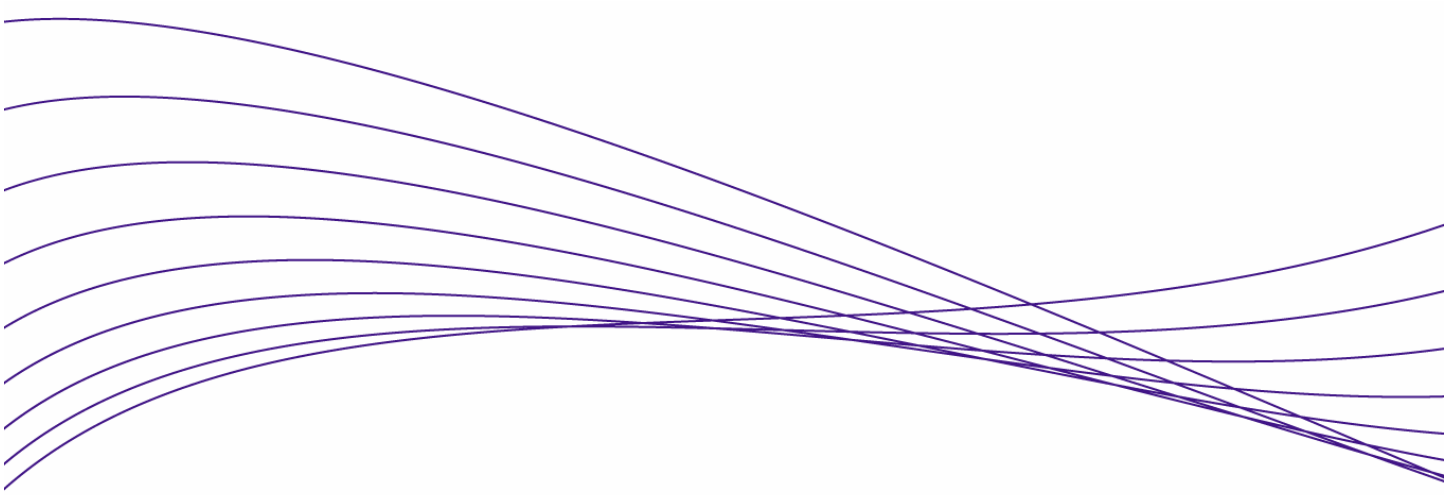
ProCurve Networking

Secure Access Configuration Guide For Wireless Clients

Part One: Browser-based Logon



Secure Access Configuration Guide For Wireless Clients

Introduction

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

tThe 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 One 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.

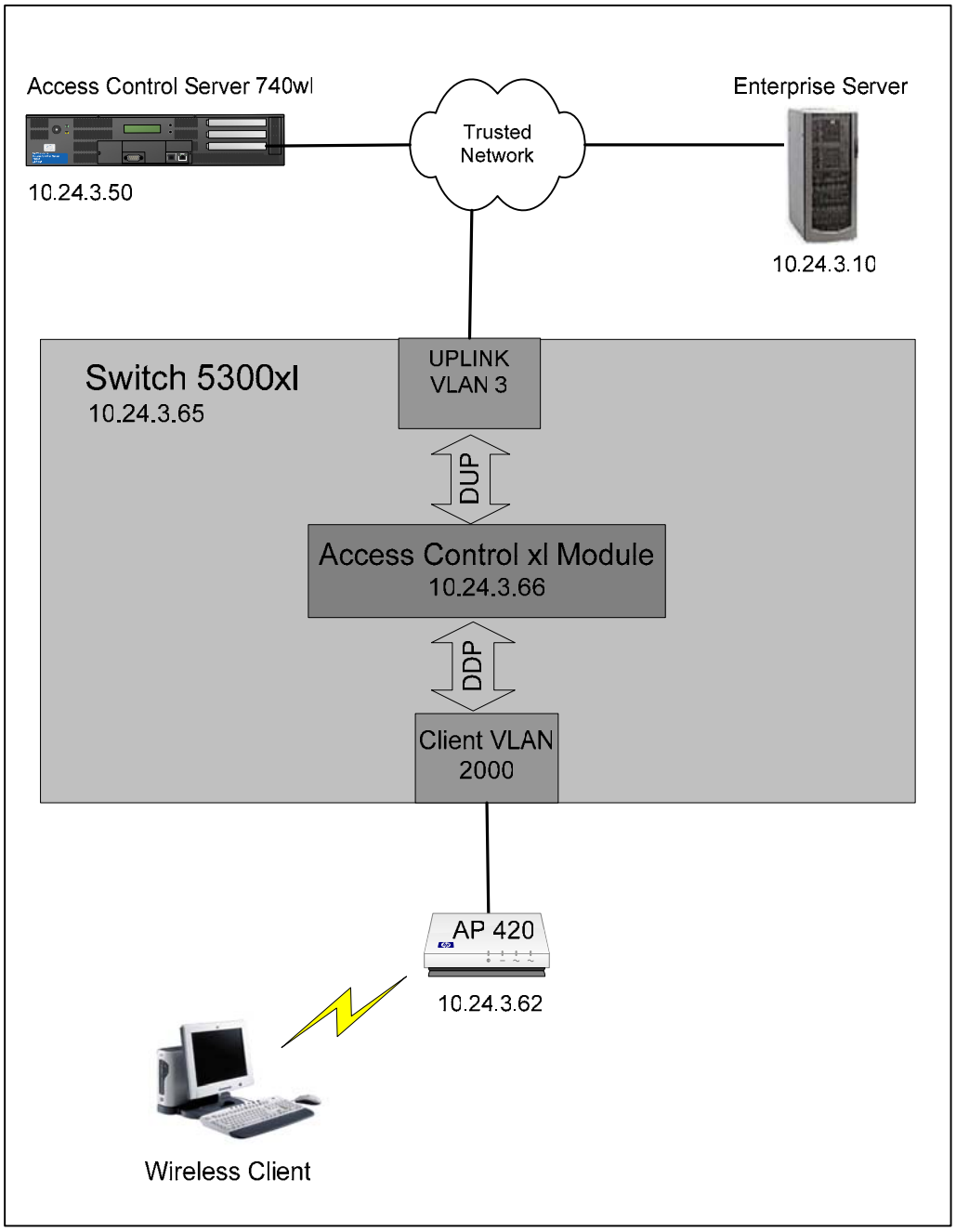


Figure A – Basic Topology

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. Configuring the Access Point for general network and wireless
   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. <u>Configuring the ACS to recognize the AP 420 as "Network Equipment"</u>
   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.

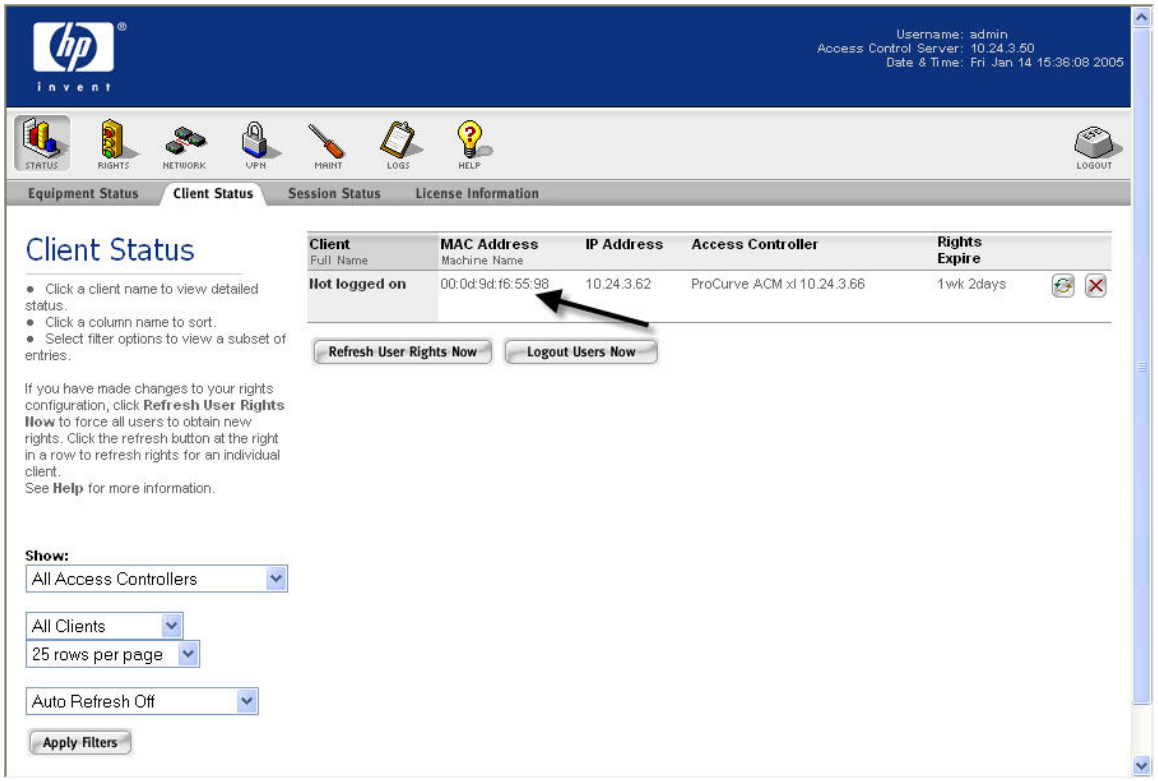


Figure B – Client Status Page

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.

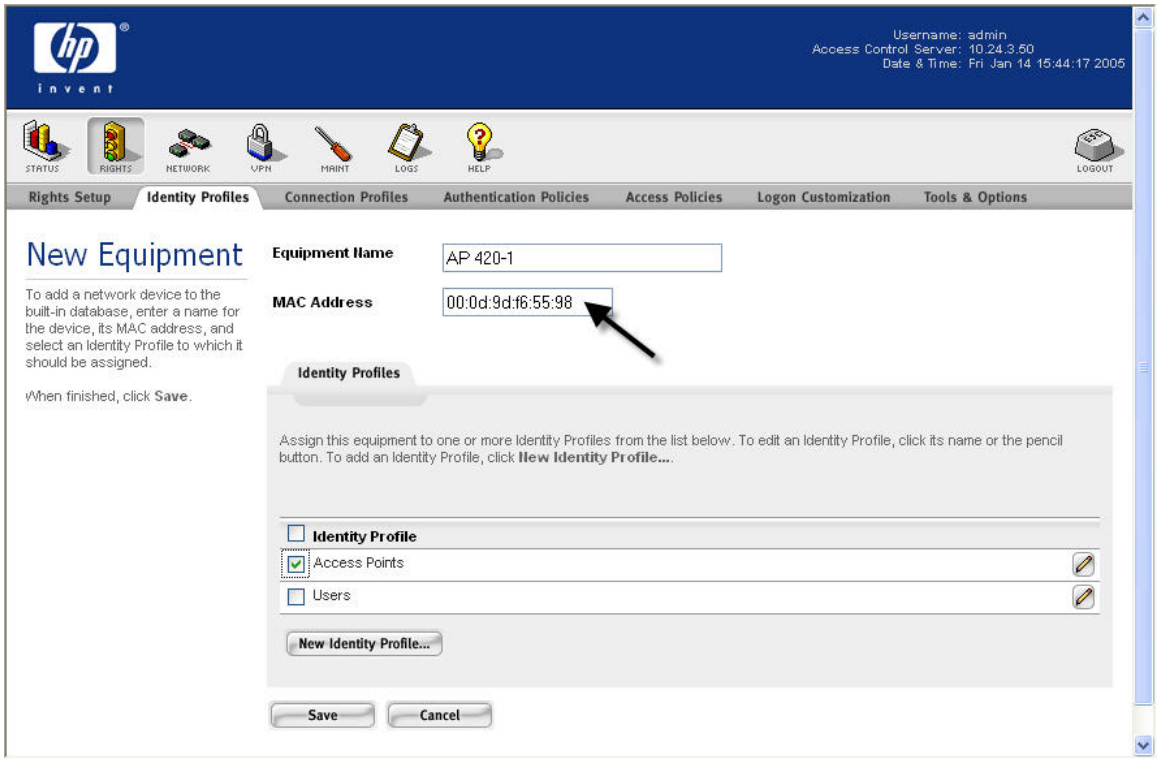


Figure C – New Equipment Page

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

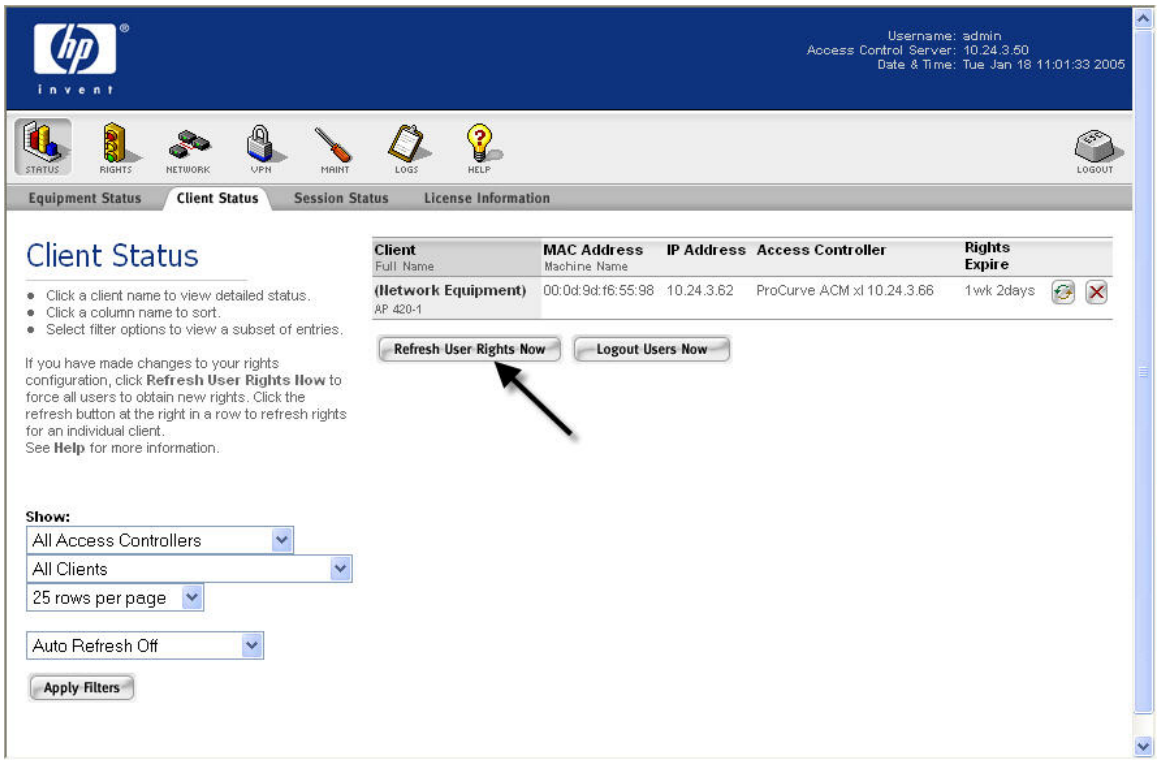


Figure C – Client Status - Refresh User Rights Now

Configuring Scenario 1: Browser-based Logon using Built-in Database Authentication

Scenario 1 consists of a wireless, Static WEP, Windows XP client authenticating to the built-in database of the Access Control Server. The tasks required are:

- On the ACS, create a new User and Identity Profile in the built-in database for authentication.
- On the AP 420, configure Static WEP wireless parameters.
- Connect Windows XP Client, logon using browser-based logon and verify authentication.

1) **Create a New User and Identity Profile in the Access Control Server Database.**
   a. Using the ACS Web browser interface, browse to Rights -> Identity Profiles and select Users. Click the **New User** button.
   b. Add a new user (`juser`) and select a password (`password`) and save changes. Do not add the new user to any identity profile yet.

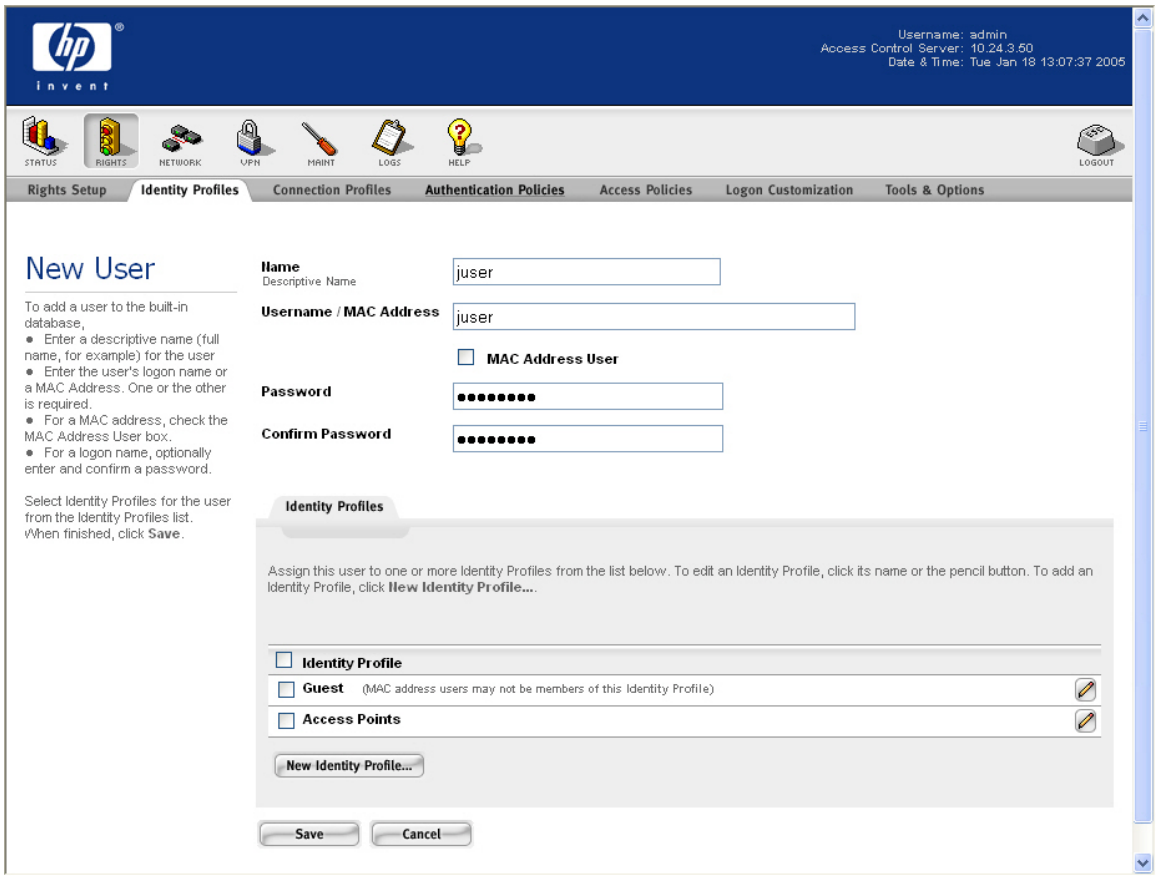


Figure 1.1 –New User Page

c. To create a new Identity Profile, browse to Rights -> Identity Profiles and select the **New Identity Profile** button. Select a name for the Identity Profile (`Users`) and save changes.

