

# ACS 4.0 と Windows 2003 を使用した Unified Wireless Network 環境での EAP-TLS

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

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

[DC CA \( wirelessdemoca \)](#)

[Cisco Secure ACS 4.0 を使用する Windows Standard 2003 のセットアップ](#)

[基本的なインストールと設定](#)

[Cisco Secure ACS 4.0 のインストール](#)

[Cisco LWAPP コントローラの設定](#)

[WPA2/WPA に必要な設定の作成](#)

[EAP-TLS 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 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](#)

[ACS 4.0 ソフトウェアでの証明書のインストール](#)

[Windows の自動機能を使用した EAP-TLS 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 ネットワーク接続の設定](#)

[関連情報](#)

## 概要

このドキュメントでは、Wireless LAN Controller ( WLC )、Microsoft Windows 2003 ソフトウェア、および Cisco Secure Access Control Server ( ACS ) 4.0 を使用して、Extensible Authentication Protocol-Transport Layer Security ( EAP-TLS ) による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：セキュリティワイヤレスの展開の詳細については、[Microsoft Wi-Fi Webサイト](#) および [Cisco SAFE Wireless Blueprint](#)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 ワイヤレス LAN コントローラ](#)』Cisco 2000 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 2000 シリーズ Wireless LAN Controller](#)』。

開始する前に、テスト ラボの各サーバに 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。コントローラおよび AP をインストールし、最新のソフトウェア アップデートが設定されていることを確認してください。

**重要：**このドキュメントの執筆時点における Windows Server 2003 の最新アップデートは SP1 で、Windows XP Professional の最新ソフトウェアは更新パッチ適用済みの SP2 です。

このドキュメントでは、EAP-TLS 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 SP 1 Enterprise Edition を使用しています。これについては、このドキュメントの「[EAP-TLS 認証](#)」セクションで説明します。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

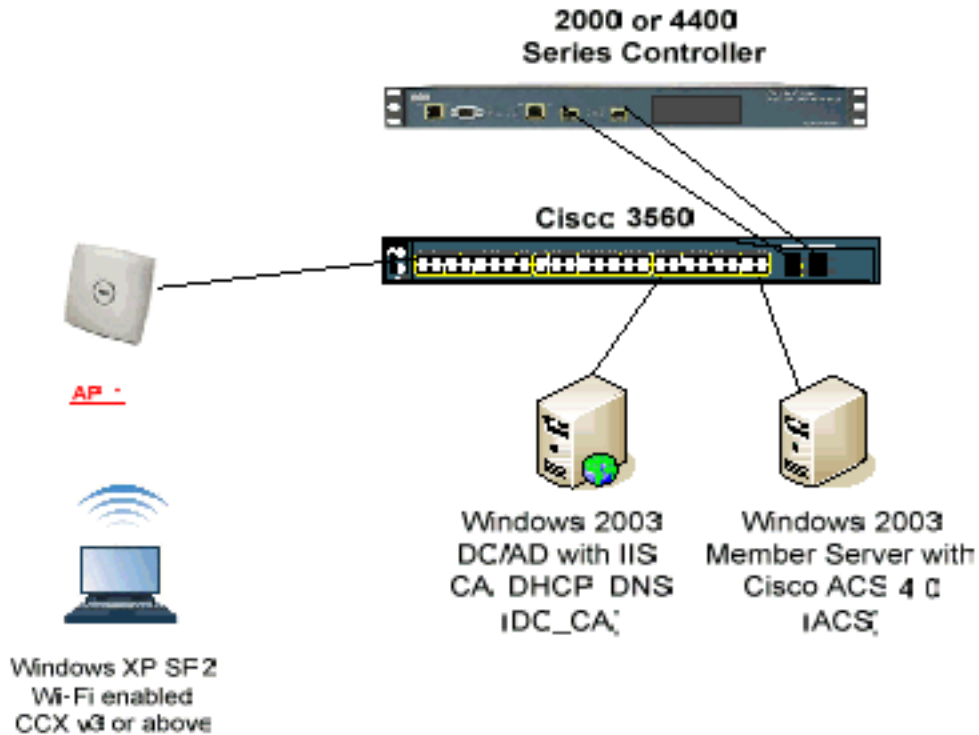
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 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ブリカント
- 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 セットアップを使用します。

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 EAP-TLS 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)を搭載したWi-Fi Protected Access(WPA)/WPA2をSPを搭載したWindows XP Professionalに追加するには、『[WPA2/Wireless Provisioning Services Information Element \(WPS IE update\)](#)』を参照してくださいWindows XP SP2用。

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。

## [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](#)

次のステップを実行します。

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。

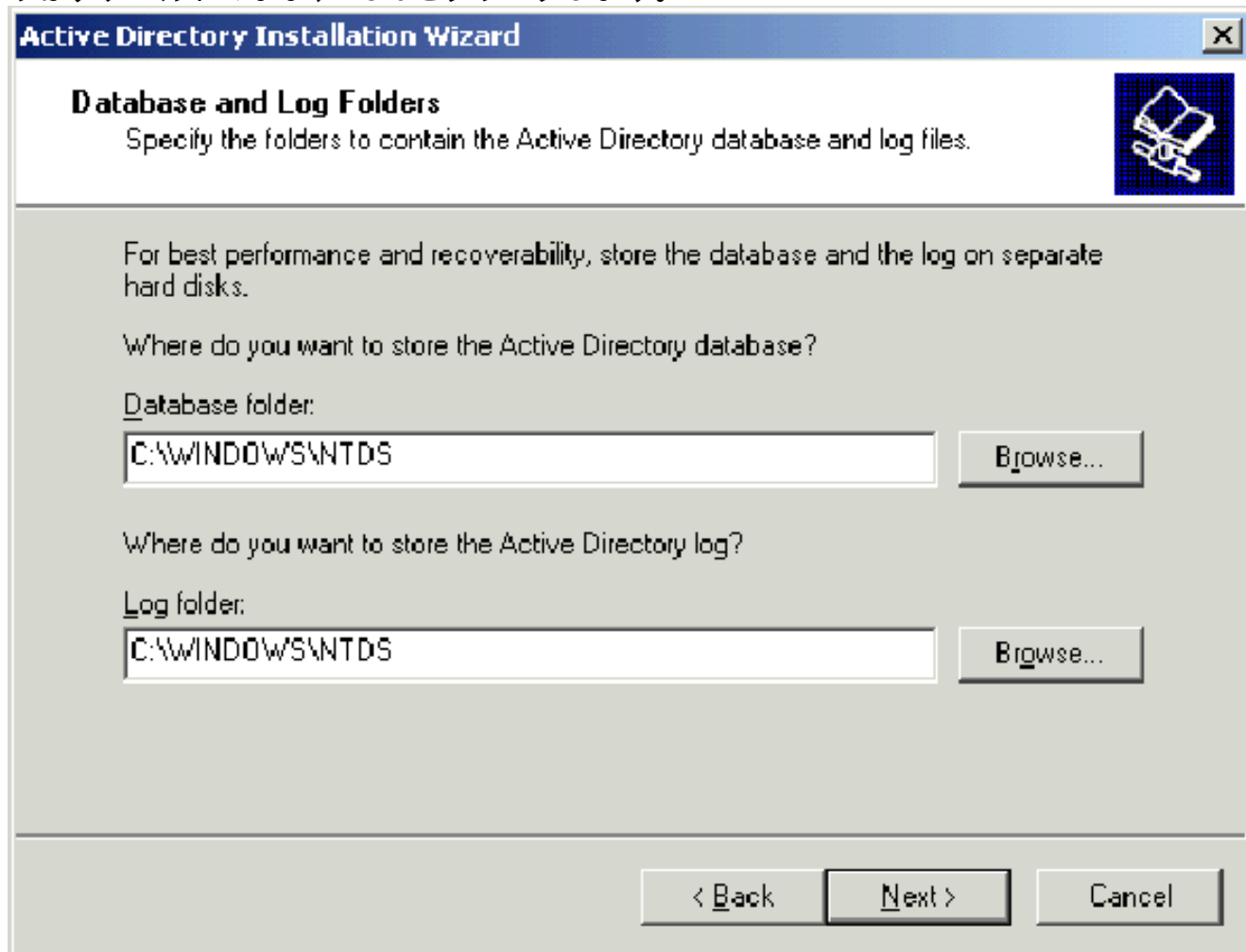
## [ステップ 2：コンピュータをドメイン コントローラとして設定する](#)

次のステップを実行します。

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、

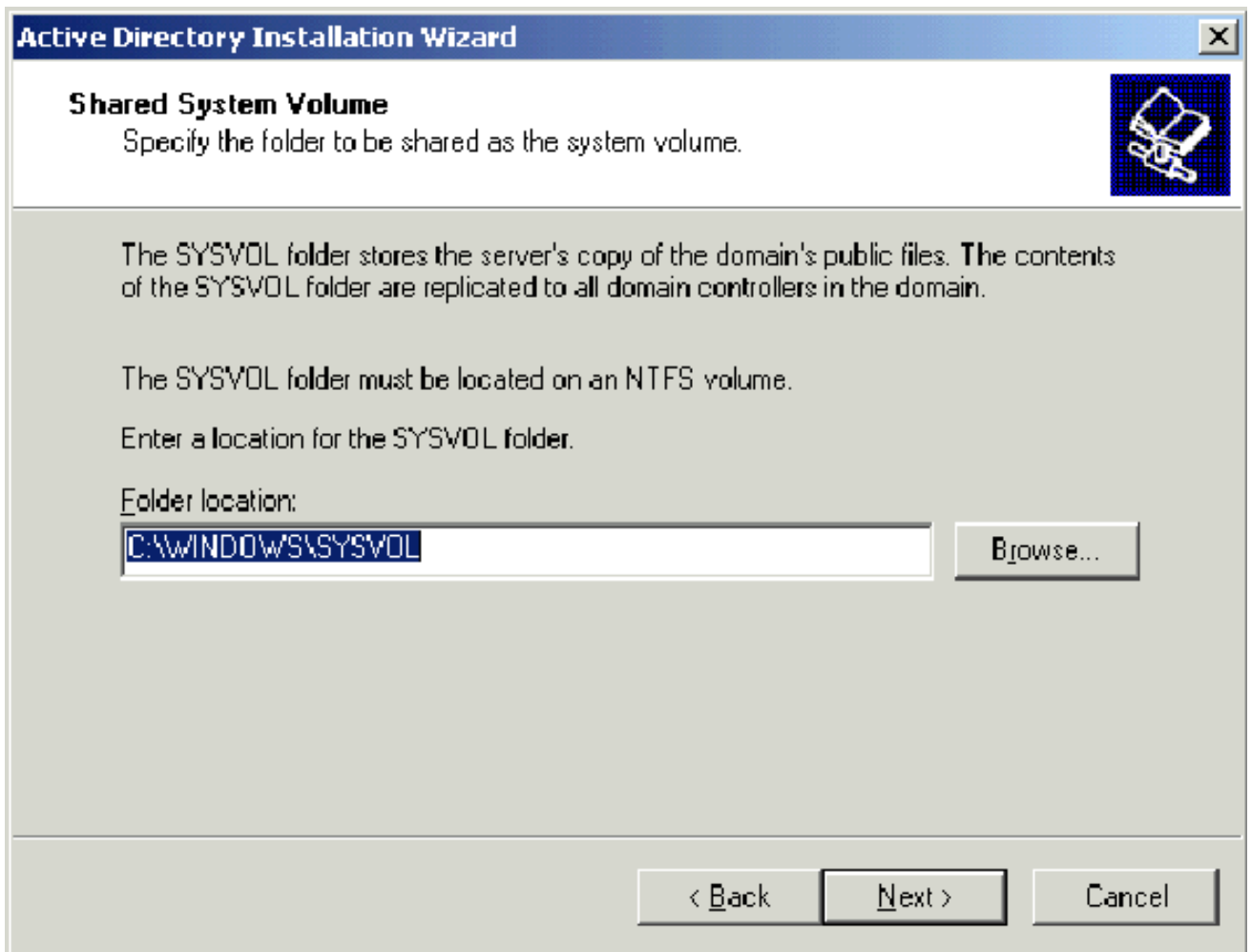
Next をクリックします。

9. Database and Log Folders Location 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。

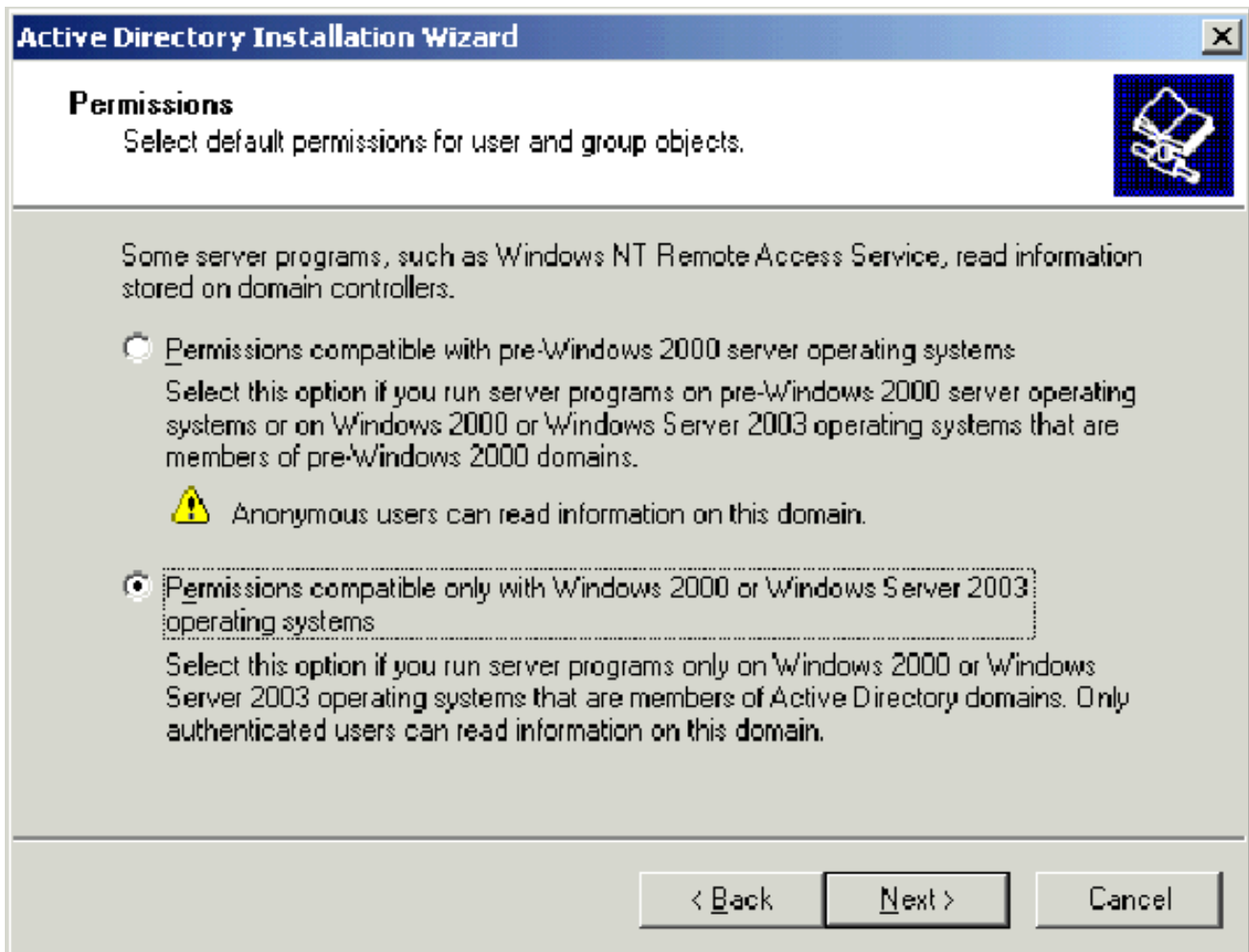


The screenshot shows a window titled "Active Directory Installation Wizard" with a close button in the top right corner. The main heading is "Database and Log Folders" with a sub-instruction: "Specify the folders to contain the Active Directory database and log files." To the right of this heading is a blue icon of a folder with a document. Below the heading, there is a note: "For best performance and recoverability, store the database and the log on separate hard disks." The main question is "Where do you want to store the Active Directory database?". Underneath, it says "Database folder:" followed by a text input field containing "C:\WINDOWS\NTDS" and a "Browse..." button. The next question is "Where do you want to store the Active Directory log?". Underneath, it says "Log folder:" followed by a text input field containing "C:\WINDOWS\NTDS" and a "Browse..." button. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

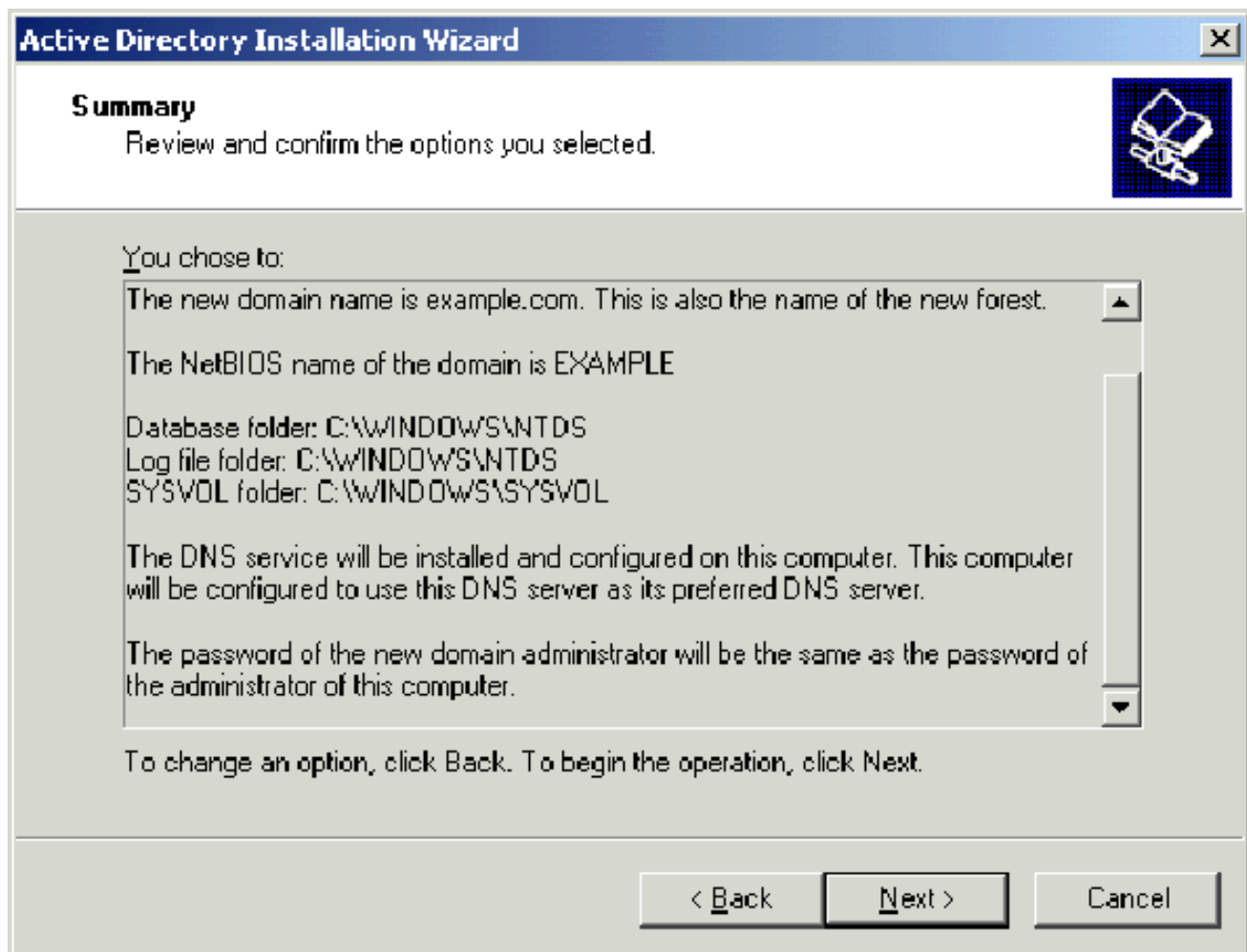
10. Shared System Volume ダイアログボックスで、デフォルトのフォルダ場所が正しいことを確認して、Next をクリックします。



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。



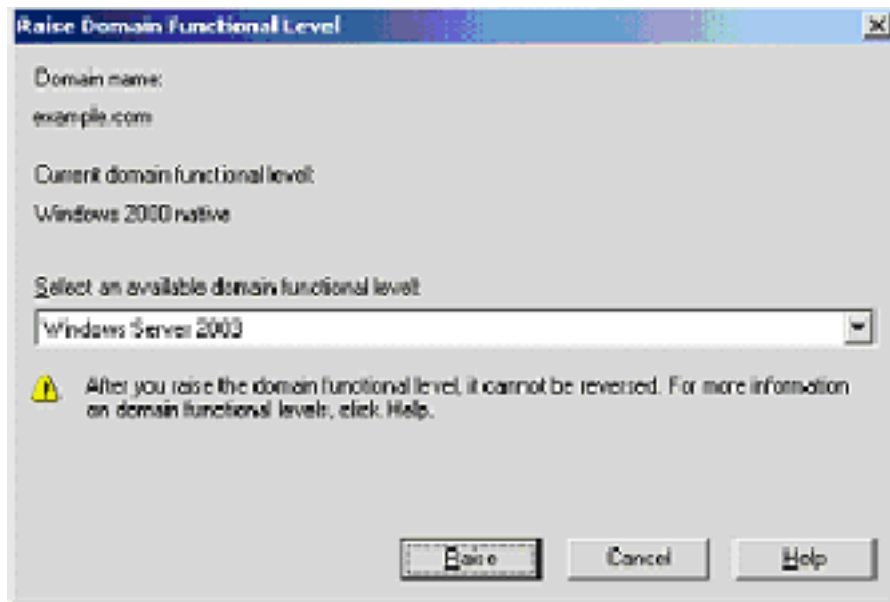
14. Completing the Active Directory Installation Wizard ページで、Finish をクリックします。
15. コンピュータの再起動を指示するプロンプトが表示されたら、[Restart Now] をクリックします。

### ステップ 3: ドメインの機能レベルを上げる

次のステップを実行します。

1. **Administrative Tools** フォルダから Active Directory Domains and Trusts スナップインを開き ( [スタート] > [管理ツール] > [Active Directory Domains and Trusts] )、ドメインコンピュータ DC\_CA.wirelessdemo.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。

#### ステップ 4 : DHCP をインストールして設定する

次のステップを実行します。

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ます ([Start] > [Programs] > [Administrative Tools] > [DHCP])。次に、DHCP サーバ DC\_CA.wirelessdemo.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 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。

## 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:

< Back

Next >

Cancel

7. [Next] をクリックし、次のようにパラメータを入力します。開始IPアドレス : 172.16.100.1[End IP address]:172.16.100.254長さ : 24サブネットマスク : 255.255.255.0

## 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:

End IP address:

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:

Subnet mask:

< Back

Next >

Cancel

- 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の範囲のIPアドレスが予約されます。これらの予約IPアドレスはDHCPサーバによって割り当てられることはありません。

## 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:

Excluded address range:

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。

## New Scope Wizard

### Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

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。

### 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

12. Domain Name and DNS Servers ページで、Parent domain フィールドに wirelessdemo.local、IP address フィールドに 172.16.100.26 と入力し、Add をクリックしてから Next 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:

Resolve

IP address:

