバに対する PEAP 認証の問題があり

ます。 これは KB885453 および Microsoft で要望に応じて 持っています利用可能 なパッチを文書化されています。

1. [Control Panel] の [Network Connections] を開きます ([Start] > [Control Panel] の順に選択) 。
2. [Wireless Network] を右クリックして、[Properties] を選択します。
3. [Wireless Network] タブで、[use windows to configure...] にチェックが入っていることを確認します。
4. リストに SSID が表示されていたら、[Configure] をクリックします。 表示されていない場合は、[Add] をクリックします。
5. SSID を入力し、[WEP] および [Key is provided for me automatically] にチェックマークを付けます。
6. [Authentication] タブを選択し、[enable network-access control using...] にチェックが入っていることを確認します。
7. [Protected EAP] を選択し、[EAP type] の [Properties] をクリックします。
8. [Trusted root certificate] の下の [CA] のボックスにチェックを入れます。
9. OK を 3 回クリックします。

Windows XP の証明書のセットアップ (SP1 なし)

次の手順を実行します。

1. [Control Panel] の [Network Connections] を開きます ([Start] > [Control Panel] の順に選択) 。
2. [Wireless Network] を右クリックして、[Properties] を選択します。
3. [Wireless Network] タブで、[use windows to configure...] にチェックが入っていることを確認します。
4. [Authentication] タブを選択し、[enable network-access control using...] にチェックが入っていることを確認します。
5. [PEAP] を選択し、[EAP type] の [Properties] をクリックします。
6. [Trusted root certificate] の下の [CA] のボックスにチェックを入れます。
7. OK を 3 回クリックします。

Windows 2000 の PEAP の設定

次の手順を実行します。

1. SP3 を実行する場合、Microsoft から 802.1X ホットフィックスをダウンロードし、 インストールして下さい。 このホットフィックスは SP4 には不要です。
2. [Start] > [Control Panel] > [Network and Dial-up Connections] を選択します。
3. [Wireless Connection] を右クリックして、[Properties] を選択します。
4. [Authentication] タブをクリックします。**注:** [Authentication] タブが表示されない場合は、802.1X サービスがディセーブル状態でインストールされています。 これを解決するには、サービスのリストで Wireless Configuration サービスをイネーブルにする必要があります。[My Computer] を右クリックし、[Manage] をクリックします。[Services] > [Applications] の順に選択して、[Services] をクリックします。サービスの [Startup] の値を [Automatic] に設定し、サービスを起動します。**注:** [Authentication] タブが表示されているのに使用できない場合には、ネットワーク アダプタのドライバで 802.1x が正しくサポートされていません。

サポートされたドライバに関しては 802.1X ホットフィックス ページまたはベンダー Webサイトの下部のでリストをチェックして下さい。
5. [Enable network access control using IEEE 802.1x] にチェックマークを付けます。
6. [EAP type] ドロップダウン メニューから [PEAP] を選択して [OK] をクリックします。

ACU を使用している場合

次の手順を実行します。

1. ACU を開きます。
2. [Manage Profile] を選択し、プロファイルを作成または編集します。
3. AP のクライアント名と SSID を入力します。
4. [Network Security] タブを選択します。
5. [Network Security Type] で、[Host-based EAP] を選択します。
6. WEP で [Use Dynamic WEP Keys] を選択します。
7. [OK] を 2 回クリックします。
8. 作成したプロファイルを選択します。**注:** Cisco のサプリカントを使用している場合、[Authentication] タブには PEAP しか表示されません。 Microsoft のサプリカントを使用している場合は、「Protected EAP (PEAP)」と表示されます。**注:** クライアントが Windows XP のためのワイヤレス アップデート巻き上げパッケージとである Microsoft からの利用可能 なパッチ部分的に軽減することができる AP（約分）に関連付けることを試みる前に非常に 長時間の遅延があります。 このパッチは、EAP-GTC 互換データベース タイプの機能を妨害する EAP- MSCHAPv2 サプリカントを再インストールする可能性があります。**注:** 関連付けが完了しない場合は、カードをディセーブルにしてから再度イネーブルにしてください。