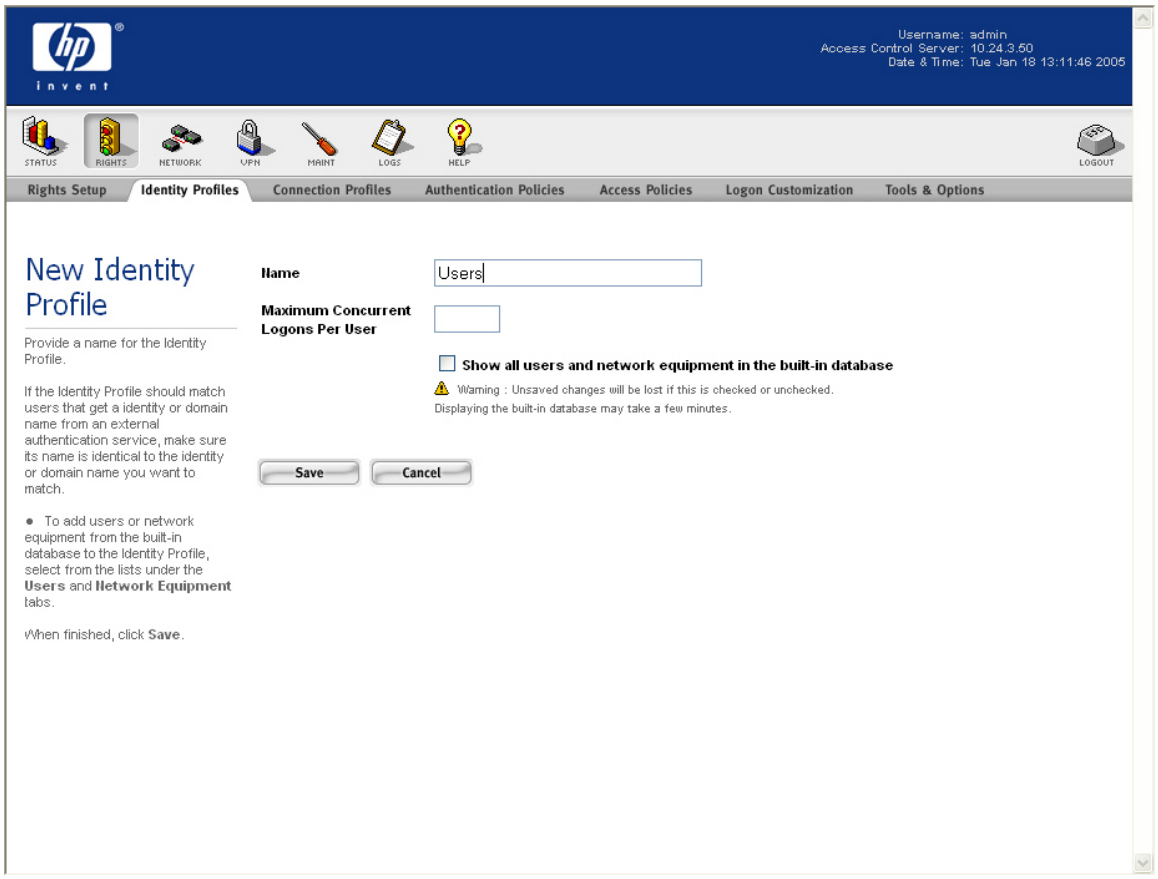


Figure 1.2 –New Identity Profile

d. Browse back to Rights -> Identity Profiles -> Users and select the new user you created above (`juser`) and add this user to the new identity profile (`Users`). Save changes.

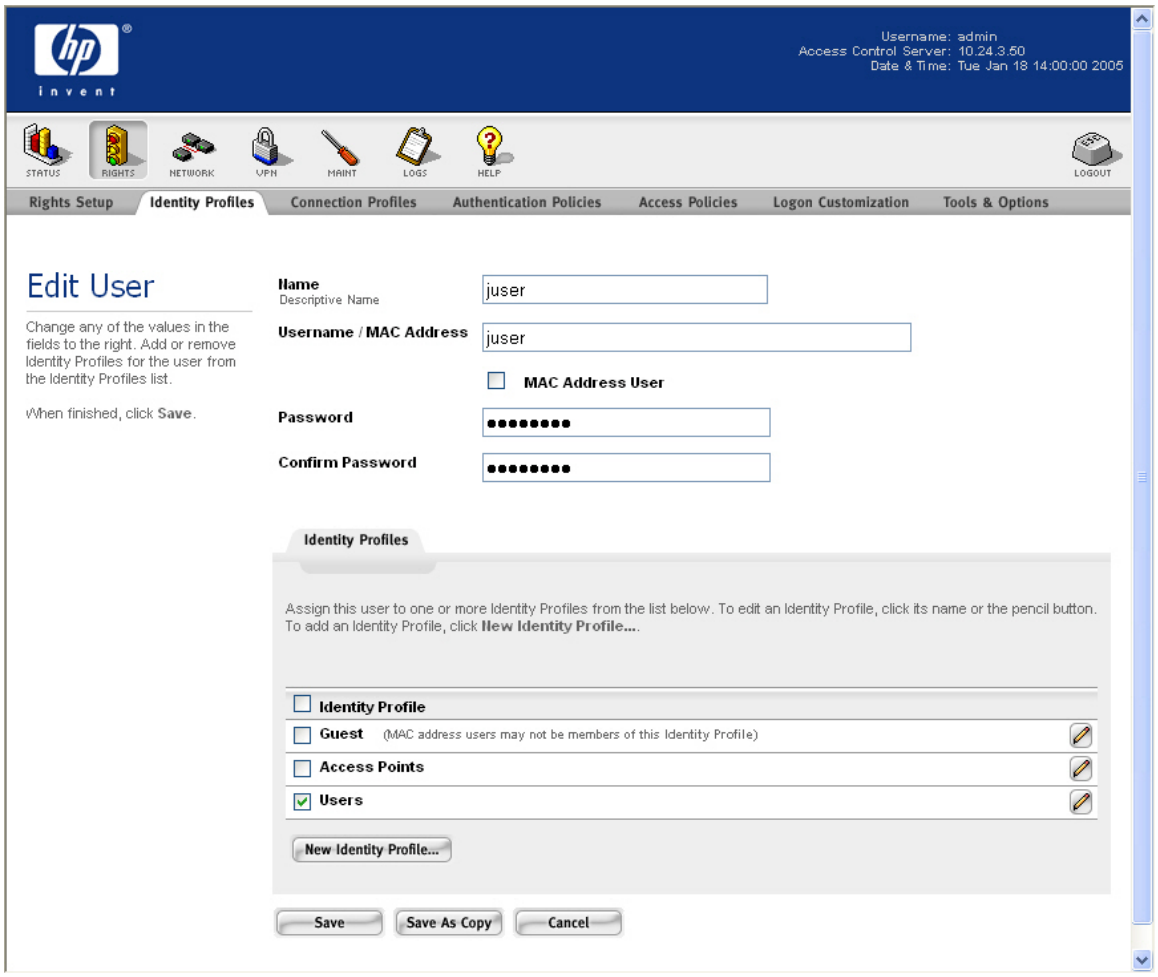


Figure 1.3 – Edit User Page

e. To create a new entry in the Rights Assignment table, browse to Rights and click the **New Rights Assignment** button. From the drop-down menus, choose the newly created Identity Profile (`Users`), a Connection Profile (`Any`) and an Access Policy (`Authenticated`). Configure the New rights Assignment as Row 1 and save changes.

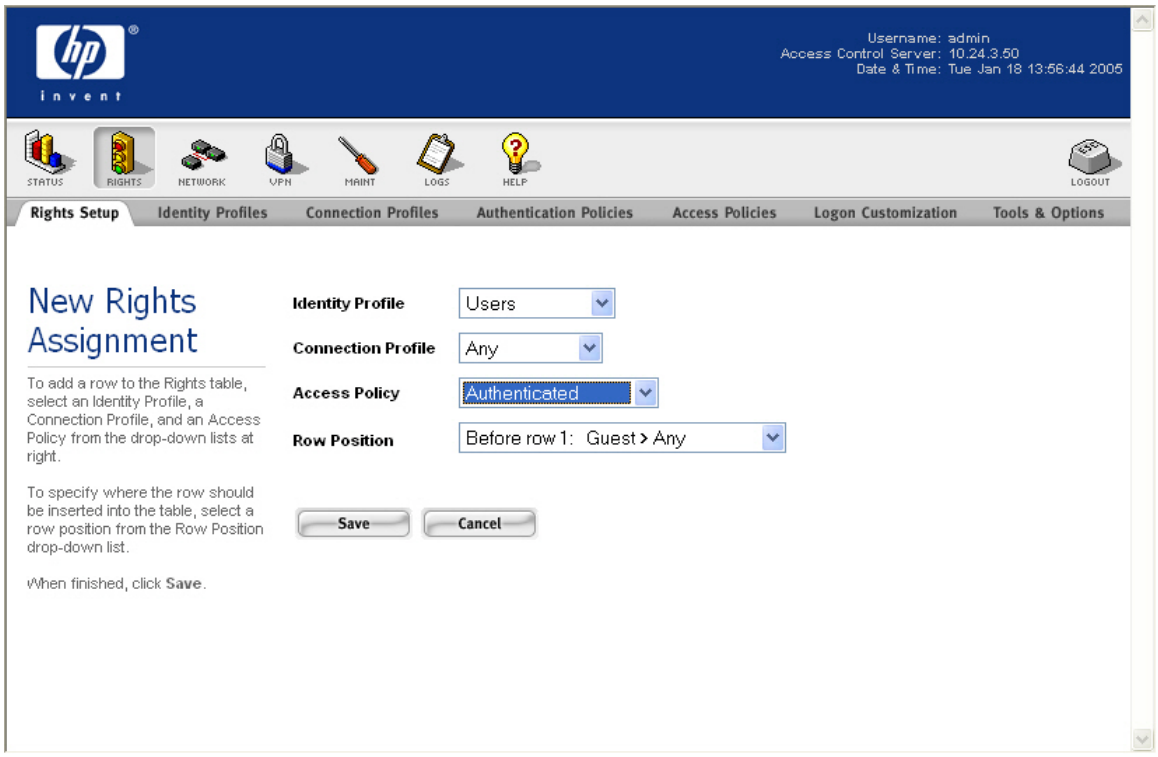


Figure 1.4 – New Rights Assignment

f. Browse to Status -> Client Status and click Refresh User Rights Now.

2) Configure Static WEP parameters on the AP 420.

a. From the AP 420 CLI, configure the Static WEP security suite, WEP key and key length.

```
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 2
HP ProCurve Access Point 420(if-wireless g)# wep-key 1 ascII
1111111111333
HP ProCurve Access Point 420(if-wireless g)# key-length-wep 128
```

3) Connect Windows XP Client, logon using browser-based logon and verify authentication.

a. Connect the wireless Windows XP client to the AP 420 using the Static WEP key.
b. Open a Web browser on the client. The 700wl logon page will appear. (You may need to configure the browser to accept all cookies).
c. Enter the username (`juser`) and password (`password`) and click the Logon User button.

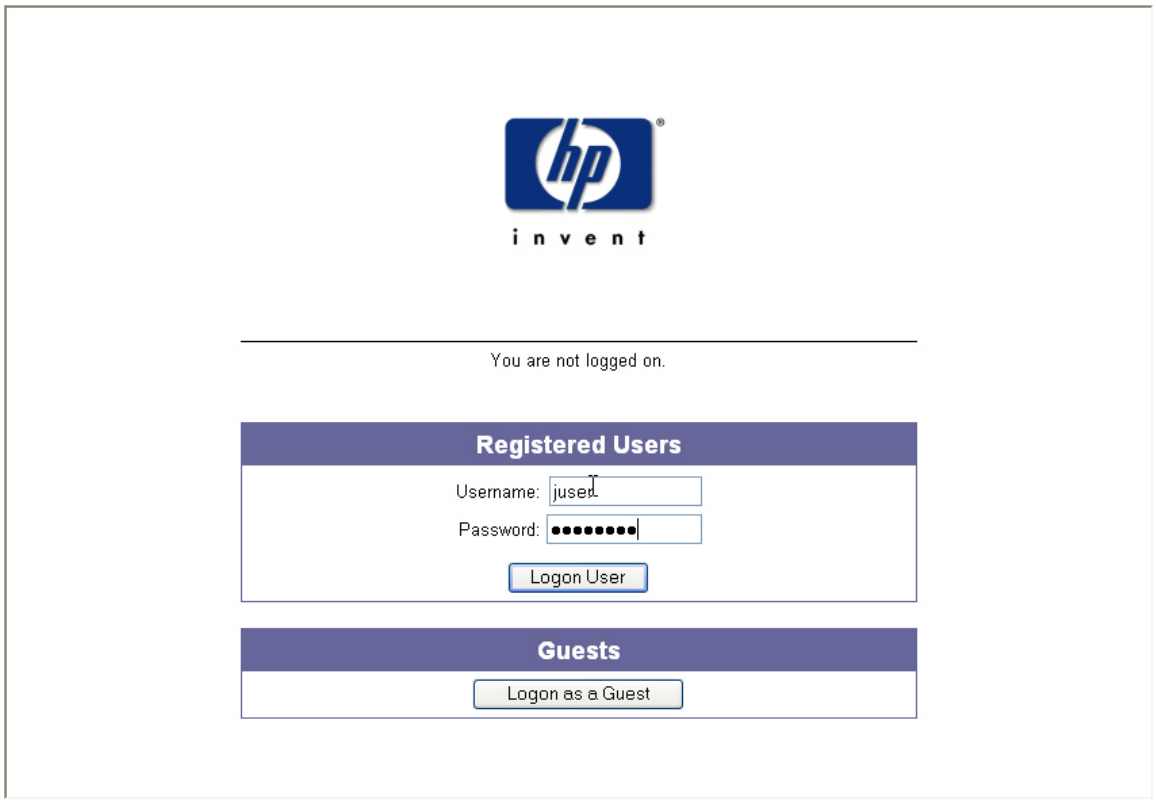


Figure 1.5 – Logon Page

d. 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 and authenticated.

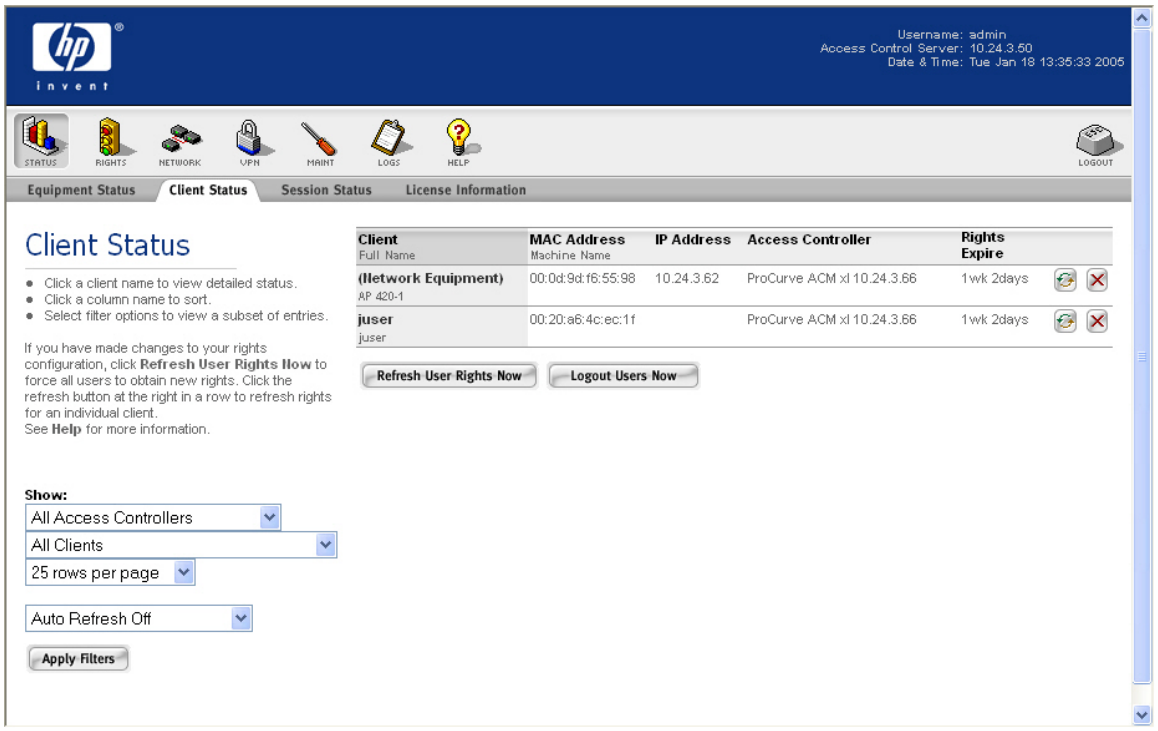


Figure 1.6 – Client Status Page

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

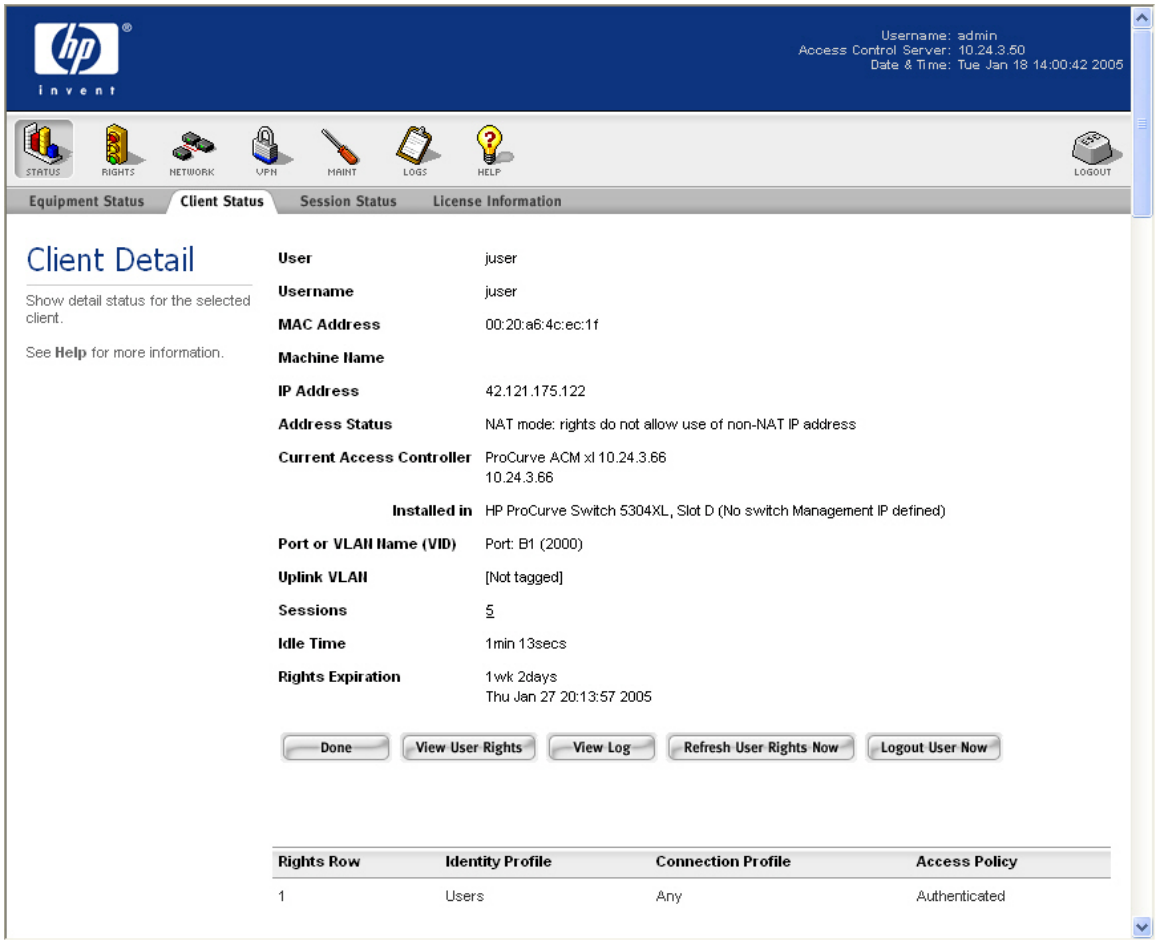


Figure 1.7 –Client Details Page

Configuring Scenario 2: Browser-based Logon using LDAP Authentication

Scenario 2 consists of a wireless, WPA-PSK, Windows XP client authenticating to an LDAP database. In this example, we will configure the ACS to authenticate users against Windows Active Directory (which is an LDAP database) and interpret group affiliation returned by the server as the user's Identity Profile. The steps required are:

- On the Enterprise Server, create a user account in Active Directory and associate it with a group.
- On the ACS, define an LDAP Authentication Service and add it to the System Authentication Policy.
- On the ACS, configure the Authenticated Access Policy to allow clients to use Real IP addresses (via DHCP).
- On the AP 420, configure WPA-PSK wireless parameters.
- Connect Windows XP Client, logon using browser-based logon and verify authentication.

