

# Secure Access Configuration Guide For Wireless Clients Part One: Browser-based Logon



2
2
2
2
3
4
4
4
5
5
5
8
. 14
. 28



# 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 browserbased 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 5300xI (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 (<u>http://www.procurve.com</u>).

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 xI 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 5300xI 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
```

#### 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
```

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.

- <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
```

 <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.

				Access Cont D	Username: admin rol Server: 10.24.3.5 ate & Time: Fri Jan 14	0 4 15:36:08 2005
Image: Status         Image: S	MAINT LOGS	HELP icense Information				LOGOUT
Client Status	Client Full Name	MAC Address Machine Name	IP Address	Access Controller	Rights Expire	
Click a client name to view detailed status.     Click a column name to sort.	Not logged on	00:0d:9d:f6:55:98	10.24.3.62	ProCurve ACM xI 10.24.3.66	1 wk 2days	
If you have made changes to your rights configuration, click <b>Refresh User Rights</b> <b>Now</b> 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 <b>Help</b> for more information.						
Show:						
All Clients 25 rows per page						

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.

Envent *				U Access Contro Dat	sername: admin Il Server: 10.24.3.50 e & Time: Fri Jan 14 15:4	4:17 2005
STATUS RIGHTS RETWORK	PPN MAINT LOGS	HELP				LOGOUT
New Equipment	Equipment Name	AP 420-1	Access Policies	Logon Customization	Tools & Options	
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.	MAC Address	00:0d:9d:f6:55:98				
ywich misned, click sawe.	Assign this equipment t button. To add an Identi	o one or more identity Profile: ty Profile, click <b>New Identity</b>	s from the list below. Profile	To edit an Identity Profile, (	click its name or the pencil	
	ldentity Profile					_
	Access Points					
	New Identity Profile	-				
	Save C	ancel				

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".

invent.				Usernam Access Control Serve Date & Tim	e: admin r: 10.24.3.50 e: Tue Jan 18	11:01:33 200
STRIUS RIAHTS AND CLIENT STATUS	Logs RELP	ion				LOGOUT
Client Status	Client Full Name	MAC Address	IP Address	Access Controller	Rights Expire	
Click a client name to view detailed status.     Click a client name to sort.     Select filter options to view a subset of entries.     If you have made changes to your rights     configuration, click <b>Refresh User Rights How</b> 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:	Refresh User Rights No	w Logout Us	ers Now			
All Access Controllers						
25 rows per page  Auto Refresh Off Apply Filters						

Figure C – Client Status - Refresh User Rights Now

#### <u>Configuring Scenario 1: Browser-based Logon using Built-in Database</u> <u>Authentication</u>

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.

			Acces	Username: admin s Control Server: 10.24.3.50 Date & Time: Tue Jan 18 13	:07:37 2005
Image: Status         Image: S	Connection Profiles Aut	RLP hentication Policies Access Poli	cies Logon Customization	Tools & Options	LOGOUT
New User To add a user to the built-in database, 1. Enter a descriptive name (full name, for example) for the user 1. Add address. One or the other is required. 2. For a MAC address, check the Add Address User box. 3. For a Gog on name, optionally enter and confirm a password. 3. Elect Identity Profiles for the user from the Identity Profiles Ist. When finished, click Save.	Name Descriptive Name Username / MAC Address Password Confirm Password Identity Profiles Assign this user to one or mon Identity Profile, click New Ident Identity Profile Guest (MAC address u Access Points New Identity Profile	juser juser juser MAC Address User MAC Address User Control of the list below re identity Profiles from the list below sers may not be members of this identity	To edit an Identity Profile, click i Profile)	ts name or the pencil button. To	add an
					~

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.

				Access	Username: admin Control Server: 10.24.3.5 Date & Time: Tue Jan 1	0 8 13:11:46 2005
Status         BIGHTS         See U         U           Rights Setup         Identity Profiles         U	PH MAINT LOGS	HELP Authentication Policies	Access Policies	Logon Customization	Tools & Options	Logout
New Identity Profile	Name Maximum Concurrent Logons Per User	Users				
Provide a name for the Identity Profile. If the Identity Profile should match users that get a identity or domain name from an external authentication service, make sure its name is identical to the identity or domain name you want to match.	Save Ca	Show all users an Muming : Unsaved chan Displaying the built-in databa	<b>d network equipr</b> nges will be lost if this i se may take a few mir	nent in the built-in datab s checked or unchecked. urtes.	ase	
To add users or network equipment from the built-in database to the Identity Profile, select from the lists under the Users and Network Equipment labs.     When finished, click Save.						
						2

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.