172.16.100.26
---------------

Add

Remove

Up

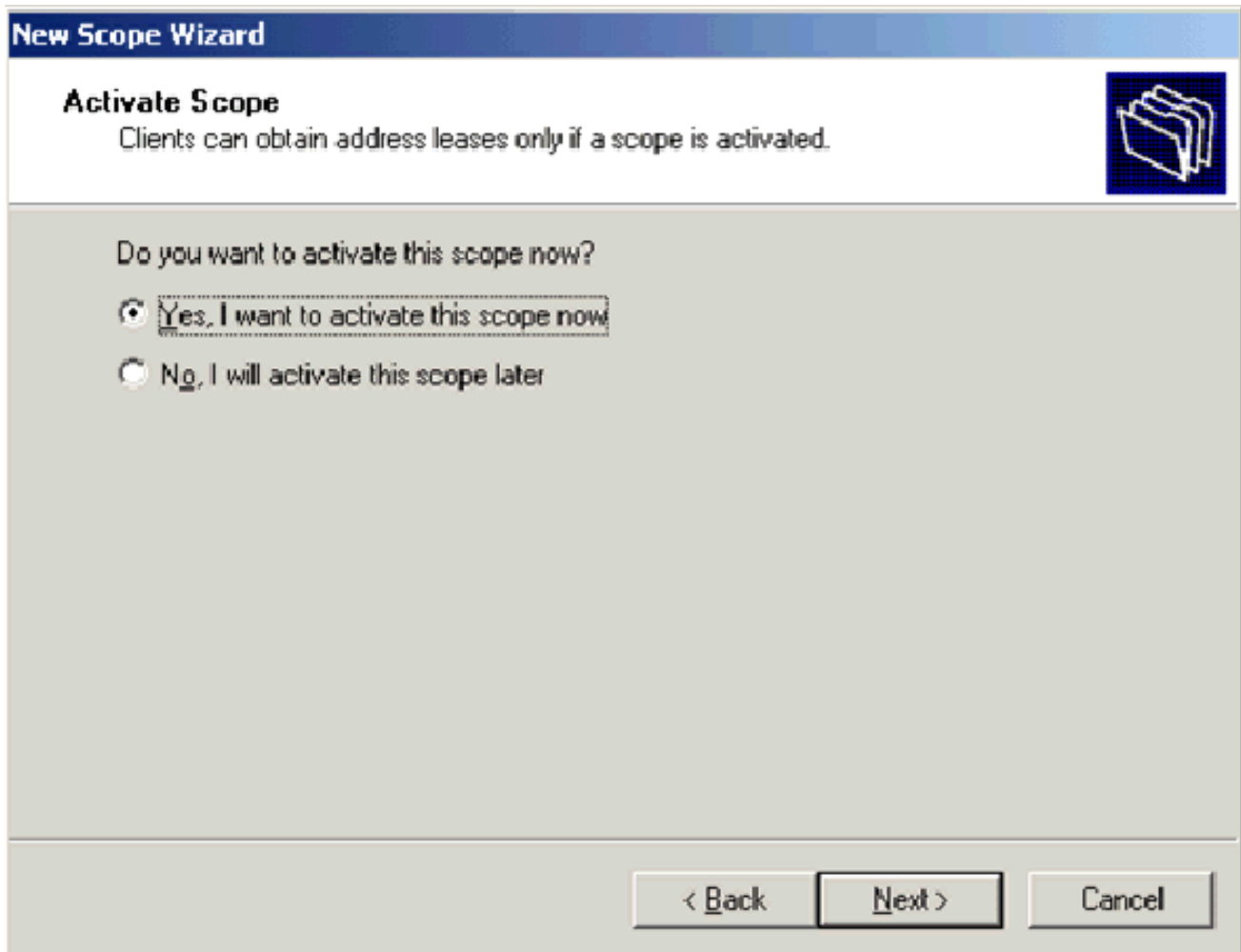
Down

< Back

Next >

Cancel

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. Completing the New Scope Wizard ページで Finish をクリックします。

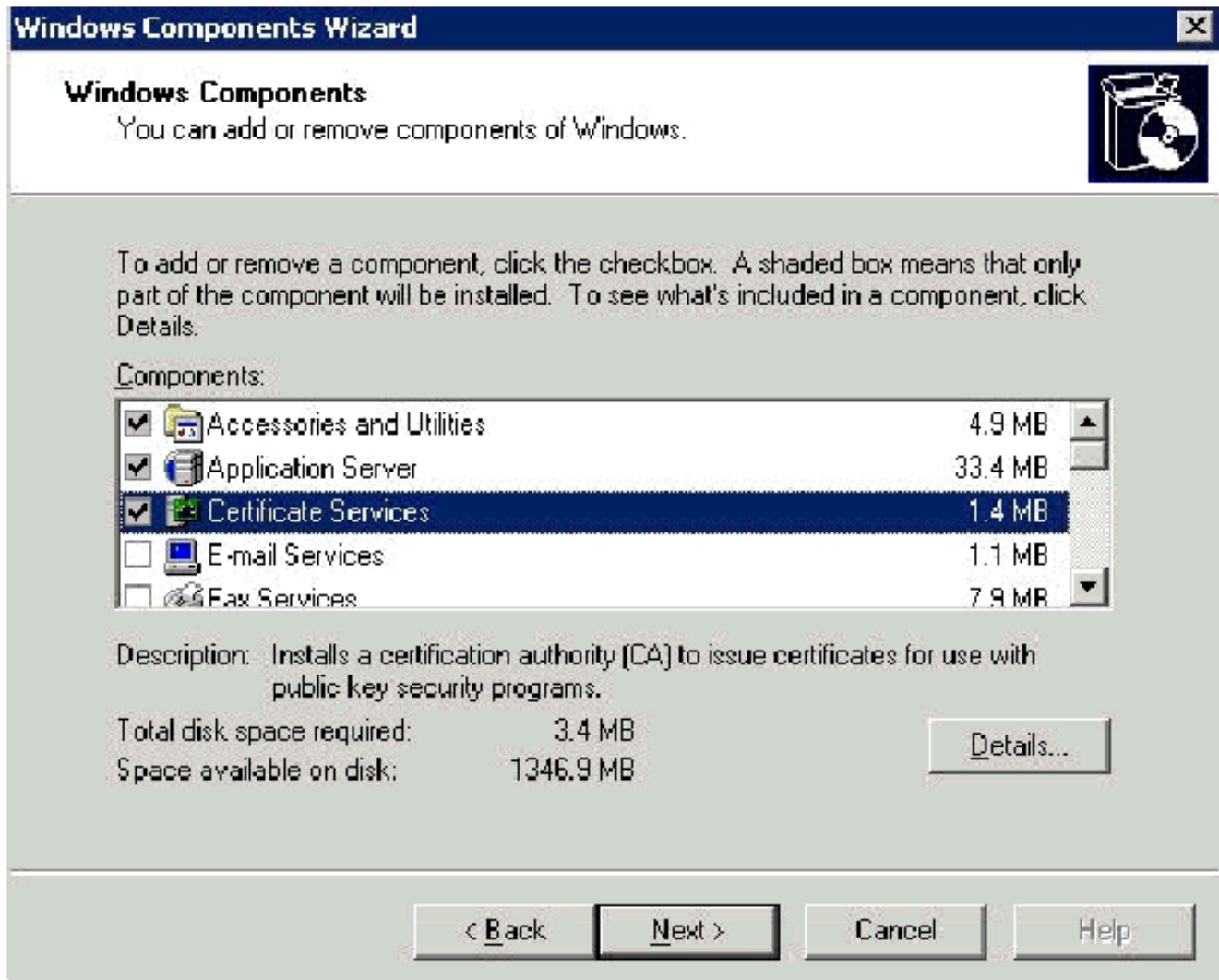
### [ステップ 5 : 証明書サービスをインストールする](#)

次のステップを実行します。

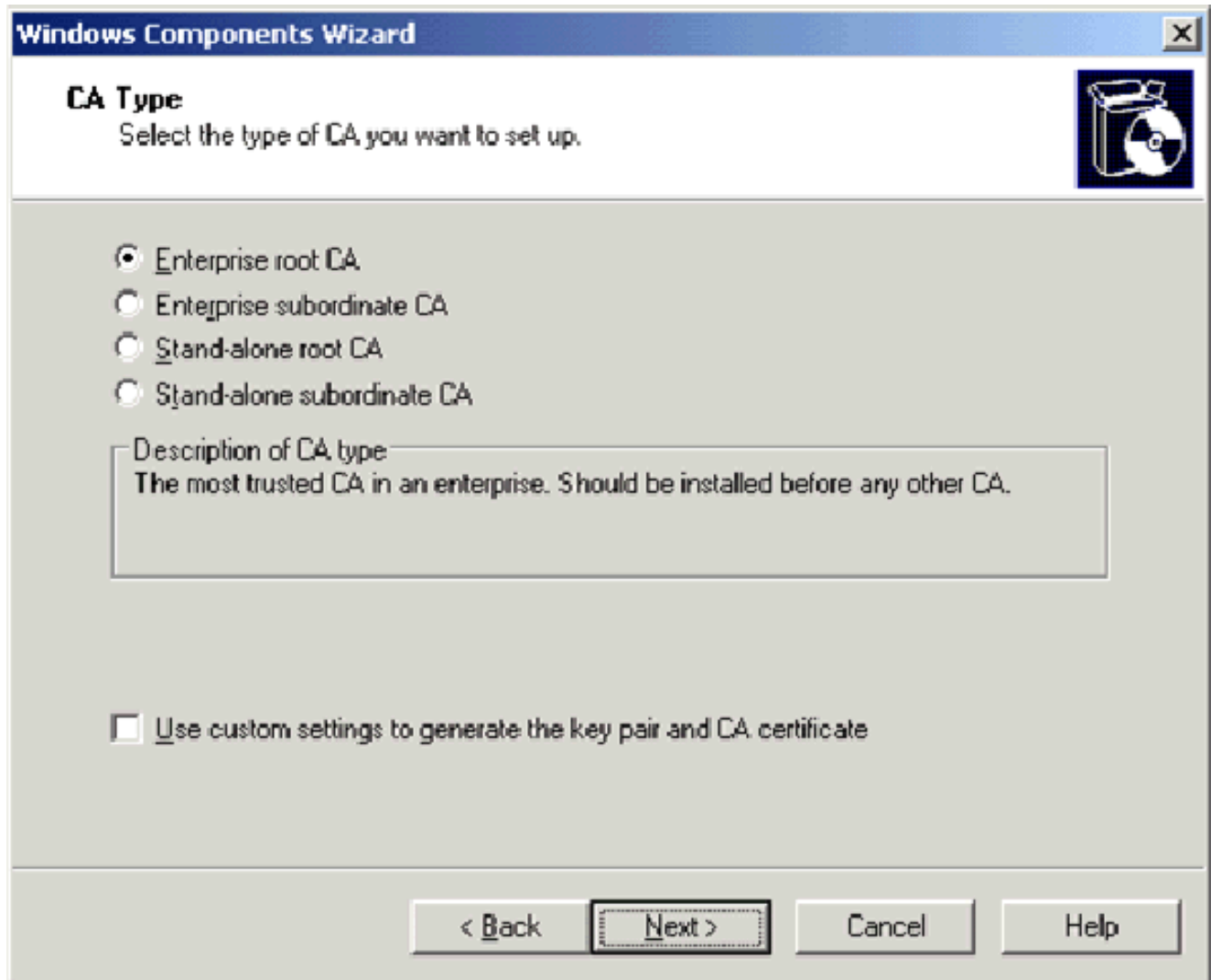
**注 :** 証明書サービスをインストールする前に IIS をインストールする必要があり、ユーザーはエンタープライズ管理者 OU の一部である必要があります。

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。

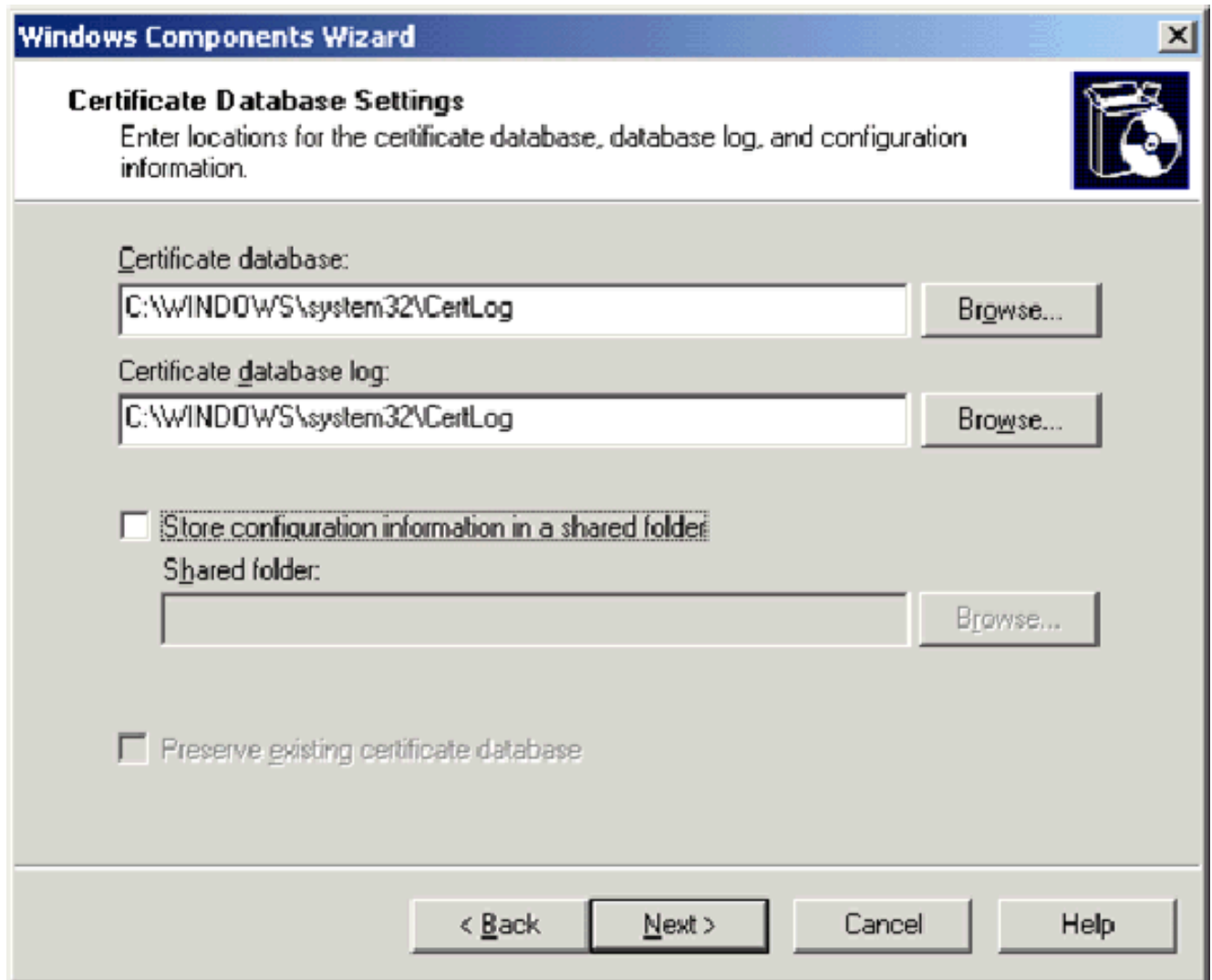




3. [CA Type] ページで [Enterprise root CA] を選択し、[Next] をクリックします。



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。必要に応じてその他の詳細オプションを入力し、Next をクリックします。Certificate Database Settings ページでデフォルトの設定を確認します。

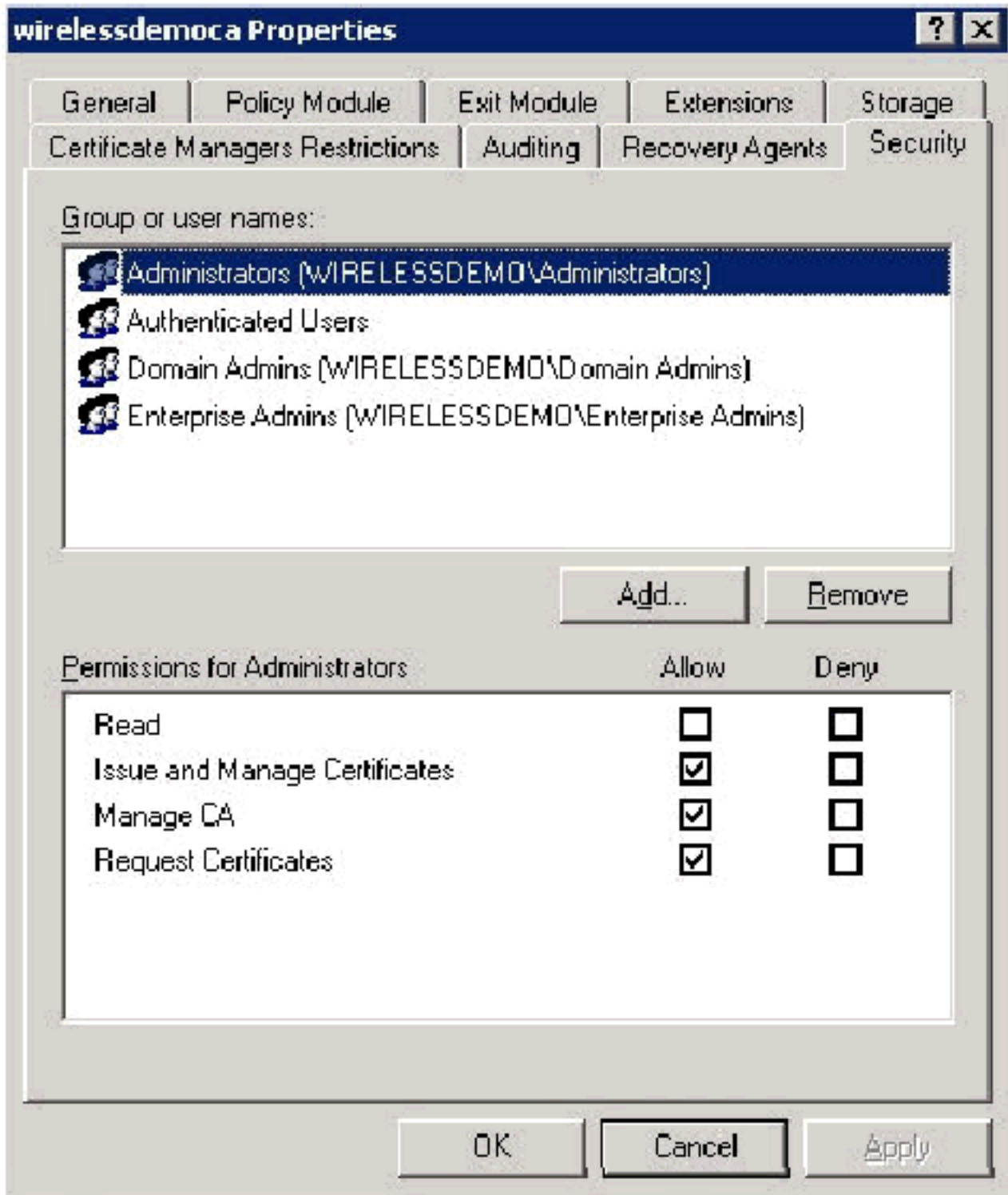


5. [next] をクリックします。インストールが完了したら、[Finish] をクリックします。
6. IIS のインストールに関する警告を読んでから、OK をクリックします。

### 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

次のステップを実行します。

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。

### [手順7: ドメインにコンピュータを追加する](#)

次のステップを実行します。

注: コンピュータが既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。

New Object - Computer

Create in: wirelessdemo.local/Users

Computer name:  
Client

Computer name (pre-Windows 2000):  
CLIENT

The following user or group can join this computer to a domain.

User or group:  
Default: Domain Admins Change...

Assign this computer account as a pre-Windows 2000 computer

Assign this computer account as a backup domain controller

< Back Next > Cancel

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

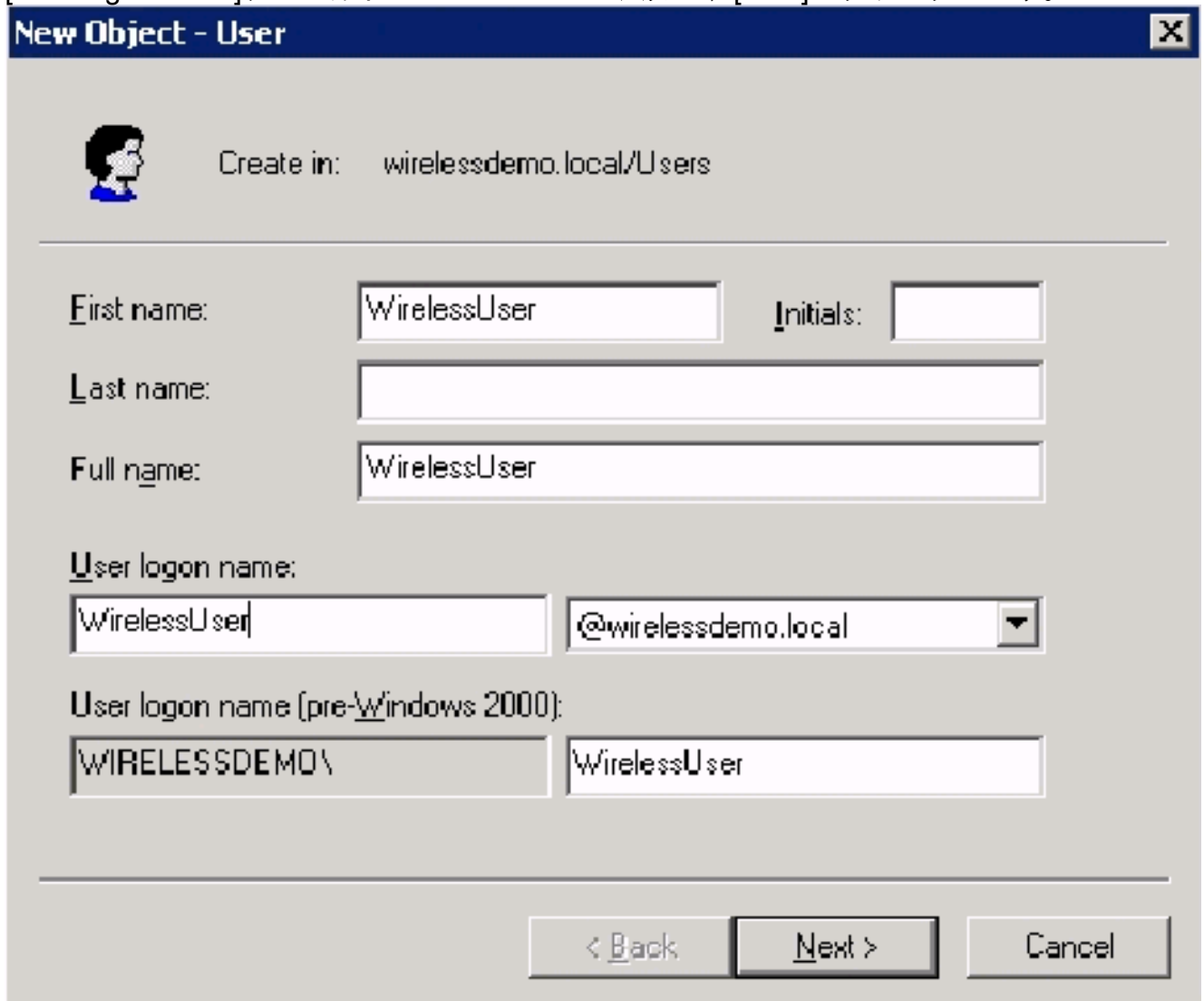
次のステップを実行します。

1. [Active Directory Users and Computers] コンソール ツリーで **[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 **[Client]** というコンピュータを使用する手順を示します。
2. **[Properties]** をクリックし、[Dial-in] タブに移動します。
3. Allow access を選択して OK をクリックします。

### 手順 9: ドメインにユーザを追加する

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] 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の[First name]フィールドにWirelessUserと入力し、[User logon name]フィールドにWirelessUserと入力し、[Next]をクリックします。



**New Object - User**

Create in: wirelessdemo.local/Users

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back    Next >    Cancel

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

Create in: wirelessdemo.local/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。
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。

