ACS 5.1 と Windows 2003 Server を使用した Unified Wireless Network 環境での PEAP

目次

概要
前提条件
要件
使用するコンポーネント
表記法
設定
ネットワーク図
IIS、Certificate Authority、DNS、DHCP を使用する Windows Enterprise 2003 のセットアップ（CA）
CA（democa）
Cisco 1121 Secure ACS 5.1
CSACS-1121 シリーズ アプライアンスを使用したインストール
ACS サーバのインストール
Cisco WLC5508 コントローラの設定
WPAv2 および WPA に必要な設定の作成
PEAP 認証
証明書テンプレート スナップインのインストール
ACS Web サーバ用の証明書テンプレートの作成
新しい ACS Web サーバ証明書テンプレートの有効化
ACS 5.1 証明書のセットアップ
エクスポート可能な ACS 用証明書の設定
ACS 5.1 ソフトウェアでの証明書のインストール
Active Directory の ACS ID ストアの設定
ACS への AAA クライアントとしてのコントローラの追加
ワイヤレス用 ACS アクセス ポリシーの設定
ACS アクセス ポリシーとサービス ルールの作成
Windows の自動機能を使用した PEAP 用クライアントの設定
基本的なインストールと設定の実行
ワイヤレス ネットワーク アダプタのインストール
ワイヤレス ネットワーク接続の設定
ACS を使用したワイヤレス認証のトラブルシューティング
ACS サーバでの PEAP 認証の失敗
関連情報

概要

このドキュメントでは、ワイヤレス LAN コントローラ、Microsoft Windows 2003 ソフトウェア、および Cisco Secure Access Control Server（ACS）5.1 で、Protected Extensible Authentication Protocol（PEAP）と Microsoft Challenge Handshake Authentication Protocol（MS-CHAP; Microsoft チャレンジ ハンドシェイク認証プロトコル）バージョン 2 を使用して、セキュアなワイヤレス アクセスを設定する方法について説明します。

注: セキュア ワイヤレスの導入の詳細については、Microsoft Wi-Fi Web サイトおよび Cisco SAFE ワイヤレス ブループリントを参照してください。

前提条件

要件

ここでは、インストール担当者が Windows 2003 と Cisco ワイヤレス LAN コントローラのインストールに関する基本的な知識を持っていることを前提とし、このドキュメントではテストを実行するための特定の設定についてのみ説明しています。

Cisco 5508 シリーズ コントローラの初期インストールと設定については、『Cisco 5500 シリーズ ワイヤレス コントローラ インストレーション ガイド』を参照してください。 Cisco 2100 シリーズ コントローラの初期インストールと設定については、『クイック スタート ガイド: Cisco 2100 シリーズ Wireless LAN Controller』を参照してください。

Microsoft Windows 2003 のインストールおよび設定のガイドについては、『Installing Windows Server 2003 R2』を参照してください。

開始する前に、テスト ラボの各サーバに Microsoft Windows Server 2003 SP1 のオペレーティング システムをインストールし、すべての Service Pack をアップデートしておいてください。 コントローラと Lightweight Access Point（LAP; Lightweight アクセス ポイント）をインストールし、最新のソフトウェア更新プログラムが設定されていることを確認します。

ここでは、PEAP 認証用のユーザ証明書とワークステーション証明書の自動登録を設定できるようにするために、Windows Server 2003 Enterprise Edition SP 1 を使用しています。 証明書の自動登録と自動更新を使用すると、証明書の期限管理と更新を自動化できるため、証明書の配布が容易になると同時に、セキュリティも向上します。

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。

- 7.0.98.0 が稼働する Cisco 2106 または 5508 シリーズ コントローラ
- Cisco 1142 Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）AP
- Windows 2003 Enterprise（Internet Information Server（IIS）、Certificate Authority（CA; 認証局）、DHCP、Domain Name System（DNS; ドメイン ネーム システム）がインストールされているもの）
- Cisco 1121 Secure Access Control System Appliance（ACS）5.1
- Windows XP Professional SP（および最新の Service Pack）と、無線ネットワーク インターフェイス カード（NIC）（CCX v3 をサポートしているもの）またはサード パーティのサプリカント
- Cisco 3750 スイッチ

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。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

シスコのセキュア ワイヤレス ラボのトポロジ
このドキュメントの第 1 の目的は、ACS 5.1 と Windows 2003 Enterprise サーバを使用する Unified Wireless Network 環境で PEAP を実装する手順を説明することです。 特に、クライアントの登録とサーバからクライアントへの証明書の取得を自動化する、クライアントの自動登録の機能に重点を置いています。

注: Temporal Key Integrity Protocol（TKIP）/Advanced Encryption Standard（AES; 高度暗号化規格）を使用する Wi-Fi Protected Access（WPA）/WPA2 を Windows XP Professional SP に追加する場合は、『WPA2/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with Service Pack 2』を参照してください。

IIS、Certificate Authority、DNS、DHCP を使用する Windows Enterprise 2003 のセットアップ（CA）

CA（democa）

CA とは、Windows Server 2003 Enterprise Edition SP2 が稼働していて、次の役割を実行するコンピュータのことです。

- IIS を実行する **demo.local** ドメインのドメイン コントローラ
- **demo.local** DNS ドメインの DNS サーバ
- DHCP サーバ
- **demo.local** ドメインのエンタープライズ ルート CA