			Usern Access Control Se Date & T	ame: admin rver: 10.24.3.50 filme: Tue Jan 18 14:00:00 2	2005
STATUS RIGHTS NETWORK	PRI MAINT LOGS	HELP		LOGO	
Rights Setup Identity Profiles	Connection Profiles Aut	hentication Policies Access Policies	Logon Customization	Tools & Options	-
Edit User	<b>Hame</b> Descriptive Name	juser	]		
Change any of the values in the fields to the right. Add or remove Identity Profiles for the user from the Identity Profiles list.	Username / MAC Address	juser 🔲 MAC Address User			
When finished, click Save.	Password	•••••	1		
	Confirm Password		]		
	Identity Profiles Assign this user to one or mo To add an Identity Profile, click	re Identity Profiles from the list below. To edit	an Identity Profile, click if	s name or the pencil button.	
	Lidontitu Drofilo				
	Guest (MAC address u:	sers may not be members of this Identity Profile)			
	Access Points				
	Vsers 🗸 🗸 Vsers				
	New Identity Profile				
	Save Save As Co	py Cancel			~

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.

				A	Username: ccess Control Server: Date & Time:	admin 10.24.3.50 Tue Jan 18 13:56:44 2005	~
	STATUS		HELP			LOGOUT	
ľ	Rights Setup Identity Profiles	Connection Profiles	Authentication Policies	Access Policies	Logon Customizatio	on Tools & Options	
	New Rights Assignment	Identity Profile Connection Profile	Users 💌				
	To add a row to the Rights table, select an Identity Profile, a Connection Profile, and an Access Policy from the drop-down lists at right.	Access Policy Row Position	Authenticated	Any 💌			
	To specify where the row should be inserted into the table, select a row position from the Row Position drop-down list.	Save	Cancel				
	When finished, click Save.						
							~

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
111111111333
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.

invent	
You are not logged on.	
Registered Users	
Username: jused Password: •••••••	
Guests	
Logon as a Guest	

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.

				Userna Access Control Ser Date & T	ame: admin rver: 10.24.3.50 i me: Tue Jan 18	13:35:3	13 2005
Image: Status         Image: S	License Informatio	n				(	.ogout
Client Status	Client Full Name	MAC Address Machine Name	IP Address	Access Controller	Rights Expire		
<ul> <li>Click a client name to view detailed status.</li> <li>Click a column name to sort</li> </ul>	(Network Equipment) AP 420-1	00:0d:9d:f6:55:98	10.24.3.62	ProCurve ACM xI 10.24.3.66	1 wk 2days	<b>5</b>	×
<ul> <li>Select filter options to view a subset of entries.</li> <li>If you have made changes to your rights configuration, click Refresh User Rights How 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.</li> <li>See Help for more information.</li> </ul>	juser <sup>juser</sup> Refresh User Rights Nov	00:20:a6:4c:ec:1f	Now	ProCurve ACM xl 10.24.3.66	1 wk 2days	<b></b>	×
Show: All Access Controllers							
25 rows per page 💌							
Auto Refresh Off   Apply Filters							

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.

			Access Co	Username: admin ontrol Server: 10.24.3.50 Date & Time: Tue Jan 18 14:00:42 2005
STATUS RIGHTS NETWORK UP	N MAINT LOGS	HELP		LOGOUT
Equipment Status Client Status	Session Status Licens	e Information		
Client Detail	User	juser		
Show detail status for the selected	Username	juser		
client.	MAC Address	00:20:a6:4c:ec:1f		
See Help for more information.	Machine Name			
	IP Address	42.121.175.122		
	Address Status	NAT mode: rights do not a	llow use of non-NAT IP address	
	Current Access Controller	ProCurve ACM xl 10.24.3. 10.24.3.66	66	
	Installed in	HP ProCurve Switch 5304	XL, Slot D (No switch Managemei	nt IP defined)
	Port or VLAN Name (VID)	Port: B1 (2000)		
	Uplink VLAN	[Not tagged]		
	Sessions	5		
	Idle Time	1min 13secs		
	Rights Expiration	1 wk 2days Thu Jan 27 20:13:57 2005	i	
	Done View Use	r Rights View Log	Refresh User Rights Now	Logout User Now
	Dista David	dia Des Cla	Owners they Des file	Access Dellars
	Rights Row Ider	ntity Profile	Connection Profile	Access Policy
	1 Use	rs	Any	Authenticated

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  $\rightarrow$  Users.
  - Select New → User.

