

Microsoft Internet Authentication Service (IAS) を使用した Unified Wireless Network での PEAP

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[PEAP の概要](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[Microsoft Windows 2003 Server の設定](#)

[Microsoft Windows 2003 Server の設定](#)

[Microsoft Windows 2003 Server での DHCP サービスのインストールと設定](#)

[Microsoft Windows 2003 Server の認証局 \(CA \) サーバとしてのインストールと設定](#)

[ドメインへのクライアントの接続](#)

[Microsoft Windows 2003 Server での Internet Authentication Service のインストールと証明書の要求](#)

[Internet Authentication Service での PEAP-MS-CHAP v2 認証の設定](#)

[Active Directory へのユーザの追加](#)

[ユーザに無線アクセスを許可する](#)

[Wireless LAN Controller と Lightweight AP の設定](#)

[MS IAS RADIUS サーバで RADIUS 認証を行うための WLC の設定](#)

[WLAN でのクライアントの設定](#)

[ワイヤレスクライアントの設定](#)

[ワイヤレスクライアントでの PEAP-MS-CHAP v2 認証の設定](#)

[確認とトラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、RADIUS サーバに Microsoft Internet Authentication Service (IAS) を使用した Cisco Unified Wireless Network で Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) バージョン 2 認証を使用した Protected Extensible Authentication Protocol (PEAP) を設定する際の設定例を紹介しています。

[前提条件](#)

[要件](#)

このドキュメントではテストを行うための特定の設定のみが取り上げられており、読者に Windows 2003 と Cisco コントローラのインストールに関する基本知識があることが前提となっています。

注：このドキュメントは、PEAP - MS CHAP 認証のために MS サーバで必要な設定の例を読者に示すことを目的としています。このセクションで示す Microsoft サーバの設定はラボでテスト済みで、期待通りに動作することが確認されています。Microsoft サーバを設定する上で問題がある場合は、Microsoft に連絡してください。Cisco TAC では、Microsoft Windows サーバの設定に関するサポートは行っていません。

Cisco 4400 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 4400 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。

[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いています。

- ファームウェア バージョン 4.0 が稼働している Cisco 4400 シリーズ コントローラ
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Internet Authentication Service (IAS)、Certificate Authority (CA; 認証局)、DHCP、および Domain Name System (DNS; ドメイン ネーム システム) のサービスを搭載した Windows 2003 Enterprise Server (SP1)
- Windows XP Professional SP2 (および最新の Service Pack) と Cisco Aironet 802.11a/b/g Wireless Network Interface Card (NIC; ネットワーク インターフェイス カード)
- Aironet Desktop Utility バージョン 4.0
- Cisco 3560 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ました。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実稼働中である場合には、どのようなコマンドについても、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。

[表記法](#)

ドキュメント表記の詳細については、『[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。

[PEAP の概要](#)

PEAP では、Transport Level Security (TLS) を使用して、ワイヤレス ラップトップなど認証対象の PEAP クライアントと Microsoft Internet Authentication Service (IAS) や任意の RADIUS サーバなどの PEAP オーセンティケータとの間に暗号化チャネルを作成します。PEAP では認証方式は指定されませんが、PEAP により提供される TLS 暗号化チャネルで動作できる EAP-MSCHAPv2 などの他の EAP 認証プロトコルに対してセキュリティが付加されます。PEAP の認証プロセスは、主に次の 2 つのフェーズで構成されます。

PEAPフェーズ1:TLS暗号化チャネル

ワイヤレス クライアントで AP とのアソシエーションが確立されます。IEEE 802.11 ベースの関連付けでは、クライアントとアクセス ポイント (LAP) でセキュアなアソシエーションが確立される前に、オープン システムや共有秘密鍵による認証が提供されます。クライアントとアクセス ポイントの間に IEEE 802.11 ベースのアソシエーションが確立されると、AP との TLS セッションがネゴシエートされます。ワイヤレス クライアントと IAS サーバの間での認証が完了すると、それらの間で TLS セッションがネゴシエートされます。このネゴシエーションで生成された鍵が、後続のすべての通信の暗号化に使用されます。

PEAPフェーズ2:EAP認証通信

PEAP 認証プロセスの最初の段階で PEAP が作成した TLS チャネルで、EAP ネゴシエーションを含む EAP 通信が発生します。IAS サーバでは、EAP-MS-CHAP v2 でワイヤレス クライアントの認証が行われます。LAP とコントローラでは、ワイヤレス クライアントと RADIUS サーバの間でのメッセージの転送だけが行われます。この WLC と LAP は TLS のエンドポイントではないため、これらのメッセージの復号化はできません。

PEAP のステージ 1 が発生し、IAS サーバと 802.1X ワイヤレス クライアントの間で TLS チャネルが作成された後、PEAP-MS-CHAP v2 でパスワード ベースの有効なクレデンシャルをユーザが提供した成功時の認証における RADIUS のメッセージシーケンスは次のようになります。

1. IAS サーバが ID 要求メッセージをクライアントに送信します (EAP-Request/Identity) 。
2. クライアントが ID 応答メッセージを返します (EAP-Response/Identity) 。
3. IAS サーバが MS-CHAP v2 チャレンジメッセージを送信します (EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge)) 。
4. クライアントが MS-CHAP v2 のチャレンジと応答で答えます (EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response)) 。
5. IAS サーバがクライアントの認証に成功すると、サーバが MS-CHAP v2 成功パケットを返します (EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success)) 。
6. クライアントがサーバの認証に成功すると、クライアントは MS-CHAP v2 成功パケットで答えます (EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success)) 。
7. IAS サーバが認証の成功を示す EAP-TLV を送信します。
8. クライアントが EAP-TLV ステータスの成功メッセージを返します。
9. サーバが認証を完了し、EAP-Success メッセージをプレーン テキストで送信します。クライアントの分離に VLAN が展開されている場合は、このメッセージに VLAN の属性が含まれています。

設定

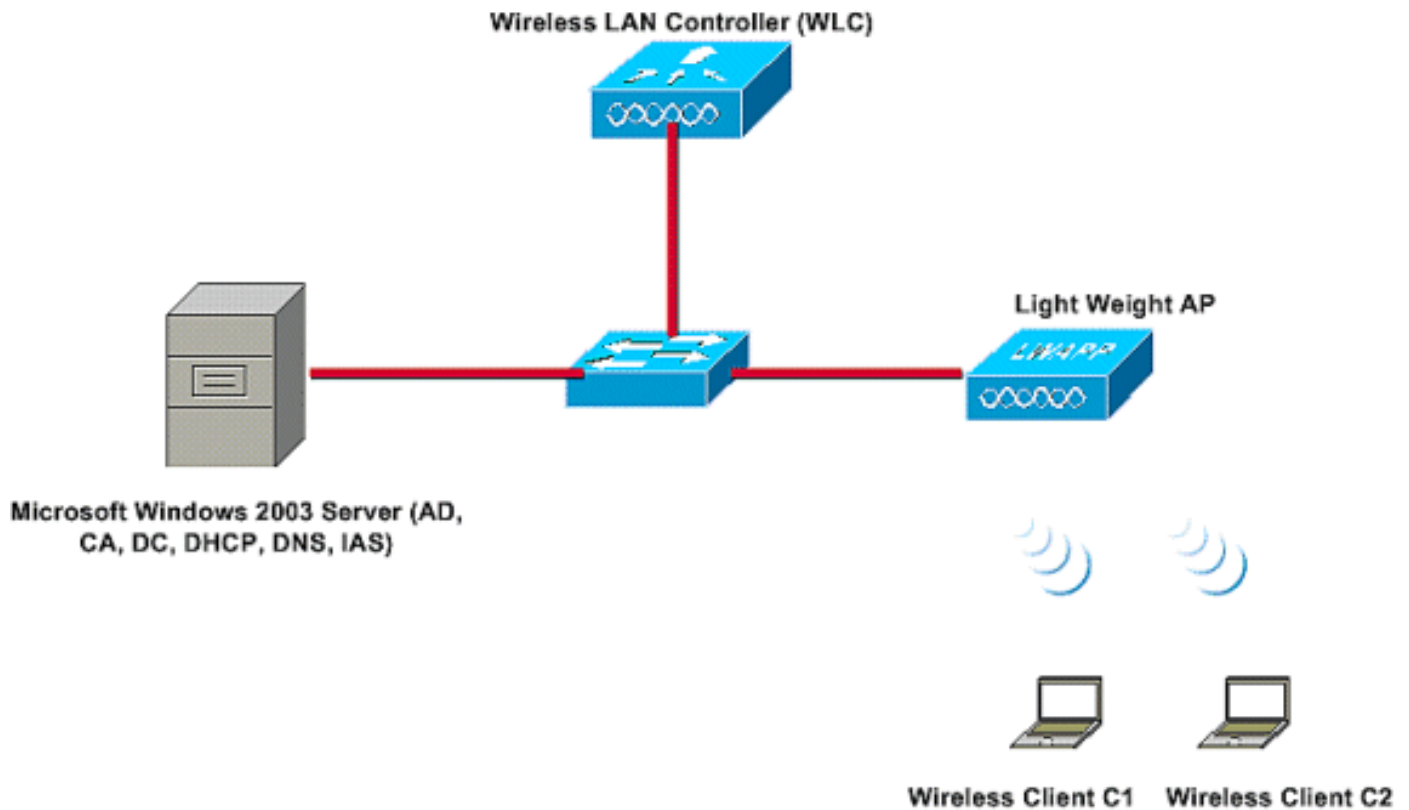
このドキュメントでは、PEAP MS-CHAP v2 の設定例を紹介しています。

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)を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

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 セットアップを使用します。



この設定では、Microsoft Windows 2003 Server は次の役割を果たします。

- ドメイン **Wireless.com** のドメイン コントローラ
- DHCP/DNS サーバ
- 認証局 (CA) サーバ
- Active Directory : ユーザ データベースの管理
- Internet Authentication Service (IAS) : ワイヤレス ユーザの認証

図のように、このサーバはレイヤ 2 スイッチを介して有線ネットワークに接続しています。

Wireless LAN Controller (WLC) と登録済み LAP もレイヤ 2 スイッチを介してネットワークに接続しています。

ワイヤレス クライアント C1 と C2 は、Wi-Fi Protected Access 2 (WPA 2) - PEAP MSCHAP v2 認証を使用してワイヤレス ネットワークに接続しています。

目標は、PEAP MSCHAP v2 認証でワイヤレス クライアントを認証するように、Microsoft 2003 Server、Wireless LAN Controller、および Light Weight AP を設定することです。

次のセクションでは、この構成でデバイスを設定する方法を説明します。

設定

このセクションでは、この WLAN に PEAP MS-CHAP v2 認証を設定するために必要な設定を確認しています。

- Microsoft Windows 2003 Server の設定
- Wireless LAN Controller (WLC) と Light Weight AP の設定
- ワイヤレス クライアントの設定

Microsoft Windows 2003 Server の設定から始めます。

Microsoft Windows 2003 Server の設定

Microsoft Windows 2003 Server の設定

ネットワーク設定のセクションで説明されているように、Microsoft Windows 2003 Server はネットワークで次の機能を行うために使用されます。

- ドメイン コントローラ : ドメイン Wireless 用
- DHCP/DNS サーバ
- 認証局 (CA) サーバ
- Internet Authentication Service (IAS) : ワイヤレス ユーザの認証
- Active Directory : ユーザ データベースの管理

Microsoft Windows 2003 Server を、上記のサービスを行うように設定します。ドメイン コントローラとしての Microsoft Windows 2003 Server の設定から開始します。

ドメイン コントローラとしての Microsoft Windows 2003 Server の設定

Microsoft Windows 2003 Server をドメイン コントローラとして設定するには、次の手順を実行します。

1. **Start**、**Run** の順にクリックし、**dcpromo.exe** と入力して **OK** をクリックし、**Active Directory Installation Wizard** を起動します。



2. **Next** をクリックして Active Directory Installation Wizard を実行します。

Active Directory Installation Wizard



Operating System Compatibility

Improved security settings in Windows Server 2003 affect older versions of Windows.



Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.

Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 or earlier, do not meet these requirements. Similarly, some non-Windows systems, including Apple Mac OS X and SAMBA clients, might not meet these requirements.

For more information, see [Compatibility Help](#).

< Back

Next >

Cancel

3. 新しいドメインを作成するため、オプション **Domain Controller for a new domain** を選択します。

Active Directory Installation Wizard

Domain Controller Type

Specify the role you want this server to have.



Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?

Domain controller for a new domain

Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.

Additional domain controller for an existing domain



Proceeding with this option will delete all local accounts on this server.

All cryptographic keys will be deleted and should be exported before continuing.

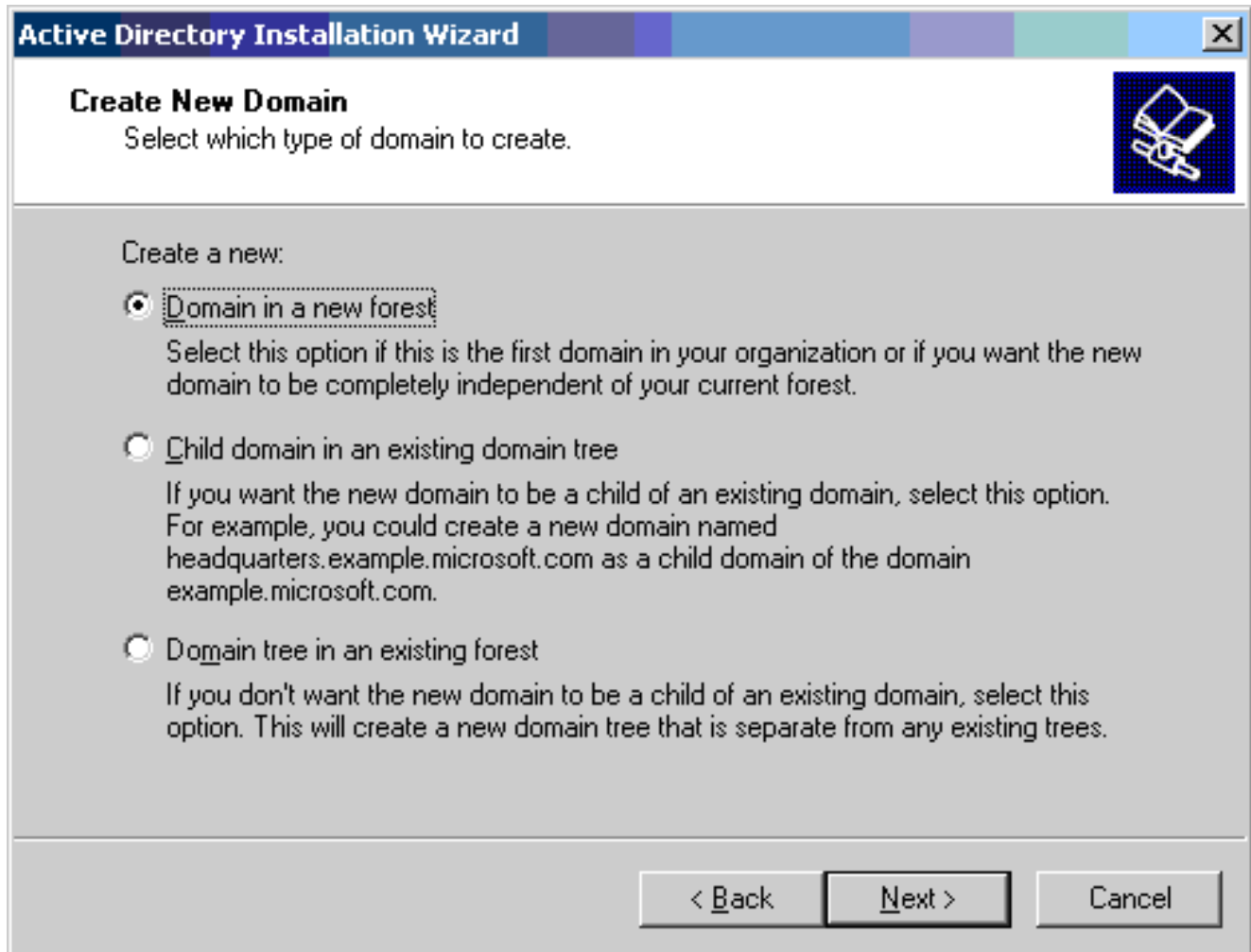
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

< Back

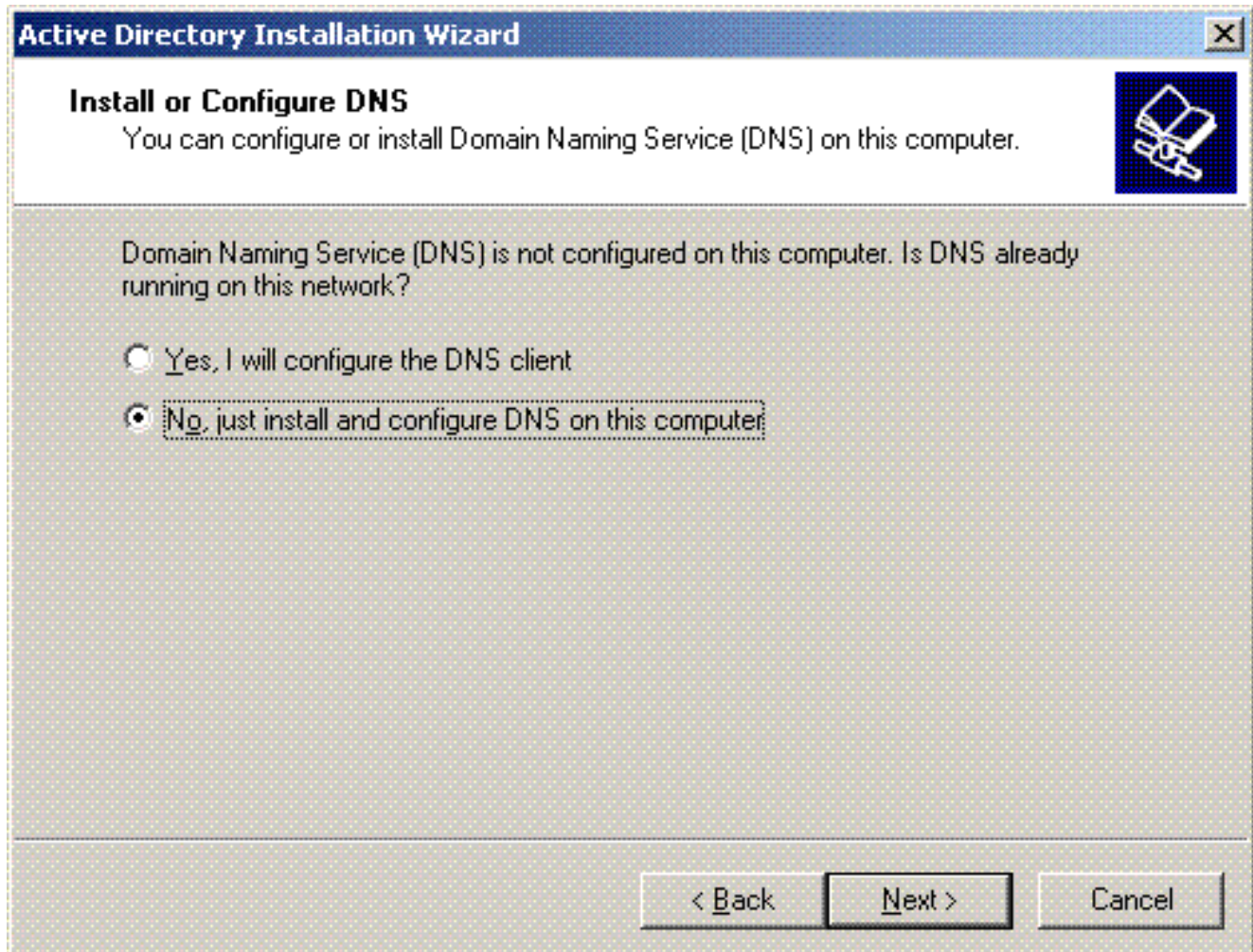
Next >

Cancel

4. **New** をクリックし、ドメイン ツリーの新しいフォレストを作成します。



5. システムに DNS がインストールされていない場合は、ウィザードにより DNS を設定するためのオプションが提示されます。このコンピュータでは **No, Just Install and Configure DNS** を選択します。[next] をクリックします。



6. 新しいドメインの完全な DNS 名を入力します。この例では、**Wireless.com** が使用されており、**Next** をクリックします。

Active Directory Installation Wizard [X]

New Domain Name
Specify a name for the new domain.

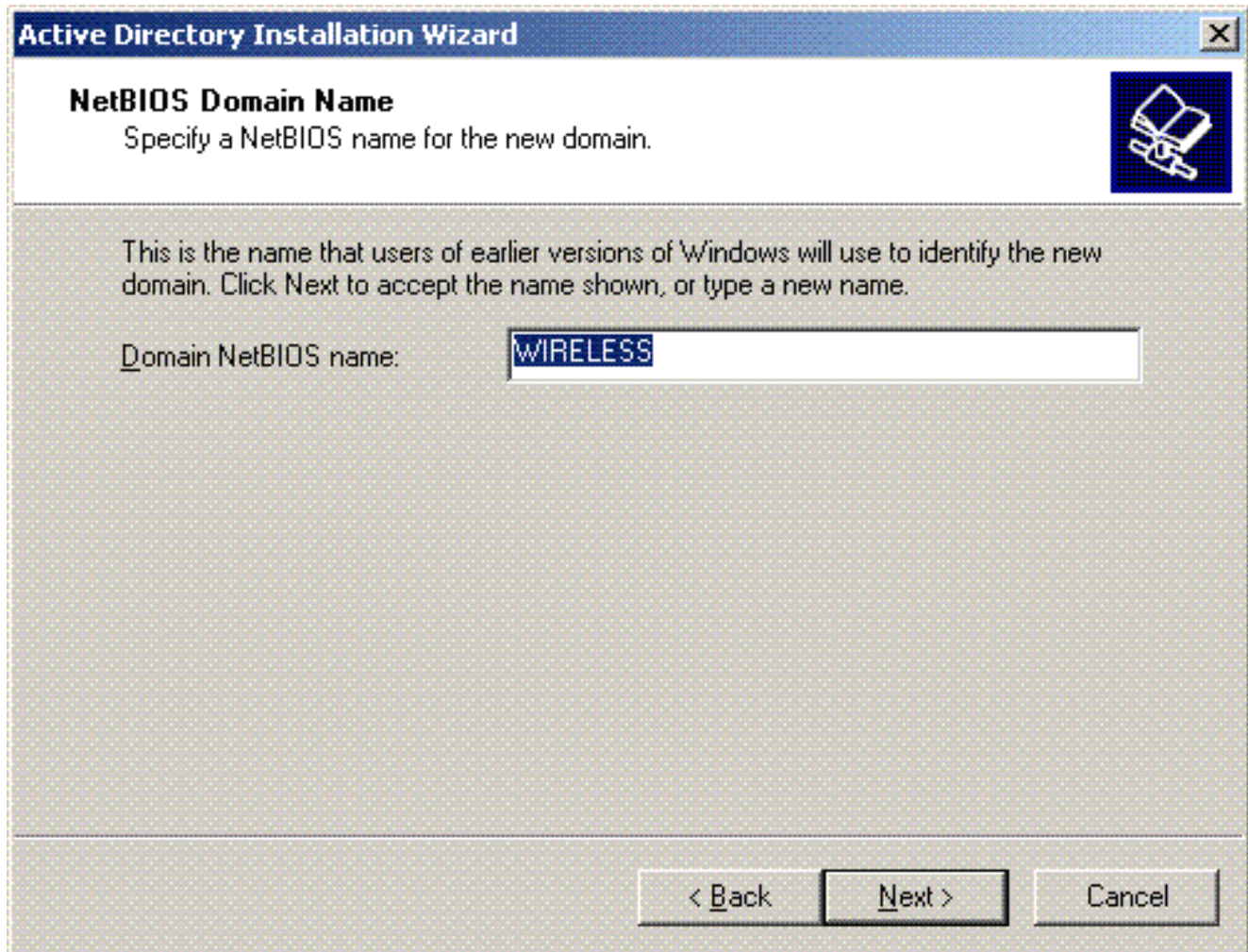
Type the full DNS name for the new domain
(for example: headquarters.example.microsoft.com).

Full DNS name for new domain:

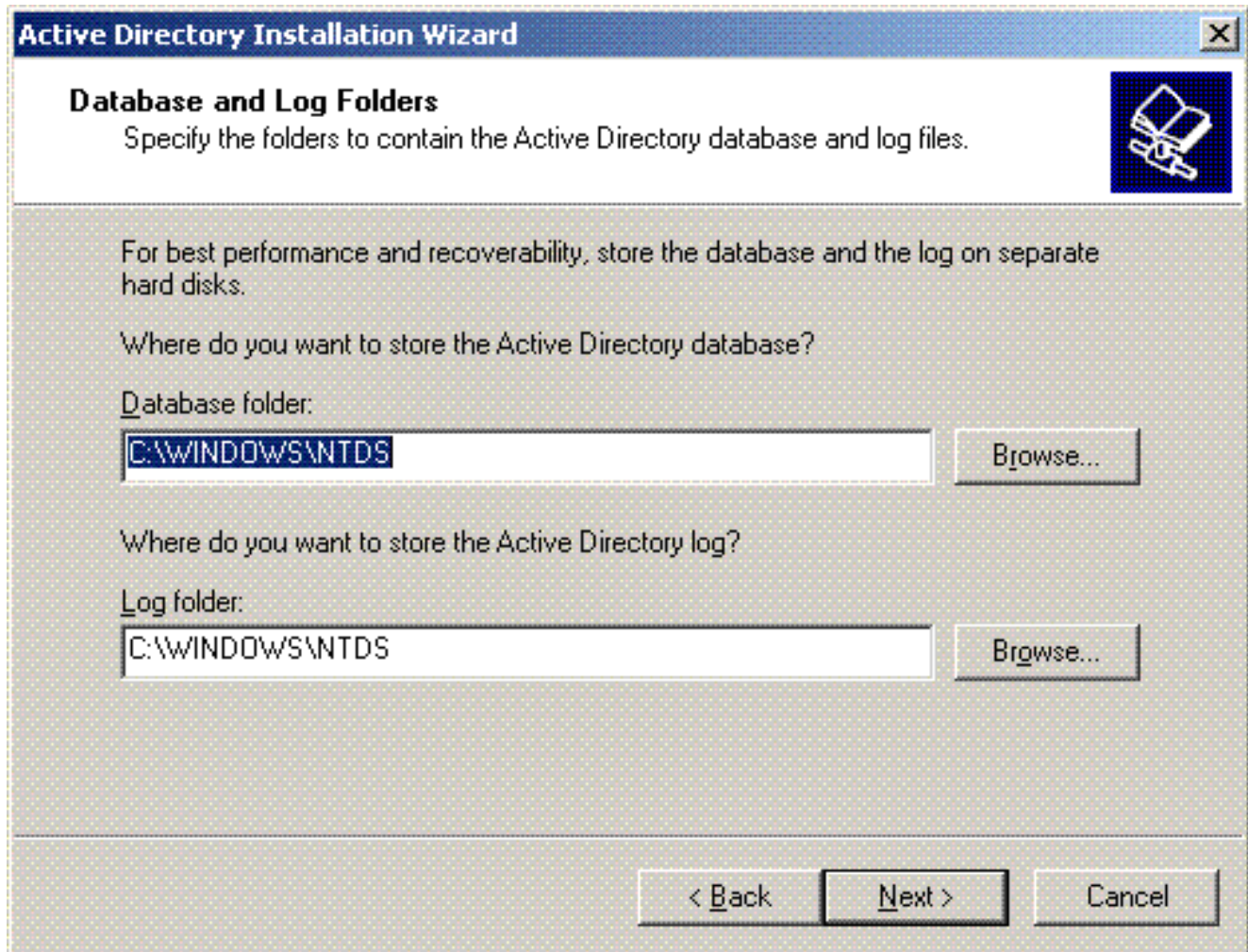
Wireless.com

< Back Next > Cancel

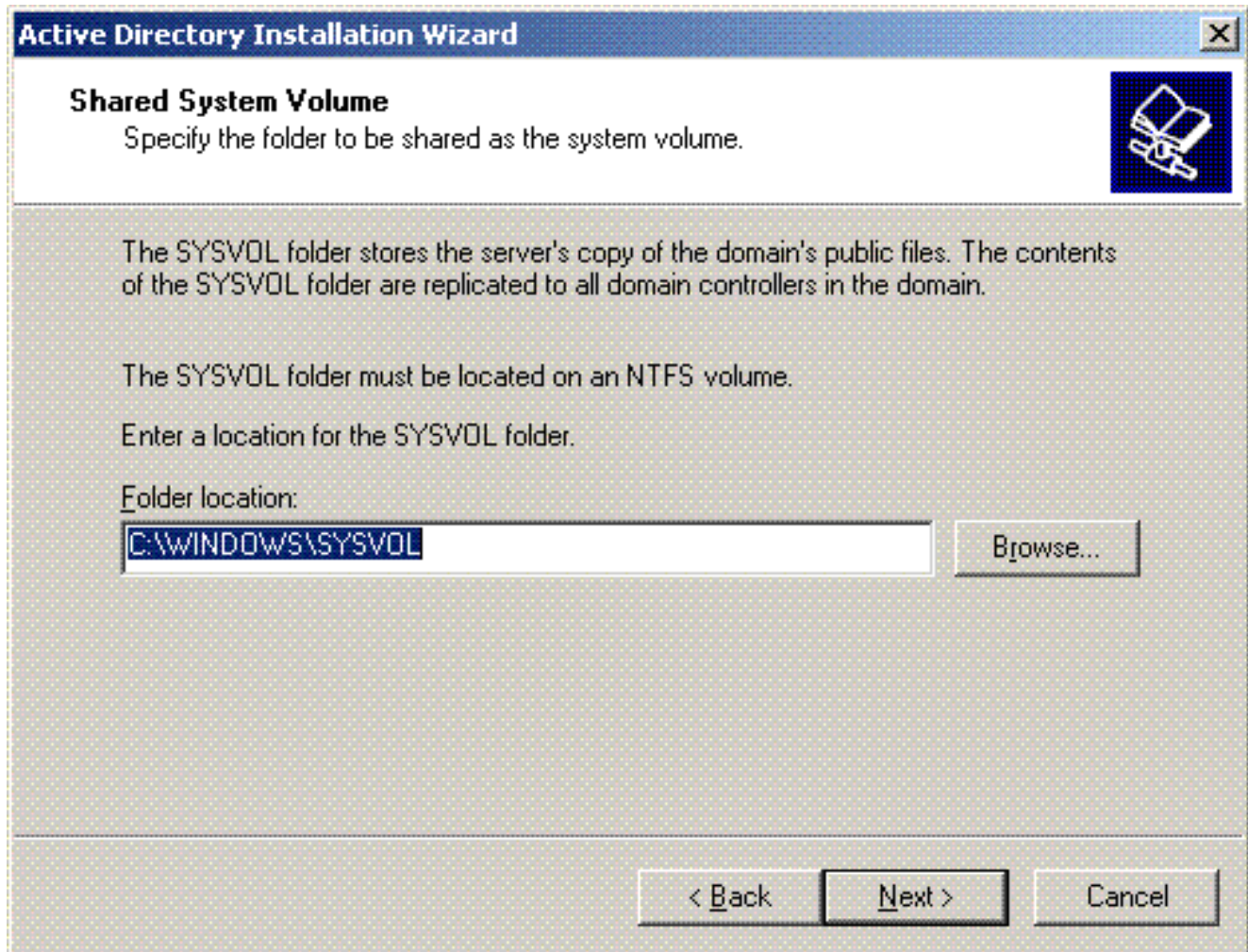
7. ドメインの NETBIOS 名を入力し、**Next** をクリックします。この例では **WIRELESS** を使用しています。