CA で、これらのサービスを実行できるように設定するには、次の手順を実行します。

1. 基本的なインストールと設定を実行する。
2. コンピュータをドメイン コントローラとして設定する。
3. ドメインの機能レベルを上げる。

4. DHCP をインストールして設定する。
5. 証明書サービスをインストールする。
6. 証明書を使用するための管理者権限を確認する
7. ドメインにコンピュータを追加する。
8. コンピュータに無線アクセスを許可する。
9. ドメインにユーザを追加する
10. ユーザに無線アクセスを許可する。
11. ドメインにグループを追加する。
12. wirelessusers グループにユーザを追加する
13. wirelessusers グループにクライアント コンピュータを追加して下さい。

基本的なインストールと設定を実行する

次の手順を実行します。

1. Windows Server 2003 Enterprise Edition SP2 をスタンドアロン サーバとしてインストールします。
2. IP アドレスは *10.0.10.10*、サブネット マスクは *255.255.255.0* で TCP/IP プロトコルを設定します。

コンピュータをドメイン コントローラとして設定する

次の手順を実行します。

1. [Start] > [Run] を選択して **dcpromo.exe** と入力し、[OK] をクリックして Active Directory のインストール ウィザードを開始します。
2. [Welcome to the Active Directory Installation Wizard] ページで、[Next] をクリックします。
3. [Operating System Compatibility] ページで、[Next] をクリックします。
4. [Domain Controller Type] ページで [**Domain Controller for a new Domain**] を選択し、[**Next**] をクリックします。
5. [Create New Domain] ページで [**Domain in a new forest**] を選択し、[**Next**] をクリックします。
6. [Install or Configure DNS] ページで [No, just install and configure DNS on this computer] を選択し、[Next] をクリックします。
7. [New Domain Name] ページで **demo.local** と入力して、[Next] をクリックします。
8. [NetBIOS Domain Name] ページで、[Domain NetBIOS name] に **demo** と入力して、[Next] をクリックします。
9. [Database and Log Folders] ページで、[Database folder] と [Log folder] のディレクトリはデフォルトのまま、**[Next]** をクリックします。
10. [Shared System Volume] ページで、デフォルトのフォルダ場所が正しいことを確認して、[Next] をクリックします。
11. [Permissions] ページで、[Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems] が選択されていることを確認して、[Next] をクリックします。
12. [Directory Services Restore Mode Administration Password] ページで、パスワードのボックスは空白のままにして、[Next] をクリックします。
13. [Summary] ページで情報を確認して [Next] をクリックします。
14. Active Directory のインストールが完了したら、[Finish] をクリックします。

15. コンピュータの再起動を指示するプロンプトが表示されたら、[Restart Now] をクリックします。

ドメインの機能レベルを上げる

次の手順を実行します。

1. [Administrative Tools] フォルダから [Active Directory Domains and Trusts] スナップインを開き（[Start] > [Programs] > [Administrative Tools] [Active Directory Domains and Trusts]）、ドメイン コンピュータの **CA.demo.local** を右クリックします。
2. [Raise Domain Functional Level] をクリックし、[Raise Domain Functional Level] ページで [Windows Server 2003] を選択します。
3. [Raise] をクリックし、[OK] をクリックしてから、もう一度 [OK] をクリックします。

DHCP をインストールして設定する

次の手順を実行します。

1. コントロール パネルの [**プログラムの追加と削除**] を使用して、**Dynamic Host Configuration Protocol（DHCP）** を **Networking Service** コンポーネントとしてインストールします。
2. [Administrative Tools] フォルダから [DHCP] スナップインを開き（[Start] > [Programs] > [Administrative Tools] [DHCP]）、DHCP サーバの **CA.demo.local** を強調表示します。
3. **[Action]** をクリックしてから **[Authorize]** をクリックし、DHCP サービスを許可します。
4. コンソール ツリーで **CA.demo.local** を右クリックして、[New Scope] をクリックします。
5. [New Scope] ウィザードの [Welcome] ページで、[Next] をクリックします。
6. [Scope Name] ページで、[Name] フィールドに **CorpNet** と入力します。
7. **[Next]** をクリックし、次のようにパラメータを入力します。[Start IP address]：**10.0.20.1**[End IP address]：**10.0.20.200**Length - **24**Subnet mask：255.255.255.0
8. [Next] をクリックし、除外するアドレスの [Start IP address] に **10.0.20.1**、[End IP address] に *10.0.20.100* と入力します。 次に [Next] をクリックします。 これにより、10.0.20.1 ~ 10.0.20.100 の範囲の IP アドレスが予約されます。 この予約 IP アドレスは、DHCP サーバから割り当てられることはありません。
9. [Lease Duration] ページで [Next] をクリックします。
10. [Configure DHCP Options] ページで [Yes, I want to configure these options now] を選択し、[Next] をクリックします。
11. [Router (Default Gateway)] ページで、デフォルト ルータ アドレスの *10.0.20.1* を追加し、[Next] をクリックします。
12. ドメイン名および DNSサーバ ページで、親 ドメイン フィールドのタイプ *demo.local は*、IP Address フィールドのタイプ 10.0.10.10、およびそれから Addand を『Next』 をクリック しますクリックします。
13. [WINS Servers] ページで **[Next]** をクリックします。
14. [Activate Scope] ページで、[Yes, I want to activate this scope now] を選択し、[Next] をクリックします。
15. [New Scope Wizard] ページが完了したら、[Finish] をクリックします。

