Management and Configuration Guide

HP ProCurve Secure Access 700wl Series

www.hp.com/go/hpprocurve

HP ProCurve
Secure Access 700wl Series

Management and Configuration Guide

© Copyright 2003 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number

5990-5988
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

Preface xi

Audience xi

How To Use This Document xi

Document Conventions xi

Organization xii

Support Information xiv

Part 1 The Administrative Interface

Chapter 1 Introduction 1-1

Overview 1-1

The HP ProCurve Secure Access 700wl Series 1-2

The Access Controller 720wl 1-3

The Access Control Server 740wl 1-3

The Integrated Access Manager 760wl 1-4

The Rights Manager 1-4

Wireless Data Privacy 1-5

User Authentication 1-5

Client Access Rights 1-6

Locations 1-6

Groups 1-7

Roaming Support 1-8

VLAN Tag Support 1-9

Chapter 2 Configuring a 700wl Series System 2-1

Configuration Overview 2-1

Administrator Login 2-2

Changing the Admin Authorization Settings 2-5

Changing the Network Configuration **2-6**
Advanced Network Settings 2-9
Configuring the Shared Secret for Access Controllers **2-16**
Setting the Shared Secret on the Access Control Server 2-17
Setting the Shared Secret and IP Address on an Access Controller 2-17
HTTP Proxy Server Configuration **2-18**
Configuring SNMP **2-20**
Specifying Location Information **2-22**
Specifying Session Logging **2-23**
Configuring the Time and Date **2-24**
Viewing Online Documentation and Help **2-26**

Chapter 3 Wireless Data Privacy 3-1

Configuring Wireless Data Privacy **3-1**
IPSec 3-1
PPTP 3-2
L2TP / IPSec 3-2
SSH 3-3
General Considerations 3-3
Configuring IPSec **3-4**
Configuring PKI for IPSec 3-6
Configuring PPTP and L2TP **3-11**
Configuring SSH **3-12**
Tunneling Configuration **3-13**

Chapter 4 Controlling the System Functions 4-1

Creating and Storing a Backup Image **4-1**
Creating a Backup Image 4-1
Saving the Backup 4-3
Restoring a Backed-Up Image **4-4**
Transferring a Backup to a Different System 4-6
Distributing Logons to Access Controllers **4-6**
Updating the System Software **4-6**
Determining if a New Software Version is Available 4-8
Downloading a Software Version 4-8
Rebooting, Shutting Down, or Resetting the System **4-10**

Chapter 5 Viewing System Status 5-1

Viewing Status Information 5-1
Filtering a Status Display 5-2

Viewing Access Controllers 5-3

Viewing the Active Client List 5-4

Viewing Active Session Information 5-7

Viewing Log Files 5-9
Informational Log File 5-9
Session Log File 5-11

Viewing Version and License Information 5-12

Part 2 The Rights Manager

Chapter 6 Getting Started with the Rights Manager 6-1

About the Rights Manager 6-1

Rights Manager Terminology 6-3
Groups 6-4
Locations 6-6
Access Rights 6-8
How Groups and Locations Interact 6-9

User Authentication 6-10
Authentication and Group Membership 6-11

Two Simple Rights Examples 6-11
Example 1: Visiting Professor 6-11
Example 2: Contractors with Extended Hours 6-12

How the Rights Manager Determines a User's Rights 6-13
Determining Group Membership 6-14

VLANs and the 700wl Series System 6-14

Network Address Translation in the 700wl Series System 6-16
NAT and VPN Tunneling 6-18

Getting to the Rights Manager 6-18
Logging Out of the Rights Manager 6-21

The Rights Manager Clients Page 6-22
Setting Up MAC Address Users and Access Points 6-22

Chapter 7 Configuring Groups 7-1

Defining Groups 7-1

The Properties of a Group 7-2
How Group Rights (Allows and Redirects) are Processed 7-3
Automatic HTTP Proxy Interaction with Group Access Rights 7-4

Viewing Groups—the Groups Manager 7-4
Selecting Allows or Redirects in the Groups Manager 7-6
Modifying the Columns in the Groups Manager 7-7

Adding or Modifying a Group—the Group Editor 7-8
Allows and Redirects for Distributed Logons 7-19
Deleting a Group 7-20
Setting Up Groups for Student Access Rights 7-20

Adding or Modifying a When—the When Editor 7-21

Defining Redirect Rights—the Redirect Editor 7-23
Adding or Modifying a Redirect 7-23
Deleting a Redirect 7-26

Defining Allow Rights—the Allow Editor 7-27
Adding or Modifying an Allow 7-28
Deleting an Allow 7-30

Example—Modifying Rights for the Guest Group 7-30
Enabling an Existing Allow—Outside World 7-30
Creating a New Allow for Restricted Access 7-31

Chapter 8 Setting Up Locations 8-1

Defining Locations 8-1

The Locations Manager 8-2
Selecting Groups in the Locations Manager 8-3
Modifying the Groups Columns in the Locations Manager 8-4

Adding or Modifying a Location—the Location Editor 8-5
Deleting a Location 8-9

Adding or Modifying a Where—the Where Editor 8-10
Deleting a Where 8-12

Adding or Modifying an Access Controller 8-12
Deleting an Access Controller 8-13

Chapter 9 User Authentication 9-1

Overview of Authentication 9-1

Authentication Services 9-3

The Built-in Authentication Service 9-5

Configuring an LDAP Authentication Service 9-5
Configuring Authentication Using the Active Directory Service 9-9

Configuring Authentication Using a Netscape or iPlanet Directory Service 9-10
Using Aliasing to Retrieve a DN and Password 9-12

Configuring RADIUS as an Authentication Service 9-12

Configuring Kerberos as an Authentication Service 9-14

Using XML-RPC for Authentication 9-15
Configuring XML-RPC as an Authentication Service 9-16
The XML-RPC Service 9-17
The Remote Profiles API 9-17

Authentication Realms 9-20
Creating or Modifying an Authentication Realm 9-22
Changing the Default Realm 9-23
Deleting a Realm 9-24

Customizing Pages for Web-based Logon 9-24
Customizing the Logo 9-27
Customizing the Logon Page 9-28
Customizing the Stop Page 9-30
Logoff Page Options 9-31
Small Browser Options 9-33
Customized Page Templates 9-33

Wireless Data Privacy Logon (PPTP/L2TP Clients) 9-34
Encryption Options by Location 9-35
PPTP/L2TP Options by Location 9-37

Monitored Logon (802.1x and NT Domain Logon) 9-39
Enabling 802.1x or NT Domain Logon 9-40
802.1x Logon Settings 9-41

Retrieving Group Information from an External Service 9-42

Retrieving MAC Addresses from an LDAP Directory 9-44
Specifying the LDAP Service for MAC Address Retrieval 9-45
Configuring the Search for MAC Addresses 9-46
Configuring the Search for Group Information 9-47

Configuring RADIUS Accounting 9-48
Configuring a RADIUS Service for Accounting 9-49
Modifying an Existing RADIUS Service to Support Accounting 9-50
Enabling RADIUS Accounting 9-51
Specifying a NAS-ID for Use with RADIUS Accounting 9-52
Accounting Packet Data 9-53

Chapter 10 Setting Up Users 10-1

The Built-In Authentication Database 10-1

Viewing Users—the Users Page **10-2**
Exporting the User List 10-3
Adding or Modifying a User—the User Editor **10-4**
Deleting a User 10-6
Setting Up Access Point Users **10-6**

Chapter 11 Global Rights Manager Settings 11-1

Global Settings Overview **11-1**
Network Access Control Console Configuration **11-2**
Configuring Network Access Control 11-3
DNS/WINS Server List Editors **11-4**
Editing the DNS Servers List 11-5
Setting Up DNS Allow/Redirect Pairs 11-5
Editing the WINS Servers List 11-7
Setting Up WINS Allow/Redirect Pairs 11-8
Automatic HTTP Proxy Configuration **11-9**
Enabling or Disabling the Automatic Proxy for a Group 11-10
Configuring the HTTP Proxy Settings for a Group 11-11
Setting Up Rights Manager Logging **11-15**
Security **11-17**
MAC Address Spoofing Detection 11-17
Obtaining and Loading an SSL Certificate 11-18

Chapter 12 Troubleshooting, Logs, and Rights Import/Export 12-1

Troubleshooting **12-1**
Tracing Authentication Service Transactions **12-1**
The User Rights Simulator **12-6**
Viewing the Rights Manager Log **12-8**
Importing and Exporting Rights **12-10**
Creating a Rights Image for Export 12-11
Exporting a Set of Rights 12-12
Importing Rights 12-13
Downloading the XML Schema 12-13

Appendix A Filter Expression Syntax A-1

Introduction **A-1**
Filter Specification Syntax **A-1**
Tcpdump Primitives **A-2**

Appendix B Creating Customized Templates B-1

Introduction **B-1**

A Simple Logon Page Template Example **B-2**

Logon Template Elements **B-3**
Required Elements B-4
Optional Elements B-5

Logon Page Template — A More Advanced Example **B-7**

The Guest Registration Template **B-10**

Using a Logoff Pop-Up with a Customized Logon Page **B-13**
Redisplaying the Logon Page in a New Window B-15

Customizing the Stop Page **B-16**

Appendix C Command Line Interface C-1

Accessing the Command Line Interface **C-1**
Command Syntax C-2

Getting CLI Command Help **C-3**

Administrator Access Control Commands **C-3**

System Status and Information Commands **C-4**

Network Configuration Commands **C-6**

Port Configuration Commands **C-8**
Access Controller Port Configuration Commands C-10

Access Controller Configuration **C-10**
Advanced Network Configuration C-11

Access Control Server Configuration **C-13**
Advanced Network Configuration C-15

Wireless Data Privacy Configuration **C-15**

Active Client Management Commands **C-17**

System Backup, Upgrade, and Shutdown Commands **C-19**
Backup and Restore C-19
Upgrading the System Software C-20
Stopping and Restarting the System C-23
Resetting to Factory Defaults C-23

Diagnostic and Log Commands **C-24**

Time Configuration **C-27**

SNMP Configuration and Reporting Commands **C-28**

Appendix D Network Access Control Console D-1

Network Access Control Console Overview **D-1**

Configuring Network Access Control **D-2**

Configuring Groups for Use with the Network Access Control Console D-2

Configuring the Network Access Control Console D-3

The Group Membership Retrieval API **D-5**

Using the Network Access Control Console **D-7**

Appendix E Glossary **E-1**

Index of Commands **IOC-1**

Index **IX-1**

PREFACE

This preface describes the audience, use, and organization of the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide.* It also outlines the document conventions, safety advisories, compliance information, related documentation, support information, and revision history.

Audience

The primary audience for this document are network administrators who want to enable their network users to communicate using the HP ProCurve Secure Access 700wl Series products. This document is intended for authorized personnel who have previous experience working with network telecommunications systems or similar equipment. It is assumed that the personnel using this document have the appropriate background and knowledge to complete the procedures described in this document.

How To Use This Document

This document contains procedural information describing the configuration and management of the HP ProCurve Access Control Server 740wl and Access Controller 720wl, or the Integrated Access Manager 760wl. Where applicable, navigation aids also refer you to supplemental information such as figures, tables, and other procedures in this document or another document. Main chapters are followed by supplemental information such as appendices and an index.

Document Conventions

The following text conventions are used in this document:

Table 1. Text Conventions

Convention	Definition
Boldface Arial	Screen menus that you click to select, commands that you select, or field names are in boldface Arial.
Boldface Italic Palatino	New terms that are introduced are in boldface italic Palatino.
Italic Palatino	Emphasized terms are in italic Palatino.
`Courier`	Filenames and text that you type are in `Courier`.

The following notices and icons are used to alert you to important information.

Table 2. Notices

Icon	Notice Type	Alerts you to...
None	Note	Helpful suggestions or information that is of special importance in certain situations.
None	Caution	Risk of loss of system functionality or loss of data.
	Warning	Risk of personal injury, system damage, or irrecoverable loss of data.

Organization

This document is organized as follows:

Part 1—The Administrative Interface

Chapter 1—“Introduction”

This chapter provides an overview HP ProCurve Secure Access 700wl Series and describes how the components operate.

Chapter 2—“Configuring a 700wl Series System”

This chapter explains how to configure your 700wl Series system.

Chapter 3—“Wireless Data Privacy”

This chapter describes how to enforce security using IPSec, L2TP, and PPTP.

Chapter 4—“Controlling the System Functions”

This chapter explains how to install new software, backup your system, and shutdown and reboot.

Chapter 5—“Viewing System Status”

This chapter explains how to view the status of the components of the 700wl Series system.

Part 2—The Rights Manager

Chapter 6—“Getting Started with the Rights Manager”

This chapter explains the concepts and terminology that are fundamental to the 700wl Series system Rights Manager. It also covers how to access the Rights Manager.

Chapter 7—“Configuring Groups”

This chapter explains how to configure Groups for use in the 700wl Series Rights Manager as the mechanism for assigning rights to clients.

Chapter 8—“Setting Up Locations”

This chapter explains how to set up locations for use with the Rights Manager.

Chapter 9—“User Authentication”

This chapter explains how to configure authentication services and authentication realms for use with the 700wl Series Rights Manager. It also explains how to configure the Rights Manager to support RADIUS accounting.

Chapter 10—“Setting Up Users”

This chapter explains how to add users to the 700wl Series built-in database for use as an authentication service or for mapping clients to groups.

Chapter 11—“Global Rights Manager Settings”

This chapter covers a number of global configuration settings for the Rights Manager, including specifying DNS or WINS servers, automatic HTTP proxy configuration, and setting options for Rights Manager logging.

Chapter 11—“Troubleshooting, Logs, and Rights Import/Export”

This chapter covers troubleshooting authentication services and client rights. It also covers viewing Rights Manager logs, and exporting and importing rights.

Appendix A—“Filter Expression Syntax”

This appendix describes the syntax of the filter specifications used by the Rights Manager for defining Allows, Redirects, Bridged traffic, and HTTP Proxy filters.

Appendix B—“Creating Customized Templates”

This appendix explains how to create customized templates for the Logon, Guest Registration, and Logoff web pages.

Appendix C—“Command Line Interface”

This appendix provides a description of the command line interface.

Appendix D—“Network Access Control Console”

This appendix explains how to configure and use the Network Access Control console enabled by the 700wl Series system.

Appendix E—“Glossary”

The Glossary explains terms that are specific to the 700wl Series system. These terms are shown in italics when first used.

Index of CLI Commands

The Index of Commands is an alphabetized list of the CLI commands with references to the pages where they are documented.

Support Information

See the HP ProCurve Networking web site at `www.hp.com/go/hpprocurve`. Click on **technical support** and select **support services** for a list of available support resources and options for contacting HP.

Part 1
The Administrative Interface

INTRODUCTION 1

This chapter gives a brief description of the HP ProCurve Secure Access 700wl Series products. It consists of the following sections:

Overview 1-1

The HP ProCurve Secure Access 700wl Series 1-2

Wireless Data Privacy 1-5

User Authentication 1-5

Client Access Rights 1-6

Roaming Support 1-8

VLAN Tag Support 1-9

Overview

The HP ProCurve Secure Access 700wl Series provides the foundation for building secure, scalable, and mission-critical 802.11 wireless networks. At the core of the wireless LAN (WLAN) a 700wl Series system provides key services including fine-grained access control, centralized management, and seamless roaming, which enables companies to deploy and manage 802.11 networks ranging from tens to thousands of access points (APs).

The 700wl Series system enables fine-grained access control and transparent Layer 3 roaming capabilities for wireless and wired IP networks. The IP traffic of each user machine or ***client*** can be individually authenticated, controlled, redirected, and logged for auditing or billing purposes. When clients move around within the enterprise, their open sessions are transparently forwarded so that the sessions are not terminated. Almost any user authentication scheme can be supported through the 700wl Series system's fully customizable Rights Manager component.

In addition, the ***Wireless Data Privacy*** feature can be used to encrypt all client traffic using standard tunneling and encryption technology including PPTP, L2TP, or IPSec.

The 700wl Series system addresses the following mandatory network infrastructure functions:

- Security:
  - — User authentication
  - — User-based access and resource control
  - — Wireless Data Privacy using PPTP, L2TP, or IPSec
- Management: tracking of wireless access points and users

- Accounting: information for accounting, logging, and billing

The 700wl Series system also addresses the following mobility functions:

- Address Mobility: no need to re-authenticate or acquire a new address when roaming
- Connection Mobility: sessions remain open when roaming

The HP ProCurve Secure Access 700wl Series

Figure 1-1 shows the topology of a typical 700wl Series system.

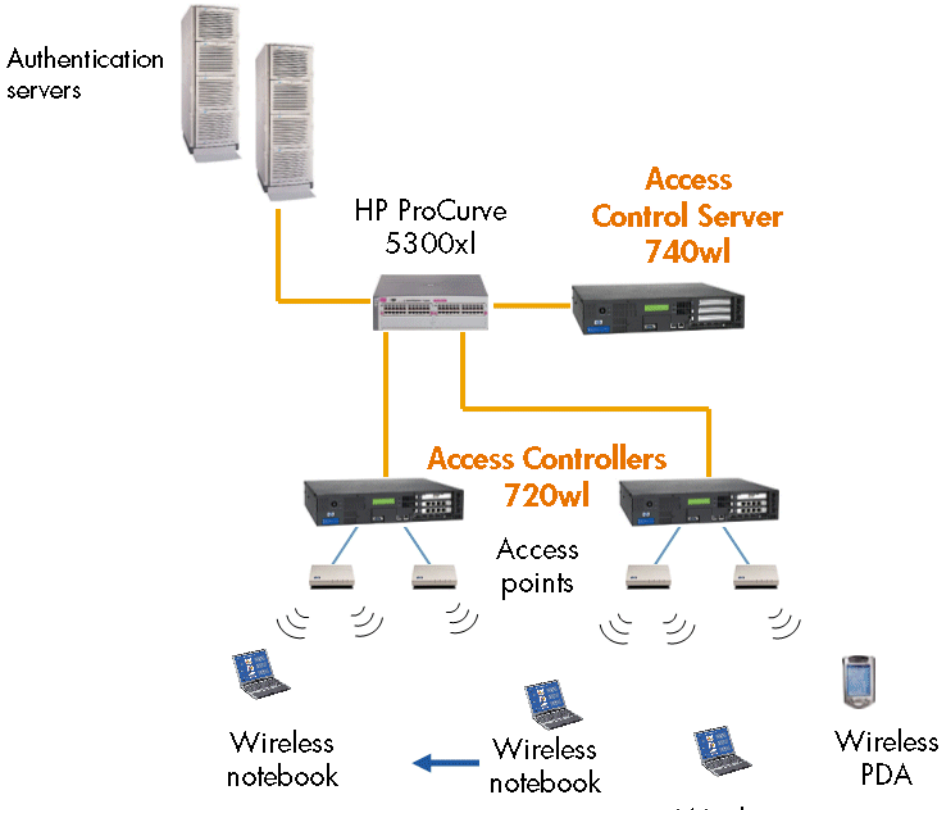

Figure 1-1. The 700wl Series system

The 700wl Series system consists of three logical functions:

- Access Controller
- Access Control Server
- Rights Manager

The HP ProCurve Secure Access 700wl Series hardware includes the Access Controller 720wl, the Access Control Server 740wl, which also incorporates the Rights Manager function, and the Integrated Access Manager 760wl, which combines an Access Control Server, the Rights Manager, and an Access Controller in a single physical unit.

The Access Controller 720wl

The Access Controller is positioned between each access point and the network. It inspects and filters each packet arriving from the wireless client through the access point, deciding whether to allow forwarding of the packet, redirect the packet, or drop the packet. The Access Controller makes these decisions by applying a set of rules that it has obtained from the Rights Manager.

Initially, the Access Controller knows of no connected devices. When a client sends a packet through a wireless access point, the AP forwards the packet to the network through the Access Controller. The Access Controller uses the received packet to determine the hardware MAC address of the client device, and requests an initial set of rights from the Rights Manager, through the Access Control Server.

The Rights Manager supplies a set of logon rights that allow specific access requests, such as DHCP, DNS, and HTTP requests, necessary to enable the client to connect to the network. The actual logon processing is normally handled by the Access Control Server—the Access Controller redirects client packets to the Access Control Server / Rights Manager, which uses the first HTTP request to require user authentication by means of an SSL-protected HTTP connection.

The Distributed Logon feature can be used to shift logon processing to the Access Controller—in this case, the Access Controller monitors client packets to detect a logon request and require user logon. After it obtains the client identity information, it requests authentication from the Rights Manager.

After verifying a user's identity, the Rights Manager sends a new rights package to the Access Controller. This rights package is based on a number of factors including the client's identity, the physical location through which he is connected to the network, and the current date and time of day. The Access Controller uses those rights to determine whether a packet from that client should be forwarded, redirected, or dropped.

The Access Controller is also responsible for maintaining Wireless Data Privacy encryption using PPTP, L2TP, or IPSec protocols.

Scalability is ensured by concentrating all packet-level inspection and rewriting functions and encryption at the Access Controller. An individual Access Control Server can easily supervise many Access Controllers.

The Access Controller provides a browser-based Administrative interface through which the administrator can configure various properties of the Access Controller. A Command-Line interface is also available through the serial console.

The Access Control Server 740wl

Each 700wl Series system administrative domain requires one Access Control Server. The Access Control Server performs several functions:

- Hosts the Rights Manager functionality
- Coordinates between the Access Controllers and the Rights Manager
- Coordinates Access Controller-to-Access Controller communications, such as a roaming handoff

When centralized logon is in place, packets from a newly connected client are forwarded by the Access Controller to the Access Control Server, which looks for logon traffic, serves up the logon page, and requests authentication from the Rights Manager.

To ensure scalability, once a client has been authenticated, all per-packet operations are confined to the Access Controllers. The Access Control Server merely coordinates the client meta-information among the Access Controllers.

In addition to filtering and redirecting packets, the Access Control Server coordinates with other Access Controllers throughout the 700wl Series system to maintain connections as a client device roams from one access point to another.

All policy and user database entries are kept in the Rights Manager, which is part of the Access Control Server.

Command and control communication between an Access Controller and the Access Control Server is through an encrypted connection. Command and control communication between Access Controllers is also through an encrypted connection. User packets that must be tunneled between Access Controllers to ensure transparent Layer 3 roaming are not encrypted.

Like the Access Controller, the Access Control Server also provides a browser-based Administrative interface through which the administrator can configure the 700wl Series system. Much of the configuration for the system as a whole is done through the Access Control Server administrative interface. A Command-Line interface is also available through the serial console.

The Integrated Access Manager 760wl

The Integrated Access Manager 760wl combines the Access Control Server and Rights Manager functinality along with an Access Controller in a single physical unit.

The Rights Manager

The Rights Manager is a module within the Access Control Server or Integrated Access Manager that supplies the Access Controller with appropriate client rights based on the characteristics of the client—who, when, and where. A client's rights include not only what access is allowed to resources on the network, but also include what type of security is required, and how addressing is handled (for example, Network Address Translation (NAT)). The Rights Manager may also handle the authentication of users, depending on the type of logon and security being used.

The Rights Manager also provides the browser-based interface that enables the network administrator to set up and edit Rights Manager settings, including the properties of groups, Locations (defined as a logical concept), "Wheres," "Whens," and users, as well as a number of global configuration options.

The overview of the Rights Manager presented in Chapter 6, "Getting Started with the Rights Manager" describes the concepts and terminology in more detail.

Wireless Data Privacy

Wireless data privacy is a feature of the 700wl Series system that enables strong encryption of data between a client and the Access Controller. Wireless data privacy provides additional security for data sent over the airwaves, supplanting the relatively insecure Wired Equivalent Privacy (WEP) of a wireless network.

The 700wl Series system offers four choices for encrypting data between a client and the Access Controller: PPTP, L2TP / IPSec, *pure* IPSec, and SSH. It also supports a variety of authentication and encryption algorithms related to these choices. It supports a number of client software packages that handle the client side of the security method.

In most cases, the 700wl Series system accepts the authentication performed by the security protocol, and provides user access rights as soon as the secure connection has been set up.

Once a secure connection as been set up, clients can roam between access points and the 700wl Series system will maintain their session, including the secure connection, transparently to the client.

User Authentication

The 700wl Series system Rights Manager provides a great deal of flexibility in how users can be authenticated. The Rights Manager supports three types of authentication:

- **Browser-based logon:** With Web-based logon, the Rights Manager presents a browser-based logon page the first time a client attempts an HTTP access. After the user enters a login ID and password, the Rights Manager authenticates the user using one or more Authentication services, such as an LDAP database, RADIUS server, Kerberos service, or through the Rights Manager's own built-in authentication database.
- **Wireless Data Privacy logon**: With wireless data privacy logon, the client initiates a connection to the network using an L2TP or PPTP client. The Rights Manager uses the login information provided by the VPN client for authentication via RADIUS or the built-in database. In this case, the user does not see theHP ProCurve logon page.
- **Monitored logon:** The 700wl Series system supports both 802.1x logon and NT Domain logon. In both these cases, the system simply forwards the packets on to the RADIUS or NT Domain server, and monitors the response to determine whether the user has been successfully authenticated. Once the client has been authenticated, rights for the client are requested from the Rights Manager. As with wireless data privacy logon, the user does not see the HP ProCurve logon page.

The Rights Manager uses the concept of authentication ***Realms***, which are simply ordered lists of one or more authentication services. By defining multiple authentication realms, you can use different authentication methods for users logging in through different locations.

An ***authentication service*** is a single instance of a service used for authentication, such as a specific Active Directory service, or RADIUS server. The Rights Manager supports the following services:

- LDAP Directory services, such as Active Directory or iPlanet LDAP server
- RADIUS servers
- Kerberos services

- XML-RPC-based services
- The Rights Manager's built-in database. This is the default authentication service. You can populate it with user names and passwords through the Rights Manager.

Both before and after authentication, clients are identified to the 700wl Series system by MAC address rather than IP address. This greatly facilitates the support of seamless, transparent roaming.

User Authentication is discussed in detail in Chapter 9, "User Authentication".

Client Access Rights

At any given time, for each client attached to an Access Controller, a certain set of rights is in effect. These rights are based on a number of factors, including whether the client has been authenticated, the client's group membership and the "location" through which he/she connected to the 700wl Series system.

- The Rights Manager uses ***Groups*** to define what network resources a user can access at any given time. Access rights are defined for a group, and an individual user's rights are determined by the groups to which he/she belongs.
- The Rights Manager uses ***Locations*** (in a logical sense rather than a strictly physical one) to define which users can access the network at any given time, what sorts of logon and authentication mechanisms may be used, and what type of security is required (for example, is encryption required or not).

Some properties, such as how a client's addressing is handled (Network Address Translation (NAT) vs. real IP addresses vs. static IP addresses) is affected both by settings at the Location and by settings for the Group.

Locations

A Location is a logical construct that represents an entry point or set of entry points to the HP ProCurve 700wl Series system. Every client that accesses the HP system is always associated with a location. A location is *associated with* a set of physical entry points, but should not be confused with the physical entry points themselves.

A location does not directly define access rights for a user (that is done by the user's group membership) but it may modify or limit the scope of a user's rights. A location has the following properties:

- A list of ***Wheres*** that defines the Access Controllers, ports, or specific clients that are associated with this location.
- A list of the times (time of day, days of the week, and so on) when access through this location is allowed. This list is actually a set of named time specifications, called ***Whens***. A When is defined independently of a location, so you can define a time specification once and then use it for multiple locations or groups.
- A list of groups that are allowed at this location. This determines which users can gain access to the system through this location.
- Whether encryption is required, allowed, or disabled, and what types are supported.

- How authentication is handled for the supported tunneling protocols.
- Whether Network Address Translation (NAT) is required for clients entering through this location. This setting interacts with the NAT setting for the location. Chapter 6, “Getting Started with the Rights Manager” includes a more extensive discussion of addressing considerations and NAT.

Location properties are discussed in detail in Chapter 8, “Setting Up Locations”.

By default, the HP ProCurve 700wl Series system provides a predefined location named **Everywhere else** which represents all entry points into the system that are not specifically included in another location. By default, it is valid at all times. Until you create another location, this is the location to which *all* clients are associated.

Groups

Groups are used to define the access rights (and certain other capabilities) for all clients / users that are members of the group. Clients / users are given access rights within the network based on their group membership. The group construct allows you to define the rights for multiple users in a single operation. The following points are key to understanding rights in the HP system:

- Access rights, as defined by packet filters and session redirectors (via “Allows” and “Redirects”) are always defined through groups, and only groups.
- Every client that accesses the 700wl Series system is *always* a member of at least one group, and that group membership is what determines the access rights that are given to the client.

In many cases, group membership is implicit, and occurs by default. For example, when a client is detected at a location, it automatically becomes a member of a Logon group. Logon group membership gives the client the access rights necessary to log on to the system. Once a client has logged on, he / she will become a member of one or more other groups based on the results of the logon / authentication process. These groups may be ones defined by the administrator, or groups provided by default with the 700wl Series system.

A group defines the following properties:

- Access rights for members of this group. This includes ***Allows***, which specify the destinations to which traffic is allowed (forwarded) for members of this group, and ***Redirects***, which specify traffic destinations that should be redirected to alternate destinations for members of this group. Allows are implemented through a set of packet filters that determine what traffic the client is allowed to generate. Redirecting client TCP and UDP sessions from their original destination IP address or port is useful, for example, to force HTTP clients to login, or to ensure that certain requests for network services, such as DNS, are directed to the appropriate servers.

  Filters and redirectors match packets using the powerful pattern matching language introduced by the `tcpdump` utility program.
- A list of the times (time of day, days of the week, and so on) when these rights are in effect, specified as a list of “Whens.”
- An ***Expiration*** timer or setting, which specifies how long a member of this group may remain logged on before he / she will be required to reauthenticate.

- A ***Linger*** timer, which defines how long a client will be maintained as logged on after it appears to have been disconnected (based on a failure to respond to probes from the Access Controller). The linger timer is used to allow a client time to roam from one Access Controller to another without needing to log on again. If the linger timer expires, the client is assumed to have disconnected and is logged off.
- Whether client addresses should be translated via NAT, and if so, under what circumstances. This setting interacts with the NAT setting for the location. Chapter 6, "Getting Started with the Rights Manager" includes a more extensive discussion of addressing considerations and NAT.

Roaming Support

One of the key features of the 700wl Series system is its support of Layer 3 roaming—enabling clients to move around physically between access points without having to reauthenticate or establish a new session.

Because the 700wl Series system identifies clients by MAC address, it is simple to detect when a device roams. The Linger Timer determines the length of time a client has to complete a roam (to appear at a new physical location after disappearing from the old physical location). If the client completes the roam within the linger time, no reconnect or authentication is needed—the client's connection state is maintained intact. Only if the client fails to complete the roam before the linger timer expires does the system decide that the client has actually disconnected and logs it off.

How the 700wl Series system handles roamed sessions depends on the protocol used to connect to the 700wl Series system, and whether the client's IP address has been mapped using NAT or not.

When a NAT'ed client roams between Access Controllers (rather than simply between ports on a single Access Controller) the Access Control Server can move the entire connection state from the original Access Controller to the "roamed-to" Access Controller. In general, sessions that are currently running are tunneled back to the original Access Controller, but new sessions are established through the new connection point. However, if the client is using a "real" IP address, then *all* connections are tunneled back to the original Access Controller. The other exception is if the client is connected via PPTP or L2TP—in that case the PPTP/L2TP session as a whole is tunneled back to the original Access Controller.

Network Address Translation

By default, an Access Controller provides Network Address Translation (NAT) services for clients that request a DHCP IP address when they initiate a connection to the Access Controller. The 700wl Series system implements NAT as a form of "overloading," where a range of private IP address are mapped to a single public IP address (the IP address of the Access Controller) by using TCP ports. When a client sends a packet through the Access Controller, the Access Controller rewrites the IP address field and the port number field to a value that is unique within the entire 700wl Series system and that can be used to identify any return packets.

Although NAT is enabled by default in the 700wl Series system, you can elect whether to use it or not, depending on your application. Following are some points in favor of using NAT within the 700wl Series system:

- NAT makes roaming much more efficient. Because each NAT address is unique for the entire 700wl Series system, the client's connection state can be moved upon a roam, rather than requiring every connection to be tunneled back to the original Access Controller.
- NAT provides some amount of protection to a client since no device other than the Access Controller can talk directly to the client. This provides rudimentary firewall protection.
- Allowing NAT can ensure that a client will be able to successfully communicate with the network—if NAT is not allowed, and a client has an IP address that is not within the subnet used by the Access Controller, return packets will not be able to reach it. This can occur if the client uses a static IP address or receives an IP address from an external DHCP server.

However, certain applications may require a host or server system to know the actual IP address of a client. Some examples include multi-player games, file transfer in Instant Messenger applications, and other peer-to-peer applications.

To allow flexibility, the 700wl Series system provides alternate addressing schemes:

- Use NAT only if the client's IP address is on the wrong subnet (i.e., not within the Access Controller's subnet). Otherwise, use the client's real or static IP address.
- Always use the client's real or static IP address and never use NAT, regardless of the subnet. (This setting is intended for use by clients that are actually Access Points, and should be used with caution).

There is one case where NAT will always be used—when PPTP/L2TP tunneling is used.

Chapter 6, "Getting Started with the Rights Manager", includes a more extensive discussion of addressing considerations and NAT. See Chapter 7, "Configuring Groups", and Chapter 8, "Setting Up Locations", for more information about configuring NAT.

VLAN Tag Support

The 700wl Series system provides support for Virtual LAN (VLAN) tagging in several ways. It can pass through VLAN ID information that is included with the traffic from a client, and can also use that VLAN tag to assign a client as a group member. It can also assign wireless clients that do not have pre-existing VLAN membership to be members of a VLAN based either on their group membership, or on the location through which they access the 700wl Series system. In this mode, the 700wl Series system adds the specified VLAN ID to the packets from the client before sending them on into the network.

The 700wl Series system does not change a client's VLAN ID if one is present in incoming packets—a pre-existing VLAN tag overrides the VLAN ID specified through a location or group.

The 700wl Series system does not enforce VLAN membership—it simply passes tagged traffic on to the network as appropriate based on the client's user rights.

The 700wl Series system supports VLAN trunking automatically—this does not require any special configuration.

CONFIGURING A 700WL SERIES SYSTEM 2

This chapter describes how to configure the Integrated Access Manager 760wl, Access Control Server 740wl, and Access Controller 720wl so that they work with your enterprise network after you have installed it, as described in the *HP ProCurve Secure Access 700wl Series Installation Guide*. It includes the following sections:

Configuration Overview 2-1
Administrator Login 2-2
Changing the Admin Authorization Settings 2-5
Changing the Network Configuration 2-6
Configuring the Shared Secret for Access Controllers 2-16
HTTP Proxy Server Configuration 2-18
Configuring SNMP 2-20
Specifying Location Information 2-22
Specifying Session Logging 2-23
Configuring the Time and Date 2-24
Viewing Online Documentation and Help 2-26

Note: *You can also use the 700wl Series command-line interface for configuration. The CLI is described in Appendix C.*

Configuration Overview

The configuration of the 700wl Series system has several aspects to it.

- Basic device configuration, such as network addressing and configuration, SNMP configuration, date and time, as well as system maintenance functions such as software updates, backup and restore, are done from the Administrative Interface on the Integrated Access Manager, Access Control Server, or Access Controller.
- Certain other configuration functions, such as enabling HTTP proxy functionality, session logging, and wireless data privacy, are done centrally on the Access Control Server or Integrated Access Manager, and the settings are then propagated to all connected Access Controllers. When the settings for any of these functions change on the Access Control Server or Integrated Access Manager, the updated information is propagated automatically to any connected Access Controllers.

The information propagated from an Access Control Server / Integrated Access Manager to connected Access Controllers includes the following:

- The Access Control Server's IP address
- The shared secret
- The session logging configuration (enabled / disabled and, if enabled the IP address of the Syslog server and the Syslog facility setting).
- The IPSec configuration (enabled / disabled and the various IPSec configuration options)
- The PPTP and L2TP settings (enabled or disabled)
- The SSH setting (enabled or disabled)
- Whether logons are handled centrally or are distributed (handled by the Access Controllers).
- The DHCP address range used to create private addresses for NAT clients.

• Finally, there are several configuration options, such as port configuration, location information, and status operations such as viewing lists of active clients and active sessions, that can be performed only from an Access Controller or from an Integrated Access Manager.

These device-related configuration functions are discussed in the first part of this manual (this chapter and the following three chapters).

In addition, there are a number of configuration options that relate to how users / clients access the 700wl Series system and through it, the network. These include logon and security options, user authentication options, and user access rights for network services, all of which can be set differently for groups of users and by access points into the system. These configuration options are set and modified through the Rights Manager which is discussed in Part 2 of this manual.

Administrator Login

To log in to the Administrative Interface, do the following:

Step 1. Set your browser to the IP address or hostname of your Integrated Access Manager, Access Control Server, or Access Controller, and press ENTER.

The Administrator Login page appears, as shown in Figure 2-1.

Note: *A system connected directly to an Access Controller's or Integrated Access Manager's downlink ports can access the Administration web interface through the specially recognized URL:* `http://42.0.0.1`.

Note: *Your browser must accept cookies to log in.*

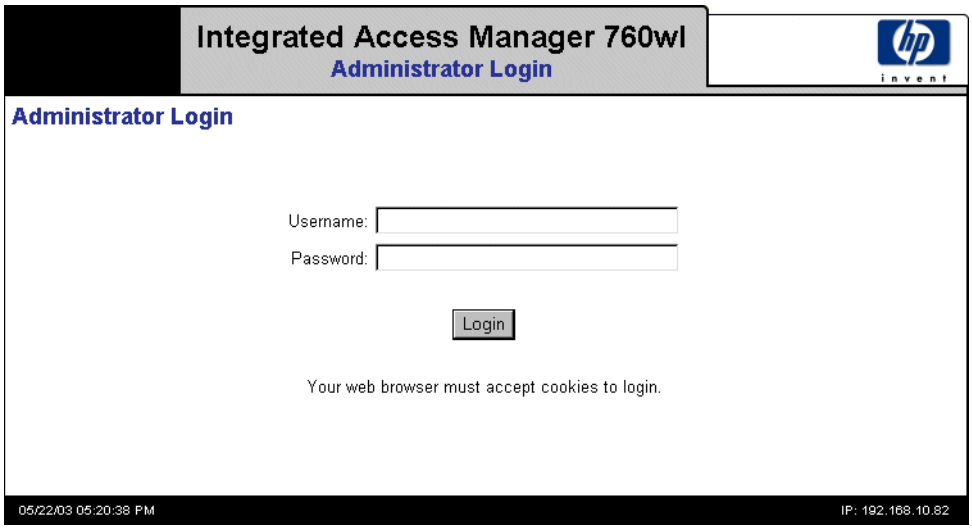

Figure 2-1. Administrator's Login to an Integrated Access Manager

> ***Note:*** *The page title appears appropriately depending on whether you are connected to an Integrated Access Manager, Access Control Server, or Access Controller.*

Step 2. Type your administrator username.

Step 3. Type your administrator password.

> ***Note:*** *By default, the system ships with the user name* `admin` *and password* `admin`*. It is strongly recommended that you change this as soon as you have set up your system.*

Step 4. Click **Login**.

The Main Menu appears. Figure 2-2 shows the Main Menu for the Integrated Access Manager. Figure 2-3 shows the Main Menu for the Access Control Server. Figure 2-4 shows the Main Menu for the Access Controller.

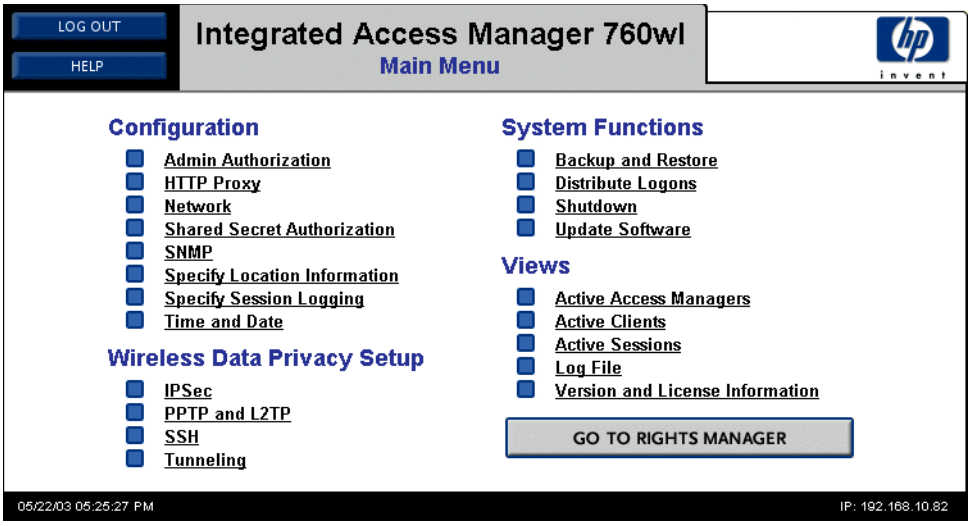

Figure 2-2. Main Menu for the Integrated Access Manager

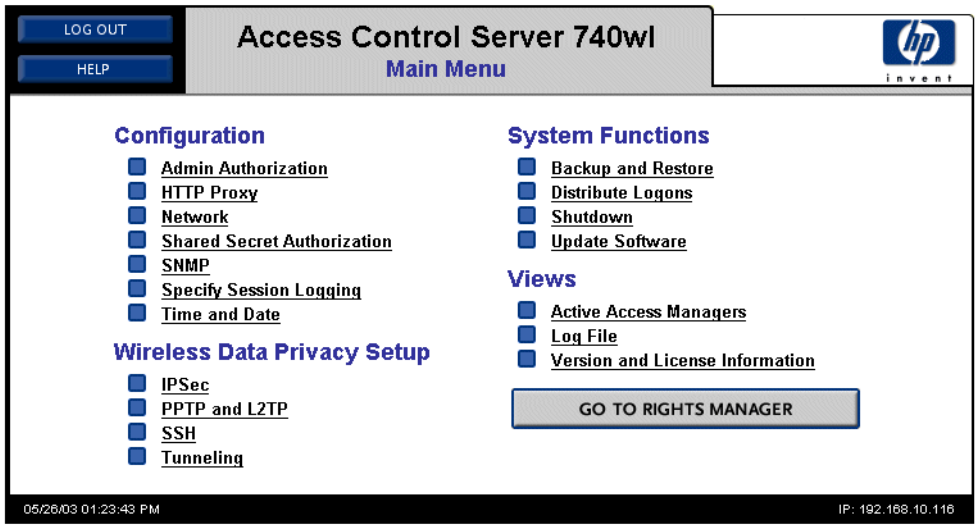

Figure 2-3. Main Menu for the Access Control Server

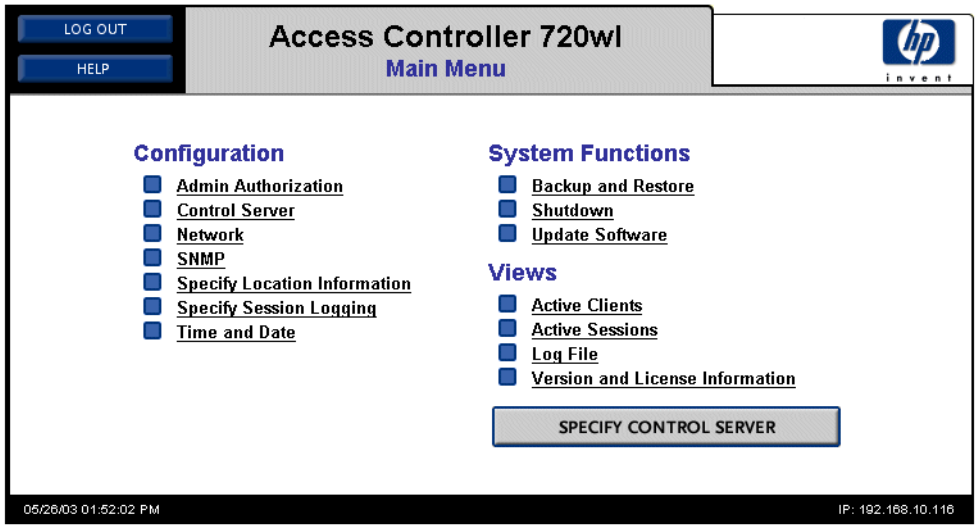

Figure 2-4. Main Menu for the Access Controller

Note: *If you have not yet specified the Access Control Server IP Address and shared secret, the* **GO TO CONTROL SERVER** *button is instead labeled* **SPECIFY CONTROL SERVER**.

This chapter explains the Configuration functions of the Main Menu; other topics are discussed in other chapters, as shown in Table 2-1.

Table 2-1. Topics in Other Chapters

Topic	Chapter
Wireless Data Privacy Setup (Integrated Access Manager and Access Control Server only)	3
System Functions	4
Views (Viewing System Status)	5

Changing the Admin Authorization Settings

The Administrator Authorization function enables you to change the administrator username and password. It is strongly recommended that you change these as part of the initial setup of your system—in fact, this is included in the installation instructions for your system. However, you can change the admin username and password at any time while you are logged in to the Administration interface.

To change the admin user name and password:

Step 1. Click **Admin Authorization** from the Main Menu.

The Admin Authorization Configuration page appears (see .

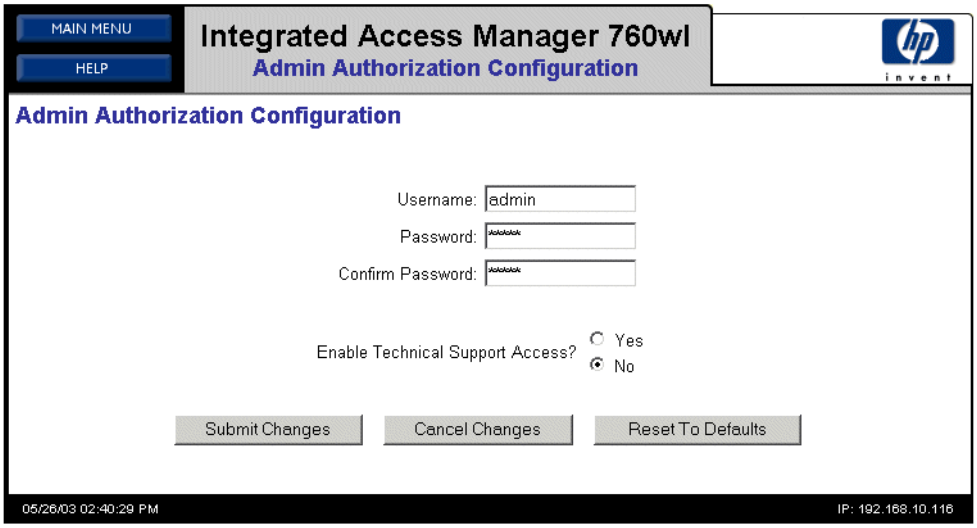

Figure 2-5. Changing the Admin username and password

Step 2. Enter the new username in the **Username** field.

Step 3. Enter the new password twice, in the **Password** and **Confirm Password** fields.

Step 4. Click **Submit Changes**.

A confirmation message is displayed indicating that these settings have been changed.

To restore the default admin username (`admin`) and password (`admin`) click the **Reset to Defaults** button. Again a confirmation message is displayed.

The Admin Authorization page is also where you can enable access for the Technical Support personnel. You should enable this feature *only* if directed to do so by your Technical Support contact.

Changing the Network Configuration

The *HP ProCurve Secure Access 700wl Series Installation Guide* leads you through the initial network configuration. However, if your network configuration changes after installation, you can modify your settings through the Administrative Interface.

To change your network configuration:

Step 1. Click **Network** from the Main Menu.

Figure 2-6 shows the Network Configuration page for an Integrated Access Manager. The display for an Access Controller looks the same.

Figure 2-7 shows the Network Configuration page for the Access Control Server.

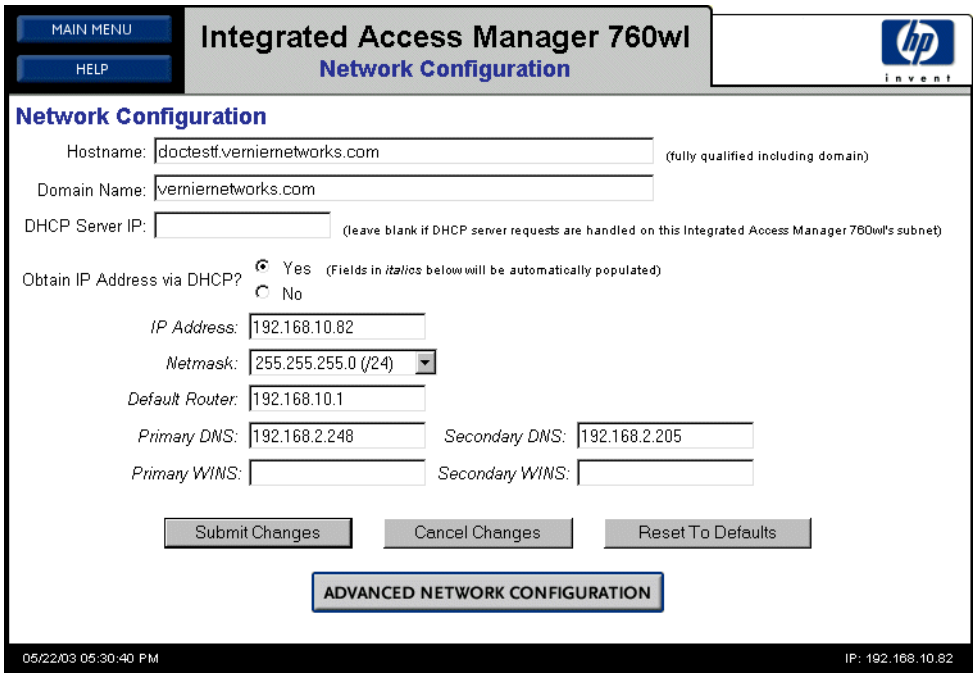

Figure 2-6. Network Configuration for the Integrated Access Manager

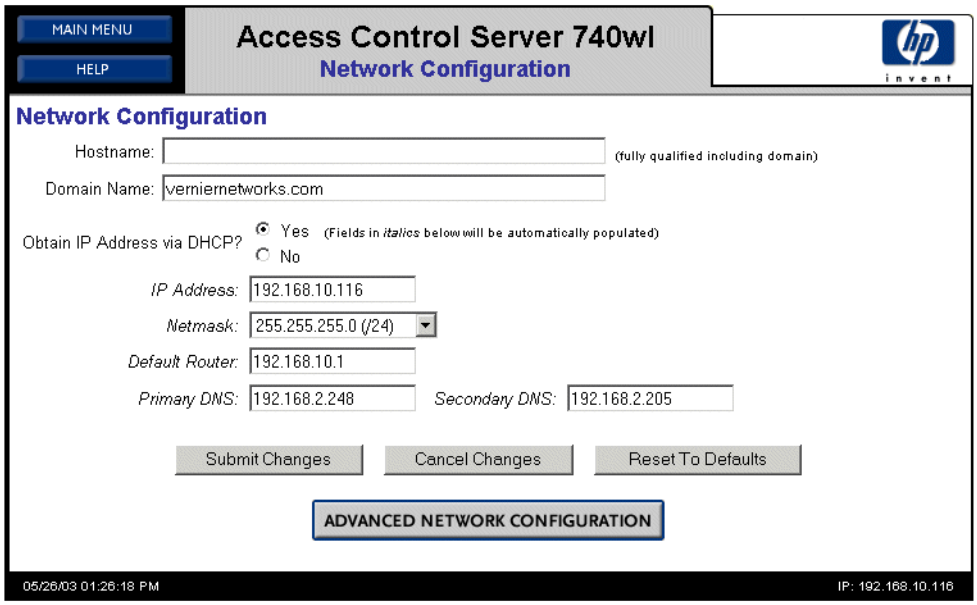

Figure 2-7. Network Configuration for the Access Control Server

Step 2. Type a hostname as a fully qualified domain name. Assigning a hostname is optional.

If you do enter a hostname, it must be fully qualified. The DNS at your site must be able to resolve the hostname to the IP address you select, with both forward and

reverse lookups. If you enter a hostname that cannot be resolved, you may not be able to access the unit.

Note: *HP recommends creating a hostname. Using a hostname prevents system users from getting SSL warnings about an unknown SSL certificate when they first access the Logon page.*

Step 3. Type the name of the domain in which this system resides. This will be used as the default domain, and appended to any host names that are not fully qualified.

Step 4. If this Integrated Access Manager or Access Controller is going to send client DHCP requests to a DHCP server that is *not* on the same subnet, and is not reachable through a DHCP-forwarding router, type the address of the DHCP server in the **DCHP Server IP** field. This enables the Access Controller to relay the client's DHCP request to the DHCP server at the specified address.

Note: *You **must** enter the DHCP server IP address if you plan to specify IP subnet ranges for individual ports on the Advanced Network Configuration page.*

Leave this field blank if DHCP server requests are handled on this Access Controller's or Integrated Access Manager's subnet.

This field does not appear on an Access Control Server.

Note: *This applies only to clients that are not using Network Address Translation (NAT), since a network-address translated client will have its DHCP request satisfied by the Integrated Access Manager or Access Controller itself.*

Step 5. If the Integrated Access Manager, Access Controller, or Access Control Server gets its own IP address through DHCP, click **Yes** to **Obtain IP Address via DHCP**.

If you choose **Yes**, the system will request its IP address, subnet mask, gateway, DNS server and WINS server IP addresses from the DHCP server. You can then skip steps 6 through 10 and go directly to step 11.

Note: *If you are changing from a static IP address to use DHCP, do not change the values in the fields that follow it (IP address, default gateway, etc.). They will be cleared and reset appropriately when you submit your changes. If you type in these fields (even just to clear them) the system assumes you are attempting to set an address, and will not enable DHCP.*

If you choose **No**, you must enter the information into the following fields.

Step 6. Type the IP address of your system.

Step 7. Choose a **Netmask** from the drop-down box. This defines the subnet for this system.

Step 8. Type the **Default Router** IP address.

Step 9. Type the **Primary DNS** server IP address, and if applicable, the **Secondary DNS** server IP address.

Step 10. If applicable, type the **Primary WINS** and **Secondary WINS** addresses. (This option does not appear for an Access Control Server.)

Step 11. Click **Submit Changes** to save your settings.

Step 12. Click the **Advanced Network Configuration** to configure advanced network settings, as described in "Advanced Network Settings".

Advanced Network Settings

From the Advanced Network Configuration page of a 700wl Series system, you can configure some additional network settings.

On an Access Controller you can configure settings for:

- Bridging— lets you enable or disable Ethernet bridging and specify the type of traffic that should be bridged
- Client Probes—lets you set the interval for probes of an idle client, and the time-out after which an idle client will be disassociated from the Access Controller.
- Broadcasting—lets you specify ports to which broadcast traffic should be forwarded
- Port Settings—lets you specify the connection type and IP subnet address for individual ports on an Access Controller or Integrated Access Manager.

  The Connection Type settings let you configure the media type of the port.

  The IP subnet address is used in two ways:

  — If you have configured an external DHCP server, then for non-NAT clients that request an IP address via DHCP, the port's subnet IP address range is used to specify to the DHCP server the IP address range for clients on this port. This subnet address range does *not* need to be related to the subnet range used by the Access Controller or Integrated Access Manager.

  — It defines the range of valid IP addresses for clients in a group with a NAT setting of **Do not NAT except for clients on the wrong subnet**. In this case, if a client appears on this port with an IP address outside the range specified for the port, that client's address will be NATed.

On an Access Control Server, you can configure settings for:

- DHCP Network for NAT Clients—lets you specify a network address range other than 42.x.x.x to be used by the internal 700wl Series system DHCP server for clients that will be NATed. You can also specify parameters such as the lease time.
- Port Connection Type—lets you configure the media type of the port used as the network uplink.

On an Integrated Access Manager, you can configure all the settings found on both the Access Control Server and Access Controller.

To configure advanced network settings:

Step 1. Click **Advanced Network Configuration** on the Network Configuration page.

The Advanced Network Configuration page appears.

For an Access Control Server, the Advanced Network Configuration page shows only the DHCP Network for NAT Clients settings, and the Connection Type column of the Port Settings table. Figure 2-8 shows the Advanced Network Configuration page for the Access Control Server.

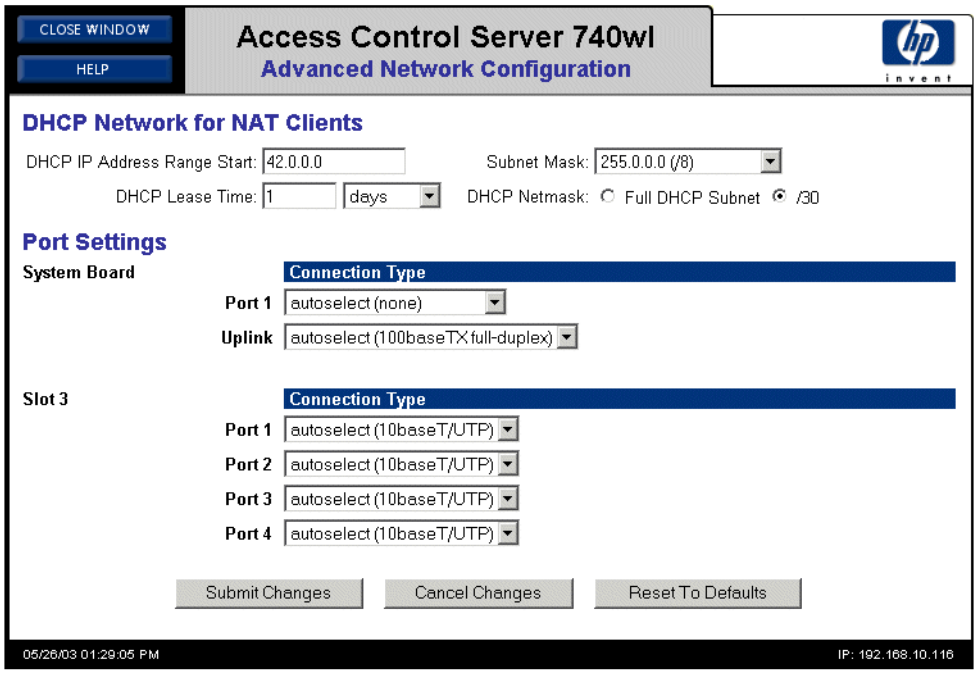

Figure 2-8. Advanced Network Configuration page for an Access Control Server

Figure 2-9 shows the Advanced Network Configuration page for an Integrated Access Manager. The page for an Access Controller is similar, but does not include the DHCP Network for NAT Clients settings.

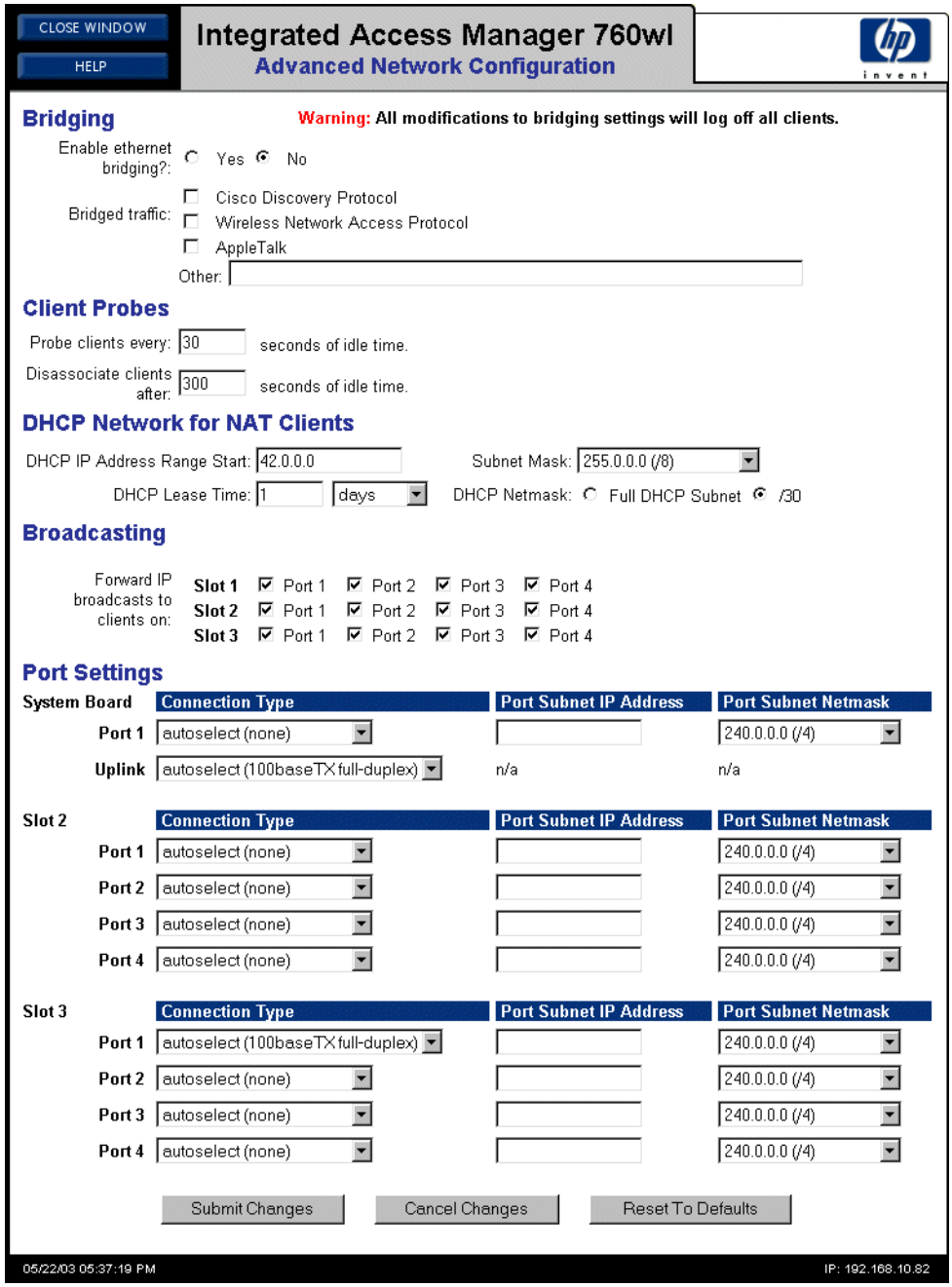

Figure 2-9. Advanced Network Configuration page for an Integrated Access Manager

The example in Figure 2-9 shows an Integrated Access Manager 760wl with two four-port option cards installed. The port shown as System Board Port 1 is the port labeled *Reserved* next to the Uplink port on a 700wl Series chassis. This port is reserved for future use as a management port, but can be used as an extra downlink port. Up to thirteen downlink ports may be displayed for an Integrated Access Manager 760wl or Access Controller 720wl, depending on your system configuration.

Note: *The Broadcasting section of this page displays only downlink ports. The default uplink port normally does not appear. However, if you have reconfigured the uplink port so that the default uplink (slot 0 port 2) is now a downlink port, then that port* ***will*** *appear on this page. The port being used as the uplink port will not appear.*

Bridging

Note: *This setting appears only on the Advanced Network Configuration page of an Access Controller or Integrated Access Manager. You cannot set this from an Access Control Server.*

A 700wl Series system provides filtering and redirection of IP packets at Layer 3. With bridging, you can specify certain Layer 2 packets to be copied across an Integrated Access Manager or Access Controller to the clients.

Caution: *Any modifications to the bridging settings will log off all clients.*

Step 1. To **Enable Ethernet Bridging** for this Integrated Access Manager or Access Controller, click **Yes**.

Bridging is disabled by default.

Step 2. Specify the type of **Bridged Traffic**:

a. Click **Cisco Discovery Protocol** to enable CDP packets through this Integrated Access Manager or Access Controller.

This Layer 2 protocol is used by Cisco network hardware and software to manage a network of Cisco devices.

b. Click **Wireless Network Access Protocol** to enable WNMP packets through this Integrated Access Manager or Access Controller.

This Layer 2 protocol is used by Symbol Technologies, Inc. network hardware to manage a network of Symbol devices.

c. Click **AppleTalk** to enable AppleTalk packets to be passed through this Integrated Access Manager or Access Controller.

d. Click **Other:** to enable bridging of other Layer 2 traffic, and type a traffic specification into the text field.

You can create a traffic specification using arbitrary `tcpdump` syntax. Any traffic specifications (`tcpdump`-enabled packets) you enter here are in addition to those enabled by checking the CDP, WNMP, or AppleTalk options.

See Appendix A for a description of the `tcpdump` syntax.

The following are some examples of traffic specifications in `tcpdump` syntax:

Traffic to enable	tcpdump syntax
Enable IPX traffic	ether[12:2] = 0x8037 or ether[12:2] = 0x8137

Note: *You may need to ensure that you also have the appropriate Allow rights defined in the Rights Manager to allow this type of traffic from a client.*

Client Probes

Note: *This setting appears only on the Advanced Network Configuration page of an Access Controller or Integrated Access Manager. You cannot set this from an Access Control Server.*

After a client has been idle for a specified period of time (by default 30 seconds), the Integrated Access Manager or Access Controller probes the client to determine if it is still connected. If the system has not received a response to repeated probes after another interval (by default five minutes) the system disassociates the client.

When the Access Controller disassociates a client, the following happens:

- The Access Controller removes the client, the client's MAC address, and the definition of its rights from memory.
- The Access Controller sends a message to the Rights Manager that the client is no longer connected. The Rights Manager starts the ***linger timer*** for that client. If the client has not re-established communication before the linger timer expires, then the client must re-authenticate.

To change the client probe settings, do the following:

Step 1. To change the interval between successive client probes, change the value in the **Probe clients every:** field. The default interval is 30 seconds.

When the client is idle, that is, when it is not sending any packets to the network, this timer runs. When the client probe timer expires, the Integrated Access Manager or Access Controller probes the client by sending it an ARP request. The Integrated Access Manager continues sending ARP requests at the specified interval as long as the client is idle, until the time-out is reached.

Step 2. To change the time-out counter, which determines when the client should be disassociated, change the number of seconds in the **Disassociate clients after:** field.

This counter determines how long a client must be idle before the Access Controller disassociates that client.

See Chapter 7, "Configuring Groups", for more information on the linger timer.

DHCP Network for NAT Clients

Note: *This setting appears only on the Advanced Network Configuration page of an Access Control Server or Integrated Access Manager. You cannot set this from an Access Controller.*

You can specify the subnet that should be used as the source of private IP addresses assigned to clients by the internal 700wl Series system DHCP server. You can also specify the DHCP lease time.

Note: *As of software version 3.1, this address is set on the Access Control Server, and affects all Access Controllers that are connected to the Access Control Server. You cannot use a different DHCP address range for NAT clients on different Access Controllers.*

Note: *When you change this range, it also changes the default address (*`http://42.0.0.1`*) for the Administrative Interface. The Administrative Interface URL will become the first address in the new range. For example, if you set the DHCP IP address range to be* `192.168.128.0/24`*, then the URL for the Administrative Interface becomes* `http://192.168.128.1`*.*

To specify the DHCP address and lease time, do the following:

Step 1. Type the starting IP address for the DHCP range into the **DHCP IP Address Range Start** field. The default address is `42.0.0.0`.

Step 2. Select the **Subnet Mask** from the drop-down list of possible masks.

Step 3. Type a value for the **DHCP Lease Time**, and choose one of the time units from the drop-down list. You can specify the lease time in seconds, minutes, hours, days, weeks or months (of 31 days each). The default lease time is 1 day.

Step 4. Normally, you should not change the **DHCP Netmask** setting. It defaults to `/30` and this is the recommended setting. However, under some circumstances where you have users with multiple interfaces (such as a laptop using a wireless connection that is plugged into a docking station with a wired interface) you may need to change this setting. If clients are having access problems caused by losing the route to the private address when a second interface is present, select the **Full DCHP Subnet** setting.

Broadcasting

Note: *These settings appear only on the Advanced Network Configuration page of an Access Controller or Integrated Access Manager. You cannot set this from an Access Control Server.*

Enabling broadcasting allows broadcast IP packets to be transmitted to all clients on the selected ports, even clients that have not been authenticated.

To enable broadcasting:

- Click the checkboxes for those ports on which you want to Forward broadcast IP packets to clients. You can click none, some, or all of the ports.

Caution: *Enabling this functionality permits broadcast IP packets to be transmitted to* ***all*** *clients on the selected ports, including unauthenticated clients. In some circumstances, broadcast IP packets may contain sensitive information that network administrators prefer to keep from unauthenticated users.*

Port Settings: Connection Type

The Connection Type settings let you specify the media type and options for each I/O port. Port Settings are available on the Advanced Network Configuration page of all 700wl Series system types.

The **Connection Type** field shows the configured connection type, and the type of the actual connection detected at the port, if different from the configured type. In Figure 2-9 (on page 2-11) all ports are configured for autoselect (allowing autonegotiation to determine the port settings). For the ports where no media is connected, the value in parentheses is **none**.

For the ports where a connection exists, the actual connection type is shown in parentheses. If the port is configured for a specific connection type, and the actual connection matches the configured type, the connection type is displayed only once (no parentheses).

For port configuration, the Connection Type field provides a drop-down list with the possible settings allowed for the port. Figure 2-10 shows an example of a drop-down list. The items in the list depend on the type of port.

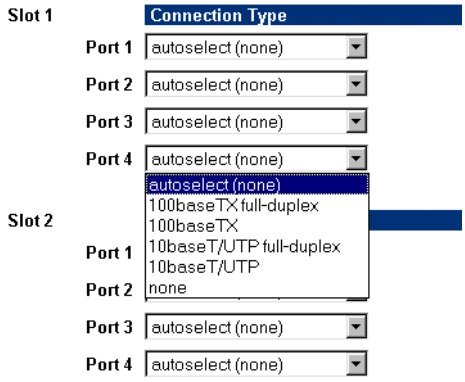

Figure 2-10. Example of a port media selection list

To configure a port for a specific port type, do the following:

Step 1. Select the port type from the list provided in the drop-down list.

> ***Note:*** *If you want to set a port to half-duplex, but half-duplex is not offered as an option in the drop-down list, you will need to select a setting that does not specify an option, and allow the port to negotiate for half-duplex. For example, as shown in Figure 2-10, there is no setting for 100baseTX half-duplex. You must specify 100baseTX and allow the port to negotiate for half-duplex.*

Step 2. Click **Submit Changes**.

A confirmation page appears.

The port configuration process takes several seconds to take effect. When you initially return to the Advanced Network Settings page, the connection type shown in parentheses may reflect the previously configured type. You may need to refresh the page to update the display for the new type.

Port Settings: Port Subnet IP Address and Netmask

> ***Note:*** *These settings appear only on the Advanced Network Configuration page of an Access Controller or Integrated Access Manager. You cannot set this from an Access Control Server.*

The Port Subnet IP Address and Port Subnet Netmask lets you specify a subnet address range for each Access Controller port. If you provide an IP address and subnet mask for a

port, then for clients that are allowed to use a real IP address (non-NAT mode clients) the following occurs:

- If the client makes a DHCP request, and you have configured an external DHCP server IP address, the Access Controller or Integrated Access Manager relays the DHCP request and indicates that the client originating the request is on the subnet as specified in the Port Settings for that particular port. This informs the external DHCP server that it should allocate an IP address on that subnet.
- If the client is allowed to use a real IP address, and the client uses an IP address on the subnet as defined by the Port Settings for that particular port, then the Access Controller or Integrated Access Manager will not NAT that client's sessions.

In either case, for packets *from* the network to a client IP address on a subnet defined in the Port Settings, the Access Controller or Integrated Access Manager will forward those packets to the appropriate client.

Note: *You **must** specify the DHCP Server IP address in the DHCP Server IP field on the main Network Configuration page in order to specify port IP subnet ranges. If you have not done so, a warning will be displayed.*

To configure subnet addresses for Access Controller or Integrated Access Manager ports:

Step 1. Configure the **Port Settings** as appropriate, by entering the IP address and selecting a netmask from the drop-down list in the Netmask field for each port.

Step 2. Click **Submit Changes**.

To restore the settings to the predefined default settings, click **Reset to Defaults**.

Note: *There are no restrictions on the IP addresses that can be used for port settings in relationship to the Integrated Access Manager or Access Controller's IP address. However, your upstream routers must have static routes configured to support routing the addresses you have configured for your ports through the Access Controller or Integrated Access Manager uplink port.*

For example, if the Access Controller's IP address is `192.168.2.20` with subnet mask `255.255.255.0 (/24)` and you configure a port to use `192.168.6.0` with mask `/24`, you must configure your router with a static route that routes the `192.168.6.x` addresses to `192.168.2.20`. You can typically do this with a command similar to:

```
ip route 192.168.6.0 255.255.255.0 192.168.2.20
```

Configuring the Shared Secret for Access Controllers

Each Access Controller system must prove to its Access Control Server (or Integrated Access Manager) that it is trusted. A shared secret is used between the Access Controller and the Access Control Server to establish this trust relationship. You must set this shared secret on both the Access Control Server and on each Access Controller that communicates with that Access Control Server. If an Integrated Access Manager controls one or more external Access Controllers, a shared secret must be configured between the Integrated Access Manager and those Access Controllers.

The *HP ProCurve Secure Access 700wl Series Installation Guide* leads you through the initial configuration of the shared secret and (on an Access Controller) the Console Server's IP address. However, you may need to change the shared secret at a later time, or reconfigure an Access Controller to communicate with a different Integrated Access Manager or Access Control Server.

Setting the Shared Secret on the Access Control Server

To set the shared secret on an Integrated Access Manager or Access Control Server:

Step 1. Click **Shared Secret Authorization** from the Main Menu.

The Shared Secret Authorization Configuration page appears, as shown in Figure 2-11.

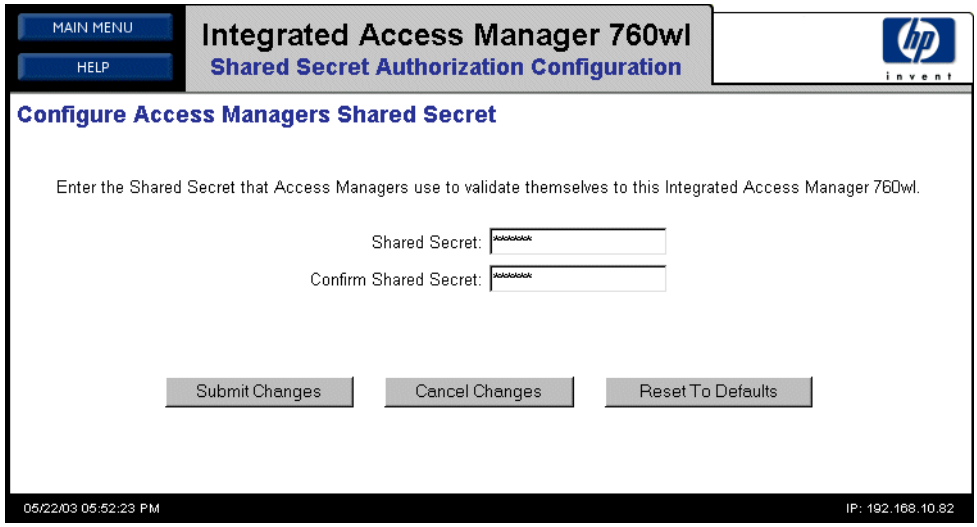

Figure 2-11. Configuring the Shared Secret for Access Controllers

Step 2. Type the shared secret.

Step 3. Type the shared secret again to confirm it.

Step 4. Click **Submit Changes** to set the secret.

Note: *When the shared secret is changed on the Access Control Server or Integrated Access Manager, the secret is propagated automatically to any connected Access Controllers managed by that Access Control Server.*

Setting the Shared Secret and IP Address on an Access Controller

In order to communicate with its Integrated Access Manager or Access Control Server, an Access Controller must know the IP address of that system. The Access Controllermust also know the shared secret in order to establish a trust relationship with the Integrated Access Manager or Access Control Server.

To set the Access Control Server IP address and shared secret on an Access Controller:

Step 1. Click **Access Control Server** from the Main Menu of the Access Controller. The Specify Access Control Server and Enter Shared Secret page appears, as shown in Figure 2-12.

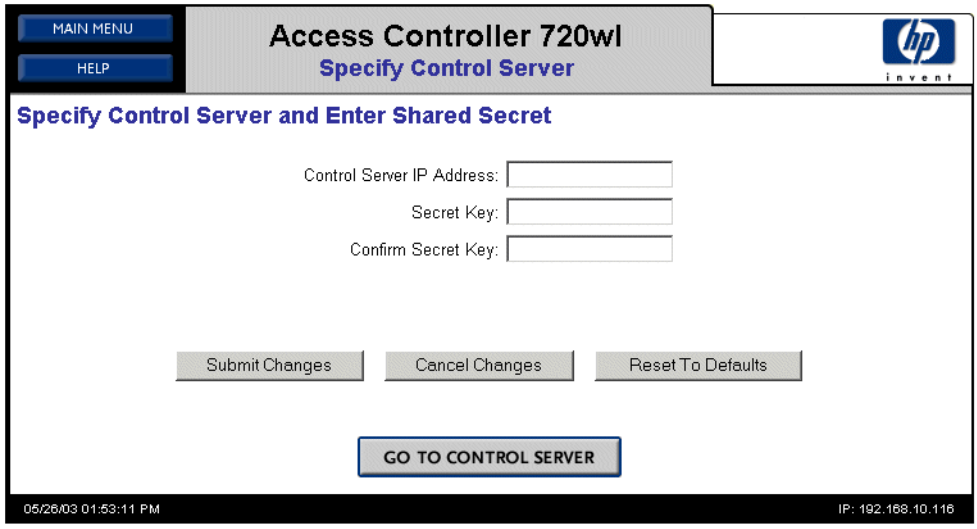

Figure 2-12. Specifying the Access Control Server IP address and secret

Step 2. Type the IP address of the Access Control Server or Integrated Access Manager in the **Access Control Server IP Address** field.

Step 3. Type the **Secret Key**.

Step 4. Retype the **Secret key** to confirm it.

Step 5. Click **Submit Changes**.

Once you have set up the Access Control Server (or Integrated Access Manager) IP address, a green **GO TO CONTROL SERVER** button appears beneath the three change buttons. This button takes you to the login page of the Administrative Interface of the Access Control Server.

Note: *Once you set the Access Control Server IP address and shared secret to enable access to and from the Access Control Server, the Access Control Server will keep this information updated—if the IP address or shared secret is changed on the Access Control Server, the changed information will be automatically propagated to the Access Controllers managed by that Access Control Server.*

HTTP Proxy Server Configuration

If your network makes use of a proxy server for HTTP traffic, you may want to ensure that HTTP traffic originating from wireless clients also goes through your proxy server. However, when mobile wireless clients connect to your network, especially if you allow Guest access, there is no guarantee that their browsers will be configured correctly for your proxy server. The Automatic HTTP Proxy feature of the 700wl Series system allows you to enforce the use of an internal HTTP proxy server (within your network) without requiring a specific

configuration on the client. Whether a client browser is configured with no proxy, or for any arbitrary proxy server, the 700wl Series system can intercept HTTP traffic and redirect it to the appropriate proxy server within your network.

The automatic Proxy feature is enabled and configured group-by-group from the Administrative Interface on an Integrated Access Manager or Access Control Server. This lets you specify an HTTP proxy only for selected groups, if appropriate. You also can configure a set of proxy filters to conditionally allow or deny specific connections. These settings are also done by groups, meaning you can specify different access for members of different groups.

There are three basic steps to enabling this functionality.

- Configuring the Proxy Server IP address so the Access Controller knows where to redirect HTTP requests. This is done through the HTTP Proxy Configuration page in the Administrative Interface for an Integrated Access Manager or Access Control Server.
- Configuring which TCP ports HTTP traffic is likely to appear on, and configuring a set of filters (Accept and Deny rules) that conditionally allow or deny specific connections for members of a group.
- Enabling the Automatic HTTP Proxy feature group-by-group.

Configuring HTTP Proxy settings for a group and enabling the feature for a group is done through the Rights Manager. See “Automatic HTTP Proxy Configuration” in Chapter 11 for details.

To configure the Proxy Server address, do the following:

Step 1. From the Main Menu, under the Configuration heading, click **HTTP Proxy**.

The HTTP Proxy Configuration page appears, as shown in Figure 2-13.

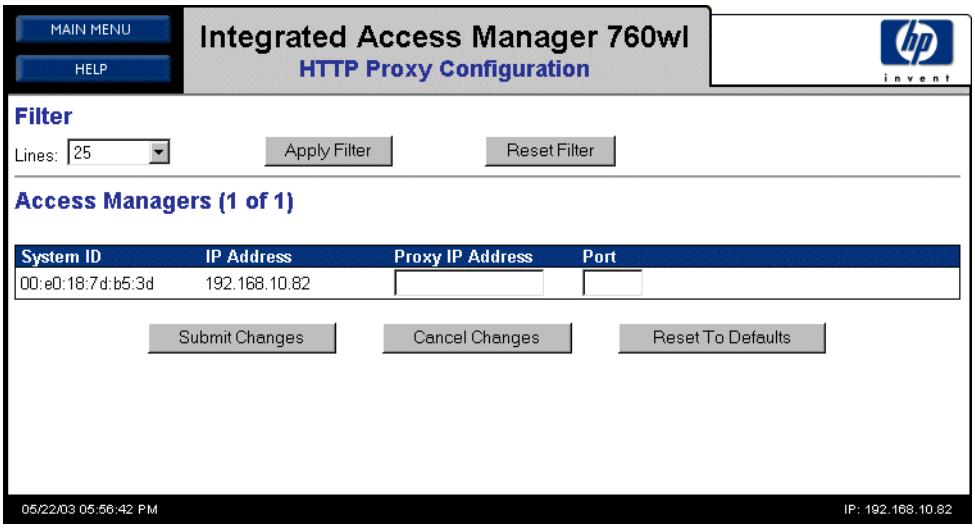

Figure 2-13. Proxy Server configuration by Access Controller

Step 2. In the **Proxy Server IP Address** field, type the IP address of the Proxy Server to which HTTP traffic should be redirected.

Step 3. In the **Proxy Server Port** field, type the TCP port number used for the proxy server.

Step 4. Click **Submit Changes** to have your configuration take effect.

Once this has been done, go to the Rights Manager to configure and enable the Automatic Proxy feature for individual groups.

Filtering the Display

If you have a large number of Access Controllers communicating with your Integrated Access Manager or Access Control Server, the Access Controller table may be very long. The Filter function at the top of this page lets you control how many lines should be displayed on a single page.

» In the Lines field, select from the drop-down list the number of lines that should be displayed on the page, then click **Apply Filter**.

You can choose 10, 25, 100, 1000, or an unlimited number of lines.

Configuring SNMP

The Simple Network Management Protocol (SNMP) is a standard for network management. SNMP enables network administrators to manage their networks.

The SNMP subsystem enables the Access Controller and Integrated Access Manager to be monitored via SNMP from a network management application such as HP OpenView or Aprisma SPECTRUM.

Note: *The 700wl Series system supports Management Information Base-2-compliant objects.*

To configure SNMP:

Step 1. Click **SNMP** from the Main Menu.

The SNMP Configuration page is displayed, as shown in Figure 2-14.

Note: *Figure 2-14 shows the page displayed for the Integrated Access Manager. The page displayed for the Access Controller is the same.*

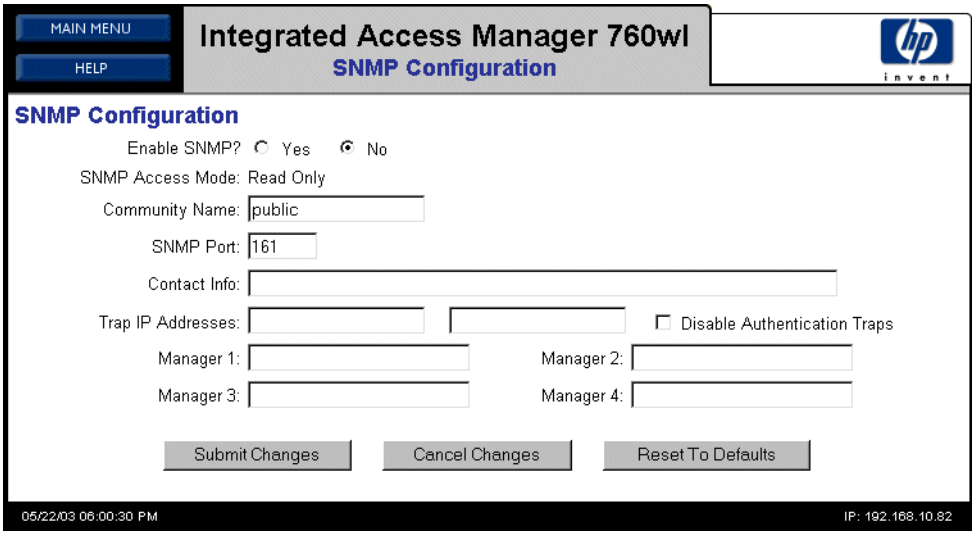

Figure 2-14. SNMP Configuration

Step 2. Determine whether you need SNMP to work with your overall network. SNMP is disabled by default. Click **Yes** to enable SNMP on your Integrated Access Manager or Access Controller.

Note: *Enabling SNMP allows Read-only access to the device.*

Step 3. Type your read-only **Community Name**, which is analogous to a password.

The default name is `public`; HP recommends that you change it to increase your security.

Step 4. Type the port number of your **SNMP Port**.

Port 161 is the default. If you change the port number, be careful that you do not use a port that is used by another application.

Step 5. Type your **Contact Info**. Typically, this is the Network Administrator's name, email address, or phone. This will be saved in the `sysContact` MIB object.

Step 6. In the **Trap IP Addresses** field, type the IP address of up to two systems that should receive traps from the 700wl Series system.

Note: *Include a trap IP address **only** if you have an SNMP trap receiver listening for this information.*

HP proprietary SNMP trap events include fan failure, fan operational, and out-of-range temperatures. General SNMP trap events include SNMP authentication failures, which are sent as trap information.

Step 7. Type up to four **Manager** IP addresses.

These are the addresses of SNMP management consoles that are authorized to request information from the Integrated Access Manager.

You can enter the Manager IP address in any of the following forms:

- An IP addresses, such as `192.168.1.1`
- An IP address with netmask, such as `192.168.1.0/24`
- A hostname such as `snmp.fiesta.com`
- A wildcard address, for example: `0.0.0.0/0`

Note: *To query the SNMP agent from an SNMP console, you **must** include at least one Manager IP address.*

Step 8. Click **Submit Changes** to save your settings.

Specifying Location Information

Specifying a name or description for the location of your HP devices is helpful in a wireless system for system debugging and management. The Integrated Access Manager location information is also saved in the sysLocation MIB object, and is accessible through SNMP. This is an optional function—providing location information is not required.

Location descriptions can be provided for an Integrated Access Manager or an Access Controller and each of their downlink ports.

To specify location descriptions:

Step 1. Click **Specify Location Information** from the Main Menu.

The Location Descriptions page appears. The example shown in Figure 2-15 shows the Location Descriptions page for an Integrated Access Manager 760wl with four ports installed. The display for an Access Controller is similar. The port shown as Slot 0 Port 1 is the port labeled *Reserved* next to the Uplink port. This port is reserved for future use as a management port, but can be used as an extra downlink port.

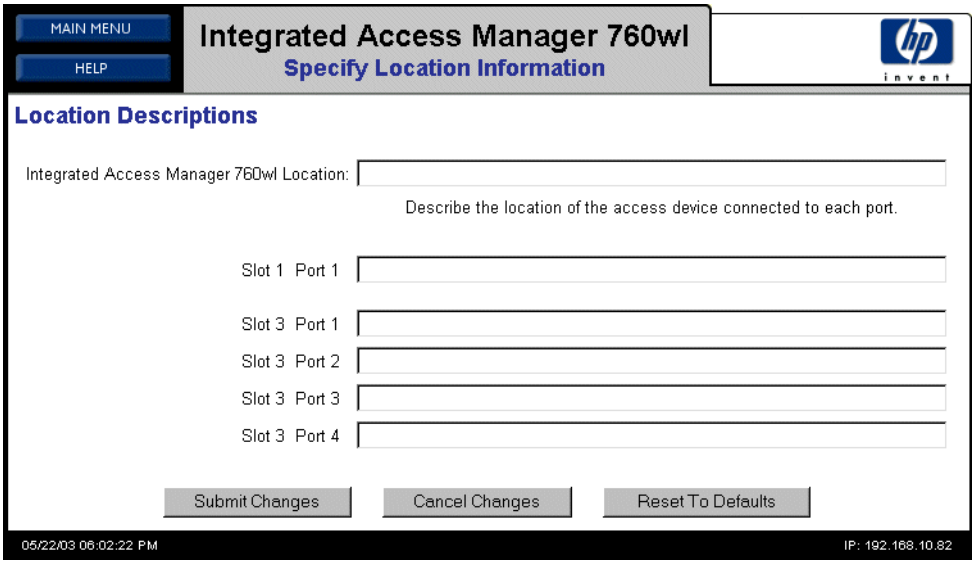

Figure 2-15. Location Information

Step 2. Type a location description for the **Location**, for example, “Network Closet 2, 4th floor, Physics Building”.

Step 3. Type a location description for each of the Ports, as shown in the example in Figure 2-15 (“Advanced Physics Lab,” “Conference Room 12” and so on).

Step 4. Click **Submit Changes** to save your choices.

Specifying Session Logging

Through session logging, the 700wl Series system creates logs of detailed session information for all sessions entering the network through an Integrated Access Manager or an Access Controller, and sends these to an external Syslog server. You can use these logs for accounting and troubleshooting.

