# Getting Started Guide

# HP ProCurve Secure Access 700wl Series

www.hp.com/go/hpprocurve

# HP ProCurve

# Secure Access 700wl Series

## Getting Started Guide

**Publication Number**

5990-3104
July 2003
Edition 1

**Applicable Products**

| | |
|---|---|
| HP ProCurve Access Controller 720wl | (J8153A) |
| HP ProCurve Access Control Server 740wl | (J8154A) |
| HP ProCurve Integrated Access Manager 760wl | (J8155A) |
| HP ProCurve 700wl 10/100 Module | (J8156A) |
| HP ProCurve 700wl Gigabit-SX Module | (J8157A) |
| HP ProCurve 700wl Gigabit-LX Module | (J8158A) |
| HP ProCurve 700wl 10/100/1000Base-T | (J8159A) |
| HP ProCurve 700wl Acceleration Module | (J8160A) |

**Trademark Credits**

Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

**Disclaimer**

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

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.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

**Warranty**

See the Customer Support / Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

# CONTENTS

# INTRODUCTION 1

This document provides instructions for a basic configuration of the HP ProCurve Secure Access 700wl Series that allows a demonstration user to:

- Connect to the 700wl Series system using a secure protocol (PPTP)
- Log in and be authenticated through the HP ProCurve 700wl Series built-in database
- Pass IP traffic and have access to network resources

A system running with this configuration is suitable for basic evaluation or demonstration purposes. Two types of deployment are described in this document; one using the Access Control Server 740wl and Access Controller 720wl, and the other for the stand-alone Integrated Access Manager 760wl.

This document may be used as a supplement to the *HP ProCurve Secure Access 700wl Series Quick Start Guide* shipped with each 700wl Series unit, which covers the basic installation and network configuration of the 700wl Series system components.

The instructions provided here include configuring the 700wl Series system to function as a VPN gateway, which allows the user to secure the connection via encryption using a protocol such as PPTP. User authentication as described in this document is based on either HP's simple built-in database, or optionally on an external RADIUS authentication server.

***Note:*** *This configuration does not require the use of an Access Point. The demonstration user connects to the 700wl Series system directly through a downlink port on the Access Controller 720wl or Integrated Access Manager 760wl.*

## Objectives

This document will guide you to accomplish the following:

- Install the components of the 700wl Series system onto your network
- Configure the 700wl Series system to create a demonstration user account ("demouser") that will be authenticated through the HP built-in user database
- Configure the 700wl Series system as a VPN gateway using PPTP encryption
- Configure a Windows client system to establish a network connection using the PPTP protocol
- Connect to the 700wl Series system as a client using the PPTP protocol, and authenticate the demonstration user ("demouser") against the built-in database
- (Optional) Configure the 700wl Series system to use an AAA RADIUS server for user authentication

# 2 DEPLOYING AN ACCESS CONTROL SERVER 740WL AND ACCESS CONTROLLER 720WL

## Procedure Overview

To accomplish the objectives listed in the Introduction to this document, these instructions lead you through the following steps:

**Step 1.** Install the 700wl Series system consisting of an Access Control Server 740wl and an Access Controller 720wl onto your network. If you are comfortable using the command language interface (CLI), you can follow the instructions in the *HP ProCurve Secure Access 700wl Series Quick Start Guide* that was included with your 700wl Series hardware. Otherwise, follow the instructions in Step I "Hardware Setup" on page 2-2.

**Step 2.** Create a "normal" user account (login ID and password) in the Rights Manager's built-in database.

**Step 3.** Connect a Windows client system to the 700wl Series system through a downlink port of the Access Controller 720wl. Log in as the user created in Step 2 against the built-in database using the 700wl Series system Logon page. The user should then have full IP access to the network. This shows that the user can successfully connect to the system and gain network access.

**Step 4.** Configure the 700wl Series system as a VPN gateway using PPTP encryption.

**Step 5.** Configure the Windows client to establish a PPTP connection with the 700wl Series system. Then connect to the 700wl Series system using the PPTP connection process. Again, this shows that the client can connect to the system and gain access to the network.

**Step 6.** (Optional) Log the client off the system.

**Step 7.** (Optional) Configure the 700wl Series system to use an AAA RADIUS server for user authentication.

**Step 8.** (Optional) Log in using a user account known to the RADIUS authentication server, and verify network access.

## Preparation

Before you begin the system installation and configuration process, review the following list to make sure you have the required components available and/or configured as specified:

**Step 1.** One Windows-based PC or laptop preset to obtain an IP address automatically (via DHCP). This system will be used both to perform the configuration of your HP

ProCurve Access Control Server 740wl and Access Controller 720wl, and to function as a client once the configuration is complete.

**Step 2.** Three standard (straight-through) Ethernet cables for the Network Uplinks of the Access Control Server 740wl, Access Controller 720wl, and to connect the PC/laptop to the Access Controller.

**Step 3.** A DHCP server that can provide IP configuration information for the Access Control Server 740wl and Access Controller 720wl Network Uplinks.

> ***Note:*** *If no DHCP server is available, then you must configure a static IP address for the Network Uplink port of each unit. Configuration parameters include: IP address, subnet mask, default router's IP address, and DNS server's IP address.*

**Step 4.** (Optional) One DB-9 Null Modem cable, required only if you plan to use the CLI to set up a static IP address, or if you intend to do the initial network configuration following the procedure in the Quick Start Guide.

**Step 5.** (Optional) One AAA RADIUS server. You must configure the RADIUS server to accept authentication requests from the Access Control Server 740wl, which acts as a RADIUS client. A user account must be created in the RADIUS database. Consult the online *HP ProCurve Secure Access 700wl Series Configuration and Management Guide* for more information on other supported external authentication servers.

# Step I. Hardware Setup

> ***Note:*** *These steps duplicate much of the information found in the HP ProCurve 700wl Series Quick Start Guide. If you have already set up your system following the instructions in the Quick Start Guide, you can skip to Step V "Creating a User Account in the Built-In Database" on page 2-5.*

**Step 1.** Connect the power cord to the Access Control Server 740wl (rear side) and into an electrical outlet.

**Step 2.** Connect the power cord to the Access Controller 720wl (rear side) and into an electrical outlet.

**Step 3.** Connect Ethernet cables to the Network Uplink ports of the Access Control Server 740wl and Access Controller 720wl, respectively. The other ends of the cables are plugged into a Hub or Switch port on the internal (secured) network.

**Step 4.** Power on the two units and wait approximately 60 seconds or until they are completely booted (by observing the status on the LCD panel of each unit).

**Step 5.** Connect the remaining Ethernet cable from the configuration PC to a Hub or Switch port on the internal (secured) network and then power on the PC. Note that the PC should receive an IP address from a DHCP server in the internal network.

**Step 6.** To configure your 700wl Series units with static IP addresses, continue with "Static IP Configuration for the Access Control Server (Optional)".

If you plan to use the IP address provided by DHCP, skip to Step IV, "Configuring the Shared Secret Authorization" on page 2-4.

# Step II. Static IP Configuration for the Access Control Server (Optional)

If you want your Access Control Server to use a static IP address, and you have not already configured the unit using the instructions in the *HP ProCurve Secure Access 700wl Series Quick Start Guide*, do the following:

**Step 1.** Connect the Null Modem cable to the Serial Console port of the Access Control Server 740wl and into a COM port, such as COM1, of the Windows PC.

**Step 2.** Start a terminal emulation program such as HyperTerminal in Microsoft Windows, and set the COM port properties to 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

**Step 3.** Initialize the terminal connection. A Login prompt appears in the terminal window.

**Step 4.** Logon to the system as the administrator. The default login is `admin` with password `admin`.

**Step 5.** Enter the following commands:

| CLI Command | Example |
|---|---|
| `set ip <ipaddress> [<netmask>]` | `set ip 192.168.10.71 255.255.255.0` |
| `set gateway <ipaddress>` | `set gateway 192.168.10.254` |
| `set dns <ipaddress> [<ipaddress>]` | `set dns 192.168.2.250 192.168.31.123` |

# Step III. Static IP Configuration for the Access Controller (Optional)

To give your Access Controller a static IP address, if you have not already configured the unit using the instructions in the *HP ProCurve Secure Access 700wl Series Quick Start Guide*, do the following:

**Step 1.** Connect the Null Modem cable to the Serial Console port of the Access Control Server 740wl and into a COM port, such as COM1, of the Windows PC.

**Step 2.** Start a terminal emulation program such as HyperTerminal in Microsoft Windows, and set the COM port properties to 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

**Step 3.** Initialize the terminal connection. A Login prompt appears in the terminal window.

**Step 4.** Logon to the system as the administrator. The default login is `admin` with password `admin`.

**Step 5.** Enter the following commands:

| CLI Command | Example |
|---|---|
| `set ip <ipaddress> [<netmask>]` | `set ip 192.168.10.71 255.255.255.0` |
| `set gateway <ipaddress>` | `set gateway 192.168.10.254` |
| `set dns <ipaddress> [<ipaddress>]` | `set dns 192.168.2.250 192.168.31.123` |

# Step IV. Configuring the Shared Secret Authorization

The shared secret is used by the Access Control Server to validate the association with an Access Controller. The shared secret you configure on the Access Control Server must also be entered on each Access Controller that will attempt to associate with this Access Control Server.

**Step 1.** Start your web browser and set it to the IP address of the Access Control Server: `http://<IPaddress>`, for example, `http://192.168.10.71`. The Administrator Login page appears.

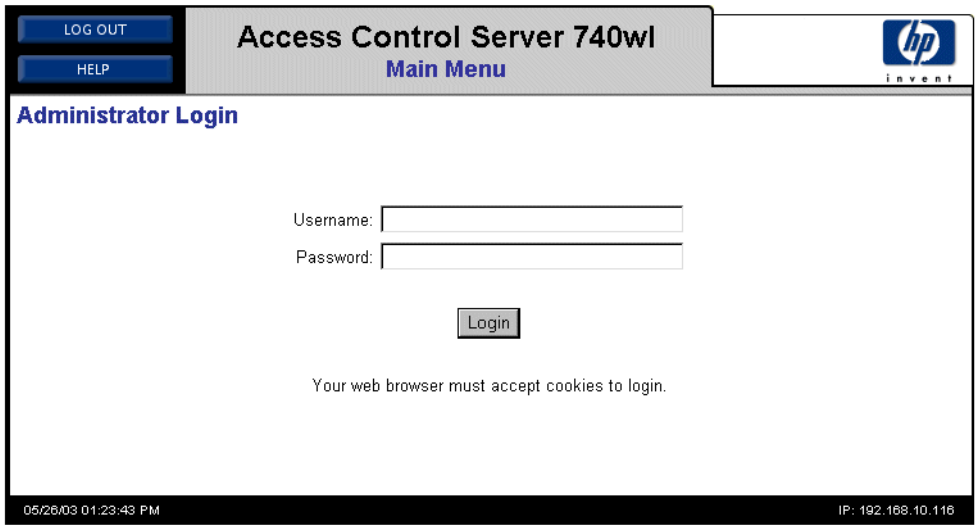


**Figure 2-1. Administrator Login page**

**Step 2.** Enter the default Administrator Username and Password (`admin` and `admin`) in the appropriate fields, then click **Login**. The **Main** Menu appears.

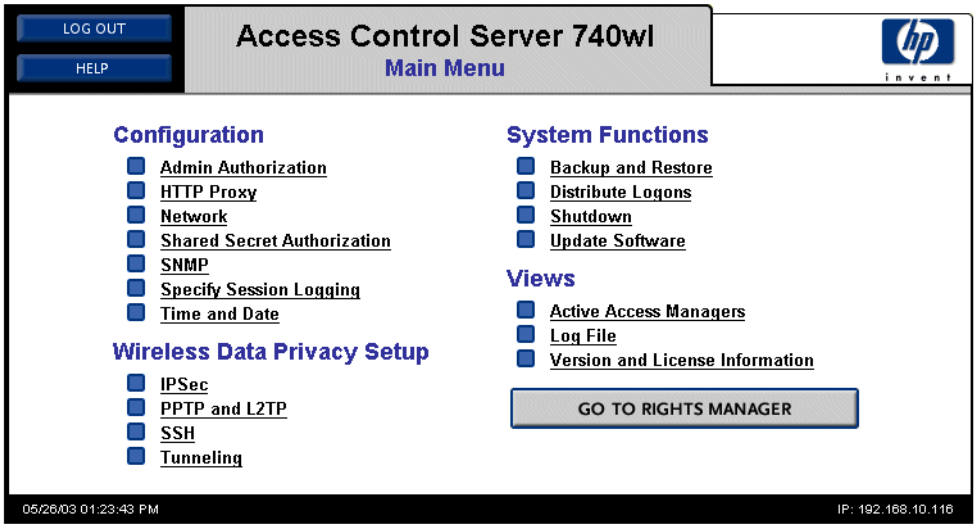


**Figure 2-2. Main Menu**

**Step 3.** Click **Shared Secret Authorization**.

The Shared Secret Authorization Configuration page appears.