1) **On the Enterprise Server, create a user account in Active Directory and associate it with a group.**
Note: In this example, the Enterprise Server is configured as a Domain Controller named "samcorp.com".

a. To create a user on the Enterprise Server, open Directory Users & Computers (Start → Administrative Tools → Active Directory Users and Computers).

- Right Click on samcorp.com → Users.
- Select New → **User**.

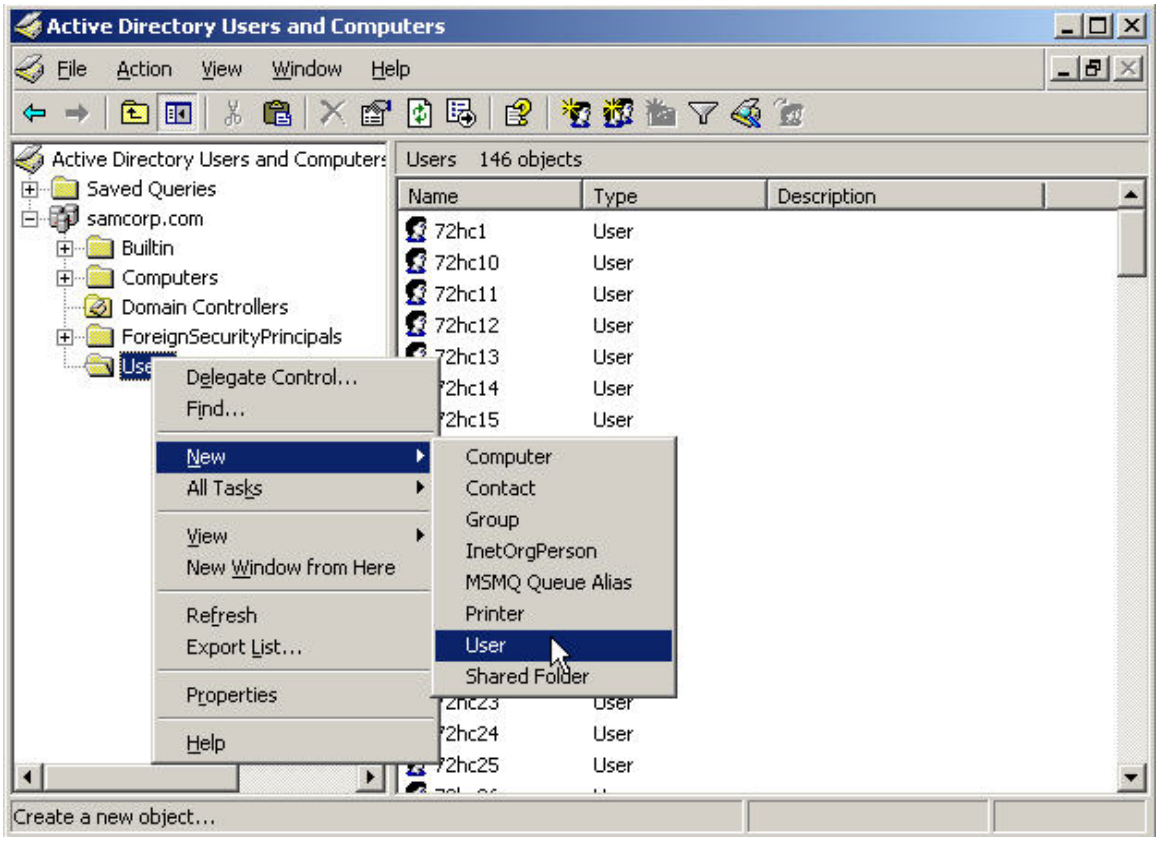


Figure 2.1 - Active Directory Users and Computers

- In the First name field enter Joe.
- In the Last name field enter User.
- In the User logon name field enter **juser** and select Next.

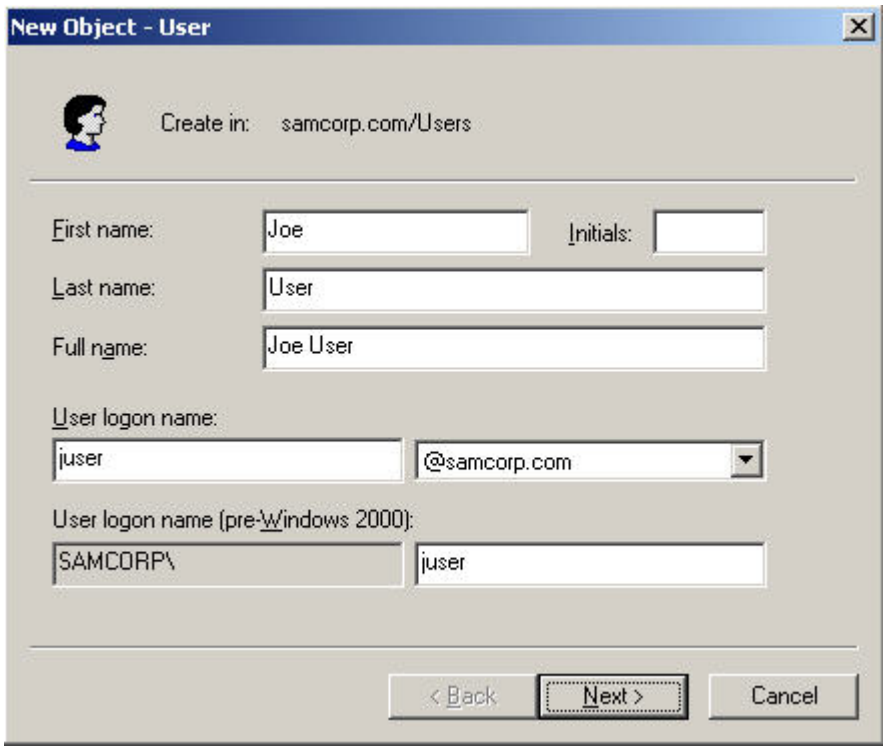


Figure 2.2 - New Object - User

- **Deselect** User must change password at next logon.
- In the password field enter "**password**".
- In the confirm password field enter "**password**" and select Next.
- Select Finish at the User summary page.

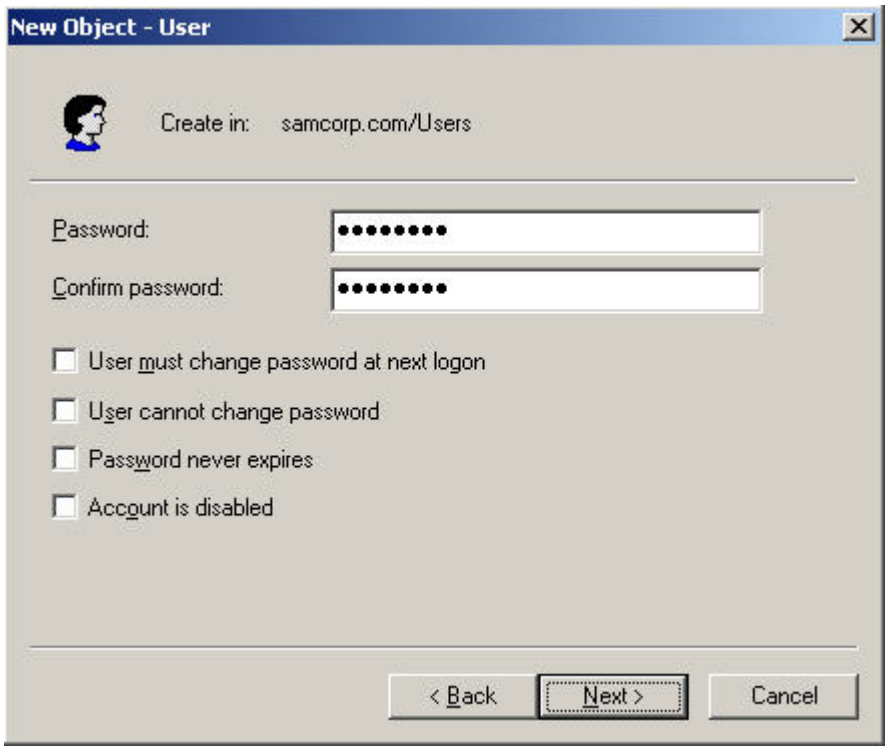


Figure 2.3 - New Object – User Password

- Highlight the newly created user.
- Right Click and Select **properties**.

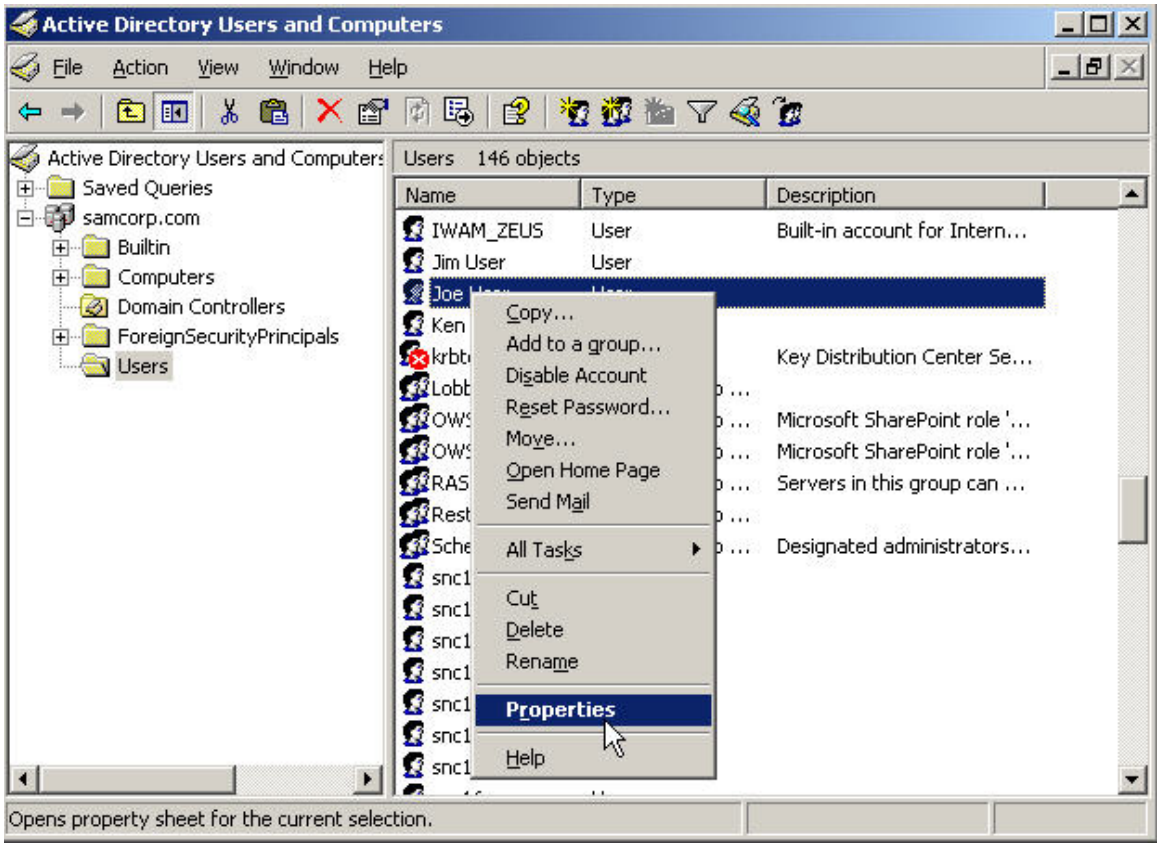


Figure 2.4 - User Properties

- In the Account tab, enable the box next to "**store passwords using reversible encryption**" in the Account options area.

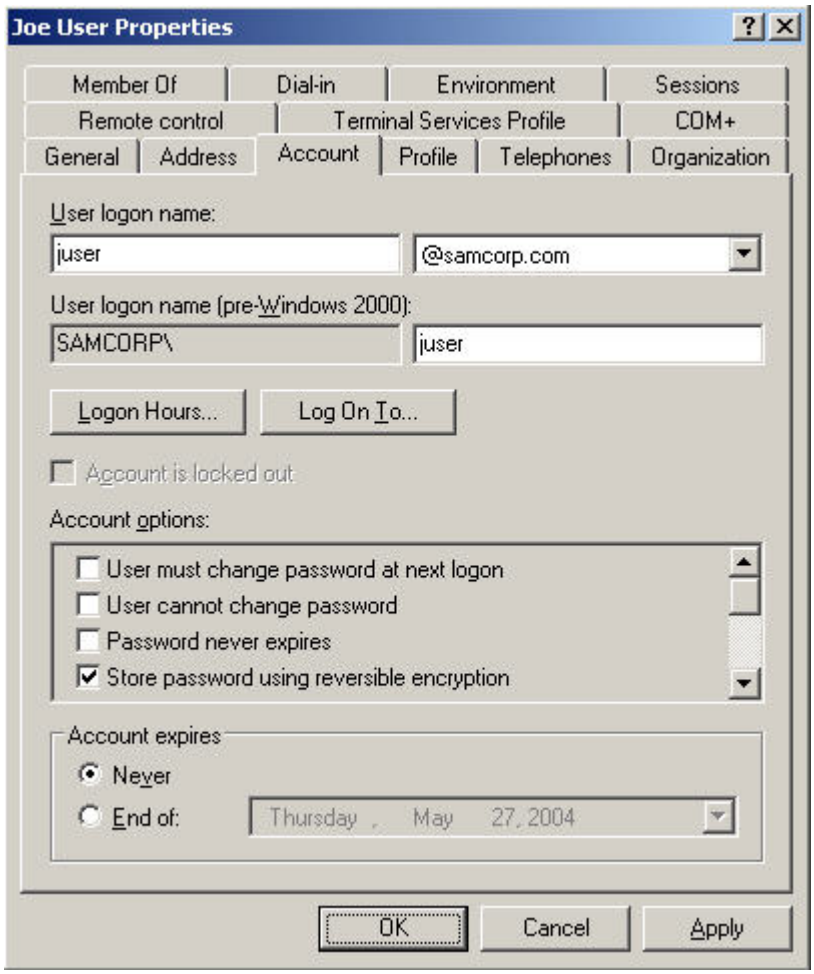


Figure 2.5 - User Properties – Account

- In the Dial-in tab, select "**Allow access**".
- Select OK.

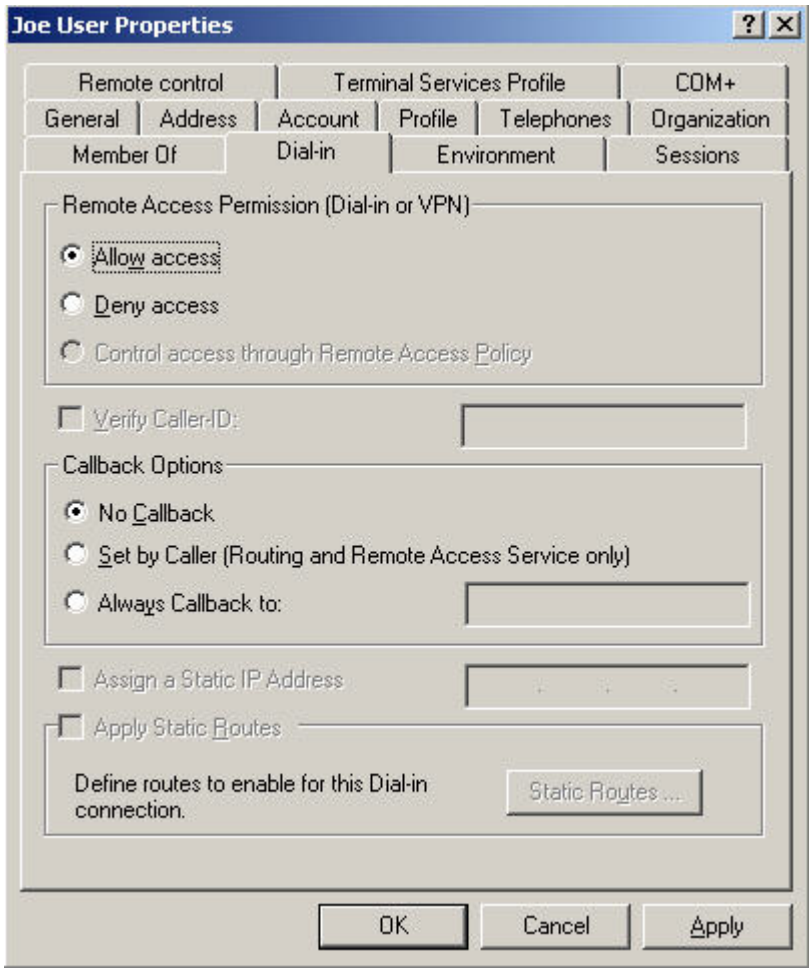


Figure 2.6 - User Properties – Dial-in

b. To create a group on the Enterprise Server for authenticated users, open **Directory Users & Computers** (Start → Administrative Tools → Active Directory Users and Computers).

