

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Sample Configurations

PEAP Under Unified Wireless Networks with Microsoft Internet Authentication Service (IAS)

[TAC Notice: What's Changing on TAC Web](#)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[PEAP Overview](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Configure the Microsoft Windows 2003 Server](#)

[Configure the Microsoft Windows 2003 Server](#)

[Install and Configure DHCP Services on the Microsoft Windows 2003 Server](#)

[Install and Configure the Microsoft Windows 2003 Server as a Certificate Authority \(CA\) Server](#)

[Connect Clients to the Domain](#)

[Install the Internet Authentication Service on the Microsoft](#)

[Windows 2003 Server and Request a Certificate](#)

[Configure the Internet Authentication Service for PEAP-MS-CHAP v2 Authentication](#)

[Add Users to the Active Directory](#)

[Allow Wireless Access to Users](#)

[Configure the Wireless LAN Controller and Lightweight APs](#)

[Configure the WLC for RADIUS Authentication through MS IAS RADIUS Server](#)

[Configure a WLAN for the Clients](#)

[Configure the Wireless Clients](#)

[Configure the Wireless Clients for PEAP-MS CHAPv2 Authentication](#)

[Verify and Troubleshoot](#)

[NetPro Discussion Forums - Featured Conversations](#)

[Related Information](#)

Help us help you.

☐

Please rate this document.

☐ Excellent

☐ Good

☐ Average

☐ Fair

☐ Poor

☐

This document solved my problem.

☐ Yes

☐ No

☐ Just browsing

☐

Suggestions for improvement:

(256 character limit)

☐

Send

Introduction

This document provides a configuration example for setting up Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 2 authentication in a Cisco Unified Wireless network with the Microsoft Internet Authentication Service (IAS) as the RADIUS server.


Prerequisites

Requirements

There is an assumption that the reader has knowledge of basic Windows 2003 installation and Cisco controller installation since this document only covers the specific configurations to facilitate the tests.

Note: This document is intended to give the readers an example on the configuration required on MS server for PEAP – MS CHAP Authentication. The Microsoft server configuration presented in this section has been tested in the lab and found to be working as expected. If you have trouble configuring the Microsoft server, contact Microsoft for help. Cisco TAC does not support Microsoft Windows server configuration.

For initial installation and configuration information for the Cisco 4400 Series Controllers, refer to the [Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers](#).

Microsoft Windows 2003 installation and configuration guides can be found at [Installing Windows Server 2003 R2](#) .

Before you begin, install the Microsoft Windows Server 2003 with SP1 operating system on each of the servers in the test lab and update all Service Packs. Install the controllers and lightweight access points (LAPs) and ensure that the latest software updates are configured.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 4400 Series Controller that runs firmware Version 4.0
- Cisco 1131 Lightweight Access Point Protocol (LWAPP) AP
- Windows 2003 Enterprise server (SP1) with Internet Authentication Service (IAS), Certificate Authority (CA), DHCP, and Domain Name System (DNS) services installed
- Windows XP Professional with SP 2 (and updated Service Packs) and Cisco Aironet 802.11a/b/g Wireless network interface card (NIC)
- Aironet Desktop Utility Version 4.0
- Cisco 3560 Switch

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

PEAP Overview

PEAP uses Transport Level Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a Wireless laptop, and a PEAP authenticator, such as Microsoft Internet Authentication Service (IAS) or any RADIUS server. PEAP does not specify an authentication method, but provides additional security for other EAP authentication protocols, such as EAP-MSCHAPv2, that can operate through the TLS encrypted channel provided by PEAP. The PEAP authentication process consists of two main phases:

PEAP phase one: TLS encrypted channel

The Wireless client associates with the AP. An IEEE 802.11-based association provides an Open System or Shared Key authentication before a secure association is created between the client and Access Point (LAP). After the IEEE 802.11-based association is successfully established between the client and the Access Point, the TLS session is negotiated with the AP. After authentication is successfully completed between the Wireless client and IAS server, the TLS session is negotiated between them. The key that is derived within this negotiation is used to encrypt all subsequent communication.

PEAP phase two: EAP-authenticated communication

EAP communication, which includes EAP negotiation, occurs inside the TLS channel created by PEAP within the first stage of the PEAP authentication process. The IAS server authenticates the Wireless client with EAP-MS-CHAP v2. The LAP and the Controller only forward messages between the Wireless client and RADIUS server. The WLC and the LAP cannot decrypt these messages because it is not the TLS end point.

After PEAP stage one occurs, and the TLS channel is created between the IAS server and the 802.1X Wireless client, for a successful authentication attempt where the user has supplied valid password-based credentials with PEAP-MS-CHAP v2, the RADIUS message sequence is this:

1. The IAS server sends an identity request message to the client: EAP-Request/Identity.
2. The client responds with an identity response message: EAP-Response/Identity.
3. The IAS server sends an MS-CHAP v2 challenge message: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
4. The client responds with an MS-CHAP v2 challenge and response: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. The IAS server sends back an MS-CHAP v2 success packet when the server has successfully authenticated the client: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success).
6. The client responds with an MS-CHAP v2 success packet when the client has successfully

authenticated the server: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success).

7. The IAS server sends an EAP-TLV that indicates successful authentication.
8. The client responds with an EAP-TLV status success message.
9. The server completes authentication and sends an EAP-Success message using plaintext. If VLANs are deployed for client isolation, the VLAN attributes are included in this message.

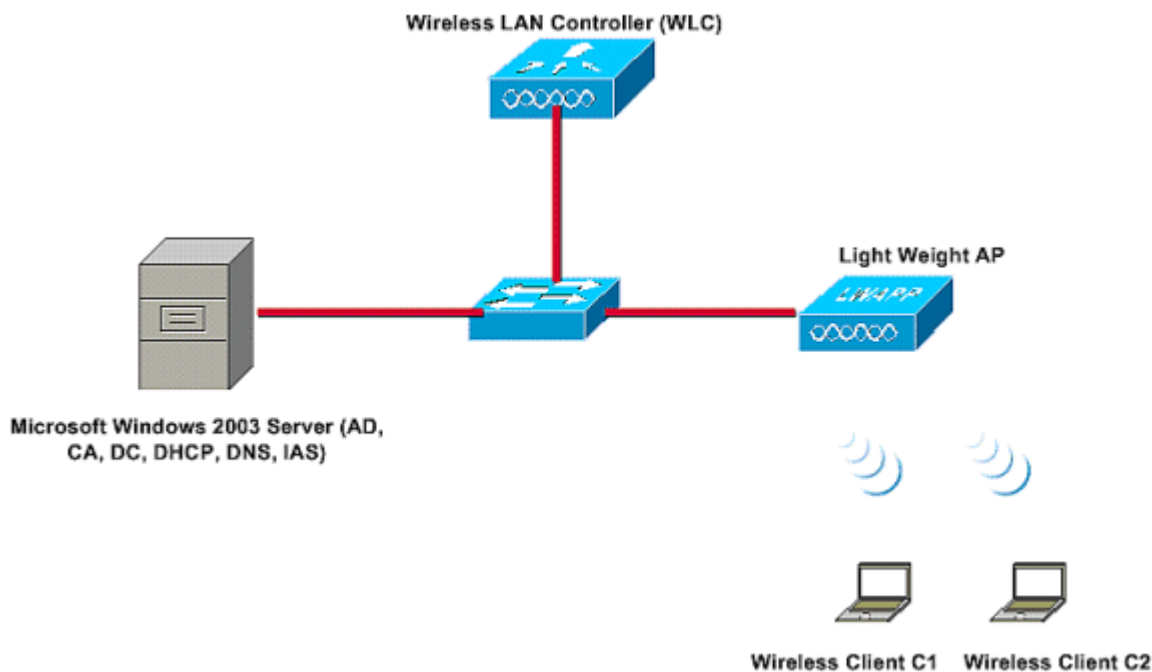
Configure

This document provides an example for the configuration of PEAP MS-CHAP v2.

Note: Use the [Command Lookup Tool](#) ([registered](#) customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



In this setup, a Microsoft Windows 2003 server performs these roles:

- Domain controller for the domain **Wireless.com**
- DHCP/DNS server
- Certificate Authority (CA) server
- Active Directory – to maintain the user database

- Internet Authentication Service (IAS) – to authenticate the Wireless users

This server connects to the wired network through a Layer 2 switch as shown.

The Wireless LAN Controller (WLC) and the registered LAP also connect to the network through the Layer 2 switch.

Wireless clients C1 and C2 will use Wi-Fi Protected Access 2 (WPA2) - PEAP MSCHAP v2 authentication to connect to the Wireless network.

The objective is to configure the Microsoft 2003 server, Wireless LAN Controller, and Light Weight AP to authenticate the Wireless clients with PEAP MSCHAP v2 authentication.

The next section explains how to configure the devices for this setup.

Configurations

This section looks at the configuration required to setup PEAP MS-CHAP v2 Authentication in this WLAN:

- Configure the Microsoft Windows 2003 Server
- Configure the Wireless LAN Controller (WLC) and the Light Weight APs
- Configure the Wireless Clients

Start with the configuration of the Microsoft Windows 2003 server.

Configure the Microsoft Windows 2003 Server

Configure the Microsoft Windows 2003 Server

As mentioned in the Network setup section, use the Microsoft Windows 2003 server in the network to perform these functions.

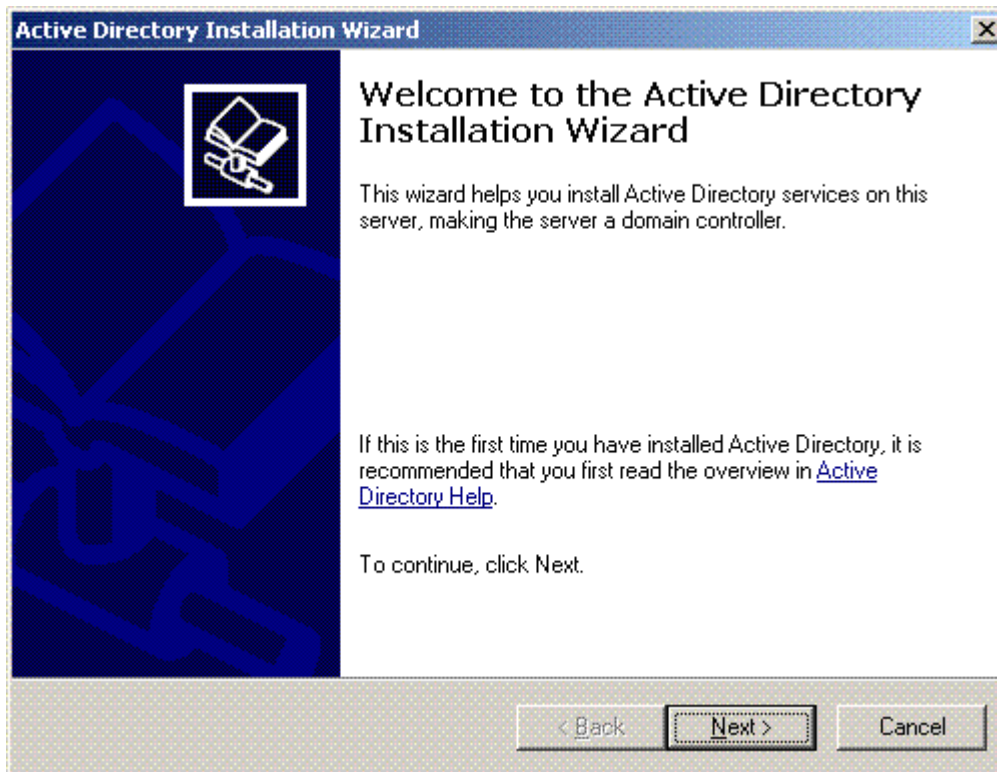
- **Domain controller** – for the domain **Wireless**
- **DHCP/DNS server**
- **Certificate Authority (CA) server**
- **Internet Authentication Service (IAS)** – to authenticate the Wireless users
- **Active Directory** – to maintain the user database

Configure the Microsoft Windows 2003 server for these services. Begin with the configuration of the Microsoft Windows 2003 server as a Domain Controller.

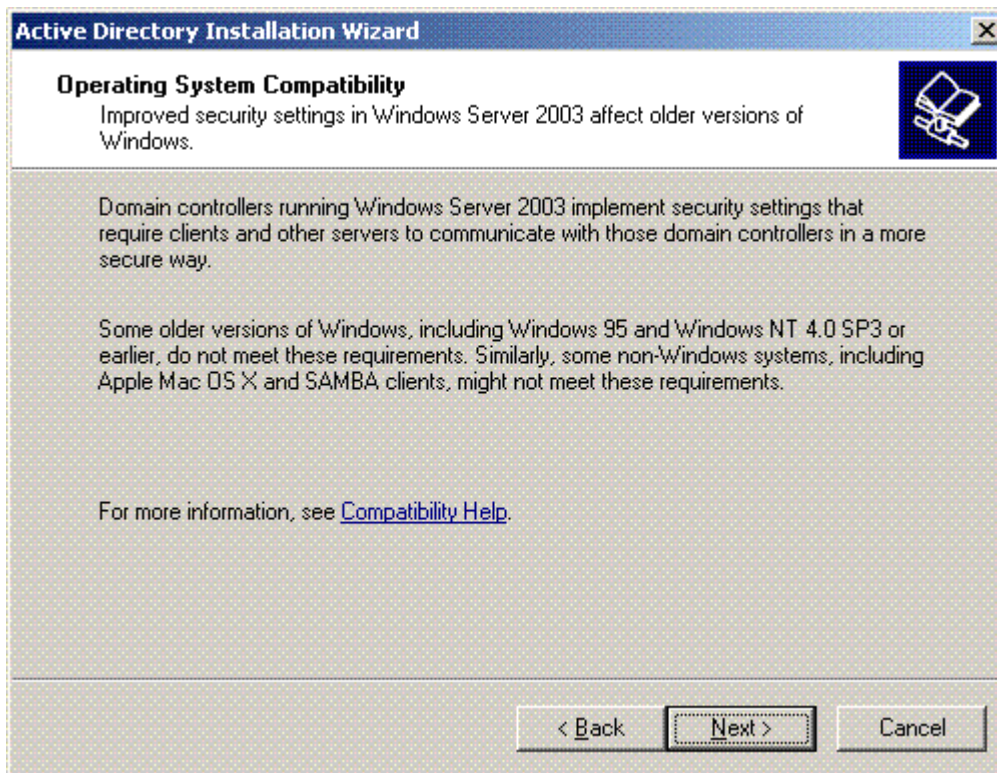
Configure the Microsoft Windows 2003 server as a Domain Controller

In order to configure the Microsoft Windows 2003 server as a Domain Controller, complete these steps:

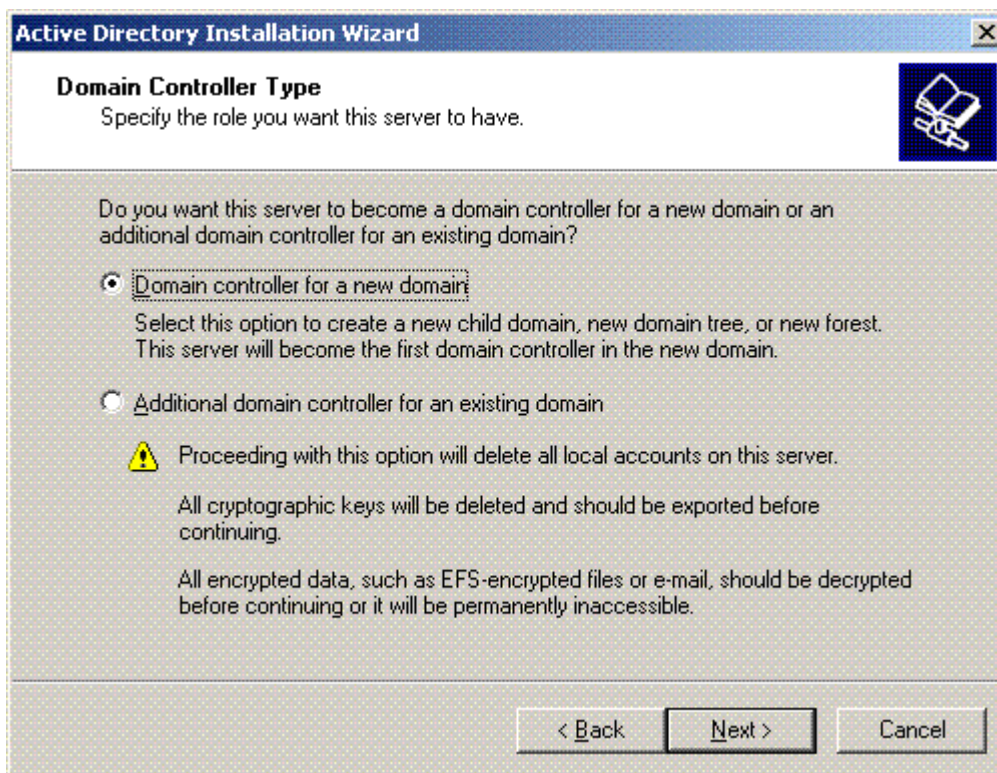
1. Click **Start**, click **Run**, type **dcpromo.exe**, and then click **OK** to start the Active Directory Installation Wizard.



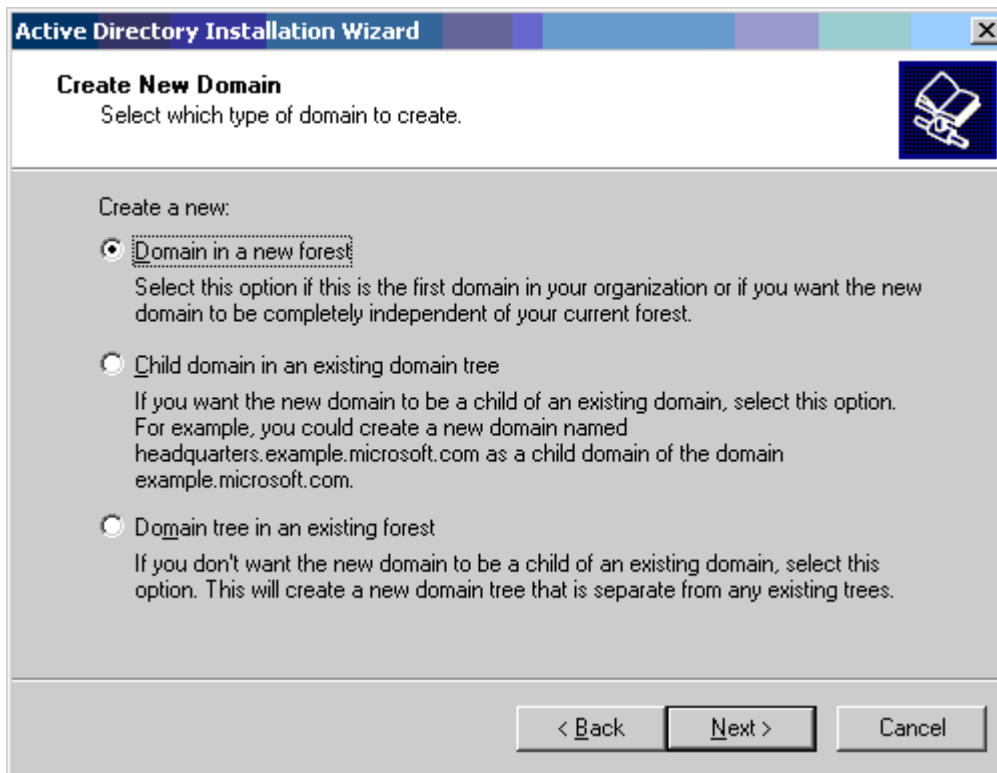
2. Click **Next** to run the Active Directory Installation Wizard.



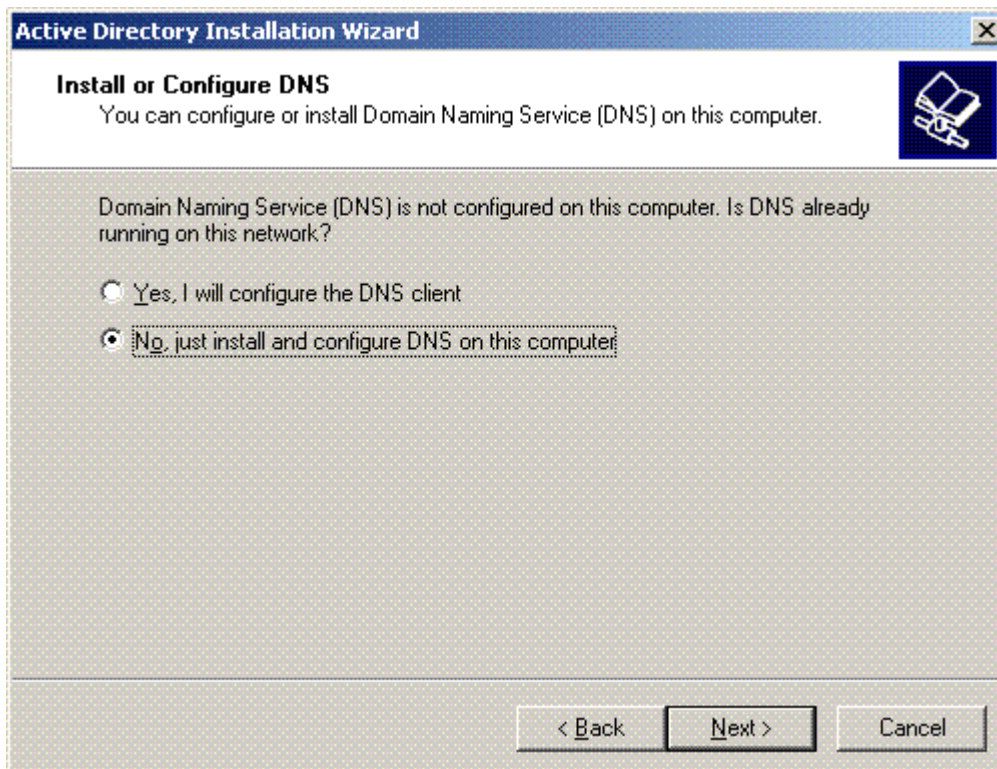
3. In order to create a new domain, choose the option **Domain Controller** for a new domain.



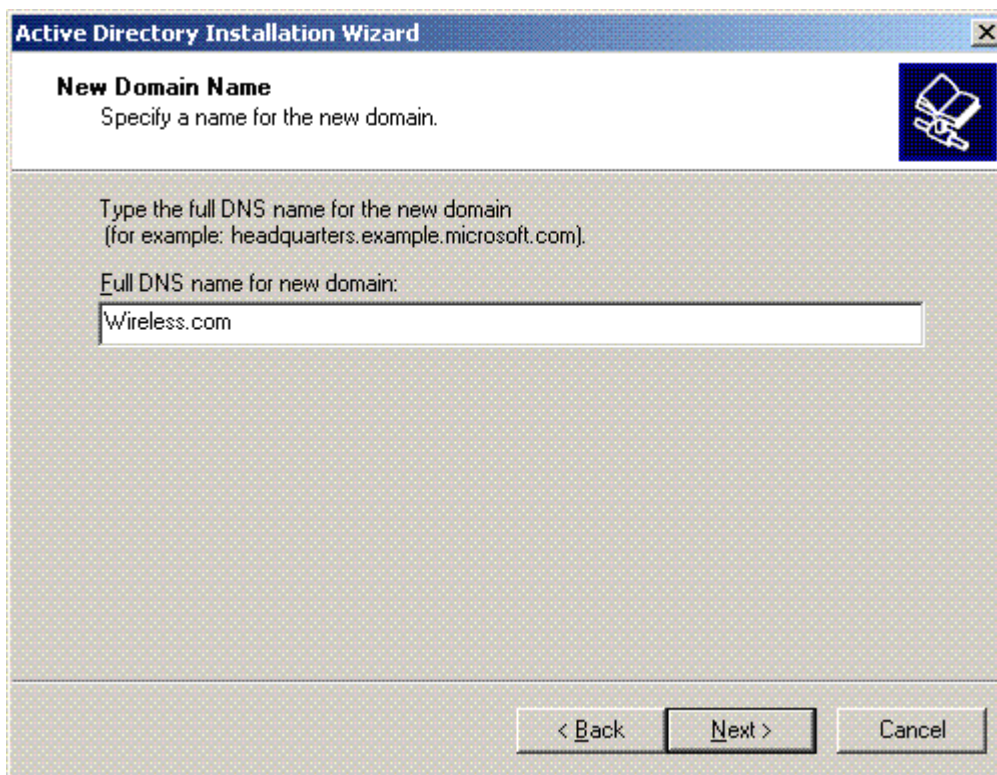
4. Click **Next** to create a new forest of domain trees.



