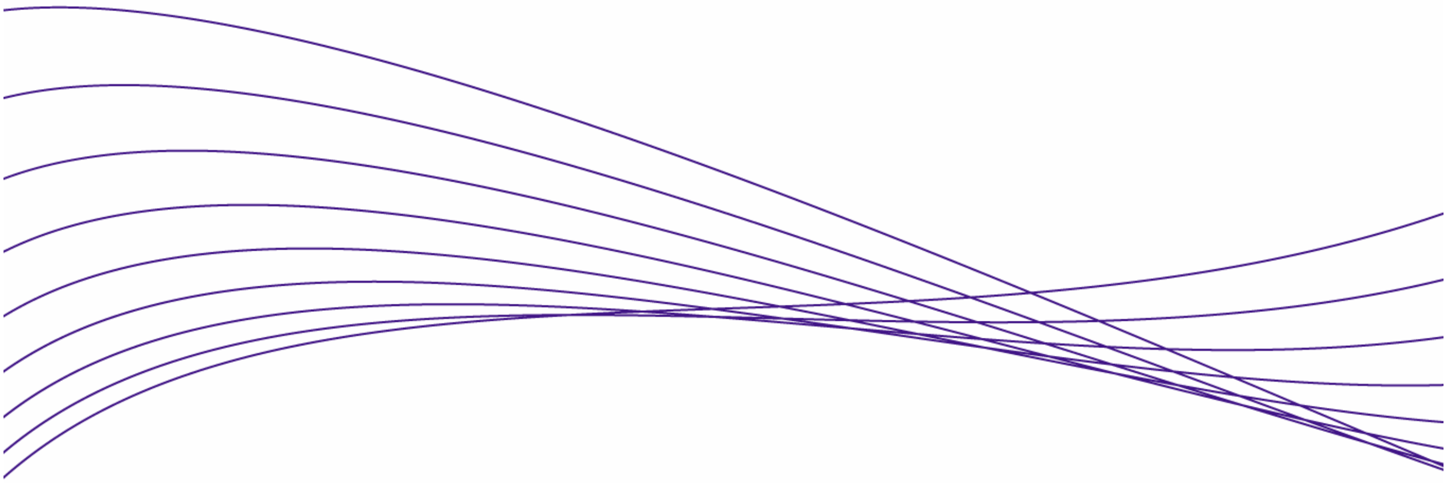
ProCurve Networking

Secure Access Configuration Guide For Wireless Clients

Part Two: Wireless Data Privacy and Monitored Logon



Secure Access Configuration Guide For Wireless Clients

Introduction

This document is Part Two of a guide that details the configuration steps for building Secure Access Solutions for Wireless Clients. Part Two of this guide creates solutions for clients using wireless data privacy or monitored logons. Part One creates solutions for clients using a browser-based logon.

The following ProCurve Networking by HP products are used:

- ProCurve Access Control Server 740wl (J8154A)
- ProCurve Access Point 420 (J8130A)
- ProCurve Access Control xl Module (J8162A)
- ProCurve Switch 5300xl (J4850A)

Configuration Scenarios

This table defines the configuration scenarios covered in Part Two of this guide.

Scenario	Secure Access Method	Airwave Security	IP address	Authentication	Client OS
1	Browser-based Logon	Static WEP	NAT	Built-in Database	Windows XP
2	Browser-based Logon	WPA-PSK	Real IP	LDAP	Windows XP
3	Browser-based Logon	Static WEP	Real IP	RADIUS	Windows 2000
4	Wireless Data Privacy Logon	PPTP VPN	NAT	VPN	Windows XP
5	Wireless Data Privacy Logon	L2TP/IPSec	NAT/Real IP	VPN	Windows XP
6	Monitored Logon (802.1x)	Dynamic WEP/802.1x	Real IP	Active Directory /RADIUS	Windows XP

Required Network Services

The configuration scenarios in the guide require the network services noted below, however, complete server installation and configuration are not shown here with the exception of specific changes required by the configuration scenario. Refer to product documentation for more information.

Microsoft 2003 Enterprise Server with the following running services:

- Microsoft Internet Authentication Service (IAS)
- Domain Controller
- Certificate Authority
- DHCP
- DNS
- Wins
- RRAS

Basic Setup and Topology

This basic setup and topology is used in this guide to configure the above scenarios.

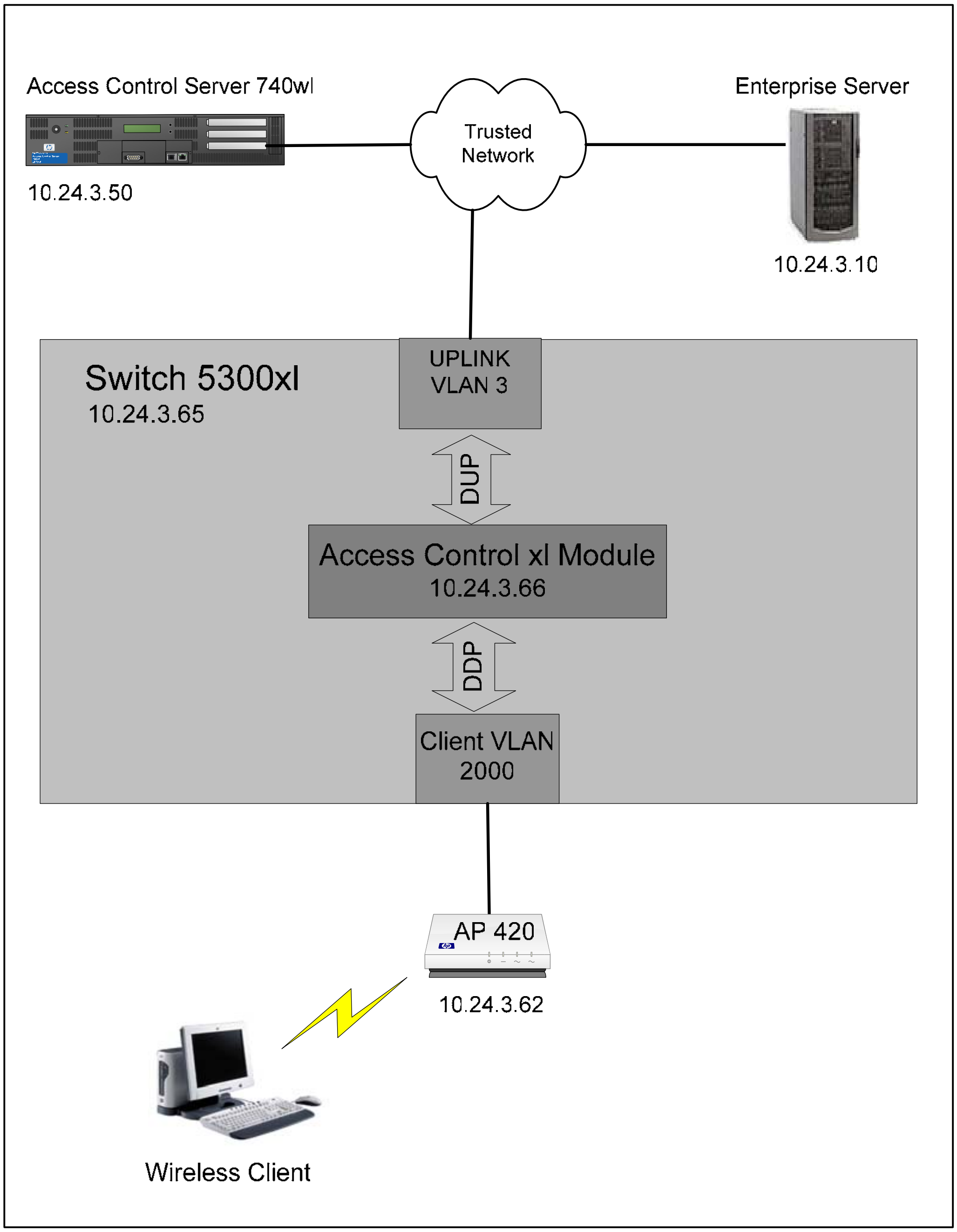


Figure A – Basic Topology

Software Versions

The table below details the software versions used for the ProCurve network equipment in this guide. For the latest software versions or more info, visit the ProCurve Networking by HP Web site (http://www.procurve.com).

Device	Version
Switch 5300xl	E.09.21
Access Control xl Module	4.1.3.93
Access Control Server 740wl	4.1.3.93
Access Point 420	2.0.38

Getting Started

Getting started with the configuration scenarios in this guide requires completion of steps 1 through 4 below to get the infrastructure prepared.

To get started, refer to the **Basic Setup and Topology** (Figure A) and complete the following tasks:

- Step 1: Configuring the Switch 5300xl
- Step 2: Configuring the Access Control Server 740wl
- Step 3: Configuring the Access Control xl Module
- Step 4: Configuring the Access Point 420

After completing Steps 1-4, then proceed to the desired Configuration Scenario.

Step 1: Configuring the Switch 5300xl

In this example configuration, the Access Control xl Module (ACM) is inserted into **slot D** of the Switch 5300xl. However, any open 5300xl switch slot may be used. For example, if the ACM is inserted in slot A, the uplink port designation would be “aup”.

Power up the switch, insert the ACM, connect a serial console cable and configure the following at the Switch 5300xl CLI:

1. Configure the default gateway on the switch.
2. Configure an uplink VLAN (`vlan 3`), IP address and subnet mask
3. Add a port (`a1`) to the uplink VLAN.
4. Add the ACM uplink port (`dup`) to the uplink VLAN (`vlan 3`).
5. Add a port (`b1`) to VLAN 2000.

Note: Upon insertion of the ACM into the Switch 5300xl, VLAN 2000 is automatically created by default and the downlink port (`ddp`) is added to this VLAN as a tagged member.

```
5300xl> en
5300xl# config term
5300xl(config)# ip default-gateway 10.24.3.1
5300xl(config)# vlan 3
5300xl(vlan-3)# ip address 10.24.3.65/24
5300xl(vlan-3)# untag a1
5300xl(vlan-3)# untag dup
5300xl(vlan-3)# vlan 2000
5300xl(vlan-2000)# untag b1
```

Step 2: Configuring the Access Control Server 740wl

This example uses an Access Control Server 740wl. The configuration steps are the same if you are using an Integrated Access Manager 760wl.

Power up the ACS, connect a serial console cable and configure the following at the ACS CLI:

1. Configure an IP address, subnet mask and default gateway.
2. Configure the shared secret (`secret`).

```
HP 700wl Series@[42.0.0.1]: set ip 10.24.3.50 255.255.255.0
HP 700wl Series@[10.24.3.50]: set gateway 10.24.3.1
HP 700wl Series@[10.24.3.50]: set sharedsecret secret secret
```

Step 3: Configuring the Access Control xl Module

To configure the ACM, go to the Switch 5300xl CLI and configure the following:

1. Enter the Access Controller configuration context.
2. Set the IP address, subnet mask and default gateway of the ACM.
3. Set the IP address of the Access Control Server 740wl that will be used to manage the ACM.
4. Set the shared secret (secret) to match the configuration on the ACS.

```
5300xl> en
5300xl# config term
5300xl(config)# access-controller d
5300xl(access-controller-D)# enable extended-commands
5300xl(access-controller-D-ext)# set ip 10.24.3.66/24
5300xl(access-controller-D-ext)# set gateway 10.24.3.1
5300xl(access-controller-D-ext)# set accesscontrolserver 10.24.3.50
5300xl(access-controller-D-ext)# set sharedsecret secret secret
```

Use the “**show status**” command to verify that the ACM is connected to the ACS.

```
5300xl(access-controller-D-ext)# show status
     Uptime:     1 hr, 7 mins.
     Access Controller Function
            Access Control Server: 10.24.3.50
            Connected: 10 mins, 27 secs
            Active Clients:  0
            Total Sessions:  0
```

Step 4: Configuring the Access Point 420

Initial configuration of the Access Point 420 for this guide requires two tasks be completed.

1. <u>Configuring the Access Point for general network and wireless</u>
   Connect a serial console cable to the AP 420 and configure the following at the AP 420 CLI:

   - IP address, subnet mask and gateway.

- Enable the Access Point radio
- Wireless SSID (`x52800cb2`) and channel (`6`).

```
HP ProCurve Access Point 420# configure
Enter configuration commands, one per line. End with CTRL/Z
HP ProCurve Access Point 420(config)# int eth
Enter Ethernet configuration commands, one per line.
HP ProCurve Access Point 420(if-ethernet)# no ip dhcp
HP ProCurve Access Point 420(if-ethernet)# ip addr 10.24.3.62
255.255.255.0 10.24.3.1
HP ProCurve Access Point 420(if-ethernet)# end
HP ProCurve Access Point 420(config)# int wireless g
Enter Wireless configuration commands, one per line.
HP ProCurve Access Point 420(if-wireless g)# no shut
HP ProCurve Access Point 420(if-wireless g)# ssid x52800cb2
HP ProCurve Access Point 420(if-wireless g)# channel 6
```

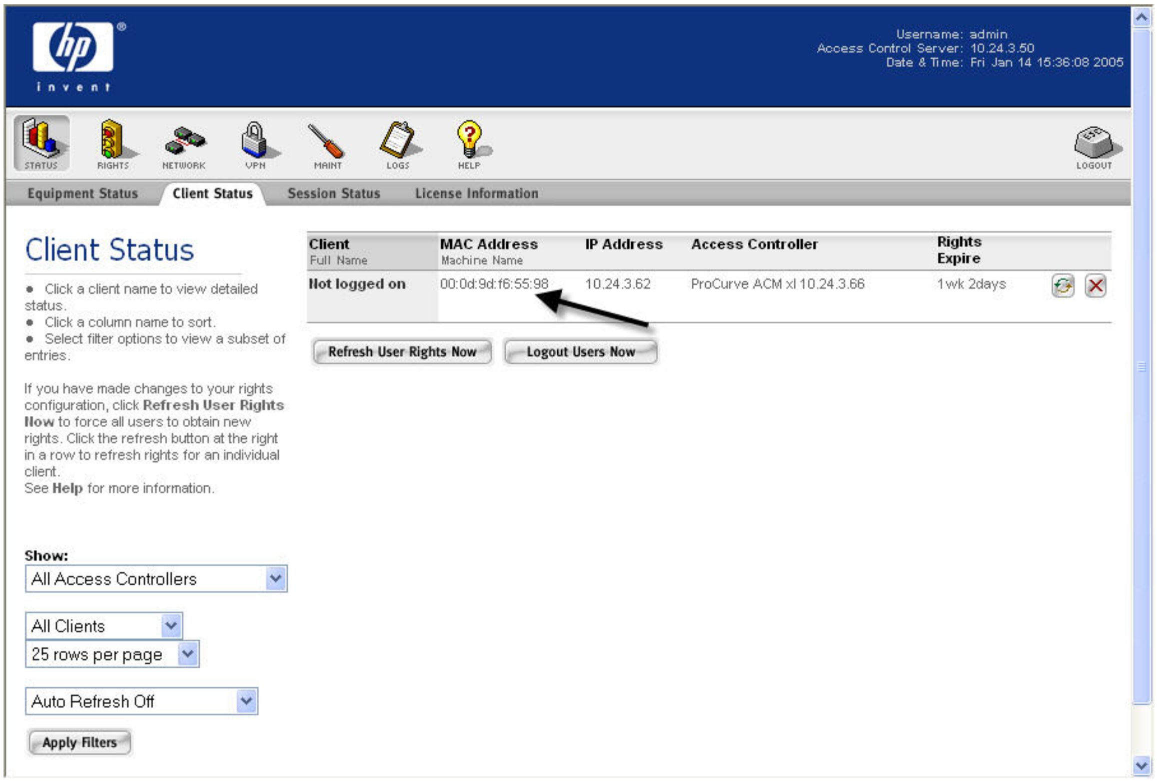
2. Configuring the ACS to recognize the AP 420 as "Network Equipment"

Connect the AP 420 to the network (see Figure A) and open the Web browser management interface to the ACS. Enter the username and password (default shown here) of the ACS:

Username: **admin**

Password: **admin**

a) Browse to Status -> Client Status and copy the **MAC address** of the AP 420.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Fri Jan 14 15:36:08 2005

Client Status

- Click a client name to view detailed status.
- Click a column name to sort.
- Select filter options to view a subset of entries.

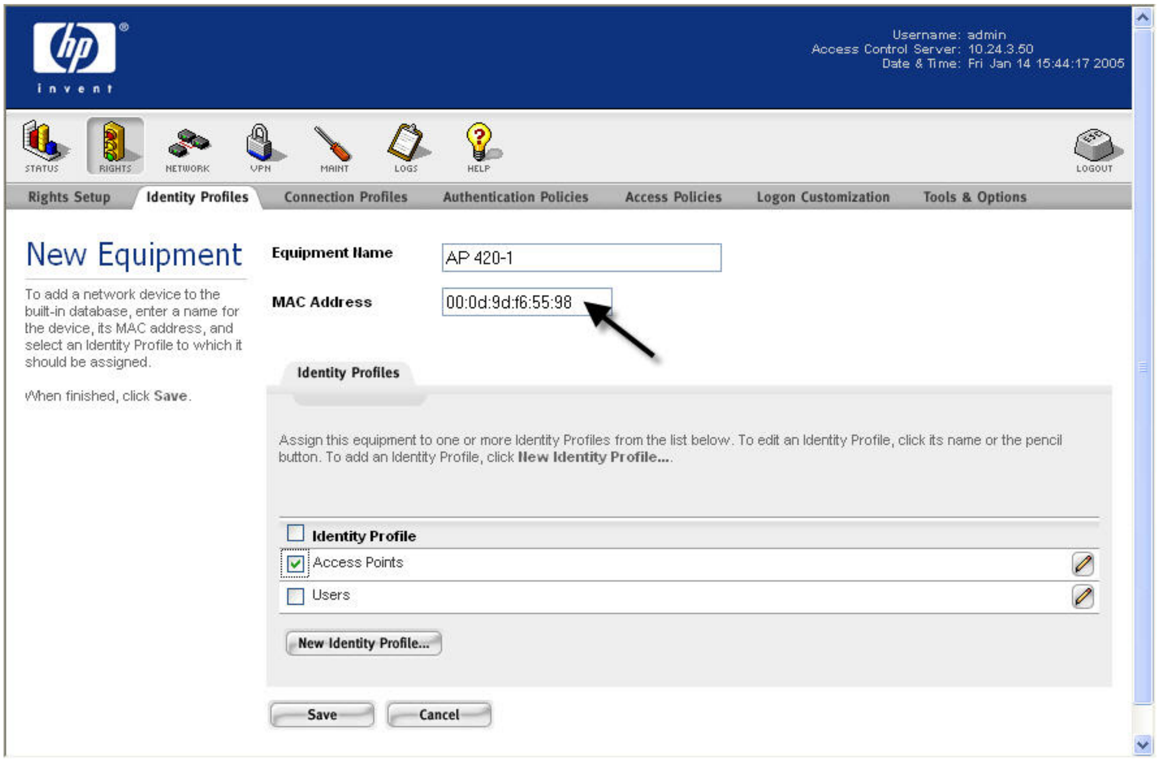
If you have made changes to your rights configuration, click **Refresh User Rights Now** to force all users to obtain new rights. Click the refresh button at the right in a row to refresh rights for an individual client.
See **Help** for more information.

Show:
All Access Controllers
All Clients
25 rows per page
Auto Refresh Off

Client Full Name	MAC Address Machine Name	IP Address	Access Controller	Rights Expire
Not logged on	00:0d:9d:f6:55:98	10.24.3.62	ProCurve ACM xl 10.24.3.66	1wk 2days

Figure B – Client Status Page

b) Browse to Rights -> Identity Profiles and Select Network Equipment. Click on New Equipment, input a descriptive name (`AP 420-1`) and paste the MAC address into the MAC Address field. Select the **Access Point Identify Profile** and save changes.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Fri Jan 14 15:44:17 2005

New Equipment

To add a network device to the built-in database, enter a name for the device, its MAC address, and select an Identity Profile to which it should be assigned.

When finished, click **Save**.

Equipment Name AP 420-1

MAC Address 00:0d:9d:f6:55:98

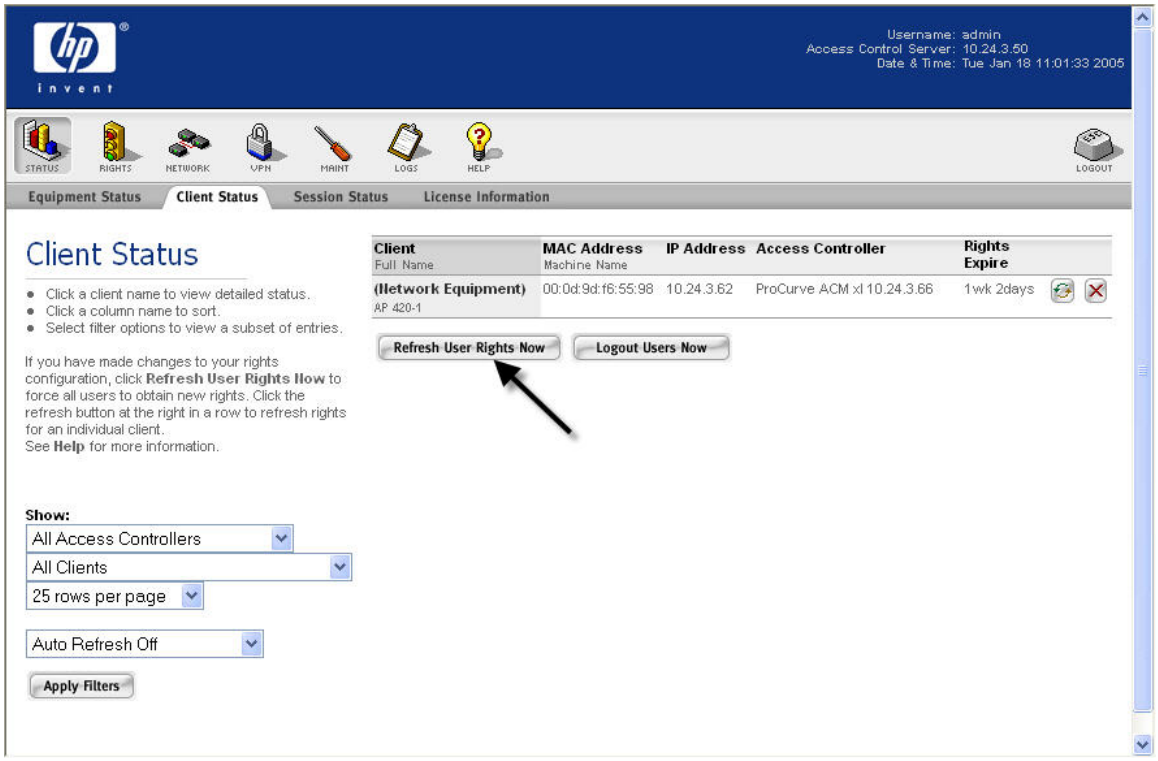
Identity Profiles

Assign this equipment to one or more Identity Profiles from the list below. To edit an Identity Profile, click its name or the pencil button. To add an Identity Profile, click **New Identity Profile...**.

☐ **Identity Profile**
☑ Access Points
☐ Users

Figure C – New Equipment Page

c) Browse to Status -> Client Status and click Refresh User Rights Now. The AP 420 is now recognized by the ACS as “Network Equipment”.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Tue Jan 18 11:01:33 2005

Client Status

- Click a client name to view detailed status.
- Click a column name to sort.
- Select filter options to view a subset of entries.

If you have made changes to your rights configuration, click **Refresh User Rights Now** to force all users to obtain new rights. Click the refresh button at the right in a row to refresh rights for an individual client.
See **Help** for more information.

Client Full Name	**MAC Address** Machine Name	**IP Address**	**Access Controller**	**Rights Expire**
(Network Equipment) AP 420-1	00:0d:9d:f6:55:98	10.24.3.62	ProCurve ACM xl 10.24.3.66	1wk 2days

Show:
All Access Controllers
All Clients
25 rows per page

Auto Refresh Off

Figure C – Client Status - Refresh User Rights Now

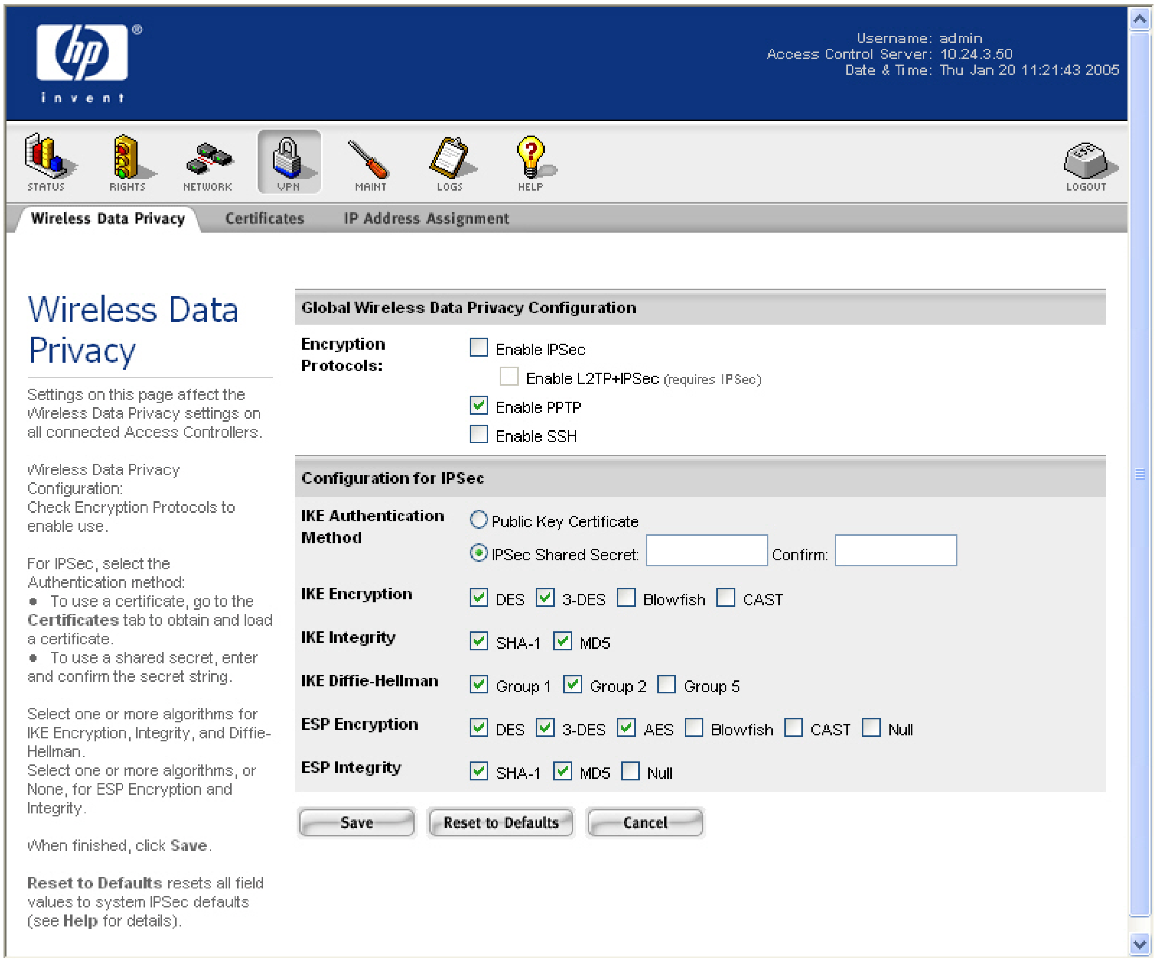
Configuring Scenario 4: Wireless Data Privacy Logon using VPN Authentication (PPTP)

Scenario 4 consists of a wireless, Windows XP client authenticating via a VPN. The VPN used in this example will be a PPTP VPN. Since VPN authentication requires a RADIUS backend, we will configure the ACS to authenticate VPN users against Internet Authentication Service (IAS), Microsoft's RADIUS implementation. In contrast to Browser-based logon, Wireless Data Privacy logon is automatic upon successful establishment of the VPN connection. The steps required are:

- On the ACS, enable PPTP VPN support globally.
- On the ACS, enable PPTP VPN support in both the Unauthenticated and Authenticated Access Policies.
- On the ACS, define a RADIUS Authentication Service, associate it to the System Authentication Policy, and enable the RADIUS server to authenticate the user during PPTP session negotiation.
- On the AP 420, configure open authentication wireless parameters.
- On the Windows XP client, connect the wireless client, configure PPTP client software (Windows XP native) and verify authentication.

1) **On the ACS, enable PPTP VPN support globally**.

   a. On the ACS, browse to VPN -> Wireless Data Privacy tab and click the **Enable PPTP** checkbox. Save changes.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Jan 20 11:21:43 2005

Wireless Data Privacy

Settings on this page affect the Wireless Data Privacy settings on all connected Access Controllers.

Wireless Data Privacy Configuration:
Check Encryption Protocols to enable use.

For IPSec, select the Authentication method:
- To use a certificate, go to the **Certificates** tab to obtain and load a certificate.
- To use a shared secret, enter and confirm the secret string.

Select one or more algorithms for IKE Encryption, Integrity, and Diffie-Hellman.
Select one or more algorithms, or None, for ESP Encryption and Integrity.

When finished, click **Save**.

Reset to Defaults resets all field values to system IPSec defaults (see **Help** for details).

Global Wireless Data Privacy Configuration

Encryption Protocols: ☐ Enable IPSec
☐ Enable L2TP+IPSec (requires IPSec)
☑ Enable PPTP
☐ Enable SSH

Configuration for IPSec

IKE Authentication Method ○ Public Key Certificate
● IPSec Shared Secret: ____ Confirm: ____

IKE Encryption ☑ DES ☑ 3-DES ☐ Blowfish ☐ CAST

IKE Integrity ☑ SHA-1 ☑ MD5

IKE Diffie-Hellman ☑ Group 1 ☑ Group 2 ☐ Group 5

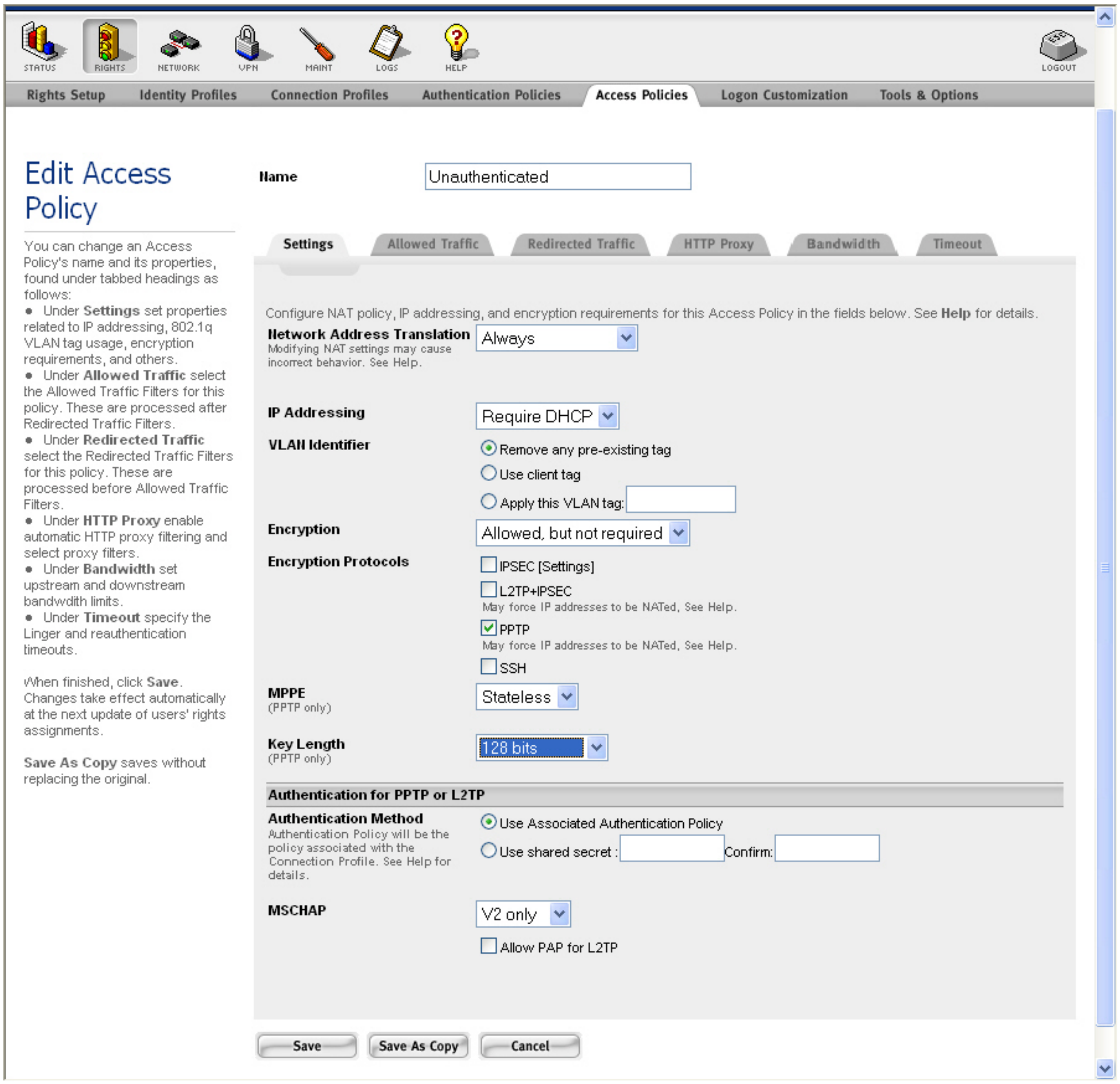
ESP Encryption ☑ DES ☑ 3-DES ☑ AES ☐ Blowfish ☐ CAST ☐ Null

ESP Integrity ☑ SHA-1 ☑ MD5 ☐ Null

Figure 4.1 – Wireless Data Privacy

b. On the ACS, browse to Rights -> Access Policies and select the **Unauthenticated** Access Policy. Configure the following parameters and save changes.