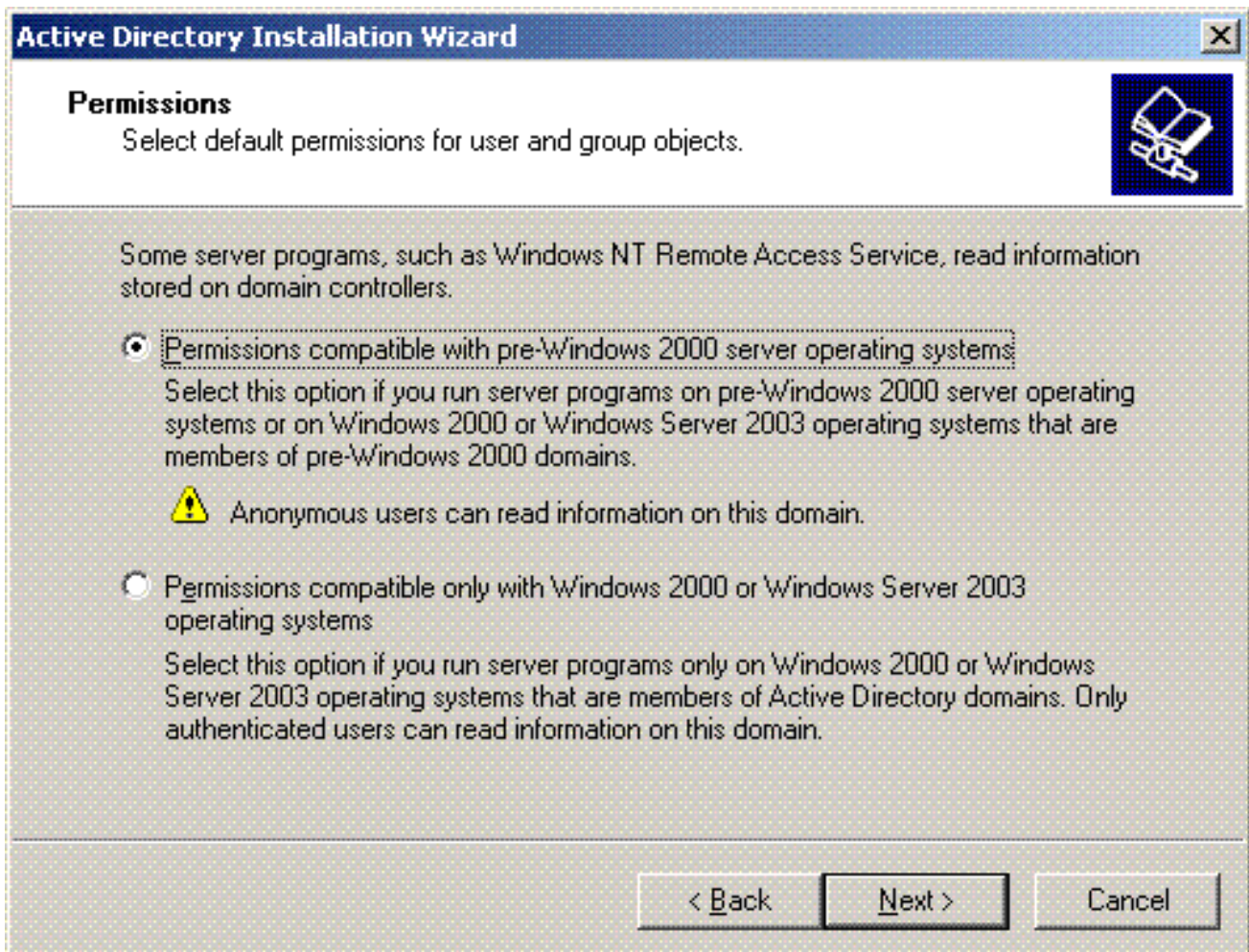
8. ドメインのデータベースとログのロケーションを選択します。[next] をクリックします。



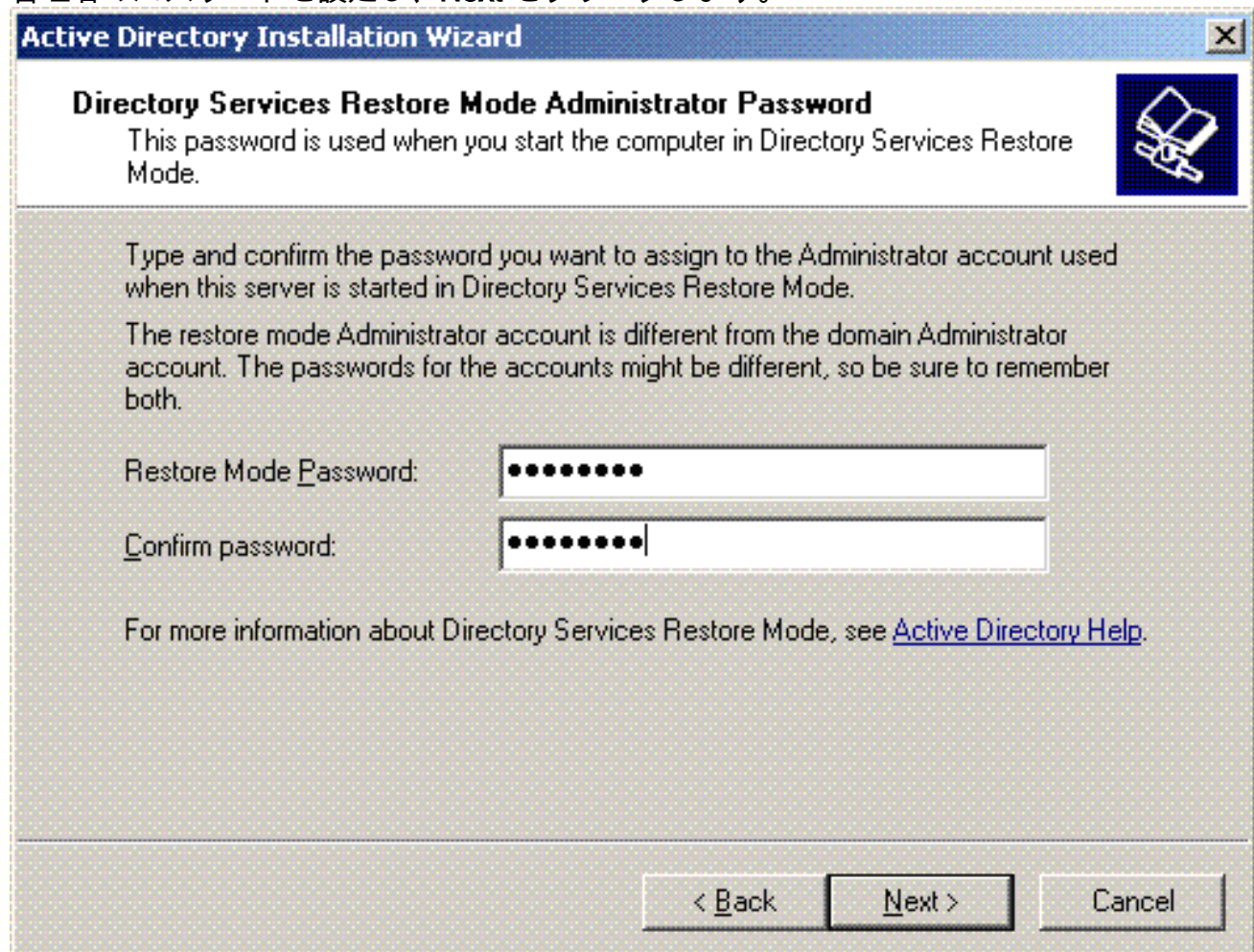
9. Sysvol フォルダのロケーションを選択します。[next] をクリックします。



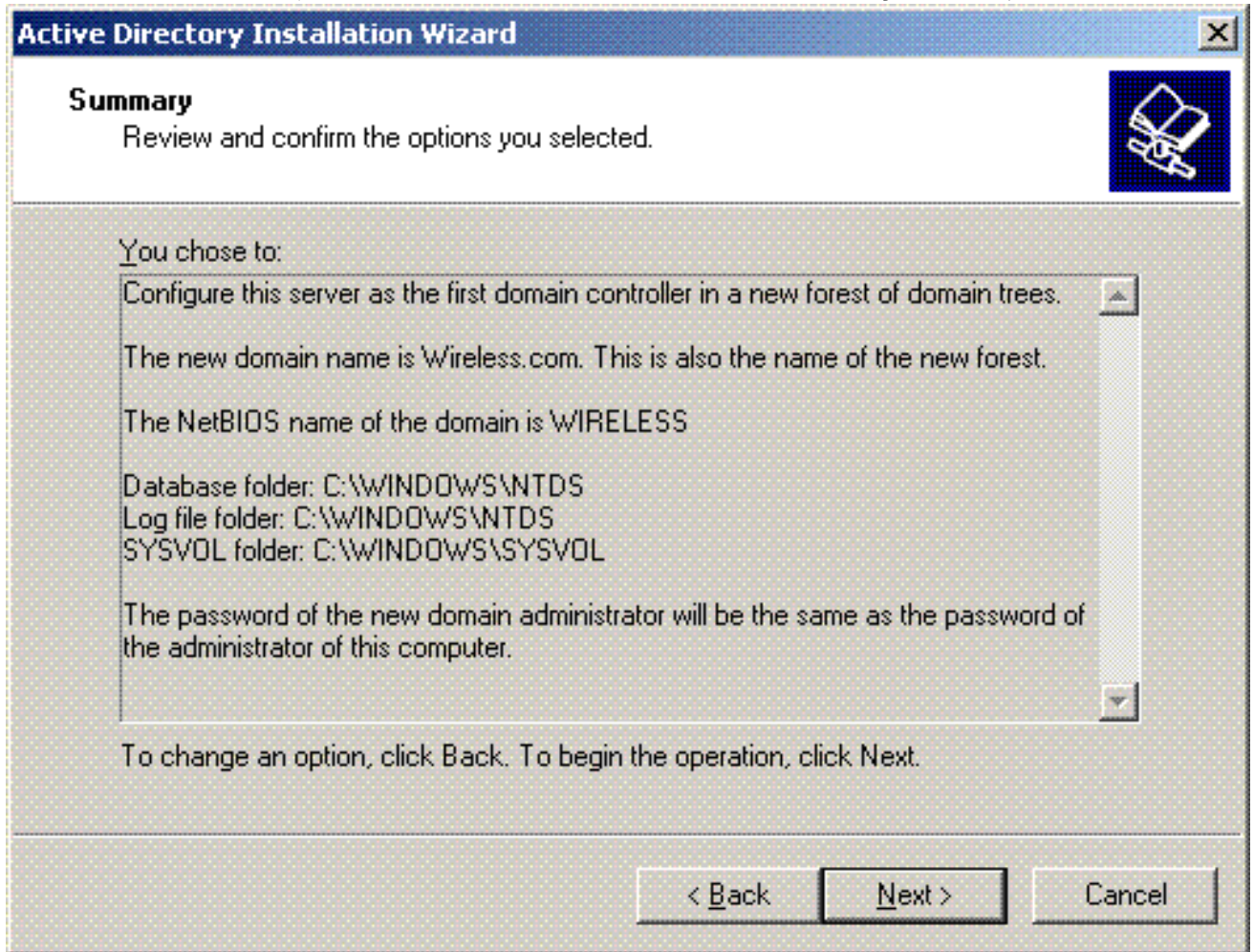
10. ユーザとグループのデフォルトのアクセス許可を選択します。[next] をクリックします。



11. 管理者のパスワードを設定し、Next をクリックします。



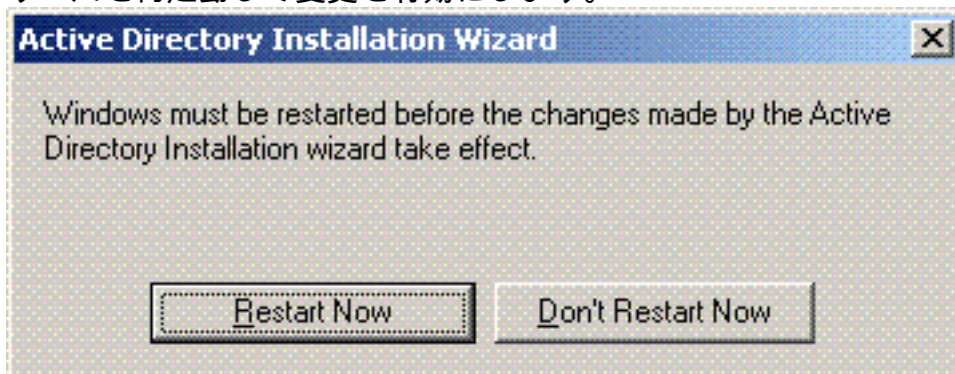
12. **Next** をクリックして、先ほど設定したドメインのオプションを承認します。



13. **Finish** をクリックして Active Directory Installation Wizard を閉じます。



14. サーバを再起動して変更を有効にします。

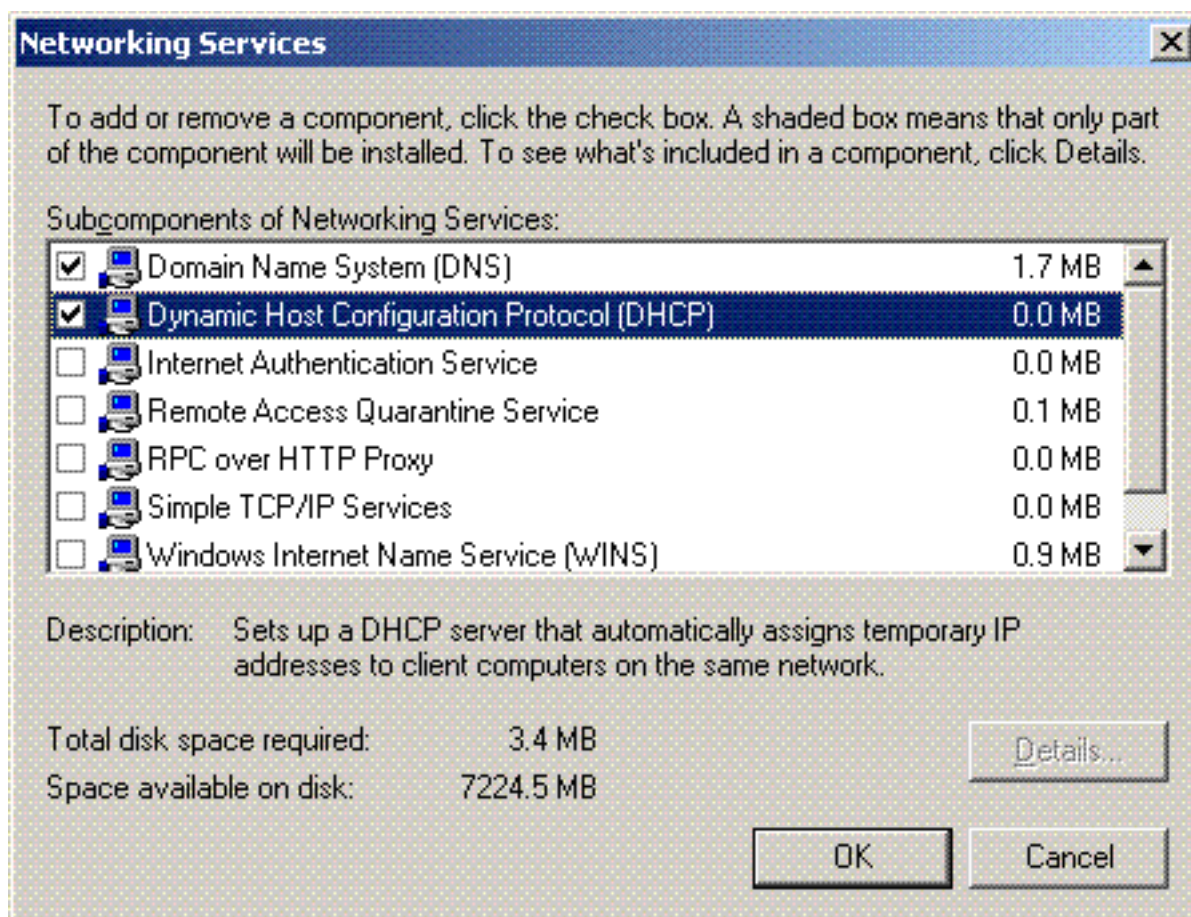


この手順では、Microsoft Windows 2003 Server をドメイン コントローラとして設定し、新しいドメイン **Wireless.com** を作成しました。次に、サーバ上に DHCP サービスを設定します。

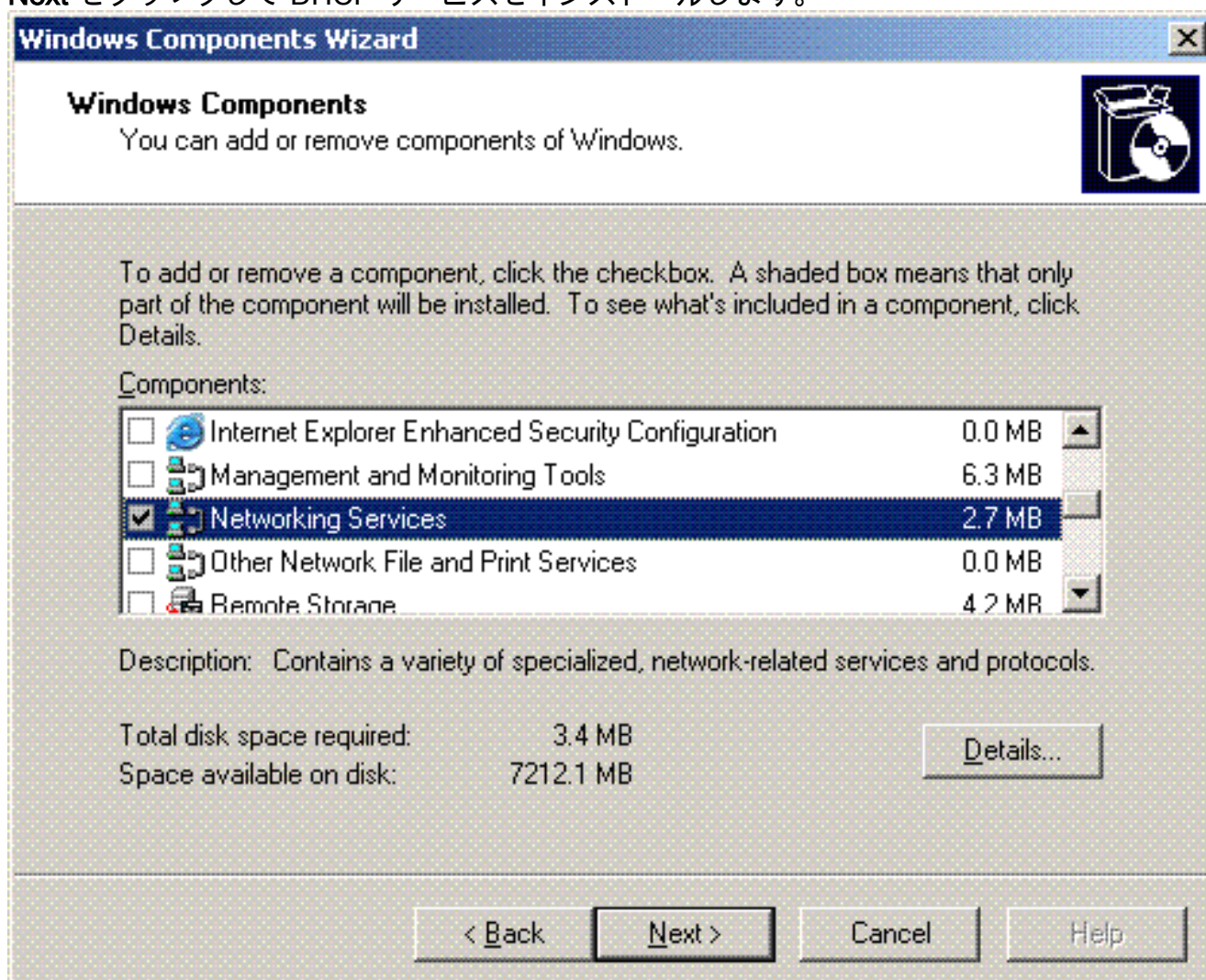
[Microsoft Windows 2003 Server での DHCP サービスのインストールと設定](#)

Microsoft 2003 Server 上の DHCP サービスは、ワイヤレス クライアントに IP アドレスを提供するために使用されます。DHCP サービスをサーバにインストールし設定するには、次の手順を実行します。

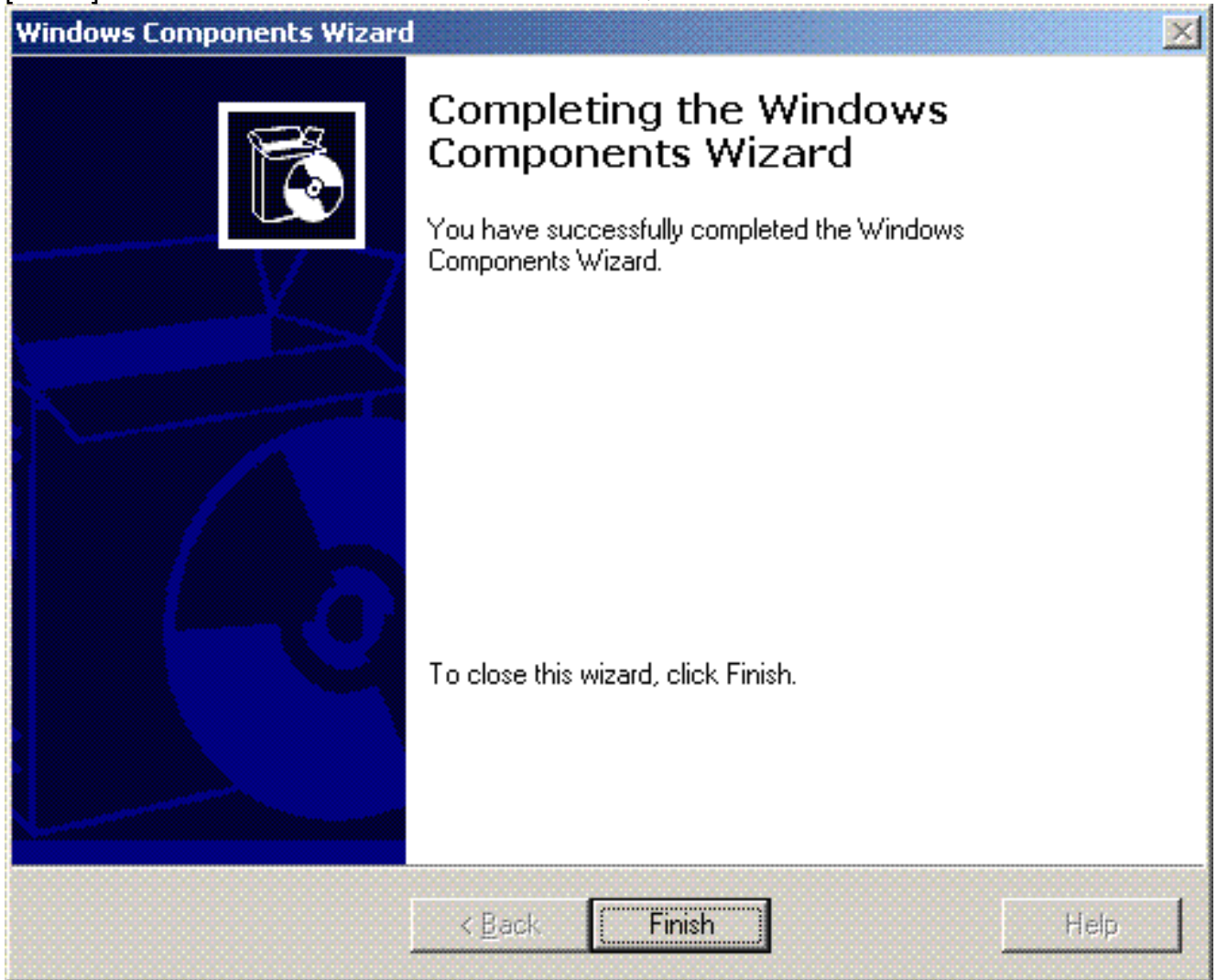
1. Control Panel で **Add or Remove Programs** をクリックします。
2. **Add/Remove Windows components** をクリックします。
3. **Networking Services** を選択し、**Details** をクリックします。
4. **Dynamic Host Configuration Protocol (DHCP)** を選択し、**OK** をクリックします。



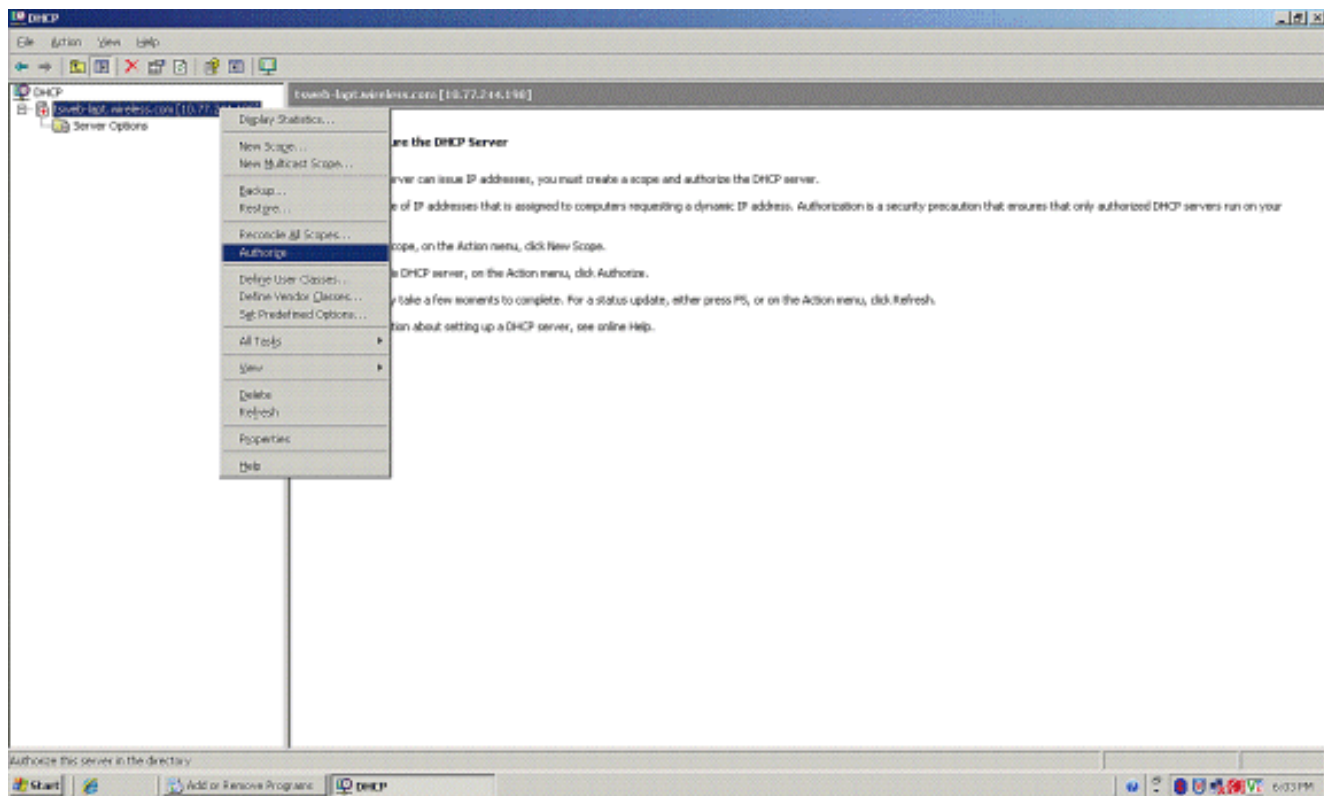
5. **Next** をクリックして DHCP サービスをインストールします。



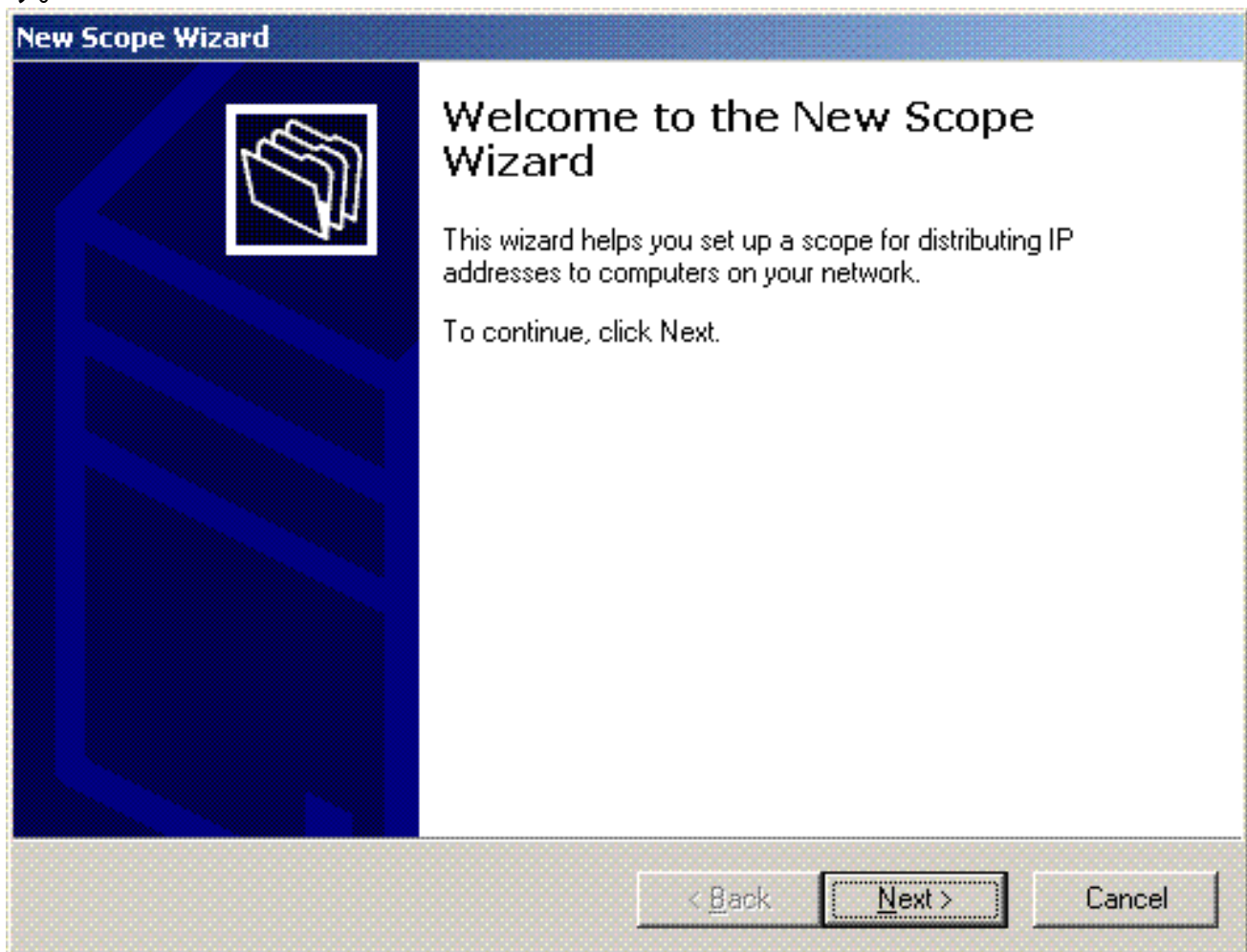
6. [Finish] をクリックしてインストールを完了します。



7. DHCP サービスを設定するため、**Start > Programs > Administrative tools** の順にクリックし、**DHCP** スナップインをクリックします。
8. DHCP サーバ (この例では **tsweb-lapt.wireless.com**) を選択します。
9. **Action** をクリックし、**Authorize** をクリックして DHCP サービスを認可します。



10. コンソール ツリーで **tsweb-lapt.wireless.com** を右クリックし、**New Scope** をクリックし、ワイヤレス クライアントの IP アドレスの範囲を定義します。
11. New Scope Wizard の Welcome to the New Scope Wizard ページで、**Next** をクリックします。



12. Scope Name ページで、DHCP のスコープ名を入力します。この例では、スコープ名に **DHCP-Clients** を使用します。[next] をクリックします。

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

13. IP Address Range ページで、範囲の最初と最後の IP アドレスを入力し、**Next** をクリックします。

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Enter the range of addresses that the scope distributes.