5. If DNS is not installed on the system, the wizard provides you options with which to configure DNS. Choose **No, Just Install and Configure DNS** on this computer. Click **Next**.

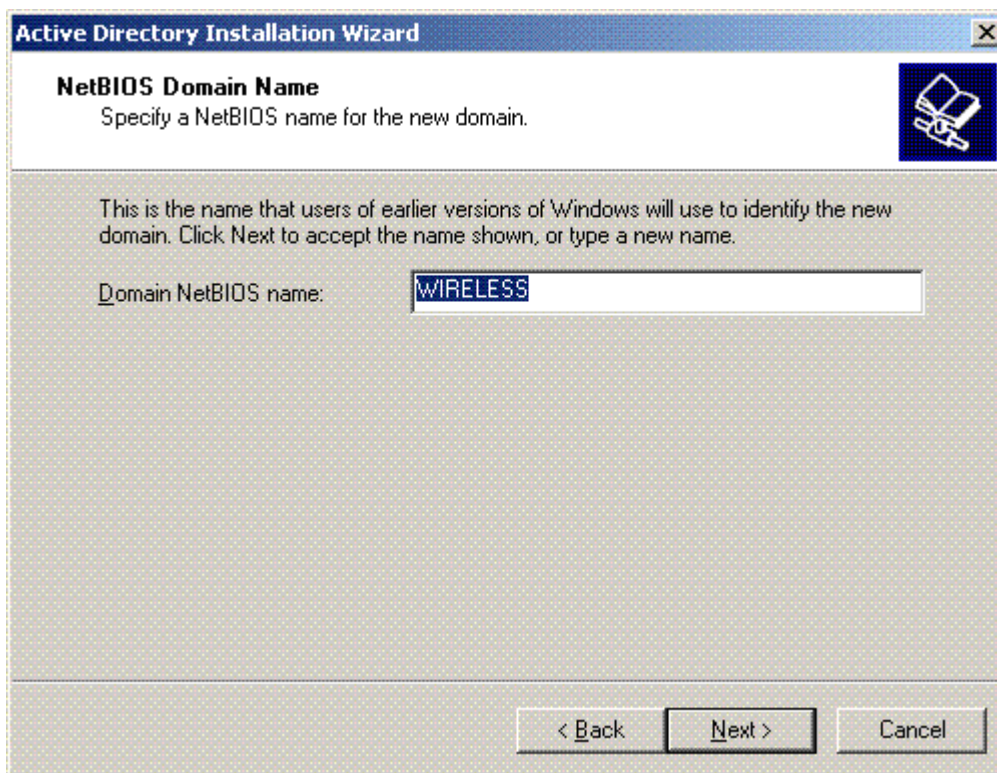


6. Type the full DNS name for the new domain. In this example **Wireless.com** is used and click **Next**.



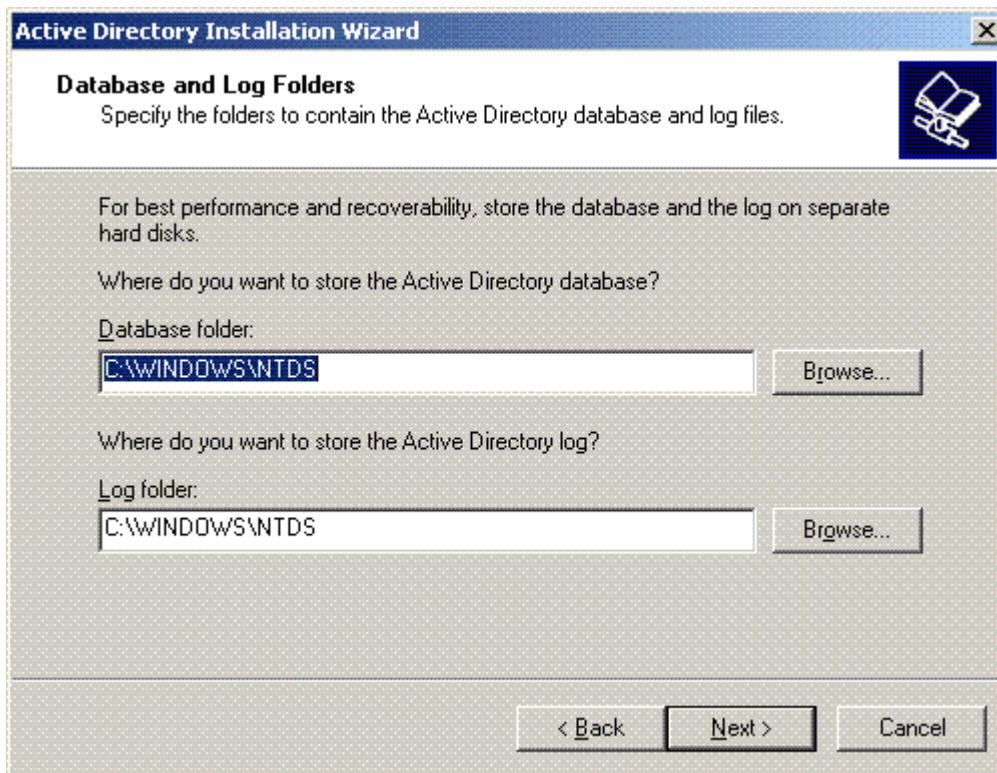
The screenshot shows the 'Active Directory Installation Wizard' window. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'New Domain Name' with the instruction 'Specify a name for the new domain.' Below this, it says 'Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).' A text box labeled 'Full DNS name for new domain:' contains the text 'wireless.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

7. Enter the NETBIOS name for the domain and click **Next**. This example uses **WIRELESS**.



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'NetBIOS Domain Name' with the instruction 'Specify a NetBIOS name for the new domain.' Below this, it says 'This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.' A text box labeled 'Domain NetBIOS name:' contains the text 'WIRELESS'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

8. Choose the database and log locations for the domain. Click **Next**.



Active Directory Installation Wizard

Database and Log Folders
Specify the folders to contain the Active Directory database and log files.

For best performance and recoverability, store the database and the log on separate hard disks.

Where do you want to store the Active Directory database?

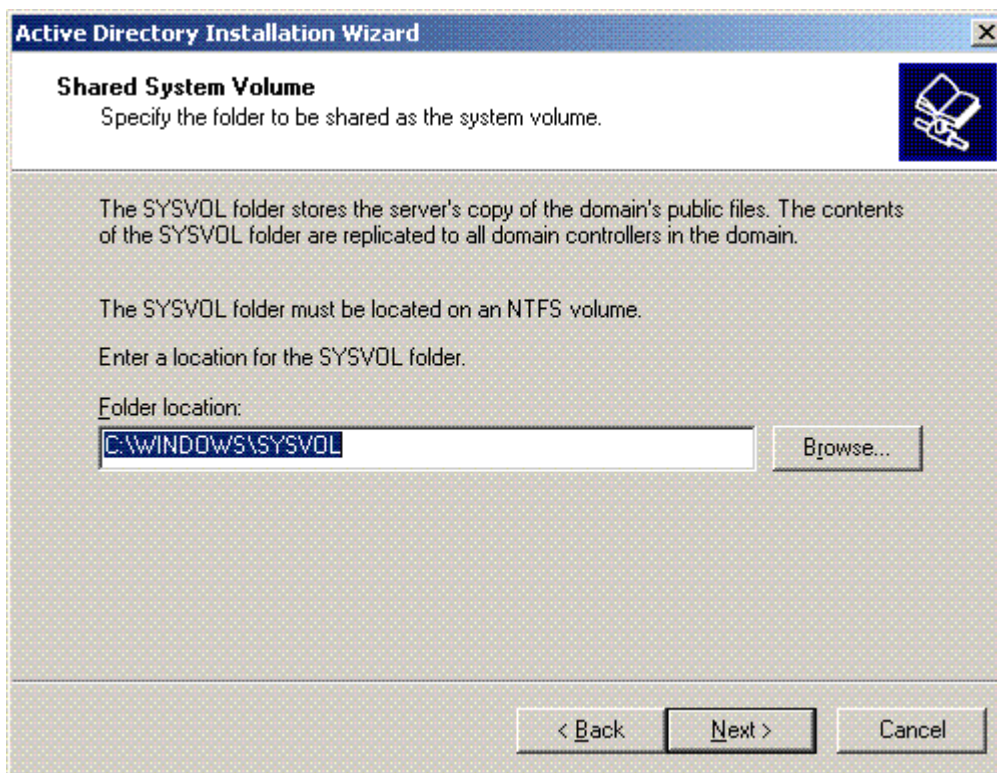
Database folder:

Where do you want to store the Active Directory log?

Log folder:

< Back Next > Cancel

9. Choose a location for the Sysvol folder. Click **Next**.



Active Directory Installation Wizard

Shared System Volume
Specify the folder to be shared as the system volume.

The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.

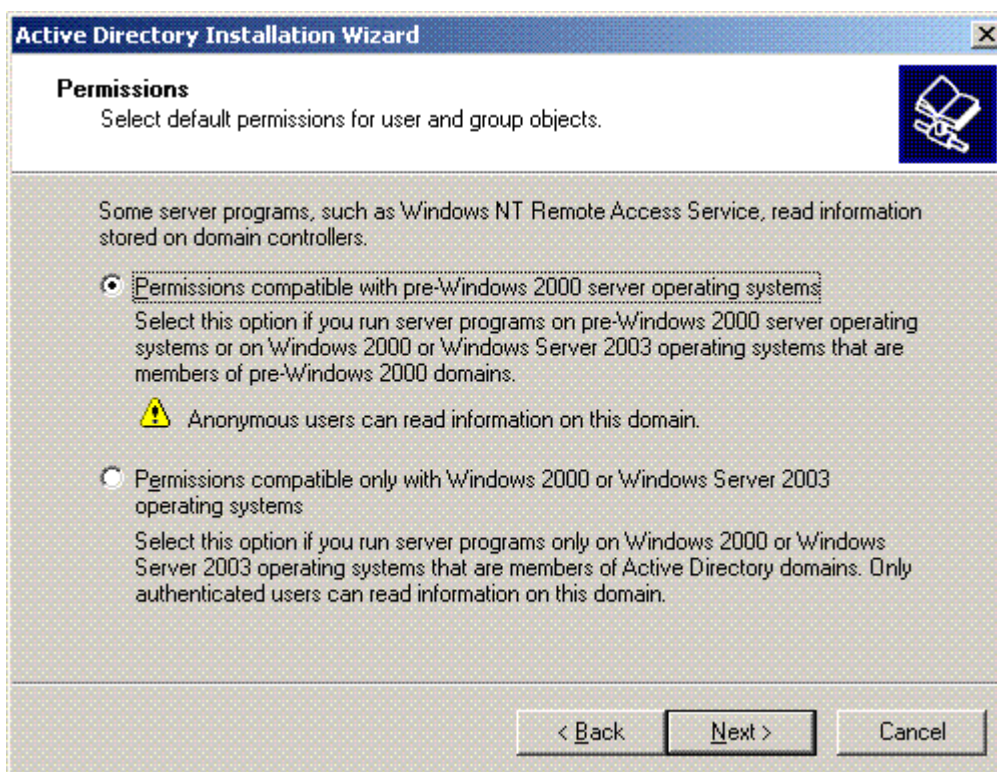
The SYSVOL folder must be located on an NTFS volume.

Enter a location for the SYSVOL folder.

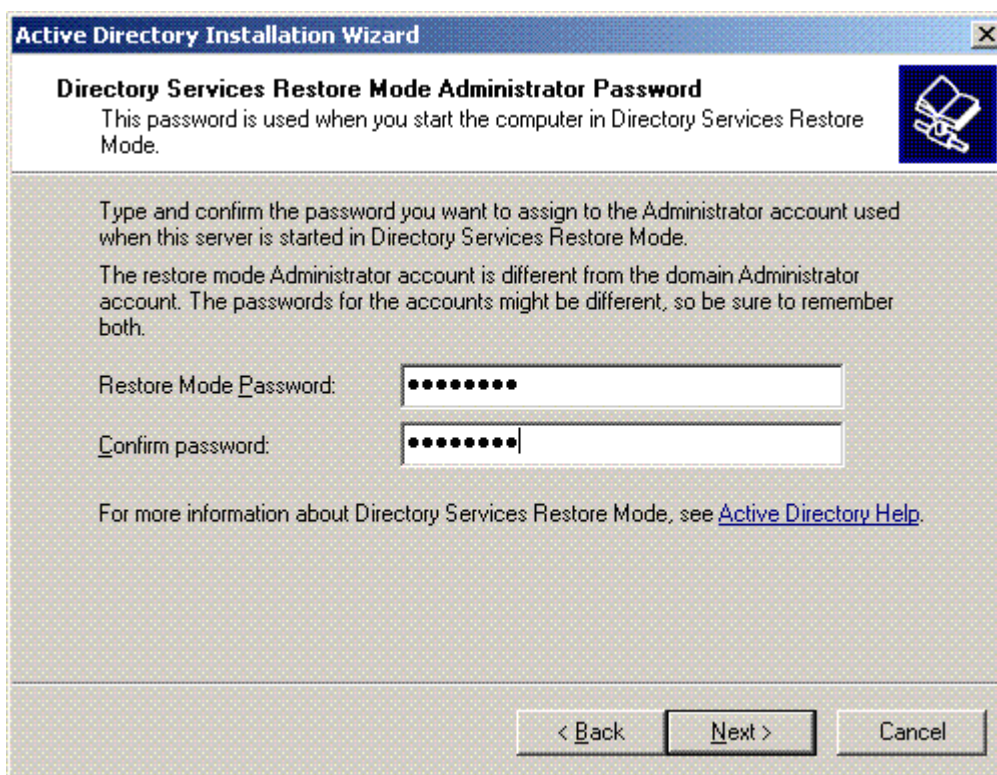
Folder location:

< Back Next > Cancel

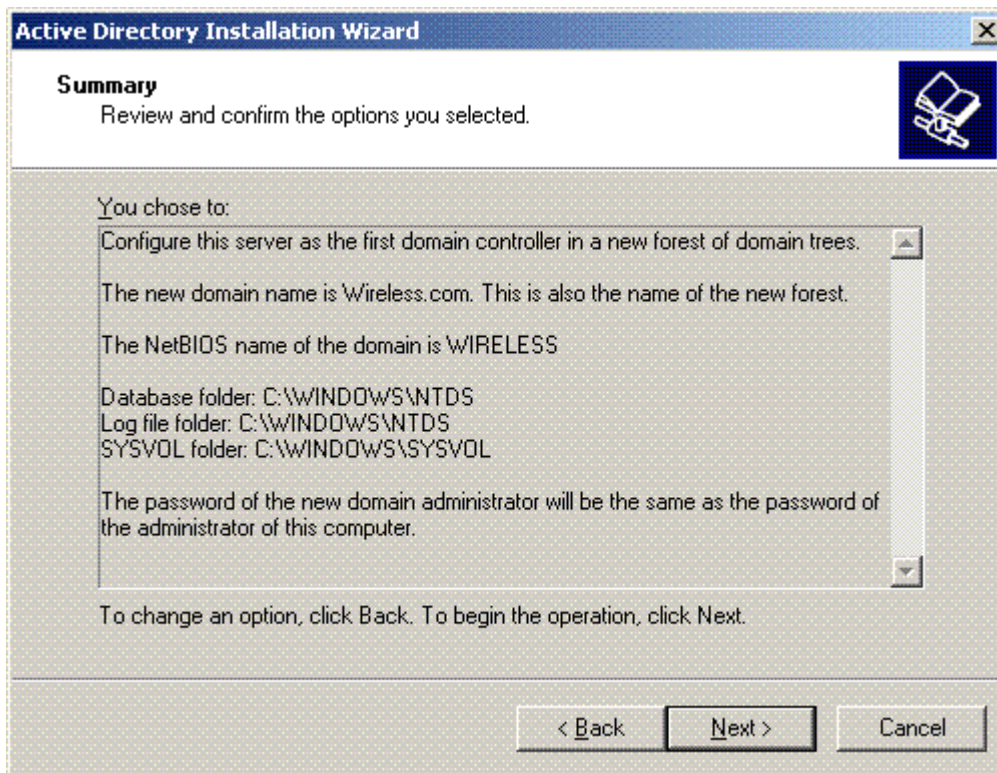
10. Choose the default permissions for the users and groups. Click **Next**.



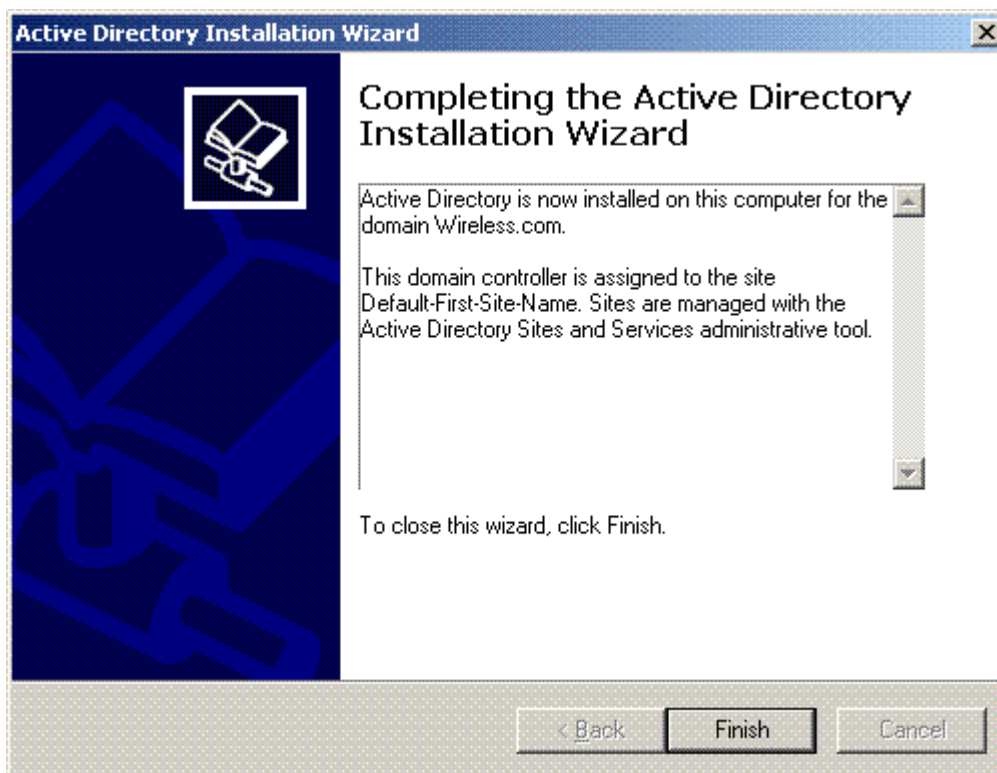
11. Set the Administrator Password and click **Next**.



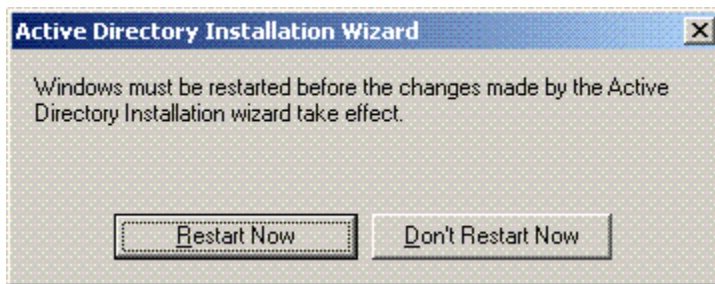
12. Click **Next** to accept the Domain Options set previously.



13. Click **Finish** to close the Active Directory Installation Wizard.



14. Restart the server for the changes to take effect.

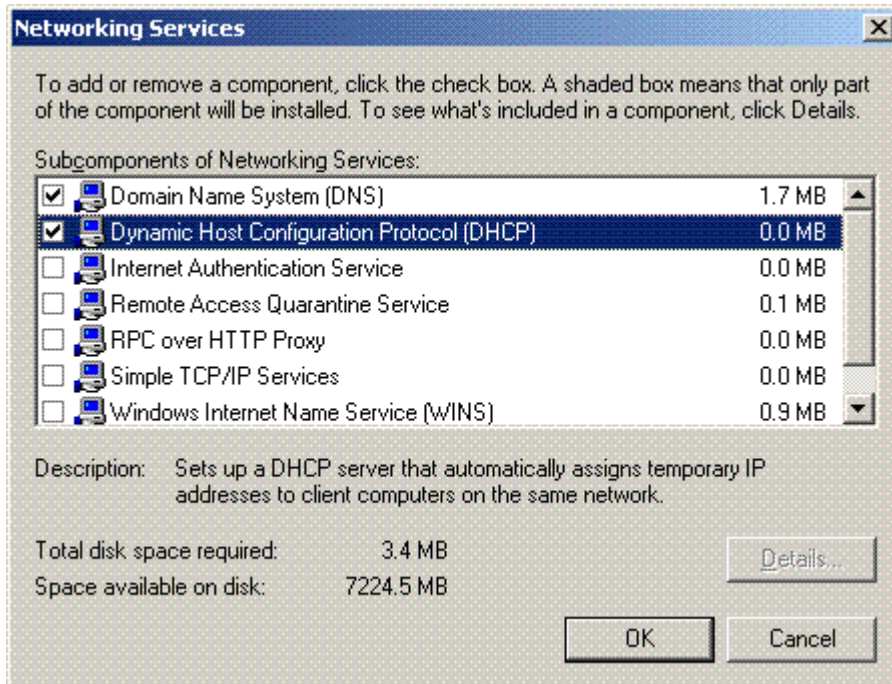


With this step, you have configured the Microsoft Windows 2003 server as a Domain controller and created a new domain **Wireless.com**. Next configure DHCP services on the server.

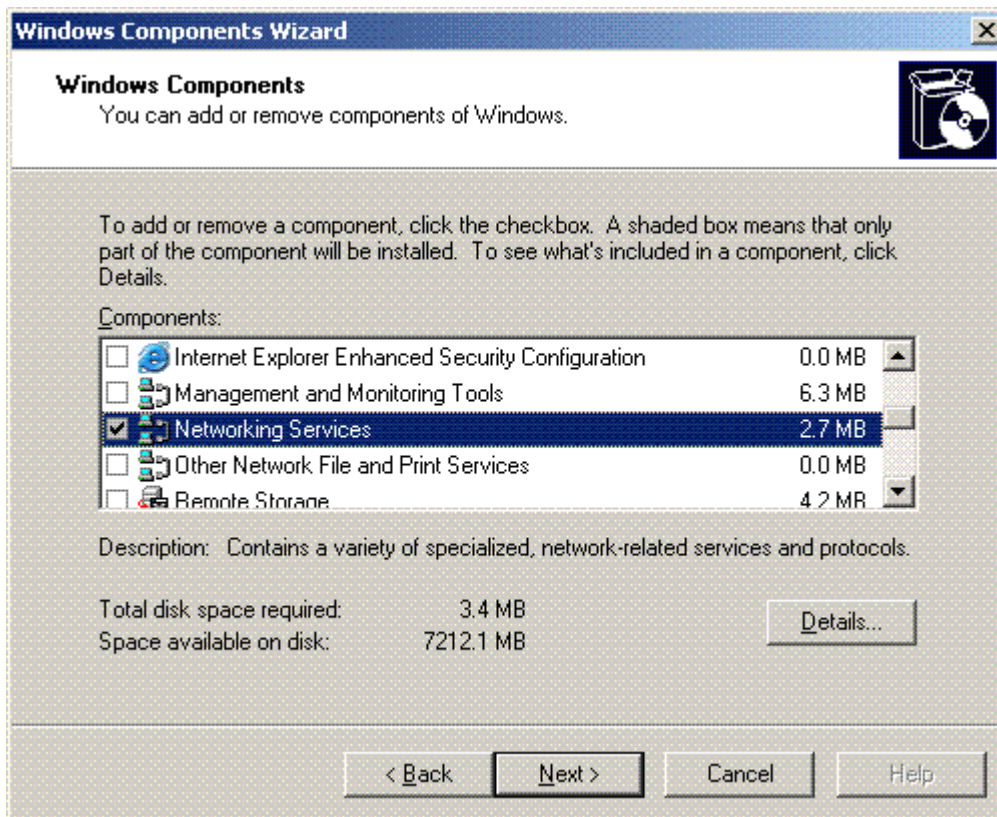
Install and Configure DHCP Services on the Microsoft Windows 2003 Server

The DHCP service on the Microsoft 2003 server is used to provide IP addresses to the Wireless clients. In order to install and configure DHCP services on this server, complete these steps:

1. Click **Add or Remove Programs** in the Control Panel.
2. Click **Add/Remove Windows Components**.
3. Choose **Networking Services** and click **Details**.
4. Choose **Dynamic Host Configuration Protocol (DHCP)** and click **OK**.



