ACS 4.0 と Windows 2003 を使用した Cisco Unified Wireless Network 環境での PEAP

目次

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)4.0 で、Protected Extensible Authentication Protocol（PEAP）と Microsoft Challenge Handshake Authentication Protocol（MS-CHAP; マイクロソフト チャレンジ ハンドシェーク認証プロトコル）バージョン 2 を使用して、セキュアな無

線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 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 4400 シリーズ コントローラ用の初期インストールおよび構成情報に関しては、クイックスタートガイドを参照して下さい: Cisco 4400 シリーズ ワイヤレス LAN コントローラ。 Cisco 2000 シリーズ コントローラ用の初期インストールおよび構成情報に関しては、クイックスタートガイドを参照して下さい: Cisco 2000 シリーズ ワイヤレス LAN コントローラ。

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。

重要： このドキュメントが書かれている時点では、SP1 が Microsoft Windows Server 2003 の最新アップデートで、SP2 とアップデート パッチが Microsoft Windows XP Professional の最新ソフトウェアです。

Windows Server 2003 Enterprise Edition SP1 を使用すると、PEAP 認証用のユーザ証明書およびワークステーション証明書の自動登録を設定できます。 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。

- バージョン 3.2.116.21 が稼働する Cisco 2006 または 4400 シリーズ コントローラ
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) 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)
- Access Control Server (ACS) 4.0 が稼働する Windows 2003 Standard
- 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 3560 スイッチ

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 4.0 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。

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。

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

DC_CA（wirelessdemoca）

DC_CA とは、Windows Server 2003 Enterprise Edition SP1 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 wirelessdemo.local ドメインのドメイン コントローラ
- wirelessdemo.local DNS ドメインの DNS サーバ
- DHCP サーバ
- wirelessdemo.local ドメインのエンタープライズ ルート CA

DC_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する。

ステップ 1： 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 SP1 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 172.16.100.26、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。

ステップ 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

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 wirelessdemo.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 wirelessdemo 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。

ステップ 3： 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. **管理ツール** フォルダ（**Start > Programs > Administrative Tools > アクティブ ディレクトリ ドメインおよび信頼**）からスナップ式**アクティブ ディレクトリ ドメインおよび信頼**を開き次にドメイン コンピュータ **DC_CA.wirelessdemo.local** を右クリックして下さい。
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。

ステップ 4： 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. **管理ツール** フォルダ（**Start > Programs > Administrative Tools > DHCP**）からの **DHCP** スナップインを開き、次に DHCPサーバを、**DC_CA.wirelessdemo.local** 強調表示して下さい。
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 DC_CA.wirelessdemo.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：172.16.100.1End IP address：172.16.100.254Length - **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 172.16.100.1、End IP address に 172.16.100.100 と入力します。 次に [Next] をクリックします。 これにより、172.16.100.1 ～ 172.16.100.100 の範囲内の 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 172.16.100.1 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 **wirelessdemo.local は**、IP Address フィールド**の**タイプ 172.16.100.26、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。

ステップ 5： 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 wirelessdemoca 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。

ステップ 6： 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. wirelessdemoca CA を右クリックし、Properties を選択します。
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 CertificatesDeny に設定されていたり、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 wirelessdemoca CA Properties ダイアログボックスを閉じ、続いて Certification Authority を終了します。

ステップ 7： 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 wirelessdemo.local を展開します。
3. Users 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。

ステップ 8： 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。 この例では、ステップ 7 で追加したコンピュータ Client を使用した手順を紹介しています。Properties をクリックし、Dial-in タブに移動します。
2. Allow access を選択して OK をクリックします。

ステップ 9： 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。

ステップ 10： 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. Allow access を選択して OK をクリックします。

ステップ 11： 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。

ステップ 12： 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。

ステップ 13： 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」セクションのステップ 1 と 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 Secure ACS 4.0 を使用する Windows Standard 2003 のセットアップ

Cisco Secure ACS は、Windows Server 2003 Standard Edition SP1 が稼働していて、コントローラに RADIUS 認証および認可を提供するコンピュータです。 ACS を RADIUS サーバ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