Start IP address: 10 . 77 . 244 . 218

End IP address: 10 . 77 . 244 . 219

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 8

Subnet mask: 255 . 0 . 0 . 0

< Back

Next >

Cancel

14. Add Exclusions ページで、DHCP スコープから留保または除外する IP アドレスを指定します。[next] をクリックします。

New Scope Wizard

Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Remove

< Back

Next >

Cancel

15. Lease Duration ページでリース期間を指定し、**Next** をクリックします。

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:

Hours:

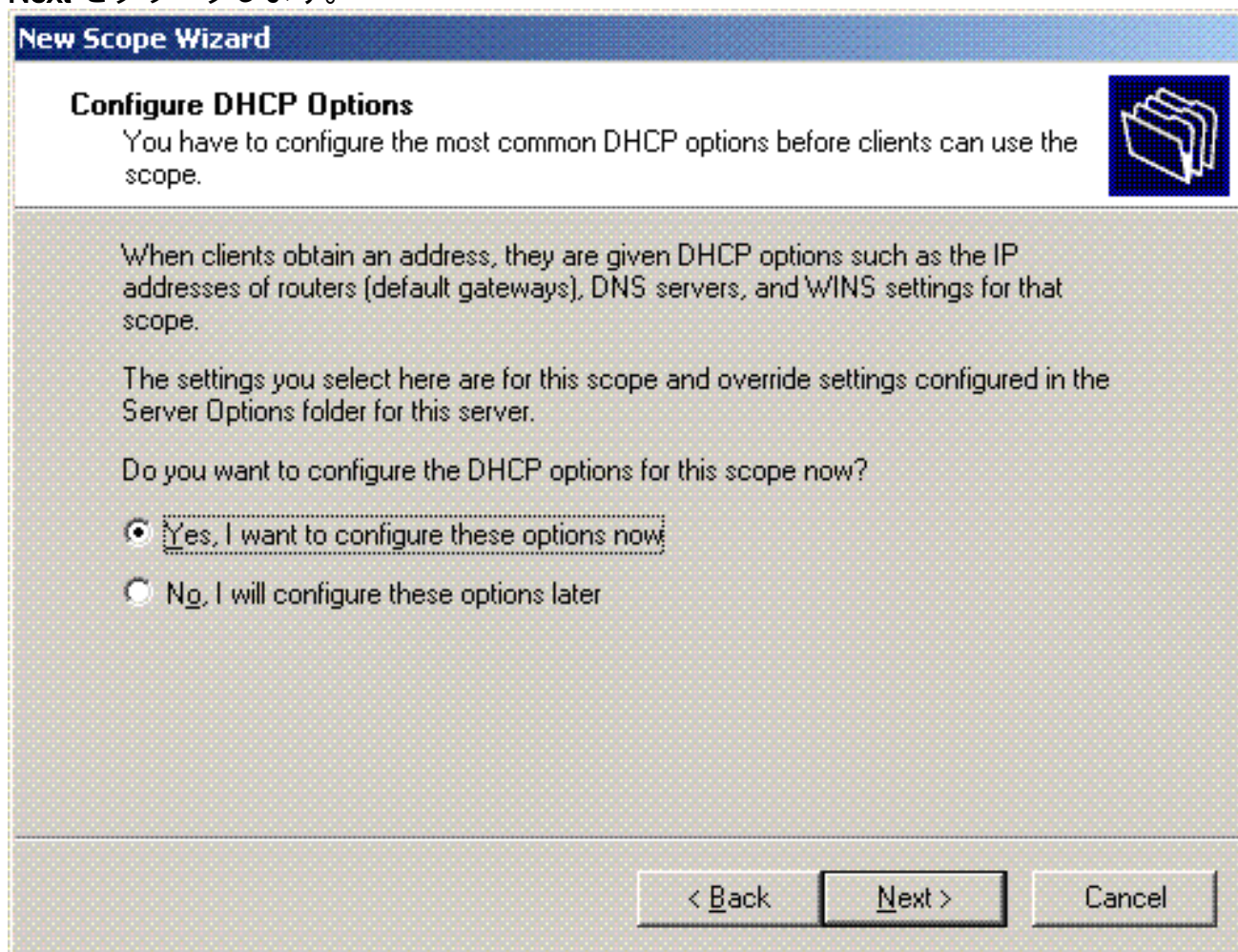
Minutes:

< Back

Next >

Cancel

16. Configure DHCP Options ページで **Yes, I want to configure DHCP Option now** を選択し、**Next** をクリックします。



17. デフォルトのゲートウェイ ルータがある場合は、Router (Default Gateway) ページでそのゲートウェイ ルータの IP アドレスを指定し、**Next** をクリックします。

New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

Add

Remove

Up

Down

< Back

Next >

Cancel

18. Domain Name and DNS Servers ページで、先ほど設定したドメインの名前を入力します。この例では、**Wireless.com** を使用します。サーバの IP アドレスを入力します。[Add] をクリックします。

New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

Add

Resolve

Remove

Up

Down

< Back

Next >

Cancel

19. [next] をクリックします。

20. WINS Server ページで **Next** をクリックします。

21. Activate Scope ページで **Yes, I want to activate the scope now** を選択し、**Next** をクリックします。

New Scope Wizard

Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

- Yes, I want to activate this scope now
- No, I will activate this scope later

< Back

Next >

Cancel

22. New Scope Wizard を終了するため、**Finish** をクリックします。

New Scope Wizard



Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

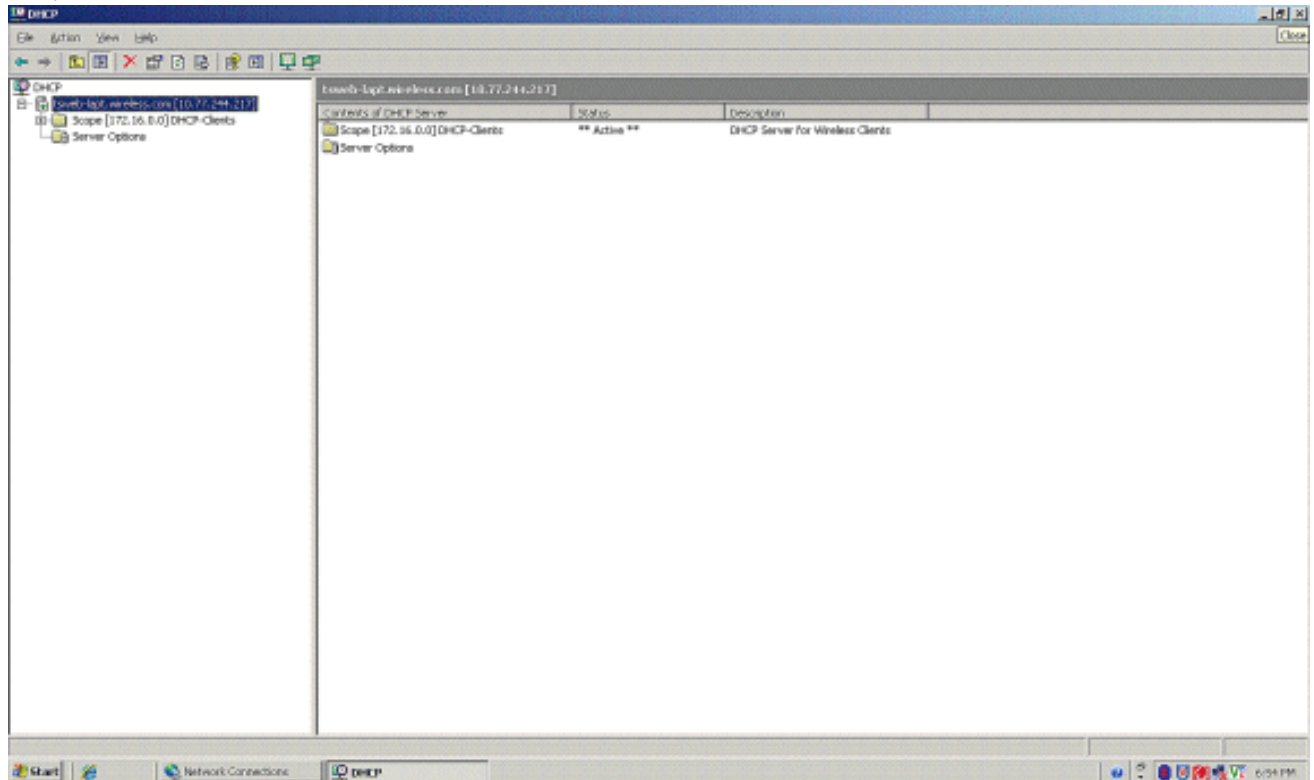
To close this wizard, click Finish.

< Back

Finish

Cancel

23. DHCP Snapin ウィンドウで、作成した DHCP スコープがアクティブであることを確認します。



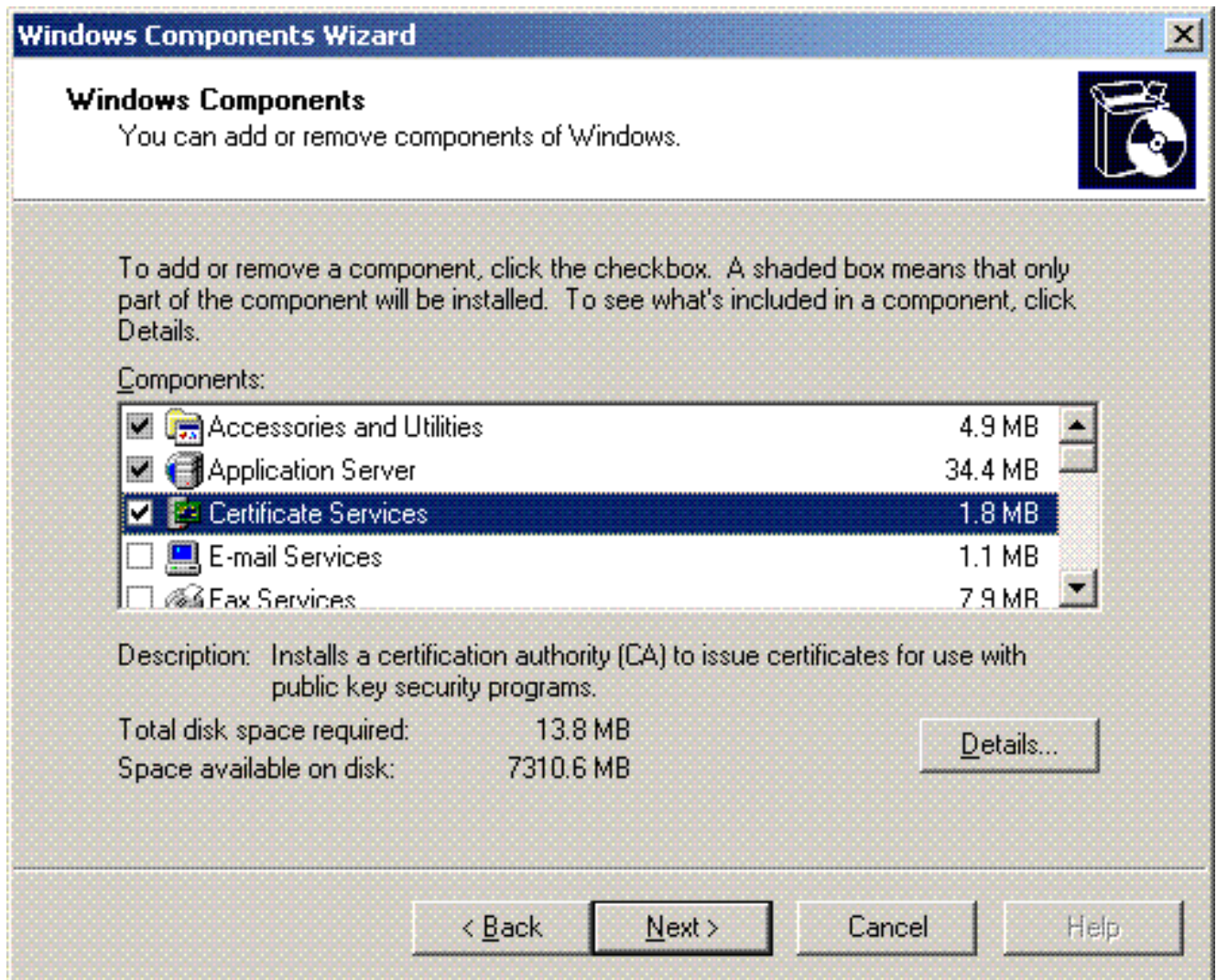
これで、サーバ上で DHCP/DNS がイネーブルになったので、サーバをエンタープライズの認証局 (CA) サーバとして設定します。

[Microsoft Windows 2003 Server の認証局 \(CA \) サーバとしてのインストールと設定](#)

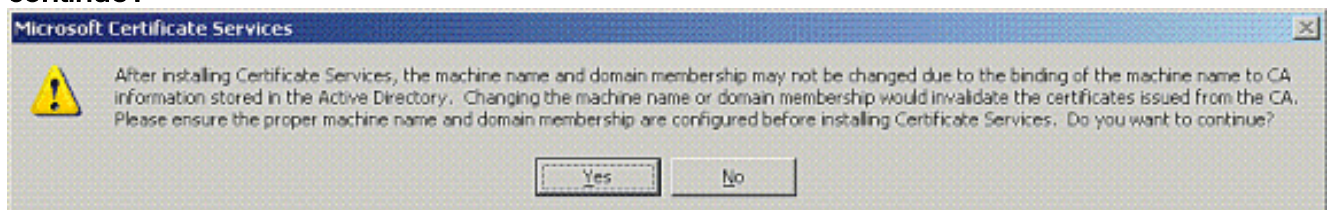
EAP-MS-CHAPv2を使用するPEAPは、サーバ上にある証明書に基づいてRADIUSサーバを検証します。また、クライアント コンピュータの信頼するパブリックな Certification Authority (CA) がサーバ証明書を発行する必要があります (つまり、パブリックな CA 証明書がクライアント コンピュータの証明書ストアの Trusted Root Certification Authority フォルダにすでに存在する必要があります)。この例では、Internet Authentication Service (IAS) へ証明書を発行する認証局 (CA) として、Microsoft Windows 2003 Server を設定します。

サーバ上に証明書サービスをインストールして設定するには、次の手順を実行します。

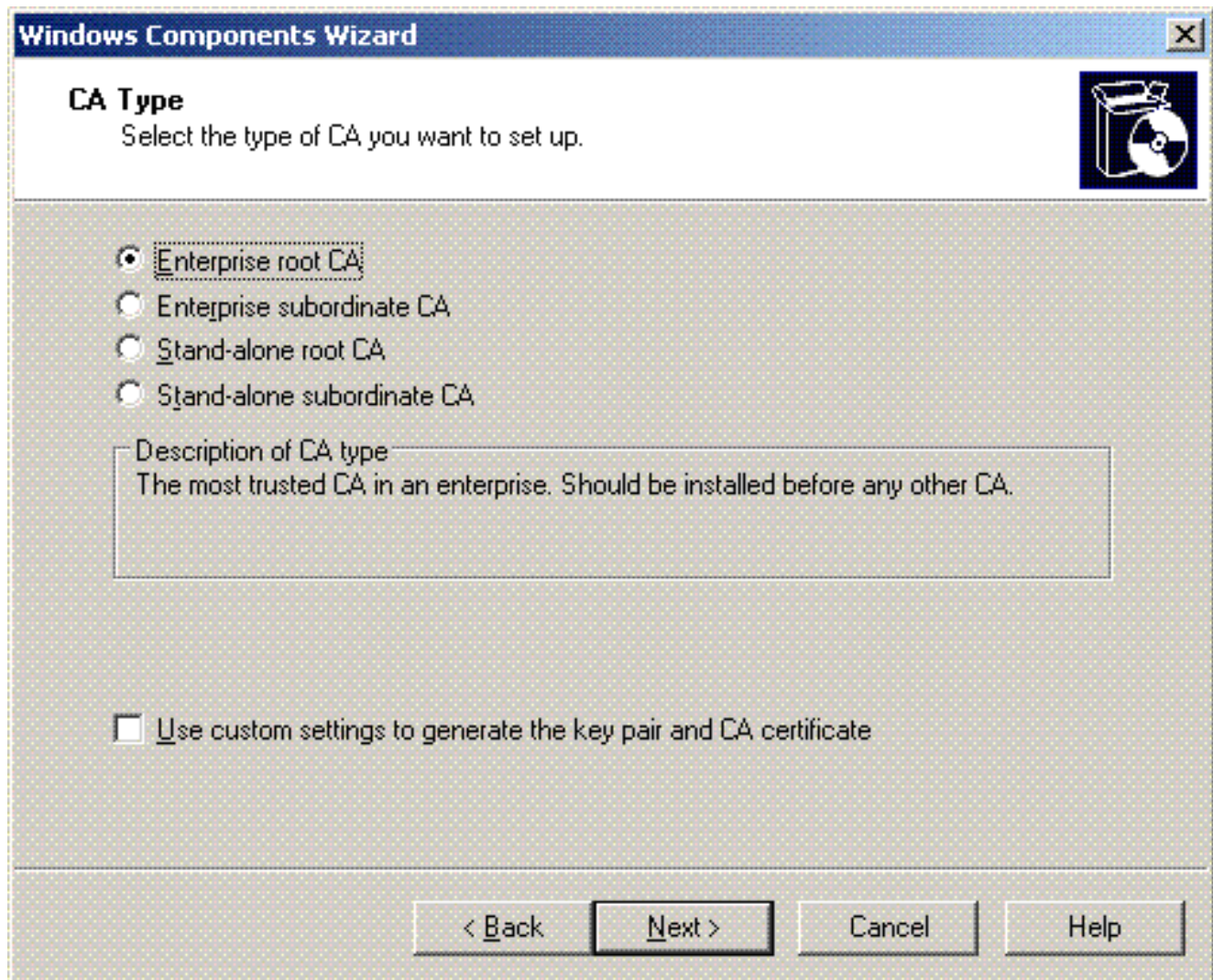
1. Control Panel で **Add or Remove programs** をクリックします。
2. Add/Remove Windows components をクリックします。
3. **Certificate Services** をクリックします。



4. 「After Installing Certificate Services, the computer cannot be renamed and the computer cannot join or be removed from a domain. Do you want to continue?




5. Certificate Authority Type で **Enterprise root CA** を選択し、**Next** をクリックします。



6. CA を識別する名前を入力します。この例では **Wireless-CA** を使用しています。[next] をクリックします。

Windows Components Wizard X

CA Identifying Information 
Enter information to identify this CA.

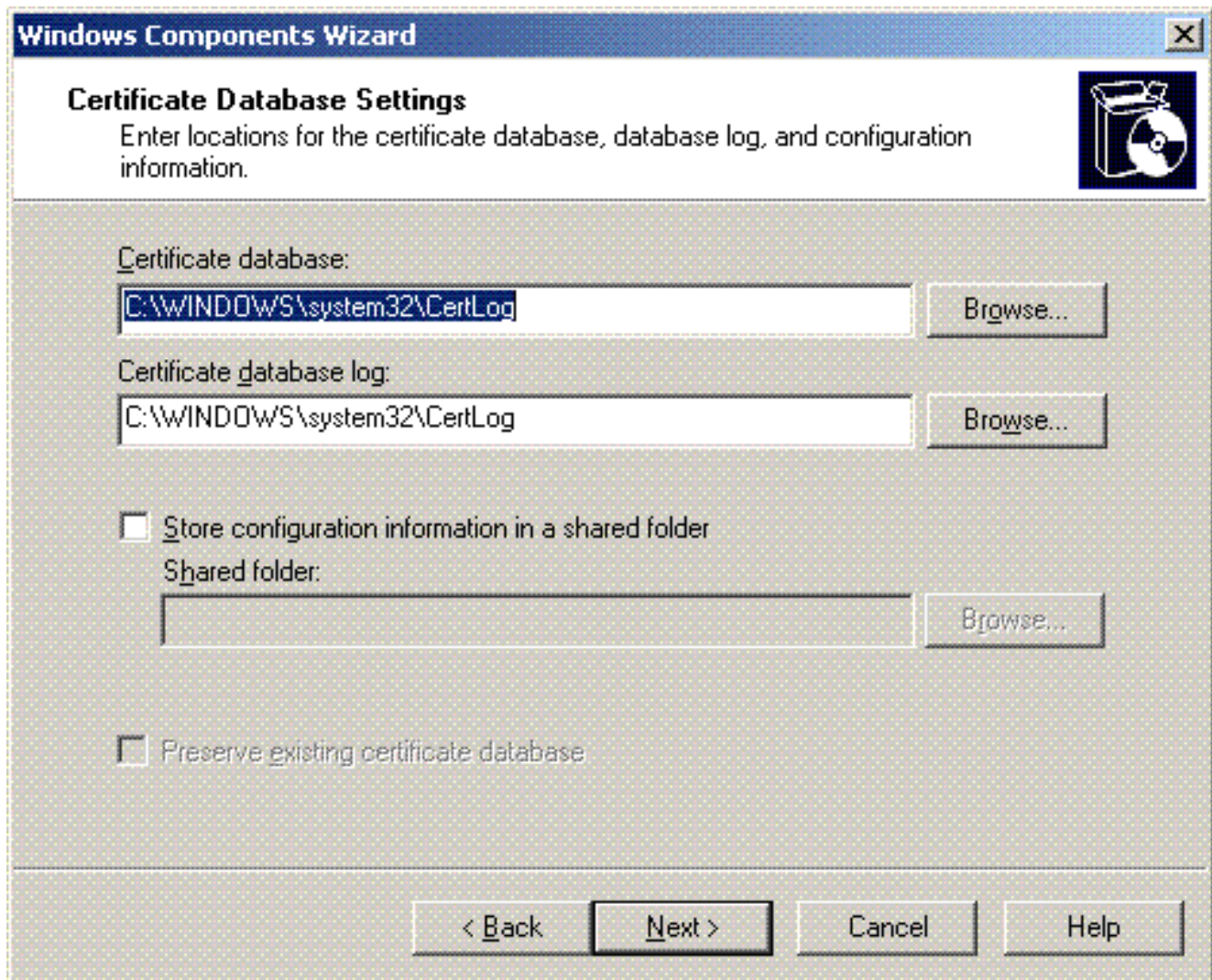
Common name for this CA:

Distinguished name suffix:

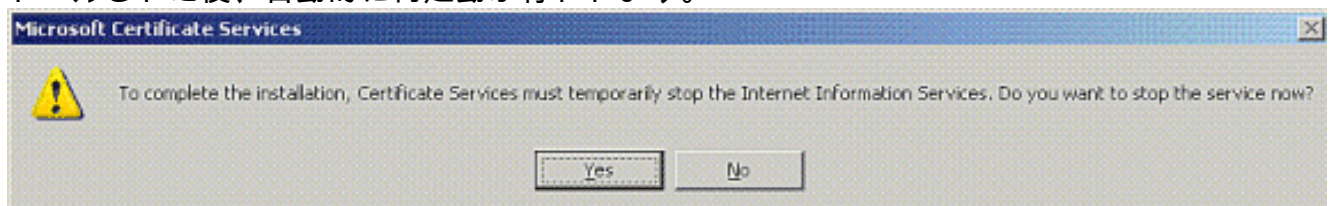
Preview of distinguished name:

Validity period:
Expiration date: 12/12/2012 7:01 PM

7. 証明書データベース ストレージとして CertLog ディレクトリが作成されます。[next] をクリックします。



8. IIS が有効になっている場合は、これを停止してから次の手順に進む必要があります。IIS を停止させる必要があるという警告メッセージに対して OK をクリックします。CA がインストールされた後、自動的に再起動が行われます。



9. Finish をクリックして、認証局 (CA) サービスのインストールを完了します。

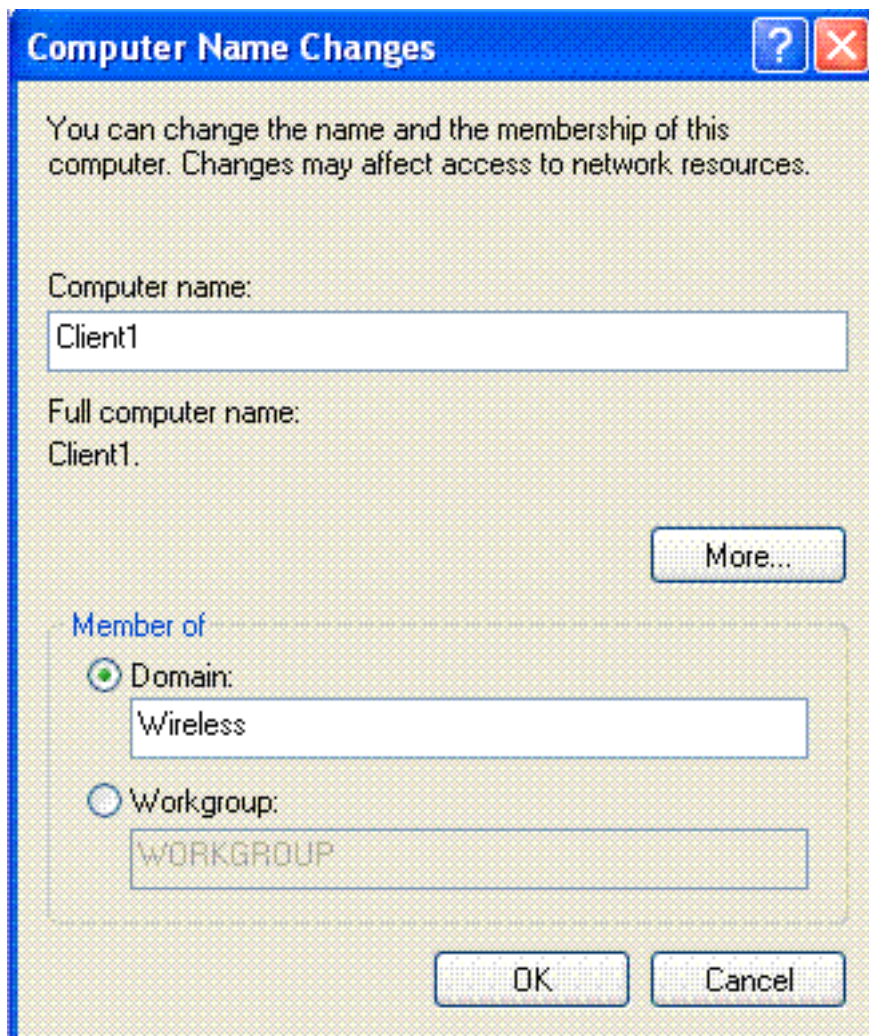


次の手順では、Microsoft Windows 2003 Server に Internet Authentication Service をインストールして設定します。

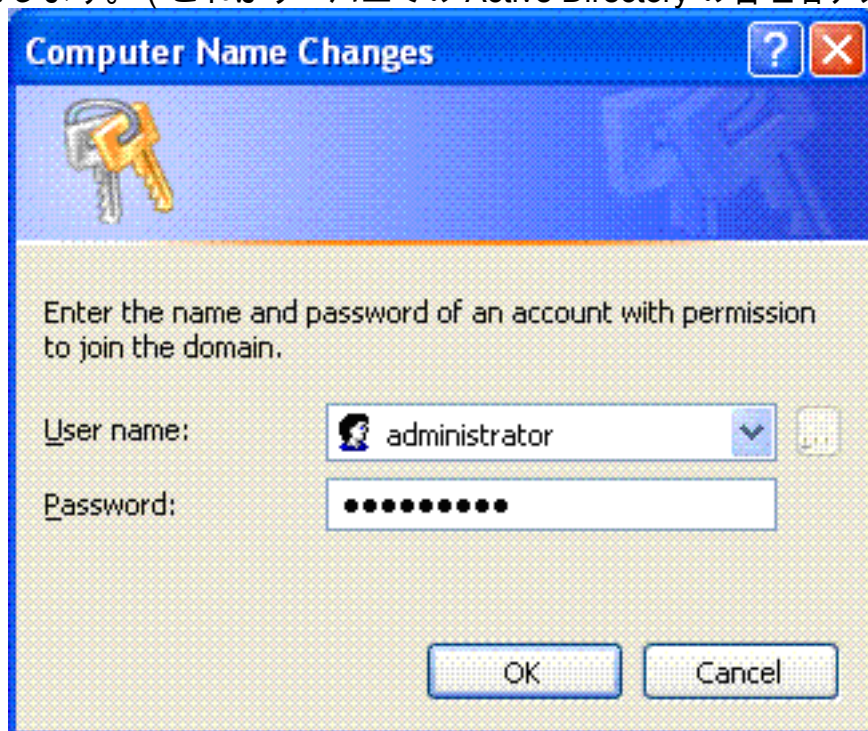
ドメインへのクライアントの接続

次の手順では、クライアントを有線ネットワークに接続させ、新しいドメインからドメイン固有の情報をダウンロードします。つまり、クライアントをドメインに接続させます。このためには、次の手順を実行します。

1. ストレート型のイーサネット ケーブルでクライアントを有線ネットワークに接続します。
2. クライアントを起動し、そのクライアントのユーザ名/パスワードでログインします。
3. **Start**、**Run** の順にクリックし、**cmd** と入力して、**OK** をクリックします。
4. コマンド プロンプトで **ipconfig** と入力し、**Enter** をクリックして、DHCP が正常に動作しクライアントが DHCP サーバから IP アドレスを受け取ったことを確認します。
5. クライアントをドメインに参加させるため、**My Computer** を右クリックし、**Properties** を選択します。
6. **[Computer Name]** タブをクリックします。
7. **[Change]** をクリックします。
8. **Domain** をクリックし、**wireless.com** と入力し、**OK** をクリックします。