Windows 2003 Mobile の PEAP の設定

次の手順を実行します。

1. Cisco ACU for Windows CE の最新リリースをインストールし、このとき、必ず PEAP サプリカントもインストールします。
2. ACU を開き、[Active Profile] ドロップダウン メニューから <External Settings> を選択します。
3. シスコのネットワーク カードを挿入し、タスクバー上のネットワーク アイコンをクリックして、[Settings] > [Advanced] > [Network Card] の順に選択します。
4. SSID（使用可能な場合）、または [Add New Settings] をクリックします。
5. [Network Name] フィールドおよび接続するネットワークで、SSID を確認します。
6. [Authentication] タブをクリックします。
7. **データ暗号化（WEP）を**チェックすれば**キーは私に提供されます**...."」
8. [Enable network access...802.1x] にチェックを入れ、[Cisco PEAP] を選択します。
9. [Properties] をクリックし、[Validate server certificate] にチェックを入れます（オプション）。**注:** このオプションにチェックを入れた場合、PocketPC にルート CA 証明書をインストールする必要があります。 Windows Mobile には、証明書をインポートおよびエクスポートできるツールが搭載されていません。 利用可能 ないくつかのユーティリティがあります 。これらのユーティリティは、シスコのサポート対象外です。 ACU を使用している場合は、Cisco PEAP サプリカントにより CA 証明書がインポートされるため、これを手動でインポートする必要はありません。 現時点では、自己署名証明書をサポートする PocketPC のオペレーション システムは存在しないため、確認のために自己署名証明書を PocketPC にイ

ンポートできません。 ただし、[Validate server certificate] オプションのチェックを外せば自己署名証明書を使用できます。

10. [OK] をクリックして、[Configure Wireless Networks] 画面に戻ります。
11. **[Connect]** をクリックします。

マシン認証に関する補足説明

マシン認証の目的は、ユーザ認証の前に EAP 認証を使用できるようにし、ネットワーク接続を確立して、ログオン スクリプトが実行されユーザがドメインにログインできるようにすることです。 マシン認証が確立され、認証が実行されるには、ドメイン メンバーシップが必要です。

マシン認証を許可するための ACS のセットアップ

次の手順を実行します。

1. [External User Databases] > [Database Configuration] の順に選択します。
2. [Windows Database] をクリックし、[Configure] を選択します。
3. [Enable PEAP machine authentication] にチェックを入れます。
4. [Submit] をクリックします。

マシン認証のためのクライアントのセットアップ

ドメインへの加入（まだドメインのメンバーではない場合）

次の手順を実行します。

1. 管理者権限を持つアカウントで Windows にログインします。
2. [My Network Places] を右クリックして、[Properties] を選択します。
3. [Choose the Computer Name] を選択し、[Change] をクリックします。
4. [Computer name] フィールドにホスト名を入力します。
5. [Domain] を選択し、ドメインの名前を入力して [OK] をクリックします。
6. ドメインに加入するためのログイン ダイアログが表示されます。 ドメインに参加する権限を持つアカウントでログインします。
7. コンピュータが正常にドメインに加入すると、コンピュータが再起動されます。 マシンがドメインのメンバーになり、OS のみが認識するドメインによりネゴシエートされた認証クレデンシャルを利用できるようになりました。 Cisco Secure ACS では、ユーザ名はホスト/ホスト名と表示されます。

マシン認証のための PEAP サプリカントのセットアップ

次の手順を実行します。

1. [Start] > [Control Panel] の順に選択し、[Control Panel] の [Network Connections] を開きます。
2. ネットワーク接続を右クリックして、[Properties] を選択します。
3. [Authentication] タブをクリックし、[Authenticate as computer] にチェックを入れます。

WPA キー管理に関する補足説明

Cisco IOS AP 12.02(13)JA1、Cisco Secure ACS 3.2、および Windows XP SP1（WPA ホットフィックス適用済み）向けの説明です。

注: Windows 2000 クライアントは WPA 鍵 管理を元々サポートしません 。 これをサポートするには、ベンダーのソフトウェアを使用する必要があります。

注: Cisco ACU では、ホストベースの EAP（EAP-TLS および PEAP）での WPA キー管理は現在サポートされていません。 そのため、Funk Odyssey クライアントまたは Meetinghouse AEGIS クライアントなどの、サードパーティ製のクライアントをインストールする必要があります。 シスコの製品における WPA サポートの詳細については、『WPA Support』を参照してください。