- Right-click on Users and select New → **Group.**

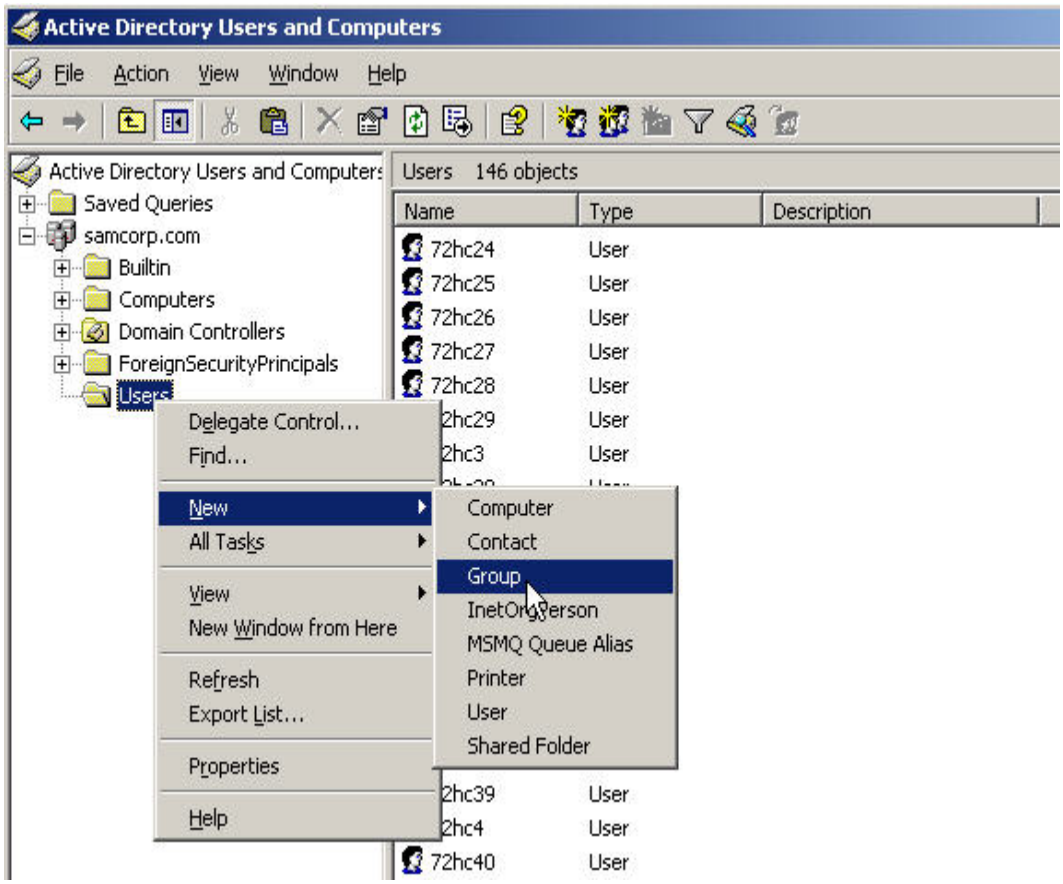


Figure 2.7 - New Group

- Enter **Authorized_Users** in the Group name text box.
- Make sure **Global** is selected for the Group scope and **Security** is selected for the Group type and press OK.

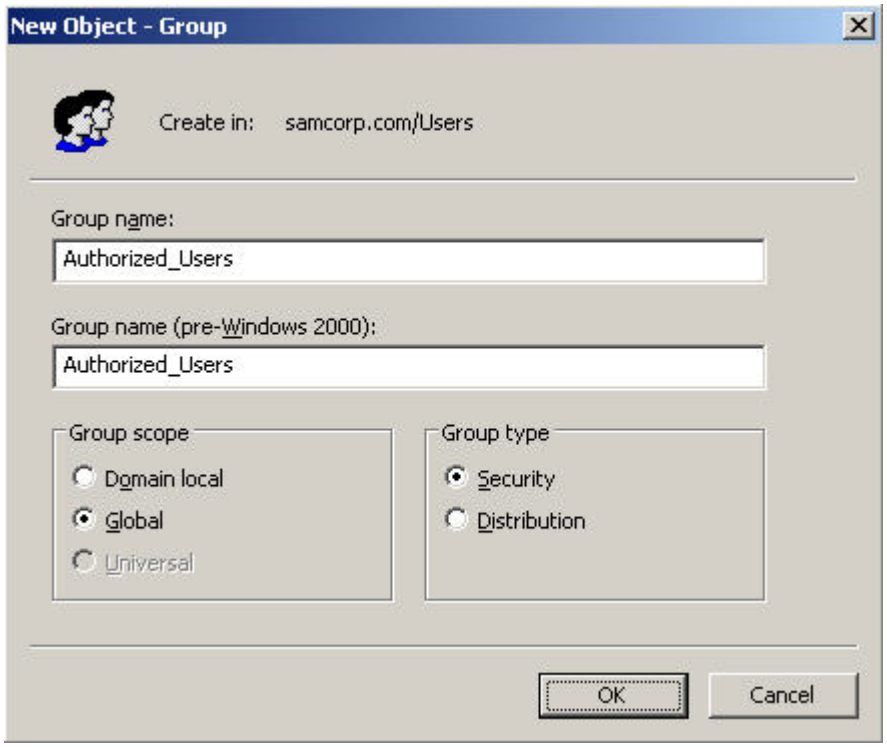


Figure 2.8 - New Object – Group

- Right-click on the user we created earlier (Joe User) and select **properties**.
- Select the **Member Of** tab and press the **Add** button.

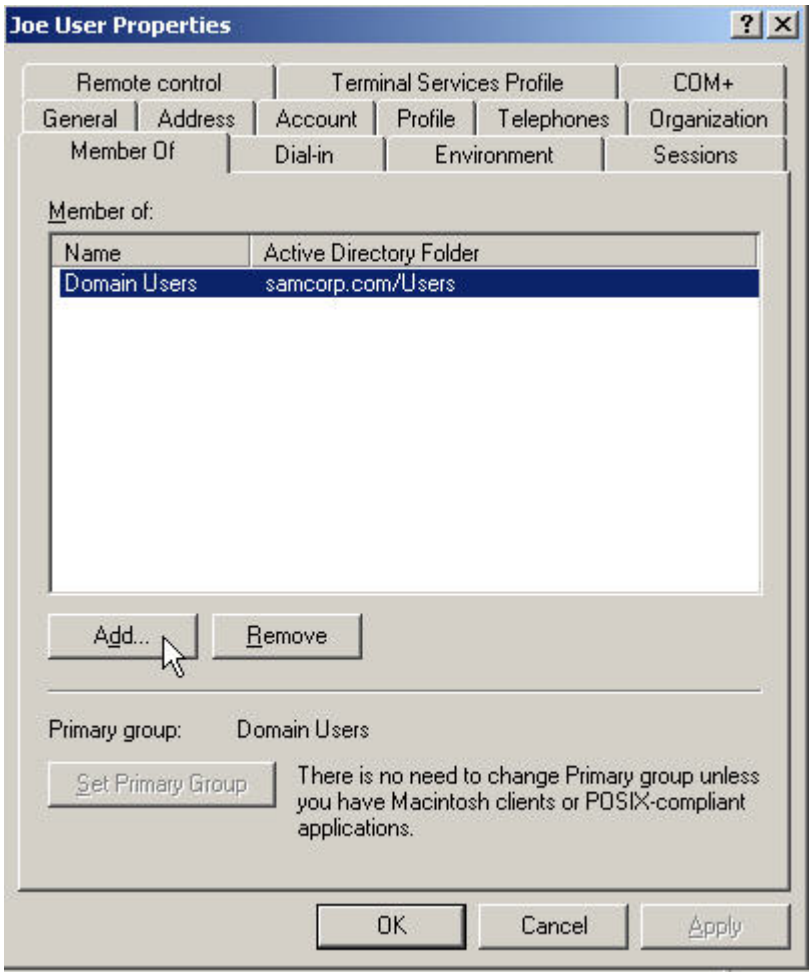


Figure 2.9 - Joe User Properties – Member Of

- In the "Enter the object names to select" text box enter "**Authorized_Users**" and select the Check Names button.

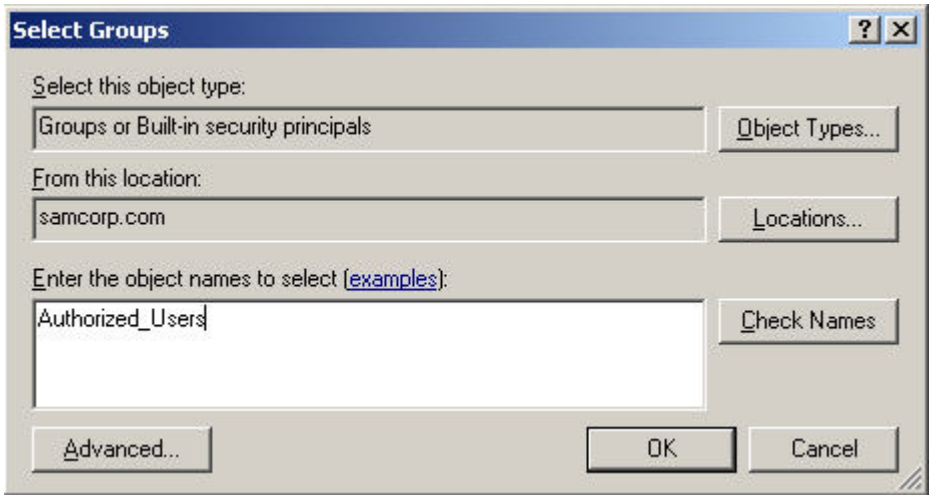


Figure 2.10 - Select Groups

- The group name will be validated and should show underlined. Press the OK button.

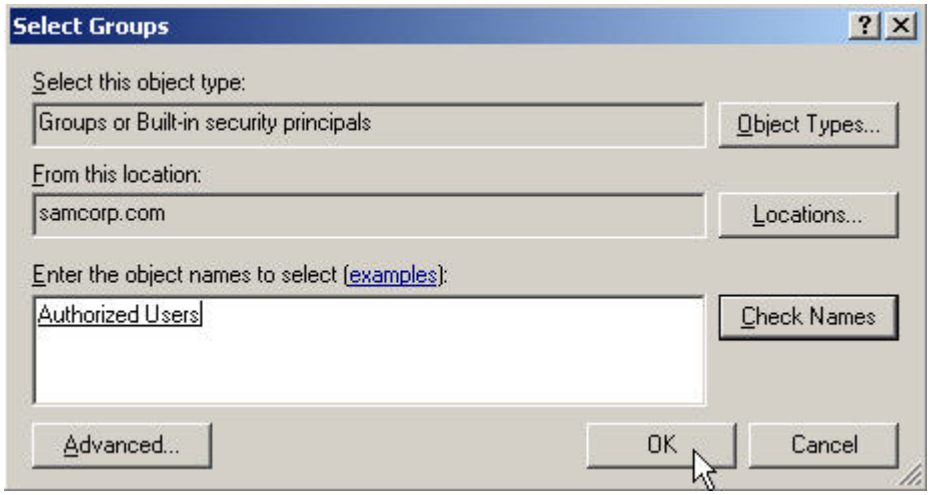


Figure 2.11 - Select Groups Validated

- The group should now show up in the Member Of box. Press the OK button to apply the changes.
- Press Alt-F4 to close the Active Directory Users and Computers Window.

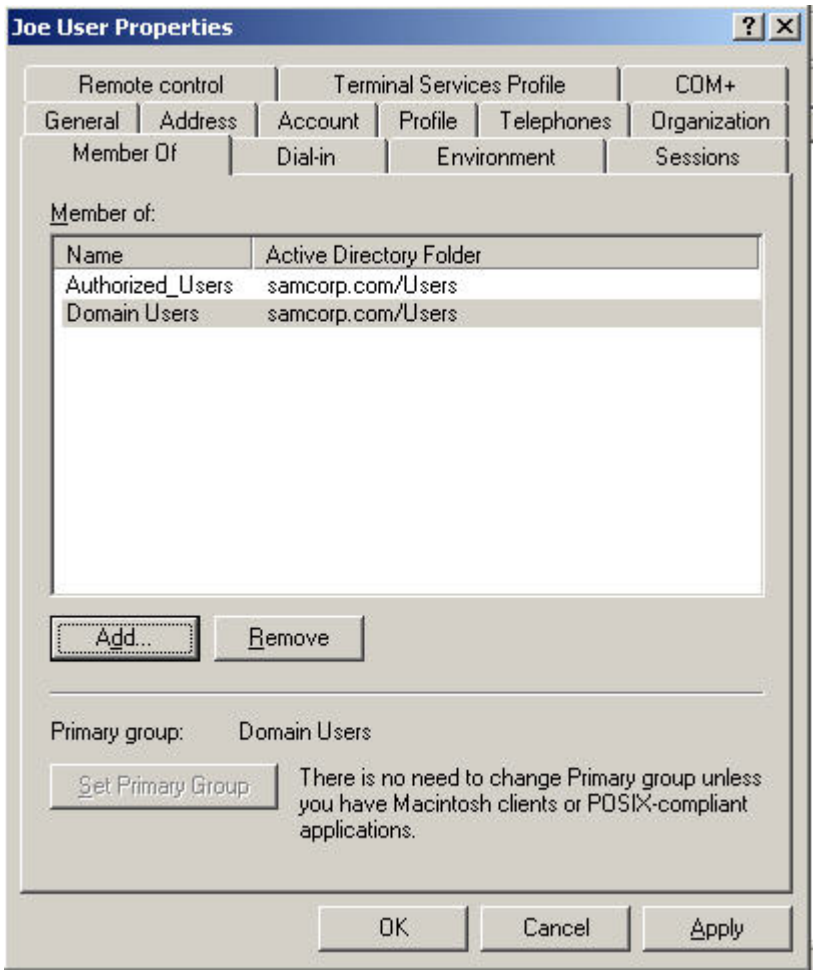


Figure 2.12 - Joe User Properties – Group Added

2) **On the ACS, define an LDAP Authentication Service and add it to the System Authentication Policy.**

a. On the ACS, browse to Rights -> Authentication Policies and select Authentication Services. Click on New Service. For this example, enter the following information and save changes.

- Name: **Active Directory**
- Server: **10.24.3.10**
- Port: 389
- Base DN: **dc=samcorp,dc=com**
- Username Field: **SAMAccountName**
- Group Identity Field: **memberOf**
- Bind Method: **User Bind**
- User Bind String: **samcorp\%s**

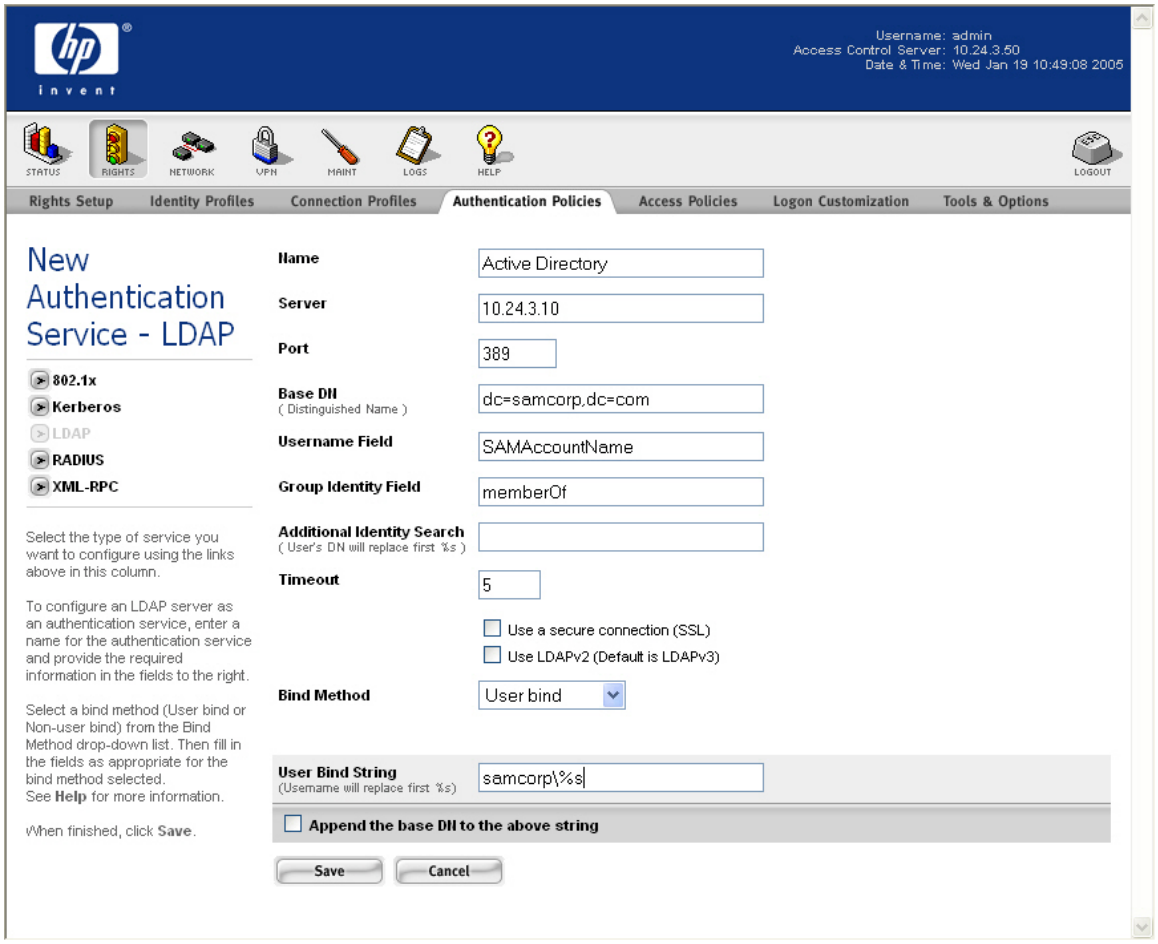


Figure 2.13 – LDAP Authentication Service

b. Browse to Rights -> Authentication Policies and select System Authentication Policy. Add the newly created **Active Directory** Authentication Service by clicking the checkbox and save changes.

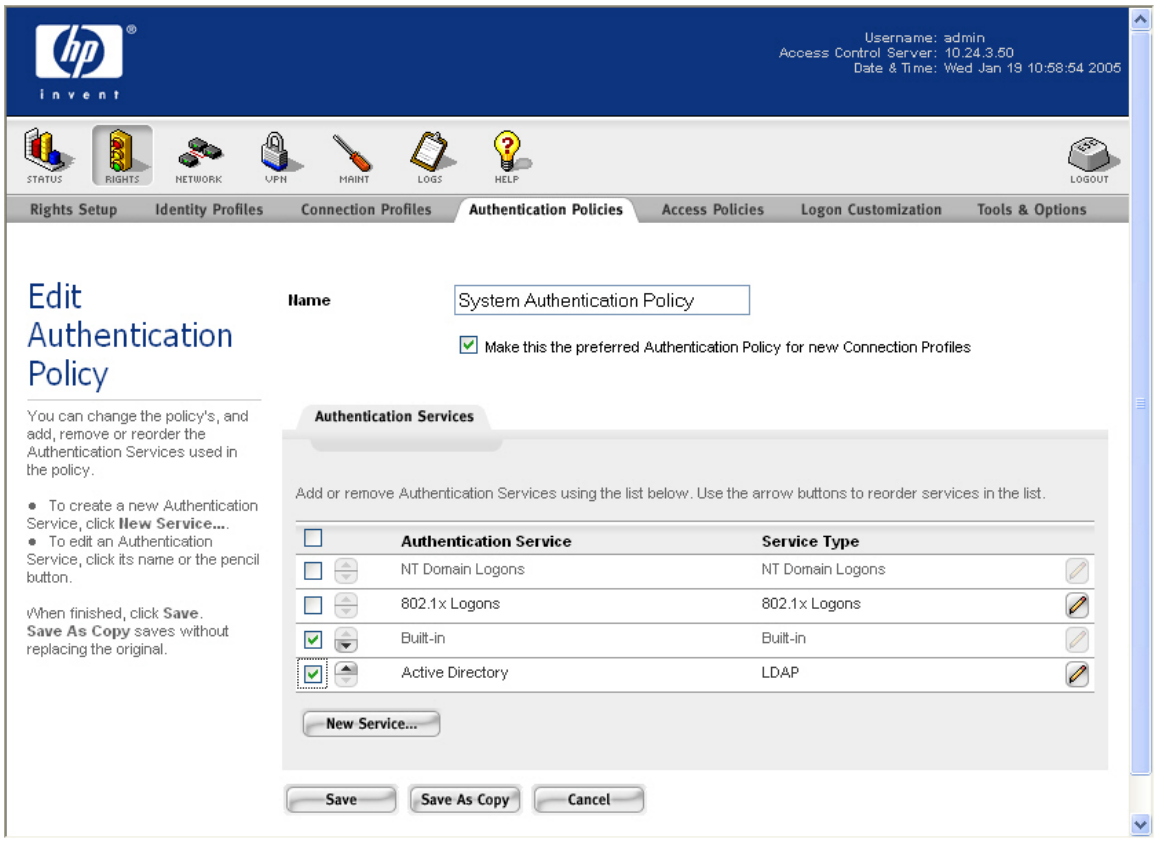


Figure 2.14 – System Authentication Policy

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

a. On the ACS, browse to Rights -> Access Policies and select the **Authenticated** Access Policy. Configure Network Address Translation to **When Necessary** and save changes.