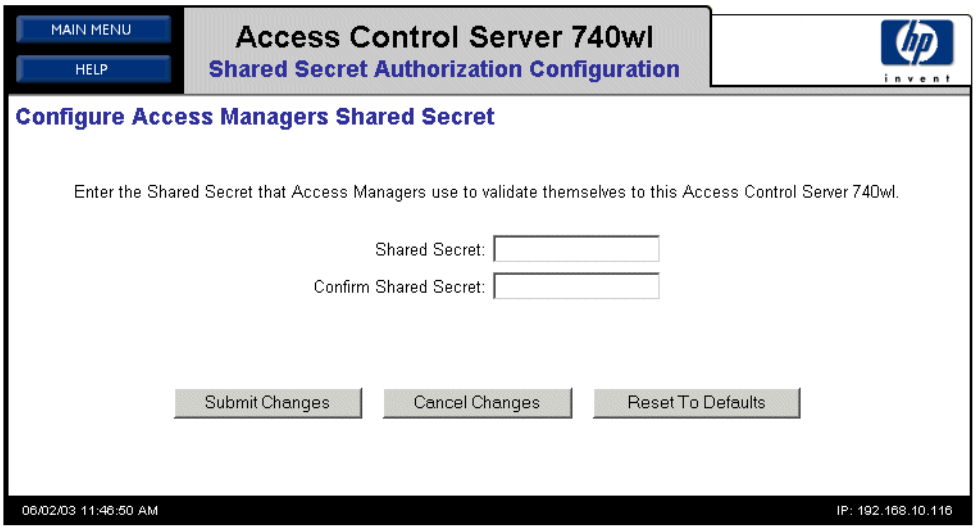


**Figure 2-3. Shared Secret Authorization Configuration page**

**Step 4.** Enter the shared secret text into the **Shared Secret** and **Confirm Shared Secret** fields and click **Submit Changes**.

**Step 5.** Click the **MAIN MENU** button (in the upper-left corner of the page) to return to the **Main** Menu.

# Step V. Creating a User Account in the Built-In Database

In order for a user to log in, the 700wl Series system must be able to authenticate the user through some authentication service. The simplest form of authentication service is the built-in database included in the 700wl Series system Rights Manager. In this step, you add a user to the built-in database so you can login to your network as that user through the 700wl Series system.

**Step 1.** From the **Main** Menu, click **GO TO RIGHTS MANAGER**.

**Step 2.** The Rights Manager Clients page appears.

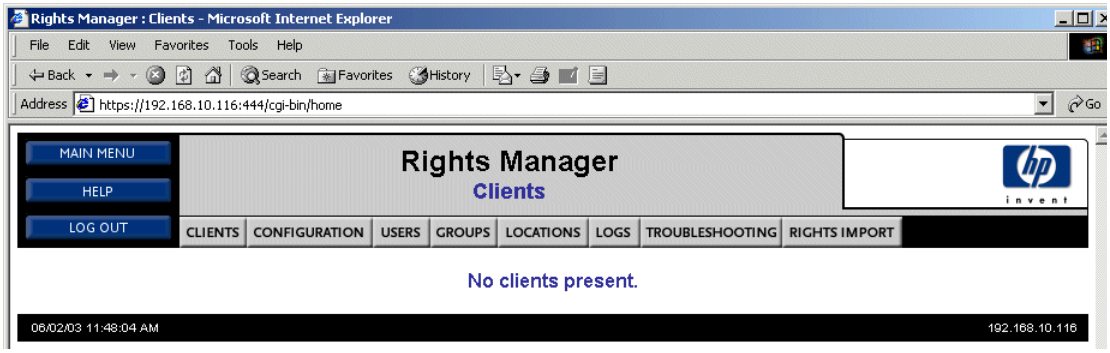


**Figure 2-4. Rights Manager Clients page**

**Step 3.** Click **USERS** at the top of the page.

The Users page appears, with an empty Users list.


**Figure 2-5. Users page**

**Step 4.** Click the **Go To the User Editor** link (see Figure 2-6).€

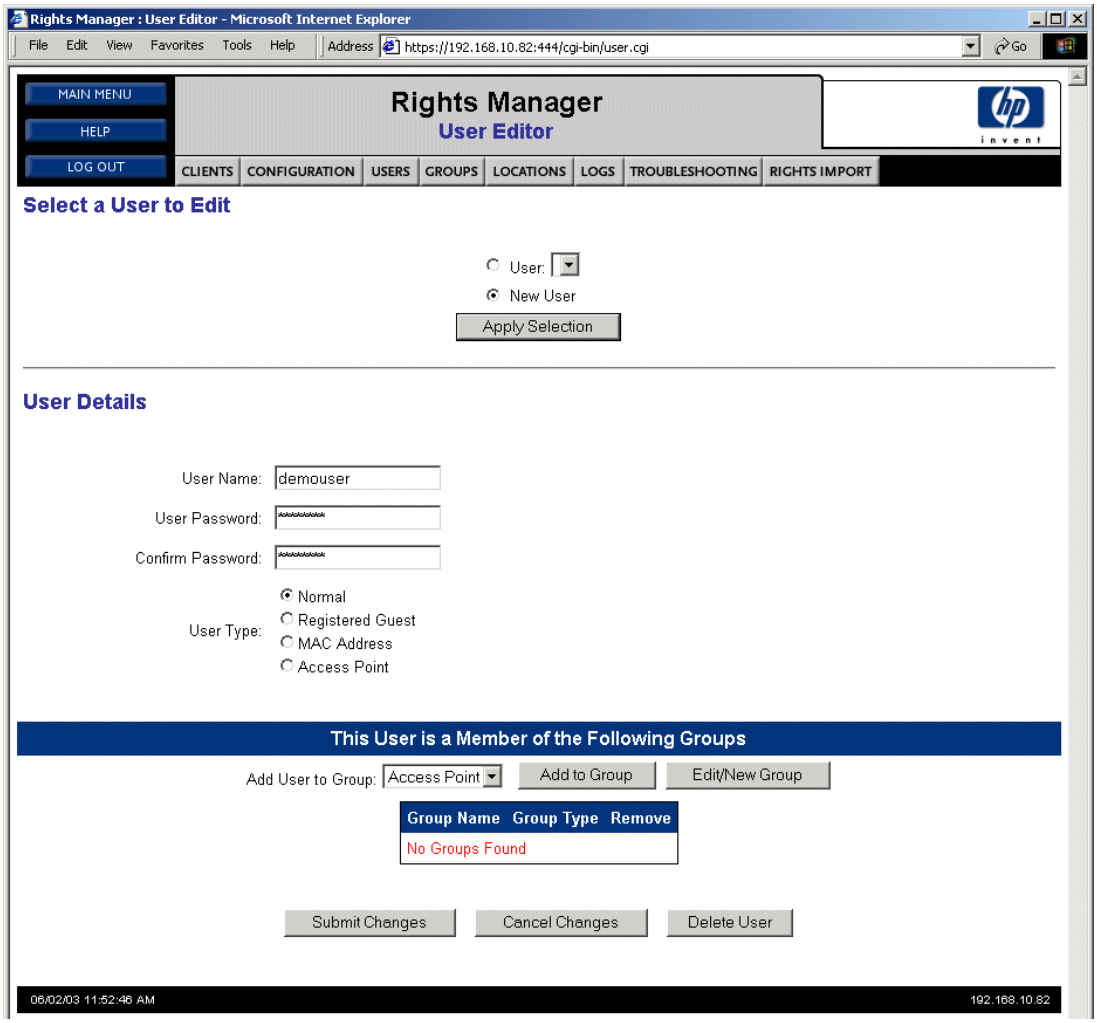


**Figure 2-6. User Editor page**

**Step 5.** Enter the following information:

- **User Name:** "demouser" (or any name you like)
- **User Password:** "password" (or any password you like)
- **Confirm Password:** "password" (must be the same as that entered into the first password field)

**Step 6.** Click **Submit Changes**.

# Step VI. Associating the Access Controller 720wl to the Access Control Server 740wl

In order to authenticate users and receive access rights for those users, you must enable communication between the Access Controller and the Access Control Server.

**Step 1.** Set your web browser to the IP address of the Access Controller: `http://<IPaddress>`, for example, `http://192.168.10.66`. The Administrator Login page appears.

**Step 2.** Enter the default Administrator Username and Password (`admin` and `admin`) in the appropriate fields, then click **Login**. The Access Controller **Main Menu** appears.

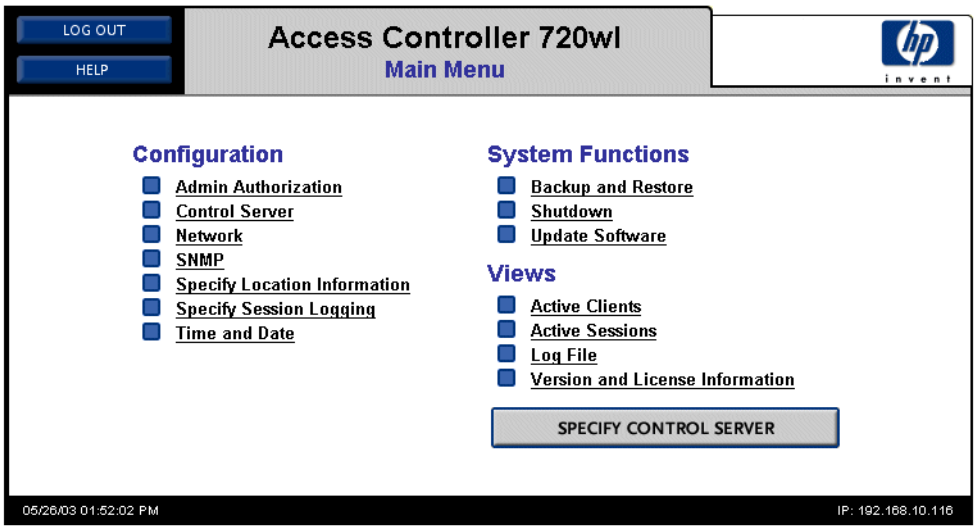


**Figure 2-7. Access Controller Main Menu**

**Step 3.** Click **Control Server**.

The Specify Access Control Server page appears.


**Figure 2-8. Specify the Access Control Server shared secret**

**Step 4.** Enter the following information:

- **Access Control Server IP Address:** the IP Address of the Access Control Server
- **Shared Secret:** the shared secret that you defined for the Access Control Server
- **Confirm Shared Secret:** type the shared secret a second time

**Step 5.** Click **Submit Changes**.

**Step 6.** Click **GO TO CONTROL SERVER**.

If the settings are correct, the Administrator Login page of the Access Control Server appears in your browser.

# Step VII. User Authentication Through the 700wl Series Logon Page

In the following steps, the Windows PC you have been using for configuration will also be used as a client system. If the PC's network interface is configured to use a static IP address, you must change its properties so that it will obtain an IP address automatically using DHCP.

In this step, you connect your Windows PC to an Access Controller port and log onto your network using the username and password you added to the built-in database. If this is successful, you should be able to access the Internet and other resources on your network as usual.

**Step 1.** Release the IP configuration (in Windows) from the network interface of the configuration PC/laptop as follows:

From the **Start** menu, click **Run...** then enter the command `ipconfig /release`.

**Step 2.** Unplug the Ethernet cable connecting the PC to your network through the Hub/Switch port and plug it into one of Access Controller 720wl's downlink ports.

**Step 3.** Obtain a new IP configuration from DHCP through the Access Controller 720wl:

From the **Start** menu, click **Run...** then enter the command `ipconfig /renew`.

The PC should receive an IP address in the `42.x.x.x` range.

**Step 4.** Start your web browser and go to any web site. The web browser will display the 700wl Series Logon page:

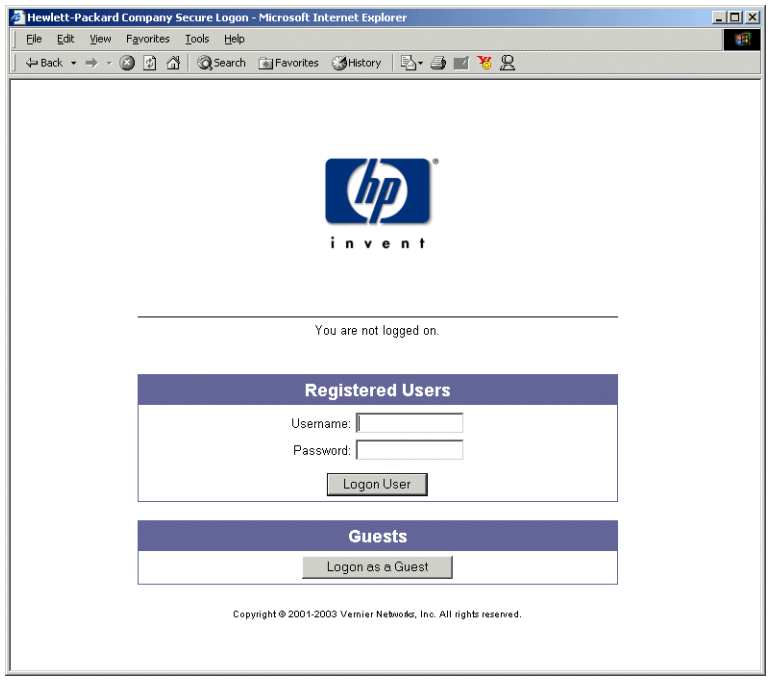


**Figure 2-9. HP ProCurve 700wl Series Login page**

**Step 5.** Enter “demouser” and “password” (or the username and password you created) in the **Username** and **Password** fields and click **Logon User**.

At this point, the web page you requested should appear, and you should be able to access the network normally.

# Step VIII. PPTP Gateway Configuration (Access Control Server 740wl)

This step configures the 700wl Series system to act as a VPN termination for PPTP. After configuring the PPTP client on your PC (see Step IX, “PPTP Client Configuration (Windows XP)”), you should be able to logon to the network via the PPTP connection interface.