注: また、ACU の PocketPC バージョンによりインストールされたシスコのカード用のドライバも、現時点では WPA をサポートしていない点に注意してください。 WPA は、サードパーティ製のサプリカントを使用しても PocketPC 上のシスコのクライアントでは動作しません。

AP の設定

次の手順を実行します。

1. [Security] > [Encryption Manager]を選択します。[WEP Cipher] を選択し、ドロップダウンから [TKIP] を選択します。[Apply] をクリックします。
2. [Security] > [SSID Manager] を選択します。[Current SSID List] から [SSID] を選択します。または [SSID] フィールドに新しい SSID を入力します。[Open Authentication] にチェックマークを付け、ドロップダウン メニューから [with EAP] を選択します。[Network EAP] にチェックマークを入れます。[Authenticated Key Management] の下で、ドロップダウン メニューから [Mandatory] を選択して [WPA] をクリックします。[Apply] をクリックします。

Windows XP SP1（KB826942 インストール済み）または SP2 クライアントの PEAP および WPA のセットアップ

次の手順を実行します。

1. [Start] > [Control Panel] の順に選択し、[Control Panel] の [Network Connections] を開きます。
2. [Wireless Network] を右クリックして、[Properties] を選択します。
3. [Wireless Network] タブで、[use windows to configure...] にチェックが入っていることを確認します。
4. リストに SSID が表示されていたら、[Configure] をクリックします。 表示されていない場合は、[Add] をクリックします。
5. SSID を入力し、[Network Authentication] で [WPA] を選択して、[Data Encryption] で [TKIP] を選択します。
6. [Authentication] タブを選択し、[enable network-access control using...] にチェックが入っていることを確認します。
7. [Protected EAP] を選択し、[EAP type] の [Properties] をクリックします。
8. [Trusted root certificate] の下の [CA] のボックスにチェックを入れます。
9. OK を 3 回クリックします。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

問題 1

このエラーは、ACS における証明書のインストールおよび認証時に発生します。

```
Unsupported private key file format
Failed to initialize PEAP or EAP-TLS authentication protocol because ACS certificate is
not installed
```

解決策

このエラーは、PEAP 証明書が正常にインストールされていない場合に発生します。 この問題を解決するには、証明書を削除してから新しい自己署名証明書をインストールしてください。

問題 2

このエラーは、ACS における証明書のインストールおよび認証時に発生します。

```
Failed to initialize PEAP or EAP-TLS authentication protocol because CA certificate is
 not installed.
```

解決策

このエラーを解決するには、ACS Certification Authority Setup を使用して CA 証明書をインストールします。 このエラーは、自己署名証明書が使用されていない場合は、不正な CA 証明書により発生します。

問題 3

このエラーは、ACS のアップグレードが実行された場合に発生します。

```
A required certificate is not within its validity period when verifying
against the current system clock or the timestamp in the signed file.
(800B0101)
```

解決策

このエラーは、管理ソフトウェアがアップグレードされていない場合に ACS のアップグレードが実行されると発生します。 この問題を解決するには、管理ソフトウェアのアップグレードを実行してから ACS ソフトウェアをアップグレードしてください。 ACS をアップグレードする方法の詳細については、『Cisco Secure ACS Appliance の管理』の「アプライアンスのアップグレード」セクションを参照してください。

問題 4

このエラーは、ACS における証明書のインストール時に発生します。

```
Private key you've selected doesn't fit to this certificate
```

解決策

このエラーの最も一般的な原因は、新しい CSR を生成することで誤って秘密キーを上書きしてしまうことです。

次の情報を確認します。

1. ACS 証明書として正しい証明書をロードしている。
2. 要求の生成中は、RSA 公開キーの長さが 1024 ビットである。
3. CSR の生成時に完全な CN=文字列を使用している。

関連情報

- Cisco Secure ACS for UNIX に関するサポート ページ
- セキュリティ製品に関する Field Notices (CiscoSecure UNIX を含む)
- Cisco Secure Access Control Server for Unix に関するドキュメント
- Cisco Secure ACS for Windows に関するサポート ページ
- Cisco Secure ACS for Windows に関するドキュメント
- テクニカルサポートとドキュメント - Cisco Systems