Session logging is separate from the system Log File and the status information that you can see through the links under the View heading on the Main Menu. The system log file keeps log entries for events, such as errors, reboots, software upgrades, and so on. Session logging keeps information about client sessions such as the date and time of login/logout, number of packets sent, and other similar information.

The Rights Manager also creates logs of useful information, and these logs can also be sent to the remote Syslog server. The combination of session logging and Rights Manager log information can provide a very comprehensive picture of a 700wl Series system operation. Rights Manager logging can be configured from the Rights Manager (see “Setting Up Rights Manager Logging” on page 11-15).

Note: *You must configure session logging from an Integrated Access Manager or Access Control Server. You cannot configure session logging from an Access Controller.*

To specify session logging:

Step 1. Click **Specify Session Logging** from the Main Menu.

The Specify Session Logging page appears, as shown in Figure 2-16.

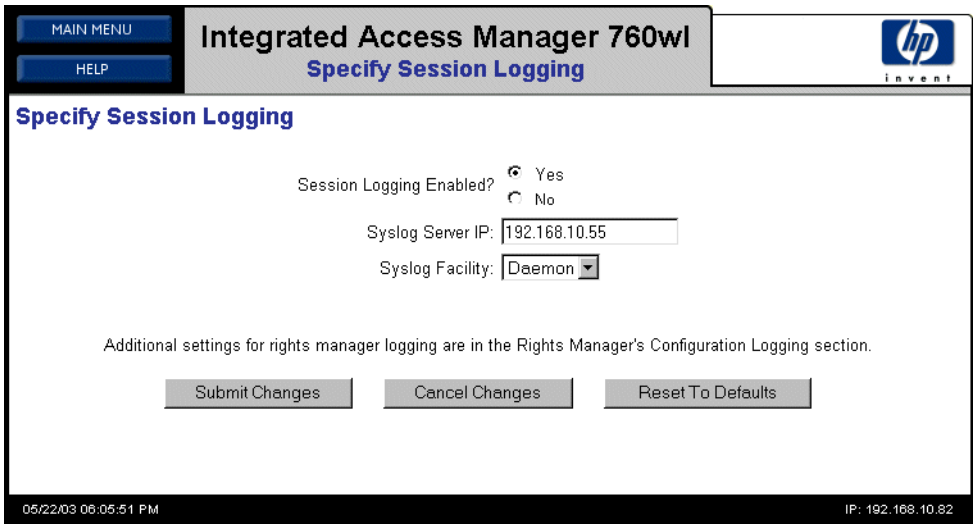

Figure 2-16. Specify Session Logging

Step 2. Click **Yes** to enable Session Logging.

Step 3. Type the IP address of your remote Syslog server in the **Syslog Server IP** field.

Step 4. Select a **Syslog Facility** from the drop-down list.

You can choose **Daemon**, **User**, or **Local 0 through 7**. Select a setting that interoperates appropriately with your enterprise Syslog server.

Step 5. Click **Submit Changes**.

The information logged to the Syslog file is described in Chapter 5, “Viewing System Status” in the section “Session Log File” on page 5-11.

Configuring the Time and Date

Accurate time and date reporting is necessary for logs and for troubleshooting. Accurate and synchronized time and dates across multiple systems is especially important. You use the Time and Date Configuration screen to set the system timezones and date.

To configure the time and date:

Step 1. Click **Time and Date** from the Main Menu.

The Time and Date Configuration page appears, as shown in Figure 2-17.

Step 2. From the drop-down list in the **Time Zone** field, select the time zone that is appropriate for your location.

Note: *Time zones are associated with major cities: for example, you would choose America/New York for Eastern Standard Time.*

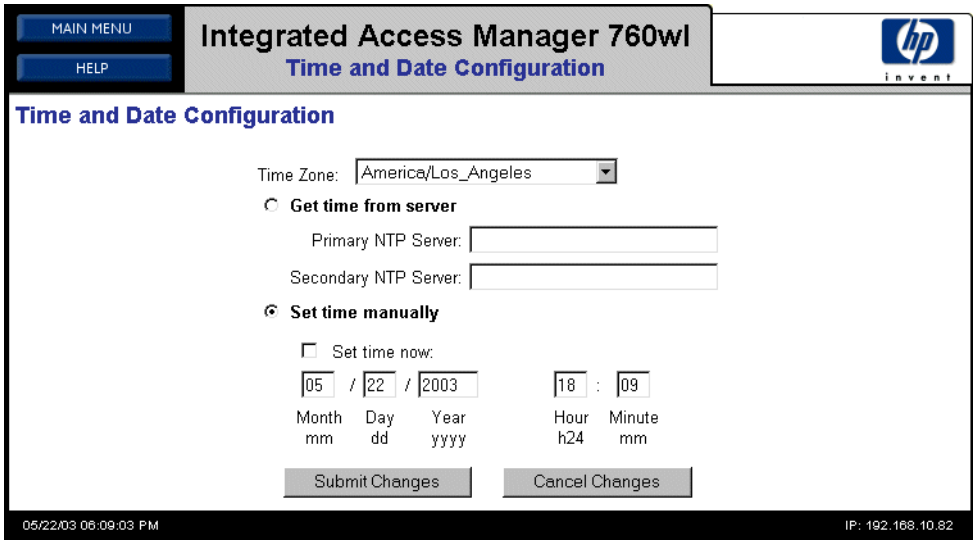

Figure 2-17. Configuring the Time and Date

You can either get the time from an NTP server or set it yourself.

Step 3. To get the time from an NTP server:

- **a.** Click **Get time from server**
- **b.** Type the hostname or IP address of the primary NTP server.
- **c.** Type the hostname or IP address of the secondary NTP server.

Step 4. To configure the time manually:

- **a.** Click **Set time manually.**
- **b.** Click **Set time now** to disconnect from the NTP server and set the date and time according to settings you entered in the following fields.
- **c.** Type the date and time in the fields provided. The hour must be in 24-hour format.

Step 5. Click **Submit Changes**.

Caution: *It is important that the system time be kept accurate, and the time should not be set backwards, either manually or by NTP, while the system is in operation. A backwards change in the time of day may cause certain internal time-outs to take longer than normal, and previously expired and logged off users may be made to appear active, until the system moves beyond the time these users logged off or had their rights expire. Therefore, if a backwards time change is necessary (for example, to return from Daylight Saving Time to Standard Time) it should be done during times when system usage is low to minimize any possible disruptions.*

Viewing Online Documentation and Help

To view online documentation and help:

Step 1. Click **Help** from the Main Menu.

The Help Menu appears, as shown in Figure 2-18 for the Integrated Access Manager.

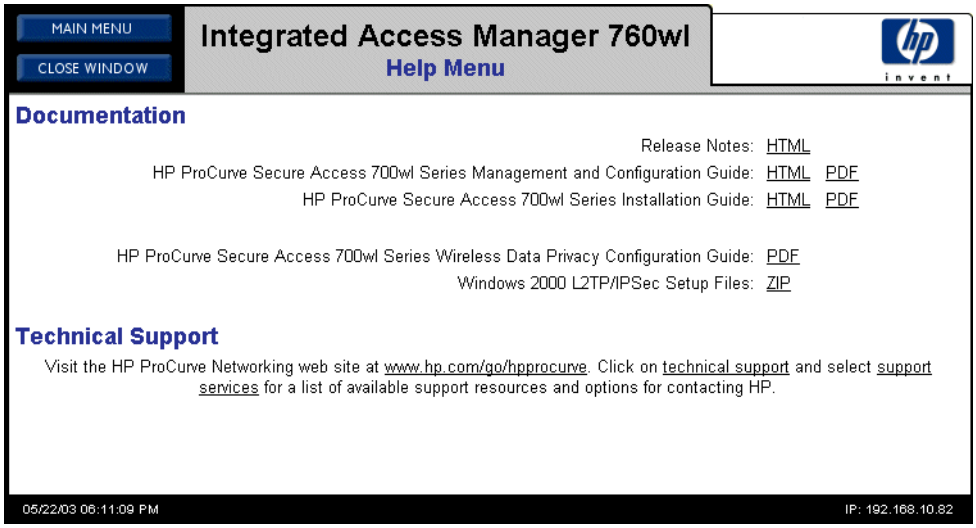

Figure 2-18. Integrated Access Manager Documentation and Release Notes

Step 2. Click the HTML or PDF link next to a document name to view that document. For documents in HTML format, hypertext links allow you to navigate easily from topic to topic. In PDF format, bookmarks and hypertext links are also provided for easy navigation.

Online help is also accessible from individual pages in the Administrative Interface. For example, if you click **Help** from the Time and Date page, the HTML version of the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* appears at the beginning of the section that contains the documentation for the Time and Date page.

Review the information in the Release Notes so that you are aware of recent changes that may not be included in the manuals. Information in release notes is the most up-to-date information and supersedes the user and installation manuals.

Note: *The Access Controller has no separate online help or documentation. If you click* **Help** *from the Administrator Interface of an Access Controller, you are presented with the Access Control Server login page, and then the Access Control Server Help page. If you are already logged in on the Access Control Server, clicking* **Help** *from the Access Controller takes you directly to the Access Control Server Help page.*

WIRELESS DATA PRIVACY 3

This chapter explains how to secure the airwaves between the client and the Access Controller 720wl or Integrated Access Manager 760wl. Wireless data privacy is an integrated feature of the HP ProCurve Secure Access 700wl Series that protects your information over the airwaves.

It includes the following topics:

Configuring Wireless Data Privacy 3-1

Configuring IPSec 3-4

Configuring PPTP and L2TP 3-11

Configuring SSH 3-12

Tunneling Configuration 3-13

Configuring Wireless Data Privacy

Wireless data privacy is an optional security feature of the HP ProCurve Secure Access 700wl Series that allows you to provide strong encryption of data between a client and the Access Controller. Wireless data privacy provides additional security for data sent over the airwaves, supplanting the relatively insecure Wired Equivalent Privacy (WEP) of a wireless network.

The HP system offers four choices for encrypting data between a client and the Access Controller: PPTP, L2TP / IPSec, *pure* IPSec, and SSH.

You must configure wireless data privacy from an Integrated Access Manager or Access Control Server. The Wireless Data Privacy Setup selections do not appear in the Administrative interface on an Access Controller.

IPSec

The IP Security protocol suite (IPSec) is an industry-standard method for encrypting networking communications that was designed specifically to work with IP networking. IPSec clients are available from a variety of vendors. Clients known to interoperate with the 700wl Series system IPSec implementation include ones from SafeNet, Netscreen, PGP, and Certicom / Movian.

The IPSec standard does not include a specification for user-level authentication. It does provide for machine-to-machine authentication using either certificate-based or shared

secret-based authentication. The 700wl Series system supports both types of IPSec authentication.

IPSec operates in two phases and uses encryption and a secure hash function for each phase. The first phase, Internet Key Exchange (IKE) sets up a session key that is used in the second phase to do the actual encryption. The second phase, Encapsulating Security Payload (ESP), does the actual data encryption. Both the IKE and ESP phases can use Data Encryption Standard (DES), Triple DES, Blowfish, or CAST encryption. The ESP phase can also use the Advanced Encryption Standard (AES) algorithm.

The secure hash used for data integrity in both the IKE and ESP phases can be either Secure Hash Algorithm 1 (SHA-1) or Message Digest 5 (MD5).

IPSec uses the Diffie-Hellman Public-Key-Interchange (PKI) to generate the per-session encryption key during the IKE phase. Supported versions of the Diffie-Hellman key exchange include Groups 1, 2, and 5.

In general, the client and the 700wl Series system negotiate the type of hash, encryption, and key-exchange algorithms. Configuration of IPSec on the Integrated Access Manager consists of selecting and setting up the IKE authentication method (shared secret or certificate) and noting which algorithms the HP system is prepared to negotiate. It is up to the client system to propose algorithms, and the HP server either agrees or not.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol defined by Microsoft for encrypting network data transfers. Its advantages include its wide availability as it comes pre-installed on all versions of the Windows operating system including Windows 9x, Windows ME, Windows NT, Windows 2000, Windows XP, and Windows CE.

PPTP can use a variety of user-level authentication algorithms, including Microsoft Challenge Handshake Authentication Protocol (MS-CHAP and MS-CHAP version 2). The 700wl Series system can use the PPTP user authentication for its own authentication. In this case, the 700wl Series system login page is not necessary. For encryption, it uses either 40-bit or 128-bit MPPE (Microsoft Point-to-Point Encryption), which employs the RC4 encryption algorithm.

L2TP/IPSec

Layer 2 Tunneling Protocol (L2TP) is also a Microsoft protocol. L2TP over IPSec (L2TP / IPSec) uses the standard IPSec (IP Security) protocol to encrypt network communications and uses L2TP, an updated and more secure version of PPTP, for IP address management and user-level authentication. L2TP clients are pre-installed on Windows 2000 and Windows XP operating systems.

L2TP can use the same user-level authentication algorithms as PPTP—MS-CHAP and MS-CHAPv2. As with PPTP, the 700wl Series system can use the L2TP user authentication as its own authentication. L2TP does not itself provide for any data encryption; instead, it uses IPSec to encrypt data.

Both PPTP and L2TP were originally designed as a means for remote users, typically the traveling business person, to access their home network while on the road. As such, both protocols include IP address assignment features that are not really necessary in a wireless

environment. Both protocols also include facilities for user-level authentication and for non-IP protocols.

SSH

Secure Shell (SSH) is an industry standard Layer 4 security protocol that runs over TCP. For client systems that cannot use PPTP, L2TP, or IPSec, such as Macintosh OS X or some handheld devices, SSH's port forwarding capability provides an alternative. As with PPTP or L2TP, the Integrated Access Manager or Access Controller can use the SSH user authentication as its own authentication.

General Considerations

Selection of a particular protocol involves several factors:

- Necessity
- Performance
- Security
- Availability

Necessity

You must first determine whether you require Wireless Data Privacy as it imposes a fairly heavy administrative burden and it slows the throughput of data between a client and an Access Controller.

Wireless Data Privacy encrypts user data that passes between a client and the network. Only those networks subject to snooping by unauthorized individuals need encryption. Even those networks might be adequately protected by WEP encryption.

If your network is susceptible to unauthorized interception of data and if WEP is inadequate to protect this data, you should consider using Wireless Data Privacy.

Performance and Security

Encryption and decryption of data imposes a computational load on both a client computer system and the Access Controller. Encrypting and decrypting data can slow data throughput by a factor of five or more. Although a more secure algorithm is generally thought to be slower, that is not necessarily the case. Table 3-1 shows a number of encryption algorithms and their relative performance.

Table 3-1. Algorithms and their Relative Performance

Encryption algorithm	Strength	Encryption speed
128-bit RC4	good	good
56-bit DES	fair	fair
168-bit (Triple) DES	excellent	slow

Table 3-1. Algorithms and their Relative Performance

Encryption algorithm	Strength	Encryption speed
Blowfish	good	good
CAST	good	good

Availability

The availability of a client is an important part of the selection of an protocol to use for Wireless Data Privacy. Table 3-2 shows availability of PPTP, L2TP / IPSec, *pure* IPSec and SSH clients known to interoperate with the 700wl Series system Wireless Data Privacy:

Table 3-2. Protocol Support on Client Platforms

Algorithm	Platform	Client Support
PPTP	Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP, Windows CE, and other vendors	Built-in
	MAC OS 9x	LAN TunnelBuilder
L2TP/IPSec	Windows 2000, Windows XP	Built-in
IPSec	Windows	SafeNet SoftRemote SSH Sentinel PGPnet for Windows
	MAC OS 9x	PGPnet for MAC OS 9
SSH	Microsoft Windows	PuTTY enTunnel (SSH port forwarding client)

The configuration of many of these clients is discussed in the *HP ProCurve Secure Access 700wl Series Wireless Data Privacy Configuration Guide* available from the Help page (accessed from the Main Menu).

Configuring IPSec

The configuration of IPSec requires four steps:

- Enabling or disabling IPSec on the Integrated Access Manager or Access Control Server.
- Setting the IKE authentication method (specifying the shared secret or obtaining and loading PKI certificates)
- Specifying the acceptable encryption and secure hash algorithms.
- Specifying how client IP address assignment is done—via DHCP or from a specified range of addresses. This specification is done once whether you are using IPSec, PPTP or L2TP.

Once IPSec is configured, you can specify whether IPSec is allowed or required on a per-location basis in the Rights Manager.

An IPSec client negotiates with the IPSec server to set the various options for encryption and integrity assurance. The IPSec configuration page allows the network administrator to specify which IKE and ESP encryption and integrity algorithms that the Integrated Access Manager and Access Controller will negotiate with the client.

To configure IPSec security:

Step 1. From the Main Menu under Airwave Security Setup, click **IPSec**.

The IPsec Configuration page appears, as shown in Figure 3-1.

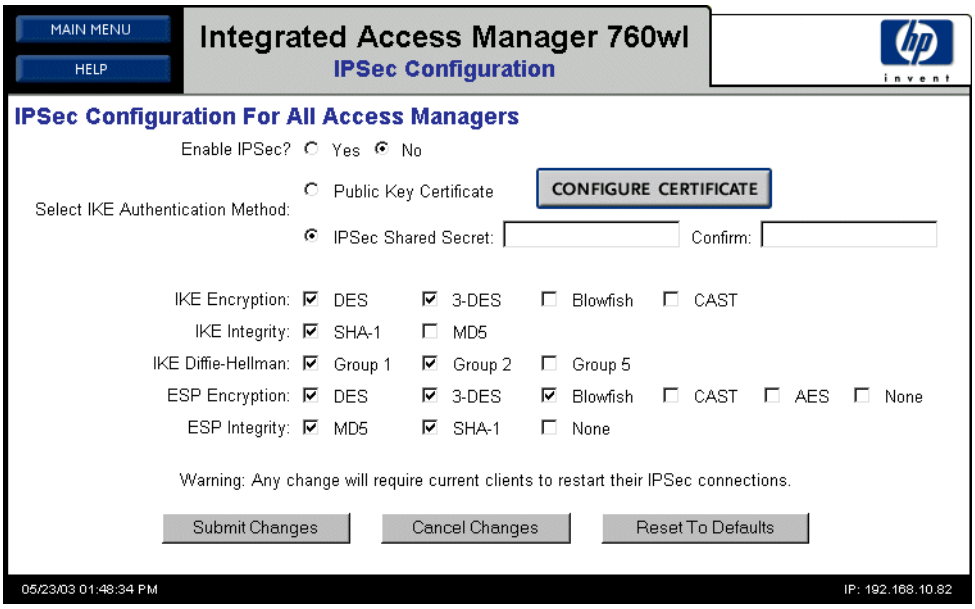

Figure 3-1. IPSec Configuration

Step 2. Click the **Yes** button to enable IPSec.

Step 3. Select the IKE authentication method you plan to use:

a. To use certificate-based authentication, click **Public Key Certificate**.

Then, click **Configure Certificate** to generate a certificate request and install the resulting certificates. See “Configuring PKI for IPSec” for details on setting up these certificates.

b. To use shared secret-based authentication, click **IPSec shared secret**, and enter your shared secret in the two fields.

You are defining a shared secret to give to your IPSec users so that their IPSec client software can prove they are authorized to use an IPSec connection.

Caution: *Using a shared secret is inherently insecure, because the secret must be known by every IPSec client, and therefore is not recommended. It is provided as a convenience for sites who cannot or choose not to use certificate-based authentication.*

Step 4. Click to select the appropriate algorithms for **IKE Encryption**. The default is DES and 3-DES.

Step 5. Click to select the algorithm to use for **IKE integrity.** The default is SHA-1.

Step 6. Click to select the appropriate **IKE Diffie-Hellman** settings. Default is Group-1 and Group-2.

Step 7. Click to select the appropriate algorithms for **ESP Encryption**. You can select multiple algorithms, or **None**. The default is DES, 3-DES, and Blowfish.

Step 8. Click the appropriate setting for **ESP Integrity.** You can select either, both, or **None**. The default is SHA-1 and MD5.

Step 9. Click **Submit Changes** to save your settings.

Note: *You must also set up how IP address assignment is to be handled. See "Tunneling Configuration" on page 3-13 for instructions on how to do this.*

You must also configure your locations through the Rights Manager to specify whether IPSec is allowed or required. See "Wireless Data Privacy Logon (PPTP/L2TP Clients)" in Chapter 9 for detailed instructions.

Configuring PKI for IPSec

To use certificated-based IKE authentication for IPSec, you must request and install a signed local certificate and a certificate from the Certificate Authority (CA) that signed the certificate. Once you have installed the certificates, you must back up your Integrated Access Manager or Access Control Server configuration to save the certificates and the private key that is provided with the certificates.

To generate and store PKI certificates, do the following:

Step 1. From the IPSec Configuration page, click **Configure Certificate**.

The PKI Configuration page appears, as shown in Figure 3-2.

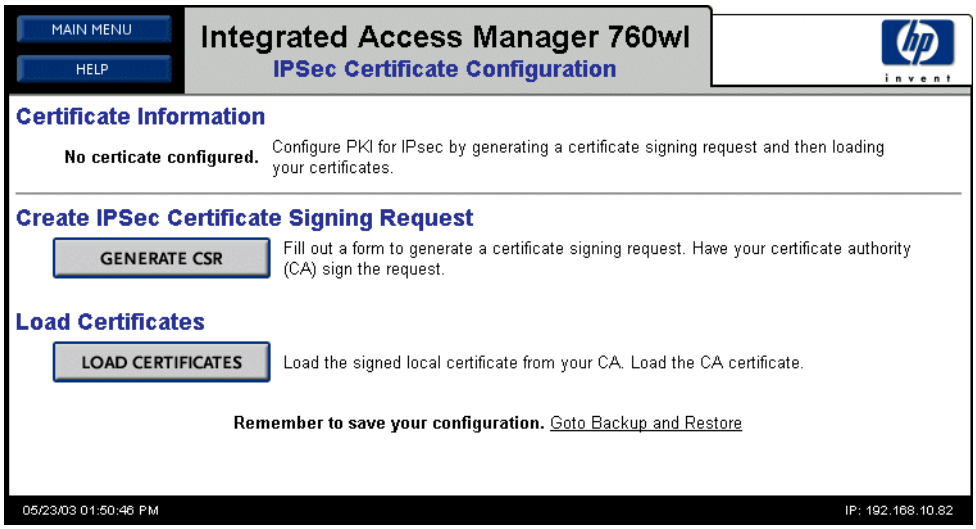

Figure 3-2. The PKI configuration page

Step 2. Click **Generate CSR** to display the certificate request form.

The Generate Certificate Request page appears (see Figure 3-3).

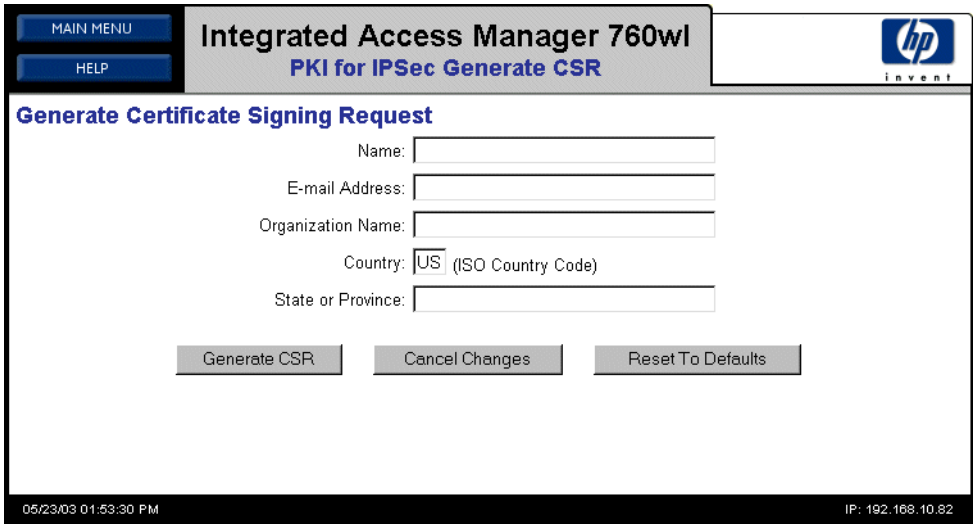

Figure 3-3. Certificate Request Generation form

Step 3. Fill in the information in this form:

a. Type the name in which the certificate should be granted. This can be an individual name or a title such as “Wireless Admin.”

b. Type the email address for the certificate contact.

c. Type the organization name. This is the name that will be published on the certificate.

d. Type your two-character ISO country code (US for the United States, UK for the United Kingdom, and so on). You can access the list of country codes at the

following URL:
`http://ftp.ics.uci.edu/pub/websoft/wwwstat/country-codes.txt`

e. Type your state or province. This is also typically a two-character abbreviation.

Step 4. Click **Generate Certificate Request** to generate a certificate request.

This produces a PKCS#10 certificate request that you can paste into a CA's certificate request form. Figure 3-4 is an example of a generated request.

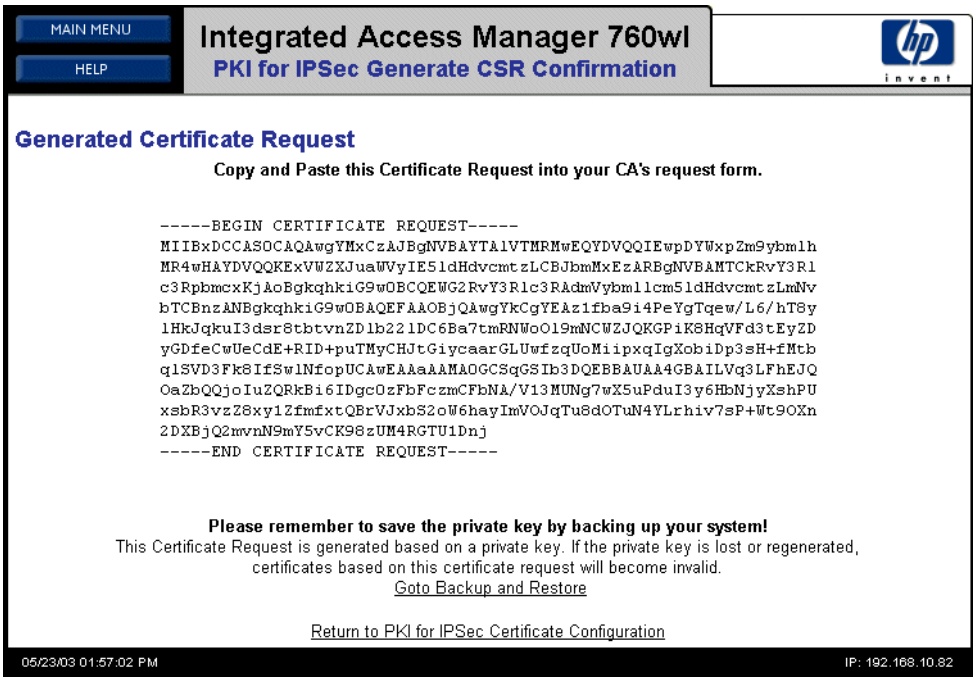

Figure 3-4. Generated certificate request

Step 5. Connect to your Certificate Authority website, and start the certificate request process.

Because you have generated a PKCS#10 certificate request, you should go to the Server Certificate Enrollment page, where you can paste your certificate request. In a Netscape Certificate Management System, this is the SSL Server page.

Caution: *You must generate a PKCS#10 certificate request through the Integrated Access Manager or Access Control Server administrative interface, and connect to the CA website system where you are running the administrative interface. You cannot request a certificate through the CA's manual request interface. Certificates you receive through that process will not work with the HP system.*

Step 6. Copy and paste the generated PKCS#10 certificate request, including the lines `----BEGIN CERTIFICATE REQUEST----` and `----END CERTIFICATE REQUEST----` into the appropriate field in the request form.

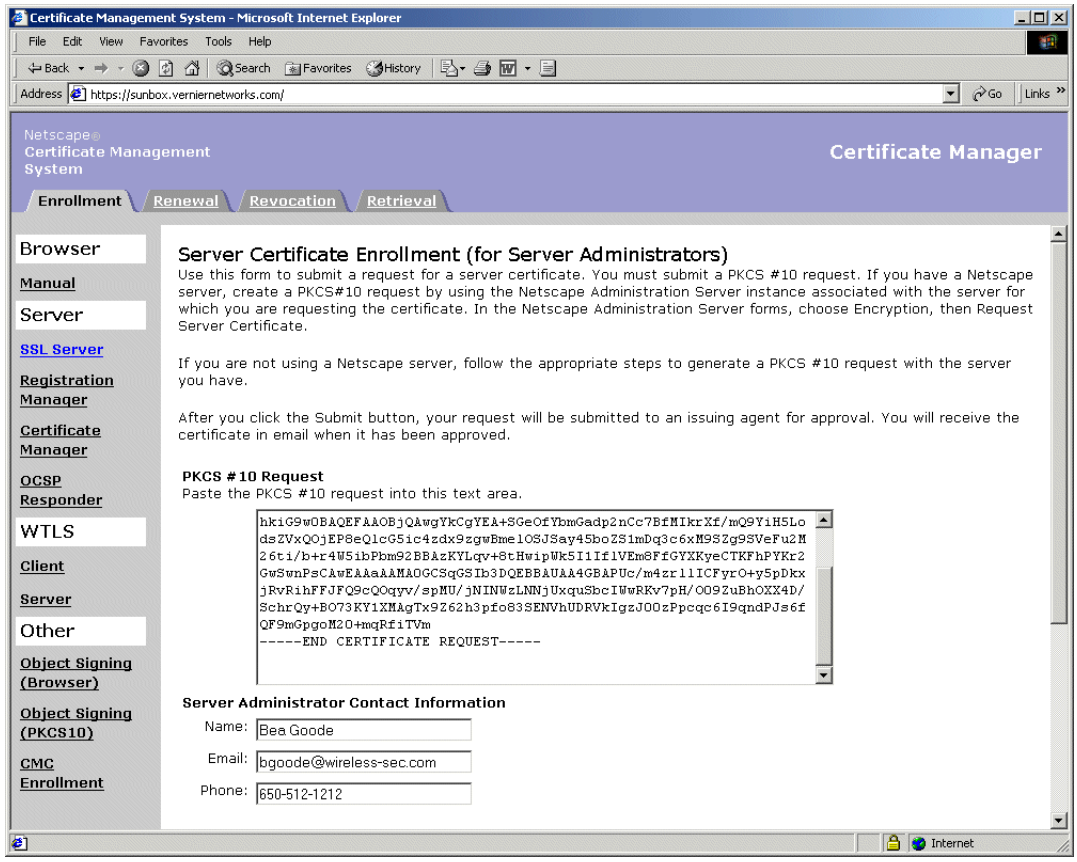

Figure 3-5. Example Server Certificate Enrollment page

Step 7. You may be asked to fill in additional information, such as your contact information. In the example shown in Figure 3-5, the contact information does not need to match the name and email you provided in the certificate request.

Step 8. When you have filled in any required information, submit the request.

You will probably receive an acknowledgment of your request, possibly with a request ID or other confirmation information.

Step 9. After the CA approves your request, you should then be able to retrieve two certificates -- your local signed certificate and the CA's certificate.

Step 10. From the Generated Certificate Request page, click the **Return to PKI for IPSec Configuration** link to return to the PKI Configuration page.

Step 11. On your CA's web site, go to the location where you can retrieve your certificates. You may need to enter the request ID or confirmation information you received when you submitted your certificate request.

When your certificate is displayed, find the portions that you can copy and paste into the HP system.

The example in Figure 3-6 shows the portion of the certificate where the information you need to copy is located. Note that it is in the same format as the certificate

request you generated. In this example, the local certificate information is in the first block, and the CA certificate is in the second block.

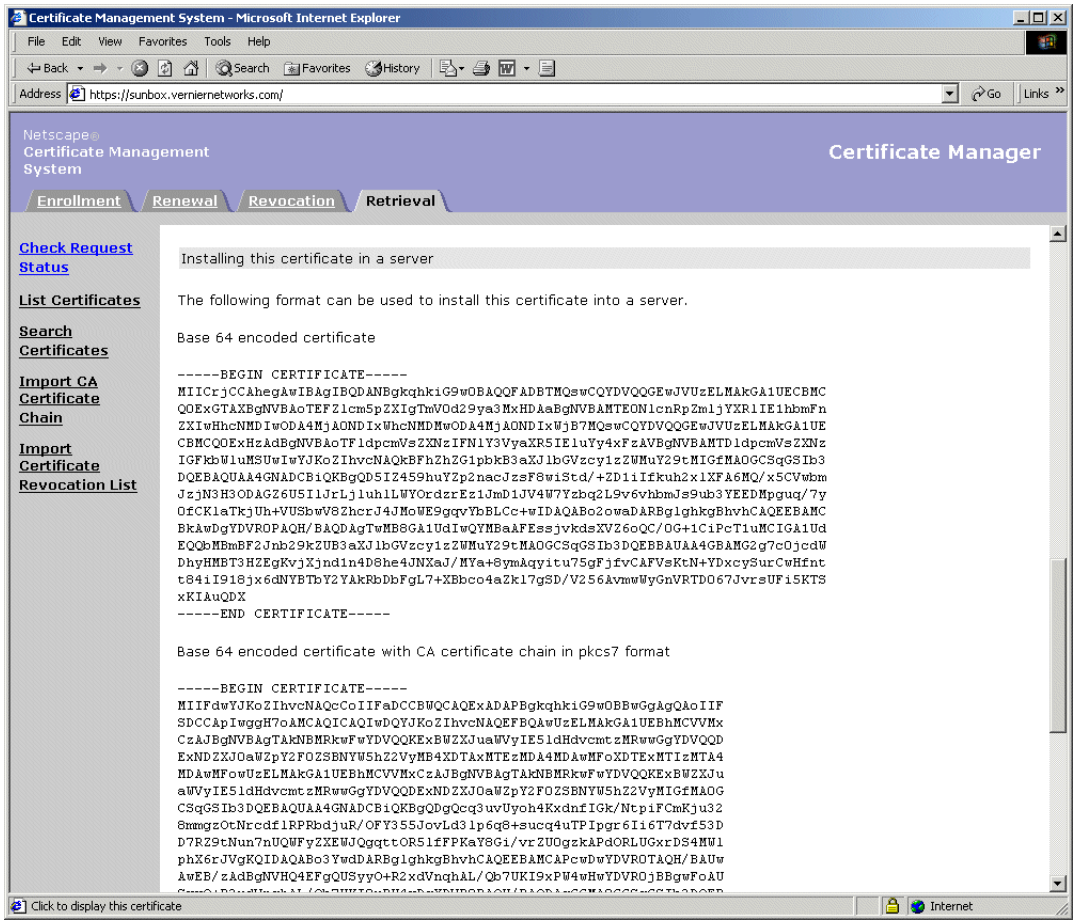

Figure 3-6. Example certificate information retrieved on CA web site

Step 12. From the PKI Configuration page, click **Load Certificates** to go to the Load Certificates page.

Caution: *Do not use the certificate import function, if there is one, from the CA's web page. It will not install the certificate on the HP system. You must paste the certificate information into the fields provided in the Load Certificates page in the HP administrative interface.*

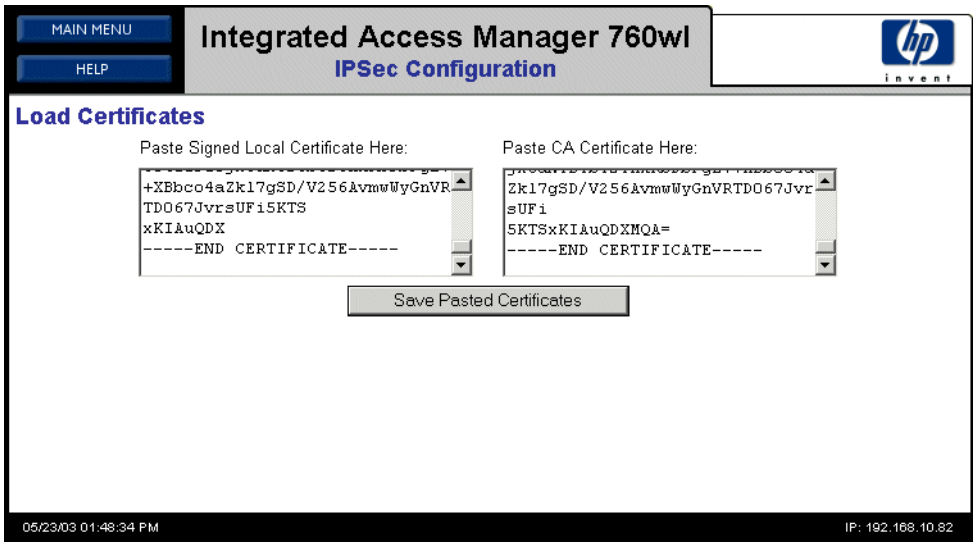

Figure 3-7. Loading the signed certificates

Step 13. Copy and paste the two certificates from your CA's web site into the two fields provided, and click **Save Pasted Certificates**.

Be sure to include the `---BEGIN CERTIFICATE---` and `---END CERTIFICATE--` lines.

A confirmation page appears confirming that your configuration has been updated.

Step 14. Immediately create and save a backup of your system. This saves both the private key and the saved certificates. You can go to the Backup and Restore page directly from the Confirmation page.

Caution: *Be sure to back up your system immediately. This is the only way to ensure that the certificates and keys can be restored if your system becomes corrupted. If the private key is lost, certificates based on that key will become invalid.*

Configuring PPTP and L2TP

Configuration of PPTP and L2TP is done through the Administrative Interface on an Integrated Access Manager or Access Control Server. There are two steps to enabling the use of PPTP and L2TP:

- Configure the Access Controllers to set up how address assignment is done for VPN tunneling—via DHCP or from a specified range of addresses. This specification is done once whether you are using PPTP or L2TP or pure IPSec.
- Configure the Access Control Server or Integrated Access Manager to enable PPTP and / or L2TP.

Once PPTP / L2TP is configured, you can specify whether PPTP and L2TP is allowed or required, and what authentication mechanism should be used, on a per-location basis through the Rights Manager.

To configure PPTP and L2TP:

Step 1. Click **PPTP and L2TP** under the Wireless Data Privacy heading on the Main Menu for an Integrated Access Manager or Access Control Server.

The PPTP and L2TP Configuration appears, as shown in Figure 3-8.

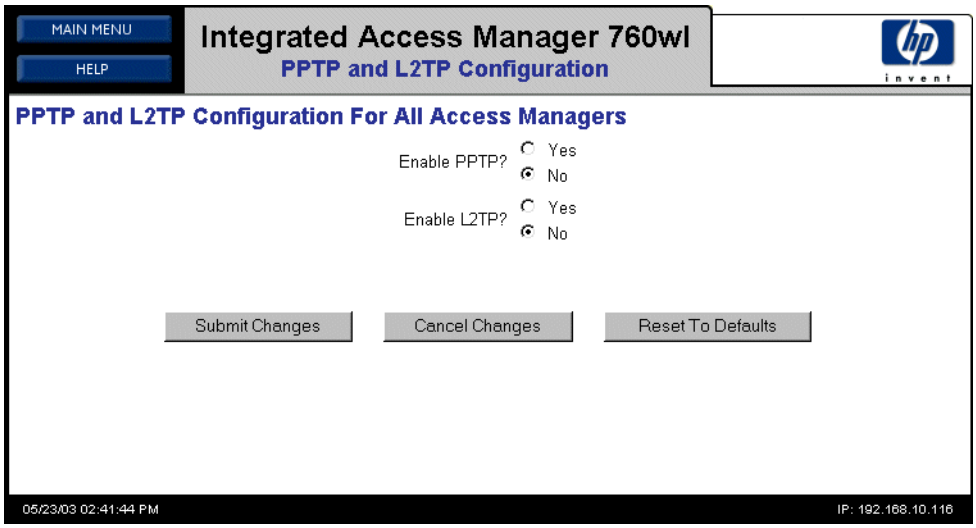

Figure 3-8. PPTP and L2TP

Step 2. Click **Yes** for **Enable PPTP**, if appropriate.

Step 3. Click **Yes** for **Enable L2TP**, if appropriate.

Step 4. Click **Submit Changes**.

Note: *To complete the PPTP or L2TP configuration, you must also set up how IP address assignment is to be handled. See "Tunneling Configuration" on page 3-13 for instructions on how to do this.*

You must also configure your locations through the Rights Manager to specify whether L2TP/PPTP is allowed or required, and how authentication should be done. See "Wireless Data Privacy Logon (PPTP/L2TP Clients)" in Chapter 9 for detailed instructions.

Configuring SSH

Enabling SSH as an wireless data privacy method enables an encrypted and authenticated channel for client systems that cannot use PPTP, L2TP, or IPSec. To enable SSH, do the following:

Step 1. From the Main Menu, under Wireless Data Privacy Setup, click **SSH**.

Step 2. Click **Yes** to enable SSH.

Step 3. Click **Submit Changes**.

This sets up the Integrated Access Manager or Access Controller to act as an SSH server, allowing users to connect to the HP system using an SSH client.

Tunneling Configuration

If you plan to use IPSec or PPTP/L2TP for wireless data privacy, you must configure the method by which your Access Controllers will assign IP addresses to the client.

Since PPTP and L2TP were originally designed as remote access protocols, used by traveling clients to access their home network, the PPTP and L2TP protocol assigns an IP address to the client computer. But in an Integrated Access Manager environment, a client usually obtains an IP address before enabling PPTP and L2TP encryption. This results in two IP addresses: an initial one that describes the PPTP or L2TP tunnel, and one that describes the actual IP address used by the client (the inner tunnel).

The Access Controller can be configured to assign this inner-tunnel address in one of two ways: it can either assign an address from a range of addresses pre-specified by the network administrator, or it can request an external DHCP server to assign an address.

The default is to have addresses assigned by a DHCP server.

Note: *The same tunnelling address assignment method is used by both PPTP/L2TP and IPSEC, if you have enabled both protocols.*

Step 1. From the Main Menu of the Administrative Interface for an Integrated Access Manager or Access Control Server, under Wireless Data Privacy, click **Tunneling**.

The Tunneling Configuration page appears (Figure 3-9).

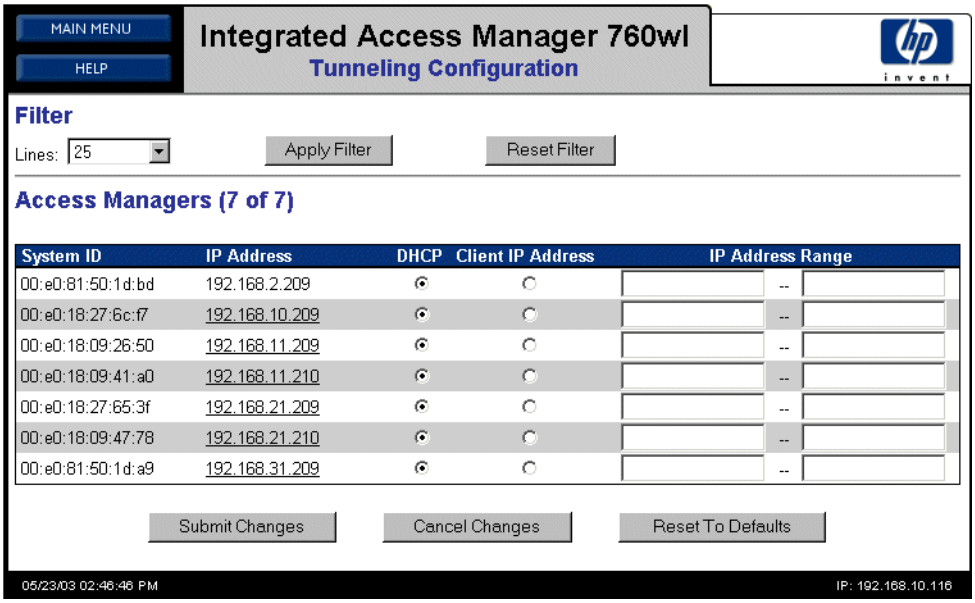

Figure 3-9. Tunneling Configuration

The Tunneling Configuration page shows all the Access Controllers connected to your Integrated Access Manager or Access Control Server. You must configure the inner-tunnel IP address assignment method individually for each Access Controller.

Step 2. Select the method you want to use to assign inner-tunnel IP addresses:

- To assign the address via an external DHCP server, click **DHCP**.
- To have the Access Controller assign the address from a range of addresses you provide, click **Client IP Address** and type the beginning and ending addresses of the range you want to use into the fields provided.

Step 3. When you have configured all your Access Controllers, click **Submit Changes**.

- To cancel your changes before you submit, click **Cancel Changes**.
- To restore the default settings (assignment via DHCP) for all Access Controllers, click **Reset to Defaults**.

Filtering the Display

If you have a large number of Access Controllers communicating with your Integrated Access Manager or Access Control Server, the Access Controller table may be very long. The Filter function at the top of this page lets you control how many lines should be displayed on a single page.

» In the Lines field, select from the drop-down list the number of lines that should be displayed on the page, then click **Apply Filter**.

You can choose 10, 25, 100, 1000, or an unlimited number of lines.

CONTROLLING THE SYSTEM FUNCTIONS 4

This chapter describes how to create, store, and restore a back up file, update system software, and shut down an HP ProCurve Integrated Access Manager 760wl, Access Control Server 740wl, or Access Controller 720wl. It also describes how to reset the 700wl Series system to its factory defaults.

It includes the following sections:

Creating and Storing a Backup Image 4-1

Restoring a Backed-Up Image 4-4

Distributing Logons to Access Controllers 4-6

Updating the System Software 4-6

Rebooting, Shutting Down, or Resetting the System 4-10

Creating and Storing a Backup Image

You should create backup files of your HP ProCurve Secure Access 700wl Series system often to ensure a relatively painless recovery from any data loss. You should *always* create a backup prior to upgrading your software, as described in "Updating the System Software", or if you are restoring to factory defaults, as described in "Rebooting, Shutting Down, or Resetting the System".

There is almost always enough configuration data in an Integrated Access Manager to make manual re-entry of data unpleasant.

Note: *Often multiple Access Controllers contain nearly identical configurations, and the amount of data kept in each Access Controller is small. You might consider manually re-entering an Access Controller's data, as necessary, rather than creating a large backup file.*

HP recommends that you create data backups on a regular basis. If you make significant changes to the Rights Manager configuration, back up these changes.

Creating a Backup Image

To create a backup image of your software and settings:

Step 1. Click **Backup and Restore** from the Main Menu.

The Backup and Restore page appears, as shown in Figure 4-1.

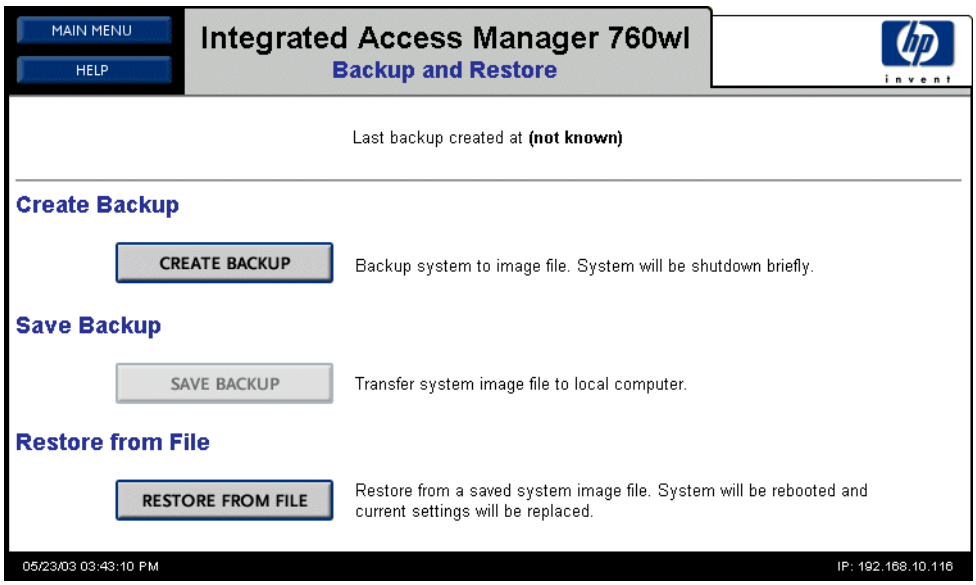

Figure 4-1. Backup and Restore

Note: *If you have not yet created a backup file, the* **Save Backup** *button is not available (dimmed).*

Step 2. Click **Create Backup**.

The Confirm Create Backup page appears, as shown in Figure 4-2.

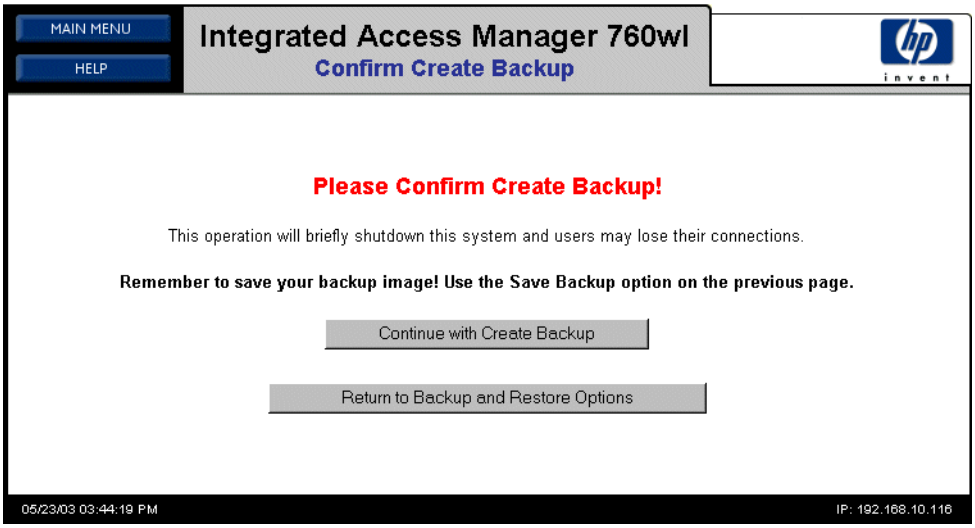

Figure 4-2. Confirm Create Backup page

Step 3. Click **Continue with Create Backup**.

The Started backup to image file page appears, as shown in Figure 4-3.

The new backup image will replace any previous backup image on your system.

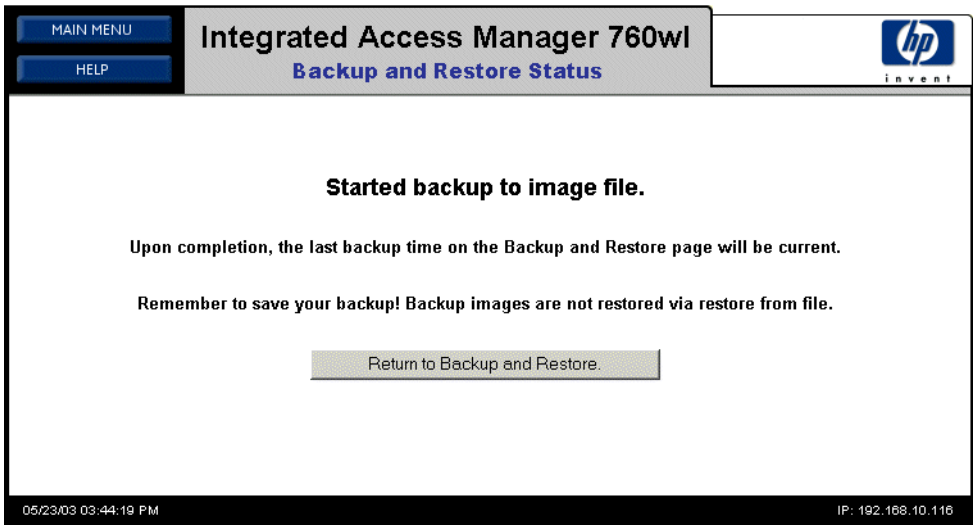

Figure 4-3. Backup Image started

Note: *No notification is given when the backup is complete. Depending on the amount of data in your system, it could take as long a 90 seconds. When you return to the Backup and Restore page, the "Last backup created" should indicate the just completed backup.*

Step 4. Click **Return to Backup and Restore Options** to return to the Backup and Restore page and save the new backup file.

It is very important that you save your back-up image to a local computer. If your 700wl Series system configuration becomes corrupted, you can restore your configuration from a backup image that is stored on another system.

Warning: *You cannot restore a backed-up image directly from an Integrated Access Manager or Access Controller. You can only restore an image from a file.*

Saving the Backup

If a backup has been successfully created, the **Save Backup** button, which is dimmed in Figure 4-1, will be available.

To save the back up image to your local computer do the following:

Step 1. Click **Save Backup** from the Backup and Restore page.

If you are using the Internet Explorer browser, the following File Download dialog box appears (Figure 4-4). Other browsers display similar windows.

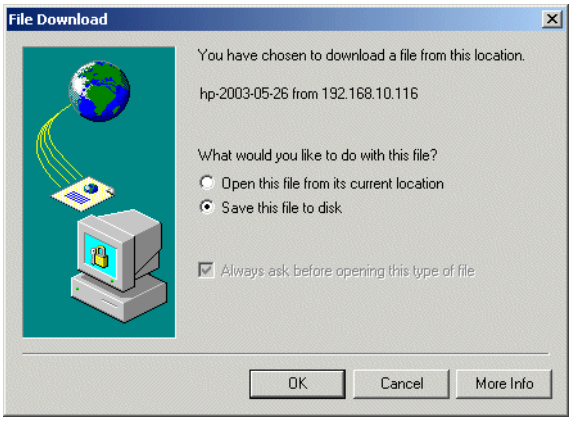

Figure 4-4. Download Backup window

Step 2. Make sure the **Save this file to disk** option is selected, and click **OK.**

The Save As dialog box appears, as shown in Figure 4-5.

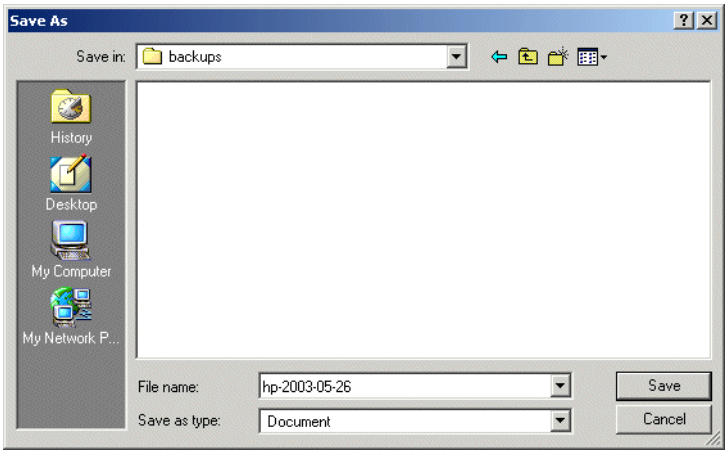

Figure 4-5. Save As window on your local computer

By default, the backup image file is named hp concatenated with the date (`-YYYY-MM-DD`). You can use this default or rename it. Choose the folder in which you want to store the backup and click **Save**.

Restoring a Backed-Up Image

Note: *Restoring an image will automatically reboot the system when the file restore is complete. If you restore an Access Control Server or Integrated Access Manager, all active clients will need to reauthenticate.*

To restore a previously backed-up image:

Step 1. From the Main Menu, click **Backup and Restore**.

Step 2. Click **Restore From File**.

The Confirm Restore from File page appears, as shown in Figure 4-6.

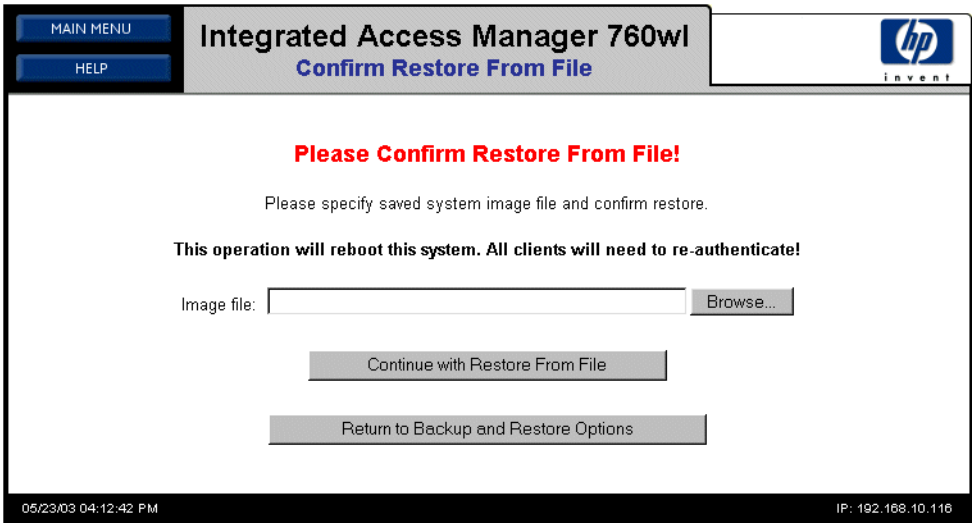

Figure 4-6. Confirm Restore From File page

Use the **Browse** feature to locate the backed-up image you want to restore or type the backup image file name in the **Image file** text box.

Step 3. Click **Continue to Restore from File.**

When the file is completely restored, the Backup and Restore Status page appears, as shown in Figure 4-7.

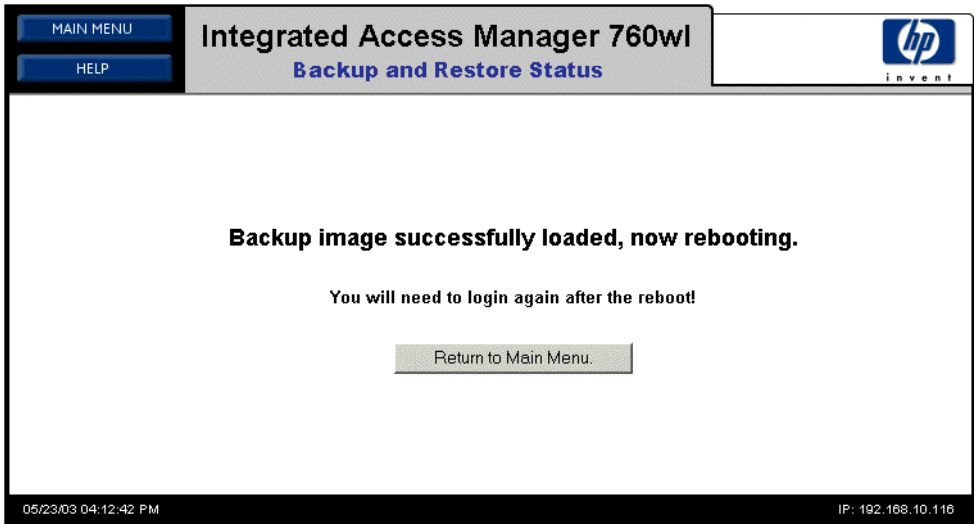

Figure 4-7. Backup and Restore Status page

Step 4. Click **Return to Main Menu**.

After the system reboots, you are presented with the Administration login page for the restored image.

Depending on the amount of data in the save image, the system can take as long as 90 seconds to reboot.

Note: *If your system settings have become corrupted (for example, due to a power failure while restoring from a backup) you can reset your system to the factory defaults and reboot to restore the initial system settings. However, resetting to defaults will require you to completely reconfigure your system. You can then restore your configured settings from a back-up image that was saved prior to the system reset.*

Transferring a Backup to a Different System

If you create and save a backup on one system, and then restore it to a different system, the restore will reconfigure the new system to match the original (backed-up) system's configuration with the following exception:

- The uplink port will *not* be changed on the new (restored) system, but will remain as configured. This is to avoid accidently changing an uplink port to a downlink port.

  For example, if the backed-up system used a option card gigabit port as the uplink, and the new system uses the default uplink, after a restore the new system will still be configured to use the default uplink. If you want to reconfigure the restored system to use a different uplink port, you must use the "set uplink" command through the CLI.

Distributing Logons to Access Controllers

The 700wl Series system by default distributes logon processing among the Access Controllers associated with the Access Control Server. By distributing the load of listening for logon traffic and serving up logon pages, the load on the Access Control Server is reduced.

In early releases of the 700wl Series system software, all logon processing was handled centrally by the Access Control Server. The Distribute Logon feature is provided to allow systems running previous versions of the software to change to Distributed Logon mode. Support for Centralized Logon mode is being discontinued.

Note: *For HP ProCurve Secure Access 700wl Series systems, since distributed logon is the default, this feature should not be used.*

Updating the System Software

Upgrading the 700wl Series system software is a two-step process:

- First, a new software image must be downloaded from a remote site, or from a distribution file. This new image becomes the ***Alternate Version***.
- Then, the system must be rebooted using the Alternate Version as the system image. This automatically makes the older image the new alternate version. This allows you to revert to the older image if the new image is unsatisfactory for any reason.

  The update preserves all your configuration settings.

Caution: *Before updating system software, you are strongly advised to create a backup of your current system software. See "Creating and Storing a Backup Image" for details.*

Note: *In order to update flash-based Access Controllers, the update process will shut down certain services to provide space for the update processing. The following subsystems will be shut down if they are running: SNMP, NTP, IPSec, PPTP, L2TP, and SSH. As a result, any clients connected through the Access Controller and using the wireless data privacy protocols will temporarily lose their connections. It is recommended that you update your flash-based Access Controllers during times when system usage is low.*

» To update the system software, click **Update Software** from the Main Menu.

The Update Software screen appears, as shown in Figure 4-8.

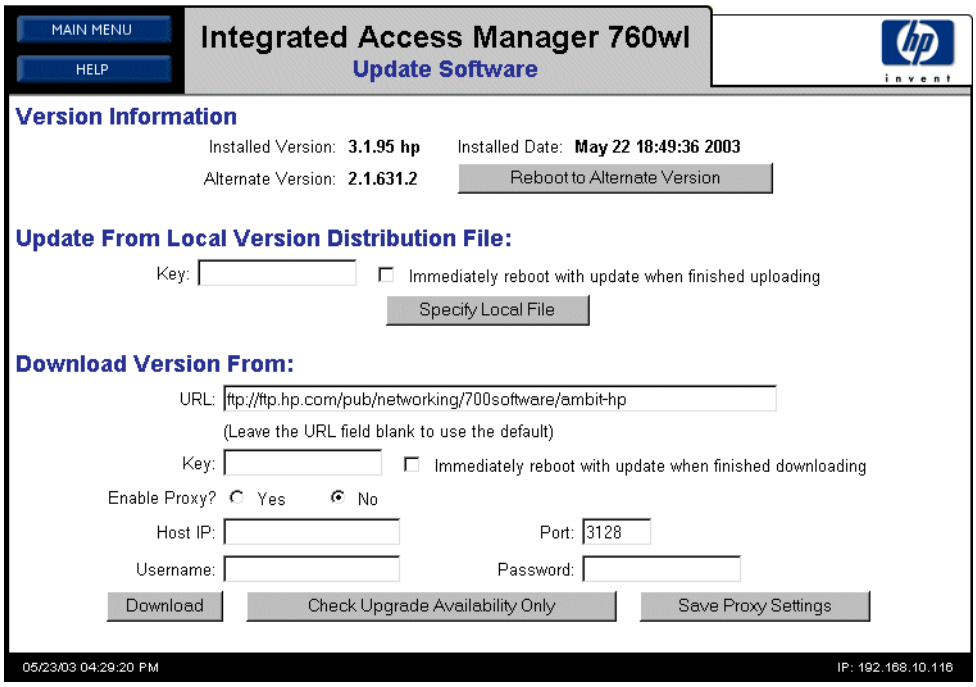

Figure 4-8. Entering the Update Software

From this page you can do the following:

- Reboot using the alternate software version
- Upload a new version from a distribution file stored on your local system (the system from which you are running the browser interface)
- Determine if there is a newer version of the software available on a remote site
- Download a new version from a remote site using the File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), or Hypertext Transfer Protocol (HTTP)

Determining if a New Software Version is Available

To determine if a new software version is available, do the following:

Step 1. Under the **Download Version From:** heading, type the URL from which you want to check software availability.

By default, this field contains the location of an FTP server site where upgrade images are stored. If you clear the field and don't enter a different URL, the system will use the default URL.

Step 2. Click **Check Upgrade Availability Only**. You do not need to enter a key to check availability.

A Confirm Software Update page appears that either informs you that the current version is up to date, or tells you that there is an update available.

Click **Return to Update Software Page** to continue with a version update.

Downloading a Software Version

To download a new software version from a remote site, do the following:

Step 1. Under the **Download Version From:** heading, type the URL from which you want to download the software.

By default, this field contains the location of an FTP server site where the most recent upgrade images are stored. If you clear the field and don't enter a different URL, the system will use the default URL.

The format of the URL is <*protocol*>://<*host*>/<*update file*> or <*protocol*>://<*username*>:<*password*>@<*host*>/<*update file*>

<*protocol*> can be FTP, HTTP, or TFTP.

<*host*> can be an IP address or a server hostname, and can include a port (<*host*>:<*port*>).

<*username*>:<*password*> specifies a username and password with access to the remote site, if required.

<*update file*> is the filename (including the path) of the software image. For TFTP or anonymous FTP, the path is relative to the anonymous FTP or TFTP root. If a username and password is required for FTP, then the full path to the update file must be specified. For HTTP, the path is always relative to the web server's site root directory.

For example:

The default URL to get the latest software from HP is:

`ftp://ftp.hp.com/pub/networking/software/700software/ambit-hp`

If you system is an Access Controller, the default URL is:

`ftp://ftp.hp.com/pub/networking/software/700software/ambit-am-hp`

To retrieve the software from an internal FTP server at "mycompany.com" that requires a username and password:

`ftp://jane:secret@ftp-int.mycompany.com/users/ftp/ambit-3.1.95`

This accesses the FTP server as user `jane` with password `secret` and downloads the image from the full path `/users/ftp/ambit-3.1.95`.

Step 2. Type your ***Key***.

The key is a password that allows you to download and use the 700wl Series system software.

Step 3. You can have the system automatically reboot immediately after downloading. To do so, check the box that says **Immediately reboot with update when finished downloading**.

Step 4. If you need to go through a proxy server, select **Yes** for the **Enable Proxy?** setting.

A proxy enables you to download the new image through an enterprise firewall.

If you enable the proxy

a. Type the IP address of the proxy server

b. Type the port number of the proxy service (default is `3128`)

c. Type the username and password needed for access.

d. If you download new system software periodically, you can save your proxy settings by clicking **Save Proxy Settings**.

Step 5. Click **Download**.

Step 6. The Update Software Process page appears, as shown in Figure 4-9.

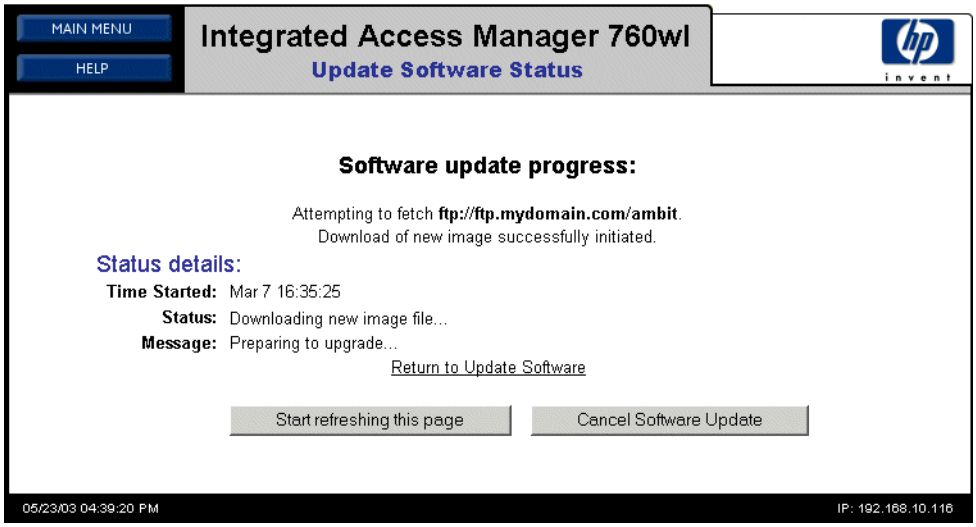

Figure 4-9. Software Update Status

Figure 4-9 shows the initial status page that normally appears immediately after you click **Download**. If you want a continuous status update, click the **Start refreshing this page** button. Otherwise, the status is not updated.

Note: *If your currently installed software is much older than the new version you are downloading, it may not be possible to revert to your old image without doing a factory reset, which will restore your unit to its default settings. If this is the case, a warning will be displayed advising you to make a backup of your system before*

proceeding with the upgrade. If you save a backup of your system, you will then be able to restore your configuration if a downgrade to your older version becomes necessary.

The status page refreshes approximately every 10 seconds, displaying updated status information. After the download and unpack operations are complete, a completion message appears: **New image successfully installed.**

If you specified an automatic reboot, the status message also displays **Initiating reboot** and the reboot operation starts.

If you did not specify an automatic reboot, you can return to the Update Software page as soon as the download has completed. This page displays both the installed software version as well as an alternate version, which should be the newly downloaded version. You must then reboot to the alternate version to complete the update of the software.

Whether the reboot was automatic or initiated from the update software page, once it has completed you can click **Main Menu** and the Administrator login page should appear.

Note: *Depending on the amount of data on your system, you might have to wait as long as 90 seconds after a reboot before you can log in again.*

When the system has rebooted, the newly downloaded version should appear as the Installed Version under the Version Information section of the Update Software page. The previously installed version should appear as the Alternate Version.

Rebooting, Shutting Down, or Resetting the System

You can reboot, shut down, or reset your Integrated Access Manager or Access Control Server to factory defaults settings from the System Shutdown page. To access the System Shutdown page:

Step 1. Click **System Shutdown** from the Main Menu.

The System Shutdown page appears, as shown in Figure 4-10.

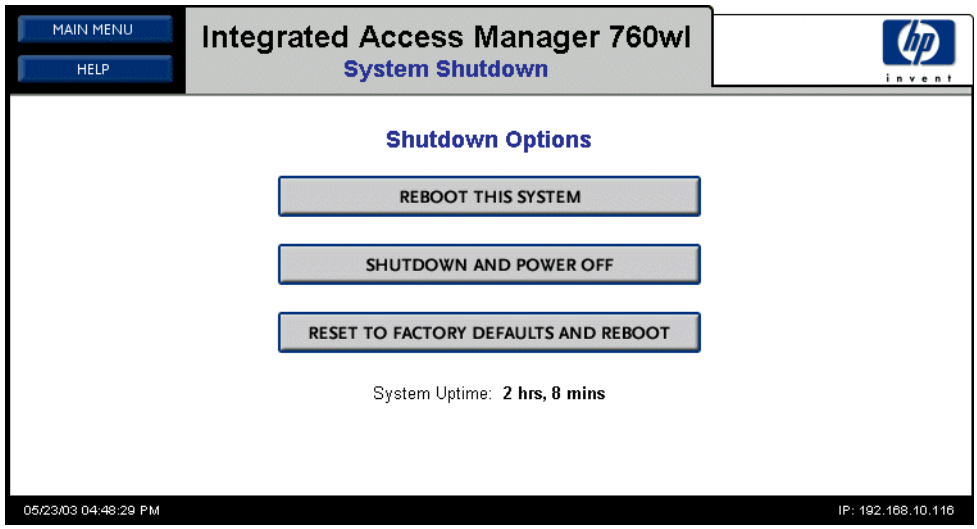

Figure 4-10. Shutdown Options

Step 2. Click **Reboot this System** to reboot.

The Confirm System Reboot page appears.

a. Click **Continue with System Reboot** button to proceed with the reboot.

b. Click **Cancel and Return to Shutdown Options** if you do not want to reboot.

Caution: *If you reboot an Access Controller or Integrated Access Manager, you will erase the logs and backup information.*

Step 3. Click **Shutdown and Power Off** to shut down the system.

The Confirm System Shutdown and Power Off page appears.

a. Click **Continue with Shutdown and Power Off** to proceed with the reboot.

b. Click **Cancel and Return to Shutdown Options** if you do not want to shutdown.

Step 4. Click **Reset to Factory Defaults and Reboot** to restore the original configuration settings, including the default network settings and uplink port configuration.

The Confirm Factory Reset and Reboot page appears, as shown in Figure 4-11**.**

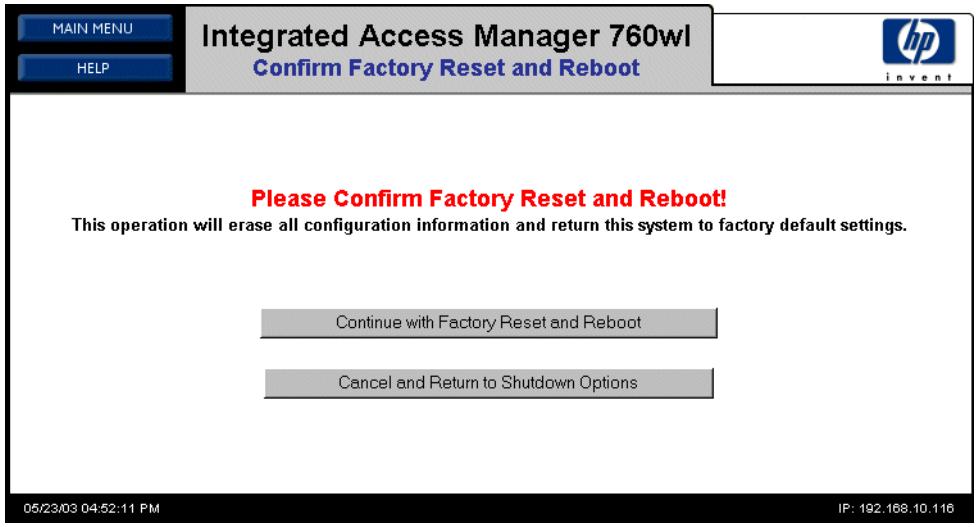

Figure 4-11. Confirm Reset to Factory Defaults

a. To proceed, click **Continue with Factory Reset and Reboot**.

If you are using the browser-based Administrative Interface over the network, and your system had a static IP address, you may need to use the `42.0.0.1` default URL to reach the system after a factory reset.

b. Click **Cancel and Return to Shutdown Options** if you do not want to reset and reboot.

Caution: *If you click* **Continue**, *all your settings and configuration options, including your network settings and uplink port configuration, are returned to the factory default settings. If you later want to restore your configuration, you must restore from a backup image that was created and saved before the reset.*

Warning: *If you have reconfigured your uplink to use a port other than the default (such as a gigabit fiber port on an option card) upon a factory reset that port will revert to a downlink port. This can have adverse effects on your network. You will also need to use the serial console interface and CLI to reconfigure the uplink port.*

If you have reconfigured your uplink port, it is recommended that you do a factory reset using the serial console and CLI so that you can reconfigure the uplink port to the correct alternate port.

VIEWING SYSTEM STATUS 5

This chapter explains how to view the system status of the Integrated Access Manager 760wl, Access Control Server 740wl, or Access Controller 720wl. It consists of the following sections:

Viewing Status Information 5-1

Viewing Access Controllers 5-3

Viewing the Active Client List 5-4

Viewing Active Session Information 5-7

Viewing Log Files 5-9

Viewing Version and License Information 5-12

Note: *The Views you can access are different depending on whether you are connected to the Administrative interface for an Integrated Access Manager, Access Control Server, or Access Controller.*

Viewing Status Information

This chapter explains how to view information about the components of your HP ProCurve Secure Access 700wl Series system. The links under the Views heading in Figure 5-1 show the information you can view from the Administration Interface on an Integrated Access Manager. Subsets of these views are available from an Access Controller or an Access Control Server.

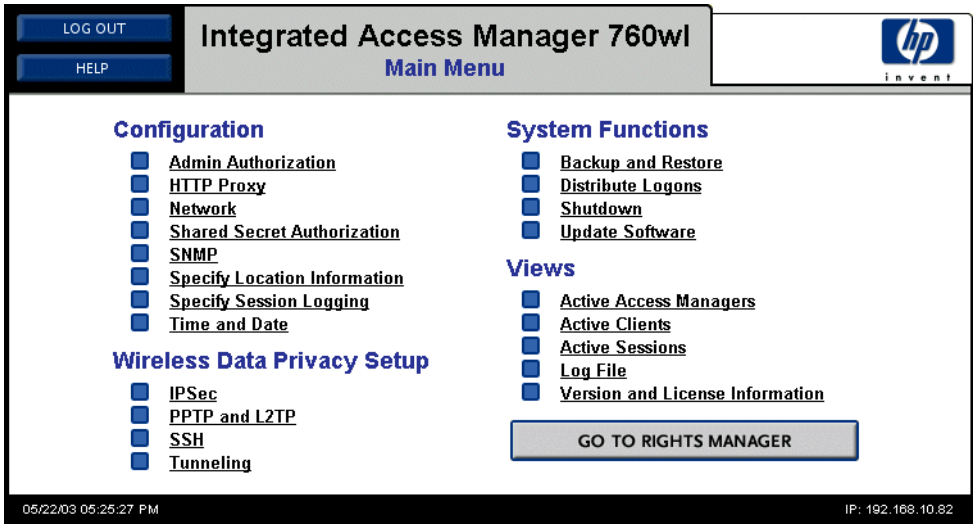

Figure 5-1. Views available from the Main Menu of an Integrated Access Manager

Filtering a Status Display

To make it easier to find the information you need from a status display, you can filter the display to show only a subset of the entries. The criteria by which you can filter depends on the display you are viewing. Table 5-1 shows the criteria you can use to filter the display in various views.

» To filter a display, select your criteria and click **Apply Filter**.

» To restore to the default filter, click **Reset Filter**.

Table 5-1. Filtering Specifications

Filter by:	In Display:	Details
Lines	All	Lets you specify the number of entries to be displayed. The default is 25. You can choose 10, 25, 100, 1000, or unlimited.
Protocol	View Active Sessions	Lets you display only sessions using a selected protocol. Select a protocol from the drop-down list. Default is All.
MAC Address	View Active Sessions	Lets you display only sessions for a selected MAC address. Select a MAC address from the drop-down list. Default is All.
Port number	View Active Sessions	Lets you display only sessions for a selected port. Select a port from the drop-down list. Default is All.
Severity	View Log File	Lets you display only log entries with the selected Severity or greater. Select a severity from the drop-down list. Default is Notice, meaning that all messages with a severity of Notice or higher are displayed.

Table 5-1. Filtering Specifications

Filter by:	In Display:	Details
Within	View Log File	Lets you display log entries within the time period you select. Select a time period from the drop-down list. The default is “The past day.”
Search	View Log File	Lets you display only those log entries whose message contains the string you specify. The search criteria only applies to the Message part of the log entry.

Sorting: You can sort a display by clicking certain column headings. Sortable columns are indicated by a heading that is also a link (underlined).

Paging Long Displays: If a display has more entries than will fit on one page (based on the Lines filter setting) Next Page and Previous Page links are provided to let you view the additional entries.

Viewing Access Controllers

The View Access Controller List shows all the currently connected Access Controllers to your Integrated Access Manager or Access Control Server. This display can help you manage your Access Controllers. This view is available only from the Main Menu of an Integrated Access Manager or Access Control Server. It cannot be viewed from an Access Controller.

To view the current list of Access Controllers:

Step 1. Click **Active Access Managers** from the Main Menu.

The View Access Manager List page appears, as shown in Figure 5-2.

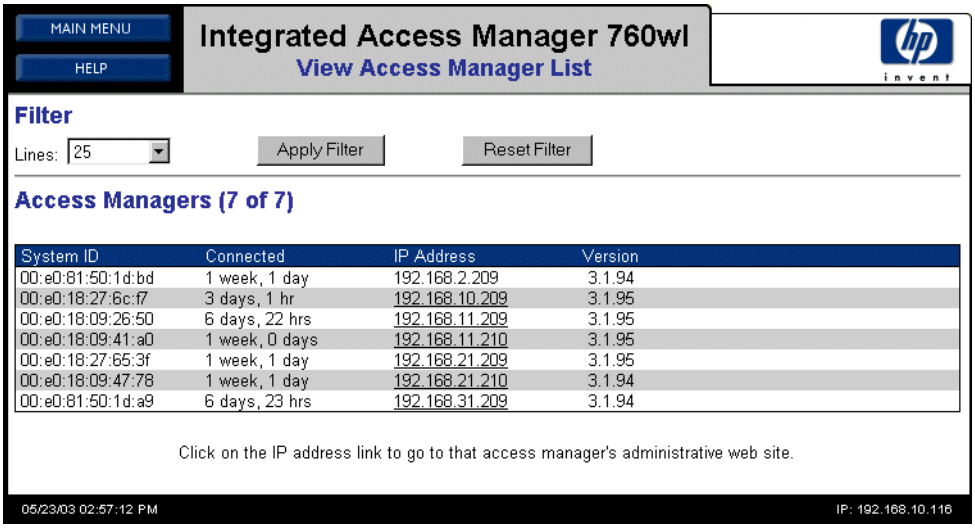

Figure 5-2. View Access Manager List (showing Access Controllers)

The Access Manager list displays the following information about each Access Controller:

Table 5-2. Active Access Managers Display

Column	Sortable	Description
System ID	No	The MAC address (hardware ID) of the Access Controller.
Connected	No	The length of time the unit has been connected to the Integrated Access Manager or Access Control Server.
IP Address	Yes	The IP address of the unit. If the address is underlined, it links to the Administrative web site for the Access Controller.
Version	No	The software version running on the system.

Step 2. If the IP address of an Access Controller in the list is underlined, click the link to go to the Administrative web site for that Access Controller.

Note: *In an Integrated Access Manager, the built-in Access Controller shares a single web interface with the Integrated Access Manager, so the IP address for that Access Controller is not underlined.*

Viewing the Active Client List

The Active Clients list shows the status of all connected clients. This display can be accessed from an Integrated Access Manager or an Access Controller. It cannot be accessed from an Access Control Server.

To view the Active Clients list:

Step 1. From the Main Menu, under the Views heading, click **Active Clients**.

The View Active Clients page appears, as shown in Figure 5-3.

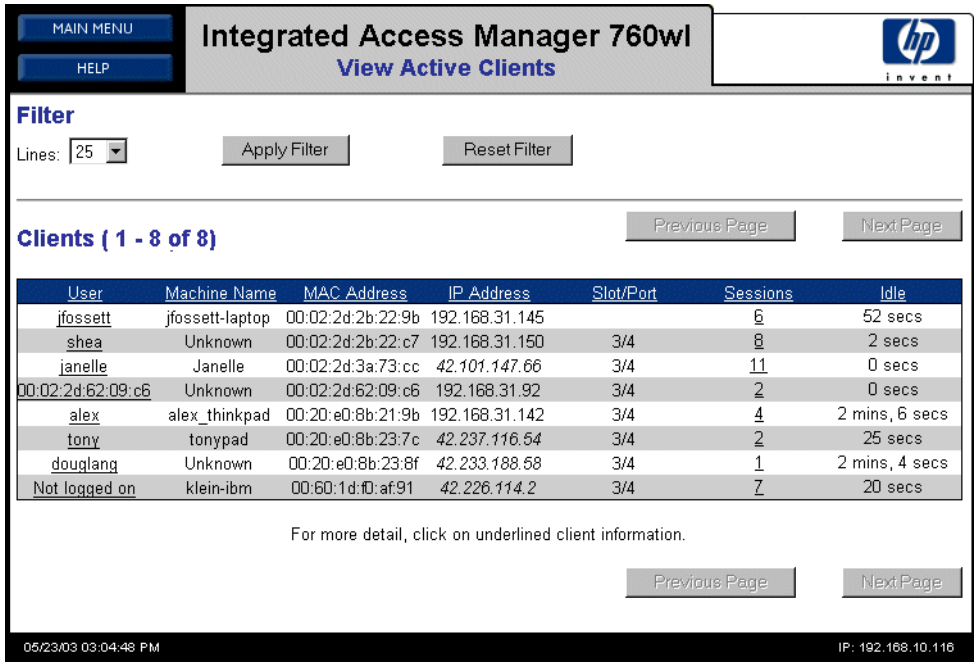

Figure 5-3. View Active Clients

For each active client the display presents the following information:

Table 5-3. Active Clients Display

Column	Sortable	Description
User	Yes	The logon name of this client. This entry links to detailed information about this client.
Machine Name	Yes	The name of the client system, if known.
MAC Address	Yes	The MAC address of the client.
IP Address	Yes	The IP address of the client. If the address is in NAT mode, it is shown in italics. If it is a real or static IP, it is shown in plain text.
Slot/Port	Yes	The slot and port on the Access Controller through which this client is connected.
Sessions	Yes	The number of sessions currently running for this client.
Idle	Yes	The amount of time, in seconds, that this client has been idle.

Note: *The statistics for a client are a snapshot of the client status at the moment that you request the display. Some entries, like Sessions and Idle time, change frequently. You can refresh your browser page to get an updated display.*

Step 2. To view details for a specific client, click the client user name in the User column.

A client information page appears for the selected client, as shown Figure 5-4.

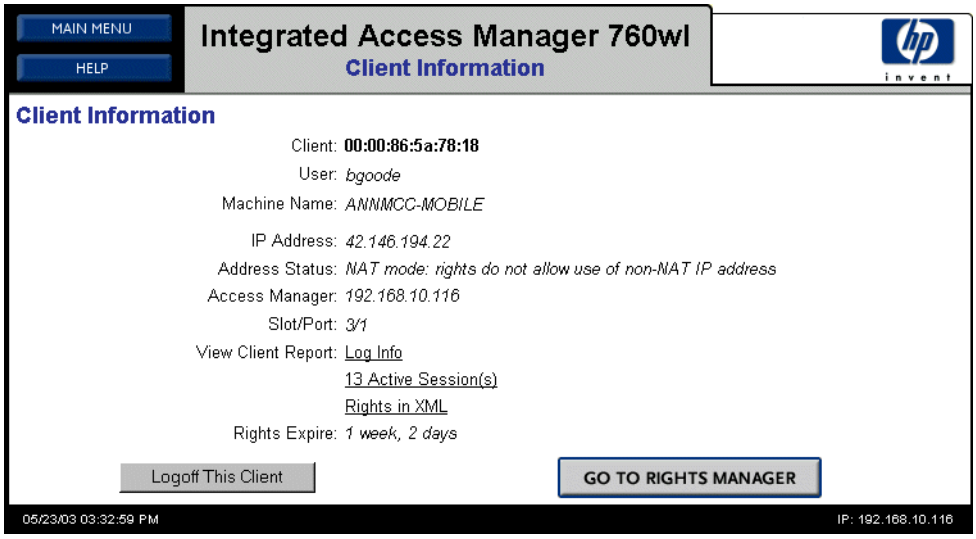

Figure 5-4. Client Information

The following information is displayed:

Table 5-4. Active Client detail information

Information	Description
Client	The MAC address (hardware ID) of the client.
User	The name or the user, if known, otherwise the MAC address.
Machine Name	The name of the machine, if known.
IP Address	The IP address assigned to the client. If the client is connected using PPTP or L2TP, this is the inside tunnel address. The outside tunnel address is also listed (“via tunnel from <outside tunnel IP>“).
Address Status	Information about the IP address. This includes: • Whether NAT mode is being used, and why • Whether a static IP is allowed • Other relevant information, depending on how the address was obtained
Access Manager	The IP address of the Access Controller to which the user is connected.
Slot/Port	The slot and port on the Access Controller to which the user is connected.
IP Security	The type of IP Security in place. ***Note:*** *This item appears only if encryption is allowed at the location where the client is connected.*

Table 5-4. Active Client detail information

Information	Description
View Client Report	Links to reports about this client: • **Log Info** displays the Log File entries for this user, filtered using the client MAC address as the search string. See “Viewing Log Files” for more information. • ***n*** **Active Session(s)** displays the Active Sessions view, filtered by the client’s MAC address. See “Viewing Active Session Information” for more information. • **Rights in XML** display the Rights definition for this client in XML format. See “The User Rights Simulator” in Chapter 12 for more information on the format of this display.
Rights Expire	The length of time (in days, hours, and minutes) remaining before this client’s rights expire.

Step 3. To log this client off, click **Logoff This Client**.

Step 4. To go to the Rights Manager, click **Go to Rights Manager**. This takes you to the main Rights Manager page on the Access Control Server or Integrated Access Manager associated with this Access Controller.

Viewing Active Session Information

Viewing active sessions provides information on a client’s open sessions. From this page, you learn more about a client’s network traffic. This display can be accessed from an Integrated Access Manager or an Access Controller. It cannot be accessed from an Access Control Server.

To view active sessions:

Step 1. Click **Active Sessions**.

Step 1. The View Active Sessions page appears, as shown in Figure 5-5.