**Step 1.** Set your web browser to the IP address of the Access Control Server: `http://<IPaddress>`, for example, `http://192.168.10.71`. The Administrator Login page appears.

**Step 2.** Enter the default Administrator Username and Password (`admin` and `admin`) in the appropriate fields, then click **Login**. The Access Control Server **Main** Menu appears.

**Step 3.** Click the **PPTP and L2TP** link in the Airwave Security Setup section of the **Main** Menu.

**Step 4.** The PPTP and L2TP Configuration page appears.

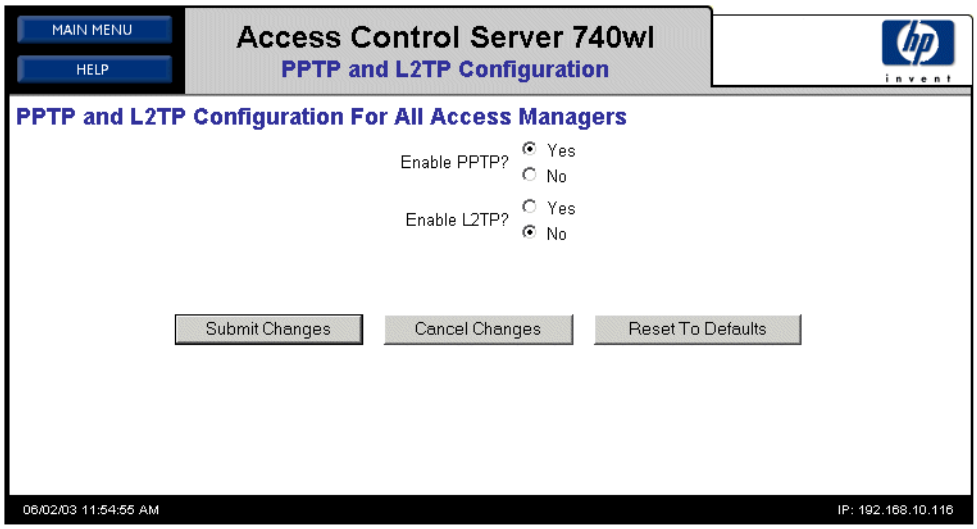


**Figure 2-10. PPTP and L2TP Configuration page**

**Step 5.** Click **Yes** to **Enable PPTP?** and then click **Submit Changes**.€

**Step 6.** Click **MAIN MENU** to return to the **Main** Menu.€

**Step 7.** Click **GO TO RIGHTS MANAGER**.€

**Step 8.** The Rights Manager Clients page appears. €

**Step 9.** Click **CONFIGURATION** at the top of the page. The Configuration page appears.€

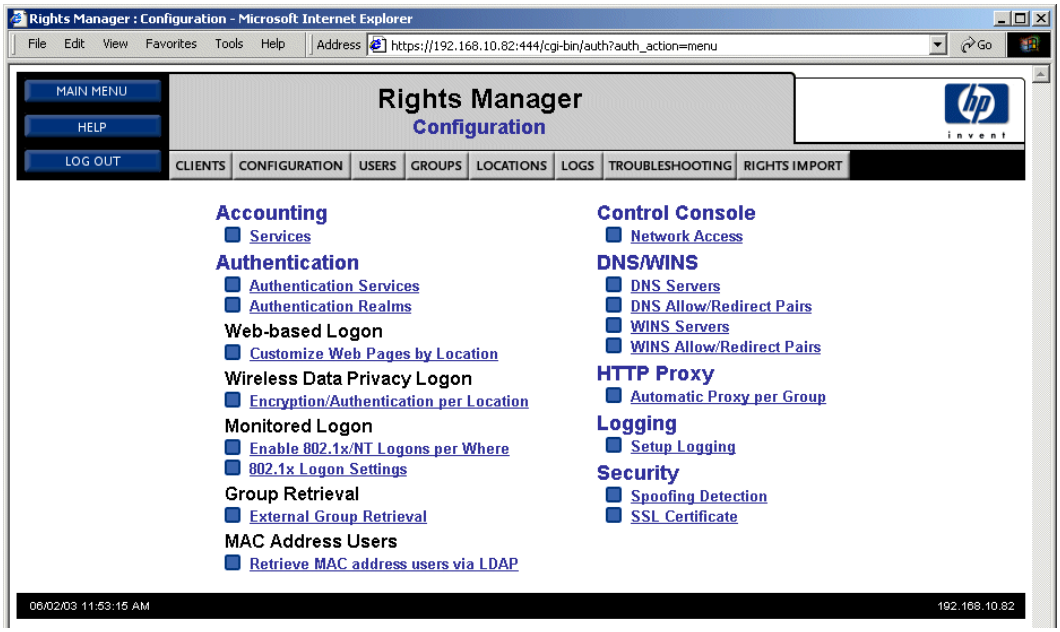


**Figure 2-11. Rights Manager Configuration page**

**Step 10.** Click the **Encryption/Authentication per Location** link. The Encryption / Authentication per Location page appears.


**Figure 2-12. Encryption/Authentication per Location page**

**Step 11.** Click the **IPSec Allowed** link in the Encryption column for the **Everywhere Else** location.

**Step 12.** In the Specify Encryption per Location page, select the **Allow the following protocols** option and then select **PPTP** from the panel to the right.

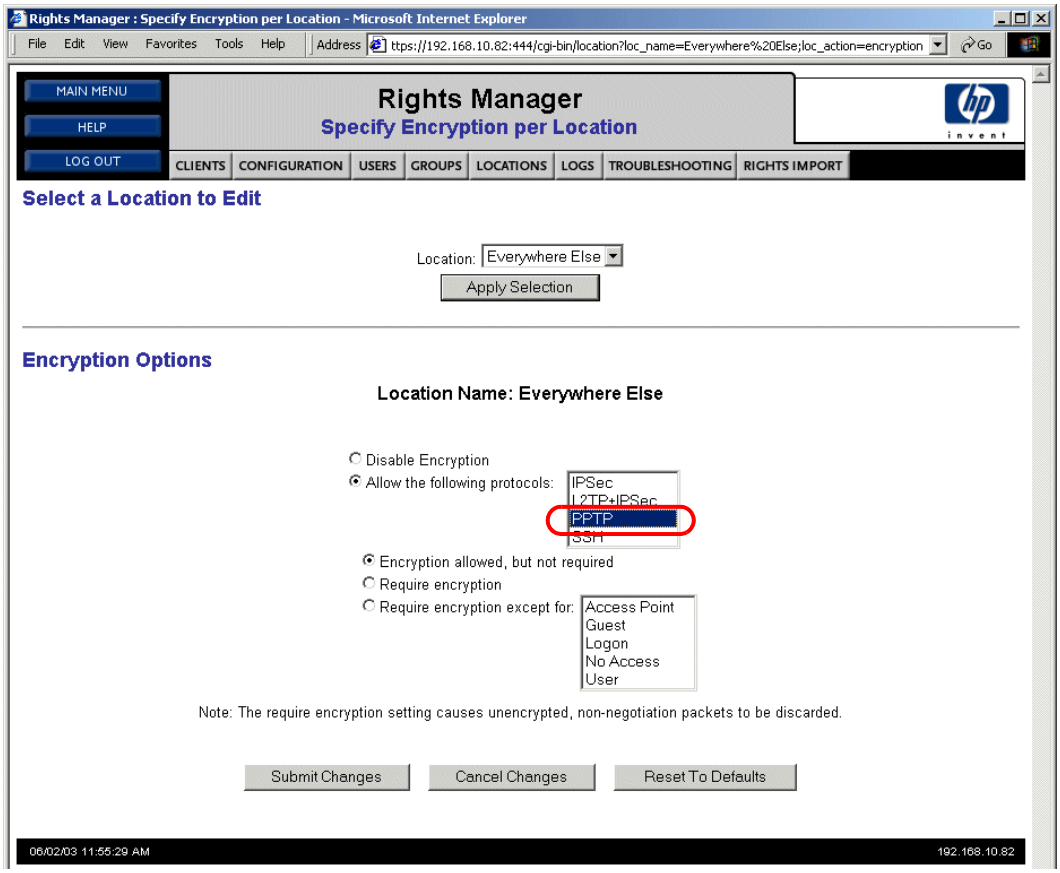


**Figure 2-13. Specifying Encryption Options for a location**

**Step 13.** Click **Submit Changes**.€

**Step 14.** Click **CLIENTS** to return to the Rights Manager's Clients page.€

**Step 15.** Click the **Refresh every client's rights** link.€

# Step IX. PPTP Client Configuration (Windows XP)

This step configures the PPTP client on the Windows PC:

**Step 1.** Open the Network Connections window:

- Click the **Start** button and select **Control Panel**.
- From the Control Panel window, double-click **Network Connections**.

The Network Connections window appears.

**Step 2.** Click the **Create a new connection** link on the Network Tasks panel.

The New Connection Wizard window appears.

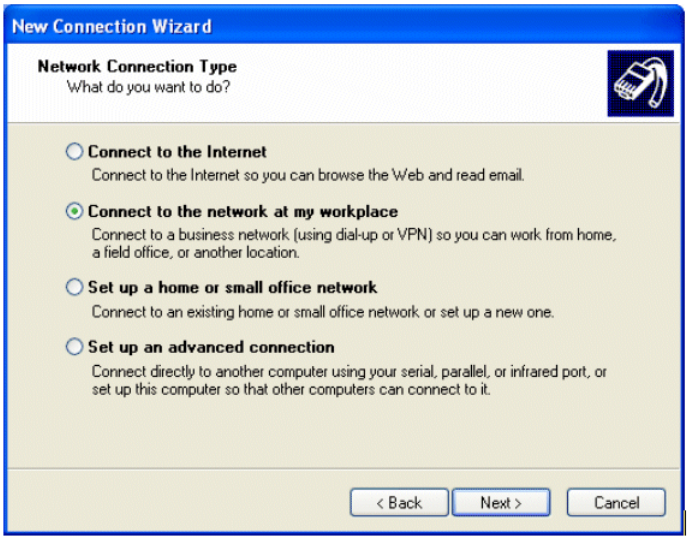


**Figure 2-14. Network Connection Type page**

**Step 3.** Click **Next>** to go to the Network Connection Type page.

**Step 4.** Select the **Connect to the network at my workplace** option and then click **Next>**.

**Step 5.** Select the **Virtual Private Network connection** option. Click **Next>**.

**Step 6.** Enter the desired connection name in the **Company Name** textbox and then click **Next>**.

**Step 7.** The Public Network page appears. Select the **Do not dial the initial connection** option and then click **Next>**.

**Step 8.** You should now be at the VPN Server Selection window (see Figure 2-15). Enter `42.0.0.1` in the **Host name or IP address** text box and then click **Next>**.

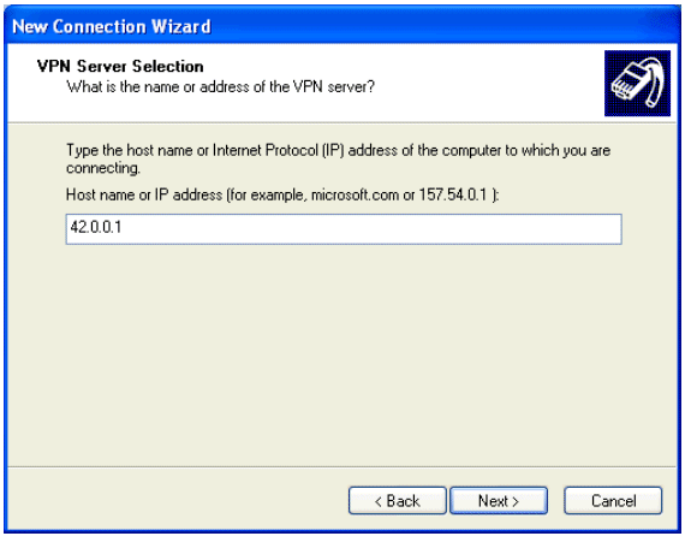


**Figure 2-15. New Connection Wizard, VPN Server Selection**

**Step 9.** The Completing the New Connection Wizard page appears. You may choose to add a shortcut to this connection to the desktop, then click **Finish**.

An icon representing the new connection appears in the Network Connections window under the Virtual Private Network section. In addition, the Sign-on window should appear on the screen; if it does not, double-click the new connection icon.


**Figure 2-16. Sign-on window**

**Step 10.** Click the **Properties** button to open the connection's properties window.

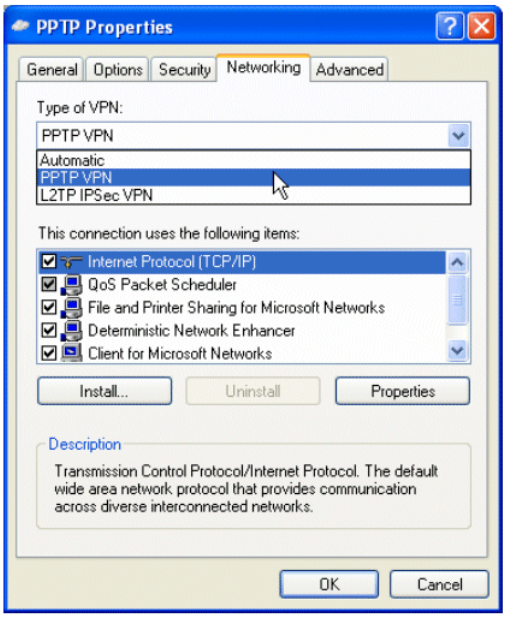


**Figure 2-17. PPTP Properties window**

**Step 11.** Click the Networking tab to specify the type of VPN.

**Step 12.** Pull down the **Type of VPN** menu and select **PPTP VPN**. Make sure that **Internet Protocol (TCP/IP)** is selected.