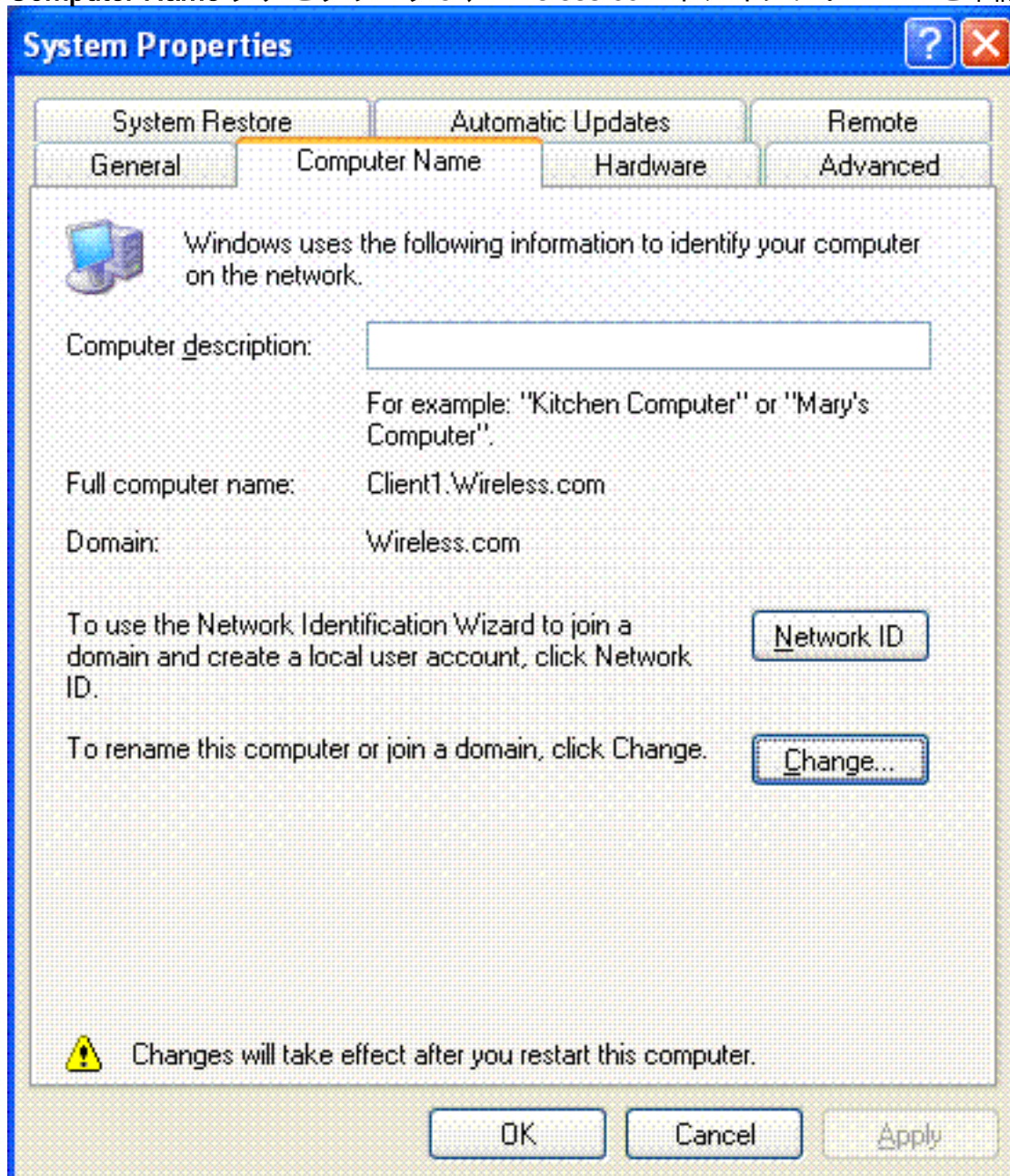


9. Username に **Administrator** と入力し、クライアントが参加するドメインのパスワードを入力します。（これはサーバ上での Active Directory の管理者アカウントです。）

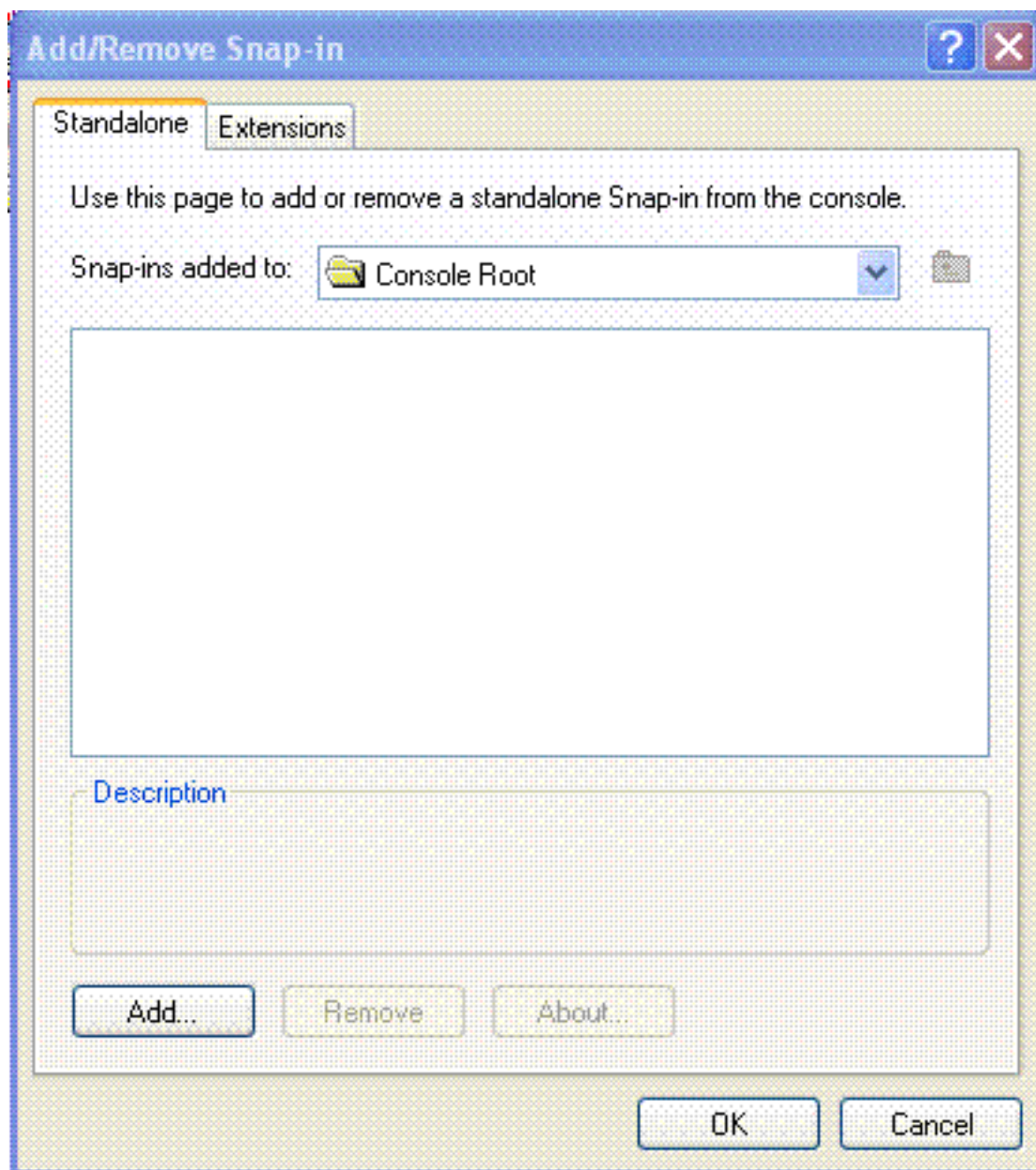




10. [OK] をクリックします。
11. [Yes] をクリックしてコンピュータを再起動させます。
12. コンピュータが再起動したら、次の情報でログインします。ユーザ名= Administrator、パスワード= <domain password>、ドメイン= Wireless。
13. My Computer を右クリックし、Properties をクリックします。
14. Computer Name タブをクリックし、Wireless.com ドメインにいることを確認します。

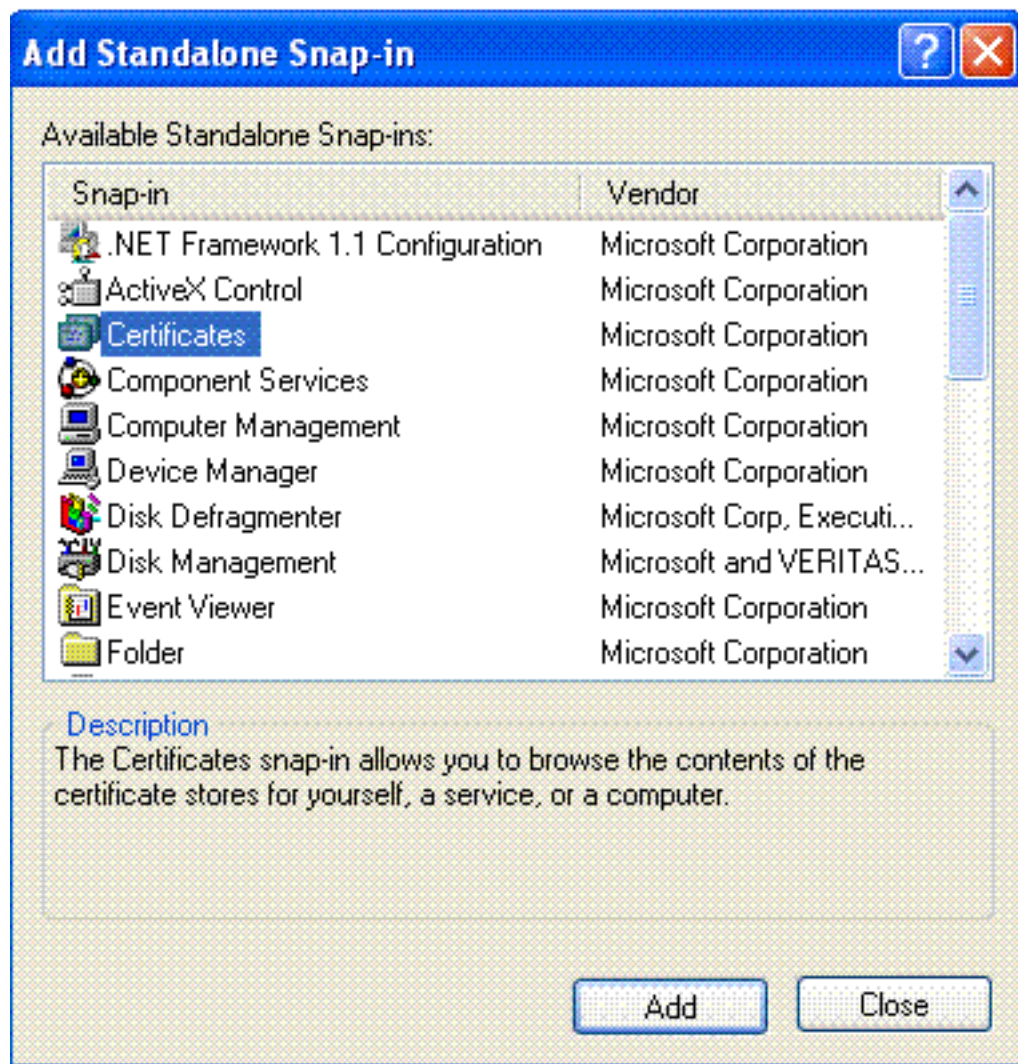


15. 次の手順では、クライアントがサーバから CA 証明書 (信頼) を受信したことを確認します。
16. Start、Run の順にクリックし、mmc と入力して、OK をクリックします。
17. [File] をクリックし、[Add/Remove] スナップインをクリックします。

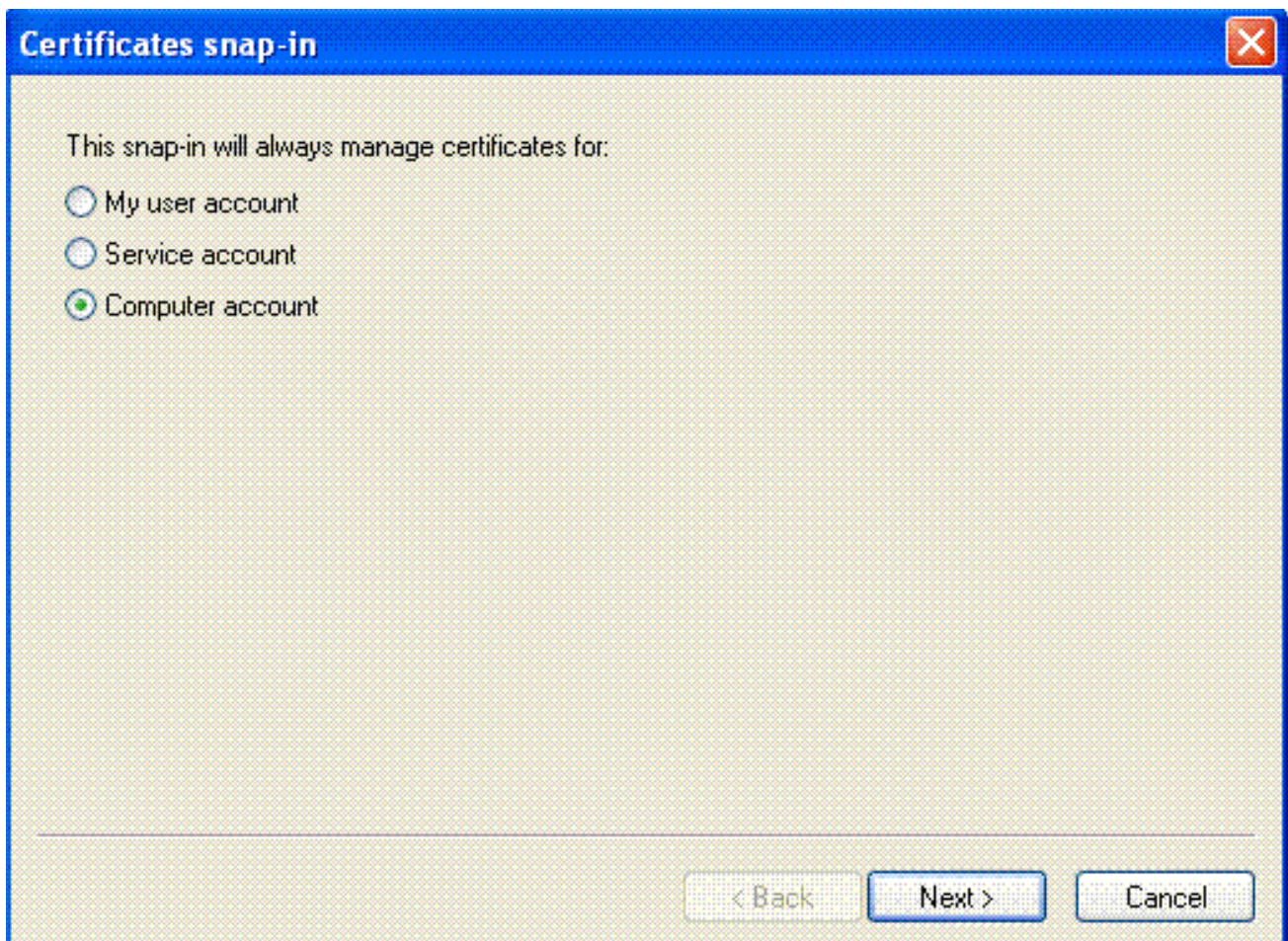


18. [Add] をクリックします。

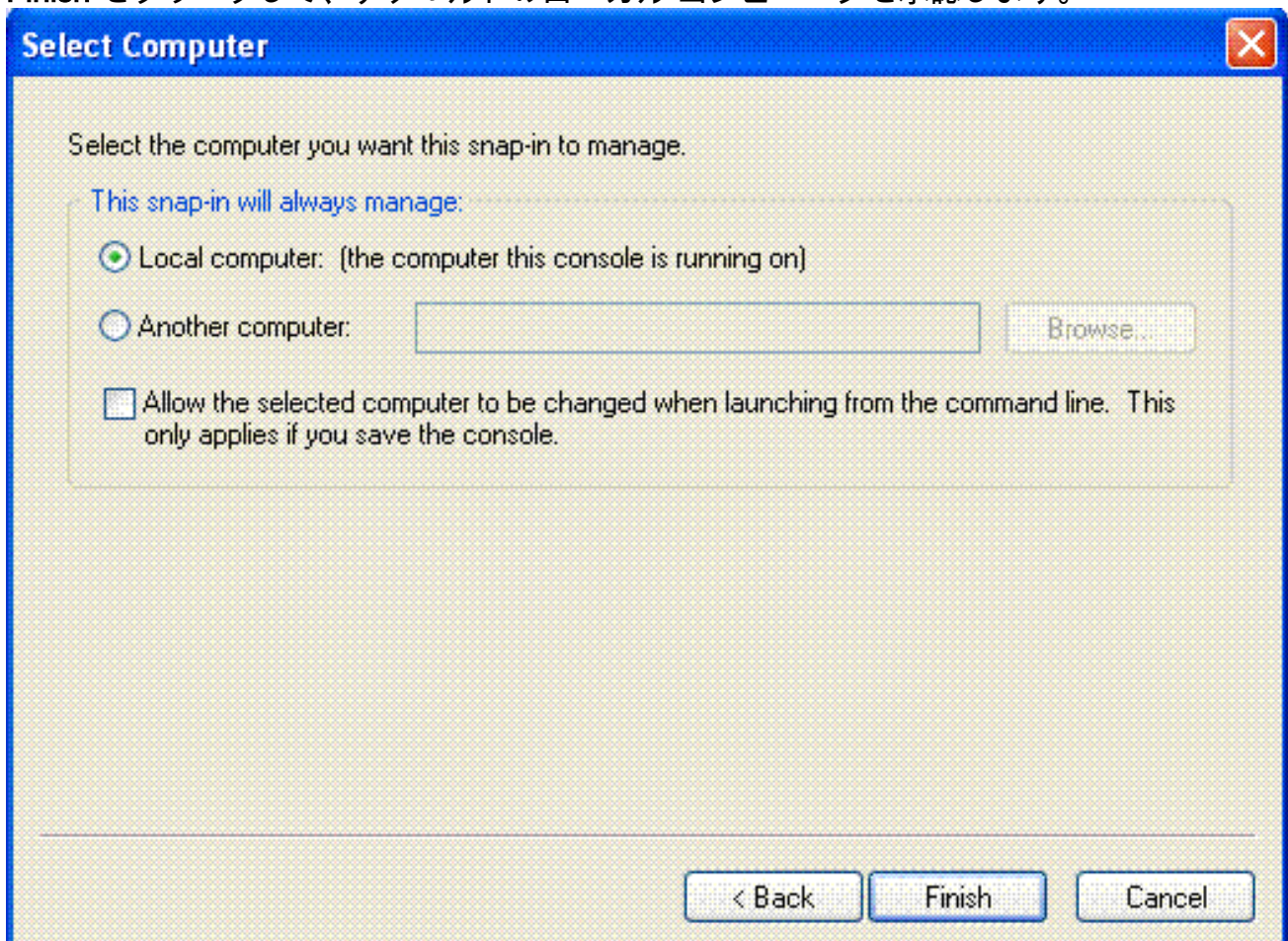
19. **Certificate** を選択し、**Add** をクリックしします。



20. **Computer account** を選択し、**Next** をクリックします。



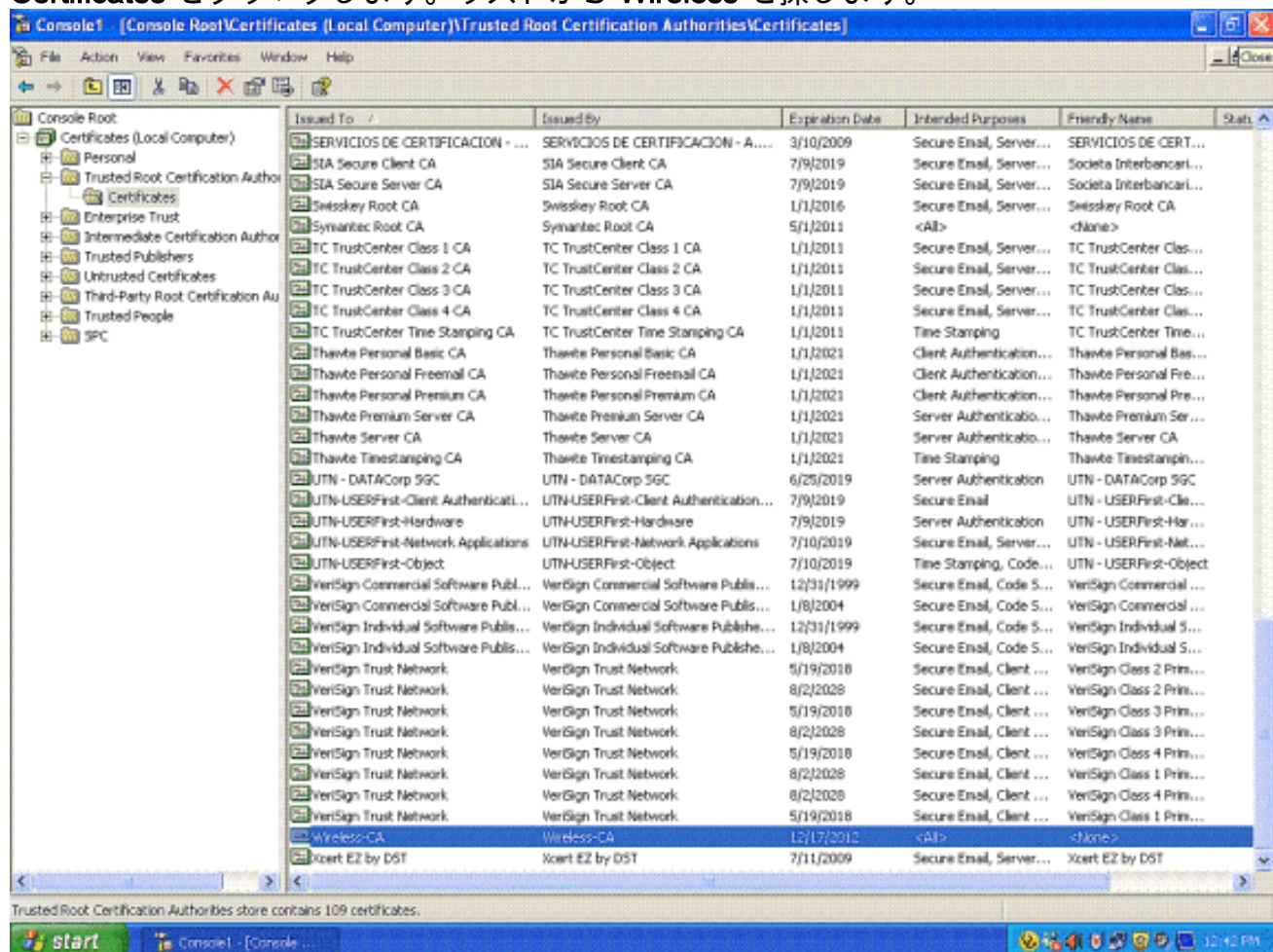
21. **Finish** をクリックして、デフォルトのローカル コンピュータを承認します。



22. **Close** をクリックし、**OK** をクリックします。

23. **Certificates (Local Computer)**、**Trusted Root Certification Authorities** の順に展開し、

Certificates をクリックします。リストから Wireless を探します。



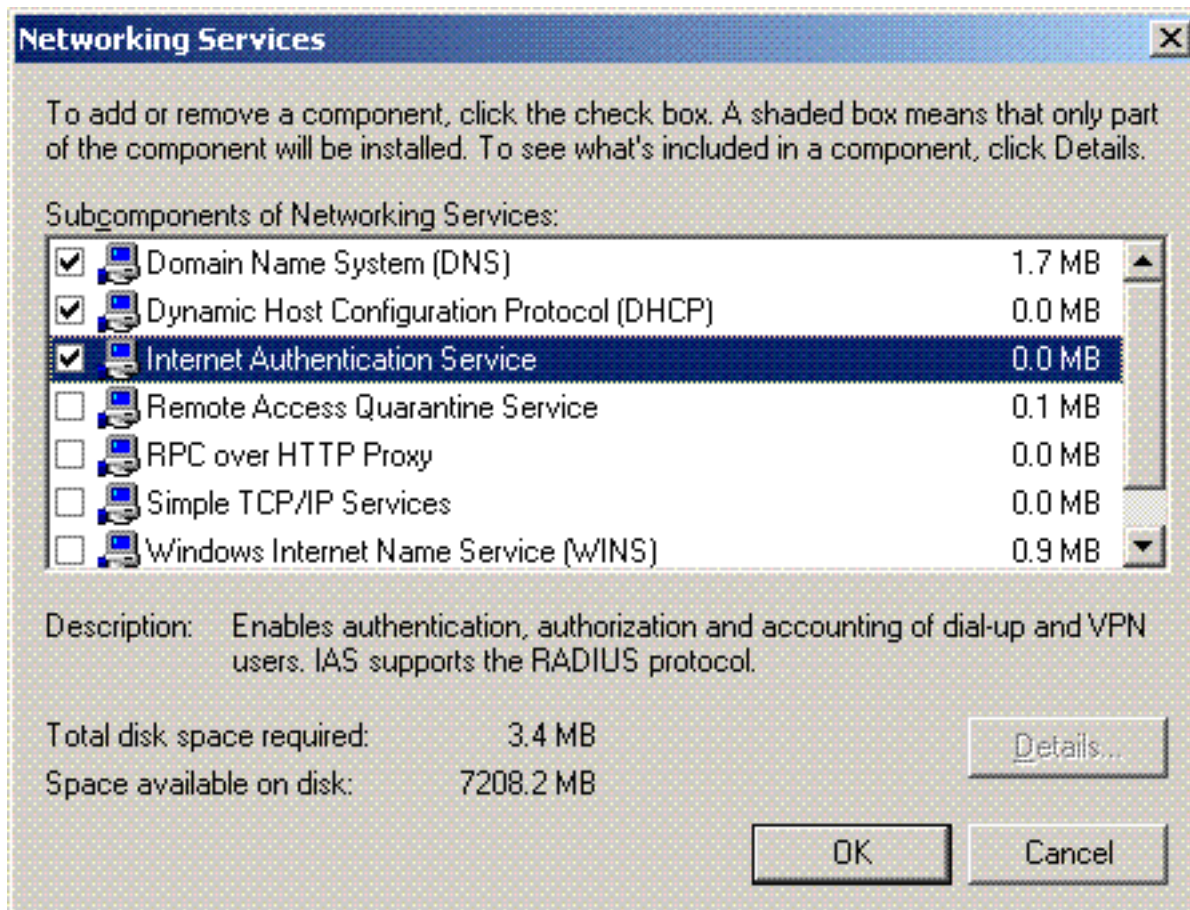
24. 別のクライアントをさらにドメインに追加するには、この手順を繰り返します。

Microsoft Windows 2003 Server での Internet Authentication Service のインストールと証明書の要求

この設定では、PEAP 認証を使用してワイヤレスクライアントを認証するために、Internet Authentication Service (IAS) を RADIUS サーバとして使用します。

次の手順を実行して、サーバ上に IAS をインストールして設定します。

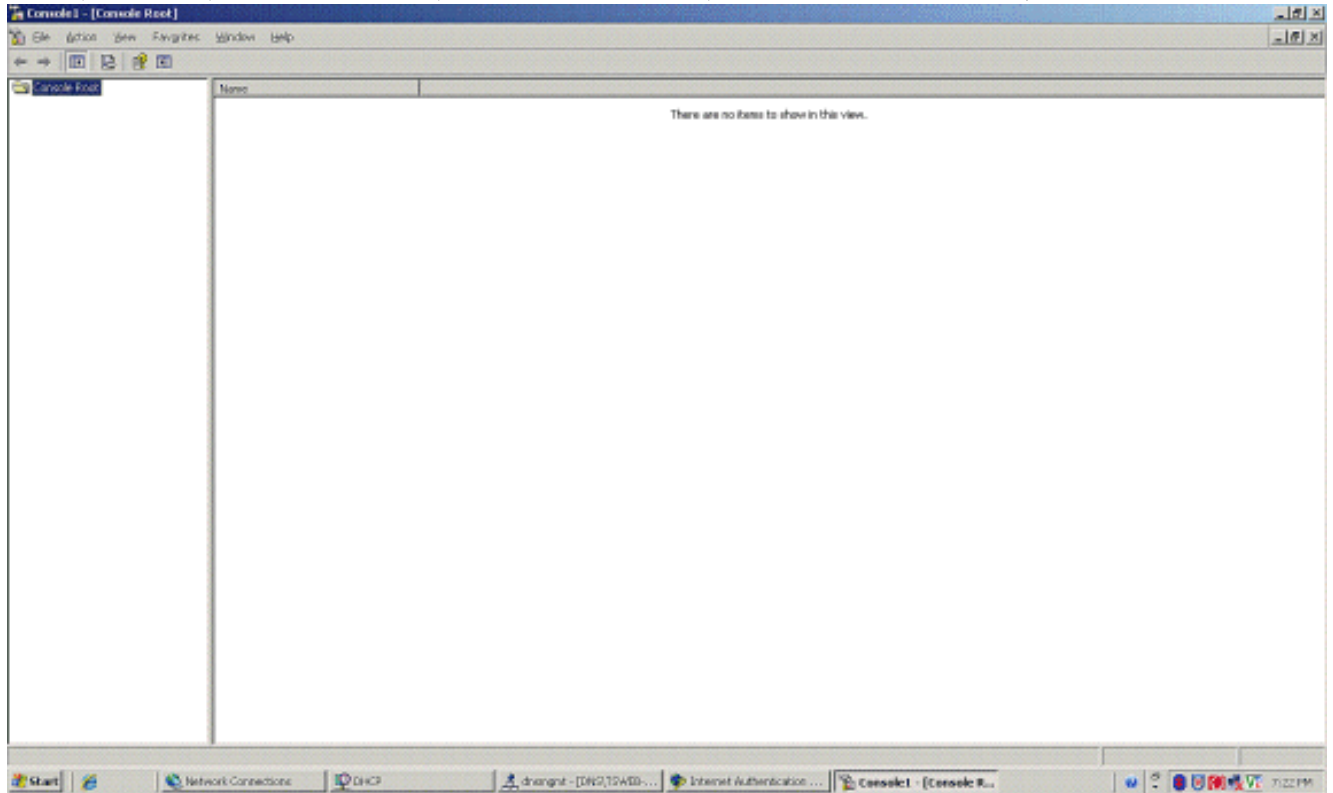
1. Control Panel で **Add or Remove Programs** をクリックします。
2. **Add/Remove Windows components** をクリックします。
3. **Networking Services** を選択し、**Details** をクリックします。
4. **Internet Authentication Service** を選択し、**OK** をクリックし、**Next** をクリックします。