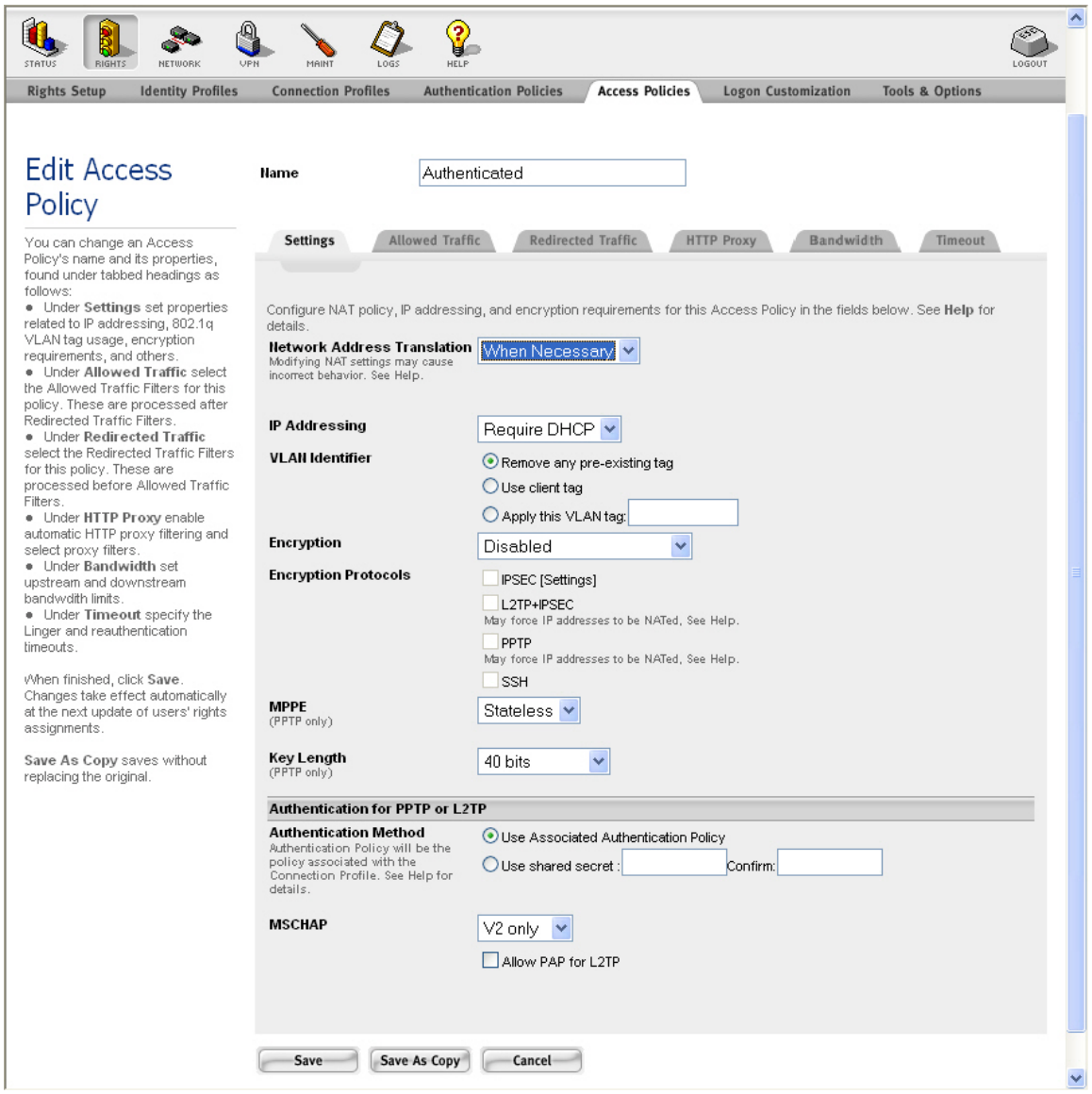


Figure 2.15 – Authenticated Access Policy

b. On the ACS, browse to Network -> Network Setup and select the **Access Control xl Module** (`10.24.3.66`). Enter the **IP address of the DHCP Server** and save changes.

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

4) On the AP 420, configure WPA-PSK wireless parameters.

a. From the AP 420 CLI, configure the WPA-PSK with TKIP security suite and preshared key (`preshared`).

```
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 4
HP ProCurve Access Point 420(if-wireless g)# wpa-preshared-key
ascII preshared
```

5) Connect Windows XP Client, logon using browser-based logon and verify authentication.

a. Connect the wireless Windows XP client to the AP 420 using WPA-PSK.
b. Open a Web browser on the client. The 700wl logon page will appear. (You may need to configure the browser to accept all cookies).
c. Enter the username (`juser`) and password (`password`) and click the Logon User button.

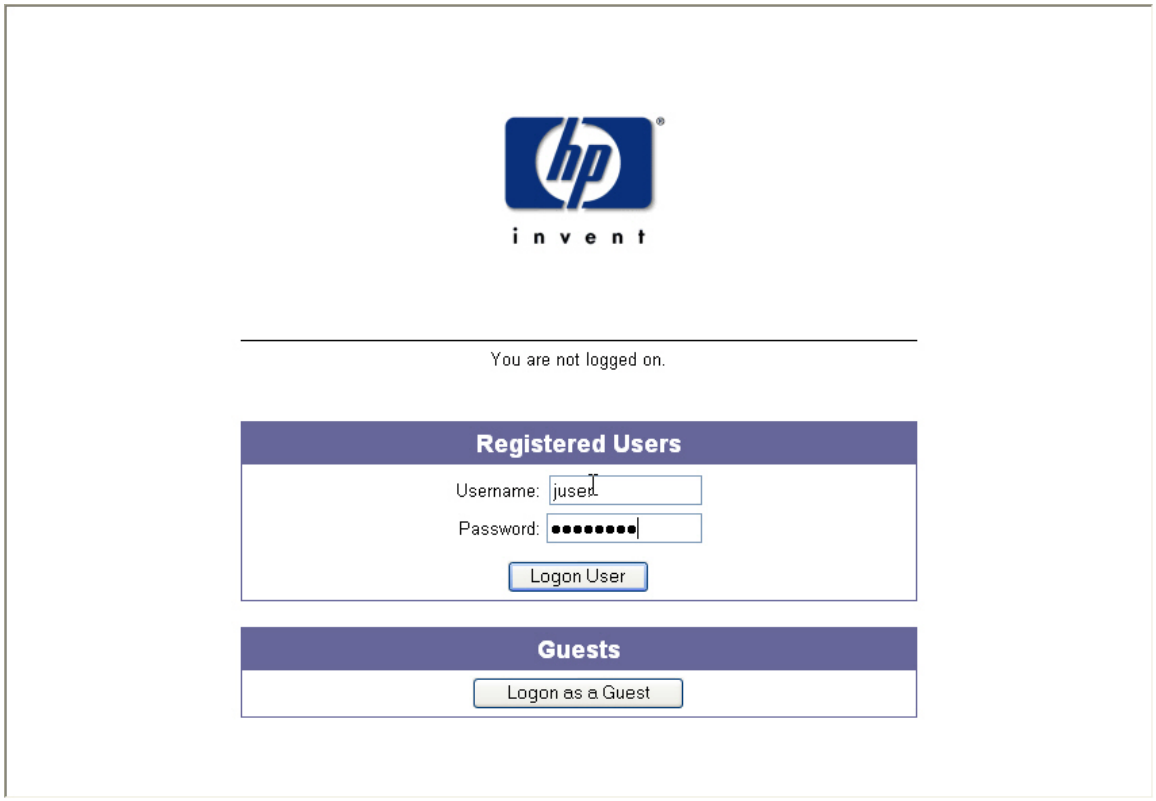


Figure 2.16 – Logon Page

d. 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) and has received a real IP address (via DHCP).

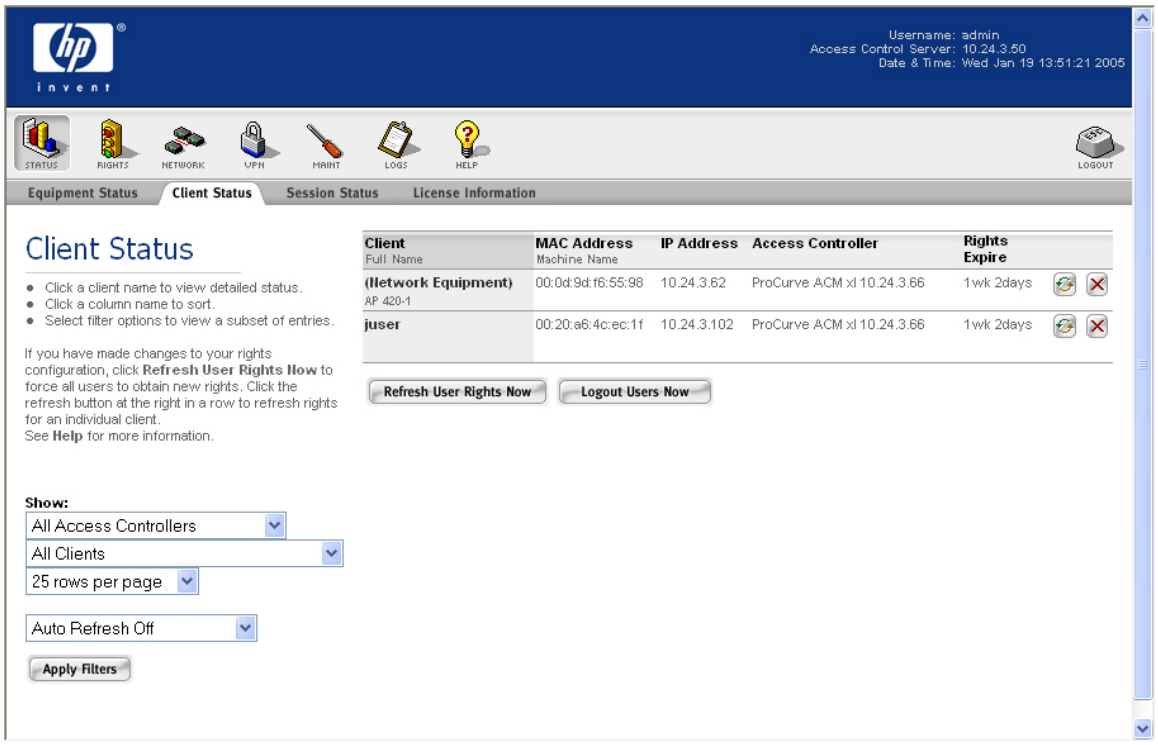


Figure 2.17 – Client Status Page

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

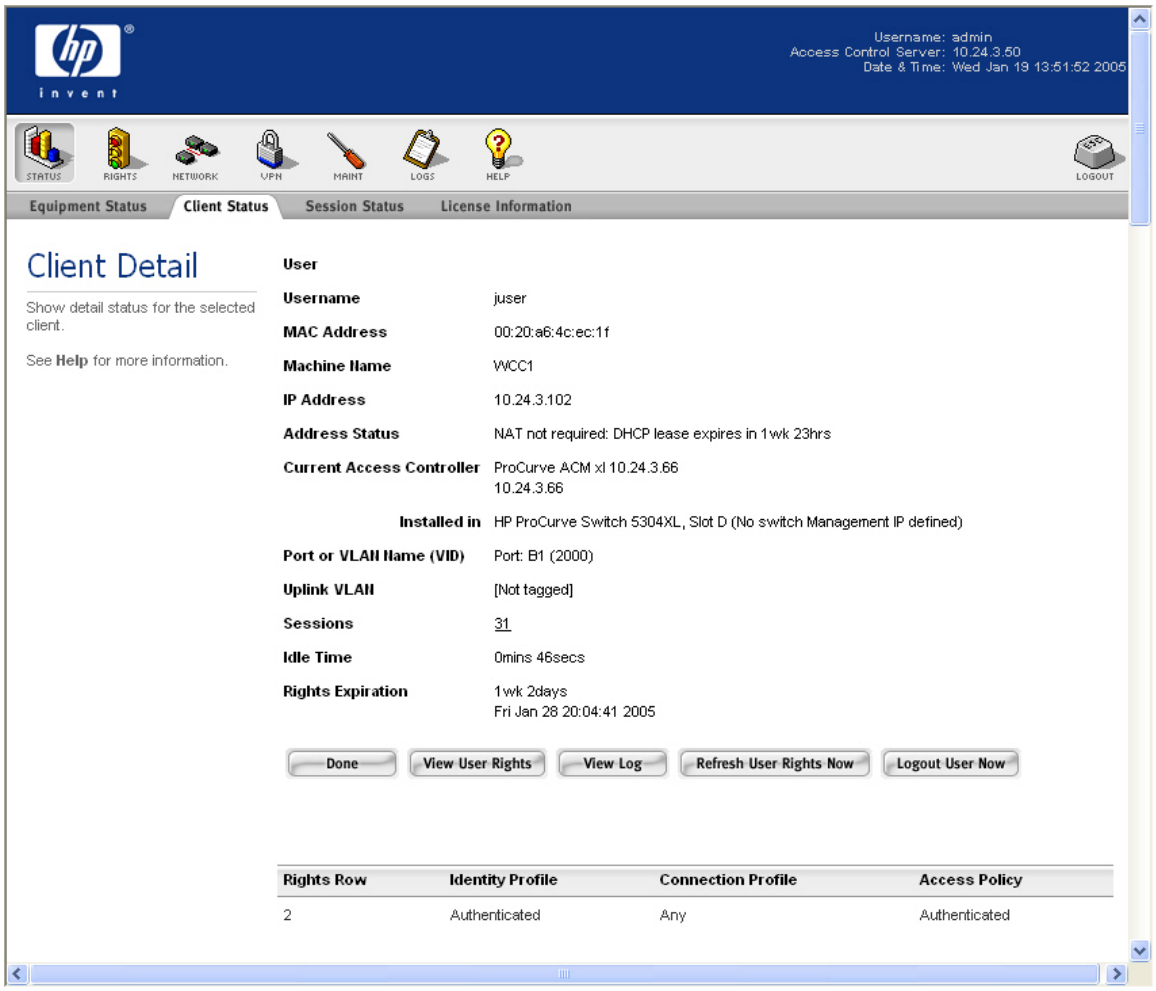


Figure 2.18 – Client Detail Page

Configuring Scenario 3: Browser-based Logon using RADIUS Authentication

Scenario 3 consists of a wireless, Static WEP, Windows 2000 client authenticating via RADIUS. In this example, we will configure the ACS to authenticate users against Internet Authentication Service (IAS), Microsoft's RADIUS implementation, and interpret group affiliation returned by the server as the user's Identity Profile. The steps required are:

Note: Scenario 3 requires that you create a user account in Active Directory and associate it with a group (see Scenario 2 for details).

- On the Enterprise Server, create a new RADIUS client (in this case, the ACS).
- 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, configure the Authenticated Access Policy to allow clients to use Real IP addresses (via DHCP).
- On the AP 420, configure Static WEP wireless parameters.
- Connect Windows 2000 Client, logon using browser-based logon and verify authentication.

1) **On the Enterprise Server, create a new RADIUS client.**
   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**.

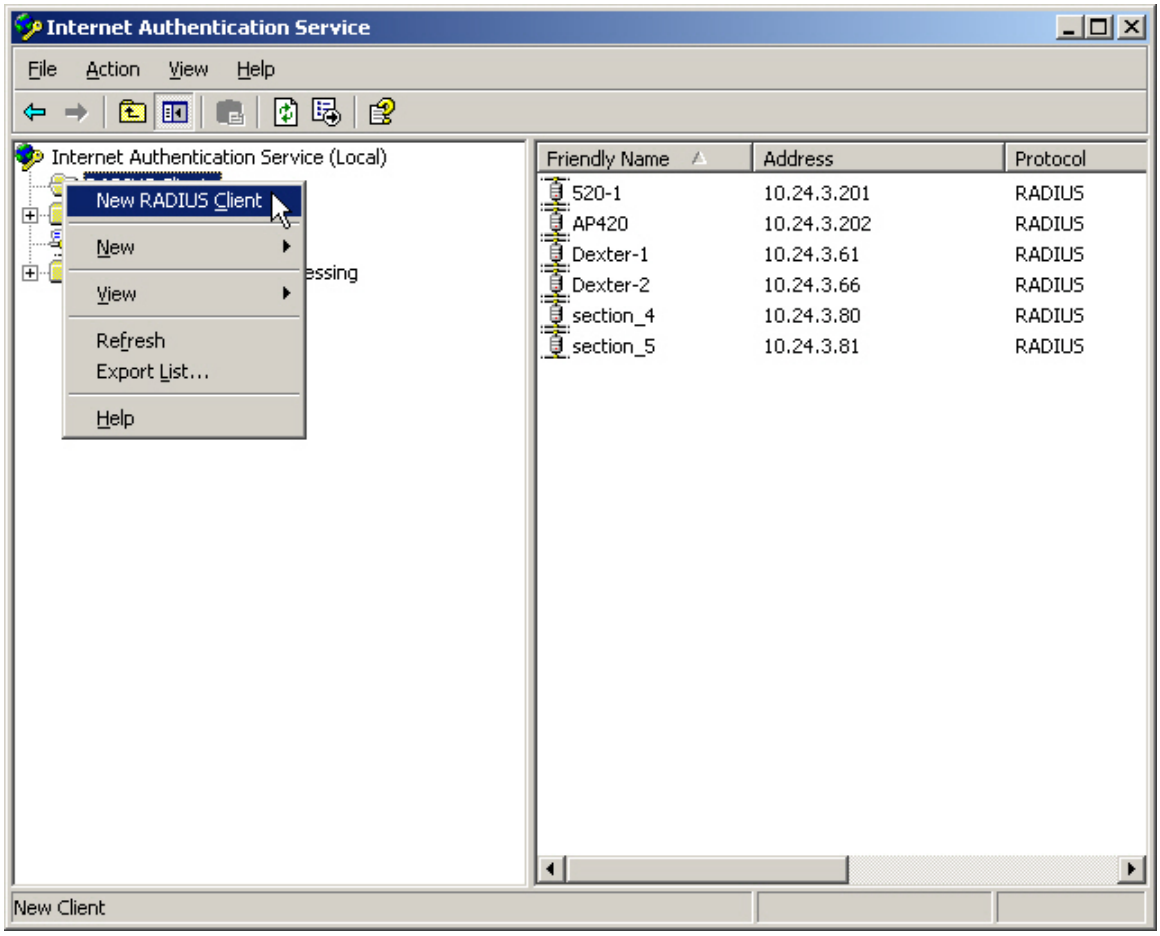


Figure 3.1 – New RADIUS Client

b. Configure a Friendly name (`740wl`) and enter the **IP address** of the **Access Control Server** (`10.24.3.50`). Click Next.