**Step 13.** Click the Security tab to customize the security protocols.

**Step 14.** Select **Advanced (custom settings)** and then click the **Settings** button.

The Advanced Security Settings window appears.

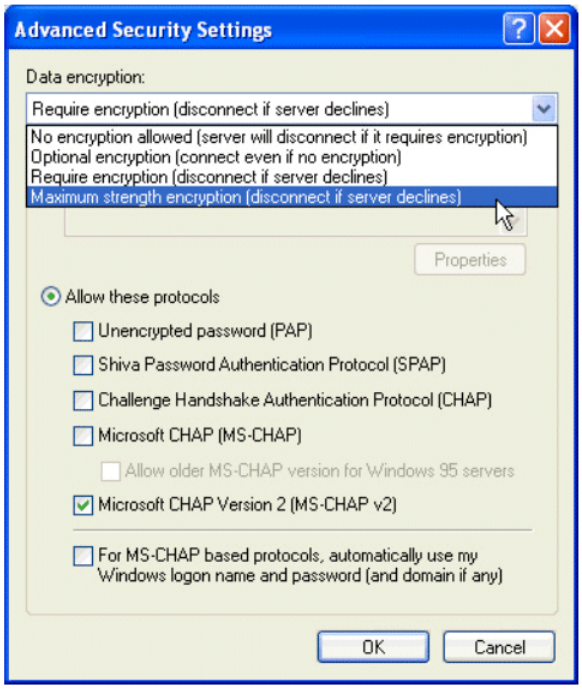


**Figure 2-18. Advanced Security Settings window**

**Step 15.** Deselect the **Microsoft CHAP (MS-CHAP)** protocol option (this protocol is selected by default). Leave **Microsoft CHAP Version 2 [MS-CHAP v2]** selected. Only MS-CHAP v2 is used with the 700wl Series system.

**Step 16.** Pull down the **Data Encryption** menu and select **Maximum strength encryption (disconnect if server declines)**. This sets the length of the encryption key to 128 bits.

**Step 17.** Click **OK** to go back to the connection's properties window.

**Step 18.** Click **OK** to go back to the Connect window.

**Step 19.** You may skip Step X, "Logoff (Optional)" if you do not wish to practice the logoff procedure. Otherwise, click **Cancel** to close the Connect window.

# Step X. Logoff (Optional)

**Step 1.** Set your web browser to the URL `http://1.1.1.1`. The 700wl Series Logon page appears showing "demouser" as logged on.

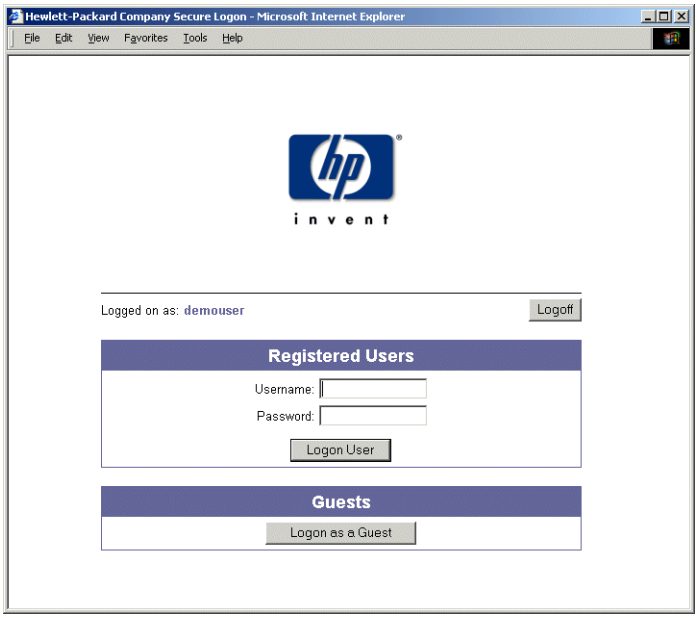


**Figure 2-19. HP ProCurve 700wl Series Logon page for a logged on user**

**Step 2.** Click the **Logoff** button (at the right of the window) to log user "demouser" off the system.

# Step XI. User Authentication Via PPTP Connection

Before starting the VPN connection, make sure your system has established a network connection with the server. You may use the `ipconfig` command to verify the IP settings and/or use the `ipconfig /renew` command to obtain an IP configuration from the Access Control Server 740wl.

**Step 1.** Open the PPTP connection created in Step IX "PPTP Client Configuration (Windows XP)" using the shortcut on your desktop or from the Network Connections window in the Control Panel.

The Connect window appears.

**Step 2.** Type "demouser" and "password" (or the user name and password you created in the built-in database) in the **Username** and **Password** fields, and click **Connect** to connect to the server. You may choose to save this username and password for future use before clicking the **Connect** button.

After the connection is successfully made, the connection icon appears in the notification area on the lower-right corner of the screen.

# Step XII. External Authentication Service Configuration (Optional)

If you use an external RADIUS authentication service and your user account already exists in the RADIUS server's database, you can configure the 700wl Series system to authenticate using the RADIUS server rather than the built-in database.

Once you have successfully completed this configuration, you should be able to logon to the network through the 700wl Series system using any legitimate username and password recognized by your RADIUS server.

To configure the Rights Manager to use a RADIUS server for authentication, do the following:

**Step 1.** Set your web browser to the IP address of the Access Control Server: `http://<IPaddress>`, for example, `http://192.168.10.71`. The Administrator Login page appears.

**Step 2.** Type the default Administrator Username and Password (`admin` and `admin`) in the appropriate fields, then click **Login**. The Access Control Server Main Menu appears.

**Step 3.** Click **GO TO RIGHTS MANAGER**.

**Step 4.** The Rights Manager's Clients page appears. Click **CONFIGURATION** at the top of the window. The Configuration page appears.

**Step 5.** Click **Authentication Services**. The Authentication Services page appears.

**Step 6.** Select **RADIUS** as the service type and then click **Add Service**. The Authentication page for configuring RADIUS appears.

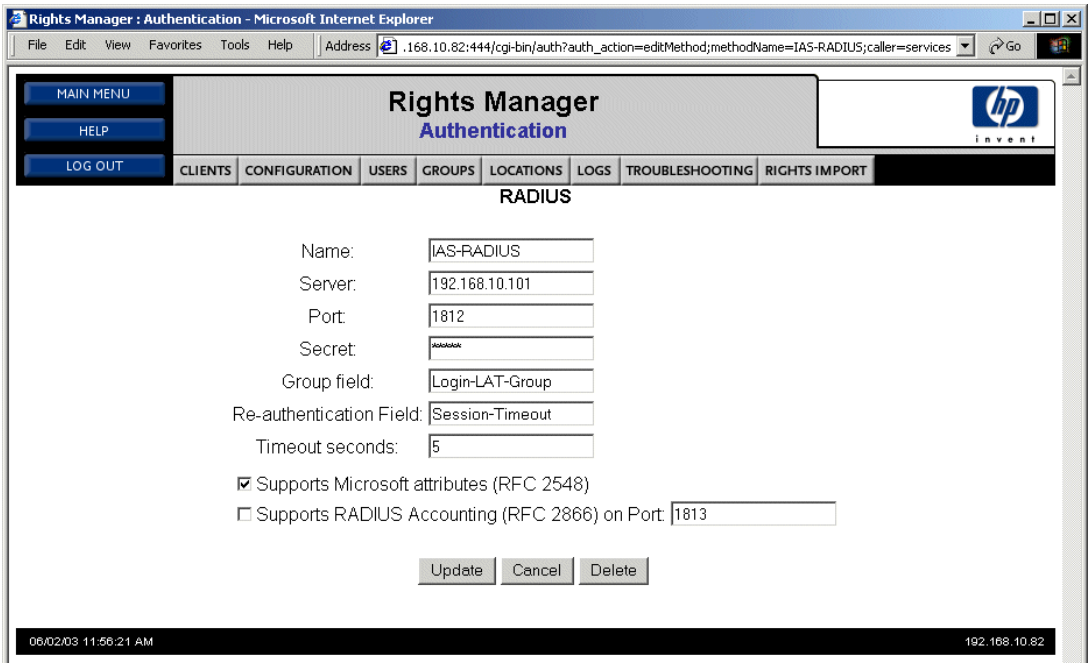


**Figure 2-20. Authentication page**

**Step 7.** Type the required information into the appropriate fields according to the example shown in Figure 2-20.

- The **Secret** must match the secret configured on your RADIUS server.
- The **Group** field can be any appropriate RADIUS attribute returned by the RADIUS server, or it can be left blank.

**Step 8.** Click **Update**.

**Step 9.** Click **CONFIGURATION** to return to the Configuration page and then click **Authentication Realms**. The Authentication Realms page appears.

**Step 10.** Click the **Default Realm** link in the table.

**Step 11.** The Authentication Realm Editor page appears. Select the newly added authentication service from the **Available Services** menu and then click **Append Service**. The new service appears in the Ordered List of Authentication Services table as show below.

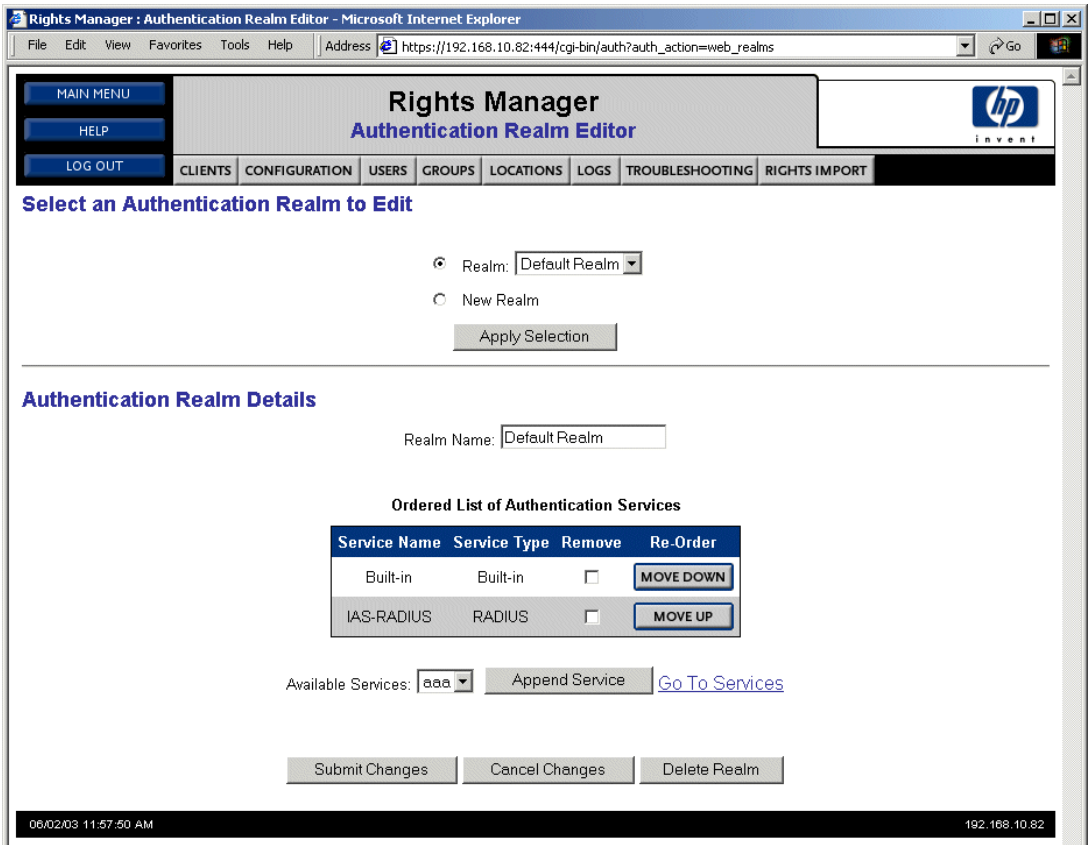


**Figure 2-21. The Default Realm with the RADIUS service added**

**Step 12.** Click **Submit Changes**.

***Note:*** *After you complete this step, you will still be able to log in using the "demouser" username, because the built-in database will still be searched before the authentication request will be sent to the RADIUS server.*

# Step XIII. Verify the External Authentication Service

The following steps allow you to verify that your RADIUS server will correctly authenticate users.

**Step 1.** Click **TROUBLESHOOTING**.

**Step 2.** The Troubleshooting page appears. Click **User Rights Simulator**.

The User Rights Simulator page appears.