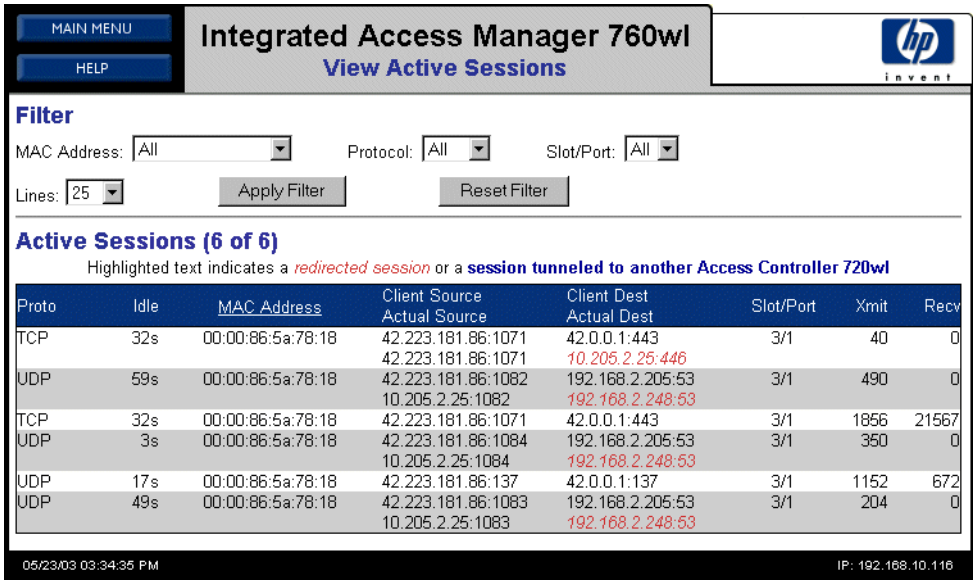

Figure 5-5. Active Sessions

The following information is displayed:

Table 5-5. View Active Sessions Information

Column	Sortable	Description
Proto	No	The protocol for the session. The following protocols are translated from their numeric strings: CMP, IGMP, TCP, UDP, ESP, AH, IP, and PPTP. All other protocol are displayed as the protocol number prefixed with a pound sign (#).
Idle	No	The time since the last packet was received, in hours (h) minutes (m) and seconds (s).
MAC address	Yes	The MAC address of the client associated with this session.
Client Source Actual Source	No	**Client Source**: The IP address and port of the client system, as placed in the packet header by the client. **Actual Source**: For a client in NAT mode, the IP address and port of the Access Controller, as re-written after translation. • If the address is shown in dark blue bold, the session has been tunneled from another Access Controller due to roaming.
Client Destination Actual Destination	No	**Client Destination**: The destination IP address as placed in the packet by the client. **Actual Destination**: The destination IP address and port as re-written by the Access Controller. • If the address is in dark red italics, this session was redirected based on the rights in effect for this location.
Slot/Port	No	The Access Controller slot and port number used by the session (if any).

Table 5-5. View Active Sessions Information

Column	Sortable	Description
Xmit	No	The total number of bytes transmitted.
Recv	No	The total number of bytes received.

Viewing Log Files

On an Integrated Access Manager, Access Control Server, or Access Controller you can view system warnings and messages kept in the HP system log files.

These systems support two types of logging:

- Informational logging captures HP system messages and warnings. This log is kept on the HP system, and occurs automatically.
- Session logging provides information about every completed session. These logs are optional. If enabled, log entries are sent to an external Syslog server that you specify when you enable session logging. For information on enabling session logging, see “Specifying Session Logging” in Chapter 2. See “Session Log File” for a description of the information that is logged to the Syslog server.

  You cannot view the session log files from the Administrative interface. However, you can view session information from the Active Sessions display discussed in “Viewing Active Session Information”.

For information about Rights Manager logs, see Chapter 12, “Troubleshooting, Logs, and Rights Import/Export”.

Informational Log File

Each Access Controller or Integrated Access Manager logs events to an internal file. Viewing these logs provides important information on the activity of the Integrated Access Manager and Access Controller.

To view the log file, do the following:

Step 1. From the Main Men under the Views heading, click **Log File**.

The Log File appears, as shown in Figure 5-6.

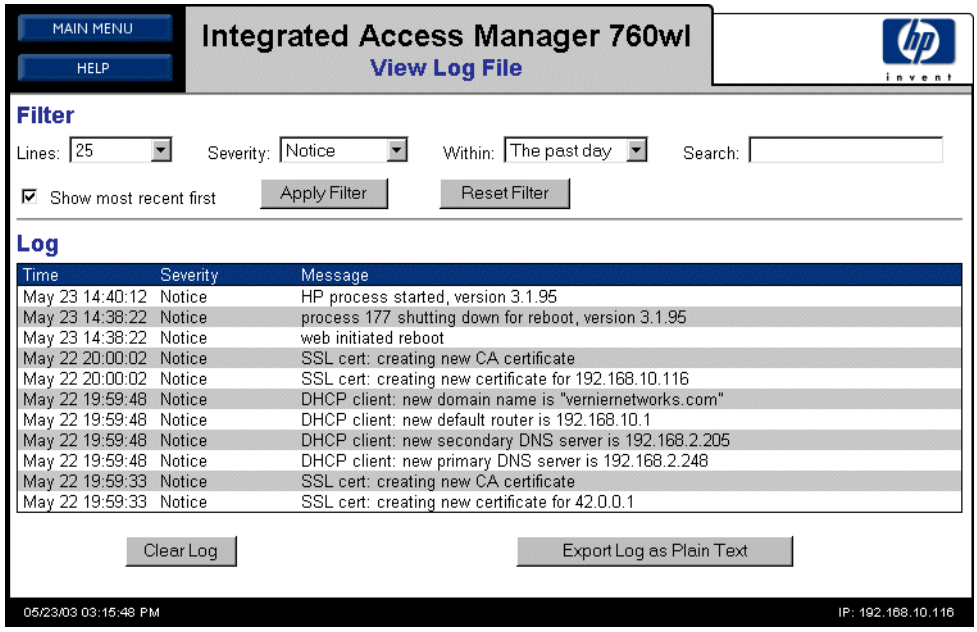

Figure 5-6. Viewing a Log FIle

The most recent entries are shown first by default.

Step 2. You can filter the entries in reverse time order by deselecting **Show most recent first** and clicking **Apply Filter**.

Step 3. You can filter to change the contents of the log display:

- From the **Lines** field drop-down list, select the number of lines to display:

  You can choose 10, 25, 100, 1000, or unlimited.

- From the **Severity** field drop-down list, select the severity level of the notices to display. The display will include all events with that severity level or higher.

  The severity levels, from highest (most severe) to lowest, are: **Critical**, **Error**, **Warning**, **Notice**, or **Informational**.

  For example, if you select Notice as the severity, all events with severities of Notice, Warning, Error, or Critical are displayed.

- From the **Within** field drop-down list, select the time period to display.

  You can choose the past hour, day, week, or no time limit.

Step 4. Click **Apply Filter** to view filtered results; click **Reset Filter** to reset to the default view.

Step 5. Click **Export Log as plain text** to save the log as a plain text file on your web browser's system. You might want to archive or forward the log file.

Note: *Click* **Clear Log File** *to empty the log file.*

Session Log File

The Session log provides information about every completed session. This log is kept on an external Syslog server. See “Specifying Session Logging” in Chapter 2 for information about setting up session logging.

The session log entries consists of a single line for each session, for example:

```
logmsg: pri 36, flags 0, from vm18.tgilman.com, msg Nov 13 01:43:50
90466740 129 00:30:65:41:da:56 udp 42.230.129.94:5353
224.0.0.251:5353 10.10.10.18:5353 224.0.0.251:5353 474 0 test
```

The information in the first line of the example (through the date and time) is added by the Syslog server. The information from the 700wl Series system starts with the second line of the example (`90466740`, which is the start time of the session). The format of the part of the entry sent by the 700wl Series system is:

```
<Start time> <Duration> <MACaddr> <Protocol> <Client Source>
<Client Destination> <Actual Source> <Actual Destination> <Bytes Transmitted>
<Bytes Received> <UserID>
```

Table 5-6 defines the items in the session log entry. The items are delimited by spaces.

Table 5-6. Session Log information

Data Item	Definition
Start time	Start time of the session, in seconds since 1/1/2000 12:00am GMT Note: to convert this to a UNIX time_t (time relative to 1/1/1970) subtract 946684800
Duration	Duration of the session in seconds
MACaddr	Client’s MAC address
Protocol	Session protocol type
Client Source	The original client source IP address and port
Client Destination	The original client destination IP address and port
Actual Source	The actual source IP address and port, if re-written after NAT
Actual Destination	The actual destination IP address and port, if redirected or tunnelled through another Access Controller
Bytes Transmitted	Total number of bytes transmitted during the session
Bytes Received	Total number of bytes received during the session
UserID	The client’ s user (login) ID

The session log also creates log entries whenever an Access Controller sends an associate or disassociate message to the Rights Manager. These entries have the form:

```
assoc <client MAC> <AM IP> <slot>/<port>
and
disassoc <client MAC> <AM IP>
```

Associate messages are sent to the Rights Manager whenever an Access Controller detects a client. This includes the initial client contact, Access Controller to Access Controller roaming, and Access Controller port-to-port roaming.

A Disassociate message is sent when a client has not sent any packets for a specified period of time and has not responded to repeated client probes. (The timing between probes and the length of time the probes should continue to be repeated can be set through the Advanced Network Configuration page. See "Advanced Network Settings" for a more detailed discussion of client disassociation.)

You cannot view the session log from the HP system Administrative interface. You must retrieve the log file from the Syslog server and view it with a text editor.

However, you can view this same information through the Active Sessions display discussed in "Viewing Active Session Information".

Note: *If you have enabled Rights Manager logging, those log entries may also appear in the Syslog file. Rights Manager logging uses Local7 as the syslog facility; if you set session logging to use Local7 as well, then the Rights Manager entries may be intermixed with the session log entries. The Rights Manager logs error messages, and may also log Logons, failed Logon attempts, Logoffs, and LDAP entries, at your option. See "Viewing the Rights Manager Log" for more information on these entries.*

Viewing Version and License Information

The Version and License Information page gives you a summary of important information about your system. This information includes the System ID, the version of software currently running in the system, the date and time of the last configuration change, how long the system has been up, and the IDs and description of all components installed in the system.

» To view version and license information, click **Version and License Information** from the Main Menu**.**

Figure 5-7 shows typical information for an Integrated Access Manager 760wl with a four-port option card installed.

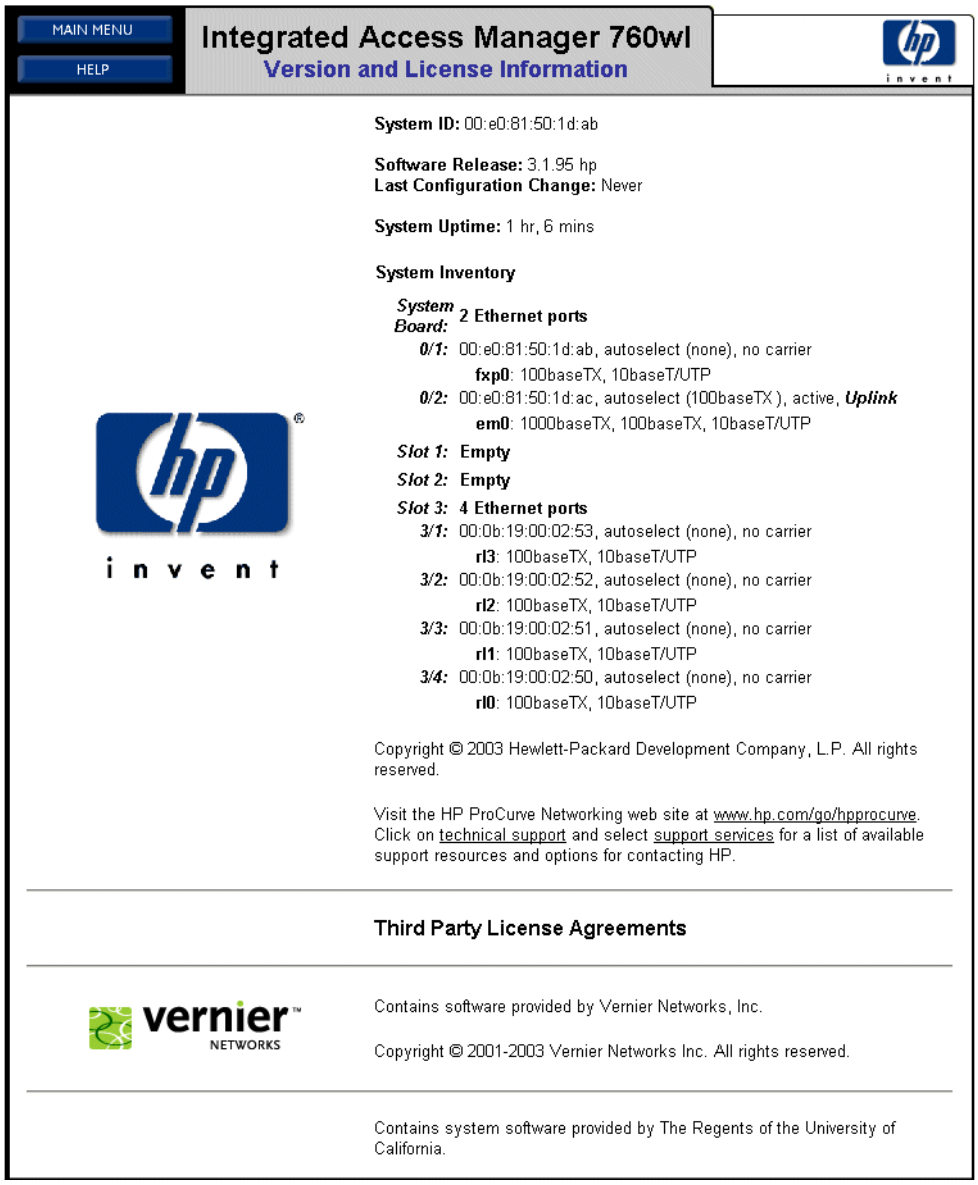

Figure 5-7. Displaying version and license information

Much of this information may be useful if you need to contact HP Technical Support. In addition, information such as the System ID may be needed for other configuration functions.

For example, you need to enter the system ID when defining an Access Controller prior to creating a Where and a Location in the Rights Manager. You can use your browser's copy and paste functions to copy the System ID (MAC address) from this Version and License information page and paste it into the System ID field in the Rights Manager's Access Controller Editor.

Part 2
The Rights Manager

6 GETTING STARTED WITH THE RIGHTS MANAGER

This chapter explains the concepts and terminology that are fundamental to the HP ProCurve Secure Access 700wl Series Rights Manager. It includes the following sections:

About the Rights Manager 6-1

Rights Manager Terminology 6-3

User Authentication 6-10

Two Simple Rights Examples 6-11

How the Rights Manager Determines a User's Rights 6-13

VLANs and the 700wl Series System 6-14

Network Address Translation in the 700wl Series System 6-16

Getting to the Rights Manager 6-18

The Rights Manager Clients Page 6-22

About the Rights Manager

The Rights Manager is the portion of the HP ProCurve Secure Access 700wl Series system that handles user authentication and allocates access rights to clients that try to access the network through the 700wl Series system. The Rights Manager enables you to configure the appropriate authentication mechanisms through which users are granted access to the network, and set up site access policies based on a client's location, group membership, the time of day, and other factors. The Rights Manager also provides tools for monitoring and troubleshooting the authentication and rights configurations for users and clients.

The Rights Manager is a component within the HP ProCurve Access Control Server 740wl or Integrated Access Manager 760wl. Once you have configured the authentication mechanisms and rights policies, the Rights Manager is responsible for authenticating users and determining the rights that should be granted to each user. The Access Controller is also responsible for enforcing those rights for the user as long as the user's session is active and valid.

Figure 6-1 shows some of the relationships that are involved in managing rights.

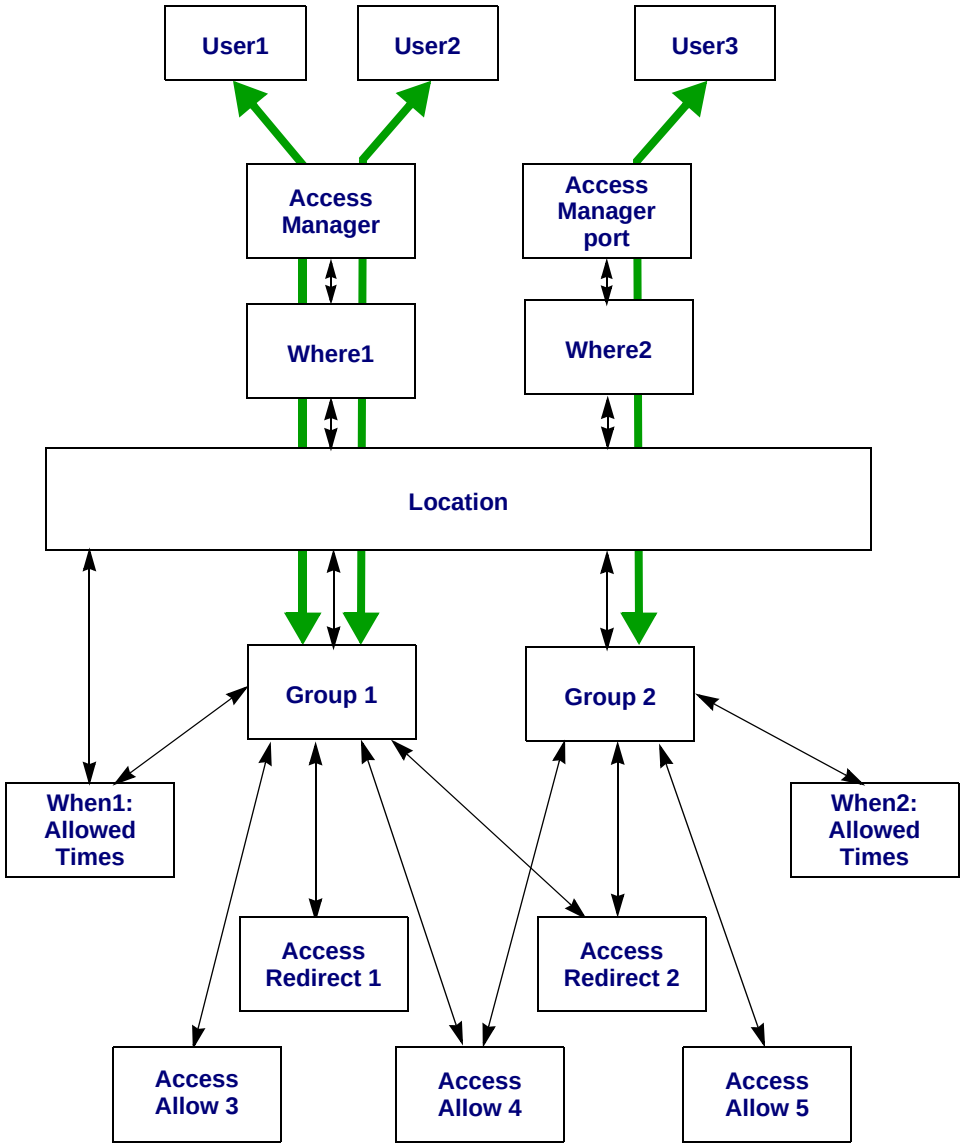

Figure 6-1. Simplified Rights diagram

The set of rights granted to a user is a function of where they connect to the system, the current day and time, and the group to which the user belongs.

- A wireless user typically connects through awireless access point connected to an HP ProCurve Access Controller port. Access Controller ports make up the entities known within the Rights Manager as "Wheres." In the diagram shown in Figure 6-1, *Where1* is defined as all ports on a specific Access Controller. *Where2* is a single port on a specific Access Controller.
- ***Wheres*** are components of a Rights Manager ***Location***. Thus, the physical point through which a user connects to the wireless LAN (WLAN) defines the Rights Manager Location with which the user is associated. The Location defines a number of the parameters that control the user's access to the network. For example, as shown in Figure 6-1, one of the

properties of a Location is a ***When***—a specification of the times (and dates if appropriate) that access is allowed through this location.

- Whens define date, day, and time specifications that are used to constrain when access to the network is allowed. Whens are used to define the times during which access through a location is allowed, and are also used define the times during which a group is ***valid*** (i.e., when the rights defined by a group are in effect). A given When may be used to define valid times for multiple locations and / or groups. *When1* in the diagram is an example of this, as it is used as a component of both the Location and of Group 1.
- A Location also specifies what groups are allowed at that location—and this effectively defines which users can access the network through that location. If a user is a member of a group that is allowed at the location, he / she will be able to log on and receive a set of access rights as defined by the group. If the user is not a member of a group allowed at that location, he / she may not be able to log on at all. It is possible to allow multiple groups with different types of rights, so that some users can log on through a location and receive extensive access, while other users may receive very limited access.
- The group(s) of which a user is a member define the actual access rights the user receives once they have been authenticated. Access rights determine whether traffic from a client (user) is allowed to pass on to its destination within the network, is redirected to an alternate destination, or is dropped. ***Redirects*** define which packets should be diverted to alternative destinations, and ***Allows*** define which packets are allowed on to their original destinations. Any packets that are not either redirected or allowed are dropped. As shown in Figure 6-1, Allows and Redirects, once defined, can be used to define the access rights for multiple groups.

The green arrows in the diagram show how rights for a user are determined when the user connects to the network. Both User 1 and User 2 connect through access points connected to the Access Controller defined as Where1. Because they are both members of Group 1, and Group 1 is allowed at this location, when they are successfully authenticated they receive the rights associated with Group 1. User 3 connects through an access point connected to the Access Controller port defined as Where2, and because she is a member of Group 2, she receives the access rights defined by Group 2. (These examples all assume that the user is successfully authenticated -- that their user ID and password are recognized by the authentication process in use by the Rights Manager.

Locations and Groups both have a number of other properties that define or constrain how clients / user can access the network, beyond the simplified explanation presented here. The sections that follow in this chapter define in greater detail the components and concepts introduced here. The chapters that follow in this Guide describe how to use the Rights Manager to configure the appropriate policies for your site.

Rights Manager Terminology

The 700wl Series system is a very flexible system that gives you a lot of fine-grained control over which users can access a network, and under what conditions they can access it. Access rights are granted based on a combination of factors including who the user is, where he / she is accessing the network from, and the time (hour, day of week, date) at which access is requested. Based on these criteria, a set of access rights are granted to the user. Traffic from the user is then either forwarded on to its destination, or redirected to a different destination, based on those rights.

Groups

Groups are used to define the access rights (and certain other capabilities) for all clients / users that are members of the group. Clients / users are given access rights within the network based on their group membership. The group construct allows you to define the rights for multiple users in a single operation. The following points are key to understanding rights in the 700wl Series system:

- Access rights (the Allows and Redirects) are always associated with groups, and only groups.
- Every client that access the 700wl Series system is *always* a member of at least one group, and that group membership is what determines the rights that are given to the client.

There are six types of groups that are supported in the 700wl Series system:

- **Guest:** a group that defines the rights given to someone who logs in as a Guest or Registered Guest using web-based logon. Users in this group are not authenticated, and their rights are usually quite restrictive. The 700wl Series system provides a predefined Guest group, with a default set of rights that does not allow a Guest user to access the network. If you plan to allow guests, you must modify the Guest group rights to allow access as appropriate to your system. You can also create additional Guest-type groups.
- **Logon:** a group that defines the rights given to a user / client who has not yet been authenticated. Users are typically only members of this group temporarily, until they are successfully authenticated. The 700wl Series system provides a predefined Logon group and you can create additional groups of this type.
- **Implicit Users:** a group that defines the default set of rights granted to all authenticated users at a location (assuming the implicit Users group is allowed at that location). If an authenticated user is not a member of any other group, he / she will at least have the rights associated with this group. If he is a member of other allowed groups, he will have implicit Users rights *in addition* to the rights from the other groups.

  The 700wl Series system provides a predefined Implicit Users group named “Users” and you can create additional groups of this type.
- **Normal:** an administrator-defined group that specifies a set of rights that should be granted to users who are members of this group. Users must be explicitly designated as members of the group, either by being added as a member through the Rights Manager UI, through retrieval of group membership information from an external authentication service, or in some cases, due to the presence of a specific 802.1Q tag associate with traffic from the client. There are no predefined groups of this type.
- **Access Point:** a special-purpose group that defines a set of rights for clients that are actually access points.
- **Stop:** a special-purpose group that defines a set of rights for clients that should be prevented from any network access. There is one predefined group of this type, named “No Access.” This group is particularly useful in conjunction with the Network Access Control Console.

A group has the following properties:

- The group type, as discussed above.
- A list of the times (time of day, days of the week, and so on) when these rights are in effect, sometimes called the Valid Times for the group. This list actually a set of named time specifications, called Whens. A ***When*** is defined independently of a group, so you can

define a time specification once and then use it for multiple groups. See “Whens” on page 6-7 for a more complete explanation.

- A list of Redirect rights, known as ***Redirects***, which specify traffic destinations that should get redirected to alternate destinations for members of this group.
- A list of Allow rights, known as ***Allows***, which specify the destinations to which traffic will be forwarded for members of this group. Allows are implemented through a set of packet filters that determine what traffic the client is allowed to generate. Any packets generated by the client that do not match one or more of the filters are rejected. You can base filters for packets on protocol, IP address, port, or other considerations. You can specify packet filters to be as granular as you want, even to the point of specifying individual bit patterns in the client’s packet.
- A number of other options, such as how IP addresses are assigned to the client, how long a set of rights remains valid before re-authentication is required, and so on.

These are discussed in detail in Chapter 7, “Configuring Groups”.

Expire and Linger Timers

In addition to the set of Whens that determine when group rights are valid, you can set an ***Expire Timer*** that specifies how long a group member can stay logged on before he/she will be forced to reauthenticate. The expire timer can be set to a relative time (duration, such as 2 hours), a fixed time (for example, 12:00 pm) or to Never expire.

When a client’s session expires, that client is logged off and must reauthenticate (log on again). If the client’s group rights are still valid after his session expires, the client will be able to log on again and regain those group rights.

If the group rights become not valid (based on the group’s Whens) the client will be logged off even if his expire time has not elapsed. The client may reauthenticate, but will no longer have the rights associated with that group.

If a client is concurrently a member of multiple groups that specify different user expire times, the following rules apply:

- If multiple fixed expire times are defined, the user is required to reauthenticate each time a set of rights expire. For example, if Group A rights expire at 2pm and Group B rights expire at 4pm, a client who is a member of both groups will be logged off at both 2 pm and 4 pm.
- If multiple relative expire times are defined, the longer of the specific expire times takes precedence. For example, if Group A rights expire in two hours, and Group B rights expire in four hours, a client who is a member of both groups will remain logged on for four hours. The client automatically gets Group A rights again after two hours, without having to reauthenticate.
- A restrictive expire time (either relative or fixed) always takes precedence over the Never expire setting. For example, if Group A rights expire in two hours, Group B rights expire in four hours, and Group C has the expire time Never, then a client who is a member of all three groups will need to reauthenticate every four hours. The longer of the restrictive expire times takes precedence.

Note that these rules assume that each Group’s rights continue to be valid for the duration of the various expiration time windows.

The ***Linger Timer*** defines how long the 700wl Series system will continue to keep a client around (i.e., logged on) after an Access Controller has determined that the client appears to have disconnected. The linger timer setting provides an interval during which a client can complete a roam without being logged off and having to reauthenticate. If the Linger timer expires and the client has not reappeared, the Rights Manager logs the client off.

Locations

A ***Location*** is a logical construct that represents an entry point or set of entry points to the 700wl Series system. Every client that accesses the 700wl Series system is associated with a location.

The location defines certain access parameters, such as the times when access through the location is permitted, the groups whose members are allowed entry through the location, what types of encryption are supported, and how authentication for tunneling protocols are handled by the location. A location is *associated with* a set of physical entry points, but should not be confused with the physical entry points themselves.

While the location itself does not directly define access rights for a user (that is done by the user's group membership) the location may modify or limit the scope of a user's rights.

A location has the following properties:

- A list of Wheres that defines the Access Controllers, ports, or specific clients that are associated with this location
- A list of the times (time of day, days of the week, and so on) when access through this location is allowed, specified as a list of Whens.
- A list of groups that are allowed at this location. This determines which users can gain access to the system through this location.
- Whether encryption is required, allowed, or disabled, and what types are supported.
- How authentication is handled for the supported tunneling protocols
- Whether Network Address Translation (NAT) is required for clients entering through this location

These are discussed in detail in Chapter 8,"Setting Up Locations".

By default, the 700wl Series system provides a predefined location named Everywhere Else which represents all entry points into the system that are not specifically included in another location. By default, it is valid at all times. Until you create another location, this is the location to which *all* clients are associated.

Wheres

The actual entry points that connect through a location are specified as a list of ***Wheres***. Wheres are used to determine what location a client should be associated with.

A Where can represent an Access Controller, a single port on an Access Controller, or a specific client identified by its MAC address. When a client accesses the system, the Where that it matches determines the location that the client will be associated with.

Wheres can overlap, with the more specific Where taking precedence when determining how to associate a client with a location.

For example, suppose you define the following Wheres and locations:

- Where (A) is defined as Access Controller A, and is included in Location A.
- Where (B) is defined as port 1 on Access Controller A, and is included in Location B.
- Where (C) is defined as the MAC address of client X, and is used in Location C

Therefore, a client that accesses the 700wl Series system via Access Controller A ports 2, 3, or 4 will be associated with Location A.

A client that accesses the 700wl Series system via Access Controller A port 1 will be associated with Location B.

When client X accesses the system via any port on Access Controller A, he will be associated with Location C.

Caution: *You can use the same Where in more than one location. For example, you might want to define one location that is valid during business hours, and another location that is valid after hours. However, you should not use the same Where in two locations that are valid at the same time. If two locations have the same Where and overlapping Whens, only one location will be accessible from the port or Access Controller defined in that Where during the times both locations are valid. Clients connecting through that When will always be associated with the location with the name that comes first alphabetically.*

Whens

A ***When*** is a named time specification that can apply to a location or a group. A When can be specified by date, days of the week, or hour of the day, or any combination. For example, you could create a When named "WorkWeek" defined as Monday through Friday from 7 AM to 5 PM for all dates. You could create another When named "TradeShowWeek" defined as August 19, 2002 through August 23, 2002, 7 AM to 5 PM. These Whens can then be used to define valid times for both groups and locations.

The Whens included for a group determine when the rights for members of that group are valid. At times outside the valid times, the user will not be granted the access rights associated with that specific group. This does not necessarily mean that the user will have no rights at all, however, as he or she will at least be a member of the Implicit Users group, and may belong to other groups as well.

The Whens included for a location determine when clients, connecting to the network through the ports associated with that location, are affected by the properties of that location. This does not mean that clients cannot connect through those ports if the location is not valid; clients connecting over those ports during non-valid times will simply be seen as connecting through a different location—typically the default Everywhere Else location—and will be subject to that location's properties.

For example, suppose that Location A includes all ports on Access Controller A (specified through the appropriate Where) and is valid from 8:00 am to 5:00 pm Monday through Friday. Clients accessing the network during those hours are seen by the Rights Manager as

connecting through Location A. However, clients that access the network outside these hours are seen as accessing the network through the default location, Everywhere Else, and the properties defined for the Everywhere Else location apply to these clients.

The Whens defined for groups, and the Whens defined for locations can interact to determine when a client has access to the network through a given location. See "How Groups and Locations Interact" for a more detailed explanation of the possible interactions.

Access Rights

Access rights determine what network resources a user can access, by specifying whether user packets are forwarded or redirected by the Access Controller. Rights for a group are defined as a set of Allows and Redirects.

Allows filter for packets that are permitted to be forwarded by an Access Controller. The specification of an Allow includes:

- The protocol type
- The destination port, if any
- The destination IP address, if any

Redirects filter for packets that should be redirected to a new destination, as specified by the Redirect. Some redirects may simply forward the packet to an alternate destination that performs the same function as the original destination—for example, a DNS server request could be redirected to the enterprise DNS server rather than the one that was originally specified. Redirects can also be used to prevent traffic from reaching a prohibited destination—in this case, the redirect may instead send the request to the 700wl Series system Stop page. A Redirect can include:

- The protocol type
- The original destination port
- The original destination IP address
- The new (redirect) destination port
- The new (redirect) IP address

Note: *Redirects are applied before Allows. Therefore, if you have both a Redirect and an Allow enabled in your group for the same traffic, the Redirect always takes precedence and the Allow is ignored.*

In addition, Redirects and Allows are applied in alphabetical order based on their name. Therefore, if you have conflicting Redirects enabled (filtering for the same traffic but redirecting to different destinations, for example) the Redirect that comes first alphabetically will succeed, and the subsequent redirects for that traffic will never be applied. The same is true of conflicting Allows. If a user is concurrently a member of multiple groups, the Allow and Redirect filters for the groups are merged, and are then applied in alphabetical order.

Note: *If you enable the Automatic HTTP Proxy feature for a group, then HTTP traffic is not affected by the Allows and Redirect rights you set for that group. Instead, proxy filters must be set to permit or deny HTTP traffic. This is done as part of the*

automatic HTTP proxy configuration. By default, if you enable the HTTP Proxy feature for a group but do not set any HTTP proxy filters, all HTTP traffic is permitted.

See Chapter 7 for more information about defining Allows and Redirects.

How Groups and Locations Interact

While Groups define the access rights a user is granted, certain properties of the location may act to bound or limit the access rights a user has through a given location.

Allowed Groups at a Location

The location configuration specifies which groups are allowed at that location. Therefore, if a user connects to the network through a location that does not support the group he belongs to, that user will not receive the rights defined by that group. On the other hand, if a user connects through a location that supports multiple groups, he will still only be granted the access rights defined by the group(s) he belongs to.

Group rights are additive: if a user is concurrently a member of multiple groups at a location, she receives all the rights defined by all the groups of which she is a member. In some cases, this could mean that the more liberal rights of one group may override the more restrictive rights of another group, or vice versa. The combined sets of Redirects and Allows are merged, and then evaluated in alphabetical order, so if there are conflicting rights between two groups, the filters that come first alphabetically take precedence, and the others are ignored.

Note: *If the implicit User group is allowed at a location, all users authenticated at this location are* ***automatically*** *members of this group in addition to any other groups, and receive User group rights in addition to the rights from other groups. By default, the predefined User group allows forwarding of All IP traffic from clients, which may undermine a more restrictive set of rights granted by another group. To avoid this problem, you can either redefine the rights for the implicit Users group, or remove the implicit Users group from the allowed groups at the location.*

For example, suppose Location A is defined to allow the default groups (Logon, Guest and User) as well as groups Contractors and Finance. Further, suppose user Joe is a member of the group Contractors, and user Sue is a member of the Finance group.

- When Joe connects to the network through Location A, after he has authenticated, he gets all rights associated with both the Contractors group and the Users group. He does not get any rights associated with group Finance.
- When Sue connects and is authenticated, she gets the rights associated with Finance and Users, but not with Contractors.

Suppose then that Location A is reconfigured and Contractors is removed from the list of groups allowed at that location.

- When Sue authenticates through Location A, she still gets the rights associated with both Users and Finance.

- When Joe authenticates, he no longer receives Contractor rights, still doesn't get Finance rights, but still receives the default Users rights defined for that location.

  If your intent in removing the Contractors group was to allow only Finance group clients (i.e., allow Sue but not Joe) then you also need to remove the Users group from the list of allowed groups to prevent Joe from getting a default set of rights.

Valid Times for Locations and Groups

The second area of interaction is between the Whens (valid times) defined for the location and the Whens defined for the group. If a location's Whens specifies valid times that are more limited than the Whens specified by the Group, then the user will only be able to access the network through that location during the times that are valid for the location. On the other hand, if the location allows more generous valid times than does the user's group, then the user's rights will be limited by the group's valid times. However, in this second scenario, the user might still have access to the network with default Implicit User rights during times when his other group rights are not valid.

For example, suppose Location A is defined with the When "WorkWeek" that allows access only Monday through Friday from 7 AM to 5 PM. Further, suppose user Joe, belongs to a group called Contractors, which is valid everyday between 1 PM and 4 PM.

- When Joe tries to connect to the network on Saturday at 2 PM, he will not be able to able to connect through Location A because it is not within the location's valid times. Instead, he will be connected through the default Everywhere Else location, which may not include Contractors as an allowed group.
- If Joe tries to access the network on Monday at 10 AM, he will be able connect through Location A, but he will only receive default User rights, because the rights associated with the Contractors group are not valid at that time.
- If he connects on Wednesday at 2 PM, he will connect through Location A and receive the full set of rights defined for the Contractors group.

User Authentication

The 700wl Series system Rights Manager provides a great deal of flexibility in how users can be authenticated. The Rights Manager supports three types of authentication:

- **Web-based logon:** when a client first makes an HTTP request, the Rights Manager presents a browser logon page, and authenticates the user using one or more Authentication services, such as an LDAP database, RADIUS server, Kerberos, an XML-RPC service or through the built-in authentication database.
- **Wireless Data Privacy logon:** when a client initiates a connection to the system using an L2TP or PPTP client, the Rights Manager can forward the packets on to the appropriate RADIUS authentication service and use the results of that to determine authentication. Alternatively, it can use its built-in database to do the user authentication.
- **Monitored logon:** the 700wl Series system supports both 802.1x logon and NT Domain logon. In these cases, the Access Controller simply forwards the packets on to the RADIUS or NT Domain server, and monitors the response to determine whether the user has been successfully authenticated. Once the client has been authenticated, rights for the client are requested from the Rights Manager.

The client is authenticated through an authentication ***Realm***, which is simply an ordered list of one or more authentication services. You can define multiple authentication realms, and then specify which realm should be used as the default realm.

An authentication *service* is an single instance of a service used for authentication, such as a specific Active Directory service, or RADIUS server. The Rights Manager supports the following services:

- LDAP Directory services, such as Active Directory or iPlanet LDAP server
- RADIUS servers
- Kerberos services
- XML-RPC-based services
- The Rights Manager's built-in database. This is the default authentication service. You can populate it with user names and passwords through the Rights Manager.

The ability to specify multiple services within a realm means that if the user is not authenticated through the first service in the list, the Rights Manager will automatically try to authenticate against the other services in the realm, in the order in which they are listed.

Authentication and Group Membership

The Rights Manager has the ability to retrieve information about a user's group membership from the authentication service, if the service supports and includes that information. LDAP and RADIUS services and the built-in database can contain group information, which can be retrieved as part of the authentication process.

For NT Domain logon, you can create groups that map to the user's domain, and the user's domain will then determine group membership.

If the service used to authenticate the user does not include group information, the Rights Manager is capable of obtaining group information separately from an authentication service that does include that information. For example, if a user authenticates through 802.1x logon, the Rights Manager can be configured to then go to an LDAP service to retrieve group information.

Two Simple Rights Examples

The following simple examples explain at a high level why you might want to change rights. First, there is the visiting professor who comes to Cold Creek University for the month of January. Second, the contractors who are implementing a new student database for Cold Creek University need extra hours to complete the project on schedule.

Example 1: Visiting Professor

Professor Lupine is visiting Cold Creek University for the month of January to share his research findings. Figure 6-2 shows a conceptual illustration of his rights compared to those of the regular professors at this location.

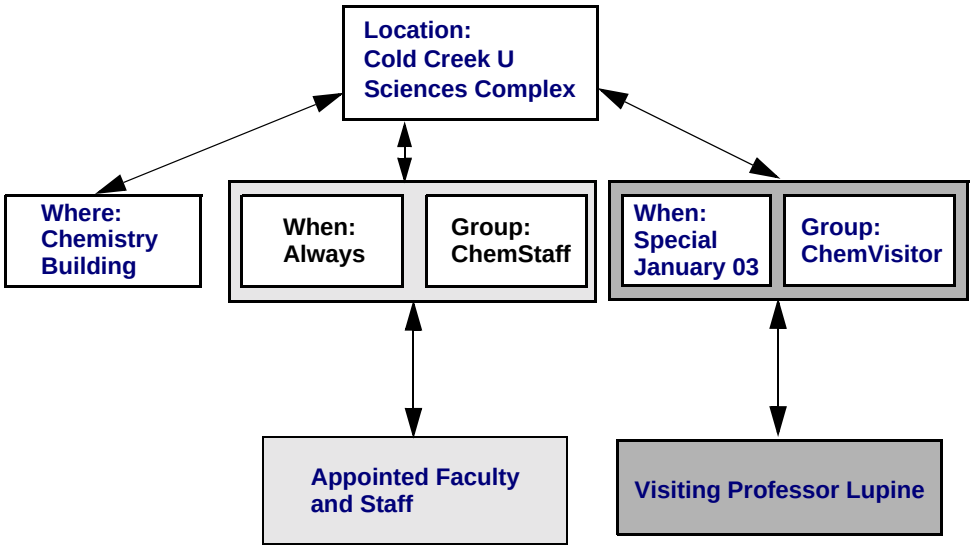

Figure 6-2. Example 1, visiting professor

In Figure 6-2, Professor Lupine needs access to the University network for the month of January. The regular professors have access to the University network though a location defined for the Sciences Complex, which includes a Where (set of Access Controller ports) that provide access to the Chemistry building. Regular faculty and staff are members of a Group named “ChemStaff” that provides them with access to network resources appropriate for their needs. Their access rights are valid at all times because the ChemStaff group includes a When (“Always”) that is valid 24 hours a day, 7 days a week. When Professor Lupine arrives, he is assigned membership in a group named “ChemVisitor,” which has similar access rights to the ChemStaff group, but includes the When named “Special January 03.” This When gives him access only for the month of January. After January, he will no longer be able to log in to the university network.

Example 2: Contractors with Extended Hours

The contractors who are completing implementation of a new student database need access for additional hours. Figure 6-3 shows the conceptual overview of giving special database contractors extended hours.

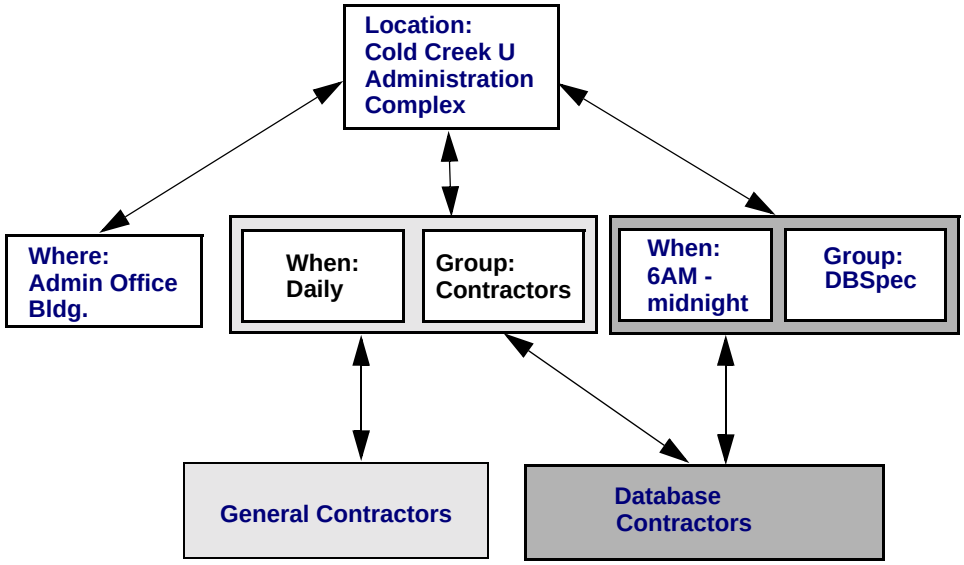

Figure 6-3. Example 2, contract database specialist

In this example, all contractors have access to the network through the access points in the Administrative Office building, and have access rights that are valid during working hours (five days a week, 8AM to 6PM). The database specialists are members of this group. However, during the period when they need extended access, they are given group membership in a second group ("DBSpec") which gives them access during extended hours for a two-week period. The rights conferred by membership in this group are granted in addition to the rights they receive as members of the Contractors group. Once the two-week period is up, they revert to having access only during the same hours as other contractors.

How the Rights Manager Determines a User's Rights

A user's ability to access the network through the 700wl Series system is determined by the group(s) he/she belongs to, modified by any restrictions imposed by the location through which he/she is connected to the network.

The user's group membership determines

- The actual access rights granted to the user
- The times when those rights are valid
- How long those rights remain in effect before re-authentication is required

The location through which the user accesses the 700wl Series system determines

- The times when the user can access the network through that location
- Whether the groups the user belongs to are allowed at that location.

For example, a user might belong to a group that allows extensive access 24 hours a day, but the location he/she tries to connect through may restrict the hours that access is allowed, or may not allow access for that group. Thus both the user's hours of access and his user rights could be limited based on the restrictions imposed by the location.

On the other hand, a location might allow access 24 hours a day, and allow a large number or groups, some of which grant extensive rights. However, if a user, accessing the system through that location, belongs only to a single group that has time restrictions and grants limited rights, that user will be bound by the time and rights restrictions imposed by his group. The fact that the location has more relaxed restrictions and supports groups with more generous rights does not affect this user.

Note that if a user is a member of multiple groups, he or she gets all the rights associated with *all* of those groups. In addition, properties like Rights expiration times are additive—the Rights Manager will use the maximum expire time from the set of valid groups for the user, to determine when the user must re-authenticate.

Determining Group Membership

A user is always a member of at least one group. The user's group membership may (and probably will) change over the course of his association with the 700wl Series system.

Initially, all clients are considered members of a Logon group as soon as they are detected at an entry point to the system.

As the user logs on, his membership is determined based on the following:

- If the user logs on as a Guest (or Registered Guest, if that option is enabled) the user is considered a member of the Guest group and receives Guest rights.
- If the user logs on as an authenticated user, then the user's group membership is determined as follows:
  - — If the user is authenticated through the Built-In authentication method, and has been added as a member to one or more groups, he is considered a member of those groups.
  - — If the user is authenticated through a external authentication service (LDAP, RADIUS, etc.), and group membership can be retrieved from the external service, then the user is considered a member of the Rights Manager group whose name matches the group name retrieved from the external service.
  - — If the user authenticated through NT Domain logon, then the user is considered to be a member of the Rights Manager group whose name matches the NT Domain name.
  - — If the user's packets include an 802.1Q VLAN ID (tag), and it matches the VLAN ID for a group that is configured to allow membership based on VLAN ID, then the user is considered a member of that group.
  - — If the user is successfully authenticated but no group affiliation can be determined, the user is considered a member of the Implicit User group.
  - — If the user cannot be authenticated, he/she continues to be a member of the Logon group, with Logon rights only.

VLANs and the 700wl Series System

The 700wl Series system provides support for 802.1Q Virtual LAN (VLAN) tags. Packets that arrive pre-tagged with a VLAN ID are passed on to the network with the tag preserved

(assuming the client's rights allow the traffic to be passed on). For clients that transmit untagged traffic, the 700wl Series system can be configured to add a tag to the traffic before transmitting it on into the network—effectively assigning wireless clients to be members of a VLAN based either on their group membership, or on the location through which they access the 700wl Series system.

Note: *The 700wl Series system does not do any blocking of traffic based on VLAN tags—it cannot be used to enforce VLAN membership.*

The 700wl Series system supports VLAN trunking automatically—this does not require any special configuration on the 700wl Series system.

Note: *If packets from a client already include a VLAN tag, that tag overrides any VLAN tags you specify for locations or groups. You cannot use the HP ProCurve VLAN feature to change a client's pre-existing VLAN association.*

To assign wireless clients to participate in the network's VLAN structure, you can specify a VLAN ID as a location property or as a group property. In either case, if the VLAN property is set, the specified VLAN tag is added to packets before the traffic is sent on through the system.

- If a VLAN ID is specified at the location, that VLAN ID is automatically added to all traffic entering the system through that location.
- If a VLAN ID is specified through the group, that VLAN ID is automatically added to all traffic origination from clients that are members of that group.
- If a VLAN ID is specified through both the location and the client's group, the group's VLAN ID overrides the location VLAN ID.
- If a client belongs concurrently to multiple groups that specify conflicting VLAN IDs, the lowest numbered VLAN ID is used.

  Note: *It is intended that either the location mechanism or the group mechanism be used to provide a VLAN ID, not both.*

  If a client changes group membership (for example, one group's rights terminate and the client remains or becomes a member of a different group) the client's VLAN ID may change based on new group membership. For example, if you configure the Logon group to have a VLAN ID, the Logon group's VLAN ID gets associated with all clients that are members of the Logon group, even though that membership is only temporary until they get authenticated. After authentication their VLAN ID may change based on the group membership they have as an authenticated user.

If packets arriving from a client contain a VLAN tag, the 700wl Series system handles it as follows:

- The VLAN ID is maintained and passed on as the traffic is forwarded or redirected. Thus, passage through the 700wl Series system does not interfere with the operation of the VLAN configuration of your network. If the client is a member of a group that specifies a different VLAN tag, the original tag (the one transmitted from the client) takes precedence—the group tag is ignored.
- If the VLAN ID matches the VLAN ID associated with a group in the Rights Manager, and that group allows a VLAN ID to determine group membership, the client becomes a

member of that group, and the group access rights are assigned to the client *in addition* to any other rights the client has based on other group memberships. This mechanism allows you to assign rights based on the VLAN ID received from the client.

Caution: *Because VLAN tags can be added to traffic or altered by the client, allowing group membership based on the incoming tag may compromise your network's security. A client could possibly use this method to get access rights to which he would not otherwise be entitled.*

Network Address Translation in the 700wl Series System

Clients connected to Access Controller or Integrated Access Manager ports can obtain an IP address in one of three ways:

- **Network Address Translation (NAT) mode:** The Access Controller or Integrated Access Manager responds to a DHCP request from a client with a "private" IP address on the subnet configured for NAT (by default, the `42.0.0.1` subnet, although this is configurable through the Advanced Network Settings page). The Access Controller or Integrated Access Manager then rewrites the original source IP address (the private IP address) and source port of client packets sent to the network (NAT and PAT functions). The original source is replaced by the IP address of the Access Controller along with a port number that is unique within the 700wl Series system. Packets received by an Access Controller or Integrated Access Manager from the network sent in reply to the NAT and PAT packets are relayed to the appropriate client with the destination IP address and destination port number rewritten as appropriate. The Access Controller maintains a connection table to map return packets back to their intended destination.
- **Non-NAT, static IP mode:** The client uses a pre-assigned IP address on the Access Controller or Integrated Access Manager's subnet. Packets received by the Access Controller or Integrated Access Manager with this static IP address in the destination IP address field are forwarded to the appropriate client. Packets from the client to the network do not have their source IP address or source port number rewritten.
- **Non-NAT, Real IP mode** (also known as dynamic IP mode): The client sends a DHCP request for an IP address which the Access Controller or Integrated Access Manager passes on to an external DHCP server. This DHCP request will obtain an IP address on the Access Controller or Integrated Access Manager's subnet. Packets received by the Access Controller or Integrated Access Manager with the IP address returned by the external DHCP server are forwarded to the appropriate client. Packets from the client to the network do not have their source IP address or source port number rewritten.

The 700wl Series system, by default, uses NAT mode. However, there are settings associated with both Locations and Groups that enable you to specify whether and under what conditions NAT is used.

Note: *If PPTP or L2TP is enabled for the location, the group and location NAT settings only affect how the inner tunnel address is assigned. See the discussion in "NAT and VPN Tunneling" for a more detailed explanation of how this is handled.*

At each ***Location***, you can specify whether NAT is required for clients connecting through that location, or whether it is allowed but not required. The default setting is to require NAT.

For each *Group*, you can specify whether NAT should be used for client members of the group always, only if the client's IP address is on the wrong subnet, or never. You can also specify whether static IP addresses are allowed for clients in the group.

The location NAT setting interacts with Group NAT settings such that:

- If the location requires NAT, then NAT will always be used for clients connecting through the location, unless they are members of a Group that prohibits NAT (via the **Never NAT** setting). In this case, a Group setting of **Do not NAT except for clients on the wrong subnet** is ignored.
- If the location does not require NAT, the Group settings determine whether NAT will be used for clients that are members of that group (unless PPTP or L2TP is enabled at that location).

The NAT settings affect client IP addressing as follows:

- If NAT is *required* then the Access Controller or Integrated Access Manager *always* uses NAT mode. Static IP addresses are translated, and client DHCP requests are satisfied by the Access Controller or Integrated Access Manager's internal DHCP server, and then translated.

  NAT mode is used when the following settings are in effect:

  — The location NAT setting is checked, and the Group specifies **NAT Clients** or **No NAT except for clients on the wrong subnet**, or

  — The location NAT setting is not checked, but the Group specifies **NAT Clients**

- If NAT is *never* allowed (the Group NAT setting is **Never NAT**) the Access Controller or Integrated Access Manager always uses one of the non-NAT modes. The client's real IP address (as obtained via DHCP) or its static IP address is always left untouched as the source address in packets going to the network. This may cause problems if the client's IP address is not within the Access Controller's subnet—return packets may not be able to reach the client. This setting is intended for use only by the Access Point group for Access Point clients, or for groups whose clients are network infrastructure devices such as switches or hubs.

  Caution: *The Never NAT setting should not be used for regular clients. If it is used for one group, then it MUST be used for the Logon group for all locations where that group is allowed, and for all other groups that an affected client could transition to.*

- If NAT is not required but is allowed (based on a location that does not require NAT, and a Group NAT setting of **Do not NAT except for clients on the wrong subnet**) then the client's IP address will be used, untouched, unless the IP address is not valid.

  The validity of the client IP address is determined as follows:

  — If the Access Controller port (through which the client is connected) has an IP address range assigned to it (via the Advanced Network Configuration), then the address is valid if it falls within that range. If the address does not fall within the port's address range, NAT is used, even if the address is within the Access Controller's subnet.

  — If there is no range assigned for the port, then the client's IP address is valid if it is within the Access Controllers subnet. NAT is used only if it is not within that subnet.

  If the IP address is not valid, then the Access Controller assigns a private IP address

and rewrites the source address in packets. With this setting it is possible that NAT might be used initially, but when the client's DHCP lease expires, it successfully gets a valid IP address, which is then used as the source IP instead of a NAT address.

Using NAT has a number of benefits for the 700wl Series system, especially in relation to roaming. Except for Access Point clients (members of the Access Point group) it is recommended that you leave NAT enabled for most groups.

NAT and VPN Tunneling

The use of VPN tunneling affects IP addressing and NAT. If PPTP or L2TP is enabled for a location (via the Specify Encryption per Location page), then addressing works as follows:

- The first DHCP request is taken to be a request for an outer tunnel address, and NAT is *always* used regardless of the setting of the group and location NAT properties.

  Note: *A side-effect of this behavior is that if encryption is* **Allowed but not Required** *at the location, and a client connects without using a tunneling protocol, that client will always be NATed upon making a DHCP request. The client will avoid being NATed only if the client's group allows static IP addresses, and the client actually uses a static IP address.*

- The inner tunnel address is assigned per the Group and Location NAT settings, as discussed above. However, if Real IP mode is used, the client's IP address is assigned as specified through the Tunneling Configuration page—either via the external DHCP service or from a specified address range.

Getting to the Rights Manager

To go to the Rights Manager:

Step 1. Point your browser to the IP address or hostname of your Integrated Access Manager or Access Control Server, and log in to the Administrative Interface.

The Main Menu appears. Figure 6-4 shows the Main Menu for an Integrated Access Manager. The Main Menu for an Access Control Server look similar, but with a subset of the choices.

If you log in to the Administrative interface for an Access Controller, the Main Menu page displays a **GO TO CONTROL SERVER** button in place of the **GO TO RIGHTS MANAGER** button. Click this to go to the Access Control Server, and login to the Access Control Server Administrative Interface.

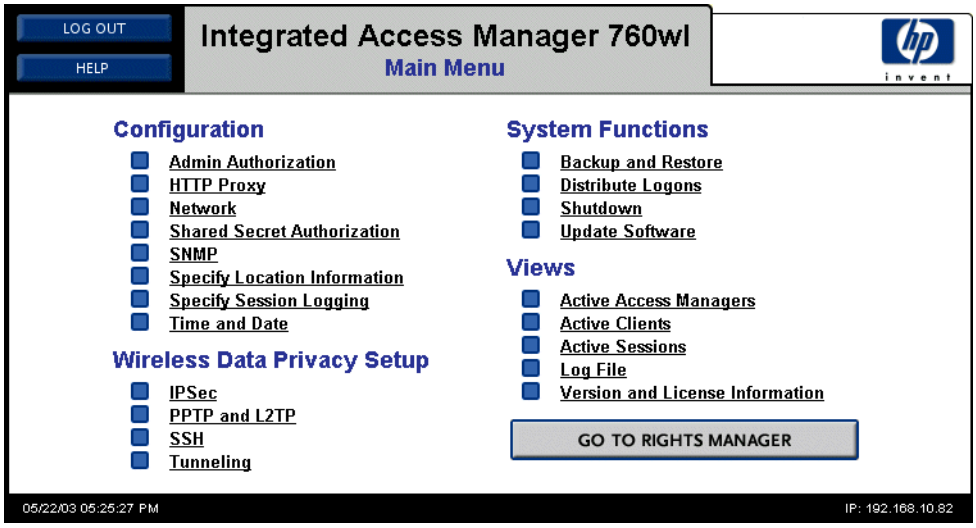

Figure 6-4. Main Menu

Step 2. Click **GOTO RIGHTS MANAGER**.

The Rights Manager Clients page appears, as shown in Figure 6-5.

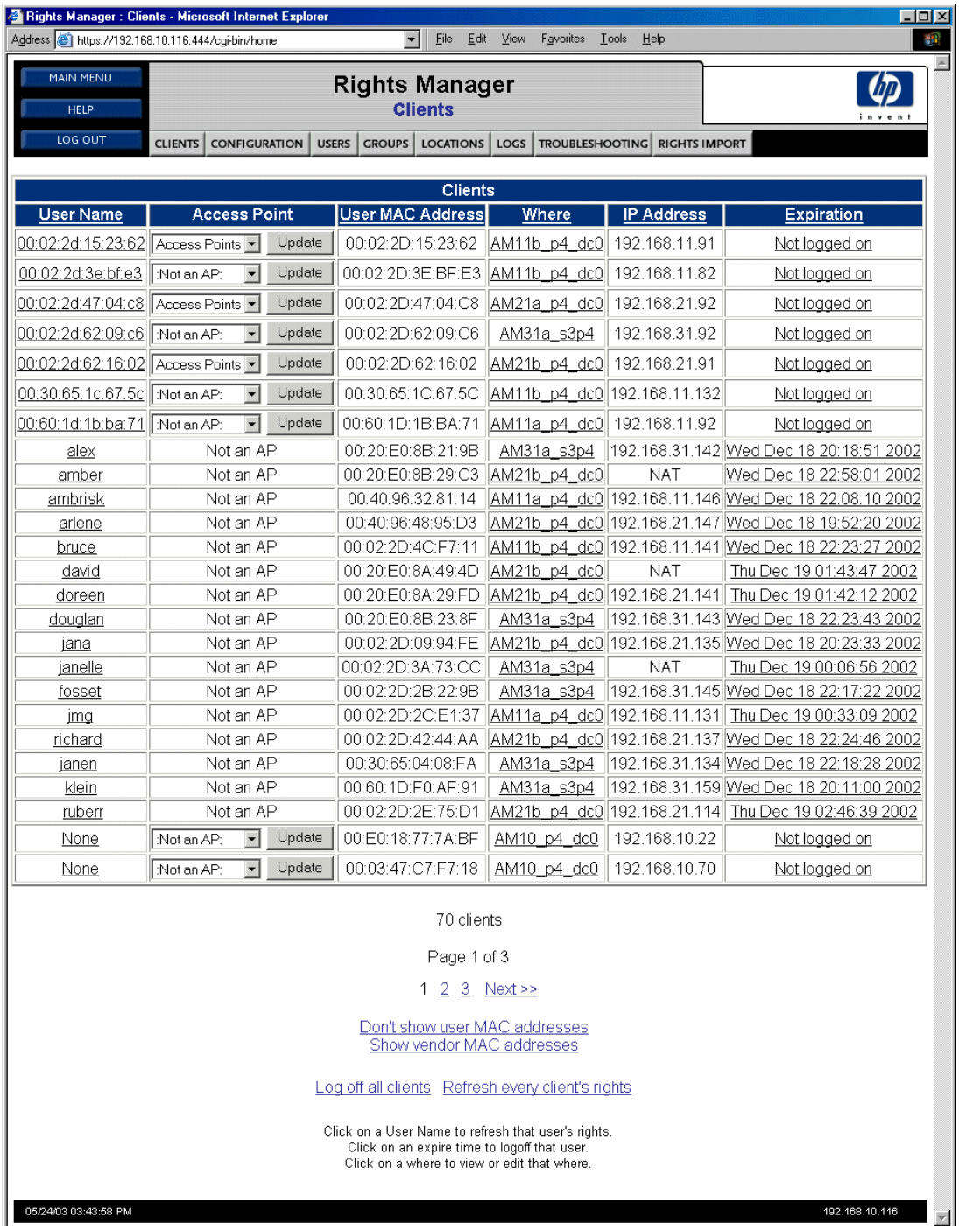

Figure 6-5. Rights Manager Clients page

Note: *Depending on your browser, you may be required to logon to the Rights Manager user interface separately from the Administrative Interface. If this is the case, you will be presented with the Rights Manager Administrator Login page. Use the same Administrator username and password that you used to access the Integrated Access Manager or Access Control Server Administrative interface. Typically, with*

Microsoft's Internet Explorer, you can access both the Administrative Interface and the Rights Manager with a single login, but with the Netscape browser you may need to log in separately to each.

The buttons across the top of the page let you access the main functional areas of the Rights Manager. These functions are:

- **CLIENTS**—displays the clients currently logged on through the 700wl Series system, as shown in Figure 6-5. This also functions as the initial display when you bring up the Rights Manager. This is discussed below in this section.
- **CONFIGURATION**—includes configuration options for authentication and various other global configuration options such as DNS/WINS rights, Rights Manager logging setup, HTTP Proxy setup, and selected security options.

  The authentication functions are described in detail in Chapter 9. The other configuration options are described in Chapter 12.
- **USERS**—provides options for adding users to the built-in database, either for purposes of authentication, or just to associate users with groups. This also enables the creation of Registered Guest, MAC Address, and Access Point users.
- **GROUPS**—provides options for creating groups and configuring group options, defining Allows and Redirects, and defining Whens. These are discussed in detail in Chapter 7.
- **LOCATIONS**—provides options for defining locations and configuring location options, Wheres, and Whens. These are discussed in detail in Chapter 8.
- **LOGS**—displays the Rights Manager log file.
- **TROUBLESHOOTING**—provides options for verifying and troubleshooting authentication service configurations (for LDAP, RADIUS, or XML-RPC-based services) as well as verifying and troubleshooting user rights.
- **RIGHTS IMPORT**—provides options for exporting and saving the current rights configuration and the XML Rights schema, and importing a saved set of rights. You can use this feature to export rights from one Rights Manager and import them to the Rights Manager on a different Integrated Access Manager or Access Control Server.

Logging Out of the Rights Manager

If you log out directly from the Rights Manager rather than returning to the Administrative Interface Main Menu, the Rights Manager logout page is displayed. Depending on your browser, this may or may not also log you out of the Access Control Server or Integrated Access Manager Administrative Interface. Generally, if you had to log in separately to the Rights Manager, then logging out of the Rights Manager does *not* log you out of the Access Control Server or Integrated Access Manager Administrative Interface.

Typically, Microsoft's Internet Explorer logs you out of both the Rights Manager and the Administrative Interface with a single logout, regardless of where you are when you do the logout. In this case, the Main Menu button on the Rights Manager logout page will take you to the Administrative Interface Login page.

If your browser logs you out of the Rights Manager only when you click the Rights Manager Logout button, then the Main Menu button returns you to the Access Control Server or Integrated Access Manager Main Menu. The Netscape browser typically works this way.

The Rights Manager Clients Page

The Rights Manager Clients page, as shown in Figure 6-5, shows the following for each client connected to the 700wl Series system:

- User Name—The user logon name. This will be NONE if the client is a MAC Address user.
- Access Point— Indicates whether the client is an Access Point or some other type of client.
- Where—The "Where" through which the client is attached to the network.
- IP Address—The client's IP Address if NAT is not used for this client. If NAT applies to this client, this column will display "NAT."
- Expiration—The date and time that the client's rights expire, or NEVER if they do not expire, or Not Logged On if the client is connected but not logged on.

The number of active clients is displayed immediately below the table. If the Clients table has more than 25 entries, clients are shown in sets of 25 clients at a time. In this case, the page includes an indicator of which page you are viewing, and provides links to navigate between the pages of the display.

From the Clients display you can do the following:

- Click the user name to refresh that user's rights. This reloads the user's current set of rights from the Rights Manager.
- Click the Expiration time for the client to logoff that client.
- Click the **Show user MAC addresses** link at the bottom of the page to display the MAC Addresses column. When MAC addresses are displayed this link changes to **Don't show user MAC addresses**.
- Click the **Show vendor MAC Addresses** link at the bottom of the page to change the MAC address display to show the vendor name/ID instead of the first three tuples of the MAC address. This link appears only while user MAC addresses are displayed. When vendor MAC addresses are displayed, this link changes to **Don't show vendor MAC addresses**. Clicking this link restores the user MAC address format.
- Click **Refresh every client's rights** to refresh the rights for all clients.
- Click **Log off all clients** to log off *all* clients.

Note: *Under certain circumstances clients may be left in the Clients list even though they are no longer connected to the system. In order to remove these non-existent clients from the Clients list you must log them off twice to completely remove them from the list.*

Setting Up MAC Address Users and Access Points

For all clients that either use a MAC address as their User Name, or do not have a User Name known to the Rights Manager, the Access Point Column displays a pull down field you can use to specify that a client is an Access Point. Figure 6-6 shows this field.

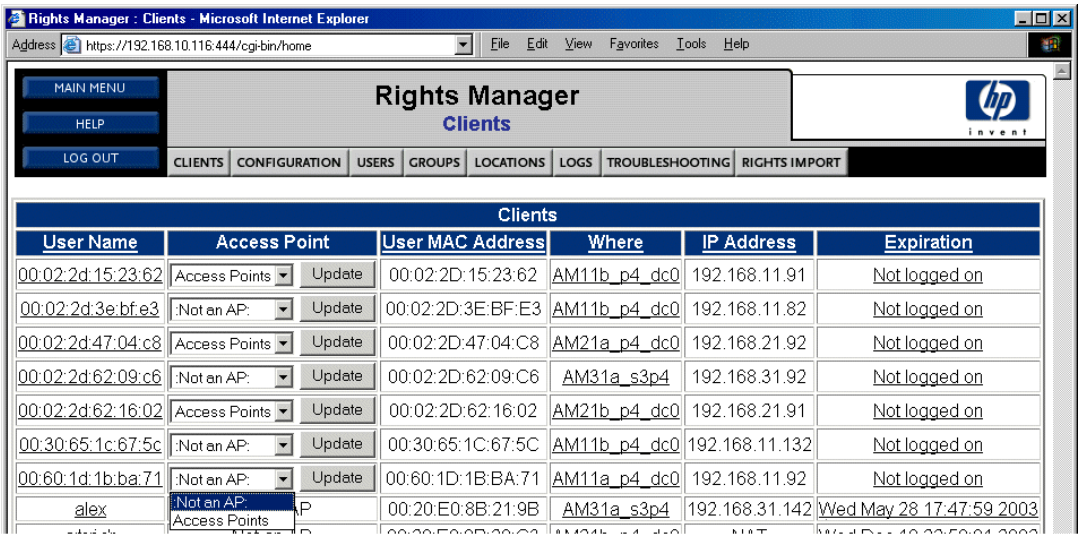

Figure 6-6. Clients page showing Access Point settings

To specify that a client is actually an Access Point:

Step 1. Select **Access Point** from the drop-down field associated with the client

Step 2. Click **Update**.

The Access Point MAC address is added to the built-in database and the predefined Access Point group.

You can also add a non-Access Point MAC address to the built-in database through this view by leaving the selection at **Not an AP** and clicking **Update**. This adds the MAC address to the built-in database but does not associate it with any group.

CONFIGURING GROUPS 7

This chapter explains how to configure Groups for use in the HP ProCurve Secure Access 700wl Series Rights Manager. It includes the following sections:

Defining Groups 7-1

Viewing Groups—the Groups Manager 7-4

Adding or Modifying a Group—the Group Editor 7-8

Adding or Modifying a When—the When Editor 7-21

Defining Redirect Rights—the Redirect Editor 7-23

Defining Allow Rights—the Allow Editor 7-27

Example—Modifying Rights for the Guest Group 7-30

This chapter assumes you have read Chapter 6, “Getting Started with the Rights Manager”. You should thoroughly understand the concepts explained there before you begin to configure groups and access rights for those groups.

Defining Groups

A group defines a set of rights that will be granted to any client who is a member of the group. The group construct allows you to define rights for multiple clients in a single operation, rather than for each client individually.

From the moment a client is detected through an Access Controller port, that client is associated with a group for the purpose of determining what rights it should be granted. Initially, most clients are members of the Logon group, which provides the rights necessary for a user to log in and be authenticated. Depending on the results of the authentication, the client will then be associated with one or more groups that define the access rights given to that user. If the implicit Users group is allowed at a location, all authenticated clients that have connected through that location are automatically members of that Users group (unless the group specifically disallows it) in addition to any other allowed groups to which they may belong.

Certain client types—those whose MAC addresses are recognized by the Access Controller—can be identified as belonging to a specific group without being required to authenticate. These clients are automatically be granted the rights appropriate to the groups to which they belong. This feature is typically used to identify and grant rights to Access Points or other devices that do not provide authentication information.

You can create as many groups as you want in order to implement your access control policies. If you want to give an individual user a unique set of rights, you can create a group that has that user as its only member.

While group properties determine the access rights a user is granted, properties associated with the user's Location (where he/she accesses the system) may interact with group properties to further limit a user's access. See Chapter 6, "Getting Started with the Rights Manager" for a more detailed explanation of the roles groups and locations play in the 700wl Series system.

The Properties of a Group

A group defines a number of important properties that affect a member user's access to the network through the 700wl Series system. These properties include:

- The group type, which determines the class of rights and other options that are associated with members of the group. The standard types are defined in Table 7-1 below.
- The times (time of day, days of the week, and so on) when these rights are in effect (the "Whens"). A ***When*** is a named time specification that is defined independently of a group, so you can define a time specification once and then use it for multiple groups.
- Redirect rights, which defines how destinations get redirected to alternate destinations for members of this group.
- Allow rights, which specify the destinations to which traffic will be forwarded for a group member.
- A number of other options, such as how IP addresses are assigned to the client, how long a session can continue without re-authenticating, whether traffic from members of the group should be given a VLAN ID (802.1Q tag), and so on.

You can add new groups, modify an existing group's properties, or delete groups.

The Rights Manager provides the following standard group types:

Table 7-1. Group Types

Group Type	Description
Normal	Defines a set of rights granted to a client who has logged in as an authenticated user, and is associated with the specific group. Normal groups are user defined, there are no groups of this type by default. This is one of the three group types to which you can add users.
Guest	Defines the rights granted to a client who logs on as a guest, or who is added to the Built-in database as a Registered Guest user. There is one predefined Guest group provided by default in the Rights Manager. **Note:** By default, this group does not allow any network access. You *must modify the rights for this group to allow access as appropriate for your site.* Users are automatically members of this group when they log in as a Guest, or if they are in the built-in database as a Registered Guest.

Table 7-1. Group Types

Group Type	Description
Logon	Defines the rights granted to a client who has not yet logged in. There is one predefined Logon group provided by default in the Rights Manager. Users are members of this group when they have connected but not yet logged in.
Implicit Users	Defines the default set of rights granted to a client who has logged in as an authenticated user, in addition to any rights granted due to membership in other groups. There is one predefined Implicit Users group, named “Users,” provided by default in the Rights Manager.
Access Point	Defines a set of rights granted to a client that is actually an access point (identified by a MAC address). There is one Access Point group provided by default in the Rights Manager. This is one of the three group types to which you can add users, but only Access Point users can be added as members of this group.
Stop	Defines a set of rights that prevents a client who has logged in as an authenticated user from accessing anything on the network. There is one predefined Stop group, named “No Access,” provided by default. This is one of the three group types to which you can add users.

Note: *Normal groups, Stop groups, and Access Point groups are the only groups to which you, as the administrator, can add members. Membership in the Access Point group is restricted to clients that are Access Point users. Membership in the other group types is determined implicitly by the Rights Manager based on whether and how the user has logged on and been authenticated.*

How Group Rights (Allows and Redirects) are Processed

Allows and ***Redirects*** are simply traffic filters: a Redirect filters for traffic meeting its definition, and redirects it to a new destination, while an Allow simply forwards traffic that meets its definition. Redirects for a group are processed first, in alphabetical order by the name of the Redirect. Any traffic that has not been redirected is then processed by the Allow filters, also in alphabetical order. Traffic that has not been redirected and is not allowed is dropped.

If a user/client is concurrently a member of multiple groups, then the rights from those groups are merged and the user is granted the combined set of rights. The Redirect and Allow filters are then applied to the client traffic in the same way as for a single group—the merged set of Redirects are applied first, in alphabetical order, then the Allows are applied.

Because Allow and Redirect filters are applied based on the alphabetical order of their names, their naming is important. You can determine the order in which Redirects or Allows will be applied by looking at the Groups Manager displays of Allows and Redirects. The Allows and Redirects are displayed in alphabetical order from left to right, so enabled filters are applied in the order in which they appear in the table.

For example, suppose you have created a set of filters that allows only selected IP traffic, and you have named them “IP 1”, “IP 2”, and so on, and these work as expected for your group. However, you then add this group as an allowed group for a location that also allows the default Implicit User group. The Implicit User group, by default, has “All IP” enabled, and all

authenticated users are automatically members of the default User group. Now, when users log in to this location, they receive the User group rights merged with your group's rights, and the "All IP" Allow from the User group is applied before your more restrictive IP filters. The result is that your filters are ignored and the users in your group have full IP access. To avoid this you can either not allow the Implicit User group at the location, or you can give your Allows names that will cause them to be processed before the All IP Allow—such as "AA IP 1", "AA IP 2", and so on.

Automatic HTTP Proxy Interaction with Group Access Rights

If you enable the Automatic HTTP Proxy feature for a group, then all HTTP requests are handled through the HTTP proxy mechanism. This means that any Allows or Redirects you may have defined for HTTP traffic will have no effect, because HTTP traffic is redirected to the proxy function. Instead, the HTTP proxy filters you define for the group determine how HTTP traffic is handled. By default, for all groups except the Access Point and Stop type groups (No Access) the Auto HTTP proxy function *accepts all* HTTP traffic. The default Auto HTTP proxy filter settings for Access Point and Stop-type groups (including the predefined No Access group) deny all HTTP traffic. Automatic HTTP proxying is disabled by default.

Viewing Groups—the Groups Manager

The Groups Manager page provides an overview of all the groups currently defined in the Rights Manager, showing the Allow or Redirect rights for each group. From this page you can enable or disable Allows (or Redirects) for one or more groups. You can also access the Group Editor, the Allow Editor, or the Redirect Editor from this page to create or modify a Group, Allow, or Redirect.

To access the Groups page, do the following:

Step 1. From within the Rights Manager, click **GROUPS**.

The Groups Manager page appears, as shown in Figure 7-1

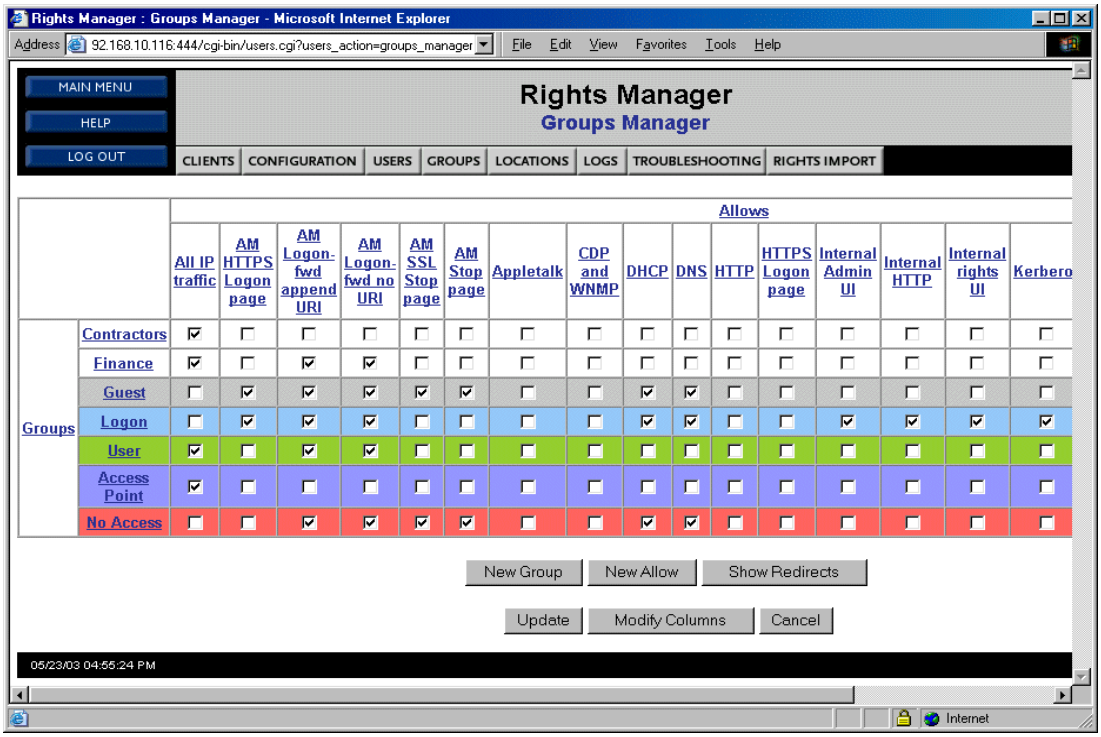

Figure 7-1. Groups Manager page, initial view

The Groups Manager page displays all the current groups in a column at the left of the display. Groups are ordered by type, with each type indicated by the color of the row. The colors are defined in Table 7-2.

Table 7-2. Group Background Color Codes

Color	Meaning
White	Normal groups—groups that define rights for authenticated users that are members of the group
Grey	Guest groups—groups that define rights for guest users
Blue	Logon groups—groups that define rights for users that have not been authenticated
Green	Implicit User groups—groups that define a default set of rights for authenticated users
Violet	Access Point groups—groups that define rights for access points
Light Red	Stop groups—groups that define rights that prevent network access

The columns in the table can show either Allows or Redirects. By default the columns show all Allows currently defined in the Rights Manager. Figure 7-1 shows the Groups Manager with Allows displayed.

» To display Redirects instead of Allows, click the **Show Redirects** button.

While Redirects are displayed, the button is relabeled **Show Allows**.

The check boxes in the table cells show which Allows or Redirects are enabled for each group. You can change the assignment of Allows or Redirects in one of two ways:

- Click the check box in the appropriate table cell to turn an Allow or Redirect on or off for the group
- Add or remove Allows or Redirects for the group using the Group Editor

The buttons at the bottom center of the page have the functions as described in Table 7-3.

Note: *If you have a large number of columns (or columns that are very wide due to long Allow or Redirect names) these buttons may appear off the page to the right. You can scroll the page horizontally to reach them.*

Table 7-3. Groups Manager button functions

Button	Function
New Group	Displays the Group Editor. See “Adding or Modifying a Group—the Group Editor”.
New Allow/New Redirect	Displays the Allow Editor or the Redirect Editor. The button is labeled to reflect the current column display. See “Defining Redirect Rights—the Redirect Editor” or “Defining Allow Rights—the Allow Editor”.
Show Redirects/Show Allows	Switches the columns to display Allows or Redirects. The button label reflects the hidden rights type.
Update	Updates all Groups to include the selected allows or redirects.
Modify Columns	Displays the Group/Allow Column Modifier page, or the Group/Redirect Column Modifier page. “Modifying the Columns in the Groups Manager”.
Cancel	Cancels any pending changes you have made to the table since the last Update.

Selecting Allows or Redirects in the Groups Manager

You can add rights to a group or remove rights from a group by checking or unchecking the checkbox in the table cell that is the intersection of the Allow or Redirect column with the row for the group.

Step 1. Specify which Allows or Redirects should be added or removed:

- To add an Allow or Redirect, click to turn the checkbox on.
- To remove an Allow or Redirect, click to turn the checkbox off.

Note: *Allows and Redirect filters are shown in alphabetical order, left to right. This also reflects the order in which they are applied—in alphabetical order based on the Allow or Redirect name. Redirects are applied first, then Allows.*

Step 2. Click **Update** to have your selections take effect. This also redisplays the main Rights Manager page (the Clients display).

- To cancel your proposed changes, click **Cancel**. This displays the Rights Manager main page without saving your changes.

Note: *If you change views, such as changing the column display from Allows to Redirects or navigating to another page before you click Update, all pending changes are lost. Also, to avoid having to navigate repeatedly between the Groups Manager and the Rights Manager main page, you should specify all your changes of the same type before you click Update, rather than doing an Update after each one.*

Modifying the Columns in the Groups Manager

You can modify the Group Allows Columns or the Group Redirects Columns so that you see only a subset of the Allows or Redirects defined in the Rights Manager.

To change which Allows or Redirects appear in the Groups Manager, do the following:

Step 1. On the Groups Manager page, make sure the table shows the columns you want to modify (Allows or Redirects).

Click **Show Redirects** or **Show Allows** to display the correct columns, if necessary.

Step 2. From the Groups Manager page click **Modify Columns**.

The appropriate Group Column Modifier page appears. Figure 7-2 shows the Group / Allow Column Modifier page. The Group / Redirect Column Modifier page looks similar.

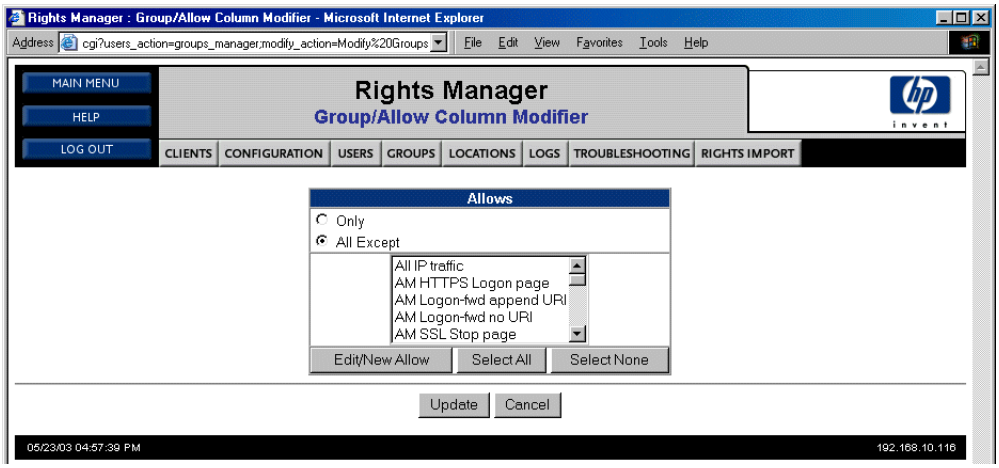

Figure 7-2. Modifying columns in the Groups Allow display

Step 3. Use the Column Modifier page to include or exclude display of Allows or Redirects in the Groups Manager.

To select the columns to display, choose one of the following options:

- To select individual Allows (or Redirects) to display in the Groups Manager table, click **Only** and then select the Allows or Redirects that you want to include in the table.
- To select multiple items in the list, press and hold the CTRL key while you select items with the left mouse button.

- To select individual Allows (or Redirects) that should not be displayed in the Groups Manager table, click **All Except** and then select the Allows or Redirects that you want to exclude from the table.
- To Add a new Allow or Redirect, or to modify an existing Allow or Redirect, click **Edit/New Allow** or **Edit/New Redirect**.

  See “Defining Redirect Rights—the Redirect Editor” and “Defining Allow Rights—the Allow Editor” for more information.
- Click **Select All** to select all items in the list, or **Select None** to select no items in the list.

Step 4. When you are done, click **Update**. The Groups Manager page appears showing only the columns you have selected.

Adding or Modifying a Group—the Group Editor

To create a new group, or modify an existing group, do the following:

Step 1. From the Groups page, click **Edit/New Group** or click the group name shown in the Group Name column.

The Group Editor page appears. The top portion of the page is shown in Figure 7-3.

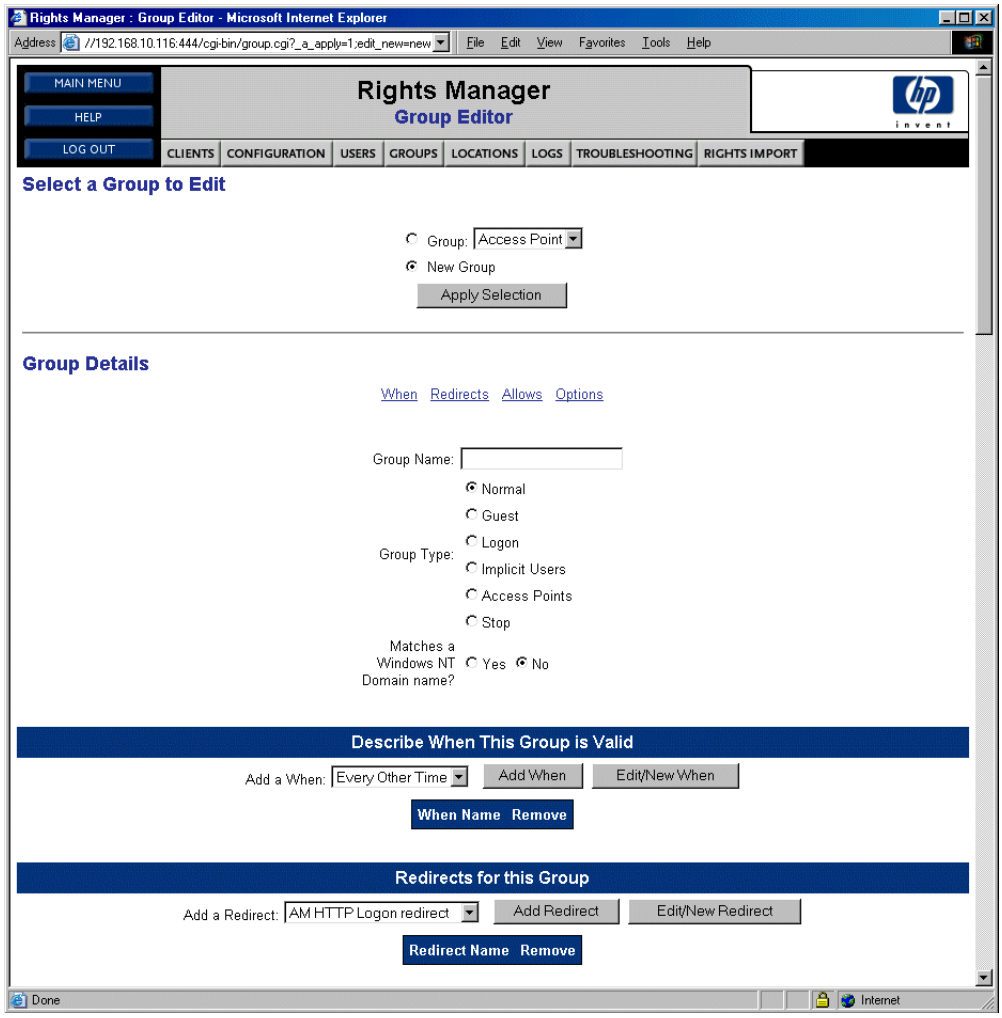

Figure 7-3. Group Editor, top portion of page

Select a Group to Edit

Step 2. To create a new group, select **New Group**.

To modify the settings for an existing group, select **Group**, then highlight the group you want to modify from the drop-down list.

Step 3. Click **Apply Selection**.

If you've selected an existing group, that group's properties appear in the fields below. Otherwise, the fields are blank or are set to their default values

Group Details

Step 4. For a new group, enter a group name. The name is already filled in for an existing group.

Note: *If you want this to define rights for users of an NT Domain, who are authenticated using NT Domain login, the group name must match the name of the Domain to which these users belong.*

Step 5. Check the appropriate Group Type.

If you are creating a group that you plan to use for specific users (either by assigning them explicitly or by getting group membership information from an external authentication source) you should select **Normal** as the type. See Table 7-1 for a definition of the group types.

Step 6. If you are going to use NT Domain logon, and want this group to define the rights for users who are authenticated in that manner, check **Yes**.

In this case, the name of the Group must match the name of the Domain of which these users are members.

Describe When this Group is Valid

The table in this section lists the Whens that define the times during which the rights associated with this group are valid. A When is simply a named time specification. Whens allow you to create a time specification once and then use it with multiple groups, rather than having to specify it individually for every group.

You can specify multiple Whens to define the valid times for the group. The valid times are taken as the sum of all the Whens specified for the group. The table lists each When, its description, and a checkbox that allows you to remove it from this group.

Note: *If you don't specify any whens, the valid time defaults to 24 hours a day, seven days a week.*

Step 7. To add an existing When to this group, highlight the When in the drop-down list, and click **Add When**.

Step 8. To create a new When and add it to the list, click **Edit/New When**.

For details of creating a When, see "Adding or Modifying a When—the When Editor" on page 7-21.

Step 9. To remove a When from the list, check the appropriate box in the Remove column.

Redirects for this Group

The table in this section lists the Redirects that have been associated with this group. A redirect specifies that packets intended for a specified destination should be redirected by the Access Controller to a different destination. Typically, the rights for a group will include a number of Redirects. A number of common Redirects are predefined in the 700wl Series system.

Step 10. To add an existing Redirect to this group, highlight the Redirect in the drop-down list, and click **Add Redirect**.

Table 7-4 shows the redirects that are predefined in the 700wl Series system.

Step 11. To create a new Redirect and add it to the list, click **Add New Redirect**. This takes you to the Redirect Editor.

For details of creating a Redirect, see "Defining Redirect Rights—the Redirect Editor" on page 7-23.

Step 12. To remove a Redirect from the list, check the appropriate box in the Remove column.