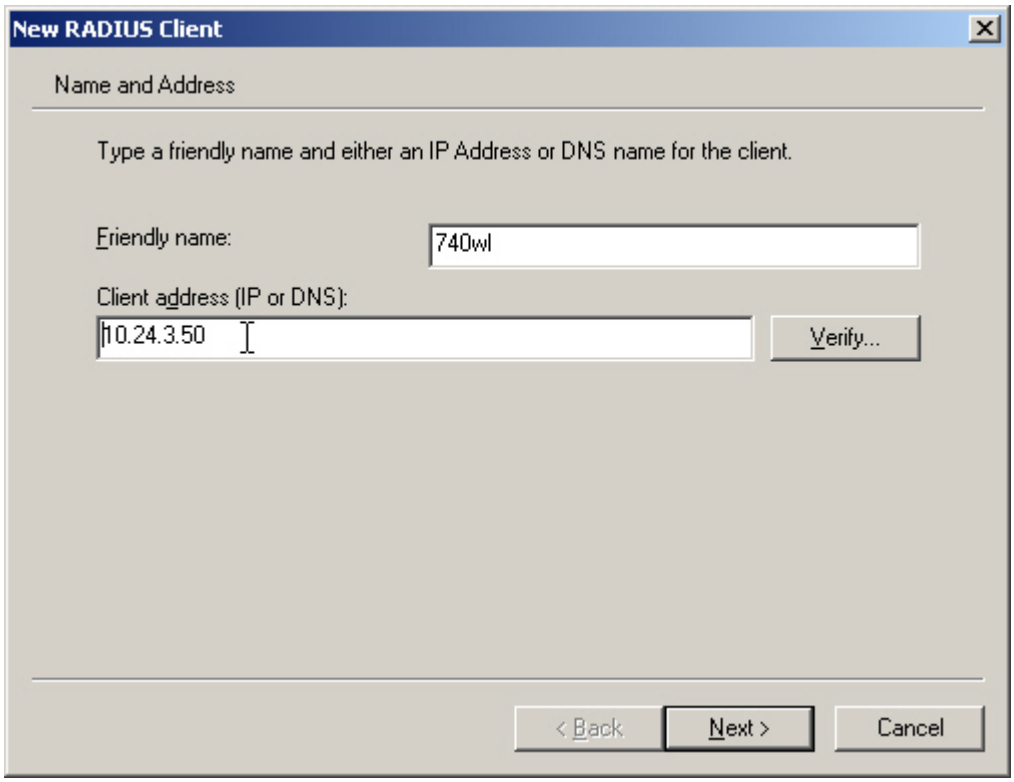


Figure 3.2 – New RADIUS Client Name and IP

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

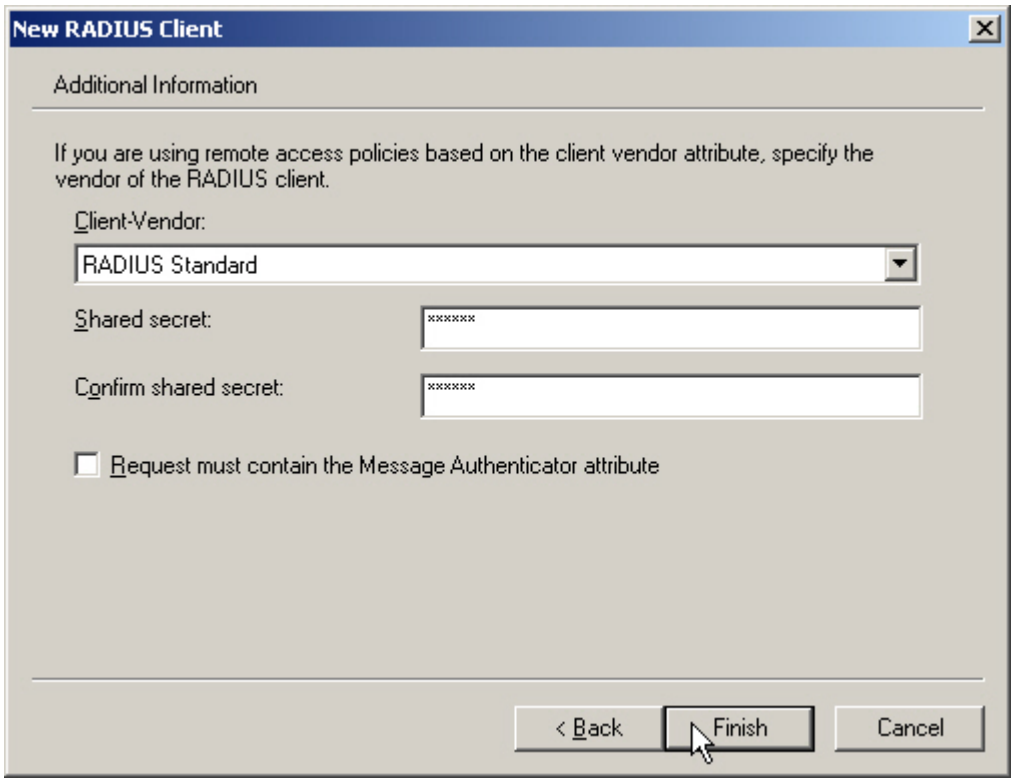


Figure 3.3 – New RADIUS Client Shared Secret

2) 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**.

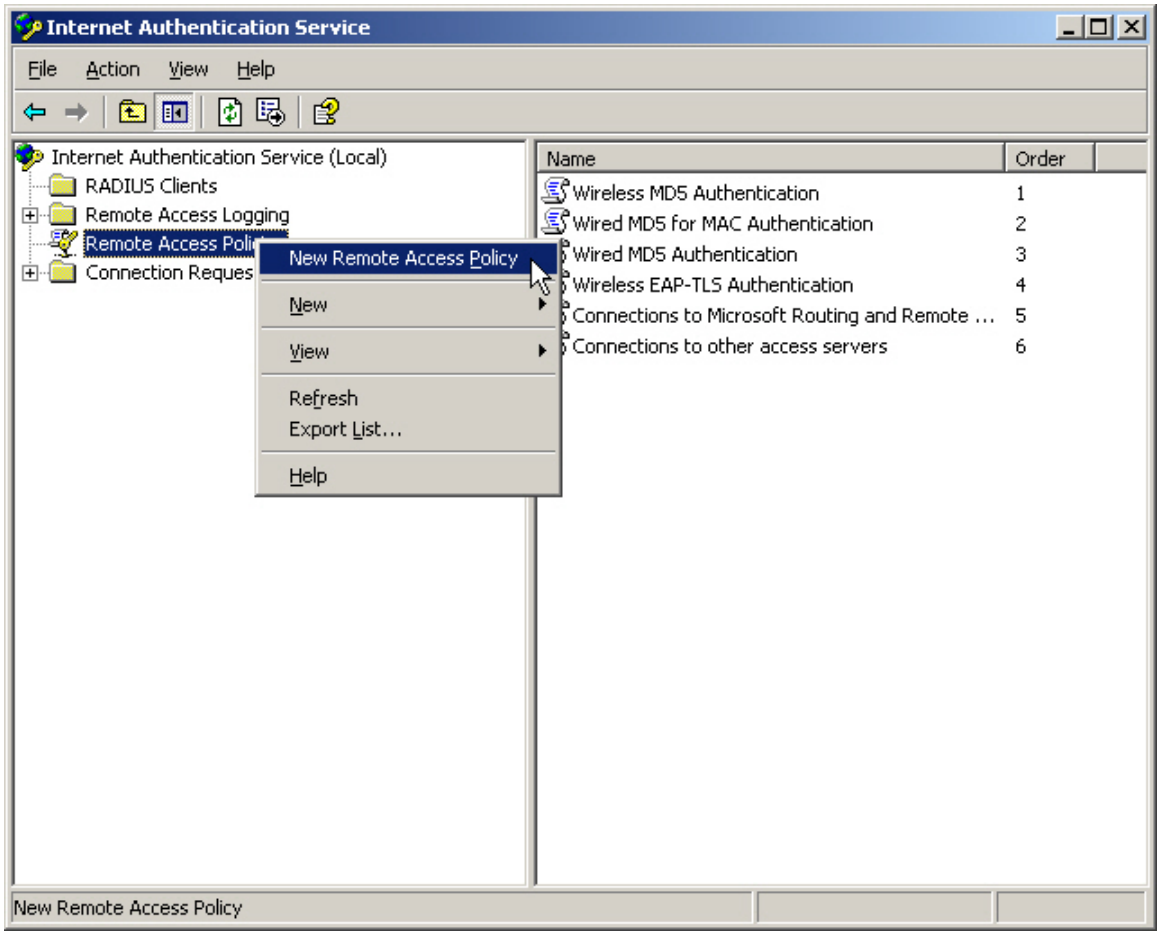


Figure 3.4 – New Remote Access Policy

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

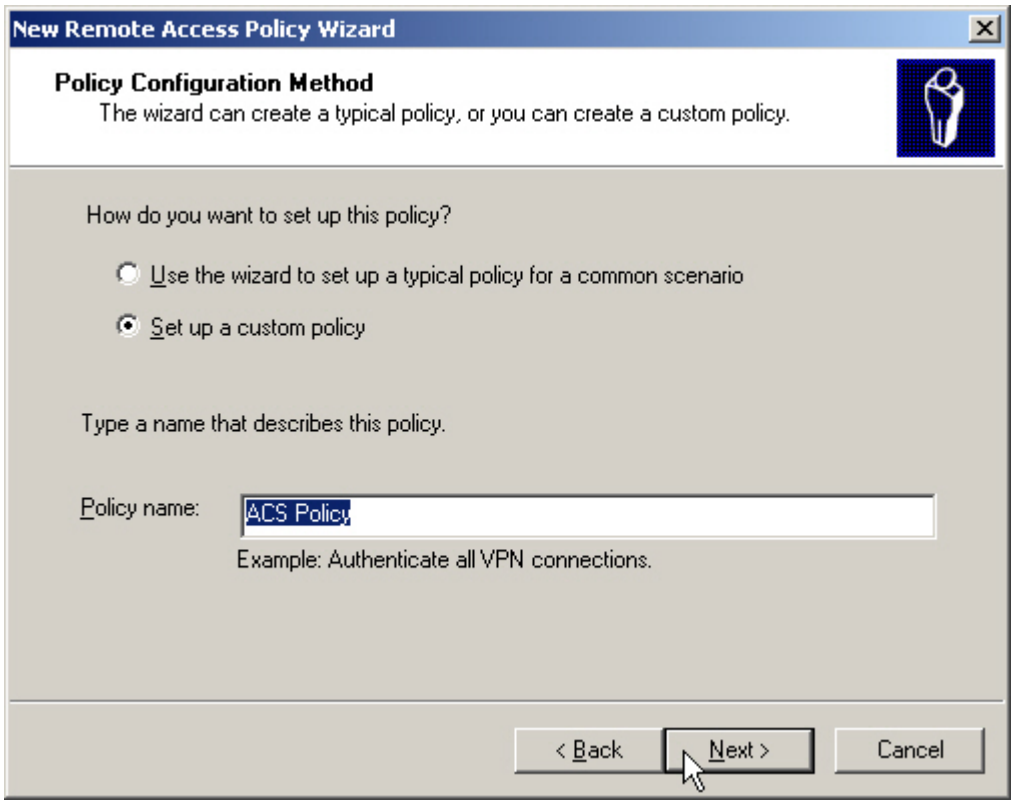


Figure 3.5 – New Remote Access Policy Name

c. Click Add to add policy conditions.

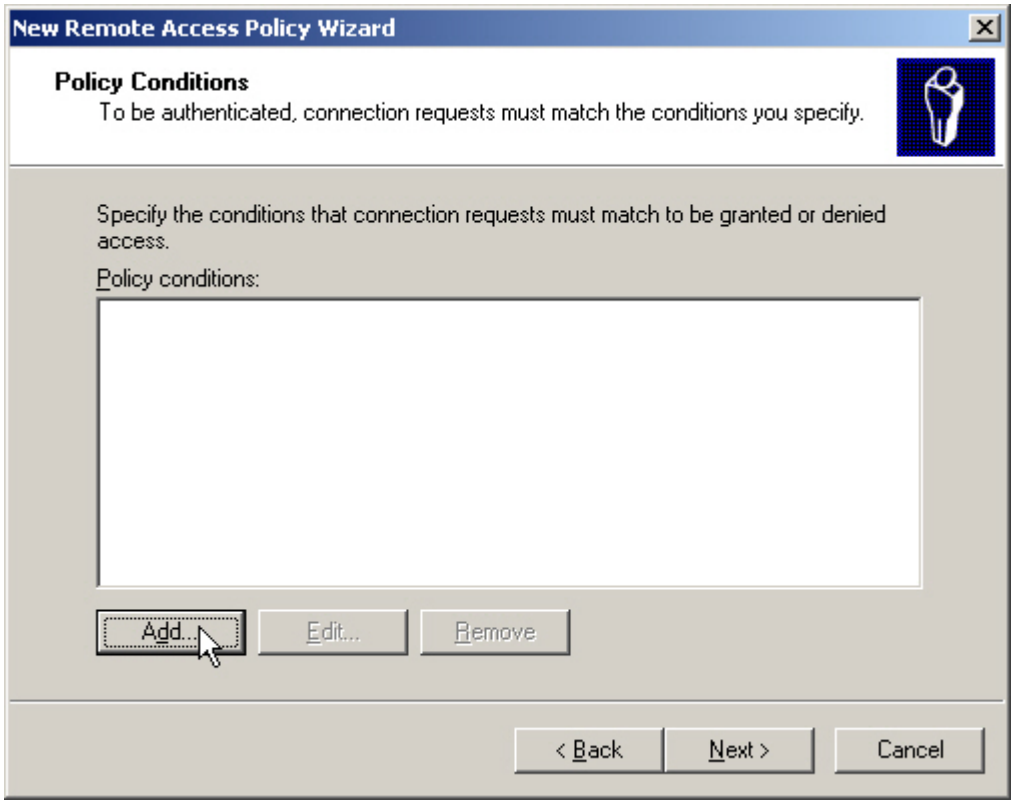


Figure 3.6 – New Remote Access Policy Conditions

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

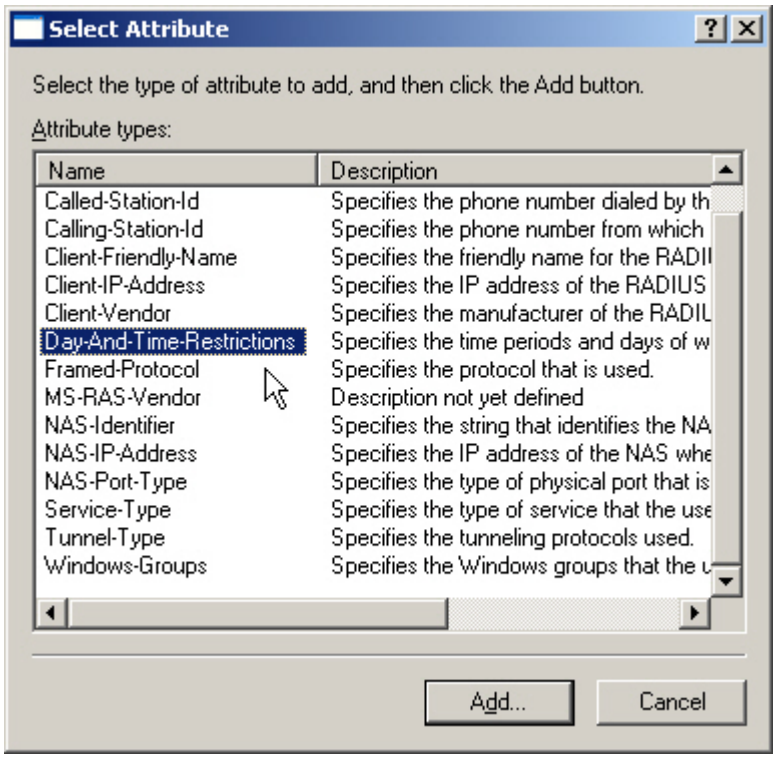


Figure 3.7 – New Remote Access Policy Attribute

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

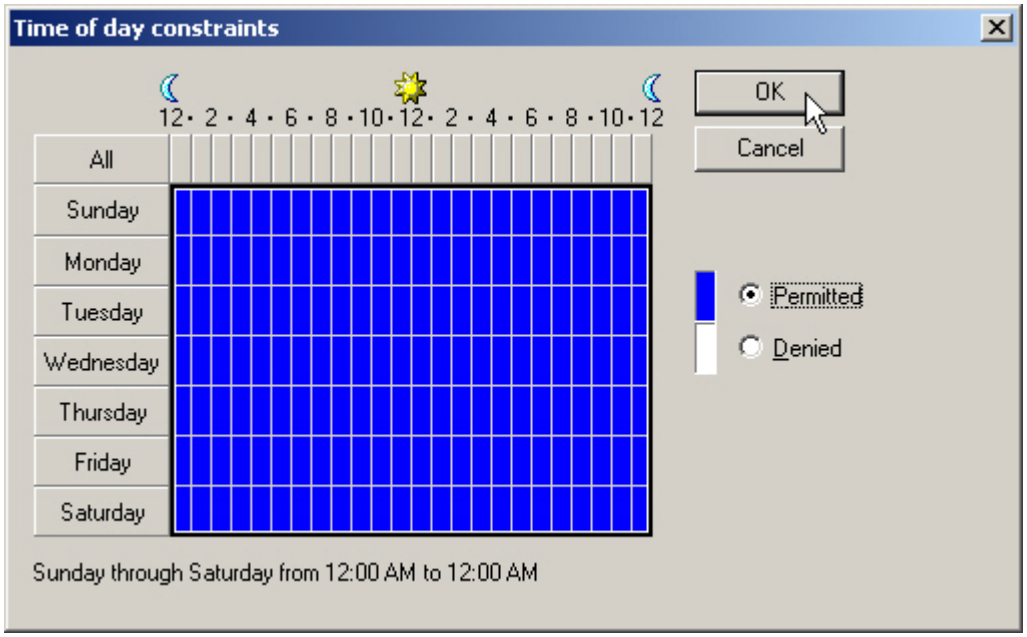


Figure 3.8 – New Remote Access Policy Attribute Conditions

f. Click the Add button again to add the **Windows-Groups** attribute.