- Network Address Translation: **Always**
- IP Addressing: **Require DHCP**
- Encryption: **Allowed, but not required**
- Encryption Protocol: **PPTP**
- MPPE: **Stateless**
- Key Length: **128 bits**
- All other parameters in the **default** state.



Edit Access Policy

You can change an Access Policy's name and its properties, found under tabbed headings as follows:

- Under **Settings** set properties related to IP addressing, 802.1q VLAN tag usage, encryption requirements, and others.
- Under **Allowed Traffic** select the Allowed Traffic Filters for this policy. These are processed after Redirected Traffic Filters.
- Under **Redirected Traffic** select the Redirected Traffic Filters for this policy. These are processed before Allowed Traffic Filters.
- Under **HTTP Proxy** enable automatic HTTP proxy filtering and select proxy filters.
- Under **Bandwidth** set upstream and downstream bandwidth limits.
- Under **Timeout** specify the Linger and reauthentication timeouts.

When finished, click **Save**. Changes take effect automatically at the next update of users' rights assignments.

Save As Copy saves without replacing the original.

Name Unauthenticated

Configure NAT policy, IP addressing, and encryption requirements for this Access Policy in the fields below. See **Help** for details.

Network Address Translation Always
Modifying NAT settings may cause incorrect behavior. See Help.

IP Addressing Require DHCP

VLAN Identifier
● Remove any pre-existing tag
○ Use client tag
○ Apply this VLAN tag:

Encryption Allowed, but not required

Encryption Protocols
□ IPSEC [Settings]
□ L2TP+IPSEC
May force IP addresses to be NATed, See Help.
☑ PPTP
May force IP addresses to be NATed, See Help.
□ SSH

MPPE (PPTP only) Stateless

Key Length (PPTP only) 128 bits

Authentication for PPTP or L2TP

Authentication Method
Authentication Policy will be the policy associated with the Connection Profile. See Help for details.
● Use Associated Authentication Policy
○ Use shared secret : Confirm:

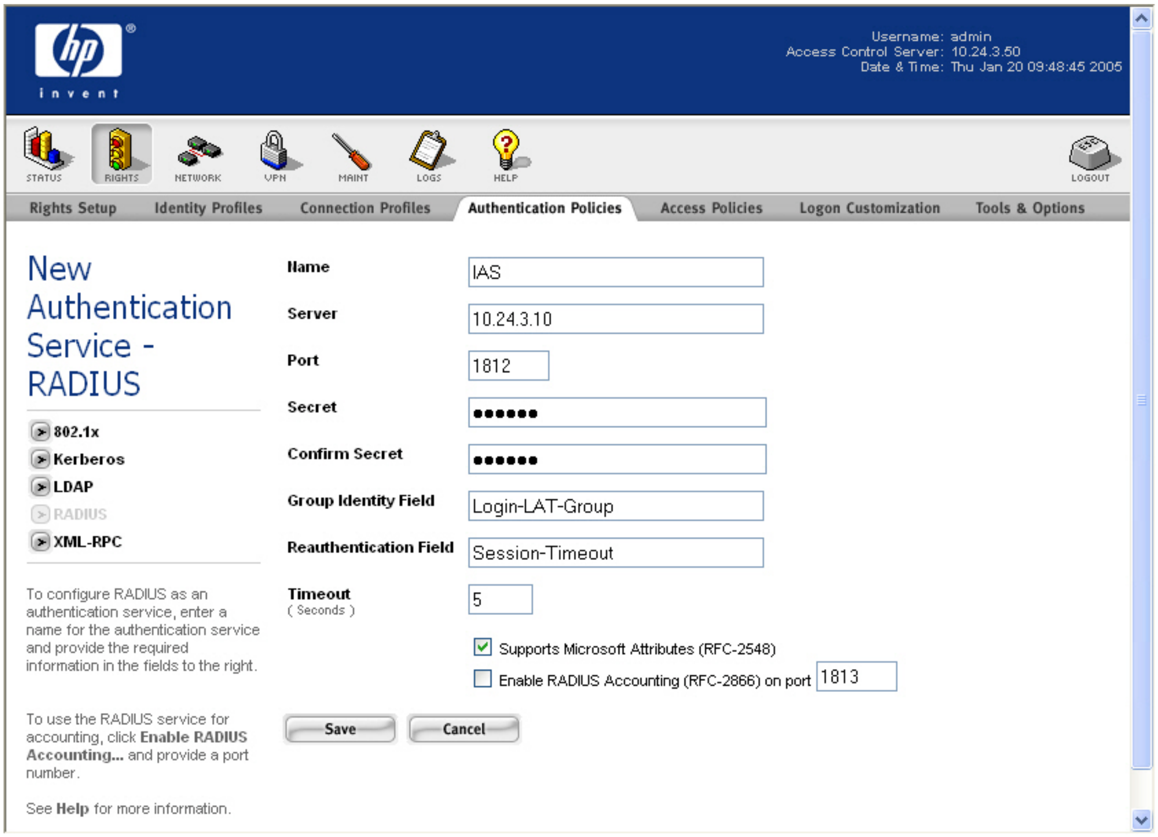
MSCHAP V2 only
□ Allow PAP for L2TP

Figure 4.2 – Unauthenticated Access Policy

c. Configure the **Authenticated** Access Policy **EXACTLY** the same as the **Unauthenticated** Access Policy and save changes.

2) **On the ACS, define a RADIUS Authentication Service, associate it to the System Authentication Policy, and enable the RADIUS server to authenticate the user during PPTP session negotiation**.

a. Follow the instructions using Configuring Scenario 3 to define a RADIUS Authentication Service and associate it to the System Authentication Policy. In addition, click the **Supports Microsoft Attribute (RFC-2548)** checkbox to enable the RADIUS server to authenticate the user during PPTP session negotiation.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Jan 20 09:48:45 2005

New Authentication Service - RADIUS

Name	IAS
Server	10.24.3.10
Port	1812
Secret	••••••
Confirm Secret	••••••
Group Identity Field	Login-LAT-Group
Reauthentication Field	Session-Timeout
Timeout (Seconds)	5

☑ Supports Microsoft Attributes (RFC-2548)

☐ Enable RADIUS Accounting (RFC-2866) on port 1813

To configure RADIUS as an authentication service, enter a name for the authentication service and provide the required information in the fields to the right.

To use the RADIUS service for accounting, click **Enable RADIUS Accounting...** and provide a port number.

See **Help** for more information.

Figure 4.3 – RADIUS Authentication Service

b. On the ACS, browse to Status -> Client Status and click **Refresh User Rights Now**.

3) On the AP 420, configure open authentication wireless parameters.

a. From the AP 420 CLI, configure **security suite 1** (open authentication, no encryption).

```
HP ProCurve Access Point 420# configure
HP ProCurve Access Point 420(config)# int wireless g
Enter Wireless configuration commands, one per line.
HP ProCurve Access Point 420(if-wireless g)# security-suite 1
```

4) **On the Windows XP client, connect the wireless client, configure PPTP client software (Windows XP native) and verify authentication.**

a. Connect the wireless Windows XP client to the AP 420 using open authentication/no encryption.

b. On the Windows XP client, open the Network connections window and click **Create a new connection**.

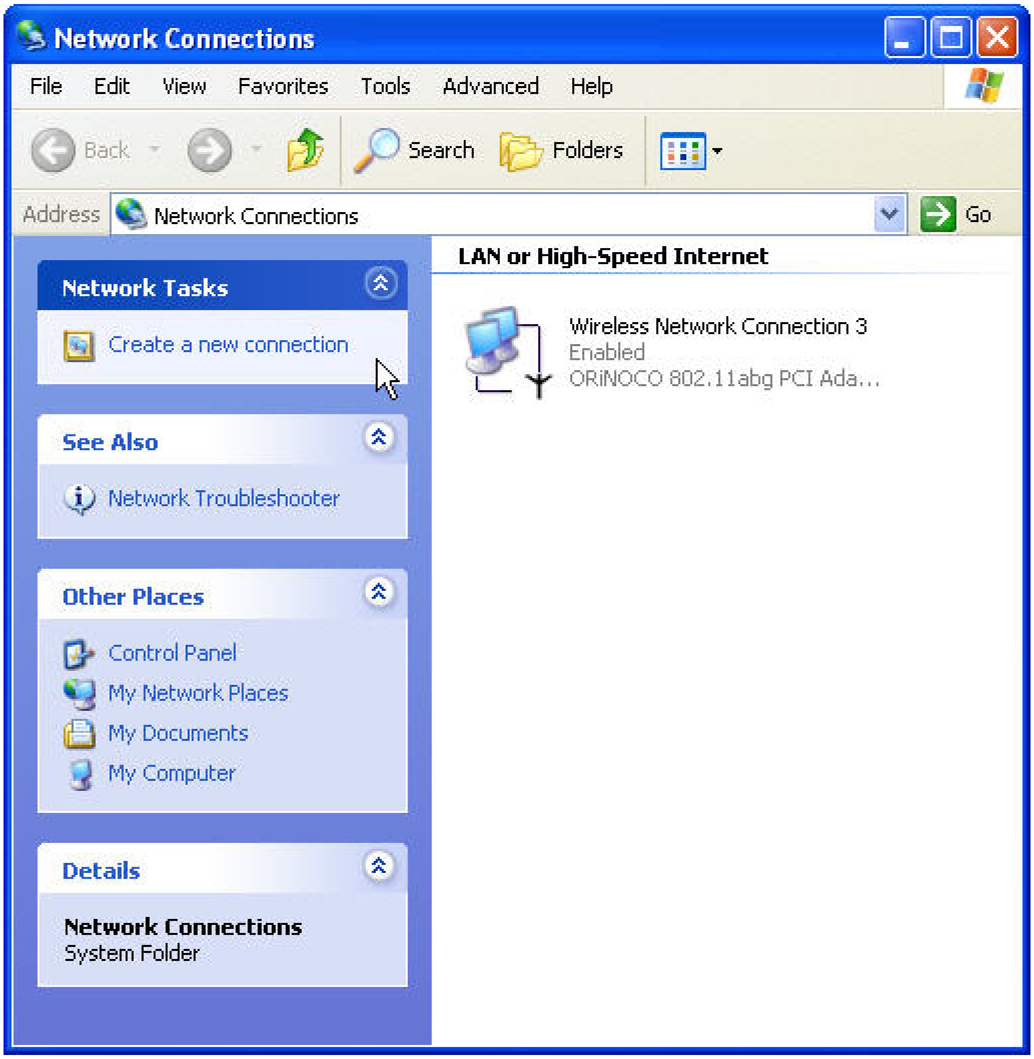
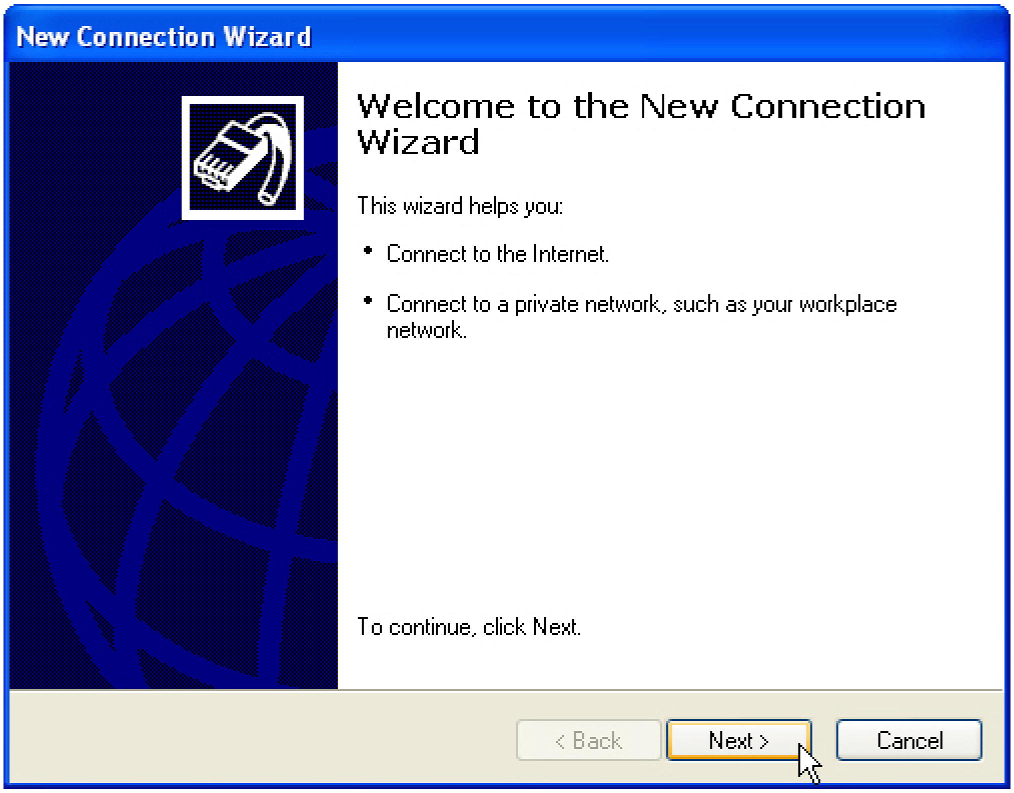


Figure 4.4 – Network Connections

c. Click **Next** to start the New Connection Wizard.



Welcome to the New Connection Wizard

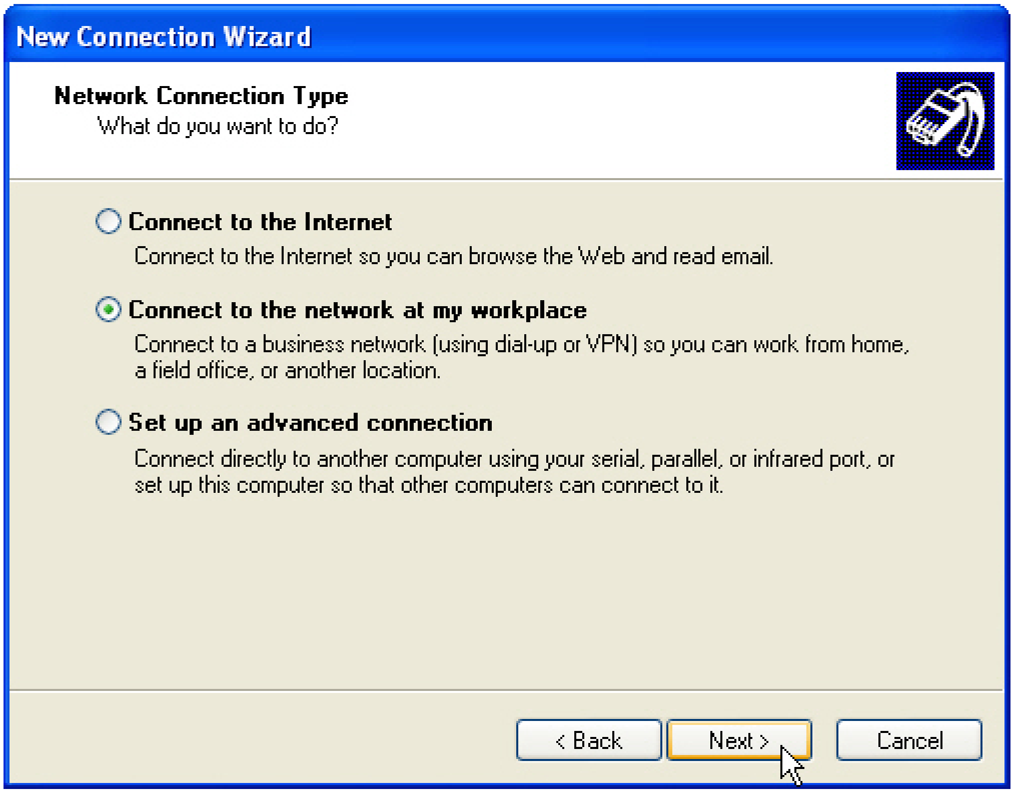
This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.

To continue, click Next.

Figure 4.5 – New Connection Wizard

d. For the Network Connection type, select the **Connect to the network at my workplace** radio button and click next.



Network Connection Type
What do you want to do?

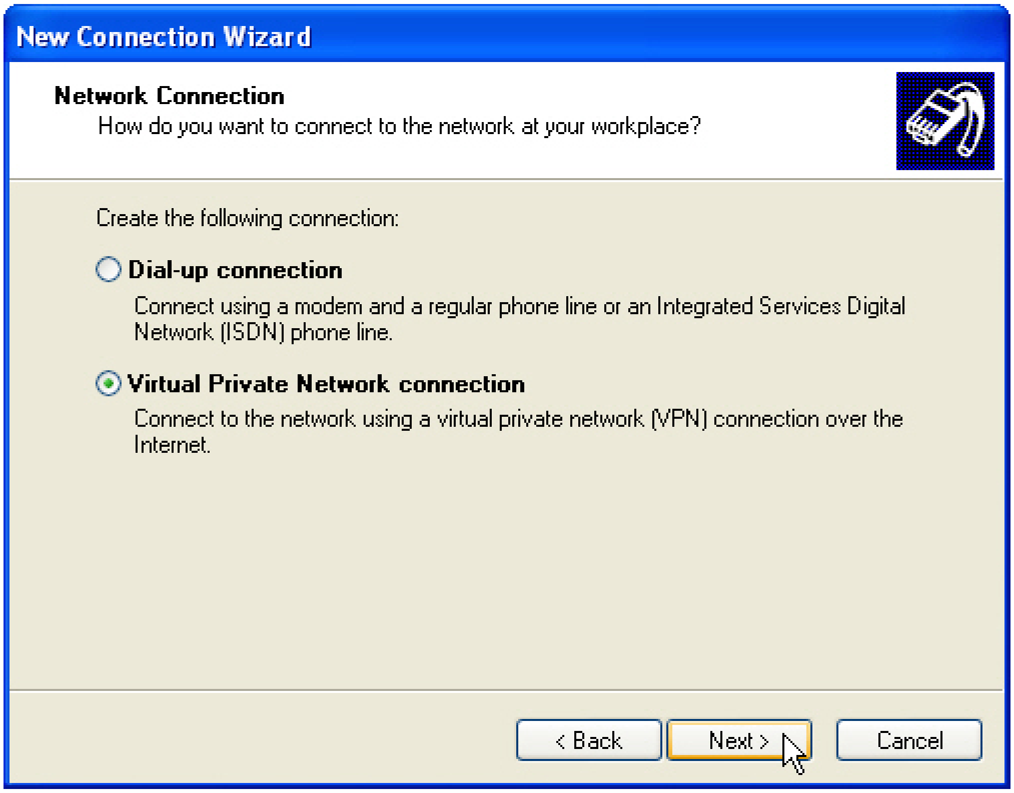
○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

Figure 4.6 – New Connection Wizard

e. Select the **Virtual Private Network connection** and click next.



New Connection Wizard

Network Connection

How do you want to connect to the network at your workplace?

Create the following connection:

○ **Dial-up connection**

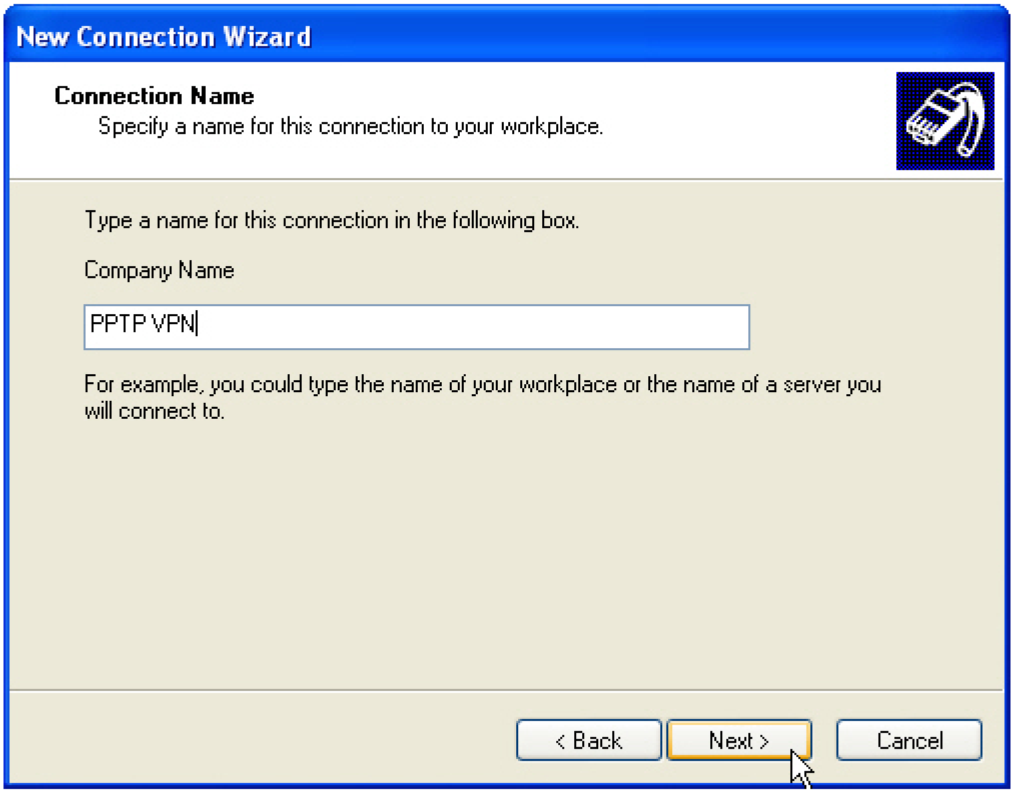
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**

Connect to the network using a virtual private network (VPN) connection over the Internet.

Figure 4.7 – New Connection Wizard

f. Configure a **Connection Name** (PPTP VPN) and click next.


New Connection Wizard

Connection Name

Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

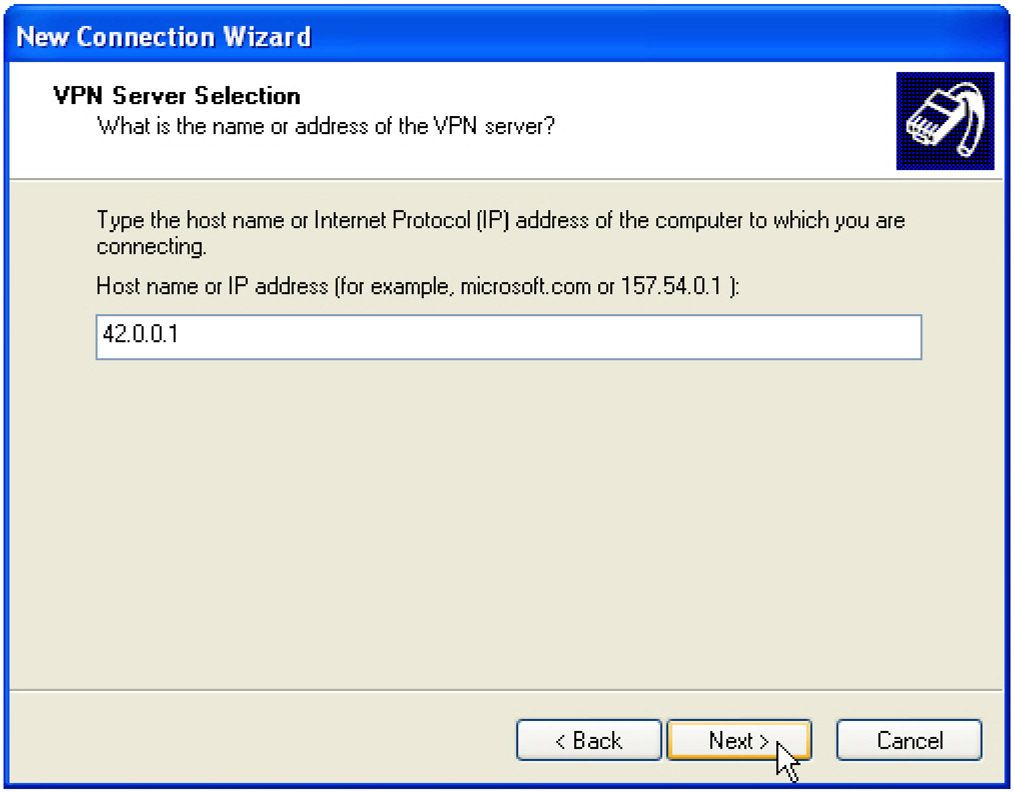
Company Name

PPTP VPN

For example, you could type the name of your workplace or the name of a server you will connect to.

Figure 4.8 – New Connection Wizard

g. Enter **42.0.0.1** as the IP address of the **VPN Server** and click next.


New Connection Wizard

VPN Server Selection

What is the name or address of the VPN server?

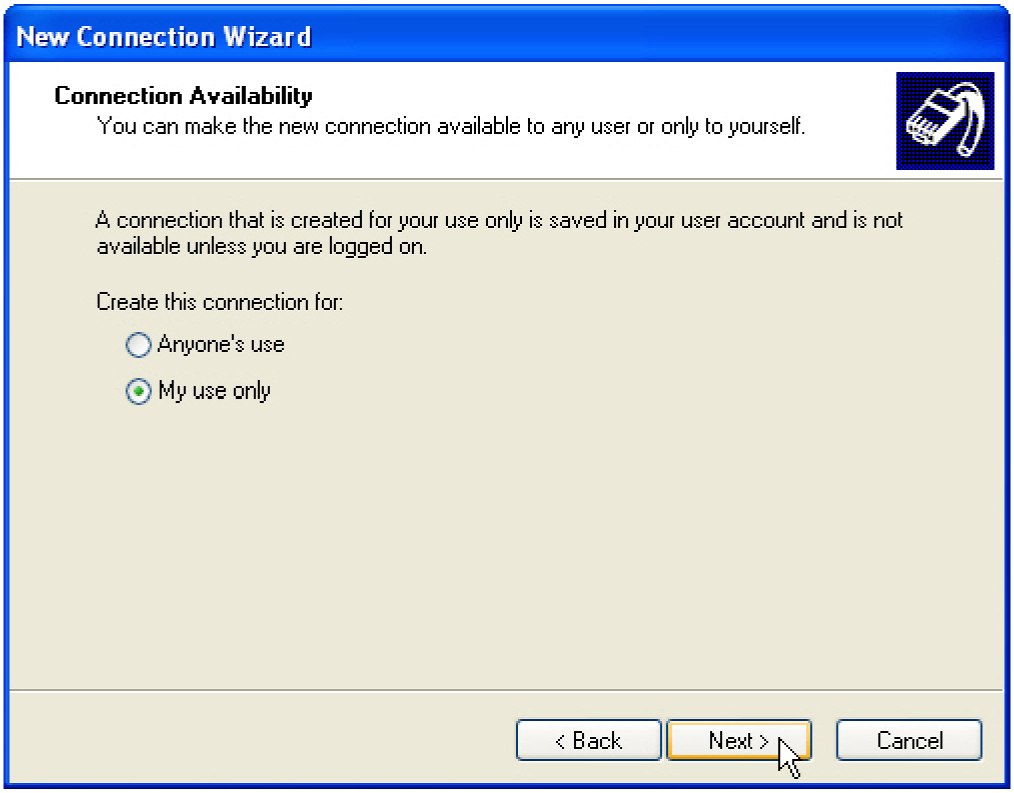
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

42.0.0.1

Figure 4.9 – New Connection Wizard

h. Chose a Connection Availability and click next.



Connection Availability

You can make the new connection available to any user or only to yourself.

A connection that is created for your use only is saved in your user account and is not available unless you are logged on.

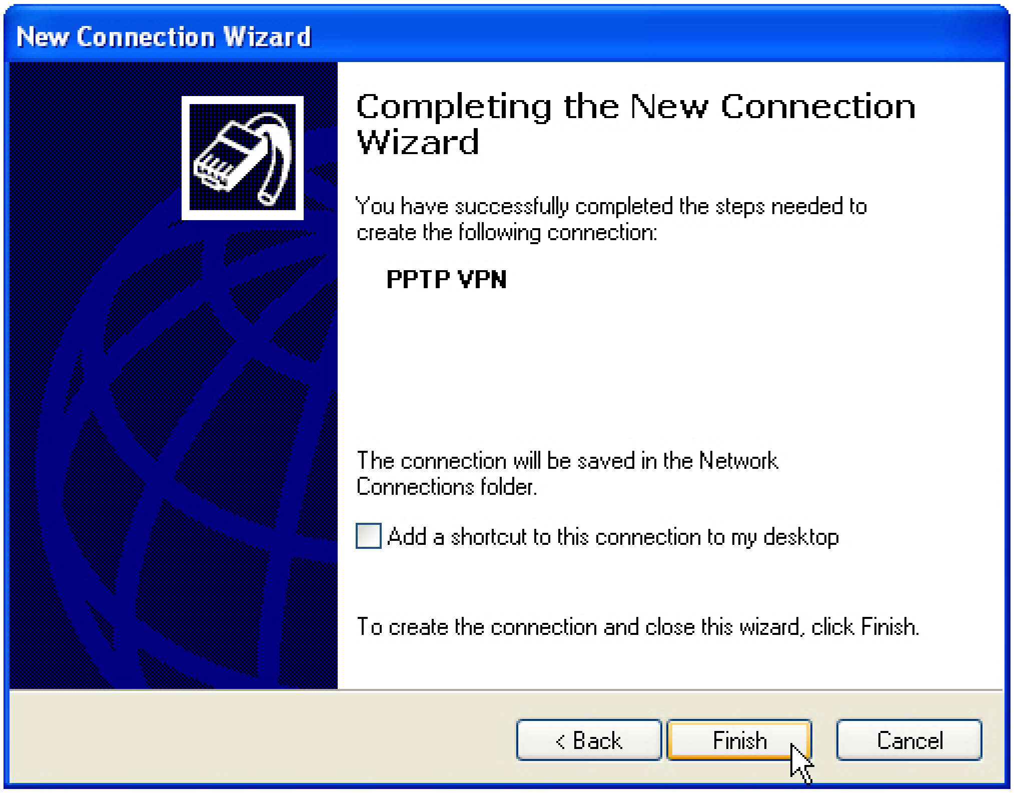
Create this connection for:

○ Anyone's use

● My use only

Figure 4.10 – New Connection Wizard

i. Click **Finish** to complete the New Connection Wizard.