🍯 Active Dire	ctory Users and Compu	iters			<u>- 0 ×</u>
🌍 Eile 🛛 Actior	n <u>V</u> iew <u>W</u> indow <u>H</u> el	p			_8×
⇔ ⇒   €	🗉   % 🛍   X 🖻	1	🤁 🖉 👛 🖓	7 🍕 🙍	
ntrive Direct	ory Users and Computers	Users 146 obje	cts		
🗄 🦲 Saved Q	ueries	Name	Туре	Description	<b>▲</b>
🖃 🗊 samcorp.	.com	🖸 72hc1	User		
		🕵 72hc10	User		
	ain Controllers	🖸 72hc11	User		
+ Dorne	ignSecurityPrincipals	🖸 72hc12	User		
Use Use	Delegate Control	72hc13	User		
	Find	2hc14	User		
-	1 jildilli	P2hc15	User		
	New	Computer	8		
	All Tas <u>k</u> s	Contact			
	View	► Group	and the second		
	New <u>W</u> indow from Here	InetOrgPe MSMQ Que	rson eue Alias		
	Refresh	Printer			
	Export List	User	>		
	Properties	Shared Fo	der User		
-	Help	'2hc24	User		
d t	•	2hc25	User		
reate a new obi	iect				

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.

	rin. sancorp	.com/osers		
First name:	Joe		Initials:	
ast name:	User			
full n <u>a</u> me:	Joe User			-
Jser logon name:				
juser	2	@samcorp	o.com	•
Jser logon name i	(pre- <u>W</u> indows 2	2000):		
SAMCORP\		juser		

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. ٠
- •

New Object - User		×
🕵 Create in: samo	orp.com/Users	
Password:	•••••	
<u>C</u> onfirm password:	•••••	
🔲 User <u>m</u> ust change passw	ord at next logon	
🔲 U <u>s</u> er cannot change pass	word	
Pass <u>w</u> ord never expires		
Account is disabled		
-		
	<u> </u>	Lext > Cancel

Figure 2.3 - New Object – User Password

- •
- Highlight the newly created user. Right Click and Select **properties**. ٠

tomp: 🐇 Active Directory Users and Comp	iters	
🎻 Eile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> e	lp	_8×
⇔ → 🗈 🖬 🐰 🛍 🗙 😭	🕅 🗟   😫   🦉 🦉 ៉ 🖓 🍕	1
Active Directory Users and Computers	Users 146 objects	24
E	Name Type	Description
E	IWAM_ZEUS User     Jim User User	Built-in account for Intern
Computers     Domain Controllers     ForeignSecurityPrincipals     Users	Joe       Copy         Ken       Copy         Add to a group       Disable Account         OWS       Disable Account         OWS       Moye         OWS       Open Home Page         RAS       Send Maji         Sche       All Tasks         Sche       All Tasks         snc1       Cut         Delete       Rename         snc1       Properties         snc1       Help	Key Distribution Center Se Microsoft SharePoint role ' Microsoft SharePoint role ' Servers in this group can Designated administrators

Figure 2.4 - User Properties

In the Account tab, enable the box next to "store passwords using reversible encryption" in the Account options area. ٠

oser Propertie	3			
Member Of Remote contro General Addre	Dial-in     Term ss Account	Enviro ninal Service   Profile	onment   s Profile Telephones	Sessions   COM+   Organizatior
User logon name: juser	1	 @samo	orp.com	-
, User logon name i	pre-Windows 20	00):	en hannin	
SAMCORP\		juser		
Account is loc Account options:	ked out	10		
Account is loc Account options:	ked out hange password t change password	at next logo	n	-
Account is loc Account options: User must c User cannol Password n V Store passw	ked out hange password t change passwo ever expires vord using reversi	at next logo ord ble encryptic	n	
C Agcount is loc Account options: C User must c C User cannol C Password n V Store passw Account expires C Ne <u>v</u> er	ked out hange password t change passwo ever expires vord using reversi	at next logo ord ble encryptio	n on	× 
<ul> <li>☐ Agcount is loc</li> <li>Account options:</li> <li>☐ User must c</li> <li>☐ User cannol</li> <li>☐ Password n</li> <li>☑ Store password</li> <li>Account expires</li> <li>④ Neyer</li> <li>④ End of:</li> </ul>	ked out hange password change passwo ever expires ford using reversion Thursday	at next logo rd ble encryptio	n on 27, 2004	• • •

Figure 2.5 - User Properties – Account

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

Remote control Terminal Serv	rices Profile	COM+
Jeneral Address Account Profile		Urganization Sessions
Remote Access Permission (Dial-in or VPN     Allow access     Deny access		
C Control access through Remote Access	s <u>P</u> olicy	
I⊻erify Caller-ID:		
- Callback Options		
• No <u>C</u> allback		
C Set by Caller (Routing and Remote Acc	cess Service only	)
C Always Callback to:		
🗖 Assign a Static IP Address		<u></u>
Apply Static <u>B</u> outes		
Define routes to enable for this Dial-in connection.	Static Roy	ites

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.