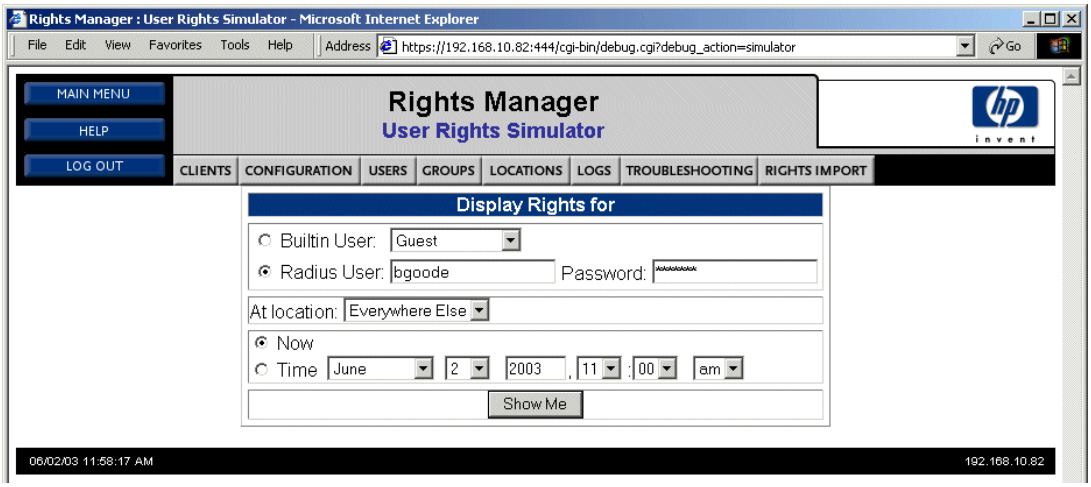


**Figure 2-22. User Rights Simulator page**

**Step 3.** Enter a known user name and password into the **Radius User and Password** fields and click **Show Me**.

**Step 4.** If this works correctly, the Display Rights for user table appears, showing the 700wl Series system rights that will be assigned to this user. If something is incorrect, you will receive the error message, "`No user in the Radius database or bad password for user`". Possible reasons for this error include:

- Wrong Username or Password or both
- The RADIUS authentication service is not configured correctly
- The RADIUS server does not recognize the Access Control Server 740wl

If an error occurs, return to Step XII, "External Authentication Service Configuration (Optional)" on page 2-18 and verify the RADIUS server configuration. Make sure to use a legitimate username and password recognized by the RADIUS server to test the RADIUS server.

# 3 DEPLOYING THE INTEGRATED ACCESS MANAGER 760WL

## Procedure Overview

To accomplish the objectives listed in the Introduction to this document, these instructions lead you through the following steps:

**Step 1.** Install the Integrated Access Manager 760wl system onto your network. If you are comfortable using the command language interface (CLI), you can follow the instructions in the *HP ProCurve Secure Access 700wl Series Quick Start Guide* that was included with your HP ProCurve 700wl Series hardware. Otherwise, follow the instructions in Step I, "Hardware Setup" on page 3-2.

**Step 2.** Create a "normal" user account (login ID and password) in the Rights Manager's built-in database.

**Step 3.** Connect a Windows client system to the 700wl Series system through a downlink port of the Integrated Access Manager 760wl. Log in as the user created in Step 2 against the built-in database using the 700wl Series system's Logon page. The user should then have full IP access to the network. This shows that the user can successfully connect to the system and gain network access.

**Step 4.** Configure the 700wl Series system as a VPN gateway using PPTP encryption.

**Step 5.** Configure the Windows client to establish a PPTP connection with the 700wl Series system. Then connect to the 700wl Series system using the PPTP connection process. Again, this shows that the client can connect to the system and gain access to the network.

**Step 6.** (Optional) Log the client off the system.

**Step 7.** (Optional) Configure the 700wl Series system to use an AAA RADIUS server for user authentication.

**Step 8.** (Optional) Log in using a user account known to the RADIUS authentication server, and verify network access.

## Preparation

Before you begin the system installation and configuration process, review the following list to make sure you have the required components available and/or configured as specified:

**Step 1.** One Windows-based PC or laptop preset to obtain an IP address automatically (via DHCP). This system will be used both to perform the configuration of your Integrated Access Manager and to function as a client once the configuration is complete.

**Step 2.** Two standard (straight-through) Ethernet cables; one for the Network Uplink of the Integrated Access Manager 760wl and the other for connecting the PC/laptop to the downlink port of the Integrated Access Manager.

**Step 3.** A DHCP server that can provide IP configuration information for the Integrated Access Manager 760wl's Network Uplink.

***Note:*** *If no DHCP server is available, then you must configure a static IP address for the Network Uplink port of each unit. Configuration parameters include: IP address, subnet mask, default router's IP address, and DNS server's IP address.*

**Step 4.** (Optional) One DB-9 Null Modem cable, required only if you plan to use the CLI to set up a static IP address, or if you intend to do the initial network configuration following the procedure in the Quick Start Guide.

**Step 5.** (Optional) One AAA RADIUS server. You must configure the RADIUS server to accept authentication requests from the Integrated Access Manager 760wl, which acts as a RADIUS client. A user account must be created in the RADIUS database. Consult the online *HP ProCurve Secure Access 700wl Series Configuration and Management Guide* for more information on other supported external authentication servers.

# Step I. Hardware Setup

***Note:*** *These steps duplicate much of the information found in the HP ProCurve 700wl Series Quick Start Guide. If you have already set up your system following the instructions in the Quick Start Guide, you can skip to Step III, "Creating a User Account in the Built-In Database" on page 3-3.*

**Step 1.** Connect the power cord to the Integrated Access Manager 760wl (rear side) and into an electrical outlet.

**Step 2.** Connect an Ethernet cable to the Network Uplink of the Integrated Access Manager 760wl. The other end of the cable is plugged into a Hub or Switch port on the internal (secured) network.

**Step 3.** Power on the unit and wait approximately 60 seconds or until it is completely booted (by observing the status on the LCD panel of the unit).

**Step 4.** Connect the configuration PC to any downlink port of the Integrated Access Manager 760wl using the remaining Ethernet cable and then power on the PC. Note that the PC should receive an IP address in the `42.x.x.x` range.

**Step 5.** If you plan to use the IP address provided by DHCP, skip to Step III, "Creating a User Account in the Built-In Database" on page 3-3. Otherwise, continue with Step II, "Static IP Configuration for the Integrated Access Manager 760wl (Optional)".

# Step II. Static IP Configuration for the Integrated Access Manager 760wl (Optional)

If you want your Integrated Access Manager to use a static IP address, and you have not already configured the unit using the instructions in the *HP ProCurve Secure Access 700wl Series Quick Start Guide*, do the following:

**Step 1.** Connect the Null Modem cable to the Serial Console port of the Integrated Access Manager 760wl and into a COM port, such as COM1, of the configuration PC.

**Step 2.** Start a terminal emulation program such as HyperTerminal in Microsoft Windows, and set the COM port properties to 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

**Step 3.** Initialize the terminal connection. A Login prompt appears in the terminal window.

**Step 4.** Logon to the system as the administrator. The default login is `admin` with password `admin`.

**Step 5.** Enter the following commands:

| CLI Command | Example |
|---|---|
| `set ip <ipaddress> [<netmask>]` | `set ip 192.168.10.71 255.255.255.0` |
| `set gateway <ipaddress>` | `set gateway 192.168.10.254` |
| `set dns <ipaddress> [<ipaddress>]` | `set dns 192.168.2.250 192.168.31.123` |

# Step III. Creating a User Account in the Built-In Database

In order for a user to log in, the 700wl Series system must be able to authenticate the user through some authentication service. The simplest form of authentication service is the built-in database included in the 700wl Series system Rights Manager. In this step, you add a user to the built-in database so you can login to your network as that user through the 700wl Series system.

**Step 1.** Start your web browser and then try to visit any web site. The 700wl Series system Logon page appears in the web browser window.

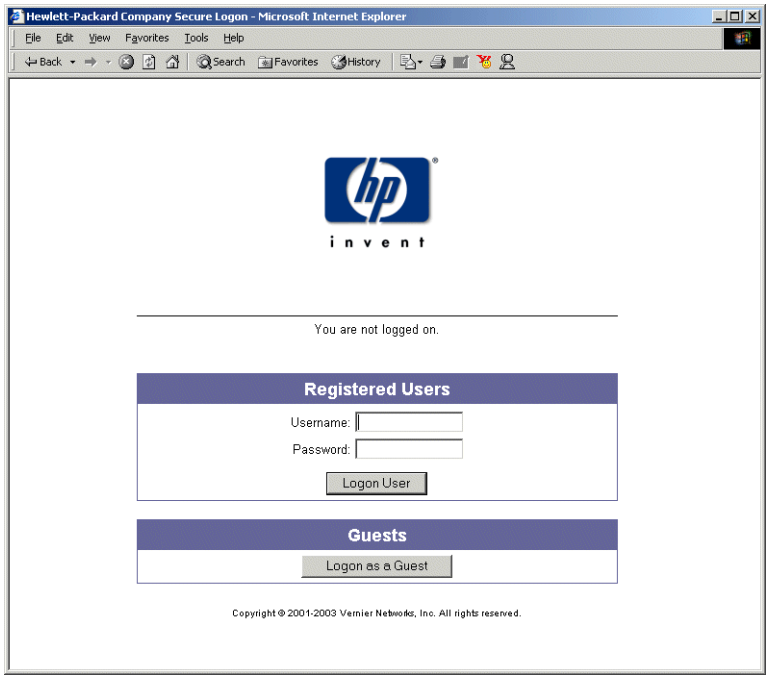


**Figure 3-1. HP ProCurve 700wl Series Login page**

**Step 2.** Open a URL to `http://42.0.0.1`. The Administrator Login page appears.€

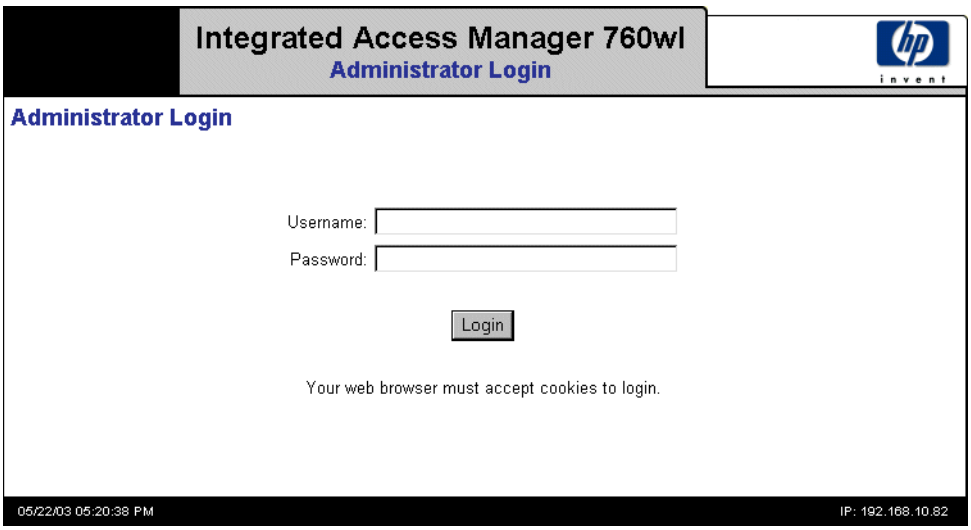


**Figure 3-2. Administrator Login page**

**Step 3.** Enter the default Administrator Username and Password (`admin` and `admin`) in the appropriate fields, and then click **Login**. The **Main** Menu appears.

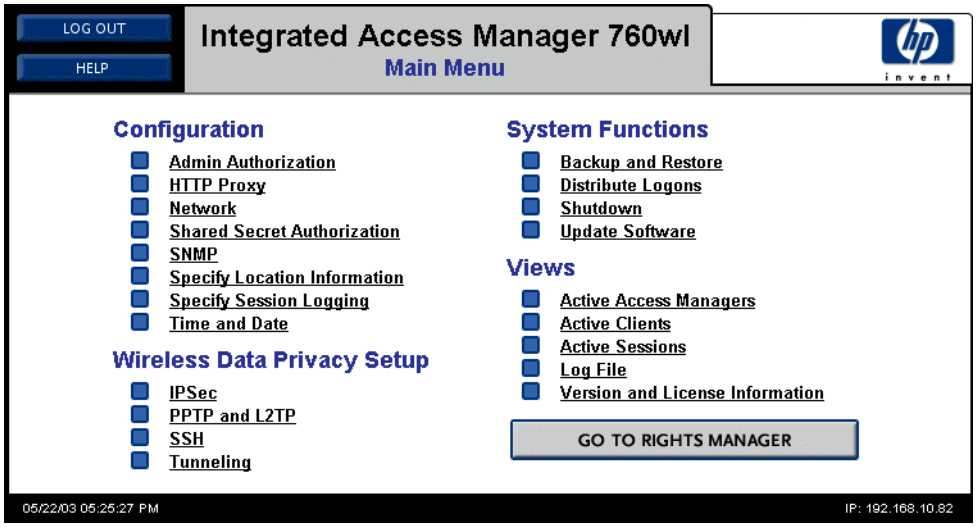


**Figure 3-3. Main Menu**

**Step 4.** From the **Main** Menu, click **GO TO RIGHTS MANAGER**.

**Step 5.** The Rights Manager's Clients page appears.

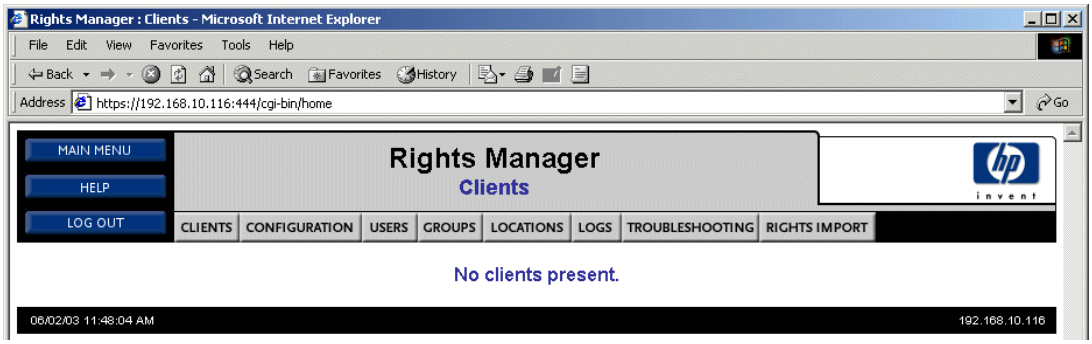


**Figure 3-4. Rights Manager Clients page**

**Step 6.** Click **USERS** at the top of the page.

The Users page appears, with an empty Users list.