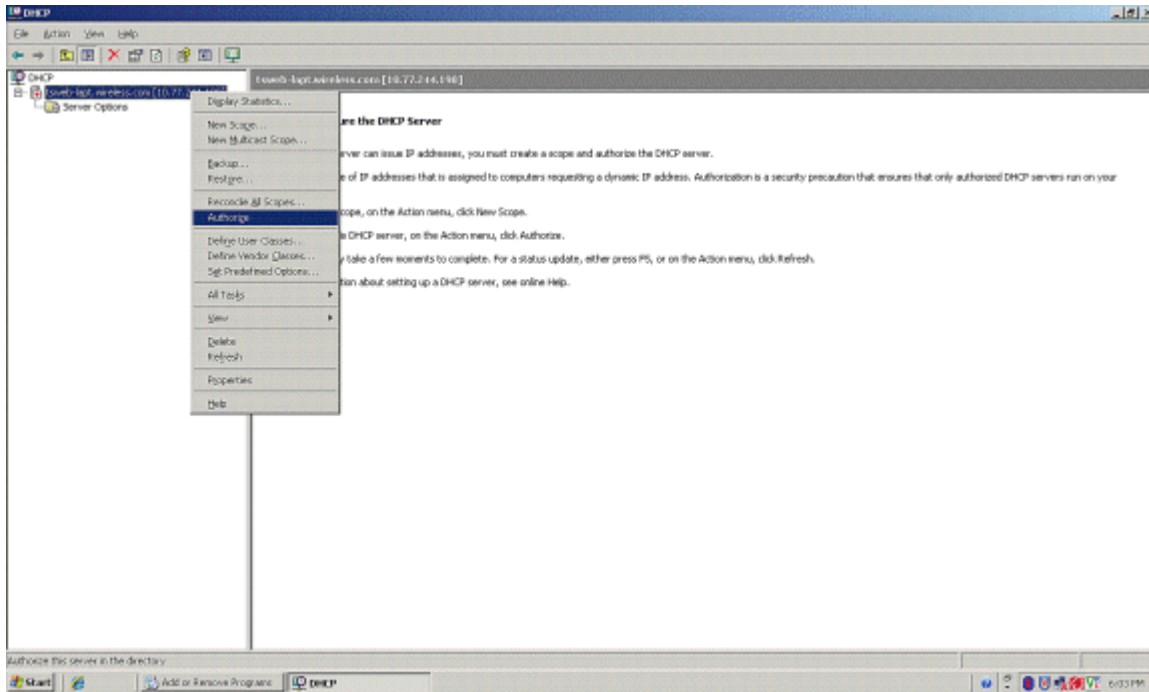
5. Click **Next** to install the DHCP service.



6. Click **Finish** to complete the installation.



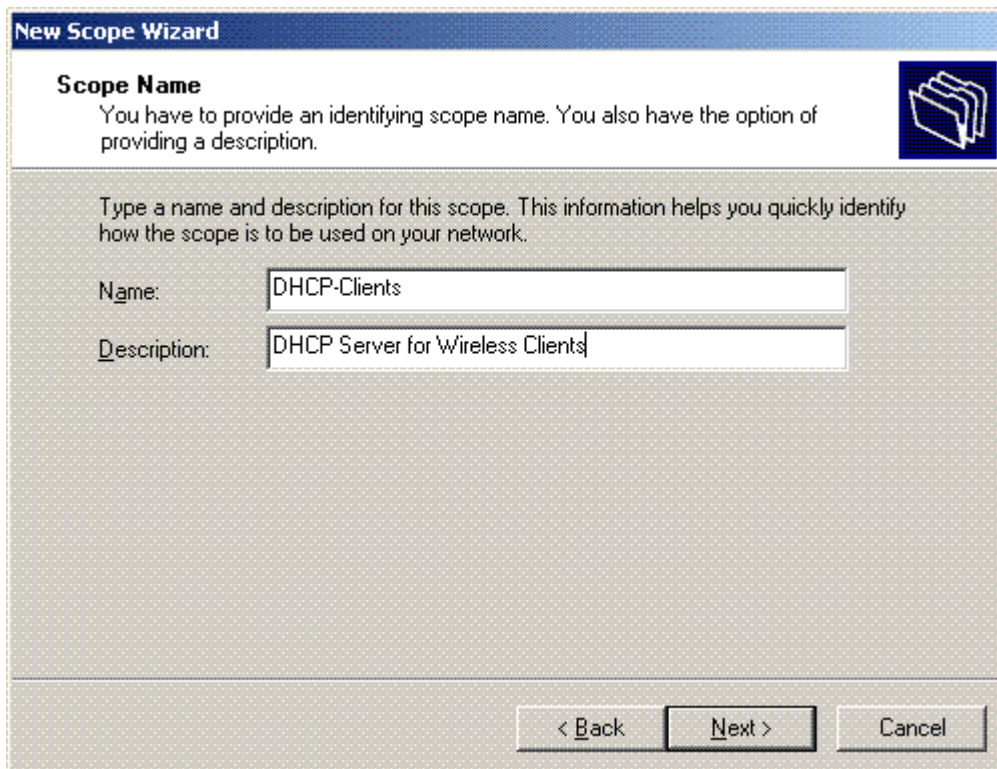
7. In order to configure DHCP services, click **Start > Programs > Administrative tools** and click the **DHCP** snap-in.
8. Choose the DHCP server - **tsweb-lapt.wireless.com** (in this example).
9. Click **Action** and then click **Authorize** to authorize DHCP service.



10. In the Console tree, right-click **tsweb-lapt.wireless.com** and then click **New Scope** to define an IP address range for the Wireless clients.
11. On the Welcome to the New Scope Wizard page of the New Scope Wizard, click **Next**.



12. On the Scope Name page, type the name of the DHCP scope. In this example, use **DHCP-Clients** as the scope name. Click **Next**.



13. On the IP Address Range page, enter the start and end IP addresses for the scope, and click **Next**.

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. On the Add Exclusions page, mention the IP address that you would like to reserve/exclude from the DHCP scope. Click **Next**.

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.

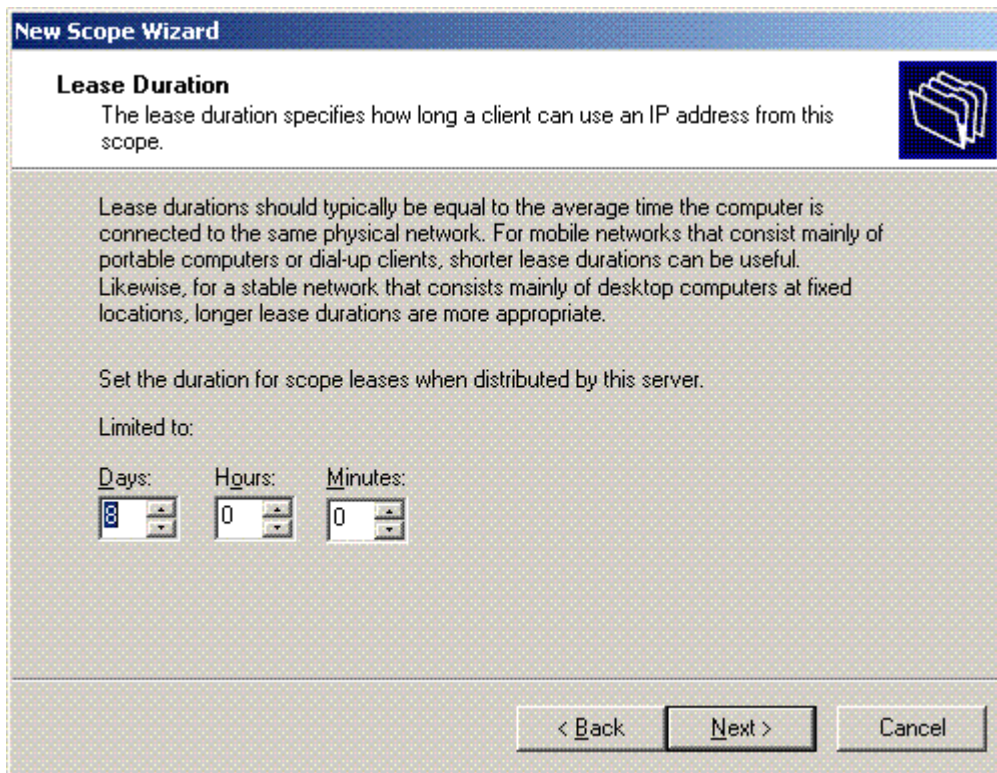
Start IP address: . . . End IP address: . . . Add

Excluded address range:

Remove

< Back Next > Cancel

15. Mention the lease duration in the Lease Duration page, and click **Next**.



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.

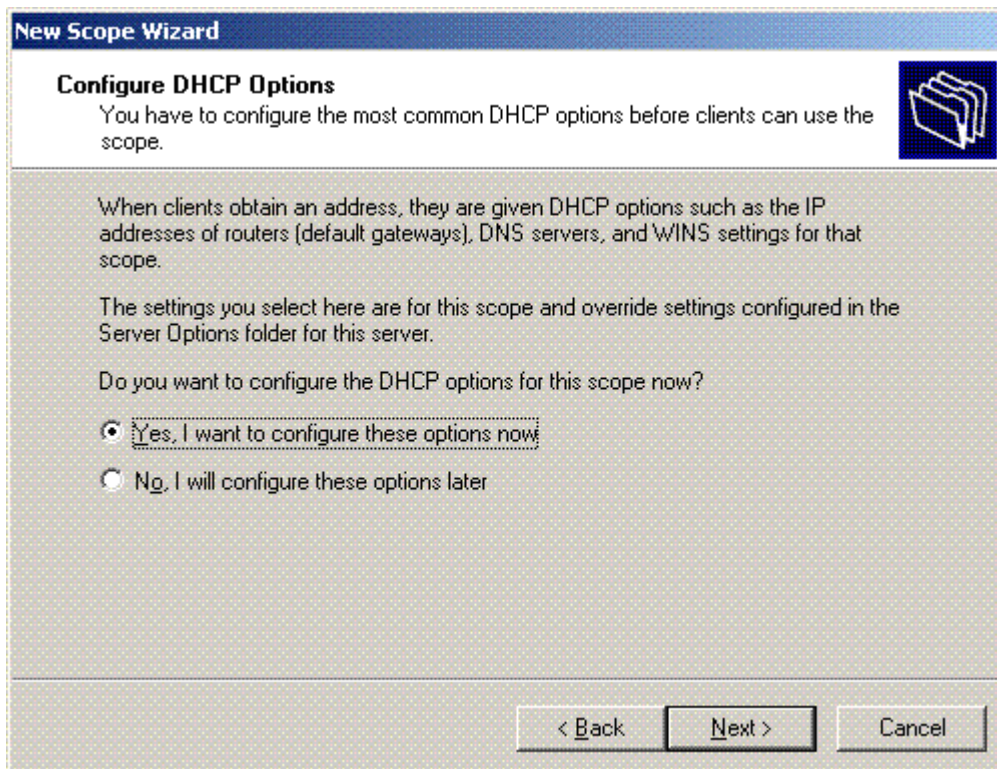
Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back Next > Cancel

16. On the Configure DHCP options page, choose **Yes, I want to configure DHCP Option now**, and click **Next**.



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

17. If there is default gateway router, mention the IP address of the gateway router in the Router (Default Gateway) page, and click **Next**.

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:

.

.

.

10.77.244.220

Add

Remove

Up

Down

< Back

Next >


Cancel

- On the Domain Name and DNS servers page, type the name of the domain that was configured previously. In the example, use **Wireless.com**. Enter the IP address of the server. Click **Add**.

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:

.

.

.

10.77.244.217

Add

Remove

Up

Down

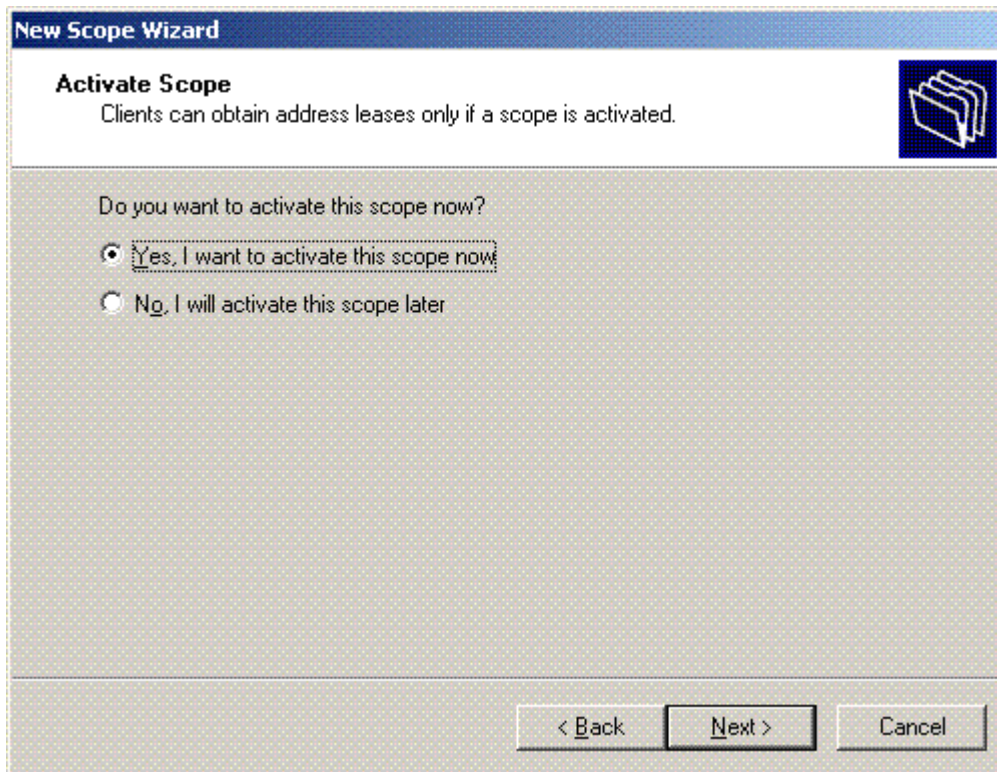
< Back

Next >

Cancel

19. Click **Next**.

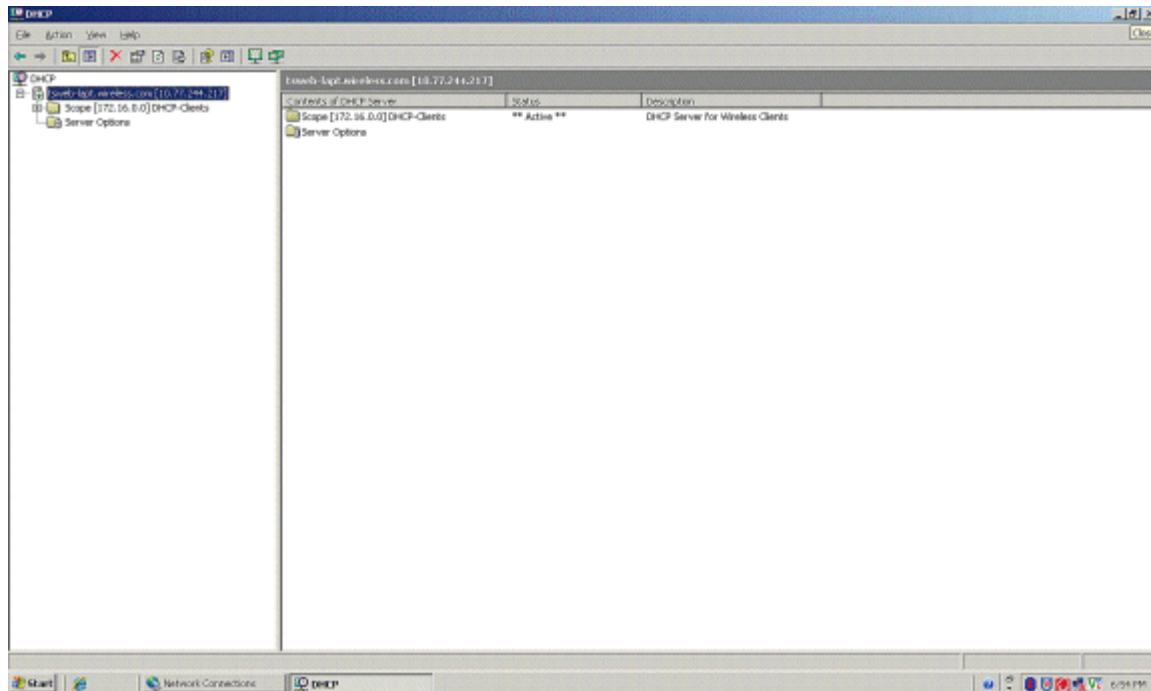
20. On the WINS Server page, click **Next**.
21. On the Activate Scope page, choose **Yes, I want to activate the scope now**, and click **Next**.



22. On completing the New Scope Wizard, click **Finish**.



23. In the DHCP Snapin window, verify that the DHCP scope that was created is active.



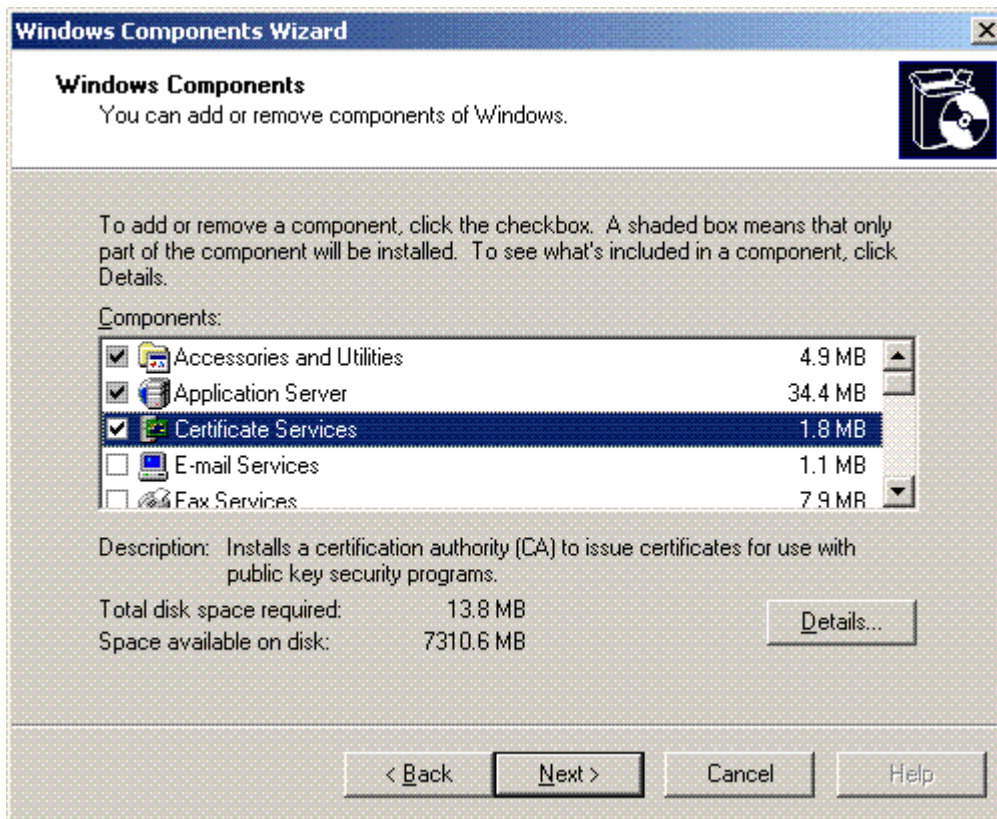
Now that the DHCP/ DNS is enabled on the server, configure the server as an enterprise Certificate Authority (CA) server.

Install and Configure the Microsoft Windows 2003 Server as a Certificate Authority (CA) Server

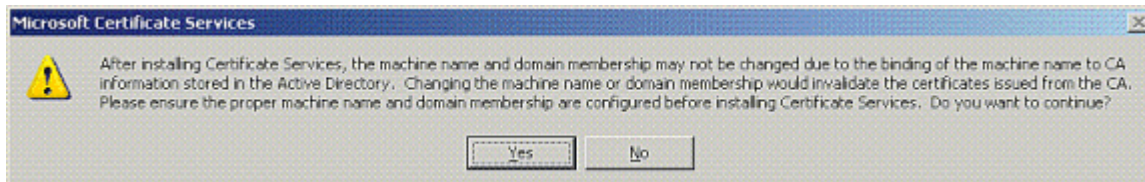
PEAP with EAP-MS-CHAPv2 validates the RADIUS server based on the certificate present on the server. Additionally, the server certificate must be issued by a public certification authority (CA) that is trusted by the client computer (that is, the public CA certificate already exists in the Trusted Root Certification Authority folder on the client computer certificate store). In this example, configure the Microsoft Windows 2003 server as a Certificate Authority (CA) that issues the certificate to the Internet Authentication Service (IAS).

In order to install and configure the certificate services on the server, complete these steps:

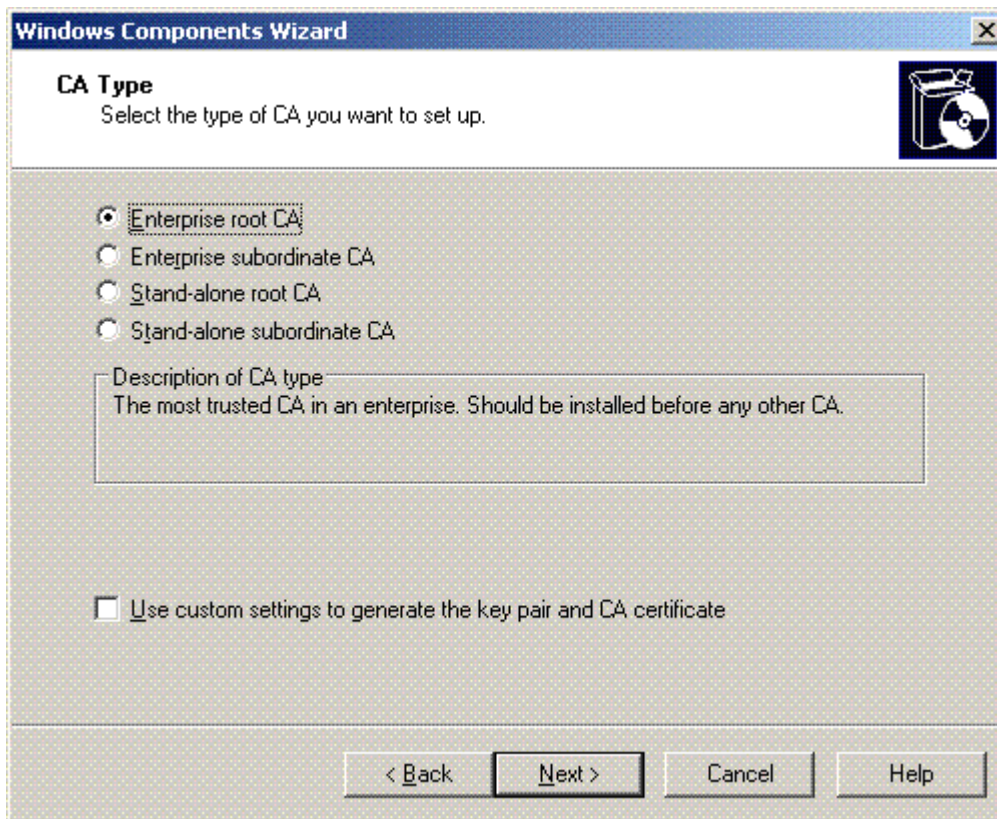
1. Click **Add or Remove programs in Control Panel**.
2. Click **Add/Remove Windows components**.
3. Click **Certificate Services**.