🍜 Active Directory Users and Comp	uters			
🌍 Eile Action View Window He	elp			
⇐ → 🖻 🖪 🐰 🖀 🗡 🖆	1 🗟 🗟	🦹 📅 📷 🖓	7 🍕 🗖	
Active Directory Users and Computers  Active Directory Users and Computers  Saved Queries  Samcorp.com  Builtin  Computers  Computers  ForeignSecurityPrincipals  Users  Delegate Control	Users 146 ob; Name 72hc24 72hc25 72hc26 72hc26 72hc27 72hc28 72hc28 2hc29	Type User User User User User User User Use	Description	
Find	2hc3	User		
All Tas <u>k</u> s	Compute     Contact	er		
<u>V</u> iew New <u>W</u> indow from Her	e Group	gerson Queue Alias		
Refresh Export <u>L</u> ist	Printer User	Folder		
Properties	2bc39	User		
Help	2hc4	User		
	<b>1</b> 721040	User		

Figure 2.7 - New Group

- ٠
- 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. ٠

roup n <u>a</u> me:	
Authorized_Users	
roup name (pre- <u>W</u> indows 20	)00):
Authorized_Users	
Group scope	Group type
C Domain local	
🖲 <u>G</u> lobal	O Distribution

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.

User Propertie	5
Remote control General Addres Member Of	Terminal Services Profile   COM+ s   Account   Profile   Telephones   Organization   Dial-in   Environment   Sessions
Member of: Name	Active Directory Folder
Domain Users	samcorp.com/Users
	- 1
<u>Add</u>	<u>R</u> emove
Primary group:	Domain Users up   There is no need to change Primary group unless
<u>set Primary Gro</u>	you have Macintosh clients or POSIX-compliant applications.

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.

elect Groups		? ×
Select this object type:		
Groups or Built-in security principals		<u>O</u> bject Types
Erom this location:		
samcorp.com		Locations
Enter the object names to select ( <u>examples</u> ):		
Authorized Users		Check Names
Authorized_Users		<u>C</u> heck Names
Authorized_Users		Check Names

Figure 2.10 - Select Groups

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

Select Groups	<u>?</u> ×
Select this object type:	
Groups or Built-in security principals	<u>O</u> bject Types
Erom this location:	
samcorp.com	Locations
Enter the object names to select ( <u>examples</u> ):	
Authorized Users	Check Names
<u>A</u> dvanced	OK Cancel

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.

Remote control General Address Member Of	Terminal Services Profile COM+ Account Profile Telephones Organization Dial-in Environment Sessions
Name Authorized_Users Domain Users	Active Directory Folder samcorp.com/Users samcorp.com/Users
	<u>R</u> emove
Add	Bemove         Domain Users         There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

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

			Usernai Access Control Serv Date & Til	me: admin ver: 10.24.3.50 me: Wed Jan 19 10:4	9:08 2005
Status         Rights         American Status         Control           Rights         Setup         Identity Profiles	PN MAINT LOGS Connection Profiles Au	HELP thentication Policies Access Policies	Logon Customization	Tools & Options	LOGOUT
New Authentication Service - LDAP	Name Server	Active Directory	]		
Societation and a second a	Port Base DII ( Distinguished Name ) Username Field	389 dc=samcorp.dc=com SAMAccountName	]		
Select the type of service you want to configure using the links	Group Identity Field Additional Identity Search (User's DN will replace first %s)	memberOf	] ]		
above in this column. To configure an LDAP server as an authentication service, enter a name for the authentication service and provide the required information in the fields to the right.	Timeout	5 Use a secure connection (SSL) Use LDAPv2 (Default is LDAPv3)			
Select a bind method (User bind or Non-user bind) from the Bind Method drop-down list. Then fill in the fields as appropriate for the	Bind Method User Bind String		1		
See Help for more information. When finished, click Save.	(Usemame will replace first %s)	o the above string	]		
	Save				~

Figure 2.13 – LDAP Authentication Service

 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.