New Connection Wizard

Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

PPTP VPN

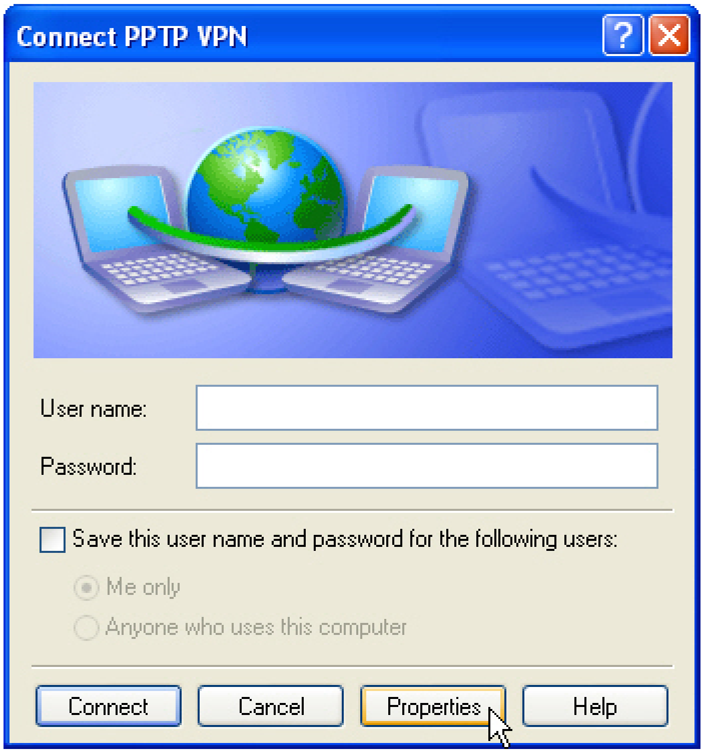
The connection will be saved in the Network Connections folder.

☐ Add a shortcut to this connection to my desktop

To create the connection and close this wizard, click Finish.

Figure 4.11 – New Connection Wizard

j. At the VPN connection window, click the **Properties** button.


Connect PPTP VPN

User name:

Password:

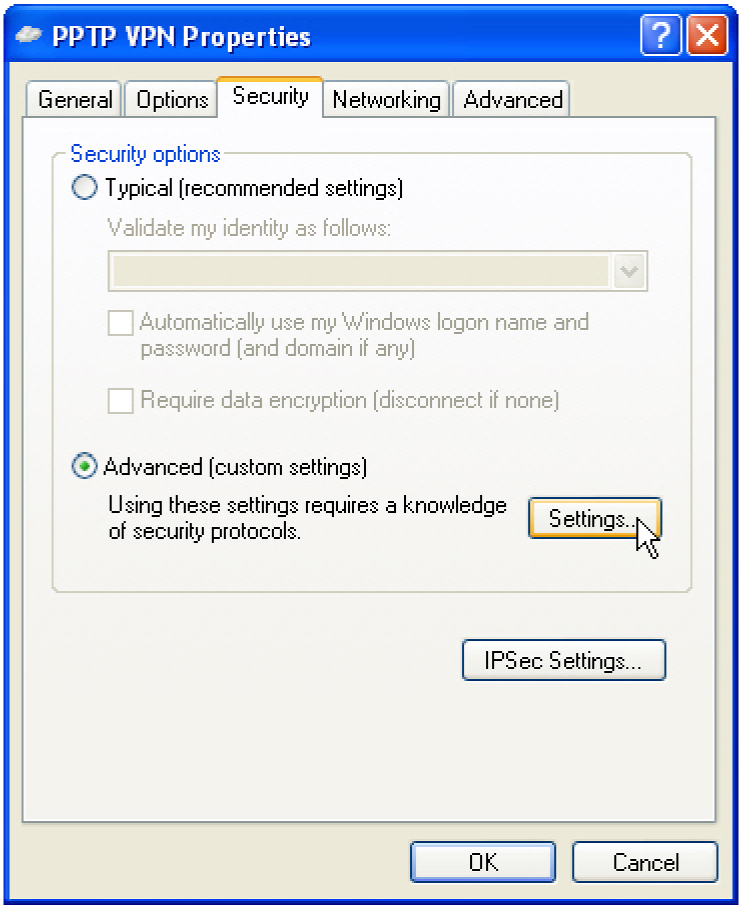
☐ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

Figure 4.12 – VPN Connection Dialog Box

k. On the **Security** tab, select the **Advanced** (custom settings) security option radio button and click the **Settings** button.



PPTP VPN Properties

Security options

○ Typical (recommended settings)

Validate my identity as follows:

□ Automatically use my Windows logon name and password (and domain if any)

□ Require data encryption (disconnect if none)

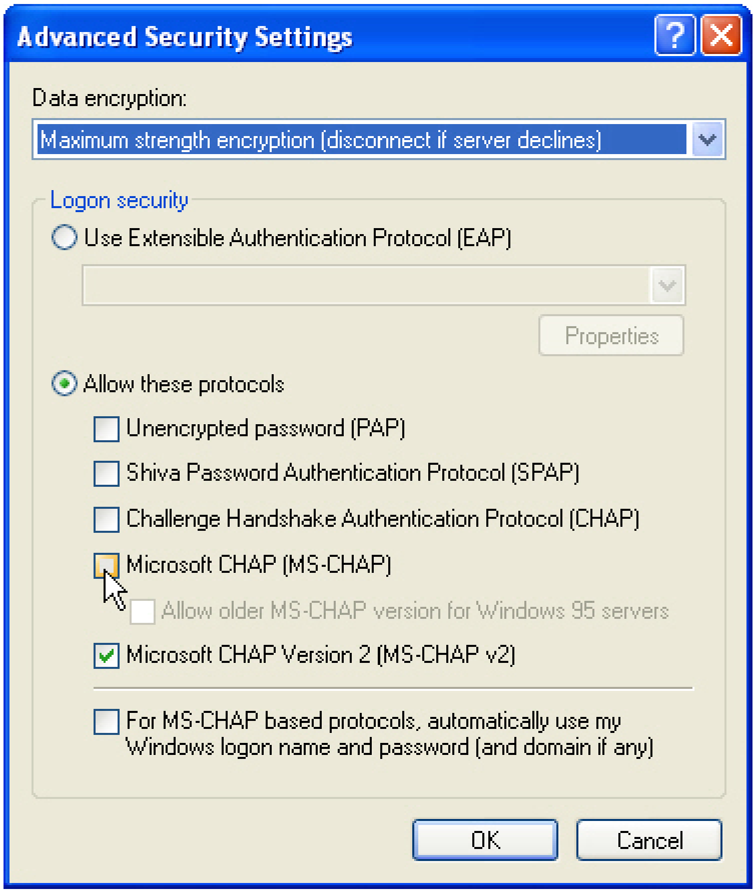
● Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

Figure 4.13 – VPN Properties

l. In the Advanced Security Settings window, configure the following and click OK.

- Data encryption: **Maximum strength encryption** (disconnect if server declines)
- Allow these protocols: configure to use **MS-CHAP v2 only**; deselect MS-CHAP if selected.



Advanced Security Settings

Data encryption:

Maximum strength encryption (disconnect if server declines)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

□ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP (MS-CHAP)

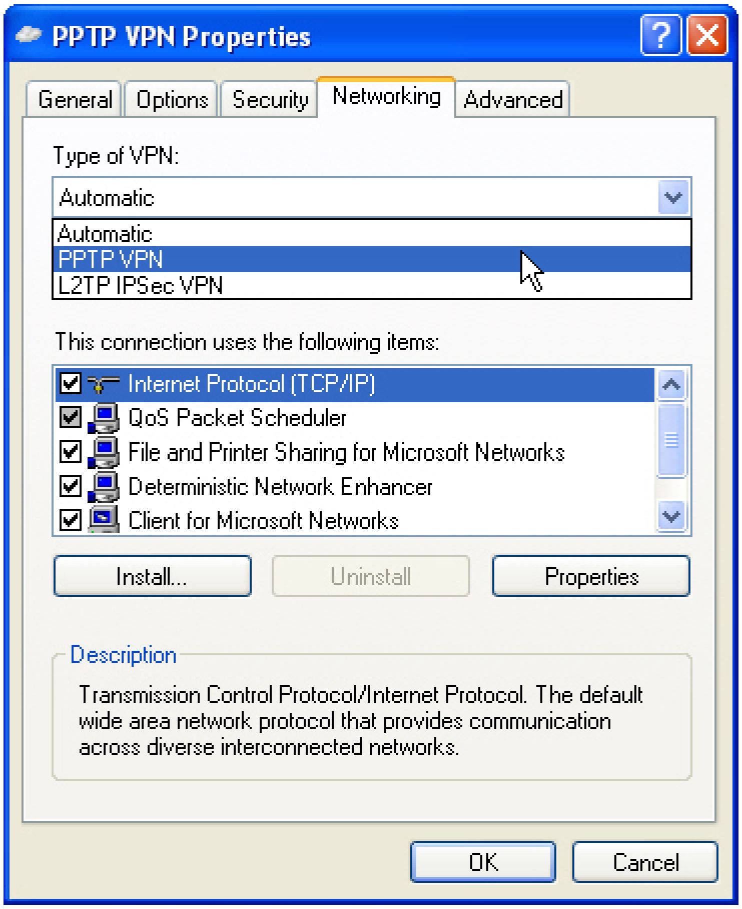
□ Allow older MS-CHAP version for Windows 95 servers

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

Figure 4.14 – VPN Advanced Settings

m. On the Networking tab, select **PPTP VPN** in the drop-down menu as the Type of VPN. Click OK to exit connection properties.



Type of VPN:

Automatic

- Automatic
- PPTP VPN
- L2TP IPSec VPN

This connection uses the following items:

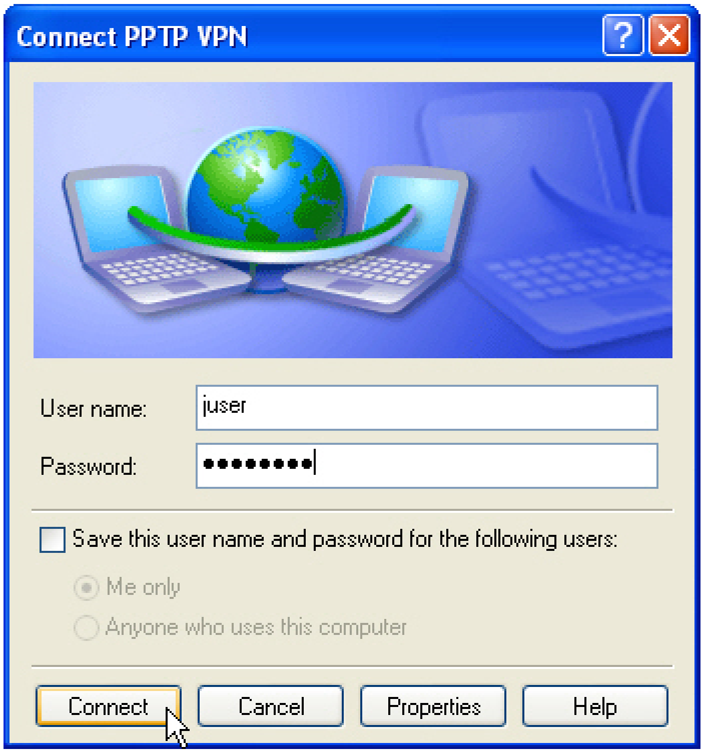
☑ Internet Protocol (TCP/IP)
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Deterministic Network Enhancer
☑ Client for Microsoft Networks

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 4.15 – VPN Properties

n. Enter the **username** (`juser`) and **password** (`password`) at the connection dialog box and click **Connect** to establish the PPTP VPN.



User name: juser

Password: •••••••••

□ Save this user name and password for the following users:

● Me only
○ Anyone who uses this computer

Figure 4.16 – VPN Connection Dialog Box

o. Validate PPTP VPN connection in the Network Connections window.

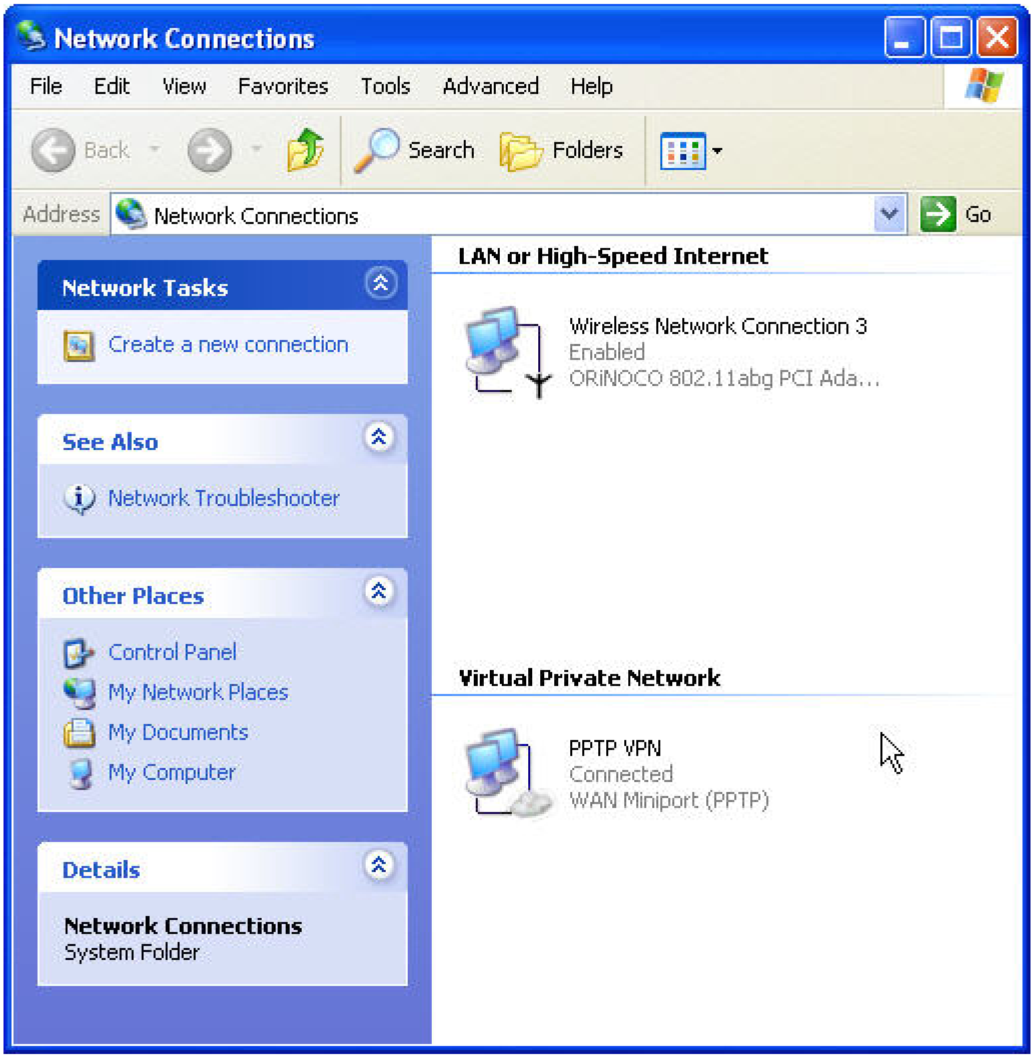
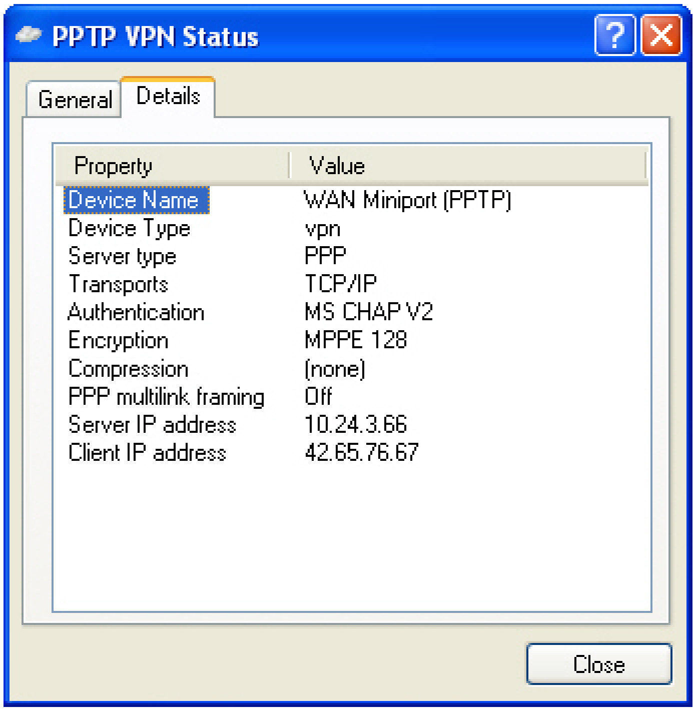


Figure 4.17 – Network Connections

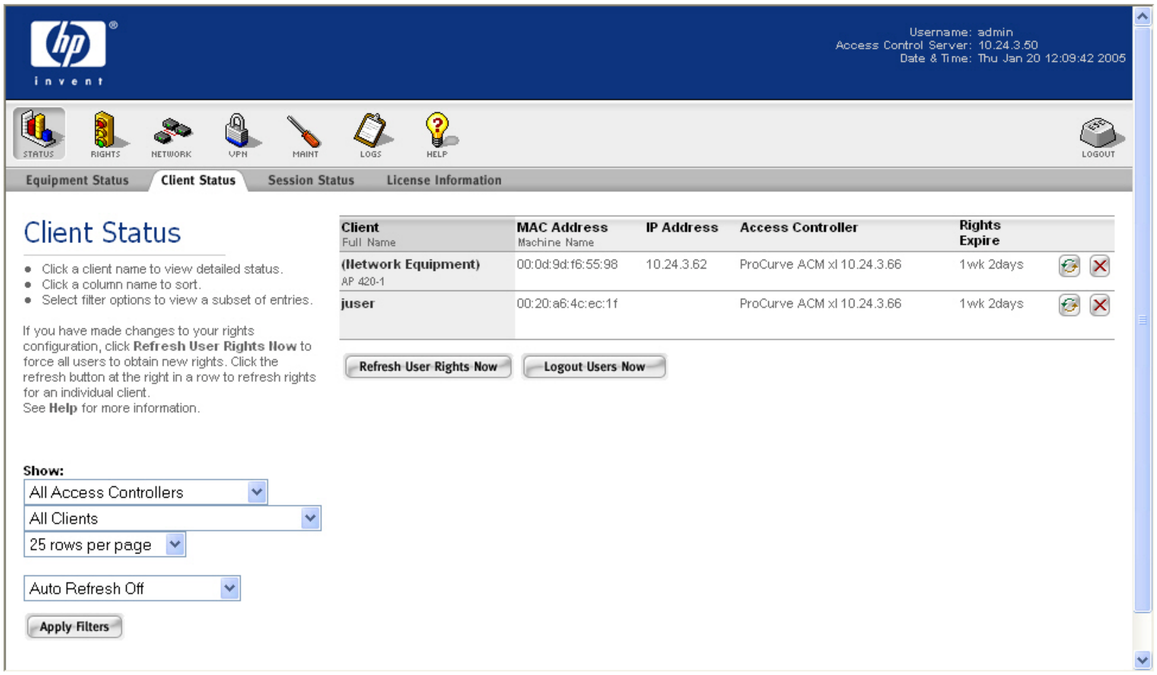
p. Double-click the Virtual Private Network Connection and select the Details tab to connection status details.



Property	Value
Device Name	WAN Miniport (PPTP)
Device Type	vpn
Server type	PPP
Transports	TCP/IP
Authentication	MS CHAP V2
Encryption	MPPE 128
Compression	(none)
PPP multilink framing	Off
Server IP address	10.24.3.66
Client IP address	42.65.76.67

Figure 4.18 – VPN Status Details

q. Back on the ACS, browse to Status -> Client Status and click the **Refresh User Rights Now** button to validate the client in now logged in (authenticated).



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Jan 20 12:09:42 2005

Client Status

- Click a client name to view detailed status.
- Click a column name to sort.
- Select filter options to view a subset of entries.

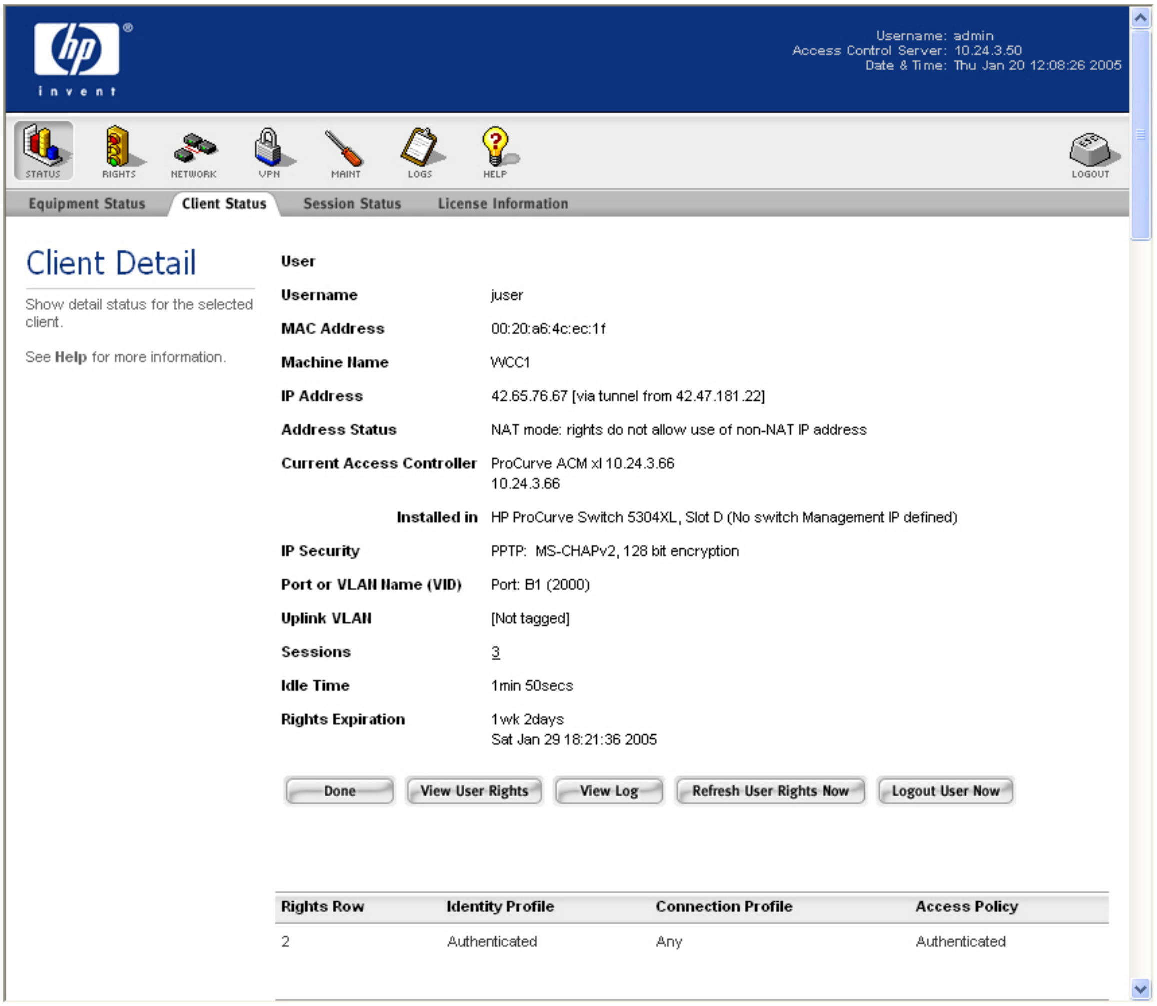
If you have made changes to your rights configuration, click **Refresh User Rights Now** to force all users to obtain new rights. Click the refresh button at the right in a row to refresh rights for an individual client.
See **Help** for more information.

Client Full Name	MAC Address Machine Name	IP Address	Access Controller	Rights Expire
(Network Equipment) AP 420-1	00:0d:9d:f6:55:98	10.24.3.62	ProCurve ACM xl 10.24.3.66	1wk 2days
juser	00:20:a6:4c:ec:1f		ProCurve ACM xl 10.24.3.66	1wk 2days

Show:
All Access Controllers
All Clients
25 rows per page
Auto Refresh Off

Figure 4.19 – Client Status Page

r. Click on the client (juser) to get **Client details**. Click the **View User Rights** button to validate that the user is authenticated correctly.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Jan 20 12:08:26 2005

Client Detail

Show detail status for the selected client.

See **Help** for more information.

User	
Username	juser
MAC Address	00:20:a6:4c:ec:1f
Machine Name	WCC1
IP Address	42.65.76.67 [via tunnel from 42.47.181.22]
Address Status	NAT mode: rights do not allow use of non-NAT IP address
Current Access Controller	ProCurve ACM xl 10.24.3.66 10.24.3.66
Installed in	HP ProCurve Switch 5304XL, Slot D (No switch Management IP defined)
IP Security	PPTP: MS-CHAPv2, 128 bit encryption
Port or VLAN Name (VID)	Port: B1 (2000)
Uplink VLAN	[Not tagged]
Sessions	3
Idle Time	1min 50secs
Rights Expiration	1wk 2days Sat Jan 29 18:21:36 2005

Rights Row	Identity Profile	Connection Profile	Access Policy
2	Authenticated	Any	Authenticated

Figure 4.20 – Client Details

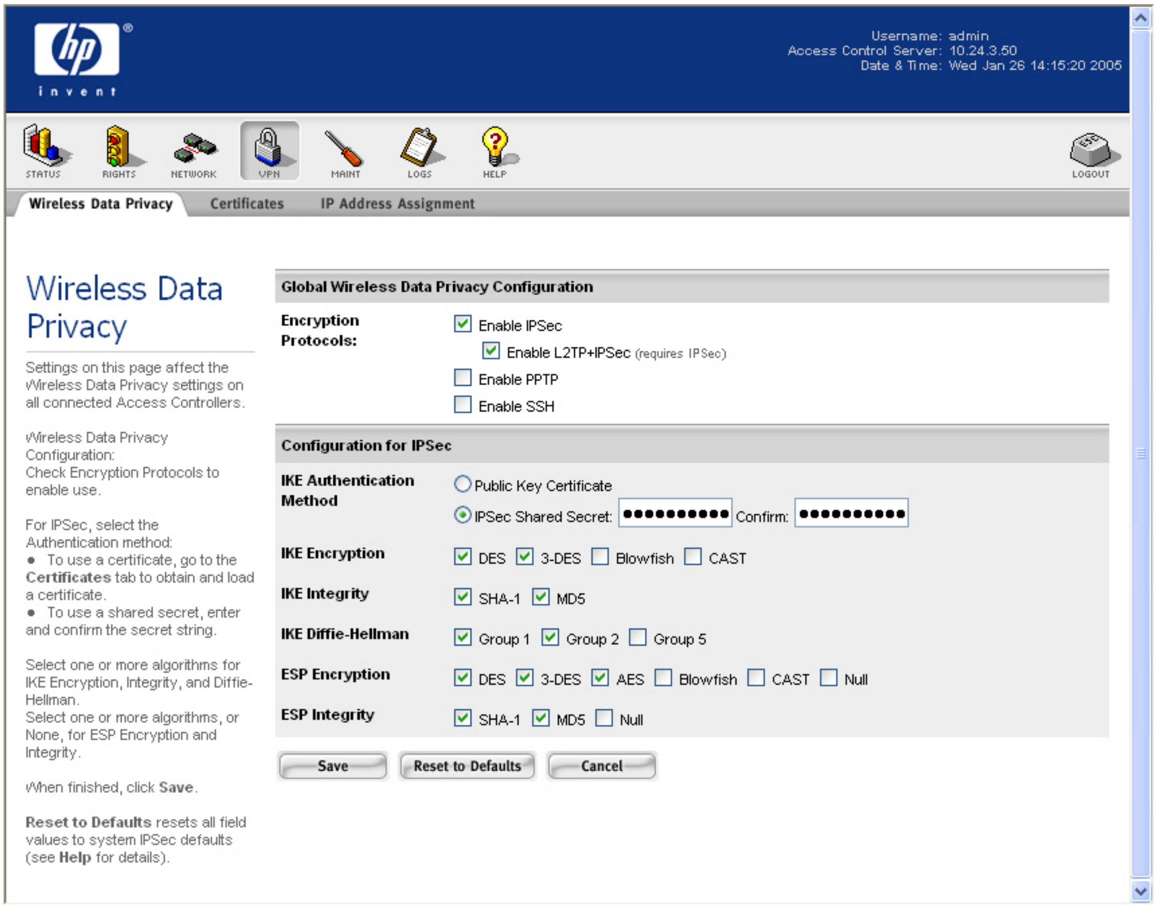
Configuring Scenario 5: Wireless Data Privacy Logon using VPN Authentication (L2TP/IPSec)

Scenario 5 consists of a wireless, Windows XP client authenticating via a VPN. The VPN used in this example will be an L2TP/IPSec VPN. Since VPN authentication requires a RADIUS backend, we will configure an ACS to authenticate VPN users against Internet Authentication Service (IAS), Microsoft's RADIUS implementation. The steps required are:

- On the ACS, enable L2TP and IPSec VPN support globally.
- On the ACS, configure Unauthenticated and Authenticated Access Policies for:
  - ➢ L2TP/IPSec VPN support
  - ➢ Real IP addresses inside the encrypted VPN tunnel
- On the ACS, define a RADIUS Authentication Service and associate it to the System Authentication Policy.
- From the ACS, configure the ProCurve Access Control xl Module with the DHCP Server IP Address to allow clients to use Real IP addresses for the inner VPN tunnel.
- On the AP 420, configure open authentication wireless parameters.
- On the wireless Windows XP client, configure the ProCurve VPN and Windows XP VPN client software for L2TP/IPSec.
- Connect and verify authentication.

1) **On the ACS, enable L2TP and IPSec support globally**.

   a. On the ACS, browse to VPN -> Wireless Data Privacy tab and click the **Enable IPSec and Enable L2TP+IPSec** checkboxes. Select the radio button to enable **IPSec Shared Secret** for IKE Authentication Method and configure an IPSec shared secret. Leave all other configuration settings default and save changes.



Wireless Data Privacy

Settings on this page affect the Wireless Data Privacy settings on all connected Access Controllers.

Wireless Data Privacy Configuration:
Check Encryption Protocols to enable use.

For IPSec, select the Authentication method:
- To use a certificate, go to the **Certificates** tab to obtain and load a certificate.
- To use a shared secret, enter and confirm the secret string.

Select one or more algorithms for IKE Encryption, Integrity, and Diffie-Hellman.
Select one or more algorithms, or None, for ESP Encryption and Integrity.

When finished, click **Save**.

Reset to Defaults resets all field values to system IPSec defaults (see **Help** for details).