証明書サービスをインストールする

次の手順を実行します。

注: 証明書サービスをインストールする場合は、IIS のインストールが完了している必要があります。また、ユーザは Enterprise Admin OU に属している必要があります。

1. コントロール パネルで **[Add or Remove Programs]** を開き、**[Add/Remove Windows Components]** をクリックします。
2. [Windows Components Wizard] ページで [Certificate Services] を選択し、[Next] をクリックします。
3. [CA Type] ページで [Enterprise root CA] を選択し、[Next] をクリックします。
4. [CA Identifying Information] ページで、[Common name for this CA] ボックスに *democa* と入力します。 その他の情報もオプションで入力できます。 次に **[Next]** をクリックし、[Certificate Database Settings] ページはデフォルトのまま使用します。
5. [Next] をクリックします。 インストールが完了したら、[Finish] をクリックします。
6. IIS のインストールに関する警告メッセージを読んでから、**[OK]** をクリックします。

証明書を使用するための管理者権限を確認する

次の手順を実行します。

1. [Start] > [Administrative Tools] > [Certification Authority] を選択します。
2. **democa CA** を右クリックし、[Properties] をクリックします。
3. [Security] タブの [Group or User names] リストで、[Administrators] をクリックします。
4. [Permissions for Administrators] リストで、次のオプションが [Allow] に設定されていることを確認します。Issue and Manage CertificatesManage CARequest Certificates[Deny] に設定されている、またはチェックマークが入っていないオプションがある場合は、権限を [Allow] に設定します。
5. [OK] をクリックして democa CA の [Properties] ダイアログボックスを閉じ、続いて [Certification Authority] を終了します。

ドメインにコンピュータを追加する

次の手順を実行します。

注: コンピュータがすでにドメインに追加されている場合は、「ドメインにユーザを追加する」に進みます。

1. **[Active Directory Users and Computers]** スナップインを開きます。
2. コンソール ツリーで **demo.local** を展開します。
3. [Computers] を右クリックして [New] をクリックし、[Computer] をクリックします。
4. [New Object – Computer] ダイアログボックスで、[Computer name] フィールドにコンピュータの名前を入力し、[Next] をクリックします。 この例では、*Client* というコンピュータ名を使用します。
5. [Managed] ダイアログボックスで [Next] をクリックします。
6. [New Object – Computer] ダイアログボックスで [Finish] をクリックします。
7. さらにコンピュータ アカウントを作成する場合は、ステップ 3 ~ 6 を繰り返します。

コンピュータに無線アクセスを許可する

次の手順を実行します。

1. [Active Directory Users and Computers] コンソール ツリーで **[Computers]** フォルダをクリックし、ワイヤレス アクセスを許可するコンピュータを右クリックします。 この例は『 Properties』 をクリック し、次に **Dial-in タブ**に行きなさいかステップ 7.で追加したかどれをコンピュータ **クライアントことを**とのプロシージャ示します。
2. [Remote Access Permission] で、[Allow access] を選択し、[OK] をクリックします。

ドメインにユーザを追加する

次の手順を実行します。

1. [Active Directory Users and Computers] コンソール ツリーで、[Users] を右クリックし、[New] をクリックして、[User] をクリックします。
2. [New Object – User] ダイアログボックスで、ワイヤレス ユーザの名前を入力します。 この例では、[First name] フィールドに *wirelessuser*、[User logon name] フィールドに *wirelessuser* という名前を使用しています。 [Next] をクリックします。
3. [New Object – User] ダイアログボックスで、[Password] および [Confirm password] フィールドに任意のパスワードを入力します。 **[User must change password at next logon]** チェックボックスをオフにし、**[Next]** をクリックします。
4. [New Object – User] ダイアログボックスで、**[Finish]** をクリックします。
5. 追加のユーザ アカウントを作成するには、ステップ 2 ~ 4 を繰り返します。

ユーザに無線アクセスを許可する

次の手順を実行します。

1. [Active Directory Users and Computers] コンソール ツリーで、[Users] フォルダをクリックし、[wirelessuser] を右クリックして [Properties] をクリックし、[Dial-in] タブに移動します。
2. [Remote Access Permission] で、[Allow access] を選択し、[OK] をクリックします。

ドメインにグループを追加する

次の手順を実行します。

1. [Active Directory Users and Computers] コンソール ツリーで、[Users] を右クリックして [New] をクリックし、[Group] をクリックします。
2. [New Object – Group] ダイアログボックスで、[Group name] フィールドにグループの名前を入力し、[OK] をクリックします。 このドキュメントでは、*wirelessusers* というグループ名を使用します。

wirelessusers グループにユーザを追加する

次の手順を実行します。

1. [Active Directory Users and Computers] の詳細ペインで、グループ [*WirelessUsers*] をダブルクリックします。