#### [手順 10 : ユーザに無線アクセスを許可する](#)

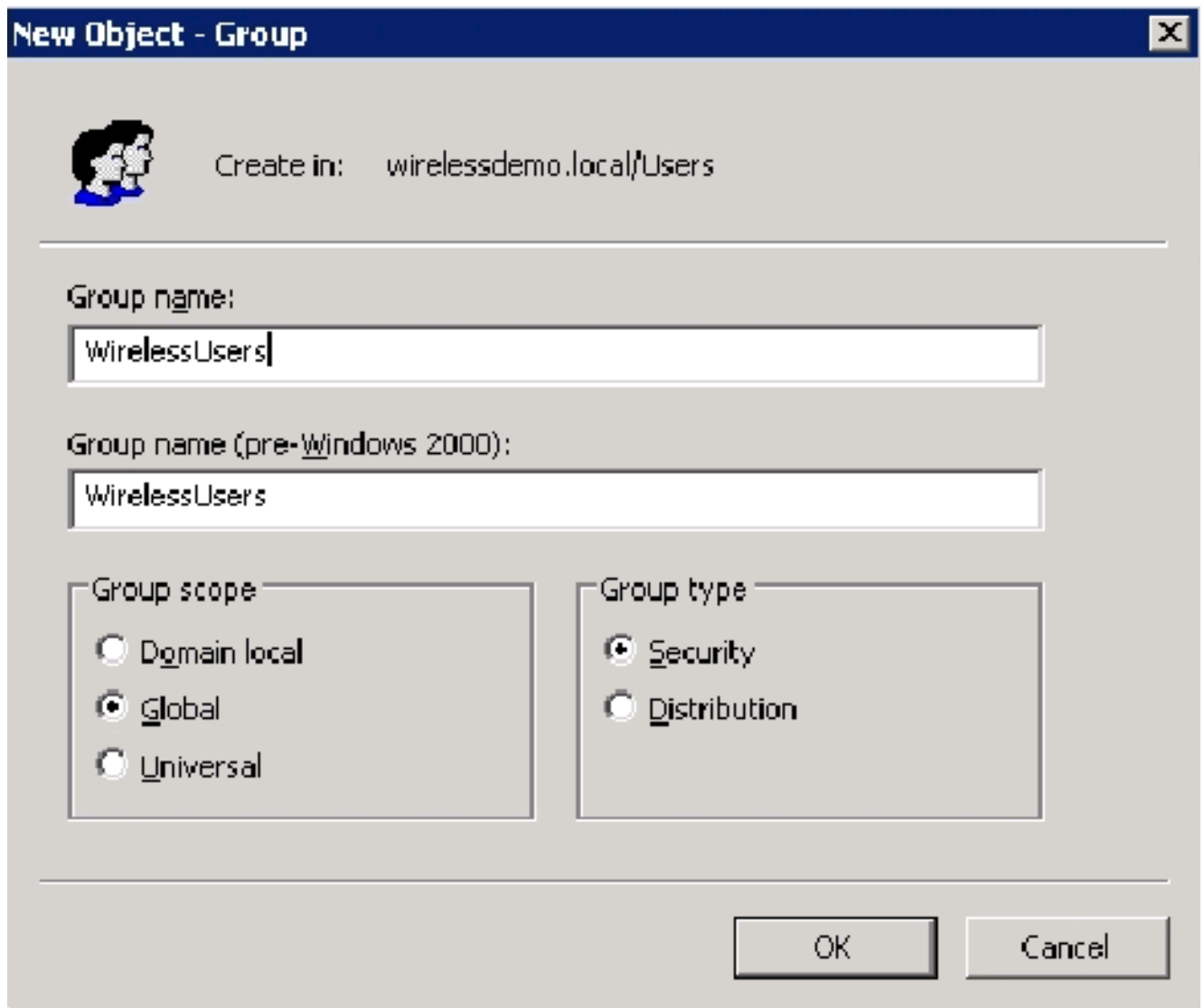
次のステップを実行します。

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] 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。

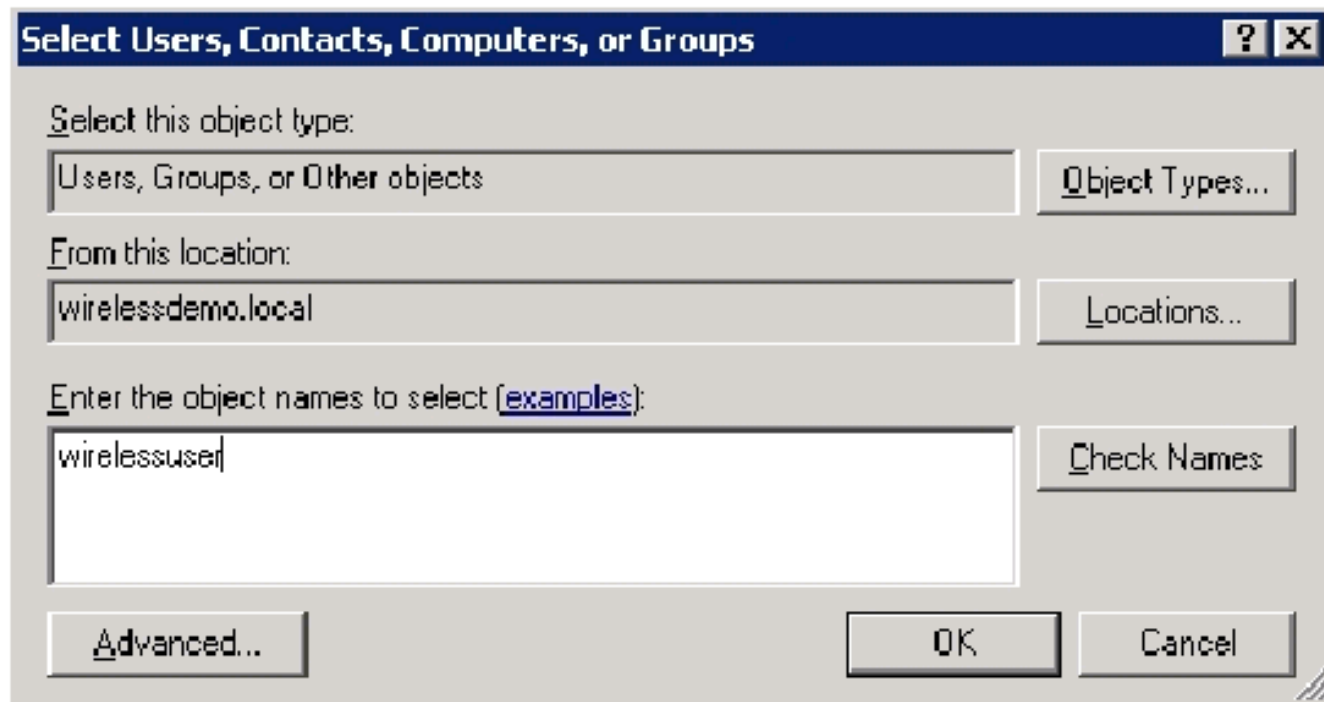


## [ステップ 12 : wirelessusers グループにユーザを追加する](#)

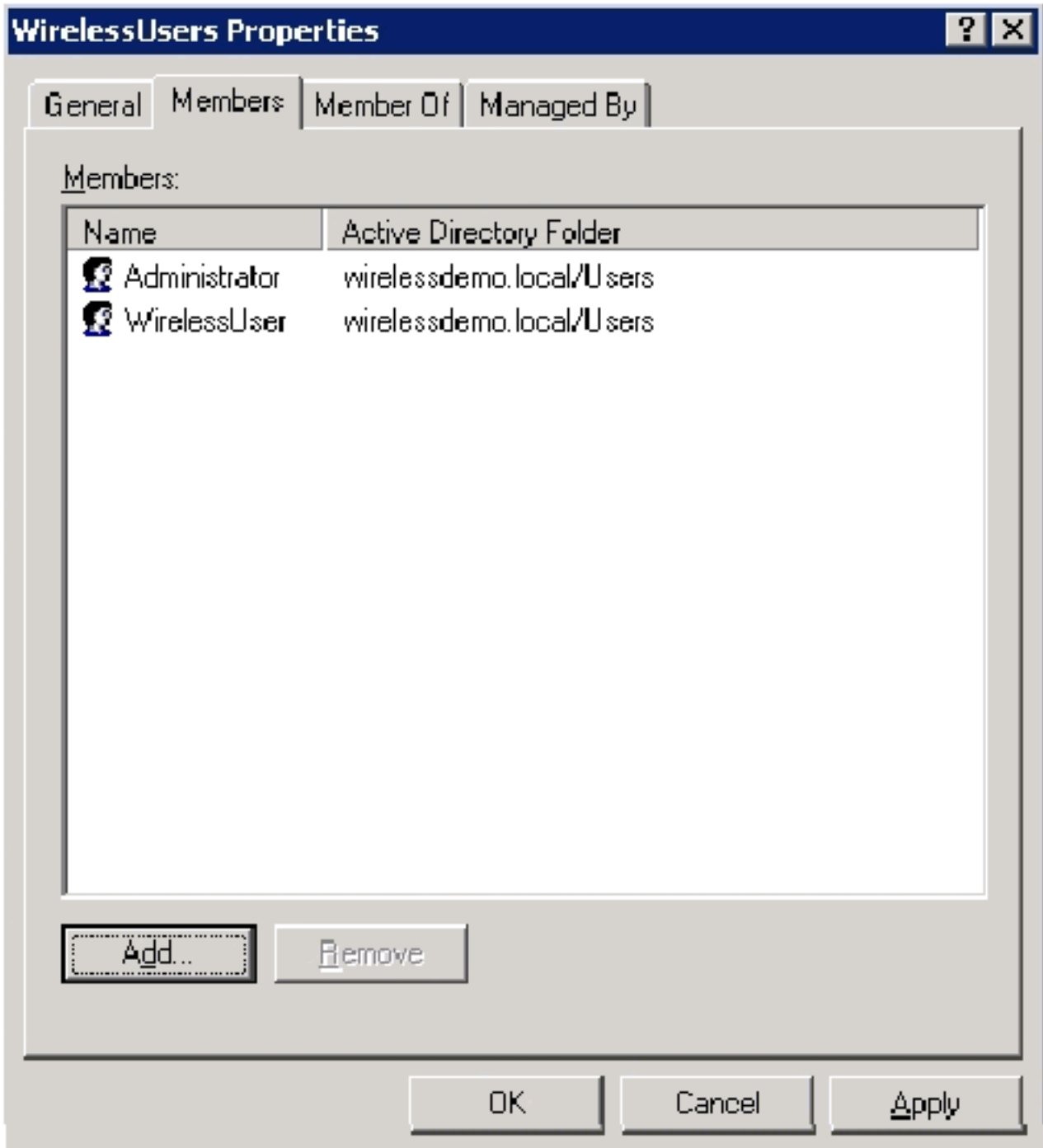
次のステップを実行します。

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。

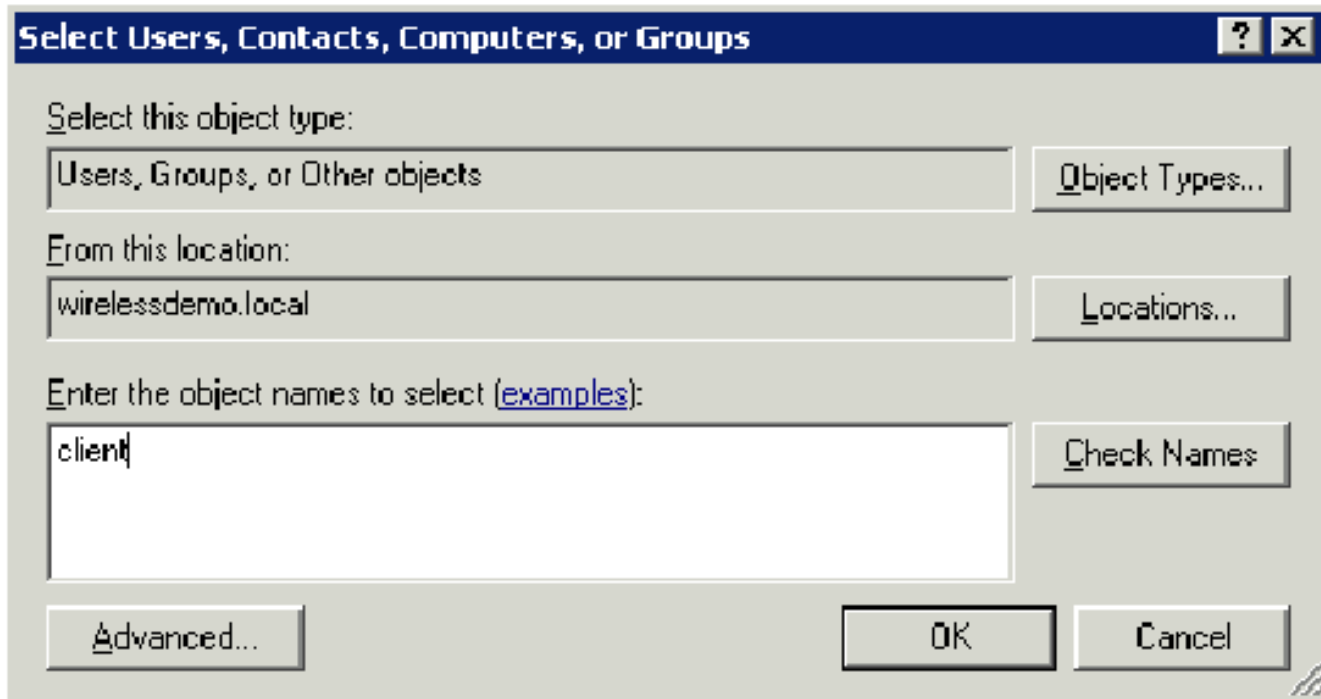


5. [OK] をクリックして、wirelessusers のグループに対する変更を保存します。
6. さらにユーザをグループに追加する場合は、この手順を繰り返します。

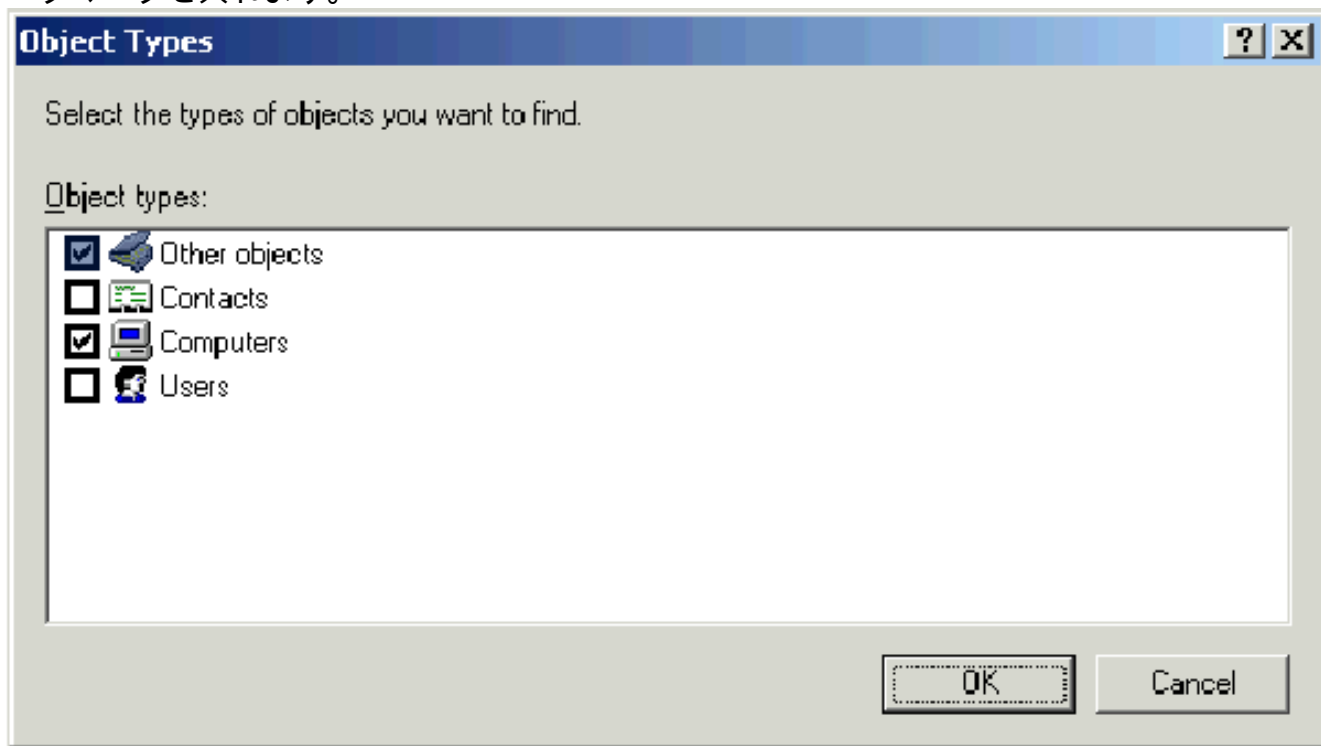
### [ステップ 13 : WirelessUsers グループにクライアント コンピュータを追加する](#)

次のステップを実行します。

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

次のステップを実行します。

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：残りの設定では、ACSサーバ名は 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](#)の設定方法の詳細については、『Cisco Secure ACS 4.0 for Windowsインストールガイド』を参照してください。

次のステップを実行します。

1. Cisco Secure ACS をインストールするには、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ます。注：Cisco Secure ACSをインストールするコンピュータでのみ実行されるインストールがサポートされます。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：コンピュータに必要なサービスパックが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：[開始前]ボックスに表示されているすべての項目を完了していない場合は、[キャンセル]をクリックして、[設定の終了]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：パスにパーセント文字「%」を含むパスは指定しないでください。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。注記：存在しないフォルダを指定した場合、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をインストールした後、Windows ユーザ データベースに加えて、すべての外部ユーザデータベースタイプの認証サポートを設定できます。
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] 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によって制御されるすべての形式のアクセスに適用されます。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：上記の機能は、Cisco Secure ACS HTML インターフェイスで有効にした場合にのみ表示されます。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、[システムの設定(System Configuration)]セクションの[アクティブサービス管理(Active Service Management)]ページでアクティブサービス監視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。是正措置なし: Cisco Secure ACSはスクリプトを実行しません。注：このオプションは、イベントメール通知を有効にする場合に便利です。リポート: Cisco Secure ACSは、Cisco Secure ACSを実行するコンピュータをリポートするスクリプトを実行します。Restart All: Cisco Secure ACSはすべてのCisco Secure ACSサービスを再起動します。RADIUS/TACACS+の再起動: Cisco Secure ACSは、RADIUSおよびTACACS+サービスのみを再起動します。
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、ACS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ある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。[next] をクリックします。
27. 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。
28. 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。はい、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Web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のメモ帳でREADME.TXTファイルを開きます。
29. [next] をクリックします。
30. 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。
31. [Finish] をクリックします。注：設定の残りの部分は、設定されているEAPタイプのセクションに記載されています。

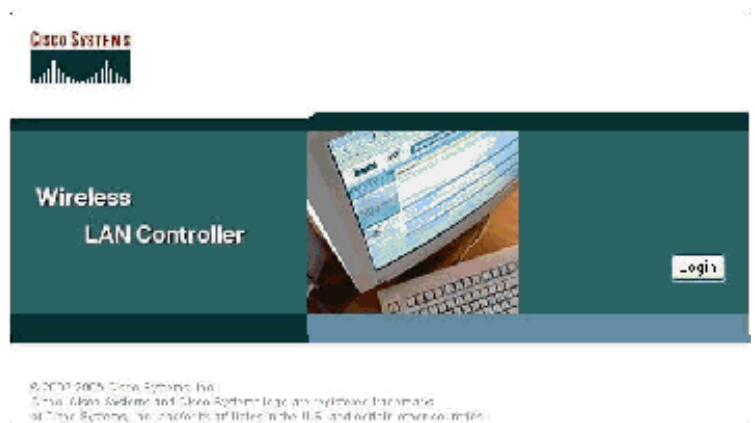
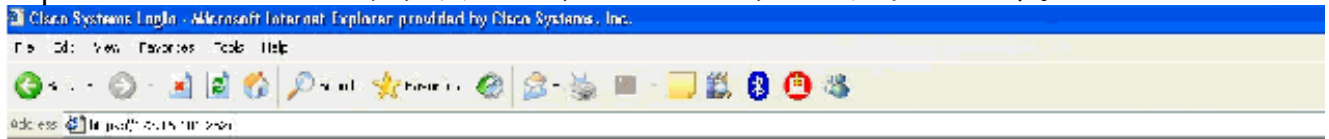
## Cisco LWAPP コントローラの設定

### WPA2/WPA に必要な設定の作成

次のステップを実行します。

注：コントローラがネットワークに基本的に接続しており、管理インターフェイスへのIP到達可能性が成功していることを前提としています。

1. <https://172.16.101.252> をブラウザして、コントローラにログインします。



2. [Login] をクリックする。
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、インターフェイスと VLAN のマッピングを作成します。
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、ネットワークで伝送される任意の VLAN を指定できます）。
9. [Apply] をクリックします。
10. 次の [Interfaces > Edit] ウィンドウが表示されるように、情報を設定します。

Back Search Favorites

Address: https://172.16.101.252/screens/frameset.html

CISCO SYSTEMS

MONITOR WLANs CONTROLLER WIRELESS SECURITY

Controller

General

Inventory

Interfaces

Internal DHCP Server

Mobility Management

Mobility Groups

Mobility Statistics

Ports

Master Controller Mode

Network Time Protocol

QoS Profiles

Interfaces > Edit

General Information

Interface Name employee

Interface Address

VLAN Identifier 20

IP Address 172.16.100.1

Netmask 255.255.255.0

Gateway 172.16.100.1

Physical Information

Port Number 1

DHCP Information

Primary DHCP Server 172.16.100.25

Secondary DHCP Server 0.0.0.0

Access Control List

ACL Name none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

11. [Apply] をクリックします。
12. WLAN をクリックします。
13. [New] をクリックします。
14. WLAN SSID フィールドに、Employee と入力します。
15. [Apply] をクリックします。
16. 次の[WLANs > Edit]ウィンドウが表示されるように、情報を設定します。注：この実習では、WPA2がレイヤ2暗号化方式として選択されています。この SSID に関連付ける TKIP-MIC クライアントで WPA を使用するには、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 のボックスにチェックマークを入れます。



## WLAN6 > Edit

WLAN ID	1
WLAN SSID	Employee

### General Policies

Radio Policy	All
Admin Status	<input checked="" type="checkbox"/> Enabled
Session Timeout (secs)	1800
Quality of Services (QoS)	Silver (best effort)
WMM Policy	Disabled
7920 Pkts Support	<input type="checkbox"/> Client CAC Limit <input type="checkbox"/> AP CAC Limit
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
Allow PPP Override	<input type="checkbox"/> Enabled
Client Exclusion	<input checked="" type="checkbox"/> Enabled ** 60 Timeout Value (secs)
DHCP Server	<input type="checkbox"/> Override
DHCP Addr. Assignment	<input checked="" type="checkbox"/> Required
Interface Name	employee

### Security Policies

Layer 2 Security	WPA2
	<input type="checkbox"/> MAC Filtering
Layer 3 Security	None
	<input type="checkbox"/> Web Policy **

\* Web Policy cannot be used in combination with IPsec and L2TP.