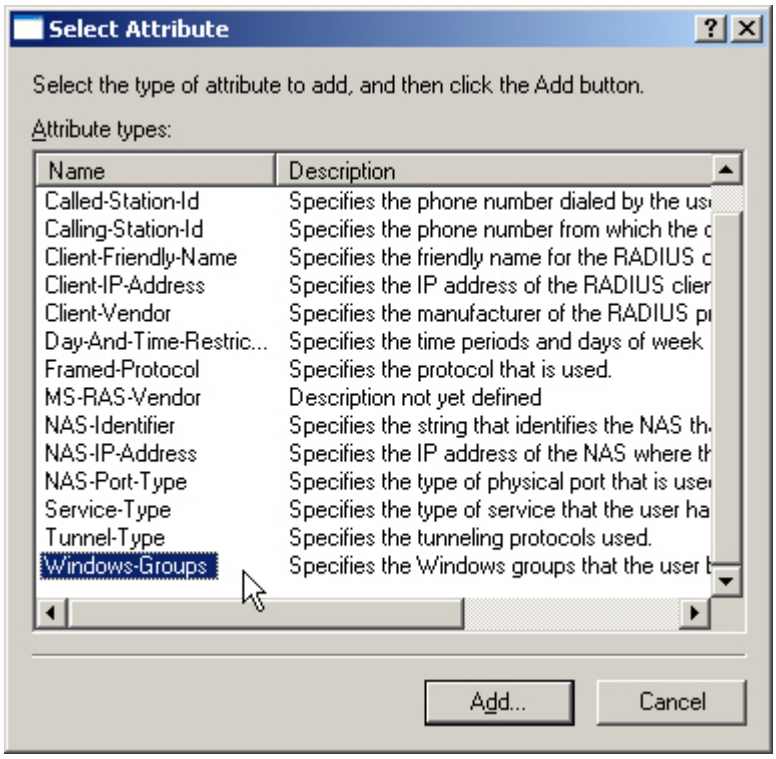


Figure 3.9 – New Remote Access Policy Attribute

g. In the Groups window click **add**, enter the **Authorized_Users** group and click OK. Click OK again.

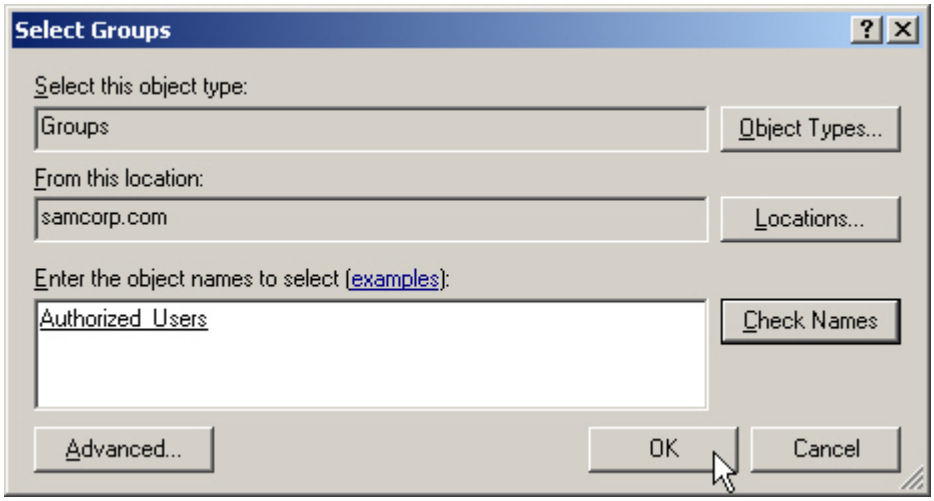


Figure 3.10 – New Remote Access Group

h. Back at the Policy Wizard, click next to accept the two new policy conditions.

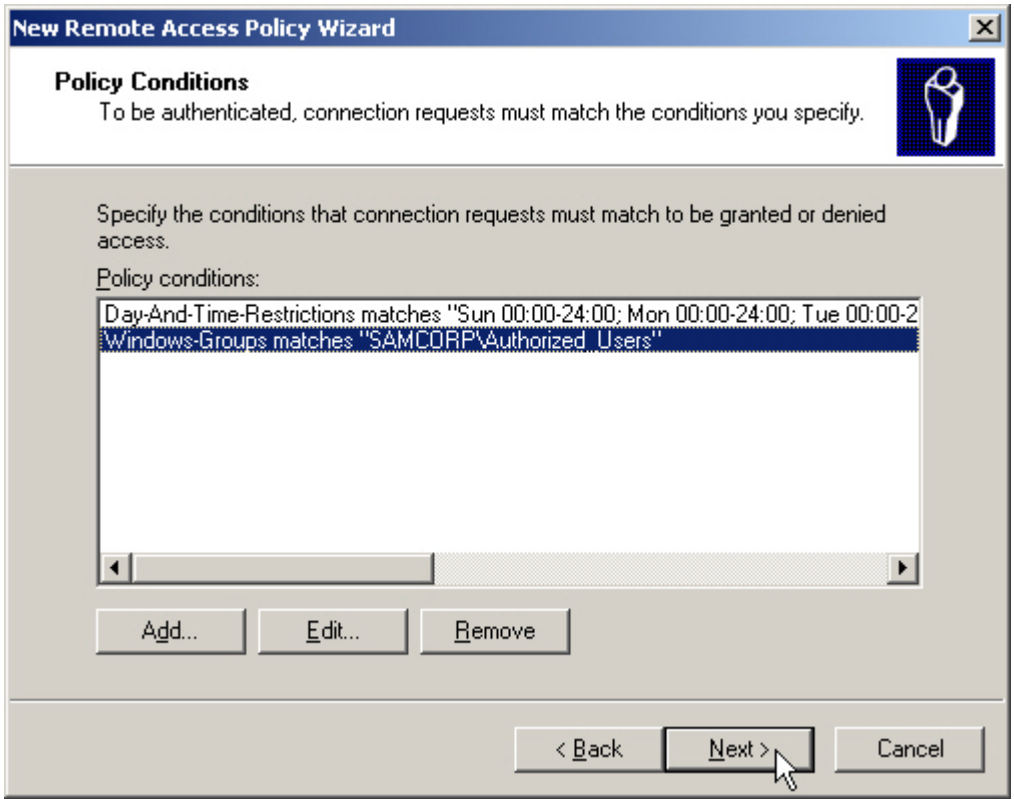


Figure 3.11 – New Remote Access Policy Conditions

i. Select the radio button to **Grant remote access permission** and click next.

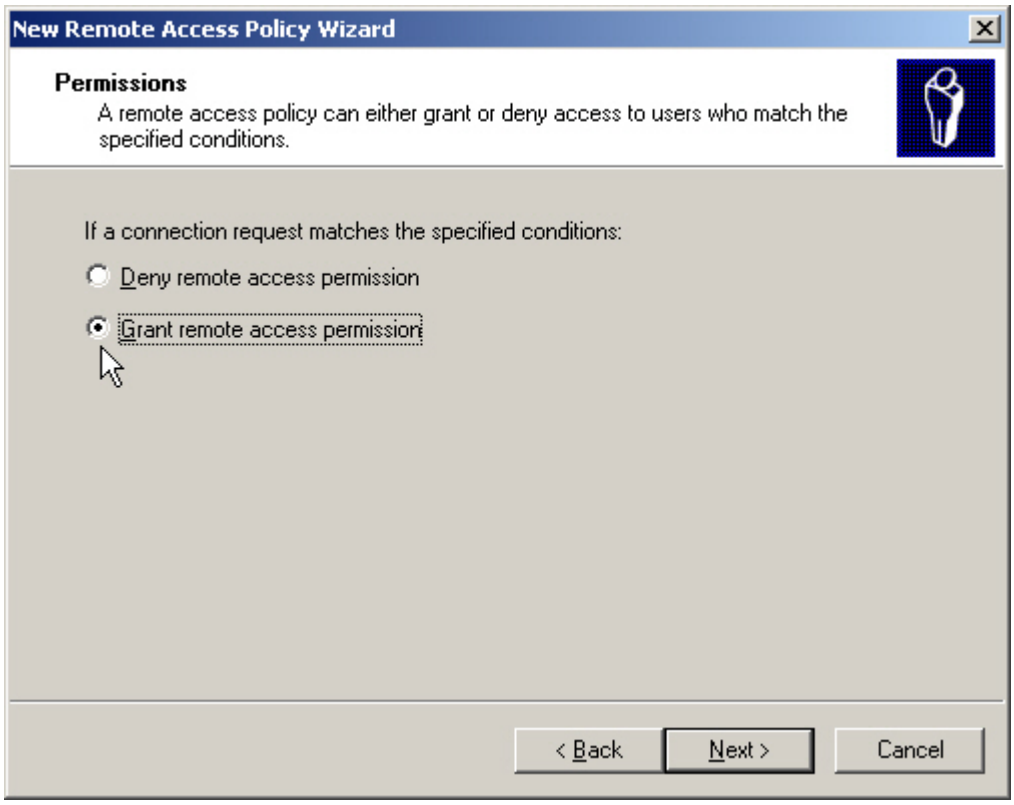


Figure 3.12 – New Remote Access Policy Permissions

j. Click the Edit Profile button, select the Authentication tab in the Edit Dial-in Profile window and ensure that **MS-CHAP v2, MS-CHAP and Unencrypted PAP** are selected. Apply changes.

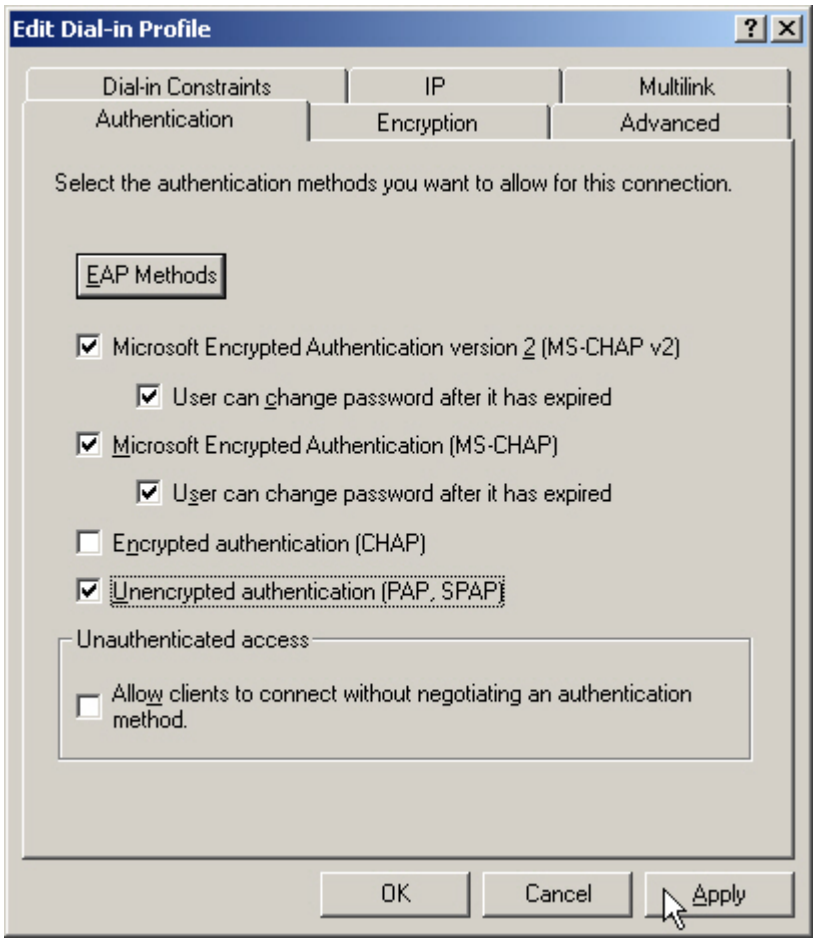


Figure 3.13 – New Remote Access Policy – Edit Profile

k. Select the Advanced tab and click the **Add** button.

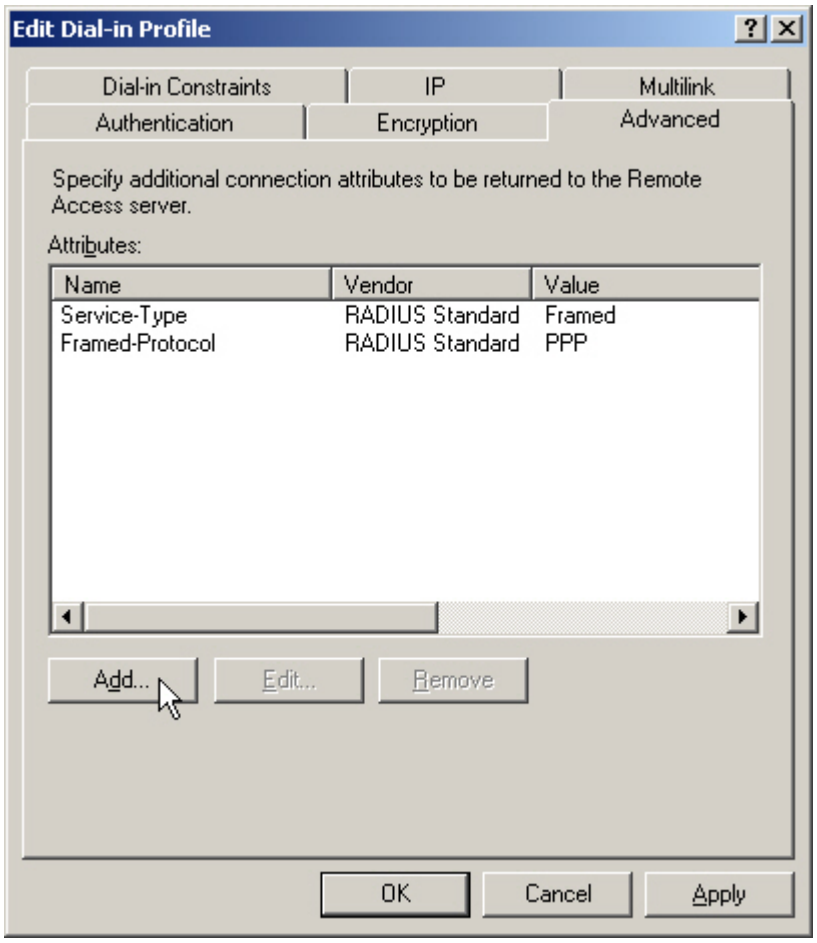


Figure 3.14 – New Remote Access Policy – Edit Profile Advanced

l. Add the **Login-LAT-Group** as an attribute for this Remote Access Policy.

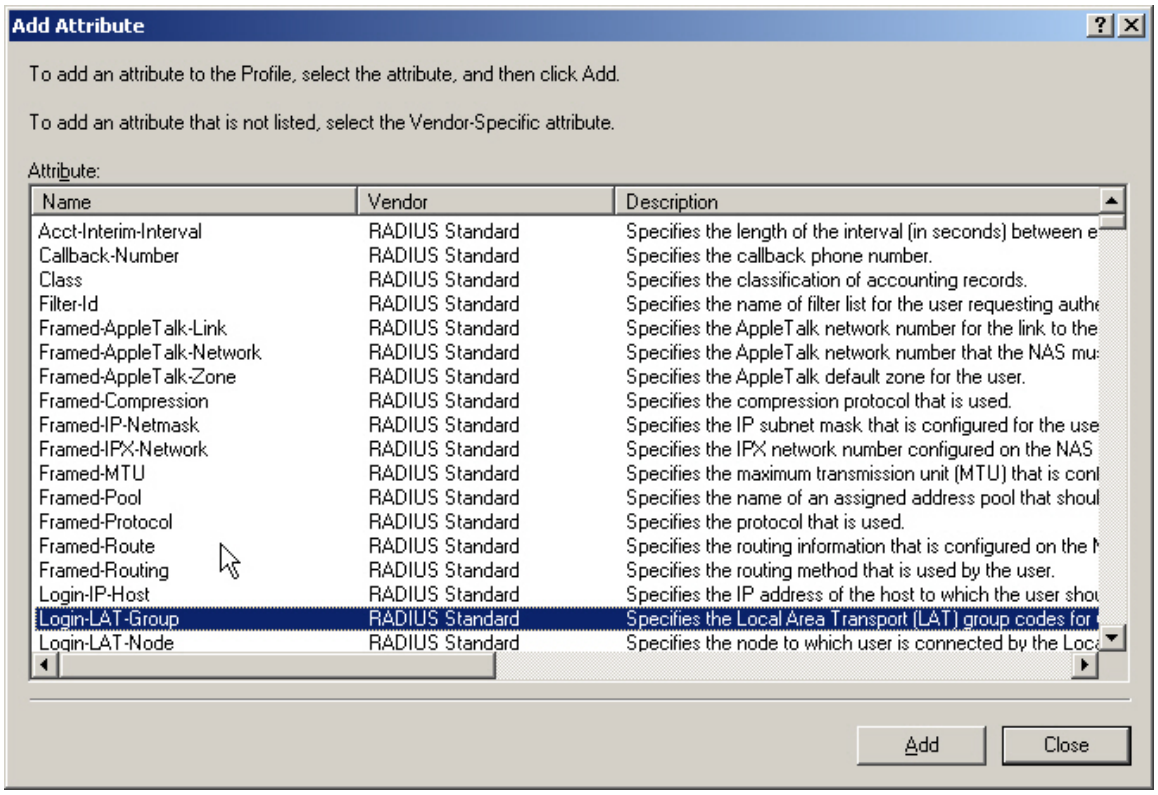


Figure 3.15 – New Remote Access Policy – Attribute

m. Configure the **Attribute Information** value with the group information (`Authorized_Users`) and click OK.

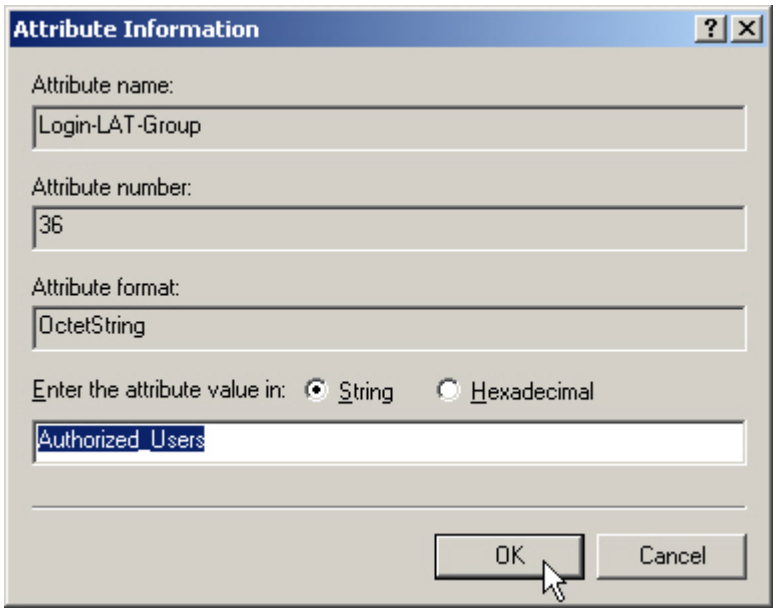


Figure 3.16 – New Remote Access Policy – Login LAT Group

n. Apply the changes and click OK to finish the Policy Wizard.