Global Wireless Data Privacy Configuration

Encryption Protocols: ☑ Enable IPSec
☑ Enable L2TP+IPSec (requires IPSec)
☐ Enable PPTP
☐ Enable SSH

Configuration for IPSec

IKE Authentication Method ○ Public Key Certificate
● IPSec Shared Secret: ●●●●●●●●●●● Confirm: ●●●●●●●●●●●

IKE Encryption ☑ DES ☑ 3-DES ☐ Blowfish ☐ CAST

IKE Integrity ☑ SHA-1 ☑ MD5

IKE Diffie-Hellman ☑ Group 1 ☑ Group 2 ☐ Group 5

ESP Encryption ☑ DES ☑ 3-DES ☑ AES ☐ Blowfish ☐ CAST ☐ Null

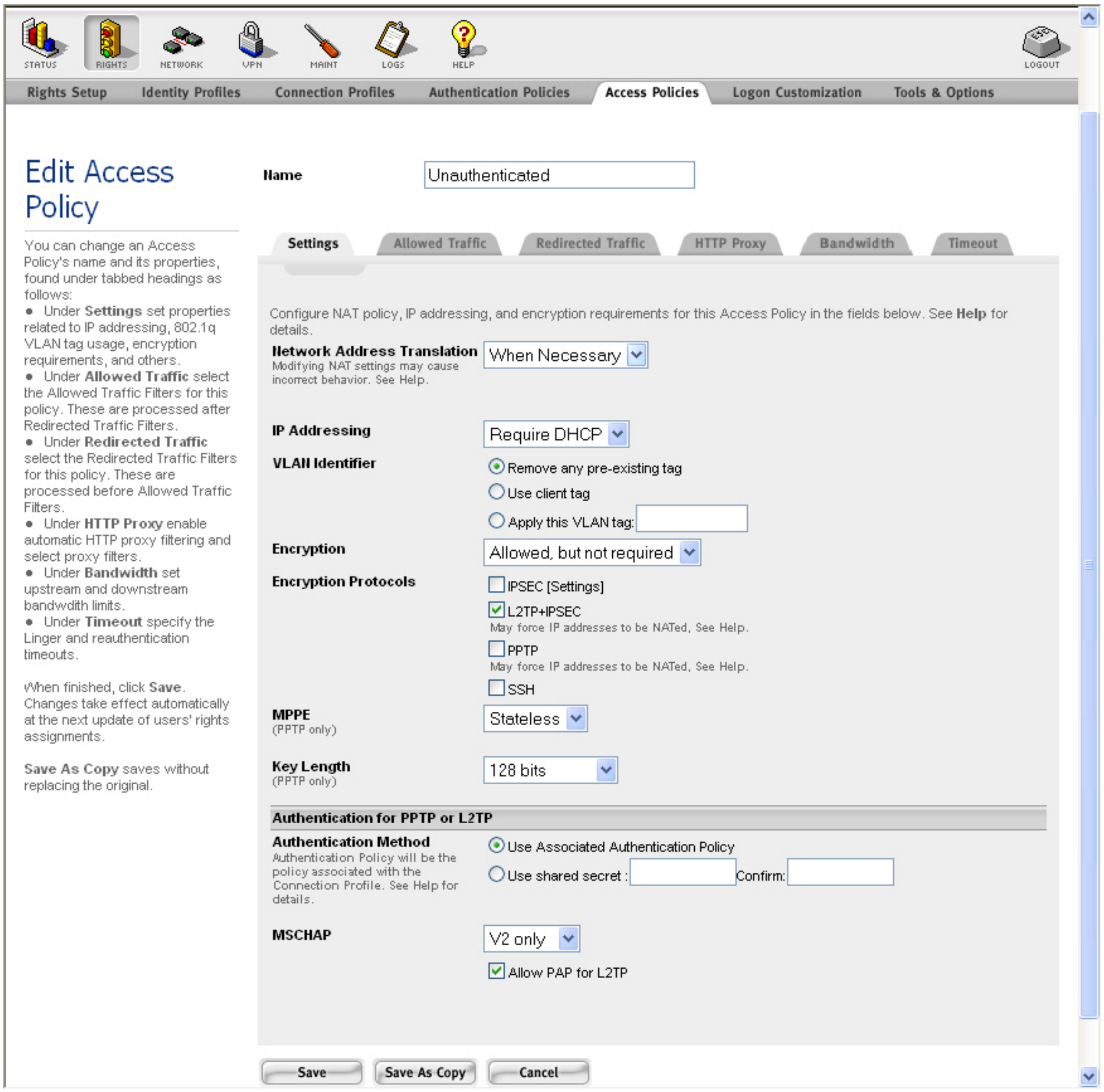
ESP Integrity ☑ SHA-1 ☑ MD5 ☐ Null

Figure 5.1 – Wireless Data Privacy

2) **On the ACS, enable L2TP/IPSec VPN support in both the Unauthenticated and Authenticated Access Policies**.

a. On the ACS, browse to Rights -> Access Policies and select the Unauthenticated Access Policy. Configure the following and Save changes.

- Network Address Translation: **When Necessary** (this allows Real IP addressing for inner tunnel).
- IP addressing: **Require DHCP**
- Encryption: **Allowed, but not required**
- Encryption Protocols: **L2TP+IPSec**
- Keep the **default** on all other settings



Edit Access Policy

You can change an Access Policy's name and its properties, found under tabbed headings as follows:

- Under **Settings** set properties related to IP addressing, 802.1q VLAN tag usage, encryption requirements, and others.
- Under **Allowed Traffic** select the Allowed Traffic Filters for this policy. These are processed after Redirected Traffic Filters.
- Under **Redirected Traffic** select the Redirected Traffic Filters for this policy. These are processed before Allowed Traffic Filters.
- Under **HTTP Proxy** enable automatic HTTP proxy filtering and select proxy filters.
- Under **Bandwidth** set upstream and downstream bandwidth limits.
- Under **Timeout** specify the Linger and reauthentication timeouts.

When finished, click **Save**. Changes take effect automatically at the next update of users' rights assignments.

Save As Copy saves without replacing the original.

Name Unauthenticated

Configure NAT policy, IP addressing, and encryption requirements for this Access Policy in the fields below. See **Help** for details.

Network Address Translation When Necessary
Modifying NAT settings may cause incorrect behavior. See Help.

IP Addressing Require DHCP

VLAN Identifier
● Remove any pre-existing tag
○ Use client tag
○ Apply this VLAN tag:

Encryption Allowed, but not required

Encryption Protocols
□ IPSEC [Settings]
☑ L2TP+IPSEC
May force IP addresses to be NATed, See Help.
□ PPTP
May force IP addresses to be NATed, See Help.
□ SSH

MPPE (PPTP only) Stateless

Key Length (PPTP only) 128 bits

Authentication for PPTP or L2TP

Authentication Method
Authentication Policy will be the policy associated with the Connection Profile. See Help for details.
● Use Associated Authentication Policy
○ Use shared secret : Confirm:

MSCHAP V2 only
☑ Allow PAP for L2TP

Figure 5.2 – Unauthenticated Access Policy

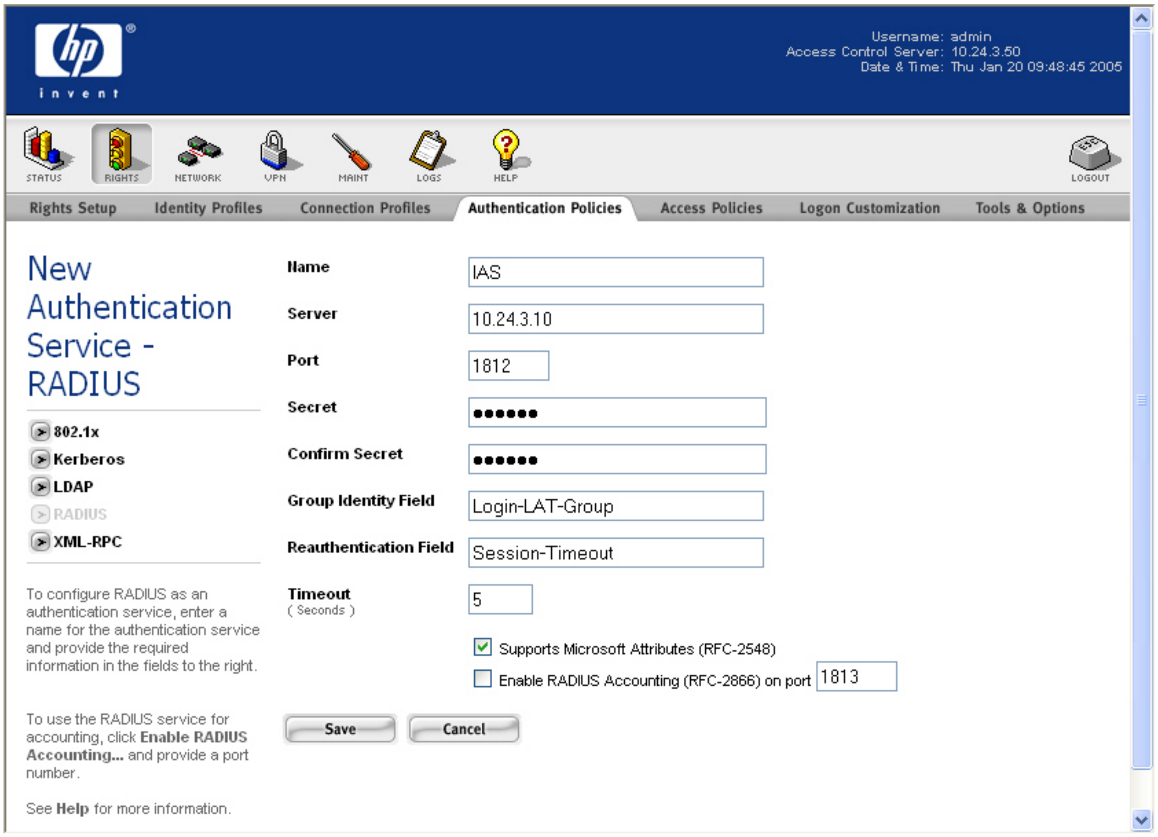
b. On the ACS, browse to Rights -> Access Policies and select the **Authenticated** Access Policy. Configure the Authenticated Access Policy **EXACTLY** the same as the **Unauthenticated** Access Policy and save changes.

c. On the ACS, browse to Status -> Client Status and click **Refresh User Rights Now**.

3) **On the ACS, define a RADIUS Authentication Service and associate it to the System Authentication Policy.**

Note: This assumes that the RADIUS server is configured and ready to authenticate clients. See Scenario 3 for more details.

a. On the ACS, browse to Rights -> Authentication Policies and click the **New Service** button. Chose the RADIUS button on the right window pane and configure the new RADIUS service with the following information and save changes.
  - Name: **IAS**
  - Server: **10.24.3.10**
  - Secret: **secret**
  - Group Identity Field: **Login-LAT-Group**
  - **Supports Microsoft Attributes (RFC-2548)**



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Jan 20 09:48:45 2005

New Authentication Service - RADIUS

Name	IAS
Server	10.24.3.10
Port	1812
Secret	••••••
Confirm Secret	••••••
Group Identity Field	Login-LAT-Group
Reauthentication Field	Session-Timeout
Timeout (Seconds)	5

☑ Supports Microsoft Attributes (RFC-2548)

☐ Enable RADIUS Accounting (RFC-2866) on port 1813

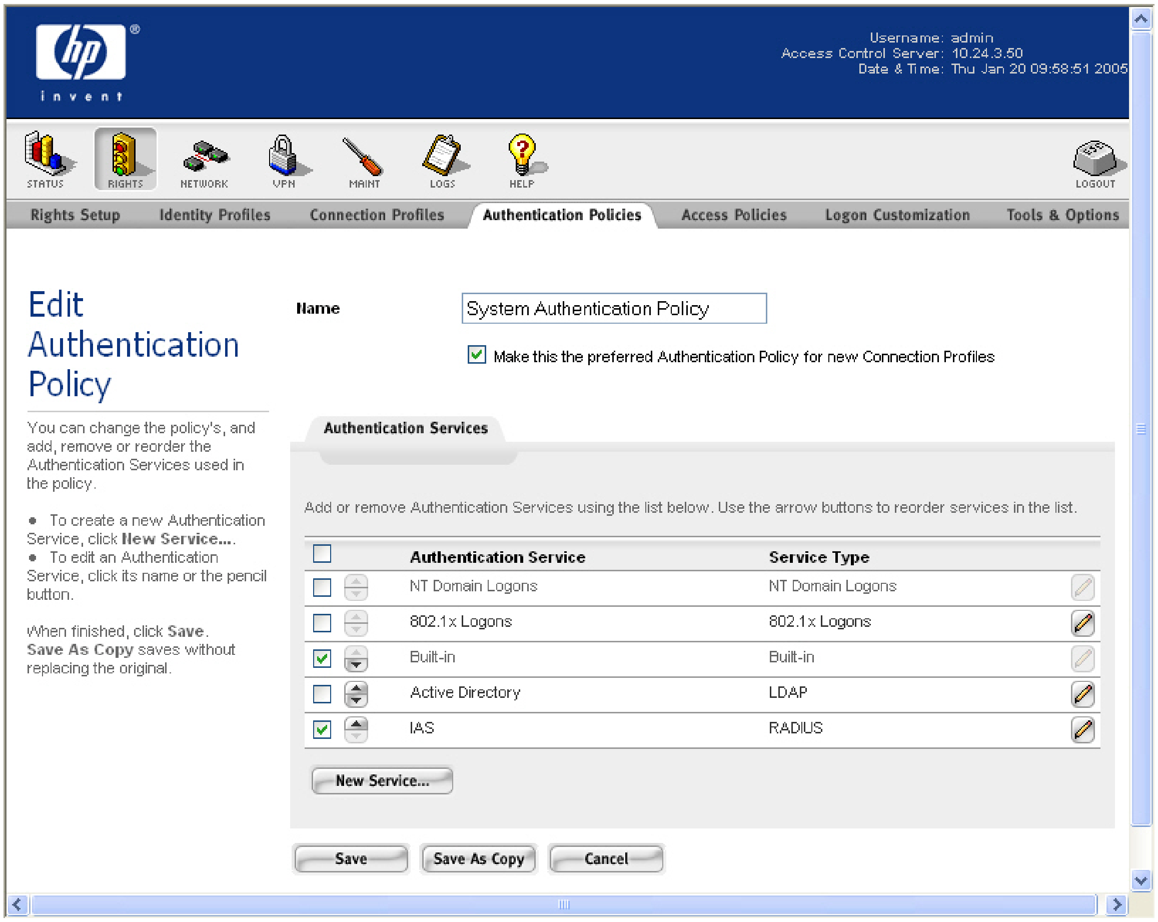
To configure RADIUS as an authentication service, enter a name for the authentication service and provide the required information in the fields to the right.

To use the RADIUS service for accounting, click **Enable RADIUS Accounting...** and provide a port number.

See **Help** for more information.

Figure 5.3 – RADIUS Authentication Service

b. Browse to Rights -> Authentication Policies and click the System Authentication Policy. Add the newly created **RADIUS Authentication Service** (IAS) to the **System Authentication Policy** and save changes.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Jan 20 09:58:51 2005

Edit Authentication Policy

You can change the policy's, and add, remove or reorder the Authentication Services used in the policy.

- To create a new Authentication Service, click **New Service...**.
- To edit an Authentication Service, click its name or the pencil button.

When finished, click **Save**. **Save As Copy** saves without replacing the original.

Name: System Authentication Policy

☑ Make this the preferred Authentication Policy for new Connection Profiles

Authentication Services

Add or remove Authentication Services using the list below. Use the arrow buttons to reorder services in the list.

☐	Authentication Service	Service Type
☐	NT Domain Logons	NT Domain Logons
☐	802.1x Logons	802.1x Logons
☑	Built-in	Built-in
☐	Active Directory	LDAP
☑	IAS	RADIUS

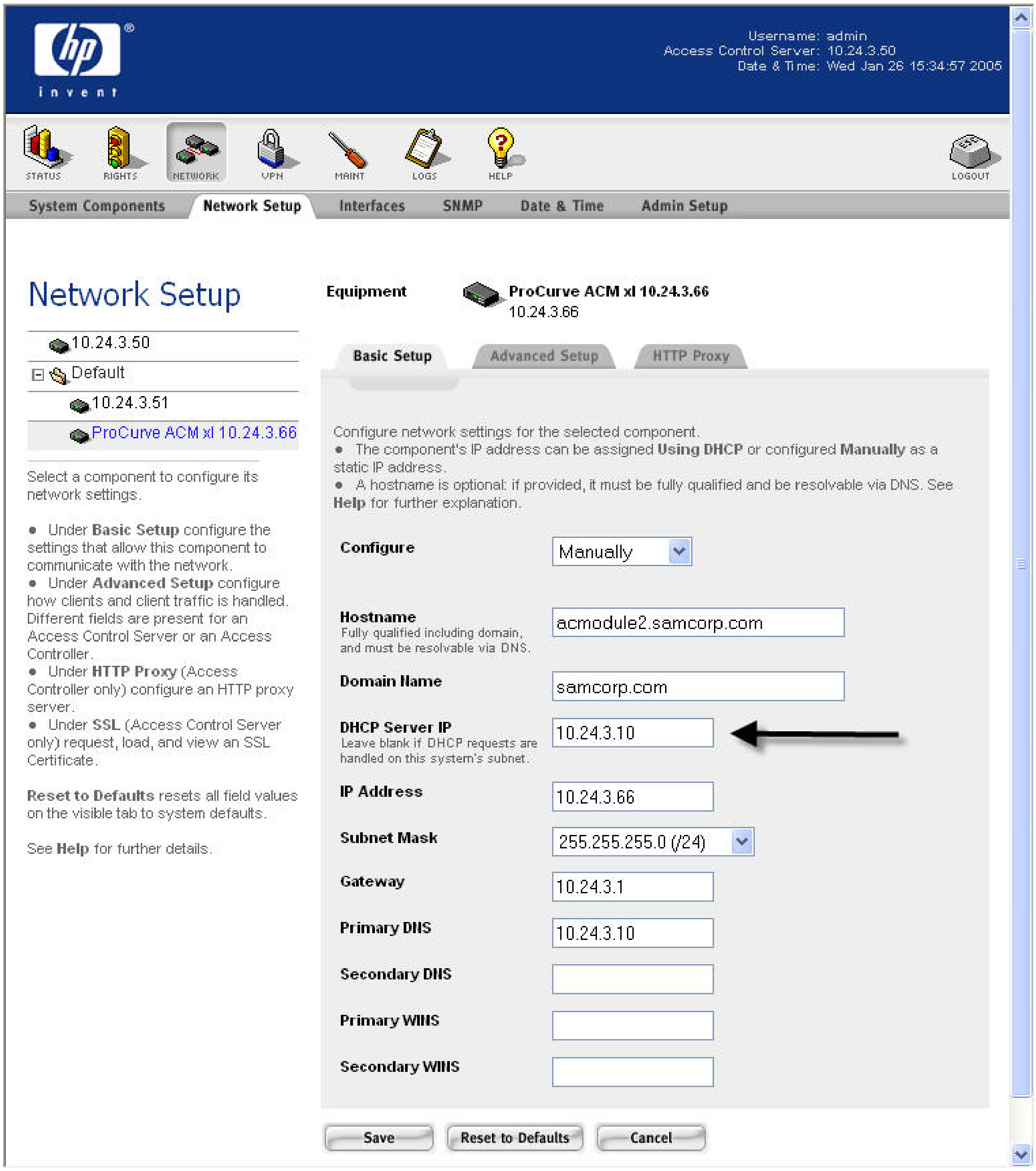
Figure 5.4 – System Authentication Policy

c. On the ACS, browse to Status -> Client Status and click **Refresh User Rights Now**.

4) **From the ACS, configure the ProCurve Access Control xl Module with the DHCP Server IP Address to allow clients to use Real IP addresses for the inner VPN tunnel.**

Note: This assumes that the DHCP server is configured and ready to provide IP addresses to clients.

a. On the ACS, browse to Network -> Network Setup and select the ACM used for authenticating client. Configure the DHCP Server IP address and save changes.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Wed Jan 26 15:34:57 2005

Network Setup

10.24.3.50
Default
10.24.3.51
ProCurve ACM xl 10.24.3.66

Select a component to configure its network settings.

- Under **Basic Setup** configure the settings that allow this component to communicate with the network.
- Under **Advanced Setup** configure how clients and client traffic is handled. Different fields are present for an Access Control Server or an Access Controller.
- Under **HTTP Proxy** (Access Controller only) configure an HTTP proxy server.
- Under **SSL** (Access Control Server only) request, load, and view an SSL Certificate.

Reset to Defaults resets all field values on the visible tab to system defaults.

See **Help** for further details.

Equipment ProCurve ACM xl 10.24.3.66
10.24.3.66

Configure network settings for the selected component.

- The component's IP address can be assigned **Using DHCP** or configured **Manually** as a static IP address.
- A hostname is optional: if provided, it must be fully qualified and be resolvable via DNS. See **Help** for further explanation.

Configure Manually

Hostname Fully qualified including domain, and must be resolvable via DNS. acmodule2.samcorp.com

Domain Name samcorp.com

DHCP Server IP Leave blank if DHCP requests are handled on this system's subnet. 10.24.3.10

IP Address 10.24.3.66

Subnet Mask 255.255.255.0 (/24)

Gateway 10.24.3.1

Primary DNS 10.24.3.10

Secondary DNS

Primary WINS

Secondary WINS

Figure 5.5 – Network Setup

b. On the ACS, browse to Status -> Client Status and click **Refresh User Rights Now**.

5) On the AP 420, configure open authentication wireless parameters.

a. From the **AP 420 CLI, configure security suite 1 (open authentication, no encryption).**

```
HP ProCurve Access Point 420# configure
HP ProCurve Access Point 420(config)# int wireless g
Enter Wireless configuration commands, one per line.
HP ProCurve Access Point 420(if-wireless g)# security-suite 1
```

6) **On the wireless Windows XP client, configure the ProCurve VPN and Windows XP VPN client software for L2TP/IPSec**.

Note: This assumes that the Access Point 420 is connected to the Access Control xl Module as "Network Equipment" and the client is associated.

Using L2TP/IPSec in this scenario is a three step process.

- First, the ProCurve VPN client is installed and configured.
- Second the Windows XP (native) VPN client software is configured.
- Third, connect the L2TP/IPSec VPN using the Windows (native) VPN client.

This process automatically establishes the IPSec tunnel using the ProCurve VPN Client and uses the Windows (native) VPN client to establish the L2TP tunnel.

Step 1: Configuring the ProCurve VPN Client

a. Install the ProCurve VPN client and reboot (required).

b. Right click on the ProCurve VPN tray icon and select the **Security Policy Editor**.

c. One the Edit menu, select **Add** -> **Connection** to create a new connection.

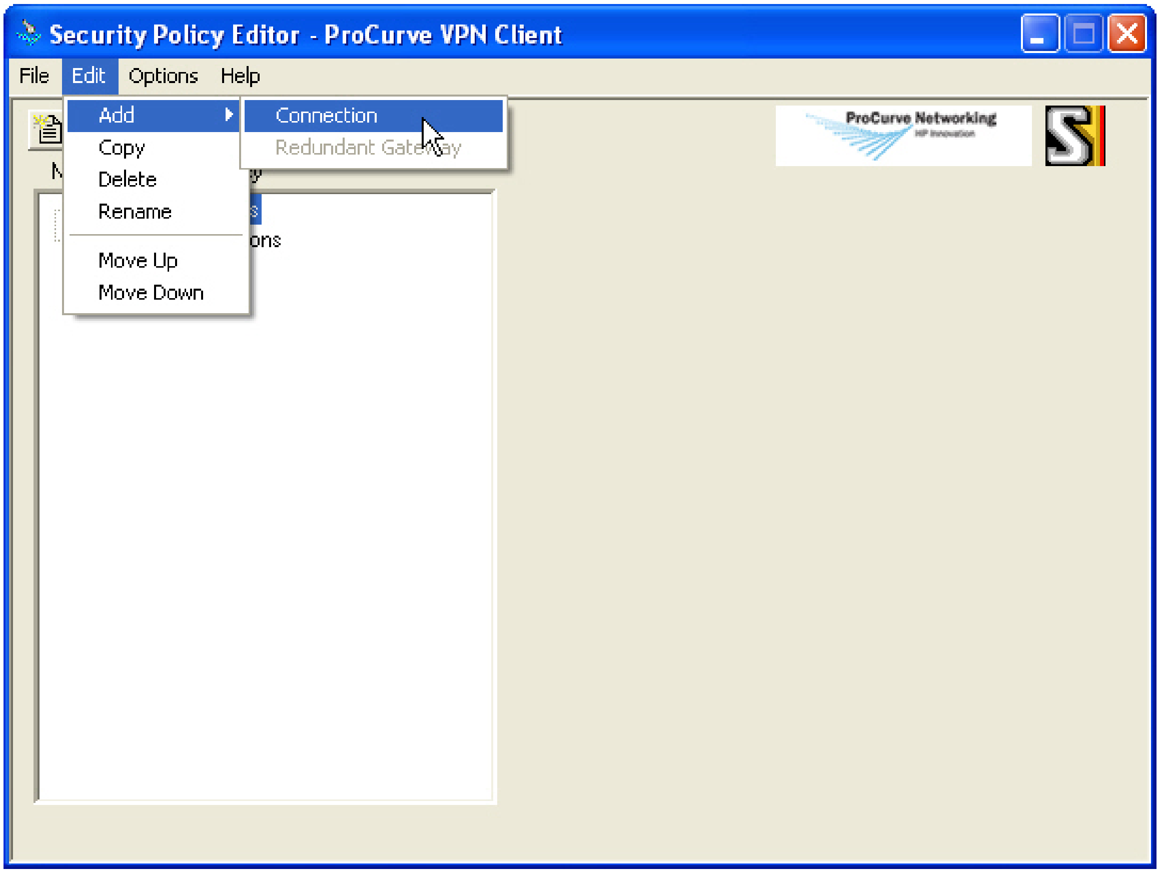
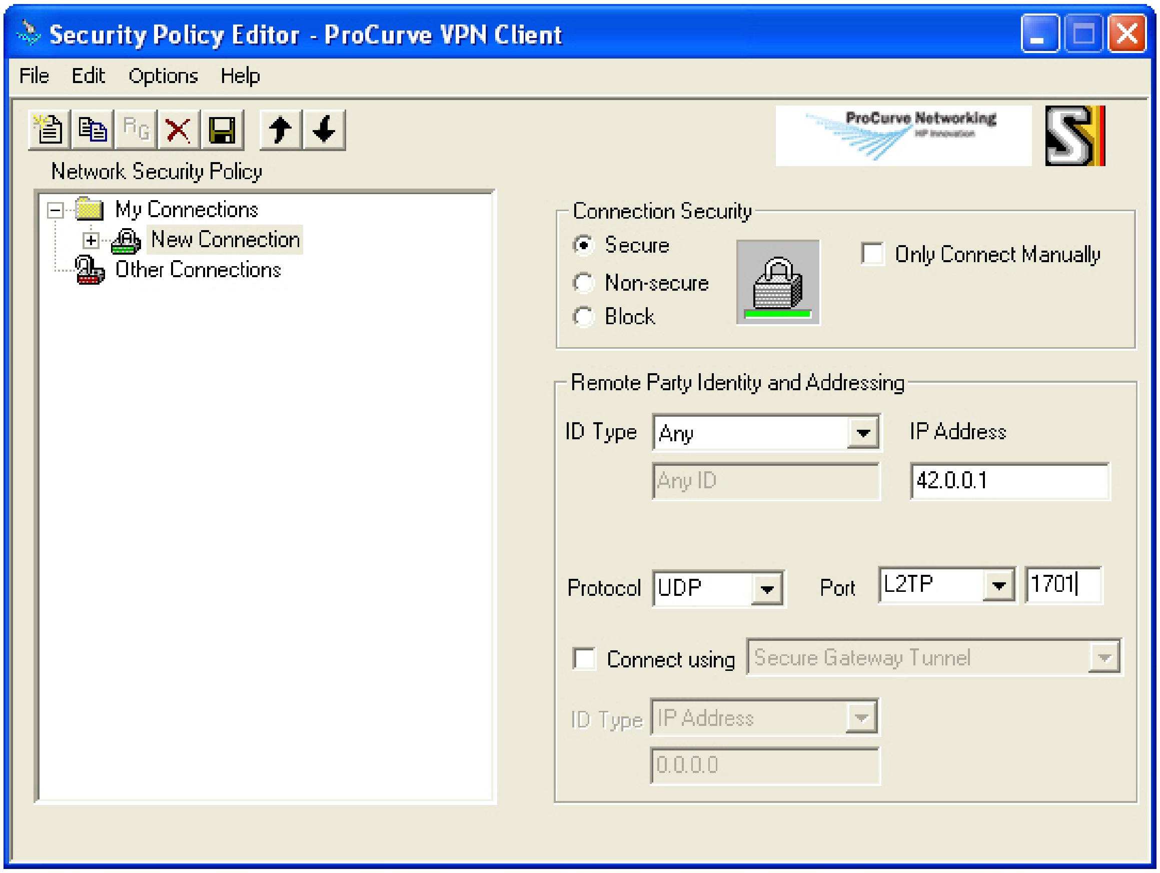


Figure 5.6 – Security Policy Editor

d. Click **New Connection** and configure the following:

- ➢ Remote Party Identity ID Type: **Any**
- ➢ IP Address: **42.0.0.1**
- ➢ Protocol: **UDP**
- ➢ Port: **L2TP (1701)**



Connection Security

● Secure

○ Non-secure

○ Block

□ Only Connect Manually

Remote Party Identity and Addressing

ID Type: Any

Any ID

IP Address: 42.0.0.1

Protocol: UDP

Port: L2TP 1701

□ Connect using Secure Gateway Tunnel

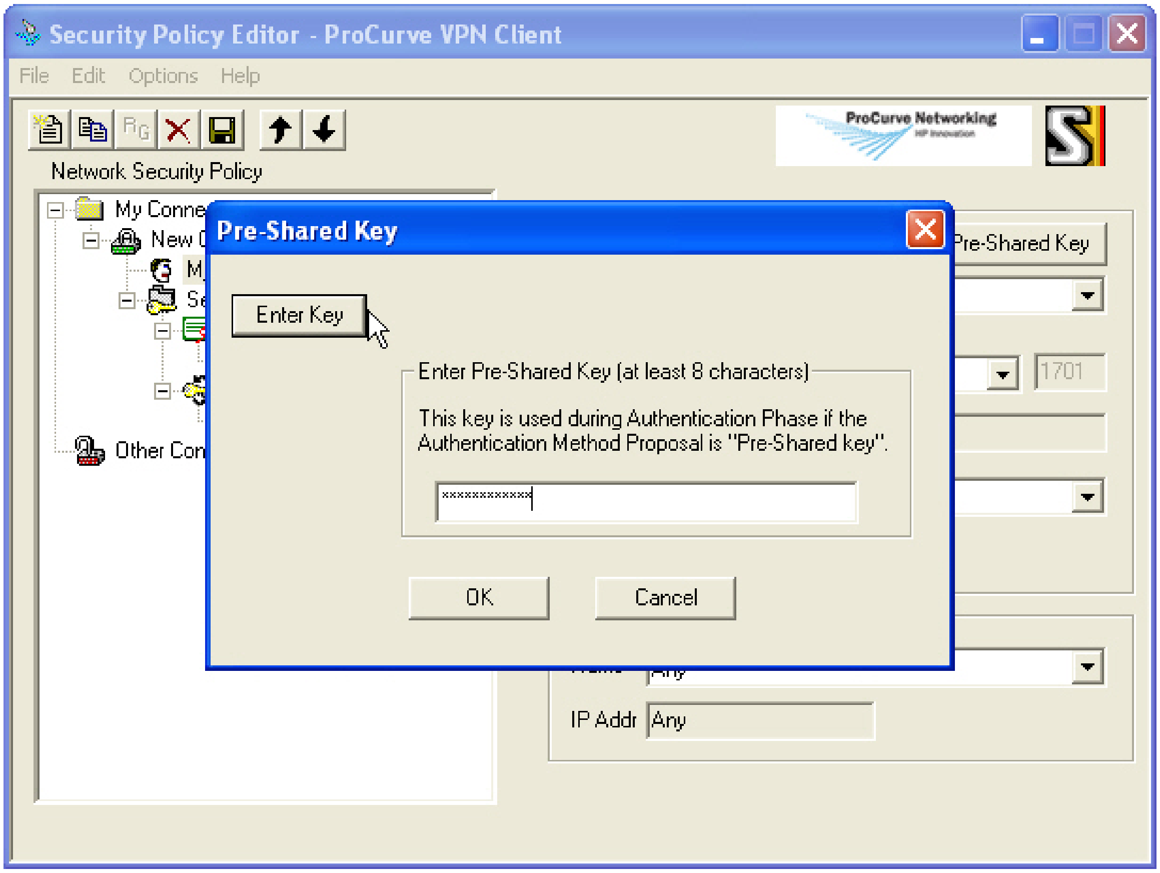
ID Type: IP Address

0.0.0.0

Figure 5.7 – Security Policy Editor

e. Expand the New Connection and click **My Identity**. In the Select Certificate drop-down window, select “**None**”. Configure the following:

- ➢ Click the Pre-shared Key button and configure the **IPSec pre-shared key** to match the key used on the ACS.
- ➢ ID type: **IP Address**
- ➢ Port: **L2TP**

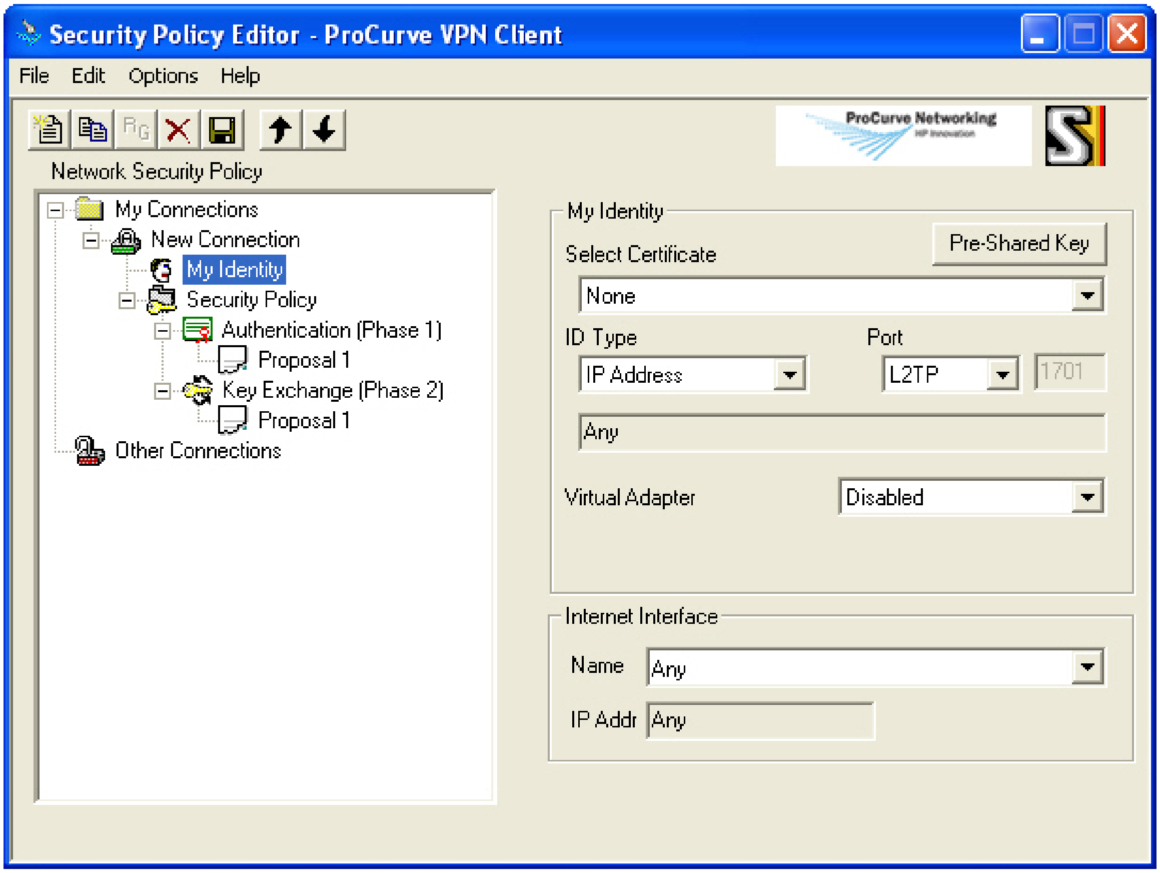


Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

****

Figure 5.8 – Pre-Shared Key



My Identity

Select Certificate: None

ID Type: IP Address

Port: L2TP 1701

Any

Virtual Adapter: Disabled

Internet Interface

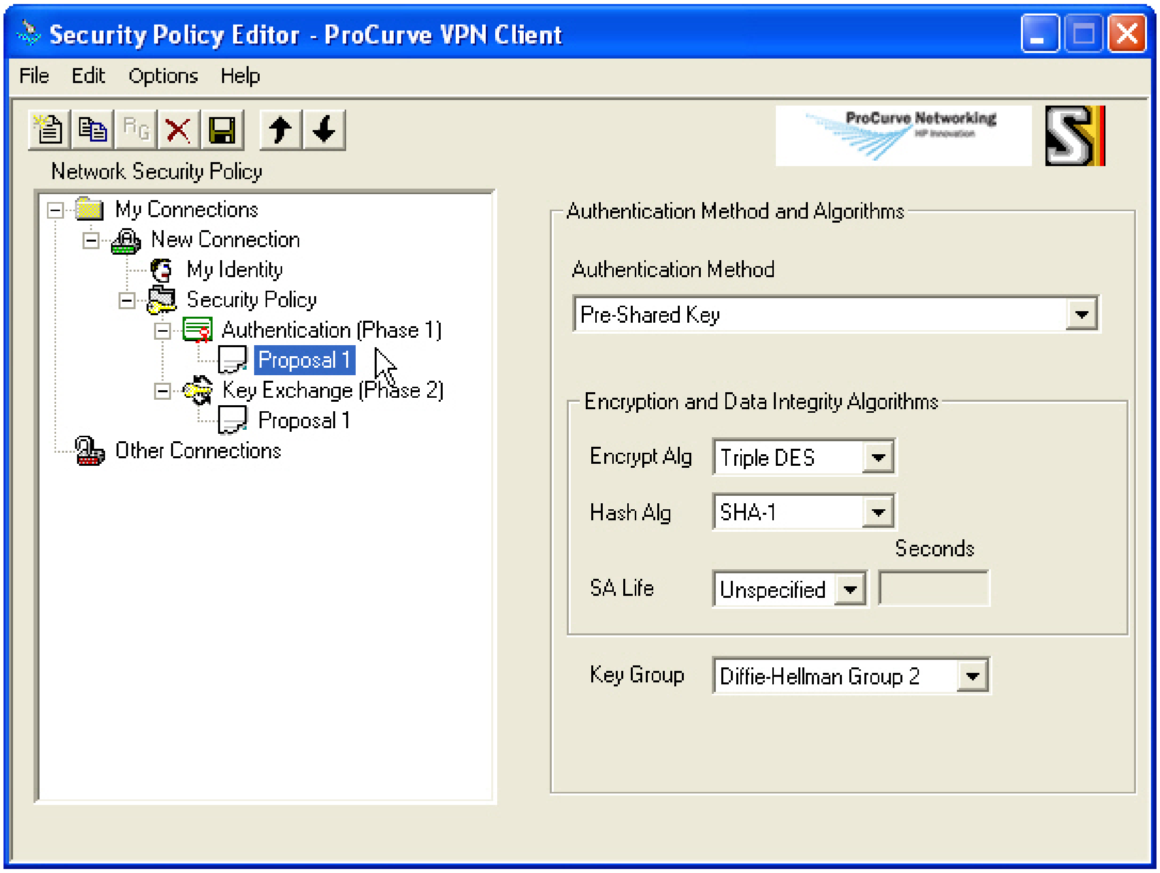
Name: Any

IP Addr: Any

Figure 5.9 – Security Policy Editor

f. Click Security Policy and expand to select **Authentication (Phase1)** and configure the following for **Proposal 1**:

- Authentication Method: **Pre-Shared Key**
- Encryp(tion) Alg(orithm): **Triple DES**
- Hash Alg(orithm): **SHA-1**
- SA Life: **Unspecified**
- Key Group: **Diffe-Hellman group 2**



Authentication Method: Pre-Shared Key

Encrypt Alg: Triple DES

Hash Alg: SHA-1

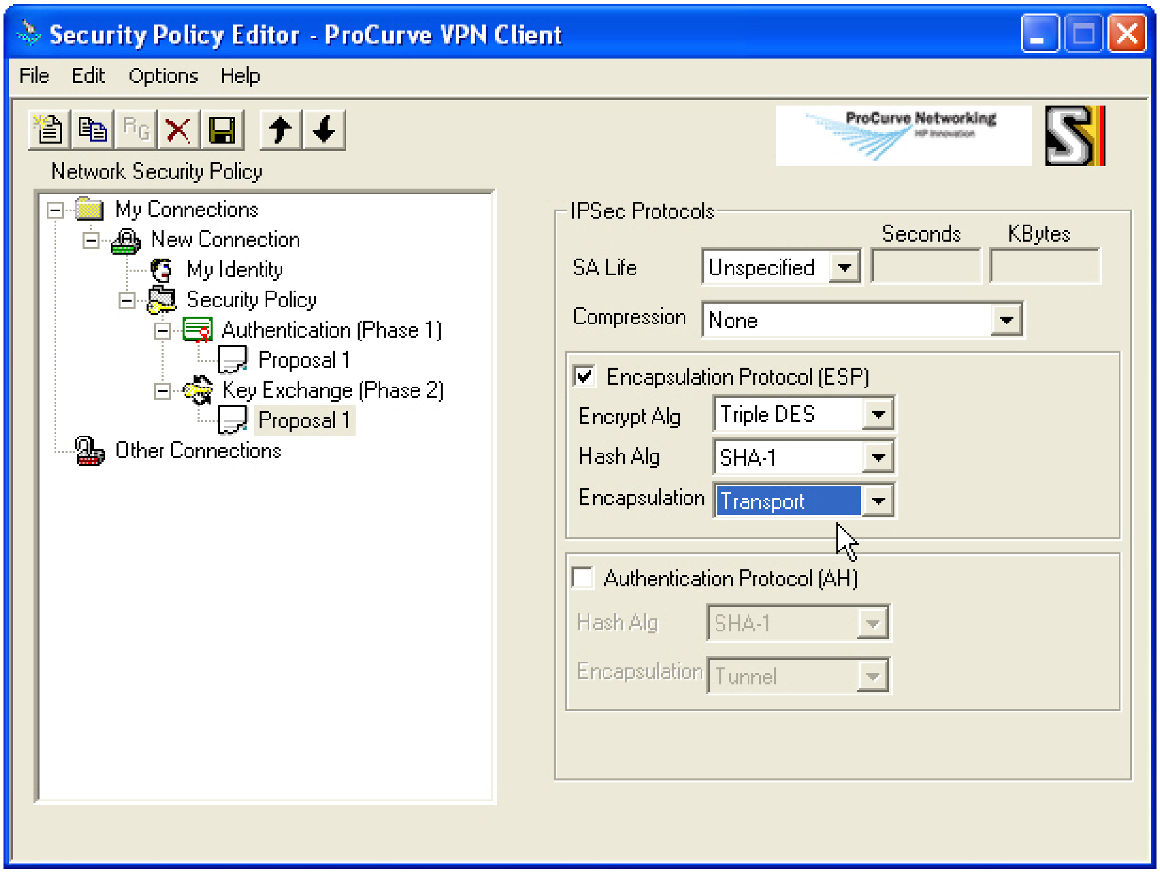
SA Life: Unspecified

Key Group: Diffie-Hellman Group 2

Figure 5.10 – Security Policy Editor

g. Select **Key Exchange (Phase 2)** and configure the following for **Proposal 1**:

- SA Life: **Unspecified**
- Compression: **None**
- Select the **Encapsulation Protocol (ESP)** checkbox
- Encryp(tion) Alg(orithm): **Triple DES**
- Hash Alg(orithm): **SHA-1**
- Encapsulation: **TRANSPORT**



Network Security Policy

- My Connections
  - New Connection
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
        - Proposal 1
      - Key Exchange (Phase 2)
        - Proposal 1
- Other Connections

IPSec Protocols

SA Life: Unspecified (Seconds, KBytes)

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Transport

□ Authentication Protocol (AH)

Hash Alg: SHA-1

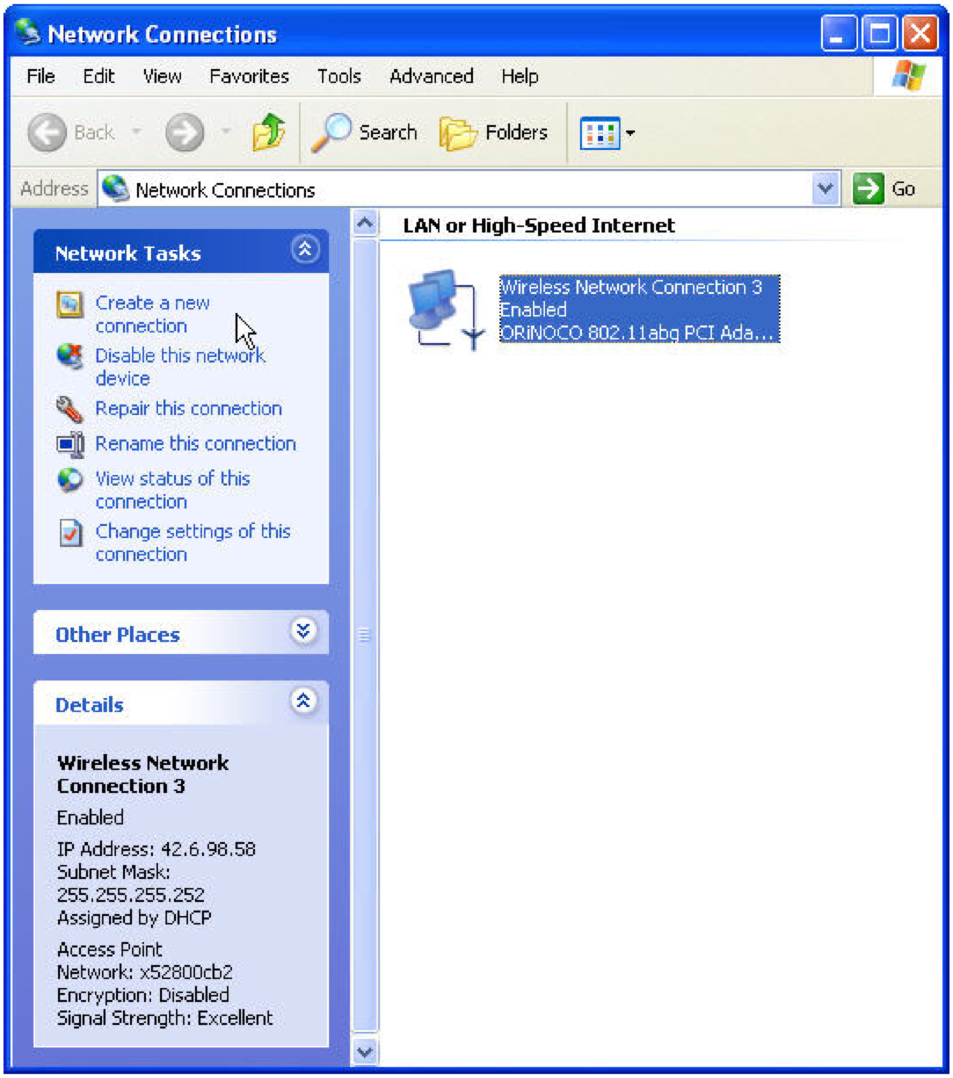
Encapsulation: Tunnel

Figure 5.11 – Security Policy Editor

h. Exit and **Save** changes.

Step 2: Configuring the Windows XP (native) VPN client

a. On the Windows XP Client, open the Network Connection window and click the **Create New Connection** icon to the left.



Wireless Network Connection 3
Enabled
ORiNOCO 802.11abg PCI Ada...

Wireless Network Connection 3

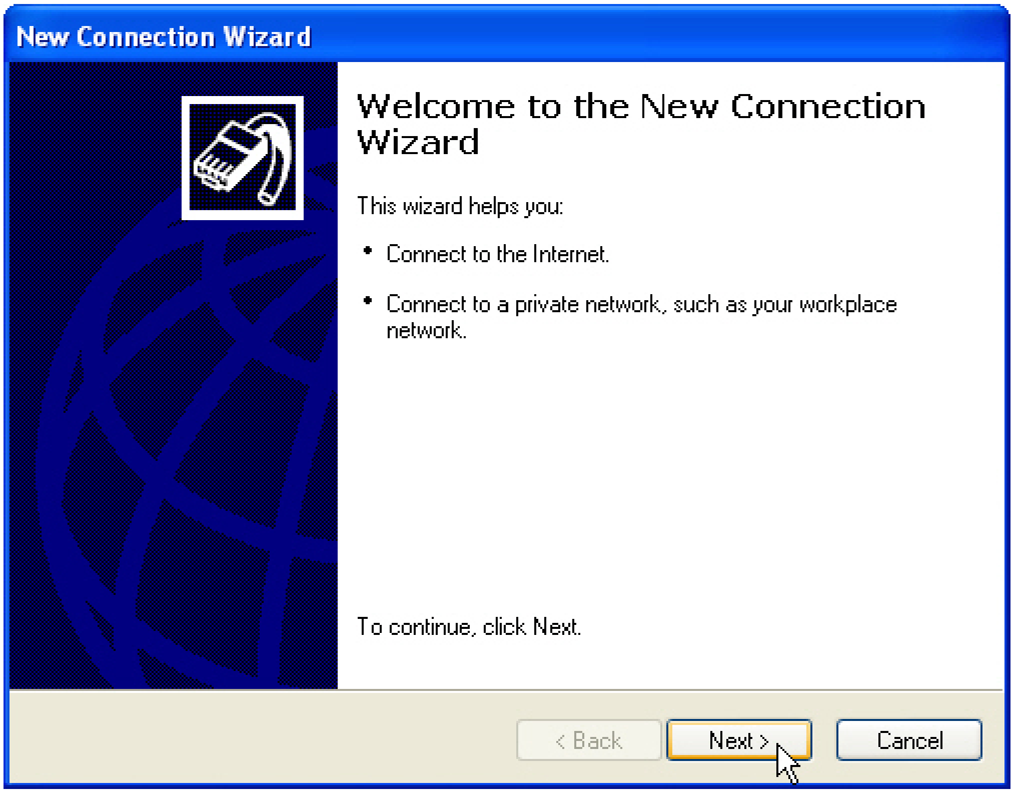
Enabled

IP Address: 42.6.98.58
Subnet Mask:
255.255.255.252
Assigned by DHCP

Access Point
Network: x52800cb2
Encryption: Disabled
Signal Strength: Excellent

Figure 5.12 – Network Connections

b. Click next to start the **New Connection Wizard**.



New Connection Wizard

Welcome to the New Connection Wizard

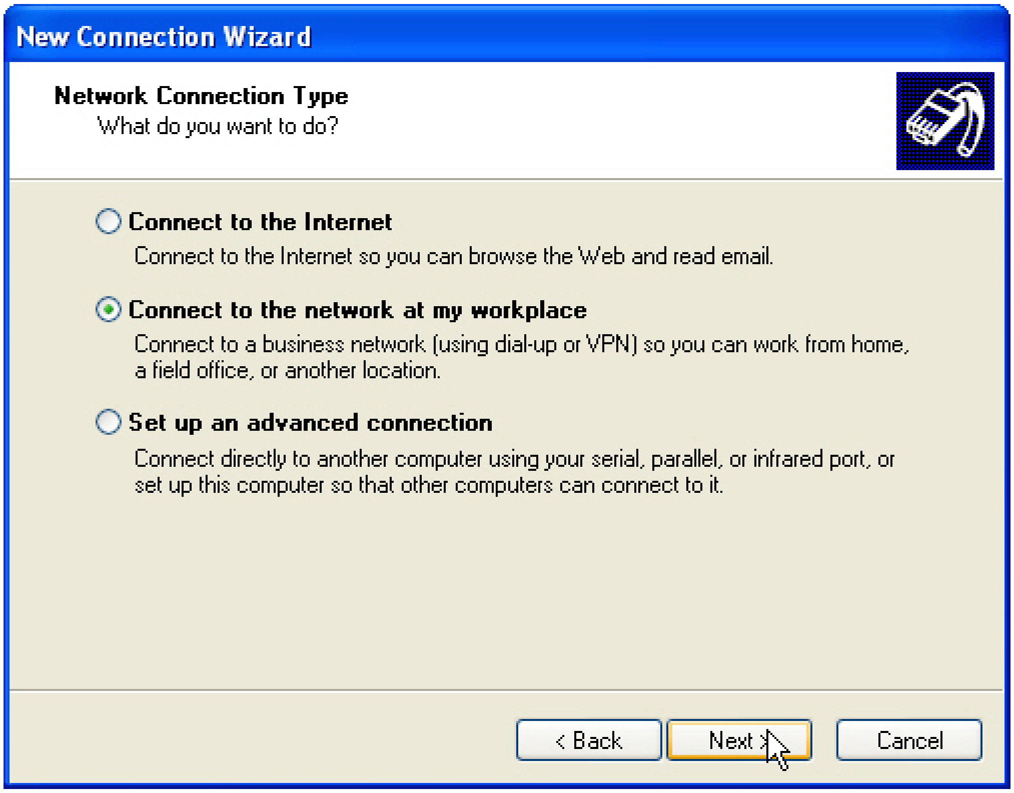
This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.

To continue, click Next.

Figure 5.13 – New Connection Wizard

c. Click the radio button to **Connect to the network at my workplace** and click next.



New Connection Wizard

Network Connection Type
What do you want to do?

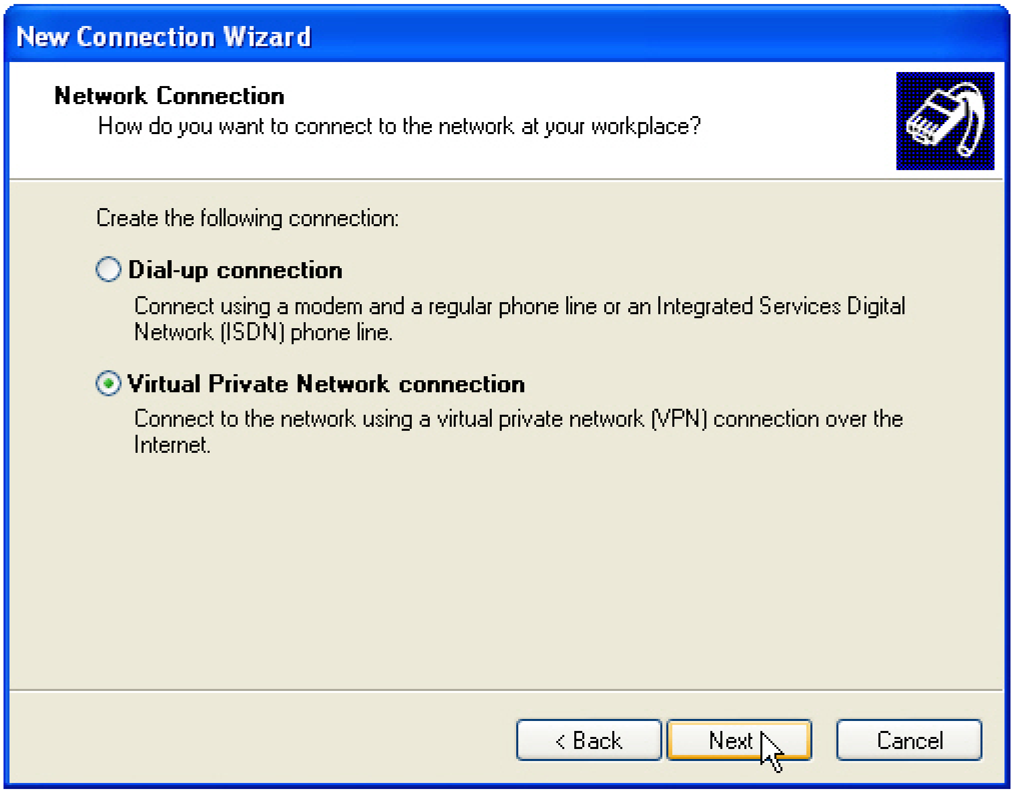
○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

Figure 5.14 – New Connection Wizard

d. Click the radio button to create a **Virtual Private Network** connection and click next.



New Connection Wizard

Network Connection

How do you want to connect to the network at your workplace?

Create the following connection:

○ **Dial-up connection**

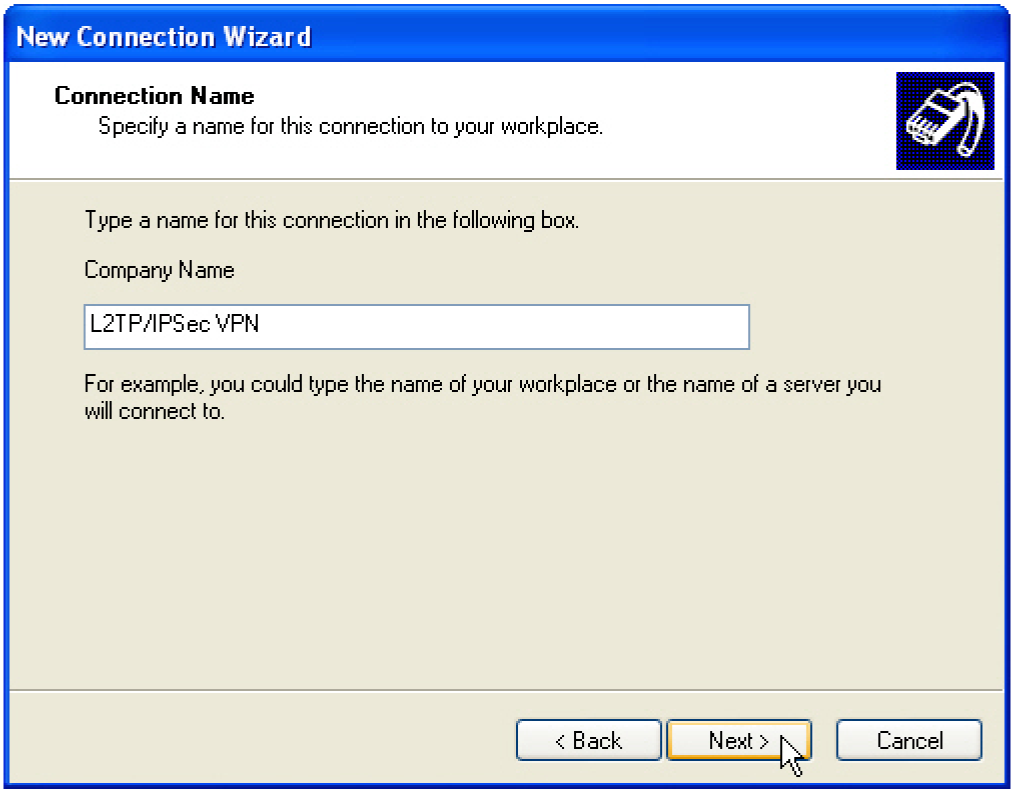
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**

Connect to the network using a virtual private network (VPN) connection over the Internet.

Figure 5.15 – New Connection Wizard

e. Name the connection and click next.



Connection Name

Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

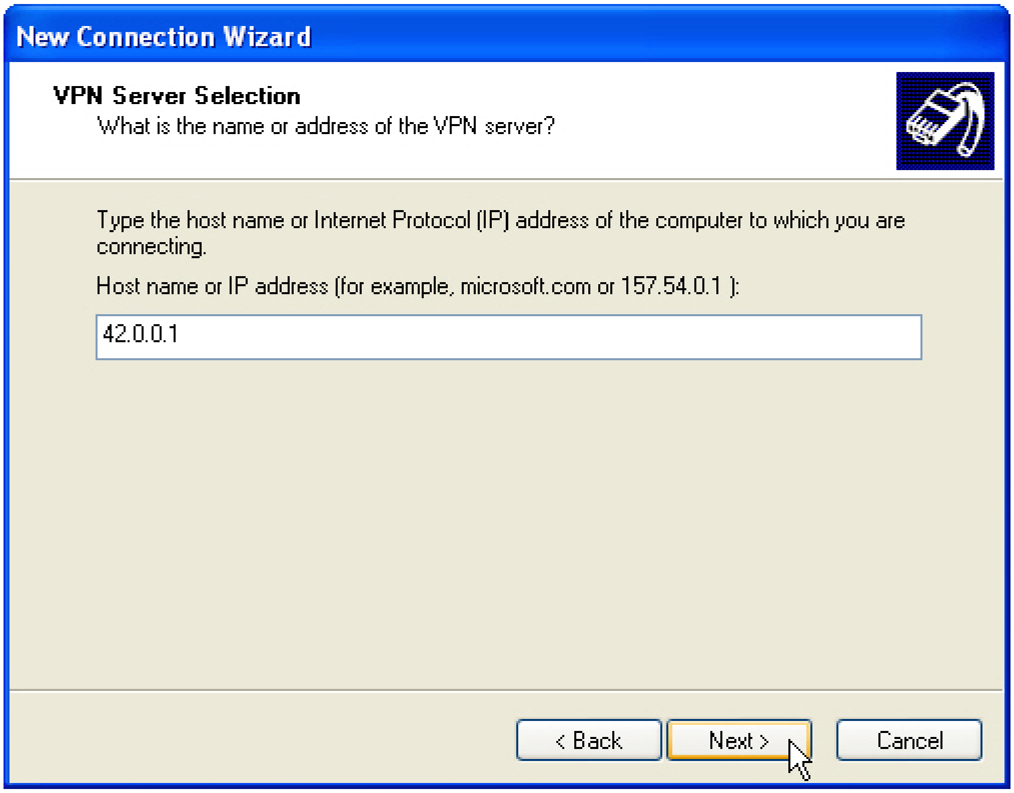
Company Name

L2TP/IPSec VPN

For example, you could type the name of your workplace or the name of a server you will connect to.

Figure 5.16 – New Connection Wizard

f. Configure the **IP address** of the VPN Server (**42.0.0.1**) and click next.



VPN Server Selection

What is the name or address of the VPN server?