- Click **Yes** to the warning message, **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?**

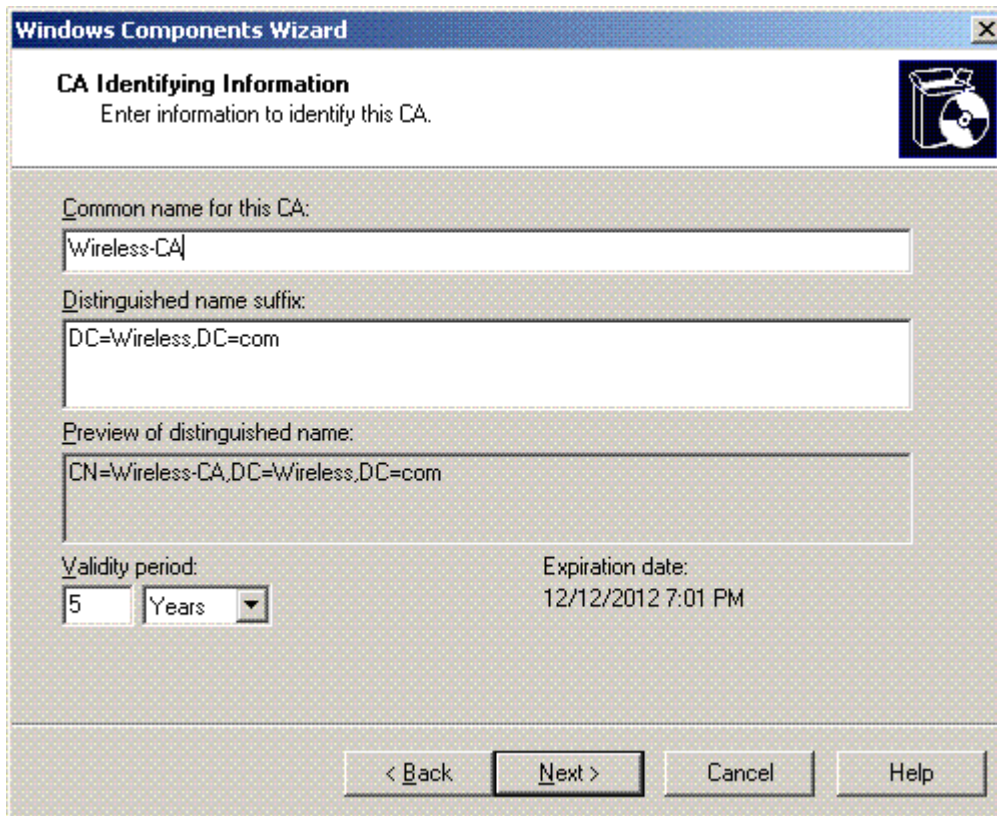


- Under Certificate Authority Type, choose **Enterprise root CA**, and click **Next**.



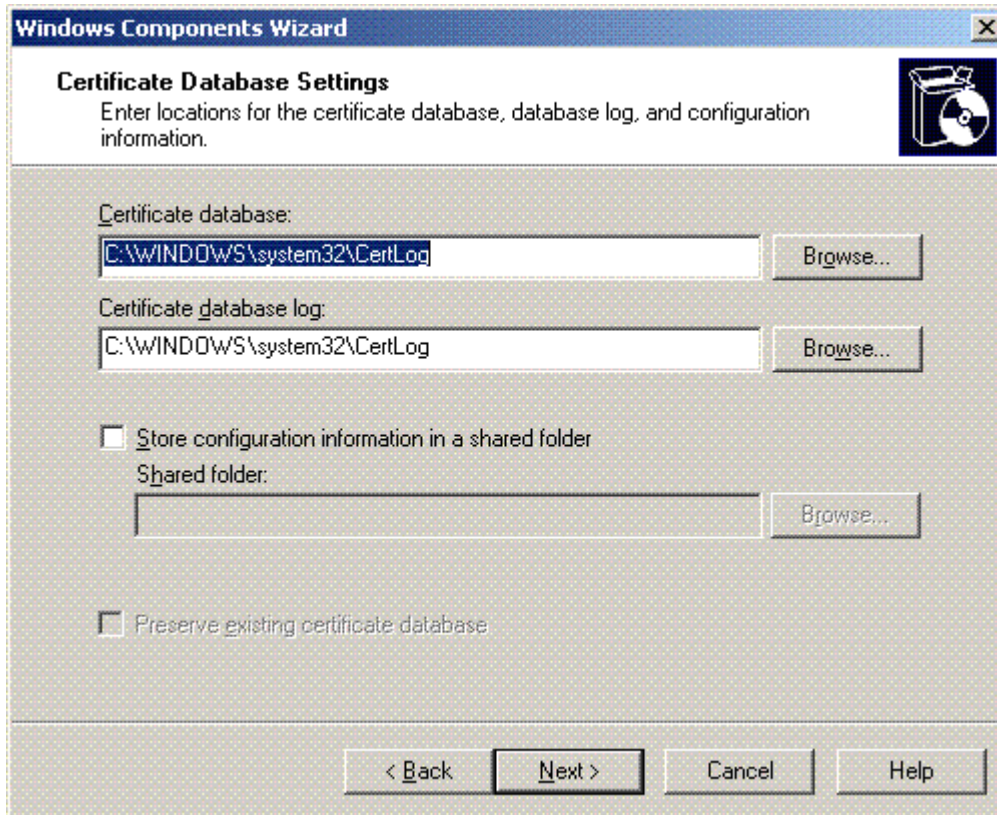
The screenshot shows the 'CA Type' step of the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The main heading is 'CA Type' with the instruction 'Select the type of CA you want to set up.' There are four radio button options: 'Enterprise root CA' (selected), 'Enterprise subordinate CA', 'Stand-alone root CA', and 'Stand-alone subordinate CA'. Below these is a text box with the description: 'Description of CA type: The most trusted CA in an enterprise. Should be installed before any other CA.' At the bottom, there is an unchecked checkbox labeled 'Use custom settings to generate the key pair and CA certificate'. Navigation buttons at the bottom include '< Back', 'Next >', 'Cancel', and 'Help'.

6. Enter a name to identify the CA. This example uses **Wireless-CA**. Click **Next**.

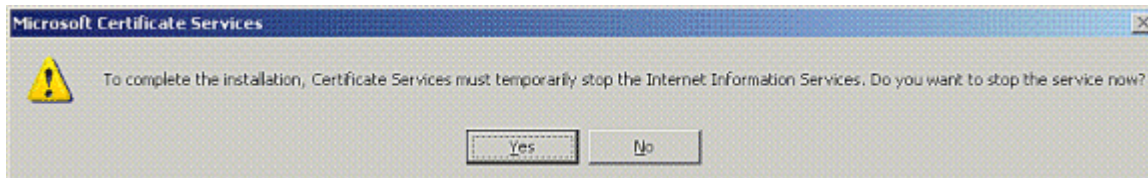


The screenshot shows the 'CA Identifying Information' step of the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The main heading is 'CA Identifying Information' with the instruction 'Enter information to identify this CA.' There are three text input fields: 'Common name for this CA:' containing 'Wireless-CA', 'Distinguished name suffix:' containing 'DC=Wireless,DC=com', and 'Preview of distinguished name:' containing 'CN=Wireless-CA,DC=Wireless,DC=com'. Below these are two sections: 'Validity period:' with a dropdown set to '5' and 'Years', and 'Expiration date:' showing '12/12/2012 7:01 PM'. Navigation buttons at the bottom include '< Back', 'Next >', 'Cancel', and 'Help'.

7. A “Cert Log” directory is created for certificate database storage. Click **Next**.



8. If IIS is enabled, it must be stopped before you proceed. Click **OK** to the warning message that IIS must be stopped. It restarts automatically after CA is installed.



9. Click **Finish** to complete the installation of Certificate Authority (CA) services.

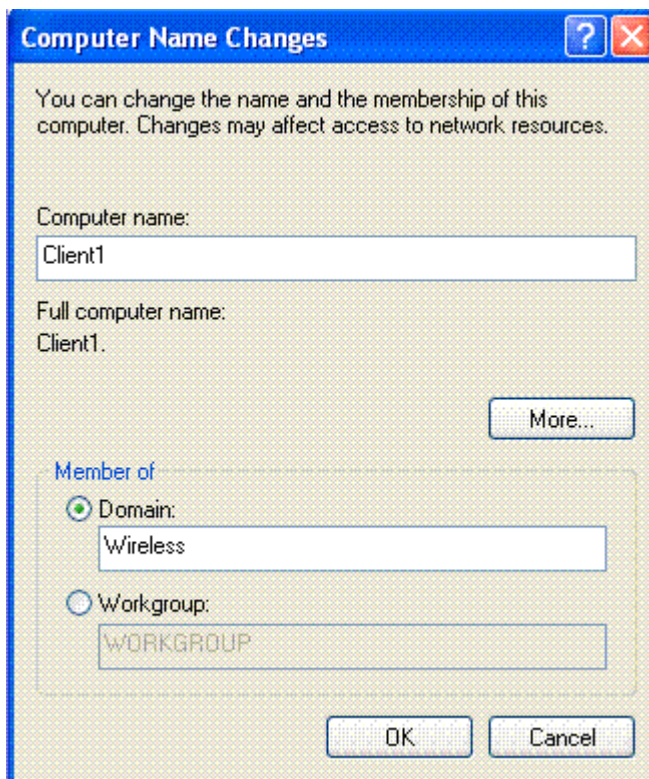


The next step is to install and configure the Internet Authentication Service on the Microsoft Windows 2003 server.

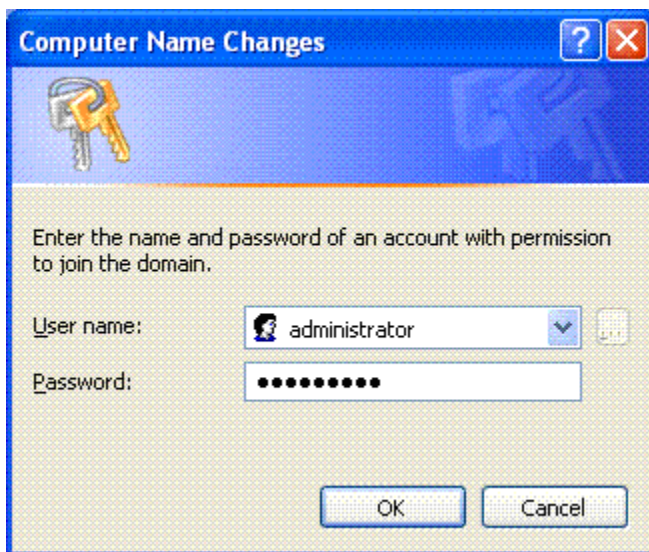
Connect Clients to the Domain

The next step is to connect the clients to the wired network and download the domain specific information from the new domain. In other words, connect the clients to the domain. In order to do this, complete these steps:

1. Connect the clients to the wired network with a straight through Ethernet cable.
2. Boot up the client and login with the username/ password of the client.
3. Click **Start**; click **Run**; type **cmd**; and click **OK**.
4. At the command prompt, type **ipconfig**, and click **Enter** to verify that DHCP works correctly and the client received an IP address from the DHCP server.
5. In order to join the client to the domain, right click **My Computer**, and choose **Properties**.
6. Click the **Computer Name** tab.
7. Click **Change**.
8. Click **Domain**; type **wireless.com**; and click **OK**.



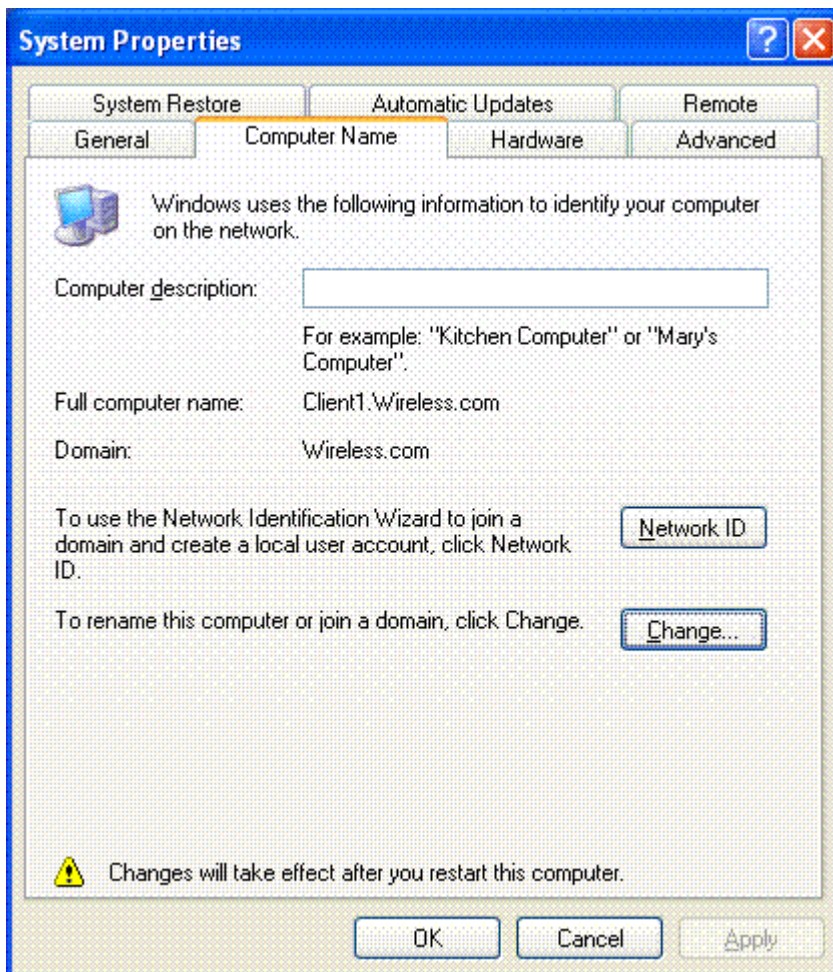
9. Type **Username Administrator** and the password specific to the domain to which the client joins. (This is the administrator account in the Active Directory on the server.)



10. Click **OK**.

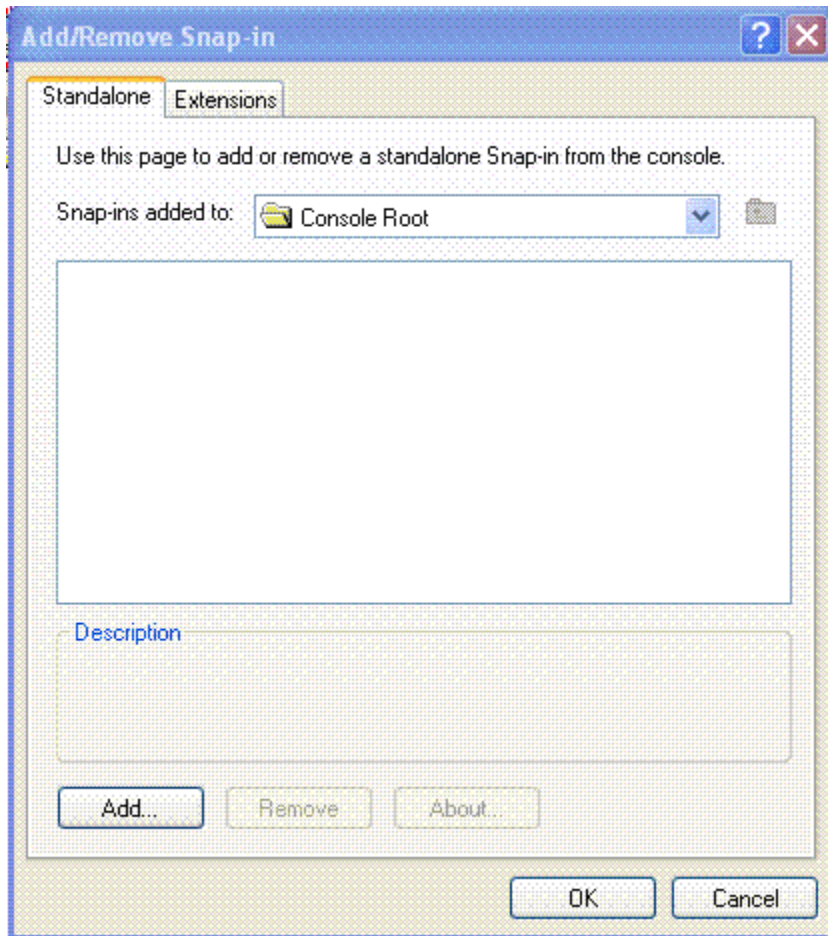


11. Click **Yes** to restart the computer.
12. Once the computer restarts, login with this information: Username = **Administrator**; Password = **<domain password>**; Domain = **Wireless**.
13. Right click **My Computer**, and click **Properties**.
14. Click the **Computer Name** tab to verify that you are on the Wireless.com domain.

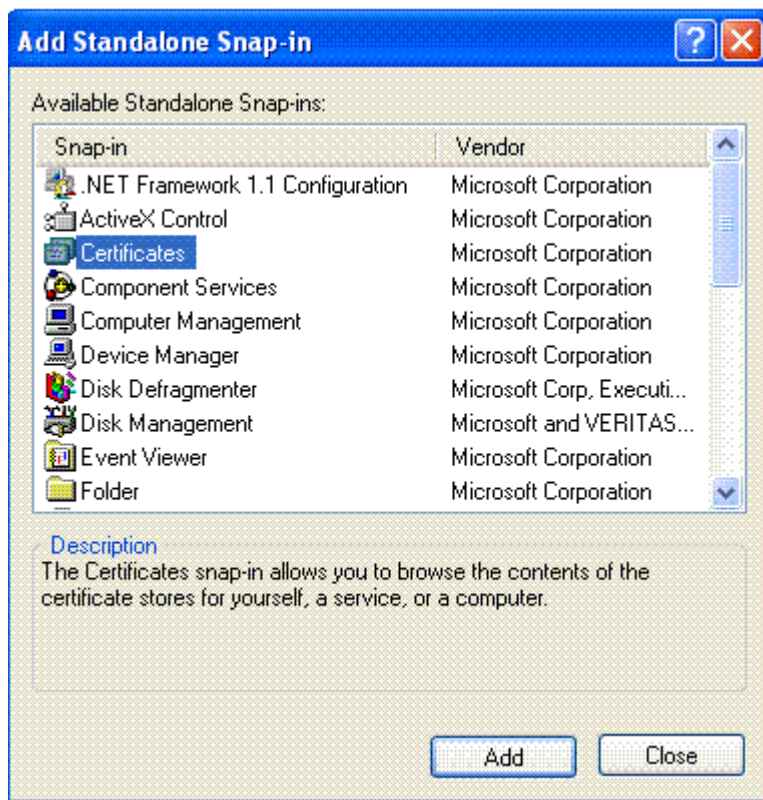


15. The next step is to verify that the client received the CA certificate (trust) from the server.
16. Click **Start**; click **Run**; type **mmc**, and click **OK**.

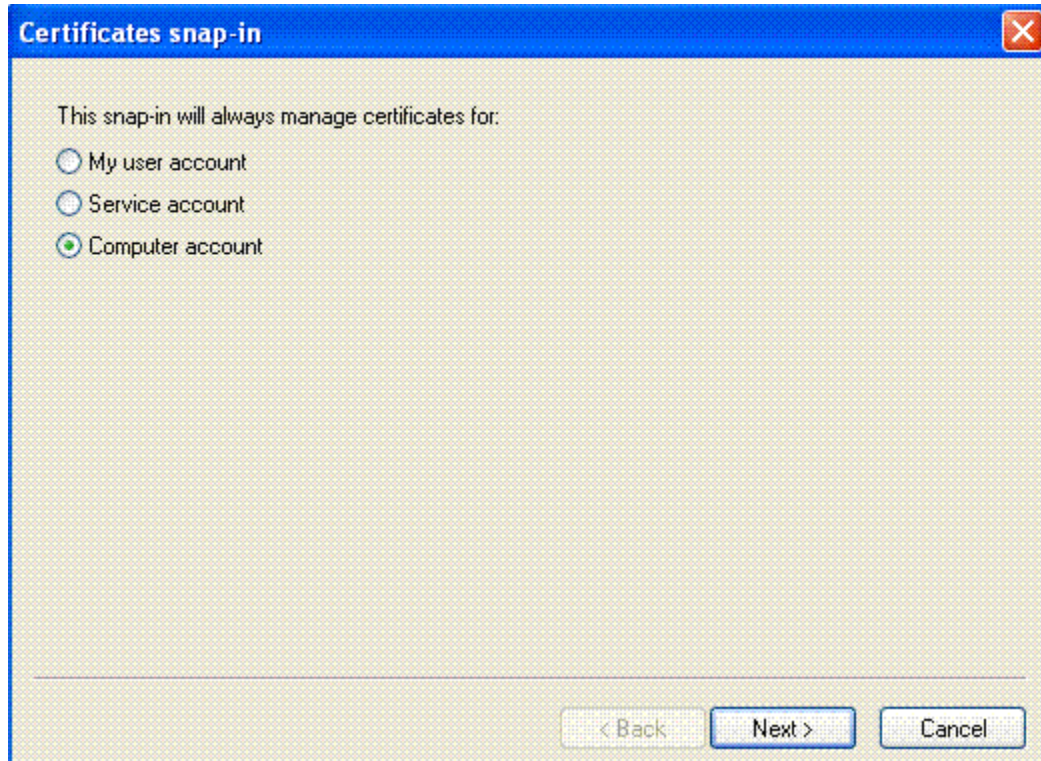
17. Click **File**, and click **Add/Remove** snap-in.



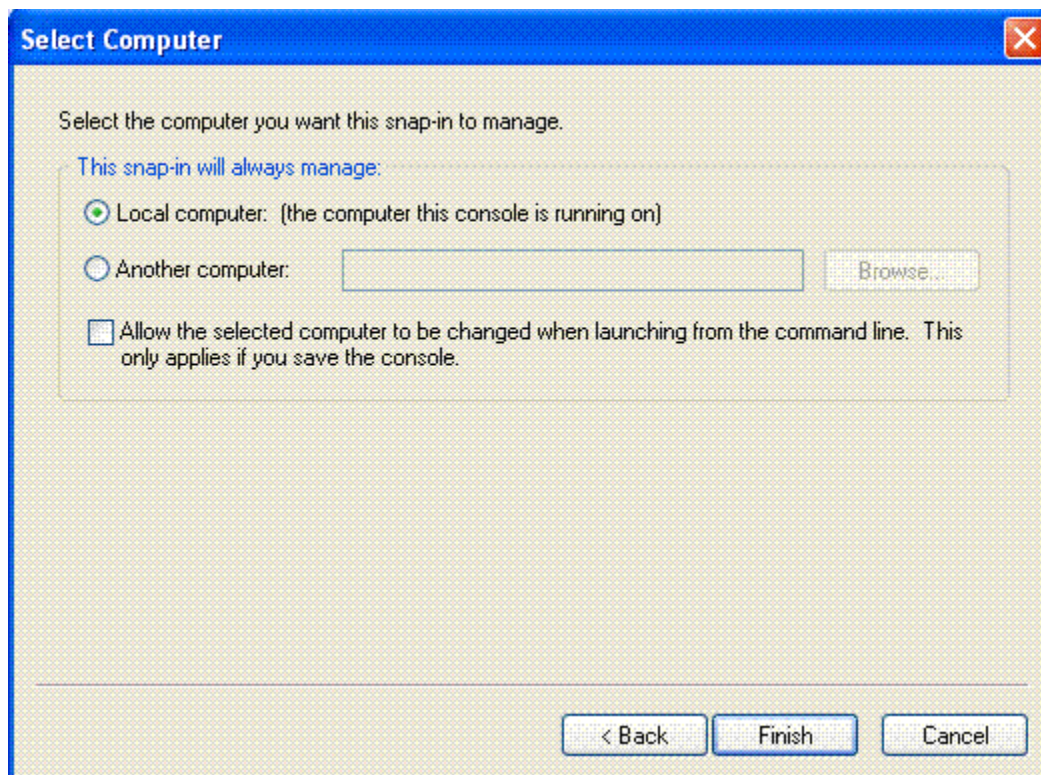
18. Click **Add**.
19. Choose **Certificate**, and click **Add**.