2. [Members] タブに移動し、**[Add]** をクリックします。
3. Select Users, Contacts, Computers, or Groups ダイアログボックスで、グループに追加するユーザの名前を入力します。 この例では、ユーザ *wirelessuser* をグループに追加する手順を説明しています。 [OK] をクリックします。
4. [Multiple Names Found] ダイアログボックスで **[OK]** をクリックします。 wirelessuser のユーザ アカウントが、wirelessusers のグループに追加されます。
5. [OK] をクリックして、wirelessusers のグループに対する変更を保存します。
6. さらにユーザをグループに追加する場合は、この手順を繰り返します。

wirelessusers グループにクライアント コンピュータを追加する

次の手順を実行します。

1. このドキュメントの「wirelessusers グループにユーザを追加する」のステップ 1 ~ 2 を繰り返します。
2. [Select Users, Contacts, or Computers] ダイアログボックスで、グループに追加するコンピュータの名前を入力します。 この例では、*client* という名前のコンピュータをグループに追加する手順を説明しています。
3. [Object Types] をクリックし、[Users] チェックボックスをオフにして、[Computers] にチェックマークを入れます。
4. [OK] を 2 回クリックします。 CLIENT のコンピュータ アカウントが、wirelessusers のグループに追加されます。
5. さらにコンピュータをグループに追加するには、この手順を繰り返します。

Cisco 1121 Secure ACS 5.1

CSACS-1121 シリーズ アプライアンスを使用したインストール

CSACS-1121 アプライアンスは、ACS 5.1 ソフトウェアと一緒にプリインストールされています。 このセクションでは、ACS をインストールする前に実行する必要のある、インストール プロセスおよびタスクの概要を説明します。

1. CSACS-1121 をネットワークおよびアプライアンス コンソールに接続します。 第 4 章「ケーブルの接続」を参照してください。
2. CSACS-1121 アプライアンスの電源を入れます。 第 4 章「CSACS-1121 シリーズ アプライアンスの電源投入」を参照してください。
3. CLI プロンプトで **setup** コマンドを実行して、ACS サーバの初期設定を行います。 「セットアップ プログラムの実行」を参照してください。

ACS サーバのインストール

このセクションでは、CSACS-1121 シリーズ アプライアンスに ACS サーバをインストールするプロセスについて説明します。

- セットアップ プログラムの実行
- インストール プロセスの検証
- インストール後のタスク

Cisco Secure ACS サーバのインストールの詳細については、『Cisco Secure Access Control System 5.1 のインストールとアップグレード ガイド』を参照してください。

Cisco WLC5508 コントローラの設定

WPAv2 および WPA に必要な設定の作成

次の手順を実行します。

注: ここでは、コントローラからネットワークへの基本的な接続が確立され、管理インターフェイスへの IP 到達可能性が確保されていることが前提となっています。

1. ブラウザで **https://10.0.1.10** を開いて、コントローラにログインします。
2. **[Login]**をクリックします。
3. デフォルト ユーザの *admin* とデフォルト パスワードの *admin* を使用してログインします。
4. [Controller] メニューから、VLAN のマッピング用の新しいインターフェイスを作成します。
5. [Interfaces] をクリックします。
6. [New] をクリックします。
7. [Interface name] フィールドに *Employee* と入力します（このフィールドには、任意の値を入力できます）。
8. [VLAN ID] フィールドに *20* と入力します（このフィールドには、ネットワークに設定されている任意の VLAN を入力できます）。
9. [Apply] をクリックします。
10. 次の [Interfaces > Edit] ウィンドウに示すとおりに、情報を設定します。[Interface IP Address]：**10.0.20.2**[Netmask]：**255.255.255.0**[Gateway]：**10.0.10.1**[Primary DHCP]：**10.0.10.10**
11. [Apply] をクリックします。
12. [WLANs] タブをクリックします。
13. [Create New] を選択して、[Go] をクリックします。
14. [Profile Name] を入力し、[WLAN SSID] フィールドに *Employee* と入力します。
15. WLAN の ID を選択し、[Apply] をクリックします。
16. [WLANs > Edit] ウィンドウが表示されたら、この WLAN の情報を設定します。**注:** このラボでは、レイヤ 2 の暗号化方式に WPAv2 を選択しています。 この SSID に関連付ける TKIP-MIC クライアントで WPA を使用させるには、802.11i AES 暗号化方式をサポートしていないクライアントで、[WPA compatibility mode] と [Allow WPA2 TKIP Clients] のチェックボックスをオンにします。
17. [WLANs > Edit] 画面で [General] タブをクリックします。
18. [Status] の [Enabled] チェックボックスがオンになっており、適切な [Interface]（employee）が選択されていることを確認します。 また、[Broadcast SSID] の [Enabled] チェックボックスがオンになっていることも確認します。
19. [Security] タブをクリックします。
20. [Layer 2] サブメニューの [Layer 2 Security] で、[WPA + WPA2] を選択します。 WPA2 暗号化の場合、TKIP クライアントを許可するには、[AES + TKIP] を選択します。
21. 認証方式には **802.1x** を選択します。
22. レイヤ 3 サブメニューは不要のため、スキップします。 RADIUS サーバを設定したら、[Authentication] メニューから適切なサーバを選択できるようになります。
23. 特別な設定が必要でない限り、[QoS] タブおよび [Advanced] タブはデフォルトのままにしておきます。