Table 7-4. Predefined Redirects

Redirect	Description
AM HTTP Logon redirect	Redirects most HTTP requests (on port 80) to the Access Controller logon page on port 82. Web requests to address `42.0.0.1` are not redirected so the system can be configured on startup. *Use this if distributed logons are implemented.*
AM HTTPS Logon redirect	Redirects most HTTPS requests on port 443, the standard SSL port, to the Access Controller SSL logon page on port 443. *Use this if distributed logons are implemented.*
AM Internal blocker	Redirects HTTP requests intended for addresses within the Access Control Server subnet (`@INTRANET@`) to the Access Controller Stop page. *Use this if distributed logons are implemented.*
AM Logon page shortcut	Redirects HTTP requests intended for 1.1.1.1 port 80 to the Access Controller logon page. *Use this if distributed logons are implemented.*
AM No SSL Web	Redirects all HTTPS requests on port 443, the standard SSL port, to the Access Controller SSL Stop page. *Use this if distributed logons are implemented.*
AM No Web	Redirects all HTTP requests on port 80 to the Access Controller Stop page. *Use this if distributed logons are implemented.*
Blackhole	Redirects all requests except for DHCP, DNS, Stop page and HTTP requests to 0.0.0.0. This effectively prevents network access.
CS-to-AM Logon redirect	Redirects requests intended for the Access Control Server SSL logon port (443) to the Access Controller SSL logon port. This redirect is needed to allow the Access Controller logon process to use the Access Control Server's SSL certificate. *Use this if distributed logons are implemented.*
CS-to-AM Stop redirect	Redirects requests intended for the Access Control Server Stop port (81) to the Access Controller Stop port. This redirect is needed to allow Stop page redirects to succeed when Distributed Logons are in use. *Use this if distributed logons are implemented.*
No external rights UI	Redirects Rights Manager UI access requests to the SSL Stop page.
No internal admin UI	Redirects Administrative Interface access requests via `42.0.0.1 @INTERNAL@`) to the Access Control Server SSL Stop page.
No internal rights UI	Redirects Rights Manager UI access requests via `42.0.0.1` (`@INTERNAL@`) to the Stop page.

Table 7-4. Predefined Redirects (Continued)

Redirect	Description
No SSL internal UI	Redirects SSL Administrative Interface access requests via `42.0.0.1` (`@INTERNAL@`) to the Stop page.
SOCKS redirect	Redirects all SOCKS requests to the Access Controller.
The following Redirects are intended for use only with centralized logon, and should not be used with an HP ProCurve Secure Access 700wl Series system.	
HTTP logon redirect	Redirects most web requests (on port 80) to the Access Control Server logon page on port 82. Web requests to address `42.0.0.1` are not redirected so the system can be configured on startup. *Use this only if centralized logons are implemented.*
HTTPS logon redirect	Redirects most web requests on port 443, the standard SSL port, to the Access Control Server SSL logon page on port 443. *Use this only if centralized logons are implemented.*
Internal blocker	Redirects HTTP requests intended for addresses within the Access Control Server subnet (`@INTRANET@`) to the Access Control Server Stop page. *Use this only if centralized logons are implemented.*
Logon page shortcut	Redirects web requests intended for 1.1.1.1 port 80 to the Access Controller logon page. *Use this only if centralized logons are implemented.*
No SSL Web	Redirects all HTTPS requests on port 443, the standard SSL port, to the Access Control Server SSL Stop page. *Use this only if centralized logons are implemented.*
No Web	Redirects all HTTP requests on port 80 to the Access Control Server Stop page. *Use this only if centralized logons are implemented.*

Caution: *If you create your own Logon, Guest, User, or Stop groups, you must ensure that you use the correct Redirects based on whether your system is configured for centralized logon or distributed (Access Controller-based) logon. See "Allows and Redirects for Distributed Logons" for more information on the Redirects (and Allows) that are affected.*

The remaining sections of the Group Editor page are shown in Figure 7-4.

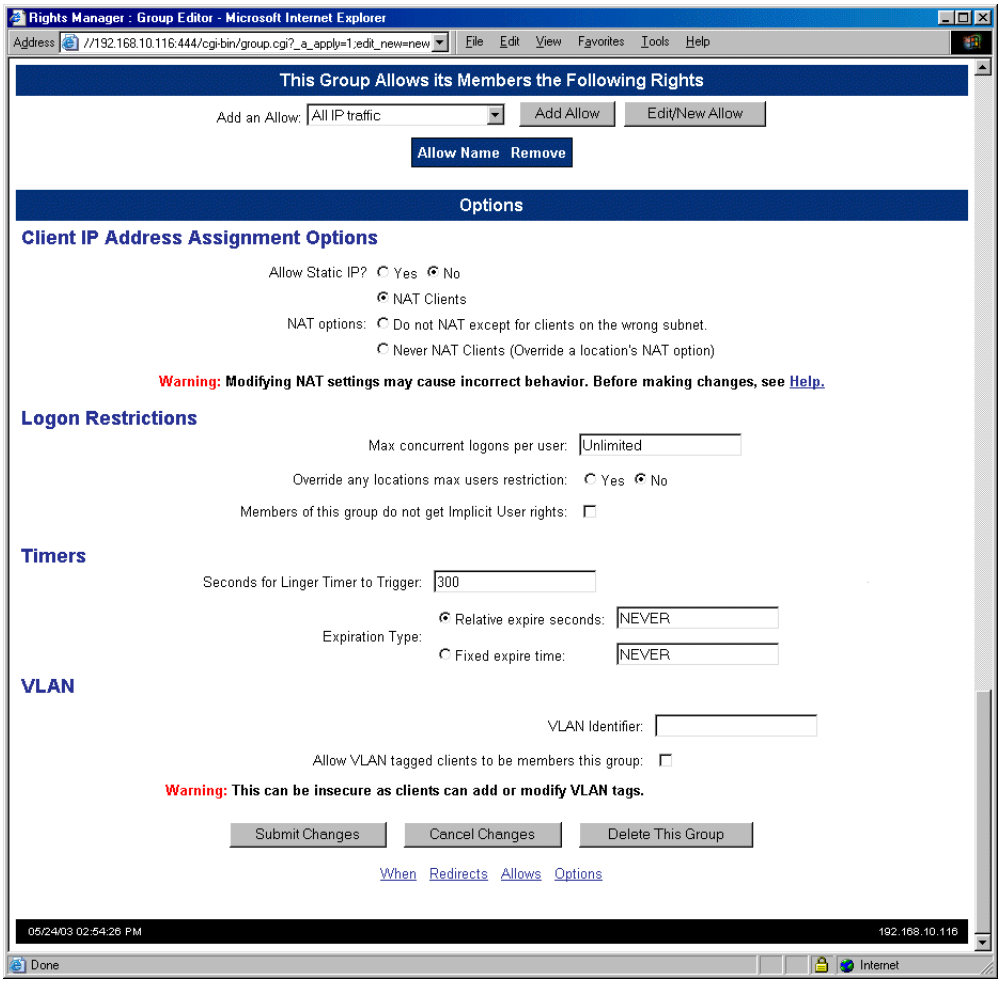

Figure 7-4. Group Editor, bottom portion of page

This Group Allows its Members the Following Rights

An Allow specifies that packets intended for a specified destination may be forwarded by the Access Controller to that destination. Typically, the rights for a group will include a number of Allows. Packets that are not allowed via an Allow (or redirected via a Redirect) are dropped.

Caution: *If you have enabled the Automatic HTTP Proxy feature for this group, then HTTP traffic will not be affected by the Allows and Redirect rights you set for this group. Instead, you must provide proxy filters to permit or deny HTTP traffic. By default, if you do not set any HTTP proxy filter, all HTTP traffic is permitted. See "Automatic HTTP Proxy Configuration" on page 11-9 for details.*

Table 7-5 defines the predefined Allows available in the 700wl Series system.

Step 13. To add an existing Allow to this group, highlight the Allow in the drop-down list, and click **Add Allow**.

You can also add an existing Allow to a group by clicking the checkbox in the appropriate cell in the display shown on the Groups Manager page.

Step 14. To create a new Allow and add it to the list, click **Edit/New Allow**. This takes you to the Allow Editor.

For details of creating an Allow, see "Defining Allow Rights—the Allow Editor" on page 7-27.

Step 15. To remove an Allow from the list, check the appropriate box in the Remove column.

Table 7-5. Predefined Allows

Rights	Description
All IP Traffic	Allows all IP packets to be forwarded
AM HTTPS Logon page	Allows access to Access Controller SSL logon page via `42.0.0.1` *Use this if distributed logons are implemented.*
AM Logon-fwd append URI	Allows requests to port 82 (Access Controller logon page), which preserves the original destination URL *Use this if distributed logons are implemented.*
AM Logon-forward no URI	Allows requests to port 83 (Access Controller logon page), which does not preserve the original destination URL *Use this if distributed logons are implemented.*
AM SSL Stop page	Allows requests to the Access Controller SSL Stop page *Use this if distributed logons are implemented.*
AM Stop page	Allows requests to the Access Controller Stop page *Use this if distributed logons are implemented.*
AppleTalk	Allows packets using the AppleTalk protocol to be forwarded
CDP and WNMP	Allows packets using the Cisco Discovery Protocol or Wireless Network Management Protocol
DHCP	Allows DHCP requests. Required by Logon and Guest groups so that clients DHCP requests are properly handled
DNS	Allows DNS requests
HTTP	Allows HTTP requests to port 80
Internal Admin UI	Allows access to the Access Controller Administrative UI pages
Internal HTTP	Allows HTTP requests to port 80 on the Access Controller defined in `@INTERNAL@` (by default `42.0.0.1`)
Internal rights UI	Allows access to the Rights Manager pages via the Access Controller defined in `@INTERNAL@` (by default `42.0.0.1`)
Kerberos	Allows packets on UDP port 88 to be forwarded
Outside World	Allows packets to be forwarded anywhere except the network defined in `@INTRANET@` (the Access Control Server's subnet)
Ping	Allows PING requests
SMB	Allows the user to access to the netbios ports 137, 138, and 139

Table 7-5. Predefined Allows (Continued)

Rights	Description
The following Allows are intended for use only with centralized logon, and should not be used with an HP ProCurve Secure Access 700wl Series system.	
HTTPS Logon page	Allows access to the Access Control Server SSL logon page on port 443 *Use this only if centralized logons are implemented.*
SSL Stop Page	Allows access to the SSL Stop page (port 446) *Use this only if centralized logons are implemented.*
Stop Page	Allows access to the Stop page (port 81) *Use this only if centralized logons are implemented.*

Caution: *If you create your own Logon, Guest, User, or Stop groups, you must ensure that you use the correct Allows based on whether your system is configured for centralized logon or distributed (Access Controller-based) logon. See "Allows and Redirects for Distributed Logons" for more information on the Allows (and Redirects) that are affected.*

Options

Step 16. Set **Client IP Address Assignment options**. These options, along with options set at the Location, determine whether the IP address of a client can be reassigned using Network Address Translation (NAT).

Note: *Before you change a group's NAT settings, you should read and understand the discussion in "Network Address Translation in the 700wl Series System", in Chapter 6, "Getting Started with the Rights Manager". Specifically, for most groups you should not use the* **Never NAT** *setting. The exception is the Access Point group, which uses the* **Never NAT** *setting. To allow clients to use real IP addresses rather than NAT'ed addresses, use the* **Do Not NAT except...** *setting.*

The group NAT settings interact with the settings from the location as explained below.

a. To allow a static IP address to be used for clients that are member of this group, click **Yes** for **Allow Static IP**. To require a dynamic IP address, click **No**.

If you allow Static IP addresses, you cannot use the **NAT Clients** setting. If these are regular clients, you should use the **No NAT except...** setting.

b. Select one of the NAT options:

Select **NAT Clients** to have the 700wl Series system use NAT addresses for clients in all circumstances.

Select **No NAT except for clients on the wrong subnet** to specify that a regular IP address (static or obtained via DHCP) should be used unless the client is on the wrong subnet (which may indicate that the client is misconfigured). The ***wrong*** subnet is defined as follows:

— If an IP address range is defined (via the Advanced Network Configuration

page) for the Access Controller port through which the client is connected, then the client address will be NAT'ed if it falls outside this range.

— If no address range is defined for the port, then the client address will be NAT'ed if it falls outside the subnet defined for the Access Controller (on the Access Controller's Network Configuration page).

The **No NAT except...** setting is recommended if you do not want your clients to receive NAT addresses under normal conditions.

Note: *You must uncheck the location NAT setting in order to have the* **No NAT except...** *option be effective. If NAT is selected for the location, then this option is ignored, and NAT is used.*

The **Never NAT** option forces the Access Controller to always use the actual IP address presented by the client, regardless of whether it appears to be a valid address or not. This setting is intended for use by the Access Point group, or by groups whose members are network infrastructure devices, such as switches or hubs. It should not be used for regular clients—the **No NAT except...** setting should be used in that case.

This setting overrides the **Require NAT** setting on the location page.

Caution: *If you choose to use the* **Never NAT** *setting, ALL groups of which the client might become a member due to authentication, time, or location (roaming) transitions MUST also use the* **Never NAT** *setting.*
For example, if the Logon group allows NAT, then a client will receive an IP address in the NAT address range (by default `42.x.x.x`*) when it connects. If, after authentication, it transitions into a group with* **Never NAT** *set, the Access Controller will take the* `42.x.x.x` *address as the real IP address and the client will no longer be reachable by return traffic.*

Note: *If you inspect the XML rights for a client, the* **NAT Clients** *setting appears as "Do NAT," and the* **Do Not NAT except...** *setting appears as "Can NAT" meaning that NAT is allowed under the appropriate circumstances. The* **Never NAT** *setting appears, as expected, as "Never NAT."*

Step 17. Set **Logon Restrictions**. These options define logon restrictions for members of this group. They interact with (and may override) logon restrictions set by the location.

a. To limit the number of times a given user can be logged on concurrently, enter a number into the **Max concurrent logons per user** field. The default is **UNLIMITED**.

b. To override a location's restriction on the maximum number of users permitted to logon, select **Yes** for **Override any locations max users restriction?**

c. To prevent group members from getting the rights associated with the Implicit Users group, even if that group is allowed at a location, check the **Members of this group do not get Implicit User rights** checkbox.

Normally, if an Implicit Users group is allowed at a location, then all user that authenticate through that location automatically get the rights granted by the Implicit Users group, in addition to the rights they may receive through groups of which they are members.

Step 18. Set values for Linger and Expiration Timers.

The ***Linger timer*** specifies how long a client / user will remain known by the Rights Manager after being disassociated from the Access Controller for failing to respond to repeated probes. This allows a roaming client to disappear temporarily as it moves between access points, without losing its rights.

The ***Expire Timers*** let you specify how long a user's rights should remain valid after that user has been authenticated. When his rights expire the user must re-authenticate to continue to have access. There are two types of Expire timers: the Relative expire timer and a Fixed expire time.

The ***Relative expire*** lets you specify a length of time, in seconds, after which the user will be required to re-authenticate. The ***Fixed Expire*** time lets you specify a time of day (for example, midnight) after which the user is required to authenticate.

a. To change the Linger timer, enter the number of seconds into the **Seconds for Linger Timer to Trigger** field. The default is 300 seconds.

b. To set a Relative expire timer, enter the number of seconds into the **Relative expire seconds** field. The default is **NEVER**—these rights do not expire.

c. To set a Fixed expire time, enter the time into the **Fixed expire time** field, in the format HH:MM:SS, for example 23:59:59. The default is **NEVER**.

Note: *An Expire timer (Fixed or Relative) interacts with the valid times for the group, as defined by the group's Whens, such that whichever ends first causes the user's rights to expire. So, if the valid time for the group ends, the user's rights are terminated, even if his expire timer has not yet run out.*

Step 19. Set a VLAN Identifier (802.1Q tag) to be associated with this group.

If a VLAN ID is specified for this group, packets transmitted from this group will be tagged with the specified VLAN ID before they are transmitted on into the network.

When you specify the VLAN ID for a group, make sure that it matches the appropriate VLAN ID as defined in your network.

Note: *A VLAN ID associated with a group overrides a VLAN ID associated with a location. If the client is concurrently a member of multiple groups with different VLAN IDs, the lowest-numbered VLAN ID is used.*

Step 20. You can use a pre-existing VLAN tag to identify clients that should be given membership in this group: check **Allow VLAN tagged clients to be members of this group** to specify that clients that transmit packets tagged with the specified ID should be considered members of this group. They will be then granted the rights associated with the group.

Caution: *Allowing the VLAN tag to determine group membership is a feature that should be used with care, as it may compromise your network's security. It is possible for a client to add a tag or modify the tag associated with the traffic it transmits, which could result in the client being granted rights to which it is not entitled.*

Step 21. When you are done click **Submit Changes.**

Table 7-6 Summarizes the properties you can set for a group.

Table 7-6. Group Editor Properties

Property	Explanation
Group Details:	
Group Name	The name of a group you want to create, modify, or delete.
Group Type	The group type, which primarily determines how users become members of the group. See Table 7-1 for a definition of the types.
Matches a Windows NT group name?	Indicates that this group should match an NT Domain name when NT Domain logon authentication is used.
Describe When This Group is Valid:	
Add a When:	Displays a list of Whens currently specified for this group, and lets you select from a list of existing Whens, or create a new When. See "Adding or Modifying a When—the When Editor" for details on creating a When.
Redirects for this Group:	
Add a Redirect:	Displays a list of Redirects currently specified for this group, and lets you select from a list of existing Redirects, or create a new Redirect. See "Defining Redirect Rights—the Redirect Editor" for details on creating a Redirect.
This Group Allows its Members the Following Rights:	
Add an Allow:	Displays a list of Allows currently specified for this group, and lets you select from a list of existing Allows, or create a new Allow. See "Defining Allow Rights—the Allow Editor" for details on creating an Allow.
Client IP Address Options:	
Allow Static IP?	Specifies whether static IP addresses are allowed. If NAT is required (the "NAT Clients" setting is selected) this must be set to "No".
NAT Clients	Specifies that NAT should always be used to replace the client IP address
No NAT except for clients on the wrong subnet	Specifies that client IP addresses should not be NAT'ed, unless the client's IP address is not in the correct subnet. If the location NAT setting specifies NAT, that overrides this group setting.
Never NAT Clients	Never use a NAT IP address for clients in this group. This overrides the location NAT setting if the location normally specifies NAT. In this case, the client's IP address will be used as the source IP address in all packets, regardless of whether it is valid (in the correct subnet).
Max concurrent logons per user	The maximum number of logons each user can have; the default is UNLIMITED.
Override any location's max user restrictions	Whether members of this group can override the maximum number of users permitted at a location.
Members of this group do not get Implicit User rights	Specifies that members of this group should not also get Implicit User rights, even if those rights are allowed by the location.
Seconds for Linger Time to Trigger	How long to wait before logging off after the client disassociates. The default is 300.

Table 7-6. Group Editor Properties

Property	Explanation
Relative expire seconds	How long these rights remain in effect, once established. User must then reauthenticate to restore rights.
Fixed Expire Time:	A specific time at which these rights cease to be in effect. User must then reauthenticate to restore rights.
VLAN Identifier	An 802.1Q VLAN tag to be added to packets originating from members of this group.
Allow VLAN tagged clients to be members of this group.	Specifies that any client that transmits tagged frames matching this VLAN tag should be considered a member of this group.

Allows and Redirects for Distributed Logons

There are several logon-related allows and redirects that are different depending on whether logons are distributed (handled by the Access Controllers) or are centralized (handled on the Access Control Server). The 700wl Series system by default distributes logon processing among the Access Controllers associated with the Access Control Server.

Becasue the 700wl Series system uses distributed logons, any groups you create that should have logon rights, or that redirect traffic to a Stop page, must use the "AM" versions of the relevant allows and redirects. You should not use the non-AM versions.

Table 7-7 and Table 7-8 show the appropriate versions of the allows and redirects for distributed or centralized logon.

Note: *If any of the Logon-related allows or redirects are included in a group, the two allows "AM Logon-fwd append URI" and "AM Logon-fwd no URI," and the "CS-to-AM Logon redirect" must also be included in the group.*

Table 7-7. Allow Mapping for Distributed vs. Centralized Logon

Allows for Distributed Logon	Allows for Centralized Logon (Should Not be Used)
AM HTTPS Logon page	HTTPS Logon page
AM SSL Stop page	SSL Stop Page
AM Stop page	Stop page
AM Logon-fwd append URI	—
AM Logon-fwd no URI	—

Table 7-8. Redirect Mapping for Distributed vs. Centralized Logon

Redirects for Distributed Logon	Redirects for Centralized Logon (Should Not be Used)
AM HTTP Logon redirect	HTTP Logon redirect
AM HTTPS Logon redirect	HTTPS Logon redirect

Table 7-8. Redirect Mapping for Distributed vs. Centralized Logon

Redirects for Distributed Logon	Redirects for Centralized Logon (Should Not be Used)
AM Internal blocker	Internal blocker
AM Logon page shortcut	Logon page shortcut
AM No SSL Web	No SSL Web
AM No Web	No Web
CS-to-AM Logon redirect	—
CS-to-AM Stop redirect	—

Deleting a Group

To delete a group:

Step 1. From the Groups page, click **Edit/New Group** or click the group name shown in the Group Name column.

The Group Editor page appears.

Step 2. In the Group Editor, if the group you want to delete is not already selected, select the group from the drop-down list in the Groups field, and click **Apply Selection**.

Information about the Group you want to delete should appear in the Group Details section of the page.

Step 3. Scroll to the bottom of the page and click **Delete This Group**.

A warning page appears that requires you to confirm that you really want to delete this group.

Step 4. To proceed to delete this group, click **Yes**. To cancel, click **No**.

The Group Editor page reappears with a confirmation message displayed.

Setting Up Groups for Student Access Rights

The XML-RPC authentication mechanism provides a way for an educational institution to use it's existing student and class schedule database for user authentication and the assignment of client access rights. This system both authenticates the student and obtains the student's schedule, and returns to the 700wl Series system a "student profile" that supplies a list of classes or other relevant activities / categories along with starting and ending times for these classes / activities.

If you plan to use XML-RPC to request authentication and retrieve student profiles from an external XML-RPC service, you must create groups that correspond to all the classes and activities for which you want to define specific, unique sets of access rights. You configure these groups with the access rights that should be granted to members of the group.

For example, given the class Biology 101, you could create a group named "Biology101" and define a set of rights that enable access to a web site that contains the laboratory exercises and support materials used during the class. Students in certain classes at the law school or

medical school might be granted access rights to specialty databases such as Lexis / Nexis or Medline.

You do not necessarily need to set up Whens for these groups. Instead, the start and stop time associated with the group in the user's profile is used to define when that group's rights are valid for that particular student. The group's Whens will be used only if no start and stop time is included in the user profile. The benefit of handling the valid times in this manner is that even if the times for a class change (from semester to semester, for example) you do not need to modify the group configurations in the Rights Manager—the new time frame can just be reflected in the students' schedules, which are sent to the Rights Manager through the student profiles.

You may also want to define a default set of rights that apply to students whenever they are logged on to the network but are not in a specific class or activity. You can set up a group specifically for this purpose (for example the "NotInClass" group) or you can use the default Implicit Users group for this purpose. Whichever you choose, however, if you want the rights associated with this group to be valid *only* when the student is *not* receiving rights from another group, you must assign this group the "EveryOtherTime" When. This When specifies that the group's rights are valid only when no other set of rights are valid.

If you want the default rights to be valid at all times, including when other group rights are in effect, then you can leave the Whens blank. The absence of a When is taken to mean "all the time" (24 hours a day, 7 days a week).

Adding or Modifying a When—the When Editor

A ***When*** is a named definition of a time frame that can be associated with a group or a location. Whens are used to specify the times during which the rights associated with a group are valid, or when users can log in through a location.

The When Editor can be accessed from the Group Editor or from the Location Editor.

To create a When for use with a group or location, do the following:

Step 1. From the Group Editor or Location Editor, click the **When** link or scroll down until you reach the section labeled **Describe When This Group is Valid** or **Describe When This Location is Valid**.

The **Edit/New When** button is at the top of this section.

Step 2. Click **Edit/New When**.

The When Editor appears as shown in Figure 7-5.

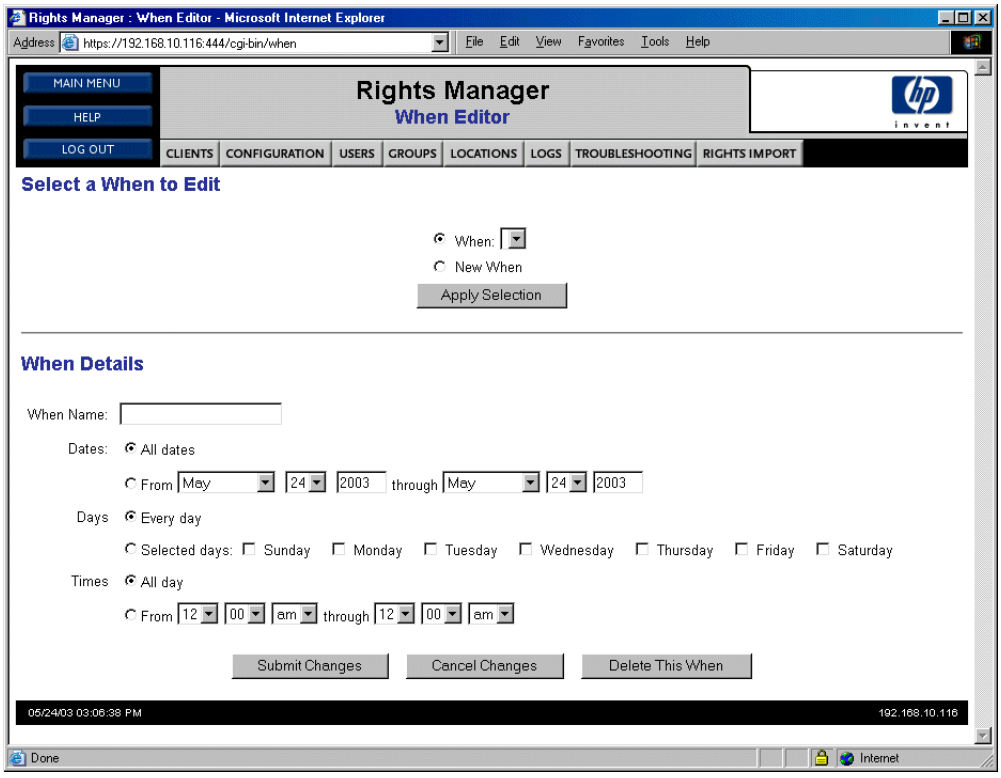

Figure 7-5. When Editor

Step 3. To create a new When, select **New When**.

To modify the settings for an existing When, select **When**, then highlight the When you want to modify from the drop-down list.

Step 4. Click **Apply Selection**.

If you have selected an existing When, that When's properties appear in the fields below. Otherwise, the fields are blank or are set to their default values

Step 5. For a new When, type a name in the **When Name** field. The name is already filled in for an existing when.

Step 6. Choose the days and times that the group has access.

a. You can choose **All dates** (the default) or click **From** and enter a specific range of dates using the drop-down selection lists.

b. You can choose **Every Day** (the default), or click **Selected Days** and check the individual days you want to include.

c. You can choose **All Day** (the default) or click **From** and select the starting and ending times from the drop-down selection lists.

Step 7. Click **Submit Changes** to have these changes take effect. A confirmation that your changes have been submitted is displayed.

If you have not yet submitted your changes, you can click **Cancel Changes** to undo your changes.

Defining Redirect Rights—the Redirect Editor

Redirects are traffic filters that identify packets sent from a client that should be redirected to a new destination Some redirects may simply forward the packet to an alternate destination that performs the same function as the original destination—for example, a DNS server request could be redirected to the enterprise DNS server rather than the one that was originally specified. Redirects can also be used to prevent traffic from reaching a prohibited destination—in this case, the redirect may instead send the request to the 700wl Series system Stop page.

The Rights Manager provides a number of predefined Redirects, and through the Groups Manager page, you can select and deselect the Redirect rights that will be granted to members of a group. Table 7-4 on page 7-11 lists the predefined Redirects provided by the Rights Manager.

You can define an Redirect in one of two ways.

- A ***Basic Redirect Filter*** lets you specify a Redirect by selecting the protocol, and providing a destination IP address and port, if appropriate. The predefined Redirects are all examples of Basic Redirect Filters.
- An ***Advanced Redirect Filter*** lets you specify a filter in `tcpdump` syntax. This enables you to define complex filters. None of the predefined Redirect filters are Advanced Redirect filters.

If you create your own Redirects, their naming is important, as it affects the order in which the filters are applied. If the order makes a difference, take care to name your filters so that they will be processed in the correct order.

Adding or Modifying a Redirect

You can access the Redirect Editor either from the Groups page, as described in the steps below, or from the Group Editor, which displays an **Edit/New Redirect** button in the Redirects for this Group section of the page.

From the Groups page, do the following:

Step 1. Make sure that the Redirects column is displayed. Click **Yes** for **Show Redirects Column** if necessary.

Step 2. Click the specific Redirect that you want to modify.

The Redirect Editor appears. Figure 7-6 shows the top portion of the page.

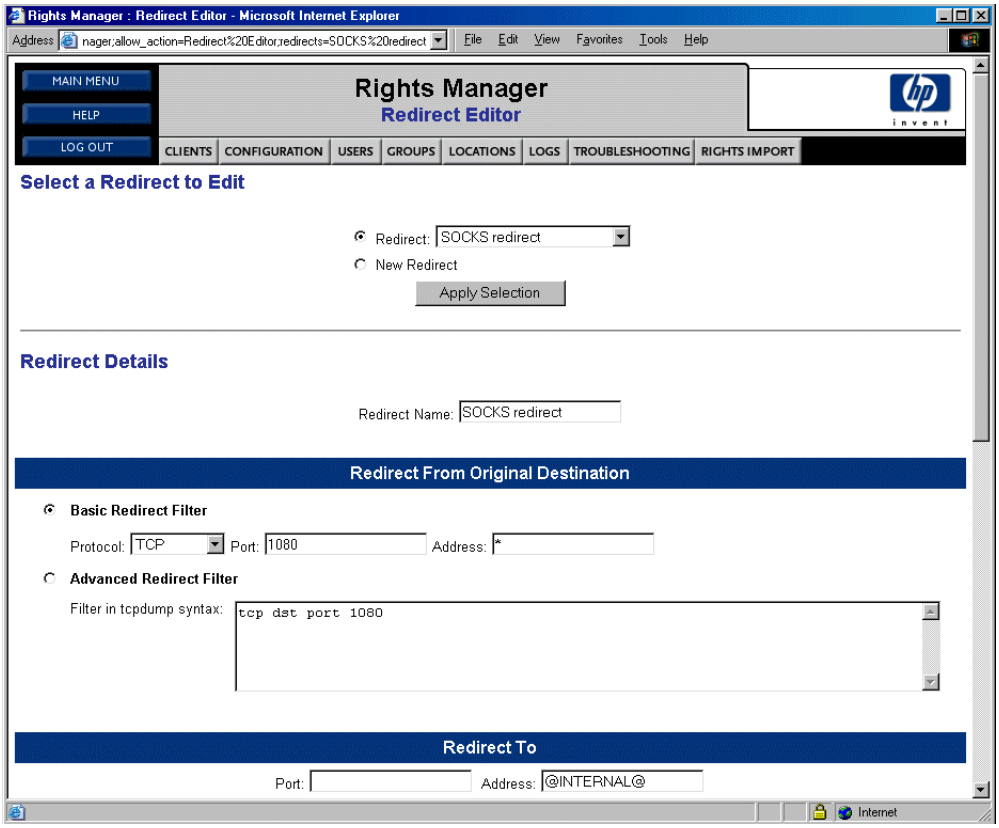

Figure 7-6. Redirect Editor, top portion of page

Step 3. To create a new Redirect, select **New Redirect**.

To modify the settings for an existing group, select **Redirect**, then highlight the Redirect you want to modify from the drop-down list. If you clicked a Redirect from the Groups Manager, it should already be selected.

Step 4. Click **Apply Selection**.

If you've selected an existing Redirect, that Redirect's properties appear in the fields below. Otherwise, the fields are blank or are set to their default values

Redirect Details

Step 5. For a new Redirect, enter a Redirect name. When selecting a name, remember that Redirects are processed in alphabetical order based on their names.

The name is already filled in for an existing Redirect.

Step 6. To specify a Redirect by protocol, address and port, select **Basic Redirect Filter**, then do the following:

a. Select the protocol of the traffic you want to Redirect from the drop-down list in the **Protocol** field.

b. If the protocol requires a destination port, type it into the **Port** field. If the protocol does not support port specifications, **N/A** appears in the port field. You can enter a single port, or use an asterisk (*) to specify all ports.

c. If you want to specify a destination IP address, type it in the **Address** field. The address field can be:

— A single IP address

— A network address (IP address plus netmask)

— An asterisk (*) for any IP address

— A built-in or user-defined Address variable

An address can be preceded by a "`!`" or "**`not`**" to negate the address.

The built-in address variables are shown in the Addresses and Port Descriptors area at the bottom of the Redirect Editor page. The built-in addresses are defined based on the network parameters you entered when you configured your Integrated Access Manager or Access Control Server. You can also create your own address variables. See "Addresses and Port Descriptions" below for more information.

Step 7. To specify a `tcpdump` expression as a Redirect filter, select **Advanced Redirect** and type the appropriate expression into the text box. See Appendix A, "Filter Expression Syntax" for details of the `tcpdump` syntax.

Note:€ `tcpdump` *syntax is case sensitive. All keywords must be in lower-case to be recognized.*

Step 8. In the **Redirect To** section, type the port and IP Address that the packet should be redirected to.

The built-in port list in the bottom section of this page displays the ports for some common destinations, such as the Stop pages or the Logon pages. The built-in addresses list provides the list of built-in addresses.

For example, to redirect packets to the Stop page, you would specify port 81 at address `@SERVER@` (the Access Control Server).

Step 9. To add the Redirect, or to replace the current Redirect, go to the end of the page and click **Submit Changes**.

Addresses and Port Descriptions

The lower portion of the Redirect Editor (Figure 7-7) displays lists of the Address variables currently defined in the Rights Manager, and the Built-in ports used by the Rights Manager. The top table displays any user-defined address variables. The second table shows the built-in addresses, and the bottom table displays the built-in port numbers.

Address variables begin and end with an @. There are four built-in addresses, and six built-in ports. The four built-in addresses are:

- `@DNS@`— the address of the primary DNS server
- `@INTERNAL@`—the internal address of the Access Controller Administrative Interface.

- @INTRANET@—the network address of the subnet on which your Access Control Server or Integrated Access Manager resides.
- @SERVER@—the IP address of your Integrated Access Manager or Access Control Server.

The built-in addresses are used in a number of the predefined Allows.

The built-in ports cannot be modified. Three of the built-in addresses can only be modified by changing the network configuration of your 700wl Series system via the Network Configuration page from the Administrative Interface Main Menu. The exception is the @INTRANET@ address, which you can change by entering it as if it were a user variable.

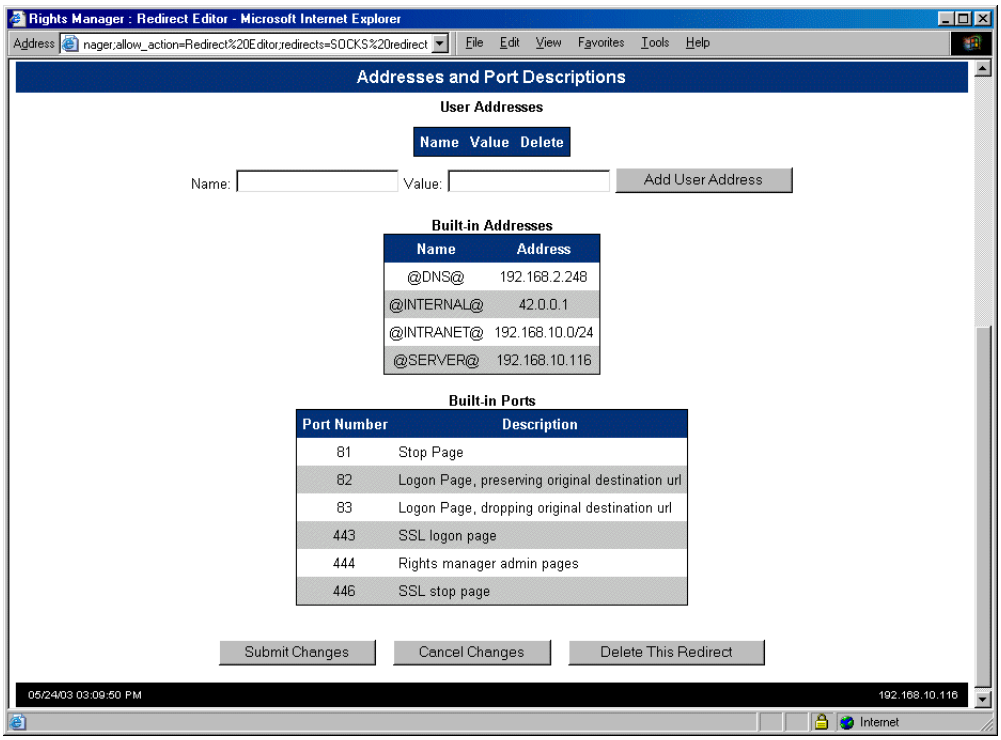

Figure 7-7. Redirect Editor, Addresses and Port Descriptions section

You can add your own address variables:

Step 1. Type a name for your variable in the **Name** field. Do not include the @ characters; the Rights Manager adds these automatically.

Step 2. Type the IP address in the **Value** field.

Step 3. Click **Add User Address**. Your new address variable appears in the Users Addresses table at the top of the Addresses and Port Descriptions section. You can then use the variable as the destination address in a Basic Allow, or include it in a tcpdump expression.

Deleting a Redirect

To delete a Redirect, do the following:

Step 1. From the Groups page, click the Redirect you want to delete.

From the Group Editor, in the **Redirects for the Group** section, click **New/Edit Redirect**.

The Redirect Editor appears, as shown in Figure 7-6.

Step 2. Select **Redirect**, then highlight the Redirect you want to delete from the drop-down list. If you clicked a specific Redirect from the Groups Manager, it should already be selected.

Step 3. Click **Apply Selection**.

That Redirect's properties appear in the fields below. Otherwise, the fields are blank or are set to their default values

Step 4. Go to the bottom of the page and click **Delete this Redirect**. The Redirect Editor displays a confirmation message, as shown in Figure 7-8.

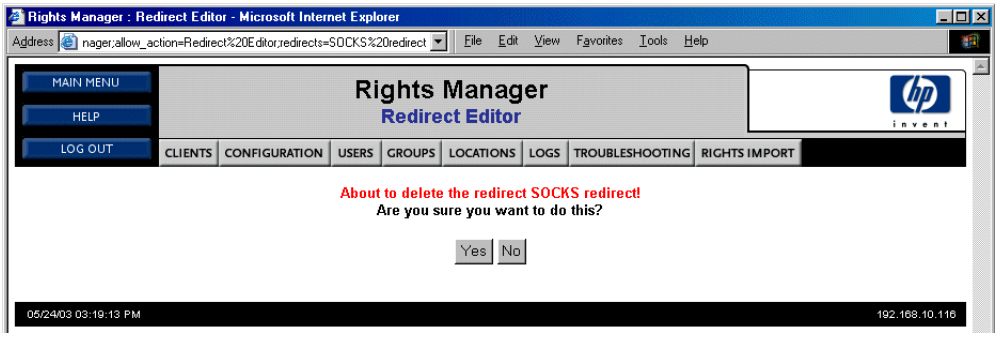

Figure 7-8. Redirect Editor Delete Confirmation page

Step 5. If you want to delete the Redirect, click **Yes**. Otherwise click **No**.

Defining Allow Rights—the Allow Editor

Allows are traffic filters that identify packets that are permitted to be forwarded by an Access Controller 720wl. The Rights Manager provides a number of predefined Allows, and through the Groups Manager page, you can select and deselect the Allows that will be granted to members of a group. Table 7-5 on page 7-14 lists the predefined allows provided by the Rights Manager.

If the predefined Allows are not sufficient for your needs, you can define additional Allows, or modify the existing Allows.

You can define an Allow in one of two ways.

- A ***Basic Allow*** lets you specify an allow by selecting the traffic protocol, and providing a destination IP address and port, if appropriate. Many of the predefined Allows, such as DHCP, HTTP, and All IP, are Basic Allows.
- An ***Advanced Allow*** lets you specify a traffic filter in `tcpdump` syntax. This enables you to define complex filters. The predefined Appletalk Allow is an example of an Advanced Allow.

If you create your own Allows, their naming is important, as it affects the order in which the filters are applied. If the order makes a difference, take care to name your filters so that they will be processed in the correct order.

Adding or Modifying an Allow

You can access the Allow Editor either from the Groups Manager page, as described in the steps below, or from the Group Editor, which displays an **Edit/New Allow** button in the Allows for this Group section of the page.

From the Groups page, do the following:

Step 1. Make sure that the Allows column is displayed. Click **Yes** for **Show Allows Column** if necessary.

Step 2. Click the specific Allow that you want to modify.

The Allow Editor appears. Figure 7-9 shows the top portion of the page.

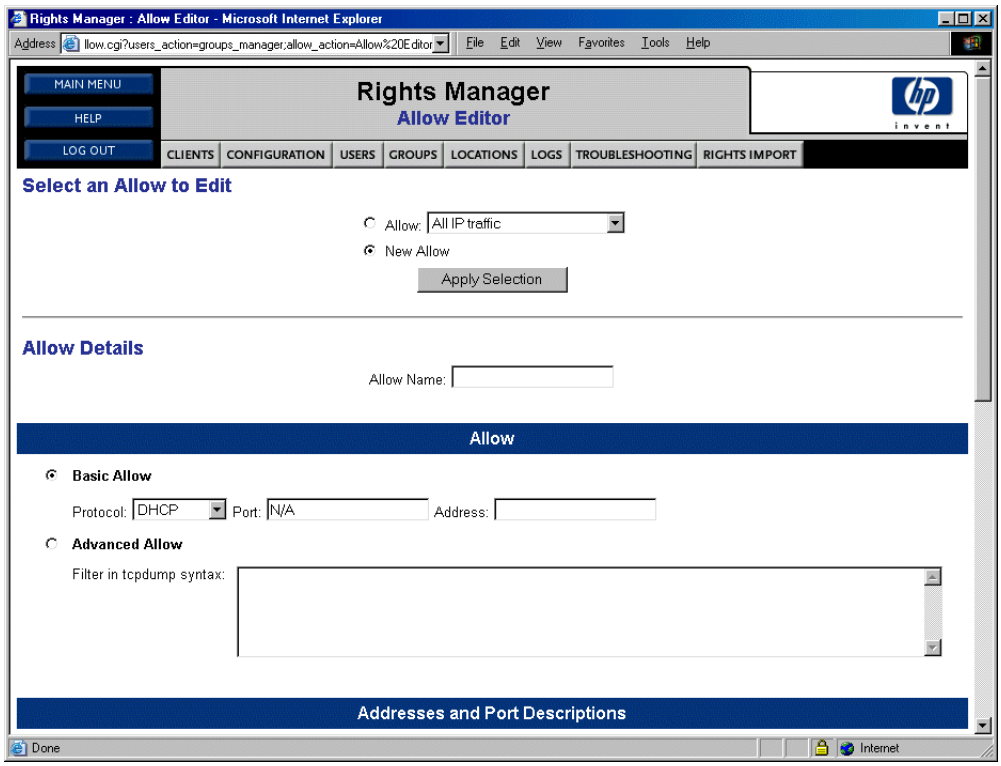

Figure 7-9. Allow Editor, top portion of page

Step 3. To create a new Allow, select **New Allow**.

To modify the settings for an existing group, select **Allow**, then highlight the Allow you want to modify from the drop-down list. If you clicked an Allow from the Groups Manager, it should already be selected.

Step 4. Click **Apply Selection**.

If you've selected an existing Allow, that Allow's properties appear in the fields below. Otherwise, the fields are blank or are set to their default values

Allow Details

Step 5. For a new Allow, enter an Allow name. When selecting a name, remember that Allows are processed in alphabetical order based on their names.

The name is already filled in for an existing Allow.

Step 6. To specify an Allow by protocol, address and port, select **Basic Allow**, then do the following:

a. Select the protocol of the traffic you want to allow from the drop-down list in the **Protocol** field.

b. If the protocol requires a destination port, type it into the **Port** field. If the protocol does not support port specifications, **N/A** appears in the port field. You can enter a single port, or use an asterisk (*) to specify all ports.

c. If you want to specify a destination IP address, type it in the **Address** field. The address field can be:

— A single IP address

— A network address (IP address plus netmask)

— An asterisk (*) for any IP address

— A built-in or user-defined Address variable

An address can be preceded by a "**!**" or "**not**" to negate the address.

The built-in address variables are shown in the Addresses and Port Descriptors area at the bottom of the Allow Editor page. The built-in addresses are defined based on the network parameters you entered when you configured your Integrated Access Manager or Access Control Server. You can also create your own address variables. See "Addresses and Port Descriptions" on page 7-25 for more information.

Step 7. To specify a `tcpdump` expression as an Allow filter, select **Advanced Allow** and type the appropriate expression into the text box. See Appendix A, "Filter Expression Syntax" for details of the `tcpdump` syntax.

Note: `tcpdump` *syntax is case sensitive. All keywords must be in lower-case to be recognized.*

Step 8. To add the Allow, or to replace the current Allow, go to the end of the page and click **Submit Changes**.

The lower portion of the Allow Editor displays lists of the Address variables currently defined in the Rights Manager, and the Built-in ports used by the Rights Manager. The top table displays any user-defined address variables. The second table shows the built-in addresses, and the bottom table displays the built-in port numbers. Address variables begin and end with an `@`. There are four built-in addresses, and six built-in ports.

This section is identical to the Addresses and Port Descriptions section of the Redirect Editor page. See "Addresses and Port Descriptions" on page 7-25 for a detailed description of these tables, and for instructions on adding user-defined address variables.

Deleting an Allow

To delete a Allow, do the following:

Step 1. From the Groups Manager, click the Allow you want to delete.

From the Group Editor, in the Allows for the Group section, click **New/Edit Allow**.

The Allow Editor appears, as shown in Figure 7-9.

Step 2. Select **Allow**, then highlight the Allow you want to delete from the drop-down list. If you clicked a specific Allow from the Groups Manager, it should already be selected.

Step 3. Click **Apply Selection**.

That Allow's properties appear in the fields below. Otherwise, the fields are blank or are set to their default values

Step 4. Go to the bottom of the page and click **Delete this Allow**. The Allow Editor displays a confirmation message, as shown in Figure 7-10.

Figure 7-10. Allow Editor Delete Confirmation page

Step 5. If you want to delete the Allow, click **Yes**. Otherwise click **No**.

Example—Modifying Rights for the Guest Group

By default the predefined Guest group includes only the Allows and Redirects that enable a Guest to log onto the system. Once logged on, a Guest has no access rights to any part of the network. If you want to allow Guest users to have access to selected parts of your network, or to the Internet, you need to modify the Guest Group access rights.

Enabling an Existing Allow—Outside World

The simplest way to modify a group's access rights is to enable or disable an existing Allow or Redirect for the group. Enabling or disabling an existing Allow or Redirect can be done from the Groups Manager page.

For example, the predefined Outside World Allow will pass client traffic to any network address except addresses within the Access Control Server's subnet. (The Access Control Server's subnet is defined by the IP address and subnet mask entered on the Access Control Server Network Configuration page, and is kept as the `@INTRANET@` built-in address.)

Enabling the Outside World allow for the Guest group means that any user that logs in as Guest will be able to access all network addresses except for those within the Access Control Server subnet.

To enable the Outside World allow for the Guest Group, do the following:

Step 1. From anywhere in the Rights Manager, click **GROUPS**.

The Groups Manager page appears.

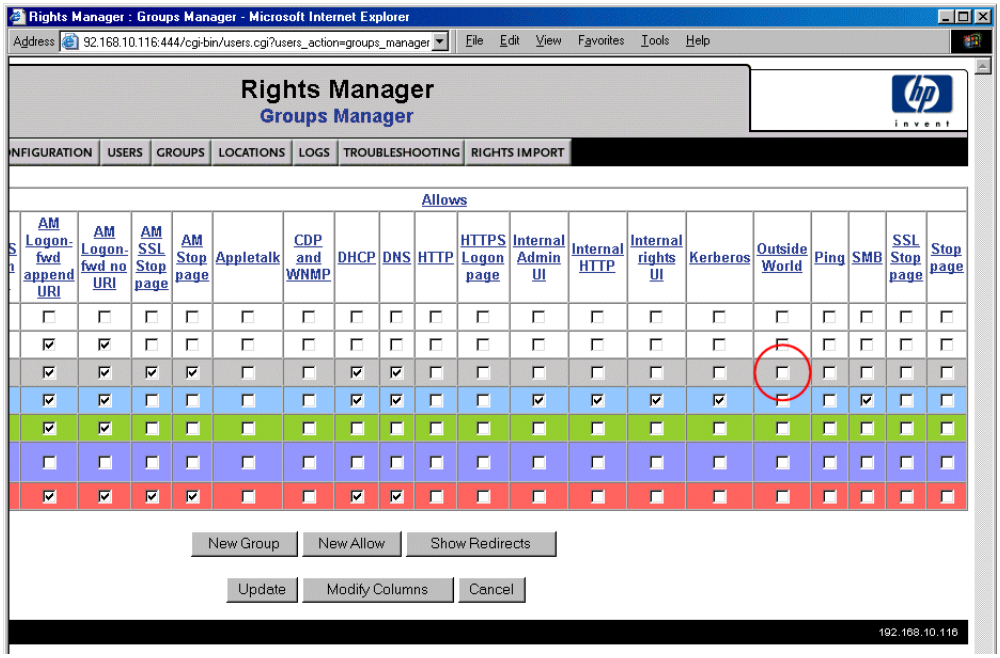

Figure 7-11. Adding the Outside World Allow to the Guest group from the Groups Manager page

Step 2. Find the column for the Outside World Allow, as shown in Figure 7-11, and click the checkbox in the Guest group row (the grey row) to turn the Allow on.

Step 3. Click **Update** to have this change take effect.

Creating a New Allow for Restricted Access

If the Outside World Allow is not sufficiently restrictive for your network environment, you can create a new allow (or modify the Outside World Allow) to restrict access to multiple subnets or IP addresses.

Step 1. From the Groups Manager table, click the Outside World Allow.

The Allow Editor appears.

Step 2. To create a new Allow, select **New Allow**. To modify the Outside World Allow, leave it selected.

Step 3. Click **Apply Selection**.

Step 4. For a new Allow, enter an Allow name. When selecting a name, remember that Allows are processed in alphabetical order based on their names.

Step 5. Select a protocol from the drop-down list in the **Protocol** field (the default is IP).

If the protocol requires a destination port, type it into the **Port** field. If the protocol does not support port specifications, **N/A** appears in the port field. You can enter a single port, or use an asterisk (*) to specify all ports.

Step 6. If you want to specify a single destination IP address or address range, type it in the **Address** field. You can also create an address variable and use it here. The address can be preceded by a "**!**" or "**not**" to negate the address.

Step 7. To specify a more complicated address filter, you can enter a `tcpdump` expression. Select **Advanced Allow** and type the appropriate expression into the text box.

For example, to allow all traffic except to subnets 10.0.0.0/8 and 20.0.0.0/8, you could enter the `tcpdump` string:

```
(not dst net 10.0.0.0/8) and (not dst net 20.0.0.0/8)
```

See Appendix A, "Filter Expression Syntax" for details of the `tcpdump` syntax.

Note: `tcpdump` *syntax is case sensitive. All keywords must be in lower-case to be recognized.*

Step 8. To add the Allow, or to replace the current Allow, go to the bottom of the page and click **Submit Changes**.

Once you have created your new Allow, you must enable the Allow for your group. When you return to the Groups Manager page, your new allow should appear as a new column in the Allows table. You can then enable it for the Guest group by checking the box in the Guest group row for the new Allow, and clicking **Update**.

SETTING UP LOCATIONS 8

This chapter explains how to configure the Rights Manager for the 700wl Series system. It includes the following sections:

Defining Locations 8-1

The Locations Manager 8-2

Adding or Modifying a Location—the Location Editor 8-5

Adding or Modifying a Where—the Where Editor 8-10

Adding or Modifying an Access Controller 8-12

Defining Locations

A Location is a set of Wheres and some set of additional properties such as Whens, allowed groups, and a few other settings. A location has the following properties:

- A list of Wheres that define the Access Controllers, ports, or specific clients that are associated with this location. Every location must include at least one Where.
- A list of the times (time of day, days of the week, and so on) when access through this location is available, specified as a list of Whens
- A list of groups that are allowed at this location. This determines which users can gain access to the system through this location
- Whether Network Address Translation (NAT) is required for clients entering through this location
- The maximum number of users allowed to connect through this location at one time
- A VLAN ID (802.1Q tag) if VLAN tagging is to be implemented by location

In addition, a location defines whether Wireless Data Privacy logon is allowed, whether encryption is allowed or required, which protocols are supported, and how authentication is done. These properties, however, are set through the global authentication configuration options for Wireless data privacy logon. See “Wireless Data Privacy Logon (PPTP/L2TP Clients)” in Chapter 9, “User Authentication”.

If you are using Web-based logon, you can also customize the Logon, Logoff and Guest Registration pages for each location. See “Customizing Pages for Web-based Logon” in Chapter 9 for more information on the types of logon and appearance customization that are supported by the Rights Manager.

Note: *In order to create a location, you must first create at least one Where. In order to create a Where, you must first configure an Access Controller. Both these steps are described in this chapter.*

By default, the Rights Manager defines a single location, Everywhere Else. This default Location has the following properties:

- It includes the predefined Where called Everywhere Else, which is every Access Controller and port not included in another valid location
- Instead of a list of Whens, it is valid "Always" — 24 hours a day, seven days a week
- It allows (by default) only the default Logon, Guest, and Implicit User groups
- It requires NAT
- It allows unlimited users to connect through the location
- It does not specify a VLAN ID

You can modify many of the options for the Everywhere Else group. However, you cannot change the Wheres or the valid times of this group.

The Locations Manager

To access the Locations Manager, do the following:

» From within the Rights Manager, click **Locations**.

The Locations Manager page appears, as shown in Figure 8-1.

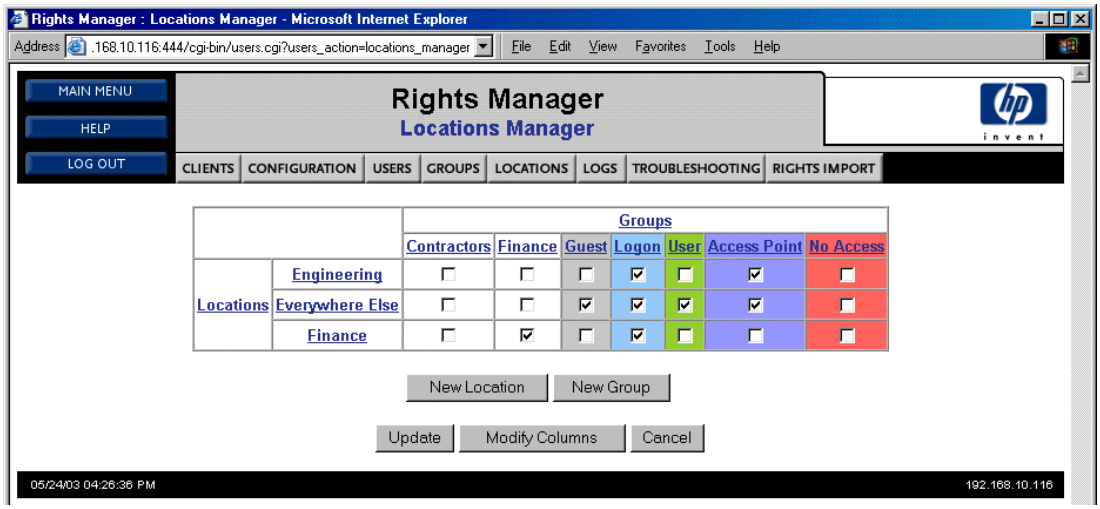

Figure 8-1. The Locations Manager

The Locations Manager displays the current locations in a column at the left of the display.

The columns in the table show all the Groups currently defined in the Rights Manager. The groups are ordered by type, with each type indicated by the color of the row. The colors are defined in Table 8-1. There can be multiple groups of each type.

Table 8-1. Group Background Color Codes

Color	Meaning
White	Normal groups—groups that define rights for authenticated users that are members of the group
Grey	Guest groups—groups that define rights for guest users
Blue	Logon groups—groups that define rights for users that have not been authenticated
Green	Implicit User groups—groups that define rights for authenticated users who are not members of any other group
Violet	Access Point groups—groups that define rights for access points
Light Red	Stop groups—groups that define rights that prevent network access

The check boxes in the table cells show which groups are allowed at each location. You can change the assignment of allowed groups in one of two ways:

- Click the check box in the appropriate table cell to enable or disable the group for that location.
- Add or remove groups for the location using the Location Editor.

The buttons at the bottom center of the page have the functions as described in Table 8-2.

Note: *If you have a large number of columns (or columns that are very wide due to long Allow or Redirect names) these buttons may appear off the page to the right. You can scroll the page horizontally to reach them.*

Table 8-2. Location Manager button functions

Button	Function
New Location	Displays the Location Editor. See “Adding or Modifying a Location—the Location Editor”.
New Group	Displays the Group Editor. See “Adding or Modifying a Group—the Group Editor”.
Update	Updates all Locations to include the selected allows or redirects.
Modify Columns	Displays the Location/Group Column Modifier page. “Modifying the Groups Columns in the Locations Manager”.
Cancel	Cancels any pending changes you have made to the table since the last Update.

Selecting Groups in the Locations Manager

You can add groups to a location or remove groups from a location through the Location Manager. You add and remove groups by checking or unchecking the checkbox in the table cell that is the intersection of the Group column with the row for the location.

Step 1. Specify what groups should be added or removed from a location:

- To add a group, click the checkbox to turn it on.

- To remove a group, click the checkbox to turn it off.

Step 2. Click **Update** to have your selections take effect. This also redisplays the main Rights Manager page (the Clients display).

- To cancel your proposed changes, click **Cancel**. This displays the Rights Manager main page without saving your changes.

Note: *If you navigate to another page before you click Update, all pending changes are lost. Also, to avoid having to navigate repeatedly between the Locations Manager and the Rights Manager main page, you should specify all your changes before you click Update, rather than doing an Update after each one.*

Modifying the Groups Columns in the Locations Manager

You can modify the Group columns so that you see only a subset of the groups defined in the Rights Manager.

Step 1. To change which Groups appear in the Locations Manager page, click **Modify Columns**.

The appropriate Group Column Modifier page appears. Figure 8-2 shows the Location / Group Column Modifier page.

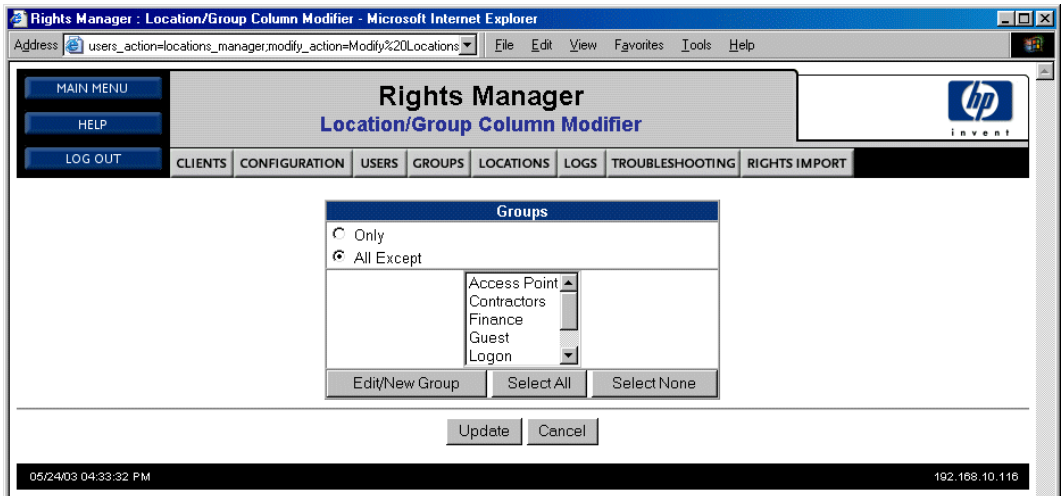

Figure 8-2. Modifying the Groups shown on the Locations page

Step 2. Use the Column Modifier page to include or exclude display of Groups in the Locations Manager.

To select the columns to display, choose one of the following options:

- To select individual Groups to display in the Locations Manager table, click **Only** and then select the Groups that you want to include in the table.
- To select multiple items in the list, press and hold the CTRL key while you select items with the left mouse button.

- To select individual Groups that should not be displayed in the Locations Manager table, click **All Except** and then select the Groups that you want to exclude from the table.
- To add a new Group, or to modify an existing Group, click **Edit/New Group**.

  See "Adding or Modifying a Group—the Group Editor" in Chapter 7 for more information.
- Click **Select All** to select all items in the list, or **Select None** to select no items in the list.

Step 3. When you are done, click **Update**. The Locations Manager page appears showing only the columns you have selected.

Adding or Modifying a Location—the Location Editor

To create a new group, or modify an existing group, do the following:

Step 1. From the Locations page, click **Edit/New Location**, or click a location name.

The Location Editor appears, as shown in Figure 8-3.

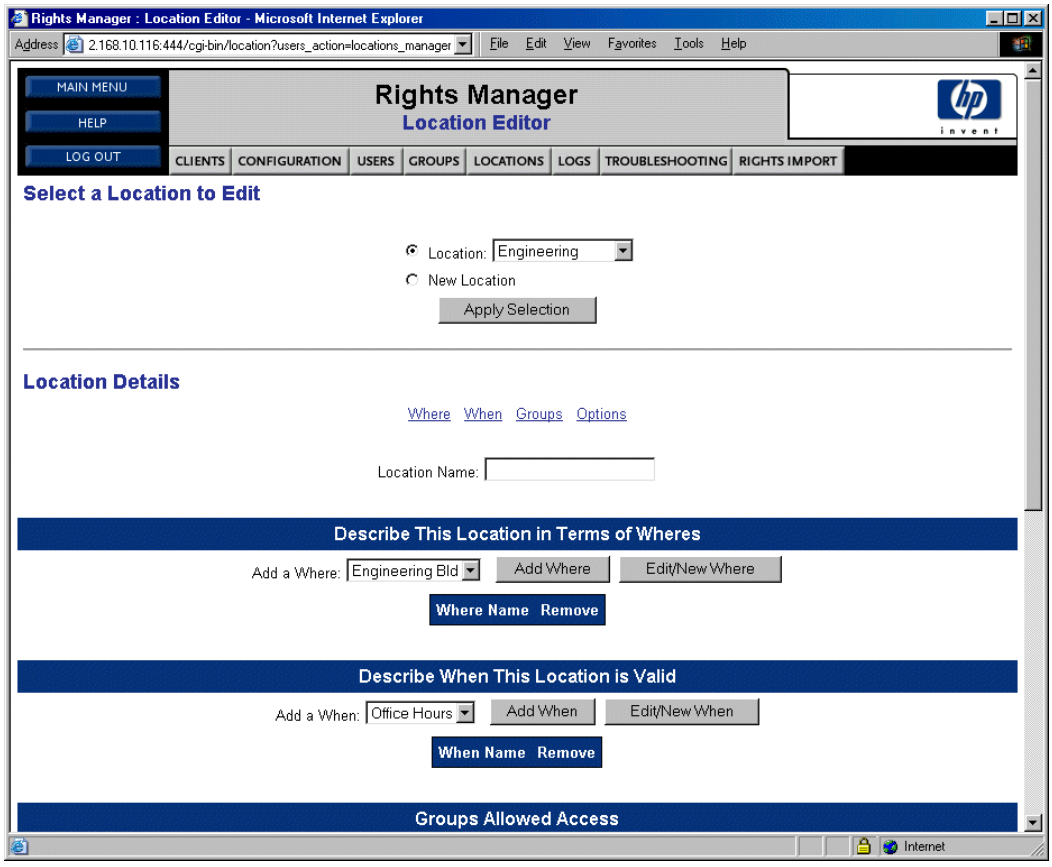

Figure 8-3. Location Editor, top portion of page

Select a Location to Edit

Step 2. To create a new location, select **New Location**.

To modify the settings for an existing location, select **Location**, then highlight the location you want to modify from the drop-down list.

Step 3. Click **Apply Selection**.

If you've selected an existing location, that location's properties appear in the fields below. Otherwise, the fields are blank or are set to their default values

Location Details

Step 4. For a new location, enter a location name. The name is already filled in for an existing location.

Note: *You cannot use a slash (/) in a location name.*

Describe this Location in Terms of Wheres

The table in this section lists the Wheres through which clients can connect to this location. A Where can represent an Access Controller, a single port on an Access Controller, or a specific client identified by its MAC address. When a client accesses the system, the Where that it matches determines the location that the client is associated with.

Wheres can overlap—for example, you can have one Where defined for an Access Controller, and another Where defined for a specific port on that Access Controller. The Where with the more specific definition takes precedence when determining how to associate a client with a location.

Caution: *You can use a Where in more than one location. For example, you might want to define one location that is valid during business hours, and another location that is valid after hours. However, it is important that those locations do not overlap in terms of their valid times (Whens). If two locations are defined with the same Wheres and overlapping Whens, only one location will be accessible from the duplicate Where during the times when the two locations are both valid.*

Step 5. To add an existing Where to this location, highlight the Where in the drop-down list, and click **Add Where**.

Step 6. To create a new Where and add it to the list, click **Edit/New Where**.

For details of creating a Where, see "Adding or Modifying a Where—the Where Editor".

Step 7. To remove a Where from the list, check the appropriate box in the Remove column.

Note: *You must have at least one Where associated with a location.*

Describe When this Location is Valid

The table in this section lists the Whens that define the times during which this location is valid. A When is simply a named time specification. Whens allow you to create a time specification once and then use it with multiple groups or locations, rather than having to specify it individually each time.

You can specify multiple Whens to define the valid times for the location. The valid times are taken as the sum of all the Whens specified for the location. The table lists each When, its description, and a checkbox that allows you to remove it from this location.

If you don't specify any Whens, the valid time defaults to Every Other Time, which is effectively 24 hours a day, seven days a week.

Note: *When a location is not valid (outside the times defined in its Whens) the location effectively does not exist. Clients that attempt to connect through a Where (Access Controller/port) defined for that location will instead be connected to an alternate location. If no other location specifically includes the same Where, then the client is connected through the default location Everywhere Else. Whether they will be allowed to log on will depend on the groups allowed at the alternate location.*

Step 1. To add an existing When to this group, highlight the When in the drop-down list, and click **Add When**.

Step 2. To create a new When and add it to the list, click **Edit/New When**.

For details of creating a When, see "Adding or Modifying a When—the When Editor" in Chapter 7.

Step 3. To remove a When from the list, check the appropriate box in the Remove column.

The remaining sections of the Location Editor are shown in Figure 8-4.

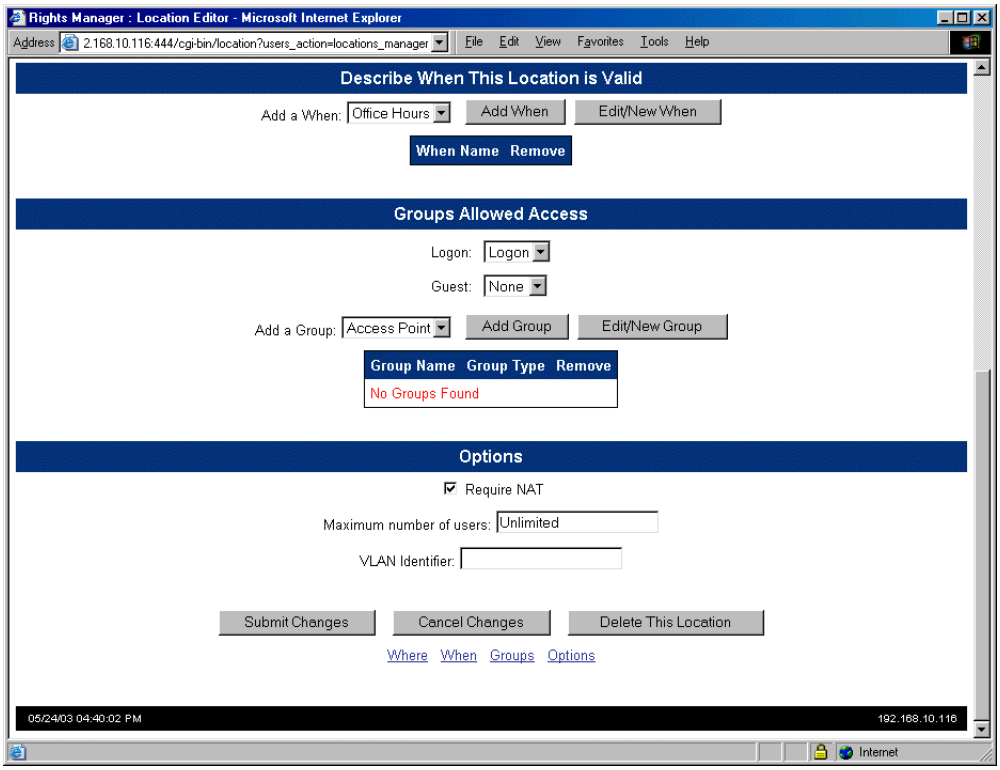

Figure 8-4. Location Editor, bottom portion of page

Groups Allowed Access

You must specify which groups are allowed at this location. This determines which users can log on through this location.

Step 1. If there are multiple Logon groups available, you can select which Logon group is allowed at this location. Select the group from the drop-down list.

You can specify only one Logon group, and you must have one selected. "None" is not an option for Logon.

To create a new Logon group, click **Edit/New Group** to go to the Group Editor.

Step 2. If there are multiple Guest groups available, you can select which Guest group is allowed at this location. Select the group from the drop-down list.

You can specify only one Guest group. You can also specify **None**, which disables all guest access (including Registered Guest access) through this location.

Note: *You can disable Guest logon through options in the Customize Web Pages by Location page for the Logon web page. However, previously registered guest users will still be able to log in using the user name and password they entered when they registered.*

To create a new Guest group, click **Edit/New Group** to go to the Group Editor.

Step 3. To add any other groups to the list of allowed groups, highlight the Group in the **Add a Group** drop-down list, and click **Add Group**. You can add Normal, Access Point, Implicit User, and Stop type groups from this list.

Note: *Only the groups you specify are allowed at this location. All other groups are disallowed.*

If you want the Implicit User or Access Point groups to be allowed, you must specifically add them here.

Other Options

Step 4. Click **NAT** for this location, if applicable.

The NAT option determines if this location uses Network Address Translation for IP addresses. The default is enable NAT; you must deselect NAT to use a real IP address.

Step 5. To limit the number of users that can be logged on through this location, type a value for **Maximum number of users**.

The default is unlimited.

Step 6. To force a VLAN tag to be added to all packets entering the system through this location, enter the VLAN ID (802.1Q tag) in the **VLAN ID** field.

Note: *A VLAN ID specified by the client's group membership overrides the VLAN ID specified by the location.*

Deleting a Location

To delete a location:

Step 1. From the Locations page (see Figure 8-1) go to the Locations Editor by clicking the location you want to delete.

Step 2. In the Location Editor, if the location you want to delete is not already displayed, select the location from the drop-down list in the Locations field, and click **Apply Selection**.

Information about the Location you want to delete should appear in the Location Details section of the page.

Step 3. Scroll to the bottom of the page and click **Delete This Location**.

A warning page appears that requires you to confirm that you really want to delete this location (see Figure 8-5).

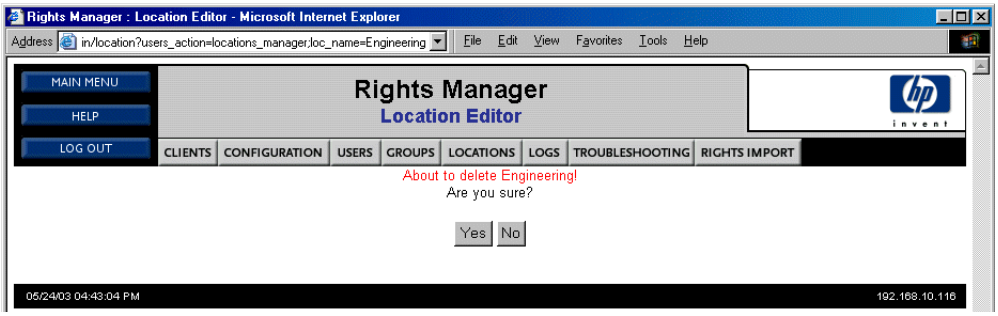

Figure 8-5. Delete Location Confirmation

Step 4. To proceed to delete this location, click **Yes**. To cancel, click **No**.

Adding or Modifying a Where—the Where Editor

A Where can represent an Access Controller, a single port on an Access Controller, or a specific client identified by its MAC address. When a client accesses the system, the Where that it matches determines the location that the client will be associated with.

Note: *Every location you create must have at least one Where associated with it.*

Wheres can overlap, with the more specific Where taking precedence when determining how to associate a client with a location.

For example, you could create one Where that represents the full Access Controller, and other Wheres that represent each port on that Access Controller. You could then create a location associated with specific Access Controller ports using the single-port Wheres, and another location associated with the full Access Controller. When the locations associated with individual ports are not available, clients connecting through those ports would instead come in through the location of the full Access Controller. This type of configuration allows you to define a location for specific ports during specific valid times, with another location that serves as a backup location for those ports the rest of the time.

To create a Where for use with a location, do the following:

Step 1. From the Location Editor, click the **Where** link or scroll down until you reach the section labeled **Describe This Location in Terms of Wheres**.

The **Edit/New Where** button is at the top of this section.

Step 2. Click **Edit/New Where**.

The Where Editor appears as shown in Figure 8-6.

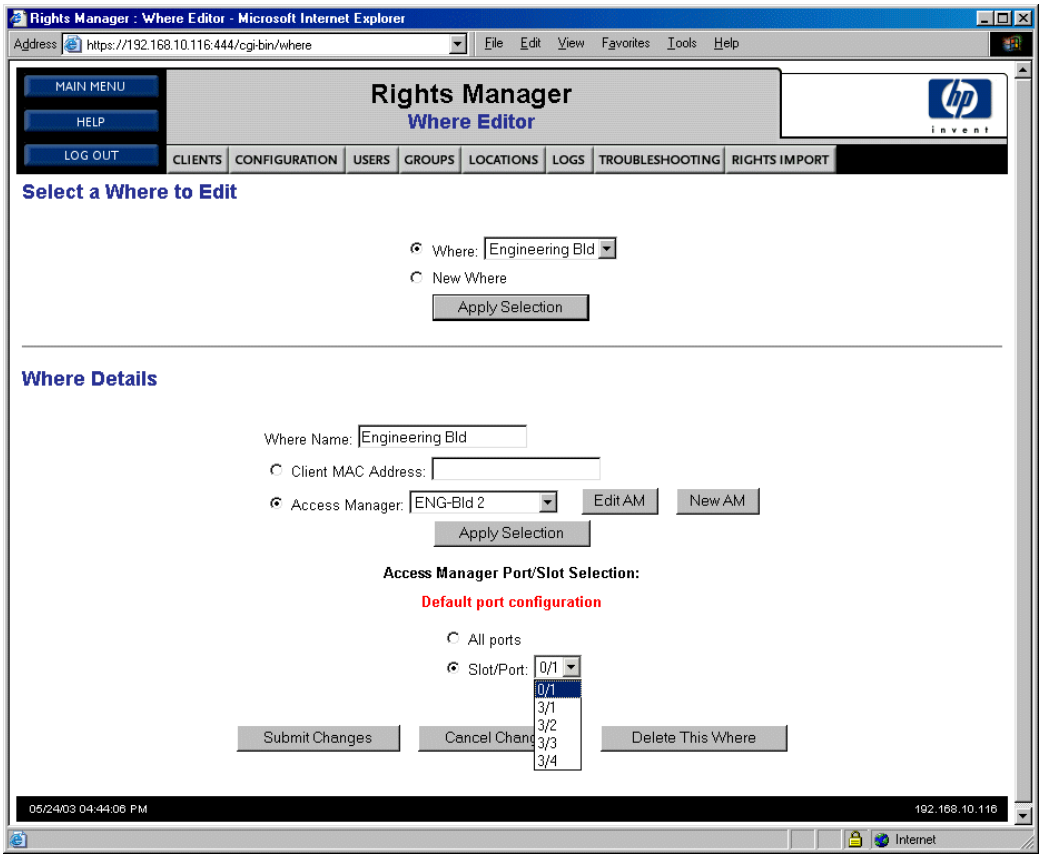

Figure 8-6. Where Editor

Step 3. To create a new Where, select **New Where**.

To modify the settings for an existing Where, select **Where**, then highlight the Where you want to modify from the drop-down list.

Step 4. Click **Apply Selection**.

If you have selected an existing Where, that Where's properties appear in the fields below. Otherwise, the fields are blank or are set to their default values

Where Details

Step 5. For a new Where, type a name in the **Where Name** field. The name is already filled in for an existing group.

Step 6. If this Where is actually a client MAC address, select **Client MAC Address** and enter the MAC address in the field provided.

Step 7. If this Where is an Access Controller or Access Controller port, select the **Access Controller** from the drop-down field.

Note: *If no Access Controllers have been configured, the Access Controller field indicates that no Access Controllers are configured. You must configure at least one Access Controller in order to proceed.*

To add a new an Access Controller or to edit the configuration of an existing Access Controller, click **Edit/New AM**. See "Adding or Modifying an Access Controller" for detailed instructions.

Step 8. When you initially select and Access Controller, a message indicates that the default port configuration is displayed. Click **Apply Selection** to update the drop-down Slot/Port list to match the actual slot/port configuration of the Access Controller.

Step 9. If this Where is the entire Access Controller click **All Ports**. If it is a single port, select the slot and port from the **Slot/Port** list.

Note: *A Where can be either an entire Access Controller or a single slot/port. It cannot include multiple ports other than all ports.*

Step 10. Click **Submit Changes** to have these changes take effect. A confirmation that your changes have been submitted is displayed.

If you have not yet submitted your changes, you can click **Cancel Changes** to undo your changes.

Deleting a Where

You may need to delete one or more Wheres if you want to remove an Access Controller from your system, because you cannot delete an Access Controller if it is used in a Where.

Note: *You cannot delete a Where if it is used in a location. You must first edit the location to remove the Where that you want to delete.*

To delete a Where:

Step 1. In the Where Editor, select the Where from the drop-down list in the Where field, and click **Apply Selection**.

Information about the Where you want to delete should appear in the Where Details section of the page.

Step 2. Scroll to the bottom of the page and click **Delete This Where**.

A warning page appears that requires you to confirm that you really want to delete this Where.

Step 3. To proceed to delete this Where, click **Yes**. To cancel, click **No**.

Adding or Modifying an Access Controller

Before you can create a Where, you must have at least one Access Controller configured. Even if you are using an Integrated Access Manager, you must configure the Access Controller portion of the Integrated Access Manager to use it in a Where.

To add an Access Controller:

Step 1. From the Where Editor, click **Edit/New AM**.

The Access Controller Editor appears, as shown in Figure 8-7.

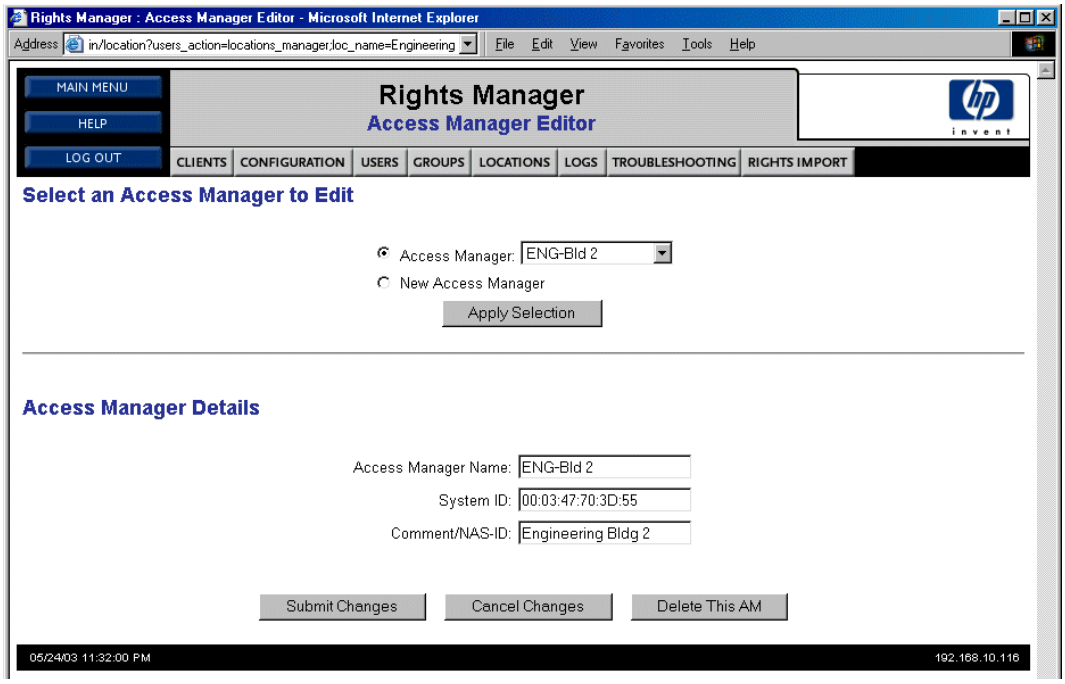

Figure 8-7. Access Manager Editor

Step 2. To modify the settings for an existing Access Controller, select **Access Manager**, then highlight the Access Controller you want to modify from the drop-down list.

Step 3. Click **Apply Selection**.

If you have selected an existing Access Controller, that Access Controller's properties appear in the fields below. Otherwise, the fields are blank or are set to their default values

Access Manager Details Section

Step 4. Type Access Controller name in the **Access Manager Name** field.

Step 5. Type the **MAC address** of the Access Controller.

You can find the MAC address in the Access Controller's Version and License screen.

Step 6. Optionally, type a descriptive comment or a NAS/ID. If you are using RADIUS accounting, the NAS-ID is sent to the RADIUS server as part of the accounting information.

Step 7. Click **Submit Changes** to configure a new Access Controller.

If you have not yet submitted your changes, you can click **Cancel Changes** to undo your changes.

Deleting an Access Controller

If you remove an Access Controller from your network, you will need to remove that Access Controller from the Rights Manager.

Note: *You cannot delete an Access Controller that is used in a Where. Therefore, before you can delete an Access Controller, you must delete any Wheres that use this Access Controller, or edit them to use a different Access Controller.*

To delete an Access Controller, do the following:

Step 1. From the Where Editor, click **Edit/New AM**.

Step 2. Select **Access Manager**, then highlight the Access Controller you want to delete from the drop-down list.

Step 3. Click **Apply Selection**.

The Access Controller's properties appear in the fields below.

Step 4. Click **Delete This AM** to delete the Access Controller.

A warning page appears that requires you to confirm that you really want to delete this Access Controller.

Step 5. To proceed to delete this Access Controller, click **Yes**. To cancel, click **No**.

USER AUTHENTICATION 9

This chapter explains how to configure the Rights Manager for the 700wl Series system. It includes the following sections:

Overview of Authentication 9-1
Authentication Services 9-3
The Built-in Authentication Service 9-5
Configuring an LDAP Authentication Service 9-5
Configuring RADIUS as an Authentication Service 9-12
Configuring Kerberos as an Authentication Service 9-14
Using XML-RPC for Authentication 9-15
Authentication Realms 9-20
Customizing Pages for Web-based Logon 9-24
Monitored Logon (802.1x and NT Domain Logon) 9-39
Wireless Data Privacy Logon (PPTP/L2TP Clients) 9-34
Retrieving Group Information from an External Service 9-42
Retrieving MAC Addresses from an LDAP Directory 9-44
Configuring RADIUS Accounting 9-48

Overview of Authentication

The HP ProCurve Secure Access 700wl Series Rights Manager provides a great deal of flexibility in the methods you can use to authenticate users who want to log on to your network through the HP ProCurve Secure Access 700wl Series.

The 700wl Series system allows the following types of authentication:

- ***Browser-based Logon***

  With browser-based logon, the user is presented with a logon page through their web browser when they first attempt to access the network. Typically the logon page allows them to enter a username and password, which the 700wl Series system attempts to authenticate using one of the following authentication services.

  — Built-in (the default service available on the 700wl Series system)

  — Lightweight Directory Access Protocol (LDAP) including Microsoft's Active Directory and iPlanet's LDAP server

  — Remote Authentication Dial-in User Service (RADIUS)

— Kerberos

— XML-RPC-based service

To use browser-based logon, you must configure the Rights Manager to use one of these services for authentication.

- ***Wireless Data Privacy Logon***

  If you have configured your 700wl Series system to use one of the Wireless Data Privacy protocols (PPTP, L2TP / IPSec, pure IPSec, or SSH), the 700wl Series system can accept the user authentication done by the wireless data privacy method as being sufficient for the 700wl Series system logon. For PPTP / L2TP, you can specify the authentication realm that should be used to authenticate these users, which can be different than the default realm used to authenticate other users that are allowed to logon through the same location.

- ***Monitored Logon***

  With monitored logon, the 700wl Series system passes on the initial packets from the client through to the network, and then monitors the returning packets looking for the message indicating that authentication has been successful. Monitored logon functions outside the authentication mechanisms (realms and services) defined within the Rights Manager.

  The 700wl Series system can monitor the following logon methods:

  — 802.1x

  — NT Domain Logon

  Monitored logon must be enabled individually by Where. You can enable one or both types of monitored logon.

For web-based logon or wireless data privacy logon, the client is authenticated through an ***authentication realm***, which is simply a named, ordered list of one or more ***authentication services*** used to perform user logon authentication for a set of clients. An authentication service is a single instance of a service used for authentication, such as a specific LDAP server or RADIUS server.

The setup for authentication is found under the Configuration page in the Rights Manager.

To display the Configuration page:

» From the Rights Manager page, click **Configuration**.

The Rights Manager Configuration page appears, as shown in Figure 9-1.

Figure 9-1. Rights Manager Configuration page

Authentication Services

An ***authentication service*** is a single instance of a service used for authentication, such as a specific LDAP server or RADIUS server. The Rights Manager supports the following services:

- LDAP Directory services, such as Active Directory or iPlanet LDAP server
- RADIUS servers
- Kerberos services
- XML-RPC-based services
- The Rights Manager's built-in database. This is the default authentication service. You can populate it with user names and passwords through the Rights Manager.

To view the list of authentication services:

» From the Rights Manager Configuration page, click **Authentication Services**.

The Web-based Authentication Services List page appears, as shown in Figure 9-2.

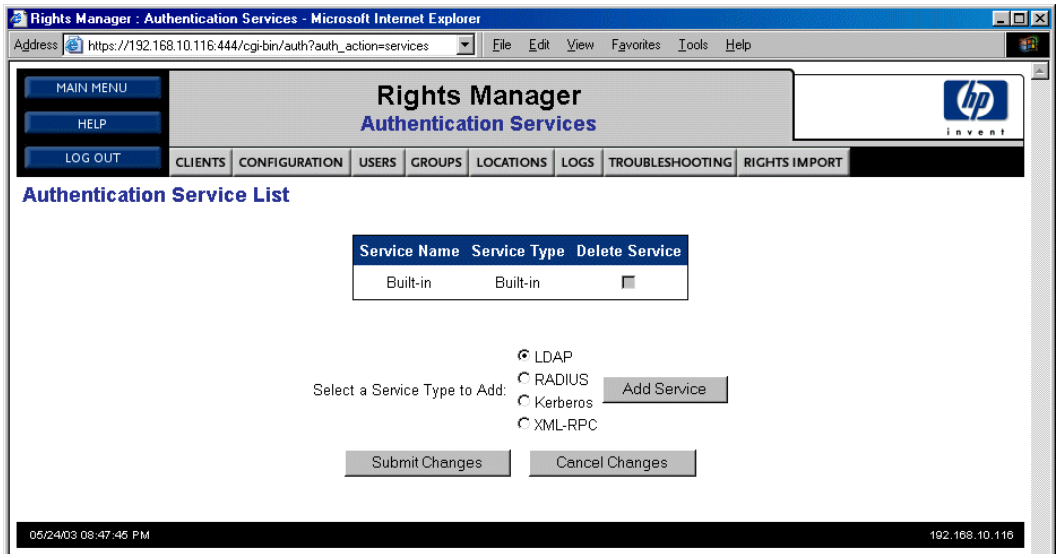

Figure 9-2. The Authentication Services List

Table 9-1 describes the information shown in this list.

Table 9-1. Authentication Services List

Column	Explanation
Service Name	The name of the authentication service. The default authentication service is named “Built-in”.
Service Type	The type of the authentication service (built-in, LDAP, RADIUS, Kerberos, or XML-RPC). There can only be one built-in service. There can be multiple services of the other types.
Authentication Service List	The authentication services included in this realm.

The Built-in authentication service lets you set up a database of users (and passwords) and their group associations within the Rights Manager. The Built-in database has two functions. The Rights Manager can use it to authenticate users—it is the default authentication service when no other external authentication service is configured. It is also used to maintain the association between users and groups, and can be used for this purpose even if you authenticate against an external authentication service.

Using an external authentication service, such as an LDAP, Kerberos, or RADIUS service, lets you authenticate users against an existing directory maintained within your organization.

Depending on your enterprise network, you might use one or more of these authentication services in combination, or you might use one as a back-up service if your primary service is not available.

Deleting a Service from the Services List

You can delete one or more services from the Services List, or you can delete a service individually from the Authentication configuration page for the service.