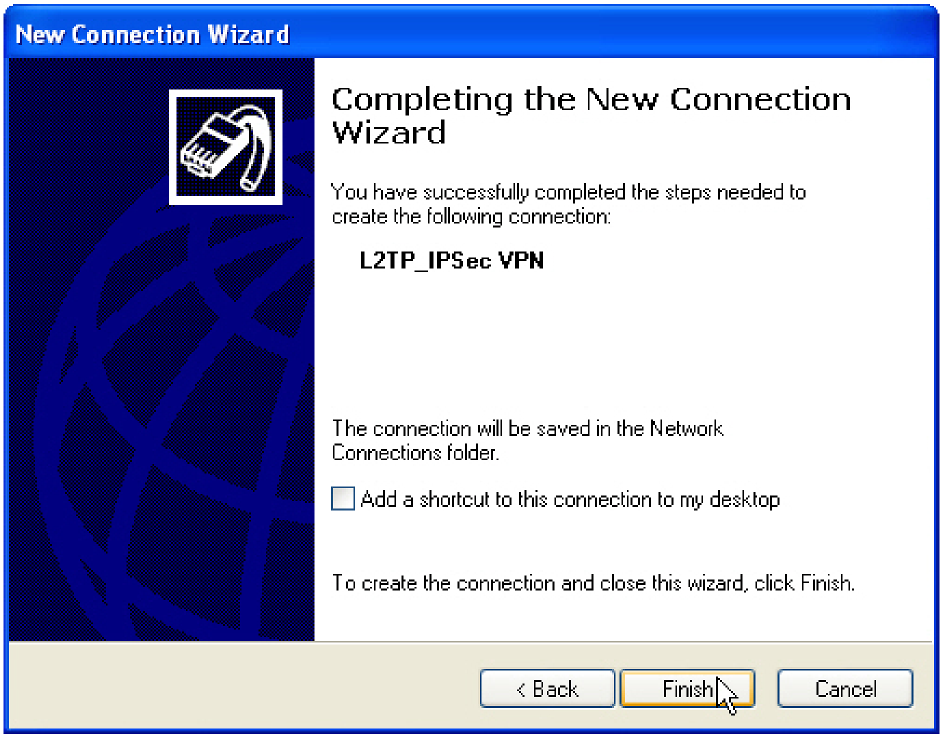
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

42.0.0.1

Figure 5.17 – New Connection Wizard

g. Select a Connection Availability and click next. Click **Finish** to complete the New Connection Wizard.



New Connection Wizard

Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

L2TP_IPSec VPN

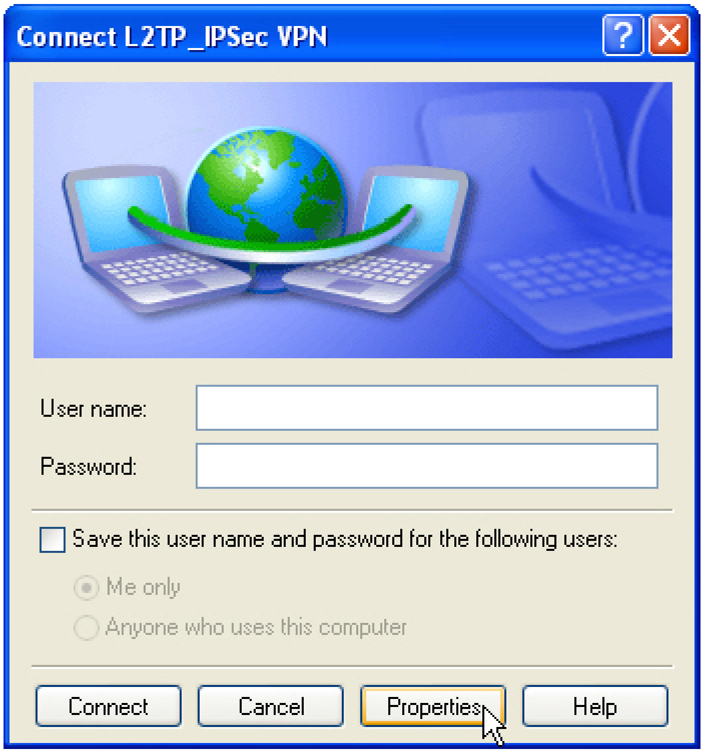
The connection will be saved in the Network Connections folder.

□ Add a shortcut to this connection to my desktop

To create the connection and close this wizard, click Finish.

Figure 5.18 – New Connection Wizard

h. At the VPN connection dialog box, click the **Properties** button.



Connect L2TP_IPSec VPN

User name:

Password:

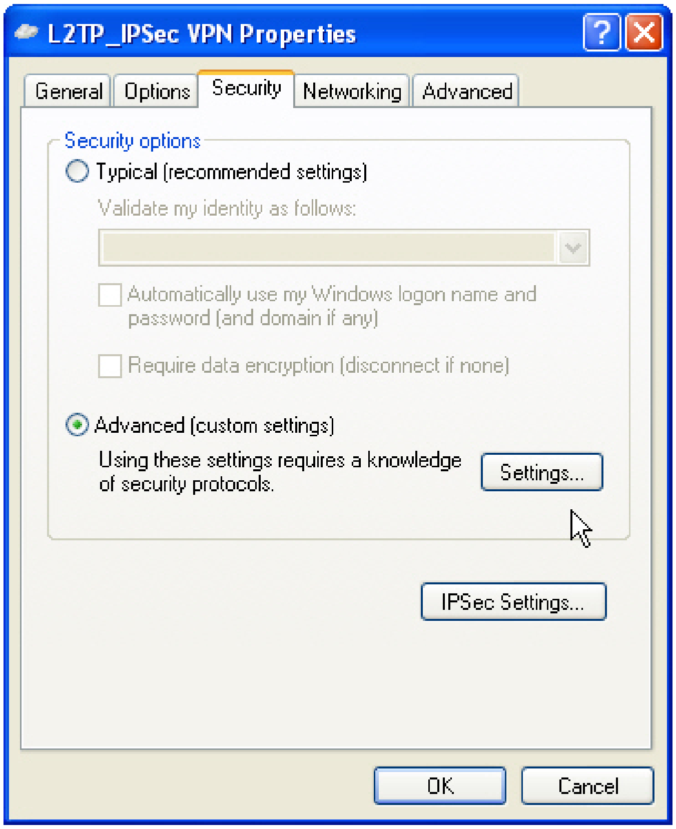
□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

Figure 5.19 – VPN Connection Dialog Box

i. In the VPN connection properties, select the **Security** tab and click the radio button to select **Advanced (custom settings).**



L2TP_IPSec VPN Properties

General | Options | Security | Networking | Advanced

Security options

○ Typical (recommended settings)

Validate my identity as follows:

□ Automatically use my Windows logon name and password (and domain if any)

□ Require data encryption (disconnect if none)

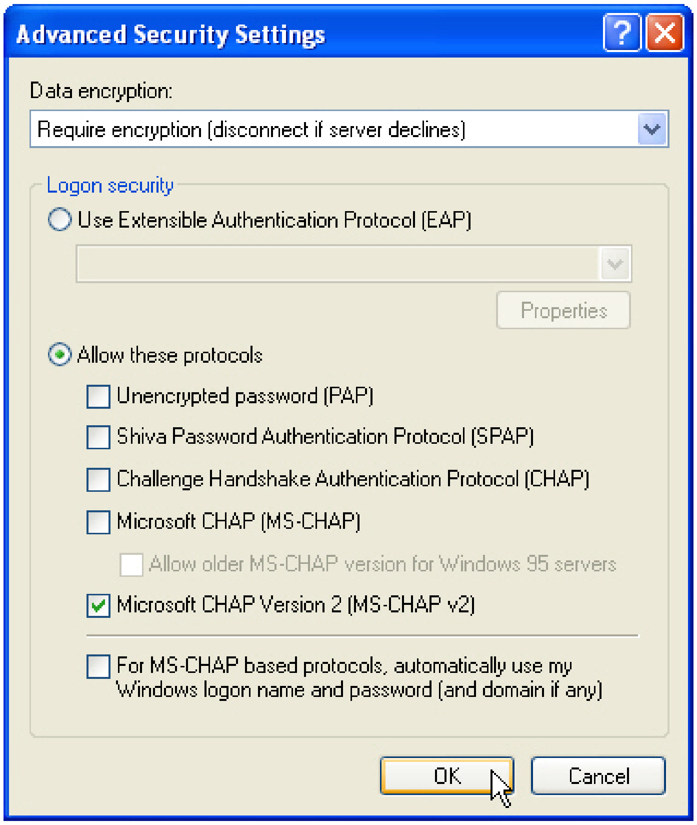
● Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

Figure 5.20 – VPN Connection Properties

j. Click the **Settings** button and configure the following and click OK.

- Data Encryption: **Require encryption (disconnect if server declines)**
- Protocols: **MS-CHAP v2 only**
- If **MS-CHAP** is selected, be sure to **DESELECT** it.



Advanced Security Settings

Data encryption:

Require encryption (disconnect if server declines)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

□ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP (MS-CHAP)

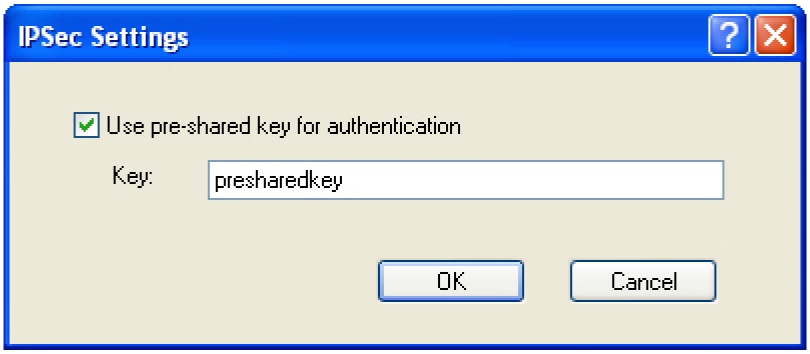
□ Allow older MS-CHAP version for Windows 95 servers

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

Figure 5.21 – Advanced Security Settings

k. Click the **IPSec Settings** button, configure the preshared key and click OK.



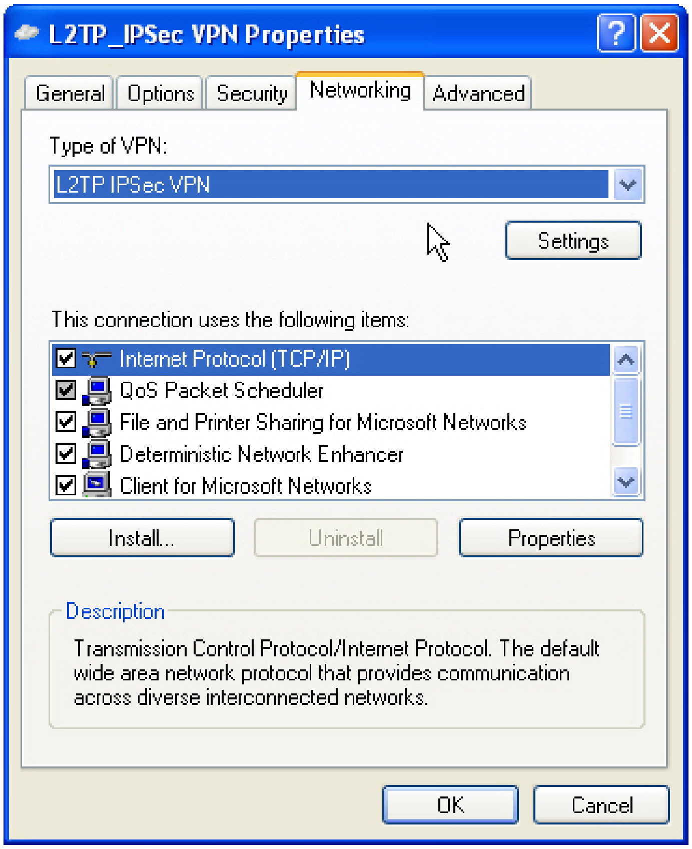
IPSec Settings

☑ Use pre-shared key for authentication

Key: presharedkey

Figure 5.22 – IPSec Settings

l. On the Networking tab, configure the Type of VPN to **L2TP IPSec VPN** and click OK.



Type of VPN: L2TP IPSec VPN

This connection uses the following items:

- ☑ Internet Protocol (TCP/IP)
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Deterministic Network Enhancer
- ☑ Client for Microsoft Networks

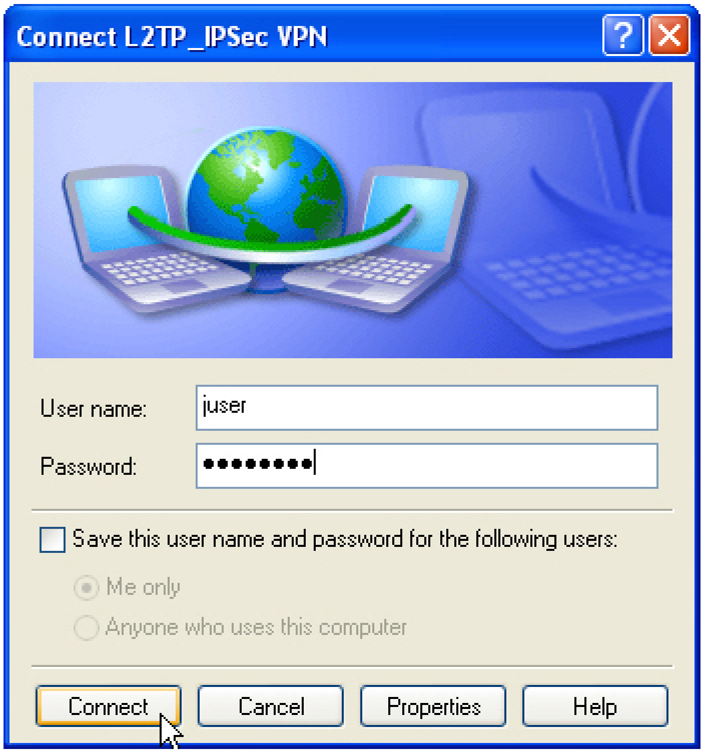
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 5.23 – VPN Connection Properties

Step 3: Connect the L2TP/IPSec VPN using the Windows (native) VPN client

a. Back at the VPN connection dialog box, input the **username** and **password** and click connect. Note: The username and password are configured on the RADIUS sever for authentication.



Connect L2TP_IPSec VPN

User name: juser

Password: ●●●●●●●●●

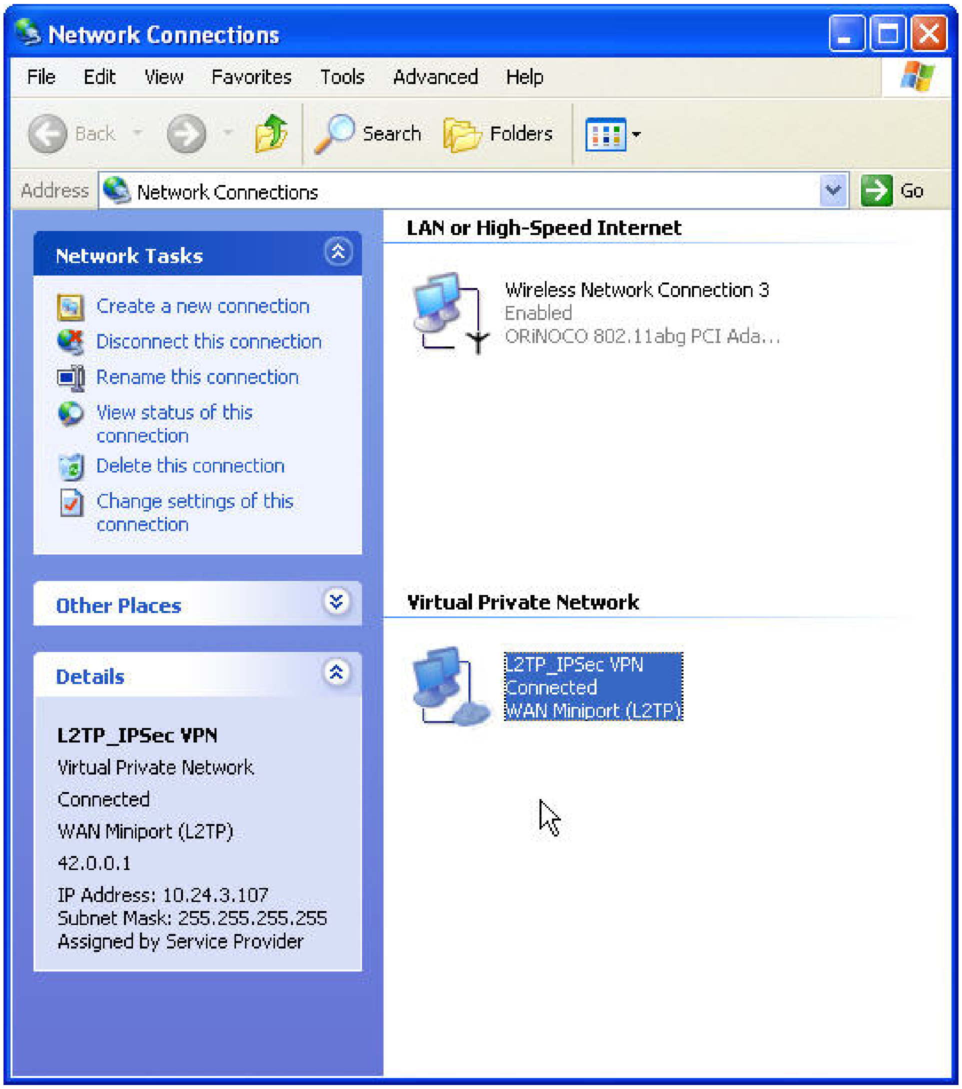
□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

Figure 5.24 – VPN Connection Dialog Box

b. Validate a successful VPN connection is established in the **Network connections** window.



Address: Network Connections

LAN or High-Speed Internet

Wireless Network Connection 3
Enabled
ORiNOCO 802.11abg PCI Ada...

Virtual Private Network

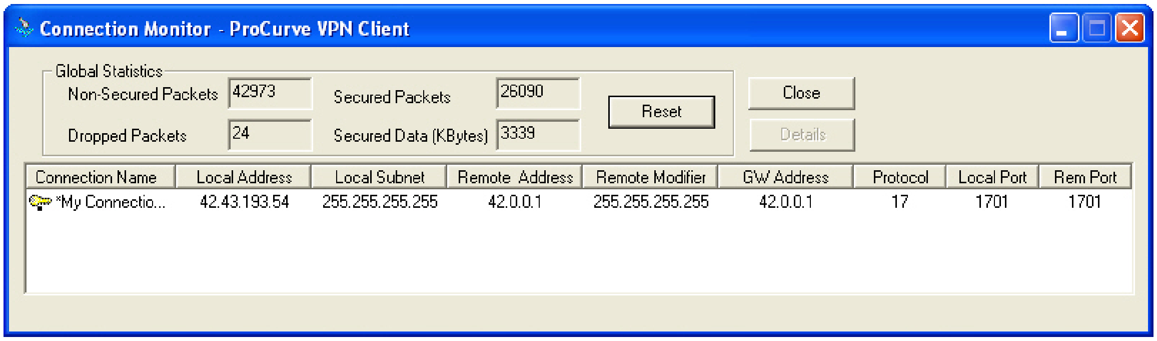
L2TP_IPSec VPN
Connected
WAN Miniport (L2TP)

Details

L2TP_IPSec VPN
Virtual Private Network
Connected
WAN Miniport (L2TP)
42.0.0.1
IP Address: 10.24.3.107
Subnet Mask: 255.255.255.255
Assigned by Service Provider

Figure 5.25 – Network Connections

c. Validate a successful VPN connection is established in the ProCurve VPN **Connection Monitor**.



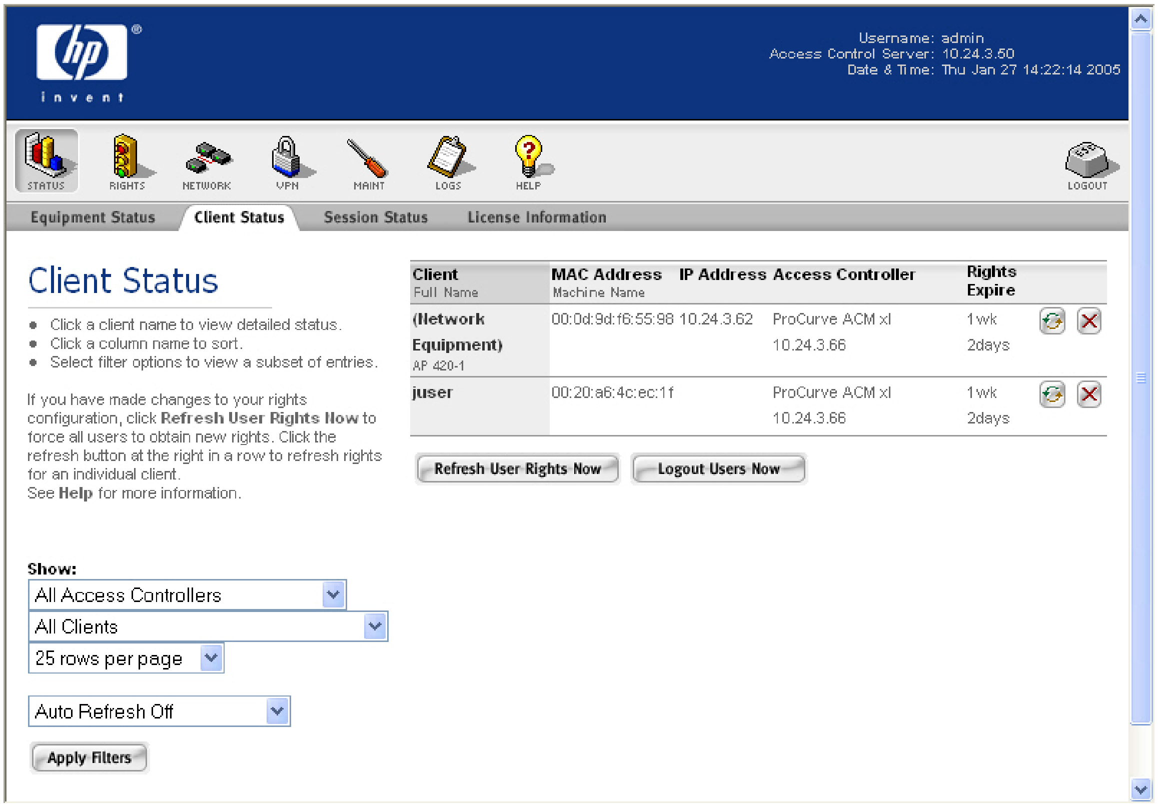
Global Statistics

Non-Secured Packets: 42973
Secured Packets: 26090
Dropped Packets: 24
Secured Data (KBytes): 3339

Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port
*My Connectio...	42.43.193.54	255.255.255.255	42.0.0.1	255.255.255.255	42.0.0.1	17	1701	1701

Figure 5.26 – ProCurve VPN Client

d. Validate a user **login / authentication** on the ACS.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Jan 27 14:22:14 2005

Client Status

- Click a client name to view detailed status.
- Click a column name to sort.
- Select filter options to view a subset of entries.

If you have made changes to your rights configuration, click **Refresh User Rights Now** to force all users to obtain new rights. Click the refresh button at the right in a row to refresh rights for an individual client.
See **Help** for more information.

Client Full Name	**MAC Address** Machine Name	**IP Address**	**Access Controller**	**Rights Expire**
(Network Equipment) AP 420-1	00:0d:9d:f6:55:98	10.24.3.62	ProCurve ACM xl 10.24.3.66	1wk 2days
juser	00:20:a6:4c:ec:1f		ProCurve ACM xl 10.24.3.66	1wk 2days

Show:
All Access Controllers
All Clients
25 rows per page

Auto Refresh Off

Figure 5.27 – Client Status

Configuring Scenario 6: Monitored Logon 802.1x Authentication

Scenario 6 consists of a wireless, Dynamic WEP, Windows XP client authenticating via 802.1x Monitored logon. In this example, the AP 420 is the authenticator for the client and the ACS monitors the logon process. 802.1 x logon authentications require both a RADIUS server (with authentication policy) and an LDAP database of users. In this example, we will be using Microsoft's IAS (RADIUS) and Active Directory to accomplish this.

Note: This scenario requires the installation and configuration of services that will not be shown here, with the exception of specific changes required by the configuration scenario. Refer to product documentation for more information.

The steps required for Scenario 6 are:

- On the Enterprise Server, create a user account in Active Directory and associate it with a group.
- On the Enterprise Server, create a new RADIUS client (in this case, the AP 420).
- On the Enterprise Server, create a Remote Access Policy for authentication.
- On the ACS, define a RADIUS Authentication Service and associate it to the System Authentication Policy
- On the ACS, create an 802.1x Authentication Service and associate it to the System Authentication Policy.
- From the ACS, configure the ProCurve Access Control xl Module with the DHCP Server IP Address to allow clients to use Real IP addresses.
- On the AP 420, configure Dynamic WEP/802.1x and add the RADIUS Server IP address and RADIUS Key.
- On the wireless Windows XP client, configure the client for 802.1x authentication, connect and verify authentication.

1) **On the Enterprise Server, create a user account in Active Directory and associate it with a group.**
    a. Refer to Scenario 2 in Part One of this guide for details on creating a User and Group affiliation in Active Directory.

2) **On the Enterprise Server, create a new RADIUS client (in this case, the AP 420).**
   Note: The Enterprise Server is configured as a Domain Controller named "samcorp.com".

    a. To create a new RADIUS client on the Enterprise Server, open IAS (Start → Administrative Tools → Internet Authentication Service). Right click on RADIUS Clients and select New RADIUS Client.

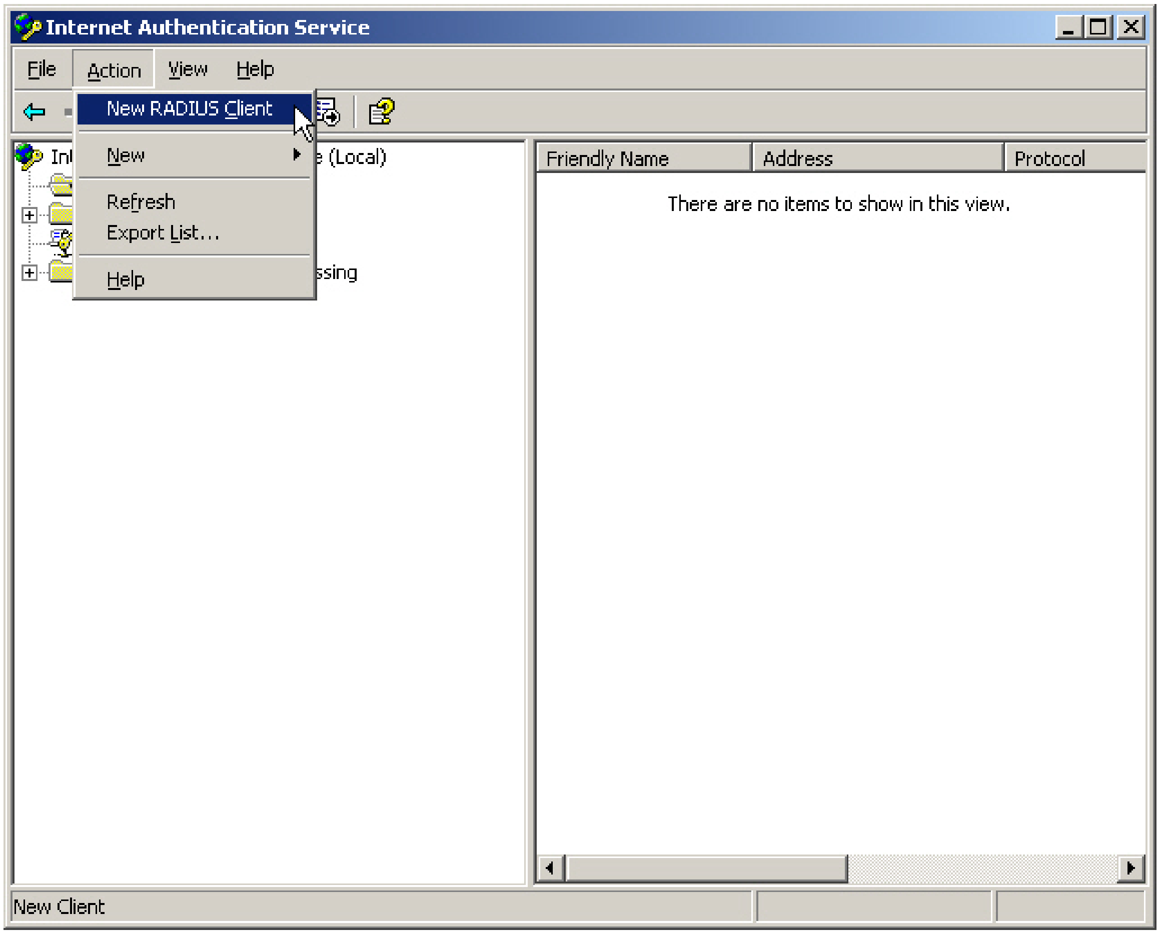
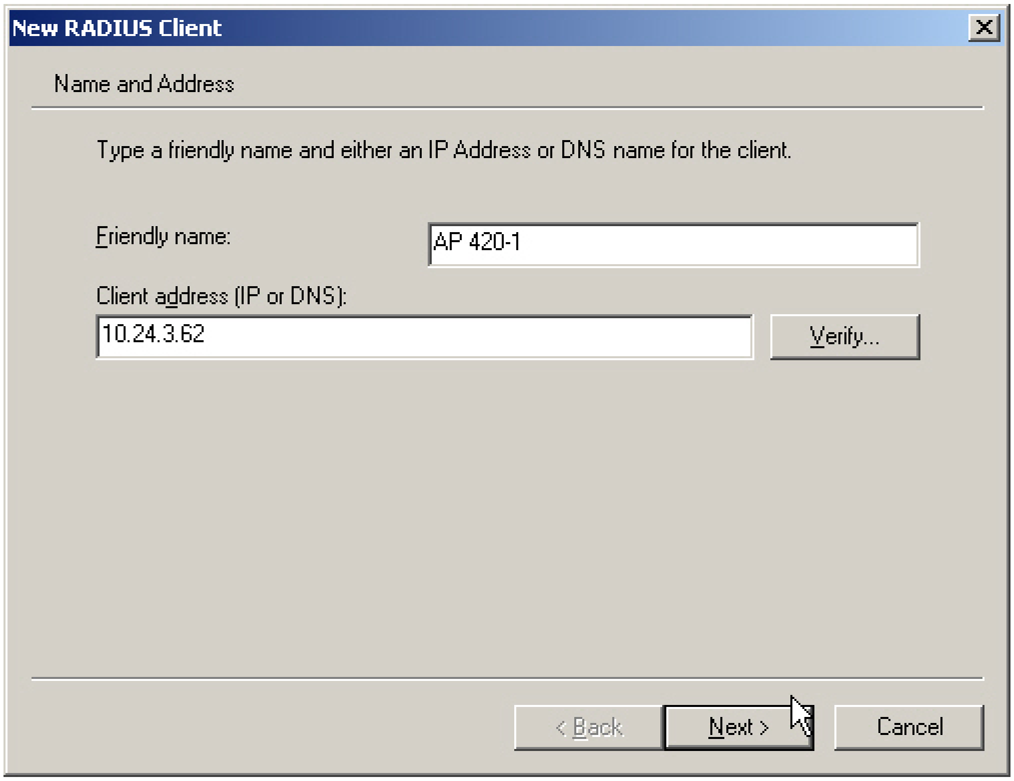


Figure 6.1 – Internet Authentication Service

b. Configure a Friendly name (AP 420-1) and enter the **IP address of the Access Point** (10.24.3.62). Click Next.