24. [Security] メニューをクリックし、RADIUS サーバを追加します。
25. [RADIUS] サブメニューで、[Authentication] をクリックします。 次に [New] をクリックします。
26. RADIUS サーバの IP アドレス (10.0.10.20) を追加します。このアドレスは、前の手順で設定した ACS サーバのものです。
27. 共有キーが、ACS サーバで設定されている AAA クライアントと一致していることを確認します。 [Network User] チェックボックスがオンになっていることを確認し、[Apply] をクリックします。
28. これで基本設定が完了し、PEAP のテストが実行できるようになりました。

PEAP 認証

MS-CHAP バージョン 2 を使用した PEAP の場合、ACS サーバの証明書は必要ですが、ワイヤレス クライアントの証明書は不要です。 ACS サーバのコンピュータ証明書自動登録を使用すると、展開が簡略化されます。

コンピュータ証明書とユーザ証明書の自動登録を実行するように CA サーバを設定するには、このセクションの手順を実行します。

注: Microsoft は、Windows 2003 Enterprise CA のリリースで Web サーバ テンプレートを変更しており、現在はキーをエクスポートできず、オプションはグレイアウトされます。 サーバ認証に使用でき、ドロップダウンで使用できるキーをエクスポート可能にマークできる機能を備えた証明書サービスでは、これ以外の証明書テンプレートは提供されていないため、これを実行する新しいテンプレートを作成する必要があります。

注: Windows 2000 ではエクスポート可能なキーが使用できるため、Windows 2000 を使用している場合は、この手順を実行する必要はありません。

証明書テンプレート スナップインのインストール

次の手順を実行します。

1. [Start] > [Run] の順に選択し、**mmc** と入力して、[OK] をクリックします。
2. [File] メニューで [Add/Remove Snap-in] をクリックし、[Add] をクリックします。
3. [Snap-in] の下にある [**Certificate Templates**] をダブルクリックし、[**Close**] をクリックしてから [**OK**] をクリックします。
4. コンソール ツリーで [Certificate Templates] をクリックします。 詳細ペインに、すべての証明書テンプレートが表示されます。
5. ステップ 2 ~ 4 を省略するには、*certtmpl.msc* と入力し、[Certificate Templates] スナップインを開きます。

ACS Web サーバ用の証明書テンプレートの作成

次の手順を実行します。

1. [Certificate Templates] スナップインの詳細ペインで、[Web Server] テンプレートをクリックします。
2. [Action] メニューで [Duplicate Template] をクリックします。
3. [Template display name] フィールドに、*ACS* と入力します。

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。 また、[Purpose] ドロップダウン メニューで [Signature and Encryption] が選択されていることを確認します。
5. [Requests must use one of the following CSPs] を選択し、[Microsoft Base Cryptographic Provider v1.0] にチェックマークを入れます。 その他の CSP のチェックマークはすべて外して、[OK] をクリックします。
6. [Subject Name] タブに移動し、[Supply in the request] を選択して [OK] をクリックします。
7. [Security] タブに移動して、[Domain Admins Group] を選択し、[Allowed] の下部にある [Enroll] オプションにチェックマークが入っていることを確認します。**注:** [Active Directory Users and Computers] スナップインでは、ワイヤレス ユーザ アカウントに電子メール名は入力しないため、この Active Directory 情報からの構築を選択する場合は、件名および電子メール名では [User principal name (UPN)] のみをチェックし、[Include email name] のチェックマークを外します。 これらの 2 つのオプションを無効にしなかった場合は、自動登録による電子メールの使用が試行され、その結果、自動登録のエラーが発生します。
8. 証明書が自動的にプッシュされてしまうことを防止する必要がある場合は、追加のセキュリティ対策が用意されています。 これらの機能は、[Issuance Requirements] タブにあります。 このドキュメントでは、詳細は説明しません。
9. [OK] をクリックしてテンプレートを保存し、[Certificate Authority] スナップインからこのテンプレートを発行するようにします。

新しい ACS Web サーバ証明書テンプレートの有効化

次の手順を実行します。

1. [Certification Authority] スナップインを開きます。 「ACS Web サーバ用の証明書テンプレートの作成」セクションのステップ 1 ~ 3 を実行し、[Certificate Authority] オプションを選択し、[Local Computer] オプションを選択して [Finish] をクリックします。
2. [Certificate Authority] コンソール ツリーで、**ca.demo.local** を展開し、[Certificate Templates] を右クリックします。
3. [New] > [Certificate Template to Issue] に移動します。
4. **ACS Certificate Template** をクリックします。
5. [OK] をクリックし、[Active Directory Users and Computers] スナップインを開きます。
6. コンソール ツリーで [Active Directory Users and Computers] をダブルクリックし、**demo.local** を右クリックして [Properties] をクリックします。
7. [Group Policy] タブで、[Default Domain Policy] をクリックし、次に [Edit] をクリックします。 これにより、Group Policy Object Editor スナップインが開きます。
8. コンソール ツリーで、[Computer Configuration] > [Windows Settings] > [Security Settings] > [Public Key Policies] を展開して、[Automatic Certificate Request Settings] を選択します。
9. [Automatic Certificate Request Settings] を右クリックして、[New] > [Automatic Certificate Request] を選択します。
10. [Welcome to the Automatic Certificate Request Setup Wizard] ページで [**Next**] をクリックします。
11. [Certificate Template] ページで [Computer] をクリックし、[Next] をクリックします。
12. Automatic Certificate Request Setup Wizard ページが完了したら、[Finish] をクリックします。 [Group Policy Object Editor] スナップインの詳細ペインに、コンピュータ証明書の種類が表示されます。
13. コンソール ツリーで、[User Configuration] > [Windows Settings] > [Security Settings] > [Public Key Policies] を展開します。