\*\* When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)

### Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:172.16.100.25, Port:1812	none
Server 2	none	none
Server 3	none	none

### WPA2 Parameters

WPA Compatibility Mode	<input checked="" type="checkbox"/> Enable
Allow WPA2 TKIP Clients	<input checked="" type="checkbox"/> Enable
Pre-Shared Key	<input type="checkbox"/> Enabled (WPA2 passphrase has been set)

- [Apply] をクリックします。
- [Security] メニューをクリックし、RADIUS サーバを追加します。
- [New] をクリックします。
- 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。
- 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。
- [Apply] をクリックします。



## Security

### AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

### Access Control Lists

### Web Auth Certificate

### Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

## RADIUS Authentication Servers > New

<b>Server Index (Priority)</b>	1 <input type="button" value="v"/>
<b>Server IP Address</b>	<input type="text" value="172.16.100.25"/>
<b>Keys Format</b>	ASCII <input type="button" value="v"/>
<b>Shared Secret</b>	<input type="password" value="••••••"/>
<b>Confirm Shared Secret</b>	<input type="password" value="••••••"/>
<b>Key Wrap</b>	<input type="checkbox"/>
<b>Port Number</b>	<input type="text" value="1812"/>
<b>Server Status</b>	Enabled <input type="button" value="v"/>
<b>Support for RFC 3576</b>	Enabled <input type="button" value="v"/>
<b>Retransmit Timeout</b>	<input type="text" value="2"/> seconds
<b>Network User</b>	<input checked="" type="checkbox"/> Enable
<b>Management</b>	<input type="checkbox"/> Enable

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser title is "CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc." and the address bar shows "http://172.16.100.25:3052/index2.htm". The page title is "Network Configuration" and the sub-page is "AAA Client Setup For DEMO\_2006\_1". The sidebar on the left contains various configuration options: User Setup, Interface Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Profile Validation, Network Access Profiles, and Favorites and... The main content area has the following fields and options:

- AAA Client IP Address: 173.16.101.253
- Key: shared secret
- Authentication Using: RADIUS (Cisco Aires-GT)
- Single Connect TACACS+ AAA Client (Record step in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

23. これで基本設定が完了し、EAP-TLS のテストが実行できるようになりました。

## EAP-TLS 認証

EAP-TLS 認証を利用するには、コンピュータ証明書とユーザ証明書を無線クライアント上に配置し、無線アクセス用のリモートアクセスポリシーに EAP タイプとして EAP-TLS を追加して、無線ネットワーク接続を再設定する必要があります。

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。

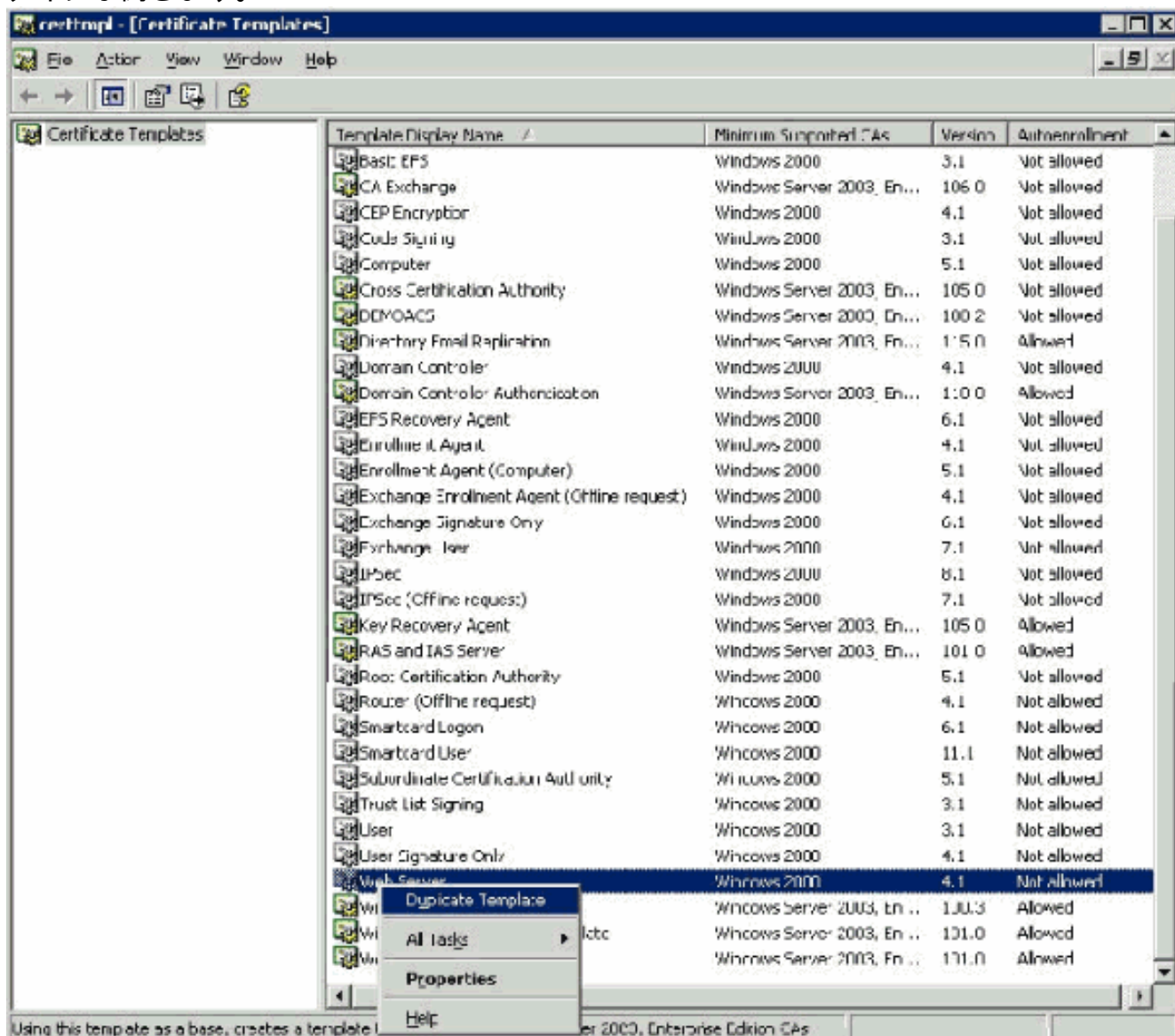
注：Microsoftは、Windows 2003 Enterprise CAのリリースでWeb Serverテンプレートを変更したため、キーがエクスポートできなくなり、オプションがグレー表示されます。サーバ認証に使用でき、ドロップダウンで使用できるキーをエクスポート可能にマークできる機能を備えた証明書サービスでは、これ以外の証明書テンプレートは提供されていないため、これを実行する新しいテンプレートを作成する必要があります。

注：Windows 2000ではエクスポート可能なキーを使用できます。Windows 2000を使用する場合は、これらの手順に従う必要はありません。

## 証明書テンプレート スナップインのインストール

次のステップを実行します。

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

次のステップを実行します。

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。

**Properties of New Template** [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Subject Name

Template display name:

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:

Validity period:  years

Renewal period:  weeks

Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply

3. Template display name フィールドに、ACS と入力します。

**Properties of New Template** [?] [X]

Issuance Requirements | Superseded Templates | Extensions | Security

General | **Request Handling** | Subject Name

Template display name:  
[ACS]

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name:  
[ACS]

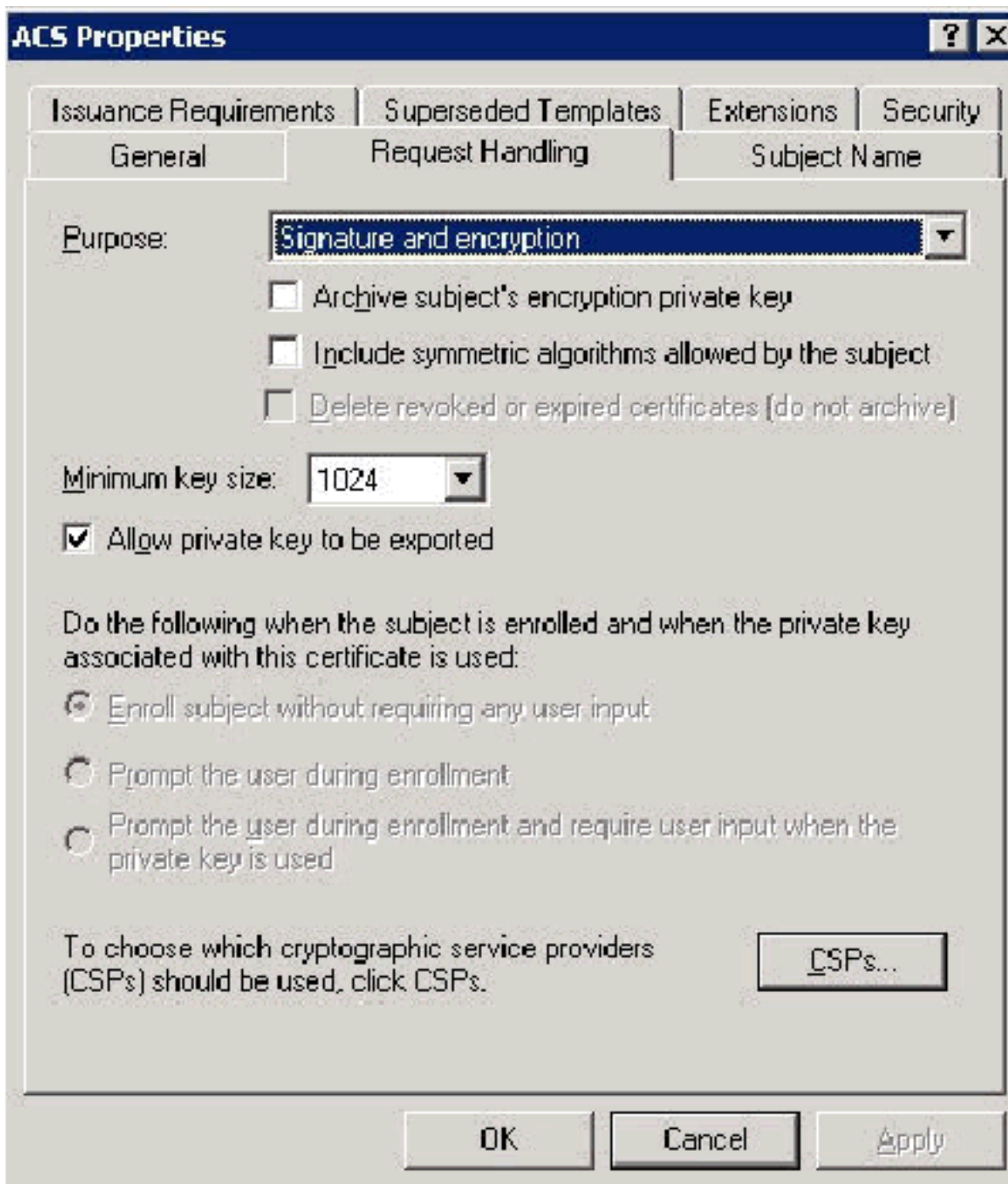
Validity period: [ 2 ] [ years ] [ v ]      Renewal period: [ 6 ] [ weeks ] [ v ]

Publish certificate in Active Directory

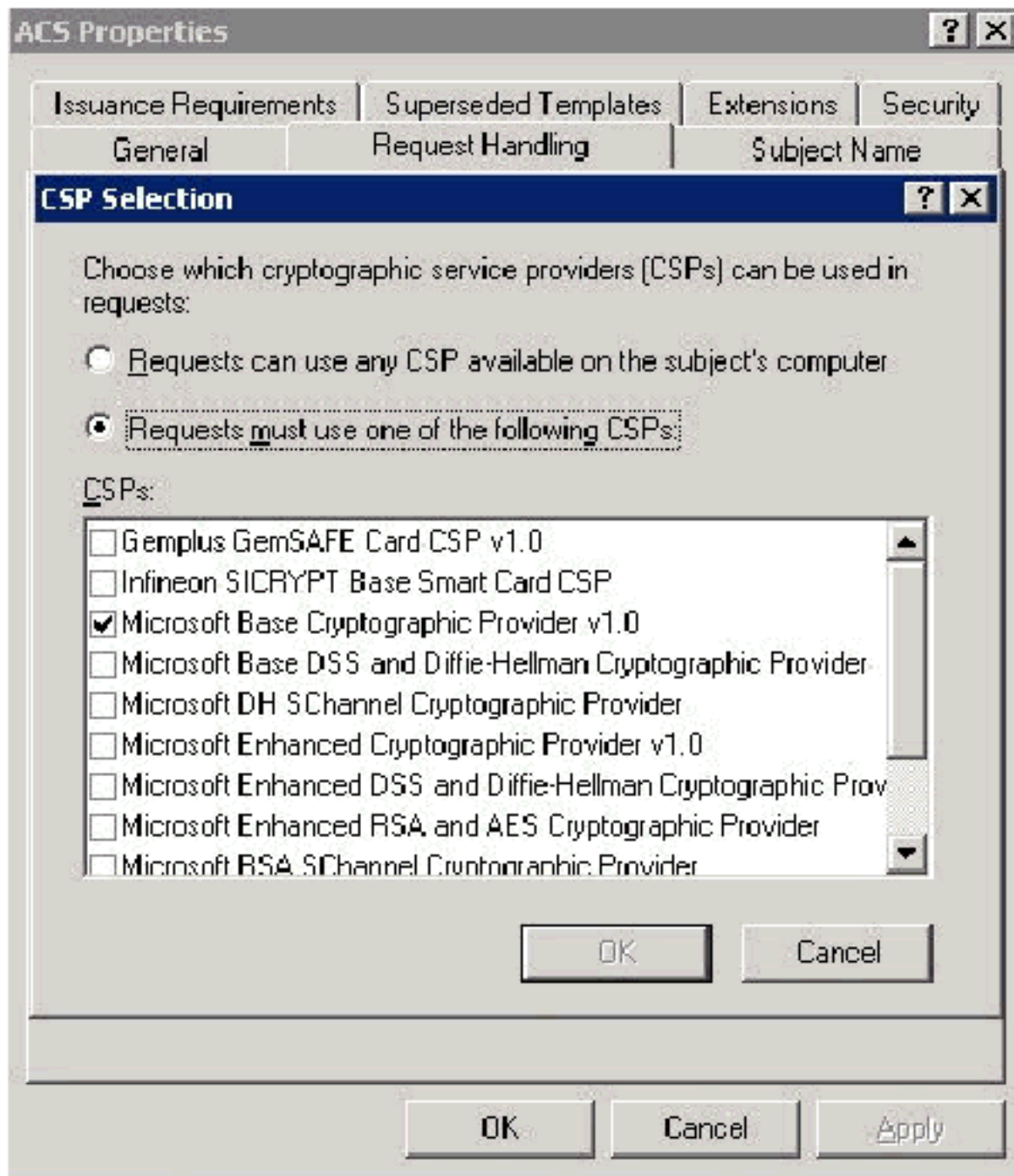
Do not automatically reenroll if a duplicate certificate exists in Active Directory

[ OK ] [ Cancel ] [ Apply ]

4. [Request Handling] タブに移動し、[Allow private key to be exported] にチェックを入れます

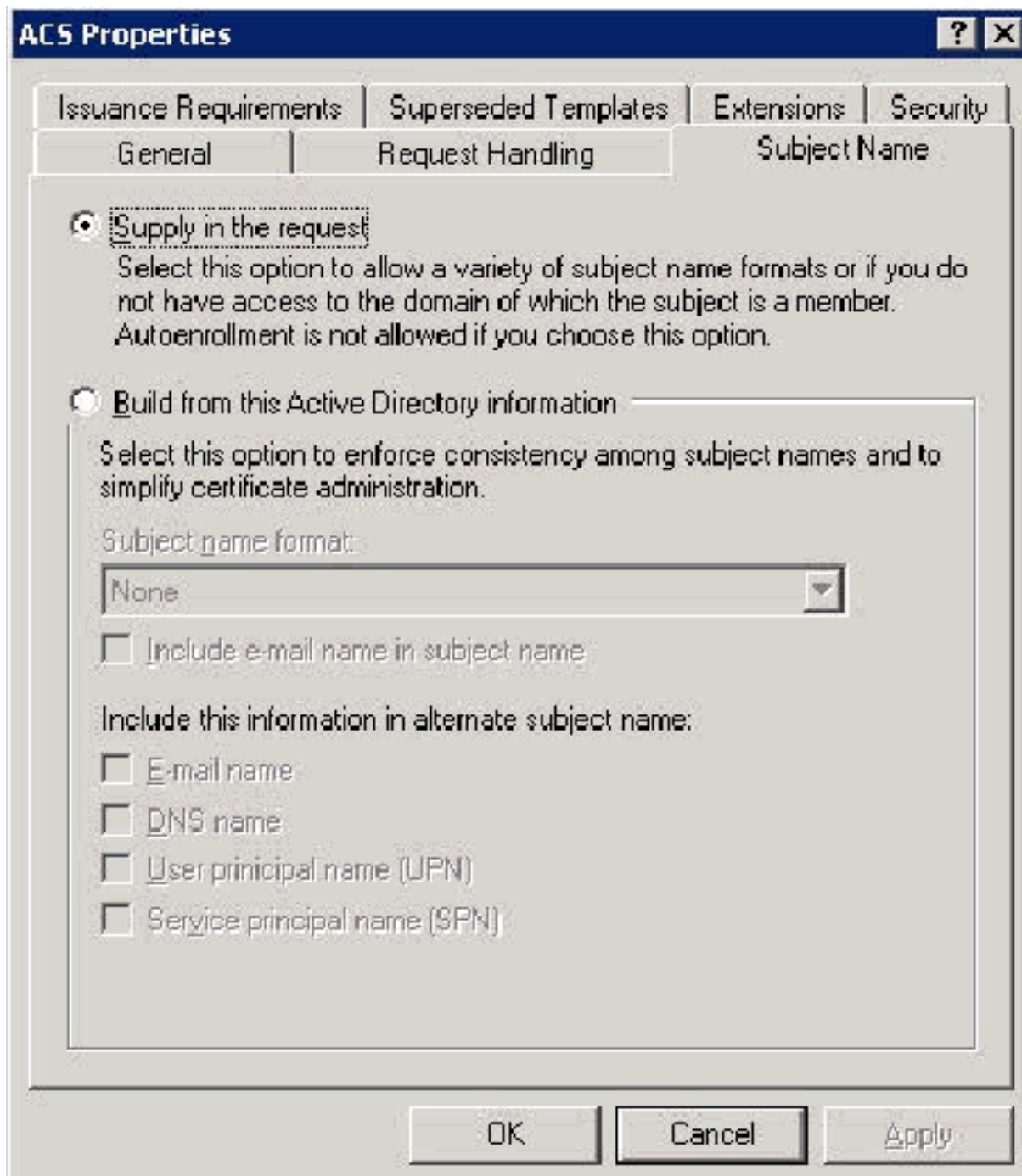


5. [Requests must use one the following CSPs]を選択し、[Microsoft Base Cryptographic Provider v1.0]をオンにします。オンになっている他のCSPのチェックマークを外して、[OK]をクリックします。

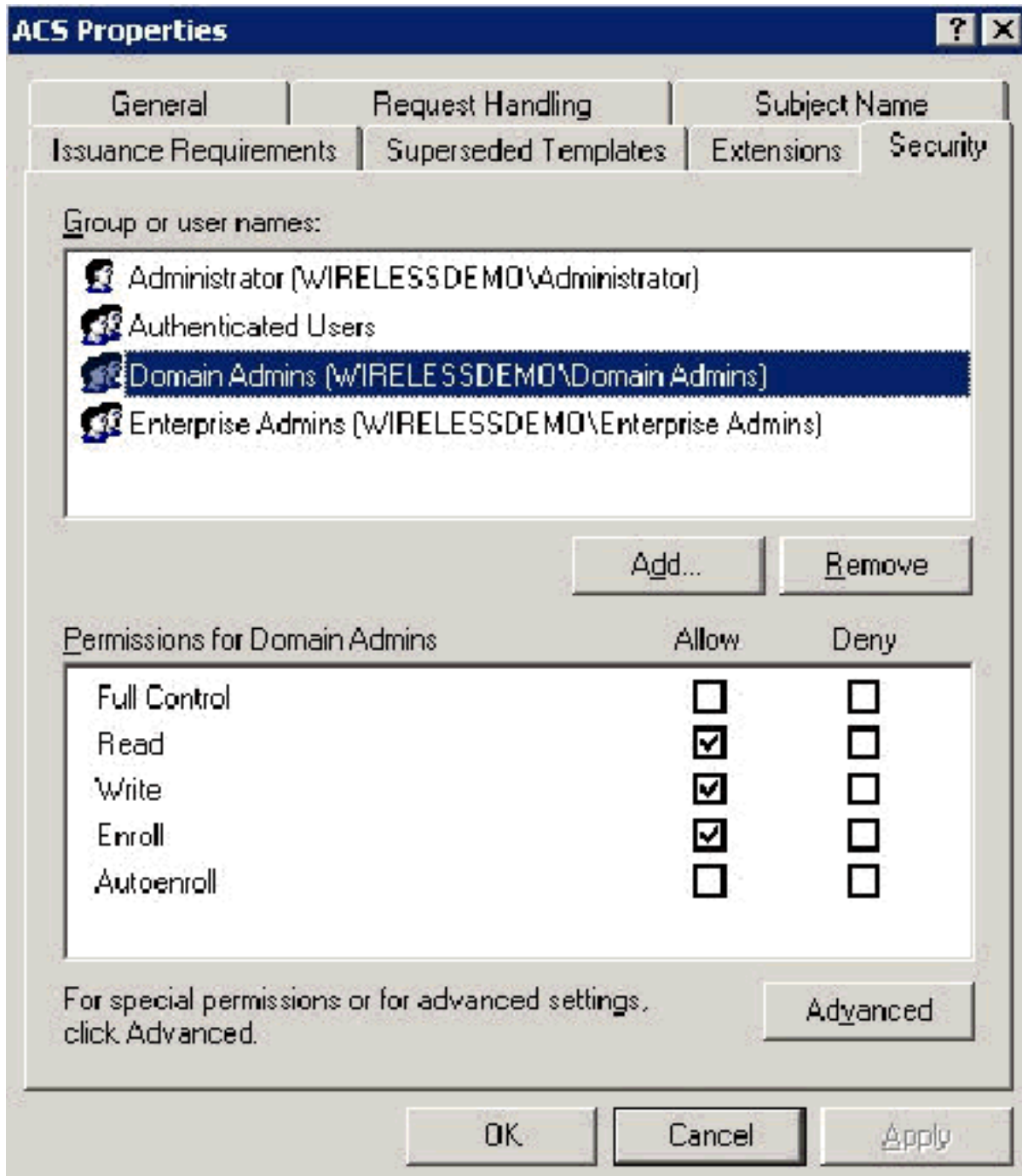


6. Subject Name タブに移動し、Supply in the request を選択して OK をクリックします。





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**：このActive Directory情報のみから構築する場合は、[User principal name (UPN)]にチェックマークを付け、Active Directory Users and ComputersスナップインのWirelessUserアカウントに電子メール名が入力されていないため、[Include email name and E-mail name]のこのチェックを外にします。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。

**ACS Properties** [?] [X]

General | Request Handling | Subject Name

Issuance Requirements | Superseded Templates | Extensions | Security

Require the following for enrollment:

CA certificate manager approval

This number of authorized signatures:

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Require the following for reenrollment:

Same criteria as for enrollment

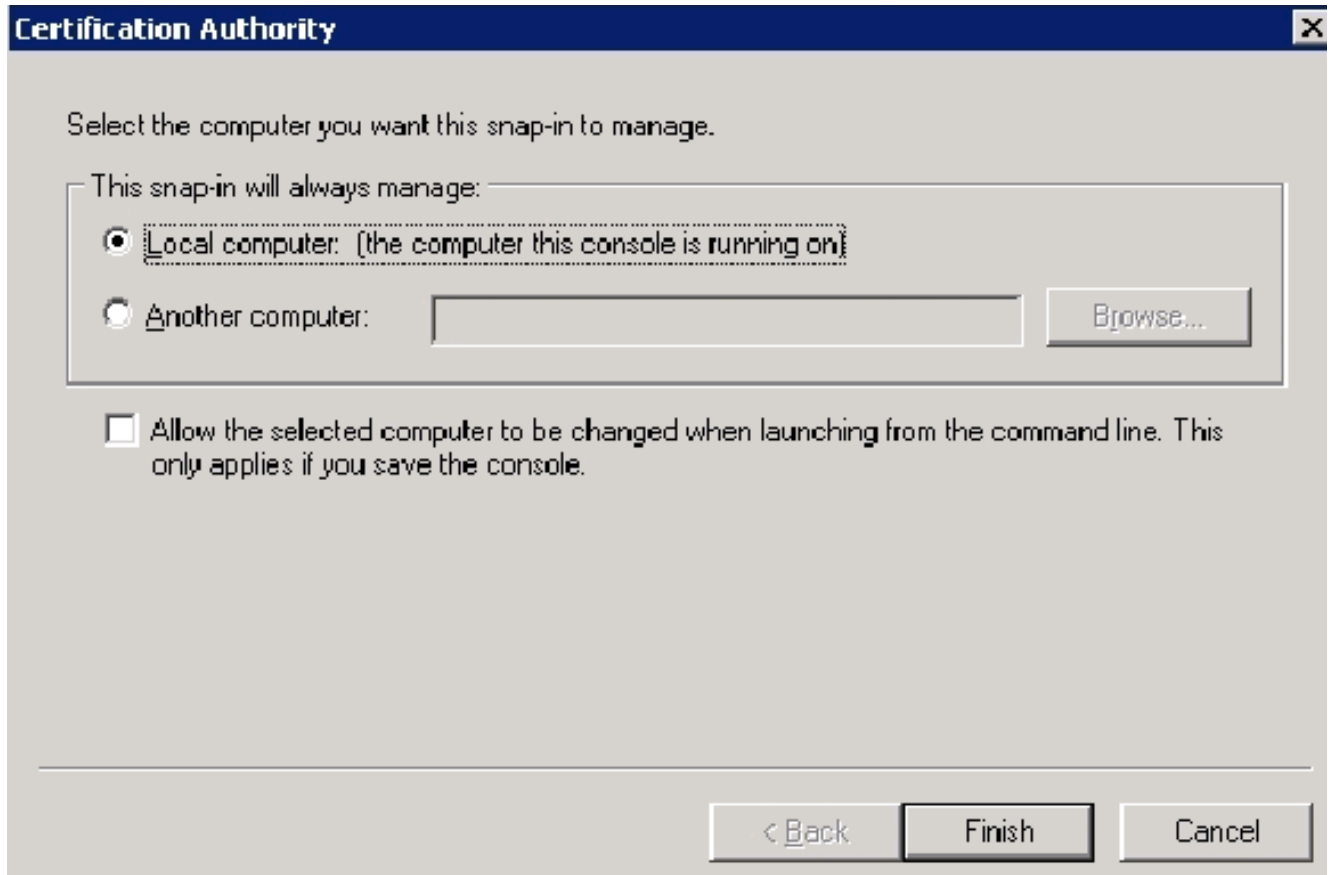
Valid existing certificate

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。

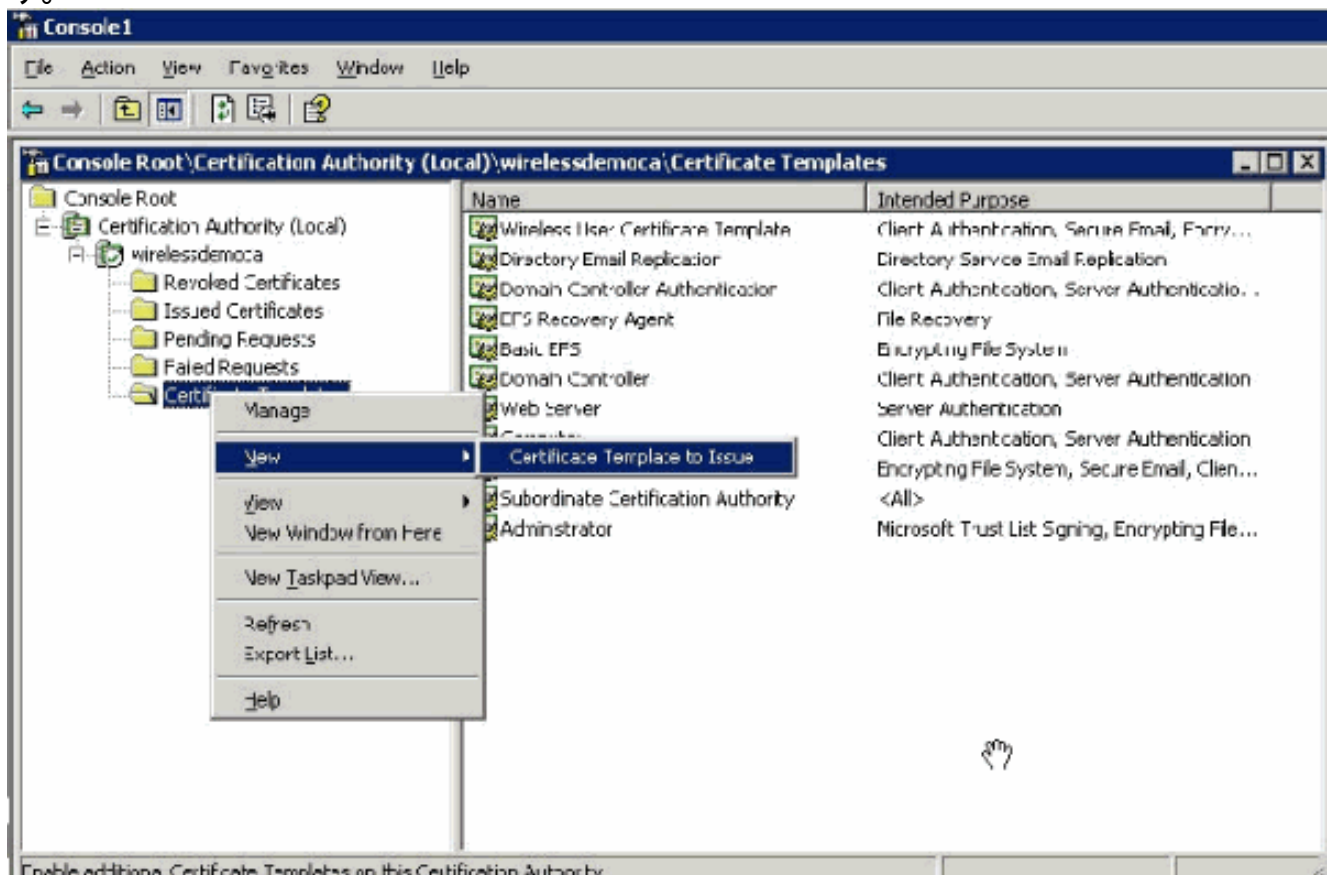
## [新しい ACS Web サーバ証明書テンプレートの有効化](#)

次のステップを実行します。

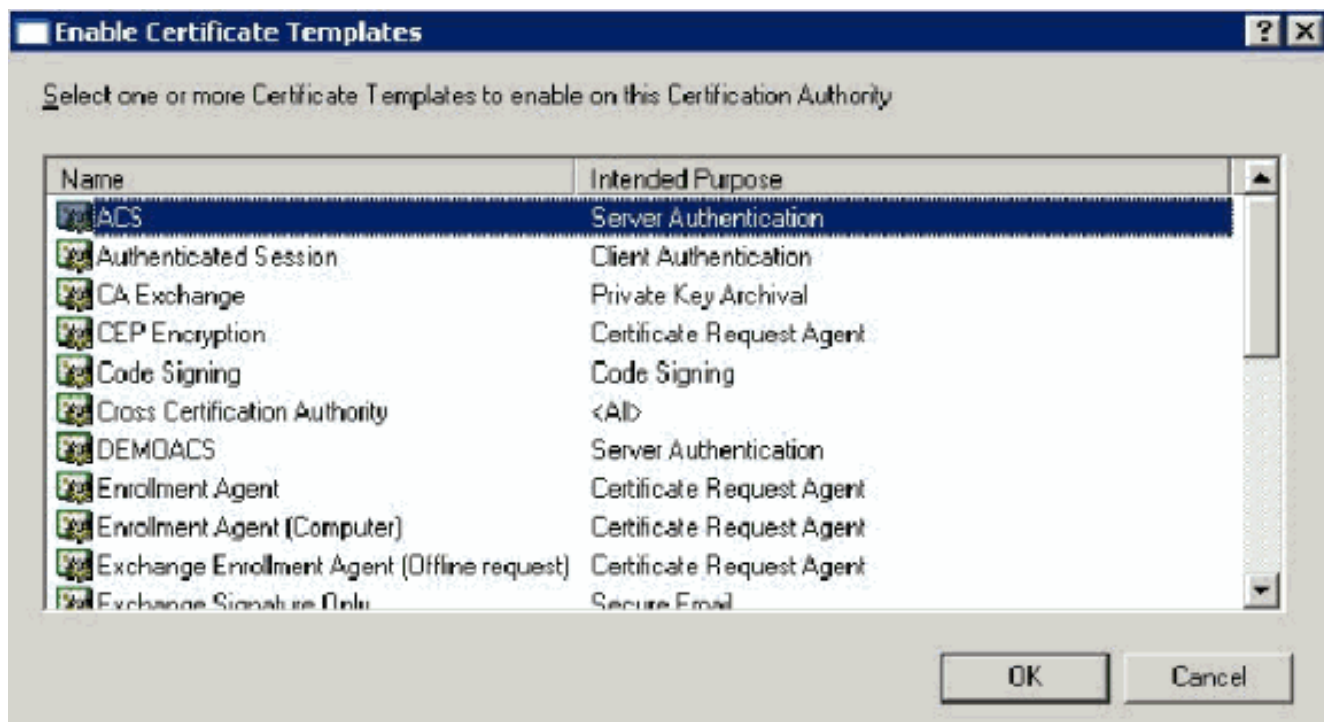
1. [Certification Authority] スナップインを開きます。「[Create the Certificate Template for the ACS Web Server](#)」セクションのステップ1 ~ 3に従って、[Certificate Authority]オプションを選択し、[Local Computer]を選択し、[Finish]をクリックします。



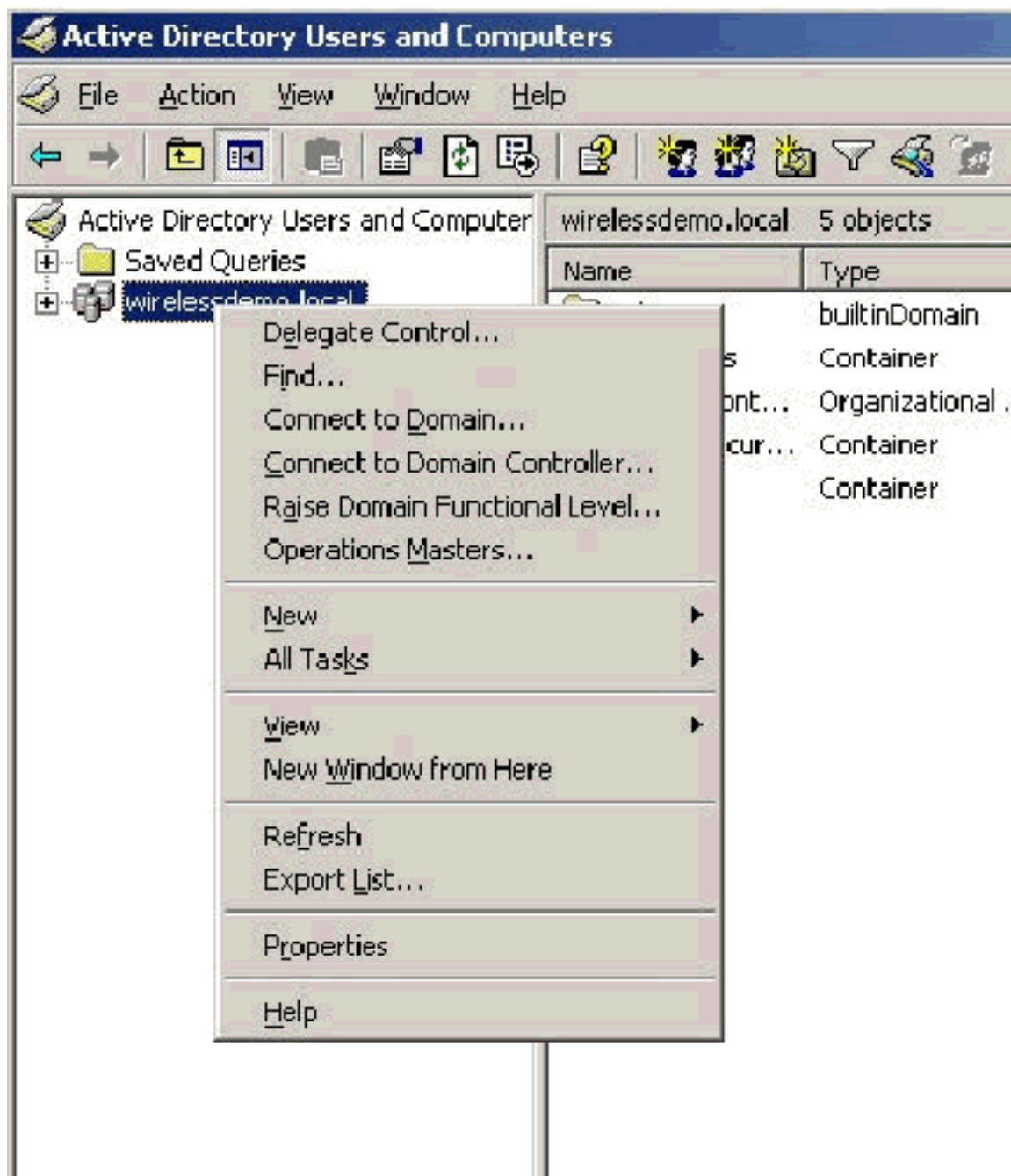
2. コンソール ツリーで、wirelessdemoca を展開し、Certificate Templates を右クリックします。



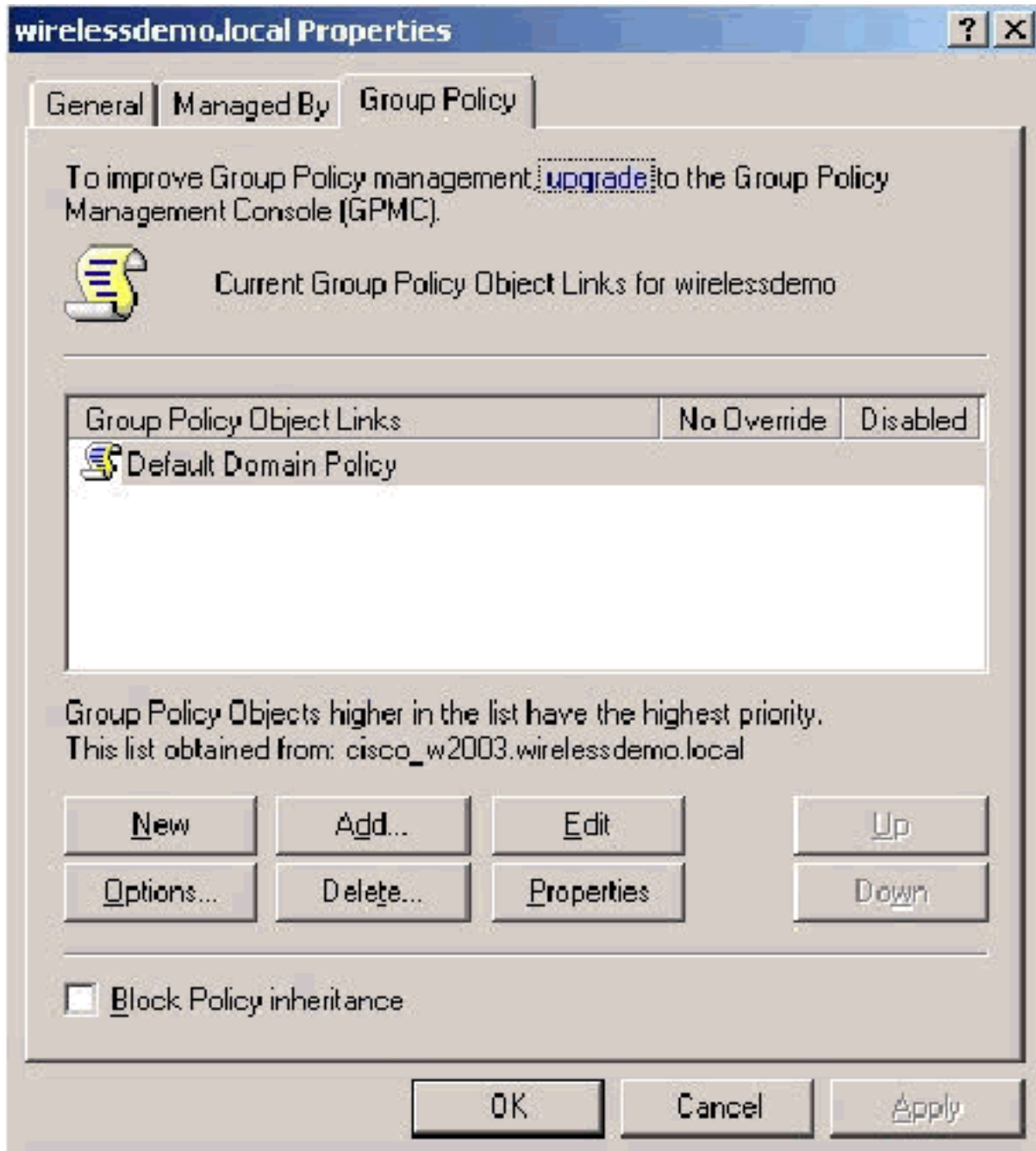
3. New > Certificate Template to Issue の順に選択します。
4. ACS Certificate Template をクリックします。



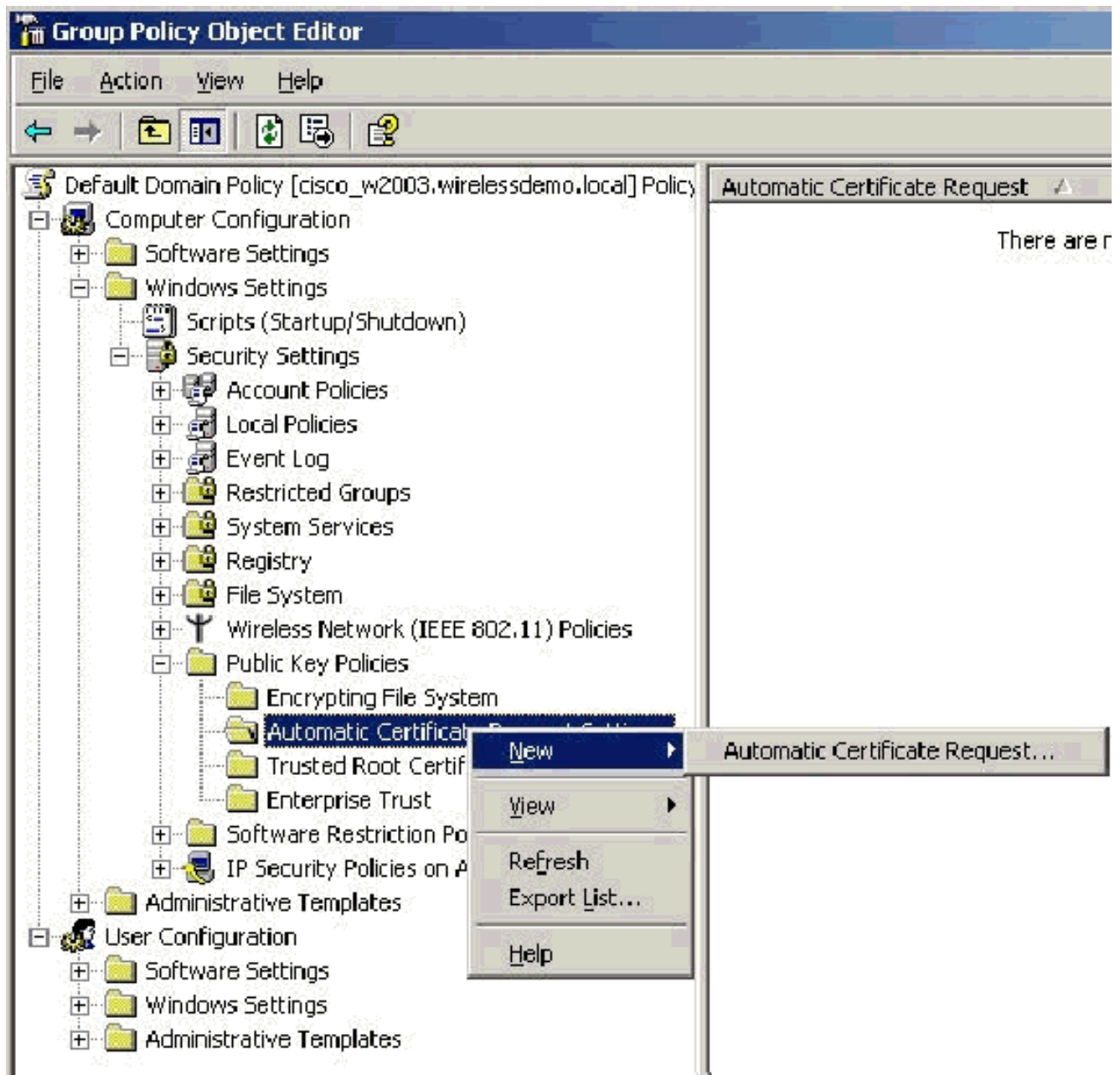
5. [OK] をクリックし、[Active Directory Users and Computers] スナップインを開きます。
6. コンソール ツリーで Active Directory Users and Computers をダブルクリックし、wirelessdemo.local domain を右クリックして Properties をクリックします。



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、[コンピュータの構成] > [Windowsの設定] > [セキュリティの設定] > [公開キーポリシー]を展開し、[自動証明書要求の設定]を選択します。

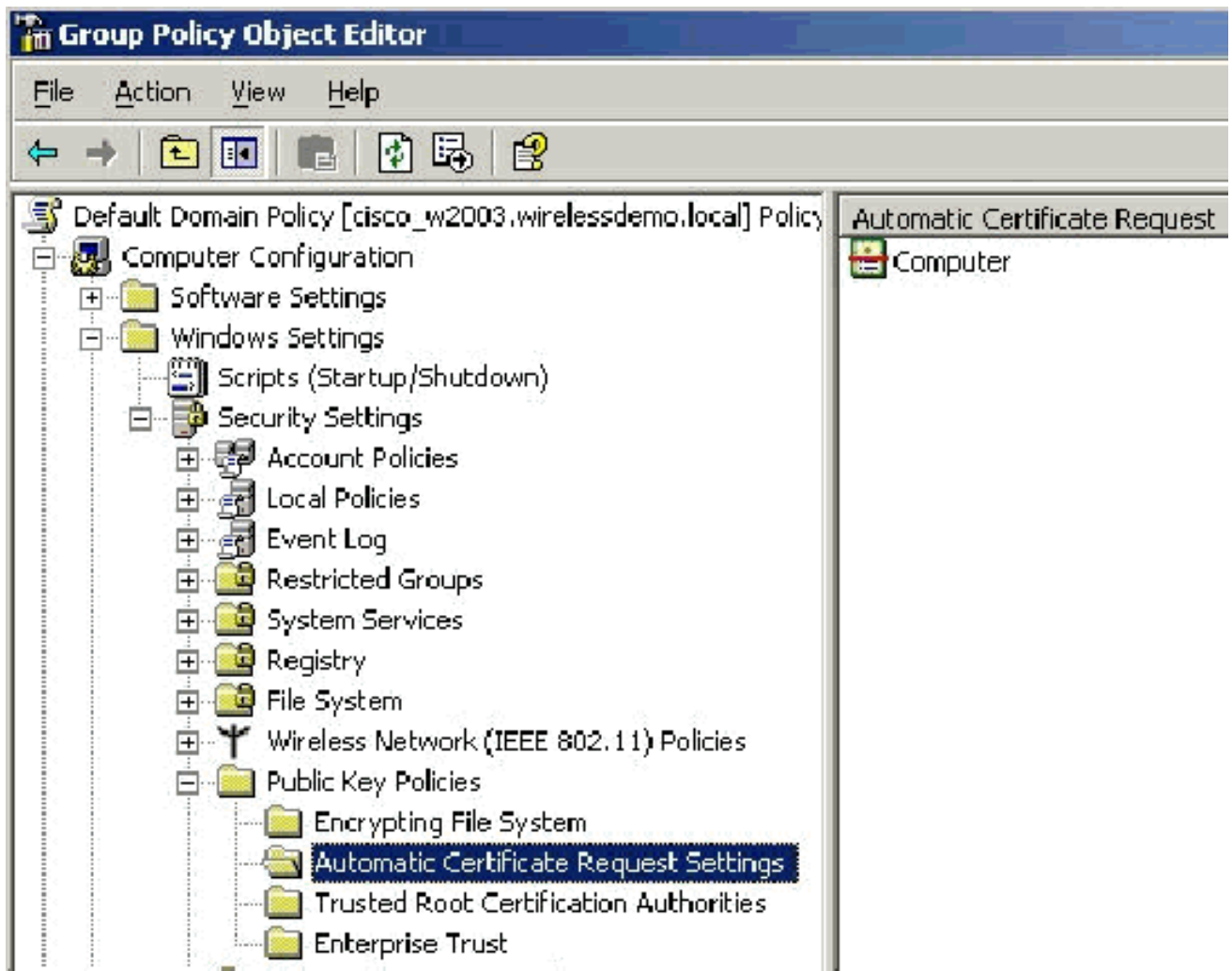


9. [Automatic Certificate Request Settings]を右クリックし、[New] > [Automatic Certificate Request]を選択します。
10. [Welcome to the Automatic Certificate Request Setup Wizard] ページで [Next] をクリックします。
11. Certificate Template ページで Computer をクリックし、Next をクリックします。