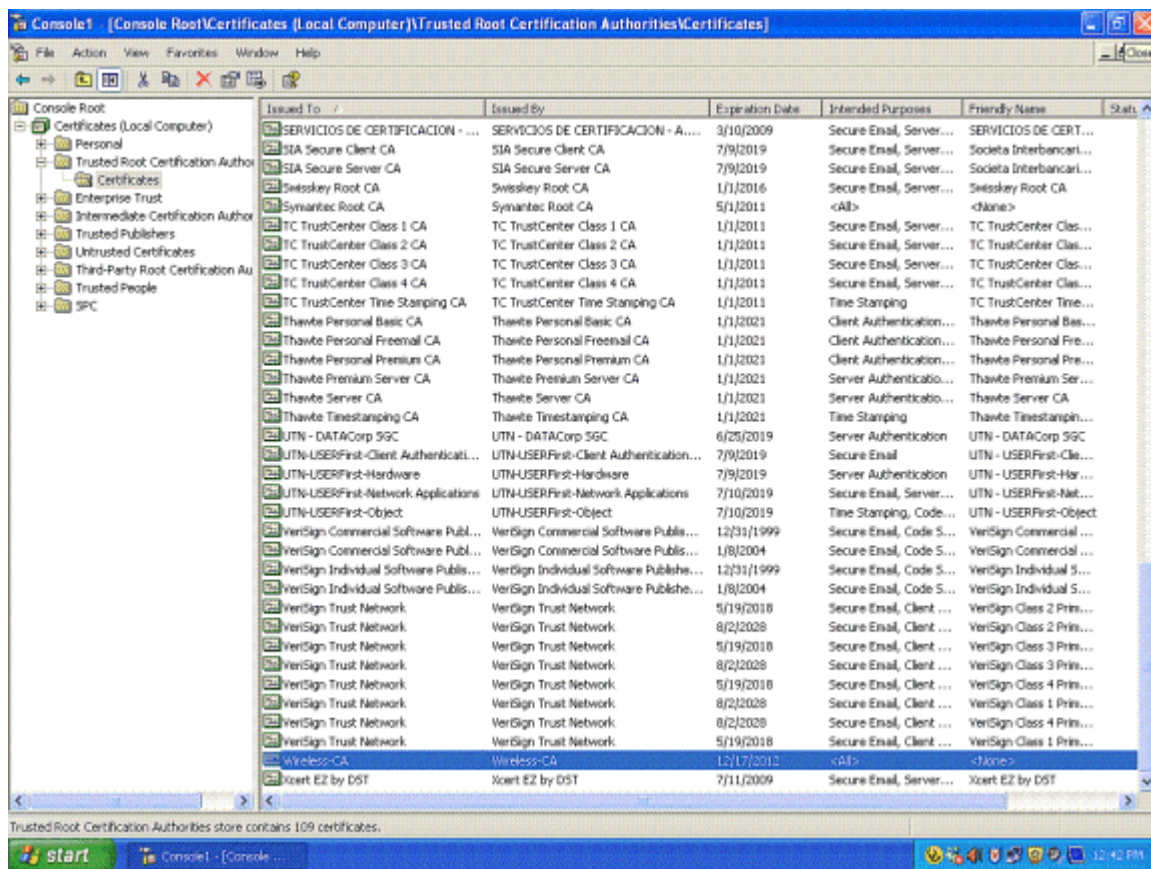
20. Choose **Computer Account**, and click **Next**.



21. Click **Finish** to accept the default local computer.



22. Click **Close**, and click **OK**.
23. Expand **Certificates (Local Computer)**; expand **Trusted Root Certification Authorities**; and click **Certificates**. Find **Wireless** in the list.



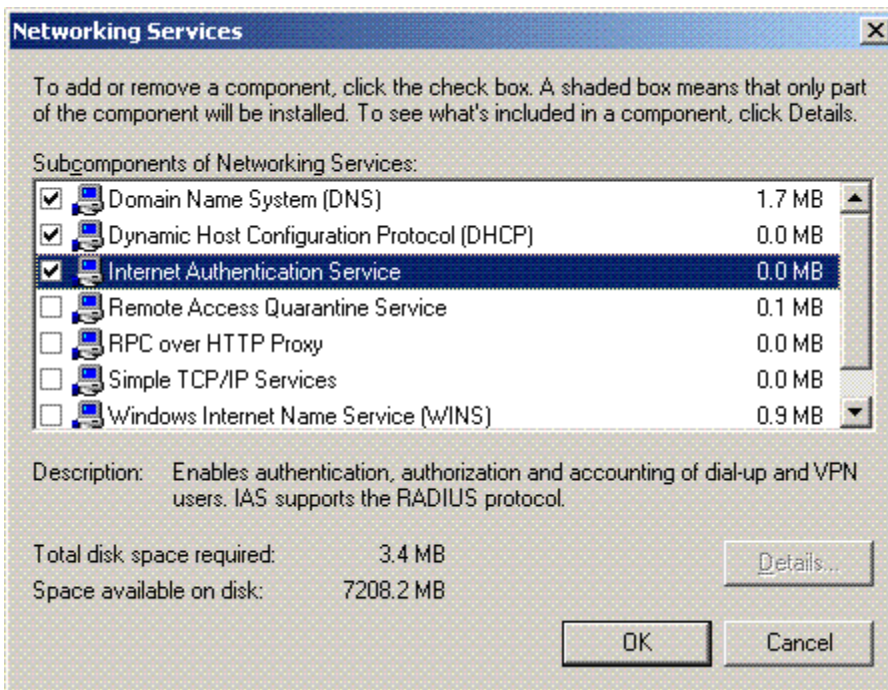
24. Repeat this procedure to add more clients to the domain.

Install the Internet Authentication Service on the Microsoft Windows 2003 Server and Request a Certificate

In this setup, the Internet Authentication Service (IAS) is used as a RADIUS server to authenticate Wireless clients with PEAP authentication.

Complete these steps to install and configure IAS on the server.

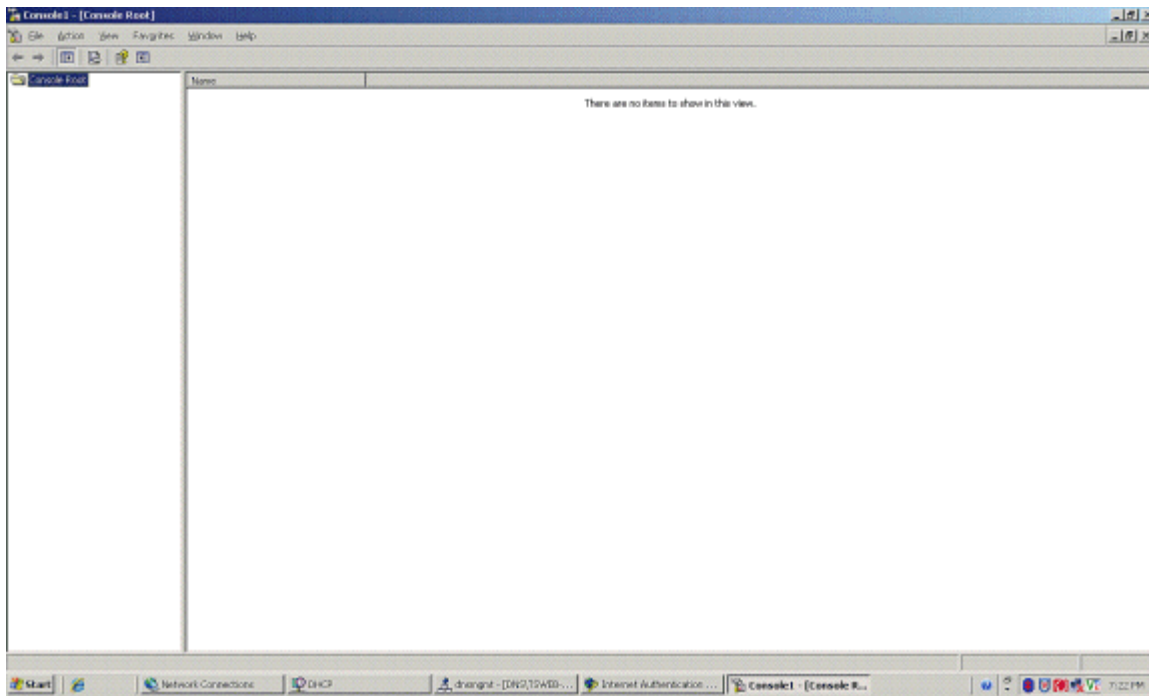
1. Click **Add or Remove Programs** in the Control Panel.
2. Click **Add/Remove Windows Components**.
3. Choose **Networking Services**, and click **Details**.
4. Choose **Internet Authentication Service**; click **OK**; and click **Next**.



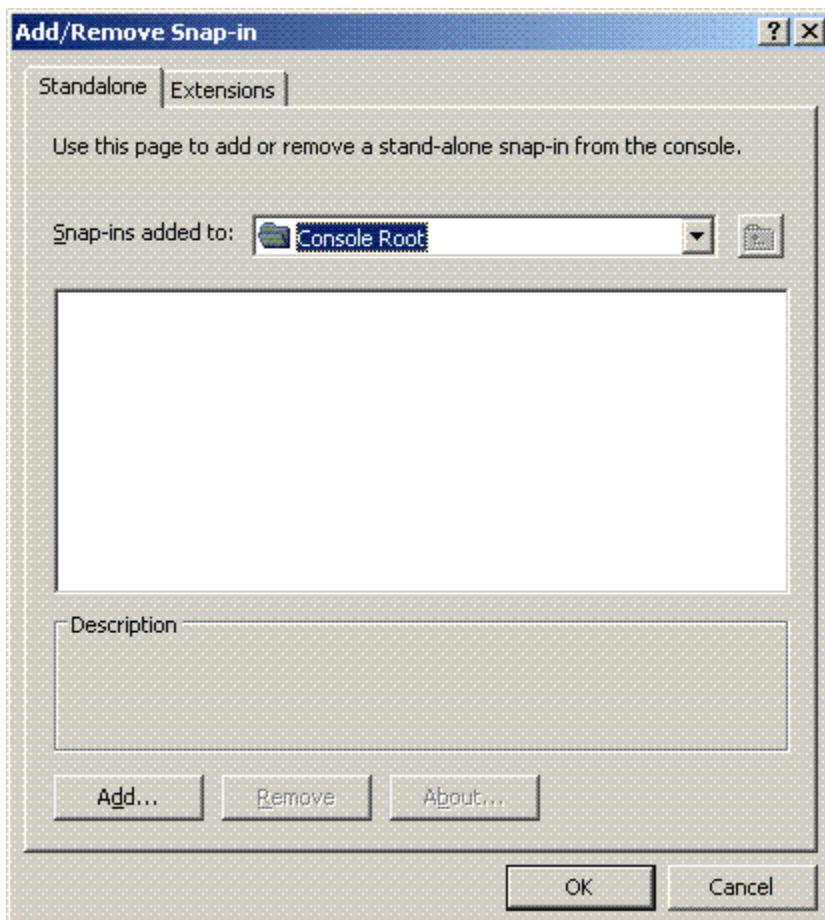
5. Click **Finish** to complete the IAS installation.



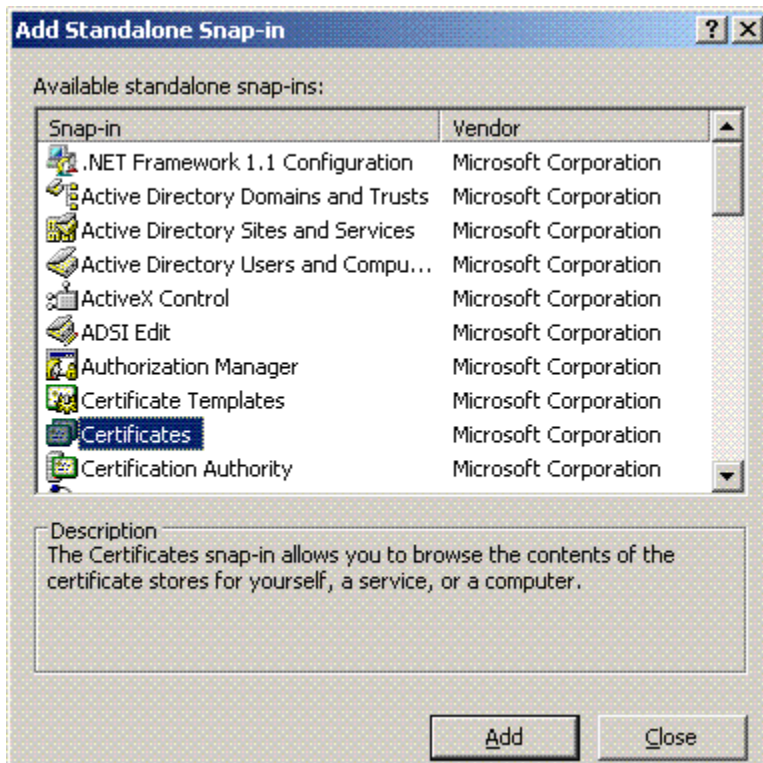
6. The next step is to install the computer certificate for the Internet Authentication Service (IAS).
7. Click **Start**; click **Run**; type **mmc**; and click **OK**.



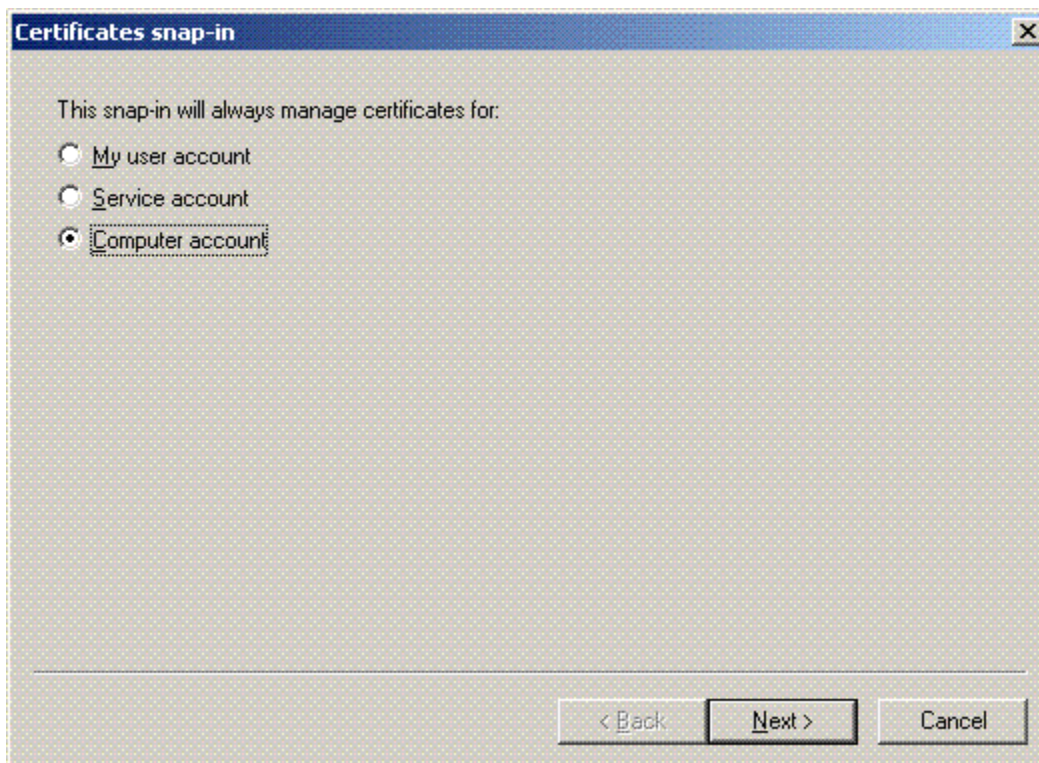
8. Click **Console** in the file menu, and then choose **Add/Remove** snap-in.
9. Click **Add** to add a snap-in.



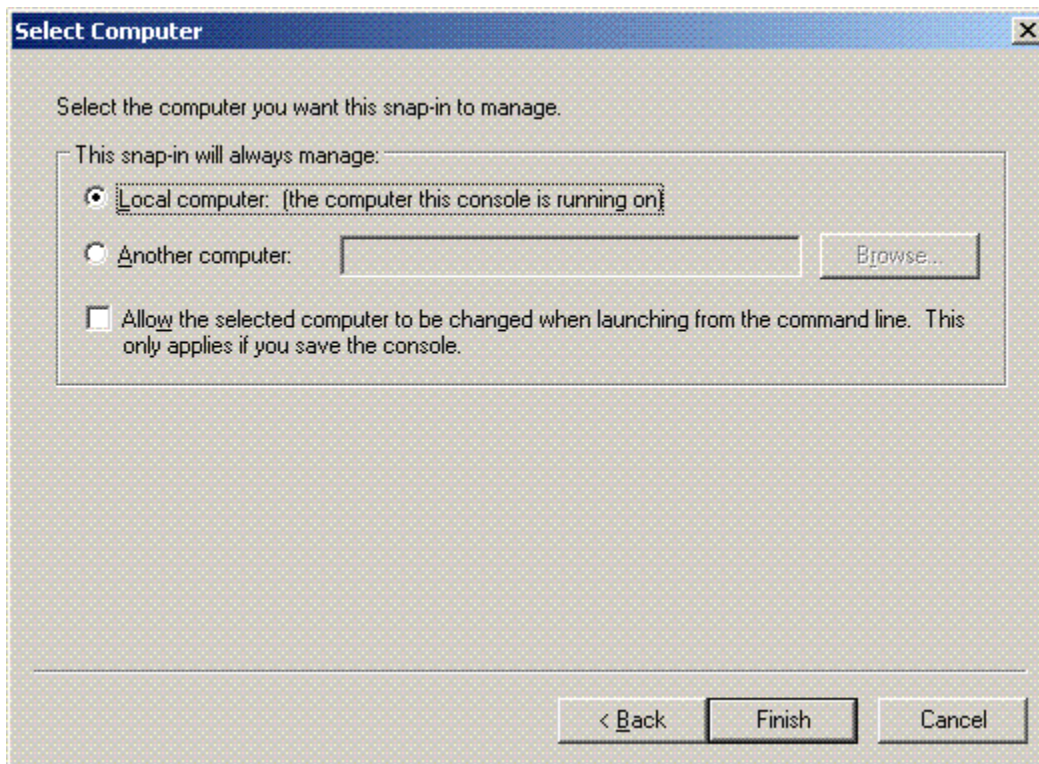
10. Choose **Certificates** from the list of snap-ins, and click **Add**.



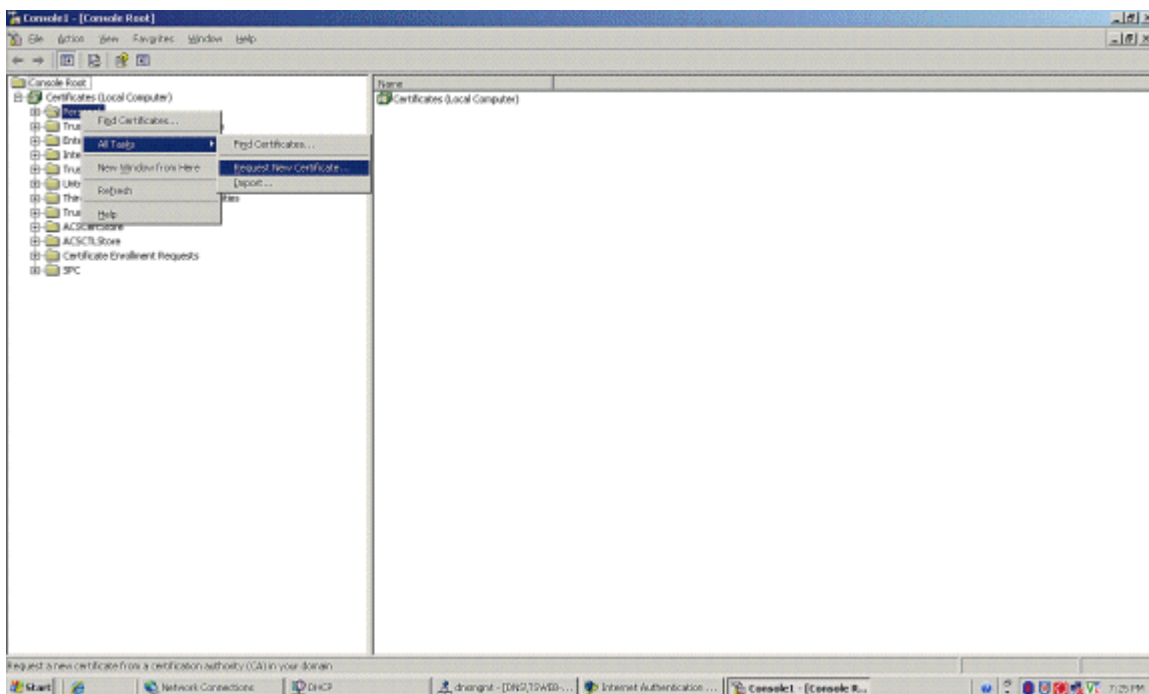
11. Choose **Computer account**, and click **Next**.



12. Choose **Local computer**, and click **Finish**.



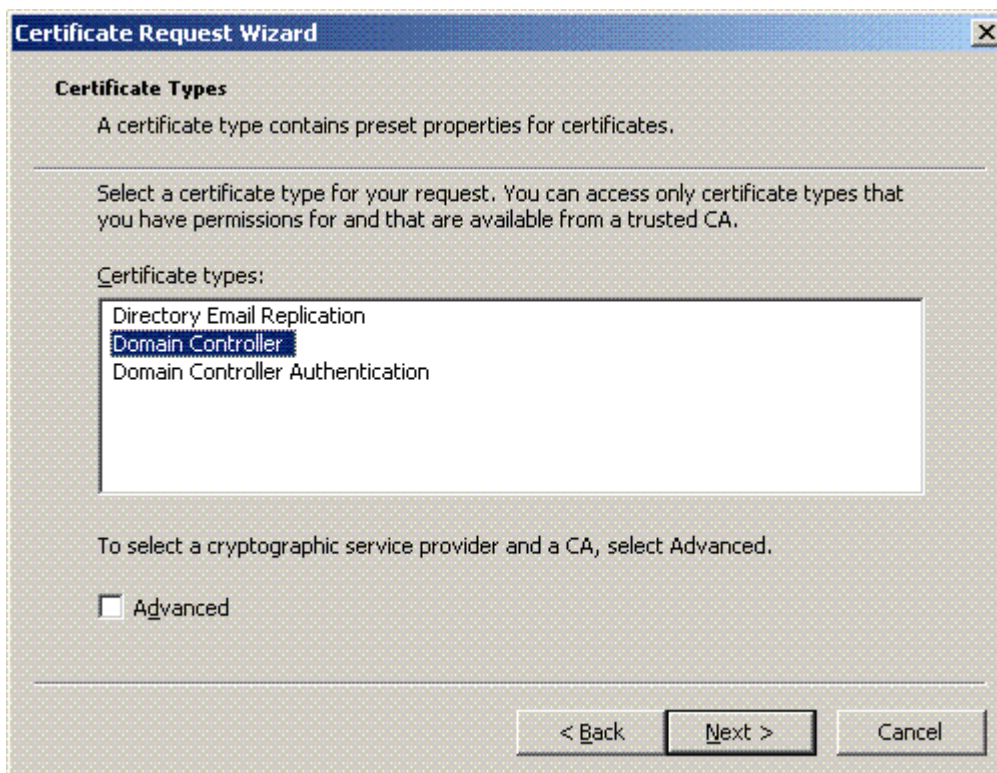
13. Click **Close**, and click **OK**.
14. Expand **Certificates (Local Computer)**; right click **Personal** folder; choose **All tasks** and then **Request New Certificate**.



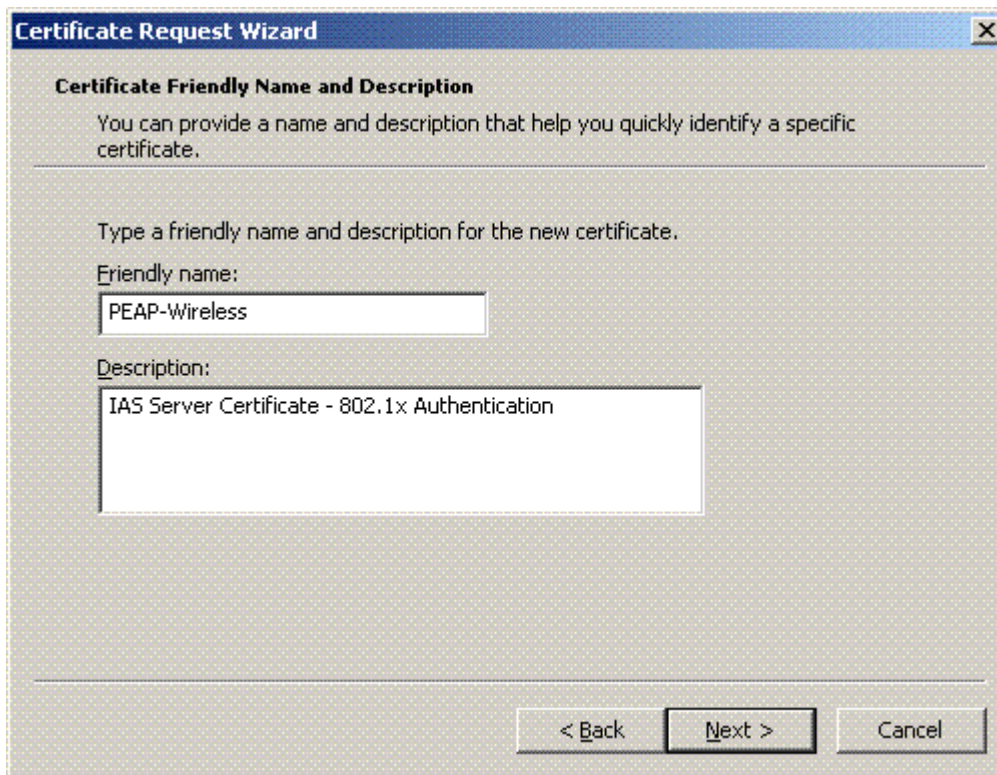
15. Click **Next** on the *Welcome to the Certificate Request Wizard*.