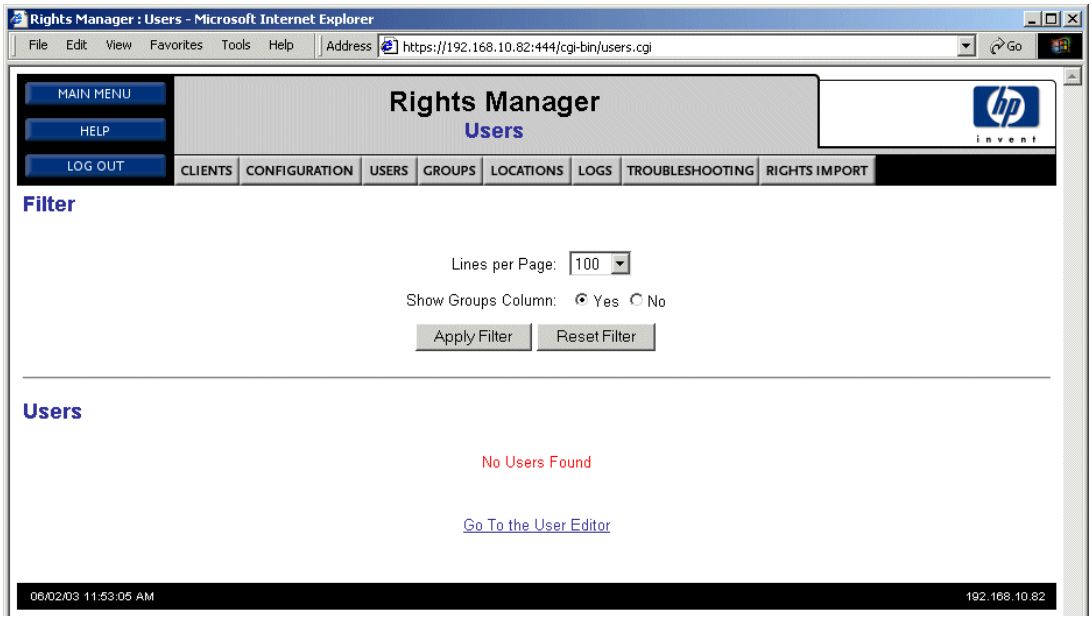


**Figure 3-5. Users page**

**Step 7.** Click the **Go To the User Editor** link.€

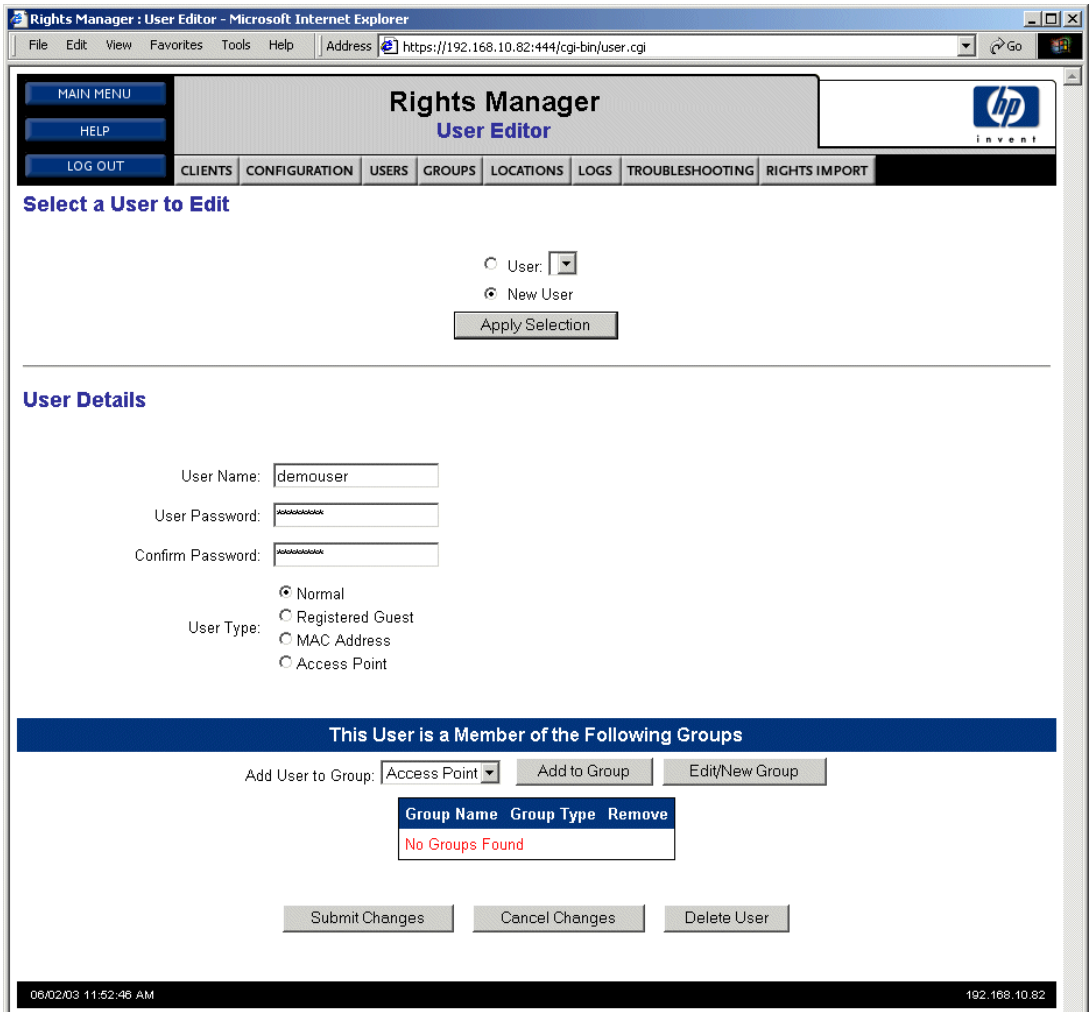


**Figure 3-6. User Details**

**Step 8.** Enter the following information:

- **User Name:** "demouser" (or any name you like)
- **User Password:** "password" (or any password you like)
- **Confirm Password:** "password" (must be the same as that entered into the first password field)

**Step 9.** Click **Submit Changes**.

# Step IV. User Authentication Through the 700wl Series Logon Page

In the following steps, the PC you have been using for configuration will also be used as a client system. If the PC's network interface is configured to use a static IP address, you must change its properties so that it will obtain an IP address automatically using DHCP.

In this step, you connect your PC to an Integrated Access Manager's downlink port and log onto your network using the username and password you added to the built-in database. If this is successful, you should be able to access the Internet and other resources on your network as usual.

**Step 1.** Start your web browser and then visit any web site. The web browser will display the 700wl Series Logon page (you have seen earlier in the previous step).

**Step 2.** Enter "demouser" and "password" (or the username and password you created) in the **Username** and **Password** field and click **Logon User**.

At this point, the web page you requested should appear, and you should be able to access the network normally.

# Step V. PPTP Gateway Configuration

This step configures the 700wl Series system to act as a VPN termination for PPTP. After configuring the PPTP client on your PC (see Step VI, "PPTP Client Configuration (Windows XP)" on page 3-10), you should be able to logon to the network via the PPTP connection interface.

**Step 1.** Set your web browser to the internal IP address of the Integrated Access Manager, `http://42.0.0.1`. The Administrator Login page appears.

**Step 2.** Enter the Administrator Username and Password (default: `admin` and `admin`) in the appropriate fields, then click **Login**. The Integrated Access Manager **Main** Menu appears.

**Step 3.** Click the **PPTP and L2TP** link in the Airwave Security Setup section of the **Main** Menu.

**Step 4.** The PPTP and L2TP Configuration page appears.

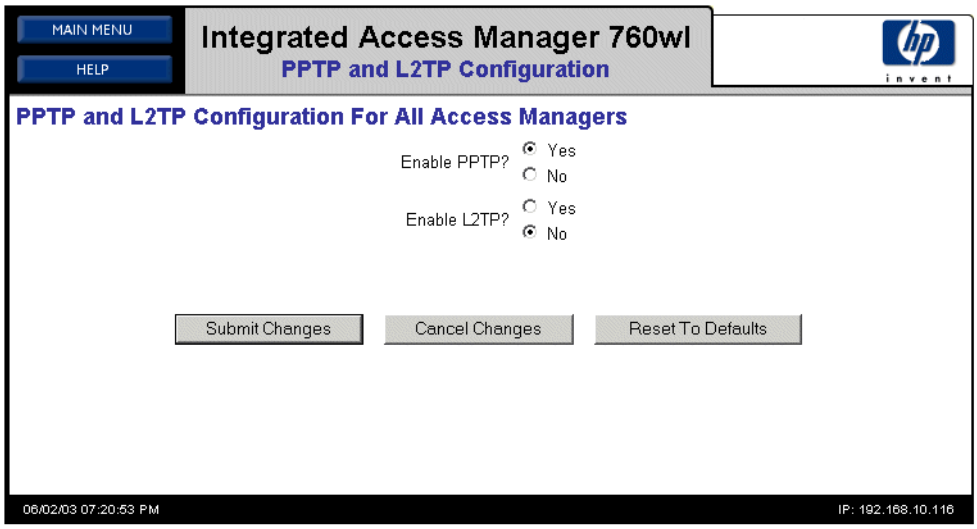


**Figure 3-7. PPTP and L2TP Configuration page**

**Step 5.** Click **Yes** to **Enable PPTP?** and then click **Submit Changes**.

**Step 6.** Click **MAIN MENU** to return to the **Main** Menu.€

**Step 7.** Click **GO TO RIGHTS MANAGER**.€

**Step 8.** The Rights Manager's Clients page appears. €

**Step 9.** Click **CONFIGURATION** at the top of the page. The Configuration page appears.€


**Figure 3-8. Configuration page**

**Step 10.** Click the **Encryption/Authentication per Location** link. The Encryption / Authentication per Location page appears.

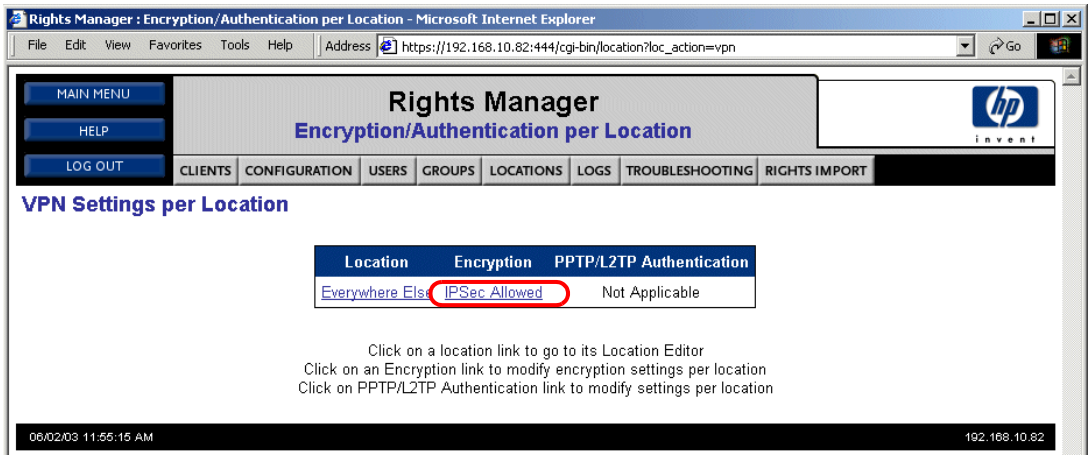


**Figure 3-9. Encryption/Authentication per Location page**

**Step 11.** Click the **IPSec Allowed** link in the Encryption column for the **Everywhere Else** location.

**Step 12.** In the Specify Encryption per Location page, select the **Allow the following protocols** option and then select **PPTP** from the panel to the right.