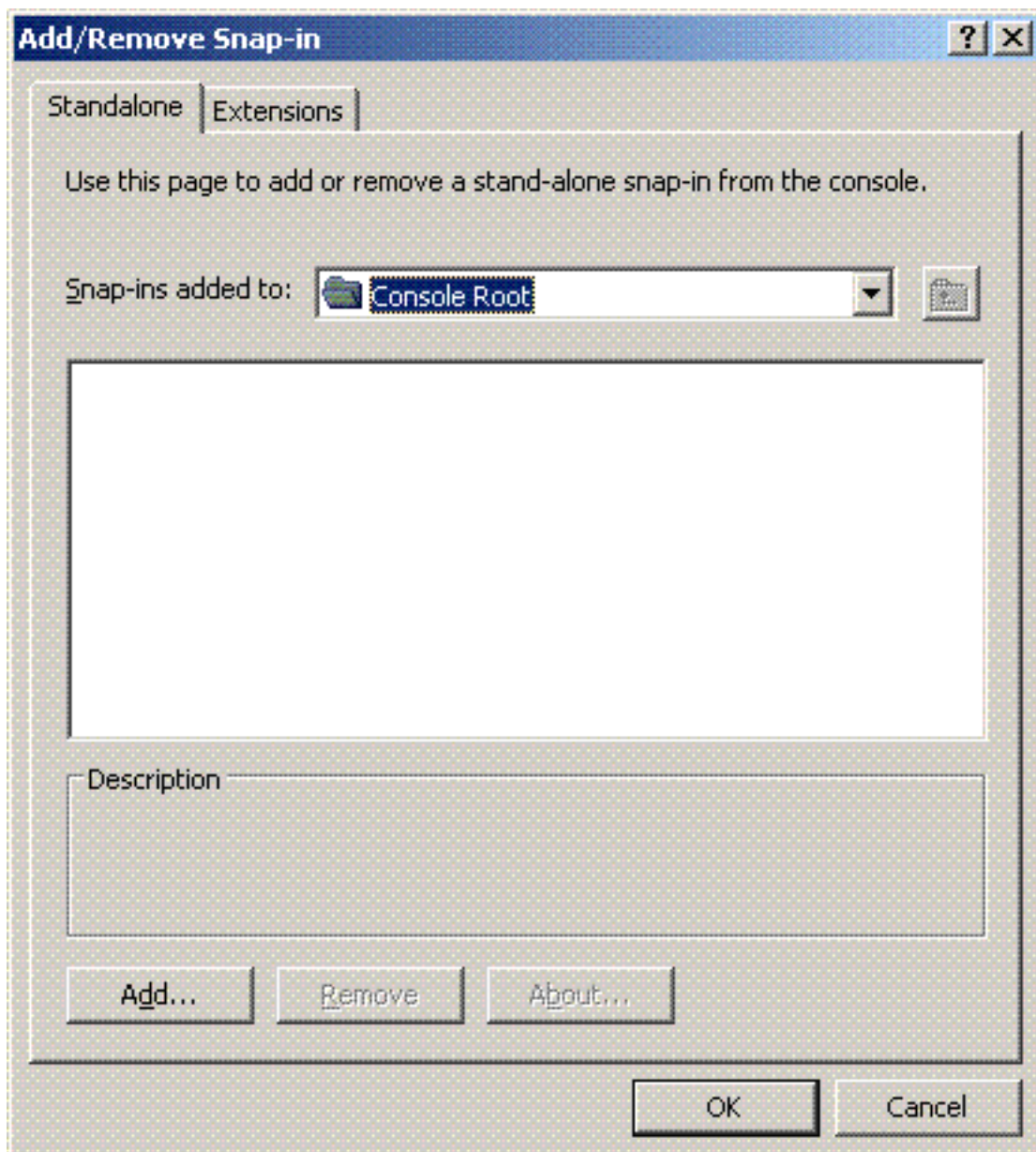
5. **Finish** をクリックして、IAS のインストールを完了します。



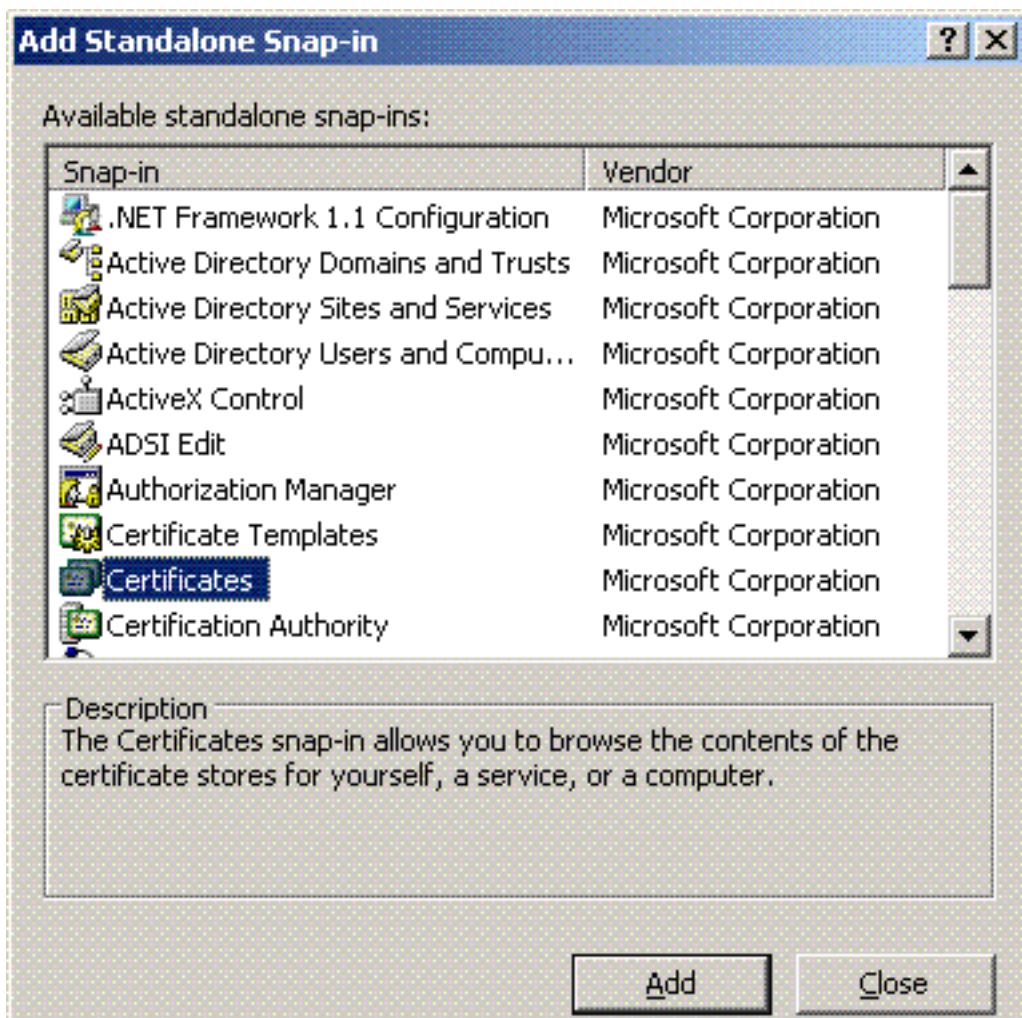
6. 次の手順では、Internet Authentication Service (IAS) に対応するコンピュータの証明書をインストールします。
7. **Start**、**Run** の順にクリックし、**mmc** と入力して、**OK** をクリックします。



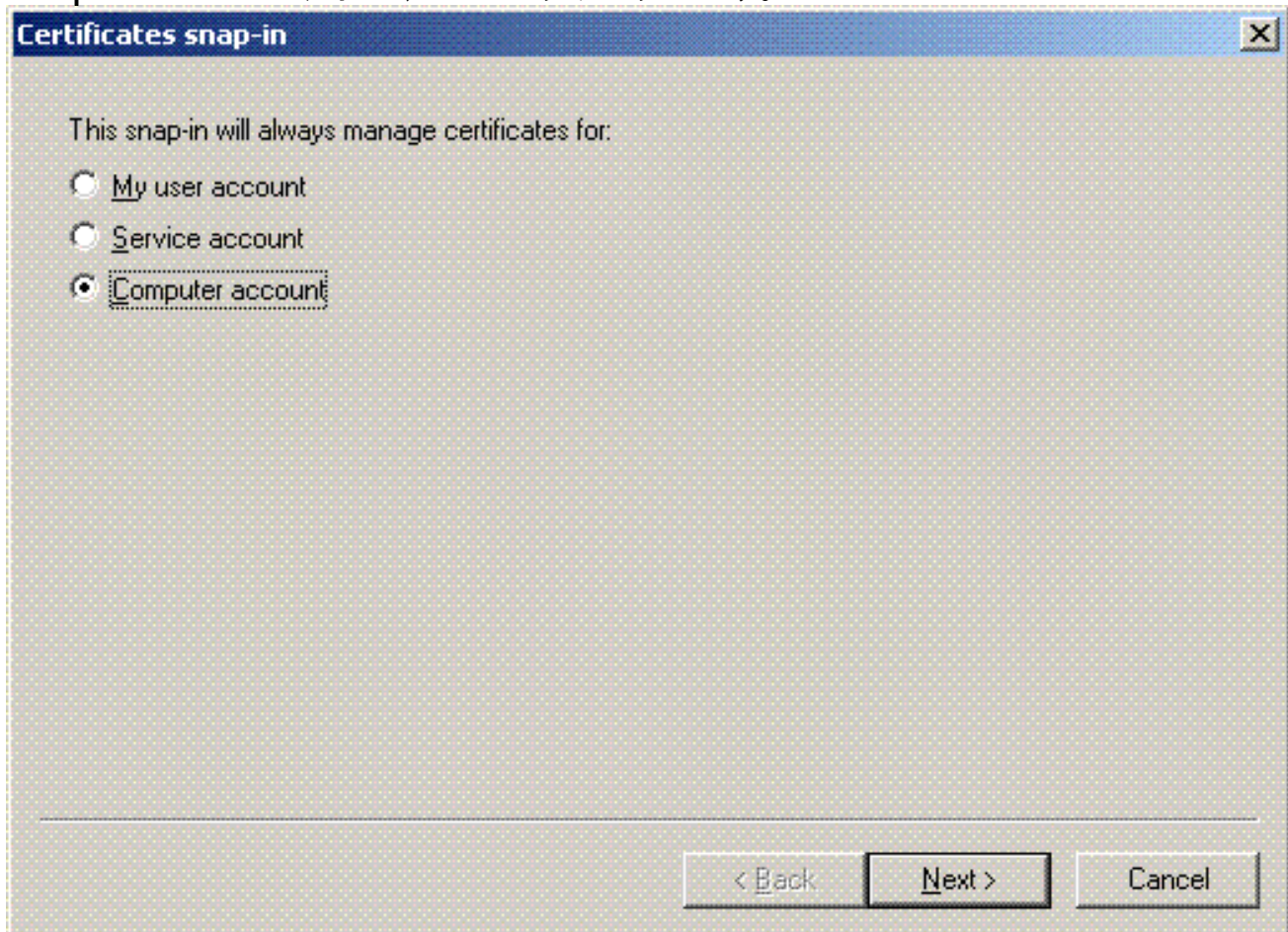
8. ファイルメニューで **Console** をクリックし、**Add/Remove** スナップインを選択します。
9. **Add** をクリックし、スナップインを追加します。



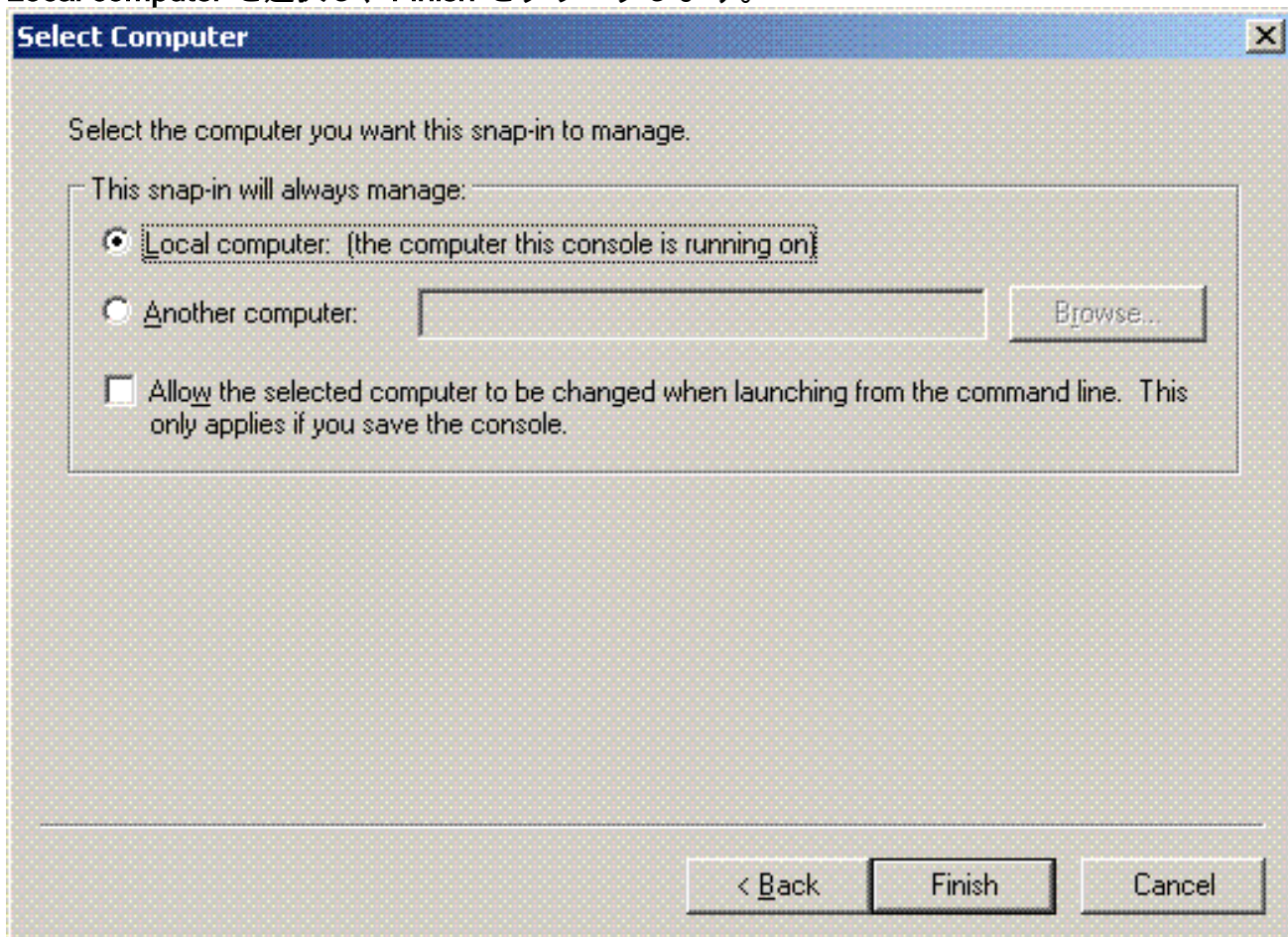
10. スナップインのリストから **Certificates** を選択し、**Add** をクリックしします。



11. **Computer account** を選択し、**Next** をクリックします。

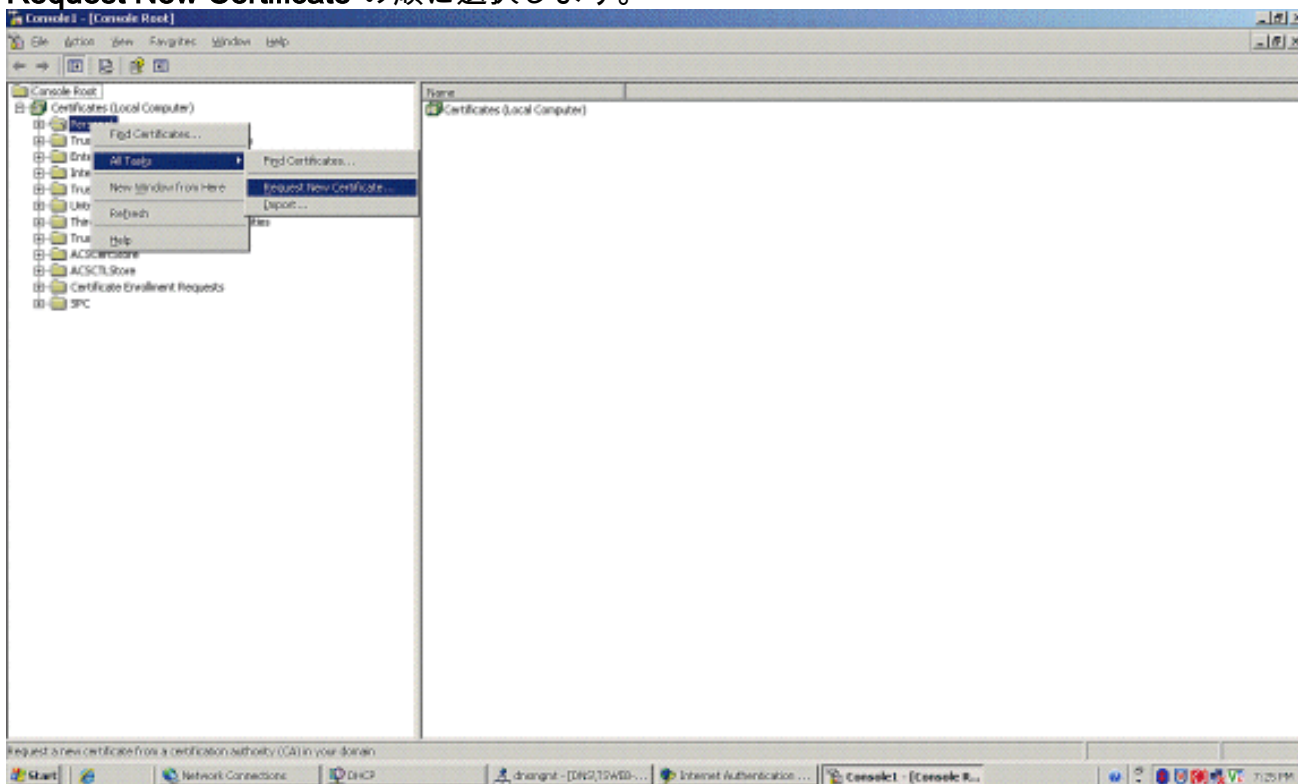


12. Local computer を選択し、Finish をクリックします。



13. Close をクリックし、OK をクリックします。

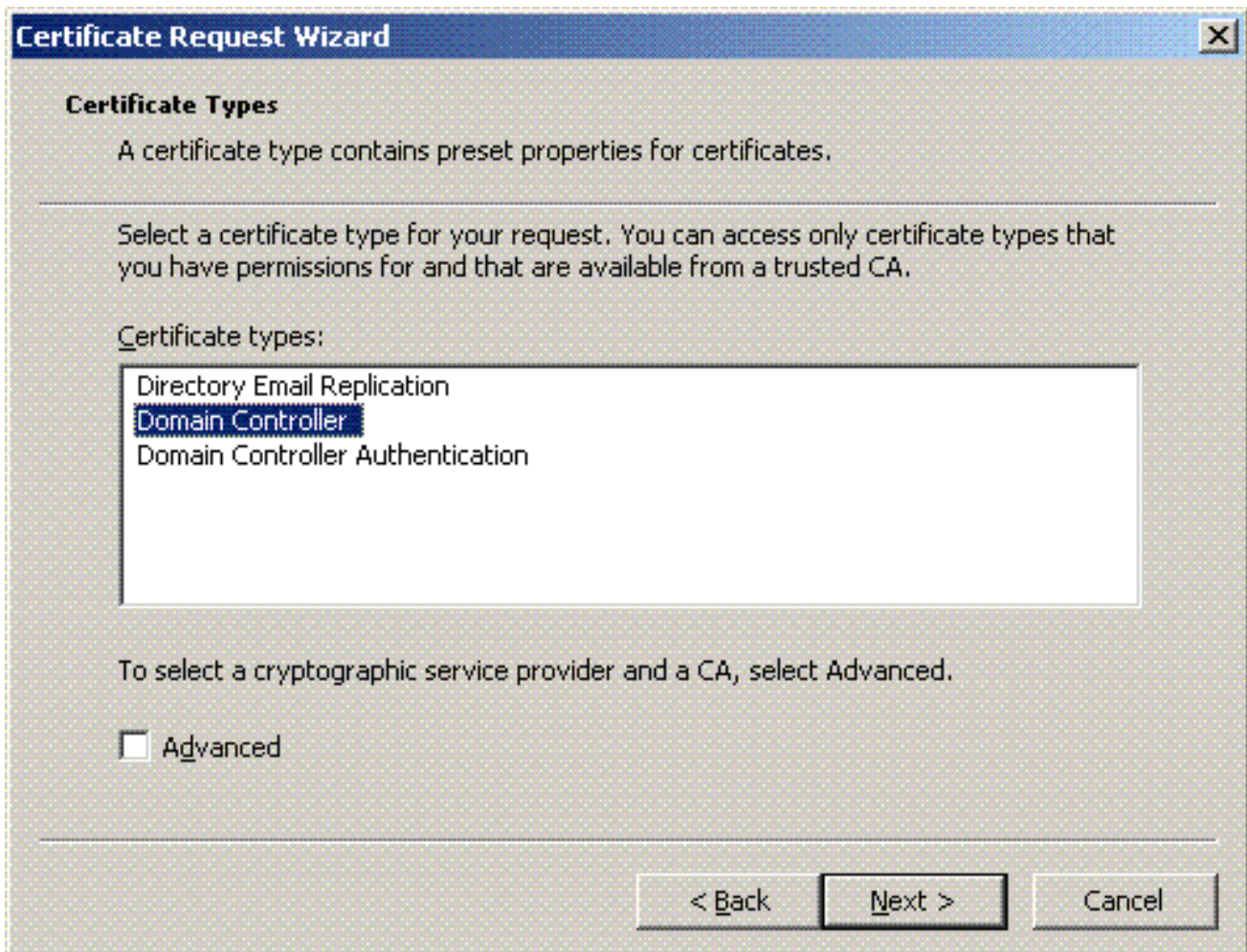
14. Certificates (Local Computer) を展開し、Personal folder を右クリックし、All tasks、Request New Certificate の順に選択します。



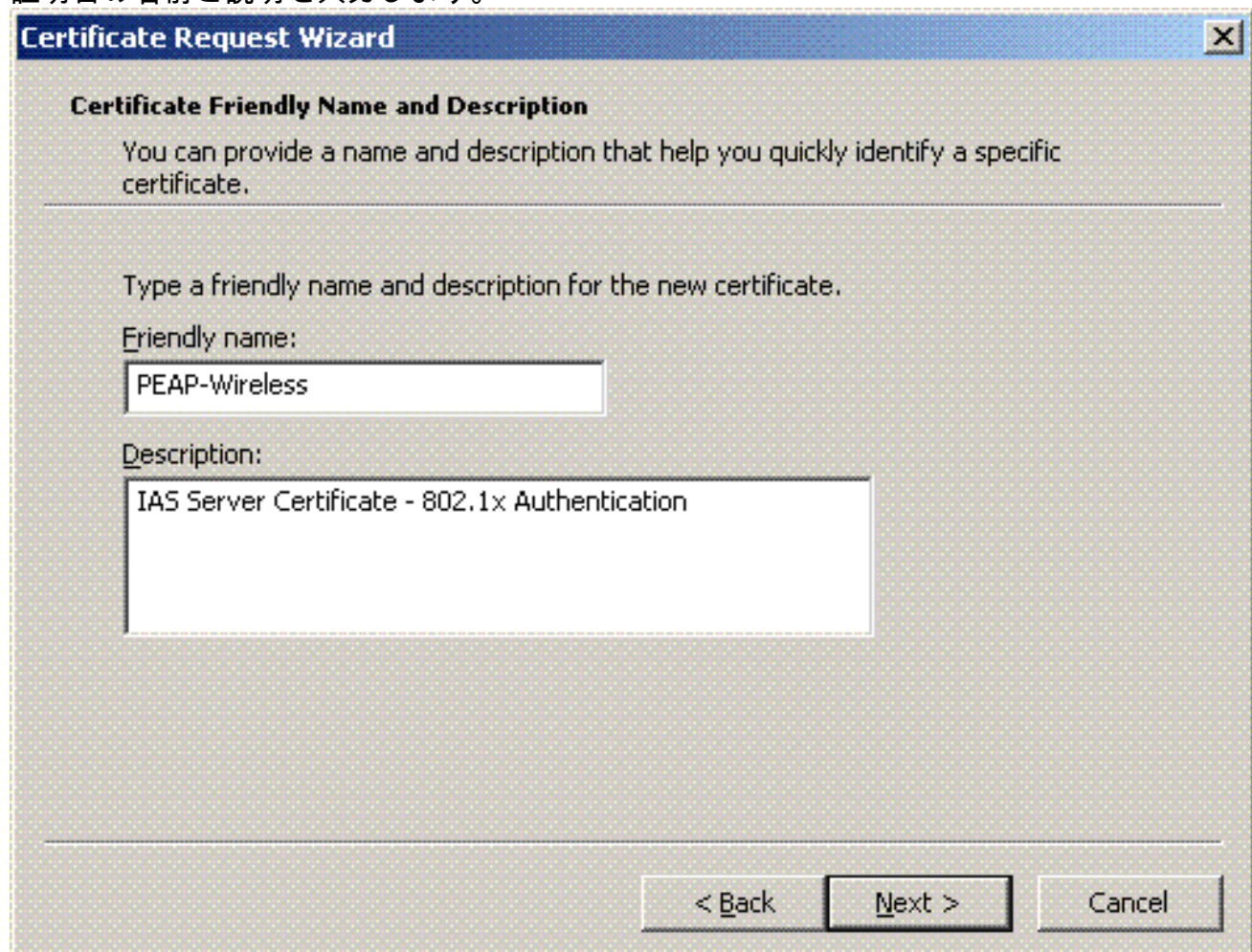
15. Welcome to the Certificate Request Wizard で Next をクリックします。



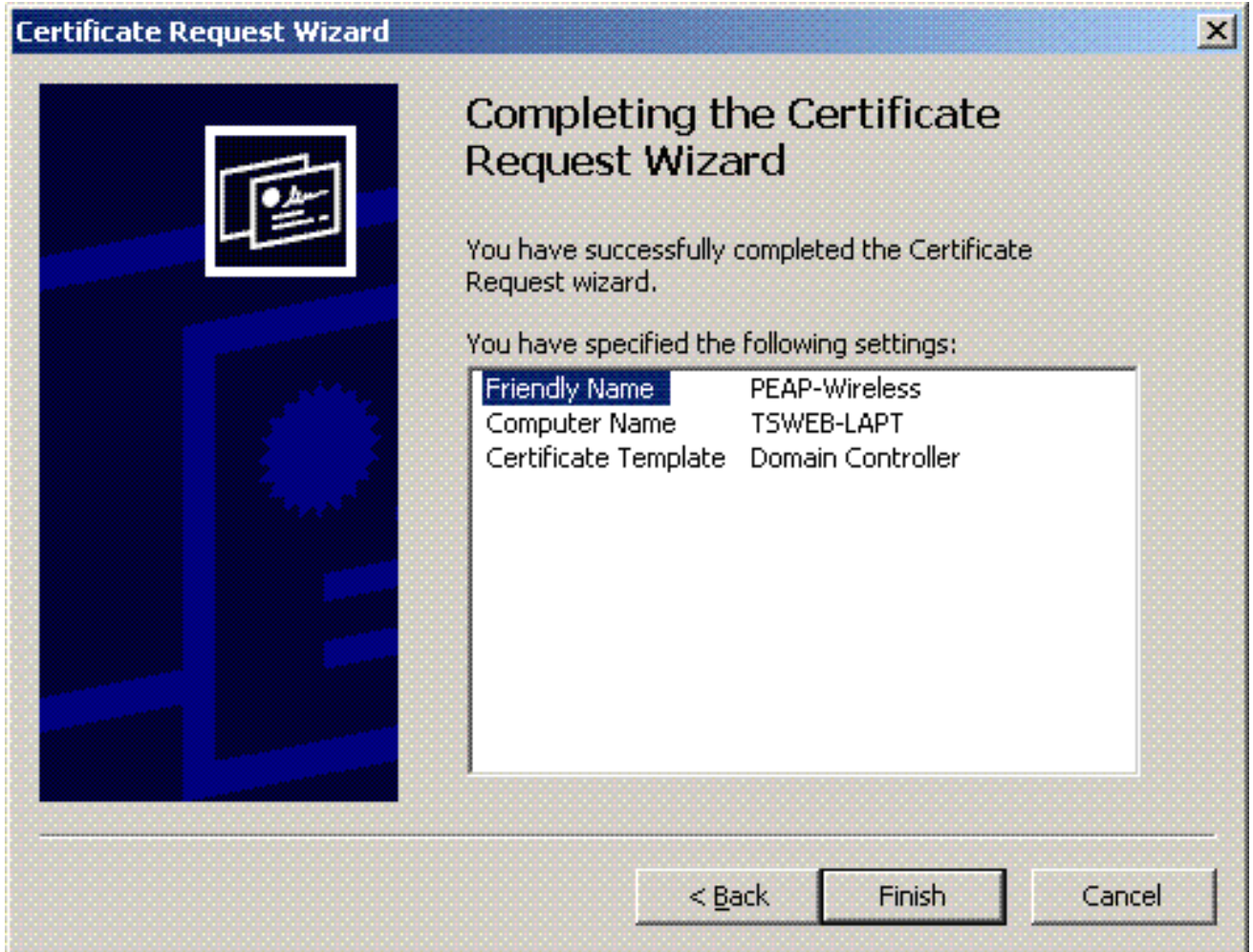
16. **Domain Controller** 証明書テンプレートを選択し (DC 以外のサーバでコンピュータ証明書を要求する場合は **Computer** 証明書テンプレートを選択し)、**Next** をクリックします。



17. 証明書の名前と説明を入力します。



18. **Finish** をクリックして、証明書要求ウィザードを完了します。

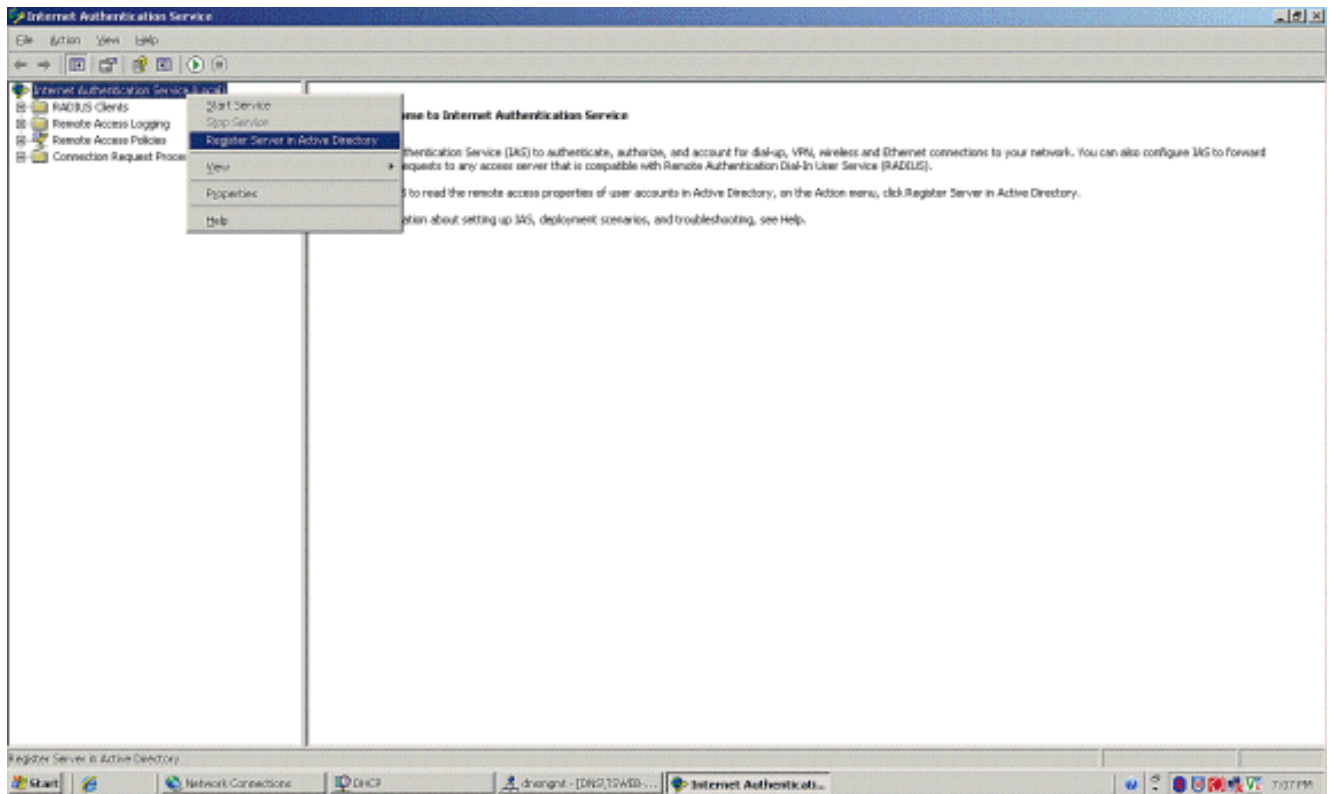


[Internet Authentication Service での PEAP-MS-CHAP v2 認証の設定](#)