14. 詳細ペインで [Auto-enrollment Settings] をダブルクリックします。
15. **[Enroll certificates automatically]** を選択し、**[Renew expired certificates, update pending certificates and remove revoked certificates]** と **[Update certificates that use certificate templates]** にチェックマークを入れます。
16. [OK] をクリックします。

ACS 5.1 証明書のセットアップ

エクスポート可能な ACS 用証明書の設定

注: ACS サーバが WLAN の PEAP クライアントの認証を実行するには、エンタープライズ ルート CA サーバからサーバ証明書を取得している必要があります。

注: 証明書の設定プロセス中は、IIS Manager が起動していないことを確認してください。IIS Manager が起動していると、キャッシュ情報に関する問題が発生することがあります。

1. Admin 権限を持っているアカウントで、ACS サーバにログインします。
2. [System Administration] > [Configuration] > [Local Server Certificates] に移動します。 [Add] をクリックします。
3. サーバ証明書の作成方法は、[Generate Certificate Signing Request] を選択します。 [Next] をクリックします。
4. 次の例のように証明書のサブジェクトとキーの長さを入力して、[Finish] をクリックします。[Certificate Subject]：**CN=acs.demo.local**[Key Length]：**1024**
5. ACS で、証明書署名要求が生成されたことを通知するプロンプトが表示されます。 [OK] をクリックします。
6. [System Administration] で、[Configuration] > [Local Server Certificates] > [Outstanding Signing Requests] に進みます。**注:** この手順を実行する理由は、Windows 2003 では、エクスポート可能なキーを使用できないため、前の手順で作成した ACS 証明書に基づいて、証明書の要求を生成する必要があるからです。
7. [Certificate Signing Request] のエントリを選択して、[Export] をクリックします。
8. ACS 証明書の **.pem** ファイルをデスクトップに保存します。

ACS 5.1 ソフトウェアでの証明書のインストール

次の手順を実行します。

1. ブラウザを開き、CA サーバ URL **http://10.0.10.10/certsrv** に接続します。
2. [Microsoft Certificate Services] ウィンドウを表示します。 [Request a certificate] を選択します。
3. **advanced certificate request** をクリックして送信します。
4. [Advanced Certificate Request] で、[Submit a certificate request using a base-64-encoded…] をクリックします。
5. ブラウザのセキュリティで許可されている場合は、[Saved Request] フィールドで前の ACS 証明書の要求ファイルをブラウズして挿入します。
6. ブラウザのセキュリティ設定によっては、ディスクのファイルにアクセスできない場合があります。 その場合は、[OK] をクリックして手動で貼り付けます。
7. 前の ACS エクスポートから ACS *.pem ファイルを探します。 テキスト エディタ（Notepad など）を使用して、ファイルを開きます。

8. ファイルの内容をすべて選択して、[Copy] をクリックします。
9. [Microsoft Certificate Services] ウィンドウに戻ります。 コピーした内容を [Saved Request] フィールドに貼り付けます（[Paste]）。
10. [Certificate Template] として [ACS] を選択して、[Submit] をクリックします。
11. 証明書が発行されたら、[Base 64 encoded] を選択して、[Download certificate] をクリックします。
12. [Save] をクリックして、証明書をデスクトップに保存します。
13. [ACS] > [System Administration] > [Configuration] > [Local Server Certificates] に移動します。 [Bind CA Signed Certificate] を選択して、[Next] をクリックします。
14. [Browse] をクリックして、保存した証明書を探します。
15. CA サーバにより発行された ACS 証明書を選択して、[Open] をクリックします。
16. また、[Protocol] の [EAP] チェックボックスをオンにして、[Finish] をクリックします。
17. ACS の [Local Certificate] に、CA により発行された ACS 証明書が表示されます。

Active Directory の ACS ID ストアの設定

次の手順を実行します。

1. ACS に接続して、Admin アカウントにログインします。
2. [Users and Identity Stores] > [External Identity Stores] > [Active Directory] に移動します。
3. アクティブ ディレクトリ ドメイン *demo.local* を入力し、サーバのパスワードを*入力し*、TestConnection をクリックして下さい。 続くために OKIN 順序を**クリックして下さい**。
4. [Save Changes] をクリックします。**注:** ACS 5.x 統合 プロシージャに関する詳細については ACS 5.x およびそれ以降を参照して下さい: Microsoft Active Directory 設定例の統合。