16. Choose the **Domain Controller** certificate template (if you request a computer certificate on a server other than the DC, choose a **Computer** certificate template), and click **Next**.



17. Type a name and description for the certificate.



Certificate Request Wizard

Certificate Friendly Name and Description

You can provide a name and description that help you quickly identify a specific certificate.

Type a friendly name and description for the new certificate.

Friendly name:
PEAP-Wireless

Description:
IAS Server Certificate - 802.1x Authentication

< Back Next > Cancel

18. Click **Finish** to complete the certification request wizard.



Certificate Request Wizard

Completing the Certificate Request Wizard

You have successfully completed the Certificate Request wizard.

You have specified the following settings:

Friendly Name	PEAP-Wireless
Computer Name	TSWEB-LAPT
Certificate Template	Domain Controller

< Back Finish Cancel

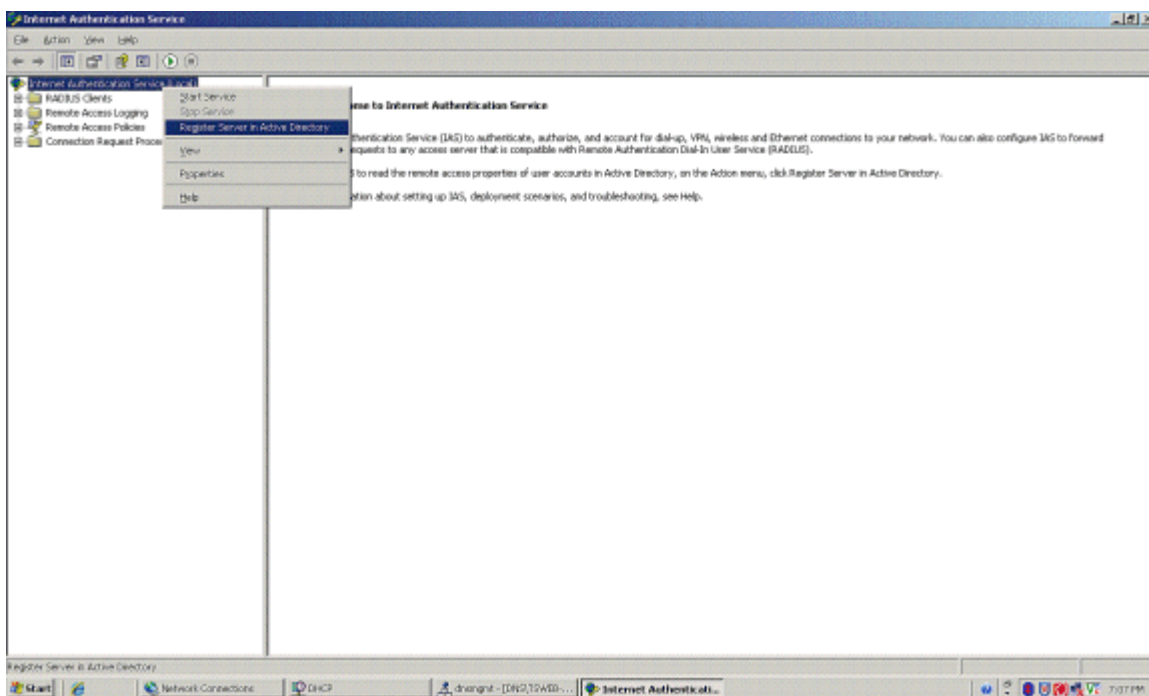


Configure the Internet Authentication Service for PEAP-MS-CHAP v2 Authentication

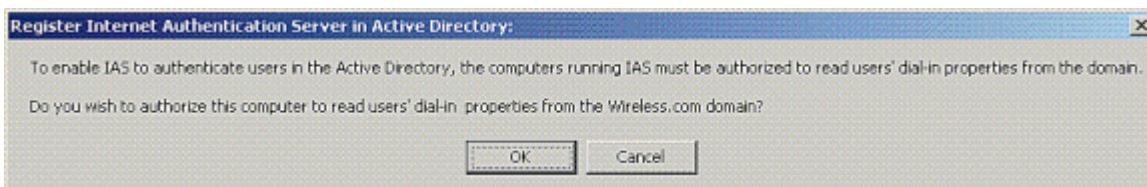
Now that you have installed and requested a certificate for the IAS, configure the IAS for authentication.

Complete these steps:

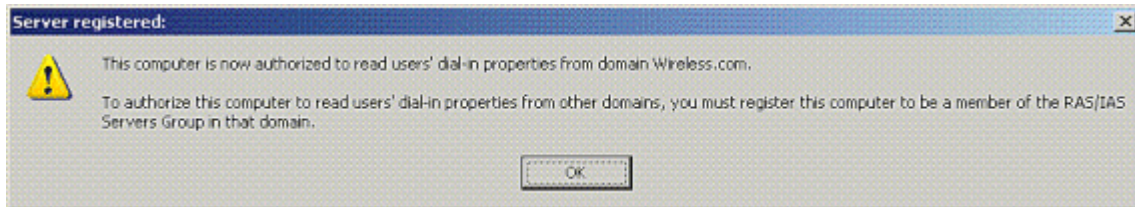
1. Click **Start > Programs > Administrative Tools**, and click **Internet Authentication Service** snap-in.
2. Right-click **Internet Authentication Service (IAS)**, and then click **Register Service in Active Directory**.



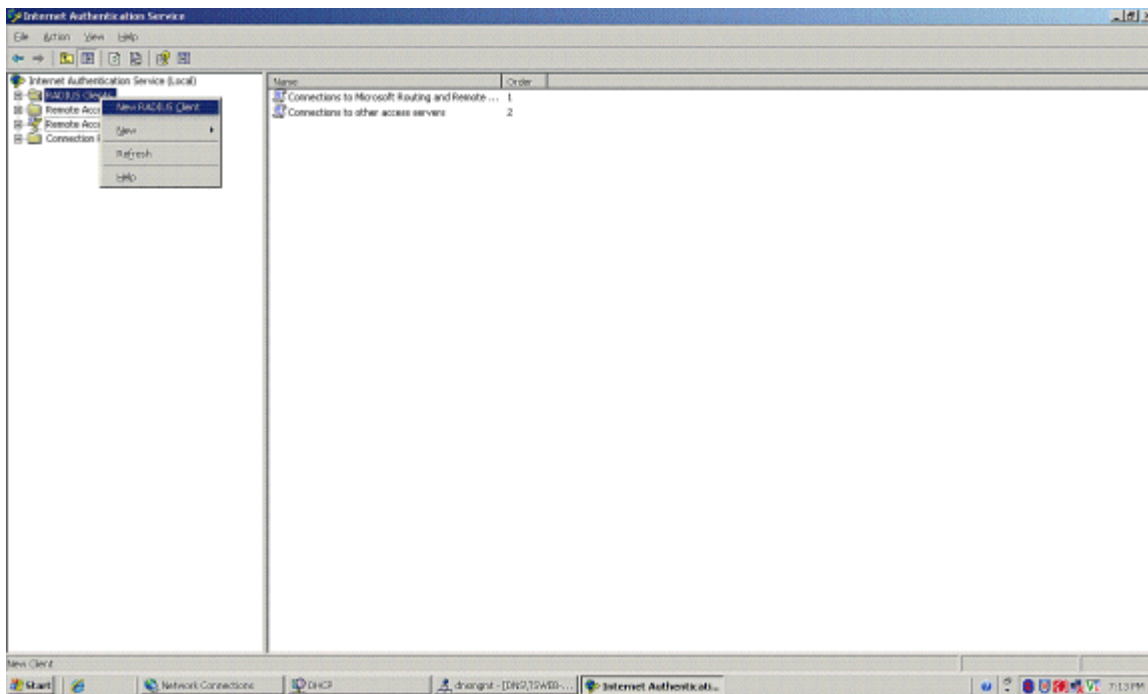
3. The **Register Internet Authentication Service in Active Directory** dialog box appears; click **OK**. This enables IAS to authenticate users in the Active Directory.



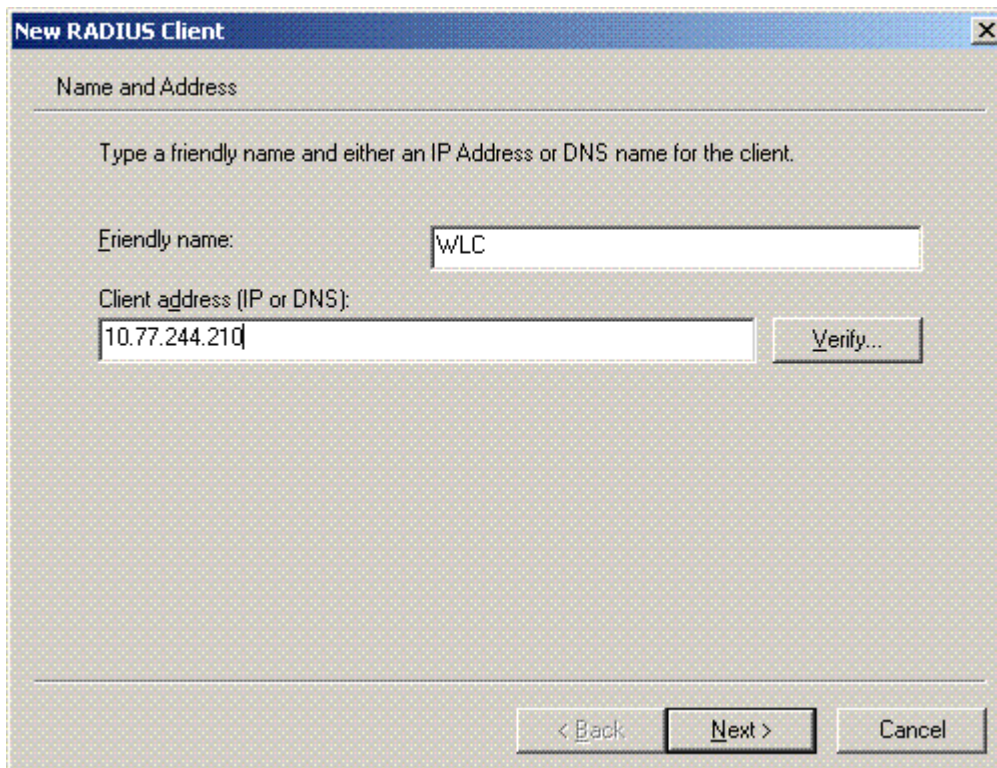
- Click **OK** in the next dialog box.



- Add the Wireless LAN Controller as an AAA client on the MS IAS server.
- Right-click **RADIUS Clients**, and choose **New RADIUS Client**.

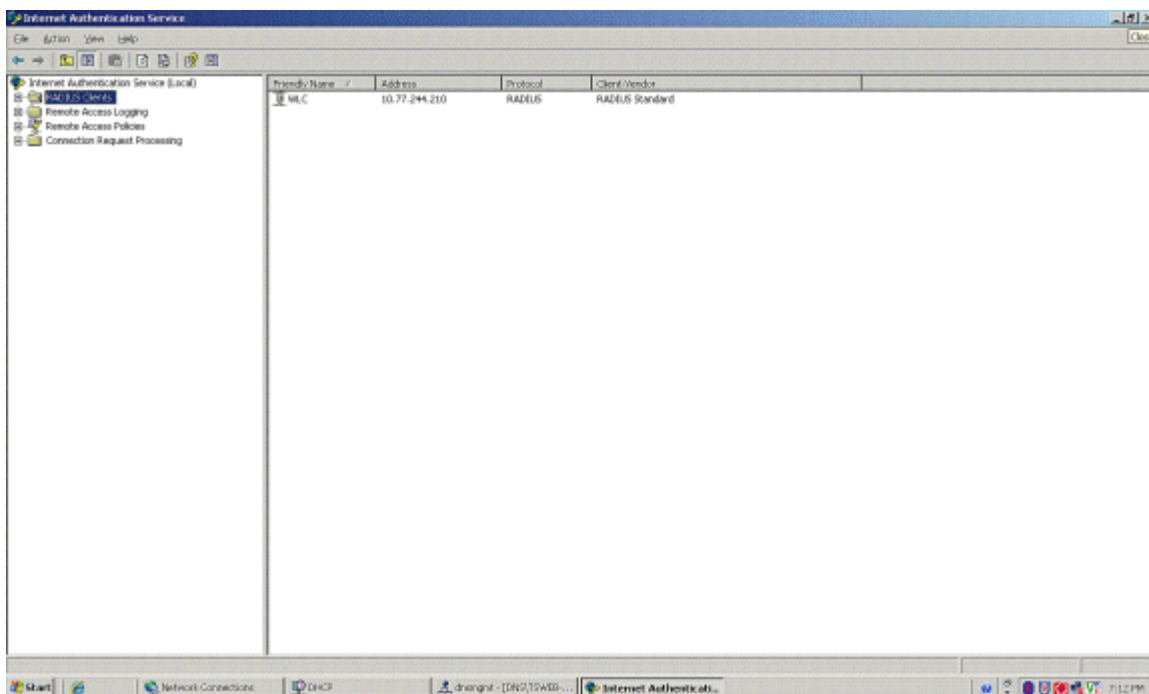


- Type the name of the client (WLC in this case), and enter the IP address of the WLC. Click **Next**.



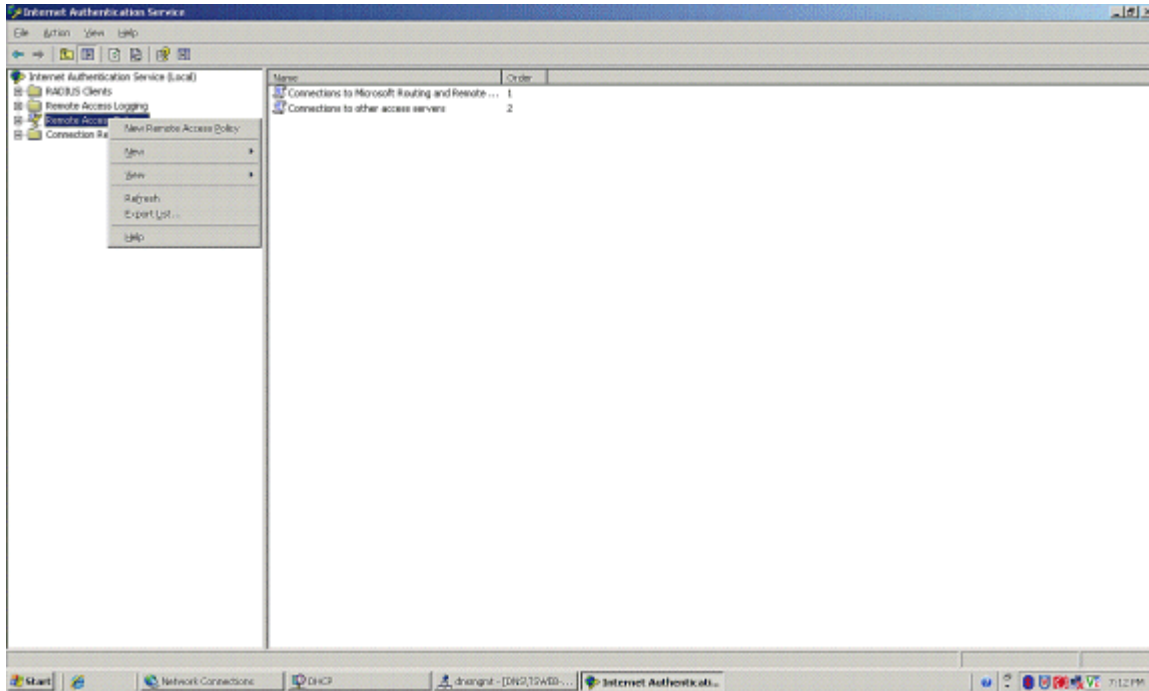
The 'New RADIUS Client' dialog box is shown. It has a title bar with 'New RADIUS Client' and a close button. The main area is titled 'Name and Address' and contains the instruction: 'Type a friendly name and either an IP Address or DNS name for the client.' There are two input fields: 'Friendly name:' with the text 'WLC' and 'Client address (IP or DNS):' with the text '10.77.244.210'. A 'Verify...' button is next to the client address field. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

8. On the next page, under Client-Vendor, choose **RADIUS Standard**; enter the shared secret; and click **Finish**.
9. Notice that the WLC is added as an AAA client on the IAS.

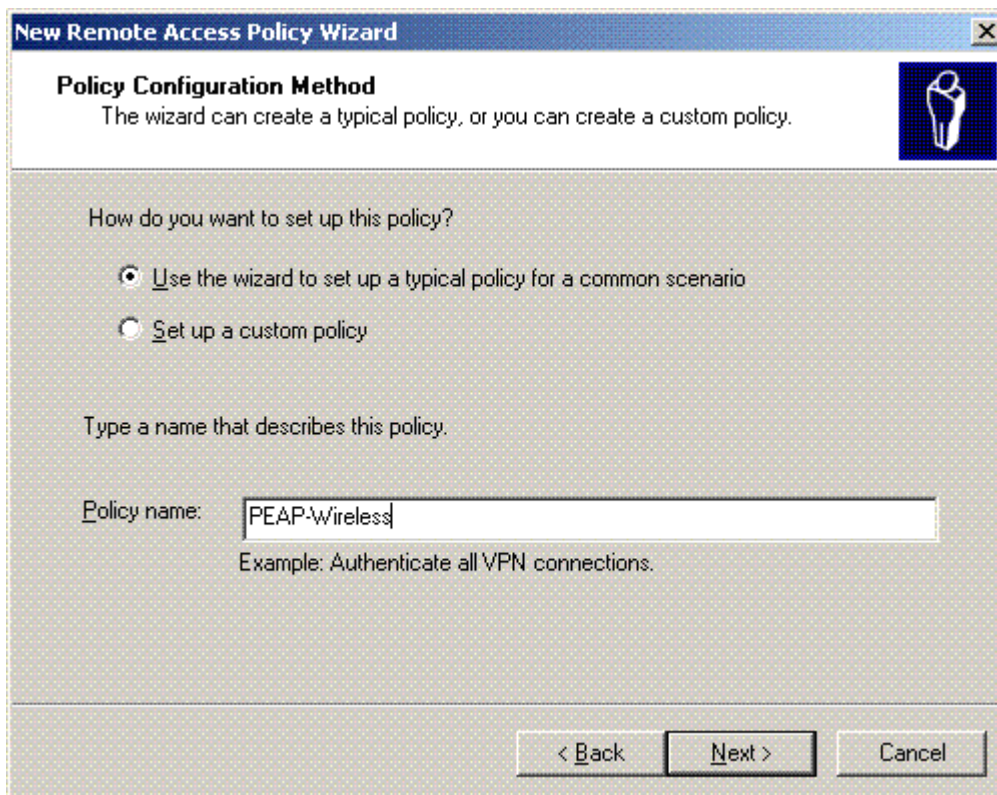


10. Create a remote access policy for the clients.

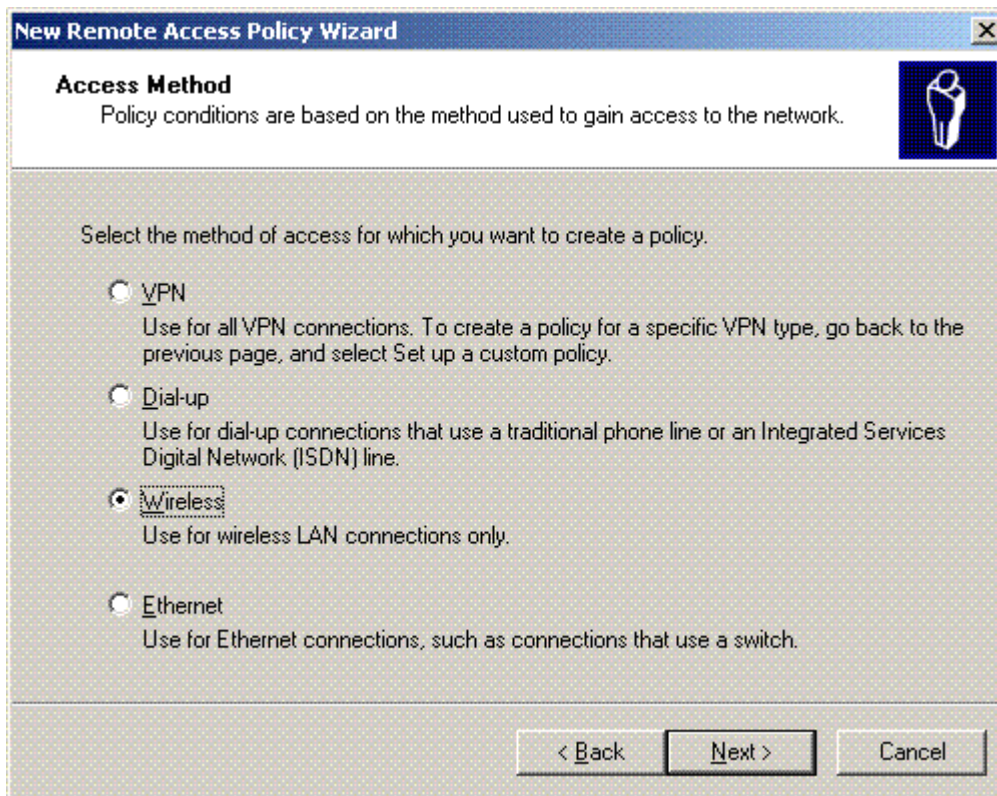
11. In order to do this, right-click **Remote Access Policies**, and choose **New Remote Access Policy**.



12. Type a name for the remote access policy. In this example, use the name **PEAP**. Then click **Next**.



13. Choose the policy attributes based on your requirements. In this example, choose **Wireless**.



New Remote Access Policy Wizard

Access Method
Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

☐ **V**PN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

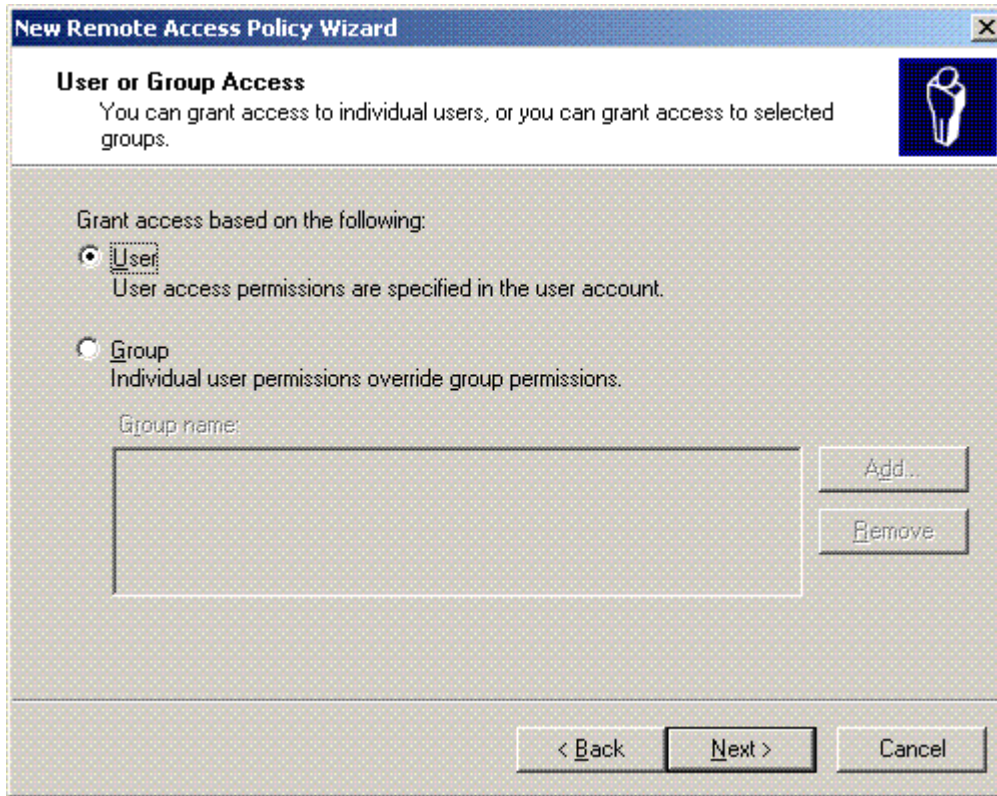
☐ **D**ial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.