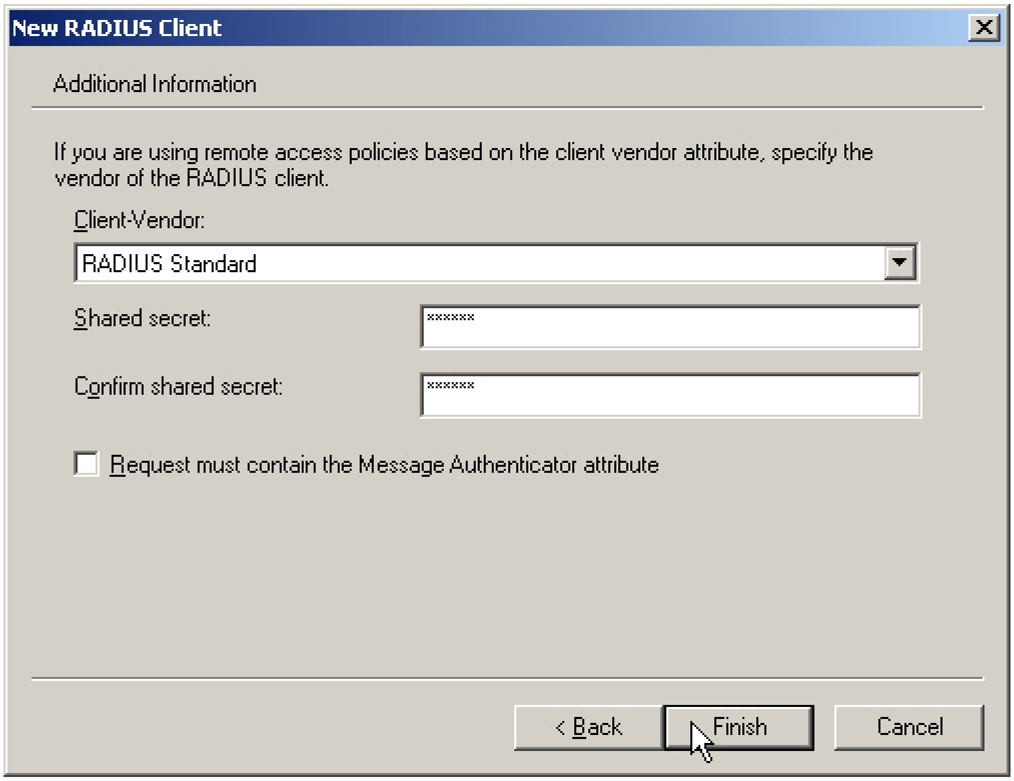
Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: AP 420-1

Client address (IP or DNS): 10.24.3.62

Figure 6.2 – New RADIUS Client

c. Ensure **RADIUS Standard** is selected as the Client-Vendor and configure a **shared secret** (`secret`). Click Finish.



Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

Shared secret: ******

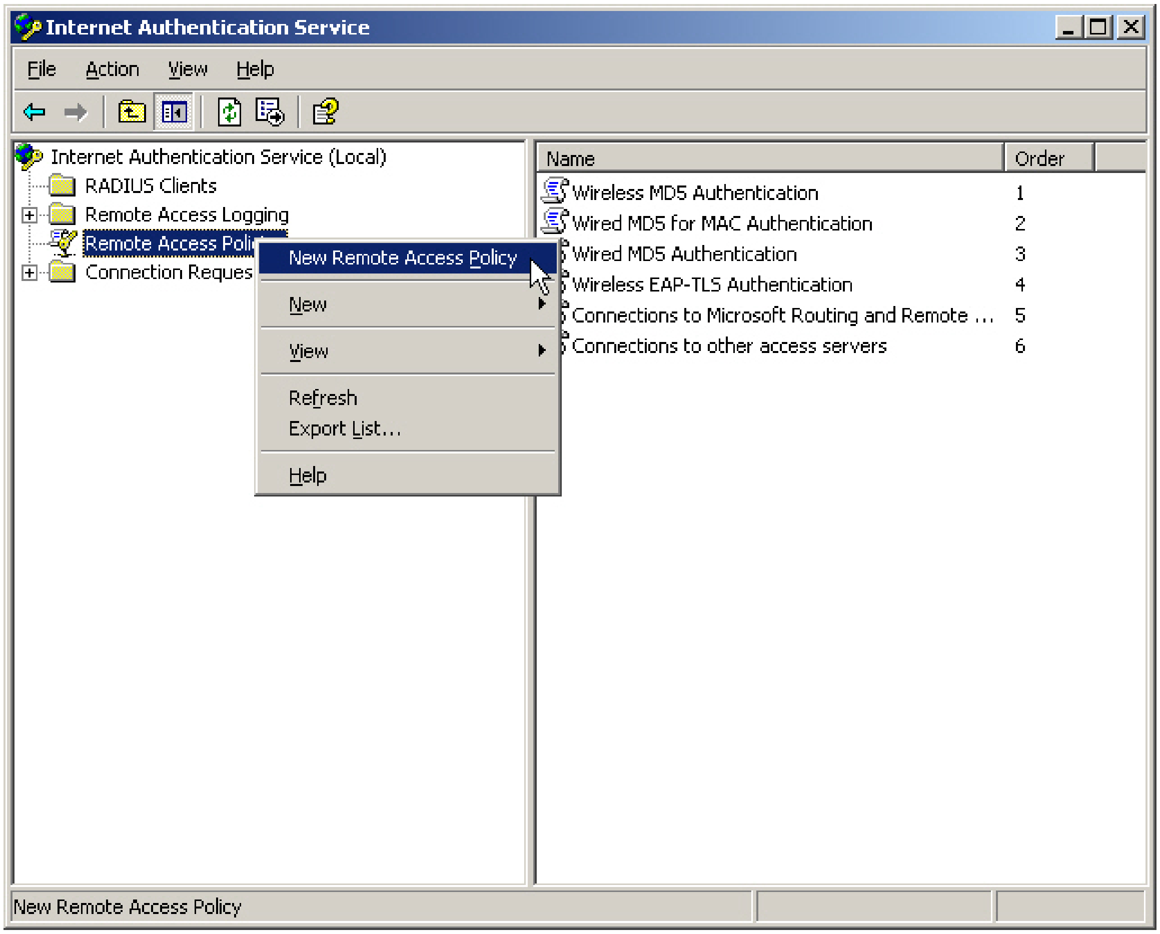
Confirm shared secret: ******

□ Request must contain the Message Authenticator attribute

Figure 6.3 – New RADIUS Client

3) On the Enterprise Server, create a Remote Access Policy for authentication.

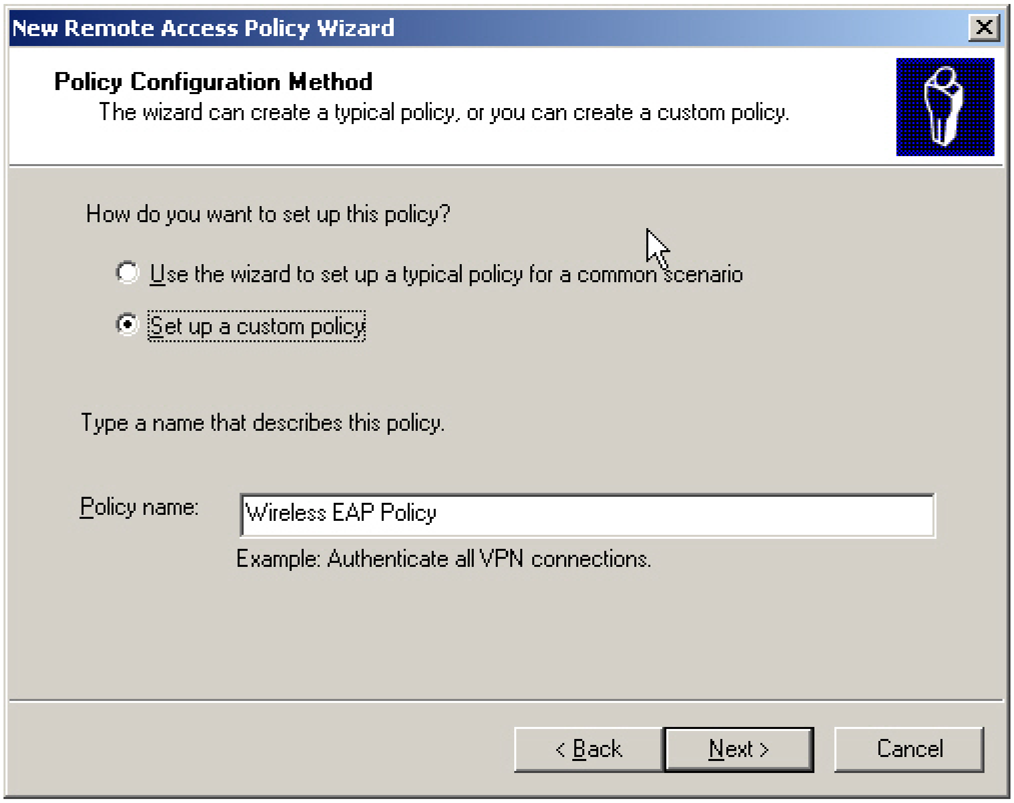
a. To create a Remote Access Policy on the Enterprise Server, open IAS (Start → Administrative Tools → Internet Authentication Service). Right click on Remote Access Policies and select **New Remote Access Policy**.



Name	Order
Wireless MD5 Authentication	1
Wired MD5 for MAC Authentication	2
Wired MD5 Authentication	3
Wireless EAP-TLS Authentication	4
Connections to Microsoft Routing and Remote ...	5
Connections to other access servers	6

Figure 6.4 – Internet Authentication Service

b. In the Policy Wizard, select the radio button to **Set up a custom policy**, configure a Policy name (Wireless EAP Policy) and click next.



New Remote Access Policy Wizard

Policy Configuration Method

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

How do you want to set up this policy?

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

● Set up a custom policy

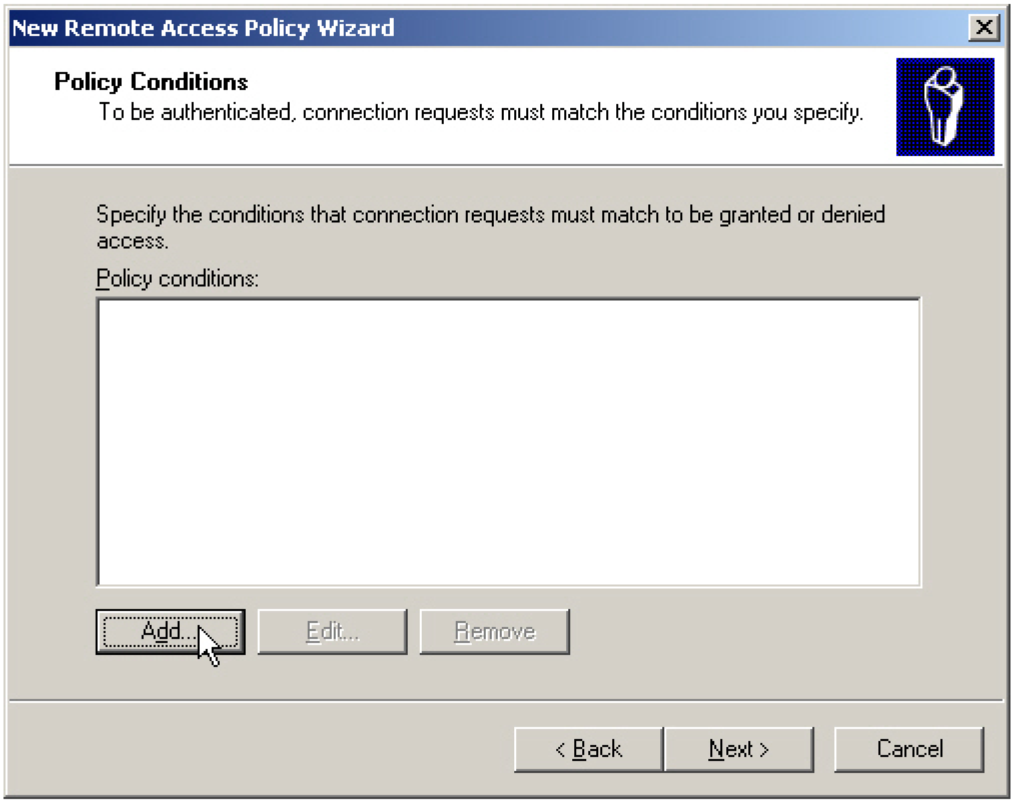
Type a name that describes this policy.

Policy name: Wireless EAP Policy

Example: Authenticate all VPN connections.

Figure 6.5 – New Remote Access Policy Wizard

c. Click **Add** to add policy conditions.



New Remote Access Policy Wizard

Policy Conditions

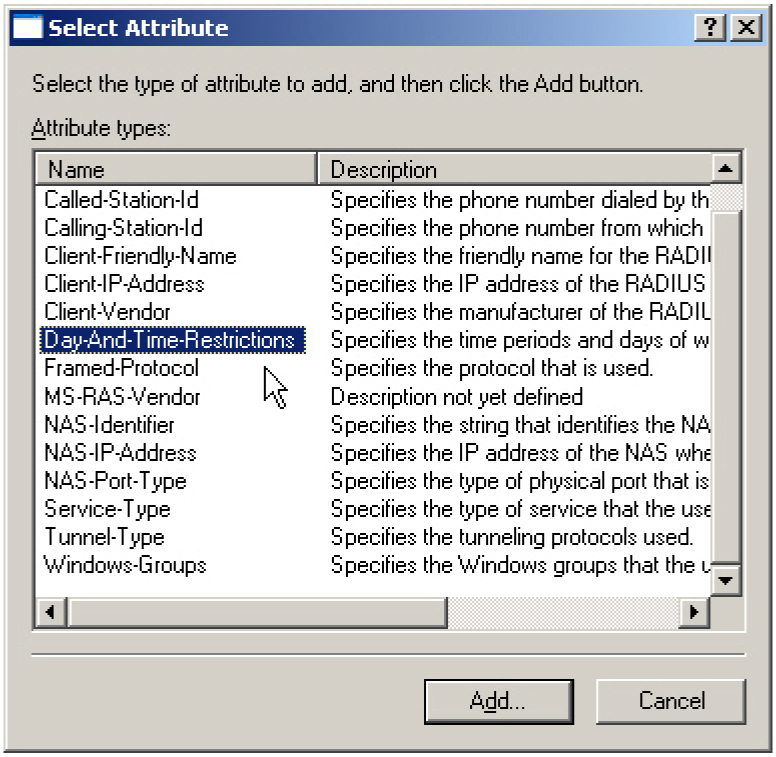
To be authenticated, connection requests must match the conditions you specify.

Specify the conditions that connection requests must match to be granted or denied access.

Policy conditions:

Figure 6.6 – New Remote Access Policy Wizard

d. Select the **Day-And-Time-Restrictions** attribute and click add.



Select Attribute

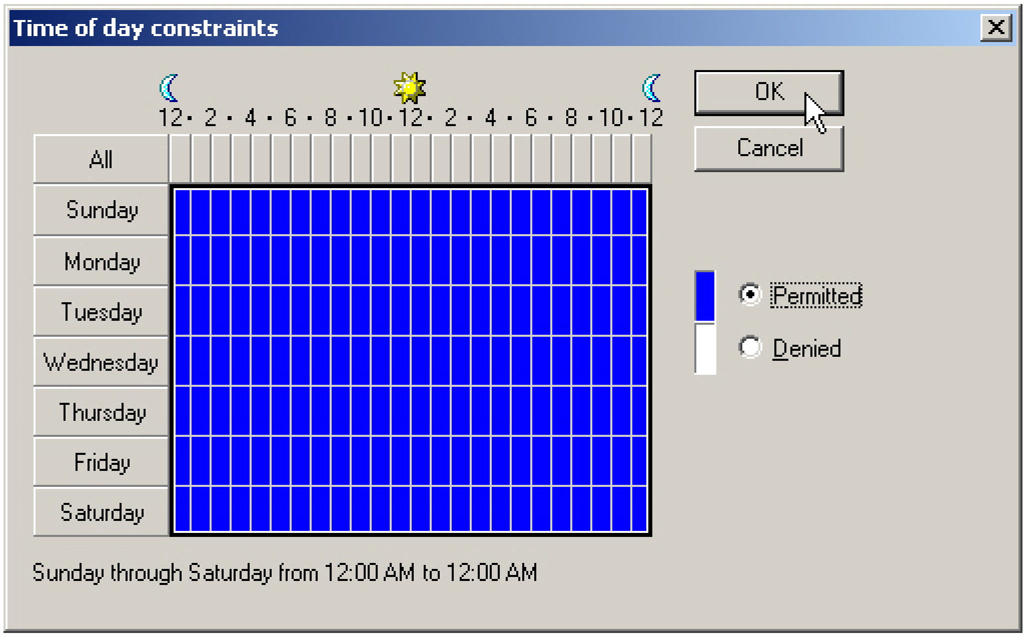
Select the type of attribute to add, and then click the Add button.

Attribute types:

Name	Description
Called-Station-Id	Specifies the phone number dialed by th
Calling-Station-Id	Specifies the phone number from which
Client-Friendly-Name	Specifies the friendly name for the RADII
Client-IP-Address	Specifies the IP address of the RADIUS
Client-Vendor	Specifies the manufacturer of the RADIL
Day-And-Time-Restrictions	Specifies the time periods and days of w
Framed-Protocol	Specifies the protocol that is used.
MS-RAS-Vendor	Description not yet defined
NAS-Identifier	Specifies the string that identifies the NA
NAS-IP-Address	Specifies the IP address of the NAS whe
NAS-Port-Type	Specifies the type of physical port that is
Service-Type	Specifies the type of service that the use
Tunnel-Type	Specifies the tunneling protocols used.
Windows-Groups	Specifies the Windows groups that the u

Figure 6.7 – Select Attribute

e. Click the **Permitted** radio button to allow access anytime and click OK.



Time of day constraints

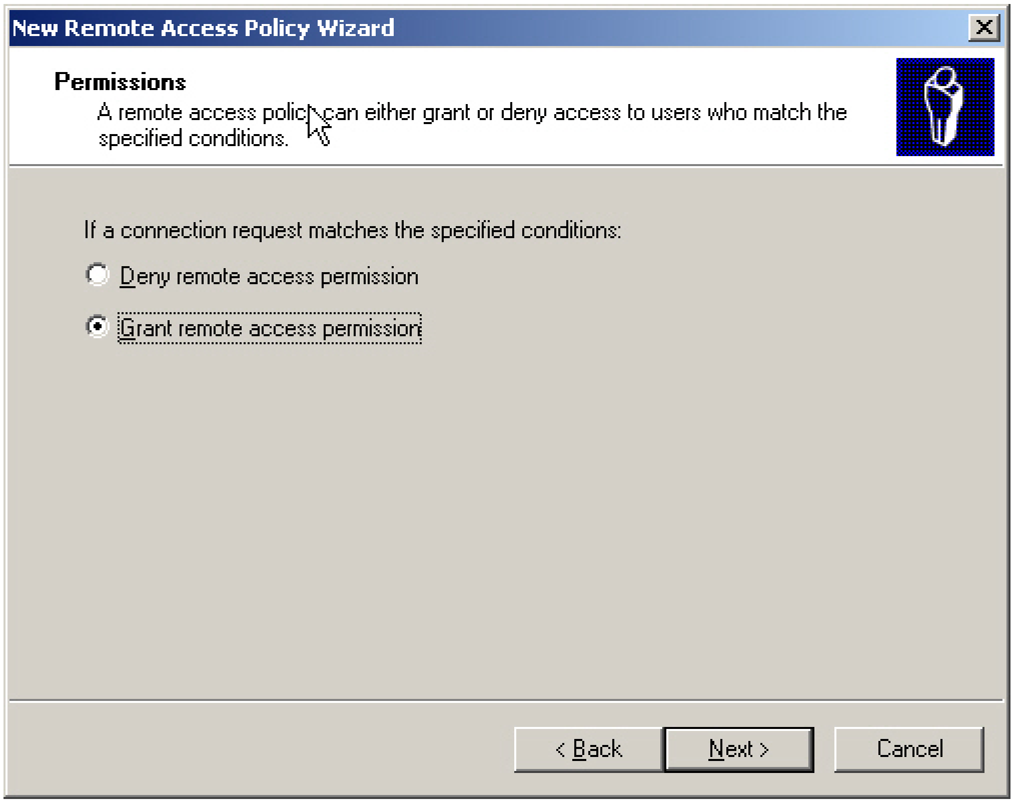
● Permitted

○ Denied

Sunday through Saturday from 12:00 AM to 12:00 AM

Figure 6.8 – Time of Day constraints

f. Click OK and Next to accept the Policy Conditions. Select the **Grant remote access permission** radio button and click next.



New Remote Access Policy Wizard

Permissions

A remote access policy can either grant or deny access to users who match the specified conditions.

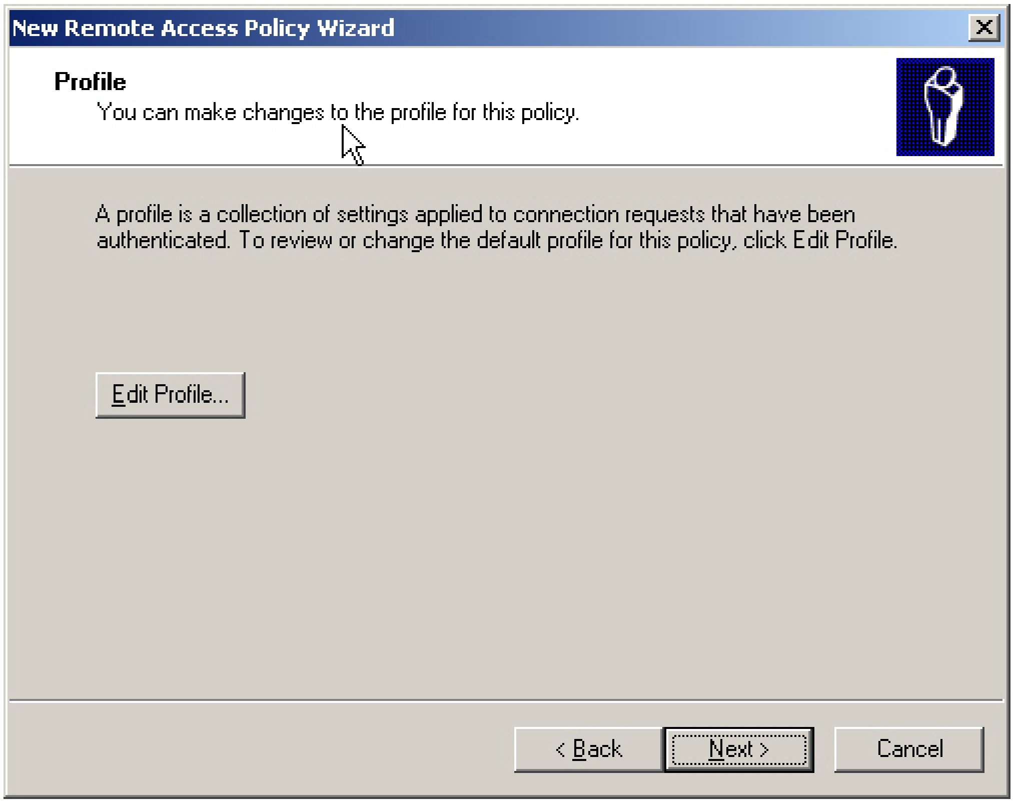
If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

Figure 6.9 – New Remote Access Policy Wizard

g. Select the **Edit Profile** button.



New Remote Access Policy Wizard

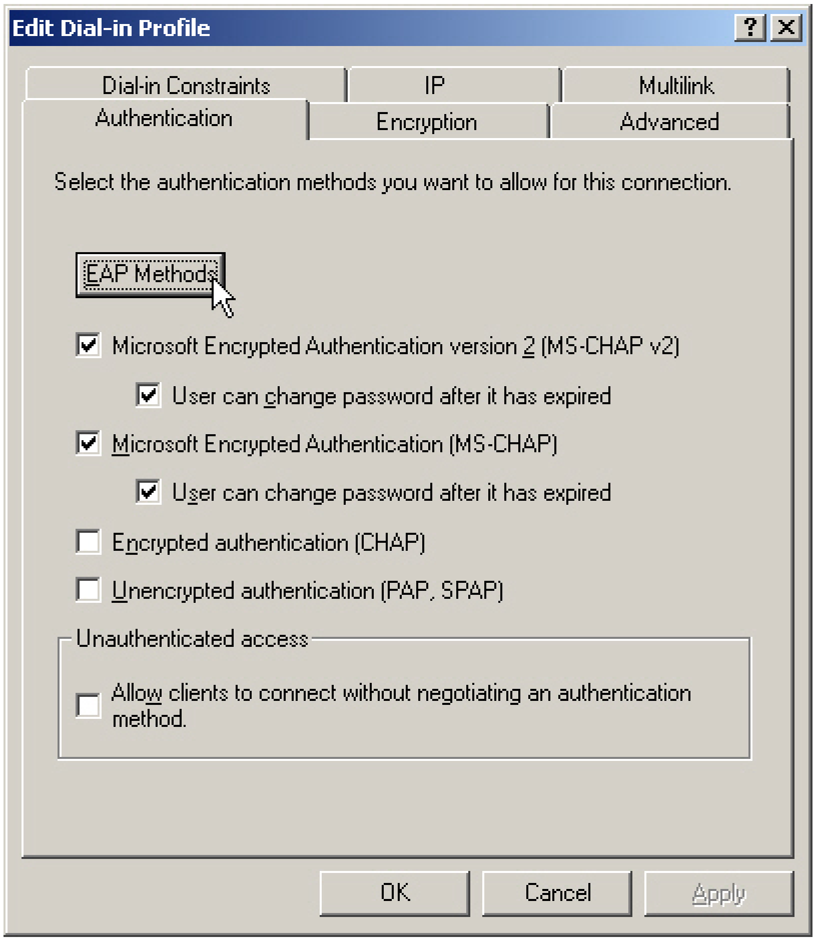
Profile

You can make changes to the profile for this policy.

A profile is a collection of settings applied to connection requests that have been authenticated. To review or change the default profile for this policy, click Edit Profile.

Figure 6.10 – New Remote Access Policy Wizard

h. Select the **Authentication tab** in the Edit Dial-in Profile window and click the **EAP Methods** button.



Select the authentication methods you want to allow for this connection.

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☑ User can change password after it has expired

☑ Microsoft Encrypted Authentication (MS-CHAP)

☑ User can change password after it has expired

□ Encrypted authentication (CHAP)

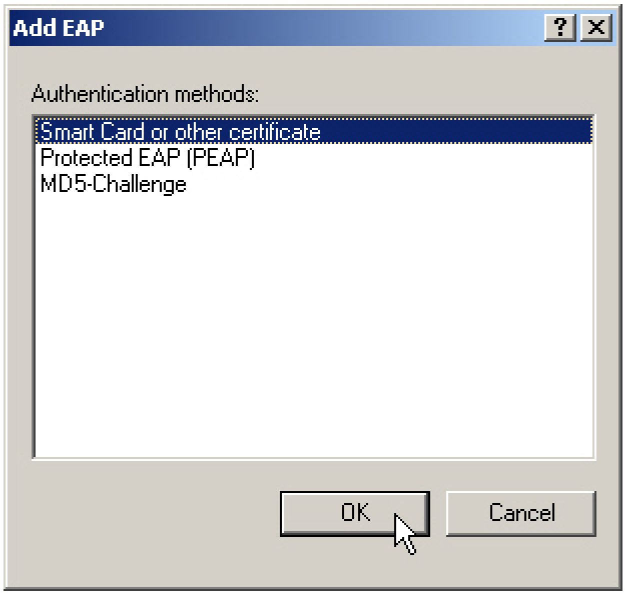
□ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

□ Allow clients to connect without negotiating an authentication method.

Figure 6.11 – Edit Dial-in-Profile

i. Select the **Add** button and add the **Smart Card of other certificate EAP** type and click OK.

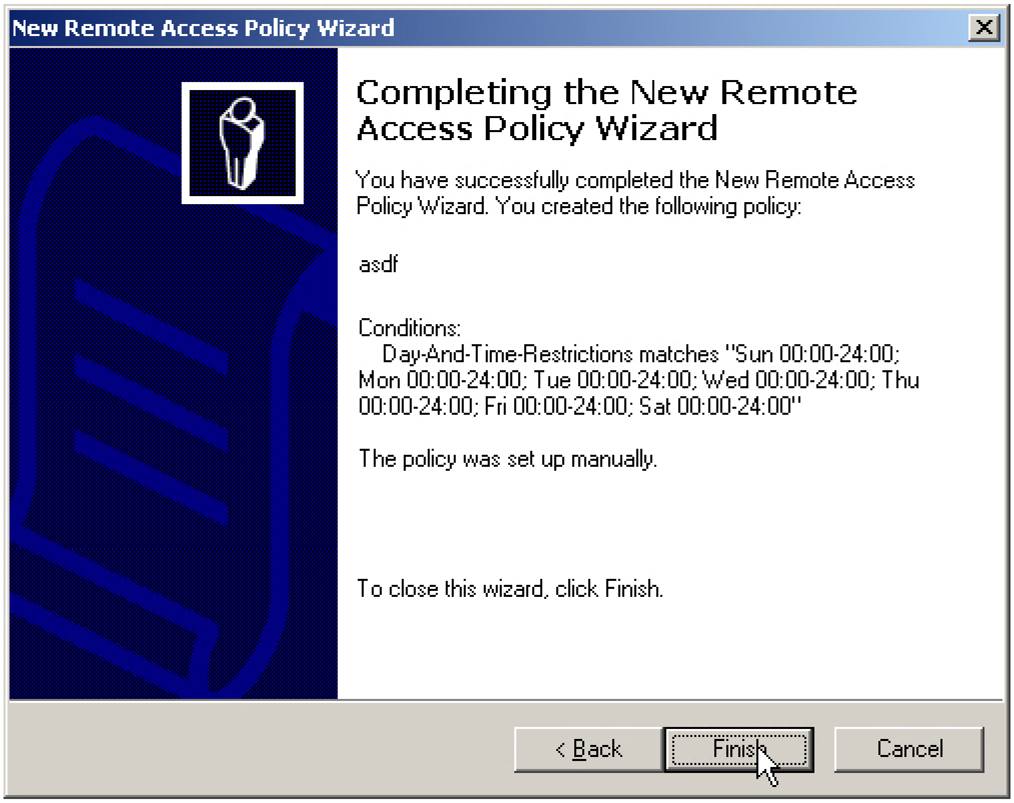

Add EAP

Authentication methods:

Smart Card or other certificate
Protected EAP (PEAP)
MD5-Challenge

Figure 6.12 – Add EAP type

j. Click OK and Next to finish the New Remote Access Policy Wizard.


New Remote Access Policy Wizard

Completing the New Remote Access Policy Wizard

You have successfully completed the New Remote Access Policy Wizard. You created the following policy:

asdf

Conditions:
Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00; Tue 00:00-24:00; Wed 00:00-24:00; Thu 00:00-24:00; Fri 00:00-24:00; Sat 00:00-24:00"

The policy was set up manually.

To close this wizard, click Finish.