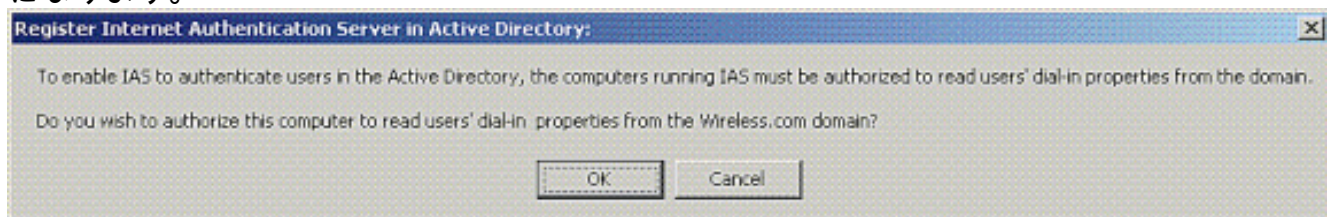
IAS をインストールし、IAS の証明書を要求できたので、IAS に認証の設定を行います。

次のステップを実行します。

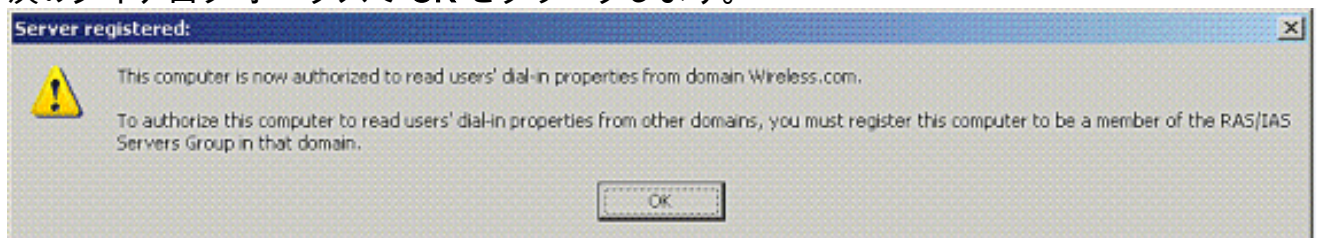
1. **Start > Programs > Administrative Tools** の順にクリックしてから、Internet Authentication Service スナップインをクリックします。
2. **Internet Authentication Service (IAS)** を右クリックし、**Register Service in Active Directory** をクリックします。



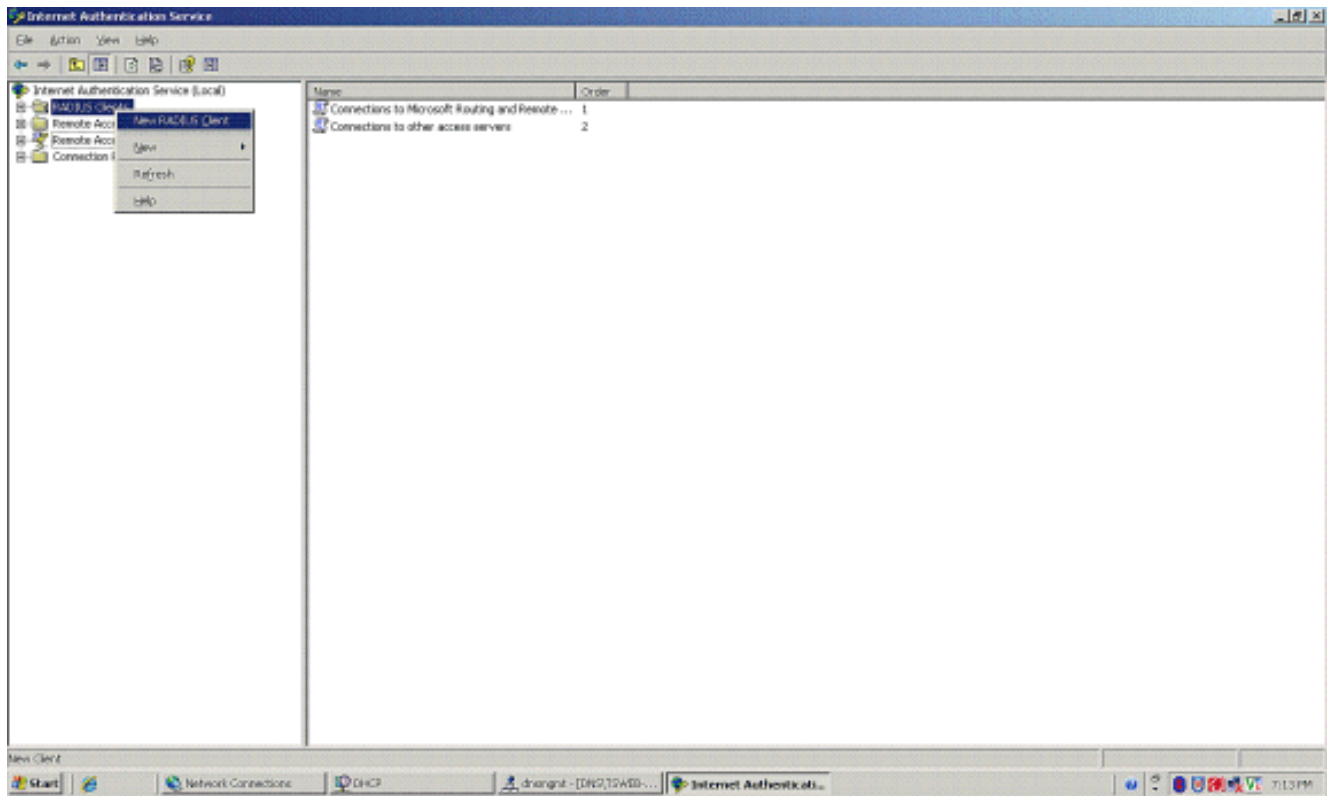
3. Register Internet Authentication Service in Active Directory ダイアログボックスが表示されるので、OK をクリックします。これで、IAS が Active Directory 内のユーザを認証できるようになります。



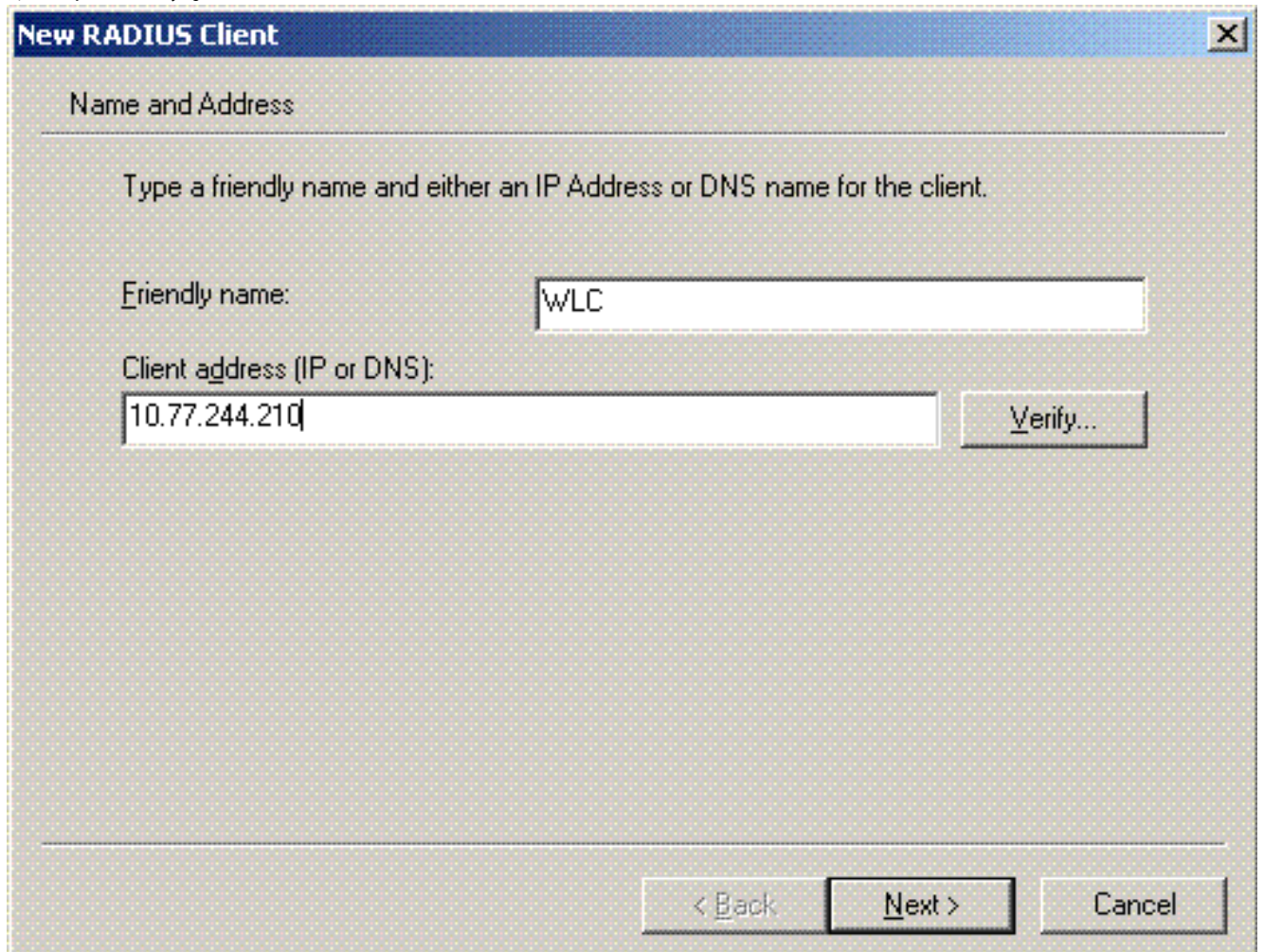
4. 次のダイアログ ボックスで OK をクリックします。



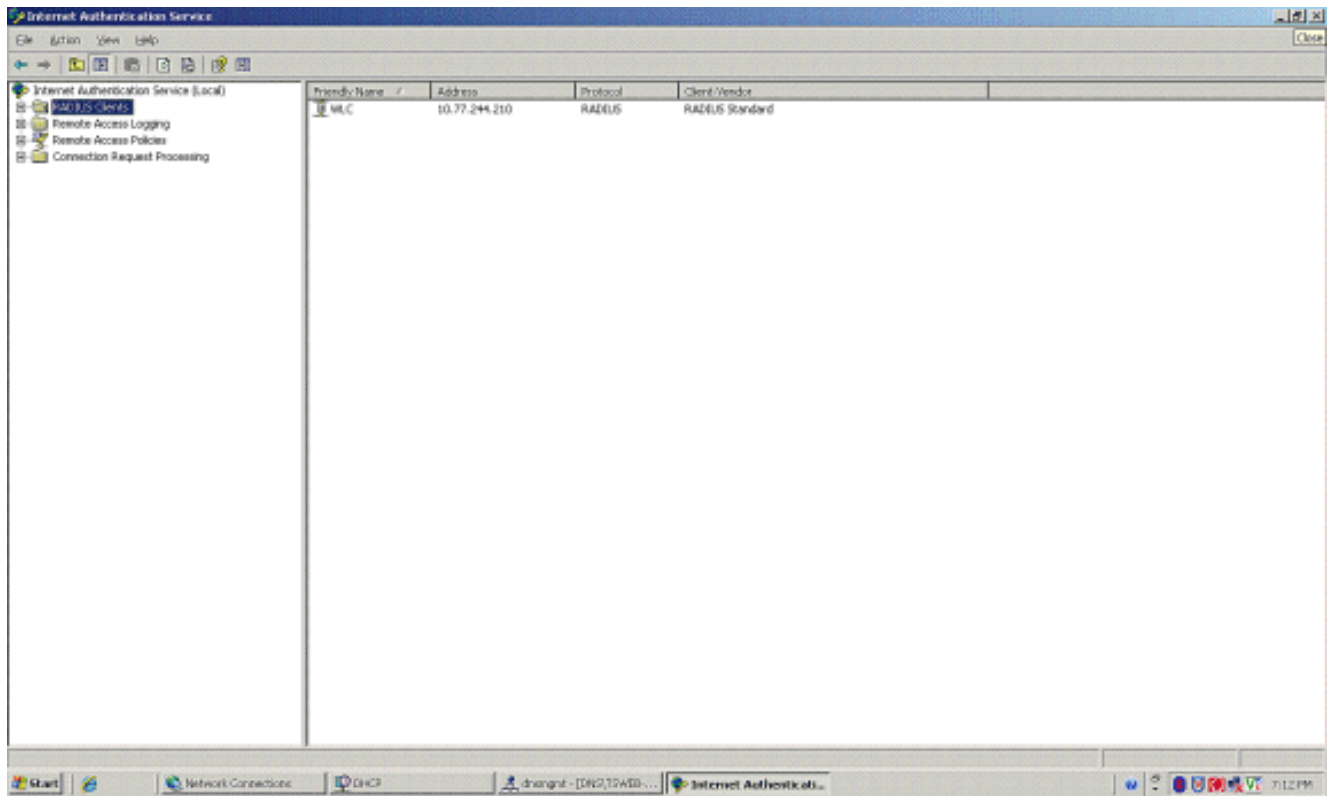
5. MS IAS サーバに、ワイヤレス LAN コントローラを AAA クライアントとして追加します。
6. [RADIUS Clients] を右クリックし、[New RADIUS Client] を選択します。



7. クライアント名 (ここでは WLC) を入力し、WLC の IP アドレスを入力します。[next] をクリックします。

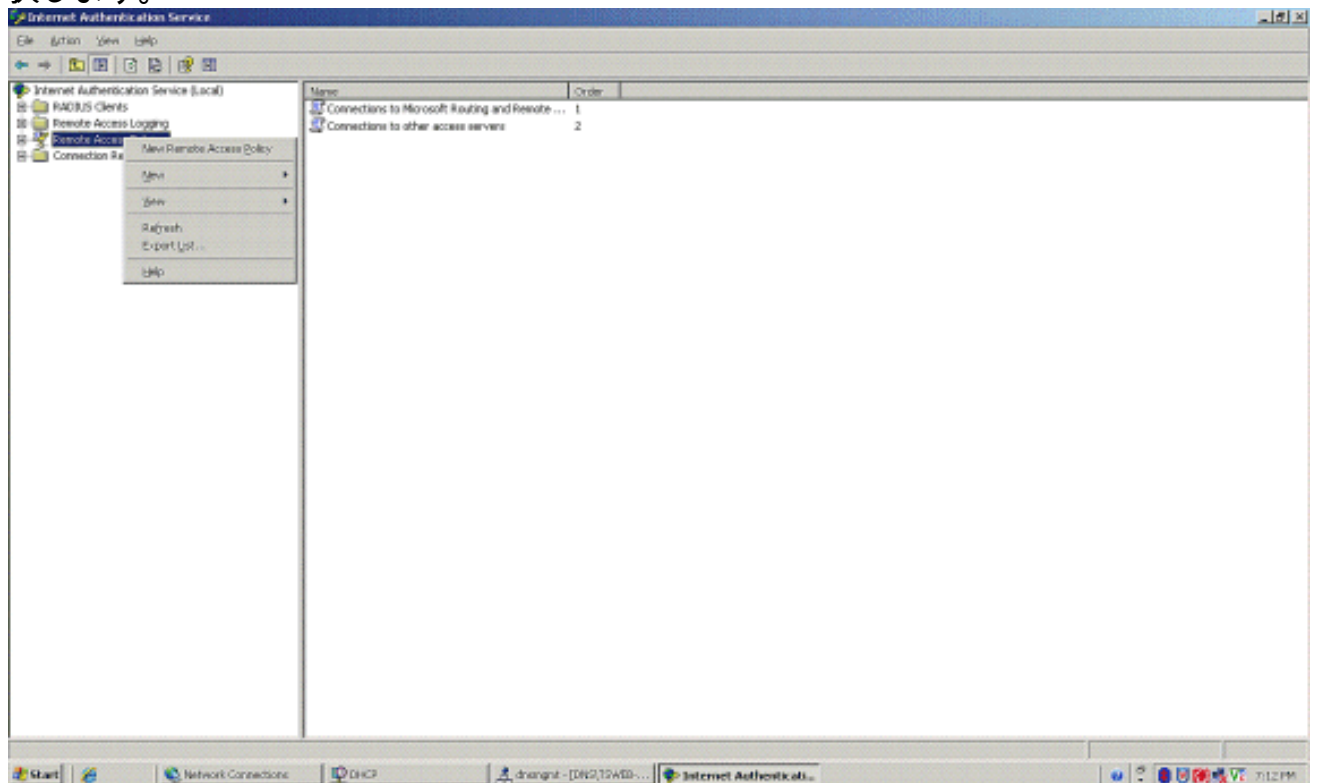


8. 次のページの Client-Vendor で **RADIUS Standard** を選択し、共有秘密鍵を入力し、**Finish** をクリックします。
9. WLC が AAA クライアントとして IAS に追加されていることに注意してください。



10. クライアントのリモート アクセス ポリシーを作成します。

11. そのためには、**Remote Access Policies** を右クリックし、**New Remote Access Policy** を選択します。




12. リモート アクセス ポリシー名を入力します。この例では、**PEAP** という名前を使用します。次に、[Next] をクリックします。

New Remote Access Policy Wizard [X]

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.



How do you want to set up this policy?

Use the wizard to set up a typical policy for a common scenario

Set up a custom policy

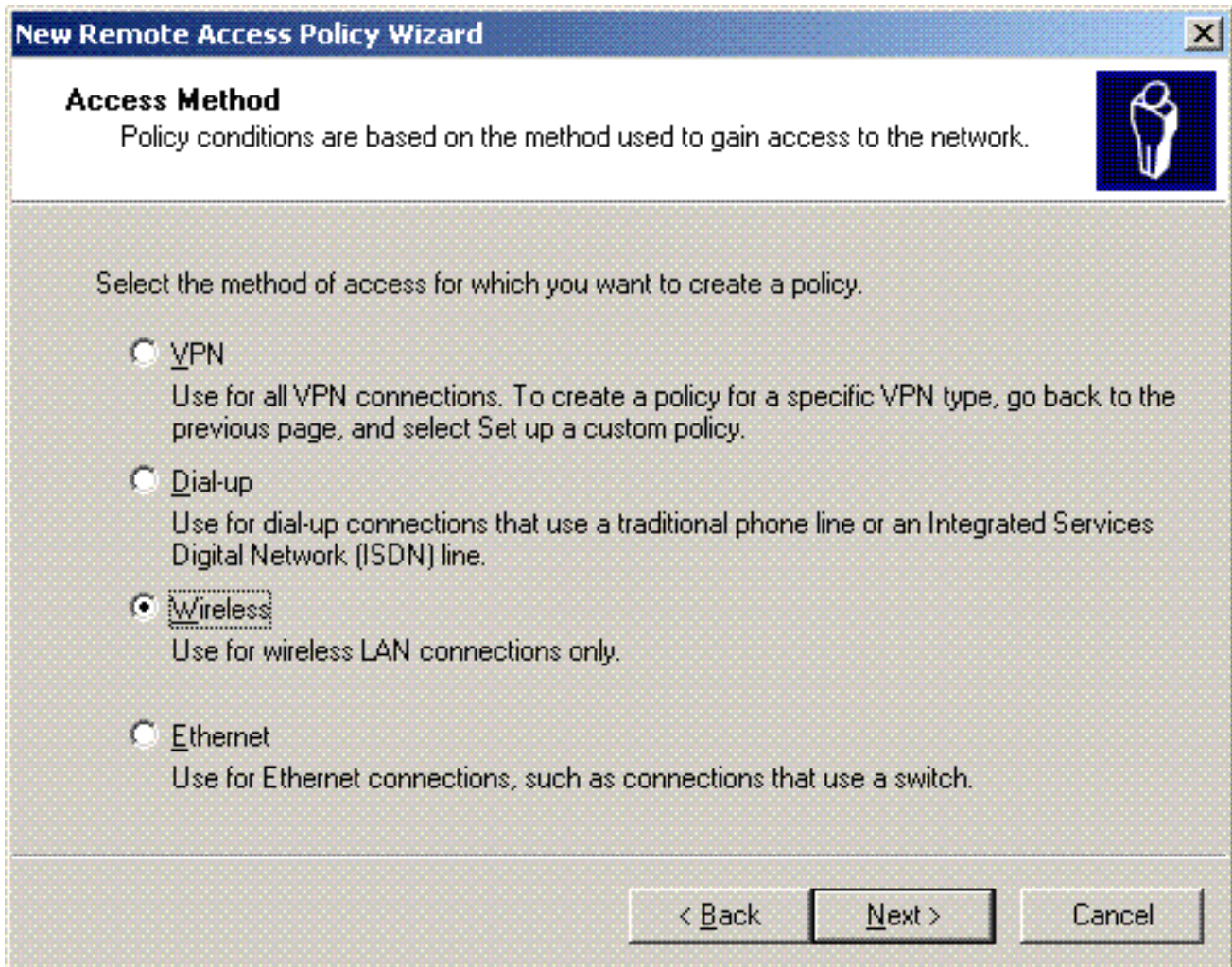
Type a name that describes this policy.

Policy name:

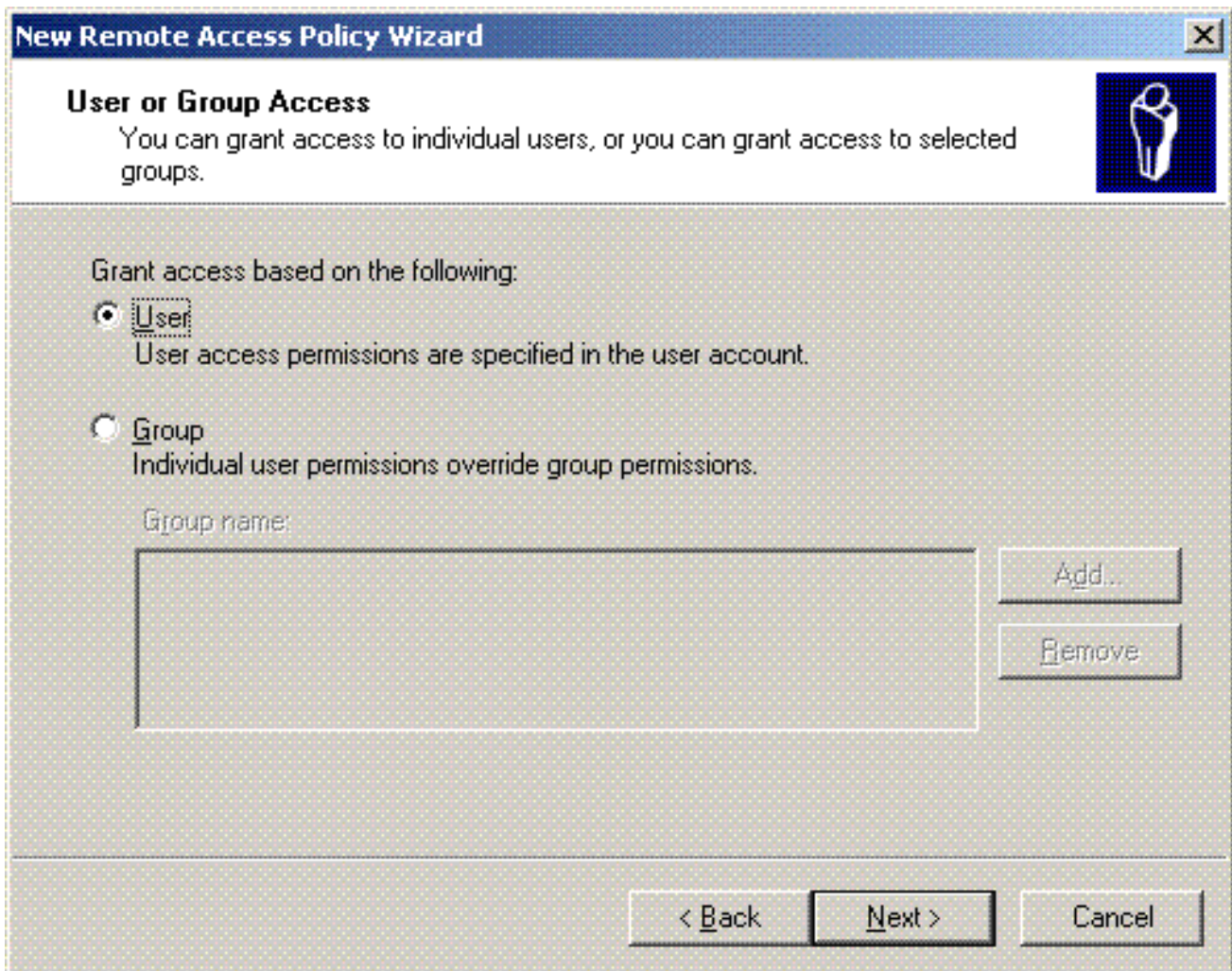
Example: Authenticate all VPN connections.

< Back Next > Cancel

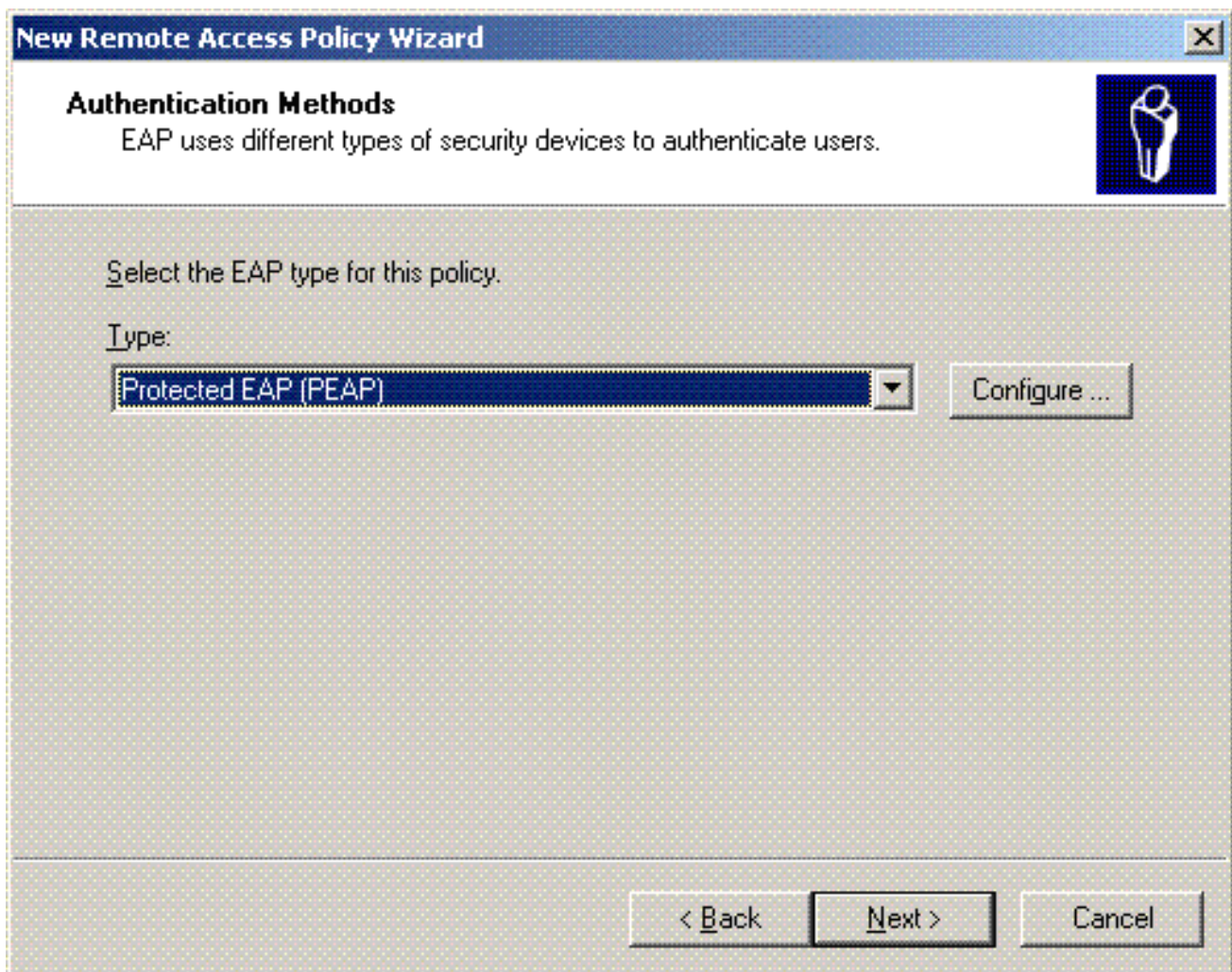
13. 要件に応じてポリシーの属性を選択します。この例では、**Wireless** を選択します。