☒ **W**ireless
Use for wireless LAN connections only.

☐ **E**thernet
Use for Ethernet connections, such as connections that use a switch.

< Back Next > Cancel

14. On the next page, choose **User** to apply this remote access policy to list of users.



New Remote Access Policy Wizard

User or Group Access
You can grant access to individual users, or you can grant access to selected groups.

Grant access based on the following:

☒ **U**ser
User access permissions are specified in the user account.

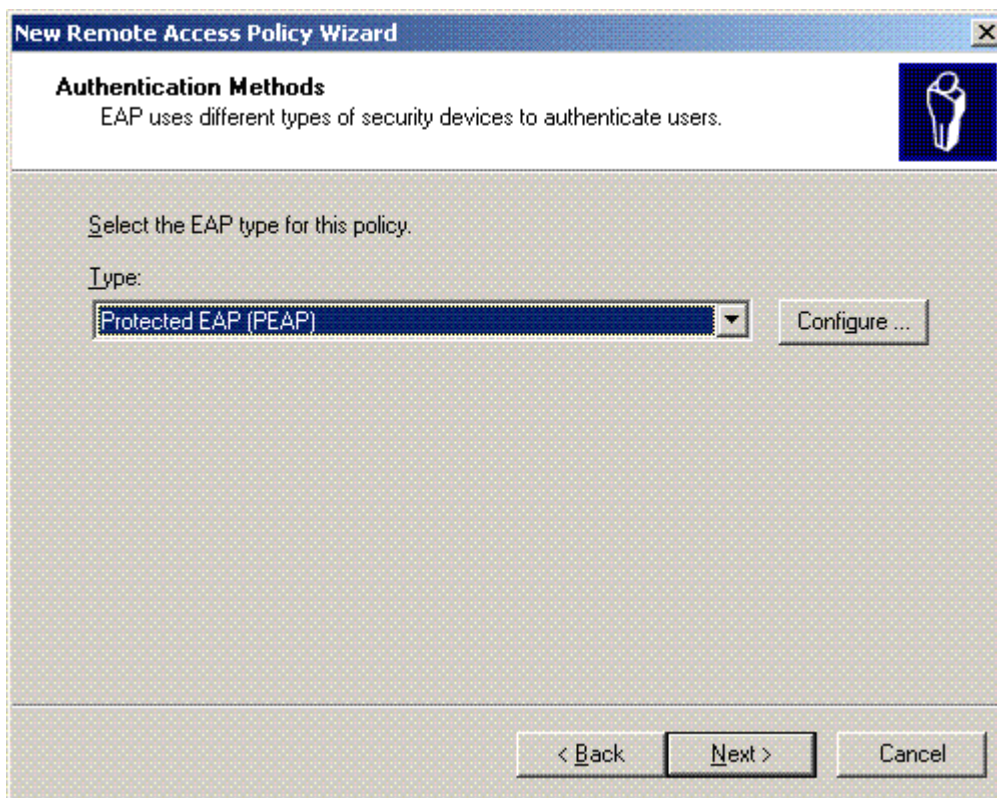
☐ **G**roup
Individual user permissions override group permissions.

Group name:

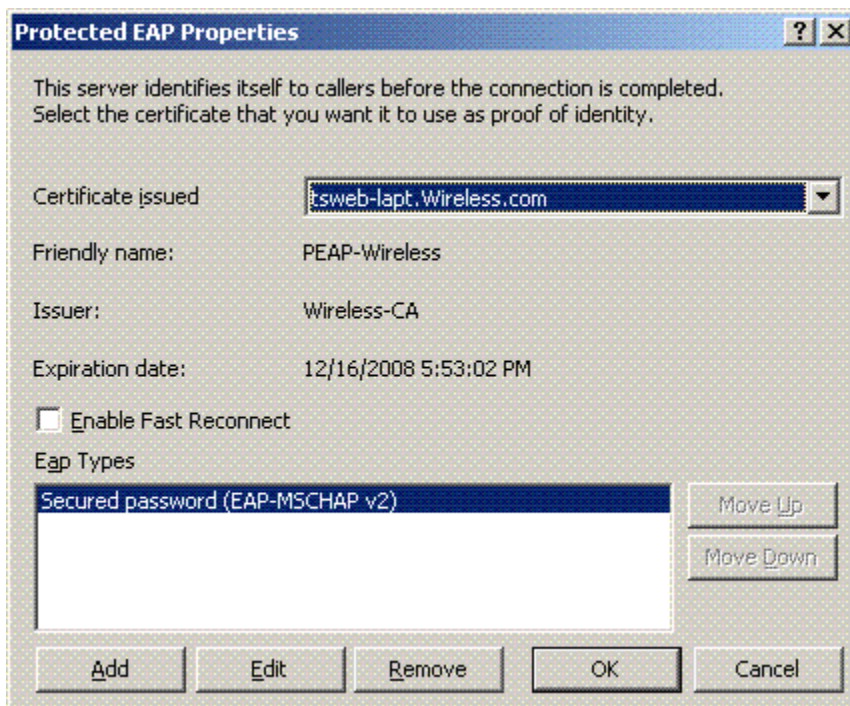
Add... Remove

< Back Next > Cancel

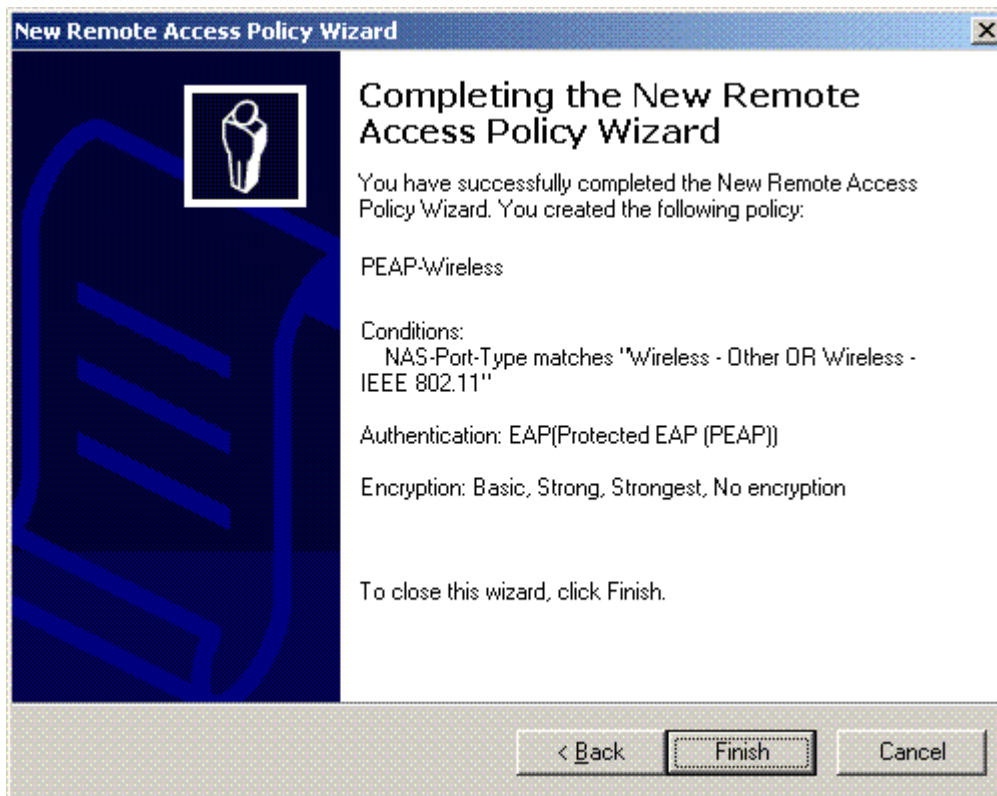
15. Under Authentication Methods, choose **Protected EAP (PEAP)**, and click **Configure**.



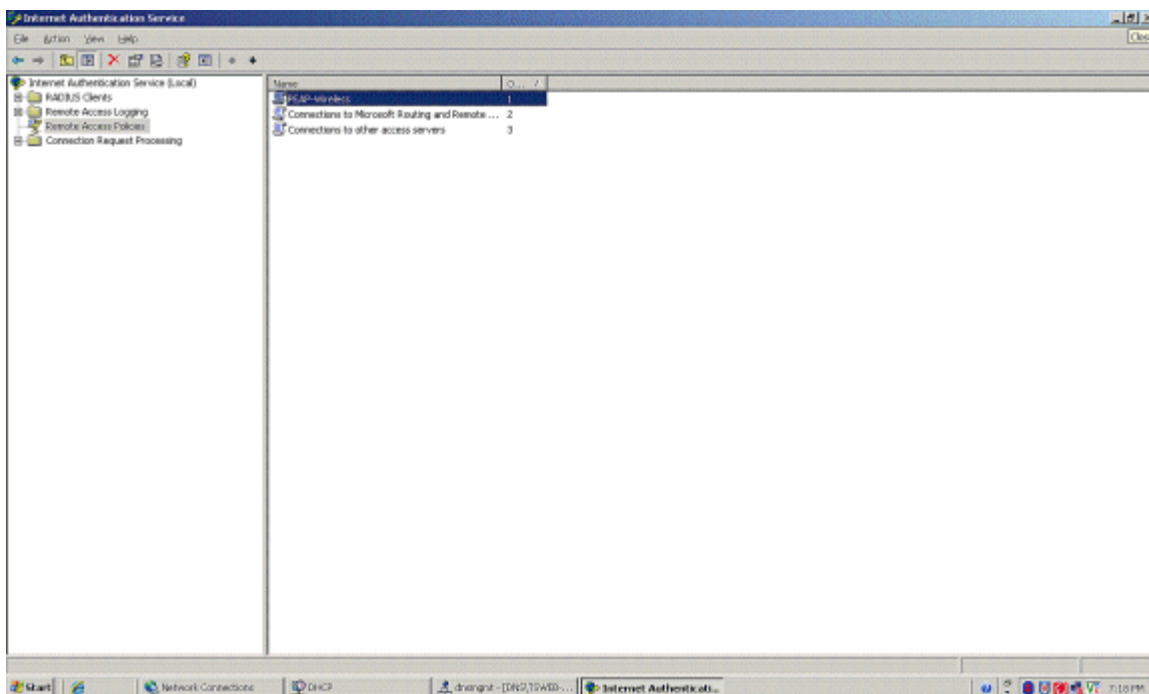
16. On the **Protected EAP Properties** page, choose the appropriate certificate from the Certificate Issued drop-down menu, and click **OK**.



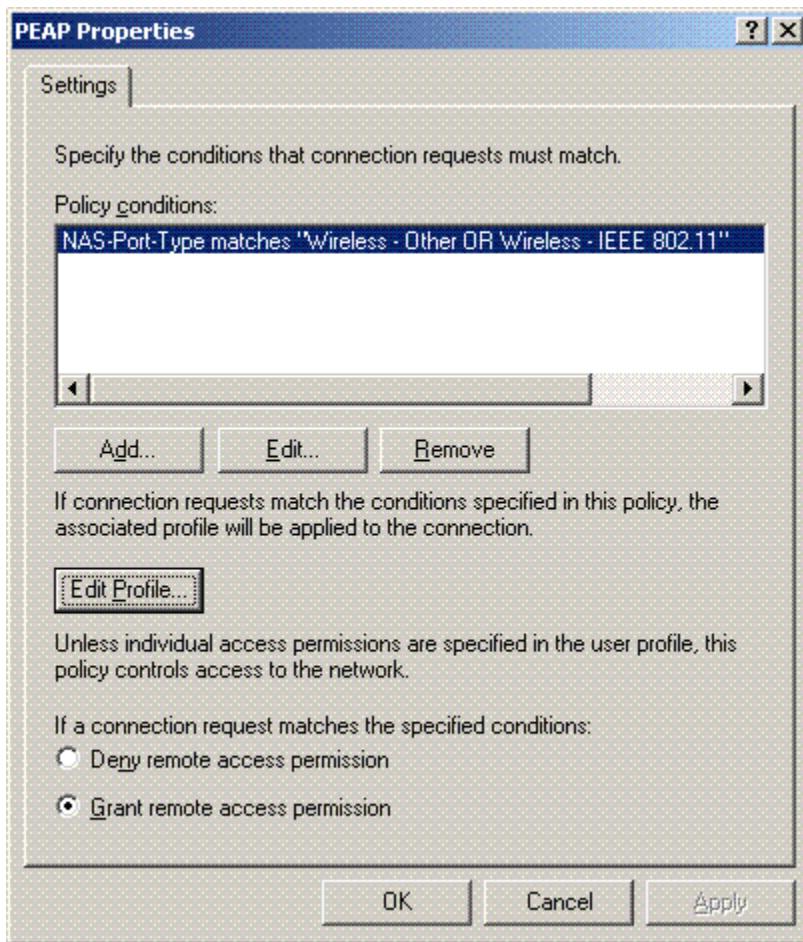
17. Verify the details of the remote access policy, and click **Finish**.



18. The remote access policy has been added to the list.



19. Right-click the policy, and click **Properties**. Choose “**Grant remote access permission**” under “**If a connection request matches the specified conditions.**”

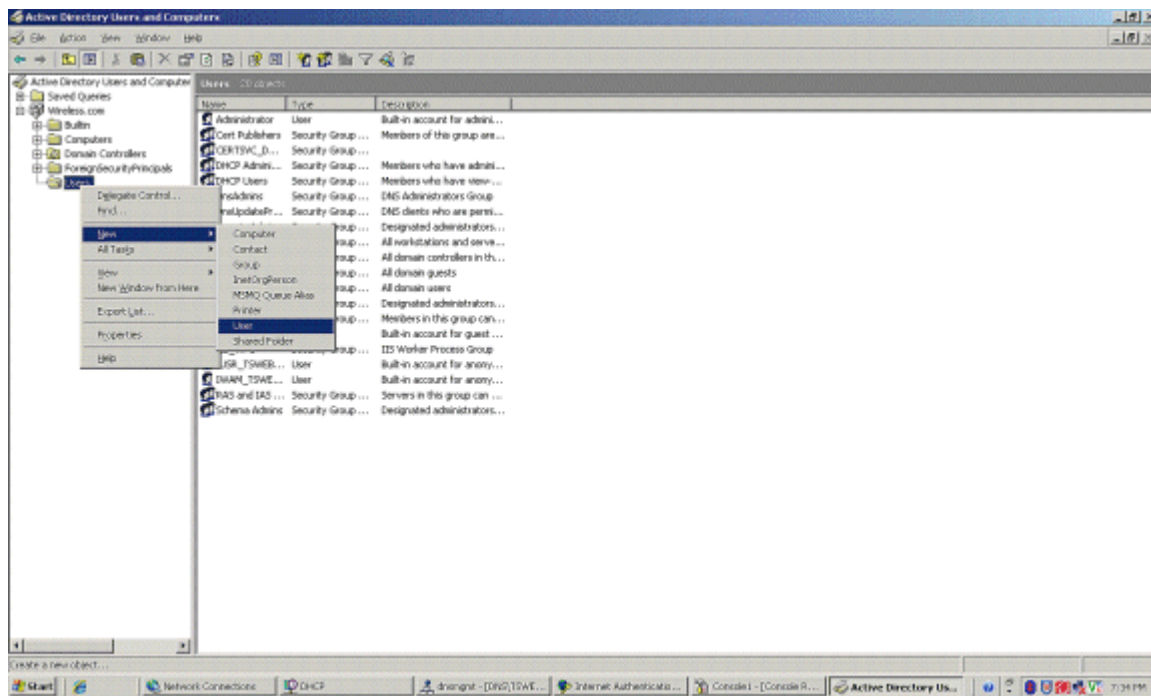


Add Users to the Active Directory

In this setup, the User database is maintained on the Active Directory.

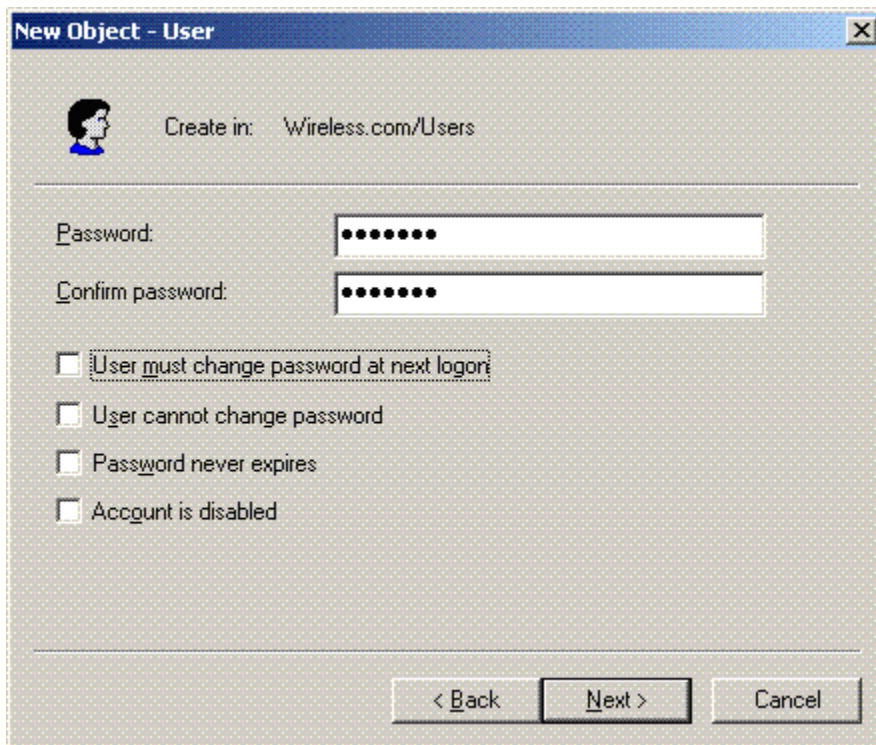
In order to add users to the Active directory database, complete these steps:

1. In the Active Directory Users and Computers console tree, right-click **Users**; click **New**; and then click **User**.



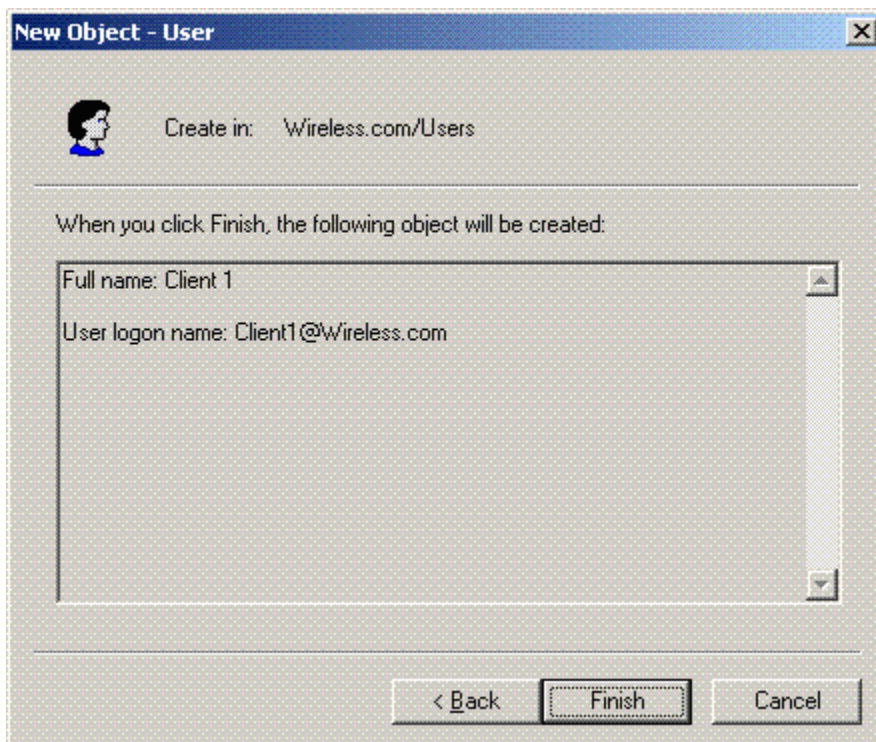
2. In the New Object – User dialog box, type the name of the Wireless user. This example uses the name **WirelessUser** in the First name field and **WirelessUser** in the User logon name field. Click **Next**.

3. In the New Object – User dialog box, type a password of your choice in the Password and Confirm password fields. Clear the **User must change password at next logon** check box, and click **Next**.



The 'New Object - User' dialog box is shown. It has a title bar with a close button. Below the title bar is a user icon and the text 'Create in: Wireless.com/Users'. There are two password fields: 'Password:' and 'Confirm password:', both with masked characters. Below these are four checkboxes: 'User must change password at next logon', 'User cannot change password', 'Password never expires', and 'Account is disabled'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

4. In the New Object – User dialog box, click **Finish**.



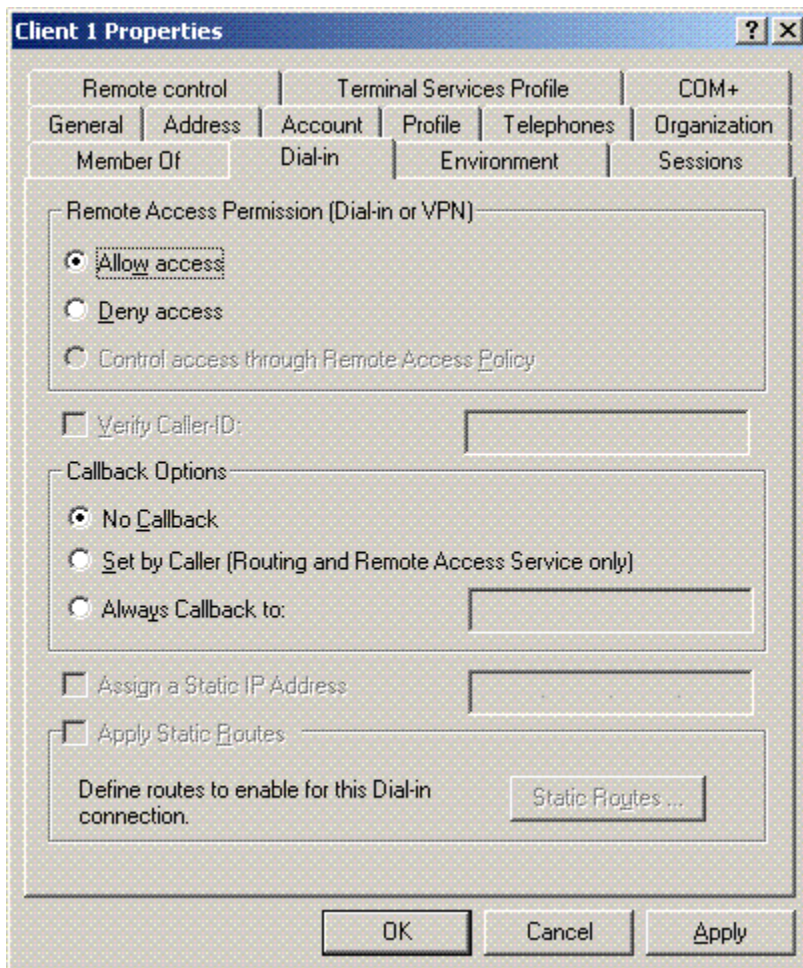
The 'New Object - User' dialog box is shown again, but now it displays the details of the object to be created. It has a title bar with a close button. Below the title bar is a user icon and the text 'Create in: Wireless.com/Users'. Below this is the text 'When you click Finish, the following object will be created:'. There is a text area containing 'Full name: Client 1' and 'User logon name: Client1@Wireless.com'. At the bottom are three buttons: '< Back', 'Finish', and 'Cancel'.