			A	Username: adr coess Control Server: 10. Date & Time: We	nin 24.3.50 d Jan 19 10:58:54 2005
Startus         Rights         Startus         C           Rights         Setup         Identity         Profiles	Connection Profiles	HELP Authentication Policies	Access Policies	Logon Customization	Logout Tools & Options
Edit Authentication Policy	Name	System Authenticatio	n Policy	or new Connection Profile:	5
You can change the policy's, and add, remove or reorder the Authentication Services used in the policy.	Authentication Serv	vices			
<ul> <li>To create a new Authentication Service, click <b>New Service</b>.</li> <li>To edit an Authentication</li> </ul>	Add or remove Authen	tication Services using the I	ist below. Use the arrov Ser	v buttons to reorder service	es in the list.
button.	NT Dor	nain Logons	NT [	)omain Logons	
When finished, click Save.	802.1×	Logons	802	1x Logons	
Save As Copy saves without replacing the original.	💽 🍙 🛛 Built-in		Built	-in	
	Active	Directory	LDA	P	
	New Service				
	Save	e As Copy Cancel	3		

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.

STATUS			LOGOUT	^
Rights Setup Identity Profiles	Connection Profiles Authen	tication Policies Access Policies Logon Customization Tools & Options		
Edit Access Policy	Name Auther	nticated		
You can change an Access Policy's mane 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 Filters the Allowed Traffic Filters. Under Redirected Traffic Filters to this policy. These are processed before Allowed Traffic Filters. Under HTTP Proxy filtering and select proxy filters. Under HTTP proxy titlering and select proxy filters. Under HTTP device the traffic 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.	Settings       Allowed Traff         Configure NAT policy, IP addressic         Configure NAT policy, IP addressic         Idetoring NatT settings may cause         incorrect behavior. See Help.         IP Addressing         VLAH Identifier         Encryption         Encryption Protocols         MPPE (PPTP only)         Athentication for PPTP to L2         Athentication Folloy will be the policy associated with the Connection Profile. See Help for data.         MSCHAP	Inc.       Redirected Traffic       HTTP Proxy       Bandwidth       Timeout         Ing, and encryption requirements for this Access Policy in the fields below. See Help for       Image: See Help for         Image: I		
	Save Save As Copy	Cancel		~

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.

i n v e n t	
You are not logged on.	
Username: jused Password: •••••••	
Guests Logon as a Guest	

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).

				Usernam Access Control Servi Date & Tim	e: admin er: 10.24.3.50 e: Wed Jan 19 1	13:51:2	1 2005
Image: Series         Image: S	Logs RELP	on				(	GOUT
Client Status	Client Full Name	MAC Address Machine Name	IP Address	Access Controller	Rights Expire		
Click a client name to view detailed status.     Click a column name to sort.	(Network Equipment) AP 420-1	00:0d:9d:f6:55:98	10.24.3.62	ProCurve ACM xI 10.24.3.66	1 wk 2days	Ø	×
<ul> <li>Select filter options to view a subset of entries.</li> </ul>	juser	00:20:a6:4c:ec:1f	10.24.3.102	ProCurve ACM xI 10.24.3.66	1 wk 2days	Ø	×
configuration, click <b>Refresh User Rights Now</b> 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 <b>Help</b> for more information.	Refresh User Rights Nor	w Logout User	rs Now				
Show:							
All Access Controllers							
25 rows per page 👻							
Auto Refresh Off							
Apply Filters							

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.

Image: Network       Image
Equipment Status     Client Status     Session Status     License Information       Client Detail     User     User       Show detail status for the selected client.     User     User       See Help for more information.     Machine Name     WCC1
Client Detail     User       Show detail status for the selected client.     Username     juser       MAC Address     00:20:a6:4c:ec:11       See Help for more information.     Machine Name     WCC1
Show detail status for the selected     Username     juser       Client.     MAC Address     00:20:a6:4c:ec:11       See Help for more information.     Machine Name     WCC1
client.     MAC Address     00:20:a6:4c:ec:11       See Help for more information.     Machine Name     WCC1
See Help for more information. Machine Hame WCC1
IP Address 10.24.3.102
Address Status NAT not required: DHCP lease expires in 1 wk 23hrs
Current Access Controller ProCurve ACM xI 10.24.3.66 10.24.3.66
Installed in HP ProCurve Switch 5304XL, Slot D (No switch Management IP defined)
Port or VLAII Name (VID) Port: B1 (2000)
Uplink VLAN [Not tagged]
Sessions <u>31</u>
Idle Time Omins 46secs
Rights Expiration 1 wk 2days Fri Jan 28 20:04:41 2005
Done View User Rights View Log Refresh User Rights Now Logout User Now
Rights Row Identity Profile Connection Profile Access Policy
2 Authenticated Any Authenticated
<

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.