ACS への AAA クライアントとしてのコントローラの追加

次の手順を実行します。

1. ACS に接続して、[Network Resources] > [Network Devices and AAA Clients] に移動します。 [Create] をクリックします。
2. 次のフィールドを入力します。[Name]：**wlc**[IP]：**10.0.1.10**[RADIUS] チェックボックス：**オン**[Shared Secret]：**cisco**
3. 完了したら、[Submit] をクリックします。 [ACS Network Devices] リストで、コントローラがエントリとして表示されます。

ワイヤレス用 ACS アクセス ポリシーの設定

次の手順を実行します。

1. ACS で、[Access Policies] > [Access Services] に移動します。
2. [Access Services] ウィンドウで、[Create] をクリックします。
3. アクセス サービスを作成して、名前（例：WirelessAD）を入力します。 [Based on service template] を選択して、[Select] をクリックします。
4. [Webpage Dialog] で、[Network Access – Simple] を選択します。 [OK] をクリックします。
5. [Webpage Dialog] で、[Network Access – Simple] を選択します。 [OK] をクリックします。テンプレートを選択したら、[Next] をクリックします。
6. [Allowed Protocols] で、[Allow MS-CHAPv2] および [Allow PEAP] チェックボックスをオン

にします。 **[Finish] をクリックします。**
7. ACS により表示される新しいサービスをアクティブにするかを尋ねるプロンプトで、[Yes] をクリックします。
8. 作成およびアクティブ化した新しいアクセス サービスで、[Identity] を展開して選択します。 [Identity Source] で、[Select] をクリックします。
9. ACS に設定した Active Directory に [AD1] を選択し、[OK] をクリックします。
10. [Identity Source] が [AD1] であることを確認して、[Save Changes] をクリックします。

ACS アクセス ポリシーとサービス ルールの作成

次の手順を実行します。

1. [Access Policies] > [Service Selection Rules] に移動します。
2. [Service Selection Policy] ウィンドウで [Create] をクリックします。 新しいルールに名前を付けます（例：*WirelessRule*）。 [Protocol] のチェックボックスをオンにして、[Radius] と一致させます。
3. [Radius] を選択して、[OK] をクリックします。
4. [Results] の [Service] に、[WirelessAD] を選択します（前の手順で作成したもの）。
5. 新しいワイヤレス ルールを作成したら、そのルールを選択して一番上に移動（[Move]）します。一番上のルールは、Active Directory を使用したワイヤレス Radius 認証の識別に使用される最初のルールになります。

Windows の自動機能を使用した PEAP 用クライアントの設定

この例では、CLIENT は、Windows XP Professional SP2 が稼働し、無線クライアントとして機能していて、無線 AP 経由でイントラネット リソースにアクセス可能なコンピュータです。 CLIENT をワイヤレス クライアントとして設定するには、このセクションの手順を実行します。

基本的なインストールと設定の実行

次の手順を実行します。

1. イーサネット ケーブルを使用して CLIENT をハブに接続し、イントラネット ネットワーク セグメントに接続します。
2. CLIENT に、Windows XP Professional SP2 をインストールします。このインストールでは、demo.local ドメインの CLIENT という名前のメンバー コンピュータとして設定します。
3. Windows XP Professional SP2 をインストールします。 このインストールは、PEAP をサポートするために必要です。**注:** Windows XP Professional SP2 では、Windows ファイアウォールが自動的に有効になります。 ファイアウォールは無効にしないでください。

ワイヤレス ネットワーク アダプタのインストール

次の手順を実行します。

1. CLIENT コンピュータをシャットダウンします。
2. CLIENT コンピュータとイントラネット ネットワーク セグメントの接続を解除します。
3. CLIENT コンピュータを再起動し、ローカル管理者アカウントを使用してログインします。

4. ワイヤレス ネットワーク アダプタをインストールします。**注:** 製造元提供の無線アダプタの設定ソフトウェアはインストールしないでください。 ワイヤレス ネットワーク アダプタ ドライバのインストールには、Add Hardware Wizard を使用します。 また、プロンプトが表示された場合は、製造元から提供された CD、または Windows XP Professional SP2 用の最新ドライバが入っているディスクを挿入します。