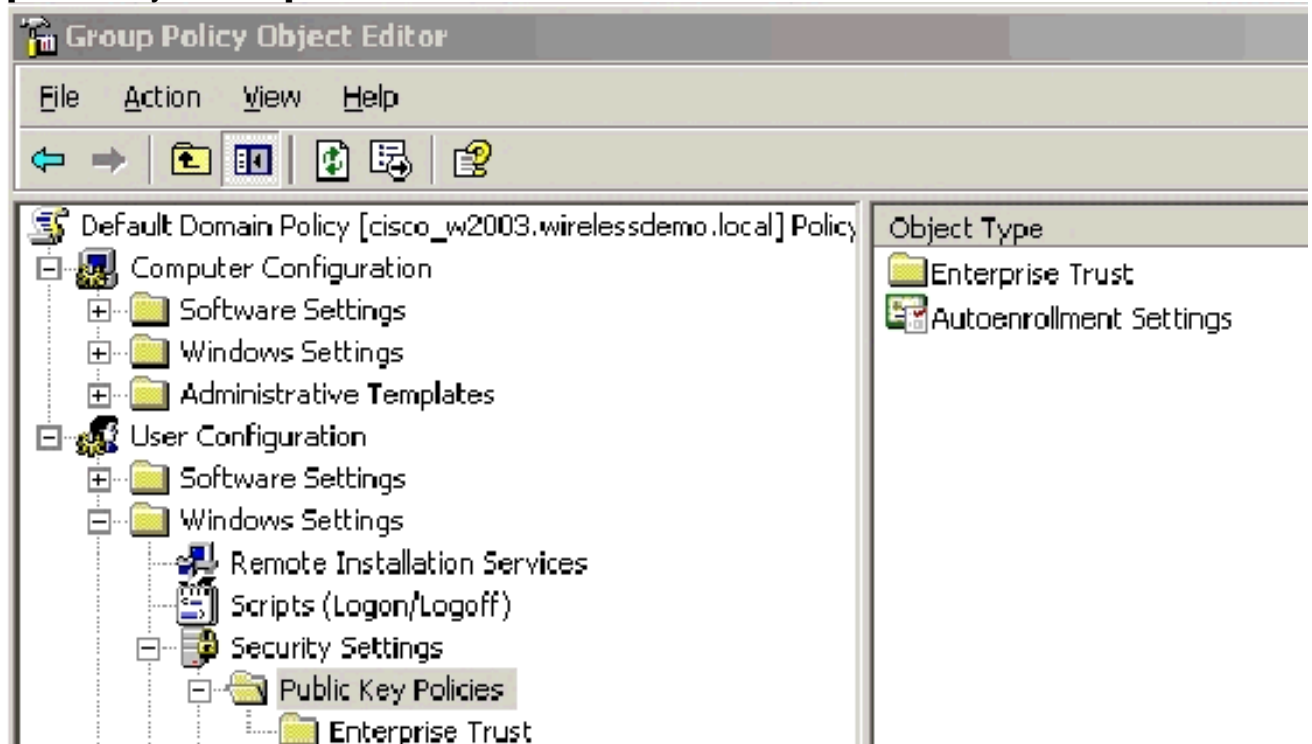




- Automatic Certificate Request Setup Wizard ページが終了したら、Finish をクリックします。[Group Policy Object Editor] スナップインの詳細ペインに、コンピュータ証明書の種類が表示されます。

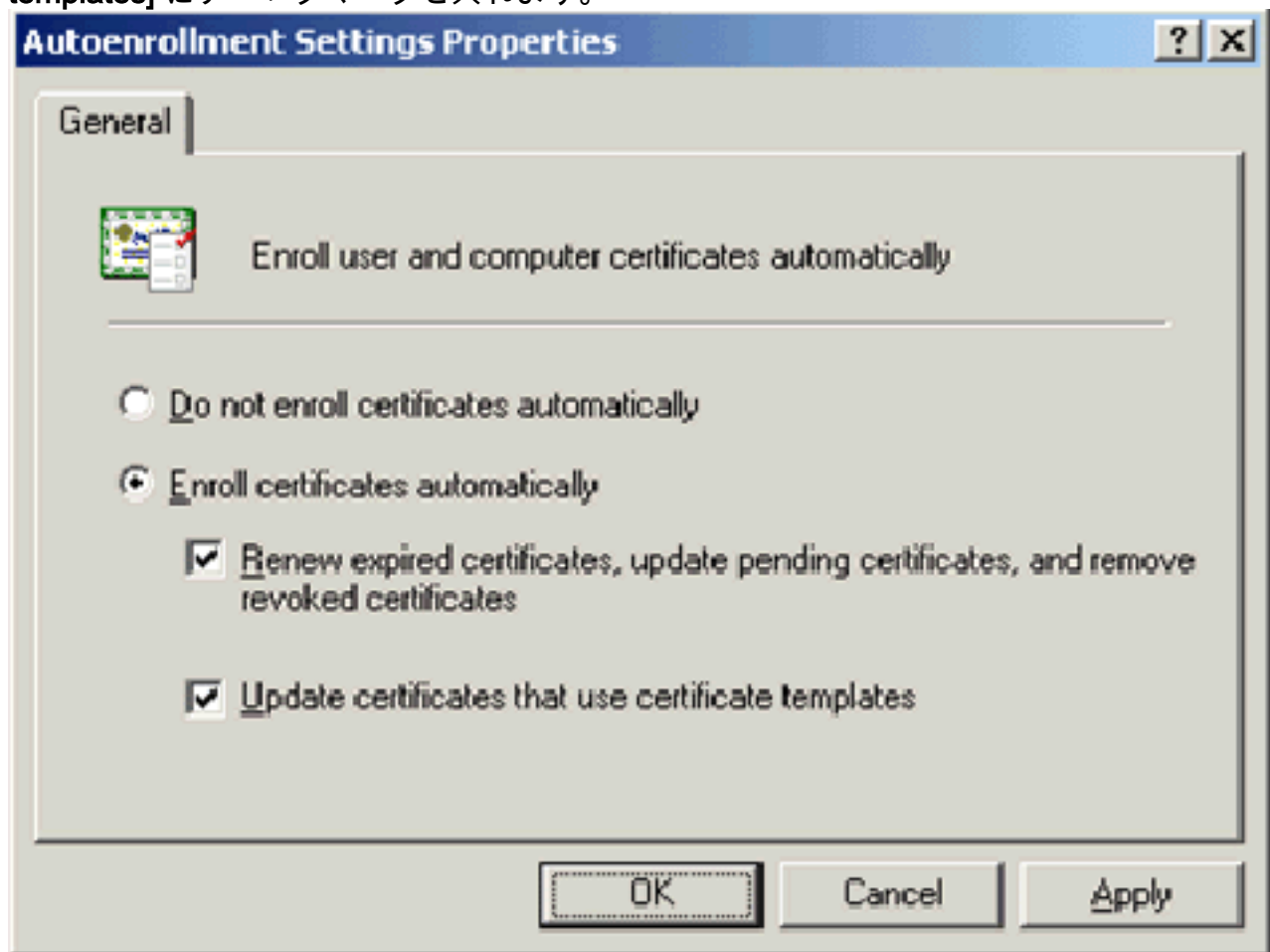


13. コンソール ツリーで、[User Configuration] > [Windows Settings] > [Security Settings] > [Public Key Policies] を展開します。



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 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](#)

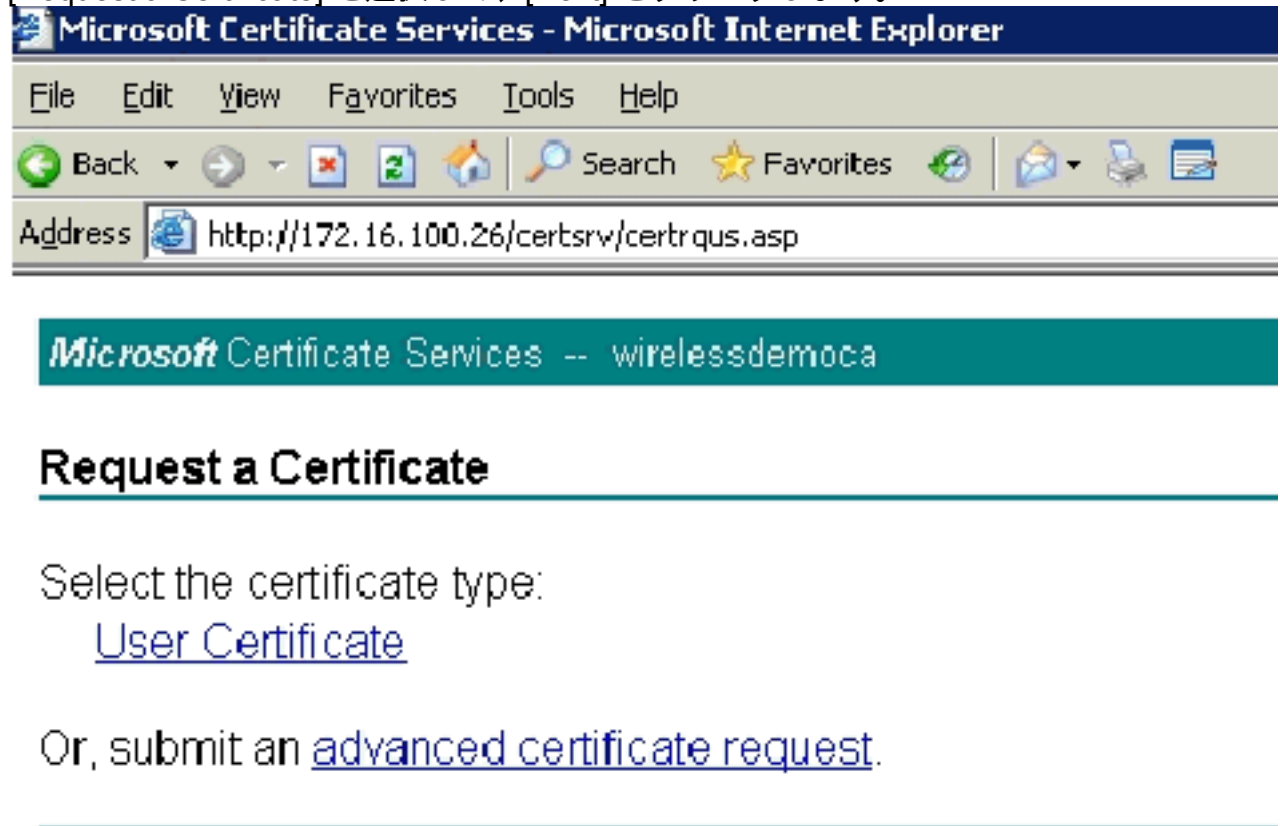
**重要：** ACS サーバが WLAN の EAP-TLS クライアントの認証を実行するには、エンタープライズルート CA サーバからサーバ証明書を取得している必要があります。

**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。

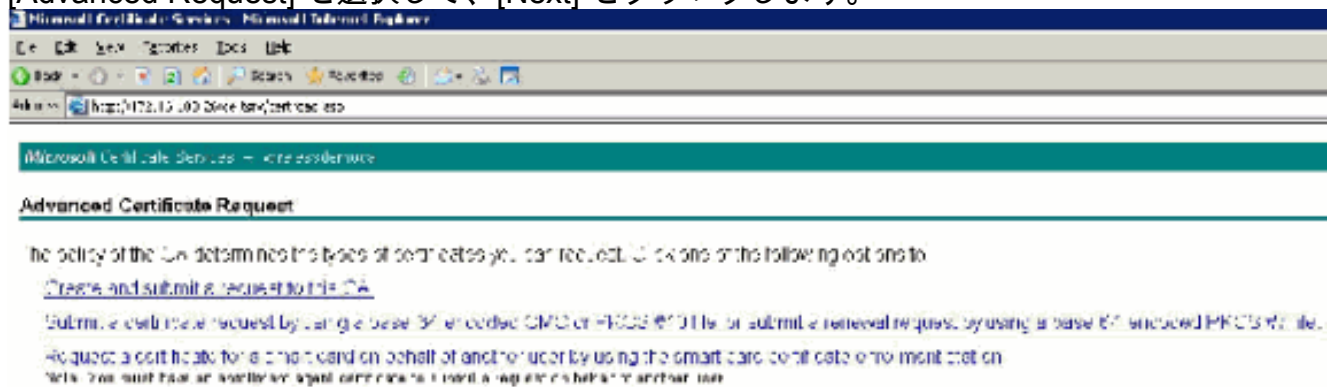
1. Enterprise Admin 権限を持っているアカウントで、ACS サーバにログインします。
2. ローカル ACS マシンで、ブラウザから `http://<ルート CA の IP アドレス>/certsrv` で Microsoft 認証局サーバを指定します。この例では、IP アドレスは 172.16.100.26 です。
3. Administrator でログインします。



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

sock - [Icons] Secret - Favorites [Icons] [Icons]

Address: http://172.16.1.10:2544/verifimain.asp

Microsoft Certificate Services - wirelessdemo.local

### Advanced Certificate Request

Certificate Template: Administrator

Key Options:

Administrator  
Basic EFS  
EFS Recovery Agent  
User  
CSP: Wireless User Certificate Template  
Key Usage: S...rdina... Certification Authority  
Key Store: Web Server  
Max. Expiration: Mar 15 2004 10:24:40 AM -0500 (UTC-05:00)

Automatic key container name  User specified key container name

Mark keys as exportable  
 Export keys to file

Enable sharing private key protection

Store certificate in the local computer certificate store  
*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

Additional Options

Request Format:  CMC  PKCS10

Hash Algorithm: SHA-1  
*Only used to sign request.*

Save request to file

Activities: [List Box]

Friendly Name: [Text Box]

[Submit >]

- 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。
- 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。[Store certificate in the local computer certificate store] がオンになっていることを確認し、[Submit] をクリックします。

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Deck Back Forward Stop Search Favorites

Address http://172.16.100.25/certsrv/certreq.asp

---

**Certificate Template:**

ACS

---

**Identifying Information For Offline Template:**

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

---

**Key Options:**

Create new key set    Use existing key set

CSP:

Key Usage:  Exchange

Key Size:    Min:1024   Max:1024   (common key sizes: 1024)

Automatic key container name    User specified key container name

Mark keys as exportable

Export keys to file

Store certificate in the local computer certificate store  
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

---

**Additional Options:**

Request Format:  CMC    PKCS10

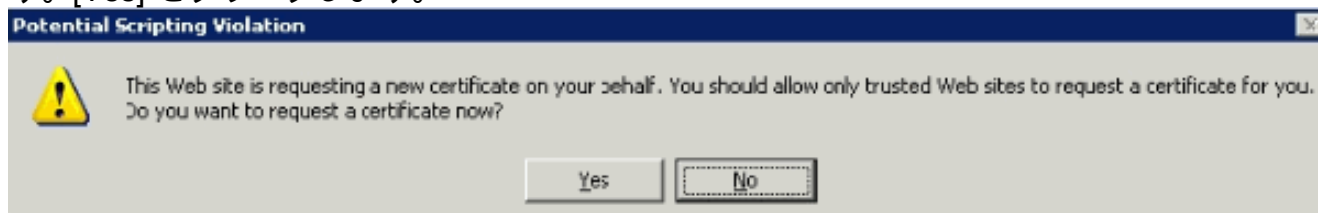
Hash Algorithm:   
Only used to sign request.

Save request to a file

Attributes:

Friendly Name:

9. ポップアップ ウィンドウに、スクリプト違反の可能性のあることを示す警告が表示されます。[Yes] をクリックします。



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



Microsoft Certificate Services -- wirelessdemoca

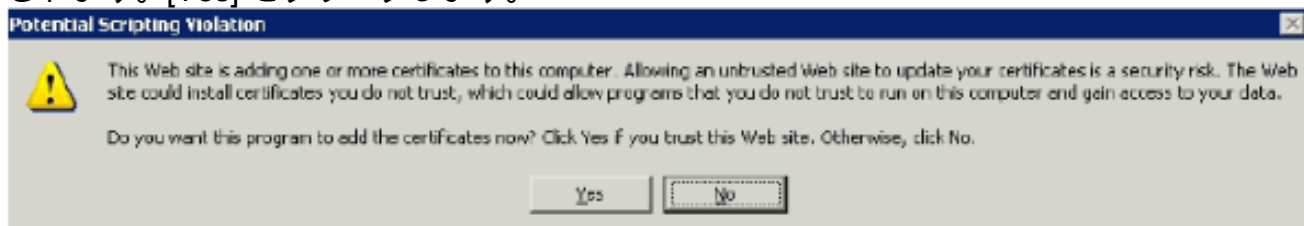
## Certificate Issued

The certificate you requested was issued to you.

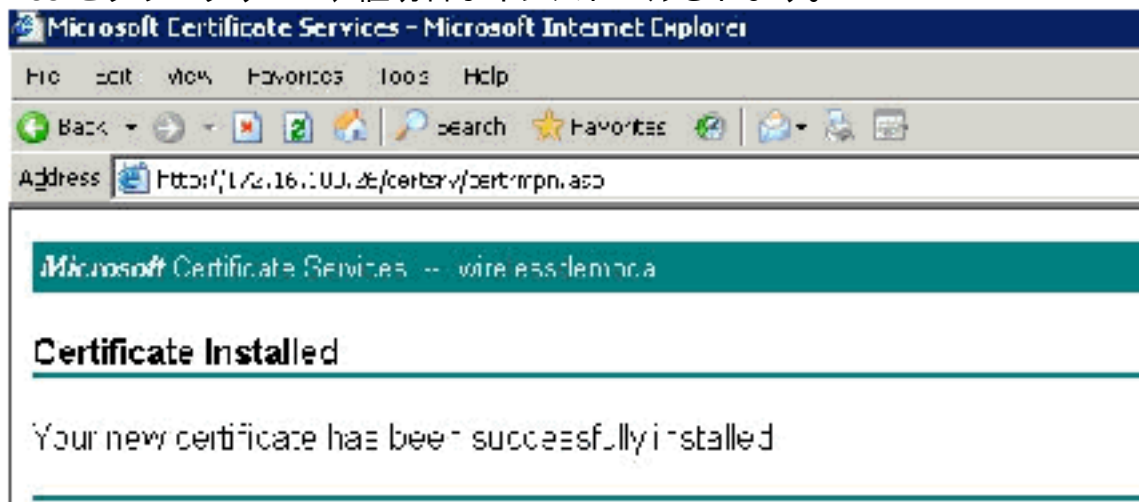


[Install this certificate](#)

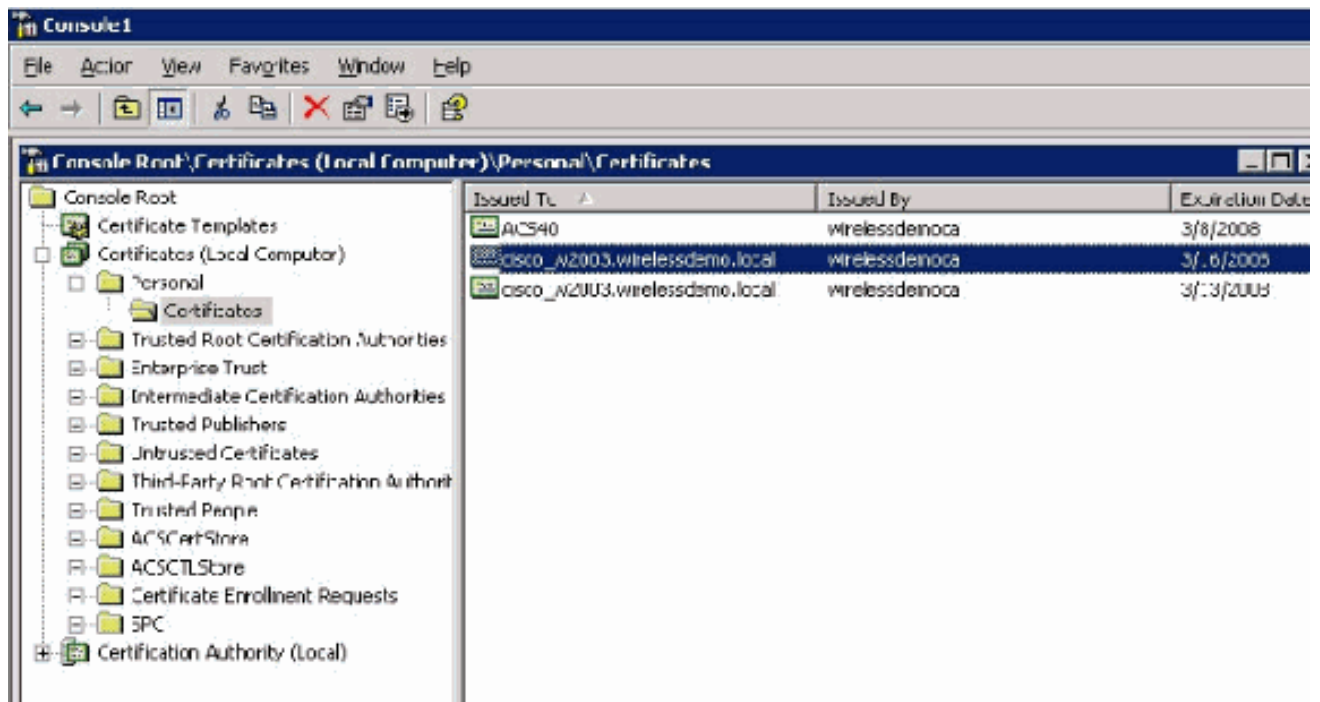
11. ポップアップ ウィンドウがもう一度表示され、スクリプト違反の可能性があることが警告されます。[Yes] をクリックします。



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、証明書が Certificates フォルダにインストールされます。このフォルダにアクセスするには、[Start] > [Run]の順に選択し、mmcと入力してEnterキーを押し、[Personal] > [Certificates]を選択します。



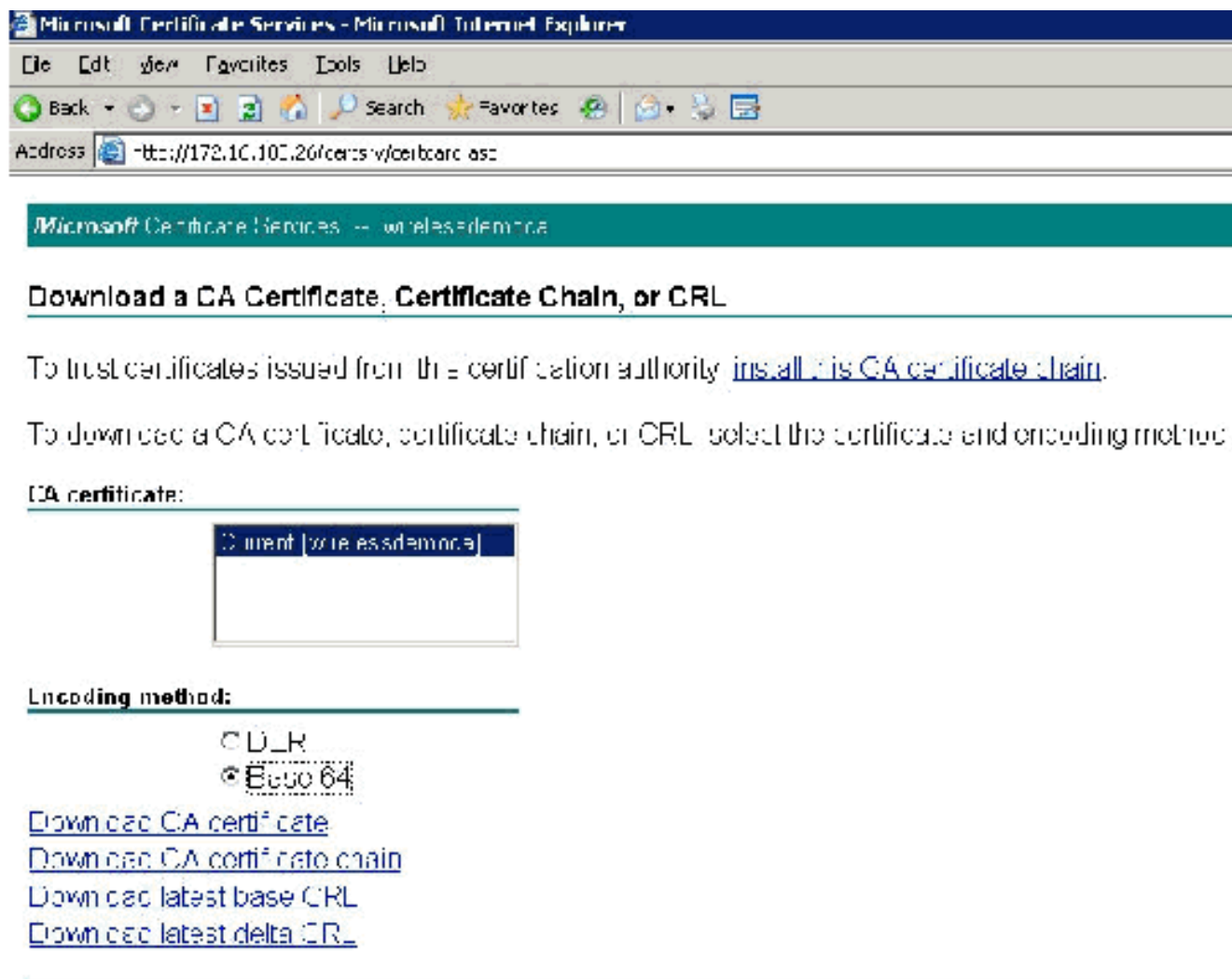
- これで、ローカルコンピュータ（この例では、ACS または cisco\_w2003）に証明書がインストールされたので、続いて ACS 4.0 の証明書ファイル設定用の証明書ファイル（.cer）を生成する必要があります。
- ACS サーバで（この例では cisco\_w2003）、ブラウザから <http://172.16.100.26/certsrv> の Microsoft 認証局サーバを指定します。