Note: *You cannot delete a service while it is used in a Realm. You must first remove it from the realm.*

To delete a service from the Services list:

Step 1. Click the checkbox in the row of the service you want to delete.

You can delete multiple services in a single operation.

Step 2. Click **Submit Changes** to delete the selected services.

If you click **Cancel Changes** before you submit, this cancels the delete operation and clears the check boxes.

The Built-in Authentication Service

The Built-in authentication service is used by default, so if you are setting up authentication for the first time, and you plan to use the built-in database, you do not need to do anything further. However, you will need to add user names and passwords to the authentication database. See Chapter 10, “Setting Up Users” for further instructions.

Configuring an LDAP Authentication Service

You can configure the 700wl Series system Rights Manager to use an external LDAP database for user authentication, and to retrieve group membership information. This section also provides specific instructions for:

- Setting up authentication using Active Directory
- Setting up authentication using a Netscape/iPlanet Directory Server

Depending on the configuration of your LDAP server, you can configure the Rights Manager to either retrieve the user’s password from the LDAP directory and then authenticate the user, or have the LDAP directory server do the authentication. The type of authentication you want to do determines the method you use to establish a session with the LDAP server. Establishing a session is known as binding to the server.

The bind methods you can use will be dictated by the configuration of your LDAP server.

- ***Non-User Binding*** allows the Rights Manager to bind to the Directory service either anonymously, or using the root Distinguished Name (DN) and password, and retrieve the user’s password. The Rights Manager then authenticates the user.
- ***User Binding*** specifies that the Rights Manager should bind to the Directory service as if it were the user, presenting the user’s DN and password. The Directory service then authenticates the user.

The Rights Manager also retrieves group information for the user from the LDAP server. This can also be done in one of two ways.

- If group membership information is included in the same record as the rest of the user information, you need to provide the name of the attribute that contains this information.
- If group membership information is kept in a separate record, you can specify a second search string to retrieve the group membership in a second operation.

You will need to know the following information about your LDAP database:

- The base DN for your database
- The attribute that contains the user logon name
- The attribute that contains the user password, if you are doing a non-user bind, and the method of encryption that the database will use to encrypt the password
- The bind string that defines the user DN, if doing user binding
- The attribute that contains the group membership information, if it is kept in the user record
- The search string to find group membership if it is kept in a separate record

To set up an LDAP authentication method:

Step 1. From the Rights Manager Web-based Authentication Service List page, as shown in Figure 9-2, select **LDAP** as the service type to add, then click **Add Service**.

The LDAP authentication page appears, as shown in Figure 9-3.

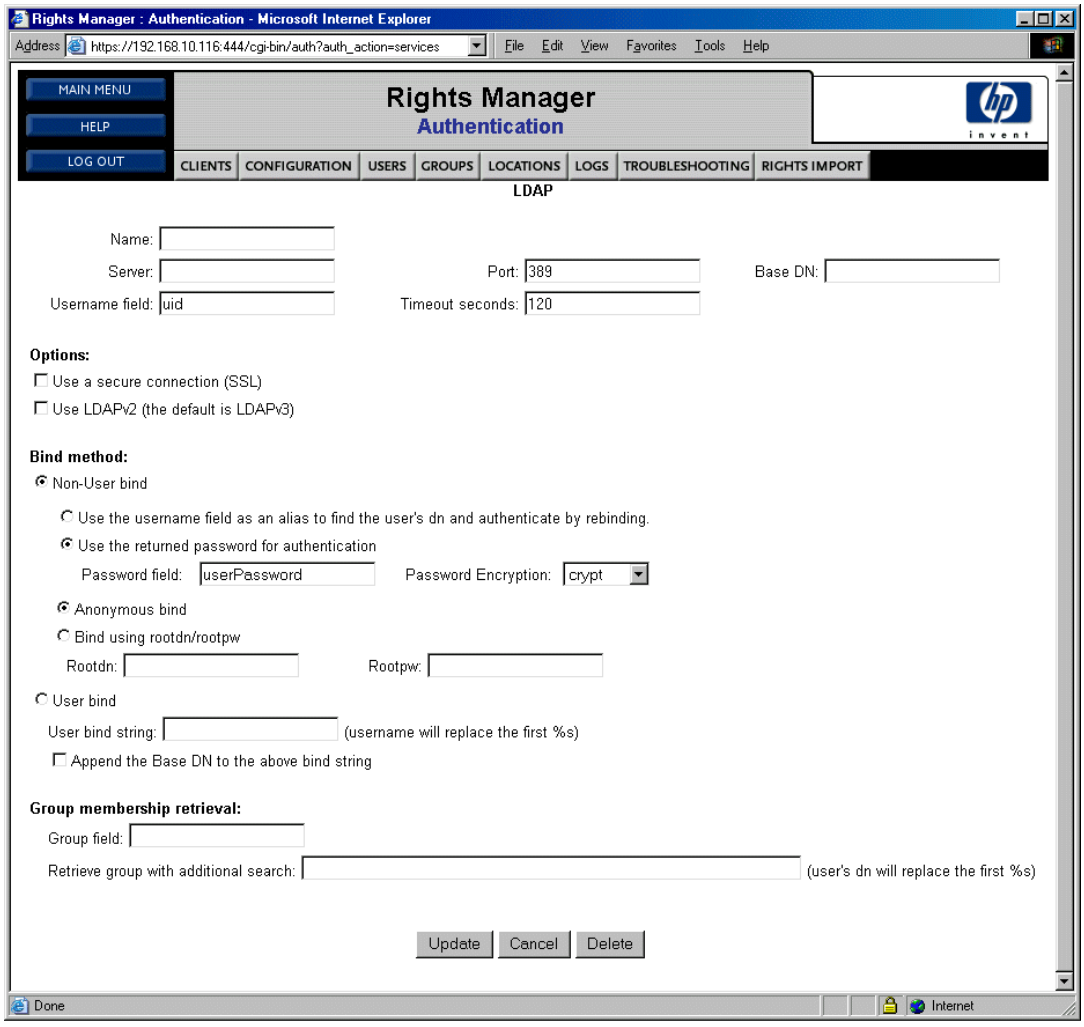

Figure 9-3. LDAP Authentication page

Step 2. Fill in the information as needed.

- Table 9-2 provides a description of the fields and options presented the LDAP Authentication page.
- For detailed instructions for setting up an Active Directory server, see "Configuring Authentication Using the Active Directory Service" on page 9-9.
- For detailed instructions for setting up a Netscape or iPlanet server, see "Configuring Authentication Using a Netscape or iPlanet Directory Service" on page 9-10.

Table 9-2. LDAP Authentication Options

Field Name/Option	Description
Name	Your name for this authentication method. You can use any alphanumeric string as the name.
Server	The Fully Qualified Domain Name (FQDN) or IP address of the server running the LDAP service.
Username field	Name of the field (attribute) in the database that holds the Username to be matched.
Port	UDP Port for LDAP (typically 389).
Timeout	Authentication timeout period (in seconds).
Base DN	The base Distinguished Name (DN) to be appended to the Username.
Options:	
Use a secure connection (SSL)	Select this option to communicate with the LDAP server using SSL. This is recommended if you are going to use one of the following options where the Rights Manager sends the user password to the LDAP server: • User binding • `Rootdn/rootpw` binding • "Use the username field as an alias…" • Password encryption set to CLEAR SSL must be enabled on the LDAP server to use this option.
Use LDAP v2	Select this option if your Directory is based on LDAP v2. The default is LDAP v3.

Table 9-2. LDAP Authentication Options

Field Name/Option	Description
Bind Method	
Non-User bind	Select this option if your LDAP server allows you to connect anonymously or using the rootDN and root password, and you want to present a user logon and retrieve the associated user password from the directory service.
Use the username field as an alias to find the user's dn and authenticate by rebinding.	Select this option if the user's DN is NOT the same as the Username field (the user logon). If this is the case, the Rights Manager does the user authentication in two steps: It first connects to the directory service with Non-user binding, and uses the Username as an alias to retrieve the actual user DN. It binds a second time with User binding, using the retrieved user DN and the user-provided password to authenticate the user.
Use the returned password for authentication.	Select this option to indicate that the password should be retrieved so the Rights Manager can use it to authenticate the user.
Password field	The attribute that contains the user password to be retrieved. Commonly this is the attribute `userPassword`.
Password Encryption	The method used to encrypt the password when returning it to the Rights Manager. Select one of the following: Crypt, SHA, SSHA, MD5, SMD5, or no encryption (CLEAR). • Crypt • SHA • SSHA • MD5 • SMD5 • CLEAR – no encryption
Anonymous bind	Bind anonymously without a username and password.
Bind using rootdn/rootpw	Bind using the root DN and password for the LDAP server.
Rootdn	The `rootdn` for your LDAP server.
Rootpw	The `rootpw` for your LDAP server.
User bind	Select this option to bind as the user, sending the user logon name and password to the Directory service for authentication.
User bind string	String defining the user DN for the user-level bind. String will be of the form `cn=%s,cn=user`. The actual user logon name is substituted for the %s variable. Optionally you can type the base DN portion into this string, or the Base DN, as specified in the Base DN field, can be appended automatically.
Append the base DN to the above bind string	Check this box to have the Base DN (as specified in the Base DN field) appended to the User bind string. **Note**: You can type a base DN directly as part of the user bind string instead of checking this option.

Table 9-2. LDAP Authentication Options

Field Name/Option	Description
Group membership retrieval:	
Group Field	Name of the attribute containing group membership information for the user, if group information is contained in the same LDAP entry as the user information. This information will be retrieved after successful authentication of the user.
Retrieve group with additional search	Search string to use to retrieve group membership information if it is not contained in the same entry as the user information. Use %s in place of the actual user logon name in this string (for example, `cn=%s`). The actual user logon name is substituted for the %s variable.

Configuring Authentication Using the Active Directory Service

This section guides you through the configuration choices for authenticating using Active Directory.

Step 1. Enter the basic information about contacting your Active Directory service:

a. Enter a name for this authentication method. This can be any alphanumeric string.

b. Enter the fully qualified host name or IP address of the server where the Active Directory is located.

c. If the server uses a port other than UPD port 389, enter the appropriate number.

d. Enter the base Distinguished Name (DN) that should be appended to the username attribute for authentication requests. For Active Directory, this is the domain name, in the form `dc=<domaincomponent>,dc=<domaincomponent>`, with no spaces between the elements of the DN.

For example, if your NT domain is `XYZCorp.com`, the Base DN would be:

`dc=XYZCorp,dc=com`

e. Enter the name of the attribute that contains a user's logon name. For Active Directory, this is "`sAMAccountName`".

f. The timeout value specifies the length of time the Rights Manager waits for a response to an authentication request before it abandons the request. The default is 120 seconds. You can change this as appropriate for your situation.

Step 2. Specify the **Options** for your server:

a. For Active Directory, you should use SSL for a secure connection, since you must use User Binding, and the Rights Manager will be sending user passwords to Active Directory with the authentication request.

Note: *This requires that you have SSL enabled on your Active Directory server.*

b. Active Directory is based on LDAP v3, so leave the second button unselected.

Step 3. Specify the **Bind Method** for this server.

Note: *If you are using Active Directory for user authentication, you must use **User binding**. If you are using Active Directory only for external group retrieval, or if you need to use aliasing because the user's login ID is not used as their DN, then you can use Non-User Binding. You cannot use anonymous binding with an Active Directory service.*

To specify user binding for authentication where the user logon ID is used as the DN, do the following.

a. Click the **User bind** button.

b. Enter the following into the **User bind string** field:

<*domain name*>\%s

For example, for domain XYZCorp.com, this would be XYZCorp\%s.

If you are using Active Directory for external group retrieval or for authentication by aliasing, you can use ***Non-User binding***. You must bind with a Rootdn and Rootpw. You cannot use anonymous binding with Active Directory.

a. Select **Non-User bind**.

b. The encryption method does not matter in this case. By default the iPlanet directory service uses SHA. However, iPlanet returns the encryption method with every record, and the Rights Manager uses the method returned in the record if it differs from the method specified in the Password Encryption field.

c. Select **Bind using rootdn/rootpw**.

d. Enter the **Rootdn** and **Rootpw** for your database.

Step 4. Enter the Group field for Group membership retrieval. For Active Directory, this is the attribute "memberof".

Step 5. Click **Update.**

Configuring Authentication Using a Netscape or iPlanet Directory Service

This section guides you through the configuration choices for authenticating a Netscape or iPlanet Directory service.

Step 1. Enter the basic information about this LDAP authentication method:

a. Enter a name for this authentication method. This can be any alphanumeric string.

b. Enter the fully qualified host name or IP address of the server where the LDAP directory is located.

c. If the server uses a port other than UPD port 389, enter the appropriate number.

d. Enter the base Distinguished Name (DN) that should be appended to the username attribute for authentication requests.

e. Enter the Username attribute (commonly "uid") that contains a user's logon name.

f. The timeout value specifies the length of time the Rights Manager waits for a response to an authentication request before it abandons the request. The default is 120 seconds. You can change this as appropriate for your situation.

Step 2. Specify the **Options** for this LDAP server:

a. If your LDAP server is configured to use SSL, the Rights Manager can use SSL to communicate with it. This is recommended if you are going to use User binding, where the Rights Manager sends the user password to the LDAP server. Click the first button to use SSL.

b. If your LDAP server is based on LDAP v2, click the second button. By default, the Rights Manager assumes LDAP v3.

Step 3. Specify the **Bind Method** for this server.

If the iPlanet Directory service is using the default configuration, you must specify user binding. However, it can be configured for non-user binding.

For **User Binding** (the default):

a. Select **User bind**

b. Specify the bind string as `uid=%s`.

c. Check the box **Append the base DN to the above bind string** or type the base DN directly into the bind string.

For **Non-User binding** (if your LDAP server allows this):

a. Select **Non-User bind**.

b. Check **Use the returned password for authentication**.

c. Specify the password field. Typically this will be `"userPassword"`

d. Specify the encryption method. By default the iPlanet directory service uses SHA.

However, iPlanet returns the encryption method with every record, and the Rights Manager uses the method returned in the record if it differs from the method specified in the Password Encryption field. This allows the Rights Manager to correctly decrypt passwords in situations where there may be multiple encryption methods used in a single database.

e. Select **Bind using rootdn/rootpw**. You cannot use anonymous binding with these directory services.

f. Enter the `Rootdn` and `Rootpw` for your database.

Step 4. Group membership retrieval requires an additional search.

a. Specify the field that will contain the Group membership information in the record to be retrieved (typically `cn`)

b. Enter the following string into the **Retrieve group with additional search** field: `(&(objectclass=groupofuniquenames)(uniquemember=%s))`

The user DN returned from the initial search (for authentication) is substituted for the `%s` in this statement.

Step 5. Click **Update**.

Using Aliasing to Retrieve a DN and Password

If your LDAP database does not use the user's logon name as the DN, you can use non-User Binding and aliasing to find the DN and retrieve the password.

To use the Aliasing feature to retrieve a user name and password, follow Steps 1 and 2 in the procedures detailed in the previous sections as appropriate for your LDAP server. Make sure you enter the attribute that contains a user's logon name in the **Username** field.

Then, for **Step 3**, do the following:

a. Select **non-User bind**.

b. Click the radio button labeled **Use the username field as an alias to find the user's dn and authenticate by rebinding**.

c. If your service allows it, you can use anonymous binding. For Active Directory, iPlanet, or other LDAP servers that don't support anonymous binding, click the **Bind using rootdn/rootpw** button, and enter the appropriate DN and password for your database.

Because you are sending a password in the clear, make sure that you are using SSL.

If you need to retrieve group membership, follow Step 4 in the procedure as appropriate for your LDAP server. Then, click **Update**.

Configuring RADIUS as an Authentication Service

To configure the Rights Manager to use a RADIUS database for user authentication, follow these steps:

Step 1. From the Rights Manager Web-based Authentication Service List page, as shown in Figure 9-2, select **RADIUS** as the service type to add, then click **Add Service**.

The RADIUS authentication page appears, as shown in Figure 9-4.

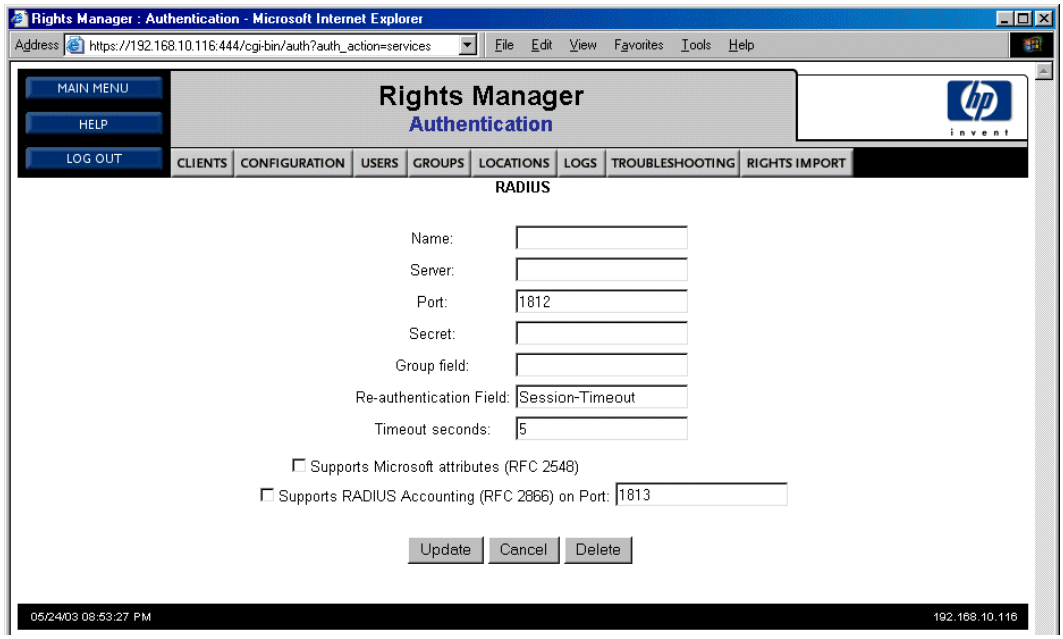

Figure 9-4. RADIUS Authentication page

Step 2. Enter the information requested.

A description of these fields is given in Table 9-3.

Table 9-3. RADIUS Authentication Options

Entry	Explanation
Name	Your name for this authentication method. You can use any alphanumeric string as the name.
Server	The Fully Qualified Domain Name (FQDN) or IP address of the server running the LDAP service.
Port	UDP Port for RADIUS (Default is 1812).
Secret	The shared secret for this RADIUS server.
Group Field	The RADIUS attribute that contains group membership information.
Reauthentication Field	The RADIUS attribute that specifies a duration (in seconds) after which the client is forced to reauthenticate.
Timeout	Authentication timeout period (in seconds).
Supports Microsoft's attributes (RFC 2548)	Check this to indicate that the RADIUS server supports Microsoft vendor-specific RADIUS attributes. **Note:** You must check this if you will use this RADIUS server to authenticate a PPTP or L2TP session.
Supports RADIUS Accounting (RFC 2866)	Check this to indicate that the RADIUS server supports RADIUS accounting. See "Configuring RADIUS Accounting" for more details about the RADIUS accounting feature.
on Port	UDP port for RADIUS accounting (Default is 1813).

Step 3. Click **Update** when you are done.

Configuring Kerberos as an Authentication Service

Note:€ *When using Kerberos authentication, you must synchronize the time between the Access Control Server and the Kerberos authentication server to within five minutes, otherwise Kerberos authentication does not work properly.*

To configure the Rights Manager to use Kerberos for user authentication, follow these steps:

Step 1. From the Rights Manager Authentication Service List page, as shown in Figure 9-2, select **Kerberos** as the service type to add, then click **Add Service**.

Step 2. The Kerberos authentication page appears, as shown in Figure 9-5.

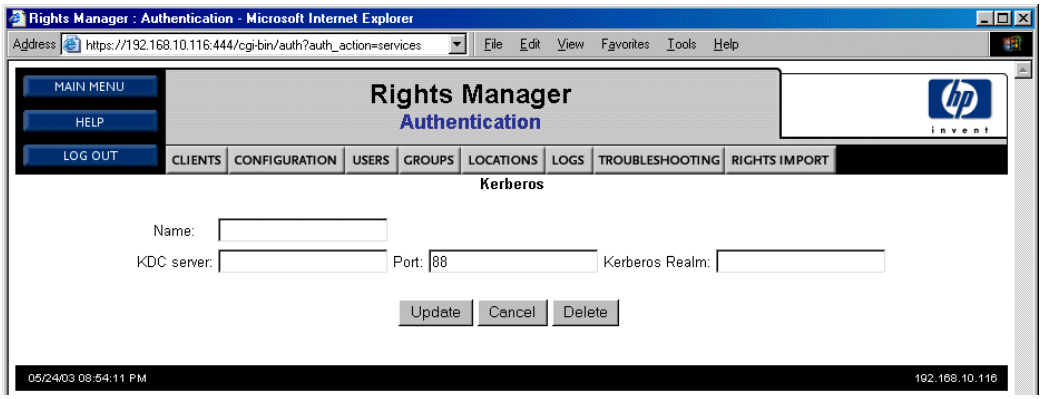

Figure 9-5. Kerberos Authentication page

Step 3. Enter the information requested.

Note:€ *If the Kerberos server you use is a Windows 2000 Server, you user must enter the Kerberos Realm name in all uppercase. If the case is lower or mixed, authentication will fail.*

A description of the Kerberos fields is given in Table 9-4.

Table 9-4. Kerberos Authentication Options

Entry	Explanation
Name	Your name for this authentication method. You can use any alphanumeric string as the name.
KDC Server	The Fully Qualified Domain Name (FQDN) or IP address of the server running the Key Distribution Center network service.
Port	Port number that the Key Distribution Center network service is running. Default is 88.

Table 9-4. Kerberos Authentication Options

Entry	Explanation
Realm	Kerberos realm to use when authenticating a user. The Kerberos protocol is designed to operate across organizational boundaries. Each organization wishing to run a Kerberos server establishes its own Kerberos realm. The name of the realm in which a client is registered is part of the client's name, and can be used by the end-service to decide whether to honor a request. **Note:** *Realm name must be all uppercase if Kerberos Server is a Windows 2000 server*

Step 4. Click **Update** to have your changes take effect.

Using XML-RPC for Authentication

The Rights Manager can use XML-RPC to request authentication and retrieve a user profile from an external XML-RPC service. XML-RPC is a simple, portable way to make remote procedure calls using HTTP as the transport and XML for encoding. Although related, it is not the same as general-purpose XML. The Rights Manager acts as an XML-RPC client, and communicates with an XML-RPC service through the 700wl Series system's XML-RPC Remote Profiles API.

Setting up the 700wl Series system to use XML-RPC for authentication and profile retrieval is a three-part process:

- You must be running an XML-RPC service on the external system from which you want to obtain authentication and user profiles. This service must accept an "authenticate" methodCall from the 700wl Series system Remote Profiles API, and to return the appropriate messageResponse. For a detailed discussion of the API, including the specification of the call and response, see "The Remote Profiles API". For more information on developing the XML-RPC service, see "The XML-RPC Service".
- You must configure the Rights Manager to send authentication requests to an XML-RPC server. This is discussed in "Configuring XML-RPC as an Authentication Service".
- Through the Rights Manager you must create groups that match the class or activity groups that can be returned in a student profile. You configure these groups with the access rights that should be granted to members of the group. See "Setting Up Groups for Student Access Rights" on page 7-20 for a further discussion of how these groups should be configured.

Once the XML-RPC authentication service has been configured, the authentication and authorization process works as follows:

- When a new student (client) connects to the 700wl Series system, the system presents a logon page, and retrieves the client's user identification information, including user name, password, the client's MAC address and the Access Controller Location through which he/she connected.
- The Rights Manager uses this information to create an XML-RPC "authenticate" methodCall, which it sends to the XML-RPC service via the URL defined in the XML-RPC authentication service configuration. The Remote Profiles API passes to the XML-RPC

service a basic set of user information (user name, password, MAC address, and a few other pieces of information) that the service can use to authenticate the client.

- The Rights Manager receives a response that indicates whether the user has been successfully authenticated (passed or failed). If the authentication was successful, the response also contains a “student profile” that specify the groups to which the user belongs, and a set of valid times for each group.
- The Rights Manager maps the group information from the user profile to the groups defined within the Rights Manager to determine the rights that should be granted to the user. It uses the start and stop times from the profile to specify the valid times for the rights associated with the group.

The current implementation of the remote profiles API uses SSL to provide the necessary security for passing passwords and other optional data. The Remote Profiles API is discussed in detail in “The Remote Profiles API”.

Configuring XML-RPC as an Authentication Service

To configure the Rights Manager to use an XML-RPC-based service for user authentication, follow these steps:

Step 1. From the Rights Manager Web-based Authentication Service List page, as shown in Figure 9-6, select **XML-RPC** as the service type to add, then click **Add Service**.

The XML-RPC page appears, as shown in Figure 9-6.

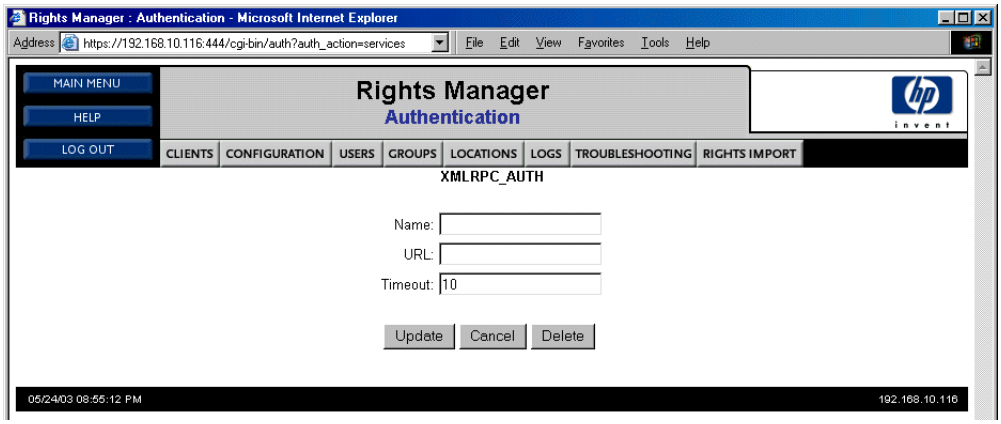

Figure 9-6. XML-RPC Authentication page

Step 2. Enter a name for this authentication method in the **Name** field.

Step 3. In the **URL** field, enter the URL of the XML-RPC service to which authentication requests should be sent.

Step 4. Click **Update** when you are done.

The XML-RPC Service

The XML-RPC authentication service required by the 700wl Series system is a piece of code that sits on the remote system between the 700wl Series system Remote Profiles API and whatever system (database, directory, or application) is used to contain student authentication and scheduling information.

The XML-RPC authentication service must perform the following tasks:

- The XML-RPC service accepts an "authenticate" methodCall from the 700wl Series system Rights Manager.
- The service extracts the user identification information, and constructs the appropriate inquiry needed to authenticate the user and retrieve his/her scheduling information.
- The service takes the returned information and constructs an XML-RPC response that includes the authentication status and, if appropriate, the user's schedule information in the form of a user profile. A user's schedule is mapped into a set of groups, and the times when the access rights associated with those groups are valid.

  For example, groups might be set up to correspond to specific classes. A set of start and stop times which could correspond to class meeting times, would specify when the rights for each group should take effect, and when they should expire.
- When the XML-RPC service has constructed the response, it sends the response back to the Rights Manager.

If you are also using the Network Access Control Console, this service should also be able to accept and respond to a `getMemberList` methodCall.

XML-RPC is a specification for doing remote procedure calls over the Internet using HTTP as the transport and XML as the encoding. Currently there do not appear to be any commercially available XML-RPC servers—typically an organization that decides to use XML-RPC writes their own server to handle their own special needs. However, there are a fairly large number of freeware/shareware server implementations and web services available through the XML-RPC web site at `http://www.xmlrpc.com`.

There is also a book, published by O'Reilly & Associates: "Programming Web Services with XML-RPC." It is available through the O'Reilly web site at `http://www.oreilly.com`.

The Remote Profiles API

The Remote Profiles API consists of a single call/response pair. The 700wl Series system issues the XML-RPC authenticate call to the XML-RPC "server" at the URL configured in the Rights Manager.

The remote XML-RPC server must generate the authenticate response. Note that the remote XML-RPC server may simply act as a front end to another database that contains the user information. In this case, the XML-RPC server would accept the authentication request from the 700wl Series system, in turn query the appropriate database, and then form and send the appropriate response.

The authenticate call to be made by the 700wl Series system is defined as follows:

```
authenticate (userid, password, location, MAC, options, randomstring)
```

These parameters are shown in Table 9-5:

Table 9-5. Parameters for authenticate call

Parameter	Type	Description
userid	string	User login from 700wl Series system login page.
password	string	Password from 700wl Series system login page, in clear text.
location	string	Name of the 700wl Series system-defined location of the user.
MAC	string	MAC address of the user, in the form 001122334455 (without colons).
options	string	A string that defines authentication and profile return options. Currently, must be set to `auth_profile`.
randomstring	string	Currently not used, but parameter must be present. Can be any string or a null string.

The following is an example of an XML-RPC authentication request for user Jane with password “easy” who is logging in from MAC address 00:01:02:03:04:05, and location Marketing:

```
<?xml version="1.0"?>
<methodCall>
<methodName>authenticate</methodName>
<params>
     <param><value><string>jane</string></value></param>
     <param><value><string>easy</string></value></param>
     <param><value><string>marketing</string></value></param>
     <param><value><string>000102030405</string></value></param>
     <param><value><string>auth_profile</string></value></param>
     <param><value><string> </string></value></param>
</params>
</methodCall>
```

Note that the password is in clear text, but security is provided by using SSL for transporting the packet.

The response is defined as follows:

```
authenticate response (profiles)
```

The response is a structure that contains name-value pairs as shown in Table 9-6:

Table 9-6. Name/Value pairs returned by authenticate response

Name	Type	Value and Description
userid	string	User login from 700wl Series system login page, as passed in authenticate request.
authentication_result	integer <i4>	0 = authentication failed 1 = authentication was successful, or no authentication is required
Profiles	array of strings	An array of strings, each of which contains a profile name and an array that defines valid times for the profile. Members are name-value pairs as follows:

Table 9-6. Name/Value pairs returned by authenticate response

Name	Type	Value and Description
profileName	string	A name that matches a Rights Manager group name.
validTimes	string	An array of strings that define the times when a user is given the rights associated with the group.
		Members are name-value pairs as follows:
startTime	string	A time in the format `hh:mm:ss` that defines the time of day at which these rights should take effect.
stopTime	string	Time in the format `hh:mm:ss` that defines the time at which these rights should cease to be in effect.
daysOfWeek	string	A concatenation of day names separated by colons. Any combination is valid, but each name may appear only once. Monday:Tuesday:Wednesday:Thursday:Friday:Saturday:Sunday.
startDate	string	Day of the year in the format YYYY-MM-DD that defines the day of the year on which these rights should take effect.
stopDate	string	Day of the year in the format YYYY-MM-DD that defines the day of the year on which these rights should cease to be in effect.
hashed_string	string	Currently not used, but parameter must be present. Can be any string or a null string.

The following is an example of an XML-RPC authentication response to the request for user Jane, providing a user profile that gives her membership in the group Class01 that is valid between 12:00 noon and 2:30 pm every Monday, Wednesday, and Friday, from April 1, 2002 through May 31, 2002:

```
<?xml version="1.0"?>
<methodResponse>
<params>
<param><value><struct>
       <member><name>userid</name>
          <value><string>jane</string></value>
       </member>
       <member><name>authenticate_result</name>
          <value><i4>1</i4></value>
       </member>
       <member><name>Profiles</name>
           <value><array>
            <data>
             <value><struct>
               <member><name>profileName</name>
                  <value><string>class01</string></value>
                     </member>
                        <member><name>validTimes</name>
                           <value><array>
                              <data>
                                <value><struct>
                                  <member><name>startTime</name>
                                   <value><string>12:00:00</string></value>
                                  </member>
                                  <member><name>stopTime</name>
                                   <value><string>14:30:00</string></value>
```

```
                                    </member>
                                    <member><name>daysOfWeek</name>
                                      <value><string>Monday:Wednesday:Friday
                                       </string></value>
                                    </member>
                                    <member><name>startDate</name>
                                     <value><string>2002-04-01</string></value>
                                    </member>
                                    <member><name>stopDate</name>
                                     <value><string>2002-05-31</string></value>
                                    </member>
                                  </struct></value>
                          </data>
                        </array></value>
                      </member>
                    </struct><value>
                </data>
            </array></value>
         </member>
           <member><name>hashed_string</name>
              <value><string> </string></value>
            </member>
        </struct></value>
    </param>
</params>
</methodResponse>
```

Authentication Realms

The Rights Manager uses the concept of an ***authentication realm*** to defined a named, ordered set of authentication services used to perform user logon authentication for a set of clients. In practice, this “set” may consist of a single authentication method.

One authentication realm is always designated as the ***default realm***, which is the realm which is used to perform user authentication under normal circumstances. The Rights Manager provides a pre-defined realm named “Default Realm” that uses the Built-in authentication service, and is designated as the operational default realm. You can modify the predefined “Default Realm” by adding other authentication services to it, or replacing the Built-in service with a different one. You can also define other named authentication realms and designate one of those as the operational default realm.

If you have multiple sources you want to use for authentication, you can create an authentication realm with multiple authentication services, ordered by the sequence in which they should be searched. This lets you create a realm where, if a user is not authenticated by the first service in the list, the Rights Manager tries the next service.

You can also define multiple authentication realms, each of which is identified by its unique name, and specify which of those should be the default realm. For example, you might want to create a primary realm and a backup realm, so you could switch the default realm to the backup realm if the authentication service used in the primary realm becomes unreachable.

Further, there are two situations where you can use different authentication realms for users logging in through different locations.

- For a location that allows clients to connect using L2TP or PPTP, you can specify the authentication realm that should be used to authenticate those clients. Users that connect using basic web-based logon would still be authenticated using the default authentication realm. See “Wireless Data Privacy Logon (PPTP / L2TP Clients)” for details.
- For web-based logon, you can customize the logon page to present the user with a list of authentication realms, and allow the user to select which realm should be used to authenticate him or her. For example, a University might use different authentication services for staff and students associated with different divisions, such as the Business School, Medical School, or Law School. “Customizing Pages for Web-based Logon” for more information.

To create or configure an authentication realm:

Step 1. from the Rights Manager Configuration page, select **Authentication Realms**.

The Authentication Realms page appears, as shown in Figure 9-7.

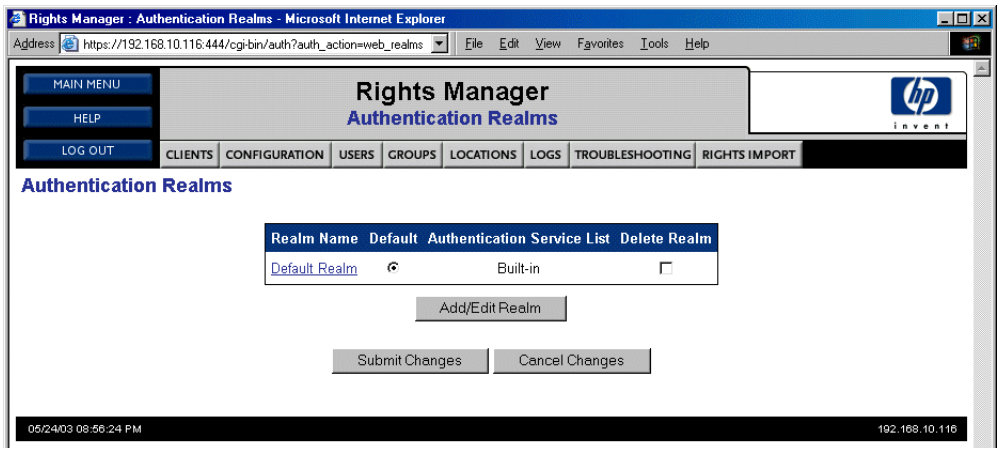

Figure 9-7. Web-based Authentication Realms

Initially, this list shows only the Default Realm, and the Default Realm includes only the Built-in service.

Table 9-4 describes the information shown in this list.

Table 9-7. Advanced Authentication Realms List

Column	Explanation
Realm Name	The name of the realm. The default realm is named “Default Realm”.
Default	The selected button indicates the realm that is currently the operational default realm.
Authentication Service List	The authentication services included in this realm.
Delete Realm	Click the checkbox to mark this realm for deletion.

Step 2. To create a new realm, or to modify the configuration of an existing realm, click **Add/Edit Realm**.

Creating or Modifying an Authentication Realm

To create a new Authentication Realm:

Step 1. From the Authentication Realms page, click **Add/Edit Realm**.

The Authentication Realm Editor appears, as shown in Figure 9-8.

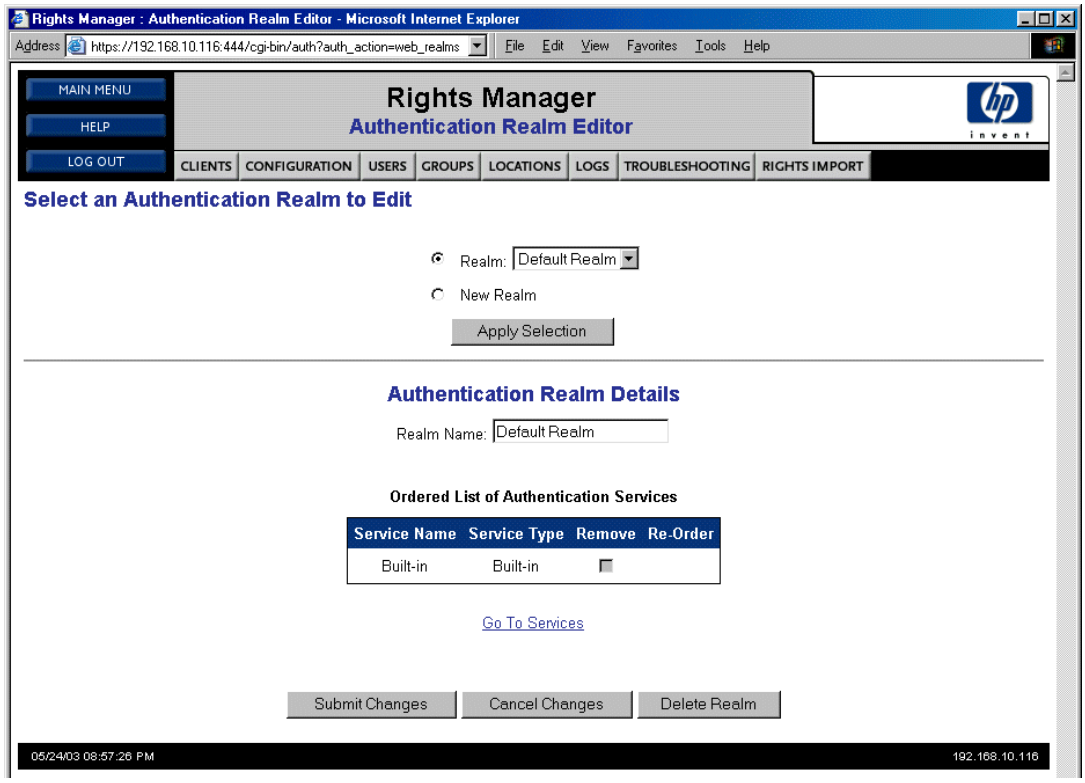

Figure 9-8. Authentication Realm Editor

Step 2. To create a new realm, select **New Realm**.

To modify the settings for an existing realm, select **Realm**, then highlight the realm you want to modify from the drop-down list.

Step 3. Click **Apply Selection**.

If you've selected an existing realm, that realm's name and the services it includes appear. Otherwise, the fields are blank.

The Ordered List of Authentication Services displays the authentication services that are included in the realm. (For a new realm, the list is empty.)

Table 9-8 describes the information in this list.

Table 9-8. Ordered List of Authentication Services

Column	Explanation
Service Name	The name of the service.
Service Type	The service type (Built-in, LDAP, RADIUS, Kerberos or XML-RPC).
Remove	Click the checkbox to mark this service for removal from the realm.
Re-Order	For realms with more than one service, displays **Move Up** and **Move Down** buttons that move the service up or down in the list.

Step 4. For a new realm, type the name into the **Realm Name** field.

Step 5. To add an authentication service to the realm, select the authentication service from the drop-down list in the **Available Services** field, then click **Append Service**.

The service is added to the end of the list of services.

- To add a new service, or to make changes to an existing service, click the **Go To Services** link. This takes you to the Authentication Services List, and from there you can add or modify a service.

Step 6. To remove a service from the realm, click the **Remove** checkbox for the service you want to remove.

Step 7. To reorder the list of services, click the **Move Up** or **Move Down** button as appropriate.

The order of services is significant: when the Rights Manager attempts to authenticate a client, it starts with the first service in the list, then tries the second service, and so on through the list. This can affect how long it takes to authenticate a client—ideally you want the authentication service which is most likely to succeed to be searched first.

Step 8. Click **Submit Changes** to create the new realm or have your changes take effect.

- To cancel any changes that you have not yet submitted, click **Cancel Changes**.

Changing the Default Realm

You can change the realm that you have set as the default realm by editing the realm settings.

Step 1. From the Rights Manager Configuration page, select **Authentication Realms**.

The Authentication Realms page appears, as shown in Figure 9-7.

Step 2. In the **Default** column, click the checkbox for the realm that you want to be the new default realm.

Step 3. Click **Submit Changes** to have this change take effect.

This realm will now become the Default Realm, replacing the realm that was previously the default.

Deleting a Realm

There are two ways to delete a realm: you can delete one or more realms from the Realms list, or you can delete a realm individually using the Realm Editor.

To delete one or more realms from the Authentication Realms list:

Step 1. Click the checkbox in the row of the realm you want to delete.

You can delete multiple realms in a single operation.

Step 2. Click **Submit Changes** to delete the selected realms.

To delete a realm using the Authentication Realm Editor:

Step 1. From the Authentication Realms page, click **Add/Edit Realm**.

The Authentication Realm Editor page appears, as shown in Figure 9-8.

Step 2. Click **Realm**, highlight the realm you want to delete in the drop-down list, and click **Apply Selection**.

The realm appears in the Authentication Realm Details section of the page.

Step 3. To delete the realm, scroll to the bottom of the page and click **Delete this Realm**.

The realm is deleted.

Note: *The authentication services used in the realm are NOT deleted when a realm is deleted.*

Customizing Pages for Web-based Logon

The 700wl Series system Rights Manager provides default Logon, Logoff, Stop, and Guest Registration pages that are displayed when users are to be authenticated using Web-based logon. The default logon page displays the HP logo, and appears as shown in Figure 9-9.

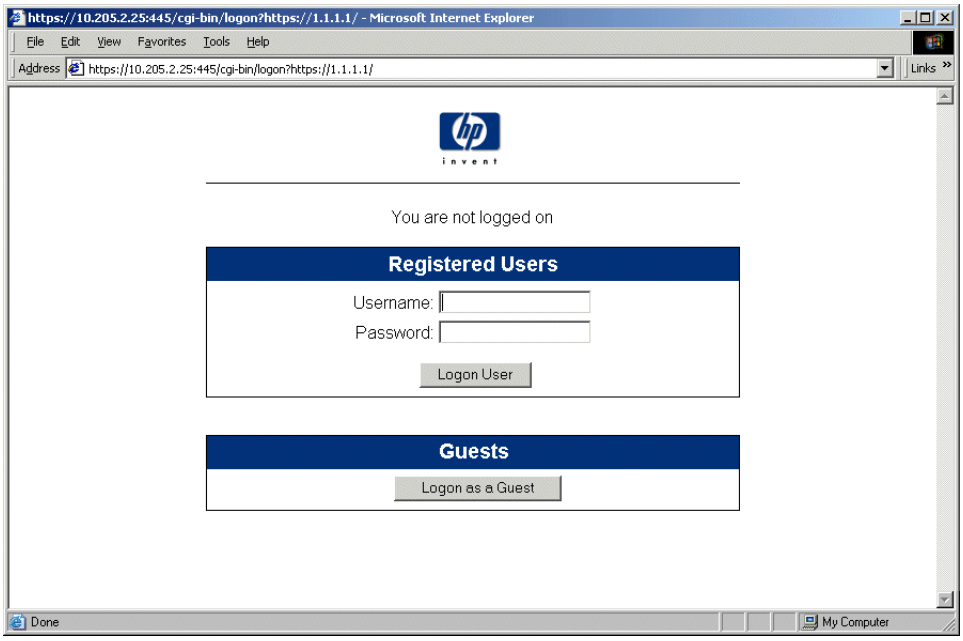

Figure 9-9. The default Logon page

Through the Rights Manager you can customize the Logon, Logoff, Stop, and Guest Registration pages. By customizing these pages you can identify your organization to the user before they log in, and confirm to the user that they are logging in to the appropriate location within the organization. If you use multiple authentication realms (for example, a Business School authentication realm and a Medical School authentication realm) you can also allow the user to choose the appropriate realm.

For special-purpose installations, such as a kiosk application, you can capture information about the users who log in to view your site by requiring Guest users to go through a registration process. A Registered Guest provides a username and password that are stored in the Rights Manager built-in database. Once registered, a registered guest can log on again using their username and password, but will always have only Guest access rights.

Through the Rights Manager, you can customize the appearance of the Logon, Logoff and Stop pages in the following ways:

- You can customize the existing Logon, Logoff, and Stop pages by including your own text and logos.
- You can associate a different customized page for each location you have created in the Rights Manager.
- You can specify whether Guest login should be allowed at this location, and whether Guest users should be required to go through a registration process.
- You can specify the Authentication Realm that should be used to authenticate users logging in through this location.
- You can customize the Logon, Logoff, and Stop pages for use with small browsers, such as those used on handheld wireless devices
- Instead of modifying the predefined pages used by the system, you can create your own customized page templates for the logon, logoff, and guest registration pages.

To access the web page customization page, do the following:

Step 1. From anywhere within the Rights Manager, click **Configuration**.

Step 2. Under the heading Web-based Logon, click **Customize Web Pages by Location.**

The Customize Web Pages by Location page appears, as shown in Figure 9-10

Figure 9-10. Selecting a location to customize

Step 3. Select the location you want to customize from the drop-down list, and click **Edit**.

The customization page for the selected location appears. Figure 9-11 shows the top portion of this page.

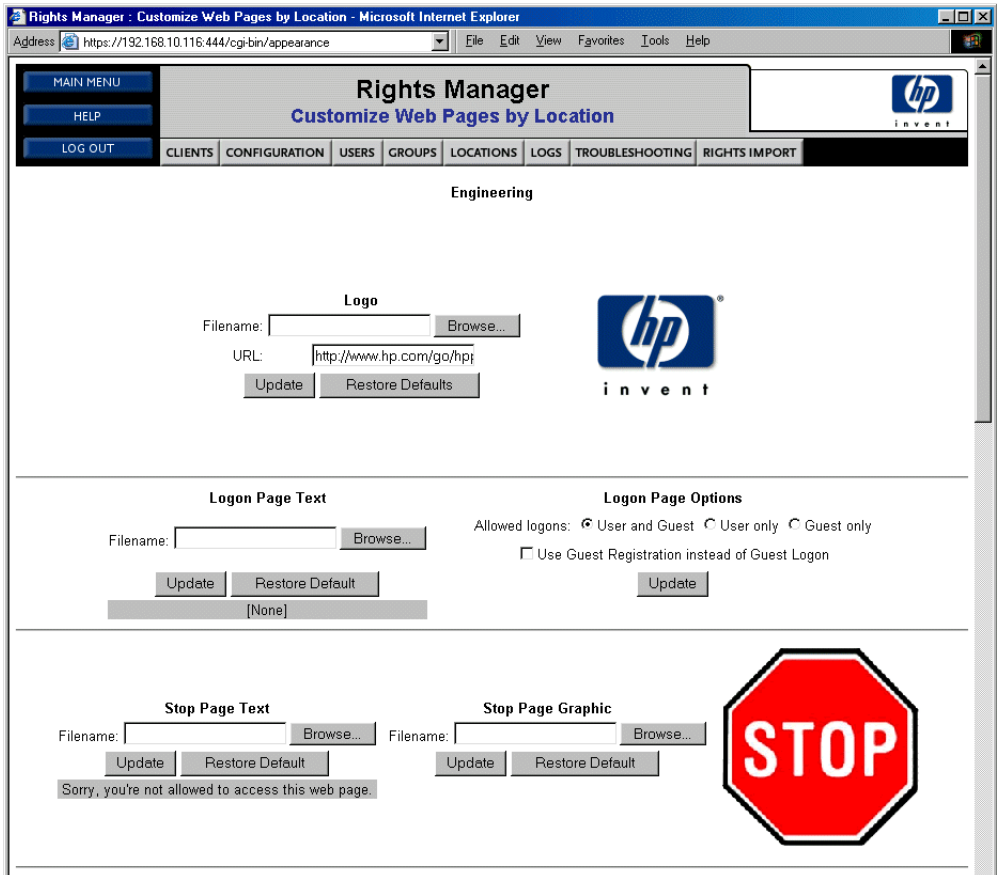

Figure 9-11. Customizing Web pages for a location, top part of page

Note: *You can customize pages only for existing locations. To define a new location, see "Defining Locations" in Chapter 8.*

You can customize your web pages in multiple ways.

Customizing the Logo

In the first section of this page you can customize the logo (image) that appears on the Logon and Logoff pages. The current logo (the HP logo by default) is displayed.

To change the logo, do the following:

Step 1. Type the path and name (case-sensitive) of a GIF, JPEG, or PNG file or other browser-compatible file format that contains the logo you want

or

Click **Browse** to locate the proper directory and file name.

Step 2. You can link the logo to a URL (for example, your organization's corporate web site) so that a user can click the logo on the logon page to go to your site. Enter the appropriate URL in the field provided.

Step 3. Click **Update** to enter these changes.

To restore the default logo, click **Restore Defaults**.

Customizing the Logon Page

You can add text to the logon page by providing a text or HTML file that contains the text you want displayed.

To update the text for the logon page:

Step 1. Go to the Logon page area of the Customization page, as shown in Figure 9-11.

Step 2. Under **Logon Page Text**, type the path and name (case-sensitive) of a text file or HTML file that contains the content you want to display to the logon user

or

Click **Browse** to locate the proper directory and file name.

Step 3. Click **Update**.

To clear the logon page text after it has been set, click **Restore Defaults**.

The grey area below the Filename field displays the text currently configured to appear on the page. The default is None.

You can also change several Logon Page Options:

Step 4. You can specify who is allowed to logon through this location. Choose either **User and Guest**, **User only**, or **Guest only**. These settings determine whether the Logon User and/or Logon as Guest buttons appear on the page.

Step 5. Click **User specified authentication realm** if you want users to choose a specific realm from a group of realms. For example, in a University users could choose the Business School authentication realm or the Medical School authentication realm.

Note: *This option does not appear if you have only one authentication realm defined.*

Step 6. To have Guest users go through a registration process, click **Use Guest Registration instead of Guest Logon**.

If you choose this option, the Logon as Guest button is replaced by a Register as Guest button, and the Guest user is taken to a registration page, as shown in Figure 9-13.

Step 7. Click **Update**.

Figure 9-12 shows an example of a customized logon page. In addition to the logo and text, it includes a field with a drop-down list where the user can choose an authentication realm, and the **Guest Registration** option.

Figure 9-12. Customized Logon Screen

If you select the **Guest Registration** option, the Guest Registration page appears as shown in Figure 9-13.

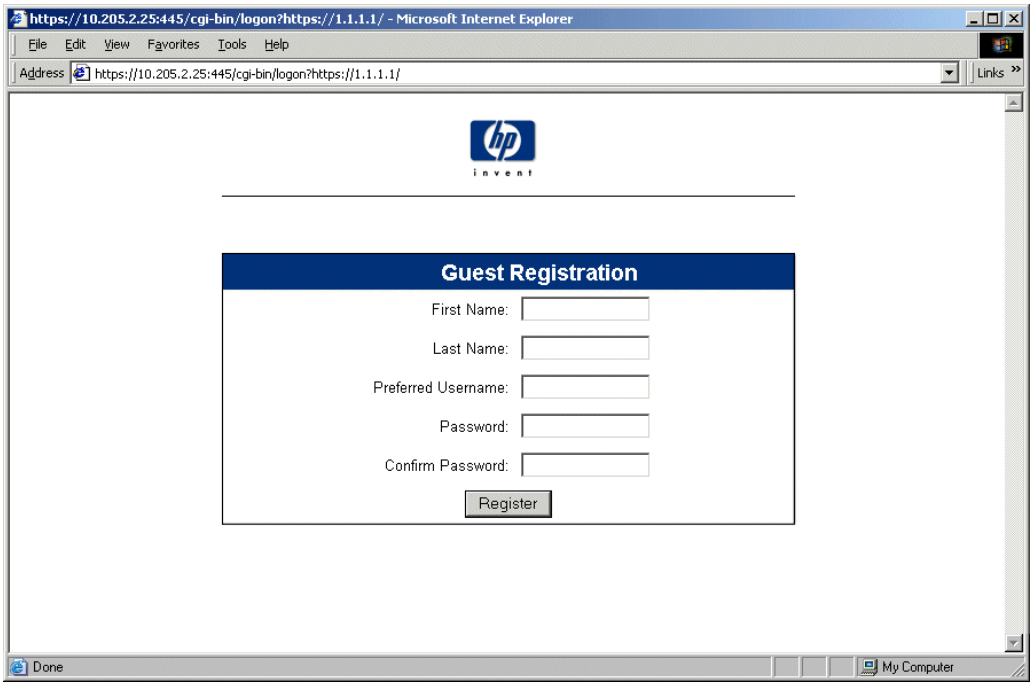

Figure 9-13. Guest Registration page

The Guest user fills in their first and last name, selects a user name and a password.

The user name and password are entered into the Rights Manager built-in database. Once registered, this user will be able to log in as a registered user (using the username and password he/she registered), but will still receive only Guest rights.

The user's first and last names are included in the Log file entry created for the logon event, similar to the following:

```
Aug 27 17:45:39 Informational Guest Registration completed for Tex satmac =
00e0187db53d, javaworks = 0, firstname = Tex, lastname = Jones
```

If you want to capture different information in the registration process, you can create a customized Guest Registration page by creating your own Guest Registration page template. See "Customized Page Templates" for more information.

Customizing the Stop Page

By customizing the logo in the top section of the Customization page, the new logo also affects the Stop page and the Logoff page.

If you want to change the text that appears on the Stop page, or the graphic (the Stop sign) you can do that as well.

To change the text for the Stop page:

Step 1. Go to the Stop page area of the Customization page (see Figure 9-11).

Step 2. Under **Stop Page Text**, type the path and name (case-sensitive) of a text file or HTML file that contains the content you want to display on the Stop page, or click **Browse** to locate the proper directory and file name.

Step 3. Click **Update**.

To clear the Stop page text after it has been set, click **Restore Defaults**.

The grey area below the Filename field displays the text currently configured to appear on the page.

To change the graphic for the Stop page:

Step 1. Under **Stop Page Graphic**, type the path and name (case-sensitive) of a GIF, JPEG, or PNG file or other browser-compatible file format that contains the graphic you want to use or click **Browse** to locate the proper directory and file name.

Step 2. Click **Update**.

To restore the default Stop page graphic, click **Restore Defaults**.

Figure shows the Stop page with the default text and Stop graphic, but with the customized logo.

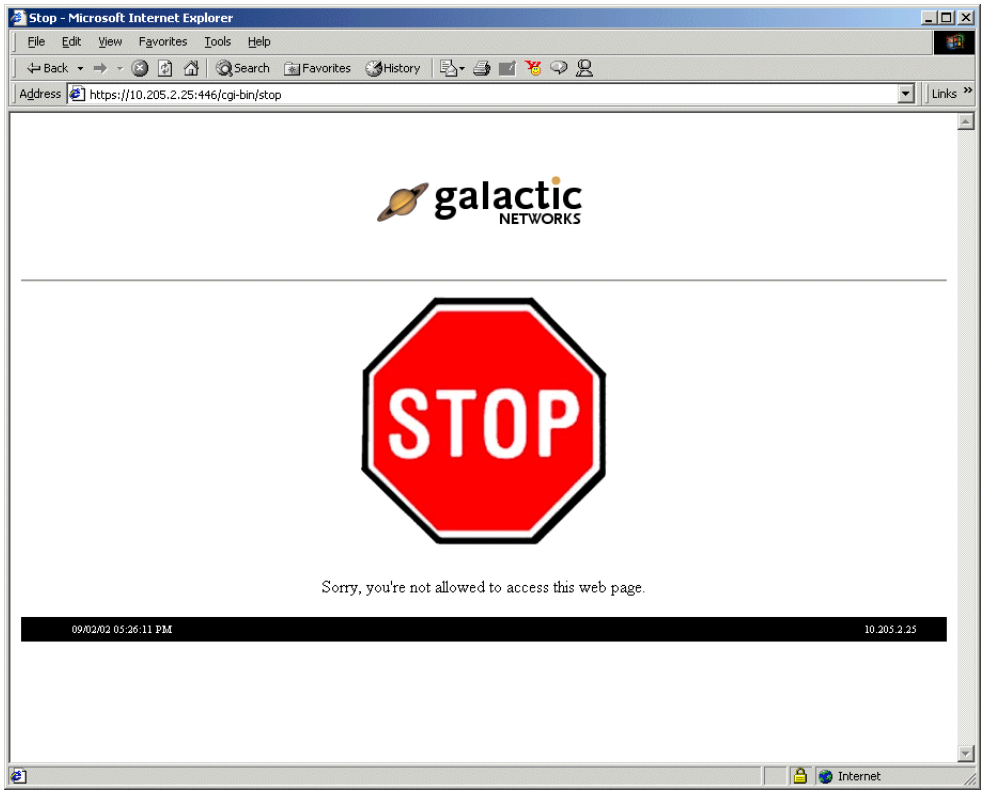

Figure 9-14. Stop page with custom logo, default text and Stop graphic

Logoff Page Options

When a user logs on, by default no logoff option is presented. Instead, the user is logged off by the Rights Manager automatically either when his or her rights expire or when he or she disconnects from the network. However, if the user goes to the logon page again while he/she is still logged on, the logon page indicates that the user is already logged on and provides a logoff button.

As an option, you can have a small logoff page open in a new window as soon as the user successfully logs on. The user can go to this page to logoff.

To specify that a logoff pop-up should be displayed:

Step 1. Scroll to the Logoff page options portion of the Customization page. Figure 9-15 shows the bottom portion of the Customization page, with the Logoff page options at the top.

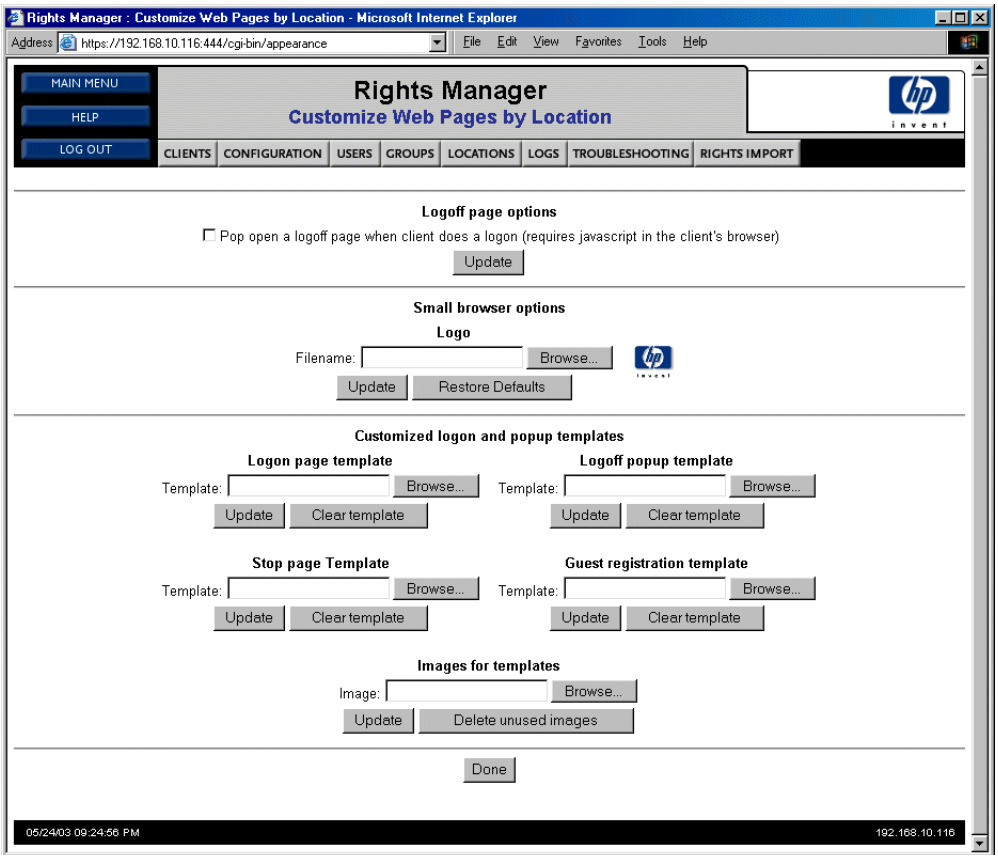

Figure 9-15. Customizing Web pages for a location, top part of page

Step 2. Click the option **Pop open a logoff page when client does a logon** in the Logoff Page Options section of the Customization page.

Note that this requires that the client browser be configured to use JavaScript.

Step 3. Click **Update**.

Figure 9-16 shows the default Logoff page. If you have customized the logo, your logo replaces the HP logo.

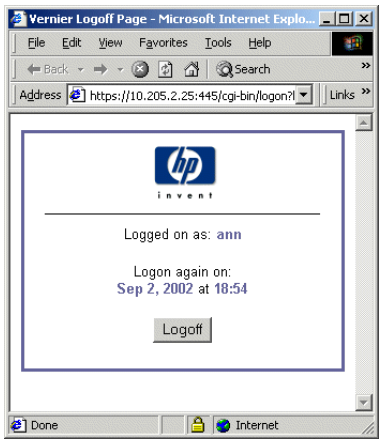

Figure 9-16. Logoff page

Small Browser Options

For clients with small browser screens, such as PDAs or mobile phones, the Rights Manager provides a small logo more appropriate to the size of a small screen. You can also specify a small logo for use with small browsers.

To change the graphic for a small-screen browser:

Step 1. Go to the Small browser options area of the Customization page, as shown in Figure 9-15.

Step 2. Type the path and name (case-sensitive) of a GIF, JPEG, or PNG file or other browser-compatible file that contains the graphic you want to use or click **Browse** to locate the proper directory and file name.

Step 3. Click **Update**.

To restore the default small browser graphic, click **Restore Defaults**.

Customized Page Templates

If you want to create pages that are customized beyond the options provided on the Customize Web Pages by Location page, you can create your own templates for the Logon, Logoff, Stop, and Guest Registration pages. Through a template you can lay out the pages in any way you want, including changing the position and even the labels of the buttons, and using other HTML elements as you see fit. For example, in a Guest Registration page you could include input fields to gather any user information you want.

A template or ***tmpl file*** contains the desired page output (in HTML) interspersed with various ***tmpl functions*** that perform operations within the Rights Manager as well as other useful functions such as control flow. Each invocation of a tmpl function is replaced in the file output by the value returned by that function. The Rights Manager takes the template file, evaluates and replaces the tmpl function with their generated values, and outputs the resulting page.

Appendix B, “Creating Customized Templates” describes in detail how to create these templates.

Note: *The template files interact with the Logon Page Options and the Logoff Page Options on the Customize Web Pages by Location page in the same way that the built-in pages do. If you want your page to use the Guest Registration page instead of Guest Logon, you must select that option under the Logon Page Options. The same is true for the Logoff page popup. Just providing a template for the Logoff page or the Guest Registration page is not sufficient—if you do not check the appropriate option, those pages will not be used.*

To use a customized template:

Step 1. In the appropriate **Template:** field, type the path and name (case-sensitive) of a `.tmpl` file that contains the template, or click **Browse** to locate the proper directory and file name.

Step 2. Click **Update**.

A confirmation noting the date and time of the file update is displayed immediately below the field where you added the file.

Note: *The Template field is cleared after you update the template file. You can tell if a template file is in use by the presence of the “Last Update at ...” message. If the default web page is in use, no message appears.*

Step 3. To clear a template file and return to the default (built-in) page, click **Clear Template**.

The default page is restored and the “`Last Update at...`” message is removed.

If your template uses any images, you must add them in the Images for Templates field. This places the images in the Rights Manager images directory where they can be accessed when your page is displayed. If you do not add them in this way, the images will be missing in your output page.

Step 4. Type the path and name (case-sensitive) of the image file (GIF, JPG, PNG or other browser compatible file) in the **Image:** field or click **Browse** to locate the file.

Step 5. Click **Update** to add the file to the Rights Manager.

To delete any unused images, click **Delete unused images**.

Wireless Data Privacy Logon (PPTP/L2TP Clients)

Wireless Data Privacy Logon uses the PPTP or L2TP client credentials for client authentication. In this situation, the 700wl Series system just acts as a VPN termination, and passes the client credentials (user name and password) on to a RADIUS or Built-in authentication service for authentication.

There are two steps to configuring Wireless Data Privacy logon for a location:

- Specifying the type of encryption, and whether it is required or allowed
- Specifying (if appropriate) the authentication mechanism that should be used for PPTP or L2TP

In addition, you must globally enable wireless data privacy on your Integrated Access Manager or Access Control Server, and specify how inner-tunnel IP addresses are to be assigned. For a more detailed explanation of wireless data privacy as supported by the 700wl Series system, see Chapter 3, “Wireless Data Privacy”.

To configure wireless data privacy logon for your locations:

Step 1. From the Rights Manager Configuration page, click **Encryption/Authentication per Location**.

The Encryption / Authentication per Location page appears, as shown in Figure 9-17.

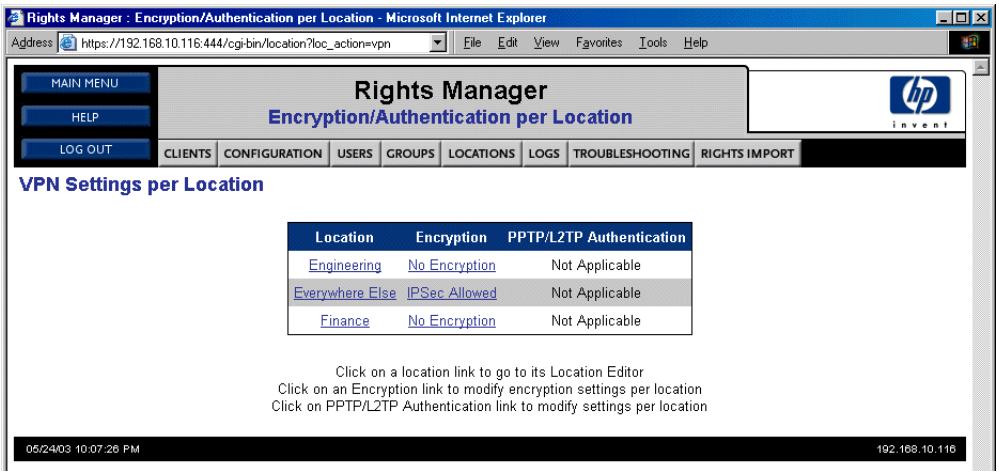

Figure 9-17. VPN Settings per Location

This page shows the locations configured in the Rights Manager, with the current Encryption and PPTP / L2TP Authentication options for each location.

Step 2. To configure the Encryption options for a location, click the link in the Encryption column for that location.

Step 3. To configure the PPTP / L2TP options for a location, click the link in the PPTP / L2TP Authentication column for that location.

You can also click the Location name to go to the Location Editor.

Encryption Options by Location

By default, encryption is disabled. You can select which of the four encryption types (IPSec, PPTP, L2TP / IPSec, and SSH encryption) should be allowed, and specify whether encryption should be required rather than just allowed at the location. You can also require encryption except for selected groups.

Step 1. To change the encryption options for a location, click the link in the Encryption column for that location.

The Encryption per Location page appears, as shown in Figure 9-18.

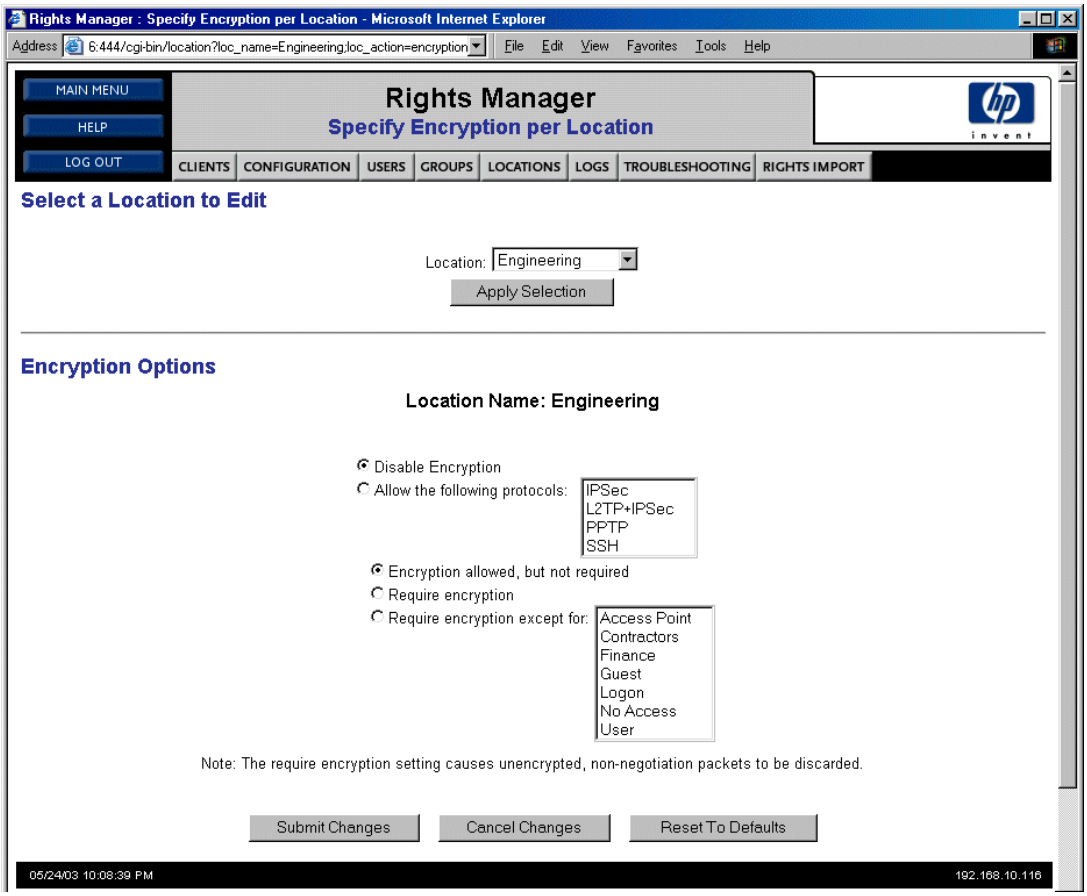

Figure 9-18. Specifying encryption options for a location

The settings for the location you selected should already be displayed.

- To change the settings for a different location, highlight the location from the drop-down list and click **Apply Selection**.

Step 2. To disable encryption at this location, click **Disable Encryption**.

Step 3. If encryption should be allowed, click **Allow the following protocols** and select the protocols you want to allow from the list. You can select multiple protocols; the method for doing this depends on your browser, but typically holding down the SHIFT or CTRL key while you click allows you to select multiple items.

Note: *Since Microsoft links L2TP with L2TP IPSec, the 700wl Series system assumes L2TP on IPSec. Enabling or requiring L2TP implicitly enables the use of IPSec. However, if your L2TP client allows use of L2TP without IPSec, then the 700wl Series system will use L2TP with MPPE.*

Step 4. Click to select one of the following:

a. **Encryption allowed but not required** to specify that the location will accept both clients that are using wireless data privacy with one of the allowed encryption protocols, and clients that are not using wireless data privacy.

b. **Require Encryption** to specify that all clients connecting to this location must use one of the allowed security protocols.

Note: *Requiring encryption means that any client not using the appropriate encryption protocol will not even see a logon page at this location.*

c. **Require Encryption except for** to specify that clients are required to use one of the allowed encryption protocols unless they are a member of one of the selected groups.

Select one or more groups from the list of groups.

For example, you might want to require encryption for all regular users, but allow Guests to log in without encryption to view selected web pages.

Caution: *If you want to make encryption required except for certain groups, you must include the location's logon group in the list of exceptions. If you do not, the users of the exempted groups will not be able to log on, since encryption would be required for the logon group.*

If you want to require encryption except for members of a certain group, there are several recommended practices that can make this work smoothly:

- Be sure to include the location's logon group in the exception list. Otherwise, no client without encryption will be able to log in, even if they are a member of the exempted group.
- If you exempt the logon group from encryption, it is recommended that you customize the logon page to display a message letting users know that encryption is required at that location unless they are members of a certain group. This is because all clients, with or without encryption, will have access to the logon page, even if they are not members of the exempted groups. A message will lessen confusion among users who are allowed to log in but then have no access rights.

Step 5. Click **Submit Changes** to have your changes take effect.

- To cancel any changes that you have not yet submitted, click **Cancel Changes**.
- To return these settings to their default settings, click **Reset to Defaults**.

PPTP/L2TP Options by Location

When you configure a location to use PPTP or L2TP, you must decide how to do PPTP and L2TP user authentication. For PPTP only, you must also specify the strength of MPPE (RC4) encryption to use.

There are three ways to perform PPTP and L2TP user authentication at a location. You can do the authentication through a RADIUS authentication server; you can use the Rights Manager's built-in username and password database, or you can use a shared secret.

If you choose to use RADIUS or built-in authentication, the 700wl Series system uses the PPTP/L2TP authentication both to authenticate the PPTP and L2TP connection and to authenticate the user to the 700wl Series system.

If you choose the shared secret, all users at this location must enter the specified shared secret when establishing their L2TP / PPTP tunnel. The 700wl Series system only uses the shared secret to set up the L2TP / PPTP connection. The user is required to authenticate to the 700wl Series system through the usual web-based logon page.

Caution: *Using a shared secret is inherently insecure and is not recommended. It is provided as a convenience for sites who cannot or choose not to use RADIUS or the built-in authentication service.*

To change the PPTP / L2TP Authentication options for a location:

Step 1. From the Encryption / Authentication per Location page, click the link in the PPTP / L2TP Authentication column for that location.

The Encryption per Location page appears, as shown in Figure 9-19.

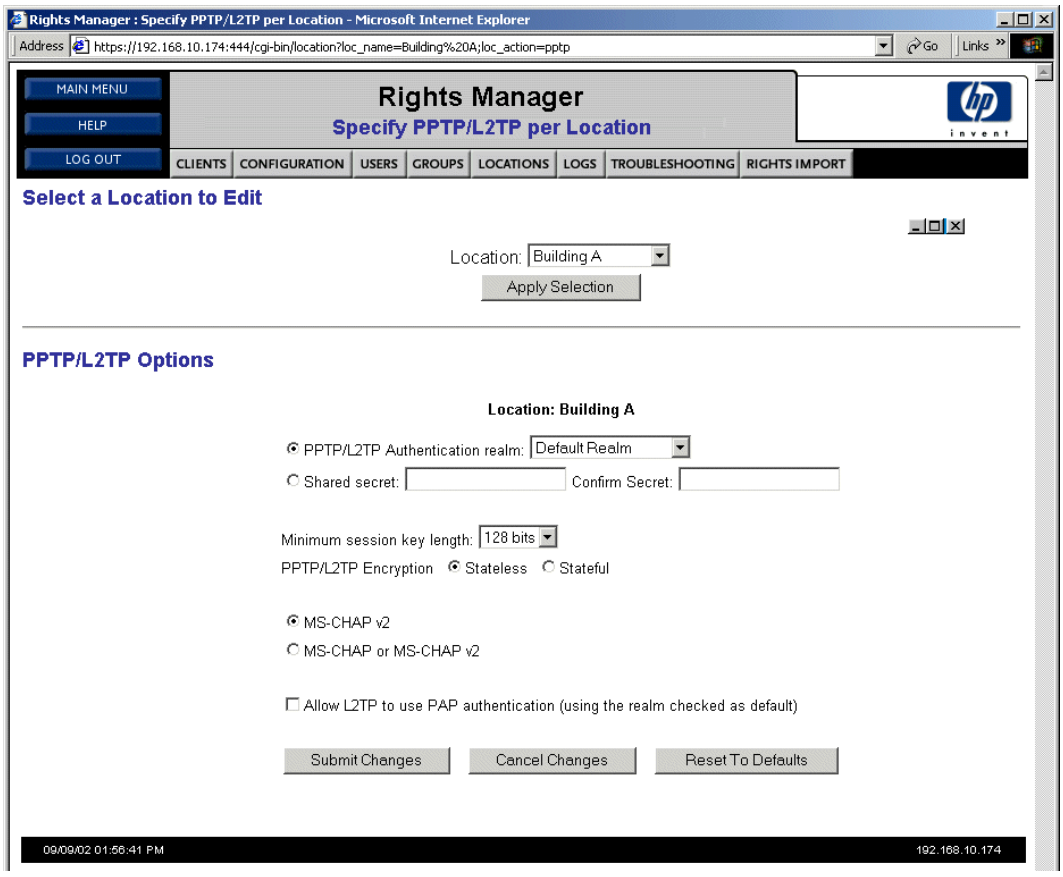

Figure 9-19. Specifying L2TP/PPTP Authentication options for a location

The settings for the location you selected should already be displayed.

- To change the settings for a different location, highlight the location from the drop-down list and click **Apply Selection**.

Step 2. Select the authentication method you want to use:

a. To use a RADIUS authentication service or the Built-in authentication service, click PPTP/L2TP Authentication realm: and select from the drop-down list the authentication realm that should be used.

Note: *Unless you are using the L2TP plus PAP option (see Step 6), your domain must include a RADIUS or built-in authentication service. If you select a realm that does not include one of these types of services, no users will be able to authenticate.*

b. To use a shared secret, click **Shared Secret** and type and confirm the secret.

Note: *The shared secret is presented by the user as the password for determining if the user is authorized to create a PPTP tunnel.* ***It is not used for authentication****. Once the connection is made, the user is then presented with the web-based logon page, is authenticated against the appropriate authentication service to determine what access is allowed to the network.*

Step 3. For L2TP or PPTP with MPPE, select the **Minimum session key length** from the drop-down list.

This sets the minimum key length for the MPPE (RC4) session key used to encrypt a session. The default value is 128 bits; alternate value is 40 bits.

Step 4. Select whether MPPE encryption should be **Stateless** or **Stateful**.

Stateful means the encryption key is reset once every 256 packets. This is better in a low packet-loss environment, and is faster.

Stateless means the encryption key is reset for every packet. This is better in a lossy environment, but is slower. This is the default.

Step 5. Click to enable either **MS-CHAP v2** or to enable **MS-CHAP or MS-CHAP v2**.

Step 6. To allow L2TP to use PAP for authentication, click the **Allow L2TP to use PAP authentication** checkbox. This will use the authentication services in the realm that you selected as the PPTP/L2TP authentication realm. In this case, there is no restriction on the type of service that must be used for authentication.

Step 7. Click **Submit Changes** to have your changes take effect.

- To cancel any changes that you have not yet submitted, click **Cancel Changes**.
- To return these settings to their default settings, click **Reset to Defaults**.

Monitored Logon (802.1x and NT Domain Logon)

Monitored logon refers to logon and authentication that is handled externally to the 700wl Series system, such as 802.1x logon or NT Domain logon. Monitored logon is enabled by individual Wheres. This lets you configure 802.1x or NT Domain logon port-by-port, if necessary.

Note: *You must define at least one Location and one Where in order to use monitored logon, because these methods are enabled by Where. You cannot use the default Everywhere Else location because it does not include a configurable Where.*

If you enable either of these authentication methods, the Rights Manager monitors the packets from clients connecting through that Where to determine if they are attempting 802.1x or NT Domain logon. If so, the 700wl Series system just passes the logon packets through to the network, and monitors the responses to determine if the client has been successfully authenticated. Clients in this case will not see the web-based logon interface, and will *not* be authenticated using any of the authentication realms or services you may have defined within the Rights Manager.

Note: *With NT Domain logon, user names cannot use "$" as the last character of the name.*

Monitored Logon options are found under the Configuration page in the Rights Manager.

Enabling 802.1x or NT Domain Logon

To enable monitored logon for one or more Wheres, do the following:

Step 1. From the Rights Manager, click **Configuration**.

Step 2. Under the Monitored Logon heading, click **Enable 802.1x/NT Logons per Where**.

The Enable 802.1x / NT Logons per Where page appears (Figure 9-20).

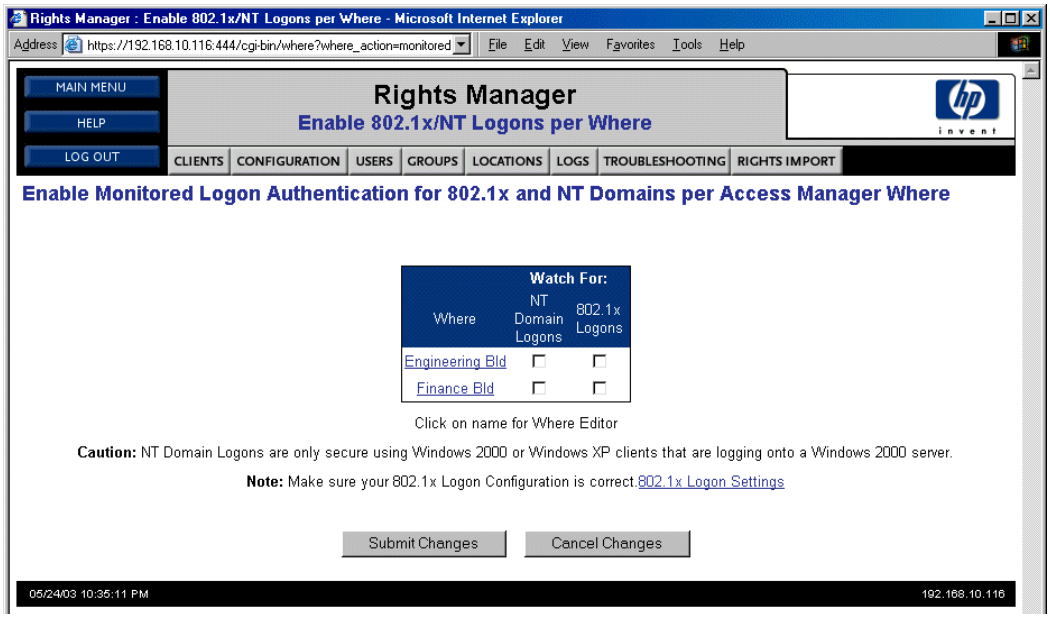

Figure 9-20. Enabling 802.1x and NT Domain logon, by Wheres

The table lists all the Wheres currently defined in the Rights Manager.

Step 3. Click the appropriate checkboxes to watch for NT Domain logon, and / or 802.1x logon.

Step 4. Click **Submit Changes** to have these settings take effect, or **Cancel Changes** to reset.

For 802.1x logon, you must also configure the Rights Manager to communicate with the RADIUS server used to authenticate clients using 802.1x. See "802.1x Logon Settings" for more information.

If you have a default authentication service configured, that service is ignored for clients using 802.1x authentication or NT Domain logon. If you do not plan to use any other authentication methods, you do not need to configure any other authentication services. By default the Built-in database is designated as the default authentication realm. If you do not plan to create specific groups to determine rights, you do not need to create any groups or add users to the built-in database.

Monitored Logon and Groups

If you want to use the Groups feature with monitored logon to specify access rights, there are several ways to do so.

For 802.1x logon, you can retrieve group membership information when the user is authenticated by specifying the field that holds the group name.

For NT Domain logon, you can create a group that matches the name of the client's logon domain. The Rights Manager can use the logon domain as the group name. You must select the **Matches a Windows NT Domain Name** option in the Group Editor when you create the group (see "Adding or Modifying a Group—the Group Editor" in Chapter 7).

There are also two other ways you can associated a user with a group:

- Use external group retrieval to get group membership information from an external LDAP service. See "Retrieving Group Information from an External Service" for more information. You must have groups set up that correspond to the group names retrieved from the external service.
- Add the clients' user names to the built-in database, and assign them group membership as appropriate. See Chapter 10, "Setting Up Users" for more information.

802.1x Logon Settings

For 802.1x logon, the 700wl Series system Rights Manager needs to view the authentication response from the RADIUS server that is handling the 802.1x authentication. Therefore, you must configure the Rights Manager to be able to communicate with the RADIUS server used for 802.1x authentication.

To specify the RADIUS server used for 802.1x authentication:

Step 1. From the Rights Manager, click **Configuration**.

Step 2. Under the **Monitored Logon** heading, click **802.1x Logon Settings**.

The 802.1x Logon Settings page appears (Figure 9-21).

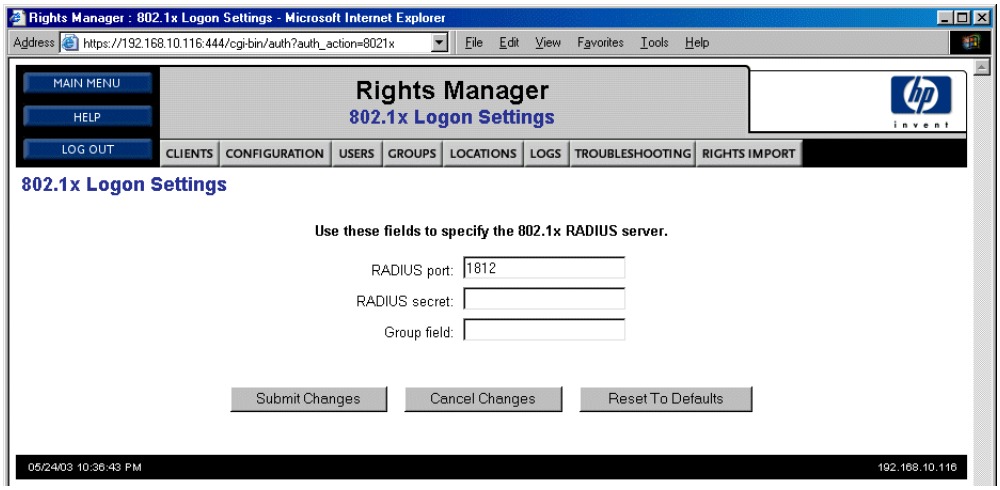

Figure 9-21. Setting up RADIUS for use with 802.1x logon

Step 3. Type the port number for the RADIUS server into the **RADIUS port** field. The default port number is 1812.

Step 4. Type the RADIUS shared secret into the **RADIUS secret** field.

Step 5. If you want to retrieve group information from the RADIUS database upon logon, type into the **Group field:** the name of the database field where a user's group information is stored.

Step 6. Click **Submit Changes**.

Retrieving Group Information from an External Service

If the service you use for user authentication does not provide group information, you can retrieve group information from an LDAP service, post-authentication, without using that service for authentication. For example, if you use a monitored logon such as NT Domain login or 802.1x authentication, you might want to retrieve group information from an LDAP directory service for each user that is successfully authenticated.

Setting up post-authentication group retrieval involves two procedures:

- First, you must configure an LDAP service to be used to retrieve the group information. You must specify **Non-User binding**—either `rootdn`/`rootpw` binding or anonymous binding (if the service allows anonymous bind). See "Configuring an LDAP Authentication Service" for details on how to set up an LDAP service.
- Second, you specify the LDAP service(s) you want to use for group retrieval.

To set up group retrieval from an external directory source, do the following:

Step 1. From anywhere in the Rights Manager, click **Configuration**.

Step 2. Click the **External Group Retrieval** link under the Global Settings heading. Figure 9-22 shows the Setup External Group Retrieval page.

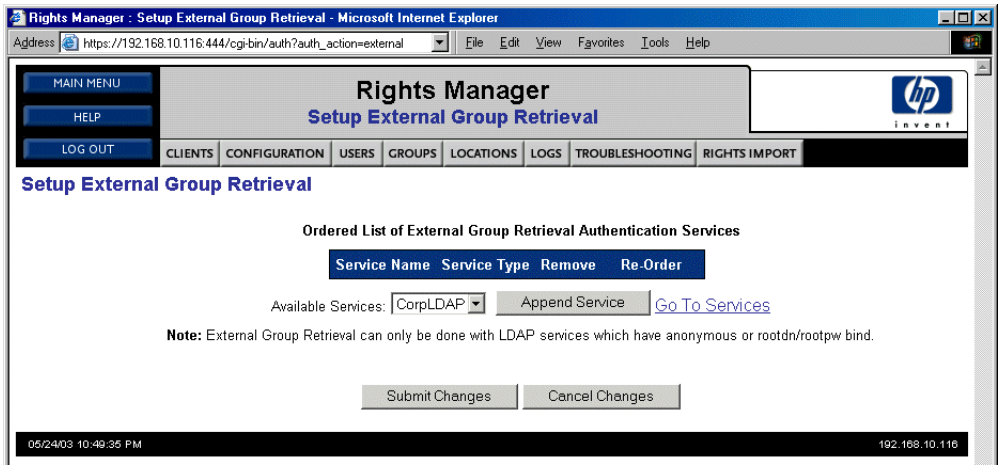

Figure 9-22. The Setup External Group Retrieval page

Step 3. If you already have one or more LDAP services that use anonymous or `rootdn`/`rootpw` binding, those services appear in the Available Services drop-down list.