5. Repeat steps 2 through 4 in order to create additional user accounts.

Allow Wireless Access to Users

Complete these steps:

1. In the **Active Directory Users and Computers** console tree, click the **Users** folder; right-click **WirelessUser**; click **Properties**; and then go to the **Dial-in** tab.
2. Choose **Allow access**, and click **OK**.



Configure the Wireless LAN Controller and Lightweight APs

Now configure the Wireless devices for this setup. This includes the configuration of the Wireless LAN Controllers, Lightweight APs, and Wireless clients.

Configure the WLC for RADIUS Authentication through MS IAS RADIUS Server

First configure the WLC to use the MS IAS as the authentication server. The WLC needs to be configured in order to forward the user credentials to an external RADIUS server. The external RADIUS server then validates the user credentials and provides access to the Wireless clients. In order to do this, add the MS IAS server as a RADIUS server in the **Security > RADIUS Authentication** page.

Complete these steps:

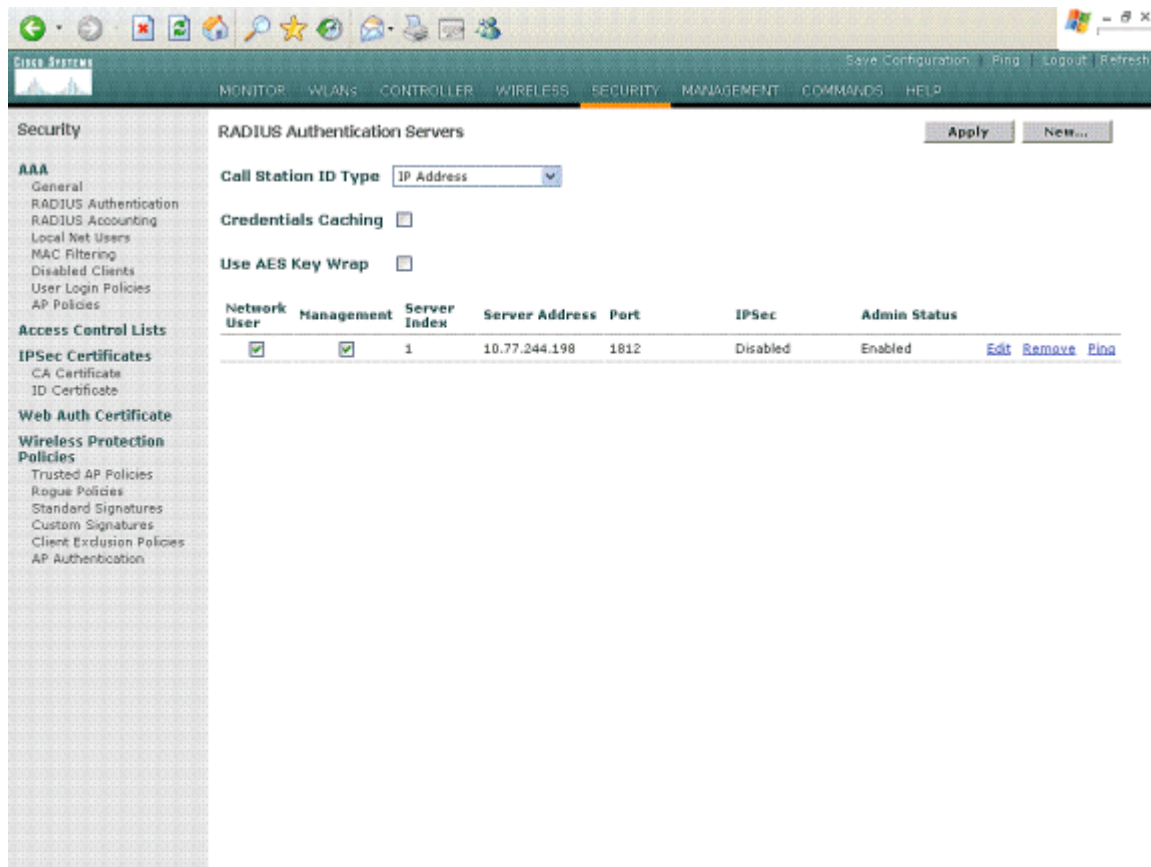
1. Choose **Security** and **RADIUS Authentication** from the controller GUI to display the RADIUS Authentication Servers page. Then click **New** in order to define a RADIUS server.

The screenshot shows the Cisco Systems GUI for configuring RADIUS Authentication Servers. The page title is "RADIUS Authentication Servers > New". The sidebar on the left lists various configuration categories under "Security", including AAA, Access Control Lists, IPsec Certificates, Web Auth Certificate, and Wireless Protection Policies. The main content area contains the following fields and options:

- Server Index (Priority):** A dropdown menu set to "1".
- Server IP Address:** A text input field containing "10.77.244.198".
- Shared Secret Format:** A dropdown menu set to "ASCII".
- Shared Secret:** A text input field with masked characters (dots).
- Confirm Shared Secret:** A text input field with masked characters (dots).
- Key Wrap:** A checkbox that is currently unchecked.
- Port Number:** A text input field containing "1812".
- Server Status:** A dropdown menu set to "Enabled".
- Support for RFC 3576:** A dropdown menu set to "Enabled".
- Retransmit Timeout:** A text input field containing "2" followed by the unit "seconds".
- Network User:** A checkbox that is checked, with the label "Enable".
- Management:** A checkbox that is checked, with the label "Enable".
- IPsec:** A checkbox that is unchecked, with the label "Enable".

At the top right of the main area, there are buttons for "< Back" and "Apply".

2. Define the RADIUS server parameters in the **RADIUS Authentication Servers > New** page. These parameters include the RADIUS Server IP Address, Shared Secret, Port Number, and Server Status. The Network User and Management check boxes determine if the RADIUS-based authentication applies for management and network users. This example uses the MS IAS as the RADIUS server with IP address 10.77.244.198.



3. Click **Apply**.
4. MS IAS server has been added to the WLC as a Radius server and can be used to authenticate Wireless Clients.

Configure a WLAN for the Clients

Configure the SSID (WLAN) to which the Wireless clients connects. In this example, create the SSID, and name it **PEAP**.

Define the Layer 2 Authentication as WPA2 so that the clients perform EAP based authentication (PEAP-MSCHAPv2 in this case) and use AES as the encryption mechanism. Leave all other values at their defaults.

Note: This document binds the WLAN with the management interfaces. When you have multiple VLANs in your network, you can create a separate VLAN and bind it to the SSID. For information on how to configure VLANs on WLCs, refer to [VLANs on Wireless LAN Controllers Configuration Example](#).

In order to configure a WLAN on the WLC complete these steps:

1. Click **WLANs** from the GUI of the controller in order to display the WLANs page. This page lists the WLANs that exist on the controller.
2. Choose **New** in order to create a new WLAN. Enter the WLAN ID and the WLAN SSID for the

WLAN, and click **Apply**.

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The 'WLANs' tab is selected. On the left, a sidebar shows the configuration tree with 'WLANs' expanded. The main content area is titled 'WLANs > New'. It contains two fields: 'WLAN ID' with a dropdown menu showing '1', and 'WLAN SSID' with a text box containing 'PEAP'. At the top right of the main area, there are '< Back' and 'Apply' buttons. The bottom of the page is a light gray grid.

3. Once you create a new WLAN, the **WLAN > Edit** page for the new WLAN appears. On this page you can define various parameters specific to this WLAN that include General Policies, RADIUS Servers, Security Policies, and 802.1x Parameters.

The screenshot shows the Cisco Systems WLAN configuration interface. The left sidebar has a tree view with 'WLANs' selected. The main content area is titled 'WLANs > Edit' and shows configuration for 'WLAN ID 1'. The 'Profile Name' is 'PEAP' and the 'WLAN SSID' is 'PEAP'. There are two main sections: 'General Policies' and 'Security Policies'.

General Policies:

- Radio Policy: All
- Admin Status: ☒ Enabled
- Session Timeout (secs): 0
- Quality of Service (QoS): Silver (best effort)
- WMM Policy: Disabled
- 7920 Phone Support: ☐ Client CAC Limit ☐ AP CAC Limit
- Broadcast SSID: ☒ Enabled
- Aironet IE: ☒ Enabled
- Allow AAA Override: ☐ Enabled
- Client Exclusion: ☒ Enabled ** 60 (Timeout Value (secs))
- DHCP Server: ☐ Override
- DHCP Addr. Assignment: ☐ Required
- Interface Name: management
- MFP Version Required: 1
- MFP Signature Generation: ☒ (Global MFP Disabled)
- H-REAP Local Switching: ☐

Security Policies:

- IPv6 Enable: ☐
- Layer 2 Security: WPA1+WPA2
 - ☐ MAC Filtering
- Layer 3 Security: None
 - ☐ Web Policy *

* Web Policy cannot be used in combination with IPsec.
 ** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)
 *** CKIP is not supported by 10xx APs

* H-REAP Local Switching not supported with IPSEC, CRANITE and FORTRESS authentications.

- Check **Admin Status** under General Policies in order to enable the WLAN. If you want the AP to broadcast the SSID in its beacon frames, check **Broadcast SSID**.
- Under Layer 2 Security, choose **WPA1+WPA2**. This enables WPA on the WLAN. Scroll down the page and choose the WPA policy. This example uses WPA2 and AES encryption. Choose the appropriate RADIUS server from the pull-down menu under RADIUS Servers. In this example, use **10.77.244.198** (IP address of the MS IAS server). The other parameters can be modified based on the requirement of the WLAN network.

The screenshot shows the 'WPA1+WPA2 Parameters' configuration page. The left sidebar has a tree view with 'WLANs' selected. The main content area is titled 'WPA1+WPA2 Parameters' and shows configuration for 'WPA1 Policy' and 'WPA2 Policy'.

WPA1+WPA2 Parameters:

- WPA1 Policy: ☐
- WPA2 Policy: ☒
- WPA2 Encryption: ☒ AES ☐ TKIP
- Auth Key Mgmt: 802.1x

- Click **Apply**.

Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies
PEAP	1	PEAP	Enabled	[WPA2][Auth(802.1x)]

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

Configure the Wireless Clients

Configure the Wireless Clients for PEAP-MS CHAPv2 Authentication

This example provides information on how to configure the Wireless client with Cisco Aironet Desktop Utility. Before you configure the client adapter, ensure that the latest version of the firmware and utility are used. Find the latest version of the firmware and utilities in the Wireless downloads page on Cisco.com.

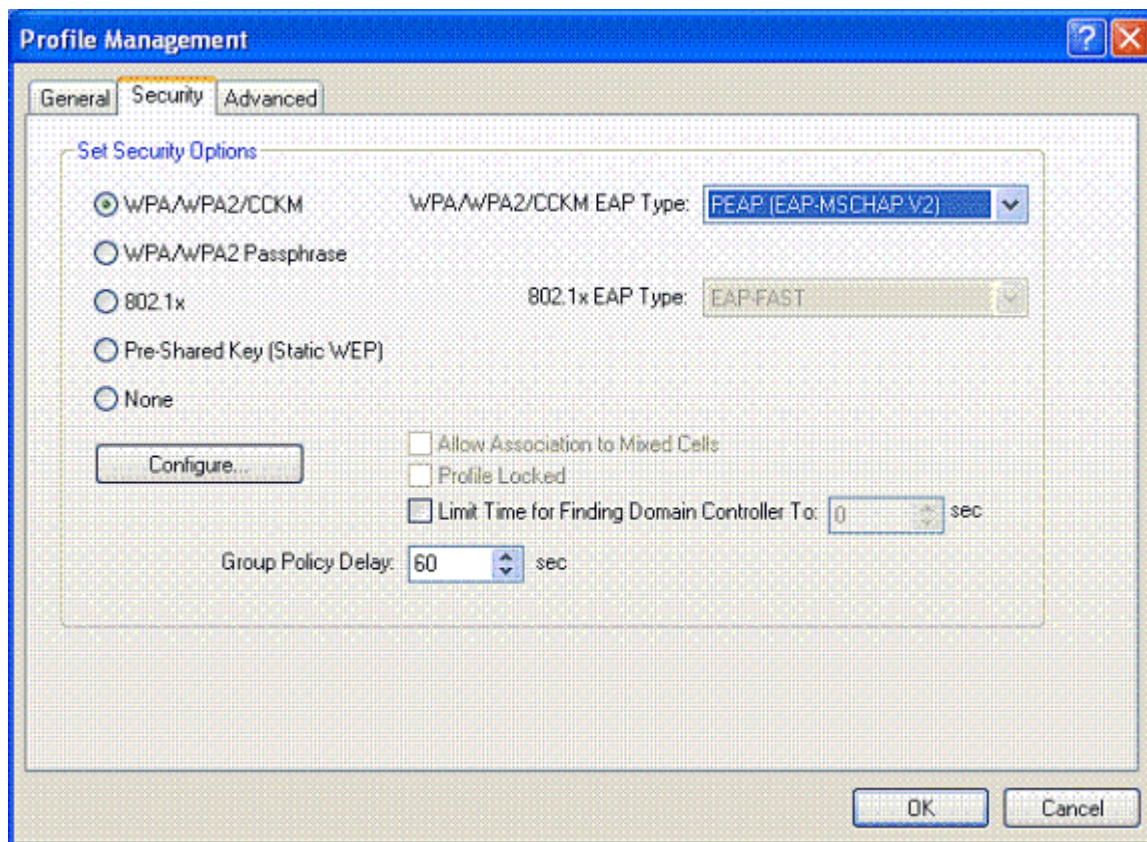
In order to configure the Cisco Aironet 802.11 a/b/g Wireless client adapter with the ADU, complete these steps:

1. Open the Aironet Desktop Utility.
2. Click **Profile Management**, and click **New** to define a profile.
3. Under the General tab, enter the Profile name and SSID. In this example, use the SSID that you configured on the WLC (PEAP).

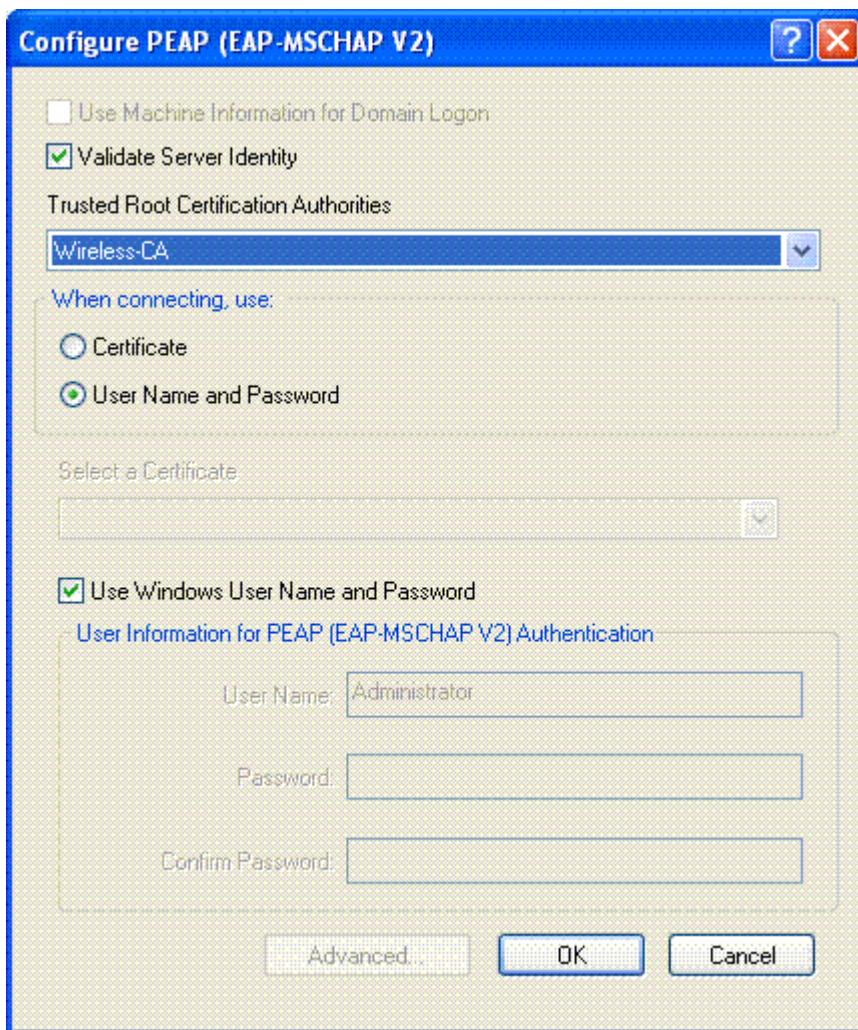
The screenshot shows a 'Profile Management' dialog box with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected. It contains two sections: 'Profile Settings' and 'Network Names'. In 'Profile Settings', 'Profile Name' is 'PEAP-MSCHAPv2' and 'Client Name' is 'CLIENT1'. In 'Network Names', 'SSID1' is 'PEAP', while 'SSID2' and 'SSID3' are empty. At the bottom right are 'OK' and 'Cancel' buttons.

Field	Value
Profile Name	PEAP-MSCHAPv2
Client Name	CLIENT1
SSID1	PEAP
SSID2	
SSID3	

4. Choose the Security tab; choose **WPA/WPA2/CCKM**; under WPA/WPA2/CCKM EAP, type choose **PEAP [EAP-MSCHAPv2]**, and click **Configure**.



5. Choose **Validate Server Certificate**, and choose **Wireless-CA** under the Trusted Root Certificate Authorities drop-down menu.

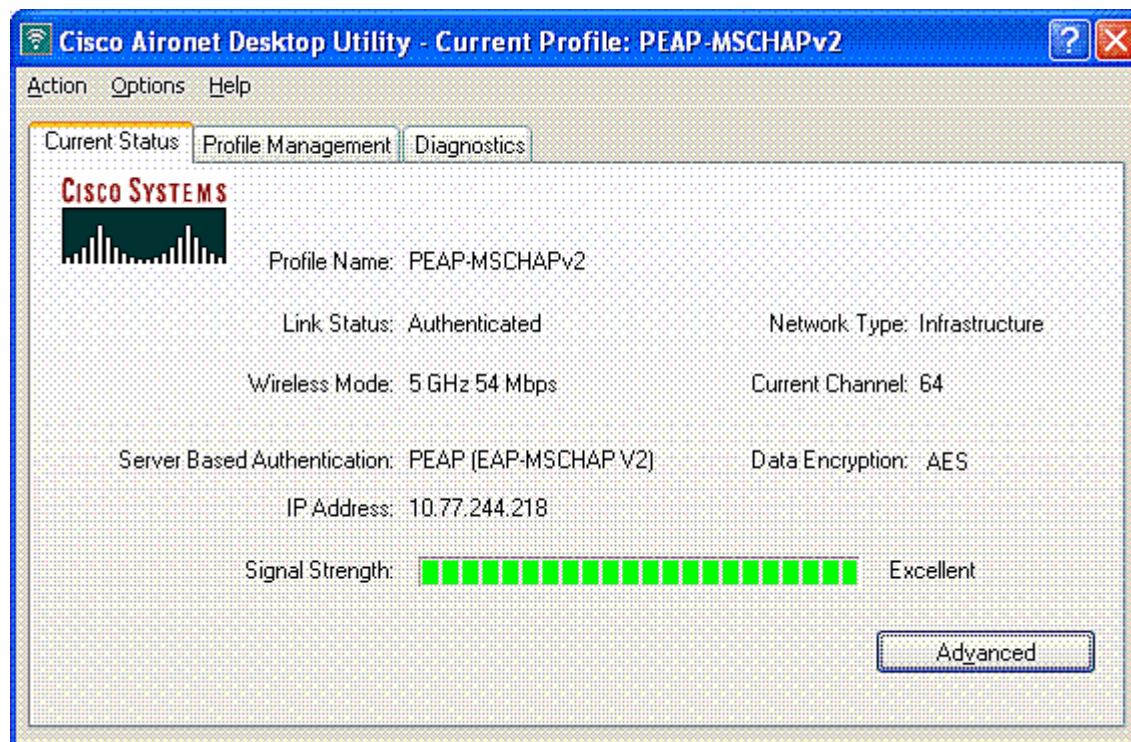


6. Click **OK**, and activate the profile.

Note: When you use Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2 (PEAP-MSCHAPv2) with Microsoft XP SP2, and the Wireless card is managed by the Microsoft Wireless Zero Configuration (WZC), you must apply the Microsoft hotfix KB885453. This prevents several issues on authentication related to PEAP Fast Resume.

Verify and Troubleshoot

In order to verify if the configuration works as expected, activate the profile PEAP-MSCHAPv2 on the Wireless client Client1.



Once the profile PEAP-MSCHAPv2 is activated on the ADU, the client performs 802.11 open authentication and then performs PEAP-MSCHAPv2 authentication. Here is an example of successful PEAP-MSCHAPv2 authentication.

Use the debug commands to understand the sequence of events that occur.

The [Output Interpreter Tool](#) ([registered](#) customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

These debug commands on the Wireless LAN Controller are useful.

- **debug dot1x events enable** —In order to configure the debugging of 802.1x events
- **debug aaa events enable** —In order to configure the debugging of AAA events
- **debug mac addr <mac address>** —In order to configure MAC debugging, use the debug mac command
- **debug dhcp message enable** —In order to configure debug of DHCP error messages

These are the example outputs from the **debug dot1x events enable** command and **debug client <mac address>** command.

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 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 06:58:51 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)**

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)**

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 06:58:51 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)**

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)**

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 06:58:51 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)**

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)**

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 06:58:51 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)**

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25)**

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 06:58:51 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 7)**

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25)**

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 06:58:51 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 8)**

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25)**

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 06:58:51 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 9)**

Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)**

Tue Dec 18 06:58:52 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 EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)**

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)**

Tue Dec 18 06:58:52 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 EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)**

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)**

Tue Dec 18 06:58:52 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 EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 12)**

```

Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from
mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Accept for
mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Creating a new PMK Cache
Entry for station 00:40:96:ac:e6:57 (RSN 0)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP-Success to
mobile 00:40:96:ac:e6:57 (EAP Id 13)
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 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 Associat
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 Associat
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

```

Note: If you use the Microsoft Supplicant to authenticate with a Cisco Secure ACS for PEAP authentication, the client potentially does not authenticate successfully. Sometimes the initial connection can authenticate successfully, but subsequent fast-connect authentication attempts do not connect successfully. This is a known issue. The details of this issue and the fix for the same are available [here](#)



NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums - Featured Conversations for Wireless
Wireless - Mobility: WLAN Radio Standards
Help with my cisco 1100 series access point - Feb 21, 2008 Issues With Vista - Feb 20, 2008 WLC and Intermec 2455 terminals - Feb 19, 2008 ASK THE EXPERT - MOBILE PERFORMANCE WITH 802.11n - Feb 19, 2008 Interference threshold violated - Feb 19, 2008
Wireless - Mobility: Security and Network Management
ipsec and default route issue - Feb 22, 2008 WLC 5.0.148.0 release notes - Feb 21, 2008 Max. number of WLCs per WCS - Feb 21, 2008

WLSE Express with IOS APs error message - Feb 20, 2008
QoS/bandwidth throttling on autonomous WAPs? - Feb 20, 2008
Wireless - Mobility: Wireless IP Voice and Video
Push-to-talk with Nortel 6140 wireless handset + WLC 4400 - Feb 22, 2008
7921G call drops and one way audio. - Feb 21, 2008
VPN Client for Nokia E-Series Mobile - Feb 20, 2008
Voice quality very poor - Feb 20, 2008
7921G Firmware update - Feb 13, 2008
Wireless - Mobility: Getting Started with Wireless
Getting wireless to work on a 876W - Feb 22, 2008
Upgrade of AP1210 system - Feb 22, 2008
DHCP with WLC 526 and LAP521 - Feb 22, 2008
Wireless Deployment - Feb 21, 2008
WLC526 DHCP issue - Feb 21, 2008
Wireless - Mobility: General
WISM backup via TFTP - Feb 22, 2008
AIR-AP1220-IOS-UPGRD - Feb 22, 2008
NM-WLC Upload Configuration Issue - Feb 22, 2008
Recommended Antenna 1242AG - Feb 22, 2008
1130AG Access Point PoE Problem with Cat 3750G-24PS-E switch - Feb 21, 2008

Related Information

- [PEAP under Unified Wireless Networks with ACS 4.0 and Windows 2003](#)
- [EAP Authentication with WLAN Controllers \(WLC\) Configuration Example](#)
- [Wireless LAN Controller \(WLC\) Software Upgrade to Versions 3.2, 4.0, and 4.1](#)
- [Cisco 4400 Series Wireless LAN Controllers Configuration Guides](#)
- [Technical Support & Documentation - Cisco Systems](#)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).