次の手順を実行します。

1. Windows Server 2003 Standard Edition SP1 を、wirelessdemo.local ドメインの ACS という名前のメンバ サーバとしてインストールします。**注:** ACS のサーバ名は、その他の設定では cisco_w2003 と表示されます。 ラボ環境の以降のセットアップでは、ACS あるいは cisco_w2003 で読み換えてください。
2. ローカルエリア接続の場合は、IP アドレスは 172.16.100.26、サブネット マスクは 255.255.255.0、DNS サーバの IP アドレスは 127.0.0.1 で、TCP/IP プロトコルを設定します。

Cisco Secure ACS 4.0 のインストール

注: Cisco Secure ACS 4.0 for Windows の設定方法については、『Cisco Secure ACS for Windows Server Version 4.0 インストレーション ガイド』を参照してください。

次の手順を実行します。

1. ドメイン管理者アカウントを使用して、ACS という名前のコンピュータにログインし、Cisco Secure ACS をインストールします。**注:** サポートされるのは、Cisco Secure ACS をインストールするコンピュータで実行したインストールだけです。 Windows Terminal Services や、Virtual Network Computing（VNC）などの製品を使用したリモート インストールはテストされておらず、サポートされていません。
2. コンピュータの CD-ROM ドライブに Cisco Secure ACS CD を挿入します。
3. CD-ROM ドライブが Windows の自動再生機能をサポートしている場合は、Cisco Secure ACS for Windows Server ダイアログボックスが表示されます。**注:** 必要な Service Pack がコンピュータにインストールされていない場合は、ダイアログボックスが表示されます。Windows の Service Pack の適用は、Cisco Secure ACS のインストール前でもインストール後でもかまいません。 インストールはそのまま続行できますが、インストール完了後に、必ず、必要な Service Pack を適用してください。 これを行わないと、Cisco Secure ACS が正常に機能しない場合があります。
4. 次のタスクのいずれかを実行します。Cisco Secure ACS for Windows Server ダイアログボックスが表示された場合は、Install をクリックします。Cisco Secure ACS for Windows Server ダイアログボックスが表示されない場合は、Cisco Secure ACS CD のルート ディレクトリにある setup.exe を実行します。
5. Cisco Secure ACS Setup ダイアログボックスに、ソフトウェア ライセンス契約書が表示されます。
6. ソフトウェア ライセンス契約書をお読みください。 ソフトウェア ライセンス契約書に同意する場合は、Accept をクリックします。Welcome ダイアログボックスに、セットアップ プログラムに関する基本的な情報が表示されます。
7. Welcome ダイアログボックスの情報を読み終わったら、Next をクリックします。
8. Before You Begin ダイアログボックスに、インストールを続行する前に完了しておく必要のある項目が一覧表示されます。 Before You Begin ダイアログボックスに表示されている項目がすべて完了していたら、各項目に対応するボックスにチェックマークを入れて、Next をクリックします。**注:** Before You Begin ダイアログボックスに表示されている項目がすべて完了していない場合は、Cancel をクリックしてから Exit Setup をクリックします。 Before You Begin ダイアログボックスに表示されているすべての項目を完了してから、インストールを再開します。
9. Choose Destination Location ダイアログボックスが表示されます。 Destination Folder にインストール場所が表示されます。 このドライブとパスが、Cisco Secure ACS がインストールされる場所になります。
10. インストール場所を変更する場合は、次の手順を実行します。[Browse] をクリックします。 Choose Folder ダイアログボックスが表示されます。 Path ボックスに、インストール場所が表示されます。インストール場所を変更します。 Path ボックスに新しい場所を入力するか、Drives and Directories リストを使用して新しいドライブとディレクトリを選択します。 インストール場所は、コンピュータのローカル ドライブである必要があります。**注:** 指定するパスの中に、パーセントの文字（%）は使用しないでください。 使用した場合、インストールは問題なく続行されるように見えますが、途中で失敗します。[OK] をクリックします。**注:** 指定したフォルダが存在しない場合は、フォルダの作成を確認するダイアログボックスが表示されます。 続行する場合は [Yes] をクリックします。
11. Choose Destination Location ダイアログボックスの Destination Folder に、新しいインストール場所が表示されます。
12. [Next] をクリックします。
13. Authentication Database Configuration ダイアログボックスに、ユーザを認証する際のオプションが一覧表示されます。 認証は、Cisco Secure ユーザ データベースだけを使用して実行するか、これに加えて Windows ユーザ データベースも使用して実行することができ