ワイヤレス ネットワーク接続の設定

次の手順を実行します。

1. ログオフし、**demo.local** ドメインの **WirelessUser** アカウントを使用してログインします。
2. [Start] > [Control Panel] を選択し、[Network Connections] をダブルクリックして、[Wireless Network Connection] を右クリックします。
3. [Properties] をクリックし、[Wireless Networks] タブに移動して、[Use Windows to configure my wireless network settings] にチェックマークが入っていることを確認します。
4. [Add] をクリックします。
5. [Association] タブで、[Network name (SSID)] フィールドに *Employee* と入力します。
6. [Network Authentication] に [WPA] を選択して、[Data encryption] が [TKIP] に設定されていることを確認します。
7. [Authentication] タブをクリックします。
8. EAP type で **Protected EAP (PEAP)** を使用するように設定されていることを確認します。設定されていない場合は、ドロップダウン メニューから選択します。
9. ログイン前にマシンの認証を実行する場合は（この場合、ログイン スクリプトやグループ ポリシー プッシュを適用できます）、[Authenticate as computer when computer information is available] にチェックマークを入れます。
10. **[Properties]**をクリックします。
11. PEAP には、クライアントによるサーバの認証が含まれているため、[Validate server certificate] がチェックされていることを確認します。 また、[Trusted Root Certification Authorities] メニューで、ACS 証明書として発行された CA にチェックマークが付いていることを確認します。
12. [Select Authentication Method] に [Secured password (EAP-MSCHAP v2)] を選択します。これは内部認証として使用されます。
13. [Enable Fast Reconnect] チェックボックスがオンになっていることを確認します。 次に、[OK] を 3 回クリックします。
14. システムトレイのワイヤレス ネットワーク接続のアイコンを右クリックして、[View Available Wireless Networks] をクリックします。
15. Employee のワイヤレス ネットワークをクリックし、[Connect] をクリックします。 接続が成功した場合は、ワイヤレス クライアントに [Connected] と表示されます。
16. 認証が成功したら、Network Connections を使用して、ワイヤレス アダプタの TCP/IP 設定を確認します。 ワイヤレス アダプタには、10.0.20.100 ~ 10.0.20.200 の範囲内のアドレスが、DHCP スコープ、または CorpNet ワイヤレス クライアント用に作成したスコープから割り当てられます。
17. 機能をテストするため、ブラウザを開いて、**http://10.0.10.10**（または、CA サーバの IP アドレス）を表示します。

ACS を使用したワイヤレス認証のトラブルシューティング

次の手順を実行します。

1. [ACS] > [Monitoring and Reports] に移動して、[Launch Monitoring & Report Viewer] をクリックします。
2. 別の ACS ウィンドウが開きます。 [Dashboard] をクリックします。
3. [My Favorite Reports] セクションで、[Authentications – RADIUS – Today] をクリックします。
4. ログにすべての RADIUS 認証が表示され、[Pass] または [Fail] が示されます。 ログに記録されているエントリで、[Details] 列の**虫眼鏡のアイコン**をクリックします。
5. [RADIUS Authentication Detail] に、ログに記録されている試行内容の詳細情報が表示されます。
6. ACS サービスの [Hit Count] に、ACS で作成したルールに一致する試行内容の概要を表示できます。 [ACS] > [Access Policies] > [Access Services] に移動して、[Service Selection Rules] をクリックします。

ACS サーバでの PEAP 認証の失敗

ご使用のクライアントが ACS サーバの PEAP 認証に失敗した場合は、ACS の [Report and Activity] メニューの [Failed attempts] オプションに、「NAS duplicated authentication attempt」エラーメッセージが表示されているかどうかを確認します。

クライアント マシンに Microsoft Windows XP SP2 がインストールされており、Windows XP SP2 が Microsoft IAS サーバ以外のサードパーティ サーバに対して認証を行う場合、このエラーメッセージを受け取る場合があります。 特に、Cisco RADIUS サーバ（ACS）は Extensible Authentication Protocol 型を計算するのに異った方法を使用します: Length: 値 形式（方式 Windows XP 使用より EAP-TLV） ID。 Microsoft では、これを XP SP2 サプリカントの不具合と特定しています。

ホットフィックスについては、Microsoft に問い合わせいただき、『PEAP authentication is not successful when you connect to a third-party RADIUS server』を参照してください。 根本的な問題は、クライアント側の Windows ユーティリティで、PEAP の [Fast Reconnect] オプションがデフォルトでディセーブルになっているのに対し、 サーバ側（ACS）ではデフォルトでイネーブルになっていることにあります。 この問題を解決するには、ACS サーバ（[Global System Options] の下）の [Fast Reconnect] オプションのチェックを外します。 または、クライアント側で [Fast Reconnect] オプションをイネーブルにして問題を解決することもできます。

次の手順を実行して、Windows ユーティリティを使用して Windows XP が稼働しているクライアントで [Fast Reconnect] をイネーブルにします。

1. [Start] > [Settings] > [Control Panel] に移動します。
2. [Network Connections] アイコンをダブルクリックします。
3. [Wireless Network Connection] アイコンを右クリックして、[Properties] をクリックします。
4. [Wireless Networks] タブをクリックします。
5. [Use Windows to configure my wireless network settings] オプションを選択して、Windows でクライアント アダプタを設定できるようにします。
6. SSID を設定済みの場合は、SSID を選択して [Properties] をクリックします。 設定していない場合は、[New] をクリックして新規の WLAN を追加します。
7. [Association] タブで SSID を入力します。 [Network Authentication] が [Open] であり、[Data Encryption] が [WEP] に設定されていることを確認します。

8. [Authentication] をクリックします。
9. [Enable IEEE 802.1x authentication for this network] オプションを選択します。
10. [EAP Type] として [PEAP] を選択して、[Properties] をクリックします。
11. ページの下部の [Enable Fast Reconnect] オプションを選択します。

関連情報

- ACS 4.0 と Windows 2003 を使用した Cisco Unified Wireless Network 環境での PEAP
- Web 認証用の Cisco ワイヤレス LAN コントローラ（WLC）および Cisco ACS 5.x（TACACS+）の設定例
- Cisco Secure Access Control System 5.1 のインストールとアップグレード ガイド
- テクニカルサポートとドキュメント - Cisco Systems