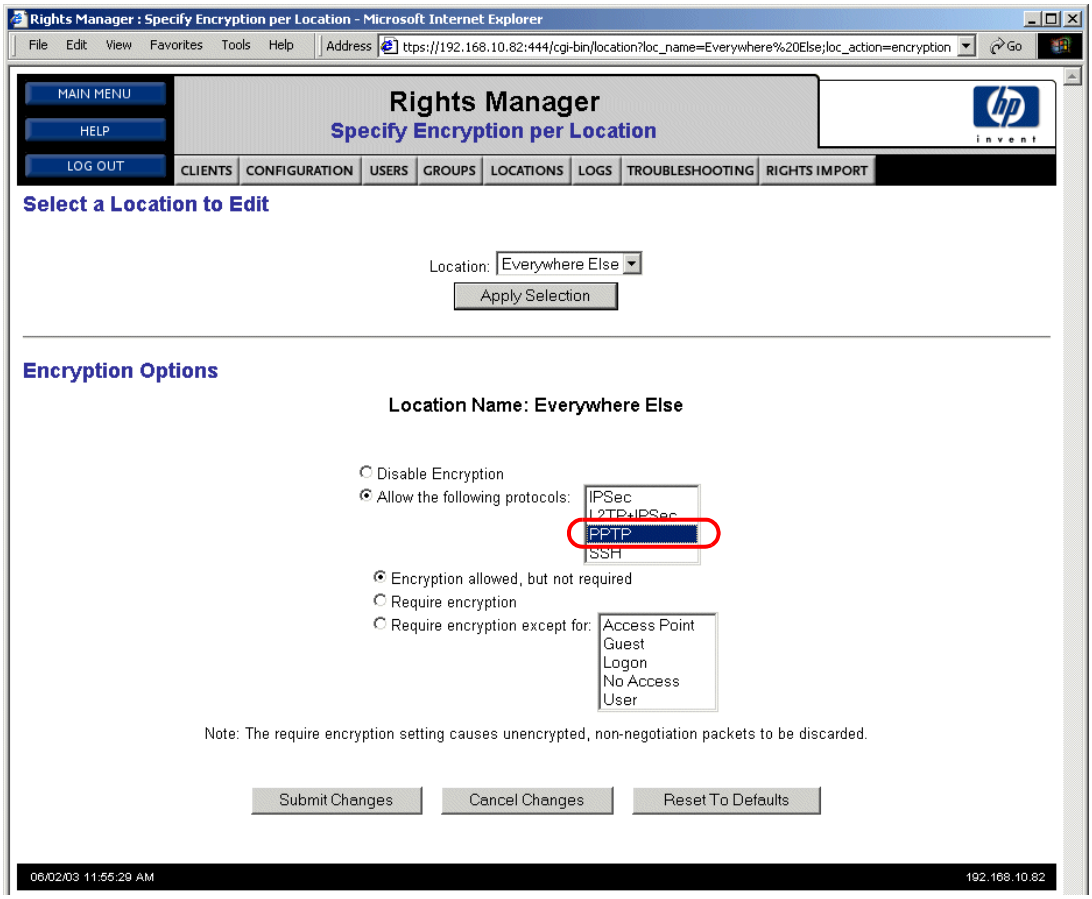


**Figure 3-10. Specify Encryption per Location page**

**Step 13.** Click **Submit Changes**.€

**Step 14.** Click **CLIENTS** to return to the Rights Manager's Clients page. €

**Step 15.** Click the **Refresh every client's rights** link.€

# Step VI. PPTP Client Configuration (Windows XP)

For details, refer to Step VI, "PPTP Client Configuration (Windows XP)" in Chapter 2 starting on page 2-13.

# Step VII. Logoff (Optional)

**Step 1.** Set your web browser to the URL `http://1.1.1.1`. The 700wl Series Logon page appears showing "demouser" as logged on.

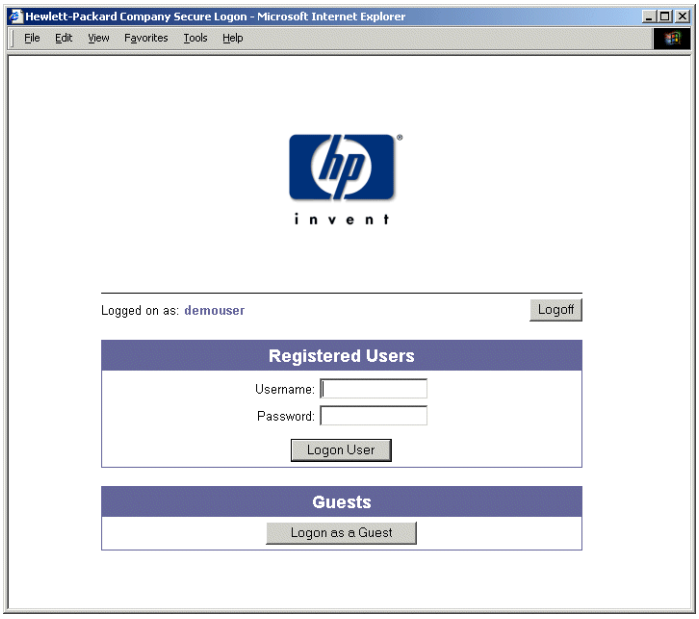


**Figure 3-11. 700wl Series Logon page for a logged on user**

**Step 2.** Click the **Logoff** button (at the right of the window) to log user "demouser" off the system.

# Step VIII. User Authentication Via PPTP Connection

Before starting the VPN connection, make sure your system has established a network connection with the server. You may use the ipconfig command to verify the IP settings and/or use the `ipconfig /renew` command to obtain an IP configuration from the Integrated Access Manager 760wl.

**Step 1.** Open the PPTP connection created in Step VI, "PPTP Client Configuration (Windows XP)" using the shortcut on your desktop or from the Network Connections window in the Control Panel.

The Connect window appears.

**Step 2.** Type "`demouser`" and "`password`" (or the user name and password you created in the built-in database) in the **Username** and **Password** fields, and click **Connect** to connect to the server. You may choose to save this username and password for future use before clicking the **Connect** button.

After the connection is successfully made, the connection icon appears in the notification area on the lower-right corner of the screen.

# Step IX. External Authentication Service Configuration (Optional)

If you use an external RADIUS authentication service and your user account already exists in the RADIUS server's database, you can configure the 700wl Series system to authenticate using the RADIUS server rather than the built-in database.

Once you have successfully completed this configuration, you should be able to logon to the network through the 700wl Series system using any legitimate username and password recognized by your RADIUS server.

To configure the Rights Manager to use a RADIUS server for authentication, do the following:

**Step 1.** Set your web browser to the URL `http://42.0.0.1`. The Administrator Login page appears.

**Step 2.** Type the Administrator Username and Password (default: `admin` and `admin`) in the appropriate fields, then click **Login**. The Integrated Access Manager **Main** Menu appears.

**Step 3.** Click **GO TO RIGHTS MANAGER**.

**Step 4.** The Rights Manager's Clients page appears. Click **CONFIGURATION** at the top of the window. The Configuration page appears.

**Step 5.** Click **Authentication Services**. The Authentication Services page appears.

**Step 6.** Select **RADIUS** as the service type and then click **Add Service**. The Authentication page for configuring RADIUS appears.

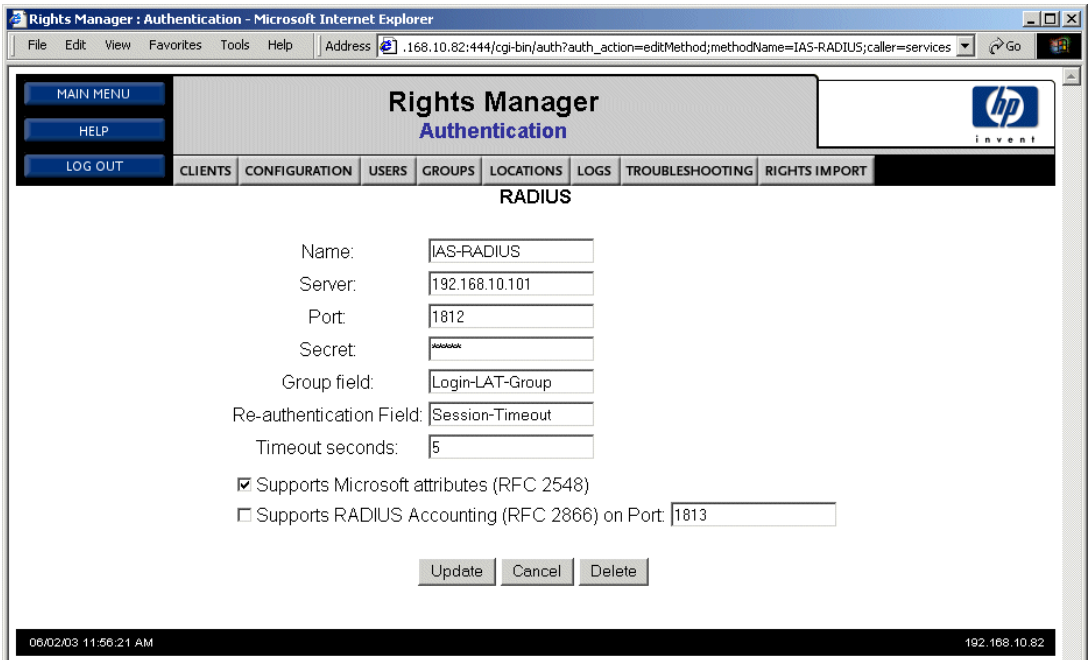


**Figure 3-12. Configuring a RADIUS authentication service**

**Step 7.** Type the required information into the appropriate fields according to the example below.

- The **Secret** must match the secret configured on your RADIUS server.
- The **Group** field can be any appropriate RADIUS attribute returned by the RADIUS server, or it can be left blank.

**Step 8.** Click **Update**.

**Step 9.** Click **CONFIGURATION** to return to the Configuration page and then click **Authentication Realms**. The Authentication Realms page appears.

**Step 10.** Click the **Default Realm** link in the table.

**Step 11.** The Authentication Realm Editor page appears. Select the newly added authentication service from the **Available Services** menu and then click **Append Service**. The new service appears in the Ordered List of Authentication Services table as show below.

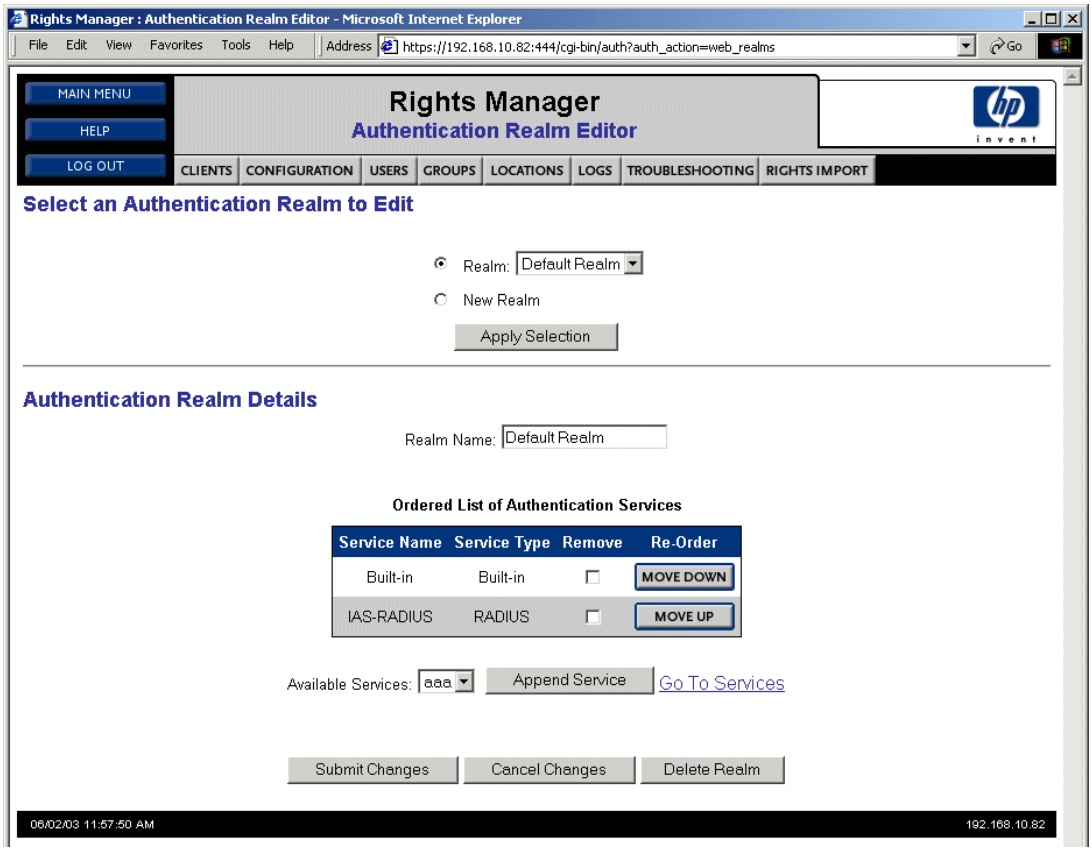


**Figure 3-13. The Default Realm with the RADIUS service added**

**Step 12.** Click **Submit Changes**.

***Note:*** *After you complete this step, you will still be able to log in using the "demouser" username, because the built-in database will still be searched before the authentication request will be sent to the RADIUS server.*

# Step X. Verify the External Authentication Service

The following steps allow you to verify that your RADIUS server will correctly authenticate users:

**Step 1.** Click **TROUBLESHOOTING**.

**Step 2.** The Troubleshooting page appears. Click **User Rights Simulator**.

The User Rights Simulator page appears.