## ACS 4.0 ソフトウェアでの証明書のインストール

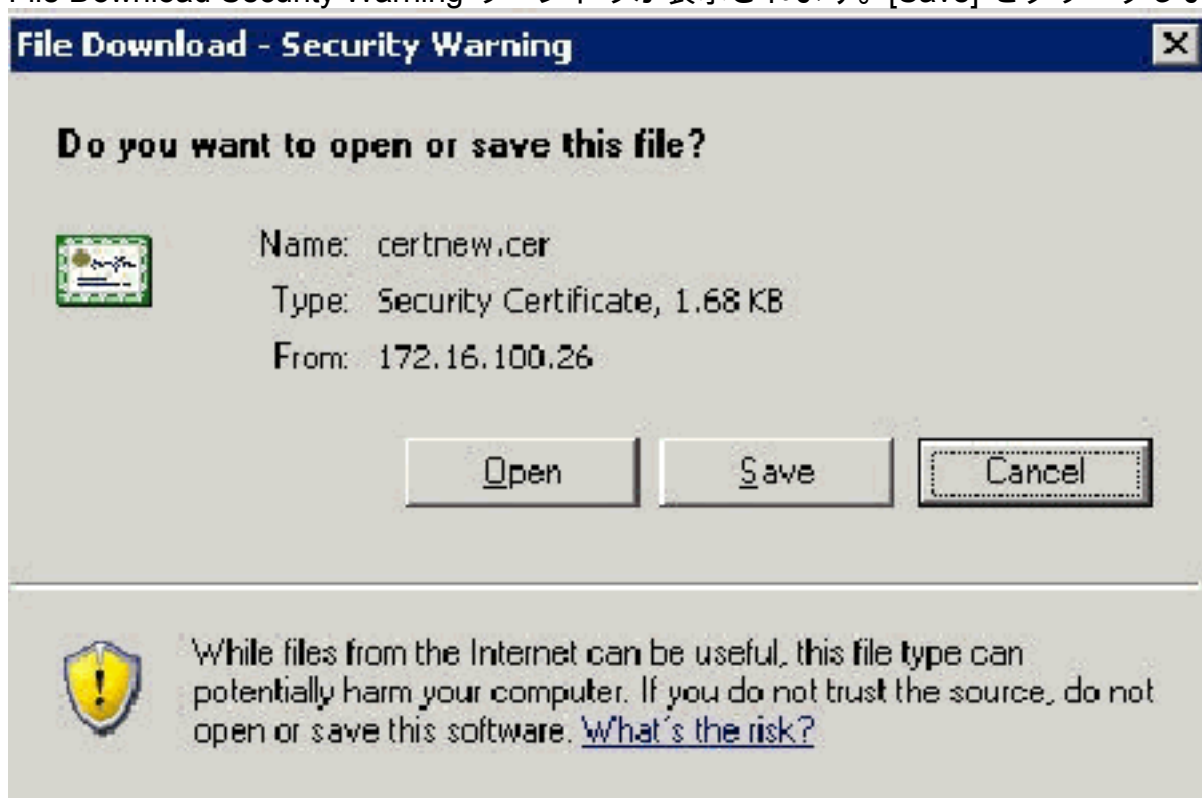
次のステップを実行します。

- 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。
- Select a Task オプションから Download a CA certificate, certificate chain or CRL を選択します。
- 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。

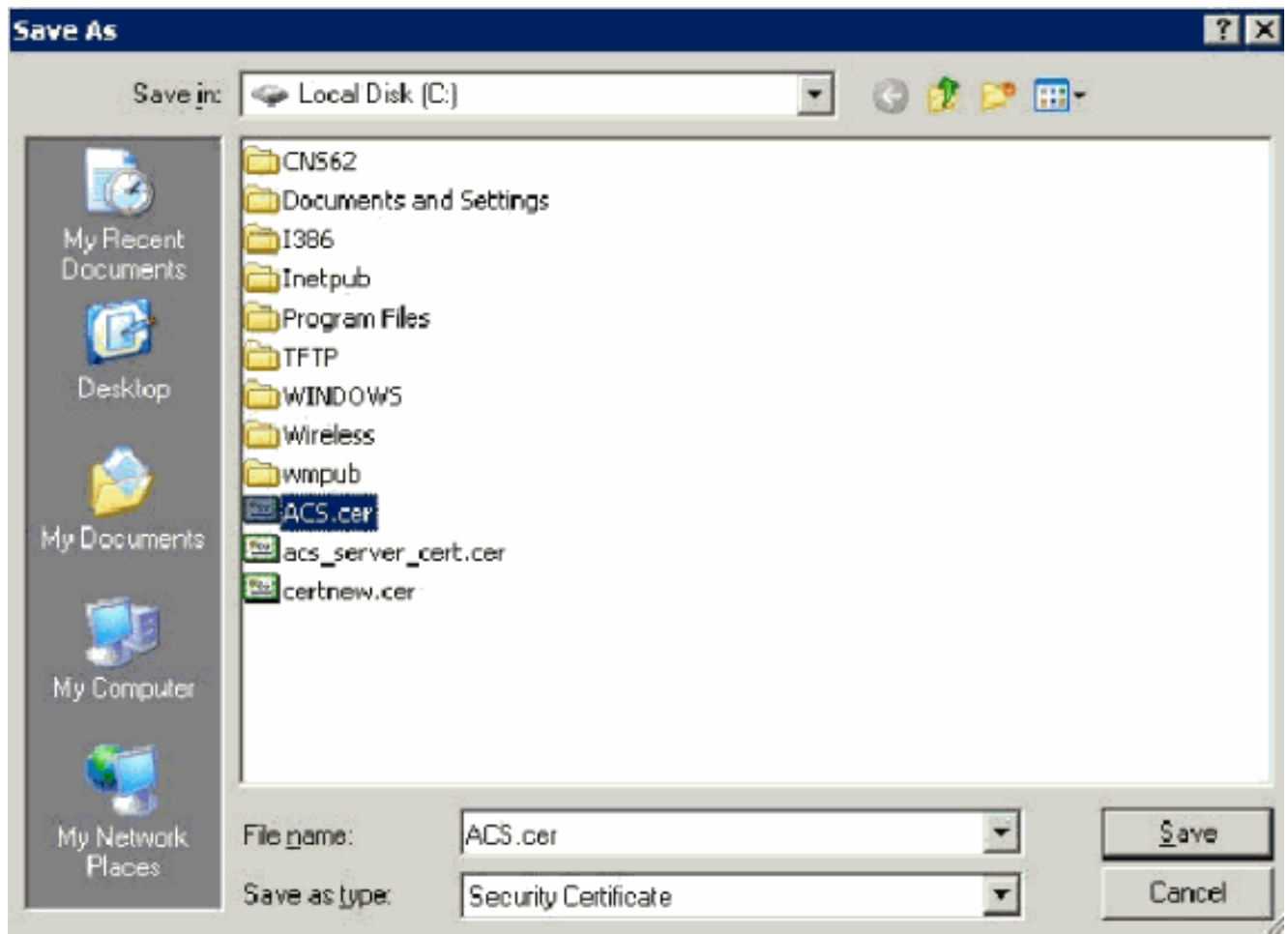




4. File Download Security Warning ウィンドウが表示されます。[Save] をクリックします。



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。

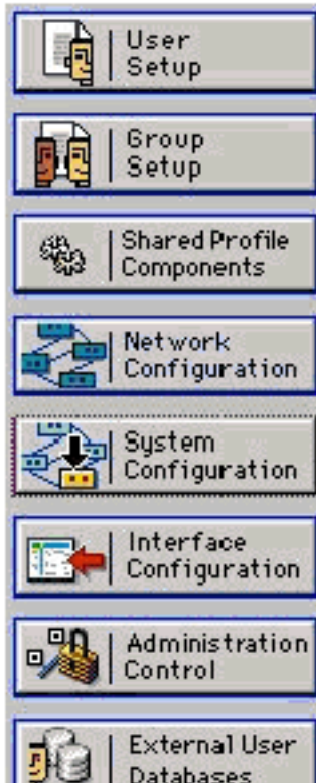


6. インストール時に作成されたデスクトップのショートカットを使用して、ACS Admin を開きます。
7. System Configuration をクリックします。



## System Configuration

### Select



-  [Service Control](#)
-  [Logging](#)
-  [Date Format Control](#)
-  [Local Password Management](#)
-  [ACS Internal Database Replication](#)
-  [ACS Backup](#)
-  [ACS Restore](#)
-  [ACS Service Management](#)
-  [VoIP Accounting Configuration](#)
-  [ACS Certificate Setup](#)
-  [Global Authentication Setup](#)

8. [ACS Certificate Setup] をクリックします。

# System Configuration

Select

## ACS Certificate Setup

-  [Install ACS Certificate](#)
-  [ACS Certification Authority Setup](#)
-  [Edit Certificate Trust List](#)
-  [Certificate Revocation Lists](#)
-  [Generate Certificate Signing Request](#)
-  [Generate Self-Signed Certificate](#)

Cancel

9. [Install ACS Certificate]をクリックします。

# System Configuration

Edit

## Install ACS Certificate

Install new certificate	
<input type="radio"/> Read certificate from file	
<b>Certificate file</b>	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
<b>Certificate CN</b>	<input type="text"/>
<b>Private key file</b>	<input type="text"/>
<b>Private key password</b>	<input type="text"/>

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。

## System Configuration

Edit

### Install ACS Certificate


Install new certificate 	
<input type="radio"/> Read certificate from file	
Certificate file	<input type="text"/>
<input checked="" type="radio"/> Use certificate from storage	
Certificate CN	<input type="text" value="cisco_w2003.wirelessdemo"/>
Private key file	<input type="text"/>
Private key password	<input type="text"/>

11. [Submit] をクリックします。

## System Configuration

Edit

### Install ACS Certificate

Installed Certificate Information 	
Issued to:	cisco_w2003.wirelessdemo.local
Issued by:	wirelessdemoca
Valid from:	March 17 2006 at 08:33:25
Valid to:	March 16 2008 at 08:33:25
Validity:	OK


**The current configuration has been changed.  
Restart ACS in "System Configuration:Service  
Control" to adopt the new settings for EAP-TLS or  
PEAP support only.**

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。

# System Configuration

Select

**CiscoSecure ACS on cisco\_w2003** 

## Is Currently Running

**Services Log File Configuration** 

Level of detail

None

Low

Full

Generate New File

Every day

Every week


Every month

When size is greater than  KB

Manage Directory

Keep only the last  files

Delete files older than  days

 [Back to Help](#)

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-TLS とその下にあるすべてのボックスにチェックマークを付けます。

# System Configuration

## Global Authentication Setup

?**EAP Configuration**

**PEAP**

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

---

**EAP-FAST**

[EAP-FAST Configuration](#)

---

**EAP-TLS**

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

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。

# System Configuration

Edit

## ACS Certification Authority Setup

CA Operations	
Add new CA certificate to local certificate storage	
CA certificate file	<input type="text" value="c:\acs.cer"/>

System Configuration

ACS Certification Authority Setup	
CA Operations	
Add new CA certificate to local certificate storage	
CA certificate file	<input type="text" value="c:\acs.cer"/>
<b>The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.</b>	

New CA certificate is successfully added into the global system certificate storage.	
CA certificate common name	wirelessdemo.ca

22. ACS サービスを再起動します。

## Windows の自動機能を使用した EAP-TLS 用クライアントの設定

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

次のステップを実行します。

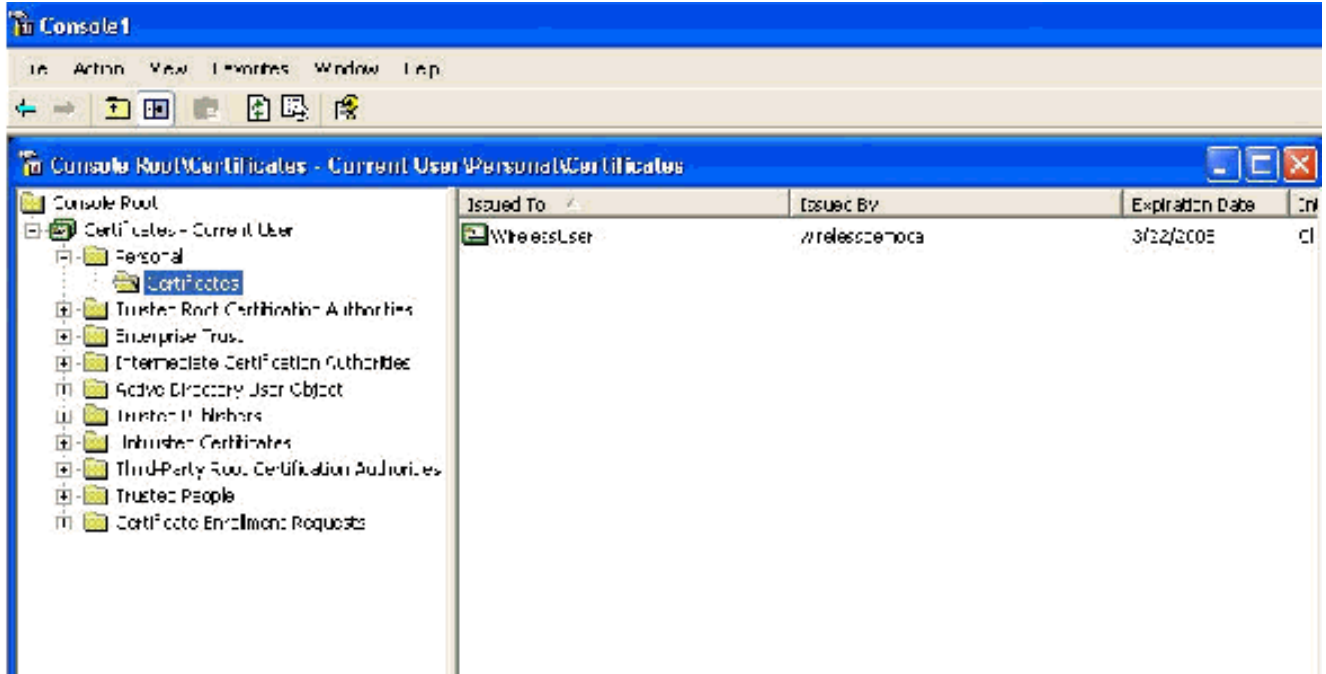
- イーサネット ケーブルを使用して CLIENT をスイッチに接続し、イントラネット ネットワーク セグメントに接続します。
- CLIENT に、Windows XP Professional SP2 をインストールします。このインストールでは、wirelessdemo.local ドメインの CLIENT という名前のメンバコンピュータとして設定します。
- Windows XP Professional SP2をインストールします。EAP-TLSおよびPEAPをサポートするには、このインストールが必要です。**注意：** Windows XP Professional SP2では、Windowsファイアウォールが自動的にオンになります。ファイアウォールをオフにしないでください。

### ワイヤレス ネットワーク接続の設定

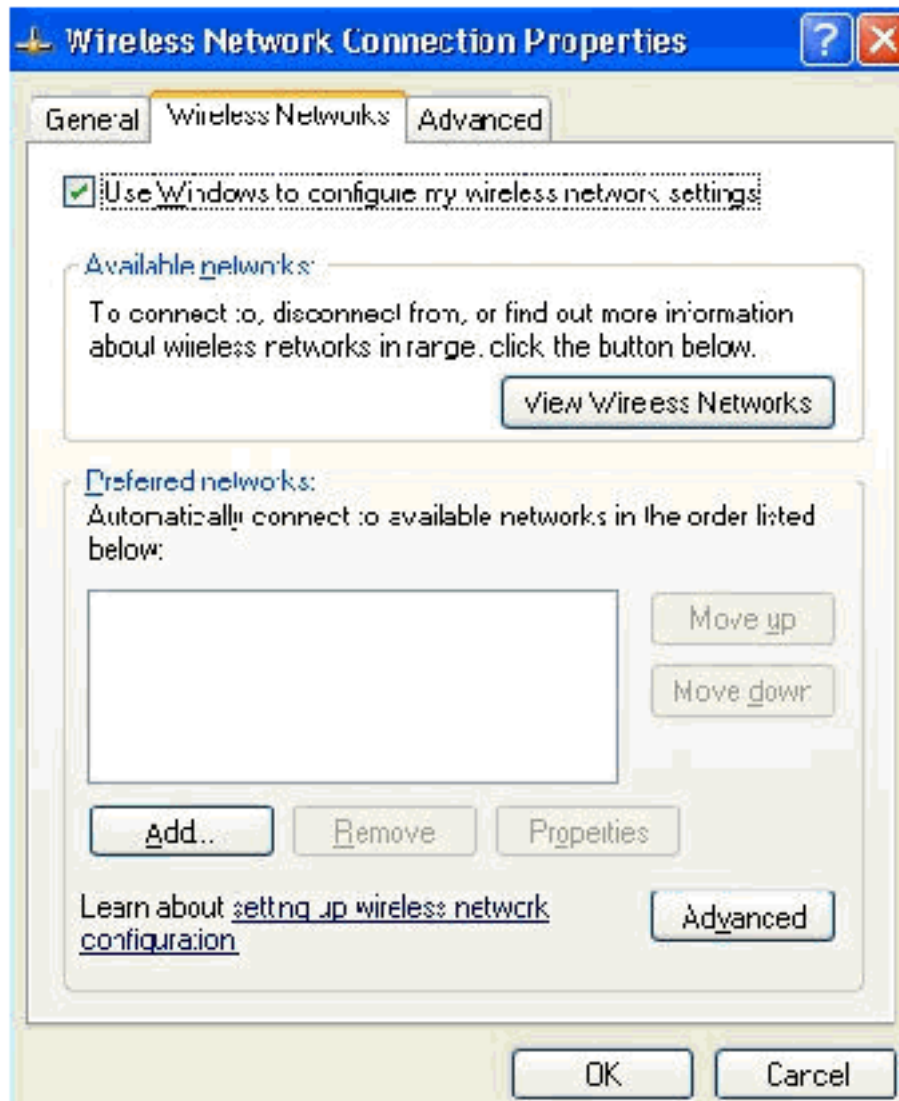
次のステップを実行します。



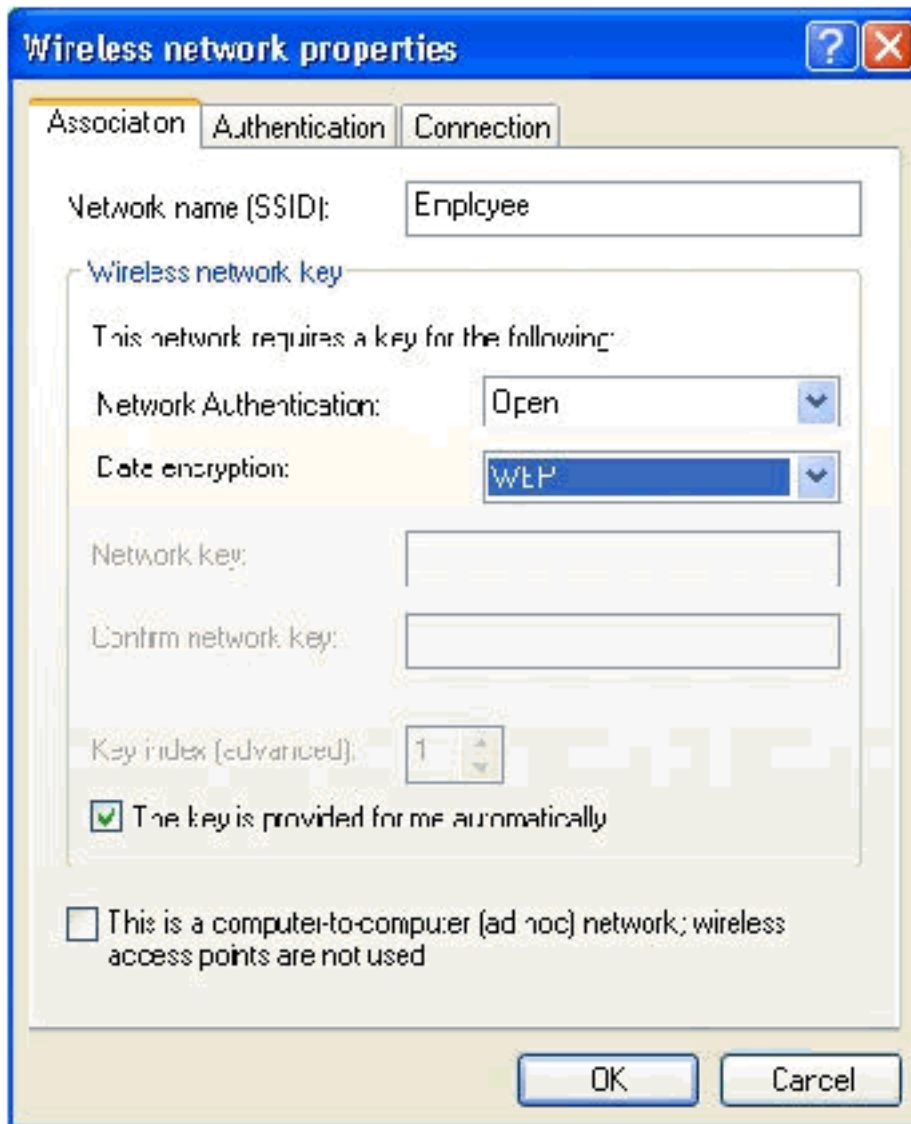
1. ログオフし、wirelessdemo.local ドメインの WirelessUser アカウントを使用してログインします。注：コマンド・プロンプトでgpupdateと入力し、コンピュータとユーザー構成のグループポリシー設定を更新し、ワイヤレスクライアントコンピュータのコンピュータとユーザー証明書を直ちに取得します。または、一度ログオフしてから再度ログインしてください。この操作は gpupdate と同じ効果があります。また、ドメインへのログオンには有線接続を使用する必要があります。注：証明書がクライアントに自動的にインストールされていることを確認するには、証明書MMCを開き、WirelessUser証明書が[Personal Certificates]フォルダで使用できることを確認します。



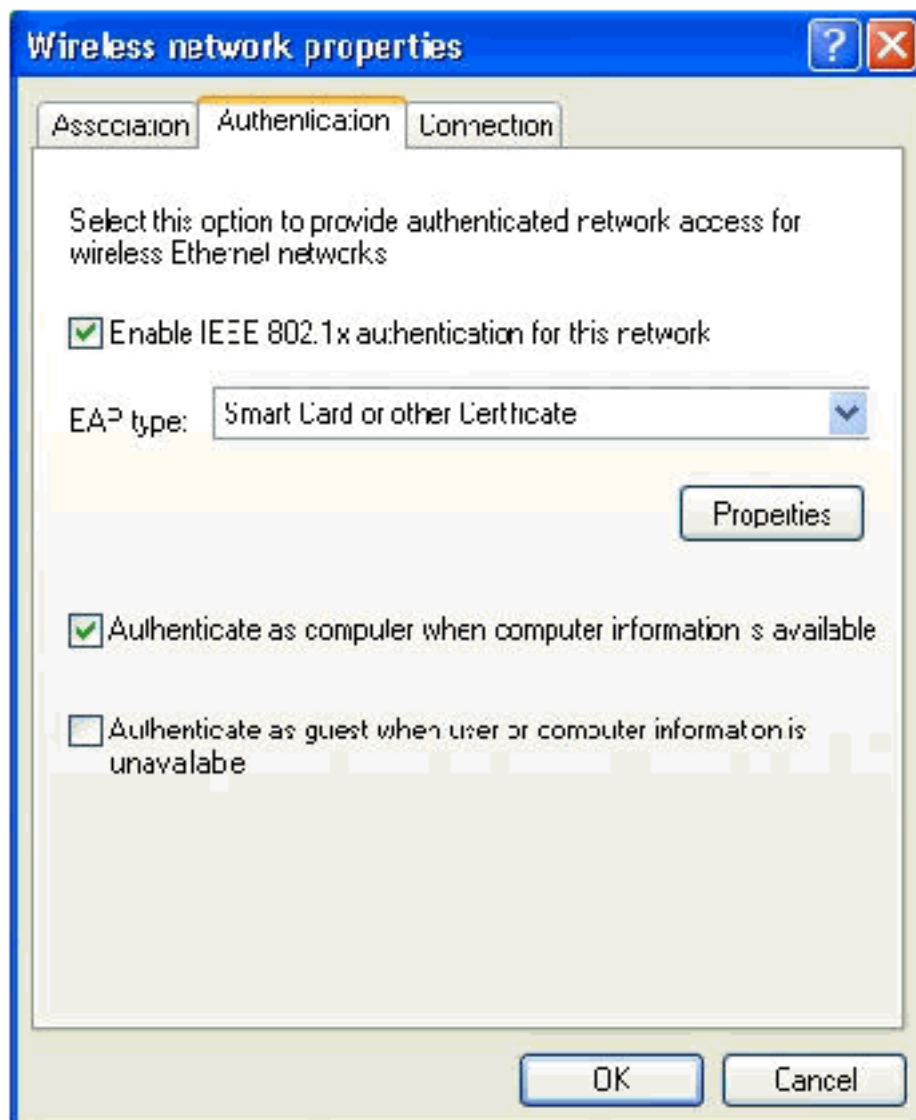
2. [Start] > [Control Panel] を選択し、[Network Connections] をダブルクリックして、[Wireless Network Connection] を右クリックします。
3. Properties をクリックし、Wireless Networks タブに移動して、Use Windows to configure my wireless network settings にチェックマークが入っていることを確認します。