ます。**注:** Cisco Secure ACS のインストール後は、Windows ユーザ データベース以外にも、あらゆる外部ユーザ データベース タイプの認証サポートが設定できるようになります。

14. ユーザの認証に、Cisco Secure ユーザ データベースだけを使用する場合は、Check the Cisco Secure ACS database only オプションを選択します。
15. ユーザの認証に、Cisco Secure ユーザ データベースに加えて、Windows Security Access Manager（SAM）ユーザ データベースまたは Active Directory ユーザ データベースを使用する場合は、次の手順を実行します。Also check the Windows User Database オプションを選択します。Yes, refer to "Grant dialin permission to user" setting チェックボックスが使用可能になります。**注:** Yes, refer to "Grant dialin permission to user" setting チェックボックスは、ダイヤルイン アクセスだけでなく、Cisco Secure ACS で制御されるすべてのアクセス形式に適用されます。 たとえば、VPN トンネル経由でネットワークにアクセスするユーザは、ネットワーク アクセス サーバにダイヤルインはしません。 しかし、Yes, refer to "Grant dialin permission to user" setting ボックスにチェックマークを入れると、Cisco Secure ACS では、ネットワークに対するユーザ アクセスの可否を判別する場合に Windows ユーザのダイヤルイン権限を適用するようになります。Windows ドメイン ユーザ データベースで認証されたユーザにつき、各ユーザが Windows アカウントでダイヤルイン権限を持っているときだけにアクセスを許可する場合は、Yes, refer to "Grant dialin permission to user" setting ボックスにチェックマークを入れます。
16. [Next] をクリックします。
17. セットアップ プログラムによって、Cisco Secure ACS がインストールされ、Windows のレジストリが更新されます。
18. Advance Options ダイアログボックスに、Cisco Secure ACS の機能がいくつか表示されます。これらの機能は、デフォルトでは無効になっています。 これらの機能の詳細については、『Cisco Secure ACS ユーザ ガイド Windows 版 Version 4.0』を参照してください。**注:** ここで説明している機能は、有効になっている場合のみ、Cisco Secure ACS HTML インターフェイスに表示されます。 インストール後は、Interface Configuration セクションの Advanced Options ページで、これらの機能を有効または無効にできます。
19. 有効にする機能につき、それぞれ対応するボックスにチェックマークを入れます。
20. [Next] をクリックします。
21. Active Service Monitoring ダイアログボックスが表示されます。**注:** インストール後は、System Configuration セクションの Active Service Management ページで、アクティブ サービス モニタリング機能を設定できます。
22. Cisco Secure ACS でユーザ認証サービスを監視する場合は、Enable Login Monitoring ボックスにチェックマークを入れます。 Script to Execute リストで、認証サービスが失敗した場合に適用するオプションを次の中から選択します。No Remedial Action Cisco Secure ACS では、スクリプトを実行しません。**注:** このオプションは、イベントのメール通知を有効にする場合に便利です。Reboot Cisco Secure ACS では、Cisco Secure ACS が稼働しているコンピュータを再起動するスクリプトを実行します。Restart All Cisco Secure ACS では、すべての Cisco Secure ACS サービスを再起動します。Restart RADIUS/TACACS+ Cisco Secure ACS では、RADIUS サービスと TACACS+ サービスだけを再起動します。
23. サービス モニタリングでイベントが検出されたときに、Cisco Secure ACS から E メール メッセージを送信させる場合は、Mail Notification ボックスにチェックマークを入れます。
24. [Next] をクリックします。
25. Database Encryption Password ダイアログボックスが表示されます。**注:** データベース暗号化パスワードは、暗号化されて ACS のレジストリに保存されます。 このパスワードは、重大な問題が発生して、データベースに手動でアクセスする必要が発生した場合などに必要になります。 このパスワードは、テクニカルサポートがデータベースにアクセスでき