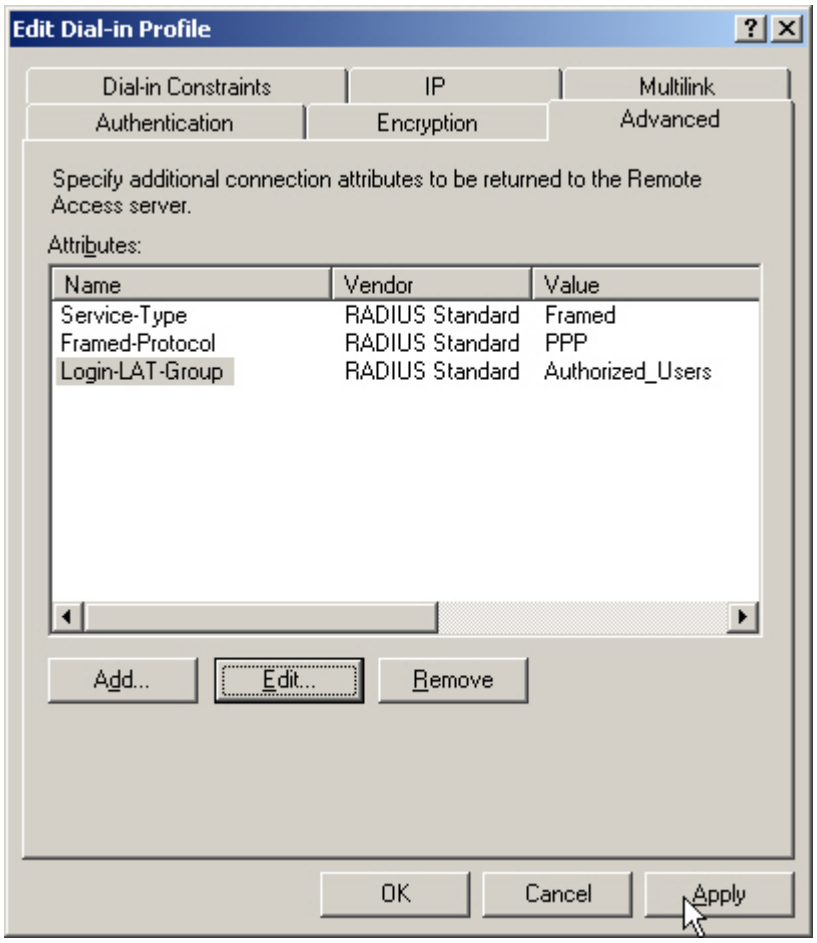


Figure 3.17 – New Remote Access Policy

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

a. On the ACS, browse to Rights -> Authentication Policies and click the **New Service** button. Chose the RADIUS button on the left 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**

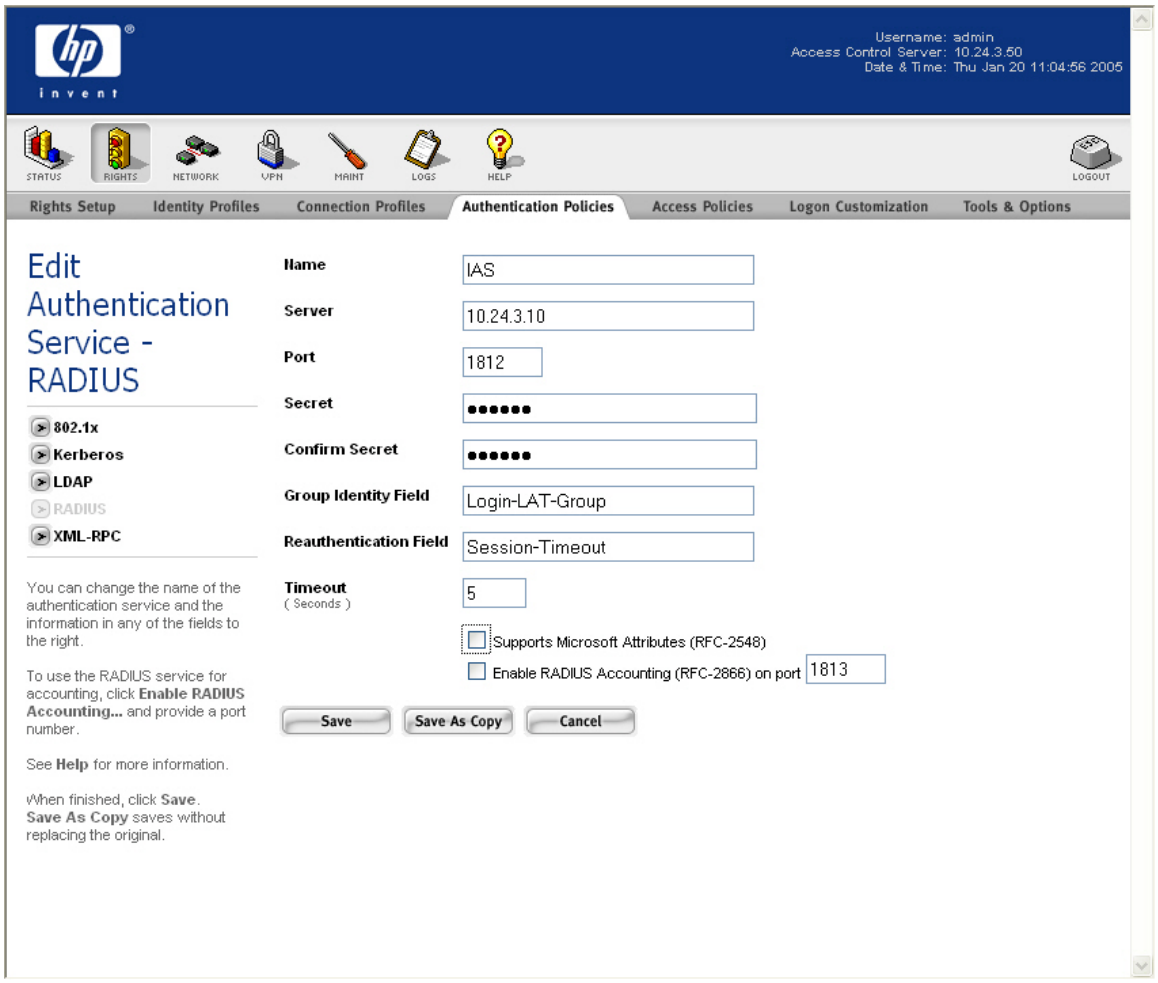


Figure 3.18 – RADIUS Authentication Service

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.

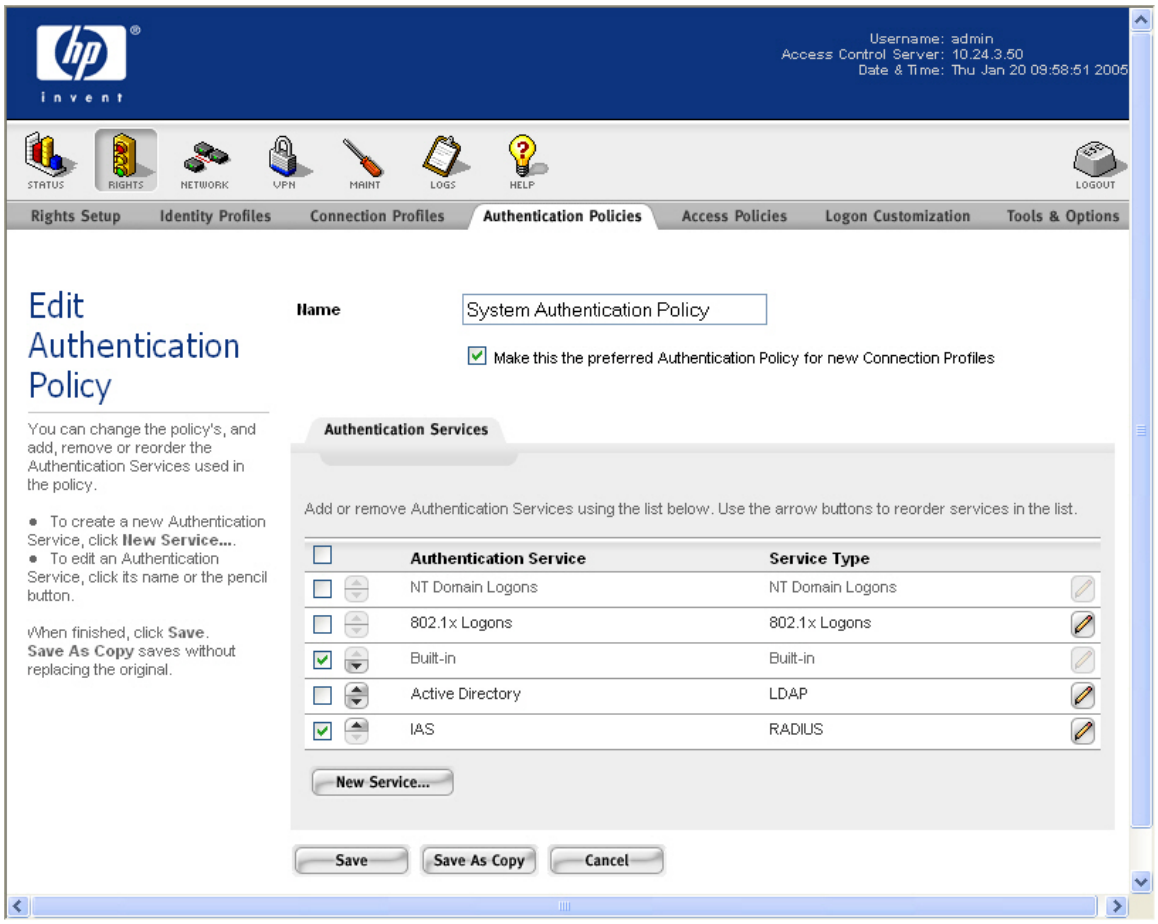


Figure 3.19 – System Authentication Policy

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

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

a. Refer to Configuring Scenario 2 to configure the Authenticated Access Policy to allow clients to use Real IP addresses.

5) On the AP 420, configure Static WEP wireless parameters.

a. Refer to Configuring Scenario 1 to configure the AP 420 for Static WEP.

6) Connect Windows 2000 Client, logon using browser-based logon and verify authentication.

a. Connect the wireless Windows 2000 client to the AP 420 using Static WEP.
b. Open a Web browser on the client. The 700wl logon page will appear. (You may need to configure the browser to accept all cookies).
c. Enter the username (`juser`) and password (`password`) and click the **Logon User** button.

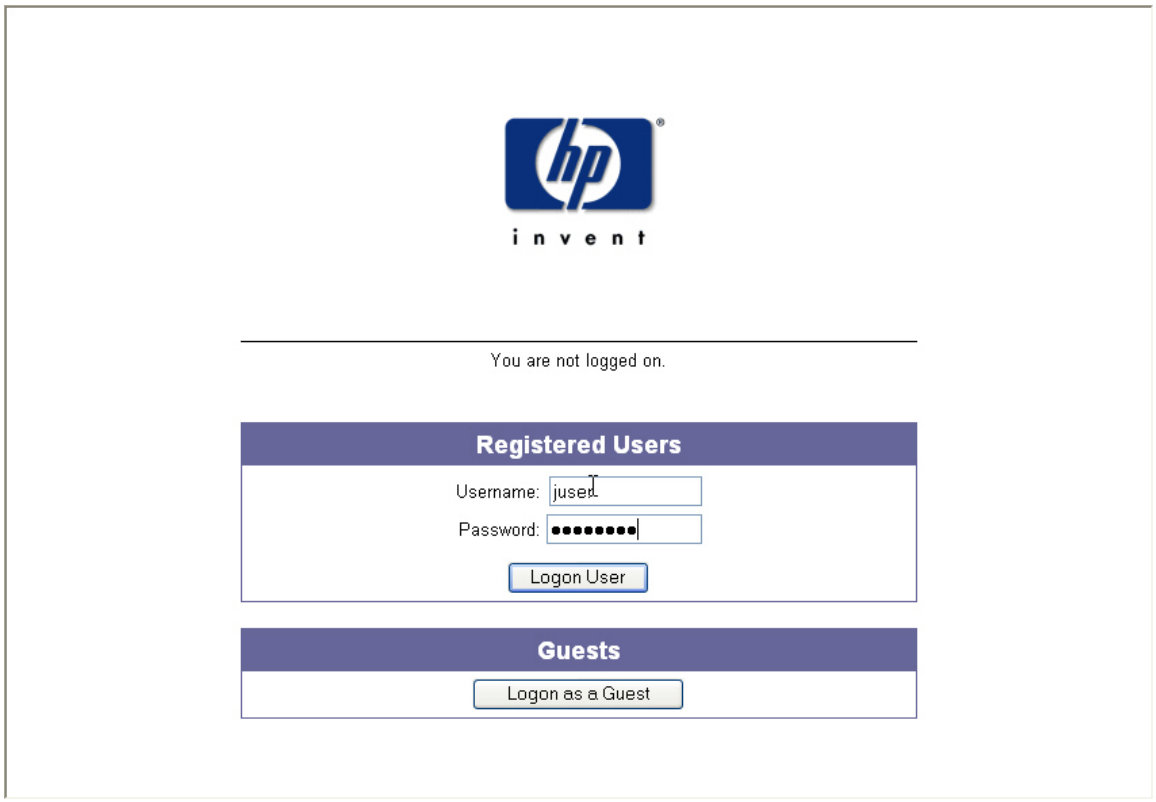


Figure 3.20 – Logon Page

d. 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) and has received a Real IP address (via DHCP).

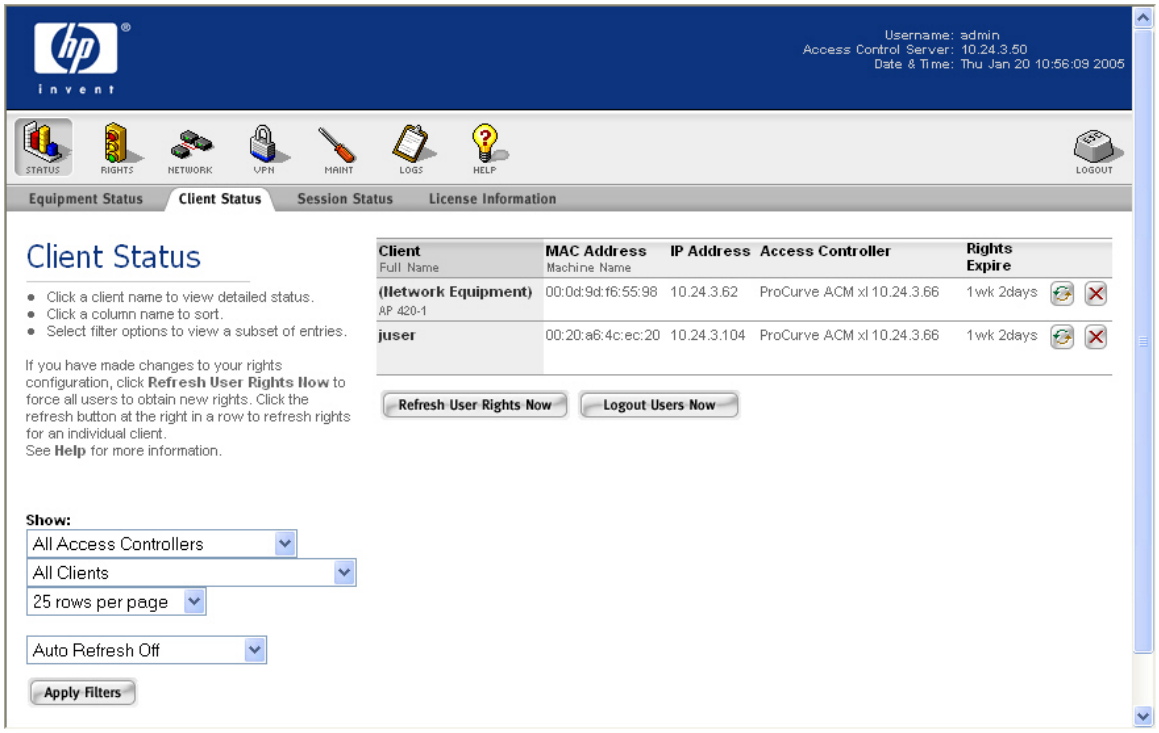


Figure 3.21 – Client Status Page

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

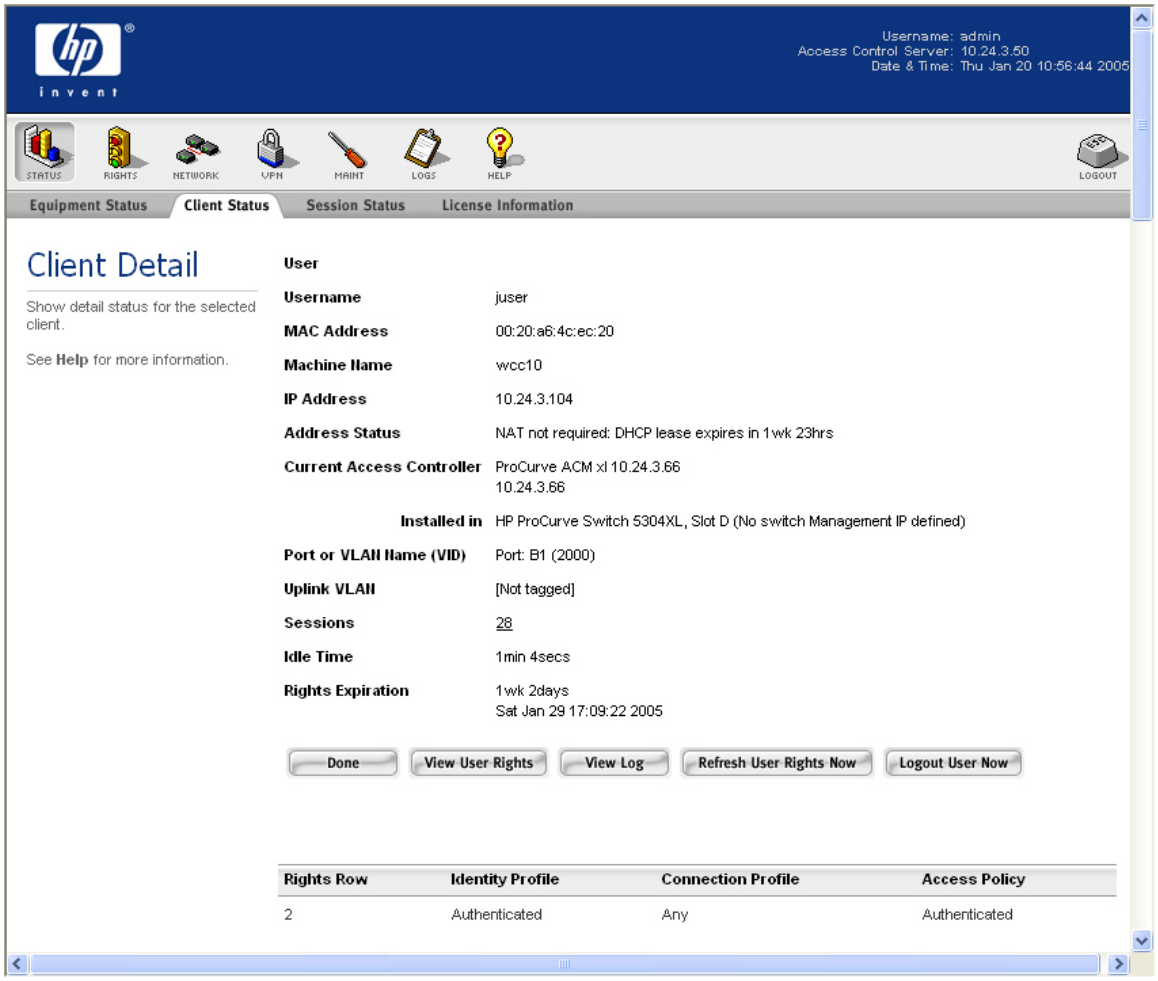


Figure 3.22 – Client Detail Page

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

www.procurve.com

March 2005