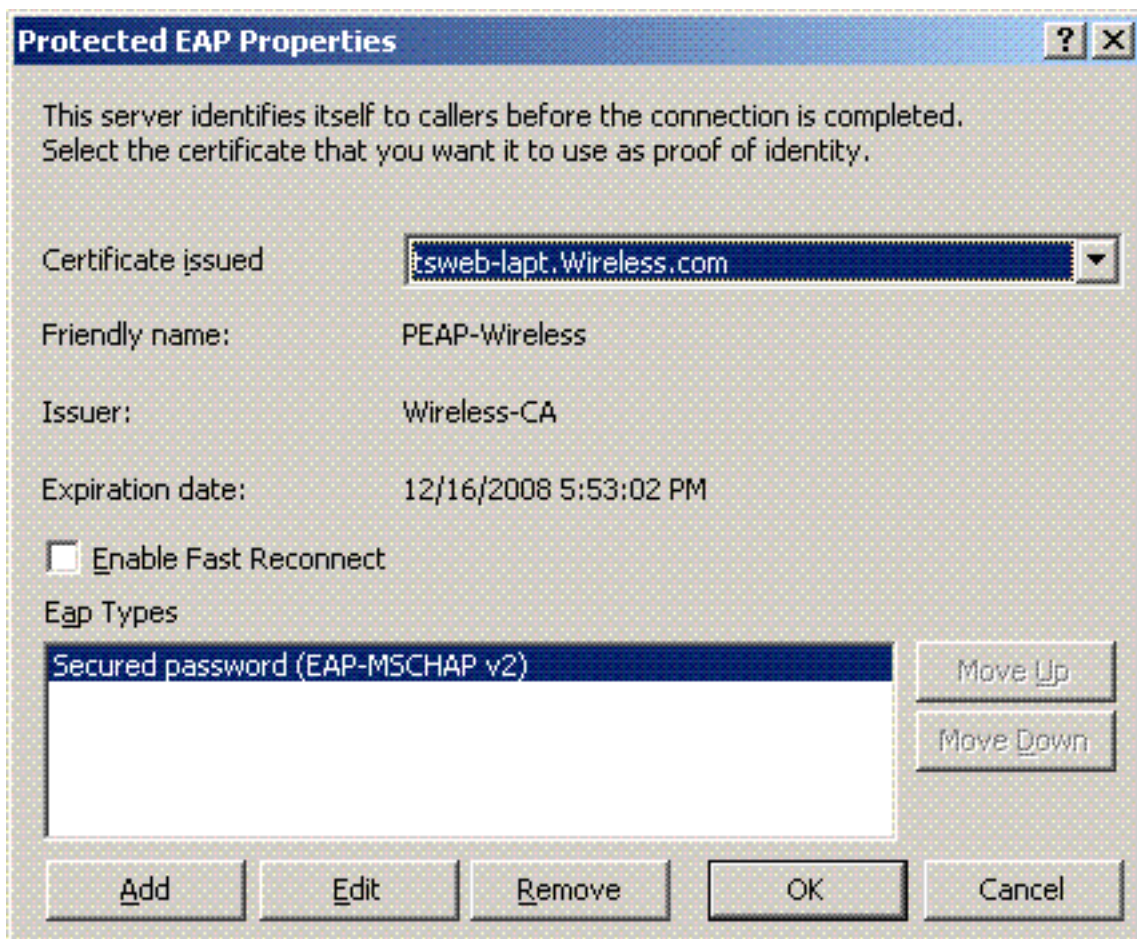
14. 次のページで **User** を選択し、このリモート アクセス ポリシーをユーザのリストに適用します。



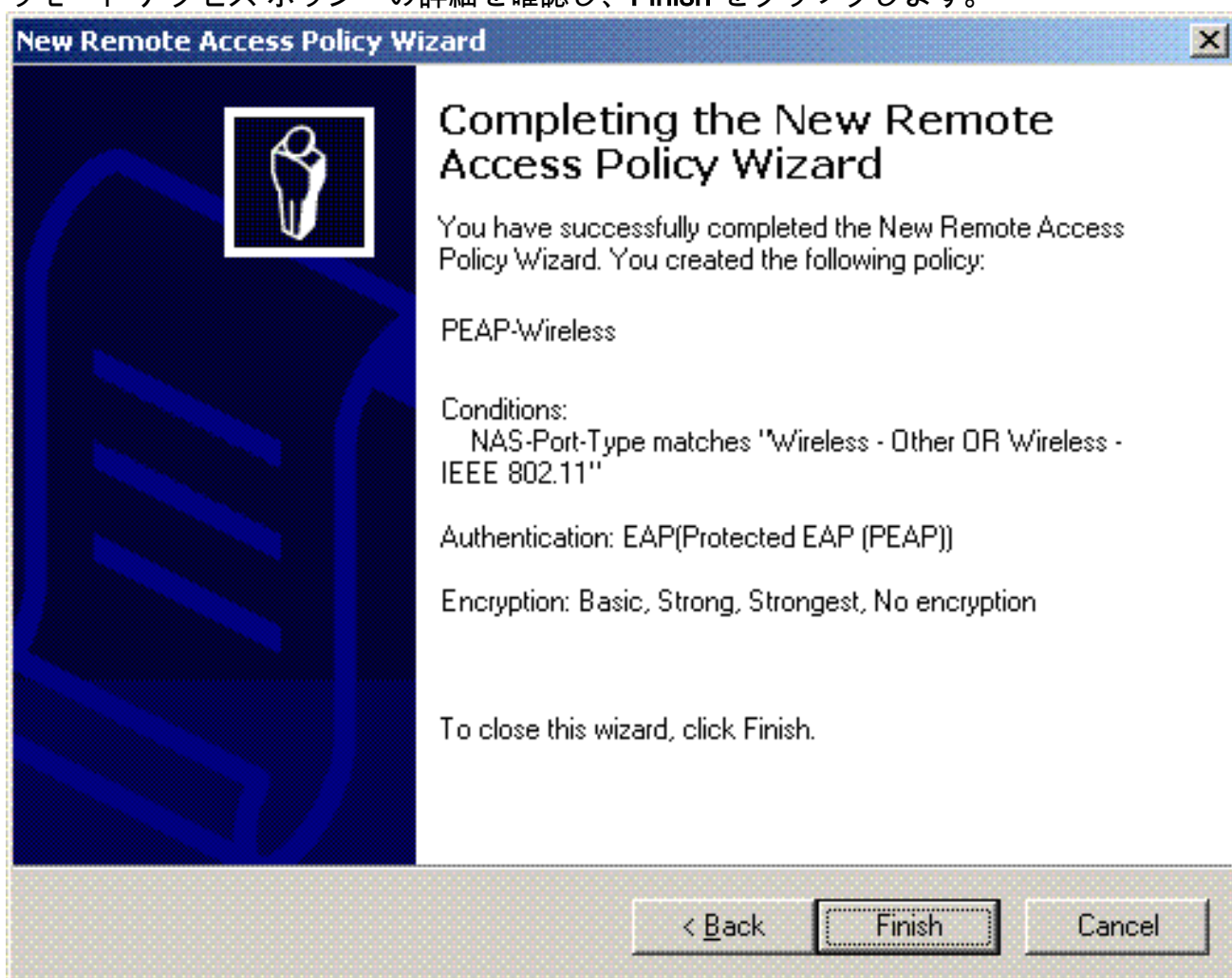
15. Authentication Methods で、Protected EAP (PEAP) を選択し、Configure をクリックします。



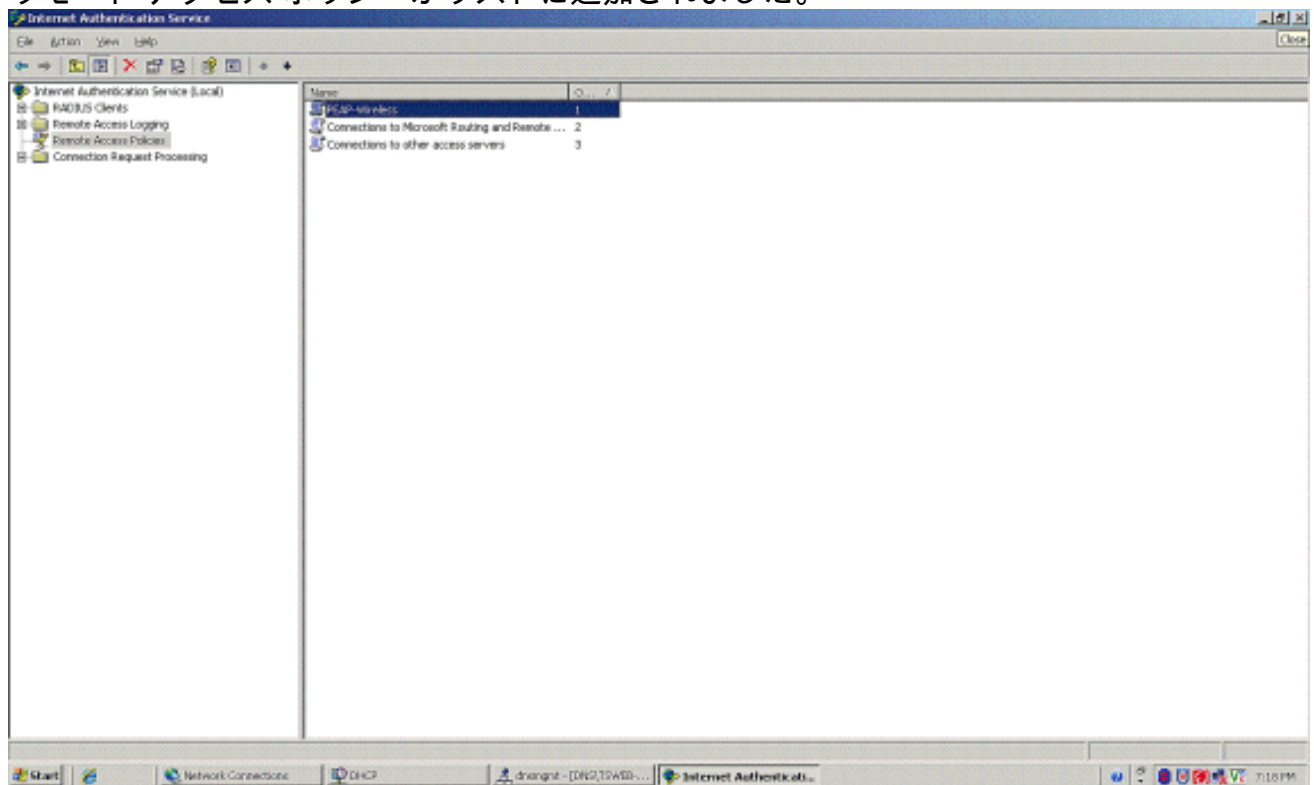
16. **Protected EAP Properties** ページで、Certificate Issued ドロップダウン メニューから該当する証明書を選択し、OK をクリックします。



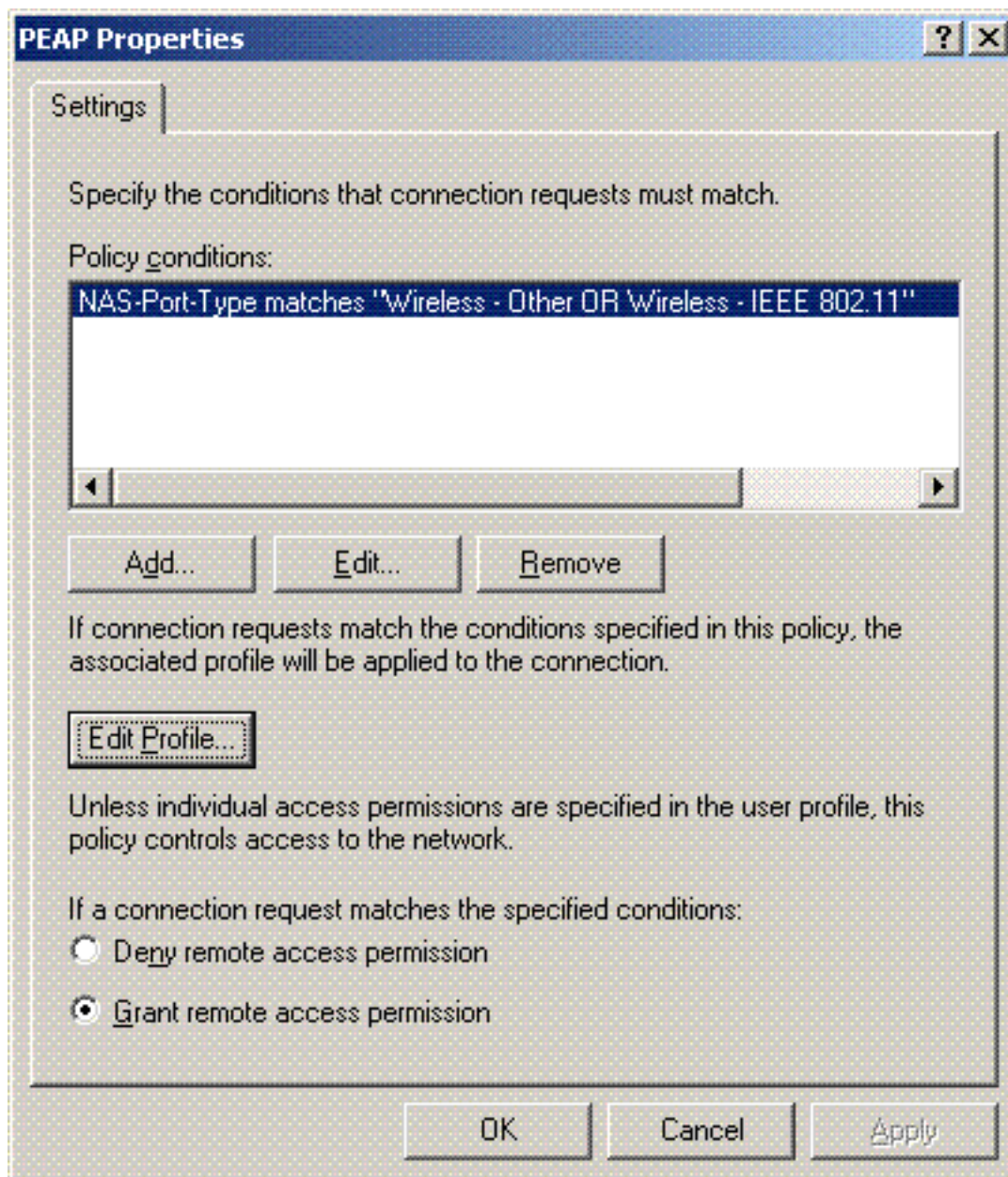
17. リモート アクセス ポリシーの詳細を確認し、**Finish** をクリックします。



18. リモート アクセス ポリシーがリストに追加されました。



19. ポリシーを右クリックして、**Properties** をクリックします。If a connection request matches the specified conditions の下で **Grant remote access permission** を選択します。

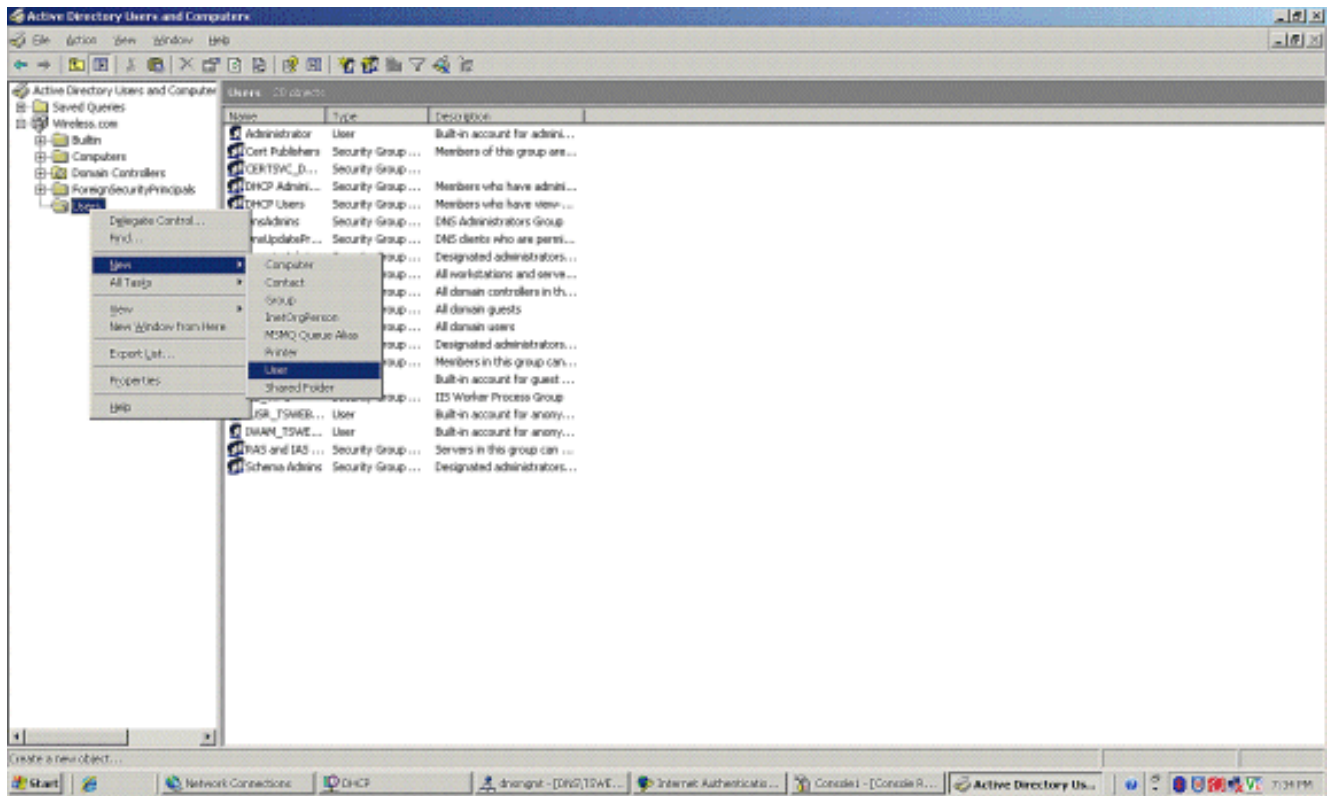


[Active Directory へのユーザの追加](#)

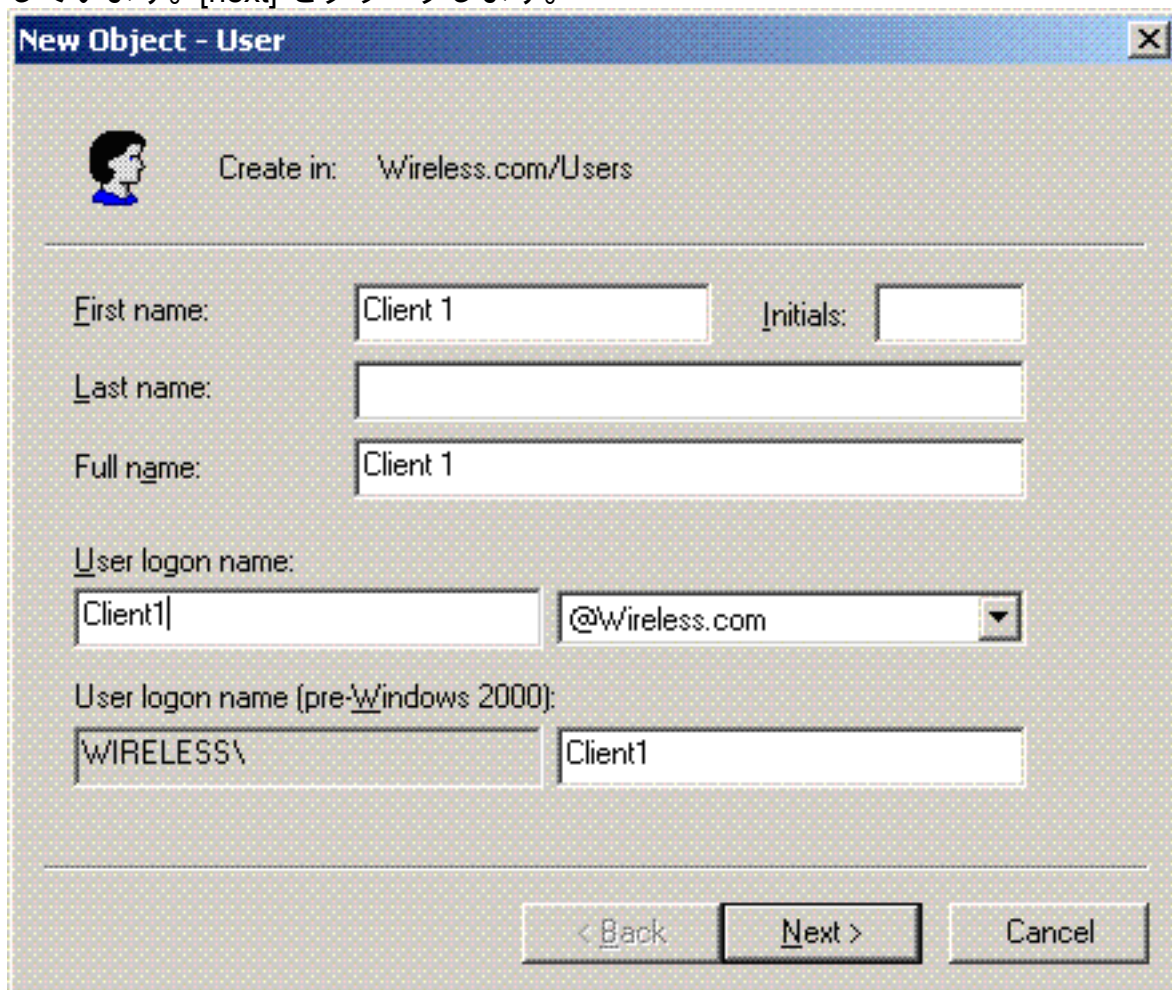
この設定では、Active Directory にユーザ データベースが維持されます。

Active Directory のデータベースにユーザを追加するには、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 **Client 1**、User logon name フィールドに **Client 1** 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。

New Object - User [X]

 Create in: Wireless.com/Users

Password:

Confirm password:

User must change password at next logon

User cannot change password


Password never expires

Account is disabled

< Back Next > Cancel

4. [New Object – User] ダイアログボックスで、[Finish] をクリックします。

New Object - User [X]

 Create in: Wireless.com/Users

When you click Finish, the following object will be created:

Full name: Client 1

User logon name: Client1@Wireless.com

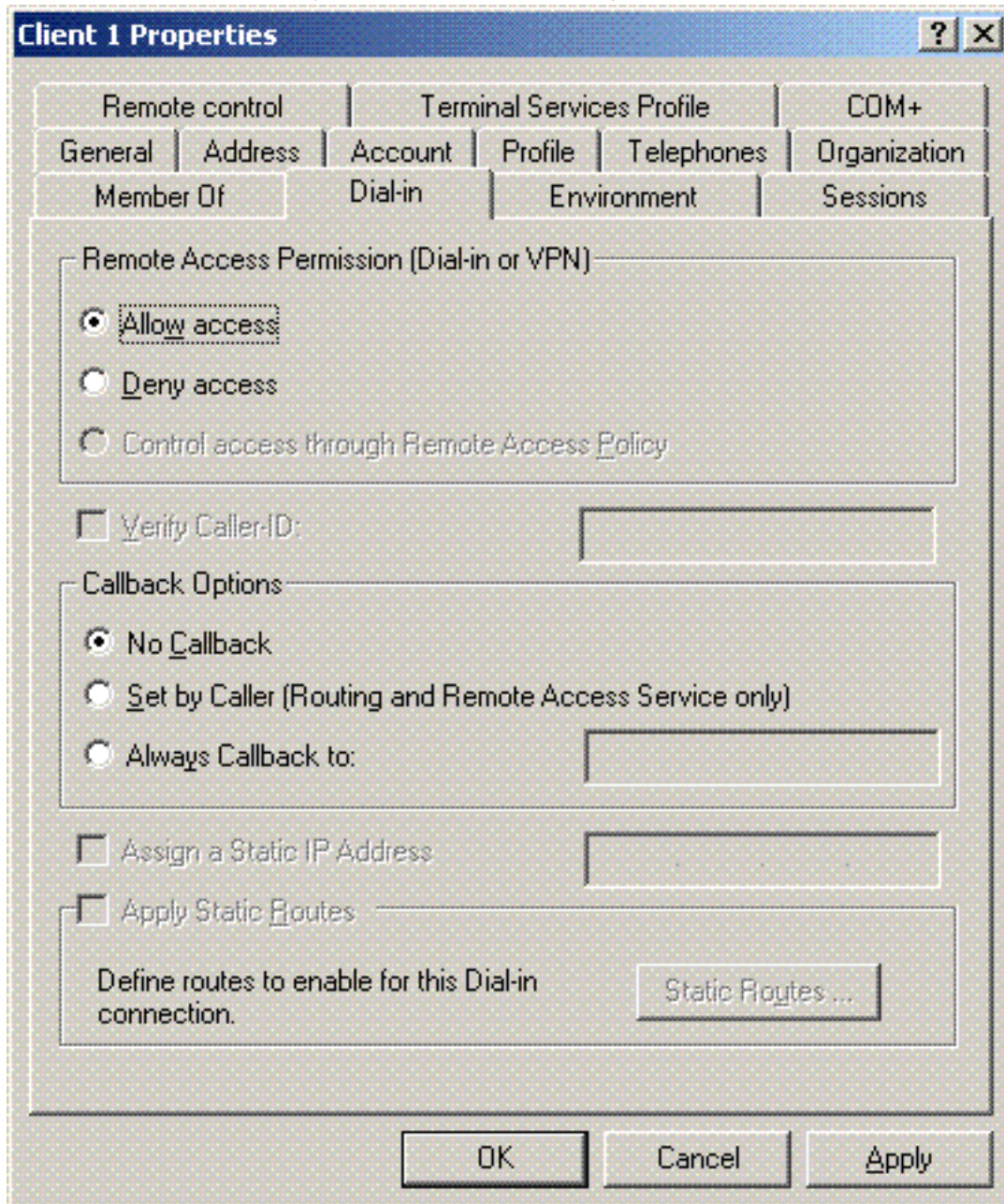
< Back Finish Cancel

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

次のステップを実行します。

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、OK をクリックします。



Wireless LAN Controller と Lightweight AP の設定

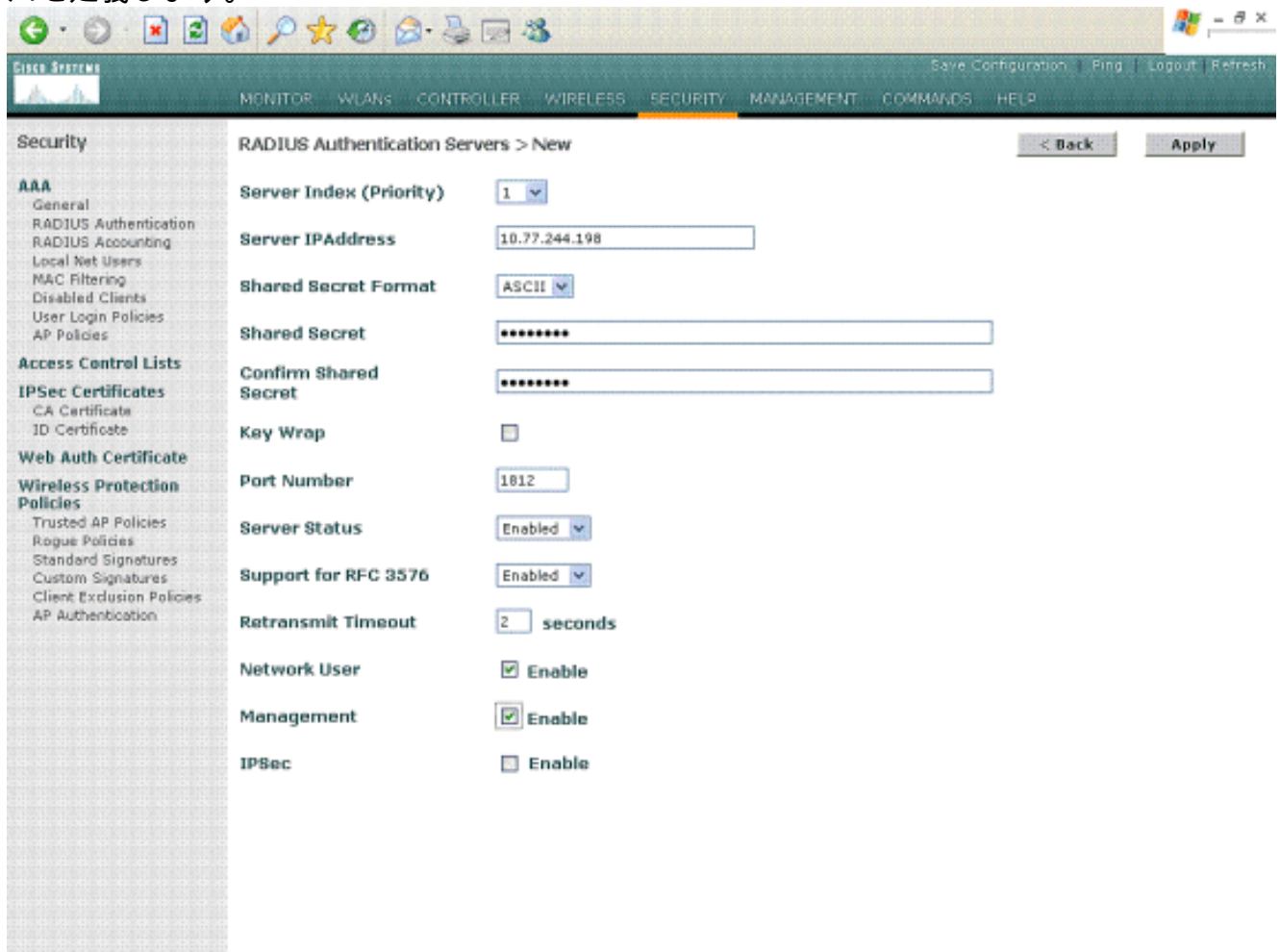
次に、この設定に合わせてワイヤレス デバイスを設定します。これには、Wireless LAN Controller (WLC)、Lightweight AP、およびワイヤレス クライアントの設定が含まれます。

MS IAS RADIUS サーバで RADIUS 認証を行うための WLC の設定

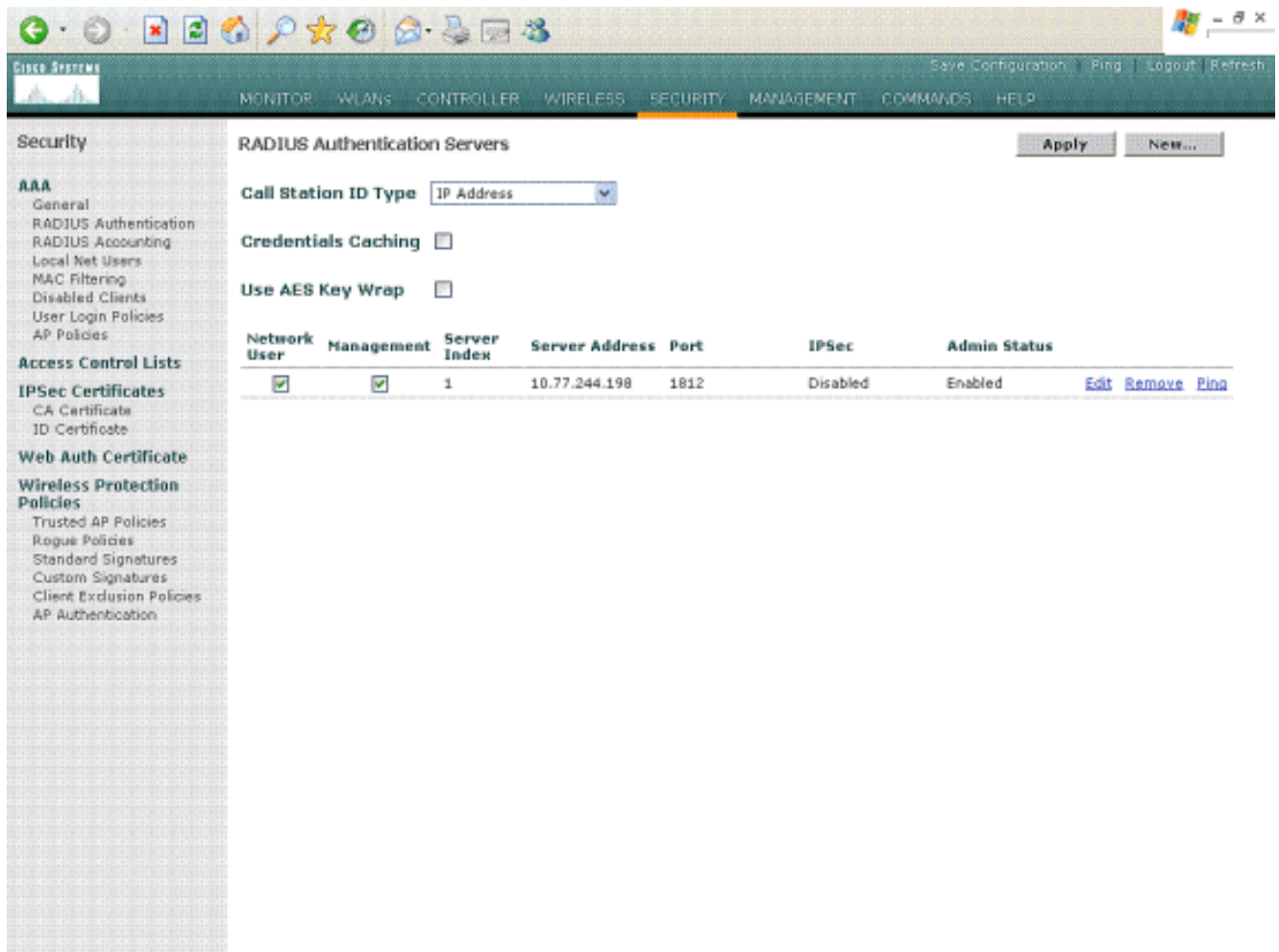
まず、MS IAS を認証サーバに使用するように WLC を設定します。ユーザ クレデンシャルを外部 RADIUS サーバに転送するには、WLC を設定する必要があります。そうすると、外部 RADIUS サーバは、ユーザのクレデンシャルを検証し、ワイヤレス クライアントにアクセス権を付与します。そのためには、**Security > RADIUS Authentication** ページで MS IAS サーバを RADIUS サーバとして追加します。