4. [Add] をクリックします。
5. Association タブに移動し、Network name (SSID) フィールドに Employee と入力します。
6. Data Encryption に WEP が設定され、The key is provided for me automatically にチェックマークが入っていることを確認します。

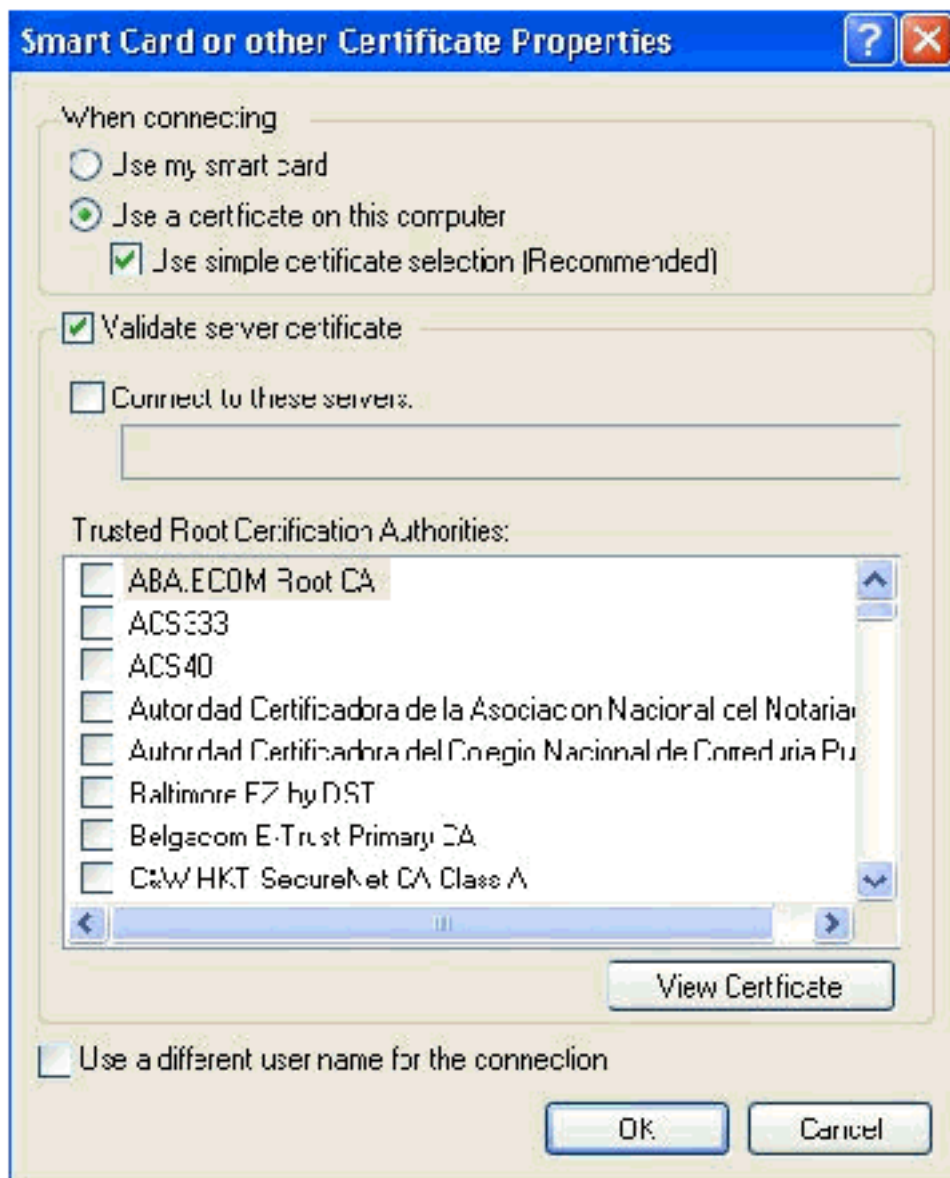


7. Authentication タブに移動します。
8. EAP タイプが Smart Card or other Certificate を使用する設定になっていることを確認します。そうならない場合は、ドロップダウンメニューでこれを選択します。
9. ログイン前にマシンの認証を実行する場合は（この場合、ログインスクリプトやグループポリシープッシュを適用できます）、Authenticate as computer when computer information is available オプションを選択します。

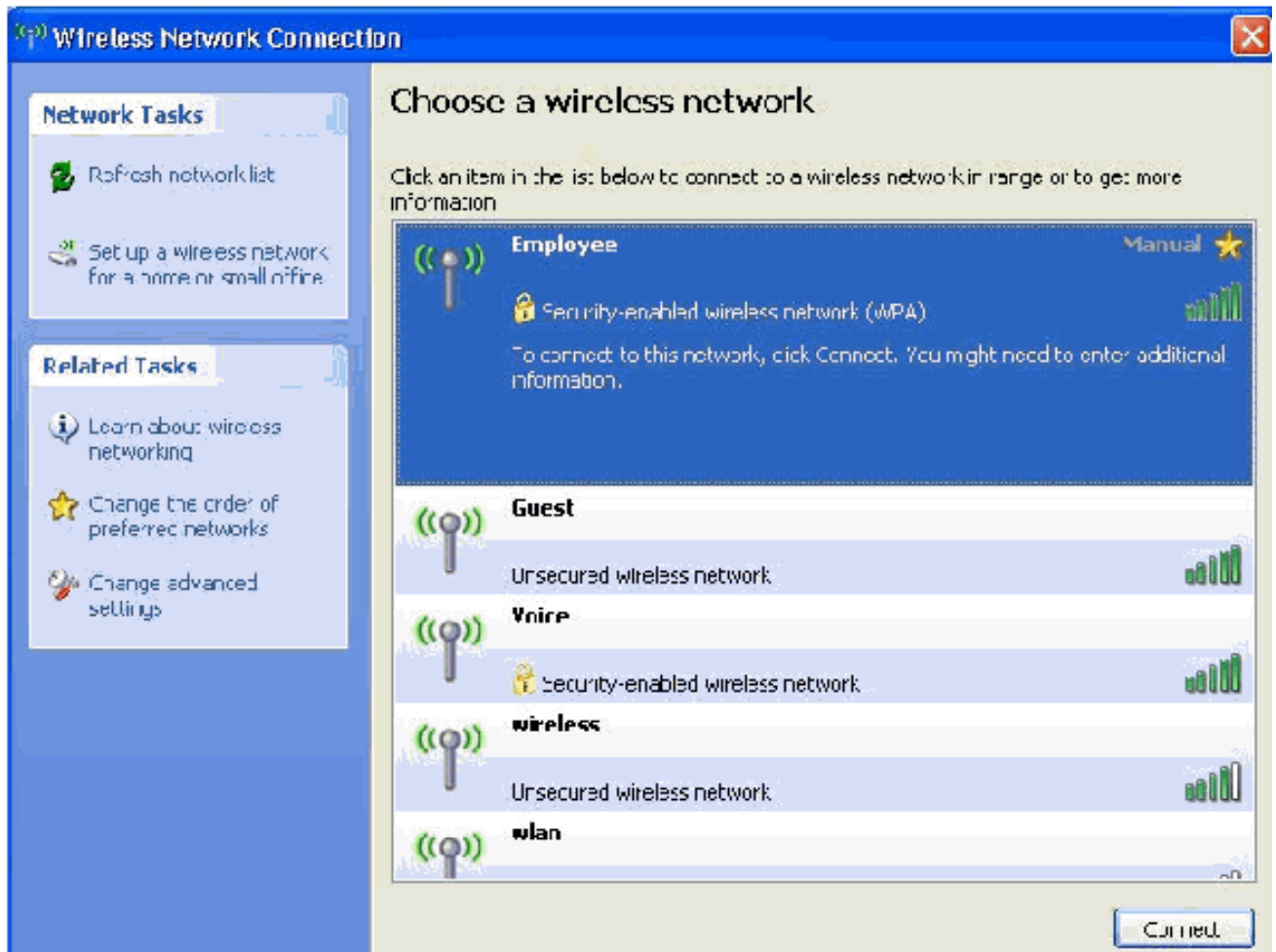


10. [Properties] をクリックします。

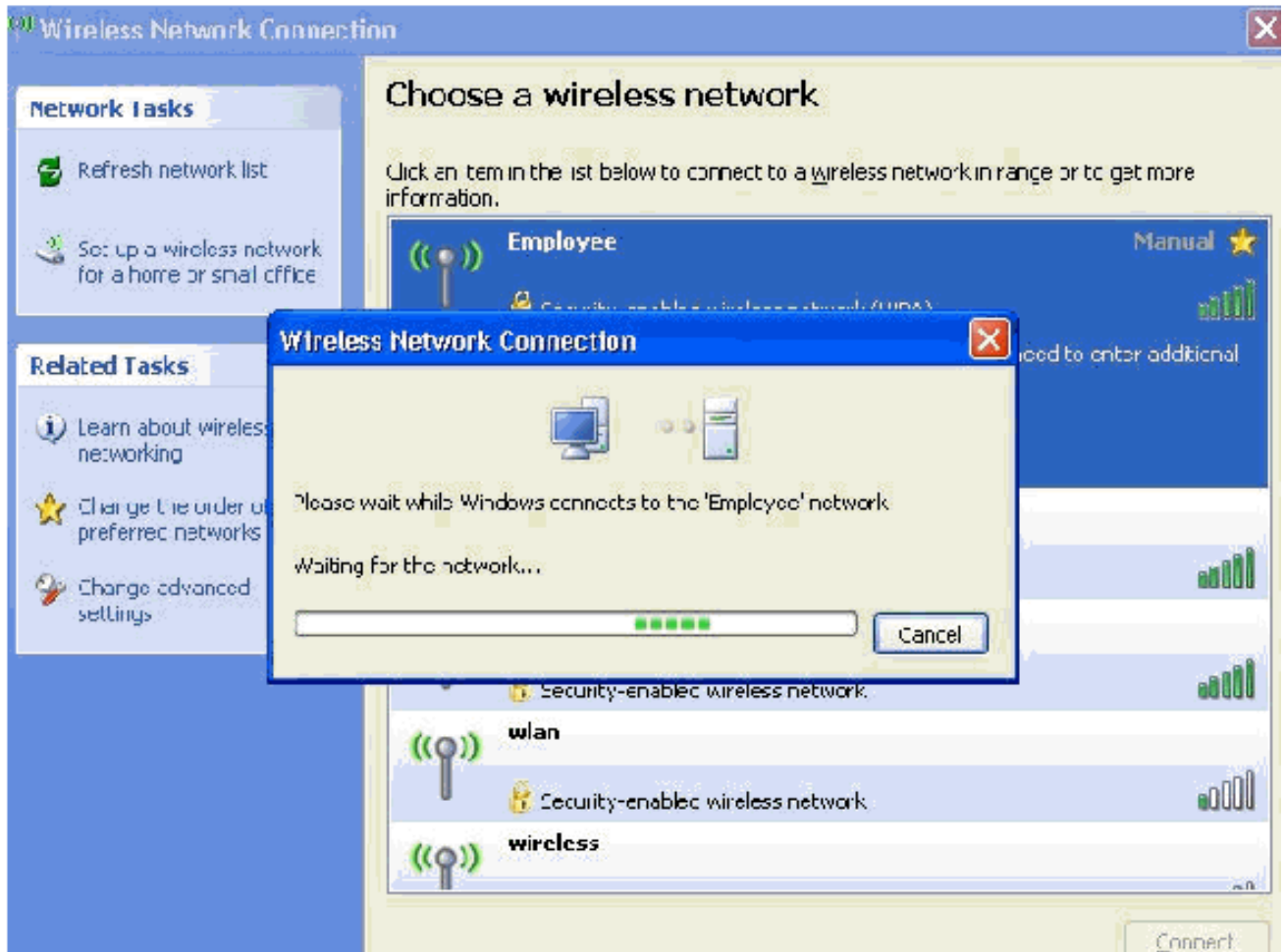
11. 次のウィンドウに示す各ボックスにチェックマークが付いていることを確認します。

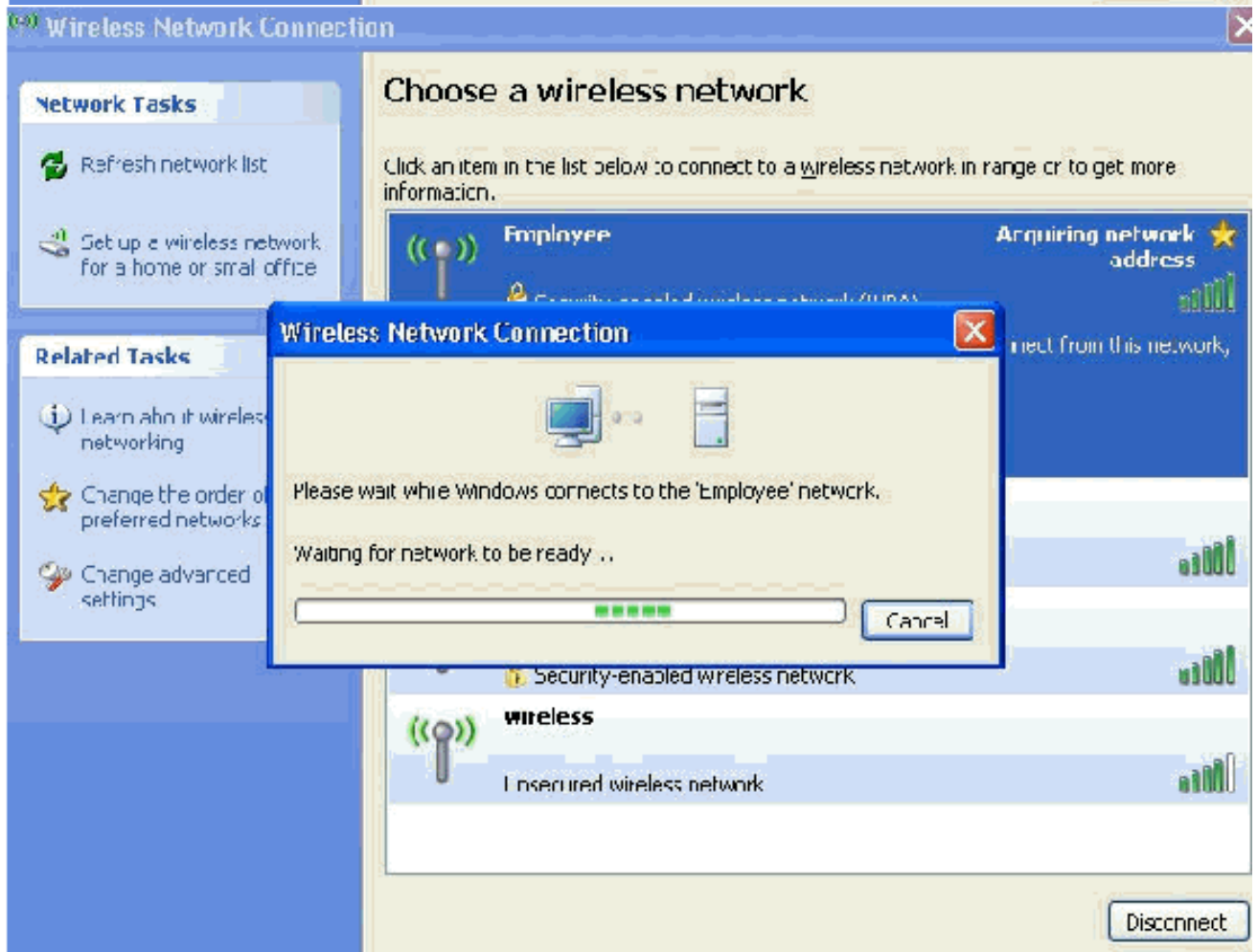
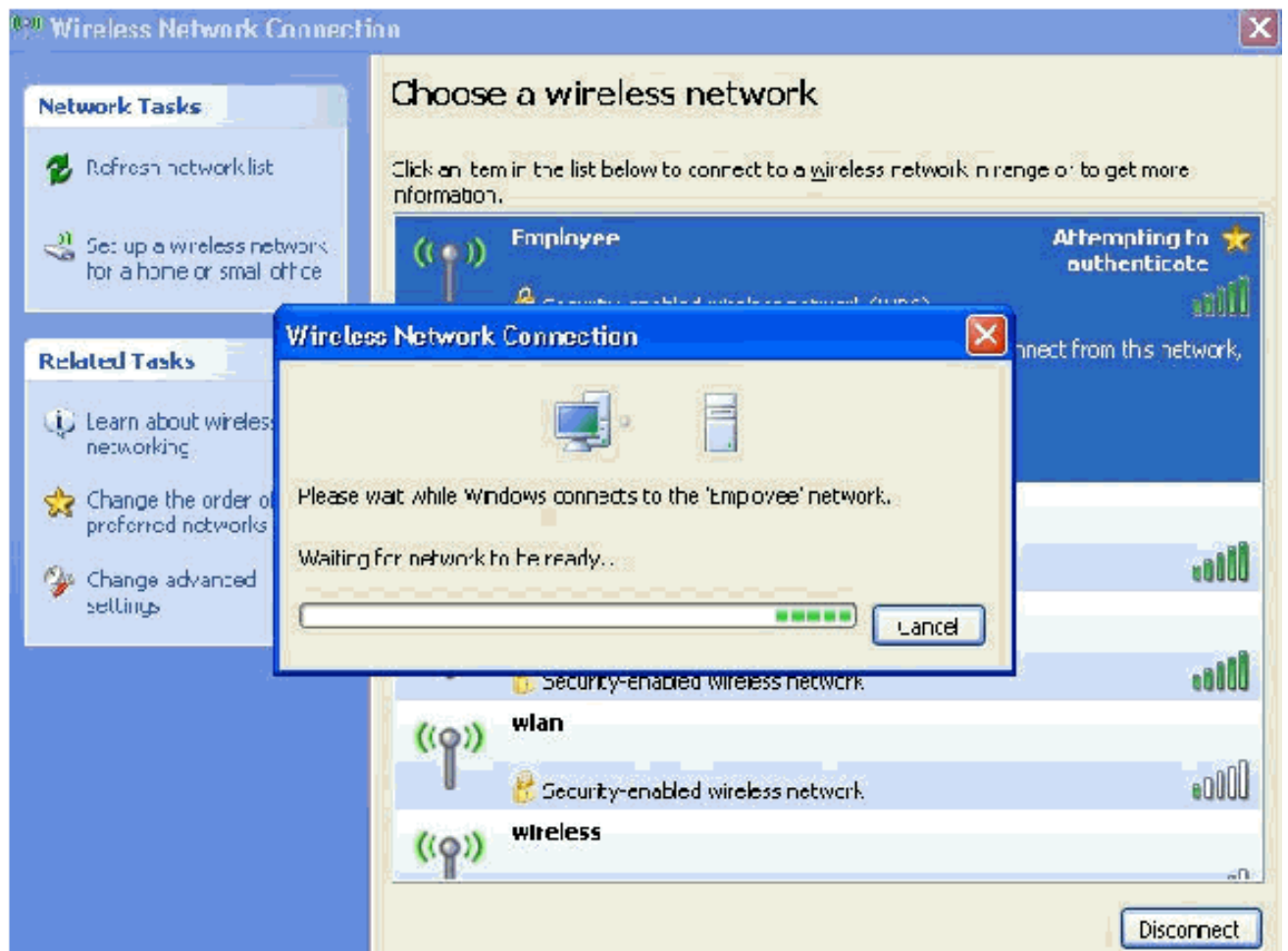


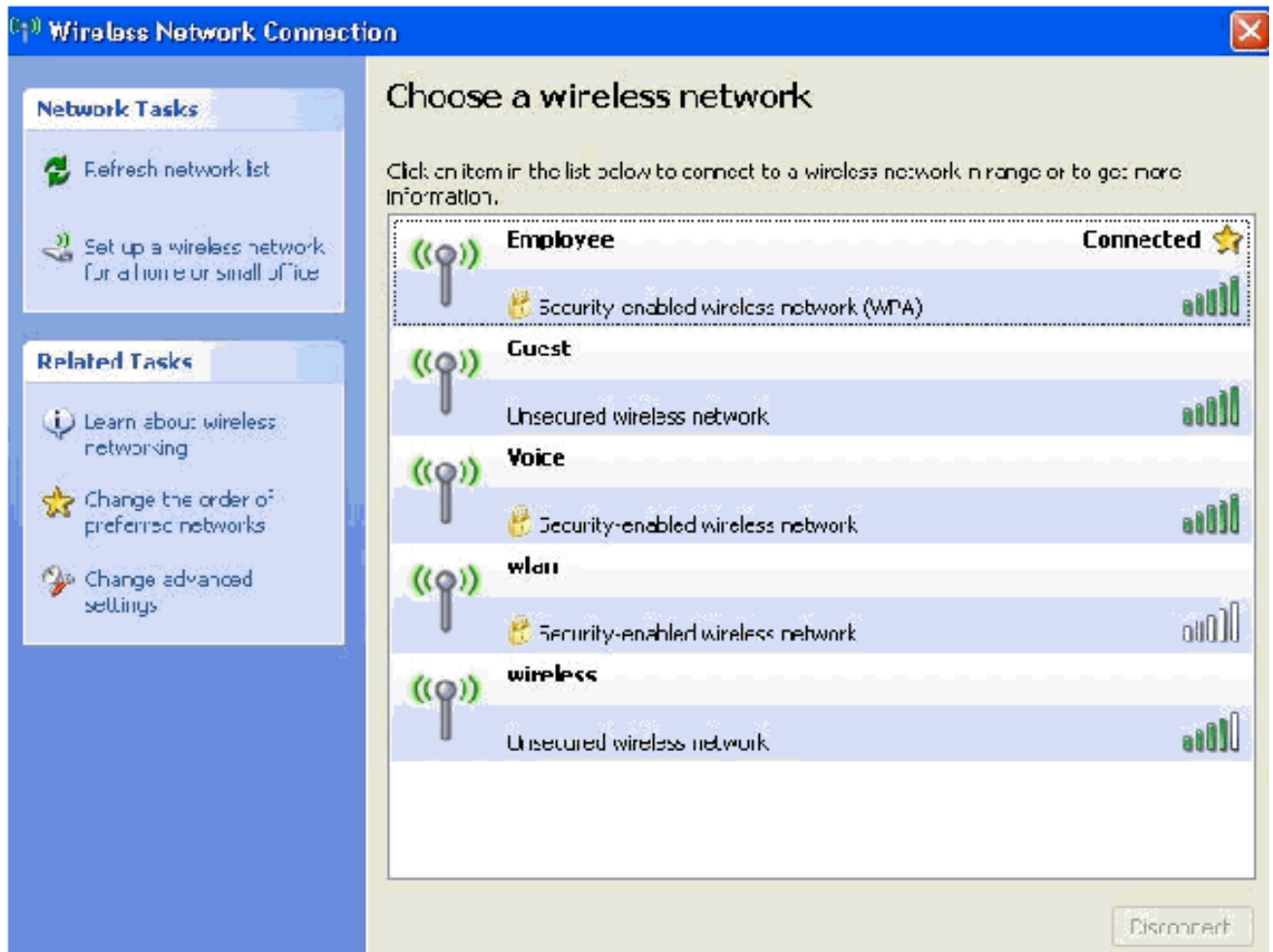
12. OK を 3 回クリックします。
13. システムトレイの無線ネットワーク接続のアイコンを右クリックして、View Available Wireless Networks をクリックします。
14. Employee の無線ネットワークをクリックし、Connect をクリックします。



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。







15. 認証が成功したら、Network Connections を使用して、無線アダプタの 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。
16. 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。

## 関連情報

- [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 コンフィギュレーション ガイド](#)
- [ワイヤレス LAN コントローラと 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](#)