Service			
<u>File Action View H</u> elp			
P Internet Authentication Service (Local)	Friendly Name 🛛	Address	Protocol
	520-1	10.24.3.201	RADIUS
	1 AP420	10.24.3.202	RADIUS
	Dexter-1	10.24.3.61	RADIUS
View >	Dexter-2	10.24.3.66	RADIUS
Definada	section_4	10.24.3.80	RADIUS
Export List	. <u>♥</u> .section_5	10.24.3.81	RADIUS
Help			
	•		Þ
New Client			

Figure 3.1 – New RADIUS Client

b. Configure a Friendly name (740w1) and enter the **IP address** of the **Access Control Server** (10.24.3.50). Click Next.

New RADIUS Client		×
Name and Address		
Type a friendly name and either an I	IP Address or DNS name for the clie	nt.
Eriendly name:	740wl	
Client address (IP or DNS):		
h0.24.3.50 I		⊻erify
	< <u>B</u> ack <u>N</u> ext >	Cancel



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

ew RADIUS Client	×
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:	
Bequest must contain the Message Authenticator attribute	
< Back Finish Cancel	

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**.

🐓 Internet Authentication Service		
Eile <u>A</u> ction <u>V</u> iew <u>H</u> elp		
<ul> <li>← → È II P E E E</li> <li>P Internet Authentication Service (Local)</li> <li>RADIUS Clients</li> <li>Remote Access Logging</li> <li>Remote Access Policy</li> <li>New Remote Access Policy</li> <li>New</li> <li>Yiew</li> <li>Refresh</li> <li>Export List</li> <li>Help</li> </ul>	Name Wireless MD5 Authentication Wired MD5 for MAC Authentication Wireless EAP-TLS Authentication Connections to Microsoft Routing and Remote Connections to other access servers	Order         1           2         3           4         5           6         6
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.

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?
$\bigcirc$ 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: ACS Policy
Example: Authenticate all VPN connections
< <u>Back</u> Cancel

Figure 3.5 – New Remote Access Policy Name

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.	Ŷ
Specify the conditions that connection requests must match to be granted or denied access.	
Add	
< <u>B</u> ack <u>N</u> ext > Cance	el

Figure 3.6 – New Remote Access Policy Conditions

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

	Select Attribute		<u>?</u> ×				
Select the type of attribute to add, and then click the Add button.							
	Attribute tupes:						
	Name	Description					
	Called-Station-Id	Specifies the phone number dialed by	th				
	Calling-Station-Id	Specifies the phone number from whic	h				
	Client-Friendly-Name	Specifies the friendly name for the RAD					
	Client-IP-Address	Specifies the IP address of the RADIU	S				
	Client-Vendor	Specifies the manufacturer of the RADIL Specifies the time periods and days of w Specifies the protocol that is used.					
	Day-And-Time-Restrictions						
	Framed-Protocol						
	MS-RAS-Vendor 4の	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 u	se				
	Tunnel-Type	<ul> <li>Specifies the tunneling protocols used.</li> </ul>					
	Windows-Groups	Specifies the Windows groups that the	· · 🚽 📃				
	•						
		A <u>d</u> d Cance	el				

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.

Select Attribute	<u>? ×</u>			
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 the us			
Calling-Station-Id	Specifies the phone number from which the c			
Client-Friendly-Name	Specifies the friendly name for the RADIUS c			
Client-IP-Address	Specifies the IP address of the RADIUS clier			
Client-Vendor	Specifies the manufacturer of the RADIUS pr			
Day-And-Time-Restric	Specifies the time periods and days of week			
Framed-Protocol	Specifies the protocol that is used.			
MS-RAS-Vendor	Description not yet defined			
NAS-Identifier Specifies the string that identifies the NAS th				
NAS-IP-Address	Specifies the IP address of the NAS where the			
NAS-Port-Type	Specifies the type of physical port that is use			
Service-Type	Specifies the type of service that the user ha			
Tunnel-Type	Specifies the tunneling protocols used.			
Windows-Groups	Specifies the Windows groups that the user t			
۰I ۲۵				
	A <u>d</u> d Cancel			

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.

Select Groups	? ×
Select this object type:	
Groups	<u>O</u> bject Types
<u>F</u> rom this location:	
samcorp.com	Locations
Enter the object names to select ( <u>examples</u> ):	
Authorized Users	<u>C</u> heck Names
Advanced	OK Cancel

Figure 3.10 – New Remote Access Group

h. Back at the Policy Wizard, click next to accept the two new 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:
Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00; Tue 00:00-2 Windows-Groups matches "SAMCORP\Authorized. Users"
Add <u>E</u> dit <u>R</u> emove
< <u>B</u> ack <u>N</u> ext > Cancel

Figure 3.11 – New Remote Access Policy Conditions

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

New Remote Access Policy Wizard	×
<b>Permissions</b> A remote access policy can either grant or deny access to users who match the specified conditions.	ŷ
If a connection request matches the specified conditions: <ul> <li>Deny remote access permission</li> <li>Grant remote access permission</li> </ul>	
< <u>B</u> ack <u>N</u> ext>	Lancel

Figure 3.12 – New Remote Access Policy Permissions

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

Edit Dial-in Profile		<u>? ×</u>				
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced				
Select the authentication methods you want to allow for this connection.						