次のステップを実行します。

1. コントローラの GUI から [Security]、[RADIUS]、[Authentication] を選択して、[RADIUS Authentication Servers] ページを表示します。次に、[New] をクリックして、RADIUS サーバを定義します。



2. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義します。RADIUS サーバ IP アドレス、共有秘密、ポート番号、サーバステータスなどのパラメータがあります。[Network User] チェックボックスと [Management] チェックボックスでは、管理ユーザとネットワークユーザに RADIUS ベースの認証を適用するかどうかを指定します。この例では、MS IAS を 10.77.244.198 という IP アドレスを持つ RADIUS サーバとして使用しています。



3. [Apply] をクリックします。
4. MS IAS サーバが Radius サーバとして WLC に追加され、ワイヤレス クライアントの認証に使用できるようになりました。

WLAN でのクライアントの設定

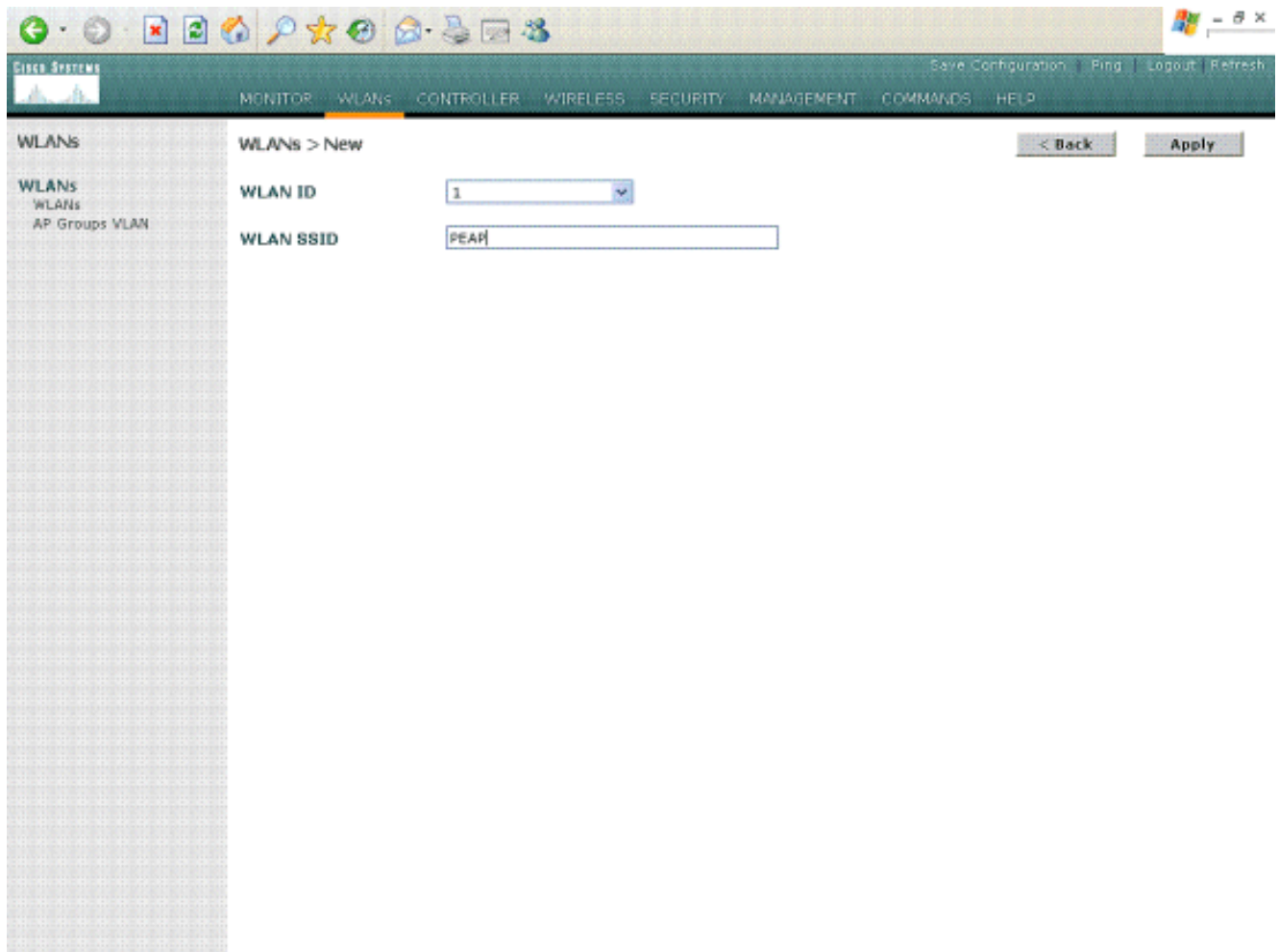
ワイヤレス クライアントの接続先の SSID (WLAN) を設定します。この例では、PEAP という名前の SSID を作成します。

クライアントが EAP ベースの認証 (ここでは PEAP-MSCHAPv2) を実行し、AES を暗号化メカニズムとして使用するよう、レイヤ 2 認証に WPA2 を定義します。他の値はすべてデフォルトのままにします。

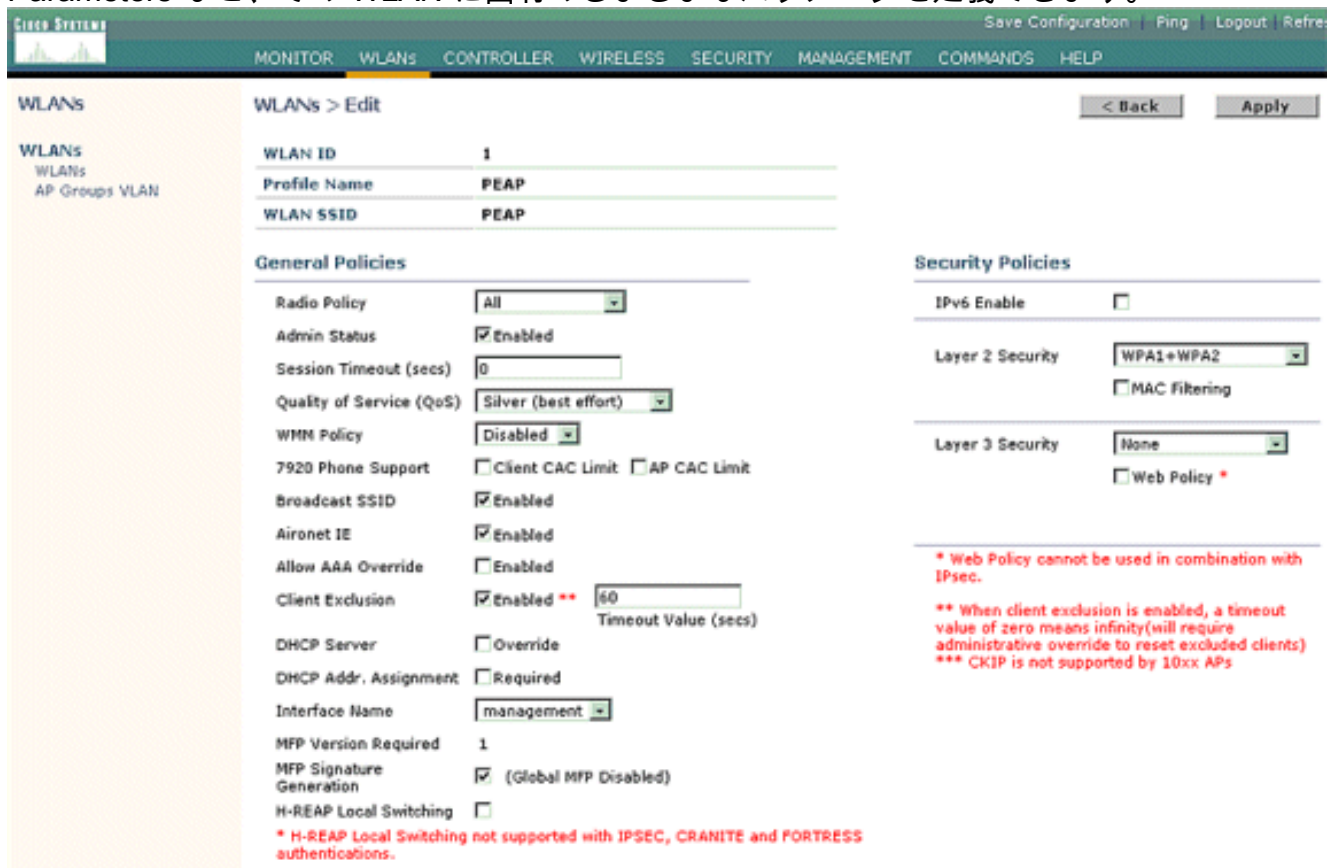
注 : このドキュメントでは、WLAN を管理インターフェイスにバインドしています。ネットワークに複数の VLAN がある場合、独立した VLAN を作成してそれを SSID にバインドすることができます。WLC に VLAN を設定する方法については、『[無線 LAN コントローラでの VLAN の設定例](#)』を参照してください。

WLC に WLAN を設定するには、次の手順を実行します。

1. コントローラの GUI で [WLANs] をクリックして、[WLANs] ページを表示します。このページには、コントローラに存在する WLAN の一覧が表示されます。
2. 新しい WLAN を作成するには、[New] をクリックします。WLAN の WLAN ID と WLAN SSID を入力し、[Apply] をクリックします。



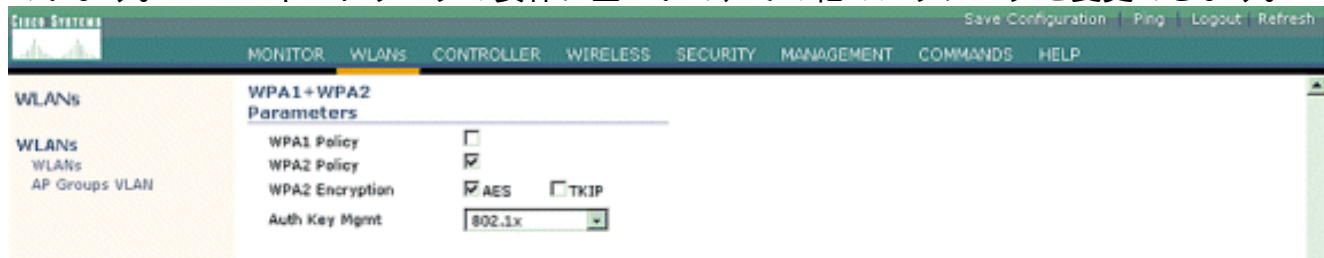
3. 新しい WLAN を作成すると、新しい WLAN に対する [WLAN] > [Edit] ページが表示されます。このページでは、General Policies、RADIUS Servers、Security Policies、802.1x Parameters など、その WLAN に固有のさまざまなパラメータを定義できます。



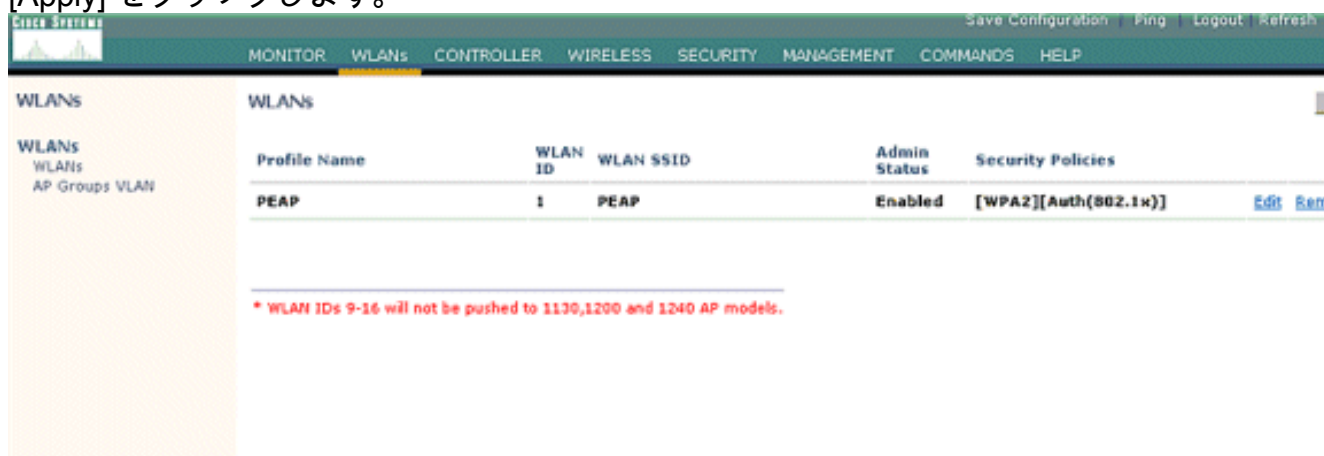
4. WLAN を有効にするには、General Policies の下の Admin Status にチェックマークを入れます。

す。AP にビーコン フレームで SSID をブロードキャストさせる場合は、**Broadcast SSID** にチェックマークを入れます。

5. Layer 2 Security で、**WPA1+WPA2** を選択します。これで、WLAN で WPA が有効になります。ページを下にスクロールし、WPA policy を選択します。この例では、WPA2 と AES 暗号化を使用しています。[RADIUS Servers] のプルダウン メニューから、適切な RADIUS サーバを選択します。この例では、**10.77.244.198** (MS IAS サーバの IP アドレス) を使用しています。WLAN ネットワークの要件に基づいて、その他のパラメータを変更できます。



6. [Apply] をクリックします。



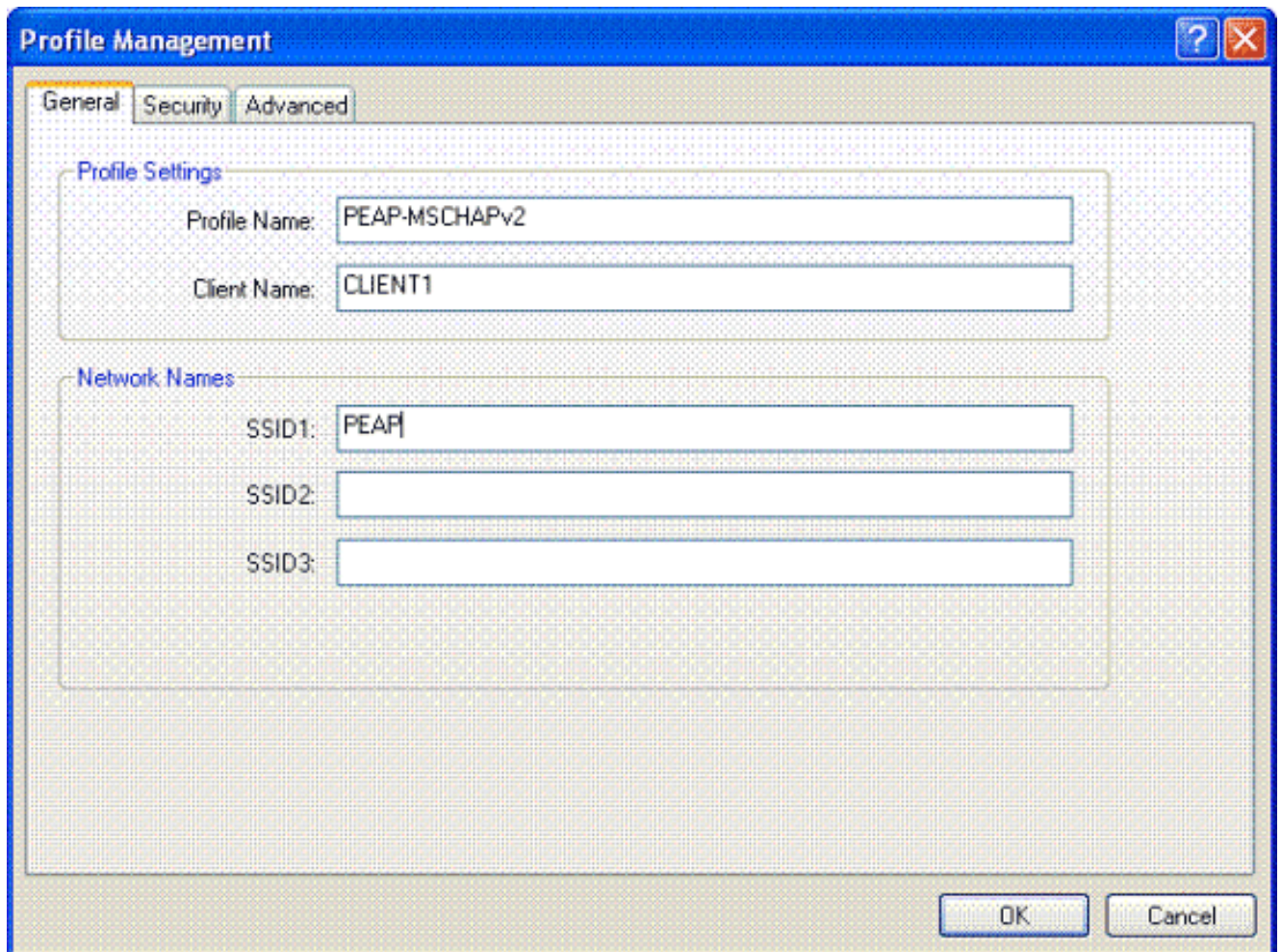
ワイヤレス クライアントの設定

ワイヤレス クライアントでの PEAP-MS-CHAP v2 認証の設定

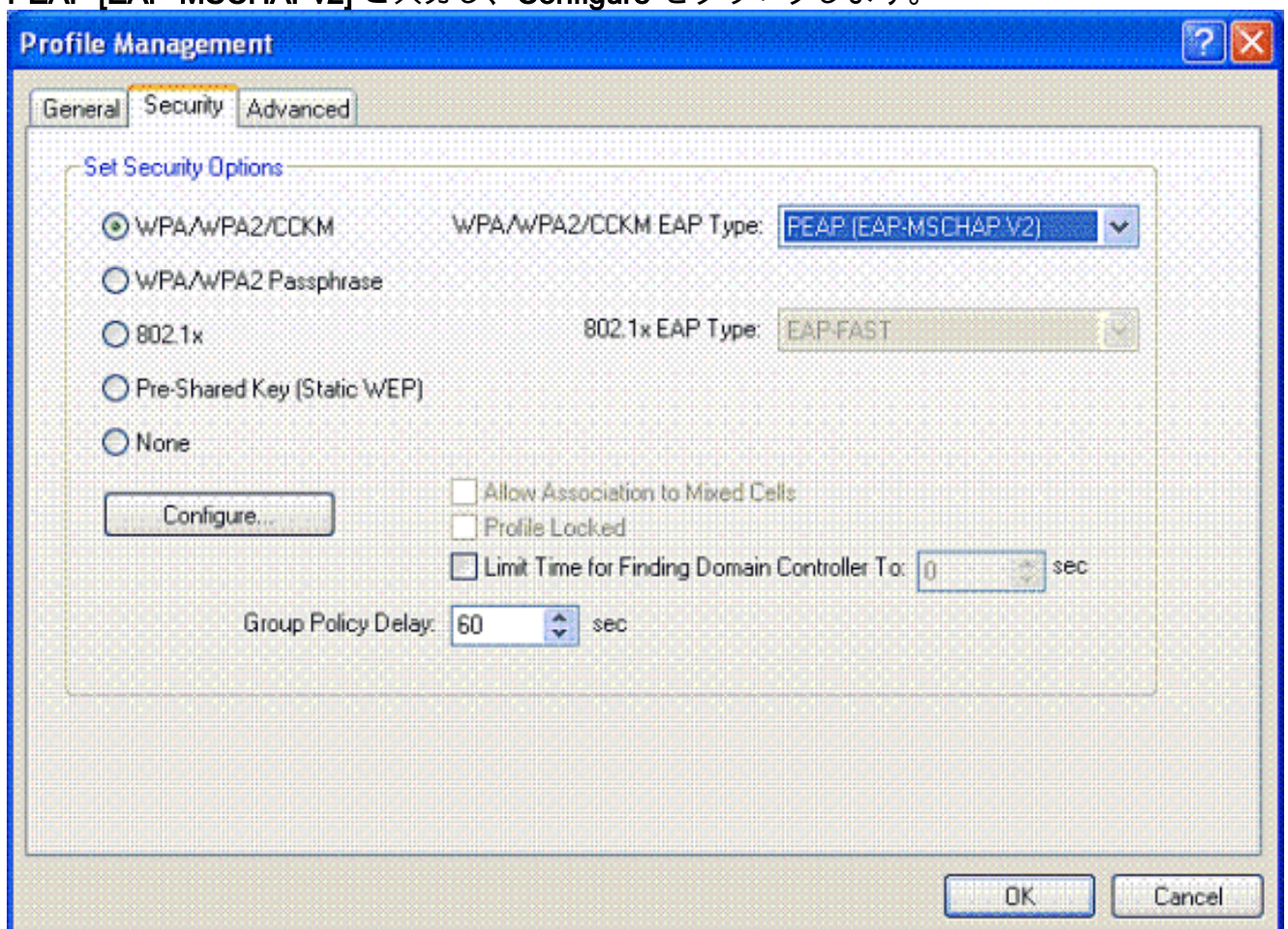
次の例では、Cisco Aironet Desktop Utility (ADU) を使用してワイヤレス クライアントを設定する方法について説明しています。クライアント アダプタの設定を行う前に、使用するファームウェアとユーティリティのバージョンが最新であることを確認してください。最新バージョンのファームウェアとユーティリティは、Cisco.com の Wireless ダウンロード ページにあります。

ADU で Cisco Aironet 802.11a/b/g ワイヤレス クライアント アダプタを設定するには、次の手順を実行します。

1. Aironet Desktop Utility を開きます。
2. **Profile Management** をクリックし、**New** をクリックしてプロファイルを定義します。
3. General タブでプロファイル名と SSID を入力します。この例では、WLC に設定した SSID (PEAP) を使用します。



4. Security タブを選択し、WPA/WPA2/CCKM を選択して、WPA/WPA2/CCKM EAP type で PEAP [EAP-MSCHAPv2] と入力し、Configure をクリックします。



5. **Validate Server Certificate** を選択し、Trusted Root Certificate Authorities ドロップダウンメニューで **Wireless-CA** を選択します。

Configure PEAP (EAP-MSCHAP V2)

Use Machine Information for Domain Logon

Validate Server Identity

Trusted Root Certification Authorities

Wireless-CA

When connecting, use:

Certificate

User Name and Password

Select a Certificate

Use Windows User Name and Password

User Information for PEAP (EAP-MSCHAP V2) Authentication

User Name: Administrator

Password:

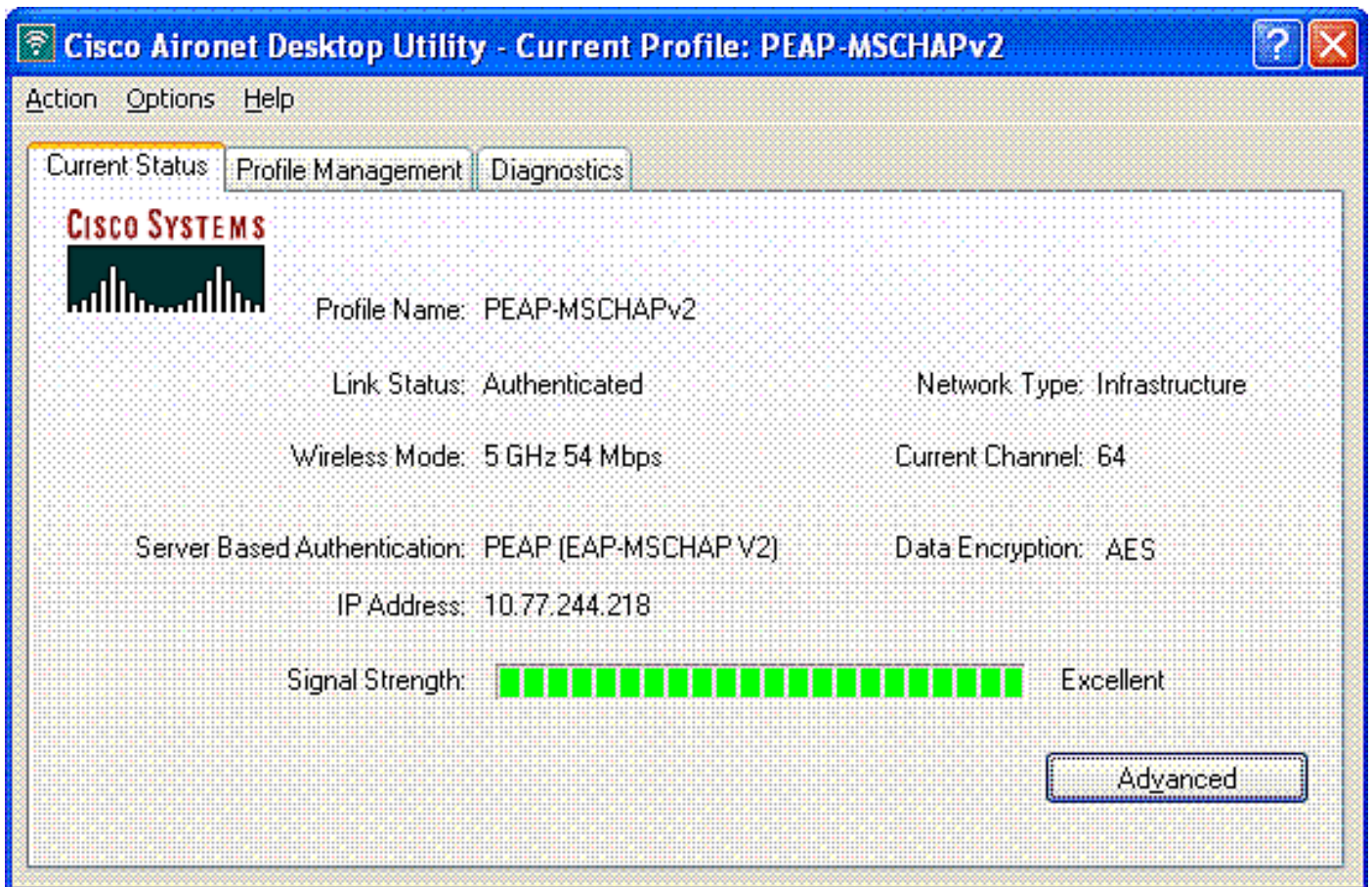
Confirm Password:

Advanced... OK Cancel

6. **OK** をクリックし、プロファイルを有効にします。注：Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2(PEAP-MSCHAPv2)をMicrosoft XP SP2で使用し、ワイヤレスカードがMicrosoft Wireless Zero Configuration(WZC)で管理されている場合は、MicrosoftホットフィックスKB885453を適用する必要があります。このホットフィックスにより、PEAP ファスト レジュームに関連した認証上のいくつかの問題が防止されます。

確認とトラブルシューティング

設定が期待通りに動作することを確認するには、ワイヤレス クライアント Client1 上のプロファイル PEAP-MSCHAPv2 を有効にします。



プロファイル PEAP-MSCHAPv2 が ADU 上で有効になると、クライアントでは 802.11 オープン認証が実行され、次に PEAP-MSCHAPv2 認証が実行されます。PEAP-MSCHAPv2 認証の成功例を次に示します。

発生するイベントのシーケンスを理解するには、デバッグ コマンドを使用します。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

ワイヤレス LAN コントローラでの次のデバッグ コマンドが有用です。

- debug dot1x events enable : 802.1x イベントのデバッグを設定
- debug aaa events enable : AAA イベントのデバッグを設定
- debug mac addr <mac address> : MAC のデバッグを設定、debug mac コマンドを使用
- debug dhcp message enable : DHCP エラー メッセージのデバッグを設定

debug dot1x events enable コマンドと debug client <mac address> コマンドの出力例を次に示します。

debug dot1x events enable

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
mobile 00:40:96:ac:e6:57
```


Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to mobile 00:40:96:ac:e6:57**
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57**
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57**

debug mac addr <MAC Address>

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 - rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20)**
Change state to START (0)
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**
Initializing policy
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0)**
Change state to AUTHCHECK (2)
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2)**
Change state to 8021X_REQD (3)
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)**
Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Connecting state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP-Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from mobile 00:40:96:ac:e6:57**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from Connecting to Authenticating for mobile 00:40:96:ac:e6:57**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Authenticating state**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Processing Access-Accept for mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending default RC4 key to mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
8021X_REQD (3) **Change state to L2AUTHCOMPLETE (4)**

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
L2AUTHCOMPLETE (4) Change state to RUN (20)

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached PLUMBFASPATH: from line 4041

Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Replacing Fast Path rule
type = Airespace AP Client
on AP 00:0b:85:51:5a:e0, slot 0, interface = 2

```
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
Card = 0 (slot 0), InHandle = 0x00000000,
OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
(20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

注 : PEAP認証用のCisco Secure ACSで認証するためにMicrosoftサブリカントを使用すると、クライアントが正常に認証されない可能性があります。最初の接続は正しく認証されるのに、後続の高速接続の認証でうまく接続が行われません。これは既知の問題です。この問題の詳細と修正方法は[ここ](#)から利用できます。

[関連情報](#)

- [ACS 4.0 と Windows 2003 を使用した Cisco Unified Wireless Network 環境での PEAP](#)
- [EAP 認証と WLAN コントローラ \(WLC \) の設定例](#)
- [ワイヤレス LAN コントローラ \(WLC \) のソフトウェア アップグレード](#)
- [Cisco 4400 シリーズ Wireless LAN Controller - 設定ガイド](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。