るように、手元に保存しておいてください。 パスワードは、有効期間が終了するごとに変更できます。
26. データベースの暗号化に使用するパスワードを入力します。 パスワードは、最低 8 文字の長さで、文字と数字の両方を含んでいる必要があります。 無効な文字はありません。
27. [Next] をクリックします。
28. セットアップ プログラムが終了し、Cisco Secure ACS Service Initiation ダイアログボックスが表示されます。
29. 適用する Cisco Secure ACS Services Initiation のオプションにつき、それぞれ対応するボックスにチェックマークを入れます。 各オプションに関連する処理はセットアップ プログラムの終了後に有効になります。Yes, I want to start the Cisco Secure ACS Service now Cisco Secure ACS を構成する Windows サービスを開始します。 このオプションを選択しなかった場合は、コンピュータを再起動するか、CSAdmin サービスを開始するまで、Cisco Secure ACS HTML インターフェイスは使用できません。Yes, I want Setup to launch the Cisco Secure ACS Administrator from my browser following installation 現在の Windows ユーザ アカウントのデフォルト ブラウザで、Cisco Secure ACS HTML インターフェイスを開きます。Yes, I want to view the Readme File Windows のメモ帳（Notepad）で README.TXT ファイルを開きます。
30. [Next] をクリックします。
31. いずれかのオプションを選択していた場合は、Cisco Secure ACS サービスが開始されます。 Setup Complete ダイアログボックスに、Cisco Secure ACS HTML インターフェイスに関する情報が表示されます。
32. **[Finish] をクリックします。注:** その他の設定は、設定する EAP タイプに関するセクションで説明しています。

Cisco LWAPP 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://172.16.101.252 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**の下で VLAN マッピングのための新しいインターフェイスを作成して下さい。
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. これが > Edit Window を示すインターフェイスさせるように情報を設定して下さい。
11. [Apply] をクリックします。

12. [WLANs] タブをクリックします。
13. **新しい**『Create』 を選択 し、『Go』 をクリック して下さい。
14. theWLAN SSID フィールド タイプ**従業員**で Profile Name を入力すれば。
15. WLAN のための ID を選択し、『Apply』 をクリック して下さい。
16. WLAN > Edit Window が示すときこの WLAN のための情報を設定して下さい。**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. ステータス ボックスが**イネーブルになったが**あるように確認され、適切な**インターフェイス** (従業員) が選択されるようにして下さい。 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. **レイヤ2** サブメニューの下でレイヤ2 セキュリティがあるように **WPA + WPA2** 確認して下さい。 WPA2 暗号化に関しては **AES + TKIP** TKIP クライアントを許可するためにチェックして下さい。
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サーバが設定されれば適切なサーバは認証 メニューから選択することができます。
23. どの特別な confiugrations でも必要とならなければ **QoS** および **Advanced タブは**デフォルトで残すことができます。
24. [Security] メニューをクリックし、RADIUS サーバを追加します。
25. **RADIUS** サブメニューの下で**認証を**クリックして下さい。 次に [New] をクリックします。
26. RADIUS サーバの IP アドレス (172.16.100.25) 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。 ネットワーク ユーザ ボックスがチェックされるし、『Apply』 をクリック して下さいように。
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 DC_CA 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 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。 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** をタイプし、『OK』 をクリック して下さい。
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 と入力すると、Certificate Templates スナップインが開きます。

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。**重要：** [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。 これら二つのオプションをディセーブルにしない場合、自動登録 エラーという結果に終る自動登録は E メールを使用するように試みます。
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。 ステップに作成の 1-3 ACS Webサーバ セクションのための証明書のテンプレート従い、オプションを**認証局（CA）**選択し、『Local Computer』 を選択 し、『Finish』 をクリック して下さい。