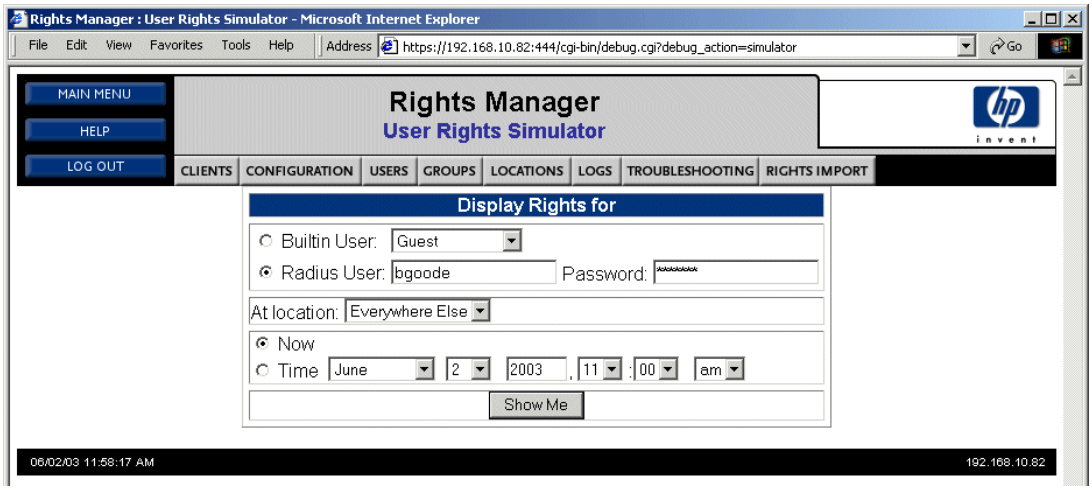


**Figure 3-14. Display User Rights for user table**

**Step 3.** Enter a known user name and password into the **Radius User** and **Password** fields and click **Show Me**.

If this works correctly, the Display Rights for user table should appear, showing the rights that will be assigned to this user. If something is incorrect, you will receive then error message, "`No user in the Radius database or bad password for user`". Possible reasons for this error include:

- Wrong Username or Password or both
- The RADIUS authentication service is not configured correctly
- The RADIUS server does not recognize the Integrated Access Manager 760wl

If an error occurs, return to Step IX, "External Authentication Service Configuration (Optional)" on page 3-12, and verify the RADIUS server configuration. Make sure to use a legitimate username and password recognized by the RADIUS server to test the RADIUS.

# SAFETY AND EMC REGULATORY STATEMENTS

A

## Safety Information

Documentation reference symbol. If the product is marked with this symbol, refer to the product documentation to get more information about the product.

**WARNING** A WARNING in the manual denotes a hazard that can cause injury or death.

**CAUTION** A CAUTION in the manual denotes a hazard that can damage equipment.

Do not proceed beyond a WARNING or CAUTION notice until you have understood the hazardous conditions and have taken appropriate steps.

### Grounding

These are safety class I products and have protective earthing terminals. There must be an uninterruptible safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

For LAN cable grounding:

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.
- LAN cables may occasionally be subject to hazardous transient voltages (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.

### Shielded Signal Cables

Use only shielded cables for connecting peripherals to any HP ProCurve 700wl Series device to reduce the possibility of interference with radio communications services. Using shielded cables ensures that you maintain the appropriate EMC classification for the intended environment.

### Pluggable Equipment

For pluggable equipment, the socket outlet shall be installed near the equipment and shall be easily accessible.

## Servicing

There are no user-serviceable parts inside these products. Any servicing, adjustment, maintenance, or repair must be performed only by service-trained personnel.

## Note for Service Personnel

***Caution:*** *There is a danger of a new battery exploding if it is incorrectly installed. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.*

# Informations concernant la sécurité

Symbole de référence à la documentation. Si le produit est marqué de ce symbole, reportez-vous à la documentation du produit afin d'obtenir des informations plus détaillées.

**WARNING** Dans la documentation, un WARNING indique un danger susceptible d'entraîner des dommages corporels ou la mort.

**CAUTION** Un texte de mise en garde intitulé CAUTION indique un danger susceptible de causer des dommages à l'équipement.

Ne continuez pas au-delà d'une rubrique WARNING ou CAUTION avant d'avoir bien compris les conditions présentant un danger et pris les mesures appropriées.

Cet appareil est un produit de classe I et possède une borne de mise à la terre. La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entrée, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débrancher le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Mise à la terre du câble de réseau local:

- si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité soient convenablement interconnectées.
- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précautions.

Aucune pièce contenue à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

***Attention:*** *Ce produit contient une pile au Lithium remplacable. Risque d'explosion si la pile est remplacee par un modele incorrect. Disposez des piles usagees selon les instructions.*

# Hinweise zur Sicherheit

Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

**WARNING** Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

**CAUTION** Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

Fahren Sie nach dem Hinweis WARNING oder CAUTION erst fort, nachdem Sie den Gefahrenzustand verstanden und die entsprechenden Maßnahmen ergriffen haben.

Dies ist ein Gerät der Sicherheitsklasse I und verfügt über einen schützenden Erdungsterminal. Der Betrieb des Geräts erfordert eine ununterbrochene Sicherheitserdung von der Hauptstromquelle zu den Geräteingabeterminals, den Netzkabeln oder dem mit Strom belieferten Netzkabelsatz voraus. Sobald Grund zur Annahme besteht, daß der Schutz beeinträchtigt worden ist, das Netzkabel aus der Wandsteckdose herausziehen, bis die Erdung wiederhergestellt ist.

Für LAN-Kabelerdung:

- Wenn Ihr LAN ein Gebiet umfaßt, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, daß die Sicherheitserdungen fest untereinander verbunden sind.
- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetzt werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponierter Metallbestandteile des Netzwerkes Vorsicht walten lassen.

Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedienungspersonal durchgeführt werden.

***Vorsicht:*** *Dieses Produkt enhalt eine wechselbare Lithium Batterie. Es besteht Explosionsgefahr wenn die Batterie durch einen falschen Typ ersetzt wird. Entsorgen Sie gebrauchte Batterien nach den Anweisungen.*

# Considerazioni sulla sicurezza

Simbolo di riferimento alla documentazione. Se il prodotto è contrassegnato da questo simbolo, fare riferimento alla documentazione sul prodotto per ulteriori informazioni su di esso.

**WARNING** La dicitura WARNINGdenota un pericolo che può causare lesioni o morte.

**CAUTION** La dicituraCAUTION denota un pericolo che può danneggiare le attrezzature.

Non procedere oltre un avviso di WARNING o di CAUTIONprima di aver compreso le condizioni di rischio e aver provveduto alle misure del caso.

Questo prodotto è omologato nella classe di sicurezza I ed ha un terminale protettivo di collegamento a terra. Dev'essere installato un collegamento a terra di sicurezza, non interrompibile che vada dalla fonte d'alimentazione principale ai terminali d'entrata, al cavo d'alimentazione oppure al set cavo d'alimentazione fornito con il prodotto. Ogniqualvolta vi sia probabilità di danneggiamento della protezione, disinserite il cavo d'alimentazione fino a quando il collegaento a terra non sia stato ripristinato.

Per la messa a terra dei cavi LAN:

- se la vostra LAN copre un'area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;
- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d'alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.

Nessun componente di questo prodotto può essere riparato dall'utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

***Attenzione:*** *questo prodotto contiene batterie ricaricabili al Litio. Se vengono utilizzate delle batterie non adatte vi e' rischio di esplosione. Eliminare le batterie usate seguendo le istruzioni fornite a riguardo.*

# Consideraciones sobre seguridad

Símbolo de referencia a la documentación. Si el producto va marcado con este símbolo, consultar la documentación del producto a fin de obtener mayor información sobre el producto.

**WARNING** Una WARNING en la documentación señala un riesgo que podría resultar en lesiones o la muerte.

**CAUTION** Una CAUTION en la documentación señala un riesgo que podría resultar en averías al equipo.

No proseguir después de un símbolo de WARNING o CAUTION hasta no haber entendido las condiciones peligrosas y haber tomado las medidas apropiadas.

Este aparato se enmarca dentro de la clase I de seguridad y se encuentra protegido por una borna de puesta a tierra. Es preciso que exista una puesta a tierra continua desde la toma de alimentación eléctrica hasta las bornas de los cables de entrada del aparato, el cable de alimentación o el juego de cable de alimentación suministrado. Si existe la probabilidad de que la protección a tierra haya sufrido desperfectos, desenchufar el cable de alimentación hasta haberse subsanado el problema.

Puesta a tierra del cable de la red local (LAN):

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.
- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.

Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

***Curdado:*** *Este producto contiente pilas remplasables de Lithium. Riesgo de exposion si la pila es remplasada con el tipo incorrecto. Deseche la pilas usadas de accuerdo a las instrucciones.*

# Safety Information (Japan)

安全性の考慮

安全記号

マニュアル参照記号。製品にこの記号がついている場合はマニュアルを参照し、注意事項等をご確認ください。

WARNING　マニュアル中の「WARNING」は人身事故の原因となる危険を示します。

CAUTION　マニュアル中の「CAUTION」は装置破損の原因となる危険を示します。

「WARNING」や「CAUTION」の項は飛ばさないで必ずお読みください。危険性に関する記載事項をよく読み、正しい手順に従った上で次の事項に進んでください。

これは安全性クラスIの製品で保護用接地端子を備えています。主電源から製品の入力配線端子、電源コード、または添付の電源コード・セットまでの間、切れ目のない安全接地が存在することが必要です。もしこの保護回路が損なわれたことが推測されるときは、接地が修復されるまで電源コードを外しておいてください。

LANケーブルの接地に関して:

- もし貴社のLANが複数の配電システムにより電力を受けている領域をカバーしている場合には、それらのシステムの安全接地が確実に相互に結合されていることを確認してください。
- LANケーブルは時として危険な過度電圧（例えば雷や、配電設備の電力網での障害）にさらされることがあります。露出した金属部分の取扱いには十分な注意をはらってください。

本製品の内部にはユーザーが修理できる部品はありません。サービス、調整、保守および修理はサービス訓練を受けた専門家におまかせください。

本製品には電源スイッチがありません。電源コードを接続したとき電源入となります。

CAUTION: この製品は交換可能なリチウム電池を使用しています。間違ったタイプに交換すると爆発の危険があります。使用済みの電池は説明書に従って処分して下さい。

# Safety Information (China)

## HP网络产品使用安全手册

### 使用须知

欢迎使用惠普网络产品，为了您及仪器的安全，请您务必注意如下事项：

1. 仪器要和地线相接，要使用有正确接地插头的电源线，使用中国国家规定 的 220V 电源。
2. 避免高温和尘土多的地方，否则易引起仪器内部部件的损坏。
3. 避免接近高温，避免接近直接热源，如直射太阳光、暖气等其它发热体。
4. 不要有异物或液体落入机内，以免部件短路。
5. 不要将磁体放置于仪器附近。

### *警告*

为防止火灾或触电事故，请不要将该机放置于淋雨或潮湿处。

如果您按照以上步骤操作时遇到了困难，或想了解其它产品性能，请在以下网页上寻找相关信息：http://www.hp.com.cn

或联系我们

中国惠普有限公司
地址：北京建国路112号中国惠普大厦
电话： 010-65643888

注意：此产品包括一可更换锂电池.用错误型号电池更换会有爆炸危险.务必按照说明处置用完的电池.

# EMC Regulatory Statements

## U.S.A.

FCC Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. Operation of this equipment in a residential area may cause interference in which case the user will be required to correct the interference at his own expense.

## Canada

This product complies with Class A Canadian EMC requirements.

## Australia/New Zealand

This product complies with Australia / New Zealand EMC Class A requirements.

## Japan

VCCI Class A

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## Korea

사용자 안내문 : A 급기기

이기기는 업무용으로 전자파 적합등록을 받은 기기이오니, 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

## BSMI

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

## Regulatory Model Identification Number

**For regulatory identification purposes, the HP ProCurve Secure Access 700wl Series system components (Access Controller 720wl, Access Control Server 740wl, Integrated Access Manager 760wl) are assigned a Regulatory Model Number. The Regulatory Model Number for these components is RSVLC-0206.**

**This regulatory number should not be confused with the marketing name or product numbers (J8153A, J8154A, J8155A)**

## European Community

**DECLARATION OF CONFORMITY**
according to ISO/IEC Guide 22 and EN 45014

**Manufacturer's Name:** Hewlett-Packard Company

**Manufacturer's Address:** 8000 Foothills Blvd.
Roseville, CA 95747-5502
U.S.A.

**declares, that the product**

**Product Name:** HP ProCurve Access Controller 720wl
HP ProCurve Access Control Server 740wl
HP ProCurve Integrated Access Manager 760wl

**Model Number(s):** J8135A, J8154A, J8155A

**Regulatory Model:** RSVLC-0206

**Product Options:** All

**conforms to the following Product Specifications:**

Safety: IEC 60950:1991 + A1, A2, A3, A4 / EN 60950:1992 + A1, A2, A3, A4, A11
IEC 60825-1:1993 / EN 60825-1:1994 + A11, Class 1 (Laser/LED)

EMC: CISPR 22:1997 / EN 55022:1998 Class A[1]
CISPR 24:1997 / EN 55024:1998
IEC 61000-3-2:1995 / EN 61000-3-2:1995 +A1, A2
IEC 61000-3-3:1994 / EN 61000-3-3:1995 +A1

**Supplementary Information**:

The product herewith complies with the requirements of the Low Voltage Directive 73/23/EEC, the EMC Directive 89/336/EEC and carries the CE marking accordingly.

1) The Product was tested in a typical configuration with system peripherals from several manufacturers.

Roseville, June 12, 2003

Mike Avery, Regulatory Engineering Mgr.

European Contact: Your local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH, Department HQ-TRE, Herrenberger Straße 140, D-71034 Böblingen (FAX: + 49-7031-14-3143)




Edition 1, July 2003

Manual Part Number
5990-3104