EAP Methods	EAP Methods					
Microsoft Encrypted.	Authentication version <u>2</u> (I	MS-CHAP v2)				
🔽 User can <u>c</u> har	nge password after it has e	expired				
Microsoft Encrypted.	Authentication (MS-CHAP	ŋ 🔰				
✓ User can change password after it has expired						
Encrypted authentica	ation (CHAP)					
☑ Unencrypted authen	tication (PAP, SPAP)					
Unauthenticated access						
Allow clients to connect without negotiating an authentication method.						
	OK Ca					

Figure 3.13 – New Remote Access Policy – Edit Profile

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

Ed	lit Dial-in Profile			<u>?</u> ×
	Dial-in Constraints	∫ IP	Multilink	4
Authentication Specify additional connection		Encryption attributes to be return	ned to the Remote	
	Attributes:			
	Name	Vendor	Value	
	Service-Type Framed-Protocol	RADIUS Standard RADIUS Standard	Framed PPP	
	•			•
	Add	<u>R</u> emove		
	.0			
-		ок (	Cancel App	oly

Figure 3.14 – New Remote Access Policy – Edit Profile Advanced

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

1. M. C. 197		
.ttri <u>b</u> ute: Name	Vendor	Description
Acct-Interim-Interval	RADIUS Standard	Specifies the length of the interval (in seconds) between e
Callback-Number	RADIUS Standard	Specifies the callback phone number.
Class	RADIUS Standard	Specifies the classification of accounting records.
Filter-Id	RADIUS Standard	Specifies the name of filter list for the user requesting authors
Framed-AppleTalk-Link	RADIUS Standard	Specifies the AppleTalk network number for the link to the
Framed-AppleTalk-Network	RADIUS Standard	Specifies the AppleTalk network number that the NAS mu
Framed-AppleTalk-Zone	RADIUS Standard	Specifies the AppleTalk default zone for the user.
Framed-Compression	RADIUS Standard	Specifies the compression protocol that is used.
Framed-IP-Netmask	RADIUS Standard	Specifies the IP subnet mask that is configured for the use
Framed-IPX-Network	RADIUS Standard	Specifies the IPX network number configured on the NAS
Framed-MTU	RADIUS Standard	Specifies the maximum transmission unit (MTU) that is con
Framed-Pool	RADIUS Standard	Specifies the name of an assigned address pool that shoul
Framed-Protocol	RADIUS Standard	Specifies the protocol that is used.
Framed-Route	RADIUS Standard	Specifies the routing information that is configured on the N
Framed-Routing 🏼 🗏 🖌	RADIUS Standard	Specifies the routing method that is used by the user.
Login-IP-Host	RADIUS Standard	Specifies the IP address of the host to which the user sho
Login-LAT-Group	RADIUS Standard	Specifies the Local Area Transport (LAT) group codes for
Login-LAT-Node	RADIUS Standard	Specifies the node to which user is connected by the Loca

Figure 3.15 – New Remote Access Policy – Attribute

m. Configure the **Attribute Information** value with the group information (Authorized\_Users) and click OK.

Attribute Information	<u>? ×</u>
Attribute name:	
Login-LAT-Group	
Attribute number:	
36	
Attribute format:	
OctetString	
Enter the attribute value in:	O <u>H</u> exadecimal
Authorized_Users	
	OK Cancel

Figure 3.16 – New Remote Access Policy – Login LAT Group

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

Edit Dial-in Profile			? ×
Dial-in Constraints	IP	Multilink	1
Authentication	Encryption	Advanced	
Specify additional connection	attributes to be return	ned to the Remote	
Access server.			