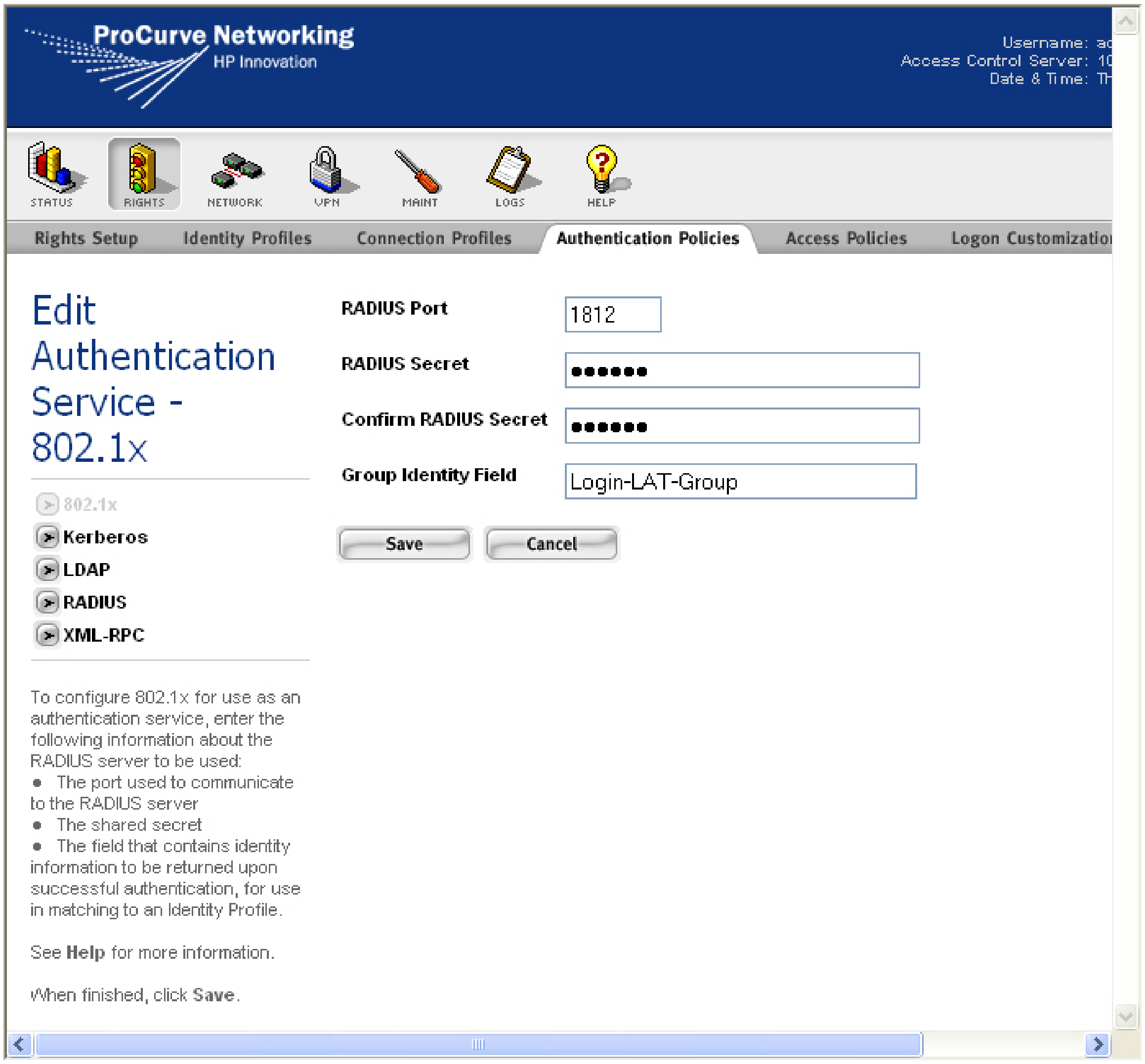
Figure 6.13 – New Remote Access Policy Wizard

4) On the ACS, define a RADIUS Authentication Service and associate it to the System Authentication Policy.

a. Refer to Scenario 3 in Part One of this guide for details on defining a RADIUS Authentication Service and Associating is to the System Authentication Policy.

5) On the ACS, configure an 802.1x Authentication Service and associate it to the System Authentication Policy.

a. On the ACS, browse to Rights -> Authentication Policies -> Authentication Services and click the 802.1x Logons Service. Configure the 802.1x Authentication Service with the following information and save changes.
   - RADIUS Port: **1812**
   - RADIUS Secret: **secret**
   - Group Identity Field: **Login-LAT-Group**



Edit Authentication Service - 802.1x

RADIUS Port: 1812

RADIUS Secret: ●●●●●●

Confirm RADIUS Secret: ●●●●●●

Group Identity Field: Login-LAT-Group

To configure 802.1x for use as an authentication service, enter the following information about the RADIUS server to be used:

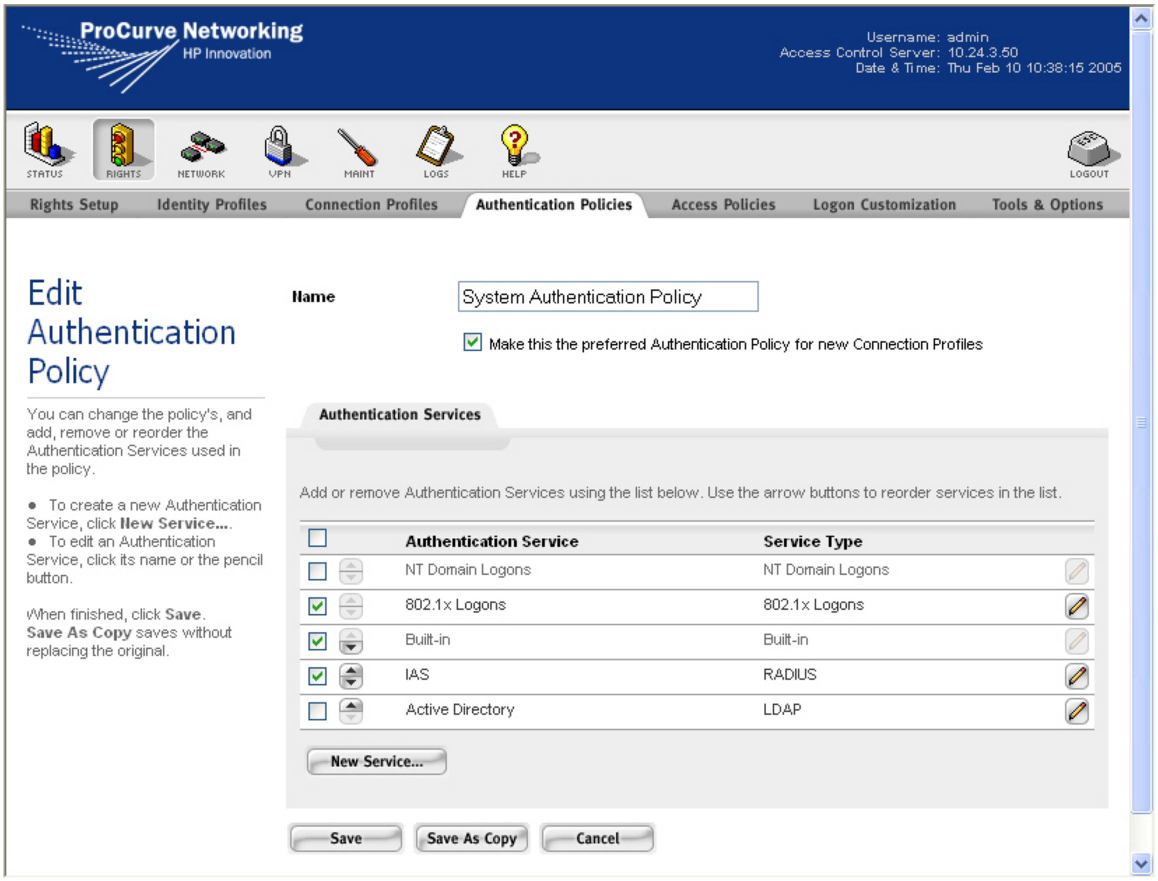
- The port used to communicate to the RADIUS server
- The shared secret
- The field that contains identity information to be returned upon successful authentication, for use in matching to an Identity Profile.

See **Help** for more information.

When finished, click **Save**.

Figure 6.14 – Authentication Service 802.1x

b. Browse to Rights -> Authentication Policies and click the System Authentication Policy. Add the newly configured **802.1x Authentication Service** to the **System Authentication Policy** and save changes.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Feb 10 10:38:15 2005

Edit Authentication Policy

You can change the policy's, and add, remove or reorder the Authentication Services used in the policy.

- To create a new Authentication Service, click **New Service...**
- To edit an Authentication Service, click its name or the pencil button.

When finished, click **Save**. **Save As Copy** saves without replacing the original.

Name System Authentication Policy

☑ Make this the preferred Authentication Policy for new Connection Profiles

Authentication Services

Add or remove Authentication Services using the list below. Use the arrow buttons to reorder services in the list.

□	Authentication Service	Service Type
□	NT Domain Logons	NT Domain Logons
☑	802.1x Logons	802.1x Logons
☑	Built-in	Built-in
☑	IAS	RADIUS
□	Active Directory	LDAP

Figure 6.15 – System Authentication Policy

6) On the ACS, configure the Authenticated Access Policy to allow clients to use Real IP addresses (via DHCP).

a. Refer to Configuring Scenario 2 in Part One of this guide to configure the Authenticated Access Policy to allow clients to use Real IP addresses.

b. On the ACS, browse to Status -> Client Status and click **Refresh User Rights Now**.

7) On the AP 420, configure Dynamic WEP/802.1x and add the RADIUS Server IP address and RADIUS Key.

a. Configure Dynamic WEP/802.1x and add the RADIUS Server IP address and RADIUS Key.

```
HP ProCurve Access Point 420# configure
HP ProCurve Access Point 420(config)# int wireless g
Enter Wireless configuration commands, one per line.
HP ProCurve Access Point 420(if-wireless g)# security-suite 5
HP ProCurve Access Point 420(if-wireless g)#end
HP ProCurve Access Point 420(config)# radius-server address
10.24.3.10
HP ProCurve Access Point 420(config)# radius-server key secret
HP ProCurve Access Point 420(config)# exit
```

8) On the wireless Windows XP client, configure the client for 802.1x authentication, connect and verify authentication.

Note: Connecting the client in Scenario 6 requires that the client have the appropriate client certificates for EAP-TLS Authentication and be a member of the Domain (in this case “samcorp.com”). See related documentation for more information.

This example uses the **Proxim Client Utility** (version 3.1.2.19) for wireless Dynamic WEP/802.1x connectivity.

a. Start the Proxim Client Utility, select the Profile Management tab and click **Modify**.

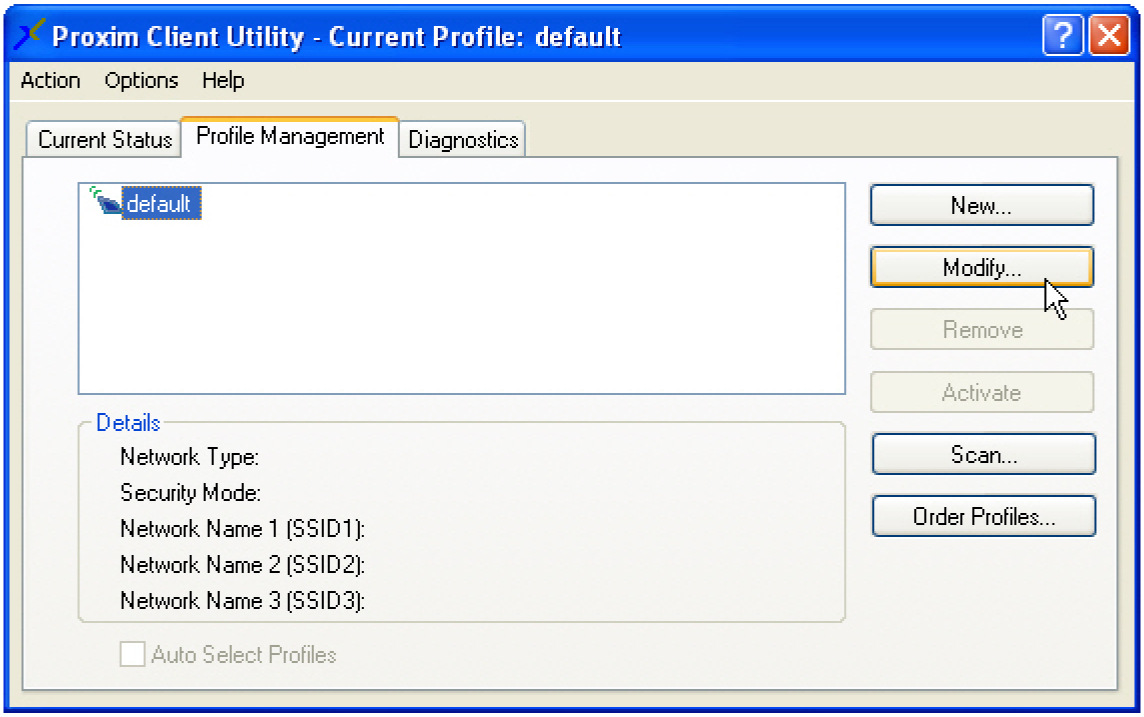
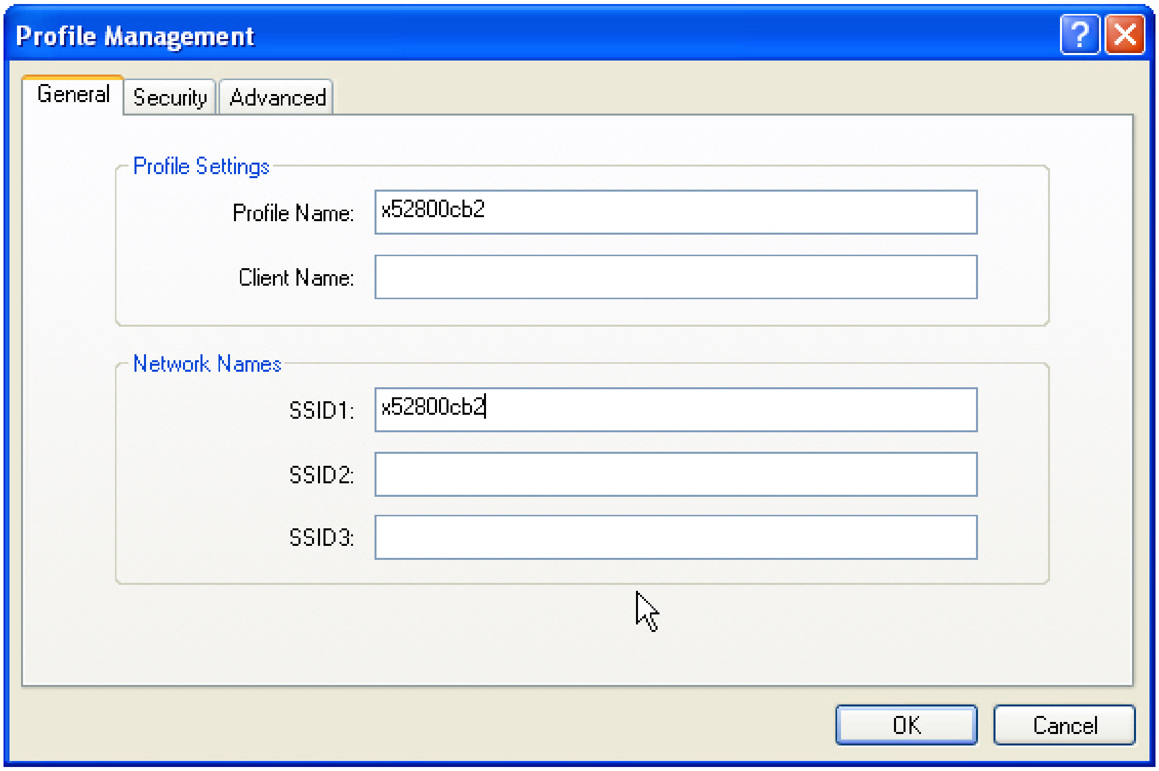


Figure 6.16 – Proxim Client Utility

b. Configure a **Profile name** and an **SSID**. Click OK.



Profile Management

Profile Settings

Profile Name: x52800cb2

Client Name:

Network Names

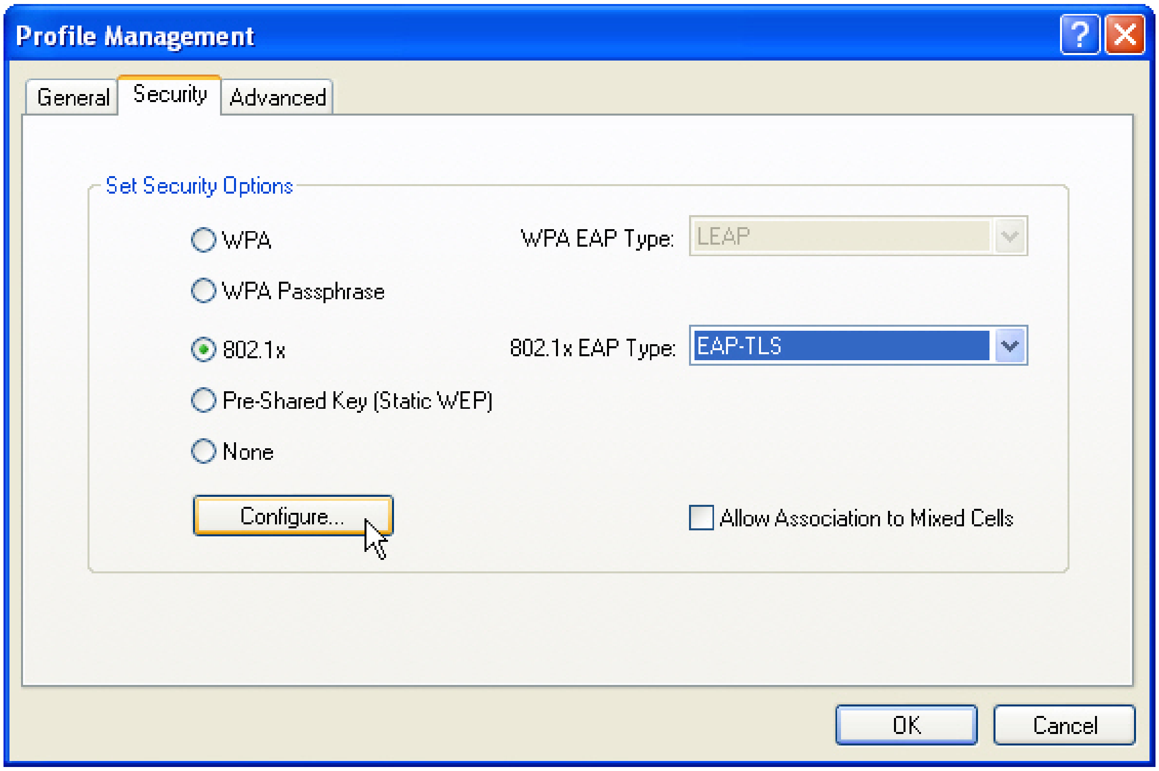
SSID1: x52800cb2

SSID2:

SSID3:

Figure 6.17 – Profile Management

c. Select the **Security Tab** and click the radio button to select **802.1x** and set the 802.1x EAP Type to **EAP-TLS**. Click the Configure button.



Profile Management

Set Security Options

○ WPA WPA EAP Type: LEAP

○ WPA Passphrase

● 802.1x 802.1x EAP Type: EAP-TLS

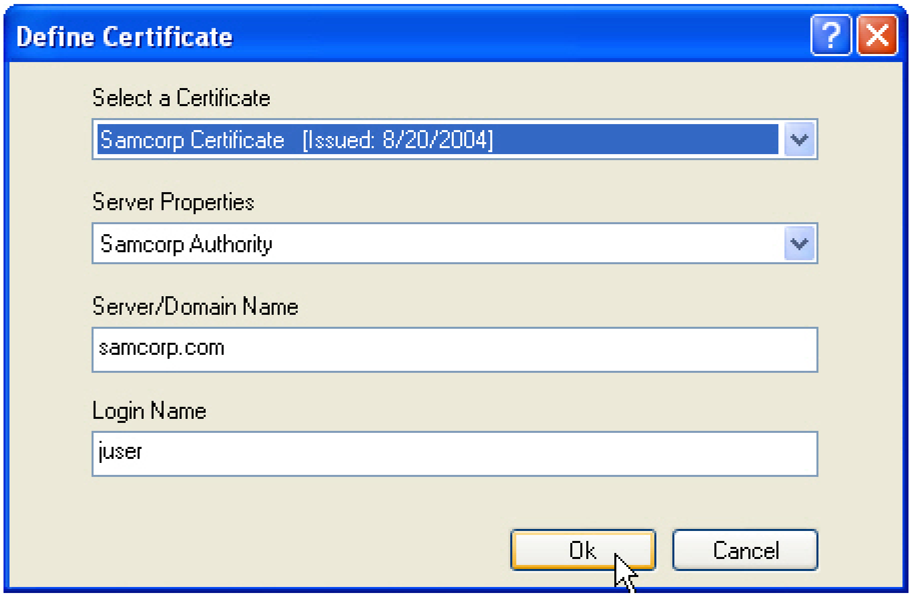
○ Pre-Shared Key (Static WEP)

○ None

□ Allow Association to Mixed Cells

Figure 6.18 – Profile Management

d. Select the appropriate **Certificate** parameters and click OK.



Define Certificate

Select a Certificate: Samcorp Certificate [Issued: 8/20/2004]

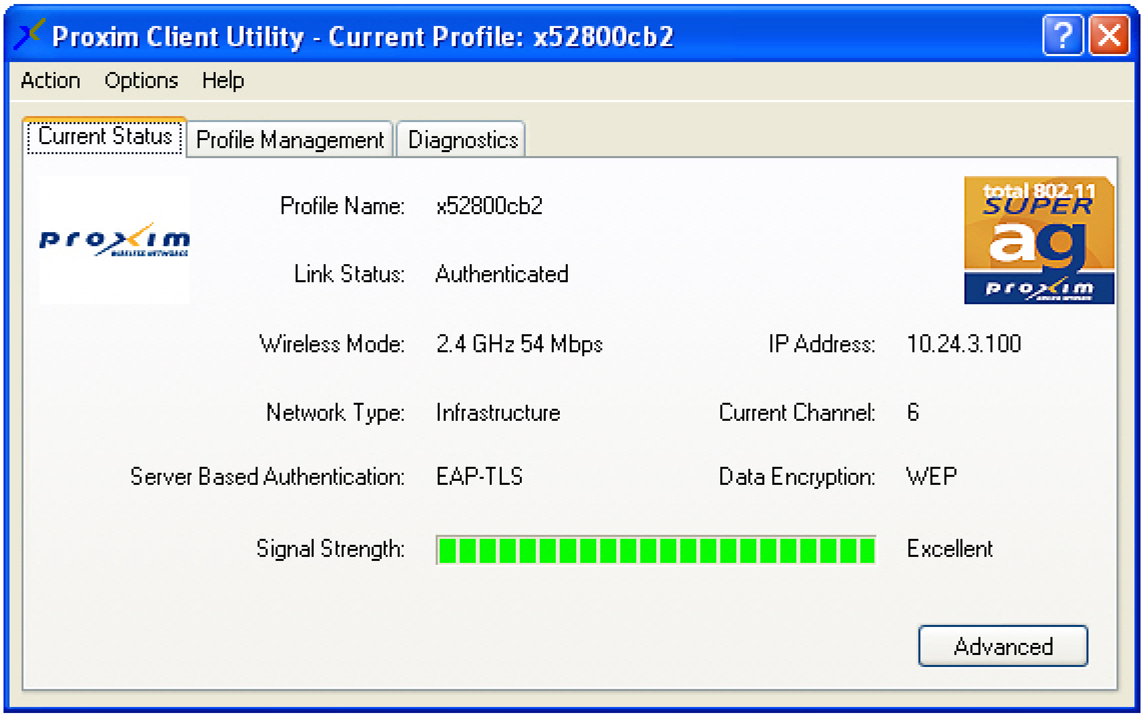
Server Properties: Samcorp Authority

Server/Domain Name: samcorp.com

Login Name: juser

Figure 6.19 – Define Certificate

e. Verify wireless client authentication and IP addressing using the Proxim Client Utility.



Proxim Client Utility - Current Profile: x52800cb2

Profile Name: x52800cb2

Link Status: Authenticated

Wireless Mode: 2.4 GHz 54 Mbps

IP Address: 10.24.3.100

Network Type: Infrastructure

Current Channel: 6

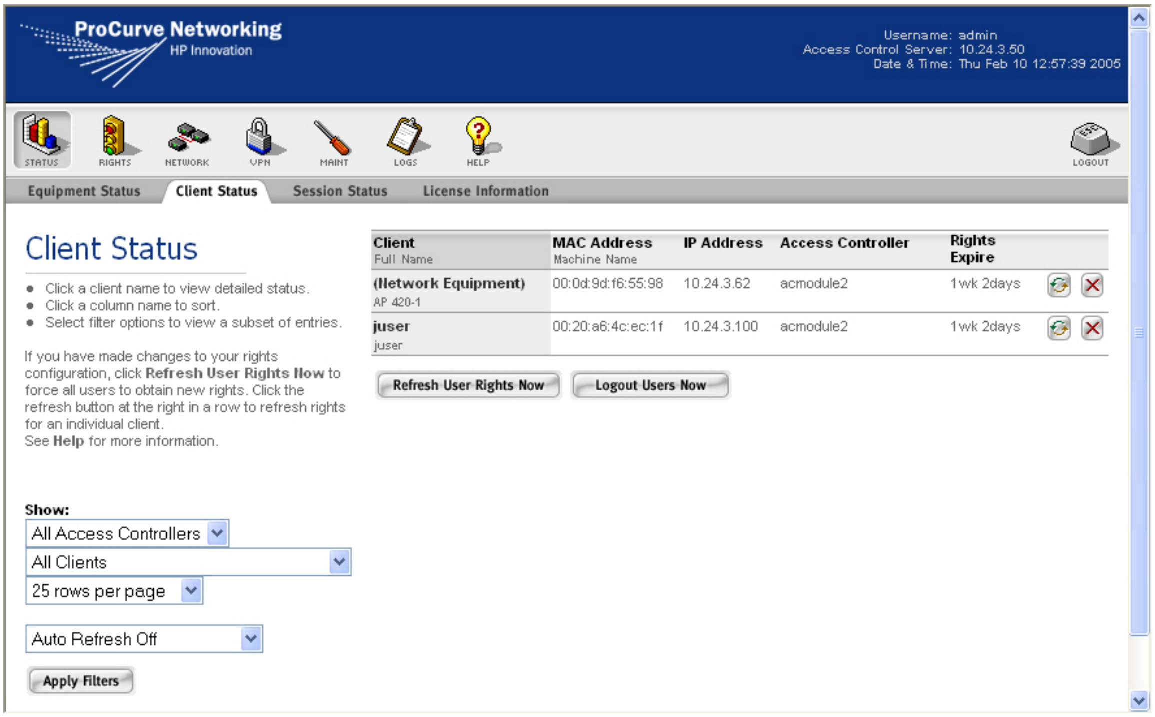
Server Based Authentication: EAP-TLS

Data Encryption: WEP

Signal Strength: Excellent

Figure 6.20 – Proxim Client Utility

f. On the ACS Management interface, verify successful authentication by browsing to Status -> Client Status.



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Feb 10 12:57:39 2005

Client Status

- Click a client name to view detailed status.
- Click a column name to sort.
- Select filter options to view a subset of entries.

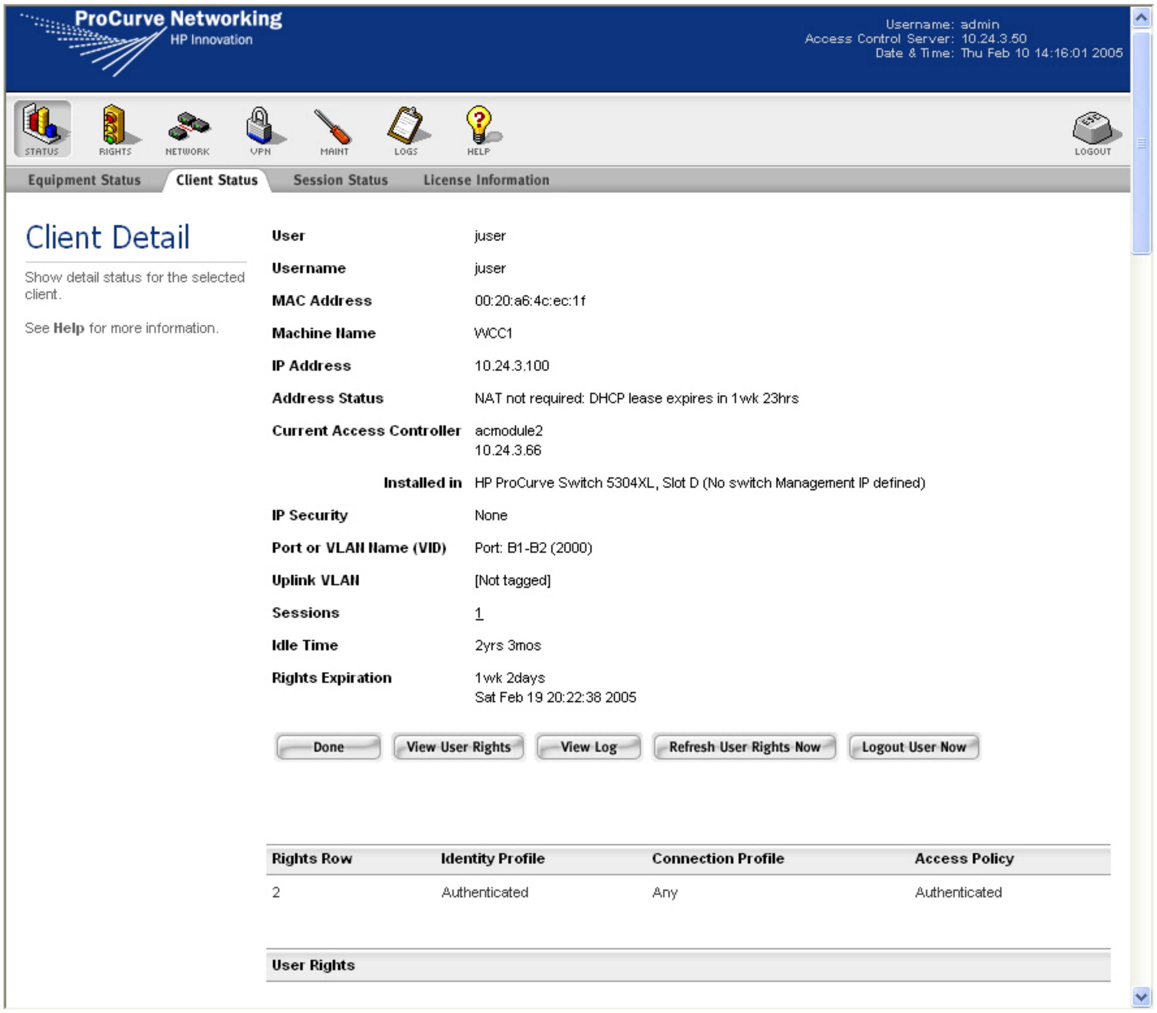
If you have made changes to your rights configuration, click **Refresh User Rights Now** to force all users to obtain new rights. Click the refresh button at the right in a row to refresh rights for an individual client.
See **Help** for more information.

Client Full Name	MAC Address Machine Name	IP Address	Access Controller	Rights Expire
(Network Equipment) AP 420-1	00:0d:9d:f6:55:98	10.24.3.62	acmodule2	1wk 2days
juser juser	00:20:a6:4c:ec:1f	10.24.3.100	acmodule2	1wk 2days

Show:
All Access Controllers
All Clients
25 rows per page

Auto Refresh Off

Figure 16.21 – Client Status



Username: admin
Access Control Server: 10.24.3.50
Date & Time: Thu Feb 10 14:16:01 2005

Client Detail

Show detail status for the selected client.

See **Help** for more information.

User	juser
Username	juser
MAC Address	00:20:a6:4c:ec:1f
Machine Name	WCC1
IP Address	10.24.3.100
Address Status	NAT not required: DHCP lease expires in 1wk 23hrs
Current Access Controller	acmodule2 10.24.3.66
Installed in	HP ProCurve Switch 5304XL, Slot D (No switch Management IP defined)
IP Security	None
Port or VLAN Name (VID)	Port: B1-B2 (2000)
Uplink VLAN	[Not tagged]
Sessions	1
Idle Time	2yrs 3mos
Rights Expiration	1wk 2days Sat Feb 19 20:22:38 2005

Rights Row	Identity Profile	Connection Profile	Access Policy
2	Authenticated	Any	Authenticated

User Rights

Figure 6.22 – Client Detail

To find out more about ProCurve Networking products and solutions, visit our Web site at

www.procurve.com

ProCurve Networking
HP Innovation

March 2005