If you do not have any such services set up, click the **Go To Services** link to create one.

Step 4. From the Available Services drop-down list, highlight the service you want to use for external group retrieval, and click **Append Service**.

This adds the selected service to the Ordered List of External Group Retrieval Authentication Services. Figure 9-23 shows this page after a two services have been added.

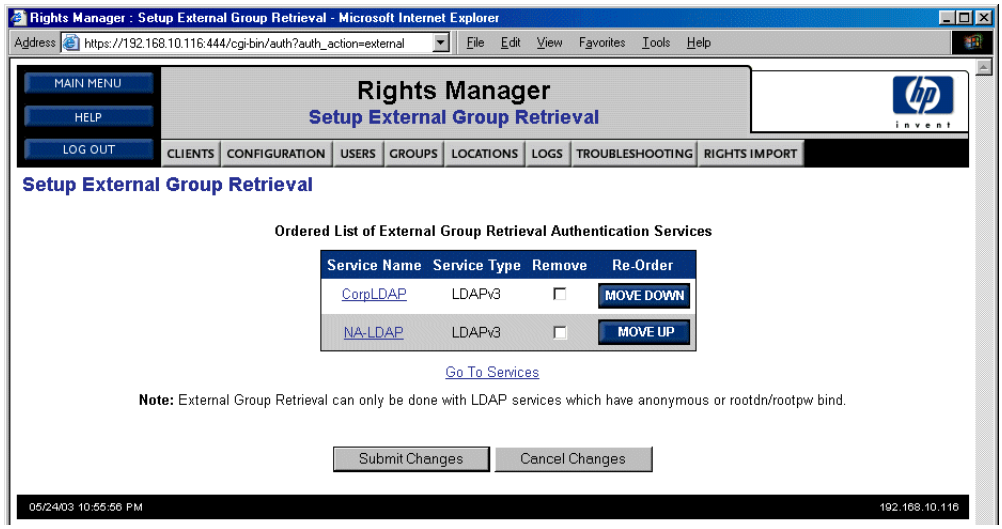

Figure 9-23. List of services to use for External Group Retrieval

Step 5. If you have several services that should be searched for group membership, they must appear in the Ordered List of External Group Retrieval Authentication Services

list in the order in which they are to be searched. After you've added them to the list, you can change their order using the **Move Up** and **Move Down** buttons.

These buttons do not appear if there is only one service in the list.

Step 6. Click **Submit Changes** to have your changes take effect, or **Cancel Changes** to abandon your changes.

Step 7. To remove a service from the list, check the box in the Remove column, and click **Submit Changes**.

Retrieving MAC Addresses from an LDAP Directory

The Rights Manager's built-in database can be used to keep the MAC addresses of Access Points and other client devices that should be authenticated based on their MAC address rather than by a user ID / password. Whenever a new client is detected through an Access Controller, the built-in database is searched for the MAC address associated with the client. If the MAC address is found in the built-in database, that client is immediately granted an appropriate set of access rights based on the group membership affiliation maintained in the database. Login via a userID and password is not required.

If an organization has a large number of these types of clients, it may be impractical to add or update MAC addresses in the built-in database by hand. In addition, some organizations may already keep an inventory of such devices in an external database. The Retrieve MAC Address Users via LDAP feature allows the built-in database to be populated and periodically updated with MAC address users and their group affiliations as maintained in an external LDAP database.

Setting up MAC address retrieval requires several steps:

- Configuration of an LDAP authentication service (with non-User binding)
- Adding the LDAP service to a list of services from which MAC addresses can be retrieved
- Configuring the retrieval specifications, including the interval for refreshing the MAC addresses in the built-in database
- Enabling retrieval from the specified LDAP services

In addition to retrieving MAC addresses on a scheduled basis, you can also initiate an immediate retrieval to update addresses upon demand.

This feature assumes that the LDAP database has one record that contains a set of attributes whose values define all the MAC addresses to be retrieved. For example, suppose you have a record, defined with `objectClass=groupofuniquenames`, and identified by the cn `MACS`, that contains MAC addresses in the attribute `uniqueMember`.

If you do not have group membership information kept in the LDAP directory, then the value of `uniqueMember` could simply be the MAC address. In this case, the record identified by `cn=MACS` could contain the following values for `uniqueMember`:

```
uniqueMember: 000122034a5b
uniqueMember: 01234567891a
uniqueMember: 22314a6721b7
```

These values will be taken as the MAC addresses and added to the built-in database.

If the value of the attribute has multiple components, the first component is assumed to be the MAC address itself; subsequent components may optionally be included to define a search string that identifies an individual record for the MAC address. For example, suppose the record identified by `cn=MACS` contained the following values for `uniqueMember`:

```
uniqueMember: cn=000122034a5b, o=XYZCorp, c=us
uniqueMember: cn=01234567891a, o=XYZCorp, c=us
uniqueMember: cn=22314a6721b7, o=XYZCorp, c=us
```

The value of cn will be taken as the actual MAC address, and added to the built-in database. The entire string can be used as the search string to find the individual record for the MAC address that contains an attribute that defines group membership for the MAC address user.

Group membership can be retrieved in one of two ways:

- If the LDAP database contains individual records for each MAC address user, an attribute in those records can define the groups to which the MAC address belongs.
- Records can be used to represent groups, each of which contains a set of MAC addresses that are members of that group.

Specifying the LDAP Service for MAC Address Retrieval

To set up MAC address retrieval from an LDAP service, do the following:

Step 1. From anywhere in the Rights Manager, click **CONFIGURATION**.

Step 2. Click the **Retrieve MAC Address Users via LDAP** link under the Global Settings heading. Figure 9-24 shows the Retrieve MAC address users via LDAP configuration page, with one LDAP service configured appropriately to allow MAC address retrieval.

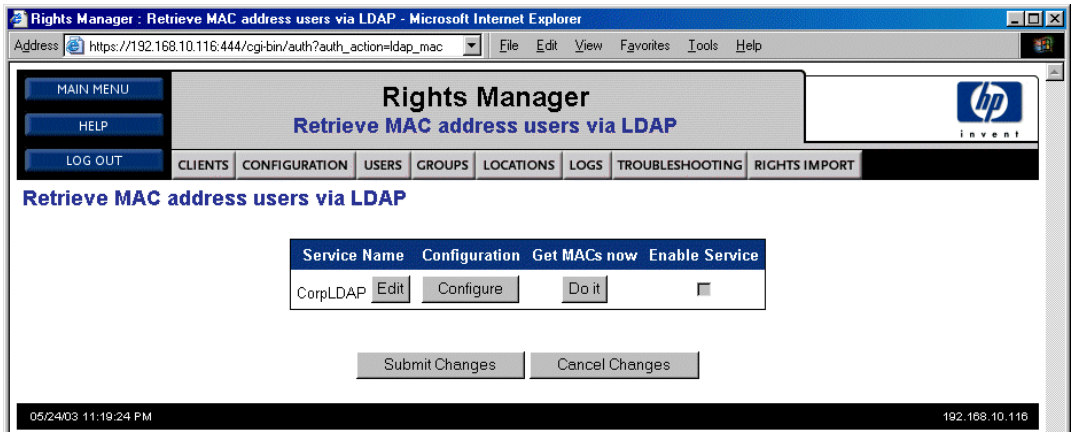

Figure 9-24. Retrieve MAC address users via LDAP setup

If there are any LDAP service configured that meet the requirements for use with this feature (specifically, they are set for non-User binding) they are displayed in the list. If there are no services in this list, you must configure at least one in order to use this feature.

Note: *If you have an LDAP service configured for User binding, that service does not appear in this list.*

» To configure an LDAP service, see “Configuring an LDAP Authentication Service” on page 9-5.

You can edit the settings of the LDAP service by clicking **Edit** next to the name of the service.

Configuring the Search for MAC Addresses

To configure the MAC address retrieval parameters:

Step 1. Click the **Configure** button in the row for the service from which you want to retrieve MAC addresses.

The Configure MAC Address User Retrieval via LDAP page appears, as shown in Figure 9-25.

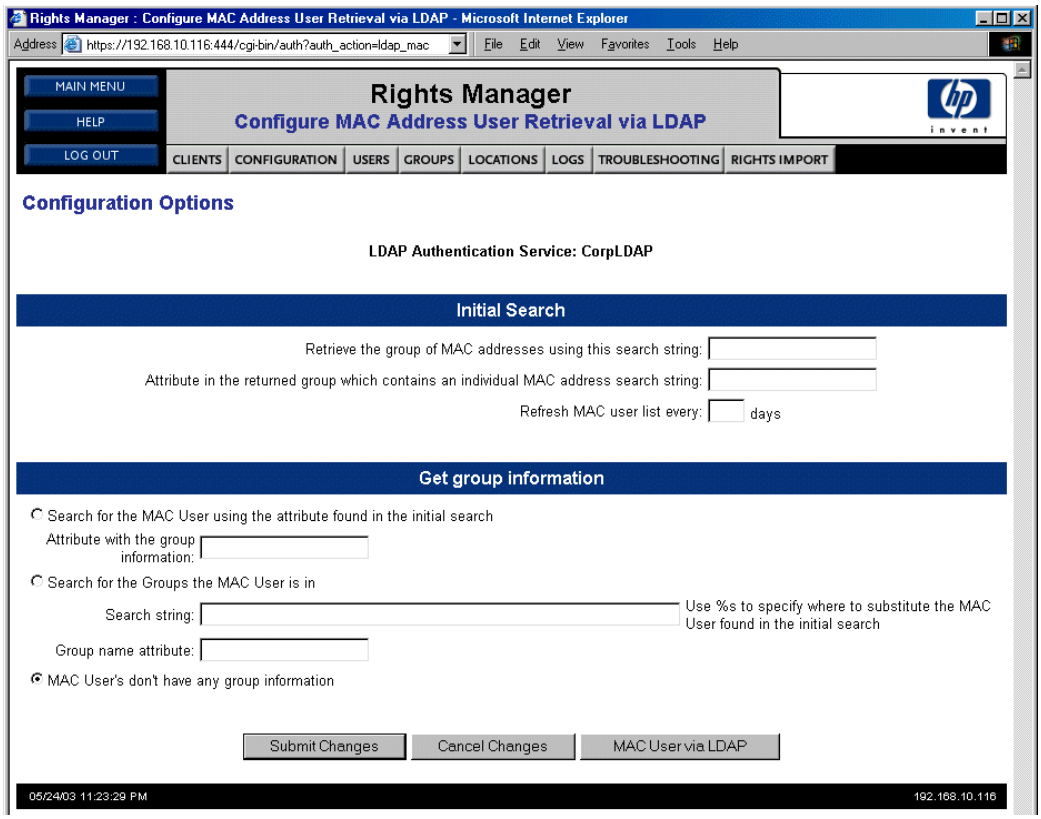

Figure 9-25. Configuring MAC address retrieval from an LDAP service

Step 2. Type the search string that specifies the group record in the database that contains the set of MAC addresses.

For example, the search string `cn=MACS` specifies that the list of MAC address users can be found in a record whose cn is MACS.

Step 3. Type the name of attribute in the record that contains the individual MAC addresses, for example, `uniqueMember`.

Instances of this attribute should contain the MAC addresses that are to be added to the 700wl Series system built-in database, as the first item in the attribute value. The value may also be used as the search string for retrieving group information for the MAC address user.

Step 4. Type a value for the number of days between refreshes of the MAC addresses in the 700wl Series system's built-in database. For example, enter "2" to have the database refreshed every other day.

If these MAC address users do not have group information kept in the LDAP database, you can submit these changes without specifying any further searches. In this case, when MAC addresses are retrieved, they will be added to the 700wl Series system built-in database with no group affiliation.

Configuring the Search for Group Information

Group membership information can be associated with a MAC address in one of two ways:

- If each MAC address has its own record in the database, its group membership information may be kept as an attribute in the record. The Rights Manager can then search for each MAC address record using the search string returned in the initial search, and retrieve the group information from the appropriate attribute.
- Additional groups may be used that include MAC addresses as members. The Rights Manager can then search for groups that contain the MAC address as a member, and return the name(s) of those groups.

The following examples illustrate this in more detail.

Retrieving Group Information from MAC Address User Records

Suppose, for each MAC address, an entry exists with attributes similar to the following:

```
dn: cn=000122034a5b, o=XYZCorp, c=us
cn: 000122034a5b, o=XYZCorp, c=us
sn: 000122034a5b
mymember: Contractors
mymember: DBSpec
```

Then, under the Get Group Information heading, do the following:

Step 1. Select **Search for the MAC User wising the attribute found in the initial search**.

This means that the Rights Manager will use the search string found in the initial search (for example, the value returned from the `uniqueMember` attribute in the `MACS` record) to search for the individual MAC address record.

Step 2. Type `mymember` in the field labeled **Attribute with the group information**.

The Rights Manager will look for instances of the attribute mymember, and take the values as group names. Then, assuming that these names match groups that exist in the Rights Manager, the MAC address user will be made a member of these groups.

For example, this configuration will return the groups Contractors and DBSpec for MAC Address User `00:01:22:03:4a:5b`.

Searching for Groups with MAC Address Users as Members

The second method for retrieving group membership assumes that you have multiple group objects, each of which contains a list of MAC address users. Group membership is retrieved by searching for each MAC Address, then returning the names of any groups in which that MAC address was found.

For example, suppose you have a second group in your LDAP database, identified by cn `CONTRACTORS`, also defined with `objectClass=groupofuniquenames`, that also contains MAC addresses in instances of the attribute `uniqueMember`.

In this case, under the Get Group Information heading, do the following:

Step 1. Select **Search for the Groups the MAC User is in**.

Step 2. In the **Search string** field, type a search string to use to find records that contain the MAC address in a specified attribute.

For example, to search for MAC addresses in the two records discussed in this section (identified by `cn=MACS` and `cn=CONTRACTORS`) you would use the search string:

```
(&(objectclass=groupofuniquenames) (uniquemember=%s))
```

This searches records of class `groupofuniquenames` for an attribute `uniquemember` whose value matches the current MAC address as retrieved by the initial search.

Step 3. In the **Group name attribute** field, type `cn`. This returns the value of the `cn` attribute, which is the name of the group in which the matching `uniquemember` was found.

This configuration will return the groups MACS and CONTRACTORS for MAC Address User `00:01:22:03:4a:5b`.

Configuring RADIUS Accounting

You can configure the Rights Manager to provide accounting information to a RADIUS accounting server, as defined in RFC 2866. RADIUS accounting gathers information at the start and end of a session about the resources (time, packets, bytes, etc.) that were used during the session.

You can use RADIUS accounting either in addition to or independently of using RADIUS for authentication. When you set up RADIUS for authentication, you can specify that it also be used for accounting. If you did not enable the accounting feature when you initially set up RADIUS authentication, you can modify the RADIUS method to include it. You can also create a new RADIUS method specifically to use for accounting.

To use a RADIUS service for accounting, you must do the following:

- In the RADIUS service configuration, check the **Supports RADIUS Accounting** option, and provide the appropriate port number

- On the Accounting Services page, check the **Enable** checkbox for each RADIUS service to which you want to send RADIUS accounting information

Configuring a RADIUS Service for Accounting

If you have a RADIUS service configured in the Rights Manager for user authentication, you can modify the configuration setting to support RADIUS accounting—see "Modifying an Existing RADIUS Service to Support Accounting" below for details.

To set up a new RADIUS service to support user accounting, follow these steps:

Step 1. From the Rights Manager, click the Configuration tab.

Step 2. Under the Authentication heading, click **Authentication Services**.

Step 3. Select **RADIUS** as the service type to add, then click **Add Service**.

The RADIUS authentication page appears, as shown in Figure 9-4.

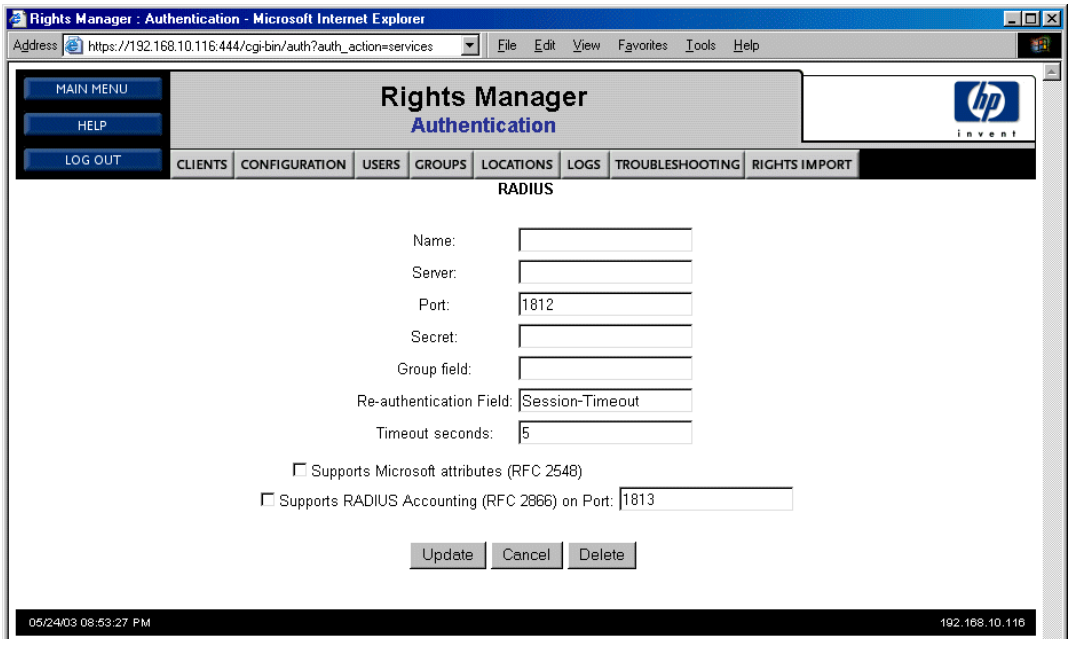

Figure 9-26. RADIUS Authentication page

Step 4. Enter the information requested.

A description of these fields is given in Table 9-3.

Table 9-9. RADIUS Authentication Options

Entry	Explanation
Name	Your name for this authentication method. You can use any alphanumeric string as the name.
Server	The Fully Qualified Domain Name (FQDN) or IP address of the server running the LDAP service.
Port	UDP Port for RADIUS (Default is 1812).
Secret	The shared secret for this RADIUS server.
Group Field	The RADIUS attribute that contains group membership information.
Timeout	Authentication timeout period (in seconds).
Supports Microsoft's attributes (RFC 2548)	Check this to indicate that the RADIUS server supports Microsoft vendor-specific RADIUS attributes. **Note:** You must check this if you will use this RADIUS server to authenticate a PPTP or L2TP session.
Supports RADIUS Accounting (RFC 2866)	Check this to indicate that the RADIUS server supports RADIUS accounting.
on Port	UDP port for RADIUS accounting (Default is 1813).

Step 5. For RADIUS Accounting, make sure you check the **Supports RADIUS Accounting** checkbox, and enter the UDP port for your RADIUS server accounting function, if it is different than the default (1813).

Step 6. Click **Update** when you are done.

Modifying an Existing RADIUS Service to Support Accounting

If you have a RADIUS service already set up for authentication, you can add support for the accounting function.

Step 1. From the Rights Manager Configuration page, under the Authentication heading, click **Authentication Services**.

Step 2. From the Authentication Service list, click the name of the RADIUS service that you want to modify.

The RADIUS Authentication page appears, similar to that shown in Figure 9-4, but displaying the settings for the existing service.

Step 3. Check the **Supports RADIUS Accounting** checkbox and enter the UDP port for your RADIUS server accounting function if it is different than the default (1813).

Step 4. Click **Update** when you are done.

Enabling RADIUS Accounting

To enable RADIUS accounting, do the following:

Step 1. From the Rights Manager Configuration page, under the Accounting heading, click **Services**.

The Rights Manager Accounting Services page appears, as shown in Figure 9-27.

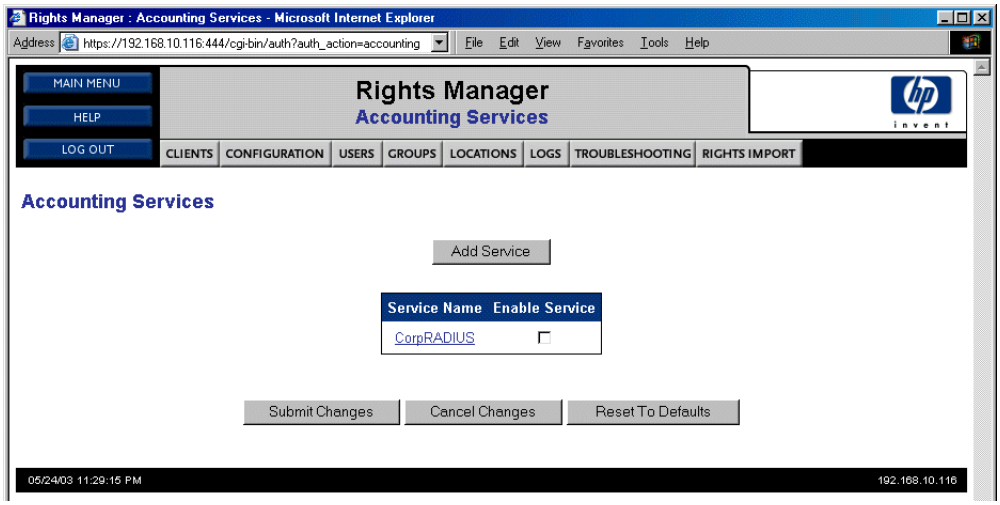

Figure 9-27. Rights Manager Accounting Services page

This page displays the RADIUS services that have been configured to allow accounting. This means they already have the **Supports RADIUS Accounting** option selected.

Step 2. To configure a new RADIUS service, click **Add Service**.

This displays the RADIUS authentication page, where you can set up a new RADIUS service to use for authentication and accounting. See "Configuring a RADIUS Service for Accounting" for instructions on configuring the RIghts Manager to use a RADIUS server. Be sure to check the **Supports RADIUS Accounting** checkbox.

Note: *To modify an existing RADIUS service to include accounting support, you can access the RADIUS configuration page from the Authentication Services page. See "Configuring a RADIUS Service for Accounting" for details of how to do this.*

Step 3. To enable RADIUS accounting using one of the RADIUS services in the table, click the checkbox in the Enable Service column for that service.

To disable accounting for a specific service, clear the checkbox for that service.

Step 4. Click **Submit Changes** to have your selections take effect.

Specifying a NAS-ID for Use with RADIUS Accounting

The RADIUS server expects to receive a NAS-ID — the name of the server that sent the accounting information — as part of the accounting information that is sent. By default, if no NAS-ID is set, the Rights Manager uses the MAC address of the Access Controller as the NAS-ID. However, you can specify a user-defined NAS-ID that will be sent instead of the MAC address. A user-defined NAS-ID may be more useful and "user-friendly" than the MAC address for purposes of identifying where the accounting information came from.

The NAS-ID is set in the Access Controller Editor. You may have entered a NAS-ID when you set up your Access Controllers as part of creating your Wheres. If you did not include a NAS-ID when you initially set up the Access Controller, you can add one through the Access Manager Editor.

Step 1. Click **Locations** from anywhere in the Rights Manager.

Step 2. Click **Edit/New Where** to display the Where Editor, then click **Edit/New AM**.

The Access Manager Editor appears, as shown in Figure 9-28.

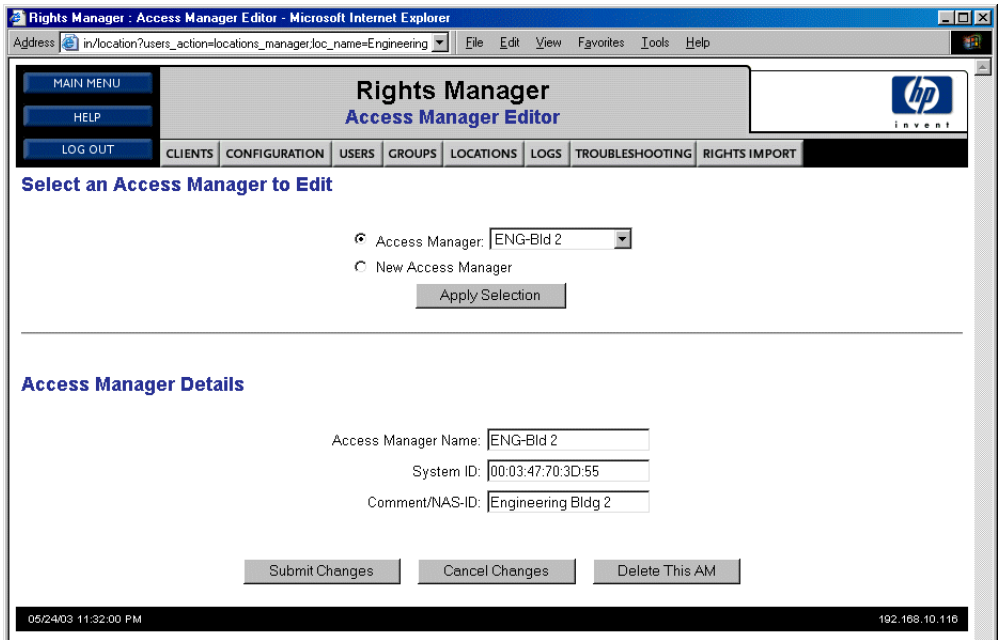

Figure 9-28. Access Manager Editor

Step 3. To modify the settings for an existing Access Controller, select **Access Manager**, then highlight the Access Controller you want to modify from the drop-down list.

Step 4. Click **Apply Selection**.

If you select an existing Access Controller, that Access Controller's properties appear in the fields below. Otherwise, the fields are blank, or are set to their default values.

See "Adding or Modifying an Access Controller" for more detailed instructions on adding an Access Controller.

Access Manager Details Section

Step 5. Type the Access Controller name **Access Manager Name** field.

Step 6. Type the **MAC address** of the Access Controller.

You can find the MAC address in the Access Controller Version and License screen.

Step 7. Optionally, type a descriptive comment or a NAS/ID. If you are using RADIUS accounting, the NAS-ID is sent to the RADIUS server as part of the accounting information.

Step 8. Click **Submit Changes** to configure a new Access Controller.

Click **Cancel Changes** to undo your changes if you have not yet submitted them.

Accounting Packet Data

The following fields are sent to the RADIUS Accounting server in the accounting packet sent at the start of a session:

Field	Data
User-Name	The user name (login name)
NAS-IP-Address	IP address of the Access Controller the client is connected through
NAS-Identifier	Administrator-specified string (NAS-ID) for the Access Controller or the MAC address of the Access Controller, if no NAS-ID is specified
Acct-Status-Type	Start (indicates a Start packet)
Calling-Station-ID	MAC address of the client
Called-Station-ID	MAC address of the Access Controller
Acct-Session-ID	A unique ID for this session

The following fields are sent to the RADIUS Accounting server in the accounting packet sent at the end of a session:

Field	Data
User-Name	The user name (login name)
NAS-IP-Address	IP address of the Access Controller the client is connected through
NAS-Identifier	Administrator-specified string (NAS-ID) for the Access Controller or the MAC address of the Access Controller, if no NAS-ID is specified
Acct-Status-Type	Stop (indicates a Stop packet)
Calling-Station-ID	MAC address of the client
Called-Station-ID	MAC address of the Access Controller
Acct-Session-ID	A unique ID for this session
Acct-Session-Time	The seconds this client was logged on this Access Controller. Sent only with a Stop packet

Note: *When a client roams to a new Access Controller, a Stop and a Start are sent to the Accounting server.*

SETTING UP USERS 10

This chapter shows you how to add, modify, or delete a user in the HP ProCurve Secure Access 700wl Series Rights Manager built-in database. It also explains how to add a client identified by its MAC address, or an Access Point, as a user. It includes the following sections:

The Built-In Authentication Database 10-1

Viewing Users—the Users Page 10-2

Adding or Modifying a User—the User Editor 10-4

Setting Up Access Point Users 10-6

The Built-In Authentication Database

The Rights Manager provides a built-in database that can be used for authenticating users if no other external Authentication service is available or appropriate. This database is simply a repository of the user names and passwords of users who are allowed to log on to the network, and group membership information for these users. A user's access rights are determined by his/her group membership, as rights are always associated with groups.

The built-in database may also contain the MAC addresses of clients that should be allowed to access the network without authenticating. MAC addresses are also associated with groups, which determine the access rights given to the client. MAC address that are actually Access Points can be given membership in the Access Point group, which provides an appropriate set of rights for the device.

The built-in database can also be used to assign group membership to users who are authenticated using a different authentication service. In this case, you can enter only their user name, and not the password.

You can populate the built-in database by adding users through the Rights Manager User Editor. The database can also be populated through the Registered Guest logon page, which is an option you can set in the Rights Manager Customize Web Pages by Location page. MAC addresses can be added through the User Editor, or through the Rights Manager Clients page (see "Setting Up MAC Address Users and Access Points"). They can also be added automatically on a periodic basis by downloading them from an LDAP database (see "Retrieving MAC Addresses from an LDAP Directory".

The built-in database may have a maximum of 5000 entries.

This chapter shows you how to add, modify, or delete users or MAC addresses in the Rights Manager built-in database. It also explains how to classify a MAC address as an Access Point.

Viewing Users—the Users Page

To access the Users page, do the following:

Step 1. From anywhere within the Rights Manager, click **Users**.

The Users page appears, as shown in Figure 10-1.

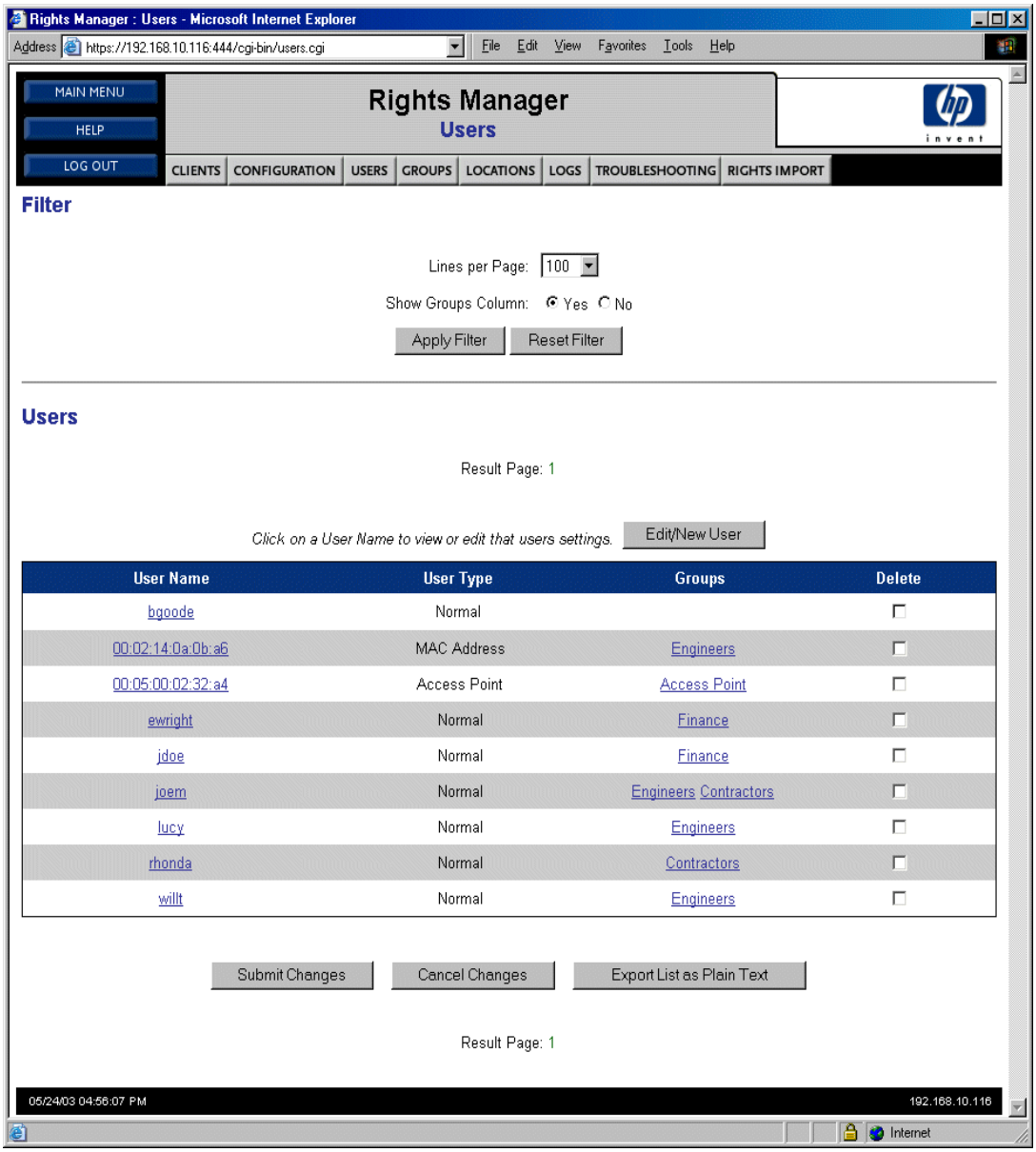

Figure 10-1. Users page

The Users page displays the users in the built-in database in a table. The contents of the table are defined in Table 10-1.

Table 10-1. Contents of the Users display

Column	Explanation
User Name	The user logon name. It is also a link to the User Editor.
User Type	The type of user (Normal, Registered Guest, MAC Address User, or Access Point).
Groups	A list of the Groups of which the user is a member. If this column is empty, the default Implicit Users group is assumed. Each group name is also a link to the Group Editor.
Delete	Click the checkbox to mark this user for deletion from the database.

Filtering the Display

If you have a large number of users, the Users table may be very long. The Filter function at the top of the page lets you control how many lines should be displayed on a single page, and whether the Groups column should be displayed.

- To change the number of lines on a page, select from the drop-down list in the **Lines** field the number of lines that should be displayed on the page, then click **Apply Filter**.

  You can choose 10, 25, 100, 1000, or an unlimited number of lines.

  If the table contains more lines that can fit on a single page, links to the other pages in the results (Next, Previous, and a list of page numbers) are provided at the bottom of the page.

- To hide the Groups column, click **No** for the **Show Groups Column**. To display the Groups, click **Yes**.

Exporting the User List

You can export the list of users to a plain text file.

» Click **Export List as Plain Text**.

The user list is displayed as plain text in your browser window. You can then print it or save it to a file. The information is exported exactly as displayed on the Users page. Each row of text includes the user name, the user type, and the list of groups to which the user belongs.

The list of users shown in Figure 10-1 produces the following text:

```
User Name    User Type    Groups       Delete
00:02:10:0a:ca:c7Access PointAccess Point
00:02:14:0a:0b:a6MAC AddressEngineers
00:05:00:02:32:a4Access PointAccess Point
ewright      Normal       Finance
jdoe         Normal       Finance
joem         Normal       Engineers Contractors
lucy         Normal       Engineers
rhonda       Normal       Contractors
willt        Normal       Engineers
```

Adding or Modifying a User—the User Editor

To add a regular user to the built-in database, do the following:

Step 1. From the Users page, click **Edit/New User**, or to modify an existing user, click the user name.

The User Editor appears, as shown in Figure 10-2.

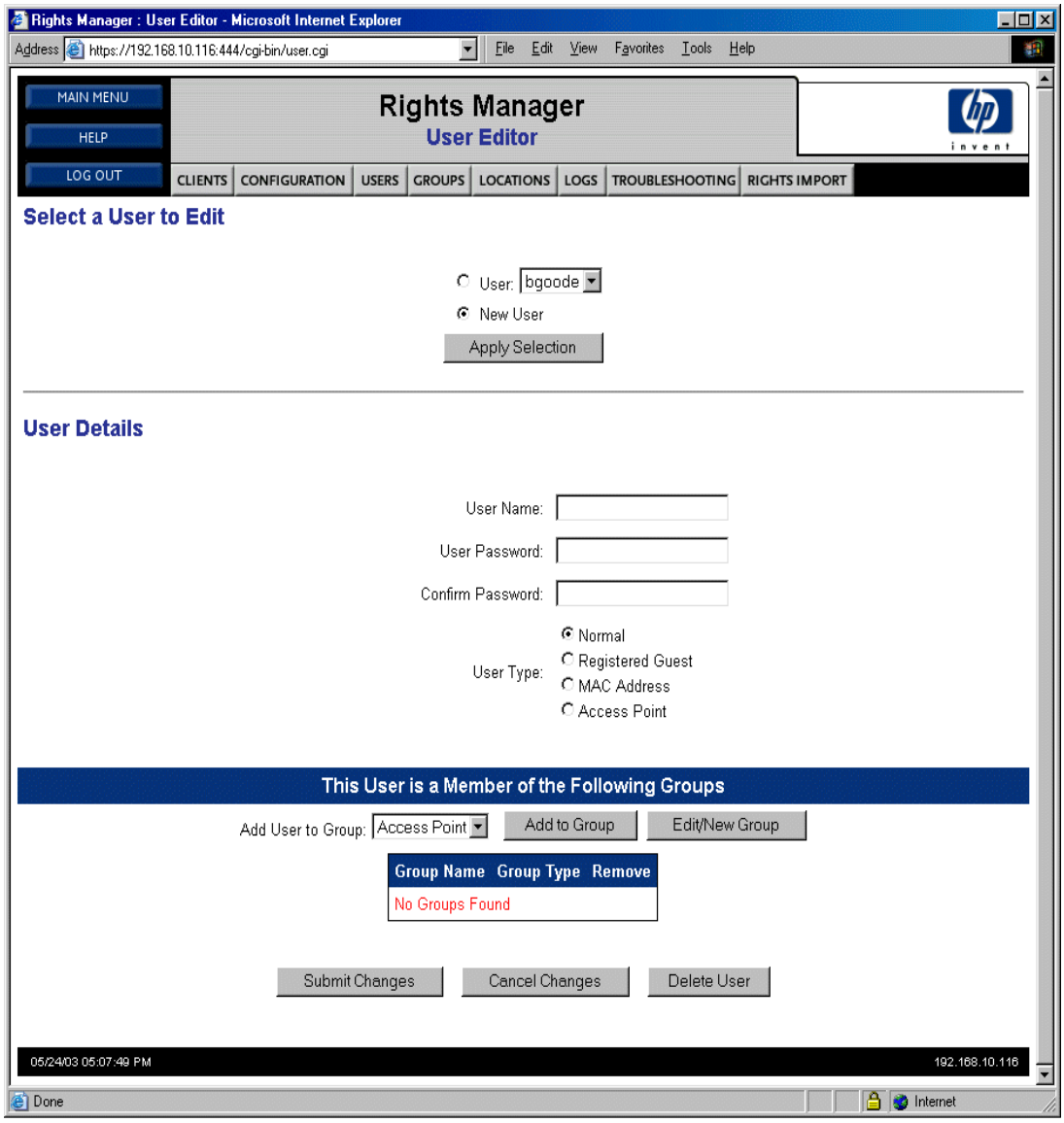

Figure 10-2. The User Editor

Step 2. To create a new user, select **New User**.

To modify the settings for an existing realm, select **User**, then highlight the user you want to modify from the drop-down list.

Step 3. Click **Apply Selection**.

If you selected a user name, that user's properties appears in the fields. Otherwise the fields are empty.

User Details

Step 4. Type the **User Name**.

- If the user is authenticated through an external authentication service, make sure the user name you enter here matches their authenticated user name.

  The user name (and password) may be up to 256 characters in length, and may contain any character except for a colon (:).

- If the "user" is really a client or Access Point identified by MAC address, type the MAC address. You can enter it with or without colons between the tuples, for example: `00:05:A3:16:00:02` or `0005A3160002`

  You can also use the wildcard character "*" (asterisk) as the last character to create a wildcard MAC address. The asterisk can replace any number of digits or tuples (including all), but must always be the last character in the address. For example, the following are valid wildcard MAC addresses:

  ```
  00:05:A3:16:00:*
  00:05:A3:16:0*
  00:05:A3:*
  0005A3*
  *
  ```

  The wildcard character cannot be used in the middle of the string: `00:05:A3:*:00:02` is not a valid wildcard MAC address.

Step 5. Type the user's password in the **User Password** field, and type it again in the **Confirm Password** field.

Note: *If you use an LDAP, RADIUS, or Kerberos service for user authentication, and use the built-in database only for group association, the password fields are not available.*

Step 6. Select the type of user:

- If this user will logon and be authenticated normally, select **Normal**.
- If you want this user to have Guest rights only, select **Registered guest**.
- If the user is a client identified by a MAC address, click **MAC Address**.
- If the "user" is really an Access Point, click **Access Point**.

Step 7. Add the user to any groups of which he/she should be a member.

a. Select a group in the **Add User to Group** drop-down list.

b. Click **Add to Group**.

The group should appear (along with its type) in the user's list of groups.

There are several caveats related to adding users to groups:

- You cannot add users to a Logon, Guest, or Implicit User group. Users are automatically made members of the Logon and Guest groups as appropriate. All users are automatically members of the implicit Users group.

- A Registered Guest cannot be added as a member of any groups (other than the Guest group, which is automatic). If you attempt to add a registered guest user to a group, a warning message appears when you submit your changes, and the user is not added to the group.
- Only Access Point users can be members of the Access Point group. If you attempt to add other types of users (including MAC Address users) to this group, a warning message appears when you submit your changes, and the user is not added to the group.

If you need to add a new group, click **Add/New Group**. This displays the Group Editor. See "Adding or Modifying a Group—the Group Editor" in Chapter 7 for instructions.

Step 8. Click **Submit Changes** to add the user to the database, or **Cancel Changes** to cancel these changes.

The new user appears in the list on the Users page.

Deleting a User

There are two ways to delete a user: you can delete one or more users from the Users list, or you can delete a user individually with the User Editor.

To delete one or more users from the Users list:

Step 1. Click the **Delete** checkbox in the row of the user you want to delete.

You can delete multiple users in a single operation.

Step 2. Click **Submit Changes** to delete the selected users.

To delete a user with the User Editor:

Step 1. From the Users page, click **Add/Edit User**, or click the user name you want to delete.

The User Editor appears, as shown in Figure 10-2.

Step 2. Click **User**, highlight the user name you want to delete in the drop-down list, and click **Apply Selection**.

The user appears in the User Details section of the page.

Step 3. To delete the user, scroll to the bottom of the page and click **Delete this User**.

A warning page appears requiring you to confirm that you really want to delete this user.

Step 4. To proceed to delete this user, click **Yes**. To cancel, click **No**.

Setting Up Access Point Users

The 700wl Series system supports Access Points as a special type of user.

All access points are visible as 700wl Series system clients, whether they have been added as users or not. The benefit of making an access point a user is that it can then be contacted from

within your network. This allows a network administrator to communicate with the access point for configuration or status monitoring purposes, for example.

To be able to communicate to an access point from within your network, there are several things you must do:

- Add the access point as a user—use the MAC address of the access point as the user name, and select its type as Access Point.
- Add the access point to the Access Point group. This is a special group that can only have access point users as members.

  Note: *You can also add Access Points through the Rights Manager Clients page. All clients that are either detected as MAC addresses or do not have a user ID associated with then are displayed with a selection field that lets you specify that a client is an Access Point. See "Setting Up MAC Address Users and Access Points" for details on designating a client as an Access Point.*

- Make sure that the Access Point group is allowed at every location that includes the port (via a Where) through which the access point is connected to the network. If you do not allow the Access Point group, the access point will not be able to respond to any requests you send it from the network. The Access Point group is NOT allowed by default at any locations.

GLOBAL RIGHTS MANAGER SETTINGS 11

This chapter explains how to configure many aspects of the Rights Manager for the HP ProCurve Secure Access 700wl Series system. It includes the following sections:

Global Settings Overview 11-1

Network Access Control Console Configuration 11-2

DNS/WINS Server List Editors 11-4

Automatic HTTP Proxy Configuration 11-9

Setting Up Rights Manager Logging 11-15

Security 11-17

Global Settings Overview

The Configuration page provides links to settings for a number of Rights Manager options in addition to the Authentication and Accounting-related settings.

- **Control Console:** These settings let you enable the Network Access Control Console feature, and configure groups to be used with the Network Access Control Console.
- **DNS/WINS:** These settings let you specify any number of DNS and / or WINS servers that should be used when an incoming packet is a DNS or WINS request. This feature includes the creation of an allow / redirect pair that will handle the incoming request, forwarding or redirecting it as appropriate.
- **Automatic Proxy per Group:** The Automatic HTTP Proxy configuration feature lets you specify, on a group-by-group basis, that all HTTP traffic entering through ports you specify should be redirected to an internal HTTP Proxy server. This means that you can enforce the use of a proxy server regardless of how the client browser is configured regarding proxy server use. In addition, you can configure Proxy filter rules that control what traffic will be forwarded on to the proxy server based on the destination URL.
- **Logging:** You can configure a number of options for Rights Manager logging.
- **Security:** Under this heading you can enable or disable MAC address spoofing detection. You can also obtain and load an SSL certificate from a recognized certificate authority to replace the default certificate issued by HP.

To access these Global settings, from anywhere in the Rights Manager click **Configuration** to display the Configuration page, as shown in Figure 11-1.

Figure 11-1. The Rights Manager Configuration Menu

The Authentication and Accounting items on this page are discussed in Chapter 9, “User Authentication”.

Network Access Control Console Configuration

The Network Access Control Console is a separate browser-based interface that provides a way for a non-administrator user to dynamically change the access rights for all members of a group on a temporary basis. The Network Access Control Console is useful in organizations such as educational institutions, where an instructor may want to temporarily suspend access rights for the students in his class during a test, for example.

In the Network Access Control Console, access for a group can be changed to disallow all network access, or a set of rights can be “borrowed” from another group and substituted for the first group’s rights. There is a pre-defined setting for No Access, but in order to temporarily “borrow” rights from another group, that group must be set up and configured with the appropriate set of access rights. This feature assumes that a group structure has been created within the Rights Manager such that when rights are modified for one group, the modifications only affect the appropriate users.

To enable dynamic rights management through the Network Access Control Console, there are three things an administrator must do:

Step 1. Enable the Network Access Control Console feature.

Step 2. Set up the “normal” groups and configure them with passwords. If a group does not have a password, its rights cannot be modified through the Network Access Control Console.

Step 3. Set up any additional groups that define rights that can temporarily replace the normal rights for another group. Add these groups to the list of groups available within the Network Access Control Console. as the source of substitute rights.

In addition, you can specify an XML-RPC service from which the Rights Manager can request a list of the users who are members of a specific group. If you include this, then the Network Access Control Console can display a list of all the members of the group, and show their status as clients. If you do not include this, no list of members is displayed.

Configuring Network Access Control

To configure the Network Access Control Console feature, do the following:

Step 1. From the Rights Manager Configuration menu, click **Network Access** under the Control Console heading.

The Network Access Control Console configuration page is displayed (Figure 11-2).

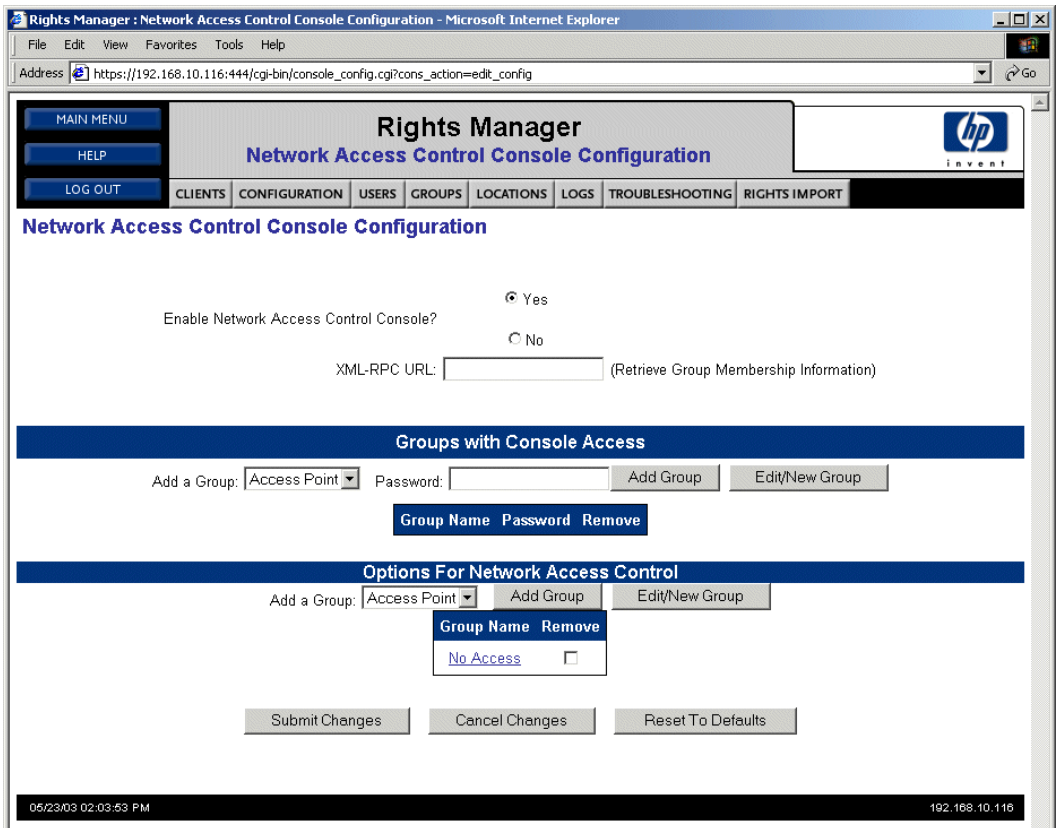

Figure 11-2. Network Access Control Console Configuration

Step 2. To enable the Network Access Control Console, click **Yes**.

To disable it, click **No**.

Step 3. If you want to retrieve lists of group members from an external XML-RPC service, type the URL of the service in the **XML-RPC URL** field.

Groups with Console Access

Step 4. Add passwords for any groups that you want a non-administrator user to be able to access from the Network Access Control Console in order to dynamically change their rights:

a. Select the group in the Add A Group drop-down list.

b. Type the group password into the **Password** field.

c. Click **Add a Group** to add this group to the list of groups accessible from the Network Access Control Console.

If you need add or edit any groups, click **Edit/New Group** or click the group name to go to the Group Editor.

Step 5. To mark a group for removal from the list of groups that allow Network Access Control Console access, click the checkbox in the Remove column for that group. The group is removed when you submit your changes.

Options for Network Access Control

Step 6. To add a group to the list of groups that can be used as a source of substitute rights, select a group from the drop-down list, and click **Add a Group**.

The groups in this list will be available in the Select New Access drop-down list that appears in the Network Access Control Console.

If you need add or edit any groups, click **Edit/New Group** or click the group name to go to the Group Editor.

Step 7. Click **Submit Changes** to have your changes take effect.

Click **Cancel Changes** to cancel any changes you have not yet submitted.

DNS/WINS Server List Editors

The DNS or WINS servers that you specified when you set up your Integrated Access Manager or Access Control Server network configuration are used by the 700wl Series system for doing address resolution for its own needs. In addition, by default, the primary DNS server is used as the destination of the predefined DNS redirect. When a client sends an address resolution request, by default it is redirected to the primary DNS server.

The DNS/WINS feature in the Rights Manager lets you specify multiple DNS or WINS servers, and create Allow/Redirect pairs for those server destinations. The Allow member of the pair forwards a DNS or WINS request that has the specified server as the destination. The Redirect member of the pair redirects any DNS or WINS requests with unknown server destinations to the specified DNS or WINS servers. You can specify multiple DNS or WINS servers, and then use those servers in an Allow or Redirect. For a Redirect with multiple servers, you can specify that the Rights Manager should select the destination address at random from its list of servers, or that it should always redirect to the same server.

Editing the DNS Servers List

To add DNS server addresses to the DNS server list, do the following:

Step 1. From the Rights Manager Configuration page, click **DNS Servers**.

The DNS Server List Editor appears, as shown in Figure 11-3.

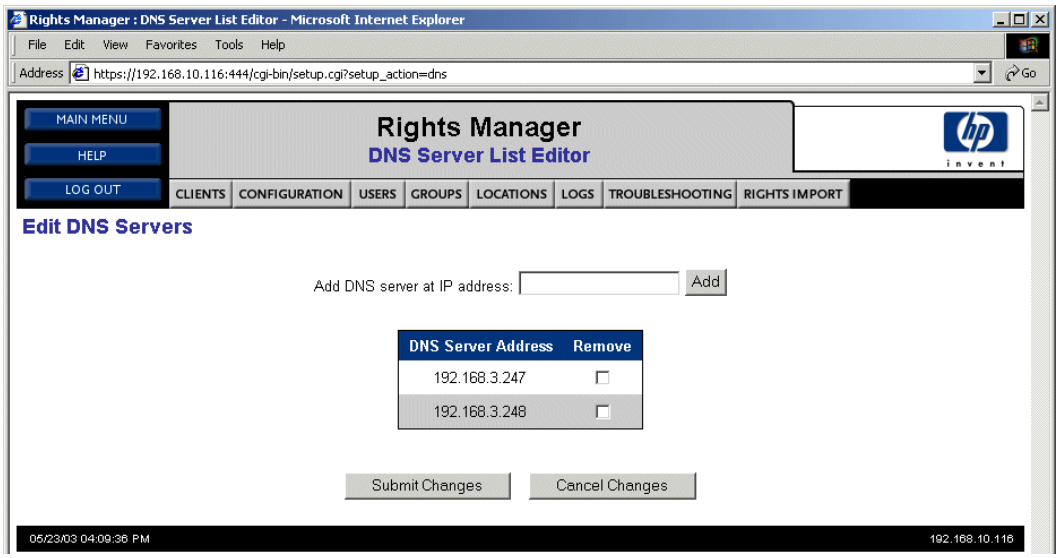

Figure 11-3. Rights Manager DNS Server List Editor

Initially the table is empty.

Step 2. Type the IP address of a DNS server into the field provided, and click **Add**.

The IP address appears in the table.

Note: *Typically you should add the primary and secondary servers that you configured when you did the network configuration.*

Step 3. Click **Submit Changes** to have your additions take effect.

Setting Up DNS Allow/Redirect Pairs

Once you have added the IP addresses of your DNS servers to the DNS Server List, you can set up allow / redirect pairs using those addresses.

Step 1. From the Rights Manager Configuration page, click **DNS allow/redirect pairs**.

The Setup DNS Allow and Redirect window appears, as show in Figure 11-4.

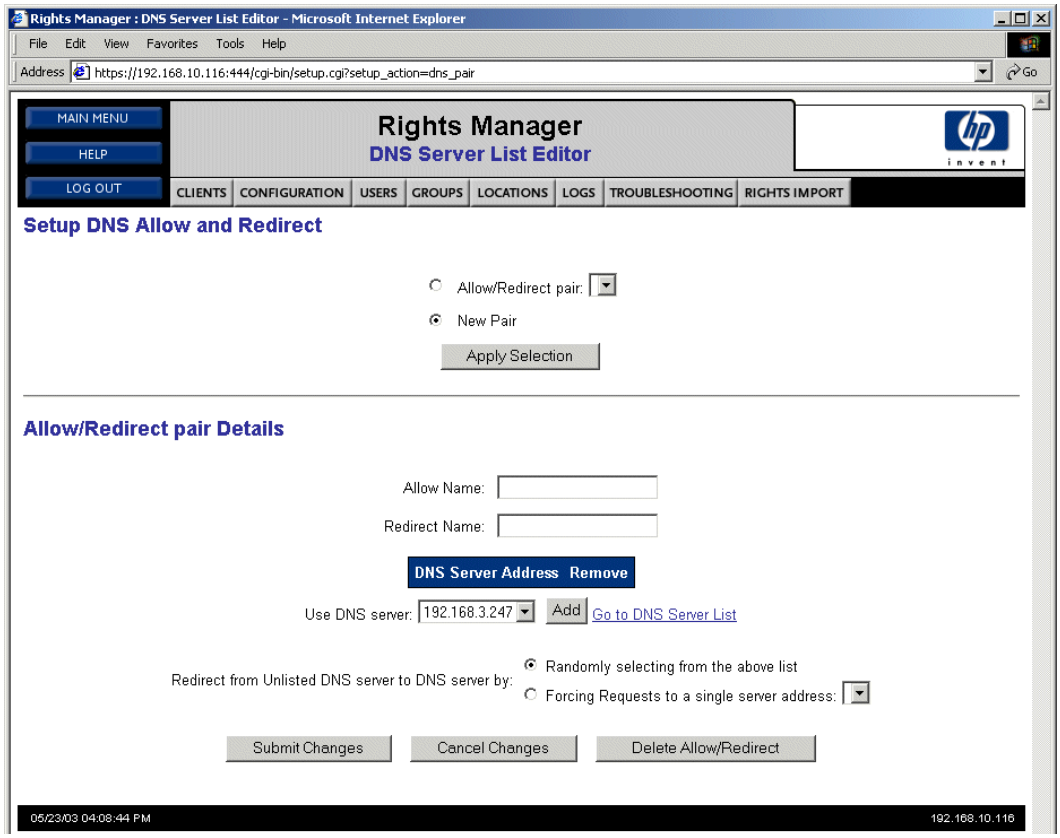

Figure 11-4. Rights Manager DNS Allow/Redirect setup

Step 2. To create a new pair, click **New** and then **Apply Selection**.

To change an existing pair, click **Allow/Redirect pair** and highlight the pair you want to modify, then click **Apply Selection**.

Step 3. Type a name for the Allow.

Step 4. Type a name for the Redirect.

Step 5. Initially, the list of destination addresses is empty. To add servers to the list for this Allow / Redirect pair, select a server from the Use DNS Server drop-down list, and click **Add**.

If there are multiple servers in your DNS Server List, you can add any or all of them to the list for this Allow / Redirect pair.

If you want to add other servers to the list, click **Go to DNS Server List** to go to the DNS Server List Editor.

Step 6. If you want the Redirect to choose a DNS server destination at random from among the servers you have added to the list for this Allow / Redirect pair, click **Randomly select from the above list**.

Note: *The selection of the destination DNS server is done by the Rights Manager at the time rights are assigned to the client. That destination only will be used until the client reauthenticates and is given new rights.*

If you want the Redirect to always go to a specific destination server, click **Force requests to go to a single server address** and select that IP address from the drop-down list.

Note: *The Allow created as a result of this process includes all the server destinations in the list you specify. The Redirect always includes just one destination—either the IP address you specified with the Force... option, or a destination selected from the list of servers at the time the client's rights are assigned.*

Step 7. To have your changes take effect, click **Submit Changes**.

The new Allow and Redirect appear in the list of Allows and Redirects available for use in the Group Editor. Remember to add these Allows and Redirects as appropriate to the set of Allows and Redirects for the groups you have defined. You should also remove the predefined DNS redirect from the list of redirects enabled for your groups.

Editing the WINS Servers List

To add WINS server addresses to the WINS server list, do the following:

Step 1. From the Rights Manager Configuration page, click **WINS Servers**.

The WINS Server List Editor appears, as shown in Figure 11-3.

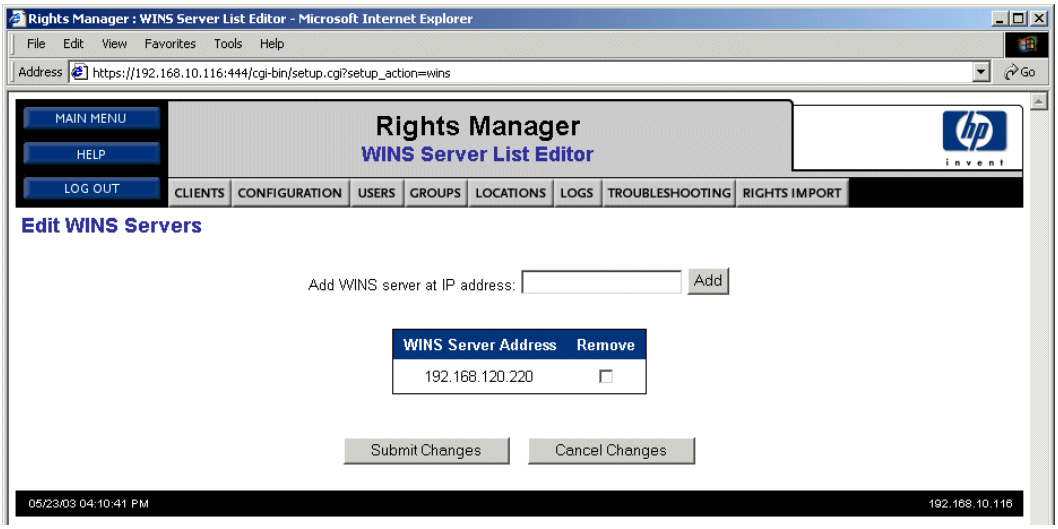

Figure 11-5. Rights Manager WINS Server List Editor

Initially the table is empty.

Step 2. Type the IP address of a WINS server into the field provided, and click **Add**.

The IP address appears in the table.

Step 3. Click **Submit Changes** to have your additions take effect.

Setting Up WINS Allow/Redirect Pairs

Once you have added the IP addresses of your WINS servers to the WINS Server List, you can set up allow / redirect pairs using those addresses.

Step 1. From the Rights Manager Configuration page, click **WINS allow/redirect pairs**.

The Setup WINS Allow and Redirect window appears, as show in Figure 11-4.

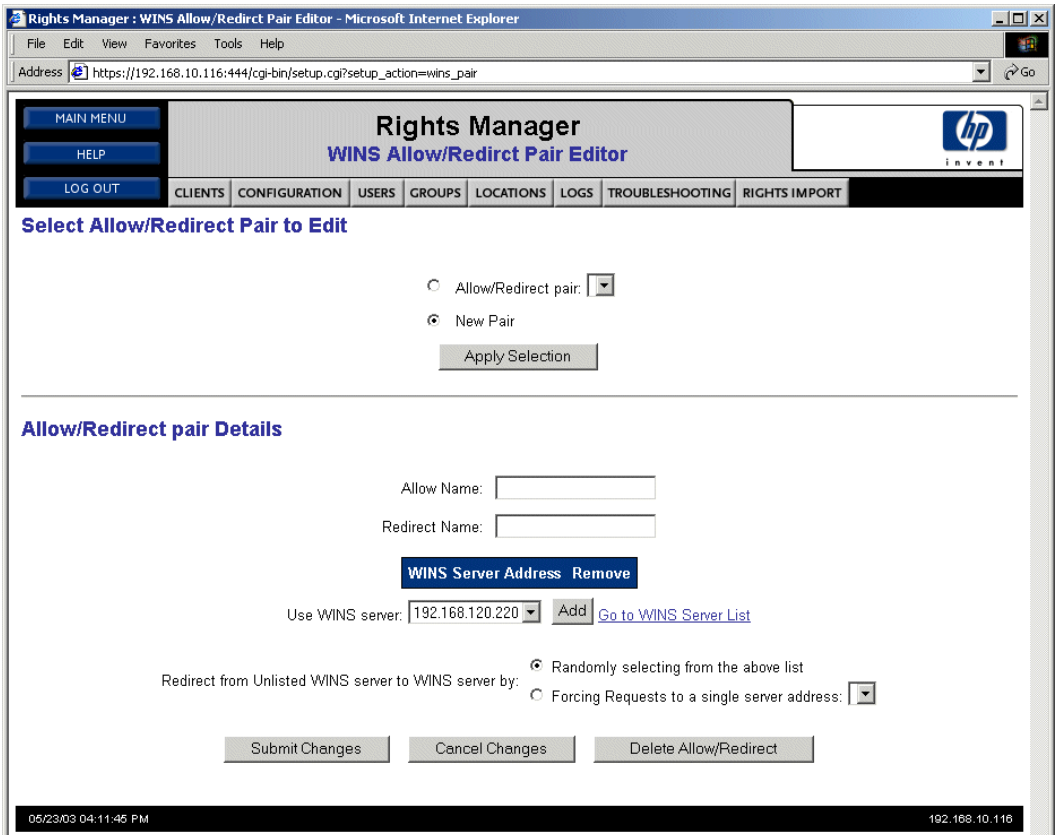

Figure 11-6. WINS Allow/Redirect setup

Step 2. To create a new pair, click **New** and then **Apply Selection**.

To change an existing pair, click **Allow/Redirect pair** and highlight the pair you want to modify, then click **Apply Selection**.

Step 3. Type a name for the Allow and for the Redirect (if this is a new pair).

Step 4. When you create a new Allow / Redirect pair, the list of destination addresses is initially empty. To add servers to the list for this Allow / Redirect pair, select a server from the Use WINS Server drop-down list, and click **Add**.

If there are multiple servers in your WINS Server List, you can add any or all of them to the list for this Allow / Redirect pair.

If you want to add other servers to the list, click **Go to WINS Server List** to go to the WINS Server List Editor.

Step 5. If you want the Redirect to choose a WINS server destination at random from among the servers you have added to the list for this Allow / Redirect pair, click **Randomly select from the above list**.

Note: *The selection of the destination WINS server is done by the Rights Manager at the time rights are assigned to the client. Only that destination is used until the client reauthenticates and is given new rights.*

If you want the Redirect to always go to a specific destination server, click **Force requests to go to a single server address** and select that IP address from the drop-down list.

Note: *The Allow created as a result of this process includes all the server destinations in the list you specify. The Redirect always includes just one destination—either the IP address you specified with the* **Force...** *option, or a destination selected from the list of servers at the time the client's rights are assigned.*

Step 6. To have your changes take effect, click **Submit Changes**.

The new Allow and Redirect appear in the list of Allows and Redirects available for use in the Group Editor. Remember to add these Allows and Redirects as appropriate to the set of Allows and Redirects enabled for the groups you have defined.

Automatic HTTP Proxy Configuration

If your network makes use of a proxy server for HTTP traffic, you may want to ensure that HTTP traffic originating from wireless clients also goes through your proxy server. However, when mobile wireless clients connect to your network, especially if you allow Guest access, there is no guarantee that their browsers will be configured correctly for your proxy server.

The Automatic HTTP Proxy feature of the 700wl Series system allows you to enforce the use of an internal HTTP proxy server (within your network) without requiring a specific configuration on the client. Whether a client browser is configured with no proxy, or for any arbitrary proxy server, the 700wl Series system can intercept HTTP traffic and redirect it to the appropriate proxy server within your network.

Note: *The exception is for SSL traffic from a client with no proxy configured. In this case, the 700wl Series system cannot intercept the traffic.*

In addition to redirecting client HTTP traffic to your proxy server, you can also specify a set of proxy filters that will allow or deny HTTP traffic based on the destination of that traffic. You can create filter rules based on fully qualified domain names, IP addresses, simple host names, network addresses (subnets), or any arbitrary destination based on matching a regular expression. These rules are configured by Groups. HHTP requests that are denied based on these proxy filters are redirected to the Stop page.

Note: *You can configure the IP address of your HTTP Proxy Server through the HTTP Proxy link on the Administrative Interface Main Menu. If you do not configure a proxy server, but you configure and enable the automatic proxy feature, the 700wl*

Series system will act as the proxy server, and will handle the traffic according to the configured ports and filters. See "HTTP Proxy Server Configuration" in Chapter 2 for instructions on configuring the IP address of your Proxy server.

Enabling or Disabling the Automatic Proxy for a Group

The automatic Proxy feature is enabled and configured group-by-group. This lets you specify an HTTP proxy only for selected groups, such as the Guest group.

There are three steps to enabling a proxy:

- Enable the proxy server for the group (optionally enabled with a browser Cookie)
- Configure the ports on which you expect to see HTTP traffic from members of this group
- Set up filters to allow or deny traffic to specific destinations.

Note: *Proxy filtering is completely independent of the Allow and Redirect rights specified for a group. If you enable the automatic proxy feature, and want to block access to certain destinations, you* ***must*** *set filters to deny HTTP access to those destinations. Redirect rights have no effect on HTTP traffic if the automatic proxy feature is enabled. The default filter is "Accept All" for Logon, Guest, User, and Normal groups. The default is "Deny All" for Access Point and Stop groups.*

To enable or disable the automatic proxy feature, do the following:

Step 1. From the Rights Manager, click **Configuration**.

Step 2. Under the heading HTTP Proxy, click **Automatic Proxy per Group**.

The Enable Automatic Proxy per Group page appears (see Figure 11-7).

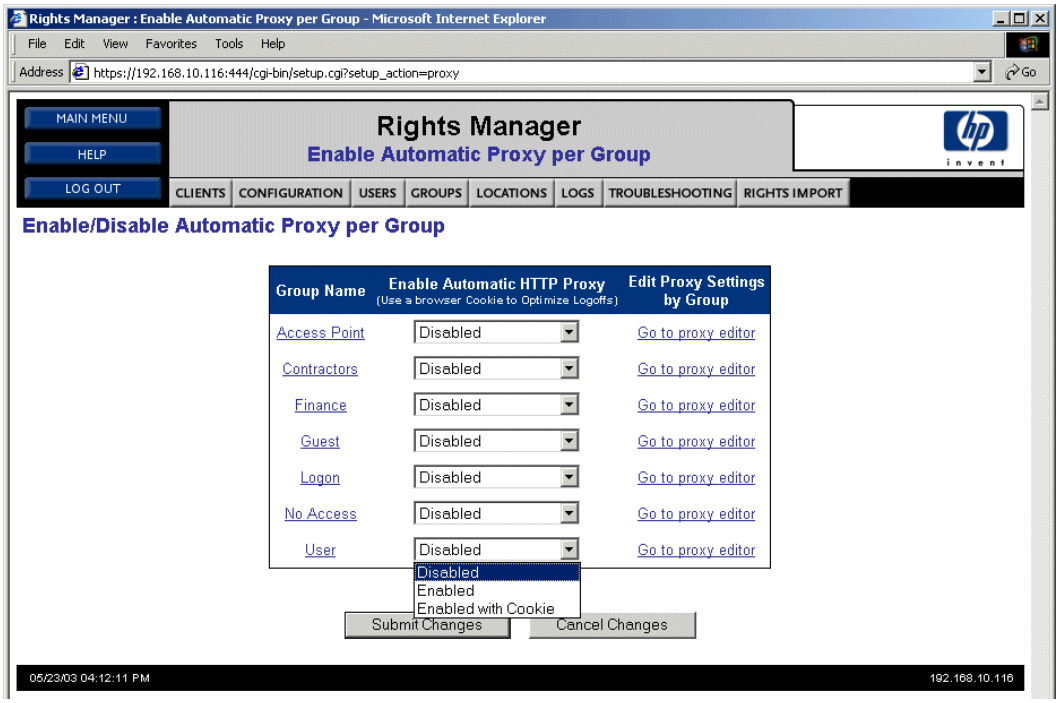

Figure 11-7. Enabling or Disabling the Automatic Proxy for groups

By default, the HTTP proxy is disabled for every group.

Step 3. To enable automatic proxy for a group, select **Enabled** or **Enabled with Cookie** from the drop-down field.

Enabling with a browser cookie will optimize logoff.

Step 4. Click **Submit Changes** to have these settings take effect.

Note: *You must also configure the Proxy Settings for the group using the Proxy Editor. If you don't specify any ports to be intercepted, enabling the proxy feature will have no effect.*

Configuring the HTTP Proxy Settings for a Group

To configure the Automatic HTTP Proxy feature, you must determine what TCP ports traffic is likely to appear on, so that the 700wl Series system can intercept and redirect that traffic. You also can configure a set of proxy filters if you want to conditionally allow or deny specific connections. These settings are also done by groups, meaning you can specify different access for members of different groups.

Step 1. From the Enable Automatic Proxy per Group page, click **Go to Proxy Editor** to configure the ports and proxy filters for a group.

The Automatic HTTP Proxy Editor page appears, as shown in Figure 11-8.

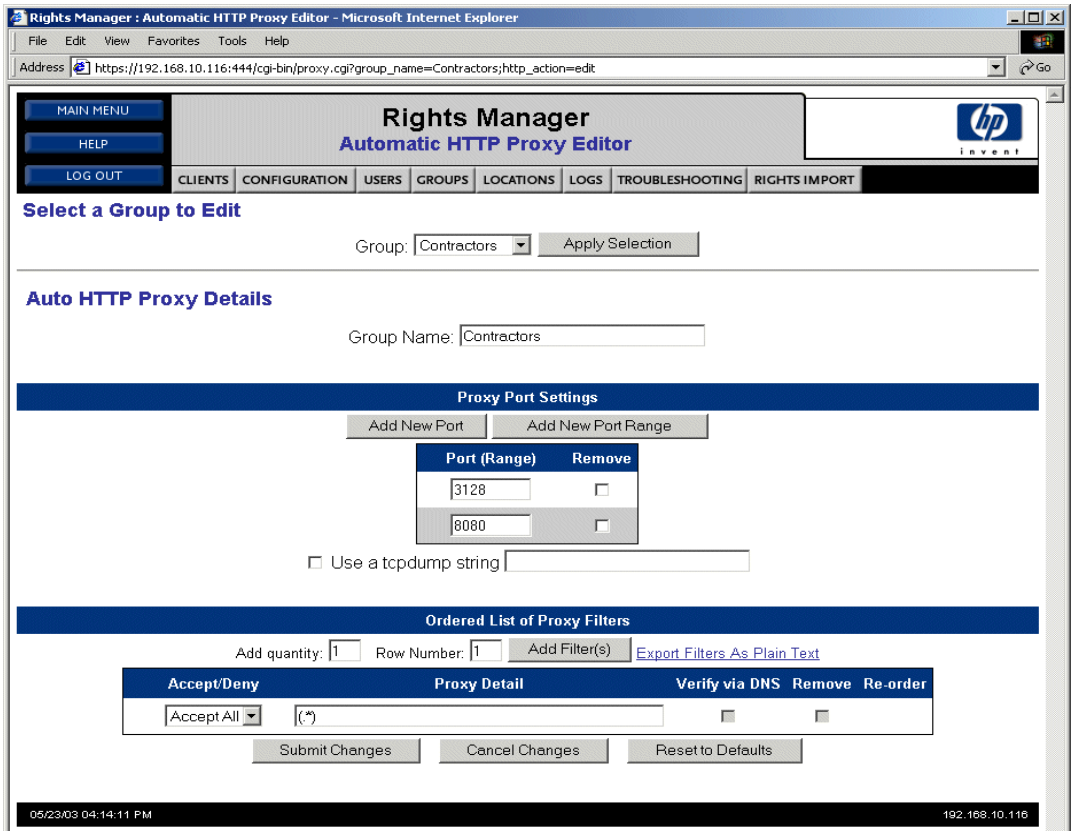

Figure 11-8. Automatic HTTP Proxy Editor

Step 2. Highlight the group you want to modify from the drop-down list and click **Apply Selection**.

If you have previously configured the proxy settings for this group, those properties appear in the fields below. Otherwise, the fields are set to their default values.

Figure 11-8 shows the defaults that appear for all groups except Access Point and Stop groups:

- By default, ports 3128 and 8080 are included.
- The default catch-all filter is set to **Accept All**. The catch-all filter is the final filter that takes effect if a packet falls through all the preceding filters.

The defaults for Access Point and Stop groups (such as the No Access group) are no ports and **Deny All** as the catch-all filter.

Proxy Port Settings

Step 3. To add a port, click **Add New Port**. A new field appears in the table, into which you can enter a port.

Step 4. To add a port range, click **Add New Port Range**. Two fields appear in the table, into which you can enter the starting and ending values for the port range.

Step 5. Click **Submit Changes** (at the bottom of the page) after *each entry* in the table.

If you do not submit each entry, it will disappear when you select the next **Add New Port** or **Add New Port Range**.

Step 6. To use a an expression in `tcpdump` syntax instead of individual port and port range specifications, click the checkbox and enter the string in the **Use a tcpdump string** field. The string `dst host 192.168.5.1 and tcp dst port 3128` is an example of a `tcpdump` string.

Note: *When the checkbox is checked, the* `tcpdump` *string is used and any ports in the table are ignored. If the checkbox is unchecked, the ports in the table are used and the* `tcpdump` *string is ignored.*

Note: `tcpdump` *syntax is case sensitive. All keywords must be in lower-case to be recognized.*

See Appendix A, "Filter Expression Syntax" for details on the `tcpdump` syntax.

Ordered List of Proxy Filters

Proxy filters let you specify what HTTP traffic should be allowed or denied access. Filters are evaluated in the order they appear in the list.

Step 7. To add one or more filters, do the following:

a. Enter a number in the **Add Quantity** field. This specifies how many rows you want to add— you can add multiple rows in one operation.

b. Enter a row number in the **Row Number** field. This determines the row number of the new filter, or the row number of the first new filter if you add multiple rows.

For example, if you add a row at row number three, the existing row three and all following rows are moved down, and the new row becomes row three.

Note: *The catch-all filter (Accept All/Deny All) must be the last row in the list, always. You cannot add rows after it.*

c. Select a filter type from the drop-down list in the **Accept/Deny** field. You can select the following filter types:

— **Accept Ip/Deny Ip**—specify a destination IP address (e.g., 192.168.2.5)

— **Accept FQDN/Deny FQDN**—specify a destination as a fully qualified domain name (e.g., `www.domain.com`)

— **Accept Host/Deny Host**—specify a host name as a destination (e.g., `www` or `home`)

— **Accept Net/Deny Net**—specify a destination network address (IP address and subnet mask) (e.g., 192.168.0.0/16)

— **Accept Reg/Deny Reg**—specify a regular expression that evaluates to a destination address or address range (for example `"(.*).domain.com"`)

An Accept rule forwards the traffic to the proxy server; a Deny rule drops the packet and redirects the client to the Stop page.

d. Type the appropriate destination in the **Proxy Detail** field.

e. To specify that the 700wl Series system should verify the destination name or address via DNS *before* forwarding it to the proxy server, check the **Verify via DNS** checkbox.

Caution: *The* **Verify via DNS** *option is a relatively expensive operation. Therefore, it is probably good practice to use it sparingly. You would typically use it with a Deny rule, especially a Deny IP or Deny Net rule, to detect and prevent requests with spoofed DNS that could result in access to restricted sites.*

f. To remove a filter from the list, check the **Remove** box for that entry.

g. To change the order of entries, click the **Move Up** or **Move Down** button for the entry, as appropriate.

h. If appropriate, you can change the catch-all filter to Deny All instead of Accept All. You cannot change the proxy detail of this filter.

Step 8. Click **Submit Changes** to have your changes take effect.

Finally, you can export your filter definitions to a browser window as plain text by clicking the **Export as Plain Text** link. You can then save them to a file. This may be useful in debugging your filter sets.

Note: *If a client is a member of multiple groups that have automatic HTTP proxy feature enabled, the proxy filter rules are applied one group at a time, taking the groups in alphabetical order. The catch-all rule will be the most restrictive of the multiple catch-all rules—in other words, if any one group has Deny All as the catch-all rule, then Deny All becomes the catch-all for that client.*

Proxy Configuration Example

The example shown in Figure 11-9 configures the automatic proxy feature for the Guest group as follows:

- Specifies that the 700wl Series system should listen on ports 3128 and 8080.
- Specifies a `tcpdump` string, but it is not used as the checkbox is not checked.
- Specifies a set of filters that allows traffic going to the external web server, prevents traffic from going to any other internal sites, and then allows any other (presumably external) destinations.

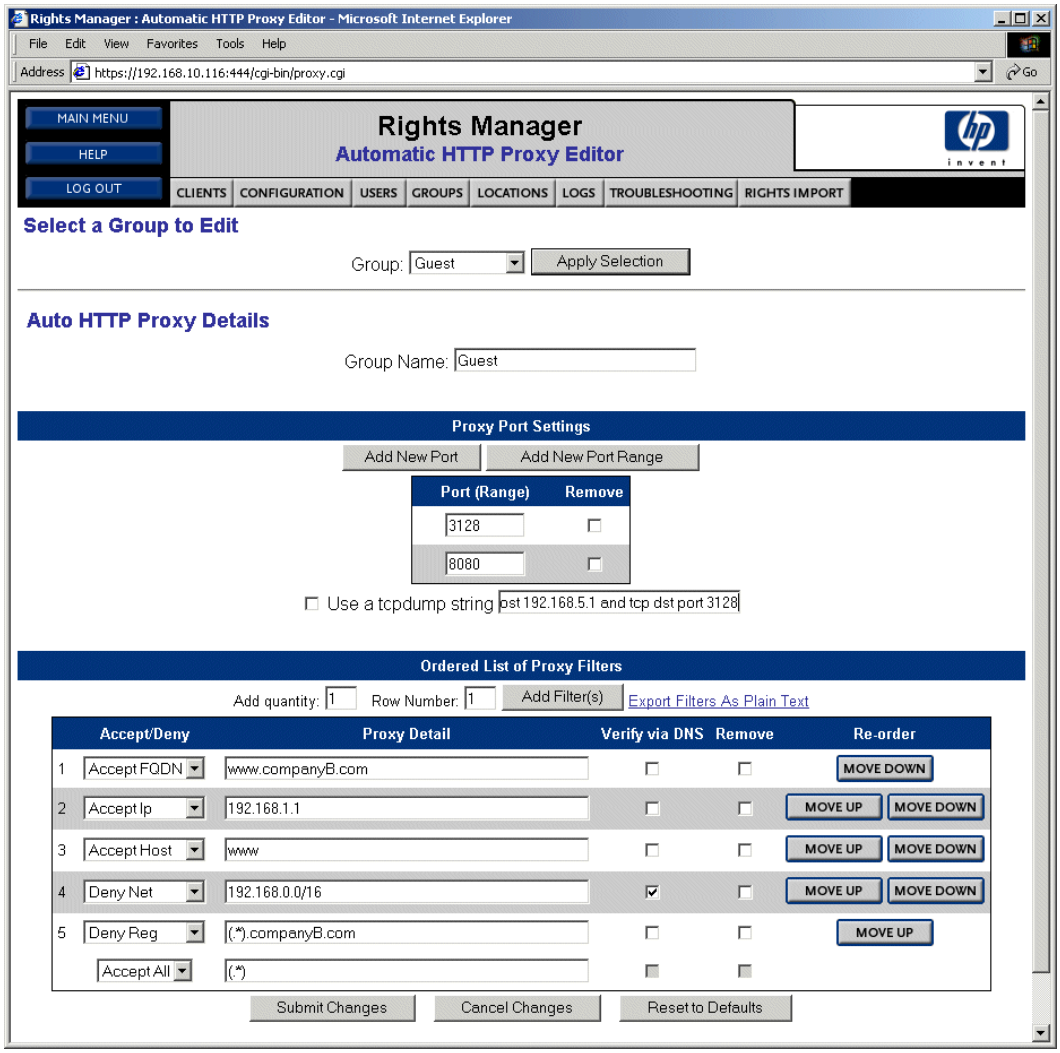

Figure 11-9. Proxy Editor with filters added

Setting Up Rights Manager Logging

The Rights Manager has its own log files, separate from the log files you can view through the 700wl Series system Main Menu. For information about the 700wl Series system's session or error logs, see "Viewing Log Files".

Rights Manager logging captures events that may be helpful in determining how the system is behaving. Rights Manager error messages are always logged. Through the Setup Logging page you can specify certain other events, such as Logons and Logoffs, to be included in the Rights Manager log file. You can also specify that Rights Manager log messages be logged to an external Syslog server.

To specify the optional Rights Manager logging behavior:

Step 1. From the Configuration page in the Rights Manager, click **Setup Logging** under the Logging heading. The Rights Manager Setup Logging page appears (see Figure 11-10).

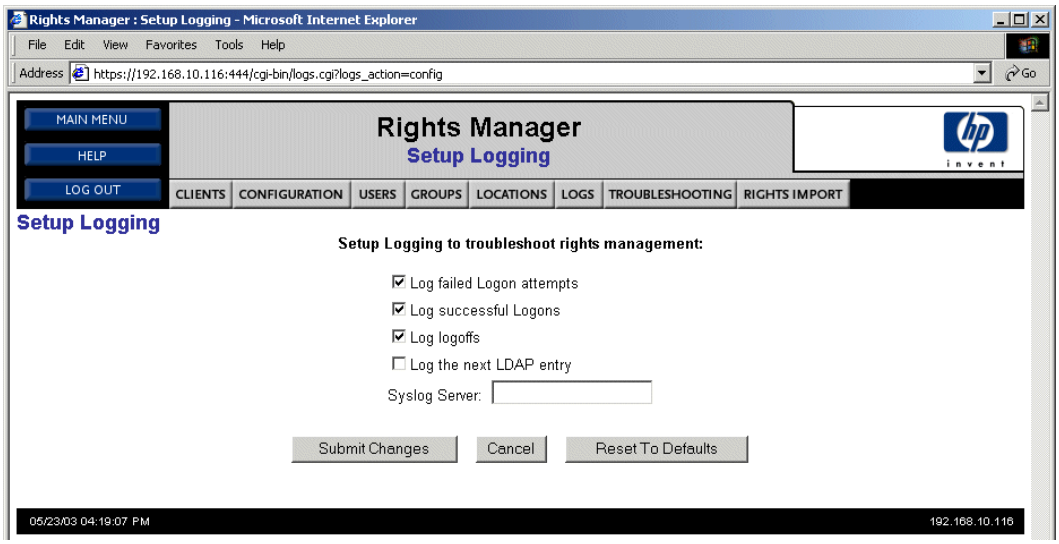

Figure 11-10. Setting up Rights Manager Logging

Step 2. Click the appropriate checkbox to enable or disable logging of the following events:

- **Log failed Logon attempts** tracks unsuccessful logon attempts.
- **Log successful Logons** tracks successful logons.
- **Log logoffs** tracks logoffs.
- **Log the next LDAP entry** logs the next LDAP authentication attempt. This may be useful if you are having problems with your LDAP authentication service, and have not been able to diagnose the problem through the LDAP Transaction Tracer tool. You can send this log to HP techncial support for analysis.

Step 3. In the **Syslog Server** field, type the IP address of the Syslog server to which you want log files sent.

Step 4. Click **Submit Changes** to have your changes take effect.

To return to the system defaults, click **Reset to Default**.

To view the Rights Manager log, click the Logs tab from anywhere within the Rights Manager. See “Viewing the Rights Manager Log” on page 12-8 for more information.

If you choose to have the Rights Manager log entries to an external Syslog server, they are logged as Syslog facility Local7. If Session logging is enabled to the same Syslog server, you will see Session Log entries intermixed with the Rights Manager log entries. See “Specifying Session Logging” on page 2-23 for information about enabling session logging.

Security

Under the security heading you can set up MAC address spoofing detection, or initiate a request for a SSL certificate signed by the Certificate Authority of your choice, and then download the certificate you obtain into the 700wl Series system.

MAC Address Spoofing Detection

MAC Address spoofing occurs when some one impersonates a legitimate client by taking over their MAC address. You can configure the 700wl Series system to detect the situation where the same MAC address appears on multiple Access Controller ports a specified number of times within a defined time period. You can configure the number of times it should appear and the time interval.

When spoofing is detected, all clients with that MAC address are logged off.

MAC address spoofing detection is enabled by default. To change the configuration of spoofing detection, or to disable it, do the following:

Step 1. From the Rights Manager Configuration page, under the Security heading, click **Spoofing Detection**.

The Spoofing Detection page appears, as shown in Figure 11-11.

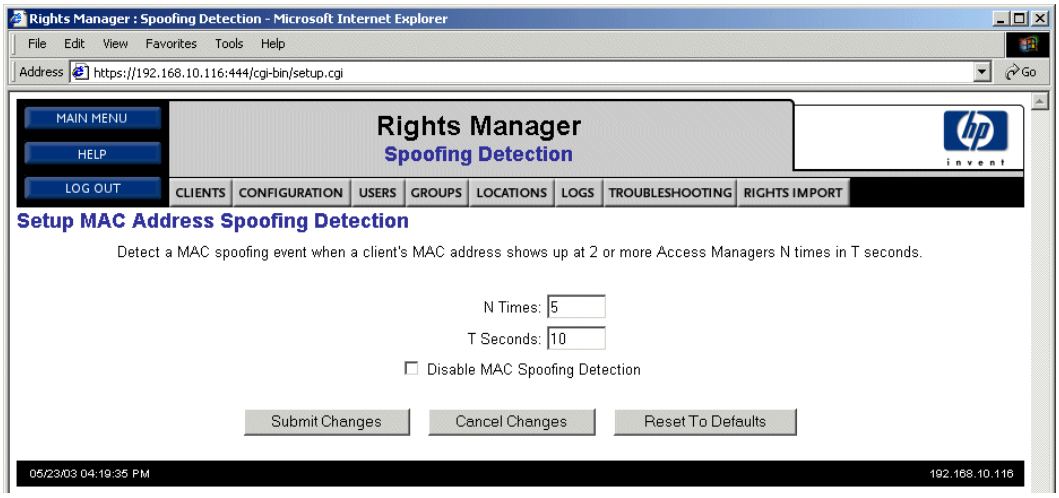

Figure 11-11. MAC Address Spoofing Detection

Step 2. Specify the number of times a MAC Address must appear on two or more Access Controller ports in order to be considered a suspected spoofing event. The default is 5.

Step 3. Specify the time frame (in seconds) in which these appearances must occur. The default is 10 seconds.

Step 4. To disable MAC spoofing detection, click the checkbox. The default is that MAC Address spoofing is enabled.

Obtaining and Loading an SSL Certificate

Users authenticate themselves to an Access Controller through an HTTPS, SSL-protected web screen. By default, the 700wl Series system comes with a SSL certificate issued by HP itself as the Certificate Authority (CA). Users accessing the logon screen receive a message warning of an untrusted certificate. Replacing the default SSL certificate with one signed by an external signing authority eliminates the warning.

If you want to use a certificate that is signed by an external signing authority, you must generate a custom certificate.