Attri <u>b</u> utes:			_
Name	Vendor	Value	
Service-Type	RADIUS Standard	Framed	
Framed-Protocol	RADIUS Standard	PPP	
Login-LAT-Group	RADIUS Standard	Authorized_Users	
•			
			-
Add Edit			
	OK (	Cancel Ap	ply

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

invent.			Username: Access Control Server: Date & Time:	admin 10.24.3.50 Thu Jan 20 11:04:56 2005
STATUS         Image: Constraint of the state of th	PN NIMIT LOSS	HELP Authentication Policies Access Policies	Logon Customization	Logour
Edit	Name	IAS		
Authentication	Server	10.24.3.10		
Service - RADIUS	Port	1812		
<ul> <li>▶ 802.1x</li> <li>▶ Kerberos</li> <li>▶ LDAP</li> </ul>	Secret Confirm Secret	•••••		
RADIUS	Group Identity Field	Login-LAT-Group		
► XML-RPC	Reauthentication Field	Session-Timeout		
You can change the name of the authentication service and the information in any of the fields to the right.	Timeout (Seconds)	5 Supports Microsoft Attributes (RFC-2548)		
To use the RADIUS service for accounting, click <b>Enable RADIUS</b> Accounting and provide a port number.	Save Save A	Enable RADIUS Accounting (RFC-2866) on	port 1813	
See Help for more information.				
When finished, click <b>Save</b> . Save As Copy saves without replacing the original.				
				~

Figure 3.18 – RADIUS Authentication Service

 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
STATUS	PN MAINT LOGS HELP	Logout
Rights Setup Identity Profiles	Connection Profiles Authentication Policies A	ccess Policies Logon Customization Tools & Options
Edit Authentication Policy	Name System Authentication Police	Cy entication Policy for new Connection Profiles
You can change the policy's, and add, remove or reorder the Authentication Services used in the policy. • To create a new Authentication	■ ow. Use the arrow buttons to reorder services in the list.	
Service, click <b>New Service</b> . To edit an Authentication	Authentication Service	Service Type
Service, click its name or the pencil button.	NT Domain Logons	NT Domain Logons
When finished, click Save,	802.1x Logons	802.1× Logons
Save As Copy saves without replacing the original	💌 🥽 Built-in	Built-in
	Active Directory	LDAP
	🗹 🍧 IAS	RADIUS
	New Service Save As Copy Cancel	
		×

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.

	invent	
-	You are not logged on.	
	And the second second	
	Registered Users	
	Usemame: jused Password: •••••••	
	Logon User	
	Guests	
	Logon as a Guest	

Figure 3.20 – Logon Page

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).

				Username Access Control Server Date & Time	: admin : 10.24.3.50 : Thu Jan 20 1)	0:56:09	9 2005
RIGHT REGIST OF UPN	LOGS RELP					Ę.	GOUT
Equipment Status Client Status Session St	atus License Informati	ion				_	_
Client Status	Client Full Name	MAC Address Machine Name	IP Address	Access Controller	Rights Expire		
<ul> <li>Click a client name to view detailed status.</li> <li>Click a column name to sort.</li> </ul>	(Network Equipment) AP 420-1	00:0d:9d:f6:55:98	10.24.3.62	ProCurve ACM xI 10.24.3.66	1 wk 2days	Ø	×
Select filter options to view a subset of entries.	juser	00:20:a6:4c:ec:20	10.24.3.104	ProCurve ACM xI 10.24.3.66	1 wk 2days	G	×
If you have made changes to your nights configuration, click <b>Refresh User Rights Now</b> 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 <b>Help</b> for more information.	Refresh User Rights No	w Logout Us	ers Now				_
Show:							
All Access Controllers							
All Clients							
25 rows per page 💌							
Auto Refresh Off 🛛 👻							_
Apply Filters							

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.

Envent .			Access Con C	Username: admin rol Server: 10.24.3.50 ate & Time: Thu Jan 20 10:56:44 2005
Equipment Status Client Status	N MAINT Logs	HELP e Information		LOGOUT
Client Detail Show detail status for the selected	User Username	juser		
See Help for more information.	MAC Address Machine Name IP Address	00:20:a6:4c:ec:20 wcc10 10.24.3.104		
	Address Status Current Access Controller	NAT not required: DHCP ProCurve ACM xI 10.24.3 10.24.3.66	lease expires in 1 wk 23hrs 3.66	
	Installed in	HP ProCurve Switch 530	14XL, Slot D (No switch Manageme	nt IP defined)
	Port or VLAN Name (VID)	Port: B1 (2000)		
	Uplink VLAN	[Not tagged]		
	Sessions	<u>28</u>		
	Idle Time	1min 4secs		
	Rights Expiration	1wk 2days Sat Jan 2917:09:22 200:	5	
	Done View User	Rights View Log	Refresh User Rights Now	Logout User Now
	Rights Row Ident	uty Profile	Connection Profile	Access Policy
	2 Authe	enticated	Any	Authenticated
<				>

Figure 3.22 – Client Detail Page

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

www.procurve.com



©Copyright 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

March 2005