2. コンソール ツリーで、wirelessdemoca を展開し、Certificate Templates を右クリックします。
3. **New > Certificate Template to Issue** の順に選択します。
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、wirelessdemo.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は、**Computer Configuration > Windows Settings > Security Settings > 公開キー ポリシーを**拡張し、次に**証明書要求設定を**『Automatic』 を選択 して下さい。
9. **自動証明書要求設定を**右クリックし、**> 自動証明書要求** 『New』 を選択 して下さい。
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. 詳細ペインの Autoenrollment 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 4.0 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

重要： 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。

重要： 証明書の設定作業中は、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. Enterprise 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. ローカル ACS マシンで、ブラウザから http://<ルート CA の IP アドレス>/certsrv で Microsoft 認証局サーバを指定します。 この例では、IP アドレスは 172.16.100.26 です。
3. Administrator でログインします。
4. [Request a Certificate] を選択して、[Next] をクリックします。
5. [Advanced Request] を選択して、[Next] をクリックします。
6. Create and submit a request to this CA を選択して、Next をクリックします。**重要：** 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 Templates で、前の手順で作成した ACS という名前の証明書テンプレートを選

択します。 テンプレートを選択すると、オプションが変更されます。
8. Name に、ACS サーバの完全修飾ドメイン名を設定します。 この場合 ACS サーバ名は cisco_w2003.wirelessdemo.local です。 **ローカル コンピュータ証明書ストアのストア 認証がチェックされるし、『SUBMIT』** をクリック して下さいように。
9. ポップアップ ウィンドウに、スクリプト違反の可能性があることを示す警告が表示されます。 [Yes] を選択します。
10. [Install this certificate] をクリックします。
11. ポップアップ ウィンドウがもう一度表示され、スクリプト違反の可能性があることが警告されます。 [Yes] を選択します。
12. Yes をクリックすると、証明書がインストールされます。
13. この時点で、認証は**個人的**の下の認証 MMC に **> 認証**インストールされています。
14. これで、ローカル コンピュータ（この例では、ACS または cisco_w2003）に証明書がインストールされたので、続いて ACS 4.0 の証明書ファイル設定用の証明書ファイル（.cer）を生成する必要があります。
15. ACS サーバで（この例では cisco_w2003）、ブラウザから http://172.16.100.26 /certsrv の Microsoft 認証局サーバを指定します。

ACS 4.0 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. ACS サーバで（この例では cisco_w2003）、ブラウザから http://172.16.100.26 /certsrv の Microsoft CA サーバを指定します。
2. Select a Task オプションから Download a CA certificate, certificate chain or CRL を選択します。
3. 無線エンコード方式として Base 64 を選択し、Download CA Certificate をクリックします。
4. File Download Security Warning ウィンドウが表示されます。 [Save] をクリックします。
5. ACS.cer など任意の名前でファイルを保存します。 この名前は、ACS 4.0 の ACS Certificate Authority のセットアップで使用しますので、覚えておいてください。
6. インストール時に作成されたデスクトップのショートカットを使用して、ACS Admin を開きます。
7. System Configuration をクリックします。
8. [ACS Certificate Setup] をクリックします。
9. [Install ACS Certificate] をクリックします。
10. Use certificate from storage を選択し、完全修飾ドメイン名の cisco_w2003.wirelessdemo.local（名前に ACS を使用している場合は ACS.wirelessdemo.local）を入力します。
11. [Submit] をクリックします。
12. System Configuration をクリックします。
13. Service Control をクリックし、Restart をクリックします。
14. System Configuration をクリックします。
15. [Global Authentication Setup] をクリックします。
16. Allow EAP-MSCHAPV2 と Allow EAP-GTC にチェックマークを入れます。
17. [Submit + Restart] をクリックします。
18. System Configuration をクリックします。
19. ACS Certification Authority Setup をクリックします。
20. ACS Certification Authority Setup ウィンドウで、前の手順で作成した *.cer ファイルの名前