Replacing the SSL certificate is a two-step process: First, you must generate a certificate signing request (CSR). You submit this CSR to an external signing authority and they return a signed SSL certificate. You then upload the certificate onto the Integrated Access Manager or Access Control Server.

Requesting an SSL Certificate

To generate an SSL Certificate Signing Request (CSR):

Step 1. From the Rights Manager, click **Configuration**.

Step 2. Under the Security heading, click **SSL Certificate**.

The SSL Certificate Configuration page appears, as shown in Figure 11-12.

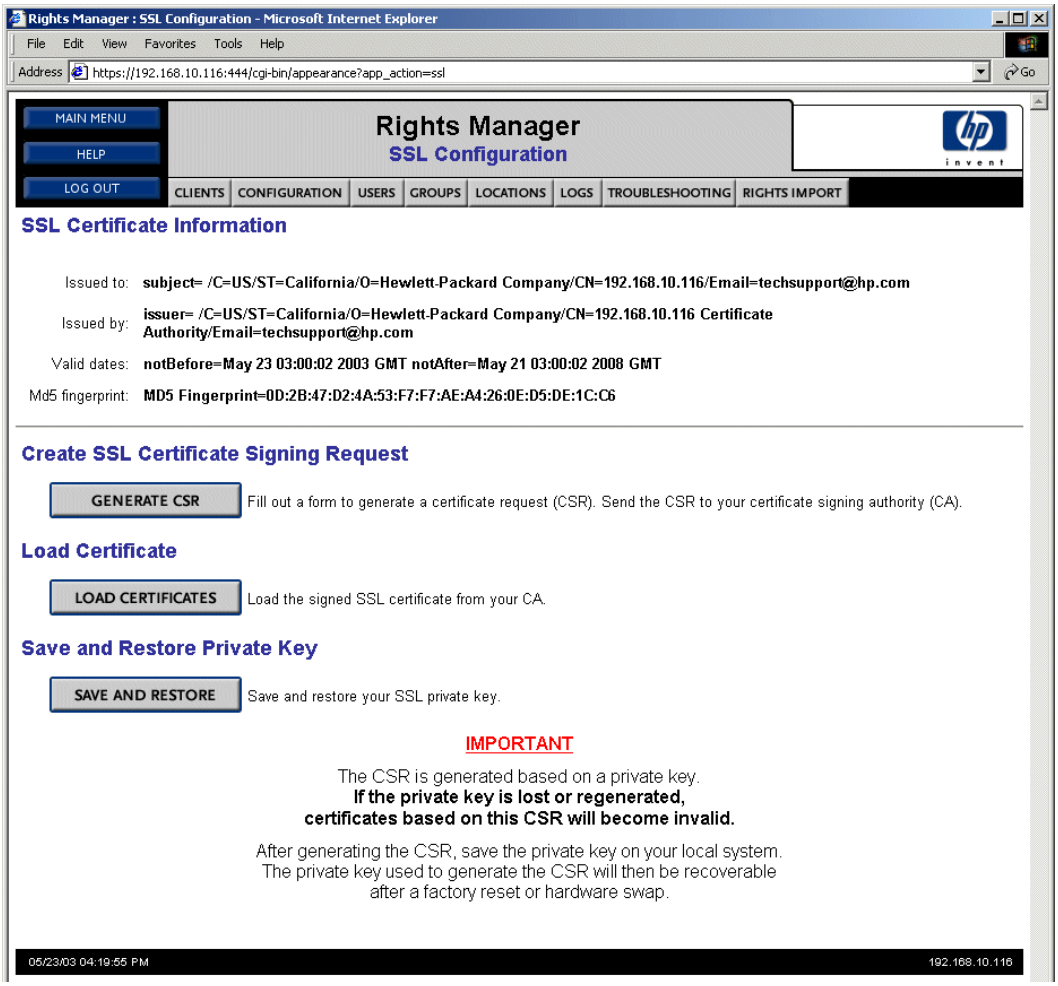

Figure 11-12. SSL Configuration page for requesting a new SSL Certificate

The information at the top of the page shows information about the current certificate. By default this will be the certificate generated by HP.

Step 3. Click **Generate CSR**.

The Generate SSL Certificate Signing Request page reappears, as shown in Figure 11-13.

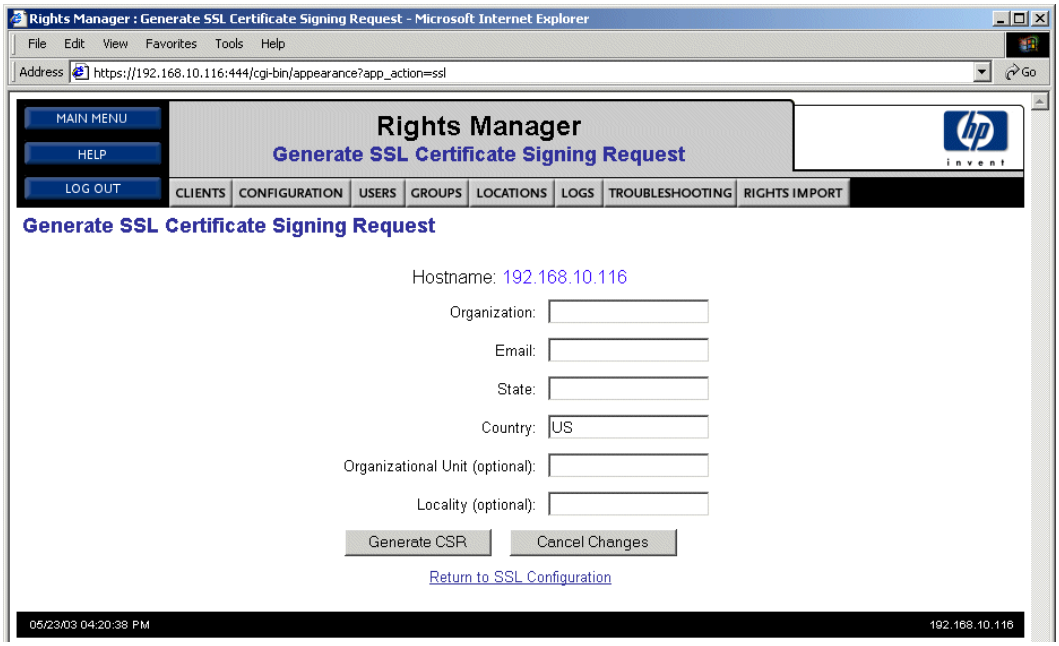

Figure 11-13. Input for generating an SSL Certificate Signing Request

Step 4. Fill in the information requested:

- **a.** Type the organization name. This is the name that will be published on the certificate.
- **b.** Type the email address for the certificate contact.
- **c.** Type your state or province. This is also typically a two-character abbreviation.
- **d.** Type your two-character ISO country code (US for the United States, UK for the United Kingdom, and so on). You can access the list of country codes at the following URL:
  `http://ftp.ics.uci.edu/pub/websoft/wwwstat/country-codes.txt`
- **e.** Type the information into the optional fields, if appropriate.

Step 5. Click **Generate CSR**.

The page reappears with the Certificate Signing Request displayed on the Right side of the page, as shown in Figure 11-14.

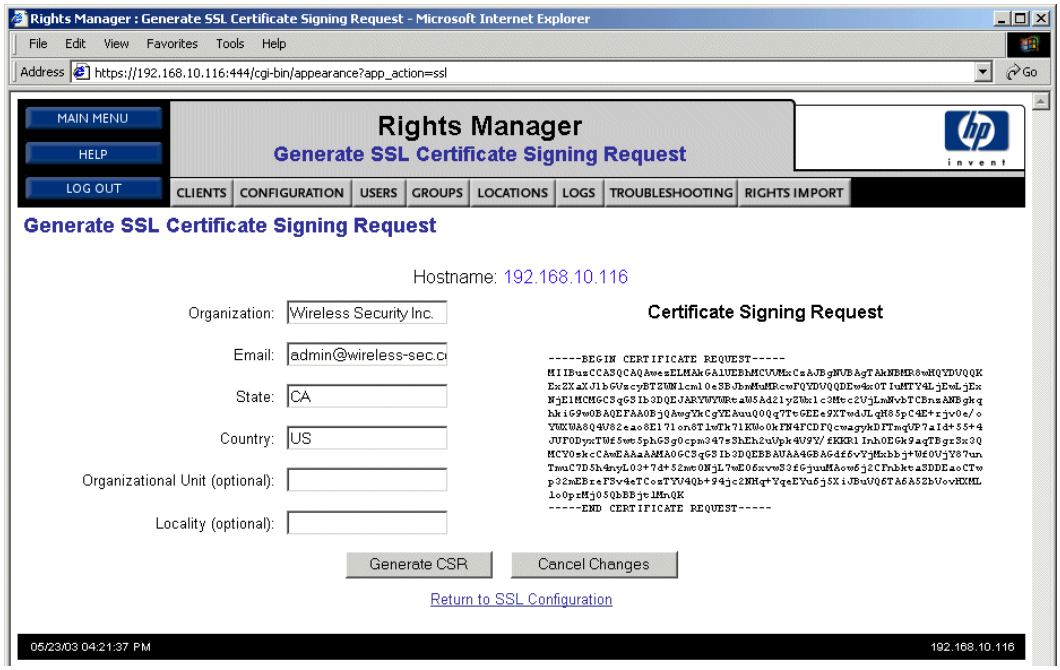

Figure 11-14. The Certificate Signing Request

You can use this certificate signing request either to request a certificate from a CA, (for example VeriSign) or to create your own self-signed certificate using an SSL toolkit, such as OpenSSL.

Step 6. Copy the CSR (including the full `BEGIN` and `END` lines and all dashes) and submit it to a certificate authority. Or you can use the CSR to generate your own self-signed certificate.

Loading the SSL Certificate

When you have receive your certificate from the CA:

Step 1. Type the filename of the certificate you received from the certificate authority (or the one you generated).

Step 2. Click **Upload Certificate**.

Note: *If you change either the hostname or IP address of the system, or if you reset to the factory defaults, then the certificate is not valid. You must apply for a new certificate.*

12 TROUBLESHOOTING, LOGS, AND RIGHTS IMPORT/EXPORT

This chapter explains how to troubleshoot authentication and user rights for the HP ProCurve Secure Access 700wl Series Rights Manager. It includes the following sections:

Troubleshooting 12-1

Tracing Authentication Service Transactions 12-1

The User Rights Simulator 12-6

Viewing the Rights Manager Log 12-8

Importing and Exporting Rights 12-10

Troubleshooting

Troubleshooting tools are provided to help you determine whether the Rights Manager functionality is working as you expect. Tools are provided that allow you to:

- Verify that an LDAP, RADIUS, or XML-RPC authentication service is working correctly
- Verify that a user will receive the rights you expect based on a given location and time frame
- View entries in the Rights Manager log file

The Rights Manager has its own log files. For information about session or error logs, see "Viewing Log Files".

Tracing Authentication Service Transactions

You can use the Rights Manager Troubleshooting tools to verify that users are being authenticated correctly, and that the correct information is returned from the authentication service. You can trace transactions to and from an LDAP directory, RADIUS service, or XML-RPC service. You enter the logon name and password of a user known to have a valid entry in the directory or service database, and the service should return the information associated with that user. If the authentication service is not set up correctly in the Rights Manager, you will receive an error code and incomplete results.

Step 1. From the Rights Manager, click **Troubleshooting**.

The Troubleshooting page appears, as shown in Figure 12-1.

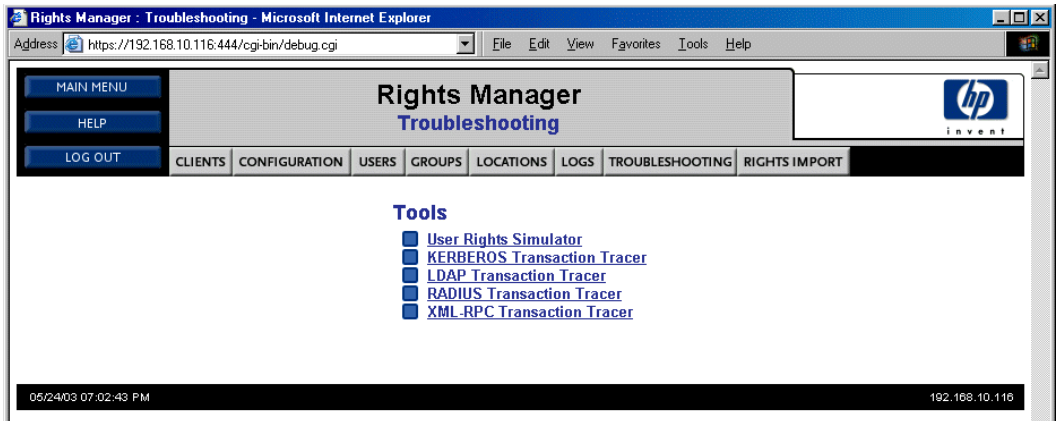

Figure 12-1. Rights Debugger

Step 2. Click the link for the service you want to trace. Your choices are **KERBEROS Transaction Tracer**, **LDAP Transaction Tracer**, **RADIUS Transaction Tracer**, and **XML-RPC Transaction Tracer**.

The appropriate Transaction Tracer page appears. Figure 12-2 shows the Transaction Tracer page for an LDAP authentication service. The pages for the other services are similar.

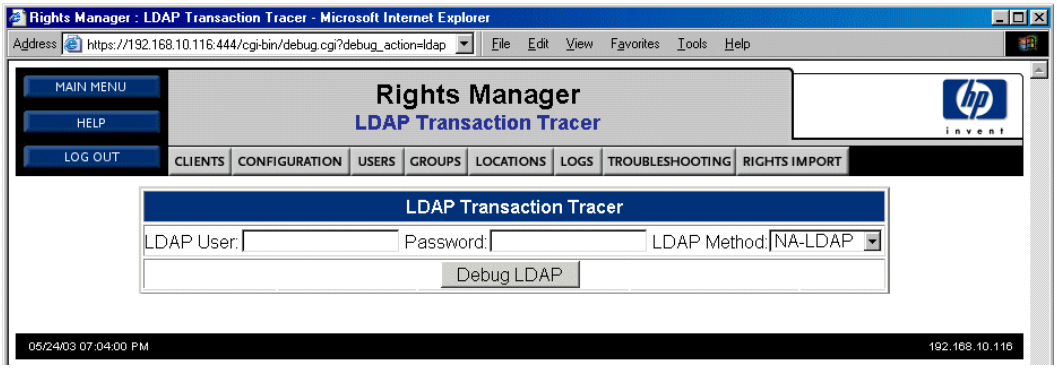

Figure 12-2. The LDAP Transaction Tracer page

Step 3. If you have more than one service defined for this authentication service type, select the service you want to debug from the drop-down list in the method field (labeled **KERBEROS method**, **LDAP method**, **RADIUS method**, or **XML-RPC method**, depending on the service you are tracing).

Step 4. Enter a known, valid user ID and password into the **User** and **Password** fields

Step 5. Click **Debug KERBEROS**, **Debug LDAP**, **Debug RADIUS**, or **Debug XML-RPC**, as appropriate. The button label will reflect the service you are trying to debug.

The Rights Debugger connects to the authentication service and attempts to retrieve the appropriate record for that user. The debugger then displays the information it sent and the results it received from the authentication service, if any.

The sections below describe the results for an LDAP, KERBEROS, RADIUS, or XML-RPC service.

Results for a KERBEROS Method

Figure 12-4 is an example of the results you might see for a KERBEROS method.

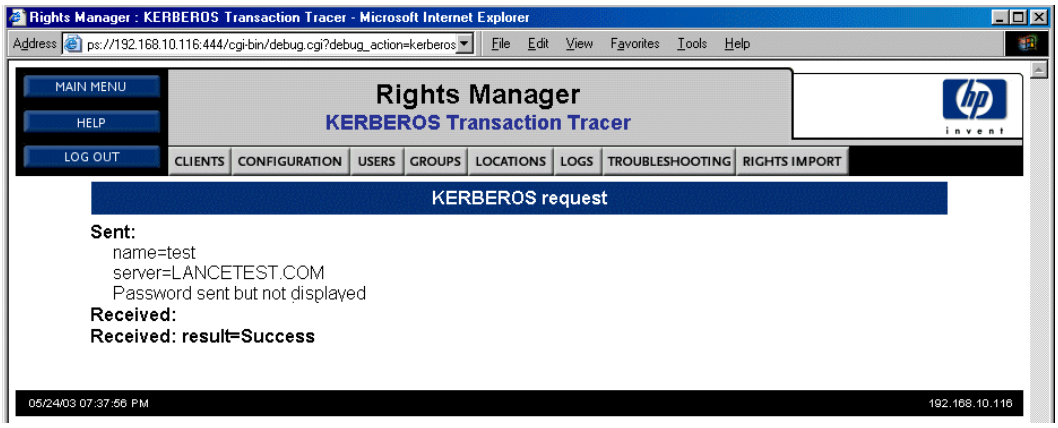

Figure 12-3. Results from KERBEROS Debug

The result shows the contents of the request and the returned (received) result. `result=Success` indicates that the authentication request was successful. If the request fails, an Authentication Failure message is displayed with a message indicating the cause of the failure.

Results for an LDAP method

Figure 12-4 is an example of the results you might see for an LDAP method. The results are returned in two parts.

The **LDAP Bind** section shows the results of the attempt to bind with the directory. If the bind succeeds, the Received field will contain `result=Success` and the returned results. The contents will depend on the configuration of your directory and whether you bind with user binding or non-user binding.

The **LDAP Search** section shows the results of a second search to find group information, or to retrieve the user password if the user's logon name was used as an alias. If the Search is successful, the results will be `result=Success` followed by the actual returned results.

If the results in either of these sections shows "results=x" where x is a non-zero value, this indicates that the server was not able to successfully perform the operation.

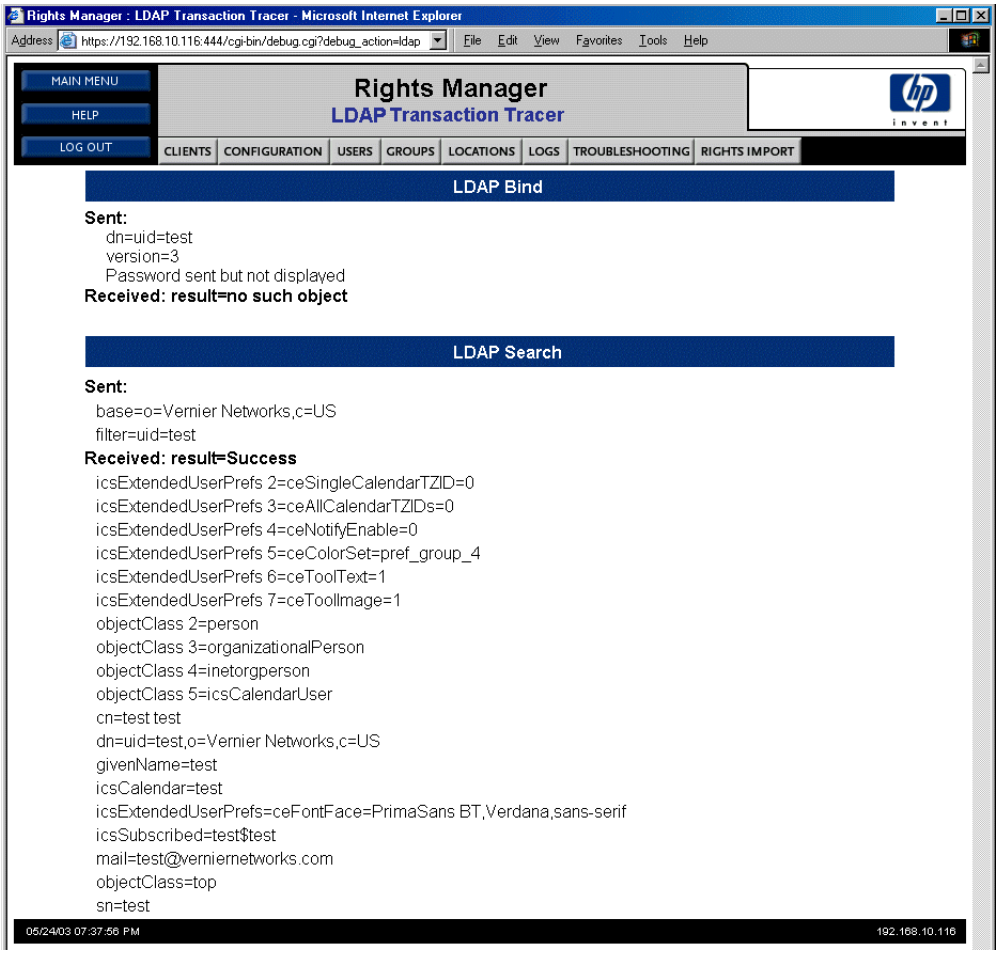

Figure 12-4. Results from LDAP Debug

Results for a RADIUS Method

Figure 12-4 is an example of the results you might see for a RADIUS method. The results are returned in two parts.

The **RADIUS Access-Request** section shows the contents of the packet sent to the RADIUS server. A `Received: result=Success` means the server received the request.

The second section shows whether the request has been accepted or rejected.

For a successful request, the section is titled **RADIUS Access-Accept** and shows the results of the request. If the request was not successful, the section is titled **RADIUS Access-Reject** and has the status `Received: result=Access-Reject`.

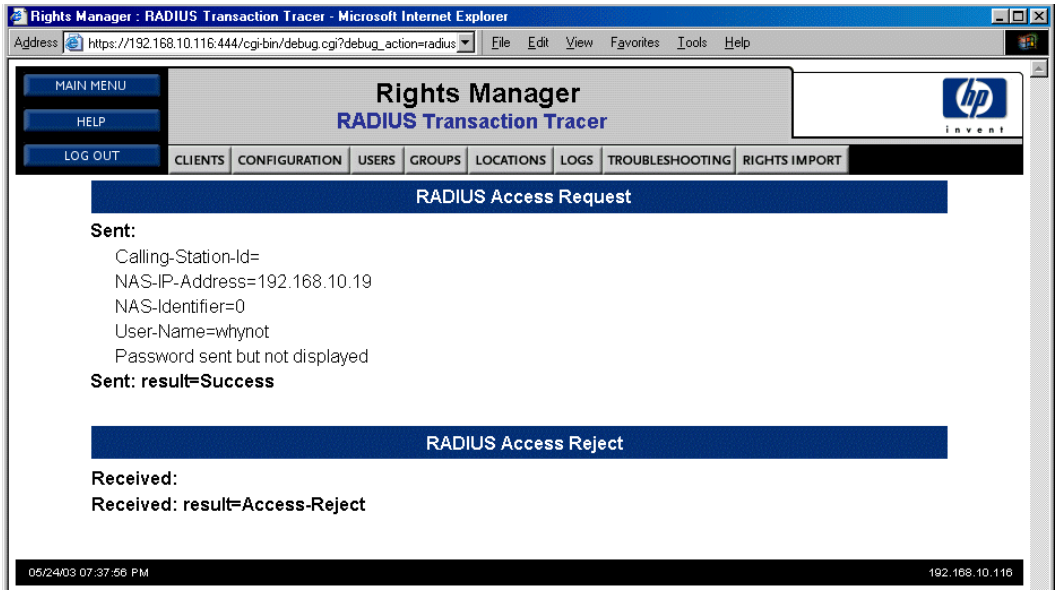

Figure 12-5. Results from RADIUS Debug

Results for an XML-RPC service

Figure 12-6 is an example of the results you might see for an XML-RPC service. The results are returned in two parts.

- The **XML-RPC request** section shows the contents of the packet sent to the XML-RPC service.
- The **XML-RPC response** section shows the profile returned for the user named in the request.

For a more detailed explanation of the contents of these two transactions, see “The Remote Profiles API” in on page 9-17.

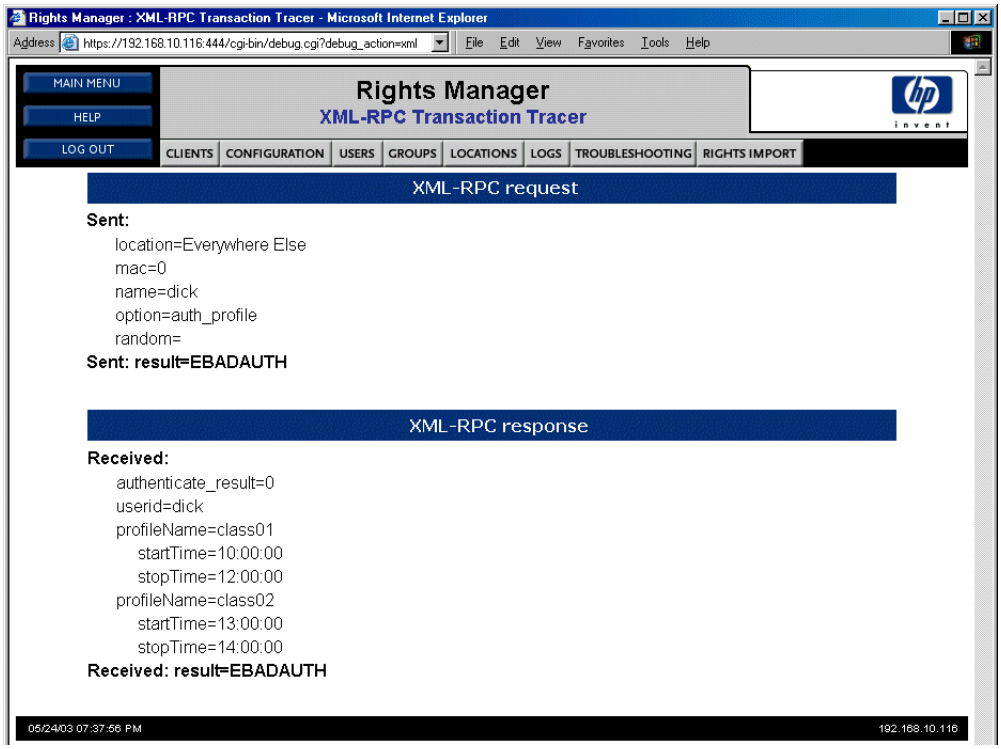

Figure 12-6. Results from XML-RPC Debug

The User Rights Simulator

You can use the User Rights Simulator to view the rights that a particular user would receive if they were log on at a specific time and location.

Note: *Note that the User Rights Simulator does NOT show you the actual rights of a user who is currently logged on, but shows you the rights a user would have if they were logged on at a particular time and location. To view the current rights for a logged-on user, see "Viewing the Active Client List" on page 5-4.*

To simulate a set of user rights, do the following:

Step 1. From the Troubleshooting page, click **User Rights Simulator**.

This takes you to the User Rights Simulator page, as shown in Figure 12-7, that lets you query for the rights a user would have if they were logged on at a time and location you specify.

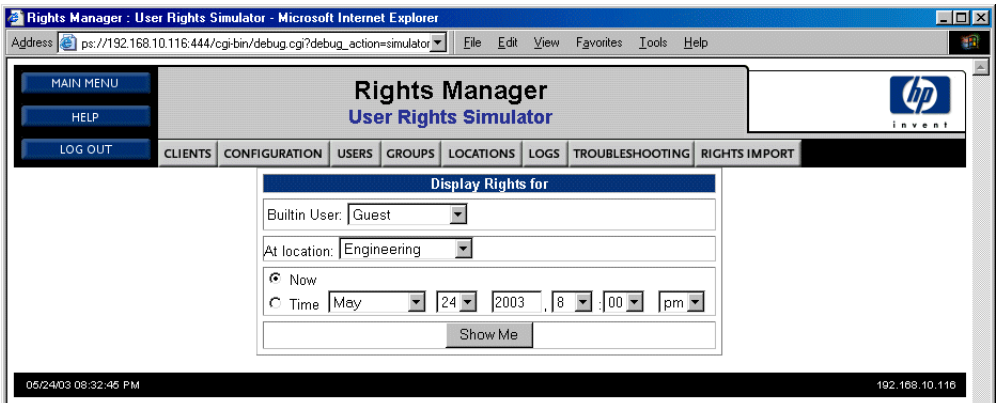

Figure 12-7. The User Rights Simulator Display Rights page

The fields displayed on this page depend on the configuration of your current Default Realm. If your default authentication realm includes a single authentication method, then you are presented with a single user identification field. If your authentication method includes several authentication methods, you are presented with a user identification field appropriate to each authentication method available in the current realm.

Step 2. Click the appropriate button and enter the user information for the user for whom you want to view rights.

- For the Built-in authentication method, click **Built-in User** and select a user name from the drop down list.

Note: *Selecting the user names "guest" "logon" or "everyone else" will display the rights for the system-defined users with those names. If you have actual users with those names, you will not be able to display their rights.*

- For an LDAP authentication method, click **LDAP User** and enter the user name and password.
- For a RADIUS authentication method, click **RADIUS User** and enter the user name and password.
- For an XML-RPC authentication method, click **XML-RPC authentication User** and enter the user name and password.

Step 3. Select a location from the drop-down list in the **At location:** field. This indicates that you want to view rights for this user as if he were logged on at the selected location.

Step 4. Select a time. Select **Now** to view rights as if the user were logged on at the current time of day, or enter a date and time to view rights as if the user were logged on at the time you specify.

Step 5. Click **Show Me**. The rights for the user you have selected appear, based on the location and time you have selected. Figure 12-8 shows the rights for a Built-in user as if she were logged in at the current time (Now) at the "Engineering" location.

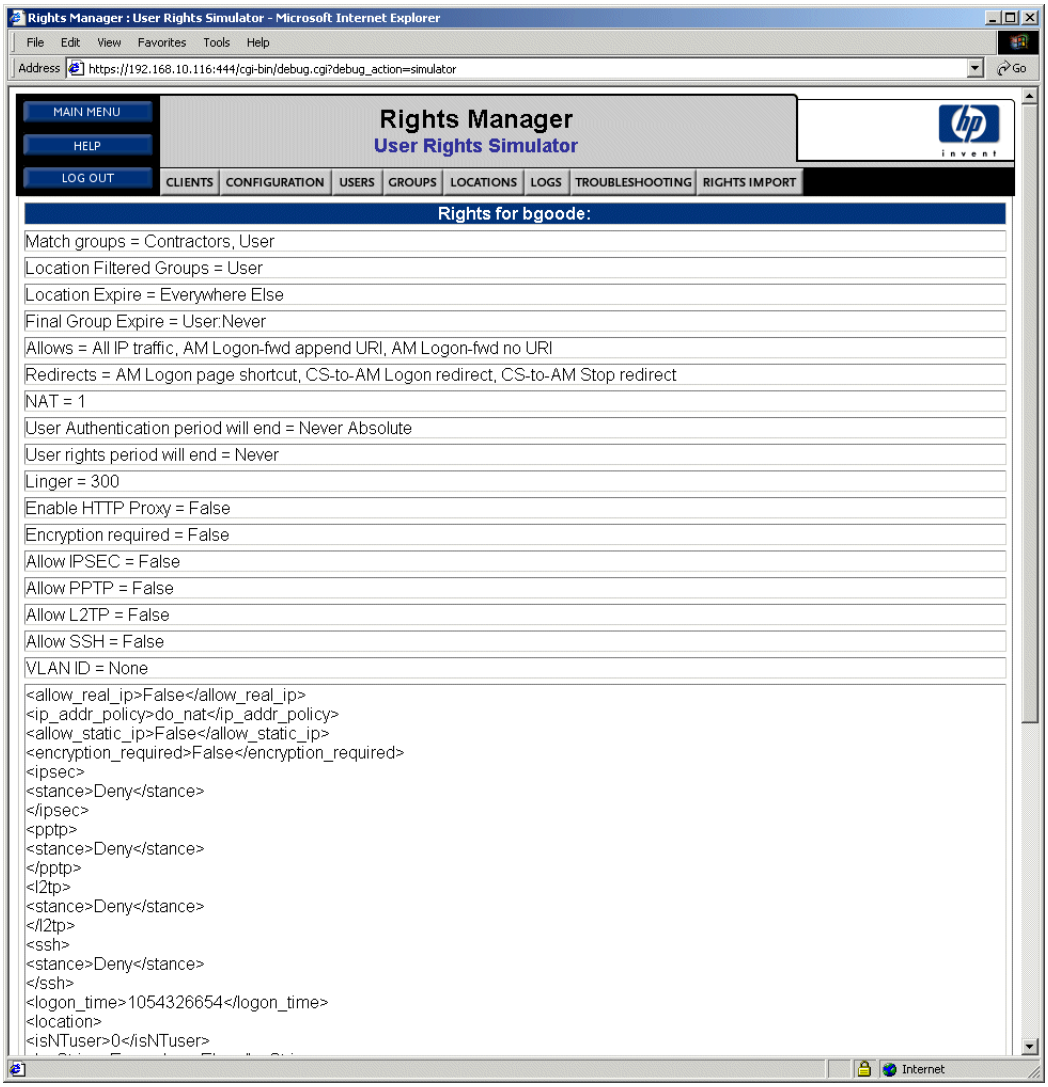

Figure 12-8. Rights for user “bgoode” if logged on at the specified time and location

Step 6. Click **Done** when you are finished viewing the rights.

The top part of the Rights display shows a summary of the rights that this user would get if logged on at the specified location and time. The bottom part of the display shows the actual XML that defines these rights.

Viewing the Rights Manager Log

The Rights Manager log file displays Rights Manager error events, and any of the other events you have specified through the Setup Login page.

Each log entry shows the time at which it was created, the severity of the event, and the message associated with the event.

To view the Rights Manager log:

Step 1. Form anywhere within the Rights Manager click **Logs**.

The Rights Manager Log Viewer appears, as shown in Figure 12-9

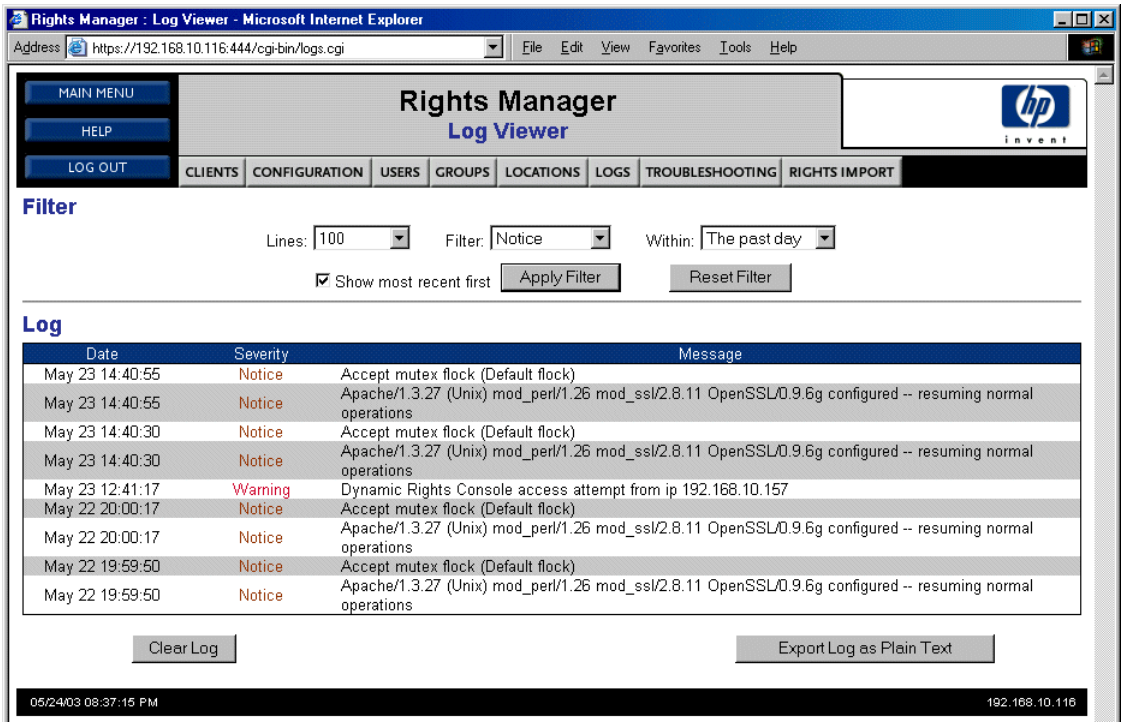

Figure 12-9. Rights Manager Log Viewer

You can filter to change the contents of the log display:

Step 1. Select the filter options you want to change:

- From the Lines field drop-down list, select the number of lines to display: You can choose 10, 100, 1000, or unlimited.
- From the Severity field drop-down list, select the severity level of the notices to display. The display will include all events with that severity level or higher.

  The severity levels, from highest (most severe) to lowest, are: **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Informational**, or **Debug**.

  For example, if you select **Notice** as the severity, all events with severities of Notice, Warning, Error, Critical, or Alert will be displayed.
- From the Within field drop-down list, select the time period to display. You can choose the past hour, day, week, or no time limit.

Step 2. Click **Apply Filter** to view filtered results; click **Reset Filter** to reset to the default view.

Step 3. Click **Export Log as plain text** to save the log as a plain text file on your web browser's system. You might want to archive or forward the log file.

Note: *Click* **Clear Log** *to empty the log file.*

The information you have logged to the Rights Manager log file can also be logged to a Syslog server. If you choose to have the Rights Manager log entries to an external Syslog server, they are logged as Syslog facility Local7. If Session logging is enabled to the same Syslog server, and also uses Local7, you may see Session Log entries intermixed with the Rights Manager log entries. See “Specifying Session Logging” on page 2-23 for information about enabling session logging.

Importing and Exporting Rights

Exporting Rights lets you save the current rights definitions in a file on your local system. From there, you can connect to the Rights Manager on a different Access Control Server or Integrated Access Manager and import those rights to that system. This lets you configure rights on one system and then replicate that configuration across multiple Rights Managers on different physical systems.

Note: *The import of rights is additive—the imported rights may replace rights of the same name in the target system, but any additional rights in the target system (that are not included in the imported set) will remain unchanged.*

In addition, you can download the XML schema that defines the structure of the rights. Given access to the schema, you could edit the set of rights before you import it back to your current Rights Manager or to the Rights Manager on another system.

To perform an export or import of rights, click **Rights Import** from any Rights Manager page.

The Import / Export page appears, as shown in Figure 12-10.

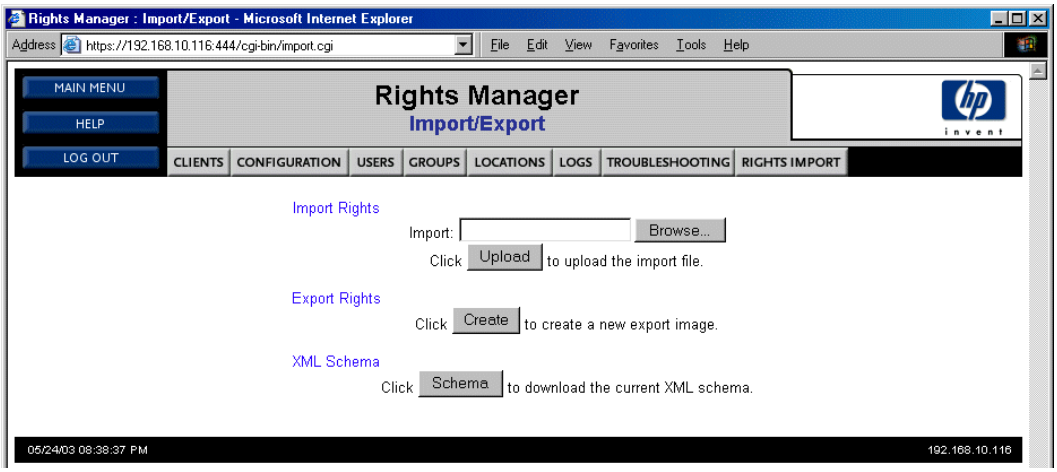

Figure 12-10. Rights Import/Export page

Creating a Rights Image for Export

There are two steps required in order to export a Rights image to your local system. You must first create an exportable image on the Integrated Access Manager or Access Control Server. You can then download that image to your local system.

To create a new image for export:

Step 1. Under Export Rights area of the page, click **Create**.

A confirmation page, as shown in Figure 12-11, appears.

Figure 12-11. Confirm Rights Export

Step 2. Click **Continue with rights export**.

The main Import/Export page reappears, with a status message now displayed, as shown in Figure 12-12

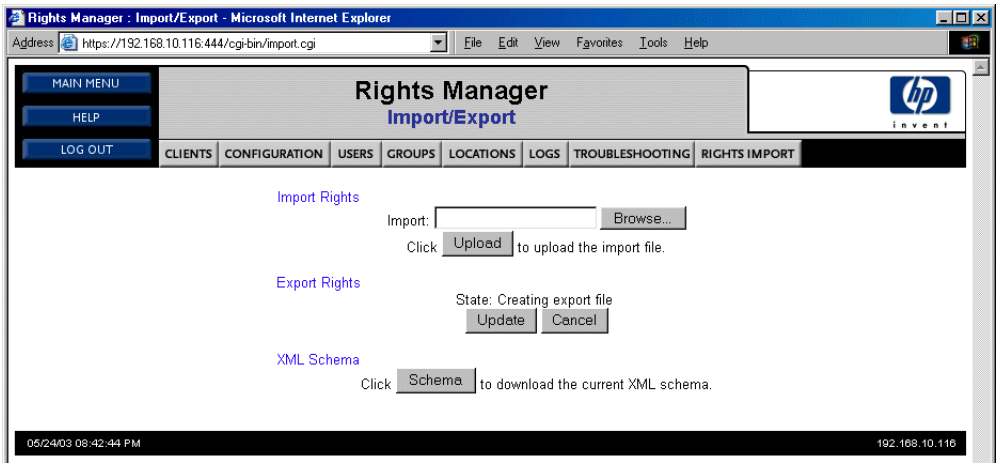

Figure 12-12. New Export Image

Note: *This replaces the previous export image file.*

Step 3. Click **Update** to update the status.

When the Rights image has been created, the Import/Export page displays the date and time that the new image was created, as shown in Figure 12-13. At this point you can download the image to your local system.

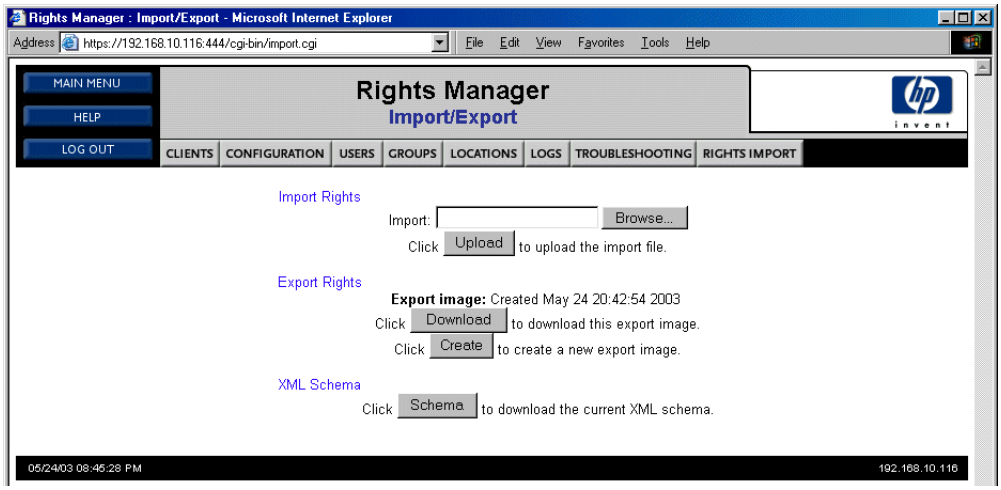

Figure 12-13. Import/Export page after successful creation of an exportable Rights image

Exporting a Set of Rights

To export a Rights image from your 700wl Series system to your local management system, you must first create an exportable image. If no image is currently available, your only choice under the Export Rights heading will be to create an image. See “Creating a Rights Image for Export” on page 12-11 for instructions.

If an export image is available, the date and time at which it was created is displayed, as shown in Figure 12-13.

To export the current Rights image to your local system, do the following:

Step 1. If the export image available for download is appropriate for download based on its date and time stamp, click **Download**.

This will start the file download process appropriate to your local system.

Step 2. Specify the location where the Rights image should be stored. If you have created a backup of your 700wl Series system image, by default the Rights image will be stored in the same directory. If you want to save the Rights image in another location, you can specify the appropriate location.

By default the downloaded image is named `export`, but you can specify any name you want.

If the current Export Image shown is out of date, click **Create** to create an new exportable Rights image. See “Creating a Rights Image for Export” on page 12-11 for instructions.

Importing Rights

To import a set of rights from your local management system to your 700wl Series system, do the following:

Step 1. Type the name of the file to be imported into the text box, or use **Browse** to locate the file on your local system. By default the file is named `export`.

Step 2. Click **Upload** to upload the import file.

The main Import/Export page re-appears with a status message displayed.

Step 3. Click **Update** to see the progress of the upload.

Downloading the XML Schema

If you plan to edit the Rights image file, you will need the XML schema that defines the file format. The schema is a text file that you can view with any text editor.

To download the XML schema to your local system:

Step 1. Under the XML Schema heading, click **Schema** to download the current XML schema.

This starts the file download process as appropriate on your local system.

Step 2. Specify the location where the schema should be stored. If you have created a backup of your 700wl Series system image, by default the schema will be stored in the same directory. If you want to save the schema in another location, you can specify the appropriate location.

By default the downloaded schema is named `export.xsd`, but you can specify any name you want.

FILTER EXPRESSION SYNTAX

A

This Appendix explains the syntax used to define user access rights (Allows and Redirects), bridged traffic, and HTTP proxy filters.

It includes the following sections:

Introduction A-1

Filter Specification Syntax A-1

Tcpdump Primitives A-2

Introduction

The Rights Manager uses filters defined in `tcpdump` syntax to specify user access rights (Allows and Redirects), bridged traffic, and proxy filters. Incoming packets are tested against these filters to determine whether those packets should be forwarded, redirected, or bridged.

This appendix describes the syntax of the filter specifications used by the Rights Manager for defining Allows, Redirects, Bridged traffic, and HTTP Proxy filters.

Filter Specification Syntax

Each filter specification is an ***expression*** formed using the `tcpdump` syntax. If an incoming packet matches the filter (the expression is "true") then the packet is forwarded, redirected, or bridged, depending on the type of filter. If no expression in the set of filters is true, the packet is dropped.

An expression consists of one or more primitives. Primitives usually consist of an ID (name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

- ***Type*** qualifiers indicate what kind of thing the ID name or number refers to. Possible types are **`host`**, **`net`**, and **`port`**. If there is no type qualifier, **`host`** is assumed.

  Examples are: "`host foo`", "`net 128.3`", or "`port 20`".

- ***Direction*** qualifiers specify a particular transfer direction— to and / or from ID. Possible directions are **`src`**, **`dst`**, **`src or dst`**, and **`src and dst`**. If there is no direction qualifier, **`src or dst`** is assumed. For null link layers (i.e. point to point protocols such as slip) the inbound and outbound qualifiers can be used to specify a desired direction.

  Examples are: "`src foo`", "`dst net 128.3`", or "`src or dst port ftp-data`".

- ***Protocol*** qualifiers restrict the match to a particular protocol. Possible protocols are: **`ether`**, **`ip`**, **`tcp`**, and **`udp`**. If there is no protocol qualifier, all protocols consistent with the type are assumed.

  Examples are: "`ether src foo`", "`ip net 128.3`", and "`tcp port 21`".

- In addition to the above, there are some special "primitive" keywords: **`broadcast`**, **`multicast`**, **`vlan`**, **`less`**, **`greater`**, and arithmetic expressions. All of these are described in Table A-1.

Primitives can be combined to create more complex filter expressions. Primitives can be combined using:

- A parenthesized group of primitives and operators.
- Negation ("**`!`**" or "**`not`**").
- Concatenation ("**`&&`**" or "**`and`**").
- Alternation ("**`||`**" or "**`or`**").

Negation has highest precedence. Alternation and concatenation have equal precedence and associate left to right. Explicit **`and`** tokens, not juxtaposition, are required for concatenation.

Examples are: "`not host foo`", or "`not port ftp or not port ftp-data`".

To save typing, identical qualifier lists can be omitted. If an identifier is given without a qualifier, the most recent qualifier is assumed.

For example: "`not host foo and ace`" is the same as "`not host foo and host ace`". Both are true if the packet includes host ace and does not include host foo (as either source or destination).

This should not be confused with: "`not (host foo or ace)`" which is true if neither host foo or host ace is.

For example: "`tcp dst port ftp or ftp-data or domain`" is the same as "`tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain`".

Tcpdump Primitives

Allowable primitives are shown in Table A-1. For more details refer to the UNIX man page `tcpdump`, and other related man pages noted in the explanation text in Table A-1.

Note: `tcpdump` *syntax is case sensitive. All keywords must be in lower-case to be recognized.*

Table A-1. Allowable Primitives

Primitive	Explanation
dst host *host*	True if the destination field of the packet is *host*, which can be either an address or a name.
src host *host*	True if the source field of the packet is *host*.

Table A-1. Allowable Primitives (Continued)

Primitive	Explanation
host *host*	True if either the source or destination of the packet is *host*.
ether dst *ehost*	True if the Ethernet destination address is *ehost*. *Ehost* can be either a name from `/etc/ethers` or a number (see *ethers*(3N) for numeric format).
ether src *ehost*	True if the Ethernet source address is *ehost*.
ether host *ehost*	True if either the ethernet source or destination address is *ehost*.
dst net *net*	True if the destination address of the packet has a network number of *net*. *Net* can be either a name from `/etc/networks` or a network number (see *networks*(4) for details).
src net *net*	True if the source address of the packet has a network number of *net*.
net *net*	True if either the source or destination address of the packet has a network number of *net*.
net *net* **mask** *mask*	True if the IP address matches *net* with the specific netmask. Can be qualified with **src** or **dst**.
net *net/len*	True if the address matches net a netmask *len* bits wide. Can be qualified with **src** or **dst**.
dst port *port*	True if the packet is ip/tcp or ip/udp, and has a destination port value of *port*. The *port* can be a number or a name used in `/etc/services` (see *tcp*(4P) and *udp*(4P)). If a name is used, both the port number and protocol are checked. If a number or ambiguous name is used, only the port number is checked (e.g., **dst port 513** will print both tcp/login traffic and udp/who traffic, and **port domain** will print both tcp/domain and udp/domain traffic).
src port *port*	True if the packet has a source port value of *port*.
port *port*	True if either the source or destination port of the packet is *port*. Any of the above port expressions can be prepended with the keywords **tcp** or **udp**, as in, for example **tcp src port** *port* which matches only tcp packets whose source port is *port*.
less *length*	True if the packet has a length less than or equal to *length*. This is equivalent to **len <=** *length*.
greater *length*	True if the packet has a length greater than or equal to *length*. This is equivalent to **len >=** *length*.
ip proto *protocol*	True if the packet is an IP packet (see *ip*(4P)) of protocol type *protocol*. *Protocol* can be a number or one of the names **icmp**, **icmp6**, **igmp**, **igrp**, **pim**, **ah**, **esp**, **udp**, or **tcp**. Note that the identifiers **tcp**, **udp**, and **icmp** are also keywords and must be escaped via backslash (\)

Table A-1. Allowable Primitives (Continued)

Primitive	Explanation
ip protochain *protocol*	True if the packet contains protocol header with type *protocol* in its protocol header chain. For example, `ip protochain 6` matches any IPv4 packet with TCP protocol header in the protocol header chain. The packet can contain, for example, authentication header, routing header, or hop-by-hop option header, between IPv4 header and TCP header. The BPF code emitted by this primitive is complex and cannot be optimized by BPF optimizer code in `tcpdump`, so this can be somewhat slow.
ether broadcast	True if the packet is an Ethernet broadcast packet. The *ether* keyword is optional.
ip broadcast	True if the packet is an IP broadcast packet. It checks for both the all-zeroes and all-ones broadcast conventions, and looks up the local subnet mask.
ether multicast	True if the packet is an ethernet multicast packet. The ether keyword is optional. This is shorthand for **ether[0] & 1!= 0**.
ip multicast	True if the packet is an IP multicast packet.
ether proto *protocol*	True if the packet is of ether type *protocol*. Protocol can be a number or one of the names *ip*.
vlan [*vlan_id*]	True if the packet is an IEEE 802.1Q VLAN packet. If [*vlan_id*] is specified, then this is only true if the packet has the specified *vlan_id*. Note that the first **vlan** keyword encountered in *expression* changes the decoding offsets for the remainder of the *expression* on the assumption that the packet is a VLAN packet.
tcp, udp, icmp	Abbreviations for **ip proto** *p*, where *p* is one of the above protocols.
expr relop expr	True if the relation holds, where *relop* is one of *>, <, >=, <=, =, !=* *expr* is an arithmetic expression composed of integer constants (expressed in standard C syntax), the normal binary operators [+, -, *, /, &, |], a length operator, and special packet data accessors. To access data inside the packet, use the syntax *proto* [*expr : size*]. • The byte offset, relative to the indicated protocol layer, is given by *expr*. • *Size* is optional and indicates the number of bytes in the field of interest; it can be either one, two, or four, and defaults to one. The length operator, indicated by the keyword **len**, gives the length of the packet.

CREATING CUSTOMIZED TEMPLATES B

This Appendix explains how to develop custom templates for the Logon page, the optional Logoff pop-up page, and the optional Guest Registration page.

It includes the following sections:

Introduction B-1

A Simple Logon Page Template Example B-2

Logon Template Elements B-3

Logon Page Template — A More Advanced Example B-7

The Guest Registration Template B-10

Using a Logoff Pop-Up with a Customized Logon Page B-13

Customizing the Stop Page B-16

Introduction

While the Rights Manager Customize Web Pages by Location page lets you change the logo and some text on the standard Logon page, the basic page layout is predefined. Further, you cannot change the standard Logoff or Guest Registration pages through the Customize Web Pages by Location page. Custom templates allow you to create pages that meet your individual needs.

The HP ProCurve Secure Access 700wl Series includes a template library that supports the programmatic generation of output (HTML files). It is this capability that you can use to create customized page templates. A template or ***tmpl file*** contains the desired output (HTML) interspersed with various ***tmpl functions*** that perform operations within the Rights Manager as well as other useful functions such as control flow. Tmpl functions take zero or more arguments, where each argument can be a double-quoted string or a nested tmpl function. Each invocation of a tmpl function is replaced in the file output by the value returned by that function.

Once you have created your template file, you enter its name into the appropriate field in the Customize Web Pages by Location page. The Rights Manager will then use your template instead of the standard Logon, Logoff, Stop, or Guest Registration page. The Rights Manager parses and executes the tmpl file to generate HTML output that is displayed.

The 700wl Series template library defines many useful functions, such as flow control and other useful utilities, and a number of system-specific functions that implement 700wl Series system functionality useful in a Logon, Logoff or Registration page.

A Simple Logon Page Template Example

The 700wl Series system logon page, in its simplest form, consists of two fields where the user enters his/her user name and password, and a button to invoke the logon function. Other optional elements can include a Logoff button, a Guest logon or Guest registration button, and possibly a display of the user name of the logged-on user, and the time his/her rights will expire.

The template file shown in Figure B-1 is an example of the most basic form of a Logon page template. It demonstrates the basic elements commonly used on a Logon page.

The template uses several Tmpl functions to do the following:

- Flow control: (`@if()`, `@endif()`)
- Determine if a user is logged on: (`@loggedon()`)
- Retrieve the user logon name: (`@username()`)
- Perform certain required functions, which do not produce visible output: (`@satmac()`, `@interface()`, `@java_works()`, `@secret()`, `@query()`)

The template also defines two input fields (for the user logon name and password), and three buttons, which must be specified as shown in the example. The form elements are described in more detail in "Logon Template Elements".

Example 1

```
<!-- This is the most basic form of the logon page -->
<html>
<head>
<title>HP ProCurve 700wl Series Logon Page</title>
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
</head>

<body bgcolor="FFFFFF">

<!-- beginning of Logon Form, with required tag and functions -->

<FORM action=/cgi-bin/logon method=post name=logonForm>

    @logon_error()<br>   <!-- outputs any errors that occur -->

<!-- if logged on, shows user name -->
    @if(@loggedon())
    You are logged on as @username()<br>
    @endif()

<!-- displays username and password input fields -->
    <p>
    username<INPUT name=username><P>
    password<INPUT name=password type=password><P>

<!-- displays the three buttons -->
    <INPUT name=logon_action type=submit value="Logon User"><P>
    <INPUT name=logon_action type=submit value=Logoff><P>
```

```
    <INPUT name=logon_action type=submit value="Logon as a Guest"><P>

<!-- required functions -->
    @satmac()
    @interface()
    @java_works()
    @secret()
    @query()

</FORM>
</body>
</html>
```

The template file is a standard HTML file with the tmpl functions included. You should be sure to include any tags or meta-tags needed to make the display correctly in your browser environment.

The template file shown in Example 1 generates the very plain page shown in Figure B-1.

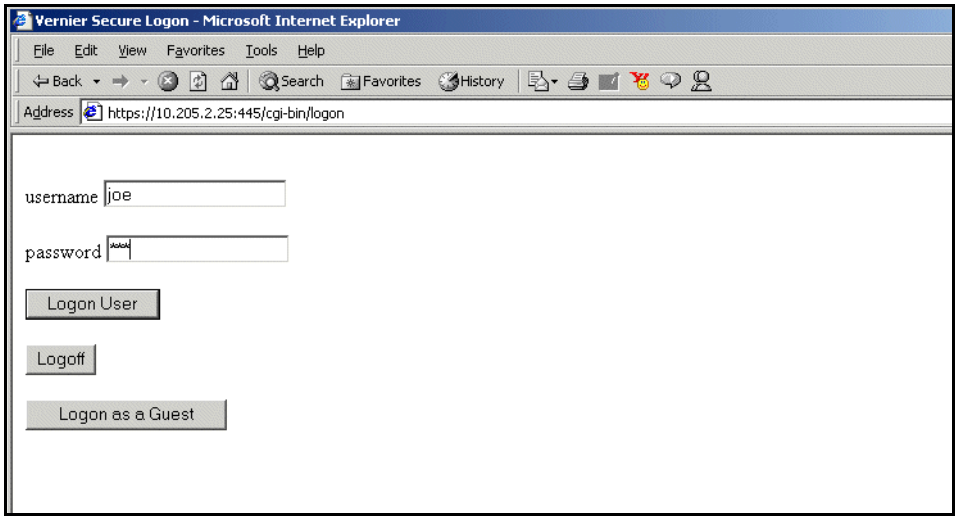

Figure B-1. Simple Logon page output

Logon Template Elements

There are a number of HTML elements and tmpl functions that are needed to create a functional Logon page template. The other templates (Logoff or Guest Registration) may also use these elements, but have fewer required elements.

Note: *The "@" character is used to identify a tmpl function. If you need to use it in your template for another purpose (for example, in an email address) you must escape it using a second @ character (@@).*

Required Elements

The Form Tag

```
<FORM action=/cgi-bin/logon method=post name=logonForm>
```

For the logon page only, there must be a form with the name attribute set to `logonForm`. The action and method attributes must also be set as shown.

Buttons

At least one of these buttons must be present on the page to enable a user to log in.

```
<INPUT name=logon_action type=submit value="Logon User">
<INPUT name=logon_action type=submit value="Logoff">
<INPUT name=logon_action type=submit value="Logon as a Guest">
<INPUT name=logon_action type=submit value="Register as Guest">
<INPUT name=logon_action type=submit value="Register">
```

For these buttons, the name, type, and value attributes *must be set exactly as shown*. The value determines the function of the button:

- "Logon User" submits a username and password for authentication.
- "Logoff" logs the user off.
- "Logon as a Guest" logs a user on as "Guest" with Guest rights. The user name and password are not used.
- "Register as a Guest" displays the Guest Registration page.

  If you plan to use a Guest Registration page (either a custom page or the default page) you must use the "Register as Guest" button. Otherwise, the Guest Registration page will never be displayed. "Logon as a Guest" and "Register as Guest" are mutually exclusive.
- "Register" submits the Guest username and password to be added to the built-in database, and logs the user in with Guest rights. The next time the user accesses the system, he will be able to log in using the user name and password he provided at registration, but will still only have Guest rights.

Changing a Button Name

If you want to change the names that appear on these buttons, you must use two INPUT statements per button: one with `type=hidden` and the value set to the required button value, and the other with `type=submit` and the value as the name you want to appear on the button. If you just change the button value, the button will no longer work as expected.

For example, the following two lines specify a Guest Logon button that appears with the label "Visitor Logon."

```
<INPUT name=logon_action type=hidden value="Logon as a Guest">
<INPUT name=logon_action type=submit value="Visitor Logon">
```

Fields

The following two fields are used to enter the user's user name and password. The name attributes must be specified as shown.

```
<INPUT name=username type=text>
<INPUT name=password type=password>
```

Required Macros

The following macros must appear within the FORM element. Each macro is replaced in the output with an INPUT element of type `hidden`.

```
@satmac()
@interface()
@java_works()
@secret()
@query()
```

Each macro is replaced in the output with an INPUT element with `type=hidden`.

For example, `@satmac()` is replaced in the output by a string similar to:
`<INPUT name=satMac type=hidden value=00e018094f7e>`
where `value` will be set to a MAC address.

Body Tag to Enable Logoff Popup

If you plan to use a Logoff pop-up window, you must include the following in the Body tag at the beginning of your Logon template:

```
<body ONLOAD="document.forms.logonForm.username.focus();
document.forms.logonForm.javaworks.value=1">
```

This enables the logon pop-up and positions the input focus (cursor) in the username field.

Optional Elements

Images

`<img src="/images/`*`image_name`*`">`

Images used by the 700wl Series system web pages are located in the `/images` directory. To use an image in a custom template, you must add it through the Rights Manager Customize Web Pages by Location page in the **Images for templates** field.

Note: *All file and path names are case sensitive. The "images" directory name must be all lower case.*

Passing an Authentication Realm Name

The realm field may be used to pass the name of an authentication realm ("*`realm_name`*") that should be used to authenticate users that log in through the location associated with this

page. To pass the authentication realm name without the user being aware of it, use a hidden input field:

```
<INPUT name=realm type=hidden value=realm_name>
```

If you want the user to be able to select among several realms when he/she logs in, you can use a SELECT statement with OPTIONS to create a drop-down selection list on your Login page.

In addition to including the realm field on the custom login page, the **User specified authentication realm** check box must be checked (on the Rights Manager Customize Web Pages by Location page). Note that this check box does not appear unless there are multiple authentication realms defined.

Rights Manager Functions

The following functions return information from the Rights Manager about the client:

`@loggedon()`	Returns 1 if the client is logged on, or was logged on but has expired. Returns 0 if the client is not logged on.
`@username()`	Returns the logon name of the client.
`@logon_error()`	Returns any error text generated during logon.
`@client_expire()`	Returns the expire time of the logged in client (UNIX time format). • Returns 0 if the client has expired • Returns -1 if the client never expires.

Miscellaneous useful functions:

The following are a number of functions that are useful for generating and presenting information on any of the customized web pages.

`@month(@client_expire())`	Returns the month as 0-11 based on the UNIX time returned by the `client_expire` function.
`@mday(@client_expire())`	Returns the day of the month as 1-31 based on the UNIX time returned by the `client_expire` function.
`@wday(@client_expire())`	Returns the day of the week as 0-6 based on the UNIX time returned by the `client_expire` function.
`@year(@client_expire())`	Returns the year as the actual year minus 1900, based on the UNIX time returned by the `client_expire` function.
`@xlate_month("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec", @client_expire_time())`	Returns the three-character month string based on the UNIX time returned by the `client_expire` function.
`@xlate_day("Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat", @client_expire_time())`	Returns the three-character day name string based on the UNIX time returned by the `client_expire` function.

`@add()`	Returns the sum of the arguments. For example, to return the current year, you would use: `@add(@year(@client_expire()), "1900")`
`@set(“variable”, “value”)`	Sets the value of a run-time variable. For example, to set the variable “month” to the month a client’s rights expire, you would use: `@set("month", @xlate_month("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec", @month(@client_expire())))` Variables are global.
`@get(“variable”)`	Returns the value of a variable.
`@gt("param1", "param2")`	Returns true if `Param1` is greater than `Param2`.

`@if()`
`@elif()`
`@else()`
`@endif()`
	Conditional execution depends on the truth value of the argument to `@if()`.
	Zero or more `@elif()`’s may be followed by zero or one `@else()`.
	`@endif()` is always required.

`@equal("arg1", "arg2")`	Returns 1 if the arguments are identical, 0 otherwise.
`@lt("arg1", "arg2")`	Returns 1 if `arg1` is less than `arg2`, 0 otherwise.
`@gt("arg1", "arg2")`	Returns 1 if `arg1` is greater than `arg2`, 0 otherwise.
`@le("arg1", "arg2")`	Returns 1 if `arg1` is greater than `arg2`, 0 otherwise.
`@ge("arg1", "arg2")`	Returns 1 if `arg1` is greater than `arg2`, 0 otherwise.
`@not("arg")`	Returns 0 if `arg` is an integer whose value is non-zero, 1 otherwise.

Logon Page Template — A More Advanced Example

Example 2 shows a more complete Logon page template. This template displays an image at the top of the page, formats the page output using tables, and also retrieves and displays the Expire Time for a logged on user who’s rights have a relative or fixed expiration.

Example 2

```
<!-- This template includes an image, displays fields in a table -->

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>HP ProCurve 700wl Series Logon Page</title>
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
</head>

<body bgcolor="FFFFFF">

<!-- specifies an image and a solid black line at the top of the form.
     The image must be stored in the Rights Manager via Images Upload -->
```

```
<center>
   <img src="/images/hp.jpg"><br>
   <img src="/dot-black.gif" width="600" height="1">
</center>

<font face="arial,helvetica,sans-serif">

@logon_error()<br>  <!-- outputs any errors that occur -->

<!-- if logged on, show user name. -->

@if(@loggedon())
  <center>
    <table width="600">
       <tr>
         <td align="left">Logged on as <font color="#666699"><b>@username()
              </b></font>
         </td>

<!-- if rights have an expiration time, display it -->

         <td align="left">
         @if(@gt(@client_expire(), "0"))
           You must logon again on <font color="#666699"><b>
           @xlate_day("Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat",
              @wday(@client_expire())),
           @xlate_month("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul",
              "Aug", "Sep", "Oct", "Nov", "Dec", @month(@client_expire()))
           @mday(@client_expire()),
           @add(@year(@client_expire()), "1900")</b></font>
           at <font color="#666699"><b>@time(@client_expire())</b></font>
         @endif() </td>
       </tr>
    </table>
  </center>

<!-- if not logged on, display message -->

@else()
    <center>You are not logged on</center><p>
@endif()

<p>
<center>

<!-- beginning of Logon Form, with required tag and functions -->

 <FORM action="/cgi-bin/logon" method=post name=logonForm>
 @satmac()
 @interface()
 @java_works()
 @secret()
 @query()

<!-- Displays user and password fields, and three buttons, in a table -->

 <table width="600" cellspacing="0" cellpadding="1" bgcolor="#000000">
```

```
   <tr><td>
       <table cellspacing="0" cellpadding="5" width="100%" bgcolor="#ffffff">
          <tr><td colspan=2" align="center" bgcolor="#99cc33"><font size=4
                  color="#ffffff"><b>User Login</b></font></td></tr>

<!-- Displays input fields -->

          <tr><td align="center">
              <table>
                 <tr><td align="right">Username:</td>
                     <td align="left"> <INPUT name=username type=text></td>
                 </tr>
                 <tr><td align="right">Password:</td>
                   <td align="left"> <INPUT name=password type=password></td>
                 </tr>
              </table>
              </td></tr>

<!-- Displays three buttons -->

          <tr><td align="center">
              <table>
                 <tr><td align="right" width="200"><INPUT name=logon_action
                         type=submit value="Logon User"></td>
                     <td align="center" width="100"><INPUT name=logon_action
                         type=submit value="Logon as a Guest"></td>
                     <td width="100" align="left"><INPUT name=logon_action
                         type=submit value=Logoff></td>
                 </tr>
              </table>
            </td></tr>
       </table>
   </td></tr>
</table>
</FORM>
</font>
</body>
</html>
```

This example generates the logon page shown in Figure B-2.

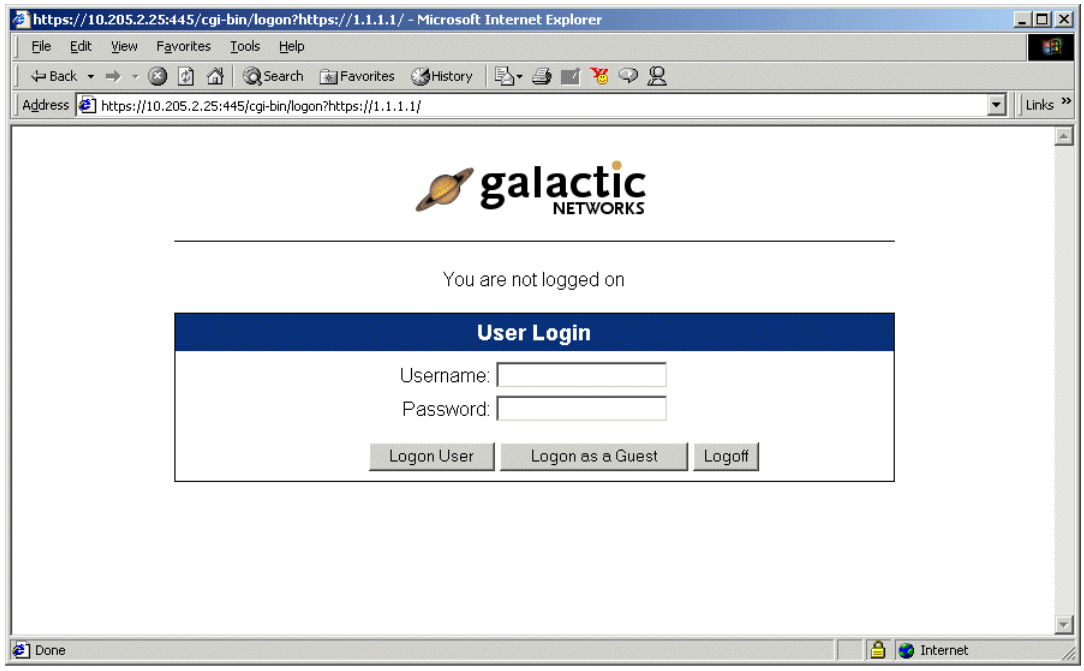

Figure B-2. Three-button logon page

The Guest Registration Template

To configure a location to allow custom guest registration, there are three elements that must be in place:

- The main logon page must have a **Register as Guest** button instead of the **Logon as a Guest** button. This requires changing the "value" attribute of the INPUT specification for the **Logon as a Guest** button.
- The **Use Guest Registration instead of Guest Logon** option *must* be selected on the Rights Manager Appearance page under Logon Options). If this is not selected, the Guest Registration page will not be displayed.
- A guest registration template may be added through the Rights Manager Customize Web Page by Location page. If you don't add a custom template, the default Guest Registration page is used. The username and password entered through the Guest Registration page is stored in the Rights Manager built-in database.

A Guest Registration template has basically the same required elements as a regular Logon page template. In addition, you can specify other input fields if you want to gather other information about your registered guests, such as their names, organizations or whatever. This information is not stored in the Rights Manager database, but will appear in the Session Log entry for the logon event.

The required elements in a Guest Registration template are:

The form tag:

```
<FORM action=/cgi-bin/logon method=post name=GuestRegForm>
```

A form with the name `GuestRegForm` is required, with action and method attributes set as shown.

Buttons:

One button must be present on the page to enable the user to log in.

```
<INPUT name=logon_action type=submit value="Register">
```

For this button, the name, type, and value attributes must be set exactly as shown. The value determines the function of the button:

- "Register" submits the Guest user name and password to be added to the built-in database, and logs the user in with Guest rights. The next time the user accesses the system, he / she will be able to log in using the username and password, but will still have only Guest rights.

Fields:

```
<INPUT name=username type=text>
<INPUT name=password type=password>
<INPUT name=confirm type=password>
```

These three fields are used to enter the user's user name and password, and to confirm the password. The name attributes must be specified as shown. Type=password is not required, but it keeps the value of the password hidden as it is typed, and is therefore recommended.

The following is an example of a Guest Registration page template. If specifies a form that includes the required input fields (username, password, and confirm) and two additional fields for **First Name** and **Last Name**. The two name fields are not added to the database, but will appear in the Session Log entry for this logon event.

The page generated by this template is shown in Figure B-3.

Example 3

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>HP ProCurve 700wl Series Guest Registration Page</title>
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
</head>

<body bgcolor="FFFFFF">

<!-- specifies an image and a solid black line at the top of the form. -->

  <center>
    <img src="/images/logo-galatic.gif"><br>
    <img src="/dot-black.gif" width="600" height="1">
  </center>
```

```
  <font face="arial,helvetica,sans-serif">

  <center>
    <br>Please register for Guest access.
  </center>

<!-- beginning of Guest Reg Form, with required tag and functions -->

<FORM action="/cgi-bin/logon" method=post name=GuestRegForm>
    @satmac()
    @interface()
    @java_works()
    @secret()
    @query()

<div align="center">
   <font color="#CC0000">
      @logon_error()  <!-- outputs any errors that occur -->
   </font>
</div>

<table width="325" cellspacing="0" cellpadding="1" bgcolor="#000000"
       align="center">
  <tr>
    <td>
      <table width="100%" cellspacing="0" cellpadding="5" bgcolor="#ffffff"
             align="center">
        <tr>
             <td colspan="2" align="center" bgcolor="#99cc33"><font size="4"
                 color="#ffffff"><b>Guest Registration</b></font></td>
        </tr>
        <tr>
             <td align="right"><font size="2"> First Name:</font></td>
             <td align="left"><INPUT type="text" name="firstname" size=15 />
             </td>
        </tr>

        <tr>
             <td align="right"><font size="2"> Last Name:</font></td>
             <td align="left"><INPUT type="text" name="lastname" size=15 />
             </td>
        </tr>

        <tr>
             <td align="right"><font size="2"> Preferred Username: </font>
             </td>
             <td align="left"><INPUT type="text" name="username"  size=15 />
             </td>
        </tr>

        <tr>
             <td align="right"><font size="2"> Password:</font></td>
             <td align="left"><INPUT type="password" name="password" size=15 />
             </td>
        </tr>

        <tr>
```

```
            <td align="right"><font size="2"> Confirm Password:</font></td>
            <td align="left"><INPUT type="password" name="confirm" size=15 />
            </td>
        </tr>

        <tr>
            <td align="center" colspan="2"><INPUT type="submit"
                name="logon_action" value="Register" /></td>
        </tr>
      </table>
    </td>
  </tr>
</table>
</FORM>
</font>
</body>
</html>
```

The page generated by this template is shown in Figure B-3.

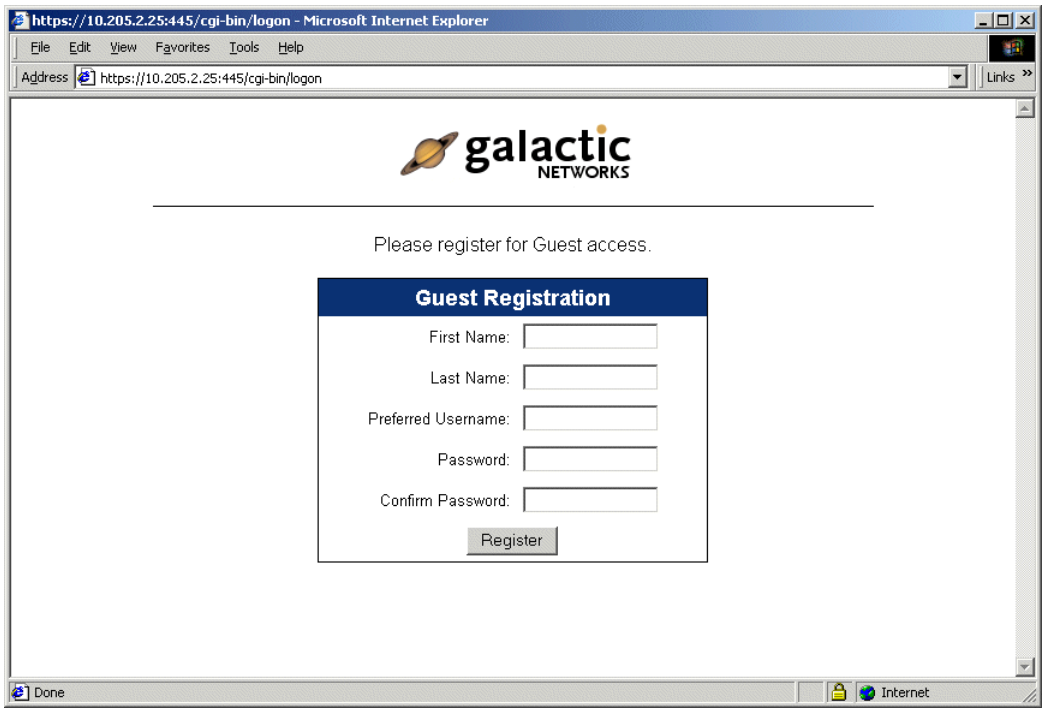

Figure B-3. Guest Registration page produced by the template in Example 3

Using a Logoff Pop-Up with a Customized Logon Page

One of options for user logoff, in browsers that support JavaScript, is to have a Logoff button appear in a pop-up browser window as soon as the user has logged on to the system. You can create your own template for this pop-up window. When the user clicks the Logoff button, he/she is logged off the 700wl Series system. By default, the Logon page is then displayed in the same window.

In addition to providing a Logoff template file through the Rights Manager Customize Web Page by Location interface, there are two other steps required to enable the Logoff pop-up feature:

Step 1. Enable the logoff pop-up capability by checking the **Pop open a logoff page when client does a logon** option in the Logoff Page Options section of the Customization page.

Step 2. Include the following statement as part of the Body tag in your customized Logon page template:

```
ONLOAD="document.forms.logonForm.username.focus();
document.forms.logonForm.javaworks.value=1"
```

For example, to enable a logoff pop-up in the template shown in “Example 2” on page B-7 you would change the body as follows:

```
<body bgcolor="FFFFFF";
ONLOAD="document.forms.logonForm.username.focus();
document.forms.logonForm.javaworks.value=1">
```

The system will use the default 700wl Series system Logoff pop-up page if you do not provide a customized Logoff page template.

The required elements in a Logoff Pop-up template are:

The form tag:

```
<FORM action=/cgi-bin/logon method=post name=logoffForm>
```

A form with the name logoffForm is required, with action and method attributes set as shown.

Buttons:

One button must be present on the page to enable the user to log off.

```
<INPUT name=logon_action type=submit value="Logoff">
```

The button name, type, and value attributes must be set exactly as shown.

The following is an example of a Logoff page template that displays the username as well as the Logoff button:

Example 4

```
<!-- Logoff Page Template File -->
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Logoff Page</title>
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<script type="text/javascript" language="JavaScript">

<!-- Hide script that controls window size
//<! [CDATA[
        window.blur();
        window.resizeTo(680, 350);
//]] End script hiding -->
```

```
</script>
</head>

<body bgcolor="FFFFFF">
<center>
  <img src="/images/hp.jpg"><br>
  <img src="/dot-black.gif" width="300" height="1">
</center>
<font face="arial,helvetica,sans-serif">

 <FORM action=/cgi-bin/logon method=post name=logoffForm>

   <table width="200" cellspacing="0" cellpadding="5" align="center">
     <tr><td align="center">Logged on as <font color="#006600">
        <b>@username()</b></font> </td></tr>
     <tr><td align="center"><INPUT name=logon_action type=submit
         value=Logoff></td></tr>
   </table>
 </FORM>

</font>
</body>
</html>
```

This generates the pop-up window shown in Figure B-4.

Figure B-4. Logoff pop-up window

When the user clicks the Logoff button, the Login window is immediately displayed in the same window, allowing the user to log in again.

Redisplaying the Logon Page in a New Window

The default 700wl Series system Logoff pop-up does not immediately display the Logon page; instead it displays a link that lets the user choose to go to the Logon page. The Logon page is displayed in a separate, fully functional browser window.

You can make use of this feature from your own Logoff pop-up window by including the following input statement within your FORM.