と場所を入力します。 この例では、作成した *.cer ファイルは ACS.cer で、ルート ディレクトリの c:\ に保存されています。
21. CA certificate file フィールドに c:\acs.cer と入力し、Submit をクリックします。
22. ACS サービスを再起動します。

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、wirelessdemo.local ドメインの CLIENT という名前のメンバ 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。**重要：** 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、wirelessdemo.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. ネットワーク認証のために『WPA』 を選択 し、データ暗号化が **TKIP** に設定 されるようにして下さい。
7. Authentication タブに移動します。
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。そうなっていない場合は、ドロップダウン メニューでこれを選択します。
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 がクライアントによってサーバの認証を含むように確認して下さいサーバ証明をチェックされる検証する。 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. システムトレイの無線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 の無線ネットワークをクリックし、Connect をクリックします。次のスクリーン ショットは、接続が正常に完了したかどうかを示しています。
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。 無線アダプタには、172.16.100.100 ～ 172.16.100.254 の範囲内のアドレスが、DHCP スコープ、または無線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://wirelessdemoca (または、エンタープライズ CA サーバの IP アドレス) を表示します。

問題： トークン認証プラットフォームの場合、Odyssey クライアントでプロンプトが 3 回表示される

この問題は、すべての Windows バージョンと 2.x のソリューションで発生します。

通常は、XP の無線サービスの設定が原因でこの問題が発生します。

この問題を解決するには、次の手順を実行します。

1. [Start] > [Settings] > [Control Panel] > [Administrative Tools] > [Services] の順に選択します。
2. リストの最後に移動して、Wireless Zero Configuration を探します。
3. この設定をダブルクリックします。
4. このサービスを停止するオプションを選択します。
5. 起動タイプの設定で disable を選択します。**注:** サービスを停止しただけでは、再起動時にサービスも再び起動してしまいます。そのため、この問題が再発しないようにするには、サービスを無効にする必要があります。
6. 設定を保存して終了します。

ACS サーバでの PEAP 認証の失敗

クライアントが認証 ACS サーバの PEAP 失敗するとき、ACS の**レポートおよびアクティビティ**メニューの下で **Failed Attempts オプション**の*「NAS によって重複させている認証 の 試み」*エラーメッセージを見つけるかどうか確認して下さい。

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関しては、Microsoft に連絡し、技術情報 KB885453 を参照して下さい。 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ために、**ファーストの再接続し、**ACS サーバのオプションを押します **submit+restart を**チェックを外して下さい。 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。

ファーストを有効に するためにこれらのステップを再接続します Windows ユーティリティを使用して Windows XP を実行するクライアントで完了して下さい:

1. Start > Settings > Control Panel の順にクリック して下さい。
2. **Network Connections アイコンを**ダブル クリックして下さい。
3. **無線ネットワーク接続** アイコンを右クリックし、『Properties』 をクリック して下さい。
4. [Wireless Networks] タブをクリックします。
5. クライアントアダプタを設定する Enable ウィンドウに*無線ネットワーク設定*オプションを*設定するために使用 Windows* をチェックして下さい。
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。 そうでなかったら、新しい WLAN を追加するために『New』 をクリック して下さい。
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. *この Network オプションがあるようにイネーブル IEEE 802.1x 認証*を確認して下さい。
10. *EAP 型*を **PEAP** として選択し、『Properties』 をクリック して下さい。
11. **イネーブル ファーストを再接続します**ページの一番下にオプションをチェックして下さい。

関連情報

- WLAN Controller（WLC）での EAP 認証の設定例
- ワイヤレスLAN コントローラ コンフィギュレーション ガイド
- Wireless LAN Controller と Lightweight アクセス ポイントの基本設定例
- 無線 LAN コントローラでの VLAN の設定例
- ワイヤレス LAN コントローラを使用した AP グループ VLAN の設定例
- テクニカルサポートとドキュメント - Cisco Systems