```
<input type="hidden" name="logoff_via_popup" value="1">
```

If you include this statement, upon clicking the Logoff button, the following is displayed in the Logoff pop-up window:

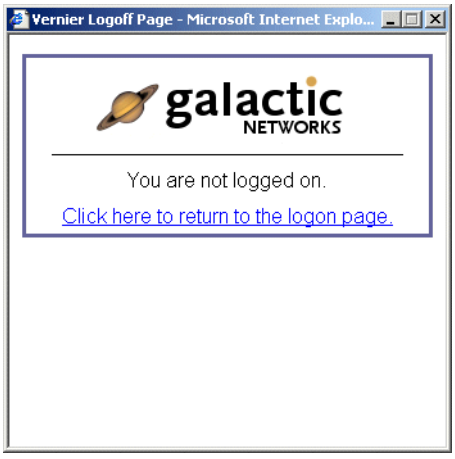

Figure B-5. Logoff confirmation window

When you click the link, the Login page opens in a new window.

Note that the appearance of this confirmation window is not currently customizable, except that the logo can be changed by customizing the logo at the top of the Rights Manager Customize Web Pages by Location page.

Customizing the Stop Page

Like the Logon, Logoff and Guest Registration pages, the Stop page can also be customized through a custom template file. However, because a Stop page typically does not require any buttons or input fields, this page in many cases may simply be a pure HTML page. There are no required elements for the Stop page. However, template functions may be used for functions such as retrieving the user name or displaying a user's expiration time, for example.

COMMAND LINE INTERFACE

C

This appendix documents the commands that are available on the serial console as part of the Command Line Interface (CLI). The CLI enables initial configuration and subsequent troubleshooting of the HP ProCurve Secure Access 700wl Series.

The Command Line Interface commands are listed in the following categories:

Accessing the Command Line Interface C-1
Getting CLI Command Help C-3
Administrator Access Control Commands C-3
System Status and Information Commands C-4
Network Configuration Commands C-6
Port Configuration Commands C-8
Access Controller Configuration C-10
Access Control Server Configuration C-13
Wireless Data Privacy Configuration C-15
Active Client Management Commands C-17
System Backup, Upgrade, and Shutdown Commands C-19
Diagnostic and Log Commands C-24
Time Configuration C-27
SNMP Configuration and Reporting Commands C-28

Note: *You can also configure these functions through the web-based interface.*

For an alphabetical listing of commands see the “Index of Commands” at the back of this manual.

Accessing the Command Line Interface

To use the Command Line Interface, you must connect a serial console to the serial port on an Access Controller, Access Control Server or Integrated Access Manager. The serial console is a terminal emulator running on another management computer. For details on connecting a serial console, see the section “Installation Using the Command Line Interface” in the Installation Guide for your 700wl Series system.

When the serial console establishes a connection, it displays a message "`Press return for console:`"

When you press return, you are prompted for your administrator login ID and password.

To exit the serial console, type the command:

```
exit
```

Command Syntax

You may see a variety of symbols shown as part of the command syntax. These symbols explain how to enter the command, and you do not type them as part of the command itself. Table C-1 summarizes command syntax symbols.

Table C-1. Command Syntax Symbols

Symbol	Description
angle brackets < >	Enclose a variable or value. You must specify the variable or value. For example, in the syntax `set datetime <date> <time>` you must supply a date string for `<date>` and a time string for `<time>` when entering the command. Do not type the angle brackets.
braces { }	Enclose a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax `logoff client {all | mac <mac-address>}` you must specify either "all" or "mac" followed by a MAC address when entering the command. Do not type the braces.
vertical bar |	Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax `set dhcp on | off` you can enter `set dhcp on` or `set dhcp off`. You cannot combine the options in a single help command. Do not type the vertical bar.
square brackets [ ]	Enclose an optional value or a list of optional arguments. For example, in the syntax `set dns <ip-address> [<ip-address>]` the second IP address (specifying a secondary DNS server) is optional. You can leave it out and specify only a primary DNS server. Do not type the square brackets.

Note: *Some commands, such as* **factoryreset**, *produce a prompt:*

```
Are you sure? [n]
```

The value in braces indicates the default value if you just Enter without typing a value.

Getting CLI Command Help

The following command provides help for the CLI commands.

help [diag | help | ipsec | snmp]

Displays a list of commands. When used without an argument, the top-level commands are listed. When a valid argument is specified, a list of commands for a command group are displayed.

Many commands, such as **add**, **clear**, **set**, or **show**, can be used with a large number of arguments. For these commands you can follow the command with a question mark to see a list of the options you can use with the command.

For example, to see a list of the possible **add** commands, type:

```
add ?
```

This produces the following output:

```
"add" commands:
 ad d bridging ...            Ad   d bridging options
 ad d snmpmanager ...         Ad   d an SNMP authorized manager
 ad d snmptrapreceiver ...    Ad   d an SNMP trap receiver
```

To see details about one of these commands, you can again use a question mark. For example to see details of the **add snmpmanager** command, you can type:

```
add snmpmanager ?
```

This produces the following output:

```
Usage: add snmpmanager <hostname> | <ip-address>[/<mask>]
```

Administrator Access Control Commands

The following commands configure web, console, and technical support access to the HP ProCurve system:

set admin <login-name> [<password> <password>]

Changes the console and web administrator login and password. Prompts for password if not entered on the command line.

clear admin

Removes the console and web administrator login and password. No login or password is required to access either Administration interface if the login and password have been cleared.

show admin

Shows the current administrator login. The password is not displayed.

set remote on | off

Enables or disables remote technical support access. The default is disabled. This should be enabled only at the direction of HP customer support personnel.

show remote

Displays the current remote technical support access setting.

System Status and Information Commands

show status

Displays an overview of the system status.

- For a Access Control Server, this command includes up time and the IP address, MAC address and connect time for each connected Access Controller.
- For an Access Controller, this command includes up time and the IP address and the connect time for itsAccess Control Server or Integrated Access Manager.
- For an Integrated Access Manager, this command includes a combination of the Access Control Server and Access Controller status.

The output for an Integrated Access Manager 760wl appears similar to the following:

```
Uptime:      4 hrs,  50 mins
Access Controller Function
 A ccess Control Server:  Use Integrated Server
 A ctive Clients:  None
Access Control Server Function
 E nabled:          Yes
 A ccess Controllers:  1 connected
    MAC Addr ess       IP A  ddress     Co   nnected
    00:e0:18 :7d:b5:3d   10.205.2.25    4    hrs, 50 mins
```

show id

Displays this system's ID, which is the MAC address of the Slot 0 port 0.

show ether [status]

Displays the configuration and status of the interface(s) in the system. The port currently configured as the uplink port has Uplink appended to the end of the status entry for that interface.

The default form of the command (`show ether`) displays the MAC Address, interface name, and supported media types (in parentheses) of each interface, as shown in the following example:

```
System Board: 1 Ethernet port
   0/1: 00: e0:18:7d:b5:3d, sis0, (100baseTX, 10baseT/UTP), Uplink

 S lot 3: 4 Ethernet ports
   3/1: 00: 80:c8:b9:21:60, dc3, (100baseTX, 10baseT/UTP)
   3/2: 00: 80:c8:b9:21:5f, dc2, (100baseTX, 10baseT/UTP)
```

```
   3/3: 00:80:c8:b9:21:5e, dc1, (100baseTX, 10baseT/UTP)
   3/4: 00:80:c8:b9:21:5d, dc0, (100baseTX, 10baseT/UTP)
```

The show ether status command displays the MAC Address, the currently configured media type/option, the active media type/option (in parentheses) and the link status, as shown in the following example:

```
Sy stem Board: 1 Ethernet port
   0/1: 00:e0:18:7d:b5:3d, autoselect (100baseTX <full-duplex>), active

Sl ot 3: 4 Ethernet ports
   3/1: 00:80:c8:b9:21:60, autoselect (none), no carrier
   3/2: 00:80:c8:b9:21:5f, autoselect (none), no carrier
   3/3: 00:80:c8:b9:21:5e, autoselect (none), no carrier
   3/4: 00:80:c8:b9:21:5d, autoselect (none), no carrier
```

show slots

Shows the card in each slot. The output for an Integrated Access Manager 760wl or Access Controller 720wl with two of the three slots filled appears as follows:

```
Slots:    3
 Sy stem Board:  2 Ethernet ports
 Sl ot 1:  Empty
 Sl ot 2:  4 Ethernet ports
 Sl ot 3:  4 Ethernet ports
```

show deviceport <device>

Shows the port or slot and port for a device.

<device>	The device name associated with a port, for example, dc0, dc1, sis0.

For example, on an Integrated Access Manager 760wl the command:

```
show deviceport sis0
```

displays the following output:

```
Slot/Port:  0/1
```

show product

Displays the product name. For example, on an Integrated Access Manager 760wl, this command displays:

```
Integrated Access Manager
```

show serial

Displays the product serial number. The output is similar to the following:

```
10-00E0187DB53D
```

show version

Displays the current software version. Also shows the alternate (upgrade, downgrade or same) version of the software, if one exists on the system. The output is similar to the following:

```
        Versi  on       Build  Date             Install Date
        -----  --       ------ --------------   --------------------
   Active: 3.1.43        Feb 2  4 18:21:49 2003  Feb 25  12:37:25 2003
      Alt: 3.0.36        Feb    7 01:22:18 2003  Feb 11  19:45:55 2003
   downgrade
```

Network Configuration Commands

set hostname <hostname>

Sets the system's hostname. The system hostname is also used as the SNMP system name. If you set a hostname, it must be resolvable through DNS.

<hostname>	The fully qualified host name of the system.

clear hostname

Clears the system's hostname.

set domainname <domainname>

Sets the domain name for a system that has not been configured with a hostname. The domain name is used to identify the domain of the system. In commands that take a hostname as an argument, such as **ping** or **nslookup**, if the hostnames are not qualified, this domain name is appended to the hostname.

clear domainname

Clears the domain name.

set ip { <ip-address> [<netmask>] | <ip-address>/<maskbits> }

Sets a static IP address for the device.

<ip-address>	The IP address to be assigned to the interface.
<netmask>	The subnet mask, in the form xxx.xxx.xxx.xxx (e.g., 255.255.255.0).
<maskbits>	The subnet mask, specified as the number of bits in the mask. For example, /30 is the equivalent of 255.255.255.252; /24 is the equivalent of 255.255.255.0.

show ip

Shows the current IP configuration. Output from this command looks similar to the following:

```
Hostname:
    Domain Name:    xyzcorp.com
    IP address:     192.168.10.157/24
    DHCP enabled:   No
    Default gateway:192.168.10.1
    DHCP server:    None configured
    DNS servers:    192.168.2.248 192.168.2.205
    WINS servers:   None configured
```

set gateway <ip-address>

Sets the IP address of the default router.

clear gateway

Clears the gateway IP address (resets to 0.0.0.0). This is the equivalent of the command **set gateway 0.0.0.0**.

set dhcp on | off

Enables dynamically assigned IP address configuration for this system. If disabled the system's IP address, subnet (netmask), gateway, and DNS servers must be set manually. The default (at factory reset) is ON.

set dhcpserver <ip-address>

Sets the IP address to be used as a DHCP server for clients connected to an Access Controller that does not use NAT.

<ip-address> The DHCP server IP address.

clear dhcpserver

Resets the currently configured DHCP server value.

show dhcpserver

Shows the currently configured DHCP server value, or "`Not Set`" if no DHCP server is configured.

set dns <primary-ip-address> [<secondary-ip-address>]

Sets the IP addresses of the DNS servers.

<primary-ip-address> The IP address of the primary DNS server for the system.

<secondary-ip-address> The IP address of the secondary DNS server for the system (optional).

clear dns

Clears the IP addresses of the DNS servers.

set sharedsecret [<secret> <secret>]

Sets the Access Controller and Access Control Server shared secret. Prompts for the secret if not entered on the command line.

clear sharedsecret

Clears the Access Controller and Access Control Server shared secret.

show sharedsecret

Shows whether the Access Controller and Access Control Server shared secret is set. The shared secret itself is not displayed. Output from this command is as follows:

```
Shared secret:  Set
```
or
```
Shared secret:  Not Set
```

Port Configuration Commands

The first set of commands in this section can be used on both an Access Controller or Access Control Server. The Access Controller-specific port commands apply only to downlink ports on an Access Controller or Integrated Access Manager.

set uplink [<slot>/<port>]

Sets the uplink port. `<slot>/<port>` specifies the port on a Gigabit Ethernet option card. For a single-port card, the port number will be 1.

There may be a slight delay before the port switch takes effect.

To reset the uplink port to the default network uplink port, enter the **set uplink** command without a port specification, or use the following port specifications:

- 0/1 (slot 0 port 1) for a 700wl Series or 5000 Series unit
- 0/2 (slot 0 port 2) for a 700wl Series unit

Caution: *Disconnect the system from the network before you issue this command. As soon as you reconfigure the uplink port, the port that was functioning as the uplink port prior to the reconfiguration becomes a downlink port. If it remains connected to your network, serious problems can occur.*

show uplink

Shows the current uplink port. Output from this command is similar to the following:

```
The uplink is configured at: Slot 0  Port 1
```

show portmedia <port> | <slot>/<port>

Shows the port media settings for the specified port or slot and port.

For example, the command:

```
show portmedia 3/1
```

displays output similar to the following:

```
Port 3/1 media settings
       Po    rt status:  active
 C  onfigured setting:  autoselect
Ac tive port setting:  100baseTX full-duplex
 S  upported settings:  autoselect
                      100b  aseTX full-duplex
                      100b  aseTX
                      10ba  seT/UTP full-duplex
                      10ba  seT/UTP
                      none
```

`Port status` can be `active` or `no carrier`.

`Configured setting` is the current setting as configured through the **set portmedia** command (or through the Advanced Network Settings page of the Administrative Notifies).

`Active port setting` is the setting actually in effect. For example, if the configured setting is `autoselect`, the Active port setting will be the actual setting as autonegotiated with the client device (computer, access point, hub, switch, etc.).

`Supported settings` lists the valid (supported) settings for the port. Any of these may be used with the **set portmedia** command for this port.

set portmedia {<port> | <slot>/<port>} "<media> [<media-option>]"

Sets the port media setting for the specified port or slot and port.

<port> | <slot>/<port>	The port, or slot and port on which to set the media type and option.
<media>	The media type, for example `100baseTX` or `10baseT/UTP`. Must match one of the valid media types for the port, as displayed in the show portmedia command for the port.
<media-option>	A media option, for example `full-duplex`. This is not required. If used, the media plus media-option specification (within the quotes) must match one of the valid settings for the port as displayed by the show portmedia command for the port.

You can use the **show portmedia** command to get a list of supported media and media option settings.

clear portmedia <port> | <slot>/<port>

Clears the port media setting for the specified port or slot and port. The setting reverts to autoselect.

Access Controller Port Configuration Commands

The following commands are available only from an Access Controller or Integrated Access Manager.

set portip { <port> | <slot>/<port> } <ip-address> <netmask>

Sets the IP address and subnet mask for the specified port.

<port> | <slot>/<port>	The port, or slot and port to which the IP address is to be assigned.
<ip-address>	The IP address to be assigned to the interface.
<netmask>	The subnet mask, in the form xxx.xxx.xxx.xxx (e.g., 255.255.255.0). The /<maskbits> form (e.g., /24) cannot be used in this command.

clear portip <port> | <slot>/<port>

Clears the IP address and subnet mask for the specified port or slot and port.

show portip

Displays the current IP address and netmask settings, if set, for all ports in the system. Output from this command is similar to the following:

```
Port settings
 S lot 1 Port 1  IP: Not set
 S lot 1 Port 2  IP: 192.168.5.1      Net   mask:  255.255.255.0
 S lot 1 Port 3  IP: 192.168.6.1      Net   mask:  255.255.255.0
 S lot 1 Port 4  IP: Not set
 S lot 2 Port 1  IP: Not set
 S lot 2 Port 2  IP: Not set
 S lot 2 Port 3  IP: Not set
 S lot 2 Port 4  IP: Not set
 S lot 3 Port 1  IP: Not set
 S lot 3 Port 2  IP: Not set
 S lot 3 Port 3  IP: Not set
 S lot 3 Port 4  IP: Not set
```

Access Controller Configuration

The commands in this section are available only on an Access Controller or an Integrated Access Manager. The exceptions are the **set controlserver**, **clear controlserver**, and **show controlserver** commands, which are not available on an Integrated Access Manager.

set controlserver <ip-address>

For an Access Controller, sets the IP address of its Integrated Access Manager.

Note: *This command is not available on an Integrated Access Manager.*

clear controlserver

For an Access Controller, clears the Access Control Serveror Integrated Access Manager IP address.

Note: *This command is not available on an Integrated Access Manager.*

show controlserver

For an Access Controller, shows the Access Control Server or Integrated Access Manager IP address. Output from this command appears similar to the following:

```
Access Control Server:  192.168.2.15
```

Note: *This command is not available on an Integrated Access Manager.*

Advanced Network Configuration

Caution: *Any modifications to the bridging settings will log off all clients.*

set bridging on | off

Enables and disables bridging. This command will log off all connected clients.

add bridging <pre-defined-type> | <quoted-custom-bridging-string>

Adds a bridging option. This command will log off all connected clients.

<pre-defined-type>	One of the following pre-defined bridge types: • cdp: Cisco Discovery Protocol • wnmp: Wireless Network Access Protocol • atalk: AppleTalk
<quoted-custom-bridging-string>	A string, enclosed in quotes, that specifies a custom bridging type. See Section 2.4.1, “Advanced Network Settings” in Chapter 2, and Appendix A, “Filter Expression Syntax” for a detailed discussion.

delete bridging <pre-defined-type> | <quoted-custom-bridging-string>

Removes a bridging option. See the table under the **add bridging** command for a specification of the argument values. This command will log off all connected clients.

show bridging

Shows the current bridging settings.

The current bridging types that may appear are:

cdp	Cisco Discovery Protocol
wnmp	Wireless Network Access Protocol

atalk	AppleTalk protocol
custom	Type was set using a custom bridging string. See Section 2.4.1, “Advanced Network Settings” in Chapter 2, and Appendix A, “Filter Expression Syntax” for a detailed discussion.

For example, output from this command, if bridging is enabled, is similar to the following:

```
Bridging is enabled
Configured bridges:
 c dp: ether [12:2] <= 1514 and ether dst 01:00:0c:cc:cc:cc
 w nmp: ether [12:2] = 0x8781 and ether[0:4] = 0x01a0f8f0
 c ustom: ether[12:2] = 0x8037 or ether[12:2] = 0x8137
```

set clientprobes <interval> <timeout>

Configures the interval and timeout for the Access Controller client probe, sent to clients that have been idle to determine if they should be disassociated. The interval specifies the length of the idle period before the Access Controller sends a client probe. If a client remains idle, the probe is sent once per interval, until the timeout is reached. The timeout specifies the total length of time to wait, given no response to the client probes, before sending a disassociate message to the Rights Manager.

<interval>	The number of idle seconds to wait before sending a client probe. The default is 30 seconds.
<timeout>	The total number of idle seconds to wait before disassociating a client that has been idle and has not responded to repeated probes. This must be at least twice the interval setting. The default is 300 seconds.

When a client is disassociated, its MAC address and set of rights are removed from the Access Controller, and the Rights Manager begins the linger timer countdown. If the linger timer expires without any activity from the client, the client will be required to re-authenticate when it resumes activity.

show clientprobes

Displays the current configuration of the client probe timers. Output from this command is similar to the following:

```
Client probes
 I nterval:  30 seco nds of idle time
 T imeout:   300 sec onds of idle time
```

set forwardipbroadcasts { none | <port-list>}

Specifies the ports that should have IP broadcast forwarding enabled.

none	Disables IP broadcast forwarding on all ports.

<port-list>	A space-separated list of one or more port numbers, in the form <port> or <slot>/<port>. For example:
	• For a Integrated Access Manager 760wl or Access Controller 720wl system, the command to set IP broadcast forwarding on all four ports is:
	`set forwardipbroadcasts 1 2 3 4`
	• For a Integrated Access Manager 760wl, Integrated Access Manager 760wl, Access Controller 720wl, or Access Controller 720wl system the command to set IP broadcast forwarding on all four ports of slot 1 is:
	`set forwardipbroadcasts 1/1 1/2 1/3 1/4`

show forwardipbroadcasts

Shows the list of ports or slots and ports that have IP broadcast forwarding enabled. For example, output from this command for an Access Controller or Integrated Access Manager with 12 ports appears as follows:

```
Enabled on:    1/1  1/2  1/3  1/4  2/1 2/2  2/3  2/4   3/1  3/2  3/3
3/4
```

Access Control Server Configuration

The following commands are available only on a Access Control Server or Integrated Access Manager, except for the **show syslogserver** and **show natdhcp** commands, which are also available on an Access Controller.

delete am mac <mac-address>

Removes an Access Controller's configuration information (tunneling and HTTP proxy settings) from the Access Control Server's or Integrated Access Manager's database. This command lets you remove the configuration information for an Access Controller that has been disconnected from the system.

show am [httpproxy | tunnel] [mac <mac-address>]

Shows Access Controller settings for one or all Access Controllers known to the Access Control Server or Integrated Access Manager. The default is to show all settings for all Access Controllers.

httpproxy	Specifies that HTTP Proxy settings should be displayed
tunnel	Specifies that PPTP/L2TP/IPSec settings should be displayed
mac <mac-address>	Specifies the MAC address of an Access Controller

The **show am** command with no parameters shows basic information about the connected Access Controllers, including the length of time they have been running and the software version currently running and the length of time the unit has been up.

set am httpproxy mac <mac-address <proxy-ip> <proxy-port>

Configures an HTTP Proxy server for one of the Access Controllers configured on this Access Control Server or Integrated Access Manager.

<mac-address>	Specifies the MAC address of the Access Controller
<proxy-ip>	Specifies the IP address of the Proxy Server
<proxy-port>	Specifies the TCP port number used by the Proxy Server

clear am httpproxy all | mac <mac-address

Clears the HTTP proxy setting for a specified Access Controller or for all Access Controllers configured on this Access Control Server or Integrated Access Manager.

all	Specifies that settings for all Access Controllers should be cleared
mac <mac-address>	Specifies the MAC address of an Access Controller

set syslogserver <ip-address< [<facility>]

Sets the IP address of a syslog server, and the logging facility. Setting the syslog server address enables session logging.

<ip-address>	The syslog server IP address.
<facility>	The syslog server logging facility. Valid facilities are daemon, user, and local0 - local7. The default is daemon.

clear syslogserver

Clears the IP address of a Syslog server. This disables session logging.

show syslogserver

Note: *Even though you can only configure the Syslog server address from a Access Control Server or Integrated Access Manager, you can also use the show syslogserver command from an Access Controller to view the syslog settings.*

Shows the current setting of the syslog server options.

Advanced Network Configuration

set natdhcp <ip-address> <subnetmask> [<lease-time> [<time-units>]]

Sets the NAT DHCP subnet and lease time.

<ip-address>	The DHCP subnet address for NAT. The default is `42.0.0.0`.
<subnetmask>	The subnet mask, in the form xxx.xxx.xxx.xxx (e.g., 255.255.255.0). The /<maskbits> form (e.g., /24) cannot be used in this command.
<lease-time>	The length of time a lease remains valid, in units as specified by the time-units parameter. Defaults to 86,400 seconds (one day).
<time-units>	The time units in which the lease time is specified. Can be one of `seconds`, `minutes`, `hours`, `days`, `weeks`, or `months`. Default is seconds.

clear natdhcp

Resets the currently configured internal DHCP server value used for NATed clients.

show natdhcp

Note: *Even though you can only configure the DHCP server NAT address range from the Access Control Server or Integrated Access Manager, you can use the show natdhcp command from an Access Controller to view these settings.*

Shows the currently configured DHCP server values for NATed clients. Output from this command appears as follows for the default NAT DHCP configuration:

```
NAT IP Base:      42.0.0.0
NAT Subnet Mask:  255.0.0.0
Lease Time:       1 day
```

Wireless Data Privacy Configuration

Wireless data privacy is configured and maintained centrally on a Access Control Server or Integrated Access Manager, but the settings are propagated to and are implemented / enforced by the Access Controller. The following commands, except for the **show airwave** command, are not available on an Access Controller.

set pptp on | off

Enables or disables PPTP.

set l2tp on | off

Enables or disables L2TP.

set ipsecsecret [<secret> <secret>]

Sets the IPSec shared secret. Prompts for the secret if not entered on the command line.

clear ipsecsecret

Clears the IPSec shared secret.

set espencryption [des] [3des] [blowfish] [cast] [aes] [none]

Sets the IPSec ESP encryption methods. You must specify at least one method.

set espintegrity [md5] [sha1] [none]

Set the IPSec ESP integrity methods. You must specify at least one method.

set ikedh [group1] [group2] [group5]

Set the IPSec IKE Diffie-Hellman groups. You must specify at least one group.

set ikeencryption [des] [3des] [blowfish] [cast]

Set the IPSec IKE encryption methods. You must specify at least one method.

set ikeintegrity [md5] [sha1]

Set the IPSec IKE integrity methods. You must specify at least one method.

set ipsec on | of}

Enables or disables IPSec.

set ssh on | off

Enables or disables ssh for wireless data privacy.

show airwave

Note: *Even though you can only configure wireless data privacy settings from the Access Control Server or Integrated Access Manager, you can use the show airwave command from an Access Controller to view these settings.*

Shows the current wireless data privacy settings. Output from this command is similar to the following:

```
IPSec:                 Disabled
  IPSec shared secret:   Not set
  IKE Encryption:        DES  3-DES
  IKE Integrity:         SHA-1
  IKE Diffie-Hellman:    Group 1  Group 2
  ESP Encryption:        DES  3-DES  Blowfish
  ESP Integrity:         MD5  SHA-1
PPTP:                  Enabled
L2TP:                  Enabled
Tunnel IP:             DHCP
  Range:                 Not set
SSH:                   Disabled
```

set am tunnel mac <mac-address> {dhcp | range <ip-address1> <ip-address2>}

Sets the range of IP addresses for PPTP, L2TP, and IPSec tunnelling for an Access Controller. These addresses can be obtained through DHCP or within a specified range of addresses.

mac <mac-address>	Specifies the MAC address of the Access Controller.
dhcp	Specifies that the addresses should be obtained via DHCP.
range	Specifies that a range of IP addresses should be used. <ip-address1> defines the first address in the range. <ip-address2> defines the last address in the range.

clear am tunnel all | mac <mac-address

Clears the PPTP, L2TP, and IPSec tunnelling settings for a specified Access Controller or for all Access Controllers connected to this Access Control Server or Integrated Access Manager.

all	Specifies that settings for all Access Controllers should be cleared.
mac <mac-address>	Specifies the MAC address of an Access Controller

Active Client Management Commands

Use these commands to manage Active Clients from an Access Controller or Integrated Access Manager. These commands cannot be used from a Access Control Server.

show clients [mac <mac-address>] [sort {mac | ip | user | machine | port | sessions | idle}] [reverse]

Lists all active clients. You can optionally sort the list by a number of criteria.

<mac-address>	MAC (Ethernet) address to display. Specified in the format: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx (colons are optional).
sort	Sort the clients according to one of the following criteria (one must be specified): • mac: by MAC address • ip: by IP address • user: by user name • machine: by machine name. (Note that some clients, such as Apple systems, may allow special characters in their names, and these may be displayed differently in this list.) • port: by Access Manage port • sessions: by number of running sessions • idle: by idle time duration
reverse	Keyword that reverses the order of the display, which normally displays the most recent events first (in ascending order).

show client mac <mac-address> [rights]

Lists active sessions for a client. Shows client rights if requested.

<mac-address>	MAC (Ethernet) address to display. Specified in the format: `xx:xx:xx:xx:xx:xx` or `xxxxxxxxxxxx` (colons are optional).
rights	Keyword that specifies that the XML that defines the client rights should be included in the display.

The following command:

```
show client mac 00:00:86:5a:78:18 rights
```

Produced the following output:

```
              User:  ann
      Machine name:  ANNMCC-MOBILE
       MAC address:  00:00:86:5a:78:18
        IP address:  42.23.184.102
    Address status:  NAT mode: rights do not allow use of non-NAT IP address
    Access Controller:  10.205.2.25
         Slot/Port:  3/1
  Client Rights
    These rights expire in 48 mins, 43 secs:
  <?xml version="1.0" standalone="yes"?>
  <client_rights>
      <expiry>2923</expiry>
      <id>ann</id>
      <allow_real_ip>False</allow_real_ip>
      <allow_static_ip>False</allow_static_ip>
      <ip_addr_policy>do_nat</ip_addr_policy>
      <encryption_required>False</encryption_required>
      <ipsec>
         <stance>Deny</stance>
      </ipsec>
      <pptp>
         <stance>Deny</stance>
         <mppe_stance>Accept</mppe_stance>
         <mppe_bits>0</mppe_bits>
         <mppe_stateful>False</mppe_stateful>
         <min_mschap>0</min_mschap>
         <allow_pap>False</allow_pap>
         <allow_chap_md5>False</allow_chap_md5>
      </pptp>

          ...  (client rights abbreviated to save space)

  </client_rights>

  Active Sessions
  Protocol      Source               Destination          Xmit   Recv   Idle
  -----         -------------------  -------------------  -----  -----  -----
  UDP   Client: 42.23.184.102:137     42.0.0.1:137        4842   2856   23s
  TCP   Client: 42.23.184.102:1223    10.205.2.25:443     1169   921    1m17s
  TCP   Client: 42.23.184.102:1221    1.1.1.1:443         951    1945   1m28s
        Actual: 42.23.184.102:1221    10.205.2.25:443
```

logoff client {all | mac < mac-address> }

Logs off a client or all clients. You are asked to confirm this action.

all	Keyword the specifies that all clients should be logged off.
<mac-address>	MAC (Ethernet) address of the client to log off. Specified in the format: `xx:xx:xx:xx:xx:xx` or `xxxxxxxxxxxx` (colons are optional).

System Backup, Upgrade, and Shutdown Commands

The following commands support the backup of the current system configuration, and restore of a saved configuration; downloading new software versions; and rebooting, shutting down the system, or resetting it to its factory default configuration.

Backup and Restore

create backup

Creates a backup image. Because this will temporarily disconnect all clients, you are prompted to confirm that you want to do this. The following is an example of the messages that appear on an Integrated Access Manager:

```
Creating a system backup will momentarily shut down this Integrated
Access Manager.
All client machines will be temporarily disconnected.

Are you sure you want to briefly shut down the system
and create a backup [n]?
```

If you respond Y to continue with the backup, the following reminder appears:

```
NOTE:  After creating the backup image, you must transfer
  it from this Integrated Access Manager onto your local computer.
```

store backup <url> [<filename>]

Stores the backup on another system using FTP. This command can be used only after a backup has been created.

<url>	The URL encoded location to store the backup. The format of the URL is `ftp://<`*`host`*`>` or `ftp://<`*`username`*`>[:<`*`password`*`>]@<`*`host`*`>`
	<*username*>[:<*password*>] specifies a username and optional password with access to the remote site, if required.
	The host must be an FTP server.
<filename>	The destination filename for the backup image. The default is `hp-yyyy-mm-dd`.
	For anonymous FTP, the path is relative to the FTP root. If a username and password is required for FTP, then the full path to the update file must be specified.

If you do not have access to an FTP site, you can use the browser-based Administrative Interface to store the file onto the local system.

get backup <url>

Retrieves a stored backup from another system using FTP.

<url>	The URL encoded location (including the file name) where the backup is stored. The format of the URL is `ftp://<host>/<backupfile>` or `ftp://<username>[:<password>]@<host>/<backupfile>` `<username>[:<password>]` specifies a username and optional password with access to the remote site, if required. `<backupfile>` is the filename (including the path) of the backup image. The host must be an FTP server.

If the backup file was stored to your local system using the browser-based Administrative Interface, you can use that same interface to retrieve and restore the backup file from your local system.

restore backup

Restores a retrieved backup.

Restoring a system backup reboots the system and replaces all current information (configuration, logs, etc.) with information stored in the backup image. All clients are disconnected by this operation. The only configured setting not replaced by the restore operation is the uplink setting. The uplink will remain as configured on the target system.

cancel backup

Cancels a running `store backup` or `get backup` task.

show backup

Displays information about the list of local backups and the status of a running store backup or get backup task. Output from this command is similar to the following:

```
Backup image created Nov 25 17:25:22 2002.
No backup image 'store' or 'get' in progress.
```

Upgrading the System Software

get upgrade <url> <key> [reboot | version | mindowngrade]

Downloads a software release from a specified URL via FTP, HTTP, or TFTP. This starts a background task that can be checked with the **show upgrade** command. If you do not include the `reboot` option, the downloaded version is stored as the alternate version, and is not activated until you reboot the system with the alternate version option

included. When you reboot to an alternate version, the new version becomes the installed version, and the previously installed version becomes the alternate.

The default URL to get the latest software from HP is:

```
ftp://ftp.hp.com/pub/networking/700software/ambit-hp
```

For a flash-based Access Controller, the default URL is:

```
ftp://ftp.hp.com/pub/networking/700software/ambit-am-hp
```

Command options can be used to do the following:

— Reboot the unit as soon as the download is complete. This makes the downloaded version the new installed version. Your configuration settings are preserved.

— Display the release version available for download without actually doing the download. This allows you to verify that the version is appropriate or what you expect before you download it.

— For the release version available at the URL you specify, display the lowest (oldest) version of the software to which you may downgrade without requiring a factory reset (which will reset the unit to its default settings).

This option allows you to determine whether, if you install the version available at the URL, you will be able to revert to your old version without having to do a factory reset.

<url>	The URL encoded location of the software release to install. The format of the URL is <*protocol*>*://*<*host*>*/*<*update file*> or <*protocol*>://<*username*>[:<*password*>]@<*host*>/<*update file*>
	<*protocol*> can be ftp, http, or tftp.
	<*username*>[:<*password*>] specifies a username and optional password with access to the remote site, if required.
	<*update file*> is the filename (including the path) of the software image. For TFTP or anonymous FTP, the path is relative to the FTP or TFTP root. If a username and password is required for FTP, then the full path to the update file must be specified. For HTTP, the path is always relative to the web server's site root directory.
	The host must be an FTP, HTTP, or TFTP server.
<key>	The software release install key obtained from HP ProCurve.
reboot	Automatically reboot after installing the upgrade. The upgraded software is activated when the system is rebooted.
version	Displays the version of the software available for download at the specified URL.
	The software is not downloaded and the system is not restarted.
mindowngrade	For the software version at the specified URL, displays the lowest version to which you may downgrade without requiring a factory reset.
	The software is not downloaded and the system is not restarted.

- When you initiate the **get upgrade** command, messages similar to the following appear:

```
Upgrade download initiated.
  Status of upgrade started Nov 26 16:35:08...
    Downloading new image file...  2.7MB/50.4MB received.
  Note:  Use the 'show upgrade' command to see the current status.
```

- When you initiate the **get upgrade** command using the **mindowngrade** argument, the version at the URL you specify is compared to the currently running image version. If a factory reset would be required in order to switch between these two versions, then a message similar to the following appears:

```
Minimum downgrade for the version at that URL: <future version here>
Installed version: 3.1.41
A factory reset would be required to return to the current version
after
installing the version at that URL.
```

  If the current version and the version at the URL are compatible (no factory reset required) then the minimum version to which you could downgrade without a factory reset is reported:

```
Minimum downgrade version: 2.1.642
```

- When you initiate the **get upgrade** command with the **version** argument, a variety of messages may appear, depending on the relationship between the current (running) version and the version at the URL you specify:

```
The version at that URL is a downgrade(Version: 3.0.36)
```

show upgrade

Shows the status of the **get upgrade** task. The output can be similar to the following:

```
Status of upgrade started Nov 26 16:35:08...
  Unpacking image file.
```

or

```
Status of upgrade started Nov 26 16:35:08...
  New image successfully installed Nov 26 16:37:45
```

cancel upgrade

Cancels the current **get upgrade** task.

set upgradeproxy [on | off] [host <ip-address> [<port>]] [user <user> [<password>]]

Configure a proxy server for retrieving software releases via FTP.

on | off	Enables and disables the proxy server.
<ip-address>	Specifies the proxy server IP address.
<port>	(Optional) TCP port for the proxy server. Default is 3128.
<user >	(Optional) User name needed for access to proxy server.
<password>	(Optional) User password.

clear upgradeproxy

Resets the proxy server settings used for retrieving software releases via FTP.

show upgradeproxy

Shows the current upgrade proxy server configuration. The following is an example of the output when no proxy is set:

```
Upgrade Proxy settings
  Proxy enabled: No
        Host IP: Not set
           Port: 3128
           User: Not set
       Password: Not set
```

Stopping and Restarting the System

reboot [upgrade | downgrade | same]

Restarts the system.

Optionally, you can specify that the reboot should use the alternate version of the system software. The alternate version installed on the system must match the type you specify. For example, if the alternate version is a newer version than the current version, it is type upgrade. If the alternate version is an older version, it is type downgrade.

Use the **show version** command to determine the type of the alternate version.

You are prompted to confirm that you want to reboot.

upgrade	Reboot using the alternate version, which is a newer version than the currently active system software.
downgrade	Reboot using the alternate version, which is an older version than the currently active system software.
same	Reboot using the alternate version, which is the same version as the currently active system software.

shutdown

Shuts down the system. You are prompted to confirm that you want to shut down the system:

```
This operation will shutdown this system and users may lose
 their connections.

Are you sure you want to shutdown this system [n]?
```

Resetting to Factory Defaults

factoryreset

Resets all user configurable data to the factory defaults. This includes all network configuration parameters. For example, if you have set a static IP address using the **set ip** command, after a factory reset DHCP is enabled and the static IP address is gone.

Warning: *A factory reset will change a reconfigured uplink port back to the default uplink. If you have reconfigured the uplink port (for example, to make use of a gigabit fiber port on an option card) that port will become a downlink port when the system comes back up after the reset. This can have adverse effects on your network.*

You are prompted to confirm that you want to do this:

```
This operation will erase all configuration information and
   return this system to factory default settings.

    Are you sure you want to perform a factory reset [n]?
```

Caution: ***ALL*** *configuration changes you have made to your system will be lost when you do a factory reset. It is* ***strongly*** *recommended that you back up your system before doing a factory reset.*

Diagnostic and Log Commands

The following commands may be used to display the 700wl Series system log files, and to diagnose network connectivity problems.

show logs [<severity>] [max <lines>] [for <count> <time-units>] [search <quoted-text>] [reverse]

Displays entries in the error log.

You can filter the display with the following arguments:

<severity>	Show only log entries that match or exceed this severity level: The default is `notice`. • crit: show only critical log entries. • err: show both error and critical log entries. • warn: show all warning, error and critical log entries. • notice: show all notice, warning, error, and critical log entries. • info: show all information, notice, warning, error, and critical log entries.
<lines>	The maximum number of lines to be displayed. The default is 23.
<count>	The number of time units to be displayed, in combination with the <time-unit> variable. If no “for” argument is given, the default is one day.
<time-unit>	The time unit associated with the <count>. May be one of seconds, minutes, hours, days, weeks, or months (31 days); If no “for” argument is given, the default is one day.
<quoted-text>	Displays entries containing the specified text string, which must be enclosed in quotes.
reverse	Keyword that reverses the order of the display, which normally displays the most recent events first.

For example, the command:

```
show logs info max 40
```

generates output similar to the following:

```
Jul 17 10:34:46: Info: Kernel: IP address 192.168.10.17 moved from
00:02:e3:14:40:3f to 00:bd:2e:dc:75:66 on the network side
Jul 17 10:34:46: Info: Kernel: IP address 192.168.10.17 moved from
00:bd:2e:dc:75:66 to 00:02:e3:14:40:3f on the network side
Jul 17 10:28:28: Info: Kernel: IP address 192.168.10.172 moved from
00:02:e3:14:40:3f to 00:80:c8:b9:aa:ed on the network side
Jul 17 10:28:27: Info: Kernel: IP address 192.168.10.172 moved from
00:80:c8:b9:aa:ed to 00:02:e3:14:40:3f on the network side
Jul 17 09:59:20: Info: Kernel: IP address 192.168.10.173 moved from
00:02:e3:14:40:3f to 00:80:c8:b9:aa:ed on the network side
Jul 16 17:15:52: Info: Uplink port configured at slot 0, port 1
Jul 16 14:19:59: Error: Kernel: stray irq 7
Jul 16 14:17:10: Info: Uplink port configured at slot 0, port 1
Jul 16 14:16:07: Info: Uplink port configured at slot 0, port 1
Jul 16 14:16:01: Info: DHCP client: lease for 192.168.10.60 to be
renewed in 282 seconds
Jul 16 14:16:00: Info: Uplink port configured at slot 0, port 1
Jul 16 14:16:00: Notice: DHCP client: new default router is
192.168.10.1
Jul 16 14:16:00: Notice: DHCP client: new DNS server is 192.168.2.248
Jul 16 14:16:00: Info: DHCP client: using IP address 192.168.10.60/24
Jul 16 14:16:00: Info: DHCP client: received DHCPACK from 192.168.10.1
Jul 16 14:15:59: Info: DHCP client: sending DHCPREQUEST to
255.255.255.255
Jul 16 14:15:59: Info: DHCP client: received DHCPOFFER from
192.168.10.1
Jul 16 14:15:59: Info: DHCP client: sending DHCPDISCOVER to
255.255.255.255
Jul 16 14:15:56: Info: Uplink port configured at slot 0, port 1
Jul 16 14:15:50: Error: Kernel: stray irq 7
Jul 16 14:15:50: Notice: HP process started, version 3.1.534
Jul 16 14:15:50: Notice: system was factory reset: requested from
console
```

clear logs

Clears the error log.

nslookup <hostname>

Returns the IP address for a hostname. If the hostname is not qualified, the domain name (as specified by the **set domainname** command) is appended.

Translates to:

```
nslookup –timeout=10 <hostname>
```

ping {<ip-address> | <hostname>}

Pings an IP address or a hostname. If the hostname is not qualified, the domain name (as specified by the **set domainname** command) is appended.

Translates to:

```
ping –c 3 <ip-address>
```

or

```
ping –c 3 <hostname>
```

debug ip [<slot>/<port>]

Shows IP traffic on an interface. The default (no slot / port specified) is the configured uplink.

<slot>/<port>	The slot and port for which IP traffic should be displayed.

This command translates to:

```
tcpdump –en –i <interface> ip
```

This command displays tcpdump output until you terminate the command with a CTRL-C. Upon termination, the console session is restarted, and you must log in again.

debug interface [<slot>/<port>]

Shows traffic on an interface. The default (no slot / port specified) is the configured uplink.

<slot>/<port>	The slot and port for which traffic should be displayed.

This command translates to:

```
tcpdump –en -i <interface>
```

This command displays tcpdump output until you terminate the command with a CTRL-C. Upon termination, the console session is restarted, and you must log in again.

debug tcpport <tcp port> [<slot>/<port>]

Shows specified TCP port traffic on an interface. The default (no slot / port specified) is the configured uplink.

<tcp port>	The TCP port number that identifies the traffic to be watched.
<slot>/<port>	The slot and port for which IP traffic should be displayed.

This command translates to:

```
tcpdump –en –i <interface> tcp port <port>
```

This command displays tcpdump output until you terminate the command with a CTRL-C. Upon termination, the console session is restarted, and you must log in again.

traceroute {<ip-address > | <hostname>} [<hops> [<probes> [<probewait>]]]

Displays the traceroute for an IP address or hostname.

If the hostname is not qualified, the domain name (as specified by the **set domainname** command) is appended.

<hops>	The maximum number of hops to trace. The default is 5.
<probes>	The maximum number of probes per hop. The default is 3.
<probewait>	The maximum number of seconds to wait for each probe. The default is 2.

This command translates to:

```
traceroute –n -m <hops> -q <probes> -w <probewait> <ip-address>
```

or

```
traceroute –n -m <hops> -q <probes> -w <probewait> <hostname>
```

Time Configuration

set timezone <general-tz> <specific-tz>

Sets the local timezone.

The `set timezone` command with no arguments returns a list of the general timezone areas. The command with only a general timezone specification returns a list of the specific timezone areas within the specified general timezone.

<general-tz>	The less specific portion of the timezone string. If the timezone is “America/Los_Angeles”, the general portion is “America”. Case-sensitive.
<specific-tz>	The more specific portion of the timezone string. If the timezone is “America/Los_Angeles” the specific portion is “Los_Angeles”. Case-sensitive.

set ntpserver{< ip-address> | <hostname>} [<ip-address> | <hostname>]

Specifies the IP address or hostname of a primary and secondary Network Time Protocol (NTP) server. Hostnames must be fully qualified if specified.

<ip-address>	An NTP server IP address.
<hostname>	An NTP server hostname. This must be a fully qualified domain name.

clear ntpserver

Clears the NTP servers IP address or hostnames. This command also disables the NTP service if it was enabled.

set ntp on | off

Enables and disables the NTP service.

set datetime <date> <time>

Manually sets the current local date and time.

<date>	The current date in yyyy/mm/dd format
<time>	The current time in h24:mm format.

This command also disables the NTP service if it was enabled

show time

Shows the current date and time, configured time zone and NTP servers. Output from this command is similar to the following:

```
Timezone:     America/Los_Angeles
NTP Service:  Disabled
NTP Servers:  None
Time:         2002/11/26 17:22
```

SNMP Configuration and Reporting Commands

Note: *The 700wl Series system supports MIB 2-compliant MIB objects.*

Note: *The 700wl Series system SNMP agent only provides read-only access to the MIB. Therefore, you cannot set or clear MIB objects such as sysLocation or sysContact from an external manager via SNMP. You must modify these objects through the web-based administrative interface or the CLI.*

set snmp on | off

Turns SNMP support on or off. Turning SNMP on enables read-only access to the MIB.

Turning it on when already on, or off when already off has no effect. By default, SNMP support is off.

set snmpport <port>

Sets the SNMP port. By default, the SNMP port is 161.

clear snmpport

Resets the SNMP port to the default, port 161.

add snmpmanager <hostname> | <ip-address> [/<maskbits>]

Specifies an authorized SNMP manager by hostname, IP address, or subnetted IP address that can query for SNMP responses.

You can specify up to four authorized SNMP managers by repeating the **add snmpmanager** command. If you try to add a fifth manager, you will receive an error message.

<hostname>	The hostname of an SNMP management system.
<ip-address>	The IP address of an SNMP management system.
<maskbits>	A subnet mask that defines a range of addresses for the SNMP management system, specified as the number of bits in the mask. For example, /30 is the equivalent of 255.255.255.252; /24 is the equivalent of 255.255.255.0.

delete snmpmanager all | <hostname> | <ip-address> [/<maskbits>]

Deletes an authorized manager, or all of them.

set snmplocation <location>

Sets the SNMP sysLocation object defined in RFC 1213 as "the physical location of this node (for example, telephone closet, 3rd floor)."

Note: *You cannot set this object from an external manager via SNMP.*

clear snmplocation

Clears the SNMP sysLocation object.

Note: *You cannot clear this object from an external manager via SNMP.*

set snmpcontact <contact>

Sets the SNMP sysContact object, defined in RFC 1213 as "the textual identification of the contact person for this managed node, together with information on how to contact this person."

Note: *You cannot set this object from an external manager via SNMP.*

clear snmpcontact

Clears the SNMP sysContact object.

Note: *You cannot clear this object from an external manager via SNMP.*

set snmpcommunity <community>

Sets the SNMP read community string. The default is public. HP strongly recommends that you change the community string. This is also used for traps.

clear snmpcommunity

Clears the SNMP community string.

add snmptrapreceiver <ip-address>

Specifies an IP address to receive traps.

You can specify two trap receivers, by executing this command twice. If you try to specify a third trap receiver, you will receive an error message.

delete snmptrapreceiver all | <ip-address>

Deletes a specified trap receiver, or both trap receivers.

set snmpauthtraps on | off

Enables or disables the generation of authentication traps.

show snmp

Shows the current SNMPv1 configuration. Output is similar to the following example:

```
SNMP:                 Disabled
  SNMP Access Mode:     Read Only
  Community Name:       public
  SNMP Port:            161
  Location:             ServerCloset Bldg2
  Contact Info:
  Device Name:          192.168.10.174
  Authentication Traps: Enabled
  Trap IP Address:      None
  Authorized Managers:  None
```

NETWORK ACCESS CONTROL CONSOLE D

This appendix explains how to configure and use the Network Access Control Console enabled by the HP ProCurve Secure Access 700wl Series. It includes the following sections:

Network Access Control Console Overview D-1

Configuring Network Access Control D-2

The Group Membership Retrieval API D-5

Using the Network Access Control Console D-7

Network Access Control Console Overview

As educational institutions deploy wireless services throughout their campus environments, the ability to provide specific and differentiated access to users throughout the day is a valuable feature. One use of this is to set up groups for specific classes, that are enabled during class meeting times, and that provide access to specific sets of information used during the class -- lecture notes, articles, illustrations, self-paced exercises, and so on. However, during a test, an instructor may want to temporarily prevent students from accessing those resources, or temporarily disable network access entirely.

The Network Access Control Console is a separate interface from the regular 700wl Series administrative interface. It allows a non-administrator user to dynamically and temporarily change the rights associated with a particular group. For example, if a group is used to provide access to specific resources for a particular class, the Network Access Control Console allows the instructor to temporarily change the access rights for the members of that class group during a test period. Access can be changed to disallow all network access, or it can be changed to “borrow” a set of access rights from another group.

Groups must be configured appropriately within the Rights Manager Administration Interface to enable dynamic rights management through the Network Access Control Console. Once the groups have been configured, an instructor can access the Network Access Control Console and manage his group’s rights without needing Administrator access to the 700wl Series Rights Manager.

In addition, if Group Membership retrieval has been set up through an XML-RPC service, the Network Access Control Console can display all the users who are members of the affected group, with their current logon status. The instructor can view the list and log off a student.

There are several steps involved in configuring the Network Access Control Console:

- Make sure that groups are set up for any classes or other activity periods for which you want to be able to temporarily modify access rights.

- Set up any groups needed to define sets of temporary rights. The “No Access” group, which denies all network access, is predefined, so you do not need to set up a group for that. However, you must make sure you add the No Access group to the appropriate location.

  If the No Access group is not allowed at a location, then the No Access setting will use the Logon group as the source of temporary rights, and users will be redirected to the Logon page with every access attempt.

- Configure the Network Access Control Console through the Network Access Control Console Configuration page:

  — Through the Network Access Control Console Configuration page, add the groups you want to modify to the Groups with Console Access list. You will need to give them passwords as part of this process. The group’s password must be provided in order to change the group’s rights through the Network Access Control Console.

  Note: *If no groups are added to the Groups with Console Access list, you will not be able to access the Network Access Control Console (the Stop page will appear when you attempt to log in).*

  — Also through the Network Access Control Console Configuration page, specify the groups who rights should be available to be “borrowed for use by another group”.

  — Enable the Network Access Control Console feature.

Configuring Network Access Control

To enable the dynamic assignment of rights through the Network Access Control Console, there are several things an administrator must do:

Step 1. Set up the “normal” groups and configure them with their normal access rights. Typically this is done when setting up the system for user authentication and authorization.

Step 2. If you want to define a specific set of rights to be granted on a temporary basis, set up a group that defines those rights.

Step 3. Make sure your optional groups are allowed at the appropriate locations, and the “No Access” group as well.

Step 4. Enable the Network Access Control Console feature. This involves specifying which groups may be access through the Network Access Control Console, specifying passwords for those groups, and specifying the groups from which rights may be “borrowed.”

Configuring Groups for Use with the Network Access Control Console

In a typical case, a group is set up for a specific class that defines access rights used during normal class periods. If the instructor simply wants to disallow all access to the network periodically, no other groups are necessary, as there is a predefined setting in the Network Access Control Console for “No Access.” In some cases, however, the instructor may not want to disable all access, but instead may want to temporarily assign a different set of access rights to the members of his class group. In this case, a second group can be set up

specifically for this purpose — defining a set of access rights that can be substituted through the Network Access Control Console.

For example, a group called “Math101” could define the rights granted to class members normal Math class periods. To define a different set of rights to be granted during a test period, a second group called “MathTest” can be created that has the rights that should be in effect during a test.

In addition, to allow access from the Network Access Control Console, the group “Math101” must be password protected. The group password is used to authenticate the access to the group for the purpose of changing its rights.

Configuring the Network Access Control Console

To enable and configure the Network Access Control Console feature, do the following:

Step 1. From the Rights Manager Configuration menu, click **Network Access** under the Control Console heading.

The Network Access Control Console configuration page is displayed (Figure D-1).

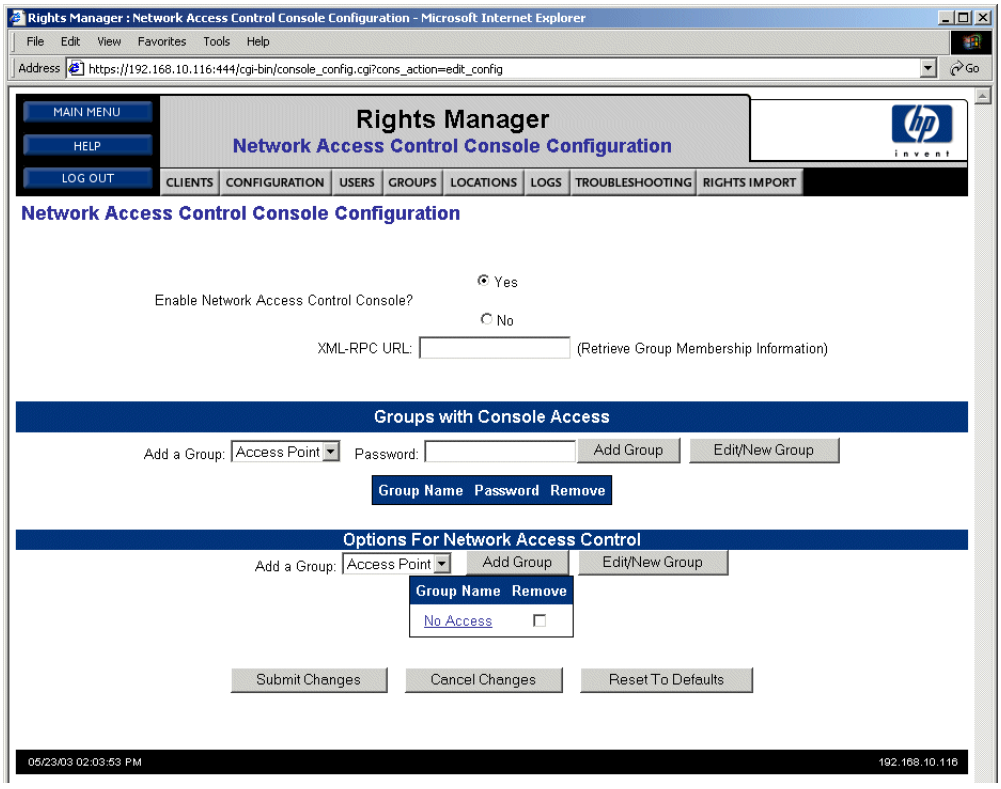

Figure D-1. Network Access Control Console Configuration

Step 2. To enable the Network Access Control Console, click **Yes**.

To disable it, click **No**.

Step 3. If you want to retrieve lists of group members from an external XML-RPC service, type the URL of the service in the **XML-RPC URL** field.

Groups with Console Access

Step 1. Add passwords for any groups that you want a non-administrator user to be able to access from the Network Access Control Console in order to dynamically change their rights:

a. Select the group in the Add A Group drop-down list.

b. Type the group password into the **Password** field. This password will need to be provided to the Network Access Control Console to allow the rights for the group to be modified.

c. Click **Add a Group** to add this group to the list of groups accessible from the Network Access Control Console.

If you need add or edit a groups, click **Edit/New Group** or click the group name. This takes you to the Group Editor. Note that when you have finished with the Group Editor, you will need to navigate your way back to the Network Access Control Console configuration page and enter your settings again.

Step 2. To mark a group for removal from the list of groups that allow Network Access Control Console access, click the checkbox in the Remove column for that group. The group is removed when you submit your changes.

Options for Network Access Control

Step 1. To add a group to the list of groups that can be used as a source of substitute rights, select a group from the drop-down list, and click **Add a Group**.

The *No Access* group is included in this list by default, and cannot be removed.

The groups in this list will be available in the **Select New Access** drop-down list that appears in the Network Access Control Console.

If you need add or edit any groups, click **Edit/New Group** or click the group name to go to the Group Editor.

Step 2. Click **Submit Changes** to have your changes take effect.

Click **Cancel Changes** to cancel any changes you have not yet submitted.

When you have finished this process, you will be able to use the Network Access Control Console to modify the rights of any of the groups you have specified in the Groups with Console Access list.

Figure D-2 shows the Network Access Control Console configuration page configured to allow an instructor to change access permissions for group *Math101*. Permissions can either be changed to those defined for the group *MathTest*, or to *No Access*.

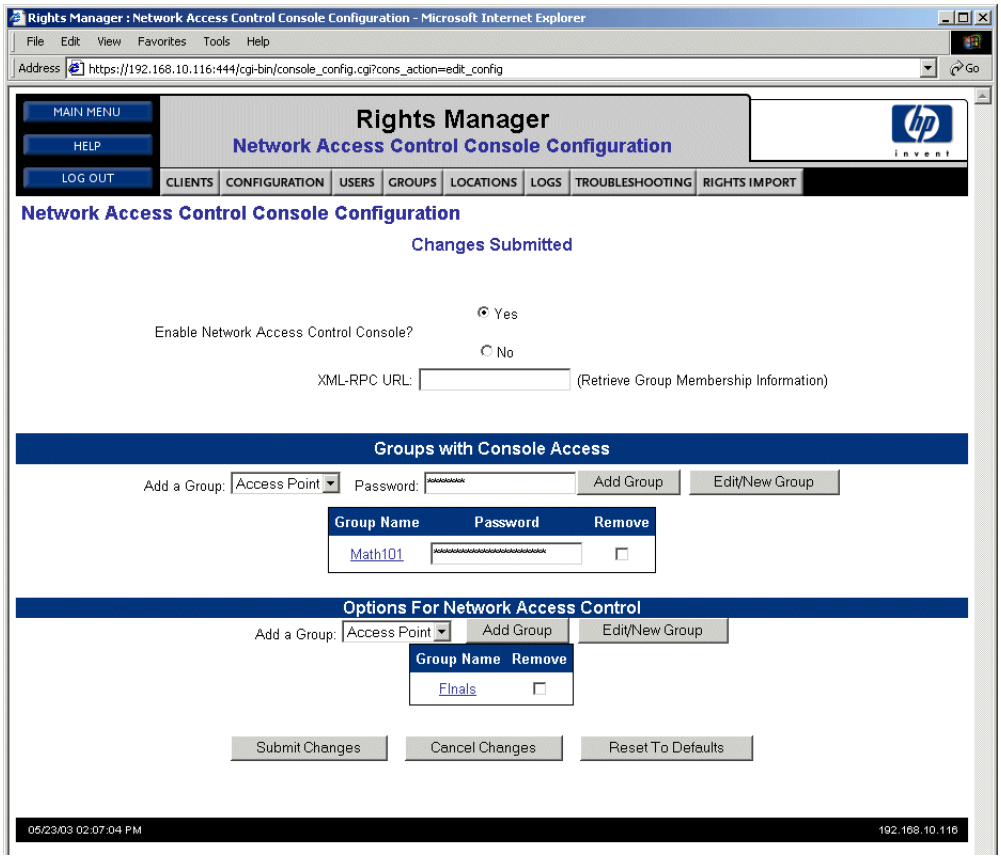

Figure D-2. Network Access Control Console configuration for Math101

The Group Membership Retrieval API

In order to retrieve group membership information for a group being managed through the Network Access Control Console, you must be running an XML-RPC service on the external system from which you want to obtain the group membership information. This service must accept a `getMemberList` methodCall from the Group Membership Retrieval API, and return the appropriate messageResponse.

If you are using XML-RPC for student authentication and user profile retrieval, that service should also be able to accept and respond to the getMemberList methodCall. See “The XML-RPC Service” in Chapter 9 for more information about the XML-RPC service.

The `getMemberList` call to be made by the Network Access Control Console is defined as follows:

```
getMemberList (groupname, randomstring)
```

These parameters are shown in Table D-1:

Table D-1. Parameters for authenticate call

Parameter	Type	Description
groupname	string	The group name that was used to login to the Network Access Control Console
randomstring	string	Currently not used, but parameter must be present. Can be any string or a null string.

The following is an example of an XML-RPC request to retrieve the members of group "math101":

```
<?xml version="1.0"?>
<methodCall>
<methodName>getMemberList</methodName>
<params>
     <param><value><string>math101</string></value></param>
     <param><value><string>random_string</string></value></param>
</params>
</methodCall>
```

The response is defined as follows:

```
getMemberList response (result, Members, hashed_string)
```

The response is a structure that contains name-value pairs as shown in Table D-2:

Table D-2. Name/Value pairs returned by authenticate response

Name	Type	Value and Description
result	integer <i4>	0 = groupname not found 1 = groupname found
Members	array of strings	An array of strings, each of which contains a MemberId and a MemberName. Members are name-value pairs as follows:
MemberId	string	The user ID from the 700wl Series system login page.
MemberName	string	The full name of the user, in the format "Lastname, Firstname".
hashed_string	string	Currently not used, but parameter must be present. Can be any string or a null string.

The following is an example of an XML-RPC authentication response to the `getMemberList` request for group `math101` that has two users, `Jane Doe` and `Sam Doe`:

```
<?xml version="1.0"?>
<methodResponse>
<params>
<param><value><struct>
       <member><name>result</name>
             <value><i4>1</i4></value>
       </member>
       <member><name>Members</name>
         <value><array>
           <data>
              <value><struct>
                <member><name>MemberId</name>
                  <value><string>jdoe</string></value>
                </member>
                <member><name>MemberName</name>
                  <value><string>Doe, Jane</string></value>
                </member>
              </struct></value>
              <value><struct>
                <member><name>MemberId</name>
                  <value><string>sdoe</string></value>
                </member>
                <member><name>MemberName</name>
                  <value><string>Doe, Sam</string></value>
                </member>
              </struct></value>
           </data>
         </array></value>
       </member>
       <member><name>hashed_string</name>
           <value><string>dF23$fI</string></value>
       </member>
</struct></value></param>
</params>
</methodResponse>
```

Using the Network Access Control Console

The Network Access Control Console lets you temporarily and dynamically change the rights for a group. You can do this by denying all access, or by assigning the rights from another group to your group.

The newly assigned rights take effect immediately, and expire at a time you specify, but not later than midnight of the same day as you assign them. This is accomplished by aliasing the original group to a second group that defines the rights that you want to be assigned temporarily to the original group.

You do not need administrator access to the HP ProCurve Integrated Access Manager or Access Control Server to run the Network Access Control console. You need to know only the following:

- The hostname or IP address of the Access Control Server or Integrated Access Manager where the group is configured.
- The name of the group for which you want to change rights, and its password.

This feature assumes that groups have already been set up by a network administrator, that the Network Access Control Console feature has been enabled, and that the groups you want to modify have been added to the Groups with Console Access list through the Network Access Control Console Configuration page within the Rights Manager.

Because the substitute rights take effect immediately and always expire no later than midnight of the same day, you cannot implement the substitution prior the to day on which it is to take effect. Typically you would initiate the rights substitution immediately prior to the time you want it to take effect.

To temporarily change the rights for a group, do the following:

Step 1. From your web browser, enter the URL for the Network Access Control Console:

`http://<host>/console`

<host> is the hostname or IP address of your Access Control Server or Integrated Access Manager.

The Network Access Control Console login page appears, as shown in Figure D-3

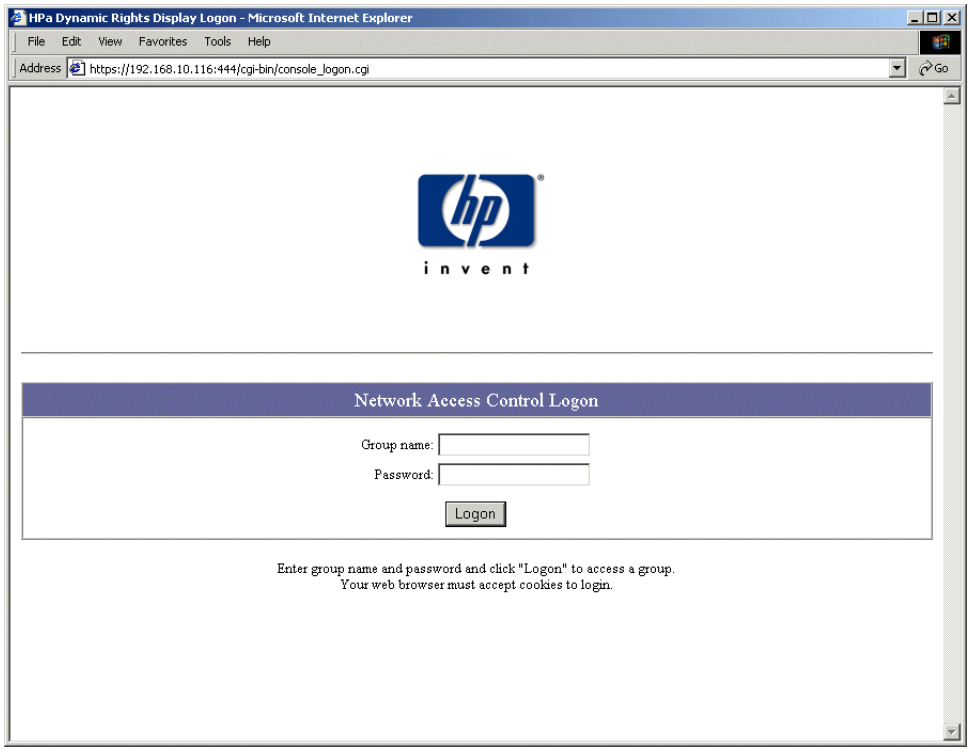

Figure D-3. The Network Access Control console login page

Step 2. Enter the group name and group password in the appropriate fields and click **Login**

For example, to temporarily change the rights for group *Math101*, enter *Math101* and its group password into the two fields, and click **Login**.

The Network Access Control Console page appears, as shown in Figure D-4.

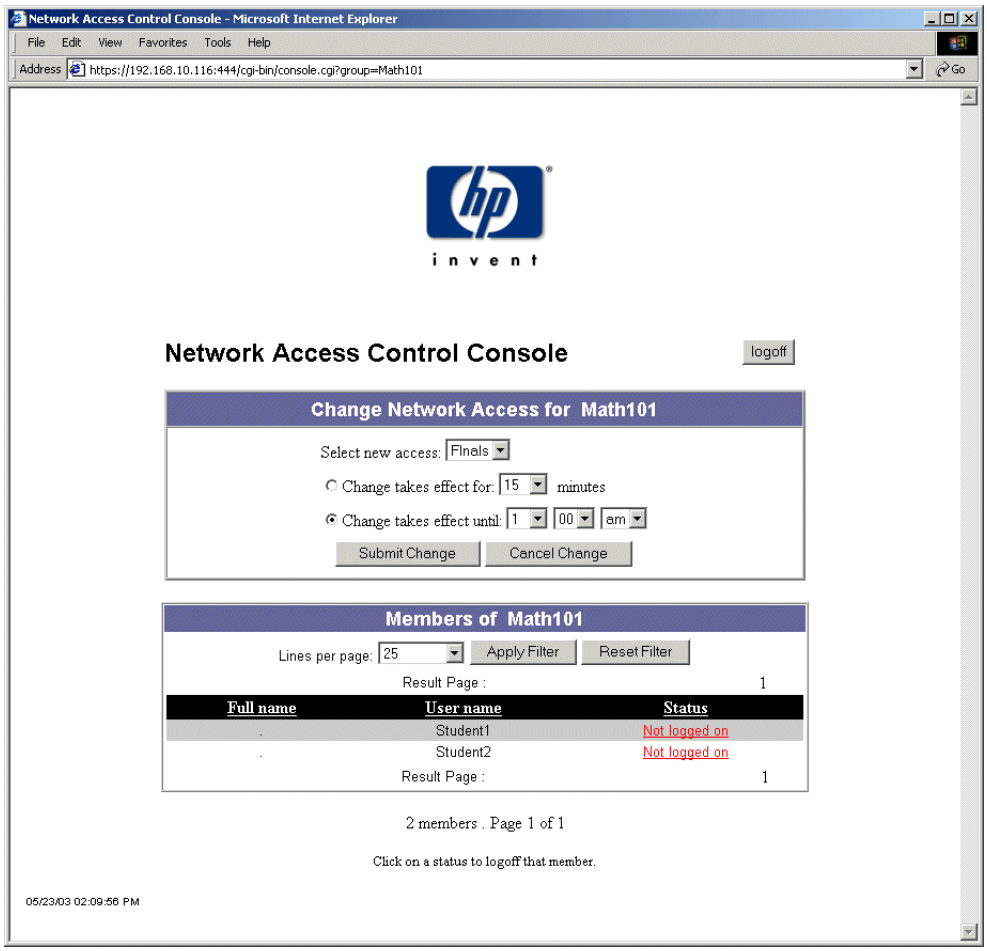

Figure D-4. The Network Access Control console page for group "Math101"

The Network Access Control Console page is divided into two parts.

- At the top of the page, you can select a new set of access rights for the group, and specify the length of time that these rights should remain in effect.
- In the lower part of the page, users who are members of the selected group are presented in a table, if the Network Access Control Console was able to retrieve a list of group members. This list is primarily useful if members are retrieved through the XMLRPC getMemberList API.

To change the group's access rights, do the following:

Step 1. In the **Select New Access** field, select from the drop-down list the set of access rights that should be temporarily assigned to the original group.

If you select **No Access**, users in the group will be redirected to the Stop page upon each access attempt for the duration you specify.

If you select another group from the drop-down list, the access rights associated with that group are "borrowed" temporarily for the original group.

In the example shown above, *MathTest* is selected as the set of rights that should be substituted for the rights normally associated with group *Math101*.

Note: *Make sure the group you select is allowed at the appropriate location. If you select* **No Access** *and the No Access group is not allowed at the relevant location, then the Logon group is used as the source of temporary rights and users will be redirected to the Logon page upon each access attempt rather than to the Stop page.*

Step 2. Select either a duration (in minutes) or enter a fixed expiration time for these rights.

a. To select a duration, click **Change takes effect for:** and select a duration from the drop-down list.

b. To select a fixed expiration time, click **Change takes effect until:** and set the time at which these rights should expire using the drop-down fields.

Temporary rights will not remain in effect past midnight of the same day that you initiate them.

Note: *The temporary rights take effect at the time you configure them, so if you configure a duration, make sure it is sufficient to last throughout the entire period that the temporary rights should be in effect.*

In our example, assuming that the class period for Math101 is 10:00 to 11:30 am, you could set these rights to a fixed expire time of 12:00 noon (pm). Alternatively, if you implement the change at the start of the class period, you could set it to a duration of 90 minutes.

Step 3. Click **Submit Change** to have this take effect, or **Cancel Change** to cancel the operation.

Submitting your change refreshes the rights for every member of the group who is currently authenticated. Members who log in after the access change has taken effect are given the new temporary set of rights.

Group Membership

The group members table shows the status of members of this group if you configured the Network Access Control Console to retrieve group membership from an external XML-RPC service, or if you have users entered in the Rights Manager's built-in database who are members of this group.

If group membership information has been retrieved from the external XML-RPC service, users' full names can be displayed in addition to their user logon name and status ("Logged on" or "not logged on").

If the Network Access Control Console cannot retrieve group members from an XML-RPC service or from the built-in database, then the member table does not appear.

You can log off individual users in the Members of group list by clicking on the status link for that user.

GLOSSARY

E

The glossary defines terms that are used throughout the 700wl Series system. Some of the following terms are in common usage but have 700wl Series system-specific meanings. These terms are defined in context in the chapter where they first appear.

Access Controller	A 700wl Series system device positioned between each access point and the network. It inspects and filters each packet arriving from the wireless client through the access point, deciding whether to allow or deny forwarding of the packet. The Access Controller functionality is also included in the Integrated Access Manager.
Access Control Server	A logical device that performs two functions: 1) Coordinates between the Access Controllers and the Rights Manager. 2) Coordinates Access Controller-to-Access Controller communications, such as a roaming handoff.
Access Points group	A group that may contain only MAC address users that are Access Points. This group defines a set of rights for the Access Points connected to the system through one or more Access Controllers.
Allows	Filters that identify client packets that are permitted to be passed by the Access Controller.
Authentication	A means of proving that a client is who it claims to be through use of a password or shared secret.
Authentication realm	A named, ordered set of authentication services used to perform user logon authentication for a set of clients.
Authentication service	A single instance of a service used for authentication, such as a specific Active Directory service, or specific RADIUS server.
Client	A machine, device, or user of the 700wl Series system.
Default realm	The authentication realm currently being used to perform web-based user authentication in most circumstances.
Downlink port	A port on an Access Controller or Integrated Access Manager to which a device at the network edge, such as a Wireless Access Point, switch, or hub, is connected.
Expire time	A timer that determines how long before a user must re-authenticate.
Everywhere else	The Rights Manager location that a client belongs to if it does not associate with any other location. Until you create another location, this is the location to which *all* clients are associated.
Group	A named entity that defines a set of access rights (Allows and Redirects) and other properties for users who are members of the group.

Guest user	A client who is authenticated as a member of the Guest group, and are granted Guest access rights. Clients who click the Guest button on the logon page become members of this group.
Implicit user	A user who is a member of the default group to which authenticated users belong. If the Implicit User group is allowed at a location, Implicit User rights are the default set of access rights given to all users at that location, in addition to any rights they may get through membership in other allowed groups.
Integrated Access Manager	A unit that combines the Access Control Server and Rights Manager with an Access Controller.
Linger time	A timer that controls how long before a client must re-authenticate after being disassociated from an Access Controller.
Location	A set of *where*s (Access Controllers or Access Controller ports) and other properties that define how client connections are set up, authenticated and granted access rights.
Logon user	A client who has not yet logged on, and has only Logon access rights.
MAC Address user	A client that is identified by its MAC address rather than a user name. Access Points are a special type of MAC address user.
Management Information Base (MIB)	A specification of a collection of objects (or data) that exists in a network device. MIBs are used primarily with network management systems using SNMP.
Network Address Translation (NAT)	A means of providing a private IP address space to a set of devices. The source addresses are then rewritten in packets that are forwarded to the network. Network Address Translation on the 700wl Series system platform implies Port Address Translation (PAT).
Normal group	An administrator-defined group that specifies a set of rights, determined by the administrator, and to which the administrator can assign users as members. (Membership in all other group types is determined by the 700wl Series system based on the client's authentication status).
Packet filters	Determine what client traffic an Access Manager will allow onto the network based on the client's rights.
Port Address Translation (PAT)	in conjunction with NAT, provides a private IP addess space to a set of devices. PAT rewrites the source port number before forwarding packets on to the network.
Real IP address	An IP address that is used as presented, and is not translated using NAT. May be a static IP address, or may be obtained using DHCP.
Realm	See Authentication Realm.
Redirects	Filters that identify and change the destination of client packets.
Rights Manager	The component of the 700wl Series system that allocates access rights to clients, and may also authenticate clients.
Roaming	The act of moving from one wireless access point to another.
Service	See Authentication service.
Session redirectors	Client TCP and UDP sessions can be redirected from their original destination IP address or port.
Static IP address	An IP address that is not obtained via a DHCP server, but that is configured directly on the device, and does not change unless specifically reconfigured.

Uplink port	The Ehternet port used to connect the 700wl Series system to the network. By default this is the built-in 10/100 or 10/100/100 port, but it can be reconfigured to be a different port.
When	A set of valid times that apply to a location or a group.
Where	An Access Controller, an Access Controller port, or a MAC address.
Wireless Data Privacy	The ability to encrypt all client traffic using standard encryption technology such as PPTP, L2TP, and IPSec.

INDEX OF COMMANDS

A

add bridging <pre-defined-type> | <quoted-custom-bridging-string> C-11
add snmpmanager <hostname> | <ip-address> [/<maskbits>] C-28
add snmptrapreceiver <ip-address> C-30

C

cancel backup C-20
cancel upgrade C-22
clear admin C-3
clear am httpproxy all | mac <mac-address C-14
clear am tunnel all | mac <mac-address C-17
clear controlserver C-11
clear dhcpserver C-7
clear dns C-8
clear domainname C-6
clear gateway C-7
clear hostname C-6
clear ipsecsecret C-16
clear logs C-25
clear natdhcp C-15
clear ntpserver C-27
clear portip <port> | <slot>/<port> C-10
clear portmedia <port> | <slot>/<port> C-9
clear sharedsecret C-8
clear snmpcommunity C-29
clear snmpcontact C-29
clear snmplocation C-29
clear snmpport C-28
clear syslogserver C-14
clear upgradeproxy C-22
create backup C-19

D

debug interface [<slot>/<port>] C-26
debug ip [<slot>/<port>] C-26

debug tcpport <tcp port> [<slot>/<port>] C-26
delete am mac <mac-address> C-13
delete bridging <pre-defined-type> | <quoted-custom-bridging-string> C-11
delete snmpmanager all | <hostname> | <ip-address> [/<maskbits>] C-29
delete snmptrapreceiver all | <ip-address> C-30

F

factoryreset C-23

G

get backup <url> C-20
get upgrade <url> <key> [reboot | version | mindowngrade] C-20

H

help [diag | help | ipsec | snmp] C-3

L

logoff client {all | mac < mac-address> } C-19

N

nslookup <hostname> C-25

P

ping {<ip-address> | <hostname>}. C-26

R

reboot [upgrade | downgrade | same] C-23
restore backup C-20

S

set admin <login-name> [<password> <password>] C-3
set am httpproxy mac <mac-address <proxy-ip> <proxy-port> C-14
set am tunnel mac <mac-address> {dhcp | range <ip-address1> <ip-address2>} C-17
set bridging on | off C-11
set clientprobes <interval> <timeout> C-12
set controlserver <ip-address> C-10
set datetime <date> <time> C-28
set dhcp on | off C-7
set dhcpserver <ip-address> C-7
set dns <primary-ip-address> [<secondary-ip-address>] C-7
set domainname <domainname> C-6

set espencryption [des] [3des] [blowfish] [cast] [aes] [none] C-16
set espintegrity [md5] [sha1] [none] C-16
set forwardipbroadcasts { none | <port-list>} C-12
set gateway <ip-address> C-7
set hostname <hostname> C-6
set ikedh [group1] [group2] [group5] C-16
set ikeencryption [des] [3des] [blowfish] [cast] C-16
set ikeintegrity [md5] [sha1] C-16
set ip { <ip-address> [<netmask>] | <ip-address>/<maskbits> } C-6
set ipsec on | of} C-16
set ipsecsecret [<secret> <secret>] C-15
set l2tp on | off C-15
set natdhcp <ip-address> <subnetmask> [<lease-time> [<time-units>]] C-15
set ntp on | off C-28
set ntpserver{< ip-address> | <hostname>} [<ip-address> | <hostname>] C-27
set portip { <port> | <slot>/<port> } <ip-address> <netmask> C-10
set portmedia {<port> | <slot>/<port>} "<media> [<media-option>]" C-9
set pptp on | off C-15
set remote on | off C-4
set sharedsecret [<secret> <secret>] C-8
set snmp on | off C-28
set snmpauthtraps on | off C-30
set snmpcommunity <community> C-29
set snmpcontact <contact> C-29
set snmplocation <location> C-29
set snmpport <port> C-28
set ssh on | off C-16
set syslogserver <ip-address< [<facility>] C-14
set timezone <general-tz> <specific-tz> C-27
set upgradeproxy [on | off] [host <ip-address> [<port>]] [user <user> [<password>]] C-22
set uplink [<slot>/<port>] C-8
show admin C-3
show airwave C-16
show am [httpproxy | tunnel] [mac <mac-address>] C-13
show backup C-20
show bridging C-11
show client mac <mac-address> [rights] C-18
show clientprobes C-12
show clients [mac <mac-address>] [sort {mac | ip | user | machine | port | sessions | idle}] [reverse] C-17
show controlserver C-11
show deviceport <device> C-5
show dhcpserver C-7
show ether [status] C-4
show forwardipbroadcasts C-13
show id C-4

show ip C-7
show logs [<severity>] [max <lines>] [for <count> <time-units>] [search <quoted-text>] [reverse] C-24
show natdhcp C-15
show portip C-10
show portmedia <port> | <slot>/<port> C-9
show product C-5
show remote C-4
show serial C-5
show sharedsecret C-8
show slots C-5
show snmp C-30
show status C-4
show syslogserver C-14
show time C-28
show upgrade C-22
show upgradeproxy C-23
show uplink C-8
show version C-6
shutdown C-23
store backup <url> [<filename>] C-19

T

traceroute {<ip-address > | <hostname>} [<hops> [<probes> [<probewait>]]] C-27

INDEX

Symbols

@DNS@ built-in address 7-25
@INTERNAL@ built-in address 7-25
@INTRANET@ built-in address 7-26
@SERVER@ built-in address 7-26

Numerics

802.1x logon 9-2, 9-39

A

Access Control Server 1-3
  configuration propagation to Access Controllers 2-2
  configuration via CLI C-13
Access Controller 1-3, 8-12
  configuration propagation from Access Control Server 2-1
  configuration via CLI C-10
  viewing list of active 5-3
Access Managers list 5-3
Access Point
  client setup 6-22
Access Point group 6-4, 7-3
access rights 1-6, 6-3, 6-8
  and groups 6-4
  and HTTP proxy 7-4
  defining via groups 7-20, D-2
  No Access D-9
  substitute rights D-4, D-10
active client management commands C-17
active clients
  viewing from Main Menu 5-4
  viewing in Rights Manager 6-22
Active Directory service 9-9
active sessions
  viewing 5-7
adding
  Allows to a group 7-6, 7-13
  location 8-5
  Redirects to a group 7-6, 7-10
  Whens to a group 7-10
address variables
  built-in 7-25
Administrator login 2-2
  changing 2-5
advanced allow 7-29, 7-32
advanced allow filter 7-27
Advanced Encryption Standard (AES) 3-2
Advanced Network Configuration 2-9
advanced redirect filter 7-23, 7-25
All IP Traffic allow 7-14
Allow Editor 7-27, 7-30
Allow Static IP option 7-15
Allows 6-8, 7-27
  adding to a group 7-13
  advanced filter 7-27, 7-29, 7-32
  and distributed logon 7-19
  basic filter 7-27, 7-29
  creating 7-28
  defined 7-3
  deleting 7-30
  displaying in Groups Manager 7-5
  for centralized logon 7-19
  for centralized vs. distrubted logon 7-19
  list of predefined 7-14
  modifying 7-28
  removing from a group 7-14
  tcpdump expression in 7-29, 7-32
AM HTTP Logon redirect 7-11
AM HTTPS Logon page allow 7-14
AM HTTPS Logon redirect 7-11
AM Internal blocker redirect 7-11
AM Logon page shortcut redirect 7-11
AM Logon-forward no URI allow 7-14
AM Logon-fwd append URI allow 7-14
AM No SSL Web redirect 7-11
AM No Web redirect 7-11
AM SSL Stop page allow 7-14
AM Stop page allow 7-14
AppleTalk 2-12
AppleTalk allow 7-14
Audience xi
authenticate call response 9-18
authenticate methodCall 9-15, 9-17
authentication 1-5, 6-10, 9-1
  802.1x 1-5, 6-10, 9-39

802.1x logon 9-2
browser-based 1-5
browser-based logon 9-1
default realm 9-20
monitored logon 9-2, 9-39
NT Domain logon 1-5, 6-10, 9-2, 9-39
realm 9-2, 9-20
service 9-2
using Active Directory 9-9
using iPlanet directory service 9-10
using Kerberos 9-14
using RADIUS 9-12
using XML-RPC 9-15
web-based 6-10
wireless data privacy based 6-10
wireless data privacy logon 9-2
wireless data privacy-based 1-5
authentication realm 1-5, 6-11
authentication service 1-5, 6-11, 9-3, 9-16
Auto HTTP proxy 2-18
automatic HTTP proxy 7-4

B

backup and restore commands C-19
backup image
creating 4-1
restoring 4-4
saving 4-3
basic allow 7-29
basic allow filter 7-27
Basic redirect filter 7-24
basic redirect filter 7-23
Blackhole redirect 7-11
Blowfish 3-2
bridging 2-12
AppleTalk traffic 2-12
CDP traffic 2-12
WNMP traffic 2-12
broadcast IP packets 2-14
broadcasting
settings 2-14
browser-based logon 1-5, 9-1
Built-in authentication service 9-1
Built-in database 10-1
adding/modifying users 10-4

C

CAST 3-2
CDP and WNMP allow 7-14
CDP bridge traffic 2-12
centralized logon
Allows and Redirects for 7-19
configuration propagation to Access Controllers 2-2
Certicom/Movian 3-1
certificate
request 3-7
Certificate Authority 3-8
certificated-based IKE authentication 3-6
Cisco Discovery Protocol 2-12
Client IP Address Assignment options 7-15
client probe 2-13
interval 2-13
time-out counter 2-13
clients
Access Points 6-22
as group members 6-4
disassociating 2-13
logging off 6-22
probe settings 2-13
refreshing rights for 6-22
Clients page (Rights Manager) 6-22
Column Modifier page 7-7
Command Line
Access Control Server configuration commands C-13
Access Controller configuration commands C-10
active client management C-17
backup and restore commands C-19
Help C-3
network configuration C-6
SNMP configuration commands C-28
status commands C-4
stopping and restarting the system C-23
system access commands C-3
upgrading system software commands C-20
Command Line Interface C-1
accessing C-1
command syntax C-2
Configuration
overview of 2-1
configuring PKI for 3-6
Connection Type 2-14
creating
Allows 7-28
groups 7-8, 7-9
redirects 7-23
Whens 7-21
CS-to-AM Logon redirect 7-11
CS-to-AM Stop redirect 7-11
custom web pages
logo image types 9-27
logoff pop-up 9-31
logon page 9-28
logon/logoff page logo 9-27
removing templates 9-34
small browser image types 9-33
small browser support 9-33

Stop image types 9-30
stop page 9-30
template files 9-34
Customize Web Pages by Location page 9-26
customizing logon/logoff/stop pages 9-25

D

Data Encryption Standard (DES) 3-2
data integrity
ESP 3-6
Message Digest 5 (MD5) 3-2
Secure Hash Algorithm (SHA-1) 3-2
date/time configuration 2-24
default realm 9-20
Default router address
in network configuration 2-8
deleting
Allows 7-30
groups 7-20
Redirects 7-26
Deleting a Location 8-9
Deleting an Access Controller 8-12
DHCP
/30 setting 2-14
for NAT 2-13
Full subnet setting 2-14
Lease Time 2-14
Netmask for NAT 2-14
DHCP allow 7-14
DHCP Network for NAT 2-13
DHCP server
in network configuration 2-8
Diffie-Hellman public-key-interchange (PKI) 3-2
Diffie-Hellman settings 3-6
Disassociate clients time-out setting 2-13
disassociating a client 2-13
distributed logon
Allows and Redirects for configuration propagation to Access Controllers 2-2
DNS
in network configuration 2-8
DNS allow 7-14
Document Conventions xi
documentation
online 2-26
domain name
in network configuration 2-8
Dynamic IP mode 6-16

E

editing
groups 7-8
Redirects 7-23
Whens 7-21
enable Ethernet bridging 2-12
Enable Technical Support Access 2-6
Encapsulating Security Payload (ESP) 3-2
encryption
AES 3-2
Blowfish 3-2
CAST 3-2
DES 3-2
ESP 3-6
Microsoft Point-to-Point Encryption (MPPE) 3-2
RC4 3-2
Triple DES 3-2
ESP
encryption 3-6
integrity 3-6
EveryOtherTime When 7-21
Everywhere else 6-6
Everywhere else (location) 1-7
Expire timers 7-17

F

Fixed Expire 7-17
forward broadcast IP packets 2-14
Full DCHP Subnet setting 2-14

G

getMemberList
call response D-6
methodCall 9-17, D-6
Go To Rights Manager 6-18
Group Allows columns 7-7
Group Editor 7-8
properties 7-18
group membership display D-10
Group Membership Retrieval API D-5
group name 7-9
group password D-4, D-9
setting 11-4
Group Redirects columns 7-7
Group Type 7-10
Groups 6-3, 6-4, 7-1
Access Point type 6-4, 7-3
Allow Static IP option 7-15
Client IP Address Assignment optiond 7-15
client members 6-4
creating 7-8
deleting 7-20
editing 7-8
Expire timers 7-17
fixed expire timer 7-17
Guest group type 6-4
Guest type 7-2

Implicit Users group type 6-4
Implicit Users type 7-3
Linger timer 7-17
Logon group type 6-4
Logon type 7-3
Max concurrent logons setting 7-16
modifying 7-8
NAT Clients option 7-15
Never NAT setting 7-16
No Access group 6-4
No NAT except... option 7-15
Normal group type 6-4
Normal type 7-2
Override location max users setting 7-16
properties of 6-4, 7-2
relative expire timer 7-17
row color definitions 7-5
Stop group type 6-4
Stop type 7-3
types 7-2
viewing 7-4
VLAN Identifier 7-17
groups 9-15
defining student access rights 7-20, D-2
for console access D-4
for rights substitution D-4
information for rights assignment 9-16
Groups Manager 7-5
Column Modifier page 7-7
modifying columns 7-7
Groups page 7-4
Guest group 6-4, 7-2
Guest Registration page
template 9-34
Guest user
logon options 9-28
registered guest 9-25
Registered Guest option 9-28

H

Help
for CLI C-3
HTML format 2-26
online 2-26
PDF format 2-26
hostname
in network configuration 2-7
HTML Help 2-26
HTTP allow 7-14
HTTP logon redirect 7-12
HTTP Proxy
server configuration 2-18
HTTP proxy 7-4
HTTP Proxy, automatic 2-18
HTTPS Logon page allow 7-15
HTTPS logon redirect 7-12

I

Idle 5-8
IKE authentication method 3-5
IKE integrity 3-6
Image file for restore 4-5
Implicit Users group 6-4
Users group 7-3
Integrated Access Manager
configuration propagation to Access Controllers 2-2
Internal Admin UI allow 7-14
Internal blocker redirect 7-12
Internal HTTP allow 7-14
Internal rights UI allow 7-14
Internet Key Encryption (IKE) 3-6
Internet Key Exchange (IKE) 3-2
ip address
setting for Access Controller port 2-15
IP address for system 2-8
iPlanet directory service 9-10
IPSec 3-1, 3-6
and authentication 9-2
certificate configuration 3-6
certificate request form 3-7
clients
Certicom / Movian 3-1
Netscreen 3-1
PGP 3-1
SafeNet 3-1
configuration propagation to Access Controllers 2-2
configuring 3-4
Diffie-Hellman public-key-interchange (PKI) 3-2
Diffie-Hellman settings 3-6
Encapsulating Security Payload (ESP) 3-2
IKE authentication method 3-5
IKE integrity 3-6
Internet Key Encryption (IKE) 3-6
Internet Key Exchange (IKE) 3-2
shared secret 3-5

K

Kerberos 9-2, 9-14, 10-5
Kerberos allow 7-14
KERBEROS authentication
debugging 12-3
Kerberos protocol 9-15
Kerberos realm 9-15
Key Distribution Center 9-14

L

L2TP
- configuration propagation to Access Controllers 2-2
- configuring 3-11
- enabling 3-12

L2TP/IPSec 3-2
- and authentication 9-2

Layer 2 packets, bridging 2-12
layer 3 roaming 1-8
LDAP authentication
- debugging 12-3

Lightweight Directory Access Protocol (LDAP) 9-1
Linger timer 2-13, 7-17
Location 1-6, 6-2, 6-6
location
- adding 8-5
- maximum number of users 8-9
- NAT setting 8-9

Location descriptions 2-22
Location Editor 8-5
log file
- viewing 5-9

logging off clients 6-22
Login page 2-2
Logo
- customizing for web pages 9-27

Logoff page
- template 9-34

Logoff pop-up page 9-31
Logon group 6-4, 7-3
Logon page
- customizing 9-28
- template 9-34

Logon page shortcut redirect 7-12

M

MAC address 5-8
Management Information Base E-2
Max concurrent logons setting 7-16
Members and Implicit User rights setting 7-16
Message Digest 5 (MD5) 3-2
Microsoft Point-to-Point Encryption (MPPE) 3-2
modifying
- Allows 7-28
- groups 7-8
- Redirects 7-23
- Whens 7-21

Monitored logon 1-5, 6-10, 9-2, 9-39
MS-CHAP 3-2, 9-39
MS-CHAP v2 3-2

N

NAT Clients option 7-15
NAT mode 6-16
Netmask
- in network configuration 2-8

Netscreen 3-1
Network Access Control Console D-1
- configuration D-2
- group membership display D-10
- how to run D-7
- logging on D-8

Network Address Translation (NAT) 1-8, 7-15
- and VPN tunneling 6-18
- DHCP Setting for 2-13
- enabling per location 8-9
- NAT Clients option for groups 7-15
- Never NAT setting for groups 7-16
- No NAT except... option for groups 7-15

network configuration 2-6, C-6
- default router address 2-8
- DHCP server 2-8
- DNS 2-8
- domain name 2-8
- hostname 2-7
- IP address 2-8
- netmask 2-8
- obtain IP address via DHCP 2-8

network management 2-20
Never NAT for groups 7-16
New Group 7-9
New Location 8-5
No Access predefined group 6-4
No external rights UI redirect 7-11
No internal admin UI redirect 7-11
No internal rights UI redirect 7-11
No NAT except for clients on the wrong subnet option 7-15
No SSL internal UI redirect 7-12
No SSL Web redirect 7-12
No Web redirect 7-12
Normal group 6-4, 7-2
NT Domain logon 9-2, 9-39
- enabling 7-10
- setting for groups 7-10

NTP server 2-25

O

Obtain IP Address via DHCP 2-8
Online documentation/help 2-26
OpenSSL 11-21
Outside World allow 7-14
Override location max users settings 7-16

P

password for group D-4, D-9
PDAs
  logon page options 9-33
PDF Help 2-26
Ping allow 7-14
PKI
  configuring for IPSec 3-6
PKI certificates
  generating 3-6
Point-to-Point Tunneling Protocol (PPTP) 3-2
port
  built-in variables 7-25
  Reserved 2-11
port settings
  Connection Type 2-14
  in advanced network configuration 2-14, 2-15
PPTP 3-2
  and authentication 9-2
  configuration propagation to Access Controllers 2-2
  configuring 3-11
  enabling 3-12
predefined Allows 7-14
predefined Redirects 7-11
Pretty Good Privacy (PGP) 3-1
probe, client 2-13
Protocol 5-8

R

RADIUS accounting 9-13
RADIUS authentication
  debugging 12-4
RADIUS authentication service 9-12
RC4 encryption algorithm 3-2
Real IP mode 6-16
realm 1-5, 6-11, 9-2, 9-20
Redirect Editor 7-23, 7-27
Redirects 6-8, 7-23
  adding to a group 7-10
  advanced filter 7-23, 7-25
  and distributed logon 7-19
  basic filter 7-23, 7-24
  built-in address and port variables 7-25
  creating 7-23
  defined 7-3
  deleting 7-26
  displaying in Groups Manager 7-5
  for centralized logon 7-19
  for centralized vs. distributed logon 7-19
  list of predefined 7-11
  modifying 7-23
  removing from a group 7-11
  tcpdump expressions 7-25
refresh client rights 6-22
Registered Guest 9-25
Relative expire 7-17
Release Notes 2-26
Remote Authentication Dial-in User Service (RADIUS) 9-1
Remote Profiles API 9-17
removing
  Allows from a group 7-6, 7-14
  groups 7-20
  Redirects from a group 7-6, 7-11
  Whens from groups 7-10
Reserved port 2-11
Rights 1-6
Rights Manager 1-4, 6-1, 6-18
  accessing 6-18
  diagram 6-2
  logout 6-21
  overview 6-1
  terminology 6-3
roaming 1-8

S

SafeNet 3-1
Secret 9-50
Secure Hash Algorithm (SHA-1) 3-2
serial console
  CLI C-1
  exiting C-2
service 1-5, 6-11, 9-2, 9-3
session log
  configuration propagation to Access Controllers 2-2
  enabling 2-24
  setting up 2-23
  viewing 5-11
shared secret 2-2
  for IPSec 3-5
  for PPTP/L2TP 9-39
  for RADIUS 9-13
  setting for Access Control Server 2-16
  setting for Access Controller 2-17
shut down system 4-10
small browser web page option 9-33
SMB allow 7-14
SNMP
  configuration via CLI C-28
  configuring 2-20
  enabling 2-21
  management console configuration 2-21
  MIB support 2-20
  settings 2-21
  traps 2-21
SOCKS redirect 7-12

SSH
and authentication 9-2
configuration propagation to Access Controllers 2-2
SSL certificate
warnings 2-8
SSL Certificate Signing Request 11-18
SSL Stop Page allow 7-15
Static IP mode 6-16
status commands C-4
Stop group 6-4, 7-3
Stop page
customizing 9-30
template 9-34
Stop Page allow 7-15
stopping and restarting the system through CLI C-23
student profile 7-20, 9-15
Syslog server 5-11
for session logging 2-24
system access commands C-3

T

tcpdump expression 7-25, 7-29, 7-32
Technical Support
enabling access for 2-6
Terminology
for the Rights Manager 6-3
time zone configuration 2-24
time/date configuration 2-24
Triple DES 3-2

U

upgrading system software
through CLI C-20
user authentication 9-1
User Editor 10-4
User Manager 10-6
User Name 10-5

V

VeriSign 11-21
View Active Clients page 5-4
Viewing
groups 7-4
viewing
active Access Controllers 5-3
active clients (Main Menu) 5-4
active clients (Rights Manager) 6-22
Virtual LANs (VLANs) 1-9
VLAN Identifier
in Groups 7-17
VLANs
setting ID per group 7-17
VPN Security
considerations 3-3

W

warranty 1-ii
web page customization 9-25
changing the logo 9-27
custom template files 9-34
logo image types 9-27
logoff page pop-up 9-31
logon page 9-28
removing templates 9-34
small browser image types 9-33
Stop image types 9-30
stop page 9-30
Web-based logon 6-10
When 7-2
When Editor 7-21
Whens 6-7
adding to a group 7-10
creating or modifying 7-21
EveryOtherTime 7-21
example 6-3
removing from a group 7-10
Wheres
example 6-2
Wired Equivalent Privacy 3-1
wireless data privacy 1-5
considerations 3-3
necessity 3-3
performance and security 3-3
wireless data privacy logon 6-10, 9-2
wireless data privacy protocols 9-2
Wireless Network Access Protocol 2-12
wirelss data privacy logon 1-5
WNMP bridged traffic 2-12

X

XML-RPC
as authentication service 9-15, 9-16
authentication debugging 12-5
XML-RPC service 9-15, 9-17
XML-RPC transactions
Tracer results 12-5
XML-RPC-based service 9-2

© Copyright 2003 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice.

Edition 1, July 2003

Manual Part Number
5990-5988